Cisco ASA 시리즈 일반 운영 ASDM 구성 가이드

소프트웨어 버전 7.3

릴리스: 2014년 7월 24일
업데이트: 2014년 9월 16일

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
주소, 전화 번호 및 팩스 번호는
Cisco 웹사이트
www.cisco.com/go/offices에서 확인하십시오.

텍스트 파트 번호: N/A, Online only

Cisco ASA 시리즈 일반 운영 ASDM 구성 가이드

목 차

설명서 정보

문서의 용도

이 설명서는 ASDM(Adaptive Security Device Manager) 를 사용하여 Cisco ASA 시리즈의 일반적인 운영을 구성하는 데 참조할 수 있습니다. 여기서는 모든 기능을 다루기보다는 가장 대표적인 컨피그레이션 시나리오에 대해서만 설명합니다.

이 설명서에서 “ASA”는 달리 명시되지 않는 한 지원되는 모델을 총칭합니다.

참고 ASDM은 여러 ASA 버전을 지원합니다. ASDM 설명서와 온라인 도움말은 ASA에서 지원하는 모든 최신 기능을 다룹니다. 이전 버전의 ASA 소프트웨어를 실행하고 있다면 설명서에 포함된 기능이 해당 버전에서 지원되지 않을 수 있습니다. 또한 어떤 기능이 오래된 주 버전 또는 부 버전의 유지 보수 릴리스에 추가된 경우, ASDM 설명서는 그 기능이 나중에 출시된 일부 ASA 릴리스에서 제공되지 않더라도 그에 대해 설명합니다. 기능이 추가된 시점은 각 장의 기능 내역표를 참조하십시오. ASA 버전별 ASDM의 최소 지원 버전은 *Cisco ASA Series 호환성*을 참조하십시오.

관련 설명서

F자세한 내용은 *Cisco ASA 시리즈 설명서(Navigating the Cisco ASA Series Documentation,* http://www.cisco.com/go/asadocs)를 참조하십시오.

표기 규칙

이 설명서는 다음과 같은 표기 규칙을 사용합니다.

표기 규칙	표시
굵은 글꼴	명령, 키워드, 사용자가 입력하는 텍스트는 **굵은** 글꼴로 표시합니다.
기울임꼴	설명서 제목, 신규 용어 또는 강조된 용어, 사용자가 값을 지정해야 하는 인수는 *기울임꼴*로 표시합니다.
[ ]	대괄호로 묶인 요소는 선택 사항입니다.
{x | y | z }	필수 대체 키워드는 대괄호로 묶고 세로 선으로 구분합니다.
[x | y | z]	선택적 대체 키워드는 괄호로 묶고 세로 선으로 구분합니다.
문자열	따옴표 없는 문자의 집합입니다. 문자열 주변에 따옴표를 사용하지 마십시오. 그럴 경우 따옴표도 문자열에 포함됩니다.
`courier` 글꼴	시스템에 표시되는 터미널 세션 및 정보는 `courier` 글꼴로 표시합니다.
`courier` 굵은 글꼴	명령, 키워드, 사용자가 입력하는 텍스트는 **굵은 `courier`** 글꼴로 표시합니다.
`courier` 기울임꼴	사용자가 값을 지정하는 인수는 *`courier` 기울임꼴*로 표시합니다.
< >	비밀번호와 같이 인쇄할 수 없는 문자는 꺾쇠괄호 안에 표시됩니다.
[ ]	시스템 프롬프트에 대한 기본 응답은 대괄호 안에 표시됩니다.
!, #	코드 라인 시작 부분에 있는 느낌표(!) 또는 우물 정자(#)는 코멘트 라인을 나타냅니다.

참고 *독자가 주목해야 하는 내용*을 가리킵니다.

팁 *다음 정보가 문제를 해결하는 데 도움이 된다는 것*을 의미합니다.

주의 *독자가 유의해야 하는 내용*을 말합니다. 이 경우, 장비 손상이나 데이터 손실이 발생할 수 있으므로 주의해야 합니다.

설명서 받기 및 서비스 요청 제출

Cisco BST(Bug Search Tool)를 이용한 문서 확보, 서비스 요청 제출, 추가 정보 수집에 관해 알아보려면 *What's New in Cisco Product Documentation* (http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html)을 참조하십시오.

Cisco의 새로운 기술 문서 및 개정된 기술 문서를 모두 소개하는 *Cisco 제품 설명서의 새로운 소식*을 RSS 피드로 구독하면 콘텐츠가 데스크톱으로 곧바로 배달되어 리더 애플리케이션으로 읽어볼 수 있습니다. RSS 피드는 무료로 제공되는 서비스입니다.

파 트 **1**

ASA 시작하기

Cisco ASA 소개

릴리스: 2014년 7월 24일
업데이트: 2014년 9월 16일

Cisco ASA에서는 고급 스테이트풀 방화벽 및 VPN 집선 장치 기능을 하나의 디바이스에서 제공하며, 일부 모델의 경우 IPS 같은 통합된 서비스 모듈을 제공합니다. ASA에는 다중 보안 컨텍스트(가상 방화벽과 유사), 클러스터링(다중 방화벽을 단일 방화벽으로 통합), 투명(레이어 2) 방화벽 또는 라우팅(레이어 3) 방화벽 가동, 고급 감시 엔진, IPsec VPN, SSL VPN 및 클라이언트리스 SSL VPN 지원 등의 다양한 기능이 포함되어 있습니다.

참고 ASDM은 여러 ASA 버전을 지원합니다. ASDM 설명서와 온라인 도움말은 ASA에서 지원하는 모든 최신 기능을 다룹니다. 이전 버전의 ASA 소프트웨어를 실행하고 있다면 설명서에 포함된 기능이 해당 버전에서 지원되지 않을 수 있습니다. 또한 어떤 기능이 오래된 주 버전 또는 부 버전의 유지 보수 릴리스에 추가된 경우, ASDM 설명서는 그 기능이 나중에 출시된 일부 ASA 릴리스에서 제공되지 않더라도 그에 대해 설명합니다. 기능이 추가된 시점은 각 장의 기능 내역표를 참조하십시오. 각 ASA 버전에 대한 ASDM의 최소 지원 버전을 보려면 *Cisco ASA 호환성*을 참조하십시오. 1-19 페이지의 특별 서비스, 사용 중단된 서비스, 레거시 서비스도 참조하십시오.

ASDM 요구 사항

ASDM 클라이언트 운영 체제 및 브라우저 요구 사항

표 1-1에서는 ASDM을 위해 지원되고 권장되는 클라이언트 운영 체제와 Java를 보여줍니다.

표 1-1 운영 체제 및 브라우저 요구 사항

운영 체제	브라우저				Java SE 플러그인
	Internet Explorer	Firefox	Safari	Chrome	
Microsoft Windows(영어 및 일본어): • 8 • 7 • Vista • 2008 Server • XP	6.0 이상	1.5 이상	지원 안 함	18.0 이상	6.0 이상
Apple OS X 10.4 이상	지원 안 함	1.5 이상	2.0 이상	18.0 이상	6.0 이상
Red Hat Enterprise Linux 5(GNOME 또는 KDE): • 데스크톱 • 워크스테이션 데스크톱	N/A	1.5 이상	N/A	18.0 이상	6.0 이상

Java 및 브라우저 호환성

표 1-2에는 Java, ASDM 및 브라우저 호환성에 대한 호환성 주의 사항이 나와 있습니다.

표 1-2 ASDM 호환성에 대한 주의 사항

Java 버전	상태	참고
7 업데이트 51	ASDM Launcher에 신뢰할 수 있는 인증서가 필요함	Launcher를 사용하여 계속 진행하려면 다음 중 하나를 수행합니다. • 알려진 CA의 신뢰할 수 있는 인증서를 ASA에 설치합니다. • 자체 서명 인증서를 설치하고 이를 Java에 등록합니다. http://www.cisco.com/go/asdm-certificate를 참조하십시오. • Java를 7 업데이트 45 이하로 다운그레이드합니다. • 또는 Java Web Start를 사용합니다. **참고** Java 7 업데이트 51에서는 ASDM 7.1(5) 이하를 지원하지 않습니다. Java를 이미 업그레이드했고 Version 7.2로 업그레이드하기 위해 ASDM을 더 이상 시작할 수 없는 경우, CLI를 사용하여 ASDM을 업그레이드하거나 ASDM으로 관리하려는 각 ASA에 대한 Java Control Panel에 보안 예외를 추가할 수 있습니다. "해결 방법" 섹션을 참조 하십시오. http://java.com/en/download/help/java_blocked.xml 보안 예외를 추가한 후 이전 ASDM을 시작한 다음 7.2로 업그레이드합니다.
	Java Web Start를 사용할 때 드물게 온라인 도움말이 로드되지 않음	온라인 도움말을 시작할 때 브라우저 창이 로드되지만 내용이 표시되지 않는 경우가 간혹 발생합니다. 브라우저에 "Unable to connect"라는 오류 메시지가 보고됩니다. 해결 방법: • ASDM Launcher를 사용합니다. 또는: • Java Runtime Parameters에서 **-Djava.net.preferIPv6Addresses=true** 매개변수를 지웁니다. a. Java Control Panel을 시작합니다. b. **Java** 탭을 클릭합니다. c. **View**를 클릭합니다. d. **-Djava.net.preferIPv6Addresses=true** 매개변수를 지웁니다. e. **OK** 및 **Apply**를 차례로 클릭한 다음 **OK**를 다시 클릭합니다.

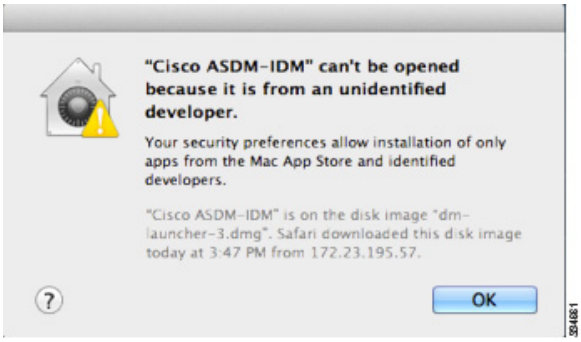
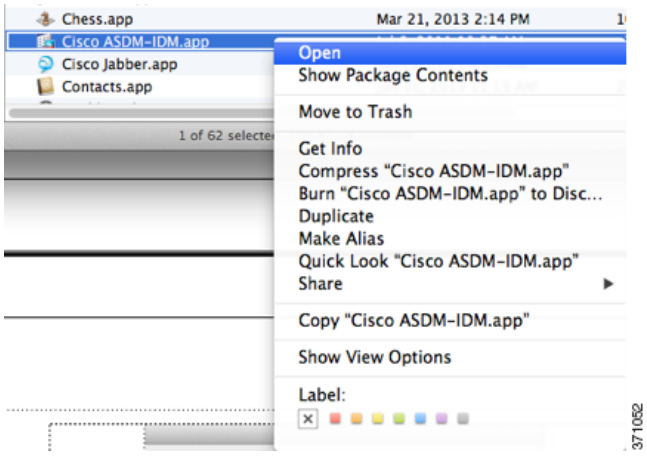
표 1-2 ASDM 호환성에 대한 주의 사항 (계속)

Java 버전	상태	참고
7 업데이트 45	신뢰할 수 없는 인증서를 사용할 경우 Permissions 속성이 누락되었다는 노란색 경고 메시지가 ASDM에 표시됨	Java의 버그로 인한 것이며 ASA에 신뢰할 수 있는 인증서가 설치되지 않은 경우 JAR 매니페스트에 Permissions 속성이 누락되었다는 노란색 경고 메시지가 표시됩니다. **이 경고는 무시해도 괜찮습니다.** ASDM 7.2에는 Permissions 속성이 포함되어 있습니다. 경고가 표시되지 않도록 하려면 알려진 CA에서 신뢰할 수 있는 인증서를 설치하거나, **Configuration > Device Management > Certificates > Identity Certificates**를 선택하여 ASA에서 자체 서명 인증서를 생성합니다. ASDM을 시작했을 때 인증서 경고가 표시될 경우 **Always trust connections to websites** 확인란을 선택합니다.
7	ASA에 강력한 암호화 라이센스(3DES/AES)가 필요함	ASDM의 경우 ASA에 대한 SSL 연결이 필요합니다. ASA에 기본 암호화 라이센스(DES)밖에 없는 경우 SSL 연결의 암호의 암호화 수준이 약해지므로 ASDM을 시작할 수 없습니다. Java 7을 제거하고 Java 6을 설치해야 합니다 (http://www.oracle.com/technetwork/java/javase/downloads/java-archive-downloads-javase6-419409.html). 약한 암호화 문제 및 Java 6에는 해결 방법을 적용해야 합니다(이 표의 아래 참조).
6	사용자 이름의 길이가 50자를 넘을 수 없음	Java 버그로 인한 것이며, Java 6을 사용할 경우 ASDM에서는 50자 이상의 사용자 이름을 지원하지 않습니다. 더 긴 사용자 이름은 Java 7에서 구현할 수 있습니다.
	ASA에 강력한 암호화 라이센스(3DES/AES) *또는* 해결 방법이 필요함	브라우저를 ASA에 처음 연결하여 ASDM 스플래시 화면을 로드하려는 경우, 브라우저에서는 ASA에 SSL 연결을 생성하고자 시도합니다. ASA에 기본 암호화 라이센스(DES)밖에 없는 경우 SSL 연결의 암호화 기능이 약해져 ASDM을 시작할 수 없으므로 ASDM 스플래시 화면에 액세스하지 못할 수 있습니다. 대부분의 최신 브라우저에서는 암호화 수준이 약한 암호를 지원하지 않습니다. 따라서 강력한 암호화 라이센스(3DES/AES)가 없을 경우 다음 해결 방법 중 하나를 사용하십시오. • 제공되는 경우, 기존에 다운로드한 ASDM Launcher 또는 Java Web Start 바로 가기를 사용합니다. 브라우저에서 지원하지 않는 경우에도 Launcher 및 Web Start 바로 가기는 Java 6 및 약한 암호화 기능과 연동됩니다. • Windows Internet Explorer의 경우, 해결 방법으로 DES를 활성화할 수 있습니다. 자세한 내용은 http://support.microsoft.com/kb/929708을 참조하십시오. • 운영 체제에서 Firefox를 사용할 경우, 해결 방법으로 security.ssl3.dhe_dss_des_sha 설정을 활성화할 수 있습니다. 숨겨진 컨피그레이션 기본 설정을 변경하는 방법을 알아보려면 http://kb.mozillazine.org/About:config를 참조하십시오.

표 1-2 ASDM 호환성에 대한 주의 사항 (계속)

Java 버전	상태	참고
모두	• 자체 서명 인증서 또는 신뢰할 수 없는 인증서 • IPv6 • Firefox 및 Safari	ASA에서 자체 서명 인증서 또는 신뢰할 수 없는 인증서를 사용할 경우, HTTPS over IPv6를 사용하여 탐색을 수행할 때 Firefox 4 이상 및 Safari에서 보안 예외를 추가할 수 없습니다. 자세한 내용은 https://bugzilla.mozilla.org/show_bug.cgi?id=633001을 참조하십시오. 이 주의 사항은 Firefox 또는 Safari에서 시작되어 ASA로 연결되는 모든 SSL 연결(ASDM 연결 포함)에 영향을 미칩니다. 이러한 주의 사항을 방지하려면 신뢰할 수 있는 인증 기관에서 발급한 올바른 인증서를 ASA에 구성해야 합니다.
	• ASA에서 SSL 암호화를 수행할 경우 RC4-MD5 및 RC4-SHA1을 모두 포함하거나, Chrome에서 SSL false start를 비활성화해야 함 • Chrome	ASA에서 SSL을 암호화할 때 RC4-MD5 및 RC4-SHA1 알고리즘을 제외하도록 변경하면, Chrome의 "SSL false start" 기능으로 인해 Chrome에서 ASDM을 시작할 수 없게 됩니다. 이 알고리즘 중 하나를 다시 활성화하는 것이 좋습니다(Configuration > Device Management > Advanced > SSL Settings 창 참조). 또는 http://www.chromium.org/developers/how-tos/run-chromium-with-flags에 따라 **--disable-ssl-false-start** 플래그를 사용하여 Chrome에서 SSL false start를 비활성화할 수 있습니다.
	서버의 IE9	서버에 Internet Explorer 9.0을 사용할 경우 “Do not save encrypted pages to disk” 옵션이 기본적으로 활성화되어 있습니다(Tools > Internet Options > Advanced 참조). 이 옵션은 초기 ASDM 다운로드가 실패하는 원인이 됩니다. ASDM 다운로드를 허용하려면 이 옵션을 비활성화하십시오.
	OS X	OS X에서 ASDM을 처음 시작할 경우 Java를 설치하라는 메시지가 표시될 수 있습니다. 필요한 경우 메시지 내용을 따릅니다. 설치가 완료되면 ASDM이 시작됩니다.

표 1-2 ASDM 호환성에 대한 주의 사항 (계속)

Java 버전	상태	참고
모두	OS X 10.8 이상	Apple Developer ID로 서명하지 않았으므로 ASDM이 실행되도록 허용해야 합니다. 보안 기본 설정을 변경하지 않으면 오류 화면이 표시됩니다.  1. ASDM이 실행되도록 허용하려면 마우스 오른쪽 버튼(또는 Ctrl-클릭)으로 **Cisco ASDM-IDM Launcher** 아이콘을 클릭하고 **Open**을 선택합니다.  2. 유사한 오류 화면이 표시되지만, 이 화면에서 ASDM을 열 수는 없습니다. **Open**을 클릭합니다. ASDM-IDM Launcher가 열립니다. 

하드웨어 및 소프트웨어 호환성

지원되는 하드웨어 및 소프트웨어의 전체 목록을 보려면 *Cisco ASA 호환성*을 참조 하십시오.
http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

VPN 호환성

*지원되는 VPN 플랫폼, Cisco ASA Series*를 참조하십시오.
http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

새로운 기능

- 1-7 페이지의 ASA 9.3(1)/ASDM 7.3(1)의 새로운 기능

참고 새 syslog 메시지, 변경된 syslog 메시지, 사용 중단된 syslog 메시지가 syslog 메시지 가이드에 나와 있습니다.

ASA 9.3(1)/ASDM 7.3(1)의 새로운 기능

릴리스: 2014년 7월 24일

표 1-3에서는 ASA Version 9.3(1)/ASDM Version 7.3(1)의 새로운 기능을 소개합니다.

표 1-3 ASA Version 9.3(1)/ASDM Version 7.3(1)의 새 기능

기능	설명
방화벽 기능	
SIP, SCCP, TLS 프록시에서 IPv6 지원	SIP, SCCP, TLS 프록시(SIP 또는 SCCP 사용)를 사용할 때 IPv6 트래픽을 검사할 수 있습니다. ASDM 화면은 수정하지 않았습니다.
Cisco Unified Communications Manager 8.6 지원	ASA가 Cisco Unified Communications Manager Version 8.6과의 상호 운용성을 제공합니다(SCCPv21 지원 포함). ASDM 화면은 수정하지 않았습니다.
액세스 그룹 및 NAT를 위한 규칙 엔진의 트랜잭션 커밋 모델	이 기능을 활성화한 경우, 규칙 매칭의 성능 저하 없이 규칙 컴파일이 완료되면 규칙 업데이트가 적용됩니다. 다음 화면을 도입했습니다. **Configuration > Device Management > Advanced > Rule Engine**

표 1-3 ASA Version 9.3(1)/ASDM Version 7.3(1)의 새 기능 (계속)

기능	설명
원격 액세스 기능	
클라이언트리스 SSL VPN을 위한 XenDesktop 7 지원	클라언트리스 SSL VPN에 XenDesktop 7 지원을 추가했습니다. 자동 로그온의 북마크를 만들 때 랜딩 페이지 URL 또는 제어 ID를 지정할 수 있습니다. 다음 화면을 수정했습니다. **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**
Mobile Enablement 프록시	ISE Mobile Enablement 솔루션의 구성 요소인 Mobile Enablement 프록시를 사용하면 오프프레미스 모바일 디바이스에서 온프레미스 모바일 디바이스와 똑같은 방식으로 모바일 디바이스를 관리할 수 있습니다. **참고** Mobile Enablement 프록시는 2015년 초에 출시될 예정인 ISE 릴리스의 ISE 지원을 필요로 합니다. 다음 화면을 도입했습니다. **Configuration > Remote Access VPN > AAA/Local Users > MDM Proxy**
AnyConnect 사용자 지정 특성 확장	사용자 지정 특성으로 ASA에 통합되지 않은 AnyConnect 기능(예: Deferred Upgrade)을 정의하고 구성합니다. 사용자 지정 특성 컨피그레이션이 여러 값과 더 긴 값을 허용하도록 확장되었습니다. 또한 이제부터는 그 유형, 이름, 값을 지정해야 합니다. 동적 액세스 정책과 그룹 정책에 추가할 수 있습니다. 9.3.x로 업그레이드하면 이전에 정의했던 사용자 지정 특성이 이 확장된 컨피그레이션 형식으로 업데이트됩니다. 다음 화면을 도입했거나 수정했습니다. **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names** **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > Advanced > AnyConnect Client > Custom Attributes** **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add/Edit > AnyConnect Custom Attributes**
데스크톱 플랫폼을 위한 ACIDex(AnyConnect Identity Extensions)	AnyConnect Endpoint Attributes 또는 Mobile Posture라고도 하는 ACIDex는 AnyConnect VPN 클라이언트에서 ASA에 포스처 정보를 전달하는 데 사용하는 방법입니다. 동적 액세스 정책에서는 사용자 권한 부여에 이 엔드포인트 특성을 사용합니다. AnyConnect VPN 클라이언트는 DAP에서 사용할 데스크톱 운영 체제(Windows, Mac OS X, Linux)용 플랫폼 식별자와 MAC 주소 풀을 제공합니다. 다음 화면을 수정했습니다. **Configuration > Remote Access VPN > Dynamic Access Policies > Add/Edit > Add/Edit (endpoint attribute)**, select **AnyConnect** for the **Endpoint Attribute Type**. **Platform** 드롭다운 목록에 운영 체제가 추가되었고 MAC Address가 **Mac Address Pool**로 바뀌었습니다.

표 1-3 ASA Version 9.3(1)/ASDM Version 7.3(1)의 새 기능 (계속)

기능	설명
VPN을 위한 TrustSec SGT 지정	원격 사용자가 연결할 때 ASA에서 TrustSec SGT(Security Group Tag)가 SGT-IP 테이블에 추가될 수 있습니다. 다음 화면을 도입했거나 수정했습니다. **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Edit User > VPN Policy** **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add a Policy**
고가용성 기능	
클러스터링의 모듈 상태 모니터링 지원 향상	클러스터링에서 모듈 상태의 모니터링을 더 효과적으로 지원합니다. ASDM 화면은 수정하지 않았습니다.
하드웨어 모듈의 상태 모니터링 비활성화	기본적으로 ASA에서는 ASA FirePOWER 모듈과 같은 설치된 하드웨어 모듈의 상태를 모니터링합니다. 하드웨어 모듈 오류 때문에 장애 조치가 수행되는 것을 원치 않을 경우 모듈 모니터링을 비활성화할 수 있습니다. 다음 화면을 수정했습니다. **Configuration > Device Management > High Availability and Scalability > Failover > Interfaces**
플랫폼 기능	
ASP 로드 밸런싱	**asp load-balance per-packet** 명령의 새로운 **auto** 옵션은 ASA가 각 인터페이스 수신 링에서 패킷별로 ASP 로드 밸런싱을 켜고 끄면서 조정할 수 있게 합니다. 이 자동 메커니즘은 비대칭형 트래픽의 유입 여부를 감지하며, 다음과 같은 문제의 예방에 도움이 됩니다. • 흐름에서 산발적인 트래픽 급증으로 인한 오버런 • 특정 인터페이스 수신 링에 초과 유입되는 대량 흐름에 의한 오버런 • 비교적 과부하 상태인 인터페이스 수신 링으로 인한 오버런. 단일 코어에서 부하를 수용할 수 없음 ASDM 화면은 수정하지 않았습니다.
SNMP MIB	CISCO-REMOTE-ACCESS-MONITOR-MIB에서 ASASM를 지원합니다.
인터페이스 기능	
투명 모드 브리지 그룹 최대 개수 250개로 증가	브리지 그룹의 최대 개수가 8개에서 250개로 늘어났습니다. 단일 모드에서 또는 다중 모드의 각 컨텍스트에서 최대 250개의 브리지 그룹을 구성할 수 있으며, 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다. 다음 화면을 수정했습니다. **Configuration > Device Setup > Interfaces** **Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface** **Configuration > Device Setup > Interfaces > Add/Edit Interface**
라우팅 기능	
ASA 클러스터링을 위한 BGP 지원	ASA 클러스터링에서 BGP 지원을 추가했습니다. 다음 화면을 수정했습니다. **Configuration > Device Setup > Routing > BGP > IPv4 Family > General**

표 1-3 ASA Version 9.3(1)/ASDM Version 7.3(1)의 새 기능 (계속)

기능	설명
NSF를 위한 BGP 지원	BGP NSF(Nonstop Forwarding) 지원을 추가했습니다. 다음 화면을 수정했습니다. **Configuration > Device Setup > Routing > BGP > General** **Configuration > Device Setup > Routing > BGP > IPv4 Family > Neighbor** **Monitoring > Routing > BGP Neighbors**
광고 맵을 위한 BGP 지원	BGPv4 광고 맵 지원을 추가했습니다. 다음 화면을 수정했습니다. **Configuration > Device Setup > Routing > BGP > IPv4 Family > Neighbor > Add BGP Neighbor > Routes**
NSF를 위한 OSPF 지원	NSF를 위한 OSPFv2 및 OSPFv3 지원을 추가했습니다. 다음 화면을 추가했습니다. **Configuration > Device Setup > Routing > OSPF > Setup > NSF Properties** **Configuration > Device Setup > Routing > OSPFv3 > Setup > NSF Properties**
AAA 기능	
레이어 2 보안 그룹 태그 도입	보안 그룹 태그와 이더넷 태그를 함께 사용하면서 정책을 적용할 수 있습니다. Layer 2 SGT Imposition이라고도 하는 SGT plus Ethernet Tagging은 ASA가 기가비트 이더넷 인터페이스에서 Cisco 전용 이더넷 프레이밍(Ether Type 0x8909)을 사용하여 보안 그룹 태그를 보내고 받을 수 있게 합니다. 즉 일반 텍스트 이더넷 프레임에 소스 보안 그룹 태그를 삽입할 수 있습니다. 다음 화면을 수정했습니다. **Configuration > Device Setup > Interfaces > Add Interface > Advanced** **Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced** **Configuration > Device Setup > Add Ethernet Interface > Advanced** **Wizards > Packet Capture Wizard** **Tools > Packet Tracer**
AAA Windows NT 도메인 인증 종료	원격 액세스 VPN 사용자를 위한 NTLM 지원을 종료했습니다. 다음 화면을 수정했습니다. **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups > Add AAA Server Group**
ASDM Identity Certificate 마법사	최신 Java 버전을 사용할 때 ASDM Launcher는 신뢰할 수 있는 인증서를 요구합니다. 이 인증서 요구 사항을 손쉽게 해결하는 방법은 자체 서명 ID 인증서를 설치하는 것입니다. ASDM Identity Certificate 마법사에서 손쉽게 자체 서명 ID 인증서를 만들 수 있습니다. 처음으로 ASDM을 시작했을 때 신뢰할 수 있는 인증서가 없으면, Java Web Start와 함께 ASDM을 시작하라는 메시지가 표시됩니다. 새 마법사가 즉시 시작됩니다. ID 인증서를 만든 다음 Java 제어판에서 등록해야 합니다. 자세한 내용은 https://www.cisco.com/go/asdm-certificate를 참조하십시오. **Wizards > ASDM Identity Certificate Wizard** 화면을 추가했습니다.

표 1-3 ASA Version 9.3(1)/ASDM Version 7.3(1)의 새 기능 (계속)

기능	설명
모니터링 기능	
물리적 인터페이스의 종합 트래픽 모니터링	**show traffic** 명령 출력이 업데이트되어 물리적 인터페이스의 종합 트래픽 정보를 포함합니다. 이 기능을 활성화하려면 먼저 **sysopt traffic detailed-statistics** 명령을 입력해야 합니다.

ASA Services Module에서 스위치 작업이 이루어지는 방식

Cisco IOS 소프트웨어를 사용하여 Catalyst 6500 Series 및 Cisco 7600 Series 스위치에서 스위치 수퍼바이저 및 통합 MSFC 양쪽에 대해 ASASM을 설치할 수 있습니다.

참고 Catalyst OS(운영 체제)는 지원되지 않습니다.

ASA에서는 자체적인 운영 체제를 실행합니다.

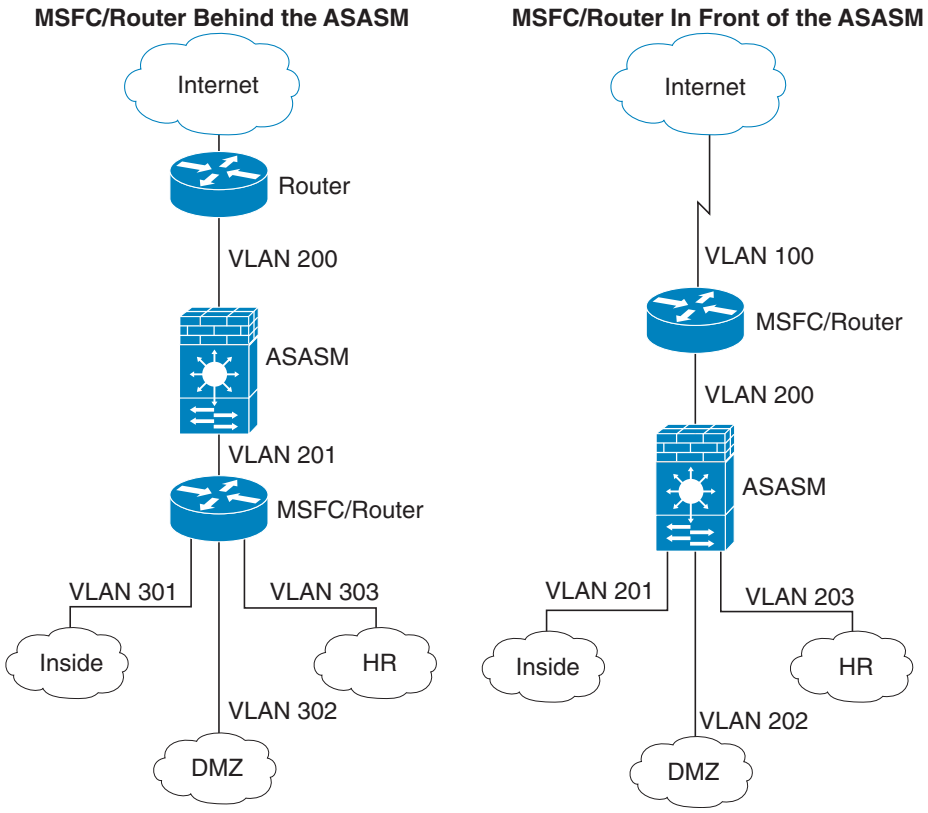
스위치에는 스위칭 프로세서(수퍼바이저) 및 라우터(MSFC)가 포함됩니다. 시스템에 MSFC가 있어야 하지만, 이를 사용할 필요는 없습니다. MSFC를 사용하도록 선택할 경우, MSFC에 하나 이상의 VLAN을 할당할 수 있습니다. 또는 MSFC 대신 외부 라우터를 사용할 수 있습니다.

단일 컨텍스트 모드의 경우 방화벽 앞이나 방화벽 뒤에 라우터를 배치할 수 있습니다(그림 1-1 참조).

라우터의 위치는 라우터에 할당하는 VLAN에 전적으로 달려 있습니다. 예를 들어, 왼쪽 그림 1-1에 표시된 예에서 VLAN 201이 ASASM의 내부 인터페이스에 할당되었으므로 라우터가 방화벽의 뒤에 있습니다. 반대로 오른쪽 그림 1-1에 표시된 예에서 VLAN 200이 ASASM의 외부 인터페이스에 할당되었으므로 라우터가 방화벽의 앞에 있습니다.

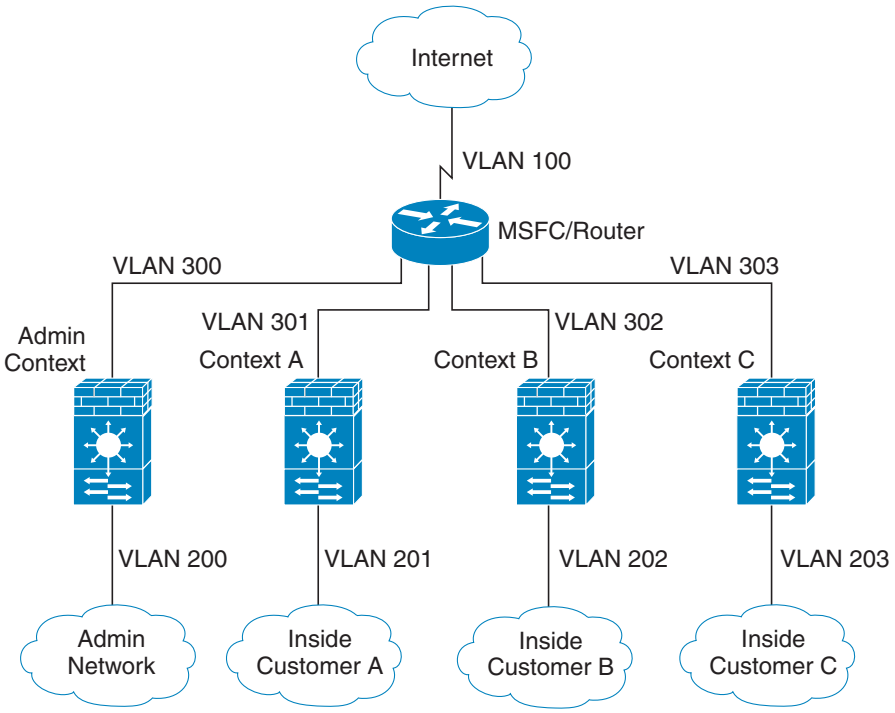
왼쪽 예에서 MSFC 또는 라우터는 VLAN 201, 301, 302, 303 사이를 라우팅하며, 내부 트래픽은 인터넷을 목적지로 하지 않는 한 ASASM을 통과하지 않습니다. 오른쪽 예의 경우 ASASM에서는 VLAN 201, 202, 203 간의 모든 트래픽을 처리하고 보호합니다.

그림 1-1 MSFC/라우터 배치



다중 컨텍스트 모드의 경우 ASASM 뒤에 라우터를 배치하면 이를 단일 컨텍스트로만 연결해야 합니다. 라우터를 다중 컨텍스트에 연결하면 라우터가 컨텍스트 간에 라우팅을 수행하며, 이는 원하는 작업 결과가 아닐 수 있습니다. 다중 컨텍스트의 일반적인 시나리오는 라우터를 모든 컨텍스트 앞에 사용하여 인터넷과 스위치 네트워크 간에 라우팅을 수행하는 것입니다(그림 1-2 참조)

그림 1-2 다중 컨텍스트로 MSFC/라우터 배치



방화벽 기능 개요

방화벽은 외부 네트워크의 사용자가 내부 네트워크에 무단 액세스하는 것을 차단합니다. 방화벽은 또한 내부 네트워크 사이에서도 상호 간 보호가 가능합니다. 인사부 네트워크를 사용자 네트워크로부터 분리하는 것 등이 그 예입니다. 웹 또는 FTP 서버 같이 외부 사용자에게 제공해야 하는 네트워크 리소스가 있을 경우, 이러한 리소스를 방화벽 뒤에 있는 DMZ(*Demilitarized Zone*)라는 별도의 네트워크에 배치할 수 있습니다. 방화벽에서는 DMZ에 제한된 액세스를 허용하지만 DMZ에는 공용 서버만 포함되므로, 이곳에 공격이 발생할 경우 해당 서버에만 영향을 미치며 다른 내부 네트워크에서는 영향을 미치지 않습니다. 또한 특정 주소만 내보내도록 허용하거나, 인증이나 권한을 요청하거나, 외부 URL 필터링 서버와 조율하는 방식을 통해 내부 사용자가 외부 네트워크에 액세스(예: 인터넷 액세스)하는 것도 제어할 수 있습니다.

방화벽에 연결된 네트워크를 이야기할 때, *외부* 네트워크는 방화벽 앞에 있고, *내부* 네트워크는 방화벽 뒤에서 보호되고 있으며, *DMZ*는 방화벽 뒤에 있으나 외부 사용자에게 제한된 액세스를 허용하는 네트워크를 일컫습니다. 그러나 ASA에서는 여러 가지 보안 정책으로 많은 인터페이스(예: 다양한 내부 인터페이스, 다양한 DMZ, 다양한 외부 인터페이스)를 구성할 수 있도록 지원하므로, 이러한 용어는 일반적인 의미로만 사용됩니다.

- 1-14 페이지의 보안 정책 개요
- 1-16 페이지의 방화벽 모드 개요
- 1-16 페이지의 스테이트풀 감시 개요

보안 정책 개요

보안 정책은 어떤 트래픽이 방화벽을 통과하여 다른 네트워크에 액세스하도록 허용할지 여부를 결정합니다. 기본적으로 ASA에서는 내부 네트워크(상위 보안 수준)에서 외부 네트워크(하위 보안 수준)로 트래픽이 자유롭게 이동하도록 허용합니다. 트래픽에 몇 가지 조치를 취하여 보안 정책을 맞춤화할 수 있습니다.

액세스 목록 규칙으로 또는 거부

액세스 규칙을 적용하여 내부에서 외부로 나가는 트래픽을 제한하거나, 외부에서 내부로 들어오는 트래픽을 허용할 수 있습니다. 투명 방화벽 모드의 경우, EtherType 액세스 목록을 적용하여 비 IP 트래픽을 허용할 수도 있습니다.

NAT 적용

NAT의 몇 가지 이점은 다음과 같습니다.

- 내부 네트워크에서 사설 주소를 사용할 수 있습니다. 사설 주소는 인터넷에서 라우팅할 수 없습니다.
- NAT는 다른 네트워크의 로컬 주소를 숨기므로, 공격자가 호스트의 실제 주소를 알 수 없습니다.
- NAT는 IP 주소 중복을 지원하여 IP 라우팅 문제를 해결할 수 있습니다.

IP 프래그먼트 방지

ASA에서는 IP 프래그먼트 방지 기능을 제공합니다. 이 기능에서는 모든 ICMP 오류 메시지를 완전히 재결합하고, ASA를 통해 라우팅된 나머지 IP 프래그먼트를 가상으로 재결합하는 작업을 수행합니다. 보안 검사에 실패한 프래그먼트는 누락 및 기록됩니다. 가상 재결합은 비활성화할 수 없습니다.

통과 트래픽에 AAA 사용

HTTP 같은 특정 유형의 트래픽에 인증 및/또는 권한 부여를 요구할 수 있습니다. ASA에서는 RADIUS 또는 TACACS+ 서버에 대한 어카운팅 정보도 전송합니다.

HTTP, HTTPS 또는 FTP 필터링 적용

액세스 목록을 사용하여 특정 웹 사이트 또는 FTP 서버에 대한 아웃바운드 액세스를 방지할 수는 있으나, 인터넷의 규모와 동적 특징을 감안했을 때 이러한 방식으로 웹 사용을 구성하고 관리하는 것은 실용적이지 않습니다.

ASA에서 Cloud Web Security를 구성하거나, URL 및 기타 필터링 서비스(예: ASA CX 또는 ASA FirePOWER)를 제공하는 ASA 모듈을 설치할 수 있습니다. ASA를 Cisco WSA(Web Security Appliance) 같은 외부 제품과 함께 사용할 수도 있습니다.

애플리케이션 감시 적용

사용자 데이터 패킷에 IP 주소 정보를 포함하거나, 동적으로 할당된 포트에서 보조 채널을 여는 서비스에는 감시 엔진이 필요합니다. 이러한 프로토콜의 경우 ASA에서 심층 패킷 감시를 수행해야 합니다.

지원되는 하드웨어 또는 소프트웨어 모듈에 트래픽 전송

일부 ASA 모델에서는 고급 서비스를 제공하기 위해 소프트웨어 모듈을 구성하거나 새시에 하드웨어 모듈을 삽입할 수 있습니다. 이러한 모듈에서는 추가적인 트래픽 감시를 제공하며 구성된 정책을 바탕으로 트래픽을 차단할 수 있습니다. 이러한 모듈에 트래픽을 전송하여 이와 같은 고급 서비스를 이용할 수 있습니다.

QoS 정책 적용

음성 및 스트리밍 비디오 같은 일부 네트워크 트래픽의 경우 긴 레이턴시 시간을 허용할 수 없습니다. QoS는 이러한 유형의 트래픽에 우선순위를 부여할 수 있는 기능입니다. QoS에서는 네트워크의 기능을 참조하여 선택된 네트워크 트래픽에 더 개선된 서비스를 제공할 수 있도록 합니다.

연결 제한 및 TCP 표준화 적용

TCP 및 UDP 연결과 초기 연결을 제한할 수 있습니다. 연결 및 초기 연결 수를 제한하면 DoS 공격을 방지할 수 있습니다. ASA에서는 초기 제한을 사용하여 TCP 가로채기를 시작하며, 이렇게 하면 TCP SYN 패킷을 인터페이스에 플러딩하여 시행된 DoS 공격으로부터 내부 시스템을 보호할 수 있습니다. 초기 연결은 소스와 목적지 간에 필요한 핸드셰이크가 완료되지 않은 연결 요청입니다.

TCP 표준화는 정상으로 보이지 않는 패킷을 누락시키기 위해 고안된 고급 TCP 연결 설정으로 이루어진 기능입니다.

위협 감지 활성화

위협 감지 검사 및 기본 위협 감지를 구성할 수 있으며, 통계를 활용하여 위협을 분석하는 방법도 구성할 수 있습니다.

기본 위협 감지 기능에서는 공격(예: DoS 공격)과 관련될 가능성이 있는 활동을 감지하고, 시스템 로그 메시지를 자동으로 전송합니다.

일반적인 공격 검사는 서브넷에 있는 모든 IP 주소의 액세스 가능성을 테스트하는 호스트로 구성되어 있습니다(서브넷에 있는 다수의 호스트를 모두 검사하거나 호스트 또는 서브넷에 있는 다수의 포트를 모두 스위핑함). 위협 감지 검사 기능은 호스트가 언제 검사를 수행해야 할지 결정합니다. 트래픽 서명을 기반으로 하는 IPS 검사 감지와 달리, ASA 위협 감지 검사 기능의 경우 검사 활동을 분석할 수 있는 호스트 통계가 포함된 방대한 데이터베이스를 유지합니다.

호스트 데이터베이스에서는 반환 활동이 없는 연결, 닫힌 서비스 포트에 액세스, 취약한 TCP 동작(예: 임의적이지 않은 IPID) 등의 수많은 동작을 비롯한 의심스러운 활동을 추적합니다.

공격자에 대한 시스템 로그 메시지를 전송하도록 ASA를 구성하거나 호스트를 자동으로 피할 수 있습니다.

봇넷 트래픽 필터 활성화

악성코드는 알 수 없는 호스트에 설치되는 악성 소프트웨어입니다. 악성코드가 알려진 악성 IP 주소에 연결을 시작하면, 봇넷 트래픽 필터에서는 개인 데이터(비밀번호, 신용카드 번호, 키 스트로크, 독점 데이터) 전송 같은 네트워크 활동을 시도하는 악성코드를 감지할 수 있습니다. 봇넷 트래픽 필터에서는 알려진 악성 도메인 이름 및 IP 주소로 구성된 동적 데이터베이스(블랙리스트)를 기준으로, 들어오고 나가는 연결을 검사한 다음 모든 의심스러운 활동을 기록합니다. 악성코드 활동에 대한 syslog 메시지가 표시되면 해당 호스트를 격리하고 감염을 치료하기 위한 단계를 수행할 수 있습니다.

Cisco Unified Communications 구성

Cisco ASA Series는 유니파이드 커뮤니케이션 구축을 위한 프록시 기능을 제공하는 전략적 플랫폼입니다. 프록시의 용도는 클라이언트와 서버 간의 연결을 종료하고 다시 시작하기 위한 것입니다. 프록시에서는 트래픽 감시, 프로토콜 확인, 정책 제어 같은 다양한 보안 기능을 제공하여 내부 네트워크의 보안을 담당합니다. 점점 더 많이 사용되고 있는 프록시의 기능은 보안 정책을 적용하는 동시에 연결의 기밀성을 유지하기 위해 암호화된 연결을 종료하는 것입니다.

방화벽 모드 개요

ASA는 다음과 같은 두 가지 다른 방화벽 모드에서 실행됩니다.

- 라우팅
- 투명

라우팅 모드에서 ASA는 네트워크의 라우터 홉으로 간주합니다.

투명 모드에서 ASA는 "비활성 엔드포인트(bump in the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하며, 라우터 홉으로 간주하지 않습니다. ASA는 내부 및 외부 인터페이스에서 동일한 네트워크에 연결됩니다.

투명 방화벽을 사용하여 네트워크 컨피그레이션을 간소화할 수 있습니다. 공격자에게 방화벽이 보이지 않게 하려는 경우에도 투명한 모드가 유용합니다. 라우팅 모드에서 차단할 트래픽에도 투명 모드를 사용할 수 있습니다. 예를 들어, 투명 방화벽에서는 EtherType 액세스 목록을 사용한 멀티캐스트 스트림을 지원합니다.

스테이트풀 감시 개요

ASA를 통과하는 모든 트래픽은 Adaptive Security Algorithm을 사용하여 감시되며 통과가 허용되거나 누락됩니다. 간단한 패킷 필터로 올바른 소스 주소, 목적지 주소, 포트를 확인할 수 있으나, 패킷 시퀀스 또는 플래그가 올바른지 여부는 확인할 수 없습니다. 또한 필터의 경우 해당 필터를 기준으로 *모든* 패킷을 확인하므로, 프로세스가 느릴 수 있습니다.

참고 TCP 상태 우회 기능을 사용하면 패킷 흐름을 맞춤화할 수 있습니다.

그러나 ASA 같은 스테이트풀 방화벽에서는 다음과 같은 패킷의 상태를 고려합니다.

- 새 연결인가?

  새 연결일 경우 ASA에서 액세스 목록을 기준으로 패킷을 확인하고 기타 작업을 수행하여 패킷을 허용 또는 거부할지 결정해야 하는가? 이러한 확인을 수행하기 위해 세션의 첫 번째 패킷은 "세션 관리 경로"를 통과하며, 트래픽의 유형에 따라 "컨트롤 플레인 경로"를 통과할 수도 있습니다.

  세션 관리 경로는 다음과 같은 작업에 직접적인 연관이 있습니다.

  - 액세스 목록 확인 수행
  - 경로 조회 수행
  - NAT 변환 할당(xlates)
  - "빠른 경로"에 세션 설정

  ASA에서는 TCP 트래픽의 빠른 경로에서 전달 및 반대 흐름을 생성합니다. 또한 ASA에서는 UDP, ICMP(ICMP 감시를 활성화할 경우) 같은 무연결 프로토콜에 대한 연결 상태 정보도 생성하여, 마찬가지로 빠른 경로를 사용할 수 있도록 합니다.

  참고 ASA의 경우 SCTP 같은 다른 IP 프로토콜에 대해서는 반대 경로 흐름을 생성하지 않습니다. 결과적으로 이러한 연결을 참조하는 ICMP 오류 패킷은 누락됩니다.

  레이어 7 감시(패킷 페이로드를 감시하거나 변경해야 함)가 필요한 일부 패킷은 컨트롤 플레인 경로로 전달됩니다. 레이어 7 감시 엔진의 경우 둘 이상의 채널(데이터 채널에서는 알려진 포트 번호를 사용하고, 제어 채널에서는 세션마다 다른 포트 번호를 사용함)이 포함된 프로토콜이 필요합니다. 이러한 프로토콜에는 FTP, H.323 및 SNMP가 포함됩니다.

- 설정되어 있는 연결인가?

  연결이 기존에 설정되어 있는 경우 ASA에서는 패킷을 다시 확인할 필요가 없습니다. 일치하는 대부분의 패킷은 양방향에서 모두 “빠른” 경로를 통과할 수 있습니다. 빠른 경로는 다음과 같은 작업에 직접적인 연관이 있습니다.

  - IP 체크섬 확인
  - 세션 조회
  - TCP 시퀀스 번호 확인
  - 기존 세션을 바탕으로 NAT 변환
  - 레이어 3 및 레이어 4 헤더 조정

  레이어 7 검사가 필요한 프로토콜의 데이터 패킷도 빠른 경로를 통과할 수 있습니다.

  설정된 세션 패킷 중 일부는 계속 세션 관리 경로 또는 컨트롤 플레인 경로를 통해 전달되어야 합니다. 세션 관리 경로를 통과하는 패킷에는 감시 또는 콘텐츠 필터링이 필요한 HTTP 패킷이 포함되어 있습니다. 컨트롤 플레인 경로를 통과하는 패킷에는 레이어 7 검사가 필요한 프로토콜의 제어 패킷이 포함되어 있습니다.

VPN 기능 개요

VPN은 사설 연결처럼 보이는 TCP/IP 네트워크(예: 인터넷) 전반의 보안 연결입니다. 이러한 보안 연결을 터널이라고 합니다. ASA에서는 터널링 프로토콜을 사용하여 보안 매개변수를 협상하고, 터널을 생성 및 관리하고, 패킷을 캡슐화하고, 터널을 통해 패킷을 주고받고, 캡슐화를 해제합니다. ASA에서는 양방향 터널 엔드포인트로서의 기능을 수행합니다. 플레인 패킷을 수신하고, 이를 캡슐화한 다음, 해당 패킷의 캡슐화가 해제되고 최종 목적지로 전송되는 터널의 다른 쪽 끝에 패킷을 전송합니다. ASA에서는 캡슐화된 패킷을 수신하고 해당 패킷의 캡슐화를 해제한 후 이를 최종 목적지로 전송할 수도 있습니다. ASA에서는 다양한 표준 프로토콜을 호출하여 이러한 기능을 구현합니다.

ASA에서는 다음과 같은 기능을 수행합니다.

- 터널 설정
- 터널 매개변수 협상
- 사용자 인증
- 사용자 주소 할당
- 데이터 암호화 및 해독
- 보안 키 관리
- 터널 전반의 데이터 전송 관리
- 터널 엔드포인트 또는 라우터로서 데이터 전송 인바운드 및 아웃바운드 관리

ASA에서는 다양한 표준 프로토콜을 호출하여 이러한 기능을 구현합니다.

보안 컨텍스트 개요

단일 ASA를 보안 컨텍스트라고 하는 다중 가상 디바이스로 분할할 수 있습니다. 각 컨텍스트는 고유한 보안 정책, 인터페이스 및 관리자가 있는 독립적인 디바이스입니다. 다중 컨텍스트는 여러 대의 독립형 디바이스가 있는 것과 비슷합니다. 다중 컨텍스트 모드에서는 라우팅 테이블, 방화벽 기능, IPS, 관리 기능을 비롯한 다양한 기능이 지원되지만 몇 가지 기능은 지원되지 않습니다. 자세한 내용은 기능 장을 참조하십시오.

다중 컨텍스트 모드에서는 ASA에 보안 정책, 인터페이스 및 독립형 디바이스에서 컨피그레이션할 수 있는 거의 모든 옵션을 식별하는, 각 컨텍스트에 대한 컨피그레이션이 포함됩니다. 시스템 관리자는 시스템 컨피그레이션(단일 모드 컨피그레이션과 마찬가지로 시작 컨피그레이션)에서 컨텍스트를 컨피그레이션하여 컨텍스트를 추가하고 관리할 수 있습니다. 시스템 컨피그레이션은 ASA를 위한 기본적인 설정을 나타냅니다. 시스템 컨피그레이션은 자체 네트워크 인터페이스나 네트워크 설정을 포함하지 않습니다. 그보다는 시스템에서 네트워크 리소스에 액세스해야 할 때(예: 서버로부터 컨텍스트 다운로드) 관리 컨텍스트로 지정된 컨텍스트 중 하나를 사용합니다.

관리자 컨텍스트는 다른 모든 컨텍스트와 같지만 예외 사항이 있습니다. 관리자 컨텍스트에 로그인한 사용자는 시스템 관리자 권한을 갖게 되며, 시스템 및 기타 모든 컨텍스트에 액세스할 수 있습니다.

ASA 클러스터링 개요

ASA 클러스터링을 사용하면 여러 개의 ASA를 하나의 논리적 디바이스로 그룹화할 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다.

마스터 유닛에서만 모든 컨피그레이션(부트스트랩 컨피그레이션 제외)을 수행해야 하며, 그 후 이러한 컨피그레이션은 컨피그레이션원 유닛으로 복제됩니다.

특별 서비스, 사용 중단된 서비스, 레거시 서비스

일부 서비스의 설명서는 주요 컨피그레이션 설명서 및 온라인 도움말 이외의 위치에 있습니다. 전체 설명서 목록을 보려면 다음을 참조하십시오.

http://www.cisco.com/go/asadocs

- 1-19 페이지의 특별 서비스 설명서
- 1-19 페이지의 사용 중단된 서비스
- 1-19 페이지의 레거시 서비스 설명서

특별 서비스 설명서

특별 서비스에서는 ASA와 기타 Cisco 제품 간의 상호 운용을 지원합니다. 이를테면 전화 서비스용 보안 프록시를 제공하거나(Unified Communications), 봇넷 트래픽 필터링을 Cisco 업데이트 서버의 동적 데이터베이스와 결합하여 제공하거나, Cisco Web Security Appliance용 WCCP 서비스를 제공하는 경우를 들 수 있습니다. 이러한 특별 서비스 중 일부는 별도의 설명서에서 다룹니다.

사용 중단된 서비스

사용 중단된 기능에 대한 내용은 현재 사용 중인 ASA 버전의 컨피그레이션 설명서를 참조하십시오. 마찬가지로, 버전 8.2와 8.3 간의 NAT 또는 버전 8.3과 8.4 간의 투명 모드 인터페이스 같은 재설계된 기능의 경우에 대한 내용도 현재 사용 중인 버전의 컨피그레이션 설명서를 참조하십시오. ASDM은 이전 버전의 ASA 릴리스와 호환 가능하지만, 컨피그레이션 설명서 및 온라인 도움말에서는 최신 릴리스에 대한 내용만 다룹니다.

레거시 서비스 설명서

레거시 서비스는 ASA에서 계속 지원되지만, 해당 서비스 대신 사용할 수 있는 향상된 대체 서비스가 제공될 수 있습니다. 레거시 서비스에 대한 내용은 별도의 설명서에서 다룹니다.

2 장

시작하기

이 장에서는 Cisco ASA를 시작하는 방법에 대해 설명합니다.

Command-Line Interface용 콘솔 액세스

일부 경우 CLI를 사용하여 ASDM 액세스를 위한 기본 설정을 구성해야 할 수 있습니다.

초기 컨피그레이션의 경우에는 콘솔 포트에서 CLI에 직접 액세스합니다. 나중에 36 장, “관리 액세스”.에 따라 텔넷이나 SSH를 사용하여 원격 액세스를 구성할 수 있습니다. 시스템이 이미 다중 컨텍스트 모드에 있는 경우, 콘솔 포트에 액세스하면 시스템 실행 영역으로 이동합니다.

참고 ASAv 콘솔 액세스에 대한 내용은 ASAv 빠른 시작 설명서를 참조하십시오.

어플라이언스 콘솔 액세스

어플라이언스 콘솔에 액세스하려면 다음 단계를 수행하십시오.

절차

1단계 제공된 콘솔 케이블을 사용하여 PC를 콘솔 포트에 연결하고, 전송 속도 9600, 8개 데이터 비트, 패리티 없음, 1개 정지 비트, 흐름 제어 없음으로 설정된 터미널 에뮬레이터를 사용하여 콘솔에 연결합니다.

콘솔 케이블에 대한 자세한 내용은 ASA 하드웨어 설명서를 참조하십시오.

2단계 **Enter** 키를 누르면 다음 프롬프트가 표시됩니다.

ciscoasa>

이 프롬프트는 현재 사용자 EXEC 모드에 있음을 의미합니다. 사용자 EXEC 모드에서는 기본 명령만 사용 가능합니다.

3단계 특권 EXEC 모드에 액세스하려면 다음 명령을 입력합니다.

```
ciscoasa> enable
```

다음 프롬프트가 나타납니다.

비밀번호:

모든 비 컨피그레이션 명령은 특권 EXEC 모드에서 사용할 수 있습니다. 또한 특권 EXEC 모드에서 컨피그레이션 모드를 입력할 수도 있습니다.

4단계 프롬프트에서 enable 비밀번호를 입력합니다.

기본적으로 비밀번호는 비어 있으며 계속하려면 **Enter** 키를 누릅니다. enable 비밀번호를 변경하려면 14-1 페이지의 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정을 참조하십시오.

프롬프트가 다음과 같이 변경됩니다.

```
ciscoasa#
```

특권 모드를 종료하려면 **disable**, **exit** 또는 **quit** 명령을 입력합니다.

5단계 전역 컨피그레이션 모드에 액세스하려면 다음 명령을 입력합니다.

```
ciscoasa# configure terminal
```

프롬프트가 다음과 같이 바뀝니다.

```
ciscoasa(config)#
```

전역 컨피그레이션 모드에서 ASA를 시작할 수 있습니다. 전역 컨피그레이션 모드를 종료하려면 **exit**, **quit** 또는 **end** 명령을 입력합니다.

ASA Services Module 콘솔 액세스

초기 컨피그레이션의 경우에는 스위치에 연결(콘솔 포트에 또는 텔넷/SSH를 사용하여 원격으로)한 다음 ASASM에 연결하여 Command-Line Interface에 액세스합니다. ASASM에는 공장 기본 컨피그레이션이 포함되어 있지 않으므로 ASDM을 사용하여 액세스하기 전에 CLI에서 일부 컨피그레이션을 수행해야 합니다. 이 섹션에서는 ASASM CLI에 액세스하는 방법을 설명합니다.

연결 방법 정보

스위치 CLI에서 다음 두 가지 방법을 사용하여 ASASM에 연결할 수 있습니다.

- 가상 콘솔 연결 — **service-module session** 명령을 사용하여 ASASM에 대한 가상 콘솔 연결을 생성하며, 여기에는 실제 콘솔 연결의 이점과 제한 사항이 모두 포함됩니다.

  혜택은 다음과 같습니다.

  - 다시 로드하는 경우에도 전반적으로 연결이 지속적이며 시간이 초과되지 않습니다.
  - ASASM 다시 로드를 통해 연결을 유지하고 시작 메시지를 볼 수 있습니다.
  - ASASM에서 이미지를 로드할 수 없는 경우 ROMMON에 액세스할 수 있습니다.
  - 초기 비밀번호 컨피그레이션이 필요하지 않습니다.

  제한 사항은 다음과 같습니다.

  - 연결 속도가 느립니다(9600baud).
  - 한 번에 하나의 콘솔만 연결할 수 있습니다.
  - **Ctrl-Shift-6**, **x**가 터미널 서버 프롬프트로 돌아가는 이스케이프 시퀀스인 경우 이 명령을 터미널 서버와 함께 사용할 수 없습니다. **Ctrl-Shift-6**, **x** 는 ASASM 콘솔에서 벗어나 스위치 프롬프트로 돌아가는 시퀀스이기도 합니다. 따라서 이러한 상황에서 ASASM 콘솔을 종료하려는 경우 터미널 서버 프롬프트에 대한 모든 방법을 종료해야 합니다. 스위치에 터미널 서버를 다시 연결할 경우 ASASM 콘솔 세션은 계속 활성화되어 있지만 스위치 프롬프트는 종료할 수 없게 됩니다. 콘솔에서 스위치 프롬프트로 돌아가려면 직접 직렬 연결을 사용해야 합니다. 이 경우 Cisco IOS 소프트웨어에서 터미널 서버 또는 스위치 이스케이프 문자를 변경하거나, 텔넷 **session** 명령을 대신 사용하십시오.

    참고 ASASM에서 올바르게 로그아웃하지 않을 경우 콘솔 연결 상태가 계속 유지되어 의도한 시간보다 오래 연결이 지속될 수 있습니다. 다른 사람이 로그인하려면 기존 연결을 끊어야 합니다.

- 텔넷 연결 — **session** 명령을 사용하여 ASASM에 대한 텔넷 연결을 생성합니다.

  참고 새 ASASM에는 이 방법을 사용하여 연결할 수 없습니다. 이 방법을 사용하려면 ASASM에 대한 텔넷 로그인 비밀번호를 구성해야 합니다(기본 비밀번호 없음). **passwd** 명령을 사용하여 비밀번호를 설정하면 이 방법을 사용할 수 있습니다.

혜택은 다음과 같습니다.

- ASASM에 대한 여러 세션을 동시에 받을 수 있습니다.
- 텔넷 세션은 연결 속도가 빠릅니다.

제한 사항은 다음과 같습니다.

- ASASM이 다시 로드될 경우 텔넷 세션이 종료되며 시간이 초과될 수 있습니다.
- 완전히 로드될 때까지 ASASM에 액세스할 수 없으며 ROMMON에 액세스할 수 없습니다.
- 먼저 텔넷 로그인 비밀번호를 설정해야 합니다. 기본 비밀번호는 없습니다.

ASA Services Module에 로그인

초기 컨피그레이션의 경우에는 스위치에 연결(스위치 콘솔 포트에 또는 텔넷/SSH를 사용하여 원격으로)한 다음 ASASM에 연결하여 Command-Line Interface에 액세스합니다.

시스템이 이미 다중 컨텍스트 모드에 있는 경우 스위치에서 ASASM에 액세스하면 시스템 실행 영역으로 이동합니다.

나중에 텔넷이나 SSH를 사용하여 ASASM에 대한 직접 원격 액세스를 구성할 수 있습니다.

절차

1단계 스위치에서 다음 중 하나를 수행합니다.

- 초기 액세스에 사용 가능한 방법 — 스위치 CLI에서 다음 명령을 입력하여 ASASM에 대한 콘솔 액세스 권한을 얻습니다.

  service-module session [**switch** {**1** | **2**}] **slot** *number*

  예:

  ```
  Router# service-module session slot 3
  ciscoasa>
  ```

  VSS에 있는 스위치의 경우 **switch** 인수를 입력합니다.

  모듈 슬롯 번호를 보려면 스위치 프롬프트에서 **show module** 명령을 입력합니다.

  사용자 EXEC 모드에 액세스합니다.

- 로그인 비밀번호 구성 후 사용 가능한 방법 — 스위치 CLI에서, 텔넷에 다음 명령을 입력하여 백플레인을 통해 ASASM에 연결합니다.

  session [**switch** {**1** |**2**}] **slot** *number* **processor 1**

  로그인 비밀번호를 묻는 메시지가 표시됩니다.

  ```
  ciscoasa passwd:
  ```

  예:

  ```
  Router# session slot 3 processor 1
  ciscoasa passwd: cisco
  ciscoasa>
  ```

  VSS에 있는 스위치의 경우 **switch** 인수를 입력합니다.

  다른 서비스 모듈에서 지원되는 **session** *slot* **processor 0** 명령은 ASASM에서 지원되지 않습니다. ASASM에는 프로세서 0이 없습니다.

  모듈 슬롯 번호를 보려면 스위치 프롬프트에서 **show module** 명령을 입력합니다.

ASASM에 로그인 비밀번호를 입력합니다. **passwd** 명령을 사용하여 비밀번호를 설정합니다. 기본 비밀번호가 없습니다.

사용자 EXEC 모드에 액세스합니다.

2단계 가장 권한 수준이 높은 특권 EXEC 모드에 액세스합니다.

enable

예:

```
ciscoasa> enable
비밀번호:
ciscoasa#
```

프롬프트에서 enable 비밀번호를 입력합니다. 기본적으로 비밀번호는 비어 있습니다.

특권 EXEC 모드를 종료하려면 **disable**, **exit** 또는 **quit** 명령을 입력합니다.

3단계 전역 컨피그레이션 모드 액세스:

configure terminal

전역 컨피그레이션 모드를 종료하려면 **disable**, **exit** 또는 **quit** 명령을 입력합니다.

관련 주제

- 36-1 페이지의 ASDM, 텔넷 또는 SSH를 위한 ASA 액세스 구성.
- 14-1 페이지의 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정

콘솔 세션에서 로그아웃

ASASM에서 로그아웃하지 않으면 콘솔 연결이 지속되므로 시간 제한이 없습니다. ASASM 콘솔 세션을 종료하고 스위치 CLI에 액세스하여 다음 단계를 수행합니다.

다른 사용자가 의도치 않게 열어둔 활성화된 연결을 끊으려면 2-6 페이지의 활성화된 콘솔 연결 끊기를 참조하십시오.

절차

1단계 스위치 CLI로 돌아가려면 다음을 입력합니다.

Ctrl-Shift-6, **x**

스위치 프롬프트로 다시 돌아갑니다.

```
asasm# [Ctrl-Shift-6, x]
Router#
```

참고 미국 및 영국 키보드에서 Shift-6을 누르면 캐럿 기호(^)가 생성됩니다. 다른 키보드를 사용 중이고 탈자 기호(^)를 독립 문자로 생성할 수 없는 경우, 이스케이프 문자를 다른 문자로 변경하는 것이 일시적으로 또는 영구적으로 불가능합니다. **terminal escape-character** *ascii_number* 명령(이 세션에서 변경하려는 경우) 또는 **default escape-character** *ascii_number* 명령(영구적으로 변경하려는 경우)을 사용하십시오. 예를 들어, 현재 세션의 시퀀스를 **Ctrl-w**, **x**로 변경하려면 **terminal escape-character 23**을 입력합니다.

활성화된 콘솔 연결 끊기

ASASM에서 올바르게 로그아웃하지 않을 경우 콘솔 연결 상태가 계속 유지되어 의도한 시간보다 오래 연결이 지속될 수 있습니다. 다른 사람이 로그인하려면 기존 연결을 끊어야 합니다.

절차

1단계 스위치 CLI에서 **show users** 명령을 사용하여 연결된 사용자를 표시합니다. 콘솔 사용자는 "con"으로 표시됩니다. 호스트 주소는 127.0.0.*slot*으로 표시되며 여기서 *slot*은 모듈의 슬롯 번호입니다.

```
Router# show users
```

예를 들어, 다음 명령의 출력 값에는 슬롯 2의 모듈 0에 있는 사용자 "con"이 표시됩니다.

```
Router# show users
Line       User       Host(s)              Idle       Location
*  0       con 0     127.0.0.20            00:00:02
```

2단계 콘솔 연결이 포함된 행을 지우려면 다음 명령을 입력합니다.

```
Router# clear line number
```

예:

```
Router# clear line 0
```

텔넷 세션에서 로그아웃

텔넷 세션을 종료하고 스위치 CLI에 액세스하여 다음 단계를 수행합니다.

절차

1단계 스위치 CLI로 돌아가려면, ASASM 특권 또는 사용자 EXEC 모드에서 **exit**를 입력합니다. 컨피그레이션 모드인 경우 텔넷 세션을 종료할 때까지 **exit**를 반복 입력합니다.

스위치 프롬프트로 다시 돌아갑니다.

```
asasm# exit
Router#
```

참고 또는 이스케이프 시퀀스 **Ctrl-Shift-6**, **x**를 사용하여 텔넷 세션을 종료할 수 있습니다. 이러한 이스케이프 시퀀스를 사용하면 스위치 프롬프트에서 **Enter** 키를 눌러 텔넷 세션을 다시 시작할 수 있습니다. 스위치에서 텔넷 세션의 연결을 끊으려면 스위치 CLI에서 **disconnect**를 입력합니다. 세션의 연결을 끊지 않을 경우 ASASM 컨피그레이션에 따라 시간이 초과될 수 있습니다.

ASDM 액세스 구성

이 섹션에서는 기본 컨피그레이션을 사용하여 ASDM에 액세스하는 방법과 기본 컨피그레이션이 없는 경우 액세스를 컨피그레이션하는 방법에 대해 알아봅니다.

- 2-7 페이지의 ASDM 액세스에 공장 기본 구성 사용(어플라이언스, ASAv)
- 2-8 페이지의 어플라이언스 및 ASAv를 위한 ASDM 액세스 맞춤화
- 2-9 페이지의 ASA Services Module에 대한 ASDM 액세스 구성

ASDM 액세스에 공장 기본 구성 사용(어플라이언스, ASAv)

공장 기본 컨피그레이션을 사용할 경우 ASDM 연결은 기본 네트워크 설정으로 사전 컨피그레이션됩니다.

절차

1단계 다음 인터페이스 및 네트워크 설정을 사용하여 ASDM에 연결합니다.

- 관리 인터페이스는 사용하는 모델에 따라 달라집니다.
  - ASA 5512-X 이상 — ASDM에 연결하는 인터페이스는 Management 0/0입니다.
  - ASAv— ASDM에 연결하는 인터페이스는 Management 0/0입니다.
- 기본 관리 주소는 다음과 같습니다.
  - ASA 어플라이언스 — 192.168.1.1.
  - ASAv— 구축 과정에서 관리 인터페이스 IP 주소를 설정합니다.
- 클라이언트에서는 ASDM 액세스를 허용합니다.
  - ASA 어플라이언스 — 클라이언트는 192.168.1.0/24 네트워크에 있어야 합니다. 기본 컨피그레이션의 경우 DHCP를 지원하므로 관리 스테이션에서는 이 범위 내에 IP 주소를 할당할 수 있습니다.
  - ASAv— 구축 과정에서 관리 클라이언트 IP 주소를 설정합니다. ASAv에서는 연결된 클라이언트의 DHCP 서버로 작동하지 않습니다.

참고 다중 컨텍스트 모드로 변경할 경우, 위의 네트워크 설정을 사용하여 관리자 컨텍스트에서 ASDM에 액세스할 수 있습니다.

관련 주제

- 2-15 페이지의 공장 기본 구성
- 7-15 페이지의 다중 컨텍스트 모드 활성화 또는 비활성화
- 2-12 페이지의 ASDM 시작

어플라이언스 및 ASAv를 위한 ASDM 액세스 맞춤화

다음 조건 중 *하나 이상*이 해당되는 경우 이 절차를 사용하십시오.

- 공장 기본 컨피그레이션이 없는 경우
- 투명 방화벽 모드를 변경하려는 경우
- 다중 컨텍스트 모드로 변경하려는 경우

단일 라우팅 모드의 경우 ASDM에 쉽고 빠르게 액세스하려면 고유한 관리 IP 주소를 설정하는 옵션에 공장 기본 컨피그레이션을 적용하는 것이 좋습니다. 이 섹션의 절차는 투명 또는 다중 컨텍스트 모드 설정 같은 특수한 상황 또는 유지해야 할 다른 컨피그레이션이 있는 경우에만 사용하십시오.

절차

1단계 콘솔 포트에서 CLI에 액세스합니다.

2단계 (선택 사항) 투명 방화벽 모드를 활성화합니다.

이 명령을 실행하면 컨피그레이션이 지워집니다.

```
firewall transparent
```

3단계 관리 인터페이스를 구성합니다.

```
interface management id
   nameif name
   security-level level
   no shutdown
   ip address ip_address mask
```

예:

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level은 1~100 사이의 숫자로 설정하며 100이 가장 안전한 수준입니다.

4단계 (직접 연결된 관리 호스트의 경우) 관리 네트워크에 DHCP 풀을 설정합니다.

```
dhcpd address ip_address-ip_address
interface_name
dhcpd enable interface_name
```

예:

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

범위에 관리 주소가 포함되어 있지 않은지 확인합니다.

5단계 (원격 관리 호스트의 경우) 관리 호스트에 대한 경로를 구성합니다.

```
route management_ifc management_host_ip mask gateway_ip 1
```

예:

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

6단계 ASDM에 대한 HTTP 서버를 활성화합니다.

```
http server enable
```

7단계 관리 호스트에서 ASDM에 액세스하도록 허용합니다.

```
http ip_address mask interface_name
```

예:

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

8단계 컨피그레이션을 저장합니다.

```
write memory
```

9단계 (선택 사항) 모드를 다중 모드로 설정합니다.

```
mode multiple
```

프롬프트가 표시되면 기존 컨피그레이션을 관리자 컨텍스트로 변환할 것을 확인합니다. 그러면 ASA를 다시 로드하라는 메시지가 표시됩니다.

예

다음 컨피그레이션에서는 방화벽 모드를 투명 모드로 변환하고, Management 0/0 인터페이스를 컨피그레이션하고, 관리 호스트에 대한 ASDM을 활성화합니다.

```
firewall transparent
interface management 0/0
    ip address 192.168.1.1 255.255.255.0
    nameif management
    security-level 100
    no shutdown
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

관련 주제

- 2-15 페이지의 공장 기본 구성 복원
- 5-9 페이지의 방화벽 모드 설정(단일 모드)
- 2-2 페이지의 어플라이언스 콘솔 액세스
- 2-12 페이지의 ASDM 시작
- 7 장, “다중 컨텍스트 모드”.

ASA Services Module에 대한 ASDM 액세스 구성

ASASM에는 물리적 인터페이스가 없으므로 ASDM 액세스가 사전 구성되어 있지 않습니다. ASASM에서 CLI를 사용하여 ASDM 액세스를 구성해야 합니다. ASDM 액세스를 위해 ASASM을 구성하려면 다음을 수행하십시오.

시작하기 전에

ASASM 빠른 시작 설명서에 따라 ASASM VLAN 인터페이스를 할당하십시오.

절차

1단계 ASASM에 연결하고 전역 컨피그레이션 모드에 액세스합니다.

2단계 (선택 사항) 투명 방화벽 모드를 활성화합니다.

```
firewall transparent
```

이 명령을 실행하면 컨피그레이션이 지워집니다.

3단계 현재 사용 중인 모드에 따라, 다음 중 하나를 수행하여 관리 인터페이스를 구성합니다.

- 라우팅 모드 — 라우팅 모드에서는 인터페이스를 다음과 같이 구성합니다.

```
interface vlan number
   ip address ip_address [mask]
   nameif name
   security-level level
```

예:

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level은 1~100 사이의 숫자로 설정하며 100이 가장 안전한 수준입니다.

- 투명 모드 — 브릿지 가상 인터페이스를 구성하고 브릿지 그룹에 관리 VLAN을 할당합니다.

```
interface bvi number
   ip address ip_address [mask]

interface vlan number
   bridge-group bvi_number
   nameif name
   security-level level
```

예:

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level은 1~100 사이의 숫자로 설정하며 100이 가장 안전한 수준입니다.

4단계 (직접 연결된 관리 호스트의 경우) 관리 인터페이스 네트워크의 관리 호스트에 대한 DHCP 풀을 활성화합니다.

```
dhcpd address ip_address-ip_address
interface_name
dhcpd enable interface_name
```

예:

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside
ciscoasa(config)# dhcpd enable inside
```

범위에 관리 주소가 포함되어 있지 않은지 확인합니다.

5단계 (원격 관리 호스트의 경우) 관리 호스트에 대한 경로를 구성합니다.

route *management_ifc management_host_ip mask gateway_ip* **1**

예:

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50
```

6단계 ASDM에 대한 HTTP 서버를 활성화합니다.

http server enable

7단계 관리 호스트에서 ASDM에 액세스하도록 허용합니다.

http *ip_address mask interface_name*

예:

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

8단계 컨피그레이션을 저장합니다.

write memory

9단계 (선택 사항) 모드를 다중 모드로 설정합니다.

mode multiple

프롬프트가 표시되면 기존 컨피그레이션을 관리자 컨텍스트로 변환할 것을 확인합니다. 그러면 ASASM를 다시 로드하라는 메시지가 표시됩니다.

예

다음 라우팅 모드 컨피그레이션에서는 VLAN 1 인터페이스를 컨피그레이션하고 관리 호스트에 대한 ASDM를 활성화합니다.

```
interface vlan 1
    nameif inside
    ip address 192.168.1.1 255.255.255.0
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

다음 컨피그레이션에서는 방화벽 모드를 투명 모드로 변환하고, VLAN 1 인터페이스를 컨피그레이션하고 이를 BVI 1에 할당하며, 관리 호스트에 대한 ASDM을 활성화합니다.

```
firewall transparent
interface bvi 1
    ip address 192.168.1.1 255.255.255.0
interface vlan 1
    bridge-group 1
    nameif inside
    security-level 100
dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

관련 주제

- 2-3 페이지의 ASA Services Module 콘솔 액세스
- 7 장, “다중 컨텍스트 모드”.
- 5-9 페이지의 방화벽 모드 설정(단일 모드)

ASDM 시작

다음 두 가지 방법을 사용하여 ASDM을 시작할 수 있습니다.

- ASDM-IDM Launcher — Launcher는 모든 ASA IP 주소에 연결하는 데 사용할 수 있는 웹 브라우저를 사용하여 ASA에서 다운로드하는 애플리케이션입니다. 다른 ASA에 연결하려면 Launcher를 다시 다운로드하지 않아도 됩니다. Launcher를 사용하면 로컬로 다운로드한 파일을 사용하여 데모 모드에서 가상 ASDM을 실행할 수도 있습니다.
- Java Web Start — ASA를 관리하는 모든 경우 웹 브라우저에 연결한 다음 Java Web Start 애플리케이션을 저장하거나 이 애플리케이션을 시작해야 합니다. 선택에 따라 PC에 바로 가기를 저장할 수는 있으나 ASA IP 주소마다 별도의 바로 가기를 지정해야 합니다.

ASDM 내에서는 여러 개의 ASA IP 주소를 선택하여 관리할 수 있습니다. Launcher와 Java Web Start 기능의 주요 차이점은 맨 처음 ASA에 연결하고 ASDM을 시작하는 방법에 있습니다.

ASDM을 사용하면 여러 개의 PC 또는 워크스테이션 간에 동일한 ASA 소프트웨어로 각각 하나의 브라우저 세션을 열 수 있습니다. 하나의 ASA에서는 단일 라우팅 모드에서 최대 5개의 동시 ASDM 세션을 지원할 수 있습니다. ASA에는 PC 또는 워크스테이션당 브라우저 하나에 1개의 세션만 지원됩니다. 다중 컨텍스트 모드의 경우, 컨텍스트당 5개의 동시 ASDM 세션이 지원되며, 각 ASA당 최대 총 32개의 연결이 지원됩니다.

이 섹션에서는 맨 처음 ASDM에 연결한 다음 Launcher 또는 Java Web Start를 사용하여 ASDM을 시작하는 방법에 대해 설명합니다.

절차

1단계 ASDM 클라이언트로 지정한 PC에서 다음 URL을 입력합니다.

`https://`*`asa_ip_address`***`/admin`**

다음 버튼이 있는 ASDM 시작 페이지가 나타납니다.

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

2단계 Launcher를 다운로드하려면

a. **Install ASDM Launcher and Run ASDM**을 클릭합니다.

b. 사용자 이름 및 비밀번호 필드를 비워 두고(신규 설치) **OK**를 클릭합니다. 어떤 HTTPS 인증도 구성되지 않았으므로 사용자 이름 없이, **enable** 비밀번호(기본적으로 비어 있음)를 사용하여 ASDM에 액세스할 수 있습니다. 참고: HTTPS 인증을 활성화한 경우 사용자 이름과 해당 비밀번호를 입력합니다.

c. 설치 프로그램을 PC에 저장한 다음 시작합니다. 설치가 완료되면 ASDM-IDM Launcher가 자동으로 열립니다.

d. 관리 IP 주소를 입력하고 사용자 이름과 비밀번호는 비워 둔 다음(신규 설치의 경우) **OK**를 클릭합니다. 참고: HTTPS 인증을 활성화한 경우 사용자 이름과 해당 비밀번호를 입력합니다.

3단계 Java Web Start를 사용하려면

a. **Run ASDM** 또는 **Run Startup Wizard**를 클릭합니다.

b. 프롬프트에 따라 바로가기를 PC에 저장합니다. 저장하지 않고 열 수도 있습니다.

c. 바로가기에서 Java Web Start를 시작합니다.

d. 표시되는 대화 상자의 안내에 따라 인증서를 승인합니다. Cisco ASDM-IDM Launcher가 나타납니다.

e. 사용자 이름 및 비밀번호를 비워 두고(신규 설치) **OK**를 클릭합니다. 참고: HTTPS 인증을 활성화한 경우 사용자 이름과 해당 비밀번호를 입력합니다.

ASDM에 대한 ID 인증서 설치

Java 7 업데이트 51 이상을 사용할 경우, ASDM Launcher에 신뢰할 수 있는 인증서가 필요합니다. 이 인증서 요구 사항을 손쉽게 해결하는 방법은 자체 서명 ID 인증서를 설치하는 것입니다. 인증서를 설치하기 전까지는 Java Web Start를 사용하여 ASDM을 시작할 수 있습니다.

ASA에 자체 서명 ID 인증서를 설치하여 ASDM을 사용하고, 해당 인증서를 Java에 등록하는 방법에 대한 내용은 다음 문서를 참조하십시오.

http://www.cisco.com/go/asdm-certificate

데모 모드에서 ASDM 사용

별도로 설치되는 애플리케이션인 ASDM 데모 모드를 사용하면 사용 가능한 실제 디바이스가 없어도 ASDM을 실행할 수 있습니다. 이 모드에서는 다음을 수행할 수 있습니다.

- ASDM을 통해 실제 디바이스와 상호 작용하는 것처럼 컨피그레이션 및 선택한 모니터링 작업을 수행합니다.
- ASDM 인터페이스를 사용하여 ASDM 또는 ASA 기능 시연
- CSC SSM을 사용하여 컨피그레이션 및 모니터링 작업을 수행합니다.
- 실시간 syslog 메시지를 비롯하여 시뮬레이션된 모니터링 및 로깅 데이터를 얻을 수 있습니다. 표시되는 데이터는 무작위로 생성되지만, 사용자에게 제공되는 환경은 사용자가 실제 디바이스에 연결했을 때 표시되는 것과 동일합니다.

이 모드는 다음 기능을 지원하도록 업데이트되었습니다.

- 전역 정책 - 단일 라우팅 모드 및 침입 방지가 적용된 ASA
- 객체 NAT - 단일 라우팅 모드 및 방화벽 DMZ가 적용된 ASA
- 봇넷 트래픽 필터 - 단일 라우팅 모드 및 보안 컨텍스트가 적용된 ASA
- IPv6를 사용하는 사이트 대 사이트 VPN(클라이언트리스 SSL VPN 및 IPsec VPN)
- 프로미큐어스 IDS(침입 방지)
- Unified Communication Wizard

이 모드에서는 다음을 지원하지 않습니다.

- GUI에 표시되는 컨피그레이션의 변경 사항 저장
- 파일 또는 디스크 작업

- 내역 모니터링 데이터
- 관리자가 아닌 사용자
- 다음 기능:
  - 파일 메뉴:

    Save Running Configuration to Flash

    Save Running Configuration to TFTP Server

    Save Running Configuration to Standby Unit

    Save Internal Log Buffer to Flash

    Clear Internal Log Buffer
  - 툴 메뉴:

    Command Line Interface

    Ping

    File Management

    Update Software

    File Transfer

    Upload Image from Local PC

    System Reload
  - Toolbar/Status 표시줄 > Save
  - Configuration > Interface > Edit Interface > Renew DHCP Lease
  - 장애 조치 후 스탠바이 디바이스 구성
- 컨피그레이션을 다시 읽는 경우가 발생하는 작업(GUI가 원래 컨피그레이션으로 변환):
  - 컨텍스트 전환
  - 인터페이스 창의 변경 사항
  - NAT 창 변경 사항
  - Clock 창 변경 사항

데모 모드에서 ASDM을 실행하려면 다음 단계를 수행하십시오.

절차

1단계 다음 위치에서 ASDM Demo Mode 설치 프로그램(asdm-demo-*version*.msi)을 다운로드하십시오.
http://www.cisco.com/cisco/web/download/index.html

2단계 설치 프로그램을 두 번 클릭하여 소프트웨어를 설치합니다.

3단계 데스크톱에서 **Cisco ASDM Launcher** 바로 가기를 두 번 클릭하거나 **Start** 메뉴에서 해당 프로그램을 엽니다.

4단계 **Run in Demo Mode** 확인란을 선택합니다.

Demo Mode 창이 나타납니다.

공장 기본 구성

공장 기본 컨피그레이션은 Cisco에서 신규 ASA에 적용하는 컨피그레이션입니다.

- ASA 어플라이언스 — 공장 기본 컨피그레이션을 통해 관리용 인터페이스가 컨피그레이션되므로 ASDM을 함께 사용하여 ASA 어플라이언스에 연결하고 컨피그레이션을 완료할 수 있습니다.
- ASAv— 구축 과정에서 구축 컨피그레이션(초기 가상 구축 설정)을 통해 관리용 인터페이스가 컨피그레이션되므로, ASDM을 함께 사용하여 ASAv에 연결하고 컨피그레이션을 완료할 수 있습니다. 또한 장애 조치 IP 주소를 구성할 수 있습니다. 필요한 경우 "공장 초기화" 컨피그레이션을 적용할 수 있습니다.
- ASASM— 기본 컨피그레이션이 없습니다. 컨피그레이션을 시작하려면 2-3 페이지의 ASA Services Module 콘솔 액세스를 참조하십시오.

공장 기본 컨피그레이션은 라우팅 방화벽 모드 및 단일 컨텍스트 모드에서만 사용할 수 있습니다.

참고 이미지 파일 및 (숨겨진) 기본 컨피그레이션 외에, 플래시 메모리에서는 log/, crypto_archive/ 및 coredumpinfo/coredump.cfg 폴더와 파일이 표준입니다. 이러한 파일의 날짜는 플래시 메모리에 있는 이미지 파일의 날짜와 일치하지 않을 수 있습니다. 이러한 파일은 잠재적인 문제 해결에 도움이 될 수 있으며 오류가 발생한 것으로 간주하지 않습니다.

- 2-15 페이지의 공장 기본 구성 복원
- 2-16 페이지의 ASAv 구축 구성 복원
- 2-17 페이지의 ASA 어플라이언스 기본 구성
- 2-17 페이지의 ASAv 구축 구성

공장 기본 구성 복원

이 섹션에서는 공장 기본 컨피그레이션을 복원하는 방법에 대해 설명합니다. CLI 및 ASDM 절차가 모두 제공됩니다. ASAv의 경우, 이 절차에서는 구축 컨피그레이션을 지우고 ASA 어플라이언스에 적용되는 것과 동일한 공장 기본 컨피그레이션을 적용합니다.

참고 ASASM에서 공장 기본 컨피그레이션을 복원하면 컨피그레이션이 지워지며 공장 기본 컨피그레이션이 존재하지 않습니다.

시작하기 전에

이 기능은 라우팅 방화벽 모드 에서만 사용할 수 있으며, 투명 모드에서는 인터페이스에 대한 IP 주소를 지원하지 않습니다. 또한 이 기능은 단일 컨텍스트 모드에서만 사용할 수 있습니다. 컨피그레이션이 지워진 ASA에는 이 기능을 사용하여 자동으로 컨피그레이션할 수 있는 정의된 컨텍스트가 없습니다.

절차

1단계 기본 ASDM 애플리케이션 창에서 **File > Reset Device to the Factory Default Configuration**을 선택합니다.

Reset Device to the Default Configuration 대화 상자가 나타납니다.

2단계 (선택 사항) 기본 주소 192.168.1.1을 사용하는 대신 관리 인터페이스의 **Management IP address**를 입력합니다.

3단계 (선택 사항) 드롭다운 목록에서 **Management Subnet Mask**를 선택합니다.

4단계 **OK**를 클릭합니다.

확인 대화 상자가 나타납니다.

참고 이 작업을 실행하면 부트 이미지 위치의 위치와 함께 나머지 컨피그레이션도 지워집니다. **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration** 창을 사용하면 외부 메모리의 이미지를 비롯한 특정 이미지에서 부팅을 수행할 수 있습니다. 공장 기본 설정을 복원한 후 다음번에 ASA를 다시 로드 할 경우, 내부 플래시 메모리의 첫 번째 이미지에서 부팅이 이루어집니다. *내부* 플래시 메모리에 이미지가 없는 경우 ASA에서는 부팅을 수행하지 않습니다.

5단계 **Yes**를 클릭합니다.

6단계 기본 컨피그레이션을 복원한 후, 이 컨피그레이션을 내부 플래시 메모리에 저장합니다. **File > Save Running Configuration to Flash**를 선택합니다.

이 옵션을 선택하면 현재 실행 중인 컨피그레이션이 시작 컨피그레이션의 기본 위치에 저장되며, 이전에 다른 위치를 컨피그레이션한 경우에도 마찬가지입니다. 해당 컨피그레이션이 지워지면 이 경로도 지워집니다.

ASAv 구축 구성 복원

이 섹션에서는 ASAv 구축 컨피그레이션을 복원하는 방법에 대해 설명합니다.

절차

1단계 장애 조치를 수행하려면 스탠바이 유닛의 전원을 끕니다.

스탠바이 유닛이 활성화되지 않도록 하려면 전원을 꺼야 합니다. 전원을 계속 켜두면 액티브 유닛 컨피그레이션을 지울 때 스탠바이 유닛이 활성화됩니다. 장애 조치 링크를 통해 이전 액티브 유닛이 다시 로드되고 연결될 경우, 새 액티브 유닛에서 기존 컨피그레이션이 동기화되어 사용자가 원하는 구축 컨피그레이션이 지워집니다.

2단계 다시 로드한 후 구축 컨피그레이션을 복원합니다. 장애 조치를 수행하려면 액티브 유닛에 다음 명령을 입력합니다.

```
write erase
```

참고 ASAv에서는 현재 실행 중인 이미지를 부팅하므로 원본 부트 이미지로 변환되지 않습니다. 원본 부트 이미지를 사용하려면 **boot image** 명령을 참조하십시오.

컨피그레이션을 저장하지 마십시오.

3단계 ASAv를 다시 로드하고 구축 컨피그레이션을 로드합니다.

```
reload
```

4단계 장애 조치를 수행하려면 스탠바이 유닛의 전원을 켭니다.

액티브 유닛이 다시 로드되면 스탠바이 유닛의 전원을 켭니다. 구축 컨피그레이션은 스탠바이 유닛에 동기화됩니다.

ASA 어플라이언스 기본 구성

ASA 어플라이언스에 대한 공장 초기 컨피그레이션에서는 다음을 컨피그레이션합니다.

- 관리 인터페이스 — Management 0/0(관리)
- IP 주소 — 관리 주소는 192.168.1.1/24입니다.
- DHCP 서버 — 관리 호스트에 사용되며 관리 인터페이스에 연결된 PC에서는 192.168.1.2~192.168.1.254 사이의 주소를 받게 됩니다.
- ASDM 액세스 — 관리 호스트를 허용합니다.

컨피그레이션은 다음 명령으로 컨피그레이션됩니다.

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

ASAv 구축 구성

ASAv를 구성할 경우 ASDM을 사용하여 Management 0/0 인터페이스에 연결할 수 있도록 지원하는 다양한 매개변수를 사전 설정할 수 있습니다. 일반적인 컨피그레이션에는 다음과 같은 설정이 포함됩니다.

- Management 0/0 인터페이스:
  - 이름이 지정된 "관리"
  - IP 주소 또는 DHCP
  - 보안 수준 0
  - 관리 전용
- 기본 게이트웨이를 통해 관리 인터페이스에서 관리 호스트 IP 주소에 이르는 고정 경로
- ASDM 서버 사용
- 관리 호스트 IP 주소에 대한 ASDM 액세스
- (선택 사항) GigabitEthernet 0/8 및 Management 0/0 스탠바이 IP 주소에 대한 장애 조치 링크 IP 주소

독립형 유닛의 경우 다음 컨피그레이션을 참조하십시오.

```
interface Management0/0
 nameif management
 security-level 0
 ip address ip_address
 management-only
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
```

장애 조치 쌍에 있는 기본 유닛의 경우 다음 컨피그레이션을 참조하십시오.

```
interface Management0/0
 nameif management
 security-level 0
 ip address ip_address standby standby_ip
 management-only
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

구성 시작

ASA를 구성하고 모니터링하려면 다음 단계를 수행합니다.

1단계 Startup Wizard를 사용하여 초기 컨피그레이션을 수행하려면 **Wizards > Startup Wizard**를 선택합니다.

2단계 IPsec VPN Wizard를 사용하여 IPsec VPN 연결을 구성하려면 **Wizards > IPsec VPN Wizard**를 선택하고 표시되는 각 화면을 완료합니다.

3단계 SSL VPN Wizard를 사용하여 SSL VPN 연결을 구성하려면 **Wizards > SSL VPN Wizard**를 선택하고 표시되는 각 화면을 완료합니다.

4단계 고가용성 및 확장성 설정을 구성하려면 **Wizards > High Availability and Scalability Wizard**를 선택합니다.

5단계 Packet Capture Wizard를 사용하여 패킷 캡처를 구성하려면 **Wizards > Packet Capture Wizard**를 선택합니다.

6단계 ASDM GUI에서 사용 가능한 다른 색상 및 스타일을 표시하려면 **View > Office Look and Feel**을 선택합니다.

7단계 기능을 컨피그레이션하려면 툴바에서 **Configuration** 버튼을 선택한 다음 기능 버튼 중 하나를 클릭하여 관련 컨피그레이션 창에 표시합니다.

참고 Configuration 화면이 비어 있는 경우 툴바에서 **Refresh**를 클릭하여 화면 내용을 표시합니다.

8단계 ASA를 모니터링하려면 툴바에서 **Monitoring** 버튼을 클릭한 다음 기능 버튼을 클릭하여 관련 모니터링 창을 표시합니다.

참고 ASDM에서는 최대 512KB의 컨피그레이션을 지원합니다. 이 용량을 초과할 경우 성능 문제가 발생할 수 있습니다.

ASDM에서 Command Line Interface 툴 사용

이 섹션에서는 ASDM을 사용하여 명령을 입력하고 CLI를 활용하는 방법에 대해 설명합니다.

- 2-19 페이지의 Command Line Interface 툴 사용
- 2-20 페이지의 ASDM에서 무시된 명령을 디바이스에서 표시

Command Line Interface 툴 사용

이 기능에서는 ASA에 명령을 보내고 결과를 볼 수 있는 텍스트 기반 툴을 제공합니다.

CLI 툴을 사용하여 입력할 수 있는 명령은 사용자 권한에 따라 달라집니다. 기본 ASDM 애플리케이션 창의 하단에 있는 상태 표시줄에서 권한 수준을 검토하여 특권 수준 CLI 명령을 실행하는 데 필요한 권한을 보유하고 있는지 확인합니다.

시작하기 전에

- ASDM CLI 툴을 통해 입력된 명령은 터미널 연결을 통해 ASA에 입력된 명령과 다르게 작동할 수 있습니다.
- 명령 오류 — 잘못된 명령을 입력하여 오류가 발생할 경우, 잘못된 명령은 건너뛰게 되며 나머지 명령이 처리됩니다. Response 영역에 표시되는 메시지에는 오류 발생 여부 및 기타 관련 정보에 대한 내용이 포함되어 있습니다.
- 대화형 명령 — CLI 툴에서는 대화형 명령이 지원되지 않습니다. 이러한 명령을 ASDM에서 사용하려면 **noconfirm** 키워드가 제공되는 경우 이 키워드를 다음 명령에 표시된 것처럼 사용합니다.

  ```
  crypto key generate rsa modulus 1024 noconfirm
  ```

- 다른 관리자와 충돌 방지 — 여러 관리자가 ASA의 현재 실행 중인 컨피그레이션을 업데이트할 수 있습니다. ASDM CLI 툴을 사용하여 컨피그레이션을 변경하기 전에 다른 관리 세션이 활성화되어 있지 않은지 확인하십시오. 여러 명의 사용자가 동시에 ASA를 구성 중인 경우 가장 최근에 수정한 변경 사항이 적용됩니다.

  같은 ASA에서 현재 활성화된 다른 관리 세션을 보려면 **Monitoring > Properties > Device Access**를 선택합니다.

절차

1단계 기본 ASDM 애플리케이션 창에서 **Tools > Command Line Interface**를 선택합니다.

Command Line Interface 대화 상자가 나타납니다.

2단계 원하는 명령 유형(한 줄 또는 여러 줄)을 선택한 다음 드롭다운 목록에서 해당 명령을 선택하거나 제공된 필드에 명령을 입력합니다.

3단계 **Send**를 클릭하여 명령을 실행합니다.

4단계 새 명령을 입력하려면 **Clear Response**를 클릭한 후 실행할 다른 명령을 선택하거나 입력합니다.

5단계 이 기능의 상황별 도움말을 제공하려면 **Enable context-sensitive help (?)** 확인란을 선택합니다. 상황별 도움말을 사용하지 않으려면 이 확인란의 선택을 취소합니다.

6단계 Command Line Interface 대화 상자를 닫은 후 컨피그레이션을 변경한 경우 ASDM에서 변경 내용을 보려면 **Refresh**를 클릭합니다.

ASDM에서 무시된 명령을 디바이스에서 표시

이 기능을 사용하면 ASDM에서 지원하지 않는 명령을 표시할 수 있습니다. 일반적으로 ASDM에서는 다음 명령이 무시됩니다. ASDM에서는 실행 중인 컨피그레이션에서 이러한 명령을 변경하거나 제거하지 않습니다. 자세한 내용은 3-32 페이지의 지원되지 않는 명령를 참조하십시오.

절차

1단계 기본 ASDM 애플리케이션 창에서 **Tools > Show Commands Ignored by ASDM on Device**를 선택합니다.

2단계 작업이 완료되면 **OK**를 클릭합니다.

ASDM 구성 메모리 늘리기

ASDM에서는 컨피그레이션 크기를 최대 512KB까지 지원합니다. 이 용량을 초과할 경우 성능 문제가 발생할 수 있습니다. 예를 들어, 컨피그레이션을 로드했을 때 상태 대화 상자에 완료된 컨피그레이션의 백분율이 표시되어 있지만 많은 양의 컨피그레이션이 늘어나지 않은 채 작업이 일시 중단된 것처럼 보일 수 있습니다. 이러한 현상은 ASDM에서 컨피그레이션을 계속 처리 중인 경우에도 일어날 수 있습니다. 이러한 상황이 발생할 경우 ASDM 시스템 힙 메모리를 늘리는 방안을 고려하는 편이 좋습니다.

ASDM 힙 메모리 크기를 늘리려면 다음 절차를 수행하여 Launcher 바로 가기를 수정합니다.

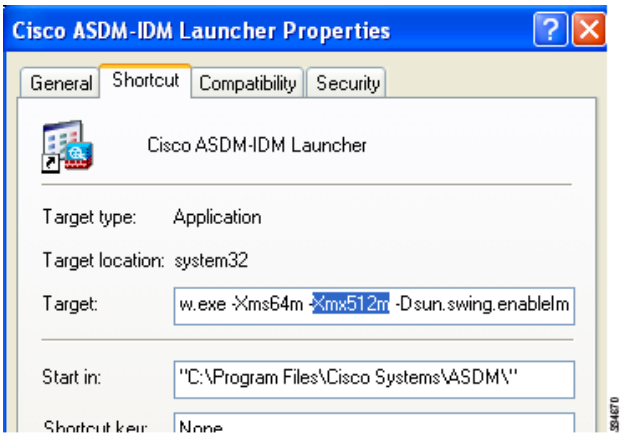
절차

1단계 Windows의 경우:

a. ASDM-IDM Launcher의 바로 가기를 마우스 오른쪽 버튼으로 클릭하고 **Properties**를 선택합니다.

b. **Shortcut** 탭을 클릭합니다.

c. **Target** 필드에서 접두사가 "-Xmx"인 인수를 변경하여 원하는 힙 크기를 지정합니다. 예를 들어, 768MB로 지정하려면 -Xmx768M으로 변경하고 1GB로 지정하려면 -Xmx1G로 변경합니다.



2단계 Macintosh의 경우:

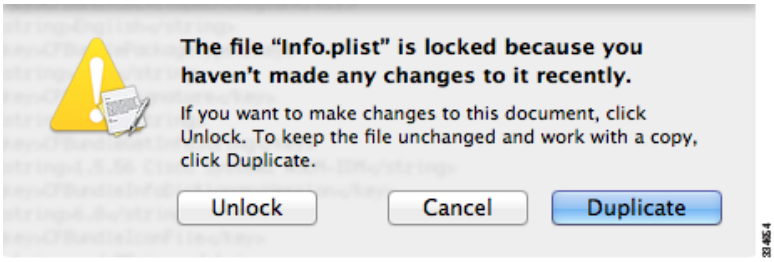
a. **Cisco ASDM-IDM** 아이콘을 마우스 오른쪽 버튼으로 클릭하고 **Show Package Contents**를 선택합니다.

b. **Contents** 폴더에서 **Info.plist** 파일을 두 번 클릭합니다. Developer 툴을 설치한 경우, 파일이 **Property List Editor**에서 열립니다. 그렇지 않을 경우 **TextEdit**에서 파일이 열립니다.

c. **Java > VMOptions** 아래에서 접두사가 "-Xmx"인 문자열을 변경하여 원하는 힙 크기를 지정합니다. 예를 들어, 768MB로 지정하려면 -Xmx768M으로 변경하고 1GB로 지정하려면 -Xmx1G로 변경합니다.

```
<key>Java</key>
<dict>
        <key>WorkingDirectory</key>
        <string>$APP_PACKAGE/Contents/Resources/Java</string>
        <key>VMOptions</key>
        <string>-Xms64mm -Xmx512mm</string>
        <key>MainClass</key>
        <string>com.cisco.launcher.Launcher</string>
        <key>JVMVersion</key>
        <string>1.5+</string>
```

d. 이 파일이 잠겨 있을 경우 다음과 같은 오류 메시지가 표시됩니다.



e. **Unlock**을 클릭하고 파일을 저장합니다.

Unlock 대화 상자가 표시되지 않을 경우 편집기를 종료하고 **Cisco ASDM-IDM** 아이콘을 마우스 오른쪽 버튼으로 클릭한 다음 **Copy Cisco ASDM-IDM**을 선택하고 쓰기 권한이 있는 위치(예: 데스크톱)에 이를 붙여넣습니다. 그런 다음 이 복사본의 힙 크기를 변경합니다.

연결에 구성 변경 사항 적용

컨피그레이션에 대한 보안 정책을 변경하면 모든 *새* 연결에서는 새로운 보안 정책을 사용합니다. 기존 연결에서는 연결을 설정할 당시 구성된 정책을 계속 사용합니다. 기존 연결에 대한 **show** 명령 출력에는 기존 컨피그레이션이 반영되며, 경우에 따라 기존 연결에 대한 데이터가 포함되지 않을 수도 있습니다.

예를 들어, 인터페이스에서 QoS **service-policy**를 제거하고 수정된 버전을 다시 추가할 경우, **show service-policy** 명령에서는 새 서비스 정책과 일치하는 새 연결과 연관된 QoS 카운터만 표시합니다. 명령 출력에는 기존 정책에 대한 기존 연결이 더 이상 표시되지 않습니다.

모든 연결에 새 정책이 사용되도록 하려면 현재 연결을 끊은 다음 모든 연결에서 새 정책을 사용하여 다시 연결하도록 해야 합니다.

연결을 끊으려면 다음 명령 중 하나를 입력합니다.

- **clear local-host** [*ip_address*] [**all**]

  이 명령을 사용하면 연결 제한 및 초기 제한 같은 클라이언트당 런타임 상태가 다시 초기화됩니다. 결과적으로 이 명령을 사용하면 이러한 제한을 사용하는 모든 연결이 제거됩니다. 호스트당 모든 현재 연결을 보려면 **show local-host all** 명령을 참조하십시오.

  인수가 없는 경우에도 이 명령을 사용하면 영향을 받는 모든 스루더박스(through-the-box) 연결이 지워집니다. 투더박스(to-the-box) 연결(현재 관리 세션 포함)도 지우려면 **all** 키워드를 사용합니다. 특정 IP 주소에서 연결을 지우려면 *ip_address* 인수를 사용합니다.

- **clear conn** [**all**] [**protocol** {**tcp** | **udp**}] [**address** *src_ip*[**-***src_ip*] [**netmask** *mask*]] [**port** *src_port*[**-***src_port*]] [**address** *dest_ip*[**-***dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[**-***dest_port*]]

  이 명령을 사용하면 모든 상태의 연결이 종료됩니다. 모든 현재 연결을 보려면 **show conn** 명령을 참조합니다.

  인수가 없는 경우에도 이 명령을 사용하면 모든 스루더박스(through-the-box) 연결이 지워집니다. 투더박스(to-the-box) 연결(현재 관리 세션 포함)도 지우려면 **all** 키워드를 사용합니다. 소스 IP 주소, 목적지 IP 주소, 포트 및/또는 프로토콜을 기준으로 특정 연결을 지우기 위해 원하는 옵션을 지정할 수 있습니다.

3 장

ASDM 그래픽 사용자 인터페이스

이 장에서는 ASDM 사용자 인터페이스를 사용하는 방법에 대해 설명합니다.

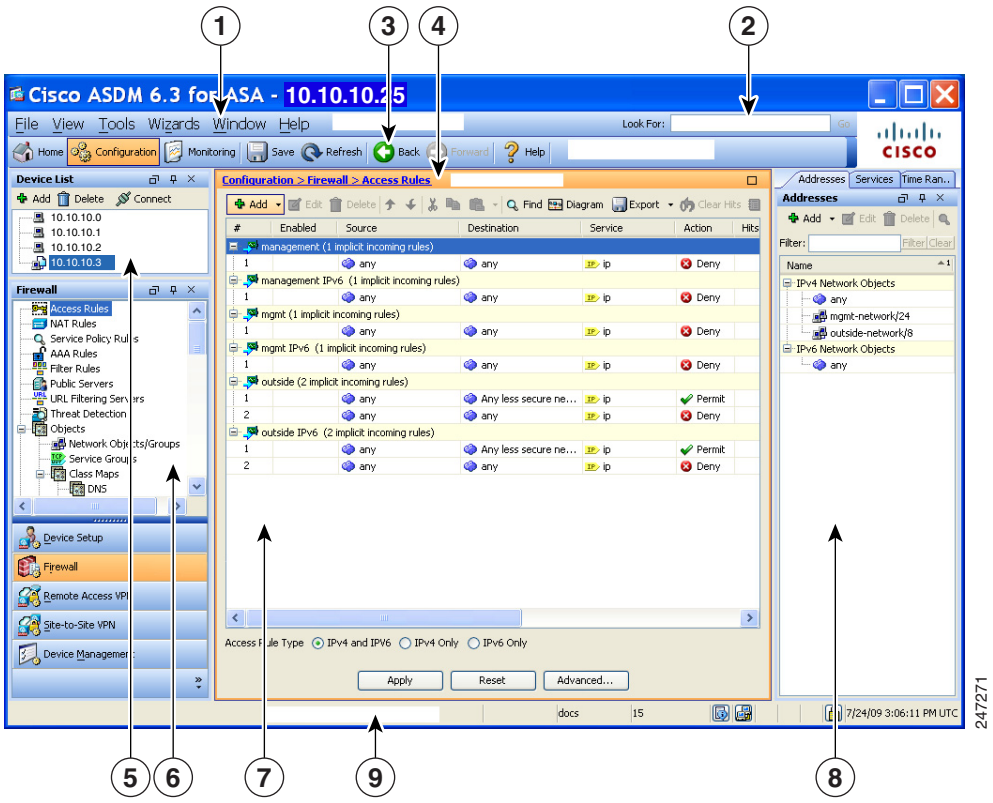
ASDM 사용자 인터페이스 정보

ASDM 사용자 인터페이스는 ASA에서 지원하는 다양한 기능에 쉽게 액세스할 수 있도록 설계되었습니다. ASDM 사용자 인터페이스에는 다음 요소가 포함됩니다.

- 파일, 툴, 마법사, 도움말에 빠른 액세스를 제공하는 메뉴 모음. 많은 메뉴 항목에는 키보드 바로 가기가 있습니다.
- ASDM을 탐색할 수 있는 툴바 툴바에서 **Home**, **Configuration** 및 **Monitoring** 창에 액세스할 수 있습니다. 또한 도움말을 참조하고 여러 창을 이동할 수 있습니다.
- 고정 가능한 **Navigation** 창을 **Configuration** 및 **Monitoring** 창을 통해 이동할 수 있습니다. 헤더의 세 가지 버튼 중 하나를 클릭하여 이 창을 최대화하거나 복원할 수 있으며, 움직이는 창으로 만들어 이를 이동하고 숨기거나 닫을 수 있습니다. **Configuration** 및 **Monitoring** 창에 액세스하려면 다음 중 하나를 수행합니다.
  - 왼쪽 **Navigation** 창에서 애플리케이션 창의 왼쪽에 있는 링크를 클릭합니다. 그러면 **Content** 창에서 선택한 창의 제목 표시줄에 경로가 표시됩니다(예: **Configuration > Device Setup > Startup Wizard**)
  - 정확한 경로를 알고 있는 경우 왼쪽 **Navigation** 창의 링크를 클릭하지 않고 애플리케이션 창의 오른쪽에 있는 **Content** 창의 제목 표시줄에 직접 경로를 입력할 수 있습니다.
- **Content** 창의 오른쪽 모서리에 있는 최대화 및 복원 버튼을 사용하면 왼쪽 **Navigation** 창을 숨기고 표시할 수 있습니다.
- 고정 가능한 **Device List** 창에는 ASDM을 통해 액세스할 수 있는 디바이스 목록이 표시됩니다. 헤더의 세 가지 버튼 중 하나를 클릭하여 이 창을 최대화하거나 복원할 수 있으며, 움직이는 창으로 만들어 이를 이동하고 숨기거나 닫을 수 있습니다.
- 애플리케이션 창의 아래쪽에 있는 상태 표시줄에는 시간, 연결 상태, 사용자, 메모리 상태, 실행 중인 컨피그레이션, 권한 수준, SSL 상태가 표시됩니다.
- 왼쪽 **Navigation** 창에는 액세스 규칙, NAT 규칙, AAA 규칙, 필터 규칙, 서비스 규칙을 생성할 때 규칙 테이블에서 사용할 수 있는 다양한 객체가 표시됩니다. 이 창 내의 탭 제목은 사용자가 보고 있는 기능에 따라 변경됩니다. 또한 이 창에는 **ASDM Assistant**가 표시됩니다.

3-3 페이지의 그림 3-1에는 ASDM 사용자 인터페이스의 요소를 표시됩니다.

그림 3-1 ASDM 사용자 인터페이스



범례

GUI 요소	설명
1	메뉴 모음
2	검색 필드
3	툴바
4	탐색 경로
5	디바이스 목록 창
6	왼쪽 탐색 창
7	콘텐츠 창
8	오른쪽 탐색 창
9	상태 표시줄

참고 **Wizards**, **Configuration** 및 **Monitoring** 창, **Status Bar**를 비롯한 GUI의 다양한 부분에 툴 설명이 추가되었습니다. 툴 설명을 보려면 상태 표시줄의 아이콘 같은 특정한 사용자 인터페이스 요소에 마우스 커서를 올려놓습니다.

ASDM 사용자 인터페이스 탐색

ASDM 사용자 인터페이스 전체를 효율적으로 이동하기 위해 이전 섹션에서 설명한 메뉴, 툴바, 고정 가능한 창, 왼쪽 및 오른쪽 **Navigation** 창을 사용할 수 있습니다. 제공되는 기능은 **Device List** 창 아래의 버튼 목록에 표시됩니다. 예시 목록에 다음과 같은 기능 버튼이 포함될 수 있습니다.

- **Device Setup**
- **Firewall**
- **Trend Micro Content Security**
- **봇넷 트래픽 필터**
- **Remote Access VPN**
- **Site to Site VPN**
- **Device Management**

표시되는 기능 버튼의 목록은 구매한 라이센스 기능을 기준으로 합니다. Configuration 뷰 또는 Monitoring 뷰를 위해 선택한 기능의 첫 번째 창에 액세스하려면 각 버튼을 클릭합니다. 기능 버튼은 Home 뷰에서는 제공되지 않습니다.

기능 버튼의 표시를 변경하려면 다음 단계를 수행합니다.

1단계 마지막 기능 버튼 아래에서 드롭다운 목록을 선택하여 컨텍스트 메뉴를 표시합니다.

2단계 다음 옵션 중 하나를 선택합니다.

- 버튼을 더 많이 표시하려면 **Show More Buttons**를 클릭합니다.
- 버튼을 더 적게 표시하려면 **Show Fewer Buttons**를 클릭합니다.
- 버튼을 추가하거나 제거하려면 **Add or Remove Buttons**를 클릭한 다음 표시되는 목록에서 추가 또는 제거할 버튼을 클릭합니다.
- 버튼 목록이 현재 순서대로 표시되는 **Option** 대화 상자를 표시하려면 **Option**을 선택합니다. 다음 중 하나를 선택합니다.
  - **Move Up**을 클릭하여 목록의 버튼을 위로 이동합니다.
  - **Move Down**을 클릭하여 목록의 버튼을 아래로 이동합니다.
  - **Reset**을 클릭하여 목록에 있는 항목의 순서를 기본 설정으로 되돌립니다.

3단계 **OK**를 클릭하여 설정을 저장하고 이 대화 상자를 닫습니다.

메뉴

마우스 또는 키보드를 사용하여 ASDM 메뉴에 액세스할 수 있습니다. 키보드에서 메뉴 모음에 액세스하는 방법에 대한 자세한 내용은 3-13 페이지의 키보드 바로 가기를 참조하십시오.

ASDM에는 다음 메뉴가 포함됩니다.

- 3-5 페이지의 파일 메뉴
- 3-6 페이지의 뷰 메뉴
- 3-7 페이지의 툴 메뉴

파일 메뉴

File 메뉴를 사용하면 ASA 컨피그레이션을 관리할 수 있습니다. 다음 표에는 **File** 메뉴를 사용하여 수행할 수 있는 작업이 나와 있습니다.

File 메뉴 항목	설명
Refresh ASDM with the Running Configuration on the Device	실행 중인 컨피그레이션의 복사본을 ASDM에 로드합니다.
Refresh	실행 중인 컨피그레이션의 현재 복사본이 ASDM에 포함되도록 합니다.
Reset Device to the Factory Default Configuration	컨피그레이션을 공장 기본값으로 복원합니다.
Show Running Configuration in New Window	현재 실행 중인 컨피그레이션을 새 창에 표시합니다.
Save Running Configuration to Flash	실행 중인 컨피그레이션의 복사본을 플래시 메모리에 씁니다.
Save Running Configuration to TFTP Server	현재 실행 중인 컨피그레이션 파일의 복사본을 TFTP 서버에 저장합니다.
Save Running Configuration to Standby Unit	기본 유닛에서 실행 중인 컨피그레이션 파일의 복사본을 장애조치 스탠바이 유닛의 실행 중인 컨피그레이션 파일로 전송합니다.
Save Internal Log Buffer to Flash	내부 로그 버퍼를 플래시 메모리에 저장합니다.
Print	현재 페이지를 인쇄합니다. 규칙을 인쇄할 경우 가로 페이지 방향을 사용하는 것이 좋습니다. Internet Explorer를 사용할 경우, 서명된 애플릿을 처음에 수락했다면 인쇄 권한이 이미 부여된 상태입니다.
Clear ASDM Cache	로컬 ASDM 이미지를 제거합니다. ASDM에서는 ASDM에 연결할 경우 이미지를 로컬로 다운로드합니다.
Clear ASDM Password Cache	새 비밀번호를 정의했으나 새 비밀번호와 다른 기존 비밀번호를 아직 보유한 경우 비밀번호 캐시를 제거합니다.
Clear Internal Log Buffer	syslog 메시지 버퍼를 비웁니다.
끝내기	ASDM을 닫습니다.

뷰 메뉴

View 메뉴를 사용하면 ASDM 사용자 인터페이스의 다양한 부분을 표시할 수 있습니다. 특정 항목은 현재 뷰에 따라 달라집니다. 현재 뷰에 표시할 수 없는 항목은 선택할 수 없습니다. 다음 표에는 **View** 메뉴를 사용하여 수행할 수 있는 작업이 나와 있습니다.

View 메뉴 항목	설명
Home	Home 뷰가 표시됩니다.
Configuration	Configuration 뷰가 표시됩니다.
Monitoring	Monitoring 뷰가 표시됩니다.
Device List	도킹 가능한 창에 디바이스 목록이 표시됩니다. 자세한 내용은 3-12 페이지의 Device List를 참조하십시오.
Navigation	Configuration 및 Monitoring 뷰에서 **Navigation** 창을 표시하거나 숨깁니다.
ASDM Assistant	특정 작업에 유용한 ASDM 절차가 포함된 도움말을 검색하고 찾습니다. 자세한 내용은 3-10 페이지의 ASDM Assistant를 참조하십시오.
SIP Details	음성 네트워크 정보를 표시하고 숨깁니다.
Latest ASDM Syslog Messages	Home 뷰에서 **Latest ASDM Syslog Messages** 창을 표시하거나 숨깁니다. 이 창은 Home 뷰에서만 사용할 수 있습니다. 가장 최신 릴리스로 업그레이드하기에 충분한 메모리가 없는 경우, 어떤 메모리가 설치되어 있고 필요한 메모리가 무엇인지 나타내는 syslog 메시지 %ASA-1-211004가 생성됩니다. 이 메시지는 메모리를 업그레이드할 때까지 24시간마다 표시됩니다.
Addresses	**Addresses** 주소 창을 표시하고 숨깁니다. **Addresses** 창은 Configuration 뷰의 **Access Rules**, **NAT Rules**, **Service Policy Rules**, **AAA Rules**, **Filter Rules** 창에만 사용할 수 있습니다.
Services	**Services** 창을 표시하고 숨깁니다. **Services** 창은 Configuration 뷰의 **Access Rules**, **NAT Rules**, **Service Policy Rules**, **AAA Rules**, **Filter Rules** 창에만 사용할 수 있습니다.
Time Ranges	**Time Ranges** 창을 표시하고 숨깁니다. **Time Ranges** 창은 Configuration 뷰의 **Access Rules**, **Service Policy Rules**, **AAA Rules**, **Filter Rules**에만 사용할 수 있습니다.
Global Pools	**Global Pools** 창을 표시하고 숨깁니다. **Global Pools** 창은 Configuration 뷰의 **NAT Rules** 창에만 사용할 수 있습니다.
Find in ASDM	기능 또는 **ASDM Assistant** 등 검색하려는 항목을 찾습니다.
Back	이전 창으로 돌아갑니다. 자세한 내용은 3-12 페이지의 일반 버튼를 참조하십시오.
Forward	이전에 방문한 다음 창으로 이동합니다. 자세한 내용은 3-12 페이지의 일반 버튼를 참조하십시오.
Reset Layout	레이아웃이 기본 컨피그레이션으로 돌아갑니다.
Office Look and Feel	화면 글꼴 및 색상을 Microsoft Office 설정으로 변경합니다.

툴 메뉴

Tools 메뉴에서는 ASDM에서 사용할 수 있는 다음과 같은 툴을 제공합니다.

Tools 메뉴 항목	설명
Command Line Interface	명령을 ASA로 보내고 결과를 봅니다.
Show Commands Ignored by ASDM on Device	ASDM에서 무시한 지원되지 않는 명령이 표시됩니다.
Packet Tracer	패킷을 지정된 소스 및 인터페이스에서 목적지까지 추적합니다. 프로토콜 및 모든 유형의 데이터 포트를 지정하고, 패킷에 수행한 작업에 대한 세부 정보와 함께 패킷의 수명을 볼 수 있습니다. 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.
Ping	ASA 및 주변 통신 링크의 컨피그레이션과 작동을 확인하고, 다른 네트워크 디바이스의 기본 테스트를 수행합니다. 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.
Traceroute	패킷이 목적지로 전달되는 경로를 결정합니다. 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.
File Management	플래시 메모리에 저장된 파일을 보기, 이동, 복사 및 삭제할 수 있습니다. 또한 플래시 메모리에 디렉터리를 생성할 수 있습니다. TFTP, 플래시 메모리, 로컬 PC를 비롯한 다양한 파일 시스템 간에 파일을 전송할 수도 있습니다.
Upgrade Software from Local Computer	ASA 이미지, ASDM 이미지 또는 PC의 기타 이미지를 플래시 메모리에 업로드합니다.
Check for ASA/ASDM Updates	마법사를 통해 ASA 소프트웨어 및 ASDM 소프트웨어를 업그레이드합니다.
Backup Configurations	ASA 컨피그레이션, Cisco Secure Desktop 이미지, SSL VPN Client 이미지 및 프로파일을 백업합니다.
Restore Configurations	ASA 컨피그레이션, Cisco Secure Desktop 이미지, SSL VPN Client 이미지 및 프로파일을 복원합니다.
System Reload	ASDM을 다시 시작하고 저장된 컨피그레이션을 메모리에 다시 로드합니다.
Administrator's Alerts to Clientless SSL VPN Users	관리자가 알림 메시지를 클라이언트리스 SSL VPN 사용자에게 보낼 수 있도록 지원합니다. 자세한 내용은 VPN 컨피그레이션 가이드를 참조하십시오.

Tools 메뉴 항목	설명
Migrate Network Object Group Members	8.3 이상으로 마이그레이션할 경우 ASA에서는 명명된 네트워크 객체를 생성하여 일부 기능의 인라인 IP 주소를 교체합니다. 명명된 객체 외에도, ASDM에서는 컨피그레이션에 사용된 모든 IP 주소를 대상으로 명명되지 않은 객체를 자동으로 생성합니다. 이러한 자동 생성된 객체는 *IP address*로만 확인되고 이름이 없으며 플랫폼 컨피그레이션에서 명명된 객체로 존재하지 않습니다. 마이그레이션 시 ASA에서 명명된 객체를 생성할 경우, 일치하는 명명되지 않은 ASDM 전용 객체가 명명된 객체와 교체됩니다. 유일한 예외 사항은 네트워크 객체 그룹의 명명되지 않은 객체입니다. ASA에서 네트워크 객체 그룹에 있는 IP 주소의 명명된 객체를 생성할 경우, ASDM에서는 명명되지 않은 객체를 그대로 유지할 뿐만 아니라 ASDM에서 중복된 객체를 생성합니다. 이러한 객체를 병합하려면 **Tools > Migrate Network Object Group Members**를 선택합니다. 자세한 내용은 *Cisco ASA 5500 Migration to Version 8.3 and Later*를 참조하십시오.
Preferences	세션 간에 지정된 ASDM 기능의 동작을 변경합니다. 자세한 내용은 3-30 페이지의 ASDM 기본 설정 정의를 참조하십시오.
ASDM Java Console	Java 콘솔이 표시됩니다.

Wizards 메뉴

Wizards 메뉴를 사용하면 여러 기능을 구성하는 데 필요한 마법사를 실행할 수 있습니다. 다음 표에는 제공되는 Wizards 및 해당 기능의 목록이 나와 있습니다.

Wizards 메뉴 항목	설명
Startup Wizard	ASA의 초기 컨피그레이션을 처음부터 끝까지 단계별로 안내합니다.
IPsec VPN Wizard	ASA에서 IPsec VPN 정책을 구성할 수 있습니다. 자세한 내용은 VPN 컨피그레이션 가이드를 참조하십시오.
SSL VPN Wizard	ASA에서 SSL VPN 정책을 구성할 수 있습니다. 자세한 내용은 VPN 컨피그레이션 가이드를 참조하십시오.
High Availability and Scalability Wizard	장애 조치를 구성할 수 있음: VPN 클러스터 로드 밸런싱 또는 ASA에서 ASA 클러스터링
Unified Communication Wizard	ASA에서 IP 전화기 같은 유니파이드 커뮤니케이션 기능을 구성할 수 있습니다. 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

Wizards 메뉴 항목	설명
ASDM Identity Certificate 마법사	Java 7 업데이트 51 이상을 사용할 경우, ASDM Launcher에 신뢰할 수 있는 인증서가 필요합니다. 이 인증서 요구 사항을 손쉽게 해결하는 방법은 자체 서명 ID 인증서를 설치하는 것입니다. 이 마법사를 활용하면 인증서를 설치하기 전까지는 Java Web Start를 사용하여 ASDM을 시작할 수 있습니다. 자세한 내용은 http://www.cisco.com/go/asdm-certificate를 참조하십시오.
Packet Capture Wizard	ASA에서 패킷 캡처를 구성할 수 있습니다. 이 마법사에서는 각 인그레스(ingress) 및 이그레스(egress) 인터페이스에서 하나의 패킷 캡처를 실행합니다. 캡처를 실행한 후에는 이를 컴퓨터에 저장한 다음 패킷 분석기로 캡처를 검토하고 분석할 수 있습니다.

창 메뉴

Window 메뉴를 사용하면 ASDM 창 사이를 이동할 수 있습니다. 활성 창은 선택한 창으로 표시됩니다.

도움말 메뉴

Help 메뉴에서는 온라인 도움말에 대한 링크와 함께 ASDM 및 ASA에 대한 정보를 제공합니다. 다음 표에는 **Help** 메뉴를 사용하여 수행할 수 있는 작업 목록이 나와 있습니다.

Help 메뉴 항목	설명
Help Topics	내용, 창 이름 순서로 왼쪽 프레임에 색인화된 새 브라우저 창을 엽니다. 이러한 방법을 사용하여 모든 주제에 대한 도움말을 찾거나 **Search** 탭을 사용하여 검색합니다.
Help for Current Screen	해당 화면에 대한 상황별 도움말을 엽니다. 마법사에서는 현재 열려 있는 화면, 창 또는 대화 상자를 실행합니다. 또는 **question mark (?) help** 아이콘을 클릭할 수도 있습니다.
Release Notes	Cisco.com에서 *ASDM 릴리스 정보*의 최신 버전을 엽니다. 릴리스 정보에는 ASDM 소프트웨어 및 하드웨어 요구 사항에 대한 최신 정보와 소프트웨어의 변경 사항에 대한 최신 정보가 포함됩니다.
ASDM Assistant	Cisco.com에서 다운로드 가능한 콘텐츠를 검색할 수 있는 **ASDM Assistant**를 엽니다. 특정 작업을 수행하는 방법에 대한 세부 정보도 함께 포함됩니다.
About Cisco Adaptive Security Appliance (ASA)	소프트웨어 버전, 하드웨어 집합, 시작 시 로드된 컨피그레이션 파일, 시작 시 로드된 소프트웨어 이미지를 비롯하여 ASA에 대한 정보가 표시됩니다. 이러한 정보는 문제 해결에 도움이 됩니다.
About Cisco ASDM	소프트웨어 버전, 호스트 이름, 권한 수준, 운영 체제, 디바이스 유형, Java 버전 같은 ASDM에 대한 정보가 표시됩니다.

툴바

아래의 **Toolbar** 메뉴에서는 Home 뷰, Configuration 뷰, Monitoring 뷰에 대한 액세스를 제공합니다. 또한 이 메뉴를 사용하면 다중 컨텍스트 모드에서 시스템 컨텍스트와 보안 컨텍스트 중에서 선택할 수 있으며, 탐색 및 자주 사용되는 기타 기능을 제공합니다. 다음 표에는 **Toolbar** 메뉴를 사용하여 수행할 수 있는 작업 목록이 나와 있습니다.

Toolbar 버튼	설명
System/Contexts	현재 어떤 컨텍스트에 있는지 표시됩니다. 컨텍스트 목록을 열려면 왼쪽 창에서 **down** 화살표를 클릭하고, 컨텍스트 드롭다운 목록을 복원하려면 **up** 화살표를 클릭합니다. 이 목록을 확장한 후 창을 축소하려면 **left** 화살표를 클릭하고, 창을 복원하려면 **right** 화살표를 클릭합니다. 시스템을 관리하려면 드롭다운 목록에서 **System**을 선택합니다. 컨텍스트를 관리하려면 드롭다운 목록에서 컨텍스트를 선택합니다.
Home	인터페이스의 상태, 실행 중인 버전, 라이센스 정보, 성능 등 ASA에 대한 중요한 정보를 볼 수 있는 **Home** 창이 표시됩니다. 자세한 내용은 3-17 페이지의 Home 창(단일 모드 및 컨텍스트)를 참조하십시오. 다중 모드에서는 시스템에 **Home** 창이 없습니다.
Configuration	ASA를 구성합니다. 기능을 구성하려면 왼쪽 **Navigation** 창에서 해당 기능의 버튼을 클릭합니다.
Monitoring	ASA를 모니터링합니다. 기능을 구성하려면 왼쪽 **Navigation** 창에서 해당 기능의 버튼을 클릭합니다.
Back	마지막으로 방문한 ASDM의 창으로 돌아갑니다.
Forward	마지막으로 방문한 ASDM의 창 앞으로 이동합니다.
Search	ASDM에서 기능을 검색합니다. Search 기능에서는 각 창의 제목을 살펴보고 일치하는 목록을 제시하며, 해당 창에 직접 연결되는 하이퍼링크를 제공합니다. **Back** 또는 **Forward**를 클릭하여 검색된 두 개의 다른 창 사이를 신속하게 전환할 수 있습니다. 자세한 내용은 3-10 페이지의 ASDM Assistant를 참조하십시오.
Refresh	Monitoring 창의 그래프를 제외하고, 현재 실행 중인 컨피그레이션으로 ASDM을 새로 고칩니다.
Save	쓰기 액세스가 가능한 컨텍스트에 대해서만 실행 중인 컨피그레이션을 시작 컨피그레이션에 저장합니다.
Help	현재 열려 있는 화면에 대한 상황별 도움말이 표시됩니다.

ASDM Assistant

ASDM Assistant를 사용하면 특정 작업에 유용한 ASDM 절차가 포함된 도움말을 검색하고 볼 수 있습니다. 이 기능은 라우팅 및 투명 모드, 단일 및 시스템 컨텍스트에서 사용할 수 있습니다.

정보에 액세스하려면 **View > ASDM Assistant > How Do I?** 를 선택하거나메뉴 모음의 **Look For** 필드에 검색 요청을 입력합니다. 검색을 시작하려면 **Find** 드롭다운 목록에서 **How Do I?** 를 선택합니다.

ASDM Assistant를 사용하려면 다음 단계를 수행합니다.

1단계 **View > ASDM Assistant**를 선택합니다.

ASDM Assistant 창이 표시됩니다.

2단계 **Search** 필드에 검색하려는 정보를 입력한 다음 **Go**를 클릭합니다.

요청한 정보가 **Search Results** 창에 표시됩니다.

3단계 자세한 내용을 보려면 **Search Results and Features** 영역에 표시되는 링크를 클릭합니다.

상태 표시줄

Status Bar는 ASDM 창의 하단에 표시됩니다. 다음 표에는 왼쪽에서 오른쪽으로 표시되는 영역이 나와 있습니다.

영역	설명
Status	컨피그레이션의 상태(예: "Device configuration loaded successfully")입니다.
Failover	장애 조치 유닛의 상태(액티브 또는 스탠바이)입니다.
User Name	ASDM 사용자의 사용자 이름입니다. 사용자 이름 없이 로그인한 경우 사용자 이름은 "admin"입니다.
User Privilege	ASDM 사용자의 권한입니다.
Commands Ignored by ASDM	이 아이콘을 클릭하면 ASDM에서 처리하지 않은 컨피그레이션의 명령 목록이 표시됩니다. 이러한 명령은 컨피그레이션에서 제거되지 않습니다.
Connection to Device	ASA에 대한 ASDM 연결 상태입니다. 자세한 내용은 3-11 페이지의 Connection to Device를 참조하십시오.
Syslog Connection	syslog 연결이 가동 중이며 ASA가 모니터링됩니다.
SSL Secure	SSL을 사용하므로 ASDM에 대한 연결이 안전합니다.
Time	ASA에서 설정된 시간입니다.

Connection to Device

ASDM에서는 ASA에 대한 상시 연결을 유지하여 **Monitoring** 및 **Home** 창 데이터를 최신으로 유지합니다. 이 대화 상자에는 연결의 상태가 표시됩니다. 컨피그레이션을 변경할 경우 ASDM에서는 컨피그레이션이 진행되는 동안 두 번째 연결을 연 다음 나중에 이 연결을 닫지만, 이 대화 상자에서는 두 번째 연결을 제공하지 않습니다.

Device List

Device List는 고정 가능한 창입니다. 헤더의 세 가지 버튼 중 하나를 클릭하여 이 창을 최대화하거나 복원할 수 있으며, 움직이는 창으로 만들어 이를 이동하고 숨기거나 닫을 수 있습니다. 이 창은 Home, Configuration, Monitoring, System 뷰에서 사용할 수 있습니다. 이 창을 사용하여 다른 디바이스로 전환할 수 있습니다. 그러나 해당 디바이스는 현재 실행 중인 ASDM과 같은 버전을 실행 중이어야 합니다. 창을 완전히 표시하려면 최소 두 개 이상의 디바이스가 목록에 있어야 합니다. 이 기능은 라우팅 및 투명 모드, 그리고 단일, 다중 및 시스템 컨텍스트에서 사용할 수 있습니다.

이 창을 사용하여 다른 디바이스에 연결하려면 다음 단계를 수행합니다.

1단계 **Add**를 클릭하여 목록에 다른 디바이스를 추가합니다.

Add Device 대화 상자가 나타납니다.

2단계 디바이스의 디바이스 이름 또는 IP 주소를 입력한 다음 **OK**를 클릭합니다.

3단계 목록에서 선택한 디바이스를 제거하려면 **Delete**를 클릭합니다.

4단계 다른 디바이스에 연결하려면 **Connect**를 클릭합니다.

Enter Network Password 대화 상자가 나타납니다.

5단계 해당 필드에 사용자 이름 및 비밀번호를 입력한 다음 **Login**을 클릭합니다.

일반 버튼

많은 ASDM 창에는 다음 표에 나열된 버튼이 포함되어 있습니다. 원하는 작업을 완료하려면 해당 버튼을 클릭합니다.

버튼	설명
Apply	ASDM의 변경 사항을 ASA로 보내고 이를 실행 중인 컨피그레이션에 적용합니다.
Save	실행 중인 컨피그레이션의 복사본을 플래시 메모리에 씁니다.
Reset	변경 사항이 취소되며, 변경 사항을 적용하기 전에 또는 Refresh나 Apply를 마지막으로 클릭했을 때 표시되는 정보로 되돌아갑니다. **Reset**을 클릭한 후에는 **Refresh**를 클릭하여 현재 실행 중인 컨피그레이션에 해당 정보가 표시되는지 확인합니다.
Restore Default	선택한 설정을 지우고 기본 설정으로 돌아갑니다.
Cancel	변경 사항을 취소하고 이전 창으로 돌아갑니다.
Enable	기능에 대한 읽기 전용 통계가 표시됩니다.
Close	열려 있는 대화 상자를 닫습니다.
Clear	필드에서 정보를 제거하거나 확인란의 선택을 제거합니다.
Back	이전 창으로 돌아갑니다.
Forward	다음 창으로 이동합니다.
Help	선택한 창 또는 대화 상자에 대한 도움말을 표시합니다.

키보드 바로 가기

키보드를 사용하여 ASDM 사용자 인터페이스를 탐색할 수 있습니다.

표 3-1에는 ASDM 사용자 인터페이스의 세 가지 주요 영역을 이동하는 데 사용할 수 있는 키보드 바로 가기 목록이 나와 있습니다.

표 3-1 기본 창의 키보드 바로 가기

표시할 메뉴	Windows/Linux	MacOS
Home 창	Ctrl+H	Shift+Command+H
Configuration 창	Ctrl+G	Shift+Command+G
Monitoring 창	Ctrl+M	Shift+Command+M
Help	F1	Command+?
Back	Alt+Left Arrow	Command+[
Forward	Alt+Rightarrow	Command+]
화면 표시 새로 고침	F5	Command+R
자르기	Ctrl+X	Command+X
복사	Ctrl+C	Command+C
붙여넣기	Ctrl+V	Command+V
컨피그레이션 저장	Ctrl+S	Command+S
팝업 메뉴	Shift+F10	—
보조 창 닫기	Alt+F4	Command+W
찾기	Ctrl+F	Command+F
끝내기	Alt+F4	Command+Q
테이블 또는 텍스트 영역 끝내기	Ctrl_Shift 또는 Ctrl+Shift+Tab	Ctril+Shift 또는 Ctrl+Shift+Tab

표 3-2에는 창을 탐색하는 데 사용할 수 있는 키보드 바로 가기 목록이 나와 있습니다.

표 3-2 창의 키보드 바로 가기

포커스를 이동할 대상	누르기
다음 필드	Tab
이전 필드	Shift+Tab
포커스가 테이블에 있을 때 다음 필드	Ctrl+Tab
포커스가 테이블에 있을 때 이전 필드	Shift+Ctrl+Tab
Next 탭(탭에 포커스가 있을 경우)	오른쪽 화살표
Previous 탭(탭에 포커스가 있을 경우)	왼쪽 화살표
테이블의 다음 셀	Tab
테이블의 이전 셀	Shift+Tab
다음 창(여러 창이 표시될 경우)	F6
이전 창(여러 창이 표시될 경우)	Shift+F6

표 3-3에는 Log Viewer와 함께 사용할 수 있는 키보드 바로 가기 목록이 나와 있습니다.

표 3-3 Log Viewer용 키보드 바로 가기

실행할 작업	Windows/Linux	MacOS
실시간 Log Viewer 일시 중지 및 다시 시작	Ctrl+U	Command+
Log Buffer 창 새로 고침	F5	Command+R
Clear Internal Log Buffer	Ctrl+Delete	Command+Delete
선택한 로그 항목 복사	Ctrl+C	Command+C
로그 저장	Ctrl+S	Command+S
Print	Ctrl+P	Command+P
보조 창 닫기	Alt+F4	Command+W

표 3-4에는 메뉴 항목에 액세스하는 데 사용할 수 있는 키보드 바로 가기 목록이 나와 있습니다.

표 3-4 메뉴 항목 액세스를 위한 키보드 바로 가기

액세스할 항목	Windows/Linux
메뉴 모음	Alt
다음 메뉴	오른쪽 화살표
이전 메뉴	왼쪽 화살표
다음 메뉴 옵션	아래쪽 화살표
이전 메뉴 옵션	위쪽 화살표
선택한 메뉴 옵션	Enter

대부분의 ASDM 창에서 기능 찾기

일부 ASDM 창에는 여러 가지 요소가 있는 테이블이 포함되어 있습니다. 특정 항목을 쉽게 검색, 강조 표시하고 편집할 수 있도록 하기 위해 몇몇 ASDM 창에는 해당 창에서 객체를 검색할 수 있는 찾기 기능이 있습니다.

검색을 수행하려면 Find 필드에 구를 입력하여 제공된 창 내에서 모든 열을 검색할 수 있습니다. 구에는 와일드카드 문자 "*" 및 "?"를 포함할 수 있습니다. *는 하나 이상의 문자와 일치하며 ?는 하나의 문자와 일치합니다. **Find** 필드의 오른쪽에 있는 위쪽 및 아래쪽 화살표를 사용하면 다음(위로) 또는 이전(아래로)에 발생한 구를 찾을 수 있습니다. 입력한 대문자 및 소문자와 정확히 일치하는 항목을 찾으려면 **Match Case** 확인란을 선택합니다.

예를 들어, B*ton-L*을 입력하면 다음과 같은 일치 결과가 반환됩니다.

```
Boston-LA, Boston-Lisbon, Boston-London
```

Bo?ton을 입력하면 다음과 같은 일치 결과가 반환됩니다.

```
Boston, Bolton
```

다음 목록에는 찾기 기능을 사용할 수 있는 ASDM 창이 나와 있습니다.

- **AAA Server Groups** 창
- **ACL Manager** 창 — ACL Manager 창의 찾기 기능은 다른 창의 찾기 기능과 다릅니다. 자세한 내용은 3-15 페이지의 ACL Manager 창의 찾기 기능를 참조하십시오.
- **Certificate-to-Conn Profile Maps-Rules** 창
- **DAP** 창
- **Identity Certificates** 창
- **IKE Policies** 창
- **IPSec Proposals (Transform Sets)** 창
- **Local User** 창
- **Portal-Bookmark** 창
- **Portal-Customization** 창
- **Portal-Port Forwarding** 창
- **CA Certificates** 창
- **Portal-Smart Tunnels** 창
- **Portal-Web Contents** 창
- **VPN Connection Profiles** 창
- **VPN Group Policies** 창

ACL Manager 창의 찾기 기능

ACL 및 ACE에는 다른 유형의 요소가 많이 포함되어 있으므로, **ACL Manager** 창의 찾기 기능을 사용하면 다른 창의 찾기 기능보다 더욱 표적화된 검색이 가능합니다.

ACL Manager 창에서 요소를 찾으려면 다음 단계를 수행합니다.

1단계 **ACL Manager** 창에서 **Find**를 클릭합니다.

2단계 **Filter** 필드의 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- **Source** — 검색 시 네트워크 객체 그룹, 인터페이스 IP 또는 트래픽이 허용되거나 거부된 모든 주소의 소스 IP 주소가 포함됩니다. 이 주소를 4단계에서 지정합니다.
- **Destination** — 검색 시 **Source** 섹션에 나열된 IP 주소로 트래픽을 보낼 수 있도록 허용되거나 거부된 목적지 IP 주소(호스트 또는 네트워크)가 포함됩니다. 이 주소를 4단계에서 지정합니다.
- **Source or Destination** — 검색 시 4단계에서 지정한 소스 또는 목적지 주소가 포함됩니다.
- **Service** — 검색 시 4단계에서 지정한 서비스 그룹 또는 사전 정의된 서비스 정책이 포함됩니다.
- **Query** — 드롭다운 목록에서 **Query**를 선택할 경우 **Query**를 클릭하여 앞서 언급한 네 가지 모든 옵션(**Source**, **Destination**, **Source or Destination**, **Service**)별로 세부 검색을 지정합니다.

3단계 두 번째 필드에서는 드롭다운 목록의 다음 옵션 중 하나를 선택합니다.

- **is** — 4단계에 입력한 세부 정보와 정확히 일치하는 결과를 지정합니다.
- **contains** — 4단계에 입력한 세부 정보가 포함되나 이에 국한되지는 않는 ACL 또는 ACE를 검색하도록 지정합니다.

4단계 세 번째 필드에는 검색하려는 ACL 또는 ACE에 대한 특정 기준을 입력하거나, **Browse**를 클릭하여 ACL/ACE 컨피그레이션의 핵심 요소를 검색합니다.

5단계 **Filter**를 클릭하여 검색을 수행합니다.

ASDM 찾기 기능에서는 지정된 기준이 포함된 ACL 및 ACE 목록을 반환합니다.

6단계 검색된 ACL 및 ACE 목록을 지우려면 **Clear**를 클릭합니다.

7단계 찾기 기능 대화 상자를 닫으려면 빨간색 **x**를 클릭합니다.

확장된 화면 판독기 지원 사용

Tab 키를 눌러 창을 탐색할 경우 기본적으로 라벨 및 설명이 탭 순서에 포함되어 있지 않습니다. JAWS 같은 일부 화면 판독기에서만 포커스가 있는 화면 객체를 읽을 수 있습니다. 확장된 화면 판독기 지원을 사용하면 탭 순서에 라벨 및 설명을 포함할 수 있습니다.

확장된 화면 판독기 지원을 사용하려면 다음 단계를 수행합니다.

1단계 **Tools > Preferences**를 선택합니다.

Preferences 대화 상자가 나타납니다.

2단계 **General** 탭에서 **Enable screen reader support** 확인란을 선택합니다.

3단계 **OK**를 클릭합니다.

4단계 ASDM을 다시 시작하여 화면 판독기 지원을 활성화합니다.

체계적인 폴더

컨피그레이션 및 모니터링 뷰를 위한 탐색 창의 일부 폴더에는 연관된 컨피그레이션 또는 모니터링 창이 없습니다. 이러한 폴더는 관련 컨피그레이션 및 모니터링 작업을 컨피그레이션하는 데 사용됩니다. 이러한 폴더를 클릭하면 오른쪽 **Navigation** 창에 하위 항목 목록이 표시됩니다. 하위 항목의 이름을 클릭하면 해당 항목으로 이동할 수 있습니다.

Help 창 정보

필요한 정보를 얻으려면 다음 테이블에 나와 있는 해당 버튼을 클릭합니다.

버튼	설명
About ASDM	호스트 이름, 버전 번호, 디바이스 유형, ASDM 소프트웨어 버전 번호, 권한 수준, 사용자 이름, 사용 중인 운영 체제를 비롯하여 ASA에 대한 정보가 표시됩니다.
Search	온라인 도움말 항목에서 정보를 검색합니다.
Using Help	온라인 도움말을 가장 효율적으로 사용하기 위한 방법을 설명합니다.
Glossary	ASDM 및 ASA에 있는 용어 목록이 나열됩니다.

버튼	설명
목차	목차를 표시합니다.
Screens	화면 이름을 기준으로 도움말 파일이 나열됩니다.
Index	ASDM 온라인 도움말에 있는 도움말 주제의 색인이 표시됩니다.

Home 창(단일 모드 및 컨텍스트)

ASDM **Home** 창을 사용하면 ASA에 대한 중요한 정보를 볼 수 있습니다. **Home** 창의 상태 정보는 10초마다 업데이트됩니다. 이 창에는 일반적으로 **Device Dashboard** 및 **Firewall Dashboard**라는 두 개의 탭이 있습니다.

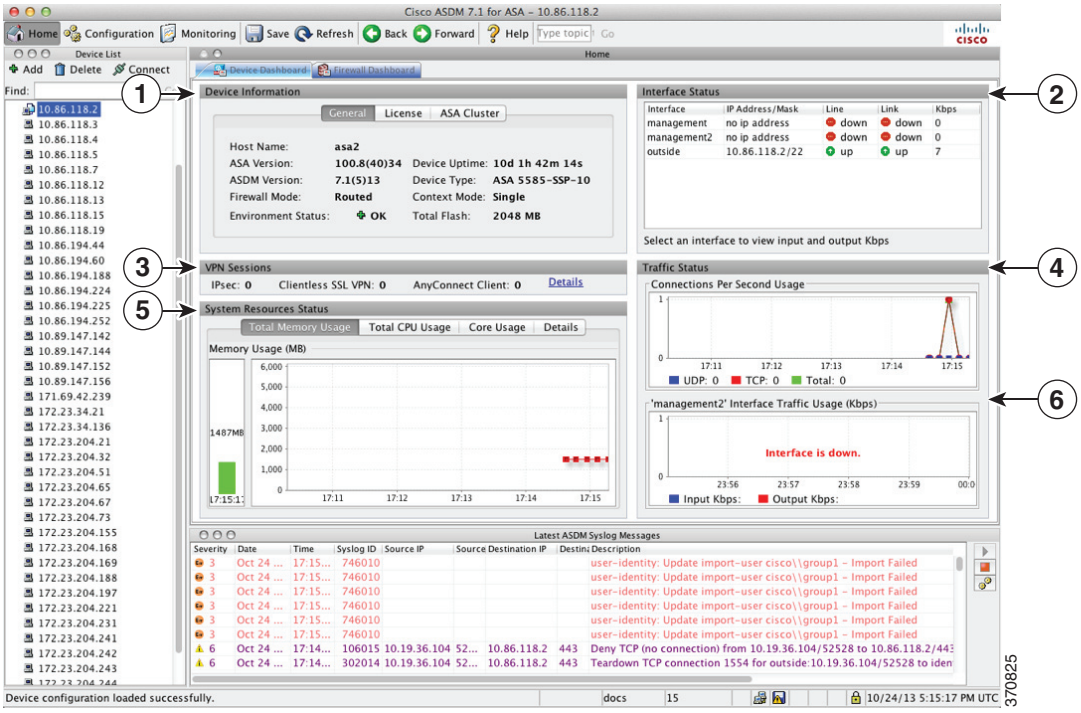
디바이스에 IPS나 CX 같은 하드웨어 또는 소프트웨어 모듈이 설치된 경우, 이러한 모듈을 위한 별도의 탭이 있습니다.

Device Dashboard 탭

Device Dashboard 탭을 사용하면 인터페이스의 상태, 실행 중인 버전, 라이센스 정보, 성능 등 ASA에 대한 중요한 정보를 한눈에 볼 수 있습니다.

그림 3-2에는 **Device Dashboard** 탭의 요소가 나와 있습니다.

그림 3-2 Device Dashboard 탭



범례

GUI 요소	설명
1	3-18 페이지의 Device Information 창
2	3-19 페이지의 Interface Status 창
3	3-19 페이지의 VPN Sessions 창
4	3-20 페이지의 Traffic Status 창
5	3-20 페이지의 System Resources Status 창
6	3-20 페이지의 Traffic Status 창
—	3-12 페이지의 Device List
—	3-20 페이지의 Latest ASDM Syslog Messages 창

Device Information 창

Device Information 창에는 디바이스 정보를 표시하는 두 개의 탭(**General** 탭 및 **License** 탭)이 포함됩니다. **General** 탭 아래에서는 시스템 상태를 한눈에 볼 수 있는 **Environment Status** 버튼에 액세스할 수 있습니다.

General 탭

이 탭에는 ASA에 대한 기본 정보가 표시됩니다.

- **Host name** — 디바이스의 호스트 이름이 표시됩니다.
- **ASA version** — 디바이스에서 실행 중인 ASA 소프트웨어의 버전이 나열됩니다.
- **ASDM version** — 디바이스에서 실행 중인 ASDM 소프트웨어의 버전이 나열됩니다.
- **Firewall mode** — 디바이스가 실행 중인 방화벽 모드가 표시됩니다.
- **Total flash** — 현재 사용 중인 총 RAM이 표시됩니다.
- **ASA Cluster Role** — 클러스터링을 활성화할 경우, 이 유닛의 역할이 마스터인지 슬레이브인지 표시됩니다.
- **Device uptime** — 최신 소프트웨어 업로드 이후로 디바이스가 가동되고 있는 시간이 표시됩니다.
- **Context mode** — 디바이스가 실행 중인 컨텍스트 모드가 표시됩니다.
- **Total Memory** — ASA에 설치된 DRAM이 표시됩니다.
- **Environment status** — 시스템 상태가 표시됩니다. ASA 5585-X에서는 하드웨어 통계를 제공하며 이는 **General** 탭의 **Environment Status** 라벨 오른쪽에 있는 더하기 기호(+)를 클릭하여 사용할 수 있습니다. 전원 공급 장치가 몇 개 설치되었는지 확인하고, 팬 및 전원 공급 모듈의 작동 상태를 추적하며, CPU의 온도와 시스템의 주변 온도를 추적할 수 있습니다.

  일반적으로 **Environment Status** 버튼을 선택하면 시스템 상태를 한눈에 볼 수 있습니다. 시스템서 모니터링되는 모든 하드웨어 구성 요소가 정상 범위 내에서 작동 중인 경우 더하기 기호(+) 버튼이 초록색 상태의 OK로 표시됩니다. 이와 반대로 하드웨어 시스템의 구성 요소가 정상 범위를 벗어나 작동 중일 경우, 더하기 기호(+)가 빨간색 원으로 바뀌어 Critical 상태로 표시되며 하드웨어 구성 요소에 즉각적인 조치가 필요함을 나타냅니다.

  특정 디바이스의 특정 하드웨어 통계에 대한 자세한 내용은 하드웨어 가이드를 참조하십시오.

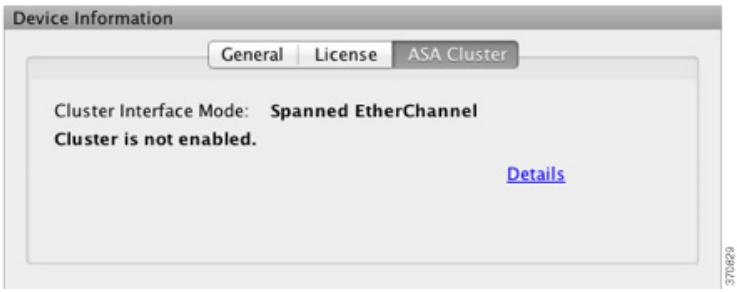
참고 ASA의 최신 릴리스로 업그레이드하기에 충분한 메모리가 없는 경우, **Memory Insufficient Warning** 대화 상자가 표시됩니다. 지원되는 방식으로 ASA 및 ASDM을 계속 사용하려면 이 대화 상자에 표시되는 지침을 따릅니다. **OK**를 클릭하여 이 대화 상자를 닫습니다.

Licenses 탭

이 탭에는 라이센스 기능의 하위 집합이 표시됩니다. 자세한 라이센스 정보를 보려면 **More Licenses**를 클릭하거나 새 활성화 키를 입력합니다. **Configuration > Device Management > Licensing > Activation Key 창**이 표시됩니다.

Cluster 탭

이 탭에는 클러스터 인터페이스 모드와 함께 클러스터 상태가 표시됩니다.



Virtual Resources 탭(ASAv)

이 탭에는 ASAv에서 사용되는 가상 리소스가 표시되며 여기에는 vCPU의 수, RAM 및 ASAv가 초과 또는 미달한 채로 프로비저닝되었는지 여부가 포함됩니다.

Interface Status 창

이 창에는 각 인터페이스의 상태가 표시됩니다. 인터페이스 행을 선택하면 입력 및 출력 처리량이 Kbps 단위로 테이블 아래에 표시됩니다.

VPN Sessions 창

이 창에는 VPN 터널 상태가 표시됩니다. **Details**를 클릭하여 **Monitoring > VPN > VPN Statistics > Sessions** 창으로 이동합니다.

Failover Status 창

이 창에는 장애 조치 상태가 표시됩니다.

Configure를 클릭하여 High Availability and Scalability Wizard를 시작합니다. 마법사를 완료하면 장애 조치 컨피그레이션 상태(액티브/액티브 또는 액티브/스탠바이)가 표시됩니다.

장애 조치가 구성되면 **Details**를 클릭하여 **Monitoring > Properties > Failover > Status** 창을 엽니다.

System Resources Status 창

이 창에는 CPU 및 메모리 사용량 통계가 표시됩니다.

Traffic Status 창

이 창에는 모든 인터페이스의 초당 연결 및 최저 보안 인터페이스의 트래픽 처리량이 그래프로 표시됩니다.

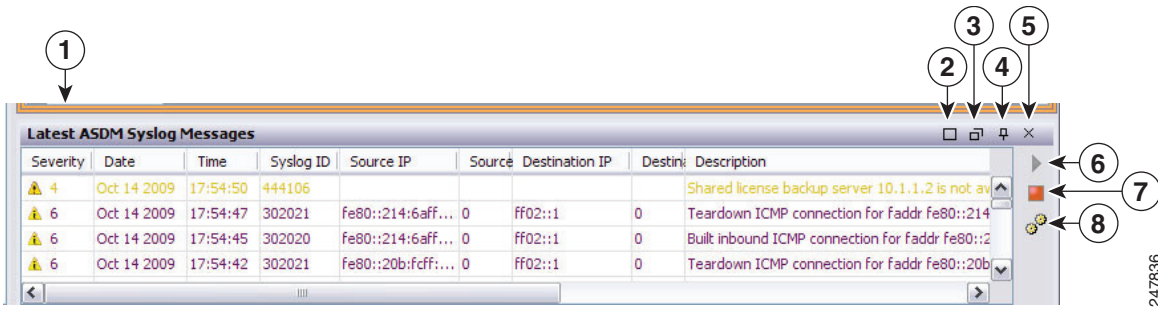
컨피그레이션에 최저 보안 수준 인터페이스가 여러 개 포함되어 있고 이 중 하나의 이름이 "outside"로 지정된 경우, 해당 인터페이스는 트래픽 처리량 그래프에 사용됩니다. 그렇지 않을 경우 ASDM에서는 알파벳 순서로 나열된 최저 보안 수준 인터페이스에서 첫 번째 인터페이스를 선택합니다.

Latest ASDM Syslog Messages 창

이 창에는 ASA에서 생성된 최신 시스템 메시지가 최대 100개까지 표시됩니다. 이 창이 비활성화된 경우 **Enable Logging**을 클릭하여 로깅을 활성화합니다.

그림 3-3에는 **Latest ASDM Syslog Messages** 창의 요소가 나와 있습니다.

그림 3-3 Latest ASDM Syslog Messages 창



범례

GUI 요소	설명
1	**구분선**을 위로 또는 아래로 끌어 창의 크기를 조정합니다.
2	창을 확대합니다. **이중 사각형** 아이콘을 클릭하면 창이 원래 크기로 돌아갑니다.
3	움직이는 창을 만듭니다. **고정된 창** 아이콘을 클릭하면 창이 고정됩니다.
4	Auto-hide를 활성화 또는 비활성화합니다. Auto-hide가 활성화되고 마우스 커서를 왼쪽 아래 모서리의 **Latest ASDM Syslog Messages** 버튼 위로 이동하면 창이 나타납니다. 커서를 창 밖으로 이동하면 창이 사라집니다.
5	창을 닫습니다. 창을 표시하려면 **View Latest ASDM Syslog Messages**를 선택합니다.
6	syslog 메시지 표시를 계속 업데이트하려면 오른쪽의 **초록색** 아이콘을 클릭합니다.
7	syslog 메시지 표시 업데이트를 중지하려면 오른쪽의 **빨간색** 아이콘을 클릭합니다.
8	**Logging Filters** 창을 열려면 오른쪽의 **필터** 아이콘을 클릭합니다.

- 현재 메시지를 지우려면 마우스 오른쪽 버튼으로 이벤트를 클릭하고 **Clear Content**를 선택합니다.
- 현재 메시지를 PC에 파일로 저장하려면 마우스 오른쪽 버튼으로 이벤트를 클릭하고 **Save Content**를 클릭합니다.
- 현재 내용을 복사하려면 마우스 오른쪽 버튼으로 이벤트를 클릭하고 **Copy**를 선택합니다.
- 심각도에 따라 syslog 메시지의 배경색 및 전경색을 변경하려면 마우스 오른쪽 버튼으로 이벤트를 클릭하고 **Color Settings**를 선택합니다.

Firewall Dashboard 탭

Firewall Dashboard 탭을 사용하면 ASA를 통해 전달되는 트래픽에 대한 중요한 정보를 볼 수 있습니다. 이 대시보드는 단일 컨텍스트 모드에 있는지 또는 다중 컨텍스트 모드에 있는지에 따라 달라집니다. 다중 컨텍스트 모드의 경우 **Firewall Dashboard**를 각 컨텍스트에서 볼 수 있습니다.

그림 3-4에는 **Firewall Dashboard** 탭의 일부 요소가 나와 있습니다.

그림 3-4 Firewall Dashboard 탭

범례

GUI 요소	설명
1	3-22 페이지의 Traffic Overview 창
2	3-22 페이지의 Top 10 Access Rules 창
3	3-22 페이지의 Top Usage Status 창

GUI 요소	설명
(표시 안 됨)	3-23 페이지의 Top Ten Protected Servers Under SYN Attack 창
(표시 안 됨)	3-23 페이지의 Top 200 Hosts 창
(표시 안 됨)	3-23 페이지의 Top Botnet Traffic Filter Hits 창

Traffic Overview 창

기본적으로 활성화되어 있습니다. 기본 위협 감지를 비활성화할 경우(방화벽 컨피그레이션 가이드 참조), 이 영역에는 기본 위협 감지를 활성화할 수 있는 **Enable** 버튼이 포함됩니다. 런타임 통계에는 다음과 같은 *표시 전용* 정보가 포함됩니다.

- 연결 및 NAT 변환 수.
- 액세스 목록 거부 및 애플리케이션 감시로 인해 초당 손실된 패킷 속도.
- 공격 검사 과정에서 확인된 초당 손실된 패킷 속도 또는 감지된 불완전한 세션(TCP SYN 공격 감지 또는 데이터 없는 UDP 세션 공격 감지).

Top 10 Access Rules 창

기본적으로 활성화되어 있습니다. 액세스 규칙에 대한 위협 감지 통계를 비활성화할 경우(방화벽 컨피그레이션 가이드 참조), 이 영역에는 액세스 규칙에 대한 통계를 활성화할 수 있는 **Enable** 버튼이 포함됩니다.

Table 뷰의 목록에서 규칙을 선택하고 마우스 오른쪽 버튼으로 규칙을 클릭하여 팝업 메뉴 항목 **Show Rule**을 표시할 수 있습니다. 이 항목을 선택하여 Access Rules 테이블로 이동하고 이 테이블에서 해당 규칙을 선택합니다.

Top Usage Status 창

기본적으로 비활성화되어 있습니다. 이 창에는 다음과 같은 4개의 탭이 포함되어 있습니다.

- **Top 10 Services** — 위협 감지 서비스
- **Top 10 Sources** — 위협 감지 서비스
- **Top 10 Destinations** — 위협 감지 서비스
- **Top 10 Users** — ID 방화벽 서비스

처음 3개 탭(**Top 10 Services**, **Top 10 Sources**, **Top 10 Destinations**)에서는 위협 감지 서비스에 대한 통계를 제공합니다. 각 탭에는 각각의 위협 감지 서비스를 활성화할 수 있는 **Enable** 버튼이 포함됩니다. 방화벽 컨피그레이션 가이드에 따라 이를 활성화할 수 있습니다.

Top 10 Services Enable 버튼을 사용하면 포트 및 프로토콜에 대한 통계가 모두 활성화됩니다(표시하려면 두 개를 모두 활성화해야 함). **Top 10 Sources** 및 **Top 10 Destinations Enable** 버튼을 사용하면 호스트에 대한 통계가 활성화됩니다. 호스트(소스 및 목적지), 포트 및 프로토콜의 상위 사용량 상태 통계가 표시됩니다.

Top 10 Users의 네 번째 탭에서는 Identity Firewall 서비스에 대한 통계를 제공합니다. Identity Firewall 서비스에서는 사용자의 ID를 기준으로 액세스 제어를 제공합니다. 소스 IP 주소를 통하는 방법 대신 사용자 이름과 사용자 그룹 이름을 기준으로 액세스 규칙 및 보안 정책을 구성할 수 있습니다. ASA에서는 IP 사용자 매핑 데이터베이스에 액세스하여 이러한 서비스를 제공합니다.

ASA에서 추가 구성 요소(Microsoft Active Directory 및 Cisco AD(Active Directory) Agent) 구성을 비롯하여 Identity Firewall 서비스를 구성한 경우에만 **Top 10 Users** 탭에 데이터가 표시됩니다.

선택하는 옵션에 따라 **Top 10 Users** 탭에는 수신된 EPS 패킷, 전송한 EPS 패킷, 상위 10명의 사용자에게 전송된 공격에 대한 통계가 표시됩니다. 이 탭에서는 (*domain\user_name*으로 표시되는) 각 사용자에 대해 평균 EPS 패킷, 현재 EPS 패킷, 트리거, 총 이벤트를 보여줍니다.

주의 통계를 활성화할 경우, 활성화한 통계 유형에 따라 ASA 성능에 영향을 미칠 수 있습니다. 호스트에 대한 통계를 활성화할 경우 성능에 중요한 영향을 미칠 수 있습니다. 트래픽 로드가 높을 경우 이러한 유형의 통계를 일시적으로 활성화하는 방법을 고려할 수 있습니다. 그러나 포트에 대한 통계를 활성화할 경우에는 큰 영향을 미치지 않습니다.

Top Ten Protected Servers Under SYN Attack 창

기본적으로 비활성화되어 있습니다. 이 영역에는 이 기능을 활성화할 수 있는 **Enable** 버튼이 포함되어 있으며, 방화벽 컨피그레이션 가이드에 따라 이 기능을 활성화할 수도 있습니다. 공격을 받는 상위 10개의 보호되는 서버에 대한 통계가 표시됩니다.

공격의 평균 속도를 파악하기 위해 ASA에서는 속도 간격(기본적으로 30분) 동안 30초마다 데이터를 샘플링합니다.

공격자가 하나 이상인 경우 마지막 공격자의 IP 주소 뒤에 “<various>”가 표시됩니다.

10개 서버가 아닌 모든 서버(최대 1000개)에 대한 통계를 보려면 **Detail**을 클릭합니다. 또한 기록 샘플링 데이터도 볼 수 있습니다. ASA에서는 속도 간격 동안 공격 횟수를 60번 샘플링하며, 기본 간격인 30분 동안 60초마다 통계가 수집됩니다.

Top 200 Hosts 창

기본적으로 비활성화되어 있습니다. ASA를 통해 연결된 상위 200개의 호스트가 표시됩니다. 호스트의 각 항목에는 호스트의 IP 주소 및 호스트에서 시작한 연결 수가 포함되며 이는 120초마다 업데이트됩니다. 이 표시를 활성화하려면 **hpm topnenable** 명령을 입력합니다.

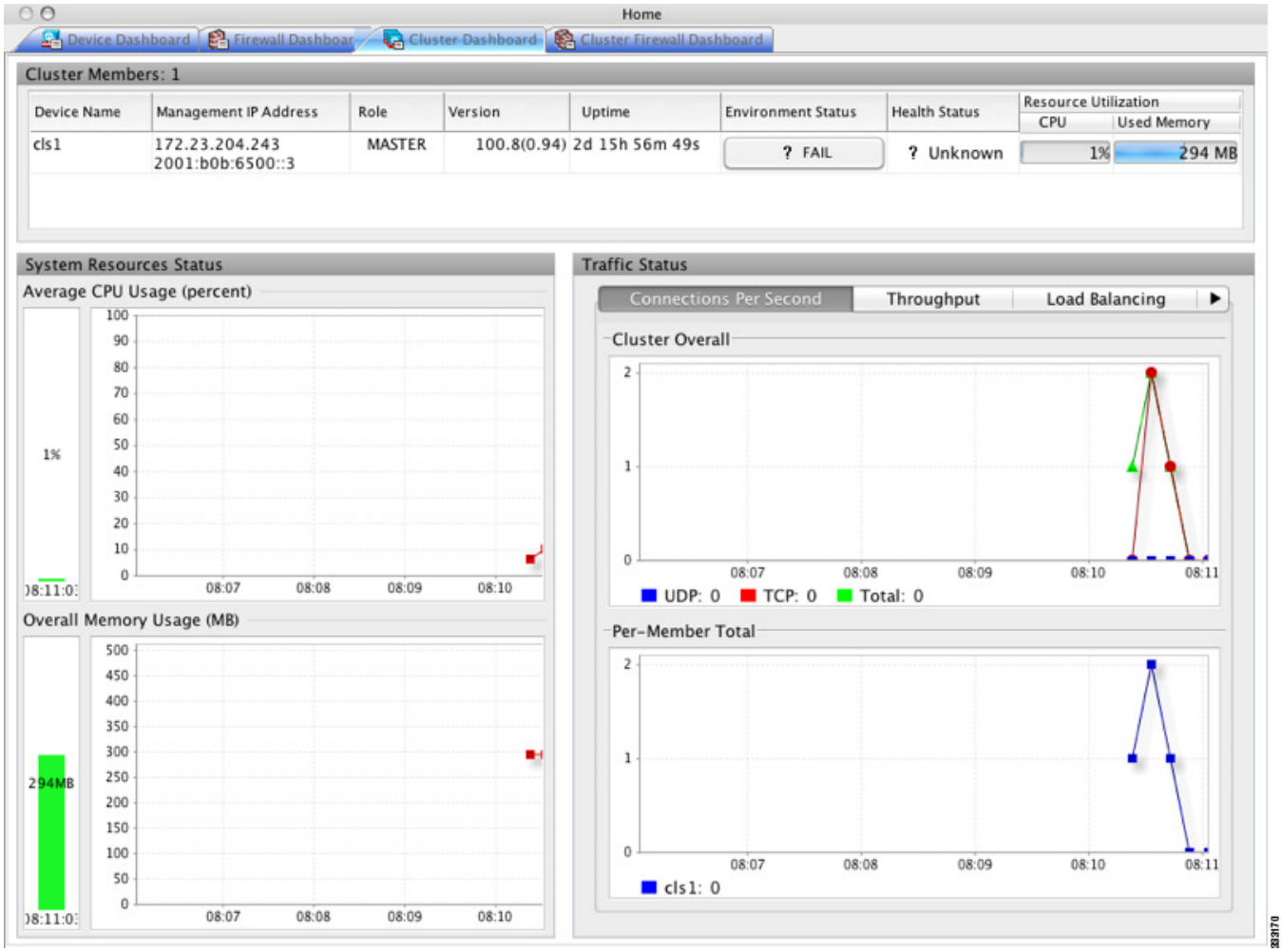
Top Botnet Traffic Filter Hits 창

기본적으로 비활성화되어 있습니다. 이 영역에는 Botnet Traffic Filter를 구성할 수 있는 링크가 포함됩니다. 상위 10개의 봇넷 사이트, 포트, 감염된 호스트에 대한 보고서에서는 데이터의 스냅샷을 제공하며, 수집을 위해 통계가 시작되므로 상위 10개 항목이 일치하지 않을 수 있습니다. 마우스 오른쪽 버튼으로 IP 주소를 클릭하면 봇넷 사이트에 대한 자세한 내용을 살펴볼 수 있는 whois 툴이 시작됩니다.

자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

Cluster Dashboard 탭

Cluster Dashboard 탭에는 클러스터 멤버 및 리소스 사용률의 요약이 표시됩니다.



- **Cluster Members** — 클러스터를 구성하는 멤버에 대한 이름과 기본 정보(관리 IP 주소, 버전, 클러스터 내 역할 등) 및 상태(환경 상태, 상태, 리소스 사용률)가 표시됩니다.

  참고 다중 컨텍스트 모드에서 ASDM을 관리자 컨텍스트에 연결한 후 다른 컨텍스트로 변경할 경우, 현재 컨텍스트 관리 IP 주소를 표시하도록 관리 IP 주소가 변경되지 않습니다. 현재 ASDM이 연결되어 있는 기본 클러스터 IP 주소를 비롯하여 관리자 컨텍스트 관리 IP 주소가 계속 표시됩니다.

- **System Resource Status** — 클러스터와 트래픽 그래프 전반에 걸쳐 클러스터 전체 및 디바이스당 리소스 사용률(CPU 및 메모리)이 모두 표시됩니다.
- **Traffic Status** — 각 탭에는 다음과 같은 그래프가 포함됩니다.
  - **Connections Per Second** 탭:

    Cluster Overall — 클러스터 전체의 초당 연결이 표시됩니다.

    Per-Member Total — 각 멤버의 초당 평균 연결이 표시됩니다.

- **Throughput** 탭:

  Cluster Overall — 클러스터 전체의 취합된 이그레스(egress) 처리량이 표시됩니다.

  Per-Member Throughput — 한 라인의 멤버 하나당 멤버 처리량이 표시됩니다.

- **Load Balancing** 탭:

  Per-Member Percentage of Total Traffic — 멤버에게 수신되는 클러스터 트래픽의 총 백분율이 각 멤버에 대해 표시됩니다.

  Per-Member Locally Processed Traffic — 로컬로 처리되는 트래픽의 백분율이 각 멤버에 대해 표시됩니다.

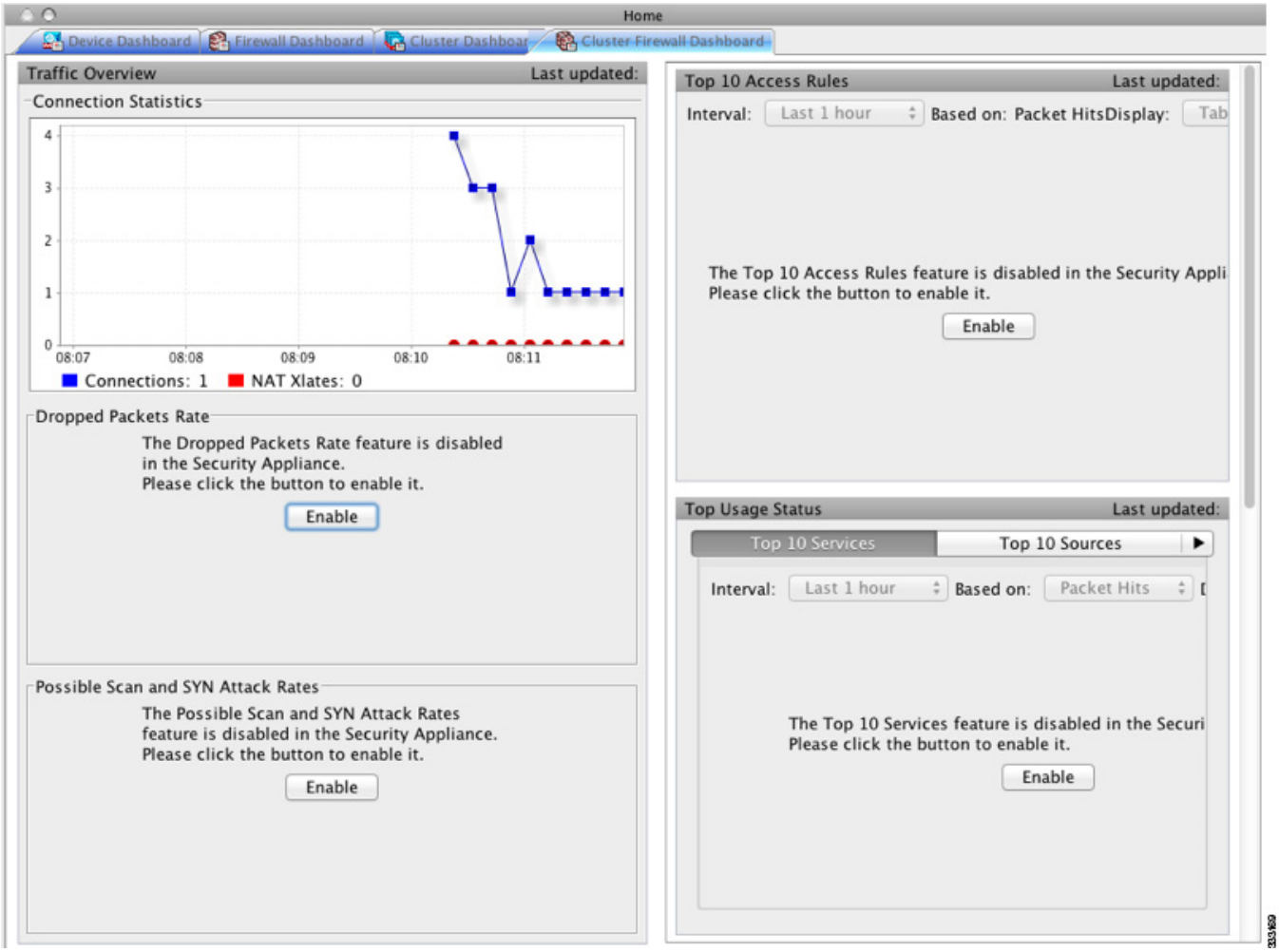
- **Control Link Usage** 탭:

  Per-Member Receival Capacity Utilization — 전송 용량의 사용량이 각 멤버에 대해 표시됩니다.

  Per-Member Transmittal Capacity Utilization — 수신 용량의 사용량이 각 멤버에 대해 표시됩니다.

Cluster Firewall Dashboard 탭

Cluster Firewall Dashboard 탭에는 트래픽 개요 및 **Firewall Dashboard**에 표시되는 것과 유사한 "top N" 통계가 표시되지만, 이 항목은 전체 클러스터에 걸쳐 취합됩니다.



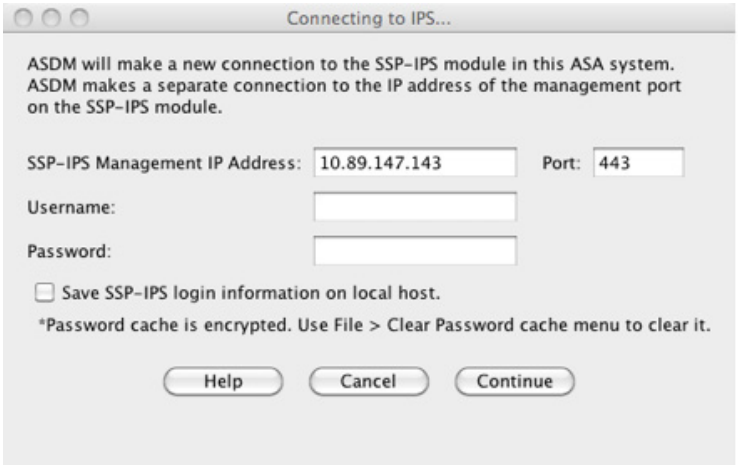
Intrusion Prevention 탭

Intrusion Prevention 탭을 사용하면 IPS에 대한 중요한 정보를 볼 수 있습니다. 이 탭은 ASA에 IPS 모듈이 설치된 경우에만 표시됩니다.

IPS 모듈에 연결하려면 다음 단계를 수행합니다.

1단계 **Intrusion Prevention** 탭을 클릭합니다.

Connecting to IPS 대화 상자가 나타납니다.



2단계 IP 주소, 포트, 사용자 이름 및 비밀번호를 입력합니다. 기본 IP 주소 및 포트는 192.168.1.2:443입니다. 기본 사용자 이름 및 비밀번호는 **cisco** 및 **cisco**입니다.

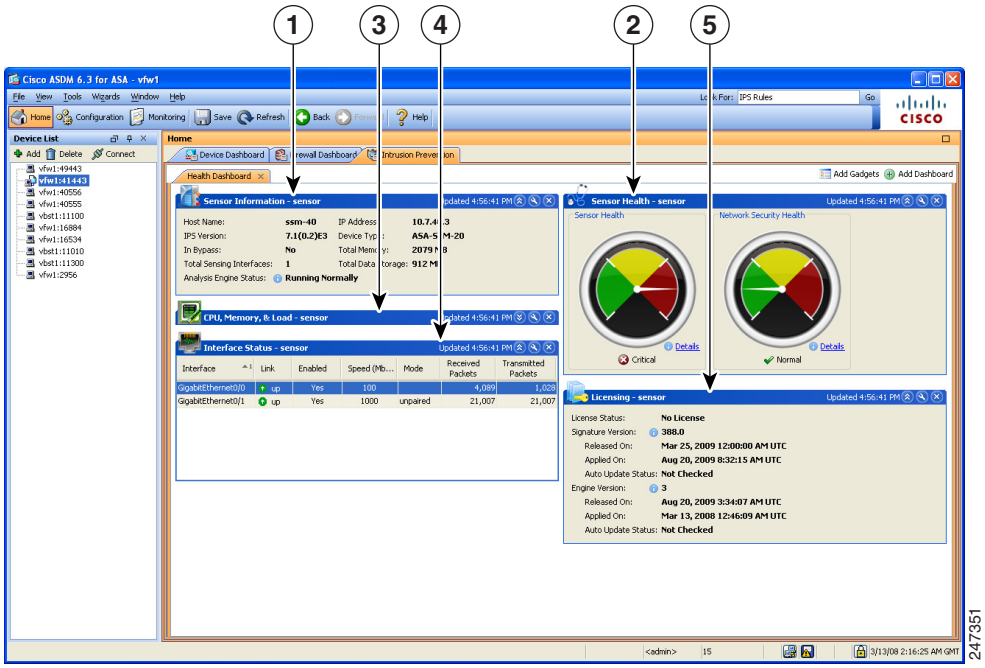
3단계 로컬 PC에 로그인 정보를 저장하려면 **Save IPS login** information on local host 확인란을 선택합니다.

4단계 **Continue**를 클릭합니다.

침입 방지에 대한 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

그림 3-5에는 **Intrusion Prevention** 탭에 있는 **Health Dashboard** 탭의 요소가 나와 있습니다.

그림 3-5 Intrusion Prevention 탭(Health Dashboard)

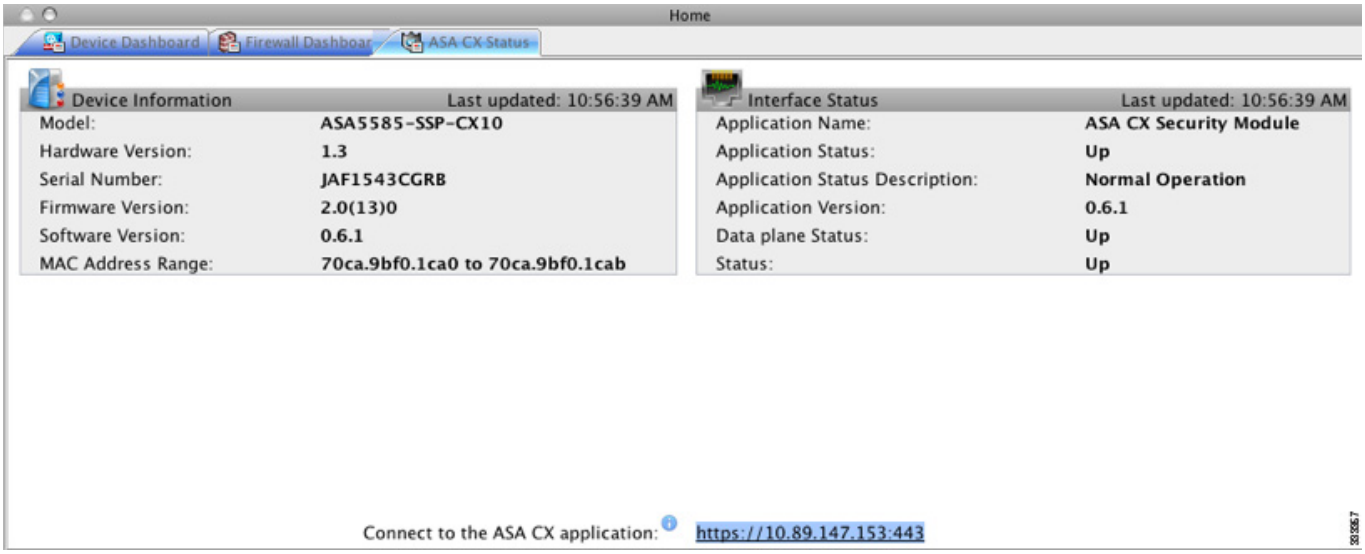


범례

GUI 요소	설명
1	**Sensor Information** 창
2	**Sensor Health** 창
3	**CPU**, **Memory**, **Load** 창
4	**Interface Status** 창
5	**Licensing** 창

ASA CX Status 탭

ASA CX Status 탭을 사용하면 ASA CX 모듈에 대한 중요한 정보를 볼 수 있습니다. 이 탭은 ASA에 ASA CX 모듈이 설치된 경우에만 표시됩니다.



ASA FirePOWER Status 탭

ASA FirePOWER Status 탭을 사용하면 모듈에 대한 중요한 정보를 볼 수 있습니다. 여기에는 모델, 일련 번호, 소프트웨어 버전, 모듈 상태(예: 애플리케이션 이름 및 상태, 데이터 플레인 상태, 전반적인 상태) 같은 모듈 정보가 포함됩니다. 모듈이 FireSIGHT Management Center에 등록된 경우, 링크를 클릭하여 애플리케이션을 열고 추가 분석 및 모듈 컨피그레이션을 수행할 수 있습니다.

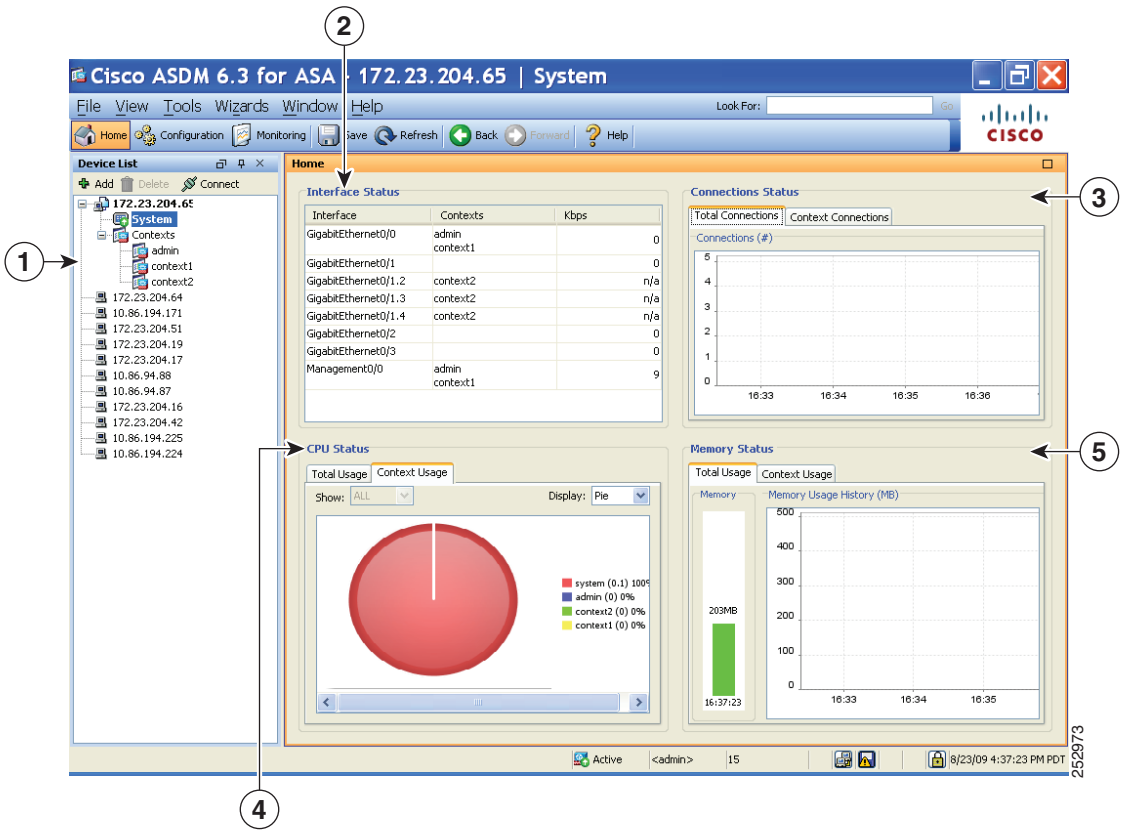
이 탭은 디바디스에 ASA FirePOWER 모듈이 설치된 경우에만 표시됩니다.

Home 창(System)

ASDM System **Home** 창을 사용하면 ASA에 대한 중요한 상태 정보를 볼 수 있습니다. ASDM System **Home** 창에서 제공되는 많은 세부 정보는 ASDM의 다른 곳에서도 제공되지만, 이 창에는 ASA가 어떻게 실행되고 있는지가 한눈에 표시됩니다. System **Home** 창의 상태 정보는 10초마다 업데이트됩니다.

3-29 페이지의 그림 3-6에는 System **Home** 창의 요소가 표시됩니다.

그림 3-6 System Home 창



범례

GUI 요소	설명
1	System 또는 Context를 선택합니다.
2	**Interface Status** 창 인터페이스를 통과하는 총 트래픽의 양을 보려는 인터페이스를 선택합니다.
3	**Connection Status** 창
4	**CPU Status** 창
5	**Memory Status** 창

ASDM 기본 설정 정의

이 기능을 사용하면 특정한 ASDM 설정의 동작을 정의할 수 있습니다.

ASDM의 다양한 설정을 변경하려면 다음 단계를 수행합니다.

1단계 **Tools > Preferences**를 선택합니다.

General, **Rules Table**, **Syslog**라는 3가지 탭이 포함된 **Preferences** 대화 상자가 표시됩니다.

2단계 설정을 정의하려면 이러한 탭 중 하나를 클릭합니다. **General** 탭에서는 일반적인 기본 설정을 지정합니다. **Rules Table** 탭에서는 Rules 테이블의 기본 설정을 지정합니다. **Syslog** 탭에서는 **Home** 창에 표시되는 syslog 메시지의 표시 여부를 지정하고, NetFlow 관련 syslog 메시지에 대한 경고 메시지 표시를 활성화합니다.

3단계 **General** 탭에서 다음을 지정합니다.

a. 시작 컨피그레이션과 실행 중인 컨피그레이션이 서로 더 이상 동기화되지 않을 경우 알림을 받으려면 **Warn that configuration in ASDM is out of sync with the configuration in ASA** 확인란을 선택합니다.

b. 시작 시 다음 메시지를 읽기 전용 사용자에게 표시하려면 **Show configuration restriction message to read-only user** 확인란을 선택합니다. 이 옵션은 기본적으로 선택되어 있습니다.

```
"You are not allowed to modify the ASA configuration, because you do not have
sufficient privileges."
```

c. ASDM을 닫으려고 할 때 종료할 것인지 확인하는 프롬프트를 표시하려면 **Confirm before exiting ASDM** 확인란을 선택합니다. 이 옵션은 기본적으로 선택되어 있습니다.

d. 화면 판독기가 작동하도록 활성화하려면 **Enable screen reader support (requires ASDM restart)** 확인란을 선택합니다. 이 옵션을 활성화하려면 ASDM을 다시 시작해야 합니다.

e. ASDM 애플리케이션에서 완전한 기능을 실행하는 데 필요한 최소 ASA 메모리 양이 부족한 경우 알림을 받으려면 **Warn of insufficient ASA memory when ASDM loads** 확인란을 선택합니다. ASDM에서는 부팅 시 텍스트 배너 메시지에 메모리 경고를 표시하고, ASDM의 제목 표시줄 텍스트에 메시지를 표시하며, 24시간마다 한 번씩 syslog 알림을 보냅니다.

f. ASDM에서 생성한 CLI 명령을 보려면 **Preview commands before sending them to the device** 확인란을 선택합니다.

g. 단일 그룹의 여러 명령을 ASA로 보내려면 **Enable cumulative (batch) CLI delivery** 확인란을 선택합니다.

h. 시간 제한 메시지를 보내려면 컨피그레이션에 대한 최소 시간(초 단위)을 입력합니다. 기본값은 60초입니다.

i. **Packet Capture Wizard**를 사용하여 캡처된 패킷을 표시하려면 네트워크 스니퍼 애플리케이션의 이름을 입력하거나 **Browse**를 클릭하여 파일 시스템에서 이를 찾습니다.

4단계 **Rules Table** 탭에서 다음을 지정합니다.

a. Display 설정을 사용하면 Rules 테이블에 규칙이 표시되는 방식을 변경할 수 있습니다.

- Auto-Expand Prefix 설정을 기준으로 자동으로 확대된 네트워크 및 서비스 객체 그룹을 표시하려면 **Auto-expand network and service object groups with specified prefix** 확인란을 선택합니다.
- **Auto-Expand Prefix** 필드에 표시될 때 자동으로 확장할 네트워크 및 서비스 객체 그룹의 접두사를 입력합니다.

- Rules 테이블에 네트워크 및 서비스 객체 그룹의 멤버와 그룹 이름을 표시하려면 **Show members of network and service object groups** 확인란을 선택합니다. 이 확인란을 선택하지 않으면 그룹 이름만 표시됩니다.
- **Limit Members To** 필드에 표시할 네트워크 및 서비스 객체 그룹의 수를 입력합니다. 객체 그룹 멤버가 표시되면 처음 *n*개의 멤버만 표시됩니다.
- Rules 테이블에 모든 작업을 표시하려면 **Show all actions for service policy rules** 확인란을 선택합니다. 선택하지 않을 경우 요약 내용이 표시됩니다.

b. Deployment 설정을 사용하면 Rules 테이블에 변경 사항을 구축했을 때 ASA의 동작을 구성할 수 있습니다.

- 새 액세스 목록을 구축할 때 NAT 테이블을 지우려면 **Issue "clear xlate" command when deploying access lists** 확인란을 선택합니다. 이 설정을 사용하면 ASA에서 구성한 액세스 목록을 모든 변환된 주소에 적용할 수 있습니다.

c. Access Rule Hit Count Settings를 사용하면 Access Rules 테이블에서 히트 수가 업데이트되는 빈도를 구성할 수 있습니다. 히트 수는 명시적 규칙에만 적용할 수 있습니다. Access Rules 테이블의 묵시적 규칙에 대해서는 히트 수가 표시되지 않습니다.

- Access Rules 테이블에서 히트 수를 자동으로 업데이트하려면 **Update access rule hit counts automatically** 확인란을 선택합니다.
- Access Rules 테이블에서 히트 수 열이 업데이트되는 빈도를 초 단위로 지정합니다. 유효한 값은 10~86400초입니다.

5단계 **Syslog** 탭에서 다음을 지정합니다.

- **Syslog Colors** 영역에서는 각 심각도 수준에 따라 메시지의 배경색 또는 전경색을 구성하여 메시지 표시를 맞춤화할 수 있습니다. **Severity** 열에는 각 심각도 수준이 이름과 숫자별로 나열됩니다. 지정된 심각도 수준에 따라 메시지의 배경색 또는 전경색을 변경하려면 해당 열을 클릭합니다. **Pick a Color** 대화 상자가 표시됩니다. 다음 탭 중 하나를 선택합니다.
  - **Swatches** 탭의 팔레트에서 색상을 선택하고 **OK**를 클릭합니다.
  - **HSB** 탭에서 H, S, B 설정을 지정하고 **OK**를 클릭합니다.
  - **RGB** 탭에서 Red, Green, Blue 설정을 지정하고 **OK**를 클릭합니다.
- 경고 메시지를 표시하여 이중 syslog 메시지를 비활성화하려면 **NetFlow** 영역에서 **Warn to disable redundant syslog messages when NetFlow action is first applied to the global service policy rule** 확인란을 선택합니다.

6단계 이러한 3개의 탭에서 설정을 지정한 후에는 **OK**를 클릭하여 설정을 저장하고 **Preferences** 대화 상자를 닫습니다.

참고 기본 설정을 선택하거나 취소할 때마다 변경 사항이 .conf 파일에 저장되며 당시 워크스테이션에서 실행 중인 모든 기타 ASDM 세션에 제공됩니다. 모든 변경 사항을 적용하려면 ASDM을 다시 시작해야 합니다.

ASDM Assistant로 검색

ASDM Assistant 툴을 사용하면 특정 작업에 유용한 ASDM 절차가 포함된 도움말을 검색하고 볼 수 있습니다.

정보에 액세스하려면 **View > ASDM Assistant > How Do I?** 를 선택하거나메뉴 모음의 **Look For** 필드에 검색 요청을 입력합니다. 검색을 시작하려면 **Find** 드롭다운 목록에서 **How Do I?**를 선택합니다.

참고 이 기능은 PIX 보안 어플라이언스에서는 사용할 수 없습니다.

ASDM Assistant를 보려면 다음 단계를 수행합니다.

1단계 **View > ASDM Assistant**를 선택합니다.

ASDM Assistant 창이 표시됩니다.

2단계 **Search** 필드에 검색하려는 정보를 입력한 다음 **Go**를 클릭합니다.

요청한 정보가 **Search Results** 창에 표시됩니다.

3단계 자세한 내용을 보려면 **Search Results and Features** 섹션에 표시되는 링크를 클릭합니다.

History Metrics 활성화

Configuration > Device Management > Advanced > History Metrics 창을 사용하면 다양한 통계의 기록을 유지하도록 ASA를 구성할 수 있으며, 이러한 기록은 ASDM에서 모든 그래프/테이블에 표시할 수 있습니다. 기록 메트릭을 활성화하지 않을 경우, 통계를 실시간으로 모니터링하는 것만 가능합니다. 기록 메트릭을 활성화하면 최종 10분, 60분, 12시간, 5일 간격으로 통계 그래프를 볼 수 있습니다.

기록 메트릭을 구성하려면 다음 단계를 수행합니다.

1단계 **Configuration > Device Management > Advanced > History Metrics**를 선택합니다.

History Metrics 창이 표시됩니다.

2단계 기록 메트릭을 활성화하려면 **ASDM History Metrics** 확인란을 선택한 다음 **Apply**를 클릭합니다.

지원되지 않는 명령

ASDM에서는 ASA에 제공되는 거의 모든 명령을 지원하지만, 기존 컨피그레이션의 일부 명령은 ASDM에서 무시됩니다. 이러한 대부분의 명령은 컨피그레이션에서 그대로 유지할 수 있습니다. 자세한 내용은 **Tools > Show Commands Ignored by ASDM on Device**를 참조하십시오.

무시된 명령 및 보기 전용 명령

표 3-5에는 CLI를 통해 컨피그레이션에 추가된 경우 ASDM에서 지원하지만 ASDM 내에서 추가 또는 편집할 수 없는 명령의 목록이 나와 있습니다. ASDM에서 명령을 무시하면 ASDM GUI에 전혀 표시되지 않습니다. 명령이 보기 전용인 경우 GUI에 표시되지만 편집할 수는 없습니다.

표 3-5 지원되지 않는 명령 목록

지원되지 않는 명령	ASDM 동작
capture	무시됩니다.
coredump	무시됩니다. 이 명령은 CLI를 사용할 경우에만 구성할 수 있습니다.
crypto engine large-mod-accel	무시됩니다.
dhcp-server (tunnel-group name general-attributes)	ASDM에서는 모든 DHCP 서버에 하나의 설정만 허용합니다.
eject	지원되지 않습니다.
established	무시됩니다.
failover timeout	무시됩니다.
fips	무시됩니다.
nat-assigned-to-public-ip	무시됩니다.
pager	무시됩니다.
pim accept-register route-map	무시됩니다. ASDM을 사용하여 **list** 옵션만 구성할 수 있습니다.

service-policy global	이 명령에서 **match access-list** 클래스를 사용할 경우 무시됩니다. 예:
	`access-list myacl extended permit ip any any`
	`class-map mycm`
	`  match access-list myacl`
	`policy-map mypm`
	`  class mycm`
	`  inspect ftp`
	`service-policy mypm global`

set metric	무시됩니다.
sysopt nodnsalias	무시됩니다.
sysopt uauth allow-http-cache	무시됩니다.
terminal	무시됩니다.
threat-detection rate	무시됩니다.

지원되지 않는 명령어가 미치는 영향

ASDM에서 기존에 실행 중인 컨피그레이션을 로드하고 지원되지 않는 기타 명령을 발견할 경우, ASDM 작업에는 영향을 미치지 않습니다. 지원되지 않는 명령을 보려면 **Tools > Show Commands Ignored by ASDM on Device**를 선택합니다.

지원되지 않는 불연속 서브넷 마스크

ASDM에서는 255.255.0.255 같은 불연속 서브넷 마스크를 지원하지 않습니다. 예를 들어, 다음과 같은 형태를 사용할 수 없습니다.

```
ip address inside 192.168.2.1 255.255.0.255
```

ASDM CLI 툴에서 지원되지 않는 대화형 사용자 명령

ASDM CLI 툴에서는 대화형 사용자 명령을 지원하지 않습니다. 대화형 확인이 필요한 CLI 명령을 입력할 경우, ASDM에는 "[yes/no]"를 입력하라는 프롬프트가 표시되지만 입력 내용을 인식하지는 못합니다. 그 후 ASDM에서는 응답 대기 시간을 초과하게 됩니다.

예:

1. **Tools > Command Line Interface**를 선택합니다.
2. **crypto key generate rsa** 명령을 입력합니다.

   ASDM에서 기본 1024비트 RSA 키를 생성합니다.
3. **crypto key generate rsa** 명령을 다시 입력합니다.

   RSA 키를 다시 생성하는 대신 기존 키를 덮어쓰면 ASDM에 다음과 같은 오류 메시지가 표시됩니다.

```
Do you really want to replace them? [yes/no]:WARNING: You already have RSA
ke0000000000000$A key
Input line must be less than 16 characters in length.

%Please answer 'yes' or 'no'.
Do you really want to replace them [yes/no]:

%ERROR: Timed out waiting for a response.
ERROR: Failed to create new RSA keys names <Default-RSA-key>
```

해결 방법:

- ASDM 창을 사용하여 사용자 대화형 작업이 필요한 대부분의 명령을 구성할 수 있습니다.
- **noconfirm** 옵션이 포함된 CLI 명령의 경우, CLI 명령을 입력할 때 이 옵션을 사용합니다. 예:

```
crypto key generate rsa noconfirm
```

Cisco ASA Version 9.3의 기능

라이센스는 제공된 Cisco ASA에서 활성화되는 옵션을 지정합니다. 이 문서에서는 라이센스 활성화 키를 얻는 방법 및 이를 활성화하는 방법에 대해 설명합니다. 또한 각, 모델에 제공되는 라이센스에 대해서도 설명합니다.

참고 이 장에서는 버전 9.3의 라이센스에 대해 설명합니다. 다른 버전의 경우 해당 버전에 적용되는 라이센스 설명서를 참조하십시오.

http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-licensing-information-listing.html

모델당 지원되는 기능 라이센스

이 섹션에서는 각 모델에 제공되는 라이센스 및 라이센스에 대한 중요한 참고 사항을 설명합니다.

모델당 라이센스

이 섹션에는 각 모델에 제공되는 기능 라이센스가 나와 있습니다.

- 4-6 페이지의 ASA 5545-X
- 4-7 페이지의 ASA 5555-X
- 4-8 페이지의 ASA 5585-X 및 SSP-10
- 4-9 페이지의 SSP-20이 포함된 ASA 5585-X
- 4-10 페이지의 SSP-40 및 -60이 포함된 ASA 5585-X
- 4-11 페이지의 ASA Services Module
- 4-12 페이지의 ASAv - 가상 CPU 1개 포함
- 4-13 페이지의 ASAv - 가상 CPU 4개 포함

*기울임 꼴*로 된 항목은 Base(또는 Security Plus 등) 라이센스 버전을 대체할 수 있는 별도로 선택 가능한 라이센스입니다. 라이센스는 여러 가지를 서로 조합할 수 있습니다. 예를 들어, Unified Communications 라이센스 24개에 Strong Encryption 라이센스를 더하거나, AnyConnect Premium 라이센스 500개에 GTP/GPRS 라이센스를 더할 수 있고, 네 가지 라이센스를 모두 조합할 수도 있습니다.

참고 일부 기능은 서로 호환되지 않습니다. 호환성 정보에 대한 내용은 개별 기능이 설명된 장을 참조하십시오.

No Payload Encryption 모델을 사용할 경우 아래의 기능 중 일부가 지원되지 않을 수 있습니다. 지원되지 않는 기능에 대한 목록은 4-30 페이지의 No Payload Encryption 모델를 참조하십시오.

라이센스에 대한 자세한 내용은 4-14 페이지의 라이센스 참고 사항를 참조하십시오.

ASA 5512-X

표 4-1 ASA 5512-X 라이센스 기능

라이센스	Base 라이센스						Security Plus 라이센스					
Firewall 라이센스												
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*					비활성화됨	*선택적 기간별 라이센스: 사용 가능*				
동시 방화벽 연결 수	100,000						250,000					
GTP/GPRS	지원 안 함						비활성화됨	*선택적 라이센스: 사용 가능*				
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*					비활성화됨	*선택적 라이센스: 사용 가능*				
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*					2	*옵션 라이센스:*				
		24	*50*	*100*	*250*	*500*		*24*	*50*	*100*	*250*	*500*
VPN 라이센스												
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*					비활성화됨	*선택적 라이센스: 사용 가능*				
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*					비활성화됨	*선택적 라이센스: 사용 가능*				
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능 (250개 세션)*					비활성화됨	*선택적 라이센스: 사용 가능 (250개 세션)*				
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*					비활성화됨	*선택적 라이센스: 사용 가능*				

표 4-1 ASA 5512-X 라이센스 기능 (계속)

라이센스	Base 라이센스					Security Plus 라이센스				
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*				2	*선택적 영구 라이센스:*			
		10	*25*	*50*	*100*	*250*	*10*	*25*	*50*	*100*	*250*
		선택적 기간별(VPN Flex) 라이센스:				*250*	*선택적 기간별(VPN Flex) 라이센스:*				*250*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:						*선택적 공유 라이센스: 참가자 또는 서버. 서버용:*				
	500~50,000(500개 단위로 증분)			*50,000~545,000(1,000개 단위로 증분)*			*500~50,000(500개 단위로 증분)*			*50,000~545,000(1,000개 단위로 증분)*	
총 VPN(세션), 모든 유형 통합	250					250					
기타 VPN(세션)	250					250					
VPN 로드 밸런싱	지원 안 함					지원					
일반 라이센스											
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*				Base(DES)	*선택적 라이센스: Strong(3DES/AES)*				
장애 조치	지원 안 함					액티브/스탠바이 또는 액티브/액티브					
모든 유형의 인터페이스, 최대 개수	716					916					
보안 컨텍스트	지원 안 함					2	*옵션 라이센스:*				*5*
클러스터링	지원 안 함					2					
IPS 모듈	비활성화됨	*선택적 라이센스: 사용 가능*				비활성화됨	*선택적 라이센스: 사용 가능*				
VLAN, 최대 개수	50					100					

ASA 5515-X

표 4-2 ASA 5515-X 라이센스 기능

라이센스	Base 라이센스						
Firewall 라이센스							
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*					
동시 방화벽 연결 수	250,000						
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*					
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*					
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*	*24*	*50*	*100*	*250*	*500*
VPN 라이센스							
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*					
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*					
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(250개 세션)*					

표 4-2 ASA 5515-X 라이센스 기능 (계속)

라이센스	Base 라이센스					
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*				
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*				
		10	*25*	*50*	*100*	*250*
		선택적 기간별(VPN Flex) 라이센스:				*250*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:					
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*
총 VPN(세션), 모든 유형 통합	250					
기타 VPN(세션)	250					
VPN 로드 밸런싱	지원					
일반 라이센스						
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*				
장애 조치	액티브/스탠바이 또는 액티브/액티브					
모든 유형의 인터페이스, 최대 개수	916					
보안 컨텍스트	2	*옵션 라이센스:*			*5*	
클러스터링	2					
IPS 모듈	비활성화됨	*선택적 라이센스: 사용 가능*				
VLAN, 최대 개수	100					

ASA 5525-X

표 4-3 ASA 5525-X 라이센스 기능

라이센스	Base 라이센스								
Firewall 라이센스									
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*							
동시 방화벽 연결 수	500,000								
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*							
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*							
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*	*24*	*50*	*100*	*250*	*500*	*750*	*1000*
VPN 라이센스									
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(750개 세션)*							
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*							
		10	*25*	*50*	*100*	*250*	*500*	*750*	
		선택적 기간별(VPN Flex) 라이센스:						*750*	
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:								
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*			
총 VPN(세션), 모든 유형 통합	750								
기타 VPN(세션)	750								
VPN 로드 밸런싱	지원								
일반 라이센스									
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*							
장애 조치	액티브/스탠바이 또는 액티브/액티브								
모든 유형의 인터페이스, 최대 개수	1316								
보안 컨텍스트	2	*옵션 라이센스:*	*5*	*10*	*20*				
클러스터링	2								
IPS 모듈	비활성화됨	*선택적 라이센스: 사용 가능*							
VLAN, 최대 개수	200								

ASA 5545-X

표 4-4 ASA 5545-X 라이센스 기능

라이센스	Base 라이센스									
Firewall 라이센스										
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*								
동시 방화벽 연결 수	750,000									
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*								
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*								
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*	*24*	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*
VPN 라이센스										
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(2,500개 세션)*								
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*
		선택적 기간별(VPN Flex) 라이센스:								*2500*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:									
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*				
총 VPN(세션), 모든 유형 통합	2500									
기타 VPN(세션)	2500									
VPN 로드 밸런싱	지원									
일반 라이센스										
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*								
장애 조치	액티브/스탠바이 또는 액티브/액티브									
모든 유형의 인터페이스, 최대 개수	1716									
보안 컨텍스트	2	*옵션 라이센스:*	*5*	*10*	*20*	*50*				
클러스터링	2									
IPS 모듈	비활성화됨	*선택적 라이센스: 사용 가능*								
VLAN, 최대 개수	300									

ASA 5555-X

표 4-5 ASA 5555-X 라이센스 기능

라이센스	Base 라이센스								
Firewall 라이센스									
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*							
동시 방화벽 연결 수	1,000,000								
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*							
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*							
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN 라이센스									
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(5,000개 세션)*							
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*							
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*							
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
		선택적 기간별(VPN Flex) 라이센스:								*5000*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:								
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*			
총 VPN(세션), 모든 유형 통합	5000								
기타 VPN(세션)	5000								
VPN 로드 밸런싱	지원								
일반 라이센스									
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*							
장애 조치	액티브/스탠바이 또는 액티브/액티브								
모든 유형의 인터페이스, 최대 개수	2516								
보안 컨텍스트	2	*옵션 라이센스:*		*5*	*10*	*20*	*50*	*100*	
클러스터링	2								
IPS 모듈	비활성화됨	*선택적 라이센스: 사용 가능*							
VLAN, 최대 개수	500								

ASA 5585-X 및 SSP-10

동일한 섀시에서 같은 수준의 SSP 2개를 사용할 수 있습니다. 수준이 혼합된 SSP는 지원되지 않습니다(예: SSP-20이 포함된 SSP-10은 지원되지 않음). 각 SSP는 컨피그레이션 및 관리가 별도로 이루어지는 독립적인 디바이스로서 기능합니다. 원하는 경우 2개의 SSP를 하나의 장애 조치 쌍으로 사용할 수 있습니다.

표 4-6 SSP-10 라이센스 기능이 포함된 ASA 5585-X

라이센스	Base 및 Security Plus 라이센스									
Firewall 라이센스										
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*								
동시 방화벽 연결 수	1,000,000									
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*								
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*								
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*								
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN 라이센스										
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(5,000개 세션)*								
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*								
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
		선택적 기간별(VPN Flex) 라이센스:									*5000*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:									
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*				
총 VPN(세션), 모든 유형 통합	5000									
기타 VPN(세션)	5000									
VPN 로드 밸런싱	지원									
일반 라이센스										
10 GE I/O	**Base 라이센스**: 비활성화됨, 1GE에서 파이버 ifcs 실행					**Security Plus 라이센스**: 활성화됨, 10GE에서 ifcs 실행				
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*								
장애 조치	액티브/스탠바이 또는 액티브/액티브									
모든 유형의 인터페이스, 최대 개수	4612									
보안 컨텍스트	2	*옵션 라이센스:*		*5*	*10*	*20*	*50*	*100*		
클러스터링	비활성화됨	*선택적 라이센스: 16개 유닛에 제공*								
VLAN, 최대 개수	1024									

SSP-20이 포함된 ASA 5585-X

동일한 섀시에서 같은 수준의 SSP 2개를 사용할 수 있습니다. 수준이 혼합된 SSP는 지원되지 않습니다(예: SSP-40이 포함된 SSP-20은 지원되지 않음). 각 SSP는 컨피그레이션 및 관리가 별도로 이루어지는 독립적인 디바이스로서 기능합니다. 원하는 경우 2개의 SSP를 하나의 장애 조치 쌍으로 사용할 수 있습니다.

표 4-7 SSP-20 라이센스 기능이 포함된 ASA 5585-X

라이센스	Base 및 Security Plus 라이센스										
Firewall 라이센스											
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*									
동시 방화벽 연결 수	2,000,000										
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*									
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*									
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 라이센스											
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(10,000개 세션)*									
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		선택적 기간별(VPN Flex) 라이센스:										*10,000*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:											
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*						
총 VPN(세션), 모든 유형 통합	10,000											
기타 VPN(세션)	10,000											
VPN 로드 밸런싱	지원											
일반 라이센스												
10 GE I/O	**Base 라이센스**: 비활성화됨, 1GE에서 파이버 ifcs 실행					**Security Plus 라이센스**: 활성화됨, 10GE에서 ifcs 실행						
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*										
장애 조치	액티브/스탠바이 또는 액티브/액티브											
모든 유형의 인터페이스, 최대 개수	4612											
보안 컨텍스트	2	*옵션 라이센스:*		*5*	*10*	*20*	*50*	*100*	*250*			
클러스터링	비활성화됨	*선택적 라이센스: 16개 유닛에 제공*										
VLAN, 최대 개수	1024											

1. 10,000-세션 UC 라이센스를 사용할 경우, 총 통합 세션은 10,000개가 될 수 있으나 전화 프록시 세션의 최대 개수는 5000개입니다.

SSP-40 및 -60이 포함된 ASA 5585-X

동일한 섀시에서 같은 수준의 SSP 2개를 사용할 수 있습니다. 수준이 혼합된 SSP는 지원되지 않습니다(예: SSP-40이 포함된 SSP-60은 지원되지 않음). 각 SSP는 컨피그레이션 및 관리가 별도로 이루어지는 독립적인 디바이스로서 기능합니다. 원하는 경우 2개의 SSP를 하나의 장애 조치 쌍으로 사용할 수 있습니다.

표 4-8 SSP-40 및 -60 라이센스 기능이 포함된 ASA 5585-X

라이센스	Base 라이센스										
Firewall 라이센스											
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*									
동시 방화벽 연결 수	**SSP-40이 포함된 5585-X**: 4,000,000					**SSP-60이 포함된 5585-X**: 10,000,000					
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*									
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*									
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 라이센스											
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(10,000개 세션)*									
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		선택적 기간별(VPN Flex) 라이센스:										*10,000*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:											
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*						
총 VPN(세션), 모든 유형 통합	10,000											
기타 VPN(세션)	10,000											
VPN 로드 밸런싱	지원											
일반 라이센스												
10 GE I/O	활성화됨, 10GE에서 파이버 ifcs 실행											
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*										
장애 조치	액티브/스탠바이 또는 액티브/액티브											
모든 유형의 인터페이스, 최대 개수	4612											
보안 컨텍스트	2	*옵션 라이센스:*			*5*	*10*	*20*	*50*	*100*	*250*		
클러스터링	비활성화됨	*선택적 라이센스: 16개 유닛에 제공*										
VLAN, 최대 개수	1024											

1. 10,000-세션 UC 라이센스를 사용할 경우, 총 통합 세션은 10,000개가 될 수 있으나 전화 프록시 세션의 최대 개수는 5000개입니다.

ASA Services Module

표 4-9 라이센스 기능ASASM

라이센스	Base 라이센스										
Firewall 라이센스											
봇넷 트래픽 필터	비활성화됨	*선택적 기간별 라이센스: 사용 가능*									
동시 방화벽 연결 수	10,000,000										
GTP/GPRS	비활성화됨	*선택적 라이센스: 사용 가능*									
Intercompany Media Eng.	비활성화됨	*선택적 라이센스: 사용 가능*									
UC 전화 프록시 세션, 총 UC 프록시 세션	2	*옵션 라이센스:*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10,000*[1]
VPN 라이센스											
Adv. Endpoint Assessment	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect for Cisco VPN Phone	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Essentials	비활성화됨	*선택적 라이센스: 사용 가능(10,000개 세션)*									
AnyConnect for Mobile	비활성화됨	*선택적 라이센스: 사용 가능*									
AnyConnect Premium(세션)	2	*선택적 영구 라이센스:*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10,000*
		선택적 기간별(VPN Flex) 라이센스:										*10,000*
	선택적 공유 라이센스: 참가자 또는 서버. 서버용:											
	500~50,000(500개 단위로 증분)					*50,000~545,000(1,000개 단위로 증분)*						
총 VPN(세션), 모든 유형 통합	10,000											
기타 VPN(세션)	10,000											
VPN 로드 밸런싱	지원											
일반 라이센스												
암호화	Base(DES)	*선택적 라이센스: Strong(3DES/AES)*										
장애 조치	액티브/스탠바이 또는 액티브/액티브											
보안 컨텍스트	2	*옵션 라이센스:*										
		5	*10*	*20*	*50*	*100*	*250*					
클러스터링	지원 안 함											
VLAN, 최대 개수	1000											

1. 10,000-세션 UC 라이센스를 사용할 경우, 총 통합 세션은 10,000개가 될 수 있으나 전화 프록시 세션의 최대 개수는 5000개입니다.

ASAv - 가상 CPU 1개 포함

표 4-10 ASAv - 1 vCPU 라이센스 기능 포함

라이센스	Standard 및 Premium 라이센스	
Firewall 라이센스		
봇넷 트래픽 필터	지원	
동시 방화벽 연결 수	100,000	
GTP/GPRS	지원	
Intercompany Media Eng.	지원	
UC 전화 프록시 세션, 총 UC 프록시 세션	250	
VPN 라이센스		
Adv. Endpoint Assessment	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect Essentials	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원되지 않음
AnyConnect for Cisco VPN Phone	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect for Mobile	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect Premium(세션)	**Standard 라이센스**: 2	**Premium 라이센스**: 250
	Shared 라이센스: 지원되지 않음	
총 VPN(세션), 모든 유형 통합	250	
기타 VPN(세션)	250	
VPN 로드 밸런싱	지원	
일반 라이센스		
암호화	Strong(3DES/AES)	
장애 조치	액티브/스탠바이	
모든 유형의 인터페이스, 최대 개수	716	
보안 컨텍스트	지원 안 함	
클러스터링	지원 안 함	
VLAN, 최대 개수	50	
RAM, vCPU 주파수 제한	2GB, 5000MHz	

ASAv - 가상 CPU 4개 포함

표 4-11 ASAv - 4 vCPU 라이센스 기능 포함

라이센스	Standard 및 Premium 라이센스	
Firewall 라이센스		
봇넷 트래픽 필터	지원	
동시 방화벽 연결 수	500,000	
GTP/GPRS	지원	
Intercompany Media Eng.	지원	
UC 전화 프록시 세션, 총 UC 프록시 세션	1000	
VPN 라이센스		
Adv. Endpoint Assessment	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect Essentials	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원되지 않음
AnyConnect for Cisco VPN Phone	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect for Mobile	**Standard 라이센스**: 지원되지 않음	**Premium 라이센스**: 지원됨
AnyConnect Premium(세션)	**Standard 라이센스**: 2	**Premium 라이센스**: 750
	Shared 라이센스: 지원되지 않음	
총 VPN(세션), 모든 유형 통합	750	
기타 VPN(세션)	750	
VPN 로드 밸런싱	지원	
일반 라이센스		
암호화	Strong(3DES/AES)	
장애 조치	액티브/스탠바이	
모든 유형의 인터페이스, 최대 개수	1316	
보안 컨텍스트	지원 안 함	
클러스터링	지원 안 함	
VLAN, 최대 개수	200	
RAM, vCPU 주파수 제한	8GB, 20000MHz **참고** 4 vCPU 라이센스를 적용하였으나 2, 3개의 vCPU를 구축하도록 선택할 경우 다음과 같은 값이 표시됩니다. 가상 CPU 2개 — 4GB RAM, vCPU 주파수 제한 10000MHz, 동시 방화벽 연결 수 250,000개 가상 CPU 3개 — 4GB RAM, vCPU 주파수 제한 15000MHz, 동시 방화벽 연결 수 350,000개	

라이센스 참고 사항

표 4-12에는 4-1 페이지의 모델당 라이센스의 여러 표에서 공유하고 있는 일반적인 각주가 포함되어 있습니다.

표 4-12 라이센스 참고 사항

라이센스	참고
AnyConnect Essentials	AnyConnect Essentials 세션에는 다음과 같은 VPN 유형이 포함됩니다. • SSL VPN • IKEv2를 사용하는 IPsec 원격 액세스 이 라이센스에서는 브라우저 기반(클라이언트리스) SSL VPN 액세스 또는 Cisco Secure Desktop을 지원하지 않습니다. 이러한 기능의 경우 AnyConnect Essentials 대신 AnyConnect Premium 라이센스를 활성화합니다. **참고** AnyConnect Essentials 라이센스를 이용할 경우 VPN 사용자는 웹 브라우저를 사용하여 로그인하고 AnyConnect 클라이언트를 다운로드 및 시작(WebLaunch)할 수 있습니다. AnyConnect 클라이언트 소프트웨어를 이 라이센스로 활성화하거나 AnyConnect Premium 라이센스로 활성화하는 모든 경우 동일한 클라이언트 기능이 제공됩니다. AnyConnect Essentials 라이센스는 제공된 ASA에서 AnyConnect Premium 라이센스(모든 유형) 또는 Advanced Endpoint Assessment 라이센스와 동시에 활성화될 수 없습니다. 그러나 같은 네트워크의 다른 ASA에서는 AnyConnect Essentials 라이센스와 AnyConnect Premium 라이센스를 실행할 수 있습니다. 기본적으로 ASA에서는 AnyConnect Essentials 라이센스를 사용하지만, **webvpn**을 입력한 후 **no anyconnect-essentials** 명령을 사용하거나, ASDM에서 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials** 창을 사용하면 이 라이센스를 비활성화하여 다른 라이센스를 사용할 수 있습니다. 4-19 페이지의 VPN 라이센스 및 기능 호환성도 참조하십시오.
AnyConnect for Cisco VPN Phone	이 라이센스를 AnyConnect Premium 라이센스와 함께 사용하면 AnyConnect 호환성을 통해 구축된 하드웨어 IP 폰에서 액세스가 가능하도록 지원할 수 있습니다.

표 4-12 라이센스 참고 사항 (계속)

라이센스	참고
AnyConnect for Mobile	이 라이센스에서는 Windows Mobile 5.0, 6.0, 6.1을 실행하는 터치스크린 모바일 디바이스용 AnyConnect Client에 대한 액세스를 제공합니다. AnyConnect 2.3 이상 버전에 모바일 액세스를 지원하려면 이 라이센스를 사용하는 것이 좋습니다. 이 라이센스를 사용하려면 AnyConnect Essentials 또는 AnyConnect Premium 라이센스 중 하나를 활성화하여 허용되는 총 SSL VPN 세션 수를 지정해야 합니다. **모바일 상태 지원** 원격 액세스 제어를 시행하고 모바일 디바이스에서 상태 데이터를 수집하려면 AnyConnect Mobile 라이센스나 AnyConnect Essentials 또는 AnyConnect Premium 라이센스를 ASA에 설치해야 합니다. 설치하는 라이센스를 기준으로 제공되는 기능은 다음과 같습니다. • AnyConnect Premium 라이센스 기능 – 지원되는 모바일 디바이스에서 DAP 정책을 시행하는 작업은 DAP 속성 및 기타 기존 엔드포인트 특성을 기준으로 이루어집니다. 여기에는 모바일 디바이스에서 원격 액세스를 허용하거나 거부하는 것도 포함됩니다. • AnyConnect Essentials 라이센스 기능 – 그룹 단위로 모바일 디바이스 액세스를 활성화 또는 비활성화하고 ASDM을 사용하여 이러한 기능을 구성합니다. – DAP 정책을 시행하거나 이러한 모바일 디바이스에 대한 원격 액세스를 거부 또는 허용할 수 있는 기능이 없어도 CLI 또는 ASDM을 통해 연결된 모바일 디바이스에 대한 정보를 표시합니다.
AnyConnect Premium	AnyConnect Premium 세션에는 다음과 같은 VPN 유형이 포함됩니다. • SSL VPN • 클라이언트리스 SSL VPN • IKEv2를 사용하는 IPsec 원격 액세스
AnyConnect Premium Shared	공유 라이센스를 사용하면 ASA에서는 여러 클라이언트ASA의 공유 라이센스 서버 역할을 수행할 수 있습니다. 공유 라이센스 풀은 용량이 크지만 각 ASA에서 사용되는 세션의 최대 수는 영구 라이센스에 나열된 최대 수를 초과할 수 없습니다.
봇넷 트래픽 필터	동적 데이터베이스를 다운로드하려면 Strong Encryption(3DES/AES) 라이센스가 필요합니다.
암호화	DES 라이센스는 비활성화할 수 없습니다. 3DES 라이센스를 설치한 경우 DES를 계속 사용할 수 있습니다. Strong Encryption만 사용하고 DES를 사용하지 않으려면, 모든 관련 명령에서 Strong Encryption만 사용하도록 구성해야 합니다.

표 4-12 라이센스 참고 사항 (계속)

라이센스	참고
Intercompany Media Engine	IME(Intercompany Media Engine) 라이센스를 활성화할 경우, 구성된 TLS 프록시 한도의 최대치까지 TLS 프록시 세션을 사용할 수 있습니다. 기본 TLS 프록시 한도보다 높은 UC(Unified Communications) 라이센스가 설치된 경우, ASA에서는 이러한 제한을 UC 라이센스 제한으로 설정하며 여기에 해당하는 모델에 따라 추가 세션 수도 추가합니다. **tls-proxy maximum-sessions** 명령을 사용하거나 ASDM에서 **Configuration > Firewall > Unified Communications > TLS Proxy** 창을 사용하여 TLS 프록시 한도를 수동으로 구성할 수 있습니다. 모델의 한도를 보려면 **tls-proxy maximum-sessions ?** 명령을 입력합니다. 또한 UC 라이센스를 설치할 경우 UC에 제공되는 TLS 프록시 세션을 IME 세션에도 사용할 수 있습니다. 예를 들어, TLS 프록시 세션의 한도를 1000으로 구성하고 750-세션 UC 라이센스를 구매할 경우, 처음 250개의 IME 세션은 UC에 제공되는 세션에 영향을 미치지 않습니다. 250개 이상의 세션이 IME에 필요할 경우, UC 및 IME에서는 플랫폼 한도의 나머지 750개 세션을 선착순으로 사용합니다. • 라이센스 부품 번호가 “K8”로 끝나는 경우, TLS 프록시 세션이 1000으로 제한됩니다. • 라이센스 부품 번호가 “K9”로 끝나는 경우, TLS 프록시 한도는 해당하는 컨피그레이션 및 플랫폼 모델에 따라 달라집니다. **참고** K8 및 K9의 경우 해당 라이센스의 내보내기 제한 여부를 참조하며, K8은 제한되지 않고 K9는 제한됩니다. 연결에 SRTP 암호화 세션을 사용할 수도 있습니다. • K8 라이센스의 경우 SRTP 세션이 250개로 제한됩니다. • K9 라이센스의 경우 제한이 없습니다. **참고** 미디어 암호화/해독이 필요한 호출만 SRTP 한도에 가산됩니다. 호출에 통과가 설정되어 있으면 두 범례가 모두 SRTP인 경우에도 해당 호출은 한도에 가산되지 않습니다.
모든 유형의 인터페이스, 최대 개수	통합된 인터페이스(예: VLAN, 물리적, 이중화, 브릿지 그룹, EtherChannel 인터페이스)의 최대 개수입니다. 컨피그레이션에 정의된 모든 **interface**은 이 한도의 대상이 됩니다.
IPS 모듈	IPS 모듈 라이센스를 사용하면 IPS 소프트웨어 모듈을 ASA에서 실행할 수 있습니다. 또한 IPS 측에 IPS 서명 서브스크립션이 있어야 합니다. 다음 지침을 참조하십시오. • 필요한 IPS 서명 서브스크립션을 구매하려면 ASA에 IPS가 사전 설치되어 있어야 합니다(부품 번호에 "IPS"가 포함되어야 함(예: ASA5515-IPS-K9)). IPS 부품 번호가 없는 ASA에 대해서는 IPS 서명 서브스크립션을 구매할 수 없습니다. • 두 유닛에 모두 IPS 서명 서브스크립션이 있어야 합니다. 이러한 서브스크립션은 ASA 라이센스가 아니므로 장애 조치에서 공유되지 않습니다. • 장애 조치를 수행하려면 IPS 서명 서브스크립션에 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이센스와 마찬가지로, IPS 모듈 라이센스는 장애 조치 클러스터 라이센스 내에서 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 장애 조치 시 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.

표 4-12 라이센스 참고 사항 (계속)

라이센스	참고
기타 VPN	기타 VPN 세션에는 다음과 같은 VPN 유형이 포함됩니다. • IKEv1을 사용하는 IPsec 원격 액세스 • IKEv1을 사용하는 IPsec 사이트 대 사이트 VPN • IKEv2를 사용하는 IPsec 사이트 대 사이트 VPN 이 라이센스는 Base 라이센스에 포함됩니다.
총 VPN(세션), 모든 유형 통합	• 최대 VPN AnyConnect 및 기타 VPN 세션 이상의 최대 VPN 세션이 추가될 경우에도, 통합된 세션은 VPN 세션 한도를 초과하면 안 됩니다. 최대 VPN 세션 수를 초과할 경우, ASA가 오버로드될 수 있으므로 네트워크의 크기를 적절하게 조정해야 합니다. • 클라이언트리스 SSL VPN 세션을 시작한 후 포털에서 AnyConnect 클라이언트 세션을 시작한 경우, 총 1개의 세션이 사용됩니다. 그러나 처음에 AnyConnect 클라이언트를 시작(예: 독립형 클라이언트에서)한 후 클라이언트리스 SSL VPN 포털에 로그인할 경우 2개의 세션이 사용됩니다.

표 4-12 라이센스 참고 사항 (계속)

라이센스	참고
UC 전화 프록시 세션, 총 UC 프록시 세션	다음 애플리케이션에서는 연결에 TLS 프록시 세션을 사용합니다. 이러한 애플리케이션에서 사용되는 각 TLS 프록시 세션의 수는 UC 라이센스 한도를 기준으로 계산됩니다. • 전화 프록시 • 프레즌스 페더레이션 프록시 • 암호화된 음성 감시 TLS 프록시 세션을 사용하는 기타 애플리케이션의 경우 UC 한도에 가산되지 않습니다. Mobility Advantage Proxy(라이센스가 필요하지 않음) 및 IME(별도의 IME 라이센스 필요)를 예로 들 수 있습니다. 일부 UC 애플리케이션에서는 연결에 다중 세션을 사용할 수 있습니다. 예를 들어, 전화를 기본으로 구성하고 Cisco Unified Communications Manager를 백업할 경우, 2개의 TLS 프록시 연결이 사용되므로 2개의 UC 프록시 세션이 사용됩니다. **tls-proxy maximum-sessions** 명령을 사용하거나 ASDM에서 **Configuration > Firewall > Unified Communications > TLS Proxy** 창을 사용하여 TLS 프록시 한도를 개별적으로 구성할 수 있습니다. 모델의 한도를 보려면 **tls-proxy maximum-sessions ?** 명령을 입력합니다. 기본 TLS 프록시 한도보다 높은 UC 라이센스를 적용할 경우, ASA에서는 TLS 프록시 한도를 UC 한도에 맞게 자동으로 설정합니다. TLS 프록시 한도는 UC 라이센스 한도보다 우선합니다. TLS 프록시 한도를 UC 라이센스보다 작게 설정하면 UC 라이센스에서 모든 세션을 사용할 수 없습니다. **참고** 라이센스 부품 번호가 "K8"로 끝날 경우(예: 사용자 수 250명 이하의 라이센스), TLS 프록시 세션은 1000으로 제한됩니다. 라이센스 부품 번호가 "K9"로 끝날 경우(예: 사용자 수가 250명 이상인 라이센스), TLS 프록시 세션 한도는 컨피그레이션 및 모델 한도에 따라 달라집니다. K8 및 K9의 경우 해당 라이센스의 내보내기 제한 여부를 참조하며, K8은 제한되지 않고 K9는 제한됩니다. 예를 들어, **clear configure all** 명령을 사용하여 컨피그레이션을 지우면 TLS 프록시 한도가 모델의 기본값으로 설정됩니다. 이 기본값이 UC 라이센스 한도보다 낮을 경우, **tls-proxy maximum-sessions** 명령을 사용하여 한도를 다시 높이라는 오류 메시지가 표시됩니다(ASDM에서 **TLS Proxy** 창 사용). 장애 조치를 사용 중이고 **write standby** 명령을 입력하거나 ASDM에서 **File > Save Running Configuration to Standby Unit**을 사용하여 기본 유닛에서 컨피그레이션 동기화를 시행할 경우, 보조 유닛에서 **clear configure all** 명령이 자동으로 생성되므로 보조 유닛에 경고 메시지가 표시될 수 있습니다. 컨피그레이션 동기화는 기본 유닛에서 TLS 프록시 한도 설정을 복원하므로 이러한 경고 메시지는 무시해도 좋습니다. 연결에 SRTP 암호화 세션을 사용할 수도 있습니다. • K8 라이센스의 경우 SRTP 세션이 250개로 제한됩니다. • K9 라이센스의 경우 제한이 없습니다. **참고** 미디어 암호화/해독이 필요한 호출만 SRTP 한도에 가산됩니다. 호출에 통과가 설정되어 있으면 두 범례가 모두 SRTP인 경우에도 해당 호출은 한도에 가산되지 않습니다.
가상 CPU	ASAv에 Virtual CPU 라이센스를 설치해야 합니다. 라이센스를 설치하지 않으면 처리량은 100Kbps로 제한되므로 사전 연결 테스트를 수행할 수 있습니다. Virtual CPU 라이센스는 일반적인 작업에 필요합니다.

표 4-12 라이센스 참고 사항 (계속)

라이센스	참고
VLAN, 최대 개수	어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다.
VPN 로드 밸런싱	VPN 로드 밸런싱에는 Strong Encryption(3DES/AES) 라이센스가 필요합니다.

VPN 라이센스 및 기능 호환성

표 4-13에는 VPN 라이센스와 기능을 조합하는 방법이 나와 있습니다.

AnyConnect Essentials 라이센스 및 AnyConnect Premium 라이센스에서 지원되는 자세한 기능 목록을 보려면 *AnyConnect Secure Mobility 클라이언트 기능, 라이센스, OS*를 참조하십시오.

- 버전 3.1:
  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect31/feature/guide/anyconnect31features.html
- 버전 3.0:
  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/feature/guide/anyconnect30features.html
- 버전 2.5:
  http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/feature/guide/anyconnect25features.html

표 4-13 VPN 라이센스 및 기능 호환성

	다음 라이센스 중 하나를 활성화:[1]	
지원되는 항목:	AnyConnect Essentials	AnyConnect Premium
AnyConnect for Cisco VPN Phone	아니요	예
AnyConnect for Mobile[2]	예	예
Advanced Endpoint Assessment	아니요	예
AnyConnect Premium Shared	아니요	예
클라이언트 기반 SSL VPN	예	예
브라우저 기반(클라이언트리스) SSL VPN	아니요	예
IPsec VPN	예	예
VPN 로드 밸런싱	예	예
Cisco Secure Desktop	아니요	예

1. AnyConnect Essentials 라이센스 또는 AnyConnect Premium 라이센스 중 하나의 유효한 라이센스 유형만 보유할 수 있습니다. 기본적으로 ASA에는 2개의 세션을 지원하는 AnyConnect Premium 라이센스가 포함됩니다. AnyConnect Essentials 라이센스를 설치하면 이 라이센스가 기본적으로 사용됩니다. Premium 라이센스를 대신 활성화하려면 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials 창을 사용합니다.
2. Mobile Posture 지원은 AnyConnect Essentials 및 AnyConnect Premium 라이센스와 다릅니다. 자세한 내용은 4-14 페이지의 표 4-12를 참조하십시오.

기능 라이센스 정보

라이센스는 제공된 ASA에서 활성화되는 옵션을 지정합니다. 라이센스는 160비트(32비트 또는 20바이트 단어 5개) 값으로 된 활성화 키로 나타냅니다. 이 값은 일련 번호(11자 문자열) 및 활성화된 기능으로 인코딩됩니다.

사전 설치된 라이센스

기본적으로 ASA에는 라이센스가 이미 설치된 상태로 배송됩니다. 이러한 라이센스는 원하는 라이센스를 더 추가할 수 있는 Base 라이센스일 수 있습니다. 또는 주문 내역 및 공급업체에서 설치한 내역에 따라 모든 라이센스가 이미 설치되어 있을 수 있습니다. 어떤 라이센스가 설치되어 있는지 확인하려면 4-36 페이지의 라이센스 모니터링 섹션을 참조하십시오.

영구 라이센스

단일한 영구 활성화 키를 설치할 수 있습니다. 영구 활성화 키에는 단일한 키로 모든 라이센스 기능이 포함됩니다. 기간별 라이센스를 설치할 경우, ASA에서는 영구 라이센스와 기간별 라이센스를 실행 중인 라이센스로 통합합니다. ASA에서 라이센스를 통합하는 방법에 대한 자세한 내용은 4-21 페이지의 영구 라이센스와 기간별 라이센스가 통합되는 원리를 참조하십시오.

기간별 라이센스

영구 라이센스 외에도, 기간별 라이센스를 구매하거나 기간 제한이 있는 평가판 라이센스를 제공받을 수 있습니다. 예를 들어, 단기간에 급증한 동시 SSL VPN 사용자 수를 처리하기 위해 기간별 AnyConnect Premium 라이센스를 구매하거나, 유효 기간이 1년인 Botnet Traffic Filter 기간별 라이센스를 주문할 수 있습니다.

기간별 라이센스 활성화 지침

- 같은 기능을 지원하는 여러 개의 라이센스를 포함하여, 여러 개의 기간별 라이센스를 설치할 수 있습니다. 그러나 기능당 기간별 라이센스는 한 번에 하나만 *활성화*할 수 있습니다. 비활성 라이센스는 설치된 채로 유지되며 사용할 준비가 되어 있습니다. 예를 들어, 1000-세션 AnyConnect Premium 라이센스 및 2500-세션 AnyConnect Premium 라이센스를 설치할 경우, 이러한 라이센스 중 하나만 활성화할 수 있습니다.
- 키에 여러 기능이 포함된 평가판 라이센스를 활성화할 경우 포함된 기능 중 하나를 지원하기 위해 다른 기간별 라이센스를 활성화할 수 없습니다. 예를 들어, 평가판 라이센스에 Botnet Traffic Filter 및 1000-세션 AnyConnect Premium 라이센스가 포함된 경우 독립형 기간별 2500-세션 AnyConnect Premium 라이센스를 활성화할 수 없습니다.

기간별 라이센스 타이머 작동 방식

- 기간별 라이센스의 타이머는 ASA에서 해당 라이센스를 활성화하면 카운트다운이 시작됩니다.
- 라이센스의 기간이 만료되기 전에 기간별 라이센스 사용을 중단할 경우 타이머가 중지됩니다. 타이머는 기간별 라이센스를 다시 활성화할 경우에만 다시 시작됩니다.
- 기간별 라이센스가 활성화되어 있고 ASA를 종료한 경우 타이머의 카운트다운은 계속 진행됩니다. 연장된 기간 동안 ASA를 종료 상태에 두려면 종료하기 전에 기간별 라이센스를 비활성화해야 합니다.

참고 기간별 라이센스를 설치한 후에는 시스템 클록을 변경하지 않는 것이 좋습니다. 시스템 클록을 이후 날짜로 설정하고 다시 로드할 경우, ASA에서는 시스템 클록을 원래 설치 시간과 비교하여 확인하며 실제로 사용한 시간보다 더 많은 시간이 지난 것으로 가정합니다. 클록을 앞으로 설정했고 실제 실행 시간이 원래 설치 시간과 시스템 클록 간의 시간보다 클 경우, 다시 로드하면 라이센스가 즉시 만료됩니다.

영구 라이센스와 기간별 라이센스가 통합되는 원리

기간별 라이센스를 활성화하면 영구 라이센스와 기간별 라이센스의 기능이 통합되어 실행 중인 라이센스가 형성됩니다. 영구 라이센스와 기간별 라이센스가 통합되는 방식은 라이센스의 유형에 따라 달라집니다. 표 4-14에는 각 기능 라이센스의 통합 규칙이 나와 있습니다.

참고 영구 라이센스를 사용할 경우에도 기간별 라이센스가 활성화되어 있으면 카운트다운이 계속 진행됩니다.

표 4-14 기간별 라이센스 통합 규칙

기간별 기능	통합된 라이센스 규칙
AnyConnect Premium 세션	기간별 또는 영구 라이센스 중 더 높은 값이 사용됩니다. 예를 들어, 영구 라이센스가 1000개 세션이고 기간별 라이센스가 2500개 세션일 경우 2500개 세션이 활성화됩니다. 일반적으로 영구 라이센스보다 기능이 적은 기간별 라이센스는 설치하지 않습니다. 이러한 라이센스를 설치할 경우 영구 라이센스가 사용됩니다.
Unified Communications 프록시 세션	기간별 라이센스 세션이 플랫폼 한도 내에서 영구 라이센스에 추가됩니다. 예를 들어, 영구 라이센스가 2500개 세션이고 기간별 라이센스가 1000개 세션일 경우 기간별 라이센스가 활성화되어 있는 한 3500개 세션이 활성화됩니다.
보안 컨텍스트	기간별 라이센스 세션이 플랫폼 한도 내에서 영구 컨텍스트에 추가됩니다. 예를 들어, 영구 라이센스가 10개 컨텍스트이고 기간별 라이센스가 20개 컨텍스트일 경우 기간별 라이센스가 활성화되어 있는 한 30개 컨텍스트가 활성화됩니다.
봇넷 트래픽 필터	사용 가능한 Botnet Traffic Filter 라이센스가 없으며 기간별 라이센스가 사용됩니다.
기타	기간별 또는 영구 라이센스 중 더 높은 값이 사용됩니다. 상태가 활성화 또는 비활성화된 라이센스의 경우, 상태가 활성화된 라이센스가 사용됩니다. 숫자 계층이 있는 라이센스의 경우, 더 높은 값이 사용됩니다. 일반적으로 영구 라이센스보다 기능이 적은 기간별 라이센스는 설치하지 않습니다. 이러한 라이센스를 설치할 경우 영구 라이센스가 사용됩니다.

통합된 라이센스를 보려면 4-36 페이지의 라이센스 모니터링를 참조하십시오.

기간별 라이센스 스태킹

대부분의 경우 기간별 라이센스를 갱신해야 할 수 있으며, 기존 라이센스에서 새 라이센스로 원활하게 전환할 수 있습니다. 기간별 라이센스에만 제공되는 기능의 경우, 새 라이센스를 적용하려면 그전에 라이센스가 만료되지 않도록 하는 것이 특히 중요합니다. ASA에서는 기간별 라이센스를 *스태킹*할 수 있도록 지원하므로, 새 라이센스를 조기에 설치하여 라이센스가 만료되거나 라이센스의 기간이 짧아지지 않을까 걱정하지 않아도 됩니다.

기존에 설치된 라이센스와 동일한 기간별 라이센스를 설치한 경우, 라이센스가 통합되며 기간은 통합된 기간과 같습니다.

예:

1. 52주 Botnet Traffic Filter 라이센스를 설치하고 해당 라이센스를 25주간 사용합니다(27주가 남음).
2. 이후 또 다른 52주 Botnet Traffic Filter 라이센스를 구매합니다. 두 번째 라이센스를 설치할 때 라이센스가 통합되어 기간이 79주가 됩니다(52주 + 27주).

유사한 사례:

1. 8주 1000-세션 AnyConnect Premium 라이센스를 설치하고 2주간 사용합니다(6주가 남음).
2. 그런 다음 또 다른 8주 1000-세션 라이센스를 설치하면 라이센스가 통합되어 14주(8주 + 6주) 1000-세션 라이센스가 됩니다.

라이센스가 동일하지 않을 경우(예: 1000-세션 AnyConnect Premium 라이센스와 2500-세션 라이센스) 라이센스가 통합되지 *않습니다*. 기능당 기간별 라이센스를 하나만 활성화할 수 있으므로 여러 라이센스 중 하나만 활성화할 수 있습니다. 라이센스 활성화에 대한 자세한 내용은 4-33 페이지의 키 활성화 또는 비활성화를 참조하십시오.

동일하지 않은 라이센스는 통합되지 않지만 현재 라이센스가 만료될 경우, 같은 기능 라이센스가 설치되어 있으면 ASA에서는 이를 자동으로 활성화합니다. 자세한 내용은 4-23 페이지의 기간별 라이센스 만료를 참조하십시오.

기간별 라이센스 만료

현재 기능 라이센스가 만료될 경우, 같은 기능 라이센스가 설치되어 있으면 ASA에서는 이를 자동으로 활성화합니다. 기능에 사용할 수 있는 기간별 라이센스가 없으면 영구 라이센스가 사용됩니다.

기능을 지원하는 추가 기간별 라이센스가 여러 개 있는 경우 ASA에서는 첫 번째 라이센스를 사용합니다. 이 라이센스는 사용자 구성 가능하지 않으며 내부 작업에 따라 달라집니다. ASA에서 활성화한 라이센스가 아닌 다른 기간별 라이센스를 사용하려면 원하는 라이센스를 수동으로 활성화해야 합니다. 4-33 페이지의 키 활성화 또는 비활성화를 참조하십시오.

기간별 2500-세션 AnyConnect Premium 라이센스(활성), 기간별 1000-세션 AnyConnect Premium 라이센스(비활성), 500-세션 AnyConnect Premium 라이센스가 있는 경우를 가정해 보겠습니다. 2500-세션 라이센스가 만료되면 ASA에서는 1000-세션 라이센스를 활성화합니다. 1000-세션 라이센스가 만료되면 ASA에서는 500-세션 영구 라이센스를 사용합니다.

Shared AnyConnect Premium 라이센스

공유 라이센스를 사용하면 AnyConnect Premium 세션을 대량으로 구매할 수 있으며, ASA 중 하나를 공유 라이센스 서버로 구성하고 나머지는 공유 라이센스 참가자로 구성하여 필요에 따라 ASA의 그룹 간에 세션을 공유할 수 있습니다. 이 섹션에서는 공유 라이센스가 어떤 방식으로 활용되는지 설명합니다.

공유 라이센스 서버 및 참가자 정보

다음 단계에서는 공유 라이센스가 어떤 방식으로 운영되는지 설명합니다.

1. 어떤 ASA가 공유 라이센스 서버가 되어야 하는지 결정하고, 디바이스 일련 번호를 사용하여 공유 라이센스 서버의 라이센스를 구매합니다.
2. 어떤 ASA가 공유 라이센스 참가자(공유 백업 서버 포함)가 되어야 하는지 결정하고, 각 디바이스 일련 번호를 사용하여 각 디바이스의 공유 라이센스 참가자 라이센스를 얻습니다.
3. (선택 사항) 두 번째 ASA를 공유 라이센스 백업 서버로 지정합니다. 하나의 백업 서버만 지정할 수 있습니다.

참고 공유 라이센싱 백업 서버에는 참가자 라이센스만 필요합니다.

4. 공유 라이센스 서버에서 공유 비밀을 구성합니다. 공유 비밀을 보유한 모든 참가자는 공유 라이센스를 사용할 수 있습니다.
5. ASA를 참가자로 지정하면 ASA에서는 로컬 라이센스 및 모델 정보를 비롯한 자체 정보를 전송하여 공유 라이센스 서버에 등록됩니다.

참고 참가자는 IP 네트워크를 통해 서버와 통신을 수행할 수 있어야 하며, 같은 서브넷에 있을 필요는 없습니다.

6. 공유 라이센스 서버에서는 참가자가 서버에 폴링하는 빈도와 관련된 정보에 응답합니다.
7. 참가자가 로컬 라이센스의 세션을 모두 사용할 경우, 추가 세션을 50-세션 늘려달라는 요청이 공유 서버에 전송됩니다.
8. 공유 라이센스 서버에서는 공유 라이센스에 응답합니다. 참가자가 사용한 총 세션 수는 플랫폼 모델의 최대 세션 수를 초과할 수 없습니다.

참고 공유 라이센스 서버는 공유 라이센스 풀에도 참가할 수 있습니다. 참가를 위해 참가자 라이센스 및 서버 라이센스를 구매하지 않아도 됩니다.

   a. 공유 라이센스 풀에 참가자가 사용할 세션이 충분히 남아 있지 않은 경우, 서버에서는 최대한 사용 가능한 세션 수에 응답합니다.
   b. 참가자는 서버에서 요청을 충분히 충족할 때까지 추가 세션을 요청하는 새로 고침 메시지를 계속 전송하게 됩니다.
9. 참가자에 대한 로드가 줄어들면 공유 세션을 릴리스하라는 메시지가 서버에 전송됩니다.

참고 ASA에서는 서버와 참가자 간에 SSL을 사용하여 모든 통신을 암호화합니다.

참가자와 서버 간의 통신 문제

참가자와 서버 간의 통신 문제에 대한 내용은 다음 지침을 참조하십시오.

- 참가자가 새로 고침 간격이 3번 지난 후 새로 고침 메시지를 전송하지 못하면 서버에서는 공유 라이센스 풀에 세션을 다시 릴리스합니다.
- 참가자가 새로 고침을 전송할 라이센스 서버에 도달하지 못할 경우, 참가자는 서버에서 받은 공유 라이센스를 최대 24시간 동안 계속 사용할 수 있습니다.
- 24시간 후에도 참가자가 라이센스 서버와 계속 통신을 수행하지 못하면, 세션이 여전히 필요한 경우에도 참가자는 공유 라이센스를 릴리스합니다. 참가자는 설정된 기존 연결을 남겨두지만 라이센스 제한을 넘는 새 연결은 수락할 수 없습니다.
- 참가자가 24시간이 만료되기 전에 서버에 다시 연결하였으나 서버에서 참가자 세션이 만료된 경우, 참가자는 해당 세션에 대해 새 요청을 전송해야 합니다. 서버에서는 참가자에게 다시 할당할 수 있는 최대한 많은 수의 세션에 응답합니다.

공유 라이센스 백업 서버 정보

백업 역할을 수행할 수 있도록 하려면 공유 라이센스 백업 서버를 기본 공유 라이센스 서버로 올바르게 등록해야 합니다. 등록이 완료되면 기본 공유 라이센스 서버 설정 및 공유 라이센스 정보(예: 등록된 참가자 목록 및 현재 라이센스 사용량 포함)가 백업과 동기화됩니다. 기본 서버 및 백업 서버에서는 10초 간격으로 데이터를 동기화합니다. 최초 동기화를 완료하면 백업 서버에서는 다시 로드된 경우에도 백업 업무를 성공적으로 수행할 수 있습니다.

기본 서버가 중단되면 백업 서버에서 서버 작업을 이어받습니다. 백업 서버의 참가자에 대한 발급 세션이 중단되고, 기존 세션이 만료된 후 백업 서버에서는 최대 30일간 연속으로 작업을 수행할 수 있습니다. 30일 내에 기본 서버를 복구해야 합니다. 15일에 중요도가 높은 syslog 메시지가 전송되며 30일에 다시 한 번 전송됩니다.

기본 서버가 다시 가동되면 기본 서버에서는 백업 서버와 동기화를 수행한 후 서버 작업을 이어받습니다.

백업 서버가 활성화되어 있지 않을 때에는 기본 공유 라이센스 서버의 일반 참가자 역할을 수행합니다.

참고 기본 공유 라이센스 서버를 처음 시작할 경우, 백업 서버는 개별적으로 5일 동안만 작동될 수 있습니다. 작동 한도는 30일에 도달할 때까지 일별로 증가합니다. 또한 기본 서버가 해당 기간에 중단될 경우, 백업 서버의 작동 한도는 일별로 감소합니다. 기본 서버가 다시 작동되면 백업 서버의 한도는 다시 일별로 증가합니다. 예를 들어, 기본 서버가 20일간 중단되었고 백업 서버가 해당 기간 동안 활성화되어 있었다면, 백업 서버의 남은 기간 한도는 10일밖에 되지 않습니다. 백업 서버에서는 20일 이상 백업을 비활성 상태로 유지한 후 최대 30일을 "재충전"할 수 있습니다. 이러한 재충전 기능은 공유 라이센스의 남용을 줄이기 위해 구현되었습니다.

장애 조치 및 공유 라이센스

이 섹션에서는 공유 라이센스가 장애 조치와 어떻게 상호 작용하는지 설명합니다.

- 4-25 페이지의 장애 조치 및 공유 라이센스 서버
- 4-26 페이지의 장애 조치 및 공유 라이센스 참가자

장애 조치 및 공유 라이센스 서버

이 섹션에서는 기본 서버와 백업 서버가 장애 조치와 어떤 방식으로 상호 작용하는지 설명합니다. 공유 라이센스 서버에서는 ASA와 마찬가지로 일반적인 업무(예: VPN 게이트웨이 및 방화벽 역할 기능 수행)도 수행하므로, 안정성을 높이기 위해서는 기본 및 백업 공유 라이센스 서버에 대한 장애 조치를 구성해야 할 수 있습니다.

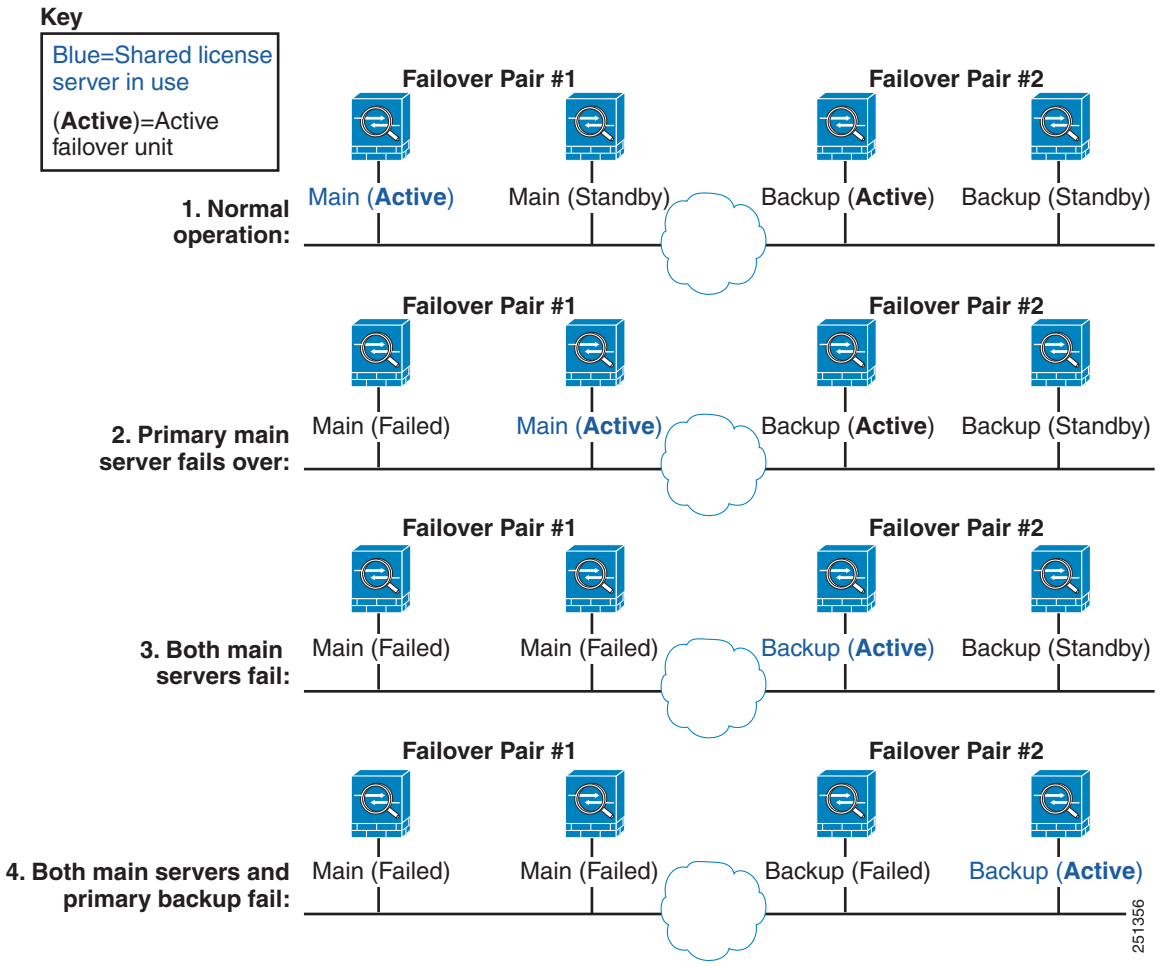
참고 백업 서버 메커니즘은 장애 조치와 분리되어 있지만 호환 가능합니다.

공유 라이센스는 단일 컨텍스트 모드에서만 지원되므로 액티브/액티브 장애 조치는 지원되지 않습니다.

액티브/스탠바이 장애 조치의 경우, 기본 유닛이 기본 공유 라이센스 서버 역할을 하며 장애 조치 후에는 스탠바이 유닛이 기본 공유 라이센스 서버 역할을 합니다. 스탠바이 유닛은 백업 공유 라이센스 서버 역할을 하지 *않습니다*. 그 대신, 원하는 경우 백업 서버 역할을 하는 두 번째 유닛 쌍을 사용할 수 있습니다.

2개의 장애 조치 쌍이 있는 네트워크를 예로 들어 보겠습니다. 1번 쌍에는 기본 라이센스 서버가 포함됩니다. 2번 쌍에는 백업 서버가 포함됩니다. 1번 쌍의 기본 유닛이 중단되면, 스탠바이 유닛이 즉시 새로운 기본 라이센스 서버가 됩니다. 2번 쌍의 백업 서버는 사용되지 않습니다. 1번 쌍의 두 유닛이 모두 중단될 경우에만 2번 쌍의 백업 서버가 공유 라이센스 서버로 사용됩니다. 1번 쌍이 계속 중단되어 있고 2번 쌍의 기본 유닛이 중단될 경우, 2번 쌍의 스탠바이 유닛이 공유 라이센스 서버로 사용됩니다(그림 4-1 참조).

그림 4-1 장애 조치 및 공유 라이센스 서버



스탠바이 백업 서버에서는 기본 백업 서버와 동일한 작동 한도를 공유합니다. 스탠바이 유닛이 액티브 상태가 되면, 기본 유닛이 중단된 곳에서 카운트다운을 계속 진행합니다. 자세한 내용은 4-25 페이지의 공유 라이센스 백업 서버 정보를 참조하십시오.

장애 조치 및 공유 라이센스 참가자

참가자 쌍의 경우, 별도의 참가자 ID를 사용하여 두 유닛을 모두 공유 라이센스 서버에 등록합니다. 액티브 유닛은 스탠바이 유닛으로 참가자 ID를 동기화합니다. 스탠바이 유닛에서는 이 ID를 사용하여 액티브 역할로 전환될 경우 전송 요청을 생성합니다. 이러한 전송 요청은 이전의 액티브 유닛에서 새 액티브 유닛으로 공유 세션을 이동하는 데 사용됩니다.

최대 참가자 수

ASA에서는 공유 라이센스의 참가자 수를 제한하지 않습니다. 그러나 공유 네트워크가 너무 클 경우 라이센스 서버의 성능에 영향을 미칠 수 있습니다. 이러한 경우 참가자 새로 고침의 지연 간격을 늘리거나, 2개의 공유 네트워크를 생성할 수 있습니다.

장애 조치 또는 ASA 클러스터 라이센스

몇 가지 예외 사항을 제외하고, 장애 조치 및 클러스터 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다. 이전 버전의 경우 해당 버전의 라이센스 설명서를 참조하십시오.

장애 조치 라이센스 요구 사항 및 예외 사항

장애 조치 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다.

이전 버전의 ASA 소프트웨어에는 각 유닛과 일치하는 라이센스가 필요했습니다. 버전 8.3(1)부터는 더 이상 동일한 라이센스를 설치하지 않아도 됩니다. 일반적으로 기본 유닛에만 라이센스를 구매하며, 액티브/스탠바이 장애 조치가 이루어질 경우 보조 유닛이 액티브 유닛이 되면 보조 유닛에서 기본 라이센스를 상속합니다. 두 유닛에 모두 라이센스가 있는 경우, 해당 라이센스는 실행 중인 단일 장애 조치 클러스터 라이센스로 통합됩니다.

이러한 규칙의 예외 사항은 다음과 같습니다.

- ASA 5512-X용 Security Plus — Base 라이센스에서는 장애 조치를 지원하지 않으므로 Base 라이센스만 있는 스탠바이 유닛에서는 장애 조치를 사용할 수 없습니다.
- 암호화 라이센스 — 두 유닛에는 모두 동일한 암호화 라이센스가 있어야 합니다.
- ASA 5555-X를 통한 ASA 5512-X용 IPS 모듈 — 두 유닛에는 모두 IPS 모듈 라이센스가 있어야 합니다. 또한 두 유닛의 IPS에는 IPS 서명 서브스크립션이 필요합니다. 다음 지침을 참조하십시오.
  - 필요한 IPS 서명 서브스크립션을 구매하려면 ASA에 IPS가 사전 설치되어 있어야 합니다(부품 번호에 "IPS"가 포함되어야 함(예: ASA5515-IPS-K9)). IPS 부품 번호가 없는 ASA에 대해서는 IPS 서명 서브스크립션을 구매할 수 없습니다.
  - 두 유닛에 모두 IPS 서명 서브스크립션이 있어야 합니다. 이러한 서브스크립션은 ASA 라이센스가 아니므로 장애 조치에서 공유되지 않습니다.
  - IPS 서명 서브스크립션에는 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이센스와 마찬가지로, IPS 모듈 라이센스는 장애 조치 클러스터 라이센스 내에서 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.
- ASAv 가상 CPU — 장애 조치를 구축할 경우 기본 유닛과 동일한 수의 vCPU가 스탠바이 유닛에 할당되어 있는지 확인하십시오(vCPU 라이센스 일치 여부도 함께 확인).

참고 유효한 영구 키가 필요합니다. 드문 경우지만 인증 키가 제거될 수 있습니다. 키가 모두 0으로 구성되어 있으면 장애 조치를 활성화하기 전에 유효한 인증 키를 다시 설치해야 합니다.

ASA 클러스터 라이센스 요구 사항 및 예외 사항

클러스터 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다. 일반적으로 마스터 유닛에만 라이센스를 구매하며, 슬레이브 유닛에서는 마스터 라이센스를 상속합니다. 여러 유닛에 라이센스가 있는 경우, 해당 라이센스는 단일하게 실행되는 ASA 클러스터 라이센스로 통합됩니다.

이러한 규칙의 예외 사항은 다음과 같습니다.

- 클러스터링 라이센스 — 각 유닛에 클러스터링 라이센스가 있어야 합니다.
- 암호화 라이센스 — 각 유닛에 동일한 암호화 라이센스가 있어야 합니다.

장애 조치 또는 ASA 클러스터 통합 방식

장애 조치 쌍 또는 ASA 클러스터의 경우, 각 유닛의 라이센스는 단일하게 실행되는 클러스터 라이센스로 통합됩니다. 각 유닛에 별도의 라이센스를 구매할 경우, 통합된 라이센스에서는 다음 규칙을 사용합니다.

- 숫자 계층(예: 세션 수)이 있는 라이센스의 경우, 각 유닛의 라이센스 값은 플랫폼 한도 내에서 통합됩니다. 사용 중인 모든 라이센스가 기간별 라이센스인 경우, 라이센스의 기간이 동시에 카운트다운됩니다.

  장애 조치 예:

  - 2개의 ASA에 각각 10개의 AnyConnect Premium 세션이 설치되어 있습니다. 이러한 라이센스는 총 20개의 AnyConnect Premium 세션으로 통합됩니다.
  - 2개의 ASA 5525-X에 각각 500개의 AnyConnect Premium 세션이 설치되어 있습니다. 플랫폼 한도는 750개이므로, 통합된 라이센스에서는 750개의 AnyConnect Premium 세션을 허용합니다.

    참고 위의 예에서 AnyConnect Premium 라이센스가 기간별 라이센스인 경우, 라이센스 중 하나를 비활성화하여 500개의 세션 라이센스가 "낭비"되지 않도록 할 수 있습니다. 플랫폼 한도로 인해 250개의 세션만 사용할 수 있기 때문입니다.

  - 2개의 ASA 5545-X ASA 중 하나에는 20개의 컨텍스트가 있고 나머지에는 10개의 컨텍스트가 있습니다. 통합된 라이센스에서는 30개의 컨텍스트를 허용합니다. 액티브/액티브 장애 조치의 경우 컨텍스트는 두 유닛 간에 분리됩니다. 예를 들어, 한 유닛에서 18개의 컨텍스트를 사용하고 다른 유닛에서 12개의 컨텍스트를 사용하는 방식으로 총 30개를 사용할 수 있습니다.

  ASA 클러스터링 예:

  - SSP-10이 포함된 4개의 ASA 5585-X ASA가 있고, 3개의 각 유닛에 50개의 컨텍스트가 있고 1개 유닛에는 기본 2개의 컨텍스트가 있습니다. 플랫폼 한도가 100이므로 통합된 라이센스에서는 최대 100개의 컨텍스트를 허용합니다. 따라서 마스터 유닛에서 최대 100개의 컨텍스트를 컨피그레이션할 수 있습니다. 각 슬레이브 유닛에서도 컨피그레이션 복제를 통해 100개의 컨텍스트를 포함할 수 있습니다.

  - SSP-60이 포함된 4개의 ASA 5585-X ASA가 있고, 3개의 각 유닛에 50개의 컨텍스트가 있고 1개 유닛에는 기본 2개의 컨텍스트가 있습니다. 플랫폼 한도가 250이므로 라이센스가 통합되면 총 152개의 컨텍스트를 지원합니다. 따라서 마스터 유닛에서 최대 152개의 컨텍스트를 컨피그레이션할 수 있습니다. 각 슬레이브 유닛에서도 컨피그레이션 복제를 통해 152개의 컨텍스트를 포함할 수 있습니다.

- 상태가 활성화 또는 비활성화된 라이센스의 경우, 상태가 활성화된 라이센스가 사용됩니다.
- 활성화 또는 비활성화된 기간별 라이센스(숫자 계층이 없는)의 경우, 모든 라이센스의 기간이 통합됩니다. 기본/마스터 유닛에서 라이센스 기간의 카운트다운을 먼저 시작하며, 해당 기간이 만료되면 보조/슬레이브 유닛에서 라이센스 기간의 카운트다운을 시작하는 순으로 진행됩니다. 이 규칙은 액티브/액티브 장애 조치 및 ASA 클러스터링에도 적용되며 모든 유닛이 활성화 상태로 작동되는 경우에도 마찬가지입니다.

  예를 들어, 두 유닛에 48주의 기간이 남은 Botnet Traffic Filter 라이센스가 있을 경우 통합된 기간은 96주입니다.

통합된 라이센스를 보려면 4-36 페이지의 라이센스 모니터링를 참조하십시오.

장애 조치 또는 ASA 클러스터 유닛 간의 통신 해제

유닛의 통신이 30일 이상 끊어지면 각 유닛에서는 설치된 라이센스를 로컬로 전환합니다. 30일의 유예 기간 동안, 실행 중인 통합 라이센스는 모든 유닛에서 계속 사용됩니다.

30일의 유예 기간 도중 통신이 복원되면 기간별 라이센스의 경우 기본/마스터 라이센스에서 경과된 시간이 공제됩니다. 기본/마스터 라이센스가 만료된 경우, 보조/슬레이브 라이센스에서만 카운트다운을 시작합니다.

30일 동안 통신이 복원되지 않으면 기간별 라이센스의 경우 모든 유닛 라이센스(설치된 경우)에서 시간이 공제됩니다. 이러한 라이센스는 별도의 라이센스로 처리되며 통합된 라이센스의 이점을 누릴 수 없습니다. 경과된 시간에는 30일의 유예 기간이 포함됩니다.

예:

1. 두 유닛에 52주 Botnet Traffic Filter 라이센스가 설치되어 있습니다. 실행 중인 통합된 라이센스에서는 총 104주의 기간을 허용합니다.
2. 유닛은 10주간 장애 조치 유닛/ASA 클러스터 역할을 수행하면, 94주는 통합된 라이센스에 남습니다(42주는 기본/마스터에, 52주는 보조/슬레이브에).
3. 유닛의 통신이 끊길 경우(예: 기본/마스터 유닛에 오류가 발생할 경우), 보조/슬레이브 유닛에서 통합된 라이센스를 계속 사용하며 94주부터 카운트다운을 계속 진행합니다.
4. 기간별 라이센스 동작은 통신이 언제 복원되었는지에 따라 달라집니다.

- 30일 이내 — 경과된 시간이 기본/마스터 유닛 라이센스에서 공제됩니다. 이 경우, 4주 후에 통신이 복원되었습니다. 따라서 기본/마스터 라이센스에서 4주가 공제되어 90주로 통합되었습니다(38주는 기본에, 52주는 보조에).
- 30일 후 — 경과된 시간이 두 유닛에서 모두 공제됩니다. 이 경우, 6주 후에 통신이 복원되었습니다. 따라서 두 기본/마스터 및 보조/슬레이브 라이센스에서 6주가 공제되어, 84주로 통합되었습니다(36주는 기본/마스터에, 46주는 보조/슬레이브에).

장애 조치 쌍 업그레이드

장애 조치 쌍의 경우 두 유닛에 동일한 라이센스가 필요하지 않으므로, 다운타임 없이 각 유닛에 새 라이센스를 적용할 수 있습니다. 다시 로드해야 하는 영구 라이센스를 적용할 경우(4-33 페이지의 표 4-15 참조) 다시 로드하는 동안 다른 유닛으로 장애 조치가 시작될 수 있습니다. 두 유닛을 모두 다시 로드해야 하는 경우 이를 별도로 다시 로드하여 다운타임을 방지할 수 있습니다.

No Payload Encryption 모델

일부 No Payload Encryption 모델을 구입할 수 있습니다. 일부 국가의 경우, Cisco ASA Series에서 페이로드 암호화를 활성화할 수 없습니다. ASA 소프트웨어에서는 No Payload Encryption 모델을 감지하고 다음 기능을 비활성화할 수 있습니다.

- 통합 커뮤니케이션
- VPN

여전히 Strong Encryption(3DES/AES) 라이센스를 관리 연결에 사용하도록 설치할 수 있습니다. 예를 들어 ASDM HTTPS/SSL, SSHv2, 텔넷 및 SNMPv3를 사용할 수 있습니다. 또한 봇넷(Botnet) Traffic Filter(SSL 사용)용 동적 데이터베이스를 다운로드할 수도 있습니다.

라이센스를 볼 경우(4-36 페이지의 라이센스 모니터링 참조), VPN 및 Unified Communications 라이센스가 나열되지 않습니다.

라이센스 FAQ

Q. AnyConnect Premium 및 Botnet Traffic Filter 같은 여러 개의 기간별 라이센스를 활성화할 수 있습니까?

A. 예. 기능당 기능별 라이센스는 한 번에 하나씩 활성화할 수 있습니다.

Q. 기간별 라이센스를 "스태킹"하여 시간 제한이 만료되었을 때 다음 라이센스를 자동으로 사용하도록 할 수 있습니까?

A. 예. 동일한 라이센스의 경우, 여러 기간별 라이센스를 설치할 때 시간 제한이 통합됩니다. 동일하지 않은 라이센스의 경우(예: 1000-세션 AnyConnect Premium 라이센스 및 2500-세션 라이센스), ASA에서는 기능에 사용할 수 있는 다음 기간별 라이센스를 자동으로 활성화합니다.

Q. 활성 상태인 기간별 라이센스는 그대로 유지하면서 새 영구 라이센스를 설치할 수 있습니까?

A. 예. 영구 라이센스를 활성화해도 기간별 라이센스에는 영향을 미치지 않습니다.

Q. 장애 조치를 위해 공유 라이센스 서버를 기본 유닛으로 사용하고, 공유 라이센스 백업 서버를 보조 유닛으로 사용할 수 있습니까?

A. 번호 보조 유닛에는 기본 유닛에서 실행 중인 것과 동일한 라이센스가 있습니다. 공유 라이센스 서버에는 서버 라이센스가 필요합니다. 백업 서버에는 참가자 라이센스가 필요합니다. 백업 서버는 두 백업 서버의 개별적인 장애 조치 쌍이 될 수 있습니다.

Q. 장애 조치 쌍의 보조 유닛에 동일한 라이센스를 구매해야 합니까?

A. 번호 버전 8.3(1)부터는 두 유닛에 같은 라이센스가 없어도 됩니다. 일반적으로 기본 유닛에만 라이센스를 구매하며, 보조 유닛이 액티브 유닛이 되면 보조 유닛에서 기본 라이센스를 상속합니다. 보조 유닛에 별도의 라이센스가 있는 경우(예: 이전 8.3 소프트웨어에 같은 라이센스를 구매한 경우), 라이센스는 모델의 한도 내에서 하나의 실행 중인 장애 조치 클러스터 라이센스로 통합됩니다.

Q. 공유 AnyConnect Premium 라이센스 외에 기간별 또는 영구 AnyConnect Premium 라이센스를 사용할 수 있습니까?

A. 예. 공유 라이센스는 로컬로 설치된 라이센스(기간별 또는 영구)가 모두 사용된 세션 이후에만 사용됩니다. **참고**: 공유 라이센스 서버에서는 영구 AnyConnect Premium 라이센스가 사용되지 않습니다. 그러나 기간별 라이센스는 공유 라이센스 서버 라이센스와 동시에 사용할 수 있습니다. 이 경우, 기간별 라이센스 세션은 로컬 AnyConnect Premium 세션에만 사용할 수 있습니다. 해당 세션은 참가자가 사용할 공유 라이센스 풀에 추가할 수 없습니다.

지침 및 제한 사항

활성화 키에 대한 다음 지침을 참조하십시오.

컨텍스트 모드 지침

- 다중 컨텍스트 모드의 경우 시스템 실행 영역에서 활성화 키를 적용합니다.
- 공유 라이센스는 다중 컨텍스트 모드에서 지원되지 않습니다.

방화벽 모드 지침

라우팅 및 투명 모드에서는 모든 라이센스 유형을 사용할 수 있습니다.

장애 조치 지침

- 공유 라이센스는 액티브/액티브 모드에서 지원되지 않습니다. 자세한 내용은 4-25 페이지의 장애 조치 및 공유 라이센스를 참조하십시오.
- 4-27 페이지의 장애 조치 또는 ASA 클러스터 라이센스를 참조하십시오.

업그레이드 및 다운그레이드 지침

임의의 이전 버전에서 최신 버전으로 업그레이드할 경우 활성화 키는 계속 호환 가능합니다. 그러나 다운그레이드 기능을 유지하려는 경우 문제가 생길 수 있습니다.

- 버전 8.1 이하로 다운그레이드 — 업그레이드 후 *8.2 이전에* 도입된 추가 기능 라이센스를 활성화할 경우, 다운그레이드를 수행하면 활성화 키가 이전 버전과 계속 호환됩니다. 그러나 *8.2 이상* 버전에 도입된 기능 라이센스를 활성화할 경우에는 활성화 키가 이전 버전과 호환되지 않습니다. 호환되지 않는 라이센스 키가 있을 경우 다음 지침을 참조하십시오.
  - 기존에 이전 버전에서 활성화 키를 입력한 경우 ASA에서 해당 키를 사용합니다(버전 8.2 이상에서 활성화된 새 라이센스 없음).
  - 새 시스템이 있으나 이전 활성화 키가 없는 경우, 이전 버전과 호환되는 새 활성화 키를 요청해야 합니다.
- 버전 8.2 이하로 다운그레이드 — 버전 8.3에는 더욱 강력한 기간별 키 용도 및 장애 조치 라이센스 변경 사항이 도입되었습니다.
  - 둘 이상의 시간 기준 활성화 키가 활성 상태일 경우, 다운그레이드하면 가장 최근에 활성화된 시간 기준 키만 활성 상태가 됩니다. 그 밖의 모든 키는 비활성 상태가 됩니다. 최근 기간별 라이센스가 8.3에 도입된 기능에 사용되는 라이센스인 경우, 이전 버전에서 사용할 수 없더라도 해당 라이센스는 활성화 라이센스 상태로 유지됩니다. 영구 키 또는 유효한 기간별 키를 다시 입력합니다.
  - 장애 조치 쌍에 일치하지 않는 라이센스가 있을 경우 다운그레이드를 수행하면 장애 조치가 비활성화됩니다. 키가 일치하더라도 사용된 라이센스는 더 이상 통합 라이센스가 아닙니다.
  - 기간별 라이센스를 설치하였으나 8.3 버전에 도입된 기능에 사용되는 라이센스인 경우, 다운그레이드를 수행하면 해당 기간별 라이센스가 활성화 상태로 유지됩니다. 기간별 라이센스를 비활성화하려면 영구 키를 다시 입력해야 합니다.

추가 지침 및 제한

- 활성화 키는 컨피그레이션 파일에 저장되지 않으며, 플래시 메모리에 숨겨진 파일로 저장됩니다.
- 활성화 키는 디바이스의 일련 번호와 연결되어 있습니다. 기능 라이센스는 디바이스 간에 이동할 수 없습니다(하드웨어 오류가 발생한 경우는 예외). 하드웨어 오류로 인해 디바이스를 교체해야 하고 Cisco TAC에서 지원되는 문제인 경우, Cisco Licensing Team에 문의하여 기존 라이센스를 새 일련 번호에 보낼 수 있습니다. Cisco Licensing Team에서는 제품 승인 키 참조 번호와 기존 일련 번호를 요청합니다.
- 구매한 후에는 환불 또는 라이센스 업그레이드를 위해 라이센스를 반환할 수 없습니다.
- 하나의 유닛에 동일한 기능을 지원하는 2개의 개별 라이센스를 함께 추가할 수 없습니다. 예를 들어, 25-세션 SSL VPN 라이센스를 구매하고 나중에 50-세션 라이센스를 구매한 경우, 세션 75개를 사용할 수 없으며 최대 50개의 세션을 사용할 수 있습니다. (업그레이드 가격으로 더 많은 라이센스(예: 25개에서 75개 세션)를 구매하게 될 수 있습니다. 이러한 유형의 업그레이드는 2개의 개별 라이센스를 함께 추가하는 경우와 구분해야 합니다.)
- 모든 라이센스 유형을 활성화할 수 있으나, 일부 기능은 서로 호환되지 않을 수 있습니다. AnyConnect Essentials 라이센스의 경우 AnyConnect Premium 라이센스, Shared AnyConnect Premium 라이센스, Advanced Endpoint Assessment 라이센스와 호환되지 않습니다. 기본적으로 AnyConnect Essentials 라이센스를 설치할 경우(해당 모델에 사용 가능한 경우), 위의 라이센스 대신 이 라이센스가 사용됩니다. 사용하거나 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials 창을 사용하여 컨피그레이션에서 AnyConnect Essentials 라이센스를 비활성화하면 다른 라이센스의 사용을 복원할 수 있습니다.

라이센스 구성

활성화 키 얻기

활성화 키를 얻으려면 Cisco 어카운트 담당자를 통해 구매할 수 있는 제품 승인 키가 필요합니다. 각 기능 라이센스에 별도의 제품 승인 키를 구매해야 합니다. 예를 들어, Base 라이센스를 보유한 경우 Advanced Endpoint Assessment 및 추가 AnyConnect Premium 세션에 대한 별도의 키를 구매할 수 있습니다.

제품 승인 키를 얻은 후에는 다음 단계를 수행하여 Cisco.com에서 해당 키를 등록합니다.

세부 단계

1단계 **Configuration > Device Management > Licensing > Activation Key**를 선택하거나(다중 컨텍스트 모드의 경우 시스템 실행 영역에서 일련 번호 확인) ASA에 대한 일련 번호를 얻습니다.

2단계 Cisco.com에 등록되어 있지 않은 경우 어카운트를 생성합니다.

3단계 아래의 라이센스 웹 페이지로 이동합니다.

http://www.cisco.com/go/license

4단계 메시지가 표시되면 다음 정보를 입력합니다.

- 제품 승인 키(키가 여러 개 있는 경우, 그중 첫 번째 키를 입력합니다. 각 키를 별도의 프로세스로 입력해야 합니다.)
- ASA에 대한 일련 번호
- 이메일 주소

활성화 키는 자동으로 생성되며 사용자가 제공한 이메일 주소로 전송됩니다. 이 키에는 영구 라이센스에 대해 현재까지 등록한 모든 기능이 포함됩니다. 기간별 라이센스의 경우, 각 라이센스에는 별도의 활성화 키가 있습니다.

5단계 추가 제품 승인 키가 있는 경우 각 제품 승인 키에 4단계를 반복합니다. 제품 승인 키를 모두 입력하면, 등록한 모든 영구 기능이 포함된 최종 활성화 키가 제공됩니다.

키 활성화 또는 비활성화

이 섹션에서는 새 활성화 키를 입력하고, 기간별 키를 활성화 및 비활성화하는 방법을 설명합니다.

전제 조건

- 다중 컨텍스트 모드인 경우, 시스템 실행 영역에 활성화 키를 입력합니다.
- 일부 영구 라이센스의 경우 활성화 후 ASA를 다시 로드해야 합니다. 표 4-15에는 다시 로드해야 하는 라이센스가 나열되어 있습니다.

표 4-15 영구 라이센스 다시 로드 요구 사항

모델	다시 로드해야 하는 라이센스 작업
모든 모델	암호화 라이센스 다운그레이드
ASAv	vCPU 라이센스 다운그레이드

제한 사항

임의의 이전 버전에서 최신 버전으로 업그레이드할 경우 활성화 키는 계속 호환 가능합니다. 그러나 다운그레이드 기능을 유지하려는 경우 문제가 생길 수 있습니다.

- 버전 8.1 이하로 다운그레이드 — 업그레이드 후 *8.2 이전에* 도입된 추가 기능 라이센스를 활성화할 경우, 다운그레이드를 수행하면 활성화 키가 이전 버전과 계속 호환됩니다. 그러나 *8.2 이상* 버전에 도입된 기능 라이센스를 활성화할 경우에는 활성화 키가 이전 버전과 호환되지 않습니다. 호환되지 않는 라이센스 키가 있을 경우 다음 지침을 참조하십시오.
  - 기존에 이전 버전에서 활성화 키를 입력한 경우 ASA에서 해당 키를 사용합니다(버전 8.2 이상에서 활성화된 새 라이센스 없음).
  - 새 시스템이 있으나 이전 활성화 키가 없는 경우, 이전 버전과 호환되는 새 활성화 키를 요청해야 합니다.
- 버전 8.2 이하로 다운그레이드 — 버전 8.3에는 더욱 강력한 기간별 키 용도 및 장애 조치 라이센스 변경 사항이 도입되었습니다.
  - 둘 이상의 시간 기준 활성화 키가 활성 상태일 경우, 다운그레이드하면 가장 최근에 활성화된 시간 기준 키만 활성 상태가 됩니다. 그 밖의 모든 키는 비활성 상태가 됩니다.
  - 장애 조치 쌍에 일치하지 않는 라이센스가 있을 경우 다운그레이드를 수행하면 장애 조치가 비활성화됩니다. 키가 일치하더라도 사용된 라이센스는 더 이상 통합 라이센스가 아닙니다.

세부 단계

1단계 **Configuration > Device Management**를 선택한 다음 해당 모델에 따라 **Licensing > Activation Key** 또는 **Licensing Activation Key** 창을 선택합니다.

2단계 영구 또는 기간별 새 활성화 키를 입력하려면 New Activation Key 필드에 새 활성화 키를 입력합니다.

