Firepower Threat Defense용 명령 참조

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CLI(Command Line Interface) 사용

다음 주제에서는 Firepower Threat Defense 디바이스에 CLI(Command Line Interface)를 사용하는 방법과 명령 참조 항목을 해석하는 방법을 설명합니다. 기본 시스템 설정 및 문제 해결을 위해 CLI를 사용합니다.

CLI(Command Line Interface) 로그인

CLI에 로그인하려면 SSH 클라이언트를 사용하여 관리 IP 주소에 연결합니다. 사용자 이름 **admin**(기본 비밀번호: Admin123) 또는 다른 CLI 사용자 계정을 사용하여 로그인합니다.

SSH 연결용 인터페이스를 여는 경우 데이터 인터페이스에 있는 주소에 연결할 수도 있습니다. 데이터 인터페이스에 대한 SSH 액세스는 기본값으로 사용 해제 상태입니다. SSH 액세스를 활성화하려면 디바이스 관리자(Firepower Management Center 또는 Firepower Device Manager)를 사용하여 특정 데이터 인터페이스에 대한 SSH 연결을 허용합니다.

configure user add 명령을 사용하면 CLI에 로그인할 수 있는 사용자 계정을 생성할 수 있습니다. 그러나 이러한 사용자는 CLI에만 로그인할 수 있으며 Firepower Device Manager 웹 인터페이스에는 로그인할 수 없습니다. CLI는 로컬 인증만 지원합니다. 외부 인증을 사용하여 CLI에 액세스할 수 없습니다.

콘솔 포트 액세스

SSH 외에 디바이스에서 콘솔 포트에 직접 연결할 수 있습니다. 디바이스에 포함된 콘솔 케이블을 사용하여 PC를 콘솔에 연결합니다(터미널 에뮬레이터 9600보드, 8 데이터 비트, 패리티 없음, 1 정지 비

트, 흐름 제어 없음). 콘솔 케이블에 대한 자세한 내용은 디바이스용 하드웨어 가이드를 참조하십시오.

사용자가 콘솔 포트에서 액세스하는 초기 CLI는 디바이스 유형에 따라 다릅니다.

- ASA Series 디바이스 — 콘솔 포트의 CLI는 일반 Firepower Threat Defense CLI입니다.
- Firepower Series 디바이스 — 콘솔 포트의 CLI는 FXOS입니다. **connect ftd** 명령을 사용하여 Firepower Threat Defense CLI에 액세스할 수 있습니다. FXOS CLI를 섀시 레벨 컨피그레이션 및 문제 해결용으로만 사용합니다. 기본 컨피그레이션, 모니터링 및 일반 시스템 문제해결 시에는 Firepower Threat Defense CLI를 사용합니다. FXOS 명령에 대한 자세한 내용은 FXOS 설명서를 참조하십시오.

명령 모드

Firepower Threat Defense 디바이스의 CLI에는 다양한 모드가 있으며 , 각각은 단일 CLI에 대한 하위 모드가 아니라 별도의 CLI입니다. 명령 프롬프트를 확인하여 현재의 모드를 구분할 수 있습니다.

일반 **Firepower Threat Defense CLI**

Firepower Threat Defense 관리 컨피그레이션 및 문제 해결을 위해 이 CLI를 사용합니다.

```
>
```

진단 **CLI**

고급 문제 해결용으로 이 CLI를 사용합니다. 이 CLI는 ASA 5506W-X에서 무선 액세스 포인트용 CLI를 시작하는 데 필요한 **session wlan console** 명령을 포함하여 추가적인 show 및 기타 명령을 포함합니다. 이 CLI에는 2개의 하위 모드가 있는데 더 많은 명령을 Privileged EXEC 모드에서 사용할 수 있습니다.

이 모드를 시작하려면 Firepower Threat Defense CLI에서 **system support diagnostic-cli**를 사용합니다.

- User EXEC 모드

  ```
  firepower>
  ```

- Privileged EXEC 모드. 이 모드를 시작하려면 **enable** 명령을 입력합니다(비밀번호를 입력하라는 메시지가 표시되면 비밀번호를 입력하지 않고 Enter를 누릅니다).

  ```
  firepower#
  ```

Expert 모드

문서에 설명되어 있는 절차에 따라 Expert 모드가 필요하다고 알려주는 경우 또는 Cisco Technical Assistance Center에서 사용하도록 요청하는 경우에만 Expert 모드를 사용합니다. 이 모드를 시작하려면 Firepower Threat Defense CLI에서 **expert** 명령을 사용합니다.

admin 사용자로 로그인하는 경우 프롬프트는 username@hostname입니다. 다른 사용자로 로그인하는 경우, 호스트 이름만 표시됩니다. hostname은 관리 인터페이스에 대해 구성된 이름입니다. 예를 들면 다음과 같습니다.

```
admin@firepower:~$
```

FXOS(Firepower eXtensible Operating System) CLI

Firepower 4100, 9300 Series 디바이스에서 FXOS는 전체 섀시를 제어하는 운영 체제입니다. 모델에 따라 컨피그레이션 및 문제 해결을 위해 FXOS를 사용합니다. FXOS에서 connect ftd 명령을 사용하여 Firepower Threat Defense CLI를 시작할 수 있습니다.

FXOS 명령 프롬프트는 다음과 같으며 모드에 따라 프롬프트가 변경됩니다. FXOS CLI 사용에 대한 자세한 정보는 FXOS 버전 및 하드웨어 모델에 대한 *Cisco FXOS CLI* 컨피그레이션 가이드를 참조하십시오.

```
Firepower-module2>
Firepower-module2#
```

구문 형식 지정

명령 구문 설명은 다음 표기 규칙을 사용합니다.

표기 규칙	설명
command	명령 텍스트는 표시되는 글자 그대로 입력할 명령 및 키워드를 나타냅니다.
variable	변수 텍스트는 값을 제공할 인수를 나타냅니다.
[x]	선택적 요소(키워드 또는 인수)를 대괄호로 묶습니다.
[x | y]	대괄호 안의 세로 막대로 구분된 키워드 또는 인수는 선택사항을 나타냅니다.
{x | y}	중괄호 안의 세로 막대로 구분된 키워드 또는 인수는 필수 선택 항목을 나타냅니다.
[x {y | z}]	중첩된 대괄호 또는 중괄호 집합은 선택 요소 또는 필수 요소 내의 선택사항 또는 필수 선택 항목을 나타냅니다. 대괄호 안의 중괄호 및 세로 막대는 선택 요소 내의 필수 선택 항목을 나타냅니다.

명령 입력

콘솔 포트 또는 SSH 세션을 통해 CLI에 로그인할 때, 다음 명령 프롬프트가 표시됩니다.

>

프롬프트에 명령을 입력하고 Enter를 눌러 명령을 실행합니다. 추가 기능은 다음과 같습니다.

- 명령 기록을 통해 스크롤 — 위로 화살표 및 아래로 화살표를 사용하여 이미 입력한 명령을 스크롤할 수 있습니다. 기록에서 명령을 다시 입력하거나 수정하고 다시 입력할 수 있습니다.
- 명령 완성 — 부분 문자열을 입력한 후 명령 또는 키워드를 완성하려면 space 또는 Tab 키를 누릅니다. 부분 문자열은 완성하려는 단일 명령 또는 키워드와 일치해야 합니다.
- 명령 약어 — 일반 CLI에서 명령을 축약할 수 없습니다. 전체 명령 문자열을 입력해야 합니다. 그러나, 진단 CLI에서 명령에 대한 몇 가지 고유한 문자로 대부분의 명령을 축약할 수 있습니다. 예를 들어, **show ver**를 **show version** 대신 입력할 수 있습니다.

show 명령 출력 필터링

파이프를 통해 출력을 필터링 명령으로 보내 **show** 명령의 출력을 필터링할 수 있습니다. 파이프를 통한 출력 전송은 모든 **show** 명령을 사용하여 작동되지만 수많은 텍스트를 생성하는 명령을 처리할 때 가장 유용합니다.

필터링 기능을 사용하려면 다음 형식을 사용합니다. 이 경우, show 명령 다음의 세로 막대 |는 파이프 문자이자 명령의 일부이며 구문 설명의 일부가 아닙니다. 필터링 옵션은 | 문자 다음에 옵니다.

show *command* | {**grep**| **include**| **exclude**| **begin**} *regular expression*

필터링 명령

다음의 필터링 명령을 사용할 수 있습니다.

- **grep** — 패턴과 일치하는 라인만 표시합니다.
- **include** — 패턴과 일치하는 라인만 표시합니다.
- **exclude** — 패턴과 일치하는 모든 라인을 제외하고 다른 라인을 모두 표시합니다.
- **begin** — 패턴을 포함하는 첫 번째 라인을 찾고 해당 라인과 모든 후속 라인을 표시합니다.

regular_expression

일반적으로 간단한 텍스트 문자열인 정규식입니다. 작은 따옴표 또는 큰 따옴표에 표현식을 포함하지 마십시오. 이 항목들은 표현식의 일부로 표시됩니다. 또한, 후속 공백도 표현식에 포함됩니다.

다음 예는 inside1_2 인터페이스에 적용하는 규칙만 표시하기 위해 **show access-list** 명령의 출력을 변경하는 방법을 보여줍니다.

```
> show access-list | include inside1_2
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
rule-id 268435458
event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
rule-id 268435458
event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
rule-id 268435458
event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
rule-id 268435458
event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
rule-id 268435458
event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
rule-id 268435458
event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xc1579ed7
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0x699725ea
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458
event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457
event-log both (hitcnt=0) 0xea5bdd6e
```

명령 도움말

다음 명령을 입력하여 커맨드 라인에서 도움말 정보를 사용할 수 있습니다.

- **?** - 모든 명령의 목록을 표시합니다.
- *command_name* **?** - 명령 옵션을 표시합니다. 예: **show ?**.
- *String?***?** - 문자열과 일치하는 명령 또는 키워드를 표시합니다. 예를 들어, **n?**은 문자 n으로 시작하는 모든 명령을 표시합니다.
- **help** *command_name* - 명령에 대한 구문 및 제한된 사용 정보를 표시합니다. 어떤 명령에 도움말 페이지가 있는지 확인하려면 **help ?**를 입력합니다.

I 부

A - R 명령

a - clear e

app-agent heartbeat

Firepower Threat Defense 디바이스에서 실행되는 앱 에이전트(애플리케이션 에이전트)에 대해 하트비트 메시지 간격을 구성하려면 **app-agent heartbeat** 명령을 사용합니다.

app-agent heartbeat [**interval** *milliseconds*] [**retry-count** *integer*]

interval*milliseconds*	하트비트 메시지 간의 시간 간격을 밀리초 단위로 300에서 6000까지 지정합니다. 기본값은 300입니다. 3개의 연속된 하트비트 메시지가 손실된 경우, 시스템의 나머지에 장애 알림을 트리거합니다. 이 간격을 100밀리초씩 증가시켜 최대 6000밀리초까지 조정할 수 있습니다. 300밀리초의 현재 기본값으로 인해 적극적인 장애 탐지 설정에 장애 오탐 위험이 있습니다.
retry-count*integer*	응답이 없거나 앱 에이전트가 하트비트 메시지에 대한 오류 응답을 3-10으로 수신할 경우 앱 에이전트가 하트비트 메시지를 재시도해야 하는 횟수를 지정합니다. 기본값은 3입니다.

기본 간격 값은 300밀리초입니다.

기본 재시도 횟수는 3입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

Firepower Threat Defense 디바이스에서 실행되는 앱 에이전트의 기본 작업은 Firepower Threat Defense 모듈과 Firepower 9300 및 4100 Series FXOS 섀시 수퍼바이저 간의 연결과 통신을 수행하는 것입니다.

하트비트 통신 채널은 FXOS 섀시와 Firepower Threat Defense 애플리케이션 에이전트 간의 링크 상태를 모니터링하는 역할을 합니다. Firepower Threat Defense 애플리케이션은 특정한 간격으로 FXOS 섀시 수퍼바이저에게 요청 메시지를 전송하며 FXOS 섀시 관리자로부터 적절한 응답을 수신할 때까지 설정된 횟수로 재시도합니다.

Firepower Threat Defense 앱 에이전트와 FXOS 섀시 수퍼바이저 간의 하트비트 메커니즘은 또한 장애에 대한 Hardware Bypass(하드웨어 바이패스) 기능을 모니터링합니다. Firepower 9300 및 4100 Series의 특정 인터페이스 모듈의 경우, Hardware Bypass 기능을 활성화할 수 있습니다. Hardware Bypass는

정전 중에 트래픽이 인라인 인터페이스 쌍 사이에서 계속 흐르도록 합니다. 이 기능은 소프트웨어 또는 하드웨어 오류의 경우 네트워크 연결성을 유지 관리하는 데 사용될 수 있습니다.

다음 예는 앱 에이전트 하트비트 간격을 600밀리초로 설정하고 재시도 간격을 6회로 설정합니다.

```
> app-agent heartbeat interval 600 retry-count 6
```

명령	설명
show app-agent	앱 에이전트 상태를 표시합니다.
show inline-set	인라인 집합 정보를 표시합니다.
show interface	인터페이스 상태 정보를 표시합니다.

asp load-balance per-packet

다중 코어에서 로드 밸런싱 동작을 패킷별 동작으로 변경하려면 **asp load-balance per-packet** 명령을 사용합니다. 로드 밸런싱 메커니즘의 기본값을 복원하려면 이 명령의 **no** 형식을 사용합니다.

asp load-balance per-packet

no asp load-balance per-packet

패킷별 로드 밸런싱은 기본적으로 비활성화되어 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

로드 밸런서의 이 작업은 패킷을 CPU 코어에 배포하고 패킷 순서를 유지 관리하는 것입니다. 기본적으로, 연결은 한번에 하나의 코어를 통해서만 처리될 수 있습니다. 이 동작으로 인해 코어의 수와 비교했을 때 적은 수의 인터페이스/RX 링이 사용 중인 경우 코어의 활용률이 낮습니다. 예를 들어 Firepower Threat Defense 디바이스에서 2개의 기가비트 이더넷 인터페이스만 사용 중인 경우, 2개의 코어만 사용됩니다. (10기가비트 이더넷 인터페이스에는 4개의 RX 링과 기가비트 이더넷(1개의 RX 링) 인터페이스가 있습니다.) 패킷별 로드 밸런싱을 활성화하는 방법으로 로드 밸런서를 최적화하여 추가 코어를 사용할 수 있습니다.

기본 로드 밸런싱 동작은 여러 인터페이스를 사용 중인 경우, 전반적인 시스템 성능을 최적화하는 반면, 패킷별 로드 밸런서는 액티브 상태인 더 적은 수의 인터페이스를 사용할 때 전반적인 시스템 성능을 최적화합니다.

패킷별 로드 밸런싱을 활성화할 경우, 하나의 코어가 인터페이스의 패킷을 처리할 때 다른 코어는 동일한 인터페이스에서 다음 패킷을 수신하고 처리할 수 있습니다. 따라서, 모든 코어가 동일한 인터페이스에서 패킷을 동시에 처리할 수 있습니다.

패킷별 로드 밸런싱은 다음의 경우 성능을 개선합니다.

- 시스템이 패킷을 드롭하는 경우
- **show cpu** 명령은 CPU 사용량이 100%보다 훨씬 더 적다는 것을 보여줍니다. CPU 사용량은 얼마나 많은 코어가 사용되고 있는지 나타내는 훌륭한 지표입니다. 예를 들어, 8코어 시스템에서 2개의 코어가 사용되는 경우, **show cpu**는 25%를, 4개의 코어는 50%를, 6개의 코어는 75%를 보여줍니다.
- 사용 중인 소수의 인터페이스가 있는 경우

참고 일반적으로 Firepower Threat Defense 디바이스에서 64개 미만의 동시 플로우가 있는 경우, 패킷별 로드 밸런싱을 활성화하면 이점보다 더 많은 오버헤드가 발생합니다.

다음 예에서는 기본 로드 밸런싱 동작을 변경하는 방법을 보여줍니다.

```
> asp load-balance per-packet
```

명령	설명
clear asp load-balance history	패킷별 ASP 로드 밸런싱 기록 통계를 생성하고 재설정합니다. OK
show asp load-balance	로드 밸런서 큐 크기를 히스토그램으로 표시합니다. OK

blocks

(**show blocks** 명령으로 표시되는) 블록 진단에 추가 메모리를 할당하려면 **blocks** 명령을 사용합니다. 이 값을 다시 기본값으로 설정하려면 이 명령의 **no** 형식을 사용합니다.

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

memory_size	(선택 사항) 블록 진단용 메모리 크기에 동적 값을 적용하지 않고 바이트 단위로 설정합니다. 이 값이 사용 가능 메모리보다 클 경우 오류 메시지가 나타나며 값이 적용되지 않습니다. 이 값이 사용 가능 메모리의 50%보다 클 경우 경고 메시지가 나타나지만 값은 적용됩니다.

블록 진단 추적에 할당되는 기본 메모리는 2136바이트입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

현재 할당된 메모리를 보려면 **show blocks queue history** 명령을 입력합니다.

Firepower Threat Defense 디바이스를 다시 로드할 경우 메모리 할당이 기본 설정으로 돌아갑니다.

할당되는 메모리의 양은 최대 150KB이지만, 사용 가능 메모리의 50%를 초과할 수 없습니다. 선택적으로 메모리 크기를 직접 지정할 수 있습니다.

다음 예에서는 블록 진단의 메모리 크기를 늘립니다.

```
> blocks queue history enable
```

다음 예에서는 메모리 크기를 3000바이트로 늘립니다.

```
> blocks queue history enable 3000
```

다음 예에서는 메모리 크기를 3000바이트로 늘리려 하지만 이 값이 사용 가능 메모리보다 큽니다.

```
> blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

다음 예에서는 메모리 크기를 3000바이트로 늘리지만, 이 값이 사용 가능 메모리의 50%보다 큽니다.

```
> blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

명령	설명
clear blocks	시스템 버퍼 통계를 지웁니다.
show blocks	시스템 버퍼 사용량을 표시합니다.

capture

패킷 스니핑 및 네트워크 오류 격리를 위해 패킷 캡처 기능을 활성화하려면 **capture** 명령을 사용합니다. 패킷 캡처 기능을 비활성화하려면 이 명령의 no 형식을 사용합니다.

네트워크 트래픽 캡처:

capture *capture_name* [**type** {**asp-drop** [**all** | *drop-code*] | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] }] {**interface** {*interface_name* | **asa_mgmt_plane**} } [**buffer** *buf_size*] [**ethernet-type** *type*] [**headers-only**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*] [**match** *protocol* {**host** *source_ip* | *source_ip mask* | **any**} [*operator src_port*] {**host** *dest_ip* | *dest_ip mask* | **any**} [*operator dest_port*]]

클러스터 제어 링크 트래픽 캡처:

capture *capture_name* **type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes*] [**circular-buffer**] [**real-time** [**dump**] [**detail**]]

capture *capture_name* **interface cluster** [**buffer** *buf_size*] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**trace**] [**match** *protocol* {**host** *source_ip* | *source_ip mask* | **any**} [*operator src_port*] {**host** *dest_ip* | *dest_ip mask* | **any**} [*operator dest_port*]]

패킷 클러스터 전체 캡처:

cluster exec capture *capture_name arguments*

패킷 캡처 중지 또는 제거:

no capture *capture_name* [*arguments*]

any	단일 IP 주소 및 마스크가 아니라 임의의 IP 주소를 지정합니다.
all	가속 보안 경로에서 드롭하는 모든 패킷을 캡처합니다.
asp-drop*drop-code*	(선택 사항) 가속 보안 경로에서 드롭하는 패킷을 캡처합니다. drop-code는 가속 보안 경로에서 드롭하는 트래픽의 유형을 지정합니다. drop-code의 목록은 CLI 도움말을 참조하십시오. **packet-length**, **circular-buffer**, **buffer** 키워드와 함께 이 키워드를 입력할 수 있습니다. 그러나 **interface** 또는 **ethernet-type** 키워드는 함께 사용하지 않습니다. 클러스터에서는 유닛 간의 드롭된 전달 데이터 패킷도 캡처합니다.
buffer*buf_size*	(선택 사항) 패킷을 저장할 버퍼 크기(바이트)를 정의합니다. 바이트 버퍼가 차면 패킷 캡처를 중지합니다. 클러스터에서 사용될 때는 모든 유닛의 합계가 아니라 유닛별 크기입니다.

capture_name	패킷 캡처의 이름을 지정합니다.. 여러 트래픽 유형을 캡처하려면 여러 **capture** 구문에 동일한 이름을 사용합니다. **show capture** 명령을 사용하여 캡처 컨피그레이션을 볼 경우 모든 옵션이 한 행으로 결합됩니다.
circular-buffer	(선택 사항) 버퍼가 차면 처음부터 버퍼를 덮어씁니다.
ethernet-type*type*	(선택 사항) 캡처할 이더넷 유형을 선택합니다. 지원되는 이더넷 유형은 8021Q, ARP, IP, IP6, IPX, LACP, PPPOED, PPPOES, RARP, VLAN 등입니다. 802.1Q 또는 VLAN 유형에는 예외 사항이 있습니다. 802.1Q 태그는 자동으로 건너뛰며, 내부 이더넷 유형은 매칭에 사용됩니다.
headers-only	(선택 사항) 데이터 없이 캡처할 패킷의 레이어 2 및 레이어 3/4 헤더를 선택합니다.
host*source_ip*, *dest_ip*	패킷을 보내거나 가져오는 호스트의 단일 IP 주소를 지정합니다.
inline-tag*tag*	특정 SGT 값의 태그를 지정하거나 미지정 상태로 두어 임의의 SGT 값을 갖는 태그 있는 패킷을 캡처합니다.
interface*interface_name*	패킷 캡처를 사용할 인터페이스의 이름을 설정합니다. **type asp-drop**을 제외하고 캡처할 모든 패킷을 처리하는 인터페이스를 구성해야 합니다. 여러 **capture** 명령을 동일한 이름으로 사용하여 여러 인터페이스를 구성할 수 있습니다. 관리 플레인에서 패킷을 캡처하려면 **interface** 키워드를 **asa_mgmt_plane**이라는 인터페이스 이름과 함께 사용할 수 있습니다. 클러스터 제어 링크 인터페이스의 트래픽을 캡처하기 위해 **cluster**를 인터페이스 이름으로 지정할 수 있습니다. type **lacp** 캡처가 구성된 경우 인터페이스 이름은 물리적 이름입니다.
ikev1, **ikev2**	IKEv1 또는 IKEv2 프로토콜 정보를 캡처합니다.
isakmp	(선택 사항) VPN 연결에 대해 ISAKMP 트래픽을 캡처합니다. ISAKMP 하위 시스템은 상위 레이어 프로토콜에 대한 액세스 권한이 없습니다. 이 캡처는 의사 캡처로서 PCAP 파서를 충족하기 위해 물리적, IP, UDP 레이어를 결합합니다. 피어 주소는 SA 교환에서 얻으며 IP 레이어에 저장됩니다.
lacp	(선택 사항) LACP 트래픽을 캡처합니다. 구성된 경우 인터페이스 이름은 물리적 인터페이스 이름입니다.
mask	IP 주소의 서브넷 마스크입니다. 예를 들어, Class C 마스크의 경우 255.255.255.0입니다.
match*protocol*	캡처할 패킷의 필터링을 허용하기 위해 5-튜플과 매칭하는 패킷을 지정합니다. 한 행에서 이 키워드를 최대 3번 사용할 수 있습니다.

operator src_port, *dest_port*	(선택 사항) 소스 또는 목적지에서 사용하는 포트 번호와 매칭합니다. 허용되는 연산자는 다음과 같습니다. • **lt** - 보다 작음 • **gt** - 보다 큼 • **eq** - 같음 • **neq** - 같지 않음 • **range** - 범위
packet-length*bytes*	(선택 사항) 캡처 버퍼에 저장할 각 패킷의 최대 바이트 수를 설정합니다.
raw-data	(선택 사항) 하나 이상의 인터페이스에서 인바운드 및 아웃바운드 패킷을 캡처합니다.
trace*trace_count*	(선택 사항) 패킷 추적 정보 및 캡처할 패킷 수를 캡처합니다. 이 옵션을 액세스 목록과 함께 사용하여 데이터 경로에 추적 패킷을 삽입함으로써 패킷이 예상대로 처리되었는지 여부를 확인할 수 있습니다.
type	(선택 사항) 캡처한 데이터의 유형을 지정합니다.

참고 다음 키워드는 파서에 표시되지만, Firepower Threat Defense에서 지원되지 않는 **asa_dataplane, cplane, webvpn** 등의 기능과 관련이 있습니다.

기본값은 다음과 같습니다.

- 기본 **type**은 **raw-data**입니다.
- 기본 **buffer***size*는 512KB입니다.
- 기본 Ethernet 유형은 IP 패킷입니다.
- 기본 **packet-length**는 1518바이트입니다.

릴리스	수정 사항
6.1	이 명령을 도입했습니다.

사용 가이드라인

패킷 캡처는 연결 문제를 해결하거나 의심스러운 활동을 모니터링할 때 유용합니다. 다중 캡처를 생성할 수 있습니다. **capture** 명령은 실행 중인 컨피그레이션에 저장되지 않으며, 가용성이 높은 상태에서는 스탠바이 유닛에 복사되지 않습니다.

Firepower Threat Defense 디바이스는 자신을 지나는 모든 IP 트래픽을 추적하고 자신을 목적지로 하는 모든 IP 트래픽을 캡처할 수 있습니다. 여기에는 모든 관리 트래픽(예: SSH 및 텔넷 트래픽)도 포함됩니다.

Firepower Threat Defense 아키텍처는 패킷 처리를 위한 서로 다른 3가지 프로세서 집합으로 구성됩니다. 이 아키텍처는 캡처 기능에 일정한 제한을 가합니다. 일반적으로 Firepower Threat Defense 디바이스의 패킷 전달 기능 대부분은 2개의 프론트엔드 네트워크 프로세서에 의해 처리되며, 이 프로세서에서 애플리케이션 검사를 필요로 하는 경우에만 컨트롤 플레인 범용 프로세서에 패킷을 보냅니다. 가속 경로 프로세서에 세션 누락이 있을 경우에만 세션 관리 경로 네트워크 프로세서에 패킷을 보냅니다.

Firepower Threat Defense 디바이스에서 전달하거나 드롭하는 모든 패킷이 2개의 프론트엔드 네트워크 프로세서를 거치므로 패킷 캡처 기능은 이 네트워크 프로세서에 구현됩니다. 따라서 Firepower Threat Defense 디바이스를 지나는 모든 패킷은 이 프론트엔드 프로세서에서 캡처할 수 있습니다. 단, 이 트래픽 인터페이스에 대해 알맞은 캡처가 구성되어야 합니다. 인그레스(ingress)에서는 패킷이 인터페이스에 도착할 때 패킷이 캡처됩니다. 이그레스(egress)에서는 패킷이 외부로 전송되기 직전에 캡처됩니다.

캡처 보기

패킷 캡처를 보려면 **show capture***name* 명령을 사용합니다. 파일에 캡처를 저장하려면 **copy capture** 명령을 사용합니다. 웹 브라우저에서 패킷 캡처 정보를 보려면 **https://***FTP-ip-address*/*admin*/**capture/***capture_name*[**/pcap**] 명령을 사용합니다. **pcap** 키워드를 지정할 경우 libpcap-format 형식의 파일이 웹 브라우저에 다운로드되며 웹 브라우저에서 이를 저장할 수 있습니다. libcap 파일은 TCPDUMP 또는 Ethereal로 볼 수 있습니다.

버퍼 내용을 ASCII 형식으로 TFTP 서버에 복사할 경우 헤더만 볼 수 있습니다. 패킷의 세부 사항 및 16진수 덤프는 볼 수 없습니다. 세부 사항 및 16진수 덤프를 보려면 버퍼를 PCAP 형식으로 전송하고 TCPDUMP 또는 Ethereal로 읽어야 합니다.

캡처 삭제

키워드 없이 **no capture**를 입력하면 캡처가 삭제됩니다. 캡처를 유지하려면 **interface** 키워드를 지정합니다. 캡처는 지정된 인터페이스에서 분리되어 보존됩니다.

클러스터링

capture 명령 앞에 **cluster exec**를 사용하여 **capture** 명령을 하나의 유닛에서 실행하고 이와 동시에 기타 모든 유닛에서 이 명령을 실행할 수 있습니다. 클러스터 전체 캡처를 수행한 다음 클러스터에 있는 모든 유닛의 동일한 캡처 파일을 TFTP 서버에 동시에 복사하려면 마스터 유닛에서 **cluster exec copy** 명령을 입력합니다.

cluster exec capture*capture_namearguments*

cluster exec copy /pcap capture:*cap_name***tftp://***location***/***path***/***filename***.pcap**

유닛당 하나씩인 여러 PCAP 파일이 TFTP 서버에 복사됩니다. 목적지 캡처 파일 이름에는 유닛 이름이 자동으로 추가됩니다(예: filename_A.pcap, filename_B.pcap 등). 이 예에서는 A와 B가 클러스터 유닛 이름입니다.

참고 파일 이름의 끝에 유닛 이름을 추가하면 다른 목적지 이름이 생성됩니다.

제한 사항

다음은 캡처 기능의 몇 가지 제한 사항입니다. 이러한 제한 대부분은 Firepower Threat Defense 아키텍처의 분산 특성 및 Firepower Threat Defense 디바이스에서 사용하는 하드웨어 가속기에서 비롯된 것입니다.

- 인라인 SGT 태그 처리된 패킷의 경우, 캡처된 패킷은 PCAP 뷰어에서 이해하지 못할 추가 CMD 헤더를 포함합니다.
- 인그레스 인터페이스가 없고 전역 인터페이스가 없을 경우 백플레인에서 전송된 패킷은 제어 패킷으로 간주됩니다. 이 패킷은 액세스 목록 검사를 건너뛰므로 항상 캡처됩니다.
- show capture 명령은 특정 asp-drop을 캡처할 때 정확한 이유를 보여줍니다. 그러나 show capture 명령은 모든 asp-drop을 캡처할 때 정확한 이유를 보여주지는 않습니다.

패킷을 캡처하려면 다음 명령을 입력합니다.

```
> capture captest interface inside
> capture captest interface outside
```

웹 브라우저에서 다음 위치로 이동하면 실행된 **capture** 명령인 "captest"의 내용을 볼 수 있습니다.

```
https://171.69.38.95/admin/capture/captest
```

(웹 브라우저에서 사용하는) libpcap 파일을 로컬 시스템에 다운로드하려면 다음 명령을 입력합니다.

```
https://171.69.38.95/capture/http/pcap
```

다음 예에서는 ARP 패킷을 캡처하는 방법을 보여줍니다.

```
> capture arp ethernet-type arp interface outside
```

클러스터링을 위한 캡처

클러스터의 모든 유닛에서 캡처를 활성화하기 위해 각 명령의 앞에 cluster exec 키워드를 추가할 수 있습니다.

다음 예에서는 클러스터링 환경에서 LACP 캡처를 생성하는 방법을 보여줍니다.

```
> capture lacp type lacp interface gigabitEthernet0/0
```

다음 예는 클러스터링 링크에서 제어 경로 패킷의 캡처를 생성하는 방법을 보여줍니다.

```
> capture cp interface cluster match udp any eq 49495 any
> capture cp interface cluster match udp any any eq 49495
```

다음 예는 클러스터를 지나는 데이터 경로 트래픽을 캡처하는 방법을 보여줍니다.

```
> capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
> capture abc interface inside match dup host 1.1.1.1 any
```

명령	설명
clear capture	캡처 버퍼를 지웁니다.
copy capture	서버에 캡처 파일을 복사합니다.
show capture	옵션을 지정하지 않은 경우의 캡처 컨피그레이션을 표시합니다.

capture-traffic

Firepower Threat Defense 인터페이스를 통과하는 패킷을 가로채고 캡처하려면 **capture-traffic** 명령을 사용합니다. 관리 인터페이스(br1) 또는 트래픽 인터페이스 중에서 표시되는 옵션 목록의 정수식과 일치하는 지정된 Firepower Threat Defense 도메인에서 트래픽을 캡처할 수 있습니다.

capture-traffic

도메인 및 TCP 덤프 옵션에 대한 프롬프트가 표시됩니다.

domain	트래픽이 캡처되는 위치의 도메인을 지정합니다. • 0 — br1, 관리 인터페이스의 트래픽을 캡처합니다. • 1 — 라우터, 구성된 데이터 인터페이스의 트래픽을 캡처합니다.
-A	각 패킷(해당 링크 수준 헤더 제외)을 ASCII로 인쇄합니다. 웹 페이지를 캡처하는 데 편리합니다.
-B	운영 체제 캡처 버퍼 크기를 buffer_size로 설정합니다.
-c	count 패킷을 수신한 후에 종료됩니다.
-C	savefile에 원시 패킷을 쓰기 전에, 파일이 현재 file_size보다 큰지 여부를 확인하고, 더 큰 경우 현재 savefile을 닫고 새 savefile을 엽니다. 첫 번째 savefile 다음의 savefile은 -w 플래그로 지정된 이름을 갖게 되고 이후에 오는 숫자는 1에서 시작하며 높은 수로 계속됩니다. file_size 단위는 수백 만 바이트입니다(1,000,000바이트이며 1,048,576바이트 아님).
-d	사용자가 읽을 수 있는 형식에서 컴파일된 패킷 매칭 코드를 표준 출력 및 중지부에 덤프합니다.
-dd	패킷 매칭 코드를 C 프로그램 조각으로 덤프합니다.
-ddd	십진수로 패킷 매칭 코드를 덤프합니다(앞에 카운트가 옴)

-D	시스템에서 사용 가능한 네트워크 인터페이스 목록을 인쇄하고 이 인터페이스에서 tcpdump가 패킷을 캡처합니다. 각 네트워크 인터페이스에 대해 인터페이스의 텍스트 설명이 이어질 수 있는 번호 및 인터페이스 이름이 인쇄됩니다. 인터페이스 이름 또는 번호는 캡처를 수행할 인터페이스를 지정하기 위해 -i 플래그에 제공될 수 있습니다. 이것은 시스템(Windows 시스템 또는 ifconfig - a가 없는 UNIX 시스템)을 나열하기 위한 명령이 없는 시스템에서 유용할 수 있습니다. 이 번호는 Windows 2000 이상인 시스템에서 유용할 수 있으며 이 경우 인터페이스 이름은 약간 복잡한 문자열입니다. tcpdump가 pcap_findaclldevs() 함수가 없는 libpcap의 이전 버전으로 구축된 경우 -D 플래그는 지원되지 않습니다.
-e	각 덤프 라인에 링크 수준 헤더를 인쇄합니다.
-E	addr로 주소가 지정된 IPsec ESP 패킷의 암호 해독을 위해 spi@ipaddr algo:secret을 사용하고 보안 파타미터 인덱스 값 spi를 포합합니다. 이 조합은 쉼표 또는 줄바꿈 구분과 함께 반복될 수 있습니다.
-f	'외부' Ipv4 주소를 기호로 인쇄하는 대신 숫자로 인쇄합니다(이 옵션은 Sun의 NIS 서버에서 심각한 중추부 손상을 해결하기 위한 것이며 보통은 로컬이 아닌 인터넷 번호의 변환을 영구적으로 중단합니다.). '외부' IPv4 주소의 테스트는 캡처가 수행되는 대상인 인터페이스의 IPv4 주소 및 넷마스크를 사용하여 수행됩니다. 캡처가 수행되는 대상인 인터페이스에 주소 또는 넷마스크가 없거나 캡처가 Linux의 '모든' 인터페이스에서 수행되기 때문에 IP 주소 또는 넷마스크를 사용할 수 없는 경우, 둘 이상의 인터페이스에서 캡처될 수 있으며 이 옵션은 제대로 작동하지 않습니다.
-F	필터 표현식에 대한 입력으로 파일을 사용합니다. 커맨드 라인에서 지정된 추가 표현식은 무시됩니다.
-G	이 옵션이 지정된 경우, -w 옵션을 사용하여 지정된 덤프 파일이 rotate_seconds 초마다 순환합니다. Savefiles는 strftime(3)에서 정의된 대로 시간 형식을 포함해야 하는 -w로 지정된 이름을 지닙니다. 시간 형식이 지정되지 않은 경우, 각각의 새 파일이 이전 파일을 덮어씁니다. -C 옵션과 함께 사용된 경우, 파일 이름은 'file<count>' 형식을 사용합니다.
-I	인터페이스를 '모니터 모드'로 설정합니다. 이 옵션은 IEEE 802.11 Wi-Fi 인터페이스에서만 지원되며 일부 운영 체제에서만 지원됩니다.

-K	TCP 체크섬을 확인하려고 시도하지 않습니다. 이 옵션은 하드웨어에서 TCP 체크섬 계산을 수행하는 인터페이스에 유용하며 기타 경우 모든 발신 TCP 체크섬이 불량으로 플래그가 지정됩니다.
-l	Stdout 라인을 버퍼링되게 합니다. 캡처하는 동안 데이터를 확인하려는 경우 유용합니다. 예: ‘‘tcpdump -l | tee dat” 또는 “tcpdump -l > dat & tail -f dat”.
-L	인터페이스의 알려진 데이터 링크 유형을 나열하고 종료합니다.
-m	파일 모듈에서 SMI MIB 모듈 정의를 로드합니다. 이 옵션은 여러 MIB 모듈을 tcpdump에 로드하기 위해 여러 번 사용될 수 있습니다.
-M	암호를 TCP-MD5 옵션(RFC 2385)을 사용하는 TCP 세그먼트에서 발견된 다이제스트를 검증하기 위한 공유 암호로 사용합니다(암호가 있는 경우).
-n	주소를 이름으로 변환하지 마십시오(예: 호스트 주소, 포트 번호 등).
-N	호스트 이름의 도메인 이름 자격을 인쇄하지 않습니다. 예를 들어, 이 플래그를 지정한 경우 tcpdump는 “nic.ddn.mil” 대신 “nic”를 인쇄합니다.
-O	패킷 매칭 코드 최적화 프로그램을 실행하지 않습니다. 이 옵션은 최적화 프로그램에서 버그가 의심되는 경우에만 유용합니다.
-p	인터페이스를 프로미스큐어스 모드로 설정하지 않습니다. 다른 몇 가지 이유 때문에 인터페이스가 프로미스큐어스 모드일 수 있습니다. 따라서 `-p'는 `ether host {local-hw-addr} 또는 ether broadcast'에 대한 약어로 사용될 수 없습니다.
-q	빠른 출력입니다. 더 적은 프로토콜 정보를 인쇄하므로 출력 라인이 더 짧습니다.
-R	ESP/AH 패킷이 기존 사양(RFC1825 ~ RFC1829)에 기반하는 것으로 가정합니다. 이 옵션이 지정된 경우, tcpdump는 재생 방지 필드를 인쇄하지 않습니다. ESP/AH 사양에 프로토콜 버전 필드가 없으므로 tcpdump가 ESP/AH 프로토콜 버전을 추론할 수 없습니다.
-r	파일(-w 옵션을 사용하여 생성됨)에서 패킷을 읽습니다. 표준 입력은 파일이 “-”인 경우 사용됩니다.
-S	상대적인 TCP 시퀀스 번호 대신 절대적인 TCP 시퀀스 번호를 인쇄합니다.

-s	기본값인 68(SunOS의 NIT, 최소값은 실제로 96임) 대신 각 패킷의 Snarfs snaplen 바이트 데이터입니다. 68바이트는 IP, ICMP, TCP 및 UDP의 경우 적절하지만 이름 서버 및 NFS 패킷(아래 참조)에서 프로토콜 정보를 자를 수 있습니다. 제한된 스냅샷 때문에 잘려진 패킷은 출력에서 "[|proto]"로 표시되며 이때 proto는 잘림이 발생한 프로토콜 수준의 이름입니다. 대규모 스냅샷을 활용하면 패킷을 처리하는 데 걸리는 시간이 증가하며 패킷 버퍼링 양이 실제적으로 감소합니다. 이 경우 패킷이 손실될 수 있습니다. 사용자가 관심을 가진 프로토콜 정보를 캡처할 가장 작은 수로 snaplen을 제한해야 합니다. snaplen을 0으로 설정하는 것은 전체 패킷을 파악하기 위해 필요한 길이를 사용하는 것을 의미합니다.
-T	지정된 유형으로 해석할 '표현식'에서 선택된 패킷을 실행합니다. 현재 알려진 유형은 aodv(Ad-hoc On-demand Distance Vector protocol), cnfp(Cisco NetFlow protocol), rpc(Remote Procedure Call), rtp(Real-Time Applications protocol), rtcp(Real-Time Applications control protocol), snmp(Simple Network Management Protocol), tftp(Trivial File Transfer Protocol), vat(Visual Audio Tool), wb(distributed White Board)입니다.
-t	각 덤프 라인에서 타임스탬프를 인쇄하지 않습니다.
-tt	각 덤프 라인에서 형식화되지 않은 타임스탬프를 인쇄합니다.
-ttt	각 덤프 라인에서 현재 및 이전 라인 간에 델타(마이크로초 해상도)를 인쇄합니다.
-tttt	각 덤프 라인에 있는 날짜가 앞에 오는 기본 형식의 타임스탬프를 인쇄합니다.
-ttttt	각 덤프 라인에서 현재 및 첫 번째 라인 간에 델타(마이크로초 해상도)를 인쇄합니다.
-u	디코딩되지 않은 NFS 핸들을 인쇄합니다.
-U	- w 옵션 "packet-buffered"를 통해 출력을 저장합니다. 즉 각 패킷이 저장되면 출력 버퍼가 찼을 때만 쓰여지지 않고 출력 파일에 쓰여집니다. tcpdump가 pcap_dump_flush() 함수가 없는 libpcap의 이전 버전으로 구축된 경우 -U 플래그는 지원되지 않습니다.
-v	구문 분석 및 인쇄 시 (약간 더 많은) 자세한 정보를 출력합니다. 예를 들어, IP 패킷의 TTL(Time to Live), ID, 총 길이 및 옵션이 인쇄됩니다. 또한 IP 및 ICMP 헤더 체크섬 확인과 같이 추가 패킷 무결성 검사를 활성화합니다. -w 옵션이 있는 파일에 쓸 경우 10초 간격으로 캡처된 패킷 수를 보고합니다.
-vv	훨씬 더 자세히 출력합니다. 예를 들어, 추가 필드는 NFS 회신 패킷에서 인쇄되고 SMB 패킷은 완전히 디코딩됩니다.

-vvv	훨씬 더 자세히 출력합니다. 예를 들어, 텔넷 SB... SE 옵션은 전체가 인쇄됩니다. -X 텔넷 옵션은 16진수로도 인쇄됩니다.
-w	원시 패킷을 구문 분석하고 인쇄하는 대신 파일에 씁니다. - r 옵션으로 나중에 인쇄할 수 있습니다. 표준 출력은 파일이 "-"인 경우 사용됩니다.
-W	-C 옵션과 함께 사용되며 이 옵션은 생성된 파일 수를 지정된 수로 제한하고 처음부터 파일 덮어쓰기를 시작하므로 '회전' 버퍼를 생성합니다. 또한 파일을 올바르게 분류하기 위해 최대 파일 수를 지원할 수 있는 충분한 수의 선행 0을 사용하여 파일의 이름을 지정합니다.
-x	각 패킷의 헤더를 인쇄하는 것 외에 구문 분석 및 인쇄할 때 각 패킷(해당 링크 수준 헤더 제외)의 데이터를 16진수로 인쇄합니다. 전체 패킷의 더 작은 수 또는 snaplen 바이트가 인쇄됩니다. 이것은 전체 링크 레이어 패킷이므로 패딩(예: Ethernet)하는 링크 레이어에 대해, 더 높은 레이어 패킷이 필요한 패딩보다 짧은 경우 패딩 바이트도 인쇄됩니다.
-xx	각 패킷의 헤더를 인쇄하는 것 외에 구문 분석 및 인쇄할 때 각 패킷(해당 링크 수준 헤더 포함)의 데이터를 16진수로 인쇄합니다.
-X	각 패킷의 헤더를 인쇄하는 것 외에 구문 분석 및 인쇄할 때 각 패킷(해당 링크 수준 헤더 제외)의 데이터를 16진수 및 ASCII로 인쇄합니다. 이것은 새 프로토콜 분석 시 매우 편리합니다.
-XX	각 패킷의 헤더를 인쇄하는 것 외에 구문 분석 및 인쇄할 때 각 패킷(해당 링크 수준 헤더 포함)의 데이터를 16진수 및 ASCII로 인쇄합니다.
-y	datalinktype에 대한 패킷을 캡처하는 동안 사용할 데이터 링크 유형을 설정합니다.
-z	- C 또는 - G 옵션과 함께 사용되며 이 옵션은 파일이 각 순환 이후에 닫히는 savefile인 위치에서 tcpdump가 'command file'을 실행하게 합니다. 예를 들어, -z gzip 또는 -z bzip2를 지정하면 gzip 또는 bzip2를 사용하여 각 savefile을 압축합니다.
-Z	권한(루트인 경우)을 삭제하고 사용자 ID를 사용자로 변경하고 그룹 ID를 사용자의 기본 그룹으로 변경합니다.

릴리스	수정
6.1	이 명령이 도입되었습니다.

사용 가이드라인

기본적으로 **capture-traffic** 명령은 가로채기하는 각 패킷당 1개의 텍스트 라인을 생성합니다. 각 라인은 타임스탬프, 프로토콜 이름, 소스 및 대상 주소(IP 패킷의 경우, 이는 IP 주소이며 기타 프로토콜의 경우, 인쇄하도록 명시적으로 요청하지 않은 경우 **capture-traffic**이 임의의 식별자를 인쇄하지 않음(**-e** 커맨드 라인 설명 참조)) 및 TCP 시퀀스 번호, 플래그, ARP/ICMP 명령을 포함하는 정보 등을 포함합니다.

캡처를 중지하려면, Control + C를 입력합니다. **-w***outputfile* 옵션을 사용하는 경우, 패킷 캡처는 /var/common/에 있는 파일 이름으로 저장됩니다. 그렇지 않은 경우, 디스플레이에 쓰여집니다.

다음 예는 관리 인터페이스에서 트래픽을 캡처하는 방법을 보여줍니다.

```
> capture-traffic
Please choose domain to capture traffic from:
  0 - br1
  1 - Router
Selection? 0
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
-v
```

명령	설명
show traffic	트래픽 통계를 표시합니다.
show interface	인터페이스 상태 정보를 표시합니다.

cd

현재 작업 디렉토리를 지정된 디렉토리로 변경하려면 **cd** 명령을 사용합니다.

cd [**disk***n***:**][*path*]

disk*n***:**	(선택 사항) 디스크 수를 지정합니다. disk0은 내부 플래시 메모리입니다. 또한 애드온 스토리지 옵션에 따라 disk1 또는 다른 디스크를 사용할 수 있습니다.
path	(선택 사항) 변경 후 디렉토리의 절대 경로.

디렉토리를 지정하지 않을 경우 루트 디렉토리로 변경됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 disk0:에서 “config” 디렉토리를 변경하는 방법을 보여줍니다.

```
> cd disk0:/config/
```

명령	설명
dir	현재의 디렉토리 내용을 표시합니다.
pwd	현재의 작업 디렉토리를 표시합니다.

clear access-list

액세스 목록 카운터를 지우려면 clear access-list 명령을 사용합니다.

clear access-list *id*

id	액세스 목록의 이름입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

clear access-list 명령을 입력할 때 카운터를 지우려면 액세스 목록의 *id*를 지정해야 합니다. ACL 목록을 보려면 **show access-list** 명령을 사용합니다.

다음 예에서는 특정 액세스 목록 카운터를 지우는 방법을 보여줍니다.

```
> clear access-list inbound
```

명령	설명
show access-list	액세스 목록 엔트리를 번호별로 표시합니다.
show running-config access-list	ASA에서 실행 중인 액세스 목록 컨피그레이션을 표시합니다.

clear arp

동적 ARP 항목 또는 ARP 통계를 지우려면 **clear arp** 명령을 사용합니다.

clear arp [**statistics** | *interface_name*]

statistics	ARP 통계를 지웁니다.
interface_name	특정 인터페이스에 대한 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 ARP 통계를 지웁니다.

```
> clear arp statistics
```

명령	설명
show arp statistics	ARP 통계를 표시합니다.
show running-config arp	ARP 시간 초과의 현재 컨피그레이션을 표시합니다.

clear asp

ASP(가속화된 보안 경로) 통계를 지우려면 **clear asp** 명령을 사용합니다.

clear asp {**cluster counter** | **dispatch** | **drop** [**flow** | **frame**] | **event dp-cp** | **inspect-dp snort** {**counters** [**instance** *number* [**queue** *number*]] | **queue-exhaustion** [**snapshot** *number*] | **load-balance history** | **overhead** | **table** [**arp** | **classify** | **filter** [**access-list** *acl_name*]]}

access-list*acl_name*	(선택 사항) 지정된 액세스 목록의 계수기만 지웁니다.
arp	(선택 사항) ASP ARP 테이블에서만 계수기를 지웁니다.
classify	(선택 사항) ASP 분류 테이블에서만 계수기를 지웁니다.
cluster counter	클러스터 카운터를 지웁니다.
카운터	데이터 경로 검사 Snort 카운터를 지웁니다.
dispatch	발송 통계를 지웁니다.
event	컨트롤 플레인 이벤트 통계에 대한 데이터 경로를 지웁니다.
필터	(선택 사항) ASP 필터 테이블에서만 계수기를 지웁니다.
flow	(선택 사항) 삭제된 플로우 통계를 지웁니다.
frame	(선택 사항) 삭제된 프레임/패킷 통계를 지웁니다.
inspect-dp snort	데이터 경로 검사 Snort 통계를 지웁니다.
instance*number*	(선택 사항) 인스턴스 ID에 따라 카운터를 지웁니다.
load-balance history	패킷별 ASP 로드 밸런싱 기록을 지우고 자동 전환이 발생한 횟수를 재설정합니다.
overhead	모든 ASP 멀티프로세서 오버헤드 통계를 지웁니다.
queue*number*	(선택 사항) 인스턴스 ID 및 대기열 ID에 따라 카운터를 지웁니다.
queue-exhaustion	데이터 경로 검사 Snort 대기열 스냅샷을 지웁니다.
snapshot*number*	(선택 사항) 스냅샷 ID에 따라 대기열 소모를 지웁니다.
table	ASP ARP 테이블의 계수기를 지우고 ASP는 테이블을 분류합니다.

릴리스	수정 사항
6.1	이 명령이 추가되었습니다.

다음 예에서는 모든 발송 통계를 지웁니다.

```
> clear asp dispatch
```

명령	설명
show asp	ASP 통계를 표시합니다.

clear bgp

하드 또는 소프트 리컨피그레이션을 통해 BGP(Border Gateway Protocol) 연결을 재설정하려면 **clear bgp** 명령을 사용합니다.

clear bgp {[***** | **external**] [**ipv4 unicast** [*as_number* | *neighbor_address* | **table-map**] | **ipv6 unicast** [*as_number* | *neighbor_address*]] [**soft**] [**in** | **out**] | *as_number* [**soft**] [**in** | **out**] | *neighbor_address* [**soft**] [**in** | **out**] | **table-map**}

*****	모든 현재 BGP 세션이 재설정되도록 지정합니다.
as_number	(선택 사항) 모든 BGP 피어 세션이 재설정될 자동 시스템 번호입니다.
external	모든 외부 BGP 세션이 재설정되도록 지정합니다.
in	(선택 사항) 인바운드 리컨피그레이션을 시작합니다. **in** 및 **out** 키워드 모두 지정되지 않을 경우 인바운드 세션과 아웃바운드 세션 모두 재설정됩니다.
ipv4 unicast	IPv4 주소군 세션에 대해 하드 또는 소프트 리컨피그레이션을 통해 BGP 연결을 재설정합니다.
ipv6 unicast	IPv6 주소군 세션에 대해 하드 또는 소프트 리컨피그레이션을 통해 BGP 연결을 재설정합니다.
neighbor_address	(선택 사항) 식별된 BGP 네이버만 재설정되도록 지정합니다. 이 인수값은 IPv4 또는 IPv6 주소가 될 수 있습니다.
out	(선택 사항) 인바운드 또는 아웃바운드 리컨피그레이션을 시작합니다. **in** 및 **out** 키워드 모두 지정되지 않을 경우 인바운드 세션과 아웃바운드 세션 모두 재설정됩니다.
soft	(선택 사항) 저속 피어(slow-peer) 상태를 강제로 해제하고 원래의 업데이트 그룹으로 이동합니다.
table-map	BGP 라우팅 테이블의 table-map 컨피그레이션 정보를 지웁니다. BGP Policy Accounting 기능으로 구성했던 트래픽-색인 정보를 지우는 데 이 명령을 사용할 수 있습니다.

릴리스	수정
6.1	이 명령이 추가되었습니다.

사용 가이드라인

clear bgp 명령을 사용하여 하드 리셋 또는 소프트 리컨피그레이션을 시작할 수 있습니다. 하드 리셋은 지정된 피어링 세션을 해제하고 재구성하며 BGP 라우팅 테이블을 재구성합니다. 소프트 리컨피그레이션은 기존 피어링 세션을 해제하지 않고 저장된 접두사 정보를 사용하여 BGP 라우팅 테이블을 재구성하고 활성화합니다. 소프트 리컨피그레이션에서는 저장된 업데이트 정보를 사용하므로 업데이트 저장을 위해 메모리를 추가로 사용합니다. 이를 통해 네트워크 중단 없이 새 BGP 정책을 적용할 수 있습니다. 소프트 리컨피그레이션은 인바운드 또는 아웃바운드 세션에 대해 구성할 수 있습니다.

다음 예에서는 모든 bgp 세션이 재설정됩니다.

```
> clear bgp *
```

다음 예에서는 네이버 10.100.0.1과의 인바운드 세션에 대해 소프트 리컨피그레이션이 시작되며 아웃바운드 세션은 영향을 받지 않습니다.

```
> clear bgp 10.100.0.1 soft in
```

다음 예에서는 BGP 네이버 라우터에서 경로 새로 고침 기능이 활성화되고 네이버 172.16.10.2와의 인바운드 세션에 대해 소프트 리컨피그레이션이 시작되며 아웃바운드 세션은 영향을 받지 않습니다.

```
> clear bgp 172.16.10.2 in
```

다음 예에서는 자율 시스템 번호 35700을 갖는 모든 라우터와의 세션에 대해 하드 리셋이 시작됩니다.

```
> clear bgp 35700
```

다음 예에서는 모든 인바운드 eBGP 피어링 세션에 대해 소프트 리컨피그레이션이 구성됩니다.

```
> clear bgp external soft in
```

다음 예에서는 모든 아웃바운드 주소군 IPv4 멀티캐스트 eBGP 피어링 세션이 지워집니다.

```
> clear bgp external ipv4 multicast out
```

다음 예에서는 자율 시스템 65400의 IPv4 유니캐스트 주소군 세션에 속하는 BGP 네이버와의 인바운드 세션에 대해 소프트 리컨피그레이션이 시작됩니다. 아웃바운드 세션은 영향을 받지 않습니다.

```
> clear bgp ipv4 unicast 65400 soft in
```

다음 예에서는 asplain 표기법 4바이트 자동 시스템 번호가 65538이고 IPv4 유니캐스트 주소군 세션에 속하는 BGP 네이버에 대해 하드 리셋이 시작됩니다.

```
> clear bgp ipv4 unicast 65538
```

다음 예에서는 asdot 표기법 4바이트 자동 시스템 번호가 1.2이고 IPv4 유니캐스트 주소군 세션에 속하는 BGP 네이버에 대해 하드 리셋이 시작됩니다.

```
> clear bgp ipv4 unicast 1.2
```

다음 예에서는 IPv4 유니캐스트 피어링 세션에 대해 테이블 맵을 지웁니다.

```
> clear bgp ipv4 unicast table-map
```

clear blocks

소모 상태와 같은 패킷 버퍼 카운터와 기록 정보를 재설정하려면 **clear blocks** 명령을 사용합니다.

clear blocks [**exhaustion** {**history** | **snapshot**} | **export-failed** | **queue** [**history** [**core-local** [*number*]]]]

core-local[*number*]	(선택 사항) 모든 코어 또는 코어 번호를 지정하는 경우 특정 코어에 대해 애플리케이션별로 대기하는 시스템 버퍼를 지웁니다.
exhaustion	(선택 사항) 소모 상태를 지웁니다.
export-failed	(선택 사항) 내보내기에 실패한 카운터를 지웁니다.
history	(선택 사항) 기록을 지웁니다.
대기열	(선택 사항) 대기열 블록을 지웁니다.
스냅샷	(선택 사항) 스냅샷 정보를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

자용 가이드라인

각 풀에서 최저 수위 카운터를 현재 사용 가능 블록으로 재설정합니다. 또한 이 명령은 마지막 버퍼 할당 실패 과정에서 저장된 기록 정보를 지웁니다.

다음 예에서는 블록을 지웁니다.

```
> clear blocks
```

명령	설명
blocks	블록 진단에 할당된 메모리를 늘립니다.

명령	설명
show blocks	시스템 버퍼 사용률을 표시합니다.

clear capture

캡처 버퍼를 지우려면 **clear capture** 명령을 사용합니다.

clear capture {/**all** | *capture_name*}

/all	모든 인터페이스에서 패킷을 지웁니다.
capture_name	패킷 캡처의 이름을 지정합니다..

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

이 예에서는 “example”이라는 캡처 버퍼의 캡처 버퍼를 지우는 방법을 보여줍니다.

```
> clear capture example
```

명령	설명
capture	패킷 스니핑 및 네트워크 오류 격리를 위해 패킷 캡처 기능을 활성화합니다.
show capture	옵션을 지정하지 않은 경우의 캡처 컨피그레이션을 표시합니다.

clear cluster info

클러스터 통계를 지우려면 **clear cluster info** 명령을 사용합니다.

clear cluster info {**flow-mobility counters** | **trace** | **transport**}

flow-mobility counters	클러스터 플로우 모빌리티 카운터를 지웁니다.
trace	클러스터 이벤트 추적 정보를 지웁니다.
transport	클러스터 전송 통계를 지웁니다..

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

클러스터 통계를 보려면 show cluster info 명령을 사용합니다.

다음 예에서는 클러스터 이벤트 추적 정보를 지웁니다.

```
> clear cluster info trace
```

명령	설명
show cluster info	클러스터 통계를 표시합니다.

clear conn

특정한 연결 또는 여러 연결을 지우려면 **clear conn** 명령을 사용합니다.

clear conn {**all** | **protocol** {**tcp** | **udp** | **sctp**} | **address** *ip*[**-***ip*] [*netmask mask*] | **port** *port*[**-***port*] | **inline-set** *name* | **security-group** {**name** | **tag**} *attribute*} | **user** [*domain_nickname*\\]*user_name* | **user-group** [*domain_nickname*\\]*user_group_name*] | **zone** [*zone_name*]}

address*ip*[**-***ip*]	지정된 소스 또는 대상 IP 주소(IPv4 또는 IPv6)와의 연결을 지웁니다. 범위를 지정하려면 대시(-)를 사용하여 IP 주소를 구분합니다. 예: 10.1.1.1-10.1.1.5
all	to-the-box 연결을 포함한 모든 연결을 지웁니다. all 키워드를 사용하지 않으면 through-the-box 연결만 지워집니다.
inline-set*name*	지정된 인라인 집합과 일치하는 연결을 지웁니다.
netmask*mask*	(선택 사항) 지정된 IP 주소에서 사용할 서브넷 마스크를 지정합니다.
port*port*[**-***port*]	지정된 소스 또는 대상 포트와의 연결을 지웁니다. 범위를 지정하려면 대시(-)를 사용하여 포트 번호를 구분합니다. 예: 1000-2000
protocol {**tcp** | **udp** | **sctp**}	지정된 프로토콜과의 연결을 지웁니다.
security-group {**name** | **tag**} *attribute*	지정된 보안 그룹 특성과의 연결을 지웁니다.
user [*domain_nickname*\] *user_name*	지정된 사용자에게 속한 연결을 지웁니다. *domain_nickname* 인수를 포함하지 않으면 시스템은 기본 도메인에서 해당 사용자의 연결을 지웁니다.
user-group [*domain_nickname*\\] *user_group_name*]	지정된 사용자 그룹에 속한 연결을 지웁니다. *domain_nickname* 인수를 포함하지 않으면 시스템은 기본 도메인에서 해당 사용자 그룹의 연결을 지웁니다.
zone [*zone_name*]	보안 영역에 속한 연결을 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

컨피그레이션에 대한 보안 정책을 변경하면 모든 새 연결에서는 새로운 보안 정책을 사용합니다. 기존 연결에서는 연결 설정 당시에 구성된 정책을 계속 사용합니다. 모든 연결에서 새 정책을 사용하게 하려면 **clear conn** 명령을 사용하여 현재의 연결을 끊고 새 정책을 통해 다시 연결하게 해야 합니다. 또는 **clear local-host** 명령을 사용하여 호스트별로 연결을 지우거나, 동적 NAT를 사용하는 연결에 대해서는 **clear xlate** 명령을 사용할 수 있습니다.

디바이스에서 보조 연결을 허용하기 위해 핀홀을 생성할 경우 이는 **show conn** 명령 출력에서 불완전한 연결로 표시됩니다. 이 불완전한 연결을 지우려면 **clear conn** 명령을 사용합니다.

참고 이 명령은 관리 인터페이스에 대한 연결을 지우지 않습니다. 이 명령은 데이터 인터페이스 또는 진단 인터페이스에 대한 관리 연결만 지울 수 있습니다.

다음 예에서는 모든 연결을 확인한 다음 10.10.10.108에서의 관리 연결을 지우는 방법을 보여줍니다.

```
> show conn all
TCP mgmt 10.10.10.108:4168 NP Identity Ifc 10.0.8.112:22, idle 0:00:00,
bytes 3084, flags UOB
> clear conn address 10.10.10.108
```

명령	설명
clear local-host	특정 로컬 호스트 또는 모든 로컬 호스트에 의한 연결을 모두 지웁니다.
clear xlate	동적 NAT 세션 및 NAT를 사용하는 모든 연결을 지웁니다.
show conn	연결 정보를 표시합니다.
show local-host	로컬 호스트의 네트워크 상태를 표시합니다.
show xlate	NAT 세션을 표시합니다.

clear console-output

현재 캡처된 콘솔 출력을 제거하려면 **clear console-output** 명령을 사용합니다.

clear console-output

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 현재 캡처된 콘솔 출력을 제거하는 방법을 보여줍니다.

```
> clear console-output
```

명령	설명
show console-output	캡처된 콘솔 출력을 표시합니다.
show running-config console timeout	디바이스에 대한 콘솔 연결의 유휴 시간 제한을 표시합니다.

clear counters

프로토콜 스택 카운터를 지우려면 **clear counters** 명령을 사용합니다.

clear counters [**all** | **summary** | **top** *n*] [**detail**] [**protocol** *protocol_name* [*counter_name*]] [**threshold** *n*]

all	(선택 사항) 모든 필터 세부사항을 지웁니다.
counter_name	(선택 사항) 이름을 기준으로 카운터를 지정합니다. 사용 가능한 카운터 이름을 보려면 **show counters protocol** 명령을 사용합니다.
detail	(선택 사항) 자세한 카운터 정보를 지웁니다.
protocol*protocol_name*	(선택 사항) 지정된 프로토콜의 카운터를 지웁니다.
요약	(선택 사항) 카운터 요약을 지웁니다.
threshold*n*	(선택 사항) 지정된 임계값에 도달하거나 이를 초과할 때 카운터를 지웁니다. 범위는 1~4294967295입니다.
top*n*	(선택 사항) 지정된 임계값에 도달하거나 이를 초과할 때 카운터를 지웁니다. 범위는 1~4294967295입니다.

clear counters summary detail 명령이 기본 설정입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 프로토콜 스택 카운터를 지우는 방법을 보여줍니다.

```
> clear counters
```

명령	설명
show counters	프로토콜 스택 카운터를 표시합니다.

clear cpu profile

CPU 프로파일링 통계를 지우려면, **clear cpu** 명령을 사용하십시오.

clear cpu profile

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 충돌 파일을 삭제하는 방법을 보여줍니다.

```
> clear cpu profile
```

명령	설명
show cpu	CPU 정보를 표시합니다.
show cpu profile	CPU 프로파일링 데이터를 표시합니다.

clear crashinfo

플래시 메모리에서 충돌 파일의 내용을 삭제하려면 **clear crashinfo** 명령을 사용합니다.

clear crashinfo [**module** {**0** | **1**}]

module{**0**	**1**}	(선택 사항) 슬롯 0 또는 1에서 모듈의 충돌 파일을 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 충돌 파일을 삭제하는 방법을 보여줍니다.

```
> clear crashinfo
```

명령	설명
crashinfo force	시스템을 강제로 충돌시킵니다.
crashinfo test	충돌 정보를 플래시 메모리의 파일에 저장하는 시스템의 기능을 테스트합니다.
show crashinfo	플래시 메모리에 저장된 충돌 파일의 내용을 표시합니다.

clear crypto accelerator statistics

암호화 가속기 MIB에서 전역 및 가속기 관련 통계를 지우려면 **clear crypto accelerator statistics** 명령을 사용합니다.

clear crypto accelerator statistics

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

글로벌 구성 모드에서 입력한 다음 예에서는 crypto accelerator 통계를 표시합니다.

```
> clear crypto accelerator statistics
>
```

명령	설명
clear crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 지웁니다.
show crypto accelerator statistics	crypto accelerator MIB의 전역 및 가속기 관련 통계를 표시합니다.
show crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 표시합니다.

clear crypto ca crls

지정된 트러스트 포인트와 연결된 모든 CRL을 CRL 캐시에서 없애고 신뢰 풀과 연결된 모든 CRL을 캐시에서 없애거나 모든 CRL의 CRL 캐시를 없애려면 **clear crypto ca crls** 명령을 사용합니다.

clear crypto ca crls [**trustpool** | **trustpoint** *trust_point_name*]

trustpoint*trust_point_name*	신뢰 지점의 이름. 이름을 지정하지 않을 경우 이 명령은 시스템에 캐싱된 모든 CRL을 지웁니다. 신뢰 지점 이름 없이 신뢰 지점 키워드를 지정할 경우 명령은 실패합니다.
trustpool	신뢰 풀의 인증서와 연결된 CRL에만 해당 작업을 적용하도록 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

별도의 다음 예에서는 모든 신뢰 풀 CRL 및 trustpoint123과 연결된 모든 CRL을 지우고 캐싱된 모든 CRL을 디바이스에서 제거합니다.

```
> clear crypto ca crl trustpool
> clear crypto ca crl trustpoint trustpoint123
> clear crypto ca crl
```

명령	설명
show crypto ca crl	캐싱된 모든 CRL 또는 지정된 신뢰 지점에 대해 캐싱된 CRL을 표시합니다.

clear crypto ca trustpool

신뢰 풀에서 모든 인증서를 제거하려면 **clear crypto ca trustpool** 명령을 사용합니다.

clear crypto ca trustpool noconfirm

noconfirm	사용자 확인 프롬프트를 억제합니다. 명령은 요청대로 처리됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 인증서를 지웁니다.

```
> clear crypto ca trustpool
>
```

명령	설명
crypto ca trustpool export	PKI 신뢰 풀을 구성하는 인증서를 내보냅니다.
crypto ca trustpool import	PKI 신뢰 풀을 구성하는 인증서를 가져옵니다.
crypto ca trustpool remove	신뢰 풀에서 지정된 단일 인증서를 제거합니다.

clear crypto ikev1

IPsec IKEv1 SA 또는 통계를 제거하려면 **clear crypto ikev1** 명령을 사용합니다.

clear crypto ikev1 {**sa** [*ip_address*] | **stats**}

sa*ip_address*	SA를 지웁니다. 모든 IKEv1 SA를 지우려면, IP 주소를 지정하지 않고 이 옵션을 사용합니다. 그렇지 않으면, 지울 SA의 IPv4 또는 IPv6 주소를 지정합니다.
stats	IKEv1 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 Firepower Threat Defense 디바이스에서 IPsec IKEv1 통계를 모두 제거합니다.

```
> clear crypto ikev1 stats
>
```

다음 예에서는 피어 IP 주소가 10.86.1.1인 SA를 삭제합니다.

```
> clear crypto ikev1 sa 10.86.1.1
>
```

명령	설명
show ipsec sa	카운터, 엔트리, 맵 이름, 피어 IP 주소, 호스트 이름 등 IPsec SA에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 구성을 표시합니다.

clear crypto ikev2

IPsec IKEv2 SA 또는 통계를 제거하려면 **clear crypto ikev2** 명령을 사용합니다.

clear crypto ikev2 {**sa** [*ip_address*] | **stats**}

sa*ip_address*	SA를 지웁니다. 모든 IKEv2 SA를 지우려면 IP 주소를 지정하지 않고 이 옵션을 사용합니다. 그렇지 않으면, 지울 SA의 IPv4 또는 IPv6 주소를 지정합니다.
stats	IKEv2 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 IPsec IKEv2 통계를 Firepower Threat Defense 디바이스에서 제거합니다.

```
> clear crypto ikev2 stats
>
```

다음 예에서는 피어 IP 주소가 10.86.1.1인 SA를 삭제합니다.

```
> clear crypto ikev2 sa 10.86.1.1
>
```

명령	설명
show ipsec sa	카운터, 엔트리, 맵 이름, 피어 IP 주소, 호스트 이름 등 IPsec SA에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 구성을 표시합니다.

clear crypto ipsec sa

IPsec SA 카운터, 엔트리, 암호 맵 또는 피어 연결을 제거하려면 **clear crypto ipsec sa** 명령을 사용합니다.

clear crypto ipsec sa [**counters** | **entry** *ip_address* {**esp** | **ah**} *spi* | **inactive** | **map** *map_name* | **peer** *ip_address*]

ah	인증 헤더입니다.
counters	모든 SAP별 IPsec 통계를 지웁니다.
entry*ip_address*	지정된 IP 주소/호스트 이름, 프로토콜, SPI 값과 매칭하는 터널을 삭제합니다.
esp	암호화 보안 프로토콜입니다.
inactive	모든 비활성 IPsec SA를 지웁니다.
map*map_name*	맵 이름으로 식별되는 지정된 암호 맵과 연결된 모든 터널을 삭제합니다.
peer*ip_address*	지정된 호스트 이름 또는 IP 주소로 식별되는 피어에 대한 모든 IPsec SA를 삭제합니다.
spi	SPI(Security Parameters Index)(16진수)를 식별합니다. 이는 인바운드 SPI여야 합니다. 아웃바운드 SPI에 대해서는 이 명령을 지원하지 않습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

모든 IPsec SA를 지우려면 인수 없이 이 명령을 사용합니다.

다음 예에서는 Firepower Threat Defense에서 모든 IPsec SA를 제거합니다.

```
> clear crypto ipsec sa
```

>

다음 예에서는 피어 IP 주소가 10.86.1.1인 SA를 삭제합니다.

```
> clear crypto ipsec sa peer 10.86.1.1
```

명령	설명
show ipsec sa	카운터, 엔트리, 맵 이름, 피어 IP 주소, 호스트 이름 등 IPsec SA에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 컨피그레이션을 표시합니다.

clear crypto isakmp

ISAKMP SA 또는 통계를 지우려면 **clear crypto isakmp** 명령을 사용합니다.

clear crypto isakmp [**sa** | **stats**]

sa	IKEv1 및 IKEv2 SA를 지웁니다.
stats	IKEv1 및 IKEv2 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

모든 ISAKMP 운영 데이터를 지우려면 인수 없이 이 명령을 사용합니다.

다음 예는 ISAKMP SA를 모두 제거합니다.

```
> clear crypto isakmp sa
>
```

명령	설명
show isakmp	ISAKMP 운영 데이터에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 컨피그레이션을 표시합니다.

clear crypto protocol statistics

암호화 가속기 MIB의 프로토콜 관련 통계를 지우려면 **clear crypto protocol statistics** 명령을 사용합니다.

clear crypto protocol statistics *protocol*

protocol	통계를 지우려는 프로토콜의 이름을 지정합니다. 다음과 같은 프로토콜을 선택할 수 있습니다. • **all** - 현재 지원되는 모든 프로토콜 • **ikev1** - IKE(Internet Key Exchange) 버전 1 • **ikev2** - IKE(Internet Key Exchange) 버전 2 • **ipsec** - IPsec(IP Security) 2단계 프로토콜 • **other** - 새 프로토콜용으로 예약됨 • **srtp** - SRTP(Secure RTP) 프로토콜 • **ssh** - SSH(Secure Shell) 프로토콜 • **ssl** - SSL(Secure Socket Layer) 프로토콜

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 암호화 가속기 통계를 지웁니다.

```
> clear crypto protocol statistics all
>
```

명령	설명
clear crypto accelerator statistics	crypto accelerator MIB의 전역 및 가속기 관련 통계를 지웁니다.

명령	설명
show crypto accelerator statistics	crypto accelerator MIB의 전역 및 가속기 관련 통계를 표시합니다.
show crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 표시합니다.

clear crypto ssl

SSL 정보를 지우려면 **clear crypto ssl** 명령을 사용합니다.

clear crypto ssl {**cache** [**all**] | **errors** | **mib** | **objects**}

cache	SSL 세션 캐시에서 만료된 세션을 지웁니다.
all	(선택 사항) SSL 세션 캐시의 모든 세션 및 통계를 지웁니다.
errors	SSL 오류를 지웁니다.
mib	SSL MIB 통계를 지웁니다.
objects	SSL 객체 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 SSL 캐시 세션과 통계를 지웁니다.

```
> clear crypto ssl cache all
```

명령	설명
show crypto ssl	SSL 정보를 표시합니다.

clear dhcpd

DHCP 서버 바인딩 및 통계를 지우려면 **clear dhcpd** 명령을 사용합니다.

clear dhcpd {**binding** [**all** | *ip_address*] | **statistics**}

all	(선택 사항) 모든 dhcpd 바인딩을 지웁니다.
바인딩	모든 클라이언트 주소 바인딩을 지웁니다.
ip_address	(선택 사항) 지정된 IP 주소에 대한 바인딩을 지웁니다.
statistics	통계 정보 카운터를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 dhcpd 통계를 지우는 방법을 보여줍니다.

```
> clear dhcpd statistics
```

명령	설명
show dhcpd	DHCP 바인딩, 통계 또는 상태 정보를 표시합니다.

clear dhcprelay statistics

DHCP 릴레이 통계 카운터를 지우려면 **clear dhcprelay statistics** 명령을 사용합니다.

clear dhcprelay statistics

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 DHCP 릴레이 통계를 지우는 방법을 보여줍니다.

```
> clear dhcprelay statistics
```

명령	설명
show dhcprelay statistics	DHCP 릴레이 에이전트 통계 정보를 표시합니다.
show running-config dhcprelay	현재 DHCP 릴레이 에이전트 컨피그레이션을 표시합니다.

clear dns

지정된 FQDN(정규화된 도메인 이름) 호스트와 연결된 모든 IP 주소를 지우려면 **clear dns** 명령을 사용합니다.

clear dns [**host** *fqdn_name*]

host*fqdn_name*	(선택 사항) 지우려는 IP 주소의 정규화된 도메인 이름을 지정합니다. 호스트를 지정하지 않은 경우, 모든 DNS 확인이 지워집니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 지정된 FQDN 호스트와 연결된 IP 주소를 지웁니다.

```
> clear dns host www.example.com
```

명령	설명
show dns-hosts	DNS 캐시를 표시합니다.

clear dns-hosts cache

DNS 캐시를 지우려면 **clear dns-hosts cache** 명령을 사용합니다.

clear dns-hosts cache

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 DNS 캐시를 지웁니다.

```
> clear dns-hosts cache
```

명령	설명
show dns-hosts	DNS 캐시를 표시합니다.

clear eigrp events

EIGRP 이벤트 로그를 지우려면 **clear eigrp events** 명령을 사용합니다.

clear eigrp [*as_number*] **events**

as_number	(선택 사항) 이벤트 로그를 지우려는 EIGRP 프로세스의 자율 시스템 번호를 지정합니다. 디바이스는 단일 EIGRP 라우팅 프로세스만 지원하므로 자율 시스템 번호(프로세스 ID)를 지정할 필요가 없습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show eigrp events 명령을 사용하여 EIGRP 이벤트 로그를 볼 수 있습니다.

다음 예에서는 EIGRP 이벤트 로그를 지웁니다.

```
> clear eigrp events
```

명령	설명
show eigrp events	EIGRP 이벤트 로그를 표시합니다.

clear eigrp neighbors

EIGRP 인접 테이블에서 엔트리를 삭제하려면 **clear eigrp neighbors** 명령을 사용합니다.

clear eigrp [*as_number*] **neighbors** [*ip_addr* | *if_name*] [**soft**]

as_number	(선택 사항) 네이버 항목을 삭제할 EIGRP 프로세스의 자동 시스템 번호를 지정합니다. 디바이스는 단일 EIGRP 라우팅 프로세스만 지원하므로 프로세스 ID인 자동 시스템 번호(AS)를 지정할 필요가 없습니다.
if_name	(선택 사항) 인터페이스의 이름입니다. 인터페이스 이름을 지정하면 이 인터페이스를 통해 학습한 모든 인접 테이블 엔트리를 제거합니다.
ip_addr	(선택 사항) 인접 테이블에서 제거하려는 인접 항목의 IP 주소.
soft	디바이스에서 인접성의 재설정 없이 인접 항목과 다시 동기화하게 합니다.

인접 IP 주소 또는 인터페이스 이름을 지정하지 않을 경우 모든 동적 엔트리가 인접 테이블에서 제거됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

clear eigrp neighbors 명령은 수동으로 정의된 인접 항목을 인접 테이블에서 제거하지 않습니다. 동적으로 검색된 인접 항목만 제거됩니다.

show eigrp neighbors 명령을 사용하여 EIGRP 인접 테이블을 볼 수 있습니다.

다음 예에서는 EIGRP 인접 테이블에서 모든 엔트리를 제거합니다.

```
> clear eigrp neighbors
```

다음 예에서는 “outside”라는 이름의 인터페이스를 통해 학습한 모든 엔트리를 EIGRP 인접 테이블에서 제거합니다.

```
> clear eigrp neighbors outside
```

명령	설명
show eigrp neighbors	EIGRP 인접 테이블을 표시합니다.

clear eigrp topology

EIGRP 토폴로지 테이블에서 엔트리를 삭제하려면 **clear eigrp topology** 명령을 사용합니다.

clear eigrp [*as_number*] **topology** *ip_addr* [*mask*]

as_number	(선택 사항) EIGRP 프로세스의 자동 시스템 번호를 지정합니다. 디바이스는 단일 EIGRP 라우팅 프로세스만 지원하므로 프로세스 ID인 자동 시스템 번호(AS)를 지정할 필요가 없습니다.
ip_addr	토폴로지 테이블에서 지울 IP 주소.
mask	(선택 사항) *ip-addr* 인수에 적용할 네트워크 마스크.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 EIGRP 토폴로지 테이블에서 기존 EIGRP 엔트리를 지웁니다. 토폴로지 테이블 엔트리를 보기 위해 **show eigrp topology** 명령을 사용할 수 있습니다.

다음 예에서는 192.168.1.0 네트워크의 엔트리를 EIGRP 토폴로지 테이블에서 제거합니다.

```
> clear eigrp topology 192.168.1.0 255.255.255.0
```

명령	설명
show eigrp topology	EIGRP 토폴로지 테이블을 표시합니다.

clear f - clear z

clear failover statistics

고가용성 통계 카운터를 지우려면 **clear failover statistics** 명령을 사용합니다.

clear failover statistics

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 **show failover statistics** 명령으로 표시되는 통계 및 **show failover** 명령 출력에서 Stateful Failover Logical Update Statistics 섹션에 있는 카운터를 지웁니다.

다음 예에서는 고가용성 통계 카운터를 지우는 방법을 보여줍니다.

```
> clear failover statistics
```

명령	설명
show failover	고가용성 컨피그레이션 및 운영 통계에 대한 정보를 표시합니다.

clear fragment

IP 프래그먼트 재결합 모듈의 운영 데이터를 지우려면 **clear fragment** 명령을 입력합니다.

clear fragment {**queue** | **statistics** [*interface_name*]}

대기열	IP 프래그먼트 재결합 대기열을 지웁니다.
statistics*interface_name*	IP 프래그먼트 재결합 통계를 지웁니다. 해당 인터페이스에 대한 통계만 지우려면 인터페이스 이름을 선택적으로 지정할 수 있습니다. 그렇지 않으면, 모든 인터페이스에 대한 통계가 지워집니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 현재 대기열에서 재결합을 기다리는 프래그먼트를 지우거나(**queue** 키워드를 입력할 경우) 모든 IP 프래그먼트 재결합 통계를 지웁니다(**statistics** 키워드를 입력할 경우). 통계는 카운터로서 성공적으로 재결합한 프래그먼트 체인 수, 재결합하지 못한 체인 수, 최대 크기를 초과하여 버퍼 오버플로가 발생한 횟수를 알려줍니다.

다음 예에서는 IP 프래그먼트 재결합 모듈의 운영 데이터를 지우는 방법을 보여줍니다.

```
> clear fragment queue
```

명령	설명
show fragment	IP 프래그먼트 재결합 모듈의 작업 데이터를 표시합니다.
show running-config fragment	IP 프래그먼트 리어셈블리 구성을 표시합니다.

clear gc

GC(garbage collection) 프로세스 통계를 제거하려면 **clear gc** 명령을 사용합니다.

clear gc

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 GC 프로세스 통계를 제거하는 방법을 보여줍니다.

```
> clear gc
```

명령	설명
show gc	GC 프로세스 통계를 표시합니다.

clear igmp

모든 IGMP 카운터, 그룹 캐시 및 트래픽을 지우려면 **clear igmp** 명령을 사용합니다.

clear igmp {**counters** [*if_name*] | **group** [**interface** *name*] | **traffic**}

counters [*if_name*]	IGMP 통계 카운터를 지웁니다. 해당 인터페이스에 대한 카운터만 지우려면 인터페이스 이름을 선택적으로 지정할 수 있습니다.
group [**interface***name*]	IGMP 그룹 캐시 항목을 삭제합니다. 해당 인터페이스에 연결된 그룹만 삭제하려면 인터페이스 이름을 선택적으로 지정할 수 있습니다. 이 명령은 통계적으로 구성된 그룹을 지우지 않습니다.
traffic	트래픽 카운터를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 IGMP 통계 카운터를 지웁니다.

```
> clear igmp counters
```

다음 예에서는 검색된 모든 IGMP 그룹을 IGMP 그룹 캐시에서 지우는 방법을 보여줍니다.

```
> clear igmp group
```

다음 예에서는 IGMP 통계 트래픽 카운터를 지웁니다.

```
> clear igmp traffic
```

명령	설명
show igmp	IGMP 정보를 표시합니다.

clear ikev1

IPsec IKEv1 SA 또는 통계를 제거하려면 **clear ikev1** 명령을 사용합니다.

clear ikev1 {**sa** [*ip_address*] | **stats**}

sa*ip_address*	SA를 지웁니다. 모든 IKEv1 SA를 지우려면, IP 주소를 지정하지 않고 이 옵션을 사용합니다. 그렇지 않으면, 지울 SA의 IPv4 또는 IPv6 주소를 지정합니다.
stats	IKEv1 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 Firepower Threat Defense 디바이스에서 IPsec IKEv1 통계를 모두 제거합니다.

```
> clear ikev1 stats
>
```

다음 예에서는 피어 IP 주소가 10.86.1.1인 SA를 삭제합니다.

```
> clear ikev1 sa 10.86.1.1
>
```

명령	설명
show ipsec sa	카운터, 엔트리, 맵 이름, 피어 IP 주소, 호스트 이름 등 IPsec SA에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 구성을 표시합니다.

clear ikev2

IPsec IKEv2 SA 또는 통계를 제거하려면 **clear ikev2** 명령을 사용합니다.

clear ikev2{**sa** [*ip_address*] | **stats**}

sa*ip_address*	SA를 지웁니다. 모든 IKEv2 SA를 지우려면 IP 주소를 지정하지 않고 이 옵션을 사용합니다. 그렇지 않으면, 지울 SA의 IPv4 또는 IPv6 주소를 지정합니다.
stats	IKEv2 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 IPsec IKEv2 통계를 Firepower Threat Defense 디바이스에서 제거합니다.

```
> clear ikev2 stats
>
```

다음 예에서는 피어 IP 주소가 10.86.1.1인 SA를 삭제합니다.

```
> clear ikev2 sa 10.86.1.1
>
```

명령	설명
show ipsec sa	카운터, 엔트리, 맵 이름, 피어 IP 주소, 호스트 이름 등 IPsec SA에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 컨피그레이션을 표시합니다.

clear interface

인터페이스 통계를 지우려면 **clear interface** 명령을 사용합니다.

clear interface [*physical_interface*[**.***subinterface*] | *interface_name*]

interface_name	(선택 사항) 인터페이스 이름을 식별합니다.
physical_interface	(선택 사항) 인터페이스 ID(예: **gigabit**ethernet0/1)를 식별합니다.
subinterface	(선택 사항) 1~4294967293 범위의 정수로 논리적 하위 인터페이스를 지정합니다.

기본적으로 이 명령은 모든 인터페이스 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 인터페이스 통계를 지웁니다.

```
> clear interface
```

명령	설명
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
show running-config interface	인터페이스 구성을 표시합니다.

clear ipsec sa

IPsec SA 카운터, 엔트리, 암호 맵 또는 피어 연결을 제거하려면 **clear ipsec sa** 명령을 사용합니다.

clear ipsec sa [**counters** | **entry** *ip_address* {**esp** | **ah**} *spi* | **inactive** | **map** *map_name* | **peer** *ip_address*]

ah	인증 헤더.
카운터	모든 SA당 IPsec 통계를 지웁니다.
entry*ip_address*	지정된 IP 주소/호스트 이름, 프로토콜, SPI 값과 일치하는 터널을 삭제합니다.
esp	암호화 보안 프로토콜.
inactive	모든 비활성 IPsec SA를 지웁니다.
map*map_name*	맵 이름으로 식별되는 지정된 암호 맵과 연결된 모든 터널을 삭제합니다.
peer*ip_address*	지정된 호스트 이름 또는 IP 주소로 식별되는 피어에 대한 모든 IPsec SA를 삭제합니다.
spi	SPI(Security Parameters Index)(16진수)를 식별합니다. 이는 인바운드 SPI여야 합니다. 아웃바운드 SPI에 대해서는 이 명령을 지원하지 않습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

모든 IPsec SA를 지우려면 인수 없이 이 명령을 사용합니다.

글로벌 구성 모드에서 입력한 다음 예에서는 모든 IPsec SA를 Firepower Threat Defense에서 제거합니다.

```
> clear ipsec sa
```

>

글로벌 구성 모드에서 입력한 다음 예에서는 피어 IP 주소가 10.86.1.1인 SA를 삭제합니다.

```
> clear ipsec sa peer 10.86.1.1
```

명령	설명
show ipsec sa	카운터, 엔트리, 맵 이름, 피어 IP 주소, 호스트 이름 등 IPsec SA에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 구성을 표시합니다.

clear ipv6 dhcprelay

IPv6 DHCP 릴레이 바인딩 엔트리 및 통계를 지우려면 **clear ipv6 dhcprelay** 명령을 사용합니다.

clear ipv6 dhcprelay {**binding** [*ip_address*] | **statistics**}

binding	IPv6 DHCP 릴레이 바인딩 엔트리를 지웁니다.
ip_address	(선택 사항) DHCP 릴레이 바인딩을 위한 IPv6 주소를 지정합니다. IP 주소가 지정될 경우 그 IP 주소와 연결된 릴레이 바인딩 엔트리만 지워집니다.
statistics	IPv6 DHCP 릴레이 에이전트 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 IPv6 DHCP 릴레이 바인딩의 통계 데이터를 지우는 방법을 보여줍니다.

```
> clear ipv6 dhcprelay binding
>
```

다음 예에서는 IPv6 DHCP 릴레이 에이전트의 통계 데이터를 지우는 방법을 보여줍니다.

```
> clear ipv6 dhcprelay statistics
```

명령	설명
show ipv6 dhcprelay binding	릴레이 에이전트에 의해 생성된 릴레이 바인딩 엔트리를 표시합니다.
show ipv6 dhcprelay statistics	IPv6 DHCP 릴레이 에이전트 정보를 표시합니다.

clear ipv6 mld traffic

IPv6 MLD(Multicast Listener Discovery) 트래픽 카운터를 지우고 재설정하려면 **clear ipv6 mld traffic** 명령을 사용합니다.

clear ipv6 mld traffic

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 IPv6 MLD에 대한 트래픽 카운터를 지우는 방법을 보여줍니다.

```
> clear ipv6 mld traffic
>
```

명령	설명
show ipv6 mld traffic	IPv6 MLD 트래픽 카운터를 표시합니다.

clear ipv6 neighbors

IPv6 네이버 검색 캐시를 지우려면 **clear ipv6 neighbors** 명령을 사용합니다.

clear ipv6 neighbors

릴리스	수정 사항
6.1	이 명령을 도입했습니다.

사용 가이드라인

이 명령은 검색된 모든 IPv6 네이버를 캐시에서 삭제합니다. 고정 엔트리는 제거하지 않습니다.

다음 예에서는 IPv6 네이버 검색 캐시에서 고정 엔트리를 제외한 모든 엔트리를 삭제합니다.

```
> clear ipv6 neighbors
>
```

명령	설명
show ipv6 neighbor	IPv6 인접 디바이스 캐시 정보를 표시합니다.

clear ipv6 ospf

OSPFv3 라우팅 파라미터를 지우려면 **clear ipv6 ospf** 명령을 사용합니다.

clear ipv6 [*process_id*] [**counters**] [**events**] [**force-spf**] [**process**] [**redistribution**] [**traffic**]

counters	OSPF 프로세스 카운터를 재설정합니다.
events	OSPF 이벤트 로그를 지웁니다.
force-ospf	OSPF 프로세스에 대한 SPF를 지웁니다.
process	OSPFv3 프로세스를 재설정합니다.
process_id	프로세스 ID 번호를 지웁니다. 유효한 값의 범위는 1 ~ 65535입니다.
redistribution	OSPFv3 경로 재배포를 지웁니다.
traffic	트래픽 관련 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 OSPFv3 경로 재배포를 지우는 방법을 보여줍니다.

```
> clear ipv6 ospf redistribution
>
```

명령	설명
show running-config ipv6 router	OSPFv3 프로세스의 실행 중인 컨피그레이션을 표시합니다.

clear ipv6 prefix-list

라우팅 IPv6 접두사 목록을 지우려면 **clear ipv6 prefix-list** 명령을 사용합니다.

clear ipv6 prefix-list [*name*]

name	명명된 IPv6 접두사 목록을 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 list1 IPv6 접두사 목록을 지우는 방법을 보여줍니다.

```
> clear ipv6 prefix-list list1
>
```

명령	설명
show running-config ipv6 prefix-list	IPv6 접두사 목록의 실행 중인 컨피그레이션을 표시합니다.

clear ipv6 route

IPv6 라우팅 테이블에서 경로를 삭제하려면 clear ipv6 route 명령을 사용합니다.

clear ipv6 route [**management-only**] {**all** | *ipv6-prefix*/*prefix-length*}

management-only	IPv6 관리 라우팅 테이블만 지웁니다.
ipv6-prefix/*prefix-length*	IPv6 접두사를 위해 라우팅된 항목을 지웁니다.
all	모든 IPv6 경로를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

clear ipv6 route 명령은 IPv6에 특정하다는 점을 제외하고는 **clear ip route** 명령과 유사합니다. 대상별 최대 전송 단위(MTU) 캐시도 지워집니다.

다음 예는 2001:0DB8::/35:의 IPv6 경로를 삭제합니다.

```
> clear ipv6 route 2001:0DB8::/35
```

명령	설명
show ipv6 route	IPv6 경로를 표시합니다.

clear ipv6 traffic

IPv6 트래픽 카운터를 재설정하려면 **clear ipv6 traffic** 명령을 사용합니다.

clear ipv6 traffic

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령을 사용하면 **show ipv6 traffic** 명령의 출력에서 카운터를 재설정합니다.

다음 예에서는 IPv6 트래픽 카운터를 재설정합니다.

```
> clear ipv6 traffic
>
```

명령	설명
show ipv6 traffic	IPv6 트래픽 통계를 표시합니다.

clear isakmp

ISAKMP SA 또는 통계를 지우려면 **clear isakmp** 명령을 사용합니다.

clear isakmp [**sa** | **stats**]

sa	(선택 사항) IKEv1 및 IKEv2 SA를 지웁니다.
stats	(선택 사항) IKEv1 및 IKEv2 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

모든 ISAKMP 운영 데이터를 지우려면 인수 없이 이 명령을 사용합니다.

다음 예는 ISAKMP SA를 모두 제거합니다.

```
> clear isakmp sa
>
```

명령	설명
show isakmp	ISAKMP 운영 데이터에 대한 정보를 표시합니다.
show running-config crypto	IPsec, 암호 맵, 동적 암호 맵, ISAKMP 등 전체 암호(crypto) 구성을 표시합니다.

clear kernel cgroup-controller

커널의 cgroup 컨트롤러 통계를 지우려면 **clear kernel cgroup-controller** 명령을 사용합니다.

clear kernel cgroup-controller [**cpu** | **memory**]

cpu	(선택 사항) cpu/cpuacct 컨트롤러 통계를 지웁니다.
memory	(선택 사항) 메모리 컨트롤러 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 cgroup-controller 통계를 지우는 방법을 보여줍니다.

```
> clear kernel cgroup-controller
```

명령	설명
show kernel cgroup-controller	cgroup 컨트롤러 통계를 표시합니다.

clear lacp

EtherChannel LACP 포트 채널 통계를 지우려면 **clear lacp** 명령을 사용합니다.

clear lacp [*channel_group_number*]

channel_group_number	(선택 사항) 1 ~ 48의 수에 따라 채널 그룹 정보를 지웁니다.

번호를 지정하지 않은 경우, 모든 포트 채널에 대한 통계가 지워집니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 포트 채널 통계를 지우는 방법을 보여줍니다.

```
> clear lacp 12
```

명령	설명
show lacp	포트 채널 정보를 표시합니다.

clear lisp eid

Lisp EID 테이블을 지우려면 **clear list eid** 명령을 사용합니다.

clear lisp eid [*ip_address*]

ip_address	EID 테이블에서 지정된 IP 주소를 제거합니다.

릴리스	수정 사항
6.2	이 명령이 도입되었습니다.

사용 가이드라인

디바이스가 EID 및 사이트 ID를 상호 연결하는 EID 테이블을 유지 관리합니다. **clear lisp eid** 명령은 테이블에서 EID 항목을 지웁니다.

명령	설명
clear cluster info flow-mobility counters	흐름 모빌리티 카운터를 지웁니다.
show cluster info flow-mobility counters	흐름 모빌리티 카운터를 표시합니다.
show conn	LISP 흐름 모빌리티에 대한 트래픽 제목을 표시합니다.
show lisp eid	EID 테이블을 표시합니다.

clear local-host

클라이언트별 런타임 상태(예: 연결 제한, 초기 제한)를 다시 초기화하려면 **clear local-host** 명령을 사용합니다.

clear local-host [*hostname* | *ip_address*] [**all**] [**zone** [*zone_name*]]

all	(선택 사항) to-the-box 트래픽을 포함한 모든 연결을 지웁니다. **all** 키워드를 사용하지 않으면 through-the-box 트래픽만 지워집니다.
hostname 또는 *ip_address*	(선택 사항) 로컬 호스트 이름 또는 IPv4 또는 IPv6 주소를 지정합니다.
zone [*zone_name*]	(선택 사항) 영역 연결을 지정합니다. 이 기능은 Firepower Threat Defense에서 지원되지 않습니다. 이는 보안 영역과 동일하지 않습니다.

모든 through-the-box 런타임 상태를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

컨피그레이션에 대한 보안 정책을 변경하면 모든 새 연결에서는 새로운 보안 정책을 사용합니다. 기존 연결에서는 연결 설정 당시에 구성된 정책을 계속 사용합니다. 모든 연결에서 새 정책을 사용하게 하려면 현재의 연결을 끊고 **clear local-host** 명령을 사용하여 새 정책을 통해 다시 연결하게 해야 합니다. 또는 더 세분화된 연결을 지우기는 데 **clear conn** 명령을 사용하거나 동적 NAT를 사용하는 연결에 대해 **clear xlate** 명령을 사용할 수 있습니다.

clear local-host 명령은 호스트에 대해 호스트 라이선스 제한을 해제합니다. **show local-host** 명령을 입력하여 라이선스 제한 대비 호스트 수를 확인할 수 있습니다.

다음 예에서는 호스트 10.1.1.15의 런타임 상태 및 관련 연결을 지웁니다.

```
> clear local-host 10.1.1.15
```

명령	설명
clear conn	어떤 상태의 연결도 종료합니다.
clear xlate	동적 NAT 세션 및 NAT를 사용하는 모든 연결을 지웁니다.
show local-host	로컬 호스트의 네트워크 상태를 표시합니다.

clear logging

로깅 버퍼를 지우려면 **clear logging** 명령을 사용합니다.

clear logging {**buffer** | **queue bufferwrap**}

buffer	내부 로깅 버퍼를 지웁니다.
queue bufferwrap	저장한 FTP 및 플래시 로깅 버퍼 대기열을 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

이 예에서는 로그 버퍼의 내용을 지우는 방법을 보여줍니다.

```
> clear logging buffer
```

다음 예에서는 저장된 로그 버퍼의 내용을 지우는 방법을 보여줍니다.

```
> clear logging queue bufferwrap
```

명령	설명
logging savelog	플래시 파일 이름(선택 사항)을 지정합니다.
show logging	로깅 정보를 표시합니다.

clear mac-address-table

동적 MAC 주소 테이블 엔트리를 지우려면 **clear mac-address-table** 명령을 사용합니다.

clear mac-address-table [*interface_name*]

interface_name	(선택 사항) 선택된 인터페이스에 대한 MAC 주소 테이블 엔트리를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 동적 MAC 주소 테이블 엔트리를 지웁니다.

```
> clear mac-address-table
```

명령	설명
show mac-address-table	MAC 주소 테이블 엔트리를 표시합니다.

clear memory

메모리 툴의 대기열 및 통계를 지우려면 **clear memory** 명령을 사용합니다.

clear memory {**delayed-free-poisoner** | **profile** [**peak**] | **tracking**}

delayed-free-poisoner	지연된 여유 메모리 포이즈너 툴 대기열에 있던 모든 메모리를 유효성 검사 없이 시스템으로 반환하고 관련 통계 카운터를 지웁니다. **memory delayed-free-poisoner enable** 명령을 사용하여 이 기능을 활성화할 수 있습니다.
profile [**peak**]	메모리 프로파일링 기능에서 유지되는 메모리 버퍼를 지웁니다. 최대 메모리 버퍼의 내용을 지우려면 선택 사항인 **peak** 키워드를 포함시킵니다. 프로필 버퍼를 지우기 전에 메모리 프로파일링을 중지하려면 **no memory profile enable** 명령을 사용합니다.
tracking	**memory tracking enable** 명령을 사용하여 수집한 메모리 추적 정보를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 지연된 여유 메모리 포이즈너 툴 대기열 및 통계를 지웁니다.

```
> clear memory delayed-free-poisoner
```

명령	설명
memory	다양한 메모리 툴을 활성화합니다.
show memory delayed-free-poisoner	지연된 여유 메모리 포이즈너 툴 대기열의 사용량 요약을 표시합니다.
show memory profile	메모리 프로파일링 결과를 표시합니다.

명령	설명
show memory tracking	메모리 추적 결과를 표시합니다.

clear mfib counters

MFIB(Multicast Forwarding Information Base) 라우터 패킷 카운터를 지우려면 **clear mfib counters** 명령을 사용합니다.

clear mfib {**cluster-stats** | **counters** [*source_or_group* [*source*]]}

cluster-stats	MFIB 클러스터 동기화 통계를 지웁니다.
count	MFIB 경로 및 패킷 수 데이터를 지웁니다. **count**를 인수 없이 사용하면 모든 경로의 경로 카운터가 지워집니다.
source_or_group [*group*]	(선택 사항) 소스 또는 그룹 IPv4, IPv6 또는 이름입니다. 두 가지를 모두 지정하는 경우, 소스를 처음에 지정합니다. 소스 주소는 유니캐스트 주소입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 MFIB 라우터 패킷 카운터를 지웁니다.

```
> clear mfib counters
```

명령	설명
show mfib	MFIB 경로 및 패킷 수 데이터를 표시합니다.

clear nat counters

NAT 정책 카운터를 지우려면 clear nat counters 명령을 사용합니다.

clear nat counters [**interface** *name*] [*ip_addr mask* | {**object** | **object-group**} *name*] [**translated** [**interface** *name*] [*ip_addr mask* | {**object** | **object-group**} *name*]]]

interface*name*	(선택 사항) 소스 또는 대상(변환된) 인터페이스를 지정합니다.
ip_addr mask	(선택 사항) IP 주소 및 서브넷 마스크를 지정합니다.
object*name*	(선택 사항) 네트워크 개체 또는 서비스 개체를 지정합니다.
object-group*name*	(선택 사항) 네트워크 개체 그룹을 지정합니다.
translated	(선택 사항) 변환된 파라미터를 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

이 예에서는 NAT 정책 카운터를 지우는 방법을 보여줍니다.

```
> clear nat counters
```

명령	설명
show nat	프로토콜 스택 카운터를 표시합니다.

clear object-group

네트워크 객체 그룹에 속한 객체의 계수기를 지우려면 **show object-group** 명령을 사용합니다.

clear object-group [*object-group name*]

object-group name	해당 카운터를 지워야 하는 객체 그룹의 이름입니다. 그룹을 지정하지 않은 경우, 모든 객체 그룹에 대한 카운터가 지워집니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 "Anet"라는 네트워크 객체 그룹의 네트워크 객체 히트 수를 지우는 방법을 보여줍니다.

```
> clear object-group Anet
```

명령	설명
show object-group	객체 그룹 정보를 표시하고, 지정된 객체 그룹이 네트워크 객체 그룹 유형일 경우 히트 수를 표시합니다.

clear ospf

OSPF 프로세스 정보를 지우려면 **clear ospf** 명령을 사용합니다.

clear ospf {**counters** [**neighbor** *interface*] | **events** | **force-spf** | **process /noconfirm** | **redistribution** | **traffic**}

카운터	OSPF 카운터를 지웁니다.
neighbor*interface*	(선택 사항) 해당 네이버에 대한 통계만 지웁니다.
이벤트	OSPF 이벤트 로그를 지웁니다.
force-spf	증분 SPF 통계를 지웁니다.
process /noconfirm	OSPF 라우팅 프로세스를 다시 시작합니다.
redistribution	OSPF 경로 재분배 통계를 지웁니다.
트래픽	OSPF 트래픽 관련 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 구성의 어느 부분도 제거하지 않고 통계만 지웁니다.

다음 예에서는 OSPF 네이버 카운터를 모두 지우는 방법을 보여줍니다.

```
> clear ospf counters
```

명령	설명
show ospf	실행 중인 구성의 모든 OSPF 정보를 표시합니다.

clear pclu

PC 논리적 업데이트 통계를 지우려면 **clear pclu** 명령을 사용합니다.

clear pclu

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 PC 정보를 지웁니다.

```
> clear pclu
```

명령	설명
show pclu	PCLU 정보를 표시합니다.

clear pim

PIM 트래픽 카운터와 매핑을 지우려면 **clear pim** 명령을 사용합니다.

clear pim {**counters** | **group-map** [*rp-address*] | **reset** | **topology** [*group*]}

counters	PIM 트래픽 카운터를 지웁니다.
group-map [*rp-address*]	RP(rendezvous point) 매핑 캐시에서 group-to-RP 매핑 엔트리를 삭제합니다. 해당 RP 전용 엔트리만 지우기 위해 RP의 이름을 선택적으로 지정할 수 있습니다. 이름은 다음을 사용할 수 있습니다. • DNS(Domain Name System) 호스트 테이블에 정의된 RP의 이름. • RP의 IP 주소. 이는 네 부분의 점으로 구분된 10진수 형식 표기법의 멀티캐스트 IP 주소입니다.
reset	강제적으로 재설정을 통한 MRIB 동기화를 수행합니다. 토폴로지 테이블의 모든 정보가 지워지며 MRIB 연결이 재설정됩니다. PIM 토폴로지 테이블과 MRIB 데이터베이스 간의 상태를 동기화하는 이 옵션을 사용할 수 있습니다.
topology [*group*]	PIM 토폴로지 테이블에서 기존 PIM 경로를 지웁니다. IGMP 로컬 멤버십과 같이 MRIB 테이블에서 얻은 정보는 보존됩니다. 토폴로지 테이블에서 삭제할 멀티캐스트 그룹 주소 또는 이름을 선택적으로 지정할 수 있습니다. 이름은 다음 중 하나일 수 있습니다. • DNS 호스트 테이블에 정의된 멀티캐스트 그룹의 이름. • 멀티캐스트 그룹의 IPv4 또는 IPv6 주소.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 PIM 트래픽 카운터를 지웁니다.

```
> clear pim counters
```

다음 예에서는 23.23.23.2 RP 주소에서 group-RP 매핑 엔트리를 삭제합니다.

```
> show pim group-map

Group Range          Proto Client Groups RP address      Info
224.0.1.39/32*       DM    static 0      0.0.0.0
224.0.1.40/32*       DM    static 0      0.0.0.0
224.0.0.0/24*        L-Localstatic 1      0.0.0.0
232.0.0.0/8*         SSM   config 0      0.0.0.0
224.0.0.0/4*         SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4          SM    BSR    0      23.23.23.2      RPF: Gi0/3,23.23.23.2
> clear pim group-map 23.23.23.2
> show pim group-map
Group Range          Proto Client Groups RP address      Info
224.0.1.39/32*       DM    static 0      0.0.0.0
224.0.1.40/32*       DM    static 0      0.0.0.0
224.0.0.0/24*        L-Localstatic 1      0.0.0.0
232.0.0.0/8*         SSM   config 0      0.0.0.0
224.0.0.0/4*         SM    config 0      9.9.9.9         RPF: ,0.0.0.0
224.0.0.0/4          SM    static 0      0.0.0.0         RPF: ,0.0.0.0
```

명령	설명
show pim	PIM 트래픽 정보를 표시합니다.

clear prefix-list

접두사 목록 항목의 적중 횟수를 재설정하려면 **clear prefix-list** 명령을 사용합니다.

clear prefix-list [*prefix_list_name*]

prefix_list_name	(선택 사항) 적중 횟수가 지워지는 접두사 목록의 이름입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 first_list라는 목록에서 접두사 목록 정보를 지우는 방법을 보여줍니다.

```
> clear prefix-list first_list
>
```

명령	설명
show prefix-list	접두사 목록 또는 접두사 목록 항목에 대한 정보를 표시합니다.

clear process

Firepower Threat Defense 디바이스에서 실행 중인 지정된 프로세스의 통계를 지우려면 clear process 명령을 사용합니다.

clear process {**cpu-hog** | **internals**}

cpu-hog	CPU 과다 사용 통계를 지웁니다.
internals	프로세스 내부 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 CPU 과다 사용 통계를 지우는 방법을 보여줍니다.

```
> clear process cpu-hog
```

명령	설명
cpu hog granular-detection	실시간 CPU 과다 사용 탐지 정보를 트리거합니다.
show processes	Firepower Threat Defense에서 실행 중인 프로세스의 목록을 표시합니다.

clear resource usage

리소스 사용량 통계를 지우려면 **clear resource usage** 명령을 사용합니다.

clear resource usage [**detail** | **resource** {[**rate**] *resource_name* | **all**}]

detail	모든 리소스 사용량 세부 사항을 지웁니다.
resource [**rate**] *resource_name*	특정 리소스의 사용량을 지웁니다. 모든 리소스의 경우 **all**(기본값)을 지정합니다. 리소스의 사용률을 지우려면 **rate**를 지정합니다. 비율로 측정되는 리소스에는 **conns**, **inspects** 및 **syslogs** 등이 있습니다. 이러한 리소스 유형에는 **rate** 키워드를 지정해야 합니다. conns 리소스는 동시 연결 수로도 측정되지만 초당 연결 수를 보려면 **rate** 키워드만 사용해야 합니다. 리소스 유형은 다음과 같습니다. • **Conns** - 호스트 하나와 여러 다른 호스트 간의 연결을 포함하여 두 호스트 간의 TCP 또는 UDP 연결입니다. • **Hosts** - 디바이스를 통해 연결할 수 있는 호스트입니다. • **IPSec** - 디바이스를 통해 연결되는 IPSec 관리 터널입니다. • **Mac-addresses** - MAC 주소 테이블에서 허용되는 MAC 주소의 수입니다. • **Routes** - 라우팅 테이블 엔트리. • **SSH** - SSH 세션. • **Storage** - 디렉토리의 스토리지 제한 크기(MB 단위). • **Telnet** - 텔넷 세션. • **VPN** - VPN 리소스. • **Xlates** - NAT 변환.

기본 리소스 이름은 **all**이며, 모든 리소스 유형을 지웁니다.

릴리스	수정 사항
6.1	이 명령을 도입했습니다.

다음 예에서는 시스템 전반 사용량 통계를 지웁니다.

```
> clear resource usage resource all
```

명령	설명
show resource types	리소스 유형의 목록을 표시합니다.
show resource usage	디바이스의 리소스 사용량을 표시합니다.

clear route

구성에서 동적으로 학습된 경로를 제거하려면 **clear route** 명령을 사용합니다.

clear route {**all** | *ip_address mask_or_prefix*}

all	모든 학습된 경로를 제거할지 지정합니다.
ip_address mask_or_prefix	제거할 경로의 IPv4 또는 IPv6 대상 주소 및 마스크 또는 접두사입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 동적으로 학습한 경로를 제거하는 방법을 보여줍니다.

```
> clear route all
```

명령	설명
show route	경로 정보를 표시합니다.

clear service-policy

사용 설정된 정책에 대한 운영 데이터 또는 통계를 지우려면 **clear service-policy** 명령을 사용합니다.

clear service-policy [**global** | **interface** *intf* | **shape** | **user-statistics**]

전역	(선택 사항) 전역 서비스 모델의 통계를 지웁니다.
interface*intf*	(선택 사항) 특정 인터페이스의 서비스 정책 통계를 지웁니다.
shape	(선택 사항) shape 정책의 통계를 지웁니다.
user-statistics	(선택 사항) 사용자 통계에 대한 전역 카운터를 지우지만 사용자별 통계는 지우지 않습니다. 이 기능은 Firepower Threat Defense에서 지원되지 않습니다.

기본값으로 이 명령은 사용 설정된 모든 서비스 정책의 모든 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

일부 검사 엔진에서는 통계를 선택하여 지울 수 있습니다. **clear service-policy inspect** 명령을 참조하십시오.

다음 예에서는 외부 인터페이스에 대한 서비스 정책 통계를 지우는 방법을 보여줍니다.

```
> clear service-policy interface outside
```

명령	설명
clear service-policy inspect	GTP, M3UA 및 RADIUS 검사 엔진에 대한 서비스 정책 통계를 지웁니다.
show service-policy	서비스 정책을 표시합니다.
show running-config service-policy	실행 중인 구성에 구성된 서비스 정책을 표시합니다.

clear service-policy inspect gtp

GTP 검사 통계를 지우려면 **clear service-policy inspect gtp** 명령을 사용합니다.

clear service-policy inspect gtp {**pdp-context** {**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*} | **requests** [**map** *name* | **version** *version_num*] | **statistics** [*IP_address*]}

pdp-context {**all** | **apn***ap_name* | **imsi***IMSI_value* | **ms-addr***IP_address* | **tid***tunnel_ID* | **version***version_num*}	PDP(Packet Data Protocol) 또는 전달자(bearer) 상황 정보를 지웁니다. 다음 키워드를 사용하여 지울 상황을 지정할 수 있습니다. • **all** — 모든 상황을 지웁니다. • **apn***ap_name* — 지정된 액세스 포인트 이름에 대한 상황을 지웁니다. • **imsi***IMSI_value* — 지정된 IMSI 16진수에 대한 상황을 지웁니다. • **ms-addr***IP_address* — 지정된 MS(mobile subscriber) IP 주소에 대한 상황을 지웁니다. • **tid***tunnel_ID* — 지정된 GTP 터널 ID(16진수)에 대한 상황을 지웁니다. • **version***version_num* — 지정된 GTP 버전(0-255)에 대한 상황을 지웁니다.
requests [**map***name* | **version***version_num*]	GTP 요청을 지웁니다. 선택적으로 다음 파라미터를 사용하여 지울 요청을 제한할 수 있습니다. • **map***name* — 지정된 GTP 검사 정책 맵과 연결된 요청을 지웁니다. • **version***version_num* — 지정된 GTP 버전(0-255)에 대한 요청을 지웁니다.
statistics [*IP_address*]	**inspect gtp** 명령에 대한 GTP 통계를 지웁니다. 엔드포인트의 주소를 지정하여 특정 엔드포인트에 대한 통계를 지울 수 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 GTP 통계를 지웁니다.

```
> clear service-policy inspect gtp statistics
```

명령	설명
show service-policy inspect gtp	GTP 통계를 표시합니다.

clear service-policy inspect m3ua

M3UA 검사 통계를 지우려면 **clear service-policy inspect m3ua** 명령을 사용합니다.

clear service-policy inspect m3ua {**drops** | **endpoint** [*ip_address*]}

drops	M3UA 삭제 통계를 지웁니다.
endpoint [*ip_address*]	M3UA 엔드포인트 통계를 지웁니다. 엔드포인트에 대한 통계만 지우려면 엔드포인트의 IP 주소를 선택적으로 포함할 수 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

M3UA 검사의 통계를 지우려면 이 명령을 사용합니다. 통계를 표시하려면 이 명령의 **show** 버전을 사용합니다.

다음 예에서는 M3UA 엔드포인트 통계를 지웁니다.

```
> clear service-policy inspect m3ua endpoint
```

명령	설명
show service-policy inspect m3ua	M3UA 통계를 표시합니다.

clear service-policy inspect radius-accounting

RADIUS 어카운팅 사용자를 지우려면 **clear service-policy inspect radius-accounting** 명령을 사용합니다.

clear service-policy inspect radius-accounting users {**all** | *ip_address* | *policy_map*}

all	모든 사용자를 지웁니다.
ip_address	이 IP 주소의 사용자를 지웁니다.
policy_map	이 정책 맵과 연관된 사용자를 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 RADIUS 어카운팅 사용자를 지웁니다.

```
> clear service-policy inspect radius-accounting users all
```

clear shun

현재 사용 설정된 모든 차단을 사용 해제하고 차단 통계를 지우려면 **clear shun** 명령을 사용합니다.

clear shun [**statistics**]

statistics	(선택 사항) 인터페이스 카운터만 지웁니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 현재 사용 설정된 모든 차단을 사용 해제하고 차단 통계를 지우는 방법을 보여줍니다.

```
> clear shun
```

명령	설명
shun	신규 연결을 막고 기존 연결에서의 패킷 전송을 허용하지 않음으로써 공격 호스트에 대한 동적 응답을 활성화합니다.
show shun	shun 정보를 표시합니다.

clear snmp-server statistics

SNMP 서버 통계(SNMP 패킷 입력 및 출력 카운터)를 지우려면 **clear snmp-server statistics** 명령을 사용합니다.

clear snmp-server statistics

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 SNMP 서버 통계를 지우는 방법을 보여줍니다.

```
> clear snmp-server statistics
```

명령	설명
show snmp-server statistics	SNMP 서버 컨피그레이션 정보를 표시합니다.

clear snort statistics

Snort 통계(패킷 카운터, 플로우 카운터 및 이벤트 카운터)를 지우려면 **clear snort statistics** 명령을 사용합니다.

clear snort statistics

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 Snort 통계를 지우는 방법을 보여줍니다.

```
> clear snort statistics
```

명령	설명
show snort statistics	Snort 서비스 컨피그레이션에 대한 정보를 표시합니다.

clear ssl

디버깅 목적으로 SSL 정보를 지우려면 **clear ssl** 명령을 사용합니다.

clear ssl {**cache** [**all**] | **errors** | **mib** | **objects**}

cache [**all**]	SSL 세션 캐시에서 만료된 세션을 지웁니다. SSL 세션 캐시에서 모든 세션 및 통계를 지우려면 선택 사항인 **all** 키워드를 추가합니다.
errors	ssl 오류를 지웁니다.
mib	SSL MIB 통계를 지웁니다.
objects	SSL 객체 통계를 지웁니다.

릴리스	수정 사항
6.1	이 명령을 도입했습니다.

사용 가이드라인

DTLS 캐시는 지우지 않습니다. AnyConnect 기능에 영향을 주기 때문입니다.

다음 예에서는 ssl 캐시를 지우고 SSL 세션 캐시의 모든 세션 및 통계를 지우는 것을 보여줍니다.

```
> clear ssl cache
SSL session cache cleared: 2
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
> clear ssl cache all
Clearing all sessions and statistics
SSL session cache cleared: 5
No SSL VPNLB session cache
No SSLDEV session cache
DLTS caches are not cleared
```

clear sunrpc-server active

Sun RPC 애플리케이션 검사에서 연 핀홀을 지우려면 **clear sunrpc-server active** 명령을 사용합니다.

clear sunrpc-server active

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

clear sunrpc-server active 명령을 사용하면 Sun RPC 애플리케이션 검사에서 열었고 NFS, NIS와 같은 서비스 트래픽의 디바이스 통과를 가능하게 하는 핀홀을 지울 수 있습니다.

다음 예에서는 SunRPC 서비스 테이블을 지우는 방법을 보여줍니다.

```
> clear sunrpc-server active
```

명령	설명
show sunrpc-server active	활성 Sun RPC 서비스에 대한 정보를 표시합니다.

clear traffic

전송 및 수신 활동에 대한 카운터를 재설정하려면 **clear traffic** 명령을 사용합니다.

clear traffic

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

clear traffic 명령은 **show traffic** 명령과 함께 표시된 전송 및 수신 활동의 카운터를 재설정합니다. 이 카운터는 마지막으로 clear traffic 명령을 입력한 이후 또는 디바이스가 온라인 상태가 된 이후 각 인터페이스를 지난 패킷 및 바이트 수를 나타냅니다. 그리고 초 수는 디바이스가 마지막 재부팅 후 온라인 상태를 유지한 기간을 나타냅니다.

다음 예에서는 **clear traffic** 명령을 보여줍니다.

```
> clear traffic
```

명령	설명
show traffic	전송 및 수신 활동에 대한 카운터를 표시합니다.

clear wccp

WCCP(Web Cache Communication Protocol) 정보를 재설정하려면 **clear wccp** 명령을 사용합니다.

clear wccp [**web-cache** | *service_number*]

web-cache	웹 캐시 서비스를 지정합니다.
service-number	서비스 정의가 캐시에 의해 지정됨을 의미하는 동적 서비스 식별자입니다. 동적 서비스 번호의 범위는 0~254입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 웹 캐시 서비스에 대해 WCCP 정보를 재설정하는 방법을 보여줍니다.

```
> clear wccp web-cache
```

명령	설명
show wccp	WCCP 컨피그레이션을 표시합니다.

clear xlate

현재 동적 NAT 변환 및 연결 정보를 지우려면 **clear xlate** 명령을 사용합니다.

clear xlate [**global** *ip1*[**-***ip2*] [**netmask** *mask*]] [**local** *ip1*[**-***ip2*] [**netmask** *mask*]] [**gport** *port1*[**-***port2*]] [**lport***port1*[**-***port2*]] [**interface** *if_name*] [**type** *type*]

global*ip1*[**-***ip2*]	(선택 사항) 전역 IP 주소 또는 주소 범위를 기준으로 활성 변환을 지웁니다.
gport*port1*[**-***port2*]	(선택 사항) 전역 포트 또는 포트 범위를 기준으로 활성 변환을 지웁니다.
interface*if_name*	(선택 사항) 인터페이스별 활성 변환을 표시합니다.
local*ip1*[**-***ip2*]	(선택 사항) 로컬 IP 주소 또는 주소 범위를 기준으로 활성 변환을 지웁니다.
lport*port1*[**-***port2*]	(선택 사항) 로컬 포트 또는 포트 범위를 기준으로 활성 변환을 지웁니다.
netmask*mask*	(선택 사항) 전역 또는 로컬 IP 주소를 정규화할 네트워크 마스크 또는 IPv6 접두사를 지정합니다.
type*type*	(선택 사항) 유형별로 활성 변환을 지웁니다. 다음 유형 중 하나를 입력할 수 있습니다. • **dynamic** — 동적 변환을 지정합니다. • **portmap** — PAT 전역 변환을 지정합니다. • **static** — 고정 변환을 지정합니다. • **twice-nat** — 수동 NAT 변환을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

clear xlate 명령은 변환 슬롯의 내용을 지웁니다("xlate"가 변환 슬롯을 의미함). 변환 슬롯은 키 교환이 끝나더라도 유지될 수 있습니다. 항상 NAT 규칙을 추가, 변경 또는 제거한 이후에 **clear xlate** 명령을 사용합니다.

xlate는 NAT 또는 PAT 세션을 설명합니다. 이 세션은 **show xlate detail** 명령을 이용하여 확인할 수 있습니다.

xlate는 고정(static) 유형과 동적(dynamic) 유형이 있습니다. 고정 xlate는 영구적 xlate로서 고정 NAT 규칙을 사용하여 생성합니다. **clear xlate** 명령은 고정 항목은 지우지 않습니다. 고정 xlate는 컨피그레이션에서 고정 NAT 규칙을 제거하는 방법으로만 제거될 수 있습니다. 컨피그레이션에서 고정 규칙을 제거할 경우 이 고정 규칙을 사용하는 기존 연결은 계속 트래픽을 전달할 수 있습니다. 이러한 연결을 비활성화하려면 **clear local-host** 또는 **clear conn** 명령을 사용합니다.

동적 xlate는 트래픽 처리 요청 시 생성되는 xlate입니다. **clear xlate** 명령은 동적 xlate와 관련 연결을 제거합니다. **clear local-host** 또는 **clear conn** 명령을 사용하여 xlate와 관련 연결을 지울 수도 있습니다. 컨피그레이션에서 동적 NAT 규칙을 제거하는 경우, 동적 xlate와 관련 연결은 계속 활성 상태일 수 있습니다. 이러한 연결을 제거하려면 **clear xlate** 명령을 사용합니다.

다음 예에서는 현재 변환 및 연결 슬롯 정보를 지우는 방법을 보여줍니다.

```
> clear xlate global
```

명령	설명
clear local-host	로컬 호스트 네트워크 정보를 지웁니다.
show conn	모든 활성 연결을 표시합니다.
show local-host	로컬 호스트 네트워크 정보를 표시합니다.
show xlate	현재 변환 정보를 표시합니다.

clf - cz

- crypto ca trustpool import, 223 페이지
- crypto ca trustpool remove, 225 페이지

cluster enable

유닛에서 클러스터링을 활성화하려면 **cluster enable** 명령을 사용합니다.

cluster enable

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

활성화된 1번째 유닛에서 마스터 유닛 선택이 일어납니다. 1번째 유닛이 지금까지는 클러스터의 유일한 멤버이므로 마스터 유닛이 됩니다. 이 기간에는 어떤 구성 변경도 하지 마십시오.

다음 예에서는 유닛에서 클러스터링을 활성화합니다.

```
> cluster enable
```

명령	설명
cluster master unit	새 유닛을 클러스터의 마스터 유닛으로 설정합니다.
cluster remove unit	클러스터에서 유닛을 제거합니다.
show cluster info	클러스터 정보를 표시합니다.
cluster exec	모든 클러스터 멤버에 명령을 보냅니다.

cluster exec

클러스터의 모든 유닛에서 또는 특정 멤버에서 명령을 실행하려면 **cluster exec** 명령을 사용합니다.

cluster exec [**unit** *unit_name*] *command*

unit*unit_name*	(선택 사항) 특정 유닛에서 명령을 수행합니다. 멤버 이름을 보려면 **cluster exec unit?**를 입력하거나 (현재 유닛을 제외한 모든 이름을 보려는 경우), **show cluster info** 명령을 입력합니다.
command	실행하려는 명령을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

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.

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_device1.pcap, capture1_device2.pcap 같은 형식이 됩니다. 이 예에서는 device1과 device2가 클러스터 유닛 이름입니다.

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)
```

명령	설명
cluster enable	유닛에서 클러스터링을 사용 설정합니다.
cluster master unit	새 유닛을 클러스터의 마스터 유닛으로 설정합니다.
cluster remove unit	클러스터에서 유닛을 제거합니다.
show cluster info	클러스터 정보를 표시합니다.
cluster exec	모든 클러스터 멤버에 명령을 보냅니다.

cluster master unit

새 유닛을 디바이스 클러스터의 마스터 유닛으로 설정하려면 **cluster master unit** 명령을 사용합니다.

cluster master unit *unit_name*

주의 마스터 유닛을 변경하는 가장 좋은 방법은 마스터 유닛의 클러스터링을 사용 해제한 후(**no cluster enable** 명령 참조) 새 마스터가 선택될 때까지 기다렸다가 클러스터링을 다시 사용 설정하는 것입니다. 마스터가 될 정확한 유닛을 지정해야 할 경우 **cluster master unit** 명령을 사용합니다. 그러나 중앙 집중식 기능의 경우 이 명령을 통해 마스터 유닛을 강제로 변경하면 모든 연결이 취소되며 새 마스터 유닛에서 연결을 다시 설정해야 합니다.

unit_name	새 마스터 유닛이 될 로컬 유닛 이름을 지정합니다. 멤버 이름을 보려면 **cluster master unit?**을 입력하거나 (현재 유닛을 제외한 모든 이름을 보려는 경우), **show cluster info** 명령을 입력합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

기본 클러스터 IP 주소에 다시 연결해야 합니다.

다음 예에서는 **device2**를 마스터 유닛으로 설정합니다.

```
> cluster master unit device2
```

명령	설명
cluster enable	유닛에서 클러스터링을 사용 설정합니다.

명령	설명
cluster exec	모든 클러스터 멤버에 명령을 보냅니다.
cluster remove unit	클러스터에서 유닛을 제거합니다.
show cluster info	클러스터 정보를 표시합니다.

cluster remove unit

클러스터에서 유닛을 제거하려면 **cluster remove unit** 명령을 사용합니다.

cluster remove unit *unit_name*

unit_name	클러스터에서 제거할 로컬 유닛 이름을 지정합니다. 멤버 이름을 보려면 **cluster remove unit ?**을 입력하거나 **show cluster info** 명령을 입력합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

부트스트랩 컨피그레이션과 마스터 유닛에서 동기화한 마지막 컨피그레이션도 그대로 유지되므로 나중에 컨피그레이션을 잃지 않고 다시 유닛을 추가할 수 있습니다. 슬레이브 유닛에 이 명령을 입력하여 마스터 유닛을 제거할 경우 새 마스터 유닛이 선택됩니다.

다음 예에서는 유닛 이름을 확인한 다음 클러스터에서 device2를 제거합니다.

```
> cluster remove unit ?
Current active units in the cluster:
device2
> cluster remove unit device2
WARNING: Clustering will be disabled on unit device2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

명령	설명
cluster enable	유닛에서 클러스터링을 활성화합니다.
cluster exec	모든 클러스터 멤버에 명령을 보냅니다.
cluster master unit	새 유닛을 클러스터의 마스터 유닛으로 설정합니다.

명령	설명
show cluster info	클러스터 정보를 표시합니다.

configure disable-https-access

모든 IP 주소에서 HTTPS 연결 시도를 거부하도록 디바이스를 구성하면서 HTTPS 액세스 목록을 지우려면 **configure disable-https-access** 명령을 사용합니다.

configure disable-https-access

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스에 대한 HTTPS 액세스를 비활성화하려면 이 명령을 사용합니다. HTTPS 액세스는 로컬 관리자, Firepower Device Manager를 사용할 때 필요합니다.

다음 예에서는 임의의 주소에서 HTTPS 연결을 거부하도록 디바이스를 구성합니다.

```
> configure disable-https-access
```

명령	설명
configure https-access-list	디바이스가 지정된 IP 주소에서 HTTPS 연결을 수락하도록 구성합니다.
show https-access-list	현재 HTTPS 액세스 목록을 표시합니다.

configure disable-ssh-access

모든 IP 주소에서 SSH 연결 시도를 거부하도록 디바이스를 구성하면서 SSH 액세스 목록을 지우려면 **configure disable-ssh-access** 명령을 사용합니다.

configure disable-ssh-access

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스에 대한 SSH 액세스를 비활성화하려면 이 명령을 사용합니다. 이 명령은 콘솔 포트를 통해 액세스하는 경우를 제외하고 CLI 액세스를 방지합니다.

다음 예에서는 임의의 주소에서 SSH 연결을 거부하도록 디바이스를 구성합니다.

```
> configure disable-ssh-access
```

명령	설명
configure ssh-access-list	디바이스가 지정된 IP 주소에서 SSH 연결을 수락하도록 구성합니다.
show ssh-access-list	현재 SSH 액세스 목록을 표시합니다.

configure firewall

방화벽 모드를 투명 모드 또는 라우팅 모드로 설정하려면 **configure firewall** 명령을 사용합니다.

configure firewall {**routed** | **transparent**}

routed	방화벽 모드를 라우팅 방화벽 모드로 설정합니다.
transparent	방화벽 모드를 투명 방화벽으로 설정합니다.

기본적으로 디바이스는 라우팅 모드에 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

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.

모드를 변경할 경우, 다수의 명령이 양쪽 모드에서 모두 지원되지는 않으므로 디바이스에서는 컨피그레이션을 지웁니다. 컨피그레이션이 이미 채워져 있는 경우 모드를 변경하기 전에 해당 컨피그레이션을 백업하십시오. 새 컨피그레이션을 생성할 때 이러한 백업을 참조할 수 있습니다.

참고 로컬 디바이스 관리자인 Firepower Device Manager를 사용 중인 경우 투명 방화벽 모드로 전환할 수 없습니다. 로컬 관리자를 사용 중이며 투명 모드로 변환하려는 경우, 먼저 **configure manager delete**를 사용하여 관리자를 제거하고 투명 모드로 변환한 다음 Firepower Management Center를 가리키도록 **configure manager add**를 사용해야 합니다.

다음 예에서는 방화벽 모드를 투명으로 변경합니다.

```
> configure firewall transparent
```

명령	설명
show running-config	실행 중인 컨피그레이션을 표시합니다.
show firewall	방화벽 모드를 표시합니다.

configure high-availability

디바이스 간의 고가용성 컨피그레이션(페일오버)을 비활성화, 일시 중단 또는 다시 시작하려면 **configure high-availability** 명령을 사용합니다.

configure high-availability {**disable** [**clear-interfaces**] | **resume** | **suspend** [**clear-interfaces**]}

clear-interfaces	(선택 사항) 고가용성 비활성화 또는 일시 중단 시 바로 인터페이스를 지웁니다.
disable	이 디바이스와 해당 피어 간의 고가용성 관계를 중단합니다.
resume	이 디바이스와 해당 피어 간 일시 중단된 고가용성 컨피그레이션을 다시 시작합니다. 비활성화된 컨피그레이션은 다시 시작할 수 없습니다.
suspend	이 디바이스와 해당 피어 간 고가용성 컨피그레이션을 일시적으로 중단합니다. 나중에 컨피그레이션을 다시 시작할 수 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

Firepower Management Center를 사용하여 2개의 디바이스를 고가용성 쌍으로 구성할 수 있습니다. 이는 쌍으로 된 나머지 디바이스에 장애가 발생할 경우 디바이스가 대체할 수 있는 페일오버 컨피그레이션으로 알려져 있습니다.

어떤 이유로든 Firepower Management Center의 컨피그레이션을 업데이트할 수 없는 경우 고가용성 쌍을 관리하기 위해 configure high-availability 명령을 사용할 수 있습니다.

예를 들어, 고가용성 쌍에 연결할 수 없는 경우, **configure high-availability disable**을 사용하여 모든 고가용성 쌍에서 페일오버 컨피그레이션을 제거할 수 있습니다. 또한 일시적으로 페일오버 컨피그레이션을 중단한 다음 나중에 다시 시작할 수 있습니다.

고가용성 쌍의 특정 유닛에서 고가용성을 일시 중단하면 다음 경우에 특히 유용합니다.

- 두 유닛이 모두 액티브-액티브 상태에 있고 이 중에서 하나를 일시 중단하려는 경우.

- 액티브 또는 스탠바이 유닛의 문제를 해결하고 이 동안에는 해당 유닛을 페일오버하지 않으려는 경우.

다음 예는 고가용성 컨피그레이션을 일시적으로 중단한 다음에 다시 시작하는 방법을 보여줍니다.

```
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
        This host: Primary - Active
                Active time: 776671 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and
'NO' if you wish to abort: Yes
Successfully suspended high-availability.
> show failover
Failover Off
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
> configure high-availability resume
Successfully resumed high-availablity.
> show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Unit Enrollment Hold action is active, timeout in 1792 seconds
Version: Ours 9.7(0)74, Mate 9.7(0)74
```

```
Serial Number: Ours 9A41CKDXQJU, Mate Unknown
Last Failover at: 20:26:06 UTC Nov 4 2016
        This host: Primary - Active
                Active time: 778071 (sec)
                slot 0: empty
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - App Sync
                Active time: 53 (sec)
                  Interface outside (0.0.0.0): Unknown (Waiting)
                  Interface inside (0.0.0.0): Unknown (Waiting)
                  Interface diagnostic (0.0.0.0): Unknown (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
(...Output truncated...)
```

명령	설명
show failover	페일오버(고가용성) 컨피그레이션을 표시합니다.
show high-availability config	페일오버(고가용성) 컨피그레이션을 표시합니다. **show failover**와 같은 출력을 제공합니다.

configure https-access-list

지정된 IP 주소에서 HTTPS 연결을 허용하도록 디바이스를 구성하려면 **configure https-access-list** 명령을 사용합니다.

configure https-access-list *address_list*

address_list	IPv4 CIDR(Classless Inter-Domain Routing) 표기법 또는 IPv6 접두사 길이 표기법을 사용하는 호스트 또는 네트워크의 IP 주소를 쉼표로 구분한 목록입니다. 예를 들어, 10.100.10.0/24 또는 2001:DB8::/96입니다. 모든 IPv4 호스트를 지정하려면 0.0.0.0/0을 입력합니다. 모든 IPv6 호스트를 지정하려면 ::/0을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

단일 명령에서 지원되는 모든 호스트 또는 네트워크를 포함해야 합니다. 이 명령에 지정된 주소는 HTTPS 액세스 목록의 현재 내용을 덮어씁니다.

HTTPS 액세스를 허용해도 사용자가 로컬 관리자에 로그인하는 것이 허용되지 않습니다. 컨피그레이션 소프트웨어에 대한 액세스 권한은 사용자 이름과 비밀번호를 통해 제어됩니다.

다음 예는 모든 IPv4 또는 IPv6 주소에서 HTTPS 연결을 수락하도록 디바이스를 구성합니다.

```
> configure https-access-list 0.0.0.0/0,::/0
The https access list was changed successfully.
> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
```

```
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:https
```

명령	설명
configure disable-https-access	HTTPS 액세스 목록을 지웁니다.
show https-access-list	HTTPS 액세스 목록을 표시합니다.

configure inspection

기본 애플리케이션 프로토콜 검사 엔진을 활성화하거나 비활성화하려면 **configure inspection** 명령을 사용합니다.

configure inspection *protocol* {**enable** | **disable**}

disable	검사 엔진을 비활성화합니다.
enable	검사 엔진을 활성화합니다.
protocol	활성화하거나 비활성화할 검사 프로토콜입니다. 옵션 목록은 사용 지침 섹션을 참고하십시오.

릴리스	수정 사항
6.2	이 명령이 도입되었습니다.

사용 가이드라인

Cisco Technical Support의 지시에 따르는 경우에만 또는 트래픽의 연관된 유형이 네트워크에서 발생하지 않을 것이라고 확인하는 경우에만 기본 검사 엔진을 비활성화합니다. 예를 들어, 검사된 포트에서 모든 트래픽을 차단하는 경우, 해당 포트에서 검사를 안전하게 비활성화할 수 있습니다. 이 검사는 모든 데이터 인터페이스에 적용됩니다.

이 검사 엔진은 Snort 검사에서 분리됩니다. 이 엔진은 다음 서비스를 제공합니다.

- 핀홀 생성—일부 애플리케이션 프로토콜은 표준 포트 또는 협상된 포트에서 보조 TCP 또는 UDP 연결을 엽니다. 검사에서는 이러한 보조 포트를 허용하기 위한 액세스 제어 규칙을 생성할 필요가 없도록 해당 포트에 대해 핀홀을 엽니다.
- NAT 재작성 - FTP 등의 프로토콜은 프로토콜의 일부분으로 패킷 데이터에 보조 연결용 IP 주소 및 포트를 포함합니다. 엔드포인트 중 하나에서 NAT 변환이 수행되는 경우 검사 엔진은 포함된 주소와 포트의 NAT 변환을 반영하기 위해 패킷 데이터를 재작성합니다. NAT 재작성이 수행되지 않으면 보조 연결은 작동하지 않습니다. NAT 제한의 경우, 디바이스(Firepower Management Center 또는 Firepower Device Manager)를 구성하기 위해 사용 중인 관리자에 대한 컨피그레이션 가이드의 NAT 장을 참조하십시오 .
- 프로토콜 적용 - 일부 검사에서는 검사된 프로토콜에 대해 특정 수준의 RFC 적합성을 적용합니다.

다음 검사 엔진을 비활성화한 다음 순차적으로 활성화할 수 있습니다. 현재 활성화된 항목을 보려면 **show running-config policy-map** 명령을 사용하고 **inspect** 명령을 찾습니다. 각 검사에 대한 기본 파라미터의 세부 사항을 보려면 **show running-config all policy-map** 명령을 사용합니다.

- **dcerpc** — (TCP 포트 135.) 분산 컴퓨팅 환경/원격 절차 호출. DCERPC 검사 엔진은 잘 알려진 TCP 포트 135에서 EPM(Endpoint Mapper)과 클라이언트 간의 기본 TCP 통신을 검사합니다. DCERPC(Microsoft Remote Procedure Call)는 DCERPC 기반으로, Microsoft에서 배포한 클라이언트 및 서버 애플리케이션에서 널리 사용되는 프로토콜로서, 소프트웨어 클라이언트가 서버의 프로그램을 원격으로 실행하도록 허용합니다. 검사는 핀홀 생성 및 NAT 서비스를 제공합니다.
- **dns** — (UDP 포트 53.) Domain Name System. DNS는 UDP 포트 53에서 검사됩니다. 검사는 NAT 서비스 및 프로토콜 실행을 제공합니다. NAT 규칙의 NAT 재작성 옵션을 사용하도록 이 검사 엔진을 활성화해야 합니다. NAT 재작성은 IPv4 및 IPv6 네트워크(NAT64/46) 간에 NAT를 수행할 때 자주 필요합니다.
- **esmtp** — (TCP 포트 25.) ESMTP(Extended Simple Mail Transfer Protocol). ESMTP 검사는 스팸, 피싱, 형식이 잘못된 메시지 공격, 버퍼 오버플로/언더플로 공격 등의 공격을 탐지합니다. 또한 애플리케이션 보안 및 프로토콜 적합성에 대한 지원을 제공하여 ESMTP 메시지의 정상성(sanity)을 적용하는 것은 물론 발신자/수신자를 차단하고, 메일 릴레이를 차단합니다. 검사 동안 적용된 제어에 대한 자세한 내용은 **show running-config all policy-map** 명령을 사용하고 "policy-map type inspect esmtp _default_esmtp_map" 회선 및 후속 파라미터를 찾습니다.

  ESMTP 애플리케이션 검사는 사용자가 사용할 수 있는 명령 및 서버가 반환할 수 있는 메시지를 제어하고 축소합니다. 이는 NAT 서비스 및 프로토콜 적합성을 제공합니다. ESMTP 검사는 세 가지 기본 작업을 수행합니다.

  - SMTP 요청을 7개의 기본 SMTP 명령 및 8개의 확장 명령으로 제한합니다. 지원되는 명령은 다음과 같습니다.

    확장 SMTP — AUTH, EHLO, ETRN, HELP, SAML, SEND, SOML, STARTTLS 및 VRFY.

    SMTP(RFC 821) — DATA, HELO, MAIL, NOOP, QUIT, RCPT, RSET.
  - SMTP 명령-응답 시퀀스를 모니터링합니다.
  - 감사 추적 생성. 메일 주소에 잘못된 문자가 포함되어 교체된 경우 Syslog 감사 레코드 108002가 생성됩니다. 자세한 내용은 RFC 821을 참조하십시오.
- **ftp** — (TCP 포트 21.) FTP(File Transfer Protocol). 검사는 핀홀 및 NAT 서비스를 제공합니다.
- **h323_h225** — (TCP 포트 1720, UDP 포트 1718.) H.323 검사는 RAS, H.225 및 H.245를 지원하며, 포함된 모든 IP 주소 및 포트를 변환하는 기능을 제공합니다. 이것은 상태 추적 및 필터링을 수행합니다. H.323 검사는 H.323 호환 애플리케이션(예: Cisco CallManager)에 대한 지원을 제공합니다. H.323은 LAN을 통한 멀티미디어 회의를 위해 ITU(International Telecommunication Union)에서 정의한 프로토콜 모음입니다. 디바이스는 버전 6에서 H.323을 지원하며, 여기에는 H.323 v3 기능인 단일 통화 신호 채널에서의 다중 통화(Multiple Calls on One Call Signaling Channel)가 포함됩니다.

  H.323 검사의 중요한 두 가지 기능은 다음과 같습니다.

  - H.225 및 H.245 메시지에 포함된 필수 IPv4 주소를 NAT 처리. H.323 메시지는 PER 인코딩 형식으로 인코딩되므로 ASA는 ASN.1 디코더를 사용하여 H.323 메시지를 디코딩합니다.

◦ 협상된 H.245 및 RTP/RTCP 연결을 동적으로 할당합니다. RAS를 사용할 경우 H.225 연결도 동적으로 할당됩니다.

- **h323_ras** — (UDP 포트 1718-1719.) **h323_h225**에 대한 설명을 참조하십시오. 이 검사는 RAS 신호용입니다.
- **icmp** — (ICMP 트래픽 전용.) ICMP 검사 엔진은 TCP 및 UDP 트래픽처럼 검사할 수 있는 "session"을 ICMP 트래픽에 포함하도록 허용합니다. ICMP 검사 엔진이 없는 경우에는 ICMP가 디바이스를 통과하도록 허용하지 않는 것이 좋습니다(액세스 제어 규칙을 통한 차단). 상태 저장 검사가 없으면 ICMP가 네트워크를 공격하는 데 사용될 수 있습니다. ICMP 검사 엔진을 사용하면 각 요청에 대해 하나의 응답만 존재할 수 있으며 시퀀스 번호의 정확성이 보장됩니다. 검사는 NAT 서비스도 제공합니다.
- **icmp_error** — (ICMP 트래픽 전용.) ICMP 오류 검사가 활성화되면 디바이스는 NAT 컨피그레이션을 기반으로 ICMP 오류 메시지를 전송하는 중간 홉(hop)에 대한 변환 세션을 만듭니다. 디바이스는 패킷을 변환된 IP 주소로 덮어씁니다. 이것은 디바이스를 통과하는 트레이스라우트(traceroute)의 의미 있는 정보를 제공하는 데 필요합니다.
- **ip-options** — (RSVP 트래픽 전용.) IP 옵션 검사는 어떤 IP 패킷이 패킷 헤더의 IP 옵션 필드의 내용에 따라 허용되는지 제어합니다. 라우터 알림 옵션이 포함된 패킷이 허용됩니다. 기타 옵션이 포함된 패킷은 드롭됩니다.
- **netbios** — (UDP 소스 포트 137, 138.) NetBIOS Name Server over IP. NetBIOS 애플리케이션 검사는 NBNS(NetBIOS name service) 패킷 및 NetBIOS 데이터그램 서비스 패킷에 포함된 IP 주소에 대해 NAT를 수행합니다. 또한 프로토콜 적합성을 적용하여 다양한 개수 및 길이 필드에서 일관성을 확인합니다.
- **rsh** — (TCP 포트 514.) RSH 프로토콜은 RSH 클라이언트에서 RSH 서버로의 TCP 연결을 사용합니다(TCP 포트 514). 클라이언트와 서버는 클라이언트가 STDERR 출력 스트림을 수신 대기하는 TCP 포트 번호를 협상합니다. 필요한 경우 RSH 검사는 핀홀을 열고 협상된 포트 번호의 NAT를 지원합니다.
- **rtsp** — (TCP 포트 554.) Real-Time Streaming Protocol. RTSP 검사 엔진은 디바이스에서 RTSP 패킷을 전달하도록 합니다. RTSP는 RealAudio, RealNetworks, Apple QuickTime, RealPlayer 및 Cisco IP/TV 연결에 사용됩니다. RTSP 애플리케이션은 잘 알려진 포트 554와 함께 제어 채널로서 TCP(매우 드물게 UDP)를 사용합니다. 디바이스에서는 RFC 2326에 따라 TCP만 지원합니다. 이 TCP 제어 채널은 클라이언트에 구성된 전송 모드에 따라 오디오/비디오 트래픽 전송에 사용되는 데이터 채널을 협상하는 데 사용됩니다. 지원되는 RDT 전송은 rtp/avp, rtp/avp/udp, x-real-rdt, x-real-rdt/udp 및 x-pn-tng/udp입니다.
- **sqlnet** — (TCP 포트 1521.) 검사 엔진은 SQL*Net 버전 1 및 2를 지원하나 TNS(Transparent Network Substrate) 형식만 지원합니다. 검사에서 TDS(Tabular Data Stream) 형식을 지원하지는 않습니다. 포함된 주소 및 포트에 대해 SQL*Net 메시지를 검사하고 NAT 재작성은 필요한 경우 적용됩니다.

  SQL 컨트롤 TCP 포트 1521과 동일한 포트에서 SQL 데이터 전송이 발생하는 경우 SQL*Net 검사를 비활성화하십시오. SQL*Net 검사가 활성화되면 보안 어플라이언스는 프록시 역할을 하여 클라이언트 기간 크기를 65000에서 약 16000으로 줄이므로 데이터 전송 문제가 발생할 수 있습니다.

- **sip** — (TCP/UDP 포트 5060.) SIP(Session Initiation Protocol) SIP는 인터넷 컨퍼런싱, 텔레포니, 프레즌스, 이벤트 알림 및 인스턴트 메시징에 가장 널리 사용되는 프로토콜입니다. 부분적으로 텍스트 기반 속성 때문에 그리고 부분적으로 유연성 때문에, SIP 네트워크는 다양한 보안 위협의 영향을 받을 수 있습니다. SIP 애플리케이션 검사는 메시지 헤더 및 본문의 주소 변환, 동적인 포트 열기, 기본적인 온전성 확인 등을 제공합니다.
- **skinny** — (TCP 포트 2000.) SCCP(Skinny Client Control Protocol) SCCP(Skinny) 애플리케이션 검사는 패킷 데이터 내에 포함된 IP 주소와 포트 번호를 변환하고 핀홀을 동적으로 엽니다. 또한 추가 프로토콜 적합성 확인 및 기본 상태 추적을 수행합니다.
- **sunrpc** — (UDP 포트 111.) NFS 및 NIS에서 Sun RPC를 사용합니다. Sun RPC 서비스는 어느 포트에서나 실행할 수 있습니다. 클라이언트가 서버의 Sun RPC 서비스에 액세스하려면 현재 서비스가 실행 중인 포트를 알아야 합니다. 이 작업은 잘 알려진 포트 111에서 포트 매퍼 프로세스(대개 rpcbind)를 쿼리하여 수행됩니다.

  클라이언트는 서비스의 Sun RPC 프로그램 번호를 전송하고 포트 매퍼 프로세스는 서비스의 포트 번호로 응답합니다. 클라이언트는 포트 매퍼 프로세스로 식별된 포트를 지정하여 Sun RPC 쿼리를 서버로 전송합니다. 서버가 회신할 때 디바이스는 이 패킷을 가로채고 해당 포트에서 원시 TCP 및 UDP 연결을 모두 엽니다. Sun RPC 페이로드 정보의 NAT 또는 PAT는 지원되지 않습니다.
- **tftp** — (UDP 포트 69.) TFTP(Trivial File Transfer Protocol). 검사 엔진은 TFTP 읽기 요청(RRQ), 쓰기 요청(WRQ), 오류 알림(ERROR)을 검사하고 TFTP 클라이언트와 서버 간 파일 전송을 허용하기 위해 필요한 경우 연결과 변환을 동적으로 생성합니다.

  유효한 읽기(RRQ) 또는 쓰기(WRQ) 요청을 수신할 경우 필요에 따라 동적 보조 채널 및 PAT 변환이 할당됩니다. 이 보조 채널은 이후 파일 전송 또는 오류 알림을 위해 TFTP에서 사용됩니다. TFTP 서버만이 보조 채널을 통해 트래픽을 시작할 수 있으며, TFTP 클라이언트와 서버 사이에는 불완전한 보조 채널이 최대 하나만 존재할 수 있습니다. 서버에서 오류 알림을 보내면 보조 채널이 닫힙니다. TFTP 트래픽 리디렉션에 고정 PAT가 사용되는 경우 TFTP 검사를 활성화해야 합니다.
- **xdmcp** — (UDP 포트 177.) X Display Manager Control Protocol. XDMCP는 UDP 포트 177을 사용하여 X 세션을 협상하는 프로토콜이며, 설정 시 TCP가 사용됩니다. 성공적으로 협상하여 XWindows 세션을 시작하려면 디바이스는 Xhosted 컴퓨터에서 오는 TCP 반환 연결을 허용해야 합니다. TCP 포트를 통해 반환 연결을 허용하려면 액세스 제어 규칙을 사용합니다.

  XWindows 세션 동안 관리자는 잘 알려진 포트 6000 | n의 디스플레이 Xserver에 연결합니다. 다음 터미널 설정으로 인해 각 디스플레이는 별도로 Xserver에 연결됩니다. **setenv DISPLAY Xserver:***n*(*n*은 디스플레이 번호임)

  XDMCP를 사용할 경우 IP 주소를 사용하여 디스플레이를 협상하며, 필요 시 디바이스에서는 NAT를 지원할 수 있습니다. XDCMP 검사는 PAT를 지원하지 않습니다.

다음 예에서는 현재 검사 컨피그레이션을 보여주고 XDMCP 검사를 비활성화합니다. 검사 엔진을 활성화하거나 비활성화할 수 있지만, 기본 동작은 변경할 수 없습니다. 예를 들어, 이 출력은 DNS/TCP

검사가 비활성화되었음을 보여줍니다. **configure inspection** 명령을 사용하여 TCP 트래픽에 적용할 DNS 검사를 구성할 수 없습니다.

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
!
> configure inspection xdmcp disable
Building configuration...
Cryptochecksum: 46dbea1d 51c2089a fcc3e42f 3dafd2d5
12386 bytes copied in 0.160 secs
[OK]
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
  inspect dcerpc
  inspect ftp
```

!

명령	설명
show running-config policy-map	검사 컨피그레이션을 포함하는 서비스 정책에 대한 정책 맵을 보여줍니다.
show service-policy	검사에 대한 통계를 포함하는 서비스 정책 통계를 보여줍니다.

configure log-events-to-ramdisk

시스템 성능을 개선하고 SSD(Solid State Drive)에 연결 이벤트 쓰기와 연관된 디스크 마모를 줄이기 위해 RAM 디스크에 대한 연결 이벤트 로깅을 사용하거나 사용하지 않으려면 **configure log-events-to-ramdisk** 명령을 사용합니다.

configure log-events-to-ramdisk {**enable** | **disable**}

사용	RAM 디스크에 대한 연결 이벤트 로깅을 사용합니다.
사용 해제	RAM 디스크에 대한 연결 이벤트 로깅을 사용 해제합니다. 그런 다음 연결 이벤트는 SSD에 로깅됩니다.

기본값이 기능을 지원하는 플랫폼에서 사용 설정됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

연결 이벤트를 로깅하기 위해 RAM 디스크 또는 물리적인 SSD 사용 사이에서 전환하려면 이 명령을 사용합니다. 이 명령이 사용 설정된 경우, 연결 이벤트는 RAM 디스크에 기록됩니다. 이 명령이 사용 하제된 경우, 연결 이벤트는 SSD에 기록됩니다. 전력이 손실된 경우, RAM 디스크에 로깅된 연결 이벤트가 손실됩니다.

이 명령은 ASA 5512, ASA 5515 및 Firepower 4100 Series에서만 사용할 수 있습니다. 지원되지 않는 플랫폼에서 이 명령을 실행하면 시스템이 다음 메시지를 반환합니다.

```
This command is not available on this platform.
```

다음 예에서는 RAM 디스크 로깅을 사용 해제합니다.

```
> configure log-events-to-ramdisk disable
```

명령	설명
show log-events-to-disk	현재 로깅 상태를 표시합니다.
show disk-manager	시스템의 각 부분(silos, low watermarks, high watermarks 등)에 대한 자세한 디스크 사용량 정보를 표시합니다.

configure manager add

관리하는 Firepower Management Center에서 연결을 수락하기 위해 디바이스를 구성하려면 **configure manager add** 명령을 사용합니다. 이 명령은 디바이스가 적극적으로 관리되지 않는 경우에만 실행됩니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *regkey* [*nat_id*]

hostname	이 디바이스를 관리해야 하는 Management Center의 DNS 호스트 이름을 지정합니다.
IPv4_address	Management Center의 IPv4 주소를 지정합니다.
IPv6_address	Management Center의 IPv6 주소를 지정합니다.
DONTRESOLVE	Management Center의 주소를 직접 지정할 수 없으면 **DONTRESOLVE**를 사용합니다. **DONTRESOLVE**를 사용하는 경우 *nat_id*가 필요합니다.
regkey	디바이스를 Management Center에 등록하는 데 필요한 고유한 영숫자 등록 키입니다.
nat_id	Management Center와 디바이스 간의 등록 프로세스 동안 사용되는 선택적인 영숫자 문자열을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

관리하는 Firepower Management Center에서 연결을 수락하도록 디바이스를 구성하려면 이 명령을 사용합니다.

디바이스를 Management Center에 등록하려면 고유한 영숫자 등록 키가 항상 필요합니다. 대부분의 경우 등록 키와 함께 호스트 이름 또는 IP 주소를 제공해야 합니다. 그러나 디바이스와 Management

Center가 NAT 디바이스에 의해 분리된 경우, 등록 키와 함께 고유한 NAT ID를 입력하고 호스트 이름 대신 DONTRESOLVE를 지정해야 합니다.

```
> configure manager add DONTRESOLVE abc123 efg456
```

명령	설명
configure manager delete	관리 Firepower Management Center를 제거합니다.
configure manager local	로컬 관리자를 구성합니다.
show managers	현재 관리자를 표시합니다.

configure manager delete

현재 관리자를 비활성화하고 No Manager 모드를 시작하려면 **configure manager delete** 명령을 사용합니다.

configure manager delete

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

현재 디바이스 관리자를 제거하려면 이 명령을 사용합니다. 디바이스는 원격 관리자를 추가하거나 로컬 관리자를 사용할 수 있는 No Manager 모드에 있습니다. 로컬 관리와 원격 관리 간에 전환할 경우 또는 원격 관리자가 더 이상 활성 상태가 아닌 경우 이 명령을 사용합니다.

명령 동작은 현재 관리자에 따라 달라집니다.

- Remote—Firepower Management Center에 연결할 수 없습니다. Management Center가 아직 작동 중인 경우, 먼저 Management Center의 인벤토리에서 디바이스를 제거합니다. 그런 다음 이 명령을 사용할 수 있습니다.
- Local—제한사항이 없습니다. No Manager 모드로 즉시 이동합니다.

다음 예에서는 현재 관리자를 제거하고 No Manager 모드를 시작합니다.

```
> configure manager delete
```

명령	설명
configure manager add	디바이스의 관리 Firepower Management Center를 구성합니다.
configure manager local	로컬 관리자를 구성합니다.
show managers	현재 관리자를 표시합니다.

configure manager local

로컬 관리자로 Firepower Device Manager를 사용하기 위해 디바이스를 구성하려면 **configure manager local** 명령을 사용합니다.

configure manager local

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

로컬 관리자로 Firepower Device Manager를 활성화하려면 다음 명령을 사용합니다. 별도의 Firepower Management Center를 사용하지 않으려는 경우 로컬 관리자를 사용합니다. 로컬 관리자를 활성화하면 **http://***management_ip_address*에서 브라우저를 사용하여 Firepower Device Manager를 열 수 있습니다.

로컬 관리자는 다음 플랫폼에서만 사용 가능합니다.

- ASA 5506-X(모든 옵션), 5508-X, 5516-X
- ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X.

다른 모든 플랫폼의 경우, **configure manager add** 명령을 사용하여 원격 관리자를 구성합니다.

추가 제한사항

- 로컬 관리자로 전환할 수 있게 되기 전에 디바이스는 No Manager(관리자 없음) 모드여야 합니다. **configure manager delete** 명령을 사용하여 No Manager(관리자 없음) 모드를 시작합니다. **show managers** 명령을 사용하여 현재 관리자를 결정합니다.

- 디바이스는 투명 방화벽 모드(**configure firewall** 명령 참조)에서 작동할 수 없습니다. 로컬 관리자는 라우팅 모드만 지원합니다.

다음 예에서는 로컬 관리자를 구성하는 방법을 보여줍니다.