이 키는 각 요소 간에 하나의 공백이 있는 5개 요소로 된 16진수 문자열입니다. 맨 앞의 0x 지정자는 선택 사항이며, 모든 값은 16진수로 가정합니다. 예:

```
ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

하나의 영구 키를 설치하고, 여러 개의 기간별 키를 설치할 수 있습니다. 새 영구 키를 입력하면 이전에 설치한 키를 덮어씁니다. 새 기간별 키를 입력하면 Time-based License Keys Installed 테이블에 해당 키가 기본적으로 활성화되고 표시됩니다. 지정된 기능에 활성화한 최종 기간별 키가 활성화 상태의 키입니다.

3단계 설치된 기간별 키를 활성화하거나 비활성화하려면 Time-based License Keys Installed 테이블을 선택하고 **Activate** 또는 **Deactivate**를 클릭합니다.

각 기능에는 하나의 기간별 키만 활성화할 수 있습니다. 자세한 내용은 4-20 페이지의 기간별 라이센스를 참조하십시오.

4단계 **Update Activation Key**를 클릭합니다.

일부 영구 라이센스의 경우 새 활성화 키를 입력한 후 ASA를 다시 로드해야 합니다. 다시 로드해야 하는 라이센스 목록은 4-33 페이지의 표 4-15를 참조하십시오. 필요한 경우 다시 로드해야 한다는 메시지가 표시됩니다.

공유 라이센스 구성

이 섹션에서는 공유 라이센스 서버 및 참가자를 구성하는 방법을 설명합니다. 공유 라이센스에 대한 자세한 내용은 4-23 페이지의 Shared AnyConnect Premium 라이센스를 참조하십시오.

공유 라이센스 서버 구성

이 섹션에서는 ASA를 공유 라이센스 서버로 구성하는 방법을 설명합니다.

전제 조건

서버에는 공유 라이센스 서버 키가 있어야 합니다.

세부 단계

1단계 **Configuration > Device Management > Licenses > Shared SSL VPN Licenses** 창을 선택합니다.

2단계 Shared Secret 필드에 4~128자의 ASCII 문자열로 된 공유 비밀을 입력합니다.

이 공유 비밀을 보유한 모든 참가자는 라이센스 서버를 사용할 수 있습니다.

3단계 (선택 사항) TCP IP Port 필드에 참가자로부터 SSL 연결을 수신하는 서버에 대한 포트 값을 1~65535 사이로 입력합니다.

기본값은 TCP 포트 50554입니다.

4단계 (선택 사항) Refresh interval 필드에 새로 고침 간격을 10~300초 사이로 입력합니다.

이 값은 참가자에게 제공되어 참가자가 서버와 통신을 수행해야 하는 빈도를 설정할 수 있도록 합니다. 기본값은 30초입니다.

5단계 공유 라이센스 영역을 지원하는 Interfaces에서, 참가자가 서버에 접속하는 모든 인터페이스에 대해 **Shares Licenses** 확인란을 선택합니다.

6단계 (선택 사항) 백업 서버를 식별하려면 Optional backup shared SSL VPN license server 영역에서 다음을 수행합니다.

a. Backup server IP address 필드에 백업 서버 IP 주소를 입력합니다.

b. Primary backup server serial number 필드에 백업 서버 일련 번호를 입력합니다.

c. 백업 서버가 장애 조치 쌍에 포함될 경우, Secondary backup server serial number 필드에서 스탠바이 일련 번호를 식별합니다.

1개의 백업 서버 및 선택적 스탠바이 유닛만 식별할 수 있습니다.

7단계 **Apply**를 클릭합니다.

다음에 할 일

자세한 내용은 4-35 페이지의 공유 라이센스 참가자 및 선택적 백업 서버 구성을(를) 참조하십시오.

공유 라이센스 참가자 및 선택적 백업 서버 구성

이 섹션에서는 공유 라이센스 참가자가 공유 라이센스 서버와 통신을 수행하도록 구성합니다. 또한 이 섹션에서는 선택에 따라 참가자를 백업 서버로 구성하는 방법에 대해서도 설명합니다.

전제 조건

참가자는 공유 라이센스 참가자 키가 있어야 합니다.

세부 단계

1단계 **Configuration > Device Management > Licenses > Shared SSL VPN Licenses** 창을 선택합니다.

2단계 Shared Secret 필드에 4~128자의 ASCII 문자열로 된 공유 비밀을 입력합니다.

3단계 (선택 사항) TCP IP Port 필드에 SSL 연결을 사용하여 서버와 통신을 수행하는 포트 값을 1~65535 사이로 입력합니다.

기본값은 TCP 포트 50554입니다.

4단계 (선택 사항) 참가자를 백업 서버로 식별하려면 Select backup role of participant 영역에서 다음을 수행합니다.

a. **Backup Server** 라디오 버튼을 클릭합니다.

b. 참가자가 백업 서버에 접속하는 모든 인터페이스에 대해 **Shares Licenses** 확인란을 선택합니다.

5단계 **Apply**를 클릭합니다.

라이센스 모니터링

최신 라이센스 보기

이 섹션에서는 최신 라이센스를 확인하는 방법 및 기간별 활성화 키의 경우 라이센스 기간이 얼마나 남았는지 확인하는 방법을 설명합니다.

지침

No Payload Encryption 모델을 보유한 상태에서 라이센스를 보려면 VPN 및 Unified Communications 라이센스가 나열되지 않습니다. 자세한 내용은 4-30 페이지의 No Payload Encryption 모델를 참조하십시오.

세부 단계

1단계 영구 라이센스와 활성화된 모든 기간별 라이센스가 통합된 실행 중인 라이센스를 보려면 **Configuration > Device Management > Licensing > Activation Key** 창을 선택하고 Running Licenses 영역을 봅니다.

다중 컨텍스트 모드의 경우 **Configuration > Device Management > Activation Key** 창을 선택하여 시스템 실행 영역에서 활성화 키를 봅니다.

장애 조치 쌍에 표시되는 실행 중인 라이센스는 기본 및 보조 유닛의 통합된 라이센스입니다. 자세한 내용은 4-28 페이지의 장애 조치 또는 ASA 클러스터 통합 방식를 참조하십시오. 숫자 값이 있는 기간별 라이센스(기간이 통합되지 않음)의 경우, License Duration 열에 기본 또는 보조 유닛의 가장 짧은 기간별 라이센스가 표시됩니다. 라이센스가 만료되면 다른 유닛의 라이센스 기간이 표시됩니다.

2단계 (선택 사항) 라이센스 및 기간이 포함된 기능 같은 기간별 라이센스 세부 정보를 보려면, Time-Based License Keys Installed 영역에서 라이센스 키를 선택하고 **Show License Details**를 클릭합니다.

3단계 (선택 사항) 장애 조치 유닛의 경우, 해당 유닛에 설치된 라이센스(기본 및 보조 유닛의 통합된 라이센스 제외)를 보려면 Running Licenses 영역에서 **Show information of license specifically purchased for this device alone**을 클릭합니다.

공유 라이센스 모니터링

공유 라이센스를 모니터링하려면 **Monitoring > VPN > Clientless SSL VPN > Shared Licenses**.

라이센스의 기능 기록

표 4-16에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 4-16 라이센스의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
연결 및 VLAN 증가	7.0(5)	다음 한도를 높였습니다. • ASA5510 Base 라이센스 연결이 32000에서 5000으로 증가하고, VLAN이 0에서 10으로 증가 • ASA5510 Security Plus 라이센스 연결이 64000에서 130000으로 증가하고, VLAN이 10에서 25으로 증가 • ASA5520 연결이 130000에서 280000으로 증가하고, VLAN이 25에서 100으로 증가 • ASA5540 연결이 280000에서 400000으로 증가하고, VLAN이 100에서 200으로 증가
SSL VPN 라이센스	7.1(1)	SSL VPN 라이센스가 도입되었습니다.
SSL VPN 라이센스 증가	7.2(1)	ASA 5550 이상 버전에 5000-사용자 SSL VPN 라이센스가 도입되었습니다.
ASA 5510의 Base 라이센스 인터페이스 증가	7.2(2)	ASA 5510의 Base 라이센스의 경우, 인터페이스의 최대 수가 3개에서 관리 인터페이스까지 추가하여 무제한 인터페이스로 증가했습니다.
VLAN 증가	7.2(2)	ASA 5505 Security Plus 라이센스의 VLAN 최대 개수를 5개(3개는 전 기능, 1개는 장애 조치, 1개는 백업 인터페이스에 한정)에서 20개 전 기능 인터페이스로 늘렸습니다. 또한 트렁크 포트 수도 1개에서 8개로 늘렸습니다. 현재 전체 기능을 지원하는 인터페이스가 20개이므로 백업 인터페이스 명령을 사용하여 백업 ISP 인터페이스를 비활성화할 필요가 없으며, 여기에 전체 기능을 지원하는 인터페이스를 사용할 수 있습니다. 백업 인터페이스 명령은 Easy 컨피그레이션에서 여전히 유용합니다. ASA 5510의 VLAN 한도도 늘어났습니다. Base 라이센스는 10개에서 50개로, Security Plus 라이센스는 25개에서 100개로 늘어났습니다. ASA 5520은 100개에서 150개로, ASA 5550은 200개에서 250개로 늘어났습니다.
ASA 5510 Security Plus 라이센스의 기가비트 이더넷 지원	7.2(3)	이제 ASA 5510에서는 Security Plus 라이센스와 함께 Ethernet 0/0 및 0/1 포트에 기가비트 이더넷(1000 Mbps)을 지원합니다. Base 라이센스에서는 이를 고속 이더넷(100 Mbps) 포트로 계속 사용할 수 있습니다. Ethernet 0/2, 0/3, 0/4는 두 라이센스에서 모두 고속 이더넷 포트로 유지됩니다. **참고** 인터페이스 이름은 Ethernet 0/0 및 Ethernet 0/1로 유지됩니다.

표 4-16 라이센스의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
Advanced Endpoint Assessment 라이센스	8.0(2)	Advanced Endpoint Assessment 라이센스가 도입되었습니다. Cisco AnyConnect 또는 클라이언트리스 SSL VPN 연결의 완벽한 상태를 지원하기 위해, 방대한 범위로 수집된 안티바이러스 및 안티스파이웨어 애플리케이션, 방화벽, 운영 체제, 관련 업데이트 정보를 원격 컴퓨터에서 검사합니다. 모든 레지스트리 항목, 파일 이름 및 사용자가 지정하는 프로세스 이름까지 검사합니다. 검사 결과는 ASA로 전송됩니다. ASA에서는 사용자 로그인 자격 증명과 컴퓨터 검사 결과를 모두 사용하여 DAP(Dynamic Access Policy)를 할당합니다. Advanced Endpoint Assessment 라이센스를 사용하면 버전 요구 사항을 충족하지 않는 비호환 컴퓨터를 업데이트하도록 구성하여 Host Scan 기능을 개선할 수 있습니다. Cisco에서는 Cisco Secure Desktop과 별개인 Host Scan에서 지원하는 애플리케이션 및 버전 목록의 업데이트를 적시에 패키지로 제공합니다.
ASA 5510을 위한 VPN 로드 밸런싱	8.0(2)	이제 ASA 5510 Security Plus에서 VPN 로드 밸런싱이 지원됩니다.
AnyConnect for Mobile 라이센스	8.0(3)	AnyConnect for Mobile 라이센스가 도입되었습니다. 이 라이센스는 Windows 모바일 디바이스에서 AnyConnect 클라이언트를 사용하여 ASA에 연결할 수 있도록 지원합니다.
기간별 라이센스	8.0(4)/8.1(2)	기간별 라이센스에 대한 지원이 도입되었습니다.
ASA 5580의 VLAN 증가	8.1(2)	ASA 5580에서 지원되는 VLAN 수가 100개에서 250개로 늘어났습니다.
Unified Communications Proxy Sessions 라이센스	8.0(4)	The UC Proxy Sessions 라이센스가 도입되었습니다. 전화 프록시, 프레즌스 페더레이션 프록시, 암호화된 음성 감시 애플리케이션에서는 TLS 프록시 세션을 사용하여 연결을 수행합니다. 각 TLS 프록시 세션의 수는 UC 라이센스 한도를 기준으로 계산됩니다. 이러한 애플리케이션은 UC 프록시를 통해 라이센스가 제공되며, 서로 조합할 수 있습니다. 이 기능은 버전 8.1에는 제공되지 않습니다.
Botnet Traffic Filter 라이센스	8.2(1)	Botnet Traffic Filter 라이센스가 도입되었습니다. Botnet Traffic Filter에서는 알려진 악성 도메인 이름 및 IP 주소에 대한 연결을 추적하여 악성코드 네트워크 활동을 차단합니다.

표 4-16 라이센스의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
AnyConnect Essentials 라이센스	8.2(1)	AnyConnect Essentials 라이센스가 도입되었습니다. 이 라이센스는 AnyConnect VPN 클라이언트가 ASA에 액세스할 수 있도록 지원합니다. 이 라이센스에서는 브라우저 기반 SSL VPN 액세스 또는 Cisco Secure Desktop을 지원하지 않습니다. 이러한 기능의 경우 AnyConnect Essentials 대신 AnyConnect Premium 라이센스를 활성화합니다. **참고** AnyConnect Essentials 라이센스를 이용할 경우 VPN 사용자는 웹 브라우저를 사용하여 로그인하고 AnyConnect 클라이언트를 다운로드 및 시작(WebLaunch)할 수 있습니다. AnyConnect 클라이언트 소프트웨어를 이 라이센스로 활성화하거나 AnyConnect Premium 라이센스로 활성화하는 모든 경우 동일한 클라이언트 기능이 제공됩니다. AnyConnect Essentials 라이센스는 제공된 ASA에서 AnyConnect Premium 라이센스(모든 유형) 또는 Advanced Endpoint Assessment 라이센스와 동시에 활성화될 수 없습니다. 그러나 같은 네트워크의 다른 ASA에서는 AnyConnect Essentials 라이센스와 AnyConnect Premium 라이센스를 실행할 수 있습니다. 기본적으로 ASA에서는 AnyConnect Essentials 라이센스를 사용하지만 Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials 창을 사용하면 이 라이센스를 비활성화하여 다른 라이센스를 사용할 수 있습니다.
SSL VPN 라이센스는 AnyConnect Premium SSL VPN Edition 라이센스로 변경되었습니다.	8.2(1)	SSL VPN 라이센스 이름은 AnyConnect Premium SSL VPN Edition 라이센스로 변경되었습니다.
SSL VPN의 공유 라이센스	8.2(1)	SSL VPN용 공유 라이센스가 도입되었습니다. 여러 ASA에서 필요에 따라 SSL VPN 세션 풀을 공유할 수 있습니다.
Mobility Proxy 애플리케이션에 Unified Communications Proxy 라이센스가 더 이상 필요하지 않습니다.	8.2(2)	Mobility Proxy에 UC Proxy 라이센스가 더 이상 필요하지 않습니다.
SSP-20이 포함된 ASA 5585-X용 10 GE I/O 라이센스	8.2(3)	파이버 포트에 10기가비트 이더넷 속도를 지원하기 위해 SSP-20이 포함된 ASA 5585-X용 10 GE I/O 라이센스를 도입했습니다. SSP-60에서는 기본적으로 10기가비트 이더넷 속도를 지원합니다. **참고** ASA 5585-X는 8.3(x)에서 지원되지 않습니다.
SSP-10이 포함된 ASA 5585-X용 10 GE I/O 라이센스	8.2(4)	파이버 포트에 10기가비트 이더넷 속도를 지원하기 위해 SSP-10이 포함된 ASA 5585-X용 10 GE I/O 라이센스를 도입했습니다. SSP-40에서는 기본적으로 10기가비트 이더넷 속도를 지원합니다. **참고** ASA 5585-X는 8.3(x)에서 지원되지 않습니다.

표 4-16 라이센스의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
동일하지 않은 장애 조치 라이센스	8.3(1)	각 유닛의 장애 조치 라이센스가 더 이상 동일하지 않아도 됩니다. 두 유닛에 사용되는 라이센스는 기본 및 보조 유닛에서 통합된 라이센스입니다. 다음 화면을 수정했습니다. Configuration > Device Management > Licensing > Activation Key.
스태킹 가능한 기간별 라이센스	8.3(1)	기간별 라이센스는 스태킹이 가능합니다. 대부분의 경우 기간별 라이센스를 갱신해야 할 수 있으며, 기존 라이센스에서 새 라이센스로 원활하게 전환할 수 있습니다. 기간별 라이센스에만 제공되는 기능의 경우, 새 라이센스를 적용하려면 그전에 라이센스가 만료되지 않도록 하는 것이 특히 중요합니다. ASA에서는 기간별 라이센스를 스*태킹*할 수 있도록 지원하므로, 새 라이센스를 조기에 설치하여 라이센스가 만료되거나 라이센스의 기간이 짧아지지 않을까 걱정하지 않아도 됩니다.
Intercompany Media Engine 라이센스	8.3(1)	IME 라이센스가 도입되었습니다.
한 번에 여러 기간별 라이센스를 활성화	8.3(1)	이제 여러 기간별 라이센스를 설치할 수 있으며, 기능당 라이센스는 한 번에 하나만 활성화할 수 있습니다. 수정된 화면: Configuration > Device Management > Licensing > Activation Key
기간별 라이센스를 별도로 활성화 및 비활성화	8.3(1)	명령을 사용하여 기간별 라이센스를 활성화하거나 비활성화할 수 있습니다. 수정된 화면: Configuration > Device Management > Licensing > Activation Key
AnyConnect Premium SSL VPN Edition 라이센스가 AnyConnect Premium SSL VPN 라이센스로 변경	8.3(1)	AnyConnect Premium SSL VPN Edition 라이센스 이름이 AnyConnect Premium SSL VPN 라이센스로 변경되었습니다.
수출용 No Payload Encryption 이미지	8.3(2)	ASA 5505~5550 버전에서 No Payload Encryption 소프트웨어를 설치할 경우 Unified Communications, Strong Encryption VPN, Strong Encryption 관리 프로토콜을 비활성화할 수 있습니다. **참고** 이러한 특수 이미지는 8.3(x)에서만 지원됩니다. 8.4(1) 이상 버전에서 No Payload Encryption을 지원하려면 특수 하드웨어 버전의 ASA를 구매해야 합니다.
ASA 5550, 5580, 5585-X 컨텍스트 증가	8.4(1)	SSP-10이 포함된 ASA 5550~ASA 5585-X의 경우, 최대 컨텍스트 수가 50에서 100으로 증가했습니다. SSP-20 이상이 포함된 ASA 5580 및 5585-X의 경우 최대 수가 50에서 250으로 증가했습니다.
ASA 5580 및 5585-X의 VLAN 증가	8.4(1)	ASA 5580 및 5585-X의 최대 VLAN 수가 250에서 1024로 증가했습니다.

표 4-16 라이센스의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
ASA 5580 및 5585-X의 연결 수 증가	8.4(1)	방화벽 연결 제한 증가: • ASA 5580-20 — 1,000,000에서 2,000,000으로 증가 • ASA 5580-40 — 2,000,000에서 4,000,000으로 증가 • ASA 5585-X(SSP-10 포함): 750,000에서 1,000,000으로 증가 • ASA 5585-X(SSP-20 포함): 1,000,000에서 2,000,000으로 증가 • ASA 5585-X(SSP-40 포함): 2,000,000에서 4,000,000으로 증가 • ASA 5585-X(SSP-60 포함): 2,000,000에서 10,000,000으로 증가
AnyConnect Premium SSL VPN 라이센스가 AnyConnect Premium 라이센스로 변경	8.4(1)	AnyConnect Premium SSL VPN 라이센스 이름이 the AnyConnect Premium 라이센스로 변경되었습니다. 라이센스 정보 표시가 “SSL VPN Peers”에서 “AnyConnect Premium Peers”로 변경되었습니다.
ASA 5580의 AnyConnect VPN 세션 수 증가	8.4(1)	AnyConnect VPN 세션 제한이 5,000에서 10,000으로 증가했습니다.
ASA 5580의 기타 VPN 세션 수 증가	8.4(1)	기타 VPN 세션 제한이 5,000에서 10,000으로 증가했습니다.
IKEv2를 사용하는 IPsec 원격 액세스	8.4(1)	IKEv2를 사용하는 IPsec 원격 액세스 VPN이 AnyConnect Essentials 및 AnyConnect Premium 라이센스에 추가되었습니다. **참고** ASA에서 IKEv2를 지원할 경우 다음과 같은 제한 사항이 있습니다. 현재로써는 이중 보안 연결을 지원하지 않습니다. IKEv2 사이트 대 사이트 세션이 다른 VPN 라이센스에 추가되었습니다(이전의 IPsec VPN). 기타 VPN 라이센스는 Base 라이센스에 포함됩니다.
수출용 No Payload Encryption 하드웨어	8.4(1)	No Payload Encryption이 제공되는 모델(예: ASA 5585-X)의 경우, ASA를 특정 국가에 수출하기 위해 ASA 소프트웨어에서는 Unified Communications 및 VPN 기능을 비활성화합니다.
SSP-20 및 SSP-40용 이중 SSP	8.4(2)	SSP-40 및 SSP-60의 경우, 동일한 섀시에서 같은 수준의 SSP 2개를 사용할 수 있습니다. 수준이 혼합된 SSP는 지원되지 않습니다(예: SSP-40이 포함된 SSP-60은 지원되지 않음). 각 SSP는 컨피그레이션 및 관리가 별도로 이루어지는 독립적인 디바이스로서 기능합니다. 원하는 경우 2개의 SSP를 하나의 장애 조치 쌍으로 사용할 수 있습니다. 섀시에 2개의 SSP를 사용할 경우, VPN이 지원되지 않으나, VPN은 비활성화되지 않습니다.
ASA 5512-X~ASA 5555-X용 IPS Module 라이센스	8.6(1)	ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X에서 IPS SSP 소프트웨어 모듈을 사용하려면 IPS 모듈 라이센스가 있어야 합니다.

표 4-16 라이센스의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
ASA 5580 및 ASA 5585-X용 클러스터링 라이센스	9.0(1)	ASA 5580 및 ASA 5585-X용 클러스터링 라이센스가 추가되었습니다.
ASASM에서 VPN 지원	9.0(1)	이제 ASASM에서 모든 VPN 기능을 지원합니다.
ASASM에서 Unified Communications 지원	9.0(1)	이제 ASASM에서는 모든 Unified Communications 기능을 지원합니다.
SSP-10 및 SSP-20(SSP-40 및 SSP-60 포함)에 ASA 5585-X 이중 SSP 지원, 이중 SSP에 VPN 지원	9.0(1)	이제 ASA 5585-X에서는 모든 SSP 모델을 사용하여 이중 SSP를 지원합니다(동일한 섀시에서 같은 수준의 SSP를 2개 사용할 수 있음). 이제 이중 SSP를 사용할 경우 VPN이 지원됩니다.
ASA 5500-X support for clustering	9.1(4)	이제 ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X에서는 2-유닛 클러스터를 지원합니다. 유닛 2개의 클러스터링은 Base 라이센스에서 기본적으로 활성화되어 있으며, ASA 5512-X의 경우 Security Plus 라이센스가 필요합니다.
ASA 5585-X에 클러스터 멤버 16개 지원	9.2(1)	이제 ASA 5585-X에서는 16-유닛 클러스터를 지원합니다.
ASAv 1 vCPU 및 4 vCPU Standard 및 Premium 라이센스 도입	9.2(1)	ASAv에 간단한 라이센스 체계가 도입되었습니다. Standard 또는 Premium 수준에서 1 vCPU 또는 4 vCPU 영구 라이센스를 제공합니다. 추가 라이센스는 제공되지 않습니다.

5 장

투명 또는 라우팅 방화벽 모드

이 장에서는 방화벽 모드를 라우팅 또는 투명 모드로 설정하는 방법 및 각 방화벽 모드에서 방화벽이 어떻게 작동하는지에 대해 설명합니다. 또한 이 장에는 투명 방화벽 작업을 맞춤화하는 방법도 포함되어 있습니다.

다중 컨텍스트 모드의 각 컨텍스트에 방화벽 모드를 개별적으로 설정할 수 있습니다.

방화벽 모드 정보

라우팅 방화벽 모드 정보

라우팅 모드에서 Cisco ASA는 네트워크의 라우터 홉으로 간주합니다. 라우팅 모드에서는 많은 인터페이스를 지원합니다. 각 인터페이스는 다른 서브넷에 있습니다. 컨텍스트 간에 인터페이스를 공유할 수 있습니다.

ASA에서는 연결된 네트워크 간에 라우터로서의 역할을 수행하며, 각 인터페이스에는 다른 서브넷에 있는 IP 주소가 필요합니다. ASA에서는 여러 동적 라우팅 프로토콜을 지원합니다. 그러나 라우팅 수요가 높을 경우 ASA에 의존하는 대신 업스트림 및 다운스트림 라우터의 고급 라우팅 기능을 사용하는 것이 좋습니다.

투명 방화벽 모드 정보

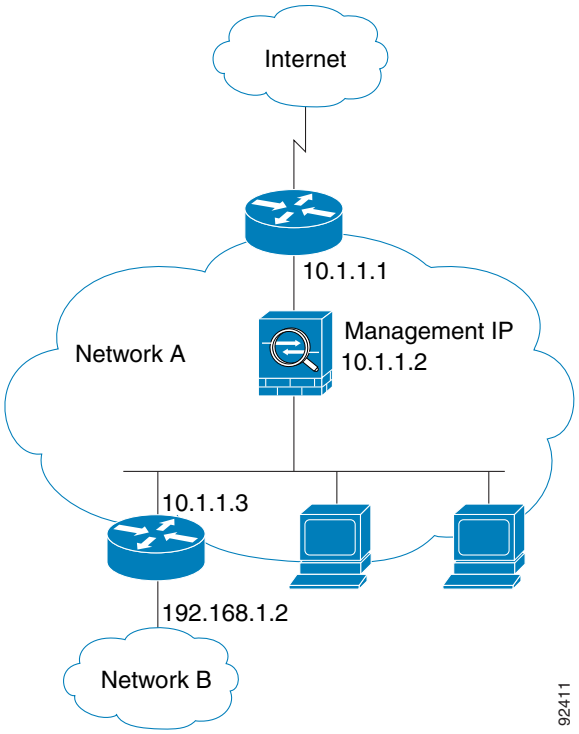
일반적으로 방화벽은 라우팅 홉이며, 해당 스크린드 서브넷 중 하나에 연결되는 호스트의 기본 게이트웨이 역할을 수행합니다. 이와 반대로 투명 방화벽은 “비활성 엔드포인트(bump in the wire)” 또는 “은폐형 방화벽(stealth firewall)” 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

네트워크에서 투명 방화벽 사용

ASA에서는 인터페이스 간의 동일한 네트워크를 연결합니다. 방화벽은 라우팅 홉이 아니므로, 투명 모드를 기존 네트워크에서 쉽게 도입할 수 있습니다.

그림 5-1에는 외부 디바이스가 내부 디바이스와 같은 서브넷에 존재하는 일반적인 투명 방화벽 네트워크가 나와 있습니다. 내부 라우터와 호스트는 외부 라우터에 직접 연결되어 있는 것으로 표시됩니다.

그림 5-1 투명 방어벽 네트워크

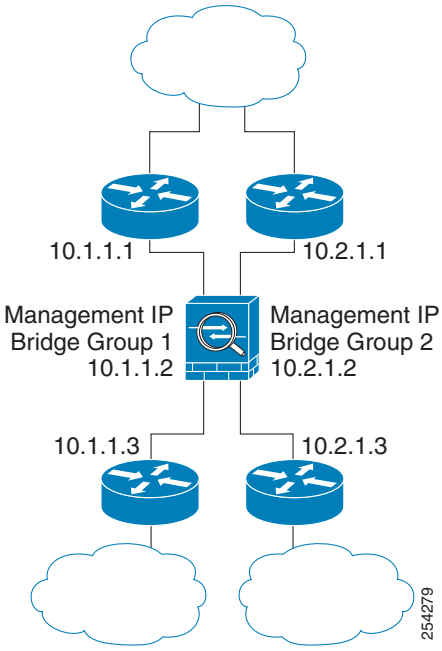


브릿지 그룹

보안 컨텍스트의 오버헤드를 원치 않을 경우 또는 보안 컨텍스트 사용을 극대화하려는 경우, 인터페이스를 하나의 브리지 그룹으로 묶은 다음 네트워크마다 하나씩, 여러 브리지 그룹을 구성할 수 있습니다. 브릿지 그룹 트래픽은 다른 브릿지 그룹과 분리됩니다. 트래픽은 ASA 내의 다른 브릿지 그룹으로 라우팅되지 않으며, 트래픽은 외부 라우터에 의해 ASA의 다른 브릿지 그룹으로 다시 라우팅되기 전에 ASA에서 나가야 합니다. 브리지 기능은 브리지 그룹마다 따로 있지만, 다른 여러 기능은 모든 브리지 그룹이 공유합니다. 예를 들어, 모든 브리지 그룹은 syslog 서버 또는 AAA 서버 컨피그레이션을 공유합니다. 완전한 보안 정책 분리를 위해서는 각 컨텍스트에서 한 브리지 그룹의 보안 컨텍스트를 사용합니다.

그림 5-2에는 2개의 브릿지 그룹이 있는 ASA에 연결된 2개의 네트워크가 나와 있습니다.

그림 5-2 2개의 브릿지 그룹이 있는 투명 방화벽 네트워크



참고 각 브리지 그룹에는 관리 IP 주소가 필요합니다. ASA에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 이 IP 주소를 사용합니다. 관리 IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. 다른 관리 방법에 대해서는 5-4 페이지의 관리 인터페이스(ASA 5512-X 이상)를 참조하십시오.

ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. 관리 IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.

관리 인터페이스(ASA 5512-X 이상)

각 브릿지 그룹 관리 IP 주소 이외에도 브릿지 그룹에 속하지 않은 별도의 관리 *슬롯/포트* 인터페이스를 추가할 수 있으며, 이렇게 하면 ASA에는 관리 트래픽만 허용됩니다. 자세한 내용은 10-2 페이지의 관리 인터페이스를 참조하십시오.

레이어 3 트래픽 허용

- ACL이 없어도 유니캐스트 IPv4 및 IPv6 트래픽이 상위 보안 인터페이스에서 하위 보안 인터페이스까지 투명 방화벽 모드를 자동으로 통과할 수 있습니다.

  참고 액세스 규칙을 사용하여 브로드캐스트 및 멀티캐스트 트래픽을 전달할 수 있습니다. 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

- ACL이 없어도 ARP가 투명 방화벽을 양방향으로 통과할 수 있습니다. ARP 트래픽은 ARP 감시로 제어할 수 있습니다.
- 하위 보안 인터페이스에서 상위 보안 인터페이스로 이동하는 레이어 3 트래픽의 경우, 하위 보안 인터페이스에 확장형 ACL이 필요합니다. 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

허용되는 MAC 주소

아래의 목적지 MAC 주소는 투명 방화벽을 통과할 수 있습니다. 이 목록에 없는 모든 MAC 주소는 손실됩니다.

- FFFF.FFFF.FFFF와 같은 TRUE 브로드캐스트 목적지 MAC 주소
- 0100.5E00.0000에서 0100.5EFE.FFFF 사이의 IPv4 멀티캐스트 MAC 주소
- 3333.0000.0000에서 3333.FFFF.FFFF 사이의 IPv6 멀티캐스트 MAC 주소
- 0100.0CCC.CCCD와 같은 BPDU 멀티캐스트 주소
- 0900.0700.0000에서 0900.07FF.FFFF 사이의 AppleTalk 멀티캐스트 MAC 주소

라우팅 모드에서 허용되지 않는 트래픽 전달

라우팅 모드에서는 일부 트래픽이 ASA를 통과하지 못할 수 있으며 ACL에서 허용한 경우에도 마찬가지입니다. 그러나 투명 방화벽 모드에서는 확장형 ACL(IP 트래픽용) 또는 EtherType ACL(비 IP 트래픽)을 사용하여 거의 모든 트래픽이 통과할 수 있습니다.

EtherType ACL을 사용하여 비 IP 트래픽(예: AppleTalk, IPX, BPDU, MPLS)이 통과되도록 구성할 수 있습니다.

참고 투명 모드 ASA에서는 CDP 패킷 또는 0x600 이상의 유효한 EtherType이 없는 패킷은 전달하지 않습니다. 예외적으로 BPDU 및 IS-IS는 지원됩니다.

라우팅 모드 기능의 트래픽 전달

투명 방화벽에서 직접 지원되지 않는 기능의 경우, 업스트림 및 다운스트림 라우터를 통해 트래픽이 전달되도록 허용하여 해당 기능을 지원할 수 있습니다. 예를 들어, 확장형 ACL을 사용하여 DHCP 트래픽(지원되지 않는 DHCP 릴레이 기능 대신) 또는 IP/TV에서 생성된 멀티캐스트 트래픽을 허용할 수 있습니다. 또한 투명 방화벽을 통해 라우팅 프로토콜 인접성을 설정할 수도 있습니다. 확장형 ACL을 기반으로 OSPF, RIP, EIGRP 또는 BGP 트래픽의 통과를 허용할 수 있습니다. 마찬가지로, HSRP 또는 VRRP 같은 프로토콜이 ASA를 통과할 수 있습니다.

BPDU 처리

Spanning Tree Protocol을 사용하여 루프를 방지하기 위해 기본적으로 BPDU가 전달됩니다. BPDU를 차단하려면 EtherType ACL에서 이를 거부하도록 구성해야 합니다. 장애 조치를 사용할 경우, 토폴로지가 변경될 때 BPDU를 차단하여 스위치 포트가 차단 상태가 되는 것을 방지하고자 할 수 있습니다. 자세한 내용은 8-14 페이지의 투명 방화벽 모드 요구 사항를 참조하십시오.

MAC 주소 조회 및 경로 조회

투명 모드에서 ASA를 실행할 경우, 패킷의 발신 인터페이스는 경로 조회 대신 MAC 주소 조회를 수행하여 결정됩니다.

그러나 다음과 같은 트래픽 유형에는 경로 조회가 필요합니다.

- ASA에서 시작된 트래픽 — syslog 서버가 원격 네트워크에 있을 경우, 고정 경로를 사용하여 ASA가 해당 서브넷에 도달할 수 있도록 해야 합니다.
- NAT가 활성화되어 있고 ASA와 홉 간격이 최소 하나 이상 떨어진 트래픽 — ASA에서는 다음 홉 게이트웨이를 찾기 위해 경로 조회를 수행해야 합니다. 실제 호스트 주소를 위해서는 ASA에 고정 경로를 추가해야 합니다.
- 감시 기능이 활성화되어 있고, ASA와 홉 간격이 최소 하나 이상 떨어진 곳에 엔드포인트가 있는 VoIP(Voice over IP) 및 DNS 트래픽 — 예를 들어, CCM과 H.323 게이트웨이 간에 투명 방화벽을 사용하고 투명 방화벽과 H.323 게이트웨이 간에 라우터가 있을 경우 H.323 게이트웨이에서 호출을 완료하려면 ASA에 고정 경로를 추가해야 합니다. 감시된 트래픽에 NAT를 활성화할 경우, 패킷에 포함된 실제 호스트 주소의 이그레스(egress) 인터페이스를 결정하려면 고정 경로가 필요합니다. 영향을 받는 애플리케이션은 다음과 같습니다.
  - CTIQBE
  - DNS
  - GTP
  - H.323
  - MGCP
  - RTSP
  - SIP
  - Skinny(SCCP)

ARP 감시

기본적으로 모든 ARP 패킷은 ASA를 통과할 수 있습니다. ARP 감시를 활성화하여 ARP 패킷의 흐름을 제어할 수 있습니다.

ARP 감시를 활성화할 경우 ASA에서는 MAC 주소, IP 주소, 모든 ARP 패킷의 소스 인터페이스를 ARP 테이블의 고정 항목과 비교하고 다음과 같은 조치를 취합니다.

- IP 주소, MAC 주소, 소스 인터페이스가 ARP 항목과 일치하면 패킷이 통과됩니다.
- MAC 주소와 IP 주소 또는 인터페이스 간에 불일치하는 항목이 있을 경우 ASA에서는 패킷을 누락시킵니다.
- ARP 패킷이 고정 ARP 테이블의 어느 항목과도 일치하지 않으면 ASA를 설정하여 패킷을 모든 인터페이스로 전달(플러딩)하거나 패킷이 누락되도록 합니다.

참고 전용 관리 인터페이스가 있다면 이 매개변수가 플러딩을 실행하도록 설정된 경우에도 패킷이 플러딩되지 않습니다.

ARP 감시 기능은 악의적인 사용자가 다른 호스트 또는 라우터로 위장(ARP 스푸핑이라고도 함)하는 것을 방지합니다. ARP 스푸핑은 "끼어들기" 공격을 활성화할 수 있습니다. 예를 들어, 호스트에서 ARP 요청을 게이트웨이 라우터에 전송할 경우 해당 게이트웨이 라우터는 게이트웨이 라우터 MAC 주소에 응답합니다. 그러나 공격자는 라우터 MAC 주소가 아닌 공격자 MAC 주소가 포함된 다른 ARP 응답을 호스트에 전송합니다. 이제 공격자는 라우터에 트래픽이 전달되기 전에 모든 호스트 트래픽을 가로챌 수 있게 됩니다.

ARP 감시 기능은 고정 ARP 테이블에 올바른 MAC 주소와 관련 IP 주소를 입력하기만 하면 공격자가 공격자 MAC 주소가 포함된 ARP 응답을 보낼 수 없도록 합니다.

MAC 주소 테이블

ASA에서는 일반적인 브릿지 또는 스위치와 유사한 방식으로 MAC 주소 테이블을 학습하고 구축합니다. 디바이스에서 ASA를 통해 패킷을 전송하면 ASA에서는 MAC 주소를 해당 테이블에 추가합니다. 테이블에서는 MAC 주소와 소스 인터페이스를 연결하므로 ASA에서는 디바이스에 대해 주소가 지정된 모든 패킷을 올바른 인터페이스로 전송할 수 있다는 사실을 파악합니다.

ASA는 방화벽이므로 패킷의 목적지 MAC 주소가 테이블에 없을 경우, 일반적인 브릿지에서는 원래 패킷을 모든 인터페이스에 플러딩하지만 ASA의 경우에는 이러한 작업을 수행하지 않습니다. 그 대신 ASA에서는 직접 연결된 디바이스 또는 원격 디바이스에 다음 패킷을 생성합니다.

- 직접 연결된 디바이스에 대한 패킷 — ASA의 경우 목적지 IP 주소에 대한 ARP 요청을 생성하므로, ASA에서는 어떤 인터페이스에서 ARP 응답을 수신하는지 알 수 있습니다.
- 원격 인터페이스에 대한 패킷 — ASA의 경우 목적지 IP 주소에 대한 Ping을 생성하므로 ASA에서는 어떤 인터페이스에서 Ping 응답을 수신하는지 알 수 있습니다.

원래 패킷은 손실됩니다.

방화벽 모드의 라이센스 요구 사항

다음 표에는 이 기능에 대한 라이센스 요구 사항이 나와 있습니다.

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

기본 설정

기본 모드는 라우팅 모드입니다.

투명 모드 기본값

- 기본적으로 모든 ARP 패킷은 ASA를 통과할 수 있습니다.
- ARP 감시를 활성화할 경우 기본 설정은 불일치 패킷을 플러딩하는 것입니다.
- 동적 MAC 주소 테이블 항목의 기본 시간 제한 값은 5분입니다.
- 기본적으로 각 인터페이스에서는 들어오는 트래픽의 MAC 주소를 자동으로 알게 되며, ASA에서는 해당 항목을 MAC 주소 테이블에 추가합니다.

지침 및 제한 사항

컨텍스트 모드 지침

컨텍스트당 방화벽 모드를 설정합니다.

투명 방화벽 지침

- 투명 방화벽 모드의 경우 관리 인터페이스에서는 MAC 주소 테이블을 데이터 인터페이스와 같은 방식으로 업데이트합니다. 따라서 스위치 포트 중 하나를 라우팅 포트로 구성하지 않는 한 관리 인터페이스와 데이터 인터페이스 두 가지 모두를 같은 스위치에 연결해서는 안 됩니다(기본적으로 Catalyst 스위치에서는 모든 VLAN 스위치 포트에 대한 MAC 주소를 공유함). 그렇지 않을 경우 트래픽이 물리적으로 연결된 스위치에서 관리 인터페이스에 전달되면 ASA에서는 데이터 인터페이스 대신 *관리* 인터페이스를 사용하여 스위치에 액세스하도록 액세스 MAC 주소 테이블을 업데이트합니다. 이 작업으로 인해 일시적인 트래픽 중단이 발생합니다. ASA에서는 보안상의 이유로 인해 스위치에서 데이터 인터페이스로 전달되는 패킷의 MAC 주소 테이블을 최소 30초간 다시 업데이트하지 않습니다.
- 직접 연결된 각 네트워크는 같은 서브넷에 있어야 합니다.
- 브릿지 그룹 관리 IP 주소를 연결된 디바이스의 기본 게이트웨이로 지정하지 마십시오. 디바이스의 경우 ASA의 다른 쪽에 있는 라우터를 기본 게이트웨이로 지정해야 합니다.
- 관리 트래픽의 반환 경로를 제공하는 데 필요한 투명 방화벽의 기본 경로는 단일한 브릿지 그룹 네트워크에서 발생하는 관리 트래픽에만 적용됩니다. 그 이유는 기본 경로에서 브릿지 그룹의 인터페이스 및 브릿지 그룹 네트워크의 라우터 IP 주소를 지정하기 때문이며, 하나의 기본 경로만 정의할 수 있습니다. 관리 트래픽이 여러 개의 브릿지 그룹 네트워크에서 발생할 경우, 관리 트래픽이 발생할 것으로 예상되는 네트워크를 식별하는 고정 경로를 지정해야 합니다.

추가 지침은 13-4 페이지의 투명 모드 인터페이스의 지침 및 제한 사항를 참조하십시오.

IPv6 지침

IPv6를 지원합니다.

추가 지침 및 제한

- 방화벽 모드를 변경할 경우, 다수의 명령이 양쪽 모드에서 모두 지원되지 않으므로 ASA에서는 실행 중인 컨피그레이션을 지웁니다. 시작 컨피그레이션은 변경되지 않고 유지됩니다. 저장하지 않고 다시 로드할 경우 시작 컨피그레이션이 로드되며 모드가 원래 설정으로 다시 전환됩니다. 컨피그레이션 파일에 대한 자세한 내용은 5-9 페이지의 방화벽 모드 설정(단일 모드)를 참조하십시오.
- **firewall transparent** 명령으로 모드를 변경하는 텍스트 컨피그레이션을 ASA에 다운로드할 경우, 컨피그레이션의 맨 위에 해당 명령을 입력해야 합니다. ASA에서는 이 명령을 읽는 즉시 모드를 변경한 다음 다운로드된 컨피그레이션을 계속 읽습니다. 명령이 컨피그레이션의 뒤에 표시될 경우 ASA에서는 컨피그레이션의 앞에 있는 모든 줄을 지웁니다.

투명 모드에서 지원되지 않는 기능

표 5-1에는 투명 모드에서 지원되지 않는 기능이 나와 있습니다.

표 5-1 투명 모드에서 지원되지 않는 기능

기능	설명
동적 DNS	—
DHCP 릴레이	투명 방화벽은 DHCP 서버 역할을 수행할 수 있으나, DHCP 릴레이 명령을 지원하지는 않습니다. 2개의 확장형 ACL을 사용하여 DHCP 트래픽이 통과되도록 할 수 있으므로 DHCP 릴레이가 필요하지 않습니다. 이러한 확장형 ACL 중 하나는 DHCP 요청이 내부 인터페이스에서 외부 인터페이스로 전달되도록 하고, 나머지 하나는 서버의 응답을 다른 방향으로 전달할 수 있도록 합니다.
동적 라우팅 프로토콜	ASA에서 시작된 트래픽에 대한 고정 경로를 추가할 수 있습니다. 또한 확장형 ACL을 사용하여 동적 라우팅 프로토콜이 ASA를 통과하도록 할 수 있습니다.
멀티캐스트 IP 라우팅	확장형 ACL에서 멀티캐스트 트래픽을 허용하여 이러한 트래픽이 ASA를 통과하도록 할 수 있습니다.
QoS	—
통과 트래픽의 VPN 종료	투명 모드에서는 관리 연결에만 사이트 대 사이트 VPN 터널을 지원합니다. 그러나 이로 인해 ASA를 통과하는 트래픽의 VPN 연결이 종료되지는 않습니다. 확장형 ACL을 사용하여 VPN 트래픽이 ASA를 통과하도록 할 수 있으나, 비 관리 연결이 종료되지는 않습니다. 클라이언트리스 SSL VPN이 지원되지 않습니다.
통합 커뮤니케이션	—

방화벽 모드 설정(단일 모드)

이 섹션에서는 CLI를 사용하여 방화벽 모드를 변경하는 방법에 대해 설명합니다. 단일 모드 및 다중 모드에서 현재 연결된 컨텍스트(일반적으로 관리자 컨텍스트)의 경우, ASDM에서 모드를 변경할 수 없습니다. 기타 다중 모드 컨텍스트의 경우에는 ASDM에서 각 컨텍스트에 대한 모드를 설정할 수 있습니다(7-19 페이지의 보안 컨텍스트 구성 참조).

참고 방화벽 모드를 변경하면 실행 중인 컨피그레이션이 지워지므로 다른 컨피그레이션을 수행하기 전에 방화벽 모드를 설정하는 것이 좋습니다.

전제 조건

모드를 변경하면 ASA에서는 실행 중인 컨피그레이션을 지웁니다(자세한 내용은 5-8 페이지의 지침 및 제한 사항 참조).

- 컨피그레이션이 이미 채워져 있는 경우 모드를 변경하기 전에 해당 컨피그레이션을 백업하십시오. 새 컨피그레이션을 생성할 때 이러한 백업을 참조할 수 있습니다.
- 모드를 변경하려면 콘솔 포트에서 CLI를 사용합니다. ASDM Command Line Interface 툴이나 SSH를 비롯한 다른 유형의 세션을 사용할 경우, 컨피그레이션이 지워지면 연결이 끊어지며 콘솔 포트를 사용하여 ASA에 다시 연결해야 합니다.
- 컨텍스트 내에서 모드를 설정합니다.

세부 단계

참고 컨피그레이션이 지워진 후에 방화벽 모드를 투명 모드로 설정하고 ASDM 관리 액세스를 컨피그레이션하려면 2-9 페이지의 Customizing ASDM Access (ASA 5512-X and Higher, ASAv) 또는 2-9 페이지의 Customizing ASDM Access (ASA 5512-X and Higher, ASAv) 를 참조하십시오.

명령	목적
firewall transparent 예: `ciscoasa(config)# firewall transparent`	방화벽 모드를 투명 모드로 설정합니다. 모드를 라우팅 모드로 변경하려면 **no firewall transparent** 명령을 입력합니다. **참고** 방화벽 모드 변경을 확인하는 메시지가 표시되지 않으며, 변경이 즉시 이루어집니다.

투명 방화벽의 ARP 감시 구성

이 섹션에서는 ARP 감시를 구성하는 방법에 대해 설명합니다.

- 5-10 페이지의 ARP 감시 구성의 작업 흐름
- 5-10 페이지의 고정 ARP 항목 추가
- 5-12 페이지의 ARP 감시 활성화

ARP 감시 구성의 작업 흐름

ARP 감시를 구성하려면 다음 단계를 수행합니다.

1단계 5-10 페이지의 고정 ARP 항목 추가에 따라 고정 ARP 항목을 추가합니다. ARP 감시 기능은 ARP 패킷을 ARP 테이블의 고정 ARP 항목과 비교하므로, 이 기능에는 고정 ARP 항목이 필요합니다.

2단계 5-12 페이지의 ARP 감시 활성화에 따라 ARP 감시를 활성화합니다.

고정 ARP 항목 추가

ARP 감시 기능은 ARP 패킷을 ARP 테이블의 고정 ARP 항목과 비교합니다. 호스트에서 IP 주소로 패킷 목적지를 식별하긴 하지만, 이더넷에서 패킷이 실제 전달되는 것은 이더넷 MAC 주소에 달려 있습니다. 라우터 또는 호스트에서 패킷을 직접 연결된 디바이스에 전달하려는 경우, IP 주소와 연관된 MAC 주소를 묻는 ARP 요청이 전송되며 그 후 ARP 응답에 따라 패킷이 MAC 주소에 전달됩니다. 호스트 또는 라우터에서는 ARP 테이블을 보관하므로, 모든 패킷을 전달할 때마다 ARP 요청을 보내지 않아도 됩니다. ARP 테이블은 ARP 응답이 네트워크로 전송될 때마다 동적으로 업데이트되며, 일정 기간 동안 사용되지 않는 항목이 있으면 해당 항목은 시간 제한으로 만료됩니다. 항목이 잘못된 경우(예: 제공된 IP 주소의 MAC 주소가 변경된 경우), 해당 항목은 업데이트되기 전에 시간 제한으로 만료됩니다.

참고 투명 방화벽에서는 ASA로 들어오고 나가는 트래픽(예: 관리 트래픽)에 ARP 테이블의 동적 ARP 항목을 사용합니다.

세부 단계

1단계 **Configuration > Device Management > Advanced > ARP > ARP Static Table** 창을 선택합니다.

2단계 (선택 사항) *동적* ARP 항목의 ARP 시간 제한을 설정하려면 ARP Timeout 필드에 값을 입력합니다.

이 필드에는 ASA에서 ARP 테이블을 재구성하기 전까지 걸리는 시간을 60~4294967초 사이로 설정합니다. 기본값은 14400초입니다. ARP 테이블을 재구성하면 새 호스트 정보가 자동으로 업데이트되고 기존 호스트 정보가 제거됩니다. 호스트 정보는 자주 변경되므로 시간 제한 값을 낮출 수 있습니다.

3단계 (선택 사항, 8.4(5)에만 해당) 비 연결 서브넷을 허용하려면 **Allow non-connected subnets** 확인란을 선택합니다. ASA ARP 캐시에는 기본적으로 직접 연결된 서브넷의 항목만 포함됩니다. ARP 캐시에 직접 연결되지 않은 서브넷도 포함되도록 설정할 수 있습니다. 그러나 보안 위험을 잘 숙지하고 있지 않다면 이 기능은 사용하지 않는 것이 좋습니다. 이 기능은 ASA에 대한 DoS(서비스 거부 시도) 공격을 촉진할 수 있습니다. 즉, 임의의 인터페이스에서 사용자가 다량의 ARP 응답을 전송하고 ASA ARP 테이블에 false 항목이 오버로드되도록 할 수 있습니다.

다음을 사용하는 경우 이 기능을 사용할 수 있습니다.

- 보조 서브넷
- 트래픽 전달을 지원하는 인접 경로의 프록시 ARP

4단계 **Add**를 클릭합니다.

Add ARP Static Configuration 대화 상자가 나타납니다.

5단계 Interface 드롭다운 목록에서 호스트 네트워크에 연결된 인터페이스를 선택합니다.

6단계 IP Address 필드에 호스트의 IP 주소를 입력합니다.

7단계 MAC Address 필드에 호스트의 MAC 주소를 입력합니다(예: 00e0.1e4e.3d8b).

8단계 이 주소의 프록시 ARP를 수행하려면, **Proxy ARP** 확인란을 선택합니다.

지정된 IP 주소의 ARP 요청이 ASA에 수신되면 ASA에서는 지정된 MAC 주소에 응답합니다.

9단계 **OK**를 클릭하고 **Apply**를 클릭합니다.

다음에 할 일

5-12 페이지의 ARP 감시 활성화에 따라 ARP 감시를 활성화합니다.

ARP 감시 활성화

이 섹션에서는 ARP 감시를 활성화하는 방법에 대해 설명합니다.

세부 단계

1단계 **Configuration > Device Management > Advanced > ARP > ARP Inspection** 창을 선택합니다.

2단계 ARP 감시를 활성화하려는 인터페이스 행을 선택하고 **Edit**를 클릭합니다.

Edit ARP Inspection 대화 상자가 나타납니다.

3단계 ARP 감시를 활성화하려면 **Enable ARP Inspection** 확인란을 선택합니다.

4단계 (선택 사항) 불일치 ARP 패킷을 플러딩하려면 **Flood ARP Packets** 확인란을 선택합니다.

기본적으로, 고정 ARP 항목의 모든 요소와 일치하지 않는 패킷은 해당 패킷이 시작된 인터페이스를 제외한 모든 인터페이스에 플러딩됩니다. MAC 주소와 IP 주소 또는 인터페이스 간에 불일치하는 항목이 있을 경우 ASA에서는 패킷을 누락시킵니다.

이 확인란의 선택을 취소하면 모든 불일치 패킷이 누락되며, ASA를 통과하는 ARP가 고정 항목으로만 제한됩니다.

참고 Management 0/0 또는 0/1 인터페이스나 하위 인터페이스가 있을 경우, 이 매개변수가 플러딩을 실행하도록 설정된 경우에도 패킷이 플러딩되지 않습니다.

5단계 **OK**를 클릭하고 **Apply**를 클릭합니다.

투명 방화벽의 MAC 주소 테이블 맞춤화

이 섹션에서는 MAC 주소 테이블을 맞춤화하는 방법에 대해 설명합니다.

- 5-12 페이지의 고정 MAC 주소 추가
- 5-13 페이지의 MAC 주소 파악 비활성화

고정 MAC 주소 추가

일반적으로 MAC 주소는 특정 MAC 주소의 트래픽이 인터페이스에 들어올 때 MAC 주소 테이블에 동적으로 추가됩니다. 원하는 경우 고정 MAC 주소를 MAC 주소 테이블에 추가할 수 있습니다. 고정 항목을 추가함으로써 얻을 수 있는 한 가지 혜택은 MAC 스푸핑을 차단할 수 있다는 점입니다. 동일한 MAC 주소를 고정 항목으로 보유한 클라이언트에서 고정 항목이 일치하지 않는 인터페이스에 트래픽을 전송하려고 시도할 경우, ASA에서는 해당 트래픽을 누락하며 시스템 메시지가 생성됩니다. 고정 ARP 항목을 추가할 경우(5-10 페이지의 고정 ARP 항목 추가 참조), 고정 MAC 주소가 MAC 주소 테이블에 자동으로 추가됩니다.

MAC 주소 테이블에 고정 MAC 주소를 추가하려면 아래 단계를 수행하여 .

1단계 **Configuration > Device Setup > Bridging > MAC Address Table** 창을 선택합니다.

2단계 (선택 사항) MAC 주소 항목이 시간 제한 전까지 MAC 주소 테이블에 유지되는 시간을 설정하려면, Dynamic Entry Timeout 필드에 값을 입력합니다.

이 값의 범위는 5~720분입니다(12시간). 5분이 기본값입니다.

3단계 **Add**를 클릭합니다.

Add MAC Address Entry 대화 상자가 나타납니다.

4단계 Interface Name 드롭다운 목록에서 MAC 주소와 연관된 소스 인터페이스를 선택합니다.

5단계 MAC Address 필드에 MAC 주소를 입력합니다.

6단계 **OK**를 클릭하고 **Apply**를 클릭합니다.

MAC 주소 파악 비활성화

기본적으로 각 인터페이스에서는 들어오는 트래픽의 MAC 주소를 자동으로 알게 되며, ASA에서는 해당 항목을 MAC 주소 테이블에 추가합니다. 원하는 경우 MAC 주소 파악을 비활성화할 수 있으나, 테이블에 MAC 주소를 고정으로 추가하지 않으면 트래픽이 ASA를 통과하여 전달될 수 없습니다.

MAC 주소 파악을 비활성화하려면다음 단계를 수행합니다.

1단계 **Configuration > Device Setup > Bridging > MAC Learning** 창을 선택합니다.

2단계 MAC 파악을 비활성화하려면 인터페이스 행을 선택하고 **Disable**을 클릭합니다.

3단계 MAC 파악을 다시 활성화려면 **Enable**을 클릭합니다.

4단계 **Apply**를 클릭합니다.

방화벽 모드 예

이 섹션에는 트래픽이 어떻게 ASA를 통과하여 이동하는지에 대한 예가 포함되어 있습니다.

- 5-13 페이지의 라우팅 방화벽 모드에서 데이터가 ASA를 통해 이동하는 방식
- 5-19 페이지의 데이터가 투명 방화벽을 통해 이동하는 방식

라우팅 방화벽 모드에서 데이터가 ASA를 통해 이동하는 방식

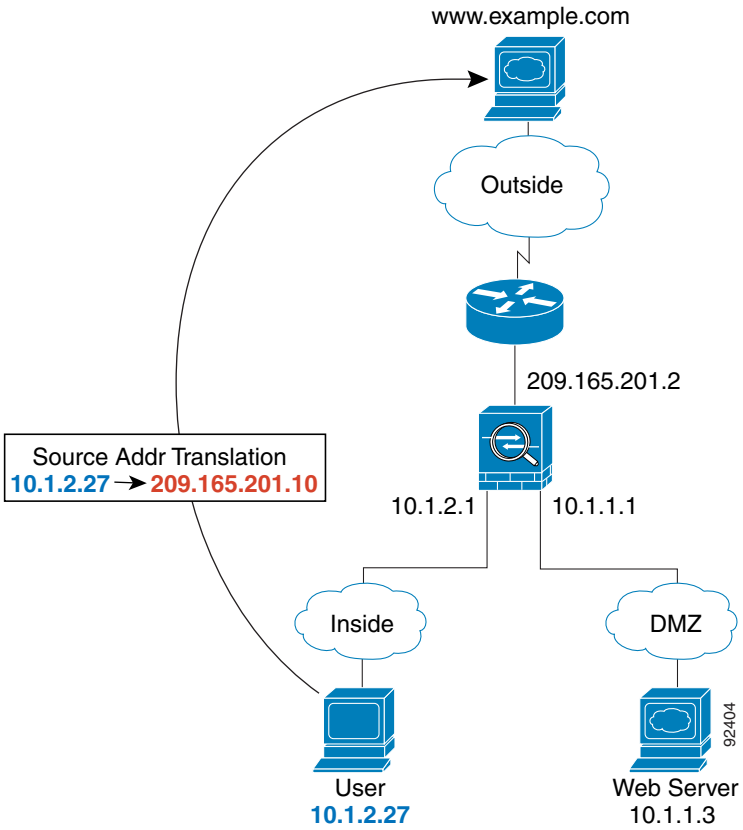
이 섹션에서는 라우팅 방화벽 모드에서 데이터가 ASA를 통과하여 이동하는 방식에 대해 설명합니다.

- 5-14 페이지의 웹 서버를 방문하는 내부 사용자
- 5-15 페이지의 DMZ의 웹 서버를 방문하는 외부 사용자
- 5-16 페이지의 DMZ의 웹 서버를 방문하는 내부 사용자
- 5-17 페이지의 내부 호스트에 액세스를 시도하는 외부 사용자
- 5-18 페이지의 내부 호스트에 액세스를 시도하는 DMZ 사용자

웹 서버를 방문하는 내부 사용자

그림 5-3에는 외부 웹 서버에 액세스하는 내부 사용자의 경우가 나와 있습니다.

그림 5-3 내부 대 외부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-3 참조).

1. 내부 네트워크의 사용자가 www.example.com에서 웹 페이지를 요청합니다.
2. ASA에 패킷이 수신되며 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

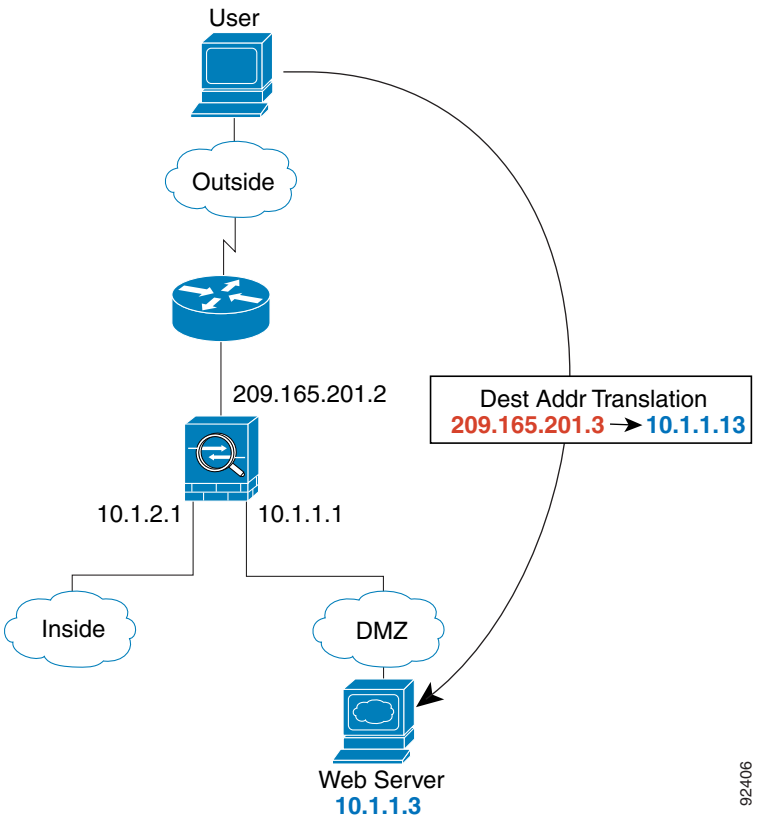
   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. ASA에서는 로컬 소스 주소(10.1.2.27)를 전역 주소(209.165.201.10)로 변환하며 이는 외부 인터페이스 서브넷에 있습니다.

   전역 주소는 모든 서브넷에 있을 수 있지만, 외부 인터페이스 서브넷에 있을 경우 라우팅이 간소화됩니다.
4. 그런 다음 ASA에서는 세션이 설정되었음을 기록하고 외부 인터페이스에서 패킷을 전달합니다.
5. www.example.com에서 요청에 응답할 경우 패킷이 ASA를 통해 이동하며, 세션이 이미 설정되어 있으므로 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회합니다. ASA에서는 전역 목적지 주소를 로컬 사용자 주소인 10.1.2.27로 변환하지 않고 NAT를 수행합니다.
6. ASA에서는 패킷을 내부 사용자에게 전달합니다.

DMZ의 웹 서버를 방문하는 외부 사용자

그림 5-4에는 DMZ 웹 서버에 액세스하는 외부 사용자의 경우가 나와 있습니다.

그림 5-4 외부 대 DMZ



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-4 참조).

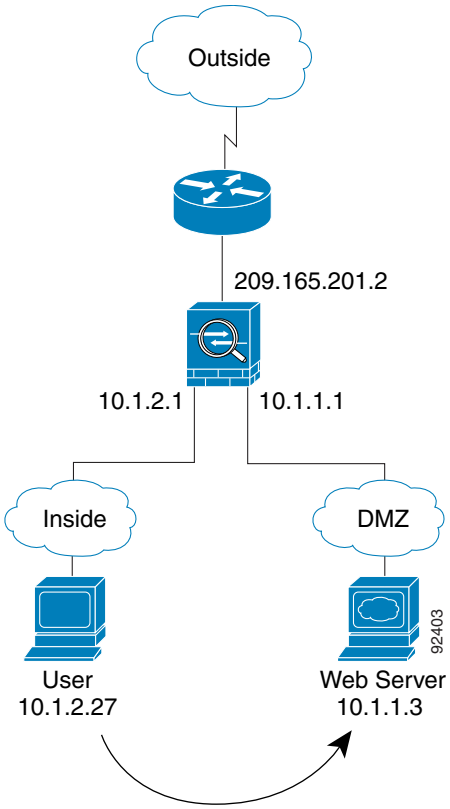
1. 외부 네트워크의 사용자가 외부 인터페이스 서브넷에 있는 전역 목적지 주소(209.165.201.3)를 사용하여 DMZ 웹 서버의 웹 페이지를 요청합니다.
2. ASA에 패킷이 수신되며 목적지 주소가 로컬 주소 10.1.1.3으로 변환되지 않습니다.
3. 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
4. 그런 다음 ASA에서는 세션 항목을 빠른 경로에 추가하고 DMZ 인터페이스에서 패킷을 전달합니다.
5. DMZ 웹 서버에서 요청에 응답할 경우 패킷이 ASA를 통해 이동하며, 세션이 이미 설정되어 있으므로 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회합니다. ASA에서는 로컬 소스 주소를 209.165.201.3으로 전환하여 NAT를 수행합니다.
6. ASA에서는 패킷을 외부 사용자에게 전달합니다.

DMZ의 웹 서버를 방문하는 내부 사용자

그림 5-5에는 DMZ 웹 서버에 액세스하는 내부 사용자의 경우가 나와 있습니다.

그림 5-5 내부 대 DMZ



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-5 참조).

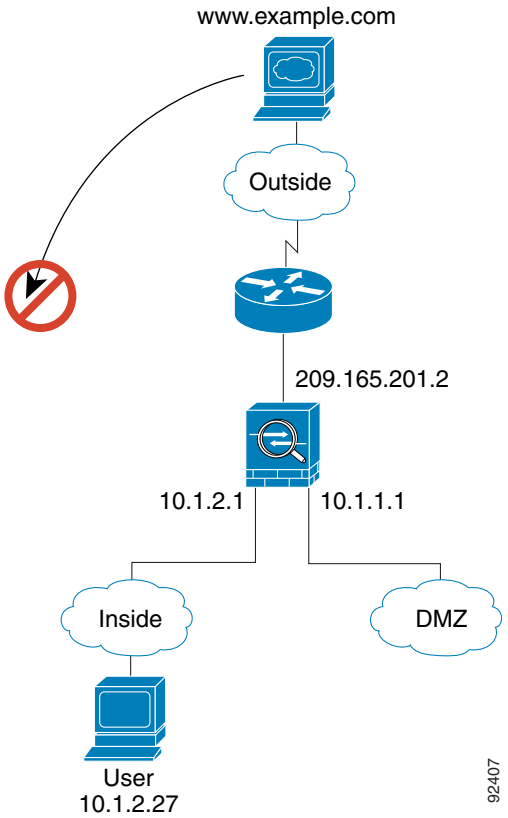
1. 내부 네트워크의 사용자가 목적지 주소(10.1.1.3)를 사용하여 DMZ 웹 서버의 웹 페이지를 요청합니다.
2. ASA에 패킷이 수신되며 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. 그런 다음 ASA에서는 세션이 설정되었음을 기록하고 DMZ 인터페이스에서 패킷을 전달합니다.
4. DMZ 웹 서버에서 요청에 응답할 경우 패킷이 빠른 경로를 통해 이동하며, 이에 따라 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회할 수 있습니다.
5. ASA에서는 패킷을 내부 사용자에게 전달합니다.

내부 호스트에 액세스를 시도하는 외부 사용자

그림 5-6에는 내부 네트워크에 액세스를 시도하는 외부 사용자의 경우가 나와 있습니다.

그림 5-6 외부 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-6 참조).

1. 외부 네트워크의 사용자가 내부 호스트에 연결하기 위해 시도합니다(해당 호스트에 라우팅 가능한 IP 주소가 있는 것으로 가정).

   내부 네트워크에서 사설 주소를 사용할 경우, 외부 사용자는 NAT 없이 내부 네트워크에 연결할 수 없습니다. 외부 사용자는 기존 NAT 세션을 사용하여 내부 사용자에게 연결을 시도하려고 할 수 있습니다.

2. ASA에 패킷이 수신되며 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

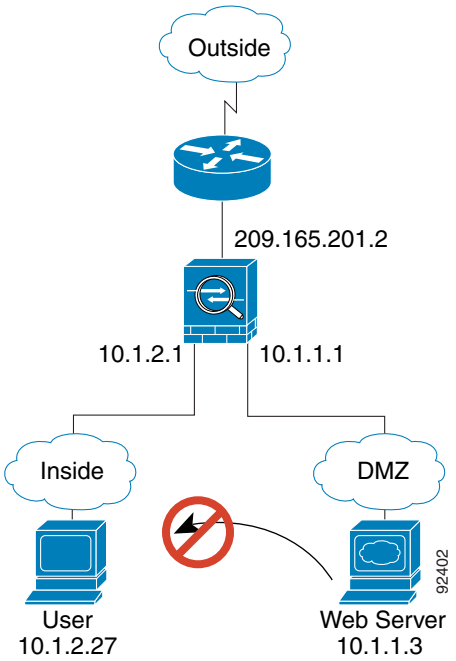
3. 패킷이 거부되며 ASA에서 해당 패킷을 누락시키고 연결 시도를 기록합니다.

   외부 사용자가 내부 네트워크에 공격을 시도할 경우, ASA에서는 다양한 기술을 사용하여 패킷이 기존에 설정된 세션에 사용할 수 있는 유효한 패킷인지 확인합니다.

내부 호스트에 액세스를 시도하는 DMZ 사용자

그림 5-7에는 DMZ 사용자가 내부 네트워크에 액세스를 시도하는 경우가 나와 있습니다.

그림 5-7 DMZ 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-7 참조).

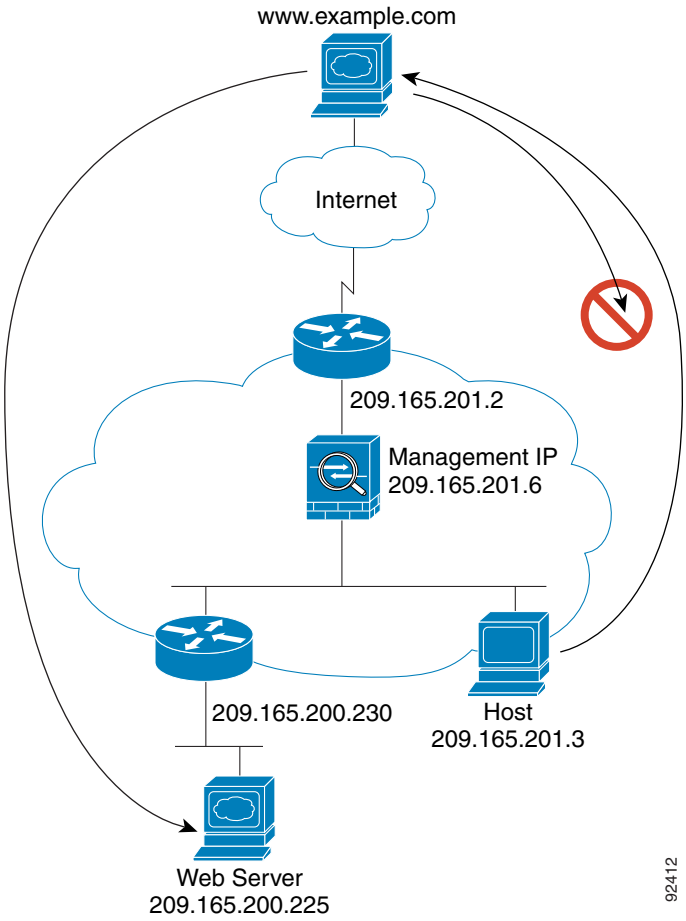
1. DMZ 네트워크 사용자가 내부 호스트에 연결하기 위해 시도합니다. DMZ에서는 인터넷의 트래픽을 라우팅해야 할 필요가 없으므로, 사설 주소 지정 체계로 라우팅을 방지할 수 없습니다.
2. ASA에 패킷이 수신되며 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   패킷이 거부되며 ASA에서 해당 패킷을 누락시키고 연결 시도를 기록합니다.

데이터가 투명 방화벽을 통해 이동하는 방식

그림 5-8에는 공용 웹 서버가 포함된 내부 네트워크에 투명 방화벽을 구현한 일반적인 예가 나와 있습니다. ASA에 액세스 목록이 있으므로 내부 사용자가 인터넷 리소스에 액세스할 수 있습니다. 다른 액세스 목록에서는 외부 사용자가 내부 네트워크의 웹 서버에만 액세스할 수 있도록 합니다.

그림 5-8 일반적인 투명 방화벽 데이터 경로



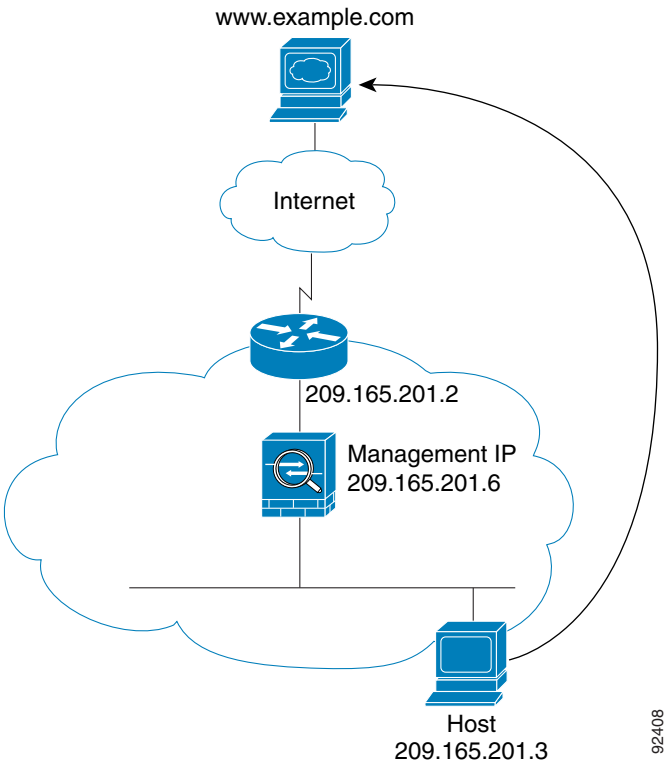
이 섹션에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다.

- 5-20 페이지의 웹 서버를 방문하는 내부 사용자
- 5-21 페이지의 NAT를 사용하여 웹 서버를 방문하는 내부 사용자
- 5-22 페이지의 내부 네트워크의 웹 서버를 방문하는 외부 사용자
- 5-23 페이지의 내부 호스트에 액세스를 시도하는 외부 사용자

웹 서버를 방문하는 내부 사용자

그림 5-9에는 외부 웹 서버에 액세스하는 내부 사용자의 경우가 나와 있습니다.

그림 5-9 내부 대 외부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-9 참조).

1. 내부 네트워크의 사용자가 www.example.com에서 웹 페이지를 요청합니다.
2. ASA에서 패킷을 수신하며 필요한 경우 MAC 주소 테이블에 소스 MAC 주소를 추가합니다. 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

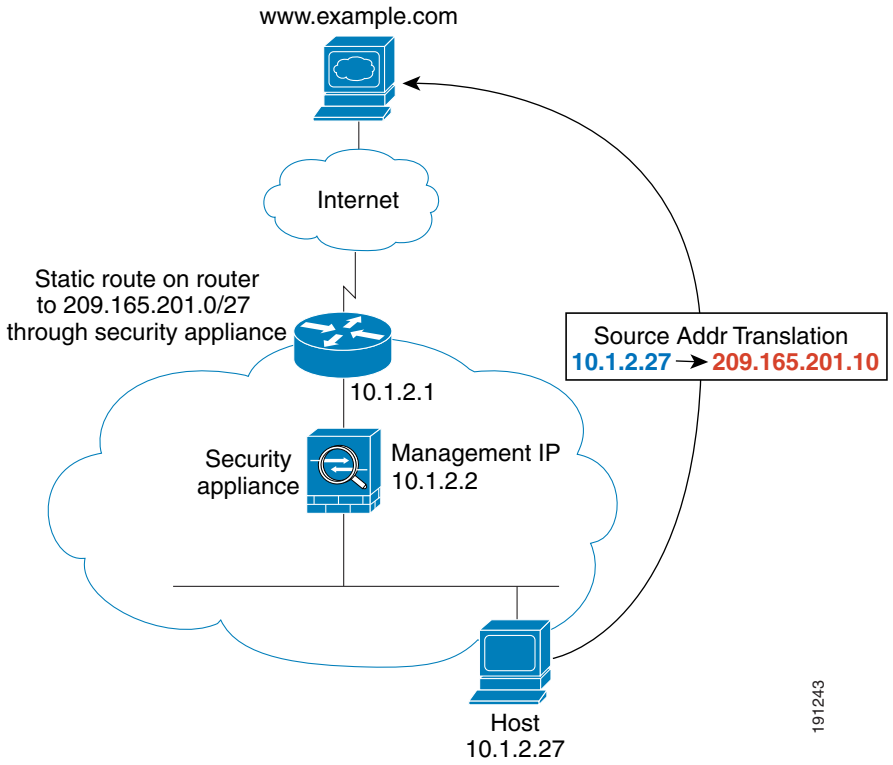
   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. ASA에서는 세션이 설정되었음을 기록합니다.
4. 목적지 MAC 주소가 테이블에 있는 경우 ASA에서는 패킷을 외부 인터페이스에 전달합니다. 목적지 MAC 주소는 업스트림 라우터의 주소이며 209.165.201.2입니다.

   목적지 MAC 주소가 ASA 테이블에 없는 경우, ASA에서는 ARP 요청 또는 Ping을 전송하여 MAC 주소를 찾으려고 합니다. 첫 번째 패킷은 손실됩니다.
5. 웹 서버에서 요청에 응답합니다. 세션이 이미 설정되어 있으므로 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회합니다.
6. ASA에서는 패킷을 내부 사용자에게 전달합니다.

NAT를 사용하여 웹 서버를 방문하는 내부 사용자

그림 5-10에는 외부 웹 서버에 액세스하는 내부 사용자의 경우가 나와 있습니다.

그림 5-10 내부 대 외부(NAT 사용)



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-10 참조).

1. 내부 네트워크의 사용자가 www.example.com에서 웹 페이지를 요청합니다.
2. ASA에서 패킷을 수신하며 필요한 경우 MAC 주소 테이블에 소스 MAC 주소를 추가합니다. 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   다중 컨텍스트 모드의 경우 ASA에서는 우선 고유한 인터페이스에 따라 패킷을 분류합니다.
3. ASA에서는 실제 주소(10.1.2.27)를 매핑된 주소 209.165.201.10으로 변환합니다.

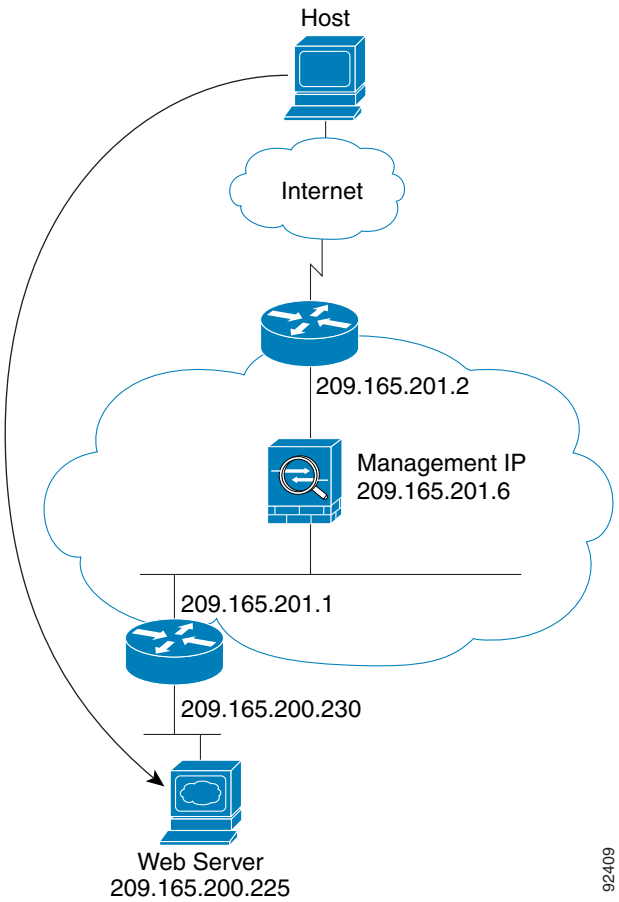
   매핑된 주소는 외부 인터페이스와 같은 네트워크에 있지 않으므로, ASA를 가리키는 매핑된 네트워크에 대한 고정 경로가 업스트림 라우터에 있어야 합니다.
4. 그런 다음 ASA에서는 세션이 설정되었음을 기록하고 외부 인터페이스에서 패킷을 전달합니다.
5. 목적지 MAC 주소가 테이블에 있는 경우 ASA에서는 패킷을 외부 인터페이스에 전달합니다. 목적지 MAC 주소는 업스트림 라우터의 주소이며 10.1.2.1입니다.

   목적지 MAC 주소가 ASA 테이블에 없는 경우, ASA에서는 ARP 요청 및 Ping을 전송하여 MAC 주소를 찾으려고 합니다. 첫 번째 패킷은 손실됩니다.
6. 웹 서버에서 요청에 응답합니다. 세션이 이미 설정되어 있으므로 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회합니다.
7. ASA에서는 매핑된 주소를 실제 주소(10.1.2.27)로 변환하지 않고 NAT를 수행합니다.

내부 네트워크의 웹 서버를 방문하는 외부 사용자

그림 5-11에는 내부 웹 서버에 액세스하는 외부 사용자의 경우가 나와 있습니다.

그림 5-11 외부 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-11 참조).

1. 외부 네트워크의 사용자가 내부 웹 서버의 웹 페이지를 요청합니다.
2. ASA에서 패킷을 수신하며 필요한 경우 MAC 주소 테이블에 소스 MAC 주소를 추가합니다. 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

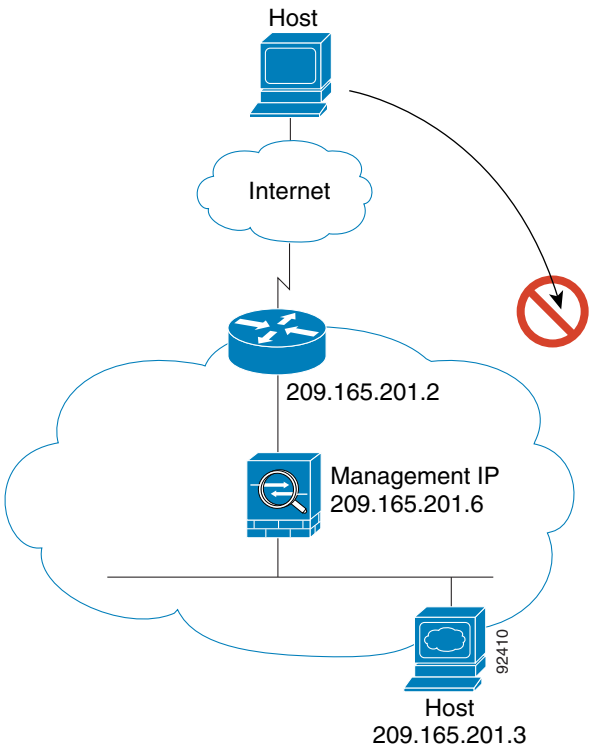
   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. ASA에서는 세션이 설정되었음을 기록합니다.
4. 목적지 MAC 주소가 테이블에 있는 경우 ASA에서는 패킷을 내부 인터페이스에 전달합니다. 목적지 MAC 주소는 업스트림 라우터의 주소이며 209.165.201.1입니다.

   목적지 MAC 주소가 ASA 테이블에 없는 경우, ASA에서는 ARP 요청 및 Ping을 전송하여 MAC 주소를 찾으려고 합니다. 첫 번째 패킷은 손실됩니다.
5. 웹 서버에서 요청에 응답합니다. 세션이 이미 설정되어 있으므로 해당 패킷은 새 연결과 관련된 여러 조회를 거치지 않고 우회합니다.
6. ASA에서는 패킷을 외부 사용자에게 전달합니다.

내부 호스트에 액세스를 시도하는 외부 사용자

그림 5-12에는 내부 네트워크의 호스트에 액세스를 시도하는 외부 사용자의 경우가 나와 있습니다.

그림 5-12 외부 대 내부



다음 단계에서는 데이터가 어떻게 ASA를 통과하여 이동하는지에 대해 설명합니다(그림 5-12 참조).

1. 외부 네트워크 사용자가 내부 호스트에 연결하기 위해 시도합니다.
2. ASA에서 패킷을 수신하며 필요한 경우 MAC 주소 테이블에 소스 MAC 주소를 추가합니다. 이 패킷은 새 세션이므로 ASA에서는 보안 정책(액세스 목록, 필터, AAA)에 따라 해당 패킷을 허용해도 되는지 확인합니다.

   다중 컨텍스트 모드의 경우 ASA에서는 패킷을 컨텍스트에 분류합니다.
3. 외부 호스트를 허용하는 액세스 목록이 없으므로 패킷이 거부되며 ASA에서 패킷을 누락시킵니다.
4. 외부 사용자가 내부 네트워크에 공격을 시도할 경우, ASA에서는 다양한 기술을 사용하여 패킷이 기존에 설정된 세션에 사용할 수 있는 유효한 패킷인지 확인합니다.

방화벽 모드의 기능 기록

표 5-2에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 5-2 방화벽 모드의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
투명 방화벽 모드	7.0(1)	투명 방화벽은 “비활성 엔드포인트(bump in the wire)” 또는 “은폐형 방화벽(stealth firewall)” 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다. 다음 명령을 도입했습니다. **firewall transparent**, **show firewall** ASDM에서는 방화벽 모드를 설정할 수 없으며, 명령줄 인터페이스를 사용해야 합니다.
ARP 감시	7.0(1)	ARP 감시 기능은 모든 ARP 패킷의 MAC 주소, IP 주소, 소스 인터페이스를 ARP 테이블의 고정 항목과 비교합니다. 다음 명령을 도입했습니다. **arp**, **arp-inspection**, **show arp-inspection**
MAC 주소 테이블	7.0(1)	투명 방화벽 모드에서는 MAC 주소 테이블을 사용합니다. 다음 명령을 도입했습니다. **mac-address-table static**, **mac-address-table aging-time**, **mac-learn disable**, **show mac-address-table**
투명 방화벽 브릿지 그룹	8.4(1)	보안 컨텍스트의 오버헤드를 원치 않을 경우 또는 보안 컨텍스트 사용을 극대화하려는 경우, 인터페이스를 하나의 브리지 그룹으로 묶은 다음 네트워크마다 하나씩, 여러 브리지 그룹을 구성할 수 있습니다. 브리지 그룹 트래픽은 다른 브리지 그룹과 분리됩니다. 단일 모드 또는 다중 모드의 컨텍스트당 최대 8개의 브릿지 그룹을 구성할 수 있으며, 브릿지 그룹당 최대 4개의 인터페이스가 포함됩니다. **참고** ASA 5505에서 여러 개의 브릿지 그룹을 구성할 수는 있으나, ASA 5505의 투명 모드에서 데이터 인터페이스가 2개로 제한된다는 것은 실제로 사용 가능한 브릿지 그룹은 1개라는 의미입니다. 다음 화면을 수정하거나 도입했습니다. Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interfaces > Add/Edit Interface

표 5-2 방화벽 모드의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
ARP cache additions for non-connected subnets	8.4(5)/9.1(2)	ASA ARP 캐시에는 기본적으로 직접 연결된 서브넷의 항목만 포함됩니다. ARP 캐시에 직접 연결되지 않은 서브넷도 포함되도록 설정할 수 있습니다. 그러나 보안 위험을 잘 숙지하고 있지 않다면 이 기능은 사용하지 않는 것이 좋습니다. 이 기능은 ASA에 대한 DoS(서비스 거부 시도) 공격을 촉진할 수 있습니다. 즉, 임의의 인터페이스에서 사용자가 다량의 ARP 응답을 전송하고 ASA ARP 테이블에 false 항목이 오버로드되도록 할 수 있습니다. 다음을 사용하는 경우 이 기능을 사용할 수 있습니다. • 보조 서브넷 • 트래픽 전달을 지원하는 인접 경로의 프록시 ARP 다음 화면을 수정했습니다. Configuration > Device Management > Advanced > ARP > ARP Static Table
Mixed firewall mode support in multiple context mode	8.5(1)/9.0(1)	다중 컨텍스트 모드에서 각 보안 컨텍스트에 방화벽 모드를 개별적으로 설정할 수 있으므로, 일부는 투명 모드에서 실행되는 동시에 다른 나머지는 라우팅 모드에서 실행될 수 있습니다. 다음 명령을 수정했습니다. **firewall transparent** 단일 모드의 경우 ASDM에서는 방화벽 모드를 설정할 수 없으며, 명령줄 인터페이스를 사용해야 합니다. 다중 모드에서 수정된 화면: Configuration > Context Management > Security Contexts
투명 모드 브리지 그룹 최대 개수 250개로 증가	9.3(1)	브리지 그룹의 최대 개수가 8개에서 250개로 늘어났습니다. 단일 모드에서 또는 다중 모드의 각 컨텍스트에서 최대 250개의 브리지 그룹을 구성할 수 있으며, 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interfaces > Add/Edit Interface

Startup Wizard

이 장에서는 Cisco ASA의 초기 컨피그레이션을 안내하고 기본 설정을 정의할 수 있도록 지원하는 ASDM Startup Wizard에 대해 설명합니다.

Startup Wizard 액세스

Startup Wizard에 액세스하려면 다음 옵션 중 하나를 선택합니다.

- **Wizards > Startup Wizard**
- **Configuration > Device Setup > Startup Wizard**를 선택하고 **Launch Startup Wizard**를 클릭합니다.

Startup Wizard에 대한 지침

컨텍스트 모드 지침

Startup Wizard는 시스템 컨텍스트에서 지원되지 않습니다.

Startup Wizard 화면

화면의 실제 순서는 지정된 컨피그레이션 선택 사항에 따라 달라집니다. 달리 명시되지 않는 한 각 화면은 모든 모델에서 사용할 수 있습니다.

시작점 또는 시작

- 기존 컨피그레이션을 변경하려면 **Modify existing configuration** 라디오 버튼을 클릭합니다.
- 공장 기본값에 대한 컨피그레이션을 설정하려면 **Reset configuration to factory defaults** 라디오 버튼을 클릭합니다.

– Management 0/0 인터페이스의 IP 주소 및 서브넷 마스크를 기본값(192.168.1.1)과 다르게 구성하려면 **Configure the IP address of the management interface** 확인란을 선택합니다.

참고 컨피그레이션을 공장 기본값으로 재설정할 경우, **Cancel**을 클릭하거나 이 화면을 닫는 방식으로는 이러한 변경 사항의 실행을 취소할 수 없습니다.

다중 컨텍스트 모드에서 이 화면에는 매개변수가 포함되지 않습니다.

기본 구성

이 화면에서 호스트 이름, 도메인 이름 및 enable 비밀번호를 설정합니다.

관련 주제

14-1 페이지의 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정

인터페이스 화면

인터페이스 화면은 선택한 모드 및 모델에 따라 달라집니다.

외부 인터페이스 구성(라우팅 모드)

- 외부 인터페이스(보안 수준이 가장 낮은 인터페이스)의 IP 주소를 구성합니다.
- IPv6 주소를 구성합니다.

관련 주제

- 12-6 페이지의 일반 인터페이스 매개 변수 구성
- 12-13 페이지의 IPv6 주소 지정 구성

외부 인터페이스 구성 - PPPoE(라우팅 모드, 단일 모드)

외부 인터페이스에 대한 PPoE 설정을 구성합니다.

관련 주제

12-10 페이지의 PPPoE IP 주소 및 경로 설정

관리 IP 주소 구성(투명 모드)

IPv4에서는 관리 트래픽과 ASA를 거칠 트래픽 모두 브리지 그룹마다 관리 IP 주소가 필요합니다. 이 화면에서는 BVI 1에 대한 IP 주소를 설정합니다.

관련 주제

13-6 페이지의 브리지 그룹 구성

기타 인터페이스 구성

기타 인터페이스에 대한 매개변수를 구성합니다.

관련 주제

- 12-6 페이지의 일반 인터페이스 매개 변수 구성
- 12-18 페이지의 동일한 보안 레벨 통신 허용

고정 경로

고정 경로를 구성합니다.

관련 주제

20-2 페이지의 고정 경로 구성

DHCP 서버

DHCP 서버를 구성합니다.

관련 주제

15-4 페이지의 DHCP 서버 구성

주소 변환(NAT/PAT)

외부(보안 수준이 가장 낮은 인터페이스)에 액세스할 경우 내부 주소(보안 수준이 가장 높은 인터페이스)의 NAT 또는 PAT를 구성합니다. 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

관리 액세스

- ASDM, 텔넷 또는 SSH 액세스를 구성합니다.
- HTTP 서버에 대한 보안 연결을 활성화하여 ASDM에 액세스하려면 **Enable HTTP server for HTTPS/ASDM access** 확인란을 선택합니다.
- **Enable ASDM history metrics** 확인란을 선택합니다.

관련 주제

- 36-3 페이지의 관리 액세스 구성
- 3-32 페이지의 History Metrics 활성화

IPS 기본 구성

단일 컨텍스트 모드의 경우 ASDM에서 Startup Wizard를 사용하여 기본 IPS 네트워크 컨피그레이션을 컨피그레이션합니다. 이러한 설정은 ASA 컨피그레이션이 아닌 IPS 컨피그레이션에 저장됩니다. 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

ASA CX 기본 구성(ASA 5585-X)

ASDM에서 Startup Wizard를 사용하여 ASA CX 관리 주소 및 Auth Proxy Port를 구성할 수 있습니다. 이러한 설정은 ASA 컨피그레이션이 아닌 ASA CX 컨피그레이션에 저장됩니다. 또한 ASA CX CLI에 추가 네트워크 설정을 설정해야 합니다. 이 화면에 대한 자세한 내용은 방화벽 컨피그레이션 가이드를 참조 하십시오.

ASA FirePOWER 기본 구성

ASDM에서 Startup Wizard를 사용하여 ASA FirePOWER 관리 주소 정보를 구성하고 EULA(최종 사용자 라이센스 계약)를 승인할 수 있습니다. 이러한 설정은 ASA FirePOWER 컨피그레이션이 아닌 ASA 컨피그레이션에 저장됩니다. ASA FirePOWER CLI에서 일부 설정을 구성할 수도 있습니다. 자세한 내용은 방화벽 컨피그레이션 가이드의ASA FirePOWER 모듈에서 해당 장을 참조하십시오.

표준 시간대 및 클록 구성

클록 매개변수를 구성합니다.

관련 주제

14-7 페이지의 날짜 및 시간 설정

자동 업데이트 서버(단일 모드)

- **Enable Auto Update Server for ASA** 확인란을 선택하여 자동 업데이트 서버를 구성합니다.
- IPS 모듈이 있는 경우 **Enable Signature and Engine Updates from Cisco.com** 확인란을 선택합니다. 다음과 같은 추가 매개변수를 설정합니다.
  - Cisco.com 사용자 이름 및 비밀번호를 입력한 다음 비밀번호를 확인합니다.
  - 24시간 클록을 사용하여 시작 시간을 hh:mm:ss 형식으로 입력합니다.

관련 주제

37-28 페이지의 자동 업데이트 구성

Startup Wizard 요약

이 화면에서는 ASA에 대해 적용한 모든 컨피그레이션 설정을 요약합니다.

- 이전 화면의 설정을 변경하려면 **Back**을 클릭합니다.
- 다음 중 하나를 선택합니다.
  - 브라우저에서 Startup Wizard를 직접 실행한 경우, **Finish**를 클릭하면 해당 마법사를 통해 생성한 컨피그레이션 설정이 ASA로 전송되고 플래시 메모리에 자동으로 저장됩니다.
  - ASDM에서 Startup Wizard를 실행한 경우, **File > Save Running Configuration to Flash**를 선택하여 플래시 메모리에 컨피그레이션을 명시적으로 저장해야 합니다.

Startup Wizard의 기록

표 6-1 Startup Wizard의 기록

기능 이름	플랫폼 릴리스	설명
Startup Wizard	7.0(1)	이 마법사가 도입되었습니다. **Wizards > Startup Wizard** 화면을 도입했습니다.
IPS 구성	8.4(1)	IPS 모듈의 경우, **IPS Basic Configuration** 화면이 Startup Wizard에 추가되었습니다. **Auto Update** 화면에는 IPS 모듈의 서명 업데이트도 추가되었습니다. ASA에서 클록이 설정되었는지 확인하기 위해 **Time Zone and Clock Configuration** 화면이 추가되었으며, IPS 모듈의 경우 ASA에서 클록을 가져옵니다. 다음 화면을 도입했거나 수정했습니다. **Wizards > Startup Wizard > IPS Basic Configuration** **Wizards > Startup Wizard > Auto Update** **Wizards > Startup Wizard > Time Zone and Clock Configuration**

파 트 **2**

우수한 가용성 및 확장성

다중 컨텍스트 모드

이 장에서는 Cisco ASA에서 다중 보안 컨텍스트를 구성하는 방법을 설명합니다.

보안 컨텍스트에 대한 정보

단일 ASA를 보안 컨텍스트라고 부르는 여러 가상 디바이스로 분할할 수 있습니다. 각 컨텍스트는 각자 보안 정책, 인터페이스, 관리자가 있는 독립적인 디바이스의 역할을 합니다. 다중 컨텍스트는 여러 대의 독립형 디바이스가 있는 것과 비슷합니다. 다중 컨텍스트 모드에서 지원되지 않는 기능에 대해서는 7-14 페이지의 지침 및 제한 사항를 참조하십시오.

이 섹션에서는 보안 컨텍스트의 개요를 제공합니다.

보안 컨텍스트의 일반적인 용도

다음과 같은 상황에서 다중 보안 컨텍스트를 사용할 수 있습니다.

- 많은 고객에게 보안 서비스를 판매하려는 서비스 공급자라면 ASA에서 다중 보안 컨텍스트를 활성화함으로써 모든 고객의 트래픽을 분리하여 안전하게 지키는, 컨피그레이션하기 용이한 경제적인 공간 절약형 솔루션을 구현할 수 있습니다.
- 각 부서/학과를 완전히 분리된 상태로 유지하려는 대기업 또는 대학 캠퍼스
- 부서별로 각기 다른 보안 정책을 제공하려는 기업
- 둘 이상의 ASA가 필요한 네트워크

컨텍스트 구성 파일

이 섹션에서는 ASA에서 다중 컨텍스트 모드 컨피그레이션을 구현하는 방법을 설명합니다.

- 7-2 페이지의 컨텍스트 구성
- 7-2 페이지의 시스템 구성
- 7-2 페이지의 관리 컨텍스트 구성

컨텍스트 구성

각 컨텍스트에서 ASA는 보안 정책, 인터페이스 그리고 독립형 디바이스에서 컨피그레이션 가능한 모든 옵션을 나타내는 컨피그레이션을 갖추고 있습니다. 컨텍스트 컨피그레이션을 플래시 메모리에 저장하거나 TFTP, FTP 또는 HTTP(S) 서버에서 다운로드할 수 있습니다.

시스템 구성

시스템 관리자는 시스템 컨피그레이션에서 각 컨텍스트 컨피그레이션 위치, 할당된 인터페이스, 기타 컨텍스트 운영 매개 변수를 컨피그레이션함으로써 컨텍스트를 추가하고 관리합니다. 이는 단일 모드 컨피그레이션처럼 시작 컨피그레이션이 됩니다. 시스템 컨피그레이션은 ASA를 위한 기본적인 설정을 나타냅니다. 시스템 컨피그레이션은 자체 네트워크 인터페이스나 네트워크 설정을 포함하지 않습니다. 그보다는 시스템에서 네트워크 리소스에 액세스해야 할 때(예: 서버로부터 컨텍스트 다운로드) *관리 컨텍스트*로 지정된 컨텍스트 중 하나를 사용합니다. 시스템 컨피그레이션은 장애 조치 트래픽만을 위한 전용 장애 조치 인터페이스를 포함합니다.

관리 컨텍스트 구성

관리 컨텍스트는 여느 컨텍스트와 비슷하지만, 사용자가 관리 컨텍스트에 로그인하면 시스템 관리자 권한을 갖게 되어 시스템 및 그 밖의 모든 컨텍스트에 액세스할 수 있다는 점이 다릅니다. 관리 컨텍스트는 어떠한 제한도 받지 않으며, 일반 컨텍스트로 사용될 수 있습니다. 그러나 관리 컨텍스트에 로그인하면 모든 컨텍스트에 대한 관리자 권한이 부여되므로, 관리 컨텍스트 액세스 권한을 적합한 사용자로 한정할 필요가 있습니다. 관리 컨텍스트는 원격 위치가 아닌 플래시 메모리에 항상 있어야 합니다.

시스템이 이미 다중 컨텍스트 모드인 경우 또는 단일 모드에서 전환한 경우, 관리 컨텍스트가 내부 플래시 메모리에 admin.cfg라는 파일로 자동 생성됩니다. 이 컨텍스트의 이름은 “admin”입니다. admin.cfg를 관리 컨텍스트로 사용하고 싶지 않다면 관리 컨텍스트를 변경할 수 있습니다.

ASA의 패킷 분류

ASA에 들어오는 각 패킷은 분류되어야 합니다. 그러면 ASA에서 어떤 컨텍스트에 패킷을 보낼지 판단할 수 있습니다.

- 7-3 페이지의 유효한 분류자 기준
- 7-4 페이지의 분류의 예

참고 목적지 MAC 주소가 멀티캐스트 또는 브로드캐스트 MAC 주소인 경우 패킷이 복제되어 각 컨텍스트에 배포됩니다.

유효한 분류자 기준

이 섹션에서는 분류자에서 사용하는 기준에 대해 설명합니다.

- 7-3 페이지의 고유 인터페이스
- 7-3 페이지의 고유 MAC 주소
- 7-3 페이지의 NAT 구성

참고 인터페이스로 갈 관리 트래픽에서는 인터페이스 IP 주소가 분류에 사용됩니다.

라우팅 테이블은 패킷 분류에 사용되지 않습니다.

고유 인터페이스

단 하나의 컨텍스트가 인그레스 인터페이스와 연결된 경우 ASA는 해당 패킷을 그 컨텍스트로 분류합니다. 투명 방화벽 모드에서는 컨텍스트에 대한 고유 인터페이스가 필요합니다. 따라서 항상 패킷 분류에 이 방법이 사용됩니다.

고유 MAC 주소

여러 컨텍스트에서 하나의 인터페이스를 공유할 경우, 분류자는 각 컨텍스트에서 인터페이스에 할당된 고유 MAC 주소를 사용합니다. 업스트림 라우터는 고유 MAC 주소가 없으면 컨텍스트에 곧바로 라우팅할 수 없습니다. 기본적으로 MAC 주소의 자동 생성이 활성화되어 있습니다. 또한 각 인터페이스를 구성할 때 직접 MAC 주소를 설정할 수도 있습니다.

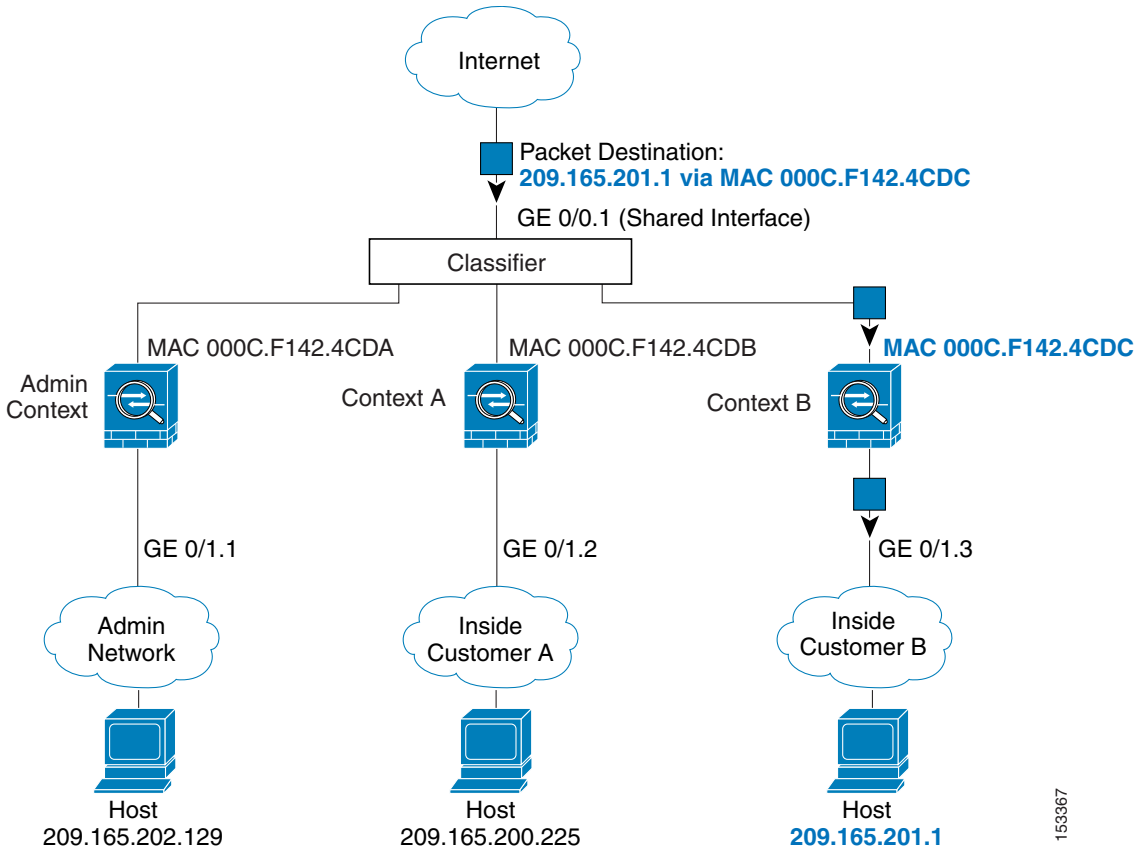
NAT 구성

고유 MAC 주소의 사용을 비활성화한 경우 ASA에서는 NAT 컨피그레이션의 매핑된 주소를 사용하여 패킷을 분류합니다. NAT 대신 MAC 주소를 사용하는 것이 좋습니다. 그러면 NAT 컨피그레이션의 완전성과 상관없이 트래픽 분류가 가능해집니다.

분류의 예

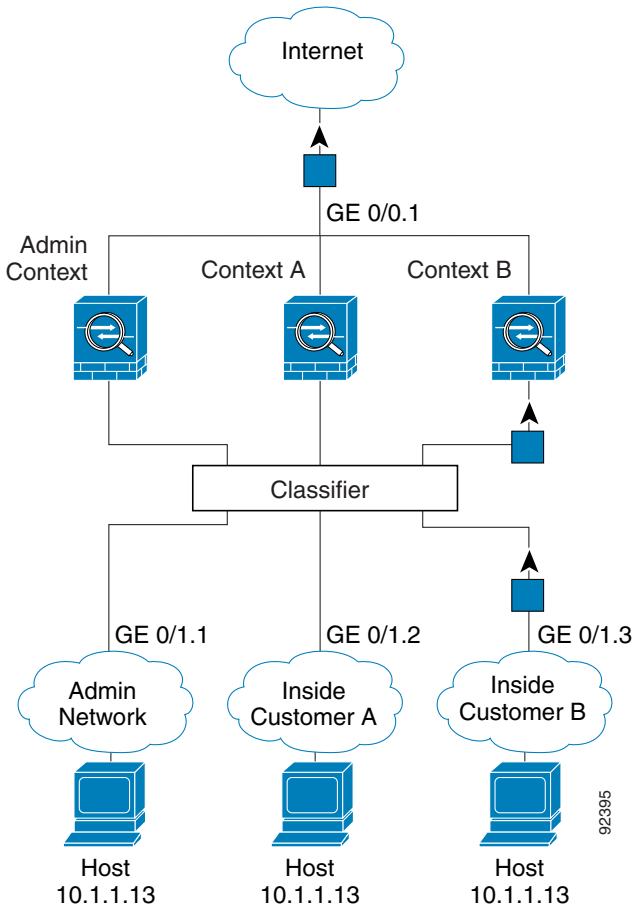
그림 7-1에서는 다중 컨텍스트가 외부 인터페이스는 공유하는 것을 보여줍니다. 분류자는 컨텍스트 B에 패킷을 지정합니다. 컨텍스트 B가 라우터에서 패킷을 보내는 패킷을 수신하는 MAC 주소를 포함하기 때문입니다.

그림 7-1 MAC 주소를 사용하는 공유 인터페이스를 통한 패킷 분류



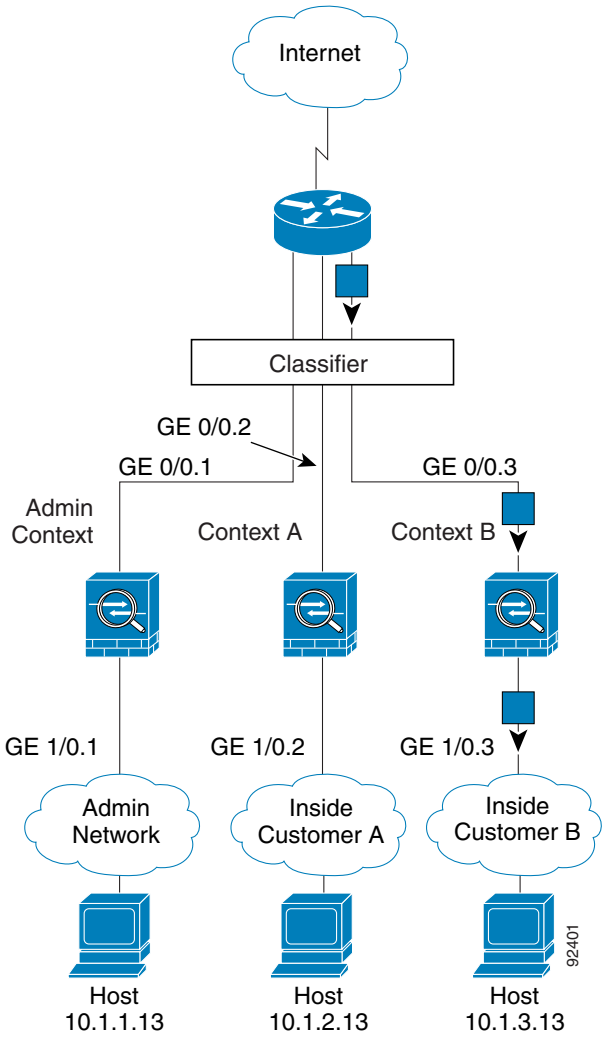
내부 네트워크에서 보낸 것을 비롯하여 모든 신규 수신 트래픽은 분류되어야 합니다. 그림 7-2에서는 인터넷에 액세스하는 컨텍스트 B 내부 네트워크의 호스트를 보여줍니다. 분류자는 컨텍스트 B에 패킷을 지정합니다. 인그레스 인터페이스가 컨텍스트 B에 지정되는 기가비트 이더넷 0/1.3이기 때문입니다.

그림 7-2 내부 네트워크에서 보내는 수신 트래픽



투명 방화벽의 경우 고유한 인터페이스를 사용해야 합니다. 그림 7-3에서는 인터넷에서 컨텍스트 B 내부 네트워크의 호스트로 갈 패킷을 보여줍니다. 분류자는 컨텍스트 B에 패킷을 지정합니다. 인그레스 인터페이스가 컨텍스트 B에 지정되는 기가비트 이더넷 1/0.3이기 때문입니다.

그림 7-3 투명 방화벽 컨텍스트



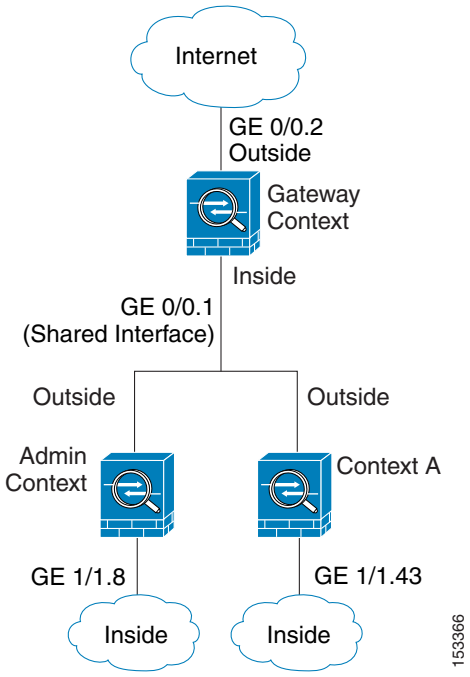
보안 컨텍스트 캐스케이딩

어떤 컨텍스트의 바로 앞에 다른 컨텍스트를 놓는 것을 *컨텍스트 캐스케이딩*이라고 합니다. 한 컨텍스트의 외부 인터페이스가 다른 컨텍스트의 내부 인터페이스가 됩니다. 최상위 컨텍스트에서 공유 매개 변수를 컨피그레이션함으로써 일부 컨텍스트의 컨피그레이션을 간소화하고 싶다면 컨텍스트 캐스케이딩이 유용할 수 있습니다.

참고 컨텍스트를 캐스케이딩하려면 컨텍스트 인터페이스별로 고유한 MAC 주소가 필요합니다(기본 설정). MAC 주소 없이 공유 인터페이스에서 패킷을 분류하면 여러 제약이 따라므로, 고유한 MAC 주소 없이 컨텍스트를 캐스케이딩하는 것은 권장되지 않습니다.

그림 7-4에서는 2개의 컨텍스트가 게이트웨이의 뒤에 있는 게이트웨이 컨텍스트를 보여줍니다.

그림 7-4 컨텍스트 캐스케이딩



보안 컨텍스트에 대한 관리 액세스

ASA에서는 다중 컨텍스트 모드에서 시스템 관리자 액세스를 제공할 뿐만 아니라 개별 컨텍스트 관리자를 위한 액세스도 제공합니다. 다음 섹션에서는 시스템 관리자나 컨텍스트 관리자로 로그인하는 것에 대해 설명합니다.

- 7-7 페이지의 시스템 관리자 액세스
- 7-8 페이지의 컨텍스트 관리자 액세스

시스템 관리자 액세스

2가지 방법으로 ASA에 시스템 관리자로 액세스할 수 있습니다.

- ASA 콘솔에 액세스합니다.

  콘솔에서 *시스템 실행 영역*에 액세스합니다. 여기서 입력하는 모든 명령은 시스템 컨피그레이션 또는 (런타임 명령의 경우) 시스템 실행에만 영향을 줍니다.

- 텔넷, SSH 또는 ASDM을 사용하여 관리 컨텍스트에 액세스합니다.

  텔넷, SSH, ASDM 액세스를 활성화하려면 36 장, “관리 액세스”,를 참조하십시오.

시스템 관리자로서 모든 컨텍스트에 액세스할 수 있습니다.

관리 또는 시스템에서 어떤 컨텍스트로 전환하면 사용자 이름이 기본 이름인 “enable_15”로 바뀝니다. 그 컨텍스트에서 명령 권한 부여를 구성한 경우 “enable_15” 사용자에 대해 권한을 구성해야 합니다. 혹은 충분한 권한을 부여한 다른 이름으로 로그인할 수도 있습니다. 새 사용자 이름으로 로그인하려면 **login** 명령을 입력합니다. 예를 들어, 사용자 이름 “admin”으로 관리 컨텍스트에 로그인합니다. 관리 컨텍스트는 어떤 명령 권한 부여 컨피그레이션도 없지만, 다른 모든 컨텍스트에 명령 권한 부여가 있습니다. 편의를 위해 각 컨텍스트 컨피그레이션에는 최대 권한을 가진 “admin” 사용자가 있습니다. 관리 컨텍스트에서 컨텍스트 A로 전환하면 사용자 이름이 enable_15로 바뀌므로, **login** 명령을 입력하여 다시 "admin"으로 로그인해야 합니다. 컨텍스트 B로 전환했으면 다시 **login** 명령을 입력하여 "admin"으로 로그인해야 합니다.

시스템 실행 영역은 AAA 명령을 지원하지 않으므로, 로컬 데이터베이스에 자체 enable 비밀번호와 사용자 이름을 구성하여 개별 로그인을 제공할 수 있습니다.

컨텍스트 관리자 액세스

텔넷, SSH 또는 ASDM을 사용하여 컨텍스트에 액세스할 수 있습니다. 비 admin 컨텍스트로 로그인한 경우 그 컨텍스트의 컨피그레이션만 액세스 가능합니다. 컨텍스트에 개별 로그인을 제공할 수 있습니다. 텔넷, SSH, ASDM 액세스를 활성화하고 관리 인증을 구성하려면 36 장, “관리 액세스”,를 참조하십시오.

리소스 관리에 대한 정보

기본적으로 모든 보안 컨텍스트는 컨텍스트별 최대 제한이 적용되는 경우는 제외하고 ASA의 리소스에 무제한으로 액세스할 수 있습니다. 유일한 예외가 VPN 리소스인데, 이는 기본적으로 비활성화되어 있습니다. 하나 이상의 컨텍스트에서 너무 많은 리소스를 사용하고 있으며 그로 인해 다른 컨텍스트의 연결이 거부되는 것과 같은 상황이 벌어진다면, 컨텍스트별 리소스 사용을 제한하는 리소스 관리를 구성할 수 있습니다. VPN 리소스의 경우 임의의 VPN 터널을 허용하도록 리소스 관리를 구성해야 합니다.

리소스 클래스

ASA에서는 컨텍스트를 리소스 클래스에 지정하는 방법으로 리소스를 관리합니다. 각 컨텍스트는 해당 클래스에서 설정한 리소스 제한을 적용합니다. 어떤 클래스의 설정을 사용하려면 컨텍스트를 정의할 때 해당 클래스에 컨텍스트를 지정합니다. 모든 컨텍스트는 별도의 클래스에 지정되지 않는 한 기본 클래스에 속해 있습니다. 직접 기본 클래스에 컨텍스트를 지정할 필요는 없습니다. 하나의 컨텍스트는 하나의 리소스 클래스에만 지정할 수 있습니다. 이 규칙의 예외는 멤버 클래스에 정의되지 않은 제한이 기본 클래스로부터 상속되는 것입니다. 즉 컨텍스트는 기본 클래스와 또 다른 클래스의 멤버가 될 수 있습니다.

리소스 제한

개별 리소스에 대한 제한을 백분율(명시적 시스템 제한이 있는 경우) 또는 절대값으로 설정할 수 있습니다.

대부분의 리소스는 ASA에서 클래스에 지정된 컨텍스트 각각에 리소스의 일부를 따로 배정하지 않습니다. 그보다는 ASA에서 컨텍스트의 최대 제한을 설정합니다. 리소스를 오버서브스크립션하거나 일부 리소스가 무제한이 되는 것을 허용할 경우, 몇몇 컨텍스트에서 이 리소스를 "소진"하여 다른 컨텍스트에 대한 서비스에 영향을 줄 수 있습니다. 오버서브스크립션할 수 없는 VPN 리소스 유형은 예외입니다. 즉, 각 컨텍스트에 할당된 리소스가 보장됩니다. VPN 세션이 일시적으로 급증하여 할당량을 넘어서는 상황에 대비하여 ASA는 "버스트(burst)" VPN 리소스 유형을 지원합니다. 이는 할당되지 않은 나머지 VPN 세션과 같습니다. 버스트 세션은 오버서브스크립션될 수 *있으며*, 선착순으로 컨텍스트에 제공됩니다.

기본 클래스

모든 컨텍스트는 별도의 클래스에 지정되지 않는 한 기본 클래스에 속해 있습니다. 직접 기본 클래스에 컨텍스트를 지정할 필요는 없습니다.

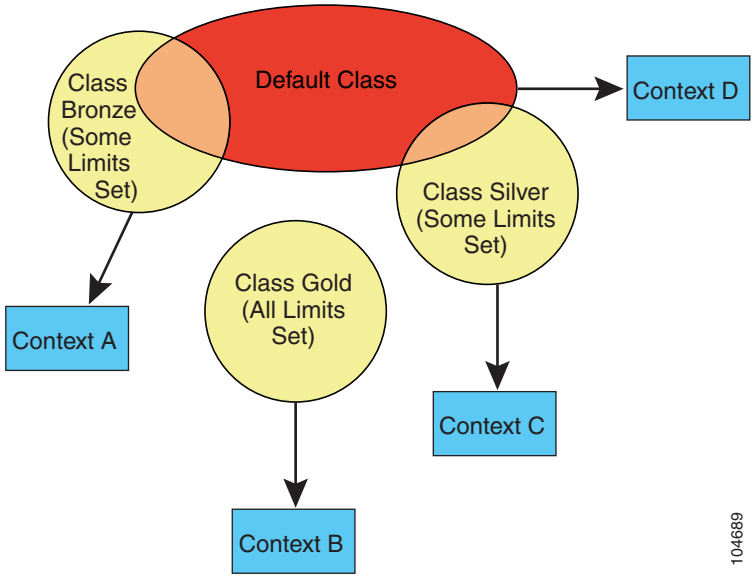
어떤 컨텍스트가 기본 클래스가 아닌 클래스에 속할 경우, 항상 이 클래스의 설정이 기본 클래스의 설정에 우선합니다. 그러나 그 클래스에서 어떤 설정이 정의되지 않았다면 멤버 컨텍스트는 기본 클래스의 해당 제한을 적용합니다. 예를 들어, 모든 동시 연결에 대한 2% 제한이 있지만 그 밖의 어떤 제한도 없는 클래스를 만든다면 그 밖의 제한은 기본 클래스로부터 상속됩니다. 이와 달리 모든 리소스에 대해 제한이 있는 클래스를 만들 경우 이 클래스는 기본 클래스의 어떤 설정도 사용하지 않습니다.

대부분의 리소스에서 기본 클래스는 다음 제한을 제외하고 모든 컨텍스트에 무제한적인 리소스 액세스를 제공합니다.

- 텔넷 세션—5개 세션 (컨텍스트당 최대 제한)
- SSH 세션—5개 세션 (컨텍스트당 최대 제한)
- IPsec 세션—5개 세션 (컨텍스트당 최대 제한)
- MAC 주소—65,535개 항목 (컨텍스트당 최대 제한)
- VPN 사이트 대 사이트 터널—0개 세션 (VPN 세션을 허용하려면 직접 클래스를 구성해야 함)

그림 7-5에서는 기본 클래스와 다른 클래스의 관계를 보여줍니다. 컨텍스트 A와 C는 몇 가지 제한이 설정된 클래스에 속해 있습니다. 다른 제한은 기본 클래스로부터 상속됩니다. 컨텍스트 B는 기본 클래스에서 어떤 제한도 상속하지 않습니다. 모든 제한이 설정되어 있는 Gold 클래스에 속해 있기 때문입니다. 컨텍스트 D는 클래스에 지정되지 않았으므로, 기본적으로 기본 클래스의 멤버입니다.

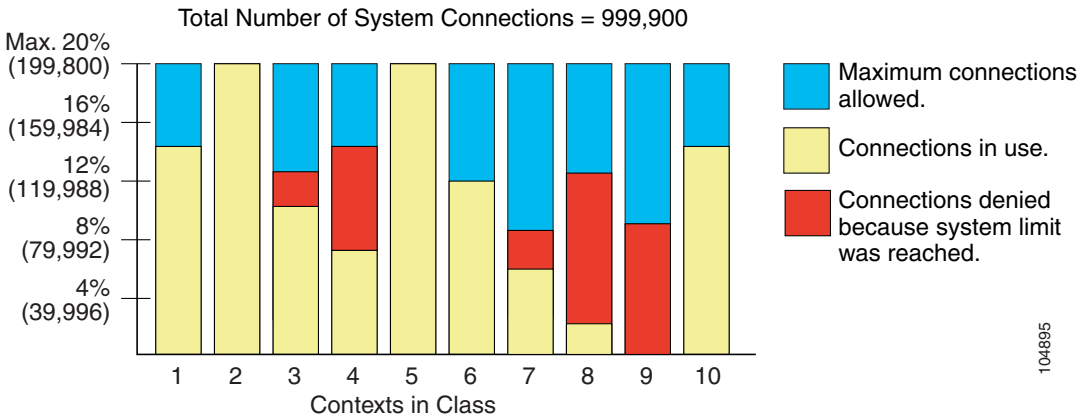
그림 7-5 리소스 클래스



오버서브스크립션된 리소스 사용

모든 컨텍스트를 통틀어 100%가 넘는 리소스를 할당함으로서 ASA를 오버서브스크립션할 수 있습니다(비 버스트 VPN 리소스는 제외). 이를테면 컨텍스트당 20%로 연결을 제한하도록 Bronze 클래스를 설정한 다음 이 클래스에 10개의 컨텍스트를 지정하여 총 200%가 되게 할 수 있습니다. 컨텍스트가 동시에 시스템 제한을 초과하여 사용할 경우 각 컨텍스트는 원래 의도했던 20%보다 적게 받습니다. 그림 7-6를 참조하십시오.

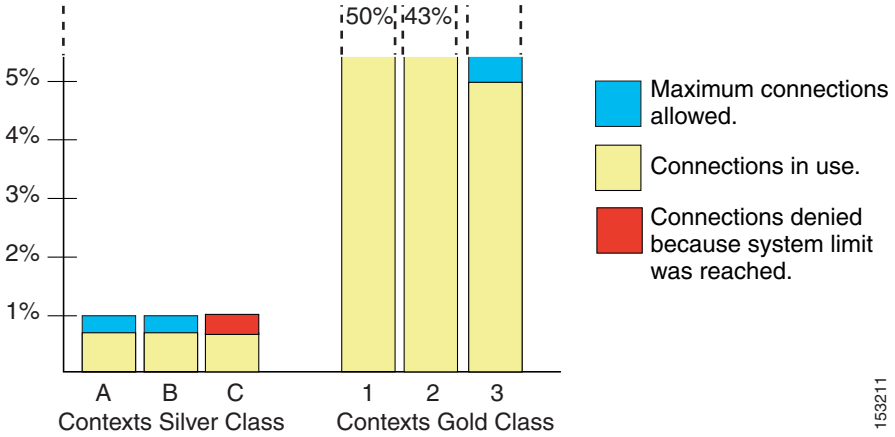
그림 7-6 리소스 오버서브스크립션



무제한 리소스 사용

ASA에서는 클래스의 하나 이상의 리소스에 대해 백분율이나 절대값이 아닌 무제한 액세스를 지정할 수 있습니다. 어떤 리소스가 무제한이 되면 컨텍스트는 시스템의 가용 제한에서 그 리소스를 최대한 많이 사용할 수 있습니다. 이를테면 컨텍스트 A, B, C는 Silver 클래스인데, 이 클래스는 각 멤버를 연결의 1%로 제한하므로 총 3%가 됩니다. 그러나 이 세 컨텍스트는 현재 모두 합쳐 2%만 사용하고 있습니다. Gold 클래스는 무제한으로 연결에 액세스합니다. Gold 클래스의 컨텍스트는 "할당되지 않은" 연결을 97% 넘게 사용할 수 있습니다. 또한 현재 컨텍스트 A, B, C에서 사용하지 않는 1% 연결도 사용 가능합니다. 그러면 컨텍스트 A, B, C는 주어진 제한(총 3%)만큼 사용할 수 없게 됩니다. (그림 7-7 참조) 무제한 액세스 설정은 ASA의 오버서브스크립션과 비슷하지만, 시스템의 오버서브스크립션 용량을 그만큼 제어하지는 않습니다.

그림 7-7 무제한 리소스



MAC 주소에 대한 정보

컨텍스트에서 인터페이스를 공유할 수 있도록 ASA에서는 기본적으로 각 공유 컨텍스트 인터페이스에 가상 MAC 주소를 부여합니다. 자동 생성을 사용자 지정하거나 비활성화하려면 7-23 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정를 참조하십시오.

이 MAC 주소는 컨텍스트 내에서 패킷을 분류하는 데 사용됩니다. 어떤 인터페이스를 공유하지만 각 컨텍스트에서 그 인터페이스에 대한 고유한 MAC 주소가 없을 경우, 다른 분류 방법을 시도하는데 전 범위를 포괄하지 못할 수도 있습니다. 패킷 분류에 대한 자세한 내용은 7-3 페이지의 ASA의 패킷 분류를 참조하십시오.

드물지만, 생성된 MAC 주소가 네트워크의 다른 사설 MAC 주소와 충돌할 경우 컨텍스트 내에서 그 인터페이스의 MAC 주소를 직접 설정할 수 있습니다. MAC 주소를 직접 설정하려면 12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성를 참조하십시오.

기본 MAC 주소

(8.5(1.7) 이상) 자동 MAC 주소 생성은 기본적으로 활성화되어 있습니다. ASA는 인터페이스의 마지막 2바이트(ASA 5500-X) 또는 백플레인(ASASM) MAC 주소를 기반으로 접두사를 자동 생성합니다. 원한다면 접두사를 사용자 지정할 수 있습니다.

MAC 주소 생성을 비활성화한 경우 다음 기본 MAC 주소를 참조하십시오.

- ASA 5500-X 시리즈 어플라이언스—물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.
- ASASM—모든 VLAN 인터페이스가 백플레인 MAC 주소에서 파생된 동일한 MAC 주소를 사용합니다.

7-12 페이지의 MAC 주소 형식도 참조하십시오.

참고 (8.5(1.6) 이하) 장애 조치 쌍을 위한 히트리스(hitless) 업그레이드를 유지하고자 ASA는 장애 조치가 활성화된 경우 다시 로드할 때 기존 레거시 자동 생성 컨피그레이션을 변환하지 않습니다. 그러나 특히 ASASM에서는 장애 조치를 사용할 때 직접 접두사 생성 방법으로 바꾸는 것이 좋습니다. 접두사 방법을 사용하지 않으면 서로 다른 슬롯 번호에 설치된 ASASM에서 장애 조치 시 MAC 주소가 바뀌어 트래픽이 중단될 수 있습니다. 업그레이드한 다음 MAC 주소 생성에 접두사 방법을 사용하려면 MAC 주소 자동 생성에서 다시 접두사를 사용할 수 있게 합니다. 레거시 방법에 대한 자세한 내용은 명령 참조에서 **mac-address auto** 명령을 참조하십시오.

수동 MAC 주소와의 상호 작용

직접 MAC 주소를 지정하고 자동 생성도 활성화한 경우 직접 지정한 수동 MAC 주소가 사용됩니다. 나중에 수동 MAC 주소를 삭제할 경우 자동 생성 주소가 사용됩니다.

자동 생성 주소는 (접두사 사용 시) A2로 시작하므로, 자동 생성도 사용하려는 경우 수동 MAC 주소가 A2로 시작해서는 안 됩니다.

장애 조치 MAC 주소

장애 조치에 사용할 수 있도록 ASA에서는 인터페이스마다 활성 MAC 주소와 대기 MAC 주소를 모두 생성합니다. 활성 유닛이 장애 조치하고 대기 유닛이 활성화되면 새 활성 유닛은 활성 MAC 주소를 사용하기 시작하므로 네트워크 중단이 최소화됩니다. 자세한 내용은 7-12 페이지의 MAC 주소 형식 섹션을 참조하십시오.

MAC 주소 형식

ASA에서는 다음 형식을 사용하여 MAC 주소를 생성합니다.

A2*xx.yyzz.zzzz*

여기서 *xx.yy*는 사용자가 정의한 접두사이거나 인터페이스의 마지막 2바이트(ASA 5500-X) 또는 백플레인(ASASM) MAC 주소를 기반으로 자동 생성된 접두사이며, *zz.zzzz*는 ASA에 의해 생성된 내부 카운터입니다. 대기 MAC 주소는 동일하지만, 내부 카운터가 1만큼 큽니다.

접두사가 어떻게 사용되는지 예를 들어 설명하자면, 접두사를 77로 설정한 경우ASA는 77을 16진수 값인 004D(*yyxx*)로 변환합니다. 접두사가 MAC 주소에서 쓰일 때는 ASA 기본 형식에 부합하도록 역전됩니다(*xxyy*).

A24**D.00***zz.zzzz*

접두사가 1009 (03F1)일 때 MAC 주소는 다음과 같습니다.

A2**F1.03***zz.zzzz*

참고 접두사 없는 MAC 주소 형식은 최신 ASA 버전에서 지원되지 않는 레거시 버전입니다. 레거시 형식에 대한 자세한 내용은 명령 참조에서 **mac-address auto** 명령을 참조하십시오.

다중 컨텍스트 모드를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASA 5512-X	• Base 라이센스: 지원 안 함 • Security Plus 라이센스: 2개 컨텍스트 *선택적 라이센스: 5개 컨텍스트*
ASA 5515-X	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5개 컨텍스트*
ASA 5525-X	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10 또는 20개 컨텍스트*
ASA 5545-X	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10, 20 또는 50개 컨텍스트*
ASA 5555-X	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10, 20, 50 또는 100개 컨텍스트*
ASA 5585-X 및 SSP-10	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10, 20, 50 또는 100개 컨텍스트*
ASA 5585-X 및 SSP-20, -40, -60	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10, 20, 50, 100 또는 250개 컨텍스트*
ASASM	Base 라이센스: 2개 컨텍스트 *선택적 라이센스: 5, 10, 20, 50, 100 또는 250개 컨텍스트*
ASAv	지원 안 함

전제 조건

다중 컨텍스트 모드에 들어온 다음 또는 관리 컨텍스트에 연결하여 시스템 컨피그레이션에 액세스합니다. 비 관리 컨텍스트에서 시스템을 구성할 수 없습니다. 기본적으로 다중 컨텍스트 모드를 활성화한 다음에는 기본 관리 IP 주소를 사용하여 관리 컨텍스트에 연결할 수 있습니다. ASA에 연결하는 것에 대한 자세한 내용은 2 장, “시작하기”,를 참조하십시오.

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원됩니다. 컨텍스트별로 방화벽 모드를 설정합니다.

장애 조치 지침

활성/활성(Active/Active) 모드 장애 조치는 다중 컨텍스트 모드에서만 지원됩니다.

IPv6 지침

IPv6를 지원합니다.

참고 교차 컨텍스트 IPv6 라우팅은 지원되지 않습니다.

지원되지 않는 기능

다중 컨텍스트 모드는 다음 기능을 지원하지 않습니다.

- RIP
- OSPFv3. (OSPFv2는 지원)
- 멀티캐스트 라우팅
- 위협 감지
- 통합 커뮤니케이션
- QoS
- 원격 액세스 VPN (사이트 대 사이트 VPN은 지원)

추가 지침

- (단일 또는 다중) 컨텍스트 모드는 재부팅할 때 유지되더라도 컨피그레이션 파일에 저장되지 않습니다. 컨피그레이션을 다른 디바이스에 복사하려면 새 디바이스의 모드를 일치하게 설정합니다.
- 플래시 메모리의 루트 디렉토리에 컨텍스트 컨피그레이션을 저장할 경우, 일부 모델에서는 가용 메모리가 있더라도 이 디렉토리의 공간이 부족해질 수 있습니다. 그러한 경우 컨피그레이션 파일을 위한 하위 디렉토리를 만듭니다. 배경 정보: ASA 5585-X와 같은 일부 모델에서는 내부 플래시 메모리에 FAT 16 파일 시스템을 사용합니다. 그리고 8.3 규격의 짧은 이름을 사용하지 않거나 대문자를 사용할 경우, 저장 가능한 파일 및 폴더는 512개보다 적습니다. 파일 시스템에서 긴 파일 이름을 저장하는 데 슬롯을 사용하기 때문입니다 (http://support.microsoft.com/kb/120138/en-us 참조).

기본 설정

- 기본적으로 ASA는 단일 컨텍스트 모드입니다.
- 7-9 페이지의 기본 클래스를 참조하십시오.
- 7-12 페이지의 기본 MAC 주소를 참조하십시오.

다중 컨텍스트 모드 구성

이 섹션에서는 다중 컨텍스트 모드를 구성하는 방법을 설명합니다.

다중 컨텍스트 모드 구성의 작업 흐름

다중 컨텍스트 모드를 구성하려면 다음 단계를 수행합니다.

1단계 다중 컨텍스트 모드를 활성화합니다. 7-15 페이지의 다중 컨텍스트 모드 활성화 또는 비활성화를 참조하십시오.

2단계 (선택 사항) 리소스 관리를 위한 클래스를 구성합니다. 7-17 페이지의 리소스 관리를 위한 클래스 구성를 참조하십시오. **참고**: VPN을 지원하려면 리소스 클래스에 VPN 리소스를 구성해야 합니다. 기본 클래스는 VPN을 허용하지 않습니다.

3단계 시스템 실행 영역에서 인터페이스를 구성합니다.

- ASA 5500-X—10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.
- ASASM—2장, “Switch Configuration for the Cisco ASA Services Module.”

4단계 보안 컨텍스트를 구성합니다. 7-19 페이지의 보안 컨텍스트 구성를 참조하십시오.

5단계 (선택 사항) MAC 주소 할당을 사용자 지정합니다. 7-23 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정를 참조하십시오.

6단계 컨텍스트에서 인터페이스 컨피그레이션을 완료합니다. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

다중 컨텍스트 모드 활성화 또는 비활성화

Cisco에 주문한 내용에 따라 ASA에서 이미 다중 보안 컨텍스트가 구성되었을 수도 있습니다. 단일 모드에서 다중 모드로 전환하려면 이 섹션의 절차를 따르십시오.

ASDM에서는 고가용성 및 확장성 마법사를 사용하고 활성/활성 장애 조치를 활성화한 경우 단일 모드에서 다중 모드로 바꿀 수 있습니다. 자세한 내용은 8 장, “고가용성을 위한 장애 조치”,를 참조하십시오. 활성/활성 장애 조치를 사용하지 않거나 다시 단일 모드로 돌아가려는 경우 CLI를 사용하여 모드를 변경해야 합니다. 모드를 변경하려면 확인이 필요하므로 명령행 인터페이스 툴을 사용할 수 없습니다. 이 섹션에서는 CLI에서 모드를 변경하는 것에 대해 설명합니다.

다중 컨텍스트 모드 활성화

단일 모드에서 다중 모드로 전환할 때 ASA는 실행 중 컨피그레이션을 (내부 플래시 메모리의 루트 디렉토리에서) 2개 파일로 변환합니다. 시스템 컨피그레이션인 새로운 시작 컨피그레이션과 관리 컨텍스트인 admin.cfg입니다. 원래의 실행 중 컨피그레이션은 old_running.cfg로 (내부 플래시 메모리의 루트 디렉토리에) 저장됩니다. 원래의 시작 컨피그레이션은 저장되지 않습니다. ASA는 관리 컨텍스트 항목을 "admin"이라는 이름으로 시스템 컨피그레이션에 자동 추가합니다.

전제 조건

시작 컨피그레이션을 백업합니다. 단일 모드에서 다중 모드로 전환할 때 ASA는 실행 중 컨피그레이션을 2개 파일로 변환합니다. 원래의 시작 컨피그레이션은 저장되지 않습니다. 37-12 페이지의 파일 관리를 참조하십시오.

세부 단계

명령	목적
mode multiple **예:** `ciscoasa(config)# mode multiple`	다중 컨텍스트 모드로 바꿉니다. ASA를 재부팅하라는 메시지가 나타납니다.

단일 컨텍스트 모드 복원

기존의 실행 중 컨피그레이션을 시작 컨피그레이션에 복사하고 모드를 단일 모드로 변경하려면 다음 단계를 수행합니다.

전제 조건

시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

	명령	목적
1단계	**copy disk0:old_running.cfg startup-config** **예:** `ciscoasa(config)# copy disk0:old_running.cfg startup-config`	원래 실행 중 컨피그레이션의 백업 버전을 현재 시작 컨피그레이션에 복사합니다.
2단계	**mode single** **예:** `ciscoasa(config)# mode single`	모드를 단일 모드로 설정합니다. ASA를 재부팅하라는 메시지가 나타납니다.

리소스 관리를 위한 클래스 구성

시스템 컨피그레이션에서 클래스를 컨피그레이션하려면 다음 단계를 수행합니다. 새 값으로 명령을 다시 입력하여 특정 리소스 제한의 값을 변경할 수 있습니다.

전제 조건

시스템 실행 영역에서 이 절차를 수행합니다.

지침

표 7-1에서는 리소스 유형과 그 제한을 보여줍니다.

표 7-1 리소스 이름 및 제한

리소스 이름	비율 또는 동시	컨텍스트당 최소 및 최대 개수	시스템 제한[1]	설명
ASDM Sessions	동시	최소 1 최대 5	32	ASDM 관리 세션. **참고** ASDM 세션은 2개의 HTTPS 연결을 사용합니다. 하나는 모니터링용으로 항상 실행되며, 다른 하나는 컨피그레이션 변경용으로 변경할 때만 실행됩니다. 예를 들어, 시스템 제한이 32개 ASDM 세션이라면 64개 HTTPS 세션을 의미합니다.
Connections Conns/sec[2]	동시 또는 비율	N/A	동시 연결: 해당 모델의 연결 제한은 4-1 페이지의 모델당 지원되는 기능 라이센스를 참조하십시오. 비율: N/A	임의의 두 호스트 간의 TCP 또는 UDP 연결. 단일 호스트와 여러 다른 호스트 간의 연결 포함
Hosts	동시	N/A	N/A	ASA를 통해 연결될 수 있는 호스트
Inspects/sec	비율	N/A	N/A	초당 애플리케이션 검사 수
MAC Entries	동시	N/A	65,535	투명 방화벽 모드의 경우 MAC 주소 테이블에서 허용되는 MAC 주소의 수
Routes	동시	N/A	N/A	동적 경로
Site-to-Site VPN Burst	동시	N/A	해당 모델의 기타 VPN 세션의 양에서 Site-to-Site VPN에 할당된 세션의 합계를 뺀 것.	Site-to-Site VPN로 컨텍스트에 할당된 양을 초과하는 허용된 사이트 대 사이트 VPN 세션 수 예를 들어, 모델에서 세션 5000개를 지원하는데 Site-to-Site VPN으로 컨텍스트 전체에 세션 4000개를 할당한 경우, 나머지 1000개 세션은 Site-to-Site VPN Burst에서 사용 가능합니다. 컨텍스트에 대한 세션을 보장하는 Site-to-Site VPN와 달리, Site-to-Site VPN Burst는 오버서브스크립션이 가능합니다. 버스트 풀은 모든 컨텍스트가 선착순으로 사용할 수 있습니다.

표 7-1 리소스 이름 및 제한 (계속)

리소스 이름	비율 또는 동시	컨텍스트당 최소 및 최대 개수	시스템 제한[1]	설명
Site-to-Site VPN	동시	N/A	해당 모델에서 사용 가능한 기타 VPN 세션은 4-1 페이지의 모델당 지원되는 기능 라이센스를 참조하십시오.	사이트 대 사이트 VPN 세션. 이 리소스는 오버서브스크립션할 수 없습니다. 모든 컨텍스트의 할당량 합계가 모델의 제한을 초과할 수 없습니다. 이 리소스에 대해 할당하는 세션은 해당 컨텍스트에 보장됩니다.
SSH	동시	최소 1 최대 5	100	SSH 세션
Syslogs/sec	비율	N/A	N/A	초당 syslog 메시지 수
Telnet	동시	최소 1 최대 5	100	텔넷 세션
xlates[2]	동시	N/A	N/A	네트워크 주소 변환

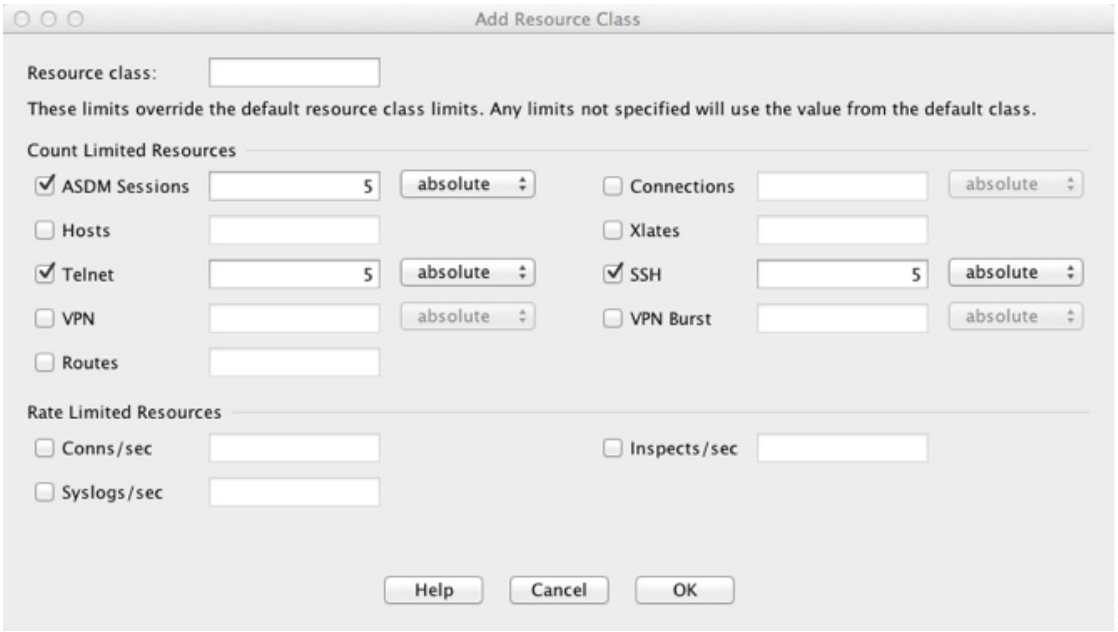
1. 이 열의 값이 N/A이면 해당 리소스에 대한 명시적 시스템 제한이 없으므로 리소스의 비율을 설정할 수 없습니다.
2. 어떤 제한이든 더 낮은 xlate 또는 conn일 때 syslog 메시지가 생성됩니다. 이를테면 xlate 제한을 7로, conn를 9로 설정한 경우 ASA는 syslog message 321001(“Resource 'xlates' limit of 7 reached for context 'ctx1'”)만 생성합니다. 321002(“Resource 'conn rate' limit of 5 reached for context 'ctx1'”)는 생성하지 않습니다.

세부 단계

1단계 아직 시스템 컨피그레이션 모드가 아닌 경우 Device List 창에서 활성 디바이스 ID 주소의 아래에 있는 **System**을 두 번 클릭합니다.

2단계 **Configuration > Context Management > Resource Class**를 선택하고 **Add**를 클릭합니다.

Add Resource Class 대화 상자가 나타납니다.



3단계 Resource Class 필드에 최대 20자의 클래스 이름을 입력합니다.

4단계 Count Limited Resources 영역에서 리소스의 동시 제한을 설정합니다.

각 리소스 유형에 대한 설명은 7-17 페이지의 표 7-1를 참조하십시오.

시스템 제한이 없는 리소스는 백분율을 설정할 수 없습니다. 절대값만 설정 가능합니다. 제한을 설정하지 않으면 기본 클래스에서 상속됩니다. 기본 클래스에서 제한을 설정하지 않은 경우 그 리소스는 무제한이거나 시스템 제한(있는 경우)까지 가능합니다. 대개의 리소스에서 0은 제한을 unlimited로 설정합니다. VPN 유형의 경우 0은 제한을 none으로 설정합니다.

5단계 Rate Limited Resources 영역에서 리소스의 비율 제한을 설정합니다.

각 리소스 유형에 대한 설명은 7-17 페이지의 표 7-1를 참조하십시오.

제한을 설정하지 않으면 기본 클래스에서 상속됩니다. 기본 클래스에서 제한을 설정하지 않으면 기본적으로 무제한이 됩니다. 0은 제한을 unlimited로 설정합니다.

6단계 **OK**를 클릭합니다.

보안 컨텍스트 구성

시스템 컨피그레이션의 보안 컨텍스트 정의는 컨텍스트 이름, 컨피그레이션 파일 URL, 컨텍스트에서 사용할 수 있는 인터페이스 및 기타 설정을 나타냅니다.

전제 조건

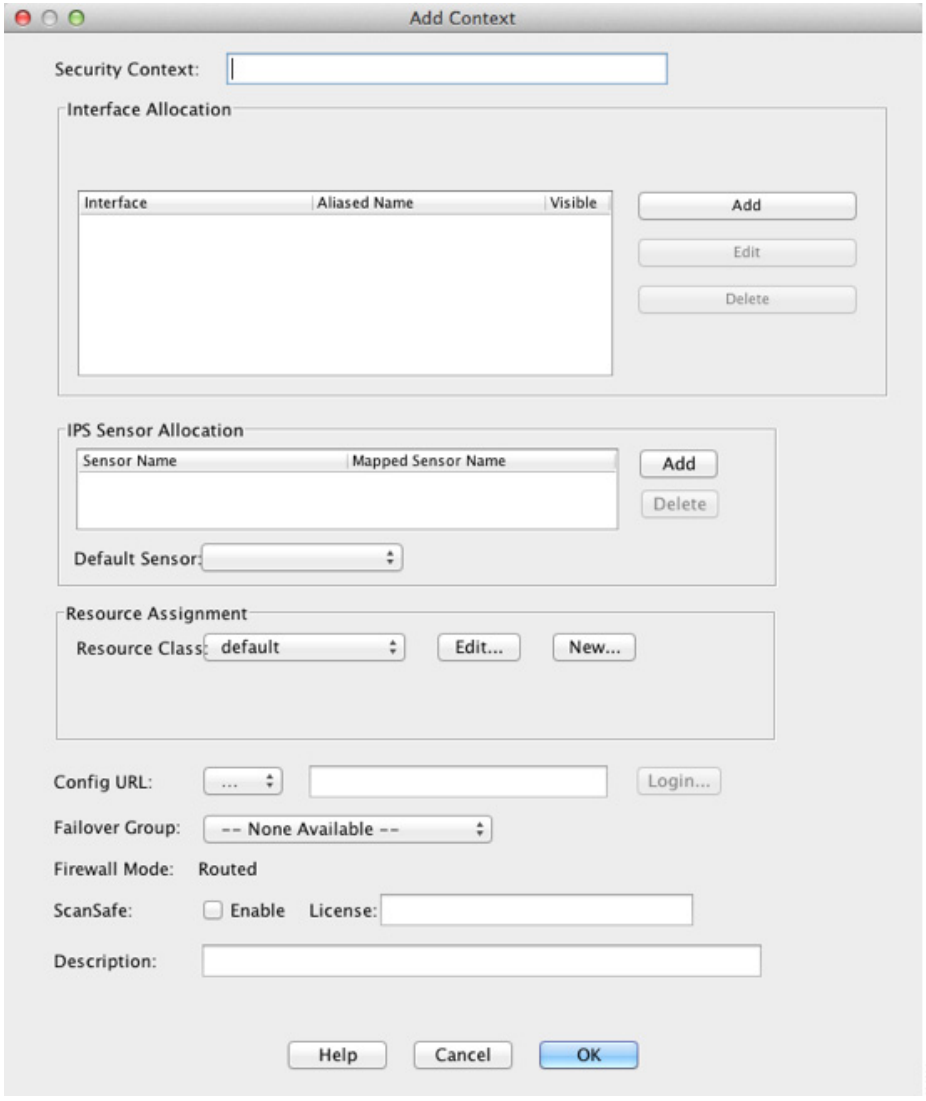
- 시스템 실행 영역에서 이 절차를 수행합니다.
- ASASM에서는 2장, “Switch Configuration for the Cisco ASA Services Module.” 에 따라 스위치의 ASASM에 VLAN을 지정합니다.
- ASA 5500-X의 경우 10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.에 따라 물리적 인터페이스 매개 변수, VLAN 하위 인터페이스, EtherChannel, 이중 인터페이스를 구성합니다.

세부 단계

1단계 아직 시스템 컨피그레이션 모드가 아닌 경우 Device List 창에서 활성 디바이스 ID 주소의 아래에 있는 **System**을 두 번 클릭합니다.

2단계 **Configuration > Context Management > Security Contexts**를 선택하고 **Add**를 클릭합니다.

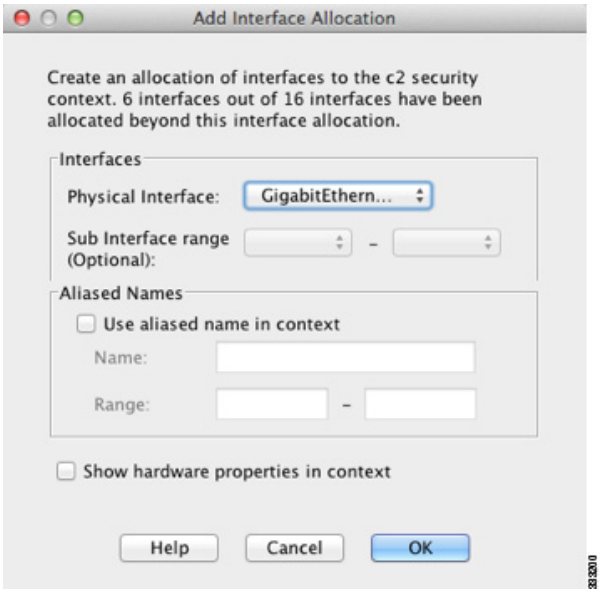
Add Context 대화 상자가 나타납니다.



3단계 Security Context 필드에 컨텍스트 이름을 최대 32자의 문자열로 입력합니다.

이 이름은 대/소문자를 구분합니다. 즉 “customerA”와 “CustomerA”는 2개의 컨텍스트입니다. “System”과 “Null”(대문자 및 소문자 모두 해당)은 예약된 이름이므로 사용할 수 없습니다.

4단계 Interface Allocation 영역에서 **Add** 버튼을 클릭하여 컨텍스트에 인터페이스를 지정합니다.



a. Interfaces > Physical Interface 드롭다운 목록에서 인터페이스를 선택합니다.

   기본 인터페이스를 지정할 수 있습니다. 그러면 하위 인터페이스 ID를 비워 둡니다. 또는 이 인터페이스와 연결되는 하위 인터페이스 또는 하위 인터페이스 범위를 지정할 수 있습니다. 투명 방화벽 모드에서는 다른 컨텍스트에 할당되지 않은 인터페이스만 표시됩니다. 기본 인터페이스가 이미 다른 컨텍스트에 지정된 경우 하위 인터페이스를 선택해야 합니다.

b. (선택 사항) Interfaces > Subinterface Range (선택 사항) 드롭다운 목록에서 하위 인터페이스 ID를 선택합니다.

   하위 인터페이스 ID 범위의 두 번째 드롭다운 목록(있는 경우)에서 마지막 ID를 선택합니다.

   투명 방화벽 모드에서는 다른 컨텍스트에 할당되지 않은 하위 인터페이스만 표시됩니다.

a. (선택 사항) 컨텍스트 컨피그레이션에서 인터페이스 ID 대신 사용할 인터페이스의 별칭을 설정하려면 Aliased Names 영역에서 **Use Aliased Name in Context**를 선택합니다.

   – Name 필드에서 별칭을 설정합니다.

     별칭은 문자로 시작하고 문자로 끝나야 하며, 그 밖의 자리에는 문자, 숫자, 밑줄만 올 수 있습니다. 이 필드에서는 문자 또는 밑줄로 끝나는 이름을 지정할 수 있습니다. 이름 다음에 선택적 숫자를 추가하려면 Range 필드에서 숫자를 설정합니다.

   – (선택 사항) Range 필드에서 별칭의 숫자 접미사를 설정합니다.

     하위 인터페이스의 범위가 있는 경우 이름의 끝에 추가될 숫자의 범위를 입력할 수 있습니다.

b. (선택 사항) 별칭을 설정했더라도 컨텍스트 사용자가 물리적 인터페이스 속성을 볼 수 있게 하려면 **Show Hardware Properties in Context**를 선택합니다.

c. **OK**를 클릭하면 Add Context 대화 상자로 돌아갑니다.

5단계 (선택 사항) IPS 가상 센서를 사용하는 경우 IPS Sensor Allocation 영역에서 컨텍스트에 센서를 지정합니다.

IPS 및 가상 센서에 대한 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

6단계 (선택 사항) 리소스 클래스에 이 컨텍스트를 지정하려면 Resource Assignment > Resource Class 드롭다운 목록에서 클래스 이름을 선택합니다.

이 영역에서 곧바로 리소스 클래스를 추가하거나 수정할 수 있습니다. 자세한 내용은 7-17 페이지의 리소스 관리를 위한 클래스 구성를 참조하십시오.

7단계 컨텍스트 컨피그레이션 위치를 설정하려면 Config URL 드롭다운 목록에서 파일 시스템 유형을 선택하고 필드에 경로를 입력하여 URL을 지정합니다.

예를 들어, FTP의 전체 URL은 다음 형식을 갖습니다.

ftp://server.example.com/configs/admin.cfg

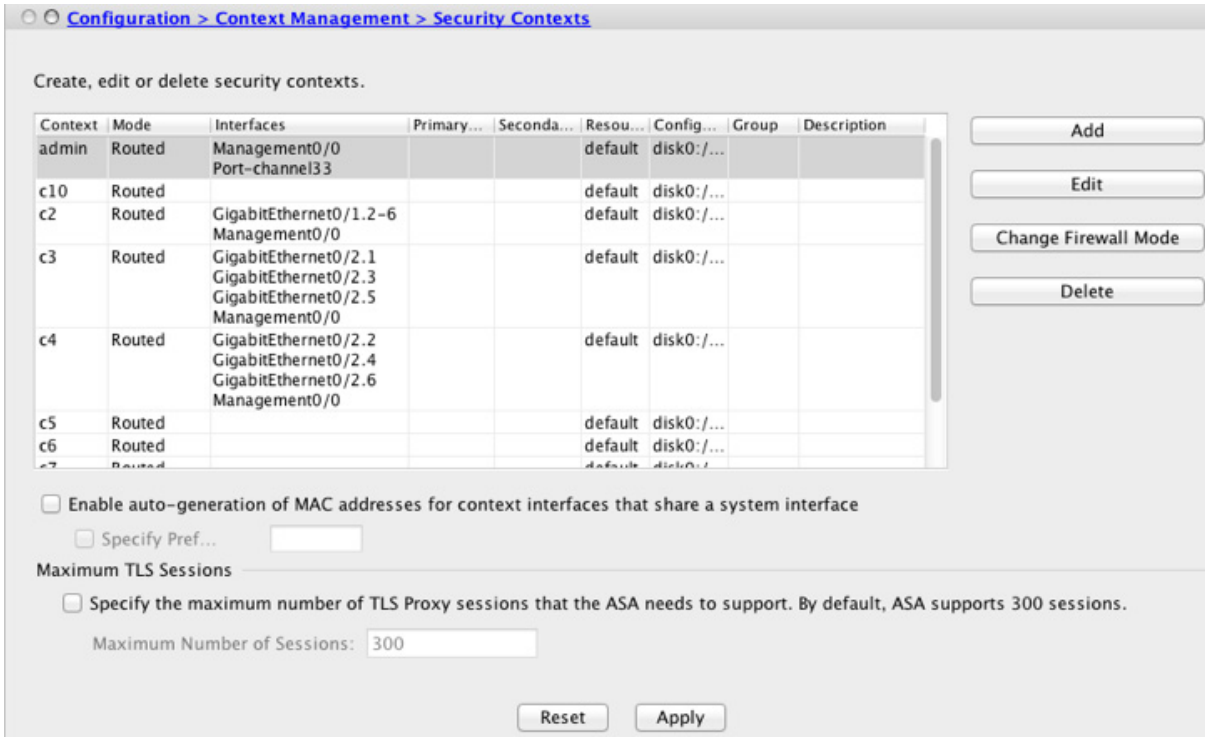
a. (선택 사항) 외부 파일 시스템의 경우 **Login**을 클릭하여 사용자 이름과 비밀번호를 설정합니다.

8단계 (선택 사항) 활성/활성 장애 조치를 위해 장애 조치 그룹을 설정하려면 Failover Group 드롭다운 목록에서 그룹 이름을 선택합니다.

9단계 (선택 사항) 이 컨텍스트에서 ScanSafe 검사를 활성화하려면 **Enable**을 클릭합니다. 시스템 컨피그레이션에 설정된 라이센스를 재정의하려면 License 필드에 라이센스를 입력합니다.

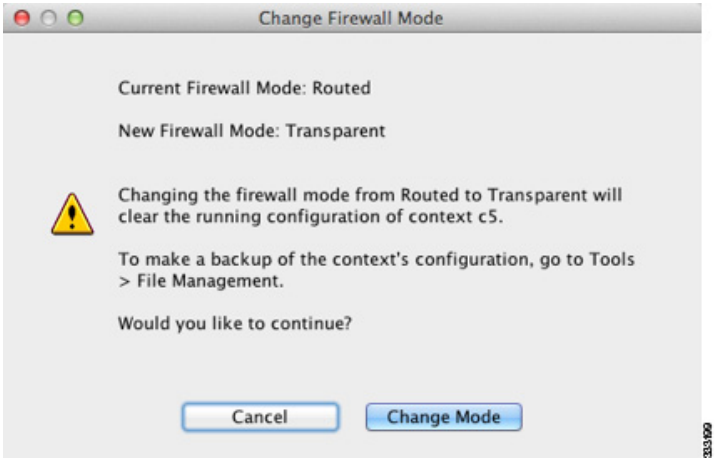
10단계 (선택 사항) Description 필드에 설명을 추가합니다.

11단계 **OK**를 클릭하면 Security Contexts 창으로 돌아갑니다.



12단계 (선택 사항) 방화벽 모드를 투명으로 설정하려면 컨텍스트를 선택하고 **Change Firewall Mode**를 클릭합니다.

다음 확인 대화 상자가 나타납니다.



새 컨텍스트일 경우 지울 컨피그레이션이 없습니다. 투명 방화벽 모드로 변경하려면 **Change Mode**를 클릭합니다.

기존 컨텍스트인 경우 모드를 변경하기 전에 반드시 컨피그레이션을 백업해야 합니다.

참고 ASDM에서 현재 연결된 컨텍스트(대개 관리 컨텍스트)의 모드는 변경할 수 없습니다. 명령줄에서 모드를 설정하려면 5-9 페이지의 방화벽 모드 설정(단일 모드)를 참조하십시오.

13단계 MAC 주소의 자동 생성을 사용자 지정하려면 7-23 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정를 참조하십시오.

14단계 디바이스의 최대 TLS 프록시 세션을 지정하려면 **Specify the maximum number of TLS Proxy sessions that the ASA needs to support** 확인란을 선택합니다. TLS 프록시에 대한 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

컨텍스트 인터페이스에 MAC 주소 자동 지정

이 섹션에서는 MAC 주소의 자동 생성을 구성하는 방법을 설명합니다.

이 MAC 주소는 컨텍스트 내에서 패킷을 분류하는 데 사용됩니다. 자세한 내용은, 특히 이전 AAA 버전에서 업그레이드하는 경우에는 7-11 페이지의 MAC 주소에 대한 정보를 참조하십시오. 7-31 페이지의 지정된 MAC 주소 보기도 참조하십시오.

지침

- 컨텍스트에서 인터페이스에 대해 name을 구성하면 새 MAC 주소가 즉시 생성됩니다. 컨텍스트 인터페이스를 구성한 다음 이 기능을 활성화한 경우, 활성화한 직후에 모든 인터페이스에 대해 MAC 주소가 생성됩니다. 이 기능을 비활성화한 경우 각 인터페이스의 MAC 주소가 기본 MAC 주소로 돌아갑니다. 예를 들어, GigabitEthernet 0/1의 하위 인터페이스는 다시 GigabitEthernet 0/1의 MAC 주소를 사용하게 됩니다.
- 드물지만, 생성된 MAC 주소가 네트워크의 다른 사설 MAC 주소와 충돌할 경우 컨텍스트 내에서 그 인터페이스의 MAC 주소를 직접 설정할 수 있습니다. MAC 주소를 직접 설정하려면 12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성를 참조하십시오.

세부 단계

1단계 아직 시스템 컨피그레이션 모드가 아닌 경우 Device List 창에서 활성 디바이스 ID 주소의 아래에 있는 **System**을 두 번 클릭합니다.

2단계 **Configuration > Context Management > Security Contexts**, and check **Mac-Address auto**를 선택합니다. 접두사를 입력하지 않으면 ASA에서 인터페이스의 마지막 2바이트(ASA 5500-X) 또는 백플레인(ASASM) MAC 주소를 기반으로 접두사를 자동으로 생성합니다.

3단계 (선택 사항) **Prefix** 확인란을 선택하고 필드에 0~65535 범위의 십진수를 입력합니다.

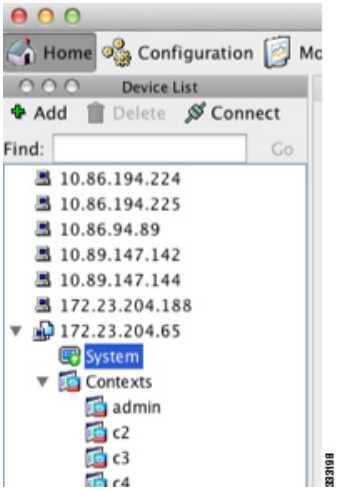
이 접두사가 4자리 16진수로 변환되어 MAC 주소의 일부로 사용됩니다. 접두사를 사용하는 방법에 대한 자세한 내용은 7-12 페이지의 MAC 주소 형식를 참조하십시오.

컨텍스트와 시스템 실행 영역 간 전환

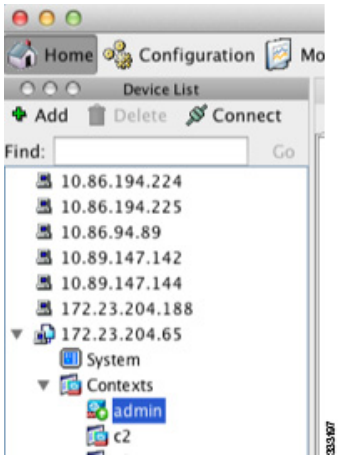
시스템 실행 영역(또는 관리 컨텍스트)에 로그인한 경우 여러 컨텍스트로 전환하면서 각 컨텍스트에서 컨피그레이션 및 모니터링 작업을 수행할 수 있습니다. 컨피그레이션 모드에서 수정하거나 위치에 따라 달라집니다. 시스템 실행 영역이라면 실행 중 컨피그레이션은 시스템 컨피그레이션으로만 이루어집니다. 컨텍스트에 있을 경우 실행 중 컨피그레이션은 그 컨텍스트로만 이루어집니다.

세부 단계

1단계 시스템을 구성하려면 Device List 창에서 활성 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.



2단계 컨텍스트를 구성하려면 Device List 창에서 활성 디바이스 IP 주소 아래의 컨텍스트 이름을 두 번 클릭합니다.



보안 컨텍스트 관리

이 섹션에서는 보안 컨텍스트를 관리하는 방법을 설명합니다.

- 7-25 페이지의 보안 컨텍스트 삭제
- 7-26 페이지의 관리 컨텍스트 변경
- 7-27 페이지의 보안 컨텍스트 URL 변경
- 7-28 페이지의 보안 컨텍스트 다시 로드

보안 컨텍스트 삭제

현재 관리 컨텍스트를 삭제할 수 없습니다..

참고 장애 조치를 사용하는 경우, 활성 유닛에서 컨텍스트를 삭제하는 시점과 대기 유닛에서 컨텍스트가 삭제되는 시점 간에 지연이 발생합니다.

전제 조건

시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

1단계 아직 시스템 컨피그레이션 모드가 아닌 경우 Device List 창에서 활성 디바이스 ID 주소의 아래에 있는 **System**을 두 번 클릭합니다.

2단계 **Configuration > Context Management > Security Contexts**를 선택합니다.

3단계 삭제할 컨텍스트를 선택하고 **Delete**를 클릭합니다.

Delete Context 대화 상자가 나타납니다.

4단계 나중에 이 컨텍스트를 다시 추가하려는 경우 그리고 나중에 사용하기 위해 컨피그레이션 파일을 보관하고 싶은 경우 **Also delete config URL file from the disk** 확인란을 선택 취소합니다.

컨피그레이션 파일을 삭제하려면 이 확인란을 선택된 상태로 둡니다.

5단계 **Yes**를 클릭합니다.

관리 컨텍스트 변경

시스템 컨피그레이션은 자체 네트워크 인터페이스나 네트워크 설정을 포함하지 않습니다. 그보다는 시스템에서 네트워크 리소스에 액세스해야 할 때(예: 서버로부터 컨텍스트 다운로드) 관리 컨텍스트로 지정된 컨텍스트 중 하나를 사용합니다.

관리 컨텍스트는 여느 컨텍스트와 비슷하지만, 사용자가 관리 컨텍스트에 로그인하면 시스템 관리자 권한을 갖게 되어 시스템 및 그 밖의 모든 컨텍스트에 액세스할 수 있다는 점이 다릅니다. 관리 컨텍스트는 어떠한 제한도 받지 않으며, 일반 컨텍스트로 사용될 수 있습니다. 그러나 관리 컨텍스트에 로그인하면 모든 컨텍스트에 대한 관리자 권한이 부여되므로, 관리 컨텍스트 액세스 권한을 적합한 사용자로 한정할 필요가 있습니다.

참고 ASDM의 경우 ASDM 내에서 관리 컨텍스트를 변경할 수 없습니다. ASDM 세션의 연결이 끊기기 때문입니다. 명령행 인터페이스 툴에서 이 절차를 수행할 수 있습니다. 새 관리 컨텍스트에 다시 연결해야 합니다.

지침

어떤 컨텍스트도 관리 컨텍스트로 설정할 수 있습니다. 단, 컨피그레이션 파일이 내부 플래시 메모리에 저장되어 있어야 합니다.

전제 조건

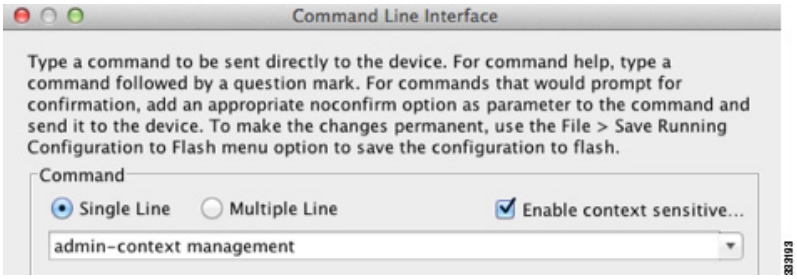
시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

1단계 아직 시스템 컨피그레이션 모드가 아닌 경우 Device List 창에서 활성 디바이스 ID 주소의 아래에 있는 **System**을 두 번 클릭합니다.

2단계 **Tools > Command Line Interface**를 선택합니다.

Command Line Interface 대화 상자가 나타납니다.



3단계 다음의 명령을 입력합니다.

admin-context *context_name*

4단계 **Send**를 클릭합니다.

텔넷, SSH, HTTPS(ASDM)와 같이 관리 컨텍스트에 연결되어 있는 원격 관리 세션은 모두 종료됩니다. 새 관리 컨텍스트에 다시 연결해야 합니다.

참고 **ntp server**와 같이 몇 가지 시스템 컨피그레이션 명령은 관리 컨텍스트에 속한 인터페이스 이름을 지정합니다. 관리 컨텍스트를 변경하는 경우, 그 인터페이스 이름이 새 관리 컨텍스트에 없다면 그 이름을 참조하는 모든 시스템 명령을 업데이트해야 합니다.

보안 컨텍스트 URL 변경

이 섹션에서는 컨텍스트 URL을 변경하는 방법을 설명합니다.

지침

- 새 URL에서 컨피그레이션을 다시 로드하지 않고는 보안 컨텍스트 URL을 변경할 수 없습니다. ASA에서는 새 컨피그레이션을 현재 실행 중인 컨피그레이션과 병합합니다.
- 동일한 URL을 다시 입력하면 역시 저장된 컨피그레이션을 실행 중인 컨피그레이션과 병합합니다.
- 병합은 새 컨피그레이션의 새로운 명령을 실행 중인 컨피그레이션에 추가합니다.
  - 컨피그레이션이 동일할 경우 어떤 변경도 없습니다.
  - 명령이 충돌하거나 명령이 컨텍스트 실행에 영향을 줄 경 경우, 병합의 효과는 명령에 따라 달라집니다. 오류가 발생할 수도, 예기치 않은 결과가 나올 수도 있습니다. 실행 중인 컨피그레이션이 비어 있을 경우(예: 서버가 사용할 수 없는 상태이고 컨피그레이션이 다운로드된 적이 없는 경우) 새로운 컨피그레이션이 사용됩니다.
- 컨피그레이션의 병합을 원치 않는다면 실행 중인 컨피그레이션을 지운 다음(해당 컨텍스트를 통한 모든 통신이 중지됨) 새 URL에서 컨피그레이션을 다시 로드하면 됩니다.

전제 조건

시스템 실행 영역에서 이 절차를 수행합니다.

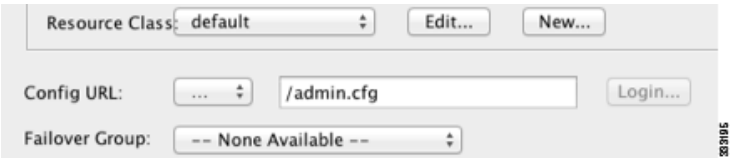
세부 단계

1단계 아직 시스템 컨피그레이션 모드가 아닌 경우 Device List 창에서 활성 디바이스 ID 주소의 아래에 있는 **System**을 두 번 클릭합니다.

2단계 **Configuration > Context Management > Security Contexts**를 선택합니다.

3단계 수정할 컨텍스트를 선택하고 **Edit**를 클릭합니다.

Edit Context 대화 상자가 나타납니다.



4단계 Config URL 필드에 새 URL을 입력하고 **OK**를 클릭합니다.

시스템에서 즉시 컨텍스트를 로드하므로 실행 중이 됩니다.

보안 컨텍스트 다시 로드

2가지 방법으로 컨텍스트를 다시 로드할 수 있습니다.

- 실행 중인 컨피그레이션을 지운 다음 시작 컨피그레이션을 가져옵니다.

  그러면 컨텍스트와 연결된 대부분의 특성(연결, NAT 테이블 등)이 사라집니다.
- 시스템 컨피그레이션에서 컨텍스트를 삭제합니다.

  그러면 문제 해결에 유용할 수 있는 추가 특성(예: 메모리 할당)이 사라집니다. 그러나 컨텍스트를 다시 시스템에 추가하려면 URL과 인터페이스를 다시 지정해야 합니다.

- 7-28 페이지의 구성을 지워 다시 로드
- 7-29 페이지의 컨텍스트를 삭제하고 다시 추가하여 다시 로드

구성을 지워 다시 로드

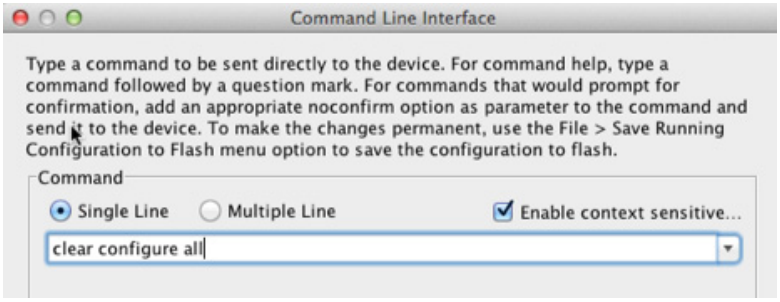
컨텍스트 컨피그레이션을 지우고 URL에서 컨피그레이션을 다시 로드하여 컨텍스트를 다시 로드하려면 다음 단계를 수행합니다.

세부 단계

1단계 Device List 창에서 활성 디바이스 IP 주소 아래의 컨텍스트 이름을 두 번 클릭합니다.

2단계 **Tools > Command Line Interface**를 선택합니다.

Command Line Interface 대화 상자가 나타납니다.



3단계 다음의 명령을 입력합니다.

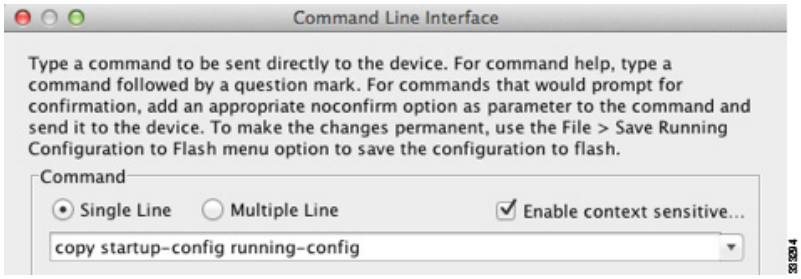
```
clear configure all
```

4단계 **Send**를 클릭합니다.

컨텍스트 컨피그레이션이 사라집니다.

5단계 **Tools > Command Line Interface**를 다시 선택합니다.

Command Line Interface 대화 상자가 나타납니다.



6단계 다음의 명령을 입력합니다.

```
copy startup-config running-config
```

7단계 **Send**를 클릭합니다.

ASA에서 컨피그레이션을 다시 로드합니다. ASA에서는 시스템 컨피그레이션에 지정된 URL에서 컨피그레이션을 복사합니다. 컨텍스트 내에서 URL을 변경할 수 없습니다.

컨텍스트를 삭제하고 다시 추가하여 다시 로드

컨텍스트를 삭제한 다음 다시 추가하는 방법으로 컨텍스트를 다시 로드하려면 다음 섹션의 단계를 수행합니다.

1. 7-25 페이지의 보안 컨텍스트 삭제. 반드시 **Also delete config URL file from the disk** 확인란을 선택 취소해야 합니다.
2. 7-19 페이지의 보안 컨텍스트 구성

보안 컨텍스트 모니터링

이 섹션에서는 컨텍스트 정보를 보고 모니터링하는 방법을 설명합니다.

컨텍스트 리소스 사용량 모니터링

시스템 실행 영역에서 모든 컨텍스트의 리소스 사용량을 모니터링하려면 다음 단계를 수행합니다.

1단계 아직 시스템 모드가 아닌 경우 Device List 창에서 활성 디바이스 ID 주소의 아래에 있는 **System**을 두 번 클릭합니다.

2단계 툴바에서 **Monitoring** 버튼을 클릭합니다.

3단계 **Context Resource Usage**를 클릭합니다.

모든 컨텍스트의 리소스 사용량을 보려면 각 리소스 유형을 클릭합니다.

- **ASDM/Telnet/SSH**—ASDM, 텔넷, SSH 연결의 사용량을 표시합니다.
  - Context—각 컨텍스트의 이름을 표시합니다.

  각 액세스 방식에서 다음 사용량 통계를 확인합니다.
  - Existing Connections (#)—기존 연결의 수를 표시합니다.
  - Existing Connections (%)—이 컨텍스트에서 사용하는 연결을 모든 컨텍스트에서 사용하는 총 연결 수 기준 백분율로 표시합니다.
  - Peak Connections (#)—**clear resource usage** 명령을 사용했거나 디바이스를 재부팅하여 마지막으로 통계를 지웠던 시점 이후 최다 연결 수를 표시합니다.
- **Routes**—동적 경로의 사용량을 표시합니다.
  - Context—각 컨텍스트의 이름을 표시합니다.
  - Existing Connections (#)—기존 연결의 수를 표시합니다.
  - Existing Connections (%)—이 컨텍스트에서 사용하는 연결을 모든 컨텍스트에서 사용하는 총 연결 수 기준 백분율로 표시합니다.
  - Peak Connections (#)—**clear resource usage** 명령을 사용했거나 디바이스를 재부팅하여 마지막으로 통계를 지웠던 시점 이후 최다 연결 수를 표시합니다.
- **Xlates**—네트워크 주소 변환의 사용량을 표시합니다.
  - Context—각 컨텍스트의 이름을 표시합니다.
  - Xlates (#)—현재 xlate의 수를 표시합니다.
  - Xlates (%)—이 컨텍스트에서 사용하는 xlate를 모든 컨텍스트에서 사용하는 총 xlate 수 기준 백분율로 표시합니다.
  - Peak (#)—**clear resource usage** 명령을 사용했거나 디바이스를 재부팅하여 마지막으로 통계를 지웠던 시점 이후 최다 xlate 수를 표시합니다.
- **NATs**—NAT 규칙의 수를 표시합니다.
  - Context—각 컨텍스트의 이름을 표시합니다.
  - NATs (#)—현재 NAT 규칙의 수를 표시합니다.

  - NATs (%)—이 컨텍스트에서 사용하는 NAT 규칙을 모든 컨텍스트에서 사용하는 총 NAT 규칙 수 기준 백분율로 표시합니다.
  - Peak NATs (#)—**clear resource usage** 명령을 사용했거나 디바이스를 재부팅하여 마지막으로 통계를 지웠던 시점 이후 최다 NAT 규칙 수를 표시합니다.
- **Syslogs**—시스템 로그 메시지의 비율을 표시합니다.
  - Context—각 컨텍스트의 이름을 표시합니다.
  - Syslog Rate (#/sec)—현재 시스템 로그 메시지의 비율을 표시합니다.
  - Syslog Rate (%)—이 컨텍스트에서 생성한 시스템 로그 메시지를 모든 컨텍스트에서 생성한 총 시스템 로그 메시지 수 기준 백분율로 표시합니다.
  - Peak Syslog Rate (#/sec)—**clear resource usage** 명령을 사용했거나 디바이스를 재부팅하여 마지막으로 통계를 지웠던 시점 이후 최고 시스템 로그 메시지 비율을 표시합니다.
- VPN—VPN 사이트 대 사이트 터널의 사용량을 표시합니다.
  - Context—각 컨텍스트의 이름을 표시합니다.
  - VPN Connections—보장된 VPN 세션의 사용량을 표시합니다.
  - VPN Burst Connections—버스트 VPN 세션의 사용량을 표시합니다.

    Existing (#)—기존 터널의 수를 표시합니다.

    Peak (#)—**clear resource usage** 명령을 사용했거나 디바이스를 재부팅하여 마지막으로 통계를 지웠던 시점 이후 최다 터널 수를 표시합니다.

4단계 화면을 새로 고치려면 **Refresh**를 클릭합니다.

지정된 MAC 주소 보기

시스템 컨피그레이션 내에서 또는 컨텍스트 내에서 자동 생성된 MAC 주소를 볼 수 있습니다.

- 7-31 페이지의 시스템 구성에서 MAC 주소 보기
- 7-32 페이지의 컨텍스트 내 MAC 주소 보기

시스템 구성에서 MAC 주소 보기

이 단원에서는 시스템 컨피그레이션에서 MAC 주소를 보는 방법을 설명합니다.

지침

직접 인터페이스에 MAC 주소를 지정하지만 자동 생성도 활성화한 경우, 수동 MAC 주소가 사용되지만 자동 생성 주소도 계속 컨피그레이션에 표시됩니다. 나중에 수동 MAC 주소를 삭제하면, 여기에 표시되었던 자동 생성 주소가 사용됩니다.

세부 단계

1단계 아직 시스템 컨피그레이션 모드가 아닌 경우 Device List 창에서 활성 디바이스 ID 주소의 아래에 있는 **System**을 두 번 클릭합니다.

2단계 **Configuration > Context Management > Security Contexts**를 선택하고 Primary MAC 및 Secondary MAC 열을 봅니다.

컨텍스트 내 MAC 주소 보기

이 섹션에서는 컨텍스트 내에서 MAC 주소를 보는 방법을 설명합니다.

세부 단계

1단계 아직 시스템 컨피그레이션 모드가 아닌 경우 Device List 창에서 활성 디바이스 ID 주소의 아래에 있는 **System**을 두 번 클릭합니다.

2단계 **Configuration > Interfaces**를 클릭하고 MAC Address 열을 봅니다.

이 테이블은 사용 중인 MAC 주소를 보여줍니다. 직접 MAC 주소를 지정하고 자동 생성도 활성화한 경우, 시스템 컨피그레이션 내에서는 사용되지 않은 자동 생성 주소만 볼 수 있습니다.

다중 컨텍스트 모드의 기능 내역

표 7-2에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 7-2 다중 컨텍스트 모드의 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
다중 보안 컨텍스트	7.0(1)	다중 컨텍스트 모드를 도입했습니다. 다음 화면을 도입했습니다. Configuration > Context Management
자동 MAC 주소 지정	7.2(1)	컨텍스트 인터페이스에 MAC 주소를 자동으로 지정하는 기능을 도입했습니다. 다음 화면을 수정했습니다. Configuration > Context Management > Security Contexts
리소스 관리	7.2(1)	리소스 관리를 도입했습니다. 다음 화면을 도입했습니다. Configuration > Context Management > Resource Management

표 7-2 다중 컨텍스트 모드의 기능 내역 (계속)

기능 이름	플랫폼 릴리스	기능 정보
IPS 가상 센서	8.0(2)	IPS 소프트웨어 버전 6.0 이상을 실행하는 AIP SSM에서 여러 가상 센서를 실행할 수 있습니다. 즉 AIP SSM에서 다중 보안 정책을 구성할 수 있습니다. 각 컨텍스트 또는 단일 모드 ASA를 하나 이상의 가상 센서에 지정하거나 여러 보안 컨텍스트를 동일한 가상 센서에 지정할 수 있습니다. 다음 화면을 수정했습니다. Configuration > Context Management > Security Contexts
자동 MAC 주소 지정 확장	8.0(5)/8.2(2)	MAC 주소 형식이 접두사를 사용하고, 고정 시작 값(A2)을 사용하고, 장애 조치 쌍에서는 기본 유닛 MAC 주소와 보조 유닛 MAC 주소에 서로 다른 체계를 사용하도록 변경되었습니다. 또한 MAC 주소는 다시 로드하더라도 유지됩니다. 명령 구문 분석기에서 자동 생성 활성화 여부를 확인합니다. 직접 MAC 주소를 지정하는 것도 원할 경우 수동 MAC 주소는 A2로 시작할 수 없습니다. 다음 화면을 수정했습니다. Configuration > Context Management > Security Contexts
ASA 5550 및 5580에서 최대 컨텍스트 증가	8.4(1)	ASA 5550의 최대 보안 컨텍스트 수가 50에서 100으로 늘어났습니다. ASA 5580의 최대 보안 컨텍스트 수가 50에서 250으로 늘어났습니다.
자동 MAC 주소 지정 기본적으로 활성화	8.5(1)	자동 MAC 주소 지정이 기본적으로 활성화되어 있습니다. 다음 화면을 수정했습니다. Configuration > Context Management > Security Contexts

표 7-2 다중 컨텍스트 모드의 기능 내역 (계속)

기능 이름	플랫폼 릴리스	기능 정보
MAC 주소 접두사 자동 생성	8.6(1)	다중 컨텍스트 모드에서 ASA의 자동 MAC 주소 생성 컨피그레이션은 기본 접두사를 사용하도록 변환됩니다. ASA는 인터페이스의 마지막 2바이트(ASA 5500-X) 또는 백플레인(ASASM) MAC 주소를 기반으로 접두사를 자동 생성합니다. 다시 로드할 때 또는 MAC 주소 생성을 다시 활성화할 경우 이 변환이 자동으로 이루어집니다. 이러한 접두사 생성 방식은 세그먼트에서 더 확실하게 고유한 MAC 주소를 보장하는 등 여러 가지 이점을 제공합니다. 접두사를 변경하려는 경우 사용자 지정 접두사로 기능을 재구성할 수 있습니다. 기존의 MAC 주소 생성 방식은 더 이상 사용되지 않습니다. **참고** 장애 조치 쌍의 히트리스 업그레이드를 유지하고자 ASA에서는 장애 조치가 활성화된 경우 다시 로드할 때 기존 컨피그레이션의 MAC 주소 방식을 변환하지 *않습니다*. 그러나 특히 ASASM에서는 장애 조치를 사용할 때 직접 접두사 생성 방법으로 바꾸는 것이 좋습니다. 접두사 방법을 사용하지 않으면 서로 다른 슬롯 번호에 설치된 ASASM에서 장애 조치 시 MAC 주소가 바뀌어 트래픽이 중단될 수 있습니다. 업그레이드한 다음 MAC 주소 생성에 접두사 방법을 사용하려면 MAC 주소 생성에서 다시 기본 접두사를 사용할 수 있게 합니다. 다음 화면을 수정했습니다. Configuration > Context Management > Security Contexts
보안 컨텍스트의 동적 라우팅	9.0(1)	EIGRP 및 OSPFv2 동적 라우팅 프로토콜이 다중 컨텍스트 모드에서 지원됩니다. OSPFv3, RIP, 멀티캐스트 라우팅은 지원되지 않습니다.
라우팅 테이블 항목의 새로운 리소스 유형	9.0(1)	각 컨텍스트에서 라우팅 테이블 항목의 최대값을 설정하기 위해 새로운 리소스 유형인 routes를 개발했습니다. 다음 화면을 수정했습니다. Configuration > Context Management > Resource Class > Add Resource Class
다중 컨텍스트 모드의 사이트 대 사이트 VPN	9.0(1)	사이트 대 사이트 VPN 터널이 다중 컨텍스트 모드에서 지원됩니다.
사이트 대 사이트 VPN 터널을 위한 새로운 리소스 유형	9.0(1)	각 컨텍스트에서 사이트 대 사이트 VPN 터널의 최대값을 설정하기 위해 새로운 리소스 유형인 vpn other와 vpn burst other를 개발했습니다. 다음 화면을 수정했습니다. Configuration > Context Management > Resource Class > Add Resource Class

고가용성을 위한 장애 조치

이 장에서는 Cisco ASA의 고가용성을 실현하기 위해 액티브/스탠바이 또는 액티브/액티브 장애 조치를 구성하는 방법에 대해 설명합니다.

장애 조치 정보

장애 조치 개요

장애 조치를 구성하려면 2개의 동일한 ASA가 전용 장애 조치 링크 또는 선택에 따라 상태 링크를 통해 서로 연결되어 있어야 합니다. 액티브 유닛 및 인터페이스의 상태를 모니터링하여 특정한 장애 조치 조건을 충족하는지 판단합니다. 이러한 조건이 충족되면 장애 조치가 이루어집니다.

ASA에서는 액티브/액티브 장애 조치 및 액티브/스탠바이 장애 조치로 된 2가지 장애 조치 모드를 지원합니다. 각 장애 조치 모드에서는 고유한 방법을 통해 장애 조치를 확인하고 수행합니다.

- 액티브/스탠바이 장애 조치에서는 하나의 유닛이 액티브 유닛입니다. 이 유닛에서 트래픽을 전달합니다. 스탠바이 유닛에서는 트래픽을 능동적으로 전달하지 않습니다. 장애 조치가 일어나면 액티브 유닛은 스탠바이 유닛으로 장애 조치를 시작하며, 이때 스탠바이 유닛이 액티브 유닛이 됩니다. 단일 또는 다중 컨텍스트 모드에서는 ASA에 액티브/스탠바이 장애 조치를 사용할 수 있습니다.
- 액티브/액티브 장애 조치 컨피그레이션에서는 두 ASA에서 모두 네트워크 트래픽을 전달할 수 있습니다. 액티브/액티브 장애 조치는 다중 컨텍스트 모드의 ASA에만 사용할 수 있습니다. 액티브/액티브 장애 조치에서 ASA의 보안 컨텍스트는 2개의 *장애 조치 그룹*으로 나뉩니다. 장애 조치 그룹은 단순히 하나 이상의 보안 컨텍스트로 구성된 논리적 그룹입니다. 한 그룹은 기본 ASA에서 액티브 상태로 할당되고 다른 그룹은 보조 ASA에서 액티브 상태로 할당됩니다. 장애 조치는 장애 조치 그룹 수준에서 수행됩니다.

두 가지 장애 조치 구성에서는 모두 스테이트풀 및 스테이트리스 장애 조치를 지원합니다.

장애 조치 시스템 요구 사항

이 절에서는 장애 조치 컨피그레이션에서 ASA의 하드웨어, 소프트웨어, 라이센스 요구 사항에 대해 설명합니다.

- 8-2 페이지의 하드웨어 요구 사항
- 8-3 페이지의 소프트웨어 요구 사항
- 8-3 페이지의 라이센스 요구 사항

하드웨어 요구 사항

장애 조치 컨피그레이션의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 모델이어야 합니다.
- 인터페이스 개수와 유형이 같아야 합니다.
- 같은 모듈을 설치해야 합니다(있을 경우).
- 같은 RAM을 설치해야 합니다.

장애 조치 컨피그레이션에서 플래시 메모리 크기가 다른 유닛을 사용 중인 경우, 용량이 플래시 메모리 용량이 작은 유닛에 소프트웨어 이미지 파일 및 컨피그레이션 파일을 수용할 수 있는 충분한 공간이 있는지 확인해야 합니다. 그렇지 않을 경우 플래시 메모리 용량이 큰 유닛에서 플래시 메모리 용량이 작은 유닛으로 컨피그레이션을 동기화할 수 없습니다.

소프트웨어 요구 사항

장애 조치 컨피그레이션의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 방화벽 모드에 있어야 합니다(라우팅 또는 투명).
- 같은 컨텍스트 모드에 있어야 합니다(단일 또는 다중).
- 주(첫 번째 번호) 및 부(두 번째 번호) 소프트웨어 버전이 같아야 합니다. 그러나 업그레이드 과정에서 일시적으로 여러 소프트웨어 버전을 사용할 수 있습니다. 예를 들어, 버전 8.3(1)에서 버전 8.3(2)으로 업그레이드하고 장애 조치를 활성 상태로 유지할 수 있습니다. 장기적으로 호환성을 보장하려면 두 유닛을 모두 같은 버전으로 업그레이드하는 것이 좋습니다.

  장애 조치 쌍에서 소프트웨어를 업그레이드하는 방법에 대한 자세한 내용은 37-6 페이지의 장애 조치 쌍 또는 ASA 클러스터 업그레이드를 참조하십시오.
- 같은 AnyConnect 이미지가 있어야 합니다. 무중단 업그레이드를 수행할 때 장애 조치 쌍에 불일치하는 이미지가 있을 경우, 업그레이드 프로세스의 마지막 재부팅 단계에서 클라이언트리스 SSL VPN 연결이 종료되고 데이터베이스에 Orphan 세션이 표시되며 IP 풀에는 클라이언트에 할당된 IP 주소가 "사용 중"인 것으로 표시됩니다.

라이센스 요구 사항

장애 조치 컨피그레이션의 유닛 2개는 라이센스가 동일하지 않아도 됩니다. 이러한 라이센스는 통합되어 장애 조치 클러스터 라이센스를 생성합니다. 자세한 내용은 4-27 페이지의 장애 조치 또는 ASA 클러스터 라이센스를 참조하십시오.

장애 조치 및 스테이트풀 장애 조치 링크

장애 조치 링크 및 옵션으로 제공되는 스테이트풀 장애 조치 링크는 2개 유닛 간의 전용 연결입니다.

- 8-3 페이지의 장애 조치 링크
- 8-4 페이지의 스테이트풀 장애 조치 링크
- 8-5 페이지의 장애 조치 및 데이터 링크 중단 방지

주의 IPsec 터널이나 장애 조치 키로 통신 보안을 설정하지 않는 한 장애 조치 및 상태 링크를 통해 전송되는 모든 정보는 일반 텍스트로 전송됩니다. ASA를 사용하여 VPN 터널을 종료할 경우, 이 정보에는 터널 설정에 사용된 모든 사용자 이름, 비밀번호, PSH(Pre-Shared key)가 포함됩니다. 이러한 민감한 데이터를 일반 텍스트로 전송할 경우 중대한 보안 위험을 초래할 수 있습니다. ASA를 사용하여 VPN 터널을 종료할 경우 IPsec 터널이나 장애 조치 키로 장애 조치 통신의 보안을 설정하는 것이 좋습니다.

장애 조치 링크

장애 조치 쌍의 유닛 2개에서는 장애 조치 링크를 통해 지속적으로 통신을 수행하여 각 유닛의 작동 상태를 확인합니다.

- 8-4 페이지의 장애 조치 링크 데이터
- 8-4 페이지의 장애 조치 링크에 대한 인터페이스
- 8-4 페이지의 장애 조치 링크 연결

장애 조치 링크 데이터

다음 정보는 장애 조치 링크를 통해 전달됩니다.

- 유닛 상태(액티브 또는 스탠바이)
- Hello 메시지(keep-alives)
- 네트워크 링크 상태
- MAC 주소 교환
- 구성 복제 및 동기화

장애 조치 링크에 대한 인터페이스

사용되지 않는 인터페이스(물리적, 이중화 또는 EtherChannel)는 모두 장애 조치 링크로 사용할 수 있습니다. 그러나 현재 이름이 구성된 인터페이스는 지정할 수 없습니다. 장애 조치 링크 인터페이스는 일반적인 네트워킹 인터페이스로 구성되지 않으며, 장애 조치 통신용으로만 존재합니다. 이 인터페이스는 장애 조치 링크용으로만 사용할 수 있습니다(또한 선택에 따라 상태 링크용으로도 사용 가능).

장애 조치 링크 연결

다음 2가지 방법 중 하나를 사용하여 장애 조치 링크를 연결합니다.

- 같은 네트워크 세그먼트(브로드캐스트 도메인 또는 VLAN)에 다른 디바이스가 없는 상태에서 스위치를 ASA의 장애 조치 인터페이스로 사용합니다.
- 외부 스위치를 사용할 필요 없이 이더넷 케이블을 사용하여 유닛을 직접 연결합니다.

유닛 간에 스위치를 사용하지 않으려는 경우 인터페이스에 오류가 발생하면 두 피어에서 링크가 중단됩니다. 이 경우 인터페이스에 오류가 발생하고 링크가 중단된 결과를 초래한 유닛이 어떤 것인지 쉽게 확인할 수 없으므로 문제 해결에 방해될 수 있습니다.

ASA에서는 구리 이더넷 포트의 Auto-MDI/MDIX를 지원하므로 crossover 케이블 또는 straight-through 케이블을 사용할 수 있습니다. Straight-through 케이블을 사용할 경우 인터페이스에서는 케이블을 자동으로 감지하고 송/수신 쌍 중 하나를 MDIX로 교체합니다.

스테이트풀 장애 조치 링크

스테이트풀 장애 조치를 사용하려면 연결 상태 정보를 전달할 스테이트풀 장애 조치 링크(상태 링크라고도 함)를 구성해야 합니다.

상태 링크에 사용 가능한 인터페이스 옵션은 3가지입니다.

- 8-5 페이지의 전용 인터페이스(권장)
- 8-5 페이지의 장애 조치 링크 공유
- 8-5 페이지의 일반 데이터 인터페이스 공유(권장하지 않음)

참고 상태 링크에는 관리 인터페이스를 사용하지 마십시오.

전용 인터페이스(권장)

상태 링크에 전용 인터페이스(물리적, 이중화 또는 EtherChannel)를 사용할 수 있습니다. 다음 두 가지 방법 중 하나를 사용하여 전용 상태 링크를 연결합니다.

- 같은 네트워크 세그먼트(브로드캐스트 도메인 또는 VLAN)에 다른 디바이스가 없는 상태에서 스위치를 ASA의 장애 조치 인터페이스로 사용합니다.
- 외부 스위치를 사용할 필요 없이 이더넷 케이블을 사용하여 어플라이언스를 직접 연결합니다.

  유닛 간에 스위치를 사용하지 않으려는 경우 인터페이스에 오류가 발생하면 두 피어에서 링크가 중단됩니다. 이 경우 인터페이스에 오류가 발생하고 링크가 중단된 결과를 초래한 유닛이 어떤 것인지 쉽게 확인할 수 없으므로 문제 해결에 방해될 수 있습니다.

  ASA에서는 구리 이더넷 포트의 Auto-MDI/MDIX를 지원하므로 crossover 케이블 또는 straight-through 케이블을 사용할 수 있습니다. Straight-through 케이블을 사용할 경우 인터페이스에서는 케이블을 자동으로 감지하고 송/수신 쌍 중 하나를 MDIX로 교체합니다.

장거리 장애 조치를 사용할 경우 최적의 성능을 보장하려면 장애 조치 링크의 레이턴시는 10밀리초 미만이어야 하고 250밀리초를 초과해서는 안 됩니다. 레이턴시가 10밀리초를 초과하는 경우 장애 조치 메시지의 재전송으로 인해 일부 성능이 저하됩니다.

장애 조치 링크 공유

충분한 인터페이스가 없는 경우 장애 조치 링크를 공유해야 할 수 있습니다. 장애 조치 링크를 상태 링크로 사용할 경우 제공되는 가장 빠른 이더넷 인터페이스를 사용해야 합니다. 해당 인터페이스에 성능 문제가 발생할 경우 상태 링크에 별도의 전용 인터페이스를 지정하는 방법을 고려하십시오.

일반 데이터 인터페이스 공유(권장하지 않음)

데이터 인터페이스를 상태 링크와 공유할 경우 재생 공격에 취약해질 수 있습니다. 또한 대량의 스테이트풀 장애 조치 트래픽이 인터페이스에서 전송되어 해당 네트워크 세그먼트에 성능 문제가 발생할 수 있습니다.

데이터 인터페이스를 상태 링크로 사용하는 방법은 단일 컨텍스트, 라우팅 모드에서만 지원됩니다.

장애 조치 및 데이터 링크 중단 방지

장애 조치 링크 및 데이터 인터페이스가 다른 경로를 통해 이동하도록 설정하여 모든 인터페이스에 동시 다발적으로 오류가 발생하는 가능성을 줄이는 것이 좋습니다. 장애 조치 링크가 중단될 경우 ASA에서는 데이터 인터페이스를 사용하여 장애 조치가 필요한지 여부를 확인합니다. 그런 다음 장애 조치 링크 상태가 복원될 때까지는 장애 조치 작업이 보류됩니다.

복원력이 뛰어난 장애 조치 네트워크를 설계하려면 다음 연결 시나리오를 참조하십시오.

시나리오 1 — 권장하지 않음

단일 스위치 또는 스위치 집합을 사용하여 두 ASA 간의 장애 조치 및 데이터 인터페이스를 모두 연결한 상태에서 스위치 또는 스위치 간 링크가 중단될 경우 두 ASA 모두 액티브 상태가 됩니다. 따라서 아래 그림 8-1 및 그림 8-2에 나온 다음 2가지 연결 방법은 권장되지 않습니다.

그림 8-1 단일 스위치로 연결 — 권장하지 않음

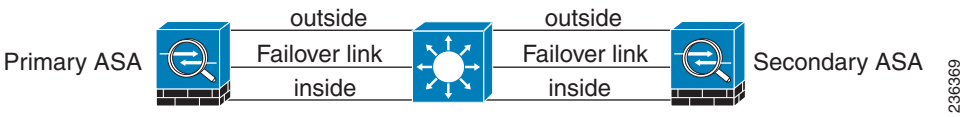
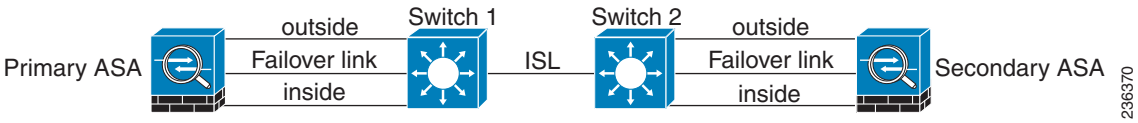


그림 8-2 이중 스위치로 연결 — 권장하지 않음



시나리오 2 — 권장

장애 조치 링크에서는 같은 스위치를 데이터 인터페이스로 사용하지 않는 것이 좋습니다. 대신 그림 8-3 및 그림 8-4에 나와 있는 것처럼 다른 스위치를 사용하거나 직접 케이블을 사용하여 장애 조치 링크에 연결합니다.

그림 8-3 다른 스위치로 연결

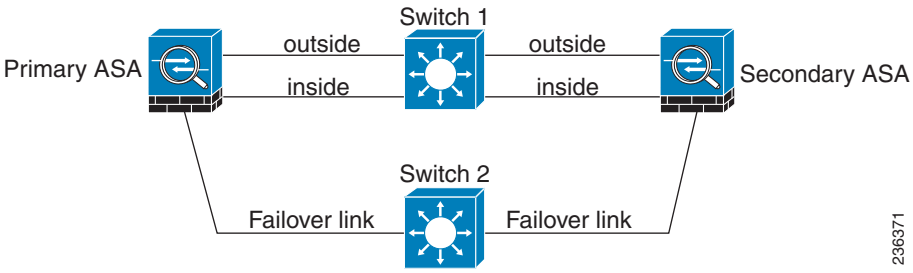
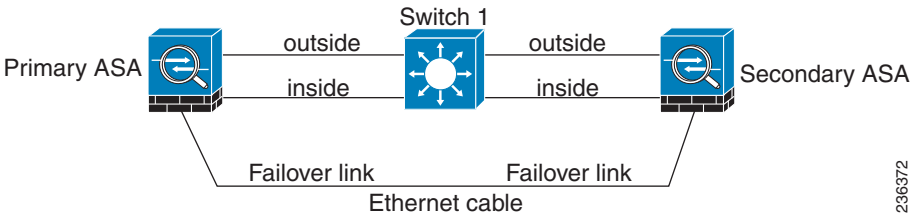


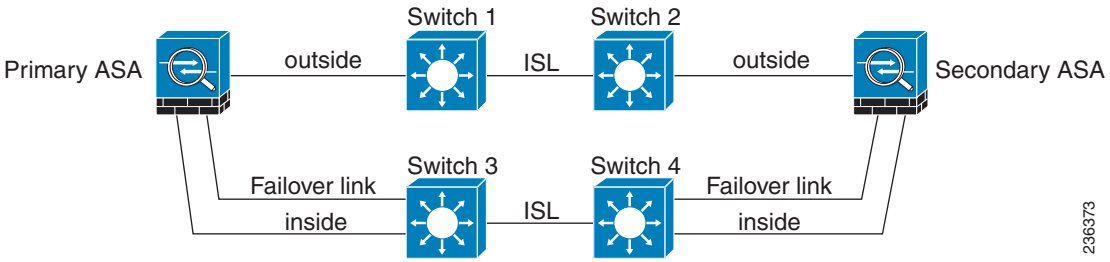
그림 8-4 케이블로 연결



시나리오 3 — 권장

ASA 데이터 인터페이스가 여러 개의 스위치 집합에 연결되어 있는 경우, 장애 조치 링크는 이러한 스위치 중 하나에 연결될 수 있으며 그림 8-5에 나온 것처럼 주로 네트워크의 보안(내부) 측에 있는 스위치일 가능성이 높습니다.

그림 8-5 보안 스위치로 연결



시나리오 4 — 권장

가장 안정적인 장애 조치 컨피그레이션의 경우 그림 8-6 및 그림 8-7에 나와 있는 것처럼 장애 조치 링크에서 이중화 인터페이스를 사용합니다.

그림 8-6 이중화 인터페이스로 연결

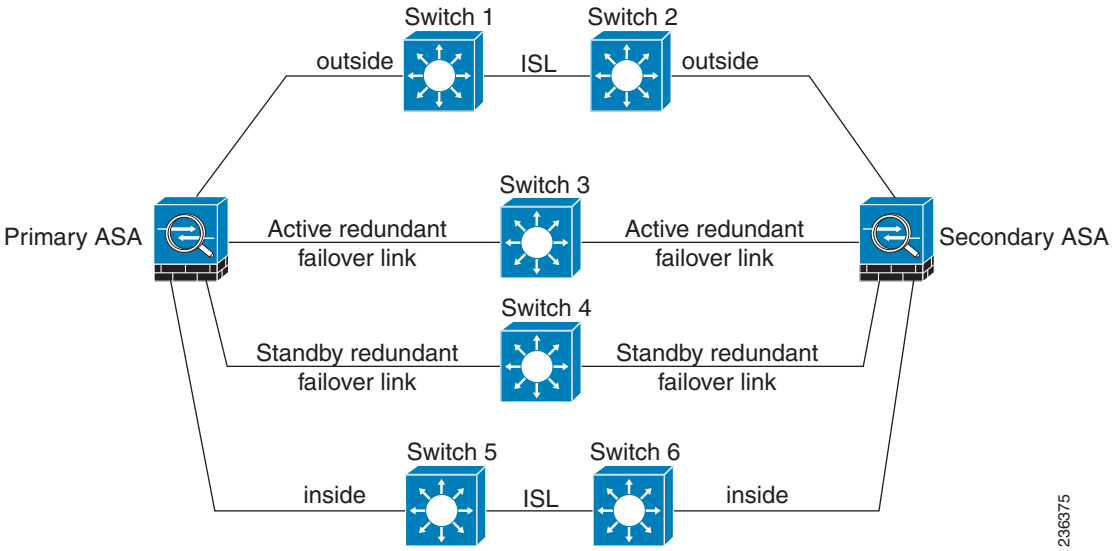
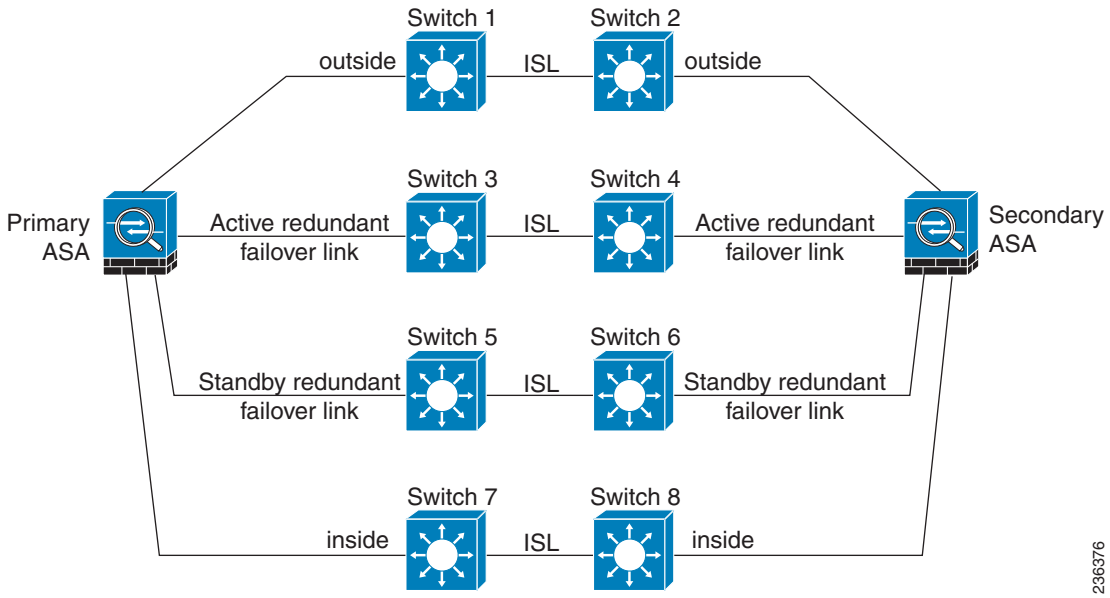


그림 8-7 스위치 간 링크로 연결



MAC 주소와 IP 주소

인터페이스를 구성할 경우, 동일한 네트워크에서 액티브 IP 주소 및 스탠바이 IP 주소를 지정해야 합니다.

1. 기본 유닛 또는 장애 조치 그룹에서 장애 조치를 시작할 경우, 보조 유닛에서는 기본 유닛의 IP 주소와 MAC 주소를 가정하고 트래픽 전달을 시작합니다.
2. 이제 스탠바이 상태가 된 유닛에서는 스탠바이 IP 주소와 MAC 주소를 인수합니다.

네트워크 디바이스에서는 MAC-IP 주소 쌍의 변화가 감지되지 않으므로, 네트워크 어디에서도 ARP 항목의 변경이나 시간 초과가 발생하지 않습니다.

참고 기본 유닛을 감지하지 않고 부팅되는 보조 유닛은 액티브 유닛이 되며 기본 유닛의 MAC 주소를 알지 못하므로 고유한 MAC 주소를 사용합니다. 그러나 기본 유닛이 사용 가능한 상태가 되면 보조(액티브) 유닛에서는 MAC 주소를 기본 유닛의 주소로 변경하므로 이 경우 네트워크 트래픽이 중단될 수 있습니다. 이와 마찬가지로 기본 유닛을 새 하드웨어로 교체할 경우에도 새로운 MAC 주소가 사용됩니다.

시작 시 보조 유닛에 액티브 MAC 주소가 알려지므로 가상 MAC 주소에서는 이러한 중단을 방지하며, 새 기본 유닛 하드웨어가 사용될 경우에도 가상 MAC 주소는 그대로 유지됩니다. 다중 컨텍스트 모드의 경우 ASA에서는 기본적으로 가상 액티브 및 스탠바이 MAC 주소를 생성합니다. 자세한 내용은 7-11 페이지의 MAC 주소에 대한 정보를 참조하십시오. 단일 컨텍스트 모드에서는 가상 MAC 주소를 수동으로 구성할 수 있습니다. 자세한 내용은 8-27 페이지의 액티브/액티브 장애 조치 구성를 참조하십시오.

가상 MAC 주소를 구성하지 않을 경우, 연결된 라우터에서 ARP 테이블을 지워 트래픽 흐름을 복원해야 할 수 있습니다. MAC 주소가 변경될 경우 ASA에서는 고정 NAT 주소에 불필요한 ARP를 전송하지 않으므로, 연결된 라우터에서는 이러한 주소의 MAC 주소 변경을 알지 못합니다.

참고 장애 조치 시 상태 링크의 IP 주소와 MAC 주소는 변경되지 않습니다. 유일한 예외는 상태 링크가 일반 데이터 인터페이스에서 구성된 경우입니다.

ASA Services Module을 위한 Intra-Chassis 및 Inter-Chassis 모듈 배치

기본 및 보조ASASM를 같은 스위치 또는 두 개의 개별 스위치 내에 배치할 수 있습니다. 다음 섹션에서는 각 옵션에 대해 설명합니다.

- 8-9 페이지의 Intra-Chassis 장애 조치
- 8-10 페이지의 Inter-Chassis 장애 조치

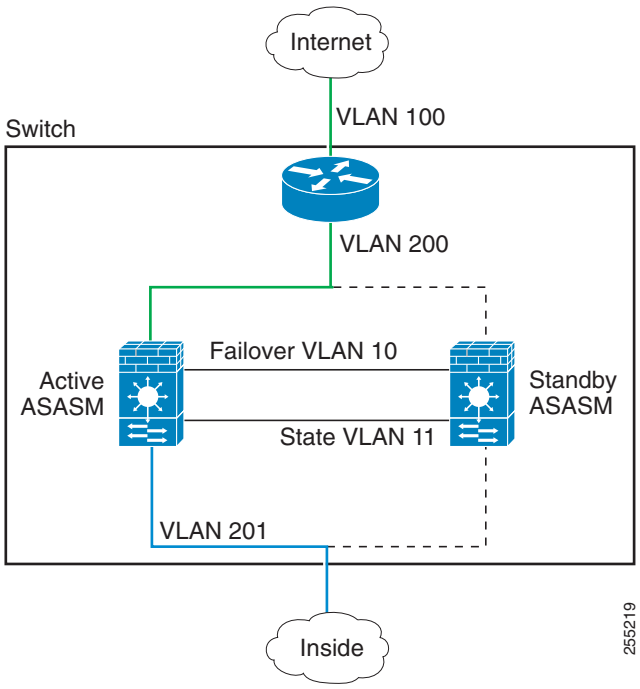
Intra-Chassis 장애 조치

기본 ASASM과 동일한 스위치에서 보조 ASASM을 설치할 경우 모듈 수준 오류를 방지할 수 있습니다. 모듈 수준 오류뿐만 아니라 스위치 수준 오류도 방지하려면 8-10 페이지의 Inter-Chassis 장애 조치를 참조하십시오.

두 ASASM이 모두 같은 VLAN에 할당된 경우에도 액티브 모듈만 네트워킹에 참여합니다. 스탠바이 모듈에서는 어떠한 트래픽도 전달하지 않습니다.

그림 8-8에는 Intra-Switch 컨피그레이션이 나와 있습니다.

그림 8-8 Intra-Switch 장애 조치



Inter-Chassis 장애 조치

스위치 수준 오류를 방지하기 위해 별도의 스위치에 보조 ASASM을 설치할 수 있습니다. ASASM에서는 스위치와 직접 장애 조치를 조정하지 않으나 스위치 장애 조치 작업과 원활하게 연동됩니다. 스위치의 장애 조치를 구성하는 방법에 대한 내용은 스위치 설명서를 참조하십시오.

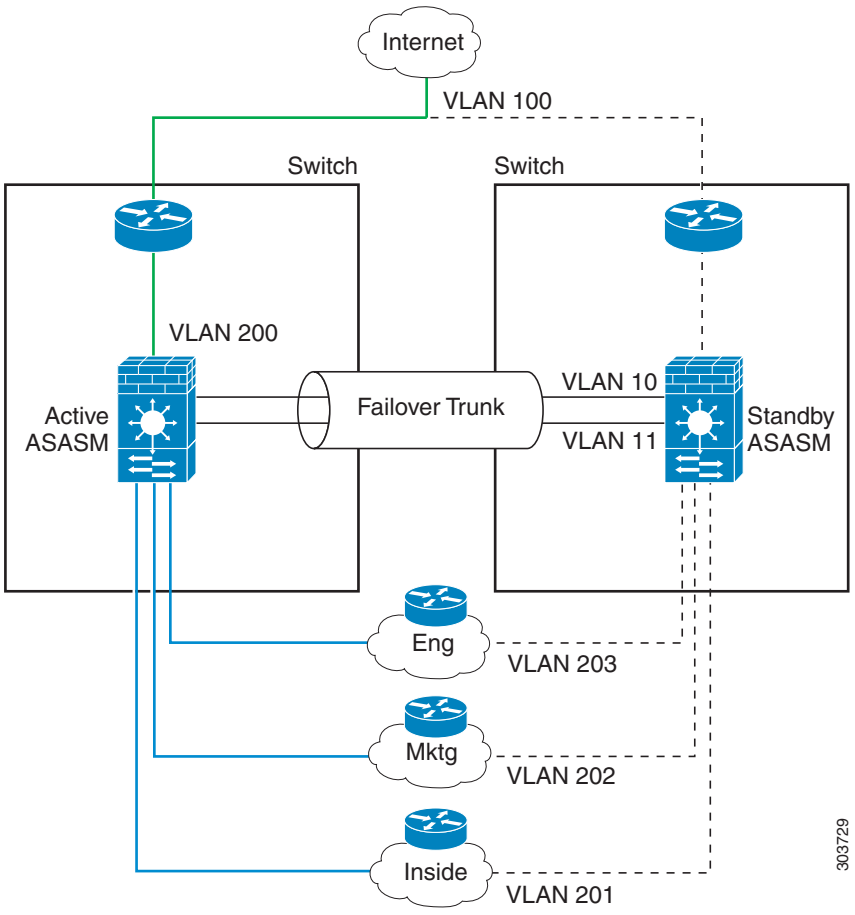
ASASM 간의 장애 조치 통신을 최대한 안정적으로 수행하려면 두 스위치 사이에 EtherChannel 트렁크 포트를 구성하여 장애 조치 및 상태 VLAN을 전송하는 것이 좋습니다.

기타 VLAN의 경우 두 스위치에 모든 방화벽 VLAN에 대한 액세스 권한이 있고, 모니터링된 VLAN에서 두 스위치 간에 hello 패킷을 올바르게 전달할 수 있는지 확인해야 합니다.

그림 8-9에는 일반적인 스위치 및 ASASM 이중화 컨피그레이션이 나와 있습니다. 두 스위치 간의 트렁크에서는 장애 조치 ASASM VLAN(VLAN 10 및 11)을 전송합니다.

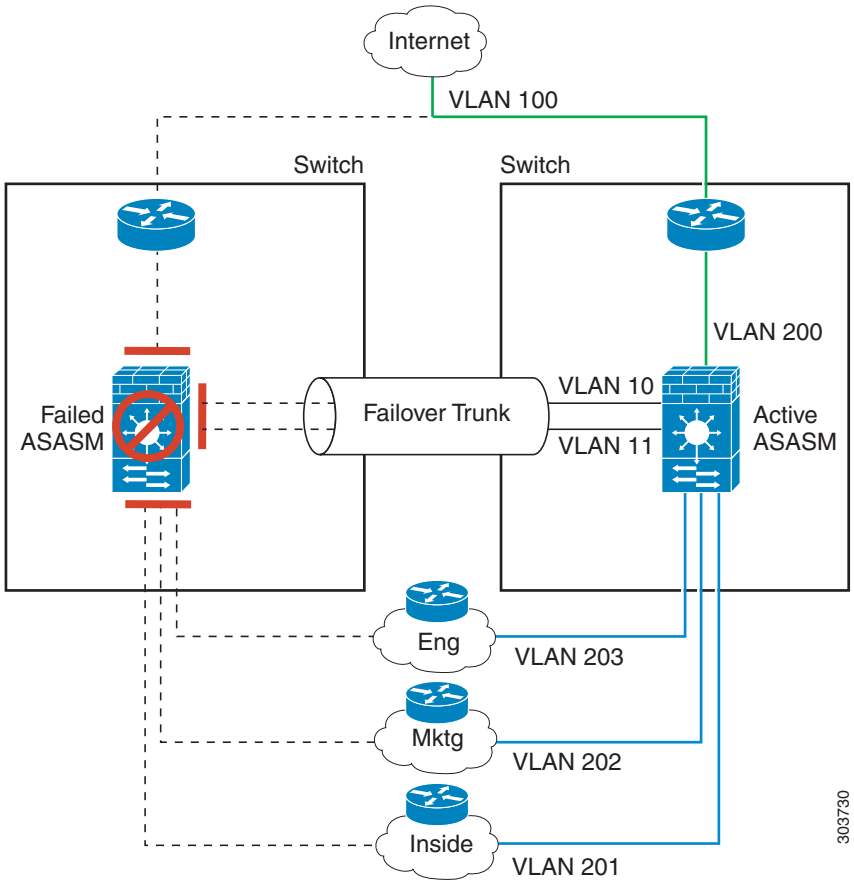
참고 ASASM 장애 조치는 스위치 장애 조치 작업과는 무관하지만, ASASM의 경우 모든 스위치 장애 조치 시나리오에서 작동합니다.

그림 8-9 정상 가동



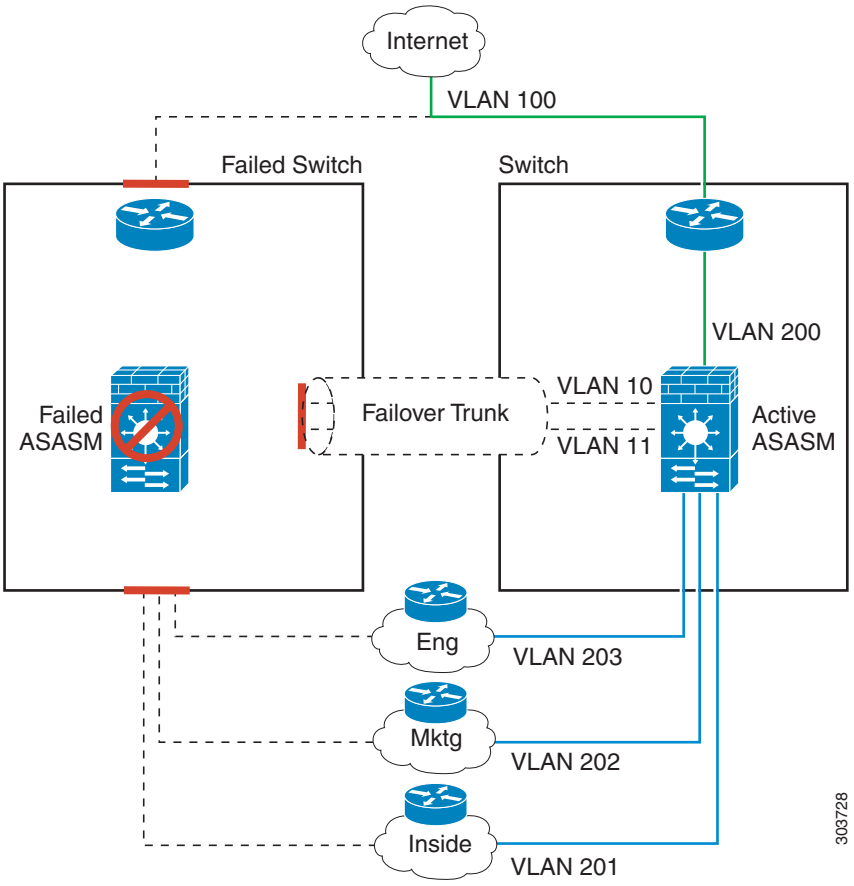
기본 ASASM에 오류가 발생하면 보조 ASASM이 액티브 상태가 되고 방화벽 VLAN을 올바르게 전달합니다(그림 8-10).

그림 8-10 ASASM 오류



ASASM을 비롯한 전체 스위치에 오류가 발생할 경우(예: 정전), 두 스위치 및 ASASM에서는 해당 보조 유닛으로 장애 조치를 시작합니다(그림 8-11).

그림 8-11 스위치 오류



스테이트리스 및 스테이트풀 장애 조치

ASA에서는 액티브/스탠바이 및 액티브/액티브 모드에 대해 두 가지 유형의 장애 조치(스테이트리스 및 스테이트풀)를 지원합니다.

- 8-13 페이지의 스테이트리스 장애 조치
- 8-13 페이지의 스테이트풀 장애 조치

참고 클라이언트리스 SSL VPN의 일부 컨피그레이션 요소(예: 책갈피 및 맞춤화)에서는 스테이트풀 장애 조치의 일부분인 VPN 장애 조치 하위 시스템을 사용합니다. 스테이트풀 장애 조치를 사용하여 상태 조치 쌍의 멤버 간에 이러한 요소를 동기화해야 합니다. 클라이언트리스 SSL VPN에는 스테이트리스 장애 조치를 권장하지 않습니다.

스테이트리스 장애 조치

장애 조치가 일어나면 모든 활성 연결이 손실됩니다. 새 액티브 유닛을 인계받을 경우 클라이언트에서는 연결을 다시 설정해야 합니다.

참고 클라이언트리스 SSL VPN의 일부 컨피그레이션 요소(예: 책갈피 및 맞춤화)에서는 스테이트풀 장애 조치의 일부분인 VPN 장애 조치 하위 시스템을 사용합니다. 스테이트풀 장애 조치를 사용하여 상태 조치 쌍의 멤버 간에 이러한 요소를 동기화해야 합니다. 클라이언트리스 SSL VPN에는 스테이트리스(일반) 장애 조치를 권장하지 않습니다.

스테이트풀 장애 조치

스테이트풀 장애 조치를 활성화한 경우 액티브 유닛에서는 연결당 상태 정보를 스탠바이 유닛으로 전달하거나 액티브/액티브 장애 조치에서 액티브 및 스탠바이 장애 조치 그룹 간에 지속적으로 전달합니다. 장애 조치가 일어난 후에는 새 액티브 유닛에서 동일한 연결 정보를 사용할 수 있습니다. 지원되는 최종 사용자 애플리케이션이 없어도 다시 연결하여 동일한 통신 세션을 그대로 유지할 수 있습니다.

- 8-13 페이지의 지원 기능
- 8-14 페이지의 지원되지 않는 기능

지원 기능

스테이트풀 장애 조치가 활성화될 경우 다음 상태 정보가 스탠바이 ASA에 전달됩니다.

- NAT 변환 테이블
- TCP 연결 상태
- UDP 연결 상태
- ARP 테이블
- 레이어 2 브릿지 테이블(투명 방화벽 모드에서 실행 중일 경우)
- HTTP 연결 상태(HTTP 복제가 활성화된 경우) — 기본적으로 ASA에서는 스테이트풀 장애 조치가 활성화된 경우 HTTP 세션을 복제하지 않습니다. 보통 HTTP 클라이언트에서는 오류가 발생한 연결을 다시 수행하려고 시도하기 때문에 HTTP 세션은 짧은 것이 일반적입니다. 따라서 HTTP 세션을 복제하지 않을 경우 중요한 데이터 또는 연결이 손실되지 않으면서 시스템 성능이 향상됩니다.
- ISAKMP 및 IPsec SA 테이블
- GTP PDP 연결 데이터베이스
- SIP 신호 세션
- ICMP 연결 상태 — ICMP 연결 복제는 해당 인터페이스가 비대칭 라우팅 그룹에 할당된 경우에만 활성화됩니다.
- 동적 라우팅 프로토콜 — 스테이트풀 장애 조치는 OSPF 및 EIGRP 같은 동적 라우팅 프로토콜에 참여하므로, 액티브 유닛에서 동적 라우팅 프로토콜을 통해 얻은 경로는 스탠바이 유닛의 RIB(라우팅 정보 베이스) 테이블에 유지됩니다. 장애 조치 이벤트 발생 시, 액티브 보조 ASA에서는 초기 규칙에 따라 기본 ASA를 미러링하므로 중단을 최소화면서도 패킷이 정상적으로 이동됩니다. 장애 조치가 끝난 직후에는 새로운 액티브 유닛에서 재통합 타이머가 시작됩니다. 그러면 RIB 테이블의 시간대 숫자가 늘어납니다. 재통합을 수행하는 동안 OSPF 및 EIGRP 경로는 새 시간대 숫자로 업데이트됩니다. 타이머가 만료되면 오래된 경로 항목(시간대 숫자에 의해 결정됨)이 테이블에서 제거됩니다. 그런 다음 RIB에 새 액티브 유닛에 대한 최신 라우팅 프로토콜 전달 정보가 포함됩니다.

참고 경로는 액티브 유닛의 링크 작동 또는 링크 중단 이벤트가 있을 경우에만 동기화됩니다. 스탠바이 유닛에서 링크가 작동하거나 중단될 경우, 액티브 유닛에서 전송된 동적 경로가 손실될 수 있습니다. 이는 일반적이고 정상적인 동작입니다.

- Cisco IP SoftPhone 세션 — 액티브 Cisco IP SoftPhone 세션 도중 장애 조치가 일어날 경우, 통화 세션 상태 정보가 스탠바이 유닛에 복제되므로 통화는 활성 상태로 유지됩니다. 통화가 종료되면 IP SoftPhone 클라이언트와 Cisco Call Manager의 연결이 해제됩니다. 이러한 연결 손실이 일어나는 이유는 스탠바이 유닛에 CTIQBE 끊기 메시지에 대한 세션 정보가 없기 때문입니다. Call Manager에서 다시 보내는 응답이 특정 시간 내에 IP SoftPhone 클라이언트에 수신되지 않을 경우, 해당 Call Manager는 전달 불가능 상태로 간주되며 자체적으로 등록이 해제됩니다.
- VPN — VPN 최종 사용자는 장애 조치 후 VPN 세션을 다시 인증하거나 다시 연결하지 않아도 됩니다. 그러나 VPN 연결을 통해 작동하는 애플리케이션의 경우 장애 조치 프로세스 도중 패킷이 손실될 수 있으며 패킷이 손실되면 복구되지 않습니다.

지원되지 않는 기능

스테이트풀 장애 조치가 활성화될 경우 다음 상태 정보가 스탠바이 ASA에 전달되지 *않습니다*.

- HTTP 연결 케이블(HTTP 복제를 활성화지 않은 경우)
- 사용자 인증(uauth) 테이블
- 고급 TCP 상태 추적이 적용되는 애플리케이션 감시 — 이러한 연결의 TCP 상태는 자동으로 복제되지 않습니다. 이러한 연결이 스탠바이 유닛에 복제되는 동안 TCP 상태를 다시 설정하기 위한 최상의 시도가 이루어집니다.
- DHCP 서버 주소 리스
- ASA IPS SSP 또는 ASA CX SSP 같은 모듈의 상태 정보
- 전화 프록시 연결 — 액티브 유닛이 중단될 경우, 통화가 되지 않으며 미디어의 흐름이 중단됩니다. 오류가 발생한 유닛에서 해당 전화의 등록을 해제하고 액티브 유닛에 대한 등록도 취소해야 합니다. 통화를 다시 설정해야 합니다.
- 선택한 클라이언트 리스 SSL VPN 기능:
  - 스마트 터널
  - 포트 전달
  - 플러그인
  - Java 애플릿
  - IPv6 클라이언트리스 또는 AnyConnect 세션
  - Citrix 인증(Citrix 사용자는 장애 조치 후 다시 인증을 수행해야 함)

투명 방화벽 모드 요구 사항

- 8-15 페이지의 어플라이언스에 대한 투명 모드 요구 사항
- 8-15 페이지의 모듈의 투명 모드 요구 사항

어플라이언스에 대한 투명 모드 요구 사항

액티브 유닛에서 스탠바이 유닛으로 장애 조치를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 연결된 스위치 포트에서는 토폴로지 변경을 인지하는 경우 30~50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 트래픽 손실을 방지하려면 스위치 포트 모드에 따라 다음 해결 방법 중 하나를 구성하십시오.

- 액세스 모드—스위치에서 STP PortFast 기능을 활성화합니다.