```
> configure manager local
```

명령	설명
configure manager add	디바이스의 관리 Firepower Management Center를 구성합니다.
configure manager delete	관리 Firepower Management Center를 제거합니다.
show managers	현재 관리자를 표시합니다.

configure network dns searchdomains

DNS 검색 도메인 목록을 구성하려면 **configure network dns searchdomains** 명령을 사용합니다.

configure network dns searchdomains [*dnslist*]

dnslist	DNS 검색 도메인의 쉼표로 구분된 목록을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

새 목록으로 DNS 검색 도메인의 현재 목록을 대체하려면 이 명령을 사용합니다. 이 도메인은 명령(예: **ping system**)에서 FQDN(Fully Qualified Domain Name)을 지정하지 않은 경우 호스트 이름에 추가됩니다. 도메인은 관리 인터페이스에서 사용되거나 관리 인터페이스를 통과하는 명령에 대해서만 사용됩니다.

다음 예에서는 새로운 검색 도메인 목록을 구성한 다음 정규화(fully-qualified)되지 않은 ping의 호스트 이름을 구성합니다.

```
> configure network dns searchdomains example.com
> show dns system
search example.com
nameserver 10.163.47.11
> ping system www
PING www.example.com (10.163.4.161) 56(84) bytes of data.
64 bytes from www.example.com (10.163.4.161): icmp_seq=1 ttl=242 time=8.01 ms
64 bytes from www.example.com (10.163.4.161): icmp_seq=2 ttl=242 time=16.7 ms
^C
--- origin-www.cisco.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 7.961/10.216/16.718/3.755 ms
```

명령	설명
configure network dns servers	DNS 서버를 구성합니다.

명령	설명
show dns system	관리 인터페이스의 현재 DNS 컨피그레이션을 표시합니다.

configure network dns servers

관리 인터페이스의 DNS 서버를 구성하려면 **configure network dns servers** 명령을 사용합니다.

configure nework dns servers [*dnslist*]

dnslist	DNS 서버의 쉼표로 구분된 목록을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

새 목록으로 DNS 서버의 현재 목록을 대체하려면 이 명령을 사용합니다. 서버는 관리 인터페이스에서만 사용됩니다. 이 서버는 데이터 인터페이스를 통과하는 명령의 FQDN(Fully Qualified Domain Name)을 확인할 수 없습니다.

다음 예에서는 관리 인터페이스의 DNS 서버를 구성합니다.

```
> configure network dns servers 10.163.47.11,10.124.1.10
> show dns system
search example.com
nameserver 10.163.47.11
nameserver 10.124.1.10
```

명령	설명
configure network dns searchdomains	DNS 검색 도메인을 구성합니다.
show dns system	관리 인터페이스의 현재 DNS 컨피그레이션을 표시합니다.

configure network hostname

디바이스의 관리 인터페이스용 호스트 이름을 구성하려면 **configure network hostname** 명령을 사용합니다.

configure network hostname *name*

name	새 호스트 이름을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 호스트 이름을 sfrocks로 설정합니다.

```
> configure network hostname sfrocks
```

명령	설명
show network	관리 인터페이스 구성을 표시합니다.

configure network http-proxy

관리 인터페이스의 HTTP 프록시를 구성하려면 **configure network http-proxy** 명령을 사용합니다.

configure network http-proxy

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스에 대한 HTTP 프록시 주소를 설정하려면 이 명령을 사용합니다. 명령을 실행하면 HTTP 프록시 주소와 포트, 프록시 인증이 필요한지 여부에 대한 프롬프트가 표시되며, 해당 인증이 필요한 경우 프록시 사용자 이름, 프록시 비밀번호, 프록시 비밀번호의 확인에 대한 프롬프트가 표시됩니다.

참고 HTTP 프록시는 원격 관리자 전용으로 사용하기 위해 지원됩니다. 이것은 로컬 관리자, Firepower Device Manager를 사용할 경우 지원되지 않습니다.

다음 예는 관리 인터페이스에 대한 HTTP 프록시를 구성합니다. 이 예에서 인증이 구성됩니다. CLI는 사용자가 입력한 비밀번호를 표시하지 않습니다.

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

명령	설명
configure network http-proxy-disable	HTTP 프록시 설정을 비활성화합니다.
show network	관리 인터페이스 컨피그레이션을 표시합니다.

configure network http-proxy-disable

관리 인터페이스의 HTTP 프록시를 제거하려면 **configure network http-proxy-disable** 명령을 사용합니다.

configure network http-proxy-disable

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 관리 인터페이스에 대한 HTTP 프록시를 제거합니다.

```
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                        : Enabled
HTTP Proxy                   : 10.100.10.10
Port                         : 80
Authentication               : Enabled
Username                     : proxyuser
> configure network http-proxy-disable
Are you sure that you wish to delete the current http-proxy configuration? (y/n): y
Configuration successfully deleted.
> show network
(...Output Truncated...)
===============[ Proxy Information ]================
State                        : Disabled
Authentication               : Disabled
```

명령	설명
configure network http-proxy	HTTP 프록시 설정을 구성합니다.
show network	관리 인터페이스 컨피그레이션을 표시합니다.

configure network ipv4 delete

디바이스 관리 인터페이스의 IPv4 컨피그레이션을 비활성화하려면 **configure network ipv4 delete** 명령을 사용합니다.

configure network ipv4 delete [*management_interface*]

management_ interface	두 개 이상의 인터페이스를 구성하는 경우 관리 인터페이스를 지정합니다. 이 파라미터는 2개 이상의 관리 인터페이스를 활성화하기 위해 **configure management-interface** 명령을 사용하는 경우에만 필요합니다. 여러 인터페이스는 Firepower 4100 및 9300 시리즈 디바이스에서만 지원됩니다. 다른 플랫폼에 이 파라미터를 지정하지 마십시오.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스 관리 인터페이스의 IPv4 컨피그레이션을 비활성화하려면 이 명령을 사용합니다. 삭제하는 IP 주소에 연결된 경우, 디바이스에 대한 연결이 손실됩니다. IPv4 주소를 제거하기 전에 구성된 IPv6 주소가 있는지 확인합니다.

IPv4 주소를 변경하기 위해 컨피그레이션을 삭제할 필요가 없습니다. IPv4 주소 지정을 유지하지만 주소를 간단하게 변경하려는 경우 **configure network ipv4 manual** 또는 **configure network ipv4 dhcp** 명령을 사용합니다.

다음 예에서는 IPv4 주소 컨피그레이션을 삭제합니다.

```
> configure network ipv4 delete
```

명령	설명
configure network ipv4 dhcp	DHCP 서버에서 주소를 얻기 위해 IPv4를 구성합니다.

명령	설명
configure network ipv4 manual	수동으로 IPv4에 고정 IP 주소를 구성합니다.
show network	관리 인터페이스 컨피그레이션을 표시합니다.

configure network ipv4 dhcp

DHCP 서버에서 IPv4 주소를 가져오도록 관리 인터페이스를 구성하려면 **configure network ipv4 dhcp** 명령을 사용합니다.

configure network ipv4 dhcp [*management_interface*]

management_ interface	하나 이상의 인터페이스를 구성하는 경우 관리 인터페이스를 지정합니다. 이 파라미터는 1개 이상의 관리 인터페이스를 사용 설정하기 위해 **configure management-interface** 명령을 사용하는 경우에만 필요합니다. 여러 인터페이스는 Firepower 4100 및 9300 Series 디바이스에서만 지원됩니다. 다른 플랫폼에 이 파라미터를 지정하지 마십시오.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스의 관리 인터페이스가 DHCP 서버에서 해당 IPv4 구성을 수신하도록 지정하려면 이 명령을 사용합니다. 관리 인터페이스는 DHCP 서버와 통신하여 구성 정보를 가져옵니다.

다음 예에서는 DHCP를 사용하여 IPv4 주소를 가져오도록 관리 인터페이스를 구성합니다.

```
> configure network ipv4 dhcp
```

명령	설명
configure network ipv4 delete	IPv4 네트워킹을 사용 해제합니다.
configure network ipv4 manual	IPv4를 수동으로 구성합니다.
show network	관리 인터페이스 구성을 표시합니다.

configure network ipv4 dhcp-server-disable

관리 인터페이스에서 DHCP 서버를 비활성화하려면 **configure network ipv4 dhcp-server-disable** 명령을 사용합니다.

configure network ipv4 dhcp-server-disable

릴리스	수정 사항
6.2	이 명령이 도입되었습니다.

사용 가이드라인

관리 인터페이스에 활성 DHCP 서버가 있는 경우, 해당 서버를 비활성화할 수 있습니다. 이 서버를 비활성화할 경우, 관리 네트워크에 있는 클라이언트는 고정 주소를 구성해야 하거나 DHCP 서버 서비스를 제공하도록 네트워크에서 다른 디바이스를 구성해야 합니다.

주소를 가져오기 위해 DHCP를 사용하도록 관리 IP 주소를 변경하는 경우, DHCP 서버(활성화된 경우)가 자동으로 비활성화됩니다.

다음 예에서는 DHCP 서버가 활성화되었는지 여부를 확인한 다음 이 서버를 비활성화하는 방법을 보여줍니다.

```
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
> configure network ipv4 dhcp-server-disable
DCHP Server Disabled
> show network-dhcp-server
DHCP Server Disabled
```

명령	설명
configure network ipv4 dhcp-server-enable	관리 인터페이스에서 DHCP 서버를 활성화합니다.
show dhcp-server	관리 인터페이스에서 DHCP 서버의 상태를 표시합니다.

configure network ipv4 dhcp-server-enable

관리 인터페이스에서 선택적인 DHCP 서버를 활성화하려면 **configure network ipv4 dhcp-server-enable** 명령을 사용합니다.

configure network ipv4 dhcp-server-enable *start_ip_address end_ip_address*

start_ip_address *end_ip_address*	DHCP 주소 풀의 시작 및 끝 IPv4 주소를 지정합니다. 관리 인터페이스는 DHCP 클라이언트 요청을 받을 때, 이러한 풀에서 주소를 제공합니다. 풀은 관리 IPv4 주소와 동일한 서브넷에 있어야 합니다. DHCP 주소 풀의 네트워크 주소, 관리 주소 또는 브로드캐스트 주소를 포함하지 마십시오.

릴리스	수정 사항
6.2	이 명령이 도입되었습니다.

사용 가이드라인

관리 인터페이스에 대해 수동(고정) IPv4 주소를 구성할 경우, 관리 네트워크의 엔드포인트에 주소를 제공하기 위해 DHCP 서버를 구성할 수 있습니다.

서버를 활성화하기 전에 관리 네트워크에 다른 DHCP 서버가 없는지 확인합니다. 네트워크당 최대 1개의 DHCP 서버를 가질 수 있습니다. 아니면 결과를 예측할 수 없습니다.

다음 예에서는 DHCP 서버를 구성하는 방법과 서버의 상태를 보여줍니다.

```
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
```

```
192.168.45.46-192.168.45.254
```

명령	설명
configure network ipv4 dhcp-server-disable	관리 인터페이스에서 DHCP 서버를 비활성화합니다.
show dhcp-server	관리 인터페이스에서 DHCP 서버의 상태를 표시합니다.

configure network ipv4 manual

관리 인터페이스에 고정 IPv4 주소를 구성하려면 **configure network ipv4 manual** 명령을 사용합니다.

configure network ipv4 manual *ipaddr netmask gw* [*management_interface*]

ipaddr	IP 주소를 지정합니다.
netmask	서브넷 마스크를 지정합니다.
gw	기본 게이트웨이의 IPv4 주소를 지정합니다. 로컬 관리자인 Firepower Device Manager를 사용 중인 경우, **data-interfaces**를 지정하는 옵션이 있는데 이 옵션은 관리 네트워크에 있는 명시적 게이트웨이 대신 디바이스에 있는 데이터 인터페이스를 게이트웨이로 사용합니다. 별도의 관리 네트워크에 물리적 관리 인터페이스를 연결하지 않으려는 경우 데이터 인터페이스를 사용합니다.
management_ interface	둘 이상의 인터페이스를 구성하는 경우 관리 인터페이스를 지정합니다. 이 파라미터는 2개 이상의 관리 인터페이스를 활성화하기 위해 **configure management-interface** 명령을 사용하는 경우에만 필요합니다. 여러 인터페이스는 Firepower 4100 및 9300 Series 디바이스에서만 지원됩니다. 다른 플랫폼에 이 파라미터를 지정하지 마십시오.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.
6.2	**data-interfaces** 키워드가 게이트웨이에 추가되었습니다.

다음 예에서는 관리 인터페이스에 고정 IPv4 주소를 구성합니다.

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

명령	설명
configure network ipv4 delete	IPv4 네트워킹을 비활성화합니다.
configure network ipv4 dhcp	DHCP를 통해 IPv4를 구성합니다.
show network	관리 인터페이스 컨피그레이션을 표시합니다.

configure network ipv6 delete

디바이스 관리 인터페이스의 IPv6 구성을 사용 해제하려면 **configure network ipv6 delete** 명령을 사용합니다.

configure network ipv6 delete [*management_interface*]

management_ interface	하나 이상의 인터페이스를 구성하는 경우 관리 인터페이스를 지정합니다. 이 매개변수는 1개 이상의 관리 인터페이스를 사용 설정하기 위해 **configure management-interface** 명령을 사용하는 경우에만 필요합니다. 여러 인터페이스는 Firepower 4100 및 9300 Series 디바이스에서만 지원됩니다. 다른 플랫폼에 이 매개변수를 지정하지 마십시오.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스 관리 인터페이스의 IPv6 구성을 사용 해제하려면 이 명령을 사용합니다. 삭제하는 IP 주소에 연결된 경우, 디바이스에 대한 연결이 손실됩니다. IPv6 주소를 제거하기 전에 구성된 IPv6 주소가 있는지 확인합니다.

IPv6 주소를 변경하기 위해 구성을 삭제할 필요가 없습니다. IPv6 주소 지정을 유지하지만 주소를 간단하게 변경하려는 경우 **configure network ipv6** {**manual** | **dhcp** | **router**} 명령을 사용합니다.

다음 예에서는 IPv6 주소 구성을 삭제합니다.

```
> configure network ipv6 delete
```

명령	설명
configure network ipv6 dhcp	DHCP를 통해 IPv6를 구성합니다.

명령	설명
configure network ipv6 manual	IPv6를 수동으로 구성합니다.
configure network ipv6 router	라우터를 통해 IPv6를 구성합니다.
show network	관리 인터페이스 구성을 표시합니다.

configure network ipv6 dhcp

DHCP 서버에서 IPv6 주소를 가져오도록 관리 인터페이스를 구성하려면 **configure network ipv6 dhcp** 명령을 사용합니다.

configure network ipv6 dhcp [*management_interface*]

management_ interface	하나 이상의 인터페이스를 구성하는 경우 관리 인터페이스를 지정합니다. 이 매개변수는 1개 이상의 관리 인터페이스를 활성화하기 위해 **configure management-interface** 명령을 사용하는 경우에만 필요합니다. 여러 인터페이스는 Firepower 4100 및 9300 Series 디바이스에서만 지원됩니다. 다른 플랫폼에 이 매개변수를 지정하지 마십시오.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스의 관리 인터페이스가 DHCP 서버에서 해당 IPv6 컨피그레이션을 수신하도록 지정하려면 이 명령을 사용합니다. 관리 인터페이스는 DHCP 서버와 통신하여 컨피그레이션 정보를 가져옵니다.

다음 예에서는 DHCP를 사용하여 IPv6 주소를 가져오도록 관리 인터페이스를 구성합니다.

```
> configure network ipv6 dhcp
```

명령	설명
configure network ipv6 delete	IPv6 네트워킹을 사용 해제합니다.
configure network ipv6 manual	IPv6를 수동으로 구성합니다.

명령	설명
configure network ipv6 router	라우터를 통해 IPv6를 구성합니다.
show network	관리 인터페이스 구성을 표시합니다.

configure network ipv6 manual

관리 인터페이스에서 고정 IPv6 주소를 구성하려면 **configure network ipv6 manual** 명령을 사용합니다.

configure network ipv6 manual *ip6addr ip6prefix* [*ip6gw*] [*management_interface*]

ip6addr	IP 주소를 지정합니다.
ip6prefix	접두사 길이를 지정합니다.
ip6gw	기본 게이트웨이의 IPv6 주소를 지정합니다. 로컬 관리자인 Firepower Device Manager를 사용 중인 경우, **data-interfaces**를 지정하는 옵션이 있는데 이 옵션은 관리 네트워크에 있는 명시적 게이트웨이 대신 디바이스에 있는 데이터 인터페이스를 게이트웨이로 사용합니다. 별도의 관리 네트워크에 물리적 관리 인터페이스를 연결하지 않으려는 경우 데이터 인터페이스를 사용합니다.
management_ interface	하나 이상의 인터페이스를 구성하는 경우 관리 인터페이스를 지정합니다. 이 매개변수는 1개 이상의 관리 인터페이스를 사용 설정하기 위해 **configure management-interface** 명령을 사용하는 경우에만 필요합니다. 여러 인터페이스는 Firepower 4100 및 9300 Series 디바이스에서만 지원됩니다. 다른 플랫폼에 이 매개변수를 지정하지 마십시오.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.
6.2	**data-interfaces** 키워드가 게이트웨이에 추가되었습니다.

다음 예에서는 관리 인터페이스에 고정 IPv6 주소를 구성합니다.

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

명령	설명
configure network ipv6 delete	IPv6 네트워킹을 사용 해제합니다.
configure network ipv6 dhcp	DHCP를 통해 IPv6를 구성합니다.
configure network ipv6 router	라우터를 통해 IPv6를 구성합니다.
show network	관리 인터페이스 구성을 표시합니다.

configure network ipv6 router

상태 비저장 자동 구성을 사용하여 라우터에서 IPv6 주소를 가져오도록 관리 인터페이스를 구성하려면 **configure network ipv6 router** 명령을 사용합니다.

configure network ipv6 router [*management_interface*]

management_ interface	하나 이상의 인터페이스를 구성하는 경우 관리 인터페이스를 지정합니다. 이 매개변수는 1개 이상의 관리 인터페이스를 사용하기 위해 **configure management-interface** 명령을 사용하는 경우에만 필요합니다. 여러 인터페이스는 Firepower 4100 및 9300 Series 디바이스에서만 지원됩니다. 다른 플랫폼에 이 매개변수를 지정하지 마십시오.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스의 관리 인터페이스가 라우터에서 해당 IPv6 구성을 수신하도록 지정하려면 이 명령을 사용합니다. 관리 인터페이스는 IPv6 라우터와 통신하여 구성 정보를 가져옵니다.

다음 예에서는 상태 비저장 자동 구성을 사용하여 라우터에서 IPv6 주소를 수신하기 위해 관리 인터페이스를 구성합니다.

```
> configure network ipv6 router
```

명령	설명
configure network ipv6 delete	IPv6 네트워킹을 비활성화합니다.
configure network ipv6 dhcp	DHCP를 통해 IPv6를 구성합니다.

명령	설명
configure network ipv6 manual	IPv6를 수동으로 구성합니다.
show network	관리 인터페이스 구성을 표시합니다.

configure network management-interface

Firepower 4100 또는 9300 Series 디바이스에서 이벤트 및 관리 트래픽을 구분하도록 여러 관리 인터페이스를 구성하려면 **configure network management-interface** 명령을 사용합니다. Firepower Threat Defense의 경우, 여러 관리 인터페이스는 Firepower 4100 및 9300 Series 디바이스에서만 사용할 수 있습니다.

configure network management-interface {**disable** | **disable-event-channel** | **disable-management-channel** | **enable** | **enable-event-channel** | **enable-management-channel**} *ethn*

configure network management-interface tcpport *number*

disable	이벤트 및 관리 트래픽 모두에 대해 지정된 관리 인터페이스를 비활성화합니다.
disable-event-channel	지정된 인터페이스에서 이벤트 채널을 비활성화합니다.
disable-management-channel	지정된 인터페이스에서 관리 채널을 비활성화합니다.
enable	이벤트 및 관리 트래픽 모두에 대해 지정된 관리 인터페이스를 활성화합니다.
enable-event-channel	지정된 인터페이스에서 이벤트 채널을 활성화합니다.
enable-management-channel	지정된 인터페이스에서 관리 채널을 활성화합니다.
ethn	사용자가 비활성화하려는 관리 인터페이스의 수(예: eth0 또는 eth1)를 지정합니다.
tcpport*number*	Firepower Management Center와의 통신에 사용되는 TCP 포트를 구성합니다. 기본값은 8305입니다. 기본값을 변경할 경우 SSH(22) 또는 HTTPS(443) 포트를 지정하지 마십시오. 1024 이상(최대 65535)인 높은 범위의 숫자를 유지합니다.

시스템 기본값은 이벤트 및 관리 트래픽 모두에 사용되는 단일 관리 인터페이스를 갖는 것입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

Firepower 4100 및 9300 Series 디바이스와 물리적 및 가상 FirePOWER Management Center 모두에서 기본 컨피그레이션을 변경하여 Firepower Management Center, 디바이스 또는 둘 다에서 관리 인터페이스를 활성화함으로써 어플라이언스 간의 트래픽을 2개의 개별 트래픽 채널로 분류할 수 있습니다. 관리 트래픽 채널은 모든 내부 트래픽(예: 어플라이언스 및 시스템의 관리에 한정된 디바이스 간 트래픽)을 전달하고, 이벤트 트래픽 채널은 모든 이벤트 트래픽(예: 웹 이벤트)을 전달합니다. 트래픽을 두 채널로 나누면 어플라이언스 간 두 연결 지점이 생성되어 처리량이 많아지고 그에 따라 성능이 개선됩니다. 또한 각각 고유한 IP 주소(IPv4 또는 IPv6)와 호스트 이름이 있는 여러 관리 인터페이스를 활성화하면 트래픽 채널을 분리하여 관리하면서 더 많은 처리량을 제공할 수 있습니다.

여러 관리 인터페이스를 활성화하고 이 인터페이스 간에 이벤트와 관리 트래픽을 분할하려면 **configure network management-interface** 명령을 사용합니다. 이 인터페이스의 주소를 구성하려면 **configure network** {**ipv4** | **ipv6**} **manual** 명령을 사용합니다.

또한 디바이스 및 관리자가 올바르게 통신할 수 있도록 Firepower Management Center에서 이 컨피그레이션을 미러링해야 합니다.

다음 예에서는 eth1을 이벤트 채널로 구성합니다.

```
> configure network management-interface enable-event-channel eth1
>
```

다음 예에서는 eth1을 이벤트 채널로 비활성화합니다.

```
> configure network management-interface disable-event-channel eth1
>
```

다음 예에서는 Firepower Management Center와의 통신에 사용되는 포트를 변경합니다.

```
> configure network management-interface tcpport 8306
Management port changed to 8306.
```

명령	설명
configure network static-routes ipv4/ipv6	관리 인터페이스에 대한 고정 경로를 구성합니다.
show network	관리 인터페이스 컨피그레이션을 표시합니다.

configure network management-port

Firepower Management Center와의 통신에 사용되는 TCP 포트를 구성하려면 **configure network management-port** 명령을 사용합니다.

configure network management-port *number*

입력	Firepower Management Center와의 통신에 사용되는 TCP 포트를 구성합니다. 기본값은 8305입니다. 기본값을 변경할 경우 SSH(22) 또는 HTTPS(443) 포트를 지정하지 마십시오. 1024 이상(최대 65535)인 높은 범위의 숫자를 유지합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

Firepower Management Center와의 관리 연결에 사용되는 포트를 변경하려면 이 명령을 사용합니다. 이 명령은 로컬 관리자, Firepower Device Manager에 사용되는 포트를 변경하지 않습니다. 이 명령은 **configure network management-interface tcpport** 명령과 동일하므로 두 가지 명령을 모두 사용할 필요는 없습니다.

다음 예에서는 Firepower Management Center와의 통신에 사용되는 포트를 변경합니다.

```
> configure network management-port 8306
Management port changed to 8306.
```

명령	설명
configure network ipv4	관리 인터페이스에 대한 IPv4 주소 지정을 구성합니다.
configure network ipv6	관리 인터페이스에 대한 IPv6 주소 지정을 구성합니다.
show network	관리 인터페이스 구성을 표시합니다.

configure network static-routes

여러 관리 인터페이스를 사용할 때 관리 주소의 고정 경로를 추가하거나 제거하려면 **configure network static-routes** 명령을 사용합니다.

configure network static-routes {**ipv4** | **ipv6**} {**add** *interface destination netmask_or_prefix gateway* | **delete**}

add	관리 인터페이스의 고정 경로를 추가합니다.
삭제	관리 인터페이스의 고정 경로를 제거합니다. 삭제할 경로를 선택하라는 메시지가 표시됩니다.
interface	관리 인터페이스의 ID입니다(예: eth0 또는 eth1).
ipv4	IPv4 관리 주소의 고정 경로를 추가하거나 삭제합니다.
ipv6	IPv6 관리 주소의 고정 경로를 추가하거나 삭제합니다.
destination	적절한 IPv4 또는 IPv6 형식으로 추가 또는 제거할 대상 IP 주소입니다. 예를 들어 10.100.10.10 또는 2001:db8::201입니다.
netmask_or_prefix	IPv4의 네트워크 주소 마스크 또는 IPv6의 접두사입니다. IPv4 넷마스크는 점으로 구분된 10진수입니다(예: 255.255.255.0). IPv6 접두사는 표준 접두사 번호입니다(예: 96).
gateway	적절한 IPv4 또는 IPv6 형식으로 추가 또는 제거할 게이트웨이 주소입니다.

릴리스	수정 사항
6.0.1	이 명령이 도입되었습니다.

사용 가이드라인

configure network management-interface 명령을 사용하여 여러 관리 인터페이스를 구성한 경우, 해당 인터페이스의 추가 고정 경로를 구성해야 할 수 있습니다. 이 경로는 through-the-box 트래픽(데이터 인터페이스에서의 트래픽)에는 영향을 주지 않습니다. 고정 경로가 없는 경우 모든 관리 트래픽은

관리 주소에 정의된 기본 게이트웨이를 사용합니다. 단일한 관리 인터페이스를 사용할 경우 일반적으로 고정 경로가 필요하지 않습니다.

다음 예에서는 관리 인터페이스 **eth1**에 대해 IPv4 고정 경로를 추가합니다. 이때 **10.115.24.0**의 대상 주소, **255.255.255.0**의 네트워크 주소 마스크 및 **10.115.9.2**의 게이트웨이 주소를 사용합니다.

```
> configure network static-routes ipv4 add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

다음 예에서는 관리 인터페이스 **eth1**에 대해 IPv6 고정 경로를 추가합니다. 이때 **2001:db8::201**의 대상 주소, **64**의 IPv6 접두사 길이 및 **2001:db8::3657**의 게이트웨이 주소를 사용합니다.

```
> configure network static-routes ipv6 add eth1 2001:db8::201 64 2001:db8::3657
```

다음 예는 고정 경로 삭제 방법을 보여줍니다.

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                 : br1
Destination               : 10.1.1.0
Gateway                   : 192.168.0.254
Netmask                   : 255.255.255.0
> configure network static-routes ipv4 delete
Please select which IPv4 Static Route to delete:
1) br1:   dest 10.1.1.0          nmask 255.255.255.0     gw 192.168.0.254
Please enter number of route to delete: 1
Interface:    br1
Destination:  1.1.1.0
Netmask:      255.255.255.0
Gateway:      192.168.0.254
Are you sure that you want to delete this route?  (y/n) [n]: y
Configuration updated successfully
> show network-static-routes
No static routes currently configured.
```

명령	설명
configure network management-interface	여러 관리 인터페이스를 구성합니다.
configure network static-routes ipv4	관리 인터페이스에 대한 IPv4 고정 경로를 추가하거나 제거합니다.
show network-static-routes	관리 인터페이스에 대해 구성된 고정 경로를 표시합니다.

configure password

사용자가 현재 로그인한 사용자 계정의 비밀번호를 변경하려면 **configure password** 명령을 사용합니다.

configure password

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령을 사용하면 현재 사용자가 CLI에서 비밀번호를 변경할 수 있습니다. 이 명령을 실행하면 현재(또는 이전) 비밀번호를 입력하라는 CLI 프롬프트가 표시된 다음 새 비밀번호를 두 번 입력하라는 프롬프트가 표시됩니다.

다음 예에서는 현재 사용자 계정의 비밀번호를 변경합니다.

```
> configure password
Enter current password: oldpassword
Enter new password: newpassword
Confirm new password: newpassword
```

명령	설명
configure user add	CLI 액세스를 위한 사용자 계정을 추가합니다.

configure ssh-access-list

지정된 IP 주소에서 SSH 연결을 허용하도록 디바이스를 구성하려면 **configure ssh-access-list** 명령을 사용합니다.

configure ssh-access-list *address_list*

address_list	IPv4 CIDR(Classless Inter-Domain Routing) 표기법 또는 IPv6 접두사 길이 표기법을 사용하는 호스트 또는 네트워크의 IP 주소를 쉼표로 구분한 목록입니다. 예를 들어, 10.100.10.0/24 또는 2001:DB8::/96입니다. 모든 IPv4 호스트를 지정하려면 0.0.0.0/0을 입력합니다. 모든 IPv6 호스트를 지정하려면 ::/0을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

단일 명령에서 지원되는 모든 호스트 또는 네트워크를 포함해야 합니다. 이 명령에 지정된 주소는 SSH 액세스 목록의 현재 내용을 덮어씁니다.

SSH 액세스를 허용해도 사용자가 로컬 관리자에 로그인하는 것은 허용되지 않습니다. 컨피그레이션 소프트웨어에 대한 액세스 권한은 사용자 이름과 비밀번호를 통해 제어됩니다.

사용자가 CLI에 현재 로그인된 IP 주소를 제외하는 경우, 연결이 끊길 수 있습니다. CLI에 항목을 다시 가져오려면 IP 주소를 변경해야 합니다.

다음 예는 모든 IPv4 또는 IPv6 주소에서 SSH 연결을 수락하도록 디바이스를 구성합니다.

```
> configure ssh-access-list 0.0.0.0/0,::/0
The ssh access list was changed successfully.
> show ssh-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
```

```
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:ssh
```

명령	설명
configure disable-ssh-access	SSH 액세스 목록을 지웁니다.
show ssh-access-list	SSH 액세스 목록을 표시합니다.

configure ssl-protocol

로컬 관리자를 사용할 때 디바이스에 대한 HTTPS 연결에서 사용할 수 있는 SSL 프로토콜 클라이언트를 구성하려면 **configure ssl-protocol** 명령을 사용합니다.

configure ssl-protocol {*protocol_list* | **default**}

기본	기본 SSL 프로토콜 목록 활성화: **TLSv1.1**, **TLSv1.2**.
protocol_list	다음 프로토콜 중 하나를 지정하는 쉼표로 구분된 목록: **TLSv1**, **TLSv1.1**, **TLSv1.2**, **SSLv3**.

기본 설정은 **TLSv1.1**, **TLSv1.2**입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 디바이스에 대한 HTTPS 웹 액세스에 사용할 수 있는 프로토콜 클라이언트를 설정합니다. 이는 로컬 관리자인 Firepower Device Manager에서 사용됩니다. 이 명령은 원격 관리자에서는 사용되지 않습니다.

참고 이 명령을 사용하여 현재 디바이스와의 통신에 사용 중인 프로토콜을 사용 해제하면 연결이 끊어집니다.

다음 예에서는 HTTPS 연결에 대한 모든 SSL 프로토콜을 수락하도록 디바이스를 구성합니다.

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
> configure ssl-protocol TLSv1,TLSv1.1,TLSv1.2,SSLv3
The following ssl protocols are now enabled:  TLSv1 TLSv1.1 TLSv1.2 SSLv3
> show ssl-protocol
```

```
The supported ssl protocols are  TLSv1 TLSv1.1 TLSv1.2 SSLv3
```

명령	설명
show ssl-protocol	현재 구성된 SSL 프로토콜을 표시합니다.

configure tcp-randomization

TCP 시퀀스 번호 임의 설정을 비활성화하려면 **configure tcp-randomization** 명령을 사용합니다.

configure tcp-randomization {**enable** | **disable**}

사용	공격자가 다음 패킷의 시퀀스 번호를 예상하는 것을 방지하기 위해 수신 및 발신 패킷의 TCP 시퀀스 번호를 임의로 변경합니다.
사용하지 않음	수신 및 발신 패킷의 TCP 시퀀스 번호를 변경하지 않습니다.

TCP 시퀀스 번호 임의 설정은 기본값으로 사용 설정되어 있습니다.

릴리스	수정 사항
6.2	이 명령이 도입되었습니다.

사용 가이드라인

각 TCP 연결에는 각각 클라이언트와 서버에서 생성된 두 개의 ISN(초기 시퀀스 번호)이 있습니다. Firepower Threat Defense 디바이스는 인바운드와 아웃바운드 두 방향 모두로 전달되는 TCP SYN의 ISN을 임의로 설정합니다.

보호된 호스트의 ISN을 임의로 설정하면 공격자가 새 연결을 위한 다음 ISN을 예측하지 못하며 잠재적으로 새 세션의 가로채기가 방지됩니다.

필요한 경우 예를 들어 데이터 암호화로 인해 TCP 초기 시퀀스 번호 임의 설정을 사용 해제할 수 있습니다. 예를 들어, 순차적 번호 매기기가 있는 TCP 패킷에 따라 소프트웨어 테스트 툴, 소프트웨어 제품 또는 하드웨어 디바이스를 사용할 수 있습니다. TCP 임의 설정을 변경하면 디바이스의 모든 인터페이스 및 모든 트래픽에 영향을 미칩니다. 특정 인터페이스 또는 트래픽 클래스를 위해 이를 변경할 수 없습니다.

임의 설정 때문에 특정한 문제가 발생하는 경우에만 TCP 시퀀스 번호 임의 설정을 사용 해제해야 합니다.

다음 예는 TCP 시퀀스 번호 임의 설정을 사용 해제합니다.

```
> configure tcp-randomization disable
```

configure user access

기존 사용자에 대한 액세스 권한 레벨을 변경하려면 **configure user access** 명령을 사용합니다.

configure user access *username* {**basic** | **config**}

username	기존 사용자의 이름을 지정합니다.
basic	사용자에게 기본 액세스 권한을 제공합니다. 이 명령은 사용자가 구성 명령을 입력하는 것을 허용하지 않습니다.
config	사용자에게 구성 액세스 권한을 제공합니다. 이 명령은 사용자에게 모든 명령에 대한 전체 관리자 권한을 제공합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

사용자 계정을 생성할 때, 사용자 액세스 권한을 지정합니다. 지정된 사용자의 액세스 레벨을 수정하려면 **configure user access** 명령을 사용합니다. 이 명령은 사용자가 다음에 로그인할 때 적용됩니다.

다음 예에서는 사용자 jdoe의 액세스 권한을 기본으로 변경합니다.

```
> configure user access jdoe basic
```

명령	설명
configure user add	새 사용자를 추가합니다.
show user	사용자 계정 및 액세스 권한을 표시합니다.

configure user add

CLI 액세스를 위해 새 사용자 계정을 생성하려면 **configure user add** 명령을 사용합니다.

configure user add *username* {**basic** | **config**}

username	기존 사용자의 이름을 지정합니다.
basic	사용자에게 기본 액세스 권한을 제공합니다. 이 명령은 사용자가 구성 명령을 입력하는 것을 허용하지 않습니다.
config	사용자에게 구성 액세스 권한을 제공합니다. 이 명령은 사용자에게 모든 명령에 대한 전체 관리자 권한을 제공합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

지정된 이름, 액세스 레벨 및 비밀번호를 가진 새 사용자를 생성하려면 이 명령을 사용합니다. 비밀번호를 입력하라는 프롬프트가 표시됩니다. 기타 모든 계정 속성은 기본 속성을 사용하여 구성됩니다.

다음 예에서는 config 액세스 권한이 있는 joecool이라는 이름의 사용자 계정을 추가합니다. 입력하고 있으므로 비밀번호가 표시되지 않습니다.

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
```

```
joecool          1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

명령	설명
configure user access	사용자 액세스 레벨을 설정합니다.
configure user aging	사용자 비밀번호 사용 기간을 설정합니다.
configure user delete	지정된 사용자를 삭제합니다.
configure user disable	지정된 사용자를 사용하지 않습니다.
configure user enable	지정된 사용자를 사용합니다.
configure user forcereset	지정된 사용자에 대해 강제로 비밀번호를 재설정합니다.
configure user maxfailedlogins	지정된 사용자에 대한 최대 실패 로그인 횟수를 설정합니다.
configure user password	지정된 사용자의 비밀번호를 설정합니다.
configure user strengthcheck	지정된 사용자의 비밀번호에 대해 강도 검사 요건을 설정합니다.
configure user unlock	지정된 사용자의 계정을 잠금 해제합니다.
show user	사용자 계정을 표시합니다.

configure user aging

사용자 비밀번호의 만료일을 설정하려면 **configure user aging** 명령을 사용합니다.

configure user aging *username max_days warn_days*

username	사용자의 이름을 지정합니다.
max_days	비밀번호가 유효한 최대 일수를 지정합니다. 값의 범위는 1에서 9999까지입니다.
warn_days	비밀번호가 만료되기 전에 비밀번호를 변경하도록 사용자에게 제공된 일수를 지정합니다. 값의 범위는 1에서 9999까지이지만 최대 일수 값보다는 작아야 합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 100일 이내에 만료되는 사용자 비밀번호를 설정하고 비밀번호 만료일 30일 이전에 사용자에게 경고를 보내기 시작합니다. show user 출력에서 Exp 및 Warn 열의 숫자를 참고하십시오.

```
> configure user aging jdoe 100 30
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

명령	설명
configure user add	새 사용자를 추가합니다.
configure user forcereset	지정된 사용자에 대해 강제로 비밀번호를 재설정합니다.
configure user password	지정된 사용자의 비밀번호를 설정합니다.
show user	사용자 계정을 표시합니다.

configure user delete

사용자 계정을 삭제하려면 **configure user delete** 명령을 사용합니다.

configure user delete *username*

username	사용자의 이름을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 사용자 계정을 삭제합니다.

```
> configure user delete jdoe
```

명령	설명
configure user add	새 사용자를 추가합니다.
configure user disable	사용자 계정을 삭제하지 않고 비활성화합니다.
show user	사용자 계정을 표시합니다.

configure user disable

삭제하지 않고 사용자 계정을 비활성화하려면 **configure user disable** 명령을 사용합니다.

configure user disable *username*

username	사용자의 이름을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

삭제하지 않고 사용자 계정을 비활성화하려면 이 명령을 사용합니다. 비활성화된 사용자는 로그인할 수 없습니다. 비활성화된 사용자 계정을 다시 활성화하려면 **configure user enable** 명령을 사용합니다.

다음 예에서는 사용자 계정을 비활성화합니다.

```
> configure user disable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
```

명령	설명
configure user add	새 사용자를 추가합니다.
configure user delete	지정된 사용자를 삭제합니다.
configure user enable	지정된 사용자를 활성화합니다.
configure user unlock	지정된 사용자의 계정을 잠금 해제합니다.

명령	설명
show user	사용자 계정을 표시합니다.

configure user enable

이전에 사용 해제한 사용자를 사용하려면 **configure user enable** 명령을 사용합니다.

configure user enable *username*

username	사용자의 이름을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

사용자를 사용하고 로그인을 허용하려면 이 명령을 사용합니다.

다음 예에서는 사용 해제된 사용자 계정을 사용 설정합니다. **show user**의 Enabled(사용함) 열의 변경 내용을 참조하십시오.

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config Disabled    No    100   30  Dis   No   5
> configure user enable jdoe
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
jdoe              1001  Local Config  Enabled    No    100   30  Dis   No   5
```

명령	설명
configure user add	새 사용자를 추가합니다.
configure user disable	지정된 사용자를 사용 해제합니다.
configure user forcereset	지정된 사용자에 대해 강제로 비밀번호를 재설정합니다.
configure user unlock	지정된 사용자의 계정을 잠금 해제합니다.

명령	설명
show user	사용자 계정을 표시합니다.

configure user forcereset

사용자가 다음에 로그인할 때 비밀번호를 변경하게 하려면 **configure user forcereset** 명령을 사용합니다.

configure user forcereset *username*

username	사용자의 이름을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

사용자가 다음에 로그인할 때 비밀번호를 재설정하게 하려면 이 명령을 사용합니다. 사용자가 로그인하여 비밀번호를 변경하면 강도 확인이 자동으로 활성화됩니다.

다음 예에서는 사용자가 다음에 로그인할 때 비밀번호를 재설정하게 합니다.

```
> configure user forcereset jdoe
```

명령	설명
configure user password	지정된 사용자의 비밀번호를 설정합니다.
configure user strengthcheck	지정된 사용자의 비밀번호에 대해 강도 검사 요건을 설정합니다.
show user	사용자 계정을 표시합니다.

configure user maxfailedlogins

사용자에 대해 로그인 실패 최대 횟수를 설정하려면 **configure user maxfailedlogins** 명령을 사용합니다.

configure user maxfailedlogins *username number*

username	사용자의 이름을 지정합니다.
number	로그인 실패 최대 횟수를 1~9999의 범위에서 지정합니다.

기본 동작 또는 값은 없습니다. 그러나, 새 계정을 만들 경우 기본 로그인 실패 최대 횟수는 5입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

계정이 잠기기 전에 지정된 사용자에 대한 연속 로그인 실패 최대 횟수를 설정하려면 이 명령을 사용합니다. 사용자 계정이 잠기게 될 경우, 해당 잠금을 해제하려면 **configure user unlock** 명령을 사용합니다.

다음 예에서는 연속 실패 로그인의 최대 수를 3으로 설정합니다.

```
> configure user maxfailedlogins jdoe 3
```

명령	설명
configure user add	새 사용자를 추가합니다.
configure user password	지정된 사용자의 비밀번호를 설정합니다.

명령	설명
configure user unlock	지정된 사용자의 계정을 잠금 해제합니다.
show user	사용자 계정을 표시합니다.

configure user password

다른 사용자의 계정에서 비밀번호를 설정하려면 **configure user password** 명령을 사용합니다.

configure user password *username*

username	사용자의 이름을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

지정된 사용자 비밀번호를 설정하려면 이 명령을 사용합니다. 사용자의 비밀번호를 입력하라는 프롬프트가 표시됩니다. 고유한 비밀번호를 변경하려면 이 명령 대신 **configure password** 명령을 사용합니다.

다음 예에서는 다른 사용자의 계정에서 비밀번호를 설정합니다. 입력하고 있으므로 비밀번호가 표시되지 않습니다.

```
> configure user password jdoe
Enter new password for user jdoe: newpassword
Confirm new password for user jdoe: newpassword
```

명령	설명
configure password	현재 로그인한 사용자의 비밀번호를 변경합니다.
configure user add	새 사용자를 추가합니다.
configure user aging	사용자 비밀번호 사용 기간을 설정합니다.
configure user forcereset	지정된 사용자에 대해 강제로 비밀번호를 재설정합니다.

명령	설명
configure user maxfailedlogins	지정된 사용자에 대한 최대 로그인 실패 횟수를 설정합니다.
configure user strengthcheck	지정된 사용자의 비밀번호에 대해 강도 검사 요건을 설정합니다.
show user	사용자 계정을 표시합니다.

configure user strengthcheck

사용자의 비밀번호에 대한 강도 요건을 사용하거나 사용하지 않으려면 **configure user strengthcheck** 명령을 사용합니다.

configure user strengthcheck *username* {**enable** | **disable**}

username	사용자의 이름을 지정합니다.
사용	지정된 사용자 비밀번호에 대한 요건을 설정합니다.
사용 해제	지정된 사용자 비밀번호에 대한 요건을 제거합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

강도 검사를 사용하거나 사용 해제하려면 이 명령을 사용합니다. 여기서 비밀번호를 변경할 때 사용자는 특정 비밀번호 기준을 충족해야 합니다. 사용자 비밀번호가 만료되거나 **configure user forcereset** 명령이 사용되면, 사용자가 다음에 로그인할 때 이 요건이 자동으로 사용 설정됩니다.

다음 예에서는 사용자 계정을 확인하는 강도 검사를 사용 설정합니다.

```
> configure user strengthcheck jdoe enable
```

명령	설명
configure user add	새 사용자를 추가합니다.
configure user forcereset	지정된 사용자에 대해 강제로 비밀번호를 재설정합니다.
configure user maxfailedlogins	지정된 사용자에 대한 최대 실패 로그인 횟수를 설정합니다.

명령	설명
configure user password	지정된 사용자의 비밀번호를 설정합니다.
configure user unlock	지정된 사용자의 계정을 잠금 해제합니다.
show user	사용자 계정을 표시합니다.

configure user unlock

로그인 실패 최대 횟수를 초과한 사용자 계정을 잠금 해제하려면 **configure user unlock** 명령을 사용합니다.

configure user unlock *username*

username	사용자의 이름을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 사용자 계정을 잠금 해제합니다.

```
> configure user unlock jdoe
```

명령	설명
configure user add	새 사용자를 추가합니다.
configure user maxfailedlogins	지정된 사용자에 대한 최대 실패 로그인 횟수를 설정합니다.
show user	사용자 계정을 표시합니다.

copy

플래시 메모리로 파일을 복사하거나 플래시 메모리에서 파일을 복사하려면 **copy** 명령을 사용합니다.

copy [**/noverify**] **/noconfirm** {**/pcap capture:/**[*buffer_name*] | *src_url* | **running-config** | **startup-config**} *dest_url*

/noverify	(선택 사항) 개발 키 서명 이미지를 복사할 때 서명 확인을 건너뜁니다.
/noconfirm	(선택 사항) 확인 프롬프트 없이 파일을 복사합니다.
/pcap capture:/ [*buffer_name*]	지정된 버퍼에서 **capture** 명령의 원시 패킷 캡처 덤프를 복사합니다.
running-config	시스템 메모리에 저장된 실행 컨피그레이션을 지정합니다.
startup-config	플래시 메모리에 저장된 시작 컨피그레이션을 지정합니다. 시작 컨피그레이션은 플래시 메모리에 숨겨진 파일입니다.

src-url *dest-url*	소스 파일, 복사 중인 파일, 대상 파일, 복사를 통해 생성 중인 파일을 지정합니다. 2개의 원격 위치 간에 복사할 수 없으므로 소스 파일이 로컬이면 대상 파일은 로컬 또는 원격일 수 있습니다. 소스 파일이 원격인 경우, 대상 파일은 로컬이어야 합니다. 파일 위치에 대해 다음 URL 구문을 사용합니다. • **disk0:/**[[*path/*]*filename*] 또는 **flash:/**[[*path/*]*filename*] — **flash** 및 **disk0** 모두 내부 플래시 메모리를 표시합니다. 두 옵션 중 하나를 사용할 수 있습니다. • **disk***n***:/**[[*path/*]*filename*] — 선택적인 외부 플래시 드라이브를 표시합니다. 이때 *n*은 드라이브 번호를 지정합니다. • **smb:/**[[*path/*]*filename*] — UNIX 서버 로컬 파일 시스템을 표시합니다. 데이터와 교환 정보를 다른 시스템과 함께 패키지로 제공하려면 LAN 관리자 및 유사 네트워크 시스템의 SMB(Server Message Block) 파일-시스템 프로토콜을 사용합니다. • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*]*filename*[**;type=***xx*]] — **type**은 **ap**(ASCII 패시브 모드), **an**(ASCII 일반 모드), **ip**(기본값—바이너리 패시브 모드), **in**(바이너리 일반 모드)과 같은 키워드 중 하나일 수 있습니다. • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]] — **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP(Secure Copy) 서버에 연결합니다. • **system:/**[[*path/*]*filename*] — 시스템 메모리를 나타냅니다. • **tftp://**[[*user*[**:***password*]@]*server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]] — 경로 이름은 공백을 포함할 수 없습니다. **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 TFTP 서버에 연결합니다. • **cluster_trace:** — cluster_trace 파일 시스템을 표시합니다.

릴리스	수정 사항
6.1	이 명령을 도입했습니다.

사용 가이드라인

클러스터 전체 캡처를 수행한 후에는, 마스터 유닛에서 다음 명령을 입력하여 동일한 캡처 파일을 클러스터의 모든 유닛으로부터 TFTP 서버로 동시에 복사할 수 있습니다.

cluster exec copy /noconfirm /pcap capture:*cap_name***tftp://***location*/*path*/*filename***.pcap**

유닛당 하나씩인 여러 PCAP 파일이 TFTP 서버에 복사됩니다. 목적지 캡처 파일 이름에는 유닛 이름이 자동으로 추가됩니다(예: filename_A.pcap, filename_B.pcap 등). 여기서 A와 B는 클러스터 유닛 이름입니다.

참고 파일 이름의 끝에 유닛 이름을 추가하면 다른 목적지 이름이 생성됩니다.

다음 예에서는 설치 로그의 복사본을 만듭니다.

```
> copy /noconfirm flash:/install.log flash:/install.save.log
Copy in progress...CC
INFO: No digital signature found
150498 bytes copied in 0.20 secs
```

다음 예에서는 디스크에서 시스템 실행 영역의 TFTP 서버로 파일을 복사하는 방법을 보여줍니다.

```
> copy /noconfirm disk0:/install.log
tftp://10.7.0.80/install.log
```

다음 예에서는 실행 중인 컨피그레이션을 TFTP 서버로 복사하는 방법을 보여줍니다.

```
> copy /noconfirm running-config tftp://10.7.0.80/firepower/device1.cfg
```

다음 예에서는 개발 키가 서명된 이미지를 검증 없이 복사하는 방법을 보여줍니다.

```
> copy /noverify /noconfirm lfbff.SSA exa_lfbff.SSA
Source filename [lfbff.SSA]?
Destination filename [exa_lfbff.SSA]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
Writing file disk0:/exa_lfbff.SSA...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Digital Signature was not verified
124125968 bytes copied in 61.740 secs (2034851 bytes/sec)
```

명령	설명
write net	실행 중인 컨피그레이션을 TFTP 서버에 복사합니다.

cpu hog granular-detection

짧은 시간에 실시간 과다 사용 탐지를 제공하고 CPU 과다 사용 임계값을 설정하려면 **cpu hog granular-detection** 명령을 사용합니다.

cpu hog granular-detection [**count** *number*] [**threshold** *value*]

count*number*	코드 실행 중단 횟수를 나타냅니다. 값은 1-10000000입니다. 권장되는 기본값은 1000입니다.
threshold*value*	범위는 1~100입니다. 설정되지 않으면 기본값이 사용됩니다. 이는 플랫폼에 따라 달라집니다.

기본 **count**는 1000입니다. 기본 **threshold**는 플랫폼마다 다양합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

cpu hog granular-detection 명령은 현재 코드 실행을 10밀리초마다 중단시키며, 총 중단 횟수가 계수입니다. 중단 시 CPU 과다 사용 여부를 확인합니다. 해당될 경우 로그에 기록합니다. 이 명령은 데이터 경로에서 CPU 과다 사용 탐지의 세분화를 낮춥니다.

각 스케줄러 기반의 과다 사용은 최대 5개의 중단 기반 과다 사용 엔트리와 연결됩니다. 각 엔트리는 최대 3개의 추적을 포함할 수 있습니다. 중단 기반의 과다 사용은 덮어쓸 수 없습니다. 공간이 없을 경우 새 것을 삭제합니다. 스케줄러 기반의 과다 사용은 LRU 정책에 따라 계속 재사용됩니다. 그러면 중단 기반의 과다 사용이 지워집니다.

다음 예에서는 CPU 과다 사용 탐지를 트리거하는 방법을 보여줍니다.

```
> cpu hog granular-detection count 1000 threshold 10
Average time spent on 1000 detections is 10 seconds, and it may take longer
under heavy traffic.
```

```
Please leave time for it to finish and use show process cpu-hog to check results.
```

명령	설명
show processes cpu-hog	CPU를 과다 사용하고 있는 프로세스를 표시합니다.
clear process cpu-hog	CPU를 과다 사용하고 있는 프로세스를 지웁니다.

cpu profile activate

CPU 프로파일링을 시작하려면 **cpu profile activate** 명령을 사용합니다.

cpu profile activate [*n_samples* [**sample-process** *process_name*] [**trigger cpu-usage** *cpu%* [*process_name*]]]

n_samples	*n*개의 샘플을 저장할 메모리를 할당합니다. 유효한 값의 범위는 1~100,000입니다.
sample-process*process_name*	특정 프로세스만 샘플링합니다.
trigger cpu-usage*cpu%*[*process_name*]	전역 5초 CPU 백분율이 더 큰 값인 한 프로파일러가 시작할 수 없게 하고 CPU 백분율이 이 값보다 낮아지면 프로파일러를 중단합니다. 프로세스 이름을 지정한 경우, 트리거로 프로세스의 5초 CPU 백분율을 사용합니다.

n_samples 기본값은 1000입니다.

cpu% 기본값은 0입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

CPU 프로파일러는 어떤 프로세스에서 더 많은 CPU를 사용하고 있는지 확인하는 데 활용할 수 있습니다. CPU 프로파일링에서는 타이머 인터럽트가 실행되었을 때 CPU에서 실행 중이던 프로세스의 주소를 캡처합니다. 이 프로파일링은 CPU 부하에 관계없이 10밀리초마다 수행됩니다. 예를 들어, 5,000개의 샘플을 수집하면 프로파일링이 완료되는 데 정확히 50초가 걸립니다. CPU 프로파일러에서 사용하는 CPU 시간의 양이 상대적으로 적을 경우 샘플 수집에 더 많은 시간이 걸립니다. CPU 프로필 레코드는 별도의 버퍼에서 샘플링됩니다.

show cpu profile 명령과 **cpu profile activate** 명령을 함께 사용하여 수집 가능한 정보 및 TAC에서 CPU 문제 해결에 사용할 수 있는 정보를 표시합니다. **show cpu profile dump** 명령 출력은 16진수 형식입니다.

CPU 프로파일러가 시작 조건이 발생하기를 대기하는 경우 **show cpu profile** 명령은 다음 출력을 표시합니다.

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

다음 예에서는 프로파일러를 사용 설정하여 1000개의 샘플(기본값)을 저장하도록 지시합니다. 다음으로, **show cpu profile** 명령은 프로파일링이 진행 중임을 표시합니다. 잠시 기다리면 다음 **show cpu profile** 명령이 프로파일링이 완료되었음을 표시합니다. 마지막으로, 결과를 가져오려면 **show cpu profile dump** 명령을 사용합니다. 출력을 복사하고 Cisco Technical Support에 제공합니다. 전체 출력을 가져오려면 SSH 세션을 로깅해야 할 수 있습니다.

```
> cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU profiling currently in progress:
    Core 0: 501 out of 1000 samples collected.
    CP: 586 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU Profiling has stopped.
    Core 0 done with 1000 samples
    CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```

명령	설명
show cpu profile	CPU 프로파일링 진행 상황을 표시합니다.
show cpu profile dump	미완료 또는 완료 프로파일링 결과를 표시합니다.

cpu profile dump

텍스트 파일에 CPU 프로파일링 결과를 저장하려면 **cpu profile dump** 명령을 사용합니다.

cpu profile dump *dest_url*

dest_url	• **disk0:**/[[*path/*]*filename*] 또는 **flash:**/[[*path/*]*filename*] — **flash** 및 **disk0** 모두 내부 플래시 메모리를 표시합니다. 두 옵션 중 하나를 사용할 수 있습니다. • **disk***n***:**/[[*path/*]*filename*] — 선택적인 외부 플래시 드라이브를 표시합니다. 이때 *n*은 드라이브 번호를 지정합니다. • **smb:**/[[*path/*]*filename*] — UNIX 서버 로컬 파일 시스템을 표시합니다. 데이터와 교환 정보를 다른 시스템과 함께 패키지로 제공하려면 LAN 매니저 및 유사 네트워크 시스템의 서버 메시지 블록 파일-시스템 프로토콜을 사용합니다. • **ftp://**[[*user*[**:***password*]@] *server*[*:port*]/[*path/*] *filename*[**;type=***xx*]] — **type**은 **ap**(ASCII 패시브 모드), **an**(ASCII 일반 모드), **ip**(기본값—바이너리 패시브 모드), **in**(바이너리 일반 모드)과 같은 키워드 중 하나일 수 있습니다. • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[*:port*]/[*path/*]*filename*] • **scp://**[[*user*[*:password*]@] *server*[*/path*]*/filename*[**;int=***interface_name*]] — **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP(Secure Copy) 서버에 연결합니다. • **tftp://**[[*user*[**:***password*]@]*server*[*:port*] /[*path/*]*filename*[**;int=***interface_name*]] — 경로 이름은 공백을 포함할 수 없습니다. **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 TFTP 서버에 연결합니다. • **cluster:** — 클러스터 파일 시스템을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

CPU profile dump 명령은 16진수 형식으로 지정된 텍스트 파일에 CPU 프로파일러 출력을 씁니다.

다음 예에서는 cpudump.txt라는 파일에 최신 CPU 프로파일 덤프를 저장합니다.

```
> cpu profile dump disk0:/cpudump.txt
```

명령	설명
show cpu profile dump	미완료 또는 완료 프로파일링 결과를 표시합니다.

crashinfo force

디바이스를 강제로 충돌시키려면 **crashinfo force** 명령을 사용합니다.

crashinfo force /noconfirm {**page-fault** | **watchdog** | **process** *process_ID*}

page-fault	(선택 사항) 페이지 결함 때문에 강제로 충돌하게 합니다.
watchdog	watchdogging 때문에 강제로 충돌하게 합니다.
process*process_ID*	process_ID로 지정된 프로세스를 강제로 충돌하게 합니다. 프로세스 ID를 확인하려면 **show kernel process** 명령을 사용합니다.

기본적으로 디바이스는 충돌 정보 파일을 플래시 메모리에 저장합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

crashinfo force 명령을 사용하여 충돌 출력 생성을 테스트할 수 있습니다. 충돌 출력에서는 실제 충돌과 **crashinfo force page-fault** 또는 **crashinfo force watchdog** 명령으로 인한 충돌과 구분할 방법이 없습니다. 후자 역시 실제 충돌이기 때문입니다. 디바이스는 크래시 덤프가 완료되면 다시 로드합니다.

주의: 생산 환경에서는 **crashinfo force** 명령을 사용하지 마십시오. **crashinfo force** 명령은 디바이스에 충돌을 일으키고 강제적으로 다시 로드하게 합니다.

다음 예에서는 강제로 페이지 결함으로 인한 충돌을 일으킵니다.

```
> crashinfo force /noconfirm page-fault
```

명령	설명
clear crashinfo	충돌 정보 파일의 내용을 지웁니다.
crashinfo test	충돌 정보를 플래시 메모리의 파일에 저장하는 디바이스의 기능을 테스트합니다.
show crashinfo	충돌 정보 파일의 내용을 표시합니다.

crashinfo test

디바이스에서 플래시 메모리의 파일에 충돌 정보를 저장하는 기능을 테스트하려면 **crashinfo test** 명령을 사용합니다.

crashinfo test

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

crashinfo test 명령을 입력하더라도 디바이스가 충돌하지 않습니다. 이전의 충돌 정보 파일이 플래시 메모리에 있을 경우 그 파일을 덮어씁니다.

다음 예에서는 충돌 정보 파일 테스트의 출력을 보여줍니다.

```
> crashinfo test
```

명령	설명
clear crashinfo	충돌 정보 파일의 내용을 지웁니다.
crashinfo force	디바이스를 강제로 충돌하게 합니다.
show crashinfo	충돌 정보 파일의 내용을 표시합니다.

crypto ca trustpool export

PKI 신뢰 풀을 구성하는 인증서를 내보내려면 **crypto ca trustpool export** 명령을 사용합니다.

crypto ca trustpool export *filename*

filename	내보낸 신뢰 풀 인증서를 저장할 파일

릴리스	수정 사항
6.1	이 명령을 도입했습니다.

사용 가이드라인

이 명령은 활성 신뢰 풀의 전체 내용을 지정된 파일 경로에 PEM 코딩 형식으로 복사합니다.

```
> crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
>
> more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE
<More>
```

명령	설명
crypto ca trustpool import	PKI 신뢰 풀을 구성하는 인증서를 가져옵니다.
crypto ca trustpool remove	PKI 신뢰 풀에서 단일 인증서를 제거합니다.
show crypto ca trustpool	PKI 신뢰 풀을 표시합니다.

crypto ca trustpool import

PKI 신뢰 풀을 구성하는 인증서를 가져오려면 **crypto ca trustpool import** 명령을 사용합니다.

crypto ca trustpool import [**clean**] **url** *url* **noconfirm** [**signature-required**]

crypto ca trustpool import [**clean**] **default noconfirm**

clean	가져오기 전에 다운로드한 모든 신뢰 풀 인증서를 제거합니다.
default	디바이스의 신뢰받는 기본 CA 목록을 복원합니다.
noconfirm	모든 대화형 프롬프트를 억제합니다.
signature-required	서명된 파일만 허용하도록 지정합니다. **signature-required** 키워드가 포함되었지만 서명이 없거나 검증할 수 없을 경우 가져오기는 실패합니다.
url*url*	가져올 신뢰 풀 파일의 위치를 지정합니다. • **disk0:/**[[*path/*]*filename*] — 내부 플래시 메모리를 표시합니다. • **disk***n***:/**[[*path/*]*filename*] — 선택적인 외부 플래시 드라이브를 표시합니다. 이때 *n*은 드라이브 번호를 지정합니다. • **smb:/**[[*path/*]*filename*] — UNIX 서버 로컬 파일 시스템을 표시합니다. 데이터와 교환 정보를 다른 시스템과 함께 패키지로 제공하려면 LAN 매니저 및 유사 네트워크 시스템의 서버 메시지 블록 파일-시스템 프로토콜을 사용합니다. • **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path*/] *filename*[**;type=***xx*]] — **type**은 **ap**(ASCII 패시브 모드), **an**(ASCII 일반 모드), **ip**(기본값—바이너리 패시브 모드), **in**(바이너리 일반 모드)과 같은 키워드 중 하나일 수 있습니다. • **http**[**s**]**://**[[*user*[**:***password*] **@**]*server*[:*port*]/[*path/*]*filename*] • **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]] — **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 SCP(Secure Copy) 서버에 연결합니다. • **tftp://**[[*user*[**:***password*]@]*server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]] — 경로 이름은 공백을 포함할 수 없습니다. **;int=***interface* 옵션은 경로 조회를 건너뛰고 항상 지정된 인터페이스를 사용하여 TFTP 서버에 연결합니다.

릴리스	수정 사항
6.1	이 명령을 도입했습니다.

사용 가이드라인

이 명령은 신뢰 풀 번들을 cisco.com에서 다운로드할 때 파일에 있는 서명의 유효성을 검사하는 기능을 제공합니다. 다른 소스의 번들 또는 서명을 지원하지 않는 형식의 번들을 다운로드할 때는 유효한 서명이 꼭 필요하지는 않습니다. 사용자는 서명의 상태를 알 수 있으며 번들을 승인하거나 거부하는 옵션이 주어집니다.

다음과 같은 대화형 경고가 나타날 수 있습니다.

- 유효하지 않은 서명의 Cisco 번들 형식
- 타사 번들 형식
- 유효한 서명의 Cisco 번들 형식

참고 다른 방법으로 파일의 적법성을 입증하지 않는 한 파일 서명을 검증할 수 없다면 인증서를 설치하지 마십시오.

다음 예에서는 기본 신뢰 풀을 복원합니다.

```
> crypto ca trustpool import clean default noconfirm
```

명령	설명
crypto ca trustpool export	PKI 신뢰 풀을 구성하는 인증서를 내보냅니다.
crypto ca trustpool remove	PKI 신뢰 풀에서 단일 인증서를 제거합니다.
show crypto ca trustpool	PKI 신뢰 풀을 표시합니다.

crypto ca trustpool remove

PKI 신뢰 풀에서 지정된 단일 인증서를 제거하려면 **crypto ca trustpool remove** 명령을 사용합니다.

crypto ca trustpool remove *cert_fingerprint* [**noconfirm**]

cert_fingerprint	인증서 핑거프린트는 16진수입니다.
noconfirm	모든 대화형 프롬프트를 억제하려면 이 키워드를 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 인증서를 제거합니다.

```
> crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0
```

명령	설명
clear crypto ca trustpool	신뢰 풀에서 모든 인증서를 제거합니다.
crypto ca trustpool export	PKI 신뢰 풀을 구성하는 인증서를 내보냅니다.
crypto ca trustpool import	PKI 신뢰 풀을 구성하는 인증서를 가져옵니다.
show crypto ca trustpool	PKI 신뢰 풀을 표시합니다.

d - r

delete

플래시 메모리에서 파일을 삭제하려면 **delete** 명령을 사용합니다.

delete /noconfirm [**/recursive**] [**/replicate**] [**disk0:** | **disk***n***:** | **flash:**][*path/*]*filename*

/noconfirm	확인 프롬프트를 표시하지 않습니다.
/recursive	(선택 사항) 지정된 파일을 모든 하위 디렉토리에서 반복적으로 삭제합니다.
/replicate	(선택 사항) 지정된 파일을 대기 유닛에서 삭제합니다.
disk0:	(선택 사항) 내부 플래시 메모리를 지정합니다.
disk*n***:**	(선택 사항) 선택적인 외부 플래시 드라이브를 표시합니다. 이때 n은 드라이브 번호를 지정합니다. 이것은 일반적으로 disk1입니다.
filename	삭제할 파일의 이름을 지정합니다.
flash:	(선택 사항) 내부 플래시 메모리를 지정합니다. 이 키워드는 **disk0**과 동일합니다.
path/	(선택 사항) 파일의 경로를 지정합니다.

디렉토리를 지정하지 않으면 현재 작업 디렉토리가 기본적으로 사용됩니다.

릴리스	수정 사항
6.1	이 명령을 도입했습니다.

사용 가이드라인

경로가 지정되지 않을 경우 현재 작업 디렉토리에서 파일이 삭제됩니다. 파일 삭제 시 와일드카드를 사용할 수 있습니다.

다음 예에서는 현재 작업 디렉토리에서 test.cfg라는 파일을 삭제하는 방법을 보여줍니다.

```
> delete /noconfirm test.cfg
```

명령	설명
cd	현재의 작업 디렉토리를 지정한 디렉토리로 변경합니다.
dir	현재 디렉토리에 있는 파일을 나열합니다.
rmdir	파일 또는 디렉토리를 제거합니다.

dir

디렉토리의 내용을 표시하려면 dir 명령을 사용합니다.

dir [**/all**] [**all-filesystems**] [**/recursive**] [**disk0:** | **disk***n***:** | **flash:** | **system:**] [*path*] [*filename*]

/all	(선택 사항) 모든 파일을 표시합니다.
/recursive	(선택 사항) 디렉토리의 내용을 순환하여 표시합니다.
all-filesystems	(선택 사항) 모든 파일 시스템의 파일을 표시합니다.
disk0:	(선택 사항) 내부 플래시 메모리와 그 뒤에 콜론을 지정합니다.
disk*n***:**	(선택 사항) 선택적인 외부 플래시 드라이브를 표시합니다. 이때 *n*은 드라이브 번호를 지정합니다. 이것은 일반적으로 disk1입니다.
flash:	(선택 사항) 기본 플래시 파티션의 디렉토리 내용을 표시합니다.
path	(선택 사항) 특정 경로를 지정합니다.
filename	(선택 사항) 파일의 이름을 지정합니다.
system:	(선택 사항) 파일 시스템의 디렉토리 내용을 표시합니다.

디렉토리를 지정하지 않으면 현재 작업 디렉토리가 기본적으로 사용됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 디렉토리 내용을 표시하는 방법을 보여줍니다.

```
> dir
Directory of disk0:/
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
```

```
60985344 bytes total (60973056 bytes free)
```

명령	설명
cd	현재 작업 디렉토리를 지정된 디렉토리로 변경합니다.
pwd	현재 작업 디렉토리를 표시합니다.
mkdir	디렉토리를 만듭니다.
rmdir	디렉토리를 제거합니다.

dns update

이 명령을 사용하지 마십시오. 이 명령은 Firepower Threat Defense에서 지원하지 않는 기능과 관련이 있습니다.

eject

외부 컴팩트 플래시 디바이스를 안전하게 제거하려면 **eject** 명령을 사용합니다.

eject /noconfirm disk*n*:

disk*n*:	꺼낼 디바이스를 지정합니다.
/noconfirm	디스크를 꺼내고 있는 것을 확인할 필요가 없음을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 디바이스를 물리적으로 제거하기 전에 **eject** 명령을 사용하여 **disk1**을 정상적으로 종료하는 방법을 보여줍니다.

```
> eject /noconfig disk1:
It is now safe to remove disk1:
```

명령	설명
show version	운영 체제 소프트웨어에 대한 정보를 표시합니다.

eotool 명령

Cisco Technical Assistance Center의 지시에 따라 **eotool** 명령만 사용합니다.

erase

파일 시스템을 지우고 다시 포맷하려면 **erase** 명령을 사용합니다. 이 명령은 숨겨진 시스템 파일을 비롯한 모든 파일을 덮어쓰고 파일 시스템을 지운 다음 파일 시스템을 재설치합니다.

⚠

주의 플래시 메모리를 지우면 플래시 메모리에 저장된 라이센싱 정보도 삭제됩니다. 플래시 메모리를 지우기 전에 라이센싱 정보를 저장합니다.

erase /noconfirm [**disk0:** | **disk***n***:** | **flash:**]

disk0:	(선택 사항) 내부 플래시 메모리를 지정합니다.
disk*n***:**	(선택 사항) 외부 컴팩트 플래시 메모리 카드를 지정합니다.
flash:	(선택 사항) 내부 플래시 메모리와 그 뒤에 콜론을 지정합니다. ASA 5500 시리즈에서는 **flash** 키워드의 별칭이 **disk0:**입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

erase 명령은 OxFF 패턴을 사용하여 플래시 메모리의 모든 데이터를 지운 다음 디바이스에 빈 파일 시스템 할당 테이블을 재작성합니다.

(숨겨진 시스템 파일을 제외하고) 표시된 파일을 모두 삭제하려면 **erase** 명령 대신 **delete /recursive** 명령을 입력합니다.

참고 **erase** 명령은 0xFF 패턴이 있는 디스크의 모든 사용자 데이터를 삭제합니다. 이와 달리 **format** 명령은 파일 시스템 제어 구조를 재설정할 뿐입니다. 원시 디스크 읽기 툴을 사용한 경우에도 이 정보를 볼 수 있습니다.

다음 예에서는 파일 시스템을 지우고 다시 포맷합니다.

```
> erase /noconfirm disk0:
```

명령	설명
delete	숨겨진 시스템 파일을 제외하고 표시된 모든 파일을 제거합니다.
format	(숨겨진 시스템 파일을 비롯하여) 모든 파일을 지우고 파일 시스템을 포맷합니다.

exit

CLI에서 종료하려면 **exit** 명령을 사용합니다.

exit

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

일반 CLI에서 **exit** 및 **logout** 명령은 디바이스의 SSH 세션을 닫는 것과 동일한 작업을 수행합니다.

전문가 모드에 있을 때 **exit**를 사용하면 전문가 모드를 벗어나 일반 CLI로 돌아갑니다.

Diagnostic CLI(**system support diagnostic-cli**)에 있을 때 **exit** 명령을 사용하면 Privileged EXEC 모드에서 User EXEC 모드로 다시 이동됩니다.

다음 예에서는 **exit** 명령을 사용하여 CLI에 대한 SSH 연결을 닫는 방법을 보여줍니다.

```
> exit
```

다음 예에서는 **exit** 명령을 사용하여 Diagnostic CLI(프롬프트에서 # 기호로 표시됨)의 Privileged EXEC 모드에서 User EXEC 모드로 다시 이동하는 방법을 보여줍니다. 로그 오프 메시지를 무시할 수 있으며 CLI 세션이 계속 액티브 상태입니다.

```
firepower# exit
Logoff
Type help or '?' for a list of available commands.
firepower>
```

명령	설명
logout	CLI 세션에서 로그 오프합니다.

expert

일부 절차에 필요한 전문가 모드를 시작하려면 **expert** 명령을 사용합니다.

expert

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

문서에 설명되어 있는 절차에 따라 전문가 모드를 시작하도록 알려주는 경우 또는 Cisco Technical Assistance Center에서 사용하도록 알려주는 경우에만 전문가 모드를 사용합니다.

다음 예에서는 전문가 모드를 시작하고 종료하는 방법을 보여줍니다. 전문가 모드 프롬프트는 username@hostname 정보를 보여줍니다.

```
> expert
admin@firepower:~$
admin@firepower:~$ exit
logout
>
```

명령	설명
exit	전문가 모드를 종료합니다.

failover active

스탠바이 디바이스의 상태를 액티브 상태로 전환하려면 **failover active** 명령을 사용합니다. 액티브 디바이스의 상태를 스탠바이 상태로 전환하려면 이 명령의 **no** 형식을 사용합니다.

failover active

no failover active

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

스탠바이 유닛에서 페일오버 스위치를 시작하려면 **failover active** 명령을 사용합니다. 또는 액티브 유닛에서 **no failover active** 명령을 사용하여 페일오버 스위치를 시작합니다. 이 기능을 사용하여 오류 상태의 유닛을 정상화하거나 유지 보수를 위해 액티브 유닛을 오프라인화할 수 있습니다. 스테이트풀 페일오버를 사용하지 않을 경우 모든 액티브 연결이 끊기며, 페일오버가 이루어진 후 클라이언트에서 다시 연결을 설정해야 합니다.

다음 예에서는 스탠바이 유닛을 액티브 상태로 전환합니다.

```
> failover active
```

명령	설명
failover reset	디바이스를 오류 상태에서 스탠바이 상태로 만듭니다.

failover exec

페일오버 쌍의 특정 유닛에서 명령을 실행하려면 **failover exec** 명령을 사용합니다.

failover exec{**active** | **standby** | **mate**} *cmd_string*

active	페일오버 쌍의 액티브 유닛 에서 명령이 실행되도록 지정합니다.
cmd_string	실행할 명령. 지원되는 명령에 대해서는 CLI 도움말을 참조하십시오.
mate	페일오버 피어에서 명령이 실행되도록 지정합니다.
standby	페일오버 쌍의 스탠바이 유닛에서 명령이 실행되도록 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

페일오버 쌍의 특정 유닛에 명령을 보내는 데 **failover exec** 명령을 사용할 수 있습니다.

명령의 출력이 현재 터미널 세션에 표시되므로, **failover exec** 명령을 사용하여 **show** 명령을 피어 유닛에 제공하고 현재 터미널에서 결과를 볼 수 있습니다.

피어 유닛에 명령을 실행하려면 로컬 유닛에 명령을 실행할 충분한 권한이 있어야 합니다.

제한 사항

- *cmd_string* 인수에서 명령 완료 및 상황 도움말이 제공되지 않습니다.
- **debug**(**undebug**) 명령은 **failover exec** 명령과 함께 사용할 수 없습니다.
- 스탠바이 유닛에 오류가 발생한 상태이고 오류의 원인이 서비스 카드 오류인 경우 **failover exec** 명령을 계속 수신할 수 있습니다. 그렇지 않을 경우에는 원격 명령을 실행할 수 없습니다.
- 재귀적 **failover exec** 명령(예: **failover exec mate failover exec mate**명령)은 입력할 수 없습니다.

- 사용자 입력 또는 확인이 필요한 명령에는 **/nonconfirm** 옵션을 사용해야 합니다.

다음 예에서는 페일오버 피어의 페일오버 컨피그레이션을 표시하기 위해 **failover exec** 명령을 사용합니다. 이 명령은 액티브 유닛인 기본 유닛에서 실행되며, 표시되는 정보는 보조 스탠바이 유닛에서 제공합니다.

```
> failover exec mate show running-config failover
failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
```

다음 예에서는 **failover exec** 명령을 사용하여 스탠바이 유닛에 **show interface** 명령을 보냅니다.

```
> failover exec standby show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

```
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
...
```

다음 예에서는 피어 유닛에 잘못된 명령을 보낼 때 반환되는 오류 메시지를 보여줍니다.

```
> failover exec mate bad command
bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

다음 예에서는 페일오버가 비활성화된 상태에서 **failover exec** 명령을 사용할 경우 반환되는 오류 메시지를 보여줍니다.

```
> failover exec mate show failover
ERROR: Cannot execute command on mate because failover is disabled
```

명령	설명
debug fover	페일오버 관련 디버깅 메시지를 표시합니다.
debug xml	**failover exec** 명령에서 사용하는 XML 파서를 위한 디버깅 메시지를 표시합니다.
show failover exec	**failover exec** 명령 모드를 표시합니다.

failover reload-standby

스탠바이 유닛을 강제로 재부팅하려면 **failover reload-standby** 명령을 사용합니다.

failover reload-standby

릴리스	수정 사항
6.1	이 명령을 도입했습니다.

사용 가이드라인

페일오버 유닛이 동기화되지 않을 때 이 명령을 사용합니다. 부팅이 끝나면 스탠바이 유닛이 재시작하고 액티브 유닛과 다시 동기화합니다.

다음 예에서는 스탠바이 유닛을 강제로 재부팅하기 위해 액티브 유닛에서 **failover reload-standby** 명령을 사용하는 방법을 보여줍니다.

```
> failover reload-standby
```

failover reset

오류가 발생한 디바이스를 오류 없는 상태로 복원하려면 **failover reset** 명령을 사용합니다.

failover reset

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

failover reset 명령을 사용하면 오류가 발생한 유닛 을 오류 없는 상태로 변경할 수 있습니다. **failover reset** 명령은 두 유닛 중 어디서도 입력할 수 있으나, 항상 액티브 유닛에서 입력하는 것이 좋습니다. 액티브 유닛에서 **failover reset** 명령을 입력하면 스탠바이 유닛이 "오류 없는 상태"가 됩니다.

show failover 명령을 사용하여 유닛의 페일오버 상태를 표시할 수 있습니다.

다음 예에서는 오류가 발생한 유닛을 오류 없는 상태로 변경하는 방법을 보여줍니다.

```
> failover reset
```

명령	설명
show failover	유닛의 장애 조치 상태에 대한 정보를 표시합니다.

file copy

FTP를 통해 공통 디렉토리에서 원격 호스트로 파일을 전송하려면 **file copy** 명령을 사용합니다.

file copy *host_name user_id path filename_1* [*filename_2 ... filename_n*]

host_name	타겟 원격 호스트의 이름 또는 IP 주소를 지정합니다.
user_id	원격 호스트에서 사용자를 지정합니다.
path	원격 호스트에서 대상 경로를 지정합니다.
filename_1~filename_n	공통 디렉토리에서 전송할 파일의 이름을 지정합니다. 여러 파일 이름이 지정된 경우, 공백으로 구분해야 합니다. 이 인수는 와일드카드를 지원합니다.

이 명령은 시스템이 문제 해결 파일을 쓰는 위치인 공통 디렉토리에 있는 파일만 전송합니다.

릴리스	수정 사항
6.0.1	이 명령이 도입되었습니다.

이 예에서는 공통 디렉토리에 있는 모든 파일을 **/pub** 디렉토리(원격 호스트 **sentinel**에 있으며 사용자 **jdoe**를 통해 액세스됨)로 전송합니다.

```
> file copy sentinel jdoe /pub *
```

명령	설명
file list	공통 디렉토리에 있는 파일을 나열합니다.
file delete	공통 디렉토리에서 파일을 삭제합니다.
file secure-copy	SCP를 통해 공통 디렉토리에 있는 파일을 전송합니다.

file delete

공통 디렉토리에서 파일을 지우려면 **file delete** 명령을 사용합니다.

file delete *filename_1* [*filename_2 ... filename_n*]

filename_1 ~ filename_n	공통 디렉토리에서 삭제할 파일의 이름을 지정합니다. 여러 파일 이름이 지정된 경우, 공백으로 구분해야 합니다. 이 인수는 와일드카드를 지원합니다.

이 명령은 시스템이 문제 해결 파일에 쓰기를 수행하는 장소인 공통 디렉토리에 있는 파일에서만 실행됩니다.

릴리스	수정 사항
6.0.1	이 명령이 도입되었습니다.

이 예에서는 단일 파일을 삭제합니다.

```
> file delete 10.83.170.31-43235986-2363-11e6-b278-aff0a43948fe-troubleshoot.tar.gz
```

명령	설명
file list	공통 디렉토리에 있는 파일을 나열합니다.
file copy	FTP를 통해 공통 디렉토리에 있는 파일을 전송합니다.
file secure-copy	SCP를 통해 공통 디렉토리에 있는 파일을 전송합니다.

file list

공통 디렉토리에 있는 파일을 나열하려면 **file list** 명령을 사용합니다.

file list [*filename_1 ... filename_n*]

filename_1 ~ filename_n	공통 디렉토리에서 나열할 파일의 이름을 지정합니다. 여러 파일 이름이 지정된 경우, 공백으로 구분해야 합니다. 이 인수는 와일드카드를 지원합니다.

릴리스	수정 사항
6.0.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 시스템이 문제 해결 파일을 쓰는 위치인 공통 디렉토리에 있는 파일만 나열합니다. 파일 이름이 지정되지 않은 경우, 공통 디렉토리에 있는 모든 파일이 나열됩니다.

이 예에서는 공통 디렉토리의 내용을 나열합니다.

```
> file list
May 26 17:46        137474048 /core_1464284811_rackham-sfr.cisco.com_diskmanager_11.21145
Jun 27 20:36       1464696832 /core_1467059810_rackham-sfr.cisco.com_lina_6.21293
```

명령	설명
file copy	FTP를 통해 공통 디렉토리에 있는 파일을 전송합니다.
file delete	공통 디렉토리에서 파일을 삭제합니다.
file secure-copy	SCP를 통해 공통 디렉토리에 있는 파일을 전송합니다.

file secure-copy

SCP를 통해 공통 디렉토리에서 원격 호스트로 파일을 전송하려면 **file secure-copy** 명령을 사용합니다.

file secure-copy *host_name user_id path filename_1* [*filename_2 ... filename_n*]

host_name	타겟 원격 호스트의 이름 또는 IP 주소를 지정합니다.
user_id	원격 호스트에서 사용자를 지정합니다.
path	원격 호스트에서 대상 경로를 지정합니다.
filename_1 ~ filename_n	공통 디렉토리에서 전송할 파일의 이름을 지정합니다. 여러 파일 이름이 지정된 경우, 공백으로 구분해야 합니다. 이 인수는 와일드카드를 지원합니다.

이 명령은 시스템이 문제 해결 파일을 쓰는 위치인 공통 디렉토리에 있는 파일만 전송합니다.

릴리스	수정 사항
6.0.1	이 명령이 도입되었습니다.

이 예에서는 공통 디렉토리에 있는 모든 파일을 원격 호스트 **101.123.31.1**에 있으며 사용자 **jdoe**를 통해 액세스할 수 있는 **/tmp** 디렉토리로 전송합니다.

```
> file secure-copy 101.123.31.1 jdoe /tmp *
```

명령	설명
file copy	FTP를 통해 공통 디렉토리에 있는 파일을 전송합니다.
file delete	공통 디렉토리에서 파일을 삭제합니다.

명령	설명
file list	공통 디렉토리에 있는 파일을 나열합니다.

format

모든 파일을 지우고 파일 시스템을 포맷하려면 **format** 명령을 사용합니다.

format /noconfirm {**disk0:** | **disk***n***:** | **flash:**}

disk0:	내부 플래시 메모리를 지정합니다.
disk*n***:**	외부 플래시 메모리 카드를 지정합니다. 여기서 n은 드라이브 번호입니다.
flash:	내부 플래시 메모리와 그 뒤에 콜론을 지정합니다. ASA 5500 시리즈에서는 **flash** 키워드의 별칭이 **disk0**입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이와 달리 **format** 명령은 파일 시스템 제어 구조를 재설정만 합니다. 원시 디스크 읽기 툴을 사용한 경우에도 이 정보를 볼 수 있습니다. 반대로, **erase** 명령은 0xFF 패턴이 있는 디스크의 모든 사용자 데이터를 없앱니다.

format 또는 **erase**를 사용하는 대신 다음과 같이 기타 옵션을 고려합니다.

- (숨겨진 시스템 파일을 제외하고) 표시된 파일을 모두 삭제하려면 **delete /recursive** 명령을 사용합니다.
- 손상된 파일 시스템을 복구하려면 **format** 명령을 입력하기 전에 **fsck** 명령을 사용해보십시오.

주의 **format** 명령은 손상된 플래시 메모리를 정리하기 위해 필요한 경우에만 각별히 주의하여 사용합니다.

이 예에서는 플래시 메모리를 포맷하는 방법을 보여줍니다.

```
> format /noconfirm disk0:
```

명령	설명
delete	사용자에게 표시되는 모든 파일을 제거합니다.
erase	모든 파일을 삭제하고 플래시 메모리를 포맷합니다.
fsck	손상된 파일 시스템을 복구합니다.

fsck

파일 시스템 검사를 수행하고 손상을 복구하려면 **fsck** 명령을 사용합니다.

fsck /noconfirm disk*n*:

disk*n*:	플래시 메모리 드라이브를 지정합니다. 여기서 *n*은 드라이브 번호입니다.
/noconfirm	프롬프트 없이 명령을 실행하도록 지정합니다. 이 키워드는 필수입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

fsck 명령이 검사하고 손상된 파일 시스템의 복구를 시도합니다. 더 영구적인 절차를 시도하기에 앞서 이 명령을 사용합니다.

FSCK 유틸리티에서 (정전, 비정상적인 종료 등으로 인한) 디스크 손상을 해결할 경우 FSCKxxx.REC라는 이름의 복구 파일을 만듭니다. 이 파일은 FSCK가 실행되는 동안 복구되었던 파일의 일부 또는 전체 파일을 포함할 수 있습니다. 드물게 데이터 복구를 위해 이 파일을 검사해야 하는 경우가 있습니다. 일반적으로 이 파일은 필요하지 않으므로 삭제해도 안전합니다.

참고 FSCK 유틸리티는 시작 시 자동으로 실행되므로 직접 **fsck** 명령을 입력하지 않았더라도 복구 파일이 표시될 수 있습니다.

다음 예에서는 플래시 메모리의 파일 시스템을 검사하는 방법을 보여줍니다.

```
> fsck /noconfirm disk0:
```

명령	설명
delete	사용자에게 표시되는 모든 파일을 제거합니다.
erase	모든 파일을 삭제하고 플래시 메모리를 포맷합니다.
format	파일 시스템을 포맷합니다.

help

지정된 명령에 대한 도움말 정보를 표시하려면 **help** 명령을 사용합니다.

help {*command* | **?**}

?	도움말이 사용 가능한 모든 명령을 표시합니다.
command	CLI 도움말을 표시할 명령을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

help 명령은 일부 명령에 대한 도움말 정보를 표시합니다. **help** 명령 다음에 명령 이름을 입력하여 개별 명령의 도움말을 확인할 수 있습니다. 명령 이름을 지정하지 않고 **?**를 대신 입력하는 경우, 도움말이 있는 모든 명령이 나열됩니다.

또한 부분 명령을 입력한 후 ?를 입력하여 도움말을 가져올 수 있습니다. 이 명령은 공통 문자열에서 해당 위치에 있는 유효한 파라미터를 보여줍니다.

다음 예에서는 **traceroute** 명령에 대해 도움말을 표시하는 방법을 보여줍니다.

```
> help traceroute
USAGE:
        traceroute <destination> [source <src_address|src_intf>]
                   [numeric] [timeout <time>] [ttl <min-ttl> <max-ttl>]
                   [probe <probes>] [port <port-value>] [use-icmp]
DESCRIPTION:
traceroute      Print the route packets take to a network host
SYNTAX:
destination     Address or hostname of destination
src_address     Source address used in the outgoing probe packets
src_intf        Interface through which the destination is accessible
numeric         Do not resolve addresses to hostnames
time            The time in seconds to wait for a response to a probe
min-ttl         Minimum time-to-live value used in probe packets
max-ttl         Maximum time-to-live value used in probe packets
probes          The number of probes to send for each TTL value
port-value      Base UDP destination port used in probes
use-icmp        Use ICMP probes instead of UDP probes
```

history

현재 세션에 대한 커맨드 라인 기록을 표시하려면 **history** 명령을 사용합니다.

history *limit*

limit	엔트리 수에 있는 기록 목록의 크기입니다. 크기를 무제한으로 설정하려면 즉, 전체 기록을 보려면 0을 입력합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

또한 위쪽 화살표를 사용하여 과거 명령 전체를 확인할 수 있습니다.

기록 보기는 명령이 입력된 순서에 대한 일련 번호를 포함합니다.

다음 예는 명령 기록을 보여줍니다.

```
> history 0
   48  show environment
   49  show network-static-routes
   50  show network
   51  show running-config
   52  show service-policy
   53  show ntp
   54  show cpu
   55  show memory
   56  history 0
>
```

logging savelog

로그 버퍼를 플래시 메모리에 저장하려면 **logging savelog** 명령을 사용합니다.

logging savelog [*savefile*]

savefile	(선택 사항) 저장된 로그의 파일 이름입니다. 파일 이름을 지정하지 않으면 시스템은 다음과 같은 기본 타임스탬프 형식을 사용하여 로그 파일을 저장합니다. `LOG-YYYY-MM-DD-HHMMSS.TXT` *YYYY*는 연도이고 *MM*은 달이며 *DD*는 날짜입니다. *HHMMSS*는 시간, 분, 초를 나타냅니다.

릴리스	수정 사항
6.1	이 명령이 추가되었습니다.

자용 가이드라인

로그 버퍼를 플래시 메모리에 저장하려면 먼저 버퍼에 대한 로깅을 활성화해야 합니다. 그렇게 하지 않으면 로그 버퍼가 데이터를 플래시 메모리에 저장할 수 없습니다. 디바이스 관리자, Firepower Management Center(원격) 또는 Firepower Device Manager(로컬)를 사용하여 버퍼 로깅을 구성합니다.

참고 **logging savelog** 명령은 버퍼를 지우지 않습니다. 버퍼를 지우려면 **clear logging buffer** 명령을 사용합니다.

다음 예는 파일 이름인 latest-logfile.txt를 사용하여 플래시 메모리에 로그 버퍼를 저장합니다.

```
> logging savelog latest-logfile.txt
```

>

명령	설명
clear logging buffer	포함하고 있는 모든 syslog 메시지의 로그 버퍼를 지웁니다.
copy	파일을 한 위치에서 TFTP 또는 FTP 서버를 비롯한 다른 위치로 복사합니다.
delete	저장된 로그 파일 등의 디스크 파티션에서 파일을 삭제합니다.

logout

CLI에서 종료하려면 **logout** 명령을 사용합니다.

logout

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

logout 명령을 사용하여 디바이스에서 로그아웃하고 CLI 세션을 종료할 수 있습니다. **exit** 명령을 사용할 수도 있습니다.

다음 예는 디바이스에서 로그아웃하는 방법을 보여줍니다.

```
> logout
```

memory delayed-free-poisoner

delayed free-memory poisoner 툴에 대한 파라미터를 설정하려면 **memory delayed-free-poisoner** 명령을 사용합니다. delayed free-memory poisoner 툴을 활성화하려면 **memory delayed-free-poisoner enable** 명령을 사용합니다. delayed free-memory poisoner 툴을 비활성화하려면 이 명령의 **no** 형식을 사용합니다. delayed free-memory poisoner 툴을 사용하면 애플리케이션에서 릴리스된 이후 여유 메모리의 변경 사항을 모니터링할 수 있습니다.

memory delayed-free-poisoner {**enable** | **desired-fragment-count** *frag_count* | **desired-fragment-size** *frag-size* | **threshold** *heap_use_percent* | **validate** | **watchdog-percent** *watchdog_limit*}

no memory delayed-free-poisoner enable

enable	delayed free-memory poisoner 툴에 대한 작업을 시작합니다.
desired-fragment-count*frag_count*	poisoner 큐에 유지할 메모리 조각의 수를 설정합니다. 올바른 값의 범위는 0~8192이며 기본값은 16입니다.
desired-fragment-size*frag-size*	poisoner 큐에 유지할 인접한 여유 메모리 조각의 수를 바이트 단위로 설정합니다. 올바른 값의 범위는 0~268435456이며 기본값은 102400입니다.
threshold*heap_use_percent*	시스템이 poisoner 큐에서 메모리를 해제할 때 사용하는 시스템 메모리의 백분율 임계값을 0~100으로 설정합니다. 기본값은 100입니다.
validate	delayed-free-poisoner 큐에 있는 모든 요소를 강제로 검증합니다.
watchdog-percent*watchdog_limit*	watchdog 제한을 watchdog 임계값(15초)의 백분율로 설정합니다. 값의 범위는 10~100입니다. 기본값은 50입니다.

memory delayed-free-poisoner enable 명령은 기본적으로 비활성화되어 있습니다.

desired-fragment-count 기본값은 16입니다.

desire-fragment-size 기본값은 102400입니다.

watchdog-percent 기본값은 50입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

delayed free-memory poisoner 툴 활성화는 메모리 사용 및 시스템 성능에 큰 영향을 미칩니다. 명령은 Cisco Technical Assistance Center의 감독하에서만 사용해야 합니다. 시스템 사용량이 많은 기간 중에는 운영 환경에서 실행해서는 안 됩니다.

이 툴을 활성화하면 디바이스에서 실행 중인 애플리케이션의 여유 메모리 요청이 FIFO 큐에 기록됩니다. 각 요청이 poisoner의 큐에 기록되므로 더 낮은 수준의 메모리 관리에서 요구되지 않는 각각의 관련 메모리 바이트는 0xcc 값으로 기록됨으로써 "중독(poisoned)"됩니다.

애플리케이션에서 시스템 여유 메모리 풀에 있는 것보다 더 많은 메모리를 요구할 때까지 여유 메모리 요청이 큐에 머물러 있게 됩니다. 추가 메모리가 필요한 경우, poisoner는 큐에서 최소 **desired-fragment-count**의 메모리 버퍼(**desired-fragment-size** 바이트)를 찾고 해당 메모리를 큐에서 가져와 검증합니다. **desired-fragment-size** 및 **desired-fragment-count**의 값을 변경하여 poisoner가 대형 메모리 요청을 충족하는 데 소모하는 시간을 조정할 수 있습니다.

수정되지 않은 메모리는 시스템 여유 메모리 풀로 반환되고, 초기 요청을 한 애플리케이션의 메모리 요청을 poisoner에서 다시 실행합니다. 요청 애플리케이션을 위한 충분한 메모리가 확보될 때까지 이 과정이 반복됩니다.

중독된 메모리가 수정되면 시스템은 강제로 충돌을 일으키고 충돌의 원인을 확인하는 데 사용할 수 있는 진단 출력을 생성합니다.

delayed free poisoner에는 프로세스의 과도한 리소스 사용을 방지하기 위한 watchdog 메커니즘이 포함되어 있습니다. watchdog 임계값은 15초이며 프로세스가 해당 시간 동안 CPU를 포기하지 않고 계속해서 실행할 경우 poisoner는 시스템을 강제로 충돌시킵니다.

watchdog 제한을 설정하여 watchdog 동작을 조정할 수 있으며 이 제한은 15초의 watchdog 임계값의 백분율을 표시하며, 기본값은 50%입니다. 따라서 delayed free poisoner가 활성인 상태에서 기본적으로 프로세스가 CPU를 포기하지 않고 7.5초 동안 계속해서 실행할 경우, 프로세스 일정을 다시 정할 때까지 프로세스에서 보낸 추가 메모리 할당 요청은 실패합니다. watchdog 제한의 값을 변경하여 이 동작을 조정할 수 있습니다.

과도한 메모리 프래그멘테이션을 방지하고 시스템 CPU 로드를 줄이려면 poisoner가 큐에서 시스템 메모리 풀로 메모리를 자동으로 해제할 때 여유 메모리 사용량의 **threshold** 백분율을 설정할 수 있습니다 (기본적으로, poisoner는 시스템 메모리가 모두 소모될 때까지 큐에서 메모리를 해제하지 않음).

delayed free-memory poisoner 툴은 정기적으로 큐의 모든 요소에 대해 자동으로 검증을 수행합니다. **memory delayed-free-poisoner validate** 명령을 사용하여 검증을 수동으로 시작할 수도 있습니다. 요소에 예기치 않은 값이 있으면 시스템은 강제로 충돌을 일으키고 진단 출력을 생성하여 충돌의 원인을 확인합니다. 예기치 않은 값이 없으면 요소들이 큐에 그대로 유지되고 툴에 의해 정상적으로 처리됩니다. **memory delayed-free-poisoner validate** 명령은 큐에 있는 메모리를 시스템 메모리 풀로 반환하지 않습니다.

명령의 **no** 형식을 사용하면, 큐의 요청에서 참조하는 모든 메모리가 검증 없이 여유 메모리 풀로 반환되고 모든 통계 카운터가 지워집니다.

다음 예는 delayed free-memory poisoner 툴을 활성화합니다.

```
> memory delayed-free-poisoner enable
```

다음은 delayed free-memory poisoner 툴에서 잘못된 메모리 재사용을 탐지하는 경우의 샘플 출력입니다.

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.
    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........
An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.
assertion "0" failed: file "delayfree.c", line 191
```

다음 표에서는 출력의 유효한 부분에 관해 설명합니다.

표 ***1:*** 잘못된 메모리 사용 출력 설명

필드	설명
heap region	요청 애플리케이션에서 사용할 수 있는 메모리의 주소 영역 및 영역의 크기입니다. 이 크기는 요청된 크기와 같지 않으며, 메모리 요청이 수행될 때 시스템에서 메모리를 나누는 방법에 따라 더 작을 수 있습니다.
memory address	오류가 탐지된 메모리의 위치입니다.
byte offset	byte offset은 heap region의 시작 부분과 관련이 있으며, 결과가 이 주소에서 시작된 데이터 구조를 유지하는 데 사용된 경우 수정된 필드를 찾는 데 사용될 수 있습니다. 값이 0이거나 heap region 바이트 수보다 큰 경우, 더 낮은 수준의 힙 패키지에 있는 예기치 못한 값이 문제임을 나타낼 수 있습니다.
allocated by/freed by	마지막 malloc/calloc/realloc 및 무료 통화가 메모리의 이 특정 영역과 관련하여 이루어진 명령 주소.

필드	설명
Dumping...	탐지된 결함이 힙 메모리 영역의 시작 부분과 얼마나 가까운가에 따라, 하나 또는 두 개 메모리 영역의 덤프. 시스템 힙 헤더 뒤의 8바이트는 각종 시스템 헤더 값의 해시 및 큐 결합을 유지하기 위해 이 툴에서 사용하는 메모리입니다. 다른 시스템 힙 트레일러가 나타날 때까지 영역에 있는 다른 모든 바이트는 0xcc로 설정해야 합니다.

명령	설명
clear memory delayed-free-poisoner	delayed free-memory poisoner 툴 대기열 및 통계를 지웁니다.
show memory delayed-free-poisoner	지연된 여유 메모리 포이즈너 툴 대기열의 사용량 요약을 표시합니다.

memory caller-address

메모리 문제를 격리하도록 호출 추적 또는 호출자 PC를 위해 프로그램 메모리의 특정 범위를 구성하려면 **memory caller-address** 명령을 사용합니다. 호출자 PC는 원시 메모리 할당을 호출한 프로그램의 주소입니다. 주소 범위를 제거하려면 이 명령의 no 형식을 사용합니다.

memory caller-address *startPC endPC*

no memory caller-address

endPC	메모리 블록의 끝 주소 범위를 지정합니다.
startPC	메모리 블록의 시작 주소 범위를 지정합니다.

메모리 추적을 위해 실제 호출자 PC가 기록됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

특정 메모리 블록으로 메모리 문제를 격리하려면 **memory caller-address** 명령을 사용합니다.

몇몇 경우에는 원시 메모리 할당의 실제 호출자 PC가 프로그램의 여러 곳에서 사용되는 알려진 라이브러리 함수입니다. 프로그램의 개별 장소를 격리하려면 라이브러리 함수의 시작 및 종료 프로그램 주소를 구성하여, 라이브러리 함수 호출자의 프로그램 주소를 기록합니다.

참고 호출자 주소 추적이 활성화되면 디바이스에서 일시적으로 성능이 저하될 수 있습니다.

다음 예는 **memory caller-address** 명령으로 구성된 주소 범위 및 **show memory caller-address** 명령의 실행 결과를 보여줍니다.

```
> memory caller-address 0x00109d5c 0x00109e08
> memory caller-address 0x009b0ef0 0x009b0f14
```

```
> memory caller-address 0x00cf211c 0x00cf4464
> show memory caller-address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

명령	설명
memory profile enable	메모리 사용량(메모리 프로파일링)의 모니터링을 활성화합니다.
memory profile text	프로파일링할 메모리의 텍스트 범위를 구성합니다.
show memory	최대 물리적 메모리와 현재 운영 체제에서 이용 가능한 여유 메모리에 대한 요약 정보를 표시합니다.
show memory binsize	특정 bin 크기에 할당된 청크에 대한 요약 정보를 표시합니다.
show memory profile	디바이스의 메모리 사용량(프로파일링)에 대한 정보를 표시합니다.
show memory caller-address	디바이스에 구성된 주소 범위를 표시합니다.

memory logging

메모리 로깅을 사용 설정하려면 **memory logging** 명령을 사용합니다. 메모리 로깅을 사용 해제하려면 이 명령의 **no** 형식을 사용합니다.

memory logging 1024-4194304 [**wrap** [**size** [**1-2147483647**] | **process** *process-name*]

no memory logging

1024-4194304	메모리 로깅 버퍼의 로깅 항목 수를 지정합니다. 이것은 유일하게 지정이 필요한 인수입니다.
process*process-name*	모니터링할 프로세스를 지정합니다. 참고 Checkheaps 프로세스는 비표준 방식으로 메모리 할당자를 사용하므로 프로세스로는 완전히 무시됩니다.
size 1-2147483647	모니터링할 항목의 크기와 수를 지정합니다.
wrap	래핑 시 버퍼를 저장합니다. 이는 한 번만 저장할 수 있습니다. 여러번 래핑하는 경우, 덮어쓰기될 수 있습니다. 버퍼 래핑 시 이벤트 관리자에게 트리거가 전송되어 데이터 저장을 사용 설정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

메모리 로깅 매개변수를 변경하려면 사용 해제했다가 다시 사용 설정해야 합니다. 로그를 보려면 **show memory logging** 명령을 사용합니다.

다음 예에서는 메모리 로깅을 사용 설정합니다.

```
> memory logging 202980
```

명령	설명
show memory logging	메모리 로깅 결과를 표시합니다.

memory profile enable

메모리 사용(메모리 프로파일링)의 모니터링을 사용 설정하려면 **memory profile enable** 명령을 사용합니다. 메모리 프로파일링을 사용 해제하려면 이 명령의 **no** 형식을 사용합니다.

memory profile enable [**peak** *peak_value*]

no memory profile enable [**peak** *peak_value*]

peak*peak_value*	메모리 사용의 스냅샷이 피크 사용 버퍼에 저장되는 메모리 사용 임계값을 지정합니다. 시스템의 피크 메모리 요구 사항을 결정하기 위해 나중에 이 버퍼의 내용을 분석할 수 있습니다.

메모리 프로파일링은 기본값으로 사용 해제되어 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

메모리 프로파일링을 사용 설정하기 전에 먼저 **memory profile text** 명령을 사용해 프로파일링할 메모리 텍스트 범위를 구성해야 합니다.

일부 메모리는 사용자가 **clear memory profile** 명령을 입력할 때까지 프로파일링 시스템에 의해 보류됩니다. **show memory profile status** 명령의 결과를 확인해보십시오.

참고 디바이스에서는 메모리 프로파일링이 사용 설정된 경우 성능이 일시적으로 저하될 수 있습니다.

다음 예는 메모리 프로파일링을 사용 설정합니다.

```
> memory profile enable
```

명령	설명
memory profile text	프로파일링할 메모리의 텍스트 범위를 구성합니다.
show memory profile	디바이스의 메모리 사용량(프로파일링)에 대한 정보를 표시합니다.

memory profile text

프로파일링할 메모리의 프로그램 텍스트 범위를 구성하려면 **memory profile text** 명령을 사용합니다. 사용 해제하려면 이 명령의 no 형식을 사용합니다.

memory profile text {*startPC endPC* | **all**} *resolution*

no memory profile text {*startPC endPC* | **all**} *resolution*

all	메모리 블록의 전체 텍스트 범위를 지정합니다.
endPC	메모리 블록의 끝 텍스트 범위를 지정합니다.
resolution	소스 텍스트 영역(1-44582263)에 대한 추적의 결정을 설정해야 합니다.
startPC	메모리 블록의 시작 텍스트 범위를 지정합니다.

릴리스	수정 사항
6.1	이 명령이 추가되었습니다.

사용 가이드라인

텍스트 범위가 작은 경우, 확인 정도 "4"가 일반적으로 명령에 대한 호출을 추적합니다. 텍스트 범위가 더 큰 경우, 첫 번째 통과에는 대략적인 확인 정도로 충분할 것입니다. 다음번 패스에서 더 작은 영역의 집합으로 범위를 좁힐 수 있습니다.

memory profile text 명령으로 텍스트 범위를 입력한 후 **memory profile enable** 명령을 입력하여 메모리 프로파일링을 시작해야 합니다. 메모리 프로파일링은 기본값으로 사용이 해제되어 있습니다.

참고 디바이스에서는 메모리 프로파일링을 사용 설정한 경우 성능이 일시적으로 저하될 수 있습니다.

다음 예는 프로파일링할 메모리의 텍스트 범위를 결정 수준 4로 구성하는 방법을 보여줍니다.

```
> memory profile text all 100
```

다음 예는 텍스트 범위의 컨피그레이션 및 메모리 프로파일링의 상태(OFF)를 보여줍니다.

```
> show memory profile status
InUse profiling: OFF
Peak profiling: OFF
Memory used by profile buffers: 0 bytes
Profile:
0x00007efc3e0227a8-0x00007efc40aa1f8e(00000100)
```

참고 메모리 프로파일링을 시작하려면 **memory profile enable** 명령을 입력해야 합니다. 메모리 프로파일링은 기본값으로 사용이 해제되어 있습니다.

명령	설명
clear memory profile	메모리 프로파일링 기능에 의해 보유된 버퍼를 지웁니다.
memory profile enable	메모리 사용의 모니터링(메모리 프로파일링)을 사용합니다.
show memory profile	디바이스의 메모리 사용량(프로파일링)에 대한 정보를 표시합니다.

memory tracking

힙 메모리 요청의 추적을 활성화하려면 **memory tracking** 명령을 사용합니다. 메모리 추적을 비활성화하려면 이 명령의 **no** 형식을 사용합니다.

memory tracking {**enable** | **allocates-by-threshold** *min_allocates* | **bytes-threshold** *min_bytes* | **filter-from-address-pool** *address*}

no memory tracking enable

enable	메모리 추적을 활성화 합니다.
allocates-by-threshold*min_allocates*	발신자의 주소 풀 항목은 최소한 포함되는 이 많은 할당 호출을 수행해야 합니다(0-4294967295).
bytes-threshold*min_bytes*	발신자의 주소 풀 항목은 최소한 포함되는 이 많은 메모리 바이트를 소모해야 합니다(0-4294967295).
filter-from-address-pool*address*	이 주소에서 주소 풀 항목을 제외합니다. 주소를 확인하려면 먼저 추적을 활성화한 다음 show memory tracking address를 사용합니다. "메모리 추적 주소 풀" 목록에서 "할당자" 주소를 찾습니다. 예를 들어, 다음이 표시될 경우 ...allocated by 0x00007efc3f80e508 다음을 사용하여 제외시킬 수 있습니다. **filter-from-address-pool 0x00007efc3f80e508**

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 힙 메모리 요청의 추적을 활성화합니다.

```
> memory tracking enable
```

명령	설명
clear memory tracking	현재 수집된 모든 정보를 지웁니다.
show memory tracking	메모리 추적 결과를 표시합니다.

mkdir

새 디렉토리를 생성하려면 **mkdir** 명령을 사용합니다.

mkdir /noconfirm [**disk0:** | **disk1:** | **flash:**]*path*

/noconfirm	확인 프롬프트를 표시하지 않습니다.
disk0:	(선택 사항) 내부 플래시 메모리와 그 뒤에 콜론을 지정합니다.
disk1:	(선택 사항) 외부 플래시 메모리 카드와 그 뒤에 콜론을 지정합니다.
flash:	(선택 사항) 내부 플래시 메모리와 그 뒤에 콜론을 지정합니다. ASA 5500 Series Adaptive Security 어플라이언스에서 **flash** 키워드의 별칭이 **disk0**입니다.
path	만들 디렉토리의 이름 및 경로입니다.

경로를 지정하지 않으면 디렉토리는 현재의 작업 디렉토리에 생성됩니다.

릴리스	수정 사항
6.1	이 명령이 추가되었습니다.

사용 가이드라인

동일한 이름의 디렉토리가 이미 존재하면 새 디렉토리가 생성되지 않습니다.

다음 예는 "backup"이라는 이름의 새 디렉토리를 만드는 방법을 보여줍니다.

```
> mkdir backup
```

명령	설명
cd	현재의 작업 디렉토리를 지정한 디렉토리로 변경합니다.
dir	디렉토리 내용을 표시합니다.
rmdir	지정한 디렉토리를 제거합니다.
pwd	현재의 작업 디렉토리를 표시합니다.

more

파일의 내용을 표시하려면 **more** 명령을 사용합니다.

more [**/ascii** | **/binary** | **/ebcdic** | **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **tftp:**]*filename*

/ascii	(선택 사항) 이진 모드에서 이진 파일 및 ASCII 파일을 표시합니다.
/binary	(선택 사항) 이진 모드에서 파일을 표시합니다.
/ebcdic	(선택 사항) EBCDIC에서 이진 파일을 표시합니다.
disk0:	(선택 사항) 내부 플래시 메모리의 파일을 표시합니다.
disk1:	(선택 사항) 외부 플래시 메모리 카드의 파일을 표시합니다.
filename	사용할 파일의 이름을 지정합니다.
flash:	(선택 사항) 내부 플래시 메모리와 그 뒤에 콜론을 지정합니다. ASA 5500 Series Adaptive Security 어플라이언스에서 **flash** 키워드의 별칭이 **disk0**입니다.
ftp:	(선택 사항) FTP 서버의 파일을 표시합니다.
http:	(선택 사항) 웹사이트의 파일을 표시합니다.
https:	(선택 사항) 보안 웹사이트의 파일을 표시합니다.
tftp:	(선택 사항) TFTP 서버의 파일을 표시합니다.

ASCII 모드.

릴리스	수정
6.1	이 명령이 추가되었습니다.

자용 가이드라인

system support view-files 명령은 로그 파일 찾기 및 보기를 위한 더 나은 옵션입니다.

다음 예는 "test.cfg"라는 이름의 로컬 파일 내용을 표시하는 방법을 보여줍니다.

```
> more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
```

```
: end
```

명령	설명
cd	지정한 디렉토리로 변경합니다.
pwd	현재의 작업 디렉토리를 표시합니다.
system support view-files	로그 파일의 내용을 찾고 확인합니다.

nslookup

정규화된 도메인 이름의 IP 주소를 조회하거나 역방향 조회를 수행하려면 **nslookup** 명령을 사용합니다.

nslookup {*hostname* | *ip_address*}

hostname	찾고 있는 IP 주소의 호스트의 정규화된 도메인 이름입니다. 예를 들어, www.example.com이 있습니다.
ip_address	찾고 있는 정규화된 도메인 이름의 호스트의 IP 주소입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

정규화된 도메인 이름을 허용하는 일부 명령에서는 해당 이름의 IP 주소를 조회하는 관리 인터페이스에 대해 구성된 DNS 서버를 사용할 수 없습니다. 이 문제가 발생할 경우, IP 주소를 확인하기 위해 **nslookup** 명령을 사용한 다음, 명령에 IP 주소를 사용합니다.

nslookup 명령은 지정된 IP 주소의 정규화된 도메인 이름을 확인하는 데에도 유용합니다.

다음 예에서는 www.cisco.com의 IP 주소를 조회합니다. 초기 서버 및 주소 정보는 DNS 서버(정규화된 도메인 이름일 수 있음), IP 주소 및 포트를 보여줍니다 (이 예에서는 주소가 조작됨). 다음 정보는 입력한 이름의 정식(실제) 호스트 이름 및 IP 주소를 표시합니다.

```
> nslookup www.cisco.com
Server:         10.102.6.247
Address:        10.102.6.247#53

www.cisco.com   canonical name = origin-www.cisco.com.
Name:   origin-www.cisco.com
Address: 173.37.145.84
```

다음 예에서는 IP 주소에 대한 역방향 조회를 수행하고 호스트 이름을 확인하는 방법을 보여줍니다. 초기 정보는 사용된 DNS 서버에 관한 것입니다. 매핑된 호스트 이름은 **name =** 필드를 사용하여 표시됩니다.

```
> nslookup 173.37.145.84
Server:         10.102.6.247
Address:        10.102.6.247#53

84.145.37.173.in-addr.arpa      name = www2.cisco.com.
```

packet-tracer

방화벽 규칙 테스트를 위해 5-튜플을 지정하여 문제 해결을 위한 패킷 추적 기능을 활성화하려면 Privileged EXEC 모드에서 **packet-tracer** 명령을 사용합니다. 명확성을 위해 구문은 ICMP, TCP/UDP 및 IP 패킷 모델링에 대해 별도로 표시됩니다.

packet-tracer input *ifc_name* **icmp** {*sip* | **user** *username*} *type code* [*ident*] {*dip* | **fqdn** *fqdn-string*} [**detailed**] [**xml**]

packet-tracer input *ifc_name* {**tcp** | **udp**} {*sip* | **user** *username*} *sport* {*dip* | **fqdn** *fqdn-string*} *dport* [**detailed**] [**xml**]

packet-tracer input *ifc_name* **rawip** {*sip* | **user** *username*} *protocol* {*dip* | **fqdn** *fqdn-string*} [**detailed**] [**xml**]

code	ICMP 패킷 추적을 위한 ICMP 코드를 지정합니다.
detailed	(선택 사항) 자세한 추적 결과 정보를 제공합니다.
dip	패킷 추적을 위한 IPv4 또는 IPv6 수신 주소를 지정합니다.
dport	TCP/UDP/SCTP 패킷 추적을 위한 대상 포트를 지정합니다.
fqdn*fqdn-string*	호스트의 FQDN(Fully Qualified Domain Name)을 지정합니다. IPv4용 FQDN만 지원합니다. 그러나, 관리 인터페이스에 대해 구성된 DNS 서버가 이 이름을 확인하는 데 사용되지 않으므로, FQDN을 사용하지 못할 수도 있습니다.
icmp	사용할 프로토콜이 ICMP임을 지정합니다.
ident	(선택 사항) ICMP 패킷 추적을 위한 ICMP 식별자를 지정합니다.
inline-tag*tag*	Layer 2 CMD 헤더에 삽입되는 보안 그룹 태그 값을 지정합니다. 유효한 값의 범위는 0 ~ 65533입니다.
input*ifc_name*	패킷을 추적할 소스 인터페이스의 이름을 지정합니다.
protocol	원시 IP 패킷 추적을 위한 프로토콜 번호를 지정합니다(0~255).
rawip	사용할 프로토콜이 원시 IP임을 지정합니다.
sip	패킷 추적을 위한 IPv4 또는 IPv6 소스 주소를 지정합니다.
sport	TCP/UDP/SCTP 패킷 추적을 위한 소스 포트를 지정합니다.
tcp	사용할 프로토콜이 TCP임을 지정합니다.

type	ICMP 패킷 추적을 위한 ICMP 유형을 지정합니다.
udp	사용할 프로토콜이 UDP임을 지정합니다.
user*username*	사용자를 소스 IP 주소로 지정하려는 경우 사용자 ID를 domain\user 형식으로 지정합니다. 사용자에 대해 가장 최근에 매핑된 주소가 있는 경우, 이는 추적에 사용됩니다.
xml	(선택 사항) 추적 결과를 XML 형식으로 표시합니다.

릴리스	수정
6.1	이 명령이 도입되었습니다.

사용 가이드라인

패킷 캡처 외에도, 패킷이 올바르게 작동하는지 확인하기 위해 Firepower Threat Defense 디바이스를 통해 패킷의 수명을 추적할 수 있습니다. **packet-tracer** 명령을 통해 다음을 수행할 수 있습니다.

- 프로덕션 네트워크의 모든 패킷 삭제를 디버깅합니다.
- 컨피그레이션이 예상대로 작동하는지 확인합니다.
- 규칙 추가를 일으킨 CLI 명령줄과 함께 패킷에 적용되는 모든 규칙을 표시합니다.
- 데이터 경로에 있는 패킷 변경의 타임라인을 표시합니다.
- 추적기 패킷을 데이터 경로에 삽입합니다.

packet-tracer 명령은 패킷 및 패킷이 Firepower Threat Defense 디바이스에서 처리되는 방법에 대한 자세한 정보를 제공합니다. 컨피그레이션의 명령으로 인해 패킷이 드롭되지 않은 경우 **packet-tracer** 명령은 원인에 대한 정보를 읽기 쉬운 형식으로 제공합니다. 예를 들어 잘못된 헤더 검증 때문에 패킷이 드롭된 경우 "packet dropped due to bad ip header (reason)" 메시지가 표시됩니다.

다음 예는 10.100.10.10 ~ 10.100.11.11의 HTTP 포트에 대해 TCP 패킷을 추적합니다. 다음 결과는 패킷이 암시적 거부 액세스 규칙에 의해 드롭될 것임을 나타냅니다.

```
> packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11 80
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside
```

```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

명령	설명
capture	추적 패킷을 포함한 패킷 정보를 캡처합니다.
show capture	옵션을 지정하지 않은 경우의 캡처 컨피그레이션을 표시합니다.

perfmon

콘솔에서 성능 정보를 표시하려면 **perfmon** 명령을 사용합니다.

perfmon {**verbose** | **interval***seconds* | **settings**}

verbose	콘솔에 성능 모니터 정보를 표시합니다. 기본값은 정보를 표시하지 않는 것이며 이것은 perfmon 설정에서 "quiet"로 표시되어 있습니다. **perfmon verbose**를 끄려면 진단 CLI에 있어야 합니다.
interval*seconds*	콘솔에서 성능 표시를 새로 고치기까지의 시간(초)을 지정합니다.
settings	간격과 perfmon이 quiet 또는 verbose인지 여부를 표시합니다.

기본 간격은 120초입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

perfmon 명령을 사용하면 디바이스의 성능을 모니터링할 수 있습니다. 정보를 즉시 표시하려면 **show perfmon** 명령을 사용합니다.

콘솔에서 각 간격마다 정보를 표시하려면 **perfmon verbose** 명령을 사용합니다.

콘솔 포트에서 CLI에 실제로 연결된 경우 또는 진단 CLI(**system support diagnostic-cli**)에 있는 경우에만 정보가 자동으로 나타납니다. 다른 포트(관리 인터페이스 포함)에서 CLI에 있는 경우, 자동으로 생성한 정보를 확인하려면 **show console-output** 명령을 사용합니다. 또는 이 명령을 사용하지 않고 간단하게 **show perfmon** 명령을 직접 사용합니다.

Cisco는 진단 CLI에서만 이 명령을 사용하는 것을 권장합니다.

참고 일반 CLI에서는 **verbose**를 끌 수 없습니다. 대신, 진단 CLI에 있는 Privileged EXEC 모드에서 이 명령을 꺼야 합니다. 예 섹션을 참고하십시오.

다음 예는 콘솔에서 성능 모니터 통계를 120초마다 표시하는 방법을 보여줍니다. 출력에서 "Fixup" 통계는 관련된 프로토콜 검사 엔진을 참조합니다.

```
> perfmon verbose
> perfmon settings
interval: 120 (seconds)
verbose
> show console-output
...
Message #109 :
Message #110 : PERFMON STATS:                      Current      Average
Message #111 : Xlates                                 0/s          0/s
Message #112 : Connections                            0/s          0/s
Message #113 : TCP Conns                              0/s          0/s
Message #114 : UDP Conns                              0/s          0/s
Message #115 : URL Access                             0/s          0/s
Message #116 : URL Server Req                         0/s          0/s
Message #117 : TCP Fixup                              0/s          0/s
Message #118 : TCP Intercept Established Conns        0/s          0/s
Message #119 : TCP Intercept Attempts                 0/s          0/s
Message #120 : TCP Embryonic Conns Timeout            0/s          0/s
Message #121 : FTP Fixup                              0/s          0/s
Message #122 : AAA Authen                             0/s          0/s
Message #123 : AAA Author                             0/s          0/s
Message #124 : AAA Account                            0/s          0/s
Message #125 : HTTP Fixup                             0/s          0/s
Message #126 :
...
```

다음 예에서는 verbose 모드를 끄는 방법을 보여줍니다. 진단 CLI에서 수행해야 합니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <Press return, do not enter a password>

firepower# perfmon quiet
firepower# perfmon settings
interval: 120 (seconds)
quiet
firepower# <Press Ctrl+a, d>

Console connection detached.
> perfmon settings
interval: 120 (seconds)
quiet
```

명령	설명
show perfmon	성능 정보를 표시합니다.

pigtail 명령

Cisco Technical Assistance Center의 지시에 따라 **pigtail** 명령만 사용합니다.

로그가 기록될 때 로그를 보려는 경우, **pigtail** 대신 **tail-logs** 명령을 사용합니다.

ping

지정된 인터페이스에서 IP 주소로의 연결을 테스트하려면 **ping** 명령을 사용합니다. 사용 가능한 파라미터는 일반 ICMP 기반 ping, TCP ping과 "시스템" ping에서 서로 다릅니다. 또한, 시스템 ping은 관리 인터페이스에서 오는 반면, 기타 ping 유형은 데이터 인터페이스를 통해 이동합니다. 테스트에 올바른 유형의 ping을 사용하십시오.

ping [**interface** *if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

ping tcp [**interface***if_name*] *host port* [**repeat** *count*] [**timeout** *seconds*] [**source** *host port*]

ping system *host*

data*pattern*	(선택 사항, ICMP 전용) 16진수 형식으로 16비트 데이터 패턴을 지정합니다(범위 0~FFFF). 기본값은 0xabcd입니다.
host	ping할 호스트의 이름 또는 IPv4 주소를 지정합니다. ICMP ping의 경우, IPv6 주소를 지정할 수 있습니다. IPv6는 TCP 또는 시스템 ping에 대해 지원되지 않습니다. Ping이 FQDN(Fully Qualified Domain Name, 정규화된 도메인 이름)(예: www.example.com)을 사용할 수 있는지 여부는 이름을 확인할 DNS 서버의 가용성에 달려 있습니다. 시스템 ping이 관리 인터페이스에 대해 DNS 서버를 사용하지만, 기타 유형의 ping은 관리 DNS 서버를 사용하지 않습니다. **ping**이 호스트 이름을 확인할 수 없는 경우, **nslookup**을 사용하여 이름과 연결된 IP 주소를 판단한 다음 IP 주소를 ping합니다.
interface*if_name*	(선택 사항) ICMP는 호스트가 인터페이스를 통해 액세스 가능한 경우 그 인터페이스 이름입니다. 호스트는 제공되지 않는 경우 IP 주소로 변경되며, 대상 인터페이스를 확인하기 위해 라우팅 테이블을 참조하게 됩니다. TCP의 경우, 소스에서 SYN 패킷을 전송하는 입력 인터페이스입니다.
port	(TCP 전용) ping하는 호스트의 TCP 포트 번호를 지정합니다(1~65535).
repeat*count*	(선택 사항) ping 요청을 반복할 횟수를 지정합니다. 기본값은 5입니다.
size*bytes*	(선택 사항, ICMP 전용) 데이터그램 크기를 바이트 단위로 지정합니다. 기본값은 100입니다.
source*host port*	(선택 사항, TCP 전용) ping을 보낼 특정 IP 주소 및 포트를 지정합니다(무작위 포트에는 port = 0 사용).

system	관리 인터페이스를 통해 호스트를 ping합니다. 데이터 인터페이스를 통해 수행하는 ping과는 달리 시스템 ping에는 기본 횟수가 없습니다. Ctrl+C를 사용하여 중지할 때까지 ping은 계속 실행됩니다.
tcp	(선택 사항) TCP를 통한 연결을 테스트합니다(기본값은 ICMP). TCP ping은 SYN 패킷을 전송하며, 목적지에서 SYN-ACK 패킷을 전송하는 경우 ping에 성공한 것으로 간주합니다. 한 번에 최대 2개의 동시 TCP ping을 실행할 수 있습니다.
timeout*seconds*	(선택 사항) 시간 제한 간격을 초 단위로 지정합니다. 기본값은 2초입니다.
validate	(선택 사항, ICMP 전용) 응답 데이터를 검증합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

ping 명령을 사용하면 디바이스에 연결이 있는지 또는 호스트를 네트워크에서 사용할 수 있는지 확인할 수 있습니다.

일반 ICMP 기반 ping을 사용하는 경우 이러한 패킷을 차단하는 ICMP 규칙이 없는지 확인해야 합니다(ICMP 규칙을 사용하지 않는 경우 모든 ICMP 트래픽이 허용됨).

TCP ping을 사용할 경우, 액세스 정책이 지정된 포트에서 TCP 트래픽을 허용하는지 확인해야 합니다.

디바이스가 **ping** 명령에서 생성된 메시지에 응답하고 이를 수락하도록 하려면 이 컨피그레이션이 필요합니다. **ping** 명령 출력은 응답이 수신되었는지를 보여줍니다. **ping** 명령을 입력한 후 호스트가 응답하지 않으면 다음과 유사한 메시지가 나타납니다.

```
> ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

디바이스가 네트워크에 연결되어 있고 트래픽을 전달하는지 확인하려면 **show interface** 명령을 사용합니다. 지정된 인터페이스 이름의 주소는 ping의 소스 주소로 사용됩니다.

다음 예에서는 데이터 인터페이스를 통해 IP 주소에 액세스 가능한지 여부를 확인하는 방법을 보여줍니다. 인터페이스가 지정되지 않았으므로 주소로 가져오는 방법을 결정하는 데 라우팅 테이블이 사용됩니다.

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

다음 예에서는 데이터 인터페이스를 통해 호스트에 액세스 가능한지 여부를 확인하기 위해 TCP ping을 사용합니다.

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

> ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms
```

다음 예에서는 관리 인터페이스를 통해 www.cisco.com에 액세스 가능한지 여부를 확인하기 위해 시스템 ping을 수행합니다. Ping을 중지하려면 Ctrl+c를 사용해야 합니다(출력에서 ^C로 표시됨).

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

명령	설명
nslookup	호스트 이름 또는 IP 주소에 대해 DNS 조회를 수행합니다.
show interface	인터페이스 컨피그레이션에 대한 정보를 표시합니다.

pmtool 명령

Cisco Technical Assistance Center의 지시에 따라 **pmtool** 명령만 사용합니다.

pwd

현재 작업 디렉토리를 표시하려면 **pwd** 명령을 사용합니다.

pwd

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 현재 작업 디렉토리를 표시하는 방법을 보여줍니다. 디렉토리의 내용을 확인하려면 **dir** 명령을 사용하고 현재 디렉토리로 변경하려면 **cd**를 사용합니다.

```
> pwd
disk0:/
```

명령	설명
cd	현재의 작업 디렉토리를 지정한 디렉토리로 변경합니다.
dir	디렉토리 내용을 표시합니다.
more	파일의 내용을 표시합니다.

reboot

디바이스를 재부팅하려면 **reboot** 명령을 사용합니다.

reboot

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

```
> reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': yes

Broadcast message from root@firepower

The system is going down for reboot NOW!
...
```

redundant-interface

이중화 인터페이스의 어떤 멤버 인터페이스를 액티브 상태로 만들 것인지를 설정하려면 **redundant-interface** 명령을 사용합니다.

redundant-interface redundant *number* **active-member** *physical_interface*

active-member*physical_interface*	액티브 멤버를 설정합니다. GigabitEthernet0/0과 같이 사용 가능한 물리적 인터페이스 이름을 확인하려면 show interface 명령을 사용합니다. 두 멤버 인터페이스 모두 물리적 유형이 같아야 합니다.
redundant*number*	이중화 인터페이스 ID(예: **redundant 1**)를 지정합니다. 숫자는 1-8입니다.

기본적으로, 액티브 인터페이스는 컨피그레이션에 나열된 사용 가능한 첫 번째 멤버 인터페이스입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스 관리자에서 이중 인터페이스를 생성합니다. 이중 인터페이스를 생성할 때 기본 인터페이스를 지정합니다. 런타임 동안에 액티브 인터페이스를 변경하려면 이 명령을 사용합니다.

어떤 인터페이스가 액티브 인터페이스인지 확인하려면 다음 명령을 입력합니다.

show interface redundant*number***detail | grep Member**

예를 들면 다음과 같습니다.

```
> show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

다음 예에서는 redundant1 인터페이스의 액티브 인터페이스를 변경합니다.

```
> show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

```
> redundant-interface redundant 1 active-member gigabitethernet0/2
```

명령	설명
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

rename

파일 또는 디렉토리 이름을 변경하려면 **rename** 명령을 사용합니다.

rename /noconfirm [**disk0:** | **disk1:** | **flash:**] *source-path* [**disk0:** | **disk1:** | **flash:**] *destination-path*

/noconfirm	확인 프롬프트를 표시하지 않습니다.
destination-path	대상 파일, 즉 새 이름의 경로를 지정합니다.
disk0::	(선택 사항) 내부 플래시 메모리를 지정합니다.
disk1::	(선택 사항) 외부 플래시 메모리 카드를 지정합니다.
flash:	(선택 사항) 내부 플래시 메모리를 지정합니다.
source-path	소스 파일의 경로를 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

파일 시스템 전체에서 파일 또는 디렉토리의 이름을 변경할 수 없습니다. 즉, 파일 이름을 변경하여 파일을 이동시킬 수 없습니다. 파일 및 현재 디렉토리를 보려면 **dir** 명령을 사용합니다. 디렉토리를 변경하려면 **cd**를 사용합니다.

다음 예는 파일 이름을 "test"에서 "test1"로 변경하는 방법을 보여줍니다.

```
> rename /noconfirm disk0:test disk0:test1
```

명령	설명
mkdir	새 디렉토리를 만듭니다.

명령	설명
rmdir	디렉토리를 제거합니다.

rmdir

디렉토리를 제거(삭제)하려면 **rmdir** 명령을 사용합니다.

rmdir /noconfirm [**disk0:** | **disk1:** | **flash:**]*path*

/noconfirm	확인 프롬프트를 표시하지 않습니다.
disk0:	(선택 사항) 비이동식 내부 플래시와 그 뒤에 콜론을 지정합니다.
disk1:	(선택 사항) 이동식 외부 플래시 메모리 카드와 그 뒤에 콜론을 지정합니다.
flash:	(선택 사항) 비이동식 내부 플래시 및 그 뒤에 콜론을 지정합니다. ASA 5500 Series Adaptive Security 어플라이언스에서 **flash** 키워드의 별칭이 **disk0**입니다.
path	(선택 사항) 제거할 디렉토리의 절대 또는 상대 경로.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디렉토리는 제거하기 전에 비어 있어야 합니다.

다음 예에서는 "test"라는 이름의 디렉토리를 제거하는 방법을 보여줍니다.

```
> rmdir test
```

명령	설명
dir	디렉토리 내용을 표시합니다.

명령	설명
mkdir	새 디렉토리를 만듭니다.
pwd	현재의 작업 디렉토리를 표시합니다.

II 부

S 명령

sa - show a

sftunnel-status

디바이스와 관리 Firepower Management Center 간의 연결(터널) 상태를 확인하려면 **sftunnel-status** 명령을 사용합니다.

sftunnel-status

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스와 관리 Firepower Management Center 간의 연결 상태를 확인하려면 **sftunnel-status** 명령을 사용합니다. 로컬 관리자인 Firepower Device Manager를 사용 중인 경우 이 명령은 어떠한 정보도 제공하지 않습니다.

상태 정보에는 다음 섹션이 있습니다.

- SFTUNNEL Status — 연결이 설정되었을 때 연결에 사용된 관리 인터페이스에 대한 정보.
- RUN STATUS — IP 주소, 암호화 및 등록 상태 정보.
- PEER INFO — Firepower Management Center와 이 디바이스에 대한 연결 정보. 이 섹션에는 ID, 상태 이벤트, RPC, NTP, IDS, 악성코드 조회, CSM_CCM(디바이스 구성에 사용됨), EStreamer, UE Channel 및 FSTREAM 등의 다양한 서비스를 위해 시스템 간에 전송될 수 있는 여러 메시지 유형에 대한 통계 블록도 포함되어 있습니다.
- RPC 상태.

다음은 **sftunnel-status** 명령의 샘플 출력입니다.

```
> sftunnel-status

SFTUNNEL Start Time: Tue Oct 11 21:44:44 2016
        Both IPv4 and IPv6 connectivity is supported
        Broadcast count = 2
        Reserved SSL connections: 0
        Management Interfaces: 1
        br1 (control events) 10.83.57.37,2001:420:2710:2556:1:0:0:37

**********************

**RUN STATUS****10.83.57.41*************
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelA Connected: Yes, Interface br1
        Cipher used = AES256-GCM-SHA384 (strength:256 bits)
        ChannelB Connected: Yes, Interface br1
```

```
        Registration: Completed.
        IPv4 Connection to peer '10.83.57.41' Start Time: Tue Oct 11 21:46:00 2016

PEER INFO:
        sw_version 6.2.0
        sw_build 2007
        Management Interfaces: 1
        eth0 (control events) 10.83.57.41,2001:420:2710:2556:1:0:0:41
        Peer channel Channel-A is valid  type (CONTROL), using 'br1',
connected to '10.83.57.41' via '10.83.57.37'
        Peer channel Channel-B is valid  type (EVENT), using 'br1',
connected to '10.83.57.41' via '10.83.57.37'

        TOTAL TRANSMITTED MESSAGES <3> for Identity service
        RECEIVED MESSAGES <2> for Identity service
        SEND MESSAGES <1> for Identity service
        HALT REQUEST SEND COUNTER <0> for Identity service
        STORED MESSAGES for Identity service (service 0/peer 0)
        STATE <Process messages> for Identity service
        REQUESTED FOR REMOTE <Process messages> for Identity service
        REQUESTED FROM REMOTE <Process messages> for Identity service

        TOTAL TRANSMITTED MESSAGES <2760> for Health Events service
        RECEIVED MESSAGES <1380> for Health Events service
        SEND MESSAGES <1380> for Health Events service
        HALT REQUEST SEND COUNTER <0> for Health Events service
        STORED MESSAGES for Health service (service 0/peer 0)
        STATE <Process messages> for Health Events service
        REQUESTED FOR REMOTE <Process messages> for Health Events service
        REQUESTED FROM REMOTE <Process messages> for Health Events service

        TOTAL TRANSMITTED MESSAGES <656> for RPC service
        RECEIVED MESSAGES <328> for RPC service
        SEND MESSAGES <328> for RPC service
        HALT REQUEST SEND COUNTER <0> for RPC service
        STORED MESSAGES for RPC service (service 0/peer 0)
        STATE <Process messages> for RPC service
        REQUESTED FOR REMOTE <Process messages> for RPC service
        REQUESTED FROM REMOTE <Process messages> for RPC service

        TOTAL TRANSMITTED MESSAGES <25131> for IP(NTP) service
        RECEIVED MESSAGES <13532> for IP(NTP) service
        SEND MESSAGES <11599> for IP(NTP) service
        HALT REQUEST SEND COUNTER <0> for IP(NTP) service
        STORED MESSAGES for IP(NTP) service (service 0/peer 0)
        STATE <Process messages> for IP(NTP) service
        REQUESTED FOR REMOTE <Process messages> for IP(NTP) service
        REQUESTED FROM REMOTE <Process messages> for IP(NTP) service

        TOTAL TRANSMITTED MESSAGES <2890> for IDS Events service
        RECEIVED MESSAGES <1445> for service IDS Events service
        SEND MESSAGES <1445> for IDS Events service
        HALT REQUEST SEND COUNTER <0> for IDS Events service
        STORED MESSAGES for IDS Events service (service 0/peer 0)
        STATE <Process messages> for IDS Events service
        REQUESTED FOR REMOTE <Process messages> for IDS Events service
        REQUESTED FROM REMOTE <Process messages> for IDS Events service

        TOTAL TRANSMITTED MESSAGES <4> for Malware Lookup Service service
        RECEIVED MESSAGES <1> for Malware Lookup Service) service
        SEND MESSAGES <3> for Malware Lookup Service service
        HALT REQUEST SEND COUNTER <0> for Malware Lookup Service service
        STORED MESSAGES for Malware Lookup Service service (service 0/peer 0)
        STATE <Process messages> for Malware Lookup Service service
        REQUESTED FOR REMOTE <Process messages> for Malware Lookup Service) service
        REQUESTED FROM REMOTE <Process messages> for Malware Lookup Service service

        TOTAL TRANSMITTED MESSAGES <372> for CSM_CCM service
        RECEIVED MESSAGES <186> for CSM_CCM service
        SEND MESSAGES <186> for CSM_CCM service
        HALT REQUEST SEND COUNTER <0> for CSM_CCM service
        STORED MESSAGES for CSM_CCM (service 0/peer 0)
        STATE <Process messages> for CSM_CCM service
```

```
        REQUESTED FOR REMOTE <Process messages> for CSM_CCM service
        REQUESTED FROM REMOTE <Process messages> for CSM_CCM service

        TOTAL TRANSMITTED MESSAGES <2907> for EStreamer Events service
        RECEIVED MESSAGES <1453> for service EStreamer Events service
        SEND MESSAGES <1454> for EStreamer Events service
        HALT REQUEST SEND COUNTER <0> for EStreamer Events service
        STORED MESSAGES for EStreamer Events service (service 0/peer 0)
        STATE <Process messages> for EStreamer Events service
        REQUESTED FOR REMOTE <Process messages> for EStreamer Events service
        REQUESTED FROM REMOTE <Process messages> for EStreamer Events service

        Priority UE Channel 1 service

        TOTAL TRANSMITTED MESSAGES <2930> for UE Channel service
        RECEIVED MESSAGES <11> for UE Channel service
        SEND MESSAGES <2919> for UE Channel service
        HALT REQUEST SEND COUNTER <0> for UE Channel service
        STORED MESSAGES for UE Channel service (service 0/peer 0)
        STATE <Process messages> for UE Channel service
        REQUESTED FOR REMOTE <Process messages> for UE Channel service
        REQUESTED FROM REMOTE <Process messages> for UE Channel service

        Priority UE Channel 0 service

        TOTAL TRANSMITTED MESSAGES <2942> for UE Channel service
        RECEIVED MESSAGES <11> for UE Channel service
        SEND MESSAGES <2931> for UE Channel service
        HALT REQUEST SEND COUNTER <0> for UE Channel service
        STORED MESSAGES for UE Channel service (service 0/peer 0)
        STATE <Process messages> for UE Channel service
        REQUESTED FOR REMOTE <Process messages> for UE Channel service
        REQUESTED FROM REMOTE <Process messages> for UE Channel service

        TOTAL TRANSMITTED MESSAGES <29286> for FSTREAM service
        RECEIVED MESSAGES <14648> for FSTREAM service
        SEND MESSAGES <14638> for FSTREAM service

        Heartbeat Send Time:     Wed Oct 12 21:58:31 2016
        Heartbeat Received Time: Wed Oct 12 21:59:48 2016

**********************

**RPC STATUS****10.83.57.41*************
  'ip' => '10.83.57.41',
  'uuid' => 'c03cb3c2-8fe2-11e6-bce8-8c278d49b0dd',
  'ipv6' => '2001:420:2710:2556:1:0:0:41',
  'name' => '10.83.57.41',
  'active' => '1',
  'uuid_gw' => '',
  'last_changed' => 'Tue Oct 11 19:32:20 2016'

Check routes:
```

명령	설명
configure manager add	원격 관리자인 Firepower Management Center를 추가합니다.

show access-control-config

액세스 제어 정책에 대한 요약 정보를 표시하려면 **show access-control-config** 명령을 사용합니다.

show access-control-config

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 각 액세스 제어 규칙의 특성을 포함하여 액세스 제어 정책의 요약 설명을 제공합니다. 출력에서는 액세스 제어 정책의 이름과 설명, 기본 작업, 보안 인텔리전스 정책 및 액세스 제어 규칙 집합과 각 액세스 제어 규칙에 대한 정보를 보여줍니다. 또한 참조된 SSL의 이름, 네트워크 분석, 침입, 파일 정책, 침입 변수 집합 데이터, 로깅 설정, 기타 고급 설정(정책 레벨 성능, 전처리, 일반 설정 포함) 등을 보여줍니다.

이 정보에는 소스 및 대상 포트 데이터(ICMP 항목의 유형 및 코드 포함)와 같은 정책 관련 연결 정보와 각 액세스 제어 규칙과 일치하는 연결 수(히트 수)가 포함됩니다.

또한 URL 필터링을 위한 인터랙티브 차단 작업 및 차단에 사용되는 HTML을 보여줍니다.

Firepower Device Manager(로컬 관리자)를 사용하는 경우, 지원되지 않는 기능은 기본 설정을 표시하거나 비어 있습니다. Firepower Management Center를 사용하는 경우, 관리자를 사용하여 이 설정을 조정할 수 있습니다. CLI를 사용하여 이 출력에 표시된 규칙 또는 옵션을 구성할 수 없습니다. 관리자를 사용해야 합니다.

다음 예에서는 Firepower Device Manager(로컬 관리자)를 사용하여 관리되는 디바이스의 액세스 제어 컨피그레이션을 보여줍니다.

```
> show access-control-config

===============[ NGFW-Access-Policy ]===============
Description               :
=================[ Default Action ]=================
Default Action            : Block
Logging Configuration
    DC                    : Enabled
    Beginning             : Disabled
    End                   : Disabled
Rule Hits                 : 0
Variable Set              : Default-Set

===[ Security Intelligence - Network Whitelist ]====
===[ Security Intelligence - Network Blacklist ]====
Logging Configuration     : Disabled
    DC                    : Disabled
```

```
=====[ Security Intelligence - URL Whitelist ]======
=====[ Security Intelligence - URL Blacklist ]======
Logging Configuration     : Disabled
    DC                    : Disabled

=======[ Security Intelligence - DNS Policy ]=======
    Name                  : Default DNS Policy

======[ Rule Set: admin_category (Built-in) ]=======

=====[ Rule Set: standard_category (Built-in) ]=====

------------[ Rule: Inside_Inside_Rule ]------------
    Action                : Fast-path

    Source Zones          : inside_zone
    Destination Zones     : inside_zone
    Users
    URLs
    Logging Configuration
      DC                  : Enabled
      Beginning           : Enabled
      End                 : Enabled
      Files               : Disabled
    Safe Search           : No
    Rule Hits             : 0
    Variable Set          : Default-Set

-----------[ Rule: Inside_Outside_Rule ]------------
    Action                : Fast-path

    Source Zones          : inside_zone
    Destination Zones     : outside_zone
    Users
    URLs
    Logging Configuration
      DC                  : Enabled
      Beginning           : Enabled
      End                 : Enabled
      Files               : Disabled
    Safe Search           : No
    Rule Hits             : 0
    Variable Set          : Default-Set

=======[ Rule Set: root_category (Built-in) ]=======

===============[ Advanced Settings ]================
General Settings
  Maximum URL Length                  : 1024
  Interactive Block Bypass Timeout    : 600
  Do not retry URL cache miss lookup  : No
  Inspect Traffic During Apply        : Yes
Network Analysis and Intrusion Policies
  Initial Intrusion Policy            : Balanced Security and Connectivity
  Initial Variable Set                : Default-Set
  Default Network Analysis Policy     : Balanced Security and Connectivity
Files and Malware Settings
  File Type Inspect Limit             : 1460
  Cloud Lookup Timeout                : 2
  Minimum File Capture Size           : 6144
  Maximum File Capture Size           : 1048576
  Min Dynamic Analysis Size           : 15360
  Max Dynamic Analysis Size           : 2097152
  Malware Detection Limit             : 10485760
Transport/Network Layer Preprocessor Settings
  Detection Settings
    Ignore VLAN Tracking Connections  : No
  Maximum Active Responses            : No Maximum
  Minimum Response Seconds            : No Minimum
  Session Termination Log Threshold   : 1048576
Detection Enhancement Settings
  Adaptive Profile                    : Disabled
```

```
Performance Settings
  Event Queue
    Maximum Queued Events             : 5
    Disable Reassembled Content Checks: False
  Performance Statistics
    Sample time (seconds)             : 300
    Minimum number of packets         : 10000
    Summary                           : False
    Log Session/Protocol Distribution : False
  Regular Expression Limits
    Match Recursion Limit             : Default
    Match Limit                       : Default
  Rule Processing Configuration
    Logged Events                     : 5
    Maximum Queued Events             : 8
    Events Ordered By                 : Content Length
Intelligent Application Bypass Settings
    State                                        : Off
Latency-Based Performance Settings
  Packet Handling                     : Disabled

============[ HTTP Block Response HTML ]============
HTTP/1.1 403 Forbidden
Connection: close
Content-Length: 506
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<title>Access Denied</title>
<style type="text/css">body {margin:0;font-family:verdana,sans-serif;} h1 {margin:0;pa
dding:12px 25px;background-color:#343434;color:#ddd} p {margin:12px 25px;} strong {col
or:#E0042D;}</style>
</head>
<body>
<h1>Access Denied</h1>
<p>
<strong>You are attempting to access a forbidden site.</strong><br/><br/>
Consult your system administrator for details.
</p>
</body>
</html>
```

명령	설명
show access-list	ACL(Access Control List)의 내용을 보여줍니다.

show access-list

액세스 목록에 대한 규칙 및 계수기를 표시하려면 **show access-list** 명령을 사용합니다.

show access-list [*id* [*ip_address* | **brief**]]

id	(선택 사항) 보기를 1개의 액세스 목록으로 제한하기 위한 기존 액세스 목록의 이름입니다.
ip_address	(선택 사항) 보기를 이 주소를 지닌 규칙으로 제한하기 위한 소스 IPv4 또는 IPv6 주소입니다.
brief	(선택 사항) 액세스 목록 식별자, 적중 횟수 및 마지막 규칙 적중의 타임스탬프를 모두 16진수 형식으로 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

시스템은 고급 ACL(Access Control List) 항목으로 액세스 제어 정책의 일부 요소를 구조화합니다. 가능한 경우, 레이어 3 조건을 기준으로 트래픽을 차단하는 액세스 제어 규칙은 ACL에서 규칙을 거부합니다. 신뢰 액세스 제어 규칙에 맞춰 조정된 ACL 규칙을 확인할 수도 있습니다.

그러나 규칙 작업이 블록인 경우에도 액세스 제어 규칙에 검사가 필요한 경우, ACL 항목은 실제로 트래픽을 허용합니다. 이 허용되는 트래픽은 검사 엔진(예: snort)에 전달된 다음 최종적으로 원치않는 트래픽을 차단할 수 있습니다.

따라서, **show access-list**와 함께 표시된 낮은 수준의 ACL 규칙과 디바이스에 대한 액세스 제어 정책 간의 일대일 관계는 존재하지 않습니다. 고급 ACL을 사용하여 시스템은 트래픽에서 조기에 의사 결정을 삭제하거나 신뢰할 수 있으므로 검사가 필요하지 않은 연결이 가능한 한 빨리 전달 또는 삭제될 수 있습니다.

ACL은 서비스 정책을 위한 경로 맵과 일치 기준 같은 기타 항목에도 사용될 수 있습니다. 표준 및 확장 ACL은 이 목적을 위해 사용됩니다.

하나의 명령에 액세스 목록 식별자를 입력하여 여러 액세스 목록을 한 번에 표시할 수 있습니다.

액세스 목록 적중 횟수, 식별자 및 타임스탬프 정보를 16진수 형식으로 표시하는 **brief** 키워드를 지정할 수 있습니다. 16진수 형식으로 표시되는 컨피그레이션 식별자는 세 열에 표시되며, syslog 106023 및 106100에서 사용되는 식별자와 동일합니다.

액세스 목록이 최근에 변경된 경우, 이 목록은 출력에서 제외됩니다. 메시지는 변경이 발생한 시기를 표시합니다.

클러스터링 지침

클러스터링을 사용할 때 단일 디바이스에서 트래픽을 받은 경우 클러스터링 디렉터 논리로 인해 나머지 디바이스에서 ACL에 대한 적중 횟수를 계속 표시할 수 있습니다. 이는 예상된 동작입니다. 클라이언트에서 직접 패킷을 받지 않은 디바이스는 소유자 요청에 대해 클러스터 제어 링크를 통해 전달된 패킷을 받을 수 있기 때문에 수신 디바이스로 패킷을 다시 보내기 전에 ACL을 확인할 수 있습니다. 따라서 디바이스에서 트래픽을 전달하지 않은 경우에도 ACL 적중 횟수가 증가합니다.

다음은 **show access-list** 명령의 샘플 출력이며 Firepower Device Manager(로컬 또는 "on box(온박스)" 관리자)를 사용할 때 액세스 제어 정책을 위해 생성된 고급 액세스 목록을 표시합니다. 설명은 ACE(액세스 제어 항목)를 이해하는 데 도움을 주기 위해 시스템에서 생성한 설명입니다. 이 설명은 연결된 규칙의 이름을 제공하며 규칙에서 생성된 ACE가 뒤에 옵니다. 이러한 설명은 아래 예에 강조 표시되어 있습니다.

```
> show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list NGFW_ONBOX_ACL; 50 elements; name hash: 0xf5cc3f88
access-list NGFW_ONBOX_ACL line 1 remark rule-id 268435458: ACCESS POLICY:
NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 2 remark rule-id 268435458: L5 RULE: Inside_Inside_Rule
access-list NGFW_ONBOX_ACL line 3 advanced trust ip ifc inside1_2 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x2c7f5801
access-list NGFW_ONBOX_ACL line 4 advanced trust ip ifc inside1_2 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xf170c15b
access-list NGFW_ONBOX_ACL line 5 advanced trust ip ifc inside1_2 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xce627c77
access-list NGFW_ONBOX_ACL line 6 advanced trust ip ifc inside1_2 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xe37dcdd2
access-list NGFW_ONBOX_ACL line 7 advanced trust ip ifc inside1_2 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x65347856
access-list NGFW_ONBOX_ACL line 8 advanced trust ip ifc inside1_2 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x6d622775
access-list NGFW_ONBOX_ACL line 9 advanced trust ip ifc inside1_3 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xc1579ed7
access-list NGFW_ONBOX_ACL line 10 advanced trust ip ifc inside1_3 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0x40968b8f
access-list NGFW_ONBOX_ACL line 11 advanced trust ip ifc inside1_3 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xc5a178c1
access-list NGFW_ONBOX_ACL line 12 advanced trust ip ifc inside1_3 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xdbc1560f
access-list NGFW_ONBOX_ACL line 13 advanced trust ip ifc inside1_3 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x3571535c
access-list NGFW_ONBOX_ACL line 14 advanced trust ip ifc inside1_3 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xc4a66c0a
access-list NGFW_ONBOX_ACL line 15 advanced trust ip ifc inside1_4 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0x1d1a8032
access-list NGFW_ONBOX_ACL line 16 advanced trust ip ifc inside1_4 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x8f7bbcdf
access-list NGFW_ONBOX_ACL line 17 advanced trust ip ifc inside1_4 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0xe616991f
access-list NGFW_ONBOX_ACL line 18 advanced trust ip ifc inside1_4 any ifc inside1_6 any
```

```
rule-id 268435458 event-log both (hitcnt=0) 0x4db9d2aa
access-list NGFW_ONBOX_ACL line 19 advanced trust ip ifc inside1_4 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0xf8a88db4
access-list NGFW_ONBOX_ACL line 20 advanced trust ip ifc inside1_4 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x1d3b5b80
access-list NGFW_ONBOX_ACL line 21 advanced trust ip ifc inside1_5 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xf508bbd8
access-list NGFW_ONBOX_ACL line 22 advanced trust ip ifc inside1_5 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x7084f3fc
access-list NGFW_ONBOX_ACL line 23 advanced trust ip ifc inside1_5 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xd989f9aa
access-list NGFW_ONBOX_ACL line 24 advanced trust ip ifc inside1_5 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xd5aa77f5
access-list NGFW_ONBOX_ACL line 25 advanced trust ip ifc inside1_5 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4a7648b2
access-list NGFW_ONBOX_ACL line 26 advanced trust ip ifc inside1_5 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x118ef4b4
access-list NGFW_ONBOX_ACL line 27 advanced trust ip ifc inside1_6 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xa6be4e58
access-list NGFW_ONBOX_ACL line 28 advanced trust ip ifc inside1_6 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0xda17cb9e
access-list NGFW_ONBOX_ACL line 29 advanced trust ip ifc inside1_6 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xc6bfe6b7
access-list NGFW_ONBOX_ACL line 30 advanced trust ip ifc inside1_6 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x5fe085c3
access-list NGFW_ONBOX_ACL line 31 advanced trust ip ifc inside1_6 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x4574192b
access-list NGFW_ONBOX_ACL line 32 advanced trust ip ifc inside1_6 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0x36203c1e
access-list NGFW_ONBOX_ACL line 33 advanced trust ip ifc inside1_7 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0x699725ea
access-list NGFW_ONBOX_ACL line 34 advanced trust ip ifc inside1_7 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x36a1e6a1
access-list NGFW_ONBOX_ACL line 35 advanced trust ip ifc inside1_7 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xe415bb76
access-list NGFW_ONBOX_ACL line 36 advanced trust ip ifc inside1_7 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x18ebff70
access-list NGFW_ONBOX_ACL line 37 advanced trust ip ifc inside1_7 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0xf9bfd690
access-list NGFW_ONBOX_ACL line 38 advanced trust ip ifc inside1_7 any ifc inside1_8 any
rule-id 268435458 event-log both (hitcnt=0) 0xf08a88b4
access-list NGFW_ONBOX_ACL line 39 advanced trust ip ifc inside1_8 any ifc inside1_2 any
rule-id 268435458 event-log both (hitcnt=0) 0xd2014e58
access-list NGFW_ONBOX_ACL line 40 advanced trust ip ifc inside1_8 any ifc inside1_3 any
rule-id 268435458 event-log both (hitcnt=0) 0x952c7254
access-list NGFW_ONBOX_ACL line 41 advanced trust ip ifc inside1_8 any ifc inside1_4 any
rule-id 268435458 event-log both (hitcnt=0) 0xfc38a46f
access-list NGFW_ONBOX_ACL line 42 advanced trust ip ifc inside1_8 any ifc inside1_5 any
rule-id 268435458 event-log both (hitcnt=0) 0x3f878e23
access-list NGFW_ONBOX_ACL line 43 advanced trust ip ifc inside1_8 any ifc inside1_6 any
rule-id 268435458 event-log both (hitcnt=0) 0x48e852ce
access-list NGFW_ONBOX_ACL line 44 advanced trust ip ifc inside1_8 any ifc inside1_7 any
rule-id 268435458 event-log both (hitcnt=0) 0x83c65e52
access-list NGFW_ONBOX_ACL line 45 remark rule-id 268435457: ACCESS POLICY:
NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 46 remark rule-id 268435457: L5 RULE: Inside_Outside_Rule
access-list NGFW_ONBOX_ACL line 47 advanced trust ip ifc inside1_2 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xea5bdd6e
access-list NGFW_ONBOX_ACL line 48 advanced trust ip ifc inside1_3 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xd7461ffc
access-list NGFW_ONBOX_ACL line 49 advanced trust ip ifc inside1_4 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0x6e13508e
access-list NGFW_ONBOX_ACL line 50 advanced trust ip ifc inside1_5 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xfe1fcdd6
access-list NGFW_ONBOX_ACL line 51 advanced trust ip ifc inside1_6 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xa4dba9a8
access-list NGFW_ONBOX_ACL line 52 advanced trust ip ifc inside1_7 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0x2cfd43cd
access-list NGFW_ONBOX_ACL line 53 advanced trust ip ifc inside1_8 any ifc outside any
rule-id 268435457 event-log both (hitcnt=0) 0xc3c3fafb
access-list NGFW_ONBOX_ACL line 54 remark rule-id 1: ACCESS POLICY: NGFW_Access_Policy
access-list NGFW_ONBOX_ACL line 55 remark rule-id 1: L5 RULE: DefaultActionRule
access-list NGFW_ONBOX_ACL line 56 advanced deny ip any any rule-id 1 (hitcnt=0)
```

```
0x84953cae
>
```

다음 예에서는 16진수 형식으로 지정된 액세스 정책(적중 횟수가 0이 아닌 ACE)에 대한 간략한 정보를 보여 줍니다. 처음 두 열에는 16진수 형식의 식별자가 표시되고, 세 번째 열에는 적중 횟수가 나열되며, 네 번째 열에는 16진수 형식의 타임스탬프 값이 표시됩니다. 적중 횟수 값은 트래픽에 의해 규칙이 적중된 횟수를 나타냅니다. 타임스탬프 값은 마지막 적중 시간을 보고합니다. 적중 횟수가 0인 경우에는 아무 정보도 표시되지 않습니다.

다음은 텔넷 트래픽이 전달되는 경우 **show access-list brief** 명령의 샘플 출력입니다.

```
> show access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
```

다음은 SSH 트래픽이 전달되는 경우 **show access-list brief** 명령의 샘플 출력입니다.

```
> show access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922 44ae5901 00000001 4a68ab66
```

명령	설명
clear access-list	액세스 목록 카운터를 지웁니다.
show running-config access-list	현재 실행 중인 access-list 구성을 표시합니다.

show app-agent heartbeat

app-agent 상태를 표시하려면 **show app-agent heartbeat** 명령을 사용합니다.

show app-agent heartbeat

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

app-agent heartbeat 통신 채널은 FXOS 섀시 수퍼바이저와 Firepower Threat Defense 애플리케이션 에이전트 간의 링크 상태를 모니터링하는 서비스에 사용됩니다. 이는 Firepower 4100 또는 9300 Series 디바이스에서 하드웨어 바이패스를 구성할 경우 사용됩니다. 이는 Firepower Threat Defense 소프트웨어를 실행하는 기타 디바이스 모델에서 사용되지 않습니다.

app-agent heartbeat 통신 채널에서 상태를 보려면 **show app-agent heartbeat** 명령을 사용합니다.

다음 예에서는 app-agent heartbeat 상태를 보여줍니다.