  ```
  interface interface_id
    spanning-tree portfast
  ```

  PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.

- 트렁크 모드 — EtherType 규칙이 있는 내부 및 외부 인터페이스에서 ASA의 BPDU를 차단합니다.

  BPDU를 차단하면 스위치의 STP가 비활성화됩니다. 네트워크 레이아웃에 ASA와 관련된 루프가 없도록 해야 합니다.

위의 옵션이 모두 가능하지 않을 경우, 다음 해결 방법 중 하나를 사용할 수 있으며 이 경우 장애 조치 기능 또는 STP 안정성에 다소 영향을 미치게 됩니다.

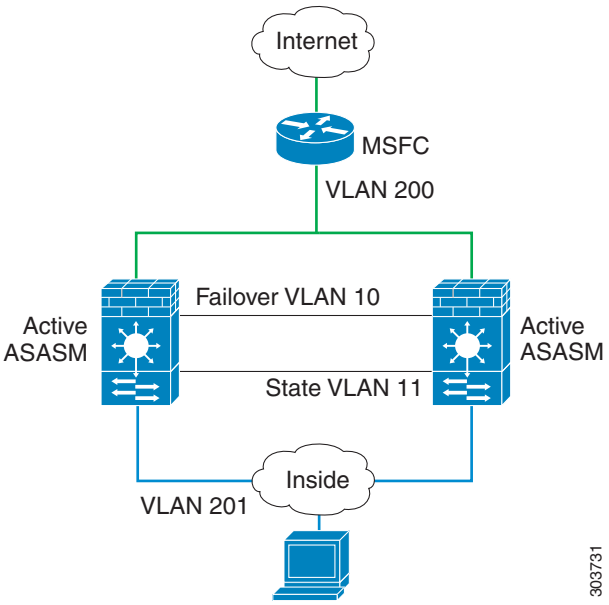
- 인터페이스 모니터링을 비활성화합니다.
- 인터페이스 대기 시간을 큰 값으로 늘려 ASA에서 장애 조치를 수행하기 전에 STP가 통합될 수 있도록 합니다.
- STP 타이머를 줄여 STP가 인터페이스 대기 시간보다 빨리 통합될 수 있도록 합니다.

모듈의 투명 모드 요구 사항

투명 모드에서 장애 조치를 사용할 경우 루프를 방지하려면 BPDU가 전달되도록 해야 하며(기본값), BPDU 전달을 지원하는 스위치 소프트웨어를 사용해야 합니다.

두 모듈이 동시에 활성 상태이거나(예: 두 모듈에서 서로의 존재를 인지할 경우), 장애 조치 링크에 오류가 발생한 경우 루프가 발생할 수 있습니다. ASASM에서는 동일한 두 개의 VLAN 간의 패킷을 연결하므로, 외부로 전달되어야 할 내부 패킷이 ASASM에 의해 끊임없이 복제될 경우 루프가 발생할 수 있습니다(그림 8-12 참조). BPDU가 적시에 교환되는 경우 Spanning Tree Protocol에서는 이러한 루프를 끊을 수 있습니다. 루프를 끊으려면 VLAN 200과 VLAN 201 간에 전송된 BPDU를 연결해야 합니다.

그림 8-12 투명 모드 루프



장애 조치 상태 모니터링

ASA에서는 각 유닛의 전체 상태 및 인터페이스 상태를 모니터링합니다. 이 섹션에는 ASA에서 각 유닛의 상태를 확인하기 위해 테스트를 수행하는 방법에 대한 정보가 포함되어 있습니다.

- 8-16 페이지의 유닛 상태 모니터링
- 8-17 페이지의 인터페이스 모니터링

유닛 상태 모니터링

ASA에서는 장애 조치 링크를 모니터링하여 다른 유닛의 상태를 확인합니다. 장애 조치 링크에서 hello 메시지가 유닛에 3번 연속으로 수신되지 않는 경우, 유닛에서는 장애 조치 링크를 비롯한 각 데이터 인터페이스에 인터페이스 hello 메시지를 전송하여 피어의 응답 여부를 확인합니다. ASA에서 취하는 조치는 다른 유닛의 응답에 따라 달라집니다. 아래의 가능한 조치를 참조하십시오.

- ASA에서 장애 조치 링크에 대한 응답을 수신하지 못할 경우 장애 조치가 이루어지지 않습니다.
- ASA에서 장애 조치 링크에 대한 응답은 수신하지 못했으나 데이터 인터페이스에 대한 응답은 수신한 경우, 유닛에서 장애 조치를 수행하지 않습니다. 장애 조치 링크가 실패한 것으로 표시됩니다. 장애 조치 링크가 중단된 동안에는 유닛에서 스탠바이 유닛으로 장애 조치할 수 없으므로 최대한 빨리 장애 조치 링크를 복원해야 합니다.
- ASA에서 인터페이스에 대한 응답을 받지 못한 경우 스탠바이 유닛은 액티브 모드로 전환되고 다른 유닛을 실패한 것으로 분류합니다.

인터페이스 모니터링

최대 250개의 인터페이스를 모니터링할 수 있습니다(다중 모드에서 해당되며 모든 컨텍스트 간에 분할됨). 중요한 인터페이스를 모니터링해야 합니다. 예를 들어, 다중 모드에서는 하나의 컨텍스트를 구성하여 공유 인터페이스를 공유할 수 있습니다. (인터페이스가 공유되므로 모든 컨텍스트에서는 모니터링으로 인한 이점을 누릴 수 있습니다.)

구성된 대기 시간의 절반 동안 모니터링된 인터페이스에 대한 hello 메시지가 유닛에 수신되지 않을 경우 다음과 같은 테스트가 실행됩니다.

1. 링크 작동/중단 테스트 — 인터페이스 상태에 대한 테스트입니다. 링크 작동/중단 테스트는 인터페이스가 작동 중인지 여부를 나타내며 ASA에서는 네트워크 테스트를 수행합니다. 이 테스트의 목적은 네트워크 트래픽을 생성하여 어떤 유닛에서 오류가 발생했는지 확인하는 것입니다. 각 테스트를 시작할 때마다 각 유닛에서는 해당 인터페이스에 대한 수신된 패킷 수를 지웁니다. 각 테스트를 종료할 때마다 각 유닛에서는 수신된 트래픽이 있는지 확인합니다. 수신된 트래픽이 있는 경우 인터페이스가 제대로 작동 중인 것으로 간주합니다. 한 유닛에는 테스트용 트래픽이 수신되고 다른 유닛에는 수신되지 않을 경우, 트래픽이 수신되지 않은 유닛은 오류가 발생한 것으로 간주합니다. 모든 유닛에 트래픽이 수신되지 않을 경우 다음 테스트가 사용됩니다.
2. 네트워크 활동 테스트 — 수신된 네트워크 활동 테스트입니다. 유닛에서는 최대 5초 동안 수신된 모든 패킷의 수를 셉니다. 이 간격 동안 언제라도 수신된 패킷이 있을 경우 인터페이스가 작동 중인 것으로 간주되며 테스트가 중지됩니다. 트래픽이 수신되지 않으면 ARP 테스트가 시작됩니다.
3. ARP 테스트 — 가장 최근에 얻은 항목 2개의 유닛 ARP 캐시를 읽는 테스트입니다. 유닛에서는 한 번에 하나씩 ARP 요청을 이러한 시스템에 전송하여 네트워크 트래픽의 시뮬레이션을 시도합니다. 각 요청 후 유닛에서는 최대 5초 동안 수신된 모든 트래픽의 수를 셉니다. 트래픽이 수신된 경우 해당 인터페이스는 제대로 작동 중인 것으로 간주합니다. 트래픽이 수신되지 않은 경우, ARP 요청이 다음 시스템에 전송됩니다. 목록 마지막에 트래픽이 수신되지 않은 경우 Ping 테스트가 시작됩니다.
4. 브로드캐스트 Ping 테스트 — 브로드캐스트 Ping 요청을 전송하는 작업으로 이루어진 Ping 테스트입니다. 그런 다음 유닛에서는 최대 5초 동안 수신된 모든 패킷의 수를 셉니다. 이 간격 동안 언제라도 수신된 패킷이 있을 경우 인터페이스가 작동 중인 것으로 간주되며 테스트가 중지됩니다.

모니터링한 인터페이스에는 다음과 같은 상태가 표시될 수 있습니다.

- Unknown — 초기 상태입니다. 이 상태는 상태를 확인할 수 없다는 의미이기도 합니다.
- Normal — 인터페이스에서 트래픽을 수신 중입니다.
- Testing — 5번의 폴링 시간 동안 Hello 메시지가 인터페이스에서 수신되지 않습니다.
- Link Down — 인터페이스 또는 VLAN의 관리 상태가 중단되었습니다.
- No Link — 인터페이스의 물리적 링크가 중단되었습니다.
- Failed — 인터페이스에 트래픽이 수신되지 않았으나, 피어 인터페이스에는 트래픽이 수신되었습니다.

인터페이스에 구성된 IPv4 및 IPv6 주소가 없는 경우 ASA에서는 IPv4 주소를 사용하여 상태 모니터링을 수행합니다.

인터페이스에 IPv6 주소만 구성된 경우 ASA에서는 ARP 대신 IPv6 인접 검색을 사용하여 상태 모니터링 테스트를 수행합니다. 브로드캐스트 Ping 테스트의 경우 ASA에서는 IPv6의 모든 노드 주소를 사용합니다(FE02::1).

인터페이스에 대한 모든 네트워크 테스트가 실패하였으나 다른 유닛에 있는 이 인터페이스에서는 지속적으로 트래픽을 전달할 수 있는 경우, 해당 인터페이스는 오류가 발생한 것으로 간주합니다. 오류가 발생한 인터페이스의 임계값이 충족될 경우 장애 조치가 실행됩니다. 다른 유닛 인터페이스에서도 모든 네트워크 테스트가 실패할 경우, 두 인터페이스 모두 "Unknown" 상태가 되며 장애 조치 제한에 대한 계산을 수행하지 않습니다.

트래픽이 수신될 경우 인터페이스는 다시 작동을 시작합니다. 인터페이스 오류 임계값이 더 이상 충족되지 않을 경우 오류가 발생한 ASA는 스탠바이 모드로 돌아갑니다.

참고 오류가 발생한 유닛에서 복구가 이루어지지 않고 오류가 발생해서는 안 되는 유닛일 경우 **failover reset** 명령을 입력하여 상태를 재설정할 수 있습니다. 그러나 장애 조치 상태가 지속되면 유닛에 다시 오류가 발생합니다.

장애 조치 시간

표 8-1에 최소, 기본 및 최대 장애 조치 시간이 나와 있습니다.

표 8-1 ASA 장애 조치 시간

장애 조치 상태	최소	기본	최대
액티브 유닛의 전원이 중단되거나 정상적인 작동이 중지됩니다.	800밀리초	15초	45초
액티브 유닛 메인 보드 인터페이스 링크가 중단됩니다.	500밀리초	5초	15초
액티브 유닛 4GE 모듈 인터페이스 링크가 중단됩니다.	2초	5초	15초
액티브 유닛 IPS 또는 CSC 모듈에 오류가 발생합니다.	2초	2초	2초
액티브 유닛 인터페이스가 작동되지만 연결 문제로 인해 인터페이스 테스트가 실행됩니다.	5초	25초	75초

구성 동기화

장애 조치에는 2가지 유형의 컨피그레이션 동기화가 포함됩니다.

- 8-18 페이지의 실행 중인 구성 복제
- 8-19 페이지의 명령 복제

실행 중인 구성 복제

하나 또는 두 디바이스가 모두 장애 조치 쌍 부팅 중일 경우 실행 중인 컨피그레이션이 복제됩니다. 구성은 액티브 유닛에서 스탠바이 유닛으로 항상 동기화됩니다. 스탠바이 유닛에서 초기 시작을 완료하면 실행 중인 컨피그레이션이 지워지며(장애 조치 명령과 액티브 유닛이 통신을 수행해야 하는 경우는 예외), 액티브 유닛에서는 전체 컨피그레이션을 스탠바이 유닛으로 보냅니다.

복제가 시작되면 액티브 유닛의 ASA 콘솔에는 "Beginning configuration replication: Sending to mate"는 메시지가 표시되며, 이 작업이 완료되면 ASA에서는 "End Configuration Replication to mate"라는 메시지를 표시합니다. 컨피그레이션의 크기에 따라 복제가 완료되기까지 몇 초에서 몇 분이 걸릴 수 있습니다.

스탠바이 유닛에서 컨피그레이션은 실행 중인 메모리에만 존재합니다. 따라 컨피그레이션을 플래시 메모리에 저장해야 합니다.

참고 복제가 실행되는 동안 액티브 유닛에 입력된 명령은 스탠바이 유닛에 제대로 복제되지 않을 수 있으며, 스탠바이 유닛에 입력된 명령은 액티브 유닛에서 복제한 컨피그레이션으로 덮어쓰기 될 수 있습니다. 컨피그레이션 복제 프로세스가 진행되는 동안에는 유닛에 명령을 입력하지 마십시오.

참고 **crypto ca server** 명령 및 관련 하위 명령은 장애 조치 피어에 동기화되지 않습니다.

참고 컨피그레이션 동기화 시 다음 파일 및 컨피그레이션 요소는 복제되지 않으므로, 이러한 파일을 수동으로 복사하여 일치시켜야 합니다.

- AnyConnect 이미지
- CSD 이미지
- AnyConnect 프로파일
- 로컬 CA(Certificate Authority)
- ASA 이미지
- ASDM 이미지

명령 복제

시작 후 액티브 유닛에 입력하는 메시지는 스탠바이 유닛에 즉시 복제됩니다.액티브 컨피그레이션을 플래시 메모리에 저장하여 명령을 복제하지 않아도 됩니다.

액티브/액티브 장애 조치의 경우,실행 영역에 입력된 명령 변경 사항은 유닛에서 활성 상태인 장애 조치 그룹 1로 복제됩니다.

명령 복제를 실행할 해당 유닛에 변경 사항을 입력하지 못할 경우 컨피그레이션이 동기화되지 않습니다. 이러한 변경 사항은 다음번에 초기 컨피그레이션 동기화가 실행될 때 손실될 수 있습니다.

다음 명령어는 스탠바이 ASA에 복제됩니다.

- **mode**, **firewall**, **failover lan unit**을 제외한 모든 컨피그레이션 명령
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

다음 명령어는 스탠바이 ASA에 복제되지 *않습니다*.

- **copy running-config startup-config**을 제외한 모든 형태의 **copy** 명령
- **write memory**를 제외한 모든 형태의 **write** 명령
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** and **pager**

액티브/스탠바이 장애 조치

액티브/스탠바이 장애 조치에서는 스탠바이 ASA를 사용해 실패한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛이 실패하면 스탠바이 상태로 변경되며, 스탠바이 유닛은 액티브 상태로 변경됩니다.

참고 다중 컨텍스트 모드의 경우 ASA에서는 전체 유닛(모든 컨텍스트 포함)으로 장애 조치를 실행할 수 있으나 개별 컨텍스트를 대상으로 별도로 장애 조치를 수행할 수는 없습니다.

- 8-20 페이지의 기본/보조 역할 및 액티브/스탠바이 상태
- 8-20 페이지의 시작 시 액티브 유닛 결정
- 8-21 페이지의 장애 조치 이벤트

기본/보조 역할 및 액티브/스탠바이 상태

장애 조치 쌍에서 두 유닛 간의 주요 차이점은 어느 유닛이 액티브 유닛에 연결되어 있고 어느 유닛이 스탠바이 유닛에 연결되어 있는지와 관련이 있으며 즉, 다시 말해 어떤 IP 주소를 사용하고 어떤 유닛에서 트래픽을 능동적으로 전달하는지에 달려 있습니다.

그러나 유닛 간의 몇몇 차이점은 어느 유닛이 기본(컨피그레이션에 지정된 사항에 따라) 유닛이고 어느 유닛이 보조 유닛인지에 따라서도 결정됩니다.

- 두 유닛이 동시에 시작되고 둘 다 정상적인 상태로 작동될 경우 기본 유닛은 항상 액티브 유닛이 됩니다.
- 기본 유닛의 MAC 주소는 액티브 IP 주소와 항상 연계됩니다. 보조 유닛이 액티브 유닛이 되고 장애 조치 링크를 통해 기본 유닛의 MAC 주소를 수신할 수 없는 경우에는 이러한 규칙에 예외가 발생합니다. 이 경우 보조 유닛의 MAC 주소가 사용됩니다.

시작 시 액티브 유닛 결정

액티브 유닛은 다음에 따라 결정됩니다.

- 유닛이 부팅되고 이미 액티브로 실행 중인 피어가 감지된 경우, 해당 유닛은 스탠바이 유닛이 됩니다.
- 유닛이 부팅되고 피어가 감지되지 않은 경우 해당 유닛은 액티브 유닛이 됩니다.
- 두 유닛이 동시에 부팅될 경우 기본 유닛이 액티브 유닛이 되고 보조 유닛은 스탠바이 유닛이 됩니다.

장애 조치 이벤트

액티브/스탠바이 장애 조치 시 장애 조치는 유닛을 기준으로 실행됩니다. 다중 컨텍스트 모드에서 실행 중인 시스템에서도 개별 또는 컨텍스트 그룹으로는 장애 조치를 수행할 수 없습니다.

표 8-2에는 각 장애 조치 이벤트에 대한 장애 조치가 나와 있습니다. 이 표에는 각 장애 조치 이벤트에 적용되는 장애 조치 정책(장애 조치 실행 또는 장애 조치 없음), 액티브 유닛에서 시행한 조치, 스탠바이 유닛에서 시행한 조치, 장애 조치 조건 및 각 조치에 대한 특별 참고 사항이 나와 있습니다.

표 8-2 장애 조치 동작

오류 이벤트	정책	액티브 조치	스탠바이 조치	참고
액티브 유닛 오류(전력 또는 하드웨어)	장애 조치	N/A	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	모니터링된 인터페이스 또는 장애 조치 링크에 대한 hello 메시지가 수신되지 않음
이전 액티브 유닛 복구	장애 조치 없음	스탠바이 상태가 됨	조치 없음	없음
스탠바이 유닛 오류(전력 또는 하드웨어)	장애 조치 없음	스탠바이가 실패한 것으로 표시됨	N/A	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 장애 조치를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.
작동 중 장애 조치 링크에 오류 발생	장애 조치 없음	장애 조치 링크가 실패한 것으로 표시됨	장애 조치 링크가 실패한 것으로 표시됨	장애 조치가 중단된 동안에는 유닛에서 스탠바이 유닛으로 장애 조치를 시작하지 못하므로 최대한 빨리 장애 조치 링크를 복구해야 합니다.
시작 시 장애 조치 링크에 오류 발생	장애 조치 없음	장애 조치 링크가 실패한 것으로 표시됨	액티브 상태가 됨	시작 시 장애 조치 링크가 중단되면 두 유닛 모두 액티브 상태가 됩니다.
상태 링크 오류 발생	장애 조치 없음	조치 없음	조치 없음	장애 조치가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
임계값을 넘은 액티브 유닛에서 인터페이스 오류 발생	장애 조치	액티브가 실패한 것으로 표시됨	액티브 상태가 됨	없음
임계값을 넘은 스탠바이 유닛에서 인터페이스 오류 발생	장애 조치 없음	조치 없음	스탠바이가 실패한 것으로 표시됨	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 장애 조치를 시도하지 않으며 인터페이스 장애 조치 임계값을 넘은 경우에도 마찬가지입니다.

액티브/액티브 장애 조치 정보

이 섹션에서는 액티브/액티브 장애 조치에 대해 설명합니다.

- 8-22 페이지의 액티브/액티브 장애 조치 개요
- 8-22 페이지의 장애 조치 그룹의 기본/보조 역할 및 액티브/스탠바이 상태
- 8-23 페이지의 장애 조치 이벤트

액티브/액티브 장애 조치 개요

액티브/액티브 장애 조치 컨피그레이션에서는 두 ASA에서 모두 네트워크 트래픽을 전달할 수 있습니다. 액티브/액티브 장애 조치는 다중 컨텍스트 모드의 ASA에만 사용할 수 있습니다. 액티브/액티브 장애 조치에서 ASA의 보안 컨텍스트는 최대 2개의 장애 조치 그룹으로 나뉩니다.

장애 조치 그룹은 단순히 하나 이상의 보안 컨텍스트로 구성된 논리적 그룹입니다. 기본 ASA에서 액티브 상태가 되는 장애 조치 그룹 1을 할당하고 보조 ASA에서 액티브 상태가 되는 장애 조치 그룹 2를 할당할 수 있습니다. 장애 조치는 장애 조치 그룹 수준에서 수행됩니다. 예를 들어, 인터페이스 오류 패턴에 따라 장애 조치 그룹 1에서 보조 ASA로 장애 조치를 실행하고, 그 후 장애 조치 그룹 2에서 기본 ASA로 장애 조치를 실행할 수 있습니다. 장애 조치 그룹 1의 인터페이스가 기본 ASA에서 중단되었으나 보조 ASA에서 작동 중이고, 장애 조치 그룹 2의 인터페이스가 보조 ASA에서는 중단되었으나 기본 ASA에서 작동 중인 경우 이러한 이벤트가 발생할 수 있습니다.

관리자 컨텍스트는 항상 장애 조치 그룹 1의 멤버입니다. 또한 할당되지 않은 모든 보안 컨텍스트도 기본적으로 장애 조치 그룹 1의 멤버입니다. 액티브/액티브 장애 조치만 수행하고 다중 컨텍스트는 사용하지 않으려는 경우, 가장 간단한 컨피그레이션 방법은 추가 컨텍스트 1개를 추가하고 이를 장애 조치 그룹 2에 할당하는 것입니다.

참고 액티브/액티브 장애 조치를 구성할 경우 두 유닛의 통합된 트래픽이 각 유닛의 용량 내에 있는지 확인해야 합니다.

참고 원하는 경우 두 장애 조치 그룹을 하나의 ASA에 할당할 수 있지만 이렇게 하면 두 액티브 ASA의 장점을 활용할 수 없게 됩니다.

장애 조치 그룹의 기본/보조 역할 및 액티브/스탠바이 상태

액티브/스탠바이 장애 조치와 마찬가지로, 액티브/액티브 장애 조치 쌍에서 한 유닛은 기본 유닛으로 지정되고 다른 유닛은 보조 유닛으로 지정됩니다. 그러나 액티브/스탠바이 장애 조치와 달리, 기본 유닛과 보조 유닛이 지정되어도 두 유닛이 동시에 시작될 때 어느 유닛이 액티브 유닛이 되는지를 나타내지는 않습니다. 그 대신 기본/보조 유닛을 지정하는 작업에서는 다음 두 가지 역할을 수행합니다.

- 동시에 부팅이 시작될 경우 기본 유닛에서는 실행 중인 컨피그레이션을 해당하는 쌍에 제공합니다.
- 컨피그레이션의 각 장애 조치 그룹은 기본 또는 보조 유닛 기본 설정으로 컨피그레이션됩니다.

시작 시 장애 조치 그룹에 대한 액티브 유닛 결정

장애 조치 그룹에서 액티브 유닛이 되는 유닛은 다음에 따라 결정됩니다.

- 피어 유닛이 제공되지 않을 때 유닛이 부팅될 경우, 두 장애 조치 그룹은 유닛에서 활성 상태가 됩니다.
- 피어 유닛이 액티브 상태일 때(두 장애 조치 그룹이 모두 활성 상태일 때) 유닛이 부팅될 경우, 장애 조치 그룹의 기본 또는 보조 기본 설정에 상관없이 장애 조치 그룹은 액티브 유닛에서 활성 상태를 유지하며 이는 다음 중 한 가지 상황이 발생하지 않는 한 유효합니다.
  - 장애 조치가 발생할 경우
  - 장애 조치를 수동으로 강제 실행할 경우

  - 장애 조치 그룹의 사전 대응 방식을 구성한 경우. 이 경우 유닛이 사용 가능한 상태가 되었을 때 장애 조치 그룹이 기본 유닛에서 자동으로 액티브 상태가 됨
- 두 유닛이 동시에 부팅될 때, 컨피그레이션 동기화 후 각 장애 조치 그룹이 기본 유닛에서 액티브 상태가 된 경우

장애 조치 이벤트

액티브/액티브 장애 조치 컨피그레이션에서 장애 조치는 시스템이 아닌 장애 조치 그룹을 기준으로 실행됩니다. 예를 들어, 기본 유닛에서 두 장애 조치 그룹을 모두 액티브로 지정할 경우 장애 조치 그룹 1에 오류가 발생하면 장애 조치 그룹 2는 기본 유닛에서 액티브 상태를 유지하는 반면 장애 조치 그룹 1은 보조 유닛에서 액티브 상태가 됩니다.

장애 조치 그룹에는 다중 컨텍스트를 포함할 수 있고 각 컨텍스트에는 여러 인터페이스가 포함될 수 있으므로, 관련된 장애 조치 그룹에 오류가 발생하는 대신 단일 컨텍스트 내의 모든 인터페이스에 오류가 발생할 수 있습니다.

표 8-3에는 각 장애 조치 이벤트에 대한 장애 조치가 나와 있습니다. 이 표에는 각 오류 이벤트에 대한 정책(장애 조치의 실행 여부 결정), 액티브 장애 조치 그룹에 대한 조치, 스탠바이 장애 조치 그룹에 대한 조치가 나와 있습니다.

표 8-3 액티브/액티브 장애 조치에 대한 장애 조치 동작

오류 이벤트	정책	액티브 그룹 조치	스탠바이 그룹 조치	참고
유닛에 전원 또는 소프트웨어 오류가 발생함	장애 조치	스탠바이가 실패한 것으로 표시됨	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	장애 조치 쌍의 유닛 1개에 오류가 발생할 경우, 해당 유닛의 액티브 장애 조치 그룹은 실패한 것으로 표시되며 피어 유닛에서 액티브 상태가 됩니다.
임계값을 넘은 액티브 장애 조치 그룹에서 인터페이스 오류 발생	장애 조치	액티브 그룹이 실패한 것으로 표시됨	액티브 상태가 됨	없음
임계값을 넘은 스탠바이 장애 조치 그룹에서 인터페이스 오류 발생	장애 조치 없음	조치 없음	스탠바이 그룹이 실패한 것으로 표시됨	스탠바이 장애 조치 그룹이 실패한 것으로 표시될 경우, 액티브 장애 조치 그룹에서는 장애 조치를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.
이전 액티브 장애 조치 그룹 복구	장애 조치 없음	조치 없음	조치 없음	장애 조치 그룹 사전 대응 방식이 구성되지 않는 한 장애 조치 그룹은 해당 유닛에서 액티브 상태를 유지합니다.
시작 시 장애 조치 링크에 오류 발생	장애 조치 없음	액티브 상태가 됨	액티브 상태가 됨	시작 시 장애 조치 링크가 중단되면 두 유닛의 두 장애 조치 그룹 모두 액티브 상태가 됩니다.

표 8-3 액티브/액티브 장애 조치에 대한 장애 조치 동작 (계속)

오류 이벤트	정책	액티브 그룹 조치	스탠바이 그룹 조치	참고
상태 링크 오류 발생	장애 조치 없음	조치 없음	조치 없음	장애 조치가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
작동 중 장애 조치 링크에 오류 발생	장애 조치 없음	N/A	N/A	각 유닛에서 장애 조치 링크가 실패한 것으로 표시됨 장애 조치가 중단된 동안에는 유닛에서 스탠바이 유닛으로 장애 조치를 시작하지 못하므로 최대한 빨리 장애 조치 링크를 복구해야 합니다.

장애 조치 라이센스

액티브/스탠바이 장애 조치

모델	라이센싱 요구 사항
ASA 5512-X	Security Plus 라이센스
ASAv	Standard 및 Premium 라이센스
기타 모델	Base 라이센스

장애 조치 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다. 두 유닛에 모두 라이센스가 있는 경우, 해당 라이센스는 실행 중인 단일 장애 조치 클러스터 라이센스로 통합됩니다. 이러한 규칙의 예외 사항은 다음과 같습니다.

- 5512-X용 Security Plus 라이센스 — Base 라이센스에서는 장애 조치를 지원하지 않으므로 Base 라이센스만 있는 스탠바이 유닛에서는 장애 조치를 사용할 수 없습니다.
- 암호화 라이센스 — 두 유닛에는 모두 동일한 암호화 라이센스가 있어야 합니다.
- ASA 5555-X를 통한 ASA 5512-X용 IPS 모듈 — 두 유닛에는 모두 IPS 모듈 라이센스가 있어야 합니다. 또한 두 유닛의 IPS에는 IPS 서명 서브스크립션이 필요합니다. 다음 지침을 참조하십시오.
  - 필요한 IPS 서명 서브스크립션을 구매하려면 ASA에 IPS가 사전 설치되어 있어야 합니다(부품 번호에 "IPS"가 포함되어야 함(예: ASA5515-IPS-K9)). IPS 부품 번호가 없는 ASA에 대해서는 IPS 서명 서브스크립션을 구매할 수 없습니다.
  - 두 유닛에 모두 IPS 서명 서브스크립션이 있어야 합니다. 이러한 서브스크립션은 ASA 라이센스가 아니므로 장애 조치에서 공유되지 않습니다.
  - IPS 서명 서브스크립션에는 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이센스와 마찬가지로, IPS 모듈 라이센스는 장애 조치 클러스터 라이센스 내에서 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.
- ASAv 가상 CPU — 장애 조치를 구축할 경우 기본 유닛과 동일한 수의 vCPU가 스탠바이 유닛에 할당되어 있는지 확인하십시오(vCPU 라이센스 일치 여부도 함께 확인).

액티브/액티브 장애 조치

모델	라이센싱 요구 사항
ASA 5512-X	Security Plus 라이센스
ASAv	지원 안 함
기타 모델	Base 라이센스

장애 조치 유닛의 경우 각 유닛에 동일한 라이센스가 필요하지 않습니다. 두 유닛에 모두 라이센스가 있는 경우, 해당 라이센스는 실행 중인 단일 장애 조치 클러스터 라이센스로 통합됩니다. 이러한 규칙의 예외 사항은 다음과 같습니다.

- 5512-X용 Security Plus 라이센스 — Base 라이센스에서는 장애 조치를 지원하지 않으므로 Base 라이센스만 있는 스탠바이 유닛에서는 장애 조치를 사용할 수 없습니다.
- 암호화 라이센스 — 두 유닛에는 모두 동일한 암호화 라이센스가 있어야 합니다.
- ASA 5555-X를 통한 ASA 5512-X용 IPS 모듈 — 두 유닛에는 모두 IPS 모듈 라이센스가 있어야 합니다. 또한 두 유닛의 IPS에는 IPS 서명 서브스크립션이 필요합니다. 다음 지침을 참조하십시오.
  - 필요한 IPS 서명 서브스크립션을 구매하려면 ASA에 IPS가 사전 설치되어 있어야 합니다(부품 번호에 "IPS"가 포함되어야 함(예: ASA5515-IPS-K9)). IPS 부품 번호가 없는 ASA에 대해서는 IPS 서명 서브스크립션을 구매할 수 없습니다.
  - 두 유닛에 모두 IPS 서명 서브스크립션이 있어야 합니다. 이러한 서브스크립션은 ASA 라이센스가 아니므로 장애 조치에서 공유되지 않습니다.
  - IPS 서명 서브스크립션에는 유닛당 고유한 IPS 모듈 라이센스가 있어야 합니다. 다른 ASA 라이센스와 마찬가지로, IPS 모듈 라이센스는 장애 조치 클러스터 라이센스 내에서 공유됩니다. 그러나 IPS 서명 서브스크립션 요구 사항으로 인해 각 유닛에 대해 별도의 IPS 모듈 라이센스를 구매해야 합니다.
- ASAv 가상 CPU — 장애 조치를 구축할 경우 기본 유닛과 동일한 수의 vCPU가 스탠바이 유닛에 할당되어 있는지 확인하십시오(vCPU 라이센스 일치 여부도 함께 확인).

장애 조치 사전 요구 사항

8-2 페이지의 장애 조치 시스템 요구 사항를 참조하십시오.

장애 조치 지침

컨텍스트 모드 지침

- 액티브/스탠바이 모드는 단일 및 다중 컨텍스트 모드에서 지원됩니다.
- 액티브/액티브 모드는 다중 컨텍스트 모드에서만 지원됩니다.
- 다중 컨텍스트 모드의 경우, 달리 명시되지 않는 한 모든 단계가 시스템 실행 영역에서 수행됩니다.
- 둘 이상의 컨텍스트에서 컨피그레이션을 동시에 변경하려고 할 경우 ASA 장애 조치 복제가 실패합니다. 해결 방법은 각 컨텍스트에서 순차적으로 컨피그레이션을 변경하는 것입니다.

추가 지침 및 제한

- ASA 장애 조치 쌍에 연결된 스위치에서 포트 보안을 구성할 경우 장애 조치 이벤트가 발생할 때 통신에 문제가 생길 수 있습니다. 이러한 문제는 한 보안 포트에서 구성하거나 확보한 보안 MAC 주소가 다른 보안 포트로 이동될 경우 발생하며, 스위치 포트 보안 기능에 의해 위반 여부가 플래그로 표시됩니다.
- 한 유닛에서 모든 컨텍스트 전반에 걸쳐 최대 250개의 인터페이스를 모니터링할 수 있습니다.
- 액티브/액티브 장애 조치의 경우 같은 ASR 그룹의 같은 컨텍스트에서 2개의 인터페이스를 구성할 수 없습니다.
- 액티브/액티브 장애 조치의 경우 최대 2개의 장애 조치 그룹을 정의할 수 있습니다.
- 액티브/액티브 장애 조치의 경우 장애 조치 그룹을 제거할 때 장애 조치 그룹 1을 마지막에 제거해야 합니다. 장애 조치 그룹 1에는 관리자 컨텍스트가 항상 포함됩니다. 장애 조치 그룹에 할당되지 않은 모든 컨텍스트는 장애 조치 그룹 1에 기본 설정됩니다. 컨텍스트가 명시적으로 할당된 장애 조치 그룹은 제거할 수 없습니다.

관련 주제

- 37-29 페이지의 장애 조치 구성에서 자동 업데이트 서버 지원

장애 조치 기본값

기본적으로 장애 조치 정책은 다음과 같이 구성됩니다.

- HTTP 복제가 없는 스테이트풀 장애 조치
- 단일 인터페이스 오류 시 장애 조치 발생
- 인터페이스 폴링 시간 5초
- 인터페이스 대기 시간 25초
- 유닛 폴링 시간 1초
- 유닛 대기 시간 15초
- 가상 MAC 주소는 다중 컨텍스트 모드에서 활성화됨. 단일 컨텍스트 모드에서는 가상 MAC 주소가 비활성화됨
- 모든 물리적 인터페이스 또는 ASASM, 모든 VLAN 인터페이스에 대한 모니터링

액티브/스탠바이 장애 조치 구성

High Availability and Scalability Wizard에서는 액티브/스탠바이 장애 조치 컨피그레이션을 생성하기 위한 단계별 프로세스를 안내합니다.

절차

1단계 **Wizards > High Availability and Scalability**를 선택합니다. 다음 단계에서 선택된 마법사 지침을 참조합니다.

2단계 **Failover Peer Connectivity and Compatibility** 화면에서 피어 유닛의 IP 주소를 입력합니다. 이 주소는 ASDM 액세스가 사용 설정된 인터페이스여야 합니다.

기본적으로 피어 주소는 ASDM 관리 인터페이스의 스탠바이 주소에 할당됩니다.

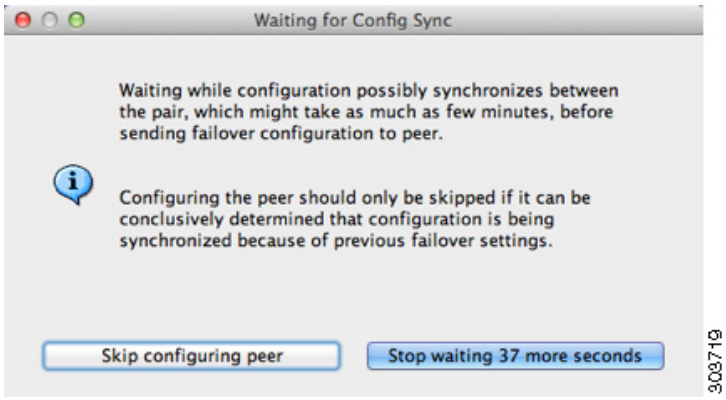
3단계 **LAN Link Configuration** 화면의 항목

- **Active IP Address** — 이 IP 주소는 사용되지 않는 서브넷에 있어야 합니다.
- **Standby IP Address** — 이 IP 주소는 액티브 IP 주소와 같은 네트워크에 있어야 합니다.
- (선택 사항) **Communications Encryption** — 장애 조치 링크의 통신을 암호화합니다. **참고**: 비밀 키 대신 IPsec 사전 공유 키를 사용하는 것이 좋습니다. 해당 키는 마법사를 종료한 후 구성할 수 있습니다(8-34 페이지의 장애 조치 설정 수정 참조).

4단계 **State Link Configuration** 화면에서 스테이트풀 장애 조치에 대한 다른 인터페이스를 선택합니다.

- **Active IP Address** — 이 IP 주소는 장애 조치 링크와 다른 사용되지 않는 서브넷에 있어야 합니다.
- **Standby IP Address** — 이 IP 주소는 액티브 IP 주소와 같은 네트워크에 있어야 합니다.

5단계 **Finish**를 클릭하면 마법사에 **Waiting for Config Sync** 화면이 표시됩니다.



지정된 기간이 종료되면 마법사에서 장애 조치 컨피그레이션을 보조 유닛으로 전송하며, 해당 장애 조치 컨피그레이션이 완료되었음을 알리는 정보가 화면에 표시됩니다.

- 보조 유닛에 장애 조치가 이미 활성화되었는지 모를 경우 지정된 기간 동안 기다리십시오.
- 장애 조치가 이미 활성화되었는지 알고 있는 경우 **Skip configuring peer**를 클릭합니다.
- 보조 유닛의 장애 조치가 아직 활성화되지 않았음을 아는 경우 **Stop waiting** *xx* **more seconds**를 클릭하면 장애 조치 부트스트랩 컨피그레이션이 보조 유닛으로 즉시 전송됩니다.

액티브/액티브 장애 조치 구성

High Availability and Scalability Wizard에서는 액티브/액티브 장애 조치 컨피그레이션을 생성하기 위한 단계별 프로세스를 안내합니다.

절차

1단계 **Wizards > High Availability and Scalability**를 선택합니다. 다음 단계에서 선택된 마법사 지침을 참조합니다.

2단계 **Failover Peer Connectivity and Compatibility Check** 화면에서 피어 IP 주소는 ASDM 액세스가 사용 설정된 인터페이스여야 합니다.

기본적으로 피어 주소는 ASDM가 연결된 인터페이스의 스탠바이 주소에 할당됩니다.

3단계 **Security Context Configuration** 화면에서 다중 컨텍스트 모드를 마법사의 일부로 변환한 경우, 관리자 컨텍스트만 표시됩니다. 마법사를 종료한 후 다른 컨텍스트를 추가할 수 있습니다.

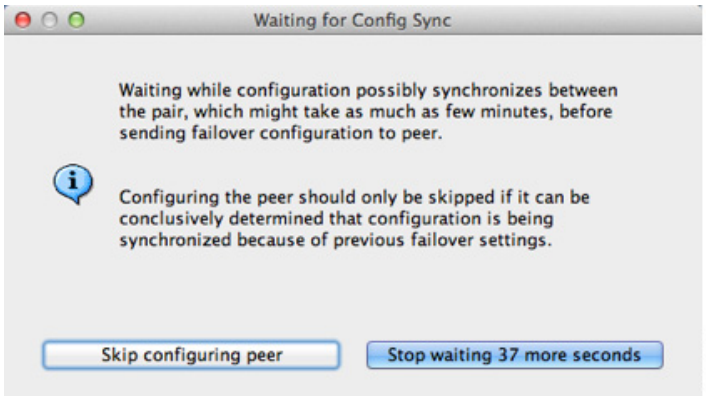
4단계 **LAN Link Configuration** 화면의 항목

- **Active IP Address** — 이 IP 주소는 사용되지 않는 서브넷에 있어야 합니다.
- **Standby IP Address** — 이 IP 주소는 액티브 IP 주소와 같은 네트워크에 있어야 합니다.
- (선택 사항) **Communications Encryption** — 장애 조치 링크의 통신을 암호화합니다. **참고**: 비밀 키 대신 IPsec 사전 공유 키를 사용하는 것이 좋습니다. 해당 키는 마법사를 종료한 후 구성할 수 있습니다(8-34 페이지의 장애 조치 설정 수정 참조).

5단계 **State Link Configuration** 화면에서 스테이트풀 장애 조치에 대한 다른 인터페이스를 선택합니다.

- **Active IP Address** — 이 IP 주소는 장애 조치 링크와 다른 사용되지 않는 서브넷에 있어야 합니다.
- **Standby IP Address** — 이 IP 주소는 액티브 IP 주소와 같은 네트워크에 있어야 합니다.

6단계 **Finish**를 클릭하면 마법사에 **Waiting for Config Sync** 화면이 표시됩니다.



지정된 기간이 종료되면 마법사에서 장애 조치 컨피그레이션을 보조 유닛으로 전송하며, 해당 장애 조치 컨피그레이션이 완료되었음을 알리는 정보가 화면에 표시됩니다.

- 보조 유닛에 장애 조치가 이미 활성화되었는지 모를 경우 지정된 기간 동안 기다리십시오.
- 장애 조치가 이미 활성화되었는지 알고 있는 경우 **Skip configuring peer**를 클릭합니다.
- 보조 유닛의 장애 조치가 아직 활성화되지 않았음을 아는 경우 **Stop waiting** *xx* **more seconds**를 클릭하면 장애 조치 부트스트랩 컨피그레이션이 보조 유닛으로 즉시 전송됩니다.

선택적 장애 조치 매개변수 구성

원하는 경우 장애 조치 설정을 맞춤화할 수 있습니다.

- 8-29 페이지의 장애 조치 기준 구성, HTTP 복제, 그룹 사전 대응 방식, MAC 주소
- 8-31 페이지의 인터페이스 모니터링 및 Standby 주소 구성
- 8-32 페이지의 비대칭 라우팅 패킷을 위한 지원 구성(액티브/액티브 모드)

장애 조치 기준 구성, HTTP 복제, 그룹 사전 대응 방식, MAC 주소

이 섹션에서 변경할 수 있는 다양한 매개변수에 대한 기본 설정은 8-26 페이지의 장애 조치 기본값를 참조하십시오. 액티브/액티브 모드에서는 장애 조치 그룹당 가장 많은 기준을 설정합니다. 이 섹션에는 액티브/액티브 모드에서 장애 조치 그룹당 HTTP 복제를 사용하는 방법이 포함됩니다. 액티브/스탠바이 모드에 대한 HTTP 복제를 구성하는 방법은 8-34 페이지의 장애 조치 설정 수정를 참조하십시오.

시작하기 전에

다중 컨텍스트 모드의 시스템 실행 영역에서 이러한 설정을 구성합니다.

절차

7단계 **Configuration > Device Management > High Availability and Scalability > Failover > Criteria** 탭을 선택합니다.

8단계 **Failover Poll Times** 영역에서 유닛 폴링 시간을 구성합니다.

- **Unit Failover** — 유닛 간의 hello 메시지의 시간 간격을 나타냅니다. 범위는 1~15초 또는 200~999밀리초입니다.
- **Unit Hold Time** — 유닛에서 장애 조치 링크에 대한 hello 메시지를 수신해야 하는 시간을 설정합니다. 이를 설정하지 않을 경우 피어 오류 발생 시 유닛에서는 테스트 프로세스를 시작합니다. 범위는 1~45초 또는 800~999밀리초입니다. 이 값은 폴링 시간보다 3배 적게 입력할 수 없습니다.

참고 이 창의 기타 설정은 액티브/스탠바이 모드에만 적용됩니다. 액티브/액티브 모드에서는 장애 조치 그룹당 나머지 매개변수를 구성해야 합니다.

9단계 (액티브/액티브 모드에만 해당) **Active/Active** 탭을 클릭한 다음 장애 조치 그룹을 선택하고 **Edit**를 클릭합니다.

10단계 (액티브/액티브 모드에만 해당) 장애 조치 그룹의 기본 역할을 변경하려면 **Primary** 또는 **Secondary**를 클릭합니다. 마법사를 사용한 경우 장애 조치 그룹 1은 기본 유닛에 할당되고, 장애 조치 그룹 2는 보조 유닛에 할당됩니다. 비표준 컨피그레이션을 사용하려면 필요한 경우 다른 유닛 기본 설정을 지정할 수 있습니다.

11단계 (액티브/액티브 모드에만 해당) 장애 조치 그룹 사전 대응 방식을 구성하려면 **Preempt after booting with optional delay of** 확인란을 선택합니다.

한 유닛이 다른 유닛보다 먼저 부팅될 경우, 기본 또는 보조 설정에 관계없이 두 장애 조치 그룹 모두 해당 유닛에서 액티브 상태가 됩니다. 이 옵션을 사용하면 유닛이 사용 가능한 상태가 되었을 때 지정된 유닛에서 장애 조치 그룹이 자동으로 액티브 상태가 됩니다.

선택적인 지연 값을 입력할 수 있으며, 이 값은 지정된 유닛에서 자동으로 액티브 상태가 되기 전에 장애 조치 그룹이 현재 유닛에서 액티브 상태로 유지되는 시간(초 단위)을 지정합니다. 올바른 값의 범위는 1부터 1200까지입니다.

참고 스테이트풀 장애 조치를 사용할 경우, 장애 조치 그룹이 현재 액티브 상태로 있는 유닛에서 연결이 복제될 때까지 사전 대응이 지연됩니다.

12단계 **Interface Policy**를 구성하려면 다음 중 하나를 선택합니다.

- **Number of failed interfaces that triggers failover** — 몇 개의 인터페이스에 오류가 발생해야 장애 조치가 일어나는지 구체적인 수를 1~250개 범위 내에서 정의합니다. 오류가 발생한 모니터링된 인터페이스 수가 사용자가 지정한 값을 초과할 경우 ASA에서는 장애 조치를 시작합니다.
- **Percentage of failed interfaces that triggers failover** — 구성된 인터페이스의 오류 발생 비율(%)이 어느 정도가 되어야 장애 조치가 일어나는지 정의합니다. 오류가 발생한 모니터링된 인터페이스 수가 사용자가 설정한 백분율을 초과할 경우 ASA에서는 장애 조치를 시작합니다.

참고 **Use system failover interface policy** 옵션은 사용하지 마십시오. 현재까지는 그룹당 정책을 설정하는 것만 가능합니다.

13단계 액티브/스탠바이 모드의 경우 **Failover Poll Time** 영역에서 인터페이스 폴링 시간을 구성합니다.

액티브/액티브 모드의 경우 **Add/Edit Failover Group** 대화 상자에서 인터페이스 폴링 시간을 구성합니다.

- **Monitored Interfaces** — 인터페이스 간의 폴링 시간 간격을 나타냅니다. 범위는 1~15초 또는 500~999밀리초입니다.
- **Interface Hold Time** — 데이터 인터페이스에서 데이터 인터페이스에 대한 hello 메시지를 수신해야 하는 시간을 설정합니다. 이 시간을 초과하면 피어에 오류가 발생한 것으로 선언됩니다. 올바른 값의 범위는 5~75초입니다.

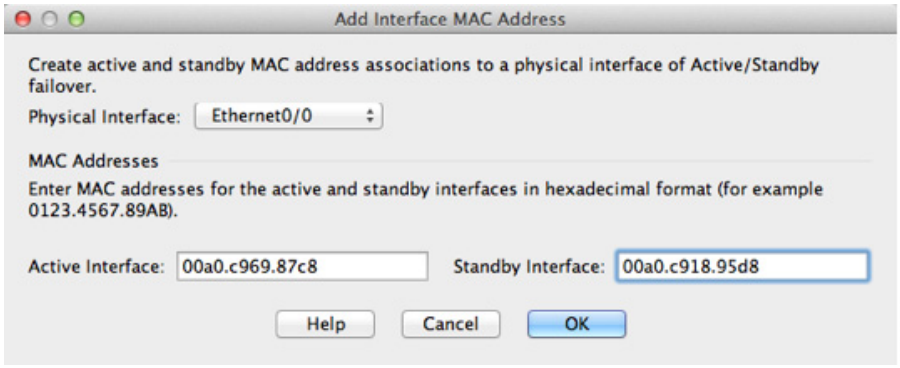
14단계 (액티브/액티브 모드에만 해당) HTTP 복제를 사용하도록 설정하려면 **Enable HTTP replication** 확인란을 선택합니다. 액티브/스탠바이 모드의 경우 8-34 페이지의 장애 조치 설정 수정를 참조하십시오. HTTP 복제 속도에 대한 내용은 두 가지 모드 모두 8-34 페이지의 장애 조치 설정 수정 섹션을 참조하십시오.

15단계 액티브/스탠바이 모드에 가상 MAC 주소를 구성하려면 **MAC Addresses** 탭을 클릭합니다.

액티브/액티브 모드의 경우 **Active/Active** 탭의 하단으로 이동합니다.

다른 방법을 사용하여 MAC 주소를 설정할 수도 있으나, 한 가지 방법만 사용하는 것이 좋습니다. 여러 방법을 사용하여 MAC 주소를 설정할 경우, 사용되는 MAC 주소는 다양한 변수에 따라 달라지며 예측하기 어려워질 수 있습니다.

16단계 새 가상 MAC 주소 항목을 추가하려면 **Add**를 클릭합니다.



Add/Edit Interface MAC Address 대화 상자가 나타납니다.

17단계 **Physical Interface** 드롭다운 목록에서 인터페이스를 선택합니다.

18단계 **Active MAC Address** 필드에서 액티브 인터페이스에 대한 새 MAC 주소를 입력합니다.

19단계 **Standby MAC Address** 필드에서 스탠바이 인터페이스에 대한 새 MAC 주소를 입력합니다.

20단계 **OK**를 클릭합니다.

인터페이스가 테이블에 추가됩니다.

21단계 (액티브/액티브 모드에만 해당) **OK**를 클릭합니다.

22단계 **Apply**를 클릭합니다.

23단계 (액티브/액티브 모드에만 해당) 필요한 경우 다른 장애 조치 그룹에 이 절차를 반복합니다.

인터페이스 모니터링 및 Standby 주소 구성

기본적으로 모니터링은 모든 물리적 인터페이스 또는 ASASM, 모든 VLAN 인터페이스, ASA에 설치된 모든 하드웨어 모듈에서 사용됩니다. 중요도가 낮은 네트워크에 연결된 인터페이스를 제외하여 장애 조치 정책에 영향을 미치지 않도록 하고자 할 수 있습니다.

마법사에서 스탠바이 IP 주소를 구성하지 않은 경우 이를 수동으로 구성할 수 있습니다.

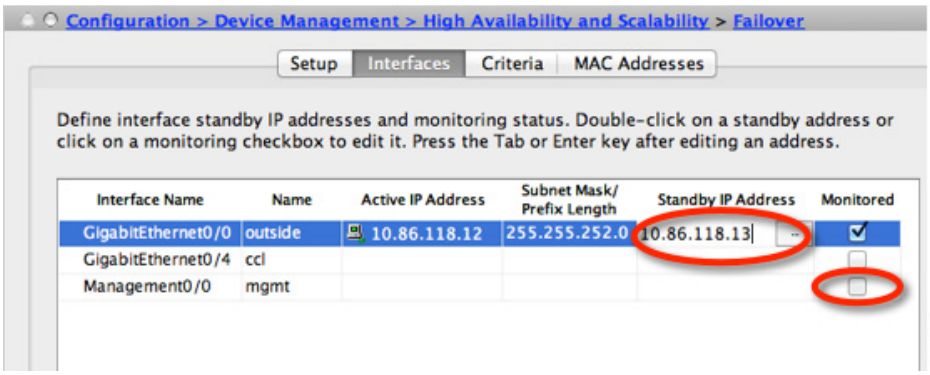
시작하기 전에

- 한 유닛에서 최대 250개의 인터페이스를 모니터링할 수 있습니다(다중 컨텍스트 모드의 전체 컨텍스트 전반에 걸쳐).
- 다중 컨텍스트 모드에서 각 컨텍스트 내에 인터페이스를 구성합니다.

절차

1단계 단일 모드에서 **Configuration > Device Management > High Availability > Failover > Interfaces**를 선택합니다.

다중 컨텍스트 모드의 경우 컨텍스트 내에서 **Configuration > Device Management > Failover > Interfaces**를 선택합니다.



구성된 인터페이스 목록과 설치된 하드웨어 모듈(예: ASA FirePOWER 모듈)이 표시됩니다. Monitored 열에는 인터페이스가 장애 조치 기준에 포함되어 모니터링되었는지 여부가 표시됩니다. 모니터링된 경우 Monitored 확인란에 확인 표시가 나타납니다.

하드웨어 모듈 오류 때문에 장애 조치가 수행되는 것을 원치 않을 경우 모듈 모니터링을 비활성화할 수 있습니다.

각 인터페이스의 IP 주소는 Active IP Address 열에 표시됩니다. 구성된 경우 인터페이스의 스탠바이 IP 주소가 Standby IP address 열에 표시됩니다. 장애 조치 링크 및 상태 링크에는 IP 주소가 표시되지 않으며, 이 탭에서는 이러한 주소를 변경할 수 없습니다.

2단계 목록에 나열된 인터페이스의 모니터링을 비활성화하려면 인터페이스에 대한 **Monitored** 확인란의 선택을 취소합니다.

3단계 목록에 나열된 인터페이스의 모니터링을 활성화하려면 인터페이스에 대한 **Monitored** 확인란을 선택합니다.

4단계 스탠바이 IP 주소가 없는 각 인터페이스의 경우, Standby IP Address 필드를 두 번 클릭하고 해당 필드에 IP 주소를 입력합니다.

5단계 **Apply**를 클릭합니다.

비대칭 라우팅 패킷을 위한 지원 구성(액티브/액티브 모드)

액티브/액티브 장애 조치에서 실행 중인 경우, 유닛의 피어 유닛을 통해 시작된 연결에 대한 반환 패킷이 유닛에 수신될 수 있습니다. 패킷을 수신하는 ASA에 패킷에 대한 연결 정보가 없으므로 패킷이 손실됩니다. 액티브/액티브 장애 조치 쌍에 있는 두 ASA가 서로 다른 서비스 공급자에 연결되어 있고, 아웃바운드 연결에서 NAT 주소를 사용하지 않을 경우 이러한 손실 현상이 자주 일어납니다.

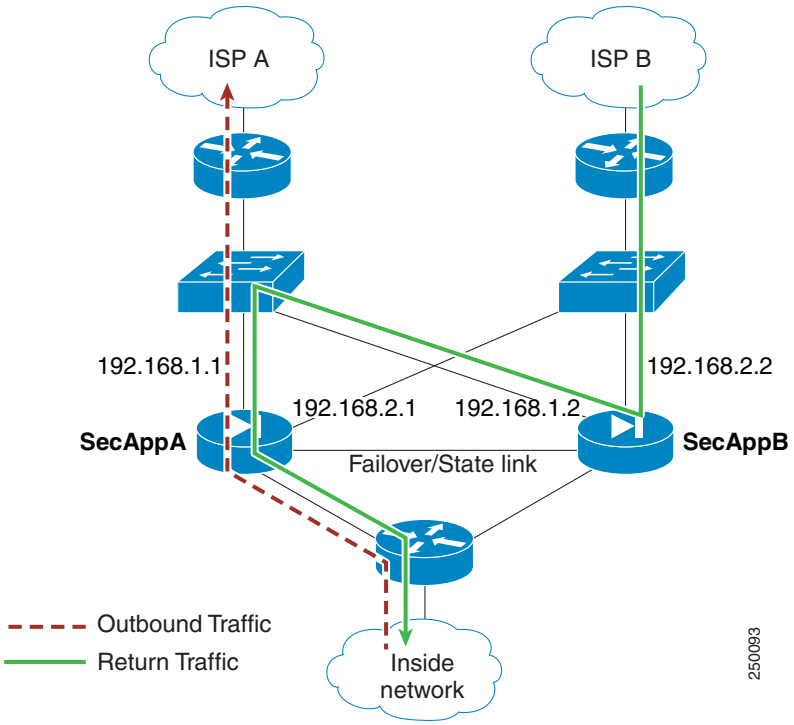
비대칭 라우팅 패킷을 사용하여 반환 패킷이 손실되는 것을 방지할 수 있습니다. 이렇게 하려면 각 ASA의 유사한 인터페이스를 동일한 ASR 그룹에 할당합니다. 예를 들어, 두 ASA는 모두 내부 인터페이스의 내부 네트워크에 연결되지만 외부 인터페이스의 별도의 ISP에 연결됩니다. 기본 유닛에서는 ASR 그룹 1에 액티브 컨텍스트 외부 인터페이스를 할당하고, 보조 유닛에서는 동일한 ASR 그룹 1에 액티브 컨텍스트 외부 인터페이스를 할당합니다. 기본 유닛의 외부 인터페이스에 세션 정보가 없는 패킷이 수신될 경우, 동일한 그룹(이 경우에는 ASR 그룹 1)에 있는 스탠바이 컨텍스트의 다른 인터페이스에 대한 세션 정보를 검사합니다. 일치하는 정보가 없을 경우 해당 패킷은 손실됩니다. 일치하는 정보가 있을 경우 다음 작업 중 하나가 실행됩니다.

- 수신 트래픽이 피어 유닛에서 시작된 경우, 레이어 2 헤더의 일부 또는 전체가 다시 작성되고 패킷이 다른 유닛에 리디렉션됩니다. 이러한 리디렉션은 세션이 활성화되어 있는 동안 지속합니다.
- 수신 트래픽이 동일한 유닛의 다른 인터페이스에서 시작된 경우, 레이어 2 헤더의 일부 또는 전체가 다시 작성되고 패킷이 스트림으로 다시 삽입됩니다.

참고 이 기능에서는 비대칭 라우팅을 제공하지 않으며, 비대칭 라우팅 패킷을 올바른 인터페이스로 복원하는 역할을 합니다.

그림 8-13에는 비대칭 라우팅 패킷의 예가 나와 있습니다.

그림 8-13 ASR 예



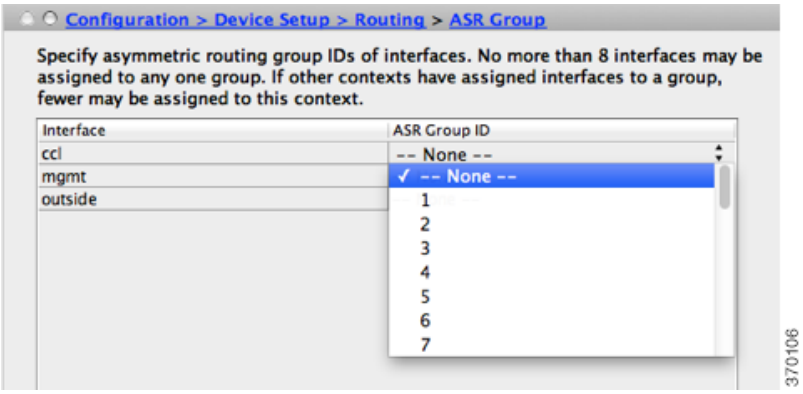
1. 아웃바운드 세션이 액티브 SecAppA 컨텍스트가 포함된 ASA를 통해 전달됩니다. 이 컨텍스트는 outsideISP-A(192.168.1.1)에 있습니다.
2. 비대칭 라우팅이 업스트림에서 구성되었으므로, 액티브 SecAppB 컨텍스트가 포함된 ASA를 통해 반환 트래픽이 인터페이스 outsideISP-B(192.168.2.2)를 통해 다시 전달됩니다.
3. 인터페이스 192.168.2.2의 트래픽에 대한 세션 정보가 없으므로 일반적으로 반환 트래픽은 손실됩니다. 그러나 인터페이스는 ASR 그룹 1의 일부로 구성됩니다. 유닛에서는 동일한 ASR 그룹 ID로 구성된 다른 인터페이스의 세션을 찾습니다.
4. 세션 정보가 인터페이스 outsideISP-A(192.168.1.2)에 있으며, 이 인터페이스는 SecAppB가 포함된 유닛에서 스탠바이 상태로 존재합니다. 스테이트풀 장애 조치를 통해 세션 정보가 SecAppA에서 SecAppB로 복제됩니다.
5. 손실되는 대신 레이어 2 헤더가 인터페이스 192.168.1.1에 대한 정보로 다시 작성되며 트래픽이 192.168.1.2 밖으로 리디렉션됩니다. 그런 다음에는 트래픽이 시작된 유닛(SecAppA의 192.168.1.1)의 인터페이스를 통해 트래픽을 반환할 수 있습니다. 이러한 전달 작업은 세션이 끝날 때까지 계속 진행되어야 합니다.

전제 조건

- 스테이트풀 장애 조치 — 액티브 장애 조치 그룹에 있는 인터페이스의 세션에 대한 상태 정보를 스탠바이 장애 조치 그룹으로 전달합니다.
- 복제 HTTP — HTTP 세션 상태 정보는 스탠바이 장애 조치 그룹으로 전달되지 않으므로, 스탠바이 인터페이스에 존재하지 않습니다. ASA에서 비대칭 라우팅 HTTP 패킷을 다시 라우팅할 수 있도록 하려면 HTTP 상태 정보를 복제해야 합니다.
- 기본 및 보조 유닛의 각 액티브 컨텍스트에서 이 절차를 수행합니다.

세부 단계

1단계 기본 유닛 액티브 컨텍스트에서 **Configuration > Device Setup > Routing > ASR Groups**를 선택합니다.



2단계 인터페이스에 비대칭 라우팅 패킷을 수신될 경우, 드롭다운 목록에서 ASR 그룹 번호를 선택합니다.

3단계 **Apply**를 클릭하여 실행 중인 컨피그레이션에 변경 사항을 저장합니다.

4단계 ASDM을 보조 유닛에 연결하고 기본 유닛 컨텍스트와 유사한 액티브 컨텍스트를 선택합니다.

5단계 **Configuration > Device Setup > Routing > ASR Groups**를 선택합니다.

6단계 이 유닛의 유사한 인터페이스에 대해 동일한 ASR 그룹 번호를 선택합니다.

7단계 **Apply**를 클릭하여 실행 중인 컨피그레이션에 변경 사항을 저장합니다.

장애 조치 관리

장애 조치 설정 수정

마법사를 사용하거나 설정을 변경하려는 경우 장애 조치 설정을 수동으로 구성할 수 있습니다. 이 섹션에는 마법사에 없는 다음과 같은 옵션이 포함되어 있으며 이러한 옵션은 수동으로 구성해야 합니다.

- 장애 조치 트래픽을 암호화하는 IPsec 사전 공유 키
- HTTP 복제 속도
- HTTP 복제(액티브/스탠바이 모드)

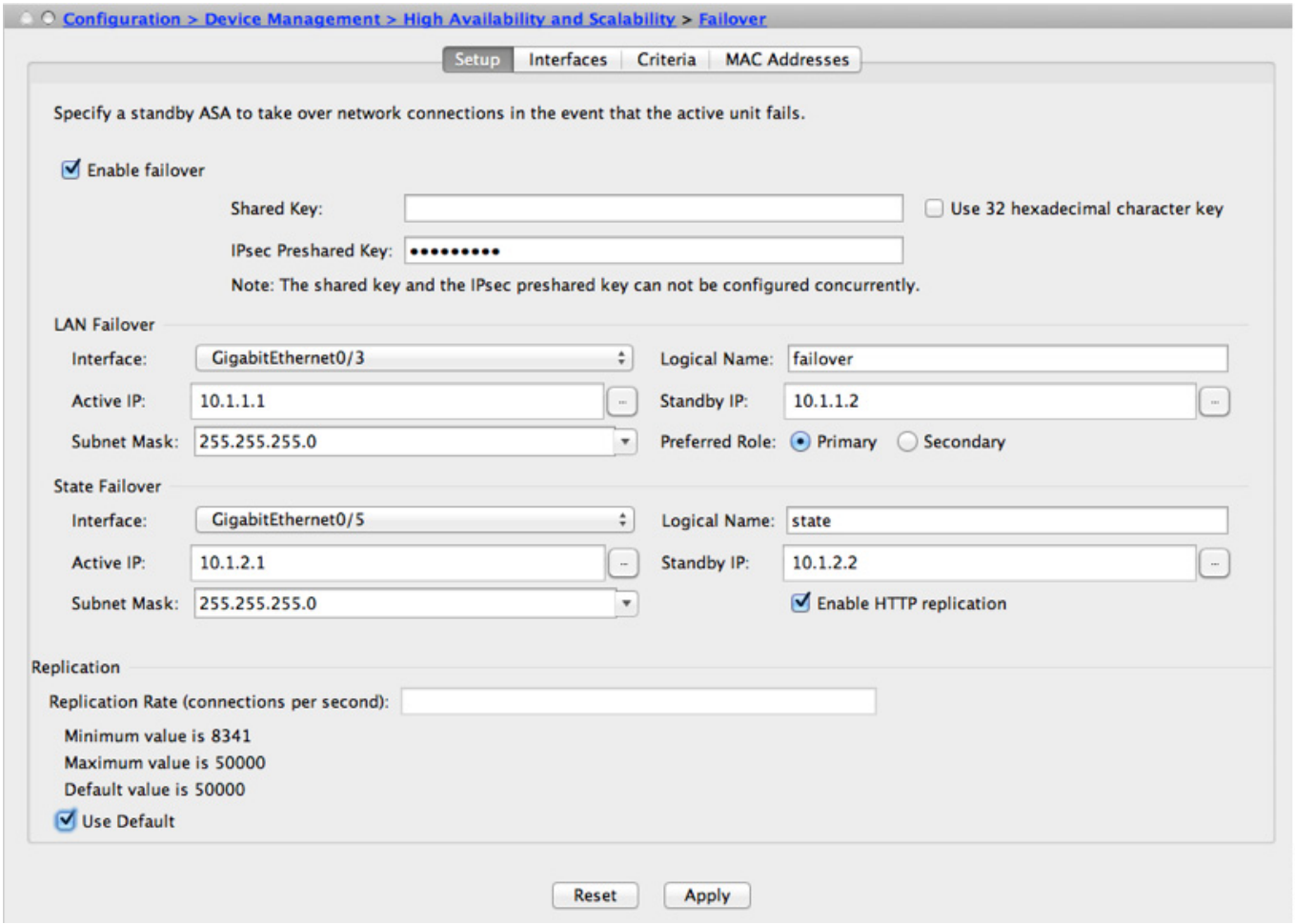
전제 조건

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

1단계 단일 모드에서 **Configuration > Device Management > High Availability and Scalability > Failover > Setup**을 선택합니다.

다중 컨텍스트 모드의 경우 시스템 실행 영역에서 **Configuration > Device Management > Failover > Setup**을 선택합니다.



2단계 **Enable Failover** 확인란을 선택합니다.

참고 변경 사항을 디바이스에 적용하기 전까지는 장애 조치가 실제로 활성화되지 않습니다.

3단계 장애 조치 및 상태 링크의 통신을 암호화하려면 다음 옵션 중 하나를 사용합니다.

- IPsec Preshared Key(권장) — 사전 공유 키는 IKEv2에서 장애 조치 유닛 간의 장애 조치 링크에 IPsec LAN-LAN 터널을 설정하는 데 사용됩니다. 참고: 장애 조치 LAN-LAN 터널의 경우 IPsec(기타 VPN) 라이센스는 계산에 포함하지 않습니다.

- Secret Key — 장애 조치 통신을 암호화하는 데 사용되는 비밀 키를 입력합니다. 이 필드를 비워 둘 경우, 명령을 복제하는 동안 전송되는 장애 조치 통신(컨피그레이션의 모든 비밀번호 또는 키 포함)의 형식은 일반 텍스트입니다.

  Use 32 hexadecimal character key — 32자 16진수 키를 비밀 키로 사용하려면 이 확인란을 선택합니다.

4단계 LAN 장애 조치 영역에서 장애 조치 링크에 대한 다음 매개변수를 설정합니다.

- Interface — 장애 조치 링크에 사용할 인터페이스를 선택합니다. 장애 조치에는 전용 인터페이스가 필요하지만 스테이트풀 장애 조치와 인터페이스를 공유할 수 있습니다.

  이 목록에는 구성되지 않은 인터페이스 또는 하위 인터페이스만 표시되며 이를 장애 조치 링크로 선택할 수 있습니다. 인터페이스를 장애 조치 링크로 지정하면 Configuration > Interfaces 창에서 해당 인터페이스를 편집할 수 없습니다.
- Logical Name — 장애 조치 통신에 사용되는 인터페이스의 논리적 이름을 지정합니다(예: “failover”). 이러한 이름은 정보를 제공하는 역할을 합니다.
- Active IP — 인터페이스에 대한 액티브 IP 주소를 지정합니다. IP 주소는 IPv4 또는 IPv6 주소일 수 있습니다. 이 IP 주소는 사용되지 않는 서브넷에 있어야 합니다.
- Standby IP — 액티브 IP 주소와 동일한 서브넷에서 인터페이스에 대한 스탠바이 IP 주소를 지정합니다.
- Subnet Mask — 서브넷 마스크를 지정합니다.
- Preferred Role — **Primary** 또는 **Secondary**를 선택하여 이 ASA의 기본 역할을 기본 또는 보조 유닛으로 지정합니다.

5단계 (선택 사항) 다음을 수행하여 상태 링크를 구성합니다.

- Interface — 상태 링크에 사용할 인터페이스를 선택합니다. 구성되지 않은 인터페이스 또는 하위 인터페이스, 장애 조치 링크, **--Use Named--** 옵션을 선택할 수 있습니다.

  참고 장애 조치 링크 및 상태 링크에는 2개로 나뉜 별도의 전용 인터페이스를 사용하는 것이 좋습니다.

  구성되지 않은 인터페이스 또는 하위 인터페이스를 선택한 경우 인터페이스에 대한 액티브 IP, 서브넷 마스크, 스탠바이 IP, 논리적 이름을 제공해야 합니다.

  장애 조치 링크를 선택한 경우 액티브 IP, 서브넷 마스크, 논리적 이름, 스탠바이 IP 값을 지정할 필요가 없으며 장애 조치 링크에 지정된 값이 사용됩니다.

  --Use Named-- 옵션을 선택할 경우 Logical Name 필드가 이름이 지정된 인터페이스 드롭다운 목록이 됩니다. 이 목록에서 인터페이스를 선택합니다. 액티브 IP, 서브넷 마스크/접두사 길이, 스탠바이 IP 값은 지정하지 않아도 됩니다. 인터페이스에 지정된 값이 사용됩니다.
- Logical Name — 상태 통신에 사용되는 인터페이스의 논리적 이름을 지정합니다(예: “state”). 이러한 이름은 정보를 제공하는 역할을 합니다.
- Active IP — 인터페이스에 대한 액티브 IP 주소를 지정합니다. IP 주소는 IPv4 또는 IPv6 주소일 수 있습니다. 이 IP 주소는 장애 조치 링크와 다른 사용되지 않는 서브넷에 있어야 합니다.
- Standby IP — 액티브 IP 주소와 동일한 서브넷에서 인터페이스에 대한 스탠바이 IP 주소를 지정합니다.
- Subnet Mask — 서브넷 마스크를 지정합니다.

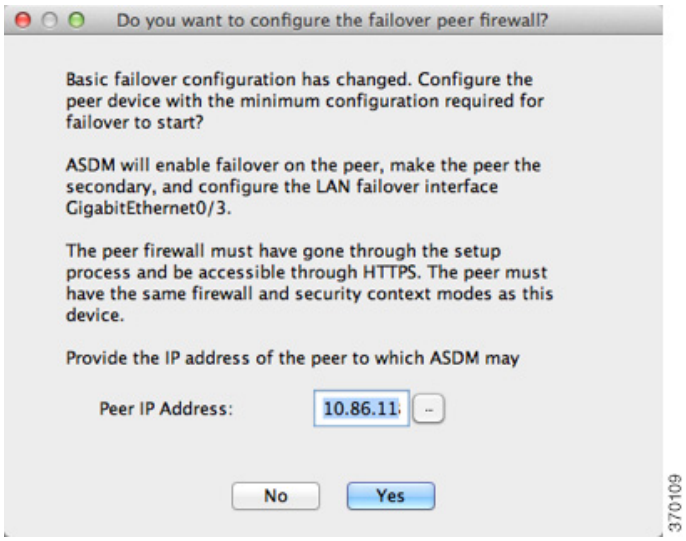
- (선택 사항, 액티브/스탠바이에만 해당) Enable HTTP Replication — **Enable HTTP Replication** 확인란을 선택하여 HTTP 복제를 활성화합니다. 이 옵션을 사용하면 스테이트풀 장애 조치에서 액티브 HTTP 세션을 스탠바이 방화벽에 복사할 수 있습니다. HTTP 복제를 허용하지 않을 경우 장애 조치가 발생하면 HTTP 연결이 끊깁니다. 액티브/액티브 모드에서 장애 조치 그룹당 HTTP 복제를 설정합니다. 8-29 페이지의 장애 조치 기준 구성, HTTP 복제, 그룹 사전 대응 방식, MAC 주소를 참조하십시오.

6단계 복제 영역에서 HTTP 복제 속도를 초당 8341~50000으로 설정합니다. 기본값은 50000입니다. 기본값을 사용하려면 **Use Default check** 확인란을 선택합니다.

7단계 **Apply**를 클릭합니다.

컨피그레이션이 디바이스에 저장됩니다.

8단계 장애 조치를 활성화한 경우 장애 조치 피어를 구성하라는 대화 상자가 표시됩니다.



- 장애 조치 피어에 나중에 연결하여 일치하는 설정을 수동으로 구성하려면 **No**를 클릭합니다.
- ASDM에서 장애 조치 피어의 관련 장애 조치 설정을 자동으로 구성하도록 하려면 **Yes**를 클릭합니다. Peer IP Address 필드에 피어 IP 주소를 입력합니다.

장애 조치 강제 실행

스탠바이 유닛을 강제로 액티브 유닛으로 만들려면 다음 절차를 수행합니다.

전제 조건

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

1단계 유닛 수준에서 장애 조치를 강제 실행하려면

a. 컨텍스트 모드에 따라 화면을 선택합니다.

- 단일 컨텍스트 모드에서 **Monitoring > Properties > Failover > Status**를 선택합니다.

- 다중 컨텍스트 모드에서는 **Monitoring > Failover > System**이 선택됩니다.

b. 다음 버튼 중 하나를 클릭합니다.

- 유닛을 이 유닛으로 만들려면 **Make Active**를 클릭합니다.
- 다른 유닛을 액티브 유닛으로 만들려면 **Make Standby**를 클릭합니다.

2단계 (액티브/액티브 모드에만 해당) 장애 조치 그룹 수준에서 장애 조치를 강제로 실행하려면

a. **Monitoring > Failover > Failover Group #**이 선택되며 # 은 제어하려는 장애 조치 그룹의 개수입니다.

b. 다음 버튼 중 하나를 클릭합니다.

- 이 유닛에서 장애 조치 그룹을 액티브 상태로 만들려면 **Make Active**를 클릭합니다.
- 다른 유닛에서 장애 조치 그룹을 액티브 상태로 만들려면 **Make Standby**를 클릭합니다.

장애 조치 비활성화

장애 조치를 비활성화하려면 다음 절차를 수행 합니다.

전제 조건

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

1단계 단일 모드에서 **Configuration > Device Management > High Availability and Scalability > Failover > Setup**을 선택합니다.

다중 컨텍스트 모드의 경우 시스템 실행 영역에서 **Configuration > Device Management > Failover > Setup**을 선택합니다.

2단계 **Enable Failover** 확인란의 선택을 취소합니다.

3단계 **Apply**를 클릭합니다.

오류가 발생한 유닛 복원

오류가 발생한 유닛을 오류가 발생하지 않은 상태로 복원하려면 다음 절차를 수행합니다.

전제 조건

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다.

세부 단계

1단계 유닛 수준에서 장애 조치를 복원하려면

a. 컨텍스트 모드에 따라 화면을 선택합니다.

- 단일 컨텍스트 모드에서 **Monitoring > Properties > Failover > Status**를 선택합니다.
- 다중 컨텍스트 모드에서는 **Monitoring > Failover > System**이 선택됩니다.

b. **Reset Failover**를 클릭합니다.

2단계 (액티브/액티브 모드에만 해당) 장애 조치 그룹 수준에서 장애 조치를 재설정하려면

a. **Monitoring > Failover > Failover Group #**이 선택되며 #은 제어하려는 장애 조치 그룹의 개수입니다.

b. **Reset Failover**를 클릭합니다.

구성 다시 동기화

복제된 명령어는 실행 중인 컨피그레이션에 저장됩니다. 복제된 명령을 스탠바이 유닛의 플래시 메모리에 저장하려면 **File > Save Running Configuration to Flash**를 선택합니다.

모니터링 장애 조치

장애 조치 메시지

장애 조치가 일어날 경우, ASA에서는 시스템 메시지를 전송합니다.

장애 조치 Syslog 메시지

ASA에서는 심각한 상황을 의미하는 우선순위 등급 2에 해당하는 장애 조치와 관련된 여러 가지 syslog 메시지를 전달합니다. 이러한 메시지를 보려면 syslog 메시지 가이드를 참조하십시오. 로깅을 사용하려면 40 장, “로깅”.을 참조하십시오.

참고 장애 조치가 실행되는 동안에는 장애 조치가 논리적으로 종료되고 인터페이스가 호출되어 syslog 메시지 411001 및 411002를 생성합니다. 이는 정상적인 동작입니다.

장애 조치 디버그 메시지

디버그 메시지를 보려면 **debug fover** 명령을 입력합니다. 자세한 내용은 명령 참조를 참조하십시오.

참고 디버깅 출력은 CPU 프로세스에서 높은 우선순위가 할당되므로 시스템 성능에 큰 영향을 미칠 수 있습니다. 따라서 **debug fover** 명령은 문제 해결 또는 Cisco TAC와의 문제 해결 세션 동안에만 사용하십시오.

SNMP 장애 조치 트랩

장애 조치를 위한 SNMP syslog 트랩을 수신하려면 SNMP 에이전트에서 SNMP 트랩을 SNMP 관리 스테이션으로 전송하도록 구성하고, syslog 호스트를 정의하고, Cisco syslog MIB를 SNMP 관리 스테이션으로 컴파일합니다. 자세한 내용은 41 장, “SNMP”를 참조하십시오.

모니터링 장애 조치

참고 장애 조치 이벤트 후에는 ASDM를 다시 시작하거나 Devices 창에서 다른 디바이스로 전환한 다음 원래 ASA로 다시 돌아와 디바이스 모니터링을 계속해야 합니다. ASDM의 연결이 끊어지고 디바이스에 다시 연결될 경우 모니터링 연결이 다시 설정되지 않으므로 이러한 작업을 수행해야 합니다.

액티브/스탠바이 장애 조치를 모니터링하려면 **Monitoring > Properties > Failover**를 선택합니다.

액티브/액티브 장애 조치를 모니터링하려면 Monitoring > Properties > Failover 영역에서 다음 화면을 사용합니다.

- 8-40 페이지의 시스템
- 8-41 페이지의 장애 조치 그룹 1 및 장애 조치 그룹 2

시스템

System 창에는 시스템의 장애 조치 상태가 표시됩니다. 다음 작업을 통해 시스템의 장애 조치 상태를 제어할 수도 있습니다.

- 디바이스의 액티브/스탠바이 상태 전환
- 오류가 발생한 디바이스 재설정
- 스탠바이 유닛 다시 로드

필드

Failover state of the system — *표시 전용입니다.* ASA의 장애 조치 상태를 표시합니다. 표시되는 정보는 **show failover** 명령에 수신되는 출력과 동일합니다. 표시되는 출력에 대한 자세한 내용은 명령 참조 를 참조하십시오.

System 창에서 다음 작업을 수행할 수 있습니다.

- Make Active — 이 버튼을 클릭하면 ASA가 액티브/스탠바이 컨피그레이션의 액티브 유닛이 됩니다. 액티브/액티브 컨피그레이션에서 이 버튼을 클릭하면 ASA의 두 장애 조치 그룹이 모두 액티브 상태가 됩니다.
- Make Standby — 이 버튼을 클릭하면 ASA가 액티브/스탠바이 구성의 스탠바이 쌍이 됩니다. 액티브/액티브 컨피그레이션에서 이 버튼을 클릭하면 ASA의 두 장애 조치 그룹이 모두 스탠바이 상태가 됩니다.
- Reset Failover—이 버튼을 클릭하면 시스템이 오류가 발생한 상태에서 스탠바이 상태로 재설정됩니다. 시스템을 액티브 상태로 재설정할 수는 없습니다. 액티브 유닛에서 이 버튼을 클릭하면 스탠바이 유닛으로 재설정됩니다.
- Reload Standby — 이 버튼을 클릭하면 스탠바이 유닛이 다시 로드됩니다.
- Refresh—이 버튼을 클릭하면 시스템 필드에서 장애 조치 상태의 상태 정보를 새로 고칩니다.

장애 조치 그룹 1 및 장애 조치 그룹 2

Failover Group 1 및 Failover Group 2 창에는 선택한 그룹의 장애 조치 상태가 표시됩니다. 또한 그룹의 액티브/스탠바이 상태를 전환하거나 오류가 발생한 그룹을 재설정하여 그룹의 장애 조치 상태를 제어할 수도 있습니다.

필드

Failover state of Group[*x*] — *표시 전용입니다.* 선택한 장애 조치 그룹의 장애 조치 상태를 표시합니다. 표시되는 정보는 **show failover group** 명령에서 수신되는 출력과 동일합니다.

이 창에서 다음 작업을 수행할 수 있습니다.

- Make Active—이 버튼을 클릭하면 장애 조치 그룹이 ASA에서 액티브 유닛이 됩니다.
- Make Standby—이 버튼을 클릭하면 장애 조치 그룹이 ASA에서 스탠바이 상태가 됩니다.
- Reset Failover—이 버튼을 클릭하면 시스템이 오류가 발생한 상태에서 스탠바이 상태로 재설정됩니다. 시스템을 액티브 상태로 재설정할 수는 없습니다. 액티브 유닛에서 이 버튼을 클릭하면 스탠바이 유닛으로 재설정됩니다.
- Refresh—이 버튼을 클릭하면 시스템 필드에서 장애 조치 상태의 상태 정보를 새로 고칩니다.

장애 조치에 대한 기능 기록

표 8-4에서는 이 기능의 출시 내역을 정리합니다.

표 8-4 선택적 액티브/스탠바이 장애 조치 설정에 대한 기능 기록

기능 이름	릴리스	기능 정보
액티브/스탠바이 장애 조치	7.0(1)	이 기능은 도입되었습니다.
액티브/액티브 장애 조치	7.0(1)	이 기능은 도입되었습니다.
장애 조치 키에 16진수 값 지원	7.0(4)	이제 장애 조치 링크 암호화에 16진수 값을 지정할 수 있습니다. 변경된 화면: Configuration > Device Management > High Availability > Failover > Setup
장애 조치 키에 마스터 암호 지원	8.3(1)	이제 장애 조치 키에서 마스터 암호를 지원하며, 이 기능은 실행 중인 컨피그레이션과 시작 컨피그레이션의 공유 키를 암호화합니다. ASA에서 다른 ASA로 공유 비밀을 복사할 경우(예: **more system:running-config** 명령에서), PSK(Pre-Shared Key)를 복사하여 붙여넣을 수 있습니다. **참고** **failover key** shared secret은 **show running-config** 출력에 *****로 표시되며, 이러한 가려진 키는 복사할 수 없습니다. ASDM 변경 사항은 없습니다.
장애 조치에 IPv6 지원이 추가되었습니다.	8.2(2)	다음 화면을 수정했습니다. Configuration > Device Management > High Availability > Failover > Setup Configuration > Device Management > High Availability > Failover > Interfaces

표 8-4 선택적 액티브/스탠바이 장애 조치 설정에 대한 기능 기록

기능 이름	릴리스	기능 정보
장애 조치 및 상태 링크 통신을 암호화하는 IPsec LAN-LAN 터널 지원	9.1(2)	장애 조치 키에 전용 암호화를 사용하는 대신, 이제 장애 조치 및 상태 링크 암호화를 위한 IPsec LAN-LAN 터널을 사용할 수 있습니다. **참고** 장애 조치 LAN-LAN 터널의 경우 IPsec(기타 VPN) 라이센스는 계산에 포함하지 않습니다. 변경된 화면: Configuration > Device Management > High Availability > Failover > Setup
하드웨어 모듈의 상태 모니터링 비활성화	9.3(1)	기본적으로 ASA에서는 ASA FirePOWER 모듈과 같은 설치된 하드웨어 모듈의 상태를 모니터링합니다. 하드웨어 모듈 오류 때문에 장애 조치가 수행되는 것을 원치 않을 경우 모듈 모니터링을 비활성화할 수 있습니다. 다음 화면을 수정했습니다. **Configuration > Device Management > High Availability and Scalability > Failover > Interfaces**

9 장

ASA 클러스터

클러스터링을 사용하면 여러 개의 ASA를 하나의 논리적 디바이스로 그룹화할 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다.

참고 클러스터링을 사용할 경우 일부 기능이 지원되지 않습니다. 9-24 페이지의 클러스터링으로 지원되지 않는 기능를 참조하십시오.

ASA 클러스터링 정보

이 섹션에서는 클러스터링 아키텍처 및 이러한 아키텍처의 작동 방식에 대해 설명합니다.

ASA 클러스터를 네트워크에 맞게 활용하는 방법

클러스터는 하나의 유닛으로 작동하는 여러 개의 ASA로 구성됩니다. 클러스터로 작동하려면 ASA에는 다음과 같은 인프라가 필요합니다.

- 클러스터 내 커뮤니케이션을 위한 분리된 고속 백플레인 네트워크(또는 *클러스터 제어 링크*라고 함)
- 컨피그레이션 및 모니터링을 지원하는 각 ASA에 대한 관리 액세스

네트워크에 클러스터를 배치할 경우, 업스트림 및 다운스트림 라우터에서는 다음 중 한 가지 방법을 사용하여 클러스터로 들어오고 나가는 데이터의 로드 밸런싱을 수행할 수 있어야 합니다.

- Spanned EtherChannel(권장) — 클러스터의 여러 멤버에 대한 인터페이스는 단일 EtherChannel로 그룹화되며, EtherChannel은 유닛 간의 로드 밸런싱을 수행합니다.
- 정책 기반 라우팅(라우팅 방화벽 모드 전용) — 업스트림 및 다운스트림 라우터에서는 경로 맵 및 ACL을 사용하여 유닛 간의 로드 밸런싱을 수행합니다.
- Equal-Cost Multi-Path 라우팅(라우팅 방화벽 모드 전용) — 업스트림 및 다운스트림 라우터에서는 Equal Cost 고정 또는 동적 라우팅을 사용하여 유닛 간의 로드 밸런싱을 수행합니다.

관련 주제

성능 확장 팩터

클러스터에 여러 유닛을 결합할 경우 성능을 대략 다음과 같이 예측할 수 있습니다.

- 통합 처리량의 70%
- 최대 연결 수의 60%
- 초당 연결 수의 50%

예를 들어, 처리량의 경우 ASA 5585-X(SSP-40 포함)를 단독 실행하면 실제 방화벽 트래픽 중 약 10Gbps를 처리할 수 있습니다. 8개 유닛으로 구성된 클러스터의 경우 최대 통합 처리량은 80Gbps의 약 70%(유닛 8개 x 10Gbps), 즉 56Gbps에 해당합니다.

클러스터 구성원

클러스터 멤버는 보안 정책 및 트래픽 흐름을 공유하기 위해 서로 연동됩니다. 이 섹션에서는 각 멤버 역할의 특성을 설명합니다.

- 9-3 페이지의 부트스트랩 구성
- 9-3 페이지의 마스터 및 슬레이브 유닛 역할
- 9-3 페이지의 마스터 유닛 선택

부트스트랩 구성

각 디바이스에서 클러스터 이름, 클러스터 제어 링크 인터페이스, 기타 클러스터 설정 등을 비롯한 최소 부트스트랩 컨피그레이션을 컨피그레이션합니다. 클러스터링을 사용하는 첫 번째 유닛이 일반적으로 *마스터* 유닛이 됩니다. 후속 유닛에서 클러스터링을 사용하도록 설정할 경우, 해당 유닛은 클러스터에 *슬레이브*로 참가합니다.

마스터 및 슬레이브 유닛 역할

클러스터의 멤버 1개는 마스터 유닛입니다. 마스터 유닛은 부트스트랩 컨피그레이션의 우선순위 설정에 따라 결정됩니다. 우선순위는 1에서 100까지 1이 가장 높은 우선순위입니다. 기타 모든 멤버는 슬레이브 유닛입니다. 클러스터를 처음 생성할 경우, 추가되는 첫 번째 유닛은 해당 단계에서 클러스터의 유일한 유닛이므로 마스터 유닛이 됩니다.

마스터 유닛에서만 모든 컨피그레이션(부트스트랩 컨피그레이션 제외)을 수행해야 하며, 그 후 이러한 컨피그레이션은 슬레이브 유닛에 복제됩니다. 인터페이스와 같은 물리적 자산의 경우 마스터 유닛의 컨피그레이션은 모든 슬레이브 유닛에 미러링됩니다. 예를 들어, GigabitEthernet 0/1을 내부 인터페이스로 구성하고 GigabitEthernet 0/0을 외부 인터페이스로 구성할 경우 이러한 인터페이스는 슬레이브 유닛에서도 내부 및 외부 인터페이스로 사용됩니다.

일부 기능은 클러스터에서 확장되지 않으며 마스터 유닛에서 이러한 기능에 대한 모든 트래픽을 처리합니다.

관련 주제

- 9-25 페이지의 클러스터링을 위한 중앙 집중식 기능

마스터 유닛 선택

클러스터의 구성원은 클러스터 제어 링크로 통신을 수행하여 다음과 같은 방식으로 마스터 유닛을 선택합니다.

1. 유닛에 클러스터링을 사용할 경우(또는 이미 사용 설정된 클러스터링을 처음 시작할 경우), 선택 요청이 3초마다 전송됩니다.
2. 다른 유닛의 우선순위가 더 높을 경우 해당 유닛이 선택 요청에 응답하게 됩니다. 우선순위는 1에서 100까지 설정되며 1이 가장 높은 우선순위입니다.
3. 45초 후에 우선순위가 더 높은 다른 유닛에서 응답을 받지 못한 유닛은 마스터 유닛이 됩니다.

참고 가장 우선순위가 높은 유닛이 공동으로 여러 개인 경우, 클러스터 유닛 이름과 일련 번호를 사용하여 마스터 유닛을 결정합니다.

4. 유닛이 우선순위가 더 높은 클러스터에 참가한다고 해서 해당 유닛이 자동으로 마스터 유닛이 되는 것은 아닙니다. 기존 마스터 유닛은 응답이 중지되지 않는 한 항상 마스터 유닛으로 유지되며 응답이 중지될 때에 새 마스터 유닛이 선택됩니다.

참고 유닛을 수동으로 강제 변경하여 마스터 유닛이 되도록 할 수 있습니다. 중앙 집중식 기능의 경우 마스터 유닛을 강제로 변경하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

관련 주제

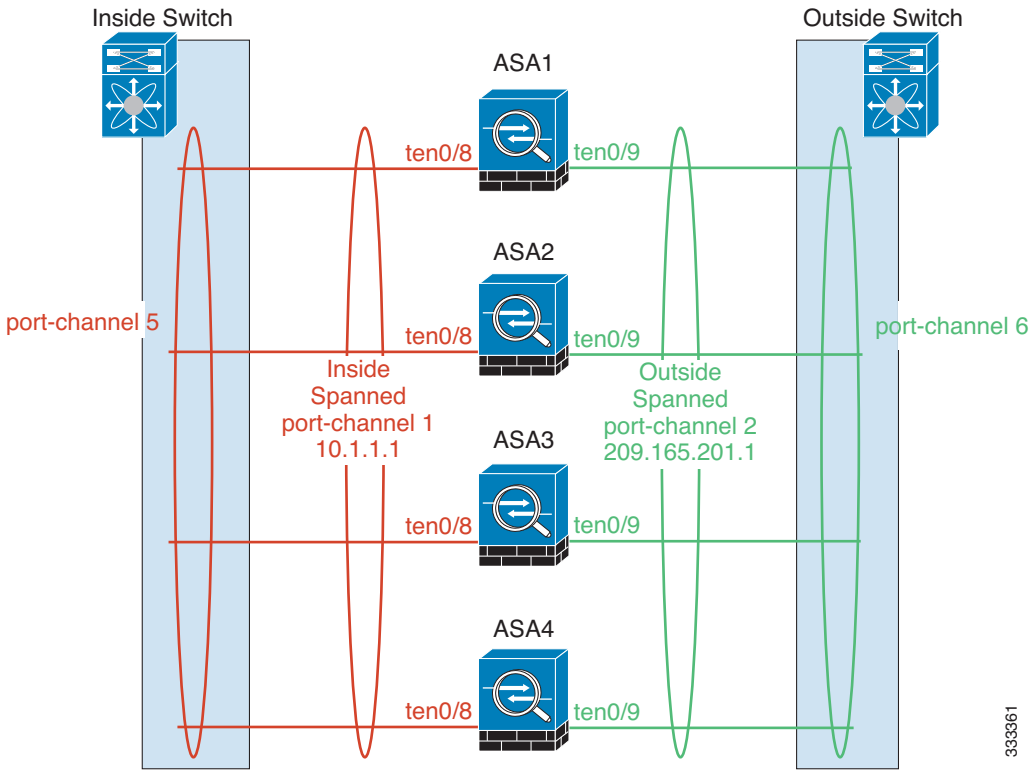
- 9-25 페이지의 클러스터링을 위한 중앙 집중식 기능

클러스터 인터페이스

데이터 인터페이스를 Spanned EtherChannel 또는 개별 인터페이스로 구성할 수 있습니다. 클러스터의 모든 데이터 인터페이스는 1가지 유형만 가능합니다.

Spanned EtherChannel(권장)

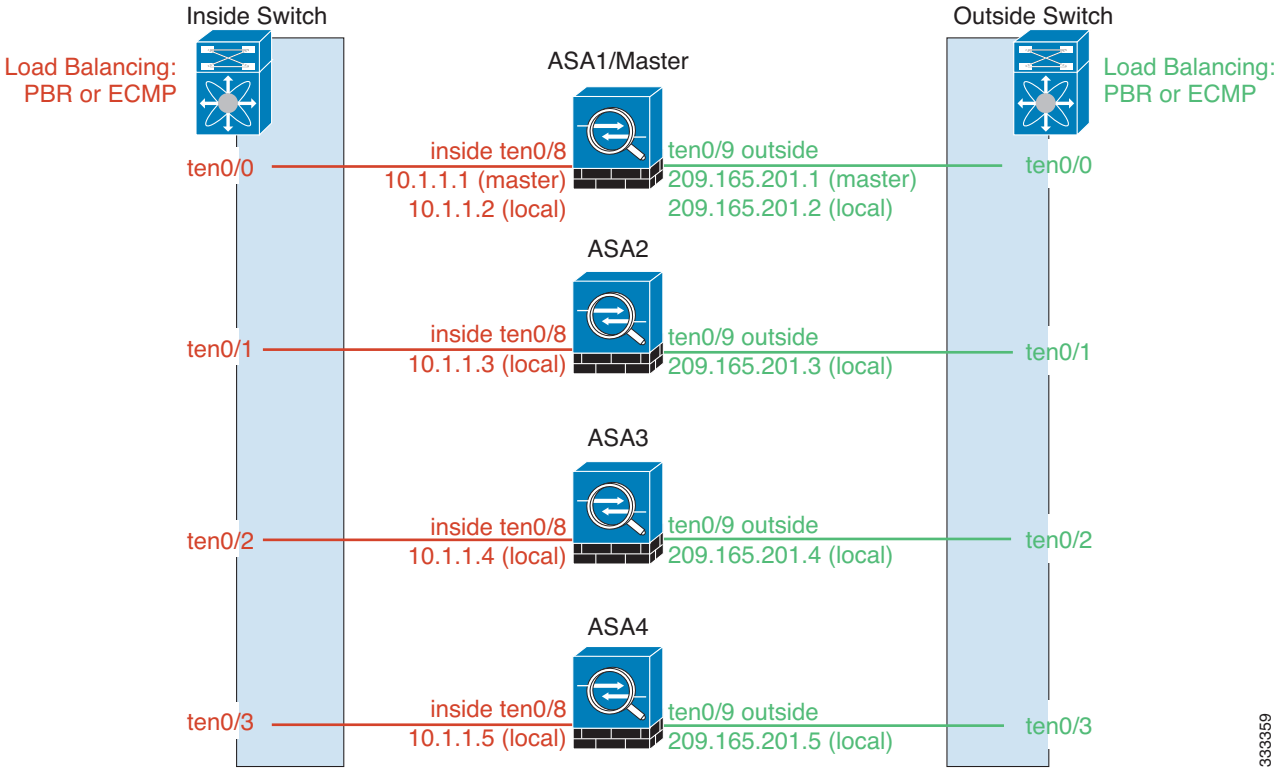
유닛당 하나 이상의 인터페이스를 클러스터 내의 모든 유닛을 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. Spanned EtherChannel은 라우팅 및 투명 방화벽 모드에서 모두 구성할 수 있습니다. 라우팅 모드의 경우 EtherChannel은 단일 IP 주소를 통해 라우팅된 인터페이스로 구성됩니다. 투명 모드의 경우 IP 주소가 인터페이스가 아닌 브릿지 그룹에 할당됩니다. EtherChannel은 기본적인 작동 시 로드 밸런싱을 함께 제공합니다.



개별 인터페이스(라우팅 방화벽 모드 전용)

개별 인터페이스는 정상적인 라우팅 인터페이스로, 각각 *로컬 IP 주소*가 있습니다. 인터페이스 컨피그레이션은 마스터 유닛에서만 컨피그레이션해야 하므로, 인터페이스 컨피그레이션을 사용하면 클러스터 컨피그레이션원에 대해 지정된 인터페이스에 사용할 IP 주소 풀을 설정할 수 있습니다. *기본 클러스터 IP 주소*는 현재 마스터 유닛에 항상 속해 있는 클러스터의 고정 주소입니다. 기본 클러스터 IP 주소는 마스터 유닛의 보조 IP 주소이며, 로컬 IP 주소는 항상 라우팅의 기본 주소입니다. 기본 클러스터 IP 주소에서는 주소에 대한 일관된 관리 액세스를 제공합니다. 마스터 유닛이 변경될 경우 주요 클러스터 IP 주소는 새 마스터 유닛으로 이동되므로 클러스터는 지속적으로 원활하게 관리됩니다. 그러나 이 경우 로드 밸런싱은 업스트림 스위치에서 별도로 구성해야 합니다.

참고 개별 인터페이스보다는 Spanned EtherChannel을 권장합니다. 그 이유는 개별 인터페이스의 경우 라우팅 프로토콜을 기반으로 트래픽의 로드 밸런싱을 수행하며, 라우팅 프로토콜은 링크 오류 발생 시 통합 속도가 느려지는 경우가 많습니다.



관련 주제

- 9-12 페이지의 로드 밸런싱 방법

클러스터 제어 링크

각 유닛에서는 최소 1개의 하드웨어 인터페이스를 클러스터 제어 링크로 지정해야 합니다.

클러스터 제어 링크 트래픽 개요

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

제어 트래픽에는 다음 사항이 해당됩니다.

- 마스터 선택
- 구성 복제
- 상태 모니터링

데이터 트래픽에는 다음 사항이 해당됩니다.

- 상태 복제
- 연결 소유권 쿼리 및 데이터 패킷 전송

관련 주제

- 9-3 페이지의 클러스터 구성원
- 9-10 페이지의 구성 복제
- 9-9 페이지의 유닛 상태 모니터링
- 9-10 페이지의 데이터 경로 연결 상태 복제
- 9-23 페이지의 클러스터 전반에 걸쳐 새 TCP 연결 재밸런싱

클러스터 제어 링크 인터페이스 및 네트워크

클러스터 제어 링크에는 모든 데이터 인터페이스를 사용할 수 있으나 다음 경우는 제외입니다.

- VLAN Subinterface는 클러스터 제어 링크로 사용할 수 없습니다.
- 관리 *x/x* 인터페이스는 단독으로든 EtherChannel로든 클러스터 제어 링크로 사용할 수 없습니다.
- ASA IPS 모듈이 포함된 ASA 5585-X의 경우 클러스터 제어 링크에 모듈 인터페이스를 사용할 수 없습니다. 그러나 ASA 5585-X 네트워크 모듈에서는 인터페이스를 사용할 수 있습니다.

EtherChannel 또는 이중화 인터페이스를 사용할 수 있습니다.

10기가비트 이더넷 인터페이스 2개가 내장된 SSP-10 및 SSP-20이 포함된 ASA 5585-X의 경우, 클러스터 제어 링크에는 하나의 인스턴스를 사용하고 데이터에는 나머지를 사용하는 것이 좋습니다. 이러한 설치 과정에서는 클러스터 제어 링크의 이중화를 수용하지 않으나, 클러스터 제어 링크의 크기를 데이터 인터페이스의 크기와 일치시켜야 하는 요구 사항은 충족합니다.

각 클러스터 제어 링크는 동일한 서브넷에 IP 주소가 있습니다. 이 서브넷은 모든 다른 트래픽과 분리되어 있어야 하며, 클러스터 제어 링크 ASA 인터페이스만 포함해야 합니다.

2-멤버 클러스터의 경우 클러스터 제어 링크를 ASA에서 다른 ASA로 직접 연결하지 마십시오. 인터페이스에 직접 연결할 경우, 유닛 하나에 오류가 발생하면 클러스터 제어 링크에도 오류가 발생하므로 나머지 정상 유닛에도 오류가 발생합니다. 스위치를 통해 클러스터 제어 링크를 연결할 경우 클러스터 제어 링크는 가동 상태를 유지하여 정상 유닛을 지원합니다.

관련 주제

- 9-7 페이지의 클러스터 제어 링크 이중화
- 9-7 페이지의 클러스터 제어 링크 크기 조정

클러스터 제어 링크 크기 조정

클러스터 제어 링크의 크기를 각 멤버의 예상 처리량에 맞게 조정해야 합니다. 예를 들어, 클러스터에 있는 유닛당 최대 14Gbps를 전달할 수 있는 ASA 5585-X(SSP-60 포함)를 보유한 경우, 최소 14Gbps를 전달할 수 있는 클러스터 제어 링크에 대한 인터페이스 또한 할당해야 합니다. 이 경우 클러스터 제어 링크의 EtherChannel에 10기가비트 이더넷 인터페이스 2개를 사용할 수 있으며, 데이터 링크에 필요한 경우 나머지 인터페이스를 사용합니다.

클러스터 제어 링크 트래픽은 주로 상태 업데이트 및 전달된 패킷으로 구성되어 있습니다. 클러스터 제어 링크의 트래픽 양은 언제든지 달라질 수 있습니다. 예를 들어, 상태 업데이트의 경우 통과 트래픽이 짧은 TCP 연결을 제외한 트래픽으로 구성되어 있다면 통과 트래픽의 최대 10%를 사용하게 될 수 있습니다. 전달된 트래픽의 양은 로드 밸런싱 효율성 또는 중앙 집중식 기능에 많은 트래픽이 있는지에 따라 좌우됩니다. 예:

- NAT의 경우 연결의 로드 밸런싱이 저하되며, 모든 반환 트래픽을 올바른 유닛으로 다시 밸런싱해야 합니다.
- 네트워크 액세스용 AAA는 중앙 집중식 기능이므로 모든 트래픽이 마스터 유닛으로 전달됩니다.
- 멤버가 변경된 경우, 클러스터에서는 다량의 연결을 다시 밸런싱해야 하므로 일시적으로 많은 양의 클러스터 제어 링크 대역폭을 사용합니다.

대역폭이 높은 클러스터 제어 링크를 사용하면 멤버가 변경될 경우 클러스터를 더 빠르게 통합할 수 있고 처리량 병목 현상을 방지할 수 있습니다.

참고 클러스터에 비대칭(다시 밸런싱된) 트래픽이 많은 경우 클러스터 제어 링크 크기를 늘려야 합니다.

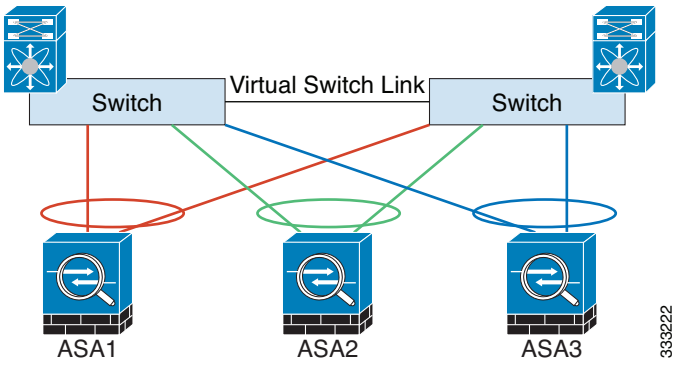
관련 주제

- 9-18 페이지의 사이트 간 클러스터링.

클러스터 제어 링크 이중화

클러스터 제어 링크에는 EtherChannel을 사용하는 편이 바람직하며, 이렇게 할 경우 EtherChannel 내의 여러 링크에 트래픽을 전달하는 동시에 이중화를 실현할 수 있습니다.

다음 다이어그램에는 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel) 환경에서 EtherChannel을 클러스터 제어 링크로 사용하는 방법이 나와 있습니다. EtherChannel의 모든 링크가 활성화되어 있습니다. 스위치가 VSS 또는 vPC의 일부일 경우 ASA 인터페이스를 동일한 EtherChannel 내에서 연결하여 VSS 또는 vPC의 스위치와 별도로 분리할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 수행하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다. 이러한 EtherChannel은 디바이스 로컬이 아닌 Spanned EtherChannel입니다.



클러스터 제어 링크 안정성

클러스터 제어 링크 기능을 보장하려면 유닛 간의 RTT(왕복 시간)가 20ms 이하여야 합니다. 이러한 최대 레이턴시는 서로 다른 지리적 사이트에 설치된 클러스터 멤버와의 호환성을 개선하는 역할을 합니다. 레이턴시를 확인하려면 유닛 간의 클러스터 제어 링크에서 Ping을 수행합니다.

클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 사이트 간 구축의 경우 전용 링크를 사용해야 합니다.

클러스터 제어 링크 오류

유닛의 클러스터 제어 링크 라인 프로토콜이 작동되지 않을 경우, 클러스터링을 사용할 수 없게 되며 데이터 인터페이스가 종료됩니다. 클러스터 제어 링크를 해결한 후 클러스터링을 다시 사용하도록 설정하여 클러스터에 수동으로 다시 참가해야 합니다.

참고 ASA가 비활성화되면 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드한 후에도 유닛이 클러스터 내에서 비활성 상태일 경우, 관리 인터페이스에서는 마스터 유닛과 동일한 기본 IP 주소를 사용하므로 관리 인터페이스에 액세스할 수 없습니다. 추가 컨피그레이션을 위해서는 콘솔 포트를 사용해야 합니다.

관련 주제

9-10 페이지의 클러스터 다시 참가

ASA 클러스터 내의 고가용성

ASA 클러스터링에서는 유닛과 인터페이스의 상태를 모니터링하고 유닛 간의 연결 상태를 복제하여 고가용성을 제공합니다.

- 9-9 페이지의 유닛 상태 모니터링
- 9-9 페이지의 인터페이스 모니터링
- 9-9 페이지의 유닛 또는 인터페이스 오류
- 9-10 페이지의 데이터 경로 연결 상태 복제

유닛 상태 모니터링

마스터 유닛에서는 클러스터 제어 링크를 통해 keepalive 메시지를 주기적으로 전송하여 모든 슬레이브 유닛을 모니터링합니다(기간은 구성 가능함). 각 슬레이브 유닛에서는 동일한 메커니즘을 사용하여 마스터 유닛을 모니터링합니다.

인터페이스 모니터링

각 유닛에서는 사용 중인 모든 하드웨어 인터페이스의 링크 상태를 모니터링하며 상태 변경 사항을 마스터 유닛에 보고합니다.

- Spanned EtherChannel — 클러스터 cLACP(Link Aggregation Control Protocol)를 사용합니다. 각 유닛에서는 링크 상태 및 cLACP 프로토콜 메시지를 모니터링하여 EtherChannel에서 포트가 아직 활성화된 상태인지 확인합니다. 상태가 마스터 유닛에 보고됩니다.
- 개별 인터페이스(라우팅 모드 전용) — 각 유닛에서는 인터페이스를 스스로 모니터링하고 인터페이스 상태를 마스터 유닛에 보고합니다.

유닛 또는 인터페이스 오류

상태 모니터링 기능이 사용 설정된 경우, 유닛에 오류가 발생하거나 유닛의 인터페이스에 오류가 발생하면 클러스터에서 해당 유닛이 제거됩니다. 특정 유닛의 인터페이스에 오류가 발생하였으나 다른 유닛의 동일한 인터페이스는 활성 상태인 경우, 클러스터에서 해당 특정 유닛이 제거됩니다. ASA에서 클러스터의 멤버를 제거하기 전까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 좌우됩니다. EtherChannel(Spanned 또는 일반)의 경우, 설정된 멤버에 대한 인터페이스가 중지될 경우 ASA에서는 9초 후에 해당 멤버를 제거합니다. ASA에서는 유닛이 클러스터에 참가하는 처음 90초 동안에는 인터페이스를 모니터링하지 않습니다. 이 시간 동안에는 인터페이스 상태가 변경되어도 ASA가 클러스터에서 제거되지 않습니다. 비 EtherChannel의 경우, 멤버 상태와 관계없이 500ms 후에 유닛이 제거됩니다.

클러스터의 유닛에 오류가 발생할 경우, 해당 유닛에서 호스팅하는 연결이 다른 유닛으로 원활하게 전송되며 트래픽에 대한 상태 정보가 제어 클러스터 링크를 통해 공유됩니다.

마스터 유닛에 오류가 발생할 경우, 우선순위가 가장 높은(숫자가 가장 낮은) 클러스터의 다른 멤버가 마스터 유닛이 됩니다.

ASA에서는 클러스터에 자동으로 다시 참가하려고 합니다.

참고 ASA가 비활성화되고 클러스터에 자동으로 다시 참가하지 못할 경우, 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드한 후에도 유닛이 클러스터 내에서 비활성 상태일 경우, 관리 인터페이스에서는 마스터 유닛과 동일한 기본 IP 주소를 사용하므로 관리 인터페이스에 액세스할 수 없습니다. 추가 컨피그레이션을 위해서는 콘솔 포트를 사용해야 합니다.

관련 주제

9-10 페이지의 클러스터 다시 참가

클러스터 다시 참가

클러스터 멤버가 클러스터에서 제거된 후 해당 멤버가 클러스터에 다시 참가할 수 있는 방법은 처음에 제거된 이유에 따라 결정됩니다.

- 클러스터 제어 링크 오류 — 클러스터 제어 링크의 문제를 해결한 후에는콘솔 포트에서 클러스터링을 다시 사용 설정함으로써 클러스터에 수동으로 다시 참가해야 합니다.
- 데이터 인터페이스 오류 — ASA에서는 5분에 다시 참가를 시도하며 그 다음에는 10분, 마지막으로 20분에 참가를 시도합니다. 20분 후에도 참가가 이루어지지 않을 경우 ASA에서는 클러스터링을 비활성화합니다. 데이터 인터페이스 문제를 해결한 후에는.
- 유닛 오류 — 유닛 상태 검사 오류로 인해 클러스터에서 유닛이 제거된 경우, 클러스터에 다시 참가할 수 있을지 여부는 오류의 원인에 따라 결정됩니다. 예를 들어, 일시적인 정전이 발생한 경우 클러스터 제어 링크가 활성 상태이고.

관련 주제

- 9-50 페이지의 ASA 클러스터 매개변수 구성

데이터 경로 연결 상태 복제

모든 연결마다 클러스터 내에 하나의 소유자 및 최소 하나의 백업 소유자가 있습니다. 백업 소유자는 오류 발생 시 연결을 인계받는 대신 TCP/UDP 상태 정보를 저장하므로, 오류가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있습니다.

소유자를 사용할 수 없을 경우, 연결에서 패킷을 받을(로드 밸런싱을 기준으로) 첫 번째 유닛이 백업 소유자에 관련 상태 정보를 문의하면 해당 백업 소유자가 새로운 소유자가 될 수 있습니다.

일부 트래픽의 경우 TCP 또는 UDP 레이어 상위에 대한 상태 정보가 필요합니다. 클러스터링 지원에 대해 알아보거나 이러한 종류의 트래픽에 대한 지원이 부족한 경우 다음 표를 참조하십시오.

표 9-1 클러스터 전반에 걸쳐 복제된 ASA 기능

트래픽	상태 지원	참고
가동 시간	예	시스템 가동 시간을 추적합니다.
ARP 테이블	예	투명 모드 전용입니다.
MAC 주소 테이블	예	투명 모드 전용입니다.
사용자 ID	예	AAA 규칙(uauth)을 포함하고 방화벽을 식별합니다.
IPv6 인접 데이터베이스	예	—
동적 라우팅	예	—
SNMP 엔진 ID	아니요	—
VPN(사이트 대 사이트)	아니요	마스터 유닛에 오류가 발생할 경우 VPN 세션의 연결이 끊어집니다.

구성 복제

클러스터의 모든 유닛에서는 단일 컨피그레이션을 공유합니다. 초기 부트스트랩 컨피그레이션을 제외하고, 마스터 유닛에서는 컨피그레이션만 변경할 수 있으며 변경 사항은 클러스터의 모든 다른 유닛에 자동으로 복제됩니다.

ASA 클러스터 관리

ASA 클러스터링을 사용하는 데 따른 여러 장점 중 하나는 관리하기가 쉽다는 점입니다. 이 섹션에서는 클러스터를 관리하는 방법에 대해 설명합니다.

관리 네트워크

모든 유닛을 단일한 관리 네트워크에 연결하는 것이 좋습니다. 이러한 네트워크는 클러스터 제어 링크와 분리되어 있습니다.

관리 인터페이스

관리 인터페이스의 경우 전용 관리 인터페이스 중 하나를 사용하는 것이 좋습니다. 관리 인터페이스를 개별 인터페이스(라우팅 및 투명 모드용 모두 해당) 또는 Spanned EtherChannel 인터페이스로 구성할 수 있습니다.

데이터 인터페이스에 Spanned EtherChannel을 사용 중인 경우에도, 관리용으로는 개별 인터페이스를 사용하는 것이 좋습니다. 개별 인터페이스를 사용하면 필요한 경우 각 유닛에 직접 연결할 수 있는 반면, Spanned EtherChannel 인터페이스의 경우에는 현재 마스터 유닛에 원격 연결만 가능합니다.

참고 Spanned EtherChannel 인터페이스 모드를 사용 중이고 관리 인터페이스를 개별 인터페이스로 구성할 경우, 관리 인터페이스에 동적 라우팅을 사용할 수 없습니다. 고정 라우팅을 사용해야 합니다.

개별 인터페이스의 경우, 기본 클러스터 IP 주소는 현재 마스터 유닛에 항상 속해 있는 클러스터의 고정 주소입니다. 각 인터페이스에는 주소의 범위를 구성하여 현재 마스터를 비롯한 각 유닛에서 해당 범위의 로컬 주소를 사용할 수 있도록 합니다. 기본 클러스터 IP 주소에서는 주소에 대한 일관된 관리 액세스를 제공합니다. 마스터 유닛이 변경될 경우 주요 클러스터 IP 주소는 새 마스터 유닛으로 이동되므로 클러스터는 지속적으로 원활하게 관리됩니다. 로컬 IP 주소는 라우팅에 사용되며 문제 해결에도 도움이 됩니다.

예를 들어, 현재 마스터 유닛에 항상 연결되어 있는 기본 클러스터 IP 주소에 연결하여 클러스터를 관리할 수 있습니다. 로컬 IP 주소에 연결하여 개별 멤버를 관리할 수 있습니다.

TFTP 또는 syslog 같은 아웃바운드 관리 트래픽의 경우 마스터 유닛을 비롯한 각 유닛에서는 로컬 IP 주소를 사용하여 서버에 연결합니다.

Spanned EtherChannel 인터페이스에는 하나의 IP 주소만 구성할 수 있으며, 해당 IP 주소는 항상 마스터 유닛에 연결됩니다. EtherChannel 인터페이스를 사용할 경우 슬레이브 유닛에 직접 연결할 수 없으며, 관리 인터페이스는 개별 인터페이스로 구성하는 것이 좋습니다. 이렇게 하면 각 유닛에 연결할 수 있습니다. 디바이스-로컬 EtherChannel을 관리용으로 사용할 수 있습니다.

마스터 유닛 관리 및 슬레이브 유닛 관리 비교

부트스트랩 컨피그레이션을 제외하고, 모든 관리 및 모니터링 작업은 마스터 유닛에서 이루어질 수 있습니다. 마스터 유닛에서 런타임 통계, 리소스 사용량 또는 모든 유닛의 기타 모니터링 정보를 확인할 수 있습니다. 또한 클러스터 내의 모든 유닛에 명령을 배포하고, 슬레이브 유닛의 콘솔 메시지를 마스터 유닛으로 복제할 수 있습니다.

필요한 경우 슬레이브 유닛을 직접 모니터링할 수 있습니다. 마스터 유닛에서도 사용 가능하지만 슬레이브 유닛에서 파일 관리를 수행할 수 있습니다(컨피그레이션 백업 및 이미지 업데이트 포함). 다음 기능은 마스터 유닛에서 사용할 수 없습니다.

- 유닛당 클러스터별 통계 모니터링
- 유닛당 Syslog 모니터링
- SNMP
- NetFlow

RSA 키 복제

마스터 유닛에서 RSA 키를 생성할 경우, 해당 키는 모든 슬레이브 유닛에 복제됩니다. 기본 클러스터 IP 주소에 대한 SSH 세션이 있는 경우 마스터 유닛에 오류가 발생하면 연결이 끊어집니다. 새 마스터 유닛에서는 SSH 연결에 동일한 키를 사용하므로, 새 마스터 유닛에 다시 연결할 때 캐시된 SSH 호스트 키를 업데이트하지 않아도 됩니다.

ASDM 연결 인증서 IP 주소 불일치

기본적으로, 자체 서명된 인증서는 로컬 IP 주소를 기준으로 ASDM 연결에 사용됩니다. ASDM을 사용하여 기본 클러스터 IP 주소를 연결할 경우, 인증서에서는 기본 클러스터 IP 주소가 아닌 로컬 IP 주소를 사용하므로 IP 주소가 일치하지 않는다는 경고 메시지가 표시됩니다. 이 메시지를 무시하고 ASDM 연결을 설정할 수 있습니다. 그러나 이러한 유형의 경고를 방지하려면 기본 클러스터 IP 주소 및 IP 주소 풀의 모든 로컬 IP 주소가 포함된 인증서를 등록하면 됩니다. 그런 다음 이 인증서를 각 클러스터 멤버에 사용할 수 있습니다.

관련 주제

- 35 장, “디지털 인증서”.

로드 밸런싱 방법

사용 가능한 로드 밸런싱 방법은 방화벽 모드 및 인터페이스 유형에 따라 다릅니다.

- 9-13 페이지의 Spanned EtherChannel(권장)
- 9-17 페이지의 정책 기반 라우팅(라우팅 방화벽 모드 전용)
- 9-18 페이지의 Equal-Cost Multi-Path 라우팅(라우팅 방화벽 모드 전용)

Spanned EtherChannel(권장)

유닛당 하나 이상의 인터페이스를 클러스터 내의 모든 유닛을 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다.

Spanned EtherChannel 이점

EtherChannel 로드 밸런싱 방식을 다른 방법보다 우선하여 권장하는 이유는 다음과 같은 이점 때문입니다.

- 신속한 오류 발견
- 빠른 통합 시간 개별 인터페이스에서는 라우팅 프로토콜을 기반으로 트래픽의 로드 밸런싱을 수행하며, 라우팅 프로토콜은 링크 오류 발생 시 통합 속도가 느려지는 경우가 많습니다.
- 컨피그레이션의 용이성

관련 주제

10-4 페이지의 EtherChannel

최대 처리량에 대한 지침

최대 처리량을 달성하기 위해서는 다음 사항을 권장합니다.

- "대칭"을 이루는 로드 밸런싱 해시 알고리즘을 사용합니다. 이는 즉, 양방향의 패킷의 해시가 동일하며 패킷이 Spanned EtherChannel 내의 동일한 ASA로 전송됨을 의미합니다. 소스와 목적지 IP 주소(기본값) 또는 소스와 목적지 포트를 해싱 알고리즘으로 사용하는 것이 좋습니다.
- ASA를 스위치에 연결할 경우 동일한 유형의 라인 카드를 사용하여 모든 패킷에 동일한 해싱 알고리즘이 적용되도록 합니다.

로드 밸런싱

소스 또는 목적지 IP 주소 및 TCP, UDP 포트 번호를 기준으로 전용 해시 알고리즘을 사용하여 EtherChannel 링크를 선택합니다.

참고 ASA에서는 로드 밸런싱 알고리즘 기본값을 변경하지 마십시오. 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 또는 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 ASA에 트래픽이 균일하지 않게 분산될 수 있기 때문입니다.

EtherChannel의 링크 수는 로드 밸런싱에 영향을 미칩니다.

경우에 따라 대칭 로드 밸런싱이 가능하지 않을 수 있습니다. NAT를 구성할 경우, 전달 및 반환 패킷의 IP 주소 및/또는 포트는 서로 다릅니다. 반환 트래픽은 해시에 따라 서로 다른 유닛에 전송되며, 클러스터에서는 가장 많이 반환되는 트래픽을 현재 유닛에 리디렉션하게 됩니다.

관련 주제

- 10-22 페이지의 EtherChannel 맞춤화
- 10-6 페이지의 로드 밸런싱
- 9-28 페이지의 NAT 및 클러스터링

EtherChannel 이중화

EtherChannel에는 이중화 기능이 내장되어 있으며, 모든 링크의 라인 프로토콜 상태를 모니터링합니다. 링크 하나에 오류가 발생하면 나머지 링크 간의 트래픽이 재밸런싱됩니다. 특정 유닛에서 EtherChannel의 모든 링크에 오류가 발생했으나 다른 유닛은 아직 가동 중인 경우, 클러스터에서 특정 유닛이 제거됩니다.

VSS 또는 vPC에 연결

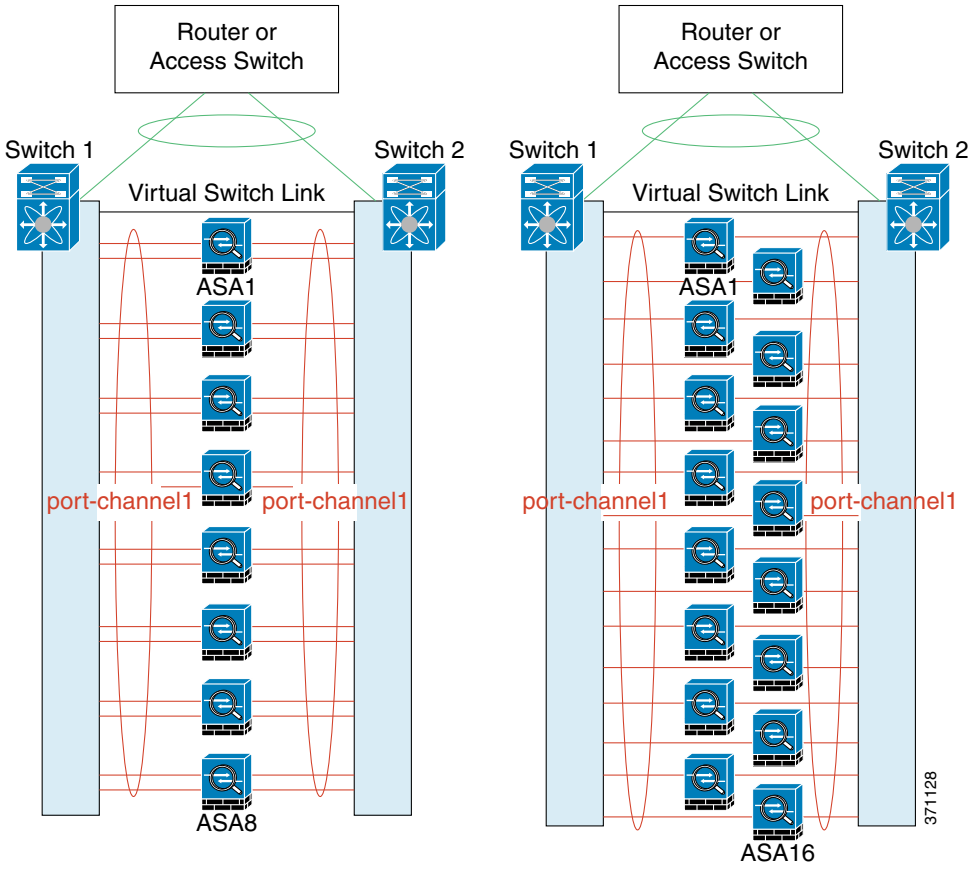
Spanned EtherChannel에서 ASA당 여러 인터페이스를 포함할 수 있습니다. ASA당 여러 인터페이스는 VSS 또는 vPC에서 두 스위치에 모두 연결하는 경우에 특히 유용합니다.

스위치에 따라 Spanned EtherChannel에서 활성 링크를 최대 32개까지 구성할 수 있습니다. 이 기능을 사용하려면 각각 16개의 활성 링크가 포함된 EtherChannel(예: F2-Series 10기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000)을 지원하는 vPC의 두 스위치가 필요합니다.

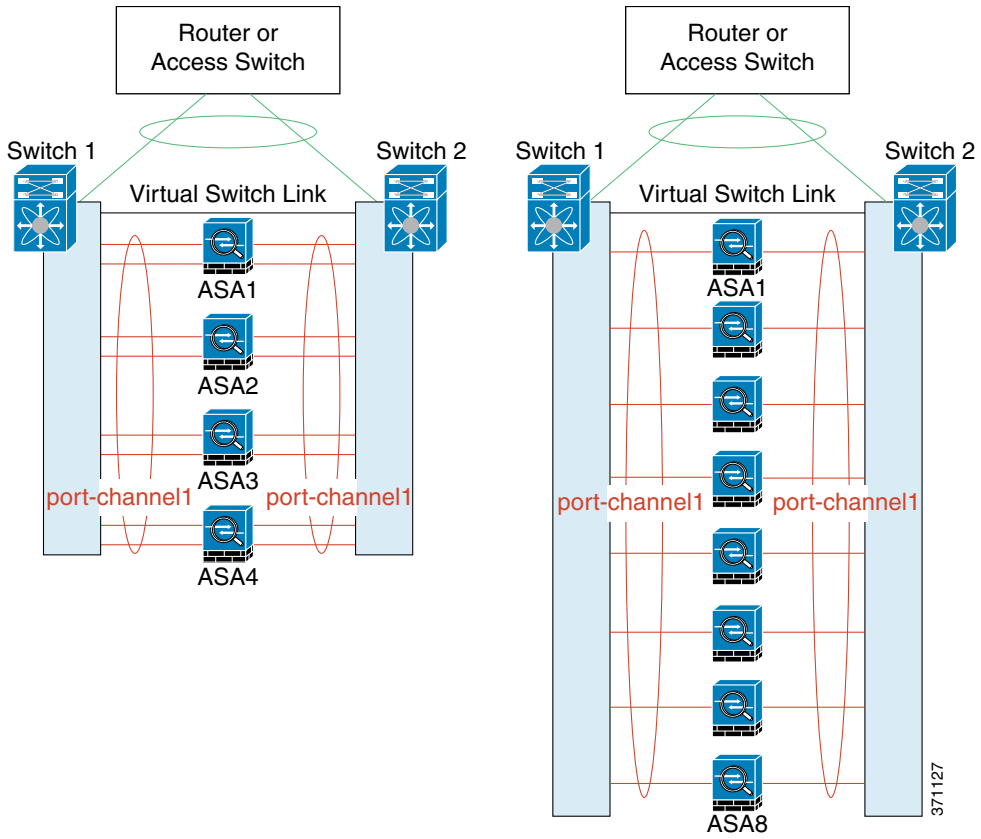
EtherChannel에서 8개의 활성 링크를 지원하는 스위치를 사용하려면, VSS/vPC에서 2개의 스위치에 연결할 때 Spanned EtherChannel에 최대 16개의 활성 링크를 구성하면 됩니다.

Spanned EtherChannel에서 활성 링크를 8개 이상 사용하려는 경우 스탠바이 링크까지 보유할 수는 없습니다. 활성 링크를 9~32개까지 지원하려면 스탠바이 링크의 사용을 허용하는 cLACP 동적 포트 우선순위를 비활성화해야 합니다. 단일 스위치에 연결하는 경우와 같이, 필요한 경우에는 활성 링크 8개와 스탠바이 링크 8개를 계속 사용할 수 있습니다.

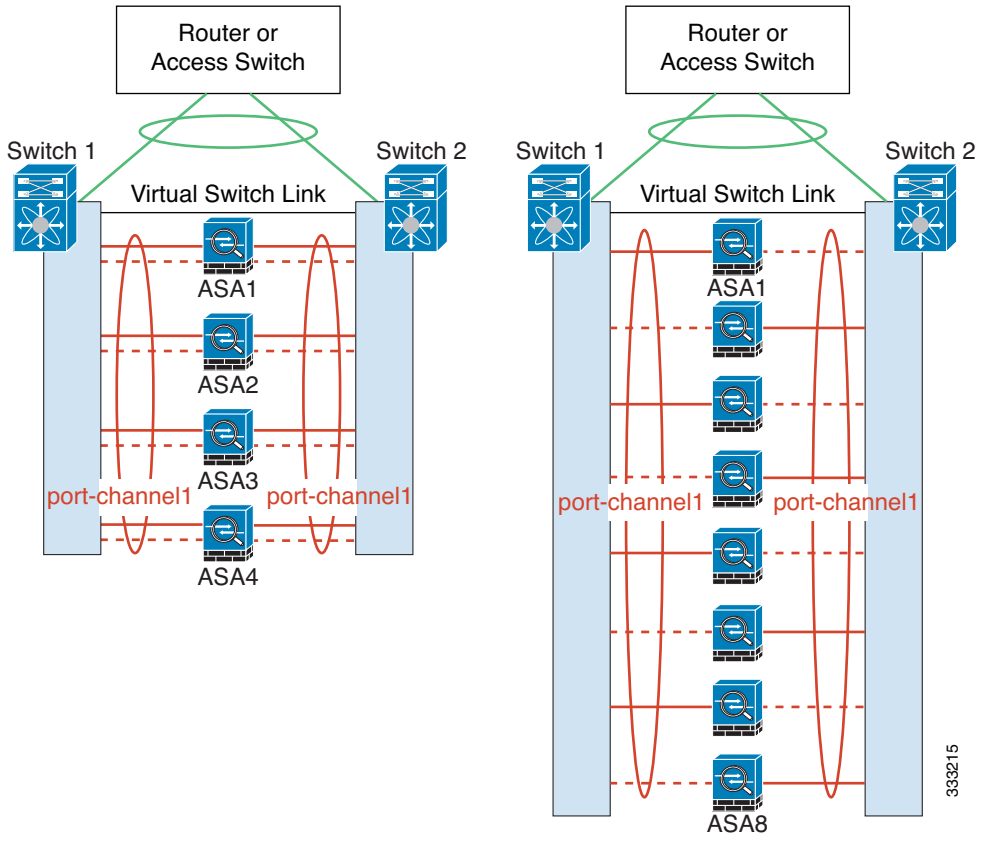
다음 그림에는 8-ASA 클러스터 및 16-ASA 클러스터의 32개 활성 링크 Spanned EtherChannel이 나와 있습니다.



다음 그림에는 4-ASA 클러스터 및 8-ASA 클러스터의 16개 활성 링크 Spanned EtherChannel이 나와 있습니다.



다음 그림에는 4-ASA 클러스터 및 8-ASA 클러스터의 8개 활성/8개 스탠바이 링크 Spanned EtherChannel이 나와 있습니다. 활성 링크는 실선으로 표시되어 있고 비활성 링크는 점선으로 표시되어 있습니다. cLACP 로드 밸런싱의 경우 EtherChannel에서 활성화할 최상의 링크 8개를 자동으로 선택합니다. 그림과 같이, cLACP를 사용하면 링크 수준에서 로드 밸런싱을 실현하는 데 도움이 됩니다.



정책 기반 라우팅(라우팅 방화벽 모드 전용)

개별 인터페이스를 사용할 경우, 각각의 ASA 인터페이스에서는 자신의 IP 주소 및 MAC 주소를 계속 사용합니다. 로드 밸런싱 방법 중 하나는 PBR(정책 기반 라우팅)입니다.

이미 PBR을 사용 중이고 기존 인프라를 활용하려는 경우 이 방법을 권장합니다. 이 방법에서는 추가적인 튜닝 옵션 및 Spanned EtherChannel을 제공할 수 있습니다.

PBR 방법의 경우 경로 맵 및 ACL을 기준으로 라우팅을 결정합니다. 클러스터에 있는 모든 ASA 간의 트래픽을 수동으로 나누어야 합니다. PBR은 고정이므로 매번 최적의 로드 밸런싱 결과를 달성할 수 있는 것은 아닙니다. 최상의 성능을 실현하려면 연결의 전달 및 반환 패킷이 동일한 물리적 ASA에 전달되도록 PBR 정책을 구성하는 것이 좋습니다. 예를 들어, Cisco 라우터가 있는 경우 Cisco IOS PBR with Object Tracking을 사용하여 이중화를 구현할 수 있습니다. Cisco IOS Object Tracking에서는 ICMP Ping을 사용하여 각각의 ASA를 모니터링합니다. 그런 다음 특정 ASA의 도달 범위를 기준으로 경로 맵을 사용하거나 사용하지 않도록 설정할 수 있습니다. 자세한 내용은 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

참고 이 로드 밸런싱 방법을 사용할 경우 디바이스-로컬 EtherChannel을 개별 인터페이스로 사용할 수 있습니다.

Equal-Cost Multi-Path 라우팅(라우팅 방화벽 모드 전용)

개별 인터페이스를 사용할 경우, 각각의 ASA 인터페이스에서는 자신의 IP 주소 및 MAC 주소를 계속 사용합니다. 로드 밸런싱 방법 중 하나는 ECMP(Equal-Cost Multi-Path) 라우팅입니다.

이미 ECMP를 사용 중이고 기존 인프라를 활용하려는 경우 이 방법을 권장합니다. 이 방법에서는 추가적인 튜닝 옵션 및 Spanned EtherChannel을 제공할 수 있습니다.

ECMP 라우팅을 사용하면 라우팅 메트릭에서 가장 순위가 높은 여러 가지 "최상의 경로"를 통해 패킷을 전달할 수 있습니다. EtherChannel과 마찬가지로, 소스와 목적지 IP 주소 및/또는 소스와 목적지 포트의 해시를 사용하여 다음 홉 중 하나로 패킷을 보낼 수 있습니다. ECMP 라우팅을 위한 고정 경로를 사용할 경우, ASA 오류가 발생하면 문제를 초래할 수 있습니다. 경로는 계속 사용할 수 있으며 오류가 발생한 ASA에 대한 트래픽은 손실됩니다. 고정 경로를 사용할 경우 Object Tracking 같은 고정 경로 모니터링 기능을 사용할 수 있는지 확인하십시오. 동적 라우팅 프로토콜을 사용하여 경로를 추가 및 제거하는 것이 좋으며, 이 경우 동적 라우팅에 참여하도록 각 ASA를 구성해야 합니다.

참고 이 로드 밸런싱 방법을 사용할 경우 디바이스-로컬 EtherChannel을 개별 인터페이스로 사용할 수 있습니다.

사이트 간 클러스터링

사이트 간 설치의 경우 다음 지침을 준수하여 ASA 클러스터링을 활용할 수 있습니다.

- 9-18 페이지의 사이트 간 클러스터링 지침
- 9-19 페이지의 데이터 센터 인터커넥트 크기 조정
- 9-20 페이지의 사이트 간 예

사이트 간 클러스터링 지침

사이트 간 클러스터링에 대한 다음 지침을 참조하십시오.

- 다음과 같은 인터페이스 및 방화벽 모드에서는 사이트 간 클러스터링을 지원합니다.

	방화벽 모드	
인터페이스 모드	라우팅	투명
개별 인터페이스	예	N/A
Spanned EtherChannel	아니요	예

- 클러스터 제어 링크 레이턴시는 RTT(왕복 시간)가 20ms 이하여야 합니다.
- 클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 전용 링크를 사용해야 합니다.
- 연결 재밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 연결이 재밸런싱됩니다.
- 클러스터를 구현할 경우 여러 사이트에 있는 멤버가 구분되지 않습니다. 따라서 하나의 특정한 연결의 연결 역할은 사이트 전체를 포괄하게 될 수 있습니다. 이는 정상적인 동작입니다.

- 투명 모드의 경우 내부 라우터에서 모두 동일한 MAC 주소를 공유하는지 확인하고, 외부 라우터에서도 모두 동일한 MAC 주소를 공유하는지 확인해야 합니다. 사이트 1의 클러스터 멤버가 사이트 2의 멤버에 연결을 전달할 경우, 목적지 MAC 주소가 유지됩니다. MAC 주소가 사이트 1의 라우터와 동일할 경우 패킷은 사이트 2의 라우터에만 도달합니다.
- Spanned EtherChannel 모드의 경우 데이터 사이트 간의 ASA 클러스터에 직접 연결된 데이터 VLAN을 확장하지 않습니다. 이렇게 할 경우 루프가 발생합니다. 확장된 데이터 VLAN은 라우터를 통해 클러스터와 분리해야 합니다.

관련 주제

- 9-23 페이지의 클러스터 전반에 걸쳐 새 TCP 연결 재밸런싱
- 9-22 페이지의 연결 역할

데이터 센터 인터커넥트 크기 조정

클러스터 제어 링크 트래픽을 처리하기 위한 DCI(데이터 센터 인터커넥트) 대역폭을 다음 계산과 같이 예약해야 합니다.

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

각 사이트의 멤버 수가 다를 경우, 더 큰 숫자를 계산에 사용합니다. DCI의 최소 대역폭은 한 멤버에 대한 클러스터 제어 링크의 크기보다 작으면 안 됩니다.

예:

- 2개 사이트에 멤버가 4개인 경우:
  - 총 클러스터 멤버 4개
  - 각 사이트당 멤버 2개
  - 멤버당 5Gbps 클러스터 제어 링크

  예약된 DCI 대역폭 = 5Gbps(2/2 x 5Gbps)
- 2개 사이트에 멤버가 8개인 경우 크기가 다음과 같이 증가함:
  - 총 클러스터 멤버 8개
  - 사이트당 멤버 4개
  - 멤버당 5Gbps 클러스터 제어 링크

  예약된 DCI 대역폭 = 10Gbps(4/2 x 5Gbps)
- 3개 사이트에 멤버가 6개인 경우:
  - 총 클러스터 멤버 6개
  - 사이트 1에 멤버 3개, 사이트 2에 멤버 2개, 사이트 3에 멤버 1개
  - 멤버당 10Gbps 클러스터 제어 링크

  예약된 DCI 대역폭 = 15Gbps(3/2 x 10Gbps)
- 2개 사이트에 멤버가 2개인 경우:
  - 총 클러스터 멤버 2개
  - 각 사이트당 멤버 1개
  - 멤버당 10Gbps 클러스터 제어 링크

예약된 DCI 대역폭 = 10Gbps(1/2 x 10Gbps = 5Gbps). 그러나 최소 대역폭은 클러스터 제어 링크의 크기(10Gbps)보다 작으면 안 됩니다.

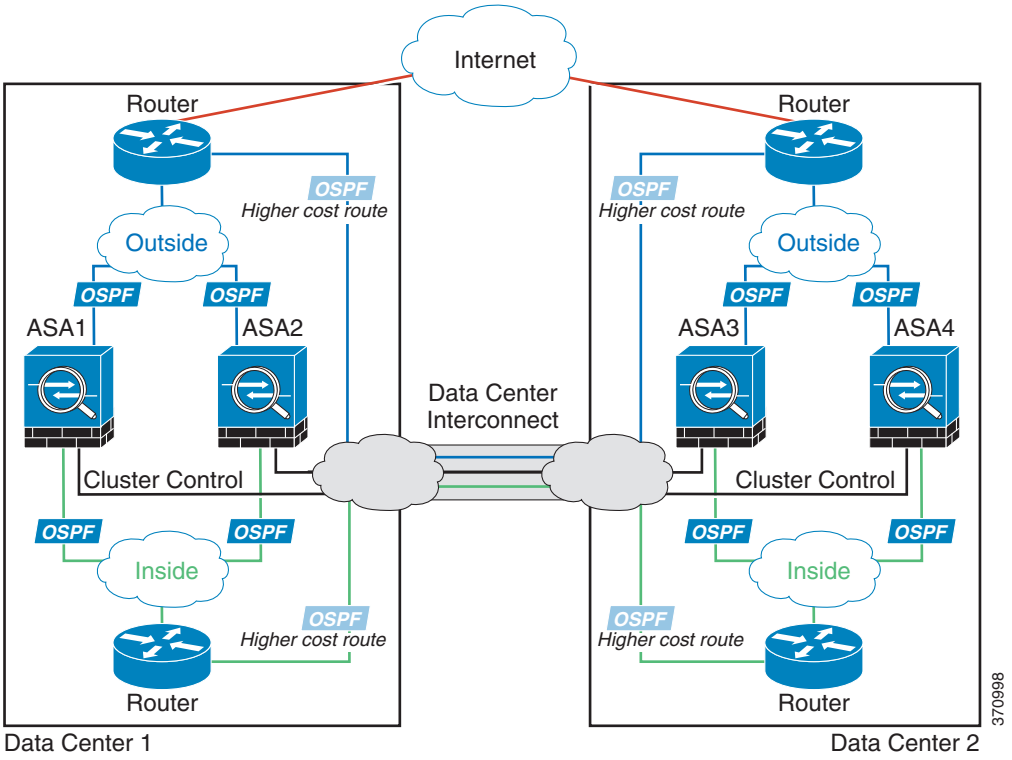
사이트 간 예

다음 예에는 지원되는 클러스터 구축에 대한 내용이 나와 있습니다.

- 9-20 페이지의 개별 인터페이스 사이트 간 예
- 9-21 페이지의 Spanned EtherChannel 투명 모드 사이트 간 예

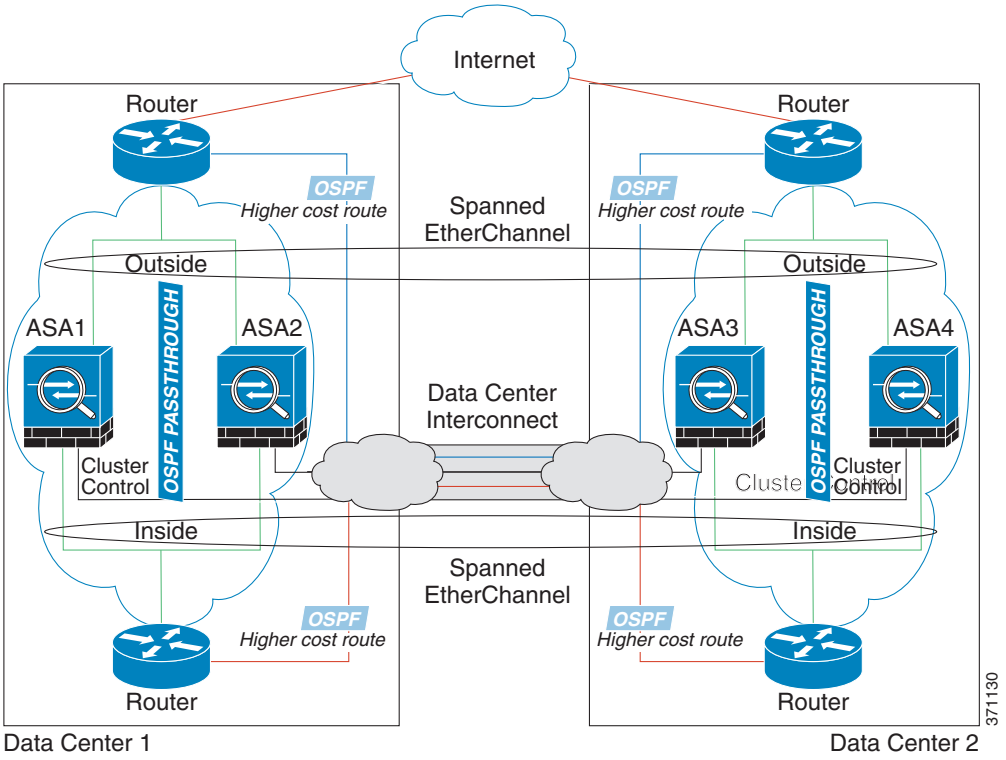
개별 인터페이스 사이트 간 예

다음 예에는 각 데이터 센터 2개의 ASA 클러스터 멤버 2개가 나와 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 데이터 센터의 내부 및 외부 라우터에서는 OSPF와 PBR 또는 ECMP를 사용하여 클러스터 멤버 간의 트래픽을 로드 밸런싱합니다. DCI를 통해 비용이 높은 경로를 할당하면 특정 사이트의 모든 ASA 클러스터 멤버가 가동 중지되지 않는 한 각 데이터 센터 내에서 트래픽이 유지됩니다. 어느 한 사이트의 모든 클러스터 멤버에 오류가 발생할 경우, 각 라우터의 트래픽은 DCI를 통해 다른 사이트의 ASA 클러스터 멤버로 이동합니다.



Spanned EtherChannel 투명 모드 사이트 간 예

다음 예에는 각 데이터 센터 2개의 ASA 클러스터 멤버 2개가 나와 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부용 Spanned EtherChannel을 사용하여 로컬 스위치에 연결됩니다. ASA EtherChannel은 클러스터의 모든 ASA 전반에 걸쳐 있습니다. 각 데이터 센터의 내부 및 외부 라우터에서는 투명 ASA를 통과하는 OSPF를 사용합니다. MAC과 달리 라우터 IP는 모든 라우터마다 고유합니다. DCI를 통해 비용이 높은 경로를 할당하면 특정 사이트의 모든 ASA 클러스터 멤버가 가동 중지되지 않는 한 각 데이터 센터 내에서 트래픽이 유지됩니다. ASA를 통과하는 비용이 낮은 경로의 경우, 클러스터의 각 사이트에 있는 같은 브릿지 그룹을 거쳐 비대칭 연결을 유지해야 합니다. 어느 한 사이트의 모든 클러스터 멤버에 오류가 발생할 경우, 각 라우터의 트래픽은 DCI를 통해 다른 사이트의 ASA 클러스터 멤버로 이동합니다.



각 사이트의 스위치 구현 과정에는 다음 사항이 포함될 수 있습니다.

- 사이트 간 VSS/vPC — 이 시나리오의 경우 데이터 센터 1에 하나의 스위치를 설치하고, 나머지 하나는 데이터 센터 2에 설치합니다. 각 데이터 센터의 ASA 클러스터 유닛에 사용할 수 있는 한 가지 옵션은 로컬 스위치에만 연결하는 반면, VSS/vPC 트래픽이 DCI를 통해 통과하도록 하는 것입니다. 이 경우 연결의 대부분은 각 데이터 센터에 로컬로 저장됩니다. DCI에서 추가 트래픽을 처리할 수 있는 경우, 선택에 따라 각 ASA 유닛을 DCI 전반의 스위치에 연결할 수 있습니다. 이 경우 트래픽이 데이터 센터 전반에 분산되므로 DCI의 성능이 매우 뛰어나야 합니다.
- 각 사이트의 로컬 VSS/vPC — 스위치 이중화를 개선하기 위해 각 사이트에 별도의 VSS/vPC 쌍을 2개씩 설치할 수 있습니다. 이 경우 ASA의 Spanned EtherChannel은 로컬 스위치에만 연결된 데이터 센터 1 ASA, 그리고 이러한 로컬 스위치에 연결된 데이터 센터 2 ASA로 이루어져 있으나, 근본적으로 Spanned EtherChannel은 "분리"되어 있습니다. 각 로컬 VSS/vPC에서는 Spanned EtherChannel을 사이트-로컬 EtherChannel로 간주합니다.

ASA 클러스터의 연결 관리 방법

클러스터의 여러 멤버에 대한 연결을 로드 밸런싱할 수 있습니다. 연결 역할은 정상적인 작동이 이루어지고 있고 가용성이 높은 상황에서 연결을 처리하는 방법을 결정합니다.

- 9-22 페이지의 연결 역할
- 9-22 페이지의 새 연결 소유권
- 9-23 페이지의 샘플 데이터 흐름
- 9-23 페이지의 클러스터 전반에 걸쳐 새 TCP 연결 재밸런싱

연결 역할

각 연결에는 3가지 종류의 다른 ASA 역할이 정의됩니다.

- 소유자 — 연결을 가장 처음 수신하는 유닛입니다. 소유자 유닛에서는 TCP 상태를 유지하고 패킷을 처리합니다. 연결이 하나인 경우 소유자 유닛도 1개뿐입니다.
- 관리자 — 전달자의 소유자 조회 요청을 처리하고 연결 상태를 유지하여 소유자 유닛에 오류가 발생한 경우 백업 역할을 수행하는 유닛입니다. 소유자가 새 연결을 수신할 경우, 소유자 유닛에서는 소스/목적지 IP 주소와 TCP 포트의 해시를 기준으로 관리자 유닛을 선택하며 관리자 유닛에 메시지를 전송하여 새 연결을 등록합니다. 패킷이 소유자 유닛이 아닌 다른 유닛에 전달될 경우, 해당 유닛에서는 관리자 유닛에 어떤 유닛이 소유자인지 조회하여 패킷이 전달될 수 있도록 합니다. 연결이 하나인 경우 관리자 유닛도 1개뿐입니다.
- 전달자 — 패킷을 소유자 유닛에 전달하는 유닛입니다. 소유하지 않은 연결 패킷이 전달자 유닛에 수신될 경우, 전달자 유닛에서는 소유자 유닛의 관리자를 조회한 다음 이러한 연결을 수신하는 기타 모든 패킷의 소유자에 대한 흐름을 설정합니다. 관리자 유닛은 전달자가 될 수도 있습니다. 전달자 유닛에서 SYN-ACK 패킷을 수신할 경우, 패킷의 SYN 쿠키에서 소유자를 직접 파생할 수 있으므로 관리자 유닛에 조회하지 않아도 됩니다. (TCP 순서 임의 설정을 사용하지 않을 경우, SYN 쿠키가 사용되지 않으며 관리자 유닛에 조회해야 합니다.) DNS 및 ICMP 같은 짧은 흐름의 경우, 조회 대신 전달자 유닛에서 패킷을 관리자 유닛에 직접 전송하며, 관리자 유닛에서는 이 패킷을 소유자 유닛에 보냅니다. 하나의 연결에 여러 개의 전달자 유닛이 있을 수 있습니다. 가장 효율적인 처리량 목표를 실현하려면 전달자가 없고 연결의 모든 패킷이 소유자 유닛에 전송되는 우수한 로드 밸런싱 방법을 사용합니다.

새 연결 소유권

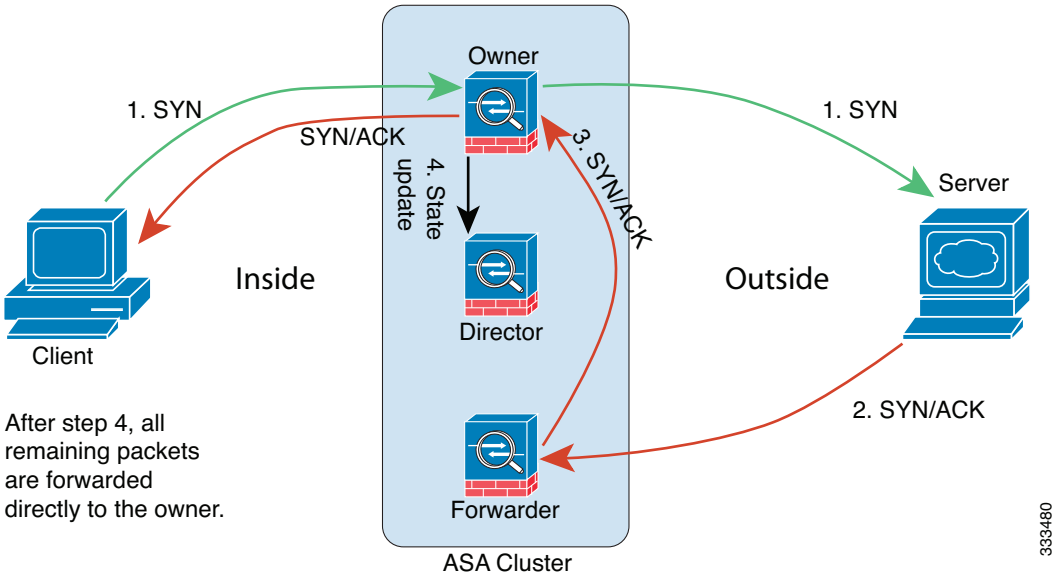
로드 밸런싱을 통해 클러스터의 멤버에 새 연결이 전송될 경우, 해당 유닛에서는 연결의 양방향을 모두 소유합니다. 다른 유닛에 연결 패킷이 전송될 경우, 해당 패킷은 클러스터 제어 링크를 통해 소유자 유닛에 전달됩니다. 최상의 성능을 실현하려면, 같은 유닛에 전송될 수 있도록 흐름의 양방향에 적절한 외부 로드 밸런싱이 필요합니다. 또한 흐름은 유닛 간에 균일하게 분산되어야 합니다. 다른 유닛에 반대 방향의 흐름이 전송될 경우, 이는 원래 유닛으로 다시 리디렉션됩니다.

관련 주제

- 9-12 페이지의 로드 밸런싱 방법

샘플 데이터 흐름

다음 예에는 새 연결을 설정하는 방법이 나와 있습니다.



1. SYN 패킷은 클라이언트에서 시작되고 ASA에 전달(로드 밸런싱 방법을 기준으로)되며, 이 유닛이 소유자 유닛이 됩니다. 소유자 유닛에서는 흐름을 생성하고, 소유자 정보를 SYN 쿠키로 인코딩하며, 패킷을 서버에 전달합니다.
2. SYN-ACK 패킷은 서버에서 시작되고 다른 ASA에 전달(로드 밸런싱 방법을 기준으로)됩니다. 이 ASA는 전달자 유닛입니다.
3. 전달자 유닛에서는 연결을 소유하지 않으므로 SYN 쿠키에서 소유자 정보를 디코딩하고, 소유자에 대한 전달 흐름을 생성하며, SYN-ACK를 소유자 유닛에 전달합니다.
4. 소유자 유닛에서는 관리자 유닛에 상태 업데이트를 보내고, SYN-ACK를 클라이언트에 전달합니다.
5. 관리자 유닛에서는 소유자 유닛을 통해 상태 업데이트를 수신하고, 소유자에 대한 흐름을 생성하며, TCP 상태 정보는 물론 소유자를 기록합니다. 관리자 유닛은 연결의 백업 소유자 역할을 수행합니다.
6. 전달자 유닛에 전달된 모든 후속 패킷은 소유자 유닛에 전달됩니다.
7. 패킷이 추가 유닛에 전달된 경우, 소유자 유닛에 관리자를 쿼리하고 흐름을 설정합니다.
8. 흐름 결과의 상태가 변경되면 소유자 유닛과 관리자 유닛의 상태도 업데이트됩니다.

클러스터 전반에 걸쳐 새 TCP 연결 재밸런싱

업스트림 또는 다운스트림 라우터의 로드 밸런싱 기능을 사용하는 도중 흐름이 균일하게 분산되지 않을 경우, 오버로드된 유닛에서 새 TCP 흐름을 다른 유닛에 리디렉션하도록 구성할 수 있습니다. 기존 흐름은 다른 유닛으로 이동되지 않습니다.

ASA 기능 및 클러스터링

일부 ASA 기능은 ASA 클러스터링이 지원되지 않으며, 일부 기능은 마스터 유닛에서만 지원됩니다. 기타 기능의 경우 올바르게 사용하는 데 필요한 주의 사항이 있을 수 있습니다.

클러스터링으로 지원되지 않는 기능

이러한 기능은 클러스터링을 사용하도록 설정한 경우 구성할 수 없으며 명령이 거부됩니다.

- 통합 커뮤니케이션
- 원격 액세스 VPN(SSL VPN 및 IPsec VPN)
- 다음과 같은 애플리케이션 감시:
  - CTIQBE
  - GTP
  - H323, H225, RAS
  - IPsec 통과
  - MGCP
  - MMP
  - RTSP
  - SIP
  - SCCP(Skinny)
  - WAAS
  - WCCP
- 봇넷 트래픽 필터
- 자동 업데이트 서버
- DHCP 클라이언트, 서버, 릴레이, 프록시
- VPN 로드 밸런싱
- 장애 조치
- ASA CX 모듈

클러스터링을 위한 중앙 집중식 기능

다음 기능은 마스터 유닛에서만 지원되며 클러스터에 확장되지 않습니다. 예를 들어, 8개 유닛으로 구성된 클러스터(SSP-60이 포함된 5585-X)가 있는 경우를 가정해 보겠습니다. 기타 VPN 라이센스에서는 하나의 ASA 5585-X(SSP-60 포함)에 사이트 대 사이트 IPsec 터널을 최대 10,000개까지 허용합니다. 8개 유닛으로 구성된 전체 클러스터에는 터널을 10,000개까지만 사용할 수 있으며 이 기능은 확장되지 않습니다.

참고 중앙 집중식 기능의 트래픽은 클러스터 제어 링크를 통해 멤버 유닛에서 마스터 유닛으로 전달됩니다.

재밸런싱 기능을 사용할 경우, 중앙 집중식 기능의 트래픽은 트래픽이 중앙 집중식 기능으로 분류되기 전에 비 마스터 유닛으로 재밸런싱될 수 있습니다. 이렇게 되면 해당 트래픽은 마스터 유닛으로 다시 전송됩니다.

중앙 집중식 기능의 경우 마스터 유닛에 오류가 발생하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

- 사이트 대 사이트 VPN
- 다음과 같은 애플리케이션 감시:
  - DCERPC
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- 동적 라우팅(Spanned EtherChannel 모드 전용)
- 멀티캐스트 라우팅(개별 인터페이스 모드 전용)
- 고정 경로 모니터링
- IGMP 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 평면 전달은 클러스터 전체에 분산됨)
- PIM 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 평면 전달은 클러스터 전체에 분산됨)
- 네트워크 액세스에 대한 인증 및 권한 부여. 어카운팅이 분산됨
- 필터링 서비스

관련 주제

- 9-7 페이지의 클러스터 제어 링크 크기 조정
- 9-23 페이지의 클러스터 전반에 걸쳐 새 TCP 연결 재밸런싱

개별 유닛에 적용되는 기능

이러한 기능은 전체 클러스터 또는 마스터 유닛이 아닌 각ASA 유닛에 적용됩니다.

- QoS — QoS 정책은 컨피그레이션 복제의 일부로 클러스터 전체와 동기화됩니다. 그러나 정책은 각 유닛에서 독립적으로 시행됩니다. 예를 들어, 출력에 대한 정책 시행을 구성할 경우 특정 ASA에 있는 트래픽에서 적응 속도 및 적응 버스트 값이 시행됩니다. 8개 유닛으로 구성되고 트래픽이 균일하게 분산된 클러스터의 경우, 적응 속도는 클러스터 *속도*의 8배가 됩니다.
- 위협 감지 — 위협 감지는 각 유닛에 개별적으로 작동됩니다. 예를 들어, 상위 통계는 유닛별로 적용됩니다. 이를테면 포트 검사 감지 기능의 경우, 검사 트래픽이 모든 유닛 간에 로드 밸런싱되고 한 유닛에 모든 트래픽이 표시되지 않으므로 이 기능은 작동하지 않습니다.
- 리소스 관리 — 다중 컨텍스트 모드에서 리소스 관리는 로컬 사용량을 기준으로 각 유닛에 개별적으로 시행됩니다.
- ASA FirePOWER 모듈 — ASA FirePOWER 모듈 간에는 컨피그레이션 동기화 또는 상태 공유 기능이 없습니다. 클러스터의 ASA FirePOWER 모듈에 일관된 정책을 유지하려면 FireSIGHT Management Center를 사용해야 합니다. 클러스터의 디바이스에 다른 ASA 인터페이스 기반 영역 정의를 사용하지 마십시오.
- ASA IPS 모듈 — IPS 모듈 간에는 컨피그레이션 동기화 또는 상태 공유 기능이 없습니다. 일부 IPS 서명의 경우 여러 연결 전반의 상태를 유지하기 위한 IPS가 필요합니다. 예를 들어, 누군가 다른 포트로 하나의 서버에 여러 개의 연결을 열고 있는 것이 IPS 모듈에 감지된 경우 포트 검사 서명이 사용됩니다. 클러스터링의 이러한 연결은 여러 ASA 디바이스 간에 균형 조정이 이루어지며, 각각에는 고유한 IPS 모듈이 있습니다. 이러한 IPS 모듈에서는 상태 정보를 공유하지 않으므로, 클러스터에서 포트 검사를 결과로 감지하지 못할 수 있습니다.

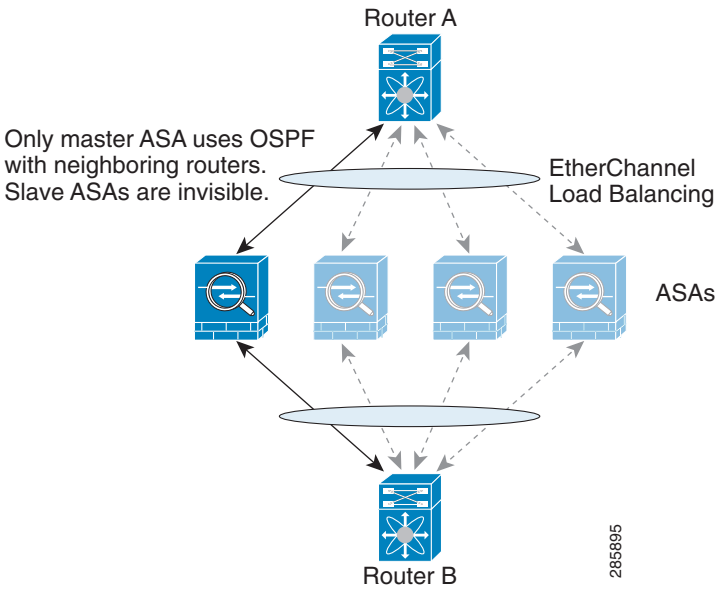
동적 라우팅 및 클러스터링

- 9-26 페이지의 Spanned EtherChannel 모드의 동적 라우팅
- 9-27 페이지의 개별 인터페이스 모드의 동적 라우팅

Spanned EtherChannel 모드의 동적 라우팅

Spanned EtherChannel 모드의 경우 라우팅 프로세스는 마스터 유닛에서만 실행되며, 마스터 유닛을 통해 경로가 파악되고 슬레이브에 복제됩니다. 라우팅 패킷이 슬레이브에 전송되면 해당 패킷은 마스터 유닛에 리디렉션됩니다.

그림 9-1 Spanned EtherChannel 모드의 동적 라우팅



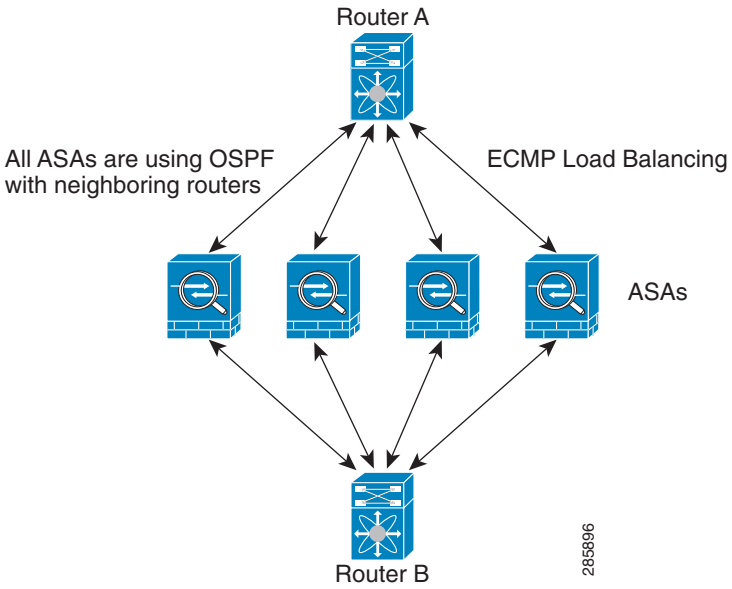
슬레이브 멤버가 마스터 유닛에서 경로를 파악하면 각 유닛에서는 전달과 관련한 결정을 개별적으로 수행합니다.

OSPF LSA 데이터베이스는 마스터 유닛에서 슬레이브 유닛으로 동기화되지 않습니다. 마스터 유닛 전환이 있을 경우, 인접한 라우터에서 재시작을 감지하며 전환 작업은 투명하게 이루어지지 않습니다. OSPF 프로세스에서 IP 주소를 해당 라우터 ID로 선택합니다. 필수는 아니지만 고정 라우터 ID를 할당하면 클러스터 전반에 걸쳐 일관된 라우터 ID를 사용하도록 할 수 있습니다.

개별 인터페이스 모드의 동적 라우팅

개별 인터페이스 모드의 경우 각 유닛에서는 라우팅 프로토콜을 독립형 라우터로 실행하며, 경로에 대한 정보 파악은 각 유닛에서 개별적으로 수행합니다.

그림 9-2 개별 인터페이스 모드의 동적 라우팅



위 다이어그램에서 라우터 A는 라우터 B에 각각 ASA를 통한 4개의 Equal-Cost 경로가 있다는 정보를 파악합니다. ECMP는 4개 경로 간의 트래픽을 로드 밸런싱하는 데 사용됩니다. 각각의 ASA는 외부 라우터와 통신할 경우 다른 라우터 ID를 선택합니다.

라우터 ID에 대한 클러스터 풀을 구성하여 유닛마다 개별 라우터 ID를 보유하도록 해야 합니다.

멀티캐스트 라우팅 및 클러스터링

멀티캐스트 라우팅은 인터페이스 모드에 따라 다르게 작동합니다.

- 9-28 페이지의 Spanned EtherChannel 모드의 멀티캐스트 라우팅
- 9-28 페이지의 개별 인터페이스 모드의 멀티캐스트 라우팅

Spanned EtherChannel 모드의 멀티캐스트 라우팅

Spanned EtherChannel 모드에서 마스터 유닛은 빠른 경로(fast-path) 전달이 설정될 때까지 모든 멀티캐스트 라우팅 패킷과 데이터 패킷을 처리합니다. 연결이 설정되면 각 슬레이브에서 멀티캐스트 데이터 패킷을 전달할 수 있습니다.

개별 인터페이스 모드의 멀티캐스트 라우팅

개별 인터페이스 모드에서 유닛은 멀티캐스트와 별개로 작동하지 않습니다. 모든 데이터 및 라우팅 패킷은 마스터 유닛을 통해 처리되고 전달되므로, 패킷 복제가 방지됩니다.

NAT 및 클러스터링

NAT는 클러스터의 전체 처리량에 영향을 미칠 수 있습니다. 로드 밸런싱 알고리즘은 IP 주소와 포트를 기반으로 할 뿐만 아니라 NAT로 인해 인바운드 및 아웃바운드 패킷의 IP 주소 및/또는 포트가 서로 달라질 수 있으므로, 인바운드 및 아웃바운드 NAT 패킷을 클러스터의 다른 ASA에 전송할 수 있습니다. 패킷이 연결 소유자가 아닌 ASA에 전달되면 해당 패킷은 클러스터 제어 링크를 통해 소유자에게 전달되며 이때 클러스터 제어 링크에 매우 많은 양의 트래픽이 발생합니다.

클러스터링에 NAT를 계속 사용하려면 다음 지침을 숙지하십시오.

- 프록시 ARP 없음 — 개별 인터페이스에서 프록시 ARP 응답은 매핑된 주소에 전송되지 않습니다. 이렇게 되면 인접한 라우터가 클러스터에 더 이상 존재하지 않는 ASA와 피어 관계를 유지하지 못하게 됩니다. 업스트림 라우터에는 기본 클러스터 IP 주소를 나타내는 매핑된 주소에 대한 고정 경로 또는 PBR(Object Tracking 포함)이 필요합니다. Spanned EtherChannel의 경우에는 하나의 IP 주소만 클러스터 인터페이스에 연결되므로 이것이 문제가 되지 않습니다.
- 개별 인터페이스에 인터페이스 PAT 없음 — 개별 인터페이스에는 인터페이스 PAT가 지원되지 않습니다.
- 동적 PAT에 NAT 풀 주소 분산 — 마스터 유닛은 클러스터 전체에 걸쳐 주소를 사전에 균일하게 분산시킵니다. 멤버에 주소가 없는 연결이 전달된 경우 해당 연결이 끊어지며, 다른 멤버는 유효한 주소를 보유한 경우에도 마찬가지입니다. 각 유닛에 주소가 전달되도록 하려면 NAT 주소는 최소한 클러스터의 유닛에 있는 수만큼 추가해야 합니다. 주소 할당을 보려면 **show nat pool cluster** 명령을 사용합니다.
- 라운드 로빈 없음 — 클러스터링에서는 PAT 풀을 위한 라운드 로빈을 지원하지 않습니다.
- 마스터 유닛에 의해 관리되는 동적 NAT xlate — 마스터 유닛에서는 xlate 테이블을 유지하고 이를 슬레이브 유닛에 복제합니다. 동적 NAT가 필요한 연결이 슬레이브 유닛에 전달되고 xlate가 테이블에 없을 경우, 슬레이브 유닛에서는 마스터 유닛에서 xlate를 요청합니다. 슬레이브 유닛에서는 이 연결을 소유합니다.
- 세션당 PAT 기능 — 클러스터링에만 해당되는 것은 아니지만, 세션당 PAT 기능을 사용하면 PAT의 확장성이 개선되며 클러스터링을 수행할 때 각 슬레이브 유닛에서 고유한 PAT 연결을 소유할 수 있게 됩니다. 이와 달리 다중 세션 PAT 연결은 마스터 유닛에 전달해야 하며 마스터 유닛에서 해당 연결을 소유하게 됩니다. 기본적으로 모든 TCP 트래픽 및 UDP DNS 트래픽에서는 세션당 PAT xlate를 사용합니다. 다중 세션 PAT가 필요한 트래픽(예: H.323, SIP 또는 Skinny)의 경우 세션당 PAT를 사용하지 않도록 설정할 수 있습니다. 세션당 PAT에 대한 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.
- 다음을 검사할 수 있는 고정 PAT 없음
  - FTP
  - PPTP
  - RSH
  - SQLNet
  - TFTP
  - XDMCP
  - 모든 VoIP(voice-over-IP) 제품

네트워크 액세스 및 클러스터링용 AAA

네트워크 액세스용 AAA는 인증, 권한 부여, 어카운팅이라는 세 가지 구성 요소로 이루어져 있습니다. 인증 및 어카운팅은 클러스터 슬레이브에 대한 데이터 구조의 복제를 통해 클러스터링 마스터에서 중앙 집중식 기능으로 구현됩니다. 마스터 유닛이 선택된 경우, 새 마스터에서는 설정된 인증 완료 사용자 및 관련 인증 작업을 중단 없이 계속 가동하는 데 필요한 모든 정보를 보유하게 됩니다. 사용자 인증의 유휴 및 절대 시간 제한은 마스터 유닛이 변경될 경우 유지됩니다.

어카운팅은 클러스터에서 분산된 기능으로 구현됩니다. 어카운팅은 흐름 하나의 단위로 수행되므로, 흐름에 대한 어카운팅이 구성되면 흐름을 소유한 클러스터에서는 어카운팅 시작 및 중지 메시지를 AAA 서버에 보냅니다.

Syslog와 NetFlow 및 클러스터링

- Syslog — 클러스터의 각 유닛에서는 고유한 syslog 메시지를 생성합니다. 각 유닛에서 syslog 메시지 헤더 필드에 동일하거나 다른 디바이스 ID를 사용하도록 로깅을 구성할 수 있습니다. 예를 들어, 호스트 이름 컨피그레이션은 클러스터의 모든 유닛에 의해 복제 및 공유됩니다. 호스트 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, 모든 유닛에서는 단일한 유닛에서 생성된 것처럼 보이는 syslog 메시지를 생성합니다. 클러스터 부트스트랩 컨피그레이션에 할당된 로컬-유닛 이름을 디바이스 ID로 사용하도록 로깅을 컨피그레이션할 경우, syslog 메시지는 다른 유닛에서 생성된 것처럼 보입니다.
- NetFlow — 클러스터의 각 유닛에는 고유한 NetFlow 스트림이 있습니다. NetFlow 컬렉터에서는 각각의 ASA를 별도의 NetFlow 내보내기 장치로만 처리할 수 있습니다.

관련 주제

- 40-20 페이지의 디바이스 ID를 Non-EMBLEM 형식 Syslog 메시지에 포함

SNMP 및 클러스터링

SNMP 에이전트에서는 로컬 IP 주소로 각각의 개별 ASA를 폴링합니다. 클러스터의 통합 데이터는 폴링할 수 없습니다.

SNMP 폴링에는 기본 클러스터 IP 주소가 아닌 로컬 주소를 항상 사용해야 합니다. SNMP 에이전트에서 기본 클러스터 IP 주소를 폴링하면서 새 마스터가 선택된 경우, 새 마스터 유닛에 대한 폴링이 이루어지지 않습니다.

VPN 및 클러스터링

사이트 대 사이트 VPN은 중앙 집중식 기능이며, 마스터 유닛에서만 VPN 연결을 지원합니다.

참고 원격 액세스 VPN은 클러스터링으로 지원되지 않습니다.

VPN 기능은 마스터 유닛에만 제한되며 클러스터 고가용성 기능을 사용하지 않습니다. 마스터 유닛에 오류가 발생할 경우, 모든 기존 VPN 연결이 손실되며 VPN 사용자에게는 서비스 중단 메시지가 표시됩니다. 새 마스터가 선택되면 VPN 연결을 다시 설정해야 합니다.

VPN 터널을 Spanned EtherChannel 주소에 연결할 경우 연결이 마스터 유닛에 자동으로 전달됩니다. PBR 또는 ECMP를 사용할 경우 개별 인터페이스에 연결하려면 항상 로컬 주소가 아닌 기본 클러스터 IP 주소에 연결해야 합니다.

VPN 관련 키 및 인증서는 모든 유닛에 복제됩니다.

FTP 및 클러스터링

- 다른 클러스터 멤버가 FTP 데이터 채널 및 제어 채널의 흐름을 소유한 경우, 데이터 채널 소유자 유닛에서는 유휴 시간 제한 업데이트를 제어 채널 소유자에게 주기적으로 전송하고 유휴 시간 제한 값을 업데이트합니다. 그러나 제어 흐름 소유자가 다시 로드되고 제어 흐름이 다시 호스팅된 경우, 부모/자식 흐름 관계가 더 이상 유지되지 않으며 제어 흐름 유휴 시간 제한도 업데이트되지 않습니다.
- FTP 액세스용 AAA를 사용할 경우 마스터 유닛에서는 제어 채널 흐름을 중앙 집중화합니다.

Cisco TrustSec 및 클러스터링

마스터 유닛에서만 SGT(보안 그룹 태그) 정보를 파악합니다. 그런 다음 마스터 유닛에서는 SGT를 슬레이브에 제공하며, 슬레이브에서는 보안 정책을 기준으로 SGT의 일치 여부를 결정할 수 있습니다.

ASA 클러스터링 라이센스

모델	라이센싱 요구 사항
ASA 5585-X	클러스터 라이센스, 최대 16개까지 지원. 클러스터 라이센스는 각 유닛에 필요합니다. 기타 기능 라이센스의 경우, 클러스터 유닛에서는 각 유닛에 동일한 라이센스를 필요로 하지 않습니다. 여러 유닛에 기능 라이센스를 보유한 경우, 해당 라이센스는 단일하게 실행되는 ASA 클러스터 라이센스로 통합됩니다. **참고** 각 유닛에는 동일한 암호화 라이센스 및 동일한 10 GE I/O 라이센스가 있어야 합니다.
ASA 5512-X	Security Plus 라이센스, 유닛 2개 지원. **참고** 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다.
ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	Base 라이센스, 유닛 2개 지원. **참고** 각 유닛에는 동일한 암호화 라이센스가 있어야 합니다.
기타 모델	지원 안 함

ASA 클러스터링의 사전 요구 사항

ASA 하드웨어 및 소프트웨어 요구 사항

클러스터의 모든 유닛은 다음과 같아야 합니다.

- 동일한 DRAM과 같은 모델이어야 합니다. 플래시 메모리는 동일하지 않아도 됩니다.
- 이미지 업그레이드 시 동일한 소프트웨어 예외를 실행해야 합니다. 무중단 업그레이드가 지원됩니다.
- 개별 인터페이스 모드를 사용할 경우 지리적으로 다른 위치(사이트 간)에 있는 클러스터 멤버를 보유할 수 있습니다.
- 동일한 보안 컨텍스트 모드(단일 또는 다중)에 있어야 합니다.
- (단일 컨텍스트 모드) 동일한 방화벽 모드(라우팅 또는 투명 모드)여야 합니다.
- 새 클러스터 컨피그레이션원은 컨피그레이션을 복제하기 전에 맨 처음 클러스터 제어 링크 통신을 수행할 경우 동일한 SSL 암호화 설정(**ssl 암호화** 명령)을 마스터 유닛으로 사용해야 합니다.
- ASA 5585-X, 10 GE I/O 라이센스의 클러스터, 암호화는 동일해야 합니다.

스위치 사전 요구 사항

- ASA에서 클러스터링을 컨피그레이션하기 전에 스위치 컨피그레이션을 완료해야 합니다.
- 다음 표에는 ASA 클러스터링과의 상호 운용을 지원하는 외부 하드웨어 및 소프트웨어 목록이 나와 있습니다.

표 9-2 ASA 클러스터링을 위한 외부 하드웨어 및 소프트웨어 지원

외부 하드웨어	외부 소프트웨어	ASA 버전
Cisco Nexus 9300	Cisco NX-OS 6.1(2)I2(1) 이상	9.2(1) 이상
Cisco Nexus 7000	Cisco NX-OS 5.2(5) 이상	9.0(1) 이상
Cisco Nexus 5000	Cisco NX-OS 7.0(1) 이상	9.1(4) 이상
Catalyst 6500(Supervisor 32, 720, 720-10GE 포함)	Cisco IOS 12.2(33)SXI7, SXI8, SXI9 이상	9.0(1) 이상
Catalyst 3750-X	Cisco IOS 15.0(2) 이상	9.1(4) 이상

ASA 사전 요구 사항

- 각 유닛이 관리 네트워크에 참가하기 전에 각 유닛에 고유한 IP 주소를 제공해야 합니다.
  - ASA 에 연결하고 관리 IP 주소를 설정하는 방법에 대한 자세한 내용은 시작 장을 참조하십시오.
  - 마스터 유닛(일반적으로 클러스터에 추가하는 첫 번째 유닛)에서 사용하는 IP 주소를 제외하고, 이러한 관리 IP 주소는 일시적으로만 사용됩니다.
  - 슬레이브가 클러스터에 참가하면 관리 인터페이스 컨피그레이션이 마스터 유닛에서 복제된 컨피그레이션으로 교체됩니다.
- 클러스터 제어 링크에 점보 프레임을 사용하려면(권장), 클러스터링을 사용하기 전에 점보 프레임 예약(Jumbo Frame Reservation)을 사용하도록 설정해야 합니다.

기타 사전 요구 사항

모든 클러스터 멤버 유닛 콘솔 포트에 액세스하려면 터미널 서버를 사용하는 것이 좋습니다. 초기 설치 및 지속적인 관리(예: 유닛이 중지될 경우)를 위해서는 터미널 서버를 사용하는 것이 원격 관리에 유용합니다.

관련 주제

- 9-32 페이지의 ASA 클러스터링 지침
- 10-28 페이지의 점보 프레임 지원 활성화
- 9-3 페이지의 부트스트랩 구성

ASA 클러스터링 지침

컨텍스트 모드

모드는 각 멤버 유닛과 일치해야 합니다.

방화벽 모드

단일 모드의 경우 방화벽 모드는 모든 유닛과 일치해야 합니다.

장애 조치

클러스터링에서는 장애 조치가 지원되지 않습니다.

IPv6

클러스터 제어 링크는 IPv4를 사용하는 경우에만 지원됩니다.

모델

지원되는 모델:

- ASA 5585-X

  10기가비트 이더넷 인터페이스 2개가 내장된 SSP-10 및 SSP-20이 포함된 ASA 5585-X의 경우, 클러스터 제어 링크에는 하나의 인스턴스를 사용하고 데이터에는 나머지를 사용하는 것이 좋습니다. 이러한 설치 과정에서는 클러스터 제어 링크의 이중화를 수용하지 않으나, 클러스터 제어 링크의 크기를 데이터 인터페이스의 크기와 일치시켜야 하는 요구 사항은 충족합니다.

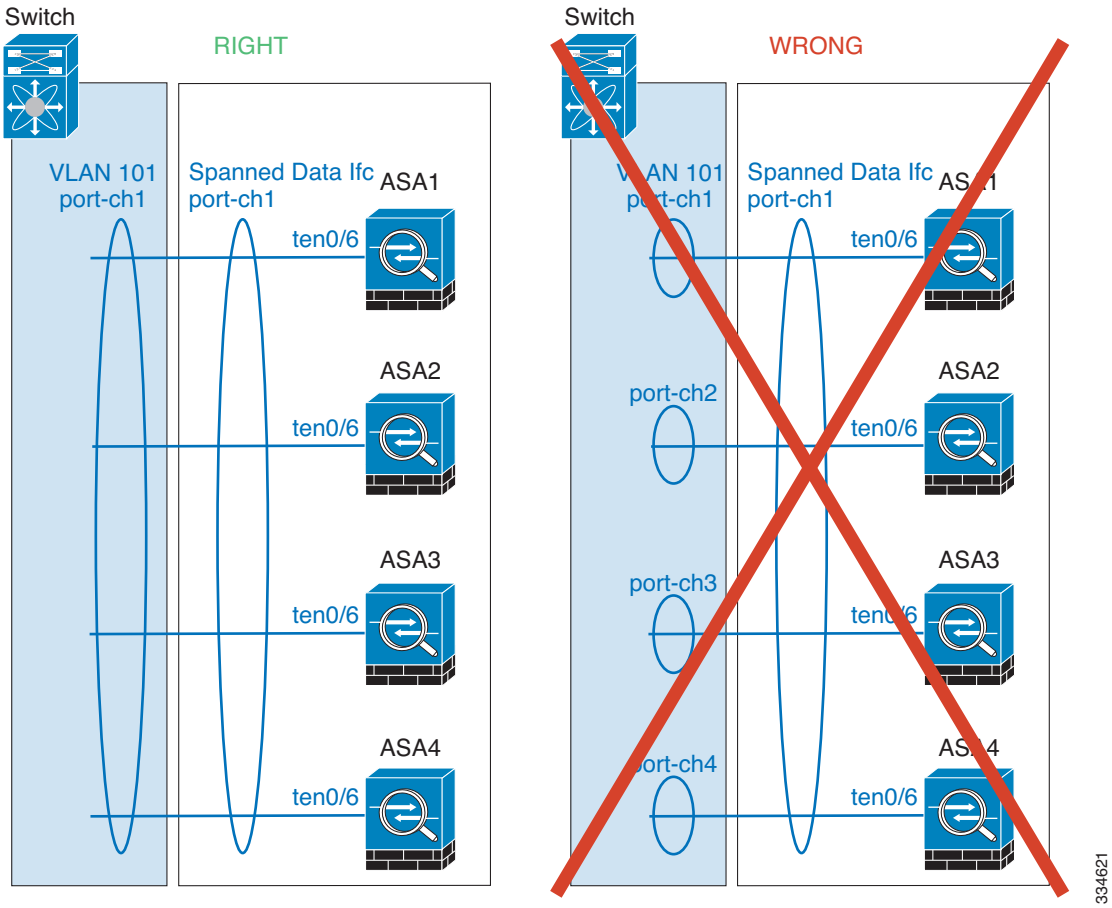
- ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X

스위치

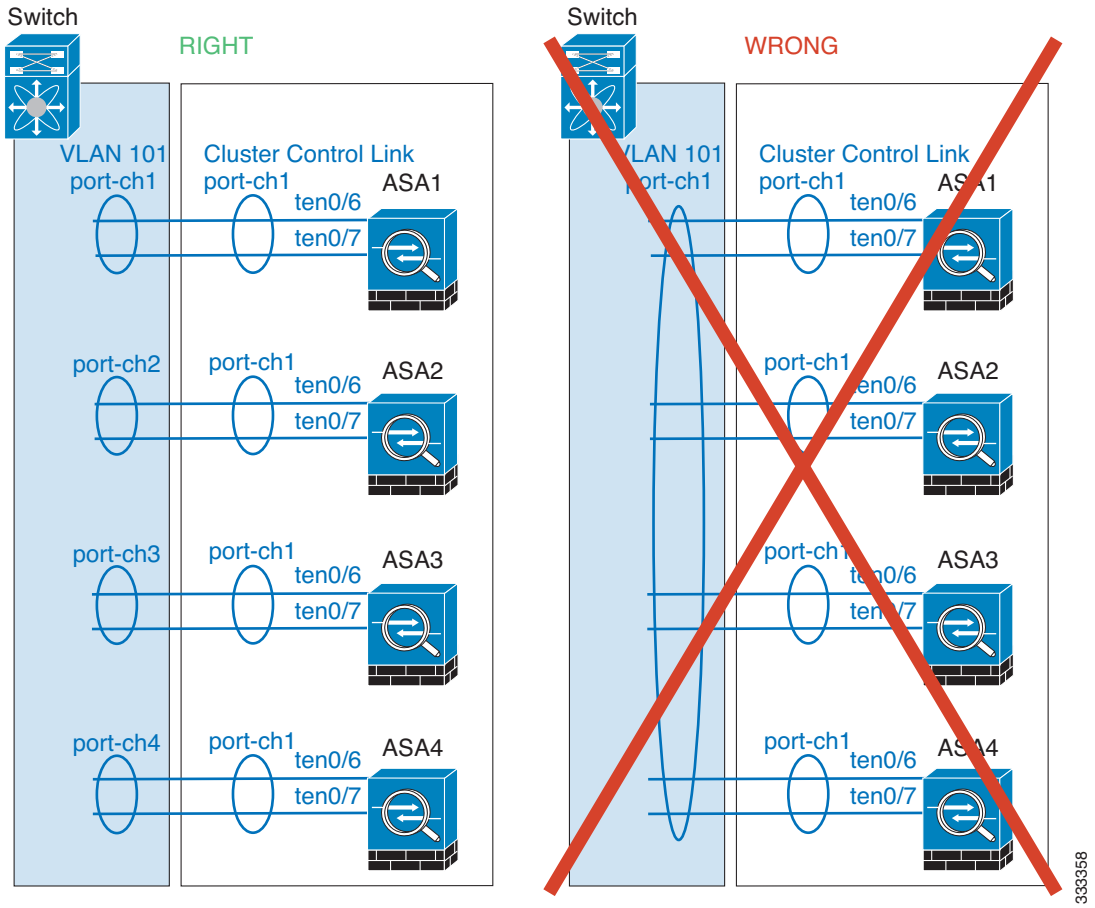
- 클러스터 제어 링크 인터페이스용 스위치의 경우, ASA에 연결된 스위치 포트에서 Spanning Tree PortFast를 사용하도록 선택하여 새 유닛에 대한 참가 프로세스 속도를 높일 수 있습니다.
- 스위치에서 Spanned EtherChannel의 번들링 속도가 저하될 경우, 스위치의 개별 인터페이스에 대한 LACP 속도를 빠르게 설정할 수 있습니다.
- 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** EtherChannel 로드 밸런싱 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 및 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 ASA에 트래픽이 균일하지 않게 분산될 수 있기 때문입니다. ASA에서 로드 밸런싱 알고리즘의 기본값을 변경하지 *마십시오*.
- 스위치에서 EtherChannel의 로드 밸런싱 알고리즘을 변경할 경우, 스위치의 EtherChannel 인터페이스에서 트래픽 전달이 일시적으로 중단되며 Spanning Tree Protocol이 재시작됩니다. 트래픽에서 흐름을 다시 시작하기 전까지 지연이 발생하게 됩니다.
- Cisco Nexus 스위치의 경우 모든 클러스터용 EtherChannel 인터페이스에서 LACP Graceful Convergence 기능을 사용하지 않도록 설정해야 합니다.
- 일부 스위치에서는 LACP를 통한 동적 포트 우선순위를 지원하지 않습니다(활성 및 스탠바이 링크). 동적 포트 우선순위를 사용하지 않도록 설정하여 Spanned EtherChannel과의 호환성을 향상할 수 있습니다.
- 클러스터 제어 링크 경로의 네트워크 요소에서는 L4 체크섬을 확인하지 않습니다. 클러스터 제어 링크를 통해 리디렉션된 트래픽에는 올바른 L4 체크섬이 없습니다. L4 체크섬을 확인하는 스위치의 경우 트래픽이 감소하는 결과를 초래할 수 있습니다.
- 포트 채널 번들링 다운타임은 구성된 keepalive 기간을 초과하면 안 됩니다.

EtherChannel

- ASA에서는 EtherChannel을 스위치 스택에 연결하도록 지원하지 않습니다. ASA EtherChannel이 교차 스택에 연결되어 있는 상태에서 마스터 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다.
- Spanned 및 디바이스-로컬 EtherChannel 구성 비교 — Spanned EtherChannel와 디바이스-로컬 EtherChannel에 대한 스위치를 올바르게 구성해야 합니다.
  - Spanned EtherChannel — 클러스터의 모든 멤버 전체를 포괄하는 ASA *Spanned* EtherChannel의 경우, 인터페이스가 스위치의 단일한 EtherChannel로 통합됩니다. 각 인터페이스가 스위치의 동일한 채널 그룹에 있는지 확인하십시오.



– 디바이스-로컬 EtherChannel — 클러스터 제어 링크에 대해 구성된 모든 EtherChannel을 비롯한 ASA *디바이스-로컬* EtherChannel*의* 경우 스위치에서 별도의 EtherChannel을 구성해야 합니다. 여러 ASA EtherChannel을 스위치에서 하나의 EtherChannel에 통합하지 마십시오.



추가 지침

- 중요한 토폴로지 변경 사항이 발생할 경우(예: EtherChannel 인터페이스 추가 또는 제거, ASA 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 생성) 상태 검사 기능을 비활성화해야 합니다. 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사 기능을 다시 사용할 수 있습니다.
- 기존 클러스터에 유닛을 추가하거나 유닛을 다시 로드할 경우, 일시적이고 제한적으로 패킷/연결이 감소하며 이는 정상적인 동작입니다. 경우에 따라 감소된 패킷으로 인해 연결이 끊어질 수 있습니다. 예를 들어, FTP 연결의 FIN/ACK 패킷이 감소할 경우 FTP 클라이언트가 끊어집니다. 이 경우 FTP 연결을 다시 설정해야 합니다.
- Spanned EtherChannel에 연결된 Windows 2003 Server를 사용할 경우 syslog 서버 포트가 중지되면 서버에서 ICMP 오류 메시지를 제한하지 않으며, 이렇게 되면 대량의 ICMP 메시지가 ASA 클러스터에 다시 전송됩니다. 이러한 메시지로 인해 ASA 클러스터의 일부 유닛에서 CPU 점유율이 높아져 성능에 영향을 미칠 수 있습니다. 이러한 문제를 방지하려면 ICMP 오류 메시지를 제한하는 것이 좋습니다.

관련 주제

- 9-7 페이지의 클러스터 제어 링크 크기 조정
- 9-3 페이지의 부트스트랩 구성
- 9-24 페이지의 클러스터링으로 지원되지 않는 기능
- 10-20 페이지의 EtherChannel 구성
- 10-11 페이지의 EtherChannel 지침

ASA 클러스터의 기본값

- Spanned EtherChannel을 사용할 경우, cLACP 시스템 ID가 자동 생성되며 시스템 우선순위는 기본적으로 1입니다.
- 클러스터 상태 검사 기능은 기본적으로 활성화되어 있으며 3초간의 대기 시간이 있습니다.
- 연결 재밸런싱은 기본적으로 비활성화되어 있습니다. 연결 재밸런싱을 활성화할 경우 로드 정보를 교환하는 데 걸리는 기본 시간은 5초입니다.

ASA 클러스터링 구성

참고 클러스터링을 활성화하거나 비활성화하려면 콘솔 연결(CLI용) 또는 ASDM 연결을 사용해야 합니다.

클러스터링을 구성하려면 다음 작업을 수행합니다.

1단계 9-31 페이지의 ASA 클러스터링의 사전 요구 사항 및 9-32 페이지의 ASA 클러스터링 지침에 따라 스위치와 ASA에 대한 사전 컨피그레이션을 모두 완료합니다.

2단계 9-36 페이지의 클러스터 유닛 케이블 연결 및 업스트림/다운스트림 장비 구성.

3단계 9-38 페이지의 구성 백업(권장).

4단계 9-39 페이지의 각 유닛의 마스터 유닛에서 클러스터 인터페이스 모드. 클러스터링의 인터페이스 유형은 Spanned EtherChannel 또는 개별 인터페이스 중 한 가지로만 구성할 수 있습니다.

5단계 9-41 페이지의 (권장, 다중 컨텍스트 모드에서 필요) 마스터 유닛의 인터페이스 구성. 인터페이스가 클러스터링을 수행할 준비가 되어 있지 않은 경우 클러스터링을 사용할 수 없습니다. 단일 컨텍스트 모드의 경우, High Availability and Scalability 마법사에서 여러 가지 인터페이스 설정을 구성할 수 있으나 마법사에서는 일부 인터페이스 옵션이 제공되지 않으며, 다중 컨텍스트 모드에서 인터페이스를 구성할 수 없습니다.

6단계 9-47 페이지의 ASA 클러스터 생성 또는 참가.

7단계 마스터 유닛에 대한 보안 정책을 구성합니다. 마스터 유닛에서 지원되는 기능을 구성하려면 이 가이드의 해당 장을 참조하십시오. 컨피그레이션은 슬레이브 유닛에 복제됩니다.

클러스터 유닛 케이블 연결 및 업스트림/다운스트림 장비 구성

클러스터링을 구성하기 전에 클러스터 제어 링크 네트워크, 관리 네트워크, 데이터 네트워크의 케이블을 연결합니다.

참고 클러스터에 참가할 유닛을 구성하기 전에 최소한 활성 클러스터 제어 링크 네트워크가 있어야 합니다.

또한 업스트림 및 다운스트림 장비도 구성해야 합니다. 예를 들어, EtherChannel을 사용할 경우 EtherChannel에 대한 업스트림 및 다운스트림 장비를 구성해야 합니다.

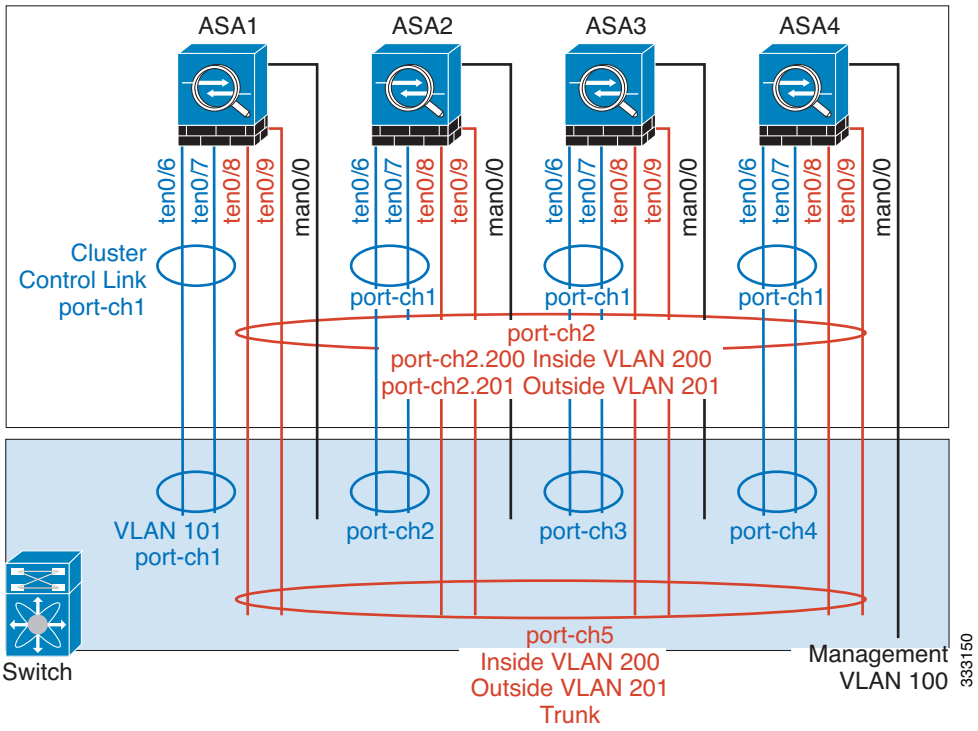
예

참고 이 예에서는 로드 밸런싱에 EtherChannel을 사용합니다. PBR 또는 ECMP를 사용할 경우 스위치 컨피그레이션이 달라집니다.

각각 4개의 ASA 5585-X에서 다음과 같은 기능을 사용하는 것으로 가정해 보겠습니다.

- 클러스터 제어 링크에 대한 디바이스-로컬 EtherChannel에서 10기가비트 이더넷 인터페이스 2개
- 내부 및 외부 네트워크에 대한 Spanned EtherChannel에서 10기가비트 이더넷 인터페이스 2개. 각 인터페이스는 EtherChannel의 VLAN 하위 인터페이스입니다. 하위 인터페이스를 사용하면 내부 및 외부 인터페이스에서 모두 EtherChannel의 이점을 활용할 수 있습니다.
- 관리 인터페이스 1개

내부 및 외부 네트워크의 스위치는 1개입니다.



목적	각 4개의 ASA에 인터페이스 연결	포트 전환
클러스터 제어 링크	TenGigabitEthernet 0/6 및 TenGigabitEthernet 0/7	총 8개 포트 각각의 TenGigabitEthernet 0/6 및 TenGigabitEthernet 0/7 쌍은 EtherChannel 4개를 구성합니다(각 ASA당 EC 1개). 이러한 EtherChannel은 모두 동일한 별도의 클러스터 제어 VLAN에 있어야 합니다(예: VLAN 101).
내부 및 외부 인터페이스	TenGigabitEthernet 0/8 및 TenGigabitEthernet 0/9	총 8개 포트 단일 EtherChannel을 구성합니다(모든ASA 전반에 걸쳐). 스위치에서 이러한 VLAN 및 네트워크를 구성합니다(예: 내부용 VLAN 200 및 외부용 VLAN 201을 포함하는 트렁크).
관리 인터페이스	Management 0/0	총 4개 포트 동일한 별도의 관리 VLAN에 모든 인터페이스를 배치합니다(예: VLAN 100).

구성 백업(권장)

슬레이브 유닛에서 클러스터링을 활성화하면 현재 컨피그레이션이 마스터 유닛에서 동기화된 컨피그레이션으로 교체됩니다. 클러스터를 완전히 벗어날 경우, 사용 가능한 관리 인터페이스 컨피그레이션으로 백업 컨피그레이션을 만드는 편이 유용합니다.

시작하기 전에

각 유닛에서 백업을 수행합니다.

절차

1단계 **Tools > Backup Configurations**를 선택합니다.

2단계 최소한 현재 실행 중인 컨피그레이션을 백업합니다. 자세한 절차는 37-24 페이지의 로컬 CA 서버 백업을 참조하십시오.

관련 주제

- 9-57 페이지의 클러스터 벗어나기

각 유닛의 마스터 유닛에서 클러스터 인터페이스 모드

클러스터링의 인터페이스 유형은 Spanned EtherChannel 또는 개별 인터페이스 중 한 가지로만 구성할 수 있으며, 클러스터에서 여러 인터페이스 유형을 함께 사용할 수 없습니다.

참고 마스터 유닛을 통해 슬레이브 유닛을 추가하지 않을 경우, 이 섹션의 설명에 따라 마스터 유닛뿐만 아니라 모든 유닛에 인터페이스 모드를 수동으로 설정해야 합니다. 반면 마스터 유닛을 통해 슬레이브를 추가할 경우, ASDM에서 슬레이브에 인터페이스 모드를 자동으로 설정합니다.

시작하기 전에

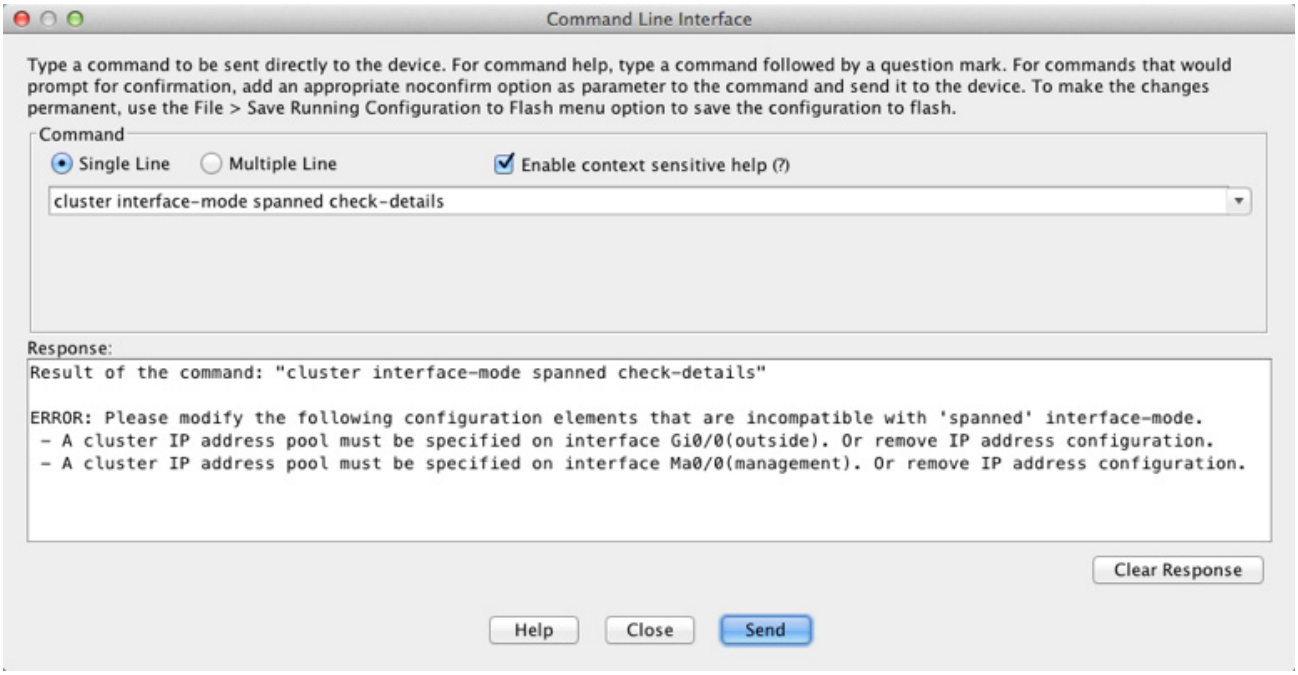
- 관리 전용 인터페이스는 항상 개별 인터페이스로 구성할 수 있으며(권장), Spanned EtherChannel 모드에서도 마찬가지입니다. 투명 방화벽 모드에서도 관리 인터페이스는 개별 인터페이스가 될 수 있습니다.
- Spanned EtherChannel 모드에서 관리 인터페이스를 개별 인터페이스로 구성할 경우, 관리 인터페이스에 동적 라우팅을 사용할 수 없습니다. 고정 라우팅을 사용해야 합니다.
- 다중 컨텍스트 모드에서는 모든 컨텍스트에 한 가지 인터페이스 유형을 선택해야 합니다. 예를 들어, 투명 및 라우팅 모드 컨텍스트를 함께 선택한 경우 투명 모드에는 한 가지 인터페이스 유형만 허용되므로 모든 컨텍스트에 Spanned EtherChannel 모드를 사용해야 합니다.

절차

1단계 마스터 유닛의 ASDM에서 **Tools > Command Line Interface**를 선택합니다. 호환되지 않는 모든 컨피그레이션을 표시하여 인터페이스 모드를 강제로 시행하여 나중에 컨피그레이션을 수정할 수 있습니다. 다음 명령을 사용할 경우 모드는 변경되지 않습니다.

```
cluster interface-mode {individual | spanned} check-details
```

예:

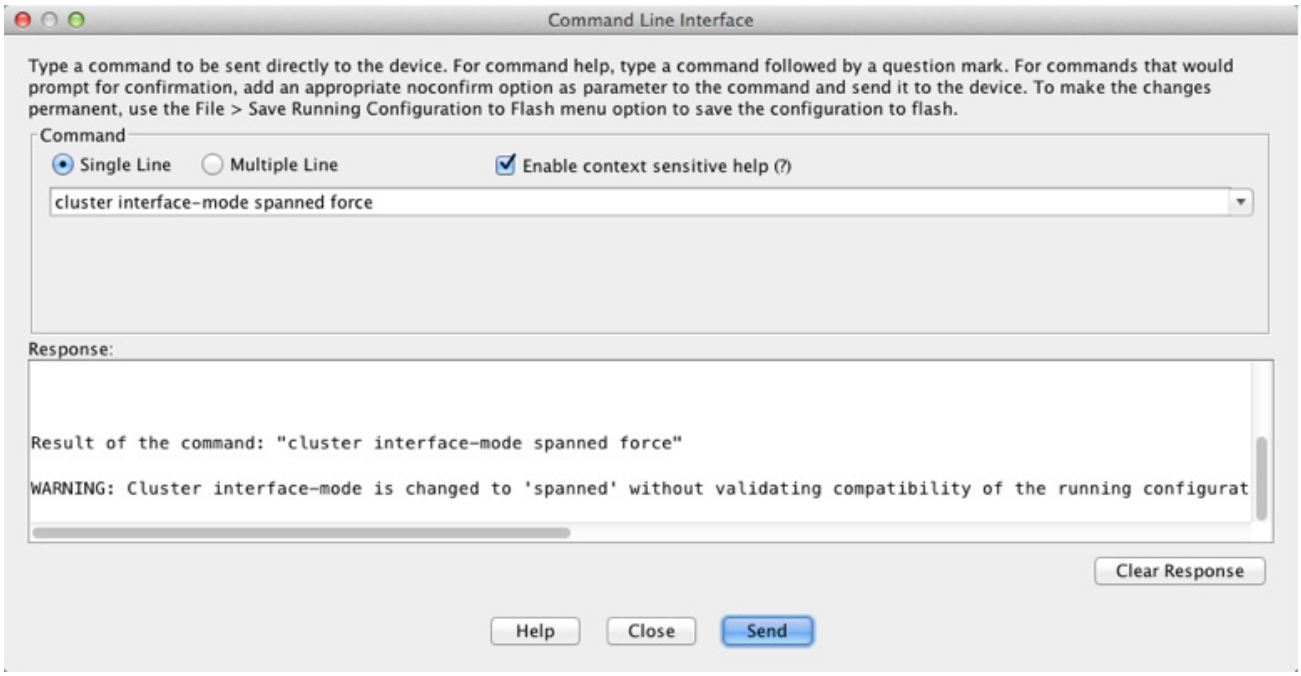


주의 인터페이스 모드를 설정한 후에는 인터페이스에 연결을 수행할 수 있습니다. 그러나 클러스터링 요구 사항을 준수하도록 관리 인터페이스를 컨피그레이션하기 전에 ASA를 다시 로드할 경우(예: 클러스터 IP 추가), 클러스터 비호환 인터페이스 컨피그레이션이 제거되므로 다시 연결할 수 없게 됩니다. 이 경우 콘솔 포트에 연결하여 인터페이스 컨피그레이션을 수정해야 합니다.

2단계 클러스터링에 대한 인터페이스 모드를 설정합니다.

```
cluster interface-mode {individual | spanned} force
```

예:



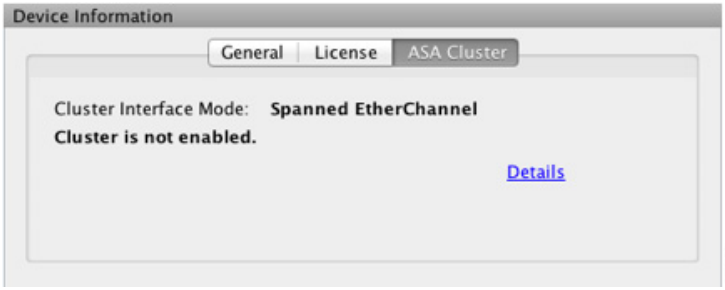
기본 설정은 없으며, 모드를 명시적으로 선택해야 합니다. 모드를 설정하지 않을 경우 클러스터링을 사용할 수 없습니다.

강제 옵션을 사용하면 컨피그레이션에 호환되지 않는 설정이 있는지 확인하지 않고 모드를 변경합니다. 모드를 변경한 후에는 수동으로 컨피그레이션 문제를 수정해야 합니다. 모드를 설정한 후에는 인터페이스 컨피그레이션을 수정하는 것만 가능하므로, **강제** 옵션을 사용하여 최소한 기존 컨피그레이션에서 시작하는 방법을 권장합니다. 자세한 지침을 보려면 모드를 설정한 후 **세부 정보 확인** 옵션을 다시 실행합니다.

강제 옵션을 사용하지 않을 경우 호환되지 않는 컨피그레이션 문제가 발생하면 컨피그레이션을 지우고 다시 로드하겠는지 묻는 메시지가 표시됩니다. 이 경우 콘솔 포트에 연결하여 관리 액세스를 다시 컨피그레이션해야 합니다. 드물게 컨피그레이션이 호환되는 경우 모드가 변경되며 해당 컨피그레이션이 유지됩니다. 컨피그레이션을 지우지 않으려면 **n**을 입력하여 명령 창에서 나옵니다.

인터페이스 모드를 제거하려면 **no cluster interface-mode** 명령을 입력합니다.

3단계 ASDM을 종료하고 다시 로드합니다. 클러스터 인터페이스 모드를 올바르게 어카운팅하려면 ASDM을 다시 시작해야 합니다. 다시 로드하면 홈 페이지에 ASA Cluster 탭이 표시됩니다.



관련 주제

- 9-41 페이지의 (권장, 다중 컨텍스트 모드에서 필요) 마스터 유닛의 인터페이스 구성

(권장, 다중 컨텍스트 모드에서 필요) 마스터 유닛의 인터페이스 구성

클러스터링을 활성화하기 *전에*, 현재 IP 주소가 구성된 모든 인터페이스가 클러스터링을 수행할 준비가 되도록 수정해야 합니다. 최소한 ASDM이 현재 연결된 관리 인터페이스는 반드시 수정해야 합니다. 그 외의 기타 인터페이스는 클러스터링을 활성화하기 전에 또는 활성화한 후에 컨피그레이션할 수 있습니다. 그러나 모든 인터페이스를 사전에 컨피그레이션하여 전체 컨피그레이션을 새 클러스터 컨피그레이션원과 동기화하는 것이 좋습니다. 다중 컨텍스트 모드의 경우 이 섹션에 설명된 절차를 사용하여 기존 인터페이스를 수정하거나 새 인터페이스를 구성해야 합니다. 그러나 단일 모드의 경우, 이 섹션을 건너뛰고 High Availability and Scalability 마법사에서 공통 인터페이스 매개변수를 구성할 수 있습니다(9-47 페이지의 ASA 클러스터 생성 또는 참가 참조). 마법사에서는 개별 인터페이스에 EtherChannel을 생성하는 것과 같은 고급 인터페이스 설정은 지원되지 않습니다.

이 섹션에서는 클러스터링과 호환되는 인터페이스를 구성하는 방법에 대해 설명합니다. 데이터 인터페이스를 Spanned EtherChannel 또는 개별 인터페이스로 구성할 수 있습니다. 각 방법에서는 다양한 로드 밸런싱 메커니즘을 사용합니다. Spanned EtherChannel 모드에서도 개별 인터페이스가 될 수 있는 관리 인터페이스를 제외하고는 같은 컨피그레이션에 두 가지 유형을 모두 컨피그레이션할 수 없습니다.

- 9-41 페이지의 개별 인터페이스 구성(관리 인터페이스 권장 사항)
- 9-44 페이지의 Spanned EtherChannel 구성

관련 주제

- 9-4 페이지의 클러스터 인터페이스

개별 인터페이스 구성(관리 인터페이스 권장 사항)

개별 인터페이스는 정상적인 라우팅 인터페이스로, 각각 IP 주소 풀에서 가져온 고유한 IP 주소가 있습니다. 기본 클러스터 IP 주소는 현재 마스터 유닛에 항상 속해 있는 클러스터의 고정 주소입니다.

Spanned EtherChannel 모드의 경우 관리 인터페이스를 개별 인터페이스로 구성하는 방법을 권장합니다. 개별 인터페이스를 사용하면 필요한 경우 각 유닛에 직접 연결할 수 있는 반면, Spanned EtherChannel 인터페이스의 경우에는 현재 마스터 유닛에 대한 연결만 가능합니다.

시작하기 전에

- 관리 전용 인터페이스를 제외하고, 개별 인터페이스 모드를 사용해야 합니다.
- 다중 컨텍스트 모드의 경우, 각 컨텍스트에서 이러한 절차를 수행합니다. 현재 컨텍스트 컨피그레이션 모드에 있지 않은 경우, Configuration > *Device List* 의 액티브 디바이스 IP 주소 아래에서 컨텍스트 이름을 두 번 클릭하여 **changeto context** *name* 명령을 입력합니다.
- 개별 인터페이스는 인접 디바이스의 로드 밸런싱을 구성해야 합니다. 관리 인터페이스에는 외부 로드 밸런싱이 필요하지 않습니다.
- (선택 사항) 인터페이스를 디바이스-로컬 EtherChannel, 이중화 인터페이스로 구성하거나 하위 인터페이스로 구성합니다.
  - EtherChannel의 경우 이러한 EtherChannel은 유닛에 대해 로컬이며 Spanned EtherChannel이 아닙니다.
  - 관리 전용 인터페이스는 이중화 인터페이스가 될 수 없습니다.
- ASDM을 사용하는 관리 인터페이스에 원격으로 연결할 경우, 잠재적인 슬레이브 유닛의 현재 IP 주소는 일시적으로 사용됩니다.
  - 각 멤버는 마스터 유닛에 정의된 클러스터 IP 풀에서 IP 주소를 할당합니다.
  - 클러스터 IP 풀에는 잠재적인 슬레이브 IP 주소를 비롯하여, 네트워크에서 이미 사용 중인 주소가 포함될 수 없습니다.

    예:

  a. 10.1.1.1을 사용하도록 마스터 유닛을 구성합니다.
  b. 다른 유닛에서는 10.1.1.2, 10.1.1.3, 10.1.1.4를 사용합니다.
  c. 마스터 유닛에서 클러스터 IP 풀을 구성할 경우, .2, .3 또는 .4 주소가 이미 사용 중이므로 해당 주소를 풀에 포함할 수 없습니다.
  d. 대신 네트워크에 .5, .6, .7, .8 같은 다른 IP 주소를 사용해야 합니다.

  참고 풀에는 마스터 유닛을 비롯하여 클러스터의 멤버 수에 상응하는 개수만큼의 주소가 있어야 합니다. 원본 .1 주소는 현재 마스터 유닛에 속하는 기본 클러스터 IP 주소입니다.

  e. 클러스터에 참가하게 되면 오래된 임시 주소는 양도되며 다른 곳에 사용할 수 있습니다.

절차

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 인터페이스 행을 선택하고 **Edit**를 클릭합니다. 인터페이스 매개변수를 설정합니다. 다음 지침을 참조하십시오.

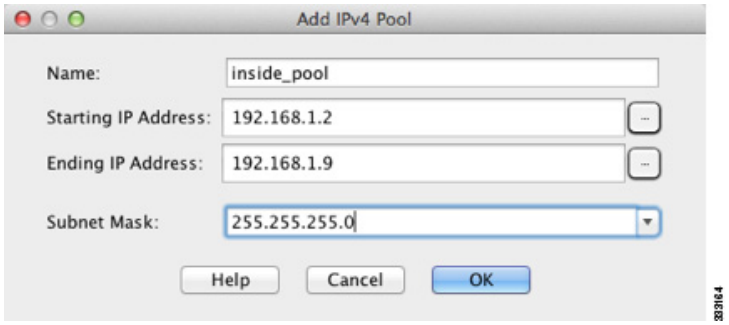
- (Spanned EtherChannel 모드의 관리 인터페이스에 필요한 사항) **이 인터페이스를 관리 전용으로 설정** — 인터페이스를 관리 전용 모드로 설정하여 트래픽을 통해 전달되지 않도록 합니다. 기본적으로 관리 유형 인터페이스는 관리 전용으로 구성됩니다. 투명 모드에서 이 명령은 관리 유형 인터페이스에 항상 사용됩니다.
- **고정 IP 사용** — DHCP 및 PPPoE가 지원되지 않습니다.

3단계 IPv4 클러스터 IP 풀을 추가하고 선택에 따라 MAC 주소 풀도 추가하려면 **Advanced** 탭을 클릭합니다.

a. **ASA Cluster** 영역에서 **IP Address Pool** 필드 옆에 있는 **...** 버튼을 클릭하여 클러스터 풀 IP를 생성합니다. 표시되는 유효한 범위는 General 탭에서 설정한 기본 IP 주소에 따라 결정됩니다.

b. **Add**를 클릭합니다.

c. 기본 클러스터 IP 주소를 포함하지 않고, 네트워크에서 현재 사용 중인 모든 주소를 포함하지 않는 주소 범위를 구성합니다. 주소 범위는 예를 들어 주소가 8개 포함될 정도로 클러스터의 크기를 고려하여 충분하게 설정해야 합니다.



d. **OK**를 클릭하여 새 풀을 생성합니다.

e. 생성한 새 풀을 선택하고 **Assign**을 할당한 다음 **OK**를 클릭합니다.

풀 이름이 **IP Address Pool** 필드에 표시됩니다.

4단계 IPv6 주소를 구성하려면 **IPv6** 탭을 클릭합니다.

a. **Enable IPv6** 확인란을 선택합니다.

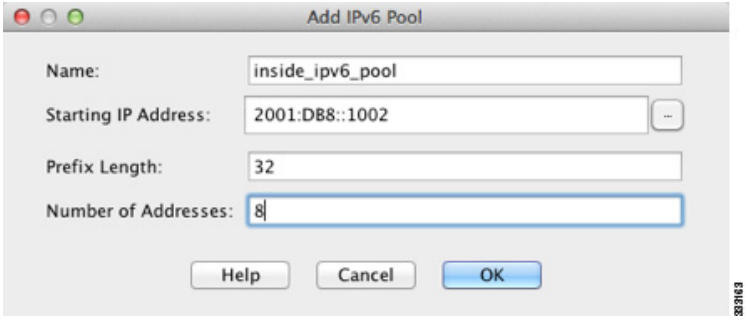
b. **Interface IPv6 Addresses** 영역에서 **Add**를 클릭합니다.

Enable address autoconfiguration 옵션은 지원되지 않습니다.

Add IPv6 Address for Interface 대화 상자가 나타납니다.

c. **Address/Prefix Length** 필드에 전역 IPv6 주소 및 IPv6 접두사 길이를 입력합니다. 예를 들면 2001:0DB8::BA98:0:3210/48입니다.**...** 버튼을 클릭하여 클러스터 IP 풀을 구성합니다.

d. **Add**를 클릭합니다.



e. 시작 IP 주소(네트워크 접두사), 접두사 길이, 풀의 주소 개수를 구성합니다.

f. **OK**를 클릭하여 새 풀을 생성합니다.

g. 생성한 새 풀을 선택하고 **Assign**을 할당한 다음 **OK**를 클릭합니다.

ASA Cluster IP Pool 필드에 풀이 표시됩니다.

h. **OK**를 클릭합니다.

5단계 **OK**를 클릭하여 Interfaces 창으로 돌아갑니다.

6단계 **Apply**를 클릭합니다.

관련 주제

- 9-11 페이지의 관리 인터페이스
- 9-39 페이지의 각 유닛의 마스터 유닛에서 클러스터 인터페이스 모드
- 9-12 페이지의 로드 밸런싱 방법
- 10-20 페이지의 EtherChannel 구성
- 10-17 페이지의 이중화 인터페이스 구성
- 10-25 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹

Spanned EtherChannel 구성

Spanned EtherChannel은 클러스터의 모든 ASA를 포괄하며, EtherChannel이 실행되는 과정의 일환으로 로드 밸런싱을 제공합니다.

시작하기 전에

- Spanned EtherChannel 인터페이스 모드에 있어야 합니다.
- 다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 시작합니다. 현재 시스템 컨피그레이션 모드에 있지 않은Configuration > Device List 창의 액티브 디바이스 IP 주소 아래에서 **System**을 두 번 클릭하여 **changeto system** 명령을 입력합니다.
- 투명 모드의 경우 브릿지 그룹을 구성합니다.
- EtherChannel에서는 최대 및 최소 링크를 지정하지 *마십시오*. EtherChannel에서는 ASA 또는 스위치에 최대 및 최소 링크를 지정하지 않는 것이 좋습니다. 사용해야 하는 경우 다음 사항을 주의하십시오.
  - ASA에 설정되는 최대 링크는 전체 클러스터의 총 활성 포트 개수입니다. 스위치에 구성된 최대 링크 값이 ASA 값보다 크지 않은지 확인하십시오.
  - ASA에 설정된 최소 링크는 *유닛당* 포트 채널 인터페이스를 가져오는 최소 활성 포트입니다. 스위치의 최소 링크는 클러스터 전체의 최소 링크이므로 이 값은 ASA 값과 일치하지 않습니다.
- 로드 밸런싱 알고리즘의 기본값을 변경하지 *마십시오*. 스위치에서는 **source-dest-ip** 또는 **source-dest-ip-port** 로드 밸런싱 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 및 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 ASA에 트래픽이 균일하지 않게 분산될 수 있기 때문입니다.
- Spanned EtherChannel을 사용할 경우, 클러스터링이 완전히 활성화될 때까지 포트 채널 인터페이스가 작동하지 않습니다. 이러한 요구 사항으로 인해 클러스터의 활성 유닛이 아닌 유닛에는 트래픽이 전달되지 않습니다.

절차

1단계 컨텍스트 모드에 따라

- 단일 모드에서는 **Configuration > Device Setup > Interfaces** 창을 선택합니다.
- 다중 모드의 경우 시스템 실행 영역에서 **Configuration > Context Management > Interfaces** 창을 선택합니다.

2단계 **Add > EtherChannel Interface**를 선택합니다.

Add EtherChannel Interface 대화 상자가 나타납니다.

3단계 다음을 활성화합니다.

- **Port Channel ID**
- **Span EtherChannel across the ASA cluster**
- **Enable Interface**(기본적으로 선택되어 있음)
- **Members in Group** — **Members in Group** 목록에서 최소 하나의 인터페이스를 추가해야 합니다. 유닛당 EtherChannel의 다중 인터페이스는 VSS 또는 vPC의 스위치에 연결할 때 유용합니다. 기본적으로 Spanned EtherChannel의 경우 클러스터의 모든 멤버 전체의 최대 16개 인터페이스 중 활성 인터페이스를 8개까지만 보유할 수 있습니다. 나머지 8개 인터페이스는 링크 오류에 대비하여 스탠바이 상태로 유지됩니다. 스탠바이 인터페이스는 그대로 두고 8개 이상의 활성 인터페이스를 사용하려면 동적 포트 우선순위를 비활성화합니다. 동적 포트 우선순위를 비활성화하면 클러스터 전체에 걸쳐 최대 32개의 활성 링크를 사용할 수 있습니다. 예를 들어, 16개의 ASA로 구성된 클러스터의 경우 각 ASA에 최대 2개의 인터페이스를 사용할 수 있으므로 Spanned EtherChannel의 인터페이스는 총 32개입니다.

  모든 인터페이스의 유형과 속도가 같은지 확인합니다. 첫 번째로 추가된 인터페이스가 EtherChannel의 유형과 속도를 결정합니다. 추가되었으나 일치하지 않는 인터페이스는 보류 상태로 됩니다. ASDM에서는 일치하지 않는 인터페이스가 추가되는 것을 방지하지 못합니다.

이 화면에 있는 필드의 나머지 부분은 이 절차의 뒷부분에서 설명합니다.

4단계 (선택 사항) 모든 멤버 인터페이스의 미디어 유형, 양방향, 속도, 흐름 제어를 위한 일시 중지 프레임을 재정의하려면 **Configure Hardware Properties**를 클릭합니다. 이러한 매개변수는 채널 그룹의 모든 인터페이스와 일치해야 하므로, 이 방법을 사용하면 이러한 매개변수를 빠르게 설정할 수 있습니다.

OK를 클릭하여 **Hardware Properties** 변경 사항을 승인합니다.

5단계 MAC 주소 및 선택적 매개변수를 구성하려면 **Advanced** 탭을 클릭합니다.

- **MAC Address Cloning** 영역에서 EtherChannel의 수동 MAC 주소를 설정합니다. 스탠바이 MAC 주소는 무시되므로 설정하지 마십시오. Spanned EtherChannel의 MAC 주소를 구성하여 현재 마스터 유닛이 클러스터를 벗어날 경우 MAC 주소가 변경되지 않도록 해야 합니다. 수동으로 구성된 MAC 주소를 사용할 경우 MAC 주소가 현재 마스터 유닛에 그대로 유지됩니다.

  다중 컨텍스트 모드에서 컨텍스트 간에 인터페이스를 공유할 경우, 기본적으로 MAC 자동 생성이 활성화됩니다. 따라서 자동 생성을 비활성화한 경우 공유 인터페이스의 MAC 주소를 수동으로 설정하기만 하면 됩니다. 공유되지 않는 인터페이스의 MAC 주소는 수동으로 구성해야 합니다. 자동 생성된 MAC 주소도 사용하려는 경우 수동 MAC 주소의 처음 2바이트는 A2가 될 수 없습니다.
- (선택 사항) ASA를 VSS 또는 vPC에 있는 두 개의 스위치에 연결할 경우, **Enable load balancing between switch pairs in VSS or vPC** 모드 확인란을 선택하여 VSS 로드 밸런싱을 활성화해야 합니다. 이 기능은 VSS(또는 vPC) 쌍에 대한 ASA 간의 물리적 링크 연결이 균형을 이루도록 보장합니다.

그런 다음 **Member Interface Configuration** 영역에서 특정 인터페이스가 **1** 또는 **2** 중 어느 스위치에 연결되는지 확인해야 합니다.

참고 **Minimum Active Members** 및 **Maximum Active Members**를 설정하지 *않는*것이 좋습니다.

6단계 (선택 사항) 이 EtherChannel에 VLAN 하위 인터페이스를 구성합니다. 이 절차의 나머지는 하위 인터페이스에 적용됩니다.

7단계 (다중 컨텍스트 모드) 이 절차를 완료하기 전에 컨텍스트에 인터페이스를 할당해야 합니다.

a. 변경 사항을 적용하려면 **OK**를 클릭합니다.

b. 인터페이스를 할당합니다.

c. 구성할 컨텍스트를 변경하려면 **Device List** 창의 액티브 디바이스 IP 주소 아래에서 컨텍스트 이름을 두 번 클릭합니다.

d. **Configuration > Device Setup > Interfaces** 창을 선택하고 맞춤화하려는 포트 채널 인터페이스를 선택한 다음 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 나타납니다.

8단계 **General** 탭을 클릭합니다.

9단계 (투명 모드) **Bridge Group** 드롭다운 목록에서 이 인터페이스를 할당할 브릿지 그룹을 선택합니다.

10단계 **Interface Name** 필드에 이름을 48자 이내로 입력합니다.

11단계 **Security level** 필드에 0(가장 낮음)~100(가장 높음) 범위의 레벨을 입력합니다.

12단계 (투명 모드) IPv4 주소의 경우 **Use Static IP** 라디오 버튼을 클릭하고 IP 주소 및 마스크를 입력합니다. DHCP 및 PPPoE는 지원되지 않습니다. 투명 모드의 경우, EtherChannel 인터페이스가 아닌 브릿지 그룹 인터페이스의 IP 주소를 구성해야 합니다.

13단계 (라우팅 모드) IPv6 주소를 구성하려면 **IPv6** 탭을 클릭합니다.

투명 모드의 경우, EtherChannel 인터페이스가 아닌 브릿지 그룹 인터페이스의 IP 주소를 구성해야 합니다.

a. **Enable IPv6** 확인란을 선택합니다.

b. **Interface IPv6 Addresses** 영역에서 **Add**를 클릭합니다.

Add IPv6 Address for Interface 대화 상자가 나타납니다.

참고: **Enable address autoconfiguration** 옵션은 지원되지 않습니다.

c. **Address/Prefix Length** 필드에 전역 IPv6 주소 및 IPv6 접두사 길이를 입력합니다. 예를 들어, 2001:DB8::BA98:0:3210/64와 같이 입력합니다.

d. (선택 사항) Modified EUI-64 인터페이스 ID를 호스트 주소로 사용하려면 **EUI-64** 확인란을 선택합니다. 이 경우 **Address/Prefix Length** 필드에 접두사만 입력합니다.

e. **OK**를 클릭합니다.

14단계 **OK**를 클릭하여 **Interfaces** 화면으로 돌아갑니다.

15단계 **Apply**를 클릭합니다.

관련 주제

- 9-39 페이지의 각 유닛의 마스터 유닛에서 클러스터 인터페이스 모드
- 13-6 페이지의 브리지 그룹 구성
- 9-47 페이지의 ASA 클러스터 생성 또는 참가
- 10-20 페이지의 EtherChannel 구성
- 10-11 페이지의 EtherChannel 지침
- 9-14 페이지의 VSS 또는 vPC에 연결
- 10-14 페이지의 물리적 인터페이스 활성화 및 이더넷 매개변수 구성
- 10-25 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹
- 7-19 페이지의 보안 컨텍스트 구성
- 12-1 페이지의 보안 레벨
- 9-50 페이지의 ASA 클러스터 매개변수 구성
- 9-32 페이지의 ASA 클러스터링 지침

ASA 클러스터 생성 또는 참가

클러스터의 각 유닛은 클러스터에 참가하려면 부트스트랩 컨피그레이션이 필요합니다. 한 유닛(이 유닛이 마스터 유닛이 됨)에서 High Availability and Scalability 마법사를 실행하여 클러스터를 생성한 후 여기에 슬레이브 유닛을 추가합니다.

참고 마스터 유닛의 경우 cLACP 시스템 ID 및 우선순위의 기본값을 변경하려면 마법사를 사용할 수 없습니다. 클러스터를 수동으로 구성해야 합니다.

시작하기 전에

- 다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 아직 System 컨피그레이션 모드가 아닐 경우 Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.
- 클러스터 제어 링크 MTU는 1600바이트 이상으로 설정하는 것이 좋습니다. 이 경우 이 절차를 계속 진행하기 전에 *각 유닛에* 점보 프레임 예약을 활성화해야 합니다. 점보 프레임 예약을 수행하려면 ASA를 다시 로드해야 합니다.
- 클러스터 제어 링크 인터페이스에 사용할 인터페이스는 연결된 스위치에서 가동 중인 상태여야 합니다.
- 실행 중인 클러스터에 유닛을 추가할 경우, 일시적이고 제한적으로 패킷/연결이 감소할 수 있으며 이는 정상적인 동작입니다.

절차

1단계 **Wizards > High Availability and Scalability Wizard**를 선택합니다. 다음 단계에서 선택된 마법사 지침을 참조합니다.

2단계 **Interfaces** 화면에서는 새로운 EtherChannel을 생성할 수 없습니다(클러스터 제어 링크의 경우는 제외).

3단계 ASA Cluster Configuration 화면에서 다음과 같은 부트스트랩 설정을 구성합니다.

- **Member Priority** — 마스터 유닛 선택을 위해 이 유닛의 우선순위를 1에서 100까지 설정하며 1의 우선순위가 가장 높습니다.
- (선택 사항) **Shared Key** — 클러스터 제어 링크의 제어 트래픽에 대한 암호화 키를 설정합니다. 공유 비밀은 1~63자로 된 ASCII 문자열입니다. 공유 비밀은 암호화 키를 생성하는 데 사용됩니다. 이 매개변수는 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다. 또한 비밀번호 암호화 서비스를 사용할 경우 이 매개변수를 구성해야 합니다.
- (선택 사항) **Enable connection rebalancing for TCP traffic across all the ASAs in the cluster** — 연결 재밸런싱을 활성화합니다. 이 매개변수는 기본적으로 비활성화되어 있습니다. 활성화할 경우 클러스터의 ASA에서는 로드 정보를 주기적으로 교환하며, 로드가 과중한 디바이스에서 적은 디바이스로 새 연결을 오프로드합니다. 빈도는 1에서 360초 사이이며, 로드 정보를 교환하는 빈도를 지정합니다. 이 매개변수는 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다.

  참고 사이트 간 토폴로지에 대한 연결 재밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 대한 연결이 재밸런싱됩니다.

- (선택 사항) **Enable health monitoring of this device within the cluster** — 유닛 검사 모니터링 및 인터페이스 상태 모니터링이 포함된 클러스터 상태 검사 기능을 활성화합니다. 유닛 상태를 확인하기 위해 ASA 클러스터 유닛에서는 다른 유닛에 대한 클러스터 제어 링크에 keepalive 메시지를 보냅니다. 피어 유닛의 keepalive 메시지가 대기 시간 내에 유닛에 전송되지 않을 경우, 해당 피어 유닛은 응답하지 않거나 중지된 상태로 간주합니다. 인터페이스 상태 검사에서는 링크 오류 여부를 모니터링합니다. 특정 유닛의 인터페이스에 오류가 발생하였으나 다른 유닛의 동일한 인터페이스는 활성 상태인 경우, 클러스터에서 해당 특정 유닛이 제거됩니다. 대기 시간 내에 인터페이스 상태 메시지가 유닛에 전송되지 않을 경우, ASA에서 클러스터의 멤버를 제거하기까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 좌우됩니다.

  참고 토폴로지에 변경 사항이 발생할 경우(예: 데이터 인터페이스 추가 또는 제거, ASA 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 생성) 상태 검사를 비활성화해야 합니다. 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사를 다시 사용할 수 있습니다.

  - **Time to Wait Before Device Considered Failed** — 이 값은 유닛 간의 keepalive 상태 메시지 시간 간격을 0.8초에서 45초 사이로 지정하며, 기본값은 3초입니다. 대기 시간 값은 *유닛* 상태 검사에만 영향을 미칩니다. 인터페이스 상태의 경우 ASA에서는 인터페이스 상태(가동 또는 중지)를 사용합니다.
  - (선택 사항) **Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support** — 클러스터 제어 링크를 EtherChannel로 구성하고(권장) 이를 VSS 또는 vPC 쌍에 연결한 경우, vss-enabled 옵션을 활성화해야 할 수 있습니다. 일부 스위치의 경우 VSS/vPC에서 유닛 하나가 중단되거나 부팅하면 해당 스위치에 연결된 EtherChannel 멤버 인터페이스가 ASA에 대해 가동되는 것으로 표시되지만, 스위치 측의 트래픽을 통과하지 않습니다. ASA 대기 시간 제한을 낮은 값으로 설정한 경우(0.8초) 클러스터에서 ASA가 잘못 제거될 수 있으며 ASA에서는 이러한 EtherChannel 인터페이스 중 하나에 keepalive 메시지를 보냅니다. 이 옵션을 활성화할 경우, ASA에서는 하나 이상의 스위치에 keepalive 메시지가 전송되도록 하기 위해 클러스터 제어 링크의 모든 EtherChannel 인터페이스에서 대량의 keepalive 메시지를 보냅니다.

- (선택 사항) **Replicate console output to the master's console** — 슬레이브 유닛에서 마스터 유닛으로 콘솔 복제를 활성화합니다. 이 기능은 기본적으로 비활성화되어 있습니다. ASA에서는 중요한 특정 이벤트 발생 시 일부 메시지를 콘솔에 직접 출력합니다. 콘솔 복제를 활성화할 경우, 슬레이브 유닛에서는 콘솔 메시지를 마스터 유닛에 전송하므로 클러스터의 콘솔 포트 하나만 모니터링하면 됩니다. 이 매개변수는 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다.
- **Cluster Control Link** — 클러스터 제어 링크 인터페이스를 지정합니다.
  - (선택 사항) **MTU** — 클러스터 제어 링크 인터페이스의 최대 전송 단위를 지정하며 64에서 65,535바이트 사이로 설정합니다. MTU 값보다 큰 데이터는 전송 전에 분할됩니다. 기본 MTU는 1500바이트입니다. 점보 프레임 예약을 이미 활성화한 경우, MTU를 1600바이트 이상으로 설정하는 것이 좋습니다. 점보 프레임을 사용할 예정이지만 점보 프레임 예약을 사전에 활성화하지 않은 경우, 마법사를 종료하고 점보 프레임을 활성화한 다음 이 절차를 다시 시작해야 합니다.

4단계 **Finish**를 클릭합니다.

5단계 ASA에서는 실행 중인 컨피그레이션을 검사하여 클러스터링에서 지원되지 않는 기능에 대한 호환되지 않는 명령을 확인하며, 여기에는 기본 컨피그레이션에 없을 수 있는 명령이 포함됩니다. **OK**를 클릭하여 호환되지 않는 명령을 삭제합니다. **Cancel**을 클릭하면 클러스터링이 활성화되지 않습니다.

6단계 ASDM에서 클러스터링을 활성화하고 ASA에 다시 연결하는 시간이 지나면, 클러스터에 ASA가 추가되었음을 확인하는 Information 화면이 나타납니다.

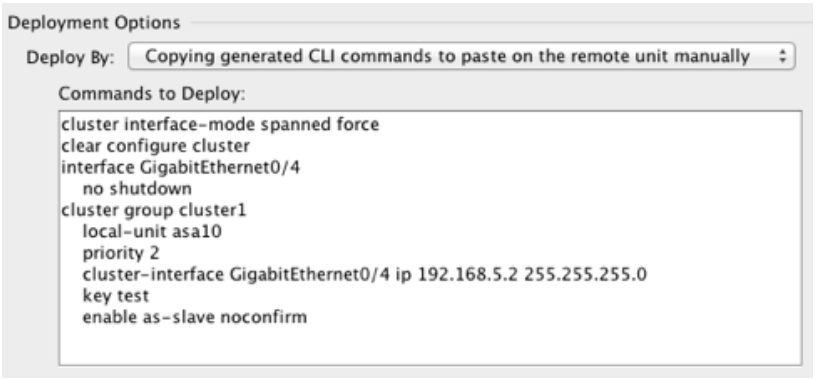
참고 경우에 따라 마법사를 완료한 후 클러스터에 참가할 때 오류가 발생할 수 있습니다. ASDM의 연결이 끊어진 경우 ASA의 후속 오류 메시지가 ASDM에 전송되지 않습니다. ASDM에 다시 연결한 후에도 클러스터링이 비활성화된 상태로 남아 있는 경우, ASA 콘솔 포트에 연결하여 클러스터링이 비활성화된 정확한 오류 상황을 확인해야 합니다. 클러스터 제어 링크가 중단되는 경우를 예로 들 수 있습니다.

7단계 슬레이브 유닛을 추가하려면 **Yes**를 클릭합니다.

마스터에서 마법사를 다시 실행할 경우, 마법사를 처음 실행할 때 **Add another member to the cluster** 옵션을 선택하여 슬레이브 유닛을 추가할 수 있습니다.

8단계 **Deployment Options** 영역에서 다음 **Deploy By** 옵션 중 하나를 선택합니다.

- **Sending CLI commands to the remote unit now —** 부트스트랩 컨피그레이션을 슬레이브(임시) 관리 IP 주소로 보냅니다. 슬레이브 관리 IP 주소, 사용자 이름, 비밀번호를 입력합니다.
- **Copying generated CLI commands to paste on the remote unit manually** — 명령을 생성하여 슬레이브 유닛 CLI에서 잘라내기/붙여넣기하거나 ASDM에서 CLI 툴을 사용합니다. Commands to Deploy 상자에서 생성된 명령을 선택 및 복사하여 나중에 사용할 수 있습니다.



관련 주제

- 9-50 페이지의 ASA 클러스터 매개변수 구성
- 10-28 페이지의 점보 프레임 지원 활성화
- 9-44 페이지의 Spanned EtherChannel 구성
- 9-41 페이지의 개별 인터페이스 구성(관리 인터페이스 권장 사항)
- 9-9 페이지의 인터페이스 모니터링

ASA 클러스터 구성원 관리

클러스터를 배치한 후에는 컨피그레이션을 변경하고 클러스터 컨피그레이션원을 관리할 수 있습니다.

- 9-50 페이지의 ASA 클러스터 매개변수 구성
- 9-53 페이지의 마스터 유닛에서 새 슬레이브 추가
- 9-55 페이지의 구성원 비활성화
- 9-56 페이지의 마스터 유닛의 슬레이브 구성원 비활성화
- 9-57 페이지의 클러스터 벗어나기
- 9-58 페이지의 마스터 유닛 변경
- 9-58 페이지의 클러스터 전체에 명령 실행

ASA 클러스터 매개변수 구성

마법사를 사용하지 않고 클러스터에 유닛을 추가하려면 클러스터 매개변수를 수동으로 구성합니다. 이미 클러스터링을 활성화한 경우, 일부 클러스터 매개변수를 편집할 수 있습니다. 나머지 매개변수는 클러스터링이 활성화된 동안에는 회색으로 비활성화되어 편집할 수 없습니다. 이 절차에는 마법사에 포함되지 않은 고급 매개변수도 포함됩니다.

시작하기 전에

- 클러스터에 참가하기 전에 각 유닛의 클러스터 제어 링크 인터페이스를 사전 구성합니다. 단일 인터페이스의 경우 이를 활성화해야 하며, 다른 설정은 구성하지 마십시오. EtherChannel 인터페이스의 경우 이를 활성화하고 EtherChannel 모드를 On으로 설정합니다.
- 다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 아직 System 컨피그레이션 모드가 아닐 경우 Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.

절차

1단계 **Configuration > Device Management > High Availability and Scalability > ASA Cluster**를 선택합니다.

클러스터에 디바이스가 이미 있고 마스터 유닛인 경우, 이 창이 Cluster Configuration 탭에 표시됩니다.

2단계 **Configure ASA cluster settings** 확인란을 선택합니다.

이 확인란을 선택하지 않으면 설정이 지워집니다. 모든 매개변수를 설정하기 전에는 **Participate in ASA cluster**를 선택하지 마십시오.

참고 클러스터링을 활성화한 후에는 **Configure ASA cluster settings** 확인란의 선택을 취소했을 때 어떤 결과가 발생하는지 잘 모르는 상태에서 선택을 취소하지 마십시오. 취소할 경우 모든 클러스터 컨피그레이션이 지워지며 ASDM이 연결된 모든 관리 인터페이스를 비롯한 모든 인터페이스도 종료됩니다. 이 경우 연결을 복원하려면 콘솔 포트의 CLI에 액세스해야 합니다.

3단계 다음과 같은 부트스트랩 매개변수를 구성합니다.

- **Cluster Name** — 클러스터의 이름을 지정합니다. 이름은 1~38자로 된 ASCII 문자열이어야 합니다. 유닛당 클러스터는 하나만 구성할 수 있습니다. 클러스터의 모든 멤버는 동일한 이름을 사용해야 합니다.
- **Member Name** — 이 클러스터 멤버의 이름을 1~38자로 된 ASCII 문자열로 지정합니다.
- **Member Priority** — 마스터 유닛 선택을 위해 이 유닛의 우선순위를 1에서 100까지 설정하며 1의 우선순위가 가장 높습니다.
- (선택 사항) **Shared Key** — 클러스터 제어 링크의 제어 트래픽에 대한 암호화 키를 설정합니다. 공유 비밀은 1~63자로 된 ASCII 문자열입니다. 공유 비밀은 암호화 키를 생성하는 데 사용됩니다. 이 매개변수는 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다. 또한 비밀번호 암호화 서비스를 사용할 경우 이 매개변수를 구성해야 합니다.
- (선택 사항) **Enable connection rebalancing for TCP traffic across all the ASAs in the cluster** — 연결 재밸런싱을 활성화합니다. 이 매개변수는 기본적으로 비활성화되어 있습니다. 활성화할 경우 클러스터의 ASA에서는 로드 정보를 주기적으로 교환하며, 로드가 과중한 디바이스에서 적은 디바이스로 새 연결을 오프로드합니다. 빈도는 1에서 360초 사이이며, 로드 정보를 교환하는 빈도를 지정합니다. 이 매개변수는 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다.

- (선택 사항) **Enable health monitoring of this device within the cluster** — 유닛 검사 모니터링 및 인터페이스 상태 모니터링이 포함된 클러스터 상태 검사 기능을 활성화합니다. **참고**: 클러스터에 새 유닛을 추가하고 ASA 또는 스위치에서 토폴로지를 변경할 경우, 클러스터가 완료될 때까지 이러한 기능을 일시적으로 비활성화해야 합니다. 클러스터 및 토폴로지 변경이 완료되면 이러한 기능을 다시 활성화할 수 있습니다. 유닛 상태를 확인하기 위해 ASA 클러스터 유닛에서는 다른 유닛에 대한 클러스터 제어 링크에 keepalive 메시지를 보냅니다. 피어 유닛의 keepalive 메시지가 대기 시간 내에 유닛에 전송되지 않을 경우, 해당 피어 유닛은 응답하지 않거나 중지된 상태로 간주합니다. 인터페이스 상태 메시지에 링크 장애가 감지됩니다. 특정 유닛의 인터페이스에 오류가 발생하였으나 다른 유닛의 동일한 인터페이스는 활성 상태인 경우, 클러스터에서 해당 특정 유닛이 제거됩니다. 대기 시간 내에 인터페이스 상태 메시지가 유닛에 전송되지 않을 경우, ASA에서 클러스터의 멤버를 제거하기까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 좌우됩니다.

  참고 토폴로지에 변경 사항이 발생할 경우(예: 데이터 인터페이스 추가 또는 제거, ASA 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS 또는 vPC 생성) 상태 검사를 비활성화해야 합니다. 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사를 다시 사용할 수 있습니다.

  - (선택 사항) **Broadcast keepalive messages to all EtherChannel cluster control link ports for VSS/vPC support** — 클러스터 제어 링크를 EtherChannel로 구성하고(권장) 이를 VSS 또는 vPC 쌍에 연결한 경우, vss-enabled 옵션을 활성화해야 할 수 있습니다. 일부 스위치의 경우 VSS/vPC에서 유닛 하나가 중단되거나 부팅하면 해당 스위치에 연결된 EtherChannel 멤버 인터페이스가 ASA에 대해 가동되는 것으로 표시되지만, 스위치 측의 트래픽을 통과하지 않습니다. ASA 대기 시간 제한을 낮은 값으로 설정한 경우(0.8초) 클러스터에서 ASA가 잘못 제거될 수 있으며 ASA에서는 이러한 EtherChannel 인터페이스 중 하나에 keepalive 메시지를 보냅니다. 이 옵션을 활성화할 경우, ASA에서는 하나 이상의 스위치에 keepalive 메시지가 전송되도록 하기 위해 클러스터 제어 링크의 모든 EtherChannel 인터페이스에서 대량의 keepalive 메시지를 보냅니다.

- (선택 사항) **Replicate console output to the master's console** — 슬레이브 유닛에서 마스터 유닛으로 콘솔 복제를 활성화합니다. 이 기능은 기본적으로 비활성화되어 있습니다. ASA에서는 중요한 특정 이벤트 발생 시 일부 메시지를 콘솔에 직접 출력합니다. 콘솔 복제를 활성화할 경우, 슬레이브 유닛에서는 콘솔 메시지를 마스터 유닛에 전송하므로 클러스터의 콘솔 포트 하나만 모니터링하면 됩니다. 이 매개변수는 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다.
- **Cluster Control Link** — 클러스터 제어 링크 인터페이스를 지정합니다. 이 인터페이스에는 구성된 이름이 올 수 없으며, 사용 가능한 인터페이스가 드롭다운 목록에 나와 있습니다.
  - **Interface** — 인터페이스 ID를 지정하며, EtherChannel이 권장됩니다. 하위 인터페이스 및 관리 유형 인터페이스는 허용되지 않습니다.
  - **IP Address** — IP 주소의 IPv4 주소를 지정합니다. 이 인터페이스에는 IPv6가 지원되지 않습니다.
  - **Subnet Mask** — 서브넷 마스크를 지정합니다.
  - (선택 사항) **MTU** — 클러스터 제어 링크 인터페이스의 최대 전송 단위를 지정하며 64에서 65,535바이트 사이로 설정합니다. MTU 값보다 큰 데이터는 전송 전에 분할됩니다. 기본 MTU는 1500바이트입니다. MTU는 1600바이트 이상으로 설정하는 것이 좋습니다. 이 경우 점보 프레임 예약을 활성화해야 합니다.

- (선택 사항) **Cluster LACP** — Spanned EtherChannel을 사용할 경우 ASA에서는 cLACP를 사용하여 EtherChannel과 인접 스위치의 협상을 수행합니다.클러스터의 ASA는 cLACP 협상 과정에서 협업을 수행하므로 스위치에 단일(가상) 디바이스로 표시됩니다.
  - **Enable static port priority** — LACP의 동적 포트 우선순위를 비활성화합니다. 일부 스위치에서는 동적 포트 우선순위를 지원하지 않으므로, 이 매개변수를 사용하면 스위치 호환성이 개선됩니다. 또한 이 명령을 사용하면 8개 이상의 활성 Spanned EtherChannel 멤버를 지원하는 것이 허용되므로 최대 32개의 멤버를 지원할 수 있습니다. 이 매개변수를 사용하지 않을 경우 8개의 활성 멤버 및 8개의 스탠바이 멤버만 지원됩니다. 이 매개변수를 활성화할 경우 스탠바이 멤버를 사용할 수 없으며 모든 멤버가 활성 상태로 됩니다. 이 매개변수는 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다.
  - **Virtual System MAC Address** — MAC 주소 형식으로 된 cLACP 시스템 ID를 설정합니다. 클러스터의 모든 ASA에서는 동일한 시스템 ID를 사용합니다. 이는 마스터 유닛에서 자동 생성되고(기본값) 모든 슬레이브에 복제됩니다. 또는 *H.H.H* 형식으로 수동으로 지정됩니다. 여기서 H는 16비트로 된 16진수를 의미합니다. 예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. 이 매개변수는 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다. 그러나 클러스터링을 활성화한 후에는 이 값을 변경할 수 없습니다.
  - **System Priority** — 시스템 우선순위를 1에서 65535까지의 범위 중에서 설정합니다. 우선순위는 번들링 결정을 담당할 유닛을 지정하는 데 사용됩니다. 기본적으로 ASA에서는 우선순위가 가장 높은 우선순위 1을 사용합니다. 우선순위는 스위치의 우선순위보다 높아야 합니다. 이 매개변수는 부트스트랩 컨피그레이션의 일부가 아니며, 마스터 유닛에서 슬레이브 유닛으로 복제됩니다. 그러나 클러스터링을 활성화한 후에는 이 값을 변경할 수 없습니다.

4단계 클러스터에 참가하려면 **Participate in ASA cluster** 확인란을 선택합니다.

5단계 **Apply**를 클릭합니다.

관련 주제

- 9-9 페이지의 인터페이스 모니터링
- 10-28 페이지의 점보 프레임 지원 활성화

마스터 유닛에서 새 슬레이브 추가

마스터 유닛을 통해 클러스터에 추가 슬레이브를 추가할 수 있습니다. High Availability and Scalability 마법사를 사용하여 슬레이브를 추가할 수도 있습니다. 마스터 유닛에서 슬레이브를 추가할 경우 클러스터 제어 링크를 구성하고, 추가하는 각 슬레이브 유닛에 클러스터 인터페이스 모드를 설정할 수 있다는 이점이 있습니다.

또는 슬레이브 유닛에 로그인하고 유닛에 직접 클러스터링을 구성할 수 있습니다. 그러나 클러스터링을 활성화한 후에는 ASDM 세션의 연결이 끊어지며 이를 다시 연결해야 합니다.

시작하기 전에

- 다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 아직 System 컨피그레이션 모드가 아닐 경우 Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.
- 관리 네트워크를 통해 부트스트랩 컨피그레이션을 전송하려면 슬레이브 유닛에 액세스 가능한 IP 주소가 있는지 확인합니다.

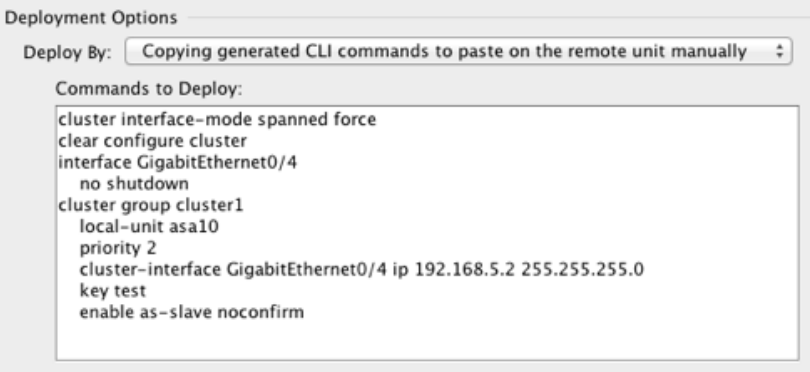
절차

1단계 **Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Members**를 선택합니다.

2단계 **Add**를 클릭합니다.

3단계 다음과 같은 매개변수를 구성합니다.

- **Member Name** — 이 클러스터 멤버의 이름을 1~38자로 된 ASCII 문자열로 지정합니다.
- **Member Priority** — 마스터 유닛 선택을 위해 이 유닛의 우선순위를 1에서 100까지 설정하며 1의 우선순위가 가장 높습니다.
- **Cluster Control Link > IP Address** — 클러스터 제어 링크(동일한 네트워크상의 마스터 클러스터 제어 링크)의 이 멤버에 고유한 IP 주소를 지정합니다.
- **Deployment Options** 영역에서 다음 **Deploy By** 옵션 중 하나를 선택합니다.
  - **Sending CLI commands to the remote unit now —** 부트스트랩 컨피그레이션을 슬레이브(임시) 관리 IP 주소로 보냅니다. 슬레이브 관리 IP 주소, 사용자 이름, 비밀번호를 입력합니다.
  - **Copying generated CLI commands to paste on the remote unit manually** — 명령을 생성하여 슬레이브 유닛 CLI에서 잘라내기/붙여넣기하거나 ASDM에서 CLI 툴을 사용합니다. Commands to Deploy 상자에서 생성된 명령을 선택 및 복사하여 나중에 사용할 수 있습니다.



4단계 **OK** 다음 **Apply**를 클릭합니다.

관련 주제

- 9-50 페이지의 ASA 클러스터 매개변수 구성

구성원 비활성화

클러스터의 컨피그레이션원을 비활성화하려면, 클러스터링 컨피그레이션은 그대로 유지한 상태로 유닛의 클러스터링을 비활성화합니다.

참고 ASA가 비활성화되면(수동으로 또는 상태 검사 오류를 통해) 모든 데이터 인터페이스가 종료되며, 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 다시 시작하려면 클러스터링을 다시 활성화합니다. 또는 클러스터에서 유닛을 모두 제거할 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드한 후에도 유닛이 클러스터 내에서 비활성 상태일 경우, 관리 인터페이스에서는 마스터 유닛과 동일한 기본 IP 주소를 사용하므로 관리 인터페이스에 액세스할 수 없습니다. 추가 컨피그레이션을 위해서는 콘솔 포트를 사용해야 합니다.

시작하기 전에

- 다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 현재 시스템 컨피그레이션 모드에 있지 않은Configuration > Device List 창의 액티브 디바이스 IP 주소 아래에서 **System**을 두 번 클릭하여 **changeto system** 명령을 입력합니다.

절차

1단계 **Configuration > Device Management > High Availability and Scalability > ASA Cluster**를 선택합니다.

클러스터에 디바이스가 이미 있고 마스터 유닛인 경우, 이 창이 Cluster Configuration 탭에 표시됩니다.

2단계 **Participate in ASA cluster** 확인란의 선택을 취소합니다.

참고 **Configure ASA cluster settings** 확인란의 선택을 취소하지 마십시오. 취소할 경우 모든 클러스터 컨피그레이션이 지워지며 ASDM이 연결된 모든 관리 인터페이스를 비롯한 모든 인터페이스도 종료됩니다. 이 경우 연결을 복원하려면 콘솔 포트의 CLI에 액세스해야 합니다.

3단계 **Apply**를 클릭합니다.

이 유닛이 마스터 유닛이었던 경우, 새 마스터가 선택되며 다른 멤버가 마스터 유닛이 됩니다.

클러스터 컨피그레이션은 그대로 유지되므로 클러스터링을 나중에 다시 활성화할 수 있습니다.

관련 주제

- 9-57 페이지의 클러스터 벗어나기

마스터 유닛의 슬레이브 구성원 비활성화

유닛에서 슬레이브 멤버를 비활성화하려면다음 단계를 수행합니다.

참고 ASA가 비활성화되면 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 다시 시작하려면 클러스터링을 다시 활성화합니다. 또는 클러스터에서 유닛을 모두 제거할 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 유닛으로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드한 후에도 유닛이 클러스터 내에서 비활성 상태일 경우, 관리 인터페이스에서는 마스터 유닛과 동일한 기본 IP 주소를 사용하므로 관리 인터페이스에 액세스할 수 없습니다. 추가 컨피그레이션을 위해서는 콘솔 포트를 사용해야 합니다.

시작하기 전에

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 현재 시스템 컨피그레이션 모드에 있지 않은Configuration > Device List 창의 액티브 디바이스 IP 주소 아래에서 **System**을 두 번 클릭하여 **changeto system** 명령을 입력합니다.

절차

1단계 클러스터에서 유닛을 제거합니다.

cluster remove unit *unit_name*

예:

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

부트스트랩 컨피그레이션뿐만 아니라 마스터 유닛에서 동기화된 최종 컨피그레이션도 그대로 유지되므로, 컨피그레이션이 손실되는 일 없이 유닛을 나중에 다시 추가할 수 있습니다. 슬레이브 유닛에 이 명령을 입력하여 마스터 유닛을 제거할 경우 새 마스터 유닛이 선택됩니다.

멤버 이름을 보려면 **cluster remove unit ?**을 입력하거나 **show cluster info** 명령을 입력합니다.

1단계 **Configuration > Device Management > High Availability and Scalability > ASA Cluster**를 선택합니다.

2단계 제거할 슬레이브를 선택하고 **Delete**를 클릭합니다.

슬레이브 부트스트랩 컨피그레이션이 그대로 유지되므로, 컨피그레이션이 손실되는 일 없이 슬레이브를 나중에 다시 추가할 수 있습니다.

3단계 **Apply**를 클릭합니다.

관련 주제

- 9-57 페이지의 클러스터 벗어나기

클러스터 벗어나기

클러스터를 모두 벗어나려는 경우, 전체 클러스터 부트스트랩 컨피그레이션을 제거해야 합니다. 각 컨피그레이션원에 대한 현재 컨피그레이션이 동일하므로(마스터 유닛에서 동기화됨), 클러스터를 벗어날 경우 백업에서 사전 클러스터링 컨피그레이션을 복원하거나, IP 주소 충돌을 피하려면 컨피그레이션을 지우고 처음부터 다시 시작하게 됩니다.

시작하기 전에

콘솔 포트를 사용해야 합니다. 클러스터 컨피그레이션을 제거하면 관리 인터페이스 및 클러스터 제어 링크를 비롯한 모든 인터페이스가 종료됩니다.

절차

1단계 슬레이브 유닛의 클러스터링을 비활성화합니다.

cluster group *cluster_name*
no enable

예:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

슬레이브 유닛에 클러스터링이 활성화되어 있는 동안에는 컨피그레이션을 변경할 수 없습니다.

2단계 클러스터 컨피그레이션을 지웁니다.

clear configure cluster

ASA에서는 관리 인터페이스 및 클러스터 제어 링크를 비롯한 모든 인터페이스를 종료합니다.

3단계 클러스터 인터페이스 모드를 비활성화합니다.

no cluster interface-mode

모드는 컨피그레이션에 저장되지 않으며 수동으로 재설정해야 합니다.

4단계 백업 컨피그레이션이 있을 경우, 실행 중인 컨피그레이션에 백업 컨피그레이션을 복사합니다.

copy *backup_cfg* **running-config**

예:

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

5단계 시작에 컨피그레이션을 저장합니다.

write memory

6단계 백업 컨피그레이션이 없는 경우 관리 액세스를 다시 컨피그레이션합니다. 인터페이스 IP 주소를 변경하고 이를테면 올바른 호스트 이름을 복원해야 합니다.

관련 주제

- 2 장, “시작하기”.

마스터 유닛 변경

주의 마스터 유닛을 변경하는 가장 좋은 방법은 마스터 유닛의 클러스터링을 비활성화한 후 새 마스터가 선택될 때까지 기다렸다가 클러스터링을 다시 활성화하는 것입니다. 마스터 유닛이 될 정확한 유닛을 지정해야 할 경우, 이 섹션을 절차를 사용하십시오. 그러나 중앙 집중식 기능의 경우 이 절차를 통해 마스터 유닛을 강제로 변경하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

마스터 유닛을 변경하려면 다음 단계를 수행하십시오.

시작하기 전에

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 현재 시스템 컨피그레이션 모드에 있지 않은Configuration > Device List 창의 액티브 디바이스 IP 주소 아래에서 **System**을 두 번 클릭하여 **changeto system** 명령을 입력합니다.

절차

1단계 **Monitoring > ASA Cluster > Cluster Summary**를 선택합니다.

2단계 **Change Master To** 드롭다운 목록에서 마스터 유닛이 될 슬레이브 유닛을 선택하고 **Make Master**를 클릭합니다.

3단계 마스터 유닛 변경을 확인하라는 메시지가 표시됩니다. **Yes**를 클릭합니다.

4단계 ASDM을 종료하고 기본 클러스터 IP 주소를 사용하여 다시 연결합니다.

관련 주제

- 9-55 페이지의 구성원 비활성화
- 9-25 페이지의 클러스터링을 위한 중앙 집중식 기능

클러스터 전체에 명령 실행

클러스터의 모든 멤버 또는 특정 멤버에 명령을 보내려면 다음 단계를 수행합니다. 모든 멤버에 **show** 명령을 보내면 모든 출력이 수집되고 해당 내용이 현재 유닛의 콘솔에 표시됩니다. **capture** 및 **copy** 같은 다른 명령의 경우 클러스터 전체 실행을 활용할 수도 있습니다.

시작하기 전에

Tools > Command Line Interface를 선택하여 Command Line Interface 툴에서 이 절차를 수행합니다.

절차

1단계 모든 멤버 또는 유닛 이름을 지정한 경우 특정 멤버에 명령을 전송합니다.

cluster exec [**unit** *unit_name*] *command*

예:

```
cluster exec show xlate
```

멤버 이름을 보려면 **cluster exec unit ?** 을 입력하거나(현재 유닛을 제외한 모든 이름을 보려는 경우), **show cluster info 정보** 명령을 입력합니다.

예

클러스터에 있는 모든 유닛의 동일한 캡처 파일을 TFTP 서버에 동시에 복사하려면 다음 명령을 마스터 유닛에 입력합니다.

```
cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

유닛당 하나씩인 여러 PCAP 파일이 TFTP 서버에 복사됩니다. 대상 캡처 파일의 이름 뒤에는 유닛 이름이 자동으로 연결되며 capture1_asa1.pcap, capture1_asa2.pcap 같은 형식이 됩니다. 이 예에서 asa1 및 asa2는 클러스터 유닛 이름 입니다.

cluster exec show port-channel 요약 명령에 대한 다음 샘플 출력에는 클러스터의 각 멤버에 대한 EtherChannel 정보가 나와 있습니다.

```
cluster exec show port-channel summary
primary(LOCAL):*************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP      Yes  Gi0/0(P)
2         Po2             LACP      Yes  Gi0/1(P)
 secondary:*********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+-----------+-----------------------------------------------
1         Po1             LACP      Yes   Gi0/0(P)
2         Po2             LACP      Yes   Gi0/1(P)
```

ASA 클러스터 모니터링

클러스터의 상태 및 연결을 모니터링하고 문제를 해결할 수 있습니다.

클러스터 상태 모니터링

클러스터 상태 모니터링에 대한 내용은 다음screens를 참조하십시오.

- **Monitoring > ASA Cluster > Cluster Summary**

  이 창에는 연결된 유닛에 대한 클러스터 정보 및 클러스터의 다른 유닛에 대한 정보가 표시됩니다. 이 창에서 마스터 유닛을 변경할 수도 있습니다.

- **Cluster Dashboard**

  마스터 유닛의 홈 페이지에서 Cluster Dashboard 및 Cluster Firewall Dashboard를 사용하여 클러스터를 모니터링할 수 있습니다.

관련 주제

- 3-24 페이지의 Cluster Dashboard 탭
- 3-26 페이지의 Cluster Firewall Dashboard 탭

클러스터 전체 패킷 캡처

클러스터의 패킷을 캡처하는 방법에 대한 내용은 다음screens를 참조하십시오.

Wizards > Packet Capture Wizard

클러스터 전체의 문제를 해결하기 위해을 사용하여 마스터 유닛에서 클러스터별 트래픽의 캡처를 활성화할 수 있습니다. 이 경우 클러스터의 모든 슬레이브 유닛에서 캡처가 자동으로 활성화됩니다.

관련 주제

- 39-1 페이지의 패킷 캡처 마법사로 캡처 구성 및 실행

클러스터 리소스 모니터링

클러스터 리소스 모니터링에 대한 내용은 다음screens를 참조하십시오.

- **Monitoring > ASA Cluster > System Resources Graphs > CPU**

  이 창을 사용하여 클러스터 전반의 CPU 사용률을 보여 주는 그래프 또는 표를 생성할 수 있습니다.

- **Monitoring > ASA Cluster > System Resources Graphs > Memory**. 이 창을 사용하여 클러스터 멤버 전반의 가용 메모리 및 사용한 메모리를 보여 주는 그래프 또는 표를 생성할 수 있습니다.

클러스터 트래픽 모니터링

클러스터 트래픽 모니터링에 대한 내용은 다음screens를 참조하십시오.

- **Monitoring > ASA Cluster > Traffic Graphs > Connections**.

  이 창을 사용하여 클러스터 전반의 연결을 보여 주는 그래프 또는 표를 생성할 수 있습니다.

- **Monitoring > ASA Cluster > Traffic Graphs > Throughput**.

  이 창을 사용하여 클러스터 전반의 트래픽 처리량을 보여 주는 그래프 또는 표를 생성할 수 있습니다.

클러스터 제어 링크 모니터링

클러스터 상태 모니터링에 대한 내용은 다음 화면을 참조하십시오.

Monitoring > Properties > System Resources Graphs > Cluster Control Link.

이 창을 사용하면 클러스터 제어 링크 수신 및 전송 용량 사용률을 보여 주는 그래프 또는 표를 생성할 수 있습니다.

클러스터링의 로깅 구성

클러스터링의 로깅 구성에 대한 내용은 다음screens를 참조하십시오.

Configuration > Device Management > Logging > Syslog Setup

클러스터의 각 유닛에서는 syslog 메시지를 독립적으로 생성합니다. 을 사용하면 디바이스 ID가 동일하거나 다른 syslog 메시지를 생성하여 클러스터의 동일한 또는 다른 유닛에서 메시지가 표시되도록 할 수 있습니다.

관련 주제

- 40-20 페이지의 디바이스 ID를 Non-EMBLEM 형식 Syslog 메시지에 포함

ASA 클러스터링의 예

이러한 예에는 일반적인 구축을 위한 모든 클러스터 관련 ASA 컨피그레이션이 포함되어 있습니다.

- 9-61 페이지의 샘플 ASA 및 스위치 구성
- 9-64 페이지의 단일화된 방화벽
- 9-66 페이지의 트래픽 분리
- 9-68 페이지의 백업 링크가 포함된 Spanned EtherChannel(기존 8 액티브 포트/8 스탠바이)

샘플 ASA 및 스위치 구성

다음 샘플 컨피그레이션에서는 ASA와 스위치 간에 다음과 같은 인터페이스를 연결합니다.

ASA Interface	Switch Interface
GigabitEthernet 0/2	GigabitEthernet 1/0/15
GigabitEthernet 0/3	GigabitEthernet 1/0/16
GigabitEthernet 0/4	GigabitEthernet 1/0/17
GigabitEthernet 0/5	GigabitEthernet 1/0/18

- 9-61 페이지의 ASA 구성
- 9-63 페이지의 Cisco IOS 스위치 구성

ASA 구성

각 유닛의 인터페이스 모드

```
cluster interface-mode spanned force
```

ASA1 마스터 부트스트랩 구성

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
```

```
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 10
 key emphyri0
 enable noconfirm
```

ASA2 슬레이브 부트스트랩 구성

```
interface GigabitEthernet0/0
 channel-group 1 mode on
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
 key emphyri0
 enable as-slave
```

마스터 인터페이스 구성

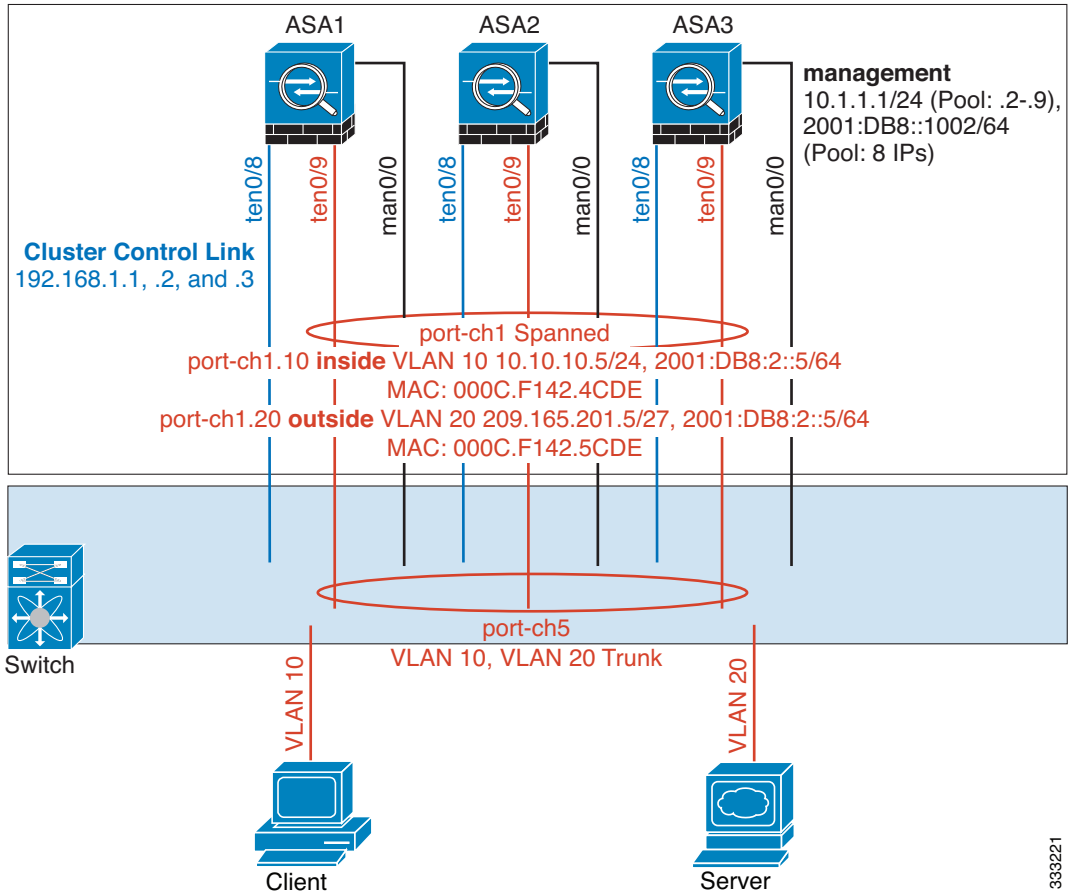
```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface GigabitEthernet0/2
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 10 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 11 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 11 mode active
 no shutdown
!
interface Management0/0
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
 no shutdown
!
interface Port-channel10
 port-channel span-cluster
```

```
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 port-channel span-cluster
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

Cisco IOS 스위치 구성

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access

interface Port-channel11
 switchport access vlan 401
 switchport mode access
```

단일화된 방화벽



서로 다른 보안 도메인의 데이터 트래픽은 서로 다른 VLAN에 연결됩니다. 예를 들어, VLAN 10은 내부 네트워크용이고 VLAN 20은 외부 네트워크용입니다. 각 ASA에는 외부 스위치 또는 라우터에 연결된 하나의 물리적 포트가 있습니다. 트렁킹이 활성화되어 있으므로 물리적 링크의 모든 패킷은 캡슐화된 802.1q입니다. ASA는 VLAN 10과 VLAN 20 사이의 방화벽입니다.

Spanned EtherChannel을 사용할 경우, 모든 데이터 링크가 스위치 측의 단일한 EtherChannel로 그룹화됩니다. ASA를 사용할 수 없게 될 경우, 스위치에서 나머지 유닛 간의 트래픽을 재밸런싱합니다.

각 유닛의 인터페이스 모드

```
cluster interface-mode spanned force
```

ASA1 마스터 부트스트랩 구성

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa1
    cluster-interface tengigabitethernet0/8 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 슬레이브 부트스트랩 구성

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface tengigabitethernet0/8 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

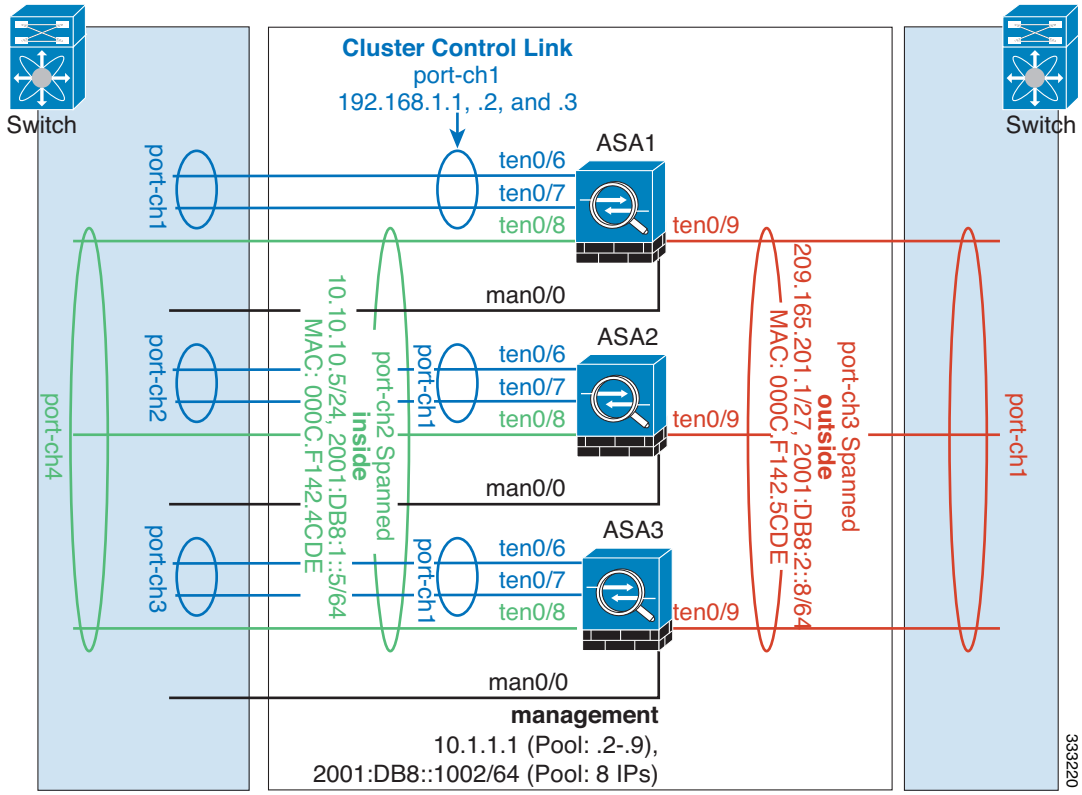
ASA3 슬레이브 부트스트랩 구성

```
interface tengigabitethernet 0/8
    no shutdown
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface tengigabitethernet0/8 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

마스터 인터페이스 구성

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/9
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    port-channel span-cluster
interface port-channel 2.10
    vlan 10
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    ipv6 address 2001:DB8:1::5/64
    mac-address 000C.F142.4CDE
interface port-channel 2.20
    vlan 20
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    ipv6 address 2001:DB8:2::8/64
    mac-address 000C.F142.5CDE
```

트래픽 분리



내부 네트워크와 외부 네트워크 간의 트래픽을 물리적으로 분리하고자 할 수 있습니다.

위의 다이어그램에 표시된 것과 같이, 왼쪽에는 내부 스위치에 연결되는 Spanned EtherChannel이 하나 있고 오른쪽에는 외부 스위치에 연결되는 Spanned EtherChannel이 있습니다. 필요한 경우 각 EtherChannel에 VLAN 하위 인터페이스를 생성할 수도 있습니다.

각 유닛의 인터페이스 모드

```
cluster interface-mode spanned force
```

ASA1 마스터 부트스트랩 구성

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 슬레이브 부트스트랩 구성

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

ASA3 슬레이브 부트스트랩 구성

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

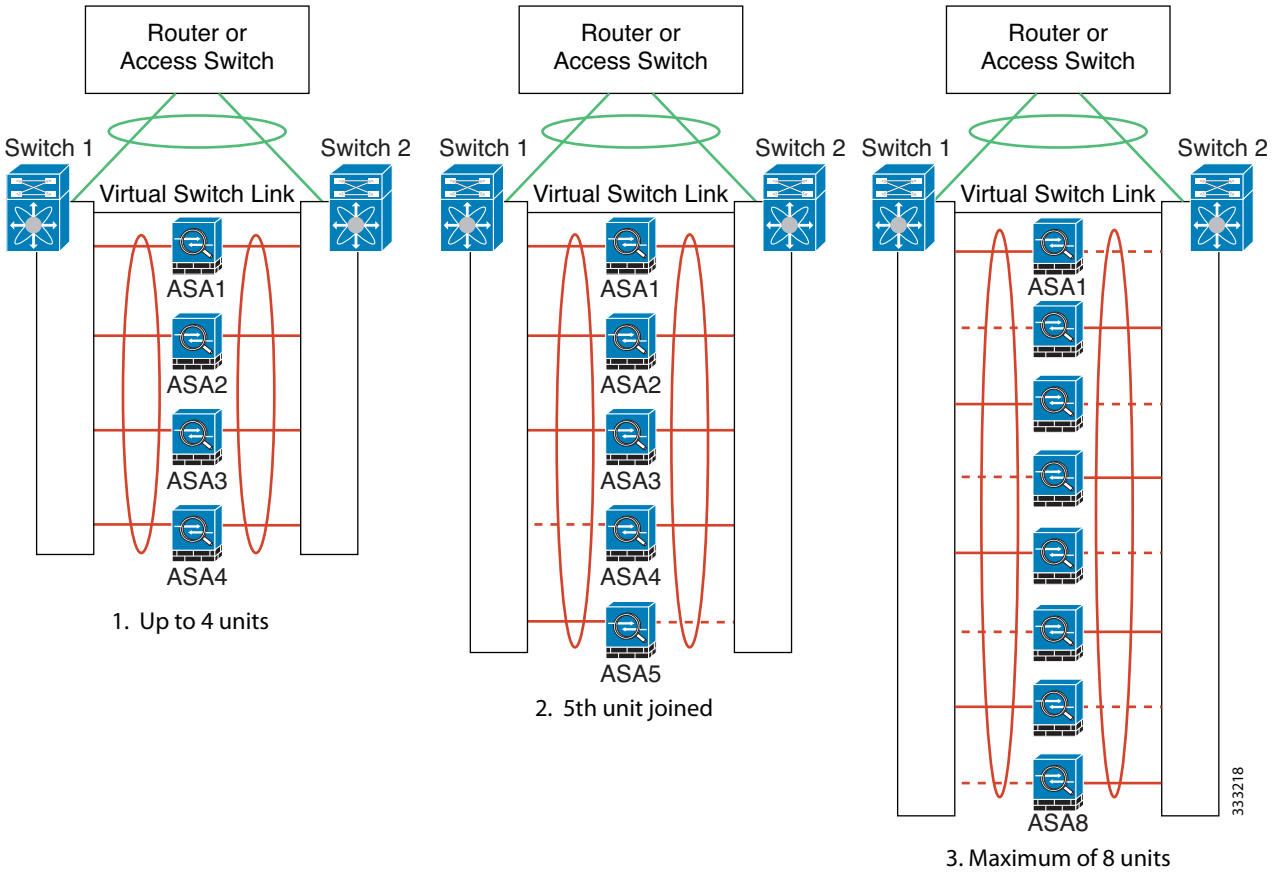
마스터 인터페이스 구성

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
    security-level 100
    management-only
    no shutdown

interface tengigabitethernet 0/8
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    port-channel span-cluster
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    ipv6 address 2001:DB8:1::5/64
    mac-address 000C.F142.4CDE

interface tengigabitethernet 0/9
    channel-group 3 mode active
    no shutdown
```

```
interface port-channel 3
    port-channel span-cluster
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    ipv6 address 2001:DB8:2::8/64
    mac-address 000C.F142.5CDE
```

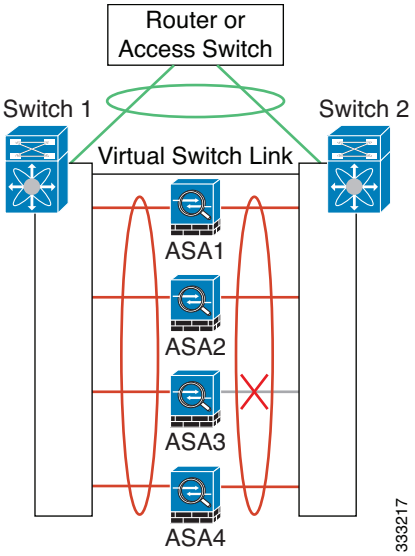
백업 링크가 포함된 Spanned EtherChannel(기존 8 액티브 포트/8 스탠바이)

기존 EtherChannel에서 활성 포트의 최대 개수는 스위치 측에서 8개로 제한됩니다. 8-ASA 클러스터가 있을 경우 유닛당 2개의 포트를 EtherChannel에 할당하며, 이렇게 하면 총 16개의 전체 포트 중 8개는 스탠바이 모드가 되어야 합니다. ASA에서는 LACP를 사용하여 어떤 링크를 활성화하거나 스탠바이 상태로 설정해야 하는지 협상을 수행합니다. VSS 또는 vPC를 사용하여 다중 스위치 EtherChannel을 활성화할 경우 스위치 간 이중화를 실현할 수 있습니다. ASA의 모든 물리적 포트는 우선 슬롯 번호를 기준으로, 그 다음에는 포트 번호를 기준으로 순서가 지정됩니다. 다음 그림에서 순서가 낮은 포트가 "기본" 포트(예: GigabitEthernet 0/0)이고, 다른 포트가 "보조" 포트(예: GigabitEthernet 0/1)입니다. 하드웨어 연결은 대칭을 이루어야 합니다. 모든 기본 링크는 하나의 스위치에서 종료되어야 하며, 모든 보조 링크는 VSS/vPC가 사용된 경우 다른 스위치에서 종료되어야 합니다. 다음 다이어그램에서는 클러스터에 참가하는 유닛의 수가 증가하여 링크의 총 개수가 증가할 경우 어떤 상황이 발생하는지 보여 줍니다.

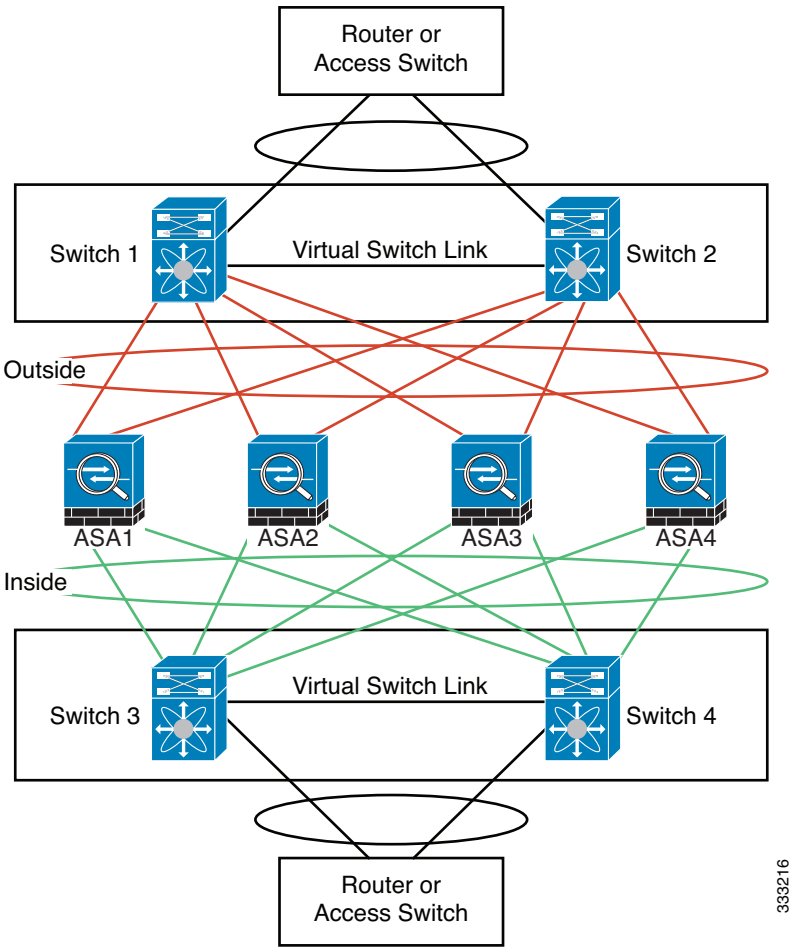


원칙적으로는 우선 채널에 있는 활성 포트의 수를 최대화하고, 그 다음에는 활성 기본 포트의 수와 활성 보조 포트의 수가 균형을 이루도록 유지하는 것입니다. 클러스터에 5번째 유닛이 참가할 경우 모든 유닛 간의 트래픽이 균일하게 조정되지 않습니다.

링크 또는 디바이스 오류는 이와 동일한 원칙에 따라 처리됩니다. 또한 완벽하지 않은 로드 밸런싱 상황에 처하게 될 수 있습니다. 다음 그림에는 유닛 중 하나에 단일 링크 오류가 발생한 4-유닛 클러스터가 나와 있습니다.



네트워크에는 여러 개의 EtherChannel이 구성될 수 있습니다. 다음 다이어그램에는 내부의 EtherChannel과 외부의 EtherChannel이 나와 있습니다. 한쪽 EtherChannel의 기본 및 보조 링크에 모두 오류가 발생할 경우 클러스터에서 ASA가 제거됩니다. 이렇게 되면 외부 네트워크와 내부 네트워크의 연결이 이미 끊긴 경우, 외부 네트워크의 트래픽이 ASA에 전달되지 않습니다.



각 유닛의 인터페이스 모드

```
cluster interface-mode spanned force
```

ASA1 마스터 부트스트랩 구성

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL
```

```
cluster group cluster1
    local-unit asa1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    enable noconfirm
```

ASA2 슬레이브 부트스트랩 구성

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa2
    cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
    priority 2
    key chuntheunavoidable
    enable as-slave
```

ASA3 슬레이브 부트스트랩 구성

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa3
    cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
    priority 3
    key chuntheunavoidable
    enable as-slave
```

ASA4 슬레이브 부트스트랩 구성

```
interface tengigabitethernet 0/6
    channel-group 1 mode on
    no shutdown
```

```
interface tengigabitethernet 0/7
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/8
    channel-group 1 mode on
    no shutdown
interface tengigabitethernet 0/9
    channel-group 1 mode on
    no shutdown
interface port-channel 1
    description CCL

cluster group cluster1
    local-unit asa4
    cluster-interface port-channel1 ip 192.168.1.4 255.255.255.0
    priority 4
    key chuntheunavoidable
    enable as-slave
```

마스터 인터페이스 구성

```
ip local pool mgmt 10.1.1.2-10.1.1.9

interface management 0/0
    channel-group 2 mode active
    no shutdown
interface management 0/1
    channel-group 2 mode active
    no shutdown
interface port-channel 2
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    security-level 100
    management-only

interface tengigabitethernet 1/6
    channel-group 3 mode active vss-id 1
    no shutdown
interface tengigabitethernet 1/7
    channel-group 3 mode active vss-id 2
    no shutdown
interface port-channel 3
    port-channel span-cluster vss-load-balance
    nameif inside
    ip address 10.10.10.5 255.255.255.0
    mac-address 000C.F142.4CDE

interface tengigabitethernet 1/8
    channel-group 4 mode active vss-id 1
    no shutdown
interface tengigabitethernet 1/9
    channel-group 4 mode active vss-id 2
    no shutdown
interface port-channel 4
    port-channel span-cluster vss-load-balance
    nameif outside
    ip address 209.165.201.1 255.255.255.224
    mac-address 000C.F142.5CDE
```

ASA 클러스터링에 대한 기록

기능 이름	플랫폼 릴리스	기능 정보
ASA 5580 및 5585-X를 위한 ASA 클러스터링	9.0(1)	ASA 클러스터링을 사용하면 여러 개의 ASA를 하나의 논리적 디바이스로 그룹화할 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다. ASA 클러스터링은 ASA 5580 및 ASA 5585-X를 지원합니다. 클러스터의 모든 유닛은 동일한 하드웨어 사양을 갖춘 동일한 모델이어야 합니다. 클러스터링이 활성화된 경우, 지원되지 않는 기능에 대한 목록은 컨피그레이션 설명서를 참조하십시오. 다음 화면을 도입했거나 수정했습니다. Home > Device Dashboard Home > Cluster Dashboard Home > Cluster Firewall Dashboard Configuration > Device Management > Advanced > Address Pools > MAC Address Pools Configuration > Device Management > High Availability and Scalability > ASA Cluster Configuration > Device Management > Logging > Syslog Setup > Advanced Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced Configuration > Device Setup > Interfaces > Add/Edit Interface > IPv6 Configuration > Device Setup > Interfaces > Add/Edit EtherChannel Interface > Advanced Configuration > Firewall > Advanced > Per-Session NAT Rules Monitoring > ASA Cluster Monitoring > Properties > System Resources Graphs > Cluster Control Link Tools > Preferences > General Tools > System Reload Tools > Upgrade Software from Local Computer Wizards > High Availability and Scalability Wizard Wizards > Packet Capture Wizard Wizards > Startup Wizard
ASA 5500-X support for clustering	9.1(4)	이제 ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X에서는 2-유닛 클러스터를 지원합니다. 유닛 2개의 클러스터링은 Base 라이센스에서 기본적으로 활성화되어 있으며, ASA 5512-X의 경우 Security Plus 라이센스가 필요합니다. ASDM 화면은 수정하지 않았습니다.

기능 이름	플랫폼 릴리스	기능 정보
VSS 및 vPC의 상태 검사 모니터링 지원 개선	9.1(4)	클러스터 제어 링크를 EtherChannel로 구성하고(권장) 이를 VSS 또는 vPC 쌍에 연결한 경우, 이제 상태 검사 모니터링 기능을 통해 안정성을 높일 수 있습니다. Cisco Nexus 5000과 같은 일부 스위치의 경우 VSS/vPC에서 유닛 하나가 중단되거나 부팅되면 해당 스위치에 연결된 EtherChannel 멤버 인터페이스가 ASA에 대해 가동되는 것으로 표시되지만, 스위치 측의 트래픽을 통과하지 않습니다. ASA 대기 시간 제한을 낮은 값으로 설정한 경우(0.8초) 클러스터에서 ASA가 잘못 제거될 수 있으며 ASA에서는 이러한 EtherChannel 인터페이스 중 하나에 keepalive 메시지를 보냅니다. VSS/vPC 상태 검사 기능을 활성화할 경우, ASA에서는 하나 이상의 스위치에 keepalive 메시지가 전송되도록 하기 위해 클러스터 제어 링크의 모든 EtherChannel 인터페이스에서 대량의 keepalive 메시지를 보냅니다. 다음 화면을 수정했습니다. **Configuration > Device Management > High Availability and Scalability > ASA Cluster**
지리적으로 다른 위치(사이트 간)에 있는 클러스터 멤버 지원(개별 인터페이스 모드 전용)	9.1(4)	이제 개별 인터페이스 모드를 사용할 경우 지리적으로 다른 위치에 클러스터 멤버를 배치할 수 있습니다. ASDM 화면은 수정하지 않았습니다.
투명 모드의 경우 지리적으로 다른 위치(사이트 간)에 있는 클러스터 멤버 지원	9.2(1)	이제 투명 방화벽 모드에서 Spanned EtherChannel 모드를 사용할 경우 지리적으로 다른 위치에 클러스터 멤버를 배치할 수 있습니다. 라우팅 방화벽 모드에서 Spanned EtherChannel을 사용한 사이트 간 클러스터링은 지원되지 않습니다. ASDM 화면은 수정하지 않았습니다.
클러스터링을 위한 고정 LACP 포트 우선순위 지원	9.2(1)	일부 스위치에서는 LACP를 통한 동적 포트 우선순위를 지원하지 않습니다(활성 및 스탠바이 링크). 이제 동적 포트 우선순위를 사용하지 않도록 설정하여 Spanned EtherChannel과의 호환성을 향상할 수 있습니다. 또한 다음 지침을 따라야 합니다. • 클러스터 제어 링크 경로의 네트워크 요소에서는 L4 체크섬을 확인하지 않습니다. 클러스터 제어 링크를 통해 리디렉션된 트래픽에는 올바른 L4 체크섬이 없습니다. L4 체크섬을 확인하는 스위치의 경우 트래픽이 감소하는 결과를 초래할 수 있습니다. • 포트 채널 번들링 다운타임은 구성된 keepalive 기간을 초과하면 안 됩니다. 다음 화면을 수정했습니다. **Configuration > Device Management > High Availability and Scalability > ASA Cluster**

기능 이름	플랫폼 릴리스	기능 정보
Spanned EtherChannel에서 32개의 활성 링크 지원	9.2(1)	이제 ASA EtherChannel에서는 최대 16개의 활성 링크를 지원합니다. *Spanned* EtherChannel까지 활용하면 vPC에서 2개의 스위치를 함께 사용할 경우, 그리고 동적 포트 우선순위를 비활성화할 경우 클러스터 전체에서 최대 32개의 활성 링크를 지원하도록 이 기능을 확장할 수 있습니다. 스위치에서는 16개의 활성 링크가 포함된 EtherChannel(예: F2-Series 10기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000)을 지원해야 합니다. VSS 또는 vPC에서 8개의 활성 링크를 지원하는 스위치를 사용하려는 경우, 이제 Spanned EtherChannel에 16개의 활성 링크를 구성하면 됩니다(각 스위치에 8개씩 연결됨). 이전에는 VSS/vPC와 함께 사용해도 Spanned EtherChannel에서 8개의 활성 링크, 8개의 스탠바이 링크만 지원되었습니다. **참고** Spanned EtherChannel에서 활성 링크를 8개 이상 사용하려는 경우 스탠바이 링크까지 보유할 수는 없습니다. 활성 링크를 9~32개까지 지원하려면 스탠바이 링크의 사용을 허용하는 cLACP 동적 포트 우선순위를 비활성화해야 합니다. 다음 화면을 수정했습니다. **Configuration > Device Management > High Availability and Scalability > ASA Cluster**
ASA 5585-X에 클러스터 멤버 16개 지원	9.2(1)	이제 ASA 5585-X에서는 16-유닛 클러스터를 지원합니다. ASDM 화면은 수정하지 않았습니다.
ASA 클러스터링을 위한 BGP 지원	9.3(1)	ASA 클러스터링에서 BGP 지원을 추가했습니다. 다음 ASDM 화면을 수정했습니다. **Configuration > Device Setup > Routing > BGP > IPv4 Family > General**

파 트 3

인터페이스

10 장

기본 인터페이스 구성(ASA 5512-X 이상)

이 장에는 이더넷 설정, 이중화 인터페이스, EtherChannel을 비롯한 Cisco ASA 5512-X 이상 버전의 인터페이스 컨피그레이션을 시작하는 작업에 대한 내용이 포함되어 있습니다.

참고 다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 모든 작업을 완료합니다. 시스템 실행 영역에 있지 않은 경우 Configuration > Device List 창에서 액티브 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.

특수한 요구 사항을 충족해야 하는 ASA 클러스터 인터페이스에 대한 내용은 9 장, “ASA 클러스터”. 를 참조하십시오.

ASA 5512-X 이상 버전의 인터페이스 구성 시작에 대한 정보

자동 MDI/MDIX 기능

RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 자동 MDI/MDIX 기능도 포함됩니다. 자동 MDI/MDIX 기능을 사용하면 자동 협상 단계에서 직선형 케이블이 감지될 경우 내부 crossover를 수행하게 되므로 crossover 케이블을 연결할 필요가 없습니다. 자동 협상을 실행하여 인터페이스에 자동 MDI/MDIX 기능을 활성화하려면 속도 또는 양방향을 설정해야 합니다. 속도 및 양방향을 모두 명시적인 고정 값으로 설정할 경우, 두 설정에 대한 자동 협상이 비활성화되며 자동 MDI/MDIX 기능도 비활성화됩니다. 기가비트 인터넷의 경우 속도와 양방향을 1000 및 최대로 설정할 경우, 인터페이스에서 항상 자동 협상이 실행되므로 자동 MDI/MDIX 기능도 활성화되며 이를 비활성화할 수 없습니다.

투명 모드의 인터페이스

투명 모드의 인터페이스는 "브릿지 그룹"에 속하며, 각 네트워크에 하나의 브릿지 그룹이 있습니다. 각 컨텍스트당 또는 단일 모드에서 인터페이스 4개당 최대 8개의 브릿지가 포함될 수 있습니다. 브릿지 그룹에 대한 자세한 내용은 13-1 페이지의 투명 모드의 브리지 그룹를 참조하십시오.

관리 인터페이스

관리 인터페이스 개요

다음에 연결하여 ASA를 관리할 수 있습니다.

- 통과 트래픽 인터페이스
- 전용 관리 *슬롯/포트* 인터페이스(모델에 제공되는 경우)

36 장, “관리 액세스”.에 따라 인터페이스에 대한 관리 액세스를 구성해야 할 수 있습니다.

관리 *슬롯/포트* 인터페이스

표 10-1에는 모델당 관리 인터페이스가 나와 있습니다.

표 10-1 모델당 관리 인터페이스

모델	Management 0/0[1]	Management 0/1	Management 1/0	Management 1/1	통과 트래픽의 구성 가능 요소[2]	하위 인터페이스 허용 여부
ASA 5512-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5515-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5525-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5545-X	예	아니요	아니요	아니요	아니요	아니요

표 10-1 모델당 관리 인터페이스 (계속)

모델	Management 0/0[1]	Management 0/1	Management 1/0	Management 1/1	통과 트래픽의 구성 가능 요소[2]	하위 인터페이스 허용 여부
ASA 5555-X	예	아니요	아니요	아니요	아니요	아니요
ASA 5585-X	예	예	예[3]	예[3]	예	예
ASASM	아니요	아니요	아니요	아니요	N/A	N/A
ASAv	예	아니요	아니요	아니요	아니요	아니요

1. Management 0/0 인터페이스는 기본 공장 컨피그레이션에 포함되어 ASDM 액세스를 위해 컨피그레이션됩니다. 자세한 내용은 2-15 페이지의 공장 기본 구성를 참조하십시오.
2. 기본적으로 Management 0/0 인터페이스는 관리 전용 트래픽을 위해 구성됩니다. 라우팅 모드에서 지원되는 모델의 경우, 제한 사항을 제거하고 통과 트래픽을 전달할 수 있습니다. 모델이 추가 관리 인터페이스가 포함될 경우 이를 통과 트래픽에도 사용할 수 있습니다. 단, 관리 인터페이스가 통과 트래픽에 최적화되어 있지 않을 수 있습니다.
3. 슬롯 1에 SSP가 설치된 경우 Management 1/0 및 1/1에서는 슬롯 1의 SSP에만 관리 액세스를 제공합니다.

참고 모듈을 설치한 경우, 모듈 관리 인터페이스에서는 해당 모듈에만 관리 액세스를 제공합니다. ASA 5512-X부터 ASA 5555-X 버전까지 소프트웨어 모듈에서 사용하는 물리적 Management 0/0 인터페이스는 ASA와 동일합니다.

관리 전용 트래픽에 모든 인터페이스 사용

모든 인터페이스를 관리 트래픽용으로 구성하여 이를 관리 전용 인터페이스로 사용할 수 있으며 여기에는 EtherChannel 인터페이스가 포함됩니다.

투명 모드의 관리 인터페이스

투명 방화벽 모드에서는 최대 허용되는 통과 트래픽 인터페이스 외에도, 관리 인터페이스(물리적 인터페이스 또는 하위 인터페이스(모델에서 지원되는 경우) 또는 여러 개의 관리 인터페이스로 구성된 EtherChannel 인터페이스(관리 인터페이스가 여러 개인 경우))를 별도의 관리 인터페이스로 사용할 수 있습니다. 다른 기타 인터페이스 유형은 관리 인터페이스로 사용할 수 없습니다.

다중 컨텍스트 모드에서는 관리 인터페이스를 비롯하여 어떤 인터페이스도 여러 컨텍스트에서 공유할 수 없습니다. 컨텍스트별 관리를 위해 관리 인터페이스의 하위 인터페이스를 만들고 각 컨텍스트에 관리 하위 인터페이스를 할당할 수 있습니다. ASA 5512-X부터 ASA 5555-X까지는 관리 인터페이스에서 하위 인터페이스를 지원하지 않습니다. 따라서 컨텍스트별 관리를 위해서는 데이터 인터페이스에 연결해야 합니다.

관리 인터페이스는 일반적인 브릿지 그룹에 포함되지 않습니다. 운영상의 용도로 인해 관리 인터페이스는 구성 불가능한 브릿지 그룹에 포함됩니다.

참고 투명 방화벽 모드의 경우 관리 인터페이스에서는 MAC 주소 테이블을 데이터 인터페이스와 같은 방식으로 업데이트합니다. 따라서 스위치 포트 중 하나를 라우팅 포트로 구성하지 않는 한 관리 인터페이스와 데이터 인터페이스 두 가지 모두를 같은 스위치에 연결해서는 안 됩니다(기본적으로 Catalyst 스위치에서는 모든 VLAN 스위치 포트에 대한 MAC 주소를 공유함). 그렇지 않을 경우 트래픽이 물리적으로 연결된 스위치에서 관리 인터페이스에 전달되면 ASA에서는 데이터 인터페이스 대신 *관리* 인터페이스를 사용하여 스위치에 액세스하도록 액세스 MAC 주소 테이블을 업데이트합니다. 이 작업으로 인해 일시적인 트래픽 중단이 발생합니다. ASA에서는 보안상의 이유로 인해 스위치에서 데이터 인터페이스로 전달되는 패킷의 MAC 주소 테이블을 최소 30초간 다시 업데이트하지 않습니다.

이중화 관리 인터페이스 미지원

이중 인터페이스는 관리 *슬롯/포트* 인스턴스를 멤버로 지원하지 않습니다. 또한 비 관리 인터페이스가 포함된 이중 인터페이스를 관리 전용으로 설정할 수 없습니다.

ASA 5512-X~ASA 5555-X의 Management 0/0 인터페이스

ASA 5512-X부터 ASA 5555-X 버전까지 Management 0/0 인터페이스의 특징은 다음과 같습니다.

- 통과 트래픽을 지원하지 않음
- 하위 인터페이스를 지원하지 않음
- 우선순위 대기열을 지원하지 않음
- 멀티캐스트 MAC을 지원하지 않음
- 소프트웨어 모듈에서는 Management 0/0 인터페이스를 공유합니다. ASA 및 모듈에서는 별도의 MAC 주소와 IP 주소가 지원됩니다. 모듈 운영 체제 내에서 모듈 IP 주소의 컨피그레이션을 수행해야 합니다. 그러나 물리적 특성(예: 인터페이스 활성화)은 ASA에서 구성됩니다.

이중화 인터페이스

논리적 이중화 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중화 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중화 인터페이스와 함께 디바이스 수준 장애 조치를 구성할 수 있습니다.

이중화 인터페이스 MAC 주소

이중화 인터페이스에서는 맨 처음 추가되는 물리적 인터페이스의 MAC 주소를 사용합니다. 컨피그레이션에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 또는 멤버 인터페이스 MAC 주소에 관계없이 사용되는 이중화 인터페이스에 MAC 주소를 할당할 수 있습니다(12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성 또는 7-15 페이지의 다중 컨텍스트 모드 구성 참조). 액티브 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작하면 같은 MAC 주소가 유지되므로 트래픽이 중단되지 않습니다.

EtherChannel

802.3ad EtherChannel은 개별 이더넷 링크(채널 그룹)의 번들로 구성된 논리적 인터페이스(일명 포트 채널 인터페이스)이므로, 단일 네트워크의 대역폭을 늘리게 됩니다. 포트 채널 인터페이스는 인터페이스 관련 기능을 구성할 경우 물리적 인터페이스와 동일한 방식으로 사용됩니다.

최대 48개의 EtherChannel을 구성할 수 있습니다.

- 10-5 페이지의 채널 그룹 인터페이스
- 10-5 페이지의 다른 디바이스에서 EtherChannel에 연결
- 10-6 페이지의 Link Aggregation Control Protocol
- 10-6 페이지의 로드 밸런싱
- 10-7 페이지의 EtherChannel MAC 주소

채널 그룹 인터페이스

각 채널 그룹에는 최대 16개의 액티브 인터페이스를 포함할 수 있습니다. 액티브 인터페이스를 8개만 지원하는 스위치의 경우, 채널 그룹 하나에 최대 16개의 인터페이스를 할당할 수 있습니다. 이 중 8개만 액티브 인터페이스가 될 수 있으며, 나머지 인터페이스는 인터페이스 오류에 대비하여 스탠바이 링크 역할을 수행할 수 있습니다. 16개의 액티브 인터페이스를 사용하려는 경우 스위치에서 해당 기능을 지원하는지 확인하십시오(예: F2-Series 10기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000).

채널 그룹의 모든 인터페이스는 유형과 속도가 같아야 합니다. 채널 그룹에 추가된 첫 번째 인터페이스에서는 올바른 유형과 속도를 결정합니다.

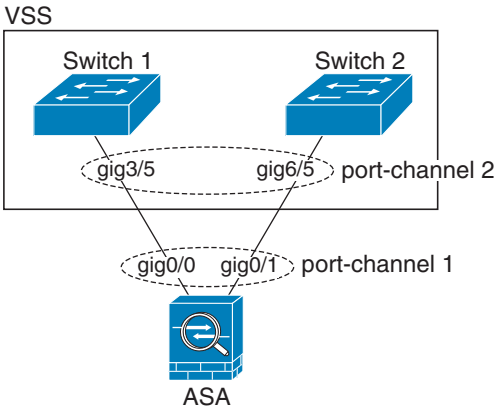
EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 소스 또는 목적지 MAC 주소, IP 주소, TCP 및 UDP 포트 번호, VLAN 번호를 기준으로 전용 해시 알고리즘을 사용하여 인터페이스를 선택합니다.

다른 디바이스에서 EtherChannel에 연결

ASA EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다. 예를 들어, Catalyst 6500 스위치 또는 Cisco Nexus 7000에 연결할 수 있어야 합니다.

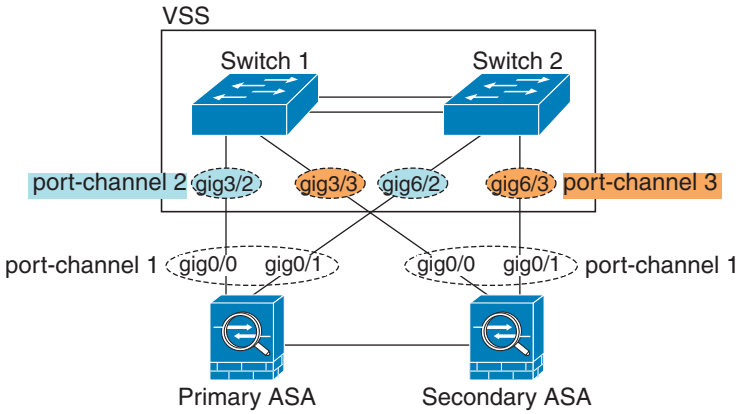
스위치가 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel)의 일부인 경우, 동일한 EtherChannel 내에서 ASA 인터페이스를 연결하여 VSS/vPC에서 스위치를 분리할 수 있습니다. 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버이므로 별도의 스위치는 단일 스위치 역할을 합니다(그림 10-1 참조).

그림 10-1 VSS/vPC에 연결



액티브/스탠바이 장애 조치 구축 시 ASA를 사용할 경우 VSS/vPC의 스위치에 각 ASA에 별도의 EtherChannel을 생성해야 합니다.(그림 10-1 참조). 각 ASA에서 단일한 EtherChannel은 두 스위치에 모두 연결됩니다. 모든 스위치 인터페이스를 ASA에 연결된 단일 EtherChannel으로 그룹화하는 것은 가능하지만(이 경우 별도의 ASA 시스템 ID로 인해 EtherChannel이 설정되지 않음), 스탠바이 ASA로 트래픽이 전송되는 것은 바람직하지 않으므로 단일 EtherChannel은 권장되지 않습니다.

그림 10-2 액티브/스탠바이 장애 조치 및 VSS/vPC



Link Aggregation Control Protocol

LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel의 각 물리적 인터페이스를 다음과 같이 구성할 수 있습니다.

- Active — LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- 패시브 — LACP 업데이트를 받습니다. 액티브 EtherChannel에서는 액티브 EtherChannel과의 연결만 설정할 수 있습니다.
- On — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 또 다른 "on" 상태의 EtherChannel과의 연결만 설정할 수 있습니다.

LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 컨피그레이션 오류를 처리하고 컨피그레이션원 인터페이스의 끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 컨피그레이션이 확인되지 않습니다.

로드 밸런싱

ASA에서는 패킷의 소스 및 목적지 IP 주소를 해싱하여 EtherChannel의 인터페이스에 패킷을 분산시킵니다(이 조건은 구성 가능하며 10-22 페이지의 EtherChannel 맞춤화를 참조하십시오). 결과의 나머지 부분에 따라 흐름을 보유하는 인터페이스가 결정되는 모듈로 작업의 액티브 링크 수를 기준으로 결과 해시가 분할됩니다. *hash_value* **mod** *active_links*의 결과가 0인 모든 패킷은 EtherChannel의 첫 번째 인터페이스가 되고, 결과가 1인 패킷은 두 번째 인터페이스, 결과가 2인 패킷은 세 번째 인터페이스 등으로 이어집니다. 예를 들어, 액티브 링크가 15개 있는 경우 모듈로 작업에서는 0에서 14까지의 값을 제공합니다. 액티브 링크가 6개인 경우 해당 값은 0~5가 되며, 이런 식으로 계속 적용할 수 있습니다.

클러스터링에서 Spanned EtherChannel의 경우 ASA 단위로 로드 밸런싱이 이루어집니다. 예를 들어, 8개의 ASA 전체에서 Spanned EtherChannel에 32개의 액티브 인터페이스가 있는 경우 EtherChannel의 ASA 하나당 인터페이스는 4개이며 ASA의 4개 인터페이스에만 로드 밸런싱이 실행됩니다.

액티브 인터페이스가 중단되고 스탠바이 인터페이스로 대체되지 않을 경우, 나머지 링크 간의 트래픽이 다시 밸런싱됩니다. 오류는 레이어 2의 스패닝 트리와 레이어 3의 라우팅 테이블에서 모두 마스킹되므로, 전환 작업은 다른 네트워크 디바이스에 투명하게 이루어집니다.

EtherChannel MAC 주소

채널 그룹의 일부인 모든 인터페이스에서는 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다.

포트-채널 인터페이스는 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 직접 구성할 수도 있습니다. 다중 컨텍스트 모드에서는 EtherChannel 포트 인터페이스를 비롯한 인터페이스에 고유한 MAC 주소를 자동으로 지정할 수 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우에 대비하여 직접 또는 다중 컨텍스트 모드라면 자동으로 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널 MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그 다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.

MTU 및 TCP 최대 세그먼트 크기로 조각화 제어

MTU 개요

MTU에서는 ASA가 지정된 이더넷 인터페이스에서 전송할 수 있는 최대 프레임 페이로드 크기를 지정합니다. MTU 값은 이더넷 헤더, FCS 또는 VLAN 태깅이 *없는* 프레임 크기입니다. 이더넷 헤더는 14바이트이고 FCS는 4바이트입니다. MTU를 1500으로 설정할 경우 예상 프레임 크기는 헤더를 포함하여 1518바이트입니다. VLAN 태깅(4바이트가 더 추가됨)을 사용 중인 상태에서 MTU를 1500으로 설정할 경우 예상 프레임 크기는 1522입니다. 이러한 헤더를 수용하기 위해 MTU 값을 이보다 더 높게 설정하지 마십시오. MTU 설정을 변경하는 대신 MTU 최대 세그먼트 크기를 변경하여 캡슐화를 위한 TCP 헤더를 수용하는 방법에 대한 자세한 내용은 10-8 페이지의 TCP 최대 세그먼트 크기 개요를 참조하십시오.

발신 IP 패킷이 지정된 MTU보다 큰 경우 해당 패킷은 2개 이상의 프레임으로 분할됩니다. 분할된 패킷은 목적지(또는 일부 경우 중간 홉에서)에서 다시 합쳐지며, 분할이 일어날 경우 성능이 저하될 수 있습니다. 따라서 분할을 방지하려면 IP 패킷이 MTU 크기 내에 맞아야 합니다.

참고 ASA에서는 메모리에 공간이 있는 한 구성된 MTU보다 큰 프레임을 수신할 수 있습니다. 큰 프레임을 지원하기 위해 메모리를 늘리는 방법은 10-28 페이지의 점보 프레임 지원 활성화를 참조하십시오.

기본 MTU

ASA의 기본 MTU는 1500바이트입니다. 이 값에는 18바이트 이상의 이더넷 헤더, CRC, VLAN 태깅 등이 포함되지 않습니다.

경로 MTU 검색

ASA에서는 경로 MTU 검색을 지원하며(RFC 1191에 규정), 이 기능을 사용하면 두 호스트 간의 네트워크 경로에 있는 모든 디바이스에서 MTU를 조율할 수 있으므로, 경로의 최저 MTU에 대한 표준을 설정할 수 있습니다.

MTU 및 점보 프레임 설정

12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성를 참조하십시오. 다중 컨텍스트 모드의 경우, 각 컨텍스트 내에서 MTU를 설정합니다.

10-28 페이지의 점보 프레임 지원 활성화를 참조하십시오. 다중 컨텍스트 모드의 경우 시스템 실행 영역에서 점보 프레임 지원을 설정합니다.

다음 지침을 참조하십시오.

- 트래픽 경로의 MTU 일치 — 모든 ASA 인터페이스 및 기타 디바이스 인터페이스의 MTU를 트래픽 경로와 동일하게 설정하는 것이 좋습니다. MTU를 일치시키면 패킷 분할 시 디바이스가 중간에 끼어드는 현상을 방지할 수 있습니다.
- 점보 프레임 수용 — 점보 프레임을 활성화할 경우, MTU를 최대 9198바이트까지 설정할 수 있습니다.

TCP 최대 세그먼트 크기 개요

TCP MSS(TCP 최대 세그먼트 크기)는 TCP 헤더가 추가되기 *전의* TCP 페이로드의 크기입니다. UDP 패킷은 영향을 받지 않습니다. 연결을 설정할 경우 클라이언트와 서버에서는 3방향 핸드셰이크 동안 TCP MSS 값을 교환합니다.

ASA에서 TCP MSS를 설정할 수 있습니다. 연결의 엔드포인트에서 ASA에 설정된 값보다 큰 TCP MSS를 요청할 경우, ASA에서는 요청 패킷의 TCP MSS를 ASA 최대값으로 덮어씁니다. 호스트 또는 서버에서 TCP MSS를 요청하지 않을 경우 ASA에서는 RFC 793 기본값을 536바이트로 추정하며 패킷을 수정하지 않습니다. 또한 최소 TCP MSS를 구성할 수 있습니다. 호스트 또는 서버에서 요청한 TCP MSS가 매우 작을 경우, ASA에서는 값을 조정하여 올릴 수 있습니다. 기본적으로 최소 TCP MSS는 활성화되어 있지 않습니다.

기본값이 1500바이트인 MTU를 구성하는 경우를 예로 들어보겠습니다. 호스트에서는 값이 1700인 MSS를 요청합니다. ASA 최대 TCP MSS가 1380이면 ASA에서는 TCP 요청 패킷의 MSS 값을 1380으로 변경합니다. 그러면 서버에서는 1380바이트 패킷을 전송합니다.

기본 TCP MSS

기본적으로 ASA의 최대 TCP MSS는 1380바이트 입니다. 이러한 기본값을 사용하면 헤더에 120바이트를 추가할 수 있는 경우 VPN 연결을 수용하는 것이 가능합니다. 이 값은 기본값이 1500바이트인 MTU에 적합합니다.

VPN 및 비 VPN 트래픽의 TCP MSS 설정

12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성를 참조하십시오. 다중 컨텍스트 모드의 경우, 각 컨텍스트 내에서 TCP MSS를 설정합니다.

다음 지침을 참조하십시오.

- 비 VPN 트래픽 — VPN을 사용하지 않고 헤더에 추가 공간이 필요하지 않은 경우, TCP MSS 제한을 비활성화하고 연결과 엔드포인트 간에 설정된 값을 승인해야 합니다. 연결 엔드포인트의 경우 대개 MTU에서 TCP MSS가 파생되므로 비 VPN 패킷은 일반적으로 이러한 TCP MSS에 적합합니다.
- VPN 트래픽 — MTU에 대한 최대 TCP MSS를 120으로 설정합니다. 예를 들어, 점보 프레임을 사용하고 MTU를 더 높은 값으로 설정할 경우 새로운 MTU를 수용할 수 있는 TCP MSS를 설정해야 합니다.

ASA 5512-X 이상 버전의 인터페이스 라이센스 요구 사항

모델	라이센싱 요구 사항
ASA 5512-X	VLAN: Base 라이센스: 50 Security Plus 라이센스: 100 모든 유형의 인터페이스: Base 라이센스: 716 Security Plus 라이센스: 916
ASA 5515-X	VLAN: Base 라이센스: 100 모든 유형의 인터페이스: Base 라이센스: 916
ASA 5525-X	VLAN: Base 라이센스: 200 모든 유형의 인터페이스: Base 라이센스: 1316
ASA 5545-X	VLAN: Base 라이센스: 300 모든 유형의 인터페이스: Base 라이센스: 1716
ASA 5555-X	VLAN: Base 라이센스: 500 모든 유형의 인터페이스: Base 라이센스: 2516

모델	라이센싱 요구 사항
ASA 5585-X	VLAN: Base 및 Security Plus 라이센스: 1024 SSP-10 및 SSP-20을 위한 인터페이스 속도: Base 라이센스—파이버 인터페이스용 1기가비트 이더넷 10GE I/O 라이센스(Security Plus)—파이버 인터페이스용 10기가비트 이더넷 (SSP-40 및 SSP-60은 10기가비트 이더넷을 기본적으로 지원) 모든 유형의 인터페이스: Base 및 Security Plus 라이센스: 4612

참고 어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다.

모든 유형의 인터페이스는 전체 인터페이스, 이를테면 VLAN 인터페이스, 물리적 인터페이스, 이중 인터페이스, 브리지 그룹 인터페이스, EtherChannel 인터페이스의 최대 개수로 이루어집니다. 컨피그레이션에 정의된 모든 **interface**은 이 한도의 대상이 됩니다.

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

컨텍스트 모드의 경우 10-13 페이지의 인터페이스 구성 시작(ASA 5512-X 이상)에 따라 시스템 실행 영역에서 물리적 인터페이스를 구성합니다. 그런 다음 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.에 따라 컨텍스트 실행 영역에서 논리적 인터페이스 매개변수를 구성합니다.

방화벽 모드 지침

- 투명 모드의 경우 컨텍스트당 또는 단일 모드 디바이스에 최대 8개의 브릿지 그룹을 구성할 수 있습니다.
- 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다.
- 다중 컨텍스트, 투명 모드의 경우 각 컨텍스트에서는 다른 인터페이스를 사용해야 하며 컨텍스트 간에 인터페이스를 공유할 수 없습니다.

장애 조치 지침

- 이중화 또는 EtherChannel 인터페이스를 장애 조치 링크로 사용할 경우, 장애 조치 쌍의 두 유닛에 모두 이를 사전 구성해야 합니다. *복제를 위해서는 장애 조치 링크 자체가 필요하므로* 이러한 인터페이스를 기본 유닛에 구성한 다음 이를 보조 유닛에 복제할 수 없습니다.
- 상태 링크에 이중화 또는 EtherChannel 인터페이스를 사용할 경우, 특별한 컨피그레이션이 필요하지 않으며 컨피그레이션을 기본 유닛에서 정상적으로 복제할 수 있습니다.

- 이때 논리적 이중화 인터페이스 이름을 참조해야 합니다. 액티브 멤버 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작할 경우, 디바이스 수준 장애 조치가 모니터링되고 있으면 이 작업을 수행해도 이중화 또는 EtherChannel 인터페이스에 오류가 발생하는 것으로 나타나지 않습니다. 모든 물리적 인터페이스에 오류가 발생한 경우에만 이중화 또는 EtherChannel 인터페이스에 오류가 발생하는 것으로 나타납니다(EtherChannel 인터페이스의 경우 오류 발생이 허용되는 인터페이스 수를 구성할 수 있음).
- 장애 조치 또는 상태 링크에 EtherChannel 인터페이스를 사용할 경우, 패킷의 오류를 방지하기 위해 EtherChannel에서 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다. 컨피그레이션을 변경하려면 변경 사항을 적용하는 동안에는 EtherChannel을 종료하거나 장애 조치를 일시적으로 비활성화해야 합니다. 이렇게 하면 해당 기간에는 장애 조치가 발생하지 않습니다.
- 장애 조치 또는 상태 인터페이스는 데이터 인터페이스와 공유할 수 없습니다.

클러스터링 지침

- Spanned EtherChannel을 구성하려면 9-44 페이지의 Spanned EtherChannel 구성를 참조하십시오.
- 개별 클러스터 인터페이스를 구성하려면 9-41 페이지의 개별 인터페이스 구성(관리 인터페이스 권장 사항)를 참조하십시오.

이중화 인터페이스 지침

- 최대 8개의 이중화 인터페이스 쌍을 구성할 수 있습니다.
- 모든 ASA 컨피그레이션에서는 컨피그레이션원 물리적 인터페이스 대신 논리적 이중화 인터페이스를 참조합니다.
- 이중화 인터페이스를 EtherChannel의 일부로 사용하거나, EtherChannel을 이중화 인터페이스 일부로 사용할 수 없습니다. 이중화 인터페이스 및 EtherChannel 인터페이스에서 동일한 물리적 인터페이스를 사용할 수 없습니다. 그러나 이러한 인터페이스에서 동일한 물리적 인터페이스를 사용하지 않을 경우 ASA에서 두 가지 유형을 구성할 수 있습니다.
- 액티브 인터페이스를 종료할 경우 스탠바이 인터페이스가 액티브 상태로 됩니다.
- 이중 인터페이스는 관리 *슬롯/포트* 인스턴스를 멤버로 지원하지 않습니다. 또한 비 관리 인터페이스가 포함된 이중 인터페이스를 관리 전용으로 설정할 수 없습니다.
- 장애 조치 지침에 대한 내용은 10-10 페이지의 장애 조치 지침를 참조하십시오.
- 클러스터링 지침에 대한 내용은 10-11 페이지의 클러스터링 지침를 참조하십시오.

EtherChannel 지침

- 최대 48개의 EtherChannel을 구성할 수 있습니다.
- 각 채널 그룹에는 최대 16개의 액티브 인터페이스를 포함할 수 있습니다. 액티브 인터페이스를 8개만 지원하는 스위치의 경우, 채널 그룹 하나에 최대 16개의 인터페이스를 할당할 수 있습니다. 이 중 8개만 액티브 인터페이스가 될 수 있으며, 나머지 인터페이스는 인터페이스 오류에 대비하여 스탠바이 링크 역할을 수행할 수 있습니다.
- 채널 그룹의 모든 인터페이스는 유형과 속도가 같아야 합니다. 채널 그룹에 추가된 첫 번째 인터페이스에서는 올바른 유형과 속도를 결정합니다.
- ASA EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다. 예를 들어, Catalyst 6500 스위치 또는 Cisco Nexus 7000에 연결할 수 있어야 합니다.
- ASA에서는 VLAN 태그 처리된 LACPDU를 지원하지 않습니다. Cisco IOS **vlan dot1Q tag native** 명령을 사용하여 인접한 스위치에서 네이티브 VLAN 태깅을 활성화할 경우, ASA에서는 태그 처리된 LACPDU를 제거합니다. 인접한 스위치에서 네이티브 VLAN 태깅을 비활성화해야 합니다. 다중 컨텍스트 모드의 경우 이러한 메시지가 패킷 캡처에 포함되지 않으므로 문제를 쉽게 진단할 수 없습니다.

- ASA에서는 EtherChannel을 스위치 스택에 연결하도록 지원하지 않습니다. ASA EtherChannel이 교차 스택에 연결되어 있는 상태에서 마스터 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다.
- 모든 ASA 컨피그레이션에서는 컨피그레이션원 물리적 인터페이스 대신 논리적 EtherChannel 인터페이스를 참조합니다.
- 이중화 인터페이스를 EtherChannel의 일부로 사용하거나, EtherChannel을 이중화 인터페이스 일부로 사용할 수 없습니다. 이중화 인터페이스 및 EtherChannel 인터페이스에서 동일한 물리적 인터페이스를 사용할 수 없습니다. 그러나 이러한 인터페이스에서 동일한 물리적 인터페이스를 사용하지 않을 경우 ASA에서 두 가지 유형을 구성할 수 있습니다.
- 장애 조치 지침에 대한 내용은 10-10 페이지의 장애 조치 지침를 참조하십시오.
- 클러스터링 지침에 대한 내용은 10-11 페이지의 클러스터링 지침를 참조하십시오.

기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다. 공장 기본 컨피그레이션에 대한 자세한 내용은 2-15 페이지의 공장 기본 구성를 참조하십시오.

인터페이스의 기본 상태

인터페이스의 기본 상태는 유형 및 컨텍스트 모드에 따라 다릅니다.

다중 컨텍스트 모드에서는 인터페이스가 시스템 실행 영역에서 어떤 상태이든 상관없이 모든 할당된 인터페이스가 기본적으로 활성화되어 있습니다. 그러나 트래픽이 인터페이스를 통과하려면 인터페이스가 시스템 실행 영역에서도 활성화되어야 합니다. 시스템 실행 영역에서 인터페이스를 종료한 경우 이 인터페이스는 이를 공유하는 모든 컨텍스트에서 중지됩니다.

단일 모드 또는 시스템 실행 영역에서 인터페이스의 기본 상태는 다음과 같습니다.

- 물리적 인터페이스 — 비활성화되어 있습니다.
- 이중화 인터페이스 — 활성화되어 있습니다. 그러나 이중화 인터페이스를 통해 트래픽을 전달하려면 멤버 물리적 인터페이스도 활성화되어야 합니다.
- 하위 인터페이스 — 활성화되어 있습니다. 그러나 하위 인터페이스를 통해 트래픽을 전달하려면 물리적 인터페이스도 활성화되어야 합니다.
- EtherChannel 포트 채널 인터페이스 — 활성화되어 있습니다. 그러나 EtherChannel을 통해 트래픽을 전달하려면 채널 그룹 물리적 인터페이스도 활성화되어야 합니다.

기본 속도와 양방향

- 기본적으로 구리(RJ-45) 인터페이스의 속도와 양방향은 자동 협상이 이루어지도록 설정됩니다.
- 5585-X용 파이버 인터페이스의 경우 자동 링크 협상에 대한 속도가 설정됩니다.

기본 커넥터 유형

일부 모델에 포함되는 커넥터 유형은 구리 RJ-45와 파이버 SFP로 된 두 가지 종류입니다. RJ-45가 기본값입니다. 파이버 SFP 커넥터를 사용하도록 ASA를 구성할 수 있습니다.

기본 MAC 주소

기본적으로 물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.

인터페이스 구성 시작(ASA 5512-X 이상)

인터페이스 구성 시작을 위한 작업 흐름

참고 기존 컨피그레이션을 보유하고 있고 사용 중인 인터페이스를 이중화 또는 EtherChannel 인터페이스로 변환하려면 CLI를 사용해 컨피그레이션을 오프라인으로 수행하여 작업 중단을 최소화하십시오. 10-29 페이지의 사용 중인 인터페이스를 이중화 또는 EtherChannel 인터페이스로 변환를 참조하십시오.

인터페이스 구성을 시작하려면 다음 단계를 수행합니다.

1단계 (다중 컨텍스트 모드) 시스템 실행 영역에서 모든 작업을 완료합니다. 시스템 컨피그레이션 모드에 있지 않은 경우 Configuration > Device List 창에서 액티브 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.

2단계 물리적 인터페이스를 활성화하고 선택에 따라 이더넷 매개변수를 변경합니다. 10-14 페이지의 물리적 인터페이스 활성화 및 이더넷 매개변수 구성를 참조하십시오.

물리적 인터페이스는 기본적으로 비활성화되어 있습니다.

3단계 (선택 사항) 이중화 인터페이스 쌍을 구성합니다. 10-17 페이지의 이중화 인터페이스 구성를 참조하십시오.

논리적 이중화 인터페이스에서는 액티브와 스탠바이 물리적 인터페이스를 쌍으로 묶습니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다.

4단계 (선택 사항) EtherChannel을 구성합니다. 10-20 페이지의 EtherChannel 구성를 참조하십시오.

EtherChannel은 여러 이더넷 인터페이스를 단일한 논리적 인터페이스로 그룹화합니다.

5단계 (선택 사항) VLAN 하위 인터페이스를 구성합니다. 10-25 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹를 참조하십시오.

6단계 (선택 사항) 10-28 페이지의 점보 프레임 지원 활성화에 따라 점보 프레임 지원을 활성화합니다.

7단계 (다중 컨텍스트 모드만 해당) 시스템 실행 영역에서 인터페이스의 컨피그레이션을 완료하려면 7장, “다중 컨텍스트 모드”에 설명된 다음 작업을 수행하십시오.

- 컨텍스트에 인터페이스를 할당하려면 7-19 페이지의 보안 컨텍스트 구성를 참조하십시오.
- (선택 사항) 고유한 MAC 주소를 컨텍스트 인터페이스에 자동으로 할당하려면 7-23 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정를 참조하십시오.

이 MAC 주소는 컨텍스트 내에서 패킷을 분류하는 데 사용됩니다. 인터페이스를 공유하고 있지만 각 컨텍스트의 인터페이스에 고유한 MAC 주소가 없는 경우, 패킷을 분류하는 데 목적지 IP 주소가 사용됩니다. 또는 12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성에 따라 컨텍스트 내에서 MAC 주소를 수동으로 할당할 수 있습니다.

8단계 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.에 따라 인터페이스 컨피그레이션을 완료합니다.

물리적 인터페이스 활성화 및 이더넷 매개변수 구성

이 섹션에서는 다음을 수행하는 방법을 설명합니다.

- 물리적 인터페이스 활성화
- 특정 속도 및 양방향 설정(제공되는 경우)
- 흐름 제어를 위한 일시 중지 프레임 활성화

전제 조건

다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 시스템 컨피그레이션 모드에 있지 않은 경우 Configuration > Device List 창에서 액티브 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.

세부 단계

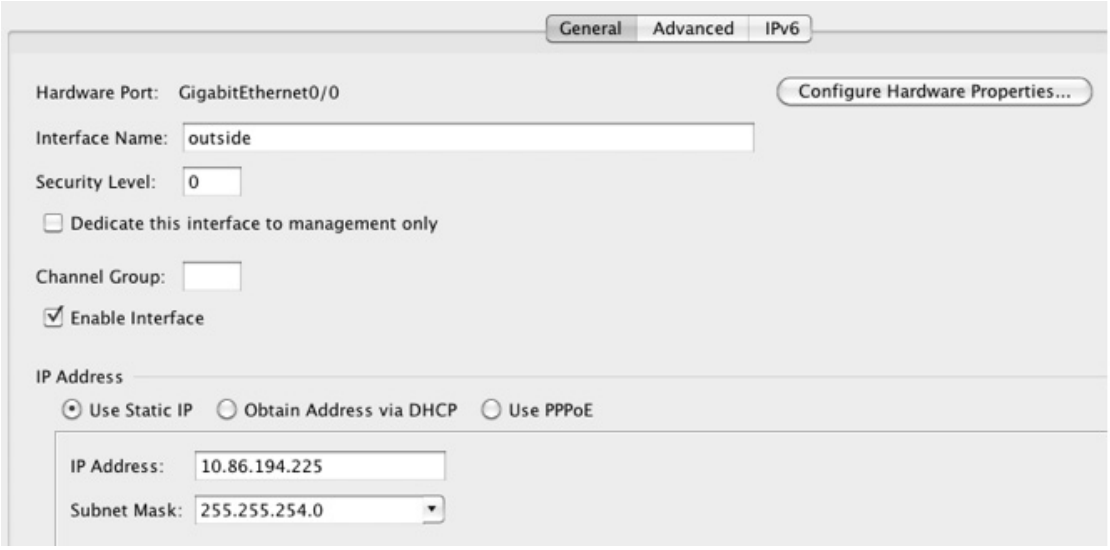
1단계 컨텍스트 모드에 따라

- 단일 모드에서는 **Configuration > Device Setup > Interfaces** 창을 선택합니다.
- 다중 모드의 경우 시스템 실행 영역에서 **Configuration > Context Management > Interfaces** 창을 선택합니다.

기본적으로 모든 물리적 인터페이스가 나열됩니다.

2단계 구성할 물리적 인터페이스를 클릭하고 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 나타납니다.



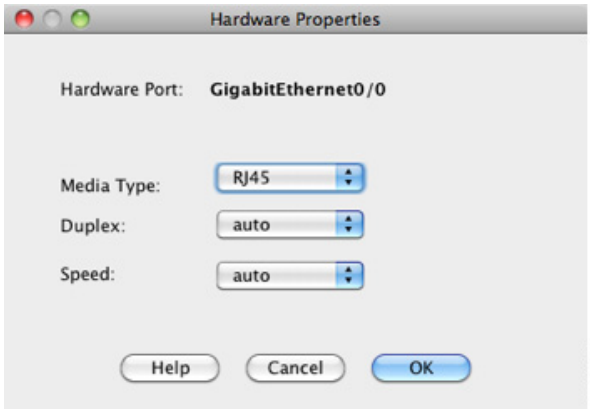
참고 단일 모드의 경우 이 절차에 포함되는 항목은 Edit Interface 대화 상자에 있는 매개변수의 하위 집합만 해당됩니다. 다른 매개변수를 컨피그레이션하려면 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오. 다중 컨텍스트 모드의 경우 인터페이스 컨피그레이션을 완료하기 전에 컨텍스트에 인터페이스를 할당해야 합니다. 7-15 페이지의 다중 컨텍스트 모드 구성를 참조하십시오.

3단계 인터페이스를 활성화하려면 **Enable Interface** 확인란을 선택합니다.

4단계 설명을 추가하려면 Description 필드에 텍스트를 입력합니다.

설명은 줄 바꿈 없이 1줄, 최대 240자로 작성합니다. 장애 조치 또는 상태 링크의 경우 이 설명은 “LAN Failover Interface”, “STATE Failover Interface” 또는“LAN/STATE Failover Interface”와 같이 고정되어 있습니다. 이 설명을 수정할 수 없습니다. 이 인터페이스를 장애 조치 또는 상태 링크로 만들 경우 고정된 설명이 사용자가 여기에 입력한 설명을 덮어씁니다.

5단계 (선택 사항) 미디어 유형, 양방향을 설정하고 흐름 제어에 대한 일시 중지 프레임을 활성화하려면 **Configure Hardware Properties**를 클릭합니다.



a. 인터페이스 유형에 따라 Media Type 드롭다운 목록에서 **RJ-45** 또는 **SFP**를 선택할 수 있습니다.

RJ-45가 기본값입니다.

b. RJ-45 인터페이스에 양방향을 설정하려면 인터페이스 유형에 따라 Duplex 드롭다운 목록에서 **Full**, **Half** 또는 **Auto**를 선택합니다.

참고 EtherChannel 인터페이스의 양방향 설정은 Full 또는 Auto여야 합니다.

c. 속도를 설정하려면 Speed 드롭다운 목록에서 값을 선택합니다.

제공되는 속도는 인터페이스 유형에 따라 다릅니다. SFP 인터페이스의 경우 Negotiate 또는 Nonegotiate에 대한 속도를 설정할 수 있습니다. Negotiate(기본값)를 사용하면 흐름 제어 매개변수와 원격 오류 정보를 교환하는 링크 협상이 활성화됩니다. Nonegotiate에서는 링크 매개변수를 협상하지 않습니다. RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 자동 MDI/MDIX 기능도 포함됩니다. 10-2 페이지의 자동 MDI/MDIX 기능를 참조하십시오.

d. 1기가비트 및 10기가비트 이더넷 인터페이스에서 흐름 제어에 일시 중지(XOFF) 프레임을 활성화하려면 **Enable Pause Frame** 확인란을 선택합니다.

트래픽 버스트가 있을 경우 이러한 버스트가 NIC에서 FIFO 버퍼의 버퍼링 용량을 초과하고 링 버퍼를 수신하면 패킷 손실이 발생할 수 있습니다. 흐름 제어를 위한 일시 중지 프레임을 활성화하면 이러한 문제를 완화할 수 있습니다. 일시 중지(XOFF) 및 XON 프레임은 FIFO 버퍼 사용량을 기준으로 NIC 하드웨어에서 자동으로 생성됩니다. 일시 중지 프레임은 버퍼 사용량이 최고 수위를 넘을 때 전송됩니다. 기본 *high_water* 값은 128KB(10 GigabitEthernet) 및 24KB(1 GigabitEthernet)이며 이 범위를 0~511(10 GigabitEthernet) 또는 0~47KB(1 GigabitEthernet) 사이로 설정할 수 있습니다. 일시 중지를 보낸 후 버퍼 사용량이 최저 수위 이하로 감소할 경우 XON 프레임이 전송될 수 있습니다. 기본적으로 *low_water* 값은 64KB(10 GigabitEthernet) 및 16KB(1 GigabitEthernet)이며 이 범위를 0~511(10 GigabitEthernet) 또는 0~47KB(1 GigabitEthernet) 사이로 설정할 수 있습니다. XON이 수신된 후 또는 XOFF가 만료된 후, 일시 중지 프레임의 타이머 값에서 제어하는 대로 링크 파트너를 다시 시작할 수 있습니다. 기본 *pause_time* 값은 26624이며 이를 0~65535 사이로 설정할 수 있습니다. 버퍼 사용량이 지속적으로 최고 수위를 넘을 경우, 일시 중지 프레임이 반복해서 전송되며 이는 일시 중지 새로 고침 임계값에 의해 제어됩니다.

Low Watermark, High Watermark, Pause Time의 기본값을 변경하려면 **Use Default Values** 확인란의 선택을 취소합니다.

참고 802.3x에 정의된 흐름 제어 프레임만 지원됩니다. 우선순위를 기반으로 하는 흐름 제어는 지원되지 않습니다.

e. **OK**를 클릭하여 Hardware Properties 변경 사항을 승인합니다.

6단계 **OK**를 클릭하여 Interface 변경 사항을 승인합니다.

다음에 할 일

선택적 작업:

- 이중화 인터페이스 쌍을 구성합니다. 10-17 페이지의 이중화 인터페이스 구성를 참조하십시오.
- EtherChannel을 구성합니다. 10-20 페이지의 EtherChannel 구성를 참조하십시오.
- VLAN 하위 인터페이스를 구성합니다. 10-25 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹를 참조하십시오.
- 점보 프레임 지원을 구성합니다. 10-28 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 다중 컨텍스트 모드의 경우, 컨텍스트에 인터페이스를 할당하고 컨텍스트 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 7-15 페이지의 다중 컨텍스트 모드 구성를 참조하십시오.
- 단일 컨텍스트 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

이중화 인터페이스 구성

논리적 이중화 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중화 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중화 인터페이스와 함께 장애 조치를 구성할 수 있습니다.

이 섹션에서는 이중화 인터페이스를 구성하는 방법에 대해 설명합니다.

이중화 인터페이스 구성

이 섹션에서는 이중화 인터페이스를 생성하는 방법에 대해 설명합니다. 기본적으로 이중화 인터페이스는 활성화되어 있습니다.

지침 및 제한 사항

- 최대 8개의 이중화 인터페이스 쌍을 구성할 수 있습니다.
- 이중화 인터페이스 지연 값은 구성 가능하나, 기본적으로 ASA에서는 멤버 인터페이스의 물리적 유형을 기준으로 기본 지연 값을 상속합니다.
- 10-11 페이지의 이중화 인터페이스 지침도 참조하십시오.

전제 조건

- 두 인터페이스 모두 물리적 유형이 같아야 합니다. 예를 들어, 모두 GigabitEthernet이어야 합니다.
- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 이중화 인터페이스에 추가할 수 없습니다. Configuration > Device Setup > Interfaces 창에서을 사용하여 우선 이름을 제거해야 합니다.
- 다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 시스템 컨피그레이션 모드에 있지 않은 경우 Configuration > Device List 창에서 액티브 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.

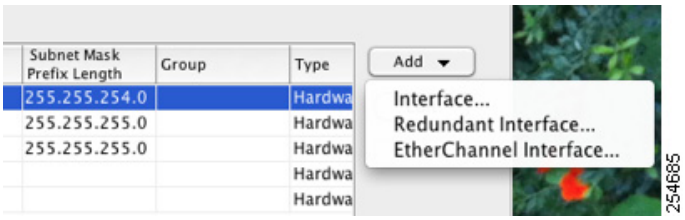
주의 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

세부 단계

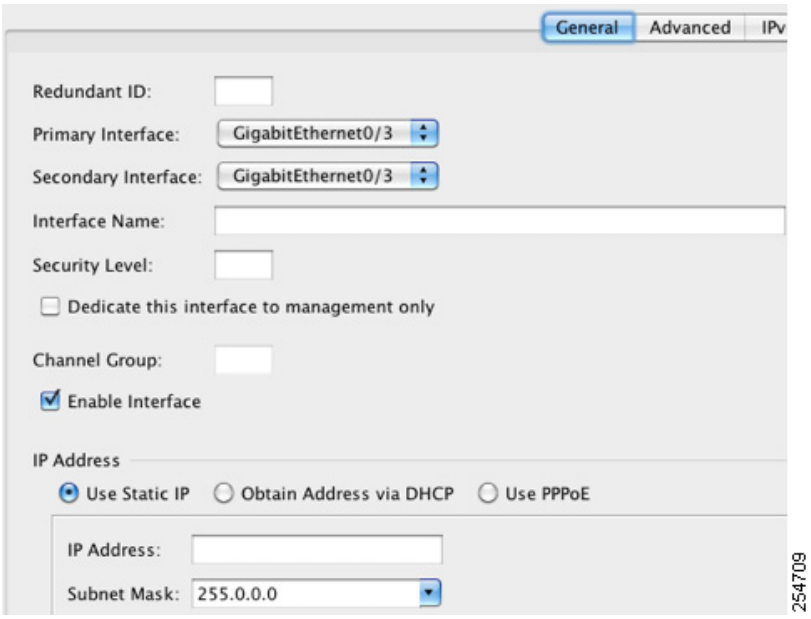
1단계 컨텍스트 모드에 따라

- 단일 모드에서는 **Configuration > Device Setup > Interfaces** 창을 선택합니다.
- 다중 모드의 경우 시스템 실행 영역에서 **Configuration > Context Management > Interfaces** 창을 선택합니다.

2단계 **Add > Redundant Interface**를 선택합니다.



Add Redundant Interface 대화 상자가 나타납니다.



참고 단일 모드의 경우 이 절차에 포함되는 항목은 Edit Redundant Interface 대화 상자에 있는 매개변수의 하위 집합만 해당됩니다. 다른 매개변수를 컨피그레이션하려면 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오. 다중 컨텍스트 모드의 경우 인터페이스 컨피그레이션을 완료하기 전에 컨텍스트에 인터페이스를 할당해야 합니다. 7-15 페이지의 다중 컨텍스트 모드 구성를 참조하십시오.

3단계 Redundant ID 필드에 1~8 사이의 정수를 입력합니다.

4단계 Primary Interface 드롭다운 목록에서 기본으로 설정하려는 물리적 인터페이스를 선택합니다.

하위 인터페이스가 없고 컨텍스트에 할당되지 않은 인터페이스를 선택해야 합니다. 이중 인터페이스는 관리 *슬롯/포트* 인스턴스를 멤버로 지원하지 않습니다.

5단계 Secondary Interface 드롭다운 목록에서 보조로 설정하려는 물리적 인터페이스를 선택합니다.

6단계 인터페이스가 아직 활성화되지 않은 경우 **Enable Interface** 확인란을 선택합니다.

인터페이스는 기본적으로 활성화되어 있습니다. 비활성화하려면 확인란의 선택을 취소합니다.

7단계 설명을 추가하려면 Description 필드에 텍스트를 입력합니다.

설명은 줄 바꿈 없이 1줄, 최대 240자로 작성합니다. 다중 컨텍스트 모드의 경우 시스템 설명은 컨텍스트 설명과 무관합니다. 장애 조치 또는 상태 링크의 경우 이 설명은 "LAN Failover Interface", "STATE Failover Interface" 또는"LAN/STATE Failover Interface"와 같이 고정되어 있습니다. 이 설명을 수정할 수 없습니다. 이 인터페이스를 장애 조치 또는 상태 링크로 만들 경우 고정된 설명이 사용자가 여기에 입력한 설명을 덮어씁니다.

8단계 **OK**를 클릭합니다.

Interfaces 창으로 돌아갑니다. 이제 멤버 인터페이스를 보면 인터페이스 ID의 왼쪽에 자물쇠가 표시되며, 이는 해당 인터페이스에 기본 매개변수만 구성할 수 있음을 나타냅니다. 이중화 인터페이스가 테이블에 추가됩니다.

GigabitEthernet0/2	Enabled	No	Redundant8	Hardware	native
GigabitEthernet0/3	Enabled	No		Hardware	native
GigabitEthernet0/3.10	Enabled	No		Logical	vlan100
GigabitEthernet0/3.11	Enabled	No		Logical	vlan11
Management0/0	Enabled	No		Hardware	native
Redundant8	Enabled	Yes		Logical	native

254710

다음에 할 일

선택적 작업:

- VLAN 하위 인터페이스를 구성합니다. 10-25 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹를 참조하십시오.
- 점보 프레임 지원을 구성합니다. 10-28 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 다중 컨텍스트 모드의 경우, 컨텍스트에 인터페이스를 할당하고 컨텍스트 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 7-15 페이지의 다중 컨텍스트 모드 구성를 참조하십시오.
- 단일 컨텍스트 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 12 장, "라우팅 모드 인터페이스", 또는 13 장, "투명 모드 인터페이스".를 참조하십시오.

액티브 인터페이스 변경

기본적으로, 액티브 인터페이스는 컨피그레이션에 나열된 사용 가능한 첫 번째 인터페이스입니다. 어떤 인터페이스가 액티브인지 보려면 Tools > Command Line Interface 툴에 다음 명령을 입력합니다.

show interface redundant*number* **detail | grep Member**

예:

```
show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

액티브 인터페이스를 변경하려면 다음 명령을 입력합니다.

redundant-interface redundant*number* **active-member** *physical_interface*

redundant*number* 인수는 이중화 인터페이스 ID(예: **redundant1**)입니다.

*physical_interface*는 액티브 인터페이스로 변경하려는 멤버 인터페이스 ID입니다.

EtherChannel 구성

이 섹션에서는 EtherChannel 포트 채널 인터페이스를 생성하고, EtherChannel에 인터페이스를 할당하며, EtherChannel을 맞춤화하는 방법에 대해 알아봅니다.

- 10-20 페이지의 EtherChannel에 인터페이스 추가
- 10-22 페이지의 EtherChannel 맞춤화

EtherChannel에 인터페이스 추가

이 섹션에서는 EtherChannel 포트 채널 인터페이스를 생성하고, EtherChannel에 인터페이스를 할당하는 방법에 대해 알아봅니다. 기본적으로 포트 채널 인터페이스는 활성화되어 있습니다.

지침 및 제한 사항

- 최대 48개의 EtherChannel을 구성할 수 있습니다.
- 각 채널 그룹에는 최대 16개의 액티브 인터페이스를 포함할 수 있습니다. 액티브 인터페이스를 8개만 지원하는 스위치의 경우, 채널 그룹 하나에 최대 16개의 인터페이스를 할당할 수 있습니다. 이 중 8개만 액티브 인터페이스가 될 수 있으며, 나머지 인터페이스는 인터페이스 오류에 대비하여 스탠바이 링크 역할을 수행할 수 있습니다.
- 클러스터링에 Spanned EtherChannel을 구성하려면 이 절차 대신 9-44 페이지의 Spanned EtherChannel 구성를 참조하십시오.
- 10-11 페이지의 EtherChannel 지침도 참조하십시오.

전제 조건

- 채널 그룹의 모든 인터페이스는 동일한 유형과 속도, 양방향이어야 합니다. 반이중은 지원되지 않습니다.
- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 채널 그룹에 추가할 수 없습니다. Configuration > Device Setup > Interfaces 창에서을 사용하여 우선 이름을 제거해야 합니다.
- 다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 시스템 컨피그레이션 모드에 있지 않은 경우 Configuration > Device List 창에서 액티브 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.

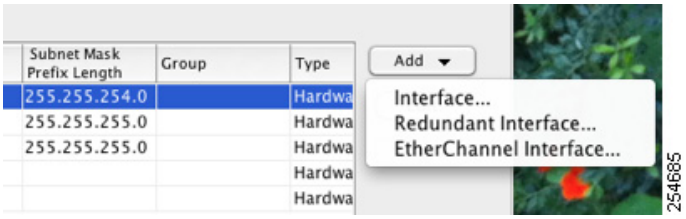
주의 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

세부 단계

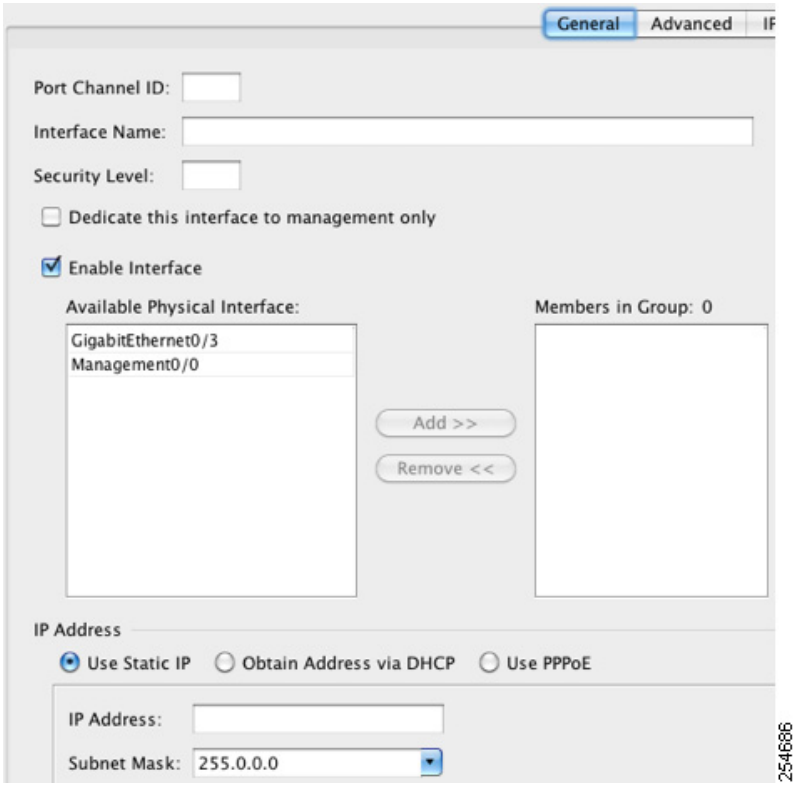
1단계 컨텍스트 모드에 따라

- 단일 모드에서는 **Configuration > Device Setup > Interfaces** 창을 선택합니다.
- 다중 모드의 경우 시스템 실행 영역에서 **Configuration > Context Management > Interfaces** 창을 선택합니다.

2단계 **Add > EtherChannel Interface**를 선택합니다.



Add EtherChannel Interface 대화 상자가 나타납니다.



참고 단일 모드의 경우 이 절차에 포함되는 항목은 Edit EtherChannel Interface 대화 상자에 있는 매개변수의 하위 집합만 해당됩니다. 다른 매개변수를 컨피그레이션하려면 12 장, "라우팅 모드 인터페이스", 또는 13 장, "투명 모드 인터페이스".를 참조하십시오. 다중 컨텍스트 모드의 경우 인터페이스 컨피그레이션을 완료하기 전에 컨텍스트에 인터페이스를 할당해야 합니다. 7-15 페이지의 다중 컨텍스트 모드 구성를 참조하십시오.

3단계 Port Channel ID 필드에 1~48 사이의 숫자를 입력합니다.

4단계 Available Physical Interface 영역에서 인터페이스를 클릭한 다음 **Add >>**를 클릭하여 해당 인터페이스를 Members in Group 영역으로 이동합니다.

투명 모드에서 여러 개의 관리 인터페이스가 있는 채널 그룹을 생성할 경우, 이 EtherChannel을 관리 전용 인터페이스로 사용할 수 있습니다.

참고 EtherChannel 모드를 On으로 설정한 경우, 처음에 하나의 인터페이스만 포함해야 합니다. 이 절차를 완료한 후 멤버 인터페이스를 편집하고 모드를 On으로 설정합니다. 변경 사항을 적용한 다음 EtherChannel을 편집하여 추가 멤버 인터페이스를 추가합니다.

5단계 채널 그룹에 추가할 각 인터페이스에 작업을 반복합니다.

모든 인터페이스의 유형과 속도가 같은지 확인합니다. 첫 번째로 추가된 인터페이스가 EtherChannel의 유형과 속도를 결정합니다. 추가되었으나 일치하지 않는 인터페이스는 보류 상태로 됩니다. ASDM에서는 일치하지 않는 인터페이스가 추가되는 것을 방지하지 못합니다.

6단계 **OK**를 클릭합니다.

Interfaces 창으로 돌아갑니다. 이제 멤버 인터페이스를 보면 인터페이스 ID의 왼쪽에 자물쇠가 표시되며, 이는 해당 인터페이스에 기본 매개변수만 구성할 수 있음을 나타냅니다. EtherChannel 인터페이스가 테이블에 추가됩니다.

7단계 **Apply**를 클릭합니다. 모든 멤버 인터페이스는 자동으로 활성화됩니다.

다음에 할 일

선택적 작업:

- EtherChannel 인터페이스를 맞춤화합니다. 10-22 페이지의 EtherChannel 맞춤화를 참조하십시오.
- VLAN 하위 인터페이스를 구성합니다. 10-25 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹를 참조하십시오.

필수 작업:

- 다중 컨텍스트 모드의 경우, 컨텍스트에 인터페이스를 할당하고 컨텍스트 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 7-15 페이지의 다중 컨텍스트 모드 구성를 참조하십시오.
- 단일 컨텍스트 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

EtherChannel 맞춤화

이 섹션에서는 EtherChannel의 인터페이스 최대 개수, 활성 상태가 되어야 할 EtherChannel의 최소 운영 인터페이스 개수, 로드 밸런싱 알고리즘, 기타 선택적 매개변수를 설정하는 방법에 대해 설명합니다.

세부 단계

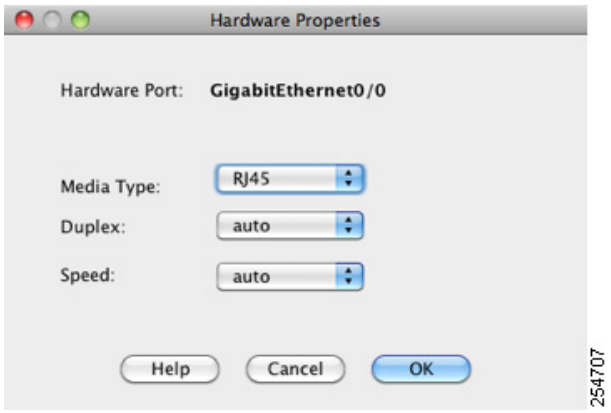
1단계 컨텍스트 모드에 따라

- 단일 모드에서는 **Configuration > Device Setup > Interfaces** 창을 선택합니다.
- 다중 모드의 경우 시스템 실행 영역에서 **Configuration > Context Management > Interfaces** 창을 선택합니다.