```
> show app-agent heartbeat
appagent heartbeat timer 1 retry-count 3
```

명령	설명
app-agent	하드웨어 바이패스를 위해 app-agent를 구성합니다.

show arp

ARP 테이블을 보려면 **show arp** 명령을 사용합니다.

show arp

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

화면 출력은 동적, 정적 및 프록시 ARP 항목이 표시됩니다. 동적 ARP 항목은 ARP 항목의 기간(초)을 포함합니다. 정적 ARP 항목은 기간 대신 대시(-)를 포함하며, 프록시 ARP 항목은 "별칭"을 나타냅니다.

ARP 테이블은 시스템 통신에 사용되는 nlp_int_tap 같은 내부 인터페이스용 항목을 포함할 수 있습니다.

다음은 **show arp** 명령의 샘플 출력입니다. 첫 번째 항목은 2초가 지난 동적 항목입니다. 두 번째 항목은 정적 항목이고, 세 번째 항목은 프록시 ARP의 항목입니다.

```
> show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

명령	설명
clear arp statistics	ARP 통계를 지웁니다.
show arp statistics	ARP 통계를 표시합니다.
show running-config all arp	ARP의 현재 시간 제한 구성을 표시합니다.

show arp-inspection

각 인터페이스에 대한 ARP 검사 설정을 보려면 **show arp-inspection** 명령을 사용합니다.

show arp-inspection

릴리스	수정 사항
6.1	이 명령이 추가되었습니다.
6.2	라우팅된 모드 지원이 추가되었습니다.

다음은 **show arp-inspection** 명령의 샘플 출력입니다.

```
> show arp-inspection
interface                arp-inspection         miss
-------------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

miss 열은 ARP 검사가 활성화된 경우 일치하지 않는 패킷에 대해 수행할 기본 작업(“flood” 또는 “no-flood”)을 표시합니다.

명령	설명
clear arp statistics	ARP 통계를 지웁니다.
show arp statistics	ARP 통계를 표시합니다.
show running-config all arp	ARP의 현재 시간 제한 컨피그레이션을 표시합니다.

show arp statistics

ARP 통계를 보려면 **show arp statistics** 명령을 사용합니다.

show arp statistics

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show arp statistics** 명령의 샘플 출력입니다.

```
> show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

다음 표는 각 필드에 관해 설명합니다.

표 ***2: show arp statistics*** 필드*(*계속*)*

필드	설명
Number of ARP entries	ARP 테이블 항목의 총 개수입니다.
Dropped blocks in ARP	IP 주소를 해당 하드웨어 주소에 대해 확인하는 동안 삭제된 블록 수입니다.
Maximum queued blocks	IP 주소를 확인할 때까지 기다리는 동안 ARP 모듈에서 대기 중이었던 최대 블록 수입니다.
Queued blocks	ARP 모듈에서 현재 대기 중인 블록 수입니다.
Interface collision ARPs received	인터페이스와 동일한 IP 주소에서 모든 인터페이스에 수신된 ARP 패킷 수입니다.
ARP-defense gratuitous ARPs sent	ARP-Defense 메커니즘의 일부로 디바이스에서 보낸 여분의 ARP 수입니다.

필드	설명
Total ARP retries	첫 번째 ARP 요청에 대한 응답에서 주소가 확인되지 않은 경우 ARP 모듈에서 보낸 총 ARP 요청 수입니다.
Unresolved hosts	ARP 모듈에서 ARP 요청을 여전히 전송 중인 확인되지 않은 호스트의 개수입니다.
Maximum unresolved hosts	마지막으로 지워졌거나 디바이스가 부팅한 이후에 ARP 모듈에 있던 확인되지 않은 호스트의 최대 개수입니다.

명령	설명
clear arp statistics	ARP 통계를 지웁니다.
show arp	ARP 테이블을 표시합니다.
show running-config all arp	ARP의 현재 시간 제한 구성을 표시합니다.

show as-path-access-list

모든 현재 AS(autonomous system) 경로 액세스 목록의 내용을 표시하려면 **show as-path-access-list** 명령을 사용합니다.

show as-path-access-list [*number*]

number	(선택 사항) AS 경로 액세스 목록 번호를 지정합니다. 유효한 값은 1~500입니다.

number 인수를 지정하지 않으면 모든 AS 경로 액세스 목록에 대한 명령 출력이 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show as-path-access-list** 명령의 샘플 출력입니다.

```
> show as-path-access-list
 AS path access list 1

 AS path access list 2
```

show asp cluster counter

클러스터링 환경에서 전역 또는 상황별 정보를 디버깅하려면 **show asp cluster counter** 명령을 사용합니다.

show asp cluster counter

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp cluster counter 명령은 문제 해결에 도움이 될 수 있는 전역 및 상황별 DP 카운터를 표시합니다. 이 정보는 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

다음은 **show asp cluster counter** 명령의 샘플 출력입니다.

```
> show asp cluster counter
Global dp-counters:
Context specific dp-counters:
MCAST_FP_TO_SP                  361136
MCAST_SP_TOTAL                  361136
MCAST_SP_PKTS                   143327
MCAST_SP_PKTS_TO_CP             143327
MCAST_FP_CHK_FAIL_NO_HANDLE     217809
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC 81192
MCAST_FP_CHK_FAIL_NO_FP_FWD     62135
```

명령	설명
show asp drop	드롭된 패킷에 대한 가속화된 보안 경로 카운터를 표시합니다.

show asp dispatch

성능 문제를 진단하는 데 유용한 디바이스의 로드 밸런싱 ASP 디스패처의 통계를 표시하려면 **show asp dispatch** 명령을 사용합니다. 이 명령은 하이브리드 폴링/중단 모드의 Firepower Threat Defense 가상 디바이스에만 사용 가능합니다.

show asp dispatch

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show asp dispatch** 명령의 샘플 출력입니다.

```
> show asp dispatch
==== Lina DP thread dispatch stats - CORE 0 ====
Dispatch loop count         :          92260212
Dispatch C2C poll count     :                 2
CP scheduler busy           :          14936242
CP scheduler idle           :          77323971
RX ring busy                :           1513632
Async lock global q busy    :            809481
Global timer q busy         :           1958684
SNP flow bulk sync busy     :               174
Purg process busy           :              2838
Block attempts              :          44594355
Maximum timeout specified   :          10000000
Minimum timeout specified   :           1572864
Average timeout specified   :           9999994
Waken up with OK status     :           2476791
Waken up with timeout       :          42117564
Sleep interrupted           :             85753
Number of interrupts        :           2492566
Number of RX interrupts     :           1454442
Number of TX interrupts     :           2492566
Enable interrupt ok         :         174566236
Disable interrupt ok        :         174231423
Maximum elapsed time        :          54082257
Minimum elapsed time        :              6165
Average elapsed time        :           9658532
Message pipe stats          :

Last clearing of asp dispatch: Never

==== Lina DP thread home-ring/interface list - CORE 0 ====
Interface Internal-Data0/0: port-id 0 irq 10 fd 37
Interface GigabitEthernet0/0: port-id 256 irq 5 fd 38
Interface GigabitEthernet0/1: port-id 512 irq 9 fd 39
Interface GigabitEthernet0/2: port-id 768 irq 11 fd 40
>
```

show asp drop

가속화된 보안 경로에 의해 삭제된 패킷 또는 연결을 디버깅하려면 **show asp drop** 명령을 사용합니다.

show asp drop [**flow** [*flow_drop_reason*] | **frame** [*frame_drop_reason*]]

flow [*flow_drop_reason*]	(선택 사항) 삭제된 흐름(연결)을 표시합니다. 선택적으로 이유를 지정할 수 있습니다. 가능한 흐름 삭제 이유의 목록을 확인하려면 ?를 사용합니다.
frame [*frame_drop_reason*]	(선택 사항) 삭제된 패킷을 표시합니다. 선택적으로 이유를 지정할 수 있습니다. 가능한 프레임 삭제 이유의 목록을 확인하려면 ?를 사용합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp drop 명령은 가속화된 보안 경로에 의해 삭제된 패킷 또는 연결을 표시하여 문제 해결을 도와줍니다. 이 정보는 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

가능한 삭제 이유에 대한 자세한 내용은 Show ASP Drop 명령 사용 문서(http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/show_asp_drop/show_asp_drop.html)를 참조하십시오.

다음은 카운터가 마지막으로 지워진 시간을 나타내는 타임스탬프가 포함된 **show asp drop** 명령의 샘플 출력입니다.

```
> show asp drop

Frame drop:
  Flow is denied by configured rule (acl-drop)                           3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                       4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                          760
  Expired flow (flow-expired)                                            1

Last clearing: Never

Flow drop:
  Flow is denied by access rule (acl-drop)                              24
  NAT failed (nat-failed)                                            28739
```

```
  NAT reverse path failed (nat-rpf-failed)                        22266
  Inspection failure (inspect-fail)                               19433

Last clearing: 17:02:12 UTC Jan 17 2012 by enable_15
```

show asp event

데이터 경로 또는 제어 경로 이벤트 큐를 디버깅하려면 **show asp event** 명령을 사용합니다.

show asp event{dp-cp| cp-dp}

dp-cp	ASP 데이터 경로에서 컨트롤 플레인으로 전송된 이벤트를 표시합니다.
cp-dp	컨트롤 플레인에서 ASP 데이터 경로로 전송된 이벤트를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp event 명령은 데이터 경로 및 제어 경로 내용을 표시하여 문제 해결을 도와줍니다. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

다음은 **show asp event dp-cp** 명령의 샘플 출력입니다.

```
> show asp event dp-cp
DP-CP EVENT QUEUE                    QUEUE-LEN  HIGH-WATER
Punt Event Queue                             0           0
Routing Event Queue                          0           0
Identity-Traffic Event Queue                 0           1
PTP-Traffic Event Queue                      0           0
General Event Queue                          0           0
Syslog Event Queue                           0           0
Non-Blocking Event Queue                     0           8
Midpath High Event Queue                     0           0
Midpath Norm Event Queue                     0           0
Crypto Event Queue                           0         146
HA Event Queue                               0           0
Threat-Detection Event Queue                 0           0
SCP Event Queue                              0           0
ARP Event Queue                              0           1
IDFW Event Queue                             0           0
CXSC Event Queue                             0           0
BFD Event Queue                              0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
crypto-msg            810          0      810        0      810           0
arp-in              17288          0    17288        0    17288           0
```

```
identity-traffic        2          0        2          0        2          0
scheduler             239          0      239          0      239          0
```

show asp inspect-dp snapshot

PDTS(snort에 대한 데이터 플레인 전송/수신 큐) 링의 스냅샷을 확인하려면 **show asp inspect-dp snapshot** 명령을 사용합니다.

show asp inspect-dp snapshot {**config** | **instance** *instance_id* **queue** *queue_id*}

config	PDTS 스냅샷을 위한 전역 구성을 표시합니다.
instance*instance_id*	지정된 PDTS 소비자 인스턴스 ID의 스냅샷을 표시합니다. 값은 0~2147483647입니다.
queue*queue_id*	PDTS 링의 지정된 데이터 경로 전송 큐 ID의 스냅샷을 표시합니다. 값은 0~2147483647입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp inspect-dp snapshot 명령은 PDTS 링 스냅샷 기능의 전역 구성을 표시합니다. 출력은 다음 정보를 표시합니다.

- 최대 스냅샷: 허용된 자동 스냅샷의 최대 수.
- 현재 사용 중: 지금까지 저장된 스냅샷의 수.
- 간격: 시간 간격 값은 동일한 PDTS 링에서 2개의 스냅샷이 허용되는 시간을 지정합니다.
- 자동 스냅샷: 자동 PDTS 스냅샷 기능을 사용하는지 또는 사용 해제되어 있는지 보여줍니다.

다음은 **show asp inspect-dp snapshot config** 명령의 샘플 출력입니다.

```
> show asp inspect-dp snapshot config
Max snapshots  Current in use  Interval (min)  Auto Snapshot
-------------  --------------  --------------  -------------
2              0               5               OFF
```

다음은 **show asp inspect-dp snapshot instance** 명령의 샘플 출력입니다.

```
> show asp inspect-dp snapshot instance 2 queue 1
0 packet captured
0 packet shown
```

show asp inspect-dp snort

모든 snort 인스턴스의 상태를 표시하려면 **show asp inspect-dp snort** 명령을 사용합니다.

show asp inspect-dp snort [instance *instance_id***]**

instance*instance_id*	특정 snort 인스턴스의 상태를 표시합니다. 유효한 값은 0~2147483647입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 모든 snort 인스턴스의 상태를 표시합니다. 출력은 다음 정보를 표시합니다.

- Id: snort 인스턴스 ID.
- PID: snort 인스턴스 프로세스 ID.
- CPU-Usage: snort 인스턴스 ID의 CPU 사용량. 총계 및 사용자/시스템 기준으로 출력됨.
- Conns: snort 인스턴스에서 현재 보유하고 있는 연결 수.
- Segs/Pkts: 세그먼트의 수 또는 snort 인스턴스에서 현재 처리된 패킷.
- Status: snort 인스턴스의 상태.

다음은 **show asp inspect-dp snort** 명령의 샘플 출력입니다.

```
> show asp inspect-dp snort
SNORT Inspect Instance Status Info
Id Pid       Cpu-Usage    Conns      Segs/Pkts  Status
           tot (usr | sys)
-- ----- ---------------- ---------- ---------- ----------
0  9188    0% (  0%|  0%)   0          0        READY
1  9187    0% (  0%|  0%)   0          0        READY
2  9186    0% (  0%|  0%)   0          0        READY
```

show asp inspect-dp snort counters

Snort 인스턴스의 PDTS 관련 원시 카운터를 표시하려면 **show asp inspect-dp snort counters** 명령을 사용합니다.

show asp inspect-dp snort counters [instance *instance_id***] [queues] [rate] [debug] [zeros]**

instance*instance_id*	특정 snort 인스턴스의 카운터를 표시합니다. 유효한 값은 0~2147483647입니다.
queues	큐 정보를 자세히 표시합니다. 인스턴스의 각 생산자 큐는 별도로 표시됩니다. 인스턴스의 큐 정보는 집계되지 않습니다.
rate	5초 동안 카운터 스냅샷을 찍으며 1초에 대한 평균을 구하며 카운터 변경 비율을 표시합니다.
debug	이것은 달리 표시되지 않는 특정한 디버그 카운터를 표시합니다.
zeros	0 카운터를 포함하는 모든 카운터가 표시됩니다.

인스턴스가 지정되지 않은 경우, 모든 인스턴스가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 snort 인스턴스의 PDTS 관련 원시 카운터를 표시합니다. 출력은 다음 정보를 표시합니다.

- Id: Snort 인스턴스 ID입니다. "All"은 집계된 모든 snort 인스턴스를 의미합니다.
- QId: Lina의 전송 큐 ID입니다. 이는 Lina의 스레드 수에 해당합니다. "All"은 모든 큐가 집계되었음을 의미합니다.
- Type: 카운터 유형입니다. 데이터 카운터, 오류 카운터, 디버그 카운터 등이 있습니다.
- Name: 카운터 이름입니다.

- Value: 사람이 읽을 수 있는 카운터 값입니다.
- Raw-Value: 카운터의 원시 값입니다.

카운터 이름:

- Tx Bytes: Lina가 snort 인스턴스에 전송한 바이트 수입니다.
- Tx Segs: Lina가 snort 인스턴스에 전송한 프레임/세그먼트 수입니다.
- Rx Bytes: Lina가 snort 인스턴스에서 수신한 바이트 수입니다.
- Rx Segs: Lina가 snort 인스턴스에서 수신한 프레임/세그먼트 수입니다.
- NewConns: snort 인스턴스에 전송된 연결 수입니다.
- RxQ-Wakeup
- TxQ-Wakeup
- TxQ-LB-Dynamic: PDTS 동적 로드 밸런싱이 작동된 횟수입니다.
- TxQ-Data-Hi-Thresh: Lina의 전송 큐에서의 '높음' 임계값 제한에 도달한 횟수입니다.
- RxQ-Full: Lina의 수신 큐가 가득 찬 횟수입니다.
- TxQ-Full: Lina의 전송 큐가 가득 찬 횟수입니다.
- TxQ-Data-Limit: Lina의 전송 큐에서의 데이터 제한에 도달한 횟수입니다.
- TxQ-LB-Failed: PDTS 동적 로드 밸런싱이 실패한 횟수입니다.
- TxQ-Unavail: Lina의 전송 큐를 사용할 수 없는 횟수입니다.
- TxQ-Not-Ready: Lina의 전송 큐가 준비되지 않은 횟수입니다.
- TxQ-Suspended: Lina의 전송 큐가 일시 중단된 횟수입니다.
- RxQ-Unavail: Lina의 수신 큐를 사용할 수 없는 횟수입니다.
- RxQ-Not-Ready: Lina의 수신 큐가 준비되지 않은 횟수입니다.
- RxQ-Suspended: Lina의 수신 큐가 일시 중단된 횟수입니다.

다음은 **show asp inspect-dp snort counters** 명령의 샘플 출력입니다.

```
> show asp inspect-dp snort counters summary instance 5 debug zeros
SNORT Inspect Instance Counters
Id   QId    Type    Name                                Value      Raw-Value
--   ----   ----    ----                                ---------  ----------
5    All    data    Tx Bytes                             3.3 GB   (3549197468)
5    All    data    Tx Segs                              4.7 M    (4671722)
5    All    data    Rx Bytes                             3.3 GB   (3495936190)
5    All    data    Rx Segs                              4.7 M    (4677344)
5    All    data    NewConns                             11.1 K   (11103)
5    All    debug   RxQ-Wakeup                           0        (0)
5    All    debug   TxQ-Wakeup                           4.7 M    (4655982)
5    All    warn    TxQ-LB-Dynamic                       0        (0)
5    All    warn    TxQ-Data-Hi-Thresh                   0        (0)
```

```
5    All    drop    RxQ-Full                    0          (0)
5    All    drop    TxQ-Full                    0          (0)
5    All    drop    TxQ-Data-Limit              0          (0)
5    All    drop    TxQ-LB-Failed               0          (0)
5    All    err     TxQ-Unavail                 0          (0)
5    All    err     TxQ-Not-Ready               0          (0)
5    All    err     TxQ-Suspended               0          (0)
5    All    err     RxQ-Unavail                 0          (0)
5    All    err     RxQ-Not-Ready               0          (0)
5    All    err     RxQ-Suspended               0          (0)
```

show asp inspect-dp snort counters summary

Snort 인스턴스의 PDTS 관련 카운터를 표시하려면 **show asp inspect-dp snort counters summary** 명령을 사용합니다. 카운터는 각 인스턴스로 집계됩니다.

show asp inspect-dp snort counters summary [instance *instance_id***] [queues] [rate]**

instance*instance_id*	특정 snort 인스턴스의 카운터를 표시합니다. 유효한 값은 0~2147483647입니다.
queues	큐 정보를 자세히 표시합니다. 인스턴스의 각 생산자 큐는 별도로 표시됩니다. 인스턴스의 큐 정보는 집계되지 않습니다.
rate	카운터의 1초 평균 증가를 표시합니다. 현재 1초 평균은 명령의 마지막과 현재 호출 간의 델타 증가를 기준으로 합니다. 델타 증가가 1초에 한 번 샘플링되는 5초 롤링 평균을 기준으로 하는 것으로 변경됩니다.

인스턴스가 지정되지 않은 경우, 모든 인스턴스가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 snort 인스턴스의 PDTS 관련 카운터를 표시합니다. 출력은 다음 정보를 표시합니다.

- Id: Snort 인스턴스 ID입니다. “All”은 집계된 모든 snort 인스턴스를 의미합니다.
- QId: Lina의 전송 큐 ID입니다. 이는 Lina의 스레드 수에 해당합니다. “All”은 모든 큐가 집계되었음을 의미합니다.
- TxBytes: Lina가 snort 인스턴스에 전송한 총 바이트 수입니다.
- TxFrames: Lina가 snort 인스턴스에 전송한 총 프레임/세그먼트 수입니다.
- RxBytes: Lina가 snort 인스턴스에서 수신한 총 바이트 수입니다.
- RxFrames: Lina가 snort 인스턴스에서 수신한 총 프레임/세그먼트 수입니다.

- Conns: snort 인스턴스에서 처리한 총 연결 수입니다.

다음은 **show asp inspect-dp snort counters summary** 명령의 샘플 출력입니다.

```
> show asp inspect-dp snort counters summary instance 2
SNORT Inspect Instance Counter Summary
Id   QId  TxBytes    TxFrames   RxBytes    RxFrames   Conns
--   ---- ---------- ---------- ---------- ---------- -----
2    All    0          0          0          0          0
```

show asp inspect-dp snort queues

동일한 인스턴스로 모든 큐를 집계하는 모든 snort 인스턴스(프로세스)에 대한 큐 정보를 표시하려면 **show asp inspect-dp snort queues** 명령을 사용합니다.

show asp inspect-dp snort queues [instance *instance_id***] [detail] [debug]**

instance*instance_id*	특정 snort 인스턴스의 큐를 표시합니다. 유효한 값은 0~2147483647입니다.
detail	큐 정보를 자세히 표시합니다. 인스턴스의 각 생산자 큐는 별도로 표시됩니다. 인스턴스의 큐 정보는 집계되지 않습니다.
debug	추가 디버그 정보도 표시됩니다.

인스턴스가 지정되지 않은 경우, 모든 인스턴스가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

동일한 인스턴스로 모든 대기열을 집계하는 모든 snort 인스턴스(프로세스)의 큐 정보를 표시합니다. 출력은 다음 정보를 표시합니다.

- Id: Snort 인스턴스 ID입니다. “All”은 집계된 모든 snort 인스턴스를 의미합니다.
- QId: Lina의 전송 큐 ID입니다. 이는 Lina의 스레드 수에 해당합니다. “All”은 모든 큐가 집계되었음을 의미합니다.
- Rx Queue: Lina의 수신 큐입니다. “Used”는 데이터의 양을 보여주며 “util”은 큐 사용률을, “state”는 공유 메모리 상태를 보여줍니다.
- TxQ: Lina의 전송 대기열입니다. “Used”는 데이터의 양을 보여주며 “util”은 대기열 사용률을, “state”는 공유 메모리 상태를 보여줍니다.

Counters:

- RxQ-Size: Lina의 수신 큐 크기입니다.

- TxQ-Size: Lina의 전송 큐 크기입니다.
- TxQ-Data-Limit: 전송 큐의 데이터 제한입니다. 이 임계값을 초과할 경우, 데이터 패킷이 드롭됩니다. 백분율은 전송 큐의 임계값을 보여줍니다.
- TxQ-Data-Hi-Thresh: 전송 큐의 '높음' 임계값입니다. 이 임계값을 초과할 경우, 다른 snort 인스턴스로 흐름의 균형을 유지하기 위해 PDTS 동적 로드 밸런싱이 작동합니다.

다음은 **show asp inspect-dp snort queues** 명령의 샘플 출력입니다.

```
> show asp inspect-dp snort counters summary instance 2
SNORT Inspect Instance Queue Configuration

RxQ-Size:              1   MB
TxQ-Size:            128   KB
TxQ-Data-Limit:      102.4 KB   (80%)
TxQ-Data-Hi-Thresh:   35.8 KB   (28%)

Id QId  RxQ         RxQ    TxQ         TxQ
        (used)      (util) (used)      (util)
-- ---- ---------- ------ ---------- ------
0  All    0        0%       0        0%
1  All    0        0%       0        0%
2  All    0        0%       0        0%
```

show asp inspect-dp snort queue-exhaustion

Snort 큐 소모가 발생할 경우의 자동 스냅샷을 표시하려면 **show asp inspect-dp snort queue-exhaustion** 명령을 사용합니다.

show asp inspect-dp snort queue-exhaustion [**snapshot** *snapshot_id*] [**export** *location*]

snapshot*snapshot_id*	이 옵션은 큐 소모 정보를 인쇄하는 특정 스냅샷을 지정합니다. 값은 1~24입니다.
export*location*	스냅샷 내용은 off-box 분석을 위해 지정된 위치의 pcap 파일로 내보냅니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

자용 가이드라인

show asp inspect-dp snort queue-exhaustion 명령은 snort 큐가 소모될 때 만든 스냅샷 내용을 표시합니다. 이 명령은 선택한 스냅샷의 내용을 보여줍니다. 출력은 **show capture** 명령의 출력과 유사합니다.

다음은 **show asp inspect-dp snort queue-exhaustion** 명령의 샘플 출력입니다.

```
> show asp inspect-dp snort queue-exhaustion snapshot 1
102 packets captured
   1: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693143043:693144411(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977907>
   2: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693144411:693145779(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172833 64977907>
   3: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693145779:693147147(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172838 64977912>
   4: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693147147:693148515(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172838 64977912>
   5: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
693153987:693155355(1368) ack 1996534769 win 235 <nop,nop,timestamp 25172858 64977932>
   6: 13:52:36.266343       10.100.26.6.80 > 192.168.26.6.45858: .
(...output truncated...)
```

show asp load-balance

로드 밸런서 큐 크기의 히스토그램을 표시하려면 **show asp load-balance** 명령을 사용합니다.

show asp load-balance [**detail**]

detail	(선택 사항) 샘플에 사용된 해시 버킷에 대한 세부 정보를 표시합니다.

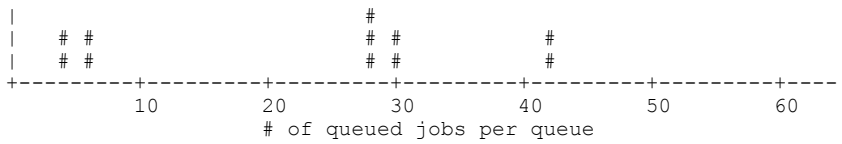
릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp load-balance 명령은 문제 해결에 도움이 될 수 있습니다. 일반적으로 패킷은 인터페이스 수신 링에서 가져온 동일한 코어에 의해 처리됩니다. 그러나 다른 코어에서 방금 받은 패킷과 동일한 연결을 이미 처리 중인 경우에는 패킷이 해당 코어의 대기열에 추가됩니다. 이 대기열 처리로 인해 다른 코어가 유휴 상태인 동안 로드 밸런서 대기열이 증가할 수 있습니다. 자세한 내용은 **asp load-balance per-packet** 명령을 참조하십시오.

다음은 **show asp load-balance** 명령의 샘플 출력입니다. X축은 서로 다른 대기열에서 대기 중인 패킷 수를 나타냅니다. Y축은 대기 중인 패킷이 있는 로드 밸런서 해시 버킷 수(히스토그램 버킷을 나타내는 히스토그램 제목의 버킷과 혼동하지 않도록)를 나타냅니다. 큐가 있는 해시 버킷의 정확한 개수를 확인하려면 **detail** 키워드를 사용합니다.

```
> show asp load-balance
Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
                     ASP load balancer queue sizes
  100 +
      |
      |
      |
S     |
a     |
m     |
p     |
l  10 +
e     |
s     |
      |
      |
```



명령	설명
asp load-balance per-packet	멀티 코어 ASA 모델의 코어 부하 균형 방식을 변경합니다.

show asp multiprocessor accelerated- features

가속화된 보안 경로의 멀티프로세서 가속화를 디버깅하려면 **show asp multiprocessor accelerated-features** 명령을 사용합니다.

show asp multiprocessor accelerated-features

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp multiprocessor accelerated-features 명령은 성능 문제 해결에 도움이 될 수 있는 멀티프로세서에 대해 가속화된 기능의 목록을 표시합니다.

다음은 **show asp multiprocessor accelerated-features** 명령의 샘플 출력입니다.

```
> show asp multiprocessor accelerated-features
MultiProcessor accelerated feature list:
        Access Lists
        DNS Guard
        Failover Stateful Updates
        Flow Operations(create, update, and tear-down)
        Inspect HTTP URL Logging
        Inspect HTTP (AIC)
        Inspect IPSec Pass through
        Inspect ICMP and ICMP error
        Inspect RTP/RTCP
        IP Audit
        IP Fragmentation & Re-assembly
        IPSec data-path
        MPF L2-L4 Classify
        Multicast forwarding
        NAT/PAT
        Netflow using UDP transport
        Non-AIC Inspect DNS
        Packet Capture
        QOS
        Resource Management
        Routing Lookup
        Shun
        SSL data-path
        Syslogging using UDP transport
        TCP Intercept
        TCP Security Engine
        TCP Transport
        Threat Detection
        Unicast RPF
        WCCP Re-direct
Above list applies to routed, transparent, single and multi mode.
```

show asp overhead

스핀 잠금과 async 손실 통계를 추적 및 표시하려면 **show asp overhead** 명령을 사용합니다.

show asp overhead [**sort-by-average**] [**sort-by-file**]

sort-by-average	호출당 평균 주기별로 결과를 정렬합니다.
sort-by-file	파일 이름별로 결과를 정렬합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show asp overhead** 명령의 샘플 출력입니다.

```
> show asp overhead
0.0% of available CPU cycles were lost to Multiprocessor overhead
        since last the MP overhead statistics were last cleared
              File Name Line Function Call             Avg         Cycles      %
---------------------- ---- ----------------------  -----  -------------  -----
```

show asp table arp

가속화된 보안 경로 ARP 테이블을 디버깅하려면 **show asp table arp** 명령을 사용합니다.

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

address*ip_address*	(선택 사항) ARP 테이블 항목을 보려는 IP 주소를 식별합니다.
interface *interface_name*	(선택 사항) ARP 테이블을 볼 특정 인터페이스를 식별합니다.
netmask*mask*	(선택 사항) IP 주소의 서브넷 마스크를 설정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show arp 명령은 컨트롤 플레인의 내용을 표시하고, **show asp table arp** 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로 내용을 표시합니다. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

다음은 **show asp table arp** 명령의 샘플 출력입니다.

```
> show asp table arp
Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0
Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
```

```
0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

명령	설명
show arp	ARP 테이블을 표시합니다.
show arp statistics	ARP 통계를 표시합니다.

show asp table classify

가속화된 보안 경로 분류자 테이블을 디버깅하려면 **show asp table classify** 명령을 사용합니다.

show asp table classify [**interface** *interface_name*] [**crypto** | **domain** *domain_name*] [**hits**] [**match** *regexp*]

crypto	(선택 사항) 암호화, 암호 해독 및 ipsec 터널 흐름 도메인만 표시합니다.
domain*domain_name*	(선택 사항) 특정 분류자 도메인에 대한 항목을 표시합니다. 사용 가능한 도메인 목록은 CLI 도움말을 참고하십시오.
hits	(선택 사항) 0이 아닌 적중 값이 있는 분류자 항목을 표시합니다.
interface*interface_name*	(선택 사항) 분류자 테이블을 볼 특정 인터페이스를 식별합니다.
match*regexp*	(선택 사항) 정규식과 일치하는 분류자 항목을 표시합니다. 정규식에 공백이 포함된 경우 따옴표를 사용합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp table classify 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 분류자 내용을 표시합니다. 분류자는 프로토콜과 같은 인커밍 패킷의 속성과 소스 및 목적지 주소를 검사하여 각 패킷을 해당 분류 규칙에 일치시킵니다. 각 규칙에는 패킷 삭제 또는 통과 허용과 같은 수행되는 작업의 유형을 확인하는 분류 도메인이 레이블로 지정됩니다. 이 정보는 디버깅에만 사용되며, 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

다음은 **show asp table classify** 명령의 샘플 출력입니다.

```
> show asp table classify
Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
```

```
        dst ip=10.86.194.60, mask=255.255.255.255, port=0, tag=any
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
...
```

다음은 마지막으로 적중 횟수를 지운 레코드가 포함된 **show asp table classify hits** 명령의 샘플 출력입니다.

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
       hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0

Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0,
       dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
       hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000,
       mask=0000.0000.0000 dst mac=0000.0000.0000, mask=0000.0000.0000
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
       hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
       mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

다음은 레이어 2 정보가 포함된 **show asp table classify hits** 명령의 샘플 출력입니다.

```
Input Table
in  id=0x7fff2de10ae0, priority=120, domain=permit, deny=false
    hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1
    src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=identity in  id=0x7fff2de135c0, priority=0,
domain=inspect-ip-options, deny=true
    hits=41, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
    src ip/id=0.0.0.0, mask=0.0.0.0, port=0
    dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
    input_ifc=LAN-SEGMENT, output_ifc=any
...

Output Table:

L2 - Output Table:

L2 - Input Table:
in  id=0x7fff2de0e080, priority=1, domain=permit, deny=false
    hits=30, user_data=0x0, cs_id=0x0, l3_type=0x608
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0000.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e580, priority=1, domain=permit, deny=false
    hits=382, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
    dst mac=0000.0000.0000, mask=0100.0000.0000
    input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e800, priority=1, domain=permit, deny=false
    hits=312, user_data=0x0, cs_id=0x0, l3_type=0x8
    src mac=0000.0000.0000, mask=0000.0000.0000
```

```
dst mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
input_ifc=LAN-SEGMENT, output_ifc=any
```

show asp table cluster chash-table

클러스터링을 위해 가속화된 보안 경로 cHash 테이블을 디버깅하려면 **show asp table cluster chash-table** 명령을 사용합니다.

show asp table cluster chash-table

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp table cluster chash-table 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 내용을 표시합니다. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

다음은 **show asp table cluster chash-table** 명령의 샘플 출력입니다.

```
> show asp table cluster chash-table
Cluster current chash table:

00003333
21001200
22000033
02222223
33331111
21110000
00133103
22222223
30000102
11222222
23222331
00002223
(...output truncated...)
```

명령	설명
show asp cluster counter	클러스터 데이터 경로 카운터 정보를 표시합니다.

show asp table interfaces

가속화된 보안 경로 인터페이스 테이블을 디버깅하려면 **show asp table interfaces** 명령을 사용합니다.

show asp table interfaces

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp table interfaces 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 인터페이스 테이블 내용을 표시합니다. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

다음은 **show asp table interfaces** 명령의 샘플 출력입니다.

```
> show asp table interfaces
** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20
Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20
Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20
Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

show asp table routing

가속화된 보안 경로 라우팅 테이블을 디버깅하려면 **show asp table routing** 명령을 사용합니다. 이 명령은 IPv4 및 IPv6 주소를 지원합니다. 관리 전용 키워드는 관리 라우팅 테이블에서 숫자 이동성 경로를 표시합니다.

show asp table routing [**management-only**] [**input** | **output**] [**address** *ip_address* [**netmask** *mask*] | **interface** *interface_name*]

address*ip_address*	라우팅 항목을 볼 IP 주소를 설정합니다. IPv6 주소의 경우 슬래시(/) 뒤에 오는 접두사(0~128)로 서브넷 마스크를 포함할 수 있습니다. 예를 들어, fe80::2e0:b6ff:fe01:3b7a/128을 입력합니다.
input	입력 경로 테이블의 항목을 표시합니다.
interface*interface_name*	(선택 사항) 라우팅 테이블을 볼 특정 인터페이스를 식별합니다.
netmask*mask*	IPv4 주소의 경우 서브넷 마스크를 지정합니다.
output	출력 경로 테이블의 항목을 표시합니다.
management-only	관리 라우팅 테이블에서 숫자 이동성 경로를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp table routing 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 라우팅 테이블 내용을 표시합니다. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오. 관리 전용 키워드는 관리 라우팅 테이블에서 숫자 이동성 경로를 표시합니다.

다음은 **show asp table routing** 명령의 샘플 출력입니다.

```
> show asp table routing
```

```
in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

명령	설명
show route	제어 평면의 라우팅 테이블을 표시합니다.

show asp table socket

가속화된 보안 경로 소켓 정보를 디버깅하려면 **show asp table socket** 명령을 사용합니다.

show asp table socket [*handle*] [**stats**]

handle	소켓의 길이를 지정합니다.
stats	가속화된 보안 경로 소켓 테이블의 통계를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp table socket 명령은 가속화된 보안 경로 소켓 문제 해결에 도움이 될 수 있는 가속화된 보안 경로 소켓 정보를 표시합니다. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

다음은 **show asp table socket** 명령의 샘플 출력입니다.

```
Protocol  Socket    Local Address               Foreign Address         State
TCP       00012bac  10.86.194.224:23            0.0.0.0:*               LISTEN
TCP       0001c124  10.86.194.224:22            0.0.0.0:*               LISTEN
SSL       00023b84  10.86.194.224:443           0.0.0.0:*               LISTEN
SSL       0002d01c  192.168.1.1:443             0.0.0.0:*               LISTEN
DTLS      00032b1c  10.86.194.224:443           0.0.0.0:*               LISTEN
SSL       0003a3d4  0.0.0.0:443                 0.0.0.0:*               LISTEN
DTLS      00046074  0.0.0.0:443                 0.0.0.0:*               LISTEN
TCP       02c08aec  10.86.194.224:22            171.69.137.139:4190     ESTAB
```

다음은 **show asp table socket stats** 명령의 샘플 출력입니다.

```
TCP Statistics:
  Rcvd:
     total 14794
     checksum errors 0
     no port 0
  Sent:
     total 0
UDP Statistics:
  Rcvd:
     total 0
```

```
     checksum errors 0
  Sent:
     total 0
     copied 0
NP SSL System Stats:
  Handshake Started: 33
  Handshake Complete: 33
  SSL Open: 4
  SSL Close: 117
  SSL Server: 58
  SSL Server Verify: 0
  SSL Client: 0
```

TCP/UDP 통계는 텔넷, SSH 또는 HTTPS와 같이 디바이스에서 실행 중이거나 수신 대기 중인 서비스를 대상으로 하여 전송 또는 수신된 패킷 수를 나타내는 패킷 카운터입니다. 체크섬 오류는 계산된 패킷 체크섬이 패킷에 저장된 체크섬 값과 일치하지 않아(즉, 패킷이 손상됨) 삭제된 패킷 수입니다. NP SSL 통계는 수신된 각 메시지 유형 수를 나타냅니다. 대부분은 SSL 서버 또는 SSL 클라이언트 인스턴스에 대한 새 SSL 연결의 시작 및 완료를 나타냅니다.

명령	설명
show asp table vpn-context	가속화된 보안 경로 VPN 상황 테이블을 표시합니다.

show asp table vpn-context

가속화된 보안 경로 VPN 상황 테이블을 디버깅하려면 **show asp table vpn-context** 명령을 사용합니다.

show asp table vpn-context [**detail**]

detail	(선택 사항) VPN 상황 테이블에 대한 추가 세부 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show asp table vpn-context 명령은 문제 해결에 도움이 될 수 있는 가속화된 보안 경로의 VPN 상황 내용을 표시합니다. 이러한 테이블은 디버깅에만 사용되며, 정보 출력이 변경될 수 있습니다. 이 명령을 사용하여 시스템을 디버깅하는 데 도움이 필요한 경우 Cisco TAC에 문의하십시오.

다음은 **show asp table vpn-context** 명령의 샘플 출력입니다.

```
> show asp table vpn-context
VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

다음은 영구 IPsec 터널링된 플로우 기능이 활성화된 경우(PRESERVE 플래그로 표시됨) **show asp table vpn-context** 명령의 샘플 출력입니다.

```
> show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000,
rk=0000000000, gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000,
rk=0000000000, gc=0
```

다음은 **show asp table vpn-context detail** 명령의 샘플 출력입니다. 영구 IPsec 터널링된 플로우 기능이 활성화된 경우 플래그는 PRESERVE 플래그를 포함합니다.

```
> show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

명령	설명
show asp drop	드롭된 패킷에 대한 가속화된 보안 경로 카운터를 표시합니다.

show asp table zone

이 명령을 사용하지 마십시오. 이 명령은 Firepower Threat Defense에서 지원되지 않는 영역 기능과 관련이 있습니다. 이 명령은 보안 영역 컨피그레이션에 대한 정보를 표시하지 않습니다.

show audit-log

시스템 감사 로그를 표시하려면 **show audit-log** 명령을 사용합니다.

show audit-log

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 감사 로그를 역시간순으로 표시합니다. 가장 최근 감사 로그 이벤트가 먼저 나열됩니다.

이벤트는 시스템 업데이트, 권한 문제, 컨피그레이션 변경 및 정책 애플리케이션을 포함할 수 있습니다. 이 정보는 Firepower Management Center만 사용하여 원격으로 관리되는 디바이스에 사용할 수 있습니다. 감사 로그는 로컬로 관리되는 시스템의 경우 비어 있습니다.

다음 예에서는 감사 로그를 보여줍니다.

```
> show audit-log
Audit Log Output:
 time                   :  1476223151 (Tue Oct 11 21:59:11 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Clam update synchronization
from firepower
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222646 (Tue Oct 11 21:50:46 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Apply AMP Dynamic Analysis C
onfiguration from firepower
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222564 (Tue Oct 11 21:49:24 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Apply Initial_Health_Policy
2016-10-11 18:54:59 from firepower
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222563 (Tue Oct 11 21:49:23 2016)
```

```
 event_type             :  notify
 subsystem              :  Health > Health Policy > Apply > Initial_Health_Policy 20
16-10-11 18:54:59 > firepower
 actor                  :  admin
 message                :  Apply
 result                 :  Success
 action_source_ip       :  127.0.0.1
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222508 (Tue Oct 11 21:48:28 2016)
 event_type             :  notify
 subsystem              :  Task Queue
 actor                  :  System
 message                :  Successful task completion : Registration '10.83.57.41'
 result                 :  Success
 action_source_ip       :  localhost
 action_destination_ip  :  localhost
-------------------------------------------------------------
 time                   :  1476222473 (Tue Oct 11 21:47:53 2016)
 event_type             :  Restart
 subsystem              :  NTP Configuration changed
 actor                  :  Default User
 message                :  Restart
 result                 :  Success
 action_source_ip       :  Default User IP
 action_destination_ip  :  Default Target IP
-------------------------------------------------------------
```

show b

- show bgp summary, 408 페이지
- show bgp update-group, 412 페이지
- show blocks, 415 페이지
- show bootvar, 420 페이지
- show bridge-group, 421 페이지

show banner

구성한 배너 메시지를 표시하려면 **show banner** 명령을 입력합니다.

show banner [**login**]

login	비밀번호 로그인 프롬프트에 대해 설정된 배너를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

```
> show banner
```

show bgp

BGP(Border Gateway Protocol) 라우팅 테이블의 항목을 표시하려면 **show bgp** 명령을 사용합니다.

show bgp [*ip-address* [*mask* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*length*] | **bestpath** | **multipaths** | **subnets**] | **bestpath** | **multipaths**] | **all** | **prefix-list** *name* | **pending-prefixes** | **route-map** *name*]]

ip-address	(선택 사항) 표시할 BGP 라우팅 테이블의 네트워크를 지정합니다.
mask	(선택 사항) 지정된 네트워크의 일부인 호스트를 필터링하거나 일치시킬 마스크입니다.
longer-prefixes	(선택 사항) 지정된 경로 및 모든 구체적인 경로를 표시합니다.
injected	(선택 사항) BGP 라우팅 테이블에 삽입된 특정 접두사를 표시합니다.
shorter-prefixes	(선택 사항) 지정된 경로 및 모든 구체적이지 않은 경로를 표시합니다.
length	(선택 사항) 접두사 길이입니다. 이 인수 값은 0~32의 숫자입니다.
bestpath	(선택 사항) 이 접두사에 대한 최상의 경로를 표시합니다.
multipaths	(선택 사항) 이 접두사에 대한 다중 경로를 표시합니다.
subnets	(선택 사항) 지정된 접두사에 대한 서브넷 경로를 표시합니다.
all	(선택 사항) BGP 라우팅 테이블의 모든 주소군 정보를 표시합니다.
prefix-list*name*	(선택 사항) 지정된 접두사 목록을 기반으로 출력을 필터링합니다.
pending-prefixes	(선택 사항) BGP 라우팅 테이블에서 삭제 보류 중인 접두사를 표시합니다.
route-map*name*	(선택 사항) 지정된 경로 맵을 기반으로 출력을 필터링합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show bgp 명령은 BGP 라우팅 테이블의 내용을 표시하는 데 사용됩니다. 특정 접두사, 접두사 길이 및 접두사 목록, 경로 맵 또는 조건부 알림을 통해 삽입된 접두사에 대한 항목을 표시하도록 출력을 필터링할 수 있습니다.

다음 샘플 출력에서는 BGP 라우팅 테이블을 보여줍니다.

```
> show bgp
BGP table version is 22, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.1/32      0.0.0.0                  0         32768 i
*>i10.2.2.2/32      172.16.1.2               0    100      0 i
*bi10.9.9.9/32      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                           0 10 10 i
* i172.16.1.0/24    172.16.1.2               0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.1.0      0.0.0.0                  0         32768 i
*>i192.168.3.0      172.16.1.2               0    100      0 i
*bi192.168.9.0      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                           0 10 10 i
*bi192.168.13.0     192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                           0 10 10 i
```

다음 표는 각 필드에 대해 설명합니다.

표 ***3: show bgp*** 필드

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
local router ID	라우터의 IP 주소입니다.

필드	설명
Status codes	테이블 항목의 상태입니다. 상태는 테이블의 각 줄 시작 부분에 표시됩니다. 다음 값 중 하나일 수 있습니다. • s - 테이블 항목이 표시되지 않습니다. • d - 테이블 항목이 감소합니다. • h - 테이블 항목이 기록입니다. • * - 테이블 항목이 유효합니다. • > - 테이블 항목이 해당 네트워크에 가장 적합한 항목입니다. • i - 테이블 항목이 iBGP(내부 BGP) 세션을 통해 학습되었습니다. • r - 테이블 항목에서 RIB 오류가 발생했습니다. • s - 테이블 항목이 오래되었습니다. • m - 테이블 항목에 해당 네트워크에 사용할 여러 경로가 있습니다. • b - 테이블 항목에 해당 네트워크에 사용할 백업 경로가 있습니다. • x - 테이블 항목에 해당 네트워크에 사용할 최상의 외부 경로가 있습니다.
Origin codes	항목의 출처입니다. 원본 코드는 테이블의 각 줄 맨 끝에 배치됩니다. 다음 값 중 하나일 수 있습니다. • i - IGP(Interior Gateway Protocol)에서 시작된 항목으로 알림이 전송됩니다. • e - EGP(외부 게이트웨이 프로토콜)에서 시작된 항목입니다. • ? - 경로의 출처가 명확하지 않습니다. 일반적으로 IGP에서 BGP로 재배포되는 라우터입니다.
Network	네트워크 엔터티의 IP 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 라우터에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
Metric	표시된 경우 내부 자동 시스템 메트릭 값입니다.
LocPrf	로컬 환경 설정 값입니다. 기본값은 100입니다.
Weight	자동 시스템 필터를 통해 설정되는 경로의 가중치입니다.
Path	대상 네트워크에 대한 자동 시스템 경로입니다. 이 필드에는 경로의 각 자동 시스템에 대해 하나의 항목이 있을 수 있습니다.

필드	설명
(stale)	지정된 자동 시스템의 다음 경로가 정상적인 재시작 프로세스 중에 “stale”로 표시되었음을 나타냅니다.

다음 샘플 출력은 BGP 라우팅 테이블의 192.168.1.0 항목에 대한 정보를 표시합니다.

```
> show bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

다음 샘플 출력은 BGP 라우팅 테이블의 10.3.3.3 255.255.255.255 항목에 대한 정보를 표시합니다.

```
> show bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
     1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
      Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

다음 표는 각 필드에 관해 설명합니다.

표 ***4: show bgp(4***바이트 자동 시스템 번호***)*** 필드

필드	설명
BGP routing table entry for	라우팅 테이블 항목의 IP 주소 또는 네트워크 번호입니다.
version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
Paths	사용 가능한 경로 수 및 설치된 최상의 경로 수입니다. 이 줄에는 최상의 경로가 IP 라우팅 테이블에 설치된 경우 “Default-IP-Routing-Table”이 표시됩니다.

필드	설명
Multipath	이 필드는 다중 경로 부하 공유가 활성화된 경우에 표시됩니다. 이 필드는 다중 경로가 iBGP인지 또는 eBGP인지를 나타냅니다.
Advertised to update-groups	알림이 처리되는 각 업데이트 그룹 수입니다.
Origin	항목의 출처입니다. 출처는 IGP, EGP 또는 incomplete일 수 있습니다. 이 줄에는 구성된 메트릭(메트릭이 구성되지 않은 경우 0), 로컬 환경 설정 값(기본값은 100) 및 경로의 상태와 유형(internal, external, multipath, best)이 표시됩니다.
Extended Community	이 필드는 경로에 확장 커뮤니티 특성이 수반되는 경우에 표시됩니다. 특성 코드가 이 줄에 표시됩니다. 확장 커뮤니티에 대한 정보는 후속 줄에 표시됩니다.

다음은 **all** 키워드와 함께 입력된 **show bgp** 명령의 샘플 출력입니다. 구성된 모든 주소군에 대한 정보가 표시됩니다.

```
> show bgp all

For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
```

다음은 **longer-prefixes** 키워드와 함께 입력된 **show bgp** 명령의 샘플 출력입니다.

```
> show bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0         10.92.72.30        8896         32768 ?
```

```
*                   10.92.72.30                            0 109 108 ?
*> 10.92.1.0        10.92.72.30         8796         32768 ?
*                   10.92.72.30                            0 109 108 ?
*> 10.92.11.0       10.92.72.30        42482         32768 ?
*                   10.92.72.30                            0 109 108 ?
*> 10.92.14.0       10.92.72.30         8796         32768 ?
*                   10.92.72.30                            0 109 108 ?
*> 10.92.15.0       10.92.72.30         8696         32768 ?
*                   10.92.72.30                            0 109 108 ?
*> 10.92.16.0       10.92.72.30         1400         32768 ?
*                   10.92.72.30                            0 109 108 ?
*> 10.92.17.0       10.92.72.30         1400         32768 ?
*                   10.92.72.30                            0 109 108 ?
*> 10.92.18.0       10.92.72.30         8876         32768 ?
*                   10.92.72.30                            0 109 108 ?
*> 10.92.19.0       10.92.72.30         8876         32768 ?
*                   10.92.72.30                            0 109 108 ?
```

다음은 **shorter-prefixes** 키워드와 함께 입력된 **show bgp** 명령의 샘플 출력입니다. 8비트 접두사 길이가 지정됩니다.

```
> show bgp 172.16.0.0/16 shorter-prefixes 8
*> 172.16.0.0         10.0.0.2                               0 ?
*                     10.0.0.2                 0             0 200 ?
```

다음은 **prefix-list** 키워드와 함께 입력된 **show bgp** 명령의 샘플 출력입니다.

```
> show bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?
*                   10.0.0.2                 0             0 200 ?
```

다음은 **route-map** 키워드와 함께 입력된 **show bgp** 명령의 샘플 출력입니다.

```
> show bgp route-map LEARNED_PATH

BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?
*                   10.0.0.2                 0             0 200 ?
```

show bgp cidr-only

CIDR(Classless Inter-Domain Routing)과 함께 경로를 표시하려면 **show bgp cidr-only** 명령을 사용합니다.

show bgp cidr-only

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp cidr-only** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                         0 1878 ?
*> 172.16.0.0/16    172.16.72.30                         0 108 ?
```

show bgp community

지정된 BGP 커뮤니티에 속한 경로를 표시하려면 **show bgp community** 명령을 사용합니다.

show bgp community [*community-number*] [**exact-match**] [**no-advertise**] [**no-export**]

community-number	(선택 사항) 유효한 값은 1~4294967295의 커뮤니티 번호 또는 AA:NN(자동 시스템:커뮤니티 번호, 2바이트 번호)입니다.
exact-match	(선택 사항) 정확히 일치하는 항목이 있는 경로만 표시합니다.
no-advertise	(선택 사항) 피어(잘 알려진 커뮤니티)로 보급되지 않는 경로만 표시합니다.
no-export	(선택 사항) 로컬 자동 시스템(잘 알려진 커뮤니티) 외부로 내보낼 수 없는 경로만 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp community** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp community 111:12345
BGP table version is 10, local router ID is 224.0.0.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 172.16.2.2/32    10.43.222.2           0             0 222 ?
*> 10.0.0.0         10.43.222.2           0             0 222 ?
*> 10.43.0.0        10.43.222.2           0             0 222 ?
*> 10.43.44.44/32   10.43.222.2           0             0 222 ?
*  10.43.222.0/24   10.43.222.2           0             0 222 i
*> 172.17.240.0/21  10.43.222.2           0             0 222 ?
*> 192.168.212.0    10.43.222.2           0             0 222 i
*> 172.31.1.0       10.43.222.2           0             0 222 ?
```

show bgp community-list

BGP(Border Gateway Protocol) 커뮤니티 목록에서 허용하는 경로를 표시하려면 **show bgp community-list** 명령을 사용합니다.

show bgp community-list {*community-list-number* | *community-list-name* [**exact-match**]}

community-list-number	1~500의 표준 또는 확장 커뮤니티 목록 번호입니다.
community-list-name	커뮤니티 목록 이름입니다. 커뮤니티 목록 이름은 표준 또는 확장일 수 있습니다.
exact-match	(선택 사항) 정확히 일치하는 항목이 있는 경로만 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp community-list**의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp community-list 20
BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

  Network          Next Hop            Metric LocPrf Weight Path
* i10.3.0.0         10.0.22.1                0    100      0 1800 1239 ?
*>i                 10.0.16.1                0    100      0 1800 1239 ?
* i10.6.0.0         10.0.22.1                0    100      0 1800 690 568 ?
*>i                 10.0.16.1                0    100      0 1800 690 568 ?
* i10.7.0.0         10.0.22.1                0    100      0 1800 701 35 ?
*>i                 10.0.16.1                0    100      0 1800 701 35 ?
*                   10.92.72.24                            0 1878 704 701 35 ?
* i10.8.0.0         10.0.22.1                0    100      0 1800 690 560 ?
*>i                 10.0.16.1                0    100      0 1800 690 560 ?
*                   10.92.72.24                            0 1878 704 701 560 ?
* i10.13.0.0        10.0.22.1                0    100      0 1800 690 200 ?
*>i                 10.0.16.1                0    100      0 1800 690 200 ?
*                   10.92.72.24                            0 1878 704 701 200 ?
* i10.15.0.0        10.0.22.1                0    100      0 1800 174 ?
*>i                 10.0.16.1                0    100      0 1800 174 ?
* i10.16.0.0        10.0.22.1                0    100      0 1800 701 i
*>i                 10.0.16.1                0    100      0 1800 701 i
*                   10.92.72.24                            0 1878 704 701 i
```

show bgp filter-list

지정된 필터 목록과 일치하는 경로를 표시하려면 **show bgp filter-list** 명령을 사용합니다.

show bgp filter-list *access-list-name*

access-list-name	자동 시스템 경로 액세스 목록의 이름입니다. 유효한 값은 1 ~ 500입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp filter-list** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp filter-list filter-list-acl
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

show bgp injected-paths

BGP(Border Gateway Protocol) 라우팅 테이블의 거부된 모든 경로를 표시하려면 **show bgp injected-paths** 명령을 사용합니다.

show bgp injected-paths

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp injected-paths** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp injected-paths
BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                             0 ?
*> 172.17.0.0/16    10.0.0.2                             0 ?
```

show bgp ipv4 unicast

IPv4(IP version 4) BGP(Border Gateway Protocol) 라우팅 테이블의 항목을 표시하려면 **show bgp ipv4 unicast** 명령을 사용합니다.

show bgp ipv4 unicast [**cidr-only**]

unicast	IPv4 유니캐스트 주소 접두사를 지정합니다.
cidr-only	(선택 사항) 부자연스러운 넷마스크가 있는 경로를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp ipv4 unicast** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp ipv4 unicast
 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

show bgp ipv6 unicast

IPv6 BGP(Border Gateway Protocol) 라우팅 테이블의 항목을 표시하려면 **show bgp ipv6** 명령을 사용합니다.

show bgp ipv6 unicast [*ipv6-prefix/prefix-length*] [**longer-prefixes**] [**labels**]

unicast	IPv6 유니캐스트 주소 접두사를 지정합니다.
ipv6-prefix	(선택 사항) IPv6 BGP 라우팅 테이블의 특정 네트워크를 표시하기 위해 입력된 IPv6 네트워크 번호입니다. 이 인수는 RFC 2373에 기술된 형식이어야 합니다. 즉 콜론 사이에 16비트 값을 사용하는 16진수로 주소를 지정합니다.
/prefix-length	(선택 사항) IPv6 접두사의 길이입니다. 접두사(주소의 네트워크 부분)를 구성하는 상위 연속 비트 수를 나타내는 10진수 값입니다. 10진수 값 앞에 슬래시가 표시되어야 합니다.
longer-prefixes	(선택 사항) 지정된 경로 및 보다 구체적인 경로를 표시합니다.
labels	(선택 사항) 주소 패밀리별로 이 네이버에 적용되는 정책을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 접두사 3FFE:500::/24에 대한 정보를 표시하는 **show bgp ipv6 unicast** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp ipv6 unicast 3FFE:500::/24
BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
  6175 7580 2500
```

```
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
> show bgp ipv6 unicast
BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, h history, * valid, > best, i -
internal,
             r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

show bgp ipv4/ipv6 unicast community

IPv4 또는 IPv6 BGP(Border Gateway Protocol) 라우팅 테이블에 있는 항목을 표시하려면 **show bgp ipv4 unicast community** 또는 **show bgp ipv6 unicast community** 명령을 각각 사용합니다.

show bgp {**ipv4** | **ipv6**} **unicast community** [*community-number*] [**exact-match**] [**local-as** | **no-advertise** | **no-export**]

unicast	IPv4 또는 IPv6 유니캐스트 주소 접두사를 지정합니다.
community-number	(선택 사항) 유효한 값은 1~4294967295의 커뮤니티 번호 또는 AA:NN(자동 시스템:커뮤니티 번호, 2바이트 번호)입니다.
exact-match	(선택 사항) 정확히 일치하는 항목이 있는 경로만 표시합니다.
local-as	(선택 사항) 로컬 자동 시스템(잘 알려진 커뮤니티) 외부로 전송되지 않는 경로만 표시합니다.
no-advertise	(선택 사항) 피어(잘 알려진 커뮤니티)로 보급되지 않는 경로만 표시합니다.
no-export	(선택 사항) 로컬 자동 시스템(잘 알려진 커뮤니티) 외부로 내보낼 수 없는 경로만 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp ipv6 unicast community** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
      Network             Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64       ::                                   0 32768 i
*> 2001:0DB8:0:1:1::/80      ::                                   0 32768 ?
*> 2001:0DB8:0:2::/64        2001:0DB8:0:3::2                        0 2 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:3::2                        0 2 ?
* 2001:0DB8:0:3::1/64        2001:0DB8:0:3::2                        0 2 ?
*>                       ::                                  0 32768 ?
*> 2001:0DB8:0:4::/64        2001:0DB8:0:3::2                        0 2 ?
```

```
*> 2001:0DB8:0:5::1/64       ::                                      0 32768 ?
*> 2001:0DB8:0:6::/64        2000:0:0:3::2                           0 2 3 i
*> 2010::/64                 ::                                      0 32768 ?
*> 2020::/64                 ::                                      0 32768 ?
*> 2030::/64                 ::                                      0 32768 ?
*> 2040::/64                 ::                                      0 32768 ?
*> 2050::/64                 ::                                      0 32768 ?
```

show bgp ipv4/ipv6 unicast community-list

IPv4 또는 IPv6 BGP(Border Gateway Protocol) 커뮤니티 목록에서 허용하는 경로를 표시하려면 **show bgp ipv4 unicast community-list** 또는 **show bgp ipv6 unicast community-list** 명령을 각각 사용합니다.

show bgp {**ipv4** | **ipv6**} **unicast community-list** {*number* | *name*} [**exact-match**]

unicast	IPv4 또는 IPv6 유니캐스트 주소 접두사를 지정합니다.
number	1~199의 커뮤니티 목록 번호입니다.
name	커뮤니티 목록 이름입니다.
exact-match	(선택 사항) 정확히 일치하는 항목이 있는 경로만 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 커뮤니티 목록 번호 3에 대한 **show bgp ipv6 unicast community-list** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp ipv6 unicast community-list 3
BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

    Network                Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64     2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:1:1::/80   2001:0DB8:0:3::1                         0 1 i
*> 2001:0DB8:0:2::1/64    ::                                     0 32768 i
*> 2001:0DB8:0:2:1::/80   ::                                     0 32768 ?
* 2001:0DB8:0:3::2/64     2001:0DB8:0:3::1                         0 1 ?
*>                       ::                                   0 32768 ?
*> 2001:0DB8:0:4::2/64    ::                                     0 32768 ?
*> 2001:0DB8:0:5::/64     2001:0DB8:0:3::1                         0 1 ?
*> 2010::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2020::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2030::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2040::/64              2001:0DB8:0:3::1                         0 1 ?
*> 2050::/64              2001:0DB8:0:3::1                         0 1 ?
```

show bgp ipv4/ ipv6 unicast neighbors

네이버에 대한 IPv4 또는 IPv6 BGP(Border Gateway Protocol) 연결에 관한 정보를 표시하려면 **show bgp ipv4 unicast neighbors** 또는 **show bgp ipv6 neighbors** 명령을 사용합니다.

show bgp {**ipv4** | **ipv6**} **unicast neighbors** [*ip-address*] [**received-routes** | **routes** | **advertised-routes** | **paths** *regular-expression*]

unicast	IPv4 또는 IPv6 유니캐스트 주소 접두사를 지정합니다.
ip-address	(선택 사항) Ipv4 또는 IPv6 BGP 발신 네이버의 주소입니다. 이 인수를 생략하면 모든 IPv4 또는 IPv6 네이버가 표시됩니다. IPv6 주소는 RFC 2373에 나와 있는 형식이어야 합니다. 즉, 콜론 사이의 16비트 값을 사용하여 16진수로 주소를 지정해야 합니다.
received-routes	(선택 사항) 지정된 네이버에서 수신된 모든 경로(허용 및 거부 모두)를 표시합니다.
routes	(선택 사항) 수신되고 허용된 모든 경로를 표시합니다. 이는 received-routes 키워드 출력의 하위 집합입니다.
advertised-routes	(선택 사항) 네트워킹 디바이스에서 네이버로 알리는 모든 경로를 표시합니다.
paths*regular-expression*	(선택 사항) 수신된 경로와 일치시키는 데 사용되는 정규식입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp ipv6 unicast neighbors** 명령의 샘플 출력입니다.

```
> show bgp ipv6 unicast neighbors
BGP neighbor is 3FFE:700:20:1::11,  remote AS 65003, external link
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 31306 messages, 20 notifications, 0 in queue
```

```
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 ***5: show bgp ipv4/ ipv6 unicast neighbors*** 필드

필드	설명
BGP neighbor	BGP 네이버의 IP 주소 및 자동 시스템 번호입니다. 네이버가 라우터와 동일한 자동 시스템에 있는 경우 둘 사이의 링크는 내부 링크입니다. 그렇지 않으면 외부로 간주됩니다.
remote AS	네이버의 자동 시스템 번호입니다.
internal link	이 피어가 iBGP(내부 Border Gateway Protocol) 피어임을 나타냅니다.
BGP version	원격 라우터와 통신하는 데 사용되는 BGP 버전입니다. 네이버의 라우터 ID(IP 주소)도 지정됩니다.
remote router ID	마침표로 구분된 4개의 옥텟으로 작성되는 32비트 숫자입니다(점으로 구분된 10진수 형식).
BGP state	이 BGP 연결의 상태를 나타냅니다.

필드	설명
up for	기본 TCP 연결이 존재한 기간입니다.
Last read	BGP에서 이 네이버의 메시지를 마지막으로 읽은 시간입니다.
hold time	피어의 메시지 간에 경과할 수 있는 최대 기간입니다.
keepalive interval	TCP 연결이 유지되도록 킵얼라이브 패킷을 전송할 시간 간격입니다.
Neighbor capabilities	이 네이버에서 보급 및 수신된 BGP 기능입니다.
Route refresh	네이버가 경로 새로 고침 기능을 사용하여 동적 소프트 재설정을 지원함을 나타냅니다.
Address family IPv6 Unicast	BGP 피어가 IPv6 연결 정보를 교환함을 나타냅니다.
Received	킵얼라이브 메시지를 포함하여 이 피어에서 수신된 총 BGP 메시지 수입니다.
notifications	피어에서 수신된 오류 메시지 수입니다.
Sent	킵얼라이브 메시지를 포함하여 이 피어로 전송된 총 BGP 메시지 수입니다.
notifications	라우터에서 이 피어로 전송한 오류 메시지 수입니다.
advertisement runs	최소 알림 간격 값입니다.
For address family	다음 필드에서 참조하는 주소 패밀리입니다.
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
neighbor version	소프트웨어에서 전송한 패킷과 이 네이버로 전송해야 하는 패킷을 추적하는 데 사용하는 번호입니다.
Route refresh request	이 네이버에서 전송 및 수신된 경로 새로 고침 요청 수입니다.
Community attribute(샘플 출력에 표시되지 않음)	이 네이버에 대해 neighbor send-community 명령이 구성되어 있는 경우 표시됩니다.
Inbound path policy(샘플 출력에 표시되지 않음)	인바운드 필터 목록 또는 경로 맵이 구성되어 있는지 여부를 나타냅니다.
Outbound path policy(샘플 출력에 표시되지 않음)	아웃바운드 필터 목록, 경로 맵 또는 표시 안 함 해제 맵이 구성되어 있는지 여부를 나타냅니다.

필드	설명
bgp-in(샘플 출력에 표시되지 않음)	IPv6 유니캐스트 주소 패밀리에 대한 인바운드 업데이트 접두사 필터 목록의 이름입니다.
aggregate(샘플 출력에 표시되지 않음)	IPv6 유니캐스트 주소 패밀리에 대한 아웃바운드 업데이트 접두사 필터 목록의 이름입니다.
uni-out(샘플 출력에 표시되지 않음)	IPv6 유니캐스트 주소군에 대한 아웃바운드 경로 맵의 이름입니다.
accepted prefixes	허용된 접두사 수입니다.
Prefix advertised	알림이 보내진 접두사 수입니다.
suppressed	표시되지 않는 접두사 수입니다.
withdrawn	취소된 접두사 수입니다.
history paths(샘플 출력에 표시되지 않음)	기록을 저장하기 위해 유지되는 경로 항목 수입니다.
Connections established	라우터가 TCP 연결을 설정하고 두 피어가 서로 BGP를 발신하도록 동의한 횟수입니다.
dropped	정상 조건이 실패하거나 중단된 횟수입니다.
Last reset	이 피어 세션이 마지막으로 재설정된 이후에 경과한 시간(시간:분:초)입니다.
Connection state	BGP 피어의 상태입니다.
unread input bytes	여전히 처리 중인 패킷의 바이트 수입니다.
Local host, Local port	로컬 라우터의 피어링 주소 및 포트입니다.
Foreign host, Foreign port	네이버의 피어링 주소입니다.
Event Timers	각 타이머의 시작 및 대기 모드 해제 수를 표시하는 테이블입니다.
snduna	로컬 호스트에서 전송했지만 확인 응답을 받지 않은 마지막 전송 시퀀스 번호입니다.
sndnxt	로컬 호스트가 다음에 전송할 시퀀스 번호입니다.
sndwnd	원격 호스트의 TCP 윈도우 크기입니다.

필드	설명
irs	초기 수신 시퀀스 번호입니다.
rcvnxt	로컬 호스트가 확인 응답을 받은 마지막 수신 시퀀스 번호입니다.
rcvwnd	로컬 호스트의 TCP 윈도우 크기입니다.
delrecvwnd	지연된 수신 창, 즉 로컬 호스트에서 연결에서 읽었지만 원격 호스트로 알림을 보낸 수신 창에서 아직 제거하지 않은 데이터입니다. 이 필드의 값은 rcvwnd 필드에 적용된 시점의 전체 크기 패킷보다 클 때까지 점진적으로 증가합니다.
SRTT	계산된 평균 왕복 시간 제한(밀리초)입니다.
RTTO	왕복 시간 제한(밀리초)입니다.
RTV	왕복 시간의 편차(밀리초)입니다.
KRTT	Karn 알고리즘을 사용하는 새 왕복 시간 제한(밀리초)입니다. 이 필드는 재전송된 패킷의 왕복 시간을 별도로 추적합니다.
minRTT	계산에 사용된 고정 값이 있는 기록된 최소 왕복 시간 제한(밀리초)입니다.
maxRTT	기록된 최대 왕복 시간 제한(밀리초)입니다.
ACK hold	로컬 호스트가 데이터를 "전송(piggyback)"하기 위해 확인 응답을 지연시키는 기간(밀리초)입니다.
Flags	BGP 패킷의 IP 우선 순위입니다.
Datagrams: Rcvd	네이버에서 수신된 업데이트 패킷 수입니다.
with data	데이터와 함께 수신된 업데이트 패킷 수입니다.
total data bytes	데이터의 총 바이트 수입니다.
Sent	전송된 업데이트 패킷 수입니다.
with data	데이터와 함께 전송된 업데이트 패킷 수입니다.
total data bytes	데이터의 총 바이트 수입니다.

다음은 **advertised-routes** 키워드와 함께 실행한 **show bgp ipv6 unicast neighbors** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes
BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                      0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2                        0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2                        0 3748 4697 i
```

다음은 **routes** 키워드와 함께 실행한 **show bgp ipv6 unicast neighbors** 명령의 샘플 출력입니다.

```
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes
BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                      0 293 3425 2500 i
*  2001:208::/35    3FFE:700:20:1::11                      0 293 7610 i
*  2001:218::/35    3FFE:700:20:1::11                      0 293 3425 4697 i
*  2001:230::/35    3FFE:700:20:1::11                      0 293 1275 3748 i
```

다음은 **paths** 키워드와 함께 실행한 **show bgp ipv6 neighbors** 명령의 샘플 출력입니다.

```
> show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
Address    Refcount Metric Path
0x6131D7DC        2      0 293 3425 2500 i
0x6132861C        2      0 293 7610 i
0x6131AD18        2      0 293 3425 4697 i
0x61324084        2      0 293 1275 3748 i
0x61320E0C        1      0 293 3425 2500 2497 i
0x61326928        1      0 293 3425 2513 i
0x61327BC0        2      0 293 i
0x61321758        1      0 293 145 i
0x61320BEC        1      0 293 3425 6509 i
0x6131AAF8        2      0 293 1849 2914 ?
0x61320FE8        1      0 293 1849 1273 209 i
0x613260A8        2      0 293 1849 i
0x6132586C        1      0 293 1849 5539 i
0x6131BBF8        2      0 293 1849 1103 i
0x6132344C        1      0 293 4554 1103 1849 1752 i
0x61324150        2      0 293 1275 559 i
0x6131E5AC        2      0 293 1849 786 i
0x613235E4        1      0 293 1849 1273 i
0x6131D028        1      0 293 4554 5539 8627 i
0x613279E4        1      0 293 1275 3748 4697 3257 i
0x61320328        1      0 293 1849 1273 790 i
0x6131EC0C        2      0 293 1275 5409 i
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 ***6: show bgp ipv6 neighbors paths*** 필드

필드	설명
Address	경로가 저장되는 내부 주소입니다.
Refcount	해당 경로를 사용하는 경로 수입니다.

필드	설명
Metric	경로에 대한 MED(Multi Exit Discriminator) 메트릭입니다. BGP 버전 2 및 3의 이 메트릭 값은 INTER_AS입니다.
Path	해당 경로에 대한 자동 시스템 경로로서, 해당 경로의 원본 코드가 뒤에 옵니다.

다음 **show bgp ipv6 neighbors** 명령의 샘플 출력에서는 IPv6 주소 2000:0:0:4::2에 대한 **received routes**를 보여줍니다.

```
> show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete

   Network                Next Hop           Metric LocPrf Weight Path
*> 2000:0:0:1::/64      2000:0:0:4::2                         0 2 1 i
*> 2000:0:0:2::/64      2000:0:0:4::2                         0 2 i
*> 2000:0:0:2:1::/80    2000:0:0:4::2                         0 2 ?
*> 2000:0:0:3::/64      2000:0:0:4::2                         0 2 ?
*  2000:0:0:4::1/64     2000:0:0:4::2                         0 2 ?
```

show bgp ipv4/ ipv6 unicast paths

데이터베이스의 모든 IPv4 또는 IPv6 BGP(Border Gateway Protocol) 경로를 표시하려면 **show bgp ipv4 unicast paths** 또는 **show bgp ipv6 unicast paths** 명령을 각각 사용합니다.

show bgp {**ipv4** | **ipv6**} **unicast paths** [*regular-expression*]

regular-expression	(선택 사항) 수신된 경로와 일치시키는 데 사용되는 정규식입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp ipv6 unicast paths** 명령의 샘플 출력입니다.

```
> show bgp ipv6 unicast paths
Address    Hash Refcount Metric Path
0x61322A78    0        2      0 i
0x6131C214    3        2      0 6346 8664 786 i
0x6131D600   13        1      0 3748 1275 8319 1273 209 i
0x613229F0   17        1      0 3748 1275 8319 12853 i
0x61324AE0   18        1      1 4554 3748 4697 5408 i
0x61326818   32        1      1 4554 5609 i
0x61324728   34        1      0 6346 8664 9009 ?
0x61323804   35        1      0 3748 1275 8319 i
0x61327918   35        1      0 237 2839 8664 ?
0x61320504   38        2      0 3748 4697 1752 i
0x61320988   41        2      0 1849 786 i
0x6132245C   46        1      0 6346 8664 4927 i
```

다음 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 ***7: Show bgp ipv4/ ipv6 unicast path*** 필드

필드	설명
Address	경로가 저장되는 내부 주소입니다.
Refcount	해당 경로를 사용하는 경로 수입니다.
Metric	경로에 대한 MED(Multi Exit Discriminator) 메트릭입니다. BGP 버전 2 및 3의 이 메트릭 값은 INTER_AS입니다.

필드	설명
Path	해당 경로에 대한 자동 시스템 경로로서, 해당 경로의 원본 코드가 뒤에 옵니다.

show bgp ipv4/ ipv6 unicast prefix-list

접두사 목록과 일치하는 경로를 표시하려면 **show bgp ipv4 prefix-list** 또는 **show bgp ipv6 prefix-list** 명령을 사용합니다.

show bgp {**ipv4** | **ipv6**} **unicast prefix-list** *name*

prefix-list*name*	지정된 접두사 목록입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp ipv6 prefix-list** 명령의 샘플 출력입니다.

```
> show bgp ipv6 unicast prefix-list pin
ipv6 prefix-list pin:
   count:4, range entries:3, sequences:5 - 20, refcount:2
   seq 5 permit 747::/16 (hit count:1, refcount:2)
   seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
   seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
   seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)
The ipv6 prefix-list match the following prefixes:
   seq 5: matches the exact match 747::/16
   seq 10:first 32 bits in prefix must match with a prefixlen of /64
   seq 15:first 32 bits in prefix must match with any prefixlen up to /128
   seq 20:first 16 bits in prefix must match with any prefixlen up to /124
```

show bgp ipv4/ ipv6 unicast regexp

자동 시스템(AS) 경로 정규식과 일치하는 IPv4 또는 IPv6 BGP(Border Gateway Protocol) 경로를 표시하려면 **show bgp ipv4 regexp** 또는 **show bgp ipv6 regexp** 명령을 사용합니다.

show bgp {**ipv4** | **ipv6**} **unicast regexp** *regular-expression*

regexp*regular-expression*	BGP 자동 시스템 경로와 일치시키는 데 사용되는 정규식입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 33으로 시작하거나 293을 포함하는 경로를 표시하는 **show bgp ipv6 unicast regexp** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp ipv6 unicast regexp ^33|293
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1                    0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
```

show bgp ipv4/ ipv6 unicast route-map

라우팅 테이블에서 설치하는 데 실패한 IPv4 또는 IPv6 BGP(Border Gateway Protocol) 경로를 표시하려면 **show bgp ipv4 unicast route-map** 또는 **show bgp ipv6 unicast route-map** 명령을 사용합니다.

show bgp {**ipv4** | **ipv6**} **unicast route-map** *name*

route-map*name*	일치시킬 지정된 경로 맵입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 rmap이라는 경로 맵에 대한 **show bgp ipv6 unicast route-map** 명령의 샘플 출력입니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp ipv6 unicast route-map rmap
BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i12:12::/64       2001:0DB8:101::1             0    100     50 ?
*>i12:13::/64       2001:0DB8:101::1             0    100     50 ?
*>i12:14::/64       2001:0DB8:101::1             0    100     50 ?
*>i543::/64         2001:0DB8:101::1             0    100     50 ?
```

show bgp ipv4/ ipv6 unicast summary

모든 IPv4 또는 IPv6 BGP(Border Gateway Protocol) 연결의 상태를 표시하려면 **show bgp ipv4 unicast summary** 또는 **show bgp ipv6 unicast summary** 명령을 각각 사용합니다.

show bgp {**ipv4** | **ipv6**} **unicast summary**

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp ipv6 unicast summary** 명령의 샘플 출력입니다.

```
> show bgp ipv6 unicast summary
BGP device identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
Neighbor          V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2  4    200    6869     6882        0    0     0  06:25:24  Active
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 ***8: show bgp ipv4/ ipv6 unicast summary*** 필드

필드	설명
BGP device identifier	네트워킹 디바이스의 IP 주소입니다.
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
main routing table version	기본 라우팅 테이블에 삽입된 BGP 데이터베이스의 마지막 버전입니다.
Neighbor	인접 항목의 IPv6 주소입니다.
V	해당 인접 항목으로 발신된 BGP 버전 번호입니다.
AS	자동 시스템입니다.
MsgRcvd	해당 인접 항목에서 수신된 BGP 메시지입니다.
MsgSent	해당 인접 항목으로 전송된 BGP 메시지입니다.
TblVer	해당 인접 항목으로 전송된 BGP 데이터베이스의 마지막 버전입니다.

필드	설명
InQ	처리 대기 중인 해당 인접 항목의 메시지 수입니다.
OutQ	해당 인접 항목으로 전송 대기 중인 메시지 수입니다.
Up/Down	BGP 세션이 Established 상태 또는 현재 상태(Established가 아닌 경우)로 유지된 기간입니다.
State/PfxRcd	디바이스가 인접 항목에서 수신한 BGP 세션의 현재 상태/접두사 수입니다. 최대 수(neighbor maximum-prefix 명령으로 설정)에 도달하면 문자열 "PfxRcd"가 항목에 표시되고, 인접 항목이 종료되며, 연결이 Idle 상태로 전환됩니다. Idle 상태의 An(Admin) 항목은 neighbor shutdown 명령을 통해 연결이 종료되었음을 나타냅니다.

show bgp neighbors

네이버에 대한 BGP(Border Gateway Protocol) 및 TCP 연결에 관한 정보를 표시하려면 show bgp neighbors 명령을 사용합니다.

show bgp neighbors [**slow** | *ip-address* [**advertised-routes** | **paths** [*reg-exp*] | **policy** [**detail**] | **received prefix-filter** | **received-routes** | **routes**]]

slow	(선택 사항) 동적으로 구성된 느린 피어에 대한 정보를 표시합니다.
ip-address	(선택 사항) IPv4 네이버에 대한 정보를 표시합니다. 이 인수를 생략하면 모든 네이버에 대한 정보가 표시됩니다.
advertised-routes	(선택 사항) 네이버에 보급된 모든 경로를 표시합니다.
paths [*reg-exp*]	(선택 사항) 지정된 네이버에서 학습된 자동 시스템 경로를 표시합니다. 선택적 정규식을 사용하여 출력을 필터링할 수 있습니다.
policy	(선택 사항) 주소군별로 이 네이버에 적용되는 정책을 표시합니다.
detail	(선택 사항) 경로 맵, 접두사 목록, 커뮤니티 목록, ACL(Access Control List: 액세스 제어 목록), 자동 시스템 경로 필터 목록 등 자세한 정책 정보를 표시합니다.
received prefix-filter	(선택 사항) 지정된 네이버에서 전송된 접두사 목록(ORF(아웃바운드 경로 필터))를 표시합니다.
received-routes	(선택 사항) 지정된 네이버에서 수신된 모든 경로(허용 및 거부 모두)를 표시합니다.
routes	(선택 사항) 수신되고 허용된 모든 경로를 표시합니다. 이 키워드를 입력한 경우에 표시되는 출력은 **received-routes** 키워드로 표시되는 출력의 하위 집합입니다.

이 명령의 출력은 모든 네이버에 대한 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show bgp neighbors 명령을 사용하여 네이버 세션에 대한 BGP 및 TCP 연결 정보를 표시할 수 있습니다. BGP의 경우 자세한 네이버 특성, 기능, 경로 및 접두사 정보가 포함됩니다. TCP의 경우 BGP 네이버 세션 설정 및 유지 관리와 관련된 통계가 포함됩니다.

접두사 활동은 알려지고 취소된 접두사 수를 기반으로 표시됩니다. 정책 거부는 알려졌으나 출력에 표시된 기능 또는 특성에 따라 무시된 경로 수를 표시합니다.

다음 예에서는 10.108.50.2에 있는 BGP 네이버에 대한 출력을 보여줍니다. 이 네이버는 iBGP(내부 BGP) 피어입니다. 이 네이버는 경로 새로 고침 및 정상 재시작 기능을 지원합니다.

```
> show bgp neighbors 10.108.50.2
BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds

 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                               Sent       Rcvd
  Prefix activity:             ----       ----
    Prefixes Current:             0          0
    Prefixes Total:               0          0
    Implicit Withdraw:            0          0
    Explicit Withdraw:            0          0
    Used as bestpath:           n/a          0
    Used as multipath:          n/a          0

                                  Outbound    Inbound
  Local Policy Denied Prefixes:   --------    -------
    Total:                               0          0

  Number of NLRIs in the update sent: max 0, min 0

  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
```

```
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0

iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539

SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6

Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

다음 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다. 앞에 별표 문자(*)가 있는 필드는 카운터 값이 0이 아닌 경우에만 표시됩니다.

표 ***9: show bgp neighbors*** 필드

필드	설명
BGP neighbor	BGP 네이버의 IP 주소 및 자동 시스템 번호입니다.
remote AS	네이버의 자동 시스템 번호입니다.
local AS 300 no-prepend(화면에 표시되지 않음)	로컬 자동 시스템 번호가 수신된 외부 경로 앞에 추가되어 있지 않은지 확인합니다. 이 출력은 자동 시스템을 마이그레이션할 때 로컬 자동 시스템 숨기기를 지원합니다.
internal link	"internal link"는 iBGP 네이버에 대해 표시됩니다. "external link"는 eBGP(외부 BGP) 네이버에 대해 표시됩니다.
BGP version	원격 라우터와 통신하는 데 사용되는 BGP 버전입니다.
remote router ID	네이버의 IP 주소입니다.
BGP state	세션 협상의 FSM(Finite State Machine) 단계입니다.
up for	기본 TCP 연결이 존재한 기간(hhmmss)입니다.
Last read	BGP가 이 네이버에서 마지막으로 메시지를 수신한 이후에 경과한 시간(hhmmss)입니다.

필드	설명
last write	BGP가 이 네이버에 마지막으로 메시지를 전송한 이후에 경과한 시간(hhmmss)입니다.
hold time	BGP가 메시지를 수신하지 않고 이 네이버와의 세션을 유지할 시간(초)입니다.
keepalive interval	킵얼라이브 메시지가 이 네이버로 전송되는 시간 간격(초)입니다.
Neighbor capabilities	이 네이버에서 보급 및 수신된 BGP 기능입니다. 두 라우터 간에 기능이 성공적으로 교환된 경우 “advertised and received”가 표시됩니다.
Route Refresh	경로 새로 고침 기능의 상태입니다.
Graceful Restart Capability	정상 재시작 기능의 상태입니다.
Address family IPv4 Unicast	이 네이버의 IP 버전 4 유니캐스트 관련 속성입니다.
Message statistics	메시지 유형별로 구성된 통계입니다.
InQ depth is	입력 대기열의 메시지 수입니다.
OutQ depth is	출력 대기열의 메시지 수입니다.
Sent	전송된 총 메시지 수입니다.
Received	수신된 총 메시지 수입니다.
Opens	전송되거나 수신된 열어 본 메시지 수입니다.
notifications	전송되거나 수신된 알림(오류) 메시지 수입니다.
Updates	전송되거나 수신된 업데이트 메시지 수입니다.
Keepalives	전송되거나 수신된 킵얼라이브 메시지 수입니다.
Route Refresh	전송되거나 수신된 경로 새로 고침 요청 메시지 수입니다.
Total	전송되거나 수신된 총 메시지 수입니다.
Default minimum time between...	알림 전송 간의 시간 간격(초)입니다.
For address family:	다음 필드에서 참조하는 주소 패밀리입니다.

필드	설명
BGP table version	테이블의 내부 버전 번호입니다. 이 번호는 테이블이 변경될 때마다 증가합니다.
neighbor version	소프트웨어에서 전송한 패킷과 전송해야 하는 패킷을 추적하는 데 사용하는 번호입니다.
update-group	이 주소 패밀리에 대한 업데이트 그룹 멤버 번호입니다.
Prefix activity	이 주소 패밀리에 대한 접두사 통계입니다.
Prefixes current	이 주소 패밀리에 대해 허용된 접두사 수입니다.
Prefixes total	수신된 총 접두사 수입니다.
Implicit Withdraw	접두사가 취소되고 다시 알려진 횟수입니다.
Explicit Withdraw	접두사가 더 이상 실행할 수 없어 취소된 횟수입니다.
Used as bestpath	최상의 경로로 설치된 수신된 접두사 수입니다.
Used as multipath	다중 경로로 설치된 수신된 접두사 수입니다.
* Saved (soft-reconfig)	소프트 재구성을 지원하는 네이버와 함께 수행된 소프트 재설정 횟수입니다. 이 필드는 카운터 값이 0이 아닌 경우에만 표시됩니다.
* History paths	이 필드는 카운터 값이 0이 아닌 경우에만 표시됩니다.
* Invalid paths	잘못된 경로 수입니다. 이 필드는 카운터 값이 0이 아닌 경우에만 표시됩니다.
Local Policy Denied Prefixes	로컬 정책 컨피그레이션으로 인해 거부된 접두사입니다. 인바운드 및 아웃바운드 정책 거부 시 카운터가 업데이트됩니다. 이 머리글 아래의 필드는 카운터 값이 0이 아닌 경우에만 표시됩니다.
* route-map	인바운드 및 아웃바운드 route-map 정책 거부를 표시합니다.
* filter-list	인바운드 및 아웃바운드 filter-list 정책 거부를 표시합니다.
* prefix-list	인바운드 및 아웃바운드 prefix-list 정책 거부를 표시합니다.
* AS_PATH too long	아웃바운드 AS-path length 정책 거부를 표시합니다.
* AS_PATH loop	아웃바운드 AS-path loop 정책 거부를 표시합니다.
* AS_PATH confed info	아웃바운드 confederation 정책 거부를 표시합니다.

필드	설명
* AS_PATH contains AS 0	AS(자동 시스템) 0에 대한 아웃바운드 거부를 표시합니다.
* NEXT_HOP Martian	아웃바운드 martian 거부를 표시합니다.
* NEXT_HOP non-local	아웃바운드 non-local next-hop 거부를 표시합니다.
* NEXT_HOP is us	아웃바운드 next-hop-self 거부를 표시합니다.
* CLUSTER_LIST loop	아웃바운드 cluster-list loop 거부를 표시합니다.
* ORIGINATOR loop	로컬 시작 루프에 대한 아웃바운드 거부를 표시합니다.
* unsuppress-map	unsuppress-map으로 인한 인바운드 거부를 표시합니다.
* advertise-map	advertise-map으로 인한 인바운드 거부를 표시합니다.
* Well-known Community	잘 알려진 커뮤니티에 대한 인바운드 거부를 표시합니다.
* SOO loop	site-of-origin으로 인한 인바운드 거부를 표시합니다.
* Bestpath from this peer	로컬 라우터에서 가져온 최상의 경로로 인한 인바운드 거부를 표시합니다.
* Suppressed due to dampening	감소 상태에 있는 네이버 또는 링크로 인한 인바운드 거부를 표시합니다.
* Bestpath from iBGP peer	iBGP 네이버에서 가져온 최상의 경로로 인한 인바운드 거부를 표시합니다.
* Incorrect RIB for CE	CE 라우터의 RIB 오류로 인한 인바운드 거부를 표시합니다.
* BGP distribute-list	배포 목록으로 인한 인바운드 거부를 표시합니다.
Number of NLRIs...	업데이트의 네트워크 레이어 연결 특성 수입니다.
Connections established	TCP와 BGP 간의 연결이 성공적으로 설정된 횟수입니다.
dropped	유효 세션이 실패하거나 중단된 횟수입니다.
Last reset	이 피어링 세션이 마지막으로 재설정된 이후에 경과한 시간입니다. 재설정 사유가 이 줄에 표시됩니다.

필드	설명
External BGP neighbor may be... (화면에 표시되지 않음)	BGP TTL 보안 검사가 활성화되었음을 나타냅니다. 로컬 및 원격 피어를 구분할 수 있는 최대 홉 수가 이 줄에 표시됩니다.
Connection state	BGP 피어의 연결 상태입니다.
Connection is ECN Disabled	명시적인 혼잡 알림 상태(enabled 또는 disabled)입니다.
Local host: 10.108.50.1, Local port: 179	로컬 BGP 스피커의 IP 주소입니다. BGP 포트 번호는 179입니다.
Foreign host: 10.108.50.2, Foreign port: 42698	네이버 주소와 BGP 대상 포트 번호입니다.
Enqueued packets for retransmit:	TCP에서 재전송 대기 중인 패킷 수입니다.
Event Timers	TCP 이벤트 타이머입니다. 시작 및 대기 모드 해제(만료된 타이머)에 대한 카운터가 제공됩니다.
Retrans	패킷이 재전송된 횟수입니다.
TimeWait	재전송 타이머 만료 대기 시간입니다.
AckHold	확인 응답 보류 타이머입니다.
SendWnd	전송 기간입니다.
KeepAlive	킵얼라이브 패킷 수입니다.
GiveUp	확인 응답이 없어 패킷이 삭제된 횟수입니다.
PmtuAger	경로 MTU 검색 타이머입니다.
DeadWait	정지된 세그먼트에 대한 만료 타이머입니다.
iss:	초기 패킷 전송 시퀀스 번호입니다.
snduna	확인 응답을 받지 않은 마지막 전송 시퀀스 번호입니다.
sndnxt:	전송할 다음 패킷 시퀀스 번호입니다.
sndwnd:	원격 네이버의 TCP 윈도우 크기입니다.

필드	설명
irs:	초기 패킷 수신 시퀀스 번호입니다.
rcvnxt:	로컬로 확인 응답을 받은 마지막 수신 시퀀스 번호입니다.
rcvwnd:	로컬 호스트의 TCP 윈도우 크기입니다.
delrcvwnd:	지연된 수신 창, 즉 로컬 호스트에서 연결에서 읽었지만 원격 호스트로 보급한 수신 창에서 아직 제거하지 않은 데이터입니다. 이 필드의 값은 rcvwnd 필드에 적용된 시점의 전체 크기 패킷보다 클 때까지 점진적으로 증가합니다.
SRTT:	계산된 평균 왕복 시간 제한입니다.
RTTO:	왕복 시간 제한입니다.
RTV:	왕복 시간의 편차입니다.
KRTT:	새 왕복 시간 제한(Karn 알고리즘 사용)입니다. 이 필드는 재전송된 패킷의 왕복 시간을 별도로 추적합니다.
minRTT:	기록된 최소 왕복 시간 제한(계산에 사용된 고정 값)입니다.
maxRTT:	기록된 최대 왕복 시간 제한입니다.
ACK hold:	로컬 호스트가 추가 데이터를 전달(piggyback)하기 위해 확인 응답을 지연시킬 기간입니다.
IP Precedence value:	BGP 패킷의 IP 우선 순위입니다.
Datagrams	네이버에서 수신된 업데이트 패킷 수입니다.
Rcvd:	수신된 패킷 수입니다.
with data	데이터와 함께 전송된 업데이트 패킷 수입니다.
total data bytes	수신된 총 데이터(바이트)입니다.
Sent	전송된 업데이트 패킷 수입니다.
Second Congestion	혼잡으로 인해 전송된 두 번째 재전송 수입니다.
Datagrams: Rcvd	네이버에서 수신된 업데이트 패킷 수입니다.
out of order:	잘못된 시퀀스로 수신된 패킷 수입니다.
with data	데이터와 함께 수신된 업데이트 패킷 수입니다.

필드	설명
Last reset	이 피어링 세션이 마지막으로 재설정된 이후에 경과한 시간입니다.
unread input bytes	여전히 처리 중인 패킷의 바이트 수입니다.
retransmit	재전송된 패킷 수입니다.
fastretransmit	재전송 타이머가 만료되기 전에 잘못된 순서의 세그먼트에 대해 재전송된 중복 확인 응답 수입니다.
partialack	부분 확인 응답을 위한 재전송(후속 확인 응답 전의 전송 또는 후속 확인 응답이 없는 전송) 수입니다.

다음 예에서는 172.16.232.178 네이버에만 알려진 경로를 표시합니다. 출력의 설명을 보려면 **show bgp** 명령을 참조하십시오.

```
> show bgp neighbors 172.16.232.178 advertised-routes
BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

다음은 **paths** 키워드와 함께 입력된 **show bgp neighbors** 명령의 샘플 출력입니다.

```
> show bgp neighbors 172.29.232.178 paths ^10
Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

다음 표는 각 필드에 대해 설명합니다.

표 ***10: show bgp neighbors paths*** 필드

필드	설명
Address	경로가 저장되는 내부 주소입니다.
Refcount	해당 경로를 사용하는 경로 수입니다.
Metric	경로에 대한 MED(Multi Exit Discriminator) 메트릭입니다. BGP 버전 2 및 3의 이 메트릭 이름은 INTER_AS입니다.
Path	해당 경로에 대한 자동 시스템 경로로서, 해당 경로의 원본 코드가 뒤에 옵니다.

다음 예에서는 10.0.0.0 네트워크가 192.168.20.72 네이버에서 수신한 모든 경로를 필터링하는 접두사 목록을 보여 줍니다.

```
> show bgp neighbors 192.168.20.72 received prefix-filter
Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

다음 샘플 출력에서는 192.168.1.2에 있는 네이버에 적용되는 정책을 보여줍니다. 네이버 디바이스에 구성된 정책이 출력에 표시됩니다.

```
> show bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

다음은 172.16.1.2에 있는 BGP 네이버에 대해 BGP TCP 경로 MTU(Maximum Transmission Unit) 검색이 활성화되어 있는지 확인하는 **show bgp neighbors** 명령의 샘플 출력입니다.

```
> show bgp neighbors 172.16.1.2
BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
....
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
...
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
....
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

show bgp paths

데이터베이스의 모든 BGP 경로를 표시하려면 **show bgp paths** 명령을 사용합니다.

show bgp paths [*regexp*]

regexp	BGP 자동 시스템 경로와 일치시킬 정규식입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp paths** 명령의 샘플 출력입니다.

```
> show bgp paths
Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

다음 표는 각 필드에 대해 설명합니다.

표 ***11: show bgp paths*** 필드

필드	설명
Address	경로가 저장되는 내부 주소입니다.
Hash	경로가 저장되는 해시 버킷입니다.
Refcount	해당 경로를 사용하는 경로 수입니다.
Metric	경로에 대한 MED(Multi Exit Discriminator) 메트릭입니다. BGP 버전 2 및 3의 이 메트릭 값은 INTER_AS입니다.
Path	해당 경로에 대한 자동 시스템 경로로서, 해당 경로의 원본 코드가 뒤에 옵니다.

show bgp prefix-list

접두사 목록 또는 접두사 목록 항목에 대한 정보를 표시하려면 **show bgp prefix-list** 명령을 사용합니다.

show bgp prefix-list [**detail** | **summary**] [*prefix-list-name* [**seq** *sequence-number* | *network/length* [**longer** | **first-match**]]]

detail | **summary**	(선택 사항) 모든 접두사 목록에 대한 상세 정보 및 요약 정보를 표시합니다.
first-match	(선택 사항) 지정된 네트워크/길이와 일치하는 지정된 접두사 목록의 첫 번째 항목을 표시합니다.
longer	(선택 사항) 지정된 네트워크/길이와 일치하거나 더 구체적으로 지정된 접두사 목록의 모든 항목을 표시합니다.
network/length	(선택 사항) 이 네트워크 주소 및 넷마스크(비트)를 사용하는 지정된 접두사 목록의 모든 항목을 표시합니다.
prefix-list-name	(선택 사항) 특정 접두사 목록의 항목을 표시합니다.
seq*sequence-number*	(선택 사항) 지정된 접두사 목록에서 지정된 시퀀스 번호가 있는 접두사 목록 항목만 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 test라는 접두사 목록에 대한 세부사항이 포함된 **show bgp prefix-list** 명령의 출력을 보여줍니다.

```
> show bgp prefix-list detail test
ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

show bgp regexp

자동 시스템 경로 정규식과 일치하는 경로를 표시하려면 **show bgp regexp** 명령을 사용합니다.

show bgp regexp *regexp*

regexp	BGP 자동 시스템 경로와 일치시킬 정규식입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp regexp** 명령의 샘플 출력입니다.

```
> show bgp regexp 108$
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                           0 109 108 ?
*  172.16.1.0       172.16.72.30                           0 109 108 ?
*  172.16.11.0      172.16.72.30                           0 109 108 ?
*  172.16.14.0      172.16.72.30                           0 109 108 ?
*  172.16.15.0      172.16.72.30                           0 109 108 ?
*  172.16.16.0      172.16.72.30                           0 109 108 ?
*  172.16.17.0      172.16.72.30                           0 109 108 ?
*  172.16.18.0      172.16.72.30                           0 109 108 ?
*  172.16.19.0      172.16.72.30                           0 109 108 ?
*  172.16.24.0      172.16.72.30                           0 109 108 ?
*  172.16.29.0      172.16.72.30                           0 109 108 ?
*  172.16.30.0      172.16.72.30                           0 109 108 ?
*  172.16.33.0      172.16.72.30                           0 109 108 ?
*  172.16.35.0      172.16.72.30                           0 109 108 ?
*  172.16.36.0      172.16.72.30                           0 109 108 ?
*  172.16.37.0      172.16.72.30                           0 109 108 ?
*  172.16.38.0      172.16.72.30                           0 109 108 ?
*  172.16.39.0      172.16.72.30                           0 109 108 ?
```

show bgp rib-failure

RIB(Routing Information Base) 테이블에 설치하지 못한 BGP(Border Gateway Protocol) 경로를 표시하려면 **show bgp rib-failure** 명령을 사용합니다.

show bgp rib-failure

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show bgp rib-failure** 명령의 샘플 출력입니다.

```
> show bgp rib-failure
Network           Next Hop                    RIB-failure   RIB-NH Matches
10.1.15.0/24      10.1.35.5          Higher admin distance             n/a
10.1.16.0/24      10.1.15.1          Higher admin distance             n/a
```

다음 표는 각 필드에 대해 설명합니다.

표 ***12: show bgp rib-failure*** 필드

필드	설명
Network	네트워크 엔터티의 IP 주소입니다.
Next Hop	대상 네트워크로 패킷을 전달할 때 사용되는 다음 시스템의 IP 주소입니다. 0.0.0.0 항목은 라우터에 이 네트워크에 대한 일부 비 BGP 경로가 있음을 의미합니다.
RIB-failure	RIB 오류 원인입니다. 더 높은 관리 영역은 고정 경로와 같은 더 나은(더 낮은) 관리 영역이 있는 경로가 IP 라우팅 테이블에 이미 있음을 의미합니다.
RIB-NH Matches	더 높은 관리 영역이 RIB-failure 열에 표시되고 사용 중인 주소군에 대해 **bgp suppress-inactive**가 구성된 경우에만 적용되는 경로 상태입니다. 다음 세 가지 선택 항목이 있습니다. • Yes - RIB의 경로에 BGP 경로와 동일한 다음 홉이 있거나 다음 홉이 BGP 다음 홉과 동일한 인접성으로 재귀적으로 작동함을 의미합니다. • No - RIB의 다음 홉이 BGP 경로의 다음 홉과 다르게 재귀적으로 작동함을 의미합니다. • n/a - 사용 중인 주소군에 대해 **bgp suppress-inactive**가 구성되어 있지 않습니다.

show bgp summary

모든 BGP(Border Gateway Protocol) 연결의 상태를 표시하려면 **show bgp summary** 명령을 사용합니다.

show bgp summary

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show bgp summary 명령은 모든 BGP 네이버 연결에 대한 BGP 경로, 접두사 및 특성 정보를 표시하는 데 사용됩니다.

접두사는 IP 주소와 네트워크 마스크입니다. 이는 전체 네트워크, 네트워크의 하위 집합 또는 단일 호스트 경로를 나타낼 수 있습니다. 경로는 지정된 대상에 대한 경로입니다. 기본적으로 BGP는 각 대상에 대해 단일 경로만 설치합니다. 다중 경로가 구성된 경우 BGP는 각 다중 모드 경로에 대한 경로 항목을 설치하며, 다중 모드 경로 중 하나의 경로만 최상의 경로로 표시됩니다.

BGP 특성 및 캐시 항목은 개별적으로 표시되거나 함께 표시됩니다. 함께 표시될 경우 최상의 경로 선택 프로세스가 영향을 받습니다. 이 출력의 필드는 관련 BGP 기능이 구성되어 있거나 특성이 수신된 경우에 표시됩니다. 메모리 사용량은 바이트 단위로 표시됩니다.

다음은 Privileged EXEC 모드에서 실행된 **show bgp summary** 명령의 샘플 출력입니다.

```
> show bgp summary
BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

다음 표는 각 필드에 대해 설명합니다.

표 ***13: show bgp summary*** 필드

필드	설명
BGP router identifier	우선 순위 및 가용성 순으로 된 라우터 식별자, 루프백 주소 또는 최상위 IP 주소입니다.
BGP table version	BGP 데이터베이스의 내부 버전 번호입니다.
main routing table version	기본 라우팅 테이블에 삽입된 BGP 데이터베이스의 마지막 버전입니다.
...network entries	BGP 데이터베이스에 있는 고유한 접두사 항목 수입니다.
...using ... bytes of memory	같은 줄에 표시된 경로, 접두사 또는 특성 항목에 사용되는 메모리(바이트)입니다.
...path entries using	BGP 데이터베이스에 있는 경로 항목 수입니다. 지정된 대상에 대해 단일 경로 항목만 설치됩니다. 다중 경로가 구성된 경우 다중 모드 경로의 각 경로에 대해 경로 항목이 설치됩니다.
...multipath network entries using	지정된 대상에 대해 설치된 다중 경로 항목 수입니다.
* ...BGP path/bestpath attribute entries using	경로가 최상의 경로로 선택된 고유한 BGP 특성 조합 수입니다.
* ...BGP rrinfo entries using	고유한 ORIGINATOR 및 CLUSTER_LIST 특성 조합 수입니다.
...BGP AS-PATH entries using	고유한 AS_PATH 항목 수입니다.
...BGP community entries using	고유한 BGP 커뮤니티 특성 조합 수입니다.
*...BGP extended community entries using	고유한 확장 커뮤니티 특성 조합 수입니다.
BGP route-map cache entries using	BGP route-map 일치 및 set 절 조합 수입니다. 0 값은 경로 캐시가 비어 있음을 나타냅니다.
...BGP filter-list cache entries using	AS-path 액세스 목록 허용 또는 거부 문과 일치하는 filter-list 항목 수입니다. 0 값은 filter-list 캐시가 비어 있음을 나타냅니다.

필드	설명
BGP advertise-bit cache entries using	보급된 bitfield 항목 수 및 관련 메모리 사용량입니다. 비트 필드 항목은 접두사가 동료에게 보급될 때 생성되는 정보 조각(1비트)을 나타냅니다. 보급된 비트 캐시는 필요할 때 동적으로 생성됩니다.
...received paths for inbound soft reconfiguration	인바운드 소프트 재컨피그레이션에 대해 수신 및 저장된 경로 수입니다.
BGP using...	BGP 프로세스에서 사용된 총 메모리 양(바이트)입니다.
Dampening enabled...	BGP 감소가 활성화되었음을 나타냅니다. 누적된 페널티가 있는 경로 수 및 감소된 경로 수가 이 줄에 표시됩니다.
BGP activity...	경로 또는 접두사에 대해 메모리가 할당되거나 해제된 횟수를 표시합니다.
Neighbor	네이버의 IP 주소입니다.
V	네이버로 발신된 BGP 버전 번호입니다.
AS	자동 시스템 번호입니다.
MsgRcvd	네이버에서 수신된 메시지 수입니다.
MsgSent	네이버로 전송된 메시지 수입니다.
TblVer	네이버로 전송된 BGP 데이터베이스의 마지막 버전입니다.
InQ	처리 대기 중인 네이버의 메시지 수입니다.
OutQ	네이버로 전송 대기 중인 메시지 수입니다.
Up/Down	BGP 세션이 Established 상태 또는 현재 상태(Established 상태가 아닌 경우)로 유지된 기간입니다.
State/PfxRcd	BGP 세션의 현재 상태 및 네이버 또는 피어 그룹에서 수신된 접두사 수입니다. 최대 수에 도달하면 문자열 "PfxRcd"가 항목에 표시되고, 네이버가 종료되며, 연결이 Idle로 설정됩니다. Idle 상태의 (Admin) 항목은 연결이 종료되었음을 나타냅니다.

다음 **show bgp summary** 명령의 출력에서는 BGP 네이버 192.168.3.2가 동적으로 생성되었으며, 수신 대기 범위 그룹 group192의 멤버임을 보여 줍니다. 또한 이 출력에서는 group192라는 수신 대기 범위 그룹에 대해 IP 접두사 범위 192.168.0.0/16이 정의되었음을 보여 줍니다.

```
> show bgp summary
```

```
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1

BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

다음 **show bgp summary** 명령의 출력에서는 서로 다른 4바이트 자동 시스템 번호 65536 및 65550에 있는 두 개의 BGP 네이버 192.168.1.2 및 192.168.3.2를 보여줍니다. 로컬 자동 시스템 65538도 4바이트 자동 시스템 번호이며, 이러한 번호는 기본 asplain 형식으로 표시됩니다.

```
> show bgp summary
BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4        65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4        65550       4       4        1    0    0 00:00:15      0
```

다음 **show bgp summary** 명령의 출력에서는 동일한 BGP 네이버 두 개를 보여 주지만 4바이트 자동 시스템 번호가 asdot 표기법 형식으로 표시되어 있습니다.

```
> show bgp summary
BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4         1.0       9       9        1    0    0 00:04:13      0
192.168.3.2     4        1.14       6       6        1    0    0 00:01:24      0
```

show bgp update-group

BGP 업데이트 그룹에 대한 정보를 표시하려면 **show bgp update-group** 명령을 사용합니다.

show bgp update-group [*index-group* | *ip-address*] [**summary**]

index-group	(선택 사항) 해당 인덱스 번호를 가진 업데이트 그룹 유형. 업데이트 그룹 인덱스 번호의 범위는 1~4294967295입니다.
ip-address	(선택 사항) 업데이트 그룹의 멤버인 단일 인접 항목의 IP 주소.
summary	(선택 사항) 업데이트 그룹 멤버 정보의 요약 표시. 출력은 index-group 또는 ip-address 인수와 함께 단일 인덱스 그룹 또는 피어를 위한 정보를 표시하기 위해 필터링될 수 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

자용 가이드라인

BGP 업데이트 그룹에 대한 정보를 표시하려면 이 명령을 사용합니다. BGP 아웃바운드 정책이 변경된 경우 라우터는 업데이트 그룹 멤버십을 자동으로 다시 계산하고 1분 타이머가 만료된 후 아웃바운드 소프트 재설정을 트리거하여 변경 사항을 적용합니다. 이 동작은 네트워크 운영자에게 실수한 경우 컨피그레이션을 변경할 수 있는 시간을 제공하기 위한 것입니다.

다음 **show bgp update-group** 명령의 샘플 출력에서는 모든 인접 항목에 대한 업데이트 그룹 정보를 보여줍니다.

```
> show bgp update-group
BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Route map for outgoing advertisements is COST1
  Update messages formatted 0, replicated 0
  Number of NLRIs in the update sent: max 0, min 0
  Minimum time between advertisement runs is 5 seconds
  Has 1 member:
  10.4.9.21
BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
  BGP Update version : 0, messages 0/0
  Update messages formatted 0, replicated 0
```

```
Number of NLRIs in the update sent: max 0, min 0
Minimum time between advertisement runs is 5 seconds
Has 2 members:
10.4.9.5 10.4.9.8
```

다음 표는 각 필드에 대해 설명합니다.

표 ***14: show bgp update-group*** 필드

필드	설명
BGP version	BGP 버전입니다.
update-group	업데이트 그룹 번호 및 유형(내부 또는 외부)입니다.
update messages formatted..., replicated...	포맷되고 복제된 업데이트 메시지 수입니다.
Number of NLRIs...	업데이트에서 전송된 NLRI 정보입니다.
.Minimum time between...	같은 줄에 표시된 경로, 접두사 또는 특성 항목에 사용되는 메모리(바이트)입니다.
...path entries using	BGP 데이터베이스에 있는 경로 항목 수입니다. 지정된 대상에 대해 단일 경로 항목만 설치됩니다. 다중 경로가 구성된 경우 다중 모드 경로의 각 경로에 대해 경로 항목이 설치됩니다.
...multipath network entries using	지정된 대상에 대해 설치된 다중 경로 항목 수입니다.
* ...BGP path/bestpath attribute entries using	경로가 최상의 경로로 선택된 고유한 BGP 특성 조합 수입니다.
* ...BGP rrinfo entries using	고유한 ORIGINATOR 및 CLUSTER_LIST 특성 조합 수입니다.
...BGP AS-PATH entries using	고유한 AS_PATH 항목 수입니다.
...BGP community entries using	고유한 BGP 커뮤니티 특성 조합 수입니다.
*...BGP extended community entries using	고유한 확장 커뮤니티 특성 조합 수입니다.
BGP route-map cache entries using	BGP route-map 일치 및 set 절 조합 수입니다. 0 값은 경로 캐시가 비어 있음을 나타냅니다.

필드	설명
...BGP filter-list cache entries using	AS-path 액세스 목록 허용 또는 거부 문과 일치하는 filter-list 항목 수입니다. 0 값은 filter-list 캐시가 비어 있음을 나타냅니다.
BGP advertise-bit cache entries using	보급된 bitfield 항목 수 및 관련 메모리 사용량입니다. 비트 필드 항목은 접두사가 동료에게 보급될 때 생성되는 정보 조각(1비트)을 나타냅니다. 보급된 비트 캐시는 필요할 때 동적으로 생성됩니다.
...received paths for inbound soft reconfiguration	인바운드 소프트 재구성에 대해 수신 및 저장된 경로 수입니다.
BGP using...	BGP 프로세스에서 사용된 총 메모리 양(바이트)입니다.
Dampening enabled...	BGP 감소가 사용 설정되었음을 나타냅니다. 누적된 페널티가 있는 경로 수 및 감소된 경로 수가 이 줄에 표시됩니다.
BGP activity...	경로 또는 접두사에 대해 메모리가 할당되거나 해제된 횟수를 표시합니다.
Neighbor	인접 항목의 IP 주소입니다.
V	인접 항목으로 발신된 BGP 버전 번호입니다.
AS	자동 시스템 번호입니다.
MsgRcvd	인접 항목에서 수신된 메시지 수입니다.
MsgSent	인접 항목으로 전송된 메시지 수입니다.
TblVer	인접 항목으로 전송된 BGP 데이터베이스의 마지막 버전입니다.
InQ	처리 대기 중인 인접 항목의 메시지 수입니다.
OutQ	인접 항목으로 전송 대기 중인 메시지 수입니다.
Up/Down	BGP 세션이 Established 상태 또는 현재 상태(Established 상태가 아닌 경우)로 유지된 기간입니다.
State/PfxRcd	BGP 세션의 현재 상태 및 인접 또는 피어 그룹에서 수신된 접두사 수입니다. 최대 수에 도달하면 문자열 "PfxRcd"가 항목에 표시되고, 인접 항목이 종료되며, 연결이 Idle로 설정됩니다. Idle 상태의 (Admin) 항목은 연결이 종료되었음을 나타냅니다.

show blocks

시스템 버퍼 사용률을 표시하려면 **show blocks** 명령을 사용합니다.

show blocks [**core** | **export-failed** | **interface**]

show blocks address *hex* [**diagnostics** | **dump** | **header** | **packet**]

show blocks {**all** | **assigned** | **free** | **old**} [**core-local** [*core-num*] [**diagnostics** | **dump** | **header** | **packet**]]

show blocks exhaustion {**history** [**list** | *snapshot_num*] | **snapshot**}

show blocks pool *block-size*

show blocks queue history [**core-local** [*core-num*]] [**detail**]

address*hex*	(선택 사항) 이 주소에 해당하는 블록을 16진수로 표시합니다.
all	(선택 사항) 모든 블록을 표시합니다.
assigned	(선택 사항) 할당되고 애플리케이션에서 사용 중인 블록을 표시합니다.
core	(선택 사항) 코어별 버퍼를 표시합니다.
core-local [*core-num*]	(선택 사항) 모든 코어의 시스템 버퍼를 표시합니다. 또한 특정 코어의 버퍼를 보려면, 코어 번호(예: 숫자 1)를 지정할 수 있습니다.
detail	(선택 사항) 각 고유 대기열 유형에 대한 첫 번째 블록의 일부(128바이트)를 표시합니다.
dump	(선택 사항) 헤더 및 패킷 정보를 포함하여 전체 블록 내용을 표시합니다. 덤프와 패킷의 차이점은 덤프에는 헤더와 패킷 사이의 추가 정보가 포함된다는 점입니다.
diagnostics	(선택 사항) 블록 진단을 표시합니다.
exhaustion snapshot	(선택 사항) 생성한 스냅샷 중 마지막 x개(여기서 x는 현재 10)와 마지막 스냅샷의 타임스탬프를 인쇄합니다. 스냅샷을 생성한 후 다른 스냅샷을 생성하려면 5분 이상이 경과해야 합니다.
exhaustion history [**list** | *snapshot_num*]	(선택 사항) 소모 스냅샷 기록을 표시합니다. 정보를 단일 스냅샷으로 제한하기 위해 스냅샷 번호를 지정하거나 스냅샷의 목록을 확인하기 위해 목록을 지정할 수 있습니다.
export-failed	(선택 사항) 시스템 버퍼 내보내기 오류 카운터를 표시합니다.
free	(선택 사항) 사용할 수 있는 블록을 표시합니다.

header	(선택 사항) 블록의 헤더를 표시합니다.
interface	(선택 사항) 인터페이스에 연결된 버퍼를 표시합니다.
old	(선택 사항) 할당된 지 1분이 넘은 블록을 표시합니다.
packet	(선택 사항) 블록의 헤더와 패킷의 내용을 표시합니다.
pool*block-size*	(선택 사항) 특정 크기의 블록을 표시합니다.
queue history	(선택 사항) Firepower Threat Defense 디바이스에서 블록을 소진한 경우 블록이 할당된 위치를 표시합니다. 경우에 따라 블록이 풀에서 할당되지만 대기열에 할당되지는 않습니다. 이 경우 위치는 블록을 할당한 코드 주소입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show blocks 명령은 Firepower Threat Defense 디바이스가 오버로드되었는지를 확인하는 데 유용합니다. 이 명령은 미리 할당된 시스템 버퍼 사용률을 나열합니다. 가득 찬 메모리 상태는 트래픽이 Firepower Threat Defense 디바이스를 통해 이동하고 있는 경우에는 문제가 되지 않습니다. **show conn** 명령을 사용하여 트래픽이 이동하고 있는지 확인할 수 있습니다. 트래픽이 이동하지 않는데 메모리가 가득 찬 경우에는 문제가 있을 수 있습니다. SNMP를 사용하여 이 정보를 볼 수도 있습니다.

다음은 **show blocks** 명령의 샘플 출력입니다.

```
> show blocks
  SIZE    MAX    LOW    CNT
     0   1450   1450   1450
     4    100     99     99
    80   1996   1992   1992
   256   4148   4135   4142
  1550   6274   6270   6272
  2048    100    100    100
  2560    164    164    164
  4096    100    100    100
  8192    100    100    100
  9344    100    100    100
 16384    100    100    100
 65536     16     16     16
```

다음 표는 각 필드에 관해 설명합니다.

표 ***15: show blocks*** 필드

필드	설명
SIZE	블록 풀의 크기(바이트)입니다. 각 크기는 특정 유형을 나타냅니다.
0	dupb 블록에서 사용됩니다.
4	DNS, ISAKMP, URL 필터링, uauth, TFTP 및 TCP 모듈과 같은 애플리케이션에서 기존 블록을 복제합니다. 또한 이 크기의 블록은 일반적으로 코드를 통해 드라이버 등으로 패킷을 전송하는 데 사용될 수 있습니다.
80	TCP 가로채기에서 확인 응답 패킷을 생성하는 데 사용되거나 페일오버 hello 메시지에 사용됩니다.
256	상태 저장 페일오버 업데이트, 시스템 로깅 및 기타 TCP 기능에 사용됩니다. 이러한 블록은 주로 스테이트풀 페일오버 메시지에 유용합니다. 액티브 Firepower Threat Defense 디바이스는 변환 및 연결 테이블을 업데이트하기 위해 패킷을 생성하고 스탠바이 Firepower Threat Defense 디바이스에 이 패킷을 전송합니다. 트래픽 양이 많아 연결 비율이 높거나 연결이 끊어질 수 있는 상황에서는 사용 가능한 블록 수가 0으로 감소할 수 있습니다. 이는 하나 이상의 연결이 스탠바이 Firepower Threat Defense 디바이스로 업데이트되지 않았음을 의미합니다. 스테이트풀 페일오버 프로토콜은 누락된 변환 또는 연결을 다음 번에 포착합니다. 256바이트 블록의 CNT 열이 연장된 기간 동안 0 또는 0에 근접한 상태에 머무는 경우 Firepower Threat Defense 디바이스에서 처리하는 초당 연결 수로 인해 Firepower Threat Defense 디바이스가 변환 및 연결 테이블을 동기화 상태로 유지하기 어렵습니다. 또한 Firepower Threat Defense 디바이스에서 전송된 syslog 메시지는 256바이트 블록을 사용하지만 256바이트 블록 풀을 소진시키는 양에서는 일반적으로 해제되지 않습니다. CNT 열에 256바이트 블록 수가 0에 가까운 것으로 표시된 경우 Debugging(수준 7)에서 syslog 서버에 기록하고 있지 않은지 확인하십시오. 이는 Firepower Threat Defense 컨피그레이션의 로깅 트랩 줄에 표시됩니다. 디버깅을 위해 추가 정보가 필요한 경우가 아니면 Notification(수준 5) 이하에서 기록을 설정하는 것이 좋습니다.
1550	Firepower Threat Defense 디바이스를 통해 처리하기 위해 Ethernet 패킷을 저장하는 데 사용됩니다. 패킷이 인터페이스로 들어오면 입력 인터페이스 큐에 배치되고 운영 체제로 전달되며 블록에 배치됩니다. 이 디바이스는 보안 정책에 따라 패킷을 허용할지 또는 거부할지 결정한 다음 아웃바운드 인터페이스의 출력 큐를 통과하도록 패킷을 처리합니다. 디바이스에서 트래픽 로드를 유지하는 데 문제가 있는 경우 사용 가능한 블록 수가 0에 가까운 곳을 가리킵니다(명령 출력의 CNT 열에 표시됨). CNT 열이 0인 경우에는 디바이스가 추가 블록을 할당하려고 시도합니다. 이 명령을 실행한 경우 최대값은 1550바이트 블록에 대해 8192보다 클 수 있습니다. 더 이상 사용 가능한 블록이 없으면 디바이스에서 패킷을 드롭합니다.
2048	컨트롤 업데이트에 사용되는 가이드 프레임 또는 컨트롤입니다.

필드	설명
16384	64비트 66MHz 기가비트 이더넷 카드(i82543)에만 사용됩니다. Ethernet 패킷에 대한 자세한 내용은 1550에 대한 설명을 참고하십시오.
MAX	지정된 바이트 블록 풀에 사용할 수 있는 최대 블록 수입니다. 최대 블록 수는 부팅 시 메모리에서 할당됩니다. 일반적으로 최대 블록 수는 변경되지 않습니다. 단, 디바이스에서 필요할 때 동적으로 추가 블록을 생성할 수 있는 256바이트 및 1550바이트 블록은 예외입니다. 이 명령을 실행한 경우 최대값은 1550바이트 블록에 대해 8192보다 클 수 있습니다.
LOW	Low-water mark. 이 숫자는 디바이스의 전원이 켜지거나 블록을 마지막으로 지운(**clear blocks** 명령 사용) 이후에 사용 가능한 이 크기의 최소 블록 수를 나타냅니다. LOW 열의 0은 메모리가 가득 찬 이전 이벤트를 나타냅니다.
CNT	해당 특정 크기의 블록 풀에서 사용할 수 있는 현재 블록 수입니다. CNT 열의 0은 메모리가 현재 가득 찼음을 의미합니다.

다음은 **show blocks all** 명령의 샘플 출력입니다.

```
> show blocks all
Class 0, size 4
     Block   allocd_by    freed_by data size  alloccnt  dup_cnt  oper location
0x01799940  0x00000000  0x00101603         0         0        0 alloc not_specified
0x01798e80  0x00000000  0x00101603         0         0        0 alloc not_specified
0x017983c0  0x00000000  0x00101603         0         0        0 alloc not_specified
...
    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

다음 표는 각 필드에 관해 설명합니다.

표 ***16: show blocks all*** 필드

필드	설명
Block	블록 주소입니다.
allocd_by	블록을 마지막으로 사용한 애플리케이션의 프로그램 주소입니다(사용되지 않은 경우 0).
freed_by	블록을 마지막으로 해제한 애플리케이션의 프로그램 주소입니다.
data size	블록 내에 있는 애플리케이션 버퍼/패킷 데이터의 크기입니다.
alloccnt	블록이 존재한 이후 이 블록이 사용된 횟수입니다.
dup_cnt	이 블록에 대한 현재 참조 수입니다. 사용된 경우 0은 1회 참조, 1은 2회 참조를 의미합니다.

필드	설명
oper	블록에서 마지막으로 수행된 네 가지 작업(alloc, get, put 또는 free) 중 하나입니다.
location	블록을 사용하는 애플리케이션 또는 블록을 마지막으로 할당한 애플리케이션의 프로그램 주소입니다(allocd_by 필드와 동일).

다음은 **show blocks exhaustion history list** 명령의 샘플 출력입니다.

```
> show blocks exhaustion history list
1 Snapshot created at 18:01:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

2 Snapshot created at 18:02:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

3 Snapshot created at 18:03:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out

4 Snapshot created at 18:04:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
```

명령	설명
blocks	블록 진단에 할당된 메모리를 늘립니다.
clear blocks	시스템 버퍼 통계를 지웁니다.
show conn	활성 연결을 표시합니다.

show bootvar

부트 파일 및 컨피그레이션 속성을 표시하려면 **show bootvar** 명령을 사용합니다.

show bootvar

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

BOOT 변수는 여러 디바이스에서 부팅 가능한 이미지 목록을 지정합니다. CONFIG_FILE 변수는 시스템을 초기화하는 동안 사용되는 컨피그레이션 파일을 지정합니다.

이 명령의 출력은 Firepower Threat Defense에서 유효하지 않을 수 있습니다.

다음은 Firepower Threat Defense의 Boot 변수를 보여주는 예입니다. 변수가 비어 있어도 이 예는 작동하는 시스템에서 가져온 것입니다.

```
> show bootvar
BOOT variable =
Current BOOT variable =
CONFIG_FILE variable =
Current CONFIG_FILE variable =
```

show bridge-group

할당된 인터페이스, MAC 주소 및 IP 주소와 같은 브리지 그룹 정보를 표시하려면 **show bridge-group** 명령을 사용합니다.

show bridge-group [*bridge_group_number*]

bridge_group_number	브리지 그룹 번호를 1에서 250 사이의 정수로 지정합니다. 번호를 지정하지 않으면 모든 브리지 그룹이 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 추가되었습니다.
6.2	Cisco는 통합 라우팅 및 브리징 사용 시 라우팅 방화벽 모드에서 지원을 추가했습니다.

다음은 **show bridge-group** 명령의 샘플 출력입니다.

```
> show bridge-group
Static mac-address entries:  0 (in use), 16384 (max)
Dynamic mac-address entries: 0 (in use), 16384 (max)
 Bridge Group: 1
 Interfaces:
 GigabitEthernet1/2
 GigabitEthernet1/3
 GigabitEthernet1/4
 GigabitEthernet1/5
 GigabitEthernet1/6
 GigabitEthernet1/7
 GigabitEthernet1/8
 Management System IP Address:  192.168.1.1 255.255.255.0
 Management Current IP Address: 192.168.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    2000:100::1, subnet is 2000:100::/64
 Static mac-address entries:  0
```

```
Dynamic mac-address entries: 0
```

명령	설명
show running-config interface bvi	브리지 그룹 인터페이스 컨피그레이션을 표시합니다.

show c

show capture

옵션을 지정하지 않은 경우 캡처 컨피그레이션을 표시하려면 **show capture** 명령을 사용합니다.

show capture [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*] [**trace**]

access-list*access_list_name*	(선택 사항) 특정 액세스 목록 식별을 위해 IP 또는 그 상위 필드를 기반으로 하는 패킷에 대한 정보를 표시합니다.
capture_name	(선택 사항) 패킷 캡처의 이름을 지정합니다.
count*number*	(선택 사항) 데이터가 지정된 패킷 수를 표시합니다. 유효한 값은 0~4294967295입니다.
decode	이 옵션은 캡처 유형 isakmp가 인터페이스에 적용된 경우에 유용합니다. 이 인터페이스를 통과하는 모든 ISAKMP 데이터는 암호 해독 후에 캡처되며 필드를 디코딩한 후 추가 정보와 함께 표시됩니다.
detail	(선택 사항) 각 패킷에 대한 추가 프로토콜 정보를 표시합니다.
dump	(선택 사항) 데이터 링크를 통해 전송되는 패킷의 16진수 덤프를 표시합니다.
packet-number*number*	(선택 사항) 지정된 패킷 번호에서 표시를 시작합니다. 유효한 값은 0~4294967295입니다.
trace	(선택 사항) 각 패킷에 대한 확장된 추적 정보를 표시합니다. 캡처가 trace 키워드를 사용하여 위에서 설명한 대로 설정된 경우, 이 옵션은 인바운드 방향의 각 패킷에 대한 패킷 트레이서의 출력을 보여줍니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

캡처 이름을 지정한 경우 해당 캡처에 대한 캡처 버퍼 내용이 표시됩니다.

dump 키워드는 16진수 덤프에 MAC 정보를 표시하지 않습니다.

패킷의 디코딩된 출력은 패킷의 프로토콜에 따라 달라집니다. 다음 표에서 대괄호 안의 출력은 **detail** 키워드를 지정한 경우에 표시됩니다.

표 ***17:*** 패킷 캡처 출력 형식

패킷 유형	캡처 출력 형식
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port:* [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port: tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/기타	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr: ip-protocol ip-length*
기타	*HH:MM:SS.ms ether-hdr: hex-dump*

Firepower Threat Defense 디바이스에서 잘못된 형식의 TCP 헤더가 있는 패킷을 받고 ASP 삭제 사유 invalid-tcp-hdr-length로 인해 이를 삭제한 경우에는 해당 패킷을 받은 인터페이스에서의 **show capture** 명령 출력에 패킷이 표시되지 않습니다.

다음 예에서는 캡처 컨피그레이션을 표시하는 방법을 보여 줍니다.

```
> show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

다음 예에서는 ARP 캡처에서 캡처한 패킷을 표시하는 방법을 보여 줍니다.

```
> show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

다음 예에서는 클러스터링 환경의 단일 디바이스에서 캡처된 패킷을 표시하는 방법을 보여 줍니다.

```
> show capture
capture 1 cluster type raw-data interface primary interface cluster [Buffer Full - 524187
bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```

다음 예에서는 클러스터링 환경의 모든 디바이스에서 캡처된 패킷을 표시하는 방법을 보여 줍니다.

```
> cluster exec show capture
mycapture (LOCAL):--------------------------------------------------------------
capture 1 type raw-data interface primary [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]

yourcapture:--------------------------------------------------------------------
capture 1 type raw-data interface primary [Capturing - 191484 bytes]
capture 2 type raw-data interface cluster [Capturing - 532354 bytes]
```

다음 예는 인터페이스에서 SGT와 이더넷 태그 지정이 활성화된 경우에 캡처된 패킷을 보여 줍니다.

```
> show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
```

SGT와 이더넷 태그 지정이 활성화된 경우에도 인터페이스에서 태그가 지정된 패킷 또는 태그가 지정되지 않은 패킷을 받을 수 있습니다. 표시된 예는 출력에 INLINE-TAG 36이 있는 태그가 지정된 패킷에 대한 예입니다. 동일한 인터페이스에서 태그가 지정되지 않은 패킷을 받은 경우에도 출력은 변경되지 않습니다(즉, 출력에 포함된 “INLINE-TAG 36” 항목이 없음).

명령	설명
capture	패킷 스니핑 및 네트워크 오류 격리를 위해 패킷 캡처 기능을 활성화합니다.
clear capture	캡처 버퍼를 지웁니다.
copy capture	서버에 캡처 파일을 복사합니다.

show checkheaps

checkheap 통계를 표시하려면 **show checkheaps** 명령을 사용합니다. checkheap은 힙 메모리 버퍼의 온전성(동적 메모리는 시스템 힙 메모리 영역에서 할당됨) 및 코드 영역의 무결성을 확인하는 정기 프로세스입니다.

show checkheaps

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show checkheaps** 명령의 샘플 출력입니다.

```
> show checkheaps
Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

show checksum

구성 체크섬을 표시하려면 **show checksum** 명령을 사용합니다.

show checksum

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show checksum 명령을 사용하면 구성 내용의 디지털 요약 역할을 하는 네 그룹의 16진수 숫자를 표시할 수 있습니다. 이 체크섬은 플래시 메모리에 구성을 저장한 경우에만 계산됩니다.

show running-config 또는 **show checksum** 명령 출력에서 체크섬 앞에 점(“.”)이 표시된 경우 이 출력은 정상적인 구성 로드 또는 쓰기 모드를 나타냅니다(Firepower Threat Defense 플래시 파티션에서 로드하거나 쓰는 경우). 점(“.”)은 Firepower Threat Defense 디바이스가 작업으로 선점되었지만 “중지”되지 않음을 표시합니다. 이 메시지는 “시스템에서 처리 중입니다. 잠시 기다려 주십시오.” 메시지와 유사합니다.

다음 예에서는 구성 또는 체크섬을 표시하는 방법을 보여 줍니다.

```
> show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

청크 통계를 표시하려면 **show chunkstat** 명령을 사용합니다.

show chunkstat

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 청크 통계를 표시하는 방법을 보여 줍니다.

```
> show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings destroyed
 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
 @ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

명령	설명
show counters	프로토콜 스택 카운터를 표시합니다.
show cpu	CPU 사용률 정보를 표시합니다.

show cluster

전체 클러스터에 대한 집계된 데이터 또는 다른 정보를 보려면 **show cluster** 명령을 사용합니다.

show cluster {access-list [*acl_name*] | **conn** [**count**] | **cpu** [**usage**] | **history** | **interface-mode** | **memory** | **resource usage** | **service-policy** | **traffic** | **xlate count**}

access-list [*acl_name*]	액세스 정책에 대한 방문 횟수 카운터를 표시합니다. 특정 ACL에 대한 카운터를 보려면 acl_name을 입력합니다.
conn [**count**]	모든 디바이스에 대한 사용 중인 연결의 집계된 수를 표시합니다. **count** 키워드를 입력하면 연결 수만 표시됩니다.
cpu [**usage**]	CPU 사용 정보를 표시합니다.
history	클러스터 스위칭 기록을 표시합니다.
interface-mode	클러스터 인터페이스 모드(spanned 또는 individual)를 표시합니다.
memory	시스템 메모리 사용률 및 기타 정보를 표시합니다.
resource usage	시스템 리소스 및 사용 현황을 표시합니다.
service-policy	MPF 서비스 정책 통계를 표시합니다.
traffic	트래픽 통계를 표시합니다.
xlate count	현재 변환 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show cluster access-list** 명령의 샘플 출력입니다.

```
> show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
```

```
  (hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0
  (hitcnt=0, 0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
  (hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
  (hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
  (hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
  (hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
  (hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
  (hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
  (hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
  (hitcnt=429, 109, 107, 109, 104)0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
  (hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
  (hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
  (hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
  (hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
  (hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
  (hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

모든 디바이스에서 사용 중인 연결의 집계된 수를 표시하려면 다음을 입력합니다.

```
> show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used
  cl1:*********************************************************************
  100 in use, 100 most used
```

명령	설명
show cluster info	클러스터 정보를 표시합니다.

show cluster info

클러스터 정보를 보려면 **show cluster info** 명령을 사용합니다.

show cluster info [**clients** | **conn-distribution** | **flow-mobility counters** | **goid** [*options*] | **health** | **incompatible-config** | **loadbalance** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** {**asp** | **cp**}]

clients	(선택 사항) 레지스터 클라이언트의 버전을 표시합니다.
conn-distribution	(선택 사항) 클러스터의 연결 배포를 표시합니다.
flow-mobility counters	(선택 사항) EID 이동 및 플로우 소유자 이동 정보를 표시합니다.
goid [*options*]	(선택 사항) 전역 개체 ID 데이터베이스를 표시합니다. 옵션에는 다음이 포함됩니다. classmap conn-set hwidb idfw-domain idfw-group interface policymap virtual-context
health	(선택 사항) 상태 모니터링 정보를 표시합니다.
incompatible-config	(선택 사항) 현재 실행 중인 컨피그레이션에서 클러스터링과 호환되지 않는 명령을 표시합니다. 이 명령은 클러스터링을 활성화하기 전에 유용합니다.
loadbalance	(선택 사항) 로드 밸런싱 정보를 표시합니다.
old-members	(선택 사항) 클러스터의 이전 멤버를 표시합니다.
packet-distribution	(선택 사항) 클러스터의 패킷 배포를 표시합니다.

trace [*options*]	(선택 사항) 클러스터링 제어 모듈 이벤트 추적을 표시합니다. 옵션에는 다음이 포함됩니다. • **latest** [*number*] - 마지막 숫자 이벤트를 표시합니다(여기서 숫자는 1~2147483647임). 기본적으로 모두 표시합니다. • **level***level* — 수준이 다음 중 하나인 경우 수준별로 이벤트를 필터링합니다. **all**, **critical**, **debug**, **informational** 또는 **warning**. • **module***module* — 모듈이 다음 중 하나인 경우 모듈을 기준으로 이벤트를 필터링합니다. **ccp**, **datapath**, **fsm**, **general**, **hc**, **license**, **rpc** 또는 **transport**. • **time** {[*month day*] [*hh:mm:ss*]} — 지정된 시간 또는 날짜 이전의 이벤트를 표시합니다.
transport {**asp** | **cp**}	(선택 사항) 다음에 대한 전송 관련 통계를 표시합니다. • **asp** - 데이터 플레인 전송 통계입니다. • **cp** - 컨트롤 플레인 전송 통계입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

아무 옵션도 지정하지 않은 경우 **show cluster info** 명령은 클러스터 이름 및 상태, 클러스터 멤버, 멤버 상태 등 일반적인 클러스터 정보를 표시합니다.

통계를 지우려면 **clear cluster info** 명령을 사용합니다.

다음은 **show cluster info** 명령의 샘플 출력입니다.

```
> show cluster info
Cluster stbu: On
  This is "C" in state SLAVE
      ID        : 0
      Site ID : 1
      Version   : 9.5(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
```

```
Other members in the cluster:
  Unit "D" in state SLAVE
      ID        : 1
      Site ID : 1
      Version   : 9.5(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state MASTER
      ID        : 2
      Site ID : 2
      Version   : 9.5(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state SLAVE
      ID        : 3
      Site ID : 2
      Version   : 9.5(1)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

다음은 **show cluster info incompatible-config** 명령의 샘플 출력입니다.

```
> show cluster info incompatible-config
INFO: Clustering is not compatible with following commands which given a
user's confirmation upon enabling clustering, can be removed automatically
from running-config.
policy-map global_policy
 class scansafe-http
  inspect scansafe http-map fail-close
policy-map global_policy
 class scansafe-https
  inspect scansafe https-map fail-close
INFO: No manually-correctable incompatible configuration is found.
```

다음은 **show cluster info trace** 명령의 샘플 출력입니다.

```
> show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at MASTER
```

다음은 **show cluster info flow-mobility counters** 명령의 샘플 출력입니다.

```
> show cluster info flow-mobility counters
EID movement notification received  : 0
EID movement notification processed : 0
Flow owner moving requested         : 0
```

명령	설명
show cluster	전체 클러스터에 대한 집계된 데이터를 표시합니다.

show community-list

특정 커뮤니티 목록에서 허용하는 경로를 표시하려면 **show community-list** 명령을 사용합니다.

show community-list [*community-list-number* | *community-list-name*]

community-list-number	(선택 사항) 1~500의 표준 또는 확장 커뮤니티 목록 번호입니다.
community-list-name	(선택 사항) 커뮤니티 목록 이름입니다. 커뮤니티 목록 이름은 표준 또는 확장일 수 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

show conn

지정한 연결 유형에 대한 연결 상태를 표시하려면 **show conn** 명령을 사용합니다. 이 명령은 IPv4 및 IPv6 주소를 지원합니다.

show conn [**count** | [**all**] [**detail**] [**long**] [**state** *state_type*] [**flow-rule**] [**inline-set**] [**protocol** {**tcp** | **udp** | **sctp**}] **address** *src_ip*[*-src_ip*] [**netmask** *mask*]] [**port** *src_port*[*-src_port*]] [**address** *dest_ip*[*-dest_ip*] [**netmask** *mask*]] [**port** *dest_port*[*-dest_port*]] [**state** *state_type*] [**zone** [*zone_name*]]

address {*src_ip*|*dest_ip*}	(선택 사항) 지정된 소스 또는 대상 IPv4 또는 IPv6 주소와의 연결을 표시합니다. 범위를 지정하려면 대시(-)를 사용하여 IP 주소를 구분합니다. 예를 들면 10.1.1.1-10.1.1.5와 같이 지정합니다.
all	(선택 사항) 통과 트래픽 연결 외에 디바이스로의 연결 또는 디바이스에서의 연결을 표시합니다.
count	(선택 사항) 활성 연결 수를 표시합니다.
detail	(선택 사항) 변환 유형 및 인터페이스 정보를 포함하여 연결을 자세히 표시합니다.
flow-rule	(선택 사항) 플로우 규칙의 연결을 표시합니다.
inline-set	(선택 사항) 인라인 집합의 연결을 표시합니다.
long	(선택 사항) 긴 형식의 연결을 표시합니다.
netmask*mask*	(선택 사항) 지정된 IP 주소에서 사용할 서브넷 마스크를 지정합니다.
port {*src_port* | *dest_port*}	(선택 사항) 지정된 소스 또는 대상 포트와의 연결을 표시합니다. 범위를 지정하려면 대시(-)를 사용하여 포트 번호를 구분합니다. 예를 들어, 1000-2000입니다.
protocol{**tcp**|**udp**|**sctp**}	(선택 사항) 연결 프로토콜을 지정합니다.
state*state_type*	(선택 사항) 연결 상태 유형을 지정합니다. 연결 상태 유형에 사용 가능한 키워드 목록의 사용량 섹션의 표를 참조하십시오.
zone [*zone_name*]	(선택 사항) 영역에 대한 연결을 표시합니다. **long** 및 **detail** 키워드는 연결이 설정된 기본 인터페이스 및 트래픽을 전달하는 데 사용되는 현재 인터페이스를 보여줍니다.

모든 통과 연결은 기본적으로 표시됩니다. 디바이스에 대한 관리 연결도 표시하려면 **all** 키워드를 사용해야 합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show conn 명령은 활성 TCP 및 UDP 연결 수를 표시하고 여러 유형의 연결에 대한 정보를 제공합니다. **show conn all** 명령을 사용하여 전체 연결 테이블을 볼 수 있습니다. 특정 QoS 규칙 ID로 속도가 제한된 라이브 연결을 찾으려면 이 명령을 사용할 수 있습니다.

참고 Firepower Threat Defense 디바이스에서 보조 연결을 허용하기 위해 핀홀을 만든 경우 이는 **show conn** 명령을 통해 불완전한 연결로 표시됩니다. 이 불완전한 연결을 지우려면 **clear conn** 명령을 사용합니다.

show conn state 명령을 사용하여 지정할 수 있는 연결 유형이 다음 표에 정의되어 있습니다. 여러 연결 유형을 지정할 때는 공백 없이 쉼표를 사용하여 키워드를 구분합니다.

표 ***18:*** 연결 상태 유형

키워드	표시되는 연결 유형
up	작동 중인 상태의 연결
conn_inbound	인바운드 연결
ctiqbe	CTIQBE 연결
data_in	인바운드 데이터 연결
data_out	아웃바운드 데이터 연결
finin	FIN 인바운드 연결
finout	FIN 아웃바운드 연결
h225	H.225 연결

키워드	표시되는 연결 유형
h323	H.323 연결
http_get	HTTP 가져오기 연결
mgcp	MGCP 연결
nojava	Java 애플릿에 대한 액세스를 거부하는 연결
rpc	RPC 연결
service_module	SSM에서 스캔 중인 연결
sip	SIP 연결
skinny	SCCP 연결
smtp_data	SMTP 메일 데이터 연결
sqlnet_fixup_data	SQL*Net 데이터 검사 엔진 연결
tcp_embryonic	TCP 원시 연결
vpn_orphan	분리된 VPN 터널링 플로우

detail 옵션을 사용하면 다음 표에 정의된 연결 플래그를 사용하여 변환 유형 및 인터페이스 정보가 표시됩니다.

표 ***19:*** 연결 플래그

플래그	설명
a	SYN에 대한 외부 ACK 대기 중
A	SYN에 대한 내부 ACK 대기 중
b	TCP 상태 우회
B	외부의 초기 SYN
C	CTIQBE(Computer Telephony Interface Quick Buffer Encoding) 미디어 연결
d	덤프
D	DNS

플래그	설명
E	외부 다시 연결. 이는 내부 호스트에서 시작해야 하는 보조 데이터 연결입니다. 예를 들어 FTP를 사용하는 경우 내부 클라이언트가 PASV 명령을 실행하고 외부 서버가 수락하면 Firepower Threat Defense는 이 플래그 세트로 외부 역방향 연결을 미리 할당합니다. 내부 클라이언트가 서버에 다시 연결하려고 하면 Firepower Threat Defense에서 이 연결 시도를 거부합니다. 외부 서버만 미리 할당된 보조 연결을 사용할 수 있습니다.
f	내부 FIN
F	외부 FIN
g	MGCP(Media Gateway Control Protocol) 연결
G	G 플래그는 연결이 그룹의 일부임을 나타냅니다. 이는 제어 연결 및 연계된 모든 보조 연결을 지정하는 GRE 및 FTP Strict 검사로 설정됩니다. 제어 연결이 종료되면 연계된 모든 보조 연결도 종료됩니다.
h	H.225
H	H.323
i	불완전한 TCP 또는 UDP 연결
I	인바운드 데이터
k	SCCP(Skinny Client Control Protocol) 미디어 연결
K	GTP t3-response
L	LISP 플로우 모빌리티에 영향을 받는 트래픽
m	SIP 미디어 연결
M	SMTP 데이터
o	오프로드된 플로우
O	아웃바운드 데이터
p	복제됨(사용되지 않음)
P	내부 역방향 연결. 이는 내부 호스트에서 시작해야 하는 보조 데이터 연결입니다. 예를 들어 FTP를 사용하는 경우 내부 클라이언트가 PORT 명령을 실행하고 외부 서버가 수락하면 Firepower Threat Defense 디바이스에서 이 플래그 세트로 내부 역방향 연결을 미리 할당합니다. 외부 서버가 클라이언트에 다시 연결하려고 하면 디바이스에서 이 연결 시도를 거부합니다. 내부 클라이언트만 미리 할당된 보조 연결만 사용할 수 있습니다.

플래그	설명
q	SQL*Net 데이터
Q	지름 연결
r	내부 확인 응답된 FIN
R	TCP 연결에 대해 외부 확인 응답된 FIN
R	UDP RPC. **show conn** 명령 출력의 각 행은 하나의 연결(TCP 또는 UDP)을 나타내기 때문에 R 플래그는 행당 하나만 있습니다.
s	외부 SYN 대기 중
S	내부 SYN 대기 중
t	SIP 임시 연결. UDP 연결의 경우 값 t는 1분 후 시간 초과됨을 나타냅니다.
T	SIP 연결. UDP 연결의 경우 값 T는 **timeout sip** 명령을 사용하여 지정된 값에 따라 연결의 시간이 초과됨을 나타냅니다.
u	STUN 연결
U	up
v	M3UA 연결
V	VPN 분리
W	WAAS
X	서비스 모듈에서 검사
y	클러스터링의 경우 백업 소유자 플로우 식별
Y	클러스터링의 경우 디렉터 플로우 식별
z	클러스터링의 경우 전달자 플로우 식별
Z	Cloud Web Security

참고 DNS 서버를 사용하는 연결의 경우 연결의 소스 포트는 **show conn** 명령 출력에 있는 DNS 서버의 IP 주소로 대체될 수 있습니다.

여러 DNS 세션이 동일한 두 호스트 간에 존재하고 세션의 5튜플(소스/대상 IP 주소, 소스/대상 포트 및 프로토콜)이 동일한 경우 여러 DNS 세션에 대해 단일 연결이 생성됩니다. DNS 식별은 *app_id*로 추적되며, 각 app_id에 대한 유휴 타이머는 독립적으로 실행됩니다.

app_id는 독립적으로 만료되므로, 정상적인 DNS 응답만이 제한된 기간 내에 Firepower Threat Defense 디바이스를 통과할 수 있으며 리소스 빌드업은 없습니다. 그러나 **show conn** 명령을 입력하면 새 DNS 세션에 의해 DNS 연결의 유휴 타이머가 재설정됩니다. 이는 공유 DNS 연결의 속성 때문이며 설계에 따른 것입니다.

참고 연결 비활성 시간 제한(기본적으로 1시간) 동안 TCP 트래픽이 없으면 연결이 닫히고 해당 연결 플래그 항목이 더 이상 표시되지 않습니다.

LAN-to-LAN/네트워크-확장 모드 터널이 삭제되고 다시 생성되지 않은 경우 여러 개의 분리된 터널 플로우가 있을 수 있습니다. 이러한 플로우는 터널 중단으로 인해 끊어지지는 않지만 이러한 통과하려고 시도하는 모든 데이터는 드롭됩니다. **show conn** 명령 출력에서는 이러한 분리된 흐름을 V 플래그로 표시합니다.

여러 연결 유형을 지정할 때는 공백 없이 쉼표를 사용하여 키워드를 구분합니다. 다음 예에서는 Up 상태의 RPC, H.323 및 SIP 연결에 대한 정보를 표시합니다.

```
> show conn state up,rpc,h323,sip
```

다음은 **show conn count** 명령의 샘플 출력입니다.

```
> show conn count
54 in use, 123 most used
```

다음은 **show conn** 명령의 샘플 출력입니다. 이 예에서는 내부 호스트 10.1.1.15와 10.10.49.10에 있는 외부 텔넷 서버 간의 TCP 세션 연결을 표시합니다. B 플래그가 없으므로 이 연결은 내부에서 시작됩니다. “U”, “I” 및 “O” 플래그는 연결이 활성 상태이고 인바운드 및 아웃바운드 데이터를 수신했음을 나타냅니다.

```
> show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
```

```
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0,
flags Ti
```

다음은 **show conn detail** 명령의 샘플 출력입니다. 이 예에서는 외부 호스트 10.10.49.10과 내부 호스트 10.1.1.15 간의 UDP 연결을 보여 줍니다. D 플래그는 이 연결이 DNS 연결임을 나타냅니다. 번호 1028은 DNS ID입니다.

```
> show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow TCP outside:10.10.49.10/23
inside:10.1.1.15/1026,
    flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
    flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
    flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
    flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
    flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000,
    flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000,
    flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405
TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060,
    flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
    flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
    flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
    flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000,
    flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
    flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
    flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

다음은 분리 흐름이 존재하는 경우(V 플래그로 표시)의 **show conn** 명령의 샘플 출력입니다.

```
> show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

보고서를 분리 흐름이 있는 연결로 제한하려면 다음 예와 같이 **vpn_orphan** 옵션을 **show conn state** 명령에 추가합니다.

```
> show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
UOVB
```

클러스터링의 경우 연결 플로우 문제를 해결하려면 먼저 마스터 유닛에서 **cluster exec show conn** 명령을 입력하여 모든 유닛의 연결을 확인합니다. 디렉터(Y), 백업(y) 및 전달자(z) 플래그가 있는 플로우를 확인합니다. 다음 예에서는 세 디바이스 모두에 대한 172.18.124.187:22와 192.168.103.131:44727 간의 SSH 연결을 보여줍니다. FTD1에는 연결의 전달자임을 나타내는 z 플래그가 있고, FTD3에는 연결의 디렉터임을 나타내는 Y 플래그가 있으며, FTD2에는 특별한 플래그가 없어 소유자임을 나타냅니다. 아웃바운드 방향에서 이 연결의 패킷은 FTD2의 내부 인터페이스로 들어가 외부 인터페이스를 나갑니다. 인바운드 방향에서 이 연결의 패킷은 FTD1 및 FTD3의 외부 인터페이스로 들어가 클러스터 제어 링크를 통해 FTD2로 전달된 다음 FTD2의 내부 인터페이스를 나갑니다.

```
> cluster exec show conn
FTD1(LOCAL):**************************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes 37240828,
 flags z
FTD2:**************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes 37240828,
 flags UIO
FTD3:**************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0, flags
  Y
```

FTD2에 대한 show conn detail의 출력은 최근 전달자가 FTD1이었음을 보여줍니다.

```
> show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow TCP outside: 172.18.124.187/22
inside: 192.168.103.131/44727,
    flags UIO , idle 0s, uptime 25s, timeout 1h0m, bytes 1036044, cluster sent/rcvd bytes
0/1032983, cluster sent/rcvd total bytes 0/1080779, owners (1,255)
Traffic received at interface outside
        Locally received: 0 (0 byte/s)
```

```
        From most recent forwarder FTD1: 1032983 (41319 byte/s)
Traffic received at interface inside
        Locally received: 3061 (122 byte/s)
```

명령	설명
clear conn	연결을 지웁니다.

show console-output

현재 캡처된 콘솔 출력을 표시하려면 **show console-output** 명령을 사용합니다.

show console-output

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show console-output** 명령의 샘플 출력입니다.

```
> show console-output
Message #1 : Message #2 : Setting the offload CPU count to 0
Message #3 :
Compiled on Fri 20-May-16 13:36 PDT by builders
Message #4 :
Total NICs found: 14
Message #5 : i354 rev03 Gigabit Ethernet @ irq255 dev 20 index 08 MAC: e865.49b8.97f1
Message #6 : ivshmem rev03 Backplane Data Interface     @ index 09 MAC: 0000.0001.0002
Message #7 : en_vtun rev00 Backplane Control Interface  @ index 10 MAC: 0000.0001.0001
Message #8 : en_vtun rev00 Backplane Int-Mgmt Interface     @ index 11 MAC: 0000.0001.0003
Message #9 : en_vtun rev00 Backplane Ext-Mgmt Interface     @ index 12 MAC: 0000.0000.0000
Message #10 : en_vtun rev00 Backplane Tap Interface     @ index 13 MAC: 0000.0100.0001
Message #11 : Running Permanent Message
#12 : Activation Key: Message
#13 : 0x00000000 Message
#14 : 0x00000000 Message
#15 : 0x00000000 Message
#16 : 0x00000000 Message
#17 : 0x00000000 Message #18 :
Message #19 : The Running Activation Key is not valid, using default settings:
Message #20 :
(...output truncated...)
```

show counters

프로토콜 스택 카운터를 표시하려면 **show counters** 명령을 사용합니다.

show counters [**all** | **summary** | **top** *N*] [**description**] [**detail**] [**protocol** *protocol_name* [:*counter_name*]] [**threshold** *N*]

all	필터 세부사항을 표시합니다.
:*counter_name*	이름으로 카운터를 지정합니다.
description	다양한 카운터 및 설명을 표시합니다.
detail	추가 카운터 정보를 표시합니다.
protocol*protocol_name*	지정된 프로토콜에 대한 카운터를 표시합니다. 옵션 목록을 보려면 ?를 입력합니다.
summary	카운터 요약을 표시합니다.
threshold*N*	지정된 임계값에 도달하거나 이를 초과하는 카운터만 표시합니다. 범위는 1~4294967295입니다.
top*N*	지정된 임계값에 도달하거나 이를 초과하는 카운터를 표시합니다. 범위는 1~4294967295입니다.

기본값은 **show counters summary detail threshold 1**입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 기본 정보를 표시하는 방법을 보여줍니다.

```
> show counters
Protocol      Counter                                   Value   Context
IP            IN_PKTS                                  785064   Summary
IP            OUT_PKTS                                  19196   Summary
```

```
IP           OUT_DROP_DWN                          177099   Summary
IP           TO_ARP                                785064   Summary
TCP          OUT_PKTS                               38378   Summary
TCP          SESS_CTOD                              19189   Summary
TCP          OUT_CLSD                               19189   Summary
TCP          HASH_ADD                               19189   Summary
TCP          SND_SYN                                19189   Summary
SSLERR       BAD_SIGNATURE                              3   Summary
SSLDEV       NEW_CTX                                    3   Summary
VPIF         BAD_VALUE                                673   Summary
VPIF         NOT_FOUND                          106843325   Summary
```

명령	설명
clear counters	프로토콜 스택 카운터를 지웁니다.

show cpu

CPU 사용률 정보를 표시하려면 **show cpu** 명령을 사용합니다.

show cpu [**detailed** | **external** | **profile** [**dump**] | **system** [*processor_num*]]

show cpu core [**all** | *core_id*]

show cpu usage [**detailed** | **core** [**all** | *core_id*]]

core [**all**	*core_id*]	각 코어의 CPU 통계를 표시합니다. 모든 코어(기본값)를 보거나 숫자별로 코어를 지정할 수 있습니다. 디바이스에서 사용 가능한 코어 수를 확인하려면 파라미터 없이 키워드를 사용합니다. 코어 수는 0으로 시작합니다. **show cpu core** 및 **show cpu usage core** 명령은 동일한 정보를 제공합니다.
detailed	(선택 사항) CPU 사용에 대한 내부 세부사항을 표시합니다.
external	(선택 사항) 외부 프로세스에 대한 CPU 사용량을 표시합니다.
profile [**dump**]	(선택 사항) CPU 프로파일링 데이터를 표시합니다. 프로파일링 데이터의 덤프를 확인하려면 **dump** 키워드를 포함합니다.
system [*processor_num*]	(선택 사항) 전체 시스템과 관련된 정보를 표시합니다. 특정 프로세서에 대한 정보를 확인하기 위해 프로세서 번호를 선택적으로 포함할 수 있습니다. CPU라는 사용 가능한 프로세서 수를 확인하려면 키워드 없이 명령을 사용합니다. 프로세서 수는 0으로 시작합니다. 따라서 출력에서 8개의 CPU를 표시하는 경우, 시스템에 유효한 숫자는 0-7입니다.
usage	(선택 사항) CPU 사용량을 표시합니다. 이것이 기본 옵션입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

CPU 사용량은 5초 단위의 로드 근사값을 계산한 다음 이 근사값을 이동 평균에 따라 두 개로 나눈 값으로 계산됩니다.

CPU 문제를 해결할 때 **show cpu profile dump** 명령을 **cpu profile activate** 명령과 함께 사용하여 TAC 사용에 대한 정보를 수집할 수 있습니다. **show cpu profile dump** 명령 출력은 16진수 형식입니다.

Firepower Threat Defense Virtual(Firepower NGFW Virtual)의 경우 **show cpu** 명령은 VM에 할당된 CPU 수가 vCPU 플랫폼 라이선스 제한을 기준으로 허용되는 제한 범위 이내에 있는지도 표시합니다. 상태는 호환, 비호환: 오버 프로비저닝 또는 비호환: 언더 프로비저닝이 있습니다. 이 정보는 정확하지 않을 수 있습니다.

다음 예에서는 CPU 사용률을 표시하는 방법을 보여 줍니다.

```
> show cpu
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

다음 예에서는 자세한 CPU 사용률 정보를 표시하는 방법을 보여 줍니다.

```
> show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  3.3 (0.0 + 3.3)  2.4 (0.0 + 2.4)
Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 99.0%; 1 minute: 99.8%; 5 minutes: 95.9%
CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%
Total CPU utilization for:
      5 seconds = 0.2%; 1 minute: 3.3%; 5 minutes: 2.5%
```

참고 "Current control point elapsed versus the maximum control point elapsed for" 문은 현재 제어 지점 부하가 정의된 기간 내에 표시된 최대 부하와 비교됨을 의미합니다. 이는 절대값이 아니라 비율입니다. 5초 간격의 경우 99%는 현재 제어 지점 부하가 이 5초 간격 동안 표시될 수 있는 최대 부하의 99%임을 의미합니다. 부하가 계속 증가하는 경우에는 항상 100%로 유지됩니다. 그러나 최대 절대값이 정의되지 않았으므로 실제 CPU에는 여유 공간이 많이 있을 수 있습니다.

다음 예는 시스템 레벨의 CPU 사용량이 표시되는 방법을 보여줍니다. 첫 라인에서 "(2 CPU)" 표시를 참조하십시오. 이것은 이 디바이스의 프로세서 수입니다.