2단계 맞춤화하려는 포트 채널 인터페이스를 클릭하고 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 나타납니다.

3단계 모든 멤버 인터페이스의 미디어 유형, 양방향, 속도, 흐름 제어를 위한 일시 중지 프레임을 재정의하려면 **Configure Hardware Properties**를 클릭합니다. 이러한 매개변수는 채널 그룹의 모든 인터페이스와 일치해야 하므로, 이 방법을 사용하면 이러한 매개변수를 빠르게 설정할 수 있습니다.



a. 인터페이스 유형에 따라 Media Type 드롭다운 목록에서 **RJ-45** 또는 **SFP**를 선택할 수 있습니다.

RJ-45가 기본값입니다.

b. RJ-45 인터페이스에 양방향을 설정하려면 인터페이스 유형에 따라 Duplex 드롭다운 목록에서 **Full** 또는 **Auto**를 선택합니다. EtherChannel에 전이중은 지원되지 않습니다.

c. 속도를 설정하려면 Speed 드롭다운 목록에서 값을 선택합니다.

제공되는 속도는 인터페이스 유형에 따라 다릅니다. SFP 인터페이스의 경우 Negotiate 또는 Nonegotiate에 대한 속도를 설정할 수 있습니다. Negotiate(기본값)를 사용하면 흐름 제어 매개변수와 원격 오류 정보를 교환하는 링크 협상이 활성화됩니다. Nonegotiate에서는 링크 매개변수를 협상하지 않습니다. RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 자동 MDI/MDIX 기능도 포함됩니다. 10-2 페이지의 자동 MDI/MDIX 기능를 참조하십시오.

d. 1기가비트 및 10기가비트 이더넷 인터페이스에서 흐름 제어에 일시 중지(XOFF) 프레임을 활성화하려면 **Enable Pause Frame** 확인란을 선택합니다.

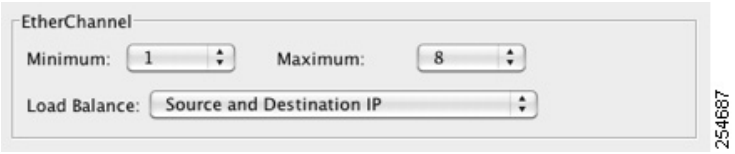
트래픽 버스트가 있을 경우 이러한 버스트가 NIC에서 FIFO 버퍼의 버퍼링 용량을 초과하고 링 버퍼를 수신하면 패킷 손실이 발생할 수 있습니다. 흐름 제어를 위한 일시 중지 프레임을 활성화하면 이러한 문제를 완화할 수 있습니다. 일시 중지(XOFF) 및 XON 프레임은 FIFO 버퍼 사용량을 기준으로 NIC 하드웨어에서 자동으로 생성됩니다. 일시 중지 프레임은 버퍼 사용량이 High Watermark를 넘을 때 전송됩니다. 기본값은 128KB이며 이 범위를 0~511 사이로 설정할 수 있습니다. 일시 중지를 보낸 후 버퍼 사용량이 Low Watermark 이하로 감소할 경우 XON 프레임이 전송될 수 있습니다. 기본적으로 이 값은 64KB이며 이 범위를 0~511 사이로 설정할 수 있습니다. XON이 수신된 후 또는 XOFF가 만료된 후, 일시 중지 프레임의 Pause Time 값에서 제어하는 대로 링크 파트너를 다시 시작할 수 있습니다. 기본값은 26624이며 이 범위를 0~65535 사이로 설정할 수 있습니다. 버퍼 사용량이 지속적으로 High Watermark를 넘을 경우, 일시 중지 프레임이 반복해서 전송되며 이는 일시 중지 새로 고침 임계값에 의해 제어됩니다.

Low Watermark, High Watermark, Pause Time의 기본값을 변경하려면 **Use Default Values** 확인란의 선택을 취소합니다.

참고 802.3x에 정의된 흐름 제어 프레임만 지원됩니다. 우선순위를 기반으로 하는 흐름 제어는 지원되지 않습니다.

e. **OK**를 클릭하여 Hardware Properties 변경 사항을 승인합니다.

4단계 EtherChannel을 맞춤화하려면 **Advanced** 탭을 클릭합니다.



a. EtherChannel 영역의 Minimum 드롭다운 목록에서 EtherChannel을 액티브 상태로 설정하는 데 필요한 액티브 인터페이스의 최소 개수를 1~16 사이에서 선택합니다. 기본값은 1입니다.

b. Maximum 드롭다운 목록에서 EtherChannel에 허용되는 액티브 인터페이스의 최대 개수를 1~16 사이에서 선택합니다. 기본값은 16입니다. 스위치에서 16개의 액티브 인터페이스를 지원하지 않을 경우, 이 명령을 8 이하로 설정합니다.

c. Load Balance 드롭다운 목록에서 그룹 채널 인터페이스 전반에 걸쳐 패킷을 로드 밸런싱하는 데 사용되는 기준을 선택합니다. 기본적으로 ASA에서는 패킷의 소스 및 목적지 IP 주소에 따라 인터페이스의 패킷 로드 밸런싱을 수행합니다. 패킷이 분류되는 속성을 변경하려면 다른 기준 집합을 선택합니다. 예를 들어, 동일한 소스와 목적지 IP 주소에 트래픽이 심하게 편중된 경우 EtherChannel의 인터페이스에 트래픽 할당이 불균형해질 수 있습니다. 다른 알고리즘으로 변경할 경우 트래픽이 보다 고르게 분산될 수 있습니다. 로드 밸런싱에 대한 자세한 내용은 10-6 페이지의 로드 밸런싱을 참조하십시오.

5단계 **OK**를 클릭합니다.

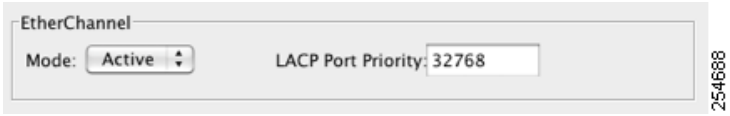
Interfaces 창으로 돌아갑니다.

6단계 채널 그룹에서 물리적 인터페이스의 모드 및 우선순위를 설정하려면

a. Interfaces 테이블에서 물리적 인터페이스를 클릭하고 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 나타납니다.

b. **Advanced** 탭을 클릭합니다.



c. EtherChannel 영역의 Mode 드롭다운 목록에서 **Active**, **Passive** 또는 **On**을 선택합니다. Active 모드(기본값)를 사용하는 것이 좋습니다. 액티브, 패시브 및 on 모드에 대한 자세한 내용은 10-6 페이지의 Link Aggregation Control Protocol를 참조하십시오.

d. LACP Port Priority 필드에서 포트 우선순위를 1~65535 사이로 설정합니다. 기본값은 32768입니다. 숫자가 높을수록 우선순위는 낮아집니다. 사용할 수 있는 인터페이스보다 더 많은 인터페이스가 할당된 경우, ASA에서는 이 설정을 사용하여 어떤 인터페이스가 액티브이고 스탠바이인지 확인합니다. 포트 우선순위 설정이 모든 인터페이스에 대해 동일한 경우, 인터페이스 ID(슬롯/포트)로 우선순위가 결정됩니다. 가장 낮은 인터페이스 ID의 우선순위가 가장 높습니다. 예를 들어, GigabitEthernet 0/0은 GigabitEthernet 0/1보다 우선순위가 더 높습니다.

인터페이스 ID가 더 큰 인터페이스에 우선순위를 부여하여 액티브 상태로 만들려면 이 명령을 더 낮은 값으로 설정합니다. 예를 들어, GigabitEthernet 1/3을 GigabitEthernet 0/7보다 우선순위가 높은 액티브 상태로 만들려면 0/7 인터페이스의 기본값인 32768과 대조적으로, 1/3 인터페이스의 우선순위 값을 12345로 설정합니다.

EtherChannel의 다른 쪽 끝에 있는 디바이스의 포트 우선순위가 충돌할 경우, 시스템 우선순위를 통해 어느 포트 우선순위를 사용해야 할지 결정됩니다. 시스템 우선순위를 설정하려면 9단계를 참조하십시오.

7단계 **OK**를 클릭합니다.

Interfaces 창으로 돌아갑니다.

8단계 **Apply**를 클릭합니다.

9단계 LACP 시스템 우선순위를 설정하려면 다음 단계를 수행합니다. EtherChannel의 다른 쪽 끝에 있는 디바이스의 포트 우선순위가 충돌할 경우, 시스템 우선순위를 통해 어느 포트 우선순위를 사용해야 할지 결정됩니다. 자세한 내용은 6단계d를 참조하십시오.

a. 컨텍스트 모드에 따라

- 단일 모드의 경우 **Configuration > Device Setup > EtherChannel** 창을 선택합니다.
- 다중 모드의 경우 시스템 실행 영역에서 **Configuration > Context Management > EtherChannel** 창을 선택합니다.

b. LACP System Priority 필드에서 우선순위를 1~65535 사이에서 입력합니다.

기본값은 32768입니다.

다음에 할 일

선택적 작업:

- VLAN 하위 인터페이스를 구성합니다. 10-25 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹를 참조하십시오.
- 점보 프레임 지원을 구성합니다. 10-28 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 다중 컨텍스트 모드의 경우, 컨텍스트에 인터페이스를 할당하고 컨텍스트 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 7-15 페이지의 다중 컨텍스트 모드 구성를 참조하십시오.
- 단일 컨텍스트 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹

하위 인터페이스를 사용하면 물리적, 이중화 또는 EtherChannel 인터페이스를 다른 VLAN ID가 태그 처리된 여러 논리적 인터페이스로 분할할 수 있습니다. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다. VLAN을 사용하면 정해진 물리적 인터페이스에서 트래픽을 따로 유지할 수 있으므로, 추가적인 물리적 인터페이스 또는 를 추가하지 않고 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 ASA있습니다. 이 기능은 다중 컨텍스트 모드에서 특히 유용하며 각 컨텍스트에 고유한 인터페이스를 할당할 수 있습니다.

지침 및 제한 사항

- 최대 하위 인터페이스 — 모델에 사용 가능한 최대 VLAN 하위 인터페이스 수를 확인하려면 10-9 페이지의 ASA 5512-X 이상 버전의 인터페이스 라이센스 요구 사항를 참조하십시오.
- 물리적 인터페이스의 태그 처리되지 않은 패킷 방지 — 하위 인터페이스를 사용할 경우, 일반적으로 물리적 인터페이스에서 트래픽을 전달하지 않도록 하고자 합니다. 물리적 인터페이스에서는 태그 처리되지 않은 패킷을 전달하기 때문입니다. 이러한 속성은 이중화 인터페이스 쌍의 물리적 인터페이스 및 EtherChannel 링크에서도 마찬가지입니다. 하위 인터페이스에서 트래픽을 전달하려면 물리적, 이중화 또는 EtherChannel 인터페이스를 활성화해야 하므로, 인터페이스의 이름을 구성하지 않고하는 방법을 통해 물리적, 이중화 또는 EtherChannel 인터페이스에서 트래픽을 전달하지 않도록 합니다. 물리적, 이중화 또는 EtherChannel 인터페이스에서 태그 처리되지 않은 패킷을 전달하는 것을 허용하려면 name을 정상적으로 구성합니다. 인터페이스 컨피그레이션 완료에 대한 자세한 내용은 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”,를 참조하십시오.
- (ASA 5512-X부터 ASA 5555-X 버전까지) Management 0/0 인터페이스에 하위 인터페이스를 구성할 수 없습니다.
- ASA에서는 DTP(Dynamic Trunking Protocol)를 지원하지 않으므로 조건 없이 트렁킹을 수행할 연결된 스위치 포트를 구성해야 합니다.

전제 조건

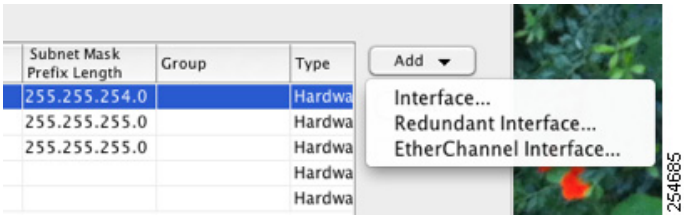
다중 컨텍스트 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 시스템 컨피그레이션 모드에 있지 않은 경우 Configuration > Device List 창에서 액티브 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.

세부 단계

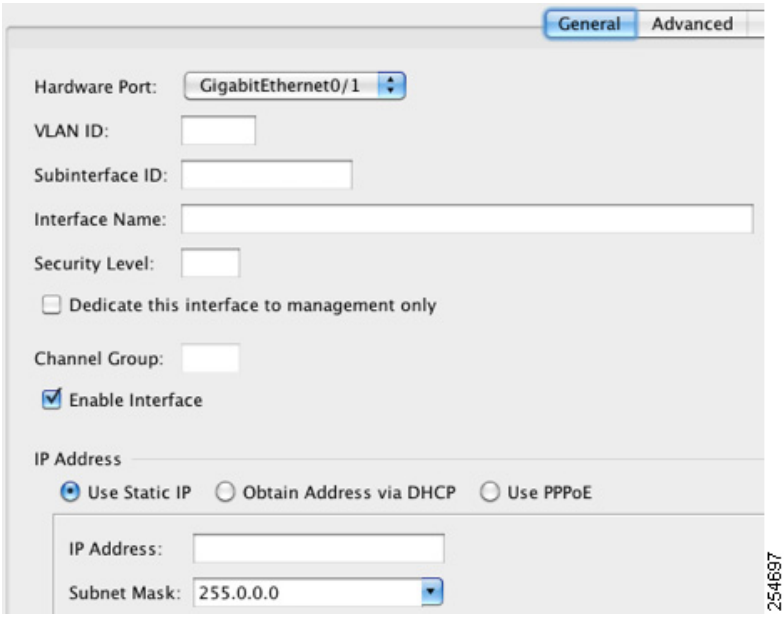
1단계 컨텍스트 모드에 따라

- 단일 모드에서는 **Configuration > Device Setup > Interfaces** 창을 선택합니다.
- 다중 모드의 경우 시스템 실행 영역에서 **Configuration > Context Management > Interfaces** 창을 선택합니다.

2단계 **Add > Interface**를 선택합니다.



Add Interface 대화 상자가 나타납니다.



참고 단일 모드의 경우 이 절차에 포함되는 항목은 Edit Interface 대화 상자에 있는 매개변수의 하위 집합만 해당됩니다. 다른 매개변수를 컨피그레이션하려면 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오. 다중 컨텍스트 모드의 경우 인터페이스 컨피그레이션을 완료하기 전에 컨텍스트에 인터페이스를 할당해야 합니다. 7-15 페이지의 다중 컨텍스트 모드 구성를 참조하십시오.

3단계 Hardware Port 드롭다운 목록에서 하위 인터페이스를 추가할 물리적, 이중화 또는 포트 채널 인터페이스를 선택합니다.

4단계 인터페이스가 아직 활성화되지 않은 경우 **Enable Interface** 확인란을 선택합니다.

인터페이스는 기본적으로 활성화되어 있습니다. 비활성화하려면 확인란의 선택을 취소합니다.

5단계 VLAN ID 필드에 1~4095 사이의 VLAN ID를 입력합니다.

일부 VLAN ID의 경우 연결된 스위치에서 예약될 수 있으므로, 자세한 내용 을 보려면 스위치 설명서를 선택하십시오.다중 컨텍스트 모드의 경우 시스템 컨피그레이션에서 VLAN만 설정할 수 있습니다.

6단계 Subinterface ID 필드에 하위 인터페이스 ID를 1~4294967293 사이의 정수로 입력합니다.

허용되는 하위 인터페이스의 개수는 플랫폼에 따라 다릅니다. 다음을 설정한 후에는 ID를 변경할 수 없습니다.

7단계 (선택 사항) Description 필드에 이 인터페이스에 대한 설명을 입력합니다.

설명은 줄 바꿈 없이 1줄, 최대 240자로 작성합니다. 다중 컨텍스트 모드의 경우 시스템 설명은 컨텍스트 설명과 무관합니다. 장애 조치 또는 상태 링크의 경우 이 설명은 “LAN Failover Interface”, “STATE Failover Interface” 또는“LAN/STATE Failover Interface”와 같이 고정되어 있습니다. 이 설명을 수정할 수 없습니다. 이 인터페이스를 장애 조치 또는 상태 링크로 만들 경우 고정된 설명이 사용자가 여기에 입력한 설명을 덮어씁니다.

8단계 **OK**를 클릭합니다.

Interfaces 창으로 돌아갑니다.

다음에 할 일

선택적 작업:

- 점보 프레임 지원을 구성합니다. 10-28 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 다중 컨텍스트 모드의 경우, 컨텍스트에 인터페이스를 할당하고 컨텍스트 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 7-15 페이지의 다중 컨텍스트 모드 구성를 참조하십시오.
- 단일 컨텍스트 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

점보 프레임 지원 활성화

점보 프레임은 최대 표준 1518바이트(레이어 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷이며, 최대 9216바이트에 이릅니다. 모든 인터페이스에서 이더넷 프레임 처리용 메모리 용량을 늘려 점보 프레임 지원을 활성화할 수 있습니다. 점보 프레임에 더 많은 메모리를 할당하면 ACL와 같은 다른 기능을 최대 한도로 사용하는 데 제약이 따를 수 있습니다. 자세한 내용은 10-7 페이지의 MTU 및 TCP 최대 세그먼트 크기로 조각화 제어를 참조하십시오.

전제 조건

- 다중 컨텍스트 모드의 경우 시스템 실행 영역에서 이 옵션을 설정합니다.
- 이 설정을 변경하면 ASA를 다시 로드해야 합니다.
- 점보 프레임을 전송해야 하는 각 인터페이스의 MTU는 기본값 1500보다 높은 값으로 설정해야 합니다. 예를 들어,을 사용하여 값을 9198로 설정합니다. 12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성를 참조하십시오. 다중 컨텍스트 모드의 경우, 각 컨텍스트 내에서 MTU를 설정합니다.
- 비 VPN 트래픽에는 TCP MSS를 비활성화하거나, 12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성에 따라 MTU에 맞춰 TCP MSS를 늘리는 방식으로 TCP MSS를 조정해야 합니다.

세부 단계

- 다중 모드 — 점보 프레임 지원을 활성화하려면 **Configuration > Context Management > Interfaces**를 선택하고 the **Enable jumbo frame support** 확인란을 클릭합니다.
- Single mode — MTU를 1500바이트보다 크게 설정할 경우 점보 프레임이 자동으로 활성화됩니다. 이 설정을 수동으로 활성화하거나 비활성화하려면 **Configuration > Device Setup > Interfaces**를 선택하고 **Enable jumbo frame support** 확인란을 클릭합니다.

다음에 할 일

- 다중 컨텍스트 모드의 경우, 컨텍스트에 인터페이스를 할당하고 컨텍스트 인터페이스에 고유한 MAC 주소를 자동으로 할당합니다. 7-15 페이지의 다중 컨텍스트 모드 구성를 참조하십시오.
- 단일 컨텍스트 모드의 경우 인터페이스 컨피그레이션을 완료합니다. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

사용 중인 인터페이스를 이중화 또는 EtherChannel 인터페이스로 변환

기존 컨피그레이션을 사용 중이고 현재 사용 중인 인터페이스에 이중화 또는 EtherChannel 인터페이스 기능의 장점을 활용하려면, 논리적 인터페이스를 변환할 경우 약간의 다운타임이 발생하게 됩니다.

이 섹션에서는 다운타임을 최소화하여 기존 인터페이스를 이중화 또는 EtherChannel 인터페이스로 변환하는 방법의 개요를 제공합니다. 자세한 내용은 10-17 페이지의 이중화 인터페이스 구성 및 10-20 페이지의 EtherChannel 구성에서 참조하십시오.

- 10-29 페이지의 자세한 단계(단일 모드)
- 10-34 페이지의 자세한 단계(다중 모드)

자세한 단계(단일 모드)

다음과 같은 이유에 따라 컨피그레이션을 오프라인에서 텍스트 파일로 업데이트한 후, 전체 컨피그레이션을 다시 가져오는 것이 좋습니다.

- 이름이 지정된 인터페이스는 이중화 또는 EtherChannel 인터페이스의 멤버로 추가할 수 없으므로, 인터페이스에서 이름을 제거해야 합니다. 인터페이스에서 이름을 제거하면 해당 이름을 참조하던 모든 명령이 삭제됩니다. 인터페이스 이름을 참조하는 명령은 컨피그레이션 전반에 걸쳐 광범위하게 존재하고 여러 기능에 영향을 미치므로, CLI 또는 ASDM에서 사용 중인 인터페이스에서 이름을 제거하면 새 인터페이스 이름과 관련된 모든 기능이 다시 컨피그레이션되는 동시에 심각한 다운타임이 발생하는 것은 물론, 컨피그레이션에 큰 손상이 발생할 수 있습니다.
- 컨피그레이션을 오프라인으로 변경하면 새 논리적 인터페이스에 동일한 인터페이스 이름을 사용할 수 있으므로, 인터페이스 이름을 참조하는 기능 컨피그레이션에 손을 댈 필요가 없습니다. 인터페이스 컨피그레이션만 변경하면 됩니다.
- 실행 중인 컨피그레이션을 지운 뒤 바로 새 컨피그레이션을 적용하면 인터페이스의 다운타임을 최소화할 수 있습니다. 인터페이스를 실시간으로 구성하기 위해 기다리지 않아도 됩니다.

1단계 ASA에 연결합니다. 장애 조치를 사용 중인 경우 액티브 ASA에 연결합니다.

2단계 장애 조치를 사용 중인 경우 **Configuration > Device Management > High Availability > Failover**를 선택하고 **Enable failover** 확인란의 선택을 취소하여 장애 조치를 비활성화합니다. **Apply**를 클릭하고 경고 메시지가 표시되어도 계속 진행합니다.

3단계 **Tools > Backup Configurations**를 선택한 다음 실행 중인 컨피그레이션을 로컬 컴퓨터에 백업하여 실행 중인 컨피그레이션을 복사합니다. 그런 다음 zip 파일을 확장하고 running-config.cfg 파일을 텍스트 편집기로 편집합니다.

편집할 때 오류가 발생할 경우에 대비하여 기존 컨피그레이션의 추가 복사본을 저장해야 합니다.

4단계 이중화 또는 EtherChannel 인터페이스에 추가할 사용 중인 각 인터페이스의 경우, 새 논리적 인터페이스를 생성하는 데 사용할 수 있도록 **interface** 명령 아래의 모든 명령을 잘라서 인터페이스 컨피그레이션 섹션의 끝에 붙여넣습니다. 유일한 예외 사항은 다음 명령이며, 이는 물리적 인터페이스 컨피그레이션에 그대로 유지됩니다.

- **media-type**
- **speed**
- **duplex**
- **flowcontrol**

참고 EtherChannel 또는 이중화 인터페이스에는 *물리적* 인터페이스만 추가할 수 있으며, 물리적 인터페이스에는 VLAN을 구성할 수 없습니다.

정해진 EtherChannel 또는 이중화 인터페이스에서 모든 인터페이스에 대해 위의 값이 일치해야 합니다. EtherChannel 인터페이스의 양방향 설정은 Full 또는 Auto여야 합니다.

예를 들어, 다음과 같은 인터페이스 컨피그레이션이 있을 수 있습니다. 굵게 표시된 명령은 3개의 새 EtherChannel 인터페이스와 함께 사용할 명령이며, 이를 잘라서 인터페이스 섹션의 끝에 붙여넣어야 합니다.

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
!
interface Management0/1
 shutdown
 no nameif
 no security-level
 no ip address
```

5단계 붙여넣은 각 명령 섹션의 위에 다음 명령 중 하나를 입력하여 새 논리적 인터페이스를 생성합니다.

- **interface redundant** *number* [1-8]
- **interface port-channel** *channel_id* [1-48]

예:

```
...

interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
 no shutdown
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 no shutdown
```

6단계 새 논리적 인터페이스에 물리적 인터페이스를 할당합니다.

- 이중화 인터페이스 — 새 **interface redundant** 명령 아래에 다음 명령을 입력합니다.

  member-interface *physical_interface1*
  member-interface *physical_interface2*

  물리적 인터페이스가 두 인터페이스와 동일한 유형입니다(이전에 사용 중 또는 미사용). 관리 인터페이스는 이중화 인터페이스에 할당할 수 없습니다.

  예를 들어, 기존 케이블 연결을 활용하려는 경우 기존 역할에서 이전에 사용 중인 인터페이스를 내부 및 외부 이중화 인터페이스의 일부로 계속 사용할 수 있습니다.

  ```
  interface redundant 1
   nameif outside
   security-level 0
   ip address 10.86.194.225 255.255.255.0
   member-interface GigabitEthernet0/0
   member-interface GigabitEthernet0/2

  interface redundant 2
   nameif inside
   security-level 100
   ip address 192.168.1.3 255.255.255.0
   member-interface GigabitEthernet0/1
   member-interface GigabitEthernet0/3
  ```

- EtherChannel 인터페이스 — EtherChannel에 추가할 각 인터페이스(이전에 사용 중 또는 미사용)의 아래에 다음 명령을 입력합니다. EtherChannel당 최대 16개의 인터페이스를 할당할 수 있습니다. 단, 8개만 액티브 상태로 설정할 수 있으며 나머지는 오류에 대비하여 스탠바이 상태로 유지됩니다.

  channel-group *channel_id* **mode active**

예를 들어, 기존 케이블 연결을 활용하려는 경우 기존 역할에서 이전에 사용 중인 인터페이스를 내부 및 외부 EtherChannel 인터페이스의 일부로 계속 사용할 수 있습니다.

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 shutdown
 no nameif
 no security-level
 no ip address

...
```

7단계 **shutdown** 명령 앞에 **no**를 추가하여 현재 논리적 인터페이스의 일부인 이전에 사용되지 않은 각 인터페이스를 활성화합니다.

예를 들어, 최종 EtherChannel 컨피그레이션은 다음과 같습니다.

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
```

```
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 no shutdown
 no nameif
 no security-level
 no ip address
!
interface port-channel 1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
!
interface port-channel 2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
!
interface port-channel 3
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
```

참고 새 컨피그레이션을 가져온 후 기타 선택적인 EtherChannel 매개변수를 컨피그레이션할 수 있습니다. 10-20 페이지의 EtherChannel 구성를 참조하십시오.

8단계 저장하여 이를변경된 인터페이스 섹션을 포함하여 전체 새 컨피그레이션을 저장합니다.

9단계 변경된 컨피그레이션과 함께 백업 폴더를 다시 압축합니다.

10단계 **Tools > Restore Configurations**를 선택하고 변경된 컨피그레이션 zip 파일을 선택합니다. 기존의 실행 중인 컨피그레이션을 병합하는 것이 아니라 교체해야 합니다. 자세한 내용은 37-23 페이지의 백업 복원를 참조하십시오.

11단계 **Configuration > Device Management > High Availability > Failover**를 선택하고 **Enable failover** 확인란을 선택하여 장애 조치를 다시 활성화합니다. 기본 장애 조치 설정을 구성하려는 경우 **Apply**를 클릭하고 메시지가 표시되면 **No**를 클릭합니다.

자세한 단계(다중 모드)

다음과 같은 이유에 따라 시스템 및 컨텍스트 컨피그레이션을 오프라인에서 텍스트 파일로 업데이트한 후 이를 다시 가져오는 것이 좋습니다.

- 할당된 인터페이스는 이중화 또는 EtherChannel 인터페이스의 멤버로 추가할 수 없으므로, 컨텍스트에서 인터페이스의 할당을 취소해야 합니다. 인터페이스 할당을 취소할 경우 해당 인터페이스를 참조하던 모든 컨텍스트 명령이 삭제됩니다. 인터페이스를 참조하는 명령은 컨피그레이션 전반에 걸쳐 광범위하게 존재하고 여러 기능에 영향을 미치므로, CLI 또는 ASDM에서 사용 중인 인터페이스에서 할당을 제거하면 새 인터페이스와 관련된 모든 기능이 다시 컨피그레이션되는 동시에 심각한 다운타임이 발생하는 것은 물론, 컨피그레이션에 큰 손상이 발생할 수 있습니다.
- 컨피그레이션을 오프라인으로 변경하면 새 논리적 인터페이스에 동일한 인터페이스 이름을 사용할 수 있으므로, 인터페이스 이름을 참조하는 기능 컨피그레이션에 손을 댈 필요가 없습니다. 인터페이스 컨피그레이션만 변경하면 됩니다.
- 실행 중인 시스템 컨피그레이션을 지운 뒤 바로 새 컨피그레이션을 적용하면 인터페이스의 다운타임을 최소화할 수 있습니다. 인터페이스를 실시간으로 구성하기 위해 기다리지 않아도 됩니다.

1단계 ASA에 연결하고 시스템으로 변경합니다. 장애 조치를 사용 중인 경우 액티브 ASA에 연결합니다.

2단계 장애 조치를 사용 중인 경우 **Configuration > Device Management > High Availability > Failover**를 선택하고 **Enable failover** 확인란의 선택을 취소하여 장애 조치를 비활성화합니다. **Apply**를 클릭하고 경고 메시지가 표시되어도 계속 진행합니다.

3단계 시스템에서 **File > Show Running Configuration in New Window**를 선택하고 표시되는 출력을 텍스트 편집기에 복사하여 실행 중인 컨피그레이션을 복사합니다.

편집할 때 오류가 발생할 경우에 대비하여 기존 컨피그레이션의 추가 복사본을 저장해야 합니다.

예를 들어, 시스템 컨피그레이션에서 인터페이스를 다음과 같이 컨피그레이션 및 할당하고 두 컨텍스트 간에 인터페이스를 공유할 수 있습니다.

시스템

```
interface GigabitEthernet0/0
    no shutdown
interface GigabitEthernet0/1
    no shutdown
interface GigabitEthernet0/2
    shutdown
interface GigabitEthernet0/3
    shutdown
interface GigabitEthernet0/4
    shutdown
interface GigabitEthernet0/5
    shutdown
interface Management0/0
    no shutdown
```

```
interface Management1/0
    shutdown
!
context customerA
    allocate-interface gigabitethernet0/0 int1
    allocate-interface gigabitethernet0/1 int2
    allocate-interface management0/0 mgmt
context customerB
    allocate-interface gigabitethernet0/0
    allocate-interface gigabitethernet0/1
    allocate-interface management0/0
```

4단계 새 EtherChannel 또는 이중화 인터페이스를 사용할 *모든* 컨텍스트 컨피그레이션의 복사본을 가져옵니다.를 참조하십시오.37-20 페이지의 구성 또는 기타 파일 백업 및 복원

예를 들어, 다음과 같은 컨텍스트 컨피그레이션(표시되는 인터페이스 컨피그레이션)을 다운로드합니다.

CustomerA Context

```
interface int1
 nameif outside
 security-level 0
 ip address 10.86.194.225 255.255.255.0
!
interface int2
 nameif inside
 security-level 100
 ip address 192.168.1.3 255.255.255.0
 no shutdown
!
interface mgmt
 nameif mgmt
 security-level 100
 ip address 10.1.1.5 255.255.255.0
 management-only
```

CustomerB Context

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.20.15.5 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.6.78 255.255.255.0
!
interface Management0/0
 nameif mgmt
 security-level 100
 ip address 10.8.1.8 255.255.255.0
 management-only
```

5단계 시스템 컨피그레이션에서 10-17 페이지의 이중화 인터페이스 구성 또는 10-20 페이지의 EtherChannel 구성에 따라 새 논리적 인터페이스를 생성합니다. 논리적 인터페이스의 일부로 사용하려는 추가적인 물리적 인터페이스에 **no shutdown** 명령을 입력해야 합니다.

참고 EtherChannel 또는 이중화 인터페이스에는 *물리적* 인터페이스만 추가할 수 있으며, 물리적 인터페이스에는 VLAN을 구성할 수 없습니다.

정해진 EtherChannel 또는 이중화 인터페이스에서 모든 인터페이스의 물리적 인터페이스 매개변수(예: 속도 및 양방향)가 일치해야 합니다. EtherChannel 인터페이스의 양방향 설정은 Full 또는 Auto여야 합니다.

예를 들어, 새 컨피그레이션은 다음과 같습니다.

시스템

```
interface GigabitEthernet0/0
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/1
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/2
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/3
 channel-group 1 mode active
 no shutdown
!
interface GigabitEthernet0/4
 channel-group 2 mode active
 no shutdown
!
interface GigabitEthernet0/5
 channel-group 2 mode active
 no shutdown
!
interface Management0/0
 channel-group 3 mode active
 no shutdown
!
interface Management0/1
 channel-group 3 mode active
 no shutdown
!
interface port-channel 1
interface port-channel 2
interface port-channel 3
```

6단계 컨텍스트당 인터페이스 할당을 변경하여 새 EtherChannel 또는 이중화 인터페이스를 사용합니다. 7-19 페이지의 보안 컨텍스트 구성를 참조하십시오.

예를 들어, 기존 케이블 연결을 활용하려는 경우 기존 역할에서 이전에 사용 중인 인터페이스를 내부 및 외부 이중화 인터페이스의 일부로 계속 사용할 수 있습니다.

```
context customerA
    allocate-interface port-channel1 int1
    allocate-interface port-channel2 int2
    allocate-interface port-channel3 mgmt
context customerB
    allocate-interface port-channel1
    allocate-interface port-channel2
    allocate-interface port-channel3
```

참고 매핑된 이름을 인터페이스에 아직 할당하지 않은 경우, 이 기회를 통해 이를 수행하고자 할 수 있습니다. 예를 들어, customerA의 컨피그레이션은 변경할 필요가 전혀 없으며 ASA에서 다시 적용하기만 하면 됩니다. 그러나 customerB 컨피그레이션의 경우에는 모든 인터페이스 ID를 변경해야 합니다. customerB에 매핑된 이름을 할당할 경우, 컨텍스트 컨피그레이션에서 인터페이스 ID를 변경해야 하는 것은 마찬가지이지만 매핑된 이름을 사용하면 나중에 인터페이스를 변경할 때 유용할 수 있습니다.

7단계 매핑된 이름을 사용하지 않는 컨텍스트의 경우 새 EtherChannel 또는 이중화 인터페이스 ID를 사용하도록 컨텍스트 컨피그레이션을 변경합니다. (매핑된 인터페이스 이름을 사용하는 컨텍스트는 변경할 필요가 없습니다.)

예:

CustomerB Context

```
interface port-channel1
 nameif outside
 security-level 0
 ip address 10.20.15.5 255.255.255.0
!
interface port-channel2
 nameif inside
 security-level 100
 ip address 192.168.6.78 255.255.255.0
!
interface port-channel3
 nameif mgmt
 security-level 100
 ip address 10.8.1.8 255.255.255.0
 management-only
```

8단계 새 컨텍스트 컨피그레이션 파일을 기존 파일에 복사합니다. 예를 들어, 플래시 메모리에 있는 컨텍스트의 경우 시스템에서 **Tools > File Management**를 선택하고 **File Transfer > Between Local PC and Flash**를 선택합니다. 이 도구를 사용하면 각 컨피그레이션 파일을 선택하고 이를 로컬 컴퓨터에 복사할 수 있습니다. 이러한 변경은 시작 컨피그레이션에만 영향을 미치며, 실행 중인 컨피그레이션에서는 기존 컨텍스트 컨피그레이션을 계속 사용합니다.

9단계 변경된 인터페이스 섹션을 포함하여 전체 새 시스템 컨피그레이션을 클립보드에 복사합니다.

10단계 ASDM에서 **Tools > Command Line Interface**를 선택하고 **Multiple Line** 라디오 버튼을 클릭합니다.

11단계 **clear configure all**을 첫 번째 행으로 선택하고 그 뒤에 새 컨피그레이션을 붙여넣은 다음 **Send**를 클릭합니다. **clear** 명령을 사용하면 새 컨피그레이션을 적용하기 전에 실행 중인 컨피그레이션(시스템 및 컨텍스트 모두)이 지워집니다.

이 경우 ASA를 통한 트래픽이 중단됩니다. 모든 새 컨텍스트 컨피그레이션이 다시 로드됩니다. 다시 로드하는 작업이 완료되면 ASA를 통한 트래픽이 다시 시작됩니다.

12단계 Command Line Interface 대화 상자를 닫고 **File > Refresh ASDM with the Running Configuration**을 선택합니다.

13단계 **Configuration > Device Management > High Availability > Failover**를 선택하고 **Enable failover** 확인란을 선택하여 장애 조치를 다시 활성화합니다. 기본 장애 조치 설정을 구성하려는 경우 **Apply**를 클릭하고 메시지가 표시되면 **No**를 클릭합니다.

인터페이스 모니터링

- 12-21 페이지의 ARP 테이블를 참조하십시오.
- 12-24 페이지의 MAC 주소 테이블를 참조하십시오.
- 12-24 페이지의 인터페이스 그래프를 참조하십시오.

다음으로 살펴볼 내용

- 다중 컨텍스트 모드의 경우:
  a. 인터페이스를 컨텍스트에 할당하고 고유한 MAC 주소를 컨텍스트 인터페이스에 자동으로 할당합니다. 7 장, “다중 컨텍스트 모드”.를 참조하십시오.
  b. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.에 따라 인터페이스 컨피그레이션을 완료합니다.
- 단일 컨텍스트 모드의 경우, 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.에 따라 인터페이스 컨피그레이션을 완료합니다.

ASA 5512-X 이상 버전의 인터페이스 기능 기록

표 10-2에서는 이 기능의 출시 내역을 정리합니다.

표 10-2 인터페이스의 기능 기록

기능 이름	릴리스	기능 정보
VLAN 증가	7.0(5)	다음 한도를 높였습니다. • ASA5510 Base 라이센스의 VLAN을 0개에서 10개로 • ASA5510 Security Plus 라이센스의 VLAN을 10개에서 25개로 • ASA5520 VLAN을 25개에서 100개로 • ASA5540 VLAN을 100개에서 200개로
ASA 5510의 Base 라이센스 인터페이스 증가	7.2(2)	ASA 5510의 Base 라이센스의 경우, 인터페이스의 최대 수가 3개에서 관리 인터페이스까지 추가하여 무제한 인터페이스로 증가했습니다.
VLAN 증가	7.2(2)	ASA 5510(Base 라이센스는 10에서 50으로, Security Plus 라이센스는 25에서 100으로), ASA 5520(100에서 150으로), ASA 5550(200에서 250으로)의 VLAN 제한이 증가했습니다.
ASA 5510 Security Plus 라이센스의 기가비트 이더넷 지원	7.2(3)	이제 ASA 5510 ASA에서는 Security Plus 라이센스와 함께 포트 0 및 1에 GE(기가비트 이더넷)를 지원합니다. Base 라이센스를 Security Plus 라이센스로 업그레이드할 경우 외부 Ethernet0/0 및 Ethernet0/1 포트의 용량이 원래의 FE(패스트 이더넷)(100Mbps)에서 GE(1000Mbps)로 증가합니다. 인터페이스 이름은 그대로 Ethernet 0/0 및 Ethernet 0/1입니다.

표 10-2 인터페이스의 기능 기록 (계속)

기능 이름	릴리스	기능 정보
이중 인터페이스	8.0(2)	논리적 이중화 인터페이스에서는 액티브와 스탠바이 물리적 인터페이스를 쌍으로 묶습니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중화 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중화 인터페이스와 함께 장애 조치를 구성할 수 있습니다. 최대 8개의 이중화 인터페이스 쌍을 구성할 수 있습니다.
ASA 5580의 점보 패킷 지원	8.1(1)	Cisco ASA 5580은 점보 프레임을 지원합니다. 점보 프레임은 표준 최대 크기인 1518바이트(레이어 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷으로 최대 크기가 9216바이트입니다. 모든 인터페이스에서 이더넷 프레임 처리용 메모리 용량을 늘려 점보 프레임 지원을 활성화할 수 있습니다. 점보 프레임에 더 많은 메모리를 할당하면 ACL와 같은 다른 기능을 최대 한도로 사용하는 데 제약이 따를 수 있습니다. 또한 이 기능은 ASA 5585-X에서도 지원됩니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced
ASA 5580의 VLAN 증가	8.1(2)	ASA 5580에서 지원되는 VLAN 수가 100개에서 250개로 늘어났습니다.
ASA 5580 10기가비트 이더넷 인터페이스에서 흐름 제어를 위한 일시 중지 프레임 지원	8.2(2)	흐름 제어를 위해 Pause(XOFF) 프레임을 활성화할 수 있습니다. 또한 이 기능은 ASA 5585-X에서도 지원됩니다. 다음 화면을 수정했습니다. (단일 모드) Configuration > Device Setup > Interfaces > Add/Edit Interface > General (다중 모드, 시스템) Configuration > Interfaces > Add/Edit Interface
기가비트 이더넷 인터페이스에서 흐름 제어를 위한 일시 중지 프레임 지원	8.2(5)/8.4(2)	이제 모든 모델에서 기가비트 이더넷 인터페이스에 흐름 제어를 위한 일시 중지(XOFF) 프레임을 사용할 수 있습니다. 다음 화면을 수정했습니다. (단일 모드) Configuration > Device Setup > Interfaces > Add/Edit Interface > General (다중 모드, 시스템) Configuration > Interfaces > Add/Edit Interface

표 10-2 인터페이스의 기능 기록 (계속)

기능 이름	릴리스	기능 정보
EtherChannel 지원	8.4(1)	8개의 액티브 인터페이스마다 최대 48개의 802.3ad EtherChannel을 구성할 수 있습니다. 다음 화면을 수정하거나 도입했습니다. Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit EtherChannel Interface Configuration > Device Setup > Interfaces > Add/Edit Interface Configuration > Device Setup > EtherChannel **참고** EtherChannel은 ASA 5505에서 지원되지 않습니다.
EtherChannel에 16개의 액티브 링크 지원	9.2(1)	이제 EtherChannel에서 최대 16개의 액티브 링크를 구성할 수 있습니다. 이전에는 액티브 링크 8개와 스탠바이 링크 8개를 구성할 수 있었습니다. 스위치에서 16개의 액티브 링크를 지원하는지 확인하십시오(예: F2-Series 10 기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000). **참고** 이전 ASA 버전에서 업그레이드할 경우 호환성을 위해 액티브 인터페이스의 최대 수는 8개로 설정됩니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Interfaces > Add/Edit EtherChannel Interface > Advanced

기본 인터페이스 구성(ASAv)

이 장에서는 이더넷 설정, 이중화 인터페이스, VLAN 하위 인터페이스를 비롯한 Cisco ASAv의 인터페이스 컨피그레이션을 시작하는 작업에 대한 내용이 포함되어 있습니다.

ASAv 인터페이스 구성 시작 정보

ASAv 인터페이스 및 가상 NIC

가상화 플랫폼의 게스트인 ASAv에서는 기본 물리적 플랫폼의 네트워크 인터페이스를 활용합니다. 각 ASAv 인터페이스는 가상 NIC(vNIC)에 매핑됩니다.

ASAv 인터페이스

ASAv에는 다음과 같은 기가비트 이더넷 인터페이스가 포함되어 있습니다.

- Management 0/0
- GigabitEthernet 0/0에서 0/8까지 포함. GigabitEthernet 0/8은 ASAv를 장애 조치 페어의 일부분으로 구축할 경우 장애 조치 링크에 사용됩니다.

지원되는 vNIC

ASAv에서는 다음 vNIC를 지원합니다.

vNIC 유형	하이퍼바이저 지원		ASAv 버전	참고
	VMWare	KVM		
VMXNET3	예	아니요	9.2(1) 이상	VMXNET3을 사용할 경우 LRO(Large Receive Offload)을 비활성화하여 TCP 성능 저하를 방지해야 합니다. 다음 VMware 지원 문서를 참조하십시오. http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1027511 http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=2055140
e1000	예	예	9.2(1) 이상	9.3(1) 이하 버전의 .

VMware에서 vNIC와 ASAv의 인터페이스 일치

vSphere Client Virtual Machine Properties 화면(ASAv 인스턴스를 마우스 오른쪽 버튼으로 클릭하고 **Edit Settings** 선택)에는 각 네트워크 어댑터 및 할당된 네트워크가 표시됩니다. 그러나 이 화면에 ASAv 인터페이스 ID는 표시되지 않습니다(네트워크 어댑터 ID만 표시). 네트워크 어댑터 ID와 ASAv ID는 다음과 같이 상호 일치된다는 점을 참조하십시오.

네트워크 어댑터 ID	ASAv 인터페이스 ID
네트워크 어댑터 1	Management 0/0
네트워크 어댑터 2	GigabitEthernet0/0
네트워크 어댑터 3	GigabitEthernet0/1
네트워크 어댑터 4	GigabitEthernet0/2
네트워크 어댑터 5	GigabitEthernet0/3
네트워크 어댑터 6	GigabitEthernet0/4
네트워크 어댑터 7	GigabitEthernet0/5
네트워크 어댑터 8	GigabitEthernet0/6
네트워크 어댑터 9	GigabitEthernet0/7
네트워크 어댑터 10	GigabitEthernet0/8

투명 모드의 인터페이스

투명 모드의 인터페이스는 "브릿지 그룹"에 속하며, 각 네트워크에 하나의 브릿지 그룹이 있습니다. 인터페이스 4개당 최대 8개의 브릿지가 포함될 수 있습니다. 브릿지 그룹에 대한 자세한 내용은 13-1 페이지의 투명 모드의 브리지 그룹를 참조하십시오.

관리 인터페이스

관리 인터페이스 개요

다음에 연결하여 ASA를 관리할 수 있습니다.

- 통과 트래픽 인터페이스
- 전용 Management 0/0 인터페이스

36 장, “관리 액세스”.에 따라 인터페이스에 대한 관리 액세스를 구성해야 할 수 있습니다.

관리 전용 트래픽에 모든 인터페이스 사용

모든 인터페이스를 관리 트래픽용으로 구성하여 이를 관리 전용 인터페이스로 사용할 수 있습니다.

투명 모드의 관리 인터페이스

투명 방화벽 모드에서는 최대 허용되는 통과 트래픽 인터페이스 외에도, Management 0/0 인터페이스(물리적 인터페이스 또는 하위 인터페이스)를 별도의 관리 인터페이스로 사용할 수도 있습니다. 다른 기타 인터페이스 유형은 관리 인터페이스로 사용할 수 없습니다. 관리 인터페이스는 일반적인 브릿지 그룹에 포함되지 않습니다. 운영상의 용도로 인해 관리 인터페이스는 구성 불가능한 브릿지 그룹에 포함됩니다.

참고 투명 방화벽 모드의 경우 관리 인터페이스에서는 MAC 주소 테이블을 데이터 인터페이스와 같은 방식으로 업데이트합니다. 따라서 스위치 포트 중 하나를 라우팅 포트로 구성하지 않는 한 관리 인터페이스와 데이터 인터페이스 두 가지 모두를 같은 스위치에 연결해서는 안 됩니다(기본적으로 Catalyst 스위치에서는 모든 VLAN 스위치 포트에 대한 MAC 주소를 공유함). 그렇지 않을 경우 트래픽이 물리적으로 연결된 스위치에서 관리 인터페이스에 전달되면 ASA에서는 데이터 인터페이스 대신 *관리* 인터페이스를 사용하여 스위치에 액세스하도록 액세스 MAC 주소 테이블을 업데이트합니다. 이 작업으로 인해 일시적인 트래픽 중단이 발생합니다. ASA에서는 보안상의 이유로 인해 스위치에서 데이터 인터페이스로 전달되는 패킷의 MAC 주소 테이블을 최소 30초간 다시 업데이트하지 않습니다.

통과 트래픽 지원되지 않음

Management 0/0 인터페이스는 항상 관리 전용으로 설정되며, 이 인터페이스는 통과 트래픽을 지원하는 용도로 사용할 수 없습니다.

이중화 인터페이스

논리적 이중화 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중화 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중화 인터페이스와 함께 디바이스 수준 장애 조치를 구성할 수 있습니다.

이중화 인터페이스 MAC 주소

이중화 인터페이스에서는 맨 처음 추가되는 물리적 인터페이스의 MAC 주소를 사용합니다. 컨피그레이션에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 또는 멤버 인터페이스 MAC 주소에 관계없이 사용되는 이중화 인터페이스에 MAC 주소를 할당할 수 있습니다(12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성 또는 7-15 페이지의 다중 컨텍스트 모드 구성 참조). 액티브 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작하면 같은 MAC 주소가 유지되므로 트래픽이 중단되지 않습니다.

MTU 및 TCP 최대 세그먼트 크기로 조각화 제어

MTU 개요

MTU에서는 ASA가 지정된 이더넷 인터페이스에서 전송할 수 있는 최대 프레임 페이로드 크기를 지정합니다. MTU 값은 이더넷 헤더, FCS 또는 VLAN 태깅이 *없는* 프레임 크기입니다. 이더넷 헤더는 14바이트이고 FCS는 4바이트입니다. MTU를 1500으로 설정할 경우 예상 프레임 크기는 헤더를 포함하여 1518바이트입니다. VLAN 태깅(4바이트가 더 추가됨)을 사용 중인 상태에서 MTU를 1500으로 설정할 경우 예상 프레임 크기는 1522입니다. 이러한 헤더를 수용하기 위해 MTU 값을 이보다 더 높게 설정하지 마십시오. MTU 설정을 변경하는 대신 MTU 최대 세그먼트 크기를 변경하여 캡슐화를 위한 TCP 헤더를 수용하는 방법에 대한 자세한 내용은 11-5 페이지의 TCP 최대 세그먼트 크기 개요를 참조하십시오.

참고 ASA에서는 메모리에 공간이 있는 한 구성된 MTU보다 큰 프레임을 수신할 수 있습니다. 큰 프레임을 지원하기 위해 메모리를 늘리는 방법은 11-15 페이지의 점보 프레임 지원 활성화를 참조하십시오.

기본 MTU

ASA의 기본 MTU는 1500바이트입니다. 이 값에는 18바이트 이상의 이더넷 헤더, CRC, VLAN 태깅 등이 포함되지 않습니다.

경로 MTU 검색

ASA에서는 경로 MTU 검색을 지원하며(RFC 1191에 규정), 이 기능을 사용하면 두 호스트 간의 네트워크 경로에 있는 모든 디바이스에서 MTU를 조율할 수 있으므로, 경로의 최저 MTU에 대한 표준을 설정할 수 있습니다.

MTU 및 점보 프레임 설정

12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성를 참조하십시오.

11-15 페이지의 점보 프레임 지원 활성화를 참조하십시오.

다음 지침을 참조하십시오.

- 트래픽 경로의 MTU 일치 — 모든 ASA 인터페이스 및 기타 디바이스 인터페이스의 MTU를 트래픽 경로와 동일하게 설정하는 것이 좋습니다. MTU를 일치시키면 패킷 분할 시 디바이스가 중간에 끼어드는 현상을 방지할 수 있습니다.
- 점보 프레임 수용 — 점보 프레임을 활성화할 경우, MTU를 최대 9000바이트까지 설정할 수 있습니다.

TCP 최대 세그먼트 크기 개요

TCP MSS(TCP 최대 세그먼트 크기)는 TCP 헤더가 추가되기 *전의* TCP 페이로드의 크기입니다. UDP 패킷은 영향을 받지 않습니다. 연결을 설정할 경우 클라이언트와 서버에서는 3방향 핸드셰이크 동안 TCP MSS 값을 교환합니다.

ASA에서 TCP MSS를 설정할 수 있습니다. 연결의 엔드포인트에서 ASA에 설정된 값보다 큰 TCP MSS를 요청할 경우, ASA에서는 요청 패킷의 TCP MSS를 ASA 최대값으로 덮어씁니다. 호스트 또는 서버에서 TCP MSS를 요청하지 않을 경우 ASA에서는 RFC 793 기본값을 536바이트로 추정하며 패킷을 수정하지 않습니다. 또한 최소 TCP MSS를 구성할 수 있습니다. 호스트 또는 서버에서 요청한 TCP MSS가 매우 작을 경우, ASA에서는 값을 조정하여 올릴 수 있습니다. 기본적으로 최소 TCP MSS는 활성화되어 있지 않습니다.

기본값이 1500바이트인 MTU를 구성하는 경우를 예로 들어보겠습니다. 호스트에서는 값이 1700인 MSS를 요청합니다. ASA 최대 TCP MSS가 1380이면 ASA에서는 TCP 요청 패킷의 MSS 값을 1380으로 변경합니다. 그러면 서버에서는 1380바이트 패킷을 전송합니다.

기본 TCP MSS

기본적으로 ASA의 최대 TCP MSS는 1380바이트 입니다. 이러한 기본값을 사용하면 헤더에 120바이트를 추가할 수 있는 경우 VPN 연결을 수용하는 것이 가능합니다. 이 값은 기본값이 1500바이트인 MTU에 적합합니다.

VPN 및 비 VPN 트래픽의 TCP MSS 설정

12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성를 참조하십시오.

다음 지침을 참조하십시오.

- 비 VPN 트래픽 — VPN을 사용하지 않고 헤더에 추가 공간이 필요하지 않은 경우, TCP MSS 제한을 비활성화하고 연결과 엔드포인트 간에 설정된 값을 승인해야 합니다. 연결 엔드포인트의 경우 대개 MTU에서 TCP MSS가 파생되므로 비 VPN 패킷은 일반적으로 이러한 TCP MSS에 적합합니다.
- VPN 트래픽 — MTU에 대한 최대 TCP MSS를 120으로 설정합니다. 예를 들어, 점보 프레임을 사용하고 MTU를 더 높은 값으로 설정할 경우 새로운 MTU를 수용할 수 있는 TCP MSS를 설정해야 합니다.

ASAv 인터페이스의 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv - 가상 CPU 1개 포함	VLAN: Standard 및 Premium 라이센스: 50 모든 유형의 인터페이스: Standard 및 Premium 라이센스: 716
ASAv - 가상 CPU 4개 포함	VLAN: Standard 및 Premium 라이센스: 200 모든 유형의 인터페이스: Standard 및 Premium 라이센스: 1316

참고 어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다.

모든 유형의 인터페이스는 통합된 인터페이스의 최대 개수로 구성되며 여기에는 VLAN, 물리적, 이중화, 브릿지 그룹 인터페이스가 해당됩니다. 컨피그레이션에 정의된 모든 **interface**은 이 한도의 대상이 됩니다.

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

방화벽 모드 지침

- 투명 모드의 경우 최대 8개의 브릿지 그룹을 구성할 수 있습니다.
- 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다.

장애 조치 지침

- 이중화 인터페이스를 장애 조치 링크로 사용할 경우, 장애 조치 쌍의 두 유닛에 모두 이를 구성해야 합니다. *복제를 위해서는 장애 조치 링크 자체가 필요하므로* 이중화 인터페이스를 기본 유닛에 구성한 다음 이를 보조 유닛에 복제할 수 없습니다.
- 상태 링크에 이중화 인터페이스를 사용할 경우, 특별한 컨피그레이션이 필요하지 않으며 컨피그레이션을 기본 유닛에서 정상적으로 복제할 수 있습니다.
- **monitor-interface**. 액티브 멤버 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작할 경우, 디바이스 수준 장애 조치가 모니터링되고 있으면 이 작업을 수행해도 이중화 인터페이스에 오류가 발생하는 것으로 나타나지 않습니다. 모든 물리적 인터페이스에 오류가 발생한 경우에만 이중화 인터페이스에 오류가 발생하는 것으로 나타납니다.
- 장애 조치 또는 상태 인터페이스는 데이터 인터페이스와 공유할 수 없습니다.

이중화 인터페이스 지침

- 최대 8개의 이중화 인터페이스 쌍을 구성할 수 있습니다.
- 모든 ASA 컨피그레이션에서는 컨피그레이션원 물리적 인터페이스 대신 논리적 이중화 인터페이스를 참조합니다.
- 액티브 인터페이스를 종료할 경우 스탠바이 인터페이스가 액티브 상태로 됩니다.
- 이중화 인터페이스는 관리 전용으로 설정할 수 없습니다.
- 장애 조치 지침에 대한 내용은 11-7 페이지의 장애 조치 지침를 참조하십시오.

기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다. 공장 기본 컨피그레이션에 대한 자세한 내용은 2-15 페이지의 공장 기본 구성를 참조하십시오.

인터페이스의 기본 상태

- 물리적 인터페이스 — 비활성화되어 있습니다.
- 이중화 인터페이스 — 활성화되어 있습니다. 그러나 이중화 인터페이스를 통해 트래픽을 전달하려면 멤버 물리적 인터페이스도 활성화되어야 합니다.
- 하위 인터페이스 — 활성화되어 있습니다. 그러나 하위 인터페이스를 통해 트래픽을 전달하려면 물리적 인터페이스도 활성화되어야 합니다.

기본 속도와 양방향

- 기본적으로 인터페이스의 속도와 양방향은 자동 협상이 이루어지도록 설정됩니다.

기본 MAC 주소

기본적으로 물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.

기본 vNIC

모든 인터페이스에서는 E1000 에뮬레이션을 사용합니다.

인터페이스 구성 시작(ASAv)

인터페이스 구성 시작을 위한 작업 흐름

인터페이스 구성을 시작하려면 다음 단계를 수행합니다.

1단계 물리적 인터페이스를 활성화하고 선택에 따라 이더넷 매개변수를 변경합니다. 11-8 페이지의 물리적 인터페이스 활성화 및 이더넷 매개변수 구성를 참조하십시오.

물리적 인터페이스는 기본적으로 비활성화되어 있습니다.

2단계 (선택 사항) 이중화 인터페이스 쌍을 구성합니다. 11-11 페이지의 이중화 인터페이스 구성를 참조하십시오.

논리적 이중화 인터페이스에서는 액티브와 스탠바이 물리적 인터페이스를 쌍으로 묶습니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다.

3단계 (선택 사항) VLAN 하위 인터페이스를 구성합니다. 11-13 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹를 참조하십시오.

4단계 (선택 사항) 11-15 페이지의 점보 프레임 지원 활성화에 따라 점보 프레임 지원을 활성화합니다.

물리적 인터페이스 활성화 및 이더넷 매개변수 구성

이 섹션에서는 다음을 수행하는 방법을 설명합니다.

- 물리적 인터페이스 활성화
- 특정 속도 및 양방향 설정
- 흐름 제어를 위한 일시 중지 프레임 활성화

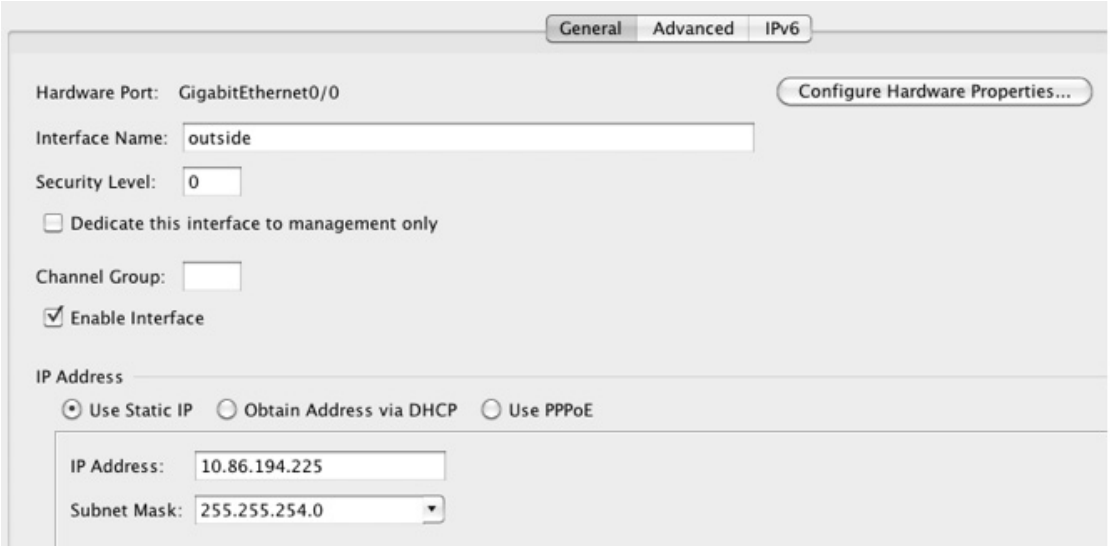
세부 단계

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

기본적으로 모든 물리적 인터페이스가 나열됩니다.

2단계 구성할 물리적 인터페이스를 클릭하고 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 나타납니다.



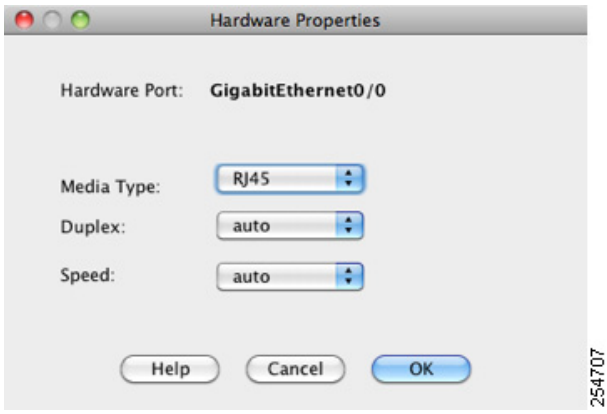
참고 이 절차에서는 Edit Interface 대화 상자의 매개변수 하위 집합에 대해서만 다룹니다. 다른 매개변수를 구성하려면 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

3단계 인터페이스를 활성화하려면 **Enable Interface** 확인란을 선택합니다.

4단계 설명을 추가하려면 Description 필드에 텍스트를 입력합니다.

설명은 줄 바꿈 없이 1줄, 최대 240자로 작성합니다. 장애 조치 또는 상태 링크의 경우 이 설명은 “LAN Failover Interface”, “STATE Failover Interface” 또는“LAN/STATE Failover Interface”와 같이 고정되어 있습니다. 이 설명을 수정할 수 없습니다. 이 인터페이스를 장애 조치 또는 상태 링크로 만들 경우 고정된 설명이 사용자가 여기에 입력한 설명을 덮어씁니다.

5단계 (선택 사항) 미디어 유형, 양방향을 설정하고 흐름 제어에 대한 일시 중지 프레임을 활성화하려면 **Configure Hardware Properties**를 클릭합니다.



참고 Media Type은 항상 RJ-45입니다.

a. RJ-45 인터페이스에 양방향을 설정하려면 인터페이스 유형에 따라 Duplex 드롭다운 목록에서 **Full**, **Half** 또는 **Auto**를 선택합니다.

b. 속도를 설정하려면 Speed 드롭다운 목록에서 값을 선택합니다.

c. **OK**를 클릭하여 Hardware Properties 변경 사항을 승인합니다.

d. 흐름 제어에 일시 중지(XOFF) 프레임을 활성화하려면 **Enable Pause Frame** 확인란을 선택합니다.

트래픽 버스트가 있을 경우 이러한 버스트가 NIC에서 FIFO 버퍼의 버퍼링 용량을 초과하고 링 버퍼를 수신하면 패킷 손실이 발생할 수 있습니다. 흐름 제어를 위한 일시 중지 프레임을 활성화하면 이러한 문제를 완화할 수 있습니다. 일시 중지(XOFF) 및 XON 프레임은 FIFO 버퍼 사용량을 기준으로 NIC 하드웨어에서 자동으로 생성됩니다. 일시 중지 프레임은 버퍼 사용량이 최고 수위를 넘을 때 전송됩니다. 기본 *high_water* 값은 24KB이며 이를 0~47KB 사이로 설정할 수 있습니다. 일시 중지를 보낸 후 버퍼 사용량이 최저 수위 이하로 감소할 경우 XON 프레임이 전송될 수 있습니다. 기본적으로 *low_water* 값은 16KB이며 이를 0~47KB 사이로 설정할 수 있습니다. XON이 수신된 후 또는 XOFF가 만료된 후, 일시 중지 프레임의 타이머 값에서 제어하는 대로 링크 파트너를 다시 시작할 수 있습니다. 기본 *pause_time* 값은 26624이며 이를 0~65535 사이로 설정할 수 있습니다. 버퍼 사용량이 지속적으로 최고 수위를 넘을 경우, 일시 중지 프레임이 반복해서 전송되며 이는 일시 중지 새로 고침 임계값에 의해 제어됩니다.

Low Watermark, High Watermark, Pause Time의 기본값을 변경하려면 **Use Default Values** 확인란의 선택을 취소합니다.

참고 802.3x에 정의된 흐름 제어 프레임만 지원됩니다. 우선순위를 기반으로 하는 흐름 제어는 지원되지 않습니다.

6단계 **OK**를 클릭하여 Interface 변경 사항을 승인합니다.

다음에 할 일

선택적 작업:

- 이중화 인터페이스 쌍을 구성합니다. 11-11 페이지의 이중화 인터페이스 구성를 참조하십시오.
- VLAN 하위 인터페이스를 구성합니다. 11-13 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹를 참조하십시오.
- 점보 프레임 지원을 구성합니다. 11-15 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 인터페이스 컨피그레이션을 완료합니다. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

이중화 인터페이스 구성

논리적 이중화 인터페이스는 액티브 인터페이스와 스탠바이 인터페이스라는 물리적 인터페이스 한 쌍으로 구성됩니다. 액티브 인터페이스에 오류가 발생할 경우, 스탠바이 인터페이스가 액티브 상태로 전환되며 트래픽 통과를 시작합니다. 이중화 인터페이스를 구성하여 ASA의 안정성을 높일 수 있습니다. 이 기능은 디바이스 수준 장애 조치와는 관련이 없으나, 필요한 경우 이중화 인터페이스와 함께 장애 조치를 구성할 수 있습니다.

이 섹션에서는 이중화 인터페이스를 구성하는 방법에 대해 설명합니다.

- 11-11 페이지의 이중화 인터페이스 구성
- 11-13 페이지의 액티브 인터페이스 변경

이중화 인터페이스 구성

이 섹션에서는 이중화 인터페이스를 생성하는 방법에 대해 설명합니다. 기본적으로 이중화 인터페이스는 활성화되어 있습니다.

지침 및 제한 사항

- 최대 8개의 이중화 인터페이스 쌍을 구성할 수 있습니다.
- 이중화 인터페이스 지연 값은 구성 가능하나, 기본적으로 ASA에서는 멤버 인터페이스의 물리적 유형을 기준으로 기본 지연 값을 상속합니다.
- 11-7 페이지의 이중화 인터페이스 지침도 참조하십시오.

전제 조건

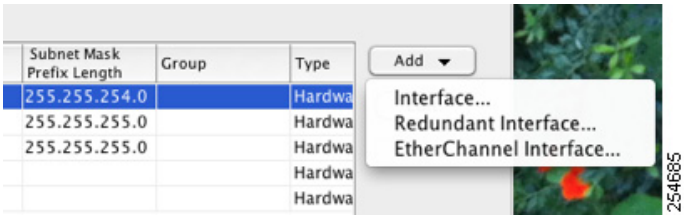
- 두 인터페이스 모두 물리적 유형이 같아야 합니다. 예를 들어, 모두 GigabitEthernet이어야 합니다.
- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 이중화 인터페이스에 추가할 수 없습니다. Configuration > Device Setup > Interfaces 창에서을 사용하여 우선 이름을 제거해야 합니다.

주의 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

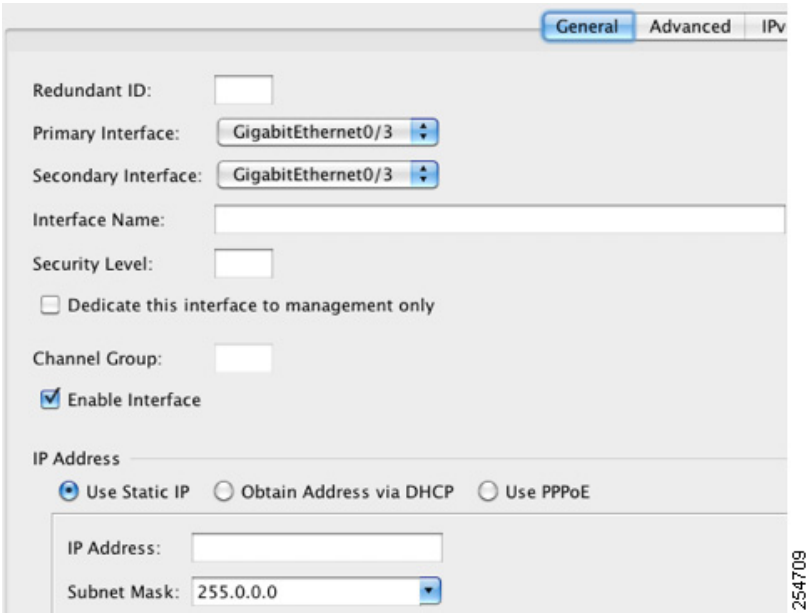
세부 단계

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 **Add > Redundant Interface**를 선택합니다.



Add Redundant Interface 대화 상자가 나타납니다.



참고 이 절차에서는 Edit Redundant Interface 대화 상자의 매개변수 하위 집합에 대해서만 다룹니다. 다른 매개변수를 구성하려면 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

3단계 Redundant ID 필드에 1~8 사이의 정수를 입력합니다.

4단계 Primary Interface 드롭다운 목록에서 기본으로 설정하려는 물리적 인터페이스를 선택합니다.

하위 인터페이스가 없고 컨텍스트에 할당되지 않은 인터페이스를 선택해야 합니다.

5단계 Secondary Interface 드롭다운 목록에서 보조로 설정하려는 물리적 인터페이스를 선택합니다.

6단계 인터페이스가 아직 활성화되지 않은 경우 **Enable Interface** 확인란을 선택합니다.

인터페이스는 기본적으로 활성화되어 있습니다. 비활성화하려면 확인란의 선택을 취소합니다.

7단계 설명을 추가하려면 Description 필드에 텍스트를 입력합니다.

설명은 줄 바꿈 없이 1줄, 최대 240자로 작성합니다. 장애 조치 또는 상태 링크의 경우 이 설명은 “LAN Failover Interface”, “STATE Failover Interface” 또는“LAN/STATE Failover Interface”와 같이 고정되어 있습니다. 이 설명을 수정할 수 없습니다. 이 인터페이스를 장애 조치 또는 상태 링크로 만들 경우 고정된 설명이 사용자가 여기에 입력한 설명을 덮어씁니다.

8단계 **OK**를 클릭합니다.

Interfaces 창으로 돌아갑니다. 이제 멤버 인터페이스를 보면 인터페이스 ID의 왼쪽에 자물쇠가 표시되며, 이는 해당 인터페이스에 기본 매개변수만 구성할 수 있음을 나타냅니다. 이중화 인터페이스가 테이블에 추가됩니다.

GigabitEthernet0/2	Enabled	No	Redundant8	Hardware	native
GigabitEthernet0/3	Enabled	No		Hardware	native
GigabitEthernet0/3.10	Enabled	No		Logical	vlan100
GigabitEthernet0/3.11	Enabled	No		Logical	vlan11
Management0/0	Enabled	No		Hardware	native
Redundant8	Enabled	Yes		Logical	native

254710

다음에 할 일

선택적 작업:

- VLAN 하위 인터페이스를 구성합니다. 11-13 페이지의 VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹를 참조하십시오.
- 점보 프레임 지원을 구성합니다. 11-15 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 인터페이스 컨피그레이션을 완료합니다. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

액티브 인터페이스 변경

기본적으로, 액티브 인터페이스는 컨피그레이션에 나열된 사용 가능한 첫 번째 인터페이스입니다. 어떤 인터페이스가 액티브인지 보려면 Tools > Command Line Interface 툴에 다음 명령을 입력합니다.

show interface redundant*number* **detail | grep Member**

예:

```
show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

액티브 인터페이스를 변경하려면 다음 명령을 입력합니다.

redundant-interface redundant*number* **active-member** *physical_interface*

redundant*number* 인수는 이중화 인터페이스 ID(예: **redundant1**)입니다.

*physical_interface*는 액티브 인터페이스로 변경하려는 멤버 인터페이스 ID입니다.

VLAN 하위 인터페이스 구성 및 802.1Q 트렁킹

하위 인터페이스를 사용하면 물리적 또는 이중화 인터페이스를 다른 VLAN ID가 태그 처리된 여러 논리적 인터페이스로 분할할 수 있습니다. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다. VLAN을 사용하면 정해진 물리적 인터페이스에서 트래픽을 따로 유지할 수 있으므로, 추가적인 물리적 인터페이스 또는 ASA를 추가하지 않고 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 있습니다.

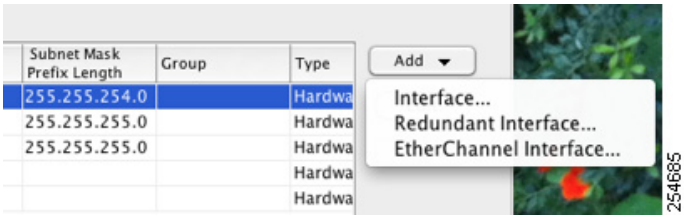
지침 및 제한 사항

- 최대 하위 인터페이스 — 모델에 사용 가능한 최대 VLAN 하위 인터페이스 수를 확인하려면 11-6 페이지의 ASAv 인터페이스의 라이센스 요구 사항를 참조하십시오.
- 물리적 인터페이스의 태그 처리되지 않은 패킷 방지 — 하위 인터페이스를 사용할 경우, 일반적으로 물리적 인터페이스에서 트래픽을 전달하지 않도록 하고자 합니다. 물리적 인터페이스에서는 태그 처리되지 않은 패킷을 전달하기 때문입니다. 이러한 속성은 이중화 인터페이스 쌍의 액티브 물리적 인터페이스에서도 마찬가지입니다. 하위 인터페이스에서 트래픽을 전달하려면 물리적 또는 이중화 인터페이스를 활성화해야 하므로, 인터페이스의 이름을 구성하지 않고 물리적 또는 이중화 인터페이스에서 태그 처리되지 않은 패킷을 전달하는 것을 허용하려면 name을 정상적으로 구성합니다. 인터페이스 컨피그레이션 완료에 대한 자세한 내용은 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”,를 참조하십시오.

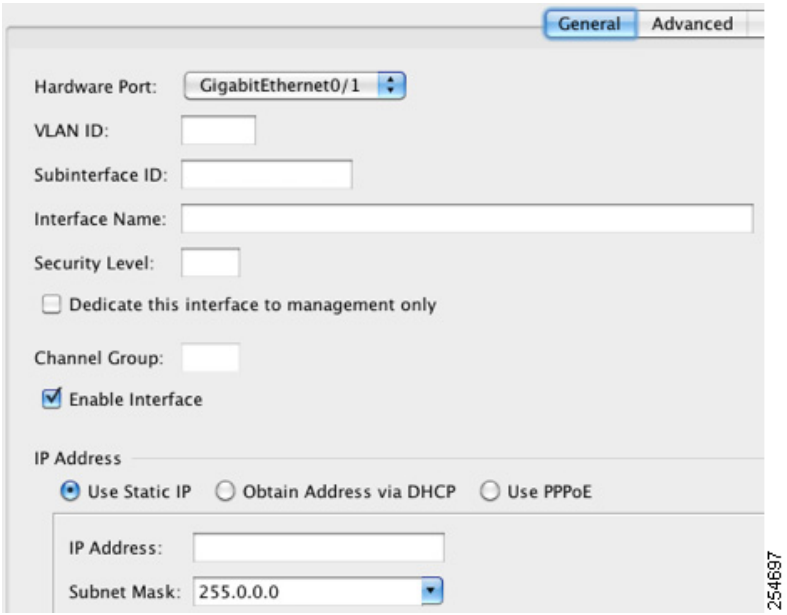
세부 단계

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 **Add > Interface**를 선택합니다.



Add Interface 대화 상자가 나타납니다.



참고 이 절차에서는 Edit Interface 대화 상자의 매개변수 하위 집합에 대해서만 다룹니다. 다른 매개변수를 구성하려면 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”. 를 참조하십시오.

3단계 Hardware Port 드롭다운 목록에서 하위 인터페이스를 추가할 물리적 또는 이중화 인터페이스를 선택합니다.

4단계 인터페이스가 아직 활성화되지 않은 경우 **Enable Interface** 확인란을 선택합니다.

인터페이스는 기본적으로 활성화되어 있습니다. 비활성화하려면 확인란의 선택을 취소합니다.

5단계 VLAN ID 필드에 1~4095 사이의 VLAN ID를 입력합니다.

일부 VLAN ID의 경우 연결된 스위치에서 예약될 수 있으므로, 자세한 내용을 보려면 스위치 설명서를 선택하십시오.

6단계 Subinterface ID 필드에 하위 인터페이스 ID를 1~4294967293 사이의 정수로 입력합니다.

허용되는 하위 인터페이스의 개수는 플랫폼에 따라 다릅니다. 다음을 설정한 후에는 ID를 변경할 수 없습니다.

7단계 (선택 사항) Description 필드에 이 인터페이스에 대한 설명을 입력합니다.

설명은 줄 바꿈 없이 1줄, 최대 240자로 작성합니다. 장애 조치 또는 상태 링크의 경우 이 설명은 “LAN Failover Interface”, “STATE Failover Interface” 또는“LAN/STATE Failover Interface”와 같이 고정되어 있습니다. 이 설명을 수정할 수 없습니다. 이 인터페이스를 장애 조치 또는 상태 링크로 만들 경우 고정된 설명이 사용자가 여기에 입력한 설명을 덮어씁니다.

8단계 **OK**를 클릭합니다.

Interfaces 창으로 돌아갑니다.

다음에 할 일

선택적 작업:

- 점보 프레임 지원을 구성합니다. 11-15 페이지의 점보 프레임 지원 활성화를 참조하십시오.

필수 작업:

- 인터페이스 컨피그레이션을 완료합니다. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

점보 프레임 지원 활성화

점보 프레임은 최대 표준 1518바이트(레이어 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷이며, 최대 9216바이트에 이릅니다. 모든 인터페이스에서 이더넷 프레임 처리용 메모리 용량을 늘려 점보 프레임 지원을 활성화할 수 있습니다. 점보 프레임에 더 많은 메모리를 할당하면 ACL와 같은 다른 기능을 최대 한도로 사용하는 데 제약이 따를 수 있습니다. 자세한 내용은 11-4 페이지의 MTU 및 TCP 최대 세그먼트 크기로 조각화 제어를 참조하십시오.

전제 조건

- 이 설정을 변경하면 ASA를 다시 로드해야 합니다.
- 점보 프레임을 전송해야 하는 각 인터페이스의 MTU는 기본값 1500보다 높은 값으로 설정해야 합니다. 예를 들어,. 12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성를 참조하십시오.

- 비 VPN 트래픽에는 TCP MSS를 비활성화하거나, 12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성에 따라 MTU에 맞춰 TCP MSS를 늘리는 방식으로 TCP MSS를 조정해야 합니다.

세부 단계

MTU를 1500바이트보다 크게 설정할 경우 점보 프레임이 자동으로 활성화됩니다. 이 설정을 수동으로 활성화하거나 비활성화하려면 **Configuration > Device Setup > Interfaces**를 선택하고 **Enable jumbo frame support** 확인란을 클릭합니다.

다음에 할 일

인터페이스 컨피그레이션을 완료합니다. 12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.를 참조하십시오.

인터페이스 모니터링

ARP 테이블

Monitoring > Interfaces > ARP Table 창에는 상태 및 동적 항목을 비롯한 ARP 테이블이 표시됩니다. ARP 테이블에는 MAC 주소를 정해진 인터페이스의 IP 주소에 매핑하는 항목이 포함됩니다.

필드

- Interface — 매핑과 관련된 인터페이스 이름이 나열됩니다.
- IP Address — IP 주소가 표시됩니다.
- MAC Address — MAC 주소가 표시됩니다.
- Proxy ARP — 인터페이스에서 프록시 ARP를 활성화할 경우 Yes로 표시됩니다. 인터페이스에서 프록시 ARP를 활성화하지 않은 경우 No로 표시됩니다.
- Clear — 동적 ARP 테이블 항목을 지웁니다. 고정 항목은 지워지지 않습니다.
- Refresh — 테이블을 ASA의 최신 정보로 새로 고치고 Last Updated 날짜 및 시간을 업데이트합니다.
- Last Updated — *표시 전용 항목입니다.* 날짜 및 시간 표시가 업데이트되었는지 표시됩니다.

MAC 주소 테이블

Monitoring > Interfaces > MAC Address Table 창에 고정 및 동적 MAC 주소 항목이 표시됩니다. MAC 주소 테이블 및 고정 항목 추가에 대한 자세한 내용은 11-16 페이지의 MAC 주소 테이블를 참조하십시오.

필드

- Interface — 항목과 관련된 인터페이스 이름이 표시됩니다.
- MAC Address — MAC 주소가 표시됩니다.

- Type — 항목이 고정인지 동적인지 표시합니다.
- Age — 항목의 기간(분 단위)을 표시합니다. 시간 제한을 설정하려면 11-16 페이지의 MAC 주소 테이블를 참조합니다.
- Refresh — 테이블을 ASA의 최신 정보로 새로 고칩니다.

인터페이스 그래프

Monitoring > Interfaces > Interface Graphs 창을 사용하면 인터페이스 통계를 그래프 또는 테이블 형식으로 볼 수 있습니다. 하위 인터페이스에 표시되는 통계 수치는 물리적 인터페이스에 표시되는 통계 수치의 하위 집합입니다.

필드

- Available Graphs for — 모니터링에 사용할 수 있는 통계 유형이 나열됩니다. 그래프 창 1개에 최대 4개의 통계 유형을 선택하여 표시할 수 있습니다. 동시에 여러 개의 그래프 창을 열 수 있습니다.
  - Byte Counts — 인터페이스에 대한 바이트 입력 및 출력의 개수가 표시됩니다.
  - Packet Counts — 인터페이스에 대한 패킷 입력 및 출력의 개수가 표시됩니다.
  - Packet Rates — 인터페이스에 대한 패킷 입력 및 출력의 속도가 표시됩니다.
  - Bit Rates — 인터페이스에 대한 입력 및 출력의 비트 속도가 표시됩니다.
  - Drop Packet Count — 인터페이스에서 손실된 패킷의 개수가 표시됩니다.

  다음과 같은 추가 통계가 물리적 인터페이스에 표시됩니다.
  - Buffer Resources — 다음 통계가 표시됩니다.

    Overruns — 입력 속도가 ASA에서 데이터를 처리할 수 있는 역량을 초과하여, 수신된 데이터를 ASA에서 하드웨어 버퍼로 넘길 수 없는 횟수입니다.

    Underruns — ASA에서 처리할 수 있는 것보다 빠른 속도로 전송 장치가 실행된 횟수입니다.

    No Buffer — 기본 시스템에 버퍼 공간이 없어 지워진 수신 패킷의 개수입니다. 이 값을 무시된 개수와 비교합니다. 이더넷 네트워크의 브로드캐스트 스톰으로 인해 입력 버퍼 없음 이벤트가 발생하는 경우가 많습니다.
  - Packet Errors — 다음과 같은 통계가 표시됩니다.

    CRC — Cyclical Redundancy Check 오류의 개수입니다. 스테이션에서 프레임을 전송할 경우, 프레임의 끝에 CRC가 추가됩니다. 이러한 CRC는 프레임의 데이터를 기반으로 한 알고리즘에서 생성됩니다. 소스와 목적지 간에 프레임이 변경된 경우, ASA에 CRC가 일치하지 않는다는 메시지가 표시됩니다. CRC 수가 높을수록 충돌이나 스테이션 전송 오류 데이터가 발생하는 경우가 많습니다.

    Frame — 프레임 오류 개수입니다. 오류 프레임에는 잘못된 길이 또는 불량 프레임 체크섬이 있는 패킷이 포함되어 있습니다. 이러한 오류로 인해 충돌이나 이더넷 디바이스 고장이 주로 발생할 수 있습니다.

    Input Errors — 여기에 나열된 기타 유형을 비롯한 입력 오류의 총 개수입니다. 입력과 관련된 기타 오류로 인해서도 입력 오류 발생 횟수가 늘어날 수 있으며, 일부 데이터그램에 여러 개의 오류가 포함될 수 있습니다. 따라서 이러한 총계는 기타 유형에 나열된 오류 수를 초과할 수 있습니다.

    Runts — 최소 패킷 크기(64바이트)보다 크기가 작아 삭제된 패킷의 개수입니다. Runt는 일반적으로 충돌로 인해 발생합니다. 또한 잘못된 배선 및 전기 간섭에 의해서도 발생할 수 있습니다.

Giants — 최대 패킷 크기를 초과하여 삭제된 패킷의 개수입니다. 예를 들어, 1518바이트보다 큰 이더넷 패킷은 giant로 간주합니다.

Deferred — FastEthernet 인터페이스에만 해당됩니다. 링크의 작업으로 인해 전송 전에 연기된 프레임의 개수입니다.

- Miscellaneous — 수신된 브로드캐스트의 통계를 표시합니다.
- Collision Counts — FastEthernet 인터페이스에만 해당됩니다. 다음과 같은 통계가 표시됩니다.

  Output Errors — 최대 충돌 수가 구성된 수를 초과하여 전송되지 않은 프레임의 개수입니다. 이 카운터는 네트워크 트래픽이 과중한 동안에만 증가해야 합니다.

  Collisions — 이더넷 충돌(단일 또는 다중 충돌)로 인해 다시 전송된 메시지의 개수입니다. 이러한 현상은 LAN을 과도하게 연장할 경우 주로 발생합니다(이더넷 또는 트랜시버 케이블을 스테이션 간의 두 중계기보다 길게 연장하거나, 다중 포트 트랜시버를 너무 많이 중첩한 경우). 충돌되는 패킷은 출력 패킷별로 한 번만 계산됩니다.

  Late Collisions — 충돌이 정상적인 충돌 범위 밖에서 발생하여 전송되지 못한 프레임의 개수입니다. 지연된 충돌은 패킷의 전송 과정에서 뒤늦게 감지된 충돌입니다. 일반적으로 이러한 현상은 일어나지 않습니다. 2개의 이더넷 호스트에서 동시에 통신을 수행하려고 할 경우 패킷에서 초기에 충돌이 발생하고 둘 다 작업을 잠시 중단하거나, 첫 번째 호스트에서 통신을 수행하고 있으니 대기해야 한다는 메시지가 두 번째 호스트에 표시됩니다. 지연된 충돌이 발생할 경우, 디바이스가 갑자기 실행되어 이더넷에 패킷을 전송하려고 시도하는 반면 ASA에서는 패킷 전송을 부분적으로 완료합니다. ASA에서 패킷의 첫 번째 부분을 보유하고 있던 버퍼를 해제했을 수 있으므로, 패킷이 다시 전송되지 않습니다. 충돌을 해결하기 위해 패킷을 다시 전송하여 네트워킹 프로토콜을 다시 설계하므로 이는 문제가 되지 않습니다. 그러나 지연된 충돌은 네트워크에 문제가 있음을 나타냅니다. 일반적인 문제는 사양을 초과하여 실행되는 대량의 반복적인 네트워크 및 이더넷 네트워크입니다.
- Input Queue — 입력 대기열의 현재 및 최대 패킷 수가 표시되며 다음 통계가 포함됩니다.

  Hardware Input Queue — 하드웨어 대기열의 패킷 수입니다.

  Software Input Queue — 소프트웨어 대기열의 패킷 수입니다.
- Output Queue — 출력 대기열의 현재 및 최대 패킷 수가 표시되며 다음 통계가 포함됩니다.

  Hardware Output Queue — 하드웨어 대기열의 패킷 수입니다.

  Software Output Queue — 소프트웨어 대기열의 패킷 수입니다.

- Add — 선택한 통계 유형을 선택한 그래프 창에 추가합니다.
- 제거 — 선택한 통계 유형을 선택한 그래프 창에서 제거합니다. 다른 창에서 추가된 항목을 제거할 경우 이 버튼 이름이 Delete로 변경되며, Available Graphs 창으로 돌아가지 않습니다.
- Show Graphs — 통계 유형을 추가하려는 그래프 창 이름을 표시합니다. 그래프 창이 이미 열려 있는 경우 새 그래프 창이 기본적으로 나열됩니다. 이미 열려 있는 그래프에 통계 유형을 추가하려면 열려 있는 그래프 창의 이름을 선택합니다. 그래프에 이미 포함된 통계는 Selected Graphs 창에 표시되며, 여기에 추가적인 유형을 추가할 수 있습니다. 그래프 창의 이름은 ASDM의 이름을 따서 명명되며 인터페이스 IP 주소 및 이름 "Graph"가 붙습니다. 후속 그래프의 이름은 “Graph (2)” 등으로 명명됩니다.
- Selected Graphs — 선택한 그래프 창에 표시하려는 통계 유형이 표시됩니다. 최대 4가지 유형을 포함할 수 있습니다.
  - Show Graphs — 그래프 창을 표시하거나 추가 통계 유형이 추가된 경우 그래프를 업데이트합니다.

그래프/테이블

Monitoring > Interfaces > Interface Graphs > Graph/Table 창에는 선택한 통계에 대한 그래프가 표시됩니다. Graph 창에는 한 번에 최대 4가지 그래프를 표시할 수 있습니다. 기본적으로 그래프 또는 테이블에는 실시간 통계가 표시됩니다. History Metrics를 활성화할 경우(3-32 페이지의 History Metrics 활성화 참조) 이전 기간의 통계를 볼 수 있습니다.

필드

- View — 그래프 또는 테이블의 기간을 설정합니다. 실시간이 아닌 기간을 보려면 History Metrics를 활성화합니다(3-32 페이지의 History Metrics 활성화 참조) 데이터는 다음 옵션의 사양에 따라 업데이트됩니다.
  - 실시간, 10초당 데이터
  - 최근 10분, 10초당 데이터
  - 최근 60분, 1분당 데이터
  - 최근 12시간, 12분당 데이터
  - 최근 5일, 2시간당 데이터
- Export — 그래프를 쉼표로 구분된 값 형식으로 내보냅니다. Graph 창에 여러 개의 그래프 또는 테이블이 있을 경우, Export Graph Data 대화 상자가 표시됩니다. 이름 옆의 확인란을 선택하여 나열된 그래프 및 테이블을 하나 이상 선택합니다.
- Print — 그래프 또는 테이블을 인쇄합니다. Graph 창에 여러 개의 그래프 또는 테이블이 있을 경우, Print Graph Data 대화 상자가 표시됩니다. Graph/Table Name 목록에서 인쇄하려는 그래프 또는 테이블을 선택합니다.
- Bookmark — Graphs 창에서 모든 그래프 및 테이블에 대한 단일 링크 및 각 그래프 또는 테이블에 대한 개별 링크가 포함된 브라우저 창을 엽니다. 브라우저에서 이러한 URL을 북마크로 복사할 수 있습니다.그래프에 대한 URL을 열 때 ASDM을 실행하지 않아도 됩니다. 브라우저에서 ASDM을 시작하고 그래프를 표시합니다.

다음으로 살펴볼 내용

12 장, “라우팅 모드 인터페이스”, 또는 13 장, “투명 모드 인터페이스”.에 따라 인터페이스 컨피그레이션을 완료합니다.

ASAv 인터페이스의 기능 기록

표 11-1 인터페이스의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
ASAv 지원	9.2(1)	ASAv는 도입되었습니다.

12 장

라우팅 모드 인터페이스

이 장에는 라우팅 방화벽 모드에서 모든 모델의 인터페이스 컨피그레이션을 완료하는 작업에 대한 내용이 포함되어 있습니다.

참고 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 섹션의 작업을 수행합니다. Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 컨텍스트 이름을 두 번 클릭합니다.

라우팅 모드에서 인터페이스 구성 완료 정보

보안 레벨

각 인터페이스는 0(가장 낮음)~100(가장 높음)의 보안 레벨이 있어야 합니다. 예를 들어, 내부 호스트 네트워크와 같이 가장 안전한 네트워크는 레벨 100으로 지정해야 합니다. 반면에 인터넷에 연결된 외부 네트워크는 레벨 0이 될 수 있습니다. DMZ와 같은 다른 네트워크는 그 사이의 값이 될 수 있습니다. 인터페이스를 동일한 보안 레벨에 지정할 수 있습니다. 자세한 내용은 12-18 페이지의 동일한 보안 레벨 통신 허용를 참조하십시오.

이 레벨은 다음 동작을 제어합니다.

- 네트워크 액세스—기본적으로 상위 보안 인터페이스에서 하위 보안 인터페이스로 암시적 허용이 이루어집니다(아웃바운드). 상위 보안 인터페이스의 호스트는 하위 보안 인터페이스의 어떤 호스트에도 액세스할 수 있습니다. 인터페이스에 ACL을 적용하여 액세스를 제한할 수 있습니다.

동일한 보안 인터페이스에 대한 통신을 활성화할 경우(12-18 페이지의 동일한 보안 레벨 통신 허용 참조), 해당 인터페이스에서 보안 레벨이 같거나 더 낮은 다른 인터페이스에 액세스하는 것이 암시적으로 허용됩니다.

- 검사 엔진—일부 애플리케이션 검사 엔진은 보안 레벨에 좌우됩니다. 동일한 보안 인터페이스에서는 검사 엔진이 어느 방향의 트래픽에도 적용됩니다.
  - NetBIOS 검사 엔진—아웃바운드 연결에만 적용됩니다.
  - SQL*Net 검사 엔진—어떤 호스트 쌍에 SQL*Net(이전의 OraServ) 포트에 대한 제어 연결이 있을 경우 인바운드 데이터 연결만 ASA에서 허용됩니다.
- 필터링—HTTP(S) 및 FTP 필터링은 아웃바운드 연결(상위에서 하위로)에만 적용됩니다.

  동일한 보안 인터페이스에 대한 통신을 활성화한 경우 어느 방향의 트래픽도 필터링할 수 있습니다.
- **established** 명령—이 명령은 상위 보안 호스트에서 하위 보안 호스트로의 연결이 이미 설정된 경우 하위 호스트에서 상위 호스트로 돌아가는 연결을 허용합니다.

  동일한 보안 인터페이스에 대한 통신을 활성화한 경우 양방향 모두에 **established** 명령을 구성할 수 있습니다.

이중 IP Stack(IPv4 및 IPv6)

Cisco ASA에서는 인터페이스에서 IPv6 및 IPv4 컨피그레이션을 모두 지원합니다. 이를 위해 특수한 명령을 입력할 필요가 없으며, 일반적으로 하는 것처럼 IPv4 컨피그레이션 명령 및 IPv6 컨피그레이션 명령을 입력하기만 하면 됩니다. IPv4 및 IPv6 모두에 대한 기본 경로를 구성해야 합니다.

라우팅 모드에서 인터페이스 구성을 완료하는 데 필요한 라이센스 요구 사항

모델	라이센싱 요구 사항
ASA 5512-X	VLAN: Base 라이센스: 50 Security Plus 라이센스: 100 모든 유형의 인터페이스: Base 라이센스: 716 Security Plus 라이센스: 916
ASA 5515-X	VLAN: Base 라이센스: 100 모든 유형의 인터페이스: Base 라이센스: 916

모델	라이센싱 요구 사항
ASA 5525-X	VLAN: Base 라이센스: 200 모든 유형의 인터페이스: Base 라이센스: 1316
ASA 5545-X	VLAN: Base 라이센스: 300 모든 유형의 인터페이스: Base 라이센스: 1716
ASA 5555-X	VLAN: Base 라이센스: 500 모든 유형의 인터페이스: Base 라이센스: 2516
ASA 5585-X	VLAN: Base 및 Security Plus 라이센스: 1024 SSP-10 및 SSP-20을 위한 인터페이스 속도: Base 라이센스—파이버 인터페이스용 1기가비트 이더넷 10GE I/O 라이센스(Security Plus)—파이버 인터페이스용 10기가비트 이더넷 (SSP-40 및 SSP-60은 10기가비트 이더넷을 기본적으로 지원) 모든 유형의 인터페이스: Base 및 Security Plus 라이센스: 4612

참고 어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다.

모든 유형의 인터페이스는 전체 인터페이스, 이를테면 VLAN 인터페이스, 물리적 인터페이스, 이중 인터페이스, 브리지 그룹 인터페이스, EtherChannel 인터페이스의 최대 개수로 이루어집니다. 컨피그레이션에 정의된 모든 **interface**은 이 한도의 대상이 됩니다.

모델	라이센싱 요구 사항
ASASM	VLAN: Base 라이센스: 1000

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

- 다중 컨텍스트 모드의 ASA 5512-X 이상에서는 시스템 실행 영역에서 10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.에 따라 물리적 인터페이스를 구성합니다. 그런 다음 컨텍스트 실행 영역에서 이 장의 내용에 따라 논리적 인터페이스 매개 변수를 구성합니다. 다중 컨텍스트 모드의 ASASM에서는 스위치에서 스위치 포트와 VLAN을 구성하고 2장, “Switch Configuration for the Cisco ASA Services Module.” 에 따라 ASASM에 VLAN을 지정합니다.

  ASAv는 다중 컨텍스트 모드를 지원하지 않습니다.
- 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 7-15 페이지의 다중 컨텍스트 모드 구성 에 따라 이미 컨텍스트에 지정한 컨텍스트 인터페이스만 컨피그레이션할 수 있습니다.
- PPPoE는 다중 컨텍스트 모드에서 지원되지 않습니다.

방화벽 모드 지침

라우팅 방화벽 모드에서 지원됩니다. 투명 모드에 대한 내용은 13 장, “투명 모드 인터페이스”.를 참조하십시오.

장애 조치 지침

이 장의 절차를 사용하여 장애 조치 인터페이스 구성을 마쳐서는 안 됩니다. 장애 조치 및 상태 링크 구성에 대해서는 8 장, “고가용성을 위한 장애 조치”,를 참조하십시오. 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 장애 조치 인터페이스가 컨피그레이션됩니다.

IPv6 지침

IPv6를 지원합니다.

ASASM를 위한 VLAN ID 지침

어떤 VLAN ID도 컨피그레이션에 추가할 수 있으나, 스위치에 의해 ASA에 지정된 VLAN만 트래픽을 전달할 수 있습니다. ASA에 지정된 모든 VLAN을 보려면 **show vlan** 명령을 사용합니다.

아직 스위치에 의해 ASA에 지정되지 않은 VLAN을 위해 인터페이스를 추가할 경우 그 인터페이스는 중지(down) 상태가 됩니다. VLAN을 ASA에 지정하면 인터페이스는 작동(up) 상태로 바뀝니다. 인터페이스 상태에 대한 자세한 내용은 **show interface** 명령을 참조하십시오.

기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다. 공장 기본 컨피그레이션에 대한 자세한 내용은 2-15 페이지의 공장 기본 구성를 참조하십시오.

기본 보안 레벨

기본 보안 레벨은 0입니다. 인터페이스의 이름을 “inside”로 지정한 다음 보안 레벨을 명시적으로 설정하지 않으면 ASA는 보안 레벨을 100으로 설정합니다.

참고 인터페이스의 보안 레벨을 변경한 경우, 기존 연결이 시간 초과될 때까지 기다리지 않고 새 보안 정보를 사용하려면 **clear local-host** 명령을 사용하여 연결을 해제합니다.

ASASM의 인터페이스 기본 상태

- 단일 모드 또는 시스템 시행 영역에서는 VLAN 인터페이스가 기본적으로 활성화되어 있습니다.
- 다중 컨텍스트 모드에서는 인터페이스가 시스템 실행 영역에서 어떤 상태이든 상관없이 모든 할당된 인터페이스가 기본적으로 활성화되어 있습니다. 그러나 트래픽이 인터페이스를 통과하려면 인터페이스가 시스템 실행 영역에서도 활성화되어야 합니다. 시스템 실행 영역에서 인터페이스를 종료한 경우 이 인터페이스는 이를 공유하는 모든 컨텍스트에서 중지됩니다.

점보 프레임 지원

기본적으로 ASASM는 점보 프레임을 지원합니다. 12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성에 따라 원하는 패킷 크기의 MTU를 구성합니다.

라우팅 모드에서 인터페이스 구성 완료

인터페이스 구성 완료의 작업 흐름

1단계 모델에 따라 인터페이스를 설정합니다.

- ASA 5512-X 이상—10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.
- ASASM—2장, “Switch Configuration for the Cisco ASA Services Module.”
- ASAv—11 장, “기본 인터페이스 구성(ASAv)”.

2단계 (다중 컨텍스트 모드) 7-15 페이지의 다중 컨텍스트 모드 구성에 따라 컨텍스트에 인터페이스를 배정합니다.

3단계 (다중 컨텍스트 모드) Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 컨텍스트 이름을 두 번 클릭합니다.

4단계 인터페이스 이름, 보안 수준, IPv4 주소를 비롯한 일반적인 인터페이스 매개변수를 구성합니다. 12-6 페이지의 일반 인터페이스 매개 변수 구성를 참조하십시오.

5단계 (선택 사항) MAC 주소 및 MTU를 구성합니다. 12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성를 참조하십시오.

6단계 (선택 사항) IPv6 주소 지정을 구성합니다. 12-13 페이지의 IPv6 주소 지정 구성를 참조하십시오.

7단계 (선택 사항) 두 인터페이스 간 통신을 허용하거나 트래픽이 동일한 인터페이스에 들어오고 나가는 것을 허용하는 방법 중 하나로 동일한 보안 레벨 통신을 허용합니다. 12-18 페이지의 동일한 보안 레벨 통신 허용를 참조하십시오.

일반 인터페이스 매개 변수 구성

이 절차에서는 이름, 보안 수준, IPv4 주소 및 기타 옵션을 설정하는 방법에 대해 설명합니다.

ASA 5512-X 이상과 ASAv의 경우 다음 인터페이스 유형에 대한 인터페이스 매개 변수를 구성해야 합니다.

- 물리적 인터페이스
- VLAN 하위 인터페이스
- 이중 인터페이스
- EtherChannel ?인터페이스

ASASM에서는 다음 인터페이스 유형에 대해 인터페이스 매개 변수를 구성해야 합니다.

- VLAN 인터페이스

지침 및 제한 사항

장애 조치를 사용하는 경우 장애 조치 및 상태 기반 시스템 대체 작동 통신 전용 인터페이스의 이름을 지정하는 데 이 절차를 사용하지 마십시오. 장애 조치 및 상태 링크 구성에 대해서는 8 장, “고가용성을 위한 장애 조치”,를 참조하십시오.

제한 사항

- PPPoE는 다중 컨텍스트 모드에서 지원되지 않습니다.
- PPPoE 및 DHCP는 ASASM에서 지원되지 않습니다.

전제 조건

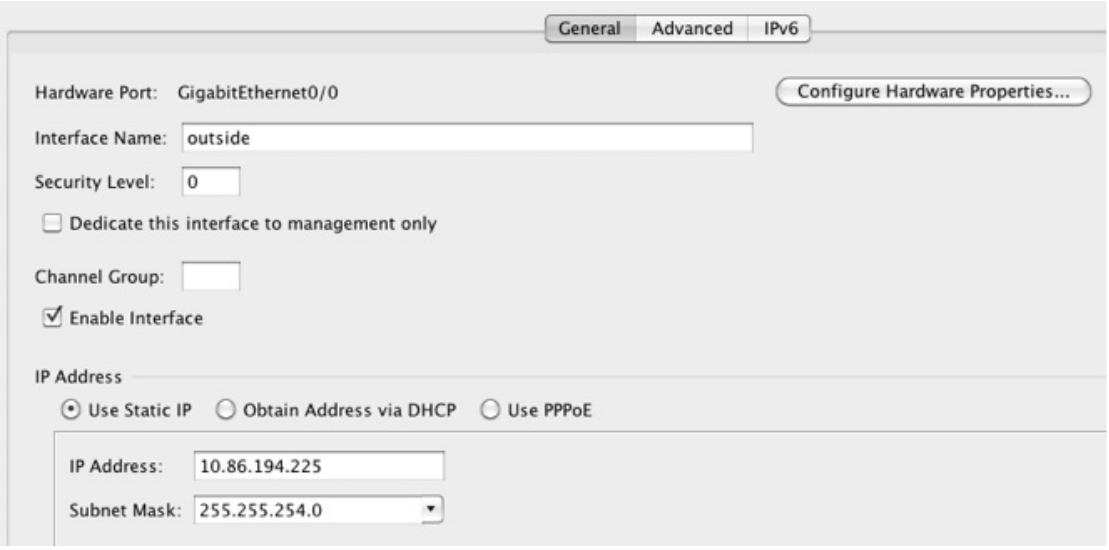
- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.
  - ASASM—2장, “Switch Configuration for the Cisco ASA Services Module.”
  - ASAv—11 장, “기본 인터페이스 구성(ASAv)”.
- 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 7-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 컨텍스트에 지정한 컨텍스트 인터페이스만 컨피그레이션할 수 있습니다.
- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 컨텍스트 컨피그레이션으로 변경하려면Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 컨텍스트 이름을 두 번 클릭합니다.

세부 단계

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 인터페이스 행을 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.



3단계 Interface Name 필드에 이름을 48자 이내로 입력합니다.

4단계 Security level 필드에 0(가장 낮음)~100(가장 높음) 범위의 레벨을 입력합니다.

자세한 내용은 12-1 페이지의 보안 레벨를 참조하십시오.

5단계 (선택 사항이며 이중화 인터페이스에 지원되지 않음) 이 인터페이스를 관리 전용 인터페이스로 설정하려면 **Dedicate this interface to management-only** 확인란을 선택합니다.

관리 전용 인터페이스에서 통과 트래픽은 허용되지 않습니다. ASA 5585-X에 대한 자세한 내용은 12-6 페이지의 전제 조건를 참조하십시오.

(ASA 5512-X부터 ASA 5555-X까지) Management 0/0 인터페이스에서 이 옵션을 비활성화할 수 없습니다.

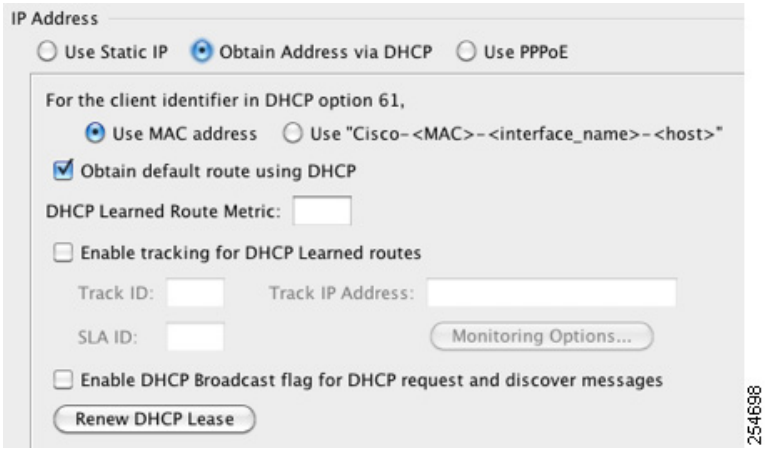
참고 Channel Group 필드는 읽기 전용이며, 인터페이스가 EtherChannel의 일부인지를 나타냅니다.

6단계 인터페이스가 아직 활성화되지 않은 경우 **Enable Interface** 확인란을 선택합니다.

7단계 IP 주소를 설정하려면 다음 옵션 중 하나를 선택합니다.

참고 장애 조치와 함께 사용할 경우 IP 주소 및 스탠바이 주소를 수동으로 설정해야 하며, DHCP 및 PPPoE는 지원되지 않습니다. Configuration > Device Management > High Availability > Failover > Interfaces 탭에서 대기 IP 주소를 설정합니다.

- 직접 IP 주소를 설정하려면 **Use Static IP** 라디오 버튼을 클릭하고 IP 주소와 마스크를 입력합니다.
- DHCP 서버에서 IP 주소를 얻으려면 **Obtain Address via DHCP** 라디오 버튼을 클릭합니다.



a. 옵션 61에 대한 DHCP 요청 패킷 안에 반드시 MAC 주소가 저장되게 하려면 **Use MAC Address** 라디오 버튼을 클릭합니다.

   일부 ISP의 경우 옵션 61이 인터페이스 MAC 주소가 됩니다. MAC 주소가 DHCP 요청 패킷에 포함되지 않은 경우 IP 주소는 지정되지 않습니다.

b. 옵션 61에 대해 일반 문자열을 사용하려면 **Use "Cisco-<MAC>-<interface_name>-<host>"**를 클릭합니다.

c. (선택 사항) DHCP 서버에서 기본 경로를 얻으려면 **Obtain Default Route Using DHCP**를 선택합니다.

d. (선택 사항) 파악된 경로에 관리 영역을 할당하려면 DHCP Learned Route Metric 필드에 1~255 사이의 값을 입력합니다. 이 필드가 비어 있는 경우, 파악된 경로의 관리 영역은 1입니다.

e. (선택 사항) DHCP 파악 경로 추적을 활성화하려면 **Enable Tracking for DHCP Learned Routes**를 선택합니다. 다음 값을 설정합니다.

   Track ID — 경로 추적 프로세스의 고유한 식별자입니다. 유효한 값은 1부터 500까지입니다.

   Track IP Address — 추적할 대상의 IP 주소를 입력합니다. 일반적으로 이 값은 경로의 다음 홉 게이트웨이의 IP 주소이지만, 해당 인터페이스에서 제공되는 모든 네트워크 객체일 수 있습니다.

참고 경로 추적은 단일 라우팅 모드에서만 사용 가능합니다.

   SLA ID — SLA 모니터링 프로세스의 고유한 식별자입니다. 유효한 값은 1부터 2147483647까지입니다.

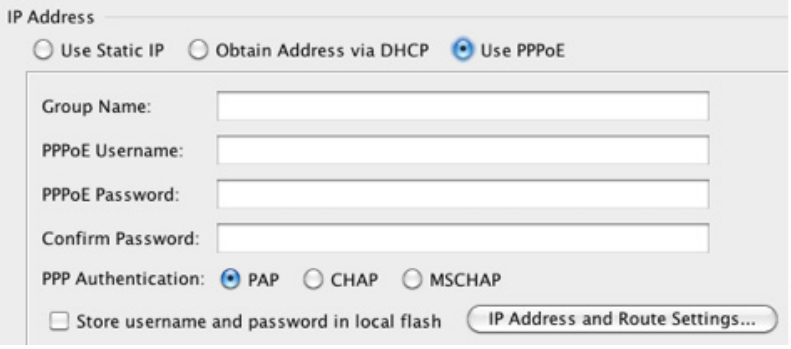
   Monitor Options — 이 버튼을 클릭하면 Route Monitoring Options 대화 상자가 열립니다. Route Monitoring Options 대화 상자에서 추적한 객체 모니터링 프로세스의 매개변수를 구성할 수 있습니다.

f. (선택 사항) DHCP 클라이언트에서 IP 주소를 요청하는 discover를 보낼 때 DHCP 패킷 헤더에서 브로드캐스트 플래그를 1로 설정하려면 **Enable DHCP Broadcast flag for DHCP request and discover messages**를 선택합니다.

   DHCP 서버가 이 브로드캐스트 플래그를 수신하고, 플래그가 1로 설정되었으면 회신 패킷을 브로드캐스트합니다.

g. (선택 사항) 임대를 갱신하려면 **Renew DHCP Lease**를 클릭합니다.

- (단일 모드만 해당) PPPoE를 사용하여 IP 주소를 얻으려면 **Use PPPoE**를 선택합니다.



  a. Group Name 필드에 그룹 이름을 지정합니다.

  b. PPPoE Username 필드에 ISP에서 제공한 사용자 이름을 지정합니다.

  c. PPPoE Password 필드에 ISP에서 제공한 비밀번호를 지정합니다.

  d. Confirm Password 필드에 비밀번호를 다시 입력합니다.

  e. PPP 인증을 수행하려면 **PAP**, **CHAP** 또는 **MSCHAP** 라디오 버튼을 클릭합니다.

     PAP에서는 인증이 진행되는 동안 일반 텍스트로 된 사용자 이름 및 비밀번호를 전달하며 이는 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.

  f. (선택 사항) 사용자 이름 및 비밀번호를 플래시 메모리에 저장하려면, **Store Username and Password in Local Flash** 확인란을 선택합니다.

     ASA에서는 NVRAM의 특수 위치에 사용자 이름 및 비밀번호를 저장합니다. Auto Update Server에서는 **clear configure** 명령을 ASA로 보낸 후 연결이 중단되면, ASA에서는 NVRAM에서 사용자 이름 및 비밀번호를 읽고 Access Concentrator에 대한 인증을 다시 수행할 수 있습니다.

  g. (선택 사항) 주소 지정 및 추적 옵션을 선택할 수 있는 PPPoE IP Address and Route Settings 대화 상자를 표시하려면 **IP Address and Route Settings**를 클릭합니다. 자세한 내용은 12-10 페이지의 PPPoE IP 주소 및 경로 설정를 참조하십시오.

8단계 (선택 사항) Description 필드에 이 인터페이스에 대한 설명을 입력합니다.

설명은 줄 바꿈 없이 1줄, 최대 240자로 작성합니다. 장애 조치 또는 상태 링크의 경우 이 설명은 “LAN Failover Interface”, “STATE Failover Interface” 또는“LAN/STATE Failover Interface”와 같이 고정되어 있습니다. 이 설명을 수정할 수 없습니다. 이 인터페이스를 장애 조치 또는 상태 링크로 만들 경우 고정된 설명이 사용자가 여기에 입력한 설명을 덮어씁니다.

참고 (ASA 5512-X 이상 버전) Configure Hardware Properties 버튼에 대한 자세한 내용은 10-14 페이지의 물리적 인터페이스 활성화 및 이더넷 매개변수 구성를 참조하십시오.

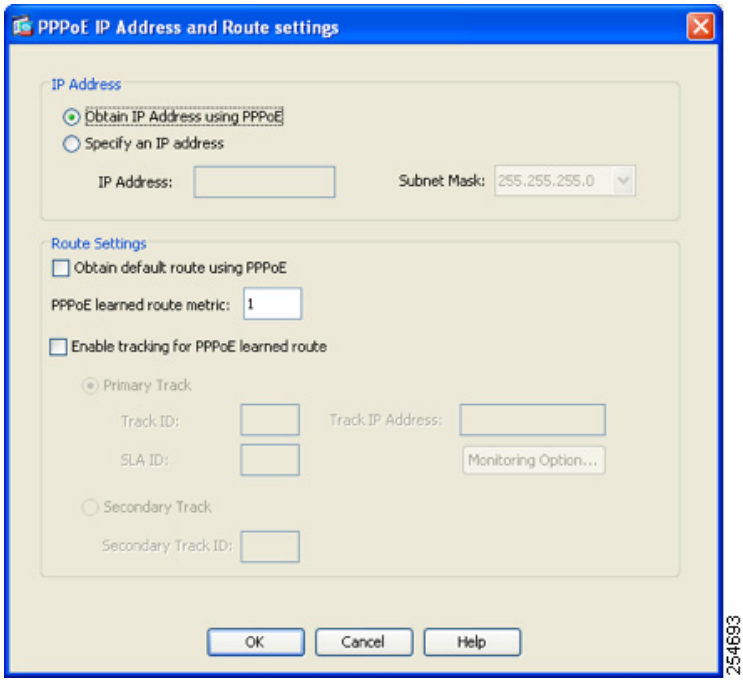
9단계 **OK**를 클릭합니다.

다음에 할 일

- (선택 사항) MAC 주소 및 MTU를 구성합니다. 12-11 페이지의 MAC Address, MTU 및 TCP MSS 구성를 참조하십시오.
- (선택 사항) IPv6 주소 지정을 구성합니다. 12-13 페이지의 IPv6 주소 지정 구성를 참조하십시오.

PPPoE IP 주소 및 경로 설정

Configuration > Interfaces > Add/Edit Interface > General > PPPoE IP Address and Route Settings > PPPoE IP Address and Route Settings 대화 상자를 사용하면 PPPoE 연결에 대한 주소 지정 및 추적 옵션을 선택할 수 있습니다.



필드

- IP Address area — PPP를 사용하여 IP 주소를 얻거나 IP 주소를 지정하는 방법 중 하나를 선택할 수 있으며, 다음 필드가 포함됩니다.
  - Obtain IP Address using PPP — ASA에서 PPP를 사용하여 IP 주소를 얻을 수 있도록 선택합니다.
  - Specify an IP Address — PPPoE 서버와 협상을 수행하여 주소를 동적으로 할당하는 대신 ASA에 사용할 IP 주소 및 마스크를 지정합니다.
- Route Settings Area — 경로 및 추적 설정을 구성할 수 있으며 다음 필드가 포함됩니다.
  - Obtain default route using PPPoE — PPPoE 클라이언트에서 아직 연결을 설정하지 않은 경우 기본 경로를 설정합니다. 이 옵션을 사용하면 컨피그레이션에 고정으로 정의된 경로가 포함될 수 없습니다.

    PPPoE learned route metric — 파악된 경로에 관리 영역을 할당합니다. 유효한 값은 1부터 255까지입니다. 이 필드가 비어 있는 경우, 파악된 경로의 관리 영역은 1입니다.

- Enable tracking — 이 확인란을 선택하여 PPPoE 파악 경로를 추적하는 경로를 활성화합니다.

  참고 경로 추적은 단일 라우팅 모드에서만 사용 가능합니다.

- Primary Track — 이 옵션을 선택하여 기본 PPPoE 경로 추적을 구성합니다.
- Track ID — 경로 추적 프로세스의 고유한 식별자입니다. 유효한 값은 1부터 500까지입니다.
- Track IP Address — 추적할 대상의 IP 주소를 입력합니다. 일반적으로 이 값은 경로의 다음 홉 게이트웨이의 IP 주소이지만, 해당 인터페이스에서 제공되는 모든 네트워크 객체일 수 있습니다.
- SLA ID — SLA 모니터링 프로세스의 고유한 식별자입니다. 유효한 값은 1부터 2147483647까지입니다.
- Monitor Options — 이 버튼을 클릭하면 Route Monitoring Options 대화 상자가 열립니다. Route Monitoring Options 대화 상자에서 추적한 객체 모니터링 프로세스의 매개변수를 구성할 수 있습니다.
- Secondary Track — 이 옵션을 선택하여 보조 PPPoE 경로 추적을 구성합니다.
- Secondary Track ID — 경로 추적 프로세스의 고유한 식별자입니다. 유효한 값은 1부터 500까지입니다.

MAC Address, MTU 및 TCP MSS 구성

이 섹션에서는 인터페이스의 MAC 주소를 구성하는 방법 및 MTU와 TCP MSS를 설정하는 방법을 설명합니다.

MAC 주소에 대한 정보

기본적으로 물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.

ASASM에서는 모든 VLAN이 백플레인에서 제공한 동일한 MAC 주소를 사용합니다.

이중 인터페이스는 사용자가 추가한 첫 번째 물리적 인터페이스의 MAC 주소를 사용합니다. 컨피그레이션에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 이 명령을 사용하여 이중 인터페이스에 MAC 주소를 지정하면 멤버 인터페이스 MAC 주소와 상관없이 이 주소가 사용됩니다.

EtherChannel의 경우 채널 그룹에 속한 모든 인터페이스가 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다. 포트-채널 인터페이스는 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 직접 구성할 수도 있습니다. 다중 컨텍스트 모드에서는 EtherChannel 포트 인터페이스를 비롯한 인터페이스에 고유한 MAC 주소를 자동으로 지정할 수 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우에 대비하여 직접 또는 다중 컨텍스트 모드라면 자동으로 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널 MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그 다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.

다중 컨텍스트 모드에서는 여러 컨텍스트가 하나의 인터페이스를 공유할 경우 각 컨텍스트에서 인터페이스에 고유한 MAC 주소를 지정할 수 있습니다. 이 기능 덕분에 ASA에서 손쉽게 알맞은 컨텍스트로 패킷을 분류할 수 있습니다. 고유한 MAC 주소 없이 공유 인터페이스를 사용할 수 있으나, 몇 가지 제한이 있습니다. 자세한 내용은 7-3 페이지의 ASA의 패킷 분류를 참조하십시오. 각 MAC 주소를 직접 지정하거나 컨텍스트에서 공유 인터페이스의 MAC 주소를 자동으로 생성할 수 있습니다. MAC 주소를 자동으로 생성하려면 7-23 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정를 참조하십시오. MAC 주소를 자동으로 생성한 경우 생성된 주소를 재정의하는 데 이 절차를 사용할 수 있습니다.

단일 컨텍스트 모드에서는 또는 다중 컨텍스트 모드에서 공유되지 않는 인터페이스에 대해서는 하위 인터페이스에 고유 MAC 주소를 지정해야 하는 경우가 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다.

MTU 및 TCP MSS에 대한 정보

10-7 페이지의 MTU 및 TCP 최대 세그먼트 크기로 조각화 제어를 참조하십시오.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.
  - ASASM—2장, “Switch Configuration for the Cisco ASA Services Module.”
  - ASAv—11 장, “기본 인터페이스 구성(ASAv)”.
- 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 7-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 컨텍스트에 지정한 컨텍스트 인터페이스만 컨피그레이션할 수 있습니다.
- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 컨텍스트 컨피그레이션으로 변경하려면Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 컨텍스트 이름을 두 번 클릭합니다.

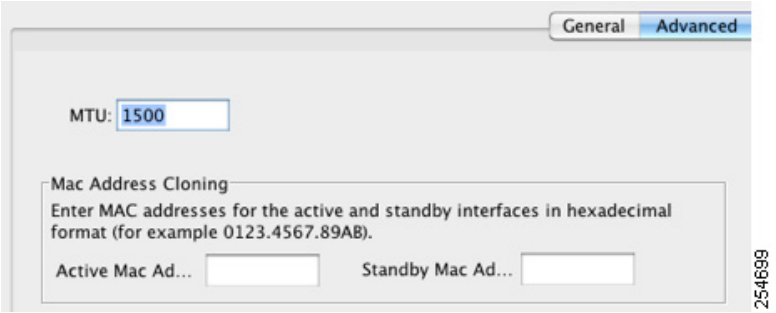
세부 단계

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 인터페이스 행을 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.

3단계 **Advanced** 탭을 클릭합니다.



4단계 MTU를 설정하거나 점보 프레임 지원을 활성화하려면(지원되는 모델만 해당) MTU 필드에 300바이트 ~ 9198바이트(ASAv는 9000바이트) 범위의 값을 입력합니다.

기본값은 1500바이트입니다.

참고 이중 또는 포트 채널 인터페이스를 위해 MTU를 설정하면 ASA는 모든 멤버 인터페이스에 이 설정을 적용합니다.

- 단일 모드에서 점보 프레임을 지원하는 모델에서 임의의 인터페이스에 대해 1500보다 큰 값을 입력한 경우 모든 인터페이스에서 점보 프레임 지원이 자동으로 활성화됩니다. 모든 인터페이스의 MTU를 1500보다 작은 값으로 다시 설정하면 점보 프레임 지원이 비활성화됩니다.
- 다중 모드에서 점보 프레임을 지원하는 모델에서 임의의 인터페이스에 대해 1500보다 큰 값을 입력한 경우 시스템 컨피그레이션에서 점보 프레임 지원을 활성화해야 합니다. 10-28 페이지의 점보 프레임 지원 활성화를 참조하십시오.

참고 점보 프레임 지원을 활성화하거나 비활성화하려면 ASA를 다시 로드해야 합니다.

5단계 이 인터페이스에 MAC 주소를 직접 지정하려면 Active Mac Address 필드에 H.H.H 형식으로 MAC 주소를 입력합니다. 여기서 H는 16비트 16진수입니다.

예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. 자동 생성된 MAC 주소도 사용하려는 경우 수동 MAC 주소의 처음 2바이트는 A2가 될 수 없습니다.

6단계 장애 조치를 사용하는 경우 Standby Mac Address 필드에 대기 MAC 주소를 입력합니다. 활성 유닛이 장애 조치되고 대기 유닛이 활성 상태가 되면, 네트워크 중단을 최소화하기 위해 새 활성 유닛에서 활성 MAC 주소를 사용하기 시작하고 기존 활성 유닛은 대기 주소를 사용합니다.

7단계 TCP MSS를 설정하려면 **Configuration > Firewall > Advanced > TCP Options**를 선택합니다. 다음 옵션을 설정합니다.

- Force Maximum Segment Size for TCP—최대 TCP 세그먼트 크기(바이트)를 48~임의의 최대값 범위에서 설정합니다. 기본값은 1380바이트입니다. bytes를 0으로 설정하여 이 기능을 비활성화할 수 있습니다.
- Force Minimum Segment Size for TCP—최대 세그먼트 크기를 48~임의의 최대값 범위에서 사용자가 설정한 bytes보다 작지 않은 값으로 재정의합니다. 이 기능은 기본적으로 비활성화되어 있습니다(0으로 설정됨).

8단계 **Secure Group Tagging**에 대해서는 33-22 페이지의 SGT plus Ethernet Tagging 활성화를 참조하십시오.

다음에 할 일

(선택 사항) IPv6 주소 지정을 구성합니다. 12-13 페이지의 IPv6 주소 지정 구성를 참조하십시오.

IPv6 주소 지정 구성

이 섹션에서는 IPv6 주소 지정의 구성 방법을 설명합니다.

- 12-17 페이지의 (선택 사항) 링크-로컬 주소 자동 구성
- 12-17 페이지의 (선택 사항) 링크-로컬 주소 수동 구성

IPv6에 대한 정보

이 섹션에서는 IPv6를 구성하는 방법을 다룹니다.

- 12-14 페이지의 IPv6 주소 지정
- 12-14 페이지의 Modified EUI-64 인터페이스 ID

IPv6 주소 지정

IPv6를 위해 2가지 유형의 유니캐스트 주소를 구성할 수 있습니다.

- Global—전역 주소는 공용 네트워크에서 사용할 수 있는 공용 주소입니다.
- Link-local—링크-로컬 주소는 직접 연결된 네트워크에서만 사용할 수 있는 사설 주소입니다. 라우터에서 링크-로컬 주소를 사용하여 패킷을 전달하지 않습니다. 이는 특정 물리적 네트워크 세그먼트에서의 통신에만 사용됩니다. 주소 컨피그레이션에 또는 주소 확인, Neighbor Discovery와 같은 ND 기능에 사용할 수 있습니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 설정하면 Link-Local 주소가 인터페이스에서 자동으로 구성되므로, Link-Local 주소를 특별히 구성하지 않아도 됩니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

Modified EUI-64 인터페이스 ID

RFC 3513: IPv6(Internet Protocol Version 6) Addressing Architecture에 따르면, 모든 유니캐스트 IPv6 주소(이진 값 000으로 시작하는 것 제외)의 인터페이스 식별자 부분은 길이가 64비트이고 Modified EUI-64 형식이어야 합니다. ASA는 로컬 링크에 연결된 호스트에 이 요구 사항을 적용할 수 있습니다.

이 기능이 인터페이스에서 활성화된 경우, 그 인터페이스에서 수신한 IPv6 패킷의 소스 주소를 소스 MAC 주소와 비교하여 검증함으로써 인터페이스 식별자가 Modified EUI-64 형식을 사용하는지 확인합니다. IPv6 패킷에서 인터페이스 식별자에 Modified EUI-64 형식을 사용하지 않을 경우 패킷은 폐기되고 다음 시스템 로그 메시지가 생성됩니다.

```
%ASA-3-325003: EUI-64 source address check failed.
```

주소 형식 검증은 흐름이 생성되는 경우에만 수행됩니다. 기존 흐름의 패킷은 검사하지 않습니다. 또한 이 주소 검증은 로컬 링크의 호스트에 대해서만 수행할 수 있습니다. 라우터 뒤에 있는 호스트로부터 받은 패킷은 주소 형식 검증을 통과하지 못해 폐기됩니다. 그 소스 MAC 주소가 호스트 MAC 주소가 아닌 라우터 MAC 주소이기 때문입니다.

전역 IPv6 주소 구성

전역 IPv6 주소를 구성하려면 다음 단계를 수행합니다.

참고 전역 주소를 자동으로 구성하면 링크-로컬 주소가 구성됩니다. 즉 따로 구성할 필요 없습니다.

제한 사항

ASA는 IPv6 애니캐스트 주소를 지원하지 않습니다.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.
  - ASASM—2장, “Switch Configuration for the Cisco ASA Services Module.”
  - ASAv—11 장, “기본 인터페이스 구성(ASAv)”.
- 다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 7-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 컨텍스트에 지정한 컨텍스트 인터페이스만 컨피그레이션할 수 있습니다.
- 다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 컨텍스트 컨피그레이션으로 변경하려면Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 컨텍스트 이름을 두 번 클릭합니다.

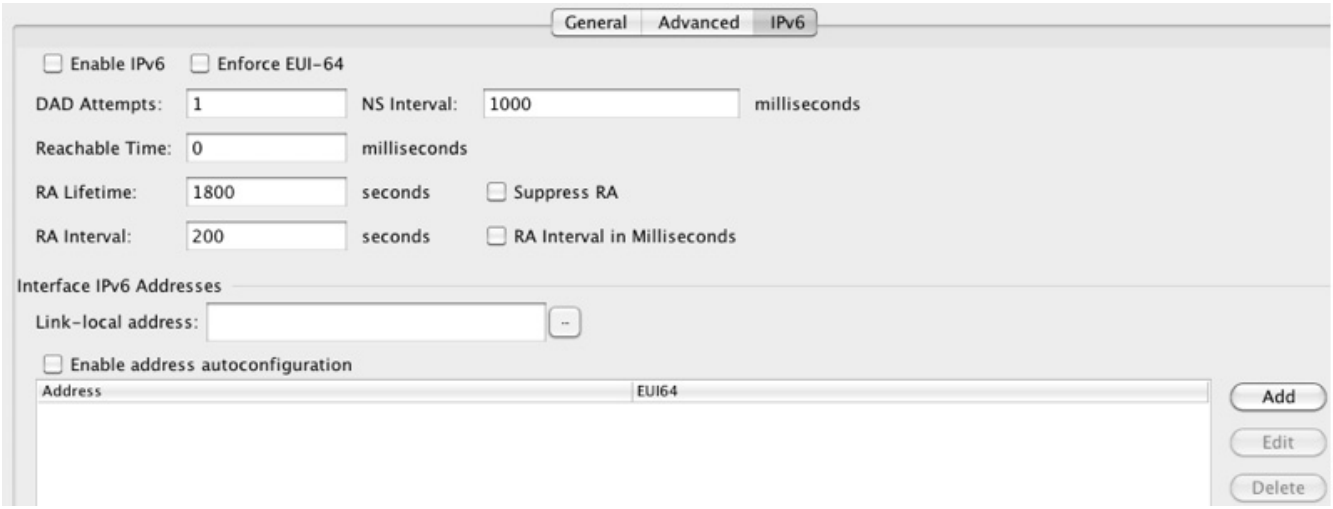
세부 단계

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.

3단계 **IPv6** 탭을 클릭합니다.



4단계 **Enable IPv6** 확인란을 선택합니다.

5단계 (선택 사항) 로컬 링크의 IPv6 주소에서 반드시 Modified EUI-64 형식 인터페이스 식별자를 사용하게 하려면 **Enforce EUI-64** 확인란을 선택합니다.

자세한 내용은 12-14 페이지의 Modified EUI-64 인터페이스 ID를 참조하십시오.

6단계 (선택 사항) 맨 위 영역에서 26 장, “IPv6 인접 디바이스 검색”.를 참조하여 IPv6 컨피그레이션을 사용자 지정합니다.

7단계 다음 방법 중 하나를 사용하여 전역 IPv6 주소를 구성합니다.

- 스테이트리스 자동 컨피그레이션 — Interface IPv6 Addresses 영역에서 **Enable address autoconfiguration** 확인란을 선택합니다.

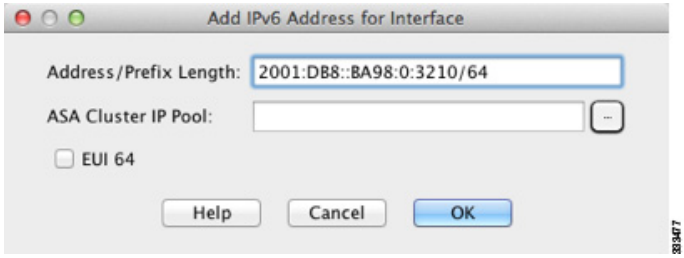
인터페이스에서 스테이트리스 자동 컨피그레이션을 활성화하면, 라우터 광고 메시지에서 수신된 접두사를 기반으로 IPv6 주소가 컨피그레이션됩니다. 스테이트리스 자동 컨피그레이션이 활성화될 경우, Modified EUI-64 인터페이스 ID를 기반으로 하는 Link-Local 주소가 인터페이스에 대해 자동으로 생성됩니다.

참고 RFC 4862에서는 스테이트리스 자동 컨피그레이션에 컨피그레이션된 호스트에서 라우터 광고 메시지를 보내지 않도록 지정하지만, 이 경우에는 ASA에서 라우터 광고 메시지를 전송합니다. 메시지를 보내지 않도록 하려면 **Suppress RA chck box**를 참조하십시오.

- 수동 컨피그레이션 — 전역 IPv6 주소를 수동으로 컨피그레이션하려면

  a. Interface IPv6 Addresses 영역에서 **Add**를 클릭합니다.

  Add IPv6 Address for Interface 대화 상자가 나타납니다.



  b. Address/Prefix Length 필드에 인터페이스 ID를 포함한 전체 전역 IPv6 주소를 입력하거나, IPv6 접두사 길이와 함께 IPv6 접두사를 입력합니다. 접두사만 입력하려면 **EUI 64** 확인란을 선택하여 Modified EUI-64 형식을 사용해 인터페이스 ID를 생성하도록 해야 합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48(전체 주소) 또는 2001:0DB8::/48(접두사, EUI 64 선택됨) 같은 형태입니다. IPv6 주소 지정에 대한 자세한 내용은 43-5 페이지의 IPv6 주소를 참조하십시오.

  참고 ASA 클러스터 IP 풀에 대한 자세한 내용은 9-41 페이지의 개별 인터페이스 구성(관리 인터페이스 권장 사항)를 참조하십시오.

  c. **OK**를 클릭합니다.

8단계 (선택 사항) 어떤 IPv6 접두사가 IPv6 라우터 광고에 포함되는지 구성하려면 26-11 페이지의 라우터 알림에서 IPv6 접두사 구성를 참조하십시오.

9단계 **OK**를 클릭합니다.

Configuration > Device Setup > Interfaces 창으로 돌아갑니다.

IPv6 Neighbor Discovery 구성

IPv6 Neighbor Discovery를 구성하려면 26 장, “IPv6 인접 디바이스 검색”,를 참조하십시오.

(선택 사항) 링크-로컬 주소 자동 구성

전역 주소를 구성하지 않고 링크-로컬 주소만 구성하려는 경우 인터페이스 MAC 주소(Modified EUI-64 형식. MAC 주소는 48비트를 사용하므로 인터페이스 ID에 필요한 64비트를 채우기 위해 추가 비트를 삽입해야 함)를 기반으로 링크-로컬 주소를 만드는 옵션이 있습니다.

링크-로컬 주소를 직접 지정하려면(권장하지 않음) 12-17 페이지의 (선택 사항) 링크-로컬 주소 수동 구성를 참조하십시오.

Modified EUI-64 형식 강제 적용, DAD 설정 등 다른 IPv6 옵션에 대해서는 12-14 페이지의 전역 IPv6 주소 구성를 참조하십시오.

인터페이스에 대한 Link-Local 주소를 자동으로 구성하려면 다음 단계를 수행합니다.

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.

3단계 **IPv6** 탭을 클릭합니다.

4단계 IPv6 컨피그레이션 영역에서 **Enable IPv6** 확인란을 선택합니다.

이 옵션을 선택하면 IPv6를 사용할 수 있으며, 인터페이스 MAC 주소를 기반으로 하는 Modified EUI-64 인터페이스 ID를 사용하여 Link-Local 주소를 자동으로 생성할 수 있습니다.

5단계 **OK**를 클릭합니다.

(선택 사항) 링크-로컬 주소 수동 구성

전역 주소를 구성하지 않고 Link-Local 주소만 구성해야 할 경우, Link-Local 주소를 수동으로 정의하는 옵션을 선택할 수 있습니다. Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

링크-로컬 주소를 자동으로 지정하려면(권장) 12-17 페이지의 (선택 사항) 링크-로컬 주소 자동 구성를 참조하십시오.

Modified EUI-64 형식 강제 적용, DAD 설정 등 다른 IPv6 옵션에 대해서는 12-14 페이지의 전역 IPv6 주소 구성를 참조하십시오.

인터페이스에 Link-Local 주소를 할당하려면 다음 단계를 수행합니다.

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.

3단계 **IPv6** 탭을 클릭합니다.

4단계 링크-로컬 주소를 설정하려면 Link-local address 필드에 주소를 입력합니다.

링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). IPv6 주소 지정에 대한 자세한 내용은 43-5 페이지의 IPv6 주소를 참조하십시오.

5단계 **OK**를 클릭합니다.

동일한 보안 레벨 통신 허용

기본적으로 동일한 보안 레벨의 인터페이스는 서로 통신할 수 없고 패킷이 동일한 인터페이스에 들어오고 나갈 수 없습니다. 이 섹션에서는 인터페이스의 보안 수준이 동일할 때 인터페이스 간 통신을 수행하는 방법, 그리고 인터페이스 내 통신을 수행하는 방법에 대해 설명합니다.

인터페이스 간 통신에 대한 정보

동일한 보안 수준에서 각 인터페이스끼리 서로 통신을 수행할 수 있도록 허용할 경우 다음과 같은 이점이 제공됩니다.

- 101개 이상의 통신 인터페이스를 구성할 수 있습니다.

  인터페이스마다 다른 수준을 사용하고 인터페이스에 동일한 보안 수준을 할당하지 않을 경우, 수준(0~100) 하나당 한 개의 인터페이스만 구성할 수 있습니다.
- 모든 동일한 보안 인터페이스 간에 ACL 없이도 트래픽 흐름이 자유롭게 이루어지도록 하고자 할 수 있습니다.

동일한 보안 인터페이스 통신을 활성화하더라도 기존처럼 여러 보안 레벨에서 인터페이스를 구성할 수 있습니다.

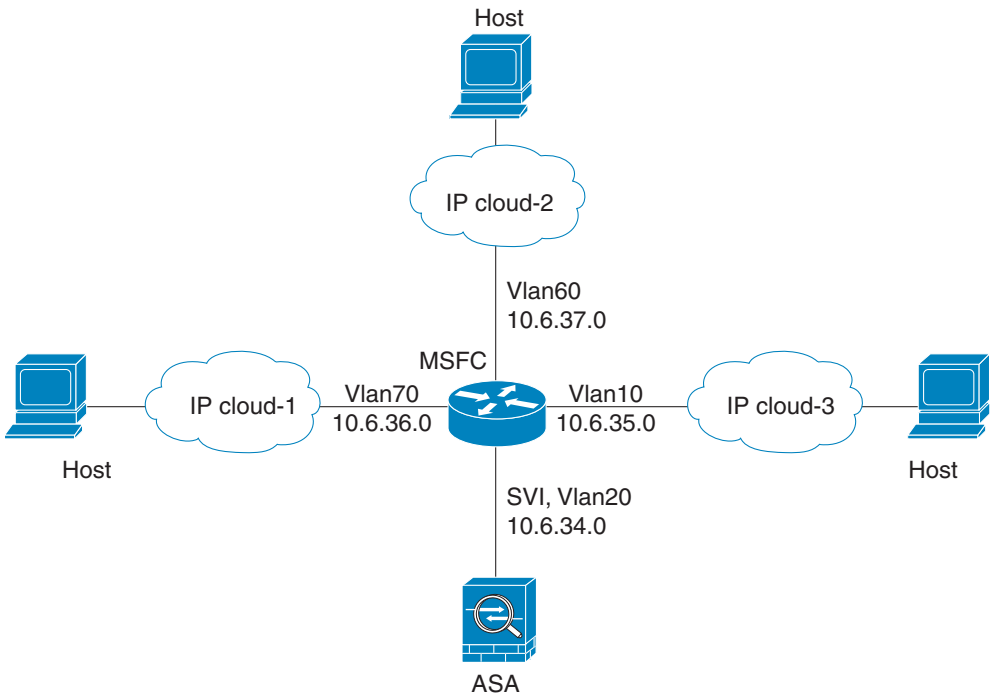
인터페이스 내 통신 정보

인터페이스 내 통신은 인터페이스에 들어오지만 동일한 인터페이스 밖으로 라우팅되는 VPN 트래픽에 유용할 수 있습니다. 이 경우 VPN 트래픽이 암호화되지 않거나 다른 VPN 연결을 위해 다시 암호화될 수 있습니다. 예를 들어, 허브 및 스포크 VPN 네트워크가 있다고 가정했을 때 ASA가 허브이고 원격 VPN 네트워크가 스포크라면, 한 스포크가 다른 스포크와 통신을 수행할 경우 트래픽은 ASA로 들어갔다 나온 후 다시 다른 스포크로 들어가야 합니다.

참고 이 기능을 통해 허용되는 모든 트래픽은 여전히 방화벽 규칙의 적용을 받습니다. 비대칭 라우팅 현상을 초래하지 않도록 주의하십시오. 이 경우 반환 트래픽이 ASA로 이동하지 않는 결과가 발생할 수 있습니다.

ASASM의 경우 이 기능을 활성화하기 전에, MSFC를 먼저 올바르게 구성하여 패킷이 스위치를 직접 통해 목적지 호스트에서 전송되는 대신 ASA MAC 주소로 전송되도록 해야 합니다. 그림 12-1에는 동일한 인터페이스의 호스트 간에 통신을 수행해야 하는 네트워크가 나와 있습니다.

그림 12-1 동일한 인터페이스에 있는 호스트 간의 통신



다음 샘플 컨피그레이션에는 Cisco IOS **route-map** 명령을 사용하여 그림 12-1에 표시된 정책 라우팅을 활성화하는 방법이 나와 있습니다.

```
route-map intra-inter3 permit 0
    match ip address 103
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter2 permit 20
    match ip address 102
    set interface Vlan20
    set ip next-hop 10.6.34.7
!
route-map intra-inter1 permit 10
    match ip address 101
    set interface Vlan20
    set ip next-hop 10.6.34.7
```

세부 단계

- 동일한 보안 레벨의 인터페이스가 서로 통신할 수 있게 하려면 Configuration > Interfaces 창에서 **Enable traffic between two or more interfaces which are configured with same security level**을 클릭합니다.
- 동일한 인터페이스에 연결된 호스트 간의 통신을 활성화하려면 **Enable traffic between two or more hosts connected to the same interface**를 선택합니다.

인터페이스 끄기 및 켜기

이 섹션에서는 인터페이스를 끄고 켜는 방법을 설명합니다.

모든 인터페이스는 기본적으로 활성화되어 있습니다. 다중 컨텍스트 모드에서는 어떤 컨텍스트 내에서 인터페이스를 비활성화하거나 다시 활성화할 경우 그 컨텍스트 인터페이스에만 적용됩니다. 그러나 시스템 실행 영역에서 인터페이스를 비활성화하거나 다시 활성화하면 모든 컨텍스트의 해당 인터페이스에 적용됩니다.

세부 단계

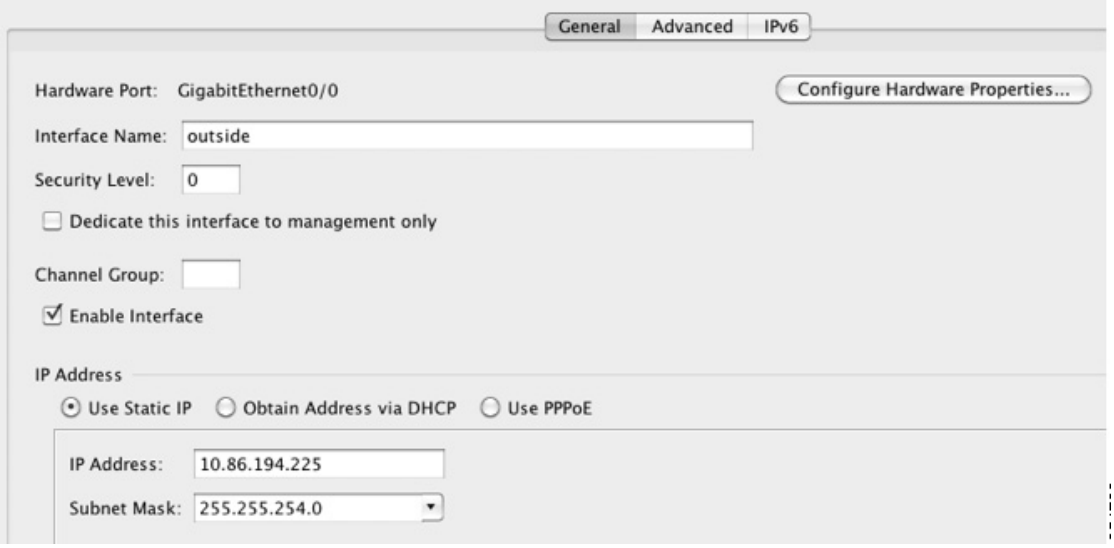
1단계 컨텍스트 모드에 따라

- 단일 모드에서는 **Configuration > Device Setup > Interfaces** 창을 선택합니다.
- 다중 모드의 경우 시스템 실행 영역에서 **Configuration > Context Management > Interfaces** 창을 선택합니다.

기본적으로 모든 물리적 인터페이스가 나열됩니다.

2단계 구성할 VLAN 인터페이스를 클릭하고 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 나타납니다.



3단계 인터페이스를 활성화하거나 비활성화하려면 **Enable Interface** 확인란을 선택하거나 선택 취소합니다.

인터페이스 모니터링

ARP 테이블

Monitoring > Interfaces > ARP Table 창에는 상태 및 동적 항목을 비롯한 ARP 테이블이 표시됩니다. ARP 테이블에는 MAC 주소를 정해진 인터페이스의 IP 주소에 매핑하는 항목이 포함됩니다.

필드

- Interface — 매핑과 관련된 인터페이스 이름이 나열됩니다.
- IP Address — IP 주소가 표시됩니다.
- MAC Address — MAC 주소가 표시됩니다.
- Proxy ARP — 인터페이스에서 프록시 ARP를 활성화할 경우 Yes로 표시됩니다. 인터페이스에서 프록시 ARP를 활성화하지 않은 경우 No로 표시됩니다.
- Clear — 동적 ARP 테이블 항목을 지웁니다. 고정 항목은 지워지지 않습니다.
- Refresh — 테이블을 ASA의 최신 정보로 새로 고치고 Last Updated 날짜 및 시간을 업데이트합니다.
- Last Updated — *표시 전용 항목입니다.* 날짜 및 시간 표시가 업데이트되었는지 표시됩니다.

DHCP

ASA를 사용하면 클라이언트에 할당된 주소, ASA 인터페이스의 리스 정보, DHCP 통계를 비롯한 DHCP 상태를 모니터링할 수 있습니다.

DHCP 서버 테이블

Monitoring > Interfaces > DHCP > DHCP Server Table 목록에는 DHCP 클라이언트에 할당된 IP 주소가 나열됩니다.

필드

- IP Address — 클라이언트에 할당된 IP 주소가 표시됩니다.
- Client-ID — 클라이언트 MAC 주소 또는 ID가 표시됩니다.
- Lease Expiration — DHCP 리스가 만료되는 날짜가 표시됩니다. 리스는 할당된 IP 주소를 클라이언트에서 사용할 수 있는 기간을 나타냅니다. 남은 시간은 초 단위로 지정되며 Last Updated 표시 전용 필드의 타임 스탬프를 기준으로 합니다.

- Number of Active Leases — DHCP 리스의 총 수가 표시됩니다.
- Refresh — ASA의 정보를 새로 고칩니다.
- Last Updated — 테이블의 데이터가 언제 마지막으로 업데이트되었는지 표시됩니다.

DHCP 클라이언트 리스 정보

DHCP 서버에서 ASA 인터페이스 IP 주소를 얻은 경우 Monitoring > Interfaces > DHCP > DHCP Server Table > DHCP Client Lease Information 창에는 DHCP 리스에 대한 정보가 표시됩니다.

필드

- Select an interface — ASA 인터페이스가 나열됩니다. DHCP 리스를 보려는 인터페이스를 선택합니다. 인터페이스에 DHCP 리스가 여러 개 있는 경우, 보려는 인터페이스 및 IP 주소 쌍을 선택합니다.
- Attribute and Value — 인터페이스 DHCP 리스의 속성 및 값이 나열됩니다.
  - Temp IP addr — *표시 전용입니다.* 인터페이스에 할당된 IP 주소입니다.
  - Temp sub net mask — *표시 전용입니다.* 인터페이스에 할당된 서브넷 마스크입니다.
  - DHCP lease server — *표시 전용입니다.* DHCP 서버 주소입니다.
  - state — *표시 전용입니다.* DHCP 리스의 상태는 다음과 같습니다.

    Initial — 초기화 상태이며 ASA에서 리스를 얻기 위한 프로세스를 시작합니다. 또한 이 상태에는 리스가 언제 끝나는지 또는 리스 협상이 언제 실패했는지 여부가 표시됩니다.

    Selecting — ASA가 하나 이상의 DHCP 서버에서 DHCPOFFER 메시지를 받기 위해 대기 중이며, 해당 메시지 중 하나를 선택할 수 있습니다.

    Requesting — ASA가 요청을 전송한 서버에서 다시 응답을 받기 위해 대기 중입니다.

    Purging — ASA가 오류 발생으로 인해 리스를 지우는 중입니다.

    Bound — ASA에 잘못된 리스가 있으며 정상적으로 작동 중입니다.

    Renewing — ASA에서 리스를 갱신하려고 시도 중입니다. ASA에서는 DHCP 서버에 정기적으로 DHCPREQUEST 메시지를 전송하고 응답을 기다립니다.

    Rebinding — ASA에서 원래 서버의 리스를 갱신하지 못했으며, 서버 또는 리스 엔드에서 응답을 받을 때까지 DHCPREQUEST 메시지를 전송합니다.

    Holddown — ASA에서 리스를 제거하기 위한 프로세스를 시작했습니다.

    Releasing — ASA에서 IP 주소가 더 이상 필요하지 않음을 알리는 릴리스 메시지를 서버에 보냅니다.
  - Lease — *표시 전용입니다.* 인터페이스에서 이 IP 주소를 사용할 수 있는 시간의 길이이며 DHCP 서버에서 지정됩니다.
  - Renewal — *표시 전용입니다.* 인터페이스에서 이 리스의 자동 갱신을 시도하는 데 걸리는 시간의 길이입니다.
  - Rebind — *표시 전용입니다.* ASA에서 DHCP 서버에 리바인딩을 시도하는 데 걸리는 시간의 길이입니다. 리바인딩은 ASA에서 원래 DHCP 서버와 통신을 수행할 수 없고, 리스 기간의 87.5%가 만료되었을 때 발생합니다. 그러면 ASA에서는 DHCP 요청을 브로드캐스트하여 사용 가능한 모든 DHCP 서버에 접속을 시도합니다.
  - Next timer fires after — *표시 전용입니다.* 내부 타이머가 시작될 때까지 소요되는 시간(초 단위)입니다.

  - Retry count — *표시 전용입니다.* ASA에서 리스 설정을 시도할 경우 이 필드에는 ASA에서 DHCP 메시지 전송을 시도한 횟수가 표시됩니다. 예를 들어, ASA가 Selecting 상태인 경우 이 값에는 ASA에서 검색 메시지를 전송한 횟수가 표시됩니다. ASA가 Requesting 상태인 경우 이 값에는 ASA에서 요청 메시지를 전송한 횟수가 표시됩니다.
  - Client-ID — *표시 전용입니다.* 서버와의 모든 통신에 사용되는 클라이언트 ID입니다.
  - Proxy — *표시 전용입니다.* 이 인터페이스가 VPN 클라이언트의 프록시 DHCP 클라이언트인지 True 또는 False로 지정합니다.
  - Hostname — *표시 전용입니다.* 클라이언트 호스트 이름입니다.

DHCP 통계

Monitoring > Interfaces > DHCP > DHCP Statistics 창에 DHCP 서버 기능의 통계가 표시됩니다.

필드

- Message Type —보내거나 받은 DHCP 메시지 유형이 나열됩니다.
  - BOOTREQUEST
  - DHCPDISCOVER
  - DHCPREQUEST
  - DHCPDECLINE
  - DHCPRELEASE
  - DHCPINFORM
  - BOOTREPLY
  - DHCPOFFER
  - DHCPACK
  - DHCPNAK
- Count — 특정 메시지를 처리한 횟수가 표시됩니다.
- Direction — 메시지 유형이 Sent인지 또는 Received인지 표시됩니다.
- Total Messages Received — ASA에서 수신한 총 메시지 수가 표시됩니다.
- Total Messages Sent — ASA에서 보낸 총 메시지 수가 표시됩니다.
- Counter — 일반적인 통계 DHCP 데이터가 표시되며 다음 항목이 포함됩니다.
  - DHCP UDP 전달 불가 오류
  - DHCP 기타 UDP 오류
  - 주소 풀
  - 자동 바인딩
  - 만료된 바인딩
  - 잘못된 형식의 메시지
- Value — 각 카운터 항목의 수가 표시됩니다.
- Refresh — DHCP 테이블 목록을 업데이트합니다.
- Last Updated — 테이블의 데이터가 언제 마지막으로 업데이트되었는지 표시됩니다.

MAC 주소 테이블

Monitoring > Interfaces > MAC Address Table 창에 고정 및 동적 MAC 주소 항목이 표시됩니다. MAC 주소 테이블 및 고정 항목 추가에 대한 자세한 내용은 12-24 페이지의 MAC 주소 테이블를 참조하십시오.

필드

- Interface — 항목과 관련된 인터페이스 이름이 표시됩니다.
- MAC Address — MAC 주소가 표시됩니다.
- Type — 항목이 고정인지 동적인지 표시합니다.
- Age — 항목의 기간(분 단위)을 표시합니다. 시간 제한을 설정하려면 12-24 페이지의 MAC 주소 테이블를 참조합니다.
- Refresh — 테이블을 ASA의 최신 정보로 새로 고칩니다.

동적 ACL

Monitoring > Interfaces > Dynamic ACLs 창에는 ASA에서 생성, 활성화 및 삭제된 ACL을 제외한 사용자 구성 ACL과 기능적으로 동일한 동적 ACL의 테이블이 표시됩니다. 이러한 ACL은 컨피그레이션에 표시되지 않으며 이 테이블에만 표시됩니다. ACL은 ACL 헤더에서 "(dynamic)" 키워드로 확인합니다.

이 테이블에서 ACL을 선택하면 해당 ACL의 내용이 아래 텍스트 필드에 표시됩니다.

필드

- ACL — 동적 ACL의 이름이 표시됩니다.
- Element Count — ACL의 요소 개수가 표시됩니다.
- Hit Count — ACL의 모든 요소의 총 히트 수가 표시됩니다.

인터페이스 그래프

Monitoring > Interfaces > Interface Graphs 창을 사용하면 인터페이스 통계를 그래프 또는 테이블 형식으로 볼 수 있습니다. 컨텍스트 간에 인터페이스가 공유될 경우, ASA에서는 현재 컨텍스트에 대한 통계만 표시합니다. 하위 인터페이스에 표시되는 통계 수치는 물리적 인터페이스에 표시되는 통계 수치의 하위 집합입니다.

필드

- Available Graphs for — 모니터링에 사용할 수 있는 통계 유형이 나열됩니다. 하나의 그래프 창에 최대 4가지 유형의 통계가 표시되도록 선택할 수 있습니다. 동시에 여러 그래프 창을 열 수 있습니다.
  - Byte Counts — 인터페이스에 대한 바이트 입력 및 출력의 개수가 표시됩니다.
  - Packet Counts — 인터페이스에 대한 패킷 입력 및 출력의 개수가 표시됩니다.
  - Packet Rates — 인터페이스에 대한 패킷 입력 및 출력의 속도가 표시됩니다.
  - Bit Rates — 인터페이스에 대한 입력 및 출력의 비트 속도가 표시됩니다.
  - Drop Packet Count — 인터페이스에서 손실된 패킷의 개수가 표시됩니다.

다음과 같은 추가 통계가 물리적 인터페이스에 표시됩니다.

- Buffer Resources — 다음 통계가 표시됩니다.

  Overruns — 입력 속도가 ASA에서 데이터를 처리할 수 있는 역량을 초과하여, 수신된 데이터를 ASA에서 하드웨어 버퍼로 넘길 수 없는 횟수입니다.

  Underruns — ASA에서 처리할 수 있는 것보다 빠른 속도로 전송 장치가 실행된 횟수입니다.

  No Buffer — 기본 시스템에 버퍼 공간이 없어 지워진 수신 패킷의 개수입니다. 이 값을 무시된 개수와 비교합니다. 이더넷 네트워크의 브로드캐스트 스톰으로 인해 입력 버퍼 없음 이벤트가 발생하는 경우가 많습니다.

- Packet Errors — 다음과 같은 통계가 표시됩니다.

  CRC — Cyclical Redundancy Check 오류의 개수입니다. 스테이션에서 프레임을 전송할 경우, 프레임의 끝에 CRC가 추가됩니다. 이러한 CRC는 프레임의 데이터를 기반으로 한 알고리즘에서 생성됩니다. 소스와 목적지 간에 프레임이 변경된 경우, ASA에 CRC가 일치하지 않는다는 메시지가 표시됩니다. CRC 수가 높을수록 충돌이나 스테이션 전송 오류 데이터가 발생하는 경우가 많습니다.

  Frame — 프레임 오류 개수입니다. 오류 프레임에는 잘못된 길이 또는 불량 프레임 체크섬이 있는 패킷이 포함되어 있습니다. 이러한 오류로 인해 충돌이나 이더넷 디바이스 고장이 주로 발생할 수 있습니다.

  Input Errors — 여기에 나열된 기타 유형을 비롯한 입력 오류의 총 개수입니다. 입력과 관련된 기타 오류로 인해서도 입력 오류 발생 횟수가 늘어날 수 있으며, 일부 데이터그램에 여러 개의 오류가 포함될 수 있습니다. 따라서 이러한 총계는 기타 유형에 나열된 오류 수를 초과할 수 있습니다.

  Runts — 최소 패킷 크기(64바이트)보다 크기가 작아 삭제된 패킷의 개수입니다. Runt는 일반적으로 충돌로 인해 발생합니다. 또한 잘못된 배선 및 전기 간섭에 의해서도 발생할 수 있습니다.

  Giants — 최대 패킷 크기를 초과하여 삭제된 패킷의 개수입니다. 예를 들어, 1518바이트보다 큰 이더넷 패킷은 giant로 간주합니다.

  Deferred — FastEthernet 인터페이스에만 해당됩니다. 링크의 작업으로 인해 전송 전에 연기된 프레임의 개수입니다.

- Miscellaneous — 수신된 브로드캐스트의 통계를 표시합니다.

- Collision Counts — FastEthernet 인터페이스에만 해당됩니다. 다음과 같은 통계가 표시됩니다.

  Output Errors — 최대 충돌 수가 구성된 수를 초과하여 전송되지 않은 프레임의 개수입니다. 이 카운터는 네트워크 트래픽이 과중한 동안에만 증가해야 합니다.

  Collisions — 이더넷 충돌(단일 또는 다중 충돌)로 인해 다시 전송된 메시지의 개수입니다. 이러한 현상은 LAN을 과도하게 연장할 경우 주로 발생합니다(이더넷 또는 트랜시버 케이블을 스테이션 간의 두 중계기보다 길게 연장하거나, 다중 포트 트랜시버를 너무 많이 중첩한 경우). 충돌되는 패킷은 출력 패킷별로 한 번만 계산됩니다.

  Late Collisions — 충돌이 정상적인 충돌 범위 밖에서 발생하여 전송되지 못한 프레임의 개수입니다. 지연된 충돌은 패킷의 전송 과정에서 뒤늦게 감지된 충돌입니다. 일반적으로 이러한 현상은 일어나지 않습니다. 2개의 이더넷 호스트에서 동시에 통신을 수행하려고 할 경우 패킷에서 초기에 충돌이 발생하고 둘 다 작업을 잠시 중단하거나, 첫 번째 호스트에서 통신을 수행하고 있으니 대기해야 한다는 메시지가 두 번째 호스트에 표시됩니다. 지연된 충돌이 발생할 경우, 디바이스가 갑자기 실행되어 이더넷에 패킷을 전송하려고 시도하는 반면 ASA에서는 패킷 전송을 부분적으로 완료합니다. ASA에서 패킷의 첫 번째 부분을 보유하고 있던 버퍼를 해제했을 수 있으므로, 패킷이 다시 전송되지 않습니다. 충돌을 해

결하기 위해 패킷을 다시 전송하여 네트워킹 프로토콜을 다시 설계하므로 이는 문제가 되지 않습니다. 그러나 지연된 충돌은 네트워크에 문제가 있음을 나타냅니다. 일반적인 문제는 사양을 초과하여 실행되는 대량의 반복적인 네트워크 및 이더넷 네트워크입니다.

  - Input Queue — 입력 대기열의 현재 및 최대 패킷 수가 표시되며 다음 통계가 포함됩니다.

    Hardware Input Queue — 하드웨어 대기열의 패킷 수입니다.

    Software Input Queue — 소프트웨어 대기열의 패킷 수입니다.
  - Output Queue — 출력 대기열의 현재 및 최대 패킷 수가 표시되며 다음 통계가 포함됩니다.

    Hardware Output Queue — 하드웨어 대기열의 패킷 수입니다.

    Software Output Queue — 소프트웨어 대기열의 패킷 수입니다.

- Add — 선택한 통계 유형을 선택한 그래프 창에 추가합니다.
- Remove — 선택한 통계 유형을 선택한 그래프 창에서 제거합니다. 다른 패널에서 추가된 항목을 제거할 경우 이 버튼 이름이 Delete로 변경되며, Available Graphs 창으로 돌아가지 않습니다.
- Show Graphs — 통계 유형을 추가하려는 그래프 창 이름을 표시합니다. 그래프 창이 이미 열려 있는 경우 새 그래프 창이 기본적으로 나열됩니다. 이미 열려 있는 그래프에 통계 유형을 추가하려면 열려 있는 그래프 창의 이름을 선택합니다. 그래프에 이미 포함된 통계는 Selected Graphs 창에 표시되며, 여기에 추가적인 유형을 추가할 수 있습니다. 그래프 창의 이름은 ASDM의 이름을 따서 명명되며 인터페이스 IP 주소 및 이름 "Graph"가 붙습니다. 후속 그래프의 이름은 “Graph (2)” 등으로 명명됩니다.
- Selected Graphs — 선택한 그래프 창에 표시하려는 통계 유형이 표시됩니다. 최대 4가지 유형을 포함할 수 있습니다.
  - Show Graphs — 그래프 창을 표시하거나 추가 통계 유형이 추가된 경우 그래프를 업데이트합니다.

그래프/테이블

Monitoring > Interfaces > Interface Graphs > Graph/Table 창에는 선택한 통계에 대한 그래프가 표시됩니다. Graph 창에는 한 번에 최대 4가지 그래프를 표시할 수 있습니다. 기본적으로 그래프 또는 테이블에는 실시간 통계가 표시됩니다. History Metrics를 활성화할 경우(3-32 페이지의 History Metrics 활성화 참조) 이전 기간의 통계를 볼 수 있습니다.

필드

- View — 그래프 또는 테이블의 기간을 설정합니다. 실시간이 아닌 기간을 보려면 History Metrics를 활성화합니다(3-32 페이지의 History Metrics 활성화 참조) 데이터는 다음 옵션의 사양에 따라 업데이트됩니다.
  - 실시간, 10초당 데이터
  - 최근 10분, 10초당 데이터
  - 최근 60분, 1분당 데이터
  - 최근 12시간, 12분당 데이터
  - 최근 5일, 2시간당 데이터
- Export — 그래프를 쉼표로 구분된 값 형식으로 내보냅니다. Graph 창에 여러 개의 그래프 또는 테이블이 있을 경우, Export Graph Data 대화 상자가 표시됩니다. 이름 옆의 확인란을 선택하여 나열된 그래프 및 테이블을 하나 이상 선택합니다.
- Print — 그래프 또는 테이블을 인쇄합니다. Graph 창에 여러 개의 그래프 또는 테이블이 있을 경우, Print Graph 대화 상자가 표시됩니다. Graph/Table Name 목록에서 인쇄하려는 그래프 또는 테이블을 선택합니다.

- Bookmark — Graphs 창에서 모든 그래프 및 테이블에 대한 단일 링크 및 각 그래프 또는 테이블에 대한 개별 링크가 포함된 브라우저 창을 엽니다. 브라우저에서 이러한 URL을 북마크로 복사할 수 있습니다.그래프에 대한 URL을 열 때 ASDM을 실행하지 않아도 됩니다. 브라우저에서 ASDM을 시작하고 그래프를 표시합니다.

PPPoE 클라이언트

Monitoring > Interfaces > PPPoE Client > PPPoE Client Lease Information 창에는 현재 PPPoE 연결에 대한 정보가 표시됩니다.

필드

Select a PPPoE interface — PPPoE 클라이언트 리스 정보를 보려는 인터페이스를 선택합니다.

Refresh — ASA에서 최신 연결 정보를 로드하여 표시합니다.

인터페이스 연결

고정 경로 추적이 구성된 경우 Monitoring > Interfaces 트리에는 Monitoring > Interfaces > *interface* 연결 노드만 표시됩니다. 몇 가지 경로를 추적한 경우, 각 인터페이스에는 추적한 경로가 포함된 노드가 형성됩니다.

경로 추적 정보에 대한 자세한 내용은 다음을 참조하십시오.

- 12-27 페이지의 추적 상태
- 12-27 페이지의 모니터링 통계

추적 상태

Monitoring > Interfaces > interface connection > Track Status for 창에는 추적한 객체에 대한 정보가 표시됩니다.

필드

- Tracked Route — *표시 전용입니다.* 추적 프로세스와 관련된 경로가 표시됩니다.
- Route Statistics — *표시 전용입니다.* 객체의 도달 범위가 표시되며 여기에는 도달 범위가 최종 변경된 시기, 작업 반환 코드, 추적을 수행 중인 프로세스가 포함됩니다.

모니터링 통계

Monitoring > Interfaces > interface connection > Monitoring Statistics for 창에는 SLA 모니터링 프로세스의 통계가 표시됩니다.

필드

- SLA Monitor ID — *표시 전용입니다.* SLA 모니터링 프로세스의 ID가 표시됩니다.
- SLA statistics — *표시 전용입니다.* 프로세스가 수정된 최종 시간, 작업 시도 횟수, 작업을 건너뛴 횟수 등을 비롯한 SLA 모니터링 통계가 표시됩니다.

라우팅 모드의 인터페이스 기능 기록

표 12-1에서는 이 기능의 출시 내역을 정리합니다.

표 12-1 인터페이스의 기능 기록

기능 이름	릴리스	기능 정보
VLAN 증가	7.0(5)	다음 한도를 높였습니다. • ASA5510 Base 라이센스의 VLAN을 0개에서 10개로 • ASA5510 Security Plus 라이센스의 VLAN을 10개에서 25개로 • ASA5520 VLAN을 25개에서 100개로 • ASA5540 VLAN을 100개에서 200개로
VLAN 증가	7.2(2)	ASA 5505 Security Plus 라이센스의 VLAN 최대 개수를 5개(3개는 전 기능, 1개는 장애 조치, 1개는 백업 인터페이스에 한정)에서 20개 전 기능 인터페이스로 늘렸습니다. 또한 트렁크 포트 수도 1개에서 8개로 늘렸습니다. 이제 20개의 전 기능 인터페이스를 지원하므로, 백업 ISP 인터페이스를 무력화하기 위해 백업 인터페이스 명령을 사용할 필요 없습니다. 이 목적으로 전 기능 인터페이스를 사용할 수 있습니다. 백업 인터페이스 명령은 Easy 컨피그레이션에서 여전히 유용합니다. ASA 5510의 VLAN 한도도 늘어났습니다. Base 라이센스는 10개에서 50개로, Security Plus 라이센스는 25개에서 100개로 늘어났습니다. ASA 5520은 100개에서 150개로, ASA 5550은 200개에서 250개로 늘어났습니다.
ASA 5510 Security Plus 라이센스의 기가비트 이더넷 지원	7.2(3)	ASA 5510 Security Plus 라이센스는 포트 0과 포트 1에서 GE(기가비트 이더넷)를 지원합니다. Base 라이센스를 Security Plus 라이센스로 업그레이드할 경우 외부 Ethernet0/0 및 Ethernet0/1 포트의 용량이 원래의 FE(패스트 이더넷)(100Mbps)에서 GE(1000Mbps)로 증가합니다. 인터페이스 이름은 그대로 Ethernet 0/0 및 Ethernet 0/1입니다.
ASA 5505의 VLAN 기본 지원	7.2(4)/8.0(4)	ASA 5505 트렁크 포트에 기본 VLAN을 포함할 수 있습니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Interfaces > Switch Ports > Edit Switch Port
ASA 5580의 점보 패킷 지원	8.1(1)	Cisco ASA 5580은 점보 프레임을 지원합니다. 점보 프레임은 표준 최대 크기인 1518바이트(레이어 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷으로 최대 크기가 9216바이트입니다. 모든 인터페이스에서 이더넷 프레임 처리용 메모리 용량을 늘려 점보 프레임 지원을 활성화할 수 있습니다. 점보 프레임에 더 많은 메모리를 할당하면 ACL와 같은 다른 기능을 최대 한도로 사용하는 데 제약이 따를 수 있습니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced

표 12-1 인터페이스의 기능 기록 (계속)

기능 이름	릴리스	기능 정보
ASA 5580의 VLAN 증가	8.1(2)	ASA 5580에서 지원되는 VLAN 수가 100개에서 250개로 늘어났습니다.
투명 모드의 IPv6 지원	8.2(1)	투명 방화벽 모드를 위한 IPv6 지원을 도입했습니다.
ASA 5580 10기가비트 이더넷 인터페이스에서 흐름 제어를 위한 일시 중지 프레임 지원	8.2(2)	흐름 제어를 위해 Pause(XOFF) 프레임을 활성화할 수 있습니다. 다음 화면을 수정했습니다. (단일 모드) Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced (다중 모드, 시스템) Configuration > Interfaces > Add/Edit Interface

13 장

투명 모드 인터페이스

이 장에서는 투명 방화벽 모드의 모든 모델에서 인터페이스 컨피그레이션을 완료하는 작업을 다룹니다.

참고 다중 모드에서는 상황 실행 영역에서 이 섹션의 작업을 수행합니다. Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 상황 이름을 두 번 클릭합니다.

투명 모드 인터페이스에 대한 정보

투명 모드의 브리지 그룹

보안 상황의 오버헤드를 원치 않을 경우 또는 보안 상황 정보 사용을 극대화하려는 경우, 인터페이스를 하나의 브리지 그룹으로 묶은 다음 네트워크마다 하나씩, 여러 브리지 그룹을 구성할 수 있습니다. 브리지 그룹 트래픽은 다른 브리지 그룹과 분리됩니다. 트래픽이 Cisco ASA 내의 다른 브리지 그룹으로 라우팅되지 않으며, 반드시 ASA를 나와야 외부 라우터에 의해 ASA의 다른 브리지 그룹으로 라우팅될 수 있습니다. 브리지 기능은 브리지 그룹마다 따로 있지만, 다른 여러 기능은 모든 브리지 그룹이 공유합니다. 예를 들어, 모든 브리지 그룹은 syslog 서버 또는 AAA 서버 컨피그레이션을 공유합니다. 완전한 보안 정책 분리를 위해서는 각 상황에서 한 브리지 그룹의 보안 상황를 사용합니다. 상황마다 또는 단일 모드에서 하나 이상의 브리지 그룹이 필요합니다.

각 브리지 그룹에는 관리 IP 주소가 필요합니다. 다른 관리 방법에 대해서는 10-2 페이지의 관리 인터페이스를 참조하십시오.

참고 ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. 관리 IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.

보안 레벨

각 인터페이스는 0(가장 낮음)~100(가장 높음)의 보안 레벨이 있어야 합니다. 예를 들어, 내부 호스트 네트워크와 같이 가장 안전한 네트워크는 레벨 100으로 지정해야 합니다. 반면에 인터넷에 연결된 외부 네트워크는 레벨 0이 될 수 있습니다. DMZ와 같은 다른 네트워크는 그 사이의 값이 될 수 있습니다. 인터페이스를 동일한 보안 레벨에 지정할 수 있습니다. 자세한 내용은 13-19 페이지의 동일한 보안 레벨 통신 허용를 참조하십시오.

이 레벨은 다음 동작을 제어합니다.

- 네트워크 액세스—기본적으로 상위 보안 인터페이스에서 하위 보안 인터페이스로 암시적 허용이 이루어집니다(아웃바운드). 상위 보안 인터페이스의 호스트는 하위 보안 인터페이스의 어떤 호스트에도 액세스할 수 있습니다. 인터페이스에 ACL을 적용하여 액세스를 제한할 수 있습니다.

  동일한 보안 인터페이스에 대한 통신을 활성화할 경우(13-19 페이지의 동일한 보안 레벨 통신 허용 참조), 해당 인터페이스에서 보안 레벨이 같거나 더 낮은 다른 인터페이스에 액세스하는 것이 암시적으로 허용됩니다.
- 검사 엔진—일부 애플리케이션 검사 엔진은 보안 레벨에 좌우됩니다. 동일한 보안 인터페이스에서는 검사 엔진이 어느 방향의 트래픽에도 적용됩니다.
  - NetBIOS 검사 엔진—아웃바운드 연결에만 적용됩니다.
  - SQL*Net 검사 엔진—어떤 호스트 쌍에 SQL*Net(이전의 OraServ) 포트에 대한 제어 연결이 있을 경우 인바운드 데이터 연결만 ASA에서 허용됩니다.
- 필터링—HTTP(S) 및 FTP 필터링은 아웃바운드 연결(상위에서 하위로)에만 적용됩니다.

  동일한 보안 인터페이스에 대한 통신을 활성화한 경우 어느 방향의 트래픽도 필터링할 수 있습니다.
- **established** 명령—이 명령은 상위 보안 호스트에서 하위 보안 호스트로의 연결이 이미 설정된 경우 하위 호스트에서 상위 호스트로 돌아가는 연결을 허용합니다.

  동일한 보안 인터페이스에 대한 통신을 활성화한 경우 양방향 모두에 **established** 명령을 구성할 수 있습니다.

투명 모드 인터페이스를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASA 5512-X	VLAN: Base 라이센스: 50 Security Plus 라이센스: 100 모든 유형의 인터페이스: Base 라이센스: 716 Security Plus 라이센스: 916

모델	라이센싱 요구 사항
ASA 5515-X	VLAN: Base 라이센스: 100 모든 유형의 인터페이스: Base 라이센스: 916
ASA 5525-X	VLAN: Base 라이센스: 200 모든 유형의 인터페이스: Base 라이센스: 1316
ASA 5545-X	VLAN: Base 라이센스: 300 모든 유형의 인터페이스: Base 라이센스: 1716
ASA 5555-X	VLAN: Base 라이센스: 500 모든 유형의 인터페이스: Base 라이센스: 2516
ASA 5585-X	VLAN: Base 및 Security Plus 라이센스: 1024 SSP-10 및 SSP-20을 위한 인터페이스 속도: Base 라이센스—파이버 인터페이스용 1기가비트 이더넷 10GE I/O 라이센스(Security Plus)—파이버 인터페이스용 10기가비트 이더넷 (SSP-40 및 SSP-60은 10기가비트 이더넷을 기본적으로 지원) 모든 유형의 인터페이스: Base 및 Security Plus 라이센스: 4612

참고 어떤 인터페이스가 VLAN 한도의 대상이 되려면 이 인터페이스에 VLAN을 지정해야 합니다.

모든 유형의 인터페이스는 전체 인터페이스, 이를테면 VLAN 인터페이스, 물리적 인터페이스, 이중 인터페이스, 브리지 그룹 인터페이스, EtherChannel 인터페이스의 최대 개수로 이루어집니다. 컨피그레이션에 정의된 모든 **interface**은 이 한도의 대상이 됩니다.

모델	라이센싱 요구 사항
ASASM	VLAN: Base 라이센스: 1000

투명 모드 인터페이스의 지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

상황 모드 가이드라인

- 다중 상황 모드의 ASA 5512-X 이상에서는 시스템 실행 영역에서 10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.에 따라 물리적 인터페이스를 구성합니다. 그런 다음 상황 실행 영역에서 이 장의 내용에 따라 논리적 인터페이스 파라미터를 구성합니다. 다중 상황 모드의 ASASM에서는 스위치에서 스위치 포트와 VLAN을 구성하고 2장, “Switch Configuration for the Cisco ASA Services Module.” 에 따라 ASASM에 VLAN을 지정합니다.

  ASAv는 다중 상황 모드를 지원하지 않습니다.
- 시스템 컨피그레이션에서을 사용하여 이미 상황에 지정한 상황 인터페이스만 컨피그레이션할 수 있습니다.

방화벽 모드 가이드라인

- 단일 모드에서 또는 다중 모드는 상황마다 최대 250개의 브리지 그룹을 구성할 수 있습니다. 하나 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.
- 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다.
- IPv4에서는 관리 트래픽과 ASA를 거칠 트래픽 모두 브리지 그룹마다 관리 IP 주소가 필요합니다.

  인터페이스마다 IP 주소가 필요한 라우티드 모드와 달리, 투명 방화벽은 브리지 그룹 전체에 IP 주소가 지정됩니다. ASA에서는 ASA에서 시작하는 패킷(예: 시스템 메시지 또는 AAA 통신)의 소스 주소로 이 IP 주소를 사용합니다. 브리지 그룹 관리 주소 외에도 일부 모델에서는 관리 인터페이스를 구성할 수도 있습니다. 자세한 내용은 10-2 페이지의 관리 인터페이스를 참조하십시오.

  관리 IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. 서브넷을 호스트 서브넷(255.255.255.255)으로 설정할 수 없습니다. ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. 관리 IP 주소와 동일한 네트워크의 트래픽만 지원됩니다. 관리 IP 서브넷에 대한 자세한 내용은 13-6 페이지의 브리지 그룹 구성를 참조하십시오.
- IPv6에서는 적어도 전달할 트래픽에 대해서는 인터페이스마다 링크-로컬 주소를 구성해야 합니다. ASA 관리 기능을 포함하여 모든 기능을 제공하려면 브리지 그룹마다 전역 IPv6 주소를 구성해야 합니다.
- 다중 상황 모드에서는 상황마다 다른 인터페이스를 사용해야 합니다. 여러 상황에서 한 인터페이스를 공유할 수 없습니다.
- 다중 상황 모드에서는 일반적으로 상황마다 다른 서브넷을 사용합니다. 겹치는 서브넷을 사용할 수도 있으나, 네트워크 토폴로지상 라우터 및 NAT 컨피그레이션에서 라우팅과 관련하여 이를 허용해야 합니다.

장애 조치 지침

이 장의 절차를 사용하여 장애 조치 인터페이스 구성을 마쳐서는 안 됩니다. 장애 조치 및 상태 링크 구성에 대해서는 8 장, “고가용성을 위한 장애 조치”,를 참조하십시오. 다중 상황 모드에서는 시스템 컨피그레이션에서 장애 조치 인터페이스가 컨피그레이션됩니다.

IPv6 지침

투명 모드에서는 IPv6 애니캐스트 주소를 지원하지 않습니다.

ASASM를 위한 VLAN ID 지침

어떤 VLAN ID도 컨피그레이션에 추가할 수 있으나, 스위치에 의해 ASA에 지정된 VLAN만 트래픽을 전달할 수 있습니다. ASA에 지정된 모든 VLAN을 보려면 **show vlan** 명령을 사용합니다.

아직 스위치에 의해 ASA에 지정되지 않은 VLAN을 위해 인터페이스를 추가할 경우 그 인터페이스는 중지(down) 상태가 됩니다. VLAN을 ASA에 지정하면 인터페이스는 작동(up) 상태로 바뀝니다. 인터페이스 상태에 대한 자세한 내용은 **show interface** 명령을 참조하십시오.

투명 모드 인터페이스의 기본 설정

이 섹션에서는 공장 기본 컨피그레이션이 없을 경우의 인터페이스 기본 설정을 소개합니다. 공장 기본 컨피그레이션에 대한 자세한 내용은 2-15 페이지의 공장 기본 구성를 참조하십시오.

기본 보안 레벨

기본 보안 레벨은 0입니다. 인터페이스의 이름을 “inside”로 지정한 다음 보안 레벨을 명시적으로 설정하지 않으면 ASA는 보안 레벨을 100으로 설정합니다.

참고 인터페이스의 보안 레벨을 변경한 경우, 기존 연결이 시간 초과될 때까지 기다리지 않고 새 보안 정보를 사용하려면 **clear local-host** 명령을 사용하여 연결을 해제합니다.

ASASM의 인터페이스 기본 상태

- 단일 모드 또는 시스템 시행 영역에서는 VLAN 인터페이스가 기본적으로 활성화되어 있습니다.
- 다중 상황 모드에서는 인터페이스가 시스템 실행 영역에서 어떤 상태이든 상관없이 모든 할당된 인터페이스가 기본적으로 활성화되어 있습니다. 그러나 트래픽이 인터페이스를 통과하려면 인터페이스가 시스템 실행 영역에서도 활성화되어야 합니다. 시스템 실행 영역에서 인터페이스를 종료한 경우 이 인터페이스는 이를 공유하는 모든 상황에서 중지됩니다.

점보 프레임 지원

기본적으로 ASASM는 점보 프레임을 지원합니다. 13-13 페이지의 MAC 주소, MTU, TCP MSS 구성에 따라 원하는 패킷 크기의 MTU를 구성합니다.

투명 모드에서 인터페이스 구성 완료

인터페이스 구성 완료의 작업 흐름

1단계 모델에 따라 인터페이스를 설정합니다.

- ASA 5512-X 이상—10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.
- ASASM—2장, “Switch Configuration for the Cisco ASA Services Module.”
- ASAv—11 장, “기본 인터페이스 구성(ASAv)”.

2단계 (다중 상황 모드) 7-15 페이지의 다중 컨텍스트 모드 구성에 따라 상황에 인터페이스를 배정합니다.

3단계 (다중 상황 모드) Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 상황 이름을 두 번 클릭합니다.

4단계 IPv4 주소를 포함하여 하나 이상의 브리지 그룹을 구성합니다. 13-6 페이지의 브리지 그룹 구성를 참조하십시오.

5단계 인터페이스가 속한 브리지 그룹, 인터페이스 이름, 보안 레벨 등 일반 인터페이스 파라미터를 구성합니다. 13-8 페이지의 일반 인터페이스 파라미터 구성를 참조하십시오.

6단계 (선택 사항) 관리 인터페이스를 구성합니다. 13-10 페이지의 관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)를 참조하십시오.

7단계 (선택 사항) MAC 주소 및 MTU를 구성합니다. 13-13 페이지의 MAC 주소, MTU, TCP MSS 구성를 참조하십시오.

8단계 (선택 사항) IPv6 주소 지정을 구성합니다. 13-15 페이지의 IPv6 주소 지정 구성를 참조하십시오.

9단계 (선택 사항) 두 인터페이스 간 통신을 허용하거나 트래픽이 동일한 인터페이스에 들어오고 나가는 것을 허용하는 방법 중 하나로 동일한 보안 레벨 통신을 허용합니다. 13-19 페이지의 동일한 보안 레벨 통신 허용를 참조하십시오.

브리지 그룹 구성

각 브리지 그룹에는 관리 IP 주소가 필요합니다. ASA에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 이 IP 주소를 사용합니다. 관리 IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. IPv4 트래픽의 경우 트래픽을 전달하려면 관리 IP 인터페이스가 필요합니다. IPv6 트래픽에서는 적어도 트래픽을 전달하기 위해서는 링크-로컬 주소를 구성해야 합니다. 그러나 원격 관리, 기타 관리 작업을 포함한 전체 기능에 하나의 전역 관리 주소를 사용하는 것이 좋습니다.

지침 및 제한 사항

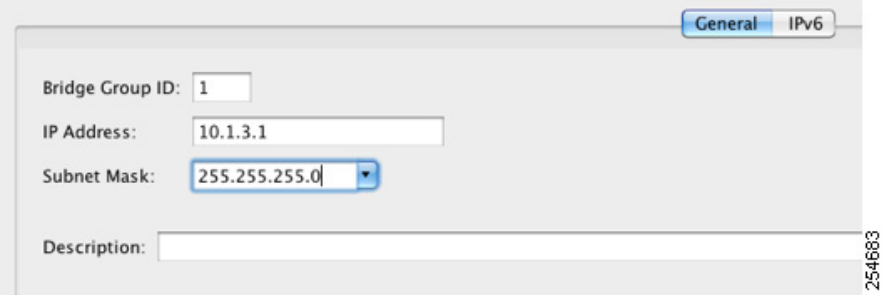
단일 모드에서 또는 다중 모드는 상황마다 최대 250개의 브리지 그룹을 구성할 수 있습니다. 하나 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.

참고 별도의 관리 인터페이스(지원되는 모델)에서는 컨피그레이션 불가한 브리지 그룹(ID 301)이 자동으로 컨피그레이션에 추가됩니다. 이 브리지 그룹은 브리지 그룹 한도의 대상이 아닙니다.

세부 단계

1단계 **Configuration > Interfaces** 창을 선택하고 **Add > Bridge Group Interface**를 선택합니다.

Add Bridge Group 대화 상자가 나타납니다.



2단계 Bridge Group ID 필드에 브리지 그룹 ID를 1~250 범위에서 입력합니다.

3단계 IP Address 필드에 관리 IPv4 주소를 입력합니다.

ASA는 보조 네트워크의 트래픽을 지원하지 않습니다. 관리 IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.

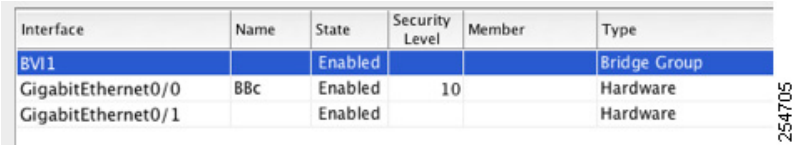
4단계 Subnet Mask 필드에 서브넷 마스크를 입력하거나 메뉴에서 하나를 선택합니다.

투명 방화벽에 호스트 주소(/32 또는 255.255.255.255)를 지정하지 마십시오. 또한 /30 서브넷(255.255.255.252)과 같이 3개 미만의 호스트 주소(업스트림 라우터, 다운스트림 라우터, 투명 방화벽 각각 하나씩)를 포함한 다른 서브넷은 사용하지 마십시오. ASA에서는 서브넷의 첫 주소 및 마지막 주소에 또는 이 주소로부터 모든 ARP 패킷을 폐기합니다. 만약 /30 서브넷을 사용하고 그 서브넷에서 업스트림 라우터에 예약된 주소를 지정할 경우 ASA는 다운스트림 라우터에서 업스트림 라우터로 ARP 요청을 폐기합니다.

5단계 (선택 사항) Description 필드에 이 브리지 그룹에 대한 설명을 입력합니다.

6단계 **OK**를 클릭합니다.

7단계 BVI(브리지 그룹 가상 인터페이스)가 물리적 인터페이스 및 하위 인터페이스와 함께 인터페이스 테이블에 추가됩니다.



다음에 할 일

일반 인터페이스 파라미터를 구성합니다. 13-8 페이지의 일반 인터페이스 파라미터 구성를 참조하십시오.

일반 인터페이스 파라미터 구성

이 절차에서는 각 투명 인터페이스의 이름, 보안 레벨, 브리지 그룹을 설정하는 방법에 대해 설명합니다.

별도의 관리 인터페이스를 구성하려면 13-10 페이지의 관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)를 참조하십시오.

ASA 5512-X 이상과 ASAv의 경우 다음 인터페이스 유형에 대한 인터페이스 파라미터를 구성해야 합니다.

- 물리적 인터페이스
- VLAN 하위 인터페이스
- 이중 인터페이스
- EtherChannel 인터페이스

ASASM에서는 다음 인터페이스 유형에 대해 인터페이스 파라미터를 구성해야 합니다.

- VLAN 인터페이스

지침 및 제한 사항

- 브리지 그룹당 최대 4개의 인터페이스를 구성할 수 있습니다.
- 보안 레벨에 대한 자세한 내용은 13-2 페이지의 보안 레벨를 참조하십시오.
- 장애 조치를 사용하는 경우 장애 조치 및 상태 기반 시스템 대체 작동 통신 전용 인터페이스의 이름을 지정하는 데 이 절차를 사용하지 마십시오. 장애 조치 및 상태 링크 구성에 대해서는 8장, “고가용성을 위한 장애 조치”,를 참조하십시오.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.
  - ASASM—2장, “Switch Configuration for the Cisco ASA Services Module.”
  - ASAv—11 장, “기본 인터페이스 구성(ASAv)”.
- 다중 상황 모드에서는 시스템 컨피그레이션에서 7-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 상황에 지정한 상황 인터페이스만 컨피그레이션할 수 있습니다.
- 다중 상황 모드에서는 상황 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 컨피그레이션으로 변경하려면Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 상황 이름을 두 번 클릭합니다.

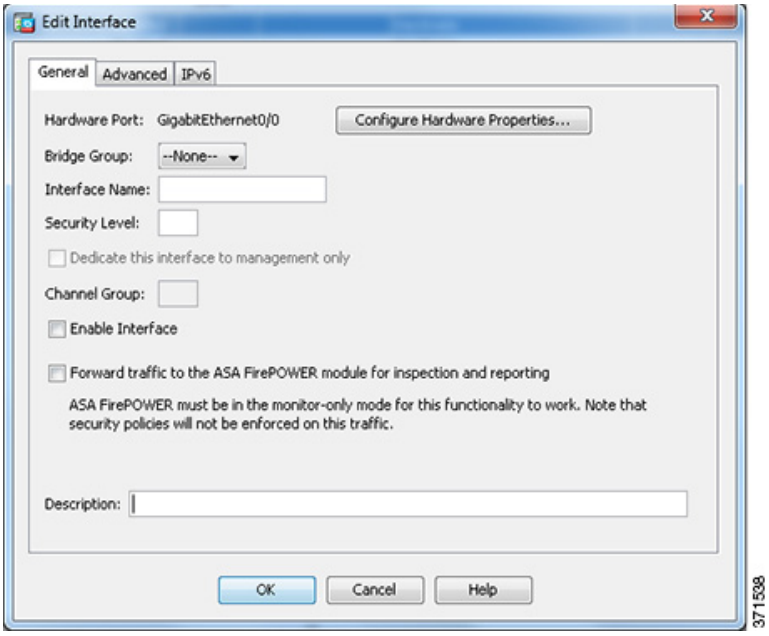
세부 단계

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

BVI가 물리적 인터페이스, 하위 인터페이스, 이중 인터페이스, EtherChannel 포트-채널 인터페이스와 함께 테이블에 표시됩니다. 다중 상황 모드에서는 시스템 실행 영역에서 상황에 지정된 인터페이스만 테이블에 표시됩니다.

2단계 비 BVI 인터페이스의 행을 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.



관리 인터페이스에는 이 절차를 사용하지 마십시오. 관리 인터페이스 구성에 대해서는 13-10 페이지의 관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)를 참조하십시오.

3단계 Bridge Group 드롭다운 메뉴에서 이 인터페이스를 지정하려는 브리지 그룹을 선택합니다.

4단계 Interface Name 필드에 이름을 48자 이내로 입력합니다.

5단계 Security level 필드에 0(가장 낮음)~100(가장 높음) 범위의 레벨을 입력합니다.

자세한 내용은 13-2 페이지의 보안 레벨를 참조하십시오.

참고 **Dedicate this interface to management only** 확인란을 클릭하지 마십시오. 이 옵션에 대해서는 13-10 페이지의 관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)를 참조하십시오.

6단계 인터페이스가 아직 활성화되지 않은 경우 **Enable Interface** 확인란을 선택합니다.

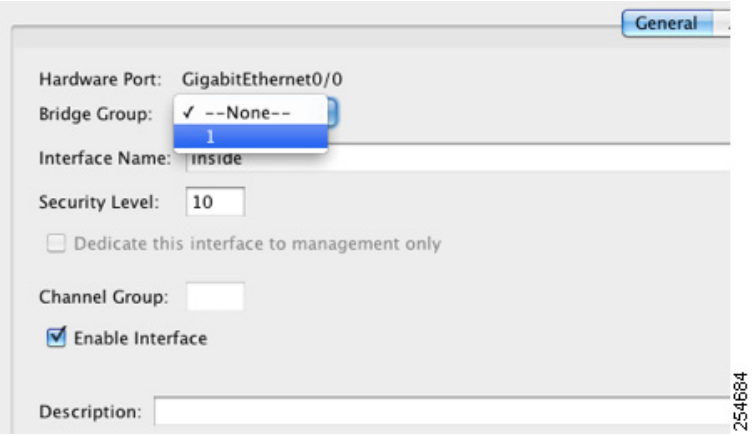
참고 Channel Group 필드는 읽기 전용이며, 인터페이스가 EtherChannel의 일부인지를 나타냅니다.

7단계 (선택 사항) ASA CX 또는 ASA FirePOWER 모듈을 설치한 경우, 비 프로덕션 ASA에서 모듈 기능을 시연하려면 **Forward traffic to the ASA module for inspection and reporting** 확인란을 선택합니다. 자세한 내용은 방화벽 컨피그레이션 가이드의 모듈 장을 참조하십시오.

8단계 (선택 사항) Description 필드에 이 인터페이스에 대한 설명을 입력합니다.

설명은 줄 바꿈 없이 1줄, 최대 240자로 작성합니다. 장애 조치 또는 상태 링크의 경우 이 설명은 “LAN Failover Interface”, “STATE Failover Interface” 또는“LAN/STATE Failover Interface”와 같이 고정되어 있습니다. 이 설명을 수정할 수 없습니다. 이 인터페이스를 장애 조치 또는 상태 링크로 만들 경우 고정된 설명이 사용자가 여기에 입력한 설명을 덮어씁니다.

참고 (ASA 5512-X 이상, 단일 모드) Configure Hardware Properties 버튼에 대한 자세한 내용은 10-14 페이지의 물리적 인터페이스 활성화 및 이더넷 매개변수 구성를 참조하십시오.



9단계 **OK**를 클릭합니다.

다음에 할 일

- (선택 사항) 관리 인터페이스를 구성합니다. 13-10 페이지의 관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)를 참조하십시오.
- (선택 사항) MAC 주소 및 MTU를 구성합니다. 13-13 페이지의 MAC 주소, MTU, TCP MSS 구성를 참조하십시오.
- (선택 사항) IPv6 주소 지정을 구성합니다. 13-15 페이지의 IPv6 주소 지정 구성를 참조하십시오.

관리 인터페이스 구성(ASA 5512-X 이상 및 ASAv)

단일 모드에서 또는 상황별로 브리지 그룹 인터페이스와는 별개인 관리 인터페이스를 구성할 수 있습니다. 자세한 내용은 10-2 페이지의 관리 인터페이스를 참조하십시오.

제한 사항

- 10-2 페이지의 관리 인터페이스를 참조하십시오.
- 이 인터페이스는 브리지 그룹에 지정하지 마십시오. 컨피그레이션 불가한 브리지 그룹(ID 101)이 자동으로 컨피그레이션에 추가됩니다. 이 브리지 그룹은 브리지 그룹 한도의 대상이 아닙니다.
- 사용하는 모델에 관리 인터페이스가 없을 경우 데이터 인터페이스에서 투명 방화벽 모드를 관리해야 합니다. 이 절차를 건너뛰십시오(예: ASASM에서).
- 다중 상황 모드에서는 관리 인터페이스를 비롯하여 어떤 인터페이스도 여러 상황에서 공유할 수 없습니다. 상황별 관리를 위해 관리 인터페이스의 하위 인터페이스를 만들고 각 상황에 관리 하위 인터페이스를 할당할 수 있습니다. ASA 5512-X부터 ASA 5555-X까지는 관리 인터페이스에서 하위 인터페이스를 지원하지 않습니다. 따라서 상황별 관리를 위해서는 데이터 인터페이스에 연결해야 합니다.

전제 조건

- 10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.의 절차를 완료합니다.
- 다중 상황 모드에서는 시스템 컨피그레이션에서 7-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 상황에 지정한 상황 인터페이스만 컨피그레이션할 수 있습니다.
- 다중 상황 모드에서는 상황 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 컨피그레이션으로 변경하려면Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 상황 이름을 두 번 클릭합니다.

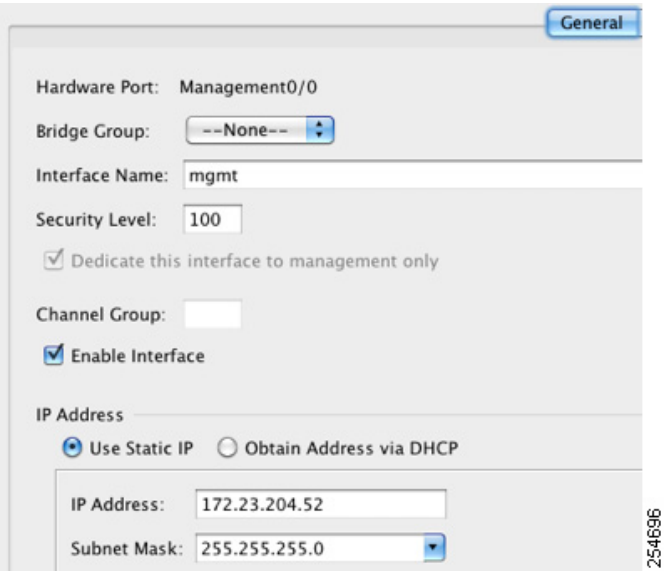
세부 단계

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

BVI가 물리적 인터페이스, 하위 인터페이스, 이중 인터페이스, EtherChannel 포트-채널 인터페이스와 함께 테이블에 표시됩니다. 다중 상황 모드에서는 시스템 실행 영역에서 상황에 지정된 인터페이스만 테이블에 표시됩니다.

2단계 관리 인터페이스, 하위 인터페이스 또는 관리 인터페이스로 구성된 EtherChannel 포츠-채널 인터페이스의 행을 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.



3단계 Bridge Group 드롭다운 메뉴에서 기본값인 **--None--**을 유지합니다. 브리지 그룹에 관리 인터페이스를 지정할 수 없습니다.

4단계 Interface Name 필드에 최대 48자의 이름을 입력합니다.

5단계 Security level 필드에 0(가장 낮음)~100(가장 높음) 범위의 레벨을 입력합니다.

자세한 내용은 13-2 페이지의 보안 레벨를 참조하십시오.

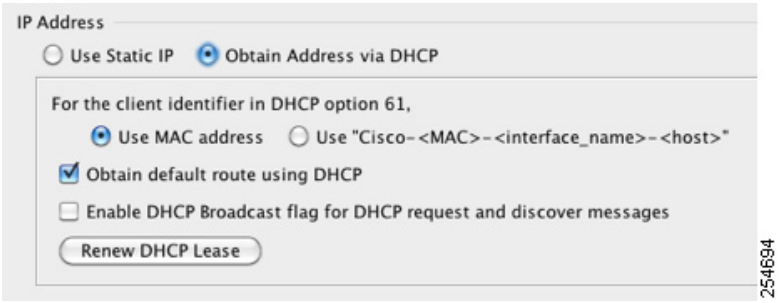
참고 **Dedicate this interface to management only** 확인란은 기본적으로 활성화되어 있으며 구성 불가합니다.

6단계 인터페이스가 아직 활성화되지 않은 경우 **Enable Interface** 확인란을 선택합니다.

7단계 IP 주소를 설정하려면 다음 옵션 중 하나를 사용합니다.

참고 장애 조치에서 사용할 경우 IP 주소와 대기 주소를 직접 설정해야 합니다. DHCP가 지원되지 않습니다. Configuration > Device Management > High Availability > Failover > Interfaces 탭에서 대기 IP 주소를 설정합니다.

- 직접 IP 주소를 설정하려면 **Use Static IP** 라디오 버튼을 클릭하고 IP 주소와 마스크를 입력합니다.
- DHCP 서버에서 IP 주소를 얻으려면 **Obtain Address via DHCP** 라디오 버튼을 클릭합니다.



a. 옵션 61에 대한 DHCP 요청 패킷 안에 반드시 MAC 주소가 저장되게 하려면 **Use MAC Address** 라디오 버튼을 클릭합니다.

   일부 ISP의 경우 옵션 61이 인터페이스 MAC 주소가 됩니다. MAC 주소가 DHCP 요청 패킷에 포함되지 않은 경우 IP 주소는 지정되지 않습니다.

b. 옵션 61에 대해 일반 문자열을 사용하려면 **Use "Cisco-<MAC>-<interface_name>-<host>"**를 클릭합니다.

c. (선택 사항) DHCP 서버에서 기본 경로를 얻으려면 **Obtain Default Route Using DHCP**를 선택합니다.

d. (선택 사항) DHCP 클라이언트에서 IP 주소를 요청하는 discover를 보낼 때 DHCP 패킷 헤더에서 브로드캐스트 플래그를 1로 설정하려면 **Enable DHCP Broadcast flag for DHCP request and discover messages**를 선택합니다.

   DHCP 서버가 이 브로드캐스트 플래그를 수신하고, 플래그가 1로 설정되었으면 회신 패킷을 브로드캐스트합니다.

e. (선택 사항) 임대를 갱신하려면 **Renew DHCP Lease**를 클릭합니다.

8단계 (선택 사항) Description 필드에 이 인터페이스에 대한 설명을 입력합니다.

설명은 줄 바꿈 없이 1줄, 최대 240자로 작성합니다.

참고 (ASA 5512-X 이상, 단일 모드) Configure Hardware Properties 버튼에 대한 자세한 내용은 10-14 페이지의 물리적 인터페이스 활성화 및 이더넷 매개변수 구성를 참조하십시오.

9단계 **OK**를 클릭합니다.

다음에 할 일

- (선택 사항) MAC 주소 및 MTU를 구성합니다. 13-13 페이지의 MAC 주소, MTU, TCP MSS 구성를 참조하십시오.
- (선택 사항) IPv6 주소 지정을 구성합니다. 13-15 페이지의 IPv6 주소 지정 구성를 참조하십시오.

MAC 주소, MTU, TCP MSS 구성

이 섹션에서는 인터페이스의 MAC 주소를 구성하는 방법 및 MTU와 TCP MSS를 설정하는 방법을 설명합니다.

MAC 주소에 대한 정보

기본적으로 물리적 인터페이스는 번인된(burned-in) MAC 주소를 사용하며, 물리적 인터페이스의 모든 하위 인터페이스도 동일한 번인된 MAC 주소를 사용합니다.

ASASM에서는 모든 VLAN이 백플레인에서 제공한 동일한 MAC 주소를 사용합니다.

이중 인터페이스는 사용자가 추가한 첫 번째 물리적 인터페이스의 MAC 주소를 사용합니다. 컨피그레이션에서 멤버 인터페이스의 순서를 변경하면 MAC 주소는 이제 첫 번째로 나열되는 인터페이스의 MAC 주소와 일치하도록 바뀝니다. 이 명령을 사용하여 이중 인터페이스에 MAC 주소를 지정하면 멤버 인터페이스 MAC 주소와 상관없이 이 주소가 사용됩니다.

EtherChannel의 경우 채널 그룹에 속한 모든 인터페이스가 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다. 포트-채널 인터페이스는 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 직접 구성할 수도 있습니다. 다중 상황 모드에서는 EtherChannel 포트 인터페이스를 비롯한 인터페이스에 고유한 MAC 주소를 자동으로 지정할 수 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우에 대비하여 직접 또는 다중 상황 모드라면 자동으로 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널 MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그 다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.

다중 상황 모드에서는 여러 상황가 하나의 인터페이스를 공유할 경우 각 상황에서 인터페이스에 고유한 MAC 주소를 지정할 수 있습니다. 이 기능 덕분에 ASA에서 손쉽게 알맞은 상황으로 패킷을 분류할 수 있습니다. 고유한 MAC 주소 없이 공유 인터페이스를 사용할 수 있으나, 몇 가지 제한이 있습니다. 자세한 내용은 7-3 페이지의 ASA의 패킷 분류를 참조하십시오. 각 MAC 주소를 직접 지정하거나 상황에서 공유 인터페이스의 MAC 주소를 자동으로 생성할 수 있습니다. MAC 주소를 자동으로 생성하려면 7-23 페이지의 컨텍스트 인터페이스에 MAC 주소 자동 지정를 참조하십시오. MAC 주소를 자동으로 생성한 경우 생성된 주소를 재정의하는 데 이 절차를 사용할 수 있습니다.

단일 상황 모드에서는 또는 다중 상황 모드에서 공유되지 않는 인터페이스에 대해서는 하위 인터페이스에 고유 MAC 주소를 지정해야 하는 경우가 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다.

MTU 및 TCP MSS에 대한 정보

10-7 페이지의 MTU 및 TCP 최대 세그먼트 크기로 조각화 제어를 참조하십시오.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.
  - ASASM—2장, “Switch Configuration for the Cisco ASA Services Module.”
  - ASAv—11 장, “기본 인터페이스 구성(ASAv)”.
- 다중 상황 모드에서는 시스템 컨피그레이션에서 7-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 상황에 지정한 상황 인터페이스만 컨피그레이션할 수 있습니다.
- 다중 상황 모드에서는 상황 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 컨피그레이션으로 변경하려면Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 상황 이름을 두 번 클릭합니다.

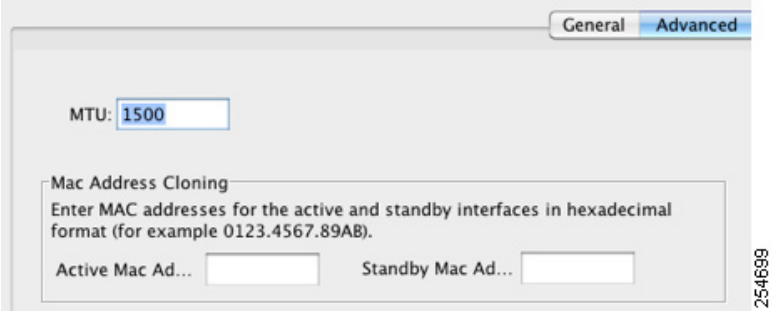
세부 단계

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 인터페이스 행을 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.

3단계 **Advanced** 탭을 클릭합니다.



4단계 MTU를 설정하거나 점보 프레임 지원을 활성화하려면(지원되는 모델만 해당) MTU 필드에 300바이트 ~ 9198바이트(ASAv는 9000바이트) 범위의 값을 입력합니다.

기본값은 1500바이트입니다.

참고 이중 또는 포트 채널 인터페이스를 위해 MTU를 설정하면 ASA는 모든 멤버 인터페이스에 이 설정을 적용합니다.

- 단일 모드에서 점보 프레임을 지원하는 모델에서 임의의 인터페이스에 대해 1500보다 큰 값을 입력한 경우 모든 인터페이스에서 점보 프레임 지원이 자동으로 활성화됩니다. 모든 인터페이스의 MTU를 1500보다 작은 값으로 다시 설정하면 점보 프레임 지원이 비활성화됩니다.
- 다중 모드에서 점보 프레임을 지원하는 모델에서 임의의 인터페이스에 대해 1500보다 큰 값을 입력한 경우 시스템 컨피그레이션에서 점보 프레임 지원을 활성화해야 합니다. 10-28 페이지의 점보 프레임 지원 활성화를 참조하십시오.

참고 점보 프레임 지원을 활성화하거나 비활성화하려면 ASA를 다시 로드해야 합니다.

5단계 이 인터페이스에 MAC 주소를 직접 지정하려면 Active Mac Address 필드에 H.H.H 형식으로 MAC 주소를 입력합니다. 여기서 H는 16비트 16진수입니다.

예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. 자동 생성된 MAC 주소도 사용하려는 경우 수동 MAC 주소의 처음 2바이트는 A2가 될 수 없습니다.

6단계 장애 조치를 사용하는 경우 Standby Mac Address 필드에 대기 MAC 주소를 입력합니다. 활성 유닛이 장애 조치되고 대기 유닛이 활성 상태가 되면, 네트워크 중단을 최소화하기 위해 새 활성 유닛에서 활성 MAC 주소를 사용하기 시작하고 기존 활성 유닛은 대기 주소를 사용합니다.

7단계 TCP MSS를 설정하려면 **Configuration > Firewall > Advanced > TCP Options**를 선택합니다. 다음 옵션을 설정합니다.

- Force Maximum Segment Size for TCP—최대 TCP 세그먼트 크기(바이트)를 48~임의의 최대값 범위에서 설정합니다. 기본값은 1380바이트입니다. bytes를 0으로 설정하여 이 기능을 비활성화할 수 있습니다.
- Force Minimum Segment Size for TCP—최대 세그먼트 크기를 48~임의의 최대값 범위에서 사용자가 설정한 bytes보다 작지 않은 값으로 재정의합니다. 이 기능은 기본적으로 비활성화되어 있습니다(0으로 설정됨).

8단계 **Secure Group Tagging**에 대해서는 33-22 페이지의 SGT plus Ethernet Tagging 활성화를 참조하십시오.

다음에 할 일

(선택 사항) IPv6 주소 지정을 구성합니다. 13-15 페이지의 IPv6 주소 지정 구성를 참조하십시오.

IPv6 주소 지정 구성

이 섹션에서는 IPv6 주소 지정의 구성 방법을 설명합니다.

IPv6에 대한 정보

이 섹션에서는 IPv6를 구성하는 방법을 다룹니다.

IPv6 주소 지정

IPv6를 위해 2가지 유형의 유니캐스트 주소를 구성할 수 있습니다.

- Global—전역 주소는 공용 네트워크에서 사용할 수 있는 공용 주소입니다. 이 주소는 인터페이스별로 구성하는 게 아니라 브리지 그룹마다 구성해야 합니다. 관리 인터페이스를 위해 전역 IPv6 주소를 구성할 수도 있습니다.

- Link-local—링크-로컬 주소는 직접 연결된 네트워크에서만 사용할 수 있는 사설 주소입니다. 라우터에서 링크-로컬 주소를 사용하여 패킷을 전달하지 않습니다. 이는 특정 물리적 네트워크 세그먼트에서의 통신에만 사용됩니다. 주소 컨피그레이션에 또는 주소 확인, Neighbor Discovery와 같은 ND 기능에 사용할 수 있습니다. 링크-로컬 주소는 세그먼트에서만 사용 가능하고 인터페이스 MAC 주소에 연결되어 있으므로 인터페이스별로 링크-로컬 주소를 구성해야 합니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 구성한 경우 각 인터페이스에서 링크-로컬 주소가 자동으로 구성됩니다. 따라서 구체적으로 링크-로컬 주소를 구성할 필요 없습니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

Modified EUI-64 인터페이스 ID

RFC 3513: IPv6(Internet Protocol Version 6) Addressing Architecture에 따르면, 모든 유니캐스트 IPv6 주소(이진 값 000으로 시작하는 것 제외)의 인터페이스 식별자 부분은 길이가 64비트이고 Modified EUI-64 형식이어야 합니다. ASA는 로컬 링크에 연결된 호스트에 이 요구 사항을 적용할 수 있습니다.

이 기능이 인터페이스에서 활성화된 경우, 그 인터페이스에서 수신한 IPv6 패킷의 소스 주소를 소스 MAC 주소와 비교하여 검증함으로써 인터페이스 식별자가 Modified EUI-64 형식을 사용하는지 확인합니다. IPv6 패킷에서 인터페이스 식별자에 Modified EUI-64 형식을 사용하지 않을 경우 패킷은 폐기되고 다음 시스템 로그 메시지가 생성됩니다.

```
%ASA-3-325003: EUI-64 source address check failed.
```

주소 형식 검증은 흐름이 생성되는 경우에만 수행됩니다. 기존 흐름의 패킷은 검사하지 않습니다. 또한 이 주소 검증은 로컬 링크의 호스트에 대해서만 수행할 수 있습니다. 라우터 뒤에 있는 호스트로부터 받은 패킷은 주소 형식 검증을 통과하지 못해 폐기됩니다. 그 소스 MAC 주소가 호스트 MAC 주소가 아닌 라우터 MAC 주소이기 때문입니다.

지원되지 않는 명령

다음 IPv6 명령은 라우터 기능을 필요로 하므로 투명 방화벽 모드에서 지원되지 않습니다.

- **ipv6 address autoconfig**
- **ipv6 nd prefix**
- **ipv6 nd ra-interval**
- **ipv6 nd ra-lifetime**
- **ipv6 nd suppress-ra**

전역 IPv6 주소 구성

브리지 그룹 또는 관리 인터페이스에 대해 전역 IPv6 주소를 구성하려면 다음 단계를 수행합니다.

참고 전역 주소를 자동으로 구성하면 링크-로컬 주소가 구성됩니다. 즉 따로 구성할 필요 없습니다.

제한 사항

ASA는 IPv6 애니캐스트 주소를 지원하지 않습니다.

전제 조건

- 모델에 따라 인터페이스를 설정합니다.
  - ASA 5512-X 이상—10 장, “기본 인터페이스 구성(ASA 5512-X 이상)”.
  - ASASM—2장, “Switch Configuration for the Cisco ASA Services Module.”
  - ASAv—11 장, “기본 인터페이스 구성(ASAv)”.
- 다중 상황 모드에서는 시스템 컨피그레이션에서 7-15 페이지의 다중 컨텍스트 모드 구성에 따라 이미 상황에 지정한 상황 인터페이스만 컨피그레이션할 수 있습니다.
- 다중 상황 모드에서는 상황 실행 영역에서 이 절차를 완료합니다. 시스템에서 상황 컨피그레이션으로 변경하려면Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 상황 이름을 두 번 클릭합니다.

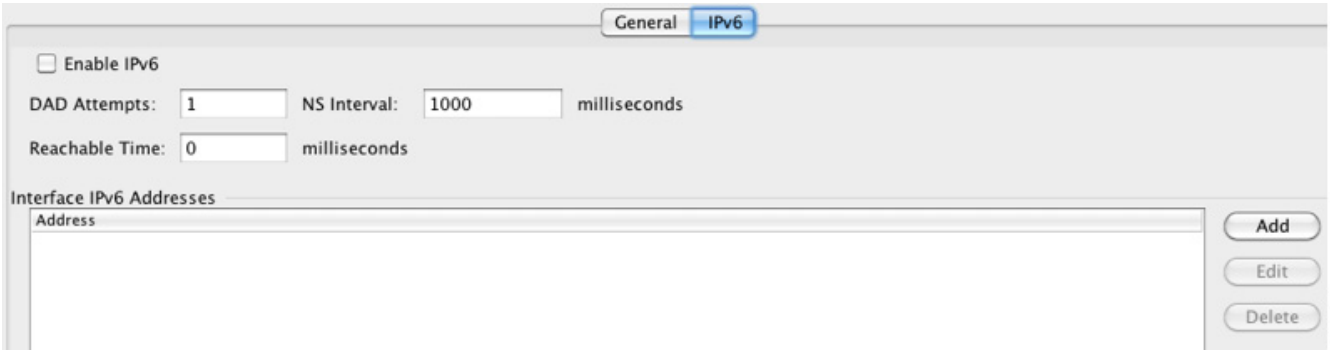
세부 단계

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 BVI 또는 관리 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.

3단계 **IPv6** 탭을 클릭합니다.



4단계 **Enable IPv6** 확인란을 선택합니다.

5단계 (선택 사항) 로컬 링크의 IPv6 주소에서 반드시 Modified EUI-64 형식 인터페이스 식별자를 사용하게 하려면 **Enforce EUI-64** 확인란을 선택합니다.

자세한 내용은 13-16 페이지의 Modified EUI-64 인터페이스 ID를 참조하십시오.

6단계 (선택 사항) 맨 위 영역에서 26 장, “IPv6 인접 디바이스 검색”.를 참조하여 IPv6 컨피그레이션을 사용자 지정합니다.

7단계 전역 IPv6 주소를 구성하려면

a. Interface IPv6 Addresses 영역에서 **Add**를 클릭합니다.

Add IPv6 Address for Interface 대화 상자가 나타납니다.

b. Address/Prefix Length 필드에 전역 IPv6 주소 및 IPv6 프리픽스 길이를 입력합니다. 예를 들면 2001:0DB8::BA98:0:3210/48입니다. IPv6 주소 지정에 대한 자세한 내용은 43-5 페이지의 IPv6 주소를 참조하십시오.

c. **OK**를 클릭합니다.

8단계 **OK**를 클릭합니다.

Configuration > Device Setup > Interfaces 창으로 돌아갑니다.

IPv6 Neighbor Discovery 구성

IPv6 Neighbor Discovery를 구성하려면 26 장, “IPv6 인접 디바이스 검색”,를 참조하십시오.

(선택 사항) 링크-로컬 주소 자동 구성

전역 주소를 구성하지 않고 링크-로컬 주소만 구성하려는 경우 인터페이스 MAC 주소(Modified EUI-64 형식. MAC 주소는 48비트를 사용하므로 인터페이스 ID에 필요한 64비트를 채우기 위해 추가 비트를 삽입해야 함)를 기반으로 링크-로컬 주소를 만드는 옵션이 있습니다.

링크-로컬 주소를 직접 지정하려면(권장하지 않음) 13-19 페이지의 (선택 사항) 링크-로컬 주소 수동 구성를 참조하십시오.

Modified EUI-64 형식 강제 적용, DAD 설정 등 다른 IPv6 옵션에 대해서는 13-16 페이지의 전역 IPv6 주소 구성를 참조하십시오.

관리 인터페이스 또는 브리지 그룹 멤버 인터페이스를 위해 링크-로컬 주소를 자동으로 구성하려면 다음 단계를 수행합니다.

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 BVI 또는 관리 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.

3단계 **IPv6** 탭을 클릭합니다.

4단계 IPv6 컨피그레이션 영역에서 **Enable IPv6**를 선택합니다.

이 옵션은 IPv6를 활성화하며, 인터페이스 MAC 주소 기반의 Modified EUI-64 인터페이스 ID를 사용하여 멤버 인터페이스의 링크-로컬 주소를 자동으로 생성합니다.

5단계 **OK**를 클릭합니다.

(선택 사항) 링크-로컬 주소 수동 구성

전역 주소를 구성하지 않고 물리적 인터페이스 또는 하위 인터페이스의 링크-로컬 주소만 구성하려는 경우 직접 링크-로컬 주소를 정의하는 옵션이 있습니다. Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

링크-로컬 주소를 자동으로 지정하려면(권장) 13-18 페이지의 (선택 사항) 링크-로컬 주소 자동 구성를 참조하십시오.

Modified EUI-64 형식 강제 적용, DAD 설정 등 다른 IPv6 옵션에 대해서는 13-16 페이지의 전역 IPv6 주소 구성를 참조하십시오.

관리 인터페이스를 비롯한 물리적 인터페이스 또는 하위 인터페이스에 링크-로컬 주소를 지정하려면 다음 단계를 수행합니다.

1단계 **Configuration > Device Setup > Interfaces** 창을 선택합니다.

2단계 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit 인터페이스 대화 상자가 나타나며, General 탭이 선택되어 있습니다.

3단계 **IPv6** 탭을 클릭합니다.

4단계 링크-로컬 주소를 설정하려면 Link-local address 필드에 주소를 입력합니다.

링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). IPv6 주소 지정에 대한 자세한 내용은 43-5 페이지의 IPv6 주소를 참조하십시오.

5단계 **OK**를 클릭합니다.

동일한 보안 레벨 통신 허용

기본적으로 동일한 보안 레벨의 인터페이스는 서로 통신할 수 없고 패킷이 동일한 인터페이스에 들어오고 나갈 수 없습니다. 이 섹션에서는 동일한 보안 레벨에 있는 인터페이스 간의 통신을 활성화하는 방법을 설명합니다.

인터페이스 간 통신에 대한 정보

동일한 보안 레벨의 인터페이스 간 통신을 허용하는 기능은 모든 동일한 보안 인터페이스 간에 ACL 없이 자유로운 트래픽 이동을 지원하려는 경우에 유용합니다.

동일한 보안 인터페이스 통신을 활성화하더라도 기존처럼 여러 보안 레벨에서 인터페이스를 구성할 수 있습니다.

세부 단계

동일한 보안 레벨의 인터페이스가 서로 통신할 수 있게 하려면 Configuration > Interfaces 창에서 **Enable traffic between two or more interfaces which are configured with same security level**을 클릭합니다.

인터페이스 끄기 및 켜기

이 섹션에서는 인터페이스를 끄고 켜는 방법을 설명합니다.

모은 인터페이스는 기본적으로 활성화되어 있습니다. 다중 상황 모드에서는 어떤 상황 내에서 인터페이스를 비활성화하거나 다시 활성화할 경우 그 상황 인터페이스에만 적용됩니다. 그러나 시스템 실행 영역에서 인터페이스를 비활성화하거나 다시 활성화하면 모든 상황의 해당 인터페이스에 적용됩니다.

세부 단계

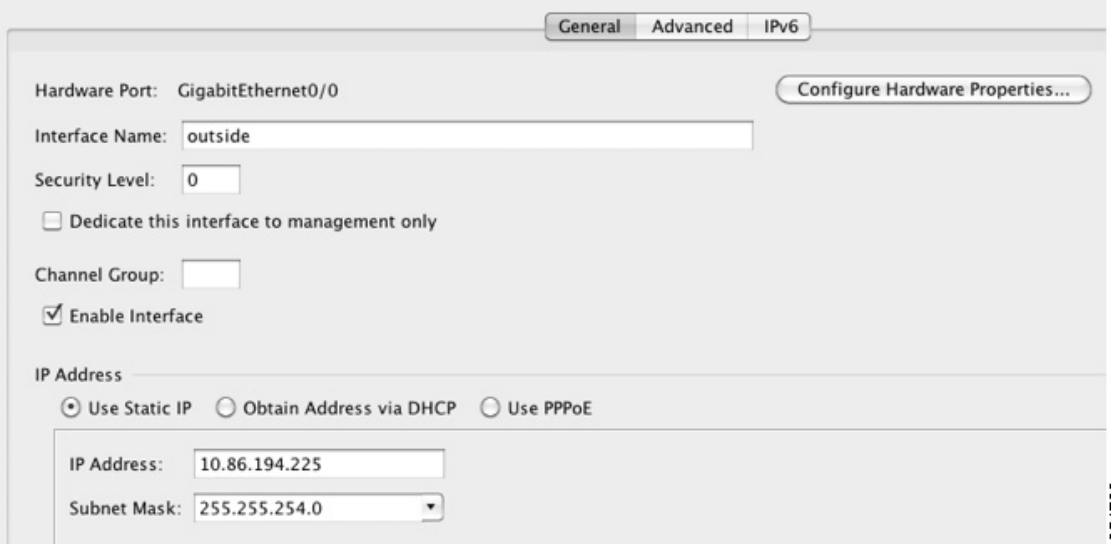
1단계 상황 모드에 따라

- 단일 모드에서는 **Configuration > Device Setup > Interfaces** 창을 선택합니다.
- 다중 모드의 경우 시스템 실행 영역에서 **Configuration > Context Management > Interfaces** 창을 선택합니다.

기본적으로 모든 물리적 인터페이스가 나열됩니다.

2단계 구성할 VLAN 인터페이스를 클릭하고 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 나타납니다.



3단계 인터페이스를 활성화하거나 비활성화하려면 **Enable Interface** 확인란을 선택하거나 선택 취소합니다.

인터페이스 모니터링

- 12-21 페이지의 ARP 테이블를 참조하십시오.
- 12-21 페이지의 DHCP를 참조하십시오.
- 12-24 페이지의 MAC 주소 테이블를 참조하십시오.
- 12-24 페이지의 동적 ACL를 참조하십시오.
- 12-24 페이지의 인터페이스 그래프를 참조하십시오.
- 12-27 페이지의 PPPoE 클라이언트를 참조하십시오.
- 12-27 페이지의 인터페이스 연결를 참조하십시오.

투명 모드 인터페이스의 기능 내역

표 13-1에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 13-1 투명 모드 인터페이스의 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
VLAN 증가	7.0(5)	다음 한도를 높였습니다. • ASA5510 Base License의 VLAN을 0개에서 10개로 • ASA5510 Security Plus License의 VLAN을 10개에서 25개로 • ASA5520 VLAN을 25개에서 100개로 • ASA5540 VLAN을 100개에서 200개로
VLAN 증가	7.2(2)	ASA 5505 Security Plus License의 VLAN 최대 개수를 5개(3개는 전 기능, 1개는 장애 조치, 1개는 백업 인터페이스에 한정)에서 20개 전 기능 인터페이스로 늘렸습니다. 또한 트렁크 포트 수도 1개에서 8개로 늘렸습니다. 이제 20개의 전 기능 인터페이스를 지원하므로, 백업 ISP 인터페이스를 무력화하기 위해 백업 인터페이스 명령을 사용할 필요 없습니다. 이 목적으로 전 기능 인터페이스를 사용할 수 있습니다. 백업 인터페이스 명령은 Easy 컨피그레이션에서 여전히 유용합니다. ASA 5510의 VLAN 한도도 늘어났습니다. Base License는 10개에서 50개로, Security Plus License는 25개에서 100개로 늘어났습니다. ASA 5520은 100개에서 150개로, ASA 5550은 200개에서 250개로 늘어났습니다.

표 13-1 투명 모드 인터페이스의 기능 내역 (계속)

기능 이름	플랫폼 릴리스	기능 정보
ASA 5510 Security Plus License의 기가비트 이더넷 지원	7.2(3)	ASA 5510 Security Plus License는 포트 0과 포트 1에서 GE(기가비트 이더넷)를 지원합니다. Base License를 Security Plus License로 업그레이드할 경우 외부 Ethernet0/0 및 Ethernet0/1 포트의 용량이 원래의 FE(패스트 이더넷)(100Mbps)에서 GE(1000Mbps)로 증가합니다. 인터페이스 이름은 그대로 Ethernet 0/0 및 Ethernet 0/1입니다.
ASA 5505의 VLAN 기본 지원	7.2(4)/8.0(4)	ASA 5505 트렁크 포트에 기본 VLAN을 포함할 수 있습니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Interfaces > Switch Ports > Edit Switch Port
ASA 5580의 점보 패킷 지원	8.1(1)	Cisco ASA 5580은 점보 프레임을 지원합니다. 점보 프레임은 표준 최대 크기인 1518바이트(레이어 2 헤더 및 FCS 포함)보다 큰 이더넷 패킷으로 최대 크기가 9216바이트입니다. 모든 인터페이스에서 이더넷 프레임 처리용 메모리 용량을 늘려 점보 프레임 지원을 활성화할 수 있습니다. 점보 프레임에 더 많은 메모리를 할당하면 ACL와 같은 다른 기능을 최대 한도로 사용하는 데 제약이 따를 수 있습니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Interfaces > Add/Edit Interface > Advanced
ASA 5580의 VLAN 증가	8.1(2)	ASA 5580에서 지원되는 VLAN 수가 100개에서 250개로 늘어났습니다.
투명 모드의 IPv6 지원	8.2(1)	투명 방화벽 모드를 위한 IPv6 지원을 도입했습니다.
ASA 5580 10기가비트 이더넷 인터페이스에서 흐름 제어를 위한 Pause 프레임 지원	8.2(2)	흐름 제어를 위해 Pause(XOFF) 프레임을 활성화할 수 있습니다. 다음 화면을 수정했습니다. (단일 모드) Configuration > Device Setup > Interfaces > Add/Edit Interface > General (다중 모드, 시스템) Configuration > Interfaces > Add/Edit Interface

표 13-1 투명 모드 인터페이스의 기능 내역 (계속)

기능 이름	플랫폼 릴리스	기능 정보
투명 모드의 브리지 그룹	8.4(1)	보안 상황의 오버헤드를 원치 않을 경우 또는 보안 상황 정보 사용을 극대화하려는 경우, 인터페이스를 하나의 브리지 그룹으로 묶은 다음 네트워크마다 하나씩, 여러 브리지 그룹을 구성할 수 있습니다. 브리지 그룹 트래픽은 다른 브리지 그룹과 분리됩니다. 단일 모드에서 또는 각 상황에서 각각 4개의 인터페이스를 포함하는 브리지 그룹을 8개까지 구성할 수 있습니다. 다음 화면을 수정하거나 도입했습니다. Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interfaces > Add/Edit Interface
투명 모드 브리지 그룹 최대 개수 250개로 증가	9.3(1)	브리지 그룹의 최대 개수가 8개에서 250개로 늘어났습니다. 단일 모드에서 또는 다중 모드의 각 상황에서 최대 250개의 브리지 그룹을 구성할 수 있으며, 각 브리지 그룹은 최대 4개의 인터페이스를 포함할 수 있습니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Interfaces Configuration > Device Setup > Interfaces > Add/Edit Bridge Group Interface Configuration > Device Setup > Interfaces > Add/Edit Interface

파 트 4

기본 설정

14 장

기본 설정

이 장에서는 일반적으로 컨피그레이션의 원활한 작동에 필요한 ASA의 기본 설정을 컨피그레이션하는 방법을 설명합니다.

호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정

호스트 이름, 도메인 이름, enable 및 텔넷 비밀번호를 설정하려면 다음 단계를 수행합니다.

시작하기 전에

- 다중 상황 모드에서는 시스템 및 상황 실행 영역 모두에서 호스트 이름과 도메인 이름을 구성할 수 있습니다.
- enable 비밀번호와 텔넷 비밀번호는 각 상황에 설정합니다. 시스템에서는 사용할 수 없습니다. 다중 상황 모드에서 스위치로부터 ASASM로 세션을 연결할 때 ASASM에서는 관리 상황에서 설정한 로그인 비밀번호를 사용합니다.
- 시스템에서 상황 컨피그레이션으로 바꾸려면 **Configuration > Device List** 창에서 활성 디바이스 IP 주소 아래의 상황 이름을 두 번 클릭합니다.

절차

1단계 **Configuration > Device Setup > Device Name/Password**를 선택합니다.

2단계 호스트 이름을 입력합니다. 기본 호스트 이름은 “ciscoasa”입니다.

호스트 이름이 명령줄 프롬프트에 나타나며, 여러 디바이스와의 세션을 설정한 경우 호스트 이름은 명령을 입력할 위치를 파악하는 데 도움이 됩니다. 호스트 이름은 syslog 메시지에도 사용됩니다.

다중 상황 모드에서는 시스템 실행 영역에서 설정한 호스트 이름이 모든 상황의 명령줄 프롬프트에 나타납니다. 상황 내에서 선택적으로 설정한 호스트 이름은 명령줄에 나타나지 않습니다. 이는 배너에 사용할 수 있습니다.

3단계 도메인 이름을 입력합니다. 기본 도메인 이름은 default.domain.invalid입니다.

ASA는 도메인 이름을 정규화되지 않은 이름에 접미사로 추가합니다. 예를 들어, 도메인 이름을 "example.com"으로 설정하고 "jupiter"라는 정규화되지 않은 이름으로 syslog 서버를 지정한 경우 ASA는 그 이름을 "jupiter.example.com"으로 정규화합니다.

4단계 특별 권한 모드 (enable) 비밀번호를 변경합니다. 기본 비밀번호는 비어 있습니다.

enable 인증을 구성하지 않은 경우 enable 비밀번호를 사용하여 특별 권한 EXEC 모드를 시작할 수 있습니다.

또한 enable 비밀번호는 HTTP 인증을 구성하지 않은 경우에 빈 사용자 이름으로 ASDM에 로그인할 수 있게 합니다.

a. **Change the privileged mode password** 확인란을 선택합니다.

b. 이전 비밀번호(기본 비밀번호는 비어 있음)와 새 비밀번호를 입력하고 새 비밀번호를 다시 입력합니다.

5단계 텔넷 액세스를 위한 로그인 비밀번호를 설정합니다. 기본 비밀번호가 없습니다.

로그인 비밀번호는 텔넷 인증을 구성하지 않은 경우 텔넷 액세스에 사용됩니다. **session** 명령을 사용하여 스위치에서 ASASM에 액세스할 때에도 이 비밀번호를 사용합니다.

a. **Change the password to access the console of the security appliance** 확인란을 선택합니다.

b. 이전 비밀번호(신규 ASA의 경우 이 필드를 비워 둠)와 새 비밀번호를 입력하고 확인을 위해 새 비밀번호를 다시 입력합니다.

6단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

Enable 비밀번호 및 텔넷 비밀번호 복구

enable 비밀번호나 텔넷 비밀번호를 잊은 경우 복구할 수 있습니다. 이 절차는 디바이스 유형에 따라 다릅니다. CLI를 사용하여 작업을 수행해야 합니다.

- 14-2 페이지의 ASA의 비밀번호 복구
- 14-4 페이지의 ASA 5506, 5506-W, ASA 5508의 비밀번호 복구
- 14-5 페이지의 ASAv의 비밀번호 또는 이미지 복구
- 14-6 페이지의 비밀번호 복구 비활성화

ASA의 비밀번호 복구

ASA의 비밀번호를 복구하려면 다음 단계를 수행합니다.

절차

1단계 ASA 콘솔 포트에 연결합니다.

2단계 ASA를 껐다가 다시 켭니다.

3단계 시작한 다음 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

4단계 컨피그레이션 레지스터 값을 업데이트하려면 다음 명령을 입력합니다.

```
rommon #1> confreg 0x41
Update Config Register (0x41) in NVRAM...
```

5단계 ASA에서 시작 컨피그레이션을 무시하도록 설정하려면 다음 명령을 입력합니다.

```
rommon #1> confreg
```

ASA는 현재 컨피그레이션 레지스터 값을 표시하고 이를 변경할지 묻습니다.

```
Current Configuration Register: 0x00000041
Configuration Summary:
  boot default image from Flash
  ignore system configuration

Do you wish to change this configuration? y/n [n]: y
```

6단계 나중에 복원할 수 있도록 현재 컨피그레이션 레지스터 값을 기록해 둡니다.

7단계 값을 변경하기 위해 프롬프트에서 **Y**를 입력합니다.

ASA 프롬프트에 새 값을 입력합니다.

8단계 "disable system configuration?" 값을 제외하고 모든 설정에 기본값을 적용합니다.

9단계 프롬프트에 **Y**를 입력합니다.

10단계 다음 명령을 입력하여 ASA를 다시 로드합니다.

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa800-226-k8.bin... Booting...Loading...
```

ASA는 시작 컨피그레이션 대신 기본 컨피그레이션을 로드합니다.

11단계 다음 명령을 입력하여 특별 권한 EXEC 모드에 액세스합니다.

```
ciscoasa# enable
```

12단계 비밀번호를 물으면 **Enter**를 누릅니다.

비밀번호는 비어 있습니다.

13단계 다음 명령을 입력하여 시작 컨피그레이션을 로드합니다.

```
ciscoasa# copy startup-config running-config
```

14단계 다음 명령을 입력하여 전역 컨피그레이션 모드에 액세스합니다.

```
ciscoasa# configure terminal
```

15단계 필요하다면 다음 명령을 입력하여 기본 컨피그레이션에서 비밀번호를 변경합니다.

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

16단계 다음 명령을 입력하여 기본 컨피그레이션을 로드합니다.

```
ciscoasa(config)# no config-register
```

기본 컨피그레이션 레지스터 값은 0x1입니다. 컨피그레이션 레지스터에 대한 자세한 내용은 명령 참조를 참조하십시오.

17단계 다음 명령을 입력하여 새 비밀번호를 시작 컨피그레이션에 저장합니다.

```
ciscoasa(config)# copy running-config startup-config
```

ASA 5506, 5506-W, ASA 5508의 비밀번호 복구

ASA 5506, 5506-W, 5508의 비밀번호를 복구하려면 다음 단계를 수행합니다.

절차

1단계 ASA 콘솔 포트에 연결합니다.

2단계 ASA를 껐다가 다시 켭니다.

3단계 시작한 다음 ROMMON 모드를 시작할지 물으면 **Escape** 키를 누릅니다.

4단계 컨피그레이션 레지스터 값을 업데이트하려면 다음 명령을 입력합니다.

```
rommon #1> confreg 0x41

새 구성이 적용되려면 초기화하거나 전원을 껐다가 켜야 합니다.
```

ASA는 현재 컨피그레이션 레지스터 값과 컨피그레이션 옵션의 목록을 표시합니다. 나중에 복원할 수 있도록 현재 컨피그레이션 레지스터 값을 기록해 둡니다.

```
Configuration Register: 0x00000041

구성 요약
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ..... auto-boot index 1 image in disks
```

5단계 다음 명령을 입력하여 ASA를 다시 로드합니다.

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASA는 시작 컨피그레이션 대신 기본 컨피그레이션을 로드합니다.

6단계 다음 명령을 입력하여 특별 권한 EXEC 모드에 액세스합니다.

```
ciscoasa# enable
```

7단계 비밀번호를 물으면 **Enter**를 누릅니다.

비밀번호는 비어 있습니다.

8단계 다음 명령을 입력하여 시작 컨피그레이션을 로드합니다.

```
ciscoasa# copy startup-config running-config
```

9단계 다음 명령을 입력하여 전역 컨피그레이션 모드에 액세스합니다.

```
ciscoasa# configure terminal
```

10단계 필요하다면 다음 명령을 입력하여 기본 컨피그레이션에서 비밀번호를 변경합니다.

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

11단계 다음 명령을 입력하여 기본 컨피그레이션을 로드합니다.

```
ciscoasa(config)# no config-register
```

기본 컨피그레이션 레지스터 값은 0x1입니다. 컨피그레이션 레지스터에 대한 자세한 내용은 명령 참조를 참조하십시오.

12단계 다음 명령을 입력하여 새 비밀번호를 시작 컨피그레이션에 저장합니다.

```
ciscoasa(config)# copy running-config startup-config
```

ASAv의 비밀번호 또는 이미지 복구

ASAv의 비밀번호 또는 이미지를 복구하려면 다음 단계를 수행합니다.

절차

1단계 실행 중인 컨피그레이션을 ASAv의 백업 파일에 복사합니다.

copy running-config *filename*

예:

```
ciscoasa# copy running-config backup.cfg
```

2단계 ASAv를 다시 시작합니다.

reload

3단계 GNU GRUB 메뉴에서 아래쪽 화살표를 누르고 **<filename> with no configuration load** 옵션을 선택한 다음 **Enter**를 누릅니다. filename은 ASAv의 기본 부트 이미지 파일 이름입니다. 기본 부트 이미지는 **fallback** 명령을 통해 자동으로 부팅되지 않습니다. 그리고 선택된 부트 이미지를 로드합니다.

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

예:

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

4단계 백업 컨피그레이션 파일을 실행 중인 컨피그레이션에 복사합니다.

copy *filename* **running-config**

예:

```
ciscoasa (config)# copy backup.cfg running-config
```

5단계 비밀번호를 초기화합니다.

enable password

예:

```
ciscoasa(config)# enable password cisco123
```

6단계 새 컨피그레이션을 저장합니다.

write memory

예:

```
ciscoasa(config)# write memory
```

비밀번호 복구 비활성화

참고 ASAv에서 비밀번호 복구를 비활성화할 수 없습니다.

허가받지 않은 사용자가 ASA를 공격할 목적으로 비밀번호 복구 메커니즘을 이용할 수 없도록 비밀번호 복구를 비활성화하려면 다음 단계를 수행합니다.

시작하기 전에

ASA에서 **no service password-recovery** 명령은 컨피그레이션을 그대로 유지하면서 ROMMON 모드를 시작할 수 없게 합니다. ROMMON 모드에 들어가면 ASA에서는 모든 플래시 파일 시스템을 지우라는 메시지를 표시합니다. ROMMON 모드를 시작하려면 먼저 이 지우기를 수행해야 합니다. 플래시 파일 시스템을 지우지 않겠다고 선택하면 ASA가 다시 로드됩니다. 비밀번호를 복구하려면 ROMMON 모드를 사용하고 기존 컨피그레이션을 유지해야 하므로, 이와 같이 지우기를 수행하면 비밀번호를 복구할 수 없게 됩니다. 그러나 비밀번호 복구를 비활성화함으로써 허가받지 않은 사용자가 컨피그레이션을 보거나 다른 비밀번호를 삽입하는 것을 막을 수 있습니다. 이러한 경우 시스템을 정상 상태로 복원하려면 새 이미지와 백업 컨피그레이션 파일(있는 경우)을 로드합니다.

참고로 **service password-recovery** 명령이 컨피그레이션 파일에 나타납니다. CLI 프롬프트에서 이 명령을 입력하면 설정이 NVRAM에 저장됩니다. 설정을 변경할 유일한 방법은 CLI 프롬프트에 명령을 입력하는 것입니다. 이 명령의 다른 버전으로 새 컨피그레이션을 로드하면 설정이 변경되지 않습니다. (비밀번호 복구를 염두에 두고) ASA에서 시작할 때 시작 컨피그레이션을 무시하도록 컨피그레이션된 상태에서 비밀번호 복구를 비활성화하면 ASA는 설정을 변경하여 평소와 같이 시작 컨피그레이션을 로드합니다. 장애 조치를 사용하는 경우, 대기 유닛이 시작 컨피그레이션을 무시하도록 컨피그레이션되어 있다면 **no service password recovery** 명령이 대기 유닛에 복제될 때 컨피그레이션 레지스터도 동일하게 변경됩니다.

절차

1단계 비밀번호 복구를 비활성화합니다.

no service password-recovery

예:

```
ciscoasa (config)# no service password-recovery
```

날짜 및 시간 설정

참고 ASASM의 날짜와 시간을 설정하지 마십시오. 이 설정은 호스트 스위치로부터 받습니다.

NTP 서버를 사용하여 날짜 및 시간 설정

NTP는 네트워크 시스템 간에 정확하게 동기화된 시간을 제공하는 계층적 서버 시스템을 구현하는 데 사용합니다. 정밀한 타임 스탬프가 포함된 CRL 검증과 같이 시간에 민감한 작업에는 이러한 정확성이 필요합니다. 여러 NTP 서버를 구성할 수 있습니다. ASA는 데이터의 신뢰도 지표인 stratum이 가장 낮은 서버를 선택합니다.

NTP 서버에서 가져온 시간은 직접 설정한 어떤 시간도 재정의합니다.

시작하기 전에

다중 상황 모드에서는 시스템 컨피그레이션에서만 시간을 설정할 수 있습니다.

절차

1단계 **Configuration > Device Setup > System Time > NTP**를 선택합니다.

2단계 **Add**를 클릭하여 **Add NTP Server Configuration** 대화 상자를 표시합니다.

3단계 NTP 서버 IP 주소를 입력합니다.

4단계 이 서버를 기본 서버로 설정하려면 **Preferred** 확인란을 선택합니다. NTP는 알고리즘을 사용하여 어떤 서버가 가장 정확한지 알아내고 그 서버와 동기화합니다. 서버의 정확도가 비슷하면 기본 서버를 사용합니다. 그러나 어떤 서버가 기본 서버보다 훨씬 더 정확할 경우 ASA는 더 정확한 쪽을 사용합니다.

5단계 드롭다운 목록에서 인터페이스를 선택합니다. 이 설정은 NTP 패킷의 발신 인터페이스를 지정합니다. 인터페이스가 비어 있는 경우 ASA는 라우팅 테이블에 따라 기본 관리 상황 인터페이스를 사용합니다. 안정성을 위해 관리 상황(및 사용 가능한 인터페이스)를 변경하려면 **None**(기본 인터페이스)를 선택합니다.

6단계 드롭다운 목록에서 키 번호를 선택합니다. 이 설정은 이 인증 키의 키 ID를 지정합니다. 그러면 MD5 인증을 사용하여 NTP 서버와 통신할 수 있습니다. NTP 서버 패킷에서도 이 키 ID를 사용해야 합니다. 이미 다른 서버를 위해 키 ID를 구성했다면 목록에서 그 ID를 선택할 수 있습니다. 그렇지 않으면 1~4294967295 범위의 숫자를 입력합니다.

7단계 **Trusted** 확인란을 선택하여 이 인증 키를 신뢰 키로 설정합니다. 이는 성공적인 인증을 위해 필요합니다.

8단계 인증 키를 설정하기 위해 키 값을 입력합니다. 이는 최대 길이가 32자인 문자열입니다.

9단계 키 값을 다시 입력하여 두 번 다 정확하게 입력했는지 확인합니다.

10단계 **OK**를 클릭합니다.

11단계 **Enable NTP authentication** 확인란을 선택하여 NTP 인증을 활성화합니다.

12단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

날짜 및 시간 직접 설정

날짜와 시간을 직접 설정하려면 다음 단계를 수행합니다.

시작하기 전에

다중 상황 모드에서는 시스템 컨피그레이션에서만 시간을 설정할 수 있습니다.

절차

1단계 **Configuration > Device Setup > System Time > Clock**을 선택합니다.

2단계 드롭다운 목록에서 표준 시간대를 선택합니다. 이 설정은 GMT에서 적정 시간 수를 더하거나 빼는 형식으로 표준 시간대를 지정합니다. Eastern Time, Central Time, Mountain Time 또는 Pacific Time 시간대를 선택하면 3월 두 번째 일요일 2:00 a.m.부터 11월 첫 번째 일요일 2:00 a.m.의 일광 절약 시간에 맞게 시간이 자동으로 조정됩니다.

참고 ASA에서 표준 시간대를 변경하면 지능형 SSM와의 연결이 끊어질 수 있습니다.

3단계 달력을 표시하려면 **Date** 드롭다운 목록을 클릭합니다. 그리고 다음 방법으로 정확한 날짜를 찾습니다.

- 월의 이름을 클릭하여 월 목록을 표시하고 원하는 월을 클릭합니다. 달력이 해당 월로 업데이트됩니다.
- 연도를 변경하려면 연도를 클릭합니다. 위쪽 및 아래쪽 화살표를 사용하여 연도를 스크롤하거나 입력 필드에 연도를 입력합니다.
- 월 및 연도의 좌우 화살표를 클릭하여 한 번에 하나씩 이전 달과 다음 달로 달력을 스크롤할 수 있습니다.
- 달력에서 원하는 날을 클릭하여 날짜를 설정합니다.

4단계 시간, 분, 초를 직접 입력합니다.

5단계 **Update Display Time**을 클릭하여 ASDM 창의 오른쪽 아래에 표시된 시간을 업데이트합니다. 현재 시간이 10초마다 자동으로 업데이트됩니다.

마스터 패스프레이즈 구성

마스터 패스프레이즈를 사용하면 일반 텍스트 비밀번호를 암호화된 형식으로 안전하게 저장할 수 있습니다. 또한 제공되는 키를 사용하여 기능 변경 없이 모든 비밀번호를 종합적으로 암호화하거나 마스킹할 수 있습니다. 다음과 같은 기능에서 마스터 패스프레이즈를 사용합니다.

- OSPF
- EIGRP
- VPN 로드 밸런싱
- VPN(원격 액세스 및 사이트 대 사이트)
- 장애 조치

- AAA 서버
- 로깅
- 공유 라이센스

참고 장애 조치가 활성화되었지만 장애 조치 공유 키가 설정되지 않은 경우, 마스터 패스프레이즈를 변경하면 오류 메시지가 나타나 마스터 패스프레이즈 변경 사항이 일반 텍스트로 전송되지 않게 하려면 장애 조치 공유 키를 입력해야 함을 알립니다.

Configuration > Device Management > High Availability > Failover를 선택하고 Shared Key 필드에 백스페이스를 제외한 임의의 문자를 입력합니다. 또는 장애 조치 16진수 키가 선택된 경우에는 16진수 32개(0-9A-Fa-f)를 입력합니다. 그리고 **Apply**를 클릭합니다.

마스터 패스프레이즈 추가 또는 변경

마스터 패스프레이즈를 추가하거나 변경하려면 다음 단계를 수행합니다.

시작하기 전에

이 절차는 보안 세션(예: 콘솔, SSH, HTTPS를 통한 ASDM)에서만 가능합니다.

절차

1단계 다음 옵션 중 하나를 선택합니다.

- 단일 상황 모드에서 **Configuration > Device Management > Advanced > Master Passphrase**를 선택합니다.
- 다중 상황 모드에서 **Configuration > Device Management > Device Administration > Master Passphrase** 를 선택합니다.

2단계 **Advanced Encryption Standard (AES) password encryption** 확인란을 선택합니다.

어떤 마스터 패스프레이즈도 유효하지 않을 경우 **Apply**를 클릭할 때 경고 메시지가 나타납니다. **OK**를 클릭하거나 **Cancel**을 클릭하여 계속할 수 있습니다.

나중에 비밀번호 암호화를 비활성화하면, 기존의 모든 암호화된 비밀번호는 바뀌지 않습니다. 그리고 마스터 패스프레이즈가 있는 한 암호화된 비밀번호는 애플리케이션의 요구 사항에 따라 해독됩니다.

3단계 **Change the encryption master passphrase** 확인란을 선택하여 새 마스터 패스프레이즈를 입력하고 확인합니다. 기본적으로 비활성화되어 있습니다.

새 마스터 패스프레이즈는 8자~128자여야 합니다.

기존 패스프레이즈를 변경하는 경우 새 패스프레이즈를 입력하기 전에 이전 패스프레이즈를 입력해야 합니다.

마스터 패스프레이즈를 삭제하려면 **New** 및 **Confirm master passphrase** 필드는 계속 비워 둡니다.

4단계 **Apply**를 클릭합니다.

마스터 패스프레이즈 비활성화

마스터 패스프레이즈를 비활성화하면 암호화된 비밀번호가 일반 텍스트 비밀번호로 돌아갑니다. 암호화된 비밀번호를 지원하지 않는 이전 소프트웨어 버전으로 다운그레이드하는 경우 패스프레이즈 삭제 기능이 유용할 수 있습니다.

시작하기 전에

- 마스터 패스프레이즈를 비활성화하려면 현재 마스터 패스프레이즈를 알아야 합니다. 패스프레이즈를 모르는 경우 14-10 페이지의 마스터 패스프레이즈 삭제를 참조하십시오.
- 이 절차는 텔넷, SSH, HTTPS를 통한 ASDM과 같은 보안 세션에서만 가능합니다.

절차

1단계 다음 옵션 중 하나를 선택합니다.

- 단일 상황 모드에서 **Configuration > Device Management > Advanced > Master Passphrase**를 선택합니다.
- 다중 상황 모드에서 **Configuration > Device Management > Device Administration > Master Passphrase**를 선택합니다.

2단계 **Advanced Encryption Standard (AES) password encryption** 확인란을 선택합니다.

어떤 마스터 패스프레이즈도 유효하지 않을 경우 **Apply**를 클릭할 때 경고 메시지가 나타납니다. **OK** 또는 **Cancel**을 클릭하여 계속합니다.

3단계 **Change the encryption master passphrase** 확인란을 선택합니다.

4단계 **Old master passphrase** 필드에 이전 마스터 패스프레이즈를 입력합니다. 마스터 패스프레이즈를 비활성화하려면 이전 마스터 패스프레이즈를 제공해야 합니다.

5단계 **New master passphrase** 및 **Confirm master passphrase** 필드는 계속 비워 둡니다.

6단계 **Apply**를 클릭합니다.

마스터 패스프레이즈 삭제

마스터 패스프레이즈를 복구할 수 없습니다. 마스터 패스프레이즈를 잊었거나 알 수 없는 경우 이를 삭제할 수 있습니다.

절차

1단계 마스터 키 및 암호화된 비밀번호가 들어 있는 컨피그레이션을 삭제합니다.

```
write erase
```

예:

```
ciscoasa(config)# write erase
```

2단계 마스터 키 또는 암호화된 비밀번호 없는 시작 컨피그레이션으로 ASA를 다시 로드합니다.

```
reload
```

예:

```
ciscoasa(config)# reload
```

Configure the DNS Server

ASA에서 호스트 이름으로 IP 주소를 확인할 수 있도록 DNS 서버를 구성해야 합니다.

- 14-11 페이지의 DNS 서버 설정
- 14-12 페이지의 DNS 캐시 모니터링

DNS 서버 설정

일부 ASA 기능에서는 도메인 이름으로 외부 서버에 액세스하려면 DNS 서버를 사용해야 합니다. 예를 들어, 봇넷 트래픽 필터 기능은 동적 데이터베이스 서버에 액세스하고 정적 데이터베이스의 항목을 확인하는 데 DNS 서버가 필요합니다. **ping**, **traceroute** 명령과 같은 기타 기능에서는 ping하거나 traceroute하려는 이름을 입력할 수 있는데, ASA는 DNS 서버와 통신하면서 그 이름을 확인합니다. 여러 SSL VPN 및 인증서 명령도 이름을 지원합니다.

또한 액세스 규칙에서 정규화된 도메인 이름(FQDN) 네트워크 객체를 사용하려면 DNS 서버를 구성해야 합니다.

참고 ASA는 기능에 따라 DNS 서버 사용을 제한적으로 지원합니다.

시작하기 전에

DNS 서버에 연결할 수 있도록 DNS 도메인 조회를 활성화하는 어떤 인터페이스에서든 알맞은 라우팅 및 액세스 규칙을 구성해야 합니다.

절차

1단계 **Configuration > Device Management > DNS > DNS Client**를 선택합니다.

2단계 하나 이상의 인터페이스에서 DNS 조회가 활성화되었는지 확인합니다. **DNS Lookup** 인터페이스 목록에서 DNS 서버 그룹 테이블 아래의 DNS Enabled 열을 클릭하고 **True**를 선택하여 인터페이스에 대한 조회를 활성화합니다.

3단계 **DNS Setup** 영역에서 다음 옵션 중 하나를 선택합니다.

- **Configure one DNS server group**.
- **Configure multiple DNS server groups**.

4단계 다음 중 하나를 수행합니다.

- DNS 그룹을 선택하고 **Edit**를 클릭합니다.
- 여러 DNS 그룹 구성을 선택한 경우 **Add**를 클릭하여 새 그룹을 추가합니다. 그룹 이름을 입력합니다.

5단계 DNS 서버 그룹을 구성합니다.

a. 구성된 서버의 IP 주소를 입력하고 **Add**를 클릭합니다.

최대 6개의 DNS 서버를 추가할 수 있습니다. ASA는 응답을 받을 때까지 각 DNS 서버를 순서대로 시도합니다. **Move Up/Move Down** 버튼을 사용하여 서버를 우선순위대로 배치합니다.

b. **Other Settings** 영역에서 목록의 다음 DNS 서버를 시도하기 전에 기다리는 시간(1초~30초)을 입력합니다. 기본값은 2초입니다. ASA에서 서버의 목록을 재시도할 때마다 시간 초과의 값이 2배가 됩니다.

c. 구성된 서버의 그룹에 대해 DNS 도메인 이름을 입력합니다.

d. **OK**를 클릭합니다.

6단계 여러 그룹이 있는 경우 사용할 그룹을 선택하고 **Set Active**를 클릭합니다. 이 서버 그룹이 DNS 요청에 사용됩니다.

7단계 쿼리마다 반드시 하나의 DNS 응답을 적용하려면 **Enable DNS Guard on all interfaces** 확인란을 선택합니다.

DNS 검사를 구성할 때 DNS Guard를 설정할 수도 있습니다. DNS 검사에 구성된 DNS Guard 설정은 특정 인터페이스에서 이 전역 설정에 우선합니다. 기본적으로 DNS 검사는 DNS Guard가 활성화된 모든 인터페이스에서 사용 가능합니다.

8단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

DNS 캐시 모니터링

ASA는 특정 클라이언트리스 SSSL VPN 및 인증서 명령에서 보낸 외부 DNS 쿼리의 DNS 정보를 로컬 캐시에 저장합니다. DNS 변환 요청이 있을 때마다 먼저 로컬 캐시를 검색합니다. 로컬 캐시에 해당 정보가 있으면 그 결과 IP 주소를 반환합니다. 로컬 캐시에서 요청을 해결하지 못하면 구성된 다양한 DNS 서버에 DNS 쿼리를 보냅니다. 외부 DNS 서버에서 요청을 해결한 경우 그 결과 IP 주소는 해당 호스트 이름과 함께 로컬 캐시에 저장됩니다.

DNS 캐시를 모니터링하려면 다음 명령을 참조하십시오.

- **show dns-hosts**

  이 명령은 DNS 캐시를 보여줍니다. 여기에는 DNS 서버로부터 동적으로 입수한 항목뿐 아니라 **name** 명령을 사용하여 직접 입력한 이름과 IP 주소가 들어 있습니다.

ASP(Accelerated Security Path) 성능 및 동작 모니터링

ASP는 정책과 컨피그레이션을 실행에 옮기는 구현 레이어입니다. Cisco Technical Assistance Center와 문제를 해결할 때가 아니면 직접적인 연관성은 없습니다. 그러나 몇 가지 성능 및 안정성 관련 동작은 조정할 수 있습니다.

- 14-13 페이지의 규칙 엔진 트랜잭션 커밋 모델 선택
- 14-13 페이지의 ASP 로드 밸런싱 활성화

규칙 엔진 트랜잭션 커밋 모델 선택

기본적으로 규칙 기반 정책(예: 액세스 규칙)을 바꾸면 그 변경 사항이 즉시 적용됩니다. 하지만 이와 같은 신속성이 다소 성능에 영향을 미칩니다. 이 성능 문제는 초당 연결 수가 많은 환경에서 매우 큰 규칙 목록을 사용할 때 더욱 두드러집니다. 예를 들면, ASA에서 초당 18,000건의 연결을 처리하는 동안 25,000개의 규칙이 포함된 정책을 변경하는 경우입니다.

규칙 엔진이 규칙 조회 속도를 높이고자 규칙을 컴파일하면서 성능에 영향을 줍니다. 기본적으로 이 시스템은 연결 시도를 평가할 때 새로운 규칙을 적용할 수 있도록 컴파일되지 않은 규칙도 검색합니다. 규칙이 컴파일되지 않았으므로 검색 시간이 늘어납니다.

규칙 엔진에서 규칙 변경을 구현할 때 트랜잭션 모델을 사용함으로써 새 규칙이 컴파일되어 사용 가능해질 때까지 기존 규칙을 계속 사용하도록 위 동작을 변경할 수 있습니다. 트랜잭션 모델을 사용하면 규칙 컴파일 과정에서 성능이 저하되지 않습니다. 다음 표에서 동작의 차이점을 확인할 수 있습니다.

모델	컴파일 전	컴파일 과정	컴파일 후
기본	기존 규칙에 매칭합니다.	새 규칙에 매칭합니다. (초당 연결 수 감소)	새 규칙에 매칭합니다.
트랜잭션	기존 규칙에 매칭합니다.	기존 규칙에 매칭합니다. (초당 연결 수 변동 없음)	새 규칙에 매칭합니다.

트랜잭션 모델의 또 다른 이점은 인터페이스에서 ACL을 대체할 때 기존 ACL을 삭제하는 시점과 새 ACL을 적용하는 시점 사이에 공백이 없다는 것입니다. 이 기능 덕분에 작업 과정에서 적합한 연결이 폐기될 가능성이 줄어듭니다.

팁 규칙 유형에 대해 트랜잭션 모델을 활성화하면 컴파일의 시작과 끝을 알리는 syslog가 생성됩니다. 이 syslog의 번호는 780001~ 780004입니다.

규칙 엔진에 트랜잭션 커밋 모델을 활성화하려면 **Configuration > Device Management > Advanced > Rule Engine**을 선택하고 원하는 옵션을 선택합니다.

- **Access group**—전역에 또는 인터페이스에 적용되는 액세스 규칙
- **NAT**—네트워크 주소 변환 규칙

ASP 로드 밸런싱 활성화

ASP 로드 밸런싱 메커니즘으로 다음 문제를 예방할 수 있습니다.

- 흐름에서 산발적인 트래픽 급증으로 인한 오버런
- 특정 인터페이스 수신 링에 초과 유입되는 대량 흐름에 의한 오버런
- 비교적 과부하 상태인 인터페이스 수신 링으로 인한 오버런. 단일 코어에서 부하를 수용할 수 없음

asp load-balance per-packet 명령은 여러 코어가 단일 인터페이스 수신 링에서 받은 패킷을 동시에 작업할 수 있게 합니다. 시스템에서 패킷을 폐기하고 **show cpu** 명령 출력이 100%보다 훨씬 적은 경우, 패킷이 관련 없는 다수의 연결에 속한 것이라면 이 명령으로 처리량을 늘릴 수 있습니다. **auto** 옵션은 ASA에서 패킷별 로드 밸런싱을 자동으로 켜거나 끌 수 있게 합니다.

멀티코어 ASA 모델에서는 다수의 패킷이 폐기되었지만 CPU 사용량이 100%에 한참 미치지 못할 경우 로드 밸런싱 옵션을 활성화해야 합니다.

Configuration > Device > Management > Advanced > ASP를 선택하고 **Enable per-packet ASP load balance** 확인란을 선택합니다.

ASA 5585에서 ASP 로드 밸런싱을 자동으로 활성화하려면 **Dynamically enable or disable ASP load balancing based on traffic monitoring** 확인란을 선택합니다.

기본 설정 기능 내역

기능 이름	플랫폼 릴리스	설명
마스터 패스프레이즈	8.3(1)	이 기능을 도입했습니다. 마스터 패스프레이즈를 사용하면 일반 텍스트 비밀번호를 암호화된 형식으로 안전하게 저장할 수 있습니다. 또한 제공되는 키를 사용하여 기능 변경 없이 모든 비밀번호를 종합적으로 암호화하거나 마스킹할 수 있습니다. 다음 화면을 도입했습니다. Configuration > Device Management > Advanced > Master Passphrase Configuration > Device Management > Device Administration > Master Passphrase.
기본 텔넷 비밀번호 삭제	9.0(2)/9.1(2)	ASA에 대한 관리 액세스의 보안을 강화하는 차원에서 텔넷을 사용하는 로그인에서는 먼저 기본 로그인 비밀번호를 직접 설정해야 합니다. **참고** 로그인 비밀번호는 텔넷 사용자 인증을 구성하지 않은 경우에 텔넷에서만 사용됩니다. 이전에는 비밀번호를 지우면 ASA에서 기본값인 “cisco”로 변경했습니다. 이제는 비밀번호를 지우면 해당 비밀번호가 삭제됩니다. 이 로그인 비밀번호는 스위치에서 ASASM로 연결하는 텔넷 세션에도 사용됩니다(**session** 명령 참조). 최초로 ASASM에 액세스할 경우 로그인 비밀번호를 설정할 때까지 **service-module session** 명령을 사용해야 합니다. ASDM 화면은 수정하지 않았습니다.
ASP 로드 밸런싱	9.3(2)	이 기능을 도입했습니다. ASP 로드 밸런싱 메커니즘은 CPU의 여러 코어에서 인터페이스 수신 링으로부터 패킷을 받고 독자적으로 작업할 수 있게 함으로써 패킷의 폐기를 줄이고 처리량을 늘립니다. 다음 화면을 도입했습니다. Configuration > Device Management > Advanced > ASP Load Balancing

DHCP 서비스

이 장에서는 DHCP 서버 또는 DHCP 릴레이를 구성하는 방법을 설명합니다.

DHCP 서버 소개

DHCP는 IP 주소와 같은 네트워크 컨피그레이션 파라미터를 DHCP 클라이언트에 제공합니다. Cisco ASA는 ASA 인터페이스에 연결된 DHCP 클라이언트에 DHCP 서버를 제공할 수 있습니다. DHCP 서버는 DHCP 클라이언트에 직접 네트워크 컨피그레이션 파라미터를 제공합니다.

클라이언트는 DHCP 서버를 찾아 예약된 링크 범위(link-scoped) 멀티캐스트 주소를 사용하여 컨피그레이션 정보의 지정을 요청합니다. 따라서 클라이언트와 서버는 동일한 링크에 연결되어야 합니다. 그러나 사용 편의성, 경제성 또는 확장성이 중요한 경우에는 DHCP 클라이언트가 동일한 링크에 연결되지 않은 서버에 메시지를 보낼 수 있게 하는 것이 좋습니다. 클라이언트 네트워크에 상주할 수 있는 DHCP 릴레이가 클라이언트와 서버 사이에서 메시지를 전달하면 됩니다. 릴레이 에이전트 작업은 클라이언트에 투명하게 이루어집니다.

IPv4 DHCP 클라이언트는 서버와 연결하는 데 멀티캐스트 주소가 아닌 브로드캐스트를 사용합니다. DHCP 클라이언트는 UDP 포트 68에서 메시지를 수신합니다. DHCP 서버는 UDP 포트 67에서 메시지를 수신합니다.

RFC 3315에 규정된 DHCPv6(DHCP for IPv6)는 IPv6 DHCP 서버에서 IPv6 노드(즉 DHCP 클라이언트)에 네트워크 주소 또는 접두사, DNS 서버 주소와 같은 컨피그레이션 파라미터를 보낼 수 있게 합니다. DHCPv6는 다음 멀티캐스트 주소를 사용합니다.

- All_DHCP_Relay_Agents_and_Servers(FF02::1:2)는 클라이언트에서 인접한(즉 on-link) 릴레이 에이전트 및 서버와 통신하는 데 사용하는 링크 범위 멀티캐스트 주소입니다. 모든 DHCPv6 서버와 릴레이 에이전트는 이 멀티캐스트 그룹의 멤버입니다.
- DHCPv6 릴레이 서비스 및 서버는 UDP 포트 547에서 메시지를 수신합니다. ASA DHCPv6 릴레이 에이전트는 UDP 포트 547과 All_DHCP_Relay_Agents_and_Servers 멀티캐스트 주소 모두에서 수신합니다.

DHCP 릴레이 에이전트 소개

인터페이스에서 수신한 DHCP 요청을 하나 이상의 DHCP 서버에 전달하도록 DHCP 릴레이 에이전트를 구성할 수 있습니다. DHCP 클라이언트는 최초 DHCPDISCOVER 메시지를 보내는 데 UDP 브로드캐스트를 사용합니다. 연결된 네트워크에 대한 정보가 없기 때문입니다. 클라이언트가 연결된 세그먼트에 서버가 없을 경우, ASA는 (브로드캐스트 트래픽을 전달하지 않으므로) 대개는 UDP 브로드캐스트를 전달하지 않습니다.

브로드캐스트를 수신하는 ASA의 인터페이스를 구성하여 DHCP 요청을 다른 인터페이스의 DHCP 서버에 전달하게 함으로써 이러한 문제를 해결할 수 있습니다.

DHCP 서비스를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

모든 ASA 모델에서 DHCP 클라이언트 주소의 최대 개수는 라이센스에 따라 달라집니다.

- 한도가 호스트 10개일 경우 최대 가용 DHCP 풀은 주소 32개입니다.
- 한도가 호스트 50개일 경우 최대 가용 DHCP 풀은 주소 128개입니다.
- 호스트 수가 무제한일 경우 최대 가용 DHCP 풀은 주소 256개입니다.

DHCP 서비스 지침

방화벽 모드 지침

투명 방화벽 모드에서 지원되지 않습니다. 자세한 내용은 15-3 페이지의 DHCP 릴레이 지침를 참조하십시오.

IPv6 지침

IPv6에서는 인터페이스 특정 DHCP 릴레이 서버를 지원하지 않습니다.

DHCP 서버 지침

- 최대 가용 DHCP 풀은 주소 256개입니다.
- ASA의 각 인터페이스에서 DHCP 서버를 1개만 구성할 수 있습니다. 각 인터페이스는 자체 주소 풀을 두고 사용할 수 있습니다. 그러나 DNS 서버, 도메인 이름, 옵션, ping 시간 초과, WINS 서버와 같은 나머지 DHCP 설정은 전역으로 구성되며 모든 인터페이스에서 DHCP 서버에 의해 사용됩니다.
- 서버가 활성화된 인터페이스에서 DHCP 클라이언트 또는 DHCP 릴레이 서비스를 구성할 수 없습니다. 또한 DHCP 클라이언트는 서버가 활성화된 인터페이스에 직접 연결되어야 합니다.
- ASA는 QIP DHCP 서버를 DHCP 프록시 서비스와 함께 사용하는 것을 지원하지 않습니다.
- DHCP 서버가 활성화되지 않으면 릴레이 에이전트도 활성화될 수 없습니다.

- ASA DHCP 서버는 BOOTP 요청을 지원하지 않습니다. 다중 컨텍스트 모드에서는 둘 이상의 컨텍스트가 사용하는 인터페이스에서 DHCP 서버 또는 DHCP 릴레이 서비스를 활성화할 수 없습니다.
- ASA는 DHCP 요청을 수신하면 DHCP 서버에 검색(discovery) 메시지를 보냅니다. 이 메시지에는 그룹 정책에서 **dhcp-network-scope** 명령으로 구성된 IP 주소(서브네트워크 내)가 들어 있습니다. 서버가 그 서브네트워크에 속하는 주소 풀을 가진 경우, 검색 메시지의 소스 IP 주소가 아니라 그 주소에 풀 정보와 함께 제안(offer) 메시지를 보냅니다.
- 클라이언트가 연결하면 ASA는 서버 목록의 모든 서버에 검색 메시지를 보냅니다. 이 메시지에는 그룹 정책에서 **dhcp-network-scope** 명령으로 구성된 IP 주소(서브네트워크 내)가 들어 있습니다. ASA는 수신한 첫 번째 제안을 선택하고 나머지 제안은 폐기합니다. 서버가 그 서브네트워크에 속하는 주소 풀을 가진 경우, 검색 메시지의 소스 IP 주소가 아니라 그 주소에 풀 정보와 함께 제안(offer) 메시지를 보냅니다. 주소의 갱신이 필요한 경우 임대 서버(확보한 주소의 출처인 서버)와 주소 갱신을 시도합니다. DHCP 갱신이 지정된 재시도 횟수(4회)만큼 실패한 경우 ASA는 미리 지정된 기간이 지나면 DHCP 리바인드 단계로 진행합니다. 리바인드 단계에서는 ASA가 그룹의 모든 서버에 동시에 요청을 보냅니다. 고가용성 환경에서는 임대 정보가 공유됩니다. 즉 다른 모든 서버가 임대를 확인할 수 있으며, ASA는 바운드 상태로 돌아갑니다. 리바인드 단계에서 (3회 재시도 후) 서버 목록의 어떤 서버로부터도 응답이 없을 경우 ASA는 항목을 삭제합니다.

  예를 들어, 서버에 범위가 209.165.200.225~209.165.200.254, 마스크가 255.255.255.0인 풀이 있고 **dhcp-network-scope** 명령에 의해 지정된 IP 주소가 209.165.200.1이라면, 서버는 ASA에 보내는 제안 메시지를 통해 그 풀을 전송합니다.

  dhcp-network-scope 명령 설정은 VPN 사용자에게만 적용됩니다.

DHCP 릴레이 지침

- 단일 모드 및 각 컨텍스트에서 전역 서버와 인터페이스 특정 서버를 포함하여 최대 10개의 DHCPv4 릴레이 서버를 구성할 수 있으며, 각 인터페이스에는 최대 4개의 서버가 가능합니다.
- 단일 모드 및 각 컨텍스트에서 최대 10개의 DHCPv6 릴레이 서버를 구성할 수 있습니다. IPv6 인터페이스 특정 서버는 지원되지 않습니다.
- DHCP 서버 기능이 활성화되지 않으면 릴레이 에이전트도 활성화될 수 없습니다.
- DHCP 릴레이 서비스가 활성화되었고 둘 이상의 DHCP 릴레이 서버가 정의되었으면, ASA는 정의된 DHCP 릴레이 서버 각각에 클라이언트 요청을 전달합니다. 클라이언트 DHCP 릴레이 바인딩이 제거될 때까지는 서버의 회신도 클라이언트에 전달됩니다. 이 바인딩은 ASA에서 DHCP 메시지 ACK, NACK, ICMP unreachable 또는 decline 중 하나를 받으면 제거됩니다.
- DHCP 프록시 서비스로 실행 중인 인터페이스에서 DHCP 릴레이 서비스를 활성화할 수 없습니다. 먼저 VPN DHCP 컨피그레이션을 삭제해야 합니다. 그러지 않으면 오류 메시지가 나타납니다. 이 오류는 DHCP 릴레이 및 DHCP 프록시 서비스 모두 활성화된 경우 발생합니다. DHCP 릴레이 또는 DHCP 프록시 서비스 중 하나만 활성화되어야 합니다.
- DHCP 릴레이 서비스는 투명 방화벽 모드에서 사용할 수 없습니다. 그러나 액세스 목록을 사용하는 방법으로 DHCP 트래픽을 허용할 수 있습니다. 투명 모드에서 DHCP 요청과 회신이 ASA를 지날 수 있게 하려면 2개의 액세스 목록을 구성해야 합니다. 하나는 내부 인터페이스에서 외부로 보내는 DHCP 요청을 허용하는 것이고 다른 하나는 반대 방향으로 서버의 회신을 허용하는 것입니다.
- IPv4에서는 클라이언트가 ASA에 직접 연결되어야 하며, 다른 릴레이 에이전트 또는 라우터를 통해 요청을 보낼 수 없습니다. IPv6에서는 ASA가 다른 릴레이 서버에서 보낸 패킷을 지원합니다.
- 다중 컨텍스트 모드에서는 둘 이상의 컨텍스트가 사용하는 인터페이스에서 DHCP 릴레이를 활성화할 수 없습니다.
- DHCP 클라이언트는 ASA에서 요청을 릴레이하는 DHCP 서버와 다른 인터페이스에 있어야 합니다.

DHCP 서버 구성

이 단원에서는 ASA에서 제공하는 DHCP 서버의 구성 방법을 설명합니다.

1단계 DHCP 서버를 활성화합니다. 15-4 페이지의 DHCP 서버 활성화를 참조하십시오.

2단계 고급 DHCP 옵션을 구성합니다. 15-6 페이지의 고급 DHCP 옵션 구성를 참조하십시오.

3단계 DHCPv4 릴레이 에이전트와 DHCPv6 릴레이 에이전트 중 하나를 구성합니다. 15-7 페이지의 DHCPv4 릴레이 에이전트 구성 또는 15-7 페이지의 DHCPv6 릴레이 에이전트 구성를 참조하십시오.

DHCP 서버 활성화

ASA 인터페이스에서 DHCP 서버를 활성화하려면 다음 단계를 수행합니다.

절차

1단계 **Configuration > Device Management > DHCP > DHCP Server**를 선택합니다.

2단계 인터페이스를 선택하고 **Edit**를 클릭합니다.

a. 선택된 인터페이스에서 DHCP 서버를 활성화하기 위해 **Enable DHCP Server** 확인란을 선택합니다.

b. **DHCP Address Pool** 필드에 DHCP 서버에서 사용하는 IP 주소의 범위를 가장 낮은 것부터 입력합니다. 이 IP 주소 범위는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소는 포함할 수 없습니다.

c. **Optional Parameters** 영역에 다음을 설정합니다.

- 인터페이스에 대해 구성된 DNS 서버(1, 2)
- 인터페이스에 대해 구성된 WINS 서버(기본, 보조)
- 인터페이스의 도메인 이름
- ASA가 인터페이스에서 ICMP ping 응답을 기다리는 시간(밀리초)
- 인터페이스에 구성된 DHCP 서버가 DHCP 클라이언트에서 지정된 IP 주소를 사용하는 것을 허용하는 기간
- ASA가 어떤 지정된 인터페이스(대개는 외부)에서 DHCP 클라이언트의 역할을 하는 경우, 자동 컨피그레이션을 위한 DNS, WINS, 도메인 이름 정보를 제공하는 DHCP 클라이언트의 인터페이스
- 다른 DHCP 옵션을 구성하려면 **Advanced**를 클릭하여 **Advanced DHCP Options** 대화 상자를 표시합니다. 자세한 내용은 15-6 페이지의 고급 DHCP 옵션 구성를 참조하십시오.

d. 선택된 DHCP 서버가 클라이언트 PTR 리소스 레코드 업데이트라는 기본 작업과 함께 다음 업데이트 작업도 수행하게 하려면 **Update DNS Clients** 확인란(**Dynamic Settings for DHCP Server** 영역)을 선택합니다.

- DHCP 서버가 A RR과 PTR RR을 모두 업데이트하게 하려면 **Update Both Records** 확인란을 선택합니다.
- DHCP 서버가 DHCP 클라이언트에 의해 요청된 모든 업데이트 작업을 재정의하게 하려면 **Override Client Settings** 확인란을 선택합니다.

e. **OK**를 클릭하여 **Edit DHCP Server** 대화 상자를 닫습니다.

3단계 ASA가 어떤 지정된 인터페이스(대개는 외부)에서 DHCP 클라이언트의 역할을 하는 경우에만 DHCP 자동 컨피그레이션을 활성화하려면 DHCP Server 테이블 아래의 **Global DHCP Options** 영역에서 **Enable Auto-configuration from interface** 확인란을 선택합니다.

DHCP 자동 컨피그레이션은 DHCP 서버가 지정된 인터페이스에서 실행 중인 어떤 DHCP 클라이언트로부터 얻은 DNS 서버, 도메인 이름, WINS 서버 정보를 DHCP 클라이언트에 제공할 수 있게 합니다. 자동 컨피그레이션을 통해 얻은 정보가 **Global DHCP Options** 영역에서도 수동으로 지정된 경우, 수동으로 지정된 정보가 검색된 정보에 우선합니다.

4단계 드롭다운 목록에서 인터페이스를 선택합니다.

5단계 인터페이스 DHCP 또는 PPPoE 클라이언트 WINS 파라미터를 VPN 클라이언트 파라미터로 재정의하려면 **Allow VPN override** 확인란을 선택합니다.

6단계 **DNS Server 1** 필드에 DHCP 클라이언트의 기본 DNS 서버 IP 주소를 입력합니다.

7단계 **DNS Server 2** 필드에 DHCP 클라이언트의 대체 DNS 서버 IP 주소를 입력합니다.

8단계 **Domain Name** 필드에 DHCP 클라이언트의 DNS 도메인 이름(예: example.com)을 입력합니다.

9단계 클라이언트가 할당받은 IP 주소를 임대 만료 전까지 사용할 수 있는 시간(초)을 **Lease Length** 필드에 입력합니다. 유효한 값의 범위는 300초~1048575초입니다. 기본값은 3600초(1시간)입니다.

10단계 **Primary WINS Server** 필드에 DHCP 클라이언트의 기본 WINS 서버 IP 주소를 입력합니다.

11단계 **Secondary WINS Server** 필드에 DHCP 클라이언트의 대체 WINS 서버 IP 주소를 입력합니다.

12단계 주소 충돌을 방지하고자 ASA는 DHCP 클라이언트에 주소를 지정하기 전에 주소에 2개의 ICMP ping 패킷을 보냅니다. ASA에서 DHCP ping 시도의 시간 초과까지 기다리는 시간(밀리초)을 **Ping Timeout** 필드에 입력합니다. 유효한 값의 범위는 10밀리초~10000밀리초입니다. 기본값은 50밀리초입니다.

13단계 추가 DHCP 옵션과 그 파라미터를 지정하려면 **Advanced**를 클릭하여 **Configuring Advanced DHCP Options** 대화 상자를 표시합니다. 자세한 내용은 15-6 페이지의 고급 DHCP 옵션 구성를 참조하십시오.

14단계 **Dynamic DNS Settings for DHCP Server** 영역에서 DHCP 서버를 위한 DDNS 업데이트 설정을 구성합니다. 선택된 DHCP 서버가 클라이언트 PTR 리소스 레코드 업데이트라는 기본 작업과 함께 다음 업데이트 작업도 수행하게 하려면 **Update DNS Clients** 확인란을 선택합니다.

- DHCP 서버가 A RR과 PTR RR을 모두 업데이트하게 하려면 **Update Both Records** 확인란을 선택합니다.
- DHCP 서버 작업이 DHCP 클라이언트에 의해 요청된 모든 업데이트 작업을 재정의하게 하려면 **Override Client Settings** 확인란을 선택합니다.

15단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

고급 DHCP 옵션 구성

ASA는 정보 전송을 위해 RFC 2132, RFC 2562, RFC 5510에 규정된 DHCP 옵션을 지원합니다.

고급 DHCP 옵션을 사용하여 DHCP 클라이언트에 DNS, WINS, 도메인 이름 파라미터를 제공할 수 있습니다. 또한 DHCP 자동 컨피그레이션 설정을 사용하여 이 값을 얻거나 직접 정의할 수도 있습니다. 이 정보를 정의하는 데 둘 이상의 방법을 사용할 경우 다음 순서로 DHCP 클라이언트에 전달됩니다.

1. 직접 구성한 설정
2. 고급 DHCP 옵션 설정
3. DHCP 자동 컨피그레이션 설정

이를테면 DHCP 클라이언트에서 수신할 도메인 이름을 직접 정의한 다음 DHCP 자동 컨피그레이션을 활성화할 수 있습니다. DHCP 자동 컨피그레이션에서 DNS 및 WINS 서버와 함께 도메인을 검색하더라도, 수동으로 정의된 도메인 이름이 검색된 DNS 및 WINS 서버 이름과 함께 DHCP 클라이언트에 전달됩니다. DHCP 자동 컨피그레이션 프로세스에 의해 검색된 도메인 이름보다 수동 정의된 도메인 이름이 우선하기 때문입니다.

절차

1단계 **Configuration > Device Management > DHCP > DHCP Server**를 선택하고 **Advanced**를 클릭합니다.

2단계 드롭다운 목록에서 옵션 코드를 선택합니다. 1, 12, 50–54, 58–59, 61, 67, 82 를 제외하고 모든 DHCP 옵션(1~255)이 지원됩니다.

3단계 구성할 옵션을 선택합니다. 일부 옵션은 표준입니다. 표준 옵션은 옵션 번호 다음에 옵션 이름이 괄호로 묶여 표시되며, 옵션 파라미터가 해당 옵션에서 지원하는 것으로 한정됩니다. 그 밖의 모든 옵션은 옵션 번호만 표시되며, 옵션과 함께 제공할 알맞은 파라미터를 선택해야 합니다. 예를 들어, DHCP Option 2 (Time Offset)를 선택한 경우 이 옵션에 16진수 값만 입력할 수 있습니다. 그 밖의 모든 DHCP 옵션에서는 모든 옵션 값 유형을 사용할 수 있으며, 알맞은 것을 선택해야 합니다.

4단계 **Option Data** 영역에서는 해당 옵션에서 DHCP 클라이언트에 반환할 정보의 유형을 지정합니다. 표준 DHCP 옵션의 경우 지원되는 옵션 값 유형만 사용 가능합니다. 그 밖의 모든 DHCP 옵션에서는 모든 옵션 값 유형을 사용할 수 있습니다. DHCP 옵션 목록에 옵션을 추가하려면 **Add**를 클릭합니다. DHCP 옵션 목록에서 옵션을 삭제하려면 **Delete**를 클릭합니다.

- IP 주소가 DHCP 클라이언트에 반환되게 하려면 **IP Address**를 클릭합니다. 최대 2개의 IP 주소를 지정할 수 있습니다. IP Address 1 및 IP Address 2는 점으로 구분된 10진수 표기법의 IP 주소입니다.

  참고 IP 주소 필드의 이름은 선택한 DHCP 옵션에 따라 달라질 수 있습니다. 예를 들어, DHCP Option 3 (Router)를 선택한 경우 필드 이름은 Router 1 및 Router 2로 바뀝니다.

- ASCII 값이 DHCP 클라이언트에 반환되게 하려면 **ASCII**를 클릭합니다. **Data** 필드에 ASCII 문자열을 입력합니다. 이 문자열은 공백을 포함할 수 없습니다.

  참고 Data 필드의 이름은 선택한 DHCP 옵션에 따라 달라질 수 있습니다. 만약 DHCP Option 14 (Merit Dump File)를 선택하면 Data 필드 이름은 File Name으로 바뀝니다.

- 16진수 값이 DHCP 클라이언트에 반환되게 하려면 **Hex**를 클릭합니다. **Data** 필드에 자릿수가 짝수이고 공백이 없는 16진수 문자열을 입력합니다. 0x 접두사를 사용할 필요 없습니다.

참고 Data 필드의 이름은 선택한 DHCP 옵션에 따라 달라질 수 있습니다. DHCP Option 2 (Time Offset)를 선택하면 Data 필드의 이름은 Offset 필드가 됩니다.

5단계 **OK**를 클릭하여 **Advanced DHCP Options** 대화 상자를 닫습니다.

6단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

DHCPv4 릴레이 에이전트 구성

DHCP 요청이 인터페이스에 들어올 때 ASA에서 그 요청을 릴레이할 DHCP 서버는 컨피그레이션에 따라 달라집니다. 다음 유형의 서버를 구성할 수 있습니다.

- 인터페이스 특정 DHCP 서버—DHCP 요청이 특정 인터페이스에 들어오면 ASA는 그 인터페이스에 특정된 서버에만 요청을 릴레이합니다.
- 전역 DHCP 서버—DHCP 요청이 인터페이스 특정 서버가 구성되지 않은 인터페이스에 들어오면 ASA는 모든 전역 서버에 요청을 릴레이합니다. 인터페이스에 인터페이스 특정 서버가 있는 경우 전역 서버는 사용되지 않습니다.

DHCPv6 릴레이 에이전트 구성

DHCPv6 요청이 인터페이스에 들어오면 ASA는 모든 DHCPv6 전역 서버에 그 요청을 릴레이합니다.

절차

1단계 **Configuration > Device Management > DHCP > DHCP Relay**를 선택합니다.

2단계 **DHCP Relay Agent** 영역에서 인터페이스별로 원하는 서비스의 확인란을 선택합니다.

- **IPv4 > DHCP Relay Enabled**.
- **IPv4 > Set Route**— 서버에서 보내는 DHCP 메시지의 기본 게이트웨이 주소를 최초의 DHCP 요청을 릴레이한 DHCP 클라이언트에 가장 가까운 ASA 인터페이스의 게이트웨이 주소로 변경합니다. 이 작업을 수행하면 클라이언트는 DHCP 서버가 다른 라우터를 지정하더라도 ASA를 가리키는 기본 경로를 설정할 수 있습니다. 패킷에 기본 라우터 옵션이 없는 경우 ASA는 인터페이스 주소를 포함하는 것을 추가합니다.
- **IPv6 > DHCP Relay Enabled**.
- **Trusted Interface**—신뢰할 DHCP 클라이언트 인터페이스를 지정합니다. DHCP Option 82를 보존하기 위해 인터페이스를 신뢰받는 인터페이스로 구성할 수 있습니다. DHCP Option 82는 다운스트림 스위치 및 라우터에서 DHCP 스누핑과 IP 소스 가드에 사용합니다. 일반적으로 ASA DHCP 릴레이 에이전트에서 Option 82가 이미 설정된 DHCP 패킷을 수신하지만 giaddr 필드(서버에 패킷을 전달하기 전에 릴레이 에이전트에 의해 설정되는 DHCP 릴레이 에이전트 주소 지정)가 0으로 설정된 경우 ASA는 기본적으로 그 패킷을 폐기합니다. 이제는 어떤 인터페이스를 신뢰받는 인터페이스로 지정함으로써 Option 82를 보존하고 패킷을 전달할 수 있습니다. 또는 **Set dhcp relay information as trusted on all interfaces** 확인란을 선택하여 모든 인터페이스를 신뢰할 수 있습니다(7단계 참조).

3단계 **Global DHCP Relay Servers** 영역에서 DHCP 요청이 릴레이될 DHCP 서버를 하나 이상 추가합니다.

a. **Add**를 클릭합니다. **Add Global DHCP Relay Server** 대화 상자가 나타납니다.

b. **DHCP Server** 필드에 DHCP 서버의 IPv4 또는 IPv6 주소를 입력합니다.

c. **Interface** 드롭다운 목록에서 지정된 DHCP 서버가 연결된 인터페이스를 선택합니다.

d. **OK**를 클릭합니다.

새로 추가된 글로벌 DHCP 릴레이 서버가 **Global DHCP Relay Servers** 목록에 나타납니다.

4단계 (선택 사항) **IPv4 Timeout** 필드에 DHCP 주소 처리에 허용된 시간(초)을 입력합니다. 유효한 값의 범위는 1초~3600초입니다. 기본값은 60초입니다.

5단계 (선택 사항) **IPv6 Timeout** 필드에 DHCP 주소 처리에 허용된 시간(초)을 입력합니다. 유효한 값의 범위는 1초~3600초입니다. 기본값은 60초입니다.

6단계 **DHCP Relay Interface Servers** 영역에서 어떤 인터페이스의 DHCP 요청이 릴레이될 인터페이스 특정 DHCP 서버를 하나 이상 추가합니다.

a. **Add**를 클릭합니다. **Add DHCP Relay Server** 대화 상자가 나타납니다.

b. **Interface** 드롭다운 목록에서 DHCP 클라이언트에 연결된 인터페이스를 선택합니다. 전역 DHCP 서버에서처럼 요청에 대해 이그레스 인터페이스를 지정하지 않습니다. 그 대신 ASA에서는 라우팅 테이블을 사용하여 이그레스 인터페이스를 확인합니다.

c. **Server to...** 필드에 DHCP 서버의 IPv4 주소를 입력하고 **Add>>**를 클릭합니다. 서버가 오른쪽 목록에 추가됩니다. 총 최대 한도에서 가능한 경우 서버를 4대까지 추가합니다. IPv6에서는 인터페이스 특정 서버가 지원되지 않습니다.

d. **OK**를 클릭합니다.

새로 추가된 인터페이스 DHCP 릴레이 서버가 **DHCP Relay Interface Servers** 목록에 나타납니다.

7단계 모든 인터페이스를 신뢰받는 인터페이스로 구성하려면 **Set dhcp relay information as trusted on all interfaces** 확인란을 선택합니다. 또는 개별 인터페이스를 신뢰할 수도 있습니다(2단계 참조).

8단계 **Apply**를 클릭하여 설정을 저장합니다.

DHCP 서비스 모니터링

DHCP 서비스를 모니터링하려면 다음 화면을 참조하십시오.

- **Monitoring > Interfaces > DHCP > DHCP Client Lease Information**.

  이 창에서는 구성된 DHCP 클라이언트 IP 주소를 표시합니다.

- **Monitoring > Interfaces > DHCP > DHCP Server Table**

  이 창에서는 구성된 동적 DHCP 클라이언트 IP 주소를 표시합니다.

- **Monitoring > Interfaces > DHCP > DHCP Statistics**

  이 창에서는 DHCP 메시지 유형, 카운터, 값, 방향, 수신 메시지, 전송 메시지를 표시합니다.

- **Tools > Command Line Interface**

  이 창에서는 ASA에 비대화형 명령을 전송하고 그 결과를 표시합니다.