```
> show cpu system
Linux 3.10.62-ltsi-WR6.0.0.27_standard (ftd1.example.com)        10/20/16        _x86_64_
  (2 CPU)

Time         CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest  %gnice
 %idle
15:48:26     all   50.36    0.00   10.04    0.78    0.00    0.03    0.00    0.00    0.00
 38.79
```

다음 표에는 **show cpu system** 출력의 필드에 대한 설명이 나와 있습니다.

표 ***20: Show CPU System*** 필드

필드	설명
Time	이 숫자가 결정된 시간.

필드	설명
CPU	프로세서 수.
%user	사용자 레벨(애플리케이션)에서 실행되는 동안 발생한 CPU 사용률.
%nice	사용자 레벨(nice 우선순위)에서 실행되는 동안 발생한 CPU 사용률.
%sys	시스템 레벨(커널)에서 실행되는 동안 발생한 CPU 사용률. interrupt 또는 softirq의 서비스에 사용된 시간은 포함되지 않습니다. softirq(software interrupt)는 여러 CPU에서 동시에 실행할 수 있는 32개의 열거된 software interrupt 중 하나입니다.
%iowait	시스템에 해결되지 않은 디스크 I/O 요청이 있을 때 CPU가 유휴 상태인 시간의 백분율.
%irq	interrupt 서비스에 CPU가 사용된 시간의 백분율.
%soft	softirq 서비스에 CPU가 사용된 시간의 백분율.
%steal	하이퍼바이저가 다른 가상 프로세서를 서비스하는 동안 가상 CPU가 비자발적으로 대기하는 데 사용된 시간의 백분율.
%guest	가상 프로세서 실행에 CPU가 사용된 시간의 백분율.
%gnice	가상 프로세서에 대해 게스트 레벨(nice 우선순위)에서 실행되는 동안 발생한 CPU 사용률.
%idle	CPU가 유휴 상태이고 시스템에 해결되지 않은 디스크 I/O 요청이 없는 시간의 백분율.

다음 예에서는 프로파일러를 활성화하여 1000개의 샘플(기본값)을 저장하도록 지시합니다. 다음으로, **show cpu profile** 명령은 프로파일링이 진행 중임을 표시합니다. 잠시 기다리면 다음 **show cpu profile** 명령이 프로파일링이 완료되었음을 표시합니다. 마지막으로, 결과를 가져오려면 **show cpu profile dump** 명령을 사용합니다. 출력을 복사하고 이를 Cisco Technical Support에 제공합니다. 전체 출력을 가져오려면 SSH 세션을 로깅해야 할 수 있습니다.

```
> cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU profiling currently in progress:
    Core 0: 501 out of 1000 samples collected.
    CP: 586 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt
profiling and display the incomplete results.
> show cpu profile
CPU profiling started: 16:13:48.279 UTC Thu Oct 20 2016
CPU Profiling has stopped.
    Core 0 done with 1000 samples
```

```
    CP done with 1000 samples
Use "show cpu profile dump" to see the results.
> show cpu profile dump
(...output omitted...)
```

명령	설명
clear cpu profile	CPU 프로파일링 데이터를 지웁니다.
cpu profile activate	CPU 프로파일링을 활성화합니다.
show counters	프로토콜 스택 카운터를 표시합니다.

show crashinfo

플래시 메모리에 저장된 충돌 파일의 내용을 표시하려면 **show crashinfo** 명령을 입력합니다.

show crashinfo [**console** | **module** *number* | **save** | **webvpn** [**detailed**]]

console	(선택 사항) crashinfo 콘솔 출력의 상태를 표시합니다.
module*number*	(선택 사항) 지정된 모듈에서 검색된 충돌 정보를 표시합니다. 예를 들어, 숫자별(예: 1)로 모듈을 표시합니다.
save	(선택 사항) 디바이스가 충돌 정보를 플래시 메모리에 저장하도록 구성되었는지를 표시합니다.
webvpn [**detailed**]	(선택 사항) Firepower Threat Defense 충돌 복구 덤프를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

자용 가이드라인

충돌 파일이 테스트 충돌로 인해 발생(**crashinfo test** 명령에서 생성)한 경우 충돌 파일의 첫 번째 문자열은 ": Saved_Test_Crash"이고 마지막 문자열은 ": End_Test_Crash"입니다. 충돌 파일이 실제 충돌로 인해 발생한 경우 충돌 파일의 첫 번째 문자열은 ": Saved_Crash"이고 마지막 문자열은 ": End_Crash"입니다. (여기에는 **crashinfo force page-fault** 또는 **crashinfo force watchdog** 명령 사용으로 인한 충돌이 포함됩니다.)

FIPS 140-2에서는 중요한 보안 파라미터(키, 비밀번호 등)를 암호화 경계(섀시) 외부에 배포하는 것을 금지하고 있습니다. 어설션 또는 checkheap 오류로 인해 디바이스가 충돌하는 경우 콘솔에 덤프된 스택 또는 메모리 영역에 민감한 데이터를 포함할 수 있습니다. 이 출력은 FIPS 모드에서 무시되어야 합니다.

다음 예에서는 crashinfo 정보가 없음을 보여줍니다.

```
> show crashinfo
------------------ show crashinfo module 1 ------------------
INFO: This module has no crashinfo available.
```

다음 예에서는 현재 충돌 정보 컨피그레이션을 표시하는 방법을 보여 줍니다.

```
> show crashinfo save
crashinfo save enable
```

다음 예에서는 crashinfo 콘솔 출력의 상태를 보여줍니다.

```
> show crashinfo console
crashinfo console enable
```

다음 예에서는 충돌 파일 테스트에 대한 출력을 보여 줍니다. 이 테스트에서는 실제로 Firepower Threat Defense 디바이스가 충돌하지 않습니다. 시뮬레이션된 예제 파일을 제공합니다.

```
> crashinfo test
> show crashinfo
: Saved_Test_Crash
Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
(...Remaining output truncated...)
```

명령	설명
clear crashinfo	충돌 파일의 내용을 삭제합니다.
crashinfo force	강제로 Firepower Threat Defense 디바이스의 충돌을 발생시킵니다.
crashinfo test	충돌 정보를 플래시 메모리의 파일에 저장하는 Firepower Threat Defense 디바이스의 기능을 테스트합니다.

show crypto accelerator load-balance

하드웨어 암호화 가속화 MIB의 가속화 특정 로드 밸런싱 정보를 표시하려면 **show crypto accelerator load-balance** 명령을 사용합니다.

show crypto accelerator load-balance [**ipsec** | **ssl** | **detail** [**ipsec** |**ssl**]]

detail	(선택 사항) 자세한 정보를 표시합니다. 이 옵션 이후에 **ipsec** 또는 **ssl** 키워드를 포함할 수 있습니다.
ipsec	(선택 사항) 암호화 가속기 IPSec 로드 밸런싱 세부 사항을 표시합니다.
ssl	(선택 사항) 암호화 가속기 SSL 로드 밸런싱 세부 사항을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 전역 암호화 가속기 로드 밸런싱 통계를 보여줍니다.

```
> show crypto accelerator load-balance

                  Crypto IPSEC Load Balancing Stats:
                  ==================================

Engine      Crypto Cores             IPSEC Sessions          Active Session
                                                             Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 1      Total:     0  Active:     0          0.0%

Commands Completed       1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Engine 0 Per Core Load Balancing Stats:
=======================================

Commands Completed       1 second         5 second        60 second
==================       ========         ========         =========
```

```
 IPSec ring 0   (load)      0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 IPSec ring 0   (load)      0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 IPSec ring 0   (load)      0.0%             0.0%             0.0%

                  Crypto SSL Load Balancing Stats:
                  ================================

Engine      Crypto Cores             SSL Sessions             Active Session
                                                              Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 1      Total:     0  Active:     0          0.0%

Commands Completed       1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Engine 0 (load)            0.0%             0.0%             0.0%

Engine 0 Per Core Load Balancing Stats:
=======================================

Commands Completed       1 second         5 second         60 second
==================       ========         ========         =========
 Admin ring 0   (load)      0.0%             0.0%             0.0%

Encrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Admin ring 0   (load)      0.0%             0.0%             0.0%

Decrypted Data           1 second         5 second         60 second
==================       ========         ========         =========
 Admin ring 0   (load)      0.0%             0.0%             0.0%
```

명령	설명
clear crypto accelerator statistics	암호화 가속기 MIB에서 전역 및 가속기 관련 통계를 지웁니다.
clear crypto protocol statistics	암호화 가속기 MIB에서 프로토콜 관련 통계를 지웁니다.
show crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 표시합니다.

show crypto accelerator statistics

하드웨어 암호화 가속기 MIB에서 전역 및 가속기 관련 통계를 표시하려면 **show crypto accelerator statistics** 명령을 사용합니다.

show crypto accelerator statistics

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

출력 통계는 다음과 같이 정의됩니다.

Accelerator 0은 소프트웨어 기반 암호화 엔진에 대한 통계를 표시합니다.

Accelerator 1은 하드웨어 기반 암호화 엔진에 대한 통계를 표시합니다.

RSA 통계는 기본적으로 소프트웨어에서 실행되는 2048비트 키에 대한 RSA 작업을 표시합니다. 즉, 2048비트 키가 있는 경우 IKE/SSL VPN은 IPsec/SSL 협상 단계 중에 소프트웨어에서 RSA 작업을 수행합니다. 실제 IPsec/SSL 트래픽은 여전히 하드웨어를 통해 처리됩니다. 이로 인해 동시에 시작하는 동시 세션이 많은 경우 CPU 사용량이 높아져 여러 RSA 키 작업이 수행되고 CPU 사용량이 증가할 수 있습니다. 따라서 CPU 사용량이 많은 조건에서 실행할 경우 1024비트 키를 사용하여 하드웨어에서 RSA 키 작업을 처리해야 합니다. 이렇게 하려면 ID 인증서를 다시 등록해야 합니다. 릴리스 8.3(2) 이상에서는 5510~5550 플랫폼에서 crypto engine large-mod-accel 명령을 사용하여 이러한 작업을 하드웨어에서 수행할 수도 있습니다.

2048비트 RSA 키를 사용하고 RSA 처리를 소프트웨어에서 수행하는 경우 CPU 프로파일링을 사용하여 CPU 사용량을 증가시키는 기능을 확인할 수 있습니다. 일반적으로 bn_* 및 BN_* 함수는 RSA에 사용된 대용량 데이터 집합에 대한 수학 연산이며, 소프트웨어에서 RSA 작업을 수행하는 동안 CPU 사용량을 검사할 때 가장 유용합니다. 예를 들면 다음과 같습니다.

```
@@@@@@@@@@@@@@@@@@@@.............................. 36.50% : _bn_mul_add_words
@@@@@@@@@@..................................... 19.75% : _bn_sqr_comba8
```

Diffie-Hellman 통계는 모듈러스(modulus) 크기가 1024보다 큰 암호화 작업이 소프트웨어에서 수행되고 있음을 보여 줍니다(예: DH5(Diffie-Hellman 그룹 5에서 1536 사용)). 이 경우 2048비트 키 인증서는 소프트웨어에서 처리되며, 이로 인해 많은 세션이 실행 중인 경우 CPU 사용량이 증가할 수 있습니다.

DSA 통계는 2단계로 키 생성을 보여 줍니다. 첫 번째 단계에서는 시스템의 여러 사용자 간에 공유할 수 있는 알고리즘 파라미터를 선택합니다. 두 번째 단계에서는 단일 사용자의 개인 키 및 공개 키를 계산합니다.

SSL 통계는 하드웨어 암호화 가속기에 대한 SSL 트랜잭션에 포함된 프로세서 집약적 공개 키 암호화 알고리즘에 대한 기록을 보여줍니다.

RNG 통계는 키로 사용할 동일한 난수 집합을 자동으로 생성할 수 있는 발신자 및 수신자에 대한 기록을 보여줍니다.

다음 예에서는 전역 암호화 가속기 통계를 보여줍니다.

```
> show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
```

```
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                            Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                            SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                            IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 1
      Random number request failures: 0
```

다음 표는 출력에 대해 설명합니다.

출력	설명
Capacity	이 섹션은 Firepower Threat Defense 디바이스에서 지원할 수 있는 암호화 가속과 관련이 있습니다.
Supports hardware crypto	(True/False) Firepower Threat Defense 디바이스는 하드웨어 암호화 가속을 지원할 수 있습니다.
Supports modular hardware crypto	(True/False) 지원되는 하드웨어 암호화 가속기를 별도의 플러그인 카드 또는 모듈로 삽입할 수 있습니다.

출력	설명
Max accelerators	Firepower Threat Defense 디바이스에서 지원하는 하드웨어 암호화 가속기의 최대 개수입니다.
Mac crypto throughput	디바이스에 대한 최대 정격 VPN 처리량입니다.
Max crypto connections	디바이스에 대해 지원되는 최대 VPN 터널 수입니다.
Global Statistics	이 섹션은 디바이스에 통합된 하드웨어 암호화 가속기와 관련이 있습니다.
Number of active accelerators	활성 하드웨어 가속기 수입니다. 활성 하드웨어 가속기가 초기화되었으며, 암호화 명령을 처리할 수 있습니다.
Number of non-operational accelerators	비활성 하드웨어 가속기 수입니다. 비활성 하드웨어 가속기가 감지되었지만 초기화를 완료하지 않았거나 실패하여 더 이상 사용할 수 없습니다.
Input packets	모든 하드웨어 암호화 가속기에서 처리된 인바운드 패킷 수입니다.
Input bytes	처리된 인바운드 패킷의 데이터 바이트 수입니다.
Output packets	모든 하드웨어 암호화 가속기에서 처리된 아웃바운드 패킷 수입니다.
Output error packets	모든 하드웨어 암호화 가속기에서 처리된 아웃바운드 패킷 중 오류가 탐지된 패킷 수입니다.
Output bytes	처리된 아웃바운드 패킷의 데이터 바이트 수입니다.
Accelerator 0	이 섹션은 각각 암호화 가속기와 관련이 있습니다. 첫 번째(Accelerator 0)는 항상 소프트웨어 암호화 엔진입니다. 하드웨어 가속기가 아니지만 Firepower Threat Defense는 이를 사용하여 특정 암호화 작업을 수행하며 해당 통계가 여기에 표시됩니다. Accelerator 1 이상은 항상 하드웨어 암호화 가속기입니다.
Status	가속기가 초기화 중인지, 활성 상태인지 또는 실패했는지를 나타내는 가속기의 상태입니다.
Software crypto engine	가속기 유형 및 펌웨어 버전(해당되는 경우)입니다.
Slot	가속기의 슬롯 번호(해당 되는 경우)입니다.
Active time	가속기가 활성 상태로 유지된 기간입니다.

출력	설명
Total crypto transforms	가속기가 수행한 총 암호화 명령 수입니다.
Total dropped packets	오류로 인해 가속기에서 드롭된 총 패킷 수입니다.
Input statistics	이 섹션은 가속기에서 처리된 입력 트래픽과 관련이 있습니다. 입력 트래픽은 해독 및/또는 인증해야 하는 암호 텍스트로 간주됩니다.
Input packets	가속기에서 처리된 입력 패킷 수입니다.
Input bytes	가속기에서 처리된 입력 바이트 수입니다.
Input hashed packets	가속기에서 해시 작업을 수행한 패킷 수입니다.
Input hashed bytes	가속기에서 해시 작업을 수행한 바이트 수입니다.
Decrypted packets	가속기에서 대칭 암호 해독 작업을 수행한 패킷 수입니다.
Decrypted bytes	가속기에서 대칭 암호 해독 작업을 수행한 바이트 수입니다.
Output statistics	이 섹션은 가속기에서 처리된 출력 트래픽과 관련이 있습니다. 입력 트래픽은 암호화 및/또는 해시되어야 하는 일반 텍스트로 간주됩니다.
Output packets	가속기에서 처리된 출력 패킷 수입니다.
Output bad packets	가속기에서 처리된 출력 패킷 중 오류가 탐지된 패킷 수입니다.
Output bytes	가속기에서 처리된 출력 패킷 수입니다.
Output hashed packets	가속기에서 아웃바운드 해시 작업을 수행한 패킷 수입니다.
Output hashed bytes	가속기에서 아웃바운드 해시 작업을 수행한 바이트 수입니다.
Encyrpted packets	가속기에서 대칭 암호화 작업을 수행한 패킷 수입니다.
Encyrpted bytes	가속기에서 대칭 암호화 작업을 수행한 바이트 수입니다.
Diffie-Hellman statistics	이 섹션은 Diffie-Hellman 키 교환 작업과 관련이 있습니다.
Keys generated	가속기에서 생성된 Diffie-Hellman 키 집합 수입니다.
Secret keys derived	가속기에서 파생된 Diffie-Hellman 공유 암호 수입니다.
RSA statistics	이 섹션은 RSA 암호화 작업과 관련이 있습니다.

출력	설명
Keys generated	가속기에서 생성된 RSA 키 집합 수입니다.
Signatures	가속기에서 수행된 RSA 서명 작업 수입니다.
Verifications	가속기에서 수행된 RSA 서명 확인 수입니다.
Encrypted packets	가속기에서 RSA 암호화 작업을 수행한 패킷 수입니다.
Decrypted packets	가속기에서 RSA 암호 해독 작업을 수행한 패킷 수입니다.
Decrypted bytes	가속기에서 RSA 암호 해독 작업을 수행한 데이터의 바이트 수입니다.
DSA statistics	이 섹션은 DSA 작업과 관련이 있습니다. DSA는 현재 버전 8.2에서 지원되지 않으므로 이러한 통계는 더 이상 표시되지 않습니다.
Keys generated	가속기에서 생성된 DSA 키 집합 수입니다.
Signatures	가속기에서 수행된 DSA 서명 작업 수입니다.
Verifications	가속기에서 수행된 DSA 서명 확인 수입니다.
SSL statistics	이 섹션은 SSL 레코드 처리 작업과 관련이 있습니다.
Outbound records	가속기에서 암호화 및 인증된 SSL 레코드 수입니다.
Inbound records	가속기에서 암호 해독 및 인증된 SSL 레코드 수입니다.
RNG statistics	이 섹션은 난수 생성과 관련이 있습니다.
Random number requests	가속기에 대한 난수 요청 수입니다.
Random number request failures	가속기에 대한 성공하지 못한 난수 요청 수입니다.

명령	설명
clear crypto accelerator statistics	암호화 가속기 MIB에서 전역 및 가속기 관련 통계를 지웁니다.
clear crypto protocol statistics	암호화 가속기 MIB에서 프로토콜 관련 통계를 지웁니다.

명령	설명
show crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 표시합니다.

show crypto ca certificates

특정 트러스트 포인트와 연결된 인증서를 표시하거나, 시스템에 설치된 모든 인증서를 표시하려면 **show crypto ca certificates** 명령을 사용합니다.

show crypto ca certificates [*trustpointname*]

trustpointname	(선택 사항) 트러스트 포인트의 이름입니다. 이름을 지정하지 않은 경우 이 명령은 Firepower Threat Defense 디바이스에 설치된 모든 인증서를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show crypto ca certificates** 명령의 샘플 출력입니다.

```
>show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
   Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = example.com
   CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
   Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
   Associated Trustpoints: tp2 tp1
```

show crypto ca crls

모든 캐시된 CRL(Certificate Revocation List)을 표시하거나 지정된 트러스트 포인트에 대해 캐시된 모든 CRL을 표시하려면 **show crypto ca crl** 명령을 사용합니다.

show crypto ca crls [**trustpool** | **trustpoint** *trustpointname*]

trustpoint*trustpointname*	(선택 사항) 트러스트 포인트의 이름입니다. 이름을 지정하지 않은 경우 이 명령은 Firepower Threat Defense 디바이스에 캐시된 모든 CRL을 표시합니다.
trustpool	모든 트러스트 풀과 관련된 CRL을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show crypto ca crl** 명령의 샘플 출력입니다.

```
> show crypto ca crl trustpoint tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@example.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
```

show crypto ca trustpoints

CA 트러스트 포인트를 표시하려면 **show crypto ca trustpoints** 명령을 사용합니다.

show crypto ca trustpoints [*trustpoint_name*]

trustpoint_name	(선택 사항) 표시할 트러스트 포인트의 이름입니다.

트러스트 포인트를 지정하지 않는 경우 모든 트러스트 포인트가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 CA 트러스트 포인트를 표시하는 방법을 보여줍니다.

```
> show crypto ca trustpoints
Trustpoint ftd-self:
    Configured for self-signed certificate generation.
```

show crypto ca trustpool

신뢰 풀을 구성하는 인증서를 표시하려면 **show crypto ca trustpool** 명령을 사용합니다.

show crypto ca trustpool [**detail** | **policy**]

detail	(선택 사항) 인증서 세부 사항을 표시합니다.
policy	(선택 사항) 구성된 신뢰 풀 정책을 표시합니다.

이 명령은 모든 신뢰 풀 인증서를 축약된 형식으로 표시합니다. **detail** 옵션을 지정하면 추가 정보가 포함됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show crypto ca trustpool 명령의 출력에 각 인증서의 지문 값이 포함됩니다. 이러한 값은 제거 작업에 필요합니다.

다음 예에서는 신뢰 풀에서 인증서를 표시하는 방법을 보여줍니다.

```
> show crypto ca trustpool
CA Certificate
Status: Available
Certificate Serial Number: 6c386c409f4ff4944154635da520ed4c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name: cn=bxb2008-root
dc=bdb2008
dc=mycompany
dc=com
Subject Name:
cn=bxb2008-root
dc=bxb2008
dc=cisco
dc=com
Validity Date:
start date:17:21:06 EST Jan 14 2009
```

```
end date:17:31:06 EST Jan 14 2024
CA Certificate
Status: Available
Certificate Serial Number: 58d1c756000000000059
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=bxb2008-root
dc=bxb2008
dc=mycompany
dc=com
Subject Name:
cn=BXB2008SUB1-CA
dc=bxb2008
dc=cisco
dc=com
OCSP AIA:
URL: http://bxb2008-1.bxb2008.mycompany.com/ocsp
CRL Distribution Points:
(1) http://bxb2008-1.bxb2008.mycompany.com/CertEnroll/bxb2008-root.crl
Validity Date:
start date:11:54:34 EST May 18 2009
end date:12:04:34 EST May 18 2011
```

다음 예에서는 신뢰 풀 정책을 표시하는 방법을 보여줍니다.

```
> show crypto ca trustpool policy
800 trustpool certificates installed
Trustpool auto import statistics:
 Last import result: SUCCESS
 Next scheduled import at 22:00:00 Tues Jul 21 2015
Trustpool Policy
Trustpool revocation checking is disabled
CRL cache time: 123 seconds
CRL next update field: required and forced
Automatic import of trustpool certificates is enabled
Automatic import URL: http://www.thawte.com
Download time: 22:00:00
Policy overrides:
map: map1
match:issuer-name eq cn=Mycompany Manufacturing CA
match:issuer-name eq cn=Mycompany CA
action:skip revocation-check
map: map2
match: issuer-name eq cn=mycompany Manufacturing CA
match: issuer-name eq cn=mycompany CA2
action: allowed expired certificates
```

명령	설명
clear crypto ca trustpool	신뢰 풀에서 모든 인증서를 제거합니다.

show crypto debug-condition

현재 구성된 필터, 일치하지 않는 상태, IPsec 및 ISAKMP 디버깅 메시지의 오류 상태를 표시하려면 **show crypto debug-condition** 명령을 사용합니다.

show crypto debug-condition

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 필터링 조건을 보여 줍니다.

```
> show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag:  OFF
IPsec debug context unmatched flag:  ON
IKE peer IP address filters:
1.1.1.0/24   2.2.2.2
IKE user name filters:
my_user
```

명령	설명
debug crypto condition	IPsec 및 ISAKMP 디버깅 메시지에 대한 필터링 조건을 설정합니다.
debug crypto condition error	필터링 조건이 지정되었는지 여부에 상관없이 디버깅 메시지를 표시합니다.
debug crypto condition unmatched	상황 정보가 부족하여 필터링할 수 없는 IPsec 및 ISAKMP에 대한 디버깅 메시지를 표시합니다.

show crypto ikev1

IKEv1(Internet Key Exchange version 1)에 대한 정보를 표시하려면 **show crypto ikev1** 명령을 사용합니다.

show crypto ikev1 {**ipsec-over-tcp** | **sa** [**detail**] | **stats**}

ipsec-over-tcp	TCP를 통한 IPsec 데이터를 표시합니다.
sa [**detail**]	IKEv1 SA(런타임 보안 연결) 데이터베이스에 대한 정보를 표시합니다. SA 데이터베이스에 대한 자세한 출력을 표시하려면 **detail** 키워드를 포함합니다.
stats	IKEv1 통계를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 SA 데이터베이스에 대한 세부 정보를 표시합니다. detail 키워드를 포함하지 않는 경우, IKE 피어, 유형, Dir, Rky 및 상태 열이 표시됩니다.

```
> show crypto ikev1 sa detail
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

다음 예는 TCP를 통한 IPsec 데이터를 표시합니다.

```
> show crypto ikev1 ipsec-over-tcp
Global IKEv1 IPSec over TCP Statistics
--------------------------------
Embryonic connections: 0
Active connections: 0
Previous connections: 0
Inbound packets: 0
Inbound dropped packets: 0
```

```
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 0
Recevied ACK heart-beat packets: 0
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
```

다음 예는 전역 IKEv1 통계를 표시합니다.

```
> show crypto ikev1 stats
Global IKEv1 Statistics
  Active Tunnels:              0
  Previous Tunnels:            0
  In Octets:                   0
  In Packets:                  0
  In Drop Packets:             0
  In Notifys:                  0
  In P2 Exchanges:             0
  In P2 Exchange Invalids:     0
  In P2 Exchange Rejects:      0
  In P2 Sa Delete Requests:    0
  Out Octets:                  0
  Out Packets:                 0
  Out Drop Packets:            0
  Out Notifys:                 0
  Out P2 Exchanges:            0
  Out P2 Exchange Invalids:    0
  Out P2 Exchange Rejects:     0
  Out P2 Sa Delete Requests:   0
  Initiator Tunnels:           0
  Initiator Fails:             0
  Responder Fails:             0
  System Capacity Fails:       0
  Auth Fails:                  0
  Decrypt Fails:               0
  Hash Valid Fails:            0
  No Sa Fails:                 0

IKEV1 Call Admission Statistics
  Max In-Negotiation SAs:                50
  In-Negotiation SAs:                     0
  In-Negotiation SAs Highwater:           0
  In-Negotiation SAs Rejected:            0
```

명령	설명
show crypto ikev2 sa	IKEv2 런타임 SA 데이터베이스를 표시합니다.
show running-config crypto isakmp	모든 활성 ISAKMP 구성을 표시합니다.

show crypto ikev2

IKEv2(Internet Key Exchange version 2)에 대한 정보를 표시하려면 **show crypto ikev2** 명령을 사용합니다.

show crypto ikev2 {**sa** [**detail**] | **stats**}

sa [**detail**]	IKEv2 SA(런타임 보안 연결) 데이터베이스에 대한 정보를 표시합니다. SA 데이터베이스에 대한 자세한 출력을 표시하려면 **detail** 키워드를 포함합니다.
stats	IKEv2 통계를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 SA 데이터베이스에 대한 세부 정보를 표시합니다.

```
> show crypto ikev2 sa detail
IKEv2 SAs:
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id            Local             Remote              Status   Role
671069399            10.0.0.0/500      10.255.255.255/500  READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/188 sec
      Session-id: 1
      Status Description: Negotiation done
      Local spi: 80173A0373C2D403       Remote spi: AE8AEFA1B97DBB22
      Local id: asa
      Remote id: asa1
      Local req mess id: 8              Remote req mess id: 7
      Local next mess id: 8             Remote next mess id: 7
      Local req queued: 8               Remote req queued: 7
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0x242a3da5/0xe6262034
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

다음 예는 IKEv2 통계를 표시합니다.

```
> show crypto ikev2 stats
Global IKEv2 Statistics
  Active Tunnels:                          0
  Previous Tunnels:                        0
  In Octets:                               0
  In Packets:                              0
  In Drop Packets:                         0
  In Drop Fragments:                       0
  In Notifys:                              0
  In P2 Exchange:                          0
  In P2 Exchange Invalids:                 0
  In P2 Exchange Rejects:                  0
  In IPSEC Delete:                         0
  In IKE Delete:                           0
  Out Octets:                              0
  Out Packets:                             0
  Out Drop Packets:                        0
  Out Drop Fragments:                      0
  Out Notifys:                             0
  Out P2 Exchange:                         0
  Out P2 Exchange Invalids:                0
  Out P2 Exchange Rejects:                 0
  Out IPSEC Delete:                        0
  Out IKE Delete:                          0
  SAs Locally Initiated:                   0
  SAs Locally Initiated Failed:            0
  SAs Remotely Initiated:                  0
  SAs Remotely Initiated Failed:           0
  System Capacity Failures:                0
  Authentication Failures:                 0
  Decrypt Failures:                        0
  Hash Failures:                           0
  Invalid SPI:                             0
  In Configs:                              0
  Out Configs:                             0
  In Configs Rejects:                      0
  Out Configs Rejects:                     0
  Previous Tunnels:                        0
  Previous Tunnels Wraps:                  0
  In DPD Messages:                         0
  Out DPD Messages:                        0
  Out NAT Keepalives:                      0
  IKE Rekey Locally Initiated:             0
  IKE Rekey Remotely Initiated:            0
  CHILD Rekey Locally Initiated:           0
  CHILD Rekey Remotely Initiated:          0

IKEV2 Call Admission Statistics
  Max Active SAs:                   No Limit
  Max In-Negotiation SAs:                250
  Cookie Challenge Threshold:          Never
  Active SAs:                              0
  In-Negotiation SAs:                      0
  Incoming Requests:                       0
  Incoming Requests Accepted:              0
  Incoming Requests Rejected:              0
  Outgoing Requests:                       0
  Outgoing Requests Accepted:              0
  Outgoing Requests Rejected:              0
  Rejected Requests:                       0
  Rejected Over Max SA limit:              0
  Rejected Low Resources:                  0
  Rejected Reboot In Progress:             0
  Cookie Challenges:                       0
```

```
Cookie Challenges Passed:                0
Cookie Challenges Failed:                0
```

명령	설명
show crypto ikev1 sa	IKEv1 런타임 SA 데이터베이스를 표시합니다.
show running-config crypto isakmp	모든 활성 ISAKMP 구성을 표시합니다.

show crypto ipsec df-bit

지정된 인터페이스에 대한 IPsec 패킷의 IPsec DF 비트 정책을 표시하려면 **show crypto ipsec df-bit** 명령을 사용합니다.

show crypto ipsec df-bit *interface*

interface	인터페이스 이름을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 inside라는 인터페이스에 대한 IPsec DF 비트 정책을 표시합니다.

```
>show crypto ipsec df-bit inside
df-bit inside copy
```

명령	설명
show crypto ipsec fragmentation	IPsec 패킷에 대한 프래그멘테이션 정책을 표시합니다.

show crypto ipsec fragmentation

IPsec 패킷에 대한 프래그멘테이션 정책을 표시하려면 **show cryptoipsec fragmentation** 명령을 사용합니다.

show crypto ipsec fragmentation *interface*

interface	인터페이스 이름을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 inside라는 인터페이스에 대한 IPsec 프래그멘테이션 정책을 표시합니다.

```
> show crypto ipsec fragmentation inside
fragmentation inside before-encryption
```

명령	설명
show crypto ipsec df-bit	지정된 인터페이스에 대한 DF 비트 정책을 표시합니다.

show crypto ipsec policy

OSPFv3에서 제공된 IPsec SS API(secure socket API) 보안 정책 정보를 표시하려면 **show crypto ipsec policy** 명령을 사용합니다. 이 명령의 대체 형식인 **show ipsec policy**를 사용할 수도 있습니다.

show crypto ipsec policy [*name*]

name	정책 이름을 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 CSSU-UTF라는 정책에 대한 암호화 보안 소켓 API에서 설치된 정책 정보를 표시합니다.

```
> show crypto ipsec policy
Crypto IPsec client security policy data
       Policy name:      CSSU-UTF
       Policy refcount:  0
       Inbound  ESP SPI:        1031 (0x407)
       Outbound ESP SPI:        1031 (0x407)
       Inbound  ESP Auth Key:   0123456789abcdef
       Outbound ESP Auth Key:   0123456789abcdef
       Inbound  ESP Cipher Key:
       Outbound ESP Cipher Key:
       Transform set:    esp-sha-hmac
```

명령	설명
show crypto ipsec fragmentation	IPsec 패킷에 대한 프래그멘테이션 정책을 표시합니다.
show crypto ipsec sa	IPsec SA 목록을 표시합니다.
show crypto ipsec df-bit	지정된 인터페이스에 대한 DF 비트 정책을 표시합니다.
show crypto sockets	암호화 보안 소켓 및 소켓 상태를 표시합니다.

show crypto ipsec sa

IPsec SA의 목록을 표시하려면 **show crypto ipsec sa** 명령을 사용합니다. 이 명령의 대체 형식인 **show ipsec sa**를 사용할 수도 있습니다.

show crypto ipsec sa [**assigned-address** | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr* | **spi** | **summary** | **user**] [**detail**]

assigned-address	(선택 사항) 할당된 주소에 대한 IPsec SA를 표시합니다.
detail	(선택 사항) 표시된 항목에 대한 자세한 오류 정보를 표시합니다.
entry	(선택 사항) 피어 주소별로 정렬된 IPsec SA를 표시합니다.
ID	(선택 사항) ESP를 포함하지 않고 ID별로 정렬된 IPsec SA를 표시합니다. 이는 축소된 형식입니다.
inactive	(선택 사항) 비활성 IPsec SA를 표시합니다.
map*map-name*	(선택 사항) 지정된 암호화 맵에 대한 IPsec SA를 표시합니다.
peer*peer-addr*	(선택 사항) 지정된 피어 IP 주소에 대한 IPsec SA를 표시합니다.
spi	(선택 사항) SPI에 대한 IPsec SA를 표시합니다.
요약	(선택 사항) 유형별 IPsec SA 요약을 표시합니다.
user	(선택 사항) 사용자에 대한 IPsec SA를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 OSPFv3로 식별된 터널을 포함하는 IPsec SA를 표시합니다.

```
> show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

참고 조각화 통계는 IPsec SA 정책에 IPsec 처리 전 조각화가 발생하도록 규정된 경우 사전 조각화 통계입니다. 사후 조각화 통계는 SA 정책에 IPsec 처리 후 조각화가 발생하도록 규정된 경우에 표시됩니다.

다음 예에서는 def라는 암호화 맵에 대한 IPsec SA를 표시합니다.

```
> show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
```

```
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 3, crypto-map: def
        sa timing: remaining key lifetime (sec): 480
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
```

다음 예에서는 키워드 **entry**에 대한 IPsec SA를 보여줍니다.

```
> show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
```

```
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
```

다음 예에서는 키워드 **entry detail**에 대한 IPsec SA를 보여줍니다.

```
> show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
```

```
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
```

다음 예에서는 키워드 **identity**에 대한 IPsec SA를 보여줍니다.

```
> show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
```

```
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

다음 예에서는 키워드 **identity** 및 **detail**에 대한 IPsec SA를 보여줍니다.

```
> show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
```

```
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
#pkts no sa (send): 0, #pkts invalid sa (rcv): 0
#pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
#pkts invalid prot (rcv): 0, #pkts verify failed: 0
#pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
#pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
#pkts replay failed (rcv): 0
#pkts internal err (send): 0, #pkts internal err (rcv): 0

local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: 3B6F6A35
```

명령	설명
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 ISAKMP 구성을 표시합니다.

show crypto ipsec stats

IPsec 통계의 목록을 표시하려면 **show crypto ipsec stats** 명령을 사용합니다.

show crypto ipsec stats

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 IPsec 통계를 표시합니다.

```
> show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
 Fragmentation successes: 3
  Pre-fragmentation successes:2
  Post-fragmentation successes: 1
 Fragmentation failures: 2
  Pre-fragmentation failures:1
  Post-fragmentation failures: 1
 Fragments created: 10
 PMTUs sent: 1
 PMTUs recvd: 2
Protocol failures: 0
```

```
Missing SA failures: 0
System capacity failures: 0
```

명령	설명
clear ipsec sa	지정된 파라미터를 기반으로 IPsec SA 또는 카운터를 지웁니다.
show ipsec sa	지정된 파라미터를 기반으로 IPsec SA를 표시합니다.
show ipsec sa summary	IPsec SA 요약을 표시합니다.

show crypto isakmp

IKEv1 및 IKEv2 모두에 대한 ISAKMP 정보를 표시하려면 **show crypto isakmp** 명령을 사용합니다.

show crypto isakmp {**sa** [**detail**] | **stats**}

sa [**detail**]	런타임 SA(security association) 데이터베이스에 대한 정보를 표시합니다. SA 데이터베이스에 대한 자세한 출력을 표시하려면 **detail** 키워드를 포함합니다.
stats	IKEv1 및 IKEv2 통계를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

Show crypto isakmp 명령은 동등한 **show crypto ikev1** 및 **show crypto ikev2** 명령의 출력을 결합합니다.

다음은 SA 정보 읽기에 대한 몇 가지 팁입니다.

- Rky는 아니요 또는 예일 수 있습니다. 예인 경우, rekey가 발생하고 있으며 두 번째로 일치하는 SA는 rekey가 완료될 때까지 다른 상태가 됩니다.
- 역할은 이니시에이터 또는 응답자 상태입니다. 이는 SA의 상태 시스템의 현재 상태입니다.
- State — MM_ACTIVE 또는 AM_ACTIVE 중 한 가지 값을 지닌 데이터를 전달하는 작동 중인 터널입니다.

다음 예는 SA 데이터베이스에 대한 세부 정보를 표시합니다.

```
> show crypto isakmp sa detail

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
```

```
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

다음 예에서는 ISAKMP 통계를 표시합니다. IKEv1 및 IKEv2는 별도로 표시됩니다.

```
> show crypto isakmp stats

Global IKEv1 Statistics
  Active Tunnels:              136
  Previous Tunnels:            0
  In Octets:                   0
  In Packets:                  0
  In Drop Packets:             0
  In Notifys:                  0
  In P2 Exchanges:             0
  In P2 Exchange Invalids:     0
  In P2 Exchange Rejects:      0
  In P2 Sa Delete Requests:    0
  Out Octets:                1344
  Out Packets:                 8
  Out Drop Packets:            0
  Out Notifys:                 0
  Out P2 Exchanges:            0
  Out P2 Exchange Invalids:    0
  Out P2 Exchange Rejects:     0
  Out P2 Sa Delete Requests:   0
  Initiator Tunnels:           2
  Initiator Fails:             2
  Responder Fails:             0
  System Capacity Fails:       0
  Auth Fails:                  0
  Decrypt Fails:               0
  Hash Valid Fails:            0
  No Sa Fails:                 0

IKEV1 Call Admission Statistics
  Max In-Negotiation SAs:                50
  In-Negotiation SAs:                    0
  In-Negotiation SAs Highwater:          0
  In-Negotiation SAs Rejected:           0
In Drop Packets: 925

Global IKEv2 Statistics
  Active Tunnels:                        132
  Previous Tunnels:                      132
  In Octets:                             195471
  In Packets:                            1854
  In Drop Packets:                       925
  In Drop Fragments:                     0
  In Notifys:                            0
  In P2 Exchange:                        132
  In P2 Exchange Invalids:               0
  In P2 Exchange Rejects:                0
  In IPSEC Delete:                       0
  In IKE Delete:                         0
  Out Octets:                            119029
  Out Packets:                           796
  Out Drop Packets:                      0
  Out Drop Fragments:                    0
  Out Notifys:                           264
  Out P2 Exchange:                       0
Out P2 Exchange Invalids:              0
  Out P2 Exchange Rejects:               0
  Out IPSEC Delete:                      0
  Out IKE Delete:                        0
  SAs Locally Initiated:                 0
  SAs Locally Initiated Failed:          0
  SAs Remotely Initiated:                0
  SAs Remotely Initiated Failed:         0
  System Capacity Failures:              0
```

```
  Authentication Failures:                0
  Decrypt Failures:                       0
  Hash Failures:                          0
  Invalid SPI:                            0
  In Configs:                             0
  Out Configs:                            0
  In Configs Rejects:                     0
  Out Configs Rejects:                    0
  Previous Tunnels:                       0
  Previous Tunnels Wraps:                 0
  In DPD Messages:                        0
  Out DPD Messages:                       0
  Out NAT Keepalives:                     0
  IKE Rekey Locally Initiated:            0
  IKE Rekey Remotely Initiated:           0
  CHILD Rekey Locally Initiated:          0
  CHILD Rekey Remotely Initiated:         0

IKEV2 Call Admission Statistics
  Max Active SAs:                   No Limit
  Max In-Negotiation SAs:                300
  Cookie Challenge Threshold:            150
  Active SAs:                              0
  In-Negotiation SAs:                      0
  Incoming Requests:                       0
  Incoming Requests Accepted:              0
  Incoming Requests Rejected:              0
  Outgoing Requests:                       0
  Outgoing Requests Accepted:              0
  Outgoing Requests Rejected:              0
  Rejected Requests:                       0
  Rejected Over Max SA limit:              0
  Rejected Low Resources:                  0
  Rejected Reboot In Progress:             0
  Cookie Challenges:                       0
  Cookie Challenges Passed:                0
  Cookie Challenges Failed:                0
```

명령	설명
clear crypto isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config crypto isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show crypto key mypubkey

키 이름, 사용량, ECDSA 또는 RSA 키에 대한 타원 곡선 크기를 표시하려면 **show crypto key mypubkey** 명령을 사용합니다.

show crypto key mypubkey {**ecdsa** | **rsa**}

ecdsa	ECDSA 공개 키를 표시합니다.
rsa	RSA 공개 키를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음의 예는 RSA 공개 키를 표시합니다.

```
> show crypto key mypubkey rsa
Key pair was generated at: 18:19:26 UTC May 26 2016
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 1024
 Key Data:

  30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c0bf77
  d651ead6 fca31c72 12064272 36f699b9 e971e198 1503ba6b f0112b63 97252a26
  38827d83 cd71863e b8962da5 bb905a47 666452a1 9eb1a36e dd8aab00 0e4493f1
  4422bf09 4bcfcb95 a83d38a9 7b9caba6 83c9b5b2 cff251f8 a0422a68 3690c9e5
  0cbbe83b 1a8b2460 1f83b43b a9b06912 7cc9f7f9 f596b81e e2a7bde7 8f020301
  0001
>
```

show crypto protocol statistics

암호화 가속기 MIB의 프로토콜 관련 통계를 표시하려면 **show crypto protocol statistics** 명령을 사용합니다.

show crypto protocol statistics *protocol*

protocol	통계를 표시할 프로토콜의 이름을 지정합니다. 프로토콜 선택 항목은 다음과 같습니다. **ikev1** - IKE(Internet Key Exchange) 버전 1 **ikev2** - IKE(Internet Key Exchange) 버전 2 **ipsec** - IP 보안 Phase-2 프로토콜 **ssl** - SSL(Secure Sockets Layer) **ssh-** - SSH(Secure Shell) 프로토콜 **srtp** - SRTP(Secure Real-Time Transport Protocol) **other** - 새 프로토콜용으로 예약됨 **all** - 현재 지원되는 모든 프로토콜

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 모든 프로토콜에 대한 암호화 가속기 통계를 표시합니다.

```
> show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
   SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
```

```
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
>
```

명령	설명
clear crypto accelerator statistics	암호화 가속기 MIB에서 전역 및 가속기 관련 통계를 지웁니다.
clear crypto protocol statistics	crypto accelerator MIB의 프로토콜 관련 통계를 지웁니다.
show crypto accelerator statistics	crypto accelerator MIB의 전역 및 가속기 관련 통계를 표시합니다.

show crypto sockets

암호화 보안 소켓 정보를 표시하려면 **show crypto sockets** 명령을 사용합니다.

show crypto sockets

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 암호화 보안 소켓 정보를 표시합니다.

```
> show crypto sockets
Number of Crypto Socket connections 1

       Gi0/1  Peers: (local): 2001:1::1
                     (remote): ::
              Local Ident (addr/plen/port/prot): (2001:1::1/64/0/89)
              Remote Ident (addr/plen/port/prot): (::/0/0/89)
              IPsec Profile: "CSSU-UTF"
              Socket State: Open
              Client: "CSSU_App(UTF)" (Client State: Active)

       Crypto Sockets in Listen state:
```

다음 표에는 **show crypto sockets** 명령 출력의 필드에 대한 설명이 나와 있습니다.

필드	설명
Number of Crypto Socket connections	시스템의 암호화 소켓 수입니다.
Socket State	이 상태는 활성 IPsec SA(Security Association: 보안 연계)가 존재하는 경우 Open이고, 활성 IPsec SA가 존재하지 않는 경우 Closed입니다.
Client	애플리케이션 이름과 해당 상태입니다.
Flags	이 필드에 “shared”가 표시된 경우 소켓이 둘 이상의 터널 인터페이스와 공유됩니다.
Crypto Sockets in Listen state	암호화 IPsec 프로파일의 이름입니다.

명령	설명
show crypto ipsec policy	암호화 보안 소켓 API에서 설치된 정책 정보를 표시합니다.

show crypto ssl

Firepower Threat Defense 디바이스의 활성 SSL 세션에 대한 정보를 표시하려면 **show crypto ssl** 명령을 사용합니다.

show crypto ssl [**cache** | **ciphers** | **errors** [**trace**] | **mib** [**64**] | **objects**]

cache	(선택 사항) SSL 세션 캐시 통계를 표시합니다.
ciphers	(선택 사항) 사용할 수 있는 SSL 암호를 표시합니다.
errors	(선택 사항) SSL 오류를 표시합니다.
trace	(선택 사항) SSL 오류 추적 정보를 표시합니다.
mib	(선택 사항) SSL MIB 통계를 표시합니다.
64	(선택 사항) SSL MIB 64비트 카운터 통계를 표시합니다.
objects	(선택 사항) SSL 개체 통계를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 사용 설정된 암호 순서, 사용 해제된 암호, 사용 중인 SSL 신뢰 지점, 인증서 인증 사용 여부 등 현재 SSLv3 이상 세션에 대한 정보를 표시합니다.

다음은 **show ssl** 명령의 샘플 출력입니다.

```
> show crypto ssl

Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
```

```
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
Certificate authentication is not enabled
```

SSL 세션 캐시 통계를 표시하려면 **show crypto ssl cache** 명령을 사용합니다.

```
> show crypto ssl cache

SSL session cache statistics:
  Maximum cache size:          100    Current cache size:           0
  Cache hits:                    0    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               0    Accepts successful:           0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
SSL VPNLB session cache statistics:
  Maximum cache size:           10    Current cache size:           0
  Cache hits:                    0    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               0    Accepts successful:           0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
SSLDEV session cache statistics:
  Maximum cache size:           20    Current cache size:           0
  Cache hits:                    0    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               0    Accepts successful:           0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
DTLS session cache statistics:
  Maximum cache size:          100    Current cache size:           0
  Cache hits:                    0    Cache misses:                 0
  Cache timeouts:                0    Cache full:                   0
  Accept attempts:               0    Accepts successful:           0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:          0
  Connect renegotiates:          0
```

SSL 암호 목록을 표시하려면 **show crypto ssl cipher** 명령을 사용합니다.

```
> show crypto ssl cipher

Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
```

```
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
```

show ctiqbe

Firepower Threat Defense 디바이스를 통해 설정된 CTIQBE 세션에 대한 정보를 표시하려면 **show ctiqbe** 명령을 사용합니다.

show ctiqbe

릴리스	수정 사항
6.2	이 명령이 도입되었습니다.

다음은 아래 조건에 따른 **show ctiqbe** 명령의 샘플 출력입니다. 디바이스 전체에 활성 CTIQBE 세션이 하나만 설정되어 있습니다. 이 세션은 로컬 주소 10.0.0.99의 내부 CTI 디바이스(예: Cisco IP SoftPhone)와 172.29.1.77의 외부 Cisco Call Manager(여기서는 TCP 포트 2748이 Cisco CallManager) 간에 설정되어 있습니다. 세션에 대한 하트비트 간격은 120초입니다.

```
> show ctiqbe

Total: 1
        LOCAL            FOREIGN          STATE   HEARTBEAT
-----------------------------------------------------------------
1       10.0.0.99/1117  172.29.1.77/2748        1       120
        ------------------------------------------
        RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
        ------------------------------------------
        MEDIA: Device ID 27     Call ID 0
               Foreign 172.29.1.99      (1028 - 1029)
               Local   172.29.1.88      (26822 - 26823)
        ------------------------------------------
```

CTI 디바이스는 CallManager에 이미 등록되었습니다. 디바이스 내부 주소와 RTP 수신 대기 포트는 172.29.1.99 UDP 포트 1028로 PAT 처리됩니다. 해당 RTCP 수신 대기 포트는 UDP 1029로 PAT 처리됩니다.

"RTP/RTCP: PAT xlates:"로 시작하는 줄은 내부 CTI 디바이스가 외부 CallManager에 등록되고 CTI 디바이스 주소 및 포트가 해당 외부 인터페이스로 PAT 처리되는 경우에만 표시됩니다. CallManager가 내부 인터페이스에 있거나, 내부 CTI 디바이스 주소 및 포트가 CallManager에서 사용하는 것과 동일한 외부 인터페이스로 NAT 변환된 경우에는 표시되지 않습니다.

출력은 이 CTI 디바이스와 172.29.1.88의 다른 디바이스 간에 통화가 설정되었음을 나타냅니다. 다른 전화의 RTP 및 RTCP 수신 대기 포트는 UDP 26822 및 26823입니다. Firepower Threat Defense 디바이스는 두 번째 전화 및 CallManager와 연계된 CTIQBE 세션 레코드를 유지하지 않기 때문에 다른 전화

는 CallManager와 동일한 인터페이스에 있습니다. CTI 디바이스 쪽의 활성 통화 레그는 디바이스 ID 27 및 통화 ID 0으로 식별될 수 있습니다.

명령	설명
inspect ctiqbe	CTIQBE 애플리케이션 검사를 사용합니다.
show service-policy	서비스 정책 정보 및 통계를 표시합니다.
show conn	서로 다른 연결 유형의 연결 상태를 표시합니다.

show curpriv

진단 CLI 세션에 대한 현재 사용자 권한을 표시하려면 **show curpriv** 명령을 사용합니다.

show curpriv

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show curpriv 명령은 현재 권한 수준을 표시합니다. 더 낮은 권한 수준 번호는 더 낮은 권한 수준을 나타냅니다.

이 정보는 **configure user** 명령을 사용하여 정의된 사용자에게 적용되지 않습니다. 대신, 이것은 **system support diagnostistic-cli** 세션 내부에 있는 사용자 권한입니다. 이 권한을 변경할 수 없습니다.

다음 예는 로그인한 사용자의 권한을 확인하는 방법을 보여줍니다. 이러한 권한은 진단 CLI에 적용되며 configure 명령을 사용하는 기능에는 적용되지 않습니다. enable_1 사용자의 권한을 구성할 수 없습니다. 이러한 권한은 **Basic** and **Config** 권한 모두에 대해 동일합니다.

```
> show curpriv
Username : enable_1
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
```

show d - show h

- show gc, 552 페이지
- show h225, 553 페이지
- show h245, 555 페이지
- show h323, 557 페이지
- show high-availability config, 558 페이지
- show https-access-list, 560 페이지

show database

시스템 데이터베이스에 대한 정보를 표시하려면 **show database** 명령을 사용합니다.

show database {**processes** | **slow-query-log**}

processes	현재 실행 중인 데이터베이스 쿼리에 대한 정보를 표시합니다.
slow-query-log	데이터베이스의 느린 쿼리 로그를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 데이터베이스 프로세스 정보를 표시하는 방법을 보여줍니다.

```
> show database processes
Database Processes:
        Id :  3
      User :  barnyard
      Host :  localhost
  Database :  sfsnort
   Command :  Sleep
      Time :  6
     State :  Null
      Info :  Null
--------------------------------------------------------------
(...Remaining output truncated...)
```

show ddns update

DDNS 업데이트 방식에 대한 정보를 표시하려면 **show ddns update interface** 명령을 사용합니다.

show ddns update {**interface** [*interface-name*] | **method** [*method-name*]}

interface [*interface-name*]	Firepower Threat Defense 인터페이스에 할당된 방법을 표시합니다. 해당 인터페이스에 대한 정보만 표시하려면 인터페이스 이름을 선택적으로 지정할 수 있습니다.
method [*method-name*]	DDNS 업데이트 방법에 대한 정보를 표시합니다. 해당 방법에 대한 정보만 표시하려면 방법의 이름을 선택적으로 입력할 수 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 내부 인터페이스에 할당된 DDNS 방법을 표시합니다.

```
> show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
>
```

다음 예에서는 ddns-2라는 DDNS 방법을 표시합니다.

```
> show ddns update method ddns-2
Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
>
```

명령	설명
show running-config ddns	실행 중인 컨피그레이션에 구성된 모든 DDNS 방법의 유형 및 간격을 표시합니다.

show debug

현재 디버깅 구성을 표시하려면 **show debug** 명령을 사용합니다.

show debug [*command* [*keywords*]]

command	(선택 사항) 현재 구성을 확인할 **debug** 명령을 지정합니다.
keywords	(선택 사항) 각 명령에 대해 명령의 뒤에 오는 키워드는 연계된 **debug** 명령에서 지원하는 키워드와 동일합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

각 명령에 대해 명령의 뒤에 오는 키워드는 연계된 **debug** 명령에서 지원하는 키워드와 동일합니다. 지원되는 구문에 대한 자세한 내용은 키워드 위치에서 ?를 입력합니다.

예를 들면 다음과 같습니다.

- **show debug ?**는 사용 가능한 명령을 나열합니다.
- **show debug tcp ?**는 TCP 디버깅에 사용 가능한 키워드를 나열합니다.

다음 예는 TCP 디버깅을 사용 설정한 후 디버깅 상태를 보여줍니다.

```
> debug tcp
debug tcp  enabled at level 1
> show debug tcp
debug tcp  enabled at level 1
debug tcp  enabled at level 1 (persistent)
```

명령	설명
debug	디버깅을 사용 설정합니다.

show dhcpd

DHCP 바인딩, 상태 및 통계 정보를 보려면 **show dhcpd** 명령을 사용합니다.

show dhcpd {**binding** [*IP_address*] | **state** | **statistics**}

바인딩	지정된 서버 IP 주소에 대한 바인딩 정보 및 연계된 클라이언트 하드웨어 주소와 임대 기간을 표시합니다.
IP_address	지정된 IP 주소에 대한 바인딩 정보를 표시합니다.
state	DHCP 서버의 상태(예: 현재 상황에서 활성화되어 있는지 여부 및 각 인터페이스에서 사용하는지 여부)를 표시합니다.
statistics	주소 풀, 바인딩, 만료된 바인딩, 잘못된 형식의 메시지, 보낸 메시지, 받은 메시지 등의 개수와 같은 통계 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show dhcpd binding 명령에 선택적 IP 주소를 포함하면 해당 IP 주소에 대한 바인딩만 표시됩니다.

다음은 **show dhcpd binding** 명령의 샘플 출력입니다.

```
> show dhcpd binding
IP Address Client-id         Lease Expiration  Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds     automatic
```

다음은 **show dhcpd state** 명령의 샘플 출력입니다. 이 예에서 외부 인터페이스는 DHCP 클라이언트인 반면 기타 많은 인터페이스는 DHCP 서버 역할을 합니다.

```
> show dhcpd state
Context  Configured as DHCP Server
Interface outside, Configured for DHCP CLIENT
Interface inside1_2, Configured for DHCP SERVER
Interface inside1_3, Configured for DHCP SERVER
Interface inside1_4, Configured for DHCP SERVER
Interface inside1_5, Configured for DHCP SERVER
```

```
Interface inside1_6, Configured for DHCP SERVER
Interface inside1_7, Configured for DHCP SERVER
Interface inside1_8, Not Configured for DHCP
Interface diagnostic, Not Configured for DHCP
Interface inside, Configured for DHCP SERVER
```

다음은 **show dhcpd statistics** 명령의 샘플 출력입니다.

```
> show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

명령	설명
clear dhcpd	DHCP 서버 바인딩 및 통계 카운터를 지웁니다.
show running-config dhcpd	현재 DHCP 서버 구성을 표시합니다.

show dhcprelay

DHCP 릴레이 에이전트 상태 및 통계 정보를 보려면 **show dhcprelay state** 명령을 사용합니다.

show dhcprelay {**state** | **statistics**}

state	각 인터페이스의 DHCP 릴레이 에이전트의 상태를 표시합니다.
statistics	DHCP 릴레이 통계를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show dhcprelay state** 명령의 샘플 출력입니다.

```
> show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

다음은 **show dhcprelay statistics** 명령의 샘플 출력을 보여줍니다.

```
> show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
```

```
DHCPACK                 3
DHCPNAK                 0
```

명령	설명
clear dhcprelay statistics	DHCP 릴레이 에이전트 통계 카운터를 지웁니다.
show dhcpd	DHCP 서버 통계 및 상태 정보를 표시합니다.

show diameter

각 Diameter 연결에 대한 상태 정보를 표시하려면 **show diameter** 명령을 사용합니다.

show diameter

릴리스	수정 사항
6.2	이 명령이 도입되었습니다.

사용 가이드라인

Diameter 연결 상태 정보를 표시하려면 Diameter 트래픽을 검사해야 합니다. Diameter 트래픽을 검사하려면 Firepower Management Center에서 FlexConfig를 구성해야 합니다.

다음은 **show diameter** 명령의 샘플 출력을 보여줍니다.

```
> show diameter
Total active diameter sessions: 5
Session 3638
       ==========
       ref_count: 1 val = .; 1096298391; 2461;
           Protocol : diameter Context id : 0
           From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

명령	설명
clear service-policy	서비스 정책 통계를 지웁니다.

show disk

Firepower Threat Defense 디바이스의 플래시 메모리 내용만 표시하려면 **show disk** 명령을 사용합니다.

show disk

show {**disk0:** | **disk1:**} [**filesys** | **all** | **controller**]

{**disk0:** | **disk1:**}	내부 플래시 메모리(disk0:) 또는 외부 플래시 메모리(disk1:)를 지정합니다. 숫자 없이 **show disk** 명령을 입력한 경우 파일 시스템에 대한 정보를 확인할 수 있습니다.
all	플래시 메모리의 내용과 파일 시스템 및 컨트롤러 정보를 표시합니다.
controller	플래시 컨트롤러 모델 번호를 표시합니다.
filesys	컴팩트 플래시 카드에 대한 정보를 표시합니다.

기본적으로 이 명령은 파일 시스템 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 파일 시스템에 대한 정보를 표시합니다.

```
> show disk
Filesystem        Size  Used Avail Use% Mounted on
tmpfs             3.9G  440K  3.9G   1% /run
tmpfs             3.9G  168K  3.9G   1% /var/volatile
none              3.8G  9.4M  3.8G   1% /dev
/dev/sdb1         7.4G  104M  7.3G   2% /mnt/disk0
/dev/mapper/root  3.7G  943M  2.6G  27% /ngfw
/dev/mapper/var    81G  4.0G   73G   6% /home
tmpfs             3.9G     0  3.9G   0% /dev/cgroups
```

다음은 **show disk0:** 명령의 샘플 출력입니다.

```
> show disk0:
--#--  --length--  -----date/time------  path
```

```
   48  107030784   Oct 05 2016 02:10:26  os.img
   49  33          Oct 11 2016 21:32:16  .boot_string
   50  150484      Oct 06 2016 15:36:02  install.log
   11  4096        Oct 06 2016 15:58:16  log
   13  1544        Oct 13 2016 18:59:06  log/asa-appagent.log
   16  4096        Oct 06 2016 15:59:07  crypto_archive
   51  4096        Oct 06 2016 15:59:12  coredumpinfo
   52  59          Oct 06 2016 15:59:12  coredumpinfo/coredump.cfg
   53  36          Oct 06 2016 16:04:47  enable_configure
   56  507281      Oct 20 2016 18:10:20  crashinfo-test_20161020_181021_UTC

7935832064 bytes total (7827599360 bytes free)
```

다음은 **show disk0: filesys** 명령의 샘플 출력입니다.

```
> show disk0: filesys

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:          245
   Number of Cylinders      1022
   Sectors per Cylinder       62
   Sector Size               512
   Total Sectors          15524180
```

다음은 **show disk0: controller** 명령의 샘플 출력입니다.

```
> show disk0: controller

Flash Model: ATA Micron_M500DC_MT
```

명령	설명
dir	디렉토리 내용을 표시합니다.

show disk-manager

시스템의 각 부분(silo, low watermark, high watermark 등)에 대한 자세한 디스크 사용량 정보를 표시하려면 **show disk-manager** 명령을 사용합니다.

show disk-manager

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 디스크 관리자 정보를 표시하는 예입니다.

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
Updates                             0 KB        5.850 GB    14.625 GB
Other Detection Engine              0 KB        2.925 GB    5.850 GB
Performance Statistics              33 KB       998.395 MB  11.700 GB
Other Events                        0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering       0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs        0 KB        3.900 GB    19.500 GB
Unified Low Priority Events         1.329 MB    4.875 GB    24.375 GB
RNA Events                          0 KB        3.900 GB    15.600 GB
File Capture                        0 KB        9.750 GB    19.500 GB
Unified High Priority Events        0 KB        14.625 GB   34.125 GB
IPS Events                          0 KB        11.700 GB   29.250 GB
```

show dns

관리 주소의 현재 DNS 서버 및 검색 도메인에 대한 정보를 표시하려면 **show dns system** 명령을 사용합니다.

show dns system

system	관리 인터페이스에 대해 구성된 DNS 서버 및 검색 도메인을 표시합니다.

system 키워드를 포함하지 않는 경우, 명령은 Firepower Threat Defense에서 지원되지 않는 기능에 사용됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 관리 주소의 DNS 컨피그레이션을 표시합니다.

```
> show dns system
search cisco.com
nameserver 72.163.47.11
```

명령	설명
show network	관리 인터페이스의 구성을 표시합니다.

show dns-hosts

DNS 캐시를 표시하려면 **show dns-hosts** 명령을 사용합니다. DNS 캐시에는 DNS 서버에서 동적으로 학습된 항목과 수동으로 입력한 이름 및 IP 주소가 포함됩니다.

show dns-hosts

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show dns-hosts** 명령의 샘플 출력입니다.

```
> show dns-hosts
Host                        Flags      Age Type   Address(es)
ns2.example.com             (temp, OK) 0    IP    10.102.255.44
ns1.example.com             (temp, OK) 0    IP    192.168.241.185
snowmass.example.com        (temp, OK) 0    IP    10.94.146.101
server.example.com          (temp, OK) 0    IP    10.94.146.80
```

다음 표는 각 필드에 대해 설명합니다.

표 ***21: show dns-hosts*** 필드

필드	설명
Host	호스트 이름을 표시합니다.
Flags	다음의 조합으로 항목 상태를 표시합니다. • temp - DNS 서버에서 가져온 항목이므로 임시 항목입니다. 디바이스에서는 비활성 시간이 72시간을 경과하면 이 항목을 제거합니다. • perm - name 명령을 통해 추가된 항목이므로 영구 항목입니다. • OK - 유효한 항목입니다. • ?? - 의심스러운 항목이므로 재활성화해야 합니다. • EX - 만료된 항목입니다.
Age	이 항목을 마지막으로 참조한 이후에 경과한 시간을 표시합니다.
Type	DNS 레코드 유형을 표시합니다. 이 값은 항상 IP입니다.

필드	설명
Address(es)	IP 주소입니다.

명령	설명
clear dns-hosts	DNS 캐시를 지웁니다.

show eigrp events

EIGRP 이벤트 로그를 표시하려면 **show eigrp events** 명령을 사용합니다.

show eigrp [*as-number*] **events** [{*start end*} | **type**]

as-number	(선택 사항) 이벤트 로그를 확인할 EIGRP 프로세스의 자동 시스템 번호를 지정합니다. Firepower Threat Defense 디바이스는 하나의 EIGRP 라우팅 프로세스만 지원하기 때문에 자동 시스템 번호를 지정할 필요가 없습니다.
end	(선택 사항) *start* 인덱스 번호로 시작하고 *end* 인덱스 번호로 끝나는 항목으로 출력을 제한합니다.
start	(선택 사항) 로그 항목 인덱스 번호를 지정하는 숫자입니다. 시작 번호를 지정하면 출력이 지정된 이벤트에서 시작하고 *end* 인수로 지정된 이벤트에서 끝납니다. 유효한 값은 1 ~ 500입니다.
type	(선택 사항) 기록할 이벤트를 표시합니다.

start 및 end를 지정하지 않으면 모든 로그 항목이 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

자용 가이드라인

show eigrp events 출력에는 최대 500개의 이벤트가 표시됩니다. 최대 이벤트 수에 도달하면 출력 맨 아래에 새 이벤트가 추가되고 출력 맨 위에서 이전 이벤트가 제거됩니다.

clear eigrp events 명령을 사용하여 EIGRP 이벤트 로그를 지울 수 있습니다.

show eigrp events type 명령은 EIGRP 이벤트 기록 상태를 표시합니다. 기본적으로 인접 변경, 인접 경고 및 DUAL FSM 메시지가 기록됩니다. DUAL FSM 이벤트 기록은 사용 해제할 수 없습니다.

다음은 **show eigrp events** 명령의 샘플 출력입니다.

```
> show eigrp events

Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

다음은 시작 및 중지 번호가 지정된 **show eigrp events** 명령의 샘플 출력입니다.

```
> show eigrp events 3 8

Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

다음은 EIGRP 이벤트 로그에 항목이 없는 경우 **show eigrp events** 명령의 샘플 출력입니다.

```
> show eigrp events

Event information for AS 100:  Event log is empty.
```

다음은 **show eigrp eventstype** 명령의 샘플 출력입니다.

```
> show eigrp events type

EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

명령	설명
clear eigrp events	EIGRP 이벤트 기록 버퍼를 지웁니다.

show eigrp interfaces

EIGRP 라우팅에 참여한 인터페이스를 표시하려면 **show eigrp interfaces** 명령을 사용합니다.

show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]

as-number	(선택 사항) 활성 인터페이스를 표시할 EIGRP 프로세스의 자동 시스템 번호를 지정합니다. Firepower Threat Defense 디바이스는 하나의 EIGRP 라우팅 프로세스만 지원하기 때문에 자동 시스템 번호를 지정할 필요가 없습니다.
detail	(선택 사항) 자세한 정보를 표시합니다.
if-name	(선택 사항) 인터페이스의 이름입니다. 인터페이스 이름을 지정하면 지정된 인터페이스에 대한 정보만 표시됩니다.

인터페이스 이름을 지정하지 않으면 모든 EIGRP 인터페이스에 대한 정보가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show eigrp interfaces 명령을 사용하여 EIGRP가 활성화된 인터페이스를 확인하고 해당 인터페이스와 관련된 EIGRP에 대한 정보를 파악할 수 있습니다.

인터페이스를 지정한 경우 해당 인터페이스만 표시됩니다. 그렇지 않으면 EIGRP가 실행 중인 모든 인터페이스가 표시됩니다.

자동 시스템을 지정한 경우 지정된 자동 시스템에 대한 라우팅 프로세스만 표시됩니다. 그렇지 않으면 모든 EIGRP 프로세스가 표시됩니다.

다음은 **show eigrp interfaces** 명령의 샘플 출력입니다.

```
> show eigrp interfaces
```

```
EIGRP-IPv4 interfaces for process 100

                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
Interface   Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
mgmt          0         0/0          0      11/434          0          0
outside       1         0/0        337       0/10           0          0
inside        1         0/0         10       1/63         103          0
```

다음 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 ***22: show eigrp interfaces*** 필드 설명

필드	설명
process	EIGRP 라우팅 프로세스에 대한 자동 시스템 번호입니다.
Peers	직접 연결된 피어 수입니다.
Xmit Queue Un/Reliable	Unreliable 및 Reliable 전송 대기열에 남아 있는 패킷 수입니다.
Mean SRTT	원활한 평균 왕복 시간 간격(초)입니다.
Pacing Time Un/Reliable	EIGRP 패킷을 인터페이스 외부로 전송해야 하는 경우(신뢰할 수 없는 패킷 및 신뢰할 수 있는 패킷)를 결정하는 데 사용되는 페이싱 시간(초)입니다.
Multicast Flow Timer	Firepower Threat Defense 디바이스에서 멀티캐스트 EIGRP 패킷을 전송할 최대 시간(초)입니다.
Pending Routes	전송 대기열에서 전송을 대기 중인 패킷의 경로 수입니다.

show eigrp neighbors

EIGRP 네이버 테이블을 표시하려면 **show eigrp neighbors** 명령을 사용합니다.

show eigrp [*as-number*] **neighbors** [**detail** | **static**] [*if-name*]

as-number	(선택 사항) 네이버 엔트리를 삭제하려는 EIGRP 프로세스의 자율 시스템 번호를 지정합니다. Firepower Threat Defense 디바이스는 하나의 EIGRP 라우팅 프로세스만 지원하기 때문에 자동 시스템 번호를 지정할 필요가 없습니다.
detail	(선택 사항) 자세한 네이버 정보를 표시합니다.
if-name	(선택 사항) 인터페이스의 이름입니다. 인터페이스 이름을 지정하면 해당 인터페이스를 통해 학습된 모든 네이버 테이블 항목이 표시됩니다.
static	(선택 사항) 고정으로 정의된 EIGRP 네이버를 표시합니다.

인터페이스 이름을 지정하지 않으면 모든 인터페이스를 통해 학습된 네이버가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

clear eigrp neighbors 명령을 사용하여 EIGRP 네이버 테이블에서 동적으로 학습된 네이버를 지울 수 있습니다. **static** 키워드를 사용하지 않는 한 고정 네이버는 출력에 포함되지 않습니다.

다음은 **show eigrp neighbors** 명령의 샘플 출력입니다.

```
> show eigrp neighbors

EIGRP-IPv4 Neighbors for process 100

Address                 Interface     Holdtime Uptime   Q      Seq  SRTT  RTO
                                      (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1     13       0:00:41  0      11   4     20
```

```
172.16.80.28            Ethernet0     14        0:02:01  0      10   12    24
172.16.80.31            Ethernet0     12        0:02:02  0      4    5     20
```

다음 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 ***23: show eigrp neighbors*** 필드 설명

필드	설명
process	EIGRP 라우팅 프로세스에 대한 자동 시스템 번호입니다.
Address	EIGRP 네이버의 IP 주소입니다.
Interface	Firepower Threat Defense 디바이스가 네이버에서 hello 패킷을 수신하는 인터페이스입니다.
Holdtime	Firepower Threat Defense 디바이스에서 작동 중지된 것으로 선언하기 전에 네이버를 수신 대기할 시간(초)입니다. 이 보류 시간은 hello 패킷을 통해 네이버에서 수신되며, 네이버에서 다른 hello 패킷이 수신될 때까지는 감소됩니다. 네이버에서 기본 보류 시간을 사용하는 경우 이 숫자는 15보다 작습니다. 피어가 기본이 아닌 보류 시간을 구성하는 경우에는 기본이 아닌 보류 시간이 표시됩니다. 이 값이 0에 도달한 경우 Firepower Threat Defense 디바이스는 해당 네이버를 연결할 수 없는 것으로 간주합니다.
Uptime	Firepower Threat Defense 디바이스가 이 네이버에서 처음 수신한 이후에 경과한 시간(시간:분:초)입니다.
Q Count	Firepower Threat Defense 디바이스가 전송 대기 중인 EIGRP 패킷(업데이트, 쿼리 및 응답) 수입니다.
Seq Num	네이버에서 마지막으로 수신된 업데이트, 쿼리 또는 응답 패킷의 시퀀스 번호입니다.
SRTT	평균 왕복 시간입니다. EIGRP 패킷을 이 네이버로 전송하고 Firepower Threat Defense 디바이스가 해당 패킷에 대한 확인 응답을 받는 데 소요되는 시간(밀리초)입니다.
RTO	재전송 시간 제한(밀리초)입니다. Firepower Threat Defense 디바이스가 재전송 대기열에서 네이버로 패킷을 다시 전송하기 전에 대기하는 시간입니다.

다음은 **show eigrp neighbors static** 명령의 샘플 출력입니다.

```
> show eigrp neighbors static

EIGRP-IPv4 neighbors for process 100
```

```
Static Address                  Interface
192.168.1.5                     management
```

다음 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 ***24: show ip eigrp neighbors static*** 필드 설명

필드	설명
process	EIGRP 라우팅 프로세스에 대한 자동 시스템 번호입니다.
Static Address	EIGRP 네이버의 IP 주소입니다.
Interface	Firepower Threat Defense 디바이스가 네이버에서 hello 패킷을 수신하는 인터페이스입니다.

다음은 **show eigrp neighbors detail** 명령의 샘플 출력입니다.

```
> show eigrp neighbors detail

EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832  5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0             11 00:04:07  768  4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0             13 1w0d        1  3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0             12 1w0d        1  3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

다음 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 ***25: show ip eigrp neighbors details*** 필드 설명

필드	설명
process	EIGRP 라우팅 프로세스에 대한 자동 시스템 번호입니다.
H	이 열에는 지정된 네이버와의 피어링 세션이 설정된 순서가 나열됩니다. 이 순서는 0에서 시작하는 순차적 번호 매기기로 지정됩니다.
Address	EIGRP 네이버의 IP 주소입니다.
Interface	Firepower Threat Defense 디바이스가 네이버에서 hello 패킷을 수신하는 인터페이스입니다.

필드	설명
Holdtime	Firepower Threat Defense 디바이스에서 작동 중지된 것으로 선언하기 전에 네이버를 수신 대기하는 시간(초)입니다. 이 보류 시간은 hello 패킷을 통해 네이버에서 수신되며, 네이버에서 다른 hello 패킷이 수신될 때까지는 감소됩니다. 네이버에서 기본 보류 시간을 사용하는 경우 이 숫자는 15보다 작습니다. 피어가 기본이 아닌 보류 시간을 구성하는 경우에는 기본이 아닌 보류 시간이 표시됩니다. 이 값이 0에 도달한 경우 Firepower Threat Defense 디바이스는 해당 네이버를 연결할 수 없는 것으로 간주합니다.
Uptime	Firepower Threat Defense 디바이스가 이 네이버에서 처음 수신한 이후에 경과한 시간(시간:분:초)입니다.
SRTT	평균 왕복 시간입니다. EIGRP 패킷을 이 네이버로 전송하고 Firepower Threat Defense 디바이스가 해당 패킷에 대한 확인 응답을 받는 데 소요되는 시간(밀리초)입니다.
RTO	재전송 시간 제한(밀리초)입니다. Firepower Threat Defense 디바이스가 재전송 대기열에서 네이버로 패킷을 다시 전송하기 전에 대기하는 시간입니다.
Q Count	Firepower Threat Defense 디바이스가 전송 대기 중인 EIGRP 패킷(업데이트, 쿼리 및 응답) 수입니다.
Seq Num	네이버에서 마지막으로 수신된 업데이트, 쿼리 또는 응답 패킷의 시퀀스 번호입니다.
Version	지정된 피어에서 실행 중인 소프트웨어 버전입니다.
Retrans	패킷이 재전송된 횟수입니다.
Retries	패킷 재전송을 시도한 횟수입니다.
Restart time	지정된 네이버가 재시작된 이후에 경과한 시간(시간:분:초)입니다.

show eigrp topology

EIGRP 토폴로지 테이블을 표시하려면 **show eigrp topology** 명령을 사용합니다.

show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

active	(선택 사항) EIGRP 토폴로지 테이블의 활성 항목만 표시합니다.
all-links	(선택 사항) 실행 가능한 successor가 아닌 경로를 포함하여 EIGRP 토폴로지 테이블의 모든 경로를 표시합니다.
as-number	(선택 사항) EIGRP 프로세스의 자율 시스템 번호를 지정합니다. Firepower Threat Defense 디바이스는 하나의 EIGRP 라우팅 프로세스만 지원하기 때문에 자동 시스템 번호를 지정할 필요가 없습니다.
ip-addr	(선택 사항) 표시할 토폴로지 테이블의 IP 주소를 정의합니다. 마스크와 함께 지정하면 항목에 대한 자세한 설명이 제공됩니다.
mask	(선택 사항) *ip-addr* 인수에 적용할 네트워크 마스크를 정의합니다.
pending	(선택 사항) EIGRP 토폴로지 테이블에서 네이버로부터의 업데이트를 대기 중이거나 네이버에 응답하기를 대기 중인 모든 항목을 표시합니다.
summary	(선택 사항) EIGRP 토폴로지 테이블에 대한 요약을 표시합니다.
zero-successors	(선택 사항) EIGRP 토폴로지 테이블에서 사용 가능한 경로를 표시합니다.

실행 가능한 successor 경로만 표시됩니다. 실행 가능한 successor가 아닌 경로를 포함하여 모든 경로를 표시하려면 **all-links** 키워드를 사용합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

clear eigrp topology 명령을 사용하여 토폴로지 테이블에서 동적 항목을 제거할 수 있습니다.

다음은 **show eigrp topology** 명령의 샘플 출력입니다.

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status

P 10.2.1.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.2.1.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
          via 10.16.80.28 (307200/281600), Ethernet0
```

아래 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 ***26: show eigrp topology*** 필드 정보

필드	설명
Codes	이 토폴로지 테이블 항목의 상태입니다. Passive와 Active는 이 대상에 대한 EIGRP 상태를 나타내고, Update, Query 및 Reply는 전송할 패킷의 유형을 나타냅니다.
P - Passive	경로가 정상으로 알려져 있으므로 이 대상에 대한 EIGRP 계산은 수행되지 않습니다.
A - Active	이 대상에 대한 EIGRP 계산이 수행됩니다.
U - Update	이 대상으로 업데이트 패킷이 전송되었음을 나타냅니다.
Q - Query	이 대상으로 쿼리 패킷이 전송되었음을 나타냅니다.
R - Reply	이 대상으로 응답 패킷이 전송되었음을 나타냅니다.
r - Reply status	소프트웨어가 쿼리를 전송하고 응답을 대기 중인 후에 설정되는 플래그입니다.
address mask	대상 IP 주소와 마스크입니다.
successors	successor 수입니다. 이 수는 IP 라우팅 테이블에 있는 다음 홉 수에 해당합니다. "successor"가 대문자로 표시된 경우에는 경로 또는 다음 홉이 전환 상태에 있습니다.

필드	설명
FD	실행 가능한 거리입니다. 실행 가능한 거리는 대상에 도달할 수 있는 최상의 메트릭 또는 경로가 활성 상태가 된 경우에 알려진 최상의 메트릭입니다. 이 값은 실행 가능성 조건 확인에 사용됩니다. 라우터의 보고된 거리(뒤에 슬래시가 있는 메트릭)가 실행 가능한 거리보다 짧은 경우 실행 가능성 조건이 충족되고 해당 경로가 실행 가능한 successor가 됩니다. 소프트웨어에서 실행 가능한 successor가 있는 것으로 확인한 후에는 해당 대상에 대한 쿼리를 보내도록 요구하지 않습니다.
via	소프트웨어에 이 대상에 대해 알려 준 피어의 IP 주소입니다. 이러한 항목의 첫 번째 n은 현재 successor입니다(여기서 n은 successor 수). 목록의 나머지 항목은 실행 가능한 successor입니다.
(cost/adv_cost)	첫 번째 숫자는 대상에 대한 비용을 나타내는 EIGRP 메트릭입니다. 두 번째 숫자는 이 피어에서 알려 준 EIGRP 메트릭입니다.
interface	정보가 학습된 인터페이스입니다.

다음은 IP 주소와 함께 사용된 **show eigrp topology** 명령의 샘플 출력입니다. 표시된 출력은 내부 경로에 대한 것입니다.