DHCP 서비스 기능 내역

표 15-1 DHCP 서비스 기능 내역

기능 이름	플랫폼 릴리스	설명
DHCP	7.0(1)	ASA에서 ASA 인터페이스에 연결된 DHCP 클라이언트에 DHCP 서버 또는 DHCP 릴레이 서비스를 제공할 수 있습니다. 다음 화면을 도입했습니다. Configuration > Device Management > DHCP > DHCP Relay Configuration > Device Management > DHCP > DHCP Server
DHCPv6(DHCP for IPv6)	9.0(1)	IPv6 지원을 추가했습니다. 다음 화면을 수정했습니다. Configuration > Device Management > DHCP > DHCP Relay
인터페이스별 DHCP 릴레이 서버(IPv4만 해당)	9.1(2)	인터페이스별로 DHCP 릴레이 서버를 구성할 수 있습니다. 그러면 해당 인터페이스에 들어오는 요청은 그 인터페이스에 지정된 서버에만 릴레이합니다. IPv6에서는 인터페이스별 DHCP 릴레이를 지원하지 않습니다. 다음 화면을 수정했습니다. Configuration > Device Management > DHCP > DHCP Relay
DHCP 신뢰받는 인터페이스	9.1(2)	DHCP Option 82를 보존하기 위해 인터페이스를 신뢰받는 인터페이스로 구성할 수 있습니다. DHCP Option 82는 다운스트림 스위치 및 라우터에서 DHCP 스누핑과 IP 소스 가드에 사용합니다. 일반적으로 ASA DHCP 릴레이 에이전트에서 Option 82가 이미 설정된 DHCP 패킷을 수신하지만 giaddr 필드(서버에 패킷을 전달하기 전에 릴레이 에이전트에 의해 설정되는 DHCP 릴레이 에이전트 주소 지정)가 0으로 설정된 경우 ASA는 기본적으로 그 패킷을 폐기합니다. 이제는 어떤 인터페이스를 신뢰받는 인터페이스로 지정함으로써 Option 82를 보존하고 패킷을 전달할 수 있습니다. 다음 화면을 수정했습니다. Configuration > Device Management > DHCP > DHCP Relay
DHCP 리바인드 기능	9.1(4)	DHCP 리바인드 단계에서 클라이언트가 터널 그룹 목록에 있는 다른 DHCP 서버와의 리바인드를 시도합니다. 이 릴리스 전에는 DHCP 임대 갱신에 실패했을 때 클라이언트가 대체 서버에 리바인드하지 않았습니다. ASDM 화면은 수정하지 않았습니다.

16 장

동적 DNS

이 장에서는 DDNS(동적 DNS) 업데이트 메서드를 어떻게 구성하는지 설명합니다.

DDNS 소개

DDNS 업데이트는 DNS와 DHCP를 통합합니다. 두 프로토콜은 상호 보완적입니다. DHCP는 IP 주소 할당을 중앙화하고 자동화합니다. DDNS 업데이트는 미리 정의된 간격에 따라 지정된 주소와 호스트 이름의 연결을 자동으로 기록합니다. DDNS는 주소-호스트 이름 연결의 잦은 변경 사항을 자주 업데이트하는 것을 허용합니다. 따라서 이를테면 모바일 호스트가 사용자 또는 관리자의 개입 없이 자유롭게 네트워크에서 이동할 수 있습니다. DDNS는 DNS 서버에서 필요한 이름-주소 매핑 및 주소-이름 매핑의 동적 업데이트와 동기화를 제공합니다.

DDNS 이름 및 주소 매핑은 DHCP 서버에서 2개의 RR(리소스 레코드)에 저장됩니다. A RR은 이름-IP 주소 매핑을 포함하는 반면 PTR RR은 이름에 주소를 매핑합니다. ASA는 DDNS 업데이트를 수행하는 2가지 메서드(RFC 2136에 의해 정의된 IETF 표준 및 일반 HTTP 메서드) 중에서 IETF 메서드를 지원합니다.

관련 주제

- 15-4 페이지의 DHCP 서버 구성

DDNS 업데이트 구성

가장 일반적인 DDNS 업데이트 컨피그레이션 2가지는 다음과 같습니다.

- DHCP 클라이언트가 A RR을 업데이트하고, DHCP 서버가 PTR RR을 업데이트합니다.
- DHCP 서버가 A RR과 PTR RR을 모두 업데이트합니다.

일반적으로 DHCP 서버가 클라이언트를 대신하여 DNS PTR RR을 유지 관리합니다. 클라이언트가 필요한 모든 DNS 업데이트를 수행하도록 구성할 수 있습니다. 서버가 이 업데이트를 인정하거나 인정하지 않도록 구성할 수 있습니다. DHCP 서버가 PTR RR을 업데이트하려면 클라이언트의 FQDN(정규화된 도메인 이름)을 알고 있어야 합니다. 클라이언트는 Client FQDN이라는 DHCP 옵션을 사용하여 서버에 FQDN을 제공합니다.

UDP 패킷 크기

DDNS는 DNS 요청자가 UDP 패킷의 크기를 알리는 것을 허용하며, 512옥텟보다 큰 패킷의 전송을 지원합니다. DNS 서버는 UDP를 통해 요청을 받으면, OPT RR로부터 UDP 패킷의 크기를 확인한 다음 요청자가 지정한 최대 UDP 패킷 크기의 허용 범위에서 최대한 많은 RR을 포함할 수 있도록 응답을 확장합니다. DNS 패킷의 최대 크기는 4096바이트(BIND) 또는 1280바이트(Windows 2003 DNS Server)입니다. 몇몇 추가 **message-length maximum** 명령을 사용할 수 있습니다.

- 기존 전역 한도: **message-length maximum 512**
- 클라이언트 또는 서버별 한도: **message-length maximum client 4096 및 message-length maximum server 4096**
- OPT RR 필드에 지정된 동적 값: **message-length maximum client auto**

3개의 명령이 동시에 있을 경우, ASA는 구성된 클라이언트 또는 서버의 최대 한도에서 자동 구성 길이를 허용합니다. 그 밖의 DNS 트래픽에서는 message-length maximum이 사용됩니다.

DDNS 지침

컨텍스트 모드 지침

DNS Client 창에서 투명 모드에서만 지원됩니다.

DDNS 구성

이 섹션에서는 DDNS 구성 방법을 설명합니다.

DDNS를 구성하고 DNS 서버를 업데이트하려면 다음 단계를 수행합니다.

절차

1단계 **Configuration > Device Management > DNS > Dynamic DNS**를 선택합니다.

2단계 **Add**를 클릭하여 **Add Dynamic DNS Update Method** 대화 상자를 표시합니다.

3단계 DDNS 업데이트 메서드의 이름을 입력합니다.

4단계 이 업데이트 메서드에 대해 구성된 DNS 업데이트 시도 간격을 일, 시간, 분, 초 단위로 지정합니다.

- 업데이트 시도 간격의 일수를 0~364에서 선택합니다.
- 업데이트 시도 간격의 시간(정수)을 0~23에서 선택합니다.
- 업데이트 시도 간격의 분(정수)을 0~59에서 선택합니다.
- 업데이트 시도 간격의 초(정수)를 0~59에서 선택합니다.

이 단위는 더해집니다. 즉 0일, 0시간, 5분, 15초를 입력한 경우, 업데이트 메서드가 활성 상태인 한 5분 15초마다 업데이트를 시도합니다.

5단계 DNS 클라이언트가 업데이트한 서버 RR 업데이트를 저장하려면 다음 옵션 중 하나를 선택합니다.

- A RR 및 PTR RR 모두
- A RR만

6단계 **OK**를 클릭하여 **Add Dynamic DNS Update Method** 대화 상자를 닫습니다.

새 DDNS 클라이언트 설정이 나타납니다.

참고 기존 메서드를 수정할 때 Name 필드는 *표시 전용*이며 수정하기 위해 선택한 메서드의 이름을 표시합니다.

7단계 **Add**를 클릭하여 **Add Dynamic DNS Interface Settings** 대화 상자를 표시하고 구성된 인터페이스별로 DDNS 설정을 추가할 수 있습니다.

8단계 드롭다운 목록에서 인터페이스를 선택합니다.

9단계 드롭다운 목록에서 해당 인터페이스에 지정된 업데이트 메서드를 선택합니다.

10단계 DDNS 클라이언트의 호스트 이름을 입력합니다.

11단계 RR 업데이트를 저장하기 위해 다음 옵션 중 하나를 선택합니다.

- Default (PTR Records) - 클라이언트가 서버의 PTR 레코드 업데이트를 요청합니다.
- Both (PTR Records and A Records) - 클라이언트가 서버의 A 및 PTR DNS RR 업데이트를 요청합니다.
- None - 클라이언트가 서버의 업데이트를 요청하지 않습니다.

참고 이 작업이 수행되려면 DHCP가 선택된 인터페이스에서 활성 상태여야 합니다.

12단계 **OK**를 클릭하여 **Add Dynamic DNS Interface Settings** 대화 상자를 닫습니다.

새 DDNS 인터페이스 설정이 나타납니다.

13단계 변경 사항을 저장하려면 **Apply**를, 변경 사항을 취소하고 새로 입력하려면 **Reset**을 클릭합니다.

DDNS 모니터링

DDNS 상태를 모니터링하려면 다음 화면을 참조하십시오.

- **Tools > Command Line Interface**

  이 창에서는 ASA에 비대화형 명령을 전송하고 그 결과를 표시합니다.

DDNS 기능 내역

표 16-1 DDNS 기능 내역

기능 이름	릴리스	기능 정보
DDNS	7.0(1)	이 기능을 도입했습니다. 다음 화면을 도입했습니다. Configuration > Device Management> DNS > DNS Client. Configuration > Device Management > DNS > Dynamic DNS

파 트 5

개체 및 ACL

17 장

액세스 제어용 객체

객체는 재사용 가능한 컨피그레이션 요소로서 컨피그레이션에 사용됩니다. Cisco ASA 컨피그레이션에서 인라인 IP 주소, 서비스, 이름 등을 대신하여 객체를 정의하고 사용할 수 있습니다. 객체로 편리하게 컨피그레이션을 유지 관리할 수 있습니다. 한군데서 객체를 수정한 다음 이를 참조하는 다른 모든 곳에 적용할 수 있기 때문입니다. 객체가 없으면 한 번이 아니라 필요할 때마다 각 기능의 매개 변수를 수정해야 합니다. 예를 들어, 네트워크 객체에서 IP 주소와 서브넷 마스크를 정의하는 경우에 주소를 변경하려면 주소를 참조하는 모든 기능이 아니라 객체 정의에서만 주소를 변경하면 됩니다.

객체 관련 지침

IPv6 지침

다음 제약 사항과 함께 IPv6를 지원합니다.

- ASA는 IPv6 중첩 네트워크 객체 그룹을 지원하지 않습니다. 따라서 IPv6 항목의 객체를 다른 IPv6 객체 그룹으로 묶을 수 없습니다.
- IPv4 항목과 IPv6 항목을 하나의 네트워크 객체 그룹에서 혼합할 수 있습니다. NAT에 대해서는 혼합 객체 그룹을 사용할 수 없습니다.

추가 지침 및 제한

- 객체는 고유한 이름을 가져야 합니다. 객체와 객체 그룹이 동일한 이름 공간을 공유하기 때문입니다. "Engineering"이라는 이름의 네트워크 객체 그룹과 역시 "Engineering"이라는 이름의 서비스 객체 그룹을 만들고 싶다면 적어도 하나의 객체 그룹 이름은 그 끝에 식별자(또는 "태그")를 추가하여 고유하게 만들어야 합니다. 이를테면 "Engineering_admins"와 "Engineering_hosts"를 사용하여 식별하기에 편리한 고유한 객체 이름 그룹으로 만들 수 있습니다.
- 객체 이름은 영숫자와 .!@#$%^&()-_{} 문자를 포함하여 64자까지 가능합니다. 객체 이름은 대소문자를 구분합니다.
- 명령에서 사용되는 객체는 제거하거나 비워 둘 수 없습니다. 단, (액세스 규칙 고급 설정에서) 을 사용하여) 전방 참조를 활성화한 경우는 제외합니다.

객체 구성

다음 섹션에서는 액세스 제어에서 주로 사용되는 객체를 구성하는 방법에 대해 설명합니다.

네트워크 객체 및 그룹 구성

네트워크 객체와 그룹은 IP 주소 또는 호스트 이름을 식별합니다. 액세스 제어 목록에서 이 객체를 사용하여 규칙을 간소화합니다.

네트워크 객체 구성

네트워크 객체는 호스트, 네트워크 IP 주소, IP 주소의 범위 또는 FQDN(정규화된 도메인 이름)을 포함할 수 있습니다.

또한 (FQDN 객체를 제외하고) 객체에 대해 NAT 규칙을 활성화할 수도 있습니다. 객체 NAT 구성에 대한 자세한 내용은 방화벽 컨피그레이션 가이드를 참조하십시오.

절차

1단계 **Configuration > Firewall > Objects > Network Objects/Group**을 선택합니다.

2단계 다음 중 하나를 수행합니다.

- 새 객체를 추가하기 위해 **Add > Network Object**를 선택합니다. 이름 및 필요하다면 설명을 입력합니다.
- 기존 객체를 선택하고 **Edit**를 클릭합니다.

3단계 객체 **Type** 및 **IP version** 필드를 기반으로 객체의 주소를 구성합니다.

- **Host**—단일 호스트의 IPv4 또는 IPv6 주소. 예를 들면 10.1.1.1 또는 2001:DB8::0DB8:800:200C:417A입니다.
- **Network**—네트워크의 주소. IPv4는 마스크를 포함합니다. 예를 들면, **IP address** = 10.0.0.0 **Netmask** = 255.0.0.0입니다. IPv6는 접두사를 포함합니다. 예를 들면, **IP Address** = 2001:DB8:0:CD30:: **Prefix Length** = 60입니다.
- **Range**—주소 범위. IPv4 또는 IPv6 범위를 지정할 수 있습니다. 마스크 또는 접두사를 포함하지 않습니다.
- **FQDN**—www.example.com과 같은 정규화된 도메인 이름, 즉 호스트의 이름입니다.

4단계 **OK**를 클릭하고 **Apply**를 클릭합니다.

이제 규칙을 만들 때 이 네트워크 객체를 사용할 수 있습니다. 객체를 수정하면 객체를 사용하는 모든 규칙에 변경 사항이 자동으로 상속됩니다.

네트워크 객체 그룹 구성

네트워크 객체 그룹에는 여러 네트워크 객체뿐 아니라 인라인 네트워크 또는 호스트도 포함될 수 있습니다. 네트워크 객체 그룹이 IPv4 주소와 IPv6 주소를 모두 포함할 수도 있습니다.

그러나 NAT를 위한 객체 그룹 또는 FQDN 객체를 포함하는 객체 그룹은 IPv4와 IPv6의 혼합이 불가합니다.

절차

1단계 **Configuration > Firewall > Objects > Network Objects/Groups**를 선택합니다.

2단계 다음 중 하나를 수행합니다.

- 새 객체 그룹을 추가하기 위해 **Add > Network Object Group**을 선택합니다. 이름 및 필요하다면 설명을 입력합니다.
- 기존 객체를 선택하고 **Edit**를 클릭합니다.

3단계 다음 방법의 조합을 통해 그룹에 네트워크 객체를 추가합니다.

- **Existing Network Objects/Groups**—이미 정의된 네트워크 객체 또는 그룹을 선택하고 **Add**를 클릭하여 그룹에 포함시킵니다.
- **Create New Network Object Member**—새 네트워크 객체에 대한 기준을 입력하고 **Add**를 클릭합니다. 객체에 이름을 지정할 경우, 변경 사항을 적용하면 새 객체가 생성되어 그룹에 추가됩니다. 호스트 또는 네트워크를 추가할 때는 이름이 선택 사항입니다.

4단계 모든 멤버 객체를 추가한 다음 **OK**를 클릭하고 **Apply**를 클릭합니다.

이제 규칙을 만들 때 이 네트워크 객체 그룹을 사용할 수 있습니다. 객체 그룹이 수정되면 객체 그룹을 사용하는 모든 규칙에 변경 사항이 자동으로 상속됩니다.

서비스 객체 및 서비스 그룹 구성

서비스 객체 및 그룹은 프로토콜과 포트를 식별합니다. 액세스 제어 목록에서 이 객체를 사용하여 규칙을 간소화합니다.

- 17-3 페이지의 서비스 객체 구성
- 17-4 페이지의 서비스 그룹 구성

서비스 객체 구성

서비스 객체는 단일 프로토콜, ICMP, ICMPv6, TCP, UDP 포트 또는 포트 범위를 포함할 수 있습니다.

절차

1단계 **Configuration > Firewall > Objects > Service Object/Group**을 선택합니다.

2단계 다음 중 하나를 수행합니다.

- 새 객체를 추가하기 위해 **Add > Service Object**를 선택합니다. 이름 및 필요하다면 설명을 입력합니다.
- 기존 객체를 선택하고 **Edit**를 클릭합니다.

3단계 서비스 유형을 선택하고 필요하다면 세부 사항을 입력합니다.

- Protocol—0-255 범위의 번호 또는 **ip**, **tcp**, **udp**, **gre** 등과 같이 잘 알려진 이름. 번호, 이름과 그 의미의 목록은 43-11 페이지의 프로토콜 및 애플리케이션를 참조하십시오.
- ICMP, ICMP6—어떤 ICMP/ICMP 버전 6 메시지와도 일치하도록 메시지 유형 및 코드 필드를 비워 둘 수 있습니다. 원한다면 이름 또는 번호(0-255)로 ICMP 유형을 지정하여 해당 메시지 유형으로 객체를 제한할 수 있습니다. 유형을 지정할 경우 그 유형(1-255)에 대한 ICMP 코드를 지정할 수 있습니다. 코드를 지정하지 않을 경우 모든 코드가 사용됩니다. ICMP 유형의 목록은 43-16 페이지의 ICMP 유형를 참조하십시오.
- TCP, UDP—원한다면 출발지, 목적지 또는 둘 다의 포트를 지정할 수 있습니다. 이름 또는 번호로 포트를 지정할 수 있습니다(목록은 43-12 페이지의 TCP 및 UDP 포트 참조). 다음 연산자를 포함할 수 있습니다.
  - <—보다 작음. 예: <80
  - >—보다 큼. 예: >80
  - **!=**—같지 않음. 예: !=80
  - **-**(하이픈)—경계를 포함하는 값의 범위. 예: 100-200

4단계 **OK**를 클릭하고 **Apply**를 클릭합니다.

서비스 그룹 구성

서비스 객체 그룹은 TCP 또는 UDP의 출발지/목적지 포트를 비롯하여 여러 프로토콜의 혼합을 포함할 수 있습니다.

시작하기 전에

여기서 설명하는 일반 서비스 객체 그룹을 사용하여 모든 서비스를 모델링할 수 있습니다. 그러나 ASA 8.3(1) 이전에 제공되었던 서비스 그룹 객체 유형도 여전히 구성 가능합니다. 이러한 레거시 객체로는 TCP/UDP/TCP-UDP 포트 그룹, 프로토콜 그룹, ICMP 그룹이 있습니다. 이 그룹의 내용은 일반 서비스 객체 그룹의 관련 컨피그레이션과 동일합니다. 단, ICMP 그룹은 ICMP6 또는 ICMP 코드를 지원하지 않습니다. 이 레거시 객체를 계속 사용하는 방법에 대한 자세한 지침은 Cisco.com에서 명령 참조의 **object-service** 명령에 대한 설명을 참조하십시오.

절차

1단계 **Configuration > Firewall > Objects > Service Objects/Groups**를 선택합니다.

2단계 다음 중 하나를 수행합니다.

- 새 객체를 추가하기 위해 **Add > Service Group**을 선택합니다. 이름 및 필요하다면 설명을 입력합니다.
- 기존 객체를 선택하고 **Edit**를 클릭합니다.

3단계 다음 방법의 조합을 통해 그룹에 서비스 객체를 추가합니다.

- **Existing Service Objects/Groups**—이미 정의된 서비스 객체 또는 그룹을 선택하고 **Add**를 클릭하여 그룹에 포함시킵니다.
- **Create New Service Object Member**—새 서비스 객체에 대한 기준을 입력하고 **Add**를 클릭합니다. 객체에 이름을 지정할 경우, 변경 사항을 적용하면 새 객체가 생성되어 그룹에 추가됩니다. 그렇지 않고 이름이 지정되지 않은 객체는 이 그룹의 멤버일 뿐입니다. TCP-UDP 객체에 이름을 지정할 수 없습니다. 이 객체는 그룹의 멤버일 뿐입니다.

4단계 모든 멤버 객체를 추가한 다음 **OK**를 클릭하고 **Apply**를 클릭합니다.

이제 규칙을 만들 때 이 서비스 객체 그룹을 사용할 수 있습니다. 객체 그룹이 수정되면 객체 그룹을 사용하는 모든 규칙에 변경 사항이 자동으로 상속됩니다.

로컬 사용자 그룹 구성

ID 방화벽을 지원하는 기능에서 사용할 로컬 사용자 그룹을 만들 수 있습니다. 확장 ACL에 이를 포함하는 방식이며, 그러면 확장 ACL은 액세스 규칙 등에 사용할 수 있습니다.

ASA는 Active Directory 도메인 컨트롤러에서 전역으로 정의된 사용자 그룹에 대한 LDAP 쿼리를 Active Directory 서버에 보냅니다. ASA에서는 ID 기반 규칙을 위해 이 그룹을 가져옵니다. 그러나 ASA에 로컬화된 네트워크 리소스가 있는 경우도 있습니다. 이러한 리소스는 전역으로 정의되지 않으며, 로컬화된 보안 정책에 따른 로컬 사용자 그룹을 필요로 합니다. 로컬 사용자 그룹은 중첩된 그룹 및 Active Directory에서 가져온 사용자 그룹을 포함할 수 있습니다. ASA에서는 로컬 그룹과 Active Directory 그룹을 통합합니다.

사용자는 로컬 사용자 그룹과 Active Directory에서 가져온 사용자 그룹에 속할 수 있습니다.

ACL에서 직접 사용자 이름과 사용자 그룹 이름을 사용할 수 있으므로, 다음과 같은 경우에만 로컬 사용자 그룹을 구성해야 합니다.

- LOCAL 데이터베이스에 정의된 사용자의 그룹을 만들려는 경우
- AD 서버에 정의된 단일 사용자 그룹에 속하지 않은 사용자 또는 사용자 그룹으로 하나의 그룹을 만들려 합니다.

ID 방화벽을 활성화하는 방법에 대한 자세한 내용은 32 장, “ID 방화벽”.를 참조하십시오.

절차

1단계 **Configuration > Firewall > Objects > Local User Groups**를 선택합니다.

2단계 다음 중 하나를 수행합니다.

- 새 객체를 추가하려면 **Add**를 선택합니다. 이름 및 필요하다면 설명을 입력합니다.
- 기존 객체를 선택하고 **Edit**를 클릭합니다.

3단계 다음 방법 중 하나를 사용하여 객체에 사용자 또는 그룹을 추가합니다.

- **기존 사용자 또는 그룹 선택**—사용자 또는 그룹이 속한 도메인을 선택한 다음 목록에서 해당 사용자 또는 그룹 이름을 선택하고 **Add**를 클릭합니다. 목록이 길 경우 Find 상자를 사용하여 사용자를 찾을 수 있습니다. 이 이름은 선택된 도메인의 서버에서 가져온 것입니다.
- **사용자 이름 직접 입력**—맨 아래 편집란에 사용자 또는 그룹 이름을 입력한 다음 **Add**를 클릭하면 됩니다. 이 방법을 사용하면 선택된 도메인 이름이 무시되며 지정하지 않은 경우에는 기본 도메인이 사용됩니다. 사용자는 *domain_name\username*; 형식이고, 그룹은 이중 \\를 사용하는 *domain_name\\group_name* 형식입니다.

4단계 모든 멤버 객체를 추가한 다음 **OK**를 클릭하고 **Apply**를 클릭합니다.

이제 규칙을 만들 때 이 사용자 객체 그룹을 사용할 수 있습니다. 객체 그룹이 수정되면 객체 그룹을 사용하는 모든 규칙에 변경 사항이 자동으로 상속됩니다.

보안 그룹 객체 그룹 구성

Cisco TrustSec를 지원하는 기능에서 사용할 보안 그룹 객체 그룹을 만들 수 있습니다. 확장 ACL에 이를 포함하는 방식이며, 그러면 확장 ACL은 액세스 규칙 등에 사용할 수 있습니다.

Cisco TrustSec와 통합할 경우 ASA는 ISE에서 보안 그룹 정보를 다운로드합니다. ISE는 Cisco TrustSec 태그-사용자 ID 매핑 및 Cisco 태그-사용자 리소스 매핑을 수행하면서 ID 저장소의 역할을 합니다. 중앙의 ISE에서 보안 그룹 ACL을 프로비저닝하고 관리합니다.

그러나 ASA에 로컬화된 네트워크 리소스가 있는 경우도 있습니다. 이러한 리소스는 전역으로 정의되지 않으며, 로컬화된 보안 정책에 따른 로컬 보안 그룹을 필요로 합니다. 로컬 보안 그룹은 ISE에서 다운로드한 중첩 보안 그룹을 포함할 수 있습니다. ASA는 로컬 및 중앙 보안 그룹을 통합합니다.

ASA에서 로컬 보안 그룹을 만들려면 로컬 보안 객체 그룹을 만듭니다. 로컬 보안 객체 그룹은 중첩 보안 객체 그룹, 보안 ID 또는 보안 그룹 이름을 하나 이상 포함할 수 있습니다. 또한 ASA에 없는 보안 ID 또는 보안 그룹 이름을 새로 만들 수도 있습니다.

ASA에서 만든 보안 객체 그룹을 사용하여 네트워크 리소스에 대한 액세스를 제어할 수 있습니다. 보안 객체 그룹을 액세스 그룹 또는 서비스 정책의 일부로 사용할 수 있습니다.

ASA를 Trustsec와 통합하는 방법에 대한 자세한 내용은 33 장, “ASA 및 Cisco TrustSec”.를 참조하십시오.

팁 ASA에 알려지지 않은 태그 또는 이름으로 그룹을 만들 경우, 그 그룹을 사용하는 어떤 규칙도 ISE에서 해당 태그 또는 이름을 확인할 때까지는 비활성 상태입니다.

절차

1단계 **Configuration > Firewall > Objects > Security Group Object Groups**를 선택합니다.

2단계 다음 중 하나를 수행합니다.

- 새 객체를 추가하려면 **Add**를 선택합니다. 이름 및 필요하다면 설명을 입력합니다.
- 기존 객체를 선택하고 **Edit**를 클릭합니다.

3단계 다음 방법 중 하나를 사용하여 객체에 보안 그룹을 추가합니다.

- **기존 로컬 보안 그룹 객체 그룹 선택**—이미 정의된 객체의 목록에서 선택하고 **Add**를 클릭합니다. 목록이 길 경우 Find 상자를 사용하여 객체를 찾을 수 있습니다.
- **ISE에서 검색한 보안 그룹 선택**—기존 그룹의 목록에서 그룹을 선택하고 **Add**를 클릭합니다.
- **보안 태그 또는 이름 직접 추가**—맨 아래의 편집란에 태그 번호 또는 보안 그룹 이름을 입력하고 **Add**를 클릭하면 됩니다. 태그는 1 ~ 65533의 번호이며 ISE에서 IEEE 802.1X 인증, 웹 인증 또는 MAB(MAC 인증 우회)를 통해 디바이스에 할당됩니다. 보안 그룹 이름은 ISE에서 만들어지며, 보안 그룹을 위해 사용하기 편리한 이름을 제공합니다. 보안 그룹 테이블은 SGT를 보안 그룹 이름에 매핑합니다. 유효한 태그 및 이름에 대해서는 ISE 컨피그레이션을 참조합니다.

4단계 모든 멤버 객체를 추가한 다음 **OK**를 클릭하고 **Apply**를 클릭합니다.

이제 규칙을 만들 때 이 보안 그룹 객체 그룹을 사용할 수 있습니다. 객체 그룹이 수정되면 객체 그룹을 사용하는 모든 규칙에 변경 사항이 자동으로 상속됩니다.

시간 범위 구성

시간 범위 객체는 특정 시간을 정의하며 시작 시간, 종료 시간, 선택 사항인 반복 항목으로 구성됩니다. ACL 규칙에서 이 객체를 사용하여 특정 기능 또는 자산에 대한 시간 기반 액세스를 제공합니다. 예를 들어, 업무 시간에만 특정 서버에 대한 액세스를 허용하는 액세스 규칙을 만들 수 있습니다.

참고 시간 범위 객체에 여러 기간 항목을 포함할 수 있습니다. 시간 범위에 절대값과 기간 값이 모두 지정된 경우, 절대 시작 시간에 도달해야 기간 값의 평가가 이루어지며 절대 종료 시간에 도달하면 더 이상 평가되지 않습니다.

시간 범위를 만들더라도 디바이스에 대한 액세스가 제한되지 않습니다. 이 절차에서는 시간 범위만 정의합니다. 그런 다음 액세스 제어 규칙에서 이 객체를 사용해야 합니다.

절차

1단계 **Configuration > Firewall > Objects > Time Ranges**를 선택합니다.

2단계 다음 중 하나를 수행합니다.

- 새 시간 범위를 추가하기 위해 **Add**를 선택합니다. 이름 및 필요하다면 설명을 입력합니다.
- 기존 시간 범위를 선택하고 **Edit**를 클릭합니다.

3단계 전체 시작 시간과 종료 시간을 선택합니다.

기본값은 지금 시작하고 영원히 끝나지 않는 것이지만, 특정 날짜와 시간을 설정할 수 있습니다. 시간 범위는 사용자가 입력하는 시간을 포함합니다.

4단계 (선택 사항) 전체 활성 시간 내에서 반복 기간을 구성합니다. 이를테면 시간 범위가 활성 상태가 되는 요일 또는 반복되는 주 간격입니다.

a. **Add**를 클릭하거나 기존 기간을 선택하고 **Edit**를 클릭합니다.

b. 다음 중 하나를 수행합니다.

- **Specify days of the week and times on which this recurring range will be active**를 클릭하고 목록에서 일과 시간을 선택합니다.
- **Specify a weekly interval when this recurring range will be active**를 클릭하고 목록에서 일과 시간을 선택합니다.

c. **OK**를 클릭합니다.

5단계 **OK**를 클릭하고 **Apply**를 클릭합니다.

객체 모니터링

네트워크, 서비스, 보안 그룹 객체는 개별 객체의 사용을 분석할 수 있습니다. **Configuration > Firewall > Objects** 폴더의 해당 페이지에서 **Where Used** 버튼을 클릭합니다.

네트워크 객체의 경우 Not Used 버튼을 클릭하여 어떤 규칙 또는 다른 객체에서 사용되지 않는 객체를 찾을 수도 있습니다. 이 화면에서는 이 미사용 객체를 삭제할 수 있는 바로가기를 제공합니다.

객체 관련 이력

기능 이름	플랫폼 릴리스	설명
객체 그룹	7.0(1)	객체 그룹으로 간단하게 ACL을 만들고 유지 관리할 수 있습니다.
정규식 및 정책 맵	7.2(1)	검사 정책 맵에서 사용하기 위해 정규식과 정책 맵을 도입했습니다. **class-map type regex**, **regex**, **match regex** 명령을 도입했습니다.
객체	8.3(1)	객체 지원을 도입했습니다.
ID 방화벽을 위한 사용자 객체 그룹	8.4(2)	ID 방화벽을 위한 사용자 객체 그룹을 도입했습니다.
Cisco TrustSec를 위한 보안 그룹 객체 그룹	8.4(2)	Cisco TrustSec를 위한 보안 그룹 객체 그룹을 도입했습니다.
IPv4/IPv6 혼합 네트워크 객체 그룹	9.0(1)	이전에는 네트워크 객체 그룹이 IPv4 주소만 또는 IPv6 주소만 포함할 수 있었습니다. 이제는 네트워크 객체 그룹에서 IPv4 주소와 IPv6 주소의 혼합을 지원합니다. **참고** NAT에는 혼합 객체 그룹을 사용할 수 없습니다.
확장 ACL 및 ICMP 코드를 기준으로 ICMP 트래픽을 필터링하기 위한 객체 개선 사항	9.0(1)	이제 ICMP 코드에 따라 ICMP 트래픽을 허용하거나 거부할 수 있습니다. 다음 화면을 도입했거나 수정했습니다. Configuration > Firewall > Objects > Service Objects/Groups Configuration > Firewall > Access Rule

18 장

액세스 제어 목록

ACL(액세스 제어 목록)은 다양한 기능에서 사용합니다. 인터페이스에 적용되거나 전역 범위에 액세스 규칙으로 적용되는 ACL은 어플라이언스를 지나는 트래픽을 허용하거나 거부합니다. 다른 기능에서는 해당 기능이 적용될 트래픽을 선택하면서 제어 서비스보다는 매칭 서비스를 수행합니다.

다음 섹션에서는 ACL의 기초와 ACL을 구성하고 모니터링할 방법을 설명합니다. 전역 범위에 또는 인터페이스에 적용되는 ACL인 액세스 규칙은 방화벽 컨피그레이션 가이드에서 자세히 설명합니다.

ACL 소개

ACL은 ACL 유형에 따라 소스 및 수신 IP 주소, IP 프로토콜, 포트, 이더 타입, 기타 매개 변수 등 하나 이상의 특성을 기준으로 삼아 트래픽 흐름을 식별합니다. ACL은 다양한 기능에서 사용됩니다. ACL은 하나 이상의 ACE(액세스 제어 항목)로 구성됩니다.

ACL 유형

ASA에서는 다음 유형의 ACL을 사용합니다.

- 확장 ACL—확장 ACL이 주요 사용할 유형입니다. 이 ACL은 해당 디바이스를 거치는 트래픽을 허용하거나 거부하는 액세스 규칙에 그리고 서비스 정책, AAA 정책, WCCP, 봇넷 트래픽 필터, VPN 그룹, DAP 정책과 같은 여러 기능에서 트래픽 매칭에 사용됩니다. ASDM에서는 이러한 기능 중 상당수가 각자 규칙 페이지가 있으며, ACL Manager에서 정의하는 확장 ACL을 사용할 수 없습니다. 하지만 ACL Manager는 그러한 페이지에 ACL을 표시합니다. 18-6 페이지의 확장 ACL 구성를 참조하십시오.
- 이더 타입 ACL—이더 타입 ACL은 투명 방화벽 모드에서 비 IP 레이어 2 트래픽에 적용됩니다. 레이어 2 트래픽의 이더 타입 값에 따라 트래픽을 허용하거나 거부하는 데 이 규칙을 사용할 수 있습니다. 이더 타입 ACL을 사용하면 해당 디바이스를 지나는 비 IP 트래픽의 흐름을 제어할 수 있습니다. 방화벽 컨피그레이션 가이드의 액세스 규칙 장을 참조하십시오.

- 웹 타입 ACL—웹 타입 ACL은 클라이언트리스 SSL VPN 트래픽을 필터링하는 데 사용됩니다. 이 ACL은 URL 또는 목적지 주소에 따라 액세스를 거부할 수 있습니다. 18-10 페이지의 웹 타입 ACL 구성를 참조하십시오.
- 표준 ACL—표준 ACL은 목적지 주소만으로 트래픽을 식별합니다. 경로 맵, VPN 필터와 같은 몇몇 기능에서만 이를 사용합니다. VPN 필터는 확장 액세스 목록도 지원하므로, 표준 ACL 사용은 경로 맵에 한정됩니다. 18-9 페이지의 표준 ACL 구성를 참조하십시오.

다음 표는 대표적인 ACL의 용도 및 사용되는 유형을 정리한 것입니다.

표 18-1 ACL 유형 및 대표적인 용도

ACL 용도	ACL 유형	설명
IP 트래픽의 네트워크 액세스 제어 (라우팅 및 투명 모드)	확장	ASA에서는 확장 ACL에서 명시적으로 허용하지 않는 한 어떤 트래픽도 하위 보안 인터페이스에서 상위 보안 인터페이스로 이동할 수 없습니다. **참고** 관리 액세스를 위해 ASA 인터페이스에 액세스하는 경우에도 ACL에서 호스트 IP 주소를 허용할 필요 없습니다. 36 장, "관리 액세스".에 따라 관리 액세스를 구성하면 됩니다.
AAA 규칙을 위한 트래픽 식별	확장	AAA 규칙에서는 트래픽 식별에 ACL을 사용합니다.
특정 사용자를 위해 IP 트래픽에 대한 네트워크 액세스 제어 보완	확장, 사용자별 AAA 서버에서 다운로드	사용자에게 적용할 동적 ACL을 다운로드하도록 RADIUS 서버를 구성할 수 있습니다. 또는 서버가 이미 ASA에서 구성된 ACL의 이름을 전송할 수 있습니다.
VPN 액세스 및 필터링	확장 표준	원격 액세스 및 사이트 대 사이트 VPN을 위한 그룹 정책은 필터링에 표준 또는 확장 ACL을 사용합니다. 원격 액세스 VPN은 클라이언트 방화벽 컨피그레이션 및 동적 액세스 정책에도 확장 ACL을 사용합니다.
Modular Policy Framework를 위한 트래픽 클래스 맵에서 트래픽 식별	확장	Modular Policy Framework를 지원하는 기능에 쓰이는 클래스 맵에서 트래픽을 식별하는 데 ACL을 사용할 수 있습니다. Modular Policy Framework를 지원하는 기능으로는 TCP 및 일반 연결 설정, 검사 등이 있습니다.
투명 방화벽 모드에서 비 IP 트래픽을 위한 네트워크 액세스 제어	이더 타입	이더 타입에 따라 트래픽을 제어하는 ACL을 구성할 수 있습니다.
경로 필터링 및 재배포 식별	표준 확장	다양한 라우팅 프로토콜에서 (경로 맵을 통한) IPv4 주소의 경로 필터링 및 재배포에 표준 ACL을, IPv6에는 확장 ACL을 사용합니다.
클라이언트리스 SSL VPN의 필터링	웹 타입	웹 타입 ACL에서 URL 및 목적지를 필터링하도록 구성할 수 있습니다.

ACL Manager

ACL Manager는 2가지 형태로 나타납니다.

- 예를 들어, 기본 창에서 **Configuration > Firewall > Advanced > ACL Manager**를 선택합니다. 이 경우에는 ACL Manager가 확장 ACL만 표시합니다. 여기에는 Access Rules, Service Policy Rules, AAA Rules 페이지에서 만든 규칙에 의해 생성된 ACL이 포함됩니다. ACL Manager에서 수정한 사항이 이 규칙에 불리하게 작용하지 않도록 주의합니다. 여기서 변경한 내용은 다른 페이지에도 반영됩니다.

- ACL이 필요한 정책에서 필드 옆의 **Manage** 버튼을 클릭합니다. 이 경우에는 ACL Manager에 표준 ACL 탭과 확장 ACL 탭이 각각 있을 수 있습니다. 단 정책에서 두 유형 각각을 허용해야 합니다. 그러지 않으면 보기는 확장 ACL 또는 웹 타입 ACL만 표시하도록 필터링됩니다. ACL Manager에서는 이더 타입 ACL을 표시하지 않습니다.

표준 ACL 및 웹 타입 ACL을 위한 별도의 페이지가 있으므로 기본 창에서 구성할 수 있습니다. 이 페이지는 기능상으로는 이름 없는 ACL Manager와 같습니다.

- 표준 ACL—**Configuration > Firewall > Advanced > Standard ACL**.
- 웹 타입 ACL—**Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**.

ACL 이름

각 ACL에는 이름 또는 숫자로 된 ID(예: outside_in, OUTSIDE_IN, 101)가 있습니다. 이름은 241자 이하여야 합니다. 모두 대문자를 사용하면 실행 중인 컨피그레이션을 볼 때 더 쉽게 이름을 찾을 수 있습니다.

ACL의 목적을 쉽게 이해할 수 있는 명명 규칙을 개발합니다. 예를 들어, ASDM에서는 *interface-name_purpose_direction* 규칙을 사용합니다. 이를테면 인바운드 방향에서 "외부" 인터페이스에 적용되는 ACL의 이름은 “outside_access_in”입니다.

예전에는 ACL ID가 숫자였습니다. 표준 ACL은 1-99 또는 1300-1999 범위였습니다. 확장 ACL은 100-199 또는 2000-2699 범위였습니다. ASA에서는 이러한 범위를 강제적으로 적용하지 않지만, 숫자를 사용하려는 경우 IOS Software를 실행하는 라우터에서 일관성을 유지하기 위해 이러한 규칙을 준수할 수 있습니다.

액세스 제어 입력 순서

ACL은 하나 이상의 ACE로 구성됩니다. 어떤 라인에 명시적으로 ACE를 삽입하지 않는 한, 어떤 ACL 이름에 대해 입력하는 ACE 각각은 ACL의 끝에 추가됩니다.

ACE의 순서는 중요합니다. ASA에서 패킷을 전달할지 폐기할지 결정할 때 ASA는 각 ACE에 대해, 각 항목이 나열된 순서에 따라 패킷을 테스트합니다. 일치하는 항목을 찾으면 더 이상 ACE를 검사하지 않습니다.

따라서 더 일반적인 규칙 다음에 더 구체적인 규칙을 배치할 경우 이 구체적인 규칙이 전혀 적용되지 않을 수 있습니다. 예를 들어, 네트워크 10.1.1.0/24를 허용하되 그 서브넷에서 호스트 10.1.1.15의 트래픽을 폐기하려는 경우 10.1.1.15를 거부하는 ACE가 10.1.1.0/24를 허용하는 ACE의 앞에 와야 합니다. 10.1.1.0/24를 허용하는 ACE가 맨 앞에 올 경우 10.1.1.15가 허용되며, 거부 ACE에 대한 매칭은 이루어지지 않습니다.

필요에 따라 상/하 버튼을 사용하여 규칙의 위치를 조정합니다.

허용/거부와 매칭/매칭하지 않음

액세스 제어 항목은 규칙에 매칭하는 트래픽을 "허용"하거나 "거부"합니다. 트래픽이 ASA에서 허용될지 또는 폐기될지 결정하는 기능(예: 전역 및 인터페이스 액세스 규칙)에 ACL을 적용할 경우 "허용"과 "거부"는 본래의 의미가 있습니다.

서비스 정책 규칙과 같은 다른 기능에서는 "허용"과 "거부"가 사실상 "매칭" 또는 "매칭하지 않음"을 의미합니다. 그러한 경우 ACL은 해당 기능의 서비스(예: 애플리케이션 검사, 서비스 모듈로 리디렉션)을 받을 트래픽을 선택하게 됩니다. "거부된" 트래픽은 ACL에 매칭하지 않아 서비스를 받지 못할 트래픽일 뿐입니다. ASDM에서는 서비스 정책 규칙에서 매칭/매칭하지 않음을, AAA 규칙은 인증/인증하지 않음을 사용하지만, CLI에서는 항상 허용/거부입니다.

액세스 제어 암시적 거부

모든 ACL은 그 끝에 암시적 거부 문이 있습니다. 즉 인터페이스에 적용되는 것과 같은 트래픽 제어 ACL에서는 어떤 트래픽 유형을 명시적으로 허용하지 않으면 해당 트래픽이 폐기됩니다. 예를 들어, 모든 사용자가 하나 이상의 특정 주소를 제외하고 ASA를 통해 네트워크에 액세스하는 것을 허용하려는 경우 그 특정 주소를 거부하고 나머지 모든 주소를 허용해야 합니다.

어떤 서비스에 대한 트래픽을 선택하는 데 쓰이는 ACL에서는 그 트래픽을 명시적으로 "허용"해야 합니다. "허용"되지 않은 모든 트래픽은 해당 서비스에 매칭하지 않습니다. "거부"된 트래픽은 그 서비스를 우회합니다.

이더 타입 ACL에서는 ACL 끝의 암시적 거부가 IP 트래픽 또는 ARP에 영향을 주지 않습니다. 예를 들어, 이더 타입 8037을 허용할 경우 ACL 끝의 암시적 거부는 앞서 확장 ACL로 허용했던 (또는 상위 보안 인터페이스에서 하위 보안 인터페이스에 암시적으로 허용했던) 어떤 IP 트래픽도 차단하지 않습니다. 그러나 어떤 이더 타입 ACE로 모든 트래픽을 *명시적으로* 거부할 경우, IP 및 ARP 트래픽이 거부됩니다. 자동 협상과 같은 물리적 프로토콜 트래픽만 계속 허용됩니다.

NAT 사용 시 확장 ACL에 쓰이는 IP 주소

NAT 또는 PAT를 사용할 때 주소 또는 포트를 변환하는데, 주로 내부 주소와 외부 주소를 매핑합니다. 변환된 주소 또는 포트에 적용되는 확장 ACL을 만들어야 할 경우 실제 (변환되지 않은) 주소나 포트 또는 매핑된 것을 사용할지 결정해야 합니다. 요구 사항은 기능에 따라 달라집니다.

실제 주소와 포트를 사용할 경우 NAT 컨피그레이션이 바뀌더라도 ACL을 변경할 필요 없습니다.

실제 IP 주소를 사용하는 기능

다음 명령과 기능에서는 ACL에 실제 IP 주소를 사용합니다. 인터페이스에 나타나는 주소가 매핑된 주소인 경우에도 그렇습니다.

- 액세스 규칙(**access-group** 명령에서 참조하는 확장 ACL)
- 서비스 정책 규칙(Modular Policy Framework의 **match access-list** 명령)
- 봇넷 트래픽 필터의 트래픽 분류(**dynamic-filter enable classify-list** 명령)
- AAA 규칙(**aaa ... match** 명령)
- WCCP(**wccp redirect-list group-list** 명령)

이를테면 내부 서버 10.1.1.5가 외부에서 공개적으로 라우팅 가능한 IP 주소 209.165.201.5를 갖도록 NAT를 구성할 경우, 외부 트래픽이 내부 서버에 액세스하는 것을 허용하는 액세스 규칙은 서버의 매핑된 주소(209.165.201.5)가 아니라 실제 IP 주소(10.1.1.5)를 참조해야 합니다.

매핑된 IP 주소를 사용하는 기능

다음 기능에서 ACL을 사용하는데, 이 ACL에서는 인터페이스에 나타나는 매핑된 값을 사용합니다.

- IPsec ACL
- **capture** 명령 ACL
- 사용자별 ACL
- 라우팅 프로토콜 ACL
- 다른 모든 기능의 ACL

시간 기준 ACE

특정 기간에만 규칙을 활성화하기 위해 확장 ACE 및 웹 타입 ACE에 시간 범위 객체를 적용할 수 있습니다. 이러한 유형의 규칙을 통해 하루 중 특정 시간에만 허용되고 그 밖의 시간에는 허용되지 않는 활동을 구별할 수 있습니다. 예를 들어, 근무 시간에 추가적인 제한을 적용하되 근무 시간 이후 또는 점심시간에는 해제할 수 있습니다. 그와 반대로 근무 시간이 아닐 때 사실상 네트워크를 종료할 수도 있습니다. 시간 범위 객체 생성에 대한 자세한 내용은 17-7 페이지의 시간 범위 구성를 참조하십시오.

참고 지정된 종료 시간이 지나고 약 80초~100초 정도 사용자가 지연을 경험한 후 ACL이 비활성화될 수도 있습니다. 예를 들어, 지정된 종료 시간이 3:50이라면 이 종료 시간이 범위에 포함되므로 3:51:00~3:51:59의 어느 시점에서 명령이 실행됩니다. 명령이 실행되면 ASA에서는 현재 실행 중인 모든 작업을 종료한 다음 명령에 따라 ACL을 비활성화합니다.

ACL 지침

방화벽 모드 지침

확장 ACL과 표준 ACL은 라우팅 및 투명 방화벽 모드에서 지원됩니다.

웹 타입 ACL은 라우팅 모드에서만 지원됩니다.

이더 타입 ACL은 투명 모드에서만 지원됩니다.

IPv6 지침

확장 ACL과 웹 타입 ACL은 IPv4 주소와 IPv6 주소의 혼합을 허용합니다.

표준 ACL에서는 IPv6 주소를 허용하지 않습니다.

이더 타입 ACL은 IP 주소를 포함하지 않습니다.

(확장 ACL만) ID 방화벽, FQDN, Cisco TrustSec ACL을 지원하지 않는 기능

다음 기능에서는 ACL을 사용하지만 ID 방화벽(사용자 또는 그룹 이름 지정), FQDN(정규화된 도메인 이름) 또는 Cisco TrustSec 값을 갖는 ACL을 허용할 수 없습니다.

- **route-map** 명령
- VPN **crypto map** 명령
- VPN **group-policy** 명령(**vpn-filter** 제외)
- WCCP
- DAP

추가 지침 및 제한

- 네트워크 마스크를 지정할 때의 방식은 Cisco IOS 소프트웨어 **access-list** 명령과 다릅니다. ASA에서는 네트워크 마스크(예: 클래스 C 마스크는 255.255.255.0)를 사용합니다. Cisco IOS 마스크는 와일드카드 비트(예: 0.0.0.255)를 사용합니다.

ACL 구성

다음 섹션에서는 일반 ACL의 다양한 유형을 구성하는 방법을 설명합니다. 단, (이더 타입을 비롯하여) 액세스 규칙, 서비스 정책 규칙, AAA 규칙으로 사용되는 ACL 및 ASDM이 규칙 기준 정책을 위한 특별 페이지를 제공하는 기타 용도의 ACL은 제외합니다. 이 기타 용도를 위해 규칙을 구성하는 방법에 대해서는 방화벽 컨피그레이션 가이드를 참조하십시오.

- 18-6 페이지의 확장 ACL 구성
- 18-9 페이지의 표준 ACL 구성
- 18-10 페이지의 웹 타입 ACL 구성

확장 ACL 구성

확장 ACL은 명명된 ACE 컨테이너로 나타납니다. 새 ACL을 만들려면 먼저 컨테이너를 생성해야 합니다. 그런 다음 ACE를 추가하고 기존 ACE를 수정하고 ACL Manager의 테이블을 사용하여 ACE를 재정렬할 수 있습니다.

확장 ACL은 IPv4 주소와 IPv6 주소를 혼합하여 사용할 수 있습니다.

절차

1단계 **Configuration > Firewall > Advanced > ACL Manager**를 선택합니다.

2단계 새 ACL을 만드는 경우 **Add > Add ACL**을 선택하고 이름을 입력하고 **OK**를 클릭합니다.

ACL 컨테이너가 테이블에 추가됩니다. 나중에 이를 선택하고 **Edit**를 클릭하여 이름을 바꿀 수 있습니다.

3단계 다음 중 하나를 수행합니다.

- ACL의 끝에 ACE를 추가하려면 ACL 이름 또는 그 안의 ACE를 선택하고 **Add > Add ACE**를 선택합니다.
- 특정 위치에 ACE를 삽입하려면 기존 ACE를 선택하고 **Add > Insert**를 선택하여 그 규칙 위에 ACE를 추가하거나 **Add > Insert After**를 선택합니다.
- 규칙을 수정하려면 선택하고 **Edit**를 클릭합니다.

4단계 ACE 속성을 채웁니다. 기본 선택 옵션은 다음과 같습니다.

- **Action: Permit/Deny**—설명된 트래픽을 허용하는지(선택) 또는 거부하는지(선택 취소, 매칭하지 않음) 여부.
- **Source/Destination criteria**—소스(시작 주소) 및 목적지(트래픽 흐름의 대상 주소) 정의. 일반적으로 호스트나 서브넷의 IPv4 또는 IPv6 주소를 구성하는데, 이는 네트워크 또는 네트워크 객체 그룹으로 나타낼 수 있습니다. 소스에 대해 사용자 또는 사용자 그룹 이름을 지정할 수도 있습니다. 또한 전체 IP 트래픽보다 더 한정된 범위에서 규칙을 적용하려는 경우, Service 필드를 사용하여 특정 트래픽 유형을 지정할 수 있습니다. Cisco TrustSec을 구현할 경우 보안 그룹을 사용하여 소스와 목적지를 정의할 수 있습니다.

이용 가능한 모든 옵션에 대한 자세한 내용은 18-7 페이지의 확장 ACE 속성를 참조하십시오.

ACE 정의를 완료하면 **OK**를 클릭하여 테이블에 규칙을 추가합니다.

5단계 **Apply**를 클릭합니다.

확장 ACE 속성

확장 ACL의 ACE를 추가하거나 수정할 때 다음 속성을 구성할 수 있습니다. 많은 필드에서 편집 상자의 오른쪽에 있는 "..." 버튼을 클릭하여 필드에 사용 가능한 객체를 선택, 생성하거나 수정할 수 있습니다.

- **Action: Permit/Deny**—설명된 트래픽을 허용하는지(선택) 또는 거부하는지(선택 취소, 매칭하지 않음) 여부.
- **Source Criteria**—규칙에 매칭할 트래픽을 보낸 발신자의 특성. Source는 필수 구성 항목이지만, 나머지 속성은 선택 사항입니다.
  - **Source**—소스의 IPv4 또는 IPv6 주소. 기본값은 **any**이며, 이는 모든 IPv4 또는 IPv6 주소에 매칭합니다. **any4**를 사용하여 IPv4만 또는 **any6**를 사용하여 IPv6만 대상으로 할 수 있습니다. 단일 호스트 주소(예: 10.100.10.5 또는 2001:DB8::0DB8:800:200C:417A), 서브넷(10.100.10.0/24 또는 10.100.10.0/255.255.255.0 형식, IPv6는 2001:DB8:0:CD30::/60 형식), 네트워크 객체 또는 네트워크 객체 그룹의 이름, 인터페이스의 이름을 지정할 수 있습니다.
  - **User**—ID 방화벽을 활성화할 경우 어떤 사용자 또는 사용자 그룹을 트래픽 소스로 지정할 수 있습니다. 사용자가 현재 사용 중인 IP 주소가 규칙에 매칭하게 됩니다. 사용자 이름(DOMAIN\user), 사용자 그룹(DOMAIN\\group, 이중 \은 그룹 이름임을 의미) 또는 사용자 객체 그룹을 지정할 수 있습니다. 이 필드에서는 "**...**"을 클릭하여 AAA 서버 그룹에서 이름을 선택하는 것이 직접 입력하는 것보다 훨씬 편리합니다.
  - **Security Group**—Cisco TrustSec을 활성화할 경우 보안 그룹 이름이나 태그(1-65533) 또는 보안 그룹 객체를 지정할 수 있습니다.
  - **More Options > Source Service**—TCP 또는 UDP를 목적지 서비스로 지정할 경우, 원한다면 TCP, UDP 또는 TCP-UDP에 대해 미리 정의된 서비스 객체를 지정하거나 사용자 고유 객체를 사용할 수도 있습니다. 일반적으로 소스 서비스가 아닌 목적지 서비스만 정의합니다. 소스 서비스를 정의할 경우 목적지 서비스 프로토콜이 그에 매칭해야 합니다. 이를테면 둘 다 TCP이고 포트 정의를 포함하거나 포함하지 않을 수 있습니다.
- **Destination Criteria**—매칭할 트래픽을 받을 대상의 특성. Destination는 필수 구성 항목이지만, 나머지 속성은 선택 사항입니다.
  - **Destination**—목적지의 IPv4 또는 IPv6 주소. 기본값은 **any**이며, 이는 모든 IPv4 또는 IPv6 주소에 매칭합니다. **any4**를 사용하여 IPv4만 또는 **any6**를 사용하여 IPv6만 대상으로 할 수 있습니다. 단일 호스트 주소(예: 10.100.10.5 또는 2001:DB8::0DB8:800:200C:417A), 서브넷(10.100.10.0/24 또는 10.100.10.0/255.255.255.0 형식, IPv6는 2001:DB8:0:CD30::/60 형식), 네트워크 객체 또는 네트워크 객체 그룹의 이름, 인터페이스의 이름을 지정할 수 있습니다.
  - **Security Group**—Cisco TrustSec을 활성화할 경우 보안 그룹 이름이나 태그(1-65533) 또는 보안 그룹 객체를 지정할 수 있습니다.
  - **Service**—트래픽의 프로토콜(예: IP, TCP, UDP)과 (선택 사항으로) TCP 및 UDP 포트. 기본값은 IP이지만, 더 세밀하게 트래픽 대상을 지정하기 위해 더 구체적인 프로토콜을 선택할 수도 있습니다. 일반적으로 몇몇 유형의 서비스 객체를 선택합니다. TCP 및 UDP에서는 포트를 지정합니다. 이를테면 tcp/80, tcp/http, tcp/10-20(포트 범위), tcp-udp/80(포트 80에서 임의의 TCP 또는 UDP 트래픽 매칭) 등입니다. 서비스 지정에 대한 자세한 내용은 18-8 페이지의 확장 ACE의 서비스 사양를 참조하십시오.

- **Description**—ACE의 목적에 대한 설명이며, 라인당 최대 100자입니다. 여러 라인을 입력할 수 있습니다. 각 라인은 CLI에서 설명으로 추가되며, 이 설명이 ACE의 앞에 위치합니다.

  참고 어떤 플랫폼(예: Windows)에서 영어가 아닌 문자로 설명을 추가한 다음 다른 플랫폼(예: Linux)에서 그 설명을 삭제하려는 경우, 수정 또는 삭제가 불가능할 수 있습니다. 원래의 문자가 제대로 인식되지 않을 가능성이 있기 때문입니다. 이러한 제약은 다른 언어의 문자를 각기 다르게 인코딩하는 기본 플랫폼의 종속성 때문입니다.

- **Enable Logging**; **Logging Level**; **More Options > Logging Interval**—로깅 옵션은 규칙에 대해 syslog 메시지가 생성되는 방식을 정의합니다. 다음 로깅 옵션을 구현할 수 있습니다.
  - **Deselect Enable Logging**—규칙에 대한 로깅을 비활성화합니다. 이 규칙에 매칭하는 트래픽에 대해서는 어떤 유형의 syslog 메시지도 표시되지 않습니다.
  - **Select Enable Logging with Logging Level = Default**—규칙에 대한 기본 로깅을 제공합니다. 거부된 패킷 각각에 대해 syslog 메시지 106023이 표시됩니다. 어플라이언스가 공격을 받은 경우 이 메시지가 표시되는 빈도가 서비스에 영향을 미칠 수 있습니다.
  - **Select Enable Logging with Non-Default Logging Level**—요약된 syslog 메시지, 즉 106023이 아닌 106100이 제공됩니다. 메시지 106100은 처음 적중했을 때 표시되고, 그 다음에는 **More Options > Logging Interval**에 구성된 간격(기본값은 300초마다, 1-600에서 지정 가능)에 따라 다시 표시되면서 해당 간격의 적중 횟수를 표시합니다. 권장되는 로깅 레벨은 **Informational**입니다.

    거부 메시지를 요약하면 공격의 영향을 줄일 수 있으며, 메시지 분석이 더 수월해질 수도 있습니다. 서비스 거부 공격을 받을 경우 메시지 106101이 표시될 수 있습니다. 이는 메시지 106100을 위해 적중 횟수를 생성하는 데 사용된 캐시에 저장된 거부 흐름의 수가 간격의 최대값을 초과했음을 의미합니다. 이 시점이 되면 다음 간격이 도래할 때까지 어플라이언스가 공격 완화를 위한 통계 수집을 중지합니다.
- **More Options > Enable Rule**—규칙이 디바이스에서 활성화될지 여부. 비활성화된 규칙은 규칙 테이블에 지우기 선이 그려진 텍스트로 나타납니다. 규칙을 비활성화하면 삭제하지 않고도 트래픽에 대한 적용을 중지할 수 있습니다. 즉 나중에 필요해질 경우 다시 활성화하면 됩니다.
- **More Options > Time Range**—규칙이 활성화되는 요일과 시간대를 정의하는 시간 범위 객체의 이름. 시간 범위를 지정하지 않을 경우 규칙은 항상 활성 상태입니다.

확장 ACE의 서비스 사양

확장 ACE의 목적지 서비스에서는 다음 기준 중 무엇이든 지정할 수 있습니다. 소스 서비스의 경우 옵션이 비슷하지만 더 제한적입니다. 즉 TCP, UDP 또는 TCP-UDP 기준으로 한정됩니다.

- Object name—서비스 객체 또는 서비스 객체 그룹 유형의 이름. 이 객체는 아래에 설명된 사양 중 상당수를 포함할 수 있으므로 ACL 간에 손쉽게 서비스 정의를 재사용할 수 있습니다. 사전 정의된 객체가 많이 있으므로, 직접 사양을 입력하거나 객체를 만들지 않고도 원하는 것을 찾을 수 있습니다.
- Protocol—1-255 범위의 번호 또는 **ip**, **tcp**, **udp**, **gre** 등과 같이 잘 알려진 이름. 번호, 이름과 그 의미의 목록은 43-11 페이지의 프로토콜 및 애플리케이션를 참조하십시오.
- TCP, UDP, TCP-UDP ports—**tcp**, **udp**, **tcp-udp** 키워드에 포트 사양을 포함할 수 있습니다. tcp-udp 키워드를 사용하면 각각 지정할 필요 없이 두 프로토콜 모두에 대한 포트를 정의할 수 있습니다. 다음 방법으로 포트를 지정할 수 있습니다.
  - 단일 포트—tcp/80, udp/80, tcp-udp/80 또는 잘 알려진 서비스 이름(예: tcp/www, udp/snmp). 포트 및 키워드의 목록은 43-12 페이지의 TCP 및 UDP 포트를 참조하십시오.
  - 포트 범위—tcp/1-100, udp/1-100, tcp-udp/1-100은 1부터 100까지의 포트에 매칭합니다.

- 어떤 포트와 같지 않음—사양의 시작에 !=을 추가합니다. 이를테면 !=tcp/80은 TCP 포트 80(HTTP)을 제외한 모든 TCP 트래픽에 매칭합니다.
- 포트 번호보다 작음—<, 이를테면 예를 들면 <tcp/150을 추가하여 150 아래의 모든 포트에서 TCP 트래픽에 매칭합니다.
- 포트 번호보다 큼—>, 이를테면 >tcp150을 추가하여 150 위의 모든 포트에서 TCP 트래픽에 매칭합니다.

참고 DNS, Discard, Echo, Ident, NTP, RPC, SUNRPC, Talk 각각에서 TCP를 위한 정의와 UDP를 위한 정의가 하나씩 필요합니다. TACACS+는 TCP의 포트 49에서 하나의 정의가 필요합니다.

- ICMP, ICMP6 메시지—특정 메시지(예: ping echo 요청, 회신 메시지)와 메시지 코드까지 대상으로 지정할 수 있습니다. ICMP(IPv4) 및 ICMP6(IPv6)를 다루는 사전 정의된 객체가 많이 있으므로 직접 기준을 정의하지 않아도 됩니다. 형식은 다음과 같습니다.

  icmp/*icmp_message_type*[/*icmp_message_code*]

  icmp6/*icmp6_message_type*[/*icmp6_message_code*]

  여기서 메시지 유형은 1-255 또는 잘 알려진 이름이고, 코드는 0-255입니다. 선택하는 번호가 실제 유형/코드와 일치해야 합니다. 그렇지 않으면 ACE에 대한 매칭이 전혀 수행되지 않습니다. ICMP 유형의 목록은 43-16 페이지의 ICMP 유형를 참조하십시오.

표준 ACL 구성

표준 ACL은 명명된 ACE 컨테이너로 나타납니다. 새 ACL을 만들려면 먼저 컨테이너를 생성해야 합니다. 그런 다음 ACE를 추가하고 기존 ACE를 수정하고 표준 ACL 테이블을 사용하여 ACE를 재정렬할 수 있습니다. ACL Manager에서 ACL을 구성하면서 이를 사용하는 정책을 구성할 때 이 테이블이 탭의 형태로 나타날 수 있습니다. 그러한 경우 절차는 이 창을 표시하는 방법을 제외하고 동일합니다.

표준 ACL에서는 IPv4 주소만 사용하며, 목적지 주소만 정의합니다.

절차

1단계 **Configuration > Firewall > Advanced > Standard ACL**을 선택합니다.

2단계 새 ACL을 만드는 경우 **Add > Add ACL**을 선택하고 이름을 입력하고 **OK**를 클릭합니다.

ACL 컨테이너가 테이블에 추가됩니다. 표준 ACL은 이름을 변경할 수 없습니다.

3단계 다음 중 하나를 수행합니다.

- ACL의 끝에 ACE를 추가하려면 ACL 이름 또는 그 안의 ACE를 선택하고 **Add > Add ACE**를 선택합니다.
- 특정 위치에 ACE를 삽입하려면 기존 ACE를 선택하고 **Add > Insert**를 선택하여 그 규칙 위에 ACE를 추가하거나 **Add > Insert After**를 선택합니다.
- 규칙을 수정하려면 선택하고 **Edit**를 클릭합니다.

4단계 ACE 속성을 채웁니다. 옵션은 다음과 같습니다.

- **Action: Permit/Deny**—설명된 트래픽을 허용하는지(선택) 또는 거부하는지(선택 취소, 매칭하지 않음) 여부.
- **Address**—트래픽 흐름의 목적지, 즉 대상 주소의 정의. 호스트 주소(예: 10.100.1.1), 네트워크(10.100.1.0/24 또는 10.100.1.0/255.255.255.0 형식)를 지정하거나 네트워크 객체를 선택할 수 있습니다. 후자의 경우, 단순히 객체의 내용을 Address 필드에 로드합니다.
- **Description**—ACE의 목적에 대한 설명이며, 라인당 최대 100자입니다. 여러 라인을 입력할 수 있습니다. 각 라인은 CLI에서 설명으로 추가되며, 이 설명이 ACE의 앞에 위치합니다.

참고 어떤 플랫폼(예: Windows)에서 영어가 아닌 문자로 설명을 추가한 다음 다른 플랫폼(예: Linux)에서 그 설명을 삭제하려는 경우, 수정 또는 삭제가 불가능할 수 있습니다. 원래의 문자가 제대로 인식되지 않을 가능성이 있기 때문입니다. 이러한 제약은 다른 언어의 문자를 각기 다르게 인코딩하는 기본 플랫폼의 종속성 때문입니다.

ACE 정의를 완료하면 **OK**를 클릭하여 테이블에 규칙을 추가합니다.

5단계 **Apply**를 클릭합니다.

웹 타입 ACL 구성

웹 타입 ACL은 클라이언트리스 SSL VPN 트래픽의 필터링에 사용되어 특정 네트워크, 서브넷, 호스트, 웹 서버에 대한 사용자 액세스를 제한합니다. 필터를 정의하지 않을 경우 모든 연결이 허용됩니다. 웹 타입 ACL은 명명된 ACE 컨테이너로 나타납니다. 새 ACL을 만들려면 먼저 컨테이너를 생성해야 합니다. 그런 다음 ACE를 추가하고 기존 ACE를 수정하고 웹 ACL 테이블을 사용하여 ACE를 재정렬할 수 있습니다. ACL Manager에서 웹 타입 ACL을 구성하면서 이를 사용하는 정책을 구성할 때 이 테이블이 나타날 수 있습니다. 그러한 경우 절차는 이 창을 표시하는 방법을 제외하고 동일합니다.

웹 타입 ACL은 URL 사양 외에도 IPv4 주소와 IPv6 주소의 혼합을 포함할 수 있습니다.

절차

1단계 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**을 선택합니다.

2단계 새 ACL을 만드는 경우 **Add > Add ACL**을 선택하고 이름을 입력하고 **OK**를 클릭합니다.

ACL 컨테이너가 테이블에 추가됩니다. 나중에 이를 선택하고 **Edit**를 클릭하여 이름을 바꿀 수 있습니다.

3단계 다음 중 하나를 수행합니다.

- ACL의 끝에 ACE를 추가하려면 ACL 이름 또는 그 안의 ACE를 선택하고 **Add > Add ACE**를 선택합니다.
- 특정 위치에 ACE를 삽입하려면 기존 ACE를 선택하고 **Add > Insert**를 선택하여 그 규칙 위에 ACE를 추가하거나 **Add > Insert After**를 선택합니다.
- 규칙을 수정하려면 선택하고 **Edit**를 클릭합니다.

4단계 ACE 속성을 채웁니다. 기본 선택 옵션은 다음과 같습니다.

- **Action: Permit/Deny**—설명된 트래픽을 허용하는지(선택) 또는 거부하는지(선택 취소, 매칭하지 않음) 여부.
- **Filter**—목적지를 기준으로 한 트래픽 매칭 기준. 프로토콜을 선택하고 서버 이름, 선택 사항으로 경로와 파일 이름까지 선택하여 URL을 지정할 수 있습니다. 또는 목적지의 IPv4 또는 IPv6 주소와 TCP 서비스를 지정할 수 있습니다.

이용 가능한 모든 옵션에 대한 자세한 내용은 18-11 페이지의 웹 타입 ACE 속성를 참조하십시오.

ACE 정의를 완료하면 **OK**를 클릭하여 테이블에 규칙을 추가합니다.

5단계 **Apply**를 클릭합니다.

웹 타입 ACE 속성

웹 타입 ACL의 ACE를 추가하거나 수정할 때 다음 속성을 구성할 수 있습니다. 많은 필드에서 편집 상자의 오른쪽에 있는 "..." 버튼을 클릭하여 필드에 사용 가능한 객체를 선택, 생성하거나 수정할 수 있습니다.

어떤 ACE에서 URL 또는 주소로 필터링할 수 있으나, 둘 다 할 수는 없습니다.

- **Action: Permit/Deny**—설명된 트래픽을 허용하는지(선택) 또는 거부하는지(선택 취소, 매칭하지 않음) 여부.
- **Filter on URL**—목적지 URL을 기준으로 트래픽에 매칭합니다. 프로토콜을 선택하고 서버 이름, 선택 사항으로 경로와 파일 이름을 입력합니다. 이를테면 http://www.example.com, 모든 서버를 포괄하려면 http://*.example.com입니다. 다음은 URL 지정에 관한 팁과 제한 사항입니다.
  - 모든 URL에 매칭하려면 **any**를 선택합니다.
  - 'Permit url any'은 protocol://server-ip/path 형식의 모든 URL을 허용하며, port-forwarding과 같이 이 패턴과 일치하지 않은 트래픽은 차단합니다. 암시적 거부가 일어나지 않도록 필요한 포트(Citrix의 경우 포트 1494)와의 연결을 허용하는 ACE가 있어야 합니다.
  - 스마트 터널과 ica plug-in인 'permit url any' ACL의 영향을 받지 않습니다. mart-tunnel:// and ica://유형에만 매칭하기 때문입니다.
  - cifs://, citrix://, citrixs://, ftp://, http://, https://, imap4://, nfs://, pop3://, smart-tunnel://, and smtp:// 프로토콜을 사용할 수 있습니다. 또한 프로토콜에 와일드카드를 사용할 수 있습니다. 예를 들어, htt*는 http 및 https에, 별표 *는 모든 프로토콜에 매칭됩니다. 예를 들어, *://*.example.com은 example.com 네트워크로 가는 모든 유형의 URL 기준 트래픽에 매칭합니다.
  - smart-tunnel:// URL을 지정할 경우 서버 이름만 포함할 수 있습니다. URL은 경로를 포함할 수 없습니다. 예를 들어, smart-tunnel://www.example.com은 허용되지만, smart-tunnel://www.example.com/index.html은 허용되지 않습니다.
  - 별표 *는 무엇과도 매칭하지 않거나 임의의 문자 수에 매칭합니다. 모든 http URL에 매칭하려면 http://*/*를 입력합니다.
  - 물음표 ?는 임의의 한 문자에만 매칭합니다.
  - 대괄호 []는 범위 연산자로서 해당 범위에 속한 모든 문자에 매칭합니다. 예를 들어, http://www.cisco.com:80/와 http://www.cisco.com:81/ 모두에 매칭하려면 **http://www.cisco.com:8[01]/**를 입력합니다.

- **Filter on Address and Service**—목적지 주소 및 서비스를 기준으로 트래픽에 매칭합니다.
  - **Address**—목적지의 IPv4 또는 IPv6 주소. 모든 주소에 매칭하려는 경우 **any**를 사용하면 모든 IPv4 또는 IPv6 주소에, **any4**는 IPv4 주소에만, **any6**는 IPv6 주소에만 매칭합니다. 단일 호스트 주소(예: 10.100.10.5, 2001:DB8::0DB8:800:200C:417A), 서브넷(10.100.10.0/24 또는 10.100.10.0/255.255.255.0 형식, IPv6의 경우 2001:DB8:0:CD30::/60)을 지정할 수 있습니다. 또는 네트워크 객체를 선택할 수 있는데, 그러면 필드가 객체의 내용으로 채워집니다.
  - **Service**—단일 TCP 서비스 사양. 기본값은 포트 없는 **tcp**입니다. 그러나 단일 포트(예: tcp/80, tcp/www) 또는 포트 범위(예: tcp/1-100)를 지정할 수 있습니다. 연산자를 추가할 수 있습니다. 예를 들어, !=tcp/80은 포트 80을 제외합니다. <tcp/80은 80보다 작은 모든 포트, >tcp/80은 80보다 큰 모든 포트입니다.
- **Enable Logging**; **Logging Level**; **More Options > Logging Interval**—로깅 옵션은 트래픽을 거부하는 규칙에 대해 syslog 메시지가 생성되는 방식을 정의합니다. 다음 로깅 옵션을 구현할 수 있습니다.
  - **Deselect Enable Logging**—규칙에 대한 로깅을 비활성화합니다. 이 규칙에 의해 거부되는 트래픽에 대해서는 어떤 유형의 syslog 메시지도 표시되지 않습니다.
  - **Select Enable Logging with Logging Level = Default**—규칙에 대한 기본 로깅을 제공합니다. 거부된 패킷 각각에 대해 syslog 메시지 106103이 표시됩니다. 어플라이언스가 공격을 받은 경우 이 메시지가 표시되는 빈도가 서비스에 영향을 미칠 수 있습니다.
  - **Select Enable Logging with Non-Default Logging Level**—요약된 syslog 메시지, 즉 106103이 아닌 106102이 제공됩니다. 메시지 106102는 처음 적중했을 때 표시되고, 그 다음에는 **More Options > Logging Interval**에 구성된 간격(기본값은 300초마다, 1-600에서 지정 가능)에 따라 다시 표시되면서 해당 간격의 적중 횟수를 표시합니다. 권장되는 로깅 레벨은 **Informational**입니다.
- **More Options > Time Range**—규칙이 활성화되는 요일과 시간대를 정의하는 시간 범위 객체의 이름. 시간 범위를 지정하지 않을 경우 규칙은 항상 활성 상태입니다.

웹 타입 ACL의 예

다음은 웹 타입 ACL을 위한 URL 기준 규칙의 예입니다.

작업	필터	효과
거부	url http://*.yahoo.com/	모든 Yahoo!에 대한 액세스를 거부합니다.
거부	url cifs://fileserver/share/directory	지정된 위치에 있는 모든 파일에 대한 액세스를 거부합니다.
거부	url https://www.example.com/ directory/file.html	지정된 파일에 대한 액세스를 거부합니다.
허용	url https://www.example.com/directory	지정된 위치에 대한 액세스를 허용합니다.
거부	url http://*:8080/	포트 8080을 지나는, 임의의 위치에 대한 HTTPS 액세스를 거부합니다.
거부	url http://10.10.10.10	10.10.10.10에 대한 HTTP 액세스를 거부합니다.
허용	url any	임의의 URL에 대한 액세스를 허용합니다. 주로 URL 액세스를 거부하는 ACL의 다음에 사용됩니다.

ACL 모니터링

ACL Manager, 표준 ACL, 웹 ACL, 이더 타입 ACL 테이블은 통합적으로 ACL을 표시합니다. 그러나 디바이스에서 무엇이 구성되었는지 정확하게 보기 위해 다음 명령을 사용할 수 있습니다. 명령을 입력하기 위해 **Tools > Command Line Interface**를 선택합니다.

명령	목적
show access-list [*name*]	ACE의 라인 번호와 적중 횟수를 포함하여 액세스 목록을 표시합니다. ACL 이름을 포함합니다. 그러지 않으면 모든 액세스 목록이 표시됩니다.
show running-config access-list [*name*]	현재 실행 중인 액세스 목록 컨피그레이션을 표시합니다. ACL 이름을 포함합니다. 그러지 않으면 모든 액세스 목록이 표시됩니다.

ACL 관련 이력

기능 이름	릴리스	설명
확장, 표준, 웹 타입 ACL	7.0(1)	네트워크 액세스를 제어하거나 여러 기능이 실행될 트래픽을 지정하는 데 ACL을 사용합니다. 확장 ACL은 through-the-box 액세스 제어 및 그 밖의 몇몇 기능에 사용합니다. 표준 ACL은 경로 맵 및 VPN 필터에 사용합니다. 웹 타입 ACL은 클라이언트리스 SSL VPN 필터링에 사용합니다. 이더 타입 ACL은 비 IP 레이어 2 트래픽을 제어합니다. ACL Manager 및 ACL 구성을 위한 기타 페이지를 추가했습니다.
확장 ACL의 실제 IP 주소	8.3(1)	NAT 또는 PAT를 사용할 경우, 일부 기능의 ACL에서 매핑된 주소 및 포트를 더 이상 사용하지 않습니다. 이러한 기능에는 변환되지 않은 실제 주소와 포트를 사용해야 합니다. 실제 주소와 포트를 사용할 경우 NAT 컨피그레이션이 바뀌더라도 ACL을 변경할 필요 없습니다. 자세한 내용은 18-4 페이지의 NAT 사용 시 확장 ACL에 쓰이는 IP 주소를 참조하십시오.
확장 ACL에서의 ID 방화벽 지원	8.4(2)	이제 소스 및 목적지에 대해 ID 방화벽 사용자와 그룹을 사용할 수 있습니다. 액세스 규칙, AAA 규칙에 또한 VPN 인증을 위해 ID 방화벽 ACL을 사용할 수 있습니다.
이더 타입 ACL의 IS-IS 트래픽 지원	8.4(5), 9.1(2)	투명 방화벽 모드에서 ASA는 이더 타입 ACL을 사용하여 IS-IS 트래픽을 제어할 수 있습니다. 다음 화면을 수정했습니다. Configuration > Device Management > Management Access > EtherType Rules

기능 이름	릴리스	설명
확장 ACL에서의 Cisco TrustSec 지원	9.0(1)	소스 및 목적지에 대해 Cisco TrustSec 보안 그룹을 사용할 수 있습니다. 액세스 규칙과 함께 ID 방화벽 ACL을 사용할 수 있습니다.
IPv4와 IPv6를 위해 통일된 확장 ACL 및 웹 타입 ACL	9.0(1)	확장 ACL 및 웹 타입 ACL에서 IPv4 주소와 IPv6 주소를 지원합니다. 소스 및 목적지에 IPv4 주소와 IPv6 주소를 혼합하여 지정할 수도 있습니다. **any** 키워드는 IPv4 트래픽과 IPv6 트래픽을 나타내도록 변경되었습니다. **any4** 키워드와 **any6** 키워드가 각각 IPv4 트래픽만, IPv6 트래픽만 나타내도록 추가되었습니다. IPv6 전용 ACL은 더 이상 사용하지 않습니다. 기존 IPv6 ACL은 확장 ACL로 마이그레이션되었습니다. 마이그레이션에 대한 자세한 내용은 릴리스 정보를 참조하십시오. 다음 화면을 수정했습니다. Configuration > Firewall > Access Rules Configuration > Remote Access VPN > Network (Client) Access > Group Policies > General > More Options
확장 ACL 및 ICMP 코드를 기준으로 ICMP 트래픽을 필터링하기 위한 객체 개선 사항	9.0(1)	이제 ICMP 코드에 따라 ICMP 트래픽을 허용하거나 거부할 수 있습니다. 다음 화면을 도입했거나 수정했습니다. Configuration > Firewall > Objects > Service Objects/Groups Configuration > Firewall > Access Rule

파 트 6

IP 라우팅

라우팅 개요

이 장에서는 Cisco ASA 내에서 라우팅의 동작 원리와 지원되는 프로토콜에 관한 기본 개념을 설명합니다.

라우팅 정보

라우팅은 소스에서 대상까지 인터네트워크에 걸친 정보의 이동입니다. 그 과정에서 적어도 하나의 중간 노드를 만나게 됩니다. 라우팅에는 2가지 기본적인 작업이 포함됩니다. 최적의 라우팅 경로를 결정하는 것과 인터네트워크를 통한 정보 그룹(패킷이라고 함)을 전송하는 것입니다. 라우팅 프로세스에서는 후자를 패킷 스위칭이라고 합니다. 패킷 스위칭은 비교적 간단하지만 경로 결정은 매우 복잡할 수 있습니다.

스위칭

스위칭 알고리즘은 상대적으로 단순하며 대부분의 라우팅 프로토콜에 대해 동일합니다. 대부분의 경우 호스트가 패킷을 다른 호스트로 보내야 한다고 결정합니다. 라우터 주소를 확보한 소스 호스트는 패킷 주소를 라우터의 물리적 (Media Access Control [MAC]-layer) 주소로 보내는 데 이번에는 대상 호스트의 프로토콜(네트워크 레이어) 주소를 함께 보냅니다.

라우터는 패킷 대상 프로토콜 주소를 검사하면서 패킷을 다음 홉으로 전달하는 방법을 알고 있는지 모르고 있는지 결정합니다. 라우터가 패킷 전달 방법을 모르는 경우 일반적으로 패킷을 버리게 됩니다. 하지만 라우터가 패킷 전달 방법을 안다면 대상 물리적 주소를 다음 홉의 주소로 바꾸고 패킷을 전송합니다.

다음 홉 주소는 궁극적인 대상 호스트가 될 수 있습니다. 아니라면 다음 홉은 보통 동일한 스위칭 결정 프로세스를 실행하는 다른 라우터입니다. 패킷이 인터네트워크를 통과하면서 물리적 주소가 변경되지만 프로토콜 주소는 유지됩니다.

경로 결정

라우팅 프로토콜은 메트릭을 사용하여 패킷이 이동할 최적의 경로를 평가합니다. 메트릭은 경로 대역폭과 같이 측정 기준으로서 대상으로의 최적 경로를 결정하는 라우팅 알고리즘에 사용됩니다. 라우팅 알고리즘은 경로 결정을 돕기 위해 경로 정보를 포함하는 라우팅 테이블을 초기화하고 유지합니다. 경로 정보는 사용된 경로 알고리즘에 따라 달라집니다.

라우팅 알고리즘은 다양한 정보로 라우팅 테이블을 채웁니다. 대상 또는 차기 홉 연결은 패킷을 특정 라우터로 보내 차기 홉이 최종 대상을 향해 가고 있음을 알림으로써 특정 대상에 최적으로 도달할 수 있음을 라우터에 알려줍니다. 라우터가 수신 패킷을 수신하면 대상 주소를 확인하고 이 주소를 차기 홉과 연결하려고 시도합니다.

라우팅 테이블은 또한 경로의 선호도와 같은 다른 정보도 포함합니다. 라우터는 메트릭을 비교하여 최적의 경로를 결정하고 이러한 메트릭은 사용된 라우팅 알고리즘의 설계에 따라 달라집니다.

라우터는 서로 통신하며 다양한 메시지의 전송을 통해 라우팅 테이블을 유지합니다. 라우팅 업데이트 메시지는 일반적으로 라우팅 테이블 전체 또는 일부로 구성되는 메시지입니다. 라우터는 다른 모든 라우터의 라우팅 업데이트를 분석함으로써 네트워크 토폴로지에 대한 자세한 그림을 그릴 수 있습니다. 라우터 간에 전송되는 메시지의 또 다른 예인 링크-상태 알림은 다른 라우터에 발신자 링크의 상태를 알려줍니다. 연결 정보는 라우터가 네트워크 대상으로의 최적의 경로를 결정할 수 있도록 네트워크 토폴로지의 완전한 그림을 그리는 데에도 사용됩니다.

참고 비대칭 라우팅은 다중 컨텍스트 모드의 액티브/액티브 장애 조치에 대해서만 지원됩니다.

지원되는 경로 유형

라우터는 몇 가지 경로 유형을 사용할 수 있습니다. ASA은(는) 다음 경로 유형을 사용합니다.

- 19-2 페이지의 고정 대 동적
- 19-3 페이지의 단일 경로 대 다중 경로
- 19-3 페이지의 평면 대 계층
- 19-3 페이지의 연결 상태 대 거리 벡터

고정 대 동적

고정 라우팅 알고리즘은 알고리즘이라고 하기 어렵고 네트워크 관리자가 라우팅 전에 설정한 테이블 매핑입니다. 이러한 매핑은 네트워크 관리자가 변경하지 않는 한 변경되지 않습니다. 고정 경로를 사용하는 알고리즘은 설계하기가 쉽고 네트워크 트래픽을 상대적으로 예측하기 쉬운 환경과 네트워크 설계가 상대적으로 단순한 환경에서 효과적입니다.

고정 라우팅 시스템은 네트워크 변화에 대응할 수 없기 때문에 꾸준히 변화하는 대규모 네트워크에는 일반적으로 적합하지 않습니다. 대부분의 주요 라우팅 알고리즘은 수신 라우팅 업데이트 메시지를 분석함으로써 네트워크 상황의 변화에 대응하는 동적 라우팅 알고리즘입니다. 메시지가 네트워크 변경 사실을 알리면 라우팅 소프트웨어가 경로를 다시 계산하고 새로운 라우팅 업데이트 메시지를 보냅니다. 이 메시지는 네트워크를 통과하며 라우터가 알고리즘을 다시 실행하고 라우팅 테이블을 그에 따라 변경하게 합니다.

동적 라우팅 알고리즘은 고정 경로로 적절히 보완할 수 있습니다. 예를 들어 최후의 수단으로 사용하는 라우터(모든 라우팅 불가 패킷이 전송되는 라우터)는 모든 라우팅 불가 패킷에 대한 저장소 역할을 하도록 지정되어 모든 메시지가 어떻게든 처리되도록 할 수 있습니다.

단일 경로 대 다중 경로

일부 고급 라우팅 프로토콜은 동일 대상에 대한 다중 경로를 지원합니다. 단일 경로 알고리즘과 달리 이러한 다중 경로 알고리즘은 여러 회선에 걸친 트래픽 멀티플렉싱을 허용합니다. 다중 경로 알고리즘의 이점은 보통 부하 공유라고 부르는 훨씬 뛰어난 처리량과 신뢰성입니다.

평면 대 계층

일부 라우팅 알고리즘은 평면 공간에서 작동하고 또 다른 일부는 라우팅 계층을 사용합니다. 평면 라우팅 시스템에서 라우터는 다른 모든 라우터의 피어입니다. 계층형 라우팅 시스템에서는 일부 라우터가 모여 라우팅 백본을 형성합니다. nonbackbone 라우터의 패킷은 백본 라우터로 이동하고 여기서 백본을 통해 대상 영역에 도달할 때까지 전송됩니다. 이 시점에서는 마지막 백본 라우터에서 하나 이상의 백본 라우터를 통해 최종 대상으로 이동합니다.

라우팅 시스템은 종종 도메인, 자율 시스템 또는 영역이라고 하는 논리적인 노드 그룹을 지정합니다. 계층형 시스템에서는 다른 도메인의 라우터와 통신할 수 있는 라우터도 있고 같은 도메인의 라우터하고만 통신할 수 있는 라우터도 있습니다. 대규모 네트워크에서는 추가적인 계층 수준이 있을 수 있고 가장 높은 계층 수준의 라우터가 라우팅 백본을 형성합니다.

계층형 라우팅의 주된 이점은 그것이 대부분의 조직 구조와 비슷하기 때문에 조직의 트래픽 패턴도 잘 지원한다는 점입니다. 대부분의 네트워크 통신은 소규모 기업 그룹(도메인) 내에서 발생합니다. 인트라도메인 라우터는 도메인 내의 다른 라우터에 대해서만 알 필요가 있으므로 라우팅 알고리즘을 간소화할 수 있고, 사용되는 라우팅 알고리즘에 따라 라우팅 업데이트 트래픽을 줄일 수 있습니다.

연결 상태 대 거리 벡터

링크 상태 알고리즘 (최단 경로 우선 알고리즘)은 인터네트워크의 모든 노드로 라우팅 정보를 전달합니다. 하지만 각 라우터는 자신의 링크 상태를 설명하는 라우팅 테이블의 일부만 전송합니다. 링크 상태 알고리즘에서는 각 라우터가 라우팅 테이블에서 전체 네트워크의 상태를 그립니다. 거리 벡터 알고리즘(Bellman-Ford 알고리즘이라고도 함)이 각 라우터를 호출하여 라우팅 테이블의 전체 또는 일부를 인접 라우터에 한해 전송하도록 합니다. 기본적으로 링크 상태 알고리즘은 모든 곳으로 소규모 업데이트를 전송하는 반면 거리 벡터 알고리즘은 대규모 업데이트를 인접 라우터로만 보냅니다. 거리 벡터 알고리즘은 인접 디바이스에 대해서만 알고 있습니다. 일반적으로 링크 상태 알고리즘은 OSPF 라우팅 프로토콜과 함께 사용됩니다.

ASA 내에서 라우팅의 작동 방식

ASA은(는) 라우팅 결정을 위해 라우팅 테이블과 XLATE 테이블을 모두 사용합니다. 대상 IP 변환 트래픽, 즉 미변환 트래픽을 처리하기 위해 ASA은(는) 기존 XLATE 또는 고정 변환을 검색하여 이그레스 인터페이스를 선택합니다.

- 19-4 페이지의 이그레스 인터페이스 선택 프로세스
- 19-4 페이지의 차기 홉 선택 프로세스

이그레스 인터페이스 선택 프로세스

선택 프로세스는 다음 단계를 따릅니다.

1. XLATE를 변환하는 대상 IP가 이미 존재하는 경우 패킷에 대한 이그레스 인터페이스는 라우팅 테이블이 아니라 XLATE 테이블에서 결정됩니다.
2. XLATE를 변환하는 대상 IP가 존재하지 않지만 일치하는 고정 변환이 존재하는 경우 이그레스 인터페이스는 고정 NAT 규칙으로부터 결정되고 XLATE이 생성되며 라우팅 테이블은 사용되지 않습니다.
3. XLATE를 변환하는 대상 IP가 존재하지 않고 일치하는 고정 변환도 없는 경우 패킷은 대상 IP 변환이 되지 않습니다. ASA이(가) 이그레이 인터페이스 선택 경로를 조회함으로써 이 패킷을 처리한 후 소스 IP 변환이 수행됩니다(필요한 경우).

   일반 동적 아웃바운드 NAT의 경우 초기 발신 패킷이 경로 테이블을 사용한 다음 XLATE를 생성함으로써 라우팅됩니다. 수신 반환 패킷은 기존 XLATE만 사용하여 전달됩니다. 고정 NAT의 경우 대상 변환된 수신 패킷은 항상 기존 XLATE 또는 고정 변환 규칙을 사용하여 전달됩니다.

차기 홉 선택 프로세스

이전에 설명한 방법을 사용하여 이그레스 인터페이스를 선택한 후 이전에 선택한 이그레스 인터페이스에 속하는 적당한 차기 홉을 찾기 위한 추가 경로 조회가 실시됩니다. 선택한 인터페이스에 속하는 라우팅 테이블에 경로가 없는 경우 다른 이그레스 인터페이스에 속하는 대상 네트워크로의 다른 경로가 있는 경우에도 패킷이 버려지고 레벨 6 syslog 메시지 110001(호스트 경로 없음)이 생성됩니다. 선택한 이그레스 인터페이스에 속하는 경로가 발견되면 패킷이 대응 차기 홉으로 전달됩니다.

단일 이그레스 인터페이스를 사용하여 여러 차기 홉을 사용할 수 있는 경우에만 ASA의 부하 공유가 가능합니다. 부하 공유로 여러 이그레스 인터페이스를 공유할 수 없습니다.

ASA에서 동적 라우팅이 사용 중이고 XLATE 생성 후 경로 테이블이 변경되는 경우(예: 경로 플랩) 경로 테이블을 통하지 않고 기존 XLATE를 사용하여 XLATE 시간 초과까지 대상 변환 트래픽이 전달됩니다. 이전 경로가 이전 인터페이스에서 삭제되고 라우팅 프로세스에 의해 다른 인터페이스에 연결될 경우 잘못된 인터페이스로 전달되거나 레벨 6 syslog 메시지 110001(호스트 경로 없음)와 함께 버려질 수 있습니다.

ASA 자체에서 경로 플랩이 없지만 주변에서 라우팅 프로세스 플래핑이 일어나고 동일 흐름에 속하는 소스 변환 패킷이 다른 인터페이스를 사용하는 ASA을(를) 통해 전송되는 경우에도 같은 문제가 발생할 수 있습니다. 대상 변환 반환 패킷이 잘못된 이그레스 인터페이스를 사용하여 전달될 수 있습니다.

이 문제는 흐름에서 초기 패킷의 방향에 따라 사실상 모든 트래픽이 소스 변환이거나 대상 변환인 일부 보안 트래픽 컨피그레이션에서 가능성이 높습니다. 이 문제가 경로 플랩 후에 발생하는 경우 **clear xlate** 명령을 사용하여 수동으로 해결하거나 XLATE 시간 초과로 자동으로 해결될 수 있습니다. 필요하면 XLATE 시간 초과를 줄일 수 있습니다. 이 문제가 잘 발생하지 않도록 하려면 ASA와(과) 그 주변에서 경로 플랩이 없도록 하십시오. 다시 말해 같은 흐름에 속하는 대상 변환 패킷이 항상 ASA을(를) 통해 똑같이 전달되도록 하십시오.

라우팅을 위한 지원되는 인터넷 프로토콜

ASA은(는) 라우팅을 위해 몇 가지 인터넷 프로토콜을 지원합니다. 각 프로토콜은 이 섹션에 간단히 설명되어 있습니다.

- EIGRP(Enhanced Interior Gateway Routing Protocol)

  EIGRP는 IGRP 라우터와의 호환성과 원활한 상호 작용을 제공하는 Cisco 고유의 프로토콜입니다. 자동 재배포 메커니즘은 IGRP 경로를 Enhanced IGRP로 가져올 수 있게 하고 그 반대도 지원합니다. 따라서 기존 IGRP 네트워크로 Enhanced IGRP를 단계적으로 추가할 수 있습니다.

  EIGRP 구성에 관한 자세한 정보는 24-4 페이지의 EIGRP 구성에서 참조하십시오.

- OSPF(Open Shortest Path First)

  OSPF는 IETF(Internet Engineering Task Force)의 내부 게이트웨이 프로토콜(IGP) 작업 그룹이 인터넷 프로토콜 (IP) 네트워크를 위해 개발한 라우팅 프로토콜입니다. OSPF는 링크 상태 알고리즘을 사용하여 알려진 모든 목적지에 도달하기 위한 최단 경로를 구축하고 계산합니다. OSPF 영역의 각 라우터는 라우터가 사용 가능한 인터페이스와 접근할 수 있는 인접 디바이스의 목록인 동일한 링크 상태 데이터베이스를 포함합니다.

  OSPF 구성에 관한 자세한 정보는 23-6 페이지의 OSPFv2 구성에서 참조하십시오.

- RIP(Routing Information Protocol)

  RIP는 홉 카운트를 메트릭으로 사용하는 거리 벡터 프로토콜입니다. RIP는 글로벌 인터넷에서 라우팅 트래픽을 위해 널리 사용되며 내부 게이트웨이 프로토콜(IGP)이기 때문에 단일 자율 시스템 내에서 라우팅을 수행합니다.

  RIP 구성에 관한 자세한 정보는 기존 기능 가이드에서 참조하십시오.

- BGP(Border Gateway Protocol)

  BGP는 자율 시스템 간 라우팅 프로토콜입니다. BGP는 인터넷을 위한 라우팅 정보 교환에 사용되며 인터넷 서비스 제공자(ISP) 간에 사용되는 프로토콜입니다. 고객은 ISP에 연결하고 ISP는 BGP를 사용하여 고객 및 ISP 경로를 교환합니다. 자율 시스템(AS) 사이에서 BGP가 사용될 때 프로토콜을 EBGP(External BGP)라고 합니다. 서비스 공급자가 AS 내에서 경로 교환을 위해 BGP를 사용할 때 프로토콜은 IBGP(Interior BGP)라고 합니다.

  BGP 구성에 관한 자세한 정보는 22-4 페이지의 BGP 구성에서 참조하십시오.

라우팅 테이블 정보

라우팅 테이블 표시

절차

1단계 ASDM에서 라우팅 테이블에 있는 모든 경로를 표시하려면 **Monitoring > Routing > Routes**를 선택합니다.

이 창에서 각 행은 1개의 경로를 의미합니다.

라우팅 테이블을 채우는 방법

ASA 라우팅 테이블은 고정 정의 경로, 직접 연결 경로, 그리고 RIP, EIGRP, OSPF 및 BGP 라우팅 프로토콜로 발견된 경로로 채울 수 있습니다. ASA은(는) 라우팅 테이블에 고정 경로와 연결 경로를 가지는 것 외에도 여러 라우팅 프로토콜을 실행할 수 있기 때문에 같은 경로가 하나 이상의 방법으로 다시 발견되거나 입력될 수 있습니다. 같은 대상으로의 두 경로를 라우팅 테이블에 넣으면 라우팅 테이블에 유지되는 항목은 다음과 같이 결정됩니다.

- 두 경로의 네트워크 접두사 길이(네트워크 마스크)가 다르면 두 경로 모두 고유한 것으로 간주되어 라우팅 테이블에 입력됩니다. 그런 다음 패킷 전달 논리가 둘 중 사용할 경로를 결정합니다.

  예를 들어 RIP와 OSPF 프로세스가 다음 경로에서 발견된 경우:

  - RIP: 192.168.32.0/24
  - OSPF: 192.168.32.0/19

  비록 OSPF 경로가 관리 거리가 더 낮지만 서로의 접두사 길이(서브넷 마스크)가 다르기 때문에 두 경로 모두 라우팅 테이블에 설치됩니다. 이들은 다른 대상으로 간주되며 패킷 전달 논리가 사용할 경로를 결정합니다.

- ASA이(가) RIP와 같이 단일 라우팅 프로토콜에서 같은 대상으로의 여러 경로를 학습하는 경우 메트릭이 더 나은 경로(라우팅 프로토콜이 결정)가 라우팅 테이블에 입력됩니다.

  메트릭은 특정 경로와 연결되어 최우선부터 최하위까지 순위를 지정합니다. 메트릭을 결정하는 데 사용되는 매개변수는 라우팅 프로토콜에 따라 다릅니다. 가장 낮은 메트릭을 갖는 경로가 최적의 경로로 선택되고 라우팅 테이블에 설치됩니다. 동일한 값의 메트릭을 갖는 동일한 목적지로의 경로가 여럿인 경우 이러한 동일 비용 경로에 대한 로드 밸런싱이 수행됩니다.

- ASA이(가) 두 개 이상이 라우팅 프로토콜로부터 대상에 대해 학습하는 경우 경로의 관리 거리를 비교하고 관리 거리가 짧은 경로가 라우팅 테이블에 입력됩니다.

경로의 관리 거리

라우팅 프로토콜에서 검색 또는 재배포되는 경로에 대한 관리 거리를 변경할 수 있습니다. 서로 다른 두 라우팅 프로토콜에서 두 경로의 관리 거리가 같은 경우 *기본* 관리 거리가 낮은 경로가 라우팅 테이블에 입력됩니다. EIGRP와 OSPF 경로의 경우 EIGRP 경로와 OSPF 경로가 같은 관리 거리를 갖는다면 기본적으로 EIGRP 경로가 선택됩니다.

관리 거리는 2개의 서로 다른 라우팅 프로토콜에서 동일한 목적지로 2개 이상의 다른 경로가 있는 경우 최적의 경로를 선택하기 위해 ASA에서 사용하는 경로 매개변수입니다. 라우팅 프로토콜은 다른 프로토콜과 구별되는 알고리즘을 기반으로 한 메트릭을 갖기 때문에 다른 라우팅 프로토콜에서 생성된 두 경로 중에 항상 최적의 경로를 확인할 수 있는 것은 아닙니다.

각 라우팅 프로토콜은 관리 거리 값을 사용하여 우선순위가 지정됩니다. 표 19-1은(는) ASA에서 지원되는 라우팅 프로토콜의 기본 관리 거리 값을 표시합니다.

표 19-1 지원되는 라우팅 프로토콜의 기본 관리 거리

경로 소스	기본 관리 거리
연결된 인터페이스	0
고정 경로	1
EIGRP 요약 경로	5
외부 BGP	20
내부 EIGRP	90
OSPF	110
RIP	120
EIGRP 외부 경로	170
내부 BGP	200
알 수 없음	255

관리 거리 값이 작을수록 프로토콜 우선순위가 높습니다. 예를 들어, ASA이(가) OSPF 라우팅 프로세스(기본 관리 거리 - 110)와 RIP 라우팅 프로세스(기본 관리 거리 - 120)로부터 모두 특정 네트워크로의 경로를 수신할 경우 ASA은(는) 우선순위가 더 높은 OSPF 경로를 선택합니다. 이 경우 라우터가 라우팅 테이블에 경로의 OSPF 버전을 추가합니다.

이 예제에서, OSPF 파생 경로의 소스가 손실된 경우(예: 전원 꺼짐) ASA은(는) OSPF 파생 경로가 다시 나타날 때까지 RIP 파생 경로를 사용합니다.

관리 거리는 로컬 설정입니다. 예를 들어 **distance-ospf** 명령을 사용하여 OSPF를 통해 얻은 관리 거리를 변경하면 이는 명령을 입력한 ASA의 라우팅 테이블에만 영향을 줍니다. 관리 거리는 라우팅 업데이트에서 알려지지 않습니다.

관리 거리는 라우팅 프로세스에 영향을 주지 않습니다. EIGRP, OSPF, RIP 및 BGP 라우팅 프로세스는 라우팅 프로세스를 통해서 검색되었거나 라우팅 프로세스로 재배포된 경로만 알립니다. 예를 들어, RIP 라우팅 프로세스는 OSPF 라우팅 프로세스를 통해 발견된 경로가 ASA 라우팅 테이블에 사용된다 할지라도, RIP 경로를 알립니다.

백업 경로

다른 경로가 설치되었기 때문에 라우팅 테이블에 경로를 설치하려는 첫 번째 시도가 실패하면 백업 경로가 등록됩니다. 라우팅 테이블에 설치된 경로가 실패할 경우 라우팅 테이블 유지 관리 프로세스는 백업 경로를 등록한 각 라우팅 프로토콜 프로세스를 호출하고 해당 경로를 라우팅 테이블에 다시 설치하도록 요청합니다. 실패한 경로에 대해 백업이 등록된 프로토콜이 여럿인 경우 관리 거리를 기준으로 우선 경로가 선택됩니다.

이 프로세스 때문에 동적 라우팅 프로토콜을 통해 발견된 경로가 실패할 때 라우팅 테이블에 설치된 유동 고정 경로를 생성할 수 있습니다. 유동 고정 경로는 단순히 ASA에서 실행되는 동적 라우팅 프로토콜보다 큰 관리 거리로 설정된 고정 경로입니다. 동적 라우팅 프로세스가 발견한 해당 경로가 실패하면 라우팅 테이블에 고정 경로가 설치됩니다.

전달 결정 방법

전달 결정은 다음과 같이 이루어집니다.

- 대상이 라우팅 테이블 내의 엔트리와 일치하지 않으면 패킷이 기본 경로에 지정된 인터페이스를 통해 전달됩니다. 기본 경로가 구성되지 않은 경우 패킷이 버려집니다.
- 대상이 라우팅 테이블의 단일 엔트리와 일치하는 경우 패킷이 해당 경로와 연결된 인터페이스를 통해 전달됩니다.
- 대상이 라우팅 테이블에 있는 두 개 이상의 엔트리와 일치하고 엔트리의 네트워크 접두사 길이가 모두 같다면 네트워크 접두사가 같고 인터페이스가 다른 두 엔트리는 라우팅 테이블 내에 공존할 수 없습니다.
- 대상이 라우팅 테이블에 있는 두 개 이상의 엔트리와 일치하고 엔트리의 네트워크 접두사 길이가 다를 경우 패킷은 네트워크 접두사가 더 긴 경로와 연결된 인터페이스를 통해 전달됩니다.

예를 들어 목적지가 192.168.32.1인 패킷이 라우팅 테이블에서 다음 경로를 가진 ASA의 인터페이스에 도착합니다.

```
ciscoasa# show route
        ....
        R   192.168.32.0/24 [120/4] via 10.1.1.2
        O   192.168.32.0/19 [110/229840] via 10.1.1.3
        ....
```

이 경우 192.168.32.1이 192.168.32.0/24 네트워크 범위에 해당되기 때문에 목적지가 192.168.32.1인 패킷은 10.1.1.2로 전달됩니다. 라우팅 테이블 내 다른 경로에도 해당되지만 라우팅 테이블에서 192.168.32.0/24의 접두사가 가장 깁니다(24비트 vs. 19비트). 패킷을 전달할 때는 항상 더 긴 접두사가 우선합니다.

동적 라우팅 및 장애 조치

고정 라우팅 시스템은 네트워크 변화에 대응할 수 없기 때문에 꾸준히 변화하는 대규모 네트워크에는 일반적으로 적합하지 않습니다. 대부분의 주요 라우팅 알고리즘은 수신 라우팅 업데이트 메시지를 분석함으로써 네트워크 상황의 변화에 대응하는 동적 라우팅 알고리즘입니다. 메시지가 네트워크 변경 사실을 알리면 라우팅 소프트웨어가 경로를 다시 계산하고 새로운 라우팅 업데이트 메시지를 보냅니다. 이 메시지는 네트워크를 통과하며 라우터가 알고리즘을 다시 실행하고 라우팅 테이블을 그에 따라 변경하게 합니다.

동적 라우팅 알고리즘은 고정 경로로 적절히 보완할 수 있습니다. 예를 들어 최후의 수단으로 사용하는 라우터(모든 라우팅 불가 패킷이 전송되는 라우터)는 모든 라우팅 불가 패킷에 대한 저장소 역할을 하도록 지정되어 모든 메시지가 어떻게든 처리되도록 할 수 있습니다.

동적 경로는 활성 유닛의 라우팅 테이블이 변경될 때 스탠바이 유닛에서 동기화되므로 활성 유닛의 모든 추가, 삭제 또는 변경 사항은 대기 유닛에 즉시 전파됩니다. 기본 유닛이 활성화된 시간이 지나고 스탠바이 유닛이 활성화되면 장애 조치 일괄 동기화 프로세스의 일부로서 경로가 동기화되어 활성/스탠바이 장애 조치 쌍의 라우팅 테이블이 동시에 표시됩니다.

고정 경로와 그 구성 방법에 관한 자세한 정보는 20-2 페이지의 고정 경로 구성에서 참조하십시오.

동적 라우팅 및 클러스터링

동적 라우팅은 클러스터에서 완벽하게 통합되고 경로는 여러 유닛에서 공유됩니다(클러스터 하나에서 최대 8개 유닛이 허용됨). 라우팅 테이블 엔트리 또한 클러스터 내 유닛에서 복제됩니다.

유닛이 마스터에서 슬레이브로 전환되면 이 RIB 테이블에 대한 시대 번호(32비트 시퀀스 번호)가 증가합니다. 전환 후 처음에는 새 마스터 유닛이 이전 마스터 유닛의 미러 이미지인 RIB 테이블 엔트리를 갖습니다. 또한 새 마스터 유닛에서 리컨버전스 타이머가 시작됩니다. RIB 테이블의 시대 번호가 증가하면 모든 기존 엔트리가 오래된 항목으로 간주됩니다. IP 패킷의 전달은 정상적으로 계속됩니다. 새 마스터 유닛에서는 동적 라우팅 프로토콜이 시작되어 기존 경로 엔트리를 업데이트하거나 새 경로 엔트리를 새로운 시대 번호로 업데이트합니다. 수정된 엔트리나 새로운 엔트리에 최신 시대 번호가 있으면 엔트리가 갱신되어 모든 슬레이브 유닛에 동기화되었다는 뜻입니다. 리컨버전스 타이머가 만료된 후 RIB 테이블의 기존 엔트리가 삭제됩니다. OSPF 경로, RIP 경로 및 EIGRP 경로를 위한 RIB 테이블 엔트리가 슬레이브 유닛에 동기화됩니다.

일괄 동기화는 유닛이 클러스터에 참여하고 참여하는 유닛에 대한 마스터 유닛에서 온 경우에만 이루어집니다.

동적 라우팅 업데이트의 경우 마스터 유닛이 OSPF, RIP 또는 EIGRP를 통한 새 경로를 학습할 때, 마스터 유닛은 신뢰할 수 있는 메시지 전송을 통해 모든 슬레이브 유닛으로 업데이트를 보냅니다. 슬레이브 유닛은 클러스터 경로 업데이트 메시지를 받은 후 해당 RIB 테이블을 업데이트합니다.

지원되는 동적 라우팅 프로토콜(OSPF, EIGRP, RIP)의 경우 슬레이브 유닛에서 레이어 2 로드 밸런싱 인터페이스의 라우팅 패킷이 마스터 유닛에 전달됩니다. 마스터 유닛만 동적 라우팅 프로토콜 패킷을 보고 처리합니다. 슬레이브 유닛이 일괄 동기화를 요청하면 레이어 2 로드 밸런싱 인터페이스를 통해 학습된 모든 라우팅 엔트리가 복제됩니다.

마스터 유닛의 레이어 2 로드 밸런싱 인터페이스를 통해 새로운 라우팅 엔트리가 학습되면 새로운 엔트리가 모든 슬레이브 유닛으로 브로드캐스트됩니다. 기존 라우팅 엔트리가 네트워크 토폴로지 변경으로 인해 수정될 경우 수정된 엔트리는 모든 슬레이브 유닛에 동기화됩니다. 기존 라우팅 엔트리가 네트워크 토폴로지 변경으로 인해 삭제될 경우 삭제된 엔트리는 모든 슬레이브 유닛에 동기화됩니다.

레이어 2 및 레이어 3 로드 밸런싱 인터페이스의 조합이 배포되고 동적 라우팅을 위해 구성되면, 슬레이브 유닛은 라우팅 프로세스에서 부분적인 토폴로지 및 인접 디바이스 정보(레이어 3 로드 밸런싱 인터페이스를 통해 얻은 정보 포함)만 갖습니다. 레이어 2 로드 밸런싱 인터페이스에 대해 오직 RIB 테이블 엔트리만 마스터 유닛에서 동기화되기 때문입니다. 레이어 2 및 레이어 3가 다른 라우팅 프로세스에 속하도록 네트워크를 구성하고 각 라우팅 프로세스의 부하를 재분배해야 합니다.

표 19-2은(는) 지원되는 컨피그레이션에 대한 요약을 제공합니다. Yes는 두 프로세스의 조합(레이어 2와 레이어 3 프로세스 하나씩)이 작동함을 의미하고 No는 작동하지 않음을 의미합니다.

표 19-2 지원되는 구성 요약

레이어 2 또는 레이어 3	OSPF(레이어 3)	EIGRP(레이어 3)	RIP(레이어 3)
OSPF(레이어 2)	예	예	예
EIGRP(레이어 2)	예	아니요	예
RIP(레이어 2)	예	예	아니요

클러스터의 모든 유닛이 동일한 모드(단일 또는 다중 컨텍스트 모드)에 있어야 합니다. 다중 컨텍스트 모드에서는 마스터 슬레이브 동기화가 동기화 메시지의 모든 컨텍스트와 모든 컨텍스트의 RIB 테이블 엔트리를 포함합니다.

클러스터링에서는 레이어 3 인터페이스를 구성한 경우 라우터 ID 풀 설정도 구성해야 합니다.

동적 라우팅 및 클러스터링에 관한 자세한 내용은 9 장, “ASA 클러스터”.에서 참조하십시오.

다중 컨텍스트 모드의 동적 라우팅

다중 컨텍스트 모드에서 각 컨텍스트는 별도의 라우팅 테이블과 라우팅 프로토콜 데이터베이스를 유지합니다. 따라서 각 컨텍스트에서 OSPFv2 및 EIGRP를 독립적으로 구성할 수 있습니다. 일부 컨텍스트에서 EIGRP를 구성하고 동일 컨텍스트 또는 다른 컨텍스트에서 OSPFv2를 구성할 수 있습니다. 혼합 컨텍스트 모드에서 라우팅 모드의 컨텍스트에서 어떤 동적 라우팅 프로토콜이라도 활성화할 수 있습니다. RIP 및 OSPFv3는 다중 컨텍스트 모드에서 지원되지 않습니다.

다음 표는 EIGRP 특성, OSPFv2, OSPFv2 및 EIGRP 프로세스로 경로 배포를 위해 사용되는 경로 맵, 그리고 다중 컨텍스트 모드로 사용할 때 영역에 들어가거나 영역을 나가는 라우팅 업데이트를 필터링하기 위해 OSPFv2에서 사용하는 접두사 목록을 나열합니다.

EIGRP	OSPFv2	경로 맵 및 접두사 목록
컨텍스트당 하나의 인스턴스가 지원됩니다.	컨텍스트당 2개의 인스턴스가 지원됩니다.	N/A
시스템 컨텍스트에서 비활성화됩니다.		N/A
2개의 컨텍스트가 사용하는 자율 시스템 번호가 같을 수도 있고 다를 수도 있습니다.	2개의 컨텍스트가 사용하는 지역 ID가 같을 수도 있고 다를 수도 있습니다.	N/A
2개의 컨텍스트가 공유하는 인터페이스는 여러 EIGRP 인스턴스를 실행할 수도 있습니다.	2개의 컨텍스트가 공유하는 인터페이스는 여러 OSPF 인스턴스를 실행할 수도 있습니다.	N/A
공유 인터페이스 간 EIGRP 인스턴스의 상호 작용이 지원됩니다.	공유 인터페이스 간 OSPFv2 인스턴스의 상호 작용이 지원됩니다.	N/A
단일 모드에서 사용 가능한 모든 CLI는 다중 컨텍스트 모드에서도 사용 가능합니다.		
각 CLI는 그것이 사용되는 컨텍스트에만 영향을 미칠 수 있습니다.		

경로 리소스 관리

*경로*라고 하는 리소스 클래스가 도입되었고 컨텍스트에 존재할 수 있는 라우팅 테이블의 최대 개수를 지정합니다. 이것은 하나의 컨텍스트가 다른 컨텍스트의 가용 라우팅 테이블에 영향을 주는 문제를 해결하고 컨텍스트당 최대 경로 엔트리 수를 더욱 효과적으로 제어할 수 있게 합니다.

시스템 제한이 따로 정해지지 않았기 때문에 이 리소스 제한에 대한 절대값만 지정할 수 있습니다. 백분율 제한은 사용할 수 없습니다. 또한 컨텍스트당 최소 및 최대 제한이 없으므로 기본 클래스는 변경되지 않습니다. 컨텍스트에서 고정 또는 동적 라우팅 프로토콜(연결, 고정, OSPF, EIGRP 및 RIP)을 위한 새로운 경로를 추가할 경우 해당 컨텍스트의 리소스 제한에 도달했다면 경로 추가가 실패하고 syslog 메시지가 생성됩니다.

프록시 **ARP** 요청 비활성화

호스트가 같은 이더넷 네트워크의 다른 디바이스로 IP 트래픽을 전송하는 경우 호스트가 디바이스의 MAC 주소를 알아야 합니다. ARP는 IP 주소를 MAC 주소에 대해 확인하는 레이어 2 프로토콜입니다. 호스트는 ARP에 요청을 전송하여 IP 주소가 누구인지 묻고 해당 IP 주소를 소유한 디바이스가 자신이 IP 주소의 소유자라고 응답하고 MAC 주소를 알려주는 것입니다.

프록시 ARP는 디바이스가 해당 IP 주소를 소유하지 않더라도 자신의 MAC 주소로 ARP 요청에 응답할 때 사용됩니다. ASA은(는) NAT를 구성할 때 프록시 ARP를 사용하고 ASA 인터페이스와 같은 네트워크에 있는 매핑된 주소를 지정합니다. 트래픽이 호스트에 도달할 수 있는 유일한 방법은 ASA이(가) 프록시 ARP를 사용하여 MAC 주소가 주소에 매핑된 대상에 할당되어 있음을 주장하는 것입니다.

아주 드문 경우 NAT 주소에 대한 프록시 ARP를 비활성화할 수 있습니다.

기존 네트워크와 겹치는 VPN 클라이언트 주소 풀이 있는 경우 ASA은(는) 기본적으로 모든 인터페이스에서 프록시 ARP 요청을 전송합니다. 동일한 레이어 2 도메인에 다른 인터페이스가 있는 경우 이 인터페이스가 ARP 요청을 보고 인터페이스의 MAC 주소로 응답할 것입니다. 따라서 내부 호스트를 향한 VPN 클라이언트의 반환 트래픽이 잘못된 인터페이스로 전달되고 버려집니다. 이 경우 원치 않는 인터페이스에 대한 프록시 ARP 요청을 비활성화해야 합니다.

절차

1단계 **Configuration > Device Setup > Routing > Proxy ARP/Neighbor Discovery**를 선택합니다.

인터페이스 필드는 인터페이스 이름을 나열합니다. **Enabled** 필드는 NAT 글로벌 주소에 대한 프록시 ARP/인접 디바이스 검색이 활성화(Yes) 상태인지 비활성화(No) 상태인지 알려줍니다.

2단계 선택한 인터페이스에 대한 프록시 ARP/인접 디바이스 검색을 활성화하려면 **Enable**을 클릭합니다. 기본적으로 프록시 ARP/인접 디바이스 검색은 모든 인터페이스에서 활성화되어 있습니다.

3단계 선택한 인터페이스에 대한 프록시 ARP/인접 디바이스 검색을 비활성화하려면 **Disable**을 클릭합니다.

4단계 **Apply**를 클릭하여 설정을 실행 중인 컨피그레이션에 저장합니다.

20장

고정 경로 및 기본 경로

이 장에서는 Cisco ASA에서 고정 경로와 기본 경로를 구성하는 방법을 설명합니다.

고정 경로 및 기본 경로 정보

트래픽을 연결되지 않은 호스트 또는 네트워크로 라우팅하려면 호스트 또는 네트워크로의 고정 경로를 정의해야 합니다. 또는 최소한 ASA이(가) 직접 연결되지 않은 네트워크에 대한 기본 경로를 정의해야 합니다(예: 네트워크와 ASA 사이에 라우터가 있는 경우).

고정 경로 또는 기본 경로가 정의되지 않은 경우 연결되지 않은 호스트 또는 네트워크로의 트래픽에서 다음 syslog 메시지가 생성됩니다.

```
%ASA-6-110001: No route to dest_address from source_address
```

다음의 경우 단일 컨텍스트 모드의 고정 경로를 사용할 수 있습니다.

- 네트워크가 EIGRP, RIP 또는 OSPF에서 다른 라우터 검색 프로토콜을 사용합니다.
- 네트워크 규모가 작고 고정 경로를 쉽게 관리할 수 있습니다.
- 트래픽이나 CPU 오버헤드를 라우팅 프로토콜과 연결하지 않는 것이 좋습니다.

가장 간단한 옵션은 트래픽을 라우팅하는 라우터에 의존하여 모든 트래픽을 업스트림 라우터로 보내는 기본 경로를 구성하는 것입니다. 그러나 기본 게이트웨이가 대상 네트워크에 도달할 수 없는 경우가 있기 때문에 보다 구체적인 고정 경로도 구성해야 합니다. 예를 들어 기본 게이트웨이가 밖에 있는 경우 기본 경로는 ASA에 직접 연결되지 않은 내부 네트워크로 트래픽을 안내할 수 없습니다.

투명 방화벽 모드에서는 ASA에서 발생하고 직접 연결되지 않은 네트워크가 목적지인 트래픽에 대해 기본 경로 또는 고정 경로를 구성하여 ASA이(가) 어떤 인터페이스로 트래픽을 보낼지 알 수 있도록 해야 합니다. ASA에서 발생하는 트래픽은 syslog 서버, Websense 또는 N2H2 서버나 AAA 서버로의 통신을 포함할 수 있습니다. 단일 기본 경로를 통해 모두 도달할 수 없는 서버가 있다면 고정 경로를 구성해야 합니다. 또한 ASA은 로드 밸런싱을 위해 동일 인터페이스에서 최대 3개의 동일 비용 경로를 지원합니다.

고정 경로 및 기본 경로를 위한 지침

장애 조치 지침

동적 라우팅 프로토콜의 상태 기반 장애 조치를 지원합니다.

추가 지침

- IPv6 고정 경로는 ASDM의 투명 모드에서 지원되지 않습니다.
- 클러스터링에서 고정 경로 모니터링은 마스터 유닛에서만 지원됩니다. 클러스터링에 대한 내용은 9 장, “ASA 클러스터”.을(를) 참고하십시오.

고정 경로 구성

고정 라우팅 알고리즘은 기본적으로 네트워크 관리자가 라우팅 시작 전에 설정한 테이블 매핑입니다. 이러한 매핑은 네트워크 관리자가 변경하지 않는 한 변경되지 않습니다. 고정 경로를 사용하는 알고리즘은 설계하기가 쉽고 네트워크 트래픽을 상대적으로 예측하기 쉬운 환경과 네트워크 설계가 상대적으로 단순한 환경에서 효과적입니다. 이러한 이유로 고정 라우팅 시스템은 네트워크 상의 변화에 대처할 수 없습니다.

고정 경로는 지정된 게이트웨이를 사용할 수 없게 되더라도 라우팅 테이블에서 유지됩니다. 지정된 게이트웨이를 사용할 수 없게 되면 라우팅 테이블에서 고정 경로를 수동으로 제거해야 합니다. 그러나 고정 경로는 지정된 인터페이스가 다운될 경우 라우팅 테이블에서 제거되고 인터페이스가 복구되면 재개됩니다.

참고 ASA에서 실행 중인 라우팅 프로토콜보다 관리 거리가 큰 고정 경로를 만드는 경우 라우팅 프로토콜로 검색된 지정된 경로로의 경로가 고정 경로보다 우선합니다. 고정 경로는 동적으로 검색된 경로가 라우팅 테이블에서 제거된 경우에만 사용됩니다.

인터페이스당 도일 대상에 대하여 최대 3개의 동일 비용 경로를 정의할 수 있습니다.
ECMP(equal-cost multipath)는 여러 인터페이스에 걸쳐 지원되지 않습니다. ECMP를 사용하면 트래픽이 경로 간에 고르게 분할되지 않을 수도 있습니다. 트래픽은 소스와 대상 IP 주소를 해싱하는 알고리즘을 기반으로 지정된 게이트웨이 사이에서 분배됩니다.

고정 null0 경로 컨피그레이션

ACL은 일반적으로 트래픽 필터링에 사용되며 헤더에 포함된 정보에 기초하여 패킷을 필터링할 수 있습니다. 패킷 필터링에서 ASA 방화벽은 패킷 헤더를 검사하여 필터링 결정을 내리고 패킷 처리에 오버헤드를 추가함으로써 성능에 영향을 줍니다.

고정 null 0 라우팅은 필터링을 보완하는 솔루션입니다. 고정 null0 경로는 black hole로 원하지 않거나 바람직하지 않은 트래픽을 전달하는 데 사용됩니다. null 인터페이스 null0은 black hole 생성에 사용됩니다. 고정 경로는 바람직하지 않은 대상에 대해 생성되며 고정 경로 컨피그레이션은 null 인터페이스를 향합니다. black hole 고정 경로와의 최적의 일치를 포함한 대상 주소의 트래픽은 자동으로 삭제됩니다. ACL과는 달리 고정 null0 경로는 성능 저하를 일으키지 않습니다.

고정 null0 경로 컨피그레이션은 라우팅 루프를 방지하는 데 사용됩니다. BGP는 Remotely Triggered Black Hole 라우팅을 위해 고정 null0 컨피그레이션을 활용합니다.

예:

```
route null0 192.168.2.0 255.255.255.0
```

고정 경로를 구성하려면 다음 중 하나를 선택하십시오.

- 20-3 페이지의 고정 경로 추가 또는 편집
- 20-5 페이지의 고정 경로 추적 구성
- 20-6 페이지의 고정 경로 삭제

고정 경로 추가 또는 편집

절차

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Static Routes**를 선택합니다.

2단계 다음 라디오 버튼 중 하나를 클릭하여 필터링할 경로를 선택합니다.

- **Both**(IPv4 및 IPv6를 모두 필터링)
- **IPv4만**
- **IPv6만**

기본적으로 두 라디오 버튼이 모두 선택되어 있고 단추를 IPv4와 IPv6 모두 창에 표시됩니다. 선택 보기를 IPv4 주소로 구성된 경로로 제한하려면 **IPv4** 라디오 버튼을 클릭합니다. 선택 보기를 IPv6 주소로 구성된 경로로 제한하려면 **IPv6** 라디오 버튼을 클릭합니다.

3단계 **Add** 또는 **Edit**를 클릭합니다.

Add or Edit Static Route 대화 상자가 나타납니다.

4단계 인터페이스 드롭다운 목록에서 Interface 필드에서 활성화된 내부 또는 외부 네트워크 인터페이스 이름을 선택합니다.

- **management**(내부 인터페이스)
- **outside**(외부 인터페이스)

5단계 IP Address 필드에서 대상 네트워크에 대한 내부 또는 외부 네트워크 IP 주소를 입력합니다.

IPv4 주소의 경우 **0.0.0.0**을 입력하여 기본 경로를 지정합니다. 0.0.0.0 IP 주소는 0으로 축약할 수 있습니다. 생략 보기를 클릭하여 주소를 찾아볼 수도 있습니다.

IPv6 주소의 경우 2개의 콜론(**::**)을 입력하여 기본 경로를 지정합니다. 생략 보기를 클릭하여 주소를 찾아볼 수도 있습니다.

6단계 Gateway IP 필드에 이 경로의 다음 홉 주소인 게이트웨이 라우터의 IP 주소를 입력합니다.

기본 경로를 입력하려면 IP 주소와 마스크를 **0.0.0.0** 또는 축약된 형태인 **0**으로 설정합니다.

생략 보기를 클릭하여 주소를 찾아볼 수도 있습니다.

참고 1개의 ASA인터페이스에서 IP 주소가 게이트웨이 IP 주소로 사용되는 경우 ASA은(는) 게이트웨이 IP 주소가 아니라 패킷의 지정된 IP 주소를 ARPing합니다.

사용자가 고정 경로에 대해 지정하는 주소는 ASA을(를) 입력하고 NAT를 수행하기 전에 패킷에 존재하는 주소입니다.

7단계 대상 네트워크에 대한 드롭다운 목록에서 넷마스크를 선택합니다. 필터링할 경로에 따라(IPv4, IPv6 또는 둘 다) 다음 중 하나를 수행합니다.

- IPv4 고정 경로의 경우(또는 IPv4 및 IPv6 고정 경로 모두) IP 주소에 해당되는 네트워크 마스크 주소를 입력합니다. **0.0.0.0**을 입력하여 기본 경로를 지정합니다. **0.0.0.0** 넷마스크는 **0**으로 축약할 수 있습니다.
- IPv6 고정 경로의 경우 접두사 길이를 입력합니다.

8단계 메트릭 필드에서 메트릭 또는 관리 거리를 입력합니다.

메트릭 또는 거리는 경로에 대한 관리 거리입니다. 값을 지정하지 않으면 기본값은 1입니다. 관리 거리는 서로 다른 라우팅 프로토콜의 경로를 비교하는 데 사용되는 매개변수입니다. 고정 경로에서 기본 관리 거리는 1이므로 동적 라우팅 프로토콜로 검색되었으나 경로에 직접 연결되지 않은 경로보다 우선합니다.

OSPF가 발견한 경로에 대한 기본 관리 거리는 110입니다. 고정 경로의 관리 거리가 동적 경로와 같다면 고정 경로가 우선합니다. 연결된 경로가 항상 고정 경로 또는 동적으로 발견된 경로보다 우선합니다.

9단계 (선택 사항) Options 영역에서 고정 경로에 대해 다음 옵션 중 하나를 선택합니다.

- **None**: 고정 경로에 대해 아무런 옵션도 지정하지 않습니다. 이는 기본 설정입니다.
- **Tunneled**: VPN 트래픽에 대한 기본 터널 게이트웨이로 경로를 지정합니다. 이 설정은 기본 경로에만 사용됩니다. 디바이스당 하나의 터널링 경로만 구성할 수 있습니다. 터널링 옵션은 투명 모드에서 지원되지 않습니다.
- **Tracked**: 경로를 추적합니다. 추적 객체 ID와 추적 대상에의 주소도 표시됩니다. 추적 옵션은 단일 라우팅 모드에서만 지원됩니다. 추적 옵션에 대해 다음 설정을 지정합니다.
  - Track ID 필드에 경로 추적 프로세스를 위한 고유한 식별자를 입력합니다.
  - Track IP Address/DNS Name 필드에 추적 대상의 IP 주소 또는 호스트 이름을 입력합니다. 일반적으로 이것은 경로의 다음 홉 게이트웨이 IP 주소이지만 해당 인터페이스에서 제공하는 어떤 네트워크 객체라도 될 수 있습니다.
  - SLA ID 필드에 SLA 모니터링 프로세스를 위한 고유한 식별자를 입력합니다.

참고 추적 옵션은 IPv6에 대해 지원되지 않습니다.

10단계 (선택 사항) **Monitoring Options**를 클릭합니다.

Route Monitoring Options 대화 상자가 나타납니다. 여기에서 다음 추적 객체 모니터링 속성을 변경합니다.

- 빈도는 ASA이(가) 추적 대상의 존재를 얼마나 자주 테스트할지 초 단위로 지정할 수 있습니다. 유효한 값은 1~604800초입니다. 기본값은 60초입니다.
- 임계값에는 임계값을 넘기는 이벤트를 나타내는 시간을 밀리초 단위로 입력할 수 있습니다. 이 값은 시간 초과 값보다 클 수 없습니다.
- 시간 초과는 경로 모니터링 작업이 요청 패킷으로부터 응답을 기다릴 시간을 밀리초 단위로 지정할 수 있습니다. 유효한 값은 0~604800000밀리초입니다. 기본값은 5000밀리초입니다.

- 데이터 크기는 에코 요청 패킷에 사용할 데이터 페이로드의 크기를 수정할 수 있습니다. 기본값은 28입니다. 유효한 값 범위는 0~16384입니다.

  참고 이 설정은 페이로드의 크기만 지정하며 전체 패킷의 크기는 지정하지 않습니다.

- ToS는 에코 요청의 IP 헤더에서 서비스 유형 바이트에 대한 값을 선택할 수 있습니다. 유효한 값은 0부터 255까지입니다. 기본값은 0입니다.
- 패킷 수는 각 테스트에 대해 전송되는 에코 요청의 횟수를 선택할 수 있습니다. 유효한 값 범위는 1~100입니다. 기본값은 1입니다.

11단계 **OK**를 클릭합니다.

12단계 **Apply**를 클릭하여 컨피그레이션을 저장합니다.

추가 또는 편집된 경로 정보는 Static Route 창에 나타납니다. 새로 구성된 경로를 저장하자마자 모니터링 프로세스가 시작됩니다.

고정 경로 추적 구성

절차

참고 고정 경로 추적은 IPv4 경로에 대해서만 이용 가능합니다.

1단계 관련 대상을 선택합니다. 대상이 에코 요청에 반드시 응답하도록 해야 합니다.

2단계 **Configuration > Device Setup > Routing > Static Routes**를 클릭하여 Static Routes 창을 엽니다.

3단계 **Add**를 클릭하여 선택한 관련 대상의 가용성을 기준으로 사용될 고정 경로를 구성합니다. 이 경로에 대한 인터페이스, IP 주소, 마스크, 게이트웨이 및 메트릭 설정을 입력해야 합니다.

4단계 Options 영역에서 이 경로에 대한 **Tracked** 라디오 버튼을 클릭합니다.

5단계 추적 속성을 구성합니다. 관련 대상의 고유한 추적 ID, 고유한 SLA ID와 IP 주소를 입력해야 합니다.

6단계 (선택 사항) 모니터링 속성을 구성하려면 Add Static Route 대화 상자에서 **Monitoring Options**를 클릭합니다.

7단계 **OK**를 클릭하여 변경 사항을 저장합니다.

추적 경로를 새로 저장하자마자 모니터링 프로세스가 시작됩니다.

8단계 단계 1에서 7까지를 반복함으로써 2차 경로를 만듭니다.

2차 경로는 추적 경로와 대상은 같지만 다른 인터페이스 또는 게이트웨이를 통하는 경로입니다. 이 경로에는 추적 경로보다 높은 관리 거리(메트릭)를 할당해야 합니다.

9단계 **OK**를 클릭하여 변경 사항을 저장합니다.

고정 경로 삭제

절차

1단계 **Configuration > Device Setup > Routing > Static Routes**를 선택합니다.

2단계 Static Route 창에서 삭제할 경로를 선택합니다.

기본적으로 Both 라디오 버튼이 모두 선택되어 있고 단추를 IPv4와 IPv6 모두 창에 표시됩니다.

- 선택 보기를 IPv4 주소로 구성된 경로로 제한하려면 **IPv4** 라디오 버튼을 클릭합니다.
- 선택 보기를 IPv6 주소로 구성된 경로로 제한하려면 **IPv6** 라디오 버튼을 클릭합니다.

3단계 **삭제**를 클릭합니다.

삭제 경로가 메인 Static Route 창의 경로 목록에서 제거됩니다.

4단계 **Apply**를 클릭하여 컨피그레이션에 변경 사항을 저장합니다.

기본 고정 경로 구성

기본 고정 경로는 ASA이(가) 학습 경로나 고정 경로를 가지고 있지 않은 모든 IP 패킷을 보낼 게이트웨이 IP 주소를 식별합니다. 기본 고정 경로는 단순히 대상 IP 주소가 0.0.0.0/0인 고정 경로입니다. 특정 대상을 식별하는 경로가 기본 경로보다 우선합니다.

참고 버전 7.0(1) 이상에서는 메트릭이 서로 다른 인터페이스에서 2개의 기본 경로를 구성한 경우 더 높은 메트릭 인터페이스에서 ASA(으)로의 연결은 실패하지만 낮은 메트릭에서 ASA(으)로의 연결은 예상대로 성공합니다.

디바이스당 최대 3개의 동일 비용 기본 경로 엔트리를 정의할 수 있습니다. 동일 비용 기본 경로 엔트리를 하나 이상 정의하면 기본 경로로 전송되는 트래픽이 지정된 게이트웨이 사이에서 분산될 수 있습니다. 기본 경로를 하나 이상 정의할 경우 각 엔트리에 대해 동일한 인터페이스를 지정해야 합니다.

3개 이상의 동일 비용 기본 경로 또는 이전에 정의된 기본 경로와 인터페이스가 다른 기본 경로를 정의하려고 하면 다음 메시지가 표시됩니다.

```
"ERROR: Cannot add route entry, possible conflict with existing routes."
```

표준 기본 경로를 가지고 터널링된 트래픽을 위한 별도의 기본 경로를 정의할 수 있습니다. 터널링 옵션으로 기본 경로를 생성하면 학습 경로나 고정 경로를 이용하여 라우팅할 수 없는 ASA에서 종료되는 터널의 모든 트래픽이 이 경로로 전송됩니다. 터널에서 발생하는 트래픽에 대하여 이 경로는 다른 구성된 기본 경로나 학습된 기본 경로를 무시합니다.

기본 고정 경로 설정 구성 제한 사항

터널링 옵션을 포함한 기본 경로에는 다음 제한 사항이 적용됩니다.

- 터널링 경로의 이그레스 인터페이스에서 유니캐스트 RPF(**ip verify reverse-path** 명령)를 활성화하지 마십시오. 이 설정 때문에 세션이 실패할 수 있습니다.

- 터널링 경로의 이그레스 인터페이스에서 TCP 인터셉트를 활성화하지 마십시오. 이 설정 때문에 세션이 실패할 수 있습니다.
- VoIP 검사 엔진(CTIQBE, H.323, GTP, MGCP, RTSP, SIP, SKINNY), DNS 검사 엔진 또는 DCE RPC 검사 엔진을 터널링 경로에 사용하지 마십시오. 이러한 검사 엔진은 터널링 경로를 무시하기 때문입니다.
- 터널링 옵션에서 두 개 이상의 기본 경로를 정의할 수 없습니다.
- 터널링 트래픽에 대한 ECMP는 지원되지 않습니다.

절차

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Static Routes**를 선택합니다.

2단계 **Add** 또는 **Edit**를 클릭합니다.

3단계 Options 영역에서 **Tunneled**를 선택합니다.

4단계 **OK**를 클릭합니다.

IPv6 기본 및 고정 경로 구성

호스트가 연결되고 IPv6 및 IPv6 ACL에 대해 활성화된 인터페이스가 트래픽을 허용할 경우 ASA은(는) 자동으로 직접 연결된 호스트 사이에 IPv6 트래픽을 라우팅합니다.

절차

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Static Routes**를 선택합니다.

2단계 **IPv6 only** 라디오 버튼을 클릭합니다.

3단계 **Add** 또는 **Edit**를 클릭합니다.

4단계 **OK**를 클릭합니다.

고정 또는 기본 경로 모니터링

고정 경로의 문제 중 하나는 경로가 정상인지 다운되었는지 확인할 수 있는 내재적인 메커니즘이 없다는 것입니다. 다음 홉 게이트웨이가 사용할 수 없게 되어도 라우팅 테이블에 남습니다. 고정 경로는 ASA의 연결된 인터페이스가 다운되는 경우에만 라우팅 테이블에서 제거됩니다.

고정 경로 추적 기능은 고정 경로의 가용성을 추적하고 기본 경로가 실패할 경우 보조 경로를 설치하는 수단을 제공합니다. 예를 들어 기본 ISP를 사용할 수 없는 경우에 대비하여 ISP 게이트웨이로의 기본 경로와 보조 ISP로의 보조 기본 경로를 정의할 수 있습니다.

ASA은(는) 사용자가 정의하는 모니터링 대상과 고정 경로를 연결하여 이 기능을 실행하고 ICMP 에코 요청을 사용하여 대상을 모니터링합니다. 에코 응답이 지정된 시간 동안 수신되지 않으면 객체는 다운된 것으로 간주되며 연결된 경로가 라우팅 테이블에서 제거됩니다. 이전에 구성된 백업 경로가 삭제된 경로의 자리에 사용됩니다.

모니터링 대상을 선택할 때, ICMP 에코 요청에 응답할 수 있는지 확인해야 합니다. 대상은 사용자가 선택하는 아무 네트워크 객체나 될 수 있지만 다음을 사용할 것을 고려해야 합니다.

- ISP 게이트웨이(이중 ISP 지원) 주소
- 다음 홉 게이트웨이 주소(게이트웨이의 가용성이 우려되는 경우)
- AAA 서버와 같이 ASA이(가) 통신해야 하는 대상 네트워크에 있는 서버
- 대상 네트워크에 있는 지속적인 네트워크 객체

참고 저녁에 전원이 꺼지는 데스크톱이나 노트북 컴퓨터는 좋은 선택이 아닙니다.

DHCP 나 PPPoE를 통해 얻은 고정으로 정의된 경로나 기본 경로를 위해 고정 경로 추적을 구성할 수 있습니다. 경로 추적이 구성된 여러 인터페이스에서만 PPPoE 클라이언트를 활성화할 수 있습니다.

절차

1단계 **Monitoring > Routing > Routes**를 선택합니다.

경로 창에서 각 행은 하나의 경로를 나타냅니다. IPv4 연결, IPv6 연결 또는 두 연결 방식으로 필터링할 수 있습니다. 라우팅 정보에는 프로토콜, 경로 유형, 대상 IP 주소, 넷마스크 또는 접두사 길이, 게이트웨이 IP 주소, 경로가 연결되는 인터페이스, 그리고 관리 거리가 포함됩니다.

2단계 현재 목록을 업데이트하려면 **Refresh**를 클릭합니다.

고정 또는 기본 경로의 예

다음 예는 라우터 10.1.2.45에 10.1.1.0/24가 목적지인 모든 트래픽을 보내는 고정 경로 생성 방법을 보여줍니다. 이 라우터는 내부 인터페이스에 연결되어 있고 트래픽을 외부 인터페이스의 3가지 게이트웨이로 안내하는 동일 비용 고정 경로 3개를 정의하며 터널링 트래픽에 기본 경로를 추가합니다. ASA은(는) 지정된 게이트웨이 간에 트래픽을 배포합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Static Routes**를 선택합니다.

2단계 Interfaces 드롭다운 목록에서 **Management**를 선택합니다.

3단계 IP Address 필드에 **10.1.1.0**을 입력합니다.

4단계 Mask 드롭다운 목록에서 **255.255.255.0**을 선택합니다.

5단계 Gateway IP 필드에 **10.1.2.45 1**을 입력합니다.

내부 인터페이스에 연결된 라우터(10.1.2.45)에 10.1.1.0/24가 목적지인 모든 트래픽을 보내는 고정 경로가 생성됩니다.

6단계 **OK**를 클릭합니다.

7단계 **Configuration > Device Setup > Routing > Static Routes**를 선택합니다.

8단계 **Add**를 클릭합니다.

9단계 IP Address 필드에 대상 네트워크의 IP 주소를 입력합니다.

이 경우 경로 IP 주소는 192.168.2.1, 192.168.2.2, 192.168.2.3 및 192.168.2.4입니다. 192.168.2.4를 추가할 때는 Options 영역에서 **Tunneled** 라디오 버튼을 클릭하십시오.

10단계 다음 홉 라우터의 주소로 Gateway IP Address 필드에 게이트웨이 IP 주소를 입력합니다.

사용자가 고정 경로에 대해 지정하는 주소는 ASA을(를) 입력하고 NAT를 수행하기 전에 패킷에 존재하는 주소입니다.

11단계 NetMask 드롭다운 목록에서 대상 네트워크에 대한 넷마스크를 선택합니다.

12단계 **OK**를 클릭합니다.

고정 경로 및 기본 경로 내역

ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 20-1 고정 경로 및 기본 경로 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
라우팅	7.0(1)	고정 및 기본 경로를 도입했습니다. 다음 화면을 도입했습니다. Configuration > Device Setup > Routing.
클러스터링	9.0(1)	마스터 유닛에서만 고정 경로 모니터링을 지원합니다.
고정 null0 경로 컨피그레이션	9.2(1)	Null0 인터페이스로 트래픽을 보내면 지정된 네트워크로 향하는 패킷이 드롭될 수 있습니다. 이 기능은 BGP를 위한 RTBH(Remotely Triggered Black Hole)를 구성할 때 유용합니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Routing > Static Routes> Add > Add Static Route

21 장

경로 맵

경로 맵 정보

경로 맵은 경로를OSPF, RIP, EIGRP 또는 BGP 라우팅 프로세스로 재배포할 때 사용됩니다. 또한 OSPF 라우팅 프로세스로 기본 경로를 생성할 때도 사용됩니다. 경로 맵은 지정된 라우팅 프로토콜에서 대상 라우팅 프로세스로 재배포를 허용할 경로를 정의합니다.

경로 맵은 널리 알려진 ACL과 여러 기능을 공유합니다. 다음은 두 가지에서 모두 일반적인 특성입니다.

- 이들은 순서가 정해진 개별 구문으로 각각 허용 또는 거부라는 결과를 갖습니다. ACL 또는 경로 맵의 평가는 미리 정의된 순서에 따른 목록 스캔과 그에 일치하는 각 구문의 기준에 대한 평가로 구성됩니다. 목록 스캔은 첫 번째 구문 일치가 발견되고 해당 구문 일치와 연결된 작업이 수행되면 중단됩니다.
- 일반 메커니즘 - 기준 일치와 일치 해석은 적용 방식에 따라 정해집니다. 같은 경로 맵이라도 다른 작업에 적용되면 다르게 해석될 수 있습니다.

다음은 경로 맵과 ACL의 차이점입니다.

- 경로 맵은 자주 ACL을 일치 기준으로 사용합니다.
- ACL 평가의 주된 결과는 예/아니요 응답입니다. ACL은 입력 데이터를 허용하거나 거부합니다. 재배포에 적용할 경우 ACL은 특정 경로를 재배포할 수 있는지(경로가 ACL 허용 구문과 일치) 아니면 재배포할 수 없는지(거부 구문과 일치) 결정합니다. 일반적인 경로 맵은 재배포된 경로를 허용할 뿐만 아니라 다른 프로토콜로 재배포될 때 경로와 연결된 정보를 수정하기도 합니다.
- 경로 맵은 ACL보다 유연하며 ACL이 확인할 수 없는 기준으로 경로를 확인할 수 있습니다. 예를 들어 경로 맵은 경로 유형이 내부인지 확인할 수 있습니다.

- 각 ACL은 설계 관행에 따라 암시적 거부 문구로 종료됩니다. 경로 맵에 대해서는 이런 관행이 없습니다. 일치 시도 중에 경로 맵의 끝에 도달하는 경우 결과는 경로 맵의 애플리케이션이 무엇인지에 따라 달라집니다. 다행히도 재배포에 적용되는 경로 맵은 ACL과 동일하게 작동합니다. 경로가 경로 맵의 조항과 일치하지 않으면 마치 경로 맵이 끝에 거부 구문을 포함한 것처럼 경로 재배포가 거부됩니다.

동적 **redistribute** 명령을 통해 경로 맵을 적용할 수 있습니다. Cisco ASDM에서 이 재배포 기능은 새로운 경로 맵을 추가하거나 편집할 때 발견할 수 있습니다(21-4 페이지의 경로 맵을 정의 참조). 재배포 중 경로 정보를 수정하려거나 ACL이 제공할 수 있는 것보다 강력한 일치 기능을 원할 경우 경로 맵이 선호됩니다. 단순히 접두사나 마스크를 기준으로 경로를 선택적으로 허용하려는 경우 경로 맵을 사용하여 **redistribute** 명령에서 직접 ACL(또는 동등한 접두사 목록)로 매핑할 것을 추천합니다. 접두사나 마스크를 기준으로 경로를 선택적으로 허용하기 위해 경로 맵을 사용하는 경우 같은 목적을 달성하기 위해 일반적으로 더 많은 컨피그레이션 명령을 사용하게 됩니다.

참고 경로 맵에 대한 일치 기준으로 표준 ACL을 사용해야 합니다. 확장 ACL을 사용하면 효과가 없으며 경로가 재배포되지 않을 것입니다. 나중에 절을 추가해야 할 경우에 대비하여 10 간격의 숫자 절을 추천합니다.

- 21-2 페이지의 허용 및 거부 절
- 21-2 페이지의 절의 일치 및 설정 값
- 21-3 페이지의 BGP 일치 및 BGP 설정 절

허용 및 거부 절

경로 맵은 허용 및 거부 절을 가질 수 있습니다. **route-map ospf-to-eigrp** 명령에는 하나의 거부 절(순차 번호 10)과 두 개의 허용 절이 있습니다. 거부 절은 재배포에서 경로 일치를 거부합니다. 따라서 다음 규칙이 적용됩니다.

- 허용 절을 사용하는 경로 맵에서 ACL을 사용할 경우 ACL이 허용한 경로가 재배포됩니다.
- 경로 맵 거부 절에서 ACL을 사용할 경우 ACL이 허용한 경로가 재배포되지 않습니다.
- 경로 맵 허용 또는 거부 절에서 ACL을 사용하고 ACL이 경로를 거부할 경우 경로 맵 절 일치 항목이 발견되지 않고 다음 경로 맵 절이 평가됩니다.

절의 일치 및 설정 값

각 경로 맵 절은 두 가지 값을 갖습니다.

- 일치 값은 이 절을 적용할 경로를 선택합니다.
- 설정 값은 대상 프로토콜로 재배포될 정보를 수정합니다.

재배포되는 각 경로에 대해 라우터는 먼저 경로 맵에 있는 절의 일치 기준을 평가합니다. 일치 기준이 성공하면 허용 또는 거부 절에 따라 경로가 재배포되거나 거부되고 ASDM의 Set Value 탭 또는 **set** 명령에서 설정된 값으로 일부 속성이 수정될 수 있습니다. 일치 기준이 실패하면 이 절은 경로에 적용되지 않고 소프트웨어가 경로 맵의 다음 절에 대해 경로를 평가합니다. **match** 명령 또는 ASDM의 Match Clause 탭에 설정된 Match Clause가 경로와 일치하거나 경로 맵의 끝에 도달할 때까지 경로 맵 검색이 계속됩니다.

다음 조건 중 하나가 존재할 경우 각 절의 일치 또는 설정 값은 누락되거나 여러 번 반복될 수 있습니다.

- 절에 여러 **match** 명령 또는 ASDM의 Match Clause 값이 존재하는 경우 주어진 경로에 대해 모두 성공해야 경로가 절에 일치할 수 있습니다(논리 AND 알고리즘이 여러 일치 명령에 적용됨).
- ASDM에서 **match** 명령 또는 Match Clause 값이 하나의 명령에서 여러 객체를 참조하는 경우 둘 중 하나가 일치합니다(논리 OR 알고리즘 적용). 예를 들어 **match ip address 101 121** 명령에서 ACL 101 또는 ACL 121이 허용할 경우 경로가 허용됩니다.
- **match** 명령이나 ASDM의 Match Clause 값이 없는 경우 모든 경로가 절에 일치합니다. 이전 예제에서 절 30에 도달하는 모든 경로가 일치하고 경로 맵의 끝에 도달하지 않습니다.
- 경로 맵 허용 절에 **set** 명령 또는 ASDM의 Set Value 값이 없는 경우 현재 속성의 수정 없이 경로가 재배포됩니다.

참고 경로 맵의 **set** 명령이 절을 거부하도록 구성하지 마십시오. 거부 절은 경로 재배포를 금지하므로 수정할 정보가 없기 때문입니다.

match 또는 **set** 명령 또는 ASDM의 Match or Set Value 탭에 설정된 Match 또는 Set Value가 없는 경로 맵의 경우 작업을 수행합니다. 빈 허용 절은 수정 없이 남은 경로의 재배포를 허용합니다. 빈 거부 절은 다른 경로의 재배포를 허용하지 않습니다(경로 맵을 완전히 스캔했으나 정확한 일치 항목을 찾지 못한 경우 이것이 기본 작업).

BGP 일치 및 BGP 설정 절

위에 설명한 일치 및 설정 값 외에 BGP는 경로 맵에 대한 추가 일치 및 설정 기능을 제공합니다.

다음 새로운 경로-맵 일치 절은 BGP에서 지원됩니다.

- match as-path
- match community
- match policy-list
- match tag

다음 새로운 경로-맵 설정치 절은 BGP에서 지원됩니다.

- set as-path
- set automatic-tag
- set community
- set local-preference
- set origin
- set weight

재배포되는 각 BGP 경로에 대해 ASA는 먼저 경로 맵에 있는 절의 BGP 일치 기준을 평가합니다. BGP 일치 기준이 성공하면 허용 또는 거부 절에 따라 경로가 재배포되거나 거부되고 ASDM의 BGP Set Clause 탭 또는 **set** 명령에서 설정된 값으로 일부 속성이 수정될 수 있습니다. 일치 기준이 실패하면 이 절은 경로에 적용되지 않고 소프트웨어가 경로 맵의 다음 절에 대해 경로를 평가합니다. **match** 명령 또는 ASDM의 BGP Match Clause 탭에 설정된 Match Clause가 경로와 일치하거나 경로 맵의 끝에 도달할 때까지 경로 맵 검색이 계속됩니다.

경로 맵에 대한 지침

방화벽 모드

라우팅된 방화벽 모드에서만 지원됩니다. 투명한 방화벽 모드는 지원되지 않습니다.

추가 지침

경로 맵은 사용자, 사용자 그룹 또는 정규화된 도메인 이름 객체를 포함하는 ACL을 지원하지 않습니다.

경로 맵을 정의

지정된 라우팅 프로토콜에서 대상 라우팅 프로세스로 재배포를 허용할 경로를 지정할 때 경로 맵을 정의해야 합니다. ASDM에서는 경로 맵 이름, 순차 번호 또는 재배포를 추가, 편집 또는 삭제함으로써 경로 맵을 정의할 수 있습니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > Route Maps**를 선택합니다.

2단계 **Add**를 클릭합니다.

Add Route Map 또는 Edit Route Map 대화 상자가 나타납니다.

3단계 경로 맵 이름과 시퀀스 번호를 입력합니다. 경로 맵 이름은 특정 경로에 할당하는 이름입니다. 순차 번호는 경로 맵 엔트리를 ASA에 추가하거나 삭제하는 순서입니다.

참고 기존 경로 맵을 수정하는 경우 경로 맵 이름과 순차 번호에 대한 필드는 미리 작성되어 있습니다.

4단계 경로 일치 항목 재배포를 거부하려면 **Deny**를 클릭합니다. 경로 맵 거부 절에서 ACL을 사용할 경우 ACL이 허용한 경로가 재배포되지 않습니다. 재배포에 대한 경로 일치를 허용하려면 **Permit**을 클릭합니다. 경로 맵 허용 절에서 ACL을 사용할 경우 ACL이 허용한 경로가 재배포됩니다.

또한 경로 맵 허용 또는 거부 절에서 ACL을 사용하고 ACL이 경로를 거부할 경우 경로 맵 절 일치 항목이 발견되지 않고 다음 경로 맵 절이 평가됩니다.

5단계 **Match Clause** 탭을 클릭하여 이 절을 적용할 경로를 선택하고 다음 매개변수를 설정합니다.

- **Match first hop interface of route** 확인란을 선택하여 경로의 첫 번째 홉 인터페이스 일치를 활성화 또는 비활성화하거나, 지정된 다음 홉 인터페이스와 경로를 일치합니다. 하나 이상의 인터페이스를 지정하는 경우 경로가 아무 인터페이스나 일치할 수 있습니다.
  - Interface 필드에 인터페이스 이름을 입력하거나 생략 부호를 클릭하여 Browse Interface 대화 상자를 표시합니다.
  - 하나 이상의 인터페이스를 선택하고 **Interface**를 클릭한 후 **OK**를 클릭합니다.
  - **Match Address** 확인란을 클릭하여 경로 또는 일치 패킷의 Match 주소를 활성화하거나 비활성화합니다.

  - **Match Next Hop** 확인란을 선택하여 경로의 차기 홉 주소 일치를 활성화하거나 비활성화합니다.
  - **Match Route Source** 확인란을 선택하여 경로의 알림 소스 주소 일치를 활성화하거나 비활성화합니다.
  - 드롭다운 목록에서 Access List to Prefix List를 선택하여 IP 주소를 일치시킵니다.
  - 이전 선택에 따라 생략 부호를 클릭하여 Browse Access List 또는 Browse Prefix List 대화상자를 표시합니다.
  - 원하는 ACL 또는 접두사 목록을 선택합니다.
- **Match metric of route** 확인란을 선택하여 경로 메트릭 일치를 활성화하거나 비활성화합니다.
  - Metric Value 필드에서 메트릭 값을 입력합니다. 여러 값을 쉼표로 구분하여 입력할 수 있습니다. 이 설정을 통해 지정된 메트릭이 있는 어떤 값과도 일치시킬 수 있습니다. 메트릭 값의 범위는 0~4294967295입니다.
- **Match Route Type** 확인란을 선택하여 경로 유형 일치를 활성화하거나 비활성화합니다. 유효한 경로 유형은 External1, External2, Internal, Local, NSSA-External1 및 NSSA-External2입니다. 활성화된 경우 목록에서 하나 이상의 경로 유형을 선택할 수 있습니다.

6단계 **Set Clause** 탭을 클릭하여 대상 프로토콜로 재배포될 다음 정보를 수정합니다.

- **Set Metric Clause** 확인란을 선택하여 대상 라우팅 프로토콜에 대한 메트릭 값을 활성화 또는 비활성화하고 Value 필드에 값을 입력합니다.
- **Set Metric Type** 확인란을 선택하여 대상 라우팅에 대한 메트릭 유형을 활성화 또는 비활성화하고 드롭다운 목록에서 메트릭 유형을 선택합니다.

7단계 **BGP Match Clause** 탭을 클릭하여 이 절을 적용할 경로를 선택하고 다음 매개변수를 설정합니다.

- **Match AS path access lists** 확인란을 선택하여 BGP 자율 시스템 경로 액세스 목록과 지정된 경로 액세스 목록의 일치를 활성화합니다. 경로 액세스 목록을 하나 이상 지정하는 경우 경로가 아무 경로 액세스 목록과도 일치할 수 있습니다.
- **Match Community** 확인란을 선택하여 지정된 커뮤니티에서 BGP 커뮤니티 일치를 활성화합니다. 하나 이상의 커뮤니티를 지정하는 경우 경로가 아무 커뮤니티나 일치할 수 있습니다. 하나 이상의 Match 커뮤니티와 일치하지 않는 경로는 아웃바운드 경로 맵에 대해 알려지지 않습니다.
  - **Match the specified community exactly** 확인란을 선택하여 BGP 커뮤니티를 지정된 커뮤니티와 정확히 일치할 수 있게 합니다.
- **Match Policy list** 확인란을 선택하여 경로 맵이 BGP 정책을 평가하고 처리하도록 구성합니다. 하나 이상의 정책 목록을 지정하는 경우 경로가 아무 정책 목록이나 처리할 수 있습니다.

8단계 **BGP Set Clause** 탭을 클릭하여 BGP 프로토콜로 재배포될 다음 정보를 수정합니다.

- **Set AS Path** 확인란을 선택하여 BGP 경로에 대한 자율 시스템 경로를 수정합니다.
  - **Prepend AS path** 확인란을 선택하여 임의의 자율 시스템 경로 문자열을 BGP 경로의 앞에 첨부합니다. 일반적으로 로컬 AS 번호가 여러 번 부착되어 자율 시스템 경로 길이가 늘어납니다. AS 경로 번호를 하나 이상 지정하면 경로는 아무 AS 번호나 추가할 수 있습니다.
  - **Prepend Last AS to the AS Path** 확인란을 선택하여 AS 경로에 마지막 AS 번호를 붙입니다. AS 번호로 1~10의 값을 입력하십시오.
  - **Convert route tag into AS Path** 확인란을 선택하여 경로의 태그를 자율 시스템 경로로 변환하십시오.
- **Set Community** 확인란을 선택하여 BGP 커뮤니티 속성을 설정합니다.
  - **Specify Community**를 클릭하여 적용 가능한 경우 커뮤니티 번호를 입력합니다. 유효한 값은 1~ 4294967200, internet, no-advertise 및 no-export입니다.

  - **Add to the existing communities**를 선택하여 커뮤니티를 이미 존재하는 커뮤니티에 추가합니다.
  - **None**을 클릭하여 경로 맵을 전달하는 접두사에서 커뮤니티 속성을 제거합니다.
- **Set local preference** 확인란을 선택하여 자율 시스템 경로에 대한 기본값을 지정합니다.
- **Set weight** 확인란을 선택하여 라우팅 테이블에 대한 BGP 가중치를 지정합니다. 0과 65535 사이의 값을 입력합니다.
- **Set origin** 확인란을 선택하여 BGP 오리진 코드를 지정합니다. 유효한 값은 Local IGP와 Incomplete입니다.
- **Set next hop** 확인란을 선택하여 경로 맵의 일치 절을 충족하는 패킷 출력 주소를 지정합니다.
  - **Specify IP address**를 클릭하여 패킷이 출력되는 다음 홉의 IP 주소를 입력합니다. 인접한 라우터가 아니어도 됩니다. IP 주소를 하나 이상 지정하면 패킷이 아무 IP 주소로나 출력될 수 있습니다.
  - **Use peer address**를 클릭하여 다음 홉을 BGP 피어 주소로 설정합니다.

9단계 **OK**를 클릭합니다.

경로 맵 사용자 정의

이 섹션은 경로 맵을 사용자 정의하는 방법을 설명합니다.

특정 대상 주소와 일치하도록 경로를 정의

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > Route Maps**를 선택합니다.

2단계 **Add**를 클릭합니다.

Add Route Map 대화 상자가 나타납니다. 이 대화 상자에서 경로 맵 이름, 순차 번호, 재배포 액세스(허용 또는 거부)를 할당하거나 선택할 수 있습니다. 경로 맵 엔트리는 순서대로 읽힙니다. 순차 번호를 사용하여 순서를 파악합니다. 그러지 않으면 ASA이(가) 엔트리를 추가하는 순서를 사용합니다.

3단계 **Match Clause** 탭을 클릭하여 이 절을 적용할 경로를 선택하고 다음 매개변수를 설정합니다.

- **Match first hop interface of route** 확인란을 선택하여 경로의 첫 번째 홉 인터페이스 일치를 활성화 또는 비활성화하거나, 지정된 다음 홉 인터페이스와 경로를 일치합니다. 하나 이상의 인터페이스를 지정하는 경우 경로가 아무 인터페이스나 일치할 수 있습니다.
  - Interface 필드에 인터페이스 이름을 입력하거나 생략 부호를 클릭하여 Browse Interface 대화 상자를 표시합니다.

  - 인터페이스 유형(**inside** 또는 **outside**)을 선택하고 **Selected Interface**를 클릭한 다음 **OK**를 클릭합니다.
  - **Match IP Address** 확인란을 클릭하여 경로 또는 일치 패킷의 Match 주소를 활성화하거나 비활성화합니다.
  - **Match Next Hop** 확인란을 선택하여 경로의 차기 홉 주소 일치를 활성화하거나 비활성화합니다.
  - **Match Route Source** 확인란을 선택하여 경로의 알림 소스 주소 일치를 활성화하거나 비활성화합니다.
  - 드롭다운 목록에서 Access List to Prefix List를 선택하여 IP 주소를 일치시킵니다.
  - 이전 선택에 따라 생략 부호를 클릭하여 Browse Access List 또는 Browse Prefix List 대화 상자를 표시합니다.
  - 원하는 ACL 또는 접두사 목록을 선택합니다.
- **Match metric of route** 확인란을 선택하여 경로 메트릭 일치를 활성화하거나 비활성화합니다.
  - Metric Value 필드에서 메트릭 값을 입력합니다. 여러 값을 쉼표로 구분하여 입력할 수 있습니다. 이 설정을 통해 지정된 메트릭이 있는 어떤 값과도 일치시킬 수 있습니다. 메트릭 값의 범위는 0~4294967295입니다.
- **Match Route Type** 확인란을 선택하여 경로 유형 일치를 활성화하거나 비활성화합니다. 유효한 경로 유형은 External1, External2, Internal, Local, NSSA-External1 및 NSSA-External2입니다. 활성화된 경우 목록에서 하나 이상의 경로 유형을 선택할 수 있습니다.

접두사 규칙 구성

참고 접두사 규칙을 구성하기 전에 접두사 목록을 구성해야 합니다.

접두사 규칙을 구성하려면 다음 단계를 수행하십시오.

1단계 ASDM에서 **Configuration > Device Setup > Routing > Prefix Rules**를 선택합니다.

2단계 **Add**를 클릭하고 **Add Prefix Rule**을 선택합니다.

Add Prefix Rule 대화 상자가 표시됩니다. 이 대화 상자에서 순차 번호를 추가하고, IP 버전(IPv4 또는 IPv6)을 선택하고, 네트워크 접두사와 재배포 액세스(허용 또는 거부)를 선택하며 최대 및 최소 접두사 길이를 지정합니다.

3단계 선택적인 순차 번호를 입력하거나 기본값을 승인합니다.

4단계 IP 주소 형식의 접두사 번호/마스크 길이를 지정합니다.

5단계 **Permit** 또는 **Deny** 라디오 버튼을 클릭하여 재배포 액세스를 표시합니다.

6단계 선택적인 최소 및 최대 접두사 길이를 입력합니다.

7단계 작업이 완료되면 **OK**를 클릭합니다.

목록에 새로운 접두사 또는 개정된 접두사 규칙이 나타납니다.

8단계 자동으로 생성된 순차 번호를 사용하려는 경우 **Enable Prefix list sequence numbering** 확인란을 선택하십시오.

9단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

접두사 목록 구성

ABR 타입 3 LSA 필터링은 OSPF를 실행하여 서로 다른 OSPF 영역 간 타입 3 LSA를 필터링하는 ABR의 기능을 확장합니다. 일단 접두사 목록이 구성되면 지정된 접두사만 하나의 OSPF 영역에서 다른 OSPF 영역으로 전송됩니다. 모든 다른 접두사는 OSPF 영역으로 제한됩니다. 이 영역 필터링 유형을 OSPF 영역에서 수신 또는 발신 트래픽에 적용하거나 해당 영역의 수신 및 발신 트래픽 모두에 적용할 수 있습니다.

접두사 목록의 여러 엔트리가 주어진 접두사와 일치하는 경우 순차 번호가 가장 낮은 엔트리가 사용됩니다. 목록 상단 근처의 가장 일반적인 일치 또는 거부에 가장 낮은 순차 번호를 할당하는 것이 효율적일 수 있습니다. 기본적으로 순차 번호는 5부터 시작하여 5씩 증가하며 자동으로 생성됩니다.

접두사 목록을 추가하려면 다음 단계를 수행하십시오.

1단계 ASDM에서 **Configuration > Device Setup > Routing > Prefix Rules**를 선택합니다.

2단계 **Add**를 클릭하여 **Add Prefix List**를 선택합니다.

Add Prefix List 대화 상자가 나타납니다.

3단계 접두사 이름과 설명을 입력한 후 **OK**를 클릭합니다.

경로 작업에 대한 메트릭 값 구성

경로 작업에 대한 메트릭 값을 구성하려면 다음 단계를 수행하십시오.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > Route Maps**를 선택합니다.

2단계 **Add**를 클릭합니다.

Add Route Map 또는 Edit Route Map 대화 상자가 나타납니다. 이 대화 상자에서 경로 맵 이름, 순차 번호, 재배포 액세스(허용 또는 거부)를 할당하거나 선택할 수 있습니다. 경로 맵 엔트리는 순서대로 읽힙니다. 순차 번호를 사용하여 순서를 파악합니다. 그러지 않으면 ASA이(가) 경로 맵 엔트리를 추가하는 순서를 사용합니다.

3단계 **Set Clause** 탭을 클릭하여 대상 프로토콜로 재배포될 다음 정보를 수정합니다.

- **Set Metric Clause** 확인란을 선택하여 대상 라우팅 프로토콜에 대한 메트릭 값을 활성화 또는 비활성화하고 Value 필드에 값을 입력합니다.
- **Set Metric Type** 확인란을 선택하여 대상 라우팅에 대한 메트릭 유형을 활성화 또는 비활성화하고 드롭다운 목록에서 메트릭 유형을 선택합니다.

경로 맵 구성 예

다음 예는 합 개수가 1과 같은 경로를 OSPF로 재배포하는 방법을 보여줍니다.

1단계 ASDM에서 **Configuration > Device Setup > Routing > Route Maps**를 선택합니다.

2단계 **Add**를 클릭합니다.

3단계 Route Map Name 필드에 **1-to-2**를 입력합니다.

4단계 Sequence Number 필드에 라우팅 순차 번호를 입력합니다.

5단계 **Permit** 라디오 버튼을 클릭합니다.

기본적으로 이 탭은 상단에 있습니다.

6단계 **Match Clause** 탭을 클릭합니다.

7단계 **Match Metric of Route** 확인란을 선택하고 메트릭 값으로 **1**을 입력합니다.

8단계 **Set Clause** 탭을 클릭합니다.

9단계 **Set Metric Value** 확인란을 선택하고 메트릭 값으로 **5**를 입력합니다.

10단계 **Set Metric-Type** 확인란을 선택하고 **Type-1**을 선택합니다.

경로 맵에 대한 기능 내역

표 21-1 경로 맵에 대한 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
경로 맵	7.0(1)	이 기능을 도입했습니다. 다음 화면을 도입했습니다. Configuration > Device Setup > Routing > Route Maps.
고정 및 동적 경로 맵에 대한 지원 개선	8.0(2)	동적 및 고정 경로 맵에 대한 향상된 지원이 추가되었습니다.
다중 컨텍스트 모드의 동적 라우팅	9.0(1)	경로 맵은 다중 컨텍스트 모드에서 지원됩니다.
BGP 지원	9.2(1)	이 기능을 도입했습니다. 다음 화면을 업데이트했습니다: Configuration > Device Setup > Routing > Route Maps(BGP match clause 및 BGP set clause의 2개의 추가 탭이 있음).

BGP

이 장에서는 BGP(Border Gateway Protocol)를 이용하여 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 Cisco ASA을(를) 구성하는 방법을 설명합니다.

BGP 소개

BGP는 자율 시스템 간 라우팅 프로토콜입니다. 자율 시스템은 공통 관리와 공통 라우팅 정책에 따르는 네트워크 또는 네트워크 그룹입니다. BGP는 인터넷을 위한 라우팅 정보 교환에 사용되며 인터넷 서비스 제공자(ISP) 간에 사용되는 프로토콜입니다.

BGP를 사용해야 하는 시기

대학 및 기업과 같은 고객 네트워크는 일반적으로 네트워크 내 라우팅 정보 교환을 위해 OSPF와 같은 IGP(Interior Gateway Protocol)를 활용합니다. 고객은 ISP에 연결하고 ISP는 BGP를 사용하여 고객 및 ISP 경로를 교환합니다. 자율 시스템(AS) 사이에서 BGP가 사용될 때 프로토콜을 EBGP(External BGP)라고 합니다. 서비스 공급자가 AS 내에서 경로 교환을 위해 BGP를 사용할 때 프로토콜은 IBGP(Interior BGP)라고 합니다.

라우팅 테이블 변경 사항

인접 디바이스 간 TCP 연결이 처음 설정되면 BGP 인접 디바이스가 전체 라우팅 정보를 교환합니다. 라우팅 테이블 변경 사항이 감지되면 BGP 라우터가 변경된 경로만 이웃으로 전송합니다. BGP 라우터는 주기적인 라우팅 업데이트를 전송하지 않고 BGP 라우팅 업데이트는 대상 네트워크로의 최적의 경로만 알립니다.

BGP를 통해 학습된 경로에는 특정 대상으로 향하는 경로가 여럿일 때 최적의 경로를 결정하는 데 사용되는 속성이 포함되어 있습니다. 이러한 속성을 BGP 속성이라고 하며 경로 선택 과정에서 사용됩니다.

- 가중치 -- Cisco가 정의한 라우터에 대한 로컬 속성입니다. 가중치 속성은 주변의 라우터에 알려지지 않습니다. 라우터가 동일한 대상에 대하여 하나 이상의 경로를 학습한 경우 가중치가 가장 높은 경로가 우선합니다.
- 로컬 우선 -- 로컬 우선 속성은 로컬 AS로부터 출구 지점을 선택하는 데 사용됩니다. 가중치 속성과 달리 로컬 우선 속성은 로컬 AS 전체에 걸쳐 전파됩니다. AS에서 출구 지점이 여럿인 경우 로컬 우선 속성이 가장 높은 출구 지점이 특정 경로에 대한 출구 지점으로 사용됩니다.
- Multi-exit discriminator -- MED(multi-exit discriminator) 또는 메트릭 속성은 메트릭에 알려지는 AS로의 우선 경로에 관한 외부 AS에 대한 제안으로 사용됩니다. MED를 수신하는 외부 AS가 경로 선택을 위해 다른 BGP 속성을 사용할 수도 있기 때문에 제안이라고 하는 것입니다. MED 메트릭이 낮은 경로가 우선합니다.
- Origin -- 발신지 속성은 BGP가 특정 경로에 관해 어떻게 학습하는지 나타냅니다. 발신지 속성은 3가지 값을 가질 수 있으며 경로 선택에 사용됩니다.
  - IGP- 경로가 발신 AS 내부에 있습니다. 이 값은 경로를 BGP로 삽입하기 위해 네트워크 라우터 컨피그레이션 명령을 사용할 때 설정됩니다.
  - EGP-경로는 EBGP(Exterior Border Gateway Protocol)를 통해 학습됩니다.
  - Incomplete- 경로의 발신지를 알 수 없거나 학습되지 않았습니다. 경로가 BGP로 재배포되면 불완전한 발신지가 됩니다.
- AS_path -- 경로 광고가 자율 시스템을 통과할 때 경로가 전달된 AS 번호의 주문 목록에 AS 번호가 추가됩니다. 가장 짧은 AS_path 목록을 가진 경로만 IP 라우팅 테이블에 설치됩니다.
- Next hop -- EBGP next-hop 속성은 전달되는 라우터에 도달하기 위해 사용되는 IP 주소입니다. EBGP 피어의 경우 next-hop 주소는 피어 간 연결의 IP 주소입니다. IBGP의 경우 EBGP next-hop 주소가 로컬 AS로 전달됩니다.
- Community -- 커뮤니티 속성은 라우팅 결정(승인, 우선, 재배포)을 적용할 수 있는 커뮤니티라는 대상 그룹화 방법을 제공합니다. 경로 맵은 커뮤니티 속성을 설정하는 데 사용됩니다. 미리 정의된 커뮤니티 속성은 다음과 같습니다.
  - no-export- 이 경로를 EBGP 피어에게 알리지 않습니다.
  - no-advertise- 이 경로를 어느 피어에게도 알리지 않습니다.
  - internet- 이 경로를 인터넷 커뮤니티에 알립니다. 네트워크의 모든 라우터가 여기 포함됩니다.

BGP 경로 선택

BGP는 같은 경로에 대해 서로 다른 소스로부터 여러 공지를 수신할 수 있습니다. BGP는 최적의 경로로 하나의 경로만 선택합니다. 이 경로가 선택된 경우 BGP는 선택된 경로를 IP 라우팅 테이블에 놓고 이웃에 전파합니다. BGP는 제시된 순서대로 다음 기준에 따라 대상에 대한 경로를 선택합니다.

- 경로가 접근할 수 없는 next hop을 지정하면 업데이트를 삭제합니다.
- 가중치가 가장 높은 경로가 우선합니다.
- 가중치가 동일한 경우 로컬 우선이 가장 높은 경로가 우선합니다.
- 로컬 우선이 동일한 경우 이 라우터에서 실행 중인 BGP에서 발생한 경로가 우선합니다.
- 경로가 시작되지 않은 경우 AS_path가 가장 짧은 경로가 우선합니다.

- 모든 경로의 AS_path 길이가 같은 경우 발신지 유형이 가장 낮은 경로(IGP가 EGP보다 낮고 EGP가 incomplete보다 낮은 경로)가 우선합니다.
- 발신지 코드가 동일한 경우 MED 속성이 가장 낮은 경로가 우선합니다.
- MED가 같은 경로의 경우 내부 경로보다 외부 경로가 우선합니다.
- 그래도 경로가 동일한 경우 가장 가까운 IGP 이웃을 통한 경로가 우선합니다.
- 두 경로 모두 외부인 경우 먼저 수신된 경로가 우선합니다(오래된 경로).
- BGP 라우터 ID가 지정한 대로 IP 주소가 가장 낮은 경로가 우선합니다.
- 여러 경로의 발신자 또는 라우터 ID가 동일할 경우 클러스터 목록 길이가 가장 짧은 경로가 우선합니다.
- 가장 낮은 이웃 주소에서 시작하는 경로가 우선합니다.

BGP용 지침

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

투명 방화벽 모드를 지원하지 않습니다. BGP는 라우터 모드에서만 지원됩니다.

장애 조치 지침

단일 및 다중 컨텍스트 모드에서 상태 기반 장애 조치를 지원합니다.

참고 클러스터가 활성화되면, 장애 조치는 지원되지 않습니다.

클러스터링 지침

BGP는 L2(EtherChannel 유형) 및 L3(개별 인터페이스 유형) 클러스터링 모드에서만 지원됩니다.

참고 사용자 컨텍스트에서 BGP 컨피그레이션을 삭제하고 다시 적용하는 경우 슬레이브/스탠바이 ASA 유닛이 동기화할 수 있도록 60초간 기다리십시오.

IPv6 지침

IPv6를 지원합니다. IPv6 주소군에 대해서는 graceful restart가 지원되지 않습니다.

BGP 구성

이 섹션에서는 시스템에서 BGP 프로세스를 활성화하고 구성하는 방법을 설명합니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP**를 선택합니다.

2단계 **General** 탭에서 **Enable BGP routing** 확인란을 선택하여 BGP 라우팅 프로세스를 활성화합니다. 22-4 페이지의 BGP 사용를 참조하십시오.

3단계 **BGP > Best Path** 탭에서 BGP 라우팅을 위한 최적의 경로 선택 프로세스와 관련된 컨피그레이션을 정의합니다. 22-5 페이지의 BGP 라우팅 프로세스를 위한 최적의 경로 정의를 참조하십시오.

4단계 **BGP > Policy Lists** 탭에서 BGP 라우팅에 대한 정책 목록을 구성합니다. 22-6 페이지의 정책 목록 구성를 참조하십시오.

5단계 **BGP > AS Path Filters** 탭에서 BGP 라우팅에 대한 AS 경로 필터를 구성합니다. 22-7 페이지의 AS 경로 필터 구성를 참조하십시오.

6단계 **BGP > Community Rules** 탭에서 BGP 라우팅에 대한 커뮤니티 규칙을 구성합니다. 22-8 페이지의 커뮤니티 규칙 구성를 참조하십시오.

7단계 **BGP > IPv4 Family** 탭에서 IPv4 주소군 설정을 구성합니다. 22-8 페이지의 IPv4 주소군 설정 구성를 참조하십시오.

BGP 사용

이 섹션에서는 BGP 라우팅 활성화, BGP 라우팅 프로세스 설정 및 일반 BGP 매개변수 구성에 필요한 단계를 설명합니다.

절차

1단계 단일 모드의 경우 ASDM에서 **Configuration > Device Setup > Routing > BGP > General**을 선택합니다.

참고 다중 모드의 경우 ASDM에서 **Configuration > Context Management > BGP**를 선택합니다. BGP를 활성화한 후 보안 컨텍스트로 전환하고 **Configuration > Device Setup > Routing > BGP > General**을 클릭하여 BGP를 활성화합니다.

General 창이 표시됩니다.

2단계 **Enable BGP Routing** 확인란을 선택합니다.

3단계 **AS Number** 필드에 BGP 프로세스에 대한 자율 시스템(AS) 번호를 입력합니다. AS 번호는 내부에 여러 자율 번호를 포함합니다. AS 번호는 1~4294967295 또는 1.0~XX.YY가 될 수 있습니다.

4단계 (선택 사항) **Limit the number of AS numbers in the AS_PATH attribute of received routes** 확인란을 선택하여 AS_PATH 속성의 숫자를 특정 숫자로 제한합니다. 유효한 값은 1부터 254까지입니다.

5단계 (선택 사항) **Log neighbor changes** 확인란을 선택하여 BGP 인접 디바이스 변경 사항(증가 또는 감사)와 재설정에 대한 로깅을 활성화합니다. 이는 네트워크 연결 문제 해결과 네트워크 안정성 측정에 도움이 됩니다.

6단계 (선택 사항) **Use TCP path MTU discovery** 확인란을 선택하고 Path MTU Discovery 기술을 사용하여 두 IP 호스트 간 네트워크 경로에서 MTU(maximum transmission unit) 크기를 결정합니다. 이는 IP 단편화를 방지합니다.

7단계 (선택 사항) **Enable fast external failover** 확인란을 선택하여 링크 장애 시 즉시 외부 BGP 세션을 재설정합니다.

8단계 (선택 사항) **Enforce that first AS is peer's AS for EBGP routes** 확인란을 선택하여 AS 번호를 AS_PATH 속성의 첫 번째 세그먼트로 나열하지 않는 외부 BGP 피어에서 수신되는 업데이트를 버립니다. 이는 잘못 구성되거나 권한이 없는 피어가 마치 다른 자율 시스템에서 소싱된 것처럼 경로를 알림으로써 트래픽을 잘못 안내하지 않도록 예방합니다.

9단계 (선택 사항) **Use dot notation for AS numbers** 확인란을 선택하여 전체 2진 4바이트 AS 번호를 각각 16비트의 두 단어로 마침표로 구분하여 나눕니다. 0~65553의 AS 번호는 10진수로 표시되고 65535보다 큰 AS 번호는 마침표를 통해 표시됩니다.

10단계 **Neighbor timers** 영역의 타이머 정보를 지정:

a. **Keepalive interval** 필드에 keepalive 메시지를 보내지 않은 후 BGP 인접 디바이스가 활성 상태를 유지하는 시간 간격을 입력합니다. 이 keepalive 간격이 지나면 전송된 메시지가 없는 경우 BGP 피어가 데드로 선언됩니다. 기본값은 60초입니다.

b. **Hold Time** 필드에 BGP 연결이 개시 및 구성되는 동안 BGP 인접 디바이스가 활성 상태를 유지할 최소 시간 간격을 입력합니다. 기본값은 180초입니다.

c. (선택 사항) **Min. Hold Time** 필드에 BGP 연결이 개시 및 구성되는 동안 BGP 인접 디바이스가 활성 상태를 유지할 최소 시간 간격을 입력합니다. 0에서 65535 사이의 값을 지정합니다.

11단계 (선택 사항) **Non Stop Forwarding** 섹션에서 다음을 수행합니다.

a. **Enable Graceful Restart** 확인란을 선택하여 ASA 피어가 전환 후 라우팅 플랩을 피할 수 있도록 합니다.

b. **Restart Time** 필드에 BGP 오픈 메시지를 수신하기 전에 이전 경로를 삭제하기까지 ASA 피어가 기다릴 시간을 입력합니다. 기본값은 120초입니다. 유효한 값은 1~3600초입니다.

c. **Stale Path Time** 필드에 재시작하는 ASA에서 EOR(end of record) 메시지가 접수된 후이전 경로를 삭제하기 전에 ASA가 대기할 시간을 입력합니다. 기본값은 360초입니다. 유효한 값은 1~3600초입니다.

12단계 **OK**를 클릭합니다.

13단계 **Apply**를 클릭합니다.

BGP 라우팅 프로세스를 위한 최적의 경로 정의

이 섹션에서는 BGP 최적의 경로 구성에 필요한 단계를 설명합니다. 최정의 경로에 대한 자세한 정보는 22-2 페이지의 BGP 경로 선택에서 참조하십시오.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > Best Path**를 선택합니다.

Best Path configuration 창이 나타납니다.

2단계 **Default Local Preference** 필드에서 0과 4294967295 사이의 값을 지정합니다. 기본값은 100입니다. 값이 높을수록 우선순위가 높습니다. 이 우선 값은 로컬 자율 시스템의 모든 라우터와 액세스 서버로 전송됩니다.

3단계 **Allow comparing MED from different neighbors** 확인란을 선택하여 서로 다른 자율 시스템의 인접 디바이스로부터 경로에 대한 MED(Multi Exit Discriminator)를 비교합니다.

4단계 **Compare router-id for identical EBGP paths** 확인란을 선택하여 최적의 경로 선택 과정 중 외부 BGP 피어에서 수신된 비슷한 경로를 비교하고 최적의 경로를 라우터 ID가 가장 낮은 경로로 전환합니다.

5단계 **Pick the best MED path among paths advertised from the neighboring AS** 확인란을 선택하여 연합 피어에서 학습된 경로 간 MED를 비교하고 새로운 네트워크 엔트리를 추가합니다. MED 간 비교는 경로에 외부 자율 시스템이 없는 경우에만 이루어집니다.

6단계 **Treat missing MED as the least preferred one** 확인란을 선택하여 누락 MED 속성 값을 무한으로 간주하고 이 경로를 최하위 순위로 만듭니다. 따라서 MED가 없는 경로가 최하위 순위가 됩니다.

7단계 **OK**를 클릭합니다.

8단계 **Apply**를 클릭합니다.

정책 목록 구성

경로 지도 내에서 정책 목록이 참조되는 경우 정책 목록의 모든 일치 문장이 평가 및 처리됩니다. 경로 지도 내에 둘 이상의 정책 목록을 구성할 수 있습니다. 정책 목록은 같은 경로 지도 내에 있으나 정책 목록 밖에서 구성된 기존 일치 항목 및 설정 문구와도 공존할 수 있습니다. 이 섹션은 정책 목록 구성에 필요한 단계를 설명합니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > Policy Lists**를 선택합니다.

2단계 **Add**를 클릭합니다.

Add Policy List 대화 상자가 나타납니다. 이 대화 상자에서 정책 목록 이름, 재배포 액세스(허용 또는 거부) 추가, 인터페이스 일치, IP 주소 지정, AS 경로 일치, 커뮤니티 이름 목록 일치, 메트릭 일치 및 태그 번호 일치를 수행할 수 있습니다.

3단계 **Policy List Name** 필드에 정책 목록에 대한 이름을 입력합니다.

4단계 **Permit** 또는 **Deny** 라디오 버튼을 클릭하여 재배포 액세스를 표시합니다.

5단계 **Match Interfaces** 확인란을 선택하여 next hop이 지정된 인터페이스를 벗어난 경로를 배포하고 다음 중 하나를 수행합니다.

- **Interface** 필드에 인터페이스 이름을 입력합니다.
- **Interface** 필드에서 타원을 클릭하여 인터페이스를 수동으로 찾아봅니다. 하나 이상의 인터페이스를 선택하고 **Interface**를 클릭한 후 **OK**를 클릭합니다.

6단계 **Specify IP** 영역에서 다음을 구성합니다.

a. **Match Address** 확인란을 선택하여 표준 액세스 목록 또는 접두사 목록으로 허용된 대상 네트워크 숫자 주소가 있는 경로를 재배포하고 패킷에 대한 정책 라우팅을 수행합니다.

   액세스 목록/접두사 목록을 지정하거나 타원을 클릭하여 수동으로 액세스 목록을 찾습니다. 하나 이상의 액세스 목록을 선택하고 **Access List**를 클릭한 후 **OK**를 클릭합니다.

b. **Match Next Hop** 확인란을 선택하여 지정된 액세스 목록 또는 접두사 목록이 전달한 next hop 라우터 주소가 있는 경로를 재배포합니다.

   액세스 목록/접두사 목록을 지정하거나 타원을 클릭하여 수동으로 액세스 목록을 찾습니다. 하나 이상의 액세스 목록을 선택하고 **Access List**를 클릭한 후 **OK**를 클릭합니다.

c. **Match Route Source** 확인란을 선택하여 액세스 목록 또는 접두사 목록이 지정한 주소에서 라우터 및 액세스 서버가 알려준 경로를 재배포합니다.

액세스 목록/접두사 목록을 지정하거나 타원을 클릭하여 수동으로 액세스 목록을 찾습니다. 하나 이상의 액세스 목록을 선택하고 **Access List**를 클릭한 후 **OK**를 클릭합니다.

7단계 **Match AS Path** 확인란을 선택하여 BGP 자율 시스템 경로를 일치시킵니다.

AS 경로 필터를 지정하거나 타원을 클릭하여 AS Path Filter를 수동으로 찾습니다. 하나 이상의 AS 경로 필터를 선택하고 **AS Path Filter**를 클릭한 후 **OK**를 클릭합니다.

8단계 **Match Community Names List** 확인란을 선택하여 BGP 커뮤니티를 일치시킵니다.

a. 커뮤니티 규칙을 지정하거나 타원을 클릭하여 커뮤니티 규칙을 수동으로 찾습니다. 하나 이상의 커뮤니티 규칙을 선택하고 **Community Rules**를 클릭한 후 **OK**를 클릭합니다.

b. **Match the specified community exactly** 확인란을 선택하여 특정 BGP 커뮤니티를 일치시킵니다.

9단계 **Match Metrices** 확인란을 선택하여 지정된 메트릭을 가진 경로를 재배포합니다. 메트릭을 하나 이상 지정한 경우 경로는 모든 메트릭과 일치할 수 있습니다.

10단계 **Match Tag Numbers** 확인란을 선택하여 지정된 태그와 일치하는 라우팅 테이블의 경로를 재배포합니다. 태그 번호를 하나 이상 지정한 경우 경로는 모든 메트릭과 일치할 수 있습니다.

11단계 **OK**를 클릭합니다.

12단계 **Apply**를 클릭합니다.

AS 경로 필터 구성

AS 경로 필터는 액세스 목록을 사용하고 업데이트 메시지 내에 개별 접두사를 살펴봄으로써 라우팅 업데이트 메시지를 필터링할 수 있습니다. 업데이트 메시지 내 접두사가 필터 기준과 일치하면 필터 엔트리에서 수행하도록 구성된 작업에 따라 해당 개별 접두사가 필터링되거나 승인됩니다. 이 섹션에서는 AS 경로 필터 구성에 필요한 단계를 설명합니다.

참고 **as-path access-lists**는 일반 방화벽 ACL과 다릅니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > AS Path Filters**를 선택합니다.

2단계 **Add**를 클릭합니다.

Add Filter 대화 상자가 나타납니다. 이 대화 상자에서 필터 이름, 재배포 액세스(허용 또는 거부) 및 정규식을 추가할 수 있습니다.

3단계 **Name** 필드에 AS Path Filter 이름을 입력합니다.

4단계 **Permit** 또는 **Deny** 라디오 버튼을 클릭하여 재배포 액세스를 표시합니다.

5단계 정규식을 지정하십시오. **Build**를 클릭하여 정규식을 구축합니다.

6단계 **Test**를 클릭하여 정규식이 선택한 문자열과 일치하는지 테스트합니다.

7단계 **OK**를 클릭합니다.

8단계 **Apply**를 클릭합니다.

커뮤니티 규칙 구성

커뮤니티는 공통 속성을 공유하는 대상 그룹입니다. 커뮤니티 목록을 사용하여 경로 지도의 일치 조항에서 사용할 커뮤니티 그룹을 만들 수 있습니다. 액세스 목록과 마찬가지로 일련의 커뮤니티 목록을 생성할 수 있습니다. 일치 항목을 찾을 때까지 구문을 확인합니다. 1개 구문이 만족되면 테스트가 종료됩니다. 이 섹션은 커뮤니티 규칙 구성에 필요한 단계를 설명합니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > Community Rules**를 선택합니다.

2단계 **Add**를 클릭합니다.

Add Community Rule 대화 상자가 표시됩니다. 이 대화 상자에서 규칙 이름, 규칙 유형, 재배포 액세스(허용 또는 거부) 및 구체적인 커뮤니티를 추가할 수 있습니다.

3단계 **Rule Name** 필드에 커뮤니티 규칙 이름을 입력합니다.

4단계 **Standard** 또는 **Expanded** 라디오 버튼을 클릭하여 커뮤니티 규칙 유형을 표시합니다.

5단계 **Permit** 또는 **Deny** 라디오 버튼을 클릭하여 재배포 액세스를 표시합니다.

6단계 표준 커뮤니티 규칙 추가:

a. **Communities** 필드에서 커뮤니티 번호를 지정합니다. 유효한 값은 1부터 4294967200까지입니다.

b. (선택 사항) **Internet**(well-known community) 확인란을 선택하여 인터넷 커뮤니티를 지정합니다. 이 커뮤니티 경로는 모든 피어(내부 및 외부)에게 알려집니다.

c. (선택 사항) **Do not advertise to any peers**(well-known community) 확인란을 선택하여 no-advertise 커뮤니티를 지정합니다. 이 커뮤니티 경로는 모든 피어(내부 또는 외부)에게 알려지지 않습니다.

d. (선택 사항) **Do not export to next AS**(well-known community) 확인란을 선택하여 no-export 커뮤니티를 지정합니다. 이 커뮤니티 경로는 같은 자율 시스템 안에 있는 피어 또는 연합 내에 다른 하위 자율 시스템으로만 알려집니다. 이 경로는 외부 피어에 알려지지 않습니다.

7단계 확장 커뮤니티 규칙 추가:

a. **Regular Expression** 필드에 정규식을 입력합니다. **또는 Build**를 클릭하여 정규식을 구축합니다.

b. 정규식이 만들어졌고 선택한 문자열과 일치하는지 테스트하려면 **Test**를 클릭합니다.

8단계 **OK**를 클릭합니다.

9단계 **Apply**를 클릭합니다.

IPv4 주소군 설정 구성

BGP에 대한 IPv4 설정은 BGP 컨피그레이션 설정 내 IPv4 주소군 옵션에서 설정 가능합니다. IPv4 주소군 섹션에는 일반 설정, 종합 주소 설정, 필터링 설정 및 인접 디바이스 설정에 대한 하위 섹션이 포함됩니다. 이 하위 섹션을 통해 IPv4 주소군에 대한 매개변수를 사용자 정의할 수 있습니다.

이 섹션에서는 BGP IPv4 주소군 설정 사용자 정의 방법을 설명합니다.

- 22-9 페이지의 IPv4 주소군 일반 설정 구성
- 22-9 페이지의 IPv4 주소군 종합 주소 설정 구성
- 22-10 페이지의 IPv4 주소군 필터링 설정 구성

IPv4 주소군 일반 설정 구성

이 섹션에서는 일반 IPv4 설정에 필요한 단계를 설명합니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > IPv4 Family**를 선택합니다.

2단계 **General**을 클릭합니다.

General IPv4 family BGP parameters 컨피그레이션 창이 표시됩니다.

3단계 Administrative Distances 영역에서 External, Internal 및 Local 거리를 지정합니다.

4단계 **Learned Routes Map** 드롭다운 목록에서 경로 지도 이름을 선택합니다. **Manage**를 클릭하여 경로 지도를 추가 및 구성합니다.

5단계 (선택 사항) **Generate Default Route** 확인란을 선택하여 기본 경로로 재배포하도록 BGP 라우팅 프로세스를 구성합니다(network 0.0.0.0).

6단계 (선택 사항) **Summarize subnet routes into network-level routes** 확인란을 선택하여 네트워크 수준 경로로의 서브넷 경로 자동 요약을 구성합니다.

7단계 (선택 사항) **Advertise inactive routes** 확인란을 선택하여 RIB(routing information base)에 설치되지 않은 경로를 알립니다.

8단계 (선택 사항) **Redistribute iBGP into an IGP** 확인란을 선택하여 IS-IS 또는 OSPF와 같은 내부 IGP(내부 게이트웨이 프로토콜)로의 iBGP 재배포를 구성합니다.

9단계 (선택 사항) 스캔 간격 필드에 next-hop 확인을 위한 BGP 라우터에 대한 스캔 간격(초)을 입력합니다. 유효한 값은 5부터 60초입니다.

10단계 (선택 사항) **Enable address tracking** 확인란을 선택하여 BGP next hop 주소 추적을 활성화합니다. **Delay Interval** 필드의 라우팅 테이블에 설치된 업데이트된 next-hop 경로에 대한 검사 간 지연 간격을 지정합니다.

11단계 (선택 사항) 라우팅 테이블에 설치할 수 있는 병렬 iBGP(internal Border Gateway Protocol) 경로의 최대 개수를 Number of paths 필드에 지정하고 **iBGP multipaths** 확인란을 선택합니다.

12단계 **Apply**를 클릭합니다.

IPv4 주소군 종합 주소 설정 구성

이 섹션에서는 하나의 경로로의 특정 경로 종합을 정의하는 데 필요한 단계를 설명합니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > IPv4 Family**를 선택합니다.

2단계 **Aggregate Address**를 클릭합니다.

Aggregate Address 매개변수 컨피그레이션 창이 표시됩니다.

3단계 **Add**를 클릭합니다.

Add Aggregate Address 창이 표시됩니다.

4단계 Network 필드에 네트워크 객체를 지정합니다.

5단계 **Generate autonomous system set path information** 확인란을 선택하여 경로 정보를 설정합니다.

6단계 **Filters all more- specific routes from the updates** 확인란을 선택하여 업데이트의 모든 more-specific 경로를 필터링합니다.

7단계 Attribute Map 드롭다운 목록에서 route-map을 선택합니다. **Manage**를 클릭하여 경로 지도를 추가 또는 구성합니다.

8단계 Advertise Map 드롭다운 목록에서 route-map을 선택합니다. **Manage**를 클릭하여 경로를 추가 또는 구성합니다.

9단계 Suppress Map 드롭다운 목록에서 route-map을 선택합니다. **Manage**를 클릭하여 경로를 추가 또는 구성합니다.

10단계 **OK**를 클릭합니다.

11단계 Aggregate Timer 필드에서 종합 타이머 값(초)을 지정합니다. 유효한 값은 0 또는 6과 60 사이의 모든 값입니다.

12단계 **Apply**를 클릭합니다.

IPv4 주소군 필터링 설정 구성

이 섹션에서는 수신 BGP 업데이트에서 수신된 경로나 네트워크 필터링에 필요한 단계를 설명합니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > IPv4 Family**를 선택합니다.

2단계 **Filtering**을 클릭합니다.

BGP 업데이트를 위한 필터 정의 창이 표시됩니다.

3단계 **Add**를 클릭합니다.

Add Filter 창이 표시됩니다.

4단계 Direction 드롭다운 목록에서 방향을 선택합니다. 방향은 필터를 인바운드 업데이트에 적용할지 아웃바운드 업데이트에 적용할지 지정합니다.

5단계 액세스 목록 드롭다운 목록에서 액세스 목록을 선택합니다. **Manage**를 클릭하여 새 ACL을 추가합니다.

6단계 Protocol 드롭다운 목록에서 프로토콜을 선택합니다. 이는 아웃바운드 방향을 선택한 경우에만 적용됩니다.

7단계 Process ID 드롭다운 목록에서 프로토콜에 대해 지정된 프로세스 ID를 선택합니다.

8단계 **OK**를 클릭합니다.

9단계 **Apply**를 클릭합니다.

IPv4 주소군 BGP 인접 디바이스 설정 구성

이 섹션은 BGP 인접 디바이스 및 인접 디바이스 설정 정의에 필요한 단계를 설명합니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > IPv4 Family**를 선택합니다.

2단계 **Neighbor**를 클릭합니다.

3단계 **Add**를 클릭합니다.

4단계 왼쪽 창의 **General**을 클릭합니다.

5단계 **IP Address** 필드에 BGP 인접 디바이스 IP 주소를 입력합니다. 이 IP 주소는 BGP 인접 테이블에 추가됩니다.

6단계 BGP 인접 디바이스가 속하는 자율 시스템을 **Remote AS** 필드에 입력합니다.

7단계 (선택 사항) BGP 인접 디바이스에 대한 설명을 **Description** 필드에 입력합니다.

8단계 (선택 사항) Shutdown neighbor administratively 확인란을 선택하여 인접 또는 피어 그룹을 비활성화합니다.

9단계 (선택 사항) Enable address family 확인란을 선택하여 BGP 인접 디바이스와의 통신을 활성화합니다.

10단계 (선택 사항) **Global Restart Functionality for this peer** 확인란을 선택하여 ASA 인접 디바이스 또는 피어 그룹에 대한 BGP(Border Gateway Protocol) graceful restart 기능을 활성화 또는 비활성화합니다.

11단계 왼쪽 창의 **Filtering**을 클릭합니다.

12단계 (선택 사항) 액세스 목록 영역을 사용하여 필터 경로에서 BGP 인접 디바이스 정보를 배포할 적절한 수신 또는 발신 액세스 제어 목록을 선택합니다. **Manage**를 클릭하여 필요에 따라 ACL 및 ACE를 추가합니다.

13단계 (선택 사항) 경로 지도 영역을 사용하여 필터 경로에서 수신 또는 발신 경로에 적용할 적절한 수신 또는 발신 경로 지도를 선택합니다. **Manage**를 클릭하여 경로 지도를 구성합니다.

14단계 (선택 사항) 접두사 목록 영역을 사용하여 필터 경로에서 BGP 인접 디바이스 정보를 배포할 적절한 수신 또는 발신 접두사 목록을 선택합니다. **Manage**를 클릭하여 접두사 목록을 구성합니다.

15단계 (선택 사항) AS 경로 필터 영역을 사용하여 필터 경로에서 BGP 인접 디바이스 정보를 배포할 적절한 수신 또는 발신 AS 경로 필터를 선택합니다. **Manage**를 클릭하여 AS 경로 필터를 구성합니다.

16단계 (선택 사항) **Limit the number of prefixes allowed from the neighbor** 확인란을 선택하여 인접 디바이스에서 수신할 수 있는 접두사 수를 제어합니다.

- Maximum prefixes 필드에 특정 인접 디바이스에서 허용할 최대 접두사 개수를 입력합니다.
- Threshold level 필드에 라우터가 경고 메시지 생성을 시작할 최대 비율을 입력합니다. 유효한 값은 1부터 100 사이의 정수입니다. 기본값은 75입니다.
- (선택 사항) **Control prefixes received from a peer** 확인란을 선택하여 피어에서 수신된 접두사에 대한 추가 제어를 지정합니다. 다음 중 하나를 수행합니다.
  - **Terminate peering when prefix limit is exceeded**를 클릭하여 접두사 한도에 도달할 때 BGP 인접 디바이스를 중단합니다. Restart interval 필드에 BGP 인접 디바이스가 재시작하는 간격을 지정합니다.
  - **Give only warning message when prefix limit is exceeded**를 클릭하여 최대 접두사 한도가 초과되었을 때 로그 메시지를 생성합니다. 여기에서는 BGP 인접 디바이스가 종료되지 않습니다.

17단계 왼쪽 창의 **Routes**를 클릭합니다.

18단계 Advertisement Interval 필드에 BGP 라우팅 업데이트 전송 최소 간격(초)을 입력합니다.

19단계 (선택 사항) **Generate Default route** 확인란을 선택하여 로컬 라우터가 기본 경로 0.0.0.0을 인접 디바이스로 전송하도록 허용합니다.

- 경로 지도 드롭다운 목록에서 경로 0.0.0.0의 조건부 삽입을 허용할 경로 지도를 선택합니다. **Manage**를 클릭하여 경로 지도를 추가하거나 구성합니다.

20단계 (선택 사항) 조건부 알림 경로를 추가하려면 다음을 수행합니다.

a. Conditionally Advertised Routes 섹션에서 **Add**를 클릭합니다.

b. Advertise Map 드롭다운 목록에서 exist 지도 또는 non-exist 지도의 조건을 충족할 경우 알릴 경로 지도를 선택합니다.

c. 다음 중 하나를 수행합니다.

- **Exist Map**을 클릭하고 경로 지도를 선택합니다. 이 경로 지도를 BGP 테이블의 경로와 비교하여 경로 지도를 알릴지 결정합니다.
- **Non-exist Map**을 클릭하고 경로 지도를 선택합니다. 이 경로 지도를 BGP 테이블의 경로와 비교하여 경로 지도를 알릴지 결정합니다.

d. **OK**를 클릭합니다.

21단계 (선택 사항) **Remove private autonomous system (AS) numbers from outbound routing updates** 확인란을 선택하여 아웃바운드 경로에서 비공개 AS 번호를 알림에서 제외합니다.

22단계 왼쪽 창의 **Timers**를 클릭합니다.

23단계 (선택 사항) **Set timers for the BGP peer** 확인란을 선택하여 keepalive 빈도, 보류 시간 및 최소 보류 시간을 설정합니다.

- Keepalive frequency 필드에 ASA가 keepalive 메시지를 인접 디바이스로 전송할 빈도(초)를 입력합니다. 유효한 값은 0~65535입니다. 기본값은 60초입니다.
- ASA가 피어 데드를 선언하는 keepalive 메시지를 수신하지 않은 후 간격(초)을 Hold time 필드에 입력합니다. 기본값은 180초입니다.
- (선택 사항) ASA가 피어 데드를 선언하는 keepalive 메시지를 수신하지 않은 후 최소 간격(초)을 Hold time 필드에 입력합니다.

24단계 왼쪽 창의 **Advanced**를 클릭합니다.

25단계 (선택 사항) **Enable Authentication** 확인란을 선택하여 두 BGP 피어 사이의 TCP 연결에 대한 MD5 인증을 활성화합니다.

- Encryption Type 드롭다운 목록에서 암호화 유형을 선택합니다.
- 비밀번호 필드에 비밀번호를 입력합니다. Confirm Password 필드에 비밀번호를 다시 입력합니다.

참고 비밀번호는 대/소문자를 구분하며 **service password-encryption** 명령이 활성화된 경우 최대 25자, **service password-encryption** 명령이 활성화되지 않은 경우 최대 81자입니다. 첫 번째 문자는 숫자가 될 수 없습니다. 문자열은 공백을 포함하여 모든 영숫자를 포함할 수 있습니다. number-space-anything 형식의 비밀번호는 지정할 수 없습니다. 숫자에 공백이 오면 인증이 실패할 수 있습니다.

26단계 (선택 사항) **Send Community Attribute to this neighbor** 확인란을 선택합니다.

27단계 (선택 사항) **Use ASA as next hop for neighbor** 확인란을 선택하여 라우터를 BGP speaking 인접 디바이스 또는 피어 그룹을 위한 next-hop으로 구성합니다.

28단계 다음 중 하나를 수행합니다.

- **Allow connections with neighbor that is not directly connected**를 클릭하여 직접 연결되지 않은 네트워크에 상주하는 외부 피어로의 BGP 연결을 승인 및 시도합니다.
  - (선택 사항) time-to-live를 TTL hops 필드에 입력합니다. 유효한 값은 1~255입니다.
  - (선택 사항) **Disable connection verification** 확인란을 선택하여 연결 확인을 비활성화하고 루프백 인터페이스를 사용하는 single-hop 피어와의 eBGP 피어링 세션을 설정합니다.
- **Limit number of TTL hops to neighbor**를 클릭하여 BGP 피어링 세션을 활성화합니다.
  - eBGP 피어를 구분하는 최대 홉 개수를 TTL hops 필드에 입력합니다. 유효한 값은 1~254입니다.

29단계 (선택 사항) BGP 인접 디바이스 연결에 대한 가중치를 Weight 필드에 입력합니다.

30단계 BGP 버전 드롭다운 목록에서 ASA가 수락할 BGP 버전을 선택합니다.

참고 버전을 2로 설정하여 소프트웨어가 지정된 인접 디바이스에서 버전 2만 사용하도록 강제할 수 있습니다. 기본값은 버전 4를 사용하고 요청 시 동적으로 버전 2까지 사용할 수 있도록 하는 것입니다.

31단계 (선택 사항) **TCP Path MTU Discovery** 확인란을 선택하여 BGP 세션에 대한 TCP 전송 세션을 활성화합니다.

32단계 TCP 전송 모드 드롭다운 목록에서 TCP 연결 모드를 선택합니다.

33단계 왼쪽 창의 **Migration**을 클릭합니다.

34단계 (선택 사항) **Customize the AS number for routes received from the neighbor** 확인란을 선택하여 eBGP 인접 디바이스에서 수신된 경로에 대한 AS_PATH 속성을 사용자 정의합니다.

- Local AS Number 필드에 로컬 자율 시스템 번호를 입력합니다. 유효한 값은 1~65535입니다.
- (선택 사항) **Do not prepend local AS number for routes received from neighbor** 확인란을 선택합니다. 로컬 AS 번호는 eBGP 피어에서 수신된 경로 앞에 추가되지 않습니다.
- (선택 사항) **Replace real AS number with local AS number in routes received from neighbor** 확인란을 선택합니다. 로컬 라우팅 프로세스에서의 AS 번호는 접두사로 추가되지 않습니다.
- (선택 사항) **Accept either real AS number or local AS number in routes received from neighbor** 확인란을 선택합니다.

35단계 **OK**를 클릭합니다.

36단계 **Apply**를 클릭합니다.

IPv4 네트워크 설정 구성

이 섹션은 BGP 라우팅 프로세스가 알릴 네트워크를 정의합니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > IPv4 Family**를 선택합니다.

2단계 **Networks**를 클릭합니다.

Define networks to be advertised by the BGP routing process configuration 창이 표시됩니다.

3단계 **Add**를 클릭합니다.

Add Network 창이 표시됩니다.

4단계 주소 필드에 BGP가 알릴 네트워크를 지정합니다.

5단계 (선택 사항) Netmask 드롭다운 목록에서 네트워크 또는 서브 네트워크 마스크를 선택합니다.

6단계 경로 지도 드롭다운 목록에서 알릴 네트워크를 필터링하기 위해 검사할 경로 지도를 선택합니다. **Manage**를 클릭하여 경로 지도를 구성하거나 추가합니다.

7단계 **OK**를 클릭합니다.

8단계 **Apply**를 클릭합니다.

재분배 설정 구성

이 섹션은 다른 라우팅 도메인의 경로로부터 BGP로 재배포하는 조건을 정의하기 위한 단계를 설명합니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > IPv4 Family**를 선택합니다.

2단계 **Redistribution**을 클릭합니다.

Redistribution 창이 표시됩니다.

3단계 **Add**를 클릭합니다.

Add Redistribution 창이 표시됩니다.

4단계 소스 프로토콜 드롭다운 목록에서 BGP 도메인으로 경로를 재배포할 프로토콜을 선택합니다.

5단계 Process ID 드롭다운 목록에서 소스 프로토콜에 대한 프로세스 ID를 선택합니다.

6단계 (선택 사항) 메트릭 필드에 재배포된 경로를 위한 메트릭을 입력합니다.

7단계 경로 지도 드롭다운 목록에서 재배포할 네트워크를 필터링하기 위해 검사할 경로 지도를 선택합니다. **Manage**를 클릭하여 경로 지도를 구성하거나 추가합니다.

8단계 Internal, External 및 NSSA External Match 확인란을 하나 이상 선택하여 OSPF 네트워크로부터 경로를 재배포합니다.

참고 이 단계는 OSPF 네트워크로부터의 재배포에만 적용됩니다.

9단계 **OK**를 클릭합니다.

10단계 **Apply**를 클릭합니다.

경로 삽입 설정 구성

이 섹션에서는 BGP 라우팅 테이블에 조건부로 삽입할 경로를 정의하기 위한 단계를 설명합니다.

절차

1단계 ASDM에서 **Configuration > Device Setup > Routing > BGP > IPv4 Family**를 선택합니다.

2단계 **Route Injection**을 클릭합니다.

Route Injection 창이 표시됩니다.

3단계 **Add**를 클릭합니다.

Add Conditionally injected route 창이 표시됩니다.

4단계 Inject Map 드롭다운 목록에서 로컬 BGP 라우팅 테이블에 삽입할 접두사를 지정하는 경로 지도를 선택합니다.

5단계 Exist Map 드롭다운 목록에서 BGP 스피커가 추적할 접두사를 포함한 경로 지도를 선택합니다.

6단계 **Injected routes will inherit the attributes of the aggregate route** 확인란을 선택하여 삽입된 경로가 종합 경로의 속성을 물려받도록 구성합니다.

7단계 **OK**를 클릭합니다.

8단계 **Apply**를 클릭합니다.

BGP 모니터링

다음 명령을 사용하여 BGP 라우팅 프로세스를 모니터링할 수 있습니다. 명령 출력의 예와 설명은 명령 참조에서 참조하십시오. 또한 인접 디바이스 변경 메시지 및 인접 디바이스 경고 메시지의 로깅을 비활성화할 수 있습니다.

다양한 BGP 라우팅 통계를 모니터링하려면 다음 단계를 수행:

참고 BGP 로그 메시지를 비활성화하려면 **no bgp log-neighbor-changes** 명령을 라우터 컨피그레이션 모드에 입력합니다. 이는 인접 디바이스 변경 메시지 로깅을 비활성화합니다. 이 명령을 BGP 라우팅 프로세스에 대한 라우터 컨피그레이션 모드에 입력합니다.
기본적으로 인접 디바이스 변경 사항은 로깅됩니다.

- **Monitoring > Routing > BGP Neighbors**

  각 행은 하나의 BGP 인접 디바이스를 나타냅니다. 각 인접 디바이스에 대해 목록은 IP 주소, AS 번호, 라우터 ID, 상태(활성, 유휴 등), 가동 시간, graceful restart 기능, 다시 시작 시간 및 stalepath 시간을 포함합니다.

- **Monitoring > Routing > BGP Routes**

  각 행은 하나의 BGP 경로를 나타냅니다. 각 행에 대해 목록은 상태 코드, IP 주소, next hop 주소, 경로 메트릭, 로컬 기본 설정 값, 가중치 및 경로를 포함합니다.

BGP 내역

표 22-1에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 22-1 BGP 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
BGP 지원	9.2(1)	데이터 라우팅, 인증 수행, Border Gateway Protocol을 사용한 라우팅 정보 재배포 및 모니터링에 대한 지원이 추가되었습니다. 다음 ASDM 화면을 도입했습니다. Configuration > Device Setup > Routing > BGP Monitoring > Routing > BGP Neighbors, Monitoring > Routing > BGP Routes 다음 ASDM 화면을 수정했습니다. Configuration > Device Setup > Routing > Static Routes> Add > Add Static Route Configuration > Device Setup > Routing > Route Maps> Add > Add Route Map
ASA 클러스터링을 위한 BGP 지원	9.3(1)	L2 및 L3 클러스터링에 대한 지원을 추가했습니다. 다음 ASDM 화면을 수정했습니다. Configuration > Device Setup > Routing > BGP > IPv4 Family > General
NSF를 위한 BGP 지원	9.3(1)	무중단 전달을 위한 지원을 추가했습니다. 다음 ASDM 화면을 수정했습니다. Configuration > Device Setup > Routing > BGP > General, Configuration > Device Setup > Routing > BGP > IPv4 Family > Neighbor, Monitoring > Routing > BGP Neighbors
광고 맵을 위한 BGP 지원	9.3(1)	BGPv4 광고 맵 지원을 추가했습니다. 다음 ASDM 화면을 수정했습니다. Configuration > Device Setup > Routing > BGP > IPv4 Family > Neighbor > Add BGP Neighbor > Routes

23장

OSPF

이 장에서는 OSPF(Open Shortest Path First) 라우팅 프로토콜을 사용하여 데이터를 라우팅하고, 인증을 수행하고, 라우팅 정보를 재배포할 수 있도록 Cisco ASA를 구성하는 방법에 대해 설명합니다.

이 장에는 다음 섹션이 포함됩니다.

OSPF 정보

OSPF는 경로 선택 시 거리 벡터 대신 링크 상태를 사용하는 내부 게이트웨이 라우팅 프로토콜입니다. OSPF는 라우팅 테이블 업데이트가 아닌 링크 상태 광고를 전파합니다. 전체 라우팅 테이블 대신 LSA만 교환되므로, OSPF 네트워크는 RIP 네트워크보다 더 빠르게 통합될 수 있습니다.

OSPF는 링크 상태 알고리즘을 사용하여 알려진 모든 목적지에 도달하기 위한 최단 경로를 구축하고 계산합니다. OSPF 영역의 각 라우터에는 동일한 링크 상태 데이터베이스가 포함되며, 여기에는 각 라우터의 사용 가능한 인터페이스 및 연결 가능한 인접 디바이스 목록이 있습니다.

RIP를 능가하는 OSPF의 장점은 다음과 같습니다.

- OSPF 링크 상태 데이터베이스 업데이트는 RIP 업데이트보다 전송되는 빈도가 적으며, 링크 상태 데이터베이스는 천천히 업데이트되지 않고 오래된 정보의 기간이 만료되는 즉시 업데이트됩니다.
- 라우팅 결정은 비용을 기준으로 하며, 이는 특정 인터페이스 전체에 패킷을 전송하는 데 필요한 오버헤드를 나타낸 것입니다. ASA에서는 목적지까지의 홉 개수가 아닌 링크 대역폭을 기준으로 인터페이스의 비용을 계산합니다. 비용을 구성하여 선호하는 경로를 지정할 수 있습니다.

최단 경로 우선 알고리즘의 단점은 CPU 주기 및 메모리가 많이 필요하다는 점입니다.

ASA에서는 OSPF 프로토콜의 프로세스 2개를 다른 인터페이스 집합에서 동시에 실행합니다. 동일한 IP 주소를 사용하는 인터페이스가 있을 경우 2개의 프로세스를 실행하고자 할 수 있습니다(NAT 사용 시 이러한 인터페이스가 공존할 수 있으나, OSPF에서는 중복 주소를 허용하지 않음). 또는 내부에서 한 프로세스를 실행하고 외부에서 다른 프로세스를 실행한 다음, 두 프로세스 간의 경로 하위 집합을 재배포하고자 할 수 있습니다. 이 경우에도 마찬가지로, 사설 주소를 공용 주소에서 분리해야 할 수 있습니다.

경로를 다른 OSPF 라우팅 프로세스, RIP 라우팅 프로세스 또는 OSPF 지원 인터페이스에서 구성된 고정 및 연결된 경로의 OSPF 라우팅 프로세스로 재배포할 수 있습니다.

ASA에서는 다음과 같은 OSPF 기능을 지원합니다.

- 영역 내, 영역 간 및 외부(유형 I 및 유형 II) 경로
- 가상 링크
- L SA 플러딩
- OSPF 패킷에 대한 인증(비밀번호 및 MD5 인증)
- ASA를 전용 라우터 또는 전용 백업 라우터로 구성. ASA는 ABR로 설정할 수도 있습니다.
- 스텁 영역 및 not-so-stubby 영역
- 영역 경계 라우터 유형 3 LSA 필터링

OSPF에서는 MD5 및 일반 텍스트 인접 디바이스 인증을 지원합니다. OSPF와 다른 프로토콜(예: RIP) 간의 경로 재배포 시 공격자가 라우팅 정보를 교란시키기 위해 이를 이용할 우려가 있으므로, 가능한 경우 모든 라우팅 프로토콜에 인증을 사용해야 합니다.

NAT를 사용하면 OSPF가 공용 및 사설 영역에서 가동되며, 주소 필터링이 필요한 경우 2개의 OSPF 프로세스를 실행해야 합니다. 하나는 공용 영역에 사용되는 프로세스이고 다른 하나는 사설 영역에서 사용되는 프로세스입니다.

여러 영역에 인터페이스가 있는 라우터는 ABR(영역 경계선 라우터)라고 합니다. OSPF를 사용하는 라우터와 다른 라우팅 프로토콜을 사용하는 라우터 간에 트래픽을 재배포하는 게이트웨이 역할을 수행하는 라우터를 ASBR(자동 시스템 경계 라우터)이라고 합니다.

ABR에서는 LSA를 사용하여 사용 가능한 경로에 대한 정보를 다른 OSPF 라우터로 전송합니다. ABR 유형 3 LSA 필터링을 사용할 경우, ABR 역할을 수행하는 ASA를 통해 별도의 사설 및 공용 영역을 확보할 수 있습니다. 유형 3 LSA(영역 간 경로)는 한 영역에서 다른 영역으로 필터링할 수 있으며, 이렇게 하면 사설 네트워크를 광고하지 않고도 NAT와 OSPF를 함께 사용할 수 있습니다.

참고 유형 3 LSA만 필터링할 수 있습니다. 사설 네트워크에서 ASA를 ASBR로 구성하면 사설 네트워크를 설명하는 유형 5 LSA가 전송되며, 이 경우 공용 영역을 비롯한 전체 AS에 플러딩이 발생합니다.

NAT가 적용되었으나 공용 영역에서 OSPF만 실행 중인 경우, 공용 네트워크에 대한 경로가 사설 네트워크 내부에 기본 또는 유형 5 AS 외부 LSA로서 재배포될 수 있습니다. 그러나 ASA에서 보호하는 사설 네트워크에 대한 고정 경로를 구성해야 합니다. 또는 동일한 ASA 인터페이스에서 공용 네트워크와 사설 네트워크를 혼합할 수 없습니다.

ASA에서 하나는 RIP 라우팅 프로세스, 다른 하나는 EIGRP 라우팅 프로세스로 된 2개의 OSPF 라우팅 프로세스를 동시에 실행할 수 있습니다.

OSPF Support for Fast Hello Packets 기능

OSPF Support for Fast Hello Packets 기능에서는 hello 패킷을 1초 미만의 간격으로 전송하도록 구성하는 방법을 제공합니다. 이러한 컨피그레이션을 통해 OSPF(Open Shortest Path First) 네트워크에서 통합 속도를 단축할 수 있습니다.

OSPF Support for Fast Hello Packets 기능의 사전 요구 사항

OSPF는 네트워크에서 기존에 구성해야 하거나 OSPF Support for Fast Hello Packets 기능과 동시에 구성해야 합니다.

OSPF Support for Fast Hello Packets 기능 정보

다음 섹션에서는 OSPF Support for Fast Hello Packets 기능과 관련된 개념에 대해 설명합니다.

- OSPF Hello 간격 및 Dead 간격
- OSPF Fast Hello Packets
- OSPF Fast Hello Packets 기능의 이점

OSPF Hello 간격 및 Dead 간격

OSPF Hello 패킷은 OSPF 프로세스에서 OSPF 인접 디바이스와의 연결을 유지하기 위해 이러한 인접 디바이스에 전송하는 패킷입니다. Hello 패킷은 구성 가능한 간격(초 단위)으로 전송됩니다. 기본값은 이더넷 링크의 경우 10초이고, 비 브로드캐스트 링크의 경우 30초입니다. Hello 패킷에는 Dead 간격 내에 수신된 Hello 패킷에 대한 모든 인접 디바이스 목록이 포함됩니다. Dead 간격도 구성 가능한 간격(초 단위)이며, 기본값은 Hello 간격 값의 4배로 설정됩니다. 모든 Hello 간격의 값은 네트워크 내에서 동일해야 합니다. 마찬가지로, 모든 Dead 간격의 값도 네트워크 내에서 동일해야 합니다.

이러한 두 간격의 상호 작용을 통해 링크가 작동 중임을 나타내어 연결을 유지할 수 있습니다. 라우터가 Dead 간격 내에 인접 디바이스에서 Hello 패킷을 수신하지 못할 경우, 해당 인접 디바이스는 중단된 것으로 선언됩니다.

OSPF Fast Hello Packets

OSPF Fast Hello 패킷은 1초 미만의 간격으로 전송되는 Hello 패킷을 참조합니다. Fast Hello 패킷에 대한 내용을 이해하려면 OSPF Fast Hello 패킷과 Dead 간격 간의 관계에 대해서도 숙지해야 합니다. 23-3 페이지의 OSPF Hello 간격 및 Dead 간격를 참조하십시오.

OSPF Fast Hello Packets 기능은 **ospf dead-interval** 명령을 사용하여 구현할 수 있습니다. Dead 간격은 1초로 설정되고, hello 승수 값은 1초 동안 전송하려는 Hello 패킷의 수로 설정되므로 1초 미만의 또는 "빠른" Hello 패킷이 제공됩니다.

Fast Hello 패킷이 인터페이스에서 구성되면, 이 인터페이스로 전송되는 Hello 패킷에서 광고되는 Hello 간격은 0으로 설정됩니다. 이 인터페이스를 통해 수신되는 Hello 인터페이스의 Hello 간격은 무시됩니다.

Dead 간격은 세그먼트에서 일정해야 하며, 1초로 설정되거나(Fast Hello 패킷의 경우) 다른 값으로 설정됩니다. Hello 승수의 경우에는 Dead 간격 내에 최소 하나 이상의 Hello 패킷이 전송된다면 전체 세그먼트에서 동일하지 않아도 됩니다.

OSPF Fast Hello Packets 기능의 이점

OSPF Fast Hello Packets 기능의 이점은 OSPF 네트워크에서 Fast Hello 패킷을 사용하지 않는 경우와 비교했을 때 더 빠른 통합이 가능하다는 점입니다. 이 기능을 사용하면 1초 내에 손실된 인접 디바이스를 감지할 수 있습니다. 이 기능은 특히 OSI(Open System Interconnection) 물리적 레이어 및 데이터 링크 레이어로 감지할 수 없는 인접 디바이스가 손실된 LAN 세그먼트에 유용합니다.

OSPFv2와 OSPFv3의 구현 차이점

OSPFv3는 이전 버전인 OSPFv2와 호환되지 않습니다. OSPF를 사용하여 IPv4와 IPv6 트래픽을 모두 라우팅하려면 OSPFv2와 OSPFv3를 동시에 실행해야 합니다. 이들은 서로 공존하지만 상호 작용을 수행하지는 않습니다.

OSPFv3에서 제공하는 추가 기능은 다음과 같습니다.

- 링크당 프로토콜 처리
- 주소 지정 시맨틱 제거
- 플러딩 범위 추가
- 링크당 다중 인스턴스 지원
- IPv6 링크-로컬 주소를 사용하여 인접 디바이스 검색 및 기타 기능 지원
- LSA를 접두사와 접두사 길이로 표시
- LSA 유형 2개 추가
- 알 수 없는 LSA 유형 처리
- RFC-4552에 지정된 대로, OSPFv3 라우팅 프로토콜 트래픽에 IPsec ESP 표준을 사용한 인증 지원

OSPF에 대한 지침

컨텍스트 모드 지침

OSPFv2에서는 단일 또는 다중 컨텍스트 모드를 지원합니다.

OSPFv3에서는 단일 모드만 지원합니다.

방화벽 모드 지침

OSPF에서는 라우팅 방화벽 모드만 지원합니다. OSPF에서는 투명 방화벽 모드를 지원하지 않습니다.

장애 조치 지침

OSPFv2 및 OSPFv3에서는 스테이트풀 장애 조치를 지원합니다.

IPv6 지침

- OSPFv2에서는 IPv6을 지원하지 않습니다.
- OSPFv3에서는 IPv6을 지원합니다.
- OSPFv3에서는 인증에 IPv6을 사용합니다.
- ASA에서는 OSPFv3 경로가 최상의 경로인 경우, 이를 IPv6 RIB에 설치합니다.
- OSPFv3 패킷은 **capture** 명령에서 IPv6 ACL을 사용하여 필터링할 수 있습니다.

클러스터링 지침

- OSPFv2 및 OSPFv3에서는 클러스터링을 지원합니다.
- OSPFv3 암호화는 지원되지 않습니다. 클러스터링 환경에서 OSPFv3 암호화를 구성하려고 할 경우 오류 메시지가 표시됩니다.
- Spanned 인터페이스 모드의 경우, 전용 관리 인터페이스에 동적 라우팅을 지원하지 않습니다.
- 개별 인터페이스 모드의 경우, 마스터 및 슬레이브 유닛을 OSPFv2 또는 OSPFv3 인접 디바이스로 설정해야 합니다.
- OSPFv2 및 EIGRP를 모두 설정할 경우, Spanned 인터페이스 모드 또는 개별 인터페이스 모드를 사용할 수 있으며 두 가지 모드를 동시에 사용할 수는 없습니다.
- 개별 인터페이스 모드의 경우, OSPFv2 인접성은 마스터 유닛의 공유 인터페이스에 있는 두 컨텍스트 간에만 설정할 수 있습니다. 고정 인접 디바이스 구성은 포인트-투-포인트 링크에서만 지원되므로, 하나의 인터페이스에서는 하나의 인접 디바이스 명령문만 허용됩니다.
- 라우터 ID는 OSPFv2, OSPFv3 및 EIGRP 경로 컨피그레이션 모드의 선택 사항입니다. 라우터 ID를 명시적으로 설정하지 않을 경우, 라우터 ID가 자동으로 생성되며 각 클러스터 유닛의 모든 데이터 인터페이스에서 가장 높은 IPv4 주소로 설정됩니다.
- 클러스터 인터페이스 모드를 구성하지 않은 경우, 점으로 구분된 단일한 십진수 IPv4 주소만 라우터 ID로 사용할 수 있으며 **cluster pool** 옵션이 비활성화됩니다.
- 클러스터 인터페이스 모드가 Spanned 컨피그레이션으로 설정된 경우, 점으로 구분된 단일한 십진수 IPv4 주소만 라우터 ID로 사용할 수 있으며 **cluster pool** 옵션이 비활성화됩니다.
- 클러스터 인터페이스 모드가 개별 컨피그레이션으로 설정된 경우, **cluster pool** 옵션을 필수이며 점으로 구분된 단일한 십진수 IPv4 주소를 라우터 ID로 사용할 수 없습니다.
- **check-detail** 또는 **nocheck** 옵션을 지정하지 않은 상태로 클러스터 인터페이스 모드가 Spanned에서 개별 컨피그레이션으로 변경되거나 그 반대로 변경될 경우, 라우터 ID를 포함한 전체 컨피그레이션이 제거됩니다.
- 동적 라우팅 프로토콜 라우터 ID 컨피그레이션이 새 인터페이스 모드와 호환되지 않을 경우, 콘솔에 오류 메시지가 표시되며 인터페이스 모드 CLI에 오류가 발생합니다. 오류 메시지에는 동적 라우팅 프로토콜(OSPFv2, OSPFv3, EIGRP)당 내용이 한 줄씩 포함되며 컨피그레이션 비호환이 발생한 각 컨텍스트의 이름이 나열됩니다.
- **cluster interface mode** 명령에 **nocheck** 옵션이 지정되지 않은 경우, 모든 라우터 ID 컨피그레이션이 새 모드와 호환되지 않는 경우에도 인터페이스 모드를 변경할 수 있습니다.
- 클러스터가 활성화되어 있으면 라우터 ID 호환성 확인이 반복됩니다. 비호환성이 감지되면 **cluster enable** 명령이 실패합니다. 관리자는 클러스터를 활성화하기 전에 호환되지 않는 ID 컨피그레이션을 올바르게 수정해야 합니다.
- 유닛에 클러스터가 슬레이브로 들어올 경우, **cluster interface mode** 명령에 **nocheck** 옵션을 지정하여 라우터 ID 호환성 확인 오류를 방지하는 것이 좋습니다. 슬레이브 유닛은 마스터 유닛에서 라우터 컨피그레이션을 계속 상속합니다.
- 클러스터에서 마스터 권한 역할이 변경될 경우, 다음 동작이 발생합니다.
  - Spanned 인터페이스 모드의 경우, 라우터 프로세스는 마스터 유닛에서만 액티브 상태이며 슬레이브 유닛에서는 일시 중단 상태입니다. 마스터 유닛에서 컨피그레이션이 동기화되었으므로 각 클러스터 유닛에서는 동일한 라우터 ID를 보유하게 됩니다. 결과적으로, 인접한 라우터에서는 역할이 변경되는 동안 클러스터의 라우터 ID 변경을 알 수 없습니다.
  - 개별 인터페이스 모드의 경우 라우터 프로세스는 모든 개별 클러스터 유닛에서 액티브 상태입니다. 각 클러스터 유닛에서는 구성된 클러스터 풀에서 고유한 개별 라우터 ID를 선택합니다. 클러스터에서 마스터 권한 역할이 변경되어도 라우팅 토폴로지는 변경되지 않습니다.

추가 지침

- OSPFv2 및 OSPFv3에서는 하나의 인터페이스에 여러 인스턴스를 지원합니다.
- OSPFv3에서는 클러스터링되지 않은 환경에서 ESP 헤더를 통해 암호화를 지원합니다.
- OSPFv3에서는 Non-Payload Encryption을 지원합니다.
- OSPFv2에서는 RFCs 4811, 4812 및 3623에서 각각 정의된 대로 Cisco NSF Graceful Restart 및 IETF NSF Graceful Restart 메커니즘을 지원합니다.
- OSPFv3에서는 RFC 5187에 정의된 대로 Graceful Restart 메커니즘을 지원합니다.

OSPFv2 구성

이 섹션에서는 ASA에 OSPFv2 프로세스를 활성화하는 방법에 대해 설명합니다.

OSPFv2를 활성화한 후에는 경로 맵을 정의해야 합니다. 자세한 내용은 21-4 페이지의 경로 맵을 정의를 참조하십시오. 그런 다음 기본 경로를 생성합니다. 자세한 내용은 20-2 페이지의 고정 경로 구성를 참조하십시오.

OSPFv2 프로세스의 경로 맵을 정의한 후에는 특정한 요구 사항에 맞게 이를 맞춤화할 수 있습니다. ASA에서 OSPFv2 프로세스를 맞춤화하는 방법을 알아보려면 23-7 페이지의 OSPFv2 맞춤화를 참조하십시오.

OSPFv2를 활성화하려면 OSPFv2 라우팅 프로세스를 생성한 후 라우팅 프로세스와 관련된 IP 주소 범위를 지정한 다음, 해당 IP 주소 범위와 관련된 영역 ID를 할당해야 합니다.

최대 2개의 OSPFv2 프로세스 인스턴스를 활성화할 수 있습니다. 각 OSPFv2 프로세스에는 고유한 관련 영역 및 네트워크가 있습니다.

OSPFv2를 활성화하려면 다음 단계를 수행합니다.

절차

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

OSPF Setup 창에서 OSPF 프로세스를 활성화하고, OSPF 영역 및 네트워크를 구성하고, OSPF 경로 요약을 정의할 수 있습니다.

2단계 ASDM에서 다음 세 가지 탭을 사용하여 OSPF를 활성화할 수 있습니다.

- **Process Instances** 탭을 사용하면 각 컨텍스트에 최대 2개의 OSPF 프로세스 인스턴스를 활성화할 수 있습니다. 단일 컨텍스트 모드 및 다중 컨텍스트 모드가 모두 지원됩니다. **Enable Each OSPF Process** 확인란을 선택한 후에는 해당 OSPF 프로세스의 고유한 식별자 숫자 ID를 입력할 수 있습니다. 이 프로세스 ID는 내부에서 사용되며 다른 OSPF 디바이스의 OSPF 프로세스 ID와 일치하지 않아도 됩니다. 유효한 값의 범위는 1~65535입니다. 각 OSPF 프로세스에는 고유한 관련 영역 및 네트워크가 있습니다.

  Advanced를 클릭하면 Edit OSPF Process Advanced Properties 대화 상자가 표시됩니다. 여기에서 각 OSPF 프로세스에 대한 Router ID, Spanned EtherChannel 또는 Individual Interface 클러스터링의 클러스터 IP 주소 풀, Adjacency Changes, Administrative Route Distances, Timers, Default Information Originate 설정을 구성할 수 있습니다.

- **Area/Networks** 탭을 사용하면 ASA에서 각 OSPF 프로세스에 포함하는 영역 및 네트워크를 표시할 수 있습니다. 이 탭에서 영역 ID, 영역 유형 및 영역의 인증 집합 유형을 표시할 수 있습니다. OSPF 영역 또는 네트워크를 추가하거나 편집하려면 23-14 페이지의 OSPFv2 영역 매개변수에서 자세한 내용을 참조하십시오.

- **Route Summarization 탭**을 사용하면 ABR을 구성할 수 있습니다. OSPF에서 ABR은 네트워크를 한 영역에서 다른 영역으로 광고합니다. 영역에 네트워크 번호가 어느 정도 할당되어 있고 번호가 연속적일 경우, ABR을 구성하여 지정된 범위에 속하는 영역 내의 모든 개별 네트워크가 포함된 요약 경로를 광고할 수 있습니다. 자세한 내용은 23-11 페이지의 OSPFv2 영역 간의 경로 요약 구성를 참조하십시오.

OSPF Fast Hello Packets 구성

이 섹션에서는 OSPF Fast Hello Packets 기능을 구성하는 방법에 대해 설명합니다.

절차

OSPFv2 맞춤화

이 섹션에서는 OSPFv2 프로세스를 맞춤화하는 방법에 대해 설명합니다.

OSPFv2에 경로 재배포

ASA에서는 OSPFv2 라우팅 프로세스 간의 경로 재배포를 제어할 수 있습니다.

참고 지정된 라우팅 프로토콜에서 어떤 경로를 대상 라우팅 프로세스로 재배포할 수 있는지 정의하여 경로를 재배포하려면, 우선 기본 경로를 생성해야 합니다. 20-2 페이지의 고정 경로 구성를 참조한 다음 21-4 페이지의 경로 맵을 정의에 따라 경로 맵을 정의합니다.

고정 경로, 연결된 경로, RIP 또는 OSPFv2 경로를 OSPFv2 프로세스에 재배포하려면 다음 단계를 수행합니다.

절차

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Redistribution**을 선택합니다.

Redistribution 창에는 하나의 라우팅 프로세스에서 OSPF 라우팅 프로세스로 경로를 재배포하기 위한 규칙이 표시됩니다. RIP 및 OSPF에서 검색된 경로를 EIGRP 라우팅 프로세스로 재배포할 수 있습니다. 고정 경로 및 연결된 경로도 EIGRP 라우팅 프로세스로 재배포할 수 있습니다. 고정 경로 또는 연결된 경로가 Setup>Networks 탭을 통해 구성된 네트워크의 범위에 속할 경우, 해당 경로를 재배포하지 않아도 됩니다.

2단계 **Add** 또는 **Edit**를 클릭합니다.

또는 Redistribution 창이 있는 경우 이 창에서 테이블 항목을 두 번 클릭하면 선택한 항목에 대한 Add/Edit OSPF Redistribution Entry 대화 상자가 열립니다.

참고 다음 모든 단계는 선택 사항입니다.

Add/Edit OSPF Redistribution Entry 대화 상자를 사용하면 Redistribution 테이블에서 새 재배포 규칙을 추가하거나 기존 재배포 규칙을 편집할 수 있습니다. 기존 재배포 규칙을 편집할 경우 일부 재배포 규칙 정보는 변경할 수 없습니다.

3단계 경로 재배포 항목과 관련된 OSPF 프로세스를 선택합니다. 기존 재배포 규칙을 편집할 경우 이 설정은 변경할 수 없습니다.

4단계 경로가 재배포되는 소스 프로토콜을 선택합니다. 다음 중 하나를 선택할 수 있습니다.

- Static — 고정 경로를 OSPF 라우팅 프로세스에 재배포합니다.
- Connected — 연결된 경로(인터페이스에서 IP 주소를 활성화하여 자동으로 설정된 경로)를 OSPF 연결 프로세스에 재배포합니다. 연결된 경로는 AS에 외부 경로로 재배포할 수 있습니다.
- OSPF — OSPF 라우팅 프로세스에서 경로를 재배포합니다. 목록에서 OSPF 프로세스 ID를 선택합니다. 이 프로토콜을 설정할 경우 이 대화 상자에서 Match 옵션이 표시됩니다. 고정 경로, 연결된 경로, RIP 또는 EIGRP 경로를 재배포할 경우 이러한 옵션이 제공되지 않습니다. 이 경우 5단계로 건너뜁니다.
- RIP — RIP 라우팅 프로세스에서 경로를 재배포합니다.
- BGP — BGP 라우팅 프로세스에서 경로를 재배포합니다.
- EIGRP — EIGRP 라우팅 프로세스에서 경로를 재배포합니다. 목록에서 EIGRP 라우팅 프로세스의 자동 시스템 번호를 선택합니다.

5단계 소스 프로토콜에 대한 OSPF를 선택한 경우, 다른 OSPF 라우팅 프로세스에서 선택한 OSPF 라우팅 프로세스로 경로를 재배포하는 데 사용되는 조건을 선택합니다. 고정 경로, 연결된 경로, RIP 또는 EIGRP 경로를 재배포할 경우 이러한 옵션이 제공되지 않습니다. 경로는 재배포하려고 선택한 조건과 일치해야 합니다. 다음과 같은 하나 이상의 일치 조건을 선택할 수 있습니다.

- Internal — 특정 AS의 내부에 있는 경로입니다.
- External 1 — 자동 시스템의 외부에 있지만, OSPF에 Type 1 외부 경로로서 가져온 경로입니다.
- External 2 — 자동 시스템의 외부에 있지만, OSPF에 Type 2 외부 경로로서 가져온 경로입니다.
- NSSA External 1 — 자동 시스템의 외부에 있지만, OSPF에 Type 2 NSSA 경로로서 가져온 경로입니다.

- NSSA External 2 — 자동 시스템의 외부에 있지만, OSPF에 Type 2 NSSA 경로로서 가져온 경로입니다.

6단계 Metric Value 필드에 재배포되는 경로의 메트릭 값을 입력합니다. 유효한 값의 범위는 1~16777214입니다.

하나의 OSPF 프로세스에서 동일한 디바이스의 다른 OSPF 프로세스로 재배포할 경우, 메트릭 값이 지정되지 않으면 한 프로세스에서 다른 프로세스로 메트릭이 이동됩니다. OSPF 프로세스에 다른 프로세스를 재배포할 경우, 메트릭 값이 지정되어 있지 않으면 기본 메트릭은 20입니다.

7단계 Metric Type에 다음 옵션 중 하나를 선택합니다.

- 메트릭이 Type 1 외부 경로이면 **1**을 선택합니다.
- 메트릭이 Type 2 외부 경로이면 **2**를 선택합니다.

8단계 Tag Value 필드에 태그 값을 입력합니다.

태그 값은 OSPF에서 직접 사용하지 않지만 ASBR 간에 정보를 주고받는 데 사용될 수 있는 각 외부 경로에 연결된 32비트 십진수 값입니다. 유효한 값의 범위는 0~4294967295입니다.

9단계 서브네팅된 경로의 재배포를 활성화하려면 **Use Subnets** 확인란을 선택 합니다. 이 확인란의 선택을 취소하면 서브네팅되지 않은 경로만 재배포됩니다.

10단계 재배포 항목에 적용할 경로 맵의 이름을 Route Map 드롭다운 목록에서 선택합니다.

11단계 경로 맵을 추가하거나 구성하려면 **Manage**를 클릭합니다.

Configure Route Map 대화 상자가 나타납니다.

12단계 **Add** 또는 **Edit**를 클릭하여 지정된 라우팅 프로토콜에서 어떤 경로를 대상 라우팅 프로세스로 재배포할 수 있는지 정의합니다. 자세한 내용은 21-4 페이지의 경로 맵을 정의를 참조하십시오.

13단계 **OK**를 클릭합니다.

경로를 OSPFv2로 재배포 시 경로 요약 구성

다른 프로토콜의 경로가 OSPF에 재배포될 경우, 각 경로는 외부 LSA에 개별적으로 광고됩니다. 그러나 ASA를 구성하여 지정된 네트워크 주소 및 마스크에 포함되는 모든 재배포된 경로에 대한 단일 경로를 광고할 수 있습니다. 이렇게 컨피그레이션하면 OSPF 링크 상태 데이터베이스의 크기가 줄어듭니다.

지정된 IP 주소 마스크 쌍과 일치하는 경로는 억제할 수 있습니다. 태그 값을 일치 값으로 사용하여 경로 맵을 통한 재배포를 제어할 수 있습니다.

경로 요약을 구성하려면 다음을 수행합니다.

- 23-9 페이지의 경로 요약 주소 추가
- 23-10 페이지의 OSPF 요약 주소 추가 또는 편집

경로 요약 주소 추가

Summary Address 창에는 각 OSPF 라우팅 프로세스에 구성된 요약 주소에 대한 정보가 표시됩니다.

다른 라우팅 프로토콜에서 파악된 경로도 요약할 수 있습니다. 요약 광고에 사용되는 메트릭은 특정 경로 중에서도 가장 작은 메트릭입니다. 요약 경로는 라우팅 테이블의 크기를 줄이는 데 도움이 됩니다.

OSPF에 요약 경로를 사용하면 OSPF ASBR에서는 단일한 외부 경로를 해당 주소에서 다루는 모든 재배포 경로의 취합본으로 광고하게 됩니다. OSPF로 재배포되는 다른 라우팅 프로토콜의 경로만 요약할 수 있습니다.

참고 OSPF에서는 요약 주소 0.0.0.0 0.0.0.0을 지원하지 않습니다.

네트워크 주소 및 마스크에 포함되는 모든 재배포 경로의 단일한 요약 경로에 대한 소프트웨어 광고를 구성하려면, 다음 단계를 수행합니다.

절차

1단계 기본 ASDM 홈 페이지에서 **Configuration > Device Setup > Routing > OSPF > Summary Address**를 선택합니다.

2단계 **Add**를 클릭합니다.

Add OSPF Summary Address Entry 대화 상자가 나타납니다. Summary Address 테이블에서 기존 항목에 새 항목을 추가할 수 있습니다. 기존 항목을 편집할 경우 일부 주소 정보를 변경할 수 없습니다.

3단계 요약 주소와 연결되어 있는 지정된 OSPF Process ID를 OSPF Process 드롭다운 목록에서 선택합니다. 기존 항목을 편집할 경우 이 정보를 편집할 수 없습니다.

4단계 IP Address 필드에 요약 주소의 IP 주소를 입력합니다. 기존 항목을 편집할 경우 이 정보를 편집할 수 없습니다.

5단계 Netmask 드롭다운 목록에서 요약 주소의 네트워크 마스크를 선택합니다. 기존 항목을 편집할 경우 이 정보를 편집할 수 없습니다.

6단계 **Advertise** 확인란을 선택하여 경로 요약을 광고합니다. 이 확인란의 선택을 취소하면 요약 주소에 속하는 경로가 억제됩니다. 기본적으로 이 확인란은 선택되어 있습니다.

Tag 값에는 각 외부 경로에 연결된 32비트 십진수 값이 표시됩니다. 이 값은 OSPF에서 직접 사용하지 않지만 ASBR 간에 정보를 주고받는 데 사용될 수 있습니다.

7단계 **OK**를 클릭합니다.

OSPF 요약 주소 추가 또는 편집

절차

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

2단계 **Route Summarization** 탭을 클릭합니다.

Add/Edit a Route Summarization Entry 대화 상자가 나타납니다.

Add/Edit a Route Summarization Entry 대화 상자를 사용하면 Summary Address에서 새 항목을 추가하거나 기존 항목을 수정할 수 있습니다. 기존 항목을 편집할 경우 일부 주소 정보를 변경할 수 없습니다.

3단계 요약 주소와 연결되어 있는 지정된 OSPF Process ID를 OSPF Process 드롭다운 목록에서 선택합니다. 기존 항목을 편집할 경우 이 정보를 편집할 수 없습니다.

4단계 IP Address 필드에 요약 주소의 IP 주소를 입력합니다. 기존 항목을 편집할 경우 이 정보를 편집할 수 없습니다.

5단계 Netmask 드롭다운 목록에서 요약 주소의 네트워크 마스크를 입력합니다. 기존 항목을 편집할 경우 이 정보를 편집할 수 없습니다.

6단계 **Advertise** 확인란을 선택하여 경로 요약을 광고합니다. 이 확인란의 선택을 취소하면 요약 주소에 속하는 경로가 억제됩니다. 기본적으로 이 확인란은 선택되어 있습니다.

OSPFv2 영역 간의 경로 요약 구성

경로 요약은 광고된 주소를 통합하는 작업입니다. 이 기능을 사용하면 영역 경계 라우터에 의해 하나의 요약 경로를 다른 영역으로 광고됩니다. OSPF의 경우, 영역 경계 라우터에서는 하나의 영역에 있는 네트워크를 다른 영역으로 광고합니다. 영역에 네트워크 번호가 어느 정도 할당되어 있고 번호가 연속적일 경우, 영역을 구성하여 지정된 범위에 속하는 영역 내의 모든 개별 네트워크가 포함된 요약 경로를 광고할 수 있습니다.

경로 요약을 위한 주소 범위를 정의하려면 다음 단계를 수행합니다.

절차

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

2단계 **Route Summarization** 탭을 클릭합니다.

Add/Edit a Route Summarization Entry 대화 상자가 나타납니다.

Add/Edit a Route Summarization Entry 대화 상자를 사용하면 Summary Address에서 새 항목을 추가하거나 기존 항목을 수정할 수 있습니다. 기존 항목을 편집할 경우 일부 주소 정보를 변경할 수 없습니다.

3단계 Area ID 필드에 OSPF Area ID를 입력합니다. 기존 항목을 편집할 경우 이 정보를 편집할 수 없습니다.

4단계 IP Address 필드에 요약 주소의 IP 주소를 입력합니다. 기존 항목을 편집할 경우 이 정보를 편집할 수 없습니다.

OSPFv2 인터페이스 매개변수 구성

필요한 경우 일부 인터페이스별 OSPFv2 매개변수를 변경할 수 있습니다. 이러한 매개변수는 변경할 필요가 없지만 the Hello interval, the Dead interval, and the Authentication key 같은 인터페이스 매개변수는 연결된 네트워크의 모든 라우터 전반에 걸쳐 일관성을 유지해야 합니다. 이러한 매개변수를 컨피그레이션할 경우, 네트워크의 모든 라우터 컨피그레이션에 호환되는 값이 있는지 확인해야 합니다.

OSPFv2 인터페이스 매개변수를 구성하려면 다음 단계를 수행합니다.

절차

ASDM에서 Interface 창을 사용하면 OSPF 메시지 인증 및 속성 같은 인터페이스별 OSPF 라우팅 속성을 구성할 수 있습니다. OSPF에서 인터페이스를 구성하는 데 도움이 되는 2개의 탭은 다음과 같습니다.

- Authentication 탭에는 ASA 인터페이스에 대한 OSPF 인증 정보가 표시됩니다.
- Properties 탭에는 각 인터페이스에 정의된 OSPF 속성이 표 형식으로 표시됩니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Interface**를 선택합니다.

2단계 **Authentication** 탭을 클릭하여 ASA 인터페이스에 대한 인증 정보를 표시합니다. 표에서 행을 두 번 클릭하면 선택한 인터페이스에 대한 Edit OSPF Authentication Interface 대화 상자가 열립니다.

3단계 **Edit**를 클릭합니다.

Edit OSPF Authentication Interface 대화 상자가 나타납니다. Edit OSPF Interface Authentication 대화 상자를 사용하면 선택한 인터페이스에 대한 OSPF 인증 유형 및 매개변수를 구성할 수 있습니다.

4단계 다음 옵션에 따라 Authentication 드롭다운 목록에서 Authentication 유형을 선택합니다.

- **None** - OSPF 인증을 비활성화합니다.
- **Authentication Password** - 일반 텍스트 비밀번호 인증(보안이 중요한 경우 권장하지 않음)을 사용합니다.
- **MD5** - MD5 인증을 사용합니다(권장).
- **Area**(기본값) - 해당 영역에 지정된 인증 유형을 사용합니다. 영역 인증 구성에 대한 자세한 내용은 23-14 페이지의 OSPFv2 영역 매개변수를 참조하십시오. 영역 인증은 기본적으로 비활성화되어 있습니다. 따라서 영역 인증 유형을 이전에 지정하지 않은 경우, 이 설정을 구성하지 않으면 영역 인증에 대한 인터페이스 집합은 인증이 비활성화되어 있습니다.

5단계 비밀번호 인증이 활성화되어 있을 때 비밀번호를 입력할 수 있는 설정이 포함된 Authentication Password 영역에서 라디오 버튼을 클릭합니다.

a. Enter Password 필드에 최대 8자의 텍스트 문자열을 입력합니다.

b. Re-enter Password 필드에 비밀번호를 다시 입력합니다.

6단계 MD5 인증이 활성화되어 있을 때 MD5 키 및 매개변수를 입력할 수 있는 설정이 포함된 ID 영역에서 MD5 ID 및 키에 대한 설정을 선택합니다. OSPF 인증을 사용하는 인터페이스의 모든 디바이스에서는 동일한 MD5 키와 ID를 사용해야 합니다.

a. Key ID 필드에 숫자 키 식별자를 입력합니다. 유효한 값의 범위는 1~255입니다. 선택한 인터페이스에 대한 Key ID가 표시됩니다.

b. Key 필드에 최대 16바이트의 영숫자 문자열을 입력합니다. 선택한 인터페이스에 대한 키가 표시됩니다.

c. **Add** 또는 **Delete**를 클릭하여 MD5 ID and Key 테이블에 지정된 MD5 키를 추가하거나 삭제합니다.

7단계 **OK**를 클릭합니다.

8단계 **Properties** 탭을 클릭합니다.

9단계 편집할 인터페이스를 선택합니다. 표에서 행을 두 번 클릭하면 선택한 인터페이스에 대한 Properties tab 대화 상자가 열립니다.

10단계 **Edit**를 클릭합니다.

Edit OSPF Interface Properties 대화 상자가 나타납니다. Interface 필드에 OSPF 속성을 구성하려는 인터페이스의 이름이 표시됩니다. 이 필드는 편집할 수 없습니다.

11단계 **Broadcast** 확인란을 선택 또는 취소하여 인터페이스가 브로드캐스트 인터페이스인지 지정합니다.

기본적으로 이 확인란은 이더넷 인터페이스에 선택되어 있습니다. 인터페이스를 포인트-투-포인트 비 브로드캐스트 인터페이스로 지정하려면 이 확인란의 선택을 취소합니다. 인터페이스를 포인트-투-포인트 비 브로드캐스트 인터페이스로 지정하면 OSPF 경로를 VPN 터널을 통해 전송할 수 있습니다.

인터페이스가 포인트-투-포인트 비 브로드캐스트로 구성된 경우, 다음과 같은 제한이 적용됩니다.

- 인터페이스 하나의 인접 디바이스만 정의할 수 있습니다.
- 인접 디바이스를 수동으로 구성해야 합니다. 자세한 내용은 23-18 페이지의 고정 OSPFv2 인접 디바이스 정의를 참조하십시오.
- 암호화 엔드포인트를 가리키는 고정 경로를 정의해야 합니다. 자세한 내용은 20-2 페이지의 고정 경로 구성를 참조하십시오.
- 인터페이스에서 터널을 통해 OSPF가 실행 중일 경우, 업스트림 라우터가 있는 일반 OSPF를 동일한 인터페이스에서 실행할 수 없습니다.
- OSPF 인접 디바이스를 지정하기 전에 암호화 맵을 인터페이스에 바인딩하여 OSPF 업데이트가 VPN 터널을 통해 전달되도록 해야 합니다. OSPF 인접 디바이스를 지정한 후에 암호화 맵을 인터페이스에 바인딩한 경우, **clear local-host all** 명령을 사용하여 OSPF 연결을 지워 OSPF 인접성이 VPN 터널을 통해 설정될 수 있도록 합니다.

12단계 다음 옵션을 구성합니다.

- Cost 필드에 인터페이스를 통한 패킷 전송의 비용을 결정하는 값을 입력합니다. 기본값은 10입니다.
- Priority 필드에 OSPF 라우터 우선순위 값을 입력합니다.

  네트워크에 라우터가 2개 연결될 경우, 두 라우터 모두 전용 라우터가 되려고 시도합니다. 라우터 우선순위가 더 높은 디바이스가 전용 라우터가 됩니다. 연관성이 있을 경우, 라우터 ID가 더 높은 라우터가 전용 라우터가 됩니다.

  이 설정의 유효한 값 범위는 0~255입니다. 기본값은 1입니다. 이 설정을 0으로 입력하면 해당 라우터는 전용 라우터 또는 백업 전용 라우터가 될 수 없습니다. 이 설정은 포인트-투-포인트 비 브로드캐스트 인터페이스로 구성된 인터페이스에는 적용되지 않습니다.
- **MTU Ignore** 확인란을 선택하거나 취소합니다.

  OSPF에서는 인접 디바이스가 공통 인터페이스의 동일한 MTU를 사용하고 있는지 여부를 확인합니다. 인접 디바이스가 DBD 패킷을 교환할 때 이러한 확인이 이루어집니다. DBD 패킷에 수신되는 MTU가 수신 인터페이스에 구성된 IP MTU보다 클 경우, OSPF 인접성이 설정되지 않습니다.
- **Database filter** 확인란을 선택하거나 취소합니다.

  이 설정을 사용하여 동기화 및 플러딩이 진행되는 동안 발신 LSA 인터페이스를 필터링합니다. 기본적으로 OSPF에서는 새로운 LSA를 동일한 영역의 모든 인터페이스로 플러딩하며, LSA가 도달하는 인터페이스는 제외입니다. 완전히 메시된 토폴로지의 경우, 이러한 플러딩이 실행되면 대역폭을 낭비하고 링크 및 CPU를 과도하게 사용할 수 있습니다. 이 확인란을 선택하면 OSPF에서 선택된 인터페이스에 LSA 플러딩을 수행하지 않습니다.

13단계 (선택 사항) **Advanced**를 클릭하여 Edit OSPF Advanced Interface Properties 대화 상자를 표시합니다. 이 대화 상자를 사용하면 OSPF Hello 간격, 재전송 간격, 전송 지연, Dead 간격의 값을 변경할 수 있습니다.

네트워크에 OSPF 문제가 발생할 경우, 일반적으로 기본값에서 이러한 값을 변경하기만 하면 됩니다.

14단계 Intervals 섹션에 다음에 대한 값을 입력합니다.

- Hello Interval - 인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다. Hello 패킷의 값이 작을수록 토폴로지 변경 사항이 더 빨리 감지되지만, 인터페이스에 전송되는 트래픽이 늘어납니다. 이 값은 특정 인터페이스의 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1~8192초입니다. 기본값은 10초입니다.

- Retransmit Interval - 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 초 단위로 지정합니다. 라우터에서 LSA를 인접 디바이스로 전송하면 라우터에서는 승인 메시지가 수신될 때까지 LSA를 보관합니다. 라우터에 승인 메시지가 전송되지 않으면 LSA를 다시 전송합니다. 이 값을 신중하게 설정하지 않으면 불필요한 재전송이 발생할 수 있습니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다. 유효한 값의 범위는 1~8192초입니다. 기본값은 5초입니다.
- Transmit Delay - 인터페이스에서 LSA 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 지정합니다. 업데이트 패킷의 LSA에는 전송 전에 이 필드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 링크를 통해 전송하기 전에 지연이 추가되지 않을 경우, LSA에서 링크를 통해 전파하는 시간은 고려되지 않습니다. 할당된 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다. 이 설정은 속도가 매우 낮은 링크에서 중요성이 더 큽니다. 유효한 값의 범위는 1~8192초입니다. 기본값은 1초입니다.

15단계 Detecting Lost Neighbors 섹션에서 다음 작업 중 하나를 수행합니다.

- **Configure interval within which hello packets are not received before the router declares the neighbor to be down**을 클릭합니다. Dead Interval 필드에서, Hello 패킷이 수신되지 않아 인접 디바이스에서 라우터 중간을 선언하기까지 소요되는 간격을 초 단위로 지정합니다. 유효한 값의 범위는 1~8192초입니다. 이 설정의 기본값은 Hello Interval 필드에 설정된 간격의 4배입니다.
- **Send fast hello packets within 1 seconds dead interval**을 클릭합니다. Hello multiplier 필드에서 1초당 전송되는 Hello 패킷의 수를 지정합니다. 유효한 값은 3~20입니다.

OSPFv2 영역 매개변수

일부 OSPF 영역 매개변수를 구성할 수 있습니다. 이러한 영역 매개변수(다음 작업 목록에 나와 있음)에는 인증 설정, 스텁 영역 정의, 기본 요약 경로에 특정 비용 할당이 포함됩니다. 인증에서는 영역에 무단 액세스를 차단하는 비밀번호 기반의 보호 기능을 제공합니다.

스텁 영역은 외부 경로에 대한 정보가 전송되지 않는 영역입니다. 그 대신, 스텁 영역에는 ABR에서 생성된 기본 외부 경로가 있으며 이는 자동 시스템 외부의 목적지를 위한 경로입니다. OSPF 스텁 영역 지원을 사용하려면 스텁 영역에서 기본 라우팅을 사용해야 합니다.

절차

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

2단계 **Area/Networks** 탭을 클릭합니다.

Add OSPF Area 대화 상자가 나타납니다.

3단계 다음 Area Type 옵션 중 하나를 선택합니다.

- **Normal**을 선택하면 영역이 표준 OSPF 영역으로 됩니다. 이 옵션은 영역을 처음 생성할 때 기본적으로 선택됩니다.
- **Stub**을 선택하면 영역이 스텁 영역으로 됩니다. 스텁 영역의 경우 외부에 라우터 또는 영역이 없습니다. 스텁 영역은 AS 외부 LSA(Type 5 LSA)가 스텁 영역으로 플러딩되는 것을 방지합니다. 스텁 영역을 생성할 때 Summary 확인란의 선택을 취소하여 요약 LSA(Types 3 및 4)가 영역으로 플러딩되는 것을 방지할 수 있습니다.
- **Summary**를 선택하면 스텁 영역에서 영역을 정의할 경우 이 확인란의 선택을 취소하면 LSA가 스텁 영역으로 전송되지 않습니다. 기본적으로 이 확인란은 스텁 영역에 선택되어 있습니다.

- **NSSA**를 선택하면 영역이 not-so-stubby 영역으로 됩니다. NSSA는 Type 7 LSA를 승인합니다. NSSA를 생성할 경우 Summary 확인란의 선택을 취소하면 요약 LSA가 영역으로 플러딩되는 것을 방지할 수 있습니다. Redistribute 확인란의 선택을 취소하고 Default Information Originate 확인란을 선택하여 경로 재배포를 비활성화할 수도 있습니다.

4단계 영역에 추가할 네트워크 또는 호스트의 IP 주소를 IP Address 필드에 입력합니다. **0.0.0.0**을 **0.0.0.0**의 넷마스크와 함께 사용하여 기본 영역을 생성합니다. 한 영역에 **0.0.0.0**만 입력할 수 있습니다.

5단계 영역에 추가할 IP 주소 또는 호스트의 네트워크 마스크를 Network Mask 필드에 입력합니다. 호스트를 추가할 경우 **255.255.255.255** 마스크를 선택합니다.

6단계 다음 옵션 중에서 OSPF Authentication 유형을 선택합니다.

- **None** - OSPF 영역 인증을 비활성화합니다. 이는 기본 설정입니다.
- **Password** - 영역 인증에 일반 텍스트 비밀번호를 제공하며, 이는 보안이 중요한 경우 권장하지 않습니다.
- **MD5** - MD5 인증을 허용합니다.

7단계 OSPF 영역에 대한 기본 비용을 지정하려면 Default Cost 필드에 값을 입력합니다.

유효한 값의 범위는 0~65535입니다. 기본값은 1입니다.

8단계 **OK**를 클릭합니다.

OSPFv2 NSSA 구성

NSSA의 OSPFv2 구현은 OSPFv2 스텁 영역과 비슷합니다. NSSA의 경우 코어의 Type 5 외부 LSA를 영역으로 플러딩하지 않으나, 제한된 방식을 통해 자동 시스템 외부 경로를 영역 내로 가져올 수 있습니다.

NSSA는 재배포를 통해 Type 7 자동 시스템 외부 경로를 NSSA 영역 내로 가져옵니다. 이러한 Type 7 LSA는 NSSA ABR에 의해 Type 5 LSA로 변환되며, 이는 전체 라우팅 도메인에 걸쳐 플러딩됩니다. 변환이 이루어지는 동안 요약 및 필터링이 지원됩니다.

OSPFv2를 사용하는 중앙 사이트를 다른 라우팅 프로토콜을 사용하는 원격 사이트에 연결해야 하는 ISP 또는 네트워크 관리자의 경우 NSSA를 통해 관리 작업을 간소할 수 있습니다.

NSSA를 구현하기 전에는, 원격 사이트의 경로를 스텁 영역으로 재배포할 수 없었고 2개의 라우팅 프로토콜을 유지해야 했기 때문에 기업 사이트 경계선 라우터와 원격 라우터 간의 연결을 OSPFv2 스텁 영역으로 실행할 수 없었습니다. 일반적으로 RIP 같은 단순 프로토콜을 실행하여 재배포를 처리했습니다. NSSA를 활용할 경우, 기업 라우터와 원격 라우터 간의 영역을 NSSA로 정의함으로써 OSPFv2를 확장하여 원격 연결을 지원할 수 있습니다.

이 기능을 사용하기 전에 다음 지침을 고려하십시오.

- 외부 목적지에 도착하는 데 사용할 Type 7 기본 경로를 설정할 수 있습니다. 구성된 경우, 라우터에서는 Type 7 기본값을 NSSA 또는 NSSA 영역 경계 라우터에 생성합니다.
- 동일한 영역 내의 모든 라우터는 해당 영역을 NSSA로 인식해야 합니다. 그렇지 않을 경우 라우터 간에 서로 통신을 수행할 수 없습니다.

절차

1단계 기본 ASDM 홈 페이지에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

2단계 **Area/Networks** 탭을 클릭합니다.

3단계 **Add**를 클릭합니다.

Add OSPF Area 대화 상자가 나타납니다.

4단계 Area Type 영역에서 **NSSA** 라디오 버튼을 클릭합니다.

이 옵션을 선택하면 영역이 not-so-stubby 영역으로 됩니다. NSSA는 Type 7 LSA를 승인합니다. NSSA를 생성할 경우 Summary 확인란의 선택을 취소하면 요약 LSA가 영역으로 플러딩되는 것을 방지할 수 있습니다. Redistribute 확인란의 선택을 취소하고 Default Information Originate 확인란을 선택하여 경로 재배포를 비활성화할 수도 있습니다.

5단계 영역에 추가할 네트워크 또는 호스트의 IP 주소를 IP Address 필드에 입력합니다. **0.0.0.0**을 **0.0.0.0**의 넷마스크와 함께 사용하여 기본 영역을 생성합니다. 한 영역에 **0.0.0.0**만 입력할 수 있습니다.

6단계 영역에 추가할 IP 주소 또는 호스트의 네트워크 마스크를 Network Mask 필드에 입력합니다. 호스트를 추가할 경우 **255.255.255.255** 마스크를 선택합니다.

7단계 Authentication 영역에서 **None** 라디오 버튼을 클릭하여 OSPF 영역 인증을 비활성화합니다.

8단계 OSPF 영역에 대한 기본 비용을 지정하려면 Default Cost 필드에 값을 입력합니다.

유효한 값의 범위는 0~65535입니다. 기본값은 1입니다.

9단계 **OK**를 클릭합니다.

클러스터링(OSPFv2 및 OSPFv3)에 대한 IP 주소 풀 구성

Individual Interface 클러스터링을 사용할 경우 라우터 ID 클러스터 풀에 대한 IPv4 주소의 범위를 할당할 수 있습니다.

절차

OSPFv2를 지원하는 Individual Interface에서 라우터 ID 클러스터에 대한 IPv4 주소의 범위를 할당하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 홈 페이지에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 편집할 OSPF 프로세스를 선택한 다음 **Advanced**를 클릭합니다.

Edit OSPF Process Advanced Properties 대화 상자가 나타납니다.

4단계 **Cluster Pool** 라디오 버튼을 클릭합니다. 클러스터링을 사용할 경우, 라우터 ID에 대한 IP 주소를 지정할 필요가 없습니다(즉, 필드를 비워둡니다). IP 주소 풀을 입력하지 않으면 ASA에서는 자동으로 생성된 라우터 ID를 사용합니다.

5단계 IP 주소 풀의 이름을 입력하거나 말줄임표 기호를 클릭하여 Select IP Address Pool 대화 상자를 표시합니다.

6단계 기존 IP 주소 풀 이름을 두 번 클릭하여 이를 Assign 필드에 추가합니다. 또는 **Add**를 클릭하여 새 IP 주소 풀을 생성합니다.

Add IPv4 Pool 대화 상자가 나타납니다.

7단계 Name 필드에 새 IP 주소 풀 이름을 입력합니다.

8단계 시작 IP 주소를 입력하거나 말줄임표 기호를 클릭하여 Browse Starting IP Address 대화 상자를 표시합니다.

9단계 항목을 두 번 클릭하여 Starting IP Address 필드에 이를 추가한 다음 **OK**를 클릭합니다.

10단계 끝 IP 주소를 입력하거나 말줄임표 기호를 클릭하여 Browse Ending IP Address 대화 상자를 표시합니다.

11단계 항목을 두 번 클릭하여 Ending IP Address 필드에 이를 추가한 다음 **OK**를 클릭합니다.

12단계 드롭다운 목록에서 서브넷 마스크를 선택한 다음 **OK**를 클릭합니다.

새로운 IP 주소 풀이 Select IP Address Pool 목록에 표시됩니다.

13단계 새 IP 주소 풀 이름을 두 번 클릭하여 Assign 필드에 이를 추가한 다음 **OK**를 클릭합니다.

새로운 IP 주소 풀 이름이 Edit OSPF Process Advanced Properties 대화 상자의 Cluster Pool 필드에 표시됩니다.

14단계 **OK**를 클릭합니다.

15단계 새로 추가된 IP 주소 풀 설정을 변경하려면 **Edit**를 클릭합니다.

Edit IPv4 Pool 대화 상자가 나타납니다.

16단계 4~14단계를 반복합니다.

참고 할당이 완료되어 하나 이상의 연결 프로파일에 이미 사용되고 있는 기존 IP 주소 풀은 편집하거나 삭제할 수 없습니다.

17단계 **OK**를 클릭합니다.

OSPFv3를 지원하는 Individual Interface에서 라우터 ID 클러스터에 대한 IPv4 주소의 범위를 할당하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 홈 페이지에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 편집할 OSPF 프로세스를 선택한 다음 **Advanced**를 클릭합니다.

Edit OSPFv3 Process Advanced Properties 대화 상자가 나타납니다.

4단계 Router ID 드롭다운 목록에서 Cluster Pool 옵션을 선택합니다. 라우터 ID에 대한 ID 주소 풀을 지정할 필요가 없을 경우, Automatic 옵션을 선택합니다. IP 주소 풀을 구성하지 않으면 ASA에서는 자동으로 생성된 라우터 ID를 사용합니다.

5단계 IP 주소 풀 이름을 입력합니다. 또는 말줄임표 기호를 클릭하여 Select IP Address Pool 대화 상자를 표시합니다.

6단계 기존 IP 주소 풀 이름을 두 번 클릭하여 이를 Assign 필드에 추가합니다. 또는 **Add**를 클릭하여 새 IP 주소 풀을 생성합니다.

Add IPv4 Pool 대화 상자가 나타납니다.

7단계 Name 필드에 새 IP 주소 풀 이름을 입력합니다.

8단계 시작 IP 주소를 입력하거나 말줄임표 기호를 클릭하여 Browse Starting IP Address 대화 상자를 표시합니다.

9단계 항목을 두 번 클릭하여 Starting IP Address 필드에 이를 추가한 다음 **OK**를 클릭합니다.

10단계 끝 IP 주소를 입력하거나 말줄임표 기호를 클릭하여 Browse Ending IP Address 대화 상자를 표시합니다.

11단계 항목을 두 번 클릭하여 Ending IP Address 필드에 이를 추가한 다음 **OK**를 클릭합니다.

12단계 드롭다운 목록에서 서브넷 마스크를 선택한 다음 **OK**를 클릭합니다.

새로운 IP 주소 풀이 Select IP Address Pool 목록에 표시됩니다.

13단계 새 IP 주소 풀 이름을 두 번 클릭하여 Assign 필드에 이를 추가한 다음 **OK**를 클릭합니다.

새로운 IP 주소 풀 이름이 Edit OSPF Process Advanced Properties 대화 상자의 Cluster Pool 필드에 표시됩니다.

14단계 **OK**를 클릭합니다.

15단계 새로 추가된 클러스터 풀 설정을 변경하려면 **Edit**를 클릭합니다.

Edit IPv4 Pool 대화 상자가 나타납니다.

16단계 4~14단계를 반복합니다.

참고 할당이 완료되어 다른 OSPFv3 프로세스에서 이미 사용되고 있는 기존 IP 주소 풀은 편집하거나 삭제할 수 없습니다.

17단계 **OK**를 클릭합니다.

고정 OSPFv2 인접 디바이스 정의

고정 OSPFv2 인접 디바이스를 정의하여 포인트-투-포인트 비 브로드캐스트 네트워크를 통해 OSPFv2 경로를 광고할 수 있습니다. 이 기능을 사용하면 GRE 터널에 광고를 캡슐화하지 않고도 기존 VPN 연결 전체에 OSPFv2 광고를 브로드캐스트할 수 있습니다.

시작하기 전에, OSPFv2 인접 디바이스에 대한 고정 경로를 생성해야 합니다. 고정 경로 생성에 대한 자세한 내용은 20 장, “고정 경로 및 기본 경로”,를 참조하십시오.

절차

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Static Neighbor**를 선택합니다.

2단계 **Add** 또는 **Edit**를 클릭합니다.

Add/Edit OSPF Neighbor Entry 대화 상자가 나타납니다. 이 대화 상자를 사용하여 새로운 고정 인접 디바이스를 정의하거나 기존 고정 인접 디바이스에 대한 정보를 변경할 수 있습니다. 각 포인트-투-포인트 비 브로드캐스트 인터페이스에 대한 고정 인접 디바이스를 정의해야 합니다. 다음과 같은 제한 사항을 참고하십시오.

- 2개의 서로 다른 OSPF 프로세스에 동일한 고정 인접 디바이스를 정의할 수 없습니다.
- 각각의 고정 인접 디바이스에 대한 고정 경로를 정의해야 합니다.

3단계 OSPF Process 드롭다운 목록에서 고정 인접 디바이스와 관련된 OSPF 프로세스를 선택합니다. 기존 고정 인접 디바이스를 편집할 경우 이 값은 변경할 수 없습니다.

4단계 Neighbor 필드에 고정 인접 디바이스의 IP 주소를 입력합니다.

5단계 Interface 필드에서 고정 인접 디바이스와 관련된 인터페이스를 선택합니다. 기존 고정 인접 디바이스를 편집할 경우 이 값은 변경할 수 없습니다.

6단계 **OK**를 클릭합니다.

경로 계산 타이머 구성

OSPFv2에서 토폴로지 변경을 수신하는 시간과 SPF 계산을 시작하는 시간 사이의 지연 시간을 구성할 수 있습니다. 두 번 연속으로 SPF를 계산하는 작업 사이의 대기 시간을 구성할 수도 있습니다.

경로 계산 타이머를 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 편집할 OSPF 프로세스를 선택한 다음 **Advanced**를 클릭합니다.

Edit OSPF Process Advanced Properties 대화 상자가 나타납니다.

4단계 Timers 영역에서는 LSA 속도 및 SPF 계산 타이머를 구성하는 데 사용되는 설정을 수정할 수 있습니다. Timers 영역에서 다음 값을 입력합니다.

- The Initial SPF Delay - OSPF에서 토폴로지 변경을 수신하는 시간과 SPF 계산을 시작하는 시간 사이의 시간(밀리초 단위)을 지정합니다. 유효한 값의 범위는 0~600000밀리초입니다.
- The Minimum SPF Hold Time - 연속적인 SPF 계산 작업 사이의 대기 시간(밀리초 단위)을 지정합니다. 유효한 값의 범위는 0~600000밀리초입니다.
- The Maximum SPF Wait Time - 두 번 연속으로 SPF를 계산하는 작업 사이의 최대 대기 시간을 지정합니다. 유효한 값의 범위는 0~600000밀리초입니다.

5단계 **OK**를 클릭합니다.

인접 디바이스 작동 또는 중단 기록

OSPFv2 인접 디바이스가 작동 또는 중단될 경우 기본적으로 syslog 메시지가 생성됩니다.

OSPFv2 인접 디바이스의 작동 또는 중단을 기록하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 **Advanced**를 클릭합니다.

Edit OSPF Process Advanced Properties 대화 상자가 나타납니다.

4단계 Adjacency Changes 영역에는 syslog 메시지가 전송될 수 있는 인접성 변경 사항을 정의하는 설정이 포함됩니다. Adjacency Changes 영역에서 다음 값을 입력합니다.

- OSPFv2 인접 디바이스가 작동 또는 중단될 때마다 ASA에서 syslog 메시지를 전송하도록 하려면 **Log Adjacency Changes** 확인란을 선택합니다. 이 설정은 기본적으로 선택되어 있습니다.
- 인접 디바이스의 작동 또는 중단뿐만 아니라 모든 상태가 변경될 때마다 ASA에서 syslog 메시지를 전송하도록 하려면 **Log Adjacency Changes Detail** 확인란을 선택합니다. 이 설정은 기본적으로 선택되어 있지 않습니다.

5단계 **OK**를 클릭합니다.

참고 인접 디바이스 작동 또는 중단 메시지를 전송하려면 로깅을 활성화해야 합니다.

OSPF의 필터링 구성

Filtering 창에는 각 OSPF 프로세스에 대해 구성된 ABR Type 3 LSA 필터가 표시됩니다.

ABR Type 3 LSA 필터는 지정된 접두사만 한 영역에서 다른 영역으로 전송되도록 허용하며 다른 모든 접두사는 제한합니다. 이러한 유형의 영역 필터링은 특정 OSPF 영역의 외부 또는 특정 OSPF 영역의 내부에 적용하거나, 동일한 OSPF 영역의 내부와 외부에 동시에 적용할 수 있습니다.

OSPF ABR Type 3 LSA 필터링은 OSPF 영역 간의 경로 재배포 제어 기능을 개선합니다.

참고 ABR에서 시작되는 Type 3 LSA만 필터링됩니다.

OSPF에서 필터링을 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Filtering**을 선택합니다.

2단계 **Add** 또는 **Edit**를 클릭합니다.

Add or Edit OSPF Filtering Entry 대화 상자를 사용하면 Filter 테이블에 새 필터를 추가하거나 기존 필터를 수정할 수 있습니다. 기존 필터를 편집할 경우 일부 필터링 정보를 변경할 수 없습니다.

3단계 OSPF Process 드롭다운 목록에서 필터 항목과 관련된 OSPF 프로세스를 선택합니다.

4단계 Area ID 드롭다운 목록에서 필터 항목과 관련된 Area ID를 선택합니다. 기존 필터 항목을 편집할 경우 이 설정은 변경할 수 없습니다.

5단계 Prefix List 드롭다운 목록에서 접두사 목록을 선택합니다.

6단계 Traffic Direction 드롭다운 목록에서 필터링할 트래픽 방향을 선택합니다.

OSPF 영역에 들어오는 LSA를 필터링하려면 Inbound를 선택하고, OSPF 영역 밖으로 나가는 LSA를 필터링하려면 Outbound를 선택합니다. 기존 필터 항목을 편집할 경우 이 설정은 변경할 수 없습니다.

7단계 **Manage**를 클릭하여 접두사 목록 및 접두사 규칙을 추가, 편집 또는 삭제할 수 있는 Configure Prefix Lists 대화 상자를 표시합니다. 자세한 내용은 21-8 페이지의 접두사 목록 구성 및 21-8 페이지의 경로 작업에 대한 메트릭 값 구성를 참고하십시오.

8단계 **OK**를 클릭합니다.

OSPF에서 가상 링크 구성

OSPF 네트워크에 영역을 추가했으나 백본 영역에 해당 영역을 직접 연결하는 것이 불가능할 경우, 가상 링크를 생성해야 합니다. 가상 링크는 트랜짓 영역이라고 하는 공통 영역이 있는 2개의 OSPF 디바이스에 연결됩니다. OSPF 디바이스 중 하나를 백본 영역에 연결해야 합니다.

새 가상 링크를 정의하거나 기존 가상 링크의 속성을 변경하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Virtual Link**를 선택합니다.

2단계 **Add** 또는 **Edit**를 클릭합니다.

새 가상 링크를 정의하거나 기존 가상 링크의 속성을 변경할 수 있는 Add or Edit OSPF Virtual Link 대화 상자가 나타납니다.

3단계 OSPF Process 드롭다운 목록에서 가상 링크와 관련된 OSPF 프로세스 ID를 선택합니다. 기존 가상 링크 항목을 편집할 경우 이 설정은 변경할 수 없습니다.

4단계 Area ID 드롭다운 목록에서 가상 링크와 관련된 Area ID를 선택합니다.

인접 디바이스 OSPF 디바이스에서 공유하는 영역을 선택합니다. 선택한 영역은 NSSA 또는 Stub 영역이 될 수 없습니다. 기존 가상 링크 항목을 편집할 경우 이 설정은 변경할 수 없습니다.

5단계 Peer Router ID 필드에 가상 링크 인접 디바이스의 라우터 ID를 입력합니다.

기존 가상 링크 항목을 편집할 경우 이 설정은 변경할 수 없습니다.

6단계 **Advanced**를 클릭하여 고급 가상 링크 속성을 편집합니다.

Advanced OSPF Virtual Link Properties 대화 상자가 나타납니다. 이 영역에서 가상 링크의 OSPF 속성을 구성할 수 있습니다. 이러한 속성에는 인증 및 패킷 간격 설정이 포함됩니다.

7단계 Authentication 영역에서, 다음 옵션 중 하나의 옆에 있는 라디오 버튼을 클릭하여 Authentication 유형을 선택합니다.

- **None** - OSPF 인증을 비활성화합니다.
- **Authentication Password** - 일반 텍스트 비밀번호 인증을 사용합니다. 이는 보안이 중요한 경우 권장하지 않습니다.
- **MD5** - MD5 인증을 사용합니다(권장).
- **Area**(기본값) - 해당 영역에 지정된 인증 유형을 사용합니다. 영역 인증 구성에 대한 자세한 내용은 23-14 페이지의 OSPFv2 영역 매개변수를 참조하십시오. 영역 인증은 기본적으로 비활성화되어 있습니다. 따라서 영역 인증 유형을 이전에 지정하지 않은 경우, 이 설정을 구성하지 않으면 영역 인증에 대한 인터페이스 집합은 인증이 비활성화되어 있습니다.

8단계 비밀번호 인증이 활성화된 경우, Authentication Password 영역에서 비밀번호를 다시 입력합니다. 비밀번호는 최대 8자의 텍스트 문자열이어야 합니다.

9단계 MD5 인증이 활성화된 경우, MD5 IDs and Key 영역에서 MD5 키 및 매개변수를 입력합니다. OSPF 인증을 사용하는 인터페이스의 모든 디바이스에서는 동일한 MD5 키와 ID를 사용해야 합니다. 다음 설정을 지정합니다.

a. Key ID 필드에 숫자 키 식별자를 입력합니다. 유효한 값의 범위는 1~255입니다. 선택한 인터페이스에 대한 Key ID가 표시됩니다.

b. Key 필드에 최대 16바이트의 영숫자 문자열을 입력합니다. 선택한 인터페이스에 대한 Key ID가 표시됩니다.

c. **Add** 또는 **Delete**를 클릭하여 MD5 ID and Key 테이블에 지정된 MD5 키를 추가하거나 삭제합니다.

10단계 Interval 영역에서 다음 옵션 중 하나를 선택하여 패킷의 간격 타이밍을 지정합니다.

- **Hello Interval** - 인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 지정합니다. Hello 패킷의 값이 작을수록 토폴로지 변경 사항이 더 빨리 감지되지만, 인터페이스에 전송되는 트래픽이 늘어납니다. 이 값은 특정 인터페이스의 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1~65535초입니다. 기본값은 10초입니다.
- **Retransmit Interval** - 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 초 단위로 지정합니다. 라우터에서 LSA를 인접 디바이스로 전송하면 라우터에서는 승인 메시지가 수신될 때까지 LSA를 보관합니다. 라우터에 승인 메시지가 전송되지 않으면 LSA를 다시 전송합니다. 이 값을 신중하게 설정하지 않으면 불필요한 재전송이 발생할 수 있습니다. 직렬 회선 및 가상 링크의 경우 이 값이 더 커야 합니다. 유효한 값의 범위는 1~65535초입니다. 기본값은 5초입니다.
- **Transmit Delay** - 인터페이스에서 LSA 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 지정합니다. 업데이트 패킷의 LSA에는 전송 전에 이 필드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 링크를 통해 전송하기 전에 지연이 추가되지 않을 경우, LSA에서 링크를 통해 전파하는 시간은 고려되지 않습니다. 할당된 값에는 인터페이스의 전송 및 전파 지연을 고려해야 합니다. 이 설정은 속도가 매우 낮은 링크에서 중요성이 더 큽니다. 유효한 값의 범위는 1~65535초입니다. 기본값은 1초입니다.
- **Dead Interval** - Hello 패킷이 수신되지 않아 인접 디바이스에서 라우터 중간을 선언하기까지 소요되는 간격을 초 단위로 지정합니다. 유효한 값의 범위는 1~65535입니다. 이 필드의 기본값은 Hello Interval 필드에 설정된 간격 집합의 4배입니다.

11단계 **OK**를 클릭합니다.

OSPFv3 구성

이 섹션에서는 OSPFv3 라우팅 프로세스를 구성하는 방법에 대해 설명합니다.

OSPFv3 활성화

OSPFv3를 활성화하려면 OSPFv3 라우팅 프로세스를 생성하고, OSPFv3에 대한 영역을 생성하고, OSPFv3에 대한 인터페이스를 활성화하고, 경로를 대상 OSPFv3 라우팅 프로세스에 재배포해야 합니다.

OSPFv3를 활성화하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 Process Instances 탭에서 **Enable OSPFv3 Process** 확인란을 선택합니다. 최대 2개의 OSPF 프로세스 인스턴스를 활성화할 수 있습니다. 단일 컨텍스트 모드만 지원됩니다.

3단계 Process ID 필드에 프로세스 ID를 입력합니다. ID는 어떠한 양수이든 사용 가능합니다.

4단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

5단계 계속하려면 23-24 페이지의 OSPFv3 영역 매개변수 구성를 참조하십시오.

OSPFv3 인터페이스 매개변수 구성

필요한 경우 특정 인터페이스별 OSPFv3 매개변수를 변경할 수 있습니다. 이러한 매개변수는 변경할 필요가 없지만, the hello interval and the dead interval 같은 인터페이스 매개변수는 연결된 네트워크의 모든 라우터 전반에 걸쳐 일관성을 유지해야 합니다. 이러한 매개변수를 컨피그레이션할 경우, 네트워크의 모든 라우터 컨피그레이션에 호환되는 값이 있는지 확인해야 합니다.

IPv6에 대한 OSPFv3 인터페이스 매개변수를 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Interfaces**를 선택합니다.

2단계 **Authentication** 탭을 클릭합니다.

3단계 인터페이스에 대한 인증 매개변수를 지정하려면 **Edit**를 클릭합니다.

Edit OSPFv3 Interface Authentication 대화 상자가 나타납니다.

4단계 Authentication Type 드롭다운 목록에서 인증 유형을 선택합니다. 사용 가능한 옵션은 Area, Interface 및 None입니다. None 옵션은 사용 중인 인증이 없음을 나타냅니다.

5단계 Authentication Algorithm 드롭다운 목록에서 인증 알고리즘을 선택합니다. 지원되는 값은 SHA-1 및 MD5입니다.

6단계 Authentication Key 필드에 인증 키를 입력합니다. MD5 인증을 사용할 경우, 키는 32자 길이의 16진수 숫자(16바이트)여야 합니다. SHA-1 인증을 사용할 경우, 키는 40자 길이의 16진수 숫자(20바이트)여야 합니다.

7단계 Encryption Algorithm 드롭다운 목록에서 암호화 알고리즘을 선택합니다. 지원되는 값은 AES-CDC, 3DES, DES입니다. Null 항목은 암호화가 없음을 나타냅니다.

8단계 Encryption Key 필드에 인증 키를 입력합니다.

9단계 **OK**를 클릭합니다.

10단계 **Properties** 탭을 클릭합니다.

11단계 수정할 속성이 있는 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit OSPFv3 Interface Properties 대화 상자가 나타납니다.

12단계 **Enable OSPFv3 on this interface** 확인란을 선택합니다.

13단계 드롭다운 목록에서 프로세스 ID를 선택합니다.

14단계 드롭다운 목록에서 영역 ID를 선택합니다.

15단계 (선택 사항) 인터페이스에 할당할 영역 인스턴스 ID를 지정합니다. 하나의 인터페이스에는 하나의 OSPFv3 영역만 포함할 수 있습니다. 여러 인터페이스에서 동일한 영역을 사용할 수 있으며, 각 인터페이스에서는 다른 영역 인스턴스 ID를 사용할 수 있습니다.

16단계 드롭다운 목록에서 네트워크 유형 ID를 선택합니다. 지원되는 옵션은 Default, Broadcast, Point-to-Point입니다.

17단계 Cost 필드에 인터페이스에서 패킷을 전송하는 비용을 입력합니다.

18단계 네트워크의 전용 라우터를 결정하는 데 도움이 되는 라우터 우선순위를 Priority 필드에 입력합니다. 유효한 값의 범위는 0~255입니다.

19단계 **Disable MTU mismatch detection** 확인란을 선택하여 DBD 패킷이 수신될 때 OSPF MTU 불일치 감지를 비활성화합니다. OSPF MTU 불일치 감지는 기본적으로 활성화되어 있습니다.

20단계 **Filter outgoing link state advertisements** 확인란을 선택하여 OSPFv3 인터페이스에 발신되는 LSA를 필터링합니다. 기본적으로 모든 발신 LSA는 인터페이스에 플러딩됩니다.

21단계 Timers 영역의 Dead Interval 필드에 인접 디바이스에서 라우터의 중단 여부를 나타내기까지 Hello 패킷이 표시되지 않아야 하는 시간을 초 단위로 입력합니다. 이 값은 네트워크의 모든 노드에서 동일해야 하며 입력 가능한 범위는 1~65535입니다.

22단계 Hello Interval 필드에 인터페이스에서 전송된 Hello 패킷 간의 간격을 초 단위로 입력합니다. 이 값은 특정 네트워크의 모든 노드에서 동일해야 하며 입력 가능한 범위는 1~65535입니다. 기본 간격은 이더넷 인터페이스의 경우 10초이고, 비 브로드캐스트 인터페이스의 경우 30초입니다.

23단계 Retransmit Interval 필드에 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 초 단위로 입력합니다. 이 시간은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간보다 커야 합니다. 유효한 값의 범위는 1~65535초입니다. 기본값은 5초입니다.

24단계 Transmit Delay 필드에 인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 초 단위로 입력합니다. 유효한 값의 범위는 1~65535초입니다. 기본값은 1초입니다.

25단계 **OK**를 클릭합니다.

26단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

OSPFv3 영역 매개변수 구성

OSPFv3 영역 매개변수를 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 **Areas** 탭을 클릭합니다.

3단계 새 영역을 추가하려면 **Add**를 클릭합니다. 기존 영역을 수정하려면 **Edit**를 클릭합니다. 선택한 영역을 제거하려면 **Delete**를 클릭합니다.

Add OSPFv3 Area 대화 상자 또는 Edit OSPFv3 Area 대화 상자가 나타납니다.

4단계 OSPFv3 Process ID 드롭다운 목록에서 프로세스 ID를 선택합니다.

5단계 경로를 요약할 영역을 지정하는 영역 ID를 Area ID 필드에 입력합니다.

6단계 Area Type 드롭다운 목록에서 영역 유형을 선택합니다. 사용 가능한 옵션은 Normal, NSSA, Stub입니다.

7단계 요약 LSA를 영역으로 전송하도록 허용하려면 **Allow sending of summary LSAs into the area** 확인란을 선택합니다.

8단계 재배포 시 경로를 Normal 및 not-so-stubby 영역으로 가져오도록 허용하려면 **Redistribution imports routes to normal and NSSA areas** 확인란을 선택합니다.

9단계 OSPFv3 라우팅 도메인에 기본 외부 경로를 생성하려면 **Default information originate** 확인란을 선택합니다.

10단계 기본 경로를 생성하는 데 사용되는 메트릭을 Metric 필드에 입력합니다. 기본값은 10입니다. 유효한 값의 범위는 0~16777214입니다.

11단계 Metric Type 드롭다운 목록에서 메트릭 유형을 선택합니다. 메트릭 유형은 OSPFv3 라우팅 도메인으로 광고되는 기본 경로와 연결된 외부 링크 유형입니다. 사용 가능한 옵션은 Type 1 외부 경로는 1, Type 2 외부 경로는 2입니다.

12단계 Default Cost 필드에 비용을 입력합니다.

13단계 **OK**를 클릭합니다.

14단계 **Route Summarization** 탭을 클릭합니다.

15단계 경로 통합 및 요약에 대한 새로운 범위를 지정하려면 **Add**를 클릭합니다. 경로 통합 및 요약에 대한 기존 범위를 수정하려면 **Edit**를 클릭합니다.

Add Route Summarization 대화 상자 또는 Edit Route Summarization 대화 상자가 나타납니다.

16단계 Process ID 드롭다운 목록에서 프로세스 ID를 선택합니다.

17단계 Area ID 드롭다운 목록에서 영역 ID를 선택합니다.

18단계 IPv6 Prefix/Prefix Length 필드에 IPv6 접두사 및 접두사 길이를 입력합니다.