```
> show eigrp topology 10.2.1.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
    Routing Descriptor Blocks:
        0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
            Composite metric is (281600/0), Route is Internal
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 1000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 0
```

다음은 IP 주소와 함께 사용된 **show eigrp topology** 명령의 샘플 출력입니다. 표시된 출력은 외부 경로에 대한 것입니다.

```
> show eigrp topology 10.4.80.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0

    State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
    Routing Descriptor Blocks:
        10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
            Composite metric is (409600/128256), Route is External
            Vector metric:
                Minimum bandwidth is 10000 Kbit
                Total delay is 6000 microseconds
                Reliability is 255/255
                Load is 1/255
                Minimum MTU is 1500
                Hop count is 1
```

```
External data:
    Originating router is 10.89.245.1
    AS number of route is 0
    External protocol is Connected, external metric is 0
    Administrator tag is 0 (0x00000000)
```

명령	설명
clear eigrp topology	EIGRP 토폴로지 테이블에서 동적으로 검색된 항목을 지웁니다.

show eigrp traffic

전송 및 수신된 EIGRP 패킷 수를 표시하려면 **show eigrp traffic** 명령을 사용합니다.

show eigrp [*as-number*] **traffic**

as-number	(선택 사항) 이벤트 로그를 확인할 EIGRP 프로세스의 자동 시스템 번호를 지정합니다. Firepower Threat Defense 디바이스는 하나의 EIGRP 라우팅 프로세스만 지원하기 때문에 자동 시스템 번호를 지정할 필요가 없습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

clear eigrp traffic 명령을 사용하여 EIGRP 트래픽 통계를 지울 수 있습니다.

다음은 **show eigrp traffic** 명령의 샘플 출력입니다.

```
> show eigrp traffic
EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

다음 표에는 화면에 표시되는 유효 필드에 대한 설명이 나와 있습니다.

표 ***27: show eigrp traffic*** 필드 설명

필드	설명
process	EIGRP 라우팅 프로세스에 대한 자동 시스템 번호입니다.
Hellos sent/received	전송 및 수신된 hello 패킷 수입니다.

필드	설명
Updates sent/received	전송 및 수신된 업데이트 패킷 수입니다.
Queries sent/received	전송 및 수신된 쿼리 패킷 수입니다.
Replies sent/received	전송 및 수신된 응답 패킷 수입니다.
Acks sent/received	전송 및 수신된 확인 응답 패킷 수입니다.
Input queue high water mark/drops	최대 수신 임계값에 근접한 수신된 패킷 수 및 삭제된 패킷 수입니다.
SIA-Queries sent/received	전송 및 수신된 SIA(Stuck-In-Active) 쿼리입니다.
SIA-Replies sent/received	전송 및 수신된 SIA(Stuck-In-Active) 응답입니다.

show environment

시스템 구성 요소에 대한 시스템 환경 정보를 표시하려면 **show environment** 명령을 사용합니다.

show environment [**driver** | **fans** | **power-supplies** | **power_consumption** | **voltage** | **temperature** [**accelerator** | **chassis** | **cpu** | **io-hub** | **mother-board** | **power-supply**]]

driver	(선택 사항) 환경 모니터링 IPMI 드라이버 상태를 표시합니다. 드라이버 상태는 다음 중 하나일 수 있습니다. • RUNNING - 드라이버가 작동 중입니다. • STOPPED - 오류가 발생하여 드라이버가 중지되었습니다.
fans	(선택 사항) 냉각 팬의 작동 상태를 표시합니다. 상태는 다음 중 하나입니다. • OK - 팬이 정상적으로 작동하고 있습니다. • Failed - 장애가 발생하여 팬을 교체해야 합니다.
power-supplies	(선택 사항) 전원 공급 디바이스의 작동 상태를 표시합니다. 각 전원 공급 디바이스의 상태는 다음 중 하나입니다. • OK - 전원 공급 디바이스가 정상적으로 작동하고 있습니다. • Failed - 장애가 발생하여 전원 공급 디바이스를 교체해야 합니다. • Not Present - 지정된 전원 공급 디바이스가 설치되어 있지 않습니다. 전원 공급 디바이스 이중화 상태도 표시됩니다. 이중화 상태는 다음 중 하나입니다. • OK - 디바이스가 완전한 리소스로 정상적으로 작동하고 있습니다. • Lost - 디바이스에서 이중화가 손실되었지만 최소 리소스로 정상적으로 작동하고 있습니다. 추가 장애 시 시스템이 종료됩니다. • N/A - 디바이스에 전원 공급 디바이스 이중화가 구성되어 있지 않습니다.
power_consumption	(선택 사항) 전력 소비량 값을 표시합니다.
voltage	(선택 사항) CPU 전압 채널 값(1~24)을 표시합니다. 작동 상태를 제외합니다.

temperature	(선택 사항) 프로세서 및 섀시의 온도 및 상태를 표시합니다. 온도는 섭씨로 제공됩니다. 특정 영역으로 출력을 제한하기 위해 키워드를 포함할 수 있습니다. 상태는 다음 중 하나입니다. • OK - 온도가 정상 작동 범위 내에 속합니다. • Critical - 온도가 정상 작동 범위를 벗어났습니다. 작동 범위는 다음과 같이 분류됩니다. • 70도 미만 - OK • 70~80 - Warm • 80~90 - Critical • 90 초과 - Unrecoverable
accelerator	(선택 사항) 가속기 온도 상태를 표시합니다.
chassis	(선택 사항) 온도 표시를 섀시로 제한합니다.
cpu	(선택 사항) 온도 표시를 프로세서로 제한합니다.
io-hub	(선택 사항) IOH 온도 상태를 표시합니다.
motherboard	(선택 사항) 마더보드 온도 상태를 표시합니다.
power-supply	(선택 사항) 전원 공급 장치 온도 상태를 표시합니다.

키워드를 지정하지 않으면 드라이버를 제외하고 모든 작동 정보가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show environment** 명령의 일반적인 샘플 출력입니다.

```
> show environment
Cooling Fans:
-------------------------------------
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan) Power Supplies:
```

```
-----------------------------------
   Power Supply Unit Redundancy: OK
   Temperature:
   -------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
   Cooling Fans:
   -------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan)
Temperature:
-----------------------------------
   Processors:
   -------------------------------
   Processor 1: 44.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 45.0 C - OK  (CPU2 Core Temperature)
   Chassis:
   -------------------------------
   Ambient 1: 28.0 C - OK  (Chassis Front Temperature)
   Ambient 2: 40.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 28.0 C - OK  (CPU1 Front Temperature)
   Ambient 4: 36.50 C - OK  (CPU1 Back Temperature)
   Ambient 5: 34.50 C - OK  (CPU2 Front Temperature)
   Ambient 6: 43.25 C - OK  (CPU2 Back Temperature)
   Power Supplies:
   -------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
```

다음은 **show environment driver** 명령의 샘플 출력입니다.

```
> show environment driver
Cooling Fans:
-----------------------------------
   Chassis Fans:
   -------------------------------
   Cooling Fan 1: 5888 RPM - OK
   Cooling Fan 2: 5632 RPM - OK
   Cooling Fan 3: 5888 RPM - OK
   Power Supplies:
   -------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK
Power Supplies:
-----------------------------------
   Left Slot (PS0): Not Present
   Right Slot (PS1): Present
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK
Temperature:
-----------------------------------
   Processors:
   -------------------------------
   Processor 1: 70.0 C - OK
   Chassis:
   -------------------------------
   Ambient 1: 36.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 31.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 39.0 C - OK  (Chassis Back Left Temperature)
   Power Supplies:
   -------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK
Voltage:
-----------------------------------
   Channel 1:  1.168 V -  (CPU Core 0.46V-1.4V)
   Channel 2: 11.954 V -  (12V)
   Channel 3:  4.998 V -  (5V)
   Channel 4:  3.296 V -  (3.3V)
```

```
Channel 5:  1.496 V -  (DDR3 1.5V)
Channel 6:  1.048 V -  (PCH 1.5V)
```

명령	설명
show version	하드웨어 및 소프트웨어 버전을 표시합니다.

show failover

유닛의 페일오버 상태에 대한 정보를 표시하려면 **show failover** 명령을 사용합니다.

show failover [**group** *num* | **history** | **interface** | **state**| **statistics**]

group*num*	지정된 페일오버 그룹의 실행 상태를 표시합니다.
history	페일오버 기록을 표시합니다. 페일오버 기록에는 이전 페일오버 상태 변경 및 해당 사유가 표시됩니다. 기록 정보는 디바이스를 재부팅하면 지워집니다.
interface	페일오버 및 상태 저장 링크 정보를 표시합니다.
state	페일오버 유닛 모두의 페일오버 상태를 표시합니다. 표시 정보는 유닛의 1차 또는 2차 상태, 유닛의 액티브/스탠바이 상태 및 페일오버를 위해 마지막으로 보고된 이유를 포함합니다. 실패 사유는 장애 사유가 지워진 경우에도 출력에 그대로 유지됩니다.
statistics	페일오버 명령 인터페이스의 전송 및 수신 패킷 수를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show failover 명령은 동적 페일오버 정보, 인터페이스 상태 및 스테이트풀 페일오버 통계를 표시합니다.

인터페이스에 IPv4 주소와 IPv6 주소가 둘 다 구성된 경우 두 주소 모두 출력에 표시됩니다. 인터페이스에 둘 이상의 IPv6 주소가 구성되어 있을 수 있으므로 링크-로컬 주소만 표시됩니다. 인터페이스에 구성된 IPv4 주소가 없는 경우 IPv4 주소는 출력에 0.0.0.0으로 표시됩니다. 인터페이스에 구성된 IPv6 주소가 없는 경우 이 주소는 출력에서 생략됩니다.

Stateful Failover Logical Update Statistics 출력은 스테이트풀 페일오버가 활성화된 경우에만 표시됩니다. “xerr” 및 “rerr” 값은 페일오버 오류를 나타내는 것이 아니라 패킷 전송 또는 수신 오류 수를 나타냅니다.

show failover 명령 출력에서 스테이트풀 페일오버 필드의 값은 다음과 같습니다.

- 스테이트풀 개체 값은 다음과 같습니다.
  - xmit - 전송된 패킷 수를 나타냅니다.
  - xerr - 전송 오류 수를 나타냅니다.
  - rcv - 수신된 패킷 수를 나타냅니다.
  - rerr - 수신 오류 수를 나타냅니다.
- 각 행은 다음과 같은 특정 개체 정적 개수에 대한 행입니다.
  - General - 모든 스테이트풀 개체의 합계를 나타냅니다.
  - sys cmd - **login** 또는 **stay alive**와 같은 논리적 업데이트 시스템 명령을 참조합니다.
  - up time - Firepower Threat Defense 디바이스가 작동 중인 시간을 표시하며 액티브 Firepower Threat Defense 디바이스가 이를 스탠바이 Firepower Threat Defense 디바이스로 전달합니다.
  - RPC services - 원격 프로시저 호출 연결 정보입니다.
  - TCP conn - 동적 TCP 연결 정보입니다.
  - UDP conn - 동적 UDP 연결 정보입니다.
  - ARP tbl - 동적 ARP 테이블 정보입니다.
  - Xlate_Timeout - 연결 변환 시간 제한 정보를 나타냅니다.
  - IPv6 ND tbl - IPv6 네이버 검색 테이블 정보입니다.
  - VPN IKE upd - IKE 연결 정보입니다.
  - VPN IPSEC upd - IPsec 연결 정보입니다.
  - VPN CTCP upd - cTCP 터널 연결 정보입니다.
  - VPN SDI upd - SDI AAA 연결 정보입니다.
  - VPN DHCP upd - 터널링된 DHCP 연결 정보입니다.
  - SIP Session - SIP 신호 처리 세션 정보입니다.
  - Route Session - 경로 동기화 업데이트에 대한 LU 통계입니다.

페일오버 IP 주소를 입력하지 않은 경우 **show failover** 명령은 IP 주소를 0.0.0.0으로 표시하며, 인터페이스 모니터링이 “waiting” 상태로 유지됩니다. 페일오버가 작동하려면 페일오버 IP 주소를 설정해야 합니다.

다음 표는 페일오버에 대한 인터페이스 상태를 설명합니다.

표 ***28:*** 페일오버 인터페이스 상태

상태	설명
Normal	인터페이스가 작동하며, 피어 디바이스의 해당 인터페이스에서 hello 패킷을 받고 있습니다.
Normal (Waiting)	인터페이스가 작동하지만 피어 디바이스의 해당 인터페이스에서 hello 패킷을 아직 받지 못했습니다. 인터페이스에 대해 대기 IP 주소가 구성되어 있는지, 그리고 두 인터페이스가 연결되어 있는지 확인하십시오.
Normal (Not-Monitored)	인터페이스가 작동하지만 페일오버 프로세스에서 모니터링되지 않습니다. 모니터링되지 않는 인터페이스 장애는 페일오버를 트리거하지 않습니다.
No Link	물리적 링크의 작동이 중지되었습니다.
No Link (Waiting)	물리적 링크의 작동이 중지되고 인터페이스가 피어 디바이스의 해당 인터페이스에서 hello 패킷을 아직 받지 못했습니다. 링크를 복원한 후 인터페이스에 대해 대기 IP 주소가 구성되고 두 인터페이스가 서로 연결되어 있는지 확인하십시오.
No Link (Not-Monitored)	물리적 링크의 작동이 중지되었지만 페일오버 프로세스에서 모니터링되지 않습니다. 모니터링되지 않는 인터페이스 장애는 페일오버를 트리거하지 않습니다.
Link Down	물리적 링크가 작동하지만 관리자에 의해 인터페이스의 작동이 중지되었습니다.
Link Down (Waiting)	물리적 링크가 작동하지만 관리자에 의해 인터페이스의 작동이 중지되고 인터페이스가 피어 디바이스의 해당 인터페이스에서 hello 패킷을 아직 받지 못했습니다. 인터페이스를 다시 작동시킨 후 인터페이스에 대해 스탠바이 IP 주소가 구성되고 두 인터페이스가 서로 연결되어 있는지 확인하십시오.
Link Down (Not-Monitored)	물리적 링크가 작동하지만 관리자에 의해 인터페이스의 작동이 중지되고 페일오버 프로세스에서 모니터링되지 않습니다. 모니터링되지 않는 인터페이스 장애는 페일오버를 트리거하지 않습니다.
Testing	피어 디바이스의 해당 인터페이스에서 hello 패킷이 누락되어 인터페이스가 테스트 모드에 있습니다.
Failed	인터페이스 테스트에 실패했으며 인터페이스가 장애가 발생한 것으로 표시되어 있습니다. 인터페이스 장애로 인해 페일오버 조건이 충족되는 경우 보조 디바이스 또는 페일오버 그룹으로 페일오버됩니다.

다음은 액티브/스탠바이 페일오버에 대한 **show failover** 명령의 샘플 출력입니다.

```
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Failover On
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
    This host: Primary - Active
        Active time: 589 (sec)
        slot 0: empty
          Interface diagnostic (0.0.0.0): Normal (Waiting)
          Interface outside (192.168.77.1): Normal (Waiting)
          Interface inside (192.168.87.1): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
    Other host: Secondary - Standby Ready
        Active time: 0 (sec)
          Interface diagnostic (0.0.0.0): Normal (Waiting)
          Interface outside (0.0.0.0): Normal (Waiting)
          Interface inside (0.0.0.0): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
Stateful Failover Logical Update Statistics
    Link : failover GigabitEthernet0/2 (up)
    Stateful Obj       xmit       xerr       rcv        rerr
    General            45         0          44         0
    sys cmd            44         0          44         0
    up time            0          0          0          0
    RPC services       0          0          0          0
    TCP conn           0          0          0          0
    UDP conn           0          0          0          0
    ARP tbl            0          0          0          0
    Xlate_Timeout      0          0          0          0
    IPv6 ND tbl        0          0          0          0
    VPN IKEv1 SA       0          0          0          0
    VPN IKEv1 P2       0          0          0          0
    VPN IKEv2 SA       0          0          0          0
    VPN IKEv2 P2       0          0          0          0
    VPN CTCP upd       0          0          0          0
    VPN SDI upd        0          0          0          0
    VPN DHCP upd       0          0          0          0
    SIP Session        0          0          0          0
    SIP Tx             0          0          0          0
    SIP Pinhole        0          0          0          0
    Route Session      0          0          0          0
    Router ID          0          0          0          0
    User-Identity      1          0          0          0
    CTS SGTNAME        0          0          0          0
    CTS PAC            0          0          0          0
    TrustSec-SXP       0          0          0          0
    IPv6 Route         0          0          0          0
    STS Table          0          0          0          0

    Logical Update Queue Information
                Cur   Max  Total
    Recv Q:     0     10    44
    Xmit Q:     0     11    238
```

다음은 액티브-스탠바이 설정에 대한 **show failover state** 명령의 샘플 출력입니다.

```
> show failover state

               State          Last Failure Reason      Date/Time
This host  -   Primary
               Negotiation    Backplane Failure        15:44:56 UTC Jun 20 2009
Other host -   Secondary
               Not Detected   Comm Failure             15:36:30 UTC Jun 20 2009

====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

다음 표에는 **show failover state** 명령의 출력에 대한 설명이 나와 있습니다.

표 ***29: show failover state*** 출력 설명

필드	설명
Configuration State	컨피그레이션 동기화의 상태를 표시합니다. 스탠바이 유닛의 가능한 컨피그레이션 상태는 다음과 같습니다. • **Config Syncing - STANDBY** - 동기화된 컨피그레이션이 실행되는 동안 설정됩니다. • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY** - 스탠바이 유닛이 액티브 유닛으로부터의 컨피그레이션 동기화를 완료한 경우에 설정됩니다. 액티브 유닛의 가능한 컨피그레이션 상태는 다음과 같습니다. • **Config Syncing** - 액티브 유닛이 스탠바이 유닛으로 컨피그레이션 동기화를 수행할 때 액티브 유닛에 설정됩니다. • **Interface Config Syncing** • **Sync Done** - 액티브 유닛이 스탠바이 유닛으로의 성공적인 컨피그레이션 동기화를 완료한 경우에 설정됩니다. • **Ready for Config Sync** - 스탠바이 유닛에서 컨피그레이션 동기화를 수신할 준비가 완료되었다는 신호를 보낸 경우 액티브 유닛에 설정됩니다.
Communication State	MAC 주소 동기화의 상태를 표시합니다. • **Mac set** - MAC 주소가 피어 유닛에서 이 유닛으로 동기화되었습니다. • **Updated Mac** - MAC 주소가 업데이트되어 다른 유닛으로 동기화해야 하는 경우에 사용됩니다. 또한 디바이스가 피어 디바이스에서 동기화된 로컬 MAC 주소를 업데이트하는 전환 기간 동안에도 사용됩니다.

필드	설명
날짜/시간	장애가 발생한 날짜 및 타임스탬프를 표시합니다.
Last Failure Reason	마지막으로 보고된 장애에 대한 사유를 표시합니다. 이 정보는 장애 조건이 삭제된 경우에도 지워지지 않습니다. 페일오버가 발생한 경우에만 변경됩니다. 가능한 실패 사유는 다음과 같습니다. • **Ifc Failure** - 장애가 발생한 인터페이스 수가 페일오버 조건을 충족하여 페일오버가 발생했습니다. • **Comm Failure** - 페일오버 링크가 실패하거나 피어의 작동이 중지되었습니다. • **Backplane Failure**
State	디바이스의 기본/보조 및 활성/대기 상태를 표시합니다.
This host/Other host	This host는 명령이 실행된 디바이스에 대한 정보를 나타냅니다. Other host는 페일오버 쌍의 다른 디바이스에 대한 정보를 나타냅니다.

다음은 **show failover history** 명령의 샘플 출력입니다.

```
> show failover history
==========================================================================
Group     From State                To State                  Reason
==========================================================================
. . .
03:42:29 UTC Apr 17 2009
    0     Sync Config               Failed
Backplane failed
03:42:29 UTC Apr 17 2009
    1     Standby Ready             Failed
Backplane failed
03:42:29 UTC Apr 17 2009
    2     Standby Ready             Failed
Backplane failed
03:44:39 UTC Apr 17 2009
    0     Failed                    Negotiation
Backplane operational
03:44:40 UTC Apr 17 2009
    1     Failed                    Negotiation
Backplane operational
03:44:40 UTC Apr 17 2009
    2     Failed                    Negotiation
Backplane operational
==========================================================================
```

각 항목은 상태 변경이 발생한 시간 및 날짜, 시작 상태, 결과 상태 및 상태 변경 사유를 제공합니다. 최신 항목은 화면의 맨 아래에 있습니다. 이전 항목은 맨 위에 표시됩니다. 최대 60개의 항목이 표시될 수 있습니다. 최대 항목 수에 도달한 후에는 새 항목이 맨 아래에 추가되면서 가장 오래된 항목이 출력의 맨 위에서 제거됩니다.

다음 표는 페일오버 상태를 보여줍니다. 안정적인 상태와 일시적인 상태의 두 가지 상태가 있습니다. 안정적인 상태는 장애와 같은 상황이 발생하여 상태가 변경될 때까지 디바이스가 그대로 유지될 수 있음을 나타냅니다. 일시적인 상태는 디바이스가 안정적인 상태에 도달하는 동안 거치는 상태입니다.

표 ***30:*** 페일오버 상태

상태	설명
Disabled(비활성화)	대체작동이 비활성화되어 있습니다. 이는 안정적인 상태입니다.
Failed(실패함)	디바이스가 실패한 상태입니다. 이는 안정적인 상태입니다.
Negotiation(협상)	디바이스가 피어와의 연결을 설정하고 소프트웨어 버전 호환성 및 활성/대기 역할을 확인하기 위해 피어와 협상합니다. 협상된 역할에 따라 디바이스가 스탠바이 유닛 상태 또는 액티브 유닛 상태로 전환되거나 실패한 상태가 됩니다. 이는 일시적인 상태입니다.
Not Detected(탐지되지 않음)	ASA가 피어의 상태를 감지할 수 없습니다. 이는 ASA가 페일오버가 활성화된 상태로 부팅되지만 피어가 존재하지 않거나 전원이 꺼진 경우에 발생할 수 있습니다.
스탠바이 유닛 상태	
Cold Standby	유닛에서 피어가 활성 상태에 도달하기를 기다리는 중입니다. 피어 유닛이 액티브 상태에 도달하면 이 유닛은 스탠바이 컨피그레이션 상태로 진행됩니다. 이는 일시적인 상태입니다.
Sync Config	유닛이 피어 디바이스에서 실행 중인 컨피그레이션을 요청합니다. 컨피그레이션 동기화 중 오류가 발생한 경우 유닛은 초기화 상태로 돌아갑니다. 이는 일시적인 상태입니다.
Sync File System	유닛이 피어 디바이스와 파일 시스템을 동기화합니다. 이는 일시적인 상태입니다.
Bulk Sync	유닛이 피어에서 상태 정보를 수신합니다. 이 상태는 스테이트풀 페일오버가 활성화된 경우에만 발생합니다. 이는 일시적인 상태입니다.
Standby Ready	유닛이 액티브 유닛에 장애가 발생하는 경우 액티브 유닛의 역할을 수행할 준비가 되어 있습니다. 이는 안정적인 상태입니다.
액티브 유닛 상태	
Just Active	액티브 유닛이 되면 시작되는 유닛의 첫 번째 상태입니다. 이 상태에 있는 동안에는 유닛이 활성화되고 인터페이스에 대해 IP 및 MAC 주소가 설정되었음을 알리는 메시지가 피어로 전송됩니다. 이는 일시적인 상태입니다.

상태	설명
Active Drain	피어의 대기열 메시지가 삭제됩니다. 이는 일시적인 상태입니다.
Active Applying Config	유닛이 시스템 컨피그레이션을 적용하는 중입니다. 이는 일시적인 상태입니다.
Active Config Applied	유닛이 시스템 컨피그레이션 적용을 완료했습니다. 이는 일시적인 상태입니다.
Active	유닛이 활성 상태이며 트래픽을 처리하는 중입니다. 이는 안정적인 상태입니다.

각 상태 변경에는 상태 변경 사유가 뒤따릅니다. 사유는 일반적으로 유닛이 일시적인 상태에서 안정적인 상태로 진행될 때 동일하게 유지됩니다. 가능한 상태 변경 사유는 다음과 같습니다.

- No Error
- Set by the CI config cmd
- Failover state check
- Failover interface become OK
- HELLO not heard from mate
- Other unit has different software version
- Other unit operating mode is different
- Other unit license is different
- Other unit chassis configuration is different
- Other unit card configuration is different
- Other unit want me Active
- Other unit want me Standby
- Other unit reports that I am failed
- Other unit reports that it is failed
- Configuration mismatch
- Detected an Active mate
- No Active unit found
- Configuration synchronization done
- Recovered from communication failure
- Other unit has different set of vlans configured
- Unable to verify vlan configuration

- Incomplete configuration synchronization
- Configuration synchronization failed
- Interface check
- My communication failed
- ACK not received for failover message
- Other unit got stuck in learn state after sync
- No power detected from peer
- No failover cable
- HA state progression failed
- Detect service card failure
- Service card in other unit has failed
- My service card is as good as peer
- LAN Interface become un-configured
- Peer unit just reloaded
- Switch from Serial Cable to LAN-Based fover
- Unable to verify state of config sync
- Auto-update request
- Unknown reason

다음은 **show failover interface** 명령의 샘플 출력입니다. 이 디바이스는 페일오버 인터페이스에 IPv6 주소가 구성되어 있습니다.

```
> show failover interface
        interface folink GigabitEthernet0/2
                System IP Address: 2001:a0a:b00::a0a:b70/64
                My IP Address    : 2001:a0a:b00::a0a:b70
                Other IP Address : 2001:a0a:b00::a0a:b71
```

명령	설명
show running-config failover	현재 컨피그레이션에서 **failover** 명령을 표시합니다.

show failover exec

지정된 유닛에 대한 **failover exec** 명령 모드를 표시하려면 **show failover exec** 명령을 사용합니다.

show failover exec {**active**| **standby** | **mate**}

active	액티브 유닛에 대한 **failover exec** 명령 모드를 표시합니다.
mate	피어 유닛에 대한 **failover exec** 명령 모드를 표시합니다.
standby	스탠바이 유닛에 대한 **failover exec** 명령 모드를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

failover exec 명령은 지정된 디바이스로 세션을 생성합니다. 기본값으로, Firepower Threat Defense가 CLI 구성을 지원하지 않는 경우에도 해당 세션은 전역 구성 모드입니다. 모드 정보는 Firepower Threat Defense와 관련이 없습니다.

show failover exec 명령은 **failover exec** 명령을 통해 전송된 명령이 실행되는 지정된 디바이스의 명령 모드를 표시합니다.

다음은 **show failover exec** 명령의 샘플 출력입니다.

```
> show failover exec mate
Standby unit Failover EXEC is at config mode
```

명령	설명
failover exec	제공된 명령을 대체작동 쌍의 지정된 디바이스에서 실행합니다.

show file

파일 시스템에 관한 정보를 표시하려면 **show file** 명령을 사용합니다.

show file [**descriptors** | **system** | **information** *filename*]

descriptors	열려 있는 모든 파일 설명자를 표시합니다.
information*filename*	파트너 애플리케이션 패키지 파일을 포함하여 특정 파일에 대한 정보를 표시합니다.
system	디스크 파일 시스템에 대한 크기, 사용 가능한 바이트 수, 미디어 유형, 플래그 및 접두사 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show file system** 명령의 샘플 출력입니다.

```
> show file system
File Systems:
     Size(b)     Free(b)      Type      Flags  Prefixes
* 7935832064    7828107264    disk      rw      disk0: flash:
             -             -  disk      rw      disk1:
             -             -  network   rw      tftp:
             -             -  opaque    rw      system:
             -             -  network   ro      http:
             -             -  network   ro      https:
             -             -  network   rw      scp:
             -             -  network   rw      ftp:
             -             -  network   wo      cluster:
             -             -  stub      ro      cluster_trace:
             -             -  network   rw      smb:
```

다음은 **show file information** 명령의 샘플 출력입니다.

```
> show file information install.log
disk0:/install.log:
```

```
type is ascii text
file size is 150484 bytes
```

명령	설명
dir	디렉토리 내용을 표시합니다.
pwd	현재의 작업 디렉토리를 표시합니다.

show firewall

현재 방화벽 모드(라우팅 또는 투명 모드)를 표시하려면 **show firewall** 명령을 사용합니다.

show firewall

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show firewall** 명령의 샘플 출력입니다.

```
> show firewall
Firewall mode: Router
```

명령	설명
configure firewall	방화벽 모드를 설정합니다.
show mode	현재의 컨텍스트 모드(single 또는 multiple)를 표시합니다.

show flash

내부 플래시 메모리의 내용을 표시하려면 **show flash:** 명령을 사용합니다.

show flash: [**all** | **controller** | **filesys**]

참고 Firepower Threat Defense에서는 **flash** 키워드 별칭이 **disk0**입니다.

all	모든 플래시 정보를 표시합니다.
controller	파일 시스템 컨트롤러 정보를 표시합니다.
filesys	파일 시스템 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show flash:** 명령의 샘플 출력입니다.

```
> show flash:
--#--  --length--  -----date/time------  path
   48  107030784   Oct 05 2016 02:10:26  os.img
   49  33          Oct 06 2016 16:15:24  .boot_string
   50  150484      Oct 06 2016 15:36:02  install.log
   11  4096        Oct 06 2016 15:58:16  log
   13  1065        Oct 06 2016 15:59:13  log/asa-appagent.log
   16  4096        Oct 06 2016 15:59:07  crypto_archive
   51  4096        Oct 06 2016 15:59:12  coredumpinfo
   52  59          Oct 06 2016 15:59:12  coredumpinfo/coredump.cfg
   53  36          Oct 06 2016 16:04:47  enable_configure

7935832064 bytes total (7828107264 bytes free)
```

명령	설명
dir	디렉토리 내용을 표시합니다.

명령	설명
show disk0:	내부 플래시 메모리의 내용을 표시합니다.
show disk1:	외부 플래시 메모리 카드의 내용을 표시합니다.

show fragment

IP 프래그먼트 리어셈블리 모듈의 운영 데이터를 표시하려면 **show fragment**를 입력합니다.

show fragment [*interface*]

interface	(선택 사항) Firepower Threat Defense 인터페이스를 지정합니다.

인터페이스가 지정되지 않을 경우 이 명령은 모든 인터페이스에 적용됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

이 예에서는 IP 프래그먼트 리어셈블리 모듈의 운영 데이터를 표시하는 방법을 보여 줍니다.

```
> show fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

명령	설명
clear configure fragment	IP 프래그먼트 리어셈블리 구성을 지우고 기본값을 재설정합니다.
clear fragment	IP 프래그먼트 리어셈블리 모듈의 운영 데이터를 지웁니다.

명령	설명
show running-config fragment	IP 프래그먼트 리어셈블리 구성을 표시합니다.

show gc

가비지 수집 프로세스 통계를 표시하려면 **show gc** 명령을 사용합니다.

show gc

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show gc** 명령의 샘플 출력입니다.

```
> show gc

Garbage collection process stats:
Total tcp conn delete response             :            0
Total udp conn delete response             :            0
Total number of zombie cleaned             :            0
Total number of embryonic conn cleaned     :            0
Total error response                       :            0
Total queries generated                    :            0
Total queries with conn present response   :            0
Total number of sweeps                     :          946
Total number of invalid vcid               :            0
Total number of zombie vcid                :            0
```

명령	설명
clear gc	가비지 수집 프로세스 통계를 제거합니다.

show h225

Firepower Threat Defense 디바이스를 통해 설정된 H.225 세션에 대한 정보를 표시하려면 **show h225** 명령을 사용합니다.

show h225

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show h225 명령은 디바이스를 통해 설정된 H.225 세션에 대한 정보를 표시합니다.

연결 수가 비정상적으로 많은 경우 설정한 기본 시간 제한 값에 따라 세션이 시간 초과되고 있는지 확인하십시오. 설정한 기본 시간 제한 값을 따르지 않는 경우 조사해야 하는 문제가 있는 것입니다.

다음은 **show h225** 명령의 샘플 출력입니다.

```
> show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
    1. CRV 9861
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
    Local:   10.130.56.4/1050   Foreign: 172.30.254.205/1720
```

이 출력은 현재 로컬 엔드포인트 10.130.56.3과 외부 호스트 172.30.254.203 간에 Firepower Threat Defense 디바이스를 통해 전달되는 활성 H.323 호출 하나가 있으며, 이러한 특정 엔드포인트 간에 현재 CRV(Call Reference Value)가 9861인 동시 호출 하나가 있음을 나타냅니다.

로컬 엔드포인트 10.130.56.4와 외부 호스트 172.30.254.205에는 동시 통화가 0개 있습니다. 이는 H.225 세션이 여전히 존재하는 경우에도 엔드포인트 간에 활성 호출이 없음을 의미합니다. 이는 **show h225** 명령이 실행될 당시에 호출이 이미 종료되었지만 H.225 세션이 아직 삭제되지 않은 경우에 발생할 수 있습니다. 또는 두 엔드포인트가 "maintainConnection"을 TRUE로 설정하여 이를 다시 FALSE로

설정하거나 구성된 H.225 시간 제한 값에 따라 세션 시간이 초과될 때까지 세션이 열린 상태로 유지되기 때문에 두 엔드포인트의 TCP 연결이 계속 열려 있음을 의미할 수도 있습니다.

명령	설명
show h245	느린 시작을 사용하여 엔드포인트에서 디바이스를 통해 설정한 H.245 세션에 대한 정보를 표시합니다.
show h323 ras	디바이스를 통해 설정된 H.323 RAS 세션에 대한 정보를 표시합니다.

show h245

느린 시작을 사용하여 엔드포인트에서 Firepower Threat Defense 디바이스를 통해 설정된 H.245 세션에 대한 정보를 표시하려면 **show h245** 명령을 사용합니다.

show h245

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show h245 명령은 느린 시작을 사용하여 엔드포인트에서 Firepower Threat Defense 디바이스를 통해 설정한 H.245 세션에 대한 정보를 표시합니다. 느린 시작은 호출의 두 엔드포인트가 H.245에 대한 다른 TCP 제어 채널을 여는 경우를 의미합니다. 빠른 시작은 H.225 제어 채널에서 H.245 메시지가 H.225 메시지의 일부로서 교환될 때 발생합니다.

다음은 **show h245** 명령의 샘플 출력입니다.

```
> show h245
Total: 1
        LOCAL            TPKT    FOREIGN          TPKT
1       10.130.56.3/1041         0       172.30.254.203/1245    0
        MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
                       Local   10.130.56.3 RTP 49608 RTCP 49609
        MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
                       Local   10.130.56.3 RTP 49606 RTCP 49607
```

현재 Firepower Threat Defense 디바이스를 통해 활성화된 H.245 제어 세션 하나가 있습니다. 로컬 엔드포인트는 10.130.56.3이며, TPKT 값이 0이므로 이 엔드포인트의 다음 패킷에 TPKT 헤더가 있어야 합니다. TKTP 헤더는 각 H.225/H.245 메시지 앞에 있는 4바이트 헤더입니다. 메시지의 길이에 4바이트의 헤더가 포함됩니다.) 외부 호스트 엔드포인트는 172.30.254.203이며, TPKT 값이 0이므로 이 엔드포인트의 다음 패킷에는 TPKT 헤더가 있을 것으로 예상됩니다.

이러한 엔드포인트 간에 협상된 미디어의 LCN(Logical Channel Number)은 258이며, 외부 RTP IP 주소/포트 쌍은 172.30.254.203/49608, RTCP IP 주소/포트는 172.30.254.203/49609, 로컬 RTP IP 주소/포트 쌍은 10.130.56.3/49608, RTCP 포트는 49609입니다.

두 번째 LCN 259의 외부 RTP IP 주소/포트 쌍은 172.30.254.203/49606, RTCP IP 주소/포트 쌍은 172.30.254.203/49607, 로컬 RTP IP 주소/포트 쌍은 10.130.56.3/49606, RTCP 포트는 49607입니다.

명령	설명
show h245	느린 시작을 사용하여 엔드포인트에서 Firepower Threat Defense 디바이스를 통해 설정한 H.245 세션에 대한 정보를 표시합니다.
show h323 ras	Firepower Threat Defense 디바이스를 통해 설정된 H.323 RAS 세션에 대한 정보를 표시합니다.

show h323

H.323 연결에 대한 정보를 표시하려면 **show h323** 명령을 사용합니다.

show h323 {**ras** | **gup**}

ras	게이트키퍼와 해당 H.323 엔드포인트 간에 Firepower Threat Defense 디바이스를 통해 설정된 H323 RAS 세션을 표시합니다.
gup	H323 게이트웨이 업데이트 프로토콜 연결에 대한 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show h323 ras 명령은 게이트키퍼와 해당 H.323 엔드포인트 간에 Firepower Threat Defense 디바이스를 통해 설정된 H.323 RAS 세션을 표시합니다.

다음은 **show h323 ras** 명령의 샘플 출력입니다.

```
> show h323 ras

Total: 1
        GK                      Caller
        172.30.254.214          10.130.56.14
```

이 출력은 게이트키퍼 172.30.254.214와 해당 클라이언트 10.130.56.14 간에 하나의 활성 등록이 있음을 보여 줍니다.

명령	설명
show h245	느린 시작을 사용하여 엔드포인트에서 Firepower Threat Defense 디바이스를 통해 설정한 H.245 세션에 대한 정보를 표시합니다.

show high-availability config

고가용성(페일오버) 구성에 관한 정보를 보려면 **show high-availability config** 명령을 사용합니다.

show high-availability config

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

자용 가이드라인

show high-availability config 명령은 **show failover** 명령의 별칭입니다. 자세한 내용은 **show failover** 참조 페이지를 참고하십시오.

다음 예에서는 액티브/스탠바이 페일오버 모드의 디바이스에 대한 페일오버 구성을 보여줍니다.

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/2 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 61 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.7(0)74, Mate 9.7(0)74
Serial Number: Ours 9A41CKDXQJU, Mate 9A3MFP0H1CP
Last Failover at: 19:23:17 UTC Oct 26 2016
        This host: Primary - Active
                Active time: 2009 (sec)
                slot 0: empty
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface outside (192.168.77.1): Normal (Waiting)
                  Interface inside (192.168.87.1): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                  Interface diagnostic (0.0.0.0): Normal (Waiting)
                  Interface outside (0.0.0.0): Normal (Waiting)
                  Interface inside (0.0.0.0): Normal (Waiting)
                slot 1: snort rev (1.0)  status (up)
                slot 2: diskstatus rev (1.0)  status (up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         235        0          234        0
        sys cmd         234        0          234        0
        up time         0          0          0          0
```

```
RPC services    0           0           0           0
TCP conn        0           0           0           0
UDP conn        0           0           0           0
ARP tbl         0           0           0           0
Xlate_Timeout   0           0           0           0
IPv6 ND tbl     0           0           0           0
VPN IKEv1 SA    0           0           0           0
VPN IKEv1 P2    0           0           0           0
VPN IKEv2 SA    0           0           0           0
VPN IKEv2 P2    0           0           0           0
VPN CTCP upd    0           0           0           0
VPN SDI upd     0           0           0           0
VPN DHCP upd    0           0           0           0
SIP Session     0           0           0           0
SIP Tx          0           0           0           0
SIP Pinhole     0           0           0           0
Route Session   0           0           0           0
Router ID       0           0           0           0
User-Identity   1           0           0           0
CTS SGTNAME     0           0           0           0
CTS PAC         0           0           0           0
TrustSec-SXP    0           0           0           0
IPv6 Route      0           0           0           0
STS Table       0           0           0           0

Logical Update Queue Information
                Cur     Max     Total
Recv Q:         0       10      234
Xmit Q:         0       11      1200
```

다음 예에서는 디바이스가 페일오버에 대해 현재 구성되어 있지 않은 경우를 보여줍니다. 페일오버가 꺼져 있음을 나타내는 첫 번째 라인은 이 출력에서 유일하게 의미 있는 부분입니다.

```
> show high-availability config
Failover Off
Failover unit Secondary
Failover LAN Interface: not Configured
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 12 of 160 maximum
MAC Address Move Notification Interval not set
```

명령	설명
show failover	페일오버(고가용성) 구성을 표시합니다.

show https-access-list

show https-access-list 명령은 디바이스에 구성된 HTTPS 액세스 목록을 표시합니다.

show https-access-list

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

HTTPS 액세스 목록은 어떤 주소가 **configure network ipv4/ipv6** 명령을 통해 구성된 관리 인터페이스에 HTTPS 연결을 수행할 수 있는지 결정합니다. 로컬 관리자, Firepower Device Manager를 사용하여 디바이스를 구성 및 관리하려면 HTTPS 연결을 사용합니다.

이 액세스 목록은 데이터 인터페이스에 대한 through-the-box 트래픽 또는 HTTPS 액세스를 제어하지 않습니다.

다음 예는 관리 인터페이스에 대한 HTTPS 액세스 목록을 보여줍니다.

```
> show https-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:https
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:https
```

명령	설명
configure https-access-list	관리 인터페이스에 있는 HTTPS 액세스 목록을 구성합니다.

show i

show idb

인터페이스 리소스를 나타내는 내부 데이터 구조인 인터페이스 설명자 블록의 상태에 대한 정보를 표시하려면 **show idb** 명령을 사용합니다.

show idb

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show idb** 명령의 샘플 출력입니다.

```
> show idb
Maximum number of Software IDBs 2252.  In use(total) 16. In use(active) 16

                    HWIDBs     SWIDBs
             Active 15         15
           Inactive 1          1
         Total IDBs 16         16
 Size each (bytes) 984         1512
        Total bytes 15744      24192

HWIDB#  1 0xdacf1420  Virtual0
HWIDB#  2 0xdac4da20  GigabitEthernet1/1
HWIDB#  3 0xdac5aa20  GigabitEthernet1/2
HWIDB#  4 0xdac651b0  GigabitEthernet1/3
HWIDB#  5 0xdac6f940  GigabitEthernet1/4
HWIDB#  6 0xdac7a0d0  GigabitEthernet1/5
HWIDB#  7 0xdac84860  GigabitEthernet1/6
HWIDB#  8 0xdac8eff0  GigabitEthernet1/7
HWIDB#  9 0xdac99780  GigabitEthernet1/8
HWIDB# 10 0xdacbda00  Internal-Control1/1
HWIDB# 11 0xdaca3f10  Internal-Data1/1
HWIDB# 12 0xdacb3260  Internal-Data1/2
HWIDB# 13 0xdacc81a0  Internal-Data1/3
HWIDB# 14 0xd409e4e0  Internal-Data1/4
HWIDB# 15 0xd409d090  Management1/1

SWIDB#  1 0xdacf1840 0x00000041 Virtual0 UP UP
SWIDB#  2 0xdac4de40 0x00000002 GigabitEthernet1/1 UP DOWN
SWIDB#  3 0xdac5ae40 0x00000003 GigabitEthernet1/2 UP DOWN
SWIDB#  4 0xdac655d0 0xffffffff GigabitEthernet1/3 DOWN DOWN
SWIDB#  5 0xdac6fd60 0xffffffff GigabitEthernet1/4 DOWN DOWN
SWIDB#  6 0xdac7a4f0 0xffffffff GigabitEthernet1/5 DOWN DOWN
SWIDB#  7 0xdac84c80 0xffffffff GigabitEthernet1/6 DOWN DOWN
SWIDB#  8 0xdac8f410 0xffffffff GigabitEthernet1/7 DOWN DOWN
SWIDB#  9 0xdac99ba0 0xffffffff GigabitEthernet1/8 DOWN DOWN
SWIDB# 10 0xdacbde20 0x0000003f Internal-Control1/1 UP UP
SWIDB# 11 0xdaca4330 0x00000043 Internal-Data1/1 UP UP
SWIDB# 12 0xdacb3680 0xffffffff Internal-Data1/2 UP UP
SWIDB# 13 0xdacc85c0 0x00000044 Internal-Data1/3 UP UP
SWIDB# 14 0xdacae210 0x00000045 Internal-Data1/4 UP UP
SWIDB# 15 0xd409d4b0 0x00000004 Management1/1 UP UP
```

다음 표는 각 필드에 대해 설명합니다.

표 ***31: show idb stats*** 필드

필드	설명
HWIDBs	모든 HWIDB에 대한 통계를 표시합니다. HWIDB는 시스템의 각 하드웨어 포트에 대해 생성됩니다.
SWIDBs	모든 SWIDB에 대한 통계를 표시합니다. SWIDB는 시스템의 각 기본 및 하위 인터페이스와 상황에 할당된 각 인터페이스에 대해 생성됩니다. 일부 다른 내부 소프트웨어 모듈에서도 IDB를 생성합니다.
HWIDB#	하드웨어 인터페이스 항목을 지정합니다. IDB 시퀀스 번호, 주소 및 인터페이스 이름이 각 줄에 표시됩니다.
SWIDB#	소프트웨어 인터페이스 항목을 지정합니다. IDB 시퀀스 번호, 주소, 해당 vPif ID 및 인터페이스 이름이 각 줄에 표시됩니다.
PEER IDB#	상황에 할당된 인터페이스를 지정합니다. IDB 시퀀스 번호, 주소, 해당 vPif ID, 상황 ID 및 인터페이스 이름이 각 줄에 표시됩니다.

명령	설명
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

show igmp groups

Firepower Threat Defense 디바이스에 직접 연결되고 IGMP를 통해 학습된 수신기가 있는 멀티캐스트 그룹을 표시하려면 **show igmp groups** 명령을 사용합니다.

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

detail	(선택 사항) 소스에 대한 자세한 설명을 제공합니다.
group	(선택 사항) IGMP 그룹의 주소입니다. 이 선택적 인수를 포함하면 지정된 그룹으로 표시가 제한됩니다.
if_name	(선택 사항) 지정된 인터페이스에 대한 그룹 정보를 표시합니다.
reserved	(선택 사항) 예약된 그룹에 대한 정보를 표시합니다.
요약	(선택 사항) 그룹 가입 요약 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

모든 선택적 인수 및 키워드를 생략한 경우 **show igmp groups** 명령은 직접 연결된 모든 멀티캐스트 그룹을 그룹 주소, 인터페이스 유형 및 인터페이스 번호별로 표시합니다.

다음은 **show igmp groups** 명령의 샘플 출력입니다.

```
> show igmp groups
IGMP Connected Group Membership
```

```
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

명령	설명
show igmp interface	인터페이스에 대한 멀티캐스트 정보를 표시합니다.

show igmp interface

인터페이스에 대한 멀티캐스트 정보를 표시하려면 **show igmp interface** 명령을 사용합니다.

show igmp interface [*if_name*]

if_name	(선택 사항) 선택한 인터페이스에 대한 IGMP 그룹 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

선택적 *if_name* 인수를 생략한 경우 **show igmp interface** 명령은 모든 인터페이스에 대한 정보를 표시합니다.

다음은 **show igmp interface** 명령의 샘플 출력입니다.

```
> show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

명령	설명
show igmp groups	Firepower Threat Defense 디바이스에 직접 연결되고 IGMP를 통해 학습된 수신기가 있는 멀티캐스트 그룹을 표시합니다.

show igmp traffic

IGMP 트래픽 통계를 표시하려면 **show igmp traffic** 명령을 사용합니다.

show igmp traffic

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show igmp traffic** 명령의 샘플 출력입니다.

```
> show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                               Received     Sent
Valid IGMP Packets                3           6
Queries                           2           6
Reports                           1           0
Leaves                            0           0
Mtrace packets                    0           0
DVMRP packets                     0           0
PIM packets                       0           0

Errors:
Malformed Packets                 0
Martian source                    0
Bad Checksums                     0
```

명령	설명
clear igmp counters	모든 IGMP 통계 카운터를 지웁니다.
clear igmp traffic	IGMP 트래픽 카운터를 지웁니다.

show inline-set

디바이스에 구성된 IPS 전용 인터페이스인 인라인 집합에 대한 정보를 보려면 **show inline-set** 명령을 사용합니다.

show inline-set [*inline-set-name* | **mac-address-table**]

inline-set-name	(선택 사항) 지정된 인라인 집합에 대한 정보를 표시합니다. 이름을 포함하지 않은 경우, 모든 인라인 집합이 표시됩니다.
mac-address-table	(선택 사항) 인라인 집합의 MAC 주소 브리지 테이블을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show inline-set** 명령의 샘플 출력입니다.

```
> show inline-set
Inline-set ips-inline
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: GigabitEthernet0/3 "inline-inside"
      Current-Status: UP
    Interface: GigabitEthernet0/4 "inline-outside"
      Current-Status: DOWN
    Bridge Group ID: 504
```

show interface

인터페이스 통계를 보려면 **show interface** 명령을 사용합니다.

show interface [{*physical_interface* | **redundant***number*}[**.***subinterface*] | *interface_name* | **BVI** *id* |] [**summary** | **stats** | **detail**]

BVI*id*	(선택 사항) 표시된 BVI(Bridge Virtual Interface)의 통계를 표시합니다. BVI 수를 입력합니다(1-250).
detail	(선택 사항) 활성화된 경우 인터페이스가 추가된 순서, 구성된 상태, 실제 상태, 비대칭 라우팅 통계 등의 자세한 인터페이스 정보를 표시합니다. 모든 인터페이스를 표시하는 경우, 시스템 통신에 사용되는 내부 인터페이스에 대한 정보도 참조하십시오. 내부 인터페이스는 사용자가 구성할 수 없으며, 정보는 디버깅용으로만 제공됩니다.
interface_name	(선택 사항) 논리적 이름을 사용하여 인터페이스를 식별합니다.
physical_interface	(선택 사항) 인터페이스 ID(예: **gigabitethernet0/1**)를 식별합니다. 사용 가능한 인터페이스는 디바이스 모델에 따라 다릅니다. 디바이스에서 사용 가능한 이름을 보려면 파라미터없이 show interface 명령을 사용합니다.
redundant*number*	(선택 사항) 이중 인터페이스 ID(예: **redundant1**)를 식별합니다.
stats	(기본값) 인터페이스 정보 및 통계를 표시합니다. 이 키워드는 기본값이므로 선택 사항입니다.
summary	(선택 사항) 인터페이스에 대한 요약 정보를 표시합니다.
subinterface	(선택 사항) 논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.

옵션을 지정하지 않은 경우 이 명령은 내부 인터페이스를 제외한 모든 인터페이스에 대한 기본 통계를 표시합니다.

릴리스	수정
6.1	이 명령이 추가되었습니다.

릴리스	수정
6.2	**BVI** 키워드가 추가되었습니다.

사용 가이드라인

하위 인터페이스에 대해 표시되는 통계 수는 물리적 인터페이스에 대해 표시되는 통계 수의 하위 집합입니다.

참고

전송되거나 수신된 바이트 수는 하드웨어 카운트와 트래픽 통계 카운트에서 서로 다릅니다.

하드웨어 카운트에서는 수량이 하드웨어에서 직접 수신되므로 계층 2 패킷 크기를 반영합니다. 반면, 트래픽 통계에서는 계층 3 패킷 크기를 반영합니다.

이러한 카운트 차이는 인터페이스 카드 하드웨어의 설계에 따라 달라집니다.

예를 들어 고속 이더넷 카드의 경우 이더넷 헤더를 포함하기 때문에 계층 2 카운트가 트래픽 카운트보다 14바이트 더 많습니다. 기가비트 이더넷 카드의 경우 이더넷 헤더와 CRC를 모두 포함하므로 계층 2 카운트가 트래픽 카운트보다 18바이트 더 많습니다.

화면 출력에 대한 설명은 "예제" 섹션을 참고하십시오.

다음은 **show interface** 명령의 샘플 출력입니다.

```
> show interface
Interface GigabitEthernet1/1 "outside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f2, MTU 1500
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
  Traffic Statistics for "outside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/2 "inside", is down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
```

```
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f3, MTU 1500
        IP address 192.168.45.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet1/3 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f4, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/4 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f5, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/5 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f6, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
```

```
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/6 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f7, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/7 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f8, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface GigabitEthernet1/8 "", is administratively down, line protocol is down
  Hardware is Accelerator rev01, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex, Auto-Speed
        Input flow control is unsupported, output flow control is off
        Available but not configured via nameif
        MAC address e865.49b8.97f9, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (2047/2047)
        output queue (blocks free curr/low): hardware (2047/2047)
Interface Management1/1 "diagnostic", is up, line protocol is up
  Hardware is en_vtun rev00, BW 1000 Mbps, DLY 10 usec
        Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
        Input flow control is unsupported, output flow control is off
        MAC address e865.49b8.97f1, MTU 1500
        IP address unassigned
```

```
       14247681 packets input, 896591753 bytes, 0 no buffer
       Received 0 broadcasts, 0 runts, 0 giants
       0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
       0 pause input, 0 resume input
       0 L2 decode drops
       0 packets output, 0 bytes, 0 underruns
       0 pause output, 0 resume output
       0 output errors, 0 collisions, 0 interface resets
       0 late collisions, 0 deferred
       0 input reset drops, 0 output reset drops
       input queue (blocks free curr/low): hardware (0/0)
       output queue (blocks free curr/low): hardware (0/0)
Traffic Statistics for "diagnostic":
       14247685 packets input, 697121911 bytes
       0 packets output, 0 bytes
       5054964 packets dropped
     1 minute input rate 2 pkts/sec,  131 bytes/sec
     1 minute output rate 0 pkts/sec,  0 bytes/sec
     1 minute drop rate, 0 pkts/sec
     5 minute input rate 2 pkts/sec,  108 bytes/sec
     5 minute output rate 0 pkts/sec,  0 bytes/sec
     5 minute drop rate, 0 pkts/sec
       Management-only interface. Blocked 0 through-the-device packets
```

다음 표는 각 필드 설명을 보여줍니다.

표 ***32: show interface*** 필드

필드	설명
인터페이스 ID	인터페이스 ID입니다.
"*interface_name*"	논리적 인터페이스 이름입니다. 이름을 구성하지 않은 경우 Hardware 줄 뒤에 다음 메시지가 표시됩니다. `Available but not configured via nameif`
is *state*	다음과 같은 관리 상태입니다. • up - 인터페이스가 종료되지 않았습니다. • administratively down - 인터페이스가 의도적으로 종료됩니다.
Line protocol is state	다음과 같은 회선 상태입니다. • up - 작동하는 케이블이 네트워크 인터페이스에 연결되어 있습니다. • down - 케이블이 잘못되었거나 인터페이스 커넥터에 연결되어 있지 않습니다.
VLAN identifier	하위 인터페이스에 대한 VLAN ID입니다.
Hardware	인터페이스 유형, 최대 대역폭, 지연, 이중 및 속도입니다. 링크가 중단되면 이중 및 속도에 구성된 값이 표시됩니다. 링크가 작동하면 이러한 필드에 실제 설정이 괄호 안에 포함된 구성된 값이 표시됩니다.

필드	설명
Media-type	(항상 표시되지는 않음) RJ-45 또는 SFP 같은 인터페이스 미디어 유형을 표시합니다.
message area	경우에 따라 메시지가 표시될 수 있습니다. 다음 예를 참고하십시오. • 이름을 구성하지 않은 경우, 다음 메시지가 표시됩니다. Available but not configured via nameif(사용 가능하나 nameif를 통해 구성됨) • 인터페이스가 이중 인터페이스의 멤버인 경우 다음 메시지가 표시됩니다. Active member of Redundant5(Redundant5의 활성 멤버)
MAC address	인터페이스의 MAC 주소입니다.
Site Specific MAC address	클러스터링의 경우, 사용 중인 사이트별 MAC 주소를 표시합니다.
MTU	이 인터페이스에서 허용되는 최대 패킷 크기(바이트)입니다. 인터페이스 이름을 설정하지 않은 경우에는 이 필드에 "MTU not set"이 표시됩니다.
IP address	DHCP 서버에서 고정되거나 수신된 인터페이스 IP 주소입니다.
Subnet mask	IP 주소의 서브넷 마스크입니다.
Packets input	이 인터페이스에서 수신된 패킷 수입니다.
Bytes	이 인터페이스에서 수신된 바이트 수입니다.
No buffer	블록 할당 실패 횟수입니다.
Received:	
Broadcasts	수신한 브로드캐스트 수입니다.
Input errors	아래 나열된 유형을 포함한 총 입력 오류 수입니다. 다른 입력 관련 오류로 인해 입력 오류 수가 증가할 수도 있으며, 일부 데이터그램에 둘 이상의 오류가 있을 수도 있습니다. 따라서 이 합계가 아래 유형에 대해 나열된 오류 수를 초과할 수 있습니다.
Runts	최소 패킷 크기(64바이트)보다 작기 때문에 삭제된 패킷 수입니다. Runt는 일반적으로 충돌로 인해 발생합니다. 또한 잘못된 배선 및 전기 간섭으로 인해 발생할 수도 있습니다.
Giants	최대 패킷 크기를 초과하기 때문에 삭제된 패킷 수입니다. 예를 들어 1518 바이트보다 큰 이더넷 패킷은 Giant로 간주됩니다.

필드	설명
CRC	Cyclical Redundancy Check 오류 수입니다. 스테이션에서는 프레임을 전송할 때 프레임 끝에 CRC를 추가합니다. 이러한 CRC는 프레임의 데이터를 기반으로 한 알고리즘에서 생성됩니다. 소스와 대상 간에 프레임이 변경된 경우 시스템은 CRC가 일치하지 않는 것으로 기록합니다. 더 많은 CRC 수는 일반적으로 충돌로 인해 발생하거나 스테이션에서 잘못된 데이터를 전송했기 때문에 발생합니다.
Frame	프레임 오류 수입니다. 잘못된 프레임에는 길이 또는 프레임 체크섬이 잘못된 패킷이 포함됩니다. 이 오류는 일반적으로 충돌 또는 이더넷 디바이스의 오작동으로 인해 발생합니다.
Overrun	입력 속도가 인터페이스에서 데이터를 처리할 수 있는 성능을 초과하기 때문에 인터페이스가 수신된 데이터를 하드웨어 버퍼로 전달하지 못한 횟수입니다.
Ignored	이 필드는 사용되지 않습니다. 값은 항상 0입니다.
Abort	이 필드는 사용되지 않습니다. 값은 항상 0입니다.
L2 decode drops	이름이 구성되지 않았거나 VLAN ID가 잘못된 프레임이 수신되어 드롭된 패킷 수입니다. 이중 인터페이스 컨피그레이션의 스탠바이 인터페이스에는 구성된 이름이 없기 때문에 이 카운터가 증가할 수 있습니다.
Packets output	이 인터페이스에서 전송된 패킷 수입니다.
Bytes	이 인터페이스에서 전송된 바이트 수입니다.
Underruns	송신기가 인터페이스에서 처리할 수 있는 것보다 빠르게 실행된 횟수입니다.
Output Errors	구성된 최대 충돌 수를 초과했기 때문에 전송되지 않은 프레임 수입니다. 이 카운터는 네트워크 트래픽이 많은 경우에만 증가합니다.
Collisions	이더넷 충돌(단일 및 다중 충돌)로 인해 재전송된 메시지 수입니다. 일반적으로 과도하게 연장된 LAN(이더넷 또는 트렌시버 케이블이 너무 길거나, 스테이션 사이에 세 개 이상의 리피터가 있거나, 연속된 다중 포트 트렌시버가 너무 많은 경우)에서 발생합니다. 충돌하는 패킷은 출력 패킷에서 한 번만 계산됩니다.
Interface resets	인터페이스가 재설정된 횟수입니다. 인터페이스가 3초 동안 전송할 수 없는 경우 시스템은 전송을 다시 시작하도록 인터페이스를 재설정합니다. 이 간격 동안 연결 상태는 유지됩니다. 인터페이스가 루프백 또는 종료된 경우에도 인터페이스 재설정이 발생할 수 있습니다.

필드	설명
Babbles	사용되지 않습니다. “babble”은 송신기가 최대 프레임을 전송하는 데 걸린 시간보다 오랫동안 인터페이스에 있었음을 의미합니다.
Late collisions	정상적인 충돌 기간을 벗어나 충돌이 발생했기 때문에 전송되지 않은 프레임 수입니다. 지연 충돌은 패킷 전송에서 늦게 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. 지연 충돌이 발생한 경우 디바이스는 Firepower Threat Defense 디바이스에서 패킷 전송을 부분적으로 완료하는 동안 이더넷에서 패킷을 전송하려고 시도합니다. Firepower Threat Defense 디바이스는 패킷의 첫 번째 부분을 유지하는 버퍼를 지웠을 수 있으므로 패킷을 다시 전송하지 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 이더넷 네트워크 및 반복되는 대규모 네트워크입니다.
Deferred	링크 활동으로 인해 전송 전에 지연된 프레임 수입니다.
input reset drops	재설정이 발생한 경우 RX 링에서 드롭된 패킷 수를 계산합니다.
output reset drops	재설정이 발생한 경우 TX 링에서 드롭된 패킷 수를 계산합니다.
Rate limit drops	기가비트가 아닌 속도로 인터페이스를 구성한 후 컨피그레이션에 따라 10Mbps 또는 100Mbps보다 빠른 속도로 전송하려고 시도한 경우 드롭된 패킷 수입니다.
Lost carrier	전송 중에 반송파 신호가 손실된 횟수입니다.
No carrier	사용되지 않습니다.
Input queue (curr/max packets):	입력 대기열의 현재 및 최대 패킷 수입니다.
Hardware	하드웨어 대기열의 패킷 수입니다.
Software	소프트웨어 대기열의 패킷 수입니다. 기가비트 이더넷 인터페이스에는 사용할 수 없습니다.
Output queue (curr/max packets):	출력 대기열의 현재 및 최대 패킷 수입니다.
Hardware	하드웨어 대기열의 패킷 수입니다.

필드	설명
Software	소프트웨어 대기열의 패킷 수입니다.
input queue (blocks free curr/low)	curr/low 항목은 인터페이스의 수신(입력) 설명자 링의 현재 슬롯 수 및 항상 사용 가능한 최소 슬롯 수입니다. 이는 기본 CPU에 의해 업데이트되므로 항상 사용 가능한 최소(인터페이스 통계가 지워지거나 디바이스가 다시 로드될 때까지) 워터마크는 그다지 정확하지 않습니다.
output queue (blocks free curr/low)	curr/low 항목은 인터페이스의 전송(출력) 설명자 링의 현재 슬롯 수 및 항상 사용 가능한 최소 슬롯 수입니다. 이는 기본 CPU에 의해 업데이트되므로 항상 사용 가능한 최소(인터페이스 통계가 지워지거나 디바이스가 다시 로드될 때까지) 워터마크는 그다지 정확하지 않습니다.
Traffic Statistics:	수신되거나 전송되거나 드롭된 패킷 수입니다.
Packets input	수신된 패킷 수와 바이트 수입니다.
Packets output	전송된 패킷 수와 바이트 수입니다.
Packets dropped	드롭된 패킷 수입니다. 일반적으로 이 카운터는 ASP(가속화된 보안 경로)에서 드롭된 패킷에 대해 증가합니다(예: 패킷이 액세스 목록 거부로 인해 삭제된 경우). 인터페이스에서 잠재적으로 드롭될 수 있는 사유는 **show asp drop** 명령을 참고하십시오.
1 minute input rate	지난 1분 동안 수신된 패킷 수(패킷/초 및 바이트/초)입니다.
1 minute output rate	지난 1분 동안 전송된 패킷 수(패킷/초 및 바이트/초)입니다.
1 minute drop rate	지난 1분 동안 드롭된 패킷 수(패킷/초)입니다.
5 minute input rate	지난 5분 동안 수신된 패킷 수(패킷/초 및 바이트/초)입니다.
5 minute output rate	지난 5분 동안 전송된 패킷 수(패킷/초 및 바이트/초)입니다.
5 minute drop rate	지난 5분 동안 드롭된 패킷 수(패킷/초)입니다.
Redundancy Information:	이중 인터페이스에 대한 멤버의 물리적 인터페이스를 표시합니다. 활성 인터페이스에는 인터페이스 ID 뒤에 “(Active)”가 표시됩니다. 멤버를 아직 지정하지 않은 경우 다음 출력이 표시됩니다. `Members unassigned`
Last switchover	이중 인터페이스에 대해 활성 인터페이스가 대기 인터페이스로 마지막으로 대체작동된 시간을 표시합니다.

다음은 **show interface detail** 명령의 샘플 출력입니다. 다음 예에서는 내부 인터페이스(플랫폼에 대해 존재하는 경우) 및 비대칭 라우팅 통계(활성화된 경우)를 포함하여 모든 인터페이스에 대한 자세한 인터페이스 통계를 보여줍니다.

```
> show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

다음 표는 **show interface detail** 명령에서 표시된 추가 필드를 설명합니다.

표 ***33: show interface detail*** 필드

필드	설명
Demux drops	(내부 데이터 인터페이스에만 해당) Firepower Threat Defense 디바이스가 기타 인터페이스의 패킷을 역다중화할 수 없어 드롭된 패킷 수입니다.
Control Point Interface States:	
Interface number	0에서 시작하여 이 인터페이스가 생성된 순서를 나타내는 디버깅용 번호입니다.

필드	설명
Interface config status	다음과 같은 관리 상태입니다. • active - 인터페이스가 종료되지 않았습니다. • not active - 인터페이스가 의도적으로 종료됩니다.
Interface state	인터페이스의 실제 상태입니다. 대부분의 경우 이 상태는 위의 config status와 일치합니다. 고가용성을 구성한 경우 Firepower Threat Defense 디바이스에서 필요에 따라 인터페이스를 작동하거나 중단하기 때문에 불일치가 발생할 수 있습니다.
Asymmetrical Routing Statistics:	
Received X1 packets	이 인터페이스에서 수신된 ASR 패킷 수입니다.
Transmitted X2 packets	이 인터페이스에서 전송된 ASR 패킷 수입니다.
Dropped X3 packets	이 인터페이스에서 드롭된 ASR 패킷 수입니다. 패킷을 전달하려고 할 때 인터페이스의 작동이 중지된 경우 패킷이 드롭될 수 있습니다.

명령	설명
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
show interface ip brief	인터페이스 IP 주소 및 상태를 표시합니다.

show interface ip brief

인터페이스 IP 주소 및 상태를 보려면 **show interface ip brief** 명령을 사용합니다.

show interface [[*physical_interface*[**.***subinterface*] | *interface_name* | **BVI** *id* |] **ip brief**

BVI*id*	(선택 사항) 표시된 BVI(브리지 가상 인터페이스)의 통계를 표시합니다. BVI 수를 입력합니다(1-250).
interface_name	(선택 사항) 인터페이스 이름을 식별합니다.
physical_interface	(선택 사항) 인터페이스 ID(예: **gigabitethernet0/1**)를 식별합니다.
subinterface	(선택 사항) 논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.

인터페이스를 지정하지 않은 경우 명령은 내부 인터페이스를 포함하여 모든 인터페이스를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.
6.2	**BVI** 키워드가 추가되었습니다.

다음은 **show ip brief** 명령의 샘플 출력입니다.

```
> show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   administratively down down
    GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
    Management0/0              209.165.201.3   YES CONFIG  up
```

다음 예에서는 대부분의 인터페이스가 BVI의 일부인 경우 주소 지정을 표시합니다. 멤버 인터페이스에는 상위 BVI와 동일한 주소가 있습니다.

```
> show interface ip brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet1/1         unassigned      YES DHCP   down                  down
GigabitEthernet1/2         192.168.1.1     YES unset  down                  down
GigabitEthernet1/3         192.168.1.1     YES unset  down                  down
GigabitEthernet1/4         192.168.1.1     YES unset  down                  down
GigabitEthernet1/5         192.168.1.1     YES unset  down                  down
GigabitEthernet1/6         192.168.1.1     YES unset  down                  down
GigabitEthernet1/7         192.168.1.1     YES unset  down                  down
GigabitEthernet1/8         192.168.1.1     YES unset  down                  down
Internal-Control1/1        127.0.1.1       YES unset  up                    up
Internal-Data1/1           unassigned      YES unset  up                    up
Internal-Data1/2           unassigned      YES unset  down                  down
Internal-Data1/3           unassigned      YES unset  up                    up
Internal-Data1/4           169.254.1.1     YES unset  up                    up
Management1/1              unassigned      YES unset  up                    up
BVI1                       192.168.1.1     YES manual up                    up
```

다음 표에서는 출력 필드를 설명합니다.

표 ***34: show interface ip brief*** 필드

필드	설명
인터페이스	인터페이스 ID. 모든 인터페이스를 표시하는 경우, 시스템 통신에 사용된 내부 인터페이스에 대한 정보도 참조하십시오. 내부 인터페이스는 사용자가 구성할 수 없으며, 정보는 디버깅용으로만 제공됩니다.
IP-Address	인터페이스 IP 주소입니다.
OK?	이 열은 현재 사용되지 않으며, 항상 "Yes"로 표시됩니다.
메서드	인터페이스에서 IP 주소를 수신한 방법입니다. 값은 다음과 같습니다. • unset - 구성된 IP 주소가 없습니다. • manual - 인터페이스에 고정 주소가 있습니다. • CONFIG - 시작 컨피그레이션에서 로드했습니다. • DHCP - DHCP 서버에서 수신했습니다.
상태	다음과 같은 관리 상태입니다. • up - 인터페이스가 종료되지 않았습니다. • down - 인터페이스가 작동하지 않으며 의도적으로 종료되지도 않습니다. • administratively down - 인터페이스가 의도적으로 종료됩니다.

필드	설명
프로토콜	다음과 같은 회선 상태입니다. • up - 작동하는 케이블이 네트워크 인터페이스에 연결되어 있습니다. • down - 케이블이 잘못되었거나 인터페이스 커넥터에 연결되어 있지 않습니다.

명령	설명
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

show inventory

네트워킹 디바이스에 설치되어 있으며 PID(Product Identifier: 제품 식별자), VID(Version Identifier: 버전 식별자) 및 SN(Serial Number: 일련 번호)이 할당된 모든 Cisco 제품에 대한 정보를 표시하려면 **show inventory** 명령을 사용합니다.

show inventory [*slot_id*]

slot_id	(선택 사항) 모듈 ID 또는 슬롯 번호 0~3을 지정합니다.

항목의 인벤토리를 표시할 슬롯을 지정하지 않으면 모든 모듈(전원 공급 디바이스 포함)의 인벤토리 정보가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show inventory 명령은 각 Cisco 제품에 대한 인벤토리 정보를 검색하여 UDI 형식으로 표시합니다. 이는 PID(Product Identifier: 제품 식별자), VID(Version Identifier: 버전 식별자) 및 SN(Serial Number: 일련 번호)이라는 세 가지 개별 데이터 요소의 조합입니다.

PID는 제품을 주문 할 수 있는 이름으로, 과거에는 "제품 이름" 또는 "부품 번호"라고 불렀습니다. 이것은 정확한 교체 부품을 주문하는 데 사용하는 식별자입니다.

VID는 제품의 버전입니다. 제품이 수정된 경우 제품 변경 고지에 적용되는 Telcordia GR-209-CORE에서 파생된 엄격한 프로세스에 따라 VID가 증가합니다.

SN은 공급업체 고유의 제품 직렬화입니다. 제조된 각 제품에는 공장에서 할당된 고유한 일련 번호가 있으며, 이는 현장에서 변경할 수 없습니다. 일련 번호는 제품의 특정한 개별 인스턴스를 식별하는 방법입니다. 디바이스의 구성 요소마다 일련 번호 길이가 다를 수 있습니다.

UDI는 각 제품을 하나의 엔터티로 참조합니다. 섀시와 같은 일부 엔터티에는 슬롯과 같은 하위 엔터티가 있습니다. 각 엔티티는 Cisco 엔터티를 기준으로 계층적으로 정렬된 논리적 순서의 프레젠테이션에서 별도의 줄에 표시됩니다.

show inventory 명령은 네트워킹 디바이스에 설치된 PID가 할당된 Cisco 엔터티 목록을 표시하는 옵션 없이 사용됩니다.

Cisco 엔터티에 PID가 할당되지 않은 이 엔터티는 검색되거나 표시되지 않습니다.

ASA 5500-X Series의 경우 하드웨어 제한으로 인해 일련 번호가 표시되지 않을 수 있습니다. 이러한 모델의 PCI-E I/O(NIC) 옵션 카드는 두 가지 유형뿐이지만 해당 UDI 표시에는 섀시 유형에 따라 6개의 출력이 표시될 수 있습니다. 이는 지정된 섀시에 따라 사용되는 PCI-E 브래킷 어셈블리가 다르기 때문입니다. 다음 예에서는 각 PCI-E I/O 카드 어셈블리에 대한 예상 출력을 보여 줍니다. 예를 들어 Silicom SFP NIC 카드가 검색된 경우 UDI 표시는 해당 카드가 설치된 디바이스에 따라 결정됩니다. VID 및 S/N 값은 전자적으로 저장되지 않으므로 N/A입니다.

ASA 5512-X 또는 5515-X에 설치된 6포트 SFP 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

ASA 5525-X에 설치된 6포트 SFP 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

ASA 5545-X 또는 5555-X에 설치된 6포트 SFP 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

ASA 5512-X 또는 5515-X에 설치된 6포트 구리 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

ASA 5525-X에 설치된 6포트 구리 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

ASA 5545-X 또는 5555-X에 설치된 6포트 구리 이더넷 NIC 카드:

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

다음은 키워드 또는 인수 없이 실행된 **show inventory** 명령의 샘플 출력입니다. 이 샘플 출력은 각각 PID에 할당된 Firepower Threat Defense 디바이스에 설치된 Cisco 엔터티의 목록을 표시합니다.

```
> show inventory
Name: "Chassis", DESCR: "ASA 5508-X with FirePOWER services, 8GE, AC, DES"
PID: ASA5508           , VID: V01     , SN: JMX1923408S

Name: "Storage Device 1", DESCR: "ASA 5508-X SSD"
PID: ASA5508-SSD       , VID: N/A     , SN: MXA184205MC
```

다음 표에는 화면에 표시되는 필드에 대한 설명이 나와 있습니다.

표 ***35: show inventory***에 대한 필드 설명

필드	설명
Name(이름)	Cisco 엔터티에 할당된 물리적 이름(텍스트 문자열)입니다. 예를 들어 디바이스의 물리적 구성요소 명명 구문에 따라 콘솔, SSP 또는 "1"과 같은 간단한 구성 요소 번호(포트 또는 모듈 번호)일 수 있습니다. RFC 2737의 entPhysicalName MIB 변수와 같습니다.
DESCR	개체를 분류하는 Cisco 엔터티에 대한 물리적 설명입니다. RFC 2737의 entPhysicalDesc MIB 변수와 같습니다.
PID	엔티티 제품 식별자입니다. RFC 2737의 entPhysicalModelName MIB 변수와 같습니다.
VID	엔터티 버전 식별자입니다. RFC 2737의 entPhysicalHardwareRev MIB 변수와 같습니다.
SN	엔터티 일련 번호입니다. RFC 2737의 entPhysicalSerialNum MIB 변수와 같습니다.

show ip address

인터페이스 IP 주소 또는 투명 모드의 경우 관리 IP 주소를 보려면 **show ip address** 명령을 사용합니다.

show ip address [[*physical_interface*[**.***subinterface*] | *interface_name* |]

interface_name	(선택 사항) 인터페이스 이름을 식별합니다.
physical_interface	(선택 사항) 인터페이스 ID(예: **gigabit**ethernet0/1)를 식별합니다.
subinterface	(선택 사항) 논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.

인터페이스를 지정하지 않은 경우 출력이 모든 인터페이스 IP 주소를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 고가용성을 구성한 경우 현재 IP 주소와 함께 기본 IP 주소(화면에서는 "System"이라고 함)를 표시합니다. 디바이스가 활성 상태이면 시스템 IP 주소와 현재 IP 주소가 일치합니다. 디바이스가 대기 상태이면 현재 IP 주소에 대기 주소가 표시됩니다.

IP 주소는 데이터 인터페이스 전용입니다. 이 명령은 투명 모드 관리 인터페이스와 동일하지 않은 진단 인터페이스에서 관리 인터페이스의 시스템 ID 주소를 표시하지 않습니다. 이 정보에는 진단 인터페이스(구성된 경우)에 대한 IP 주소 정보가 포함됩니다. 관리 인터페이스에 대한 정보를 보려면 **show network** 명령을 사용합니다.

다음은 **show ip address** 명령의 샘플 출력입니다.

```
> show ip address
System IP Addresses:
Interface                Name         IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt         10.7.12.100     255.255.255.0     CONFIG
```

```
GigabitEthernet0/1       inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface                Name         IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz          209.165.200.225 255.255.255.224   manual
```

다음 표는 각 필드에 대해 설명합니다.

표 ***36: show ip address*** 필드

필드	설명
인터페이스	인터페이스 ID.
이름	인터페이스 이름입니다.
IP 주소	인터페이스 IP 주소입니다.
Subnet mask	IP 주소 서브넷 마스크입니다.
메서드	인터페이스에서 IP 주소를 수신한 방법입니다. 값은 다음과 같습니다. • unset - 구성된 IP 주소가 없습니다. • manual - 인터페이스에 고정 주소가 있습니다. • CONFIG - 시작 컨피그레이션에서 로드했습니다. • DHCP - DHCP 서버에서 수신했습니다.

명령	설명
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.
show interface ip brief	인터페이스 IP 주소 및 상태를 표시합니다.

show ip address dhcp

인터페이스의 DHCP 리스 또는 서버에 대한 자세한 정보를 보려면 **show ip address dhcp** 명령을 사용합니다.

show ip address {*physical_interface*[**.***subinterface*] | *interface_name*} **dhcp server**

show ip address {*physical_interface*[**.***subinterface*] | *interface_name*} **dhcp lease** [**proxy** | **server**] [**summary**]

interface_name	인터페이스 이름을 식별합니다.
lease	DHCP 리스에 대한 정보를 표시합니다.
physical_interface	인터페이스 ID(예: **gigabitethernet0/1**)를 식별합니다.
proxy	IPL 테이블의 프록시 항목을 표시합니다.
server	IPL 테이블의 서버 항목을 표시합니다.
subinterface	논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.
summary	항목에 대한 요약을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ip address dhcp lease** 명령의 샘플 출력입니다.

```
> show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

다음 표는 각 필드에 대해 설명합니다.

표 ***37: show ip address dhcp lease*** 필드

필드	설명
Temp IP Addr	인터페이스에 할당된 IP 주소입니다.
Temp sub net mask	인터페이스에 할당된 서브넷 마스크입니다.
DHCP Lease server	DHCP 서버 주소입니다.
state	다음과