19단계 (선택 사항) 목적지까지의 최단 경로를 결정하는 OSPF SPF 계산 과정에 사용되는 요약 경로의 메트릭 또는 비용을 입력합니다. 유효한 값의 범위는 0~16777215입니다.

20단계 **Advertised** 확인란을 선택하여 주소 범위 상태를 advertised로 설정하고 Type 3 요약 LSA를 생성합니다.

21단계 **OK**를 클릭합니다.

22단계 계속하려면 23-25 페이지의 가상 링크 인접 디바이스 구성를 참조하십시오.

가상 링크 인접 디바이스 구성

가상 링크 인접 디바이스를 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Virtual Link**를 선택합니다.

2단계 새 가상 링크 인접 디바이스를 추가하려면 **Add**를 클릭합니다. 기존 가상 링크 인접 디바이스를 수정하려면 **Edit**를 클릭합니다. 선택한 가상 링크 인접 디바이스를 제거하려면 **Delete**를 클릭합니다.

Add Virtual Link dialog box 또는 Edit Virtual Link 대화 상자가 나타납니다.

3단계 Process ID 드롭다운 목록에서 프로세스 ID를 선택합니다.

4단계 Area ID 드롭다운 목록에서 영역 ID를 선택합니다.

5단계 Peer Router ID 필드에 피어 라우터 ID(즉, IP 주소)를 입력합니다.

6단계 (선택 사항) TTL Security 필드에 가상 링크에 대한 TTL(Time-to-Live) 보안 홉 개수를 입력합니다. 홉 개수 값의 범위는 1~254입니다.

7단계 인접 디바이스에서 Dead Interval 필드에 라우터가 중단되었음을 나타내기까지 Hello 패킷이 표시되지 않은 시간을 Timers 영역에 초 단위로 입력합니다. Dead 간격은 무부호 정수입니다. 기본값은 Hello 간격의 4배이거나 40초입니다. 이 값은 공통 네트워크에 연결된 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1~8192입니다.

8단계 인터페이스에서 전송되는 Hello 패킷 간의 시간을 Hello Interval 필드에 초 단위로 입력합니다. Hello 간격은 Hello 패킷에 광고되는 무부호 정수입니다. 이 값은 공통 네트워크에 연결된 모든 라우터 및 액세스 서버에서 동일해야 합니다. 유효한 값의 범위는 1~8192입니다. 기본값은 10입니다.

9단계 인터페이스에 속하는 인접성에 대해 LSA를 재전송하는 동안의 시간을 Retransmit Interval 필드에 초 단위로 입력합니다. 재전송 간격은 연결된 네트워크에 있는 두 라우터 간의 예상 왕복 지연 시간입니다. 이 값은 예상 왕복 지연 시간보다 커야 하며 입력 가능한 범위는 1~8192입니다. 기본값은 5입니다.

10단계 인터페이스에서 링크 상태 업데이트 패킷을 전송하는 데 필요한 예상 시간을 Transmit Delay 필드에 초 단위로 입력합니다. 이 정수 값은 0보다 커야 합니다. 업데이트 패킷의 LSA에는 전송 전에 이 키워드에서 지정한 양만큼 증가된 LSA의 기간이 포함됩니다. 입력 가능한 값의 범위는 1~8192입니다. 기본값은 1입니다.

11단계 Authentication 영역에서 **Enable Authentication** 확인란을 선택하여 인증을 활성화합니다.

12단계 Security Policy Index 필드에 보안 정책 색인을 지정하며, 이 값의 범위는 256~4294967295 사이여야 합니다.

13단계 Authentication Algorithm 드롭다운 목록에서 인증 알고리즘을 선택합니다. 지원되는 값은 SHA-1 및 MD5입니다. MD5 인증을 사용할 경우, 키는 32자 길이의 16진수 숫자(16바이트)여야 합니다. SHA-1 인증을 사용할 경우, 키는 40자 길이의 16진수 숫자(20바이트)여야 합니다.

14단계 Authentication Key 필드에 인증 키를 입력합니다. 이 키에는 32자 16진수 문자가 포함되어야 합니다.

15단계 Encryption Algorithm 드롭다운 목록에서 암호화 알고리즘을 선택합니다. 지원되는 값은 AES-CDC, 3DES, DES입니다. Null 항목은 암호화가 없음을 나타냅니다.

16단계 Encryption Key 필드에 인증 키를 입력합니다.

17단계 **OK**를 클릭합니다.

18단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

OSPFv3 패시브 인터페이스

OSPFv3 패시브 인터페이스를 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 편집할 OSPFv3 프로세스를 선택한 다음 **Advanced**를 클릭합니다.

Edit OSPFv3 Process Advanced Properties 대화 상자가 나타납니다.

4단계 Passive Interfaces 영역을 사용하면 인터페이스에서 OSPFv3 라우팅을 활성화할 수 있습니다. 패시브 라우팅에서는 OSPFv3 라우팅 정보의 광고를 제어할 수 있도록 지원하고, 인터페이스에서 OSPFv3 라우팅 업데이트의 전송 및 수신을 비활성화합니다. Passive Interfaces 영역에서 다음 설정을 선택합니다.

- **Global passive** 확인란을 선택하여 테이블에 나열된 모든 인터페이스를 패시브로 만듭니다. 개별 인터페이스의 선택을 취소하여 비 패시브 인터페이스로 만듭니다.
- **Global passive** 확인란을 선택하여 모든 인터페이스를 비 패시브로 만듭니다. 개별 인터페이스를 선택하여 패시브 인터페이스로 만듭니다.

5단계 **OK**를 클릭합니다.

6단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

OSPFv3 관리 영역 구성

IPv6 경로에 대한 OSPFv3 관리 영역을 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 편집할 OSPF 프로세스를 선택한 다음 **Advanced**를 클릭합니다.

Edit OSPFv3 Process Advanced Properties 대화 상자가 나타납니다.

Administrative Route Distances 영역을 사용하면 관리 경로 영역을 구성하는 데 사용된 설정을 수정할 수 있습니다. 관리 경로 영역의 값은 10~254 사이의 정수입니다. Administrative Route Distances 영역에 다음 값을 입력합니다.

- Inter Area - IPv6 경로에 대한 OSPV의 영역 간 경로를 지정합니다.
- Intra Area - IPv6 경로에 대한 OSPF의 영역 간 경로를 지정합니다.
- External - IP6 경로에 대한 OSPF의 외부 Type 5 및 Type 7을 지정합니다.

4단계 **OK**를 클릭합니다.

5단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

OSPFv3 타이머 구성

OSPFv3에 대한 LSA 도착, LSA 속도 및 속도 제한 타이머를 설정할 수 있습니다.

ASA에서 OSPFv3 인접 디바이스의 동일한 LSA를 수락하는 최소 간격을 설정하려면 다음 단계를 수행합니다.

LSA 플러딩 패킷 속도를 구성하려면 다음 단계를 수행합니다.

OSPFv3 LSA를 그룹으로 수집 및 새로 고침하고, 체크섬 또는 시간 경과가 이루어지는 간격을 변경하려면 다음 단계를 수행합니다.

LSA 재전송 패킷 속도를 구성하려면 다음 단계를 수행합니다.

LSA 및 SPF 속도 제한 기능에서는 밀리초 단위의 LSA 속도 제한을 제공하여 네트워크가 불안정한 시간 동안 OSPFv3 LSA 업데이트 속도를 줄이고, OSPFv3 통합 시간을 단축할 수 있는 동적 메커니즘을 제공합니다.

LSA 및 SPF 속도 제한 타이머를 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 편집할 OSPFv3 프로세스를 선택한 다음 **Advanced**를 클릭합니다.

Edit OSPFv3 Process Advanced Properties 대화 상자가 나타납니다.

4단계 Timers 영역에서는 LSA 도착, LSA 속도, LSA 재전송, LSA 속도 제한, SPF 속도 제한 시간을 구성하는 데 사용되는 설정을 수정할 수 있습니다. Timers 영역에서 다음 값을 입력합니다.

- LSA Arrival - 인접 디바이스에서 도착하는 동일한 LSA를 수락하는 동안 소요될 수밖에 없는 최소 지연 시간을 밀리초 단위로 지정합니다. 범위는 0에서 6000,000밀리초입니다. 기본값은 1000밀리초입니다.
- LSA Flood Pacing - 업데이트 중 플러딩 대기열에서 LSA가 유지되고 있는 속도를 밀리초 단위의 시간으로 지정합니다. 구성 가능한 범위는 5~100밀리초입니다. 기본값은 33밀리초입니다.
- LSA Group Pacing - LSA를 그룹으로 수집 및 새로 고침하고, 체크섬 또는 시간 경과가 이루어지는 간격을 초 단위로 지정합니다. 유효한 값의 범위는 10~1800입니다. 기본값은 240입니다.
- LSA Retransmission Pacing - 플러딩 대기열에서 LSA가 유지되고 있는 속도를 밀리초 단위의 시간으로 지정합니다. 구성 가능한 범위는 5~200밀리초입니다. 기본값은 66밀리초입니다.
- LSA Throttle Initial - LSA의 첫 번째 어커런스를 생성하는 데 필요한 지연 시간을 밀리초 단위로 지정합니다. 기본값은 0밀리초입니다.
- LSA Throttle Min Hold - 동일한 LSA를 시작하는 데 필요한 최소 지연 시간을 밀리초 단위로 지정합니다. 기본값은 5000밀리초입니다.
- LSA Throttle Max Wait - 동일한 LSA를 시작하는 데 필요한 최대 지연 시간을 밀리초 단위로 지정합니다. 기본값은 5000밀리초입니다.

참고 LSA 속도 제한의 경우, 최소 또는 최대 시간이 첫 번째 어커런스 값보다 작으면 OSPFv3에서 첫 번째 어커런스 값을 자동으로 수정합니다. 이와 마찬가지로, 최대 지연 값이 최소 지연 값보다 작게 지정될 경우 OSPFv3에서 최소 지연 값을 자동으로 수정합니다.

- SPF Throttle Initial - SPF 계산의 변경 사항을 수신하는 데 필요한 지연 시간을 밀리초 단위로 지정합니다. 기본값은 5000밀리초입니다.
- SPF Throttle Min Hold - 첫 번째와 두 번째 SPF 계산 사이의 지연 시간을 밀리초 단위로 지정합니다. 기본값은 10000밀리초입니다.
- SPF Throttle Max Wait - SPF 계산에 소요되는 최대 대기 시간을 밀리초 단위로 지정합니다. 기본값은 10000밀리초입니다.

참고 SPF 속도 제한의 경우, 최소 또는 최대 시간이 첫 번째 어커런스 값보다 작으면 OSPFv3에서 첫 번째 어커런스 값을 자동으로 수정합니다. 이와 마찬가지로, 최대 지연 값이 최소 지연 값보다 작게 지정될 경우 OSPFv3에서 최소 지연 값을 자동으로 수정합니다.

5단계 **OK**를 클릭합니다.

6단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

고정 OSPFv3 인접 디바이스 정의

고정 OSPFv3 인접 디바이스를 정의하여 포인트-투-포인트 비 브로드캐스트 네트워크를 통해 OSPF 경로를 광고할 수 있습니다. 이 기능을 사용하면 GRE 터널에 광고를 캡슐화하지 않고도 기존 VPN 연결 전체에 OSPFv3 광고를 브로드캐스트할 수 있습니다.

시작하기 전에, OSPFv3 인접 디바이스에 대한 고정 경로를 생성해야 합니다. 고정 경로 생성에 대한 자세한 내용은 20 장, “고정 경로 및 기본 경로”,를 참조하십시오.

고정 OSPFv3 인접 디바이스를 정의하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Static Neighbor**를 선택합니다.

2단계 **Add** 또는 **Edit**를 클릭합니다.

Add or Edit Static Neighbor 대화 상자가 나타납니다. 이 대화 상자를 사용하여 새로운 고정 인접 디바이스를 정의하거나 기존 고정 인접 디바이스에 대한 정보를 변경할 수 있습니다. 각 포인트-투-포인트 비 브로드캐스트 인터페이스에 대한 고정 인접 디바이스를 정의해야 합니다. 다음과 같은 제한 사항을 참고하십시오.

- 2개의 서로 다른 OSPFv3 프로세스에 동일한 고정 인접 디바이스를 정의할 수 없습니다.
- 각각의 고정 인접 디바이스에 대한 고정 경로를 정의해야 합니다.

3단계 Interface 드롭다운 목록에서 고정 인접 디바이스와 연결된 인터페이스를 선택합니다. 기존 고정 인접 디바이스를 편집할 경우 이 값은 변경할 수 없습니다.

4단계 Link-local Address 필드에 고정 인접 디바이스의 IPv6 주소를 입력합니다.

5단계 (선택 사항) Priority 필드에 우선순위를 입력합니다.

6단계 (선택 사항) Poll Interval 필드에 폴링 간격을 초 단위로 입력합니다.

7단계 **OK**를 클릭합니다.

Syslog 메시지 전송

OSPFv3 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하도록 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 편집할 OSPF 프로세스를 선택한 다음 **Advanced**를 클릭합니다.

Edit OSPFv3 Process Advanced Properties 대화 상자가 나타납니다.

Adjacency Changes 영역에서는 OSPFv3 인접 디바이스가 작동 또는 중단될 경우 syslog 메시지를 전송하기 위한 설정을 수정할 수 있습니다. Adjacency Changes 영역에서 다음을 수행합니다.

- OSPFv3 인접 디바이스가 작동 또는 중단될 경우 라우터에서 syslog 메시지를 전송하려면 **Log Adjacency Changes** 확인란을 선택합니다.
- OSPFv3 인접 디바이스가 작동 또는 중단되는 경우뿐만 아니라 각각의 상태에 대한 syslog 메시지를 전송하려면 **Include Details** 확인란을 선택합니다.

4단계 **OK**를 클릭합니다.

5단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

Syslog 메시지 억제

지원되지 않는 LSA Type 6 멀티캐스트 OSPF(MOSPF) 패킷이 경로에 전송될 경우 syslog 메시지가 전송되는 것을 억제하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 편집할 OSPFv3 프로세스를 선택한 다음 **Advanced**를 클릭합니다.

Edit OSPFv3 Process Advanced Properties 대화 상자가 나타납니다.

4단계 **Ignore LSA MOSPF** 확인란을 선택한 다음 **OK**를 클릭합니다.

요약 경로 비용 계산

RFC 1583에 따라 요약 경로 비용을 계산하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 편집할 OSPF 프로세스를 선택한 다음 **Advanced**를 클릭합니다.

Edit OSPFv3 Process Advanced Properties 대화 상자가 나타납니다.

4단계 **RFC1583 Compatible** 확인란을 선택한 다음 **OK**를 클릭합니다.

OSPFv3 라우팅 도메인에 기본 외부 경로 생성

OSPFv3 라우팅 도메인에 기본 경로를 생성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭합니다.

3단계 편집할 OSPFv3 프로세스를 선택한 다음 **Advanced**를 클릭합니다.

Edit OSPFv3 Process Advanced Properties 대화 상자가 나타납니다.

4단계 Default Information Originate Area에서 다음을 수행합니다.

a. **Enable** 확인란을 선택하여 OSPFv3 라우팅 프로세스를 활성화합니다.

b. **Always advertise** 확인란을 선택하여 기본 경로의 존재 여부에 상관없이 항상 기본 경로를 광고합니다.

c. 기본 경로를 생성하는 데 사용되는 메트릭을 Metric 필드에 입력합니다. 유효한 값의 범위는 0~16777214입니다. 기본값은 10입니다.

d. Metric Type 드롭다운 목록에서 메트릭 유형은 OSPFv3 라우팅 도메인으로 광고되는 기본 경로와 연결된 외부 링크 유형을 선택합니다. 유효한 값은 다음과 같습니다.

- 1 — Type 1 외부 경로
- 2 — Type 2 외부 경로

기본값은 Type 2 외부 경로입니다.

e. Route Map 드롭다운 목록에서 경로 맵이 충족된 경우 기본 경로를 생성하는 라우팅 프로세스를 선택합니다.

5단계 **OK**를 클릭합니다.

6단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

IPv6 요약 접두사 구성

IPv6 요약 접두사를 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Summary Prefix**를 선택합니다.

2단계 새 요약 접두사를 추가하려면 **Add**를 클릭합니다. 기존 요약 접두사를 수정하려면 **Edit**를 클릭합니다. 요약 접두사를 제거하려면 **Delete**를 클릭합니다.

Add Summary Prefix 대화 상자 또는 Edit Summary Prefix 대화 상자가 나타납니다.

3단계 Process ID 드롭다운 목록에서 프로세스 ID를 선택합니다.

4단계 IPv6 Prefix/Prefix Length 필드에 IPv6 접두사 및 접두사 길이를 입력합니다.

5단계 **Advertise** 확인란을 선택하여 지정된 접두사 및 마스크 쌍과 일치하는 경로를 광고합니다. 지정된 접두사 및 마스크 쌍과 일치하는 경로를 억제하려면 이 확인란의 선택을 취소합니다.

6단계 경로 맵을 통한 재배포를 제어하기 위한 일치 값으로 사용할 수 있는 태그 값을 Tag 필드에 입력합니다.

7단계 **OK**를 클릭합니다.

8단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

IPv6 경로 재배포

연결된 경로를 OSPFv3 프로세스에 재배포하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Redistribution**을 선택합니다.

2단계 연결된 경로를 OSPFv3 프로세스에 재배포하기 위한 새 매개변수를 추가하려면 **Add**를 클릭합니다. 연결된 경로를 OSPFv3 프로세스에 재배포하기 위한 기존 매개변수를 수정하려면 **Edit**를 클릭합니다. 선택한 매개변수 집합을 제거하려면 **Delete**를 클릭합니다.

Add Redistribution 대화 상자 또는 Edit Redistribution 대화 상자가 나타납니다.

3단계 Process ID 드롭다운 목록에서 프로세스 ID를 선택합니다.

4단계 Source Protocol 드롭다운 목록에서 경로가 재배포될 소스 프로토콜을 선택합니다. 지원되는 프로토콜은 connected, static, OSPF입니다.

5단계 Metric 필드에 메트릭 값을 입력합니다. 하나의 OSPF 프로세스에서 동일한 라우터의 다른 OSPF 프로세스로 경로를 재배포할 경우, 메트릭 값이 지정되지 않으면 한 프로세스에서 다른 프로세스로 메트릭이 이동됩니다. OSPF 프로세스에 다른 프로세스를 재배포할 경우, 메트릭 값이 지정되어 있지 않으면 기본 메트릭은 20입니다.

6단계 Metric Type 드롭다운 목록에서 메트릭 유형을 선택합니다. 제공되는 옵션은 None, 1, 2입니다.

7단계 (선택 사항) Tag 필드에 태그 값을 입력합니다. 이 매개변수는 ASBR 간에 정보를 주고받는 데 사용될 수 있는 각 외부 경로에 연결된 32비트 십진수 값을 지정합니다. 아무 것도 지정하지 않을 경우, 원격 자동 시스템 번호가 BGP 및 EGP의 경로에 사용됩니다. 다른 프로토콜에는 0이 사용됩니다. 유효한 값의 범위는 0~4294967295입니다.

8단계 Route Map 드롭다운 목록에서 경로 맵을 선택하여 소스 라우팅 프로토콜에서 현재 라우팅 프로토콜로 경로 가져오기를 필터링합니다. 이 매개변수를 지정하지 않으면 모든 경로가 재배포됩니다. 이 매개변수를 지정하였으나 경로 맵 태그가 나열되지 않으면 경로를 가져오지 않습니다.

9단계 연결된 경로를 재배포에 포함하려면 **Include connected** 확인란을 선택합니다.

10단계 **Match** 확인란을 선택하여 경로를 다른 라우팅 도메인으로 재배포한 다음, 다음 확인란 중 하나를 선택합니다.

- **Internal** - 특정 자동 시스템의 내부에 있는 경로
- **External 1** - 자동 시스템의 외부에 있지만, OSPFv3에 Type 1 외부 경로로서 가져온 경로
- **External 2** - 자동 시스템의 외부에 있지만, OSPFv3에 Type 2 외부 경로로서 가져온 경로
- **NSSA External 1** - 자동 시스템의 외부에 있지만 IPv6를 지원하는 NSSA의 OSPFv3에 Type 1 외부 경로로서 가져온 경로
- **NSSA External 2** - 자동 시스템의 외부에 있지만 IPv6를 지원하는 NSSA의 OSPFv3에 Type 2 외부 경로로서 가져온 경로

11단계 **OK**를 클릭합니다.

12단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

Graceful Restart 구성

ASA에 몇 가지 알려진 오류가 발생할 수 있으며, 이러한 상황은 스위칭 플랫폼 전반의 패킷 전달에 영향을 미치지 않아야 합니다. NSF(무중단 전달) 기능을 사용하면 알려진 경로를 계속 사용하여 데이터를 전달하는 동시에 라우팅 프로토콜 정보를 복원할 수 있습니다. 이 기능은 구성 요소에 오류가 발생하거나(예: 액티브 유닛이 장애 조치(HA) 모드 역할을 수행 중인 스탠바이 유닛과 충돌하거나, 마스터 유닛이 클러스터 모드에서 새 마스터로 선택된 슬레이브 유닛과 충돌한 경우), 무중단 소프트웨어 업그레이드가 예약된 경우 유용합니다.

Graceful Restart는 OSPFv2 및 OSPFv3에서 모두 지원됩니다. NSF Cisco(RFC 4811 및 RFC 4812) 또는 NSF IETF(RFC 3623)를 사용하여 OSPFv2에서 Graceful Restart를 구성할 수 있습니다. graceful-restart(RFC 5187)를 사용하여 OSPFv3에서 Graceful Restart를 구성할 수 있습니다.

NSF Graceful Restart 기능을 구성하려면 기능을 구성하고, 디바이스를 NSF 지원 또는 NSF 인식 디바이스로 구성하는 두 단계를 수행해야 합니다. NSF 지원 디바이스는 해당 디바이스의 재시작 작업을 인접 디바이스에 나타낼 수 있으며, NSF 인식 디바이스는 인접 디바이스를 초기화하도록 지원할 수 있습니다.

디바이스는 몇 가지 조건에 따라 NSF 지원 또는 NSF 인식 디바이스로 구성할 수 있습니다.

- 디바이스는 현재 속한 모드에 관계없이 NSF 인식 디바이스로 구성할 수 있습니다.
- NSF 지원 디바이스로 구성하려면 디바이스가 Failover 또는 Spanned Etherchannel(L2) 클러스터 모드에 있어야 합니다.
- NSF 인식 또는 NSF 지원 디바이스가 되려면, 필요에 따라 불투명 LSA(Link State Advertisements)/LLS(Link Local Signaling) 블록 처리 기능과 함께 디바이스를 구성해야 합니다.

참고 OSPFv2에 Fast Hello를 구성한 경우, 액티브 유닛이 다시 로드된 후 스탠바이 유닛이 액티브 유닛이 될 때 Graceful Restart가 실행되지 않습니다. 이는 역할 변경에 소요되는 시간이 구성된 Dead 간격보다 더 많기 때문입니다.

OSPFv2에 대한 Graceful Restart 구성

OSPFv2에 사용할 수 있는 두 가지 Graceful Restart 메커니즘은 Cisco NSF 및 IETF NSF입니다. ospf 인스턴스에는 Graceful Restart 메커니즘을 한 번에 하나만 구성할 수 있습니다. NSF 인식 디바이스는 Cisco NSF 헬퍼 및 IETF NSF 헬퍼 모두로 구성할 수 있으나, NSF 지원 디바이스는 Cisco NSF 또는 IETF NSF 모드를 한 번에 하나씩 ospf 인스턴스에 구성할 수 있습니다.

OSPFv2에 Cisco NSF Graceful Restart 구성

OSPFv2, NSF 지원 디바이스 또는 NSF 인식 디바이스에 Cisco NSF Graceful Restart를 구성하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup > Advanced > Add NSF Properties**를 선택합니다.

2단계 Configuring Cisco NSF 아래에서 **Enable Cisco nonstop forwarding (NSF)** 확인란을 선택합니다.

3단계 (선택 사항) 필요한 경우 **Cancels NSF restart when non-NSF-aware neighboring networking devices are detected** 확인란을 선택합니다.

4단계 (선택 사항) Configuring Cisco NSF helper 아래에서 **Enable Cisco nonstop forwarding (NSF) for helper mode** 확인란의 선택을 취소합니다.

참고 이 확인란은 기본적으로 선택되어 있습니다. NSF 인식 디바이스에서 Cisco NSF 헬퍼 모드를 비활성화하려면 이 확인란의 선택을 취소합니다.

5단계 **OK**를 클릭합니다.

6단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

OSPFv2에 IETF NSF Graceful Restart 구성

OSPFv2, NSF 지원 디바이스 또는 NSF 인식 디바이스에 IETF NSF Graceful Restart를 구성하려면 다음 단계를 수행합니다

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup > Advanced > Add NSF Properties**를 선택합니다.

2단계 Configuring Cisco NSF 아래에서 **Enable IETF nonstop forwarding (NSF)** 확인란을 선택합니다.

3단계 (선택 사항) Length of graceful restart interval 필드에 재시작 간격을 초 단위로 입력합니다.

참고 기본값은 120초입니다. 재시작 간격이 30초 미만일 경우 Graceful Restart가 종료됩니다.

4단계 (선택 사항) Configuring IETF NSF helper 아래에서 **Enable IETF nonstop forwarding (NSF) for helper mode** 확인란의 선택을 취소합니다.

참고 이 확인란은 기본적으로 선택되어 있습니다. NSF 인식 디바이스에서 IETF NSF 헬퍼 모드를 비활성화하려면 이 확인란의 선택을 취소합니다.

5단계 **OK**를 클릭합니다.

6단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

OSPFv3에 Graceful Restart 구성

OSPFv3에 NSF Graceful Restart 기능을 구성하려면 디바이스를 NSF 지원 디바이스로 구성하고, 디바이스를 NSF 인식 디바이스로 구성하는 두 단계를 수행해야 합니다. OSPFv3에 Graceful Restart를 구성하려면 다음 단계를 수행합니다다음 명령을 입력합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup > Advanced > Add NSF Properties**를 선택합니다.

2단계 Configuring Graceful Restart 아래에서 **Enable Graceful Restart** 확인란을 선택합니다.

3단계 (선택 사항) Restart Interval 필드에 재시작 간격의 값을 입력합니다.

참고 기본값은 120초입니다. 재시작 간격이 30초 미만일 경우 Graceful Restart가 종료됩니다.

4단계 Configuring Graceful Restart Helper 아래에서 **Enable Graceful Restart Helper** 확인란을 선택합니다.

참고 이 확인란은 기본적으로 선택되어 있습니다. NSF 인식 디바이스에서 Graceful-restart 헬퍼 모드를 비활성화하려면 이 확인란의 선택을 취소합니다.

5단계 (선택 사항) **Enable LSA checking** 확인란을 선택하여 strict 링크 상태 광고 확인을 활성화합니다.

참고 이를 활성화하면 재시작 라우터에 플러딩되는 LSA의 변경 사항이 감지되거나, Graceful Restart 프로세스가 시작되었을 때 재시작 라우터의 재전송 목록에 있는 LSA가 변경된 경우, 헬퍼 라우터가 재시작 라우터 프로세스를 종료하는 것을 나타냅니다.

6단계 **OK**를 클릭합니다.

7단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

OSPF 구성 제거

기존에 활성화한 전체 OSPFv2 컨피그레이션을 제거하려면, 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

2단계 **Enable this OSPF Process** 확인란의 선택을 취소합니다.

3단계 **Apply**를 클릭합니다.

기존에 활성화한 전체 OSPFv3 컨피그레이션을 제거하려면, 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 **Enable OSPFv3 Process** 확인란의 선택을 취소합니다.

3단계 **Apply**를 클릭합니다.

OSPFv2의 구성 예

다음 예에는 다양한 선택적 프로세스로 OSPFv2를 활성화하고 구성하는 방법이 나와 있습니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

2단계 **Process Instances** 탭을 클릭하고 OSPF Process 1 필드에 **2**를 입력합니다.

3단계 **Area/Networks** 탭을 클릭하고 **Add**를 클릭합니다.

4단계 Area ID 필드에 **0**을 입력합니다.

5단계 Area Networks 영역의 IP Address 필드에 **10.0.0.0**을 입력합니다.

6단계 Netmask 드롭다운 목록에서 255.0.0.0을 선택합니다.

7단계 **OK**를 클릭합니다.

8단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Redistribution**을 선택합니다.

9단계 **Add**를 클릭합니다.

Add/Edit OSPF Redistribution Entry 대화 상자가 나타납니다.

10단계 Protocol 영역에서 **OSPF** 라디오 버튼을 클릭하여 경로가 재배포되는 소스 프로토콜을 선택합니다. 다른 OSPF 라우팅 프로세스에서 OSPF 재배포 경로를 선택합니다.

11단계 OSPF Process 드롭다운 목록에서 OSPF 프로세스 ID를 선택합니다.

12단계 Match 영역에서 **Internal** 확인란을 선택합니다.

13단계 Metric Value 필드에 재배포되는 경로의 메트릭 값을 **5**로 입력합니다.

14단계 Metric Type 드롭다운 목록에서 Metric Type 값을 1로 선택합니다.

15단계 Route Map 드롭다운 목록에서 1을 선택합니다.

16단계 **OK**를 클릭합니다.

17단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Interface**를 선택합니다.

18단계 Properties 탭에서 **inside** 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit OSPF Properties 대화 상자가 나타납니다.

19단계 Cost 필드에 **20**을 입력합니다.

20단계 **Advanced**를 클릭합니다.

21단계 Retransmit Interval 필드에 **15**를 입력합니다.

22단계 Transmit Delay 필드에 **20**을 입력합니다.

23단계 Hello Interval 필드에 **10**을 입력합니다.

24단계 Dead Interval 필드에 **40**을 입력합니다.

25단계 **OK**를 클릭합니다.

26단계 Edit OSPF Properties 대화 상자의 Priorities 필드에 **20**을 입력하고 **OK**를 클릭합니다.

27단계 **Authentication** 탭을 클릭합니다.

Edit OSPF Authentication 대화 상자가 나타납니다.

28단계 Authentication 영역에서 **MD5** 라디오 버튼을 클릭합니다.

29단계 MD5 and Key ID 영역의 MD5 Key 필드에 **cisco**를 입력하고 MD5 Key ID 필드에 **1**을 입력합니다.

30단계 **OK**를 클릭합니다.

31단계 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택하고 **Area/Networks** 탭을 클릭합니다.

32단계 **OSPF 2** 프로세스를 선택하고 **Edit**를 클릭합니다.

Edit OSPF Area 대화 상자가 나타납니다.

33단계 Area Type 영역에서 **Stub**을 선택합니다.

34단계 Authentication 영역에서 **None**을 선택하고 Default Cost 필드에 **20**을 입력합니다.

35단계 **OK**를 클릭합니다.

36단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPF > Setup**을 선택합니다.

37단계 **Process Instances** 탭을 클릭하고 **OSPF process 2** 확인란을 선택합니다.

38단계 **Advanced**를 클릭합니다.

Edit OSPF Area 대화 상자가 나타납니다.

39단계 Timers 영역에서 SPF Delay Time에 **10**을 입력하고 SPF Hold Time 필드에 **20**을 입력합니다.

40단계 Adjacency Changes 영역에서 **Log Adjacency Change Details** 확인란을 선택합니다.

41단계 **OK**를 클릭합니다.

42단계 **Reset**을 클릭합니다.

OSPFv3 구성의

다음 예에는 ASDM에서 OSPFv3 라우팅을 구성하는 방법이 나와 있습니다.

1단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Setup**을 선택합니다.

2단계 Process Instances 탭에서 다음을 수행합니다.

a. **Enable OSPFv3 Process** 확인란을 선택합니다.

b. Process ID 필드에 **1**을 입력합니다.

3단계 **Areas** 탭을 클릭합니다. 그런 다음 **Add**를 클릭하여 Add OSPFv3 Area 대화 상자를 표시합니다.

4단계 OSPFv3 Process ID 드롭다운 목록에서 **1**을 선택합니다.

5단계 Area ID 필드에 **22**를 입력합니다.

6단계 Area Type 드롭다운 목록에서 **Normal**을 선택합니다.

7단계 Default Cost 필드에 **10**을 입력합니다.

8단계 **Redistribution imports routes to normal and NSSA areas** 확인란을 선택합니다.

9단계 Metric 필드에 **20**을 입력합니다.

10단계 Metric Type 드롭다운 목록에서 **1**을 선택합니다.

11단계 **inside** 확인란을 사용되는 지정된 인터페이스로 선택합니다.

12단계 **Enable Authentication** 확인란을 선택합니다.

13단계 Security Policy Index 필드에 **300**을 입력합니다.

14단계 Authentication Algorithm 드롭다운 목록에서 **SHA-1**을 선택합니다.

15단계 Authentication Key 필드에 **12345ABCDE**를 입력합니다.

16단계 Authentication 드롭다운 목록에서 **DES**를 선택합니다.

17단계 Encryption Key 필드에 **1122334455aabbccddee**를 입력합니다.

18단계 **OK**를 클릭합니다.

19단계 **Route Summarization** 탭을 클릭한 다음 **Add**를 클릭하여 Add Route Summarization 대화 상자를 표시합니다.

20단계 Process ID 드롭다운 목록에서 **1**을 선택합니다.

21단계 Area ID 드롭다운 목록에서 **22**을 선택합니다.

22단계 IPv6 Prefix/Prefix Length 필드에 **2000:122::/64**를 입력합니다.

23단계 (선택 사항) Cost 필드에 **100**을 입력합니다.

24단계 **Advertised** 확인란을 선택합니다.

25단계 **OK**를 클릭합니다.

26단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > OSPFv3 > Interface**를 선택합니다.

27단계 **Properties** 탭을 클릭합니다.

28단계 **inside** 확인란을 선택하고 **Edit**를 클릭하여 Edit OSPF Properties 대화 상자를 표시합니다.

29단계 Cost 필드에 **20**을 입력합니다.

30단계 Priority 필드에 **1**을 입력합니다.

31단계 **point-to-point** 확인란을 선택합니다.

32단계 Dead Interval 필드에 **40**을 입력합니다.

33단계 Hello Interval 필드에 **10**을 입력합니다.

34단계 Retransmit Interval 필드에 **15**를 입력합니다.

35단계 Transmit Delay 필드에 **20**을 입력합니다.

36단계 **OK**를 클릭합니다.

37단계 기본 ASDM 창에서 **Configuration > Device Setup > Routing > Redistribution**을 선택합니다.

38단계 Process ID 드롭다운 목록에서 **1**을 선택합니다.

39단계 Source Protocol 드롭다운 목록에서 **OSPF**를 선택합니다.

40단계 Metric 필드에 **50**을 입력합니다.

41단계 Metric Type 드롭다운 목록에서 **1**을 선택합니다.

42단계 **OK**를 클릭합니다.

43단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

OSPF 모니터링

IP 라우팅 테이블, 캐시, 데이터베이스의 내용 같은 특정 통계를 표시할 수 있습니다. 제공된 정보를 사용하여 리소스 사용률을 결정하고 네트워크 문제를 해결할 수도 있습니다. 또한 노드 도달 범위에 대한 정보를 표시하고 디바이스 패킷이 네트워크를 통해 들어오는 라우팅 경로를 검색할 수 있습니다.

ASDM에서 다양한 OSPFv2 경로 통계를 모니터링하거나 표시하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Monitoring > Routing > OSPF LSAs**를 선택합니다.

2단계 OSPF LSA, Types 1~5, 7을 선택하고 모니터링할 수 있습니다. 각 창에는 하나의 LSA 유형이 다음과 같이 표시됩니다.

- Type 1 LSAs는 프로세스의 영역에 있는 경로를 나타냅니다.
- Type 2 LSAs는 라우터를 광고하는 전용 라우터의 IP 주소를 표시합니다.
- Type 3 LSAs는 목적지 네트워크의 IP 주소를 표시합니다.
- Type 4 LSAs는 AS 경계 라우터의 IP 주소를 표시합니다.
- Type 5 LSAs 및 Type 7 LSAs는 AS 외부 네트워크의 IP 주소를 표시합니다.

3단계 **Refresh**를 클릭하여 각 LSA 유형 창을 업데이트합니다.

4단계 기본 ASDM 창에서 **Monitoring > Routing > OSPF Neighbors**를 선택합니다.

OSPF Neighbors 창의 각 행은 OSPF 인접 디바이스를 나타냅니다. 또한 OSPF Neighbors 창에는 인접 디바이스가 실행 중인 네트워크, 우선순위, 상태, Dead 시간(초 단위), 인접 디바이스의 IP 주소, 인접 디바이스가 실행 중인 인터페이스가 표시됩니다. OSPF 인접 디바이스의 가능한 상태 목록을 보려면 RFC 2328을 참조하십시오.

5단계 **Refresh**를 클릭하여 OSPF Neighbors 창을 업데이트합니다.

ASDM에서 다양한 OSPFv3 경로 통계를 모니터링하거나 표시하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 창에서 **Monitoring > Routing > OSPFv3 LSAs**를 선택합니다.

2단계 OSPFv3 LSAs를 선택하고 모니터링할 수 있습니다. Link State 유형 드롭다운 목록에서 지정된 매개변수에 따라 링크 상태 유형을 선택하여 해당 상태를 표시합니다. 지원되는 링크 상태 유형은 router, network, inter-area prefix, inter-area router, AS external, NSSA, link, intra-area prefix입니다.

3단계 **Refresh**를 클릭하여 각 링크 상태 유형을 업데이트합니다.

4단계 기본 ASDM 창에서 **Monitoring > Routing > OSPFv3 Neighbors**를 선택합니다.

OSPFv3 Neighbors 창의 각 행은 OSPFv3 인접 디바이스를 나타냅니다. 또한 OSPFv3 Neighbors 창에는 인접 디바이스의 IP 주소, 우선순위, 상태, Dead 시간(초 단위), 인접 디바이스가 실행 중인 인터페이스가 표시됩니다. OSPFv3 인접 디바이스의 가능한 상태 목록을 보려면 RFC 5340을 참조하십시오.

5단계 **Refresh**를 클릭하여 OSPFv3 Neighbors 창을 업데이트합니다.

추가 참조 자료

RFC

RFC	제목
2328	OSPFv2
4552	OSPFv3 Authentication
5340	OSPF for IPv6

OSPF의 기능 기록

표 23-1에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 23-1 OSPF의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
OSPF 지원	7.0(1)	OSPF(Open Shortest Path First) 라우팅 프로토콜을 사용한 데이터 라우팅, 인증, 라우팅 정보의 재배포 및 모니터링에 대한 지원이 추가되었습니다. 다음 화면을 도입했습니다. Configuration > Device Setup > Routing > OSPF

표 23-1 OSPF의 기능 기록 (계속)

기능 이름	플랫폼 릴리스	기능 정보
다중 컨텍스트 모드의 동적 라우팅	9.0(1)	다중 컨텍스트 모드에서 OSPFv2 라우팅이 지원됩니다. 도입된 화면: Configuration > Device Setup > Routing > OSPF > Setup
클러스터링		클러스터링 환경에서 OSPFv2 및 OSPFv3에 대해 벌크 동기화, 경로 동기화, Spanned EtherChannel 로드 밸런싱이 지원됩니다.
IPv6에 OSPFv3 지원		IPv6에 OSPFv3 라우팅이 지원됩니다. 다음 명령을 도입했습니다. Configuration > Device Setup > Routing > OSPFv3 > Setup, Configuration > Device Setup > Routing > OSPFv3 > Interface, Configuration > Device Setup > Routing > OSPFv3 > Redistribution, Configuration > Device Setup > Routing > OSPFv3 > Summary Prefix, Configuration > Device Setup > Routing > OSPFv3 > Virtual Link, Monitoring > Routing > OSPFv3 LSAs, Monitoring > Routing > OSPFv3 Neighbors
OSPF Support for Fast Hellos	9.2(1)	OSPF Supports the Fast Hello Packets 기능을 컨피그레이션에 사용하면 OSPF 네트워크에서 통합 속도를 단축할 수 있습니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Routing > OSPF > Interface > Edit OSPF Interface Advanced Properties
타이머		새 OSPF 타이머가 추가되었으며, 기존 타이머는 사용이 중단되었습니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Routing > OSPF > Setup > Edit OSPF Process Advanced Properties
액세스 목록을 사용한 경로 필터링		이제 ACL을 사용한 경로 필터링이 지원됩니다. 다음 화면령을 도입했습니다. Configuration > Device Setup > Routing > OSPF > Filtering Rules > Add Filter Rules
OSPF 모니터링 개선 사항		추가적인 OSPF 모니터링 정보가 추가되었습니다.
OSPF 재배포 BGP		OSPF 재배포 기능이 추가되었습니다. 다음 화면을 추가했습니다. Configuration > Device Setup > Routing > OSPF > Redistribution
NSF를 위한 OSPF 지원	9.3(1)	NSF를 위한 OSPFv2 및 OSPFv3 지원을 추가했습니다. 다음 화면을 추가했습니다. Configuration > Device Setup > Routing > OSPF > Setup > NSF Properties, Configuration > Device Setup > Routing > OSPFv3 > Setup > NSF Properties

EIGRP

이 장에서는 EIGRP(Enhanced Interior Gateway Routing Protocol)를 이용하여 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 Cisco ASA을(를) 구성하는 방법을 설명합니다.

EIGRP 정보

EIGRP는 Cisco에서 개발한 IGRP의 향상된 버전입니다. IGRP 및 RIP와 달리 EIGRP는 주기적인 경로 업데이트를 전송하지 않습니다. EIGRP 업데이트는 네트워크 토폴로지가 변경될 때만 전송됩니다. EIGRP를 다른 라우팅 프로토콜과 차별화하는 핵심 기능으로는 빠른 컨버전스, variable-length 서브넷 마스크 지원, 부분 업데이트 지원, 다중 네트워크 계층 프로토콜 지원이 있습니다.

EIGRP를 실행하는 라우터는 모든 인접 라우팅 테이블을 저장하여 다른 경로에 빠르게 적응할 수 있습니다. 적절한 경로가 존재하지 않는 경우 EIGRP는 인접 디바이스를 쿼리하여 대체 경로를 찾습니다. 이 쿼리는 대체 경로를 발견할 때까지 전파됩니다. variable-length 서브넷 마스크 지원을 통해 네트워크 숫자 경계에서 경로를 자동으로 요약할 수 있습니다. 또한 EIGRP는 모든 인터페이스의 모든 비트 경계에서 요약되도록 구성할 수 있습니다. EIGRP는 주기적인 업데이트를 만들지 않습니다. 대신 경로의 메트릭이 변경될 때만 부부적인 업데이트를 전송합니다. 부분 업데이트 전파가 자동으로 바운딩되므로 정보가 필요한 라우터만 업데이트됩니다. 이 두 기능 덕분에 EIGRP는 IGRP보다 훨씬 적은 대역폭을 사용합니다.

인접 디바이스 탐색은 ASA가 직접 연결된 네트워크의 다른 라우터를 동적으로 학습하기 위해 사용하는 프로세스입니다. EIGRP 라우터는 멀티캐스트 hello 패킷을 전송하여 네트워크에서 존재를 알립니다. ASA가 새로운 인접 디바이스에서 hello 패킷을 수신하면 초기화 비트 세트와 함께 토폴로지 테이블을 인접 디바이스로 보냅니다. 초기화 비트 세트와 함께 토폴로지 업데이트를 수신한 인접 디바이스는 토폴로지 테이블을 다시 ASA로 전달합니다.

hello 패킷은 멀티캐스트 메시지로 전달됩니다. hello 메시지에는 응답할 필요가 없습니다. 고정으로 정의된 인접 디바이스의 경우 예외입니다. **neighbor** 명령을 사용하거나 ASDM에서 hello 간격을 구성하여 인접 디바이스를 구성할 경우 인접 디바이스로 전송되는 hello 메시지는 유니캐스트 메시지로 전송됩니다. 라우팅 업데이트 및 확인은 유니캐스트 메시지로 전송됩니다.

이 인접 관계가 설정되면 네트워크 토폴로지의 변화가 없는 한 라우팅 업데이트가 교환되지 않습니다. 인접 관계는 hello 패킷을 통해 유지됩니다. 인접 디바이스에서 수신된 각 hello 패킷은 보류 시간을 포함합니다. 이 시간은 ASA이(가) 해당 인접 디바이스로부터 hello 패킷을 수신할 것으로 예상되는 시간입니다. ASA이(가) 해당 인접 디바이스가 알린 보류 시간 내에 인접 디바이스로부터 hello 패킷을 수신하지 않으면 ASA은(는) 해당 인접 디바이스를 사용할 수 없는 것으로 간주합니다.

EIGRP 프로토콜은 경로 연산에 중요한 인접 디바이스 검색/복구, RTP(Reliable Transport Protocol) 및 DUAL을 포함하여 4가지 주요 알고리즘 기술을 사용합니다. DUAL은 least-cost 경로뿐 아니라 토폴로지 테이블의 대상에 대한 모든 경로를 저장합니다. least-cost 경로가 라우팅 테이블로 삽입됩니다. 다른 경로는 토폴로지 테이블에 남아 있습니다. 기본 경로가 실패할 경우 가능한 successor에서 다른 경로가 선택됩니다. successor는 대상에 대한 least-cost 경로를 가진 패킷 전달에 사용되는 인접 라우터입니다. 가능성 계산은 경로가 라우팅 루프의 일부가 아님을 보장합니다.

토폴로지 테이블에서 가능한 successor를 찾을 수 없는 경우 경로 재계산이 이루어져야 합니다. 경로 재계산 중 DUAL이 EIGRP 인접 디바이스에 경로를 쿼리하면 EIGRP 인접 디바이스가 다시 자신의 인접 디바이스에 쿼리합니다. 경로에 대한 가능한 successor가 없는 라우터는 도달할 수 없음 메시지를 반환합니다.

경로 재계산 중 DUAL은 경로를 활성으로 표시합니다. 기본적으로 ASA은(는) 인접 디바이스로부터 응답을 수신하기 위해 3분을 대기합니다. ASA이(가) 인접 디바이스로부터 응답을 수신하지 않는 경우 경로가 stuck-in-active로 표시됩니다. 가능한 successor로서 응답이 없는 인접 디바이스를 가리키는 토폴로지 테이블의 모든 경로는 제거됩니다.

참고 EIGRP 인접 관계는 GRE 터널 없이 IPsec 터널을 통해 지원되지 않습니다.

클러스터 사용

EIGRP과 클러스터링 사용에 관한 정보는 19-9 페이지의 동적 라우팅 및 클러스터링에서 참조하십시오.

EIGRP 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명한 방화벽 모드는 지원되지 않습니다.

장애 조치 지침

단일 및 다중 컨텍스트 모드에서 상태 기반 장애 조치를 지원합니다.

IPv6 지침

IPv6를 지원하지 않습니다.

클러스터링 지침

- EIGRP 및 OSPFv2를 모두 사용하도록 구성된 경우 Spanned EtherChannel 및 Individual Interface 클러스터링을 지원합니다.
- Individual Interface 클러스터 설정에서 EIGRP 인접성은 마스터 유닛의 공유 인터페이스에 있는 두 컨텍스트 사이에서만 설정할 수 있습니다. 각 클러스터 노드에 대응하는 여러 인접 구문을 별도로 구성하여 이 문제를 해결할 수 있습니다.

추가 지침

- EIGRP 인스턴스는 멀티캐스트 트래픽의 컨텍스트 간 교환이 지원되지 않기 때문에 공유 인터페이스에서 서로 인접 관계를 형성할 수 없습니다.
- 최대 하나의 EIGRP 프로세스가 지원됩니다.

EIGRP 프로세스 구성을 위한 작업 목록

ASA에서 EIGRP 라우팅을 구성하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP**를 선택합니다.

2단계 Process Instances 탭의 **Enable this EIGRP process** 확인란을 선택하여 EIGRP 라우팅 프로세스를 활성화합니다. 24-4 페이지의 EIGRP 활성화 또는 24-5 페이지의 EIGRP Stub 라우팅 활성화을(를) 참조합니다.

3단계 Setup > Networks 탭의 EIGRP 라우팅에 참여하는 네트워크와 인터페이스를 정의합니다. 자세한 내용은 24-7 페이지의 EIGRP 라우팅 프로세스를 위한 네트워크 정의를 참조하십시오.

4단계 (선택 사항) Filter Rules 창에서 경로 필터를 정의합니다. 경로 필터링은 EIGRP 업데이트에서 송수신이 허용된 경로에 대한 더 많은 컨트롤을 제공합니다. 자세한 내용은 24-13 페이지의 EIGRP의 필터링 네트워크를 참조하십시오.

5단계 (선택 사항) Redistribution 창에서 경로 재배포를 정의합니다.

RIP 및 OSPF에서 검색된 경로를 EIGRP 라우팅 프로세스로 재배포합니다. EIGRP 라우팅 프로세스로의 고정 경로 및 연결 경로를 재배포할 수도 있습니다. 자세한 내용은 24-12 페이지의 EIGRP로 경로 재배포를 참조하십시오.

6단계 (선택 사항) Static Neighbor 창에서 고정 EIGRP 인접 디바이스를 정의합니다.

자세한 내용은 24-11 페이지의 EIGRP 인접 디바이스 정의를 참조하십시오.

7단계 (선택 사항) Summary Address 창에서 요약 주소를 정의합니다.

요약 주소 정의에 관한 자세한 정보는 24-9 페이지의 인터페이스에서 요약 종합 주소 구성에서 참조합니다.

8단계 (선택 사항) Interfaces 창에서 interface-specific EIGRP 매개변수를 정의합니다. 이 매개변수에는 EIGRP 메시지 인증, 보류 시간, hello 간격, 지연 메트릭, split-horizon 사용이 포함됩니다. 자세한 내용은 24-7 페이지의 EIGRP를 위한 인터페이스 구성를 참조하십시오.

9단계 (선택 사항) Default Information 창에서 EIGRP 업데이트의 기본 경로 정보 송수신을 제어합니다. 기본적으로 기본 경로가 전송되고 승인됩니다. 자세한 내용은 24-16 페이지의 EIGRP에서 기본 정보 구성를 참조하십시오.

EIGRP 구성

이 섹션에서는 시스템에서 EIGRP 프로세스를 활성화하는 방법을 설명합니다. EIGRP를 활성화한 후에는 다음 섹션을 참조하여 시스템에서 EIGRP 프로세스를 사용자 정의하는 방법을 알아보십시오.

- 24-4 페이지의 EIGRP 활성화
- 24-5 페이지의 EIGRP Stub 라우팅 활성화

EIGRP 활성화

ASA에서 하나의 EIGRP 라우팅 프로세스만 활성화할 수 있습니다.

EIGRP를 활성화하려면다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

메인 EIGRP Setup 창의 3개 탭은 다음과 같이 EIGRP 활성화에 사용됩니다.

- Process Instances 탭을 통해 각 컨텍스트에 대한 EIGRP 라우팅 프로세스를 활성화할 수 있습니다. 단일 컨텍스트 모드 및 다중 컨텍스트 모드가 모두 지원됩니다. 자세한 내용은 24-4 페이지의 EIGRP 활성화 및 24-5 페이지의 EIGRP Stub 라우팅 활성화에서 참조하십시오.
- 네트워크가 EIGRP 라우팅 프로세스에서 사용하도록 지정하는 Networks 태블릿입니다. 인터페이스가 EIGRP 라우팅에 참여하려면 네트워크 엔트리에 의해 정의된 주소 범위에 해당해야 합니다. 직접 연결 및 고정 네트워크를 알리려면 네트워크 엔트리 범위에 해당해야 합니다. 자세한 내용은 24-7 페이지의 EIGRP 라우팅 프로세스를 위한 네트워크 정의를 참조하십시오.
- 하나 이상의 인터페이스를 패시브 인터페이스로 구성하는 Passive Interfaces 태블릿입니다. EIGRP에서 패시브 인터페이스는 라우팅 업데이트를 보내거나 받지 않습니다. 패시브 인터페이스 테이블은 패시브 인터페이스로 구성된 각 인터페이스를 나열합니다.

2단계 **Enable this EIGRP process** 확인란을 선택합니다.

디바이스에서 하나의 EIGRP 라우팅 프로세스만 활성화할 수 있습니다. 변경 사항을 저장하기 전에 EIGRP Process 필드에 라우팅 프로세스에 대한 자율 시스템 번호(AS)를 입력해야 합니다.

3단계 EIGRP Process 필드에 EIGRP 프로세스에 대한 자율 시스템(AS) 번호를 입력합니다. AS 번호 범위는 1~65535입니다.

4단계 (선택 사항) **Advanced**를 클릭하여 라우터 ID, 기본 메트릭, stub 라우팅, 인접 디바이스 변경 사항과 같은 EIGRP 프로세스 설정과 EIGRP 경로를 위한 관리 거리를 구성합니다.

5단계 **Networks** 탭을 클릭합니다.

6단계 새 네트워크 엔트리를 추가하려면 **Add**를 클릭합니다.

Add EIGRP Network 대화 상자가 나타납니다. 네트워크 엔트리를 삭제하려면 테이블의 엔트리를 선택하고 **Delete**를 클릭합니다.

7단계 드롭다운 목록에서 EIGRP 라우팅 프로세스의 AS 번호를 선택합니다.

8단계 IP Address 필드에서 EIGRP 라우팅 프로세스에 참여할 네트워크의 IP 주소를 입력합니다.

참고 네트워크 엔트리를 변경하려면 먼저 엔트리를 제거한 후 새로 추가해야 합니다. 기존 엔트리를 수정할 수 없습니다.

9단계 Network Mask 필드에 IP 주소에 적용할 네트워크 마스크를 입력합니다.

10단계 **OK**를 클릭합니다.

EIGRP Stub 라우팅 활성화

ASA을(를) EIGRP stub 라우터로 활성화하고 구성할 수 있습니다. Stub 라우팅은 ASA에 대한 메모리 및 처리 능력 요구 사항을 낮춥니다. stub 라우터로서 ASA은(는) 모든 로컬이 아닌 트래픽을 배포 라우터로 전달하기 때문에 전체 EIGRP 라우팅 테이블을 유지할 필요가 없습니다. 일반적으로 배포 라우터는 기본 경로 외에 아무 것도 stub 라우터로 보낼 필요가 없습니다.

지정된 경로만 stub 라우터에서 배포 라우터로 전파됩니다. stub 라우터로서 ASA은(는) 요약, 연결된 경로, 재배포된 고정 경로, 외부 경로 및 "inaccessible" 메시지를 포함한 내부 경로에 대한 모든 쿼리에 응답합니다. ASA이(가) stub으로 구성된 경우 특수 피어 정보 패킷을 모든 인접 디바이스 라우터로 보내 그 상태를 stub 라우터에 보고합니다. stub 상태를 알려주는 패킷 정보를 수신하는 모든 인접 디바이스는 경로에 대해 일체 stub 라우터에 쿼리하지 않고 stub 피어가 있는 라우터는 피어에 쿼리하지 않습니다. stub 라우터는 올바른 업데이트를 모든 피어에 전송하기 위해 배포 라우터에 의지합니다.

ASA을(를) EIGRP stub 라우팅 프로세스로 활성화하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 EIGRP Process 필드에 EIGRP 프로세스에 대한 자율 시스템(AS) 번호를 입력합니다. AS 번호 범위는 1~65535입니다.

4단계 **Advanced**를 클릭하여 EIGRP stub 라우팅 프로세스를 구성합니다.

Edit EIGRP Process Advanced Properties 대화 상자가 나타납니다.

5단계 Edit EIGRP Process Advanced Properties 대화 상자의 stub 영역에서 다음 EIGRP stub 라우팅 프로세스 중 하나 이상을 선택합니다.

- Stub Receive only—EIGRP stub 라우팅 프로세스가 인접 라우터로부터 경로 정보를 수신하되 인접 디바이스로 경로 정보를 보내지 않도록 구성합니다. 이 옵션을 선택하면 다른 stub 라우팅 옵션을 선택할 수 없습니다.
- Stub Connected—연결된 경로를 알립니다.
- Stub Static—고정 경로를 알립니다.
- Stub Redistributed—재배포된 경로를 알립니다.
- Stub Summary—요약 경로를 알립니다.

6단계 **OK**를 클릭합니다.

7단계 **Networks** 탭을 클릭합니다.

8단계 **Add**를 클릭하여 새 네트워크 엔트리를 추가합니다.

Add EIGRP Network 대화 상자가 나타납니다. 네트워크 엔트리를 삭제하려면 테이블의 엔트리를 선택한 다음 **Delete**를 클릭합니다.

9단계 드롭다운 목록에서 EIGRP 라우팅 프로세스의 AS 번호를 선택합니다.

10단계 IP Address 필드에서 EIGRP 라우팅 프로세스에 참여할 네트워크의 IP 주소를 입력합니다.

참고 네트워크 엔트리를 변경하려면 먼저 엔트리를 제거한 후 새로 추가해야 합니다. 기존 엔트리를 수정할 수 없습니다.

11단계 Network Mask 필드에 IP 주소에 적용할 네트워크 마스크를 입력합니다.

12단계 **OK**를 클릭합니다.

EIGRP 사용자 정의

이 섹션에서는 EIGRP 라우팅을 사용자 정의하는 방법을 설명합니다.

EIGRP 라우팅 프로세스를 위한 네트워크 정의

네트워크 테이블을 통해 EIGRP 라우팅 프로세스가 사용하는 네트워크를 지정할 수 있습니다. 인터페이스가 EIGRP 라우팅에 참여하려면 네트워크 엔트리에 의해 정의된 주소 범위에 해당해야 합니다. 직접 연결 및 고정 네트워크를 알리려면 네트워크 엔트리 범위에 해당해야 합니다.

네트워크 테이블은 EIGRP 라우팅 프로세스에 대해 지정된 네트워크를 표시합니다. 테이블의 각 행은 네트워크 주소와 지정된 EIGRP 라우팅 프로세스에 대해 구성된 연결된 마스크를 표시합니다.

네트워크를 추가하거나 정의하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 EIGRP Process 필드에 EIGRP 프로세스에 대한 자율 시스템(AS) 번호를 입력합니다. AS 번호 범위는 1~65535입니다.

4단계 **Networks** 탭을 클릭합니다.

5단계 **Add**를 클릭하여 새 네트워크 엔트리를 추가합니다.

Add EIGRP Network 대화 상자가 나타납니다. 네트워크 엔트리를 삭제하려면 테이블의 엔트리를 선택한 다음 **Delete**를 클릭합니다.

6단계 드롭다운 목록에서 EIGRP 라우팅 프로세스의 AS 번호를 선택합니다.

7단계 IP Address 필드에서 EIGRP 라우팅 프로세스에 참여할 네트워크의 IP 주소를 입력합니다.

참고 네트워크 엔트리를 변경하려면 먼저 엔트리를 제거한 후 새로 추가해야 합니다. 기존 엔트리를 수정할 수 없습니다.

8단계 Network Mask 필드에 IP 주소에 적용할 네트워크 마스크를 입력합니다.

9단계 **OK**를 클릭합니다.

EIGRP를 위한 인터페이스 구성

EIGRP 라우팅에 참여를 원하지 않지만 알리고 싶은 네트워크에 연결된 인터페이스가 있다면 인터페이스가 연결된 네트워크를 포함하는 ASA 을 구성하고을 사용하여 인터페이스가 EIGRP 업데이트를 보내거나 받지 않도록 할 수 있습니다.

EIGRP에 대한 인터페이스를 구성하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 **OK**를 클릭합니다.

4단계 **Configuration > Device Setup > Routing > EIGRP > Interfaces**를 선택합니다.

인터페이스 창이 나타나고 EIGRP 인터페이스 컨피그레이션을 표시합니다. Interface Parameters 테이블은 ASA의 모든 인터페이스를 표시하고 인터페이스별로 다음 설정을 수정할 수 있게 합니다.

- 인증 키와 모드.
- EIGRP hello 간격 및 보류 시간.
- EIGRP 메트릭 계산에 사용되는 인터페이스 지연 메트릭.
- 인터페이스의 split-horizon 사용.

5단계 인터페이스 엔트리를 두 번 클릭하여 인터페이스를 선택하거나 엔트리를 클릭한 후 **Edit**를 클릭합니다.

Edit EIGRP Interface Entry 대화 상자가 표시됩니다.

6단계 EIGRP Process 필드에 EIGRP 프로세스에 대한 AS 번호를 입력합니다. AS 번호 범위는 1~65535입니다.

7단계 Hello Interval 필드에 인터페이스에서 EIGRP hello 패킷이 전송되는 간격을 입력합니다.

유효한 값의 범위는 1~65535초입니다. 기본값은 5초입니다.

8단계 Hold Time 필드에 보류 시간을 초 단위로 입력합니다. 유효한 값의 범위는 1~65535초입니다. 기본값은 15초입니다.

9단계 Split Horizon에 대한 **Enable** 확인란을 선택합니다.

10단계 Delay 필드에 지연 값을 입력합니다. 지연 시간은 10마이크로초 단위입니다. 유효한 값은 1부터 16777215입니다.

11단계 **Enable MD5 Authentication** 확인란을 선택하여 EIGRP 프로세스 메시지의 MD5 인증을 활성화합니다.

12단계 Key 또는 Key ID 값을 입력합니다.

- Key 필드에 EIGRP 업데이트를 인증할 키를 입력합니다. 키는 최대 16자를 포함할 수 있습니다.
- Key ID 필드에 key identification 값을 입력합니다. 유효한 값의 범위는 1~255입니다.

13단계 **OK**를 클릭합니다.

패시브 인터페이스 구성

하나 이상의 인터페이스를 패시브 인터페이스로 구성할 수 있습니다. EIGRP에서 패시브 인터페이스는 라우팅 업데이트를 보내거나 받지 않습니다.

패시브 인터페이스를 구성하려면 다음 단계를 수행하십시오.

참고 ASDM에서 Passive Interface 테이블은 패시브 인터페이스로 구성된 각 인터페이스를 나열합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 **OK**를 클릭합니다.

4단계 **Passive Interfaces** 탭을 클릭합니다.

5단계 드롭다운 목록에서 구성하려는 인터페이스를 선택합니다.

6단계 **Suppress routing updates on all interfaces** 확인란을 선택하여 모든 인터페이스를 패시브로 지정합니다. Passive Interface 테이블에 인터페이스가 표시되지 않더라도 확인란이 선택되어 있다면 패시브로 구성됩니다.

7단계 **Add**를 클릭하여 패시브 인터페이스 엔트리를 추가합니다.

Add EIGRP Passive Interface 대화 상자가 표시됩니다. 패시브로 설정할 인터페이스를 선택하고 **Add**를 추가합니다. 패시브 인터페이스를 제거하려면 테이블에서 인터페이스를 선택한 다음 **Delete**를 클릭합니다.

8단계 **OK**를 클릭합니다.

인터페이스에서 요약 종합 주소 구성

인터페이스별로 요약 주소를 구성할 수 있습니다. 네트워크 숫자 경계에서 발생하지 않는 요약 주소를 생성하려는 경우 또는 자동 경로 요약을 비활성화하고 ASA에서 요약 주소를 사용하려는 경우 요약 주소를 수동으로 정의해야 합니다. 라우팅 테이블에 다른 특정 경로가 있는 경우 EIGRP는 모든 추가 경로의 최소값과 동등한 메트릭을 통해 인터페이스로 요약 주소를 알립니다.

요약 주소를 생성하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Interfaces**를 선택합니다.

인터페이스 창은 EIGRP 인터페이스 컨피그레이션을 표시합니다. Interface Parameters 테이블은 ASA의 모든 인터페이스를 표시하고 인터페이스별로 설정을 수정할 수 있게 합니다. 이 설정에 대한 자세한 내용은 24-7 페이지의 EIGRP를 위한 인터페이스 구성에서 참조하십시오.

2단계 인터페이스에 대한 EIGRP 매개 변수를 구성하려면 인터페이스 엔트리를 두 번 클릭하거나 엔트리를 선택하고 **Edit**를 클릭합니다.

3단계 **OK**를 클릭합니다.

4단계 **Configuration > Device Setup > Routing > EIGRP > Summary Address**를 선택합니다.

Summary Address 창은 고정으로 정의된 EIGRP 요약 주소 테이블을 표시합니다. 기본적으로 EIGRP는 네트워크 수준에 대한 서브넷 경로를 요약합니다. Summary Address 창에서 서브넷 수준으로의 고정으로 정의된 EIGRP 요약 주소를 생성할 수 있습니다.

5단계 **Add**를 클릭하여 새 EIGRP 요약 주소를 추가하거나 **Edit**를 클릭하여 테이블에서 기존 EIGRP 요약 주소를 편집합니다.

Add Summary Address 또는 Edit Summary Address 대화 상자가 표시됩니다. 테이블의 엔트리를 두 번 클릭하여 엔트리를 클릭할 수도 있습니다.

6단계 EIGRP Process 필드에 EIGRP 프로세스에 대한 자율 시스템(AS) 번호를 입력합니다. AS 번호 범위는 1~65535입니다.

7단계 인터페이스 드롭다운 목록에서 요약 주소를 알릴 인터페이스를 선택합니다.

8단계 IP Address 필드에 요약 경로의 IP 주소를 입력합니다.

9단계 Netmask 필드에서 IP 주소에 적용할 네트워크 마스크를 선택하거나 입력합니다.

10단계 Administrative Distance 필드에 경로에 대한 관리 거리를 입력합니다. 비워두면 경로는 기본 관리 거리인 5로 설정됩니다.

11단계 **OK**를 클릭합니다.

인터페이스 지연 값 변경

인터페이스 지연 값은 EIGRP 거리 계산에 사용됩니다. 인터페이스별로 이 값을 수정할 수 있습니다.

인터페이스 지연 값을 변경하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Interfaces**를 선택합니다.

인터페이스 창은 EIGRP 인터페이스 컨피그레이션을 표시합니다. Interface Parameters 테이블은 ASA의 모든 인터페이스를 표시하고 인터페이스별로 설정을 수정할 수 있게 합니다. 이 설정에 대한 자세한 내용은 24-7 페이지의 EIGRP를 위한 인터페이스 구성에서 참조하십시오.

2단계 인터페이스 엔트리를 두 번 클릭하거나 인터페이스 엔트리를 선택하고 **Edit**를 클릭하여 인터페이스에 대한 EIGRP 매개변수의 지연 값을 구성합니다.

Edit EIGRP Interface Entry 대화 상자가 표시됩니다.

3단계 지연 필드에 10마이크로초 단위로 지연 시간을 입력합니다. 유효한 값은 1~16777215입니다.

4단계 **OK**를 클릭합니다.

인터페이스에서 EIGRP 인증 활성화

EIGRP 경로 인증은 EIGRP 라우팅 프로토콜로부터 라우팅 업데이트의 MD5 인증을 제공합니다. 각 EIGRP 패킷의 MD5 키 입력 다이제스트를 사용하여 승인되지 않은 소스로부터 허가되지 않거나 잘못된 라우팅 메시지가 수신되는 것을 방지할 수 있습니다.

EIGRP 경로 인증은 인터페이스별로 구성됩니다. EIGRP 메시지 인증을 구성된 인터페이스의 모든 EIGRP 인접 디바이스는 인접성을 위한 동일한 인증 모드와 키로 구성되어야 설정 가능합니다.

참고 EIGRP 경로 인증을 활성화하기 전에 EIGRP를 활성화해야 합니다.

인터페이스에서 EIGRP 인증을 활성화하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 **EIGRP Process** 필드에 EIGRP 프로세스에 대한 자율 시스템(AS) 번호를 입력합니다. AS 번호 범위는 1~65535입니다.

4단계 **Networks** 탭을 클릭합니다.

5단계 **Add**를 클릭하여 새 네트워크 엔트리를 추가합니다.

Add EIGRP Network 대화 상자가 나타납니다. 네트워크 엔트리를 삭제하려면 테이블의 엔트리를 선택한 다음 **Delete**를 클릭합니다.

6단계 드롭다운 목록에서 EIGRP 라우팅 프로세스의 AS 번호를 선택합니다.

7단계 IP Address 필드에 EIGRP 라우팅 프로세스에 참여할 네트워크의 IP 주소를 입력합니다.

참고 네트워크 엔트리를 변경하려면 먼저 엔트리를 제거한 후 새로 추가해야 합니다. 기존 엔트리를 수정할 수 없습니다.

8단계 Network Mask 필드에서 IP 주소에 적용할 네트워크 마스크를 선택하거나 입력합니다.

9단계 **OK**를 클릭합니다.

10단계 **Configuration > Device Setup > Routing > EIGRP > Interfaces**를 선택합니다.

인터페이스 창은 EIGRP 인터페이스 컨피그레이션을 표시합니다. Interface Parameters 테이블은 ASA의 모든 인터페이스를 표시하고 인터페이스별로 설정을 수정할 수 있게 합니다. 이 설정에 대한 자세한 내용은 24-7 페이지의 EIGRP를 위한 인터페이스 구성에서 참조하십시오.

11단계 **Enable MD5 Authentication** 확인란을 선택하여 EIGRP 프로세스 메시지의 MD5 인증을 활성화합니다. 이 확인란을 선택한 후 다음 중 하나를 제공합니다.

- Key 필드에 EIGRP 업데이트를 인증할 키를 입력합니다. 키는 최대 16자를 포함할 수 있습니다.
- Key ID 필드에 key identification 값을 입력합니다. 유효한 값의 범위는 1~255입니다.

12단계 **OK**를 클릭합니다.

EIGRP 인접 디바이스 정의

EIGRP hello 패킷은 멀티캐스트 패킷으로 전송됩니다. EIGRP 인접 디바이스가 터널과 같이 브로드캐스트가 아닌 네트워크에 위치한 경우 해당 인접 디바이스를 수동으로 정의해야 합니다. EIGRP 인접 디바이스를 수동으로 정의할 경우 hello 패킷은 유니캐스트 메시지로 해당 인접 디바이스에 전송됩니다.

EIGRP 인접 디바이스를 수동으로 정의하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 EIGRP Process 필드에 EIGRP 프로세스에 대한 AS 번호를 입력합니다. AS 번호 범위는 1~65535입니다.

4단계 **Configuration > Device Setup > Routing > EIGRP > Static Neighbor**를 선택합니다.

Static Neighbor 창이 나타나고 고정으로 정의된 EIGRP 인접 디바이스를 표시합니다. EIGRP 인접 디바이스는 EIGRP 라우팅 정보를 ASA와(과) 송수신합니다. 일반적으로 인접 디바이스는 인접 디바이스 검색 프로세스를 통해 동적으로 검색됩니다. 그러나 point-to-point, nonbroadcast 네트워크에서는 인접 디바이스를 고정으로 정의해야 합니다.

Static Neighbor 테이블의 각 행은 각 인접 디바이스에 대한 EIGRP 자율 시스템 번호, 인접 디바이스 IP 주소, 인접 디바이스가 제공되는 인터페이스를 표시합니다.

Static Neighbor 창에서 고정 인접 디바이스를 추가하거나 편집할 수 있습니다.

5단계 EIGRP 고정 인접 디바이스를 추가하거나 편집하려면 **Add** 또는 **Edit**를 클릭합니다.

Add or Edit EIGRP Neighbor Entry 대화 상자가 표시됩니다.

6단계 인접 디바이스가 구성되는 EIGRP 프로세스에 대한 드롭다운 목록에서 EIGRP AS 번호를 선택합니다.

7단계 인터페이스 이름 드롭다운 목록에서 인접 디바이스가 제공되는 인터페이스의 이름을 선택합니다.

8단계 Neighbor IP Address 필드에 인접 디바이스의 IP 주소를 입력합니다.

9단계 **OK**를 클릭합니다.

EIGRP로 경로 재배포

RIP 및 OSPF에서 검색된 경로를 EIGRP 라우팅 프로세스로 재배포할 수 있습니다. 고정 경로 및 연결된 경로도 EIGRP 라우팅 프로세스로 재배포할 수 있습니다. EIGRP 컨피그레이션에서 **network** 구문 범위에 해당하는 경우 연결된 경로를 재배포할 필요가 없습니다.

참고 RIP만 해당: 이 절차를 시작하기 전에 지정된 라우팅 프로토콜에서 어떤 경로가 RIP 라우팅 프로세스로 재배포될지 정의하기 위해 경로 지도를 생성해야 합니다. 경로 지도 생성에 관한 자세한 정보는 21 장, “경로 맵”,에서 참조하십시오.

EIGRP 라우팅 프로세스로 경로를 재배포하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 EIGRP Process 필드에 EIGRP 프로세스에 대한 AS 번호를 입력합니다. AS 번호 범위는 1~65535입니다.

4단계 **Configuration > Device Setup > Routing > EIGRP > Redistribution**을 선택합니다.

Redistribution 창은 다른 라우팅 프로토콜의 경로를 EIGRP 라우팅 프로세스로 재배포할 때의 규칙을 표시합니다. 고정인 연결 경로를 EIGRP 라우팅 프로세스에 재배포할 경우 메트릭 구성이 권장되나 필수 사항은 아닙니다. 재배포 창 테이블의 각 행은 경로 재배포 엔트리를 포함합니다.

5단계 **Add**를 클릭하여 새로운 재배포 규칙을 추가합니다. 기존 재배포 규칙을 편집하는 경우 6단계로 이동합니다.

Add EIGRP Redistribution Entry 대화 상자가 표시됩니다.

6단계 테이블의 주소를 선택하고 **Edit**를 클릭하여 기존 EIGRP 고정 인접 디바이스를 편집합니다. 테이블의 엔트리를 두 번 클릭하여 편집할 수도 있습니다.

Edit EIGRP Redistribution Entry 대화 상자가 표시됩니다.

7단계 드롭다운 목록에서 엔트리를 적용할 EIGRP 라우팅 프로세스의 AS 번호를 선택합니다.

8단계 프로토콜 영역에서 라우팅 프로세스에 대한 다음 프로토콜 중 하나에 대한 라디오 버튼을 클릭합니다.

- **Static**을 선택하면 고정 경로를 EIGRP 라우팅 프로세스로 재배포합니다. 네트워크 구문 범위에 해당하는 고정 경로는 EIGRP로 자동으로 재배포됩니다. 이에 대한 재배포 규칙을 정의할 필요가 없습니다.
- **Connected**을 선택하면 연결된 경로를 EIGRP 라우팅 프로세스로 재배포합니다. 네트워크 구문 범위에 해당하는 연결된 경로는 EIGRP로 자동으로 재배포됩니다. 이에 대한 재배포 규칙을 정의할 필요가 없습니다.
- **RIP**를 선택하면 EIGRP로의 RIP 라우팅 프로세스에서 발견된 경로를 재배포합니다.
- **OSPF**를 선택하면 EIGRP로의 OSPF 라우팅 프로세스에서 발견된 경로를 재배포합니다.

9단계 Optional Metrics 영역에서 경로 재배포에 사용되는 다음 메트릭 중 하나를 선택합니다.

- **Bandwidth**:초당 킬로비트 단위의 EIGRP 대역폭. 유효한 값은 1부터 4294967295입니다.
- **Delay**: 10마이크로초 단위의 EIGRP 지연 메트릭. 유효한 값의 범위는 0~4294967295입니다.
- **Reliability**: EIGRP 신뢰성 메트릭. 유효한 값 범위는 0~255입니다. 255는 100% 신뢰성을 나타냅니다.
- **Loading**: EIGRP 유효 대역폭(로딩) 메트릭. 유효한 값 범위는 1~255입니다. 255는 100% 로딩을 나타냅니다.
- **MTU**: 경로의 MTU. 유효한 값의 범위는 1~65535입니다.

10단계 Route Map 드롭다운 목록에서 경로 지도를 선택하여 어떤 경로가 EIGRP 라우팅 프로세스로 재배포될지 정의합니다. 경로 지도 구성에 관한 자세한 정보는 21 장, “경로 맵”.에서 참조하십시오.

11단계 Optional OSPF Redistribution 영역에서 다음 OSPF 라디오 버튼 중 하나를 클릭하여 어떤 OSPF 경로를 EIGRP 라우팅 프로세스로 재배포할지 지정합니다.

- **Match Internal**을 클릭하면 지정된 OSPF 프로세스 내부의 경로와 일치시킵니다.
- **Match External 1**을 클릭하면 지정된 OSPF 프로세스 외부의 타입 1 경로와 일치시킵니다.
- **Match External 2**을 클릭하면 지정된 OSPF 프로세스 외부의 타입 2 경로와 일치시킵니다.
- **Match NSSA-External 1**을 클릭하면 지정된 OSPF NSSA 외부의 타입 1 경로와 일치시킵니다.
- **Match NSSA-External 2**을 클릭하면 지정된 OSPF NSSA 외부의 타입 2 경로와 일치시킵니다.

12단계 **OK**를 클릭합니다.

EIGRP의 필터링 네트워크

참고 이 프로세스를 시작하기 전에 알리고자 하는 경로를 정의하는 표준 ACL을 생성해야 합니다. 업데이트 송신 또는 수신에서 필터링하려는 경로를 정의하는 표준 ACL을 생성하는 것입니다.

EIGRP에서 네트워크를 필터링하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 EIGRP Process 필드에 EIGRP 프로세스에 대한 AS 번호를 입력합니다. AS 번호 범위는 1~65535입니다.

4단계 **Configuration > Device Setup > Routing > EIGRP > Filter Rules**를 선택합니다.

Filter Rules 창이 나타나고 EIGRP 라우팅 프로세스에 대해 구성된 경로 필터링 규칙을 표시합니다. 필터 규칙을 통해 EIGRP 라우팅 프로세스가 수락하거나 알리는 경로를 제어할 수 있습니다.

필터 규칙 테이블의 각 행은 특정 인터페이스 또는 라우팅 프로토콜을 위한 필터 규칙에 대해 설명합니다. 예를 들어 바깥 인터페이스에서 안쪽 방향으로의 필터 규칙은 바깥 인터페이스에서 수신된 모든 EIGRP 업데이트에 필터링을 적용합니다. 라우팅 프로토콜로 OSPF 10이 지정된 바깥 방향의 필터 규칙은 아웃바운드 EIGRP 업데이트에서 EIGRP 라우팅 프로세스로 재배포되는 경로에 필터 규칙을 적용합니다.

5단계 **Add**를 클릭하여 필터 규칙을 추가합니다. 기존 필터 규칙을 편집하는 경우 6단계로 건너뜁니다.

Add Filter Rules 대화 상자가 나타납니다.

6단계 필터 규칙을 편집하려면 테이블에서 필터 규칙을 선택하고 **Edit**를 클릭합니다.

Edit Filter Rules 대화 상자가 나타납니다. 필터 규칙을 두 번 클릭하여 규칙을 편집할 수도 있습니다. 필터 규칙을 삭제하려면 테이블에서 필터 규칙을 선택하고 **Delete**를 클릭합니다.

7단계 EIGRP 라우팅 프로세스의 드롭다운 목록에서 엔트리가 적용되는 AS 번호를 선택합니다.

8단계 드롭다운 목록에서 필터 경로의 방향을 선택합니다.

수신 EIGRP 라우팅 업데이트에서 경로를 필터링하는 규칙에 대해 **in**을 선택합니다. **out**을 선택하면 ASA이(가) 전송한 EIGRP 라우팅 업데이트의 경로를 필터링할 수 있습니다.

out을 선택하면 Routing process 필드가 활성화됩니다. 필터링할 경로 유형을 선택합니다. 고정, 연결, RIP 및 OSPF 라우팅 프로세스에서 재배포되는 경로를 필터링할 수 있습니다. 라우팅 프로세스를 지정하는 필터는 모든 인터페이스에서 전송된 업데이트로부터의 경로를 필터링합니다.

9단계 ID 필드에 OSPF 프로세스 ID를 입력합니다.

10단계 **Interface** 라디오 버튼을 클릭하고 필터를 적용할 인터페이스를 선택합니다.

11단계 **Add** 또는 **Edit**를 클릭하여 필터 규칙에 대한 ACL을 정의합니다. **Edit**를 클릭하면 선택한 네트워크 규칙에 대한 Network Rule 대화 상자가 열립니다.

Network Rule 대화 상자가 나타납니다.

12단계 Action 드롭다운 목록에서 Permit을 선택하여 지정된 네트워크의 알림을 허용하고 Deny를 선택하여 지정된 네트워크의 알림을 막습니다.

13단계 IP Address 필드에 허용 또는 거부되는 네트워크의 IP 주소를 입력합니다. 모든 주소를 허용하거나 거부하려면 IP 주소 **0.0.0.0**을(를) **0.0.0.0** 네트워크 마스크와 함께 사용합니다.

14단계 Netmask 드롭다운 목록에서 네트워크 IP 주소에 적용할 네트워크 마스크를 선택합니다. 이 필드에 네트워크 마스크를 입력하거나 목록에서 공통 마스크 중 하나를 선택합니다.

15단계 **OK**를 클릭합니다.

EIGRP hello 간격 및 보류 시간 사용자 정의

ASA은(는) 주기적으로 hello 패킷을 전송하여 인접 디바이스를 발견하고 인접 디바이스가 도달 불가 또는 작동 불능 상태가 되는 시간을 파악합니다. 기본적으로 hello 패킷은 5초 간격으로 전송됩니다.

hello 패킷은 ASA보류 시간을 알립니다. 보류 시간은 EIGRP 인접 디바이스에 ASA을(를) 도달 가능으로 간주할 시간 길이를 알려줍니다. 인접 디바이스가 알려진 보류 시간 내에 hello 패킷을 수신하지 못하면 ASA은(는) 도달 불가로 간주됩니다. 기본적으로 알려지는 보류 시간은 15초(hello 간격의 3배)입니다.

hello 간격과 알려진 보류 시간은 인터페이스별로 구성됩니다. 보류 시간은 hello 간격의 최소 3배로 설정하는 것이 좋습니다.

hello 간격과 알려진 보류 시간을 구성하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 **OK**를 클릭합니다.

4단계 **Configuration > Device Setup > Routing > EIGRP > Interfaces**를 선택합니다.

인터페이스 창이 나타나고 모든 EIGRP 인터페이스 컨피그레이션을 표시합니다.

5단계 인터페이스 엔트리를 두 번 클릭하거나 엔트리를 클릭하고 **Edit**를 클릭합니다.

Edit EIGRP Interface Entry 대화 상자가 표시됩니다.

6단계 드롭다운 목록에서 EIGRP 라우팅 프로세스를 활성화했을 때 설정된 시스템 숫자로 채워진 EIGRP AS 번호를 선택합니다.

7단계 Hello Interval 필드에 인터페이스에서 EIGRP hello 패킷이 전송되는 간격을 입력합니다.

유효한 값의 범위는 1~65535초입니다. 기본값은 5초입니다.

8단계 Hold Time 필드에 보류 시간을 초 단위로 지정합니다.

유효한 값의 범위는 1~65535초입니다. 기본값은 15초입니다.

9단계 **OK**를 클릭합니다.

자동 경로 요약 비활성화

기본적으로 자동 경로 요약이 활성화되어 있습니다. EIGRP 라우팅 프로세스는 네트워크 번호 경계에서 요약됩니다. 불연속 네트워크를 가진 경우 라우팅 문제가 발생할 수 있습니다.

예를 들어 네트워크 192.168.1.0, 192.168.2.0 및 192.168.3.0이 연결된 라우터가 있고 이러한 네트워크가 모두 EIGRP에 참여하는 경우 EIGRP 라우팅 프로세스가 해당 경로에 대해 요약 주소 192.168.0.0을 생성합니다. 네트워크 192.168.10.0 및 192.168.11.0으로 라우터가 추가되고 해당 네트워크가 EIGRP에 참여할 경우에도 192.168.0.0으로 요약됩니다. 잘못된 위치에 트래픽이 라우팅될 가능성을 방지하려면 충돌하는 요약 주소를 만드는 라우터에서 자동 경로 요약을 비활성화해야 합니다.

ASDM에서 자동 경로 요약을 비활성화하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 **Process Instance** 탭을 클릭합니다.

4단계 **Advanced**를 클릭합니다.

5단계 요약 영역에서 **Auto-Summary** 확인란 선택을 취소합니다.

참고 이 설정은 기본적으로 활성화되어 있습니다.

6단계 **OK**를 클릭합니다.

EIGRP에서 기본 정보 구성

EIGRP 업데이트에서 기본 경로 정보의 송수신을 제어할 수 있습니다. 기본적으로 기본 경로가 전송되고 승인됩니다. 기본 정보 수신을 금지하도록 ASA을(를) 구성하면 수신된 경로에서 후보 기본 경로 비트가 차단됩니다. 기본 정보 전송을 금지하도록 ASA을(를) 구성하면 알려진 경로에서의 기본 경로 비트 설정이 비활성화됩니다.

ASDM에서 Default Information 창은 EIGRP 업데이트의 기본 경로 정보 송수신 제어를 위한 규칙 테이블을 표시합니다. 각 EIGRP 라우팅 프로세스에 대해 하나의 in 규칙과 out 규칙을 가질 수 있습니다(현재 하나의 프로세스만 지원됨).

기본적으로 기본 경로가 전송되고 승인됩니다. 기본 경로 정보 송수신을 제한하거나 비활성화하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

메인 EIGRP 설정 창이 표시됩니다.

2단계 **Enable EIGRP routing** 확인란을 선택합니다.

3단계 **OK**를 클릭합니다.

4단계 다음 중 하나를 수행합니다.

- **Add**를 클릭하여 새 엔트리를 만듭니다.
- 엔트리를 편집하려면 테이블의 엔트리를 두 번 클릭하거나 엔트리를 클릭한 다음 **Edit**를 클릭합니다.

  해당 엔트리에 대한 Add Default Information 또는 Edit Default Information 대화 상자가 나타납니다. EIGRP 필드의 EIGRP AS 번호가 자동으로 선택됩니다.

5단계 Direction 필드에서 다음 옵션 중 규칙에 대한 방향을 선택합니다.

- **in**—규칙이 수신 EIGRP 업데이트에서 기본 경로 정보를 필터링합니다.
- **out**—규칙이 발신 EIGRP 업데이트에서 기본 경로 정보를 필터링합니다.

  각 EIGRP 프로세스에 대해 하나의 in 규칙과 하나의 out 규칙을 가질 수 있습니다.

6단계 네트워크 규칙 테이블에 네트워크 규칙을 추가합니다. 네트워크 규칙은 기본 경로 정보를 보내거나 받을 때 허용할 네트워크와 허용하지 않을 네트워크를 정의합니다. 기본 정보 필터 규칙에 추가하려는 각 네트워크 규칙에 대해 다음 단계를 반복합니다.

a. **Add**를 클릭하여 네트워크 규칙을 추가합니다. 기존 네트워크 규칙을 두 번 클릭하여 규칙을 편집합니다.

b. Action 필드에서 **Permit**을 클릭하여 네트워크를 허용하거나 **Deny**를 클릭하여 차단합니다.

c. IP Address 및 Network Mask 필드에 규칙을 통해 허용하거나 거부할 네트워크의 IP 주소와 네트워크 마스크를 입력합니다.

   모든 기본 경로 정보 수신을 거부하려면 네트워크 주소로 **0.0.0.0**을 입력하고 네트워크 마스크로 **0.0.0.0**을 선택합니다.

d. **OK**를 클릭하여 지정된 네트워크 규칙을 기본 정보 필터 규칙에 추가합니다.

7단계 **OK**를 클릭하여 기본 정보 필터 규칙을 승인합니다.

EIGRP Split Horizon 비활성화

Split horizon은 EIGRP 업데이트 및 쿼리 패킷의 전송을 제어합니다. 인터페이스에서 split horizon이 활성화된 경우 업데이트 및 쿼리 패킷이 이 인터페이스가 next hop인 대상으로 전송되지 않습니다. 이 방식으로 업데이트 및 쿼리 패킷을 제어하면 라우팅 루프 가능성이 줄어듭니다.

기본적으로 split horizon은 모든 인터페이스에서 활성화되어 있습니다.

Split horizon은 경로 정보를 해당 정보가 발생하는 인터페이스 밖의 라우터가 알릴 수 없도록 합니다. 이러한 행동은 일반적으로 특히 링크가 깨졌을 때 여러 라우팅 디바이스 간 통신을 최적화합니다. 하지만 비브로드캐스트 네트워크의 경우 이 행동이 필요하지 않은 상황이 있을 수 있습니다. 이 경우 EIGRP를 구성한 네트워크를 포함하여 split horizon을 비활성화할 수 있습니다.

인터페이스에서 split horizon을 비활성화하는 경우 해당 인터페이스의 모든 라우터와 액세스 서버에서 비활성화해야 합니다.

EIGRP split horizon을 비활성화하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Interfaces**를 선택합니다.

인터페이스 창이 나타나고 EIGRP 인터페이스 컨피그레이션을 표시합니다.

2단계 인터페이스 엔트리를 두 번 클릭하거나 엔트리를 클릭하고 **Edit**를 클릭합니다.

Edit EIGRP Interface Entry 대화 상자가 표시됩니다.

3단계 드롭다운 목록에서 EIGRP 라우팅 프로세스를 활성화했을 때 설정된 시스템 숫자로 채워진 EIGRP AS(Autonomous system) 번호를 선택합니다.

4단계 **Split Horizon** 확인란 선택을 취소합니다.

5단계 **OK**를 클릭합니다.

EIGRP 프로세스 재시작

EIGRP 프로세스를 다시 시작하거나 재배포 또는 카운터를 지우려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > EIGRP > Setup**을 선택합니다.

EIGRP 설정 창이 표시됩니다.

2단계 **Reset**을 클릭합니다.

EIGRP 모니터링

다음 명령을 사용하여 EIGRP 라우팅 프로세스를 모니터링할 수 있습니다. 명령 출력의 예와 설명은 명령 참조에서 참조하십시오. 또한 인접 디바이스 변경 메시지 및 인접 디바이스 경고 메시지의 로깅을 비활성화할 수 있습니다.

다양한 EIGRP 라우팅 통계를 모니터링하거나 비활성화하려면 다음 단계를 수행:

1단계 메인 ASDM 창에서 **Monitoring > Routing > EIGRP Neighbor**를 선택합니다.

각 행은 하나의 EIGRP 인접 디바이스를 나타냅니다. 각 인접 디바이스에 대해 목록은 IP 주소, 인접 디바이스가 연결된 인터페이스, 보류 시간, 가동 시간, 대기열 길이, 순서 번호, 완화된 왕복 시간, 재전송 시간 초과를 포함합니다. 가능한 상태 변경 목록은 다음과 같습니다.

- NEW ADJACENCY—새로운 인접 디바이스가 설정되었습니다.
- PEER RESTARTED—다른 인접 디바이스가 나머지 인접 디바이스 관계를 초기화합니다. 이 메시지를 받는 라우터가 인접 디바이스를 재설정하는 라우터가 아닙니다.
- HOLD TIME EXPIRED—라우터가 보류 시간 제한 내에 인접 디바이스로부터 EIGRP 패킷을 수신하지 못했습니다.
- RETRY LIMIT EXCEEDED—EIGRP가 EIGRP 신뢰 패킷에 대해 인접 디바이스로부터 확인을 받지 못했고 EIGRP가 이미 믿을 수 있는 패킷을 16회 전송하려 시도했으나 성공하지 못했습니다.
- ROUTE FILTER CHANGED—경로 필터 변경 사항이 있기 때문에 EIGRP 인접 디바이스가 재설정됩니다.
- INTERFACE DELAY CHANGED—인터페이스에서 지연 매개 변수의 수동 컨피그레이션 변경이 있기 때문에 EIGRP 인접 디바이스가 재설정됩니다.
- INTERFACE BANDWIDTH CHANGED—인터페이스에서 인터페이스 대역폭의 수동 컨피그레이션 변경이 있기 때문에 EIGRP 인접 디바이스가 재설정됩니다.
- STUCK IN ACTIVE— EIGRP가 활성 상태로 고정되었기 때문에 EIGRP 인접 디바이스가 재설정됩니다. 인접 디바이스가 재설정되는 것은 stuck-in-active 상태의 결과입니다.

2단계 모니터링할 EIGRP 인접 디바이스를 클릭합니다.

3단계 현재 인접 디바이스 목록을 제거하려면 **Clear Neighbors**를 클릭합니다.

4단계 현재 인접 디바이스 목록을 갱신하려면 **Refresh**를 클릭합니다.

참고 기본적으로 인접 디바이스 변경 및 경고 메시지는 로깅됩니다.

EIGRP 기능 내역

표 24-1에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 24-1 EIGRP 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
EIGRP 지원	7.0(1)	데이터 라우팅, 인증 수행, EIGRP(Enhanced Interior Gateway Routing Protocol)을 사용한 라우팅 정보 재배포 및 모니터링에 대한 지원이 추가되었습니다. 다음 화면을 도입했습니다. Configuration > Device Setup > Routing > EIGRP.
다중 컨텍스트 모드의 동적 라우팅	9.0(1)	EIGRP 라우팅이 다중 컨텍스트 모드에서 지원됩니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Routing > EIGRP > Setup.
클러스터링	9.0(1)	EIGRP의 경우 일괄 동기화, 경로 동기화 및 계층 2 로드 밸런싱은 클러스터링 환경에서 지원됩니다.
EIGRP Auto-Summary	9.2(1)	EIGRP의 경우, 이제 Auto-Summary 필드가 기본적으로 비활성화됩니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Routing > EIGRP > Setup > Edit EIGRP Process Advanced Properties

25 장

멀티캐스트 라우팅

이 장에서는 멀티캐스트 라우팅 프로토콜을 사용하도록 Cisco ASA을(를) 구성하는 방법을 설명합니다.

멀티캐스트 라우팅 정보

멀티캐스트 라우팅은 단일 정보 스트림을 수천 개의 기업 수신자와 가정으로 동시에 제공함으로써 트래픽을 줄이는 대역폭 절약 기술입니다. 멀티캐스트 라우팅을 활용하는 분야로는 화상 회의, 기업 통신, 원거리 학습, 소프트웨어 배포, 주식 시세 및 뉴스가 있습니다.

멀티캐스트 라우팅 프로토콜은 소스나 수신자에 추가적인 부담을 주지 않고 경쟁 기술 중에서도 가장 적은 네트워크 대역폭을 사용하여 소스 트래픽을 여러 수신자에게 보냅니다. 멀티캐스트 패킷은 PIM(Protocol Independent Multicast) 및 기타 지원 멀티캐스트프로토콜이 지원하는 Cisco 라우터에 의해 네트워크에서 복제되어 여러 수신자에게 데이터를 가장 효율적으로 제공할 수 있게 됩니다.

ASA은(는) stub 멀티캐스트 라우팅과 PIM 멀티캐스트 라우팅을 모두 지원합니다. 하지만 두 라우팅을 하나의 ASA에 동시에 구성할 수는 없습니다.

참고 멀티캐스트 라우팅에 대해 UDP 및 비 UDP 전송이 모두 지원됩니다. 그러나 비 UDP 전송에는 FastPath 최적화가 없습니다.

Stub 멀티캐스트 라우팅

Stub 멀티캐스트 라우팅은 동적 호스트 등록을 제공하고 멀티캐스트 라우팅을 촉진합니다. stub 멀티캐스트 라우팅에 대해 구성된 경우 ASA은(는) IGMP 프록시 에이전트 역할을 합니다. 멀티캐스트 라우팅에 완전히 참여하는 대신 ASA은(는) IGMP 메시지를 업스트림 멀티캐스트 라우터로 전송하고 이 라우터가 멀티캐스트 데이터 전송을 설정합니다. stub 멀티캐스트 라우팅에 대해 구성된 경우 ASA은(는) PIM에 대해 구성될 수 없습니다.

ASA은(는) PIM-SM과 양방향 PIM을 모두 지원합니다. PIM-SM은 기본 유니캐스트 라우팅 정보 기반 또는 별도의 멀티캐스트 지원 라우팅 정보 기반을 사용하는 멀티캐스트 라우팅 프로토콜입니다. 멀티캐스트 그룹당 단일 Rendezvous Point를 루트로 삼는 단방향 공유 트리를 구축하고 선택적으로 멀티캐스트 소스별로 최단 경로 트리를 생성합니다.

PIM 멀티캐스트 라우팅

양방향 PIM은 멀티캐스트 소스와 수신자를 연결하는 양방향 공유 트리를 구축하는 PIM-SM의 변형입니다. 양방향 트리는 멀티캐스트 토폴로지의 각 링크에서 작동하는 DF 선택 프로세스를 사용하여 구축됩니다. 멀티캐스트 데이터는 DF의 도움을 받아 소스에서 Rendezvous Point로 전달되고 따라서 소스별 상태 없이도 공유 트리에서 수신자를 따르게 됩니다. DF 선택은 Rendezvous Point 검색 중에 이루어지고 Rendezvous Point에 대한 기본 경로를 제공합니다.

참고 ASA이(가) PIM Rendezvous Point인 경우 ASA의 번역되지 않은 외부 주소를 Rendezvous Point 주소로 사용하십시오.

멀티캐스트 그룹 개념

멀티캐스트는 그룹 개념을 기반으로 합니다. 임의의 수신자 그룹이 특정 데이터 스트림 수신에 관심을 표현합니다. 이 그룹은 물리적 또는 지리적 경계가 없이 호스트가 인터넷의 어디에나 위치할 수 있습니다. 특정 그룹으로 향하는 데이터 수신에 관심이 있는 호스트는 IGMP를 사용하여 그룹에 참여해야 합니다. 호스트가 그룹의 일원이어야만 데이터 스트림을 받을 수 있습니다. 멀티캐스트 그룹 구성에 관한 정보는 25-14 페이지의 멀티캐스트 그룹 구성을(를) 참조하십시오.

멀티캐스트 주소

멀티캐스트 주소는 그룹에 참여하고 이 그룹으로 전송된 트래픽을 수신하고자 하는 임의의 IP 호스트 그룹입니다.

클러스터링

멀티캐스트 라우팅은 클러스터링을 지원합니다. 레이어 2 클러스터링에서는 fast-path 전달이 설정될 때까지 마스터 유닛이 모든 멀티캐스트 라우팅 패킷과 데이터 패킷을 전송합니다. fast-path 전달이 설정된 후에는 슬레이브 유닛이 멀티캐스트 데이터 패킷을 전송할 수 있습니다. 모든 데이터 흐름은 완전한 흐름입니다. Stub 전달 흐름도 지원됩니다. 레이어 2 클러스터링에서는 하나의 유닛만 멀티캐스트 패킷을 받기 때문에 마스터 유닛으로의 리디렉션이 일반적입니다. 레이어 3 클러스터링에서는 유닛이 독립적으로 작동하지 않습니다. 모든 데이터 및 라우팅 패킷은 마스터 유닛에 의해 처리 및 전달됩니다. 슬레이브 유닛은 전송된 모든 패킷을 삭제합니다.

클러스터링에 대한 자세한 내용은 9 장, “ASA 클러스터”.을(를) 참고하십시오.

멀티캐스트 라우팅을 위한 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 컨텍스트 모드에서 지원됩니다. 다중 컨텍스트 모드에서 미공유 인터페이스와 공유 인터페이스는 지원되지 않습니다.

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다. 투명한 방화벽 모드는 지원되지 않습니다.

IPv6 지침

IPv6를 지원하지 않습니다.

추가 지침

클러스터링에서는 IGMP 및 PIM에 대해 이 기능은 마스터 유닛에서만 지원됩니다.

멀티캐스트 라우팅 활성화

멀티캐스트 라우팅을 활성화하면 ASA에서 멀티캐스트 라우팅을 사용할 수 있습니다. 멀티캐스트 라우팅을 활성화하면 모든 인터페이스에서 기본적으로 IGMP 및 PIM이 활성화됩니다. IGMP는 그룹에서 어떤 멤버가 직접 연결된 서브넷에 존재하는지 학습하는 데 사용됩니다. 호스트는 IGMP 보고 메시지를 전송함으로써 멀티캐스트 그룹에 참여합니다. PIM은 멀티캐스트 데이터 그램을 전달하기 위한 전달 테이블 유지에 사용됩니다.

참고 멀티캐스트 라우팅에 대해서는 UDP 전송 레이어만 지원됩니다.

멀티캐스트 라우팅을 활성화하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast**를 선택합니다.

2단계 Multicast 창에서 **Enable Multicast** 라우팅 확인란을 선택합니다.

이 확인란을 선택하면 ASA에서 IP 멀티캐스트 라우팅이 활성화됩니다. 이 확인란 선택을 취소하면 IP 멀티캐스트 라우팅이 비활성화됩니다. 기본적으로 멀티캐스트는 비활성화되어 있습니다. 멀티캐스트 라우팅을 활성화하면 모든 인터페이스에서 멀티캐스트가 활성화됩니다. 인터페이스별로 멀티캐스트를 비활성화할 수 있습니다.

표 25-1은(는) ASA의 RAM을 기준으로 특정 멀티캐스트 테이블에 대한 최대 엔트리 개수를 열거합니다. 이 제한에 도달하면 새로운 엔트리가 삭제됩니다.

표 25-1 멀티캐스트 테이블 엔트리 제한

표	16MB	128MB	128MB 이상
MFIB	1000	3000	30000
IGMP 그룹	1000	3000	30000
PIM 경로	3000	7000	72000

멀티캐스트 라우팅 사용자 정의

이 섹션에서는 멀티캐스트 라우팅을 사용자 정의하는 방법을 설명합니다.

Stub 멀티캐스트 라우팅 구성 및 IGMP 메시지 전달

참고 Stub 멀티캐스트 라우팅 및 PIM은 동시에 지원되지 않습니다.

stub 영역으로의 게이트웨이 역할을 하는 ASA은(는) PIM에 참여할 필요가 없습니다. 대신 IGMP 프록시 에이전트 역할을 하고 IGMP 메시지를 하나의 인터페이스에 연결된 호스트에서 다른 인터페이스에 연결된 업스트림 멀티캐스트 라우터로 전달하도록 구성할 수 있습니다. IGMP 프록시 에이전트로 ASA을(를) 구성하려면 호스트 참가를 전달하고 stub 영역 인터페이스에서 업스트림 인터페이스로 메시지를 남깁니다.

호스트 참가를 전달하고 메시지를 남기려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast**를 선택합니다.

2단계 Multicast 창에서 **Enable Multicast** 라우팅 확인란을 선택합니다.

3단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

4단계 **Configuration > Device Setup > Routing > Multicast > IGMP > Protocol**을 선택합니다.

5단계 IGMP 메시지를 전달할 특정 인터페이스를 수정하려면 인터페이스를 선택하고 **Edit**를 클릭합니다.

Configure IGMP Parameters 대화 상자가 나타납니다.

6단계 **Forward Interface** 드롭다운 목록에서 IGMP 메시지를 전달할 특정 인터페이스를 선택합니다.

7단계 **OK**를 클릭하여 대화 상자를 닫고 **Apply**를 클릭하여 변경 사항을 저장합니다.

Static Multicast Route 구성

고정 멀티캐스트 경로를 구성함으로써 유니캐스트 트래픽에서 멀티캐스트 트래픽을 분리할 수 있습니다. 예를 들어 소스와 대상 사이의 경로가 멀티캐스트 라우팅을 지원하지 않을 경우 해결책은 두 멀티캐스트 디바이스 사이에 GRE 터널을 구성하여 멀티캐스트 패킷을 터널을 통해 전송하는 것입니다.

PIM을 사용하는 경우 ASA은(는) 유니캐스트 패킷을 다시 소스로 보내는 인터페이스와 같은 인터페이스에서 패킷을 수신할 것으로 기대합니다. 멀티캐스트 라우팅을 지원하지 않는 경로를 바이패스할 때와 같이 일부 경우에서는 유니캐스트 패킷이 하나의 경로를 따르고 멀티캐스트 패킷이 다른 경로를 따르도록 할 수 있습니다.

고정 멀티캐스트 경로가 알려지거나 재배포되지 않습니다.

고정 멀티캐스트 경로 또는 stub 영역에 대한 고정 멀티캐스트 경로를 구성하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > MRoute**를 선택합니다.

2단계 **Add** 또는 **Edit**를 선택합니다.

Add or Edit Multicast Route 대화 상자가 나타납니다.

Add Multicast Route 대화 상자를 사용하여 새로운 고정 멀티캐스트 경로를 ASA에 추가합니다. Edit Multicast Route 대화 상자를 사용하여 기존 고정 멀티캐스트 경로를 변경합니다.

3단계 Source Address 필드에 멀티캐스트 소스의 IP 주소를 입력합니다. 기존 고정 멀티캐스트 경로를 편집할 때는 이 값을 변경할 수 없습니다.

4단계 Source Mask 드롭다운 목록에서 멀티캐스트 소스의 IP 주소에 대한 네트워크 마스크를 선택합니다.

5단계 Incoming Interface 영역에서 **RPF Interface** 라디오 버튼을 클릭하여 경로를 전달할 RPF를 선택하거나 **Interface Name** 라디오 버튼을 클릭한 후 다음을 입력합니다.

- Source Interface 필드의 드롭다운 목록에서 멀티캐스트 경로에 대한 수신 인터페이스를 선택합니다.
- Destination Interface 필드의 드롭다운 목록에서 경로가 전달되는 대상 인터페이스를 선택합니다.

참고 인터페이스 또는 RPF 인접 디바이스를 지정할 수 있지만 동시에 둘 다 지정할 수는 없습니다.

6단계 Administrative Distance 필드에서 고정 멀티캐스트 경로의 관리 거리를 선택합니다. 고정 멀티캐스트 경로가 유니캐스트 경로와 관리 거리가 같은 경우 고정 멀티캐스트 경로가 우선합니다.

7단계 **OK**를 클릭합니다.

IGMP 기능 구성

IP 호스트가 IGMP(Internet Group Management Protocol)를 사용하여 그룹 멤버십을 직접 연결된 멀티캐스트 라우터로 보고합니다.

IGMP는 특정 LAN의 멀티캐스트 그룹에서 개별 호스트를 동적으로 등록하는 데 사용됩니다. 호스트는 IGMP 메시지를 로컬 멀티캐스트 라우터로 전송함으로써 그룹 멤버십을 식별합니다. IGMP에서 라우터가 IGMP 메시지를 듣고 주기적으로 쿼리를 보내 특정 서브넷에서 어떤 그룹이 활성 상태이고 어떤 그룹이 비활성 상태인지 파악합니다.

IGMP는 그룹 주소(Class D IP 주소)를 그룹 식별자로 사용합니다. 호스트 그룹 주소 범위는 224.0.0.0~239.255.255.255입니다. 224.0.0.0 주소는 어떤 그룹에도 할당되지 않습니다. 224.0.0.1 주소는 서브넷의 모든 시스템에 할당됩니다. 224.0.0.2 주소는 서브넷의 모든 라우터에 할당됩니다.

ASA에서 멀티캐스트 라우팅을 활성화할 경우 IGMP 버전 2가 모든 인터페이스에서 자동으로 활성화됩니다.

참고 **show run** 명령을 사용할 경우 인터페이스 컨피그레이션에 **no igmp** 명령만 표시됩니다. 디바이스 컨피그레이션에 **multicast-routing** 명령이 나타날 경우 IGMP가 자동으로 모든 인터페이스에서 활성화됩니다.

이 섹션은 인터페이스별로 선택적인 IGMP 설정을 구성하는 방법을 설명합니다.

인터페이스에서 IGMP 비활성화

특정 인터페이스에서 IGMP를 비활성화할 수 있습니다. 이 정보는 특정 인터페이스에 멀티캐스트 호스트가 없음을 알고 있고 ASA이(가) 해당 인터페이스로 호스트 쿼리 메시지를 보내는 것을 막고 싶을 때 유용합니다.

인터페이스에서 IGMP를 비활성화하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > IGMP > Protocol**을 선택합니다.

Protocol 창에 ASA의 각 인터페이스에 대한 IGMP 매개변수가 표시됩니다.

2단계 비활성화할 인터페이스를 선택하고 **Edit**를 클릭합니다.

3단계 지정된 인터페이스를 비활성화하려면 **Enable IGMP** 확인란 선택을 취소합니다.

4단계 **OK**를 클릭합니다.

Protocol 창은 IGMP가 인터페이스에서 활성화된 경우 Yes를 표시하고 비활성화된 경우 No를 표시합니다.

IGMP 그룹 멤버십 구성

ASA을(를) 멀티캐스트 그룹의 멤버로 구성할 수 있습니다. ASA을(를) 멀티캐스트 그룹에 참여하도록 구성하면 업스트림 라우터가 해당 그룹에 대한 멀티캐스트 라우팅 테이블 정보를 유지하고 해당 그룹에 대한 경로를 활성 상태로 유지하게 됩니다.

참고 특정 그룹에 대한 멀티캐스트 패킷을 인터페이스로 전달하면서 ASA이(가) 패킷을 해당 그룹의 일부로 수락하지 않도록 하려면 25-7 페이지의 고정 참여 IGMP 그룹 구성을(를) 참조하십시오.

ASA이(가) 멀티캐스트 그룹에 참여하도록 하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > IGMP > Join Group**을 선택합니다.

Join Group 창이 표시됩니다.

2단계 **Add** 또는 **Edit**를 클릭합니다.

Add IGMP Join Group 대화 상자를 통해 인터페이스를 멀티캐스트 그룹의 멤버로 구성할 수 있습니다. Edit IGMP Join Group 대화 상자를 통해 기존 멤버십 정보를 수정할 수 있습니다.

3단계 Interface Name 필드의 드롭다운 목록에서 인터페이스 이름을 선택합니다. 기존 엔트리를 편집할 경우 이 값을 변경할 수 없습니다.

4단계 Multicast Group Address 필드에 인터페이스가 속하는 멀티캐스트 그룹의 주소를 입력합니다. 유효한 그룹 주소는 224.0.0.0~ 239.255.255.255입니다.

5단계 **OK**를 클릭합니다.

고정 참여 IGMP 그룹 구성

때로는 일부 컨피그레이션으로 인해 또는 네트워크 세그먼트의 그룹에 멤버가 없기 때문에 그룹 멤버가 멤버십을 보고할 수 없는 경우도 있습니다. 하지만 해당 네트워크 세그먼트로 여전히 해당 그룹에 대한 멀티캐스트 트래픽을 보내려고 합니다. 고정 참여 IGMP 그룹을 구성하면 해당 그룹에 대한 멀티캐스트 트래픽을 해당 세그먼트로 보낼 수 있습니다.

메인 ASDM 창에서 **Configuration > Routing > Multicast > IGMP > Static Group**을 선택하여 ASA을(를) 고정으로 연결된 그룹 멤버로 구성합니다. 이 방법을 통해 ASA은(는) 패킷 자체를 수신하지 않고 전달만 합니다. 따라서 빠른 전환이 가능합니다. 발신 인터페이스는 IGMP 캐시에 나타나지만 이 인터페이스는 멀티캐스트 그룹의 멤버가 아닙니다.

인터페이스의 고정 연결 멀티캐스트 그룹을 구성하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > IGMP > Static Group**을 선택합니다.

Static Group 창이 표시됩니다.

2단계 **Add** 또는 **Edit**를 클릭합니다.

Add IGMP Static Group 대화 상자를 이용하여 멀티캐스트 그룹을 고정으로 인터페이스에 할당합니다. Edit IGMP Static Group 대화 상자를 이용하여 기존 고정 그룹 할당을 변경합니다.

3단계 Interface Name 필드의 드롭다운 목록에서 인터페이스 이름을 선택합니다. 기존 엔트리를 편집할 경우 이 값을 변경할 수 없습니다.

4단계 Multicast Group Address 필드에 인터페이스가 속하는 멀티캐스트 그룹의 주소를 입력합니다. 유효한 그룹 주소는 224.0.0.0~ 239.255.255.255입니다.

5단계 **OK**를 클릭합니다.

멀티캐스트 그룹에 대한 액세스 제어

ASA 인터페이스의 호스트가 참여할 수 있는 멀티캐스트 그룹을 제어하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > IGMP > Access Group**을 선택합니다.

Access Group 창이 표시됩니다. Access Group 창의 테이블 엔트리는 위에서 아래로 처리됩니다. 테이블 위쪽으로는 보다 구체적인 엔트리를, 아래쪽으로는 보다 일반적인 엔트리를 더 많이 배치합니다. 예를 들어 특정 멀티캐스트 그룹을 허용하는 액세스 그룹 엔트리는 테이블 위쪽에 배치하고 허용 규칙의 그룹을 포함하여 멀티캐스트 그룹의 범위를 거부하는 액세스 그룹 엔트리는 그 아래에 배치합니다. 허용 규칙이 거부 규칙보다 먼저 적용되므로 그룹이 허용됩니다.

테이블의 테이블을 두 번 클릭하면 선택한 엔트리에 대한 Add or Edit Access Group 대화 상자가 열립니다.

2단계 **Add** 또는 **Edit**를 클릭합니다.

Add Access Group 또는 Edit Access Group 대화 상자가 나타납니다. Add Access Group 대화 상자를 통해 새로운 액세스 그룹을 Access Group Table에 추가할 수 있습니다. Edit Access Group 대화 상자를 통해 기존 액세스 그룹 엔트리에 대한 정보를 수정할 수 있습니다. 기존 엔트리를 수정할 때 일부 필드가 흐리게 표시됩니다.

3단계 Interface 드롭다운 목록에서 액세스 그룹이 연결된 인터페이스 이름을 선택합니다. 기존 액세스 그룹을 편집할 때는 연결된 인터페이스를 변경할 수 없습니다.

4단계 Action 드롭다운 목록에서 허용을 선택하여 선택된 인터페이스에서 멀티캐스트 그룹을 허용합니다. Action 드롭다운 목록에서 거부를 선택하여 선택된 인터페이스에서 멀티캐스트 그룹을 필터링합니다.

5단계 Multicast Group Address 필드에 액세스 그룹이 적용되는 멀티캐스트 그룹의 주소를 입력합니다.

6단계 멀티캐스트 그룹 주소에 대한 네트워크 마스크를 입력하거나 Netmask 드롭다운 목록에서 공통 네트워크 마스크 중 하나를 선택합니다.

7단계 **OK**를 클릭합니다.

인터페이스에서 IGMP 상태의 개수 제한

인터페이스별로 IGMP 멤버십 보고에서 비롯되는 IGMP 멤버십 상태의 수를 제한할 수 있습니다. 구성된 제한을 초과하는 멤버십 보고는 IGMP 캐시에 입력되지 않고 초과된 멤버십 보고에 대한 트래픽은 전달되지 않습니다.

인터페이스에서 IGMP 상태의 수를 제한하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > IGMP > Protocol**을 선택합니다.

2단계 Protocol 창의 테이블에서 제한하려는 인터페이스를 선택하고 **Edit**를 클릭합니다.

Configure IGMP Parameters 대화 상자가 나타납니다.

3단계 Group Limit 필드에 인터페이스에서 연결할 수 있는 호스트의 최대 수를 입력합니다. 유효한 값 범위는 0~500입니다. 기본값은 500입니다. 이 값을 0으로 설정하면 학습된 그룹이 추가되지 않지만 수동으로 정의한 멤버십은 여전히 허용됩니다.

4단계 **OK**를 클릭합니다.

멀티캐스트 그룹으로의 쿼리 메시지 수정

ASA은(는) 쿼리 메시지를 보내 어떤 멀티캐스트 그룹이 인터페이스에 연결된 네트워크의 멤버인지 확인합니다. 멤버는 특정 그룹에 대한 멀티캐스트 패킷을 받고 싶다는 의미의 IGMP 보고 메시지로 응답합니다. 쿼리 메시지는 주소가 224.0.0.1이고 time-to-live 값이 1인 전체 시스템 멀티캐스트 그룹으로 전달됩니다.

이 메시지는 주기적으로 전송되어 ASA에 저장된 멤버십 정보를 새로 고침합니다. ASA이(가) 아직 인터페이스에 연결된 멀티캐스트 그룹의 로컬 멤버가 없다고 확인하면 해당 그룹의 멀티캐스트 패킷을 연결된 네트워크로 더 이상 전달하지 않고 prune 메시지를 다시 패킷 소스로 전송합니다.

기본적으로 서브넷의 PIM 지정 라우터가 쿼리 메시지 전송을 담당합니다. 기본적으로 125초마다 한 번 전송됩니다.

쿼리 응답 시간을 변경할 경우 IGMP 쿼리에서 알려지는 최대 쿼리 응답 시간은 기본적으로 10초입니다. 이 시간 안에 ASA이(가) 호스트 쿼리에 대한 응답을 받지 못하면 그 그룹이 삭제됩니다.

쿼리 간격, 쿼리 응답 시간 및 쿼리 시간 초과 값을 변경하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > IGMP > Protocol**을 선택합니다.

2단계 Protocol 창의 테이블에서 제한하려는 인터페이스를 선택하고 **Edit**를 클릭합니다.

Configure IGMP Parameters 대화 상자가 나타납니다.

3단계 Query Interval 필드에서 지정된 라우터가 IGMP 호스트-쿼리 메시지를 보낼 간격을 초 단위로 입력합니다. 유효한 값의 범위는 1초~3600초입니다. 기본값은 125초입니다.

ASA이(가) 지정된 시간 초과 값 동안 쿼리 메시지를 받지 못하면 ASA이(가) 지정 라우터가 되고 쿼리 메시지 전송을 시작합니다.

4단계 Query Timeout 필드에서 이전 요청자가 역할을 중지한 후 ASA가 인터페이스의 요청자 역할을 대신하기 전까지의 시간을 초 단위로 입력합니다. 유효한 값은 60~300초입니다. 기본값은 255초입니다.

5단계 **OK**를 클릭합니다.

IGMP 버전 변경

기본적으로 ASA은(는) IGMP Version 2를 실행합니다.

서브넷의 모든 멀티캐스트 라우터는 같은 버전의 IGMP를 지원해야 합니다. ASA은(는) 자동으로 Version 1 라우터를 감지하고 Version 1로 전환하지 않습니다. 그러나 IGMP Version 1과 2 호스트를 서브넷에서 혼용할 수는 있습니다. ASA 실행 중인 IGMP 버전 2는 IGMP 버전 1 호스트가 있을 때에도 정상 작동합니다.

인터페이스에서 실행되는 IGMP 버전을 제어하려면다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > IGMP > Protocol**을 선택합니다.

2단계 Protocol 창의 테이블에서 IGMP 버전을 변경할 인터페이스를 선택하고 **Edit**를 클릭합니다.

Configure IGMP Interface 대화 상자가 나타납니다.

3단계 Version 드롭다운 목록에서 버전 번호를 선택합니다.

4단계 **OK**를 클릭합니다.

PIM 기능 구성

라우터는 PIM을 사용하여 멀티캐스트 다이어그램 전달을 위한 전달 테이블을 유지합니다. ASA에서 멀티캐스트 라우팅을 활성화할 경우 PIM 및 IGMP가 모든 인터페이스에서 자동으로 활성화됩니다.

참고 PIM은 PAT에서 지원되지 않습니다. PIM 프로토콜은 포트를 사용하지 않고 PAT는 포트를 사용하는 프로토콜에서만 작동합니다.

이 섹션은 선택적인 PIM 설정을 구성하는 방법을 설명합니다.

인터페이스에서 PIM 활성화 및 비활성화

특정 인터페이스에서 PIM을 활성화하거나 비활성화할 수 있습니다. 인터페이스에서 PIM을 활성화하거나 비활성화하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > PIM > Protocol**을 선택합니다.

2단계 Protocol 창의 테이블에서 PIM을 활성화하려는 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit PIM Protocol 대화 상자가 나타납니다.

3단계 **Enable PIM** 확인란을 선택합니다. PIM을 비활성화하려면 이 확인란 선택을 취소합니다.

4단계 **OK**를 클릭합니다.

고정 Rendezvous Point 주소 구성

일반 PIM sparse mode 또는 bidir 도메인을 가진 모든 라우터는 PIM RP 주소를 알아야 합니다. 이 주소는 **pim rp-address** 명령을 사용하여 고정으로 구성됩니다.

참고 ASA은(는) Auto-RP 또는 PIM BSR을 지원하지 않습니다

ASA이(가) 하나 이상의 그룹에 대해 RP 역할을 하도록 구성할 수 있습니다. ACL에 지정된 그룹 범위가 PIM RP 그룹 매핑을 결정합니다. ACL이 지정되지 않은 경우 해당 그룹에 대한 RP가 전체 멀티캐스트 그룹 범위(224.0.0.0/4)에 적용됩니다.

PIM PR의 주소를 구성하려면 다음 단계를 수행합니다.

참고 실제 양방향 컨피그레이션에 관계없이 ASA은(는) PIM hello 메시지에서 항상 양방향 기능을 알립니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > PIM > Rendezvous Points**를 선택합니다.

2단계 **Add** 또는 **Edit**를 클릭합니다.

Add or Edit Rendezvous Point 대화 상자가 나타납니다. Add Rendezvous Point 대화 상자를 통해 Rendezvous Point 테이블에 새로운 엔트리를 추가할 수 있습니다. Edit Rendezvous Point 대화 상자를 통해 기존 RP 엔트리를 변경할 수 있습니다. 또한 **Delete**를 클릭하여 선택한 멀티캐스트 그룹 엔트리를 테이블에서 삭제할 수 있습니다.

RP에는 다음 제한 사항이 적용됩니다.

- 동일한 RP 주소를 두 번 사용할 수 없습니다.
- 하나 이상의 RP에 All Groups를 지정할 수 없습니다.

3단계 Rendezvous Point Address 필드에 RP에 대한 IP 주소를 입력합니다.

기존 RP 엔트리를 편집하는 경우 이 값을 변경할 수 없습니다.

4단계 지정된 멀티캐스트 그룹이 양방향 모드에서 작동하는 경우 **Use bi-directional forwarding** 확인란을 선택하십시오. Rendezvous Point 창은 지정된 멀티캐스트 그룹이 양방향 모드에서 작동할 경우 Yes를 표시하고 sparse mode에서 작동할 경우 No를 표시합니다. 양방향 모드에서 ASA이(가) 멀티캐스트 패킷을 수신하고 직접 연결된 멤버나 PIM 인접 디바이스가 없는 경우 다시 소스로 prune 메시지를 보냅니다.

5단계 **Use this RP for All Multicast Groups** 라디오 버튼을 클릭항 인터페이스의 모든 멀티캐스트 그룹에 대해 지정된 RP를 사용하거나 **Use this RP for the Multicast Groups as specified below** 라디오 버튼을 사용하여 지정된 RP와 함께 사용할 멀티캐스트 그룹을 지정합니다.

멀티캐스트 그룹에 관한 자세한 정보는 25-14 페이지의 멀티캐스트 그룹 구성을(를) 참조하십시오.

6단계 **OK**를 클릭합니다.

지정된 라우터 우선순위 구성

DR은 PIM 등록, 참여 및 prune 메시지를 RP로 보내는 것을 담당합니다. 네트워크 세그먼트에 멀티캐스트 라우터가 하나 이상 있는 경우 DR 선택은 DR 우선순위를 따릅니다. 여러 디바이스의 DR 우선순위가 동일한 경우 IP 주소가 가장 높은 디바이스가 DR이 됩니다.

기본적으로 ASA의 DR 우선순위는 1입니다. 이 값을 변경하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > PIM > Protocol**을 선택합니다.

2단계 Protocol 창의 테이블에서 PIM을 활성화하려는 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit PIM Protocol 대화 상자가 나타납니다.

3단계 DR Priority 필드에 선택한 인터페이스에 대한 지정 라우터 우선순위 값을 입력합니다. 서브넷에서 DR 우선순위가 가장 높은 라우터가 지정 라우터가 됩니다. 유효한 값 범위는 0~4294967294입니다. 기본 DR 우선순위는 1입니다. 이 값을 0으로 설정하면 ASA 인터페이스가 기본 라우터가 될 자격을 잃게 됩니다.

4단계 **OK**를 클릭합니다.

PIM 레지스터 메시지 구성 및 필터링

ASA이(가) RP 역할을 수행하는 경우 특정 멀티캐스트 소스의 등록을 제한하여 권한이 없는 소스가 RP에 등록하지 못하도록 할 수 있습니다. Request Filter 창을 통해 ASA이(가) PIM 레지스터 메시지를 수락하는 멀티캐스트 소스를 정의할 수 있습니다.

PIM 레지스터 메시지를 필터링하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > PIM > Request Filter**를 선택합니다.

2단계 **Add**를 클릭합니다.

Request Filter Entry 대화 상자를 통해 ASA이(가) RP 역할을 할 때 ASA에 등록을 허용할 멀티캐스트 소스를 정의할 수 있습니다. 소스 IP 주소 및 대상 멀티캐스트 주소를 기준으로 필터 규칙을 생성할 수 있습니다.

3단계 Action 드롭다운 목록에서 Permit을 선택하여 지정된 멀티캐스트 트래픽의 지정된 소스를 ASA에 등록할 수 있도록 허용하는 규칙을 생성하거나 Deny를 선택하여 지정된 멀티캐스트 트래픽의 지정된 소스를 ASA에 등록할 수 없도록 하는 규칙을 생성합니다.

4단계 Source IP Address 필드에 레지스터 메시지의 소스에 대한 IP 주소를 입력합니다.

5단계 Source Netmask 필드에 레지스터 메시지의 소스에 대한 드롭다운 목록에서 네트워크 마스크를 입력하거나 선택합니다.

6단계 Destination IP Address 필드에 멀티캐스트 대상 주소를 입력합니다.

7단계 Destination Netmask 필드의 드롭다운 목록에서 멀티캐스트 대상 주소에 대한 네트워크 마스크를 입력하거나 선택합니다.

8단계 **OK**를 클릭합니다.

PIM 메시지 간격 구성

PIM DR 선택을 위해 라우터 쿼리 메시지가 사용될 수 있습니다. PIM DR은 라우터 쿼리 메시지 전송을 담당합니다. 기본적으로 라우터 쿼리 메시지는 30초마다 전송됩니다. 또한 ASA은(는) 60초마다 PIM 참여 또는 prune 메시지를 보냅니다.

이 간격을 변경하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > PIM > Protocol**을 선택합니다.

2단계 Protocol 창의 테이블에서 PIM을 활성화하려는 인터페이스를 선택하고 **Edit**를 클릭합니다.

Edit PIM Protocol 대화 상자가 나타납니다.

3단계 Hello Interval 필드에 인터페이스가 PIM hello 메시지를 전송하는 빈도를 초 단위로 입력합니다.

4단계 Prune Interval 필드에 인터페이스가 PIM 참여 및 prune 알림을 전송하는 빈도를 초 단위로 입력합니다.

5단계 **OK**를 클릭합니다.

경로 트리 구성

기본적으로 PIM 리프 라우터는 첫 번째 패킷이 새로운 소스에 도달한 직후 가장 짧은 경로의 트리에 참여합니다. 이 방법은 지연을 줄이지만 공유 트리보다 더 많은 메모리가 필요합니다. 모든 멀티캐스트 그룹에 대해 또는 특정 멀티캐스트 주소에 한정하여 ASA이(가) 최단 경로 트리에 참여할지 아니면 공유 트리를 사용할지 구성할 수 있습니다.

PIM 리프 라우터 트리를 구성하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > PIM > Route Tree**를 선택합니다.

2단계 다음 라디오 버튼 중 하나를 클릭합니다.

- **Use Shortest Path Tree for All Groups**—모든 멀티캐스트 그룹에 대해 최단 경로 트리를 사용하려면 이 옵션을 선택합니다.
- **Use Shared Tree for All Groups**—모든 멀티캐스트 그룹에 대해 공유 트리를 사용하려면 이 옵션을 선택합니다.
- **Use Shared Tree for the Groups specified below**—Multicast Groups 테이블에 지정된 그룹에 대해 공유 트리를 사용하려면 이 옵션을 선택합니다. Multicast Groups 테이블에 지정되지 않은 그룹에 대해서는 최단 경로 트리가 사용됩니다.

  Multicast Groups 테이블은 공유 트리를 사용할 멀티캐스트 그룹을 표시합니다.

  테이블 엔트리는 위에서 아래로 처리됩니다. 특정 그룹에 대한 거부 규칙을 테이블 상단에 배치하고 멀티캐스트 그룹 범위에 대한 허용 규칙을 거부 구문 아래에 배치하면 일정한 범위의 멀티캐스트 그룹을 포함하되 해당 범위 내 특정 그룹을 제외하는 엔트리를 만들 수 있습니다.

  멀티캐스트 그룹을 편집하려면 25-14 페이지의 멀티캐스트 그룹 구성을 참조하십시오.

멀티캐스트 그룹 구성

멀티캐스트 그룹은 어떤 멀티캐스트 주소가 그룹의 일부인지 정의하는 액세스 규칙의 목록입니다. 멀티캐스트 그룹은 단일 멀티캐스트 주소 또는 특정 범위의 멀티캐스트 주소를 포함할 수 있습니다. Add Multicast Group 대화 상자를 사용하여 새로운 멀티캐스트 그룹 규칙을 생성하십시오. 기존 멀티캐스트 그룹 규칙을 수정하려면 Edit Multicast Group 대화 상자를 사용하십시오.

멀티캐스트 그룹을 구성하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > PIM > Rendezvous Points**를 선택합니다.

2단계 Rendezvous Point 창이 나타납니다. 구성할 그룹을 클릭합니다.

Edit Rendezvous Point 대화 상자가 나타납니다.

3단계 **Use this RP for the Multicast Groups as specified below** 라디오 버튼을 클릭하여 지정된 RP와 함께 사용할 멀티캐스트 그룹을 지정합니다.

4단계 **Add** 또는 **Edit**를 클릭합니다.

Add or Edit Multicast Group 대화 상자가 나타납니다.

5단계 Action 드롭다운 목록에서 Permit을 선택하여 지정된 멀티캐스트 주소를 허용하는 그룹 규칙을 생성하거나 Deny를 선택하여 지정된 멀티캐스트 주소를 필터링하는 그룹 규칙을 생성합니다.

6단계 Multicast Group Address 필드에서 그룹과 연결된 멀티캐스트 주소를 입력합니다.

7단계 Netmask 드롭다운 목록에서 멀티캐스트 그룹 주소에 대한 네트워크 마스크를 선택합니다.

8단계 **OK**를 클릭합니다.

PIM 인접 디바이스 필터링

PIM 인접 디바이스가 될 수 있는 라우터를 정의할 수 있습니다. PIM 인접 디바이스가 될 수 있는 라우터를 필터링함으로써 다음을 할 수 있습니다.

- 권한이 없는 라우터가 PIM 인접 디바이스가 되는 것을 막습니다.
- 연결된 stub 라우터가 PIM에 참여하는 것을 막습니다.

PIM 인접 디바이스가 될 수 있는 인접 디바이스를 정의하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > PIM > Neighbor Filter**를 선택합니다.

2단계 **Add/Edit/Insert**를 클릭하여 테이블에서 구성할 PIM 인접 디바이스를 선택합니다.

Add/Edit/Insert Neighbor Filter Entry 대화 상자가 표시됩니다. Add/Edit/Insert Neighbor Filter Entry 대화 상자를 통해 멀티캐스트 경계 ACL에 대한 ACL 엔트리를 만들 수 있습니다. 선택한 PIM 인접 디바이스 엔트리를 삭제할 수도 있습니다.

3단계 Interface Name 드롭다운 목록에서 인터페이스 이름을 선택합니다.

4단계 Action 드롭다운 목록에서 인접 디바이스 필터 ACL 엔트리에 대한 Permit 또는 Deny를 선택합니다.

Permit을 선택하면 멀티캐스트 그룹 알림이 인터페이스를 통과하게 됩니다. Deny를 선택하면 지정된 멀티캐스트 그룹 알림이 인터페이스를 통과할 수 없습니다. 인터페이스에서 멀티캐스트 경계가 구성된 경우 모든 멀티캐스트 트래픽은 인접 디바이스 필터 엔트리로 허용되지 않는 한 인터페이스를 통과할 수 없습니다.

5단계 IP Address 텍스트 필드에 허용 또는 거부되는 멀티캐스트 PIM 그룹의 IP 주소를 입력합니다. 유효한 그룹 주소는 Valid 224.0.0.0~239.255.255.255.255입니다.

6단계 Netmask 드롭다운 목록에서 멀티캐스트 그룹 주소에 대한 넷마스크를 선택합니다.

7단계 **OK**를 클릭합니다.

양방향 인접 필터 구성

Bidirectional Neighbor Filter 창은 ASA에 구성된 PIM 양방향 인접 필터를 보여줍니다. PIM 양방향 인접 디바이스 필터는 인접 디바이스가 DF 선택에 참여할 수 있다고 정의하는 ACL입니다. 인터페이스에 대해 PIM 양방향 인접 디바이스 필터가 구성되지 않은 경우에는 제한 사항이 없습니다. PIM 양방향 인접 디바이스 필터가 구성된 경우 ACL에서 허용된 인접 디바이스만 DF 선택 프로세스에 참여할 수 있습니다.

PIM 양방향 인접 필터 컨피그레이션이 ASA에 적용된 경우 ACL이 *interface-name*_multicast라는 이름으로 실행 중인 컨피그레이션에 표시되며 *interface-name*은 멀티캐스트 경계 필터가 적용되는 인터페이스의 이름입니다. 이 이름의 ACL이 이미 존재하는 경우 이름 앞에 숫자가 추가됩니다(예: inside_multicast_1). 이 ACL은 ASA의 PIM 인접 디바이스가 될 수 있는 디바이스를 정의합니다.

양방향 PIM은 멀티캐스트 라우터가 축소된 상태 정보를 유지할 수 있게 합니다. 세그먼트의 모든 멀티캐스트 라우터가 bidir에 대해 양방향으로 활성화되어 있어야 DF를 선택할 수 있습니다.

PIM 양방향 인접 디바이스 필터는 DF 선택에 참여할 라우터 지정을 허용하는 동시에 모든 라우터가 sparse-mode 도메인에 참여할 수 있게 함으로써 sparse-mode-only 네트워크에서 bidir 네트워크로의 전환을 가능하게 합니다. bidir-enabled 라우터는 bidir 라우터가 세그먼트에 없어도 자기들 끼리 DF를 선택할 수 있습니다. non-bidir 라우터의 멀티캐스트 경계는 bidir 그룹의 PIM 메시지 및 데이터가 bidir 그룹이나 bidir 서브셋 클라우드에서 유출되지 않도록 합니다.

PIM 양방향 인접 디바이스 필터가 활성화된 경우 ACL에 의해 허용된 라우터는 양방향을 지원하는 것으로 간주됩니다. 따라서 다음은 참입니다.

- 허용된 인접 디바이스가 bidir을 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 인접ㅈ 장치가 bidir을 지원할 경우 DF 선택이 일어나지 않습니다.
- 거부된 인접 디바이스가 bidir을 지원하지 않을 경우 DF 선택이 일어날 수 있습니다.

PIM 양방향 인접 디바이스 필터가 될 수 있는 인접 디바이스를 정의하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > PIM > Bidirectional Neighbor Filter**를 선택합니다.

2단계 PIM Bidirectional Neighbor Filter 테이블에서 엔트리를 두 번 클릭하여 해당 엔트리에 대한 Edit Bidirectional Neighbor Filter Entry 대화 상자를 엽니다.

3단계 **Add/Edit/Insert**를 클릭하여 테이블에서 구성할 PIM 인접 디바이스를 선택합니다.

Add/Edit/Insert Bidirectional Neighbor Filter Entry 대화 상자가 표시되어 PIM 양방향 인접 디바이스 필터 ACL에 대한 ACL 엔트리를 생성할 수 있습니다.

4단계 Interface Name 드롭다운 목록에서 인터페이스 이름을 선택합니다. PIM 양방향 인접 디바이스 필터 ACL 엔트리를 구성할 인터페이스를 선택합니다.

5단계 Action 드롭다운 목록에서 인접 디바이스 필터 ACL 엔트리에 대한 Permit 또는 Deny를 선택합니다.

Permit을 클릭하여 지정된 디바이스가 DF 선택 프로세스에 참여할 수 있도록 합니다. Deny를 선택하여 지정된 디바이스가 DF 선택 프로세스에 참여할 수 없게 합니다.

6단계 IP Address 텍스트 필드에 허용 또는 거부되는 멀티캐스트 PIM 그룹의 IP 주소를 입력합니다. 유효한 그룹 주소는 Valid 224.0.0.0~239.255.255.255.255입니다.

7단계 Netmask 드롭다운 목록에서 멀티캐스트 그룹 주소에 대한 넷마스크를 선택합니다.

8단계 **OK**를 클릭합니다.

멀티캐스트 경계 구성

주소 범위 지정은 도메인 경계를 정의하여 같은 IP 주소를 가진 RP 도메인이 서로 섞이지 않도록 합니다. 범위 지정은 대형 도메인 내 서브넷 경계와 도메인과 인터넷 사이의 경계에서 이루어집니다.

choosing **Configuration > Routing > Multicast > MBoundary** in ASDM를 선택하여 멀티캐스트 그룹 주소에 대한 인터페이스에서 관리적으로 범위가 지정된 경계를 설정할 수 있습니다. IANA는 관리적으로 범위가 지정된 주소로 239.0.0.0~239.255.255.255의 멀티캐스트 주소 범위를 지정했습니다. 이 주소 범위는 다른 조직이 관리하는 도메인에서 재사용될 수 있습니다. 주소는 고유한 글로벌 값이 아니라 로컬로 간주됩니다.

표준 ACL은 영향을 받는 주소의 범위를 정의합니다. 경계를 설정할 때 어느 방향으로도 경계를 건너는 멀티캐스트 데이터 패킷 흐름은 허용되지 않습니다. 경계를 통해 동일한 멀티캐스트 그룹 주소를 다른 관리 도메인에서 재사용할 수 있습니다.

를 입력하면 Auto-RP 검색 및 알림 메시지를 관리적으로 범위가 지정된 경계에서 구성, 검사 및 필터링할 수 있습니다. 경계 ACL에 의해 거부된 Auto-RP 패킷의 모든 Auto-RP 패킷 그룹 범위 알림은 삭제됩니다. Auto-RP 그룹 범위 알림은 Auto-RP 그룹 범위의 모든 주소가 경계 ACL에 의해 허용된 경우에만 경계에서 허용 및 통과됩니다. 주소가 하나라도 허용되지 않은 경우 전체 그룹 범위가 필터링되고 Auto-RP 메시지가 전달되기 전에 Auto-RP 메시지에서 삭제됩니다.

멀티캐스트 경계를 구성하려면 다음 단계를 수행합니다.

1단계 메인 ASDM 창에서 **Configuration > Routing > Multicast > MBoundary**를 선택합니다.

MBoundary 창을 통해 관리적으로 범위가 지정된 멀티캐스트 주소에 대한 멀티캐스트 경계를 구성할 수 있습니다. 멀티캐스트 경계는 멀티캐스트 데이터 패킷 흐름을 제한하고 동일한 멀티캐스트 그룹 주소를 다른 관리 도메인에서 재사용할 수 있게 합니다. 인터페이스에서 특정 멀티캐스트 경계가 정의된 경우 필터 ACL에 의해 허용된 멀티캐스트 트래픽만 인터페이스를 통과합니다.

2단계 **Edit**를 클릭합니다.

Edit Boundary Filter 대화 상자가 나타나고 멀티캐스트 경계 필터 ACL을 표시합니다. 이 대화 상자를 통해 경계 필터 ACL 엔트리를 추가하고 삭제할 수 있습니다.

ASA에 경계 필터 컨피그레이션이 적용되면 ACL이 실행 중인 컨피그레이션에 *interface-name*_multicast라는 이름으로 나타나고 여기서 *interface-name*은 멀티캐스트 경계 필터가 적용되는 인터페이스의 이름입니다. 이 이름의 ACL이 이미 존재하는 경우 이름 앞에 숫자가 추가됩니다(예: inside_multicast_1).

3단계 Interface 드롭다운 목록에서 멀티캐스트 경계 필터 ACL을 구성할 인터페이스를 선택합니다.

4단계 경계 ACL에 의해 거부된 소스에서 Auto-RP 메시지를 필터링하려면 **Remove any Auto-RP group range** 확인란을 선택합니다. **Remove any Auto-RP group range** 확인란이 선택되지 않은 경우 모든 Auto-RP 메시지가 통과됩니다.

5단계 **OK**를 클릭합니다.

멀티캐스트 라우팅의 구성 예

다음 예는 다양한 프로세스 옵션으로 멀티캐스트 라우팅을 활성화하고 구성하는 방법을 보여줍니다.

1단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast**를 선택합니다.

2단계 Multicast 창에서 **Enable Multicast** 라우팅 확인란을 선택하고 **Apply**를 클릭합니다.

3단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > MRoute**를 선택합니다.

4단계 **Add** 또는 **Edit**를 클릭합니다.

Add or Edit Multicast Route 대화 상자가 나타납니다.

Add Multicast Route 대화 상자를 사용하여 새로운 고정 멀티캐스트 경로를 ASA에 추가합니다. Edit Multicast Route 대화 상자를 사용하여 기존 고정 멀티캐스트 경로를 변경합니다.

5단계 Source Address 필드에 멀티캐스트 소스의 IP 주소를 입력합니다. 기존 고정 멀티캐스트 경로를 편집할 때는 이 값을 변경할 수 없습니다.

6단계 Source Mask 드롭다운 목록에서 멀티캐스트 소스의 IP 주소에 대한 네트워크 마스크를 선택합니다.

7단계 Incoming Interface 영역에서 **RPF Interface** 라디오 버튼을 클릭하여 경로를 전달할 RPF를 선택하거나 **Interface Name** 라디오 버튼을 클릭한 후 다음을 입력합니다.

- Source Interface 필드의 드롭다운 목록에서 멀티캐스트 경로에 대한 수신 인터페이스를 선택합니다.
- Destination Interface 필드의 드롭다운 목록에서 선택한 인터페이스를 통해 경로를 전달할 대상 인터페이스를 선택합니다.

참고 인터페이스 또는 RPF 인접 디바이스를 지정할 수 있지만 동시에 둘 다 지정할 수는 없습니다.

8단계 Administrative Distance 필드에서 고정 멀티캐스트 경로의 관리 거리를 선택합니다. 고정 멀티캐스트 경로가 유니캐스트 경로와 관리 거리가 같은 경우 고정 멀티캐스트 경로가 우선합니다.

9단계 **OK**를 클릭합니다.

10단계 메인 ASDM 창에서 **Configuration > Device Setup > Routing > Multicast > IGMP > Join Group**을 선택합니다.

Join Group 창이 표시됩니다.

11단계 **Add** 또는 **Edit**를 클릭합니다.

Add IGMP Join Group 대화 상자를 통해 인터페이스를 멀티캐스트 그룹의 멤버로 구성할 수 있습니다. Edit IGMP Join Group 대화 상자를 통해 기존 멤버십 정보를 수정할 수 있습니다.

12단계 Interface Name 필드의 드롭다운 목록에서 인터페이스 이름을 선택합니다. 기존 엔트리를 편집할 경우 이 값을 변경할 수 없습니다.

13단계 Multicast Group Address 필드에 인터페이스가 속하는 멀티캐스트 그룹의 주소를 입력합니다. 유효한 그룹 주소는 224.0.0.0~ 239.255.255.255입니다.

14단계 **OK**를 클릭합니다.

추가 참조 자료

라우팅에 관한 자세한 내용은 다음 섹션을 참조하십시오.

- 25-18 페이지의 관련 문서
- 25-18 페이지의 RFC

관련 문서

관련 항목	문서 제목
SMR 기능 구현을 위해 사용되는 IGMP 및 멀티캐스트 라우팅 표준에 관한 기술 정보	IETF draft-ietf-idmr-igmp-proxy-01.txt

RFC

RFC	제목
RFC 2113	IP 라우터 경고 옵션
RFC 2236	IGMPv2
RFC 2362	PIM-SM
RFC 2588	IP 멀티캐스트와 방화벽

멀티캐스트 라우팅에 대한 기능 내역

표 25-2에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 25-2 멀티캐스트 라우팅에 대한 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
멀티캐스트 라우팅 지원	7.0(1)	멀티캐스트 라우팅 데이터, 인증 및 재배포, 멀티캐스트 라우팅 프로토콜을 이용한 라우팅 정보의 재배포와 모니터링에 대한 지원이 추가되었습니다. 다음 화면을 도입했습니다. Configuration > Device Setup > Routing > Multicast.
클러스터링 지원	9.0(1)	클러스터링 지원이 추가되었습니다.

26 장

IPv6 인접 디바이스 검색

IPv6 인접 디바이스 검색에 관한 정보

IPv6 인접 디바이스 검색 프로세스는 ICMPv6 메시지와 solicited-node 멀티캐스트 주소를 사용하여 동일 네트워크(로컬 링크)에 있는 인접 디바이스의 링크 계층 주소를 확인하고 인접 디바이스의 가독성을 확인하며 주변 라우터를 추적합니다.

노드(호스트)는 인접 디바이스 검색을 사용하여 연결된 링크에 상주하는 것으로 알려진 인접 디바이스에 대한 링크 계층 주소를 확인하고 무효화되는 충돌 값을 빠르게 삭제합니다. 호스트는 또한 인접 디바이스 검색을 사용하여 대신 패킷을 전달할 의사가 있는 주변 라우터를 찾기도 합니다. 또한 노드는 프로토콜을 이용하여 인접 디바이스의 접근 가능 여부를 능동적으로 추적하고 변경된 링크 계층 주소를 감지합니다. 라우터 또는 라우터 경로가 실패할 경우 호스트가 정상 작동하는 대안을 능동적으로 검색합니다.

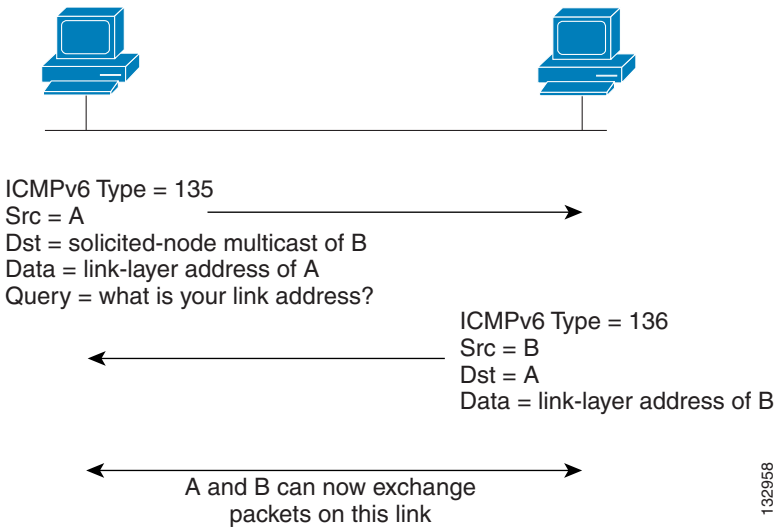
인접 디바이스 요청 메시지

인접 디바이스 요청 메시지(ICMPv6 Type 135)는 로컬 링크에 있는 다른 노드의 링크 계층 주소를 발견하려는 노드가 로컬 링크에서 전송합니다. 인접 디바이스 요청 메시지는 요청된 노드의 멀티캐스트 주소로 전송됩니다. 인접 디바이스 요청 메시지의 소스 주소는 인접 디바이스 요청 메시지를 보내는 노드의 IPv6 주소입니다. 인접 디바이스 요청 메시지는 또한 소스 노드의 링크 계층 주소도 포함합니다.

인접 디바이스 요청 메시지를 수신한 후 대상 노드는 로컬 링크에서 인접 디바이스 광고 메시지(ICPMv6 Type 136)를 전송함으로써 응답합니다. 인접 디바이스 알림 메시지의 소스 주소는 인접 디바이스 알림 메시지를 보내는 노드의 IPv6 주소입니다. 대상 주소는 인접 디바이스 요청 메시지를 보낸 노드의 IPv6 주소입니다. 인접 디바이스 알림 메시지의 데이터 부분은 인접 디바이스 알림 메시지를 보내는 노드의 링크 계층 주소를 포함합니다.

소스 노드가 인접 디바이스 알림을 수신한 후 소스 노드와 대상 노드가 통신할 수 있습니다. 그림 26-1은(는) 인접 디바이스 요청 및 응답 프로세스를 보여줍니다.

그림 26-1 IPv6 인접 디바이스 검색-인접 디바이스 요청 메시지



인접 디바이스 요청 메시지는 인접 디바이스의 링크 계층 주소를 식별한 후 인접 디바이스의 연결성을 확인하는 데 사용됩니다. 노드가 인접 디바이스의 연결성을 확인하고자 하는 경우 인접 디바이스 요청 메시지의 대상 주소는 인접 디바이스의 유니캐스트 주소입니다.

인접 디바이스 알림 메시지는 로컬 링크에 있는 노드의 링크 계층 주소가 변경될 경우에도 전송됩니다. 이러한 변화가 있을 인접 알림에 대한 대상 주소는 올-노드 멀티캐스트 주소입니다.

인접 디바이스 연결 가능 시간

인접 디바이스 연결 가능 시간은 사용할 수 없는 인접 디바이스를 감지할 수 있게 합니다. 시간을 짧게 구성하면 사용할 수 없는 인접 디바이스를 보다 빠르게 감지할 수 있지만 IPv6 네트워크 대역폭과 모든 IPv6 네트워크 디바이스의 처리 리소스를 더 많이 소비합니다. 일반적인 IPv6 운영에서는 시간을 너무 짧게 구성하지 않는 것이 좋습니다.

중복 주소 감지

무상태 자동 컨피그레이션 프로세스 중 Duplicate Address Detection이 새로운 유니캐스트 IPv6 주소의 고유성을 먼저 확인한 후 주소가 인터페이스에 할당됩니다(Duplicate Address Detection 수행 중에는 새로운 주소가 임시 상태를 유지). Duplicate Address Detection은 먼저 새로운 링크-로컬 주소에서 수행됩니다. 링크-로컬 주소가 고유한 것으로 확인되면 인터페이스의 모든 다른 IPv6 유니캐스트 주소에서 Duplicate Address Detection이 수행됩니다.

관리상 다운된 인터페이스에서는 Duplicate Address Detection이 중지됩니다. 인터페이스가 관리상 다운된 동안에는 인터페이스에 할당된 유니캐스트 IPv6 주소가 대기 상태로 설정됩니다. 관리상 가동 상태로 복귀하는 인터페이스는 인터페이스의 모든 유니캐스트 IPv6 주소에 대한 Duplicate Address Detection을 재시작합니다.

중복 주소가 확인되면 주소 상태가 DUPLICATE으로 설정되고 주소가 사용되지 않으며 다음 오류 메시지가 생성됩니다.

```
%ASA-4-325002: Duplicate address ipv6_address/MAC_address on interface
```

중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 비활성화됩니다. 중복 주소가 글로벌 주소인 경우 주소가 사용되지 않습니다. 하지만 주소 상태가 DUPLICATE로 설정된 동안 중복 주소와 연결된 모든 컨피그레이션 명령은 컨피그레이션된 상태를 유지합니다.

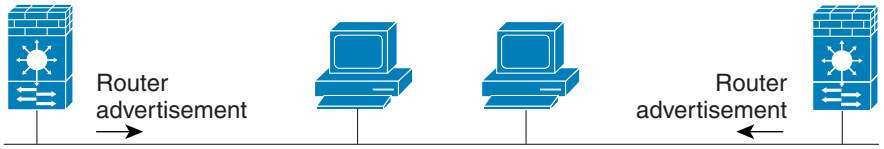
인터페이스의 링크-로컬 주소가 변경된 경우 새로운 링크-로컬 주소에서 Duplicate Address Detection이 수행되고 인터페이스와 연결된 모든 다른 IPv6 주소가 다시 생성됩니다(Duplicate Address Detection은 새로운 링크-로컬 주소에서만 수행됨).

ASA은(는) 인접 디바이스 요청 메시지를 사용하여 Duplicate Address Detection을 수행합니다. 기본적으로 인터페이스가 Duplicate Address Detection을 수행하는 횟수는 1입니다.

라우터 광고 메시지

Cisco ASA은(는) 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 라우터 알림 메시지(ICMPv6 Type 134)는 주기적으로 ASA의 각 구성된 IPv6 인터페이스로 전송됩니다. 라우터 알림 메시지가 all-nodes 멀티캐스트 주소로 전송됩니다. 그림 26-2은(는) IPv6 구성 인터페이스에서 라우터 알림 메시지 전송 방법의 예를 보여줍니다.

그림 26-2 IPv6 인접 디바이스 검색 - 라우터 알림 메시지



라우터 알림 메시지는 일반적으로 다음 정보를 포함합니다.

- 로컬 링크의 노드가 IPv6 주소 자동 구성에 사용할 수 있는 하나 이상의 IPv6 접두사
- 알림에 포함된 각 접두사에 대한 수명 정보
- 완료할 수 있는 자동 컨피그레이션의 유형(무상태 또는 상태 기반)을 나타내는 플래그 세트
- 기본 라우터 정보(알림을 보내는 라우터를 기본 라우터로 사용할지, 만약 그렇다면 라우터를 얼마 동안 기본 라우터로 사용할지(초))
- 호스트가 해당 호스트에서 발생하는 패킷에서 사용할 홉 제한과 MTU와 같이 호스트에 대한 추가 정보
- 주어진 링크에서 인접 디바이스 요청 메시지 재전송 사이의 시간
- 노드가 인접 디바이스를 접근 가능으로 고려하는 시간

라우터 광고는 라우터 요청 메시지에 대한 응답으로도 전송됩니다(ICMPv6 타입 133). 다음 예정된 라우터 알림 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다. 라우터 요청 메시지는 보통 시스템 시동 시에 호스트에 의해 전송되고 호스트에 구성된 유니캐스트 주소가 없기 때문에 라우터 요청 메시지의 소스 주소는 보통 지정되지 않은 IPv6 주소(0:0:0:0:0:0:0:0)입니다. 호스트에 유니캐스트 주소가 구성되어 있는 경우 라우터 요청 메시지를 보내는 인터페이스의 유니캐스트 주소가 메시지에서 소스 주소로 사용됩니다. 라우터 요청 메시지의 대상 주소는 링크 범위의 모든 라우터 멀티캐스트 주소입니다. 라우터 요청에 대한 응답으로 라우터 알림이 전송되면 라우터 알림 메시지의 대상 주소가 라우터 요청 메시지 소스의 유니캐스트 주소입니다.

라우터 알림 메시지에 대한 다음 설정을 구성할 수 있습니다.

- 정기적인 라우터 알림 메시지 사이의 시간 간격
- IPv6 노드가 ASA을(를) 기본 라우터로 간주할 시간을 나타내는 라우터 수명 값
- 해당 링크에서 사용되는 IPv6 네트워크 접두사
- 인터페이스의 라우터 알림 메시지 전송 여부

따로 언급이 없으면 라우터 알림 메시지 설정은 인터페이스마다 다르며 인터페이스 컨피그레이션 모드에서 입력됩니다.

고정 IPv6 인접 디바이스

IPv6 인접 디바이스 캐시의 인접 디바이스를 수동으로 정의할 수 있습니다. 지정된 IPv6 주소에 대한 엔트리가 인접 디바이스 검색 캐시에 존재하는 경우(IPv6 인접 디바이스 검색 프로세스를 통해 학습) 이 엔트리는 고정 엔트리로 자동 변환됩니다. IPv6 인접 디바이스 검색 캐시의 고정 엔트리는 인접 디바이스 검색 프로세스로 인해 변경되지 않습니다.

IPv6 인접 디바이스 검색에 대한 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

IPv6 인접 디바이스 검색 조건

12-13 페이지의 IPv6 주소 지정 구성에 따라 IPv6 주소를 구성합니다.

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우팅 모드에서만 지원됩니다. 투명 모드는 지원되지 않습니다.

추가 지침 및 제한

- 간격 값은 이 인터페이스를 통해 발송되는 모든 IPv6 라우터 알림에 포함됩니다.
- 구성된 시간을 통해 사용할 수 없는 인접 디바이스를 감지할 수 있습니다. 시간을 짧게 구성하면 사용할 수 없는 인접 디바이스를 보다 빠르게 감지할 수 있지만 IPv6 네트워크 대역폭과 모든 IPv6 네트워크 디바이스의 처리 리소스를 더 많이 소비합니다. 일반적인 IPv6 운영에서는 시간을 너무 짧게 구성하지 않는 것이 좋습니다.
- 전송 사이의 간격은 ASA이(가) **ipv6 nd ra-lifetime** 명령을 사용하여 기본 라우터로 구성된 경우 IPv6 라우터 알림 수명보다 작거나 같아야 합니다. 다른 IPv6 노드와의 동기화를 방지하려면 사용되는 실제 값을 지정된 값의 20% 범위로 임의로 조정하십시오.
- **ipv6 nd prefix** 명령을 통해 접두사 알림 여부를 포함하여 접두사별로 개별 매개변수를 제어할 수 있습니다.
- 기본적으로 **ipv6 address** 명령을 사용해서 인터페이스에서 주소로 구성된 접두사는 라우터 알림에서 알려집니다. **ipv6 nd prefix** 명령을 사용하여 접두사를 구성할 경우 해당 접두사만 알려집니다.

- **default** 키워드는 모든 접두사에 대한 기본 매개변수 설정에 사용할 수 있습니다.
- 날짜는 접두사의 만료를 지정하도록 설정할 수 있습니다. 유효 수명과 기본 수명은 실시간으로 계산됩니다. 만료 날짜가 되면 접두사가 더 이상 알려지지 않습니다.
- onlink가 켜진 경우(기본값) 지정된 접두사가 링크에 할당됩니다. 지정된 접두사를 포함한 주소로 트래픽을 보내는 노드는 대상을 링크에서 로컬로 도달 가능한 것으로 간주합니다.
- 자동 컨피그레이션이 켜진 경우(기본값) 지정된 접두사를 IPv6 자동 컨피그레이션에 사용할 수 있음을 호스트에 알려주는 것입니다.
- 무상태 자동 컨피그레이션이 바르게 작동하려면 라우터 알림 메시지의 알려진 접두사 길이가 항상 64비트여야 합니다.
- 라우터 수명 값은 인터페이스에서 발송된 모든 IPv6 라우터 알림에 포함됩니다. 이 값은 이 인터페이스에서 기본 라우터로서 ASA의 유용성을 나타냅니다.
- 0이 아닌 값으로 설정하면 ASA을(를) 이 인터페이스의 기본값으로 간주해야 함을 나타냅니다. 0이 아닌 라우터 수명 값은 라우터 알림 간격보다 적으면 안 됩니다.

고정 IPv6 인접 디바이스 구성에는 다음 지침과 제한 사항이 적용됩니다.

- **ipv6 neighbor** 명령은 **arp** 명령과 유사합니다. 지정된 IPv6 주소에 대한 엔트리가 인접 디바이스 검색 캐시에 존재하는 경우(IPv6 인접 디바이스 검색 프로세스를 통해 학습) 이 엔트리는 고정 엔트리로 자동 변환됩니다. 이 엔트리는 컨피그레이션 저장을 위해 copy 명령이 사용될 때 컨피그레이션에 저장됩니다.
- **show ipv6 neighbor** 명령을 사용하여 IPv6 인접 디바이스 검색 캐시의 고정 엔트리를 봅니다.
- **clear ipv6 neighbor** 명령은 IPv6 인접 디바이스 검색 캐시에서 고정 엔트리를 제외한 모든 엔트리를 삭제합니다. **no ipv6 neighbor** 명령은 인접 디바이스 검색 캐시에서 특정 고정 엔트리를 삭제합니다. 이 명령은 동적 엔트리(IPv6 인접 디바이스 검색 프로세스에서 학습한 엔트리)를 캐시에서 삭제하지 않습니다. **no ipv6 enable** 명령을 사용하여 인터페이스에서 IPv6를 비활성화하면 고정 엔트리를 제외하고 해당 인터페이스에 대한 모든 IPv6 인접 디바이스 검색 캐시 엔트리가 삭제됩니다(엔트리 상태가 INCMP [Incomplete]로 변경됨).
- IPv6 인접 디바이스 검색 캐시의 고정 엔트리는 인접 디바이스 검색 프로세스로 인해 변경되지 않습니다.
- **clear ipv6 neighbor** 명령은 IPv6 인접 디바이스 검색 캐시에서 고정 엔트리를 삭제하지 않습니다. 동적 엔트리만 삭제합니다.
- 생성된 ICMP syslog는 IPv6 인접 디바이스 엔트리의 정기적인 갱신에 의한 것입니다. IPv6 인접 디바이스 엔트리에 대한 ASA 기본 타이머는 ASA가 30초마다 ICMPv6 인접 디바이스 검색과 응답 패킷을 생성하도록 30초입니다. ASA가 IPv6 주소로 구성된 장애 조치 LAN과 상태 인터페이스를 모두 가지고 있는 경우 30초마다 ICMPv6 인접 디바이스 검색과 응답 패킷이 구성된 주소와 링크-로컬 IPv6 주소 모두에 대해 생성됩니다. 또한 각 패킷이 여러 syslog(ICMP 연결 및 로컬-호스트 생성 또는 해체)를 생성하여 연속적인 ICMP syslog가 생성되는 것으로 보일 수 있습니다. IPV6 인접 디바이스 엔트리에 대한 갱신 시간은 일반 데이터 인터페이스에서 구성 가능하나 장애 조치 인터페이스에서는 구성할 수 없습니다. 그러나 이 ICMP 인접 디바이스 검색 트래픽의 CPU에 대한 영향은 거의 없습니다.

IPv6 인접 디바이스 검색 기본 설정

표 26-1은(는) IPv6 인접 디바이스 검색을 위한 기본 설정을 나열합니다.

표 26-1 기본 IPv6 인접 디바이스 검색 매개변수

매개변수	기본
인접 디바이스 요청 전송 메시지 간격 *값*	인접 디바이스 요청 전송 사이의 1000초
인접 디바이스 도달 가능 시간 *값*	기본값은 0입니다.
라우터 알림 전송 간격 *값*	기본값은 200초입니다.
라우터 수명 *값*	기본값은 1800초입니다.
DAD 중 전송되는 연속 인접 디바이스 요청 메시지의 개수 *값*	기본값은 메시지 1개입니다.
접두사 수명	기본 수명은 2592000초(30일)이며 기본 수명은 604800초(7일)입니다.
온링크 플래그	이 플래그는 기본적으로 켜져 있어 접두사가 알림 인터페이스에서 사용됩니다.
자동 구성 플래그	이 플래그는 기본적으로 켜져 있어 접두사가 자동 컨피그레이션에 사용됩니다.
고정 IPv6 인접 디바이스	고정 엔트리는 IPv6 인접 디바이스 검색 캐시에 구성되지 않습니다.

IPv6 Neighbor Discovery 구성

- 26-8 페이지의 인접 디바이스 요청 메시지 간격 구성
- 26-8 페이지의 인접 디바이스 도달 가능 시간 구성
- 26-9 페이지의 라우터 알림 전송 간격 구성
- 26-9 페이지의 라우터 수명 값 구성
- 26-10 페이지의 DAD 설정 구성
- 26-10 페이지의 라우터 알림 메시지 억제
- 26-11 페이지의 IPv6 DHCP 릴레이에 대한 주소 구성 플래그 구성
- 26-11 페이지의 라우터 알림에서 IPv6 접두사 구성
- 26-12 페이지의 고정 IPv6 인접 디바이스 구성

인접 디바이스 요청 메시지 간격 구성

인터페이스에서 IPv6 인접 디바이스 요청 재전송 간격을 구성하려면 다음 단계를 수행합니다.

세부 단계

1단계 **Configuration > Device Setup > Interfaces**를 선택합니다.

2단계 인접 디바이스 요청 간격을 구성할 인터페이스를 선택합니다. 인터페이스가 IPv6 주소로 구성되어 있어야 합니다. 자세한 내용은 12-13 페이지의 IPv6 주소 지정 구성를 참조하십시오.

3단계 **Edit**를 클릭합니다. Edit Interface 대화 상자가 General, Advanced, IPv6의 3개 탭과 함께 나타납니다.

4단계 **IPv6** 탭을 클릭합니다.

5단계 NS Interval 필드에 시간 간격을 입력합니다.

6단계 **OK**를 클릭합니다.

7단계 **Apply**를 클릭하여 실행 중인 컨피그레이션을 저장합니다.

인접 디바이스 도달 가능 시간 구성

도달 가능성 확인 이벤트 발생 후 원격 IPv6 노드를 도달 가능한 것으로 간주하는 시간을 구성하려면 다음 단계를 수행합니다.

세부 단계

1단계 **Configuration > Device Setup > Interfaces**를 선택합니다.

2단계 시간을 구성할 인터페이스를 선택합니다. 인터페이스가 IPv6 주소로 구성되어 있어야 합니다. 자세한 내용은 12-13 페이지의 IPv6 주소 지정 구성를 참조하십시오.

3단계 **Edit**를 클릭합니다. Edit Interface 대화 상자가 General, Advanced, IPv6의 3개 탭과 함께 나타납니다.

4단계 **IPv6** 탭을 클릭합니다.

5단계 Reachable Time 필드에 유효한 값을 입력합니다.

6단계 **OK**를 클릭합니다.

7단계 **Apply**를 클릭하여 실행 중인 컨피그레이션을 저장합니다.

라우터 알림 전송 간격 구성

인터페이스에서 IPv6 라우터 알림 전송 간격을 구성하려면 다음 단계를 수행합니다.

세부 단계

1단계 **Configuration > Device Setup > Interfaces**를 선택합니다.

2단계 시간을 구성할 인터페이스를 선택합니다.

인터페이스가 IPv6 주소로 구성되어 있어야 합니다. 자세한 내용은 12-13 페이지의 IPv6 주소 지정 구성를 참조하십시오.

3단계 **Edit**를 클릭합니다. Edit Interface 대화 상자가 General, Advanced, IPv6의 3개 탭과 함께 나타납니다.

4단계 **IPv6** 탭을 클릭합니다.

5단계 RA Interval 필드에 유효한 전송 간격 값을 입력합니다.

참고 (선택 사항) 라우터 알림 전송 간격 값을 밀리초로 추가하려면 **RA Interval in Milliseconds** 확인란을 선택하고 500~ 1800000의 값을 입력합니다.

6단계 **OK**를 클릭합니다.

7단계 **Apply**를 클릭하여 실행 중인 컨피그레이션을 저장합니다.

라우터 수명 값 구성

인터페이스에서 IPv6 라우터 알림의 라우터 수명 값을 구성하려면 다음 단계를 수행합니다.

세부 단계

1단계 **Configuration > Device Setup > Interfaces**를 선택합니다.

2단계 구성할 인터페이스를 선택하십시오.

인터페이스가 IPv6 주소로 구성되어 있어야 합니다. 자세한 내용은 12-13 페이지의 IPv6 주소 지정 구성을(를) 참고하십시오.

3단계 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 General, Advanced, IPv6의 3개 탭과 함께 나타납니다.

4단계 **IPv6** 탭을 클릭합니다.

5단계 RA Lifetime 필드에 유효한 수명 값을 입력하십시오.

6단계 **OK**를 클릭합니다.

7단계 **Apply**를 클릭하여 실행 중인 컨피그레이션을 저장합니다.

DAD 설정 구성

인터페이스의 DAD 설정을 지정하려면 다음 단계를 수행합니다.

세부 단계

1단계 **Configuration > Device Setup > Interfaces**를 선택합니다.

2단계 구성할 인터페이스를 선택하십시오.

인터페이스가 IPv6 주소로 구성되어 있어야 합니다. 자세한 내용은 12-13 페이지의 IPv6 주소 지정 구성를 참조하십시오.

3단계 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 General, Advanced, IPv6의 3개 탭과 함께 나타납니다.

4단계 **IPv6** 탭을 클릭합니다.

5단계 허용된 DAD 시도 횟수를 입력합니다. 이 설정은 IPv6 주소에 대한 DAD를 수행하는 동안 인터페이스에서 전송되는 연속 인접 디바이스 요청 메시지의 개수를 구성합니다. 유효한 값은 0부터 600입니다. 값을 0으로 입력하면 지정된 인터페이스에서 DAD 처리가 비활성화됩니다. 기본값은 메시지 1개입니다.

라우터 알림 메시지 억제

라우터 알림 메시지는 라우터 요청 메시지에 대한 응답으로 자동 전송됩니다. ASA이(가) IPv6 접두사를 전송하길 원치 않는 인터페이스에서 이 메시지를 비활성화할 수 있습니다(예: 인터페이스 외부).

인터페이스에서 IPv6 라우터 알림의 라우터 수명 값을 억제하려면 다음 단계를 수행합니다.

세부 단계

1단계 **Configuration > Device Setup > Interfaces**를 선택합니다.

2단계 라우터 알림 전송을 억제할 인터페이스를 선택합니다. 인터페이스가 IPv6 주소로 구성되어 있어야 합니다.

3단계 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 General, Advanced, IPv6의 3개 탭과 함께 나타납니다.

4단계 **IPv6** 탭을 클릭합니다.

5단계 **Suppress RA** 확인란을 선택합니다.

IPv6 DHCP 릴레이에 대한 주소 구성 플래그 구성

IPv6 라우터 알림에 플래그를 추가하여 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 IPv6 주소 및/또는 DNS 서버 주소와 같은 추가 정보를 획득하라고 알릴 수 있습니다.

세부 단계

1단계 **Configuration > Device Setup > Interfaces**를 선택합니다.

2단계 구성할 인터페이스를 선택하십시오.

3단계 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 General, Advanced, IPv6의 3개 탭과 함께 나타납니다.

4단계 **IPv6** 탭을 클릭합니다.

5단계 **Hosts should use DHCP for address config** 확인란을 선택하여 IPv6 라우터 알림 패킷에서 Managed Address Config 플래그를 설정합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 주소와 무상태 자동 컨피그레이션 주소를 획득하라고 알려줍니다.

Hosts should use DHCP for non-address config 확인란을 선택하여 IPv6 라우터 알림 패킷에서 Other Address Config 플래그를 설정합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 DHCPv6에서 DNS 서버 주소와 같은 추가 정보를 획득하라고 알려줍니다.

라우터 알림에서 IPv6 접두사 구성

어떤 IPv6 접두사를 IPv6 라우터 알림에 포함할지 구성하려면 다음 단계를 수행합니다.

세부 단계

1단계 **Configuration > Device Setup > Interfaces**를 선택합니다.

2단계 라우터 알림 전송을 억제할 인터페이스를 선택합니다. 인터페이스가 IPv6 주소로 구성되어 있어야 합니다.

3단계 **Edit**를 클릭합니다.

Edit Interface 대화 상자가 General, Advanced, IPv6의 3개 탭과 함께 나타납니다.

4단계 **IPv6** 탭을 클릭합니다.

5단계 인터페이스 IPv6 Prefixes 영역에서 **Add**를 클릭합니다.

Add IPv6 Prefix for Interface 대화 상자가 나타납니다.

6단계 IPv6 주소와 접두사 길이를 입력합니다.

7단계 (선택 사항) IPv6 주소를 수동으로 구성하려면 **No Auto-Configuration** 확인란을 선택합니다. 이 설정은 로컬 링크의 호스트에게 지정된 접두사를 IPv6 자동 컨피그레이션에 사용할 수 없음을 알려줍니다.

8단계 (선택 사항) IPv6 접두사가 알려지지 않음을 나타내려면 **No Advertisements** 확인란을 선택합니다.

9단계 (선택 사항) **Off Link** 확인란은 지정된 접두사가 링크에 할당됨을 나타냅니다. 지정된 접두사를 포함한 주소로 트래픽을 보내는 노드는 대상을 링크에서 로컬로 도달 가능한 것으로 간주합니다. 이 접두사는 온 링크 결정에 사용할 수 없습니다.

10단계 Prefix Lifetime 영역에서 **Lifetime Duration** 라디오 버튼을 클릭하고 다음을 지정합니다.

a. 드롭다운 목록에서 접두사에 대한 유효한 수명(초)을 지정합니다. 이 설정은 지정된 IPv6 접두사를 유효한 접두사로 알릴 시간입니다. 최대값은 무한대를 나타냅니다. 유효한 값의 범위는 0~4294967295입니다. 기본값은 2592000(30일)입니다.

b. 드롭다운 목록에서 접두사에 대한 기본 수명을 지정합니다. 이 설정은 지정된 IPv6 접두사를 기본 접두사로 알릴 시간입니다. 최대값은 무한대를 나타냅니다. 유효한 값의 범위는 0~4294967295입니다. 기본 설정은 604800(7일)입니다.

11단계 접두사 수명 만료 날짜를 정의하려면 **Lifetime Expiration Date** 라디오 버튼을 클릭하고 다음을 지정합니다.

a. 드롭다운 목록에서 유효한 달과 일을 선택하고 hh:mm 형식으로 시간을 입력합니다.

b. 드롭다운 목록에서 기본 달과 일을 선택하고 hh:mm 형식으로 시간을 입력합니다.

12단계 **OK**를 클릭하여 설정을 저장합니다.

Interface IPv6 Prefixes Address 필드가 기본 및 유효 날짜와 함께 표시됩니다.

고정 IPv6 인접 디바이스 구성

인접 디바이스를 추가하기 전에 하나 이상의 인터페이스에서 IPv6가 활성화되었는지 확인하십시오. 그러지 않으면 ASDM이 컨피그레이션이 실패했다는 오류 메시지를 반환합니다.

IPv6 주소 구성에 관한 정보는 12-13 페이지의 IPv6 주소 지정 구성에서 참조하십시오.

IPv6 고정 인접 디바이스를 추가하려면 다음 단계를 수행하십시오.

세부 단계

1단계 **Configuration > Device Management > Advanced > IPv6 Neighbor Discovery Cache**를 선택합니다.

2단계 **Add**를 클릭합니다.

Add IPv6 Static Neighbor 대화 상자가 나타납니다.

3단계 Interface Name 드롭다운 목록에서 인접 디바이스를 추가할 인터페이스를 선택합니다.

4단계 IP Address 필드에 로컬 데이터-링크 주소에 해당하는 IPv6 주소를 입력하거나 생략 부호(...)를 클릭하여 주소를 찾습니다.

지정된 IPv6 주소에 대한 엔트리가 인접 디바이스 검색 캐시에 존재하는 경우(IPv6 인접 디바이스 검색 프로세스를 통해 학습) 이 엔트리는 고정 엔트리로 자동 변환됩니다.

5단계 MAC 주소 필드에 로컬 데이터-라인(하드웨어) MAC 주소를 입력합니다.

6단계 **OK**를 클릭합니다.

참고 변경 사항을 적용하고 컨피그레이션을 저장하기 전에 **Reset**을 클릭하면 변경 사항이 취소되고 원래의 값으로 돌아갑니다.

7단계 **Apply**를 클릭하여 실행 중인 컨피그레이션을 저장합니다.

동적으로 검색된 인접 디바이스 보기 및 지우기

호스트 또는 노드가 인접 디바이스와 통신할 때 인접 디바이스가 인접 디바이스 검색 캐시에 추가됩니다. 더 이상 해당 인접 디바이스와 통신이 없을 때 캐시에서 인접 디바이스가 제거됩니다.

동적으로 검색된 인접 디바이스를 보고 이러한 인접 디바이스를 IPv6 인접 디바이스 검색 캐시에서 삭제하려면 다음 단계를 수행합니다.

1단계 **Monitoring > Interfaces > IPv6 Neighbor Discovery Cache**를 선택합니다.

IPv6 Neighbor Discovery Cache 창에서 모든 고정 인접 디바이스 및 동적으로 검색된 인접 디바이스를 볼 수 있습니다.

2단계 캐시에서 모든 동적으로 검색된 인접 디바이스를 삭제하려면 **Clear Dynamic Neighbor Entries**를 클릭합니다.

동적으로 검색된 인접 디바이스가 캐시에서 삭제됩니다.

참고 이 절차는 캐시에서 동적으로 검색된 인접 디바이스만 삭제하며 고정 인접 디바이스는 삭제하지 않습니다.

추가 참조 자료

IPv6 접두사 구현에 관한 추가 정보는 다음 항목을 참조하십시오.

- 26-13 페이지의 IPv6 접두사 관련 문서
- 26-13 페이지의 IPv6 접두사 및 문서를 위한 RFC

IPv6 접두사 관련 문서

관련 항목	문서 제목
ipv6 명령	*명령 참조*

IPv6 접두사 및 문서를 위한 RFC

RFC	제목
RFC 2373은 라우터 알림에서 IPv6 네트워크 주소 숫자를 표시하는 방법을 보여주는 전체 문서를 포함합니다. *ipv6-prefix* 명령 인수는 콜론 사이에 16비트 값을 사용하여 16진수 형식으로 주소를 지정해야 하는 네트워크 숫자를 나타냅니다.	IP 버전 6 주소 아키텍처
RFC 3849는 문서에서 IPv6 주소 접두사 사용에 관한 요구 사항을 지정합니다. 문서에서 사용이 예약된 IPv6 유니캐스트 주소 접두사는 2001:DB8::/32입니다.	문서를 위해 예약된 IPv6 주소 접두사

IPv6 인접 디바이스 검색을 위한 기능 내역

표 26-2에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 26-2 IPv6 인접 디바이스 검색을 위한 기능 내역

기능 이름	릴리스	기능 정보
IPv6 인접 디바이스 검색	7.0(1)	이 기능을 도입했습니다. 다음 화면을 도입했습니다. Monitoring > Interfaces > IPv6 Neighbor Discovery Cache Configuration > Device Management > Advanced > IPv6 Neighbor Discovery Cache Configuration > Device Setup > Interfaces > IPv6
IPv6 DHCP 릴레이에 대한 주소 구성 플래그	9.0(1)	다음 화면을 수정했습니다. Configuration > Device Device Setup > Interfaces > IPv6.

파 트 7

AAA 서버 및 로컬 데이터베이스

27 장

AAA 정보

이 장에서는 인증, 권한 부여 및 어카운팅(AAA, “트리플 A”로 발음)에 대해 설명합니다. AAA는 컴퓨터 리소스에 대한 액세스 제어를 위한 서비스의 집합으로, 정책을 구현하고, 사용량을 평가하고 서비스에 대한 청구에 필요한 정보를 제공합니다. 이 과정은 효과적인 네트워크 관리 및 보안을 위해 중요한 부분으로 간주됩니다.

인증

인증은 액세스를 부여하기 전에 보통 사용자 이름과 비밀번호를 입력하도록 요구하는 방식으로 효과적인 사용자 확인 방법을 제공합니다. AAA 서버는 사용자의 인증 자격 증명을 데이터베이스에 저장된 다른 사용자의 자격 증명과 비교합니다. 자격 증명이 일치하면 사용자는 네트워크에 액세스할 수 있습니다. 자격 증명이 일치하지 않으면, 인증에 실패하고 네트워크 액세스가 거부됩니다.

Cisco ASA이(가) 다음 항목을 인증하도록 구성할 수 있습니다.

- 다음 세션을 포함한ASA 모든 관리 연결:
  - 텔넷
  - SSH
  - 시리얼 콘솔
  - HTTPS를 사용하는 ASDM
  - VPN 관리 액세스
- **enable** 명령어
- 네트워크 액세스
- VPN 접속

권한 부여

승인은 정책을 구현하는 프로세스로 사용자의 액세스가 허용된 활동, 리소스 또는 서비스 유형을 판단하는 것입니다. 사용자가 인증되면 해당 사용자는 다양한 액세스 또는 활동 유형에 대한 허가를 받을 수 있습니다.

ASA이(가) 다음 항목을 승인하도록 구성할 수 있습니다.

- 관리 명령
- 네트워크 액세스
- VPN 접속

어카운팅

어카운팅은 사용자가 액세스 중 소비하는 리소스를 측정합니다. 여기에는 시스템 사용 시간, 사용자가 세션 중 보내거나 받는 데이터의 양 등이 포함됩니다. 어카운팅은 세션 통계 및 사용량 정보 기록을 통해 이루어지며 이는 승인 제어, 청구, 경향 분석, 리소스 활용도 및 용량 계획 활동에 사용됩니다.

인증, 권한 부여 및 어카운팅 간 상호 작용

인증을 단독으로 사용하거나 권한 부여 및 어카운팅과 함께 사용할 수 있습니다. 인증은 항상 사용자를 먼저 확인해야 합니다. 어카운팅을 단독으로 사용하거나 인증 및 권한 부여와 함께 사용할 수 있습니다.

AAA 서버

AAA 서버는 액세스 제어를 위해 사용되는 네트워크 서버입니다. 인증은 사용자를 식별합니다. 인증은 사용자가 액세스할 수 있는 리소스와 서비스를 결정하는 정책을 구현합니다. 어카운팅은 청구 및 분석을 위해 사용되는 시간과 데이터를 추적합니다.

AAA 서버 그룹

인증, 권한 부여 또는 어카운팅을 위해 외부 AAA 서버를 사용하려면 먼저 AAA 프로토콜당 최소 1개의 AAA 서버 그룹을 만들고 하나 이상의 서버를 각 그룹에 추가해야 합니다. AAA 서버 그룹은 이름으로 구분합니다. 각 서버 그룹은 1가지 유형의 서버 또는 서비스에만 해당됩니다.

로컬 데이터베이스 지원

ASA는 사용자가 사용자 프로필을 저장할 수 있는 로컬 데이터베이스를 유지합니다. AAA 서버 대신 로컬 데이터베이스를 사용하여 사용자 인증, 권한 부여 및 어카운팅을 제공할 수 있습니다.

28장

AAA의 로컬 데이터베이스

이 장에서는 AAA에 로컬 서버를 구성하는 방법에 대해 설명합니다.

로컬 데이터베이스 정보

다음 기능에 로컬 데이터베이스를 사용할 수 있습니다.

- ASDM 사용자당 액세스
- 콘솔 인증
- 텔넷 및 SSH 인증
- **enable** 명령 인증

  이 설정은 CLI 액세스에만 적용되며 Cisco ASDM 로그인에는 영향을 미치지 않습니다.
- 명령 권한 부여

  로컬 데이터베이스를 사용하여 명령 권한 부여를 켜면 Cisco ASA에서는 사용자 권한 수준을 참조하여 어떤 명령을 사용할 수 있는지 확인합니다. 그렇지 않을 경우 권한 수준은 일반적으로 사용되지 않습니다. 기본적으로 모든 명령의 권한 수준은 0 또는 15입니다. ASDM에서는 사전 정의된 3개의 권한 수준을 사용할 수 있도록 지원하며 수준 15(관리자), 수준 5(읽기 전용), 수준 3(모니터링 전용)에 명령이 할당됩니다. 사전 정의된 수준을 사용하면 이 3가지 권한 수준 중 하나에 사용자가 할당됩니다.
- 네트워크 액세스 인증
- VPN 클라이언트 인증

다중 컨텍스트 모드의 경우, 시스템 실행 영역에서 사용자 이름을 구성하면 **login** 명령을 사용하여 CLI에서 개별 로그인을 제공할 수 있습니다. 그러나 시스템 실행 영역에서 로컬 데이터베이스를 사용하는 AAA 규칙은 구성할 수 없습니다.

참고 네트워크 액세스 권한 부여에는 로컬 데이터베이스를 사용할 수 없습니다.

폴백(Fallback) 지원

로컬 데이터베이스는 몇 가지 기능을 지원하기 위한 폴백 방법으로서의 역할을 수행할 수 있습니다. 이러한 동작은 ASA가 실수로 잠기는 것을 방지하기 위해 고안된 것입니다.

사용자가 로그인할 경우 그룹의 서버는 한 번에 하나씩 차례로 액세스되고, 컨피그레이션에서 지정한 첫 번째 서버부터 시작되며 서버가 응답할 때까지 계속됩니다. 그룹의 모든 서버를 사용할 수 없는 경우, 로컬 데이터베이스가 폴백 방법(인증 및 권한 부여에만 사용)으로 구성되어 있으면 ASA에서는 로컬 데이터베이스를 사용하려고 시도합니다. 폴백 방법이 없는 경우, ASA에서는 AAA 서버에 대한 시도를 계속 수행합니다.

폴백 지원이 필요한 사용자의 경우, 로컬 데이터베이스의 사용자 이름 및 비밀번호가 AAA 서버의 사용자 이름 및 비밀번호와 일치하는 것이 좋습니다. 이러한 방식을 사용하면 투명 폴백 지원이 제공됩니다. 사용자는 서비스를 제공하는 것이 AAA 서버인지 또는 로컬 데이터베이스인지 확인할 수 없으므로, 로컬 데이터베이스의 사용자 이름 및 비밀번호와 다른 사용자 이름 및 비밀번호를 AAA 서버에서 사용할 경우, 해당 사용자는 어떤 사용자 이름 및 비밀번호를 제공하는 게 맞는지 정확히 알 수 없게 됩니다.

로컬 데이터베이스에서는 다음과 같은 폴백 기능을 지원합니다.

- 콘솔 및 enable 비밀번호 인증 — 그룹의 서버를 모두 사용할 수 없는 경우 ASA에서는 로컬 데이터베이스를 사용하여 관리 액세스 권한을 인증하며, 여기에는 enable 비밀번호 인증도 포함될 수 있습니다.
- 명령 인증 — 그룹의 TACACS+ 서버를 모두 사용할 수 없는 경우, 로컬 데이터베이스를 사용하여 권한 수준을 기준으로 명령을 인증합니다.
- VPN 인증 및 권한 부여 — 정상적으로 VPN 서비스를 지원하는 AAA 서버를 사용할 수 없는 경우, ASA에 원격 액세스할 수 있도록 VPN 인증 및 권한 부여가 지원됩니다. 로컬 데이터베이스로 폴백을 수행하도록 구성된 터널 그룹을 관리자의 VPN 클라이언트에서 지정할 경우, 로컬 데이터베이스가 필요한 속성으로 구성되어 있으면 AAA 서버 그룹을 사용할 수 없는 경우에도 VPN 터널을 설정할 수 있습니다.

그룹의 여러 서버에서 폴백이 작동하는 방식

서버 그룹에 여러 개의 서버를 구성하고 서버 그룹의 로컬 데이터베이스에 폴백을 사용하도록 설정할 경우, 해당 그룹의 서버가 ASA의 인증 요청에 반응하지 않으면 폴백이 실행됩니다. 명확히 이해하기 위해 다음 시나리오를 가정해 보십시오.

2개의 Active Directory 서버가 서버 1, 서버 2의 순서대로 포함된 LDAP 서버 그룹을 구성합니다. 원격 사용자가 로그인하면 ASA에서는 서버 1에 인증을 시도합니다.

서버 1이 인증 오류에 응답할 경우(예: *사용자가 없음*), ASA에서는 서버 2에 인증을 시도하지 않습니다.

서버 1이 시간 제한 내에 응답하지 않을 경우(또는 인증 시도 횟수가 구성된 최대 횟수를 초과할 경우), ASA에서는 서버 2의 응답을 시도합니다.

그룹의 두 서버가 모두 응답하지 않고 로컬 데이터베이스에 폴백을 수행하도록 ASA가 구성된 경우, ASA에서는 로컬 데이터베이스를 인증하려고 시도합니다.

로컬 데이터베이스에 대한 지침

인증 또는 권한 부여에 로컬 데이터베이스를 사용할 경우 ASA가 잠기는 것을 방지해야 합니다.

관련 주제

36-28 페이지의 잠금에서 복구

로컬 데이터베이스에 사용자 어카운트 추가

로컬 데이터베이스에 사용자를 추가하려면 다음 단계를 수행합니다.

절차

1단계 **Configuration > Device Management > Users/AAA > User Accounts**를 선택한 다음 **Add**를 클릭합니다.

Add User Account-Identity 대화 상자가 나타납니다.

2단계 사용자 이름을 4~64자 길이로 입력합니다.

3단계 비밀번호는 3~32자로 입력합니다. 비밀번호는 대소문자를 구분합니다. 필드에는 별표만 표시됩니다. 보안을 위해 비밀번호의 길이는 최소 8자 이상인 것이 좋습니다.

참고 User Accounts 창에서 enable 비밀번호를 구성하려면 enable_15 사용자의 비밀번호를 변경합니다. enable_15 사용자는 User Accounts 창에 항상 표시되며 기본 사용자 이름을 나타냅니다. 이러한 enable 비밀번호 컨피그레이션 방법은 시스템 컨피그레이션을 위해 ASDM에서만 사용할 수 있는 방법입니다. CLI에서 다른 enable 수준 비밀번호(예: enable 비밀번호 10)를 구성한 경우, 해당 사용자는 enable_10 등으로 목록에 표시됩니다.

4단계 비밀번호를 다시 입력합니다.

보안상의 이유로 비밀번호 필드에는 별표만 표시됩니다.

5단계 사용자가 속한 VPN 그룹을 지정하려면 **Member of** 필드에 그룹 이름을 입력하고 **Add**를 클릭합니다.

6단계 **Access Restriction** 영역에 사용자의 관리 액세스 수준을 설정합니다. **Configuration > Device Management > Users/AAA > AAA Access > Authorization** 탭에서 **Perform authorization for exec shell access** 옵션을 클릭하여 관리 권한 부여를 먼저 활성화해야 합니다.

다음 옵션 중 하나를 선택합니다.

- **Full Access (ASDM, Telnet, SSH and console)** — 로컬 데이터베이스를 사용하여 관리 액세스에 대한 인증을 구성할 경우, 이 옵션을 선택하면 사용자가 ASDM, SSH, 텔넷, 콘솔 포트를 사용할 수 있습니다. 또한 인증을 활성화하면 사용자가 전역 컨피그레이션 모드에 액세스할 수 있습니다.
  - **Privilege Level** — 이 사용자가 로컬 명령 권한 부여를 사용하는 데 필요한 권한 수준을 선택합니다. 범위는 0(최저)부터 15(최고)까지입니다.
- **CLI login prompt for SSH, Telnet and console (no ASDM access)** — 로컬 데이터베이스를 사용하여 관리 액세스에 대한 인증을 구성할 경우, 이 옵션을 선택하면 사용자가 SSH, 텔넷, 콘솔 포트를 사용할 수 있습니다. HTTP 인증을 컨피그레이션한 경우 사용자는 ASDM을 컨피그레이션에 사용할 수 없습니다. ASDM 모니터링이 허용됩니다. 또한 인증을 활성화하면 사용자가 전역 컨피그레이션 모드에 액세스할 수 없습니다.

- **No ASDM, SSH, Telnet, or console access** — 로컬 데이터베이스를 사용하여 관리 액세스에 대한 인증을 구성할 경우, 이 옵션을 선택하면 사용자는 관리자가 구성한 모든 관리 액세스 방법에 액세스할 수 없습니다(Serial 옵션은 제외이며 직렬 액세스는 허용됨).

7단계 (선택 사항) 사용자 한 명 단위로 ASA에 대한 SSH 연결을 지원하는 공개 키 인증을 사용하려면 **Navigation** 창에서 다음 옵션 중 하나를 클릭합니다.

- **Public Key Authentication** — Base64-인코딩 공개 키로 붙여넣습니다. 인증서 없이 SSH-RSA로 키(raw key)를 생성하는 것이 가능한 SSH 키 생성 소프트웨어(예: ssh keygen)를 사용하여 키를 생성할 수 있습니다. 기존 키를 볼 경우 해당 키는 SHA-256 해시를 사용하여 암호화됩니다. 해시된 키를 복사 및 붙여넣기 해야 할 경우 **Key is hashed** 확인란을 선택합니다.

  인증 키를 제거하려면 **Delete Key**를 클릭하여 확인 대화 상자를 표시합니다. 인증 키를 제거하려면 **Yes**를 클릭하고 유지하려면 **No**를 클릭합니다.

- **Public Key Using PKF — Specify a new PKF key** 확인란을 선택하고, 최대 4096비트의 PKF(공개 키 파일) 형식 키를 붙여넣거나 가져옵니다. 이 형식은 키의 크기가 Base64 형식으로 붙여넣기에는 너무 클 때 사용합니다. 예를 들어, ssh keygen을 사용하여 4096비트 키를 생성한 후 이를 PKF로 변환하고 이 창으로 가져올 수 있습니다. 기존 키를 볼 경우 해당 키는 SHA-256 해시를 사용하여 암호화됩니다. 해시된 키를 복사 및 붙여넣기 해야 할 경우, **Public Key Athentication** 창에서 해당 키를 복사하고 **Key is hashed** 확인란을 선택한 상태에서 새 ASA의 창에 키를 붙여넣습니다.

  인증 키를 제거하려면 **Delete Key**를 클릭하여 확인 대화 상자를 표시합니다. 인증 키를 제거하려면 **Yes**를 클릭하고 유지하려면 **No**를 클릭합니다.

8단계 이 사용자에 대한 VPN 정책 속성을 구성하려면 **VPN Policy**를 클릭합니다. VPN 컨피그레이션 가이드를 참조하십시오.

9단계 **Apply**를 클릭합니다.

사용자가 로컬 데이터베이스에 추가되며, 실행 중인 컨피그레이션에 변경 사항이 저장됩니다.

팁 **Configuration > Device Management > Users/AAA > User Accounts** 창의 각 열에서 특정 텍스트를 검색할 수 있습니다. **Find** 상자에서 찾으려는 특정 텍스트를 입력한 다음 **Up** 또는 **Down** 화살표를 클릭합니다. 텍스트 검색에 별표("*") 및 물음표("?")를 와일드카드 문자로 사용할 수도 있습니다.

다음 예에서는 Linux 또는 Macintosh 시스템에서 SSH용 공유 키를 생성하고 이를 ASA에 가져옵니다.

1단계 4096비트용 ssh-rsa 공개 및 개인 키를 컴퓨터에 생성합니다.

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
```

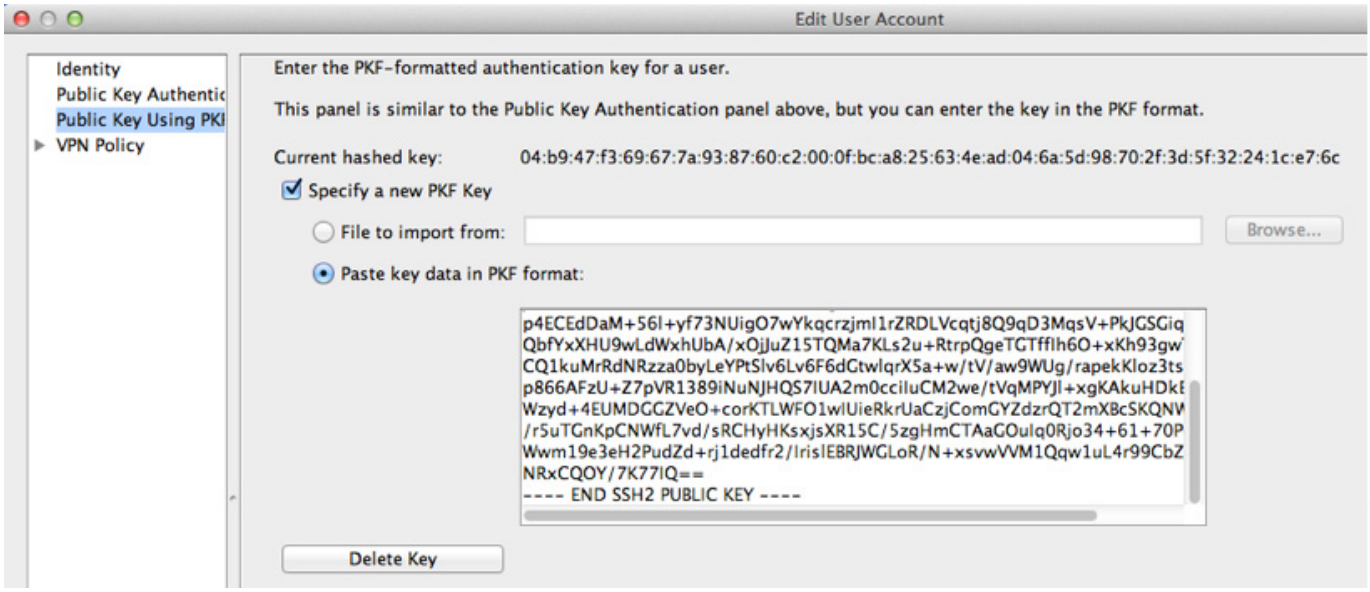
```
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
+-----------------+
```

2단계 Convert the key to PKF format:

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by ramona@rboersma-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3단계 키를 클립보드에 복사합니다.

4단계 ASDM에서 **Configuration > Device Management > Users/AAA > User Accounts**를 선택하고 사용자 이름을 선택한 다음 **Edit**를 클릭합니다. **Public Key Using PKF**를 클릭하고 키를 창에 붙여넣습니다.



5단계 사용자(테스트)가 ASA에 SSH를 수행할 수 있는지 확인합니다.

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

암호를 입력하라는 다음과 같은 대화 상자가 나타납니다.

한편, 터미널 세션에는 다음과 같은 메시지가 표시됩니다.

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

로컬 데이터베이스 인증 및 권한 부여 테스트

ASA에서 로컬 데이터베이스에 접속하고, 사용자에 대한 인증 또는 권한 부여를 수행할 수 있는지 확인하려면 다음 단계를 수행합니다.

절차

1단계 **Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups** 테이블에서 서버가 상주하는 서버 그룹을 클릭합니다.

2단계 **Servers in the Selected Group** 테이블에서 테스트할 서버를 클릭합니다.

3단계 **Test**를 클릭합니다.

선택된 서버에 대한 **Test AAA Server** 대화 상자가 나타납니다.

4단계 수행할 테스트 유형 **Authentication** 또는 **Authorization**을 클릭합니다.

5단계 사용자 이름을 입력합니다.

6단계 인증을 테스트하는 경우 사용자 이름의 비밀번호를 입력합니다.

7단계 **OK**를 클릭합니다.

ASA에서 인증 또는 권한 부여 테스트 메시지를 서버에 전송합니다. 테스트가 실패한 경우 ASDM는 오류 메시지를 표시합니다.

로컬 데이터베이스 모니터링

로컬 데이터베이스를 모니터링하려면 다음 screens를 참조하십시오.

- **Monitoring > Properties > AAA Servers**

  이 창에는 AAA 서버 통계가 표시됩니다.

로컬 데이터베이스에 대한 기록

표 28-1 로컬 데이터베이스에 대한 기록

기능 이름	플랫폼 릴리스	기능 정보
AAA의 로컬 데이터베이스 컨피그레이션	7.0(1)	AAA 사용을 위해 로컬 데이터베이스를 구성하는 방법에 대해 설명합니다. 다음 화면을 도입했습니다. Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > User Accounts
SSH 공개 키 인증 지원	9.1(2)	이제 사용자 한 명 단위로 ASA에 대한 SSH 연결을 지원하는 공개 키 인증을 사용할 수 있습니다. PKF(공개 키 파일) 형식의 키 또는 Base64 키를 지정할 수 있습니다. PKF 키는 최대 4096비트입니다. ASA의 Base64 형식 지원 범위(최대 2048비트)에 비해 너무 큰 키에는 PKF 형식을 사용합니다. 다음 화면을 도입했습니다. Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Authentication Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Using PKF *8.4(4.1)에서도 사용 가능. PKF 키 형식은 9.1(2)에서만 지원됩니다.*

AAA를 위한 RADIUS 서버

이 장에서는 AAA를 위한 RADIUS 서버 구성 방법을 설명합니다.

RADIUS 서버에 대한 정보

Cisco ASA는 AAA를 위해 다음의 RFC 규격 RADIUS 서버를 지원합니다.

- Cisco Secure ACS 3.2, 4.0, 4.1, 4.2 및 5.x
- Cisco ISE(Identity Services Engine)
- RSA Authentication Manager 5.2, 6.1 및 7.x의 RSA RADIUS
- Microsoft

지원되는 인증 방법

ASA은(는) RADIUS 서버에서 다음 인증 방법을 지원합니다.

- PAP—모든 연결 유형에 대해 지원됩니다.
- CHAP 및 MS-CHAPv1—L2TP-over-IPsec 연결에 대해 지원됩니다.
- MS-CHAPv2—L2TP-over-IPsec 연결 및 일반 IPsec 원격 액세스 연결(비밀번호 관리 기능이 활성화된 경우)에 대해 지원됩니다. 클라이언트 없는 연결로 MS-CHAPv2를 사용할 수도 있습니다.
- Authentication Proxy modes—RADIUS-to Active-Directory, RADIUS-to-RSA/SDI, RADIUS-to-Token 서버 및 RSA/SDI-to-RADIUS 연결에 대해 지원됩니다.

참고 VPN 연결을 위해 ASA 및 RADIUS 서버 사이에 사용되는 프로토콜로 MS-CHAPv2를 활성화하려면 터널 그룹 일반 속성에서 비밀번호 관리가 활성화되어 있어야 합니다. 비밀번호 관리를 활성화하면 ASA에서 RADIUS 서버로 MS-CHAPv2 인증 요청이 생성됩니다. 자세한 내용은 **password-management** 명령 설명을 참조하십시오.

터널 그룹에서 이중 인증을 사용하고 비밀번호 관리를 활성화하는 경우 기본 및 보조 인증 요청은 MS-CHAPv2 요청 속성을 포함합니다. RADIUS 서버가 MS-CHAPv2를 지원하지 않는 경우 **no mschapv2-capable** 명령을 사용하여 서버가 non-MS-CHAPv2 인증 요청을 보내도록 구성할 수 있습니다.

VPN 연결 사용자 인증

ASA은(는) 동적 ACL 또는 사용자별 ACL 이름을 사용하여 VPN 원격 액세스 및 방화벽 cut-through-proxy 세션의 사용자 인증에 RADIUS 서버를 이용할 수 있습니다. 동적 ACL을 구현하려면 이를 지원하도록 RADIUS 서버를 구성해야 합니다. 사용자가 인증되면 RADIUS 서버가 다운로드 가능한 ACL 또는 ACL 이름을 ASA(으)로 전송합니다. 주어진 서비스에 대한 액세스가 ACL에 의해 허용 또는 거부됩니다. 인증 세션이 만료되면 ASA이(가) ACL을 삭제합니다.

ACL 외에도 ASA은(는) VPN 원격 액세스 및 방화벽 cut-through proxy 세션에 대한 권한 부여 및 설정을 위한 다른 많은 속성도 지원합니다.

지원되는 RADIUS 속성 집합

ASA은(는) 다음 RADIUS 속성 집합을 지원합니다.

- RFC 2138에 정의된 인증 속성
- RFC 2139에 정의된 어카운팅 속성
- RFC 2868에 정의된 터널링된 프로토콜 지원을 위한 RADIUS 속성
- RADIUS 공급업체 ID 9로 식별되는 Cisco IOS VSA(Vendor-Specific Attributes)
- RADIUS 공급업체 ID 3076으로 식별되는 Cisco VPN 관련 VSA
- RFC 2548에 정의된 Microsoft VSA
- 1은 최저, 15는 최저 수준을 나타내는 표준 0~15의 숫자 권한 순위를 제공하는 Cisco VSA(Cisco-Priv-Level) 0 수준은 권한이 없음을 나타냅니다. 첫 번째 수준(로그인)은 이 수준에서 이용 가능한 명령에 대해 권한이 있는 EXEC 액세스를 허용합니다. 두 번째 수준(활성화)은 CLI 컨피그레이션 권한을 허용합니다.

지원되는 RADIUS 권한 부여 속성

권한 부여는 권한 또는 속성을 적용하는 프로세스를 가리킵니다. RADIUS 서버는 권한이나 속성이 구성된 경우 이를 적용하는 인증 서버로 정의됩니다. 이러한 속성은 공급업체 ID 3076을 가지고 있습니다.

표 29-1은(는) 사용자 권한 부여에 사용할 수 있는 지원되는 RADIUS 속성을 나열합니다.

참고 RADIUS 속성 이름은 cVPN3000 접두사를 포함하지 않습니다. Cisco Secure ACS 4.x는 이 새로운 명명법을 지원하지만 4.0 이전 ACS 릴리스의 속성은 여전히 cVPN3000 접두사를 포함합니다. ASA은(는) 속성 이름이 아닌 속성 숫자 ID를 기반으로 RADIUS 속성을 적용합니다.

표 29-1의 모든 속성은 146, 150, 151 및 152 속성 번호를 제외하고 RADIUS 서버에서 ASA(으)로 전송되는 다운스트림 속성입니다. 이러한 속성 번호는 ASA에서 RADIUS 서버로 전송되는 업스트림 속성입니다. RADIUS 속성 146과 150은 인증과 권한 부여 요청을 위해 ASA에서 RADIUS 서버로 전송됩니다. 이전에 나열한 4개의 속성은 모두 어카운팅 시작, 임시 업데이트 및 중단 요청을 위해 ASA에서 RADIUS 서버로 전송됩니다. 업스트림 RADIUS 속성 146, 150, 151 및 152는 버전 8.4(3)에서 도입되었습니다.

Cisco ACS 5.x 및 Cisco ISE는 버전9.0(1)에서 RADIUS 인증을 사용하는 IP 주소 할당을 위한 IPv6 프레임드 IP 주소를 지원하지 않습니다.

표 29-1 지원되는 RADIUS 권한 부여 속성

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
Access-Hours	Y	1	문자열	단일	시간 범위의 이름(예: 업무 시간)
Access-List-Inbound	Y	86	문자열	단일	ACL ID
Access-List-Outbound	Y	87	문자열	단일	ACL ID
Address-Pools	Y	217	문자열	단일	IP 로컬 풀의 이름
Allow-Network-Extension-Mode	Y	64	부울	단일	0 = Disabled 1 = Enabled
Authenticated-User-Idle-Timeout	Y	50	정수	단일	1~35791394분
Authorization-DN-Field	Y	67	문자열	단일	가능한 값: UID, OU, O, CN, L, SP, C, EA, T, N, GN, SN, I, GENQ, DNQ, SER, use-entire-name
Authorization-Required		66	정수	단일	0 = No 1 = 예
Authorization-Type	Y	65	정수	단일	0 = None 1 = RADIUS 2 = LDAP
Banner1	Y	15	문자열	단일	Cisco VPN 원격 액세스 세션에 대해 표시할 배너 문자열: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2 및 Clientless SSL

표 29-1 지원되는 RADIUS 권한 부여 속성 (계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
Banner2	Y	36	문자열	단일	Cisco VPN 원격 액세스 세션에 대해 표시할 배너 문자열: IPsec IKEv1, AnyConnect SSL-TLS/DTLS/IKEv2 및 Clientless SSL Banner2 문자열은 Banner1 문자열로 연결됩니다(구성된 경우).
Cisco-IP-Phone-Bypass	Y	51	정수	단일	0 = Disabled 1 = Enabled
Cisco-LEAP-Bypass	Y	75	정수	단일	0 = Disabled 1 = Enabled
Client Type	Y	150	정수	단일	1 = Cisco VPN Client (IKEv1) 2 = AnyConnect Client SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 = AnyConnect Client IPsec VPN (IKEv2)
Client-Type-Version-Limiting	Y	77	문자열	단일	IPsec VPN 버전 번호 문자열
DHCP-Network-Scope	Y	61	문자열	단일	IP 주소
Extended-Authentication-On-Rekey	Y	122	정수	단일	0 = Disabled 1 = Enabled
Group-Policy	Y	25	문자열	단일	원격 액세스 VPN 세션에 대한 그룹 정책을 설정합니다. 버전 8.2.x 이상에서는 IETF-Radius-Class 대신 이 속성을 사용하십시오. 다음 형식 중 하나를 사용할 수 있습니다. • *group policy name* • OU=*group policy name* • OU=*group policy name*;
IE-Proxy-Bypass-Local		83	정수	단일	0 = None 1 = Local
IE-Proxy-Exception-List		82	문자열	단일	줄바꿈(\n)으로 구분된 DNS 도메인 목록
IE-Proxy-PAC-URL	Y	133	문자열	단일	PAC 주소 문자열
IE-Proxy-Server		80	문자열	단일	IP 주소
IE-Proxy-Server-Policy		81	정수	단일	1 = No Modify 2 = No Proxy 3 = Auto detect 4 = Use Concentrator Setting
IKE-KeepAlive-Confidence-Interval	Y	68	정수	단일	10~300초
IKE-Keepalive-Retry-Interval	Y	84	정수	단일	2~10초
IKE-Keep-Alives	Y	41	부울	단일	0 = Disabled 1 = Enabled

표 29-1 지원되는 RADIUS 권한 부여 속성 (계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
Intercept-DHCP-Configure-Msg	Y	62	부울	단일	0 = Disabled 1 = Enabled
IPsec-Allow-Passwd-Store	Y	16	부울	단일	0 = Disabled 1 = Enabled
IPsec-Authentication		13	정수	단일	0 = None 1 = RADIUS 2 = LDAP(인증 전용) 3 = NT Domain 4 = SDI 5 = Internal 6 = RADIUS with Expiry 7 = Kerberos/Active Directory
IPsec-Auth-On-Rekey	Y	42	부울	단일	0 = Disabled 1 = Enabled
IPsec-Backup-Server-List	Y	60	문자열	단일	서버 주소(공백 구분)
IPsec-Backup-Servers	Y	59	문자열	단일	1 = Use Client-Configured list 2 = Disable and clear client list 3 = Use Backup Server list
IPsec-Client-Firewall-Filter-Name		57	문자열	단일	클라이언트에 방화벽 정책으로 푸시할 필터의 이름을 지정
IPsec-Client-Firewall-Filter-Optional	Y	58	정수	단일	0 = Required 1 = Optional
IPsec-Default-Domain	Y	28	문자열	단일	클라이언트로 보낼 단일 기본 도메인 이름을 지정합니다(1~255자).
IPsec-IKE-Peer-ID-Check	Y	40	정수	단일	1 = Required 2 = If supported by peer certificate 3 = Do not check
IPsec-IP-Compression	Y	39	정수	단일	0 = Disabled 1 = Enabled
IPsec-Mode-Config	Y	31	부울	단일	0 = Disabled 1 = Enabled
IPsec-Over-UDP	Y	34	부울	단일	0 = Disabled 1 = Enabled
IPsec-Over-UDP-Port	Y	35	정수	단일	4001- 49151. 기본값은 10000입니다.
IPsec-Required-Client-Firewall-Capability	Y	56	정수	단일	0 = None 1 = Policy defined by remote FW Are-You-There (AYT) 2 = Policy pushed CPP 4 = Policy from server
IPsec-Sec-Association		12	문자열	단일	보안 연결의 이름

표 29-1 지원되는 RADIUS 권한 부여 속성 (계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
IPsec-Split-DNS-Names	Y	29	문자열	단일	클라이언트로 보낼 보조 도메인 이름의 목록을 지정합니다(1~255자).
IPsec-Split-Tunneling-Policy	Y	55	정수	단일	0 = No split tunneling 1 = Split tunneling 2 = Local LAN permitted
IPsec-Split-Tunnel-List	Y	27	문자열	단일	분할 터널 포함 목록을 설명하는 네트워크 또는 ACL의 이름을 지정합니다.
IPsec-Tunnel-Type	Y	30	정수	단일	1 = LAN-to-LAN 2 = Remote access
IPsec-User-Group-Lock		33	부울	단일	0 = Disabled 1 = Enabled
IPv6-Address-Pools	Y	218	문자열	단일	IP 로컬 풀-IPv6의 이름
IPv6-VPN-Filter	Y	219	문자열	단일	ACL 가치
L2TP-Encryption		21	정수	단일	비트맵: 1 = Encryption required 2 = 40 bits 4 = 128 bits 8 = Stateless-Req 15= 40/128-Encr/Stateless-Req
L2TP-MPPC-Compression		38	정수	단일	0 = Disabled 1 = Enabled
Member-Of	Y	145	문자열	단일	쉼표로 구분된 문자열, 예: 엔지니어링, 판매 동적 액세스 정책에서 사용할 수 있는 관리 속성입니다. 이것은 그룹 정책을 설정하지 않습니다.
MS-Client-Subnet-Mask	Y	63	부울	단일	IP 주소
NAC-Default-ACL		92	문자열		ACL
NAC-Enable		89	정수	단일	0 = No 1 = 예
NAC-Revalidation-Timer		91	정수	단일	300~86400초
NAC-Settings	Y	141	문자열	단일	NAC 정책의 이름
NAC-Status-Query-Timer		90	정수	단일	30~1800초
Perfect-Forward-Secrecy-Enable	Y	88	부울	단일	0 = No 1 = 예

표 29-1 지원되는 RADIUS 권한 부여 속성 (계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
PPTP-Encryption		20	정수	단일	비트맵: 1 = Encryption required 2 = 40 bits 4 = 128 bits 8 = Stateless-Required 15= 40/128-Encr/Stateless-Req
PPTP-MPPC-Compression		37	정수	단일	0 = Disabled 1 = Enabled
Primary-DNS	Y	5	문자열	단일	IP 주소
Primary-WINS	Y	7	문자열	단일	IP 주소
Privilege-Level	Y	220	정수	단일	0과 15 사이의 정수입니다.
Required-Client- Firewall-Vendor-Code	Y	45	정수	단일	1 = Cisco Systems(Cisco Integrated Client 포함) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems(Cisco Intrusion Prevention Security Agent 포함)
Required-Client-Firewall-Description	Y	47	문자열	단일	문자열
Required-Client-Firewall-Product-Code	Y	46	정수	단일	Cisco Systems 제품: 1 = Cisco Intrusion Prevention Security Agent 또는 Cisco Integrated Client (CIC) Zone Labs 제품: 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity NetworkICE 제품: 1 = BlackIce Defender/Agent Sygate 제품: 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	정수	단일	0 = Disabled 1 = Enabled
Require-HW-Client-Auth	Y	48	부울	단일	0 = Disabled 1 = Enabled
Secondary-DNS	Y	6	문자열	단일	IP 주소
Secondary-WINS	Y	8	문자열	단일	IP 주소
SEP-Card-Assignment		9	정수	단일	사용되지 않음

표 29-1 지원되는 RADIUS 권한 부여 속성 (계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
세션 하위 유형	Y	152	정수	단일	0 = None 1 = Clientless 2 = Client 3 = Client Only 세션 하위 유형은 세션 유형(151) 속성에 1, 2, 3, 4의 값이 포함될 때만 적용됩니다.
Session Type	Y	151	정수	단일	0 = None 1 = AnyConnect Client SSL VPN 2 = AnyConnect Client IPSec VPN (IKEv2) 3 = Clientless SSL VPN 4 = Clientless Email Proxy 5 = Cisco VPN Client (IKEv1) 6 = IKEv1 LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN Load Balancing
Simultaneous-Logins	Y	2	정수	단일	0-2147483647
Smart-Tunnel	Y	136	문자열	단일	스마트 터널의 이름
Smart-Tunnel-Auto	Y	138	정수	단일	0 = Disabled 1 = Enabled 2 = AutoStart
Smart-Tunnel-Auto-Signon-Enable	Y	139	문자열	단일	도메인 이름이 추가된 스마트 터널 자동 로그인 목록의 이름
Strip-Realm	Y	135	부울	단일	0 = Disabled 1 = Enabled
SVC-Ask	Y	131	문자열	단일	0 = Disabled 1 = Enabled 3 = Enable default service 5 = Enable default clientless (2 및 4는 사용되지 않음)
SVC-Ask-Timeout	Y	132	정수	단일	5~120초
SVC-DPD-Interval-Client	Y	108	정수	단일	0 = Off 5~3600초
SVC-DPD-Interval-Gateway	Y	109	정수	단일	0 = Off) 5~3600초
SVC-DTLS	Y	123	정수	단일	0 = False 1 = True
SVC-Keepalive	Y	107	정수	단일	0 = Off 15~600초
SVC-Modules	Y	127	문자열	단일	문자열(모듈 이름)
SVC-MTU	Y	125	정수	단일	MTU 가치 256~1406바이트

표 29-1 지원되는 RADIUS 권한 부여 속성 (계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
SVC-Profiles	Y	128	문자열	단일	문자열(프로필 이름)
SVC-Rekey-Time	Y	110	정수	단일	0 = Disabled 1~10080분
터널 그룹 이름	Y	146	문자열	단일	1~253자
Tunnel-Group-Lock	Y	85	문자열	단일	터널 그룹의 이름 또는 “none”
Tunneling-Protocols	Y	11	정수	단일	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 8과 4는 함께 사용할 수 없습니다. 0 - 11, 16 - 27, 32 - 43, 48 - 59는 올바른 값입니다.
Use-Client-Address		17	부울	단일	0 = Disabled 1 = Enabled
VLAN	Y	140	정수	단일	0-4094
WebVPN-Access-List	Y	73	문자열	단일	Access-List 이름
WebVPN ACL	Y	73	문자열	단일	디바이스의 WebVPN ACL 이름
WebVPN-ActiveX-Relay	Y	137	정수	단일	0 = Disabled Otherwise = Enabled
WebVPN-Apply-ACL	Y	102	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Auto-HTTP-Signon	Y	124	문자열	단일	예약
WebVPN-Citrix-Metaframe-Enable	Y	101	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Content-Filter-Parameters	Y	69	정수	단일	1 = Java ActiveX 2 = Java Script 4 = Image 8 = Cookies in images
WebVPN-Customization	Y	113	문자열	단일	사용자 정의의 이름
WebVPN-Default-Homepage	Y	76	문자열	단일	http://example-example.com과 같은 URL
WebVPN-Deny-Message	Y	116	문자열	단일	올바른 문자열(최대 500 자)
WebVPN-Download_Max-Size	Y	157	정수	단일	0x7fffffff
WebVPN-File-Access-Enable	Y	94	정수	단일	0 = Disabled 1 = Enabled
WebVPN-File-Server-Browsing-Enable	Y	96	정수	단일	0 = Disabled 1 = Enabled

표 29-1 지원되는 RADIUS 권한 부여 속성 (계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
WebVPN-File-Server-Entry-Enable	Y	95	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	Y	78	문자열	단일	와일드카드(*) 옵션을 포함한 쉼표로 구분된 DNS/IP(예: *.cisco.com, 192.168.1.*, wwwin.cisco.com)
WebVPN-Hidden-Shares	Y	126	정수	단일	0 = None 1 = Visible
WebVPN-Home-Page-Use-Smart-Tunnel	Y	228	부울	단일	클라이언트리스 홈페이지가 스마트 터널을 통해 만들어지는 경우 활성화됩니다.
WebVPN-HTML-Filter	Y	69	비트맵	단일	1 = Java ActiveX 2 = Scripts 4 = Image 8 = Cookies
WebVPN-HTTP-Compression	Y	120	정수	단일	0 = Off 1 = Deflate Compression
WebVPN-HTTP-Proxy-IP-Address	Y	74	문자열	단일	http= 또는 https= 접두사를 포함한 쉼표로 구분된 DNS/IP:port(예: http=10.10.10.10:80, https=11.11.11.11:443)
WebVPN-Idle-Timeout-Alert-Interval	Y	148	정수	단일	0-30. 0 = Disabled.
WebVPN-Keepalive-Ignore	Y	121	정수	단일	0-900
WebVPN-Macro-Substitution	Y	223	문자열	단일	무제한. 다음 URL의 *SSL VPN 배포 가이드*에서 예제를 참조하십시오. http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Macro-Substitution	Y	224	문자열	단일	무제한. 다음 URL의 *SSL VPN 배포 가이드*에서 예제를 참조하십시오. http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html
WebVPN-Port-Forwarding-Enable	Y	97	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	정수	단일	0 = Disabled 1 = Enabled
WebVPN-Port-Forwarding-List	Y	72	문자열	단일	포트 전달 목록 이름

표 29-1 지원되는 RADIUS 권한 부여 속성 (계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
WebVPN-Port-Forwarding-Name	Y	79	문자열	단일	문자열 이름(예: “Corporate-Apps”). 이 텍스트는 클라이언트리스 포털 홈페이지에서 기본 문자열인 “Application Access”를 대체합니다.
WebVPN-Post-Max-Size	Y	159	정수	단일	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	정수	단일	0-30. 0 = Disabled.
WebVPN Smart-Card-Removal-Disconnect	Y	225	부울	단일	0 = Disabled 1 = Enabled
WebVPN-Smart-Tunnel	Y	136	문자열	단일	스마트 터널의 이름
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	문자열	단일	도메인 이름이 추가된 스마트 터널 자동 로그인 목록의 이름
WebVPN-Smart-Tunnel-Auto-Start	Y	138	정수	단일	0 = Disabled 1 = Enabled 2 = Auto Start
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	문자열	단일	“e networkname,” “i networkname,” 또는 “a” 중 하나로 여기서 networkname은 Smart Tunnel 네트워크 목록의 이름을, e는 제외된 터널을, i는 지정된 터널을, a는 모든 터널을 나타냅니다.
WebVPN-SSL-VPN-Client-Enable	Y	103	정수	단일	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Keep-Installation	Y	105	정수	단일	0 = Disabled 1 = Enabled
WebVPN-SSL-VPN-Client-Required	Y	104	정수	단일	0 = Disabled 1 = Enabled
WebVPN-SSO-Server-Name	Y	114	문자열	단일	올바른 문자열
WebVPN-Storage-Key	Y	162	문자열	단일	
WebVPN-Storage-Objects	Y	161	문자열	단일	
WebVPN-SVC-Keepalive-Frequency	Y	107	정수	단일	15~600초, 0=Off
WebVPN-SVC-Client-DPD-Frequency	Y	108	정수	단일	5~3600초, 0=Off
WebVPN-SVC-DTLS-Enable	Y	123	정수	단일	0 = Disabled 1 = Enabled
WebVPN-SVC-DTLS-MTU	Y	125	정수	단일	MTU 값은 256~1406바이트입니다.
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	정수	단일	5~3600초, 0=Off
WebVPN-SVC-Rekey-Time	Y	110	정수	단일	4~10080분, 0=Off
WebVPN-SVC-Rekey-Method	Y	111	정수	단일	0 (Off), 1 (SSL), 2 (New Tunnel)
WebVPN-SVC-Compression	Y	112	정수	단일	0 (Off), 1 (Deflate Compression)
WebVPN-UNIX-Group-ID (GID)	Y	222	정수	단일	유효한 UNIX 그룹 ID

표 29-1 지원되는 RADIUS 권한 부여 속성 (계속)

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
WebVPN-UNIX-User-ID (UIDs)	Y	221	정수	단일	유효한 UNIX 사용자 ID
WebVPN-Upload-Max-Size	Y	158	정수	단일	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	정수	단일	0 = Disabled 1 = Enabled
WebVPN-URL-List	Y	71	문자열	단일	URL 목록 이름
WebVPN-User-Storage	Y	160	문자열	단일	
WebVPN-VDI	Y	163	문자열	단일	설정 목록

지원되는 IETF RADIUS 권한 부여 속성

표 29-2은(는) 지원되는 IETF RADIUS 속성을 나열합니다.

표 29-2 지원되는 IETF RADIUS 속성

속성 이름	ASA	Attr. 번호	Syntax/ Type	Single or Multi-Valued	Description or Value
IETF-Radius-Class	Y	25		단일	버전 8.2.x 이상에서는 표 29-1의 설명대로 Group-Policy 속성(VSA 3076, #25)을 사용하십시오. • *group policy name* • OU=*group policy name* • OU=*group policy name*
IETF-Radius-Filter-Id	Y	11	문자열	단일	ASA에 정의된 ACL 이름으로 풀 터널 IPsec 및 SSL VPN 클라이언트에만 적용됩니다.
IETF-Radius-Framed-IP-Address	Y	N/A	문자열	단일	IP 주소
IETF-Radius-Framed-IP-Netmask	Y	N/A	문자열	단일	IP 주소 마스크
IETF-Radius-Idle-Timeout	Y	28	정수	단일	초
IETF-Radius-Service-Type	Y	6	정수	단일	초 사용 가능한 서비스 유형 값: • .Administrative—사용자에게 구성 프롬프트 액세스가 허용됩니다. • .NAS-Prompt—사용자에게 실행 프롬프트 액세스가 허용됩니다. • .remote-access—사용자에게 네트워크 액세스가 허용됩니다.
IETF-Radius-Session-Timeout	Y	27	정수	단일	초

RADIUS 어카운팅 연결 종료 사유 코드

이 코드는 ASA가 패킷 전송 중 연결이 끊길 때 반환됩니다.

연결 종료 사유 코드
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

RADIUS 서버의 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

IPv6를 지원합니다.

추가 지침

- 단일 모드로 최대 100개의 서버 그룹 또는 다중 모드로 컨텍스트당 4개의 서버 그룹을 포함할 수 있습니다.
- 각 그룹은 단일 모드에서 최대 16개의 서버 또는 다중 모드에서 4대의 서버를 포함할 수 있습니다.
- 로컬 데이터베이스를 이용하여 폴백 지원을 구성해야 하는 경우 28-2 페이지의 폴백(Fallback) 지원 및 28-2 페이지의 그룹의 여러 서버에서 폴백이 작동하는 방식을(를) 참조하십시오.
- RADIUS 인증을 이용할 때 ASA에서 잠금을 방지하려면 36-28 페이지의 잠금에서 복구을(를) 참조하십시오.

RADIUS 서버 구성

RADIUS 서버 구성을 위한 작업 흐름

1단계 RADIUS 서버로 ASA 속성을 로드합니다. 속성을 로드하는 데 사용하는 방법은 사용하는 RADIUS 서버 유형에 따라 다릅니다.

- Cisco ACS를 사용하는 경우: 서버에 이미 이러한 속성이 통합되어 있습니다. 이 단계를 건너뛸 수 있습니다.
- 다른 공급업체의 RADIUS 서버(예: Microsoft Internet Authentication Service): 각 ASA 속성을 수동으로 정의해야 합니다. 속성을 정의하려면 속성 이름 또는 번호, 유형, 값 및 공급업체 코드(3076)를 사용합니다.

2단계 RADIUS 서버 그룹을 추가합니다. 29-15 페이지의 RADIUS 서버 그룹 구성를 참조하십시오.

3단계 서버 그룹의 경우 그룹에 서버를 추가합니다. 29-16 페이지의 그룹에 RADIUS 서버 추가를 참조하십시오.

4단계 (선택 사항) AAA 인증 질문 과정에서 사용자에게 표시할 텍스트를 지정합니다. 29-18 페이지의 인증 프롬프트 추가를 참조하십시오.

RADIUS 서버 그룹 구성

인증, 권한 부여 또는 어카운팅을 위해 외부 RADIUS 서버를 사용하려면 먼저 RADIUS 프로토콜당 최소 1개의 AAA 서버 그룹을 만들고 하나 이상의 서버를 각 그룹에 추가해야 합니다. AAA 서버 그룹은 이름으로 구분합니다.

RADIUS 서버 그룹을 추가하려면 다음 단계를 수행하십시오.

세부 단계

1단계 **Configuration > Device Management > Users/AAA > AAA Server Groups**를 선택합니다.

2단계 AAA Server Groups 영역에서 **Add**를 클릭합니다.

Add AAA Server Group 대화 상자가 나타납니다.

3단계 서버 그룹 필드에 그룹 이름을 입력합니다.

4단계 Protocol 드롭다운 목록에서 RADIUS 서버 유형을 선택합니다.

5단계 Accounting Mode 필드에서 **Simultaneous** 또는 **Single**을 클릭합니다.

Single 모드에서는 ASA이(가) 어카운팅 데이터를 하나의 서버로만 전송합니다.

Simultaneous 모드에서는 ASA이(가) 어카운팅 데이터를 그룹의 모든 서버로 전송합니다.

6단계 Reactivation Mode 필드에서 **Depletion** 또는 **Timed**를 클릭합니다.

Depletion 모드에서는 그룹의 모든 서버가 비활성 상태가 되어야 실패한 서버가 재활성화됩니다.

Timed 모드에서는 가동 중단 후 30초가 지나면 실패한 서버가 재활성화됩니다.

7단계 Depletion 재활성화 모드를 선택한 경우 Dead Time 필드에 시간 간격을 입력합니다.

Dead Time은 그룹의 마지막 서버가 비활성화된 시점부터 나중에 모든 서버가 다시 활성화된 시점까지 경과한 시간(분)입니다.

8단계 Max Failed Attempts 필드에 허용할 시도 실패 횟수를 입력합니다.

이 옵션은 무응답 서버를 비활성 상태로 선언하기 전에 허용되는 연결 실패 횟수를 설정합니다.

9단계 (선택 사항) RADIUS 서버 유형을 추가하는 경우 다음 단계를 수행하십시오.

a. 클라이언트리스 SSL 및 AnyConnect 세션을 위한 멀티 세션 어카운팅을 활성화하려면 **Enable interim accounting update** 확인란을 선택하십시오.

b. **Enable Active Directory Agent Mode** 확인란을 선택하여 ASA 및 AD 에이전트 사이의 공유 비밀번호를 지정하고 RADIUS 서버 그룹이 전체-기능 RADIUS 서버가 아닌 AD 에이전트를 포함함을 나타냅니다. 이 옵션을 사용하여 구성된 RADIUS 서버 그룹만 사용자 ID에 연결될 수 있습니다.

c. **Enable dynamic authorization** 확인란을 선택하여 ISE가 CoA(Change of Authorization) RADIUS 패킷을 활성화합니다. 이를 통해 ISE의 정책 변경 사항을 VPN 연결 수명 동안 적용할 수 있습니다.

d. **Dynamic Authorization Port**를 입력합니다. 이 포트는 RADIUS CoA 요청에 대한 리스닝 포트입니다. 일반적으로 1700입니다. 범위는 1에서 65535까지입니다.

e. **Use authorize only mode** 확인란을 선택하여 RADIUS 서버 그룹에 대한 authorize-only 모드를 활성화합니다. 이 확인란이 선택된 경우 개별 AAA 서버에 대해 구성된 공통 비밀번호가 필요 없으며 구성하지 않아도 됩니다.

f. **VPN3K Compatibility Option** 아래쪽 화살표를 클릭하여 목록을 확장하고 다음 옵션 중 하나를 클릭하여 RADIUS 패킷에서 수신된 다운로드 가능한 ACL을 Cisco AV 쌍 ACL과 병합할지 지정합니다.

- **병합 안 함**
- **다운로드 가능 ACL을 Cisco AV 쌍 ACL 뒤에 배치**
- **다운로드 가능 ACL을 Cisco AV 쌍 ACL 앞에 배치**

10단계 **OK**를 클릭합니다.

Add AAA Server Group 대화 상자가 닫히고 새 서버 그룹이 AAA Server Groups 테이블에 추가됩니다.

11단계 AAA Server Groups 대화 상자에서 **Apply**를 클릭하여 변경 사항을 실행 중인 컨피그레이션에 저장합니다.

그룹에 RADIUS 서버 추가

RADIUS 서버를 그룹에 추가하려면 다음 단계를 수행하십시오.

세부 단계

1단계 **Configuration > Device Management > Users/AAA > AAA Server Groups**를 선택하고 AAA Server Groups 영역에서 서버를 추가할 서버 그룹을 클릭합니다.

테이블에서 행이 강조 표시됩니다.

2단계 Servers in the Selected Group 영역(하단 창)에서 **Add**를 클릭합니다.

서버 그룹에 대한 Add AAA Server Group 대화 상자가 나타납니다.

3단계 Interface Name 드롭다운 목록에서 인증 서버가 상주하는 인터페이스 이름을 선택합니다.

4단계 Server Name 또는 IP Address 필드에 그룹에 추가하려는 서버의 서버 이름이나 IP 주소를 추가합니다.

5단계 Timeout 필드에서 시간 초과 값을 추가하거나 기본값을 유지합니다. timeout은 ASA이(가) 백업 서버로 요청을 보내기 전에 기본 서버에서 응답을 기다리는 시간(초)입니다.

6단계 ACL Netmask Convert 필드에 다운로드 가능한 ACL에서 수신된 넷마스크를 ASA이(가) 어떻게 처리할지 지정하십시오. 다음 옵션 중에서 선택합니다.

- Detect automatically—ASA이(가) 사용된 넷마스크의 유형 파악을 시도합니다. ASA이(가) 와일드카드 넷마스크 표현을 감지하면 ASA이(가) 이를 표준 넷마스크 표현으로 변환합니다.

  참고 일부 와일드카드 표현은 명확한 감지가 어렵기 때문에 이 설정은 와일드카드 넷마스크 표현을 표준 넷마스크 표현으로 잘못 해석할 수 있습니다.

- Standard—ASA이(가) RADIUS에서 수신된 다운로드 가능 ACL이 표준 넷마스크 표현만 포함한다고 가정합니다. 와일드카드 넷마스크 표현에 대한 변환이 이루어지지 않습니다.
- Wildcard—ASA이(가) RADIUS 서버에서 수신된 다운로드 가능 ACL이 와일드카드 넷마스크 표현만 포함한다고 가정하고 ACL이 다운로드될 때 이를 모두 표준 넷마스크 표현으로 변환합니다.

7단계 Common Password 필드에 이 ASA을(를) 통해 RADIUS 권한 부여 서버에 액세스하는 사용자 간에 공통된 대/소문자를 구분하는 비밀번호를 지정합니다. 이 정보를 RADIUS 서버 관리자에게 이 정보를 제공해야 합니다.

참고 인증 RADIUS 서버(권한 부여 아님)의 경우 공통 비밀번호를 구성하지 마십시오.

이 필드를 공백으로 두면 사용자 이름이 이 RADIUS 권한 부여 서버에 액세스하기 위한 비밀번호가 됩니다.

RADIUS 권한 부여 서버를 인증에 사용하지 마십시오. 공통 비밀번호 또는 비밀번호를 사용자 이름으로 사용하는 것은 고유한 사용자 비밀번호 할당보다 보안 수준이 낮습니다.

RADIUS 프로토콜 및 RADIUS 서버는 비밀번호를 요구하지만 사용자가 이를 알 필요는 없습니다.

8단계 터널 그룹에서 이중 인증을 사용하고 비밀번호 관리를 활성화하는 경우 기본 및 보조 인증 요청은 MS-CHAPv2 요청 속성을 포함합니다. RADIUS 서버가 MS-CHAPv2를 지원하지 않는 경우 이 확인란 선택을 취소하여 서버가 non-MS-CHAPv2 인증 요청을 보내도록 구성할 수 있습니다.

9단계 Retry Interval 필드에 ASA이(가) 서버 연락 시도 사이에 대기할 시간 간격을 1~10초로 지정합니다.

참고 다음 재시도까지의 간격은 입력한 재시도 간격 설정과 무관하게 항상 50 또는 100밀리초입니다. 이것은 의도된 것입니다.

10단계 Accounting Mode 필드에서 **Simultaneous** 또는 **Single**을 클릭합니다.

Single 모드에서는 ASA이(가) 어카운팅 데이터를 하나의 서버로만 전송합니다.

Simultaneous 모드에서는 ASA이(가) 어카운팅 데이터를 그룹의 모든 서버로 전송합니다.

11단계 Server Accounting Port 필드에 사용자 어카운팅에 사용할 서버 포트를 지정합니다. 기본 포트는 1646입니다.

12단계 Server Authentication Port 필드에 사용자 인증에 사용할 서버 포트를 지정합니다. 기본 포트는 1645입니다.

13단계 Server Secret Key 필드에 RADIUS 서버를 ASA에 인증하는 데 사용되는 공유 비밀 키를 지정합니다. 서버 비밀번호는 RADIUS 서버에서 구성한 것과 일치해야 합니다. 서버 비밀번호를 모르는 경우 RADIUS 서버 관리자에게 문의하십시오. 최대 필드 길이는 64자입니다.

14단계 **OK**를 클릭합니다.

Add AAA Server Group 대화 상자가 닫히고 AAA 서버가 AAA 서버 그룹에 추가됩니다.

15단계 AAA Server Groups 창에서 **Apply**를 클릭하여 변경 사항을 실행 중인 컨피그레이션에 저장합니다.

인증 프롬프트 추가

RADIUS 서버로부터의 사용자 인증을 요구할 때 ASA을(를) 통해 HTTP, FTP 및 텔넷 액세스에 대한 AAA 챌린지 텍스트를 지정할 수 있습니다. 이 텍스트는 기본적으로 장식용으로 사용자가 로그인할 때 사용자 이름과 비밀번호 프롬프트 위에 표시됩니다. 인증 프롬프트를 지정하지 않으면 RADIUS 서버에서 인증할 때 사용자에게 다음이 표시됩니다.

연결 유형	기본 프롬프트
FTP	FTP 인증
HTTP	HTTP 인증
텔넷	없음

인증 프롬프트를 추가하려면 다음 단계를 수행하십시오.

1단계 Configuration > Device Management > Users/AAA > Authentication Prompt 창의 Prompt 필드에 사용자가 로그인할 때 사용자 이름 및 비밀번호 프롬프트 위에 메시지로 표시할 텍스트를 입력합니다.

다음 표는 인증 프롬프트에서 허용되는 문자 수를 보여줍니다.

애플리케이션	최대 허용 문자 수
Microsoft Internet Explorer	37
텔넷	235
FTP	235

2단계 메시지 영역에서 사용자 동의함 메시지와 사용자 거부함 메시지 필드에 메시지를 추가합니다.

사용자 인증이 텔넷에서 발생하는 경우 사용자 승인 메시지와 사용자 거부 메시지 옵션을 사용하여 서로 다른 상태 프롬프트를 표시함으로써 RADIUS 서버에서 인증 시도가 승인되었는지 혹은 거부되었는지 나타낼 수 있습니다.

RADIUS 서버가 사용자를 인증할 경우 ASA은(는) 사용자 승인됨 메시지(지정된 경우)를 사용자에게 표시하고 그렇지 않을 경우 ASA은(는) 사용자 거부됨 메시지를 표시합니다. HTTP 및 FTP 세션 인증은 프롬프트에서 챌린지 텍스트만 표시합니다. 사용자 승인 메시지와 사용자 거부 메시지 텍스트는 표시되지 않습니다.

3단계 **Apply**를 클릭하여 실행 중인 컨피그레이션에 변경 사항을 저장합니다.

RADIUS 서버 인증 및 권한 부여 테스트

ASA이(가) RADIUS 서버에 접속하고 사용자를 인증하거나 권한을 부여할 수 있는지 결정하려면 다음 단계를 수행하십시오.

1단계 Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups 테이블에서 서버가 상주하는 서버 그룹을 클릭합니다.

테이블에서 행이 강조 표시됩니다.

2단계 Selected Group 테이블의 서버 중에서 테스트할 서버를 클릭합니다.

테이블에서 행이 강조 표시됩니다.

3단계 **Test**를 클릭합니다.

선택된 서버에 대한 Test AAA Server 대화 상자가 나타납니다.

4단계 수행할 테스트 유형 **Authentication** 또는 **Authorization**을 클릭합니다.

5단계 Username 필드에 사용자 이름을 입력합니다.

6단계 인증을 테스트하는 경우 비밀번호 필드에 사용자 이름에 대한 비밀번호를 입력합니다.

7단계 **OK**를 클릭합니다.

ASA에서 인증 또는 권한 부여 테스트 메시지를 서버에 전송합니다. 테스트가 실패한 경우 ASDM는 오류 메시지를 표시합니다.

RADIUS 서버 모니터링

RADIUS 서버를 모니터링하려면 다음 창을 참조하십시오.

Path	목적
Monitoring > Properties > AAA Servers	구성된 RADIUS 서버 통계를 보여줍니다.
Monitoring > Properties > AAA Servers	컨피그레이션을 실행 중인 RADIUS 서버를 보여줍니다.

추가 참조 자료

RADIUS 서버를 통한 AAA 구현에 관한 추가 정보는 29-19 페이지의 RFC에서 참조하십시오.

RFC

RFC	제목
2138	*원격 인증 다이얼-인 사용자 서비스(RADIUS)*
2139	*RADIUS 어카운팅*
2548	*Microsoft 공급업체별 RADIUS 속성*
2868	*터널 프로토콜 지원을 위한 RADIUS 속성*

RADIUS 서버에 대한 기능 내역

표 29-3에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 29-3 RADIUS 서버에 대한 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
AAA를 위한 RADIUS 서버	7.0(1)	AAA에 대한 RADIUS 서버를 구성하는 방법을 설명합니다. 다음 화면을 도입했습니다. Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > Authentication Prompt.
ASA에서 RADIUS 액세스 요청 및 어카운팅 요청 패킷으로 전송되는 주요 VSA(vendor-specific attribute)	8.4(3)	4개의 새로운 VSA—Tunnel Group Name (146) 및 Client Type (150)은 ASA에서 RADIUS 액세스 요청 패킷으로 전송됩니다. Session Type (151) 및 Session Subtype (152)은 ASA에서 RADIUS 어카운팅 요청 패킷으로 전송됩니다. 4가지 속성은 모두 모든 어카운팅 요청 패킷 유형(Start, Interim-Update 및 Stop)에 대해 전송됩니다. 그러면 RADIUS 서버(예: ACS 및 ISE)가 권한 부여 또는 정책 속성을 시행하거나 이를 어카운팅 및 청구 목적으로 사용할 수 있습니다.

30장

AAA용 TACACS+ 서버

이 장에서는 AAA에서 사용되는 TACACS+ 서버 구성 방법을 설명합니다.

TACACS+ 서버에 관한 정보

ASA은(는) ASCII, PAP, CHAP 및 MS-CHAPv1 프로토콜을 통한 TACACS+ 서버 인증을 지원합니다.

TACACS+ 속성 사용

Cisco ASA 은(는) TACACS+ 속성을 지원합니다. TACACS+ 속성은 인증, 권한 부여 및 어카운팅 기능을 분리합니다. 이 프로토콜은 필수 및 선택의 두 가지 속성 유형을 지원합니다. 서버와 클라이언트가 모두 필수 속성을 이해해야 하고 필수 속성이 사용자에게 적용되어야 합니다. 선택 속성은 이해 또는 사용될 수도 있고 그렇지 않을 수도 있습니다.

참고 TACACS+ 속성을 사용하려면 NAS에서 AAA 서비스를 활성화해야 합니다.

표 30-1은(는) cut-through-proxy 연결을 위한 지원되는 TACACS+ 권한 부여 응답 속성을 나열합니다. 표 30-2은(는) 지원되는 TACACS+ 어카운팅 속성을 나열합니다.

표 30-1 지원되는 TACACS+ 권한 부여 응답 속성

특성	설명
ACL	연결에 적용할 로컬로 구성된 ACL을 식별합니다.
idletime	비활성 상태가 몇 분간 지속되면 인증된 사용자 세션을 종료할지 나타냅니다.
timeout	인증된 사용자 세션을 종료하기 전에 인증 자격 증명을 활성 상태로 유지할 절대적인 시간(분)을 지정합니다.

표 30-2 지원되는 TACACS+ 어카운팅 속성

특성	설명
bytes_in	이 연결 중에 전송된 입력 바이트의 수를 지정합니다(중단 레코드만 해당).
bytes_out	이 연결 중에 전송된 출력 바이트의 수를 지정합니다(중단 레코드만 해당).
cmd	실행되는 명령을 정의합니다(명령 어카운팅만 해당).
disc-cause	연결이 끊긴 원인을 식별하는 숫자 코드를 나타냅니다(중단 레코드만 해당).
elapsed_time	연결에 대한 경과 시간을 초로 정의합니다(중단 레코드만 해당).
foreign_ip	터널 연결을 위한 클라이언트의 IP 주소를 지정합니다. cut-through-proxy 연결을 위한 가장 낮은 수준의 보안 인터페이스 주소를 정의합니다.
local_ip	클라이언트가 터널 연결을 위해 연결된 IP 주소를 지정합니다. cut-through-proxy 연결을 위한 가장 높은 수준의 보안 인터페이스 주소를 정의합니다.
NAS 포트	해당 연결을 위한 세션 ID를 포함합니다.
packs_in	이 연결 중에 전송되는 입력 패킷의 수를 지정합니다.
packs_out	이 연결 중에 전송되는 출력 패킷의 수를 지정합니다.
priv-level	명령 어카운팅 요청에 대한 사용자 권한 수준으로 설정합니다. 아니면 1로 설정됩니다.
rem_iddr	클라이언트의 IP 주소를 나타냅니다.
제공	사용하는 서비스를 지정합니다. 명령 어카운팅에 한해 항상 “shell”로 설정합니다.
task_id	어카운팅 거래에 대한 고유한 작업 ID를 지정합니다.
username	사용자의 이름을 나타냅니다.

TACACS+ 서버의 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

IPv6를 지원합니다.

추가 지침

- 단일 모드로 최대 100개의 서버 그룹 또는 다중 모드로 컨텍스트당 4개의 서버 그룹을 포함할 수 있습니다.
- 각 그룹은 단일 모드에서 최대 16개의 서버 또는 다중 모드에서 4대의 서버를 포함할 수 있습니다.
- 로컬 데이터베이스를 이용하여 폴백 지원을 구성해야 하는 경우 28-2 페이지의 폴백(Fallback) 지원 및 28-2 페이지의 그룹의 여러 서버에서 폴백이 작동하는 방식을(를) 참조하십시오.
- TACACS+ 인증 또는 권한 부여를 이용할 때 ASA에서 잠금을 방지하려면 36-28 페이지의 잠금에서 복구을(를) 참조하십시오.

TACACS+ 서버 구성

TACACS+ 서버 구성을 위한 작업 흐름

1단계 TACACS+ 서버 그룹을 추가합니다. 30-4 페이지의 TACACS+ 서버 그룹 구성를 참조하십시오.

2단계 서버 그룹의 경우 그룹에 서버를 추가합니다. 30-4 페이지의 그룹에 TACACS+ 서버 추가를 참조하십시오.

3단계 (선택 사항) AAA 인증 질문 과정에서 사용자에게 표시할 텍스트를 지정합니다. 30-5 페이지의 인증 프롬프트 추가를 참조하십시오.

TACACS+ 서버 그룹 구성

인증, 권한 부여 또는 어카운팅을 위해 TACACS+ 서버를 사용하려면 먼저 1개 이상의 TACACS+ 서버 그룹을 생성하고 각 그룹에 하나 이상의 서버를 추가해야 합니다. TACACS+ 서버 그룹은 이름으로 구분합니다.

TACACS+ 서버 그룹을 추가하려면 다음 단계를 수행하십시오.

세부 단계

1단계 **Configuration > Device Management > Users/AAA > AAA Server Groups**를 선택합니다.

2단계 AAA Server Groups 영역에서 **Add**를 클릭합니다.

Add AAA Server Group 대화 상자가 나타납니다.

3단계 서버 그룹 필드에 그룹 이름을 입력합니다.

4단계 프로토콜 드롭다운 목록에서 TACACS+ 서버 유형을 선택합니다.

5단계 Accounting Mode 필드에서 **Simultaneous** 또는 **Single**을 클릭합니다.

Single 모드에서는 ASA이(가) 어카운팅 데이터를 하나의 서버로만 전송합니다.

Simultaneous 모드에서는 ASA이(가) 어카운팅 데이터를 그룹의 모든 서버로 전송합니다.

6단계 Reactivation Mode 필드에서 **Depletion** 또는 **Timed**를 클릭합니다.

Depletion 모드에서는 그룹의 모든 서버가 비활성 상태가 되어야 실패한 서버가 재활성화됩니다.

Timed 모드에서는 가동 중단 후 30초가 지나면 실패한 서버가 재활성화됩니다.

7단계 Depletion 재활성화 모드를 선택한 경우 Dead Time 필드에 시간 간격을 입력합니다.

Dead Time은 그룹의 마지막 서버가 비활성화된 시점부터 나중에 모든 서버가 다시 활성화된 시점까지 경과한 시간(분)입니다.

8단계 Max Failed Attempts 필드에 허용할 시도 실패 횟수를 입력합니다.

이 옵션은 무응답 서버를 비활성 상태로 선언하기 전에 허용되는 연결 실패 횟수를 설정합니다.

9단계 **OK**를 클릭합니다.

Add AAA Server Group 대화 상자가 닫히고 새 서버 그룹이 AAA Server Groups 테이블에 추가됩니다.

10단계 AAA Server Groups 대화 상자에서 **Apply**를 클릭하여 변경 사항을 실행 중인 컨피그레이션에 저장합니다.

그룹에 TACACS+ 서버 추가

TACACS+ 서버를 그룹에 추가하려면 다음 단계를 수행하십시오.

세부 단계

1단계 **Configuration > Device Management > Users/AAA > AAA Server Groups**를 선택하고 AAA Server Groups 영역에서 서버를 추가할 서버 그룹을 클릭합니다.

테이블에서 행이 강조 표시됩니다.

2단계 Servers in the Selected Group 영역(하단 창)에서 **Add**를 클릭합니다.

서버 그룹에 대한 Add AAA Server Group 대화 상자가 나타납니다.

3단계 Interface Name 드롭다운 목록에서 인증 서버가 상주하는 인터페이스 이름을 선택합니다.

4단계 Server Name 또는 IP Address 필드에 그룹에 추가하려는 서버의 서버 이름이나 IP 주소를 추가합니다.

5단계 Timeout 필드에서 시간 초과 값을 추가하거나 기본값을 유지합니다. 시간 초과는 ASA에서 백업 서버에 요청을 보내기 전에 기본 서버의 응답을 기다리는 시간(초)입니다.

6단계 서버 포트를 지정하십시오. 서버 포트는 포트 번호 139이거나 ASA에서 TACACS+ 서버와 통신에 사용하는 TCP 포트입니다.

7단계 서버 비밀 키를 지정하십시오. TACACS+ 서버를 ASA에서 인증하는 데 사용되는 공유 비밀 키입니다. 여기서 구성하는 서버 비밀이 TACACS+ 서버에서 구성된 것과 일치해야 합니다. 서버 비밀을 모르는 경우 TACACS+ 서버 관리자에게 문의하십시오. 최대 필드 길이는 64자입니다.

8단계 **OK**를 클릭합니다.

Add AAA Server Group 대화 상자가 닫히고 AAA 서버가 AAA 서버 그룹에 추가됩니다.

9단계 AAA Server Groups 창에서 **Apply**를 클릭하여 변경 사항을 실행 중인 컨피그레이션에 저장합니다.

인증 프롬프트 추가

과제 AAA 인증 과정에서 사용자에게 표시할 텍스트를 지정할 수 있습니다. TACACS+ 서버로부터의 사용자 인증을 요구할 때 ASA을(를) 통해 HTTP, FTP 및 텔넷 액세스에 대한 AAA 챌린지 텍스트를 지정할 수 있습니다. 이 텍스트는 기본적으로 장식용으로 사용자가 로그인할 때 사용자 이름과 비밀번호 프롬프트 위에 표시됩니다.

인증 프롬프트를 지정하지 않으면 TACACS+ 서버에서 인증할 때 사용자에게 다음이 표시됩니다.

연결 유형	기본 프롬프트
FTP	FTP 인증
HTTP	HTTP 인증
텔넷	없음

인증 프롬프트를 추가하려면 다음 단계를 수행하십시오.

1단계 **Configuration > Device Management > Users/AAA > Authentication Prompt.를 선택합니다.**

2단계 프롬프트 필드에 텍스트를 입력하여 사용자가 로그인하면 사용자 이름과 비밀번호 프롬프트 위에 표시할 메시지로 추가합니다.

다음 표는 인증 프롬프트에서 허용되는 문자 수를 보여줍니다.

애플리케이션	인증 프롬프트 문자 제한
Microsoft Internet Explorer	37
텔넷	235
FTP	235

3단계 메시지 영역에서 사용자 동의함 메시지와 사용자 거부함 메시지 필드에 메시지를 추가합니다.

사용자 인증이 텔넷에서 발생하는 경우 사용자 승인 메시지와 사용자 거부 메시지 옵션을 사용하여 서로 다른 상태 프롬프트를 표시함으로써 AAA 서버에서 인증 시도가 승인되었는지 혹은 거부되었는지 나타낼 수 있습니다.

AAA 서버가 사용자를 인증할 경우 ASA은(는) 사용자 승인됨 메시지(지정된 경우)를 사용자에게 표시하고 그렇지 않을 경우 ASA은(는) 사용자 거부됨 메시지를 표시합니다. HTTP 및 FTP 세션 인증은 프롬프트에서 챌린지 텍스트만 표시합니다. 사용자 승인 메시지와 사용자 거부 메시지 텍스트는 표시되지 않습니다.

4단계 **Apply**를 클릭하여 실행 중인 컨피그레이션에 변경 사항을 저장합니다.

TACACS+ 서버 인증 및 권한 부여 테스트

ASA이(가) TACACS+ 서버에 접속하고 사용자를 인증하거나 권한을 부여할 수 있는지 결정하려면 다음 단계를 수행하십시오.

1단계 Configuration > Device Management > Users/AAA > AAA Server Groups > AAA Server Groups 테이블에서 서버가 상주하는 서버 그룹을 클릭합니다.

테이블에서 행이 강조 표시됩니다.

2단계 Selected Group 테이블의 서버 중에서 테스트할 서버를 클릭합니다.

테이블에서 행이 강조 표시됩니다.

3단계 **Test**를 클릭합니다.

선택된 서버에 대한 Test AAA Server 대화 상자가 나타납니다.

4단계 수행할 테스트 유형 **Authentication** 또는 **Authorization**을 클릭합니다.

5단계 Username 필드에 사용자 이름을 입력합니다.

6단계 인증을 테스트하는 경우 비밀번호 필드에 사용자 이름에 대한 비밀번호를 입력합니다.

7단계 **OK**를 클릭합니다.

ASA에서 인증 또는 권한 부여 테스트 메시지를 서버에 전송합니다. 테스트가 실패한 경우 ASDM는 오류 메시지를 표시합니다.

TACACS+ 서버 모니터링

TACACS+ 서버를 모니터링하려면 다음 창을 참조하십시오.

Path	목적
Monitoring > Properties > AAA Servers	구성된 TACACS+ 서버 통계를 보여줍니다.
Monitoring > Properties > AAA Servers	컨피그레이션을 실행 중인 TACACS+ 서버를 보여줍니다.

TACACS+ 서버에 대한 기능 내역

표 30-3에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 30-3 TACACS+ 서버에 대한 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
TACACS+ 서버	7.0(1)	AAA에 대한 TACACS+ 서버를 구성하는 방법을 설명합니다. 다음 화면을 도입했습니다. Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > Authentication Prompt.

31 장

AAA를 위한 LDAP 서버

이 장에서는 AAA에서 사용되는 LDAP 서버의 구성 방법을 설명합니다.

LDAP 및 AAA에 대한 정보

Cisco ASA는 다음을 포함하여 대부분의 LDAPv3 디렉토리 서버와 호환됩니다.

- Sun Microsystems JAVA System Directory Server - 현재는 Oracle Directory Server Enterprise Edition에 포함됨. 이전 이름은 Sun ONE Directory Server
- Microsoft Active Directory
- Novell
- OpenLDAP

기본적으로 ASA는 Microsoft Active Directory, Sun LDAP, Novell, OpenLDAP 또는 일반 LDAPv3 디렉토리 서버와의 연결 여부를 자동으로 감지합니다. 그러나 자동 감지 기능에서 LDAP 서버 유형을 확인하지 못한 경우 수동으로 구성할 수 있습니다.

LDAP 서버 지침

LDAP 서버를 구성할 때 다음 지침에 유의하십시오.

- Sun 디렉토리 서버에 액세스하기 위해 ASA에 구성된 DN은 그 서버의 기본 비밀번호 정책에 액세스할 수 있어야 합니다. 디렉토리 관리자 또는 DN과 같은 디렉토리 관리자 권한이 있는 사용자를 이용하는 것이 좋습니다. 또는 기본 비밀번호 정책에 ACL을 포함할 수 있습니다.
- Microsoft Active Directory 및 Sun 서버로 비밀번호를 관리할 수 있도록 SSL을 통한 LDAP을 구성해야 합니다.

- ASA에서는 Novell, OpenLDAP, 기타 LDAPv3 디렉토리 서버를 사용한 비밀번호 관리를 지원하지 않습니다.
- VPN 3000 집중 디바이스와 ASA/PIX 7.0 소프트웨어는 권한 부여 작업에 Cisco LDAP 스키마가 필요했습니다. 버전 7.1.x부터 ASA는 기본 LDAP 스키마를 사용하여 인증 및 권한 부여를 수행하므로 Cisco 스키마가 더 이상 필요하지 않습니다.

인증에서의 LDAP 사용

ASA는 인증 과정에서 해당 사용자의 LDAP 서버에 대한 클라이언트 프록시의 역할을 하며, 일반 텍스트로 또는 SASL 프로토콜을 사용하여 LDAP 서버에 인증합니다. 기본적으로 ASA는 일반 텍스트 형식으로 인증 매개 변수(대개 사용자 이름과 비밀번호)를 LDAP 서버에 전달합니다.

ASA는 강도가 낮은 순서로 나열된 다음 SASL 메커니즘을 지원합니다.

- Digest-MD5—ASA는 사용자 이름과 비밀번호로 계산한 MD5 값을 사용하여 LDAP 서버에 응답합니다.
- Kerberos—ASA는 GSSAPI Kerberos 메커니즘을 사용하여 사용자 이름과 영역을 보내는 방법으로 LDAP 서버에 응답합니다.

ASA와 LDAP 서버는 이 SASL 메커니즘의 어떤 조합도 지원합니다. 여러 메커니즘을 구성한 경우, ASA는 그 서버에 구성된 SASL 메커니즘의 목록을 검색하고 ASA 및 서버 모두에 구성된 가장 강력한 것으로 인증 메커니즘을 설정합니다. 예를 들어, LDAP 서버와 ASA 모두 두 메커니즘을 지원할 경우 ASA는 둘 중 더 강력한 Kerberos를 선택합니다.

사용자 인증이 성공했으면 LDAP 서버는 인증된 사용자의 특성을 반환합니다. VPN 인증의 경우, 일반적으로 이 특성에는 VPN 세션에 적용된 권한 부여 데이터가 포함됩니다. 이러한 경우 LDAP을 사용하면 단일 단계에서 인증과 권한 부여가 이루어집니다.

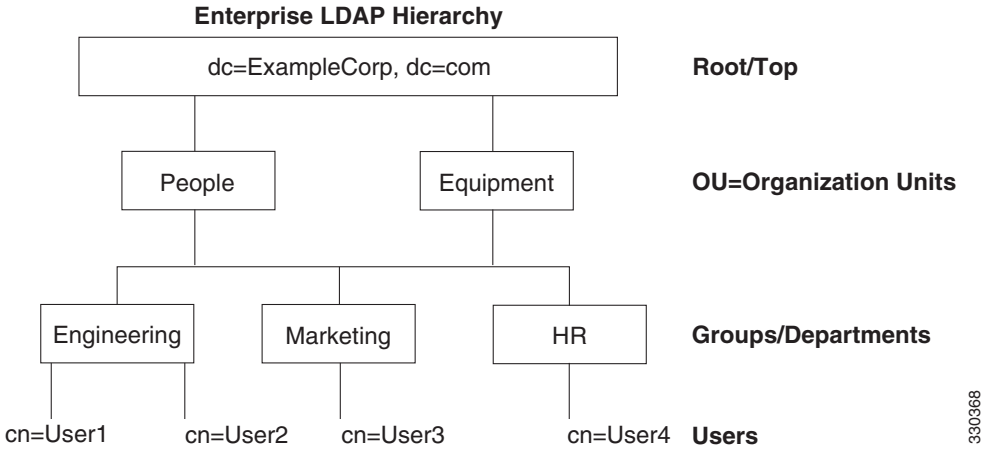
참고 LDAP 프로토콜에 대한 자세한 내용은 RFC 1777, 2251, 2849를 참조하십시오.

LDAP 계층 구조 소개

LDAP 컨피그레이션은 조직의 논리적 계층 구조를 반영해야 합니다. Example Corporation이라는 회사에 Employee1이라는 직원이 있다고 가정합니다. Employee1은 Engineering 그룹에서 일합니다. LDAP 계층 구조는 단일 단계 또는 여러 단계를 포함할 수 있습니다. 단일 단계 계층 구조로 설정할 경우 Employee1은 Example Corporation의 멤버로 간주됩니다. 또는 다단계 계층 구조로 설정할 수 있는데, 그러면 Employee1은 Engineering 부서의 멤버이고 이 부서는 People이라는 조직 단위의 멤버이며, People은 Example Corporation의 멤버입니다. 다단계 계층 구조의 예는 그림 31-1를 참조하십시오.

다단계 계층 구조가 더 상세한 내용을 포함하지만, 검색 결과는 단일 단계 계층 구조에서 더 빨리 얻을 수 있습니다.

그림 31-1 다단계 LDAP 계층 구조



LDAP 계층 구조 검색

ASA에서는 LDAP 계층 구조 내 검색을 맞춤 구성할 수 있습니다. ASA의 다음 3개 필드를 구성하여 LDAP 계층 구조에서 검색을 시작할 위치, 범위, 찾으려는 정보 유형을 정의합니다. 이 필드가 종합적으로 작용하여 사용자 권한을 포함하는 부분으로만 계층 구조 검색을 한정합니다.

- LDAP Base DN은 서버가 ASA로부터 권한 부여 요청을 받았을 때 LDAP 계층 구조의 어디에서 사용자 정보 검색을 시작할 것인가를 정의합니다.
- Search Scope는 LDAP 계층 구조에서 검색의 범위를 정의합니다. 검색에서는 계층 구조상 LDAP Base DN 아래의 여러 단계에서 이 작업을 진행합니다. 서버가 바로 아래 단계만 검색하게 하거나, 전체 하위 트리를 검색할 수도 있습니다. 단일 레벨 검색이 더 빠르지만, 하위 트리 검색은 더 광범위합니다.
- Naming Attribute(s)는 LDAP 서버의 항목을 고유하게 식별하는 RDN을 정의합니다. cn(Common Name), sAMAccountName, userPrincipalName과 같은 명명 특성이 주로 사용됩니다.

그림 31-1에서는 Example Corporation의 샘플 LDAP 계층 구조를 보여줍니다. 이 계층 구조에서 여러 가지 방법으로 검색을 정의할 수 있습니다. 표 31-1에서는 2가지 샘플 검색 컨피그레이션을 보여줍니다.

첫 번째 컨피그레이션 예에서는 Employee1이 LDAP 권한 부여가 필요한 IPsec 터널을 설정하자 ASA에서 LDAP 서버에 검색 요청을 보내면서 Engineering 그룹에서 Employee1을 찾도록 지시합니다. 이 검색은 빠르게 수행됩니다.

두 번째 컨피그레이션 예에서는 ASA가 검색 요청을 보내면서 서버에 Example Corporation 내에서 Employee1을 검색하도록 지시합니다. 이 검색은 더 오래 걸립니다.

표 31-1 검색 구성의 예

번호	LDAP 기본 DN	검색 범위	명명특성	결과
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	단일 레벨	cn=Employee1	더 빠른 검색
2	dc=ExampleCorporation,dc=com	하위 트리	cn=Employee1	더 오래 걸리는 검색

LDAP 서버와의 바인딩 소개

ASA에서는 로그인 DN과 로그인 비밀번호를 사용하여 LDAP 서버와의 신뢰(바인딩)를 설정합니다. Microsoft Active Directory 읽기 전용 작업(예: 인증, 권한 부여, 그룹 검색)을 수행할 때 ASA는 더 적은 권한의 로그인 DN을 사용하여 바인딩할 수 있습니다. 이를테면 로그인 DN은 AD "Member Of" 지정이 Domain Users의 일부인 사용자일 수 있습니다. VPN 비밀번호 관리 작업의 경우 로그인 DN은 상승된 권한이 필요하며 Account Operators AD 그룹의 일원이어야 합니다.

다음은 로그인 DN의 예입니다.

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA에서는 다음 인증 방식을 지원합니다.

- 포트 389에서 암호화되지 않은 비밀번호를 사용하는 단순 LDAP 인증
- 포트 636의 LDAP-S(Secure LDAP)
- SASL(Simple Authentication and Security Layer) MD5
- SASL Kerberos

ASA에서는 익명 인증을 지원하지 않습니다.

참고 LDAP 클라이언트인 ASA는 익명 바인딩 또는 요청의 전송을 지원하지 않습니다.

LDAP 서버를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

IPv6를 지원합니다.

LDAP 서버 구성

LDAP 서버 구성의 작업 흐름

1단계 LDAP 서버 그룹을 추가합니다. 31-7 페이지의 LDAP 서버 그룹 구성를 참조하십시오.

2단계 그룹에 서버를 추가하고 서버 매개 변수를 구성합니다. 31-8 페이지의 그룹에 LDAP 서버 추가 를 참조하십시오.

3단계 LDAP 특성 맵을 구성합니다. 31-5 페이지의 LDAP 특성 맵 구성를 참조하십시오.
LDAP 서버 그룹에 LDAP 서버를 추가하기 전에 특성 맵을 추가해야 합니다.

LDAP 특성 맵 구성

ASA에서는 사용자 인증을 위해 LDAP 디렉토리를 사용할 수 있습니다.

- VPN 원격 액세스 사용자
- 방화벽 네트워크 액세스/컷스루 프록시 세션
- 정책 권한(권한 부여 특성이라고도 함) 설정(예: ACL, 북마크 목록, DNS 또는 WINS 설정, 세션 타이머)
- 로컬 그룹 정책의 키 특성 설정

ASA에서는 기본 LDAP 사용자 특성을 Cisco ASA 특성으로 변환하는 데 LDAP 특성 맵을 사용합니다. 이 특성 맵을 LDAP 서버에 바인딩하거나 삭제할 수 있습니다. 특성 맵을 표시하거나 지울 수도 있습니다.

지침

LDAP 특성 맵은 다중값 특성을 지원하지 않습니다. 예를 들어, 사용자가 여러 AD 그룹의 멤버이고 LDAP 특성 맵이 둘 이상의 그룹에 매칭할 경우, 매칭된 항목의 알파벳순에 따라 값이 선택됩니다.

특성 매핑 기능을 올바르게 사용하려면 LDAP 특성의 이름 및 값 그리고 사용자 정의 특성의 이름 및 값까지 알고 있어야 합니다.

자주 매핑되는 LDAP 특성의 이름 및 일반적으로 이 특성이 매핑되는 사용자 정의 특성의 유형에는 다음이 포함됩니다.

- IETF-Radius-Class(ASA 버전 8.2 이상의 Group_Policy)—디렉토리 부서 또는 사용자 그룹(예: Microsoft Active Directory memberOf) 특성 값을 기반으로 그룹 정책을 설정합니다. 이 그룹 정책 특성은 IETF-Radius-Class 특성을 ASDM 버전 6.2/ASA 버전 8.2 이상으로 대체합니다.
- IETF-Radius-Filter-Id—액세스 제어 목록, 즉 ACL을 VPN 클라이언트, IPsec, SSL에 적용합니다.
- IETF-Radius-Framed-IP-Address—VPN 원격 액세스 클라이언트, IPsec, SSL에 할당되는 정적 IP 주소를 지정합니다.

- Banner1—VPN 원격 액세스 사용자가 로그인할 때 문자 배너를 표시합니다.
- Tunneling-Protocols—액세스 유형에 따라 VPN 원격 액세스 세션을 허용하거나 거부합니다.

참고 단일 LDAP 특성 맵은 하나 이상의 특성을 포함할 수 있습니다. 특정 LDAP 서버에서 하나의 LDAP 특성만 매핑할 수 있습니다.

LDAP 기능을 매핑하려면 다음 단계를 수행합니다.

세부 단계

1단계 **Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map**(로컬 사용자) 또는 **Configuration > Device Management > Users/AAA > LDAP Attribute Map(그 밖의 모든 사용자)**을 선택하고 **Add**를 클릭합니다.

Add LDAP Attribute Map 대화 상자가 나타납니다. Map Name 탭이 활성 상태입니다.

2단계 Name 필드에서 이 특성 맵의 이름을 만듭니다.

3단계 LDAP Attribute Name 필드에서 매핑할 LDAP 특성의 이름을 추가합니다.

4단계 Cisco Attribute Name 드롭다운 목록에서 Cisco 특성을 선택합니다.

5단계 **Add**를 클릭합니다.

6단계 특성이 매핑되었습니다. 다른 특성을 매핑하려면 1단계단계부터 5단계단계까지 반복합니다.

7단계 어떤 LDAP 특성의 값을 매핑된 Cisco 특성의 새 값에 매핑하려면 **Map Value** 탭을 클릭합니다.

8단계 **Add**를 클릭합니다.

Add Mapping of Attribute Name 대화 상자가 나타납니다.

9단계 드롭다운 목록에서 LDAP 특성을 선택합니다.

10단계 LDAP Attribute Value 필드에 LDAP 서버에서 반환할 이 LDAP 특성의 값을 입력합니다.

11단계 Cisco Attribute Value 필드에서는 이 LDAP 특성이 이전의 LDAP 특성 값을 포함할 경우에 Cisco 특성에서 사용할 값을 입력합니다.

12단계 **Add**를 클릭합니다.

값이 매핑됩니다.

13단계 다른 값을 매핑하려면 8단계단계부터 12단계단계까지 반복합니다.

14단계 **OK**를 클릭하여 Map Value 탭으로 돌아가고 **OK**를 다시 클릭하여 대화 상자를 닫습니다.

15단계 LDAP Attribute Map 창에서 **Apply**를 클릭하여 값 매핑을 실행 중인 컨피그레이션에 저장합니다.

LDAP 서버 그룹 구성

인증, 권한 부여 및/또는 어카운팅에 외부 LDAP 서버를 사용하려면 먼저 하나 이상의 LDAP 서버 그룹을 만들고 각 그룹에 하나 이상의 서버를 추가해야 합니다. LDAP 서버 그룹은 이름으로 식별합니다. 각 서버 그룹은 하나의 서버 유형에 특정됩니다.

지침

- 단일 모드에서는 최대 100개의 LDAP 서버 그룹을, 다중 모드에서는 컨텍스트당 4개의 LDAP 서버 그룹을 가질 수 있습니다.
- 각 그룹은 단일 모드에서 최대 16개의 LDAP 서버를, 다중 모드에서는 4개의 LDAP 서버를 가질 수 있습니다.
- 사용자가 로그인하면, 컨피그레이션에서 지정한 첫 번째 LDAP 서버부터 시작하여 서버가 응답할 때까지 한 번에 하나씩 서버에 액세스합니다. 그룹의 모든 서버가 사용할 수 없는 경우 ASA는 로컬 데이터베이스를 시도합니다. 단, 로컬 데이터베이스가 대비책으로 구성되었어야 합니다(관리 인증 및 권한 부여만 해당). 대비책이 없을 경우 ASA는 계속 LDAP 서버 액세스를 시도합니다.

세부 단계

다음 단계에서는 LDAP 서버 그룹을 만들어 구성하고 그 그룹에 LDAP 서버를 추가하는 방법을 보여줍니다.

1단계 **Configuration > Device Management > Users/AAA > AAA Server Groups** 또는 VPN 사용자의 경우 **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**를 선택합니다.

2단계 AAA Server Groups 영역에서 **Add**를 클릭합니다.

Add AAA Server Group 대화 상자가 나타납니다.

3단계 AAA Server Group 필드에 이 AAA 서버 그룹의 이름을 지정합니다.

4단계 Protocol 드롭다운 목록에서 LDAP 서버 유형을 선택합니다.

5단계 Reactivation Mode 필드에서 사용할 모드의 라디오 버튼(**Depletion** 또는 **Timed**)을 클릭합니다.

Depletion 모드에서는 그룹의 모든 서버가 비활성 상태가 되어야 실패한 서버가 재활성화됩니다.

Timed 모드에서는 가동 중단 후 30초가 지나면 실패한 서버가 재활성화됩니다.

a. Depletion 재활성화 모드를 선택한 경우 Dead Time 필드에 시간 간격을 입력합니다.

Dead Time은 그룹의 마지막 서버가 비활성화된 시점부터 나중에 모든 서버가 다시 활성화된 시점까지 경과한 시간(분)입니다.

6단계 Max Failed Attempts 필드에 서버 연결 시도 실패 허용 횟수를 추가합니다.

이 옵션은 무응답 서버를 비활성 상태로 선언하기 전에 허용되는 연결 실패 횟수를 설정합니다.

7단계 **OK**를 클릭합니다.

Add AAA Server Group 대화 상자가 닫히고 새 서버 그룹이 AAA Server Groups 테이블에 추가됩니다.

8단계 AAA Server Groups 대화 상자에서 **Apply**를 클릭하여 변경 사항을 저장합니다.

변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

그룹에 LDAP 서버 추가

1단계 **Configuration > Device Management > Users/AAA > AAA Server Groups** 또는 VPN 사용자라면 **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**를 선택하고 AAA Server Groups 영역에서 서버를 추가할 서버 그룹을 선택합니다.

2단계 Servers in Selected Groups 목록 옆의 **Add**를 클릭합니다.

선택된 서버 그룹에 대한 Add AAA Server 대화 상자가 나타납니다.

3단계 Interface Name 드롭다운 목록에서 LDAP 서버에 연결되는 인터페이스의 이름을 선택합니다.

4단계 Server Name 또는 IP Address 필드에서 LDAP 서버의 서버 이름 또는 IP 주소 중 하나를 추가합니다.

5단계 Timeout 필드에서 시간 초과 값을 추가하거나 기본값을 유지합니다. 시간 초과는 ASA에서 백업 서버에 요청을 보내기 전에 기본 서버의 응답을 기다리는 시간(초)입니다.

6단계 LDAP Parameters for authentication/authorization 영역에서 다음 필드를 구성합니다.

- **Enable LDAP over SSL**(secure LDAP 또는 LDAP-S라고도 함)—ASA와 LDAP 서버 같의 통신을 보호하는 데 SSL을 사용하려면 선택합니다.

참고 SASL 프로토콜을 구성하지 않은 경우 LDAP 통신을 SSL로 보호하는 것이 좋습니다.

- **Server Port**—ASA에서 단순(비보안) 인증을 위해 LDAP 서버에 액세스할 때 사용하는 포트인 TCP 포트 번호 389 또는 보안 인증(LDAP-S)에 사용하는 TCP 포트 636을 입력합니다. 모든 LDAP 서버가 인증 및 권한 부여를 지원합니다. Microsoft AD 및 Sun LDAP 서버만 VPN 원격 액세스 비밀번호 관리 기능을 추가로 제공하는데, 여기에는 LDAP-S가 필요합니다.
- **Server Type**—드롭다운 목록에서 LDAP 서버 유형을 지정합니다. 다음과 같은 옵션을 사용할 수 있습니다.
  - Detect Automatically/Use Generic Type
  - Microsoft
  - Novell
  - OpenLDAP
  - Sun(현재는 Oracle Directory Server Enterprise Edition에 포함)
- **Base DN**—서버가 LDAP 요청을 받았을 때 검색을 시작할 기본 DN 또는 LDAP 계층 구조상의 위치를 입력합니다(예: OU=people, dc=cisco, dc=com).
- **Scope**—서버가 권한 부여 요청을 받았을 때 LDAP 계층 구조에서 수행할 검색의 범위를 드롭다운 목록에서 지정합니다. 다음 옵션을 사용할 수 있습니다.
  - One Level—기본 DN의 바로 아래 단계만 검색합니다. 이 옵션이 더 빠릅니다.
  - All Levels—기본 DN 아래의 모든 단계를 검색합니다. 즉 하위 트리 계층 구조 전체를 검색합니다. 이 옵션은 시간이 더 걸립니다.
- **Naming Attribute(s)**—LDAP 서버의 항목을 고유하게 식별하는 Relative Distinguished Name 특성을 입력합니다. 주로 사용되는 명명 특성은 Common Name (CN), sAMAccountName, userPrincipalName, User ID (uid)입니다.
- **Login DN and Login Password**—ASA에서 로그인 DN과 로그인 비밀번호를 사용하여 LDAP 서버와의 신뢰(바인딩)를 설정합니다. 로그인 DN 사용자 어카운트의 비밀번호인 로그인 비밀번호를 지정합니다. 입력하는 문자가 별표로 바뀝니다.

- **LDAP Attribute Map**—이 LDAP 서버에서 사용하도록 생성한 특성 맵 중 하나를 선택합니다. 이 특성 캡은 LDAP 특성 이름을 Cisco 특성 이름 및 값으로 매핑합니다.
- **SASL MD5 authentication** SASL의 MD5 메커니즘에서 ASA와 LDAP 서버 간의 통신을 인증할 수 있게 합니다.
- **SASL Kerberos authentication**—SASL의 Kerberos 메커니즘에서 ASA와 LDAP 서버 간의 통신을 보안 인증할 수 있게 합니다. Kerberos 서버를 정의했어야 이 옵션을 활성화할 수 있습니다.
- **LDAP Parameters for Group Search**—이 영역의 필드는 ASA에서 AD 그룹을 요청하는 방법을 구성합니다.
  - **Group Base DN**—LDAP 계층 구조에서 AD 그룹(즉 memberOf 열거의 목록) 검색을 시작할 위치를 지정합니다. 이 필드가 구성되지 않은 경우 ASA에서는 AD 그룹 검색에 기본 DN을 사용합니다. ASDM에서는 동적 액세스 정책을 위해 AAA 선택 기준을 정의하는 데 검색된 AD 그룹의 목록을 사용합니다. 자세한 내용은 **show ad-groups** 명령을 참조하십시오.
  - **Group Search Timeout**—사용 가능한 그룹을 쿼리한 AD 서버의 응답을 기다리는 최대 시간을 지정합니다.

7단계 **OK**를 클릭합니다.

Add AAA Server 대화 상자가 닫히고 AAA 서버가 AAA 서버 그룹에 추가됩니다.

8단계 AAA Server Groups 창에서 **Apply**를 클릭하여 변경 사항을 실행 중인 컨피그레이션에 저장합니다.

LDAP 서버 인증 및 권한 부여 테스트

ASA에서 LDAP 서버에 접속하고 사용자 인증 또는 권한 부여를 수행할 수 있는지 확인하려면 다음 단계를 수행합니다.

1단계 Configuration > Device Management > Users/AAA > AAA Server Groups 창에서 서버가 속한 서버 그룹을 선택합니다.

2단계 Servers in the Selected Group 영역에서 테스트할 서버를 선택합니다.

3단계 **Test**를 클릭합니다.

선택된 서버에 대한 Test AAA Server 대화 상자가 나타납니다.

4단계 수행할 테스트 유형 **Authentication** 또는 **Authorization**을 클릭합니다.

5단계 사용자 이름을 입력합니다.

6단계 인증을 테스트하는 경우 사용자 이름의 비밀번호를 입력합니다.

7단계 **OK**를 클릭합니다.

ASA에서는 서버에 인증 또는 권한 부여 테스트 메시지를 보냅니다. 테스트가 실패한 경우 ASDM는 오류 메시지를 표시합니다.

LDAP 서버 모니터링

LDAP 서버를 모니터링하려면 다음 단계를 수행합니다.

1단계 ASDM에서 **Monitoring > Properties > AAA Servers**를 선택합니다.

2단계 LDAP 서버 상태를 업데이트하려면 그 서버를 선택하고 **Update Server Statistics**를 클릭합니다.

Update AAA Server Status 대화 상자가 나타나고 드롭다운 목록에 해당 LDAP 서버가 선택되어 있습니다.

3단계 **OK**를 클릭합니다.

4단계 현재 표시된 통계를 업데이트하려면 **Clear Server Statistics**를 클릭합니다.

LDAP 서버 기능 내역

표 31-2에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 31-2 AAA 서버 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
AAA를 위한 LDAP 서버	7.0(1)	LDAP 서버에서 AAA 지원과 LDAP 서버 구성 방법에 대해 설명합니다. 다음 화면을 도입했습니다. Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Remote Access VPN > AAA Local Users > LDAP Attribute Map

ID 방화벽

이 장에서는 ID 방화벽을 위해 ASA를 구성하는 방법을 설명합니다.

ID 방화벽에 대한 정보

ID 방화벽 개요

엔터프라이즈 환경에서는 사용자가 하나 이상의 서버 리소스에 액세스해야 하는 경우가 많습니다. 일반적으로 방화벽은 사용자의 ID를 인식하지 않으므로 ID에 따라 보안 정책을 적용할 수 없습니다. 사용자별 액세스 정책을 구성하기 위해서는 사용자 인증 프록시를 구성해야 하는데, 이는 사용자 상호 작용(사용자 이름/비밀번호 쿼리)을 필요로 합니다.

ASA의 ID 방화벽은 사용자의 ID를 기반으로 더 세부적인 액세스 제어를 제공합니다. 소스 IP 주소가 아닌 사용자 이름과 사용자 그룹 이름을 기반으로 한 액세스 규칙 및 보안 정책을 구성할 수 있습니다. ASA에서는 IP 주소와 Windows Active Directory 로그인 정보의 연결을 기반으로 한 보안 정책을 적용하고, 네트워크 IP 주소 대신 매핑된 사용자 이름을 기반으로 하여 이벤트를 보고합니다.

ID 방화벽은 실제 ID 매핑을 담당하는 외부 AD(Active Directory) 에이전트와 연계하여 Microsoft Active Directory와 통합됩니다. ASA에서는 특정 IP 주소에 대한 현재 사용자 ID 정보를 검색하는 소스로 Windows Active Directory를 사용하며, Active Directory 사용자를 위한 투명한 인증을 허용합니다.

ID 기반 방화벽 서비스는 소스 IP 주소 대신 사용자 또는 그룹을 지정할 수 있게 하여 기존 액세스 제어 및 보안 정책 메커니즘을 확장합니다. ID 기반 보안 정책은 기존 IP 주소 기반 규칙의 사이에 제약 없이 끼워 넣을 수 있습니다.

ID 방화벽은 다음과 같은 주요 이점을 제공합니다.

- 보안 정책에서 네트워크 토폴로지 분리
- 보안 정책 생성 간소화
- 네트워크 리소스에 대한 사용자 활동을 손쉽게 식별
- 사용자 활동 모니터링 간소화

ID 방화벽 구축을 위한 아키텍처

ID 방화벽은 실제 ID 매핑을 담당하는 외부 AD(Active Directory) 에이전트와 연계하여 Windows Active Directory와 통합됩니다.

ID 방화벽은 3가지 구성 요소로 이루어졌습니다.

- ASA
- Microsoft Active Directory

  Active Directory가 ASA의 ID 방화벽에 포함되어 있지만 Active Directory 관리자가 이를 관리합니다. 데이터의 신뢰성 및 정확성은 Active Directory의 데이터에 좌우됩니다.

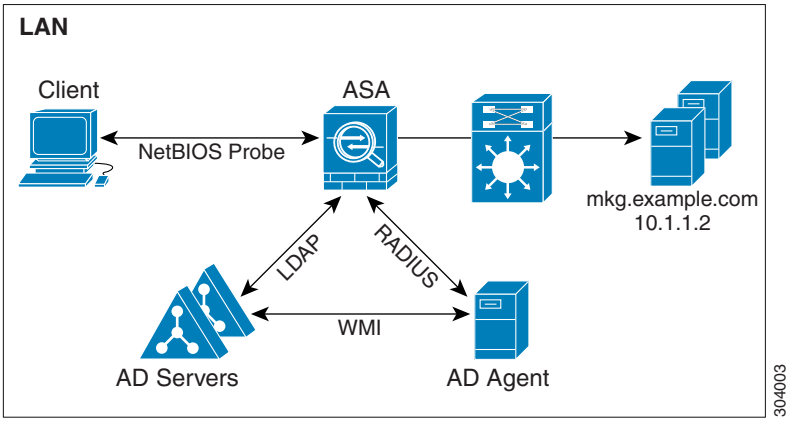
  지원되는 버전으로는 Windows Server 2003, Windows Server 2008, Windows Server 2008 R2 서버 등이 있습니다.
- AD 에이전트

  AD 에이전트는 Windows 서버에서 실행됩니다. 지원되는 Windows 서버로는 Windows 2003, Windows 2008, Windows 2008 R2 등이 있습니다.

참고 Windows 2003 R2는 AD 에이전트 서버로 지원되지 않습니다.

그림 32-1에서는 ID 방화벽의 구성 요소를 보여줍니다. 그 다음 표에서는 이 구성 요소의 역할 및 서로 통신하는 방법을 설명합니다.

그림 32-1 ID 방화벽의 구성 요소



1	**ASA에서**: 관리자가 로컬 사용자 그룹 및 ID 방화벽 정책을 구성합니다.	4	**클라이언트 <-> ASA**: 클라이언트가 Microsoft Active Directory를 통해 네트워크에 로그인합니다. AD 서버가 사용자를 인증하고 사용자 로그인 보안 로그를 생성합니다. 또는 클라이언트가 컷스루 프록시 또는 VPN을 통해 네트워크에 로그인할 수도 있습니다.
2	**ASA <-> AD 서버**: ASA에서 AD 서버에 구성된 Active Directory 그룹에 대한 LDAP 쿼리를 보냅니다. ASA에서 로컬 및 AD 그룹을 통합하고 사용자 ID 기반의 액세스 규칙 및 Modular Policy Framework 보안 정책을 적용합니다.	5	**ASA <-> 클라이언트**: ASA에 구성된 정책에 따라 클라이언트에 대한 액세스를 허용하거나 거부합니다. 구성된 경우 ASA는 클라이언트의 NetBIO를 프로브하여 비활성 사용자와 무응답 사용자를 통과시킵니다.
3	**ASA <-> AD 에이전트**: ID 방화벽 컨피그레이션에 따라 ASA는 IP-사용자 데이터베이스를 다운로드하거나 사용자의 IP 주소를 묻는 AD 에이전트에 RADIUS 요청을 보냅니다. ASA에서는 웹 인증 및 VPN 세션을 통해 습득한 새로운 매핑된 항목을 AD 에이전트에 전달합니다.	6	**AD 에이전트 <-> AD 서버**: AD 에이전트는 사용자 ID와 IP 주소의 매핑 항목에 대한 캐시를 유지합니다. 그리고 ASA에 변경 사항을 알립니다. AD 에이전트는 syslog 서버에 로그를 보냅니다.

ID 방화벽의 기능

ID 방화벽은 다음과 같은 주요 기능을 제공합니다.

유연성

- ASA는 AD 에이전트에 새로운 IP 주소 각각을 쿼리하거나 전체 사용자 ID 및 IP 주소 데이터베이스의 로컬 사본을 유지하는 방법으로 AD 에이전트로부터 사용자 ID 및 IP 주소 매핑을 검색할 수 있습니다.
- 사용자 ID 정책의 목적지로 호스트 그룹, 서브넷 또는 IP 주소를 지원합니다.
- 사용자 ID 정책의 소스 및 목적지로 FQDN(정규화된 도메인 이름)을 지원합니다.
- 5-튜플 정책과 ID 기반 정책의 조합을 지원합니다. ID 기반 기능은 기존 5-튜플 솔루션과 연계하면서 작동합니다.
- IPS 및 애플리케이션 검사 정책의 사용을 지원합니다.
- 원격 액세스 VPN, AnyConnect VPN, L2TP VPN, 컷스루 프록시에서 사용자 ID 정보를 검색합니다. 검색된 모든 사용자는 AD 에이전트와 연결된 모든 ASA에 보내집니다.

확장성

- 각 AD 에이전트는 100대의 ASA를 지원합니다. 여러 ASA가 단일 AD 에이전트와 통신하면서 대규모 네트워크 구축 환경에서 확장성을 제공할 수 있습니다.
- 30대의 Active Directory 서버를 지원합니다. 단 IP 주소가 모든 도메인의 전 범위에서 고유해야 합니다.
- 한 도메인에 있는 각 사용자 ID는 최대 8개의 IP 주소를 가질 수 있습니다.

- ASA 5500 Series 모델의 경우 활성 정책에서 최대 64,000개의 사용자 ID-IP 주소 매핑 항목을 지원합니다. 이 제한으로 정책이 적용되는 사용자의 최대 수를 제어합니다. 총 사용자 수는 각기 다른 모든 컨텍스트에 구성된 전체 사용자를 합한 것입니다.
- 활성 ASA 정책에서 최대 256개의 사용자 그룹을 지원합니다.
- 단일 액세스 규칙에서 하나 이상의 사용자 그룹 또는 사용자를 수용할 수 있습니다.
- 다중 도메인을 지원합니다.

가용성

- ASA에서는 AD에서 그룹 정보를 검색하고, AD 에이전트에서 소스 IP 주소를 사용자 ID에 매핑하지 못할 경우에는 웹 인증을 통해 IP 주소를 얻습니다.
- AD 서버 중 하나가 또는 ASA가 응답하지 않더라도 AD 에이전트는 계속 작동합니다.
- ASA에서 기본 AD 에이전트와 보조 AD 에이전트를 구성하는 것을 지원합니다. 기본 AD 에이전트가 더 이상 응답하지 않을 경우 ASA는 보조 AD 에이전트로 전환할 수 있습니다.
- AD 에이전트를 사용할 수 없는 경우 ASA는 컷스루 프록시, VPN 인증과 같은 기존 ID 소스를 대신 사용할 수 있습니다.
- AD 에이전트는 watchdog 프로세스를 실행하는데, 이 프로세스의 서비스는 중지하더라도 자동으로 재시작합니다.
- 분산 IP 주소/사용자 매핑 데이터베이스를 ASA끼리 사용하는 것을 허용합니다.

구축 시나리오

환경의 요구 사항에 따라 다음 방법으로 ID 방화벽의 구성 요소를 구축할 수 있습니다.

그림 32-2에서는 이중화를 지원하기 위해 ID 방화벽의 구성 요소를 구축하는 방법을 보여줍니다. 시나리오 1은 구성 요소의 이중화 없는 간단한 설치입니다. 시나리오 2 역시 이중화 없는 간단한 설치입니다. 그러나 이 구축 시나리오에서는 AD 서버와 AD 에이전트가 동일한 Windows 서버에 함께 배치되어 있습니다.

그림 32-2 이중화 없는 구축 시나리오

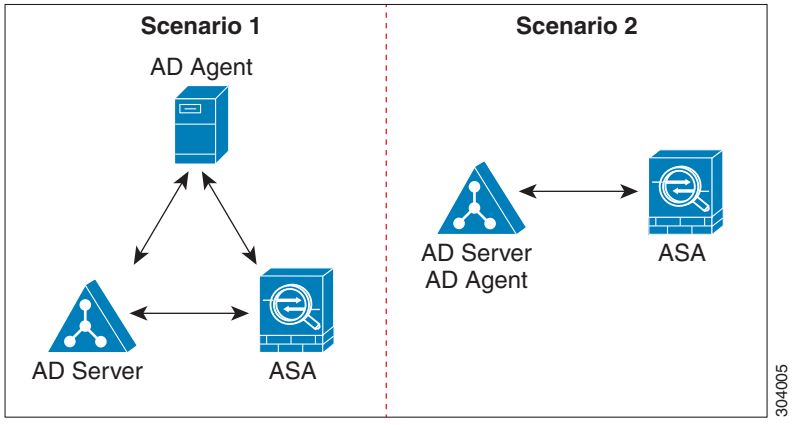


그림 32-3에서는 이중화를 지원하기 위해 ID 방화벽 구성 요소를 구축하는 방법을 보여줍니다. 시나리오 1은 여러 AD 서버 및 별도의 Windows 서버에 설치된 단일 AD 에이전트로 구성된 구축 환경입니다. 시나리오 2는 여러 AD 서버 및 별도의 Windows 서버에 설치된 여러 AD 에이전트로 구성된 구축 환경입니다.

그림 32-3 이중 구성 요소의 구축 시나리오

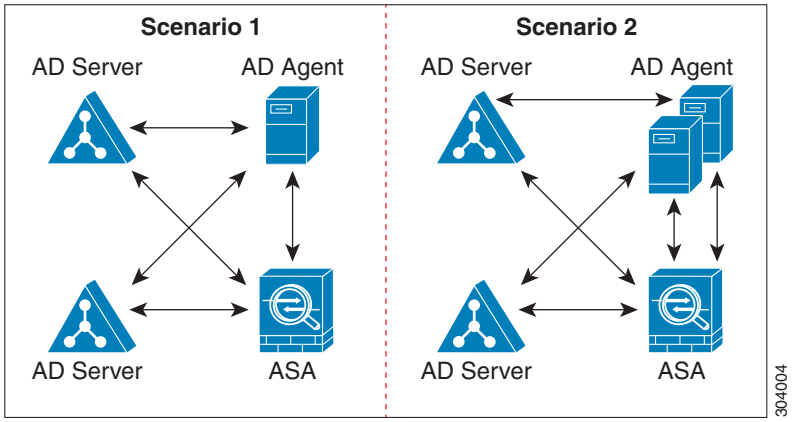


그림 32-4에서는 모든 ID 방화벽 구성 요소(AD 서버, AD 에이전트, 클라이언트)가 어떻게 설치되고 LAN을 통해 통신하는지 보여줍니다.

그림 32-4 LAN 기반 구축

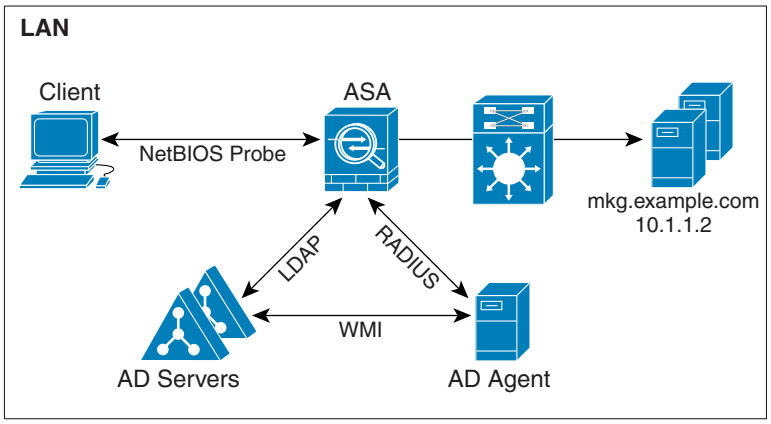


그림 32-5에서는 원격 사이트를 지원하는 WAN 기반 구축을 보여줍니다. AD 서버와 AD 에이전트가 기본 사이트 LAN에 설치되어 있습니다. 클라이언트는 원격 사이트에 있으며 WAN을 통해 ID 방화벽 구성 요소에 연결됩니다.

그림 32-5 WAN 기반 구축

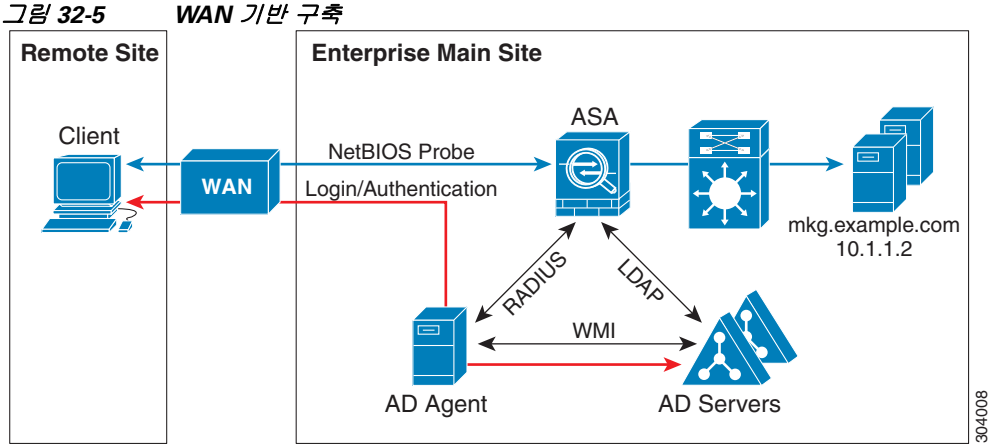


그림 32-6에서는 원격 사이트를 지원하는 WAN 기반 구축도 보여줍니다. Active Directory 서버는 기본 사이트 LAN에 설치됩니다. 그러나 AD 에이전트는 설치된 다음 원격 사이트의 클라이언트에 의해 액세스됩니다. 원격 클라이언트는 WAN을 통해 기본 사이트에 있는 AD 서버에 연결합니다.

그림 32-6 원격 AD 에이전트로 구성된 WAN 기반 구축

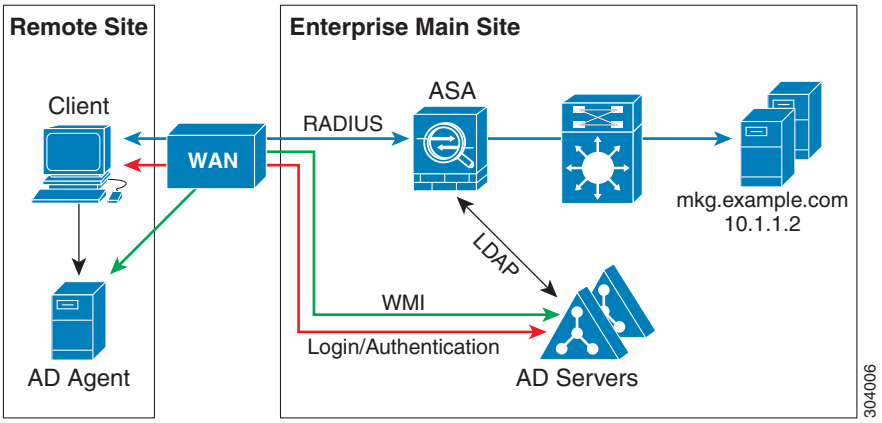
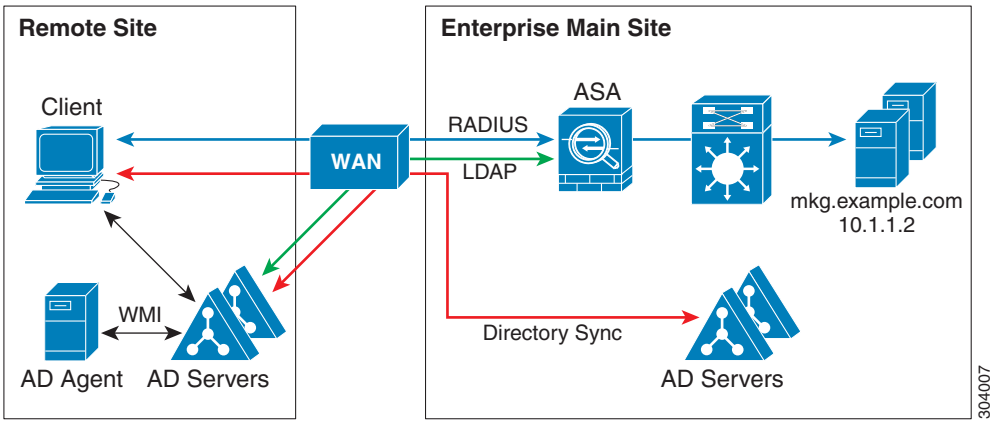


그림 32-7에서는 확장된 원격 사이트 설치를 보여줍니다. AD 에이전트와 AD 서버가 원격 사이트에 설치됩니다. 클라이언트는 기본 사이트에 위치한 네트워크 리소스에 로그인할 때 로컬에서 이 구성 요소에 액세스합니다. 원격 AD 서버는 기본 사이트에 있는 중앙 AD 서버와 데이터를 동기화해야 합니다.

그림 32-7 원격 AD 에이전트와 AD 서버로 구성된 WAN 기반 구축



ID 방화벽을 위한 라이센싱

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원됩니다.

장애 조치 지침

- ID 방화벽은 사용자 ID-IP 주소 매핑을 지원하고 상태 기반 시스템 대체 작동(Stateful Failover)이 활성화된 경우 활성 시스템에서 대기 시스템으로 AD 에이전트 상태를 복제하는 것도 지원합니다. 그러나 사용자 ID-IP 주소 매핑, AD 에이전트 상태, 도메인 상태만 복제됩니다. 사용자 및 사용자 그룹 레코드는 대기 ASA에 복제되지 않습니다.

- 장애 조치가 구성되면 대기 ASA 역시 AD 에이전트에 직접 연결하여 사용자 그룹을 검색하도록 구성되어야 합니다. ID 방화벽에 대한 NetBIOS 검사 옵션이 구성된 경우에도 대기 ASA는 클라이언트에 NetBIOS 패킷을 보내지 않습니다.
- 클라이언트가 활성 ASA에 의해 비활성 상태로 확인되면 그 정보가 대기 ASA에 전달됩니다. 사용자 통계는 대기 ASA에 전달되지 않습니다.
- 장애 조치가 구성되면 AD 에이전트가 활성 및 대기 ASA 모두와 통신하도록 구성해야 합니다. AD 에이전트 서버에 ASA를 구성하는 단계는 *AD 에이전트 설치 및 설정 설명서*를 참조하십시오.

IPv6 지침

- IPv6를 지원합니다.
- AD 에이전트는 엔드포인트에 IPv6 주소를 지원합니다. 로그 이벤트에서 IPv6 주소를 수신하고 캐시에 저장했다가 RADIUS 메시지를 통해 보낼 수 있습니다.
- IPv6를 통한 NetBIOS는 지원되지 않습니다.

추가 지침 및 제한

- 목적지 주소에서 전체 URL은 지원되지 않습니다.
- NetBIOS 검사 기능이 작동하려면 ASA, AD 에이전트, 클라이언트를 연결하는 네트워크에서 UDP 캡슐화 NetBIOS 트래픽을 지원해야 합니다.
- 중간 라우터가 있으면 ID 방화벽의 MAC 주소 검사가 수행되지 않습니다. 동일한 라우터의 뒤에 있는 클라이언트에 로그인한 사용자는 MAC 주소가 같습니다. 이러한 구현에서는 동일한 라우터에서 보내는 모든 패킷이 검사를 통과할 수 있습니다. ASA에서 라우터 뒤에 있는 실제 MAC 주소를 확인할 수 없기 때문입니다.
- 다음 ASA 기능은 확장 ACL에서 ID 기반 객체와 FQDN을 사용하는 것을 지원하지 않습니다.
  - 경로 맵
  - 암호 맵
  - WCCP
  - NAT
  - 그룹 정책(VPN 필터에 대한 것 제외)
  - DAP
- **user-identity update active-user-database** 명령을 사용하여 AD 에이전트로부터 사용자-IP 주소를 다운로드하는 프로세스를 능동적으로 시작할 수 있습니다.

  이전의 다운로드 세션이 끝난 경우 ASA에서 이 명령의 재실행을 허용하지 않도록 설계되었습니다.

  따라서 사용자-IP 주소가 매우 클 경우, 이전 다운로드 세션이 끝나지 않은 상태에서 다시 **user-identity update active-user-database** 명령을 실행하면 다음 오류 메시지가 나타납니다.

  ```
  "ERROR: one update active-user-database is already in progress."
  ```

  이전 세션이 완전히 끝날 때까지 기다려야 합니다. 그러면 다시 **user-identity update active-user-database** 명령을 실행할 수 있습니다.

  AD 에이전트에서 ASA로 보내는 패킷이 손실된 경우에도 이와 같은 동작이 일어납니다.

  user-identity update active-user-database 명령을 실행하면 ASA는 다운로드할 사용자-IP 매핑 항목의 총 개수를 요청합니다. 그러면 AD 에이전트는 ASA와의 UDP 연결을 시작하고 권한 부여 요청 패킷의 변경 사항을 보냅니다.

어떤 이유로 패킷이 손실된 경우 ASA에서 이를 알 방법이 없습니다. 따라서 ASA는 4~5분간 세션을 유지합니다. 이 상태에서 **user-identity update active-user-database** 명령을 실행하면 이 오류 메시지가 계속 나타납니다.

- Cisco CDA(Context Directory Agent)를 ASA 또는 Cisco Ironport WSA(Web Security Appliance)와 함께 사용할 경우 다음 포트를 열어 두어야 합니다.
  - UDP 인증 포트—1645
  - UDP 어카운팅 포트—1646
  - UDP 수신 포트—3799

    수신 포트는 CDA에서 ASA에 또는 WSA에 권한 부여 요청의 변경 사항을 보낼 때 사용합니다.
- 도메인 이름에는 \/:*?"<>| 문자를 사용할 수 없습니다. 명명 규칙에 대해서는 http://support.microsoft.com/kb/909264를 참조하십시오.
- 사용자 이름에는 \/[]:;=,+*?"<>|@ 문자를 사용할 수 없습니다.
- 사용자 그룹 이름에는 \/[]:;=,+*?"<>| 문자를 사용할 수 없습니다.

전제 조건

ASA에서 ID 방화벽을 구성하기 전에 AD 에이전트 및 Microsoft Active Directory의 전제 조건을 충족해야 합니다.

AD 에이전트

- AD 에이전트는 ASA에서 액세스할 수 있는 Windows 서버에 설치해야 합니다. 또한 AD 에이전트가 AD 서버로부터 정보를 얻고 ASA와 통신할 수 있도록 구성해야 합니다.
- 지원되는 Windows 서버로는 Windows 2003, Windows 2008, Windows 2008 R2 등이 있습니다.

참고 Windows 2003 R2는 AD 에이전트 서버로 지원되지 않습니다.

- AD 에이전트를 설치하고 구성하는 단계에 대해서는 *AD 에이전트 설치 및 설정 설명서*를 참조하십시오.
- ASA에서 AD 에이전트를 구성하기 전에 AD 에이전트와 ASA의 통신에 사용할 암호 키 값을 얻습니다. 이 값은 AD 에이전트와 ASA 모두에서 일치해야 합니다.

Microsoft Active Directory

- Microsoft Active Directory는 Windows 서버에 설치되고, ASA에서 액세스할 수 있어야 합니다. 지원되는 버전으로는 Windows 2003, 2008, 2008 R2 서버 등이 있습니다.
- ASA에서 AD 서버를 구성하기 전에 Active Directory에서 ASA를 위한 사용자 어카운트를 만듭니다.
- 또한 ASA는 LDAP을 통해 활성화된 SSL을 사용하여 AD 서버에 암호화된 로그인 정보를 보냅니다. SSL이 AD 서버에서 활성화되어야 합니다. AD를 위해 SSL을 활성화하는 방법에 대해서는 Microsoft Active Directory 설명서를 참조하십시오.

참고 AD 에이전트 설치 프로그램을 실행하기 전에 AD 에이전트가 모니터링하는 각 Microsoft Active Directory 서버에 *Cisco AD 에이전트를 위한 README First*에 명시된 패치를 설치해야 합니다. 이 패치는 AD 에이전트가 도메인 컨트롤러 서버에 설치되는 경우에도 필요합니다.

ID 방화벽 구성

이 단원에서는 다음 항목을 다룹니다

ID 방화벽 구성의 작업 흐름

ID 방화벽을 구성하려면 다음 단계를 수행합니다.

1단계 ASA에 AD 도메인을 구성합니다.

32-10 페이지의 AD 도메인 구성 및 32-11 페이지의 AD 서버 그룹 구성를 참조하십시오.

또한 32-4 페이지의 구축 시나리오에서 해당 환경의 요구 사항에 맞게 AD 서버를 구축하는 방법도 알아보십시오.

2단계 ASA에 AD 에이전트를 구성합니다.

32-11 페이지의 AD 서버 그룹 구성 및 32-12 페이지의 AD 에이전트 그룹 구성를 참조하십시오.

또한 32-4 페이지의 구축 시나리오에서 해당 환경의 요구 사항에 맞게 AD 에이전트를 구축하는 방법도 알아보십시오.

3단계 ID 옵션을 구성합니다.

32-13 페이지의 ID 옵션 구성를 참조하십시오.

4단계 ID 기반 보안 정책을 구성합니다. AD 도메인과 AD 에이전트가 구성된 다음에는 여러 기능에서 사용할 ID 기반 객체 그룹과 ACL을 만들 수 있습니다.

32-15 페이지의 ID 기반 보안 정책 구성를 참조하십시오.

AD 도메인 구성

ASA에서 AD 그룹을 다운로드하려면 그리고 AD 에이전트로부터 IP-사용자 매핑을 받을 때 특정 도메인의 사용자 ID를 승인하기 위해서는 ASA에 AD 도메인 컨피그레이션이 필요합니다.

전제 조건

- Active Directory 서버 IP 주소
- LDAP 기반 DN의 고유 이름
- ID 방화벽에서 AD 도메인 컨트롤러에 연결하는 데 사용하는 AD 사용자의 고유 이름 및 비밀번호

AD 도메인을 구성하려면 다음 단계를 수행합니다.

1단계 **Configuration > Firewall > Identity Options**를 선택합니다.

2단계 필요한 경우 **Enable User Identity** 확인란을 선택하여 사용자 ID를 활성화합니다.

3단계 Domains 섹션에서 **Add**를 클릭하거나 목록에서 도메인을 선택하여 **Edit**를 클릭합니다.

Domain 대화 상자가 나타납니다.

4단계 Domain NETBIOS Name 필드에 최대 32자이고 [a-z], [A-Z], [0-9], [!@#$%^&()-_=+[]{};,.]로 구성된 이름을 입력합니다. 맨 앞에 '.'와 ' '이 올 수 없습니다. 도메인 이름이 공백을 포함할 경우 그 공백 문자를 따옴표로 묶어야 합니다. 도메인 이름은 대/소문자를 구분하지 않습니다.

기존 도메인의 이름을 수정할 때 기존 사용자 및 사용자 그룹과 연결된 도메인 이름은 바뀌지 않습니다.

5단계 AD Server Group 목록에서 이 도메인과 연결할 AD 서버를 선택하거나 **Manage**를 클릭하여 목록에 새 서버 그룹을 추가합니다. 32-11 페이지의 AD 서버 그룹 구성를 참조하십시오.

6단계 **OK**를 클릭하여 도메인 설정을 저장하고 이 대화 상자를 닫습니다.

다음에 할 일

32-11 페이지의 AD 서버 그룹 구성 및 32-12 페이지의 AD 에이전트 그룹 구성를 참조하십시오.

AD 서버 그룹 구성

AD 서버 그룹을 구성하려면 다음 단계를 수행합니다.

1단계 **Configuration > Firewall > Identity Options > Add > Manage**를 선택합니다.

Configure Active Directory Server Groups 대화 상자가 나타납니다.

2단계 ID 방화벽을 위해 AD 서버 그룹을 추가하려면 **Add**를 클릭합니다.

Add Active Directory Server Group 대화 상자가 나타납니다.

3단계 AD 서버 그룹에 서버를 추가하려면 Active Directory Server Groups 목록에서 그룹을 선택하고 **Add**를 클릭합니다.

Add Active Directory Server 대화 상자가 나타납니다.

4단계 **OK**를 클릭하여 설정을 저장하고 이 대화 상자를 닫습니다.

다음에 할 일

32-12 페이지의 AD 에이전트 구성 및 32-12 페이지의 AD 에이전트 그룹 구성를 참조하십시오.

AD 에이전트 구성

전제 조건

AD 에이전트를 구성하기 전에 다음 정보가 있어야 합니다.

- AD 에이전트 IP 주소
- ASA와 AD 에이전트의 공유 암호

AD 에이전트를 구성하려면 다음 단계를 수행합니다.

1단계 **Configuration > Firewall > Identity Options**를 선택합니다.

2단계 필요한 경우 **Enable User Identity** 확인란을 선택하여 이 기능을 활성화합니다.

3단계 Active Directory Agent 섹션에서 **Manage**를 클릭합니다.

Configure Active Directory Agents 대화 상자가 나타납니다.

4단계 AD 에이전트를 추가하려면 **Add** 버튼을 클릭합니다. 또는 목록에서 에이전트 그룹을 선택하고 **Edit**를 클릭합니다.

계속하려면 32-12 페이지의 AD 에이전트 그룹 구성를 참조하십시오.

5단계 **OK**를 클릭하여 변경 사항을 저장합니다.

다음에 할 일

AD 에이전트 그룹을 구성합니다. 32-12 페이지의 AD 에이전트 그룹 구성를 참조하십시오.

ID 방화벽을 위한 액세스 규칙을 구성합니다. 32-15 페이지의 ID 기반 보안 정책 구성를 참조하십시오.

AD 에이전트 그룹 구성

AD 에이전트 서버 그룹을 위해 기본 및 보조 AD 에이전트를 구성합니다. ASA에서 기본 AD 에이전트가 응답하지 않음을 탐지한 경우, 보조 에이전트가 지정되어 있다면 ASA는 보조 AD 에이전트로 전환합니다. AD 에이전트의 AD 서버는 RADIUS를 통신 프로토콜로 사용합니다. 따라서 ASA와 AD 에이전트의 공유 암호에 대한 키 특성을 지정해야 합니다.

AD 에이전트 그룹을 구성하려면 다음 단계를 수행합니다.

1단계 Configure Active Directory Agents 대화 상자에서 **Add**를 클릭합니다.

Add Active Directory Agent Group 대화 상자가 나타납니다.

2단계 AD 에이전트 그룹의 이름을 입력합니다.

3단계 Primary Active Directory Agent 섹션에서 ASA가 AD 에이전트 서버로부터 트래픽을 수신하는 인터페이스를 지정하고 서버의 FQDN 또는 IP 주소를 입력합니다.

4단계 Primary Active Directory Agent 섹션에서 시간 초과 간격 및 AD 에이전트가 응답하지 않을 때 ASA에서 연결을 재시도하는 간격을 입력합니다.

5단계 기본 AD 에이전트와 ASA가 사용하는 공유 암호 키를 입력합니다.

6단계 Secondary Active Directory Agent 섹션에서 ASA가 AD 에이전트 서버로부터 트래픽을 수신하는 인터페이스를 지정하고 서버의 FQDN 또는 IP 주소를 입력합니다.

7단계 Secondary Active Directory Agent 섹션에서 시간 초과 간격 및 AD 에이전트가 응답하지 않을 때 ASA에서 연결을 재시도하는 간격을 입력합니다.

8단계 보조 AD 에이전트와 ASA가 사용하는 공유 암호 키를 입력합니다.

9단계 **OK**를 클릭하여 변경 사항을 저장하고 이 대화 상자를 닫습니다.

다음에 할 일

ID 방화벽을 위한 액세스 규칙을 구성합니다. 32-15 페이지의 ID 기반 보안 정책 구성를 참조하십시오.

ID 옵션 구성

이 창을 사용하여 ID 방화벽 기능을 추가하거나 수정합니다. 이 기능을 활성화하려면 **Enable** 확인란을 선택합니다. 기본적으로 ID 방화벽 기능은 비활성화되어 있습니다.

전제 조건

ID 방화벽을 위한 ID 옵션을 구성하기 전에 AD 에이전트 및 Microsoft Active Directory의 전제 조건을 충족해야 합니다. AD 에이전트 및 Microsoft Active Directory 설치의 요구 사항은 32-9 페이지의 전제 조건를 참조하십시오.

ID 방화벽을 위한 ID 옵션을 구성하려면 다음 단계를 수행합니다.

1단계 **Configuration > Firewall > Identity Options**를 선택합니다.

2단계 필요한 경우 **Enable User Identity** 확인란을 선택하여 이 기능을 활성화합니다.

3단계 ID 방화벽을 위해 도메인을 추가하려면 **Add**를 클릭하여 Add Domain 대화 상자를 표시합니다.

4단계 계속하려면 32-10 페이지의 AD 도메인 구성를 참조하십시오.

5단계 이미 Domains 목록에 추가된 도메인의 경우, AD 도메인 컨트롤러가 응답하지 않아 도메인이 중지했을 때 규칙을 비활성화할지를 선택합니다.

도메인이 중지한 상태에서 해당 도메인에 대해 이 옵션이 선택되어 있다면 ASA는 도메인의 사용자와 연결된 사용자 ID 규칙을 비활성화합니다. 또한 그 도메인에 속한 모든 사용자 IP 주소의 상태는 Monitoring > Properties > Identity > Users 창에서 disabled로 표시됩니다.

6단계 Default Domain 드롭다운 목록에서 ID 방화벽의 기본 도메인을 선택합니다.

기본 도메인은 모든 사용자 및 사용자 그룹에 사용되는데, 해당 사용자 또는 그룹에 대해 어떤 도메인도 명시적으로 구성되지 않은 경우에 쓰입니다. 기본 도메인이 지정되지 않았으면 사용자 및 그룹의 기본 도메인은 LOCAL이 됩니다.

또한 ID 방화벽은 모든 로컬에 정의된 사용자 그룹 또는 로컬에 정의된 사용자(VPN 또는 웹 포털을 사용하여 로그인하고 인증한 사용자)에게 LOCAL 도메인을 사용합니다.

참고 기본 도메인 이름은 AD 도메인 컨트롤러에 구성된 NetBIOS 도메인 이름과 일치하도록 선택해야 합니다. 도메인 이름이 일치하지 않을 경우, AD 에이전트는 사용자-IP 매핑 항목을 ASA 구성 시 입력한 도메인 이름과 잘못 연결합니다.
NetBIOS 도메인 이름을 보려면 임의의 텍스트 편집기에서 AD 사용자 이벤트 보안 로그를 엽니다.

다중 컨텍스트 모드의 경우, 컨텍스트마다 또는 시스템 실행 영역 내에서 기본 도메인 이름을 설정할 수 있습니다.

7단계 Active Directory Agent 섹션의 드롭다운 목록에서 AD 에이전트 그룹을 선택합니다. AD 에이전트 그룹을 추가하려면 **Manage**를 클릭합니다. 자세한 내용은 32-12 페이지의 AD 에이전트 구성를 참조하십시오.

8단계 Hello Timer 필드에 10초~65535초 범위의 숫자를 입력합니다.

ASA와 AD 에이전트 간의 hello 타이머는 ASA가 hello 패킷을 교환하는 빈도를 정의합니다. ASA는 ASA 복제 상태(in-sync 또는 out-of-sync) 및 도메인 상태(up 또는 down)를 확인하는 데 hello 패킷을 사용합니다. ASA가 AD 에이전트로부터 응답을 받지 못한 경우 지정된 간격이 지나면 hello 패키지를 다시 보냅니다.

ASA에서 AD 에이전트에 hello 패킷을 재전송하는 횟수를 지정합니다. 기본적으로, 시간(초)은 30으로, 재시도 횟수는 5로 설정되어 있습니다.

9단계 ASA에서 각 식별자에 대해 수신하는 최종 이벤트 타임 스탬프를 추적할 수 있게 하려면 또는 이벤트 타임 스탬프가 ASA의 시계보다 5분 이상 오래되었거나 타임 스탬프가 최종 이벤트 타임 스탬프보다 빠를 경우에 어떤 메시지든 삭제하려면 **Enable Event Timestamp**를 선택합니다.

최종 이벤트 타임 스탬프를 모르는 새로 부팅된 ASA의 경우, ASA에서 이벤트 타임 스탬프를 자체 시계와 비교합니다. 이벤트가 5분 이상 더 오래되었다면 ASA는 메시지를 수락하지 않습니다.

ASA, Active Directory, AD 에이전트끼리 NTP를 사용하여 시계를 동기화하도록 구성하는 것이 좋습니다.

10단계 Poll Group Timer 필드에는 ASA에서 FQDN을 확인하기 위해 DNS 서버를 쿼리하는 데 사용하는 시간을 입력합니다. 기본적으로 폴링 타이머는 4시간으로 설정됩니다.

11단계 Retrieve User Information의 목록에서 옵션을 선택합니다.

- On Demand—ASA가 새로운 연결이 필요한 패킷을 수신할 때, 그 소스 IP 주소의 사용자가 사용자-ID 데이터베이스에 없다면 ASA에서 AD 에이전트로부터 IP 주소의 사용자 매핑 정보를 검색하도록 지정합니다.
- Full Download—ASA에서 AD 에이전트에 요청을 보내 ASA 시작 시 전체 IP-사용자 매핑 테이블을 다운로드하도록 그리고 사용자가 로그인하고 로그아웃할 때 추가된 IP-사용자 매핑을 수신하도록 지정합니다.

참고 On Demand를 선택하면 수신된 패킷의 사용자만 쿼리하고 저장하므로 메모리를 더 적게 사용한다는 이점이 있습니다.

12단계 Error Conditions 섹션에서 AD 에이전트가 응답하지 않을 때 규칙을 비활성화할지를 선택합니다.

AD 에이전트가 중지한 상태에서 이 옵션이 선택되어 있다면 ASA는 해당 도메인의 사용자와 연결된 사용자 ID 규칙을 비활성화합니다. 또한 그 도메인에 속한 모든 사용자 IP 주소의 상태는 Monitoring > Properties > Identity > Users 창에서 disabled로 표시됩니다.

13단계 Error Conditions 섹션에서 NetBIOS 프로브가 실패할 때 사용자의 IP 주소를 삭제할지를 선택합니다.

이 옵션을 선택함으로써 사용자에 대한 NetBIOS 프로브가 차단되었을 때(예: 사용자 클라이언트가 NetBIOS 프로브에 응답하지 않음) 어떻게 할지 지정합니다. 해당 클라이언트에 대한 네트워크 연결이 차단될 수 있습니다. 또는 클라이언트가 활성 상태가 아닙니다. 이 옵션이 선택되면 ASA는 그 사용자의 IP 주소와 연결된 ID 규칙을 비활성화합니다.

14단계 Error Conditions 섹션에서 사용자의 MAC 주소가 현재 ASA에서 현재 그 MAC 주소에 매핑한 IP 주소와 일치하지 않을 경우 해당 주소를 삭제할지를 선택합니다. 이 옵션이 선택되면 ASA는 해당 사용자와 연결된 사용자 ID 규칙을 비활성화합니다.

15단계 Error Conditions 섹션에서 찾지 못한 사용자를 추적할지를 선택합니다.

16단계 Users 섹션에서 Idle Timeout 옵션을 선택하고 1분~65535분 범위에서 시간(분)을 입력합니다. 기본적으로 유휴 타이머는 60분으로 설정됩니다.

이 옵션을 활성화함으로써 활성 사용자가 유휴 상태로 간주될 때의 타이머를 구성합니다. 즉 ASA는 지정된 시간을 초과하여 사용자의 IP 주소로부터 트래픽을 받지 못했습니다. 타이머가 만료되면 사용자의 IP 주소는 비활성 상태로 표시되고 로컬 캐시에 저장된 IP-사용자 데이터베이스에서 삭제됩니다. 그리고 ASA는 더 이상 AD 에이전트에 그 IP 주소에 대해 알리지 않습니다. 기존 트래픽은 계속 전달될 수 있습니다. Idle Timeout 옵션이 활성화되면 ASA는 NetBIOS Logout Probe가 구성된 경우에도 비활성 타이머를 실행합니다.

참고 Idle Timeout 옵션은 VPN 또는 컷스루 프록시 사용자에게는 적용되지 않습니다.

17단계 NetBIOS Logout Probe 섹션에서 NetBIOS 프로브를 활성화하고, 사용자의 IP 주소가 프로브되기까지의 프로브 타이머(1분~65535분) 및 프로브 재시도 간격(1회~256회)을 설정합니다.

이 옵션을 활성화함으로써 ASA에서 사용자 클라이언트가 계속 활성 상태인지 확인하기 위해 사용자 호스트를 프로브하는 빈도를 구성합니다. NetBIOS 패킷을 최소화하기 위해 ASA에서는 사용자가 Idle Timeout 필드에 지정된 시간(분)을 초과하여 유휴 상태였을 때만 클라이언트에 NetBIOS 프로브를 보냅니다.

18단계 NetBIOS Logout Probe 섹션의 User Name 목록에서 옵션을 선택합니다.

- Match Any—호스트의 NetBIOS 응답이 IP 주소에 지정된 사용자의 사용자 이름을 포함하는 한 사용자 ID는 유효한 것으로 간주됩니다. 이 옵션을 지정하려면 호스트에서 Messenger 서비스를 활성화했고 WINS 서버를 구성했어야 합니다.
- Exact Match—IP 주소에 지정된 사용자의 사용자 이름은 NetBIOS 응답에서 하나뿐이어야 합니다. 그렇지 않으면 IP 주소의 사용자 ID는 유효하지 않은 것으로 간주됩니다. 이 옵션을 지정하려면 호스트에서 Messenger 서비스를 활성화했고 WINS 서버를 구성했어야 합니다.
- User Not Needed—ASA에서 호스트로부터 NetBIOS 응답을 받는 한 사용자 ID는 유효한 것으로 간주됩니다.

19단계 **Apply**를 클릭하여 ID 방화벽 컨피그레이션을 저장합니다.

다음에 할 일

Active Directory 도메인 및 서버 그룹을 구성합니다. 32-10 페이지의 AD 도메인 구성 및 32-11 페이지의 AD 서버 그룹 구성를 참조하십시오.

AD 에이전트를 구성합니다. 32-11 페이지의 AD 서버 그룹 구성를 참조하십시오.

ID 기반 보안 정책 구성

다양한 ASA 기능에 ID 기반 정책을 통합할 수 있습니다. (32-7 페이지의 지침 및 제한 사항에서 지원되지 않는다고 표시된 것을 제외하고) 확장 ACL을 사용하는 어떤 기능도 ID 방화벽을 활용할 수 있습니다. 이제 네트워크 기반 매개 변수뿐 아니라 사용자 ID 인수를 확장 ACL에 추가할 수 있습니다.

다음과 같은 기능에서 ID를 사용할 수 있습니다.

- 액세스 규칙—액세스 규칙은 네트워크 정보를 사용하여 인터페이스에서 트래픽을 허용하거나 거부합니다. ID 방화벽을 사용하면 사용자 ID를 기반으로 액세스를 제어할 수 있습니다. 방화벽 컨피그레이션 가이드를 참조하십시오.

- AAA 규칙—(컷스루 프록시라고도 하는) 인증 규칙은 사용자를 기반으로 네트워크 액세스를 제어합니다. 이 기능은 액세스 규칙에 ID 방화벽을 더한 것과 매우 비슷하므로, 사용자의 AD 로그인이 만료될 경우 대체 인증 방법으로 AAA 규칙을 사용할 수 있습니다. 예를 들어, 유효한 로그인이 없는 사용자에 대해 AAA 규칙을 트리거할 수 있습니다. 유효한 로그인이 없는 사용자에 한해 AAA 규칙이 트리거되도록 액세스 규칙 및 AAA 규칙에 쓰이는 확장 ACL에 해당 사용자 이름을 지정할 수 있습니다(None(유효한 로그인이 없는 사용자) 및 Any(유효한 로그인이 있는 사용자)). 액세스 규칙에서는 사용자 및 그룹에 대해 평소와 같이 정책을 구성하되 모든 None 사용자를 허용하는 AAA 규칙을 포함합니다. 이 사용자를 허용해야 나중에 AAA 규칙이 트리거될 수 있습니다. 그리고 Any 사용자(이 사용자는 AAA 규칙의 대상이 아니며, 이미 액세스 규칙에 의해 처리되었음)를 거부하되 모든 None 사용자를 허용하는 AAA 규칙을 구성합니다. 예:

```
access-list 100 ex permit ip user CISCO\xyz any any
access-list 100 ex deny ip user CISCO\abc any any
access-list 100 ex permit ip user NONE any any
access-list 100 ex deny any any
access-group 100 in interface inside

access-list 200 ex deny ip user ANY any any
access-list 200 ex permit user NONE any any
aaa authenticate match 200 inside user-identity
```

  자세한 내용은 기존 기능 가이드를 참조하십시오.

- Cloud Web Security—어떤 사용자를 Cloud Web Security 프록시 서버에 보낼지 제어할 수 있습니다. 또한 Cloud Web Security에 보내진 ASA 트래픽 헤더에 포함된 사용자 그룹을 기반으로 하는 정책을 Cloud Web Security ScanCenter에서 구성할 수 있습니다. 방화벽 컨피그레이션 가이드를 참조하십시오.
- VPN 필터—VPN은 일반적으로 ID 방화벽 ACL을 지원하지 않지만, ASA에서 VPN 트래픽에 대해 ID 기반 액세스 규칙을 강제적으로 적용하도록 구성할 수 있습니다. 기본적으로 VPN 트래픽은 액세스 규칙의 대상이 아닙니다. VPN 클라이언트에서 ID 방화벽 ACL을 사용하는 액세스 규칙을 반드시 준수하게 할 수 있습니다(**no sysopt connection permit-vpn** 명령 사용). 또한 VPN 필터 기능과 함께 ID 방화벽 ACL을 사용할 수 있습니다. VPN 필터는 대체로 허용 액세스 규칙과 비슷한 효과를 발휘합니다.

ID 방화벽 모니터링

AD 에이전트 모니터링

ID 방화벽의 AD 에이전트 구성 요소를 모니터링하려면 다음 단계를 수행합니다.

1단계 **Monitoring > Properties > Identity > AD Agent**를 선택합니다.

2단계 **Refresh**를 클릭하여 창의 데이터를 업데이트합니다.

이 창에서는 기본 및 보조 AD 에이전트에 대한 다음 정보를 표시합니다.

- AD 에이전트의 상태
- 도메인의 상태
- AD 에이전트의 통계

그룹 모니터링

ID 방화벽에 대해 구성된 사용자 그룹을 모니터링하려면 다음 단계를 수행합니다.

1단계 **Monitoring > Properties > Identity > Group**을 선택합니다.

2단계 선택된 그룹을 사용하여 액세스 규칙의 목록을 표시하려면 **Where used**를 클릭합니다.

3단계 **Refresh**를 클릭하여 창의 데이터를 업데이트합니다.

이 창에서는 사용자 그룹의 목록을 *domain\group_name* 형식으로 표시합니다.

ID 방화벽의 메모리 사용량 모니터링

ASA에서 ID 방화벽이 사용하는 메모리의 양을 모니터링하려면 다음 단계를 수행합니다.

1단계 **Monitoring > Properties > Identity > Memory Usage**를 선택합니다.

2단계 **Refresh**를 클릭하여 창의 데이터를 업데이트합니다.

이 창에서는 ID 방화벽에 있는 여러 모듈의 메모리 사용량을 바이트로 표시합니다.

- 사용자
- 그룹
- 사용자 통계
- LDAP

  ASA에서는 AD 서버에 구성된 AD 그룹에 대한 LDAP 쿼리를 보냅니다. AD 서버가 사용자를 인증하고 사용자 로그인 보안 로그를 생성합니다.
- AD 에이전트
- 기타
- 총 메모리 사용량

참고 ID 방화벽에서 AD 에이전트로부터 사용자 정보를 검색하도록 어떻게 구성했느냐에 따라 이 기능의 메모리 사용량이 달라집니다. ASA에서 온디맨드 검색을 아니면 전체 다운로드 검색을 사용할 것인지 지정합니다. 온디맨드 검색을 선택하면 수신된 패킷의 사용자만 쿼리하고 저장하므로 메모리를 더 적게 사용한다는 이점이 있습니다. 자세한 내용은 32-13 페이지의 ID 옵션 구성를 참조하십시오.

ID 방화벽의 사용자 모니터링

ID 방화벽에서 사용하는 IP-사용자 매핑 데이터베이스에 포함된 모든 사용자에 대한 정보를 표시하려면 다음 단계를 수행합니다.

1단계 **Monitoring > Properties > Identity > User**를 선택합니다.

참고 활성 사용자는 녹색으로 강조 표시됩니다.

2단계 활성 사용자에 대한 추가 정보를 표시하려면 목록에서 사용자를 선택하고 **Details**를 클릭합니다. Details 버튼은 활성 사용자에 대해서만 사용 가능합니다.

3단계 선택된 사용자를 사용하여 액세스 규칙의 목록을 표시하려면 **Where used**를 클릭합니다.

4단계 **Refresh**를 클릭하여 창의 데이터를 업데이트합니다.

이 창에서는 사용자에 대한 다음 정보를 표시합니다.

domain\user_name 상태(활성 또는 비활성) 연결 유휴 시간(분)

기본 도메인 이름은 실제 도메인 이름, 특별 예약어 또는 LOCAL일 수 있습니다. ID 방화벽은 모든 로컬에 정의된 사용자 그룹 또는 로컬에 정의된 사용자(VPN 또는 웹 포털을 사용하여 로그인하고 인증한 사용자)에게 LOCAL 도메인 이름을 사용합니다. 기본 도메인이 지정되지 않은 경우 기본 도메인은 LOCAL입니다.

유휴 시간은 사용자의 IP 주소를 기준으로 하지 않고 사용자별로 저장됩니다.

AD 서버가 중지되었고 도메인이 중지되었을 때 규칙을 비활성화하는 옵션 또는 AD 서버가 중지되었고 AD 에이전트가 중지되었을 때 규칙을 비활성화하는 옵션이 선택된 경우, 로그인한 모든 사용자는 비활성(disabled) 상태가 됩니다. Identity Options 창에서 이 옵션을 구성합니다.

Firewall Dashboard 창에서 사용자의 통계를 볼 수도 있습니다. Firewall Dashboard 탭에서는 ASA를 지나는 트래픽에 대한 중요한 정보를 볼 수 있습니다. **Home > Firewall Dashboard > Top Usage Statistics > Top 10 Users** 탭을 선택합니다.

Top 10 Users 탭은 ASA에서 ID 방화벽 기능을 구성한 경우에만 데이터를 표시합니다. 여기에는 Microsoft Active Directory, Cisco AD(Active Directory) 에이전트와 같은 추가 구성 요소를 구성하는 것도 포함됩니다. 자세한 내용은 32-10 페이지의 ID 방화벽 구성를 참조하십시오.

선택하는 옵션에 따라 Top 10 Users 탭에는 수신된 EPS 패킷, 전송한 EPS 패킷, 상위 10명의 사용자에게 전송된 공격에 대한 통계가 표시됩니다. 이 탭에서는 (*domain\user_name*으로 표시되는) 각 사용자에 대해 평균 EPS 패킷, 현재 EPS 패킷, 트리거, 총 이벤트를 보여줍니다.

참고 Top Usage Status 영역의 첫 3개 탭은 위협 감지 데이터를 표시하며, ID 방화벽 기능과는 무관합니다.

ID 방화벽 기능 내역

표 32-1에서는 이 기능의 출시 내역을 정리합니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 32-1 ID 방화벽 기능 내역

기능 이름	릴리스	기능 정보
ID 방화벽	8.4(2)	ID 방화벽 기능을 도입했습니다. 다음 화면을 도입했거나 수정했습니다. Configuration > Firewall > Identity Options Configuration > Firewall > Objects > Local User Groups Monitoring > Properties > Identity

33 장

ASA 및 Cisco TrustSec

Cisco TrustSec과 통합된 ASA 정보

Cisco TrustSec 정보

전통적으로 방화벽과 같은 보안 기능은 미리 정의된 IP 주소, 서브넷 및 프로토콜에 따라 액세스 제어를 수행했습니다. 하지만 기업이 경계 없는 네트워크로 전환함에 따라 사람과 조직을 연결하는 기술과 데이터 및 네트워크 보호를 위한 보안 요구 사항 모두 크게 달라졌습니다. 엔드포인트의 유동성이 점차 심해지고 사용자는 다양한 엔드포인트(예: 노트북과 데스크톱, 스마트폰 또는 태블릿)를 사용하기 때문에 사용자 속성과 엔트포인트 속성이 조합되면서 기존 6-tuple 기반 규칙에 더하여 방화벽 기능을 갖춘 스위치나 라우터 또는 전용 방화벽과 같은 디바이스를 안정적으로 액세스 제어 결정에도 활용할 수 있는 조건을 갖추게 되었습니다.

따라서 엔드포인트 속성 또는 클라이언트 ID 속성의 가용성과 전파가 고객 네트워크 전반, 네트워크의 액세스, 배포 및 핵심 레이어, 그리고 데이터 센터의 보안을 지원하는 중요한 요구 사항이 되고 있습니다.

Cisco TrustSec은 기존 identity-aware 인프라 위에 구축되어 네트워크 디바이스 간 데이터 기밀을 보장하고 하나의 플랫폼으로 보안 액세스 서비스를 통합합니다. Cisco TrustSec 기능에서 적용 디바이스는 사용자 속성과 엔드포인트 속성의 조합을 사용하여 역할 기반 및 ID 기반 액세스 제어 결정을 내립니다. 이 정보의 가용성과 전파는 네트워크의 액세스, 배포 및 핵심 레이어에서 네트워크 전반의 보안을 활성화합니다.

Cisco TrustSec을 구현하면 다음과 같은 이점을 얻을 수 있습니다.

- 점차 늘어나는 모바일 및 복합 인력이 어떤 디바이스에서든 더 안전하고 알맞은 액세스를 할 수 있게 해줍니다.
- 누가 무엇으로 유선 또는 무선 네트워크에 연결하는지 포괄적인 가시성을 제공하여 보안 위험을 완화합니다.
- 물리적 또는 클라우드 기반 IT 리소스에 액세스하는 네트워크 사용자의 활동에 대한 뛰어난 관리 기능을 제공합니다.
- 고도로 안전한 중앙 집중식 액세스 정책 관리 및 확장 가능한 적용 메커니즘을 통해 총 소유 비용을 줄입니다.

다양한 Cisco 제품에서의 Cisco TrustSec 기능 사용에 관한 자세한 정보는 33-24 페이지의 추가 참조 자료을(를) 참조하십시오.

Cisco TrustSec에서의 SGT 및 SXP 지원 정보

Cisco TrustSec 기능에서 보안 그룹 액세스는 토폴로지 인식 네트워크를 역할 기반 네트워크로 바꾸어 역할 기반 액세스 제어(RBAC)로 엔드-투-엔드 정책을 적용할 수 있게 합니다. 인증 과정에서 얻은 디바이스와 사용자 자격 증명은 보안 그룹별로 패킷을 분류하는 데 사용됩니다. Cisco TrustSec 클라우드에 진입하는 모든 패킷은 SGT(security group tag)로 태그됩니다. 태깅은 믿을 수 있는 매개자가 패킷의 소스 ID를 확인하고 데이터 경로를 따라 보안 정책을 적용할 수 있게 합니다. SGT는 SGT가 보안 그룹 ACL 정의에 사용될 때 도메인 전반에서 권한 수준을 나타냅니다.

SGT는 RADIUS vendor-specific 속성으로 이루어지는 IEEE 802.1X 인증, 웹 인증 또는 MAC 인증 바이패스(MAB)를 통해 디바이스에 할당됩니다. SGT는 특정 IP 주소 또는 스위치 인터페이스에 전략적으로 할당될 수 있습니다. SGT는 인증 성공 후 스위치 또는 액세스 포인트에 동적으로 전달됩니다.

SXP(Security-group eXchange Protocol)는 SGT 지원 하드웨어가 없는 네트워크 디바이스 전반에서 IP-to-SGT 매핑 데이터베이스를 SGT와 보안 그룹 ACL을 지원하는 하드웨어로 전파하도록 Cisco TrustSec을 위해 개발된 프로토콜입니다. 컨트롤 플레인 프로토콜인 SXP는 인증 포인트(레거시 액세스 레이어 스위치 등)에서 네트워크의 업스트림 디바이스로 IP-SGT 매핑을 전달합니다.

SXP 연결은 point-to-point 연결이며 TCP를 기본 전송 프로토콜로 사용합니다. SXP는 잘 알려진 TCP 포트 번호인 64999를 사용하여 연결을 개시합니다. 또한 SXP 연결은 소스와 대상 IP 주소를 통해 고유하게 식별됩니다.

Cisco TrustSec 기능의 역할

ID 및 정책 기반 액세스 정책을 위해 Cisco TrustSec 기능은 다음 역할을 포함합니다.

- 액세스 요청자(AR)—액세스 요청자는 네트워크의 보호된 리소스에 대한 액세스를 요청하는 엔드포인트 디바이스입니다. 아키텍처의 주된 주체이며 이들의 액세스 권한은 ID 자격 증명에 달려 있습니다.

  액세스 요청자에는 PC, 랩톱, 휴대폰, 프린터, 카메라 및 MACsec-capable IP 전화와 같은 엔드포인트 디바이스가 포함됩니다.

- PDP(Policy Decision Point)—정책 결정 포인트는 액세스 제어 결정을 책임집니다. PDP는 802.1x, MAB 및 웹 인증과 같은 기능을 제공합니다. PDP는 VLAN, DACL을 통한 인증 및 정책 적용, 보안 그룹 액세스(SGACL/SXP/SGT)를 지원합니다.

  Cisco TrustSec 기능에서는 Cisco ISE(Identity Services Engine)가 PDP 역할을 합니다. Cisco ISE는 ID 및 액세스 제어 정책 기능을 제공합니다.

- PIP(Policy Information Point)—정책 정보 포인트는 외부 정보(예: 평판, 위치 및 LDAP 속성)를 정책 결정 포인트로 제공하는 소스입니다.

  정책 정보 포인트는 Session Directory, Sensor IPS 및 Communication Manager와 같은 디바이스를 포함합니다.

- PAP(Policy Administration Point)—정책 관리 포인트는 권한 부여 시스템으로의 정책을 정의하고 삽입합니다. PAP는 Cisco TrustSec tag-to-user ID 매핑과 Cisco TrustSec tag-to-server 리소스 매핑을 제공함으로써 ID 저장소 역할을 합니다.

  Cisco TrustSec 기능에서는 Cisco Secure Access Control System(802.1x 및 SGT 지원이 통합된 정책 서버)이 PAP 역할을 합니다.

- PEP(Policy Enforcement Point)—정책 시행 포인트는 각 AR에 대해 PDP가 결정한 사항(정책 규칙 및 작업)을 실행합니다. PEP 디바이스는 네트워크에 걸쳐 존재하는 기본 통신 경로를 통해 ID 정보를 학습합니다. PEP 디바이스는 엔드포인트 에이전트, 권한 부여 서버, 피어 시행 디바이스 및 네트워크 흐름과 같은 여러 소스로부터 각 AR의 ID 속성을 학습합니다. PEP 디바이스는 SXP를 사용하여 네트워크 전체의 신뢰할 수 있는 피어 디바이스로 IP-SGT 매핑을 전파합니다.

  정책 시행 포인트는 Catalyst 스위치, 라우터, 방화벽(특히 ASA), 서버, VPN 디바이스 및 SAN 디바이스와 같은 네트워크 디바이스를 포함합니다.

Cisco ASA은(는) ID 아키텍처에서 PEP 역할을 수행합니다. SXP를 사용하여 ASA은(는) 인증 포인트로부터 직접 ID 정보를 학습하고 이를 이용하여 ID 기반 정책을 적용합니다.

보안 그룹 정책 적용

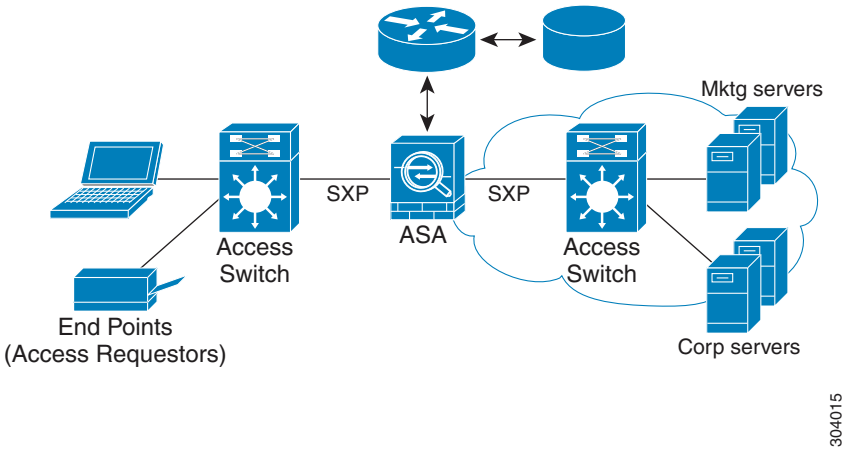
보안 정책 시행은 보안 그룹 이름을 기반으로 합니다. 엔드포인트 디바이스가 데이터 센터의 리소스 액세스를 시도합니다. 방화벽에 구성된 기존 IP 기반 정책과 달리 ID 기반 정책은 사용자 및 디바이스 ID를 기준으로 구성됩니다. 예를 들어 mktg-contractor는 mktg-servers에 액세스할 수 있고 mktg-corp-users는 mktg-server 및 corp-servers에 액세스할 수 있습니다.

이 배포 유형의 장점은 다음과 같습니다.

- 사용자 그룹과 리소스는 단일 객체(SGT) 간소화 정책 관리를 이용하여 정의 및 시행됩니다.
- 사용자 ID 및 리소스 ID는 Cisco TrustSec-capable 스위치 인프라 전반에서 보존됩니다.

그림 33-1은(는) 보안 그룹 이름 기반 정책 시행 배포를 보여줍니다.

그림 33-1 보안 그룹 이름 기반 정책 시행 배포



Cisco TrustSec을 구현하면 서버 분할을 지원하고 다음을 포함하는 보안 정책을 구성할 수 있습니다.

- 정책 관리 간소화를 위해 서버 풀에 SGT를 할당할 수 있습니다.
- SGT 정보는 Cisco TrustSec 지원 스위치 인프라 내에 보존됩니다.
- ASA은(는) Cisco TrustSec 도메인 전체에 걸쳐 정책 시행을 위해 IP-SGT 매핑을 사용합니다.
- 서버에 대한 802.1x 권한 부여가 필수이므로 구축 간소화가 가능합니다.

ASA의 보안 그룹 기반 정책 시행 방법

참고 사용자 기반 보안 정책과 보안 그룹 기반 정책이 ASA에서 공존할 수 있습니다. 네트워크 사용자 기반 및 보안 그룹 기반 속성의 어떤 조합이라도 보안 정책에서 구성할 수 있습니다. 사용자 기반 보안 정책 구성에 관한 정보는 32 장, "ID 방화벽"에서 참조하십시오.

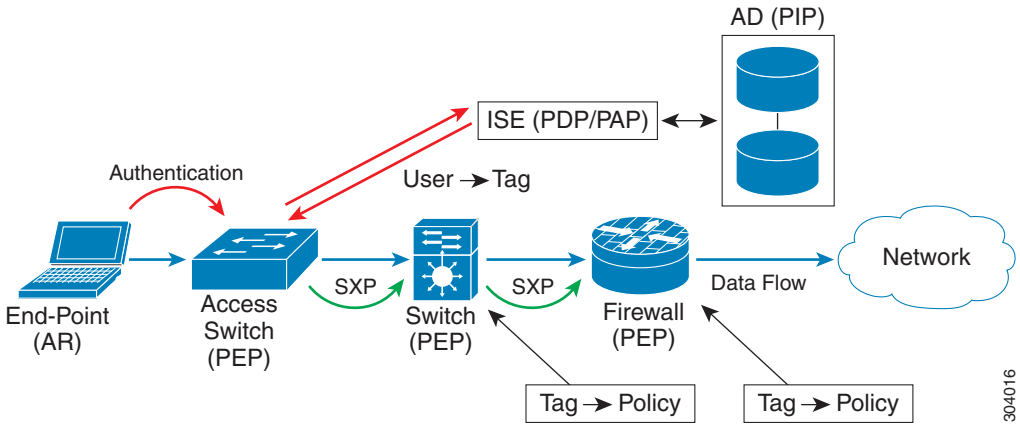
ASA을(를) Cisco TrustSec과 함께 작동하도록 구성하려면 ISE에서 PAC(Protected Access Credential) 파일을 가져와야 합니다. 자세한 내용은 33-15 페이지의 PAC 파일 가져오기를 참조하십시오.

PAC 파일을 ASA(으)로 가져오면 ISE와의 안전한 통신 채널이 설정됩니다. 채널을 설정하고 나면 ASA이(가) ISE와 PAC 보안 RADIUS 트랜잭션을 시작하고 Cisco TrustSec 환경 데이터(보안 그룹 테이블)를 다운로드합니다. 보안 그룹 테이블은 SGT를 보안 그룹 이름에 매핑합니다. 보안 그룹 이름은 ISE에서 만들어지며, 보안 그룹을 위해 사용하기 편리한 이름을 제공합니다.

ASA이(가) 보안 그룹 테이블을 처음 다운로드할 때 테이블의 모든 엔트리를 점검하고 구성된 보안 정책에 포함된 모든 보안 그룹 이름을 확인하고 나면 ASA이(가) 이 보안 정책을 로컬로 활성화합니다. ASA이(가) 보안 그룹 이름을 확인할 수 없다면 알 수 없는 보안 그룹 이름에 대한 syslog 메시지를 생성합니다.

그림 33-2은(는) Cisco TrustSec에서 보안 정책 시행 방식을 보여줍니다.

그림 33-2 보안 정책 시행



1. 엔드포인트 디바이스가 액세스 디바이스에 직접 연결하거나 원격 액세스를 통해 연결하고 Cisco TrustSec으로 인증합니다.
2. 액세스 레이어 디바이스는 802.1X 또는 웹 인증과 같은 인증 방식을 사용하여 ISE로 엔드포인트 디바이스를 인증합니다. 엔드포인트 디바이스가 역할 및 그룹 멤버십 정보를 전달하여 디바이스를 적절한 보안 그룹으로 분류합니다.
3. 액세스 레이어 디바이스는 SXP를 사용하여 IP-SGT 매핑을 업스트림 디바이스로 전파합니다.
4. ASA이(가) 패킷을 수신하고 SXP가 전달한 IP-SGT 매핑을 이용하여 SGT에서 소스 및 대상 IP 주소를 찾습니다.

   신규 매핑의 경우 ASA이(가) 로컬 IP-SGT Manager 데이터베이스에 기록합니다. 컨트롤 플레인에서 실행되는 IP-SGT Manager 데이터베이스는 각 IPv4 또는 IPv6 주소에 대해 IP-SGT 매핑을 추적합니다. 데이터베이스는 매핑을 학습한 소스를 기록합니다. SXP 연결의 피어 IP 주소가 매핑 소스로 사용됩니다. 각 IP-SGT 매핑 엔트리에 대해 여러 소스가 존재할 수 있습니다.

   ASA이(가) Speaker로 구성된 경우 ASA은(는) 모든 IP-SGT 매핑 엔트리를 SXP 피어로 전송합니다. 자세한 내용은 33-6 페이지의 ASA에서 스피커 및 리스너 역할에 관해를 참조하십시오.
5. 보안 정책이 ASA에서 해당 SGT 또는 보안 그룹 이름으로 구성된 경우 ASA이(가) 정책을 시행합니다. (ASA에서 SGT 또는 보안 그룹 이름을 포함하는 보안 정책을 생성할 수 있습니다. 보안 그룹 이름을 기준으로 정책을 시행하기 위해 ASA은(는) 보안 그룹 이름을 SGT에 매핑할 보안 그룹 테이블을 필요로 합니다.)

   ASA이(가) 보안 그룹 테이블에서 보안 그룹 이름을 찾을 수 없고 이것이 보안 정책에 포함된 경우 ASA은(는) 보안 그룹 이름을 알 수 없는 것으로 간주하고 syslog 메시지를 생성합니다. ASA이(가) ISE에서 보안 그룹 테이블을 갱신하고 보안 그룹 이름을 알게된 후 ASA은(는) syslog 메시지를 생성하여 보안 그룸 이름이 확인되었음을 알립니다.

ISE의 보안 그룹 변경이 주는 영향

ASA은(는) ISE에서 업데이트된 테이블을 다운로드함으로써 보안 그룹 테이블을 주기적으로 갱신합니다. 다운로드할 때마다 ISE에서 보안 그룹이 변경될 수 있습니다. 이러한 변화는 보안 그룹 테이블을 갱신하기 전에는 ASA에 반영되지 않습니다.

팁 유지 관리 중에 ISE에서 정책 컨피그레이션 변경을 예약한 후 ASA에서 수동으로 보안 그룹 테이블을 갱신하여 보안 그룹 변경 사항이 통합되도록 확인하는 것이 좋습니다.

이 방법으로 정책 컨피그레이션 변경 사항을 다루면 보안 그룹 이름 확인 및 보안 정책의 즉각적인 활성화 가능성이 높아집니다.

보안 그룹 테이블은 환경 데이터 타이머가 만료되면 자동으로 갱신됩니다. 또한 온디맨드로 보안 그룹 테이블 갱신을 트리거할 수 있습니다.

ISE에서 보안 그룹이 변경되면 ASA이(가) 보안 그룹 테이블을 갱신할 때 이벤트가 발생합니다.

- 보안 그룹 이름을 사용하여 구성된 보안 그룹 정책만 보안 그룹 테이블로 확인할 필요가 있습니다. 보안 그룹 태그를 포함하는 정책은 항상 활성 상태입니다.
- 보안 그룹 테이블을 처음 사용할 수 있게 되면 보안 그룹 이름을 가진 모든 정책이 설명되고 보안 그룹 이름이 확인되며 정책이 활성화됩니다. 태그가 지정된 모든 정책이 설명되고 알려진 태그에 대해 syslogs가 생성됩니다.
- 보안 그룹 테이블이 만료되면 직접 삭제할 때까지 또는 새로운 테이블을 사용할 수 있을 때까지 가장 최근에 다운로드한 보안 그룹 테이블에 따라 정책이 계속해서 시행됩니다.
- 확인된 보안 그룹 이름이 ASA에서 알 수 없음 상태가 되면 보안 정책이 비활성화됩니다. 하지만 보안 정책은 ASA 실행 중인 컨피그레이션에 계속 남습니다.
- PAP에서 기존 보안 그룹이 삭제되면 이전에 알려진 보안 그룹 태그가 알 수 없는 상태가 되지만 ASA에서 정책 상태는 변하지 않습니다. 이전에 알려진 보안 그룹 이름이 미확인 상태가 되고 정책이 비활성화됩니다. 보안 그룹 이름이 재사용되면 정책이 새로운 태그를 이용하여 다시 컴파일됩니다.
- PAP에 새로운 보안 그룹이 추가되면 이전에 알려지지 않았던 보안 그룹 태그가 알려지고 syslog 메시지가 생성되지만 정책 상태는 변하지 않습니다. 이전에 알려지지 않았던 보안 그룹 이름이 확인되고 연결된 정책이 활성화됩니다.
- PAP에서 태그 이름이 변경되면 태그를 이용하여 구성되었던 정책이 새로운 이름을 표시하고 정책 상태는 변경되지 않습니다. 보안 그룹 이름으로 구성되었던 정책이 새로운 태그 값을 사용하여 다시 컴파일됩니다.

ASA에서 스피커 및 리스너 역할에 관해

ASA은(는) 다른 네트워크 디바이스로부터 IP-SGT 매핑 엔트리를 주고받도록 SXP를 지원합니다. SXP를 사용하면 보안 디바이스와 방화벽이 하드웨어 업그레이드나 변경 없이 액세스 스위치로부터 ID 정보를 학습할 수 있습니다. SXP는 또한 IP-SGT 매핑 엔트리를 업스트림 디바이스(데이터 센터 디바이스 등)에서 다운스트림 디바이스로 전달할 때도 사용됩니다. ASA은(는) 업스트림 및 다운스트림 방향 모두에서 정보를 받을 수 있습니다.

ASA에서 SXP 피어로 SXP 연결을 구성할 때는 해당 연결에 대해 ASA을(를) 스피커 또는 리스너로 지정하여 ID 정보를 교환할 수 있도록 해야 합니다.

- 스피커 모드—ASA이(가) ASA에서 수집한 모든 활성 IP-SGT 매핑 엔트리를 정책 시행을 위해 업스트림 디바이스로 전달할 수 있도록 구성합니다.

- 리스너 모드—ASA이(가) 다운스트림 디바이스(SGT 지원 스위치)로부터 IP-SGT 매핑 엔트리를 수신하고 이 정보를 사용하여 정책 정의를 생성할 수 있도록 구성합니다.

SXP 연결의 한 쪽이 스피커로 구성된 경우 다른 한쪽은 리스너로 구성되어야 합니다. SXP 연결의 양쪽에 있는 두 디바이스가 모두 같은 역할(둘 다 스피커 또는 리스너)로 구성된 경우 SXP 연결이 실패하고 ASA이(가) syslog 메시지를 생성합니다.

Multiple SXP 연결은 IP-SGT 매핑 데이터베이스에서 다운로드된 IP-SGT 매핑 엔트리를 학습할 수 있습니다. ASA에서 SXP 피어로의 SXP 연결이 설정된 후 리스너가 전체 IP-SGT 데이터베이스를 스피커에서 다운로드합니다. 이후 발생하는 모든 변경 사항은 네트워크에 새로운 디바이스가 나타날 때만 전송됩니다. 따라서 SXP 정보 흐름의 속도는 호스트가 네트워크에 인증되는 속도에 비례합니다.

SXP 연결을 통해 학습된 IP-SGT 매핑 엔트리는 SXP IP-SGT 매핑 데이터베이스에서 유지됩니다. 서로 다른 SXP 연결을 통해 동일한 매핑 엔트리를 학습할 수 있습니다. 매핑 데이터베이스는 학습한 각 매핑 엔트리에 대해 하나의 사본을 유지합니다. 동일한 IP-SGT 매핑 값을 가진 여러 매핑 엔트리는 매핑이 학습된 연결에서 피어 IP 주소에 의해 식별됩니다. SXP는 새로운 매핑이 처음 학습되면 IP-SGT Manager가 매핑 엔트리를 추가하고 SXP 데이터베이스의 마지막 사본이 삭제되면 매핑 엔트리를 삭제하도록 요청합니다.

SXP 연결이 스피커로 구성되어 있으면 SXP는 항상 IP-SGT Manager에게 디바이스에서 수집된 모든 매핑 엔트리를 피어로 전달할 것을 요청합니다. 새로운 매핑이 로컬로 학습되면 IP-SGT Manager는 SXP가 스피커로 구성된 연결을 통해 이를 전달할 것을 요청합니다.

ASA을(를) SXP 연결을 위한 스피커와 리스너로 동시에 구성하면 SXP 루핑이 발생하여 SXP 데이터를 처음에 전송한 SXP 피어가 다시 이 데이터를 수신하게 됩니다.

SXP Chattiness

SXP 정보 흐름의 속도는 호스트가 네트워크에 인증되는 속도에 비례합니다. SXP 피어링이 설정된 후 리스너 디바이스가 스피커 디바이스에서 전체 IP-SGT 데이터베이스를 다운로드합니다. 그 후 모든 변경 사항은 새로운 디바이스가 네트워크에 나타나거나 네트워크를 떠날 때만 증분적으로 전송됩니다. 또한 새로운 디바이스에 연결된 액세스 디바이스만 업스트림 디바이스로의 이러한 증분적인 업데이트를 시작할 수 있습니다.

다시 말하면 SXP 프로토콜은 인증 서버의 기능으로 제한되는 인증 속도보다 빠르지 않습니다. 따라서 SXP chattiness는 중요한 문제가 아닙니다.

SXP 타이머

- Retry Open Timer—열기 재시도 타이머는 디바이스의 특정 SXP 연결이 연결되지 않은 경우 트리거됩니다. 열기 재시도 타이머가 종료되면 디바이스가 전체 연결 데이터베이스를 점검하고 연결이 꺼져 있거나 "대기" 상태인 경우 열기 재시도 타이머가 재시작됩니다. 기본 타이머 값은 120초입니다. 값이 0이면 재시도 타이머가 시작되지 않습니다. 열기 재시도 타이머는 모든 SXP 연결이 설정될 때까지 또는 열기 재시도 타이머가 0으로 구성될 때까지 계속됩니다.
- Delete Hold-Down Timer—연결별 삭제 보류 타이머는 리스너의 연결이 해제될 때 트리거됩니다. 학습된 매핑 엔트리는 즉시 삭제되지 않고 삭제 보류 타이머가 만료될 때까지 유지됩니다. 이 타이머가 만료된 후 매핑 엔트리가 삭제됩니다. 삭제 보류 타이머 값은 120초로 설정되며 변경할 수 없습니다.

- Reconciliation Timer—삭제 보류 타이머 시간 내에 SXP 연결이 연결되면 이 연결에 대한 일괄 업데이트가 수행됩니다. 이는 가장 최근의 매핑 엔트리가 학습되어 새로운 연결 인스턴스 생성 식별자와 연결되었음을 의미합니다. 주기적인 연결별 조정 타이머가 백그라운드에서 시작됩니다. 이 조정 타이머가 만료되면 전체 SXP 매핑 데이터베이스를 검색하고 현재 연결 세션에서 학습되지 않은 모든 매핑 엔트리(연결 인스턴스 생성 식별자가 일치하지 않는 매핑 엔트리)를 식별한 후 삭제 표시를 합니다. 이 엔트리는 다음의 조정 검토에서 삭제됩니다. 기본 조정 타이머 값은 120초입니다. 사용하지 않는 엔트리가 기한 없이 남아 정책 시행에 예기치 못한 영향을 미치지 않도록 하기 위하여 ASA에서는 제로 값이 허용되지 않습니다.
- HA Reconciliation Timer—HA가 활성화된 경우 활성 및 스탠바이 유닛의 SXP 매핑 데이터베이스가 동기화된 것입니다. 새로운 활성 유닛이 모든 피어에 대한 새로운 SXP 연결 설정을 시도하고 최신 매핑 엔트리를 입수합니다. HA 조정 타이머는 이전 매핑 엔트리를 식별하고 삭제하는 수단을 제공합니다. 조정 타이머는 장애 조치가 발생한 후 시작되어 ASA이(가) 최신 매핑 엔트리를 입수할 시간을 제공합니다. HA 조정 타이머가 만료된 후 ASA은(는) 전체 SXP 매핑 데이터베이스를 스캔하고 현재 연결 세션에서 학습되지 않은 모든 매핑 엔트리를 식별합니다. 일치하지 않는 인스턴트 생성 식별자를 가진 매핑 엔트리에 삭제 표시가 됩니다. 이 조정 메커니즘은 조정 타이머와 동일합니다. 시간 값은 조정 타이머와 동일하며 구성이 가능합니다.

SXP 피어가 SXP 연결을 종료하고 나면 ASA이(가) 삭제 보류 타이머를 시작합니다. 리스너로 지정된 SXP 피어만 연결을 종료할 수 있습니다. SXP 피어가 삭제 보류 타이머 실행 중에 연결되는 경우 ASA이(가) 조정 타이머를 시작하고 ASA은(는) IP-SGT 매핑 데이터베이스를 업데이트하여 가장 최근의 매핑을 학습합니다.

IP-SGT Manager 데이터베이스

IP-SGT Manager 데이터베이스는 활성 유닛의 엔트리를 스탠바이 유닛으로 동기화하지 않습니다. IP-SGT Manager 데이터베이스가 IP-SGT 매핑 엔트리를 수신하는 각 소스는 활성 유닛에서 스탠바이 유닛으로 데이터베이스를 동기화한 후 최종 IP-SGT 매핑을 스탠바이 유닛의 IP-SGT Manager에 제공합니다.

버전 9.0(1)의 경우 IP-SGT Manager 데이터베이스는 SXP 소스에서만 IP-SGT 매핑 업데이트를 수신합니다.

ASA-Cisco TrustSec 통합의 기능

ASA은(는) ID 기반 방화벽 기능의 일부로서 Cisco TrustSec을 포함합니다. Cisco TrustSec은 다음과 같은 기능을 제공합니다.

유연성

- ASA은(는) SXP 스피커 또는 리스너 또는 스피커이자 리스너로 구성할 수 있습니다.
- ASA은(는) IPv6 및 IPv6 지원 네트워크 디바이스를 위한 SXP를 지원합니다.
- SXP는 IPv4 및 IPv6 주소를 위한 매핑 엔트리를 변경할 수 있습니다.
- SXP 엔드포인트는 IPv4 및 IPv6 주소를 지원합니다.
- ASA은(는) SXP 버전 2만 지원합니다.
- ASA은(는) 서로 다른 SXP 지원 네트워크 디바이스를 사용하여 SXP 버전을 협상합니다. SXP 버전 협상을 하면 고정 버전 컨피그레이션이 필요 없게 됩니다.
- SXP 조정 타이머가 만료되면 ASA이(가) 보안 그룹 테이블을 갱신하도록 구성하고 온디맨드로 보안 그룹 테이블을 다운로드할 수 있습니다. ASA의 보안 그룹 테이블이 ISE에서 업데이트되면 변경 사항이 적정 보안 정책에 반영됩니다.

- ASA은(는) 소스 또는 대상 필드 또는 두 필드 모두에서 보안 그룹 이름을 기반으로 보안 정책을 지원합니다. 보안 그룹, IP 주소, Active Directory 그룹/사용자 이름 및 FQDN을 기준으로 ASA에서 보안 정책을 구성할 수 있습니다.

가용성

- Active/Active 및 Active/Standby 컨피그레이션으로 ASA에서 보안 그룹 기반 정책을 컨피그레이션할 수 있습니다.
- ASA은(는) 고가용성(HA)을 위해 구성된 ISE와 통신할 수 있습니다.
- 여러 ISE 서버를 ASA에서 구성하고 첫 번째 서버가 도달 불가능한 경우 다음 서버로 이동할 수 있습니다. 그러나 서버 목록이 Cisco TrustSec 환경 데이터의 일부로 다운로드된 경우 무시됩니다.
- ISE에서 다운로드된 PAC 파일이 ASA에서 만료되고 업데이트된 보안 그룹 테이블을 다운로드할 수 없는 경우 ASA은(는) ASA이(가) 업데이트된 테이블을 다운로드할 때까지 마지막으로 다운로드된 보안 그룹 테이블을 기준으로 보안 정책을 시행합니다.

클러스터링

- 레이어 2 네트워크의 경우 모든 유닛이 동일한 IP 주소를 공유합니다. 인터페이스 주소를 변경하면 변경된 컨피그레이션이 다른 모든 유닛으로 전송됩니다. IP 주소가 특정 유닛의 인터페이스에서 업데이트되면 알림이 전송되어 이 유닛의 IP-SGT 로컬 데이터베이스를 업데이트합니다.
- 레이어 3 네트워크의 경우 마스터 유닛의 각 인터페이스에 대해 주소 풀이 컨피그레이션되고 이 컨피그레이션이 슬레이브 유닛으로 동기화됩니다. 마스터 유닛에서 인터페이스에 할당된 IP 주소 알림이 전송되고 IP-SGT 로컬 데이터베이스가 업데이트됩니다. 각 슬레이브 유닛의 IP-SGT 로컬 데이터베이스는 여기에 동기화된 주소 풀 컨피그레이션을 사용하여 마스터 유닛에 대한 IP 주소로 업데이트될 수 있습니다. 여기서 각 인터페이스에 대한 풀의 첫 번째 주소는 항상 마스터 유닛에 속합니다.

  슬레이브 유닛이 부팅되면 마스터 유닛에 알립니다. 그러면 마스터 유닛이 각 인터페이스의 주소 풀을 검토하고 알림을 보낸 새로운 슬레이브 유닛에 대한 IP 주소를 계산하며 마스터 유닛에서 IP-SGT 로컬 데이터베이스를 업데이트합니다. 마스터 유닛은 또한 다른 슬레이브 유닛에 새로운 슬레이브 유닛에 대해 알려줍니다. 이 알림 처리의 일부로서 각 슬레이브 유닛은 새로운 슬레이브 유닛에 대한 IP 주소를 계산하고 이 각 슬레이브 유닛의 IP-SGT 로컬 데이터베이스에 이 엔트리를 추가합니다. 모든 슬레이브 유닛은 IP 주소 값을 결정하기 위한 주소 풀 컨피그레이션을 갖습니다. 각 인터페이스에 대해 이 값은 다음과 같이 결정됩니다.

  Master IP + (M-N):

  M—최대 유닛 수(최대 8개)

  N—알림을 보낸 슬레이브 유닛 번호

  인터페이스에서 IP 주소 풀이 변경되면 모든 슬레이브 유닛과 마스터 유닛에 대한 IP 주소가 다시 조정되고 마스터 유닛은 물론 다른 모든 슬레이브 유닛의 IP-SGT 로컬 데이터베이스에서 업데이트되어야 합니다. 이전 IP 주소를 삭제하고 새로운 IP 주소를 추가해야 합니다.

  컨피그레이션 변경 처리 과정의 일부로서 이 변경된 주소 풀 컨피그레이션이 슬레이브 유닛에 동기화되면 각 슬레이브 유닛은 IP 주소가 변경된 마스터 유닛과 다른 모든 슬레이브 유닛에 대한 IP 주소를 다시 계산하고 이전 IP 주소 엔트리를 삭제하고 새로운 IP 주소를 추가합니다.

확장성

표 33-1은(는) ASA이(가) 지원하는 IP-SGT 매핑 엔트리의 수를 표시합니다.

표 33-1 IP-SGT 매핑 엔트리에 대한 용량 숫자

ASA 모델	IP-SGT 매핑 엔트리 수
5585-X(SSP-10 포함)	18,750
5585-X(SSP-20 포함)	25,000
5585-X(SSP-40 포함)	50,000
5585-X(SSP-60 포함)	100,000

표 33-2은(는) ASA이(가) 지원하는 SXP 연결의 수를 표시합니다.

표 33-2 SXP 연결

ASA 모델	SXP TCP 연결 수
5585-X(SSP-10 포함)	150
5585-X(SSP-20 포함)	250
5585-X(SSP-40 포함)	500
5585-X(SSP-60 포함)	1000

Cisco TrustSec 라이센스 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

Cisco TrustSec 사용 전제 조건

ASA을(를) Cisco TrustSec을 사용하도록 구성하기 전에 다음 작업을 수행해야 합니다.

- 33-11 페이지의 ISE에 ASA을(를) 등록
- 33-11 페이지의 ISE에서 보안 그룹 생성
- 33-11 페이지의 PAC 파일 생성

ISE에 ASA을(를) 등록

ASA이(가) SE에 인정되는 Cisco TrustSec 네트워크 디바이스로 구성되어 있어야 ASA이(가) 성공적으로 PAC 파일을 가져올 수 있습니다. ISE에 ASA을(를) 등록하려면 다음 단계를 수행하십시오.

1. ISE에 로그인합니다.
2. **Administration > Network Devices > Network Devices**를 선택합니다.
3. **Add**를 클릭합니다.
4. ASA의 IP 주소를 입력합니다.
5. 사용자 인증을 위해 ISE가 사용되는 경우 Authentication Settings 영역에 공유 암호를 입력합니다.

   ASA에서 AAA 서버를 구성할 때는 ISE에서 생성한 공유 암호를 입력하십시오. ASA의 AAA 서버는 이 공유 암호를 사용하여 ISE와 통신합니다.
6. ASA에 대한 디바이스 이름, 디바이스 ID, 비밀번호, 다운로드 간격을 지정합니다. 이 작업 수행 방법은 ISE 문서를 참조하십시오.

ISE에서 보안 그룹 생성

ISE와 통신하도록 ASA을(를) 구성할 때는 AAA 서버를 지정합니다. ASA에서 AAA 서버를 구성할 때는 서버 그룹을 지정해야 합니다. 보안 그룹은 RADIUS 프로토콜을 사용하도록 구성되어야 합니다. ISE에서 보안 그룹을 생성하려면 다음 단계를 수행합니다.

1. ISE에 로그인합니다.
2. **Policy > Policy Elements > Results > Security Group Access > Security Group**을 선택합니다.
3. ASA에 대한 보안 그룹을 추가합니다. (보안 그룹은 글로벌이며 ASA별로 다르지 않습니다.)

   ISE가 Security Groups 아래에 태그가 지정된 엔트리를 생성합니다.
4. Security Group Access 영역에서 ASA에 대한 디바이스 ID 자격 증명과 비밀번호를 구성합니다.

PAC 파일 생성

PAC 파일을 생성하기 전에 ASA을 ISE에 등록해야 합니다. PAC 파일을 생성하려면 다음 단계를 수행하십시오.

1. ISE에 로그인합니다.
2. **Administration > Network Resources > Network Devices**를 선택합니다.
3. 디바이스 목록에서 ASA을(를) 선택합니다.
4. SGA(Security Group Access)에서 **Generate PAC**를 클릭합니다.
5. PAC 파일을 암호화하려면 비밀번호를 입력합니다.

   PAC 파일 암호화를 위해 입력하는 비밀번호(또는 암호화 키)는 ISE에서 디바이스 자격 증명의 일부로서 구성된 비밀번호와 별개입니다.

ISE가 PAC 파일을 생성합니다. ASA은(는) 플래시 메모리 또는 TFTP, FTP, HTTP, HTTPS, SMB를 통한 원격 서버로부터 PAC 파일을 가져올 수 있습니다. PAC 파일은 파일을 가져오기 전에 ASA 플래시에 상주하지 않아도 됩니다.

PAC 파일에 대한 정보는 33-15 페이지의 PAC 파일 가져오기을(를) 참조하십시오.

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

SXP 엔드포인트를 위한 IPv6를 지원합니다.

클러스터링 지침

클러스터링 환경의 마스터 유닛 및 슬레이브 유닛에서 지원됩니다.

장애 조치 지침

컨피그레이션을 통한 서버 목록을 지원합니다. 첫 번째 서버에 도달할 수 없는 경우 ASA이(가) 목록의 다음 서버에 도달을 시도합니다. 그러나 Cisco TrustSec 환경 데이터의 일부로 다운로드된 서버 목록은 무시됩니다.

Active/Standby 및 Active/Active 시나리오를 모두 지원합니다. 모든 SXP 데이터가 활성 유닛에서 스탠바이 유닛으로 복제됩니다.

추가 지침

Cisco TrustSec은 단일 컨텍스트 모드 및 다중 컨텍스트 모드에서 Smart Call Home 기능을 지원하지만 시스템 컨텍스트에서는 지원하지 않습니다.

제한 사항

- ASA은(는) 단일 Cisco TrustSec 도메인에서만 상호 운용되도록 구성할 수 있습니다.
- ASA은(는) 디바이스에서 SGT-이름 매핑의 고정 컨피그레이션을 지원하지 않습니다.
- NAT는 SXP 메시지에서 지원되지 않습니다.
- SXP는 네트워크의 시행 포인트로 IP-SGT 매핑을 전달합니다. 액세스 레이어 스위치가 시행 포인트와 다른 NAT 도메인에 속하는 경우 그것이 업로드하는 IP-SGT 맵은 유효하지 않고 시행 디바이스의 IP-SGT 매핑 데이터베이스 조회에서 유효한 결과가 반환되지 않습니다. 따라서 ASA이(가) 시행 디바이스에서 보안 그룹-인식 보안 정책을 적용할 수 없습니다.
- ASA에 대해 SXP 연결에 사용할 기본 비밀번호를 구성하거나 비밀번호를 사용하지 않기로 선택할 수도 있지만 연결별 비밀번호는 SXP 피어에 대해 지원되지 않습니다. 구성된 기본 SXP 비밀번호는 배포 네트워크 전체에서 일관되어야 합니다. 연결별로 비밀번호를 구성하면 연결이 실패하고 경고 메시지가 나타납니다. 기본 비밀번호로 연결을 구성하면 비밀번호 없이 연결을 구성한 것과 마찬가지 결과가 나타납니다.
- 디바이스가 피어로 양방향 연결되었을 때 또는 양방향으로 연결된 디바이스 체인의 일부일 때 SXP 연결 루프가 발생합니다. (ASA이(가) 데이터 센터의 액세스 레이어로부터 리소스에 대한 IP-SGT 매핑을 학습할 수 있습니다. ASA이(가) 이러한 태그를 다운스트림 디바이스로 전파해야 할 수 있습니다.) SXP 연결 루프는 SXP 메시지 전송에서 예기치 않은 동작을 야기할 수 있습니다. ASA이(가) 스피커와 리스너로 구성된 경우 SXP 연결 루프가 발생하여 SXP 데이터를 전송한 피어가 이 데이터를 다시 받게 될 수 있습니다.

- ASA 로컬 IP 주소를 변경할 때는 모든 SXP 피어가 피어 목록을 업데이트했는지 확인해야 합니다. 또한 SXP 피어가 IP 주소를 변경할 경우 이러한 변경 사항이 ASA에 반영되는지 확인해야 합니다.
- 자동 PAC 파일 프로비저닝은 지원되지 않습니다. ASA 관리자는 ISE 관리 인터페이스에서 PAC 파일을 요청하고 ASA(으)로 가져와야 합니다. PAC 파일에 대한 정보는 33-11 페이지의 PAC 파일 생성 및 33-15 페이지의 PAC 파일 가져오기을(를) 참조하십시오.
- PAC 파일에는 기한이 있습니다. 현재 PAC 파일이 만료되기 전에 업데이트된 PAC 파일을 가져와야 합니다. 그러지 않으면 ASA이(가) 환경 데이터 업데이트를 가져올 수 없습니다.
- ISE에서 보안 그룹이 변경되는 경우(이름이 변경되거나 삭제되는 경우) ASA이(가) 변경된 보안 그룹과 연결된 SGT 또는 보안 그룹 이름을 포함하는 ASA 보안 정책의 상태를 변경하지 않습니다. 하지만 ASA은(는) syslog 메시지를 생성하여 해당 보안 정책이 변경되었음을 나타냅니다.

  33-18 페이지의 환경 데이터 갱신에서 ISE의 변경 사항을 포함하기 위한 보안 그룹 테이블 수동 업데이트에 관한 정보는 ASA을(를) 참조하십시오.
- 멀티캐스트 유형은 ISE 1.0에서 지원되지 않습니다.
- SXP 연결은 다음 예에서와같이 ASA에 의해 서로 연결된 두 SXP 피어 사이에서 초기화 상태에 머뭅니다.

  (SXP 피어 A) - - - - (ASA) - - - (SXP 피어 B)

  따라서 Cisco TrustSec과의 통합을 위해 ASA을(를) 구성할 때는 ASA에서 no-NAT, no-SEQ-RAND 및 MD5-AUTHENTICATION TCP 옵션을 활성화하여 SXP 연결을 구성해야 합니다. SXP 피어 사이에서 SXP 포트 TCP 64999로 향하는 트래픽에 대해 TCP 상태 바이패스 정책을 생성합니다. 그런 다음 적절한 인터페이스에 정책을 적용하십시오.

  예를 들어, 다음 명령 집합은 TCP 상태 바이패스 정책에 대해 ASA을(를) 구성하는 방법을 보여줍니다.

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
 tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
 match access-list SXP-MD5-ACL

policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

- ASA 5585-X의 하드웨어 아키텍처는 일반 패킷의 로드 밸런싱을 최적화하도록 설계되었으나 Layer 2 Security Group Tagging Imposition을 포함한 인라인 태그 패킷의 경우는 다릅니다. 수신 인라인 태그 패킷을 처리할 때는 ASA 5585-X에 상단한 성능 저하가 발생할 수 있습니다. 이 문제는 다른 ASA 플랫폼의 인라인 태그 패킷과 ASA 5585-X의 태그가 지정되지 않은 패킷에서는 발생하지 않습니다. 한 가지 해결 방법은 액세스 정책을 오프로드하여 ASA 5585-X로 전달되는 인라인 태그 패킷을 최소화함으로써 스위치가 태그 정책 시행을 처리할 수 있도록 하는 것입니다. 다른 해결 방법은 ASA 5585-X가 태그 패킷을 수신할 필요 없이 IP 주소를 보안 태그에 매핑할 수 있도록 SXP를 사용하는 것입니다.
- ASASM은(는) Layer 2 Security Group Tagging Imposition을 지원하지 않습니다.

Cisco TrustSec 통합을 위한 ASA 구성

Cisco TrustSec 통합을 위한 AAA 서버 구성

Cisco TrustSec과의 통합을 위한 ASA 구성의 일부로써 ASA이(가) ISE와 통신할 수 있도록 구성해야 합니다.

전제 조건

- 참조 서버 그룹은 RADIUS 프로토콜을 사용하도록 구성되어야 합니다. 비 RADIUS 서버 그룹을 ASA에 추가하면 컨피그레이션이 실패합니다.
- ISE가 사용자 인증에도 사용되는 경우 ISE에 ASA을(를) 등록할 때 ISE에 입력한 공유 암호를 얻으십시오. ISE 관리자에게 문의하여 이 정보를 확보하십시오.

Cisco TrustSec 통합을 위해 ASA을(를) ISE와 통신하도록 구성하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 애플리케이션 창에서 **Configuration > Firewall > Identity By TrustSec**을 선택합니다.

2단계 ASA에 서버 그룹을 추가하려면 Server Group Setup 영역에서 **Manage**를 클릭합니다. Configure AAA Server Group 대화 상자가 나타납니다.

3단계 AAA Server Group 필드에 ISE에서 ASA에 대해 생성된 보안 그룹의 이름을 입력합니다.

여기에 지정하는 서버 그룹 이름은 ISE에서 ASA에 대해 생성된 보안 그룹 이름과 반드시 일치해야 합니다. 두 그룹 이름이 일치하지 않으면 ASA이(가) ISE와 통신할 수 없습니다. ISE 관리자에게 문의하여 이 정보를 확보하십시오.

4단계 Protocol 드롭다운 목록에서 RADIUS를 선택합니다.

AAA Server Group 대화 상자의 나머지 필드 작성에 관한 정보는 29-15 페이지의 RADIUS 서버 그룹 구성에서 참조하십시오.

5단계 **OK**를 클릭합니다. ASA이(가) 그룹을 AAA Server Groups 목록에 추가합니다.

6단계 서버를 그룹에 추가하려면 방금 생성한 AAA 서버 그룹을 선택하고 Selected Group 영역의 Servers에서 **Add**를 추가합니다(하단 창). Add AAA Server 대화 상자가 나타납니다.

7단계 Interface Name 필드에서 ISE 서버가 상주하는 네트워크 인터페이스를 선택합니다.

8단계 Server Name 또는 IP Address 필드에 ISE 서버의 IP 주소를 입력합니다.

AAA Server 대화 상자의 나머지 필드 작성에 관한 정보는 29-16 페이지의 그룹에 RADIUS 서버 추가에서 참조하십시오.

9단계 **OK**를 클릭합니다. ASA이(가) ISE 서버를 AAA 서버 목록에 추가합니다.

10단계 **Apply**를 클릭하여 Cisco TrustSec 통합을 위한 ISE 서버 및 서버 그룹 추가 사항을 저장합니다.

변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

PAC 파일 가져오기

PAC(protected access credential) 파일을 ASA(으)로 가져오면 ISE와의 연결이 설정됩니다. 채널을 설정하고 나면 ASA이(가) ISE와 보안 RADIUS 트랜잭션을 시작하고 Cisco TrustSec 환경 데이터(보안 그룹 테이블)를 다운로드합니다. 보안 그룹 테이블은 SGT를 보안 그룹 이름에 매핑합니다. 보안 그룹 이름은 ISE에서 만들어지며, 보안 그룹을 위해 사용하기 편리한 이름을 제공합니다.

보다 구체적으로는 RADIUS 트랜잭션 전에는 아무 채널도 설정되지 않습니다. ASA은(는) 인증을 위한 PAC 파일을 사용하여 ISE와의 RADIUS 트랜잭션을 개시합니다.

팁 PAC 파일은 ASA 및 ISE가 둘 사이의 RADIUS 트랜잭션을 보안할 수 있는 공유 키를 포함합니다. 이 키는 매우 중요하므로 ASA에 안전하게 저장되어야 합니다.

PAC 파일을 가져오면 파일이 ASCII HEX 형식으로 변환되고 비 대화식 모드에서 ASA(으)로 전송됩니다.파일을 성공적으로 가져온 후에는 ASA이(가) ISE에 구성된 디바이스 비밀번호 없이 ISE에서 Cisco TrustSec 환경 데이터를 다운로드합니다.

전제 조건

- ASA이(가) SE에 인정되는 Cisco TrustSec 네트워크 디바이스로 구성되어 있어야 ASA이(가) PAC 파일을 생성할 수 있습니다. ASA은(는) 어떤 PAC 파일이든 가져올 수 있지만 바르게 구성된 ISE에 의해 파일이 생성되었을 때 ASA에서만 동작합니다. 자세한 내용은 33-11 페이지의 ISE에 ASA을(를) 등록를 참조하십시오.
- ISE에서 생성할 때 PAC 파일 암호화에 사용되는 비밀번호를 확보합니다.

  ASA는 PAC 파일 가져오기 및 암호 해독에 이 비밀번호를 필요로 합니다.
- ISE가 PAC 파일에 대한 액세스를 생성합니다. ASA은(는) 플래시 메모리 또는 TFTP, FTP, HTTP, HTTPS, SMB를 통한 원격 서버로부터 PAC 파일을 가져올 수 있습니다. PAC 파일은 파일을 가져오기 전에 ASA 플래시에 상주하지 않아도 됩니다.
- 서버 그룹이 ASA에 대해 구성되었습니다.

제한 사항

- ASA이(가) 장애 조치 컨피그레이션의 일부인 경우 PAC 파일을 기본 ASA 디바이스로 가져와야 합니다.
- ASA이(가) 클러스터링 컨피그레이션의 일부인 경우 PAC 파일을 마스터 디바이스로 가져와야 합니다.

PAC 파일을 가져오려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 애플리케이션 창에서 **Configuration > Firewall > Identity By TrustSec**을 선택합니다.

2단계 SXP를 활성화하려면 **Enable Security Exchange Protocol** 확인란을 선택합니다.

3단계 Server Group Setup 영역에서 **Import PAC**를 클릭합니다. Import PAC 대화 상자가 나타납니다.

4단계 Filename 필드에 다음 형식 중 하나를 사용하여 PAC 파일에 대한 경로와 파일 이름을 입력합니다.

- disk0: disk0의 경로 및 파일 이름
- disk1: disk1의 경로 및 파일 이름
- flash: 플래시의 경로 및 파일 이름

5단계 Password 필드에 PAC 파일 암호화에 사용된 비밀번호를 입력합니다. 비밀번호는 디바이스 자격 증명의 일부로서 ISE에 구성된 비밀번호와는 별개입니다.

6단계 Confirm Password 필드에 비밀번호를 다시 입력하여 확인합니다.

7단계 **Import**를 클릭합니다.

8단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

Security Exchange Protocol 구성

SXP(Security Exchange Protocol)를 구성하려면 ASA에서 프로토콜을 활성화하고 SXP에 대한 다음 기본값을 설정해야 합니다.

- SXP 연결의 소스 IP 주소
- SXP 피어 간의 인증 비밀번호
- SXP 연결을 위한 재시도 간격
- Cisco TrustSec SXP 조정 기간

참고 SXP가 ASA에서 작동하려면 최소 하나의 인터페이스가 UP/UP 상태여야 합니다.

현재 모든 인터페이스가 다운된 상태로 SXP가 활성화된 경우 ASA은(는) SXP가 작동하지 않거나 활성화할 수 없음을 나타내는 메시지를 표시하지 않습니다. **show running-config** 명령을 입력하여 컨피그레이션을 확인하면 명령 출력이 다음 메시지를 표시합니다.

```
"경고: SXP 컨피그레이션이 진행 중입니다. 잠시 기다린 후 다시 시도하십시오."
```

이 메시지는 일반적인 메시지로 SXP가 작동하지 않는 이유를 명시하지는 않습니다.

Cisco TrustSec과의 ASA 통합을 위한 기본 설정을 구성하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 애플리케이션 창에서 **Configuration > Firewall > Identity By TrustSec**을 선택합니다.

2단계 SXP를 활성화하려면 **Enable Security Exchange Protocol** 확인란을 선택합니다. 기본적으로 SXP는 비활성화되어 있습니다.

다중 컨텍스트 모드에서는 사용자 컨텍스트에서 SXP를 활성화합니다.

3단계 Default Source 필드에 SXP 연결을 위한 기본 로컬 IP 주소를 입력합니다. IP 주소는 IPv4 또는 IPv6 주소가 될 수 있습니다.

참고 ASA은(는) 피어 IP 주소가 도달할 수 있는 발신 인터페이스 IP 주소로서 SXP 연결을 위한 로컬 IP 주소를 결정합니다. 구성된 로컬 주소가 발신 인터페이스 IP 주소와 다른 경우 ASA은(는) SXP 피어에 연결할 수 없고 syslog 메시지를 생성합니다.

4단계 Default Password 필드에 SXP 피어를 통한 TCP MD5 인증을 위한 기본 비밀번호를 입력합니다. 기본적으로 SXP 연결에는 설정된 비밀번호가 없습니다.

최대 162자의 암호화된 문자열 또는 최대 80자의 ASCII 키 문자열로 비밀번호를 지정할 수 있습니다. 비밀번호에 대한 암호화 수준 구성은 선택 사항입니다. 암호화 수준을 구성할 경우 하나의 수준만 설정할 수 있습니다.

- 수준 0—암호화되지 않은 일반 텍스트
- 수준 8—암호화된 텍스트

5단계 Retry Timer 필드에 SXP 피어 간 새로운 SXP 연결 설정 시도 사이의 기본 시간 간격을 ASA입력합니다.

ASA은(는) 연결에 성공할 때까지 새로운 SXP 피어에 연결을 시도합니다. ASA에서 연결되지 않은 SXP 연결이 하나 있는 한 재시도 타이머가 트리거됩니다.

0~64000초 범위의 숫자로 재시도 타이머 값을 입력합니다. 0초로 지정하면 타이머가 만료되지 않고 ASA이(가) SXP 피어 연결을 시도하지 않습니다. 타이머 기본값은 120초입니다.

재시도 타이머가 만료되면 ASA이(가) 연결 데이터베이스를 검토하고 데이터베이스에 꺼져 있거나 "보류" 상태인 연결이 있는 경우 ASA이(가) 재시도 타이머를 다시 시작합니다.

6단계 Reconcile Timer 필드에 기본 조정 타이머 값을 입력합니다.

SXP 피어가 SXP 연결을 종료하고 나면 ASA이(가) 보류 타이머를 시작합니다. SXP 피어가 보류 타이머 실행 중에 연결되는 경우 ASA이(가) 조정 타이머를 시작하고 ASA은(는) SXP 매핑 데이터베이스를 업데이트하여 가장 최근의 매핑을 학습합니다.

조정 타이머가 만료되면 ASA이(가) SXP 매핑 데이터베이스를 스캔하여 오래된 매핑 엔트리(이전 연결 세션에서 학습한 엔트리)를 식별합니다. ASA이(가) 이러한 연결을 오래된 연결로 표시합니다. 조정 타이머가 만료되면 ASA이(가) 오래된 엔트리를 SXP 매핑 데이터베이스에서 삭제합니다.

1~64000초 범위의 숫자로 조정 타이머 값을 입력합니다. 타이머 기본값은 120초입니다.

참고 타이머를 0초로 지정하면 조정 타이머가 시작되지 않기 때문에 안 됩니다. 조정 타이머 실행을 허용하지 않으면 오래된 엔트리가 무기한 남아서 정책 시행에서 예기치 못한 결과를 초래할 수 있습니다.

7단계 **Apply**를 클릭하여 기본 설정을 저장합니다.

변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

SXP 연결 피어 추가

피어 간 SXP 연결은 point-to-point 연결이며 TCP를 기본 전송 프로토콜로 사용합니다.

SXP 연결 피어를 추가하려면 다음 단계를 수행하십시오.

1단계 메인 ASDM 애플리케이션 창에서 **Configuration > Firewall > Identity By TrustSec**을 선택합니다.

2단계 필요한 경우 **Enable Security Exchange Protocol** 확인란을 선택하여 SXP를 활성화합니다.

3단계 **Add**를 클릭합니다. Add Connection 대화 상자가 나타납니다.

4단계 Peer IP Address 필드에 SXP 피어의 IPv4 또는 IPv6 주소를 입력합니다. 피어 IP 주소는 ASA 발신 인터페이스에서 도달 가능해야 합니다.

5단계 (선택 사항) Source IP Address 필드에 SXP 연결의 로컬 IPv4 또는 IPv6 주소를 입력합니다. 소스 IP 주소 지정은 선택 사항이나 지정할 경우 컨피그레이션 오류를 방지할 수 있습니다.

6단계 Password 드롭다운 목록에서 다음 값 중 하나를 선택하여 SXP 연결을 위한 인증 키 사용 여부를 지정합니다.

- Default—SXP 연결을 위해 구성된 기본 비밀번호를 사용합니다.

  33-16 페이지의 Security Exchange Protocol 구성를 참조하십시오.
- None—SXP 연결을 위해 비밀번호를 사용하지 않습니다.

7단계 (선택 사항) Mode 드롭다운 목록에서 다음 값 중 하나를 선택하여 SXP 연결 모드를 지정합니다.

- Local—로컬 SXP 디바이스를 사용합니다.
- Peer—피어 SXP 디바이스를 사용합니다.

8단계 Role 드롭다운 목록에서 ASA이(가) SXP 연결에 대한 Speaker 기능을 할지, Listener 기능을 할지 지정합니다.

- Speaker— ASA이(가) IP-SGT 매핑을 업스트림 디바이스로 전달할 수 있습니다.
- Listener—ASA이(가) IP-SGT 매핑을 다운스트림 디바이스에서 수신할 수 있습니다.

33-6 페이지의 ASA에서 스피커 및 리스너 역할에 관해를 참조하십시오.

9단계 **OK**를 클릭합니다. 피어가 Connection Peers 목록에 표시됩니다.

10단계 **Apply**를 클릭하여 설정을 저장합니다.

변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

환경 데이터 갱신

ASA은(는) ISE에서 환경 데이터를 다운로드하며 여기에는 SGT(Security Group Tag) 이름 테이블이 포함됩니다. ASA에서 다음 작업을 완료하면 ASA은(는) ISE에서 수집한 환경 데이터를 자동으로 업데이트합니다.

- ISE와 통신할 AAA 서버를 구성합니다.
- ISE에서 PAC 파일을 가져옵니다.
- ASA이(가) Cisco TrustSec 환경 데이터의 검색에 사용할 AAA 서버 그룹을 식별합니다.

보통은 ISE의 환경 데이터를 수동으로 갱신할 필요가 없지만 ISE에서 보안 그룹이 달라질 수 있습니다. 이러한 변경 사항은 ASA 보안 그룹 테이블에서 데이터를 갱신하기 전에는 ASA에 반영되지 않으므로 ASA에서 데이터를 갱신하여 ISE의 보안 그룹 변경 사항이 ASA에 반영되도록 하십시오.

팁 ISE의 정책 컨피그레이션 변경과 ASA의 수동 데이터 갱신을 유지 관리 기간 중에 예약하는 것이 좋습니다. 이 방법으로 정책 컨피그레이션 변경 사항을 처리하면 ASA에서 보안 그룹 이름이 확인되고 보안 정책이 즉시 활성화될 가능성이 극대화됩니다.

전제 조건

ASA이(가) ISE에서 인정되는 Cisco TrustSec 네트워크 디바이스로 구성되어 있고 ASA이(가) PAC 파일 가져오기에 성공해야만 Cisco TrustSec에 대한 변경 사항이 ASA에 적용됩니다.

제한 사항

- ASA이(가) HA 컨피그레이션의 일부인 경우 기본 ASA 디바이스에서 환경 데이터를 갱신해야 합니다.
- ASA이(가) 클러스터링 컨피그레이션의 일부인 경우 마스터 디바이스에서 환경 데이터를 갱신해야 합니다.

환경 데이터를 갱신하려면다음 단계를 수행합니다.

1단계 메인 ASDM 애플리케이션 창에서 **Configuration > Firewall > Identity By TrustSec**을 선택합니다.

2단계 Server Group Setup 영역에서 **Refresh Environment Data**를 클릭합니다.

ASA이(가) ISE에서 Cisco TrustSec 환경 데이터를 갱신하고 조정 타이머를 설정된 기본값으로 재설정합니다.

보안 정책 구성

Cisco TrustSec 정책을 여러 ASA 기능에서 통합할 수 있습니다. 확장 ACL을 사용하는 모든 기능(이 장에서 미지원으로 명시된 경우 제외)은 Cisco TrustSec을 이용할 수 있습니다. 이제 보안 그룹 인수는 물론 기존의 네트워크 기반 매개변수를 확장 ACL에 추가할 수 있습니다.

- 액세스 규칙을 구성하려면 방화벽 컨피그레이션 가이드을(를) 참조하십시오.
- ACL에서 사용할 수 있는 보안 그룹 객체 그룹을 구성하려면 17-6 페이지의 보안 그룹 객체 그룹 구성을(를) 참조하십시오.

예를 들어 액세스 규칙은 네트워크 정보를 사용하여 인터페이스의 트래픽을 허용하거나 거부합니다. Cisco TrustSec을 통해 보안 그룹을 기반으로 액세스를 제어할 수 있습니다. 예를 들어 sample_securitygroup1 10.0.0.0 255.0.0.0을 위한 액세스 규칙을 만들 수 있으므로 보안 그룹은 서브넷 10.0.0.0/8의 어떤 IP 주소라도 가질 수 있습니다.

보안 그룹 이름의 조합(서버, 사용자, 비관리 디바이스 등), 사용자 기반 속성, 기존 IP 주소 기반 객체(IP 주소, Active Directory 객체 및 FQDN)를 기반으로 보안 정책을 구성할 수 있습니다. 보안 그룹 멤버십은 역할을 넘어 확장되어 디바이스 및 위치 속성을 포함할 수 있으며 사용자 그룹 멤버십과는 별개입니다.

레이어 2 Security Group Tagging Imposition 구성

Cisco TrustSec은 각 네트워크 사용자와 리소스를 식별 및 인증하고 SGT(Security Group Tag)라는 16비트 숫자를 할당합니다. 그러면 이 식별자가 네트워크 홉 사이에 전파되어 ASA, 스위치 및 라우터와 같은 중개 디바이스가 이 ID 태그를 기반으로 정책을 시행할 수 있습니다.

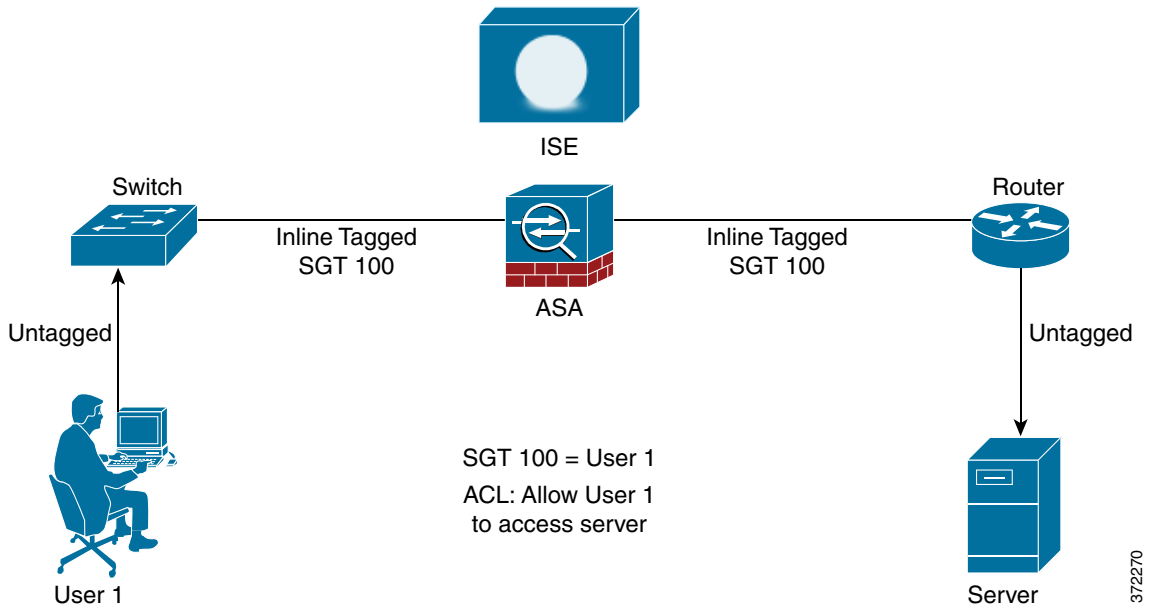
레이어 2 SGT Imposition이라고도 하는 SGT plus Ethernet Tagging은 ASA이(가) Cisco 고유의 이더넷 프레이밍(EtherType 0x8909)을 사용하여 이더넷 인터페이스에서 보안 그룹 태그를 보내고 받도록 하여 소스 보안 그룹 태그를 일반 텍스트 이더넷 프레임으로 삽입할 수 있게 됩니다. ASA은(는) 발신 패킷에 보안 그룹 태그를 삽입하고 수동 인터페이스별 컨피그레이션에 따라 수신 패킷에서 보안 그룹 태그를 처리합니다. 이 기능을 통해 네트워크 디바이스에 걸쳐 엔드포인트 ID를 인라인 hop-by-hop으로 전파할 수 있고 각 홉 사이에서 원활한 레이어 2 SGT Imposition이 가능합니다.

제한 사항

- 물리적 인터페이스, VLAN 인터페이스, 포트 채널 인터페이스 및 중복 인터페이스에서만 지원됩니다.
- BVI와 같은 논리적 인터페이스나 가상 인터페이스에서는 지원되지 않습니다.
- SAP 협상 및 MACsec을 이용한 링크 암호화를 지원하지 않습니다.
- 장애 조치 링크에서는 지원되지 않습니다.
- 클러스터 제어 링크에서는 지원되지 않습니다.
- ASA은(는) SGT가 변경된 경우 기존 흐름을 다시 분류하지 않습니다. 이전 SGT를 기반으로 만들어진 정책 결정은 흐름의 수명 동안 효력을 유지합니다. 그러나 ASA은(는) 이전 SGT를 기반으로 분류된 흐름에 속한 패킷이라도 SGT 변경 사항을 이그레스 패킷에 즉시 반영할 수 있습니다.

그림 33-3은(는) 레이어 2 SGT Imposition의 일반적인 예입니다.

그림 33-3 레이어 2 SGT Imposition



활용 시나리오

표 33-3은(는) 이 기능을 구성할 때 인그레스 트래픽의 예상 동작을 설명합니다.

표 33-3 인그레스 트래픽

인터페이스 구성	수신된 태그 패킷	수신된 태그가 없는 패킷
명령이 발행되지 않습니다.	패킷이 버려집니다.	SGT 값은 IP-SGT Manager에서 가져옵니다.
cts manual 명령이 발행됩니다.	SGT 값은 IP-SGT Manager에서 가져옵니다.	SGT 값은 IP-SGT Manager에서 가져옵니다.
cts manual 명령과 **policy static sgt** *sgt_number* 명령이 모두 발행됩니다.	SGT 값은 **policy static sgt** *sgt_number* 명령에서 가져옵니다.	SGT 값은 **policy static sgt** *sgt_number* 명령에서 가져옵니다.
cts manual 명령과 **policy static sgt** *sgt_number* **trusted** 명령이 모두 발행됩니다.	SGT 값은 패킷의 인라인 SGT에서 가져옵니다.	SGT 값은 **policy static sgt** *sgt_number* 명령에서 가져옵니다.

참고 If IP-SGT Manager에서 일치하는 IP-SGT 매핑이 없는 경우 “Unknown”에 대해 예약된 SGT 값인 “0x0”이 사용됩니다.

표 33-4은(는) 이 기능을 구성할 때 이그레스 트래픽의 예상 동작을 설명합니다.

표 33-4 이그레스 트래픽

인터페이스 구성	전송된 태그 또는 태그가 없는 패킷
명령이 발행되지 않습니다.	태그 없음
cts manual 명령이 발행됩니다.	태그 있음
cts manual 명령과 **propagate sgt** 명령이 모두 발행됩니다.	태그 있음
cts manual 명령과 **no propagate sgt** 명령이 모두 발행됩니다.	태그 없음

표 33-5은(는) 이 기능을 구성할 때 to-the-box 및 from-the-box 트래픽의 예상 동작을 설명합니다.

표 33-5 To-the-box 및 From-the-box 트래픽

인터페이스 구성	수신된 태그 또는 태그가 없는 패킷
to-the-box 트래픽에 대한 인그레스 인터페이스에서 명령이 발행되지 않습니다.	패킷이 버려집니다.
to-the-box traffic에 대한 인그레스 트래픽에서 **cts manual** 명령이 발행됩니다.	패킷이 승인되지만 정책 시행 또는 SGT 전파가 없습니다.
cts manual 명령이 발행되지 않거나 from-the-box 트래픽에 대한 이그레스 인터페이스에서 **cts manual** 명령 및 **no propagate sgt** 명령이 모두 발행됩니다.	태그 없는 패킷이 전송되지만 정책 시행이 없습니다. SGT 번호는 IP-SGT Manager에서 가져옵니다.
cts manual 명령이 발행되거거나 from-the-box 트래픽에 대한 이그레스 인터페이스에서 **cts manual** 명령 및 **propagate sgt** 명령이 모두 발행됩니다.	태그가 있는 패킷이 전송됩니다. SGT 번호는 IP-SGT Manager에서 가져옵니다.

참고 If IP-SGT Manager에서 일치하는 IP-SGT 매핑이 없는 경우 “Unknown”에 대해 예약된 SGT 값인 “0x0”이 사용됩니다.

SGT plus Ethernet Tagging 활성화

SGT plus Ethernet Tagging을 활성화하려면 다음 단계를 수행합니다.

1단계 ASDM에서 다음 옵션 중 하나를 선택합니다.

- **Configuration > Device Setup > Interfaces > Add Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Ethernet Interface > Advanced**

2단계 Secure Group Tagging 영역에서 **Enable secure group tagging for Cisco TrustSec** 확인란을 선택합니다.

인터페이스의 보안 그룹 태그 전파

인터페이스에서 보안 태그의 전파를 활성화 또는 비활성화하려면 다음 단계를 수행합니다.

1단계 ASDM에서 다음 옵션 중 하나를 선택합니다.

- **Configuration > Device Setup > Interfaces > Add Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Ethernet Interface > Advanced**

2단계 Secure Group Tagging 영역에서 **Enable secure group tagging for Cisco TrustSec** 확인란을 선택합니다.

3단계 **Tag egress packets with service group tags** 확인란을 선택합니다.

수동으로 구성된 Cisco TrustSec 링크에 정책 적용

수동 구성 CTS 링크에 정책을 적용하려면 다음 단계를 수행하십시오.

1단계 ASDM에서 다음 옵션 중 하나를 선택합니다.

- **Configuration > Device Setup > Interfaces > Add Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced**
- **Configuration > Device Setup > Interfaces > Add Ethernet Interface > Advanced**

2단계 Secure Group Tagging 영역에서 **Enable secure group tagging for Cisco TrustSec** 확인란을 선택합니다.

3단계 **Tag egress packets with service group tags** 확인란을 선택합니다.

4단계 **Add a static secure group tag to all ingress packets** 확인란을 선택합니다.

5단계 보안 그룹 태그 번호를 입력합니다. 유효한 값 범위는 2~65519입니다.

6단계 **This is a trusted interface. Do not override existing secure group tags** 확인란을 선택합니다.

7단계 **OK**를 클릭하여 설정을 저장하고 Advanced 탭을 닫습니다.

수동으로 IP-SGT 바인딩 구성

IP-SGT 바인딩을 수동으로 구성하려면 다음 단계를 수행합니다.

1단계 **Configuration > Firewall Identity by TrustSec**을 선택합니다.

2단계 SGT Map Setup 영역에서 **Add**를 클릭합니다. (기존 IP-SGT 바인딩을 수정하려면 선택한 다음 **Edit**를 클릭합니다. (기존 IP-SGT 바인딩을 삭제하려면 선택한 다음 **Delete**를 클릭합니다.

Add SGT Map 대화 상자가 나타납니다.

3단계 SGT Map IP 주소와 SGT 값을 적절한 필드에 입력합니다. 유효한 SGT 번호 값은 2~65519입니다.

4단계 **OK**를 클릭하고 **Apply**를 클릭합니다.

새로 구성된 IP-SGT 바인딩이 SGT Map Setup 영역에 표시됩니다.

Cisco TrustSec을 위한 AnyConnect VPN 지원

ASA 버전 9.3(1)은 VPN 세션의 보안 그룹 태깅을 완벽히 지원합니다. SGT(Security Group Tag)는 외부 AAA 서버를 사용하거나 로컬 사용자 데이터베이스 컨피그레이션을 통해 VPN 세션에 할당할 수 있습니다. 그러면 이 태그를 레이어 2 이더넷을 통해 Cisco TrustSec 시스템으로 전파할 수 있습니다. 보안 그룹 태그는 AAA 서버가 SGT를 제공할 수 없을 때 그룹 정책과 로컬 사용자에게 유용합니다.

속성에 AAA 서버에서 VPN 사용자에 할당할 SGT가 없는 경우 ASA은(는) 기본 그룹 정책의 SGT를 사용합니다. 그룹 정책에 SGT가 없다면 0x0 태그가 할당됩니다.

원격 사용자의 서버 연결을 위한 일반적인 단계

1. 사용자가 ASA에 연결합니다.
2. ASA이(가) ISE에서 SGT를 포함할 수 있는 AAA 정보를 요청합니다. ASA은(는) 또한 사용자의 터널링된 트래픽에 대한 IP 주소도 할당합니다.
3. ASA은(는) AAA 정보를 이용하여 터널을 인증하고 생성합니다.
4. ASA은(는) AAA 정보의 SGT와 할당된 IP 주소를 이용하여 SGT를 레이어 2 헤더에 추가합니다.
5. SGT를 포함하는 패킷이 Cisco TrustSec 네트워크의 다음 피어 디바이스로 전달됩니다.

로컬 사용자 및 그룹에 SGT 추가

ASDM의 다음 대화 상자를 통해 SGT 태그를 추가할 수 있습니다.

- Configuration > Remote Access VPN > AAA/Local Users > Local Users 사용자를 추가하거나 편집하려면 VPN Policy 창을 선택하고 Security Group Tag(STG) 값을 입력합니다.
- Configuration > Remote Access VPN > Network (Client) Access > Group Policies, General 탭에서 More Options를 확장하고 Security Group Tag(SGT)에 값을 입력합니다.

Cisco TrustSec 모니터링

ASA에서 Cisco TrustSec을 모니터링하려면 ASDM에서 다음 경로 중 하나를 선택합니다.

Path	목적
Monitoring > Properties > Identity By TrustSec > SXP Connections	Cisco TrustSec 인프라와 SXP 명령에 대해 구성된 기본값을 표시합니다.
Monitoring > Properties > Connections	모든 SXP 연결의 데이터를 표시합니다.IP 주소-보안 그룹 테이블 매핑 엔트리를 필터링하여 데이터를 보안 그룹 테이블 값, 보안 그룹 이름 또는 IP 주소별로 봅니다.
Monitoring > Properties > Identity By TrustSec > Environment Data	ASA의 보안 그룹 테이블에 포함된 Cisco TrustSec 환경 정보를 봅니다.
Monitoring > Properties > Identity By TrustSec > IP Mapping	데이터 경로에 유지되는 IP 주소-보안 그룹 테이블 매핑 데이터베이스에서 IP 주소-보안 그룹 테이블 매핑 엔트리를 표시합니다. IP 주소-보안 그룹 테이블 매핑 엔트리를 필터링하여 데이터를 보안 그룹 테이블 값, 보안 그룹 이름 또는 IP 주소별로 봅니다. **팁** **Where Used**를 클릭하여 선택한 보안 그룹 객체가 ACL에서 또는 다른 보안 그룹 객체와 중첩되어 사용되는 위치를 표시합니다.
Monitoring > Properties > Identity By TrustSec > PAC	ISE에서 ASA(으)로 가져온 PAC 파일에 관한 정보를 표시합니다. PAC 파일이 만료되거나 30일 내에 만료될 경우 경고 메시지를 표시합니다.

추가 참조 자료

참조	설명
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html	기업을 위한 Cisco TrustSec 시스템 및 아키텍처에 대해 설명합니다.
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html	구성 요소 설계 가이드 링크를 포함하여 기업에서 Cisco TrustSec 솔루션 배포를 위한 지침을 제공합니다.
http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf	ASA, 스위치, 무선 LAN(WLAN) 컨트롤러 및 라우터와 함께 사용하는 Cisco TrustSec 솔루션의 개요를 제공합니다.
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html	Cisco TrustSec 솔루션을 지원하는 Cisco 제품을 나열하는 Cisco TrustSec Platform Support Matrix를 제공합니다.

Cisco TrustSec 통합 기능 내역

표 33-6에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 33-6 Cisco TrustSec 통합 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
Cisco TrustSec Integration	9.0(1)	Cisco TrustSec은 기존 identity-aware 인프라 위에 구축되어 네트워크 디바이스 간 데이터 기밀을 보장하고 하나의 플랫폼으로 보안 액세스 서비스를 통합합니다. Cisco TrustSec 기능에서 적용 디바이스는 사용자 속성과 엔드포인트 속성의 조합을 사용하여 역할 기반 및 ID 기반 액세스 제어 결정을 내립니다. 이 릴리스에서는 ASA이(가) Cisco TrustSec과 통합되어 보안 그룹 기반 정책 시행을 제공합니다. Cisco TrustSec 도메인 내의 액세스 정책은 토폴로지에 종속되지 않으며 네트워크 IP 주소가 아닌 소스 및 대상 디바이스의 역할을 기반으로 합니다. ASA은(는) Cisco TrustSec 기능을 애플리케이션 검사와 같은 다른 유형의 보안 그룹 기반 정책에 사용할 수 있습니다. 예를 들어 보안 그룹 기반의 액세스 정책을 포함하는 클래스 맵을 구성할 수 있습니다. 다음 화면을 도입했거나 수정했습니다. Configuration > Firewall > Identity By TrustSec Configuration > Firewall > Objects > Security Groups Object Groups Configuration > Firewall > Access Rules > Add Access Rules Monitoring > Properties > Identity By Tag.
레이어 2 보안 그룹 태그 도입	9.3(1)	보안 그룹 태그와 이더넷 태그를 함께 사용하면서 정책을 적용할 수 있습니다. 레이어 2 SGT Imposition이라고도 하는 SGT plus Ethernet Tagging은 ASA이(가) Cisco 고유의 이더넷 프레이밍(EtherType 0x8909)을 사용하여 이더넷 인터페이스에서 보안 그룹 태그를 보내고 받도록 하여 소스 보안 그룹 태그를 일반 텍스트 이더넷 프레임으로 삽입할 수 있게 됩니다. 다음 화면을 수정했습니다. Configuration > Device Setup > Interfaces > Add Interface > Advanced Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced Configuration > Device Setup > Add Ethernet Interface > Advanced.

ASA 및 Cisco 모바일 지원

ASA 및 Cisco 모바일 지원

Cisco ASA는 ISE(Cisco Identity Services Engine)의 구성 요소인 Cisco ME(Mobile Enablement)에서 관리되는 모바일 디바이스용 기업 네트워크에 대한 오프프레미스 액세스를 제공하는 에지 디바이스입니다. ISE ME를 지원하는 이러한 NAD(네트워크 액세스 디바이스) 역할에서 ASA는 모바일 디바이스 권한 부여, 등록 및 주기적인 체크인을 위한 프록시 역할을 수행합니다. ASA에서는 오프프레미스 원격 모바일 디바이스(AnyConnect Device Management 클라이언트)와 모바일 디바이스 관리자(ISE Mobile Enablement 서버) 간에 안전한 통신 경로를 제공합니다. 이를 통해 AnyConnect 클라이언트 애플리케이션을 실행 중인 오프프레미스 모바일 디바이스에서는 온프레미스 모바일 디바이스와 동일한 방식으로 모바일 디바이스 관리에 참여할 수 있습니다.

이 섹션에서는 ASA별 컨피그레이션 및 동작에 대해서만 설명합니다.

다음을 지정하여 ASA에서 ME 프록시 기능을 구성합니다.

- AnyConnect ME 클라이언트에서 등록 및 체크인 요청을 위해 사용하는 ASA 인터페이스 및 포트
- 클라이언트 인증에 사용되는 AAA 서버. 일반적으로 ISE Mobile Enablement 솔루션에 포함된 Radius 서버입니다.
- ASA를 식별하고 Mobile Enablement 서버에 인증하는 데 사용되는 트러스트 포인트

ASA MDM 프록시 지침 및 제한 사항

- ME Proxy 기능은 단일 컨텍스트 라우터 모드에서만 지원됩니다.
- ME Proxy를 사용하는 데 필요한 ASA 라이센스 요구 사항은 없습니다. ME 라이센스는 ISE에서 시행됩니다.

- 모바일 디바이스에서 실행되는 AnyConnect ME 클라이언트에서는 사용자가 온프레미스(기업 네트워크에 있음)인지 오프프레미스(공용 네트워크에 있음)인지 여부에 상관없이, ME 서버와 통신하는 데 필요한 것과 동일한 URI를 사용합니다. 이를 지원하려면 네트워크의 DNS 컨피그레이션에서는 오프프레미스 지원용 ASA 게이트웨이 및 온프레미스 지원용 ISE PSN(Policy Server Node)에 대한 ME URI를 해석해야 합니다.
- AnyConnect ME 클라이언트와 ASA 간의 인증 및 ASA와 ISE ME 서버 간의 인증을 위해서는 디지털 인증서가 필요합니다. ASA ME Proxy가 통합된 Mobile Enablement 솔루션의 인증서를 계획 및 구성할 경우, 다음을 고려하십시오.
  - ASA를 ISE Policy Service Node에 인증하는 인증서의 경우 동시에 프록시된 디바이스의 표시를 허용해야 합니다.
  - 등록 과정에서 SCEP의 결과로 수신된 모바일 디바이스의 AnyConnect 클라이언트 인증서의 경우, 오프프레미스 상태일 때 ASA에 대한 인증을 거부하고, 온프레미스 상태일 때 ISE를 인증해야 합니다. 마찬가지로, 이와 같은 방식으로 수신된 Applie iOS 모바일 디바이스의 추가 Apple iOS 클라이언트 인증서의 경우에도 이러한 방식으로 작동해야 합니다.
  - Subject Alternative Name(SAN) 필드에서 두 서버의 FQDN을 지정하여, 두 ASA 및 ISE를 모바일 디바이스의 클라이언트에 인증하도록 단일한 인증서를 정의할 수 있습니다.
- 오프프레미스로 관리되는 모바일 디바이스의 경우 ISE My Devices 포털을 사용할 수 없습니다. 이 포털에 액세스하려는 모바일 디바이스 사용자는 온프레미스 상태여야 합니다.

ASA를 MDM Proxy로 구성

시작하기 전에

- 권한 부여 및 어카운팅을 지원하려면 Radius 서버 그룹이 ISE AAA Radius 서버에 액세스할 수 있도록 구성해야 합니다.
- AnyConnect 클라이언트 대신 ASA를 ISE MDM 서버에 인증하려면 트러스트포인트를 구성해야 합니다.

절차

1단계 **Configuration > Remote Access VPN > AAA/Local Users > MDM Proxy**로 이동합니다.

2단계 **Access Interface** 필드를 설정합니다.

- **MDM Server Access Interface(s)** — 클라이언트에서 MDM Proxy 요청을 서비스하는 인터페이스를 선택합니다.
- **Enrollment Port** — 선택한 인터페이스에서 MDM 클라이언트 인증 및 등록 요청에 사용되는 포트를 지정합니다. 기본값은 포트 443입니다.
- **Check-in Port** — (선택 사항) 선택한 인터페이스에서 MDM 체크인 요청에 사용되는 포트를 1~65535 중에서 지정합니다. 이 포트는 다른 서비스에서 사용할 수 없습니다.

3단계 **Radius Server Groups** 필드를 설정합니다.

- **Authentication Server Group** — MDM 클라이언트 인증에 사용되는 인증 서버 그룹을 지정합니다. 사전 구성된 서버 그룹을 선택하거나 새 그룹을 지정합니다.
- **Accounting Server Group** — 다양한 MDM 클라이언트 작업을 기록하는 데 사용되는 어카운팅 서버 그룹을 지정합니다. 사전 구성된 서버 그룹을 선택하거나 새 그룹을 지정합니다.

4단계 **MDM Server Authentication** 필드를 설정합니다.

- **Device Certificate** — ASA에 사용되는 트러스트 포인트를 지정하여 이를 MDM Server(ISE에서)에 인증합니다. 사전 구성된 서버 그룹을 선택하거나 **New**를 선택하여 **Create Radius Server Group for MDM Proxy** 대화 상자를 열고 ISE MDM Radius 서버를 구성합니다.
- **Password Expiration** — 비밀번호가 만료되기 전에 경고 메시지를 전송할 날짜를 지정합니다.

5단계 **OK**를 클릭합니다.

Mobile Enablement Proxy 활동 모니터링

ASA에서 Mobile Enablement 통계를 보려면 ASDM에서 다음 경로를 선택합니다.

Monitoring > VPN > VPN Statistics > MDM Proxy Statistics

ASA Mobile Enablement Proxy의 기능 기록

기능 이름	플랫폼 릴리스	기능 정보
Mobile Enablement 프록시	9.3(1)	ISE Mobile Enablement 솔루션의 구성 요소인 Mobile Enablement 프록시를 사용하면 오프프레미스 모바일 디바이스에서 온프레미스 모바일 디바이스와 똑같은 방식으로 모바일 디바이스를 관리할 수 있습니다. 다음 명령을 도입했습니다. **Configuration > Remote Access VPN > AAA/Local Users > MDM Proxy**

35 장

디지털 인증서

이 장에서는 디지털 인증서를 구성하는 방법에 대해 설명합니다.

디지털 인증서 소개

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. CA는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 컨텍스트에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다.

디지털 인증서를 사용하여 인증할 경우, 적어도 하나의 ID 인증서와 이를 발급한 CA 인증서가 ASA에 있어야 합니다. 이 컨피그레이션에서는 복수의 ID, 루트, 인증서 계층 구조가 가능합니다. ASA는 ID 인증서부터 시작하여 하위 CA 체인을 따라 올라가면서 CRL(Certificate Revocation List)과 대조하는 방식으로 서드파티 인증서를 평가합니다.

다음은 사용 가능한 각기 다른 디지털 인증서의 유형에 대한 설명입니다.

- *CA 인증서*는 다른 인증서에 서명하는 데 사용합니다. 자체 서명되며 *루트 인증서*라고도 합니다. 다른 CA 인증서를 통해 발급된 인증서를 *하위 인증서(subordinate certificate)*라고 합니다.
- CA는 *ID 인증서(identity certificate)*도 발급하는데, 이는 특정 시스템이나 호스트를 위한 인증서입니다.
- *코드 서명 인증서(code-signer certificate)*는 특수한 인증서로서 코드 서명을 위한 디지털 서명을 만드는 데 사용합니다. 서명된 코드 자체에서 인증서의 출처를 나타냅니다.

로컬 CA는 독립적인 CA 기능을 ASA에 통합하고, 인증서를 배포하고, 발급된 인증서에 대해 안전한 해지 검사를 실시합니다. 로컬 CA는 웹사이트 로그인 페이지를 통한 사용자 등록 기능과 함께 안전하고 구성 가능한 내부 인증서 인증 권한을 제공합니다.

참고 CA 인증서와 ID 인증서는 사이트 대 사이트(site-to-site) VPN 연결과 원격 액세스 VPN 연결 모두에 적용됩니다. 이 문서의 절차는 ASDM GUI에서 원격 액세스 VPN을 사용하는 것을 대상으로 합니다.

디지털 인증서는 인증을 위해 디지털 신원 확인을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. CA는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 컨텍스트에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다.

디지털 인증서를 사용하여 인증할 경우, 적어도 하나의 ID 인증서와 이를 발급한 CA 인증서가 ASA에 있어야 합니다. 이 컨피그레이션에서는 복수의 ID, 루트, 인증서 계층 구조가 가능합니다. 다음은 사용 가능한 각기 다른 디지털 인증서의 유형에 대한 설명입니다.

- *CA 인증서*는 다른 인증서에 서명하는 데 사용합니다. 자체 서명되며 *루트 인증서*라고도 합니다.
- 다른 CA 인증서를 통해 발급된 인증서를 *하위 인증서(subordinate certificate)*라고 합니다.

CA는 인증서 요청을 관리하고 디지털 인증서를 발급하는 기능을 담당합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. 디지털 인증서는 사용자 또는 디바이스의 공개 키 사본 하나도 포함합니다. CA는 VeriSign과 같이 신뢰받는 서드파티이거나, 조직 내에서 설정한 전용 (내부) CA일 수 있습니다.

팁 인증서 컨피그레이션 및 로드 밸런싱이 포함된 시나리오의 예는 다음 URL에서 확인하십시오. https://supportforums.cisco.com/docs/DOC-5964

공개 키 암호 방식

공개 키 암호 방식에 의한 디지털 인증서는 디바이스와 사용자를 인증할 방법을 제공합니다. RSA 암호화 시스템과 같은 공개 키 암호 방식에서는 각 사용자가 공개 키와 개인 키로 구성된 키 쌍을 갖습니다. 키는 상호 보완적 역할을 하는데, 둘 중 하나의 키로 암호화된 것은 다른 하나의 키를 사용하여 해독할 수 있습니다.

간단하게 설명하자면, 개인 키를 사용하여 데이터를 암호화할 때 서명이 생성됩니다. 이 서명이 데이터에 첨부되어 수신자에게 전송됩니다. 수신자는 발신자의 공개 키를 데이터에 적용합니다. 데이터와 함께 보내진 서명이 공개 키를 데이터에 적용한 결과와 일치하면 메시지가 유효한 것으로 확인됩니다.

이 프로세스에서는 수신자가 발신자의 공개 키 사본을 가지고 있어야 하며 이 키가 발신자를 가장하는 누군가가 아닌 발신자 본인의 것이어야 합니다.

발신자의 공개 키를 취득하는 것은 대개 외부에서 이루어지거나 설치 시 수행되는 어떤 작업을 통해 이루어집니다. 예를 들어, 대부분의 웹 브라우저는 기본적으로 여러 CA의 루트 인증서가 구성되어 있습니다. VPN의 경우 IPsec의 구성 요소인 IKE 프로토콜에서 보안 연결을 설정하기에 앞서 피어(peer) 디바이스를 인증하는 데 디지털 서명을 사용할 수 있습니다.

인증서 확장성

디지털 인증서가 없으면 IPsec 피어 각각에서 통신 대상인 피어를 하나씩 컨피그레이션해야 합니다. 따라서 네트워크에 새 피어를 추가할 때마다 이 피어가 안전하게 통신하려는 피어 각각의 컨피그레이션을 변경해야 합니다.

디지털 인증서를 사용하면 각 피어가 CA에 등록됩니다. 두 피어가 통신을 시도할 때 서로 인증서를 교환하고 데이터에 디지털 서명을 하여 상대방을 인증합니다. 새로운 피어가 네트워크에 추가되면 그 피어를 CA에 등록하며, 나머지 피어 중 어느 것도 수정할 필요 없습니다. 새 피어가 IPsec 연결을 시도할 때 인증서가 자동으로 교환되고 이 피어는 인증될 수 있습니다.

CA를 이용할 경우, 피어가 원격 피어로 인증서를 보내고 공개 키 암호 작업을 수행하는 방법으로 원격 피어에 자신을 인증합니다. 각 피어가 CA에서 발급한 자신의 고유한 인증서를 보냅니다. 이러한 프로세스는 각 인증서가 해당 피어의 공개 키를 캡슐화하고 각 인증서가 CA에 의해 인증되며 모든 참여 피어가 CA를 인증 기관으로 인정하기 때문에 효과적입니다. 이를 RSA 서명을 사용하는 IKE라고 합니다.

피어는 인증서가 만료될 때까지 계속해서 여러 IPsec 세션을 위해, 여러 IPsec 피어로 인증서를 보낼 수 있습니다. 인증서가 만료되면 피어 관리자가 CA로부터 새로운 인증서를 받아야 합니다.

CA는 더 이상 IPsec에 참여하지 않는 피어의 인증서를 폐기할 수도 있습니다. 폐기된 인증서는 다른 피어에서 유효한 것으로 인정하지 않습니다. 폐기된 인증서는 CRL에 나열되는데, 각 피어는 다른 피어가 보낸 인증서를 받아들이기 전에 이 목록을 점검할 수 있습니다.

어떤 CA는 그 구현에 RA가 포함되어 있습니다. RA란 CA를 위해 프록시 역할을 하는 서버로서 CA가 사용 불가능한 상태이더라도 CA 기능이 계속될 수 있게 합니다.

키 쌍

키 쌍은 다음과 같은 특성을 갖는 RSA 키입니다.

- RSA 키는 SSH 또는 SSL에 사용할 수 있습니다.
- SCEP 등록에서는 RSA 키의 인증을 지원합니다.
- 키를 생성할 때 RSA 키의 최대 키 모듈러스는 2048비트입니다. 기본 크기는 1024입니다. RSA 키 쌍이 1024비트를 초과하는 ID 인증서를 사용하는 SSL 연결 중 상당수는 ASA 및 거부된 클라이언트리스(clientless) 로그인에서 CPU 사용량이 많아질 수 있습니다.
- 서명 작업에서 지원되는 최대 키 크기는 4096비트입니다. 크기가 2048 이상인 키를 사용하는 것이 좋습니다.
- 서명 및 암호화에 모두 사용되는 범용 RSA 키 쌍을 생성하거나, 용도별로 각각 RSA 키 쌍을 생성할 수 있습니다. 서명용 키와 암호화용 키를 달리하면 키의 노출을 줄일 수 있습니다. SSL에서는 서명이 아닌 암호화 용도로 키를 사용하기 때문입니다. 그러나 IKE는 암호화가 아닌 서명을 위해 키를 사용합니다. 각각에 별도의 키를 사용하면 키 노출이 최소화됩니다.

신뢰 지점

신뢰 지점(Trustpoint)을 사용하여 CA와 인증서를 관리하고 추적할 수 있습니다. 신뢰 지점은 CA 또는 ID 쌍을 나타낸 것입니다. 신뢰 지점에는 CA의 ID, CA별 컨피그레이션 매개변수, 하나의 등록된 ID 인증서와의 연결 관계가 포함되어 있습니다.

신뢰 지점을 정의했으면 CA를 지정해야 하는 명령에서 그 이름을 참조할 수 있습니다. 여러 신뢰 지점을 구성할 수 있습니다.

참고 Cisco ASA에서 여러 신뢰 지점이 동일한 CA를 가리킬 경우, 그중 하나만 사용자 인증서의 유효성 검사에 사용할 수 있습니다. 동일한 CA를 가리키는 신뢰 지점 중 어느 것을 그 CA가 발급한 사용자 인증서의 유효성 검사에 사용할 것인가는 **support-user-cert-validation** 명령을 사용하여 제어합니다.

자동 등록의 경우, 등록 URL과 함께 신뢰 지점을 구성해야 하고 그 신뢰 지점이 가리키는 CA가 네트워크에서 사용 가능하고 SCEP를 지원해야 합니다.

신뢰 지점과 연결된 키 쌍 및 발급된 인증서를 PKCS12 형식으로 내보내고 가져올 수 있습니다. 이 형식은 신뢰 지점 컨피그레이션을 다른 ASA에서 수동으로 복제하는 데 유용합니다.

인증서 등록

ASA에서는 신뢰 지점별로 1개의 CA 인증서가 필요하고, 신뢰 지점에서 사용하는 키의 컨피그레이션에 따라 그 자신을 위한 인증서가 1개 또는 2개 필요합니다. 신뢰 지점에서 서명과 암호화에 각기 다른 RSA 키를 사용할 경우 ASA에서는 용도별로 하나씩, 2개의 인증서가 필요합니다. 다른 키 컨피그레이션에서는 인증서 1개만 있으면 됩니다.

ASA에서는 SCEP 자동 등록과 수동 등록을 지원합니다. 즉 터미널에 곧바로 base64 인코딩 인증서를 붙여넣을 수 있습니다. 사이트 대 사이트 VPN에서는 각 ASA를 등록해야 합니다. 원격 액세스 VPN에서는 각 ASA와 각 원격 액세스 VPN 클라이언트를 등록해야 합니다.

SCEP 요청을 위한 프록시

ASA는 AnyConnect와 서드파티 CA 사이에서 SCEP 요청을 프록시할 수 있습니다. CA는 프록시의 역할을 하는 경우에만 ASA에 대한 액세스가 필요합니다. ASA에서 이러한 서비스를 제공하려면, ASA에서 등록 요청을 보내기에 앞서 사용자가 AAA에서 지원하는 방법 중 하나로 인증해야 합니다. 호스트 스캔 및 동적 액세스 정책을 사용하여 등록 자격 요건 규칙을 적용할 수도 있습니다.

ASA에서는 AnyConnect SSL 또는 IKEv2 VPN 세션을 사용하는 경우에만 이 기능을 지원합니다. Cisco IOS CS, Windows Server 2003 CA, Windows Server 2008 CA 등 SCEP 규격을 준수하는 모든 CA를 지원합니다.

클라이언트리스(브라우저 기반) 액세스에서는 SCEP 프록시를 지원하지 않습니다. 단, WebLaunch(클라이언트 없이 시작된 AnyConnect)는 이를 지원합니다.

ASA에서는 인증서에 대한 폴링을 지원하지 않습니다.

ASA에서는 이 기능을 위한 로드 밸런싱을 지원합니다.

폐기 검사

발급된 인증서는 일정한 기간 동안 유효합니다. CA가 유효 기한 전에, 이를테면 보안상의 이유로 또는 이름이나 연결의 변경 때문에 인증서를 폐기하는 경우도 있습니다. CA는 정기적으로 폐기 인증서 목록에 서명하여 이를 배포합니다. 폐기 검사를 활성화할 경우, ASA에서는 인증 목적으로 인증서를 사용할 때마다 CA가 인증서를 폐기하지 않았음을 확인해야 합니다.

폐기 검사를 활성화하면 ASA에서는 PKI 인증서 유효성 검사 과정에서 인증서 폐기 상태를 확인합니다. 이를 위해 CRL 검사, OCSP 또는 둘 다 사용할 수 있습니다. OCSP는 CRL 검사 방법에서 오류가 생긴 경우(예: 서버를 사용할 수 없다는 메시지 표시)에만 사용합니다.

CRL 검사에서 ASA는 CRL에 대한 검색, 구문 분석, 캐싱을 수행합니다. CRL은 폐기된 (그리고 폐기되지 않은) 인증서와 그 인증서 일련 번호의 전체 목록입니다. ASA는 ID 인증서부터 시작하여 하위 CA 체인을 따라 올라가면서 권한 폐기 목록이라고도 하는 CRL을 토대로 인증서를 평가합니다.

OCSP는 보다 확장 가능한 방식으로 폐기 상태를 검사합니다. 즉 특정 인증서의 상태를 쿼리하는 VA(validation authority)를 통해 인증서 상태를 로컬화합니다.

지원되는 CA 서버

ASA에서는 다음 CA 서버를 지원합니다.

Cisco IOS CS, ASA 로컬 CA, 다음을 비롯한 서드파티 X.509 규격 준수 CA 벤더:

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

CRL은 ASA에서 유효 기한이 지나지 않은 어떤 인증서가 그 발급 CA에 의해 폐기되었는지를 확인할 수 있는 방법 중 하나입니다. CRL 컨피그레이션은 신뢰 지점 컨피그레이션에 포함되어 있습니다.

ASA에서 인증서를 확인할 때마다 반드시 CRL 검사를 수행하도록 **revocation-check crl** 명령을 사용하여 구성할 수 있습니다. 또한 **revocation-check crl none** 명령을 사용하여 CRL 검사를 선택 사항으로 설정할 수도 있습니다. 그러면 CA에서 업데이트된 CRL 데이터를 제공할 수 없는 경우에도 인증서 인증에 성공할 수 있습니다.

ASA에서는 HTTP, SCEP 또는 LDAP을 사용하여 CA로부터 CRL을 검색할 수 있습니다. 각 신뢰 지점에 대해 검색된 CRL은 신뢰 지점별로 구성 가능한 기간만큼 캐시에 저장할 수 있습니다.

ASA에서 구성된 기간보다 오랫동안 CRL을 캐시에 보관할 경우, ASA에서는 CRL을 너무 "오래되어" 신뢰할 수 없는 것으로 간주합니다. ASA는 다음번에 인증서 인증을 위해 오래된 CRL을 검사해야 할 때 더 새로운 버전의 CRL 검색을 시도합니다.

ASA에서 CRL을 캐시에 보관하는 기간은 다음 2가지 변수에 따라 결정됩니다.

- **cache-time** 명령에서 지정한 분 수. 기본값은 60분입니다.
- 검색된 CRL의 NextUpdate 필드. 이 필드가 CRL에 없을 수도 있습니다. ASA에서 NextUpdate 필드를 필수 항목으로 하고 사용할 것인가는 **enforcenextupdate** 명령으로 제어합니다.

ASA에서는 이 2가지 변수를 다음과 같이 사용합니다.

- NextUpdate 필드가 필수 항목이 아닐 경우, ASA에서는 **cache-time** 명령으로 지정된 기간이 지나면 오래된 CRL로 표시합니다.

- NextUpdate 필드가 필수 항목일 경우, ASA에서는 **cache-time** 명령으로 지정된 값과 NextUpdate 필드의 값 중 더 빠른 시점에 오래된 CRL로 표시합니다. 예를 들어, **cache-time** 명령에서 100분으로 설정되었고 NextUpdate 필드에서 다음 업데이트가 70분 후라고 지정되었다면 ASA는 70분이 지나면 CRL을 오래되었다고 표시합니다.

ASA에서 어떤 신뢰 지점에 대해 캐시된 모든 CRL을 저장하기에 메모리가 부족할 경우, 가장 오래 전에 사용한 CRL을 삭제하여 새로 검색된 CRL을 위한 공간을 마련합니다.

OCSP

OCSP는 ASA에서 유효 기한이 지나지 않은 어떤 인증서가 그 발급 CA에 의해 폐기되었는지를 확인할 수 있는 방법 중 하나입니다. OCSP 컨피그레이션은 신뢰 지점 컨피그레이션에 포함되어 있습니다.

OCSP는 VA(OCSP 서버, *responder*라고도 함)에서 인증서 상태를 로컬화합니다. ASA는 VA에 특정 인증서의 상태를 쿼리합니다. 이는 CRL 검사보다 확장 가능한 방법이고 더 최신 버전의 폐기 상태 정보를 제공합니다. 또한 PKI 설치 규모가 큰 조직에서 보안 네트워크를 구축하고 확장하는 데 유용합니다.

참고 ASA에서는 OCSP 응답에서 5초의 시간 지연(time skew)을 허용합니다.

ASA에서 인증서를 확인할 때마다 반드시 OCSP 검사를 수행하도록 **revocation-check ocsp** 명령을 사용하여 구성할 수 있습니다. 또한 **revocation-check ocsp none** 명령을 사용하여 OCSP 검사를 선택 사항으로 설정할 수도 있습니다. 그러면 VA에서 업데이트된 OCSP 데이터를 제공할 수 없는 경우에도 인증서 인증에 성공할 수 있습니다.

OCSP에서는 3가지 방법으로 OCSP 서버 URL을 정의할 수 있습니다. ASA에서는 다음 순서대로 이 서버를 사용합니다.

1. **match certificate** 명령을 사용하여 일치 인증서 재정의(override) 규칙에 정의한 OCSP URL
2. **ocsp url** 명령을 사용하여 구성한 OSCP URL
3. 클라이언트 인증서의 AIA 필드

참고 자체 서명된 OCSP responder 인증서의 유효성 검사를 위한 신뢰 지점을 구성하려면, 자체 서명된 responder 인증서를 신뢰할 수 있는 CA 인증서로 간주하면서 해당 신뢰 지점으로 가져옵니다. 그런 다음 클라이언트 인증서의 유효성을 검사하는 신뢰 지점에서 **match certificate** 명령을 구성하여 responder 인증서의 유효성 검사에 자체 서명된 OCSP responder 인증서가 포함된 신뢰 지점을 사용하게 합니다. 클라이언트 인증서의 유효성 검사 경로에 속하지 않은 responder 인증서의 유효성 검사를 구성하는 데에도 동일한 절차를 사용합니다.

일반적으로 OCSP 서버(responder) 인증서가 OCSP 응답에 서명합니다. ASA에서는 응답을 받은 후 responder 인증서의 확인을 시도합니다. 일반적으로 CA는 OCSP responder 인증서의 수명을 상대적으로 짧게 설정하여 문제가 발생할 가능성을 최소화합니다. 일반적으로 CA는 responder 인증서에 ocsp-no-check 확장도 포함하는데, 이는 해당 인증서에 대해 폐기 상태 검사가 필요하지 않음을 나타냅니다. 그러나 이 확장이 없을 경우 ASA에서는 신뢰 지점에 지정된 방식을 사용하여 폐기 상태 검사를 시도합니다. responder 인증서가 확인 불가할 경우 폐기 검사는 실패합니다. 이러한 상황을 방지하기 위해 **revocation-check none** 명령을 사용하여 responder 인증서의 유효성을 검사하는 신뢰 지점을 구성하고 **revocation-check ocsp** 명령을 사용하여 클라이언트 인증서를 구성합니다.

로컬 CA

로컬 CA는 다음 작업을 수행합니다.

- ASA에서 기본 CA 작업 통합
- 인증서 배포
- 발급된 인증서에 대해 안전한 폐기 검사 실시
- ASA에서 브라우저 기반 및 클라이언트 기반 SSL VPN 연결에 사용할 CA 제공
- 외부 인증서 권한 부여를 이용할 필요 없이 사용자에게 신뢰할 수 있는 디지털 인증서 제공
- 안전한 내부 인증서 인증 권한 제공, 웹사이트 로그인을 통한 간편한 사용자 등록 기능 제공

로컬 CA 파일의 저장소

ASA에서는 사용자 정보, 발급된 인증서, 해지 목록의 액세스 및 구현에 로컬 CA 데이터베이스를 사용합니다. 이 데이터베이스는 기본적으로 로컬 플래시 메모리에 상주하지만, ASA에 마운트되고 액세스 가능한 외부 파일 시스템에 상주하도록 구성할 수도 있습니다.

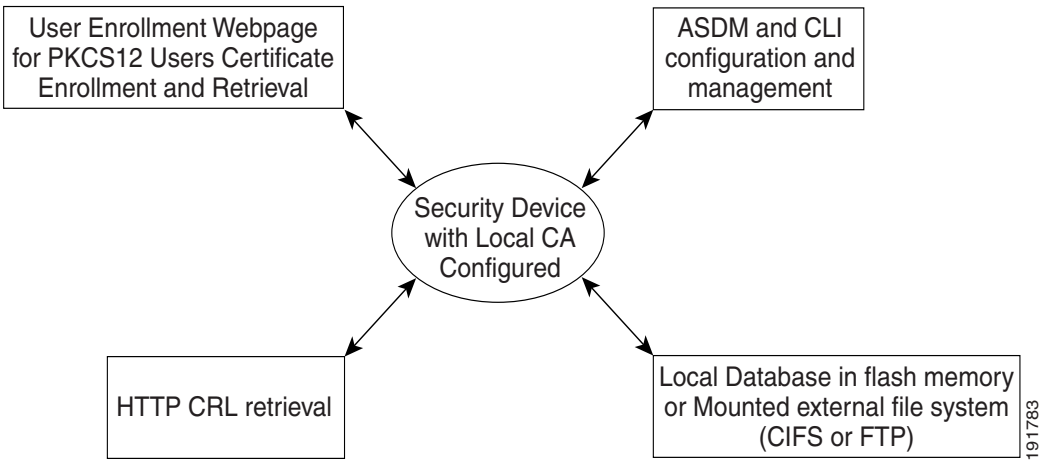
로컬 CA 사용자 데이터베이스에 저장할 수 있는 사용자 수에는 제한이 없습니다. 그러나 플래시 메모리 저장소 문제가 생길 경우, syslog가 생성되어 관리자에게 조치를 취하도록 알리며 저장소 문제가 해결될 때까지 로컬 CA를 사용하지 못할 수도 있습니다. 플래시 메모리는 사용자 수가 3,500명 이하인 데이터베이스를 저장할 수 있습니다. 사용자 수가 3,500명이 넘는 데이터베이스는 외부 저장소가 필요합니다.

로컬 CA 서버

ASA에서 로컬 CA 서버를 구성한 다음에는 사용자가 웹 사이트에 로그인하고 사용자 이름과 로컬 CA 관리자가 제공한 일회용 비밀번호를 입력하여 등록 자격을 검증하는 방법으로 인증서에 등록할 수 있습니다.

그림 35-1에서는 로컬 CA 서버가 ASA에 상주하고 있음을 알리고 웹 사이트 사용자의 등록 요청, 다른 인증서 유효성 검사 디바이스 및 ASA의 CRL 문의를 처리합니다. 로컬 CA 데이터베이스와 컨피그레이션 파일은 ASA 플래시 메모리(기본 저장소) 또는 별도의 스토리지 디바이스에서 유지 관리합니다.

그림 35-1 로컬 CA



인증서 및 사용자 로그인 자격 증명

다음 섹션에서는 인증 및 권한 부여에 인증서와 사용자 로그인 자격 증명(사용자 이름과 비밀번호)을 사용하는 여러 가지 방법에 대해 설명합니다. 이 방법은 IPsec, AnyConnect, 클라이언트리스 SSL VPN에 적용됩니다.

어떤 경우에도 LDAP 권한 부여에서는 비밀번호를 자격 증명으로 사용하지 않습니다. RADIUS 권한 부여에서는 모든 사용자의 공통 비밀번호 또는 사용자 이름을 비밀번호로 사용합니다.

사용자 로그인 자격 증명

기본적인 인증 및 권한 부여 방법에서는 사용자 로그인 자격 증명을 사용합니다.

- 인증
  - ASDM 연결 프로필이라고도 하는 터널 그룹의 인증 서버 그룹 설정을 통해 활성화
  - 사용자 이름과 비밀번호를 자격 증명으로 사용
- 권한 부여
  - ASDM 연결 프로필이라고도 하는 터널 그룹의 권한 부여 서버 그룹 설정을 통해 활성화
  - 사용자 이름을 자격 증명으로 사용

인증서

사용자 디지털 인증서가 구성된 경우 ASA에서는 먼저 인증서의 유효성을 검사합니다. 그러나 인증서의 어떤 DN도 인증용 사용자 이름으로 사용하지 않습니다.

인증과 권한 부여 모두 활성화된 경우 ASA에서는 사용자 로그인 자격 증명을 사용자 인증 및 권한 부여 모두에 사용합니다.

- 인증
  - 인증 서버 그룹 설정에 의해 활성화됨
  - 사용자 이름과 비밀번호를 자격 증명으로 사용
- 권한 부여
  - 권한 부여 서버 그룹 설정에 의해 활성화됨
  - 사용자 이름을 자격 증명으로 사용

인증이 비활성화되고 권한 부여가 활성화된 경우 ASA에서는 기본 DN 필드를 권한 부여에 사용합니다.

- 인증
  - 인증 서버 그룹 설정에 의해 비활성화됨(None으로 설정됨)
  - 자격 증명 사용 안 함
- 권한 부여
  - 권한 부여 서버 그룹 설정에 의해 활성화됨
  - 인증서 기본 DN 필드의 사용자 이름 값을 자격 증명으로 사용

참고 기본 DN 필드가 인증서에 없을 경우 ASA에서는 보조 DN 필드 값을 권한 부여 요청의 사용자 이름으로 사용합니다.

예를 들어, 다음 주체 DN(Subject DN) 필드와 값을 갖는 사용자 인증서가 있다고 가정합니다.

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

기본 DN = EA(E-mail Address)이고 보조 DN = CN(Common Name)이라면 권한 부여 요청에서 쓰일 사용자 이름은 anyuser@example.com입니다.

로컬 인증서의 전제 조건

로컬 인증서는 먼저 다음 조건을 충족해야 합니다.

- ASA가 인증서를 지원하도록 올바르게 구성되어야 합니다. ASA가 잘못 구성되면 등록이 실패하거나 부정확한 정보가 들어 있는 인증서를 요청할 수 있습니다.
- ASA의 호스트 이름과 도메인 이름이 올바르게 구성되어야 합니다. 현재 구성된 호스트 이름 및 도메인 이름을 보려면 **show running-config** 명령을 입력합니다.
- CA 구성에 앞서 ASA 시계가 정확하게 설정되어야 합니다. 인증서는 유효 기간이 시작하고 종료하는 날짜와 시간이 있습니다. ASA에서 CA에 등록하여 인증서를 받을 때 ASA는 현재 시간이 인증서의 유효 기간에 속하는지 확인합니다. 그 범위를 벗어나면 등록이 실패합니다.

SCEP 프록시 지원의 전제 조건

ASA를 서드파티 인증서 요청을 제출하기 위한 프록시로 구성하려면 다음 요구 사항을 충족해야 합니다.

- 엔드포인트에서 AnyConnect Secure Mobility Client 3.0 이상이 실행되고 있어야 합니다.
- 그룹 정책의 연결 프로필에 구성된 인증 방법이 AAA와 인증서 인증을 모두 사용하도록 설정되어야 합니다.
- IKEv2 VPN 연결을 위한 SSL 포트가 열려 있어야 합니다.
- CA가 자동 허용(auto-grant) 모드여야 합니다.

디지털 인증서 지침

컨텍스트 모드 지침

- 서드파티 CA의 경우 단일 컨텍스트 모드에서만 지원됩니다.

장애 조치 지침

- 스테이트풀 장애 조치에서는 세션 복제를 지원하지 않습니다.
- 로컬 CA에 대해서는 장애 조치를 지원하지 않습니다.

IPv6 지침

IPv6를 지원하지 않습니다.

추가 지침

- CA 서버 또는 클라이언트로 구성된 ASA의 경우, 인증서 유효 기한을 권장 종료일인 03:14:08 UTC, 2038년 1월 19일보다 빠르게 설정합니다. 이 지침은 서드파티 벤더로부터 가져온 인증서에도 해당됩니다.

- 장애 조치가 활성화된 상태에서는 로컬 CA를 구성할 수 없습니다. 장애 조치 없는 독립형 ASA에 대해서만 로컬 CA 서버를 구성할 수 있습니다. 자세한 내용은 CSCty43366을 참조하십시오.
- 인증서 등록이 완료되면 ASA는 사용자의 키 쌍과 인증서 체인이 들어 있는 PKCS12 파일을 저장합니다. 이를 위해 각 등록에서 약 2KB의 플래시 메모리 또는 디스크 공간이 필요합니다. 실제 디스크 공간 용량은 구성된 RSA 키 크기 및 인증서 필드에 따라 달라집니다. 사용 가능한 플래시 메모리의 양이 제한된 ASA에서 보류 중인 인증서 등록을 다수 추가할 때 이 점을 염두에 두십시오. 이 PKCS12 파일은 구성된 등록 검색 타임아웃에 도달할 때까지 플래시 메모리에 저장되기 때문입니다. 크기가 2048 이상인 키를 사용하는 것이 좋습니다.
- **lifetime ca-certificate** 명령은 로컬 CA 서버 인증서가 처음 생성될 때(즉, 처음에 로컬 CA 서버를 구성하고 **no shutdown** 명령을 실행할 때) 효력을 발휘합니다. CA 인증서가 만료되면, 구성된 수명 값을 사용하여 새 CA 인증서를 생성합니다. 기존 CA 인증서의 수명 값은 변경할 수 없습니다.
- ASA에서 관리 인터페이스에 대한 ASDM 트래픽 및 HTTPS 트래픽을 보호하는 데 ID 인증서를 사용하도록 구성해야 합니다. SCEP로 자동 생성된 ID 인증서는 재부팅할 때마다 다시 생성되므로, 각자의 ID 인증서를 수동으로 설치해야 합니다. SSL에만 적용되는 이 절차의 예는 다음 URL에서 확인할 수 있습니다.
http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml
- ASA와 AnyConnect 클라이언트는 X520Serialnumber 필드(Subject Name의 일련 번호)가 PrintableString 형식인 인증서에 대해서만 유효성 검사를 수행할 수 있습니다. 일련 번호 형식에서 UTF8과 같은 인코딩을 사용할 경우 인증서 권한 부여가 실패합니다.
- ASA에 인증서 매개 변수를 가져올 때 유효한 문자와 값만 사용합니다.
- 와일드카드(*) 기호를 사용하려면 문자열 값에서 이 문자가 허용되는 인코딩을 CA 서버에서 사용해야 합니다. RFC 5280에서 UTF8String 또는 PrintableString 중 하나를 사용하도록 권장하지만, UTF8String을 사용해야 합니다. PrintableString은 와일드카드를 유효한 문자로 인식하지 않기 때문입니다. ASA에서는 가져오기 과정에서 유효하지 않은 문자 또는 값이 발견되면 그 가져온 인증서를 거부합니다. 예:

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read
162*H÷ytes as CA certificate:0U0= \Ivr"phÕV°3é¼þ0 CRYPTO_PKI(make trustedCerts list)
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

디지털 인증서 구성

이 섹션에서는 로컬 CA 인증서를 구성하는 방법을 설명합니다. 이 유형의 디지털 인증서를 올바르게 구성하려면 제시된 순서대로 작업을 수행해야 합니다.

CA 인증서 인증 구성

CA Certificates 창에서는 사용 가능한 인증서(발급 대상 및 발급자 CA 서버에 의해 식별됨), 인증서가 만료되는 날짜, 해당 신뢰 지점, 인증서 사용법 또는 목적을 표시합니다. CA Certificates 창에서 다음 작업을 수행할 수 있습니다.

- 자체 서명 또는 하위 CA 인증서 인증
- ASA에 CA 인증서 설치
- 새 인증서 컨피그레이션 생성
- 기존 인증서 컨피그레이션 수정
- 수동으로 CA 인증서 취득 및 가져오기
- ASA에서 SCEP를 사용하여 CA에 연결한 다음 자동으로 인증서를 취득 및 설치하도록 지정
- 선택된 인증서의 세부사항 및 발급자 정보 표시
- 기존 CA 인증서의 CRL 액세스
- 기존 CA 인증서의 컨피그레이션 제거
- 신규 또는 수정된 CA 인증서 컨피그레이션 저장
- 변경 사항 취소 및 인증서 컨피그레이션을 원래의 설정으로 되돌리기
- 35-11 페이지의 CA 인증서 추가 또는 설치
- 35-12 페이지의 CA 인증서 구성 수정 또는 제거
- 35-12 페이지의 CA 인증서 세부사항 표시

CA 인증서 추가 또는 설치

PEM 형식 인증서의 수동 구문 분석 또는 SCEP를 사용한 자동 등록을 통해 기존 파일로부터 새 인증서 컨피그레이션을 추가할 수 있습니다. SCEP는 보안 메시징 프로토콜로서 사용자 개입의 필요성을 최소화합니다. 그리고 오로지 VPN Concentrator Manager를 사용한 인증서 등록 및 설치만 허용합니다.

CA 인증서를 추가하거나 설치하려면 다음 단계를 수행합니다.

1단계 ASDM 애플리케이션 기본 창에서 **Configuration > Remote Access VPN > Certificate Management > CA Certificates**를 선택합니다.

2단계 **Add**를 클릭합니다.

Install Certificate 대화 상자가 나타납니다. 선택된 신뢰 지점 이름이 읽기 전용 형식으로 나타납니다.

3단계 기존 파일에서 인증서 컨피그레이션을 추가하려면 **Install from a file** 라디오 버튼을 클릭합니다(기본 설정).

4단계 경로와 파일 이름을 입력하거나 **Browse**를 클릭하여 파일을 찾습니다. 그런 다음 **Install Certificate**를 클릭합니다.

5단계 Certificate Installation 대화 상자가 나타나고 인증서가 성공적으로 설치되었다는 확인 메시지가 표시됩니다. **OK**를 클릭하여 이 대화 상자를 닫습니다.

6단계 수동으로 등록하려면 **Paste certificate in PEM format** 라디오 버튼을 클릭합니다.

7단계 PEM 형식(base64 또는 16진수)을 복사하여 제공된 영역에 붙여넣고 **Install Certificate**를 클릭합니다.

8단계 Certificate Installation 대화 상자가 나타나고 인증서가 성공적으로 설치되었다는 확인 메시지가 표시됩니다. **OK**를 클릭하여 이 대화 상자를 닫습니다.

9단계 자동으로 등록하려면 **Use SCEP** 라디오 버튼을 클릭합니다. ASA에서 SCEP를 사용하여 CA에 연결하고 인증서를 받아서 디바이스에 설치합니다. SCEP를 사용하려면 SCEP를 지원하는 CA에 등록하고 인터넷을 통해 등록해야 합니다. SCEP를 사용하는 자동 등록에서는 다음 정보를 제공해야 합니다.

- 자동으로 설치할 인증서의 경로 및 파일 이름
- 인증서 설치를 재시도할 수 있는 최대 시간(분). 기본 설정은 1분입니다.
- 인증서 설치 재시도 횟수 기본값은 0입니다. 즉 재시도 기간에 무제한으로 재시도할 수 있습니다.

참고 인증서 설치에 SCEP 방식을 사용하려는 경우 SCEP 프록시 지원의 전제 조건을 참조하십시오.

10단계 신규 및 기존 인증서에 대한 추가 컨피그레이션 옵션을 표시하려면 **More Options**를 클릭합니다.

Configuration Options for CA Certificates 창이 나타납니다.

11단계 계속하려면 35-12 페이지의 CA 인증서 구성 수정 또는 제거를 참조하십시오.

CA 인증서 구성 수정 또는 제거

기존 CA 인증서 컨피그레이션을 변경하거나 제거하려면

1단계 기존 CA 인증서 컨피그레이션을 변경하려면 선택한 다음 **Edit**를 클릭합니다.

Edit Options for CA Certificates 창이 나타납니다. 이 설정 중 하나라도 변경하려면 다름 섹션의 절차를 참조하십시오.

- 35-13 페이지의 CRL 검색 정책 구성
- 35-14 페이지의 CRL 검색 방법 구성
- 35-14 페이지의 OCSP 규칙 구성
- 35-15 페이지의 고급 CRL 및 OCSP 설정 구성

2단계 CA 인증서 컨피그레이션을 제거하려면 이를 선택하고 **Delete**를 클릭합니다.

참고 삭제한 인증서 컨피그레이션은 복원할 수 없습니다. 삭제된 인증서를 다시 생성하려면 **Add**를 클릭하여 모든 인증서 컨피그레이션 정보를 다시 입력합니다.

CA 인증서 세부사항 표시

선택된 CA 인증서에 대한 자세한 정보를 표시하려면 **Show Details**를 클릭하여 Certificate Details 대화 상자를 표시합니다. 여기에는 다음 3가지 *표시 전용* 탭이 있습니다.

- General 탭에서는 유형, 일련 번호, 상태, 사용법, 공개 키 유형, CRL 배포 지점, 인증서 유효 기한, 해당 신뢰 지점을 표시합니다. 이 값은 사용 가능 상태와 보류 중 상태 모두에 적용됩니다.
- Issued to 탭에서는 주체 DN 또는 인증서 소유자의 X.500 필드와 그 값을 표시합니다. 이 값은 사용 가능 상태에만 적용됩니다.
- Issued by 탭에서는 인증서를 부여하는 엔티티의 X.500 필드를 표시합니다. 이 값은 사용 가능 상태에만 적용됩니다.

CA 인증서의 폐기 구성

CA 인증서의 폐기를 구성하려면 단일 컨텍스트 또는 다중 컨텍스트 모드에서 다음 사이트 대 사이트 작업을 수행합니다.

1단계 ASDM 애플리케이션 창에서 **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add**를 선택하여 Install Certificates 대화 상자를 표시합니다. 그런 다음 **More Options**를 클릭합니다.

2단계 Configuration Options for CA Certificates 창에서 **Revocation Check** 탭을 클릭합니다.

3단계 인증서의 폐기 검사를 비활성화하려면 **Do not check certificates for revocation** 라디오 버튼을 클릭합니다.

4단계 하나 이상의 폐기 검사 방법(CRL 또는 OCSP)을 선택하려면 **Check certificates for revocation** 라디오 버튼을 클릭합니다.

5단계 Revocation Methods 영역의 오른쪽에 사용 가능한 방법이 표시됩니다. 어떤 방법을 오른쪽으로 이동하여 사용 가능하게 하려면 **Add**를 클릭합니다. 방법의 순서를 변경하려면 **Move Up** 또는 **Move Down**을 클릭합니다.

선택한 방법은 추가한 순서대로 구현됩니다. 어떤 방법에서 오류가 발생할 경우 다음 폐기 검사 방법이 활성화됩니다.

6단계 인증서 유효성 검사 과정에서 폐기 검사 오류를 무시하려면 **Consider certificate valid if revocation checking returns errors** 확인란을 선택합니다.

7단계 Revocation Check 탭을 닫으려면 **OK**를 클릭합니다. 또는 계속하려면 35-13 페이지의 CRL 검색 정책 구성를 참조하십시오.

CRL 검색 정책 구성

CRL 검색 정책을 구성하려면 다음 단계를 수행합니다.

1단계 ASDM 애플리케이션 창에서 **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add**를 선택하여 Install Certificates 대화 상자를 표시합니다. 그런 다음 **More Options**를 클릭합니다.

2단계 검사 중인 인증서의 CRL 배포 지점에서 폐기 검사를 수행하려면 **Use CRL Distribution Point from the certificate** 확인란을 선택합니다.

3단계 CRL 검색에 사용할 URL을 나열하려면 **Use Static URLs configured below** 확인란을 선택합니다. 선택한 URL은 추가한 순서대로 구현됩니다. 지정된 URL에서 오류가 발생할 경우 다음 순서의 URL을 사용합니다.

4단계 Static Configuration 영역에서 **Add**를 클릭합니다.

Add Static URL 대화 상자가 나타납니다.

5단계 URL 필드에 CRL 배포에 사용할 정적 URL을 입력하고 **OK**를 클릭합니다.

입력한 URL이 Static URLs 목록에 나타납니다.

6단계 정적 URL을 변경하려면 이를 선택하고 **Edit**를 클릭합니다.

7단계 기존 정적 URL을 제거하려면 이를 선택하고 **Delete**를 클릭합니다.

8단계 정적 URL이 표시되는 순서를 변경하려면 **Move Up** 또는 **Move Down**을 클릭합니다.

9단계 이 탭을 닫으려면 **OK**를 클릭합니다. 또는 계속하려면 35-14 페이지의 CRL 검색 방법 구성를 참조하십시오.

CRL 검색 방법 구성

CRL 검색 방법을 구성하려면 다음 단계를 수행합니다.

1단계 ASDM 애플리케이션 창에서 **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add**를 선택하여 Install Certificates 대화 상자를 표시합니다. 그런 다음 **More Options**를 클릭합니다.

2단계 Configuration Options for CA Certificates 창에서 **CRL Retrieval Methods** 탭을 클릭합니다.

3단계 다음 3가지 검색 방법 중 하나를 선택합니다.

- CRL 검색에 LDAP을 사용하려면 **Enable Lightweight Directory Access Protocol (LDAP)** 확인란을 선택합니다. CRL 검색에서 LDAP을 사용할 경우, 비밀번호로 액세스하는 명명된 LDAP 서버에 연결하면서 LDAP 세션을 시작합니다. 기본적으로 TCP 포트 389에서 연결됩니다. 다음 필수 매개 변수를 입력합니다.
  - Name
  - Password
  - Confirm Password
  - Default Server(서버 이름)
  - Default Port(389)
- CRL 검색에 HTTP를 사용하려면 **Enable HTTP** 확인란을 선택합니다.

4단계 이 탭을 닫으려면 **OK**를 클릭합니다. 또는 계속하려면 35-14 페이지의 OCSP 규칙 구성를 참조하십시오.

OCSP 규칙 구성

ASA에서는 OCSP 규칙을 우선순위대로 검사하고 가장 먼저 일치하는 것을 적용합니다. X.509 디지털 인증서는 CRL 사용의 대안입니다.

참고 OCSP 규칙을 추가하기 전에 인증서 맵을 구성했는지 확인합니다. 인증서 맵이 구성되지 않은 경우 오류 메시지가 나타납니다. 인증서 맵을 구성하려면 **Configuration > Site-to-Site VPN > Advanced > Certificate to Connection Profile Maps > Rules > Add**를 선택합니다.

X.509 디지털 인증서의 폐기 상태를 확인하기 위한 OCSP 규칙을 구성하려면 다음 단계를 수행합니다.

1단계 ASDM 애플리케이션 창에서 **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add**를 선택하여 Install Certificates 대화 상자를 표시합니다. 그런 다음 **More Options**를 클릭합니다.

2단계 Configuration Options for CA Certificates 창에서 **OCSP Rules** 탭을 클릭합니다.

3단계 인증서 맵을 선택하여 이 OCSP 규칙과 일치하는지 확인합니다. 인증서 맵에서는 사용자 권한이 인증서의 특정 필드와 일치하는지 확인합니다. ASA에서 responder 인증서의 유효성 검사에 사용하는 CA 이름이 Certificate 필드에 나타납니다. 규칙의 우선순위 번호가 Index 필드에 나타납니다. 이 인증서의 OCSP 서버 URL이 URL 필드에 나타납니다.

4단계 새 OCSP 규칙을 추가하려면 **Add**를 클릭합니다.

Add OCSP Rule 대화 상자가 나타납니다.

5단계 드롭다운 목록에서 사용할 인증서 맵을 선택합니다.

6단계 드롭다운 목록에서 사용할 인증서를 선택합니다.

7단계 규칙의 우선순위 번호를 입력합니다.

8단계 이 인증서의 OCSP 서버 URL을 입력합니다.

9단계 완료했으면 **OK**를 클릭하여 이 대화 상자를 닫습니다.

새로 추가된 OCSP 규칙이 목록에 나타납니다.

10단계 기존 OCSP 규칙을 수정하려면 이를 선택하고 **Edit**를 클릭합니다.

11단계 OCSP 규칙을 삭제하려면 이를 선택하고 **Delete**를 클릭합니다.

12단계 이 탭을 닫으려면 **OK**를 클릭합니다. 또는 계속하려면 35-15 페이지의 고급 CRL 및 OCSP 설정 구성를 참조하십시오.

고급 CRL 및 OCSP 설정 구성

발급된 인증서는 일정한 기간 동안 유효합니다. CA가 유효 기한 전에, 이를테면 보안상의 이유로 또는 이름이나 연결의 변경 때문에 인증서를 폐기하는 경우도 있습니다. CA는 정기적으로 폐기 인증서 목록에 서명하여 이를 배포합니다. 폐기 검사를 활성화하면 ASA에서는 CA에서 검증 대상 인증서를 폐기하지 않았음을 확인해야 합니다. ASA에서는 폐기 상태를 확인하는 2가지 방법을 지원합니다. CRL과 OCSP입니다.

추가 CRL 및 OCSP 설정을 구성하려면 다음 단계를 수행합니다.

1단계 ASDM 애플리케이션 창에서 **Configuration > Site-to-Site VPN > Certificate Management > CA Certificates > Add**를 선택하여 Install Certificates 대화 상자를 표시합니다. 그런 다음 **More Options**를 클릭합니다.

2단계 Configuration Options for CA Certificates 창에서 **Advanced** 탭을 클릭합니다.

3단계 CRL Options 영역에서 캐시 새로 고침 간격(분)을 입력합니다. 기본값은 60분입니다. 1분~1440분 범위에서 선택할 수 있습니다. 동일한 CRL을 CA에서 반복적으로 검색할 필요 없이 ASA에서 검색된 CRL을 로컬에 저장할 수 있는데, 이를 CRL 캐싱이라고 합니다. CRL 캐시 용량은 플랫폼에 따라 다르며 모든 컨텍스트를 포괄하여 누적됩니다. 새로 검색된 CRL을 캐시에 저장하려는데 저장 한도를 초과할 경우, ASA에서는 가장 오래전에 사용된 CRL을 제거하면서 사용 가능한 공간을 늘립니다.

4단계 유효한 CRL에서 만료되지 않은 Next Update 값을 갖게 하려면 **Enforce next CRL update** 확인란을 선택합니다. 유효한 CRL에서 Next Update 값이 없거나 만료된 Next Update 값을 갖는 것을 허용하려면 **Enforce next CRL update** 확인란을 선택 취소합니다.

5단계 OCSP Options 영역에서 OCSP 서버의 URL을 입력합니다. ASA에서는 다음 순서대로 OCSP 서버를 사용합니다.

1. 일치하는 인증서 재정의 규칙의 OCSP URL
2. 선택된 OCSP Options 특성에 구성된 OCSP URL
3. 사용자 인증서의 AIA 필드

6단계 기본적으로 **Disable nonce extension** 확인란이 선택되는데, 그러면 암호 기술을 사용하여 요청과 응답을 바인딩함으로써 반복 공격을 방지합니다. 이 프로세스에서는 요청의 확장을 응답의 확장과 일치하는지 비교하면서 동일함을 보장합니다. 사용 중인 OCSP 서버가 이와 같이 일치하는 nonce 확장을 포함하지 않는 미리 생성된 응답을 보내는 경우, **Disable nonce extension** 확인란을 선택 취소합니다.

7단계 Other Options 영역에서 다음 옵션 중 하나를 선택합니다.

- **Accept certificates issued by this CA** 확인란을 선택하면 ASA에서 지정된 CA의 인증서를 승인합니다.
- **Accept certificates issued by the subordinate CAs of this CA** 확인란을 선택하면 ASA에서 하위 CA의 인증서를 승인합니다.

8단계 **OK**를 클릭하여 이 탭을 닫고 **Apply**를 클릭하여 컨피그레이션 변경 사항을 저장합니다.

다음에 할 일

35-30 페이지의 CRL 모니터링를 참조하십시오.

ID 인증서 인증 구성

ID 인증서는 ASA를 통해 VPN 액세스를 인증하는 데 사용할 수 있습니다. 또한 ASDM Launcher를 통해 ASDM에 액세스하는 데에도 ID 인증서를 사용할 수 있습니다. ASDM ID 인증서 마법사 및 지침(http://www.cisco.com/go/asdm-certificate)을 참조하십시오.

Identity Certificates Authentication 창에서 다음 작업을 수행할 수 있습니다.

- 새 ID 인증서 추가 또는 가져오기
- ID 인증서의 세부사항 표시
- 기존 ID 인증서 삭제
- 기존 ID 인증서 내보내기
- 기존 ID 인증서 설치
- Entrust에 ID 인증서 등록

- 35-17 페이지의 ID 인증서 추가 또는 가져오기
- 35-18 페이지의 ID 인증서 세부사항 표시
- 35-19 페이지의 ID 인증서 삭제
- 35-19 페이지의 ID 인증서 내보내기
- 35-20 페이지의 인증서 서명 요청 생성
- 35-21 페이지의 ID 인증서 설치

ID 인증서 추가 또는 가져오기

새 ID 인증서 컨피그레이션을 추가하거나 가져오려면 다음을 수행합니다.

1단계 ASDM 애플리케이션 기본 창에서 **Configuration > Remote Access VPN > Certificate Management > Identity Certificates**를 선택합니다.

2단계 **Add**를 클릭합니다.

Add Identity Certificate 대화 상자가 나타나고, 선택된 신뢰 지점 이름이 맨 위에 표시됩니다.

3단계 기존 파일의 ID 인증서를 가져오려면 **Import the identity certificate from a file (PKCS12 format with Certificate(s) + Private Key)** 라디오 버튼을 클릭합니다.

4단계 PKCS12 파일의 해독에 사용한 패스프레이즈를 입력합니다.

5단계 파일의 경로 이름을 입력하거나 **Browse**를 클릭하여 Import ID Certificate File 대화 상자를 표시합니다. 인증서 파일을 찾고 **Import ID Certificate File**을 클릭합니다.

6단계 새 ID 인증서를 추가하려면 **Add a new identity certificate** 라디오 버튼을 클릭합니다.

7단계 **New**를 클릭하여 Add Key Pair 대화 상자를 표시합니다.

8단계 **RSA** 또는 **ECDSA** 키 유형을 선택합니다.

9단계 기본 키 쌍 이름을 사용하려면 **Use default keypair name** 라디오 버튼을 클릭합니다.

10단계 새 키 쌍 이름을 사용하려면 **Enter a new key pair name** 라디오 버튼을 클릭하고 새 이름을 입력합니다. ASA에서는 여러 키 쌍을 지원합니다.

11단계 드롭다운 목록에서 모듈러스 크기를 선택합니다. 모듈러스 크기를 모를 경우 Entrust에 문의하십시오.

12단계 **General purpose** 라디오 버튼(기본) 또는 **Special** 라디오 버튼을 클릭하여 키 쌍의 용도를 선택합니다. **Special** 라디오 버튼을 선택하면 ASA에서는 2개의 키 쌍을 생성하며, 이는 각각 서명용과 암호화용입니다. 이와 같이 선택하면 해당 ID에 2개의 인증서가 필요함을 의미합니다.

13단계 **Generate Now**를 클릭하여 새 키 쌍을 생성한 다음 **Show**를 클릭하여 Key Pair Details 대화 상자를 표시합니다. 여기에는 다음과 같은 *표시 전용* 정보가 들어 있습니다.

- 공개 키를 인증할 키 쌍의 이름
- 키 쌍이 생성되는 날짜와 시간
- RSA 키 쌍의 용도
- 키 쌍의 모듈러스 크기(비트): 512, 768, 1024, 2048. 기본값은 1024입니다.
- 키 데이터 - 텍스트 형식의 구체적인 키 데이터 포함

14단계 완료했으면 **OK**를 클릭하여 Key Pair Details 대화 상자를 닫습니다.

15단계 ID 인증서의 DN을 구성하기 위해 인증서 주체 DN을 선택합니다. 그리고 **Select**를 클릭하여 Certificate Subject DN 대화 상자를 표시합니다.

16단계 드롭다운 목록에서 추가할 DN 특성을 하나 이상 선택하고 값을 입력한 다음 **Add**를 클릭합니다. 인증서 주체 DN에 사용 가능한 X.500 특성은 다음과 같습니다.

- Common Name(CN)
- Department(OU)
- Company Name(O)
- Country(C)
- State/Province(ST)

- Location(L)
- E-mail Address(EA)

17단계 완료했으면 **OK**를 클릭하여 Certificate Subject DN 대화 상자를 닫습니다.

18단계 자체 서명 인증서를 생성하려면 **Generate self-signed certificate** 확인란을 선택합니다.

19단계 ID 인증서가 로컬 CA의 기능을 하게 하려면 **Act as local certificate authority and issue dynamic certificates to TLS proxy** 확인란을 선택합니다.

20단계 추가 ID 인증서 설정을 하려면 **Advanced**를 클릭합니다.

Advanced Options 대화 상자가 나타납니다. 여기에는 Certificate Parameters, Enrollment Mode, SCEP Challenge Password의 3개 탭이 있습니다.

참고 자체 서명 인증서는 등록 모드 설정과 SCEP 챌린지 비밀번호를 사용할 수 없습니다.

21단계 **Certificate Parameters** 탭을 클릭하고 다음 정보를 입력합니다.

- FQDN - DNS 트리 계층 구조에서 노드의 위치를 나타내는 명확한 도메인 이름
- ID 인증서와 연결된 이메일 주소
- 점으로 구분된 4개의 십진수로 표기되는 네트워크상의 ASA IP 주소
- 인증서 매개 변수에 ASA 일련 번호를 추가하려면 **Include serial number of the device** 확인란을 선택합니다.

22단계 **Enrollment Mode** 탭을 클릭하고 다음 정보를 입력합니다.

- **Request by manual enrollment** 라디오 버튼 또는 **Request from a CA** 라디오 버튼을 클릭하여 등록 방법을 선택합니다.
- SCEP를 통해 자동으로 설치할 인증서의 등록 URL
- ID 인증서 설치를 재시도할 수 있는 최대 시간(분). 기본 설정은 1분입니다.
- ID 인증서 설치를 재시도할 수 있는 최대 횟수. 기본값은 0입니다. 즉 재시도 기간에 횟수 제한 없이 재시도할 수 있습니다.

23단계 **SCEP Challenge Password** 탭을 클릭하고 다음 정보를 입력합니다.

- SCEP 비밀번호
- SCEP 비밀번호 확인

24단계 완료했으면 **OK**를 클릭하여 Advanced Options 대화 상자를 닫습니다.

25단계 Add Identity Certificate 대화 상자에서 **Add Certificate**를 클릭합니다.

새 ID 인증서가 Identity Certificates 목록에 나타납니다.

26단계 **Apply**를 클릭하여 새 ID 인증서 컨피그레이션을 저장합니다.

ID 인증서 세부사항 표시

선택된 ID 인증서에 대한 자세한 정보를 표시하려면 **Show Details**를 클릭하여 Certificate Details 대화 상자를 표시합니다. 여기에는 다음 3가지 *표시 전용* 탭이 있습니다.

- General 탭에서는 유형, 일련 번호, 상태, 사용법, 공개 키 유형, CRL 배포 지점, 인증서 유효 기한, 해당 신뢰 지점을 표시합니다. 이 값은 사용 가능 상태와 보류 중 상태 모두에 적용됩니다.

- Issued to 탭에서는 주체 DN 또는 인증서 소유자의 X.500 필드와 그 값을 표시합니다. 이 값은 사용 가능 상태에만 적용됩니다.
- Issued by 탭에서는 인증서를 부여하는 엔티티의 X.500 필드를 표시합니다. 이 값은 사용 가능 상태에만 적용됩니다.

ID 인증서 삭제

ID 인증서 컨피그레이션을 제거하려면 이를 선택하고 **Delete**를 클릭합니다.

참고 삭제한 인증서 컨피그레이션은 복원할 수 없습니다. 삭제된 인증서를 다시 생성하려면 **Add**를 클릭하여 모든 인증서 컨피그레이션 정보를 다시 입력합니다.

ID 인증서 내보내기

인증서 컨피그레이션을 모든 연결 키 및 인증서와 함께 PKCS12 형식으로 내보낼 수 있습니다. 이는 공개 키 암호 기술 표준이며, base64 인코딩 또는 16진수 형식이 가능합니다. 완전한 컨피그레이션에는 전체 체인(루트 CA 인증서, ID 인증서, 키 쌍)이 포함되지만, 등록 설정(주체 이름, FQDN 등)은 포함되지 않습니다. 이 기능은 주로 장애 조치 또는 로드 밸런싱 컨피그레이션에서 ASA 그룹 전 범위에 인증서를 복제하는 데 사용합니다. 이를테면 원격 액세스 클라이언트가 중앙 조직을 호출하는데, 이 조직은 이 호출을 서비스할 여러 단위가 있습니다. 이 단위는 동일한 인증서 컨피그레이션을 가져야 합니다. 이러한 경우 관리자는 ASA 그룹 전반에서 인증서 컨피그레이션을 내보낸 다음 가져오기를 수행할 수 있습니다.

ID 인증서를 내보내려면 다음 단계를 수행합니다.

1단계 **Export**를 클릭하여 Export Certificate 대화 상자를 표시합니다.

2단계 인증서 컨피그레이션 내보내기에 사용할 PKCS12 형식 파일의 이름을 입력합니다. 또는 **Browse**를 클릭하여 Export ID Certificate File 대화 상자를 표시하고 인증서 컨피그레이션을 내보낼 파일을 찾습니다.

3단계 **PKCS12 Format** 라디오 버튼 또는 **PEM Format** 라디오 버튼을 클릭하여 인증서 형식을 선택합니다.

4단계 내보낼 PKCS12 파일을 암호화하는 데 사용한 패스프레이즈를 입력합니다.

5단계 암호화 패스프레이즈를 확인합니다.

6단계 **Export Certificate**를 클릭하여 인증서 컨피그레이션을 내보냅니다.

정보 대화 상자가 나타나 인증서 컨피그레이션 파일을 지정된 위치에 성공적으로 내보냈음을 알립니다.

인증서 서명 요청 생성

Entrust에 보낼 인증서 서명 요청을 생성하려면 다음 단계를 수행합니다.

1단계 Generate Certificate Signing Request 대화 상자를 표시하기 위해 **Enroll ASA SSL VPN with Entrust**를 클릭합니다.

2단계 Key Pair 영역에서 다음 단계를 수행합니다.

a. 드롭다운 목록에서 구성된 키 쌍 중 하나를 선택합니다.

b. Key Details 대화 상자를 표시하기 위해 **Show**를 클릭합니다. 여기서는 선택된 키 쌍에 대한 정보, 이를테면 생성된 날짜와 시간, 용도(일반 또는 특수한 목적), 모듈러스 크기, 키 데이터를 제공합니다.

c. 완료했으면 **OK**를 클릭하여 Key Details 대화 상자를 닫습니다.

d. **New**를 클릭하여 Add Key Pair 대화 상자를 표시합니다. 계속하려면 35-17 페이지의 ID 인증서 추가 또는 가져오기의 8단계로 진행합니다. 키 쌍을 생성하면 ASA에 보내거나 파일에 저장할 수 있습니다.

3단계 Certificate Subject DN 영역에서 다음 정보를 입력합니다.

a. ASA의 FQDN 또는 IP 주소

b. 회사 이름

c. 2자로 된 국가 코드

4단계 Optional Parameters 영역에서 다음 단계를 수행합니다.

a. Additional DN Attributes 대화 상자를 표시하기 위해 **Select**를 클릭합니다.

b. 드롭다운 목록에서 추가할 특성을 선택하고 값을 입력합니다.

c. **Add**를 클릭하여 특성 테이블에 각 특성을 추가합니다.

d. 특성 테이블에서 어떤 특성을 제거하려면 **Delete**를 클릭합니다.

e. 완료했으면 **OK**를 클릭하여 Additional DN Attributes 대화 상자를 닫습니다.

추가된 특성이 Additional DN Attributes 필드에 나타납니다.

5단계 CA에서 요구할 경우 추가 FQDN 정보를 입력합니다.

6단계 **Generate Request**를 클릭하여 인증서 서명 요청을 생성합니다. 그런 다음 이를 Entrust에 보내거나 파일에 저장했다가 나중에 보냅니다.

Enroll with Entrust 대화 상자가 나타나고 CSR이 표시됩니다.

7단계 등록 프로세스를 마치려면 **request a certificate from Entrust** 링크를 클릭합니다. 제공된 CSR을 복사하여 붙여넣은 다음 제출하면 됩니다. Entrust 웹 양식(http://www.entrust.net/cisco/)을 사용합니다. 또는 나중에 등록하려면 생성된 CSR을 파일에 저장했다가 Identity Certificates 창에서 **enroll with Entrust** 링크를 클릭하여 등록 프로세스를 완료합니다.

8단계 Entrust에서 요청의 진위를 확인한 다음 인증서를 발급합니다. 며칠이 걸릴 수도 있습니다. 이제 Identity Certificate 창에서 보류 중인 요청을 선택하고 **Install**을 클릭하여 인증서를 설치해야 합니다. **Close**를 클릭하여 Enroll with Entrust 대화 상자를 닫습니다.

ID 인증서 설치

Identity Certificates 창의 Install 버튼은 보류 중인 등록이 없는 한 흐리게 표시되어 있습니다. ASA에서 CSR을 수신할 때마다 Identity Certificates 창은 보류 중인 ID 인증서를 표시합니다. 보류 중인 ID 인증서를 선택하면 Install 버튼이 활성화됩니다.

보류 중인 요청을 CA에 전송하면 CA는 이를 등록하고 ASA에 인증서를 보냅니다. 인증서를 수신한 다음 **Install**을 클릭하고 알맞은 ID 인증서를 강조 표시하여 작업을 완료합니다.

보류 중인 ID 인증서를 설치하려면 다음 단계를 수행합니다.

1단계 Identity Certificates 창에서 **Add**를 클릭하여 Add Identity Certificate 대화 상자를 표시합니다.

2단계 Add Identity Certificate 대화 상자에서 **Add a new identity certificate** 라디오 버튼을 클릭합니다.

3단계 (선택 사항) 키 쌍을 변경하거나 새 키 쌍을 만듭니다. 키 쌍이 필요합니다.

4단계 Certificate Subject DN 정보를 입력하고 **Select**를 클릭하여 Certificate Subject DN 대화 상자를 표시합니다.

5단계 CA에서 요구하는 모든 주체 DN 특성을 지정한 다음 **OK**를 클릭하여 Certificate Subject DN 대화 상자를 닫습니다.

6단계 Add Identity Certificate 대화 상자에서 **Advanced**를 클릭하여 Advanced Options 대화 상자를 표시합니다.

7단계 계속하려면 35-16 페이지의 ID 인증서 인증 구성의 17단계부터 23단계까지 참조하십시오.

8단계 Add Identity Certificate 대화 상자에서 **Add Certificate**를 클릭합니다.

Identity Certificate Request 대화 상자가 나타납니다.

9단계 텍스트 형식의 CSR 파일 이름(예: c:\verisign-csr.txt)을 입력하고 **OK**를 클릭합니다.

10단계 CA에 CSR 텍스트 파일을 보냅니다. 또는 CA 웹사이트의 CSR 등록 페이지에 텍스트 파일을 붙여넣을 수 있습니다.

11단계 CA에서 ID 인증서를 보내면 Identity Certificates 창에서 보류 중인 인증서 항목을 선택하고 **Install**을 클릭합니다.

Install Identity Certificate 대화 상자가 나타납니다.

12단계 라디오 버튼을 클릭하여 다음 옵션 중 하나를 선택합니다.

- **파일에서 설치**

  또는 **Browse**를 클릭하여 파일 검색

- **base64 형식으로 인증서 데이터 붙여넣기**

  복사한 인증서 데이터를 제공된 영역에 붙여넣기

13단계 **Install Certificate**를 클릭합니다.

14단계 **Apply**를 클릭하여 새로 설치한 인증서를 ASA 컨피그레이션과 함께 저장합니다.

다음에 할 일

35-22 페이지의 코드 서명 인증서 구성를 참조하십시오.

코드 서명 인증서 구성

코드 서명에서는 실제 실행 코드에 디지털 서명을 추가합니다. 이 디지털 서명은 서명자를 인증하고 코드가 서명된 후 수정되지 않았음을 확인하기에 충분한 정보를 제공합니다.

코드 서명 인증서는 해당 개인 키가 디지털 서명 생성에 사용되는 특수한 인증서입니다. 코드 서명에 사용되는 인증서는 CA로부터 받습니다. 여기서 서명된 코드는 인증서의 출처를 보여줍니다. Code Signer 창에서 코드 서명 인증서를 가져오거나 **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Java Code Signer**를 선택합니다.

Code Signer 창에서 다음 작업을 수행할 수 있습니다.

- 코드 서명 인증서의 세부사항 표시
- 기존 코드 서명 인증서 삭제
- 기존 코드 서명 인증서 가져오기
- 기존 코드 서명 인증서 내보내기
- Entrust에 코드 서명 인증서 등록

- 35-22 페이지의 코드 서명 인증서 세부사항 표시
- 35-22 페이지의 코드 서명 인증서 삭제
- 35-23 페이지의 코드 서명 인증서 가져오기
- 35-23 페이지의 코드 서명 인증서 내보내기

코드 서명 인증서 세부사항 표시

선택된 ID 인증서에 대한 자세한 정보를 표시하려면 **Show Details**를 클릭하여 Certificate Details 대화 상자를 표시합니다. 여기에는 다음 3가지 *표시 전용* 탭이 있습니다.

- General 탭에서는 유형, 일련 번호, 상태, 사용법, 공개 키 유형, CRL 배포 지점, 인증서 유효 기한, 해당 신뢰 지점을 표시합니다. 이 값은 사용 가능 상태와 보류 중 상태 모두에 적용됩니다.
- Issued to 탭에서는 주체 DN 또는 인증서 소유자의 X.500 필드와 그 값을 표시합니다. 이 값은 사용 가능 상태에만 적용됩니다.
- Issued by 탭에서는 인증서를 부여하는 엔티티의 X.500 필드를 표시합니다. 이 값은 사용 가능 상태에만 적용됩니다.

코드 서명 인증서 삭제

코드 서명 인증서 컨피그레이션을 제거하려면 이를 선택하고 **Delete**를 클릭합니다.

참고 삭제한 인증서 컨피그레이션은 복원할 수 없습니다. 삭제된 인증서를 다시 생성하려면 **Import**를 클릭하여 모든 인증서 컨피그레이션 정보를 다시 입력합니다.

코드 서명 인증서 가져오기

코드 서명 인증서를 가져오려면 다음 단계를 수행합니다.

1단계 Code Signer 창에서 **Import**를 클릭하여 Import Certificate 대화 상자를 표시합니다.

2단계 PKCS12-format 파일의 해독에 사용한 패스프레이즈를 입력합니다.

3단계 가져올 파일의 이름을 입력하거나 **Browse**를 클릭하여 Import ID Certificate File 대화 상자를 표시하고 파일을 검색합니다.

4단계 가져올 파일을 선택하고 **Import ID Certificate File**을 클릭합니다.

선택된 인증서 파일이 Import Certificate 대화 상자에 나타납니다.

5단계 **Import Certificate**를 클릭합니다.

가져온 인증서가 Code Signer 창에 나타납니다.

6단계 **Apply**를 클릭하여 새로 가져온 코드 서명 인증서 컨피그레이션을 저장합니다.

코드 서명 인증서 내보내기

코드 서명 인증서를 내보내려면 다음 단계를 수행합니다.

1단계 Code Signer 창에서 **Export**를 클릭하여 Export Certificate 대화 상자를 표시합니다.

2단계 인증서 컨피그레이션 내보내기에 사용할 PKCS12 형식 파일의 이름을 입력합니다.

3단계 Certificate Format 영역에서 공개 키 암호 표준(base64 인코딩 또는 16진수 형식)을 사용하려면 **PKCS12 format** 라디오 버튼을 클릭합니다. 그러지 않으면 **PEM format** 라디오 버튼을 클릭합니다.

4단계 **Browse**를 클릭하여 **Export ID Certificate File** 대화 상자를 표시하고 인증서 컨피그레이션을 내보낼 파일을 찾습니다.

5단계 파일을 선택하고 **Export ID Certificate File**을 클릭합니다.

선택된 인증서 파일이 Export Certificate 대화 상자에 나타납니다.

6단계 내보낼 PKCS12 형식 파일의 해독에 사용한 패스프레이즈를 입력합니다.

7단계 해독 패스프레이즈를 확인합니다.

8단계 **Export Certificate**를 클릭하여 인증서 컨피그레이션을 내보냅니다.

다음에 할 일

35-24 페이지의 로컬 CA를 사용하는 인증를 참조하십시오.

로컬 CA를 사용하는 인증

로컬 CA는 ASA에 상주하면서 안전하고 구성 가능한 방식으로 인증서 인증을 지원하며, 이는 브라우저 기반 및 클라이언트 기반 SSL VPN 연결에서 사용할 수 있습니다.

사용자는 지정된 웹 사이트에 로그인하여 등록합니다. 로컬 CA는 기본적인 인증서 인증 작업을 ASA에 통합하고, 인증서를 배포하고, 발급된 인증서에 대해 안전한 폐기 검사를 실시합니다.

로컬 CA로 다음 작업을 수행할 수 있습니다.

- 로컬 CA 서버 구성
- 로컬 CA 인증서 폐기 및 폐기 해제
- CRL 업데이트
- 로컬 CA 사용자 추가, 수정, 삭제

- 35-24 페이지의 로컬 CA 서버 구성
- 35-27 페이지의 로컬 CA 서버 삭제

로컬 CA 서버 구성

ASA에서 로컬 CA 서버를 구성하려면 다음 단계를 수행합니다.

1단계 **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server**를 선택합니다.

2단계 로컬 CA 서버를 활성화하려면 **Enable Certificate Authority Server** 확인란을 선택합니다. 기본 설정은 비활성화되어 있습니다(선택되지 않음). 로컬 CA 서버를 활성화하면 ASA에서 로컬 CA 서버 인증서, 키 쌍, 필요한 데이터베이스 파일을 생성하고 로컬 CA 서버 인증서와 키 쌍을 PKCS12 파일에 보관합니다.

참고 구성된 로컬 CA를 활성화하기 전에 모든 선택적 설정을 신중하게 검토합니다. 활성화한 다음에는 인증서의 발급자 이름 및 키 크기 서버 값을 변경할 수 없습니다.

자체 서명 인증서 키 사용 확장은 키 암호화, 키 서명, CRL 서명, 인증서 서명을 지원합니다.

3단계 로컬 CA를 처음으로 활성화할 때 7자 이상의 영숫자 활성화 패스프레이즈를 입력하고 확인해야 합니다. 이 패스프레이즈는 로컬 CA 인증서와 저장소에 보관된 로컬 CA 인증서 키 쌍을 보호하고, 로컬 CA 서버가 무단으로 또는 실수로 종료되는 것을 방지합니다. 포컬 CA 인증서 또는 키 쌍을 분실하여 복원해야 하는 경우 PKCS12 아카이브를 잠금 해제하는 데 이 패스프레이즈가 필요합니다.

참고 활성화 패스프레이즈는 로컬 CA 서버를 활성화하는 데 필요합니다. 활성화 패스프레이즈를 기록하여 안전한 곳에 보관하십시오.

4단계 **Apply**를 클릭하여 로컬 CA 인증서 및 키 쌍을 저장합니다. 그러면 ASA를 재부팅하더라도 컨피그레이션이 사라지지 않습니다.

5단계 로컬 CA를 처음으로 구성한 다음 로컬 CA를 변경하거나 재구성하려면 ASA에서 **Enable Certificate Authority Server** 확인란을 선택 취소하여 로컬 CA 서버를 종료해야 합니다. 이 상태에서는 컨피그레이션 및 모든 연결 파일이 저장소에 남아 있으며 등록이 비활성화됩니다.

구성된 로컬 CA를 활성화한 다음에는 다음 2가지 설정이 *표시 전용*이 됩니다.

- Issuer Name 필드 - 발급자 주체 이름과 도메인 이름을 나열하며, 사용자 이름과 subject-name-default DN 설정인 cn=FQDN을 사용하여 구성됩니다. 로컬 CA 서버는 인증서를 부여하는 엔티티입니다. 기본 인증서 이름은 cn=hostname.domainname 형식으로 제공됩니다.
- CA Server Key Size 설정 - 로컬 CA 서버를 위해 생성된 서버 인증서에 사용됩니다. 키 크기는 키당 512비트, 768비트, 1024비트 또는 2048비트가 가능합니다. 기본값은 키당 1024비트입니다. 2048 이상의 키 크기를 사용하는 것이 좋습니다.

6단계 드롭다운 목록에서 로컬 CA 서버에서 발급하는 사용자 인증서별로 생성될 키 쌍의 클라이언트 키 크기를 선택합니다. 키 크기는 키당 512비트, 768비트, 1024비트 또는 2048비트가 가능합니다. 기본값은 키당 1024비트입니다. 2048 이상의 키 크기를 사용하는 것이 좋습니다.

7단계 CA 인증서 수명의 값을 입력합니다. 이는 CA 서버 인증서의 유효 기간(일)을 지정합니다. 기본값은 3650일(10년)입니다. 인증서의 유효 기한이 권장 종료일인 03:14:08 UTC, 2038년 1월 19일보다 빨라야 합니다.

로컬 CA 서버는 만료 30일 전에 자동으로 대체 CA 인증서를 생성합니다. 이 대체 인증서를 다른 모든 디바이스에 내보내고 가져오는 방법으로 만료 후에도 로컬 CA에서 발급한 사용자 인증서에 대한 로컬 CA 인증서 유효성 검사를 수행할 수 있습니다.

사용자에게 만료가 임박했음을 알리기 위해 다음 syslog 메시지가 Latest ASDM Syslog Messages 창에 나타납니다.

```
%ASA-1-717049: Local CA Server certificate is due to expire in days and a replacement
certificate is available for export.
```

참고 관리자는 이 자동 롤오버에 대한 알림을 받으면 기존 인증서가 만료되기 전에 필요한 모든 디바이스에서 새 로컬 CA 인증서의 가져오기가 이루어졌는지 확인해야 합니다.

8단계 클라이언트 인증서 수명의 값을 입력합니다. CA 서버가 발급한 사용자 인증서의 유효 기간(일)을 지정합니다. 기본값은 365일(1년)입니다. 인증서의 유효 기한이 권장 종료일인 03:14:08 UTC, 2038년 1월 19일보다 빨라야 합니다.

SMTP Server & Email Settings 영역에서 다음 설정을 지정하여 로컬 CA 서버에 대한 이메일 액세스를 설정합니다.

a. SMTP 메일 서버 이름 또는 IP 주소를 입력합니다. 또는 말줄임표(...)를 클릭하여 Browse Server Name/IP Address 대화 상자를 표시하고, 여기서 서버 이름 또는 IP 주소를 선택할 수 있습니다. 완료했으면 **OK**를 클릭하여 Browse Server Name/IP Address 대화 상자를 닫습니다.

b. 로컬 CA 사용자에게 이메일 메시지를 보낼 발신 주소를 “adminname@hostname.com” 형식으로 입력합니다. 자동 이메일 메시지를 통해 일회용 비밀번호가 신규 등록 사용자에게 전달되고, 인증서 갱신 또는 업데이트가 필요할 때 이메일 메시지가 발송됩니다.

c. 제목을 입력합니다. 이는 로컬 CA 서버에서 사용자에게 보내는 모든 메시지의 제목줄입니다. 제목을 지정하지 않을 경우 기본값은 “Certificate Enrollment Invitation”이 됩니다.

9단계 추가 옵션을 구성하려면 **More Options** 드롭다운 화살표를 클릭합니다.

10단계 CRL 배포 지점을 입력합니다. 이는 ASA의 CRL 위치입니다. 기본 위치는 http://hostname.domain/+CSCOCA+/asa_ca.crl입니다.

11단계 어떤 인터페이스 및 포트에서 HTTP 다운로드에 CRL을 사용할 수 있게 하려면 드롭다운 목록에서 publish-CRL 인터페이스를 선택합니다. 그런 다음 1-65535 범위에서 임의의 포트 번호를 입력합니다. 기본 포트 번호는 TCP 포트 80입니다.

참고 CRL의 이름을 변경할 수 없습니다. 항상 LOCAL-CA-SERVER.crl이어야 합니다.

이를테면 URL인 http://10.10.10.100/user8/my_crl_file을 입력합니다. 그러면 지정된 IP 주소의 인터페이스만 작동하며, 요청이 수신되면 ASA에서는 /user8/my_crl_file경로가 구성된 URL과 일치하는지 확인합니다. 경로가 일치하면 ASA는 저장된 CRL 파일을 반환합니다.

12단계 CRL의 수명, 즉 유효 기간(시간)을 입력합니다. CA 인증서의 기본값은 6시간입니다.

사용자 인증서가 폐기되거나 폐기 해제될 때마다 로컬 CA가 CRL을 업데이트하고 재배포하지만, 폐기 변경이 없을 경우에는 각 CRL 수명 기간에 한 번씩 CRL이 재배포됩니다. CA Certificates 창에서 **Request CRL**을 클릭하면 즉시 CRL이 업데이트되고 재생성됩니다.

13단계 데이터베이스 저장 위치를 입력하여 로컬 CA 컨피그레이션 및 데이터 파일의 저장 영역을 지정합니다. ASA에서는 사용자 정보, 발급된 인증서, 해지 목록의 액세스 및 구현에 로컬 CA 데이터베이스를 사용합니다. 또는 외부 파일을 지정하려면 외부 파일의 경로 이름을 입력하거나 **Browse**를 클릭하여 Database Storage Location 대화 상자를 표시합니다.

14단계 표시되는 폴더 목록에서 저장 위치를 선택하고 **OK**를 클릭합니다.

참고 플래시 메모리는 사용자 수가 3,500명 이하인 데이터베이스를 저장할 수 있습니다. 사용자 수가 3,500명이 넘는 데이터베이스는 외부 저장소가 필요합니다.

15단계 발급된 인증서에서 사용자 이름에 추가할 기본 주체(DN 문자열) 를 입력합니다.다음 목록의 DN 특성을 사용할 수 있습니다.

- CN(Common Name)
- SN(Surname)
- O(Organization Name)
- L(Locality)
- C(Country)
- OU(Organization Unit)
- EA(E-mail Address)
- ST(State/Province)
- T(Title)

16단계 등록된 사용자가 사용자 인증서 등록 및 검색을 위해 PKCS12 등록 파일을 검색할 수 있는 기간(시간)을 입력합니다. 등록 기간은 OTP 만료 기간과 상관없습니다. 기본값은 24시간입니다.

참고 로컬 CA의 인증서 등록은 클라이언트리스 SSL VPN 연결에서만 지원됩니다. 이 연결 유형에서는 클라이언트와 ASA 간의 통신이 표준 HTML을 사용하는 웹 브라우저를 통해 이루어집니다.

17단계 등록된 사용자에게 이메일로 전달된 일회용 비밀번호의 유효 기간을 입력합니다. 기본값은 72시간입니다.

18단계 며칠 전에 만료 알림 이메일을 사용자에게 보낼 것인지 입력합니다. 기본값은 14일입니다.

19단계 **Apply**를 클릭하여 신규 또는 수정된 CA 인증서 컨피그레이션을 저장합니다. 또는 **Reset**을 클릭하여 모든 변경을 취소하고 원래의 설정으로 돌아갈 수 있습니다.

로컬 CA 서버 삭제

ASA에서 로컬 CA 서버를 제거하려면 다음 단계를 수행합니다.

1단계 CA Server 창에서 **Delete Certificate Authority Server**를 클릭합니다.

Delete Certificate Authority 대화 상자가 나타납니다.

2단계 CA 서버를 삭제하려면 **OK**를 클릭합니다. CA 서버를 유지하려면 **Cancel**을 클릭합니다.

참고 삭제한 로컬 CA 서버는 복원하거나 복구할 수 없습니다. 삭제된 CA 서버 컨피그레이션을 다시 생성하려면 모든 CA 서버 컨피그레이션 정보를 다시 입력해야 합니다.

다음에 할 일

35-27 페이지의 사용자 데이터베이스 관리를 참조하십시오.

사용자 데이터베이스 관리

로컬 CA 사용자 데이터베이스에는 사용자 식별 정보와 사용자 상태(등록됨, 허용됨, 폐기됨 등) 정보가 들어 있습니다. Manage User Database 창에서 다음 작업을 수행할 수 있습니다.

- 로컬 CA 데이터베이스에 사용자 추가
- 기존 사용자 식별 정보 변경
- 로컬 CA 데이터베이스에서 사용자 삭제
- 사용자 등록
- CRL 업데이트
- 사용자에게 이메일로 OTP 제공
- OTP 보기 또는 재생성(대체)

- 35-28 페이지의 로컬 CA 사용자 추가
- 35-28 페이지의 최초 OTP 전송 또는 OTP 대체
- 35-28 페이지의 로컬 CA 사용자 수정
- 35-29 페이지의 로컬 CA 사용자 삭제
- 35-29 페이지의 사용자 등록 허용
- 35-29 페이지의 OTP 보기 또는 재생성

로컬 CA 사용자 추가

로컬 CA 사용자를 추가하려면 다음 단계를 수행합니다.

1단계 로컬 CA 데이터베이스에 새 사용자를 추가하려면 **Add**를 클릭하여 Add User 대화 상자를 표시합니다.

2단계 유효한 사용자 이름을 입력합니다.

3단계 기존의 유효한 이메일 주소를 입력합니다.

4단계 주체(DN 문자열)를 입력합니다. 또는 **Select**를 클릭하여 Certificate Subject DN 대화 상자를 표시합니다.

5단계 드롭다운 목록에서 추가할 DN 특성을 하나 이상 선택하고 값을 입력한 다음 **Add**를 클릭합니다. 인증서 주체 DN에 사용 가능한 X.500 특성은 다음과 같습니다.

- Common Name(CN)
- Department(OU)
- Company Name(O)
- Country(C)
- State/Province(ST)
- Location(L)
- E-mail Address(EA)

6단계 완료했으면 **OK**를 클릭하여 Certificate Subject DN 대화 상자를 닫습니다.

7단계 **Allow enrollment** 확인란을 선택하여 사용자를 등록하고 **Add User**를 클릭합니다.

Manage User Database 창에 새 사용자가 나타납니다.

최초 OTP 전송 또는 OTP 대체

새로 추가된 사용자에게 고유한 OTP 및 로컬 CA 등록 URL이 포함된 등록 허가 알림 이메일을 자동으로 보내려면 **Email OTP**를 클릭합니다.

OTP가 신규 사용자에게 전송되었음을 알리는 대화 상자가 나타납니다.

기존 또는 신규 사용자에게 자동으로 새 OTP를 재배포하고 새 비밀번호가 포함된 알림 이메일을 보내려면 **Replace OTP**를 클릭합니다.

로컬 CA 사용자 수정

데이터베이스의 기존 CA 사용자에 대한 정보를 수정하려면 다음 단계를 수행합니다.

1단계 해당 사용자를 선택하고 **Edit**를 클릭하여 Edit User 대화 상자를 표시합니다.

2단계 유효한 사용자 이름을 입력합니다.

3단계 기존의 유효한 이메일 주소를 입력합니다.

4단계 주체(DN 문자열)를 입력합니다. 또는 **Select**를 클릭하여 Certificate Subject DN 대화 상자를 표시합니다.

5단계 드롭다운 목록에서 변경할 DN 특성을 하나 이상 선택하고 값을 입력한 다음 **Add** 또는 **Delete**를 클릭합니다. 인증서 주체 DN에 사용 가능한 X.500 특성은 다음과 같습니다.

- Common Name(CN)
- Department(OU)
- Company Name(O)
- Country(C)
- State/Province(ST)
- Location(L)
- E-mail Address(EA)

6단계 완료했으면 **OK**를 클릭하여 Certificate Subject DN 대화 상자를 닫습니다.

7단계 **Allow enrollment** 확인란을 선택하여 사용자를 재등록하고 **Edit User**를 클릭합니다.

업데이트된 사용자 세부사항이 Manage User Database 창에 나타납니다.

로컬 CA 사용자 삭제

사용자를 데이터베이스에서 삭제하고 그 사용자에게 발급된 인증서를 로컬 CA 데이터베이스에서 제거하려면 사용자를 선택하고 **Delete**를 클릭합니다.

참고 삭제된 사용자는 복원할 수 없습니다. 삭제된 사용자 레코드를 다시 생성하려면 **Add**를 클릭하여 모든 사용자 정보를 다시 입력합니다.

사용자 등록 허용

선택된 사용자를 등록하려면 **Allow Enrollment**를 클릭합니다.

Manage User Database 창에서 사용자의 상태가 "enrolled"로 바뀝니다.

참고 사용자가 이미 등록된 경우 오류 메시지가 나타납니다.

OTP 보기 또는 재생성

선택된 사용자의 OTP를 보거나 재생성하려면 다음 단계를 수행합니다.

1단계 **View/Regenerate OTP**를 클릭하여 View & Regenerate OTP 대화 상자를 표시합니다.

현재 OTP가 나타납니다.

2단계 완료했으면 **OK**를 클릭하여 View & Regenerate OTP 대화 상자를 닫습니다.

3단계 OTP를 재생성하려면 **Regenerate OTP**를 클릭합니다.

새로 생성된 OTP가 나타납니다.

4단계 **OK**를 클릭하여 View & Regenerate OTP 대화 상자를 닫습니다.

다음에 할 일

35-30 페이지의 사용자 인증서 관리를 참조하십시오.

사용자 인증서 관리

인증서 상태를 변경하려면 다음 단계를 수행합니다.

1단계 Manage User Certificates 창에서 사용자 이름 또는 인증서 일련 번호를 참조하여 인증서를 선택합니다.

2단계 다음 옵션 중 하나를 선택합니다.

- 사용자 인증서 수명이 다한 경우 사용자 액세스를 제거하려면 **Revoke**를 클릭합니다. 또한 로컬 CA가 인증서 데이터베이스에서 해당 인증서를 폐기됨으로 표시하고 자동으로 정보를 업데이트하며 CRL을 재배포합니다.
- 액세스를 복원하려면 폐기된 인증서를 선택하고 **Unrevoke**를 클릭합니다. 또한 로컬 CA가 인증서 데이터베이스에서 해당 인증서를 폐기 해제됨으로 표시하고 자동으로 인증서 정보를 업데이트하며 업데이트된 CRL을 재배포합니다.

3단계 완료했으면 **Apply**를 클릭하여 변경 사항을 저장합니다.

다음에 할 일

35-30 페이지의 CRL 모니터링를 참조하십시오.

CRL 모니터링

CRL을 모니터링하려면 다음 단계를 수행합니다.

1단계 ASDM 기본 애플리케이션 창에서 **Monitoring > Properties > CRL**을 선택합니다.

2단계 CRL 영역의 드롭다운 목록에서 CA 인증서 이름을 선택합니다.

3단계 CRL 세부사항을 표시하려면 **View CRL**을 클릭합니다. 예:

```
CRL Issuer Name:
    cn=asa4.cisco.com
    LastUpdate: 09:58:34 UTC Nov 11 2010
    NextUpdate: 15:58:34 UTC Nov 11 2010
    Cached Until: 15:58:34 UTC Nov 11 2010
    Retrieved from CRL Distribution Point:
      ** CDP Not Published - Retrieved via SCEP
    Size (bytes): 224
    Associated Trustpoints: LOCAL-CA-SERVER
```

4단계 완료했으면 **Clear CRL**을 클릭하여 CRL 세부사항을 제거하고 표시할 다른 CA 인증서를 선택합니다.

인증서 관리 기능 내역

표 35-1 인증서 관리 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
인증서 관리	7.0(1)	디지털 인증서(CA 인증서, ID 인증서, 코드 서명 인증서 포함)가 인증을 위한 디지털 식별을 수행합니다. 디지털 인증서에는 어떤 디바이스나 사용자를 식별하는 정보, 이를테면 이름, 일련 번호, 회사, 부서 또는 IP 주소가 들어 있습니다. CA는 인증서에 "서명"하여 그 진위를 확인함으로써 해당 디바이스 또는 사용자의 ID를 보장하는 신뢰받는 기관입니다. CA는 PKI 컨텍스트에서 디지털 인증서를 발급하는데, PKI에서는 공개 키 또는 개인 키 암호화를 사용하여 보안을 보장합니다. 다음 화면을 도입했습니다. Configuration > Remote Access VPN > Certificate Management Configuration > Site-to-Site VPN > Certificate Management 다음 화면을 도입했거나 수정했습니다. Configuration > Firewall > Advanced > Certificate Management > CA Certificates Configuration > Device Management > Certificate Management > CA Certificates
인증서 관리	7.2(1)	
인증서 관리	8.0(2)	
SCEP 프록시	8.4(1)	서드파티 CA의 디바이스 인증서를 안전하게 배포하는 이 기능을 도입했습니다.

파 트 8

시스템 관리

36 장

관리 액세스

이 장에서는 텔넷, SSH, HTTPS(ASDM 사용)를 통한 시스템 관리를 위해 Cisco ASA에 액세스하는 방법, 사용자를 인증하고 권한을 부여하는 방법, 로그인 배너를 만드는 방법을 설명합니다.

참고 관리 액세스를 위해 ASA 인터페이스에 액세스할 때 호스트 IP 주소를 허용하는 액세스 규칙은 필요 없습니다. 이 장의 섹션에 따라 관리 액세스를 구성하면 됩니다.

ASDM, 텔넷 또는 SSH를 위한 ASA 액세스 구성

이 섹션에서는 클라이언트에서 ASDM, 텔넷 또는 SSH를 사용하여 ASA에 액세스하는 방법을 설명합니다.

ASA에서 ASDM, 텔넷 또는 SSH에 액세스하기 위한 라이센싱 요구 사항

다음 표는 이 기능의 라이센싱 요구 사항을 보여줍니다.

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

IPv6를 지원합니다.

모델 지침

ASASM에서는 스위치에서 ASASM로의 세션이 텔넷 세션입니다. 그러나 이 섹션에 따른 텔넷 액세스 컨피그레이션은 필요 없습니다.

추가 지침

- VPN 터널 내에서 텔넷을 사용하지 않는 한 텔넷을 최하위 보안 인터페이스에서 사용할 수 없습니다.
- ASA 를 시작할 때 사용한 것과 다른 인터페이스에 대한 관리 액세스는 지원되지 않습니다. 예를 들어, 관리 호스트가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 관리 연결만 시작할 수 있습니다. 이 규칙의 유일한 예외는 VPN 연결을 거치는 경우입니다. 36-8 페이지의 VPN 터널을 통한 관리 액세스 구성를 참조하십시오.
- ASA에서는 다음을 허용합니다.
  - 컨텍스트당 최대 5개의 동시 텔넷 연결 가능. 모든 컨텍스트에서 최대 100개의 연결 할당 가능
  - 컨텍스트당 최대 5개의 동시 SSH 연결 가능. 모든 컨텍스트에서 최대 100개의 연결 할당 가능
  - 컨텍스트당 최대 5개의 동시 ASDM인스턴스 가능. 모든 컨텍스트에서 최대 32개의 ASDM 인스턴스 가능.
- ASA는 SSH 버전 1 및 버전 2에서 제공하는 SSH 원격 셸 기능을 지원하고, DES 및 3DES 암호를 지원합니다.
- SSL 및 SSH를 통한 XML 관리는 지원하지 않습니다.

- (8.4 이상) SSH 기본 사용자 이름은 더 이상 지원하지 않습니다. 이제는 **pix** 또는 **asa** 사용자 이름 및 로그인 비밀번호를 사용하여 SSH를 통해 ASA에 연결할 수 없습니다. SSH를 사용하려면 Configuration > Device Management > Users/AAA > AAA Access > Authentication을 사용하여 AAA 인증을 구성해야 합니다. 그런 다음 Configuration > Device Management > Users/AAA > User Accounts를 사용하여 로컬 사용자를 정의합니다. 로컬 데이터베이스 대신에 AAA 서버를 인증에 사용하려는 경우, 만일에 대비하여 로컬 인증도 구성하는 것이 좋습니다.
- (9.1(2) 이상) 기본 텔넷 로그인 비밀번호가 제거되었습니다. 텔넷을 사용하기 전에 직접 비밀번호를 설정해야 합니다. 14-1 페이지의 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정를 참조하십시오.
- ASA 인터페이스와의 텔넷 또는 SSH 연결이 안 될 경우 36-1 페이지의 ASDM, 텔넷 또는 SSH를 위한 ASA 액세스 구성의 설명에 따라 ASA와의 텔넷 또는 SSH를 활성화했는지 확인하십시오.

관리 액세스 구성

텔넷, SSH 또는 ASDM을 사용하여 ASA에 연결하는 것이 허용된 클라이언트 IP 주소를 지정하려면 다음 단계를 수행합니다.

전제 조건

다중 컨텍스트 모드에서는 컨텍스트 실행 영역에서 이 절차를 완료합니다. 시스템에서 컨텍스트 컨피그레이션으로 바꾸려면 Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 컨텍스트 이름을 두 번 클릭합니다.

절차

1단계 ASDM에서 **Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH**를 선택하고 **Add**를 클릭합니다.

Add Device Access Configuration 대화 상자가 나타납니다.

2단계 나열되는 3가지 옵션, 즉 **ASDM/HTTPS**, **Telnet**, **SSH** 중에서 세션 유형을 선택합니다.

3단계 관리 인터페이스를 선택하고 허용된 호스트 IP 주소를 설정한 다음 **OK**를 클릭합니다.

4단계 **Enable HTTP Server** 확인란이 선택되어야 합니다. 기본적으로 활성화되어 있습니다. 원한다면 다른 HTTP 서버 옵션을 설정합니다.

5단계 (선택 사항) 텔넷 설정을 구성합니다. 시간 초과의 기본값은 5분입니다.

6단계 (선택 사항) SSH 설정을 구성합니다. **DH Key Exchange**에서는 DH(Diffie-Hellman) Key Exchange Group 1 또는 Group 14를 선택하기 위해 해당 라디오 버튼을 클릭합니다. DH 그룹 1 및 그룹 14 키 교환 방식 모두 ASA에서 지원됩니다. 어떤 DH 그룹 키 교환 방식도 지정되지 않은 경우 DH Group 1 키 교환 방식이 사용됩니다. DH 키 교환 방식 사용에 대한 자세한 내용은 RFC 4253을 참조하십시오.

7단계 **Apply**를 클릭합니다.

변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

8단계 (텔넷의 필수 사항) 텔넷으로 연결하려면 먼저 로그인 비밀번호를 설정합니다. 기본 비밀번호가 없습니다.

a. **Configuration > Device Setup > Device Name/Password**를 선택합니다.

b. **Telnet Password** 영역에서 **Change the password to access the console of the security appliance** 확인란을 선택합니다.

c. 이전 비밀번호(신규 ASA의 경우 이 필드를 비워 둠)와 새 비밀번호를 입력하고 확인을 위해 새 비밀번호를 다시 입력합니다.

d. **Apply**를 클릭합니다.

9단계 (SSH의 필수 사항) SSH 사용자 인증을 구성합니다.

a. **Configuration > Device Management > Users/AAA > AAA Access > Authentication**을 선택합니다.

b. **SSH** 확인란을 선택합니다.

c. **Server Group** 드롭다운 목록에서 **LOCAL** 데이터베이스를 선택합니다. 혹은 AAA 서버를 사용하여 인증을 구성할 수도 있습니다.

d. **Apply**를 클릭합니다.

e. 로컬 사용자를 추가합니다. **Configuration > Device Management > Users/AAA > User Accounts**를 클릭하고 **Add**를 클릭합니다.

Add User Account-Identity 대화 상자가 나타납니다.

f. 사용자 이름과 비밀번호를 입력하고 비밀번호 확인을 위해 다시 입력합니다.

g. **OK**를 클릭하고 **Apply**를 클릭합니다.

HTTP 리디렉션 구성

HTTPS는 ASDM을 사용하여 ASA에 연결할 때 사용합니다. 편의를 위해 관리 인터페이스와의 HTTP 연결을 HTTPS로 리디렉션할 수 있습니다. 예를 들어, HTTP를 리디렉션하면 http://10.1.1.4/admin/ 또는 https://10.1.8.4/admin/ 중 어느 것을 입력하더라도 HTTPS 주소의 ASDM 시작 페이지에 연결됩니다.

리디렉션을 활성화하려면 ASDM 액세스를 지원하는 인터페이스별로 다음 절차를 수행합니다.

팁 관리 인터페이스의 액세스 규칙에서는 HTTP 연결과 HTTPS 연결을 모두 허용해야 합니다. 일반적으로 이 프로토콜은 각각 포트 80과 443을 사용합니다.

1단계 **Configuration > Device Management > HTTP Redirect**를 선택합니다.

나타나는 표는 현재 구성된 인터페이스 및 인터페이스에서 리디렉션이 활성화되었는지를 보여줍니다.

2단계 ASDM에 사용하는 인터페이스를 선택하고 **Edit**를 클릭합니다.

3단계 Edit HTTP/HTTPS Settings 대화 상자에서 다음 옵션을 구성합니다.

- Redirect HTTP to HTTPS—HTTP 요청을 HTTPS에 리디렉션할지 여부.
- HTTP Port—인터페이스가 어떤 포트에서 HTTPS 연결을 리디렉션하는지 지정합니다. 기본값은 80입니다.

4단계 OK를 클릭합니다.

텔넷 클라이언트 사용

텔넷을 사용하여 ASA CLI에 액세스하려면 텔넷을 사용하기 전에 직접 비밀번호를 설정해야 합니다. 14-1 페이지의 호스트 이름, 도메인 이름, Enable 및 텔넷 비밀번호 설정를 참조하십시오.

텔넷 인증을 구성하는 경우(36-15 페이지의 CLI 및 , enable 명령 액세스를 위한 인증 구성 참조) AAA 서버 또는 로컬 데이터베이스에 의해 정의된 사용자 이름과 비밀번호를 입력합니다.

SSH 클라이언트 사용

관리 호스트의 SSH 클라이언트에에서 구성했던 사용자 이름과 비밀번호를 입력합니다. SSH 세션을 시작하면 ASA 콘솔에 점(.)이 표시되고 다음 SSH 사용자 인증 프롬프트가 나타납니다.

```
ciscoasa(config)#.
```

점이 표시되더라도 SSH의 기능에 영향을 주지 않습니다. 점은 서버 키를 생성할 때 또는 사용자 인증에 앞서 SSH 키 교환 과정에서 개인 키를 사용하여 메시지를 해독할 때 콘솔에 나타납니다. 이 작업은 최대 2분 이상 걸릴 수 있습니다. 점은 ASA가 작업 중이고 멈춘 상태가 아님을 알리는 일종의 진행 표시입니다.

비밀번호를 사용하지 않고 그 대신 공개 키를 구성할 수도 있습니다. 28-3 페이지의 로컬 데이터베이스에 사용자 어카운트 추가를 참조하십시오.

CLI 매개 변수 구성

CLI 매개 변수를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

로그인 배너 구성

사용자가 ASA에 연결할 때 사용자 로그인 전에 또는 사용자가 특별 권한 EXEC 모드를 시작하기 전에 표시할 메시지를 구성할 수 있습니다.

제한 사항

배너가 추가된 다음 ASA와의 텔넷 또는 SSH 세션이 종료될 때가 있습니다.

- 배너 메시지를 처리하기에는 시스템 메모리가 충분하지 않을 경우
- 배너 메시지를 표시하려 할 때 TCP 쓰기 오류가 발생한 경우

지침

- 보안의 관점에서는 배너에서 무단 액세스를 방지하는 것이 중요합니다. “welcome” 또는 “please”와 같은 문구는 침입자를 불러들이는 것 같으므로 사용하지 마십시오. 다음과 같은 배너로 무단 액세스에 대해 적절한 어조를 유지할 수 있습니다.

  ```
  You have logged in to a secure device. If you are not authorized to access this
  device, log out immediately or risk possible criminal consequences.
  ```

- 배너 메시지에 대한 자세한 내용은 RFC 2196을 참조하십시오.

로그인 배너를 구성하려면 다음 단계를 수행합니다.

세부 단계

1단계 **Configuration > Device Management > Management Access > Command Line (CLI) > Banner**를 선택하고 CLI를 위해 만드는 배너 유형의 필드에 배너 텍스트를 추가합니다.

- 사용자가 CLI에서 특별 권한 EXEC 모드에 액세스할 때 세션 (exec) 배너가 나타납니다.
- 사용자가 CLI에 로그인할 때 로그인 배너가 나타납니다.
- 사용자가 처음으로 CLI에 연결할 때 message-of-the-day(motd) 배너가 나타납니다.
- 사용자 인증 후 사용자가 ASDM에 연결할 때 ASDM 배너가 나타납니다. 사용자는 2가지 옵션으로 배너를 닫을 수 있습니다.
  - Continue—배너를 닫고 로그인을 완료합니다.
  - Disconnect—배너를 닫고 연결을 종료합니다.
- ASCII 문자만 허용됩니다. 새 라인(Enter)도 가능하며, 2개의 문자로 간주됩니다.
- 탭은 CLI 버전에서 유지되지 않으므로 배너에 사용하지 마십시오.
- RAM 및 플래시 메모리에 대한 제한을 제외하면 배너의 길이 제한은 없습니다.
- 문자열 **$(hostname)**과 **$(domain)**을 넣어 ASA의 호스트 이름 또는 도메인 이름을 동적으로 추가할 수 있습니다.
- 시스템 컨피그레이션에서 배너를 컨피그레이션한 경우, 컨텍스트 컨피그레이션에서 **$(system)** 문자열을 사용하여 컨텍스트 내에 배너 텍스트를 사용할 수 있습니다.

2단계 **Apply**를 클릭합니다.

새 배너가 실행 중인 컨피그레이션에 저장됩니다.

CLI 프롬프트 사용자 지정

CLI 프롬프트 창에서는 CLI 세션에 사용되는 프롬프트를 사용자 지정할 수 있습니다. 기본적으로 프롬프트는 ASA의 호스트 이름을 표시합니다. 다중 컨텍스트 모드에서는 프롬프트가 컨텍스트 이름도 표시합니다. CLI 프롬프트에서 다음 항목을 표시할 수 있습니다.

cluster-unit	(단일 모드 및 다중 모드) 클러스터 유닛 이름을 표시합니다. 클러스터의 각 유닛은 고유한 이름을 가질 수 있습니다.
context	(다중 모드만) 현재 컨텍스트의 이름을 표시합니다.
domain	도메인 이름을 표시합니다.
hostname	호스트 이름을 표시합니다.
priority	장애 조치 우선순위를 pri(1차) 또는 sec(2차)로 표시합니다.
state	유닛의 트래픽 전달 상태를 표시합니다. 상태에 대해 표시되는 값은 다음과 같습니다. • act—장애 조치가 활성화되었으며, 해당 유닛은 능동적으로 트래픽을 전달하고 있습니다. • stby—장애 조치가 활성화되었으며, 해당 유닛은 트래픽을 전달하는 중이 아니고 대기, 실패 또는 그 밖의 비활성 상태에 있습니다. • actNoFailover—장애 조치가 활성화되지 않았으며, 해당 유닛은 능동적으로 트래픽을 전달하고 있습니다. • stbyNoFailover—장애 조치가 활성화되지 않았고, 해당 유닛은 트래픽을 전달하는 중이 아닙니다. 대기 유닛의 임계값을 초과하는 인터페이스 오류가 있을 경우 이러한 조건이 발생할 수 있습니다. 클러스터에서 유닛의 역할(마스터 또는 슬레이브)을 표시합니다. 예를 들어, 프롬프트 ciscoasa/cl2/slave에서 호스트 이름은 ciscoasa, 유닛 이름은 cl2, 상태 이름은 slave입니다.

세부 단계

CLI 프롬프트를 사용자 지정하려면 다음 단계를 수행합니다.

1단계 **Configuration > Device Management > Management Access > Command Line (CLI) > CLI Prompt**를 선택하고 다음 중 하나를 수행하여 프롬프트를 사용자 지정합니다.

- 프롬프트에 특성을 추가하려면 Available Prompts 목록에서 특성을 클릭하고 **Add**를 클릭합니다. 프롬프트에 여러 특성을 추가할 수 있습니다. 특성이 Available Prompts 목록에서 Selected Prompts 목록으로 이동합니다.
- 프롬프트에서 특성을 제거하려면 Selected Prompts 목록에서 특성을 클릭하고 **Delete**를 클릭합니다. 특성이 Selected Prompts 목록에서 Available Prompts 목록으로 이동합니다.
- 명령 프롬프트에서 특성이 나타나는 순서를 변경하려면 Selected Prompts 목록에서 특성을 클릭하고 **Move Up** 또는 **Move Down**을 클릭하여 순서를 변경합니다.

프롬프트가 변경되어 CLI Prompt Preview 필드에 표시됩니다.

2단계 **Apply**를 클릭합니다.

새 프롬프트가 실행 중인 컨피그레이션에 저장됩니다.

콘솔 시간 초과 변경

콘솔 시간 초과는 어떤 연결에서 특별 권한 EXEC 모드 또는 컨피그레이션 모드가 얼마나 오래 유지될 수 있는가를 설정합니다. 시간 초과에 도달하면 세션은 사용자 EXEC 모드로 전환됩니다. 기본적으로 세션은 시간 초과가 없습니다. 이 설정은 사용자가 얼마나 오랫동안 콘솔 포트와의 연결 상태를 유지할 수 있는가에 영향을 주지 않습니다. 이 연결 상태는 시간 초과가 없습니다.

콘솔 시간 초과를 변경하려면 다음 단계를 수행합니다.

세부 단계

1단계 새 시간 초과 값(분)을 정의하려면 **Configuration > Device Management > Management Access > Command Line (CLI) > Console Timeout**을 선택합니다.

2단계 시간을 무한으로 지정하려면 **0**을 입력합니다. 기본값은 0입니다.

3단계 **Apply**를 클릭합니다.

시간 초과 값이 변경되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

VPN 터널을 통한 관리 액세스 구성

VPN 터널이 어떤 인터페이스에서 종료했지만 다른 인터페이스에 액세스하여 ASA를 관리하려는 경우, 그 인터페이스를 관리 액세스 인터페이스로 지정할 수 있습니다. 예를 들어, 외부 인터페이스에서 ASA에 들어올 경우 이 기능은 ASDM, SSH, Telnet 또는 SNMP를 사용하여 내부 인터페이스에 연결할 수 있게 합니다. 또는 외부 인터페이스에서 들어올 때 내부 인터페이스를 ping할 수 있습니다. 관리 액세스는 IPsec 클라이언트, IPsec 사이트 대 사이트(site-to-site), AnyConnect SSL VPN 클라이언트의 VPN 터널 유형을 통해 사용할 수 있습니다.

- 36-8 페이지의 관리 인터페이스를 위한 라이센싱 요구 사항
- 36-2 페이지의 지침 및 제한 사항
- 36-9 페이지의 관리 인터페이스 구성

관리 인터페이스를 위한 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 모드에서 지원합니다.

방화벽 모드 지침
라우티드 모드에서 지원합니다.

IPv6 지침
IPv6를 지원합니다.

추가 지침
관리 액세스 인터페이스를 하나만 정의할 수 있습니다.

참고 후속 컨피그레이션에서는 192.168.10.0/24가 AnyConnect 또는 IPsec VPN 클라이언트를 위한 VPN 풀입니다. 각 컨피그레이션에서는 VPN 클라이언트 사용자가 관리 인터페이스 IP 주소를 사용하여 ASDM에 연결하거나 ASA에 SSH 연결하는 것을 허용합니다.

VPN 클라이언트 사용자만 ASDM 또는 HTTP에 액세스하게 하려면(다른 모든 사용자의 액세스 거부) 다음 명령을 입력합니다.

```
ciscoasa(config)# http server enable
ciscoasa(config)# http 192.168.10.0 255.255.255.0 management_interface
```

VPN 클라이언트 사용자만 SSH를 사용하여 ASA에 액세스하게 하려면(다른 모든 사용자의 액세스 거부) 다음 명령을 입력합니다.

```
ciscoasa(config)# ssh 192.168.10.0 255.255.255.0 management_interface
```

관리 인터페이스 구성

관리 인터페이스를 구성하려면 다음 단계를 수행합니다.

세부 단계

1단계 Configuration > Device Management > Management Access > Management Interface 창의 Management Access Interface 드롭다운 목록에서 최고 보안 레벨의 인터페이스(내부 인터페이스)를 선택합니다.

2단계 **Apply**를 클릭합니다.

관리 인터페이스가 지정되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

시스템 관리자를 위한 AAA 구성

이 섹션에서는 시스템 관리자를 위해 인증 및 명령 권한 부여를 활성화하는 방법을 설명합니다.

시스템 관리자를 위한 AAA에 대한 정보

이 섹션에서는 시스템 관리자를 위해 AAA에 대해 설명합니다.

관리 인증에 대한 정보

이 섹션에서는 관리 액세스를 위한 인증에 대해 설명합니다.

인증 있는 CLI 액세스와 인증 없는 CLI 액세스 비교

ASA에 로그인하는 방법은 인증을 활성화했는지에 따라 달라집니다.

- 인증 없음—텔넷에 대해 어떤 인증도 활성화하지 않을 경우 사용자 이름을 입력하지 않습니다. 로그인 비밀번호를 입력합니다. SSH는 인증 없이 사용 불가합니다. 사용자 EXEC 모드에 액세스합니다.
- 인증—이 섹션에 따라 텔넷 또는 SSH 인증을 활성화한 경우 AAA 서버 또는 로컬 사용자 데이터베이스에 정의된 사용자 이름과 비밀번호를 입력합니다. 사용자 EXEC 모드에 액세스합니다.

로그인한 다음 특별 권한 EXEC 모드를 시작하려면 **enable** 명령을 입력합니다. **enable**의 작동 방식은 인증을 활성화했는지에 따라 달라집니다.

- 인증 없음—enable 인증을 구성하지 않은 경우, **enable** 명령을 입력할 때 시스템 enable 비밀번호를 입력합니다. 그러나 enable 인증을 사용하지 않을 경우, **enable** 명령을 입력한 다음에는 더 이상 특정 사용자로 로그인한 상태가 아닙니다. 사용자 이름을 유지하려면 enable 인증을 사용합니다.
- 인증—enable 인증을 구성한 경우, ASA에서는 사용자 이름과 비밀번호를 다시 묻습니다. 사용자가 입력 가능한 명령을 확인하는 데 사용자 이름이 중요한 역할을 하는 명령 권한 부여에서 이 기능은 매우 유용합니다.

로컬 데이터베이스를 사용하는 enable 인증에서는 **login** 명령을 **enable** 명령 대신 사용할 수 있습니다. **login**은 사용자 이름을 유지하지만, 인증을 실행하는 데 어떤 컨피그레이션도 필요하지 않습니다.

인증 있는 ASDM 액세스와 인증 없는 CLI 액세스 비교

기본적으로 빈 사용자 이름과을 통해 설정된 enable 비밀번호를 사용하여 ASDM에 로그인할 수 있습니다. 로그인 화면에서 (사용자 이름을 비워 두지 않고) 사용자 이름과 비밀번호를 입력한 경우 ASDM은 로컬 데이터베이스에 일치하는 항목이 있는지 확인합니다.

HTTP 인증을 구성하면 더 이상 빈 사용자 이름과 enable 비밀번호로 ASDM을 사용할 수 없게 됩니다.

스위치에서 ASA Services Module로의 세션 인증

스위치에서 ASASM에 연결하는 세션(**session** 명령 사용)을 위해 텔넷 인증을 구성할 수 있습니다. 스위치에서 ASASM로의 가상 콘솔 연결(**service-module session** 명령 사용)에는 시리얼 포트 인증을 구성할 수 있습니다.

다중 컨텍스트 모드에서는 시스템 컨피그레이션에서 어떤 AAA 명령도 컨피그레이션할 수 없습니다. 그러나 관리 컨텍스트에서 텔넷 또는 시리얼 인증을 구성한 경우, 스위치에서 ASASM로의 세션에도 인증이 적용됩니다. 이 경우에는 관리 컨텍스트 AAA 서버 또는 로컬 사용자 데이터베이스가 사용됩니다.

명령 권한 부여에 대한 정보

이 섹션에서는 명령 권한 부여에 대해 설명합니다.

- 36-11 페이지의 지원되는 명령 권한 부여 방식
- 36-12 페이지의 사용자 자격 증명 유지에 대한 정보
- 36-12 페이지의 보안 컨텍스트 및 명령 권한 부여

지원되는 명령 권한 부여 방식

다음 2가지 명령 권한 부여 방식 중 하나를 사용할 수 있습니다.

- 로컬 권한 레벨—ASA에서 명령 권한 레벨을 구성합니다. 로컬, RADIUS 또는 LDAP(LDAP 특성을 RADIUS 특성에 매핑한 경우) 사용자가 CLI 액세스를 위해 인증할 경우, ASA에서는 로컬 데이터베이스, RADIUS 또는 LDAP 서버에 의해 정의된 권한 레벨을 사용자에게 부여합니다. 사용자는 부여받은 권한 레벨 이하의 명령에 액세스할 수 있습니다. 모든 사용자가 처음 로그인할 때는 사용자 EXEC 모드에 액세스합니다(레벨 0 또는 1의 명령). 사용자는 **enable** 명령을 사용하여 다시 인증해야 특별 권한 EXEC 모드(레벨 2 이상의 명령)에 액세스할 수 있습니다. 또는 **login** 명령을 사용하여 로그인할 수 있습니다(로컬 데이터베이스만).

참고 로컬 데이터베이스에 어떤 사용자도 없는 상태에서, CLI 또는 **enable** 인증 없이 로컬 명령 권한 부여를 사용할 수 있습니다. 그 대신 **enable** 명령을 입력할 때는 시스템 enable 비밀번호를 입력합니다. 그러면 ASA에서는 레벨 15를 부여합니다. 그러면 각 레벨의 enable 비밀번호를 만들 수 있습니다. 즉 **enable** *n*(2~15)을 입력하면 ASA에서는 레벨 *n*을 부여합니다. 이러한 레벨은 로컬 명령 권한 부여를 활성화한 경우에만 사용됩니다(36-21 페이지의 로컬 명령 권한 부여 구성 참조). 명령 참조에서 **enable** 명령에 대해 자세히 알아볼 수 있습니다.

- TACACS+ 서버 권한 레벨—TACACS+ 서버에서 사용자 또는 그룹이 CLI 액세스를 위한 인증 이후에 사용할 수 있는 명령을 구성합니다. 사용자가 CLI에서 입력하는 모든 명령에 대해 TACACS+ 서버를 사용한 유효성 검사가 실시됩니다.

사용자 자격 증명 유지에 대한 정보

사용자가 ASA에 로그인할 때 사용자는 인증을 위한 사용자 이름과 비밀번호를 제공해야 합니다. ASA에서는 세션에서 나중에 추가적인 인증이 필요할 경우에 대비하여 이 세션 자격 증명을 보존합니다.

다음 컨피그레이션이 있으면 사용자는 로컬 서버와의 인증만으로 로그인할 수 있습니다. 이후의 시리얼 권한 부여에서는 저장된 자격 증명을 사용합니다. 또한 사용자는 권한 레벨 15의 비밀번호를 입력해야 합니다. 특별 권한 모드를 종료할 때 사용자가 다시 인증됩니다. 특별 권한 모드에서는 사용자 자격 증명이 보존되지 않습니다.

- 로컬 서버가 사용자 액세스를 인증하도록 구성되었습니다.
- 권한 레벨 15 명령 액세스가 비밀번호가 필요하도록 구성되었습니다.
- 사용자 어카운트에서 (콘솔 또는 ASDM에 대한 액세스 없이) 시리얼 전용 권한 부여가 구성되었습니다.
- 사용자 어카운트에서 권한 레벨 15 명령 액세스가 구성되었습니다.

다음 표는 이러한 경우에 ASA에서 어떻게 자격 증명을 사용하는지 보여줍니다.

필요한 자격 증명	사용자 이름 및 비밀번호 인증	시리얼 권한 부여	특별 권한 모드의 명령 권한 부여	특별 권한 모드의 종료 권한 부여
사용자 이름	예	아니요	아니요	예
비밀번호	예	아니요	아니요	예
특별 권한 모드 비밀번호	아니요	아니요	예	아니요

보안 컨텍스트 및 명령 권한 부여

다음은 다중 보안 컨텍스트로 명령 권한 부여를 구현할 때 중요하게 고려할 사항입니다.

- AAA 설정은 컨텍스트끼리 공유하지 않고 컨텍스트마다 다릅니다.

  명령 권한 부여를 구성할 때 각 보안 컨텍스트를 따로 구성해야 합니다. 이러한 컨피그레이션에서는 여러 보안 컨텍스트에서 각기 다른 명령 권한 부여를 적용하는 것이 가능합니다.

  보안 컨텍스트 간 전환에서 관리자는 로그인 시 지정된 사용자 이름에 대해 허용된 명령이 새 컨텍스트 세션에서는 다를 수 있음을 또는 새 컨텍스트에서는 명령 권한 부여가 아예 구성되지 않았을 수도 있음을 알고 있어야 합니다. 명령 권한 부여가 보안 컨텍스트마다 다를 수 있음을 모르는 관리자는 혼란스러워 할 수도 있습니다. 이는 다음 사항 때문에 더욱 복잡해집니다.

- **changeto** 명령으로 시작한 새 컨텍스트 세션은 항상 기본 enable_15 사용자 이름을 관리자 ID로 사용합니다. 이전 컨텍스트 세션에서 어떤 사용자 이름을 사용했는가는 상관없습니다. 따라서 enable_15 사용자에 대해 명령 권한 부여가 구성되지 않은 경우 또는 enable_15 사용자에 대한 권한 부여가 이전 컨텍스트 세션 사용자에 대한 권한 부여와 다를 경우 혼란이 일어날 수 있습니다.

  이러한 동작은 명령 어카운팅에도 영향을 줍니다. 명령 어카운팅은 실행된 각 명령을 특정 관리자와 정확하게 연결할 수 있는 경우에만 유용합니다. **changeto** 명령을 사용할 권한이 있는 모든 관리자는 다른 컨텍스트에서 enable_15 사용자 이름을 사용할 수 있으므로 명령 어카운팅 레코드에서 누가 enable_15 사용자 이름으로 로그인했는지 즉시 식별하기 어렵습니다. 컨텍스트마다 다른 어카운팅 서버를 사용하는 경우, 누가 enable_15 사용자 이름을 사용하고 있었는지 추적하려면 여러 서버의 데이터를 연계하여 파악해야 합니다.

명령 권한 부여를 구성할 때 다음 사항을 고려하십시오.

- **changeto** 명령을 사용할 권한이 있는 관리자는 enable_15 사용자에게 허용된 모든 명령을 사실상 다른 모든 컨텍스트에서 사용할 수 있습니다.
- 명령 권한 부여를 컨텍스트마다 다르게 하려는 경우, 각 컨텍스트에서 enable_15 사용자 이름에게 허용되지 않은 명령은 **changeto** 명령 사용 권한을 가진 관리자에게도 거부되어야 합니다.

다른 보안 컨텍스트로 전환할 때 관리자는 특별 권한 EXEC 모드를 종료하고 **enable** 명령을 다시 입력하여 필요한 사용자 이름을 사용할 수 있습니다.

참고 시스템 실행 영역에서는 AAA 명령을 지원하지 않습니다. 따라서 시스템 실행 영역에서는 명령 권한 부여를 사용할 수 없습니다.

시스템 관리자를 위한 AAA의 라이센싱 요구 사항

모델	라이센싱 요구 사항
ASAv	표준(Standard) 또는 프리미엄(Premium) 라이센스
기타 모델	Base 라이센스

전제 조건

AAA 서버 또는 로컬 데이터베이스의 전제 조건

AAA 서버 또는 로컬 데이터베이스에서 사용자를 구성해야 합니다. AAA 서버의 경우 ASA에서 이 서버와 통신하도록 구성하는 작업도 필요합니다. 다음 장을 참조하십시오.

- AAA 서버—해당 AAA 서버 유형에 대한 장을 참조하십시오.
- 로컬 데이터베이스—28-3 페이지의 로컬 데이터베이스에 사용자 어카운트 추가를 참조하십시오.

관리 인증의 전제 조건

ASA에서 텔넷, SSH 또는 HTTP 사용자를 인증하려면 먼저 ASA와의 통신이 허용되는 IP 주소를 확인해야 합니다. ASASM의 경우, 다중 컨텍스트 모드의 시스템 액세스는 예외입니다. 스위치에서 ASASM에 연결하는 세션은 텔넷 세션이지만, 텔넷 액세스 컨피그레이션은 필요하지 않습니다. 자세한 내용은 36-1 페이지의 ASDM, 텔넷 또는 SSH를 위한 ASA 액세스 구성를 참조하십시오.

로컬 명령 권한 부여의 전제 조건

- **enable** 인증을 구성합니다. 36-15 페이지의 CLI 및 , enable 명령 액세스를 위한 인증 구성를 참조하십시오.

  enable 인증은 사용자가 **enable** 명령에 액세스한 다음 사용자 이름을 유지하려면 필요합니다.

  또는 컨피그레이션이 필요 없는 **login** 명령을 사용할 수도 있습니다. 이는 인증과 관련해서는 **enable** 명령과 동일한 기능을 하지만, 로컬 데이터베이스에서만 가능합니다. 이 옵션은 **enable** 인증만큼 안전하지 않으므로 이 옵션은 권장하지 않습니다.

  CLI 인증을 사용할 수도 있지만, 필수는 아닙니다.

- 사용자 유형별로 다음 전제 조건을 확인하십시오.
  - 로컬 데이터베이스 사용자—0~15의 권한 레벨로 로컬 데이터베이스의 각 사용자를 구성합니다.
  - RADIUS 사용자—값이 0~15인 Cisco VSA CVPN3000-Privilege-Level로 사용자를 구성합니다.
  - LDAP 사용자—0~15의 권한 레벨로 사용자를 구성한 다음31-5 페이지의 LDAP 특성 맵 구성에 따라 LDAP 특성을 Cisco VSA CVPN3000-Privilege-Level에 매핑합니다.

TACACS+ 명령 권한 부여의 전제 조건

- CLI 및 **enable** 인증을 구성합니다(36-15 페이지의 CLI 및 , enable 명령 액세스를 위한 인증 구성 참조).

관리 어카운팅의 전제 조건

- CLI 및 **enable** 인증을 구성합니다(36-15 페이지의 CLI 및 , enable 명령 액세스를 위한 인증 구성 참조).

지침 및 제한 사항

이 섹션에서는 이 기능에 대한 지침과 제한 사항을 소개합니다.

컨텍스트 모드 지침

단일 및 다중 컨텍스트 모드에서 지원

방화벽 모드 지침

라우티드 및 투명 방화벽 모드에서 지원

IPv6 지침

IPv6를 지원합니다.

기본 설정

기본 명령 권한 레벨

기본적으로 다음 명령이 권한 레벨 0에 지정됩니다. 다른 모든 명령은 권한 레벨 15에 지정됩니다.

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**

- **show pager**
- **clear pager**
- **quit**
- **show version**

어떤 컨피그레이션 모드 명령을 15보다 낮은 레벨로 이동한 경우, 그 **configure** 명령도 그 레벨로 이동해야 합니다. 그러지 않으면 사용자가 컨피그레이션 모드를 시작할 수 없게 됩니다.

모든 권한 레벨을 보려면 36-22 페이지의 로컬 명령 권한 레벨 보기를 참조하십시오.

CLI 및 , enable 명령 액세스를 위한 인증 구성

CLI, ASDM, enable 명령 액세스를 위한 인증이 필요할 수 있습니다.

전제 조건

- 36-1 페이지의 ASDM, 텔넷 또는 SSH를 위한 ASA 액세스 구성에 따라 텔넷, SSH 또는 HTTP 액세스를 구성합니다.
- SSH 액세스의 경우 SSH 인증을 구성해야 합니다. 기본 사용자 이름이 없습니다.

세부 단계

1단계 **enable** 명령을 사용하는 사용자를 인증하려면 **Configuration > Device Management > Users/AAA > AAA Access > Authentication**을 선택하고 다음 설정을 구성합니다.

a. **Enable** 확인란을 선택합니다.

b. Server Group 드롭다운 목록에서 서버 그룹 이름 또는 LOCAL 데이터베이스를 선택합니다.

c. (선택 사항) AAA를 선택한 경우, AAA 서버를 사용할 수 없을 때 로컬 데이터베이스를 대신 사용하도록 ASA를 구성할 수 있습니다. **Use LOCAL when server group fails** 확인란을 클릭합니다. 로컬 데이터베이스에서 AAA 서버와 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다. ASA 프롬프트에서는 어떤 방법을 사용 중인지 알려주지 않기 때문입니다.

2단계 CLI 또는 ASDM에 액세스하는 사용자를 인증하려면 **Configuration > Device Management > Users/AAA > AAA Access > Authentication**을 선택하고 다음 설정을 구성합니다.

a. 다음 확인란을 하나 이상 선택합니다.

- **HTTP/ASDM**—HTTPS를 사용하여 ASA에 액세스하는 ASDM 클라이언트를 인증합니다. HTTP 관리 인증에서는 AAA 서버 그룹에 대해 SDI 프로토콜을 지원하지 않습니다.
- **Serial**—콘솔 포트를 사용하여 ASA에 액세스하는 사용자를 인증합니다. ASASM에서는 이 매개 변수가 **service-module session** 명령을 사용하여 스위치로부터 액세스하는 가상 콘솔에 영향을 줍니다. 다중 모드 액세스는 36-11 페이지의 스위치에서 ASA Services Module로의 세션 인증를 참조하십시오.
- **SSH**—SSH를 사용하여 ASA에 액세스하는 사용자를 인증합니다.
- **Telnet**—텔넷을 사용하여 ASA에 액세스하는 사용자를 인증합니다. ASASM에서는 이 매개 변수가 **session** 명령을 사용하는 스위치로부터의 세션에도 영향을 줍니다. 다중 모드 액세스는 36-11 페이지의 스위치에서 ASA Services Module로의 세션 인증를 참조하십시오.

b. 선택한 서비스 각각에 대해 Server Group 드롭다운 목록에서 서버 그룹 이름 또는 LOCAL 데이터베이스를 선택합니다.

c. (선택 사항) AAA를 선택한 경우, AAA 서버를 사용할 수 없을 때 로컬 데이터베이스를 대신 사용하도록 ASA를 구성할 수 있습니다. **Use LOCAL when server group fails** 확인란을 클릭합니다. 로컬 데이터베이스에서 AAA 서버와 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다. ASA 프롬프트에서는 어떤 방법을 사용 중인지 알려주지 않기 때문입니다.

3단계 **Apply**를 클릭합니다.

관리 권한 부여로 사용자 CLI 및 ASDM 액세스 제한

ASA에서는 사용자가 RADIUS, LDAP, TACACS+ 또는 로컬 사용자 데이터베이스를 사용하여 인증할 때 관리 사용자와 원격 액세스 사용자를 구분할 수 있습니다. 사용자 역할 차별화를 통해 원격 액세스 VPN 및 네트워크 액세스 사용자가 ASA와의 관리 연결을 설정하는 것을 방지할 수 있습니다.

참고 시리얼 액세스는 관리 권한 부여에 포함되지 않습니다. 따라서 Authentication > Serial 옵션을 활성화한 경우 인증하는 모든 사용자가 콘솔 포트에 액세스할 수 있습니다.

세부 단계

1단계 다음 옵션 중 하나를 선택합니다.

- 관리 권한 부여를 활성화하려면 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**을 선택하고 **Perform authorization for exec shell access > Enable** 확인란을 선택합니다.

  LOCAL 옵션이 구성되었으면, 로컬 사용자 데이터베이스가 입력된 사용자 이름, 지정된 Service-Type 및 Privilege-Level 특성의 소스가 됩니다.

  이 옵션을 선택하면 RADIUS의 관리 사용자 권한 레벨도 지원할 수 있는데, 이는 로컬 명령 레벨과 함께 명령 권한 부여에 사용할 수 있습니다. 자세한 내용은 36-21 페이지의 로컬 명령 권한 부여 구성를 참조하십시오.

  authentication-server 옵션이 구성된 경우, 동일한 서버가 인증과 권한 부여에 사용됩니다.

- 관리 권한 부여를 활성화하려면 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**을 선택하고 **Allow privileged users to enter into EXEC mode on login** 확인란을 선택합니다.

  auto-enable 옵션은 로그인 인증 서버에서 충분한 권한을 가진 사용자가 곧바로 특별 권한 EXEC 모드에 들어가는 것을 허용합니다. 그렇지 않은 사용자는 사용자 EXEC 모드가 됩니다. 이러한 권한은 각 EXEC 모드에 들어가는 데 필요한 Service-Type 및 Privilege-Level 특성에 의해 결정됩니다. 특별 권한 EXEC 모드를 시작하려면 사용자에게 지정된 Service-Type 특성이 Administrative이고 Privilege Level 특성이 1보다 커야 합니다.

  이 옵션은 시스템 컨텍스트에서는 지원되지 않습니다. 그러나 관리 컨텍스트에서 텔넷 또는 시리얼 인증을 구성한 경우, 스위치에서 ASASM로의 세션에도 인증이 적용됩니다.

  aaa authorization exec 명령만 입력하면 아무런 효과가 없습니다.

  관리 권한 부여에 시리얼 인증을 사용할 때는 **auto-enable** 옵션이 포함되지 않습니다.

  aaa authentication http 명령은 **auto-enable** 옵션의 영향을 받지 않습니다.

auto-enable 옵션을 구성하기 전에 두 프로토콜 로그인을 구성하고 인증을 활성화하는 것이 좋습니다. 그리고 다음 예와 같이 모든 인증 요청이 동일한 AAA 서버 그룹으로 전달되는 것이 좋습니다.

```
ciscoasa (config)# aaa authentication ssh console RADIUS
ciscoasa (config)# aaa authentication enable console RADIUS
ciscoasa (config)# aaa authorization exec authentication-server auto-enable
```

다른 유형의 컨피그레이션을 사용하는 것은 권장되지 *않습니다*.

2단계 관리 권한 부여를 위해 사용자를 구성하려면 각 AAA 서버 유형 또는 로컬 사용자에 대한 다음 요구 사항을 확인하십시오.

RADIUS 또는 LDAP(매핑됨) 사용자

사용자가 LDAP을 통해 인증되면 기본 LDAP 특성과 그 값이 Cisco ASA 특성에 매핑되어 특정 권한 부여 기능을 제공할 수 있습니다. Cisco VSA CVPN3000-Privilege-Level을 0~15의 값으로 구성합니다. 그리고을 사용하여 LDAP 특성을 Cisco VAS CVPN3000-Privilege-Level에 매핑합니다. 자세한 내용은 31-5 페이지의 LDAP 특성 맵 구성를 참조하십시오.

RADIUS IETF **service-type** 특성은, RADIUS 인증 및 권한 부여 요청의 결과인 access-accept 메시지를 통해 전송될 때, 어떤 서비스 유형이 인증된 사용자에게 허가될지 지정하는 데 쓰입니다.

- Service-Type 6 (Administrative)— Authentication 탭 옵션에 의해 지정되는 임의의 서비스에 대한 전체 액세스를 허용합니다.
- Service-Type 7 (NAS prompt)— 텔넷 또는 SSH 인증 옵션을 컨피그레이션할 때 CLI에 대한 액세스를 허용합니다. 그러나 HTTP 옵션을 컨피그레이션한 경우에는 ASDM 컨피그레이션 액세스를 거부합니다. ASDM 모니터링 액세스는 허용됩니다. **enable** 인증을 구성하는 데 Enable 옵션을 사용한 경우, 사용자는 **enable** 명령을 사용하여 특별 권한 EXEC 모드에 액세스할 수 없습니다. Framed (2) 서비스 유형과 Login (1) 서비스 유형은 동일하게 처리됩니다.
- Service-Type 5 (Outbound)—관리 액세스를 거부합니다. 사용자는 Authentication 탭 옵션에 의해 지정되는 임의의 서비스를 사용할 수 없습니다(Serial 옵션 제외, 시리얼 액세스는 허용됨). 원격 액세스(IPsec 및 SSL) 사용자는 여전히 원격 액세스 세션을 인증하고 종료할 수 있습니다. 그 밖의 모든 서비스 유형(Voice, FAX 등)은 동일하게 처리됩니다.

RADIUS Cisco VSA **privilege-level** 특성(Vendor ID 3076, sub-ID 220)은, access-accept 메시지를 통해 전송될 때, 사용자의 권한 레벨을 지정하는 데 쓰입니다.

인증된 사용자가 ASDM, SSH 또는 텔넷을 통해 ASA에 대한 관리 액세스를 시도하지만 그에 적합한 권한 레벨이 아닐 경우, ASA에서는 syslog 메시지 113021을 생성합니다. 이 메시지는 부적합한 관리 권한 때문에 로그인 시도가 실패했음을 사용자에게 알립니다.

TACACS+ 사용자

"service=shell"로 권한 부여가 요청되고, 서버는 PASS 또는 FAIL로 응답합니다.

- PASS, 권한 레벨 1— Authentication 탭 옵션에서 지정한 임의의 서비스에 대한 전체 액세스를 허용합니다.
- PASS, 권한 레벨 2 이상— 텔넷 또는 SSH 인증 옵션을 컨피그레이션할 때 CLI에 대한 액세스를 허용합니다. 그러나 HTTP 옵션을 컨피그레이션한 경우에는 ASDM 컨피그레이션 액세스를 거부합니다. ASDM 모니터링 액세스는 허용됩니다. **enable** 인증을 구성하는 데 Enable 옵션을 사용한 경우, 사용자는 **enable** 명령을 사용하여 특별 권한 EXEC 모드에 액세스할 수 없습니다. enable 권한 레벨이 14 이하로 설정된 경우 **enable** 명령을 사용하여 특별 권한 EXEC 명령에 액세스할 수 없습니다.
- FAIL—관리 액세스를 거부합니다. 사용자는 Authentication 탭 옵션에 의해 지정되는 임의의 서비스를 사용할 수 없습니다(Serial 옵션 제외, 시리얼 액세스는 허용됨).

로컬 사용자

어떤 사용자 이름에 대한 Access Restriction 옵션을 구성합니다. 액세스 제한은 기본적으로 Full Access입니다. 그러면 Authentication 탭 옵션에 의해 지정된 임의의 서비스에 대한 전체 액세스를 허용합니다. 자세한 내용은 28-3 페이지의 로컬 데이터베이스에 사용자 어카운트 추가를 참조하십시오.

로컬 데이터베이스 사용자를 위한 비밀번호 정책 구성

로컬 데이터베이스를 사용하여 CLI 또는 ASDM 액세스를 위한 인증을 구성할 때, 일정한 시간이 지나면 사용자가 비밀번호를 변경해야 하고 최소 길이, 변경된 문자의 최소 개수와 같은 비밀번호 기준의 준수를 요구하는 비밀번호 정책을 구성할 수 있습니다.

비밀번호 정책은 로컬 데이터베이스를 사용하는 관리 사용자에게만 적용됩니다. 로컬 데이터베이스를 사용할 수 있는 기타 트래픽 유형(예: 네트워크 액세스를 위한 VPN 또는 AAA) 및 AAA 서버에서 인증한 사용자에게는 적용되지 않습니다.

비밀번호 정책 구성

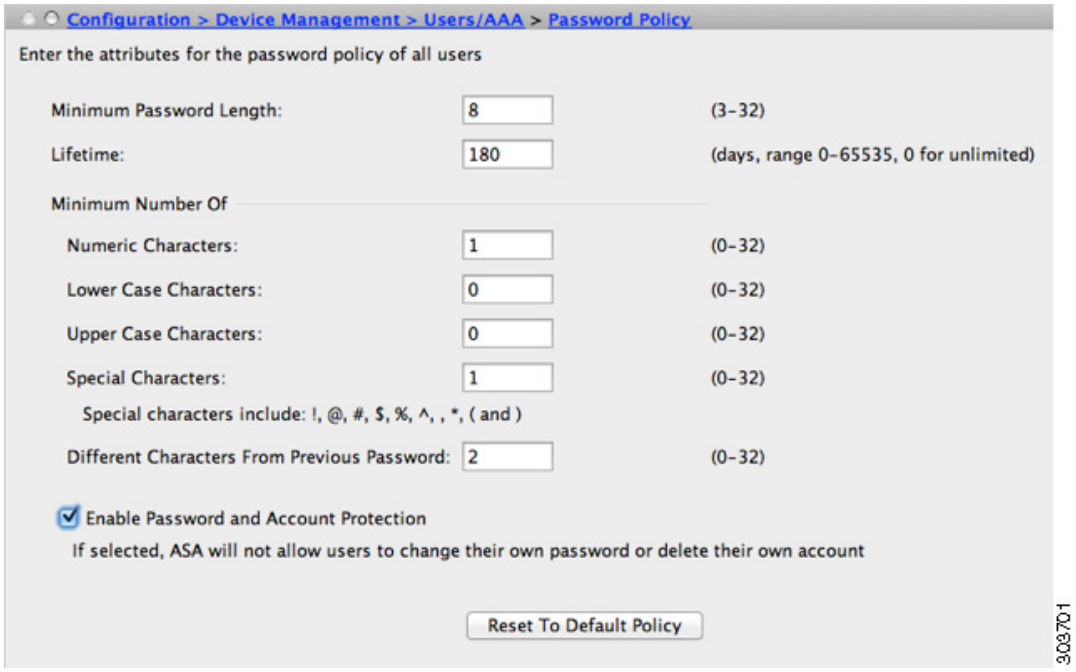
비밀번호 정책을 구성한 다음 (본인의 또는 다른 사용자의) 비밀번호를 변경할 때 비밀번호 정책이 새 비밀번호에 적용됩니다. 기존 비밀번호는 적용 대상에서 제외됩니다. 새 정책은 User Accounts 창 및 Change My Password 창을 사용하여 비밀번호를 변경하는 경우에 적용됩니다.

전제 조건

- 36-15 페이지의 CLI 및 , enable 명령 액세스를 위한 인증 구성에 따라 CLI/ASDM 및 enable 인증을 모두 구성합니다. 로컬 데이터베이스를 지정해야 합니다.

세부 단계

1단계 **Configuration > Device Management > Users/AAA > Password Policy**를 선택합니다.



2단계 다음 옵션을 원하는 대로 조합하여 구성합니다.

- Minimum Password Length—비밀번호의 최소 길이를 입력합니다. 유효한 값의 범위는 3자~64자입니다. 권장되는 비밀번호 최소 길이는 8자입니다.
- (선택 사항) 원격 사용자(SSH, 텔넷, HTTP)의 비밀번호가 만료될 때까지의 기한(일)을 입력합니다. 콘솔 포트의 사용자는 비밀번호 만료로 인해 잠기는 일이 없습니다. 유효한 값의 범위는 0일~65536일입니다. 기본값은 0일입니다. 즉 비밀번호가 절대 만료되지 않습니다.

  비밀번호가 만료되기 7일 전에 경고 메시지가 나타납니다. 비밀번호가 만료되면 원격 사용자는 시스템 액세스가 거부됩니다. 만료 후 액세스 권한을 얻으려면 다음 중 하나를 수행합니다.
  - 다른 관리자가 비밀번호를 변경하게 합니다.
  - 물리적 콘솔 포트에 로그인하여 비밀번호를 변경합니다.
- Minimum Number Of—다음 유형 문자의 최소 개수를 지정합니다.
  - Numeric Characters—비밀번호에 포함해야 할 숫자의 최소 개수를 입력합니다. 유효한 값의 범위는 0자~64자입니다. 기본값은 0입니다.
  - Lower Case Characters—비밀번호에 포함해야 할 소문자의 최소 개수를 입력합니다. 유효한 값의 범위는 0자~64자입니다. 기본값은 0입니다.
  - Upper Case Characters—비밀번호에 포함해야 할 대문자의 최소 개수를 입력합니다. 유효한 값의 범위는 0자~64자입니다. 기본값은 0입니다.
  - Special Characters—비밀번호에 포함해야 할 특수 문자의 최소 개수를 입력합니다. 유효한 값의 범위는 0자~64자입니다. 특수 문자에는 !, @, #, $, %, ^, &, *, '(' 및 ')'가 포함됩니다. 기본값은 0입니다.

- Different Characters from Previous Password—새 비밀번호에서 기존 비밀번호와 다르게 해야 할 문자의 최소 개수를 입력합니다. 유효한 값의 범위는 0자~64자입니다. 기본값은 0입니다. 문자 매칭은 위치와 상관없습니다. 즉 새 비밀번호 문자가 기존 비밀번호의 어느 위치에도 없어야 변경된 것으로 간주됩니다.

3단계 (선택 사항) 사용자가 User Accounts 창이 아닌 Change My Password 창에서 비밀번호를 변경하게 하려면 **Authentication Enable** 확인란을 선택합니다. 기본 설정은 disabled입니다. 즉 사용자는 두 방법 중 어느 쪽이든 사용하여 비밀번호를 변경할 수 있습니다.

이 기능을 활성화한 경우, User Accounts 창에서 비밀번호를 변경하려고 시도하면 다음 오류 메시지가 생성됩니다.

```
ERROR: Changing your own password is prohibited
```

4단계 비밀번호 정책을 기본값으로 재설정하려면 **Reset to Default**를 클릭합니다.

5단계 **Apply**를 클릭하여 컨피그레이션 설정을 적용합니다.

비밀번호 변경

비밀번호 정책에서 비밀번호 수명을 구성한 경우, 기존 비밀번호가 만료되면의 비밀번호를 새로운 비밀번호로 변경해야 합니다. 비밀번호 정책 인증을 활성화한 경우 반드시 이 비밀번호 변경 방법을 사용해야 합니다. 비밀번호 정책 인증이 활성화되지 않은 경우에는 이 방법을 사용하거나 User Accounts 창을 사용하여 직접 사용자 어카운트를 변경할 수도 있습니다.

세부 단계

1단계 **Configuration > Device Management > Users/AAA > Change Password**를 선택합니다.

2단계 기존 비밀번호를 입력합니다.

3단계 새 비밀번호를 입력합니다.

4단계 새 비밀번호를 확인합니다.

5단계 **Make Change**를 클릭합니다.

6단계 **Save** 아이콘을 클릭하여 변경 사항을 실행 중인 컨피그레이션에 저장합니다.

명령 권한 부여 구성

명령에 대한 액세스를 제어하고 싶은 경우 ASA에서 명령 권한 부여를 구성할 수 있습니다. 이는 사용자가 어떤 명령을 사용할 수 있는가를 결정하는 것입니다. 기본적으로 로그인할 때 사용자 EXEC 모드에 액세스할 수 있습니다. 이 모드는 최소한의 명령만 제공합니다. **enable** 명령(또는 로컬 데이터베이스를 사용할 때는 **login** 명령)을 입력하면 특별 권한 EXEC 모드와 고급 명령(컨피그레이션 명령 포함)에 액세스할 수 있습니다.

다음 2가지 명령 권한 부여 방식 중 하나를 사용할 수 있습니다.

- 로컬 권한 레벨
- TACACS+ 서버 권한 레벨

명령 권한 부여에 대한 자세한 내용은 36-11 페이지의 명령 권한 부여에 대한 정보를 참조하십시오.

- 36-21 페이지의 로컬 명령 권한 부여 구성
- 36-22 페이지의 로컬 명령 권한 레벨 보기
- 36-22 페이지의 TACACS+ 서버의 명령 구성
- 36-25 페이지의 TACACS+ 명령 권한 부여 구성

로컬 명령 권한 부여 구성

로컬 명령 권한 부여에서는 16가지 권한 레벨(0~15) 중 하나에 명령을 지정할 수 있습니다. 기본적으로 각 명령은 권한 레벨 0 또는 15 중 하나에 지정됩니다. 각 사용자를 특정 권한 레벨로 정의할 수 있으며, 각 사용자는 지정된 권한 레벨 이하의 어떤 명령도 입력할 수 있습니다. ASA에서는 로컬 데이터베이스, RADIUS 서버 또는 (LDAP 특성을 RADIUS 특성에 매핑한 경우) LDAP 서버에 정의된 사용자 권한 레벨을 지원합니다. 자세한 내용은 다음 절을 참조하십시오.

- 28-3 페이지의 로컬 데이터베이스에 사용자 어카운트 추가
- 29-2 페이지의 지원되는 인증 방법
- 31-5 페이지의 LDAP 특성 맵 구성

로컬 명령 권한 부여를 구성하려면 다음 단계를 수행합니다.

세부 단계

1단계 명령 권한 부여를 활성화하려면 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**을 선택하고 **Enable authorization for command access > Enable** 확인란을 선택합니다.

2단계 Server Group 드롭다운 목록에서 LOCAL을 선택합니다.

3단계 로컬 명령 권한 부여를 활성화한 경우, 개별 명령이나 명령 그룹에 직접 권한 레벨을 부여하거나 미리 정의된 사용자 어카운트 권한을 활성화할 수 있습니다.

- 미리 정의된 사용자 어카운트 권한을 사용하려면 **Set ASDM Defined User Roles**를 클릭합니다.

  ASDM Defined User Roles Setup 대화 상자는 명령과 그 레벨을 표시합니다. 미리 정의된 사용자 어카운트 권한, 즉 Admin(권한 레벨 15, 모든 CLI 명령에 대한 전체 액세스), Read Only(권한 레벨 5, 읽기 전용 액세스), Monitor Only(권한 레벨 3, Monitoring 섹션만 액세스)를 사용하려면 **Yes**를 클릭합니다.

- 명령 레벨을 직접 구성하려면 **Configure Command Privileges**를 클릭합니다.

  Command Privileges Setup 대화 상자가 나타납니다. Command Mode 드롭다운 목록에서 --All Modes--를 선택하여 모든 명령을 보거나 컨피그레이션 모드를 선택하여 그 모드에서 이용 가능한 명령을 볼 수 있습니다. 예를 들어, 컨텍스트를 선택한 경우 컨텍스트 컨피그레이션 모드에서 사용 가능한 모든 명령을 볼 수 있습니다. 사용자 EXEC 모드 또는 특별 권한 EXEC 모드뿐 아니라 컨피그레이션 모드에서도 어떤 명령을 입력할 수 있고 이 명령이 각 모드에서 다른 작업을 수행할 경우, 이 모드 각각에 대한 권한 레벨을 설정할 수 있습니다.

  Variant 열은 show, clear 또는 cmd를 표시합니다. 명령의 show, clear 또는 configure 형식에 대해서만 권한을 설정할 수 있습니다. 명령의 configure 형식은 일반적으로 컨피그레이션 변경을 일으키는 형식으로서 수정되지 않은 명령(**show** 또는 **clear** 접두사 없음)이거나 **no** 형식입니다.

  명령의 레벨을 변경하려면 두 번 클릭하거나 **Edit**를 클릭합니다. 0~15의 레벨을 설정할 수 있습니다. *주(main)* 명령의 권한 레벨만 구성할 수 있습니다. 이를테면 모든 **aaa** 명령의 레벨을 구성할 수 있으나, **aaa authentication** 명령과 **aaa authorization** 명령의 레벨을 각각 구성할 수는 없습니다.

  나타나는 모든 명령의 레벨을 변경하려면 **Select All**을 클릭하고 **Edit**를 클릭합니다.

  변경 사항을 적용하려면 **OK**를 클릭합니다.

4단계 RADIUS의 관리 사용자 권한 레벨을 지원하려면 **Perform authorization for exec shell access > Enable** 확인란을 선택합니다.

이 옵션을 사용하지 않을 경우 ASA에서는 로컬 데이터베이스 사용자의 권한 레벨만 지원하며, 그 밖의 모든 사용자 유형은 기본적으로 레벨 15가 됩니다.

이 옵션은 로컬, RADIUS, 매핑된 LDAP, TACACS+ 사용자에 대한 관리 권한 부여도 활성화합니다. 자세한 내용은 36-16 페이지의 관리 권한 부여로 사용자 CLI 및 ASDM 액세스 제한를 참조하십시오.

5단계 **Apply**를 클릭합니다.

권한 부여 설정이 지정되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

로컬 명령 권한 레벨 보기

다음 명령을 Tools > Command Line Interface 툴에서 입력하면 명령에 대한 권한 레벨을 볼 수 있습니다.

TACACS+ 서버의 명령 구성

Cisco Secure ACS(Access Control Server) TACACS+ 서버의 명령을 어떤 그룹 또는 개별 사용자를 위한 공유 프로필 구성 요소로 구성할 수 있습니다. 타사 TACACS+ 서버의 경우 명령 권한 부여 지원에 대한 자세한 내용은 서버 설명서를 참조하십시오.

Cisco Secure ACS Version 3.1의 명령 구성에 대한 다음 지침을 참조하십시오. 그중 상당수는 타사 서버에도 적용됩니다.

- ASA에서 셸 명령으로 권한 부여될 명령을 보냅니다. 즉 TACACS+ 서버의 명령을 셸 명령으로 구성합니다.

참고 Cisco Secure ACS에 "pix-shell"이라는 명령 유형이 포함되었을 수 있습니다. ASA 명령 권한 부여에는 이 유형을 사용하지 마십시오.

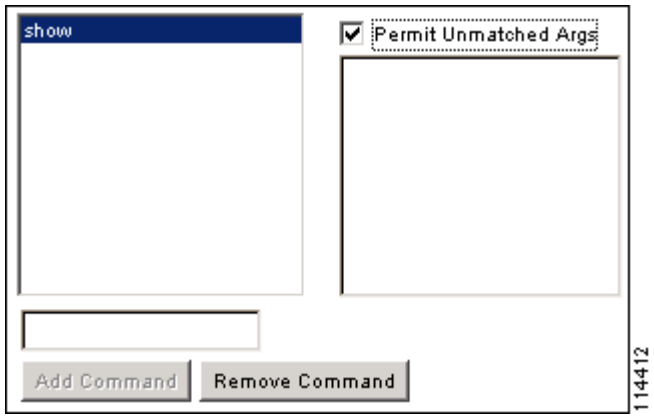
- 이 명령의 첫 단어를 주 명령으로 간주합니다. 모든 추가 단어는 인수로 간주하는데, 앞에 **permit** 또는 **deny**를 붙여야 합니다.

  예를 들어, **show running-configuration aaa-server** 명령을 허용하려면 command 필드에 **show running-configuration**을 추가하고 arguments 필드에 **permit aaa-server**를 입력합니다.

- **Permit Unmatched Args** 확인란을 선택하면 명시적으로 거부하지 않은 명령의 모든 인수를 허용할 수 있습니다.

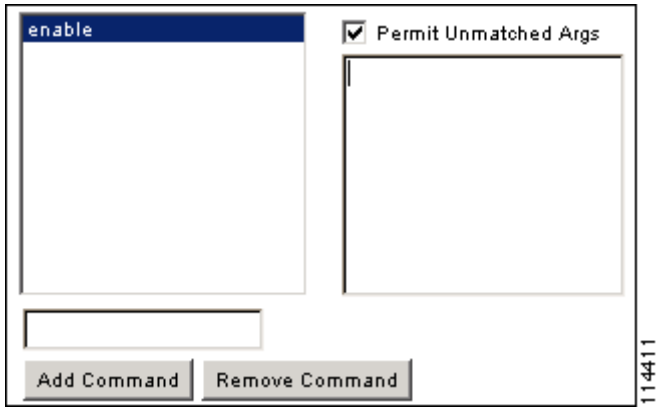
  예를 들어, **show** 명령만 구성할 수 있으며, 그러면 모든 **show** 명령이 허용됩니다. 이 방법을 사용하는 것이 좋습니다. 그러면 약어와 물음표(CLI 사용법 표시)를 비롯하여 명령의 모든 버전을 예상할 필요 없습니다(그림 36-1 참조).

그림 36-1 모든 관련 명령 허용



- 하나의 단어인 명령에 대해서는 *반드시* 일치하지 않음(unmatched) 인수를 허용해야 합니다. **enable**, **help**처럼 인수가 없는 경우도 해당됩니다(그림 36-2 참조).

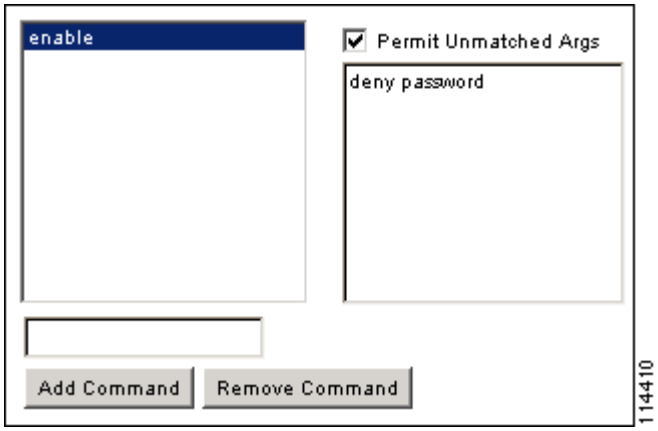
그림 36-2 단일 단어 명령 허용



- 일부 인수를 허용하지 않으려면 그 인수 앞에 **deny**를 입력합니다.

  예를 들어, **enable**을 허용하되 **enable password**는 허용하지 않으려면 commands 필드에 **enable**을 입력하고 arguments 필드에 **deny password**라고 입력합니다. 반드시 **Permit Unmatched Args** 확인란을 선택하여 **enable**만 계속 허용되게 해야 합니다(그림 36-3 참조).

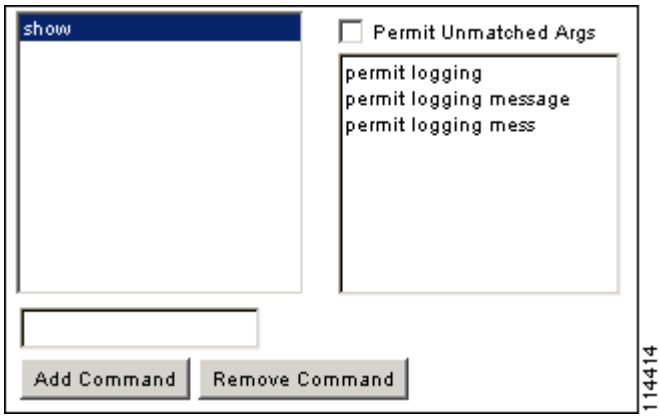
그림 36-3 인수를 허용하지 않기



- 명령줄에서 어떤 명령을 축약하면 ASA는 접두사와 주 명령을 전체 텍스트로 확장합니다. 그러나 추가 인수는 입력하는 대로 TACACS+ 서버에 보냅니다.

  예를 들어, **sh log**를 입력하면 ASA에서는 전체 명령, 즉 **show logging**을 TACACS+ 서버에 보냅니다. 그러나 **sh log mess**를 입력하면 ASA는 확장된 명령 **show logging message**가 아닌 **show logging mess**를 TACACS+ 서버에 보냅니다. 약어를 예상하여 동일 인수의 여러 철자를 구성할 수 있습니다(그림 36-4 참조).

그림 36-4 약어 지정



- 모든 사용자에게 다음 기본 명령을 허용하는 것이 좋습니다.
  - **show checksum**
  - **show curpriv**
  - **enable**
  - **help**
  - **show history**

- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

TACACS+ 명령 권한 부여 구성

TACACS+ 명령 권한 부여를 활성화한 경우 어떤 사용자가 CLI에서 명령을 입력하면 ASA에서는 TACACS+ 서버에 명령과 사용자 이름을 보내 권한 부여된 명령인지 확인합니다.

TACACS+ 명령 권한 부여를 활성화하려면 먼저 TACACS+ 서버에 정의된 사용자로 ASA에 로그인해야 하며 ASA 구성을 계속 진행하는 데 필요한 명령 권한이 있어야 합니다. 예를 들어, 모든 명령 권한을 갖는 관리 사용자로 로그인해야 합니다. 그러지 않으면 뜻하지 않게 잠기게 될 수 있습니다.

원하는 대로 컨피그레이션이 작동할 때까지는 컨피그레이션을 저장하지 마십시오. 실수로 잠긴 경우 대개는 ASA를 다시 시작하면 액세스를 복구할 수 있습니다. 그래도 잠겨 있다면 36-28 페이지의 잠금에서 복구를 참조하십시오.

TACACS+ 시스템이 확실히 안정적이고 신뢰할 수 있는지 확인합니다. 필요한 수준의 신뢰도에 이르기 위해서는 일반적으로 완전 이중 TACACS+ 서버 시스템이 있고 ASA와 완전 이중 방식으로 연결되어야 합니다. 예를 들어, TACACS+ 서버 풀에서 인터페이스 1과 연결된 서버 1대와 인터페이스 2와 연결된 또 다른 서버를 포함합니다. TACACS+ 서버를 사용할 수 없을 경우를 위한 대비책으로 로컬 명령 권한 부여를 구성할 수도 있습니다. 그러한 경우 36-21 페이지의 명령 권한 부여 구성의 절차에 따라 로컬 사용자 및 명령 권한 레벨을 구성해야 합니다.

TACACS+ 명령 권한 부여를 구성하려면 다음 단계를 수행합니다.

세부 단계

1단계 TACACS+ 서버를 사용하여 명령 권한 부여를 수행하려면 **Configuration > Device Management > Users/AAA > AAA Access > Authorization**을 선택하고 **Enable authorization for command access > Enable** 확인란을 선택합니다.

2단계 Server Group 드롭다운 목록에서 AAA 서버 그룹 이름을 선택합니다.

3단계 (선택 사항) ASA에서 AAA 서버를 사용할 수 없을 때 로컬 데이터베이스를 대신 사용하도록 구성할 수 있습니다. 그러기 위해서는 **Use LOCAL when server group fails** 확인란을 선택합니다. 로컬 데이터베이스에서 AAA 서버와 동일한 사용자 이름과 비밀번호를 사용하는 것이 좋습니다. ASA 프롬프트에서는 어떤 방법을 사용 중인지 알려주지 않기 때문입니다. 반드시 로컬 데이터베이스의 사용자(28-3 페이지의 로컬 데이터베이스에 사용자 어카운트 추가 참조)와 명령 권한 레벨(36-21 페이지의 로컬 명령 권한 부여 구성 참조)을 구성해야 합니다.

4단계 **Apply**를 클릭합니다.

명령 권한 부여 설정이 지정되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

관리 액세스 어카운팅 구성

CLI에서 **show** 명령이 아닌 임의의 명령을 입력할 때 TACACS+ 어카운팅 서버에 어카운팅 메시지를 보낼 수 있습니다. 사용자가 로그인할 때, 사용자가 **enable** 명령을 입력할 때 또는 사용자가 명령을 실행할 때 어카운팅을 구성할 수 있습니다.

명령 어카운팅에는 TACACS+ 서버만 사용할 수 있습니다.

관리 액세스를 구성하고 명령 어카운팅을 활성화하려면 다음 단계를 수행합니다.

세부 단계

1단계 사용자가 **enable** 명령을 입력할 때 사용자 어카운팅을 활성화하려면 다음 단계를 수행합니다.

a. **Configuration > Device Management > Users/AAA > AAA Access > Accounting**을 선택하고 **Require accounting to allow accounting of user activity > Enable** 확인란을 선택합니다.

b. Server Group 드롭다운 목록에서 RADIUS 또는 TACACS+ 서버 그룹 이름을 선택합니다.

2단계 사용자가 텔넷, SSH 또는 시리얼 콘솔을 사용하여 ASA에 액세스할 때 사용자 어카운팅을 활성화하려면 다음 단계를 수행합니다.

a. Require accounting for the following types of connections 영역에서 Serial, SSH 및/또는 Telnet 확인란을 선택합니다.

b. 각 연결 유형에 대해 Server Group 드롭다운 목록에서 RADIUS 또는 TACACS+ 서버 그룹 이름을 선택합니다.

3단계 명령 어카운팅을 구성하려면 다음 단계를 수행합니다.

a. Require command accounting 영역에서 **Enable** 확인란을 선택합니다.

b. Server Group 드롭다운 목록에서 TACACS+ 서버 그룹 이름을 선택합니다. RADIUS는 지원되지 않습니다.

CLI에서 **show** 명령이 아닌 임의의 명령을 입력할 때 TACACS+ 어카운팅 서버에 어카운팅 메시지를 보낼 수 있습니다.

c. Command Privilege Setup 대화 상자를 사용하여 명령 권한 레벨을 사용자 지정할 경우, Privilege level 드롭다운 목록에서 최소 권한 레벨을 지정하는 방법으로 ASA에서 어카운팅을 수행할 명령을 제한할 수 있습니다. ASA는 최소 권한 레벨보다 낮은 명령에 대해서는 어카운팅을 수행하지 않습니다.

4단계 **Apply**를 클릭합니다.

어카운팅 설정이 지정되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

현재 로그인한 사용자 보기

현재 로그인한 사용자를 보려면Tools > Command Line Interface 툴에 다음 명령을 입력합니다.

```
ciscoasa# show curpriv
```

예

다음은 **show curpriv** 명령 출력의 샘플입니다.

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

표 36-1에서는 **show curpriv** 명령 출력에 대해 설명합니다.

표 36-1 show curpriv 명령 출력 설명

필드	설명
Username	사용자 이름. 기본 사용자로 로그인할 경우 이름은 enable_1(사용자 EXEC) 또는 enable_15(특별 권한 EXEC)입니다.
Current privilege level	레벨은 0부터 15까지입니다. 로컬 명령 권한 부여를 구성하고 중간 권한 레벨에 명령을 지정하지 않는 한, 레벨 0과 15만 사용됩니다.
Current Modes	사용 가능한 액세스 모드는 다음과 같습니다. • P_UNPR—사용자 EXEC 모드(레벨 0과 1) • P_PRIV—특별 권한 EXEC 모드(레벨 2~15) • P_CONF—구성 모드

관리 세션 할당량 설정

동시 관리 세션의 최대 개수를 설정할 수 있습니다. 최대 개수에 도달하면 더 이상 추가 세션이 허용되지 않으며 syslog 메시지가 생성됩니다. 시스템 잠금을 방지하는 차원에서 관리 세션 할당량 메커니즘이 콘솔 세션을 차단할 수 없습니다.

관리 세션 할당량을 설정하려면 다음 단계를 수행합니다.

1단계 **Configuration > Device Management > Management Access > Management Session Quota**를 선택합니다.

2단계 ASA에서 허용되는 동시 ASDM, SSH, 텔넷 세션의 최대 개수를 입력합니다. 유효한 값의 범위는 0~10000입니다.

참고 관리 할당량 세션 개수를 초과하면 오류 메시지가 나타나고 ASDM이 닫힙니다.

3단계 **Apply**를 클릭하여 컨피그레이션 변경 사항을 저장합니다.

잠금에서 복구

명령 권한 부여 또는 CLI 권한 부여를 활성화할 때 ASA CLI에서 잠기는 경우가 있습니다. 대개는 ASA를 다시 시작하여 액세스를 복구할 수 있습니다. 그러나 이미 컨피그레이션을 저장한 경우 잠길 수 있습니다. 표 36-2에서는 대표적인 잠금 조건과 그로부터 복구하는 방법을 소개합니다.

표 36-2 CLI 인증 및 명령 권한 부여 잠금 시나리오

기능	잠금 조건	설명	해결 방법: 단일 모드	해결 방법: 다중 모드
로컬 CLI 권한 부여	로컬 데이터베이스에 어떤 사용자도 구성되지 않았습니다.	로컬 데이터베이스에 사용자가 없을 경우 로그인할 수 없고 어떤 사용자도 추가할 수 없습니다.	로그인하고 비밀번호 및 **aaa** 명령을 재설정합니다.	스위치에서 ASA로 세션 연결. 시스템 실행 영역에서 컨텍스트로 변경하고 사용자를 추가할 수 있습니다.
TACACS+ 명령 권한 부여 TACACS+ CLI 인증 RADIUS CLI 인증	서버가 중지했거나 연결 불가한 상태이며, 구성된 대비책이 없습니다.	서버가 연결 불가한 상태라면 로그인할 수 없고 어떤 명령도 입력할 수 없습니다.	1. 로그인하고 비밀번호 및 AAA 명령을 재설정합니다. 2. 로컬 데이터베이스를 대비책으로 구성하여 서버가 중지하더라도 잠기지 않게 합니다.	1. ASA에서 네트워크 컨피그레이션이 올바르지 않아 서버 연결이 불가할 경우 스위치에서 ASA로 세션 연결합니다. 시스템 실행 영역에서 컨텍스트로 변경하고 네트워크 설정을 재구성할 수 있습니다. 2. 로컬 데이터베이스를 대비책으로 구성하여 서버가 중지하더라도 잠기지 않게 합니다.
TACACS+ 명령 권한 부여	충분한 권한이 없는 사용자 또는 존재하지 않는 사용자로 로그인한 상태입니다.	명령 권한 부여를 활성화했지만, 해당 사용자가 더 이상 어떤 명령도입력할수없음을 알게 되었습니다.	TACACS+ 서버 사용자 어카운트의 문제를 해결합니다. TACACS+ 서버에 대한 액세스 권한이 없는데 즉시 ASA를 구성해야 하는 경우, 유지보수 파티션으로 로그인하고 비밀번호와 **aaa** 명령을 재설정합니다.	스위치에서 ASA로 세션 연결. 시스템 실행 공간에서 컨텍스트로 변경하고 컨피그레이션 변경 사항을 완료할 수 있습니다. 또한 TACACS+ 컨피그레이션의 문제를 해결할 때까지 명령 권한 부여를 비활성화할 수도 있습니다.
로컬 명령 권한 부여	충분한 권한이 없는 사용자로 로그인했습니다.	명령 권한 부여를 활성화했지만, 해당 사용자가 더 이상 어떤 명령도입력할수없음을 알게 되었습니다.	로그인하고 비밀번호 및 **aaa** 명령을 재설정합니다.	스위치에서 ASA로 세션 연결. 시스템 실행 공간에서 컨텍스트로 변경하고 사용자 레벨을 변경할 수 있습니다.

디바이스 액세스 모니터링

디바이스 액세스를 모니터링하려면 다음 창을 확인합니다.

경로	목적
Monitoring > Properties > Device Access > ASDM/HTTPS/Telnet/SSH Sessions	맨 위 창은 연결 유형, 세션 ID, SDM, HTTPS, 텔넷 세션을 통해 연결된 사용자의 IP 주소를 나열합니다. 특정 세션의 연결을 끊으려면 **Disconnect**를 클릭합니다. 맨 아래 창은 클라이언트, 사용자 이름, 연결 상태, 소프트웨어 버전, 수신 암호화 유형, 발신 암호화 유형, 수신 HMAC, 발신 HMAC, SSH 세션 ID, 나머지 rekey 데이터, 나머지 rekey 시간, 데이터 기반 rekey, 시간 기준 rekey, 마지막 rekey 시간을 나열합니다. 특정 세션의 연결을 끊으려면 **Disconnect**를 클릭합니다.
Monitoring > Properties > Device Access > Authenticated Users	사용자 이름, IP 주소, 동적 ACL, 무활동 시간 초과(해당되는 경우), AAA 서버에 의해 인증된 사용자의 절대 시간 초과를 나열합니다.
Monitoring > Properties > Device Access > AAA Local Locked Out Users	잠긴 AAA 로컬 사용자의 사용자 이름, 인증 시도 실패 횟수, 사용자가 잠겼던 시간을 나열합니다. 특정 사용자의 잠금을 해제하려면 **Clear Selected Lockout**를 클릭합니다. 모든 사용자의 잠금을 해제하려면 **Clear All Lockouts**를 클릭합니다.

관리 액세스 기능 내역

표 36-3에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 36-3 관리 액세스 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
관리 액세스	7.0(1)	이 기능을 도입했습니다. 다음 화면을 도입했습니다. Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH Configuration > Device Management > Management Access > Command Line (CLI) > Banner Configuration > Device Management > Management Access > CLI Prompt Configuration > Device Management > Management Access > ICMP Configuration > Device Management > Management Access > File Access > FTP Client Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server Configuration > Device Management > Management Access > File Access > Mount-Points Configuration > Device Management > Users/AAA > AAA Access > Authentication Configuration > Device Management > Users/AAA > AAA Access > Authorization Configuration > Device Management > Users/AAA > AAA Access > > Accounting.
SSH 보안을 강화했습니다. SSH 기본 사용자 이름은 더 이상 지원되지 않습니다.	8.4(2)	8.4(2)부터는 pix 또는 asa 사용자 이름 및 로그인 비밀번호를 사용하여 SSH를 통해 ASA에 연결할 수 없습니다. SSH를 사용하려면 **aaa authentication ssh console LOCAL** 명령(CLI)을 사용하거나 Configuration > Device Management > Users/AAA > AAA Access > Authentication(ASDM)을 사용하여 AAA 인증을 구성해야 합니다. 그런 다음 **username** 명령(CLI)을 입력하거나 Configuration > Device Management > Users/AAA > User Accounts(ASDM)를 사용하여 로컬 사용자를 정의합니다. 로컬 데이터베이스 대신에 AAA 서버를 인증에 사용하려는 경우, 만일에 대비하여 로컬 인증도 구성하는 것이 좋습니다.
로컬 데이터베이스를 사용할 때 관리자 비밀번호 정책 지원	8.4(4.1), 9.1(2)	로컬 데이터베이스를 사용하여 CLI 또는 ASDM 액세스를 위한 인증을 구성할 때, 일정한 시간이 지나면 사용자가 비밀번호를 변경해야 하고 최소 길이, 변경된 문자의 최소 개수와 같은 비밀번호 기준의 준수를 요구하는 비밀번호 정책을 구성할 수 있습니다. 다음 화면을 도입했습니다. Configuration > Device Management > Users/AAA > Password Policy

표 36-3 관리 액세스 기능 내역 (계속)

기능 이름	플랫폼 릴리스	기능 정보
SSH 공개 키 인증 지원	8.4(4.1), 9.1(2)	사용자별로 ASA와의 SSH 연결에 대해 공개 키 인증을 활성화할 수 있습니다. PKF(공개 키 파일) 형식의 키 또는 Base64 키를 지정할 수 있습니다. PKF 키는 최대 4096비트입니다. ASA의 Base64 형식 지원 범위(최대 2048비트)에 비해 너무 큰 키에는 PKF 형식을 사용합니다. 다음 화면을 도입했습니다. Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Authentication Configuration > Device Management > Users/AAA > User Accounts > Edit User Account > Public Key Using PKF. *PKF 키 형식은 9.1(2) 이상에서만 지원됩니다.*
SSH 키 교환에 Diffie-Hellman 그룹 14 지원	8.4(4.1), 9.1(2)	SSH 키 교환을 위한 Diffie-Hellman 그룹 14 지원이 추가되었습니다. 이전에는 그룹 1만 지원되었습니다. 다음 화면을 수정했습니다. Configuration > Device Management > Management Access > ASDM/HTTPS/Telnet/SSH
관리 세션 최대 개수 지원	8.4(4.1), 9.1(2)	동시 ASDM, SSH, 텔넷 세션의 최대 개수를 설정할 수 있습니다. 다음 화면을 도입했습니다. Configuration > Device Management > Management Access > Management Session Quota
다중 컨텍스트 모드의 ASASM에서는 스위치로부터의 텔넷 및 가상 콘솔 인증 지원.	8.5(1)	다중 컨텍스트 모드의 스위치에서 ASASM로의 연결이 시스템 실행 영역으로 연결되지만, 관리 컨텍스트에서 이러한 연결에 적용할 인증을 구성할 수 있습니다.
SSH를 위한 AES-CTR 암호화	9.1(2)	ASA의 SSH 서버 인증에서 이제 AES-CTR 모드 암호화를 지원합니다.
SSH rekey 간격 향상		SSH 연결은 연결 시간이 60분이 지났거나 데이터 트래픽이 1GB를 초과하면 키가 다시 생성됩니다.
일회용 비밀번호 인증 향상	9.2(1)	충분한 권한이 있는 관리자는 인증 자격 증명을 한 번 입력하면 특별 권한 EXEC 모드에 들어갈 수 있습니다. **auto-enable** 옵션이 **aaa authorization exec** 명령에 추가되었습니다. 다음 화면을 수정했습니다. Configuration > Device Management > Users/AAA > AAA Access > Authorization

37 장

소프트웨어 및 구성

이 장에서는 Cisco ASA 소프트웨어 및 컨피그레이션을 관리하는 방법을 설명합니다.

소프트웨어 업그레이드

업그레이드 경로 및 마이그레이션

- 9.0 이전 릴리스에서 업그레이드하는 경우, ACL 마이그레이션 때문에 향후 다운그레이드할 수 없습니다. 다운그레이드해야 할 경우에 대비하여 반드시 컨피그레이션 파일을 백업하십시오. 자세한 내용은 9.0 업그레이드 설명서의 ACL 마이그레이션 섹션을 참조하십시오.
- 9.1(2.8) 이전 버전에서 9.1(2.8) 이상으로 업그레이드하려면 다음 버전 중 하나를 실행하고 있어야 합니다.
  - 8.4(5) 이상
  - 9.0(2) 이상
  - 9.1(2)

더 오래된 버전을 실행하고 있다면 9.1(2.8) 이상으로 곧바로 업그레이드할 수 없습니다. *먼저* 위 버전 중 하나로 업그레이드해야 합니다. 예:

9.1(2.8) 이전 ASA 버전	1차 업그레이드할 버전:	그 다음에 업그레이드할 버전:
8.2(1)	8.4(7)	9.3(1) 이상
8.4(4)	8.4(7)	9.3(1) 이상
9.0(1)	9.0(4)	9.3(1) 이상
9.1(1)	9.1(2)	9.3(1) 이상

- 8.3 이전 버전에서 업그레이드하는 경우
  - 컨피그레이션 마이그레이션에 대한 자세한 내용은 *Cisco ASA 5500 버전 8.3으로의 마이그레이션 설명서*를 참조하십시오.
  - 9.0 이상으로 곧바로 업그레이드할 수 없습니다. 성공적인 마이그레이션을 위해서는 먼저 버전 8.4로 업그레이드해야 합니다.
- 제로 다운타임 업그레이드를 위한 소프트웨어 버전 요구 사항

  장애 조치 컨피그레이션 또는 ASA 클러스터에 포함된 유닛은 주 소프트웨어 버전(1번째 번호)과 부 소프트웨어 버전(2번째 번호)이 동일해야 합니다. 그러나 업그레이드 프로세스에서는 유닛의 버전을 일치시킬 필요는 없습니다. 각 유닛에서 여러 버전의 소프트웨어가 실행되고 있더라도 장애 조치는 계속 지원됩니다. 장기적인 호환성 및 안정성을 위해 가급적 서둘러 모든 유닛을 동일한 버전으로 업그레이드하는 것이 좋습니다.

  표 37-1에서는 지원되는 제로 다운타임 업그레이드 시나리오를 소개합니다.

표 37-1 제로 다운타임 업그레이드 지원

업그레이드 유형	지원
유지 보수 릴리스	임의의 유지 보수 릴리스에서 부(minor) 릴리스 범위의 다른 유지 보수 릴리스로 업그레이드할 수 있습니다. 예를 들면, 9.1(1)에서 9.1(5)로 업그레이드할 수 있습니다. 먼저 그 사이에 유지 보수 릴리스를 설치할 필요 없습니다.
부 릴리스	부 릴리스에서 다음 부 릴리스로 업그레이드할 수 있습니다. 부 릴리스를 건너뛸 수 없습니다. 예를 들어, 9.0에서 9.1로 업그레이드할 수 있습니다. 9.0에서 9.2로 곧바로 업그레이드하는 경우 제로 다운타임 업그레이드가 지원되지 않습니다. 먼저 9.1로 업그레이드해야 합니다. **참고** 제로 다운타임 업그레이드는 기능 컨피그레이션이 마이그레이션된 경우에도 가능합니다.

표 37-1 제로 다운타임 업그레이드 지원 (계속)

업그레이드 유형	지원
주 릴리스	이전 버전의 최종 부 릴리스에서 다음 주 릴리스로 업그레이드할 수 있습니다. 예를 들어, 8.6에서 9.0으로 업그레이드할 수 있습니다. 단, 8.6이 해당 모델의 8.x 릴리스에서 마지막 부 버전이어야 합니다. 8.6에서 9.1로 곧바로 업그레이드하는 경우에는 제로 다운타임 업그레이드가 지원되지 않습니다. 먼저 9.0으로 업그레이드해야 합니다. 부 릴리스에서 지원되지 않는 모델의 경우, 부 릴리스를 건너뛸 수 있습니다. 예를 들어, ASA 5585-X(8.5 또는 8.6에서 지원되지 않는 모델)는 8.4에서 9.0으로 업그레이드할 수 있습니다. **참고** 제로 다운타임 업그레이드는 기능 컨피그레이션이 마이그레이션된 경우에도 가능합니다.

현재 버전 보기

ASDM 홈 페이지에 소프트웨어 버전이 나타납니다. 홈 페이지를 보면서 ASA의 소프트웨어 버전을 확인합니다.

Cisco.com에서 소프트웨어 다운로드

ASDM Upgrade 마법사를 사용하는 경우 소프트웨어를 미리 다운로드할 필요 없습니다. 장애 조치 업그레이드 등을 위해 수동으로 업그레이드하는 경우 로컬 컴퓨터에 이미지를 다운로드합니다.

Cisco.com 로그인이 가능한 경우 다음 웹 사이트에서 OS 및 ASDM 이미지를 얻을 수 있습니다.

http://www.cisco.com/go/asa-software

독립형 유닛 업그레이드

이 섹션에서는 ASDM 및 OS(운영 체제) 이미지를 설치하는 방법을 설명합니다.

- 37-3 페이지의 로컬 컴퓨터에서 업그레이드
- 37-5 페이지의 Cisco.com 마법사를 사용한 업그레이드

로컬 컴퓨터에서 업그레이드

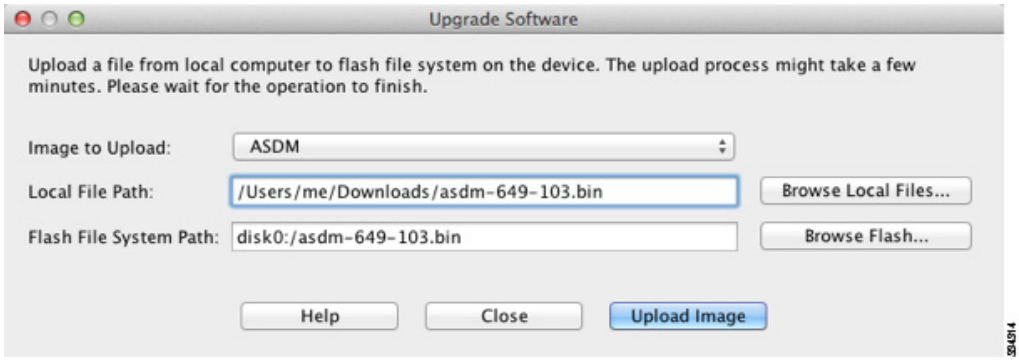
Upgrade Software from Local Computer 툴을 사용하면 컴퓨터의 이미지 파일을 플래시 파일 시스템에 업로드하여 ASA를 업로드할 수 있습니다.

절차

1단계 (컨피그레이션 마이그레이션이 있는 경우) ASDM에서 **Tools > Backup Configurations** 툴을 사용하여 기존 컨피그레이션을 백업합니다.

2단계 기본 ASDM 애플리케이션 창에서 **Tools > Upgrade Software from Local Computer**를 선택합니다.

Upgrade Software 대화 상자가 나타납니다.



3단계 **Image to Upload** 드롭다운 목록에서 **ASDM**을 선택합니다.

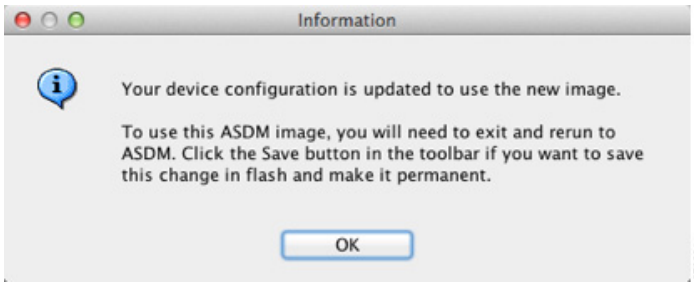
4단계 **Local File Path** 필드에 컴퓨터에 있는 파일의 로컬 경로를 입력하거나 **Browse Local Files**를 클릭하여 PC의 파일을 찾습니다.

5단계 **Flash File System Path** 필드에 플래시 파일 시스템의 경로를 입력하거나 **Browse Flash**를 클릭하여 플래시 파일 시스템의 디렉토리 또는 파일을 찾습니다.

6단계 **Upload Image**를 클릭합니다. 업로드 프로세스에 몇 분이 걸릴 수 있습니다.

7단계 이 이미지를 ASDM 이미지로 설정할지 묻습니다. **Yes**를 클릭합니다.

8단계 ASDM을 종료하고 컨피그레이션을 저장하라는 메시지가 다시 표시됩니다. **OK**를 클릭합니다. Upgrade 툴을 종료합니다. **참고:** ASA 소프트웨어를 업그레이드한 *다음* 컨피그레이션을 저장하고 ASDM을 다시 로드합니다.



9단계 2단계부터 8단계까지 반복하면서 Image to Upload 드롭다운 목록에서 **ASA**를 선택합니다. 다른 파일 유형을 업로드하는 데에도 이 절차를 사용할 수 있습니다.

10단계 ASA를 로드하기 위해 **Tools > System Reload**를 선택합니다.

새 창이 나타나 다시 로드하기 위한 세부 사항을 확인합니다.

a. **Save the running configuration at the time of reload** 라디오 버튼(기본값)을 클릭합니다.

b. 다시 로드할 시간(예: 기본값인 **Now**)을 선택합니다.

c. **Schedule Reload**를 클릭합니다.

다시 로드하는 과정이 진행되면 Reload Status 창이 나타나 다시 로드하는 작업이 수행되고 있음을 알립니다. ASDM 종료 옵션도 제공됩니다.

11단계 ASA가 다시 로드된 다음 ASDM을 다시 시작합니다.

Cisco.com 마법사를 사용한 업그레이드

Upgrade Software from Cisco.com 마법사에서는 ASDM과 ASA를 최신 버전으로 자동 업그레이드할 수 있습니다.

이 마법사에서는 다음을 수행할 수 있습니다.

- 업그레이드할 ASA 이미지 파일 및/또는 ASDM 이미지 파일을 선택합니다.

참고 ASDM은 빌드 번호가 포함된 최신 이미지 버전을 다운로드합니다. 예를 들어, 9.2(1)을 다운로드하는 경우 9.2(1.2)가 다운로드될 수 있습니다. 이는 정상적인 동작이므로 예정된 업그레이드를 계속 진행하면 됩니다.

- 선택한 업그레이드 변경 사항을 검토합니다.
- 이미지를 다운로드하고 설치합니다.
- 설치 상황을 검토합니다.
- 설치가 성공적으로 완료되면 ASA를 다시 시작하여 컨피그레이션을 저장하고 업그레이드를 완료합니다.

절차

1단계 (컨피그레이션 마이그레이션이 있는 경우) ASDM에서 **Tools > Backup Configurations** 툴을 사용하여 기존 컨피그레이션을 백업합니다.

2단계 **Tools > Check for ASA/ASDM Updates**를 선택합니다.

다중 상황 모드에서는 System에서 이 메뉴에 액세스합니다.

Cisco.com Authentication 대화 상자가 나타납니다.

3단계 Cisco.com 사용자 이름과 비밀번호를 입력하고 **Login**을 클릭합니다.

Cisco.com Upgrade 마법사가 나타납니다.

참고 사용 가능한 업그레이드가 없으면 대화 상자가 나타납니다. **OK**를 클릭하면 마법사를 종료합니다.

4단계 **Next**를 클릭하면 **Select Software** 화면이 표시됩니다.

현재 ASA 버전 및 ASDM 버전이 나타납니다.

5단계 ASA 버전과 ASDM 버전을 업그레이드하려면 다음 단계를 수행합니다.

a. **ASA** 영역에서 **Upgrade to** 확인란을 선택한 다음 드롭다운 목록에서 어떤 ASA 버전으로 업그레이드할지 선택합니다.

b. **ASDM** 영역에서 **Upgrade to** 확인란을 선택한 다음 드롭다운 목록에서 어떤 ASDM 버전으로 업그레이드할지 선택합니다.

6단계 **Next**를 클릭하면 **Review Changes** 화면이 표시됩니다.

7단계 다음 항목을 확인합니다.

- 다운로드한 ASA 이미지 파일 및/또는 ASDM 이미지 파일이 정확합니다.
- 업로드하려는 ASA 이미지 파일 및/또는 ASDM 이미지 파일이 정확합니다.
- 정확한 ASA 부트 이미지가 선택되었습니다.

8단계 **Next**를 클릭하여 업그레이드 설치를 시작합니다.

그런 다음 업그레이드 설치의 진행 상황을 확인합니다.

Results 화면이 나타납니다. 여기서는 업그레이드 설치 상태(성공 또는 실패)와 같은 추가 세부 사항을 제공합니다.

9단계 업그레이드 설치가 성공한 경우, 업그레이드 버전이 적용되기 위해서는 **Save configuration and reload device now** 확인란을 선택하여 ASA를 다시 시작하고 ASDM도 다시 시작합니다.

10단계 마법사를 종료하고 컨피그레이션 변경 사항을 저장하려면 **Finish**를 클릭합니다.

참고 그 다음으로 높은 버전이 있어 그 버전으로 업그레이드하려면 마법사를 다시 시작해야 합니다.

장애 조치 쌍 또는 ASA 클러스터 업그레이드

활성/대기(Active/Standby) 장애 조치 쌍 업그레이드

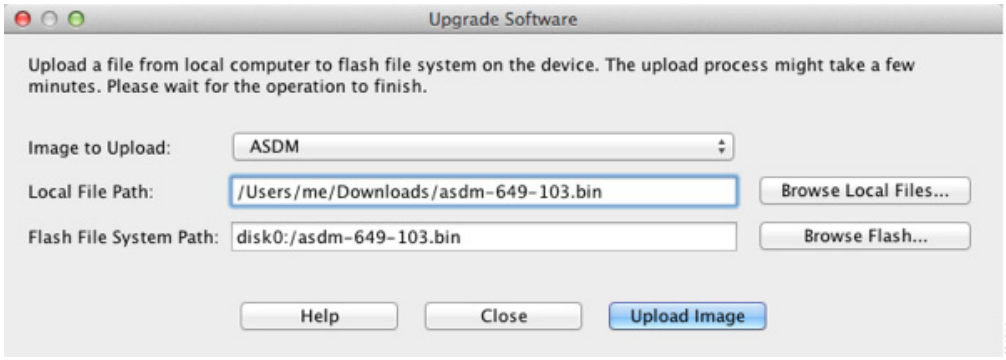
활성/대기 장애 조치 쌍을 업그레이드하려면 다음 단계를 수행합니다.

절차

1단계 (컨피그레이션 마이그레이션이 있는 경우) ASDM에서 **Tools > Backup Configurations** 툴을 사용하여 기존 컨피그레이션을 백업합니다.

2단계 활성 유닛의 기본 ASDM 애플리케이션 창에서 **Tools > Upgrade Software from Local Computer**를 선택합니다.

Upgrade Software 대화 상자가 나타납니다.



3단계 Image to Upload 드롭다운 목록에서 **ASDM**을 선택합니다.

4단계 Local File Path 필드에 컴퓨터에 있는 파일의 로컬 경로를 입력하거나 **Browse Local Files**를 클릭하여 PC의 파일을 찾습니다.

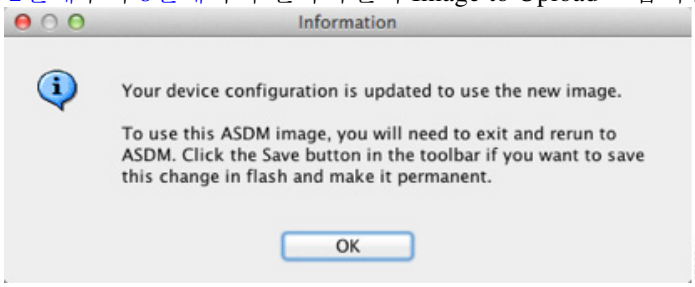
5단계 Flash File System Path 필드에 플래시 파일 시스템의 경로를 입력하거나 **Browse Flash**를 클릭하여 플래시 파일 시스템의 디렉토리 또는 파일을 찾습니다.

6단계 **Upload Image**를 클릭합니다. 업로드 프로세스에 몇 분이 걸릴 수 있습니다.

7단계 이 이미지를 ASDM 이미지로 설정할지 묻습니다. **Yes**를 클릭합니다.

8단계 ASDM을 종료하고 컨피그레이션을 저장하라는 메시지가 다시 표시됩니다. **OK**를 클릭합니다. Upgrade 툴을 종료합니다. **참고:** ASA 소프트웨어를 업그레이드한 *다음* 컨피그레이션을 저장하고 ASDM을 다시 로드합니다.

9단계 2단계부터 8단계까지 반복하면서 Image to Upload 드롭다운 목록에서 **ASA**를 선택합니다.



10단계 도구 모음에서 **Save** 아이콘을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

11단계 ASDM을 *대기* 유닛에 연결하고 2단계~9단계에 따라 활성 유닛에서 사용한 것과 동일한 파일 위치를 사용하여 ASA 및 ASDM 소프트웨어를 업로드합니다.

12단계 대기 ASA를 로드하기 위해 **Tools > System Reload**를 선택합니다.

새 창이 나타나 다시 로드하기 위한 세부 사항을 확인합니다.

a. **Save the running configuration at the time of reload** 라디오 버튼(기본값)을 클릭합니다.

b. 다시 로드할 시간(예: 기본값인 **Now**)을 선택합니다.

c. **Schedule Reload**를 클릭합니다.

다시 로드하는 과정이 진행되면 Reload Status 창이 나타나 다시 로드하는 작업이 수행되고 있음을 알립니다. ASDM 종료 옵션도 제공됩니다.

13단계 대기 ASA가 다시 로드된 다음 ASDM을 다시 시작하고 대기 유닛에 연결하여 실행 중임을 확인합니다.

14단계 ASDM을 *활성* 유닛에 다시 연결합니다.

15단계 **Monitoring > Properties > Failover > Status**를 선택하고 **Make Standby**를 클릭하여 강제적으로 활성 유닛을 대기 유닛에 장애 조치합니다.

16단계 (이전의) 활성 ASA를 로드하기 위해 **Tools > System Reload**를 선택합니다.

새 창이 나타나 다시 로드하기 위한 세부 사항을 확인합니다.

a. **Save the running configuration at the time of reload** 라디오 버튼(기본값)을 클릭합니다.

b. 다시 로드할 시간(예: 기본값인 **Now**)을 선택합니다.

c. **Schedule Reload**를 클릭합니다.

다시 로드하는 과정이 진행되면 Reload Status 창이 나타나 다시 로드하는 작업이 수행되고 있음을 알립니다. ASDM 종료 옵션도 제공됩니다.

ASA가 시작하면 이제 대기 유닛이 됩니다.

활성/활성(Active/Active) 장애 조치 쌍 업그레이드

활성/활성 장애 조치 컨피그레이션의 두 유닛을 업그레이드하려면 다음 단계를 수행합니다.

시작하기 전에

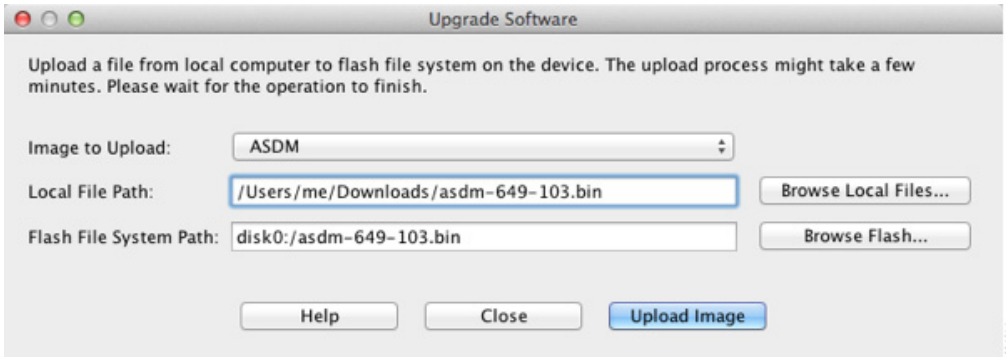
시스템 실행 영역에서 다음 단계를 수행합니다.

절차

1단계 (컨피그레이션 마이그레이션이 있는 경우) ASDM에서 **Tools > Backup Configurations** 툴을 사용하여 기존 컨피그레이션을 백업합니다.

2단계 기본 유닛의 기본 ASDM 애플리케이션 창에서 **Tools > Upgrade Software from Local Computer**를 선택합니다.

Upgrade Software 대화 상자가 나타납니다.



3단계 Image to Upload 드롭다운 목록에서 **ASDM**을 선택합니다.

4단계 Local File Path 필드에 컴퓨터에 있는 파일의 로컬 경로를 입력하거나 **Browse Local Files**를 클릭하여 PC의 파일을 찾습니다.

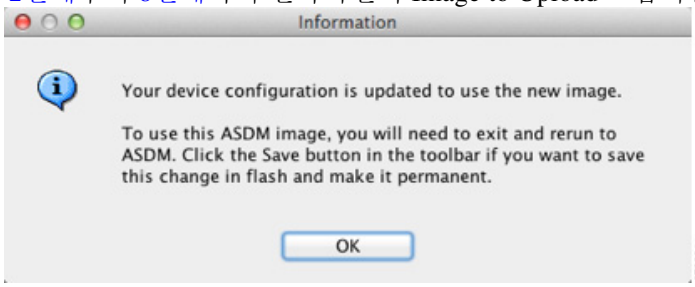
5단계 Flash File System Path 필드에 플래시 파일 시스템의 경로를 입력하거나 **Browse Flash**를 클릭하여 플래시 파일 시스템의 디렉토리 또는 파일을 찾습니다.

6단계 **Upload Image**를 클릭합니다. 업로드 프로세스에 몇 분이 걸릴 수 있습니다.

7단계 이 이미지를 ASDM 이미지로 설정할지 묻습니다. **Yes**를 클릭합니다.

8단계 ASDM을 종료하고 컨피그레이션을 저장하라는 메시지가 다시 표시됩니다. **OK**를 클릭합니다. Upgrade 툴을 종료합니다. **참고:** ASA 소프트웨어를 업그레이드한 *다음* 컨피그레이션을 저장하고 ASDM을 다시 로드합니다.

9단계 2단계부터 8단계까지 반복하면서 Image to Upload 드롭다운 목록에서 **ASA**를 선택합니다.



10단계 도구 모음에서 **Save** 아이콘을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

11단계 기본 유닛에서 두 장애 조치 그룹 모두 활성 상태로 만들기 위해 **Monitoring > Failover > Failover Group #**을 선택합니다. 여기서 **#**은 기본 유닛으로 이동할 장애 조치 그룹의 번호입니다. 그리고 **Make Active**를 클릭합니다.

12단계 ASDM을 *보조* 유닛에 연결하고 2단계~9단계에 따라 활성 유닛에서 사용한 것과 동일한 파일 위치를 사용하여 ASA 및 ASDM 소프트웨어를 업로드합니다.

13단계 보조 ASA를 로드하기 위해 **Tools > System Reload**를 선택합니다.

새 창이 나타나 다시 로드하기 위한 세부 사항을 확인합니다.

a. **Save the running configuration at the time of reload** 라디오 버튼(기본값)을 클릭합니다.

b. 다시 로드할 시간(예: 기본값인 **Now**)을 선택합니다.

c. **Schedule Reload**를 클릭합니다.

다시 로드하는 과정이 진행되면 Reload Status 창이 나타나 다시 로드하는 작업이 수행되고 있음을 알립니다. ASDM 종료 옵션도 제공됩니다.

14단계 ASDM을 *기본* 유닛에 연결하고, **Monitoring > Failover > System**을 선택하여 보조 유닛이 언제 다시 로드되는지 확인합니다.

15단계 보조 유닛이 시작하면 **Monitoring > Properties > Failover > System**을 선택하고 **Make Standby**를 눌러 강제적으로 기본 유닛을 보조 유닛에 장애 조치합니다.

16단계 (이전의) 활성 ASA를 로드하기 위해 **Tools > System Reload**를 선택합니다.

새 창이 나타나 다시 로드하기 위한 세부 사항을 확인합니다.

a. **Save the running configuration at the time of reload** 라디오 버튼(기본값)을 클릭합니다.

b. 다시 로드할 시간(예: 기본값인 **Now**)을 선택합니다.

c. **Schedule Reload**를 클릭합니다.

다시 로드하는 과정이 진행되면 Reload Status 창이 나타나 다시 로드하는 작업이 수행되고 있음을 알립니다. ASDM 종료 옵션도 제공됩니다.

장애 조치 그룹이 Preempt Enabled로 구성된 경우, 우선적 지연 시간이 지나면 지정된 유닛에서 자동으로 활성 상태가 됩니다. 장애 조치 그룹이 Preempt Enabled로 구성되지 않은 경우 **Monitoring > Failover > Failover Group #** 창을 사용하여 지정된 유닛에서 활성 상태로 되돌릴 수 있습니다.

ASA 클러스터 업그레이드

ASA 클러스터의 모든 유닛을 업그레이드하려면 마스터 유닛에서 다음 단계를 수행합니다. 다중 상황 모드에서는 시스템 실행 영역에서 이 단계를 수행합니다.

절차

1단계 마스터 유닛에서 ASDM을 실행합니다.

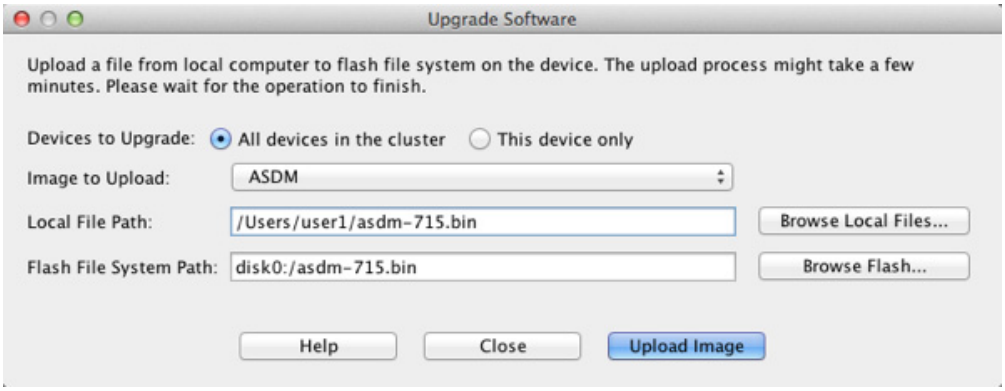
2단계 (컨피그레이션 마이그레이션이 있는 경우) ASDM에서 **Tools > Backup Configurations** 툴을 사용하여 기존 컨피그레이션을 백업합니다.

3단계 기본 ASDM 애플리케이션 창에서 **Tools > Upgrade Software from Local Computer**를 선택합니다.

Upgrade Software from Local Computer 대화 상자가 나타납니다.

4단계 **All devices in the cluster** 라디오 버튼을 클릭합니다.

Upgrade Software 대화 상자가 나타납니다.



5단계 Image to Upload 드롭다운 목록에서 **ASDM**을 선택합니다.

6단계 Local File Path 필드에 컴퓨터에 있는 파일의 로컬 경로를 입력하거나 **Browse Local Files**를 클릭하여 PC의 파일을 찾습니다.

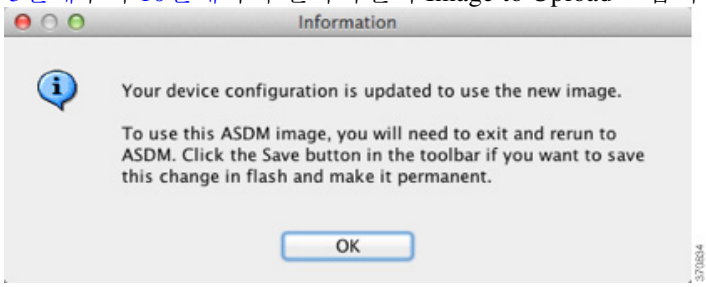
7단계 Flash File System Path 필드에 플래시 파일 시스템의 경로를 입력하거나 **Browse Flash**를 클릭하여 플래시 파일 시스템의 디렉토리 또는 파일을 찾습니다.

8단계 **Upload Image**를 클릭합니다. 업로드 프로세스에 몇 분이 걸릴 수 있습니다.

9단계 이 이미지를 ASDM 이미지로 설정할지 묻습니다. **Yes**를 클릭합니다.

10단계 ASDM을 종료하고 컨피그레이션을 저장하라는 메시지가 다시 표시됩니다. **OK**를 클릭합니다. Upgrade 툴을 종료합니다. **참고:** ASA 소프트웨어를 업그레이드한 *다음* 컨피그레이션을 저장하고 ASDM을 다시 로드합니다.

11단계 3단계부터 10단계까지 반복하면서 Image to Upload 드롭다운 목록에서 **ASA**를 선택합니다.

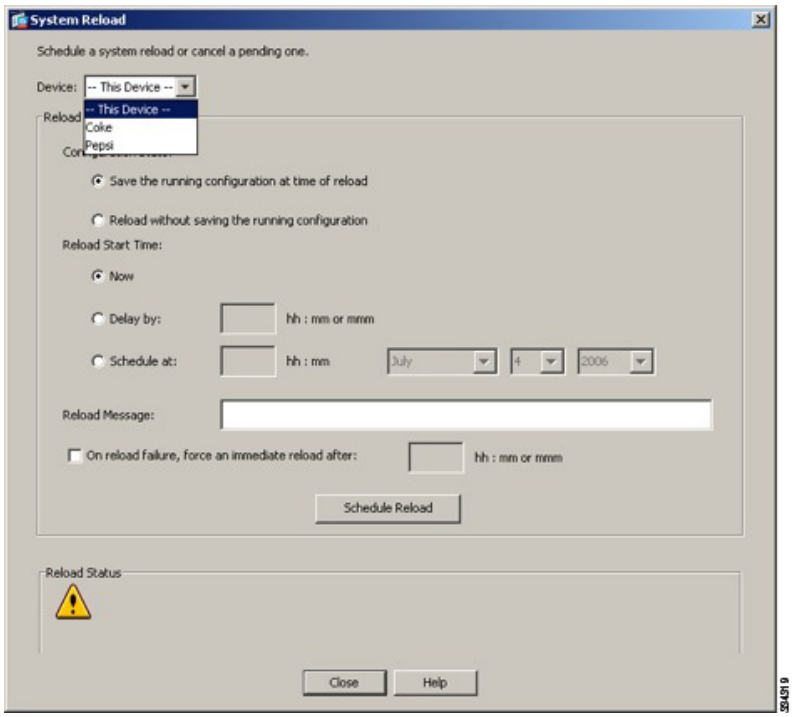


12단계 도구 모음에서 **Save** 아이콘을 클릭하여 컨피그레이션 변경 사항을 저장합니다.

13단계 **Tools > System Reload**를 선택합니다.

System Reload 대화 상자가 나타납니다.

14단계 Device 드롭다운 목록에서 슬레이브 유닛 이름을 선택하고 **Schedule Reload**를 클릭하여 지금 유닛을 다시 로드하면서 한 번에 하나씩 슬레이브 유닛을 다시 로드합니다.



연결 손실을 방지하고 트래픽이 안정화될 수 있도록 각 유닛이 다시 시작할 때까지 기다렸다가(약 5분) 다음 유닛을 다시 로드합니다. 유닛이 언제 클러스터에 다시 합류하는지 보려면 Monitoring > ASA Cluster > Cluster Summary 창을 확인합니다.

15단계 모든 슬레이브 유닛이 다시 로드된 다음 **Configuration > Device Management > High Availability and Scalability > ASA Cluster**를 선택하여 마스터 유닛의 클러스터링을 비활성화하고 **Participate in ASA cluster** 확인란을 선택 취소한 다음 **Apply**를 클릭합니다.

새 마스터가 선택되고 트래픽이 안정화될 때까지 5분가량 기다립니다. 이전의 마스터 유닛은 다시 클러스터에 합류하면 슬레이브가 됩니다.

컨피그레이션을 저장하지 마십시오. 마스터 유닛이 다시 로드될 때 그 유닛에서 클러스터링이 활성화되어야 합니다.

16단계 **Tools > System Reload**를 선택하고 System Reload 대화 상자의 Device 드롭다운 목록에서 **--This Device--**를 선택하여 마스터 유닛을 다시 로드합니다.

17단계 ASDM을 종료하고 다시 시작합니다. 새 마스터 유닛에 다시 연결됩니다.

파일 관리

ASDM에서는 기본적인 파일 관리 작업을 지원하기 위해 여러 파일 관리 툴을 제공합니다. File Management 툴을 사용하여 플래시 메모리에 저장된 파일을 조회, 이동, 복사, 삭제하고 파일을 전송하고 원격 스토리지 디바이스(탑재 지점)의 파일을 관리할 수 있습니다.

참고 다중 상황 모드에서는 시스템 보안 상황에서만 이 툴을 사용할 수 있습니다.

파일 액세스 구성

FTP 클라이언트 모드 구성

ASA에서는 FTP를 사용하여 FTP 서버에 이미지 파일이나 컨피그레이션 파일을 업로드하거나 FTP 서버로부터 다운로드할 수 있습니다. 패시브 FTP에서는 클라이언트가 제어 연결과 데이터 연결을 모두 시작합니다. 패시브 모드에서 데이터 연결의 수신자가 되는 서버는 해당 연결을 수신하는 포트의 번호를 알려주며 응답합니다.

세부 단계

1단계 Configuration > Device Management > Management Access > File Access > FTP Client 창에서 **Specify FTP mode as passive** 확인란을 선택합니다.

2단계 **Apply**를 클릭합니다.

FTP 클라이언트 컨피그레이션이 변경되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

ASA를 SCP 서버로 구성

ASA에서 SCP(Secure Copy) 서버를 활성화할 수 있습니다. SSH를 사용하여 ASA에 액세스하는 것이 허용된 클라이언트만 SCP 연결을 설정할 수 있습니다.

제한 사항

- 이 서버에서는 디렉토리가 지원되지 않습니다. 디렉토리가 지원되지 않으므로 ASA 내부 파일에 대한 원격 클라이언트 액세스가 제한됩니다.
- 이 서버는 배너를 지원하지 않습니다.
- 이 서버는 와일드카드를 지원하지 않습니다.

전제 조건

- ASA에서 36-3 페이지의 관리 액세스 구성에 따라 SSH를 설정합니다.
- ASA 라이센스에 강력한 암호화(3DES/AES) 라이센스가 있어야 SSH 버전 2 연결을 지원할 수 있습니다.

세부 단계

1단계 **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server**를 선택하고 **Enable secure copy server** 확인란을 선택합니다.

2단계 **Apply**를 클릭합니다.

예

외부 호스트의 클라이언트에서 SCP 파일 전송을 수행합니다. 예를 들어, Linux에서는 다음 명령을 입력합니다.

```
scp -v -pw password source_filename username@asa_address:{disk0|disk1}:/dest_filename
```

-v는 상세 표시를 의미하며, **-pw**가 지정되지 않은 경우 비밀번호를 입력해야 합니다.

ASA SCP 클라이언트 사용자 지정

온보드 SCP 클라이언트를 사용하여 ASA에 파일을 복사하거나 복사해 올 수 있습니다 37-17 페이지의 File Management 툴 액세스 참조). 이 섹션에서는 SCP 클라이언트 작업을 사용자 지정할 수 있습니다.

전제 조건

다중 상황 모드에서는 시스템 실행 영역에서 이 절차를 완료합니다. 아직 System 컨피그레이션 모드가 아닐 경우 Configuration > Device List 창에서 활성 디바이스 IP 주소 아래의 **System**을 두 번 클릭합니다.

세부 단계

1단계 상황 모드에 따라

- 단일 모드는 **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP)**를 선택합니다.
- System의 다중 모드는 **Configuration > Device Management > Device Administration > Secure Copy**를 선택합니다.

2단계 ASA에서는 연결되는 각 SCP 서버의 SSH 호스트 키를 저장합니다. 원한다면 ASA 데이터베이스에서 직접 서버와 키를 추가하거나 삭제할 수 있습니다.

키를 추가하려면

a. 새 서버를 위해 **Add**를 클릭하거나 Trusted SSH Hosts 테이블에서 서버를 선택하고 **Edit**를 클릭합니다.

b. 새 서버인 경우 Host 필드에 서버 IP 주소를 입력합니다.

c. **Add public key for the trusted SSH host** 확인란을 선택합니다.

d. 다음 키 중 하나를 지정합니다.

   – Fingerprint—이미 해시된 키를 입력합니다. 이를테면 **show** 명령 출력에서 복사한 키입니다.

– Key—SSH 호스트의 공개 키 또는 해시된 값을 입력합니다. key string은 원격 피어의 Base64 인코딩 RSA 공개 키입니다. 열린 SSH 클라이언트에서, 즉 .ssh/id_rsa.pub 파일에서 공개 키 값을 얻을 수 있습니다. Base64 인코딩 공개 키를 전송하면 그 키가 SHA-256을 통해 해시됩니다.

키를 삭제하려면

a. Trusted SSH Hosts 테이블에서 서버를 선택하고 **Delete**를 클릭합니다.

3단계 새 호스트 키가 탐지되었을 때 이를 알리게 하려면 **Inform me when a new host key is detected** 확인란을 선택합니다.

기본적으로 이 옵션은 활성화되어 있습니다. 이 옵션이 활성화된 경우, 호스트 키가 아직 ASA에 저장되지 않았다면 호스트 키를 승인하거나 거부하라는 메시지가 나타납니다. 이 옵션이 비활성화된 경우, 호스트 키가 아직 저장되지 않았다면 ASA는 자동으로 호스트 키를 승인합니다.

4단계 **Apply**를 클릭합니다.

ASA TFTP 클라이언트 경로 구성

TFTP는 단일 클라이언트/서버 파일 전송 프로토콜이며, RFC 783 및 RFC 1350 Rev에 기술되어 있습니다. 2. ASA를 TFTP *클라이언트*로 구성하여 TFTP *서버*에 파일을 복사하거나 복사해 오도록 할 수 있습니다(37-18 페이지의 파일 전송 참조). 이와 같은 방법으로 컨피그레이션 파일을 백업하여 여러 ASA에 배포할 수 있습니다.

이 섹션에서는 TFTP 서버의 경로를 미리 정의하는 방법을 알아봅니다. 그러면 **copy**, **configure net**과 같은 명령에서 그 경로를 입력하지 않아도 됩니다.

세부 단계

1단계 **Configuration > Device Management > Management Access > File Access > TFTP Client**를 선택하고 **Enable** 확인란을 선택합니다.

2단계 Interface Name 드롭다운 목록에서 TFTP 클라이언트로 사용할 인터페이스를 선택합니다.

3단계 IP Address 필드에 컨피그레이션 파일이 저장될 TFTP 서버의 IP 주소를 입력합니다.

4단계 Path 필드에 컨피그레이션 파일이 저장된 TFTP 서버의 경로를 입력합니다.

예: **/tftpboot/asa/config3**

5단계 **Apply**를 클릭합니다.

탑재 지점 추가

- 37-16 페이지의 CIFS 탑재 지점 추가
- 37-16 페이지의 FTP 탑재 지점 추가

CIFS 탑재 지점 추가

CIFS(Common Internet File System) 탑재 지점을 정의하려면 다음 단계를 수행합니다.

1단계 **Configuration > Device Management > Management Access > File Access > Mount-Points**를 선택하고 **Add > CIFS Mount Point**를 클릭합니다.

Add CIFS Mount Point 대화 상자가 나타납니다.

2단계 **Enable mount point** 확인란을 선택합니다.

이 옵션은 ASA의 CIFS 파일 시스템을 UNIX 파일 트리에 추가합니다.

3단계 Mount Point Name 필드에 기존 CIFS 위치의 이름을 입력합니다.

4단계 Server Name 또는 IP Address 필드에 탑재 지점이 위치하는 서버의 이름이나 IP 주소를 입력합니다.

5단계 Share Name 필드에 CIFS 서버의 폴더 이름을 입력합니다.

6단계 NT Domain Name 필드에 서버가 상주하는 NT 도메인의 이름을 입력합니다.

7단계 User Name 필드에는 서버에 탑재되는 파일 시스템을 사용하도록 승인받은 사용자의 이름을 입력합니다.

8단계 Password 필드에는 서버에 탑재되는 파일 시스템을 사용하도록 승인받은 사용자의 비밀번호를 입력합니다.

9단계 Confirm Password 필드에 비밀번호를 다시 입력합니다.

10단계 **OK**를 클릭합니다.

Add CIFS Mount Point 대화 상자가 닫힙니다.

11단계 **Apply**를 클릭합니다.

FTP 탑재 지점 추가

참고 FTP 탑재 지점의 경우 FTP 서버가 UNIX 디렉토리 목록 스타일을 가져야 합니다. Microsoft FTP 서버는 기본적으로 MS-DOS 디렉토리 목록 스타일입니다.

1단계 **Configuration > Device Management > Management Access > File Access > Mount-Points**를 선택하고 **Add > FTP Mount Point**를 클릭합니다.

Add FTP Mount Point 대화 상자가 나타납니다.

2단계 **Enable** 확인란을 선택합니다.

이 옵션은 ASA의 FTP 파일 시스템을 UNIX 파일 트리에 추가합니다.

3단계 Mount Point Name 필드에 기존 FTP 위치의 이름을 입력합니다.

4단계 Server Name 또는 IP Address 필드에 탑재 지점이 위치하는 서버의 이름이나 IP 주소를 입력합니다.

5단계 Mode 필드에서는 FTP 모드(**Active** 또는 **Passive**)의 라디오 버튼을 클릭합니다. Passive 모드를 선택하면 클라이언트는 FTP 제어 연결과 데이터 연결을 모두 시작합니다. 서버는 이 연결의 수신 포트 번호를 알려주며 응답합니다.

6단계 Path to Mount 필드에 FTP 파일 서버의 디렉토리 경로 이름을 입력합니다.

7단계 User Name 필드에는 서버에 탑재되는 파일 시스템을 사용하도록 승인받은 사용자의 이름을 입력합니다.

8단계 Password 필드에는 서버에 탑재되는 파일 시스템을 사용하도록 승인받은 사용자의 비밀번호를 입력합니다.

9단계 Confirm Password 필드에 비밀번호를 다시 입력합니다.

10단계 **OK**를 클릭합니다.

Add FTP Mount Point 대화 상자가 닫힙니다.

11단계 **Apply**를 클릭합니다.

File Management 툴 액세스

File Management 툴을 사용하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 애플리케이션 창에서 **Tools > File Management**를 선택합니다.

File Management 대화 상자가 나타납니다.

- Folders 창에 디스크에서 사용 가능한 폴더가 표시됩니다.
- Flash Space는 플래시 메모리의 총량과 사용 가능한 메모리의 양을 보여줍니다.
- Files 영역은 선택된 폴더의 파일에 대한 다음 정보를 표시합니다.
  - 경로
  - 파일 이름
  - 크기(바이트)
  - 수정된 시간
  - 상태 - 선택된 파일이 부트 컨피그레이션 파일, 부트 이미지 파일, ASDM 이미지 파일, SVC 이미지 파일, CSD 이미지 파일 또는 APCF 이미지 파일로 지정되었는지 나타냅니다.

2단계 선택된 파일을 브라우저에서 보려면 **View**를 클릭합니다.

3단계 선택된 파일을 잘라내어 다른 디렉토리에 붙여넣으려면 **Cut**을 클릭합니다.

4단계 선택된 파일을 복사하여 다른 디렉토리에 붙여넣으려면 **Copy**를 클릭합니다.

5단계 복사한 파일을 선택된 위치에 붙여넣으려면 **Paste**를 클릭합니다.

6단계 선택된 파일을 플래시 메모리에서 삭제하려면 **Delete**를 클릭합니다.

7단계 파일의 이름을 바꾸려면 **Rename**을 클릭합니다.

8단계 파일을 저장할 새 디렉토리를 만들려면 **New Directory**를 클릭합니다.

9단계 File Transfer 대화 상자를 열려면 **File Transfer**를 클릭합니다. 자세한 내용은 37-18 페이지의 파일 전송를 참조하십시오.

10단계 Manage Mount Points 대화 상자를 열려면 **Mount Points**를 클릭합니다. 자세한 내용은 37-15 페이지의 탑재 지점 추가 를 참조하십시오.

파일 전송

File Transfer 툴을 사용하면 로컬 위치 또는 원격 위치에 있는 파일을 전송할 수 있습니다. 컴퓨터나 플래시 파일 시스템에 있는 로컬 파일을 ASA에 전송하거나 반대로 전송받을 수 있습니다. HTTP, HTTPS, TFTP, FTP 또는 SMB를 사용하여 ASA에 원격 파일을 전송하거나 반대로 전송받을 수 있습니다.

참고 IPS SSP 소프트웨어 모듈의 경우, disk0에 IPS 소프트웨어를 다운로드하기 전에 플래시 메모리의 50% 이상이 비어 있는지 확인합니다. IPS를 설치할 때 IPS는 내부 플래시 메모리의 50%를 파일 시스템용으로 예약합니다.

- 37-18 페이지의 로컬 PC와 플래시 간의 파일 전송
- 37-18 페이지의 원격 서버와 플래시 간의 파일 전송

로컬 PC와 플래시 간의 파일 전송

로컬 컴퓨터와 플래시 파일 시스템이 서로 파일을 전송하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 애플리케이션 창에서 **Tools > File Management**를 선택합니다.

File Management 대화 상자가 나타납니다.

2단계 **File Transfer** 옆의 아래쪽 화살표를 클릭하고 **Between Local PC and Flash**를 클릭합니다.

File Transfer 대화 상자가 나타납니다.

3단계 업로드하거나 다운로드할 로컬 컴퓨터 또는 플래시 파일 시스템에서 파일을 선택하여 원하는 위치로 *끕니다*. 또는 업로드하거나 다운로드할 로컬 컴퓨터 또는 플래시 파일 시스템에서 파일을 선택하고 오른쪽 또는 왼쪽 화살표를 클릭하여 원하는 위치로 파일을 전송합니다.

4단계 완료하면 **Close**를 클릭합니다.

원격 서버와 플래시 간의 파일 전송

원격 서버와 플래시 파일 시스템이 서로 파일을 전송하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 애플리케이션 창에서 **Tools > File Management**를 선택합니다.

File Management 대화 상자가 나타납니다.

2단계 File Transfer 드롭다운 목록에서 아래쪽 화살표를 클릭하고 **Between Remote Server and Flash**를 클릭합니다.

File Transfer 대화 상자가 나타납니다.

3단계 원격 서버로부터 파일을 전송하려면 **Remote server** 옵션을 클릭합니다.

4단계 전송할 소스 파일을 정의합니다.

a. 파일 위치에 대한 경로를 서버의 IP 주소까지 포함하여 선택합니다.

참고 파일 전송에서는 IPv4 주소와 IPv6 주소를 지원합니다.

b. 원격 서버의 유형(경로가 FTP인 경우) 또는 포트 번호(경로가 HTTP 또는 HTTPS인 경우)를 입력합니다. 유효한 FTP 유형은 다음과 같습니다.
   - ap—패시브 모드의 ASCII 파일
   - an—비 패시브 모드의 ASCII 파일
   - ip—패시브 모드의 이진 아미지 파일
   - in—비 패시브 모드의 이진 이미지 파일

5단계 플래시 파일 시스템으로부터 파일을 전송하려면 **Flash file system** 옵션을 클릭합니다.

6단계 파일 위치의 경로를 입력하거나 **Browse Flash**를 클릭하여 파일 위치를 찾습니다.

7단계 또한 CLI를 사용하여 시작 컨피그레이션, 실행 중인 컨피그레이션 또는 SMB 파일 시스템의 파일을 복사할 수 있습니다. **copy** 명령 사용에 대한 지침은 CLI 컨피그레이션 가이드를 참조하십시오.

8단계 전송될 파일의 목적지를 정의합니다.

a. 플래시 파일 시스템으로 파일을 전송하려면 **Flash file system** 옵션을 선택합니다.

b. 파일 위치의 경로를 입력하거나 **Browse Flash**를 클릭하여 파일 위치를 찾습니다.

9단계 원격 서버로 파일을 전송하려면 **Remote server** 옵션을 선택합니다.

a. 파일 위치의 경로를 입력합니다.

b. FTP 전송의 경우 유형을 입력합니다. 유효한 유형은 다음과 같습니다.
   - ap—패시브 모드의 ASCII 파일
   - an—비 패시브 모드의 ASCII 파일
   - ip—패시브 모드의 이진 아미지 파일
   - in—비 패시브 모드의 이진 이미지 파일

10단계 **Transfer**를 클릭하여 파일 전송을 시작합니다.

Enter Username and Password 대화 상자가 나타납니다.

11단계 원격 서버의 사용자 이름, 비밀번호, 도메인(필요한 경우)을 입력합니다.

12단계 **OK**를 클릭하여 파일 전송을 진행합니다.

파일 전송 프로세스에 몇 분가량 걸릴 수 있습니다. 끝날 때까지 기다려야 합니다.

13단계 파일 전송이 끝나면 **Close**를 클릭합니다.

사용할 이미지 및 시작 구성 설정

둘 이상의 ASA 또는 ASDM 이미지가 있을 경우 부팅할 이미지를 지정해야 합니다. 이미지를 설정하지 않은 경우 기본 부트 이미지가 사용되는데, 원하는 이미지가 아닐 수 있습니다. 시작 컨피그레이션에서는 선택 사항으로 컨피그레이션 파일을 지정할 수 있습니다.

기본 설정

ASA 이미지

- Physical ASA—내부 플래시 메모리에서 발견한 첫 번째 애플리케이션 이미지를 부팅합니다.
- ASAv—최초로 구축했을 때 생성한 읽기 전용 boot:/ 파티션의 이미지를 부팅합니다. 플래시 메모리의 이미지를 업그레이드하고 그 이미지에서 부팅할 ASAv를 구성할 수 있습니다. 나중에 컨피그레이션을 지울 경우, ASAv는 원래로 돌아가 최초의 구축 이미지를 로드합니다.

ASDM 이미지

All ASAs—내부 플래시 메모리에서 발견한 첫 번째 ASDM 이미지를 부팅합니다. 내부 플래시 메모리에 없을 경우 외부 플래시 메모리의 첫 번째 ASDM 이미지를 부팅합니다.

시작 구성

기본적으로 ASA는 숨겨진 파일인 시작 컨피그레이션으로부터 부팅합니다.

세부 단계

1단계 **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration**을 선택합니다.

시작 이미지로 사용할 최대 4개의 로컬 이진 이미지 파일을 지정하고, 디바이스가 부팅할 TFTP 서버에 위치한 하나의 이미지를 지정할 수 있습니다. TFTP 서버에 위치한 이미지를 지정한 경우 이 이미지가 목록의 첫 번째가 되어야 합니다. 디바이스는 이미지를 로드하기 위해 TFTP 서버에 연결할 수 없는 경우, 플래시에 위치한 목록의 다음 이미지 파일을 로드하려 합니다.

2단계 Boot Image/Configuration 창에서 **Add**를 클릭합니다.

3단계 부팅할 이미지를 찾습니다. TFTP 이미지의 경우, File Name 필드에 TFTP URL을 입력합니다. **OK**를 클릭합니다.

4단계 Move Up 및 Move Down 버튼을 사용하여 이미지를 순서대로 정렬합니다.

5단계 (선택 사항) Boot Configuration File Path 필드에서 **Browse Flash**를 클릭하고 컨피그레이션을 선택하여 시작 컨피그레이션 파일을 지정합니다. **OK**를 클릭합니다.

6단계 ASDM Image File Path 필드에서 **Browse Flash**를 클릭하고 ASDM 이미지를 선택하여 지정합니다. **OK**를 클릭합니다.

7단계 **Apply**를 클릭합니다.

구성 또는 기타 파일 백업 및 복원

Tools 메뉴의 Backup and Restore 옵션을 사용하여 ASA의 실행 중인 컨피그레이션, 시작 컨피그레이션, 설치된 애드온 이미지, SSL VPN 클라이언트 이미지와 프로필을 백업하고 복원할 수 있습니다.

ASDM의 Backup Configurations 화면에서는 백업할 파일 유형을 선택할 수 있으며, 이를 단일 zip 파일로 압축한 다음 컴퓨터에서 선택한 디렉토리로 전송합니다. 파일을 복원할 때도 컴퓨터에서 소스 zip 파일을 선택한 다음 복원할 파일 형식을 선택합니다.

- 37-24 페이지의 로컬 CA 서버 백업
- 37-24 페이지의 로컬 CA 서버 백업
- 37-25 페이지의 실행 중인 구성을 TFTP 서버에 저장

전체 시스템 백업 또는 복원 수행

이 절차에서는 컨피그레이션과 이미지를 zip 파일로 백업 및 복원하고 로컬 컴퓨터에 전송하는 방법을 설명합니다.

- 37-21 페이지의 시작하기 전에
- 37-22 페이지의 시스템 백업
- 37-23 페이지의 백업 복원

시작하기 전에

- ASA는 단일 상황 모드여야 합니다.
- 백업 중에 또는 백업 후에 컨피그레이션을 변경할 경우, 이 변경 사항은 백업에 포함되지 않습니다. 백업한 후 컨피그레이션을 변경한 다음 복원을 수행할 경우, 이 컨피그레이션 변경 사항은 덮어쓰기됩니다. 따라서 ASA가 다르게 작동할 수 있습니다.
- 한 번에 하나의 백업 또는 복원만 시작할 수 있습니다.
- 최초의 백업을 수행했을 때와 동일한 ASA 버전에만 컨피그레이션을 복원할 수 있습니다. 복원 툴을 사용하여 어떤 ASA 버전의 컨피그레이션을 다른 버전으로 마이그레이션할 수 없습니다. 컨피그레이션 마이그레이션이 필요할 경우, ASA에서는 새 ASA OS를 로드할 때 상주하는 시작 컨피그레이션을 자동으로 업그레이드합니다.
- 클러스터링을 사용할 경우, 마스터 유닛의 시작 컨피그레이션, 실행 중인 컨피그레이션, ID 인증서만 백업하거나 복원할 수 있습니다.
- 장애 조치를 사용할 경우, 활성 유닛과 대기 유닛의 백업을 따로 생성하고 복원해야 합니다.
- ASA에 대해 마스터 패스프레이즈를 설정한 경우, 이 절차로 생성한 백업 컨피그레이션을 복원하는 데 마스터 패스프레이즈가 필요합니다. ASA의 마스터 패스프레이즈를 모를 경우, 백업을 진행하기 전에 14-8 페이지의 마스터 패스프레이즈 구성에서 재설정 방법을 확인하십시오.
- PKCS12 데이터를 가져왔고(**crypto ca trustpoint** 명령 사용) 신뢰 지점에서 RSA 키를 사용할 경우, 가져온 키 쌍에는 신뢰 지점과 동일한 이름이 지정됩니다. 이러한 제한 때문에 ASDM 컨피그레이션을 복원한 다음 신뢰 지점과 그 키 쌍의 이름을 다르게 지정할 경우, 시작 컨피그레이션은 원래의 컨피그레이션과 동일하지만 실행 중인 컨피그레이션은 다른 키 쌍 이름을 가지게 됩니다. 따라서 키 쌍과 신뢰 지점에 서로 다른 이름을 사용하는 경우 원래의 컨피그레이션을 복원할 수 없습니다. 이 문제를 해결하려면 신뢰 지점과 그 키 쌍에 동일한 이름을 사용해야 합니다.
- 각 백업 파일에는 다음 내용이 들어 있습니다.
  - 실행 중인 컨피그레이션
  - 시작 컨피그레이션
  - 모든 보안 이미지

    Cisco Secure Desktop & Host Scan 이미지

    Cisco Secure Desktop & Host Scan 설정

    AnyConnect(SVC) 클라이언트 이미지 및 프로필

    AnyConnect(SVC) 사용자 지정 및 변환
  - ID 인증서(ID 인증서와 연결된 RSA 키 쌍 포함, 독립형 키는 제외)
  - VPN 사전 공유 키
  - SSL VPN 컨피그레이션
  - APCF(Application Profile Custom Framework)
  - 북마크
  - 사용자 지정 설정
  - DAP(동적 액세스 정책)
  - 플러그인
  - 미리 채워진 연결 프로필 스크립트
  - 프록시 자동 구성

- 변환 테이블
- 웹 콘텐츠
- 버전 정보

시스템 백업

이 절차에서는 전체 시스템 백업을 수행하는 방법을 설명합니다.

절차

1단계 백업 파일을 저장할 폴더를 컴퓨터에 만듭니다. 그러면 나중에 복원해야 할 때 쉽게 찾을 수 있습니다.

2단계 **Tools > Backup Configurations**를 선택합니다.

Backup Configurations 대화 상자가 나타납니다. **SSL VPN Configuration** 영역에서 아래쪽 화살표를 클릭하여 SSL VPN 컨피그레이션의 옵션을 표시합니다. 기본적으로 모든 컨피그레이션 파일이 선택되어 있으며, 사용 가능한 경우 백업됩니다. 목록의 모든 파일을 백업하려면 5단계단계로 진행합니다.

3단계 백업할 컨피그레이션을 선택하려면 **Backup All** 확인란을 선택 취소합니다.

4단계 백업할 옵션 옆의 확인란을 선택합니다.

5단계 **Browse Local**을 클릭하여 backup .zip 파일의 디렉토리 및 파일 이름을 지정합니다.

6단계 Select 대화 상자에서 백업 파일을 저장할 디렉토리를 선택합니다.

7단계 **Select**를 클릭합니다. 경로가 Backup File 필드에 나타납니다.

8단계 디렉토리 경로 다음에 대상 백업 파일의 이름을 입력합니다. 백업 파일 이름의 길이는 3자~232자여야 합니다.

9단계 **Backup**을 클릭합니다. 인증서를 백업하거나 ASA에서 마스터 패스프레이즈를 사용하는 경우를 제외하고 백업이 즉시 진행됩니다.

10단계 ASA에 마스터 패스프레이즈를 구성하고 활성화한 경우, 백업을 진행하기 전에 경고 메시지가 나타나 마스터 패스프레이즈를 모른다면 이를 변경할 수 있음을 알려줍니다. 마스터 패스프레이즈를 알고 있다면 **Yes**를 클릭하여 백업을 진행합니다. ID 인증서를 백업하는 경우를 제외하고 백업이 즉시 진행됩니다.

11단계 ID 인증서를 백업하는 경우, 인증서 인코딩에 사용할 별도의 패스프레이즈를 PKCS12 형식으로 입력하라는 메시지가 나타납니다. 패스프레이즈를 입력하거나 이 단계를 건너뛸 수 있습니다.

참고 ID 인증서는 이 프로세스를 통해 백업됩니다. 그러나 CA 인증서는 백업되지 않습니다. CA 인증서 백업에 대한 지침은 37-24 페이지의 로컬 CA 서버 백업를 참조하십시오.

- 인증서를 해독하려면 Certificate Passphrase 대화 상자에 인증서 패스프레이즈를 입력하고 확인한 다음 **OK**를 클릭합니다. 인증서를 복원할 때 이 대화 상자에 입력한 비밀번호를 기억해야 합니다.
- **Cancel**을 클릭하면 이 단계를 건너뛰며 인증서를 백업하지 않습니다.

OK또는 Cancel을 클릭하면 백업이 즉시 시작합니다.

12단계 백업이 완료되면 상태 창이 닫히고 Backup Statistics 대화 상자가 나타나 성공 및 실패 메시지를 제공합니다.

참고 백업 "실패 메시지"는 대개 지정된 유형에 대한 컨피그레이션이 없기 때문에 발생합니다.

13단계 **OK**를 클릭하여 Backup Statistics 대화 상자를 닫습니다.

백업 복원

로컬 컴퓨터에 있는 zip 파일에서 복원할 컨피그레이션과 이미지를 지정할 수 있습니다.

절차

1단계 **Tools > Restore Configurations**를 선택합니다.

2단계 Restore Configurations 대화 상자에서 **Browse Local Directory**를 클릭합니다. 복원할 컨피그레이션이 들어 있는 zip 파일을 로컬 컴퓨터에서 선택하고 **Select**를 클릭합니다. 경로 및 zip 파일 이름이 **Local File** 필드에 나타납니다.

복원할 zip 파일은 **Tools > Backup Configurations** 옵션을 선택하여 만들어야 합니다.

3단계 **Next**를 클릭합니다. 두 번째 Restore Configuration 대화 상자가 나타납니다. 복원하려는 컨피그레이션 옆의 확인란을 선택합니다. 사용 가능한 모든 SSL VPN 컨피그레이션이 기본적으로 선택됩니다.

4단계 **Restore**를 클릭합니다.

5단계 백업 파일을 만들 때 인증서 해독에 사용할 인증서 패스프레이즈를 지정한 경우, ASDM은 패스프레이즈 입력 화면을 표시합니다.

6단계 실행 중인 컨피그레이션을 복원하도록 선택한 경우 실행 중인 컨피그레이션을 병합할지, 실행 중인 컨피그레이션을 대체할지 또는 복원 프로세스의 이 단계를 건너뛸지 묻습니다.

- 컨피그레이션을 병합하면 현재 실행 중인 컨피그레이션과 백업된 실행 중 컨피그레이션이 합쳐집니다.
- 실행 중인 컨피그레이션을 대체하면 백업된 실행 중 컨피그레이션만 사용합니다.
- 이 단계를 건너뛰면 백업된 실행 중 컨피그레이션은 복원하지 않습니다.

ASDM은 복원 작업이 끝날 때까지 상태 대화 상자를 표시합니다.

7단계 실행 중인 컨피그레이션을 대체했거나 병합한 경우 ASDM을 닫고 다시 시작합니다. 실행 중인 컨피그레이션을 복원하지 않은 경우 ASDM 세션을 새로 고치면 변경 사항이 적용됩니다.

로컬 CA 서버 백업

ASDM 백업을 수행할 때 로컬 CA 서버 데이터베이스는 포함하지 않습니다. 즉 이 서버에 저장된 CA 인증서는 백업하지 않습니다. 로컬 CA 서버를 백업하려면 ASA CLI에서 다음 수동 프로세스를 수행합니다.

1단계 **show run crypto ca server** 명령을 입력합니다.

```
crypto ca server
 keysize server 2048
 subject-name-default OU=aa,O=Cisco,ST=ca,
 issuer-name CN=xxx,OU=yyy,O=Cisco,L=Bxb,St=Mass
 smtp from-address abcd@cisco.com
 publish-crl inside 80
 publish-crl outside 80
```

2단계 **crypto ca import** 명령을 사용하여 로컬 CA PKCS12 파일을 가져와 LOCAL-CA-SERVER 신뢰 지점을 만들고 키 쌍을 복원합니다.

```
crypto ca import LOCAL-CA-SERVER pkcs12 <passphrase> (paste the pkcs12
base64 data here)
```

참고 이 단계에서 정확한 이름 “LOCAL-CA-SERVER”를 사용해야 합니다.

3단계 LOCAL-CA-SERVER 디렉토리가 없으면 **mkdir LOCAL-CA-SERVER**를 입력하여 만들어야 합니다.

4단계 로컬 CA 파일을 LOCAL-CA-SERVER 디렉토리에 복사합니다.

```
copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.ser
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.cdb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.udb
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.crl
disk0:/LOCAL-CA-SERVER/

copy ftp://10.10.1.1/CA-backup/LOCAL-CA-SERVER.p12
disk0:/LOCAL-CA-SERVER/
```

5단계 **crypto ca server** 명령을 입력하여 로컬 CA 서버를 활성화합니다.

```
crypto ca server
 no shutdown
```

6단계 **show crypto ca server** 명령을 입력하여 로컬 CA 서버가 실행 중인지 확인합니다.

7단계 컨피그레이션을 저장합니다.

실행 중인 구성을 TFTP 서버에 저장

이 기능은 현재 실행 중인 컨피그레이션 파일의 사본을 TFTP 서버에 저장합니다.

실행 중인 컨피그레이션을 TFTP 서버에 저장하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 애플리케이션 창에서 **File > Save Running Configuration to TFTP Server**를 선택합니다.

Save Running Configuration to TFTP Server 대화 상자가 나타납니다.

2단계 TFTP 서버 IP 주소와 TFTP 서버에서 컨피그레이션 파일이 저장될 파일 경로를 입력하고 **Save Configuration**을 클릭합니다.

참고 기본 TFTP 설정을 구성하려면 **Configuration > Device Management > Management Access > File Access > TFTP Client**를 선택합니다. 이 설정을 구성하면 TFTP 서버 IP 주소와 TFTP 서버상의 파일 경로가 이 대화 상자에 자동으로 나타납니다.

시스템 재시작 예약

System Reload 툴에서는 시스템 재시작을 예약하거나 보류 중인 재시작을 취소할 수 있습니다.

시스템 재시작을 예약하려면 다음 단계를 수행합니다.

1단계 기본 ASDM 애플리케이션 창에서 **Tools > System Reload**를 선택합니다.

2단계 Reload Scheduling 영역에서 다음 설정을 정의합니다.

a. Configuration State에서 재시작할 때 실행 중 컨피그레이션을 저장하거나 삭제하도록 선택합니다.

b. Reload Start Time은 다음 옵션 중에서 선택합니다.

- 즉시 재시작하려면 **Now**를 클릭합니다.
- 지정된 시간만큼 재시작을 늦추려면 **Delay by**를 클릭합니다. 재시작할 때까지의 지연 시간을 시간과 분 단위로 또는 분 단위로만 입력합니다.
- 특정 날짜와 시간에 재시작하도록 예약하려면 **Schedule at**을 클릭합니다. 재시작할 시간대를 입력하고 예약된 재시작의 날짜를 선택합니다.

c. Reload Message 필드에 재시작 시 열려 있는 ASDM의 인스턴스에 보낼 메시지를 입력합니다.

d. 재시작을 다시 시도할 때까지 경과한 시간을 시간과 분 단위로 또는 분 단위로만 표시하려면 **On reload failure force immediate reload after** 확인란을 선택합니다.

e. 구성된 대로 재시작을 예약하려면 **Schedule Reload**를 클릭합니다.

Reload Status 영역은 재시작의 상태를 표시합니다.

3단계 다음 중 하나를 선택합니다.

- 예약된 재시작을 중지하려면 **Cancel Reload**를 클릭합니다.
- 예약된 재시작이 끝난 후 Reload Status 화면을 새로 고치려면 **Refresh**를 클릭합니다.
- 예약된 재시작의 결과를 표시하려면 **Details**를 클릭합니다.

소프트웨어 다운그레이드

버전 8.3으로 다운그레이드할 때 컨피그레이션이 마이그레이션됩니다. 기존 컨피그레이션은 자동으로 플래시 메모리에 저장됩니다. 예를 들어, 버전 8.2(1)에서 8.3(1)로 업그레이드하면 기존 8.2(1) 컨피그레이션은 플래시 메모리에서 8_2_1_0_startup_cfg.sav라는 파일에 저장됩니다.

참고 다운그레이드하기 전에 직접 기존 컨피그레이션을 복원해야 합니다.

이 섹션에서는 다운그레이드 방법을 설명합니다.

- 37-26 페이지의 활성화 키 호환성 정보
- 37-26 페이지의 다운그레이드 수행

활성화 키 호환성 정보

임의의 이전 버전에서 최신 버전으로 업그레이드할 경우 활성화 키는 계속 호환 가능합니다. 그러나 다운그레이드 기능을 유지하려는 경우 문제가 생길 수 있습니다.

- 버전 8.1 이하로 다운그레이드—업그레이드한 다음 *8.2 이전*에 도입되었던 추가 기능 라이센스를 활성화한 경우, 다운그레이드하더라도 활성화 키는 계속 이전 버전과 호환 가능합니다. 그러나 버전 8.2 이상에서 도입되었던 기능 라이센스를 활성화할 경우, 활성화 키는 역호환성을 가지지 않습니다. 호환되지 않는 라이센스 키가 있다면 다음 지침을 참조하십시오.
  - 이전 버전에서 활성화 키를 입력한 적이 있는 경우, ASA에서는 (버전 8.2 이상에서 활성화했던 어떤 신규 라이센스도 포함하지 않고) 그 키를 사용합니다.
  - 신규 시스템이 있는데 이전의 활성화 키가 없을 경우, 그 이전 버전과 호환되는 새 활성화 키를 요청해야 합니다.
- 버전 8.2 이하로 다운그레이드—버전 8.3에서는 더 강력한 시간 기준 키 사용법과 장애 조치 라이센스 변경 사항이 도입되었습니다.
  - 둘 이상의 시간 기준 활성화 키가 활성 상태일 경우, 다운그레이드하면 가장 최근에 활성화된 시간 기준 키만 활성 상태가 됩니다. 그 밖의 모든 키는 비활성 상태가 됩니다.
  - 장애 조치 쌍에서 라이센스가 일치하지 않을 경우 다운그레이드하면 장애 조치가 불가능해집니다. 키가 일치하더라도 사용된 라이센스는 더 이상 통합 라이센스가 아닙니다.

다운그레이드 수행

컨피그레이션 마이그레이션에 대한 자세한 내용은 37-20 페이지의 Tools 메뉴의 Backup and Restore 옵션을 사용하여 ASA의 실행 중인 컨피그레이션, 시작 컨피그레이션, 설치된 애드온 이미지, SSL VPN 클라이언트 이미지와 프로필을 백업하고 복원할 수 있습니다.를 참조하십시오.

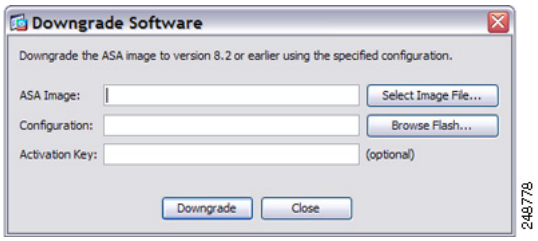
버전 8.3에서 다운그레이드하려면 다음 단계를 수행합니다.

세부 단계

1단계 **Tools > Downgrade Software**를 선택합니다.

Downgrade Software 대화 상자가 나타납니다.

그림 37-1 소프트웨어 다운그레이드



2단계 ASA Image에서 **Select Image File**을 클릭합니다.

Browse File Locations 대화 상자가 나타납니다.

3단계 다음 라디오 버튼 중 하나를 클릭합니다.

- **Remote Server**—드롭다운 목록에서 **ftp**, **smb** 또는 **http**를 선택하고 기존 이미지 파일의 경로를 입력합니다.
- **Flash File System**—**Browse Flash**를 클릭하여 로컬 플래시 파일 시스템에 있는 기존 이미지 파일을 선택합니다.

4단계 Configuration에서는 **Browse Flash**를 클릭하여 마이그레이션 이전 컨피그레이션 파일을 선택합니다. 기본적으로 이는 disk0에 저장되었습니다.

5단계 (선택 사항) 8.3 이전의 활성화 키로 돌아가야 하는 경우 Activation Key 필드에 기존 활성화 키를 입력합니다.

자세한 내용은 37-26 페이지의 활성화 키 호환성 정보를 참조하십시오.

6단계 **Downgrade**를 클릭합니다.

이 툴을 사용하면 다음 기능을 간단하게 완수할 수 있습니다.

1. 부트 이미지 컨피그레이션 지우기(**clear configure boot**)
2. 부트 이미지를 기존 이미지가 되게 설정(**boot system**)
3. (선택 사항) 새 활성화 키 입력(**activation-key**)
4. 실행 중인 컨피그레이션을 시작에 저장(**write memory**). 이는 BOOT 환경 변수를 기존 이미지로 설정합니다. 따라서 다시 로드할 때 기존 이미지가 로드됩니다.
5. 기존 컨피그레이션을 시작 컨피그레이션에 복사(**copy** *old_config_url* **startup-config**)
6. 다시 로드(**reload**)

자동 업데이트 구성

자동 업데이트에 대한 정보

자동 업데이트는 자동 업데이트 서버에서 다수의 ASA에 컨피그레이션 및 소프트웨어 이미지를 다운로드할 수 있게 하고 중앙에서 ASA에 대한 기본적인 모니터링을 제공할 수 있는 프로토콜 사양입니다.

자동 업데이트 클라이언트 또는 서버

ASA는 클라이언트 또는 서버로 구성할 수 있습니다. 자동 업데이트 클라이언트일 경우 정기적으로 자동 업데이트 서버에 폴링하여 소프트웨어 이미지 및 컨피그레이션 파일에 대한 업데이트를 확인합니다. 자동 업데이트 서버는 자동 업데이트 클라이언트로 구성된 ASA를 위해 업데이트를 배포합니다.

자동 업데이트의 이점

자동 업데이트는 다음과 같이 관리자가 ASA 관리에서 겪는 여러 문제점을 해결하는 데 효과적입니다.

- 동적 주소 지정 및 NAT 문제 해결
- 하나의 작업으로 컨피그레이션 변경 사항 커밋
- 믿을 수 있는 소프트웨어 업데이트 방법 제공
- 잘 알려진 고가용성(장애 조치) 방식 활용
- 개방적인 인터페이스로 유연성 제공
- 서비스 공급자 환경을 위한 보안 솔루션 간소화

자동 업데이트 사양은 원격 관리 애플리케이션에서 ASA 컨피그레이션과 소프트웨어 이미지를 다운로드하고 중앙에서 또는 여러 위치에서 기본적인 모니터링을 수행하는 데 필요한 인프라를 제공합니다.

자동 업데이트 사양은 자동 업데이트 서버가 ASA에 컨피그레이션 정보를 푸시하고 정보 요청을 보내거나 컨피그레이션 정보를 가져올 수 있도록 ASA에서 정기적으로 자동 업데이트 서버에 폴링하게 합니다. 또한 자동 업데이트 서버는 언제라도 ASA에 명령을 보내 즉각적인 폴링을 요청할 수 있습니다. 자동 업데이트 서버와 ASA가 통신하려면 각 ASA에 통신 경로 및 로컬 CLI 컨피그레이션이 있어야 합니다.

장애 조치 구성에서 자동 업데이트 서버 지원

활성/대기(Active/Standby) 장애 조치 컨피그레이션에서 자동 업데이트 서버를 사용하여 ASA에 소프트웨어 이미지 및 컨피그레이션 파일을 배포할 수 있습니다. 활성/대기 장애 조치 컨피그레이션에서 자동 업데이트를 활성화하려면 장애 조치 쌍의 기본 유닛에 자동 업데이트 서버 컨피그레이션을 입력합니다.

다음 제한 사항과 동작은 장애 조치 컨피그레이션에서의 자동 업데이트 서버 지원에 적용됩니다.

- 단일 모드에서만 활성/대기 컨피그레이션이 지원됩니다.
- 새 플랫폼 소프트웨어 이미지를 로드할 때 장애 조치 쌍은 트래픽 전달을 중지합니다.
- LAN 기반 장애 조치를 사용할 때 새로운 컨피그레이션이 장애 조치 링크 컨피그레이션을 변경해서는 안 됩니다. 그러면 유닛 간의 통신이 실패합니다.
- 기본 유닛만 자동 업데이트 서버에 대한 콜 홈(call home)을 수행합니다. 기본 유닛은 활성 상태에서 콜 홈을 수행할 수 있습니다. 활성 상태가 아닐 경우 ASA는 자동으로 기본 유닛에 장애 조치합니다.
- 기본 유닛만 소프트웨어 이미지 또는 컨피그레이션 파일을 다운로드합니다. 그런 다음 소프트웨어 이미지 또는 컨피그레이션 파일은 보조 유닛에 복사됩니다.
- 인터페이스 MAC 주소 및 하드웨어 시리얼 ID는 기본 유닛에서 나옵니다.
- 자동 업데이트 서버 또는 HTTP 서버에 저장된 컨피그레이션 파일은 기본 유닛만을 대상으로 합니다.

자동 업데이트 프로세스 개요

다음은 장애 조치 컨피그레이션의 자동 업데이트 프로세스에 대한 개요입니다. 이 프로세스에서는 장애 조치가 활성화되어 작동 중이라고 가정합니다. 유닛에서 컨피그레이션을 동기화하고 있는 경우, 대기 유닛이 SSM 카드 고장을 제외한 어떤 이유로든 고장 상태에 있는 경우 또는 장애 조치 링크가 중단된 경우에는 자동 업데이트 프로세스가 수행될 수 없습니다.

1. 두 유닛 모두 플랫폼 및 ASDM 소프트웨어 체크섬과 버전 정보를 주고받습니다.
2. 기본 유닛이 자동 업데이트 서버에 접속합니다. 기본 유닛이 활성 상태가 아닌 경우 ASA는 먼저 기본 유닛에 장애 조치한 다음 자동 업데이트 서버에 접속합니다.
3. 자동 업데이트 서버가 응답하면서 소프트웨어 체크섬 및 URL 정보를 보냅니다.
4. 기본 유닛이 활성 유닛 또는 대기 유닛의 플랫폼 이미지 파일을 업데이트해야 한다고 판단하면 다음 단계가 진행됩니다.
   a. 기본 유닛이 자동 업데이트 서버가 보낸 URL을 사용하여 HTTP 서버에서 해당 파일을 검색합니다.
   b. 기본 유닛이 대기 유닛에 이미지를 복사한 다음 자신의 이미지를 업데이트합니다.
   c. 두 유닛 모두 새 이미지를 가지고 있는 경우 보조(대기) 유닛 먼저 다시 로드됩니다.
   – 보조 유닛이 부팅할 때 히트리스(hitless) 업그레이드를 수행할 수 있는 경우, 보조 유닛이 활성 유닛이 되고 기본 유닛이 다시 로드됩니다. 기본 유닛이 로딩을 마치면 활성 유닛이 됩니다.
   – 대기 유닛이 부팅할 때 히트리스 업그레이드를 수행할 수 없는 경우에는 두 유닛이 동시에 다시 로드됩니다.
   d. 보조(대기) 유닛에만 새 이미지가 있는 경우 보조 유닛만 다시 로드됩니다. 기본 유닛은 보조 유닛이 다시 로드되는 것이 끝날 때까지 기다립니다.
   e. 기본(활성) 유닛에만 새 이미지가 있을 경우, 보조 유닛이 활성 유닛이 되고 기본 유닛이 다시 로드됩니다.

f. 업데이트 프로세스가 1단계부터 다시 시작합니다.

5. ASA에서 기본 유닛이나 보조 유닛 중 하나의 ASDM 파일을 업데이트해야 한다고 판단하면 다음 단계가 진행됩니다.
   a. 기본 유닛이 자동 업데이트 서버가 보낸 URL을 사용하여 HTTP 서버에서 ASDM 이미지 파일을 검색합니다.
   b. 필요하다면 기본 유닛이 대기 유닛에 ASDM 이미지를 복사합니다.
   c. 기본 유닛이 자신의 ASDM 이미지를 업데이트합니다.
   d. 업데이트 프로세스가 1단계부터 다시 시작합니다.
6. 기본 유닛에서 컨피그레이션을 업데이트해야 한다고 판단하면 다음 단계가 진행됩니다.
   a. 기본 유닛이 지정된 URL을 사용하여 컨피그레이션 파일을 검색합니다.
   b. 두 유닛에서 동시에 새 컨피그레이션이 기존 컨피그레이션을 대체합니다.
   c. 업데이트 프로세스가 1단계부터 다시 시작합니다.
7. 모든 이미지 및 컨피그레이션 파일에서 체크섬이 일치할 경우 어떤 업데이트도 필요 없습니다. 다음 폴링 시간까지 프로세스는 종료됩니다.

자동 업데이트 프로세스 모니터링

debug auto-update client 또는 **debug fover cmd-exe** 명령을 사용하여 자동 업데이트 프로세스에서 수행되는 작업을 표시합니다. 다음은 **debug auto-update client** 명령의 샘플 출력입니다. 터미널 세션에서 **debug** 명령을 실행합니다.

```
Auto-update client: Sent DeviceDetails to /cgi-bin/dda.pl of server 192.168.0.21
Auto-update client: Processing UpdateInfo from server 192.168.0.21
   Component: asdm, URL: http://192.168.0.21/asdm.bint, checksum:
0x94bced0261cc992ae710faf8d244cf32
   Component: config, URL: http://192.168.0.21/config-rms.xml, checksum:
0x67358553572688a805a155af312f6898
   Component: image, URL: http://192.168.0.21/cdisk73.bin, checksum:
0x6d091b43ce96243e29a62f2330139419
Auto-update client: need to update img, act: yes, stby yes
name
ciscoasa(config)# Auto-update client: update img on stby unit...
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 1501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 2501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 3501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 4501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 5501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 6501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 7501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8001, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 8501, len = 1024
auto-update: Fover copyfile, seq = 4 type = 1, pseq = 9001, len = 1024
auto-update: Fover file copy waiting at clock tick 6129280
fover_parse: Rcvd file copy ack, ret = 0, seq = 4
auto-update: Fover filecopy returns value: 0 at clock tick 6150260, upd time 145980 msecs
Auto-update client: update img on active unit...
```

```
fover_parse: Rcvd image info from mate
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
auto-update: HA safe reload: reload active waiting with mate state: 20
Beginning configuration replication: Sending to mate.
auto-update: HA safe reload: reload active waiting with mate state: 50
auto-update: HA safe reload: reload active waiting with mate state: 50

auto-update: HA safe reload: reload active waiting with mate state: 80
        Sauto-update: HA safe reload: reload active unit at clock tick: 6266860
Auto-update client: Succeeded: Image, version: 0x6d091b43ce96243e29a62f2330139419
```

다음 syslog 메시지는 자동 업데이트 프로세스가 실패하면 생성됩니다.

```
%ASA4-612002: Auto Update failed: file version: version reason: reason
```

*file*은 어떤 업데이트가 실패했느냐에 따라 “image”, “asdm” 또는 “configuration”이 됩니다. *version*은 업데이트의 버전 번호입니다. *reason*은 업데이트가 실패한 이유입니다.

지침 및 제한 사항

- 자동 업데이트 서버로부터 ASA 컨피그레이션이 업데이트된 경우 ASDM에 알리지 않습니다. 최신 컨피그레이션을 얻으려면 **Refresh** 또는 **File > Refresh ASDM with the Running Configuration on the Device**를 선택해야 하며, ASDM의 컨피그레이션을 변경한 내용은 잃게 됩니다.
- HTTPS가 자동 업데이트 서버와의 통신 프로토콜로 선택된 경우 ASA는 SSL을 사용합니다. 따라서 ASA에 DES 또는 3DES 라이센스가 있어야 합니다.
- 자동 업데이트는 단일 상황 모드에서만 지원됩니다.

자동 업데이트 서버와의 통신 구성

세부 단계

자동 업데이트 기능을 구성하려면 **Configuration > Device Management > System Image/Configuration > Auto Update**를 선택합니다. Auto Update 창은 Auto Update Servers 테이블과 2개의 영역, 즉 Timeout 영역 및 Polling 영역으로 구성됩니다.

Auto Update Servers 테이블에서는 이전에 구성한 자동 업데이트 서버의 매개 변수를 볼 수 있습니다. ASA는 먼저 테이블의 맨 위에 있는 서버에 폴링합니다. 테이블에 있는 서버의 순서를 변경하려면 **Move Up** 또는 **Move Down**을 클릭합니다. Auto Update Servers 테이블은 다음 열로 구성됩니다.

- Server—자동 업데이트 서버의 이름 또는 IP 주소
- User Name—자동 업데이트 서버에 액세스하는 데 쓰이는 사용자 이름

- Interface—자동 업데이트 서버에 요청을 보낼 때 사용하는 인터페이스
- Verify Certificate—ASA에서 자동 업데이트 서버가 반환한 인증서를 CA 루트 인증서로 검사하는지 여부. 자동 업데이트 서버와 ASA는 동일한 CA를 사용해야 합니다.

Auto Update Server 테이블의 어떤 행이든 두 번 클릭하면 Edit Auto Update Server 대화 상자가 열립니다. 여기서 자동 업데이트 서버 매개 변수를 수정할 수 있습니다. 이 변경 사항은 테이블에 즉시 반영되지만, 컨피그레이션에 저장하려면 **Apply**를 클릭해야 합니다.

Timeout 영역에서는 ASA에서 얼마나 자동 업데이트 서버를 기다린 후 시간 초과가 되는지 설정할 수 있습니다. Timeout 영역은 다음 필드로 구성됩니다.

- Enable Timeout Period—자동 업데이트 서버가 응답하지 않을 경우 ASA에서 시간 초과가 되게 하려면 선택합니다.
- Timeout Period (Minutes)—자동 업데이트 서버에서 응답이 없을 경우 ASA에서 시간 초과 시점까지 기다리는 시간(분)을 입력합니다.

Polling 영역에서는 ASA에서 자동 업데이트 서버로부터 정보를 얻기 위해 폴링하는 빈도를 구성합니다. Polling 영역은 다음 필드로 구성됩니다.

- Polling Period (minutes)—ASA에서 새 정보를 얻고자 자동 업데이트 서버에 폴링하기 위해 기다리는 시간(분)
- Poll on Specified Days—폴링 일정을 지정할 수 있습니다.
- Set Polling Schedule—Set Polling Schedule 대화 상자를 표시하며, 여기에서 자동 업데이트 서버를 폴링할 요일과 시간대를 구성할 수 있습니다.
- Retry Period (minutes)—서버 폴링 시도가 실패한 경우 ASA에서 새 정보를 얻고자 자동 업데이트 서버를 폴링하기 위해 기다리는 시간(분)
- Retry Count—ASA에서 새 정보를 얻고자 자동 업데이트 서버에 대한 폴링을 재시도하는 횟수

자동 업데이트 서버 추가 또는 수정

Add/Edit Auto Update Server 대화 상자는 다음 필드로 구성됩니다.

- URL—자동 업데이트 서버가 ASA와의 통신에 사용하는 프로토콜(HTTP 또는 HTTPS) 및 자동 업데이트 서버의 경로
- Interface—자동 업데이트 서버에 요청을 보낼 때 사용하는 인터페이스
- Do not verify server's SSL certificate—자동 업데이트 서버가 반환한 인증서를 CA 루트 인증서로 검증하지 않으려면 선택합니다. 자동 업데이트 서버와 ASA는 동일한 CA를 사용해야 합니다.

User 영역은 다음 필드로 구성됩니다.

- User Name (Optional)—자동 업데이트 서버에 액세스하는 데 필요한 사용자 이름을 입력합니다.
- Password—자동 업데이트 서버의 사용자 비밀번호를 입력합니다.
- Confirm Password—자동 업데이트 서버의 사용자 비밀번호를 다시 입력합니다.
- Use Device ID to uniquely identify the ASA—디바이스 ID를 사용한 인증을 활성화합니다. 디바이스 ID는 자동 업데이트 서버에게 ASA를 고유하게 식별하는 데 사용됩니다.
- Device ID—사용할 디바이스 ID의 유형
  - Hostname—호스트의 이름
  - Serial Number—디바이스 시리얼 번호
  - IP Address on interface—선택된 인터페이스의 IP 주소. 자동 업데이트 서버에 ASA를 고유하게 식별하는 데 사용됩니다.

- MAC Address on interface—선택된 인터페이스의 MAC 주소. 자동 업데이트 서버에 ASA를 고유하게 식별하는 데 사용됩니다.
- User-defined value—고유한 사용자 ID

폴링 일정 설정

Set Polling Schedule 대화 상자에서는 ASA에서 자동 업데이트 서버에 폴링하는 요일과 시간대를 구체적으로 구성할 수 있습니다.

Set Polling Schedule 대화 상자는 다음 필드로 구성됩니다.

Days of the Week—ASA에서 자동 업데이트 서버에 폴링할 요일을 선택합니다.

Daily Update 창 그룹에서는 ASA에서 자동 업데이트 서버를 폴링할 시간대를 구성할 수 있으며, 다음 필드가 있습니다.

- Start Time—자동 업데이트 폴링을 시작할 시간과 분을 입력합니다.
- Enable randomization—ASA에서 자동 업데이트 서버를 폴링할 시간을 무작위로 선택하게 하려면 선택합니다.

소프트웨어 및 구성 기능 내역

표 37-2에는 각 기능의 변경 사항 및 구현된 플랫폼 릴리스가 나와 있습니다. ASDM은 여러 플랫폼 릴리스와의 역호환성을 지원하므로, 지원이 추가된 ASDM 릴리스가 구체적으로 명시되지 않았습니다.

표 37-2 소프트웨어 및 구성 기능 내역

기능 이름	플랫폼 릴리스	기능 정보
SCP(Secure Copy) 클라이언트	9.1(5)/9.2(1)	ASA에서 SCP 클라이언트와 SCP 서버 간의 파일 전송을 지원합니다. 다음 화면을 수정했습니다. Tools > File Management > ile Transfer > Between Remote Server and Flash **Configuration > Device Management > Management Access > File Access > Secure Copy (SCP) Server**
자동 업데이트 서버 인증서 검증이 기본적으로 활성화되었습니다.	9.2(1)	자동 업데이트 서버 인증서 검증이 기본적으로 활성화됩니다. 신규 컨피그레이션의 경우 명시적으로 인증서 검증을 비활성화해야 합니다. 이전 릴리스에서 업그레이드하는 경우, 인증서 검증을 활성화하지 않았다면 인증서 검증을 할 수 없고 다음 경고가 표시됩니다. `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` The configuration will be migrated to explicitly configure no verification. 다음 화면을 수정했습니다. Configuration > Device Management > System/Image Configuration > Auto Update > Add Auto Update Server

38 장

시스템 이벤트에 대한 응답 자동화

이 장에서는 EEM(Embedded Event Manager)을 구성하는 방법에 대해 설명합니다.

EEM 정보

EEM 서비스에서는 문제를 디버그할 수 있도록 지원하며 문제 해결을 위한 일반적인 용도의 로깅 기능을 제공합니다. 이 서비스는 두 가지 구성 요소로 구성됩니다. 하나는 EEM에서 응답 또는 수신하는 이벤트이며, 하나는 작업 및 EEM에서 응답하는 이벤트를 정의하는 이벤트 관리자 애플릿입니다. 여러 이벤트 관리자 애플릿을 구성하여 다양한 이벤트에 응답하고 여러 작업을 수행할 수 있습니다.

지원되는 이벤트

EEM에서는 다음과 같은 이벤트를 지원합니다.

- Syslog — ASA에서는 syslog 메시지 ID를 사용하여 이벤트 관리자 애플릿을 시행하는 syslog 메시지를 식별합니다. 여러 syslog 이벤트를 구성할 수 있지만, syslog 메시지 ID는 단일 이벤트 관리자 애플릿에서 중복되지 않을 수 있습니다.
- Timers — 타이머를 사용하여 이벤트를 트리거할 수 있습니다. 각 타이머는 각 이벤트 관리자 애플릿에 한 번만 구성할 수 있습니다. 각 이벤트 관리자 애플릿에는 최대 3개의 타이머가 포함될 수 있습니다. 타이머의 3가지 유형은 다음과 같습니다.
  - Watchdog(주기적) 타이머는 애플릿 작업이 완료된 후 지정된 기간이 지나면 이벤트 관리자 애플릿을 시행하며 자동으로 다시 시작됩니다.
  - Countdown(일회성) 타이머는 지정된 기간이 지나면 이벤트 관리자 애플릿을 한 번 시행하며 제거한 후 다시 추가하지 않으면 다시 시작되지 않습니다.
  - Absolute(하루 한 번) 타이머는 지정된 시간에 하루 한 번씩 이벤트를 실행하며 자동으로 다시 시작됩니다. 시간 형식은 hh:mm:ss입니다.

  각 이벤트 관리자 애플릿의 각 유형에는 하나의 타이머 이벤트만 구성할 수 있습니다.

- None — CLI 또는 ASDM을 사용하여 수동으로 이벤트 관리자 애플릿을 실행할 경우 이벤트가 시행됩니다.
- Crash — ASA가 충돌할 경우 충돌 이벤트가 시행됩니다. **output** 명령의 값에 상관없이, **action** 명령은 crashinfo 파일에 직접 적용됩니다. 출력 결과는 **show tech** 명령 앞에 생성됩니다.

이벤트 관리자 애플릿에 대한 작업

이벤트 관리자 애플릿이 시행되면 이벤트 관리자 애플릿에 대한 작업이 수행됩니다. 각 작업에는 작업의 순서를 지정하는 데 사용되는 번호가 있습니다. 이 순서 번호는 이벤트 관리자 애플릿에서 고유해야 합니다. 이벤트 관리자 애플릿에 여러 작업을 구성할 수 있습니다. 명령은 **show blocks** 같은 일반적인 CLI 명령입니다.

출력 대상

output 명령을 사용하여 지정된 위치에 작업의 출력을 보낼 수 있습니다. 한 번에 하나의 출력 값만 활성화할 수 있습니다. 기본값은 **output none**입니다. 이 값은 **action** 명령의 모든 출력을 무시합니다. 명령은 전역 컨피그레이션 모드에서 권한 수준이 15(가장 높음)인 사용자 권한으로 실행됩니다. 명령은 비활성화되므로 입력을 승인하지 않습니다. 다음 세 위치 중 한 곳에 **action** CLI 명령을 보낼 수 있습니다.

- **None** - 기본값이며 출력을 무시합니다.
- **Console** - 출력을 ASA 콘솔로 보냅니다.
- **File** - 출력을 파일로 보냅니다. 다음과 같은 4개의 파일 옵션이 제공됩니다.
  - **Create a unique file** - 이벤트 관리자 애플릿이 호출될 때마다 새로운 고유한 이름의 파일을 생성합니다.
  - **Create/overwrite a file** - 이벤트 관리자 애플릿이 호출될 때마다 지정된 파일을 덮어씁니다.
  - **Create/append to a file** - 이벤트 관리자 애플릿이 호출될 때마다 지정된 파일에 추가합니다. 해당 파일이 아직 없는 경우 파일이 생성됩니다.
  - **Create a set of files** - 이벤트 관리자 애플릿이 호출될 때마다 순환되는 고유한 이름의 파일 집합을 생성합니다.

EEM에 대한 지침

컨텍스트 모드 지침

다중 컨텍스트 모드에서 지원되지 않습니다.

추가 지침

- 충돌이 발생한 동안 ASA의 상태는 일반적으로 알 수 없습니다. 이러한 상황에서 일부 명령을 실행할 경우 안전하지 않을 수 있습니다.
- 이벤트 관리자 애플릿의 이름에는 공백을 포함할 수 없습니다.
- None 이벤트 및 Crashinfo 이벤트 매개변수는 수정할 수 없습니다.
- syslog 메시지가 EEM에 전송되어 처리되므로 성능에 영향을 미칠 수 있습니다.
- 각 이벤트 관리자 애플릿의 기본 출력은 **output none**입니다. 이 설정을 변경하려면 다른 출력 값을 입력합니다.
- 각 이벤트 관리자 애플릿에는 출력 옵션을 하나만 정의할 수 있습니다.

EEM 구성

EEM 구성은 다음과 같은 작업으로 이루어집니다.

1단계 이벤트 관리자 애플릿을 생성한 다음 다양한 이벤트를 구성합니다. 38-3 페이지의 이벤트 관리자 애플릿 생성 및 이벤트 구성를 참조하십시오.

2단계 이벤트 관리자 애플릿에 대한 작업을 구성한 다음 작업의 출력 대상을 구성합니다. 38-4 페이지의 작업 및 작업의 출력 대상 구성를 참조하십시오.

3단계 이벤트 관리자 애플릿을 실행합니다. 38-5 페이지의 이벤트 관리자 애플릿 실행를 참조하십시오.

이벤트 관리자 애플릿 생성 및 이벤트 구성

이벤트 관리자 애플릿을 생성하고 이벤트를 구성하려면 다음 단계를 수행하십시오.

절차

1단계 ASDM에서 **Configuration > Device Management > Advanced > Embedded Event Manager**를 선택합니다.

2단계 **Add**를 클릭하여 **Add Event Manager Applet** 대화 상자를 표시합니다.

3단계 애플릿의 이름을 공백 없이 입력하고 수행하는 작업을 설명합니다. 설명의 길이는 최대 256자로 구성할 수 있습니다. 설명 텍스트가 따옴표 안에 있는 경우 설명 텍스트에 공백을 포함할 수 있습니다.

4단계 **Events** 영역에서 **Add**를 클릭하여 the **Add Event Manager Applet Event** 대화 상자를 표시합니다.

5단계 **Type** 드롭다운 목록에서 구성하려는 이벤트 유형을 선택합니다. 제공되는 옵션은 **crashinfo**, **None**, **Syslog**, **Once-a-day timer**, **One-shot timer**, **Periodic** 타이머입니다.

- **Syslog**: 단일한 syslog 메시지 또는 다양한 syslog 메시지를 입력합니다. 지정된 개별 syslog 메시지 또는 다양한 syslog 메시지와 일치하는 syslog 메시지가 발생할 경우, 이벤트 관리자 애플릿이 시행됩니다. (선택 사항) 호출되는 이벤트 관리자 애플릿에 syslog 메시지가 발생해야 하는 횟수를 **occurrences** 필드에 입력합니다. 기본값은 0초마다 1 어러컨스입니다. 유효한 값의 범위는 1~4294967295입니다. (선택 사항) 작업을 호출하기 위해 syslog 메시지가 발생해야 하는 시간 간격을 초 단위로 **period** 필드에 입력합니다. 이 값은 이벤트 관리자 애플릿의 호출 빈도를 구성된 기간 동안 최대한 한 번으로 제한합니다. 유효한 값의 범위는0~604800입니다. 0 값은 정의된 기간이 없음을 의미합니다.
- **Periodic**: 기간을 초 단위로 입력합니다. 초 단위의 범위는 1~604800으로 지정할 수 있습니다.
- **Once-a-day timer**: 시간을 hh:mm:ss 형식으로 입력합니다. 시간 범위는 00:00:00(자정)에서 23:59:59까지입니다.
- **One-shot timer**: 기간을 초 단위로 입력합니다. 초 단위의 범위는 1~604800으로 지정할 수 있습니다.
- **None**: 이벤트 관리자 애플릿을 수동으로 호출하려면 이 옵션을 선택합니다.
- **crashinfo**: ASA가 충돌할 경우 충돌 이벤트를 시행하려면 이 옵션을 선택합니다.

작업 및 작업의 출력 대상 구성

작업 및 작업의 출력을 전송할 특정 대상을 구성하려면 다음 단계를 수행합니다.

절차

1단계 **Add**를 클릭하여 **Add Event Manager Applet** 대화 상자를 표시합니다.

2단계 애플릿의 이름을 공백 없이 입력하고 수행하는 작업을 설명합니다. 설명의 길이는 최대 256자로 구성할 수 있습니다.

3단계 **Events** 영역에서 **Add**를 클릭하여 the **Add Event Manager Applet Action** 대화 상자를 표시합니다.

4단계 **Sequence #** 필드에 고유한 순서 번호를 입력합니다. 유효한 순서 번호의 범위는 0~4294967295입니다.

5단계 **CLI Command** 필드에 CLI 명령을 입력합니다. 명령은 전역 컨피그레이션 모드에서 권한 수준이 15(가장 높음)인 사용자 권한으로 실행됩니다. 명령은 비활성화되어 있으므로 입력을 승인하지 않습니다.

6단계 **OK**를 클릭하여 **Add Event Manager Applet Action** 대화 상자를 닫습니다.

새로 추가된 작업이 **Actions** 목록에 표시됩니다.

7단계 **Add**를 클릭하여 **Add Event Manager Applet** 대화 상자를 엽니다.

8단계 사용 가능한 출력 대상 옵션 중 하나를 선택합니다.

- **Output Location** 드롭다운 목록에서 **None** 옵션을 선택하여 **action** 명령의 모든 출력을 무시합니다. 이는 기본 설정입니다.
- **Output Location** 드롭다운 목록에서 **Console**을 선택하여 **action** 명령의 출력을 콘솔에 전송합니다.

참고 이 명령을 실행할 경우 성능에 영향을 미칩니다.

- **Output Location** 드롭다운 목록에서 **File** 옵션을 선택하여 **action** 명령의 출력을 호출된 각 이벤트 관리자 애플릿에 대한 새 파일에 전송합니다. **Create a unique file** 옵션이 기본값으로 자동 선택됩니다.

  파일 이름은 eem-*applet-timestamp*.log 형식으로 되어 있습니다. 여기서 *applet*은 이벤트 관리자 애플릿의 이름이고 *timestamp*는 YYYYMMDD-hhmmss 형식의 날짜 타임 스탬프입니다..
- **Output Location** 드롭다운 목록에서 **File** 옵션을 선택한 다음, 드롭다운 목록에서 **Create a set of files** 옵션을 선택하여 순환된 파일 집합을 생성합니다.

  새 파일이 작성되면 기존 파일이 삭제되며, 첫 번째 파일이 작성되기 전에 모든 후속 파일의 번호가 다시 지정됩니다. 최신 파일은 0으로 표시되고, 기존 파일은 가장 높은 숫자로 표시됩니다. 유효한 순환 값의 범위는 2~100입니다. 파일 이름 형식은 eem-*applet-x*.log이며, 여기서 *applet*은 애플릿의 이름이고 *x*는 파일 번호입니다.
- **Output Location** 드롭다운 목록에서 **File** 옵션을 선택한 다음, 드롭다운 목록에서 **Create/overwrite a file** 옵션을 선택하여 **action** 명령 출력을 단일한 파일에 작성하며, 이 파일은 매번 덮어써집니다.
- **Output Location** 드롭다운 목록에서 **File** 옵션을 선택한 다음, 드롭다운 목록에서 **Create/append a file** 옵션을 선택하여 **action** 명령 출력을 단일한 파일에 작성합니다. 단, 이 파일은 매번 추가됩니다.

9단계 **OK**를 클릭하여 **Add Event Manager Applet** 대화 상자를 닫습니다.
지정된 출력 대상이 **Embedded Event Manager** 창에 표시됩니다.

이벤트 관리자 애플릿 실행

이벤트 관리자 애플릿을 실행하려면 다음 단계를 수행합니다.

절차

1단계 **Embedded Event Manager** 창의 목록에서 **None** 이벤트로 구성된 이벤트 관리자 애플릿을 선택합니다.

2단계 **Run**을 클릭합니다.

EEM의 예

다음 예에는 매시간마다 차단 유출 정보를 기록하고, 순환되는 로그 파일 집합에 출력을 작성하여 그날 하루의 가치 있는 로그를 보관하는 이벤트 관리자 애플릿이 나와 있습니다.

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description "Log block usage"
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24
ciscoasa(config-applet)# action 1 cli command "show blocks old"
```

다음 예에는 오전 1시마다 ASA를 재부팅하여 필요한 경우 컨피그레이션을 저장하는 이벤트 관리자 애플릿이 나와 있습니다.

```
ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description "Reboot every night"
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "reload save-config noconfirm"
```

다음 예에는 자정에서 오전 3시 사이에 지정된 인터페이스를 비활성화하는 이벤트 관리자 애플릿이 나와 있습니다.

```
ciscoasa(config)# event manager applet disableintf
ciscoasa(config-applet)# description "Disable the interface at midnight"
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description "Enable the interface at 3am"
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "no shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"
```

EEM 모니터링

EEM을 모니터링하려면 다음 screens를 참조하십시오.

- **Monitoring > Properties > EEM Applets**

  이 창에는 EEM 애플릿의 목록 및 히트 수 값이 나와 있습니다.

- **Tools > Command Line Interface**

  이 창에서는 다양한 비 대화형 명령을 내보내고 결과를 볼 수 있습니다.

EEM에 대한 기록

표 38-1 EEM에 대한 기록

기능 이름	플랫폼 릴리스	설명
EEM(Embedded Event Manager)	9.2(1)	EEM 서비스에서는 문제를 디버그할 수 있도록 지원하며 문제 해결을 위한 일반적인 용도의 로깅 기능을 제공합니다. 이 서비스는 두 가지 구성 요소로 구성됩니다. 하나는 EEM에서 응답 또는 수신하는 이벤트이며, 하나는 작업 및 EEM에서 응답하는 이벤트를 정의하는 이벤트 관리자 애플릿입니다. 여러 이벤트 관리자 애플릿을 구성하여 다양한 이벤트에 응답하고 여러 작업을 수행할 수 있습니다. 다음 명령을 도입했습니다. Configuration > Device Management > Advanced > Embedded Event Manager, Monitoring > Properties > EEM Applets

39장

문제 해결

이 장에서는 Cisco ASA의 문제 해결 방법을 설명합니다.

패킷 캡처 마법사로 캡처 구성 및 실행

패킷 캡처 마법사(Packet Capture Wizard)를 사용하여 오류 해결을 위해 캡처를 구성하고 실행할 수 있습니다. 캡처에서는 캡처되는 트래픽 유형, 소스 및 목적지 주소와 포트, 하나 이상의 인터페이스를 제한하기 위해 ACL을 사용할 수 있습니다. 이 마법사는 인그레스 및 이그레스 인터페이스 각각에서 하나의 캡처를 실행합니다. 캡처를 PC에 저장했다가 패킷 분석기에서 살펴볼 수 있습니다.

참고 이 툴은 클라이언트리스 SSL VPN 캡처를 지원하지 않습니다.

캡처를 구성하고 실행하려면 다음 단계를 수행합니다.

절차

1단계 **Wizards > Packet Capture Wizard**를 선택합니다.

Overview of Packet Capture 화면이 나타나고, 마법사의 안내를 받아 수행할 작업의 목록이 표시됩니다. 다음과 같은 작업이 포함됩니다.

- 인그레스 인터페이스 선택
- 이그레스 인터페이스 선택
- 버퍼 매개 변수 설정
- 캡처 실행
- PC에 캡처 저장(선택 사항)

2단계 **Next**를 클릭합니다.

클러스터링 환경에서는 **Cluster Option** 화면이 나타납니다. 3단계로 진행합니다.

비 클러스터링 환경에서는 **Ingress Traffic Selector** 화면이 나타납니다. 4단계로 진행합니다.

3단계 캡처를 실행하려면 **Cluster Option** 화면에서 **This device only** 또는 **The whole cluster** 옵션 중 하나를 선택하고 **Next**를 클릭하여 **Ingress Selector** 화면을 표시합니다.

4단계 인터페이스의 패킷을 캡처하려면 **Select Interface** 라디오 버튼을 클릭합니다. ASA CX 데이터 플레인의 패킷을 캡처하려면 **Use backplane channel** 라디오 버튼을 클릭합니다.

5단계 **Packet Match Criteria** 영역에서 다음 중 하나를 수행합니다.

- 패킷 매칭에 사용할 ACL을 지정하기 위해 **Specify access-list** 라디오 버튼을 클릭하고 **Select ACL** 드롭다운 목록에서 ACL을 선택합니다. **Manage**를 클릭하여 **ACL Manager** 창을 표시합니다. 앞서 구성한 ACL을 현재 드롭다운 목록에 추가할 수 있습니다. ACL을 선택하고 **OK**를 클릭합니다.
- 패킷 매개 변수를 지정하기 위해 **Specify Packet Parameters** 라디오 버튼을 클릭합니다.

6단계 계속하려면 39-3 페이지의 인그레스 트래픽 선택기를 참조하십시오.

7단계 **Next**를 클릭하여 **Egress Traffic Selector** 화면을 표시합니다. 계속하려면 39-4 페이지의 이그레스 트래픽 선택기를 참조하십시오.

참고 소스 포트 서비스, 목적지 포트 서비스, ICMP 유형은 읽기 전용이며, **Ingress Traffic Selector** 화면에서 선택한 사항을 기반으로 합니다.

8단계 **Next**를 클릭하여 **Buffers & Captures** 화면을 표시합니다. 계속하려면 39-4 페이지의 버퍼를 참조하십시오.

9단계 자동으로 10초마다 최신 캡처를 얻으려면 **Capture Parameters** 영역에서 **Get capture every 10 seconds** 확인란을 선택합니다. 기본적으로 이 캡처에서는 순환형 버퍼를 사용합니다.

10단계 **Buffer Parameters** 영역에서 버퍼 크기와 패킷 크기를 지정합니다. 버퍼 크기는 캡처에서 패킷 저장에 사용할 수 있는 메모리의 최대량입니다. 패킷 크기는 캡처에서 수용 가능한 가장 긴 패킷입니다. 최대한 많은 정보를 캡처하도록 가장 긴 패킷 크기를 사용하는 것이 좋습니다.

a. 패킷 크기를 입력합니다. 유효한 크기 범위는 14바이트~1522바이트입니다.

b. 버퍼 크기를 입력 합니다. 유효한 크기 범위는 1534바이트~33554432바이트입니다.

c. 캡처된 패킷을 저장하려면 **Use circular buffer** 확인란을 선택합니다.

참고 이 설정을 선택한 경우, 버퍼 저장 공간이 모두 사용되면 캡처는 가장 오래된 패킷부터 덮어쓰기합니다.

11단계 **Next**를 클릭하여 **Summary** 화면을 표시합니다. 여기서는 클러스터의 모든 유닛에 대한 클러스터 옵션(클러스터링을 사용하는 경우), 트래픽 선택기, 입력한 버퍼 매개 변수를 표시합니다. 계속하려면 39-4 페이지의 요약를 참조하십시오.

12단계 **Next**를 클릭하여 **Run Captures** 화면을 표시하고, **Start**를 클릭하여 패킷 캡처링을 시작합니다. 캡처를 종료하려면 **Stop**을 클릭합니다. 계속하려면 39-4 페이지의 Run Captures를 참조하십시오. 클러스터링을 사용하는 경우 14단계로 진행합니다.

13단계 남은 버퍼 공간이 얼마나 되는지 확인하려면 **Get Capture Buffer**를 클릭합니다. 버퍼의 현재 내용을 삭제하고 다른 패킷을 캡처할 공간을 확보하려면 **Clear Buffer on Device**를 클릭합니다.

14단계 클러스터링 환경에서는 **Run Captures** 화면에서 다음 단계를 하나 이상 수행합니다.

- **Get Cluster Capture Summary**를 클릭하면 클러스터의 모든 유닛에 대한 패킷 캡처 정보가 요약되어 표시된 다음 각 유닛의 패킷 캡처 정보가 표시됩니다.
- **Get Capture Buffer**를 클릭하면 클러스터의 각 유닛에 남아 있는 버퍼 공간을 확인할 수 있습니다. **Capture Buffer from Device** 대화 상자가 나타납니다.
- **Clear Capture Buffer**를 클릭하면 버퍼에서 클러스터의 한 유닛 또는 모든 유닛의 현재 내용을 삭제하고 다른 패킷을 캡처할 공간을 확보할 수 있습니다.

15단계 **Save captures**를 클릭하면 **Save Capture** 대화 상자가 표시됩니다. 인그레스 캡처, 이그레스 캡처 또는 둘 다 저장할 수 있습니다. 계속하려면 39-5 페이지의 캡처 저장를 참조하십시오.

16단계 **Save Ingress Capture**를 클릭하면 **Save capture file** 대화 상자가 표시됩니다. PC에서 저장 위치를 지정하고 **Save**를 클릭합니다.

17단계 **Launch Network Sniffer Application**을 클릭하면 **Tools > Preferences**에 지정된 패킷 분석 애플리케이션을 시작하여 인그레스 캡처를 분석할 수 있습니다.

18단계 **Save Engress Capture**를 클릭하면 **Save capture file** 대화 상자가 표시됩니다. PC에서 저장 위치를 지정하고 **Save**를 클릭합니다.

19단계 **Launch Network Sniffer Application**을 클릭하면 **Tools > Preferences**에 지정된 패킷 분석 애플리케이션을 시작하여 이그레스 캡처를 분석할 수 있습니다.

20단계 **Close**를 클릭한 다음 **Finish**를 클릭하여 마법사를 종료합니다.

인그레스 트래픽 선택기

패킷 캡처를 위해 인그레스 인터페이스, 소스 및 목적지 호스트 또는 네트워크, 프로토콜을 구성하려면 다음 단계를 수행합니다.

절차

1단계 드롭다운 목록에서 인그레스 인터페이스 이름을 선택합니다.

2단계 인그레스 소스 호스트 및 네트워크를 입력합니다. ASA CX 데이터 플레인의 패킷을 캡처하려면 **Use backplane channel** 라디오 버튼을 클릭합니다.

3단계 인그레스 목적지 호스트 및 네트워크를 입력합니다.

4단계 캡처할 프로토콜 유형을 입력합니다. ah, eigrp, esp, gre, icmp, icmp6, igmp, igrp, ip, ipinip, nos, ospf, pcp, pim, snp, tcp 또는 udp를 프로토콜로 지정할 수 있습니다.

a. ICMP에 대해서만 ICMP 유형을 입력합니다. all, alternate address, conversion-error, echo, echo-reply, information-reply, information-request, mask-reply, mask-request, mobile-redirect, parameter-problem, redirect, router-advertisement, router-solicitation, source-quench, time-exceeded, timestamp-reply, timestamp-request, traceroute 또는 unreachable을 유형으로 지정할 수 있습니다.

b. TCP 및 UDP 프로토콜에 한해 소스 및 목적지 포트 서비스를 지정합니다. 다음과 같은 옵션을 사용할 수 있습니다.

- 모든 서비스를 포함하려면 **All Services**를 선택합니다.
- 한 서비스 그룹을 포함하려면 **Service Groups**를 선택합니다.

  특정 서비스를 포함하려면 aol, bgp, chargen, cifx, citrix-ica, ctiqbe, daytime, discard, domain, echo, exec, finger, ftp, ftp-data, gopher, h323, hostname, http, https, ident, imap4, irc, kerberos, klogin, kshell, ldap, ldaps, login, lotusnotes, lpd, netbios-ssn, nntp, pcanywhere-data, pim-auto-rp, pop2, pop3, pptp, rsh, rtsp, sip, smtp, sqlnet, ssh, sunrpc, tacacs, talk, telnet, uucp 또는 whois 중 하나를 선택합니다.

5단계 Cisco TrustSec 서비스에 대해 패킷 캡처를 활성화하려면 **Security Group Tagging** 영역에서 **SGT number** 확인란을 선택하고 보안 그룹 태그 번호를 입력합니다. 유효한 보안 그룹 태그 번호 범위는 2~65519입니다.

이그레스 트래픽 선택기

패킷 캡처를 위해 이그레스 인터페이스, 소스 및 목적지 호스트/네트워크, 소스 및 목적지 포트 서비스를 구성하려면 다음 단계를 수행합니다.

절차

1단계 인터페이스의 패킷을 캡처하려면 **Select Interface** 라디오 버튼을 클릭합니다. ASA CX 데이터 플레인의 패킷을 캡처하려면 **Use backplane channel** 라디오 버튼을 클릭합니다.

2단계 드롭다운 목록에서 이그레스 인터페이스 이름을 선택합니다.

3단계 이그레스 소스 호스트 및 네트워크를 입력합니다.

4단계 이그레스 목적지 호스트 및 네트워크를 입력합니다.

인그레스 컨피그레이션 중에 선택한 프로토콜 유형이 이미 표시되어 있습니다.

버퍼

패킷 캡처를 위해 패킷 크기, 버퍼 크기, 순환형 버퍼 사용을 구성하려면 다음 단계를 수행합니다.

절차

1단계 캡처에서 수용 가능한 가장 긴 패킷을 입력합니다. 최대한 많은 정보를 캡처하도록 가장 긴 크기를 사용합니다.

2단계 캡처에서 패킷 저장에 사용할 수 있는 메모리의 최대량을 입력합니다.

3단계 패킷 저장에 순환형 버퍼를 사용합니다. 순환형 버퍼의 모든 공간이 사용되면 캡처는 가장 오래된 패킷부터 덮어씁니다.

요약

Summary 화면에서는 클러스터 옵션(클러스터링을 사용하는 경우), 트래픽 선택기, 이전 마법사 화면에서 선택했던 패킷 캡처를 위한 버퍼 매개 변수를 표시합니다.

Run Captures

캡처 세션을 시작, 종료하고 캡처 버퍼를 보고 네트워크 분석기 애플리케이션을 실행하고 패킷 캡처를 저장하고 버퍼를 지우려면 다음 단계를 수행합니다.

절차

1단계 선택한 인터페이스에서 패킷 캡처 세션을 시작하려면 **Start**를 클릭합니다.

2단계 선택한 인터페이스에서 패킷 캡처 세션을 중지하려면 **Stop**을 클릭합니다.

3단계 인터페이스에서 캡처한 패킷의 스냅샷을 얻으려면 **Get Capture Buffer**를 클릭합니다.

4단계 인그레스 인터페이스의 캡처 버퍼를 표시하려면 **Ingress**를 클릭합니다.

5단계 이그레스 인터페이스의 캡처 버퍼를 표시하려면 **Egress**를 클릭합니다.

6단계 디바이스의 버퍼를 지우려면 **Clear Buffer on Device**를 클릭합니다.

7단계 **Launch Network Sniffer Application**을 클릭하면 **Tools > Preferences**에 지정된 패킷 분석 애플리케이션을 시작하여 인그레스 캡처 또는 이그레스 캡처를 분석할 수 있습니다.

8단계 **Save Captures**를 클릭하면 인그레스 및 이그레스 캡처를 ASCII 또는 PCAP 형식으로 저장할 수 있습니다.

캡처 저장

추후 패킷 분석을 위해 인그레스 및 이그레스 패킷 캡처를 ASCII 또는 PCAP 파일 형식으로 저장하려면 다음 단계를 수행합니다.

절차

1단계 캡처 버퍼를 ASCII 형식으로 저장하려면 **ASCII**를 클릭합니다.

2단계 캡처 버퍼를 PCAP 형식으로 저장하려면 **PCAP**를 클릭합니다.

3단계 인그레스 패킷 캡처를 저장할 파일을 지정하려면 **Save ingress capture**를 클릭합니다.

4단계 이그레스 패킷 캡처를 저장할 파일을 지정하려면 **Save egress capture**를 클릭합니다.

ASAv의 vCPU 사용량

ASAv vCPU 사용량에서는 데이터 경로, 제어 지점, 외부 프로세스에 사용된 vCPU의 양을 보여줍니다.

vSphere에서 보고하는 vCPU 사용량에는 앞서 설명한 ASAv 사용량과 함께 다음 항목도 포함되어 있습니다.

- ASAv 유휴 시간
- ASAv VM에 사용된 %SYS 오버헤드
- vSwitch, vNIC, pNIC 간 패킷 이동의 오버헤드 이 오버헤드가 상당히 클 수 있습니다.

CPU 사용량의 예

다음은 보고된 vCPU 사용량이 상당한 차이를 보이는 예입니다.

- ASAv 보고서: 40%
- DP: 35%
- 외부 프로세스: 5%
- vSphere 보고서: 95%

- ASA(ASAv 보고서): 40%
- ASA 유휴 폴링: 10%
- 오버헤드: 45%

이 오버헤드는 하이퍼바이저 기능을 수행하고 vSwitch를 사용하여 NIC와 vNIC 간에 패킷을 이동하는 데 사용됩니다.

사용량이 100%를 초과하기도 합니다. ESXi 서버에서 ASAv 대신 추가 컴퓨팅 리소스를 오버헤드로 사용할 수 있기 때문입니다.

VMware CPU 사용량 보고

vSphere에서 **VM Performance** 탭을 클릭하고 **Advanced**를 클릭하여 **Chart Options** 드롭다운 목록을 표시합니다. 여기서는 VM의 상태별 vCPU 사용량(%USER, %IDLE, %SYS 등)을 보여줍니다. 이 정보는 VMware의 관점에서 CPU 리소스 사용처를 파악하는 데 유용합니다.

ESXi 서버 셸(SSH로 호스트에 연결하는 방법으로 액세스)에서 esxtop을 사용할 수 있습니다. esxtop은 Linux **top** 명령과 비슷하게 생겼고 다음과 같이 vSphere 성능에 대한 VM 상태 정보를 제공합니다.

- vCPU, 메모리, 네트워크 사용량 세부 사항
- 각 VM의 상태별 vCPU 사용량
- 메모리(실행 중에 M 입력) 및 네트워크(실행 중에 N 입력), 통계, RX 드롭 수

ASAv 및 vCenter 그래프

ASAv와 vCenter의 CPU % 수치가 다릅니다.

- vCenter 그래프 수치가 항상 ASAv 수치보다 높습니다.
- vCenter에서는 이를 %CPU usage, ASAv에서는 %CPU utilization이라고 부릅니다.

용어 "%CPU utilization"과 "%CPU usage"의 의미는 서로 다릅니다.

- CPU utilization은 물리적 CPU의 통계를 제공합니다.
- CPU usage는 논리적 CPU의 통계로서 CPU 하이퍼스레딩을 기반으로 합니다. 그러나 단 하나의 vCPU가 사용되므로 하이퍼스레딩은 켜져 있지 않습니다.

vCenter는 %CPU usage를 다음과 같이 계산합니다.

활발하게 사용 중인 가상 CPU의 양 - 총 가용 CPU 기준 백분율로 표시

이 계산은 게스트 운영 체제가 아닌 호스트의 관점에서 본 CPU 사용량입니다. 그리고 가상 머신에 있는 사용 가능한 모든 가상 CPU의 평균 CPU 사용률입니다.

예를 들어, 가상 CPU 1개를 사용하는 가상 시스템이 4개의 물리적 CPU를 가진 호스트에서 실행되는 중이고 CPU usage가 100%라면 가상 머신에서 하나의 물리적 CPU를 온전히 사용하는 것입니다. 가상 CPU uage는 다음과 같이 계산합니다.

사용량(MHz) / 가상 CPU 수 x 코어 주파수

사용량(MHz)을 비교하면 vCenter 수치와 ASAv 수치가 동일합니다. vCenter 그래프에 의거하여 MHz % CPU usage는 다음과 같이 계산됩니다.

60/(2499 x 1 vCPU) = 2.4

파 트 9

로깅, SNMP, Smart Call Home

로깅

이 장에서는 시스템 메시지를 기록하고 문제 해결에 활용하는 방법을 설명합니다.

로깅 정보

시스템 로깅은 디바이스의 메시지를 syslog 데몬을 실행 중인 서버로 수집하는 방식입니다. 중앙 syslog 서버에 로깅하면 로그와 경고를 종합하는 데 도움이 됩니다. Cisco 디바이스는 로그 메시지를 UNIX 스타일 syslog 서비스로 전송할 수 있습니다. syslog 서비스는 메시지를 수신하고 파일로 저장하거나 간단한 컨피그레이션 파일에 따라 인쇄합니다. 이 로깅 양식을 통해 로그를 안전하게 장기 보관할 수 있습니다. 로그는 일상적인 문제 해결과 사고 처리에 모두 유용합니다.

Cisco ASA 시스템 로그는 ASA 모니터링 및 문제 해결에 필요한 정보를 제공합니다. 로깅 기능을 사용하면 다음을 할 수 있습니다.

- 어떤 syslog 메시지를 기록해야 하는지 지정합니다.
- syslog 메시지의 심각도를 비활성화하거나 변경합니다.
- 내부 버퍼, 하나 이상의 syslog 서버, ASDM, SNMP 관리 스테이션, 지정된 이메일 주소 또는 텔넷 및 SSH 세션을 포함하여 syslog 메시지를 보낼 장소를 하나 이상 지정합니다.
- 심각도 수준 또는 메시지 클래스와 같은 그룹으로 syslog 메시지를 구성하고 관리합니다.
- syslog 생성에 속도 제한 적용 여부를 지정합니다.
- 내부 로그 버퍼가 가득 찰 때 작업을 지정합니다. 버퍼를 덮어쓰거나, FTP 서버에 버퍼 내용을 보내거나, 내부 플래시 메모리에 내용을 저장합니다.
- 위치, 심각도, 클래스 또는 사용자 지정 메시지 목록별로 syslog 메시지를 필터링합니다.

다중 컨텍스트 모드에서의 로깅

각 보안 컨텍스트는 자체 로깅 컨피그레이션을 포함하고 자체 메시지를 생성합니다. 시스템 또는 관리자 컨텍스트에 로그인한 후 다른 컨텍스트로 변경하면 세션에서는 현재 컨텍스트와 관련된 메시지만 볼 수 있습니다.

장애 조치 메시지를 포함하여 시스템 실행 공간에서 생성된 syslog 메시지는 관리자 컨텍스트에서 생성된 메시지와 함께 관리자 컨텍스트에서 보게 됩니다. 시스템 실행 공간에서 로깅을 구성하거나 로깅 정보를 볼 수 없습니다.

각 메시지에 컨텍스트 이름을 포함하도록 ASA 및 ASASM을(를) 구성하면 하나의 syslog 서버로 전송되는 컨텍스트 메시지를 구분하는 데 도움이 됩니다. 이 기능을 사용하면 관리자 컨텍스트에서 전송된 메시지와 시스템에서 전송된 메시지를 구분하는 데 도움이 됩니다. 시스템 실행 공간에서 발생한 메시지는 **시스템**의 디바이스 ID를 사용하고 관리자 컨텍스트에서 발생한 메시지는 관리자 컨텍스트의 이름을 디바이스 ID로 사용합니다.

Syslog 메시지 분석

다음은 다양한 syslog 메시지를 검토함으로써 얻을 수 있는 정보 유형의 예입니다.

- ASA 및 ASASM 보안 정책에서 허용된 연결. 이러한 메시지는 보안 정책의 허점을 찾는 데 도움이 됩니다.
- ASA 및 ASASM 보안 정책에서 거부된 연결. 이러한 메시지는 보안된 내부 네트워크로 어떤 유형의 활동이 전송되는지 보여줍니다.
- ACE 거부 속도 로깅 기능을 사용하면 ASA 또는ASA Services Module에서 발생하는 공격을 볼 수 있습니다.
- IDS 활동 메시지는 발생한 공격을 보여줄 수 있습니다.
- 사용자 인증 및 명령 사용량은 보안 정책 변화에 대한 감사 추적을 제공합니다.
- 대역폭 사용량 메시지는 설정된 연결과 해제된 연결, 사용된 트래픽의 길이와 볼륨을 보여줍니다.
- 프로토콜 사용량 메시지는 각 연결에 대해 사용된 프로토콜 및 포트 번호를 보여줍니다.
- 주소 변환 감사 추적 메시지는 설정되거나 해제되는 NAT 또는 PAT 연결을 기록하여 네트워크 내부에서 외부로 악성 활동이 보고될 때 유용합니다.

Syslog 메시지 형식

Syslog 메시지는 백분율 기호(%)로 시작하며 다음과 같은 구조를 갖습니다.

```
%ASA Level Message_number: Message_text
```

필드 설명은 다음과 같습니다.

ASA	ASA 및 ASASM에서 생성된 메시지에 대한 syslog 메시지 시설 코드입니다. 이 값은 항상 ASA입니다.
수준	1부터 7까지입니다. 수준은 syslog 메시지가 설명하는 상태의 심각도를 반영합니다. 숫자가 낮을수록 심각한 상태입니다.
Message_number	syslog 메시지를 식별하는 고유한 6자리 숫자입니다.
Message_text	상태를 설명하는 문자열입니다. syslog 메시지의 이 부분은 IP 주소, 포트 번호 또는 사용자 이름을 포함하기도 합니다.

심각도

표 40-1 syslog 메시지 심각도 수준을 나열합니다. ASDM 로그 뷰어에서 구별하기 쉽도록 각 심각도에 컬러를 할당할 수 있습니다. syslog 메시지 컬러 설정을 구성하려면 **Tools > Preferences > Syslog** 탭을 선택하거나 로그 뷰어의 툴바에서 **Color Settings**를 클릭하십시오.

표 40-1 Syslog 메시지 심각도 수준

수준 번호	심각도	설명
0	**긴급 상황**	시스템을 사용할 수 없습니다.
1	**알림**	즉각적인 행동이 필요합니다.
2	**위험**	심각한 상태입니다.
3	**오류**	오류 상태입니다.
4	**경고**	경고 상태입니다.
5	**알림**	일반적이지만 중요한 상태입니다.
6	**정보**	정보 메시지만 해당됩니다.
7	**디버깅**	디버깅 메시지만 해당됩니다.

참고 ASA 및 ASASM은 심각도 수준 0(응급)으로 syslog 메시지를 생성하지 않습니다. 이 수준은 UNIX syslog 기능과의 호환성을 위해 **logging** 명령에서 제공되지만 ASA에서 사용되지 않습니다.

메시지 클래스와 Syslog ID의 범위

각 syslog 메시지 클래스와 거기 연결된 syslog 메시지 ID의 범위 목록은 syslog 메시지 가이드에서 참조하십시오.

Syslog 메시지 필터링

특정 syslog 메시지만 특정 출력 대상에 전송되도록 생성된 syslog 메시지를 필터링할 수 있습니다. 예를 들어 모든 syslog 메시지를 하나의 출력 대상으로 전송하고 이 syslog 메시지의 하위 집합을 다른 출력 대상으로 보내도록 ASA 및 ASASM을(를) 구성할 수 있습니다.

구체적으로 syslog 메시지가 다음 기준에 따라 출력 대상으로 전송되도록 ASA 및 ASASM을(를) 구성할 수 있습니다.

- Syslog 메시지 ID 번호
- Syslog 메시지 심각도 수준
- Syslog 메시지 클래스(ASA 및 ASASM의 기능 영역에 해당)

출력 대상을 설정할 때 지정할 수 있는 메시지 목록을 생성함으로써 이 기준을 사용자 지정할 수 있습니다. 또는 특정 메시지 클래스를 메시지 목록과는 별개로 각 출력 대상 유형으로 전송하도록 ASA 또는 ASASM을(를) 구성할 수도 있습니다.

syslog 메시지 클래스를 2가지 방법으로 사용할 수 있습니다.

- **logging class** 명령을 사용하여 전체 syslog 메시지 카테고리에 대한 출력 위치를 지정합니다.
- **logging list** 명령을 사용하여 메시지 클래스를 지정하는 메시지 목록을 생성합니다.

syslog 메시지 클래스는 ASA 및 ASASM의 기능에 해당하는 유형에 따라 syslog 메시지를 분류하는 방식을 제공합니다. 예를 들어 vpnc 클래스는 VPN 클라이언트를 의미합니다.

특정 클래스의 모든 syslog 메시지는 syslog 메시지 ID 번호의 첫 3자리가 같습니다. 예를 들어 611로 시작하는 모든 syslog 메시지 ID는 vpnc(VPN 클라이언트)와 연결되어 있습니다. VPN 클라이언트 기능에 연결된 syslog 메시지는 611101부터 611323까지입니다.

또한 대부분의 ISAKMP syslog 메시지는 터널 식별을 돕는 공통의 접두사가 있는 객체 세트를 갖습니다. 이러한 객체가 있는 경우 syslog 메시지의 설명 텍스트 앞에 위치합니다. syslog 메시지가 생성되는 시점에 객체를 알 수 없는 경우 구체적인 *heading* = *value* 조합은 표시되지 않습니다.

객체는 다음과 같이 접두사가 붙습니다.

그룹 = *groupname*, 사용자 이름 = *user*, IP = *IP_address*

그룹이 터널-그룹인 경우 사용자 이름은 로컬 데이터베이스 또는 AAA 서버의 사용자 이름이고 IP 주소는 원격 액세스 클라이언트 또는 레이어 2 피어의 공용 IP 주소입니다.

로그 뷰어에서 메시지 정렬

모든 ASDM 로그 뷰어(실시간 로그 뷰어, 로그 버퍼 뷰어 및 최신 ASDM Syslog 이벤트 뷰어)에서 메시지를 정렬할 수 있습니다. 여러 열을 기준으로 테이블을 정렬하려면 정렬할 첫 번째 열의 헤더를 클릭하고 **Ctrl** 키를 누른 채로 정렬 순서에 포함할 다른 열의 헤더를 클릭합니다. 메시지를 시간순으로 정렬하려면 열의 날짜와 시간을 모두 선택하십시오. 그러지 않으면 메시지는 날짜(시간 무시) 또는 시간(날짜 무시)으로만 정렬됩니다.

실시간 로그 뷰어 및 최신 ASDM Syslog 이벤트 뷰어에서 메시지를 정렬할 때 새로운 메시지가 평소처럼 상단이 아닌 정렬된 순서로 나타납니다. 즉, 나머지 메시지와 혼합됩니다.

사용자 정의 메시지 목록

사용자 정의 메시지 목록을 만드는 것은 어떤 syslog 메시지를 어떤 출력 대상으로 보낼지 제어하는 유연한 방법입니다. 사용자 정의 syslog 메시지 목록에서 심각도, 메시지 ID, syslog 메시지 ID 또는 메시지 클래스 등의 기준을 사용하여 syslog 메시지 그룹을 지정합니다.

예를 들어 메시지 목록을 사용하여 다음을 할 수 있습니다.

- 심각도 수준이 1과 2인 syslog 메시지를 선택하고 하나 이상의 이메일 주소로 보냅니다.
- 메시지 클래스와 연결된 모든 syslog 메시지를 선택하고 내부 버퍼에 저장합니다.

메시지 목록은 메시지 선택을 위한 여러 기준을 포함할 수 있습니다. 하지만 새로운 명령 엔트리와 함께 각 메시지 선택 기준을 추가해야 합니다. 겹치는 메시지 선택 기준을 포함하는 메시지 목록을 만들 수 있습니다. 메시지 목록에서 2개의 기준이 같은 메시지를 선택하면 메시지는 한 번만 로깅됩니다.

클러스터링

syslog 메시지는 클러스터링 환경에서 어카운팅, 모니터링 및 문제 해결을 위한 필수 도구입니다. 클러스터의 각 ASA 유닛(최대 8개의 유닛이 허용됨)은 syslog 메시지를 독립적으로 생성합니다. 특정 **logging** 명령어를 통해 타임 스탬프와 디바이스 ID를 포함하는 헤더 필드를 제어할 수 있습니다. syslog 서버는 디바이스 ID를 사용하여 syslog 생성기를 식별합니다. **logging device-id** 명령을 사용하면 디바이스 ID가 동일하거나 다른 syslog 메시지를 생성하여 클러스터의 동일한 또는 다른 유닛에서 메시지가 표시되도록 할 수 있습니다.

참고 클러스터의 유닛에서 syslog 메시지를 모니터링하려면 모니터링할 각 유닛으로 ASDM 세션을 열어야 합니다.

로깅 지침

IPv6 지침

IPv6를 지원하지 않습니다.

추가 지침

- syslog 서버는 syslogd라는 서버 프로그램을 실행해야 합니다. Windows(Windows 95 및 Windows 98 제외) 운영 체제에는 syslog 서버가 포함되어 있습니다. Windows 95 및 Windows 98의 경우 다른 업체로부터 syslogd 서버를 구해야 합니다.
- ASA 또는 ASASM에서 생성된 로그를 보려면 로깅 출력 대상을 지정해야 합니다. 로깅 출력 대상을 지정하지 않고 로깅을 활성화하면 ASA 및 ASASM은(는) 메시지를 생성하지만 메시지를 볼 수 있는 위치에 저장하지 않습니다. 각 다른 로깅 출력 대상을 별도로 지정해야 합니다. 예를 들어 두 개 이상의 syslog 서버를 출력 대상으로 지정하려면 각 syslog 서버에 대해 **Syslog Server** 창에서 별도의 엔트리를 지정합니다.
- 대기 ASA에서는 TCP를 통한 syslog 전송이 지원되지 않습니다.
- ASA은(는) 단일 컨텍스트 모드에서 **logging host** 명령을 통해 16개 syslog 서버의 컨피그레이션을 지원합니다. 다중 컨텍스트 모드에서는 컨텍스트당 서버 4개로 제한됩니다.
- syslog 서버는 ASA 및 ASASM을(를) 통해 도달할 수 있습니다. syslog 서버가 도달할 수 없는 인터페이스의 ICMP 도달 불가 메시지를 거부하고 syslog를 동일한 서버로 전송하도록 ASASM을(를) 구성할 수 있습니다. 모든 심각도 수준에 대해 로깅을 활성화했는지 확인합니다. syslog 서버가 충돌하지 않게 하려면 syslogs 313001, 313004 및 313005의 생성을 억제하십시오.
- 액세스 목록만 일치하도록 사용자 정의 메시지 목록을 사용할 경우 로깅 심각도 수준이 디버깅(수준 7)으로 상승한 액세스 목록에 대해서 액세스 목록 로그가 생성되지 않습니다. 기본 로깅 심각도는 **logging list** 명령에 대해 6으로 설정됩니다. 이 기본 동작은 설계에 따른 것입니다. 액세스 목록 컨피그레이션의 심각도 수준을 디버깅으로 확실히 변경할 경우 로깅 컨피그레이션 자체도 변경해야 합니다.

  다음은 로깅 심각도 수준이 디버깅으로 변경되었기 때문에 액세스 목록 일치 결과를 포함하지 않는 **show running-config logging** 명령의 출력 샘플입니다.

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

  다음은 액세스 목록 일치 결과를 포함하는 **show running-config logging** 명령의 출력 샘플입니다.

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

이 경우 액세스 목록 컨피그레이션이 변경되지 않고 액세스 목록 일치 개수가 다음 예시와 같이 표시됩니다.

```
ciscoasa(config)# access-list global line 1 extended permit icmp any host 4.2.2.2 log
debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended permit tcp host 10.1.1.2 any eq
www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended permit ip any any (hitcnt=543)
0x25f9e609
```

로깅 구성

이 섹션에서는 로깅 구성 방법을 설명합니다.

1단계 로깅을 활성화합니다. 40-6 페이지의 로깅 활성화를 참조하십시오.

2단계 syslog 메시지의 출력 대상을 구성합니다. 40-6 페이지의 출력 대상 구성를 참조하십시오.

참고 최소 컨피그레이션은 ASA 및 ASASM에서 하려고 하는 작업과 syslog 메시지 처리 요구 사항이 무엇인지에 따라 달라집니다.

로깅 활성화

로깅을 활성화하려면 다음 단계를 수행하십시오.

절차

1단계 ASDM에서 다음 중 하나를 선택합니다.

- **Home > Latest ASDM Syslog Messages > Enable Logging**
- **Configuration > Device Management > Logging > Logging Setup**
- **Monitoring > Real-Time Log Viewer > Enable Logging**
- **Monitoring > Log Buffer > Enable Logging**

2단계 **Enable logging** 확인란을 선택하여 로깅을 켭니다.

출력 대상 구성

문제 해결 및 성능 모니터링을 위해 syslog 메시지 사용을 최적화하려면 syslog 메시지를 보낼 위치를 하나 이상 지정하는 것이 좋습니다(내부 로그 버퍼, 하나 이상의 외부 syslog 서버, ASDM, SNMP 관리 스테이션, 콘솔 포트, 지정된 이메일 주소 또는 텔넷 및 SSH 세션 포함).

Syslog 메시지를 외부 Syslog 서버로 전송

외부 syslog 서버의 사용 가능한 디스크 공간에 따라 메시지를 보관할 수 있으며, 저장한 후에 로그 데이터를 조작할 수 있습니다. 예를 들어 특정 유형의 syslog 메시지가 기록될 때 실행할 작업을 지정하고, 로그에서 데이터를 추출하고 보고를 위해 기록을 다른 파일에 저장하거나, 사이트별 스크립트를 사용하여 통계를 추적할 수 있습니다.

외부 syslog 서버로 syslog 메시지를 전송하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Logging Setup**을 선택합니다.

2단계 **Enable logging** 확인란을 선택하여 ASA에 대한 로깅을 켭니다.

3단계 가능한 경우 **Enable logging on the failover standby unit** 확인란을 선택하여 대기 ASA에 대한 로깅을 켭니다.

4단계 **Send debug messages as syslogs** 확인란을 클릭하여 모든 디버깅 추적 출력을 시스템 로그로 리디렉션합니다. 이 옵션이 활성화되어 있으면 syslog 메시지가 콘솔에 표시되지 않습니다. 따라서 디버깅 메시지를 보려면 콘솔에서 로깅을 활성화하고 디버깅 syslog 메시지 번호 및 심각도 수준에 대한 대상으로 구성해두어야 합니다. 사용할 syslog 메시지 번호는 **711001**입니다. 이 syslog 메시지에 대한 기본 심각도 수준은 디버깅입니다.

5단계 syslog 서버를 제외한 모든 로깅 대상에 대해 사용되도록 **Send syslogs in EMBLEM format** 확인란을 선택하여 EMBLEM 형식을 활성화하십시오.

6단계 로깅 버퍼를 활성화한 경우 syslog 메시지가 저장되는 내부 로그 버퍼의 크기를 지정합니다. 버퍼가 채워지면 로그를 FTP 서버나 내부 플래시 메모리에 저장하지 않는 한 메시지를 덮어씁니다. 기본 버퍼 크기는 4096바이트입니다. 범위는 4096에서 1048576까지입니다.

7단계 덮어 쓰이기 전에 FTP 서버에 버퍼 내용을 저장하려면, **Save Buffer To FTP Server** 확인란을 선택합니다. 버퍼 내용의 덮어쓰기를 허용하려면 이 확인란 선택을 취소합니다.

8단계 FTP 서버를 식별하고 버퍼 내용 저장에 사용되는 FTP 매개변수를 구성하려면 **Configure FTP Settings**를 클릭합니다.

9단계 덮어 쓰이기 전에 버퍼 내용을 내부 플래시 메모리에 저장하려면 **Save Buffer To Flash** 확인란을 선택합니다.

참고 이 옵션은 라우팅 또는 투명 단일 모드에서만 사용할 수 있습니다.

10단계 내부 플래시 메모리에서 로깅에 사용할 최대 공간과 보존할 최소 여유 공간을 지정하려면 **Configure Flash Usage**를 클릭합니다(KB). 이 옵션을 활성화하면 디바이스 디스크에 메시지가 저장되는 “syslog”라는 디렉토리가 생성됩니다.

참고 이 옵션은 단일 라우팅 또는 투명 모드에서만 사용할 수 있습니다.

11단계 ASA 또는 ASASM에서 볼 수 있는 시스템 로그에 대한 대기열 크기를 지정합니다.

FTP 설정 구성

로그 버퍼 내용을 저장하는 데 사용되는 FTP 서버에 대한 컨피그레이션을 지정하려면 다음 단계를 수행하십시오.

절차

1단계 FTP 클라이언트의 컨피그레이션을 활성화하려면 **Enable FTP client** 확인란을 선택합니다.

2단계 FTP 서버의 IP 주소를 지정하십시오.

3단계 FTP 서버에서 저장된 로그 버퍼 내용을 저장할 디렉토리 경로를 지정합니다.

4단계 FTP 서버에 로그인할 사용자 이름을 지정합니다.

5단계 FTP 서버에 로그인하려면 사용자 이름과 연결된 비밀번호를 지정합니다.

6단계 비밀번호를 확인한 다음 **OK**를 클릭합니다.

로깅 플래시 사용 구성

내부 플래시 메모리의 로그 버퍼 내용 저장 한도를 지정하려면 다음 단계를 수행하십시오.

절차

1단계 로깅에 사용할 수 있는 내부 플래시 메모리의 최대량을 지정합니다(KB).

2단계 유지할 내부 플래시 메모리의 양을 지정합니다(KB). 내부 플래시 메모리가 한도에 가까워지면 새로운 로그가 더 이상 저장되지 않습니다.

3단계 **OK**를 클릭하여 **Configure Logging Flash Usage** 대화 상자를 닫습니다.

Syslog 메시징 구성

syslog 메시징을 구성하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Syslog Setup**을 선택합니다.

2단계 파일 메시지의 기반으로 사용할 syslog 서버에 대한 시스템 로그를 선택합니다. 기본값은 대부분의 UNIX 시스템이 기대하는 LOCAL(4)20입니다. 하지만 네트워크 디바이스가 8개의 이용 가능한 시설을 공유하기 때문에 시스템 로그에 대한 이 값을 변경해야 할 수 있습니다.

3단계 전송되는 각 syslog 메시지에 날짜와 시간을 추가하려면 **Include timestamp in syslogs** 확인란을 선택합니다.

4단계 **Syslog ID** 테이블에 표시할 정보를 선택합니다. 사용 가능한 옵션은 다음과 같습니다.

- **Show all syslog ID**를 선택하여 **Syslog ID** 테이블이 syslog 메시지 ID의 전체 목록을 표시하도록 지정합니다.
- **Show disabled syslog ID**를 선택하여 **Syslog ID** 테이블이 명시적으로 비활성화된 syslog 메시지 ID만 표시하도록 지정합니다.

- **Show syslog IDs with changed logging**을 선택하여 기본값에서 변경된 심각도 수준이 있는 syslog 메시지 ID만 **Syslog ID** 테이블에 표시되도록 지정합니다.
- **Show syslog IDs that are disabled or with a changed logging level**을 선택하여 **Syslog ID** 테이블이 심각도 수준이 변경된 syslog 메시지 ID와 명시적으로 비활성화된 syslog 메시지 ID만 표시하도록 지정합니다.

5단계 **Syslog ID Setup Table**은 Syslog ID Setup Table의 설정을 기준으로 syslog 메시지 목록을 표시합니다. 수정하려는 개별 메시지 또는 메시지 ID 범위를 선택합니다. 선택한 메시지 ID를 비활성화하거나 심각도 수준을 수정할 수 있습니다. 목록에서 메시지 하나 이상의 메시지 ID를 선택하려면, 범위의 첫 번째 ID를 클릭한 다음 Shift 클릭으로 범위의 마지막 ID를 선택합니다.

6단계 디바이스 ID를 포함하도록 syslog 메시지를 구성하려면 **Advanced**를 클릭합니다.

Syslog ID 설정 편집

syslog 메시지 설정을 변경하려면 다음 단계를 수행합니다.

참고 **Syslog ID** 필드는 표시 전용입니다. 이 영역에 표시되는 값은 **Syslog ID** 테이블(**Syslog Setup** 창에 위치)에서 선택하는 엔트리에 따라 결정됩니다.

절차

1단계 **Disable Message(s)** 확인란을 선택하여 **Syslog ID** 목록에 표시되는 syslog 메시지 ID에 대한 메시지를 비활성화합니다.

2단계 **Syslog ID** 목록에 표시되는 syslog 메시지 ID에 대해 전송되는 로깅 심각도 수준을 선택합니다. 심각도 수준은 다음과 같이 정의됩니다.

- 긴급(수준 0, 시스템을 사용할 수 없음)

  참고 심각도 수준 0을 사용하는 것은 권장하지 않습니다.

- 알림(수준 1, 즉각적인 조치 필요)
- 심각(수준 2, 심각한 상태)
- 오류(수준 3, 오류 상태)
- 경고(수준 4, 경고 상태)
- 알림(수준 5, 정상적이나 중요한 상태)
- 정보(수준 6, 정보 메시지만 해당)
- 디버깅(수준 7, 디버깅 메시지만 해당)

3단계 **OK**를 클릭하여 **Edit Syslog ID Settings** 대화 상자를 닫습니다.

Non-EMBLEM 형식 Syslog 메시지에 디바이스 ID 포함

non-EMBLEM 형식 syslog 메시지에 디바이스 ID를 포함하려면 다음 단계를 수행하십시오.

절차

1단계 **Enable syslog device ID** 확인란을 선택하여 디바이스 ID가 모든 non-EMBLEM 형식 syslog 메시지에 포함되도록 지정합니다.

2단계 무엇을 디바이스 ID로 사용할지 지정하려면 다음 옵션 중 하나를 선택합니다.

- ASA의 호스트 이름
- 인터페이스 IP 주소

  드롭다운 목록에서 선택된 IP 주소에 해당하는 인터페이스 이름을 선택합니다.

  클러스터링을 사용하는 경우 **In an ASA cluster, always use master's IP address for the selected interface** 확인란을 선택하십시오.
- 문자열

  영숫자, 사용자 정의 문자열을 지정합니다.
- ASA 클러스터 이름

3단계 **OK**를 클릭하여 **Advanced Syslog Configuration** 대화 상자를 닫습니다.

Syslog 메시지를 내부 로그 버퍼로 전송

임시 저장 위치 역할을 하는 내부 로그 버퍼로 어떤 syslog 메시지를 전송할지 지정해야 합니다. 새 메시지가 목록의 끝에 추가됩니다. 버퍼가 가득 차는 경우, 즉 버퍼가 줄 바꿈되는 경우 가득 찬 버퍼를 다른 위치로 저장하도록 ASA 및 ASASM을 구성하지 않는 한 새로운 메시지가 생성되면서 이전 메시지를 덮어씁니다.

syslog 메시지를 내부 로그 버퍼로 보내려면 다음 단계를 수행합니다.

절차

1단계 다음 옵션 중 하나를 선택하여 내부 로그 버퍼로 어떤 syslog 메시지를 보낼지 지정합니다.

- **Home > Latest ASDM Syslog Messages > Configure ASDM Syslog Filters**
- **Configuration > Device Management > Logging > Logging Filters**

2단계 **Monitoring > Logging > Log Buffer > View**를 선택합니다. 그런 다음 **File > Clear Internal Log Buffer**를 **Log Buffer** 창에서 선택하여 내부 로그 버퍼를 비웁니다.

3단계 내부 로그 버퍼 크기를 변경하려면 **Configuration > Device Management > Logging > Logging Setup**을 선택합니다. 기본 버퍼 크기는 4KB입니다.

ASA 및 ASASM은(는) 계속해서 새로운 메시지를 내부 로그 버퍼에 저장하고 전체 로그 버퍼 내용을 내부 플래시 메모리에 저장합니다. 버퍼 내용을 다른 위치에 저장할 때는 ASA 및 ASASM이(가) 다음 타임 스탬프 형식을 사용하는 이름으로 로그 파일을 생성합니다.

LOG-YYYY-MM-DD-HHMMSS.TXT

*YYYY*는 연도이고 *MM*는 달이며 *DD*는 날짜입니다. *HHMMSS*는 시간, 분, 초를 나타냅니다.

4단계 새 메시지를 다른 위치에 저장하려면 다음 옵션 중 하나를 선택합니다.

- **Flash** 확인란을 선택하여 새로운 메시지를 내부 플래시 메모리로 보낸 다음 **Configure Flash Usage**를 클릭합니다. **Configure Logging Flash Usage** 대화 상자가 표시됩니다.
  a. 로깅에 사용할 최대 플래시 메모리양을 KB 단위로 지정합니다.
  b. 플래시 메모리에서 로깅이 유지할 최소 여유 공간을 KB 단위로 지정합니다.
  c. **OK**를 클릭하여 이 대화 상자를 닫습니다.
- 새로운 메시지를 FTP 서버로 보내려면 **FTP Server** 확인란을 클릭하고 **Configure FTP Settings**를 클릭합니다. 그러면 **Configure FTP Settings** 대화 상자가 나타납니다.
  a. **Enable FTP Client** 확인란을 선택합니다.
  b. 제공된 필드에 FTP 서버 IP 주소, 경로, 사용자 이름 및 비밀번호를 입력합니다.
  c. 비밀번호를 확인한 다음 **OK**를 클릭하여 이 대화 상자를 닫습니다.

내부 로그 버퍼를 플래시에 저장

내부 로그 버퍼를 플래시 메모리에 저장하려면 다음 단계를 수행하십시오.

절차

1단계 **File > Save Internal Log Buffer to Flash**를 선택합니다.

Enter Log File Name 대화 상자가 나타납니다.

2단계 로그 버퍼를 기본 파일 이름인 LOG-YYYY-MM-DD-hhmmss.txt로 저장하려면 첫 번째 옵션을 선택합니다.

3단계 로그 버퍼에 대한 이름을 지정하려면 두 번째 옵션을 선택합니다.

4단계 로그 버퍼에 대한 파일 이름을 입력하고 **OK**를 클릭합니다.

ASDM Java 콘솔을 통해 로깅된 엔트리를 보고 복사

ASDM Java 콘솔을 통해 로깅된 엔트리를 텍스트 형식으로 보고 복사하면 ASDM 오류 해결에 도움이 됩니다.

ASDM Java Console에 액세스하려면 다음 단계를 수행하십시오.

절차

1단계 **Tools > ASDM Java Console**을 선택합니다.

2단계 가상 머신 메모리 통계를 표시하려면 콘솔에 **m**을 입력합니다.

3단계 휴지통 모으기를 수행하려면 콘솔에서 **g**를 입력합니다.

4단계 Windows 작업 관리자를 열고 **asdm_launcher.exe** 파일을 두 번 클릭하여 메모리 사용량을 모니터링합니다.

참고 허용되는 최대 메모리 할당은 256MB입니다.

이메일 주소로 Syslog 메시지 보내기

이메일 주소로 syslog 메시지를 보내려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > E-Mail Setup**을 선택합니다.

2단계 이메일 메시지로 전송되는 syslog 메시지의 소스 주소로 사용할 이메일 주소를 지정합니다.

3단계 지정된 syslog 메시지의 새로운 이메일 주소 수신자를 입력하려면 **Add**를 클릭합니다.

4단계 드롭다운 목록에서 수신자에게 전송되는 syslog 메시지의 심각도 수준을 선택합니다. 대상 이메일 주소에 사용되는 syslog 메시지 심각도 필터는 지정된 심각도 수준 이상의 메시지가 전송되도록 만듭니다. **Logging Filters** 창에 지정된 글로벌 필터도 각 이메일 수신자에 적용됩니다.

5단계 **Edit**를 클릭하여 이 수신자에게 전송된 syslog 메시지의 기존 심각도 수준을 수정합니다.

6단계 **OK**를 클릭하여 **Add E-mail Recipient** 대화 상자를 닫습니다.

이메일 수신자 추가 또는 편집

이메일 수신자 및 심각도 수준을 추가하거나 편집하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > E-Mail Setup**을 선택합니다.

2단계 **Add** 또는 **Edit**를 클릭하여 **Add/Edit E-Mail Recipient** 대화 상자를 표시합니다.

3단계 대상 이메일 주소를 입력하고 드롭다운 목록에서 syslog 심각도 수준을 선택합니다. 심각도 수준은 다음과 같이 정의됩니다.

- 긴급(수준 0, 시스템을 사용할 수 없음)

참고 심각도 수준 0을 사용하는 것은 권장하지 않습니다.

- 알림(수준 1, 즉각적인 조치 필요)
- 심각(수준 2, 심각한 상태)
- 오류(수준 3, 오류 상태)
- 경고(수준 4, 경고 상태)
- 알림(수준 5, 정상적이나 중요한 상태)
- 정보(수준 6, 정보 메시지만 해당)
- 디버깅(수준 7, 디버깅 메시지만 해당)

참고 대상 이메일 주소에 대한 메시지 필터링에 사용되는 심각도 수준은 **Add/Edit E-Mail Recipient** 대화 상자에 지정된 심각도 수준과 **Logging Filters** 창의 모든 이메일 수신자에 대해 설정된 글로벌 필터보다 높습니다.

4단계 **OK**를 클릭하여 **Add/Edit E-Mail Recipient** 대화 상자를 닫습니다.

E-mail Recipients 창에 추가 또는 수정된 엔트리가 표시됩니다.

5단계 **Apply**를 클릭하여 실행 중인 컨피그레이션에 변경 사항을 저장합니다.

원격 SMTP 서버 구성

특정 이벤트에 대한 응답으로 이메일 경고 및 알림이 전송되는 원격 SMTP 서버를 구성하려면 다음 단계를 수행합니다.

절차

1단계 **Configuration > Device Setup > Logging > SMTP**를 선택합니다.

2단계 기본 SMTP 서버의 IP 주소를 입력합니다.

3단계 (선택 사항) 대기 SMTP 서버의 IP 주소를 입력하고 **Apply**를 클릭하여 실행 중인 컨피그레이션에 변경 사항을 저장합니다.

ASDM에서 Syslog 메시지 보기

1단계 **Home > Latest ASDM Syslog Messages**를 선택하여 ASDM으로 전송된 최신 syslog 메시지를 봅니다.

ASA 또는 ASASM은(는) ASDM으로 전송 대기 중인 syslog 메시지에 대한 버퍼 영역을 남겨두고 생성되는 메시지를 버퍼에 저장합니다. ASDM 로그 버퍼는 내부 로그 버퍼와 다른 버퍼입니다. ASDM 로그 버퍼가 가득 차면 ASA 또는 ASASM은(는) 가장 오래된 syslog 메시지를 삭제하여 새로운 메시지를 위한 버퍼 공간을 확보합니다. ASDM의 기본 설정은 새로운 메시지를 위해 가장 오래된 syslog 메시지를 삭제하는 것입니다.

로깅 대상에 메시지 필터 적용

로깅 대상에 메시지 필터를 적용하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Logging Filters**를 선택합니다.

2단계 필터를 적용할 로깅 대상의 이름을 선택합니다. 이용 가능한 로깅 대상은 다음과 같습니다.

- ASDM
- 콘솔 포트
- 이메일
- 내부 버퍼
- SNMP 서버
- Syslog 서버
- 텔넷 또는 SSH 세션

이 선택의 두 번째 열에는 Syslogs From All Event Classes가 포함되어 있고 세 번째 열에는 Syslogs From Specific Event Classes가 포함되어 있습니다. 두 번째 열은 로깅 대상에 대한 메시지 필터링에 사용할 심각도 또는 이벤트 클래스를 나열하고 모든 이벤트 클래스에 대한 로깅이 비활성화되어 있는지 보여줍니다. 세 번째 열은 해당 로깅 대상에 대한 메시지 필터링에 사용할 이벤트 클래스를 나열합니다.

3단계 **Edit**를 클릭하여 **Edit Logging Filters** 대화 상자를 표시합니다. 필터를 적용, 수정 또는 비활성화하려면 40-14 페이지의 로깅 필터 적용을(를) 참조하십시오.

로깅 필터 적용

필터를 적용하려면 다음 단계를 수행하십시오.

절차

1단계 syslog 메시지를 심각도 수준에 따라 필터링하려면 **Filter on severity** 옵션을 선택합니다.

2단계 이벤트 목록에 따라 syslog 메시지를 필터링하려면 **Use event list** 옵션을 선택합니다.

3단계 **Disable logging from all event classes** 옵션을 선택하여 선택한 대상에 대한 모든 로깅을 비활성화합니다.

4단계 **New**를 클릭하여 새 이벤트 목록을 추가합니다. 새 이벤트 목록을 추가하려면 40-16 페이지의 사용자 지정 이벤트 목록 생성을 참조하십시오.

5단계 드롭다운 목록에서 이벤트 클래스를 선택합니다. 이용 가능한 이벤트 클래스는 사용 중인 디바이스 모드에 따라 변경됩니다.

6단계 드롭다운 목록에서 로깅 메시지의 수준을 선택합니다. 심각도 수준은 다음과 같습니다.

- 긴급(수준 0, 시스템을 사용할 수 없음)

  참고 심각도 수준 0을 사용하는 것은 권장하지 않습니다.

- 알림(수준 1, 즉각적인 조치 필요)
- 심각(수준 2, 심각한 상태)
- 오류(수준 3, 오류 상태)
- 경고(수준 4, 경고 상태)
- 알림(수준 5, 정상적이나 중요한 상태)
- 정보(수준 6, 정보 메시지만 해당)
- 디버깅(수준 7, 디버깅 메시지만 해당)

7단계 **Add**를 클릭하여 이벤트 클래스와 심각도를 추가하고 **OK**를 클릭합니다.

필터에 대해 선택한 로깅 대상이 상단에 나타납니다.

메시지 클래스와 심각도 필터 추가 또는 수정

메시지 필터링을 위한 메시지 클래스와 심각도 수준을 추가하거나 수정하려면 다음 단계를 수행하십시오.

절차

1단계 드롭다운 목록에서 이벤트 클래스를 선택합니다. 이용 가능한 이벤트 클래스는 사용 중인 디바이스 모드에 따라 변경됩니다.

2단계 드롭다운 목록에서 로깅 메시지의 수준을 선택합니다. 심각도 수준은 다음과 같습니다.

- 긴급(수준 0, 시스템을 사용할 수 없음)

  참고 심각도 수준 0을 사용하는 것은 권장하지 않습니다.

- 알림(수준 1, 즉각적인 조치 필요)
- 심각(수준 2, 심각한 상태)
- 오류(수준 3, 오류 상태)
- 경고(수준 4, 경고 상태)
- 알림(수준 5, 정상적이나 중요한 상태)
- 정보(수준 6, 정보 메시지만 해당)
- 디버깅(수준 7, 디버깅 메시지만 해당)

3단계 선택이 끝나면 **OK**를 클릭합니다.

Syslog 메시지 ID 필터 추가 또는 편집

syslog 메시지 ID 필터를 추가하거나 편집하려면 40-9 페이지의 Syslog ID 설정 편집을(를) 참조하십시오.

Syslog 메시지를 콘솔 포트로 전송

syslog 메시지를 콘솔 포트로 보내려면 다음 단계를 수행하십시오.

절차

1단계 다음 옵션 중 하나를 선택합니다.

- **Home > Latest ASDM Syslog Messages > Configure ASDM Syslog Filters**
- **Configuration > Device Management > Logging > Logging Filters**

2단계 **Logging Destination** 열에서 콘솔을 선택하고 **Edit**를 클릭합니다.

Edit Logging Filters 대화 상자가 나타납니다.

3단계 syslogs from all event classes 또는 syslogs from specific event classes 중 하나를 선택하여 콘솔 포트로 어떤 syslog 메시지를 보낼지 지정합니다.

Syslog 메시지를 텔넷이나 SSH 세션으로 전송

syslog 메시지를 텔넷이나 SSH 세션으로 전송하려면 다음 단계를 수행하십시오.

절차

1단계 다음 옵션 중 하나를 선택합니다.

- **Home > Latest ASDM Syslog Messages > Configure ASDM Syslog Filters**
- **Configuration > Device Management > Logging > Logging Filters**

2단계 **Telnet** 및 **SSH Sessions**를 **Logging Destination** 열에서 선택한 후 **Edit**를 클릭합니다.

Edit Logging Filters 대화 상자가 나타납니다.

3단계 syslogs from all event classes 또는 syslogs from specific event classes 중 하나를 선택하여 텔넷 또는 SSH 세션으로 어떤 syslog 메시지를 보낼지 지정합니다.

4단계 **Configuration > Device Management > Logging > Logging Setup**을 선택하여 현재 세션에 대해서만 로깅을 허용합니다.

5단계 **Enable logging** 확인란을 선택한 후 **Apply**를 클릭합니다.

사용자 지정 이벤트 목록 생성

다음 3개의 기준을 이용하여 이벤트 목록을 정의합니다.

- 이벤트 클래스
- 심각도
- 메시지 ID

특정 로깅 대상(예: SNMP 서버)으로 보낼 사용자 지정 이벤트 목록을 생성하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Event Lists**를 선택합니다.

2단계 **Add**를 클릭하여 **Add Event List** 대화 상자를 표시합니다.

3단계 이벤트 목록 이름을 입력합니다. 공백은 허용되지 않습니다.

4단계 **Add**를 클릭하여 **Add Class and Severity Filter** 대화 상자를 표시합니다.

5단계 드롭다운 목록에서 이벤트 클래스를 선택합니다. 이용 가능한 이벤트 클래스는 사용 중인 디바이스 모드에 따라 변경됩니다.

6단계 드롭다운 목록에서 심각도 수준을 선택합니다. 심각도 수준은 다음과 같습니다.

- 긴급(수준 0, 시스템을 사용할 수 없음)

  참고 심각도 수준 0을 사용하는 것은 권장하지 않습니다.

- 알림(수준 1, 즉각적인 조치 필요)
- 심각(수준 2, 심각한 상태)

- 오류(수준 3, 오류 상태)
- 경고(수준 4, 경고 상태)
- 알림(수준 5, 정상적이나 중요한 상태)
- 정보(수준 6, 정보 메시지만 해당)
- 디버깅(수준 7, 디버깅 메시지만 해당)

7단계 **OK**를 클릭하여 **Add Event List** 대화 상자를 닫습니다.

8단계 **Add**를 클릭하여 **Add Syslog Message ID Filter** 대화 상자를 표시합니다.

9단계 필터에 포함할 syslog 메시지 ID 또는 ID 범위(예: 101001-199012)를 입력합니다.

10단계 **OK**를 클릭하여 **Add Event List** 대화 상자를 닫습니다.

관심 이벤트가 목록에 표시됩니다.

EMBLEM 형식의 Syslog 메시지를 Syslog 서버에 생성

EMBLEM 형식의 syslog 메시지를 syslog 서버에 생성하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Syslog Server**를 선택합니다.

2단계 **Add**를 클릭하여 새 syslog 서버를 추가합니다.

Add Syslog Server 대화 상자가 나타납니다.

참고 보안 컨텍스트당 최대 4개의 syslog 서버를 설정할 수 있습니다(최대 총 16개).

3단계 syslog 서버가 사용 중일 때 ASA 또는 ASASM에서 대기열에 허용되는 메시지 수를 지정합니다. 값이 0이면 대기 가능한 메시지 수에 제한이 없음을 의미합니다.

4단계 syslog 서버가 다운되었을 때 모든 트래픽을 제한할지 지정하려면 **Allow user traffic to pass when TCP syslog server is down** 확인란을 선택합니다. TCP를 지정한 경우 ASA 또는 ASASM은(는) syslog 서버의 장애를 감지하고 보호 조치로서 ASA을(를) 통한 새로운 연결을 차단합니다. UDP를 지정한 경우 ASA 또는 ASASM은(는) syslog 서버 작동 여부에 관계없이 새로운 연결을 계속 허용합니다. 각 프로토콜에 대한 유효한 포트 값은 1025부터 65535입니다. 기본 UDP 포트는 514입니다. 기본 TCP 포트는 1470입니다.

참고 대기 ASA에서는 TCP를 통한 syslog 전송이 지원되지 않습니다.

Syslog 서버 설정 추가 또는 수정

syslog 서버 설정을 추가하거나 편집하려면 다음 단계를 수행하십시오.

절차

1단계 드롭다운 목록에서 syslog 서버와 통신할 때 사용되는 인터페이스를 선택합니다.

2단계 syslog 서버와의 통신에 사용되는 IP 주소를 입력합니다.

syslog 서버가 ASA 또는 ASASM와(과) 통신하는 데 사용하는 프로토콜(TCP 또는 UDP)을 선택합니다. UDP 또는 TCP를 사용하여 syslog 서버에 데이터를 전송하도록 ASA 및 ASASM을(를) 구성할 수 있지만 둘 다 사용할 수는 없습니다. 프로토콜을 지정하지 않으면 기본 프로토콜은 UDP입니다.

3단계 syslog 서버가 ASA 또는 ASASM와(과) 통신하는 데 사용하는 포트 번호를 입력합니다.

4단계 **Log messages in Cisco EMBLEM format (UDP only)** 확인란을 선택하여 Cisco EMBLEM 형식의 메시지 로깅 여부를 지정합니다(프로토콜로 UDP가 선택된 경우만 사용 가능).

5단계 **Enable secure logging using SSL/TLS (TCP only)** 확인란을 선택하여 syslog 서버로의 연결을 SSL/TLS over TCP를 통해 보안할지, syslog 메시지 내용을 암호화할지 지정합니다.

6단계 **OK**를 클릭하여 컨피그레이션을 마칩니다.

다른 출력 대상으로 EMBLEM 형식의 Syslog 메시지 생성

EMBLEM 형식의 syslog 메시지를 다른 출력 대상으로 생성하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Logging Setup**을 선택합니다.

2단계 **Send syslogs in EMBLEM format** 확인란을 선택합니다.

로그에 사용할 수 있는 내부 플래시 메모리양을 변경

로그에 사용할 수 있는 내부 플래시 메모리의 양을 변경하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Logging Setup**을 선택합니다.

2단계 **Enable Logging** 확인란을 선택합니다.

3단계 **Logging to Internal Buffer** 영역의 **Save Buffer to Flash** 확인란을 선택합니다.

4단계 **Configure Flash Usage**를 클릭합니다.

Configure Logging Flash Usage 대화 상자가 표시됩니다.

5단계 로깅에 사용할 수 있는 최대 플래시 메모리의 양을 KB 단위로 입력합니다.

기본적으로 ASA은(는) 로그 데이터를 위해 최대 1MB의 내부 플래시 메모리를 사용할 수 있습니다. 로그 데이터 저장을 위해 ASA 및 ASASM에서 비어 있어야 하는 내부 플래시 메모리의 최소 용량은 3MB입니다. 내부 플래시 메모리에 저장되는 로그 파일로 인해 남을 내부 플래시 메모리가 구성된 최소 용량보다 작아질 경우 ASA 또는 ASASM은(는) 가장 오래된 로그 파일을 삭제하여 새 로그 파일을 저장한 후에 최소 여유 공간을 확보할 수 있도록 합니다. 삭제할 파일이 없거나 모든 오래된 파일을 삭제한 후에도 여유 메모리가 부족하면 ASA 또는 ASASM은 새 로그 파일을 저장할 수 없습니다.

6단계 플래시 메모리에서 로깅을 위해 유지할 최소 여유 공간을 KB 단위로 입력합니다.

7단계 **OK**를 클릭하여 **Configure Logging Flash Usage** 대화 상자를 닫습니다.

로깅 대기열 구성

로깅 대기열을 구성하려면 다음 작업을 수행합니다.

절차

1단계 **Configuration > Device Management > Logging > Logging Setup**을 선택합니다.

2단계 **Enable Logging** 확인란을 선택합니다.

3단계 ASA 및 ASASM이(가) 구성된 출력 대상으로 보내기 전에 대기열에 저장할 수 있는 syslog 메시지의 수를 입력합니다.

ASA 및 ASASM은(는) 메모리에 고정된 개수의 블록을 가지고 있고 이 블록은 구성된 출력 대상으로 전송을 기다리는 동안 syslog 메시지 버퍼링을 위해 할당될 수 있습니다. 필요한 블록 개수는 syslog 메시지 대기열의 길이와 지정된 syslog 서버의 수에 따라 달라집니다. 기본 대기열 크기는 syslog 메시지 512개입니다. 대기열 크기는 이용 가능한 블록 메모리로만 제한됩니다. 유효한 값은 플랫폼에 따라 0~8192개의 메시지입니다. 로깅 대기열이 0으로 설정된 경우 대기열은 최대 구성 가능한 크기(메시지 8192개)가 됩니다.

4단계 **Apply**를 클릭하여 실행 중인 컨피그레이션에 변경 사항을 저장합니다.

클래스의 모든 Syslog 메시지를 지정된 출력 대상으로 전송

클래스의 모든 syslog 메시지를 지정된 출력 대상으로 전송하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Logging Filters**를 선택합니다.

2단계 지정된 출력 대상의 컨피그레이션을 무시하려면 변경하려는 출력 대상을 선택한 다음 **Edit**를 클릭합니다.

Edit Logging Filters 대화 상자가 나타납니다.

3단계 **Syslogs from All Event Classes** 또는 **Syslogs from Specific Event Classes** 영역에서 설정을 수정한 후 **OK**를 클릭하여 이 대화 상자를 닫습니다.

예를 들어 심각도 수준 7의 메시지가 내부 로그 버퍼로 전송되도록 지정하고 심각도 수준 3의 ha 클래스 메시지가 내부 로그 버퍼로 전송되도록 지정한 경우 후자의 컨피그레이션이 우선합니다.

클래스가 2개 이상의 대상으로 전송되도록 지정하려면 각 출력 대상에 대해 다른 필터링 옵션을 선택합니다.

안전한 로깅 활성화

안전한 로깅을 활성화하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Syslog Server**를 선택합니다.

2단계 안전한 로깅을 활성화할 syslog 서버를 선택한 후 **Edit**를 클릭합니다.

Edit Syslog Server 대화 상자가 나타납니다.

3단계 **TCP** 라디오 버튼을 클릭합니다.

참고 안전한 로깅은 UDP를 지원하지 않습니다. 이 프로토콜을 사용하려고 하면 오류가 발생합니다.

4단계 **Enable secure syslog with SSL/TLS** 확인란을 선택한 후 **OK**를 클릭합니다.

디바이스 ID를 Non-EMBLEM 형식 Syslog 메시지에 포함

디바이스 ID를 non-EMBLEM 형식 syslog 메시지에 포함하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration**을 선택합니다**.**

2단계 **Enable syslog device ID** 확인란을 선택합니다.

3단계 **Hostname**, **Interface IP Address** 또는 **String** 라디오 버튼을 클릭합니다(**Device ID** 영역).

- **Interface IP Address** 옵션을 선택하는 경우 드롭다운 목록에서 올바른 인터페이스가 선택되었는지 확인하십시오.
- **String** 옵션을 선택할 경우 **User-Defined ID** 필드에 디바이스 ID를 입력합니다. 문자열은 최대 16자를 포함할 수 있습니다.

참고 활성화된 경우 디바이스 ID가 EMBLEM 형식 syslog 메시지나 SNMP 트랩에 표시되지 않습니다.

4단계 **OK**를 클릭하여 **Advanced Syslog Configuration** 대화 상자를 닫습니다.

Syslog 메시지에 날짜와 시간 포함

syslog 메시지에 날짜와 시간을 포함하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Syslog Setup**을 선택합니다.
2단계 **Include timestamp in syslogs** 확인란을 선택합니다(**Syslog ID Setup** 영역).
3단계 **Apply**를 클릭하여 변경 사항을 저장합니다.

Syslog 메시지 비활성화

지정된 syslog 메시지를 비활성화하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Syslog Setup**을 선택합니다.
2단계 테이블에서 비활성화할 syslog를 선택한 다음 **Edit**를 클릭합니다.
Edit Syslog ID Settings 대화 상자가 나타납니다.
3단계 **Disable messages** 확인란을 선택한 후 **OK**를 클릭합니다.

Syslog 메시지의 심각도 수준 변경

syslog 메시지의 심각도 수준을 변경하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Syslog Setup**을 선택합니다.
2단계 테이블에서 심각도 수준을 변경할 syslog를 선택한 후 **Edit**를 클릭합니다.
Edit Syslog ID Settings 대화 상자가 나타납니다.
3단계 **Logging Level** 드롭다운 목록에서 원하는 심각도 수준을 선택한 다음 **OK**를 클릭합니다.

Syslog 메시지 생성 속도 제한

syslog 메시지 생성 속도를 제한하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Logging > Rate Limit**을 선택합니다.

2단계 속도 제한을 할당할 로깅 수준(메시지 심각도 수준)을 선택합니다. 심각도 수준은 다음과 같이 정의됩니다.

설명	심각도
긴급	0—시스템을 사용할 수 없음
알림	1—즉각적인 행동 필요
위험	2—심각한 상태
오류	3—오류 상태
경고	4—경고 상태
알림	5—정상적이나 중요한 상태
정보	6—정보 메시지만 해당
디버깅	7—디버깅만 해당

3단계 메시지 수 필드는 전송된 메시지 개수를 표시합니다. 간격(초) 필드는 이 로깅 수준에서 전송할 수 있는 메시지 수 제한에 사용되는 간격을 초 단위로 표시합니다. 테이블에서 로깅 수준을 선택하고 **Edit**를 클릭하여 **Edit Rate Limit for Syslog Logging Level** 대화 상자를 표시합니다.

4단계 계속하려면 40-22 페이지의 개별 Syslog 메시지에 대한 속도 제한 할당 또는 변경를 참조하십시오.

개별 Syslog 메시지에 대한 속도 제한 할당 또는 변경

개별 syslog 메시지에 대한 속도 제한을 할당하거나 변경하려면 다음 단계를 수행하십시오.

절차

1단계 특정 syslog 메시지의 속도 제한을 할당하려면 **Add**를 클릭하여 **Add Rate Limit for Syslog Message** 대화 상자를 표시합니다.

2단계 계속하려면 40-23 페이지의 Syslog 메시지 속도 제한 추가 또는 변경를 참조하십시오.

3단계 특정 syslog 메시지의 속도 제한을 변경하려면 **Edit**를 클릭하여 **Edit Rate Limit for Syslog Message** 대화 상자를 표시합니다.

4단계 계속하려면 40-23 페이지의 Syslog 심각도 수준에 대한 속도 제한을 변경를 참조하십시오.

Syslog 메시지 속도 제한 추가 또는 변경

특정 syslog 메시지에 대한 속도 제한을 추가하거나 변경하려면 다음 단계를 수행하십시오.

절차

1단계 특정 syslog 메시지에 속도 제한을 추가하려면 **Add**를 클릭하여 **Add Rate Limit for Syslog Message** 대화 상자를 표시합니다. syslog 메시지에 대한 속도 제한을 변경하려면 **Edit**를 클릭하여 **Edit Rate Limit for Syslog Message** 대화 상자를 표시합니다.

2단계 제한하려는 syslog 메시지의 메시지 ID를 입력합니다.

3단계 지정된 시간 간격 동안 전송 가능한 최대 메시지 수를 입력합니다.

4단계 특정 메시지의 속도를 제한하는 데 사용할 시간을 초 단위로 입력한 후 **OK**를 클릭합니다.

참고 메시지를 무제한 허용하려면 **Number of Messages** 및 **Time Interval** 필드를 모두 비워둡니다.

Syslog 심각도 수준에 대한 속도 제한을 변경

지정된 syslog 심각도 수준의 속도 제한을 변경하려면 다음 단계를 수행하십시오.

절차

1단계 이 심각도 수준에서 전송 가능한 최대 메시지 개수를 입력합니다.

2단계 이 심각도 수준에서 메시지 속도 제한에 사용할 시간을 초 단위로 입력한 후 **OK**를 클릭합니다.

선택한 메시지 심각도 수준이 나타납니다.

참고 메시지를 무제한 허용하려면 **Number of Messages** 및 **Time Interval** 필드를 모두 비워둡니다.

로그 모니터링

로깅 상태 모니터링을 위해 다음 screens를 참조합니다.

- **Monitoring > Logging > Log Buffer > View**
- **Monitoring > Logging > Real-Time Log Viewer > View**
- **Tools > Command Line Interface**

  이 창에서는 다양한 비 대화형 명령을 내보내고 결과를 볼 수 있습니다.

로그 뷰어를 통한 Syslog 메시지 필터링

실시간 로그 뷰어와 로그 버퍼 뷰어의 열에 대응하는 하나 이상의 값을 기준으로 syslog 메시지를 필터링할 수 있습니다.

로그 뷰어 중 하나를 통해 syslog 메시지를 필터링하려면 다음 단계를 수행하십시오.

절차

1단계 다음 옵션 중 하나를 선택합니다.

- **Monitoring > Logging > Real-Time Log Viewer > View**
- **Monitoring > Logging > Log Buffer > View**

2단계 **Real-Time Log Viewer** 또는 **Log Buffer Viewer** 대화 상자에서 도구 모음의 **Build Filter**를 클릭합니다.

3단계 **Build Filter** 대화 상자에서 syslog 메시지에 적용할 필터링 기준을 지정합니다.

a. **Date and Time** 영역에서 실시간, 특정 시간 또는 시간 범위의 3가지 옵션 중 하나를 선택합니다. 특정 시간을 선택하는 경우 숫자를 입력하고 드롭다운 목록에서 시간과 분을 선택함으로써 시간을 표시합니다. 시간 범위를 선택하는 경우 **Start Time** 필드에서 드롭다운 화살표를 클릭하여 달력을 표시합니다. 드롭다운 목록에서 시작 날짜와 시작 시간을 선택한 후 **OK**를 클릭합니다. **End Time** 필드의 드롭다운 화살표를 클릭하여 달력을 표시합니다. 드롭다운 목록에서 종료 날짜와 종료 시간을 선택한 후 **OK**를 클릭합니다.

b. **Severity** 필드에서 유효한 심각도 수준을 입력합니다. 또는 **Edit** 아이콘을 **Severity** 필드 오른쪽에서 클릭합니다. 목록에서 필터링할 심각도 수준을 클릭합니다. 심각도 수준 1-7을 포함하려면 **All**을 클릭합니다. **OK**를 클릭하여 **Build Filter** 대화 상자에서 이러한 설정을 표시합니다. 올바른 입력 형식에 관한 추가 정보를 보려면 **Info** 아이콘(**Severity** 필드 오른쪽)을 클릭합니다.

c. **Syslog ID** 필드에 올바른 syslog ID를 입력합니다. 또는 **Edit** 아이콘을 **Syslog ID** 필드 오른쪽에서 클릭합니다. 드롭다운 목록에서 필터링 대상을 선택하고 **Add**를 클릭합니다. **OK**를 클릭하여 **Build Filter** 대화 상자에서 이러한 설정을 표시합니다. 올바른 입력 형식에 관한 추가 정보를 보려면 **Info** 아이콘(**Syslog ID** 필드 오른쪽)을 클릭합니다.

d. 유효한 소스 IP 주소를 **Source IP Address** 필드에 입력하거나 **Edit** 아이콘(**Source IP Address** 필드 오른쪽)을 클릭합니다. 단일 IP 주소 또는 지정된 범위의 IP 주소를 선택한 후 **Add**를 클릭합니다. **Do not include (exclude) this address or range** 확인란을 선택하여 특정 IP 주소나 IP 주소 범위를 제외하고 **OK**를 클릭하여 이러한 설정을 **Build Filter** 대화 상자에 표시합니다. 올바른 입력 형식에 관한 추가 정보를 보려면 **Info** 아이콘(**Source IP Address** 필드 오른쪽)을 클릭합니다.

e. **Source Port** 필드에 유효한 소스 포트를 입력하거나 **Edit** 아이콘(**Source Port** 필드 오른쪽)을 클릭합니다. 드롭다운 목록에서 필터링 대상을 선택하고 **Add**를 클릭합니다. **OK**를 클릭하여 **Build Filter** 대화 상자에서 이러한 설정을 표시합니다. 올바른 입력 형식에 관한 추가 정보를 보려면 **Info** 아이콘(**Source Port** 필드 오른쪽)을 클릭합니다.

f. 유효한 대상 IP 주소를 **Detination IP Address** 필드에 입력하거나 **Edit** 아이콘(**Destination IP Address** 필드 오른쪽)을 클릭합니다. 단일 IP 주소 또는 지정된 범위의 IP 주소를 선택한 후 **Add**를 클릭합니다. **Do not include (exclude) this address or range** 확인란을 선택하여 특정 IP 주소 또는 IP 주소 범위를 제외합니다. **OK**를 클릭하여 **Build Filter** 대화 상자에서 이러한 설정을 표시합니다. 올바른 입력 형식에 관한 추가 정보를 보려면 **Info** 아이콘(**Destination IP Address** 필드 오른쪽)을 클릭합니다.

g. **Destination Port** 필드에 유효한 대상 포트를 입력하거나 **Edit** 아이콘(**Destination Port** 필드 오른쪽)을 클릭합니다. 드롭다운 목록에서 필터링 대상을 선택하고 **Add**를 클릭합니다. **OK**를 클릭하여 **Build Filter** 대화 상자에서 이러한 설정을 표시합니다. 올바른 입력 형식에 관한 추가 정보를 보려면 **Info** 아이콘(**Destination Port** 필드 오른쪽)을 클릭합니다.

h. **Description** 필드에 대한 필터링 텍스트를 입력합니다. 텍스트는 정규식을 포함하여 하나 이상의 문자를 포함한 어떤 문자열이라도 될 수 있습니다. 그러나 세미콜론은 유효한 문자가 아니며 이 설정은 대/소문자를 구분합니다. 다중 엔트리는 쉼표로 구분해야 합니다.

i. **OK**를 클릭하여 방금 지정한 필터 설정을 로그 뷰어의 **Filter By** 드롭다운 목록에 추가합니다. 필터 문자열은 특정 형식을 따릅니다. 접두사 FILTER: **Filter By** 드롭다운 목록에 표시되는 모든 사용자 지정 필터를 지정합니다. 이 필드에 임의의 텍스트를 입력할 수도 있습니다.

   다음 테이블은 사용되는 형식의 예를 보여줍니다.

Build Filter 예제	필터 문자열 형식
Source IP = 192.168.1.1 or 0.0.0.0 Source Port = 67	FILTER: srcIP=192.168.1.1,0.0.0.0;srcPort=67;
Severity = Informational Destination IP = 1.1.1.1 through 1.1.1.10	FILTER: sev=6;dstIP=1.1.1.1-1.1.1.10;
Syslog ID not in the range 725001 through 725003	FILTER: sysID=!725001-725003;
Source IP = 1.1.1.1 Description = Built outbound	FILTER: srcIP=1.1.1.1;descr=Built outbound

4단계 **Filter By** 드롭다운 목록의 설정 하나를 선택하여 syslog 메시지를 필터링한 후 도구 모음의 **Filter**를 클릭합니다. 이 설정은 모든 향후 syslog 메시지에도 적용됩니다. 도구 모음에서 **Show All**을 클릭하여 모든 필터를 제거합니다.

참고 **Build Filter** 대화 상자에서 지정한 필터를 저장할 수 없습니다. 이러한 필터는 필터가 생성된 ASDM 세션에 대해서만 유효합니다.

필터링 설정 편집

Build Filter 대화 상자를 이용하여 생성한 필터링 설정을 편집하려면 다음 단계를 수행하십시오.

절차

1단계 다음 옵션 중 하나를 선택합니다.

- **Filter By** 드롭다운 목록에 변경 사항을 직접 입력하여 필터를 수정합니다.
- **Filter By** 드롭다운 목록에서 필터를 선택한 후 **Build Filter**를 클릭하여 **Build Filter** 대화 상자를 표시합니다. **Clear Filter**를 클릭하여 현재 필터 설정을 제거하고 새 필터를 입력합니다. 아니면 나타나는 설정을 변경하고 **OK**를 클릭합니다.

참고 이러한 필터 설정은 **Build Filter** 대화 상자에 정의된 것에만 적용됩니다.

- 도구 모음의 **Show All**을 클릭하여 필터링을 중단하고 모든 syslog 메시지를 표시합니다.

로그 뷰어를 사용하여 특정 명령을 발행

로그 뷰어를 사용하여 **ping**, **traceroute**, **whois** 및 **dns lookup** 명령을 발행할 수 있습니다.

이 명령어를 실행하려면 다음 단계를 수행하십시오.

절차

1단계 다음 옵션 중 하나를 선택합니다.

- **Monitoring > Logging > Real-Time Log Viewer > View**
- **Monitoring Logging > Log Buffer > View**

2단계 **Tools** (**Real-Time Log Viewer** 또는 **Log Buffer** 창)를 클릭한 후 실행할 명령을 선택합니다. 또는 목록의 특정 syslog 메시지를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 표시하고 실행하려는 명령을 선택할 수 있습니다.

Entering command 대화 상자가 나타나고 드롭다운 목록에 선택한 명령어가 자동으로 표시됩니다.

3단계 선택한 syslog 메시지의 소스 또는 대상 IP 주소를 **Address** 필드에 입력한 후 **Go**를 클릭합니다.

제공된 영역에 명령 출력이 표시됩니다.

4단계 **Clear**를 클릭하여 출력을 제거하고 드롭다운 목록에서 실행할 다른 명령을 선택합니다. 필요한 경우 3단계를 반복합니다. 완료하면 **Close**를 클릭합니다.

로깅 내역

표 40-2 로깅 내역

기능 이름	플랫폼 릴리스	설명
로깅	7.0(1)	다양한 출력 대상을 통해 ASA 네트워크 로깅 정보를 제공하며 로그 파일을 보고 저장할 수 있는 옵션을 포함합니다. 다음 화면을 도입했습니다. Configuration > Device Management > Logging > Logging Setup
속도 제한	7.0(4)	syslog 메시지가 생성되는 속도를 제한합니다. 다음 화면을 수정했습니다. Configuration > Device Management > Logging > Rate Limit

표 40-2 로깅 내역 (계속)

기능 이름	플랫폼 릴리스	설명
로깅 목록	7.2(1)	다른 명령에서 다양한 기준(로깅 수준, 이벤트 클래스 및 메시지 ID)으로 메시지를 지정하는 데 사용할 로깅 목록을 생성합니다. 다음 화면을 수정했습니다. Configuration > Device Management > Logging > Event Lists
안전한 로깅	8.0(2)	원격 로깅 호스트로의 연결이 SSL/TLS를 사용할지 지정합니다. 이 옵션은 선택된 프로토콜이 TCP인 경우에만 유효합니다. 다음 화면을 수정했습니다. Configuration > Device Management > Logging > Syslog Server
로깅 클래스	8.0(4), 8.1(1)	ipaa 이벤트 클래스 로깅 메시지에 대한 지원이 추가되었습니다. 다음 화면을 수정했습니다. Configuration > Device Management > Logging > Logging Filters
로깅 클래스 및 저장된 로깅 버퍼	8.2(1)	dap 이벤트 클래스 로깅 메시지에 대한 지원이 추가되었습니다. 저장된 로깅 버퍼 지우기에 대한 지원이 추가되었습니다(ASDM, 내부, FTP 및 플래시). 다음 화면을 수정했습니다. Configuration > Device Management > Logging > Logging Setup
비밀번호 암호화	8.3(1)	비밀번호 암호화 지원이 추가되었습니다.
로그 뷰어	8.3(1)	로그 뷰어에 소스 및 대상 IP 주소가 추가되었습니다.
향상된 로깅 및 연결 차단	8.3(2)	TCP를 사용하도록 syslog 서버를 구성하고 syslog 서버를 사용할 수 없는 경우 ASA은(는) 서버를 다시 사용할 수 있을 때까지 syslog 메시지를 생성하는 새로운 연결을 차단합니다(예: VPN, 방화벽 및 cut-through-proxy 연결). 이 기능은 ASA의 로깅 대기열이 가득 찼을 때도 새로운 연결을 차단하도록 개선되었습니다. 로깅 대기열이 비워지면 연결이 재개됩니다. 이 기능은 EAL4 공통 평가 기준 준수를 위해 추가되었습니다. 요청이 없다면 syslog 메시지를 보내거나 받을 수 없을 때 연결을 허용할 것을 권장합니다. 연결을 허용하려면 계속해서을 사용하십시오. **Allow user traffic to pass when TCP syslog server is down** 확인란(Configuration > Device Management > Logging > Syslog Servers 창)을 선택하십시오. 다음 syslog 메시지를 도입했습니다. 414005, 414006, 414007 및 414008 ASDM 화면은 수정하지 않았습니다.

표 40-2 로깅 내역 (계속)

기능 이름	플랫폼 릴리스	설명
Syslog 메시지 필터링 및 정렬	8.4(1)	다음에 대한 지원이 추가되었습니다. • 다양한 열에 대응하는 여러 문자열을 기준으로 하는 Syslog 메시지 필터링 • 사용자 정의 필터의 생성 • 메시지의 열 정렬. 자세한 내용은 ASDM 컨피그레이션 가이드을(를) 참고하십시오. 다음 화면을 수정했습니다. Monitoring > Logging > Real-Time Log Viewer > View. Monitoring > Logging > Log Buffer Viewer > View. 이 기능은 모든 ASA 버전과 상호 운용됩니다.
클러스터링	9.0(1)	ASA 5580 및 5585-X에서의 클러스터링 환경에서 syslog 메시지 생성에 대한 지원을 추가했습니다. Configuration > Logging > Syslog Setup > Advanced > Advanced Syslog Configuration 화면을 수정했습니다.

SNMP

이 장에서는 Cisco ASA을(를) 모니터링하기 위한 SNMP(Simple Network Management Protocol) 구성 방법을 설명합니다.

SNMP 소개

SNMP는 네트워크 디바이스 간의 관리 정보 교환을 촉진하기 위한 애플리케이션 계층 프로토콜이며 TCP/IP 프로토콜 군의 일부입니다. ASA, ASAv 및 ASASM은(는) SNMP 버전 1, 2c 및 3을 사용하여 네트워크 모니터링을 지원하고 모든 3개 버전의 동시 사용도 지원합니다. 인터페이스에서 실행되는 SNMP 에이전트를 사용하면 HP OpenView와 같은 NMS(네트워크 관리 시스템)을 통해 ASA ASA 및 ASASM을(를) 모니터링할 수 있습니다. ASA, ASAv 및 ASASM은(는) GET 요청 발행을 통해 SNMP 읽기 전용 액세스를 지원합니다. SNMP 쓰기 액세스는 허용되지 않으므로 SNMP를 사용하여 변경할 수는 없습니다. 또한 SNMP SET 요청은 지원되지 않습니다.

ASA, ASAv 및 ASASM을(를) NMS로의 특정 이벤트(알림 포함)에 대해 관리 디바이스에서 관리 스테이션으로 전송되는 요청하지 않은 메시지인 트랩을 보내도록 구성하거나 NMS를 사용하여 ASA에서 MIB(Management Information Bases)를 찾아볼 수 있습니다. MIB는 정의 모음이고 ASA, ASAv 및 ASASM은 각 정의에 대한 값 데이터베이스를 유지합니다. MIB를 찾아보는 것은 NMS에서 MIB 트리에 대한 일련의 GET-NEXT 또는 GET-BULK 요청을 발행하는 것을 의미합니다.

ASA, ASAv 및 ASASM에는 예를 들어 네트워크 링크가 실행 또는 중단 상태로 전환될 때 알림이 필요하도록 사전 정의된 이벤트가 발생하는 경우 지정된 관리 스테이션에 알려주는 SNMP 에이전트가 있습니다. 이때 보내는 알림은 관리 스테이션에 스스로를 식별하는 SNMP OID를 포함합니다. ASA,ASAv 또는ASASM SNMP 에이전트는 관리 스테이션이 정보를 요구할 때 응답하기도 합니다.

SNMP 용어

표 41-1은(는) SNMP에서 작업할 때 일반적으로 쓰이는 용어를 나열합니다.

표 41-1 SNMP 용어

용어	설명
에이전트	ASA에서 실행되는 SNMP 서버입니다. SNMP 에이전트는 다음과 같은 특징을 갖습니다. • 정보 요청 및 네트워크 관리 스테이션의 작업에 대해 응답합니다. • SNMP 관리자가 보거나 변경할 수 있는 객체 모음인 MIB(Management Information Base)에 대한 액세스를 제어합니다. • SET 작업을 허용하지 않습니다.
브라우징	디바이스의 SNMP 에이전트에서 필요한 정보를 폴링함으로써 네트워크 관리 스테이션에서 해당 디바이스의 상태를 모니터링합니다. 이 작업은 값을 결정하기 위해 네트워크 관리 스테이션에서 MIB 트리에 대한 일련의 GET-NEXT 또는 GET-BULK 요청을 생성하는 것을 포함할 수 있습니다.
MIB(Management Information Base)	패킷, 연결, 버퍼, 장애 조치 등에 관한 정보를 수집하기 위한 표준화된 데이터 구조입니다. MIB는 대부분의 네트워크 디바이스에서 사용되는 제품, 프로토콜 및 하드웨어 표준으로 정의됩니다. SNMP 네트워크 관리 스테이션은 MIB를 찾아보고 특정 데이터나 이벤트 전송을 실시간으로 요청할 수 있습니다.
NMS(Network Management Station)	SNMP 이벤트를 모니터링하고 ASA, ASAv 및 ASASM 등의 디바이스를 관리하도록 설정된 PC나 워크스테이션입니다.
OID(Object Identifier)	NMS에서 디바이스를 식별하고 사용자에게 모니터링 및 표시되는 정보의 소스를 보여주는 시스템입니다.
트랩	SNMP 에이전트에서 NMS로 메시지를 생성하는 사전 정의된 이벤트입니다. 이벤트는 linkup, linkdown, coldstart, warmstart, authentication 또는 syslog messages와 같은 경보 조건을 포함합니다.

SNMP 버전 3 개요

SNMP 버전 3은 SNMP 버전 1 또는 버전 2c에는 제공되지 않는 향상된 보안을 제공합니다. SNMP 버전 1 및 2c는 일반 텍스트로 SNMP 서버와 SNMP 에이전트 간에 데이터를 전송합니다. SNMP 버전 3은 프로토콜 작동을 보호하기 위한 인증 및 프라이버시 옵션을 추가합니다. 또한 이 버전은 USM(User-based Security Model) 및 VACM(View-based Access Control Model)을 통해 SNMP 에이전트와 MIB 객체에 대한 액세스를 제어합니다. ASA 및 ASASM 또한 SNMP 그룹 및 사용자는 물론 호스트 생성을 지원하며 이는 안전한 SNMP 통신을 위한 전송 인증 및 암호화 활성화를 위해 필요합니다.

보안 모델

컨피그레이션을 위해 인증 및 프라이버시 옵션은 보안 모델로 그룹화됩니다. 보안 모델은 사용자와 그룹에 적용되며 다음 3개 유형으로 나누어집니다.

- NoAuthPriv—No Authentication and No Privacy로 메시지에 보안이 적용되지 않음을 의미합니다.
- AuthNoPriv—Authentication but No Privacy로 메시지가 인증을 받음을 의미합니다.
- AuthPriv—Authentication and Privacy로 메시지가 인증을 받고 암호화됨을 의미합니다.

SNMP 그룹

SNMP 그룹은 사용자를 추가할 수 있는 액세스 제어 정책입니다. 각 SNMP 그룹은 보안 모델로 구성되며 SNMP 보기와 연결됩니다. SNMP 그룹 내의 사용자는 SNMP 그룹의 보안 모델과 일치해야 합니다. 이러한 매개 변수는 SNMP 그룹 내 사용자가 이용하는 인증 및 프라이버시 유형을 지정합니다. 각 SNMP 그룹 이름 및 보안 모델 쌍은 고유해야 합니다.

SNMP 사용자

SNMP 사용자는 지정된 사용자 이름, 사용자가 속하는 그룹, 인증 비밀번호, 암호화 비밀번호 및 승인, 그리고 사용할 암호화 알고리즘을 가져야 합니다. 인증 알고리즘 옵션은 MD5와 SHA입니다. 암호화 알고리즘 옵션은 DES, 3DES 및 AES(128, 192 및 256 버전으로 이용 가능)입니다. 사용자를 생성할 때 반드시 SNMP 그룹과 연결해야 합니다. 그러면 사용자에게 그룹의 보안 모델이 상속됩니다.

SNMP 호스트

SNMP 호스트는 SNMP 알림 및 트랩이 전송되는 IP 주소입니다. 트랩은 구성된 사용자에게만 전송되기 때문에 SNMP 버전 3 호스트를 대상 IP 주소와 함께 구성하려면 사용자 이름을 구성해야 합니다. SNMP 대상 IP 주소 및 대상 매개 변수 이름은 ASA 및 ASA Services Module에서 고유해야 합니다. 각 SNMP 호스트는 연결된 하나의 사용자 이름만 가질 수 있습니다. SNMP 트랩을 수신하려면 SNMP NMS를 구성하고 ASA 및 ASASM에 대한 자격 증명과 일치하도록 NMS의 사용자 자격 증명을 구성해야 합니다.

ASA, ASA Services Module 및 Cisco IOS 소프트웨어의 구현 차이

ASA 및 ASASM에서 SNMP 버전 3 구현은 Cisco IOS 소프트웨어에서의 SNMP 버전 3 구현과 다음과 같은 차이가 있습니다.

- 로컬 엔진 및 원격 엔진 ID를 구성할 수 없습니다. 로컬 엔진 ID는 ASA 또는 ASASM이(가) 시작할 때 또는 컨텍스트가 생성될 때 생성됩니다.
- 무제한 MIB 브라우징을 야기하는 보기 기반 액세스 제어는 지원되지 않습니다.
- 지원은 다음 MIB로 제한됩니다. USM, VACM, FRAMEWORK 및 TARGET
- 정확한 보안 모델로 사용자 및 그룹을 생성해야 합니다.
- 사용자, 그룹 및 호스트를 올바른 순서로 제거해야 합니다.
- **snmp-server host** 명령을 사용하면 SNMP 트래픽 허용을 위한 ASA, ASAv 또는 ASASM 규칙이 생성됩니다.

SNMP Syslog 메시징

SNMP는 212*nnn* 형식으로 번호가 매겨지는 상세한 syslog 메시지를 생성합니다. Syslog 메시지는 ASA 또는 ASASM에서 특정 인터페이스의 지정된 호스트로 SNMP 요청, SNMP 트랩, SNMP 채널 및 SNMP 응답의 상태를 알려줍니다.

syslog 메시지에 대한 자세한 설명은 syslog 메시지 가이드을(를) 참조하십시오.

참고 SNMP syslog 메시지가 높은 속도(초당 약 4000)를 초과하면 SNMP 폴링이 실패합니다.

애플리케이션 서비스 및 타사 도구

SNMP 지원에 대한 자세한 내용은 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

SNMP 버전 3 MIB를 위한 타사 도구 사용에 관한 정보는 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP용 지침

장애 조치 지침

각 ASA, ASAv 또는 ASASM의 SNMP 클라이언트는 피어와 엔진 데이터를 공유합니다. 엔진 데이터는 SNMP-FRAMEWORK-MIB의 engineID, engineBoots 및 engineTime 객체를 포함합니다. 엔진 데이터는 flash:/snmp/*contextname*에 바이너리 파일로 저장됩니다.

IPv6 지침

IPv6를 지원하지 않습니다.

추가 지침

- Cisco Works for Windows 또는 다른 SNMP MIB-II 규격 브라우저가 있어야 SNMP 트랩을 수신하거나 MIB를 찾아볼 수 있습니다.
- 보기 기반 액세스 제어를 지원하지 않지만 VACM MIB를 이용한 브라우징으로 기본 보기 설정을 결정할 수 있습니다.
- ENTITY-MIB는 비관리 컨텍스트에서 이용할 수 없습니다. 비관리 컨텍스트에서는 IF-MIB를 대신 사용하십시오.
- AIP SSM 또는 AIP SSC를 위한 SNMP 버전 3을 지원하지 않습니다.
- SNMP 디버깅을 지원하지 않습니다.
- ARP 정보 검색을 지원하지 않습니다.
- SNMP SET 명령어를 지원하지 않습니다.
- NET-SNMP 버전 5.4.2.1을 사용할 때는 AES128 버전의 암호화 알고리즘만 지원합니다. AES256 또는 AES192의 암호화 알고리즘 버전은 지원하지 않습니다.
- 기존 컨피그레이션을 변경했을 때 SNMP 기능이 일관성을 잃게 되면 변경이 거부됩니다.
- SNMP 버전 3의 경우 그룹, 사용자, 호스트 순서로 컨피그레이션이 이루어져야 합니다.
- 그룹을 삭제하기 전에 해당 그룹에 연결된 모든 사용자가 삭제되었는지 확인해야 합니다.
- 사용자를 삭제하기 전에 해당 사용자 이름과 연결된 호스트가 구성되지 않았는지 확인해야 합니다.
- 사용자가 특정 보안 모델 내에서 특정 그룹에 속하도록 구성되어 있고 해당 그룹의 보안 수준이 변경되는 경우 다음을 순서대로 수행해야 합니다.
  - 해당 그룹에서 사용자를 제거합니다.
  - 그룹 보안 수준을 변경합니다.
  - 새 그룹에 속한 사용자를 추가합니다.

- MIB 객체 하위 집합에 대한 사용자 액세스를 제한하기 위한 맞춤 보기 생성은 지원되지 않습니다.
- 모든 요청 및 트랩은 기본 읽기/알림 보기에서만 이용 가능합니다.
- connection-limit-reached 트랩은 관리 컨텍스트에서 생성됩니다. 이 트랩을 생성하려면 연결 제한에 도달한 사용자 컨텍스트에서 SNMP 서버 호스트가 1개 이상 구성되어 있어야 합니다.
- ASA 5585 SSP-40(NPE)의 섀시 온도를 쿼리할 수 없습니다.
- NMS가 성공적으로 객체를 요청할 수 없거나 ASA(으)로부터 수신 트랩을 제대로 처리할 수 없으면 패킷 캡처를 수행하는 것이 문제를 확인하는 유용한 방법입니다. **Wizards > Packet Capture Wizard**를 선택하고 화면상의 지침에 따릅니다.
- 최대 4000개의 호스트를 추가할 수 있습니다. 하지만 이 중 128개만 트랩에 사용할 수 있습니다.
- 지원되는 액티브 폴링 대상의 총수는 128개입니다.
- 네트워크 객체를 지정하여 호스트 그룹으로 추가할 개별 호스트를 나타낼 수 있습니다.
- 하나의 호스트에 사용자를 두 명 이상 연결할 수 있습니다.
- 다른 **host-group** 명령어에서 겹치는 네트워크 객체를 지정할 수 있습니다. 마지막 호스트 그룹에 대해 지정하는 값은 다른 네트워크 객체의 호스트 공통 집합에서 적용됩니다.
- 다른 호스트 그룹과 겹치는 호스트 그룹 또는 호스트를 삭제할 경우 호스트는 구성된 호스트 그룹에서 지정된 값으로 다시 설정됩니다.
- 호스트가 획득하는 값은 명령 실행에 사용하는 지정된 순서에 따라 다릅니다.
- SNMP가 보내는 메시지 크기의 한도는 1472바이트입니다.
- 클러스터 구성원은 SNMPv3 엔진 ID를 동기화하지 않습니다. 따라서 클러스터의 각 유닛은 고유한 SNMPv3 사용자 컨피그레이션을 가져야 합니다.

SNMP 구성

이 섹션에서는 SNMP 구성 방법을 설명합니다.

1단계 SNMP 에이전트 및 SNMP 서버를 활성화합니다. 41-6 페이지의 SNMP 에이전트 및 SNMP 서버를 활성화합니다.를 참조하십시오.

2단계 SNMP 관리 스테이션을 구성하여 ASA(으)로부터 요청을 수신합니다. 41-6 페이지의 SNMP 관리 스테이션 구성를 참조하십시오.

3단계 SNMP 트랩을 구성합니다. 41-7 페이지의 SNMP 트랩 구성를 참조하십시오.

4단계 SNMP 버전 1 및 2c 매개 변수 또는 SNMP 버전 3 매개 변수를 구성합니다. 41-7 페이지의 SNMP 버전 1 또는 2c에 대한 매개 변수 구성 또는 41-8 페이지의 SNMP 버전 3에 대한 매개변수 구성를 참조하십시오.

SNMP 에이전트 및 SNMP 서버를 활성화합니다.

SNMP 에이전트 및 SNMP 서버를 활성화하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Management Access > SNMP**를 선택합니다. SNMP 서버는 기본적으로 활성화되어 있습니다.

2단계 계속하려면 41-6 페이지의 SNMP 관리 스테이션 구성를 참조하십시오.

SNMP 관리 스테이션 구성

SNMP 관리 스테이션을 구성하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Management Access > SNMP**를 선택합니다.

2단계 **SNMP 관리 스테이션** 창에서 **Add**를 클릭합니다.

SNMP 호스트 액세스 항목 추가 대화 상자가 나타납니다.

3단계 SNMP 호스트가 상주하는 인터페이스를 선택합니다.

4단계 SNMP 호스트 IP 주소를 입력합니다.

5단계 SNMP 호스트 UDP 포트를 입력하거나 기본값인 포트 162를 유지합니다.

6단계 SNMP 호스트 커뮤니티 문자열을 추가합니다. 관리 스테이션에 대한 커뮤니티 문자열이 지정되지 않은 경우 **SNMP 관리 스테이션** 창에서 **커뮤니티 문자열**(기본) 필드에 설정된 값이 사용됩니다.

7단계 SNMP 호스트가 사용하는 SNMP 버전을 선택하십시오.

8단계 이전 단계에서 SNMP 버전 3을 선택한 경우 구성된 사용자의 이름을 선택합니다.

9단계 이 NMS와의 통신 방식을 지정하려면 **Poll** 또는 **Trap** 확인란을 선택합니다.

10단계 **OK**를 클릭합니다.

SNMP 호스트 액세스 항목 추가 대화 상자가 닫힙니다.

11단계 **Apply**를 클릭합니다.

NMS가 컨피그레이션되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다. SNMP 버전 3 NMS 도구에 관한 자세한 정보는 다음 URL을 참조하십시오.

http://www.cisco.com/en/US/docs/security/asa/asa82/snmp/snmpv3_tools.html

SNMP 트랩 구성

SNMP 에이전트가 생성하는 트랩과 그것이 수집되어 NMS로 전송되는 방식을 지정하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Management Access > SNMP**를 선택합니다.

2단계 **Configure Traps**를 클릭합니다.

SNMP Trap Configuration 대화 상자가 나타납니다.

3단계 **SNMP Server Traps Configuration** 확인란을 선택합니다.

트랩은 다음 범주로 구분됩니다. 표준, IKEv2, 엔티티 MIB, IPsec, 원격 액세스, 리소스, NAT, syslog, CPU 사용률, CPU 사용률 및 모니터링 간격 및 SNMP 인터페이스 임계값 및 간격 SNMP 트랩을 통해 SNMP 이벤트를 알리려면 해당 확인란을 선택합니다. 기본 컨피그레이션에서는 모든 SNMP 표준 트랩이 활성화되어 있습니다. 트랩 유형을 지정하지 않으면 기본값은 syslog 트랩입니다. 기본 SNMP 트랩이 syslog 트랩과 함께 활성화를 유지합니다. 모든 다른 트랩은 기본적으로 비활성화되어 있습니다. 트랩을 비활성화하려면 해당 확인란 선택을 취소합니다. syslog 트랩 심각도를 구성하려면 **Configuration > Device Management > Logging > Logging Filters**를 선택합니다.

4단계 **OK**를 클릭하여 **SNMP Trap Configuration** 대화 상자를 닫습니다.

5단계 **Apply**를 클릭합니다.

SNMP 트랩이 컨피그레이션되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

SNMP 버전 1 또는 2c에 대한 매개 변수 구성

SNMP 버전 1 또는 2c에 대한 매개 변수를 구성하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Management Access > SNMP**를 선택합니다.

2단계 SNMP 버전 1 또는 2c를 사용 중인 경우 **Community String**(기본) 필드에 커뮤니티 문자열을 입력합니다. ASA에 요청을 보낼 때 SNMP NMS가 사용하는 비밀번호를 입력합니다. SNMP 커뮤니티 문자열은 SNMP NMS와 관리 대상 네트워크 노드 사이에서 비밀로 공유됩니다. ASA은(는) 이 비밀번호를 사용하여 수신 SNMP 요청이 유효한지 판단합니다. 비밀번호는 대/소문자를 구분하며 최대 32자의 영숫자입니다. 공백은 허용되지 않습니다. 기본값은 공개됩니다. SNMP 버전 2c에서는 각 NMS에 대해 별도의 커뮤니티 문자열을 설정할 수 있습니다. NMS에 대해 커뮤니티 문자열이 구성되지 않은 경우 기본적으로 여기서 설정된 값이 사용됩니다.

3단계 ASA 시스템 관리자의 이름을 입력합니다. 텍스트는 대/소문자를 구분하며 최대 127자의 영문자입니다. 공백이 허용되지만 여러 개의 공백은 하나의 공백으로 단축됩니다.

4단계 SNMP가 관리하는 ASA의 위치를 입력합니다. 텍스트는 대/소문자를 구분하며 최대 127자까지 가능합니다. 공백이 허용되지만 여러 개의 공백은 하나의 공백으로 단축됩니다.

5단계 NMS로부터 SNMP 요청을 듣는 ASA 포트의 번호를 입력하거나 기본값인 161번으로 유지합니다.

6단계 **SNMP Host Access List** 창의 **Add**를 클릭합니다.

SNMP 호스트 액세스 항목 추가 대화 상자가 나타납니다.

7단계 드롭다운 목록에서 트랩이 전송되는 인터페이스 이름을 선택합니다.

8단계 ASA에 연결할 수 있는 NMS 또는 SNMP 관리자의 IP 주소를 입력합니다.

9단계 UDP 포트 번호를 입력합니다. 기본값은 162입니다.

10단계 드롭다운 목록에서 사용 중인 SNMP 버전을 선택합니다. 버전 1 또는 버전 2c를 선택하면 커뮤니티 문자열을 입력해야 합니다. 버전 3을 선택하면 드롭다운 목록에서 사용자 이름을 선택해야 합니다.

11단계 **Server Poll/Trap Specification** 영역에서 **Poll** 확인란을 선택하여 NMS를 요청 전송(폴링)으로만 제한합니다. NMS를 트랩 수신으로만 제한하려면 **Trap** 확인란을 선택합니다. 두 확인란을 모두 선택하면 SNMP 호스트의 두 기능을 모두 수행할 수 있습니다.

12단계 **OK**를 클릭하여 **Add SNMP Host Access Entry** 대화 상자를 닫습니다.

새로운 호스트가 **SNMP Host Access List** 창에 나타납니다.

13단계 **Apply**를 클릭합니다.

버전 1, 2c 또는 3에 대한 SNMP 매개변수가 컨피그레이션되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

SNMP 버전 3에 대한 매개변수 구성

SNMP 버전 3에 대한 매개변수를 구성하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Management Access > SNMP**를 선택합니다.

2단계 **SNMPv3 Users** 창의 **SNMPv3 User/Group** 탭에서 **Add > SNMP User**를 클릭하여 구성된 사용자 또는 신규 사용자를 그룹에 추가합니다. 그룹의 마지막 사용자를 제거하면 ASDM은 그룹을 삭제합니다.

참고 사용자가 생성된 후에는 해당 사용자가 속한 그룹을 변경할 수 없습니다.

Add SNMP User Entry 대화 상자가 나타납니다.

3단계 SNMP 사용자가 속해 있는 그룹을 선택합니다. 사용 가능한 그룹은 다음과 같습니다.

- **Auth&Encryption**: 사용자의 인증 및 암호화가 구성되어 있음
- **Authentication_Only**: 사용자의 인증만 구성되어 있음
- **No_Authentication**: 사용자의 인증이나 암호화가 구성되어 있지 않음

참고 그룹 이름은 변경할 수 없습니다.

4단계 사용자 보안 모델(USM) 그룹을 사용하려면 **USM Model** 탭을 클릭합니다.

5단계 **Add**를 클릭합니다.

Add SNMP USM Entry 대화 상자가 나타납니다.

6단계 그룹 이름을 입력합니다.

7단계 드롭다운 목록에서 보안 수준을 선택합니다. 이 설정을 통해 구성된 USM 그룹을 보안 수준으로 SNMPv3 사용자에게 할당할 수 있습니다.

8단계 구성된 사용자 또는 새로운 사용자의 이름을 입력합니다. 사용자 이름은 선택된 SNMP 서버 그룹에 대해 고유해야 합니다.

9단계 **Encrypted** 또는 **Clear Text** 라디오 버튼 중 하나를 클릭하여 사용할 비밀번호 유형을 지정합니다.

10단계 **MD5** 또는 **SHA** 라디오 버튼 중 하나를 클릭하여 사용할 인증 유형을 지정합니다.

11단계 인증에 사용할 비밀번호를 입력합니다.

12단계 **DES**, **3DES** 또는 **AES** 라디오 버튼 중 하나를 클릭하여 사용할 암호화 유형을 지정합니다.

13단계 AES 암호화를 선택할 경우 **128**, **192** 또는 **256** 중 사용할 AES 암호화 수준도 선택합니다.

14단계 암호화에 사용할 비밀번호를 입력합니다. 이 비밀번호에 허용되는 영숫자 문자의 최대 길이는 64자입니다.

15단계 **OK**를 클릭하여 그룹을 생성하고(이 사용자가 해당 그룹의 첫 번째 사용자인 경우) 그룹을 **Group Name** 드롭다운 목록에 표시하고 해당 그룹에 대한 사용자를 생성합니다.

Add SNMP User Entry 대화 상자가 닫힙니다.

16단계 **Apply**를 클릭합니다.

버전 3에 대한 SNMP 매개변수가 컨피그레이션되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

사용자 그룹 구성

지정된 사용자 그룹을 포함한 SNMP 사용자 목록을 구성하려면 다음 단계를 수행하십시오.

절차

1단계 **Configuration > Device Management > Management Access > SNMP**를 선택합니다.

2단계 SNMPv3 Users 창의 **SNMPv3 User/Group** 탭에서 **Click Add > SNMP User Group**을 클릭하고 구성된 사용자 그룹 또는 새로운 사용자 그룹을 추가합니다. 그룹의 마지막 사용자를 제거하면 ASDM은 그룹을 삭제합니다.

Add SNMP User Group 대화 상자가 나타납니다.

3단계 사용자 그룹 이름을 입력합니다.

4단계 기존 사용자 또는 사용자 그룹을 선택하려면 **Existing User/User Group** 라디오 버튼을 클릭합니다.

5단계 새 사용자를 만들려면 **Create new user** 라디오 버튼을 클릭합니다.

6단계 SNMP 사용자가 속해 있는 그룹을 선택합니다. 사용 가능한 그룹은 다음과 같습니다.

- **Auth&Encryption**: 사용자의 인증 및 암호화가 구성되어 있음
- **Authentication_Only**: 사용자의 인증만 구성되어 있음
- **No_Authentication**: 사용자의 인증이나 암호화가 구성되어 있지 않음

7단계 구성된 사용자 또는 새로운 사용자의 이름을 입력합니다. 사용자 이름은 선택된 SNMP 서버 그룹에 대해 고유해야 합니다.

8단계 **Encrypted** 또는 **Clear Text** 라디오 버튼 중 하나를 클릭하여 사용할 비밀번호 유형을 지정합니다.

9단계 **MD5** 또는 **SHA** 라디오 버튼 중 하나를 클릭하여 사용할 인증 유형을 지정합니다.

10단계 인증에 사용할 비밀번호를 입력합니다.

11단계 인증에 사용할 비밀번호를 확인합니다.

12단계 **DES**, **3DES** 또는 **AES** 라디오 버튼 중 하나를 클릭하여 사용할 암호화 유형을 지정합니다.

13단계 암호화에 사용할 비밀번호를 입력합니다. 이 비밀번호에 허용되는 영숫자 문자의 최대 길이는 64자입니다.

14단계 암호화에 사용할 비밀번호를 확인합니다.

15단계 **Add**를 클릭하여 새로운 사용자를 **Members in Group** 창의 지정된 사용자 그룹에 추가합니다. **Remove**를 클릭하여 **Members in Group** 창에서 기존 사용자를 삭제합니다.

16단계 **OK**를 클릭하여 지정된 사용자 그룹에 대한 새로운 사용자를 생성합니다.

Add SNMP User Group 대화 상자가 닫힙니다.

17단계 **Apply**를 클릭합니다.

버전 3에 대한 SNMP 매개변수가 컨피그레이션되고 변경 사항이 실행 중인 컨피그레이션에 저장됩니다.

SNMP 모니터링

SNMP 모니터링에 대한 다음 screens를 참조하십시오.

- **Tools > Command Line Interface**

  이 창에서는 다양한 비 대화형 명령을 내보내고 결과를 볼 수 있습니다.

SNMP 내역

표 41-2 SNMP 내역

기능 이름	플랫폼 릴리스	설명
SNMP 버전 1 및 2c	7.0(1)	일반 텍스트 커뮤니티 문자열을 통해 SNMP 서버와 SNMP 에이전트 간에 데이터를 전송함으로써 ASA, ASAv 및 ASASM 네트워크 모니터링과 이벤트 정보를 제공합니다. 다음 화면을 수정했습니다. Configuration > Device Management > Management Access > SNMP
SNMP 버전 3	8.2(1)	3DES 또는 AES 암호화를 제공하고 지원 보안 모델 중 가장 안전한 SNMP 버전 3을 지원합니다. 이 버전에서는 USM을 사용하여 사용자, 그룹 및 호스트는 물론 인증 특성도 구성할 수 있습니다. 또한 이 버전은 에이전트 및 MIB 객체에 대한 액세스 제어가 가능하며 추가 MIB 지원을 포함합니다. 다음 화면을 수정했습니다. Configuration > Device Management > Management Access > SNMP
비밀번호 암호화	8.3(1)	비밀번호 암호화를 지원합니다.

표 41-2 SNMP 내역 (계속)

기능 이름	플랫폼 릴리스	설명
SNMP 트랩 및 MIB	8.4(1)	다음 추가 키워드를 지원합니다. **connection-limit-reached**, **cpu threshold rising**, **entity cpu-temperature**, **entity fan-failure**, **entity power-supply**, **ikev2 stop | start**, **interface-threshold**, **memory-threshold**, **nat packet-discard**, **warmstart**. 센서, 팬, 전원 공급 장치 및 관련 구성 요소에 대한 entPhysicalTable 보고 항목. 다음 추가 MIB를 지원합니다. CISCO-ENTITY-SENSOR-EXT-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-PROCESS-MIB, CISCO-ENHANCED-MEMPOOL-MIB, CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB, DISMAN-EVENT-MIB, DISMAN-EXPRESSION-MIB, ENTITY-SENSOR-MIB, NAT-MIB. 다음 추가 트랩을 지원합니다. ceSensorExtThresholdNotification, clrResourceLimitReached, cpmCPURisingThreshold, mteTriggerFired, natPacketDiscard, warmStart. 다음 화면을 수정했습니다. Configuration > Device Management > Management Access > SNMP
IF-MIB ifAlias OID 지원	8.2(5)/8.4(2)	이제 ASA이(가) ifAlias OID를 지원합니다. IF-MIB를 찾아볼 때 ifAlias OID는 인터페이스 설명에 설정된 값으로 설정됩니다.
ASA Services Module (ASASM)	8.5(1)	ASASM은(는) 다음을 제외하고 8.4(1)의 모든 MIB 및 트랩을 지원합니다. 8.5(1)에서 지원되지 않는 MIB: • CISCO-ENTITY-SENSOR-EXT-MIB(entPhySensorTable 그룹의 객체만 지원됨). • ENTITY-SENSOR-MIB(entPhySensorTable 그룹의 객체만 지원됨). • DISMAN-EXPRESSION-MIB(expExpressionTable, expObjectTable 및 expValueTable 그룹의 객체만 지원됨). 8.5(1)에서 지원되지 않는 트랩: • ceSensorExtThresholdNotification(CISCO-ENTITY-SENSOR-EXT-MIB). 이 트랩은 전원 공급 장치 및 팬 고장, CPU 고온 이벤트에만 사용됩니다. • InterfacesBandwidthUtilization.
SNMP 트랩	8.6(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X에 대해 다음 추가 키워드를 지원합니다. **entity power-supply-presence**, **entity power-supply-failure**, **entity chassis-temperature**, **entity chassis-fan-failure, entity power-supply-temperature**. 다음 명령을 수정했습니다. **snmp-server enable traps**

표 41-2 SNMP 내역 (계속)

기능 이름	플랫폼 릴리스	설명
VPN-related MIB	9.0(1)	차세대 암호화 기능 지원을 위해 업데이트된 버전의 CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB가 구현되었습니다. 다음 MIB가 ASASM에 대해 활성화되었습니다. • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	다음 MIB가 추가되었습니다. CISCO-TRUSTSEC-SXP-MIB.
SNMP OID	9.1(1)	ASA 5512-X, 5515-X, 5525-X, 5545-X 및 5555-X 지원을 위해 5개의 새로운 SNMP 물리적 공급업체 유형 OID가 추가되었습니다.
NAT MIB	9.1(2)	xlate_count 및 max_xlate_count 엔트리 지원을 위해 cnatAddrBindNumberOfEntries 및 cnatAddrBindSessionCount OID가 추가되었습니다. 이는 **show xlate count** 명령을 사용한 폴링 허용과 대등합니다.
SNMP 호스트, 호스트 그룹 및 사용자 목록	9.1(5)	이제 최대 4000개의 호스트를 추가할 수 있습니다. 지원되는 액티브 폴링 대상의 수는 128개입니다. 네트워크 객체를 지정하여 호스트 그룹으로 추가할 개별 호스트를 나타낼 수 있습니다. 하나의 호스트에 사용자를 두 명 이상 연결할 수 있습니다. 다음 화면을 수정했습니다. Configuration > Device Management > Management Access > SNMP
SNMP 메시지 크기	9.2(1)	SNMP가 전송하는 메시지 크기 제한이 1472바이트로 증가했습니다.
SNMP MIB 및 트랩	9.3(2)	CISCO-PRODUCTS-MIB 및 CISCO-ENTITY-VENDORTYPE-OID-MIB가 새로운 ASA 5506-X, ASA 5506W-X 및 ASA 5508-X를 지원하도록 업데이트되었습니다. ASA 5506-X 및 ASA 5508-X이(가) SNMP sysObjectID OID 및 entPhysicalVendorType OID 테이블에 새로운 제품으로 추가되었습니다. 이제 ASA에서 CISCO-CONFIG-MAN-MIB를 지원하므로 다음 작업을 수행할 수 있습니다. • 특정 컨피그레이션에 대해 어떤 명령이 입력되었는지 알 수 있습니다. • 컨피그레이션 실행 중 변경이 발생하면 NMS에게 알립니다. • 실행 중인 컨피그레이션이 마지막으로 변경되거나 저장된 시간에 대한 타임 스탬프를 추적합니다. • 터미널 정보 및 명령 소스와 같은 기타 명령 변경 사항을 추적합니다. 다음 화면을 수정했습니다. Configuration > Device Management > Management Access > SNMP > Configure Traps > SNMP Trap Configuration.

42 장

Anonymous Reporting 및 Smart Call Home

이 장에서는 Anonymous Reporting 및 Smart Call Home 서비스를 구성하는 방법을 설명합니다.

Anonymous Reporting 정보

Anonymous Reporting을 활성화하면 Cisco가 안전하게 디바이스에서 최소 오류 및 상태 정보를 받을 수 있으므로 Cisco ASA 플랫폼을 개선하는 데 도움이 됩니다. 기능을 활성화해도 고객 ID가 익명으로 남으며 신원을 알 수 있는 정보는 전송되지 않습니다.

Anonymous Reporting을 활성화하면 신뢰 포인트가 생성되고 인증서가 설치됩니다. CA 인증서는 ASA에서 Smart Call Home 웹 서버에 있는 서버 인증서를 확인하고 HTTPS 세션을 형성하여 ASA가 안전하게 메시지를 전송할 수 있도록 하기 위해 필요합니다. Cisco는 소프트웨어에서 미리 정의된 인증서를 가져옵니다. Anonymous Reporting을 활성화하기로 결정하면 인증서가 _SmartCallHome_ServerCA라는 하드 코딩된 신뢰 포인트 이름으로 ASA에 설치됩니다. Anonymous Reporting을 활성화하면 이 신뢰 포인트가 생성되고 적절한 인증서가 설치되며 이 활동에 대한 메시지를 받게 됩니다. 그런 다음 컨피그레이션에 인증서가 표시됩니다.

Anonymous Reporting을 활성화할 때 컨피그레이션에 이미 적절한 인증서가 존재하는 경우 신뢰 포인트가 생성되지 않고 인증서가 설치되지 않습니다.

참고 Anonymous Reporting을 활성화할 때 Cisco 또는 Cisco의 공급업체로 지정된 데이터를 전송함에 동의합니다(미국 외부의 국가 포함).
Cisco는 모든 고객의 개인 정보를 유지 관리합니다. Cisco의 개인 정보 관리 방법에 대한 자세한 내용은 다음 URL에 있는 Cisco의 개인 정보 보호 정책을 참조 하십시오.
http://www.cisco.com/web/siteassets/legal/privacy.html

DNS 요구 사항

Cisco Smart Call Home 서버에 연결하고 Cisco에 메시지를 전송할 수 있도록 ASA에 대한 DNS 서버가 올바르게 구성되어야 합니다. ASA가 사설 네트워크에 상주하고 공용 네트워크에 대한 액세스 권한이 없을 수 있기 때문에 Cisco는 DNS 설정을 확인한 다음 필요한 경우 다음과 같이 컨피그레이션을 대행합니다.

1. 구성된 모든 DNS 서버에 대한 DNS 조회 실시
2. 최고 수준의 보안 인터페이스에서 DHCPINFORM 메시지를 전송하여 DHCP 서버에서 DNS 서버로 연결
3. 조회용 Cisco DNS 서버 사용
4. 무작위로 tools.cisco.com에 대한 고정 IP 주소 사용

이러한 작업은 현재 컨피그레이션을 변경하지 않고 수행됩니다. 예를 들어 DHCP에서 학습된 DNS 서버는 컨피그레이션에 추가되지 않습니다.

구성된 DNS 서버가 없고 ASA가 Cisco Smart Call Home 서버에 연결 할 수 없는 경우 Cisco는 전송된 각 Smart Call Home 메시지에 대한 경고 심각도 수준과 함께 syslog 메시지를 생성하여 DNS를 바르게 구성하라고 알려줍니다.

syslog 메시지에 대한 자세한 내용은syslog 메시지 가이드을 참조 하십시오.

Smart Call Home 정보

완전히 구성된 Smart Call Home은 사이트의 문제를 감지하고 이를 Cisco 또는 다른 사용자 정의 채널(이메일이나 직접 연락)로 보고합니다. 문제가 있음을 알기도 전에 보고를 받는 경우도 많습니다. 이 문제의 심각성에 따라 Cisco에서는 다음 서비스를 제공하여 시스템 컨피그레이션 문제, 제품 단종 공지, 보안 권고 사항 등에 대응합니다.

- 지속적인 모니터링, 실시간 사전 경고 및 상세한 진단을 통해 신속하게 문제를 파악합니다.
- 서비스 요청이 등록되어 있고 모든 진단 데이터가 첨부된 Smart Call Home 알림을 통해 잠재적인 문제를 파악할 수 있습니다.
- Cisco TAC의 전문가와 직접적이고 자동적으로 연락함으로써 중요한 문제를 더 빨리 해결합니다.
- 문제 해결 시간을 단축하여 인력 자원을 더욱 효율적으로 활용합니다.
- Cisco TAC 서비스 요청을 자동으로 생성(서비스 계약을 체결한 경우)하고 적절한 지원 팀으로 라우팅하면 해당 팀이 자세한 진단 정보를 제공하여 문제 해결을 가속합니다.

Smart Call Home 포털은 다음을 수행하는 데 필요한 정보에 대한 빠른 액세스를 제공합니다.

- 모든 Smart Call Home 메시지, 진단 및 권장 사항을 한 곳에서 확인합니다.
- 서비스 요청 상태를 확인합니다.
- 모든 Smart Call Home 지원 디바이스에 대한 최신 인벤토리 및 컨피그레이션 정보를 확인합니다.

Anonymous Reporting 및 Smart Call Home에 대한 지침

Anonymous Reporting

- DNS를 구성해야 합니다.
- Anonymous Reporting 메시지를 한 번에 전송할 수 없는 경우 ASA는 메시지를 삭제하기 전에 두 번 더 시도합니다.
- Anonymous Reporting은 기존 컨피그레이션을 변경하지 않고 다른 Smart Call Home 컨피그레이션과 공존할 수 있습니다. 예를 들어, Smart Call Home이 Anonymous Reporting을 활성화하기 전에 비활성화된 경우 Anonymous Reporting을 활성화한 후에도 비활성 상태를 유지합니다.
- Anonymous Reporting이 활성화되면 신뢰 포인트를 제거할 수 없고 Anonymous Reporting이 비활성화되어도 신뢰 포인트가 유지됩니다. Anonymous Reporting이 비활성화된 경우 신뢰 포인트를 제거할 수 있으나 Anonymous Reporting을 비활성화한다고 신뢰 포인트가 자동으로 삭제되지는 않습니다.
- 여러 컨텍스트 모드 컨피그레이션을 사용하는 경우 **dns**, **interface** 및 **trustpoint** 명령어는 관리 컨텍스트에 상주하고 **call-home** 명령어는 시스템 컨텍스트에 상주합니다.

Smart Call Home

- 다중 컨텍스트 모드에서 **subscribe-to-alert-group snapshot periodic** 명령어는 두 명령어로 분리됩니다. 하나는 시스템 컨피그레이션에서 정보를 가져오는 것이고 하나는 사용자 컨텍스트에서 정보를 가져오는 것입니다.
- Smart Call Home 백엔드 서버는 XML 형식의 메시지만 수락할 수 있습니다.
- 클러스터링을 활성화하고 위험 심각도 수준의 진단 경고 그룹에 등록하도록 Smart Call Home을 구성한 경우 Smart Call Home 메시지가 Cisco에 전달되어 중요한 클러스터 이벤트를 보고합니다. 다음 이벤트에 대해서만 Smart Call Home 클러스터링 메시지가 전송됩니다.
  - 유닛이 클러스터에 참여할 때
  - 유닛이 클러스터를 떠날 때
  - 클러스터 유닛이 클러스터 마스터가 될 때
  - 보조 유닛이 클러스터에서 실패할 때

  전송되는 각 메시지는 다음 정보를 포함합니다.
  - 액티브 클러스터 멤버 수
  - 클러스터 마스터에서 **show cluster info** 명령과 **show cluster history** 명령의 출력

관련 주제

- 42-2 페이지의 DNS 요구 사항
- 14-11 페이지의 Configure the DNS Server

Anonymous Reporting 및 Smart Call Home 구성

Anonymous Reporting은 Smart Call Home 서비스의 일부이며 Cisco가 디바이스로부터 최소한의 오류 및 상태 정보를 익명으로 수신할 수 있게 하지만 Smart Call Home 서비스는 Cisco TAC가 디바이스를 모니터링하고 문제가 있을 때 케이스를 열 수 있도록 시스템 상태에 대한 맞춤 지원을 제공하기도 합니다. 귀하가 문제 발생 사실을 알기 전에 케이스가 열리는 경우도 많습니다.

시스템에 대해 두 서비스 모두 동시에 구성할 수 있습니다. 다만 Smart Call Home 서비스를 구성하면 Anonymous Reporting과 동일한 기능에 맞춤 서비스가 추가로 제공됩니다.

Anonymous Reporting 구성

Anonymous Reporting을 구성하려면 다음 단계를 수행합니다.

절차

1단계 메뉴에서 **Configuration > Device Management > Smart Call Home**을 선택합니다.

2단계 **Enable Anonymous Reporting** 확인란을 선택합니다.

3단계 시스템이 메시지를 보낼 수 있는지 확인하기 위해 **Test Connection**을 클릭합니다.

ASDM이 성공 또는 오류 메시지를 반환하여 테스트 결과를 알려줍니다.

4단계 **Apply**를 클릭하여 컨피그레이션을 저장하고 Anonymous Reporting을 활성화합니다.

Smart Call Home 구성

Smart Call Home 서비스, 시스템 설정, 경고 서브스크립션 프로필을 구성하려면 다음 단계를 수행합니다.

절차

1단계 메뉴에서 **Configuration > Device Management > Smart Call Home**을 선택합니다.

2단계 **Enable Registered Smart Call Home** 확인란을 선택하여 Smart Call Home을 활성화하고 Cisco TAC에서 ASA를 등록합니다.

3단계 **Advanced System Setup**을 두 번 클릭합니다. 이 영역은 3개의 창으로 구성됩니다. 각 창의 제목 행을 두 번 클릭하면 확대하거나 축소할 수 있습니다.

a. **Mail Servers** 창에서 Smart Call Home 메시지가 이메일 가입자에게 전달되는 메일 서버를 설정할 수 있습니다.

b. **Contact Information** 창에서 ASA(Smart Call Home 메시지에 표시됨)에 대한 연락처 정보를 입력할 수 있습니다. 이 창에는 다음 정보가 포함됩니다.

- 연락처의 이름.
- 연락 전화 번호.
- 연락처의 우편 주소.
- 연락처의 이메일 주소.

- Smart Call Home 의 "보내는 사람" 이메일 주소.
- Smart Call Home 의 "회신 주소" 이메일 주소.
- 고객 ID.
- 사이트 ID.
- 계약 ID.

c. 경고 **제어** 창에서 경고 제어 매개변수를 조정할 수 있습니다. 이 창은 다음 경고 그룹의 상태(활성화 또는 비활성화)를 나열하는 **Alert Group Status** 창을 포함합니다.

- 진단 경고 그룹.
- 컨피그레이션 경고 그룹.
- 환경 경고 그룹.
- 인벤토리 경고 그룹.
- 스냅샷 경고 그룹.
- syslog 경고 그룹.
- 원격 분석 경고 그룹.
- 위협 경고 그룹.
- 분당 처리되는 최대 Smart Call Home 메시지 수.
- Smart Call Home 의 "보내는 사람" 이메일 주소.

4단계 경**고 서브스크립션 프로필**을 두 번 클릭합니다. 이름이 지정된 각 서브스크립션 프로필로 가입자와 경고 그룹을 구분할 수 있습니다.

a. **Add** 또는 **Edit**를 클릭하여 **Subscription Profile Editor**를 열면 새 서브스크립션 프로필을 만들거나 기존 서브스크립션 프로필을 편집할 수 있습니다.

b. 선택한 프로필을 제거하려면 **Delete**를 클릭합니다.

c. 선택된 서브스크립션 프로필의 Smart Call Home 메시지를 가입자에게 전송하려면 **Active** 확인란을 선택합니다.

5단계 **Add** 또는 **Edit**를 클릭하여 **Add** 또는 **Edit Alert Subscription Profile** 대화 상자를 표시합니다.

a. **Name** 필드는 읽기 전용이며 수정할 수 없습니다.

b. **Enable this subscription profile** 확인란을 선택하여 특정 프로필을 활성화하거나 비활성화합니다.

c. **HTTP** 또는 **Email** 라디오 버튼을 클릭합니다(**Alert Delivery Method** 영역).

d. 이메일 주소 또는 웹 주소를 **Subscribers** 필드에 입력합니다.

e. **경고 전달** 영역에서는 관리자가 가입자에게 어떤 Smart Call Home 정보 유형을 어떤 조건에 따라 보낼지 지정할 수 있습니다. 경고 유형은 시간 기준과 이벤트 기준의 두 가지이며 경고 트리거 방식에 따라 선택합니다. 구성, 재고, 스냅샷 및 원격 분석 경고 그룹은 시간 기준입니다. 진단, 환경, Syslog 및 위협은 이벤트 기준입니다.

f. **메시지 매개 변수** 영역에서는 기본 메시지 형식 및 최대 메시지 크기를 포함하여 가입자에게 보내는 메시지를 제어하는 매개변수를 조정할 수 있습니다.

6단계 시간 기준 경고의 경우 **Add** 또는 **Edit**(**Alert Dispatch** 영역)를 클릭하여 **Add** 또는 **Edit Configuration Alert Dispatch Condition** 대화 상자를 표시합니다.

a. 가입자에게 정보를 전송할 빈도를 **Alert Dispatch Frequency** 영역에서 지정합니다.

- 월간 서브스크립션의 경우 정보를 보낼 날짜와 시간을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다.

- 주간 서브스크립션의 경우 정보를 요일과 시간을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다.
- 일간 서브스크립션의 경우 정보를 보낼 시간을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다.
- 시간별 서브스크립션의 경우 정보를 보낼 시간(분)을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다. 시간별 서브스크립션은 스냅샷 및 원격 분석 경고 그룹에만 적용됩니다.

b. **Basic** 또는 **Detailed** 라디오 버튼을 클릭하여 가입자에게 보낼 정보의 수준을 지정합니다.

c. **OK**를 클릭하여 컨피그레이션을 저장합니다.

7단계 진단, 환경 및 위협 기준 경고의 경우 **Add** 또는 **Edit**(**Alert Dispatch** 영역)를 클릭하여 **Create** 또는 **Edit Diagnostic Alert Dispatch Condition** 대화 상자를 표시합니다.

8단계 **Event Severity** 드롭다운 목록에서 가입자에게 경고 전달을 트리거할 이벤트 심각도를 지정한 다음 **OK**를 클릭합니다.

9단계 인벤토리 기준 경고의 경우 **Add** 또는 **Edit**(**Alert Dispatch** 영역)를 클릭하여 **Create** 또는 **Edit Inventory Alert Dispatch Condition** 대화 상자를 표시합니다.

10단계 **Alert Dispatch Frequency** 드롭다운 목록에서 가입자에게 경고를 전달할 빈도를 지정한 다음 **OK**를 클릭합니다.

11단계 스냅샷 기준 경고의 경우 **Add** 또는 **Edit**(**Alert Dispatch** 영역)를 클릭하여 **Create** 또는 **Edit Snapshot Alert Dispatch Condition** 대화 상자를 표시합니다.

a. 가입자에게 정보를 전송할 빈도를 **Alert Dispatch Frequency** 영역에서 지정합니다.
- 월간 서브스크립션의 경우 정보를 보낼 날짜와 시간을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다.
- 주간 서브스크립션의 경우 정보를 요일과 시간을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다.
- 일간 서브스크립션의 경우 정보를 보낼 시간을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다.
- 시간별 서브스크립션의 경우 정보를 보낼 시간(분)을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다. 시간별 서브스크립션은 스냅샷 및 원격 분석 경고 그룹에만 적용됩니다.
- 간격 서브스크립션의 경우 가입자에게 정보가 전달되는 빈도를 분 단위로 지정합니다. 이 요구 사항은 스냅샷 경고 그룹에만 해당됩니다.

b. **OK**를 클릭하여 컨피그레이션을 저장합니다.

12단계 sylog 기준 경고의 경우 **Add** 또는 **Edit**(**Alert Dispatch** 영역)를 클릭하여 **Create** 또는 **Edit Syslog Alert Dispatch Condition** 대화 상자를 표시합니다.

a. **가입자에게 경고 전달을 트리거할 이벤트 심각도를 지정** 확인란을 선택하고 드롭다운 목록에서 이벤트 심각도를 선택합니다.

b. **가입자에게 경고 전달을 트리거할 syslog의 메시지 ID 지정** 확인란을 선택합니다.

c. 화면상의 지침에 따라 가입자에게 경고 전달을 트리거하는 syslog 메시지 ID를 지정합니다.

d. **OK**를 클릭하여 컨피그레이션을 저장합니다.

13단계 원격 분석 기준 경고의 경우 **Add** 또는 **Edit**(**Alert Dispatch** 영역)를 클릭하여 **Create** 또는 **Edit Telemetry Alert Dispatch Condition** 대화 상자를 표시합니다.

a. 가입자에게 정보를 전송할 빈도를 **Alert Dispatch Frequency** 영역에서 지정합니다.

- 월간 서브스크립션의 경우 정보를 보낼 날짜와 시간을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다.
- 주간 서브스크립션의 경우 정보를 요일과 시간을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다.
- 일간 서브스크립션의 경우 정보를 보낼 시간을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다.
- 시간별 서브스크립션의 경우 정보를 보낼 시간(분)을 지정합니다. 지정되지 않은 경우 ASA에서 적절한 값을 선택합니다. 시간별 서브스크립션은 스냅샷 및 원격 분석 경고 그룹에만 적용됩니다.

b. **OK**를 클릭하여 컨피그레이션을 저장합니다.

14단계 구성된 경고가 올바르게 작동하는지 확인하기 위하여 **Test**를 클릭합니다.

Anonymous Reporting 및 Smart Call Home 모니터링

Anonymous Reporting 및 Smart Call Home 서비스 모니터링은 다음 화면을 참조하십시오.

- **Tools > Command Line Interface**

  이 창에서는 다양한 비 대화형 명령을 내보내고 결과를 볼 수 있습니다.

Anonymous Reporting 및 Smart Call Home 내역

표 42-1 Anonymous Reporting 및 Smart Call Home 내역

기능 이름	플랫폼 릴리스	설명
Smart Call Home	8.2(2)	Smart Call Home 서비스는 ASA에 대한 사전 예방적 진단 및 실시간 경고를 제공하고 더욱 뛰어난 네트워크 가용성과 운영 효율성을 실현합니다. 다음 화면을 도입했습니다. Configuration > Device Management > Smart Call Home.
Anonymous Reporting	9.0(1)	Anonymous Reporting을 활성화하면 Cisco가 안전하게 디바이스에서 최소 오류 및 상태 정보를 받을 수 있으므로 ASA 플랫폼 개선에 도움이 됩니다. 다음 화면을 수정했습니다. Configuration > Device Management > Smart Call Home.

표 42-1 Anonymous Reporting 및 Smart Call Home 내역 (계속)

기능 이름	플랫폼 릴리스	설명
Smart Call Home	9.1(2)	**show local-host** 명령이 원격 분석 경고 그룹 보고를 위해 **show local-host | include interface** 명령으로 변경되었습니다.
Smart Call Home	9.1(3)	클러스터링을 활성화하고 위험 심각도 수준의 진단 경고 그룹에 등록하도록 Smart Call Home을 구성한 경우 Smart Call Home 메시지가 Cisco에 전달되어 중요한 클러스터 이벤트를 보고합니다. 다음 3가지 이벤트에 대해서만 Smart Call Home 클러스터링 메시지가 전송됩니다. • 유닛이 클러스터에 참여할 때 • 유닛이 클러스터를 떠날 때 • 클러스터 유닛이 클러스터 마스터가 될 때 전송되는 각 메시지는 다음 정보를 포함합니다. • 액티브 클러스터 멤버 수 • 클러스터 마스터에서 **show cluster info** 명령과 **show cluster history** 명령의 출력

파 트 10

참조

43 장

주소, 프로토콜 및 포트

이 장에서는 IP 주소, 프로토콜 및 애플리케이션에 대한 빠른 참조를 제공합니다.

IPv4 주소 및 서브넷 마스크

이 섹션에서는 Cisco ASA에서 IPv4 주소를 사용하는 방법에 대해 설명합니다. IPv4 주소는 점으로 구분된 십진수 표기법으로 나타낸 32비트 숫자입니다. 4개의 8비트 필드(옥텟)가 이진수에서 십진수로 변환된 것이며, 점으로 구분됩니다. IP 주소의 첫 번째 부분은 호스트가 상주하는 네트워크를 식별하고, 두 번째 부분은 제공된 네트워크의 특정 호스트를 식별합니다. 네트워크 번호 필드는 네트워크 접두사라고 합니다. 제공된 네트워크의 모든 호스트에서는 동일한 네트워크 접두사를 공유하지만 고유한 호스트 번호가 있어야 합니다. 클래스풀 IP의 경우, 주소의 클래스는 네트워크 접두사와 호스트 번호 간의 경계를 확인합니다.

클래스

IP 호스트 주소는 클래스 A, 클래스 B, 클래스 C로 된 3개의 다른 주소 클래스로 나눕니다. 각 클래스는 32비트 주소 내의 다른 지점에 있는 네트워크 접두사와 호스트 번호 간의 경계를 고정합니다. 클래스 D 주소는 멀티캐스트 IP를 위해 남겨둡니다.

- 클래스 A 주소(1.xxx.xxx.xxx through 126.xxx.xxx.xxx)에서는 첫 번째 옥텟만 네트워크 접두사로 사용합니다.
- 클래스 B 주소(128.0.xxx.xxx through 191.255.xxx.xxx)에서는 처음 두 개의 옥텟을 네트워크 접두사로 사용합니다.
- 클래스 C 주소(192.0.0.xxx through 223.255.255.xxx)에서는 처음 세 개의 옥텟을 네트워크 접두사로 사용합니다.

클래스 A 주소에는 16,777,214개의 호스트 주소가 있고 클래스 B 주소에는 65,534개의 호스트가 있으므로, 서브넷 마스킹을 사용하여 대형 네트워크를 더 작은 서브넷으로 분할할 수 있습니다.

사설 네트워크

네트워크에 많은 주소가 필요하고 인터넷에서 라우팅할 필요가 없는 경우, IANA(Internet Assigned Numbers Authority)에서 권장하는 사설 IP 주소를 사용할 수 있습니다(RFC 1918 참조). 다음 주소 범위는 광고할 수 없는 사설 네트워크로 지정됩니다.

- 10.0.0.0~10.255.255.255
- 172.16.0.0~172.31.255.255
- 192.168.0.0~192.168.255.255

서브넷 마스크

서브넷 마스크를 사용하면 단일한 클래스 A, B 또는 C 네트워크를 여러 네트워크로 변환할 수 있습니다. 서브넷 마스크를 통해 호스트 번호의 비트를 네트워크 접두사에 추가하는 확장된 네트워크 접두사를 생성할 수 있습니다. 예를 들어, 클래스 C 네트워크 접두사는 항상 IP 주소의 처음 3개의 옥텟으로 구성됩니다. 그러나 클래스 C 확장된 네트워크 접두사에서는 네 번째 옥텟의 일부도 사용합니다.

점으로 구분된 십진수 대신 이진수 표기법을 사용하면 서브넷 마스킹을 쉽게 이해할 수 있습니다. 서브넷 마스크의 비트는 인터넷 주소에 일대일로 대응됩니다.

- IP 주소의 해당 비트가 확장된 네트워크 접두사의 일부일 경우 비트는 1로 설정됩니다.
- 비트가 호스트 번호의 일부일 경우 비트는 0으로 설정됩니다.

예시 1: 클래스 B 주소가 129.10.0.0이고 세 번째 옥텟 전체를 호스트 번호 대신 확장된 네트워크 접두사로 사용하려면, 서브넷 마스크를 11111111.11111111.11111111.00000000으로 지정해야 합니다. 이러한 서브넷 마스크는 클래스 B 주소를 클래스 C 주소와 상응하게 변환하며, 여기에서는 호스트 번호가 마지막 옥텟으로만 구성됩니다.

예시 2: 확장형 네트워크 접두사에 세 번째 옥텟의 일부만 사용하려면 서브넷 마스크를 11111111.11111111.11111000.00000000 형태로 지정해야 합니다. 여기에서는 확장된 네트워크 접두사에 세 번째 옥텟의 5비트만 사용합니다.

서브넷 마스크를 점으로 구분된 십진수 마스크 또는 */비트*("슬래시 *비트*") 마스크로 작성할 수 있습니다. 예시 1에서 점으로 구분된 십진수 마스크의 경우, 각 이진수 옥텟을 십진수 번호로 변환합니다(255.255.255.0). */비트* 마스크의 경우 1s: /24 번호를 추가합니다. 예시 2에서 십진수는 255.255.248.0 이며 /비트는 /21입니다.

확장된 네트워크 접두사에 대한 세 번째 옥텟의 일부를 사용하여 여러 개의 클래스 C 네트워크를 대규모 네트워크로 수퍼네팅(supernet)할 수 있습니다. 예를 들어, 192.168.0.0/20과 같습니다.

서브넷 마스크를 결정

표 43-1을 참조하여 원하는 호스트 개수를 기준으로 서브넷 마스크를 결정합니다.

참고 단일 호스트를 식별하는 /32를 제외하고, 서브넷의 첫 번째 및 마지막 번호는 예약됩니다.

표 43-1 호스트, 비트, 점으로 구분된 십진수 마스크

호스트	/비트 마스크	점으로 구분된 십진수 마스크
16,777,216	/8	255.0.0.0 클래스 A 네트워크
65,536	/16	255.255.0.0 클래스 B 네트워크
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 클래스 C 네트워크
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240
8	/29	255.255.255.248
4	/30	255.255.255.252
사용하지 않음	/31	255.255.255.254
1	/32	255.255.255.255 단일 호스트 주소

서브넷 마스크와 함께 사용할 주소 결정

다음 섹션에서는 클래스 C 규모 및 클래스 B 규모 네트워크의 서브넷 마스크와 함께 사용할 네트워크 주소를 결정하는 방법에 대해 설명합니다.

클래스 C 규모 네트워크 주소

2~254개의 호스트로 구성된 네트워크의 경우, 네 번째 옥텟은 0으로 시작하는 호스트 주소 수의 배수에 들어갑니다. 예를 들어, 표 43-2에는 192.168.0.x 형태의 호스트 서브넷(/29) 8개가 나와 있습니다.

참고 서브넷의 첫 번째 및 마지막 주소는 예약됩니다. 첫 번째 서브넷 예제에서는 192.168.0.0 또는 192.168.0.7을 사용할 수 없습니다.

표 43-2 클래스 C 규모 네트워크 주소

마스크 /29가 포함된 서브넷(255.255.255.248)	주소 범위
192.168.0.0	192.168.0.0~192.168.0.7
192.168.0.8	192.168.0.8~192.168.0.15
192.168.0.16	192.168.0.16~192.168.0.31
—	—
192.168.0.248	192.168.0.248~192.168.0.255

클래스 B 규모 네트워크 주소

호스트 수가 254~65,534개인 네트워크의 서브넷 마스크와 함께 사용할 네트워크 주소를 결정하려면, 사용 가능한 각 확장된 네트워크 접두사의 세 번째 옥텟 값을 결정해야 합니다. 예를 들어, 주소 형태가 10.1.*x*.0 같은 서브넷을 원할 수 있습니다. 여기에서 처음 두 개의 옥텟은 확장된 네트워크 접두사에 사용되므로 고정되며, 네 번째 옥텟은 모든 비트가 호스트 번호에 사용되므로 0입니다.

세 번째 옥텟의 값을 결정하려면 다음 단계를 수행합니다.

1단계 65,536(세 번째 및 네 번째 옥텟을 사용하는 총 주소 개수)을 원하는 호스트 주소의 수로 나누어 네트워크에서 생성할 수 있는 서브넷의 수를 계산합니다.

예를 들어 65,536은 4096개의 호스트로 나뉘며 몫은 16입니다.

따라서 각 클래스 B 규모 네트워크에는 4096개의 주소로 구성된 16개의 서브넷이 있습니다.

2단계 256(세 번째 옥텟의 값 수)을 서브넷 수로 나누어 세 번째 옥텟 값의 배수를 결정합니다.

이 예에서는 256/16 = 16입니다.

세 번째 옥텟은 0으로 시작하는 배수 16에 들어갑니다.

표 43-3에는 네트워크 10.1의 서브넷 16개가 나와 있습니다.

참고 서브넷의 첫 번째 및 마지막 주소는 예약됩니다. 첫 번째 서브넷 예에는 10.1.0.0 또는 10.1.15.255를 사용할 수 없습니다.

표 43-3 네트워크의 서브넷

마스크 /20이 포함된 서브넷(255.255.240.0)	주소 범위
10.1.0.0	10.1.0.0~10.1.15.255
10.1.16.0	10.1.16.0~10.1.31.255
10.1.32.0	10.1.32.0~10.1.47.255
—	—
10.1.240.0	10.1.240.0~10.1.255.255

IPv6 주소

IPv6는 IPv4 이후의 차세대 인터넷 프로토콜입니다. IPv6 주소는 확장된 주소 공간, 간소화된 헤더 형식, 개선된 확장 및 옵션 지원, 흐름 레이블링 기능, 인증 및 개인 정보 보호 기능을 제공합니다. IPv6는 RFC 2460에 설명되어 있습니다. IPv6 주소 지정 아키텍처는 RFC 3513에 설명되어 있습니다.

이 섹션에서는 IPv6 주소 형식 및 아키텍처에 대해 설명합니다.

관련 주제

12-13 페이지의 IPv6 주소 지정 구성

IPv6 주소 형식

IPv6 주소는 콜론(:)으로 구분된 16비트 16진수 필드 8개로 나타내며 x:x:x:x:x:x:x:x 형식으로 표시합니다. 다음은 IPv6 주소의 2가지 예입니다.

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

참고 IPv6 주소의 16진수 문자는 대소문자를 구분하지 않습니다.

주소의 개별 필드에 선행 0이 포함되지 않아도 되지만, 각 필드에는 최소 하나 이상의 숫자가 포함되어야 합니다. 왼쪽에서 세 번째 필드부터 여섯 번째 필드까지 선행 0을 제거하면 예시 주소 2001:0DB8:0000:0000:0008:0800:200C:417A는 2001:0DB8:0:0:8:800:200C:417A로 줄일 수 있습니다. 모두 0으로 된 필드는 0 하나로 줄일 수 있습니다(왼쪽에서 세 번째 및 네 번째 필드). 왼쪽에서 다섯 번째 필드는 3개의 선행 0이 제거되어 필드에 8 하나만 남았으며, 왼쪽에서 여섯 번째 필드는 1개의 선행 0이 제거되어 필드에 800이 남았습니다.

IPv6 주소에는 0으로 된 연속적인 16진수 필드가 몇 개 포함되는 것이 일반적입니다. 이중 콜론(::)을 사용하여 IPv6 주소의 맨 앞, 중간 또는 끝에 0이 연속으로 나오는 필드를 압축할 수 있습니다(콜론은 0이 연속으로 나오는 16진수 필드를 의미합니다). 표 43-4에는 다른 유형의 IPv6 주소의 주소 압축에 대한 몇 가지 예가 나와 있습니다.

표 43-4 IPv6 주소 압축 예

주소 유형	표준 형식	압축된 형식
유니캐스트	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
멀티캐스트	FF01:0:0:0:0:0:0:101	FF01::101
루프백	0:0:0:0:0:0:0:1	::1
지정되지 않음	0:0:0:0:0:0:0:0	::

참고 이중 콜론(::)은 0이 연속으로 나오는 필드를 나타내기 위해 IPv6 주소에서 한 번만 사용할 수 있습니다.

IPv4 및 IPv6 주소가 모두 포함된 환경을 처리할 경우에는 IPv6 형식의 대체 형식이 자주 사용됩니다. 이러한 대체 형식은 x:x:x:x:x:x:y.y.y.y입니다. 여기서 x는 IPv6 주소의 높은 자리 부분 6개의 16진수 값을 나타내고, y는 주소의 32비트 IPv4 부분의 십진수 값을 나타냅니다(IPv6 주소의 나머지 2개의 16비트 부분을 대신함). 예를 들어, IPv4 주소 192.168.1.1은 IPv6 주소 0:0:0:0:0:0:FFFF:192.168.1.1 또는 ::FFFF:192.168.1.1으로 표시할 수 있습니다.

IPv6 주소 유형

다음은 IPv6 주소의 3가지 기본 유형입니다.

- **유니캐스트** — 유니캐스트 주소는 단일 인터페이스의 식별자입니다. 유니캐스트 주소로 전송된 패킷은 해당 주소로 식별된 인터페이스에 전달됩니다. 인터페이스에는 할당된 것보다 여러 개의 유니캐스트 주소가 있을 수 있습니다.
- **멀티캐스트** — 멀티캐스트 주소는 인터페이스 집합의 식별자입니다. 멀티캐스트 주소로 전송된 패킷은 해당 주소로 식별된 인터페이스에 전달됩니다.
- **애니캐스트** — 애니캐스트 주소는 인터페이스 집합의 식별자입니다. 멀티캐스트 주소와 달리 애니캐스트 주소로 전송된 패킷은 라우팅 프로토콜의 거리를 측정하여 확인된 "가장 가까운" 인터페이스에만 전달됩니다.

참고 IPv6에는 브로드캐스트 주소가 없습니다. 멀티캐스트 주소에서는 브로드캐스트 기능을 제공합니다.

유니캐스트 주소

이 섹션에서는 IPv6 유니캐스트 주소에 대해 설명합니다. 유니캐스트 주소는 네트워크 노드의 인터페이스를 식별합니다.

전역 주소

IPv6 글로벌 유니캐스트 주소의 일반적인 형식은 전역 라우팅 접두사 뒤에 서브넷 ID가 오고 그 뒤에 인터페이스 ID가 옵니다. 전역 라우팅 접두사는 다른 IPv6 주소 유형에서 예약되지 않은 모든 접두사가 해당될 수 있습니다.

이진수 000으로 시작하는 주소를 제외한 모든 전역 유니캐스트 주소는 Modified EUI-64 형식의 64비트 인터페이스 ID가 포함됩니다.

이진수 000으로 시작하지 않는 전역 유니캐스트 주소에는 주소의 인터페이스 ID 부분에 아무런 제한 없이 모든 크기 또는 구조가 올 수 있습니다. 이러한 유형으로 된 주소의 한 가지 예는 IPv4 주소가 포함된 IPv6 주소입니다.

관련 주제

- 43-10 페이지의 IPv6 주소 접두사
- 43-8 페이지의 인터페이스 식별자
- 43-7 페이지의 IPv4 호환 IPv6 주소

사이트-로컬 주소

사이트-로컬 주소는 사이트 내에서 주소를 지정하는 데 사용됩니다. 이러한 주소를 사용하면 전역에서 고유한 접두사를 사용하지 않고 전체 사이트의 주소를 지정할 수 있습니다. 사이트-로컬 주소에는 접두사 FEC0::/10이 포함되고 54비트 서브넷 ID가 뒤에 오며 Modified EUI-64 형식의 64비트 인터페이스 ID로 끝납니다.

사이트-로컬 라우터에서는 사이트 외부의 소스 또는 목적지에 대한 사이트-로컬 주소가 포함된 패킷을 전달하지 않습니다. 따라서 사이트-로컬 주소는 사설 주소로 간주할 수 있습니다.

링크-로컬 주소

모든 인터페이스에는 최소한 하나 이상의 링크-로컬 주소가 있어야 합니다. 인터페이스당 여러 개의 IPv6 주소를 구성할 수 있으나, 링크-로컬 주소는 하나만 구성 가능합니다.

링크-로컬 주소는 링크-로컬 접두사 FE80::/10 및 Modified EUI-64 형식의 인터페이스 식별자를 사용하여 모든 인터페이스에서 자동으로 구성할 수 있는 IPv6 유니캐스트 주소입니다. 링크-로컬 주소는 인접 검색 프로토콜 및 스테이트풀 자동 컨피그레이션 프로세스에서 사용됩니다. 링크-로컬 주소가 포함된 노드에서는 통신을 수행할 수 있으며, 통신을 위해 사이트-로컬 또는 전역에서 고유한 주소가 필요하지 않습니다.

라우터에서는 소스 또는 목적지의 링크-로컬 주소가 포함된 패킷은 전달하지 않습니다. 따라서 링크-로컬 주소는 사설 주소로 간주할 수 있습니다.

IPv4 호환 IPv6 주소

IPv4 주소를 포함할 수 있는 IPv6 주소에는 2가지 유형이 있습니다.

첫 번째 유형은 IPv4 호환 IPv6 주소입니다. IPv6 전환 메커니즘에는 IPv4 라우팅 인프라를 통해 IPv6 패킷을 동적으로 터널링할 수 있는 호스트 및 라우터를 지원하는 기술이 포함됩니다. 이러한 기술을 사용하는 IPv6 노드에는 낮은 자리 32비트 형식의 전역 IPv4 주소를 전달하는 특수 IPv6 유니캐스트 주소가 할당됩니다. 이러한 유형의 주소는 IPv4 호환 IPv6 주소라고 하며 ::y.y.y.y 형식으로 되어 있습니다. 여기서 y.y.y.y는 IPv4 유니캐스트 주소입니다.

참고 IPv4 호환 IPv6 주소에 사용되는 IPv4 주소는 전역에서 고유한 IPv4 유니캐스트 주소가 있어야 합니다.

두 번째 유형의 IPv6 주소는 내장된 IPv4 주소를 수용하며, IPv4 매핑 IPv6 주소라고 합니다. 이러한 주소 유형은 IPv4 노드의 주소를 IPv6 주소로 표현하는 데 사용됩니다. 이러한 주소 유형의 형식은 ::FFFF:y.y.y.y이며, 여기서 y.y.y.y는 IPv4 유니캐스트 주소입니다.

지정되지 않은 주소

지정되지 않은 주소 0:0:0:0:0:0:0:0은 IPv6 주소가 없음을 나타냅니다. 예를 들어, IPv6 네트워크에서 새로 초기화된 노드에서는 IPv6 주소를 수신할 때까지 해당 패킷에서 지정되지 않은 주소를 소스 주소로 사용할 수 있습니다.

참고 IPv6 지정되지 않은 주소는 인터페이스에 할당할 수 없습니다. 지정되지 않은 IPv6 주소를 IPv6 패킷 또는 IPv6 라우팅 헤더에서 목적지 주소로 사용해서는 안 됩니다.

루프백 주소

루프백 주소 0:0:0:0:0:0:0:1는 IPv6 패킷을 자신에게 전송하려는 노드에서 사용할 수 있습니다. IPv6의 루프백 주소는 IPv4 루프백 주소(127.0.0.1)와 동일한 기능을 수행합니다.

참고 IPv6 루프백 주소는 물리적 인터페이스에 할당할 수 없습니다. IPv6 루프백 주소를 소스 또는 목적지 주소로 포함한 패킷은 패킷이 생성된 노드 내에 그대로 있어야 합니다. IPv6 라우터에서는 IPv6 루프백 주소를 소스 또는 목적지 주소로 포함한 패킷을 전달하지 않습니다.

인터페이스 식별자

IPv6 유니캐스트 주소의 인터페이스 식별자는 링크의 인터페이스를 식별할 때 사용됩니다. 이러한 식별자는 서브넷 접두사에서 고유해야 합니다. 대부분의 경우, 인터페이스 식별자는 인터페이스 링크 계층 주소에서 파생됩니다. 동일한 인터페이스 식별자는 인터페이스가 다른 서브넷에 연결되어 있는 한 단일 노드의 여러 인터페이스에 사용될 수 있습니다.

이진수 000으로 시작하는 주소를 제외한 모든 유니캐스트 주소의 경우, 64비트 길이의 Modified EUI-64 형식으로 구성하려면 인터페이스 식별자가 필요합니다. Modified EUI-64 형식은 주소의 범용/로컬 비트를 변환하고, MAC 주소의 상위 3개 바이트와 하위 3개 바이트 사이에 16진수 숫자 FFFE를 삽입하는 방법을 통해 48비트 MAC 주소에서 생성됩니다.

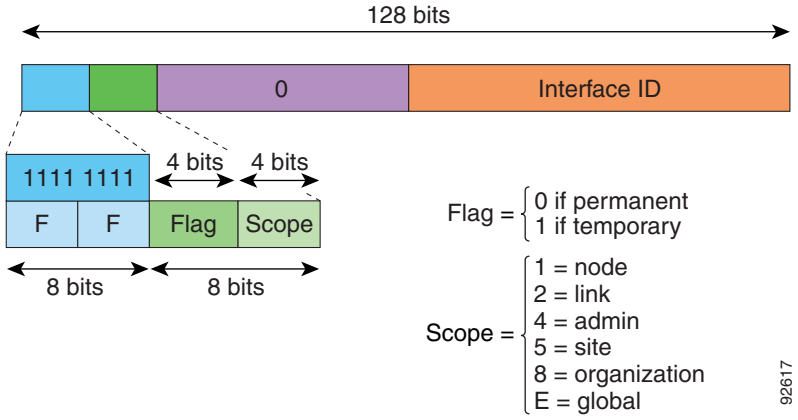
예를 들어, MAC 주소가 00E0.b601.3B7A인 인터페이스의 64비트 인터페이스 ID는 02E0:B6FF:FE01:3B7A가 될 수 있습니다.

멀티캐스트 주소

IPv6 멀티캐스트 주소는 일반적으로 다른 노드에 있는 인터페이스 그룹의 식별자입니다. 멀티캐스트 주소로 전송된 패킷은 해당 주소로 식별된 모든 인터페이스에 전달됩니다. 인터페이스는 멀티캐스트 그룹에 얼마든지 속할 수 있습니다.

IPv6 멀티캐스트 주소의 접두사는 FF00::/8(1111 1111)입니다. 접두사 뒤의 옥텟은 멀티캐스트 주소의 유형과 범위를 정의합니다. 영구적으로 할당된(잘 알려진) 멀티캐스트 주소에는 0에 상응하는 플래그 매개변수가 있습니다. 임시(일시적) 멀티캐스트 주소에는 1에 상응하는 플래그 매개변수가 있습니다. 노드, 링크, 사이트 또는 조직의 범위나 전역 범위가 포함된 멀티캐스트 주소에는 각각 1, 2, 5, 8 또는 E로 된 범위 매개변수가 포함됩니다. 예를 들어, 접두사가 FF02::/16인 멀티캐스트 주소는 링크 범위가 포함된 영구 멀티캐스트 주소입니다. 그림 43-1에는 IPv6 멀티캐스트 주소의 형식이 나와 있습니다.

그림 43-1 IPv6 멀티캐스트 주소 형식



다음 멀티캐스트 그룹에 참여하려면 IPv6 노드(호스트 및 라우터)가 있어야 합니다.

- All Nodes 멀티캐스트 주소:
  - FF01::(인터페이스-로컬)
  - FF02::(링크-로컬)
- 노드의 각 IPv6 유니캐스트 및 애니캐스트 주소에 대한 Solicited-Node 주소이며 FF02:0:0:0:0:1:FFXX:XXXX/104 형식으로 되어 있습니다. 여기서 XX:XXXX는 유니캐스트 또는 애니캐스트 주소의 낮은 자리 24비트 부분입니다.

참고 Solicited-Node 주소는 Neighbor Solicitation 메시지에 사용됩니다.

다음 멀티캐스트 그룹에 참여하려면 IPv6 라우터가 있어야 합니다.

- FF01:: 2(인터페이스-로컬)
- FF02:: 2(링크-로컬)
- FF05:: 2(사이트-로컬)

멀티캐스트 주소는 IPv6 패킷에서 소스 주소로 사용해서는 안 됩니다.

참고 IPv6에는 브로드캐스트 주소가 없습니다. IPv6 멀티캐스트 주소는 브로드캐스트 주소 대신 사용됩니다.

애니캐스트 주소

IPv6 애니캐스트 주소는 일반적으로 다른 노드에 속한 여러 개의 인터페이스에 할당된 유니캐스트 주소입니다. 애니캐스트 주소에 라우팅된 패킷은 해당 주소가 포함된 가장 가까운 인터페이스에 라우팅되며, 인접성은 적용되는 라우팅 프로토콜에 의해 결정됩니다.

애니캐스트 주소는 유니캐스트 주소 영역에서 할당됩니다. 애니캐스트 주소는 여러 개의 인터페이스에 할당된 유니캐스트 주소이며, 인터페이스는 주소를 애니캐스트 주소로 인식할 수 있도록 구성해야 합니다.

애니캐스트 주소에는 다음과 같은 제한 사항이 적용됩니다.

- 애니캐스트 주소는 IPv6 패킷의 소스 주소로 사용할 수 없습니다.
- 애니캐스트 주소는 IPv6 호스트에 할당할 수 없으며, IPv6 라우터에만 할당할 수 있습니다.

참고 애니캐스트 주소는 ASA에서 지원되지 않습니다.

필수 주소

IPv6 호스트에는 최소 다음과 같은 주소를 구성해야 합니다(자동 또는 수동으로).

- 각 인터페이스의 링크-로컬 주소
- 루프백 주소
- All Nodes 멀티캐스트 주소
- 각 유니캐스트 또는 애니캐스트 주소의 Solicited-Node 멀티캐스트 주소

IPv6 라우터에는 최소 다음과 같은 주소를 구성해야 합니다(자동 또는 수동으로).

- 필수 호스트 주소
- 라우터 역할을 수행하도록 구성된 모든 인터페이스의 Subnet-Router 애니캐스트 주소
- All-Routers 멀티캐스트 주소

IPv6 주소 접두사

ipv6-prefix/prefix-length 형식으로 된 IPv6 주소 접속사를 사용하여 전체 주소 영역의 비트 인접 블록을 표시할 수 있습니다. IPv6 접두사는 RFC 2373에 설명된 형식으로 구성해야 하며, 해당 주소는 콜론 사이에 16비트 값을 사용한 16진수로 지정해야 합니다. 접두사 길이는 접두사(주소의 네트워크 부분)로 구성된 주소의 높은 자리 인접 비트가 몇 개 있는지 나타내는 십진수 값입니다. 예를 들어, 2001:0DB8:8086:6502::/32는 올바른 IPv6 접두사입니다.

IPv6 접두사는 IPv6 주소의 유형을 식별합니다. 표 43-5에는 각 IPv6 주소 유형의 접두사가 나와 있습니다.

표 43-5 IPv6 주소 유형 접두사

주소 유형	이진 접두사	IPv6 표기법
지정되지 않음	000...0(128비트)	::/128
루프백	000...1(128비트)	::1/128
멀티캐스트	11111111	FF00::/8
링크-로컬(유니캐스트)	1111111010	FE80::/10
사이트-로컬(유니캐스트)	1111111111	FEC0::/10
전역(유니캐스트)	기타 모든 주소	
애니캐스트	유니캐스트 주소 영역에서 가져옴	

프로토콜 및 애플리케이션

표 43-6에는 프로토콜 리터럴 값 및 포트 번호가 나와 있으며, 이를 ASA 명령에 입력할 수 있습니다.

표 43-6 프로토콜 리터럴 값

리터럴	값	설명
ah	51	IPv6용 Authentication Header, RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol
esp	50	IPv6용 Encapsulated Security Payload, RFC 1827
gre	47	Generic Routing Encapsulation
icmp	1	Internet Control Message Protocol, RFC 792
icmp6	58	IPv6용 Internet Control Message Protocol, RFC 2463
igmp	2	Internet Group Management Protocol, RFC 1112
igrp	9	Interior Gateway Routing Protocol
ip	0	Internet Protocol
ipinip	4	IP-in-IP encapsulation
ipsec	50	IP Security. ipsec 프로토콜 리터럴을 입력할 경우 esp 프로토콜 리터럴을 입력하는 것에 상응합니다.
nos	94	Network Operating System(Novell의 NetWare)
ospf	89	Open Shortest Path First 라우팅 프로토콜, RFC 1247
pcp	108	Payload Compression Protocol
pim	103	Protocol Independent Multicast
pptp	47	Point-to-Point Tunneling Protocol. pptp 프로토콜 리터럴을 입력할 경우 gre 프로토콜 리터럴을 입력하는 것에 상응합니다.
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol, RFC 793
udp	17	User Datagram Protocol, RFC 768.

IANA 웹 사이트에서 프로토콜 번호를 볼 수 있습니다.
http://www.iana.org/assignments/protocol-numbers

TCP 및 UDP 포트

표 43-7에는 프로토콜 리터럴 값 및 포트 번호가 나와 있으며, 이를 ASA 명령에 입력할 수 있습니다. 다음 주의 사항을 참조하십시오.

- ASA에서는 SQL*Net에 포트 1521를 사용합니다. 이는 SQL*Net용 Oracle에서 사용되는 기본 포트입니다. 그러나 이 값은 IANA 포트 할당과 일치하지 않습니다.
- ASA에서는 포트 1645 및 1646에서 RADIUS를 수신합니다. RADIUS 서버에서 표준 포트 1812 및 1813을 사용할 경우, **authentication-port** 및 **accounting-port** 명령을 사용하여 ASA에서 이러한 포트를 수신하도록 구성할 수 있습니다.
- DNS 액세스를 위한 포트를 할당하려면 **dns** 대신 **domain** 리터럴 값을 사용합니다. **dns**를 사용할 경우 ASA에서는 **dnsix** 리터럴 값을 사용하겠다는 것으로 간주합니다.

IANA 웹 사이트에서 포트 번호를 온라인으로 볼 수 있습니다.

http://www.iana.org/assignments/port-numbers

표 43-7 포트 리터럴 값

리터럴	TCP 또는 UDP?	값	설명
aol	TCP	5190	America Online
bgp	TCP	179	Border Gateway Protocol, RFC 1163
biff	UDP	512	메일 시스템에서 새 메일이 수신되었음을 사용자에게 알리기 위해 사용됨
bootpc	UDP	68	Bootstrap Protocol Client
bootps	UDP	67	Bootstrap Protocol Server
chargen	TCP	19	Character Generator
citrix-ica	TCP	1494	Citrix Independent Computing Architecture(ICA) 프로토콜
cmd	TCP	514	**cmd**의 경우 자동 인증이 있다는 점을 제외하고 **exec**과 유사함
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	Day time, RFC 867
discard	TCP, UDP	9	Discard
domain	TCP, UDP	53	DNS
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
echo	TCP, UDP	7	Echo
exec	TCP	512	Remote process execution
finger	TCP	79	Finger
ftp	TCP	21	File Transfer Protocol(제어 포트)

표 43-7 포트 리터럴 값 (계속)

리터럴	TCP 또는 UDP?	값	설명
ftp-data	TCP	20	File Transfer Protocol(데이터 포트)
gopher	TCP	70	Gopher
https	TCP	443	HTTP over SSL
h323	TCP	1720	H.323 호출 신호
hostname	TCP	101	NIC Host Name Server
ident	TCP	113	Ident 인증 서비스
imap4	TCP	143	Internet Message Access Protocol, 버전 4
irc	TCP	194	Internet Relay Chat protocol
isakmp	UDP	500	Internet Security Association and Key Management Protocol
kerberos	TCP, UDP	750	Kerberos
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn Shell
ldap	TCP	389	Lightweight Directory Access Protocol
ldaps	TCP	636	Lightweight Directory Access Protocol(SSL)
lpd	TCP	515	Line Printer Daemon - printer spooler
login	TCP	513	Remote login
lotusnotes	TCP	1352	IBM Lotus Notes
mobile-ip	UDP	434	Mobile IP-Agent
nameserver	UDP	42	Host Name Server
netbios-ns	UDP	137	NetBIOS Name Service
netbios-dgm	UDP	138	NetBIOS Datagram Service
NetBIOS ssn	TCP	139	NetBIOS Session Service
nntp	TCP	119	Network News Transfer Protocol
ntp	UDP	123	Network Time Protocol
pcanywhere-status	UDP	5632	pcAnywhere 상태
pcanywhere-data	TCP	5631	pcAnywhere 데이터
pim-auto-rp	TCP, UDP	496	Protocol Independent Multicast, reverse path flooding, dense mode
pop2	TCP	109	Post Office Protocol - 버전 2
POP3	TCP	110	Post Office Protocol - 버전 3
pptp	TCP	1723	Point-to-Point Tunneling Protocol

표 43-7 포트 리터럴 값 (계속)

리터럴	TCP 또는 UDP?	값	설명
radius	UDP	1645	Remote Authentication Dial-In User Service
radius-acct	UDP	1646	Remote Authentication Dial-In User Service (accounting)
rip	UDP	520	Routing Information Protocol
secureid-udp	UDP	5510	SecureID over UDP
SMTP	TCP	25	Simple Mail Transport Protocol
snmp	UDP	161	Simple Network Management Protocol
snmptrap	UDP	162	Simple Network Management Protocol - Trap
sqlnet	TCP	1521	Structured Query Language Network
ssh	TCP	22	Secure Shell
sunrpc (rpc)	TCP, UDP	111	Sun Remote Procedure Call
syslog	UDP	514	System Log
tacacs	TCP, UDP	49	Terminal Access Controller Access Control System Plus
talk	TCP, UDP	517	Talk
telnet	TCP	23	RFC 854 Telnet
tftp	UDP	69	Trivial File Transfer Protocol
time	UDP	37	Time
uucp	TCP	540	UNIX-to-UNIX Copy Program
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP	80	World Wide Web
xdmcp	UDP	177	X Display Manager Control Protocol

로컬 포트 및 프로토콜

표 43-8에는 ASA에 지정된 트래픽을 처리하기 위해 ASA에서 열 수 있는 프로토콜, TCP 포트, UDP 포트가 나와 있습니다. 표 43-8에 나열된 기능 및 서비스를 활성화하지 않으면, ASA에서는 로컬 프로토콜이나 TCP 또는 UDP를 열지 *않습니다*. 수신하는 기본 프로토콜 또는 포트를 열려면 ASA에 대한 기능 또는 서비스를 구성해야 합니다. 대부분의 경우, 기능 또는 서비스를 활성화할 때 기본 포트 대신 여러 포트를 구성할 수 있습니다.

표 43-8 기능 및 서비스를 통해 연 프로토콜 및 포트

기능 또는 서비스	프로토콜	포트 번호	코멘트
DHCP	UDP	67,68	—
장애 조치 제어	105	N/A	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	N/A	—
IGMP	2	N/A	목적지 IP 주소 224.0.0.1에서만 열리는 프로토콜
ISAKMP/IKE	UDP	500	구성 가능합니다.
IPsec(ESP)	50	N/A	—
IPsec over UDP(NAT-T)	UDP	4500	—
IPsec over UDP(Cisco VPN 3000 Series 호환 가능)	UDP	10000	구성 가능합니다.
IPsec over TCP(CTCP)	TCP	—	기본 포트는 사용되지 않습니다. IPsec over TCP를 구성할 경우 포트 번호를 지정해야 합니다.
NTP	UDP	123	—
OSPF	89	N/A	목적지 IP 주소 224.0.0.5 및 224.0.0.6에서만 열리는 프로토콜
PIM	103	N/A	목적지 IP 주소 224.0.0.13에서만 열리는 프로토콜
RIP	UDP	520	—
RIPv2	UDP	520	목적지 IP 주소 224.0.0.9에서만 열리는 프로토콜
SNMP	UDP	161	구성 가능합니다.
SSH	TCP	22	—
스테이트풀 업데이트	8(비보안) 9(보안)	N/A	—
텔넷	TCP	23	—
VPN 로드 밸런싱	UDP	9023	구성 가능합니다.
VPN 개별 사용자 인증 프록시	UDP	1645, 1646	VPN 터널을 통해서만 액세스할 수 있는 포트입니다.

ICMP 유형

표 43-9에는 ASA 명령에 입력할 수 있는 ICMP 유형의 번호 및 이름이 나와 있습니다.

표 43-9 ICMP 유형

ICMP 번호	ICMP 이름
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect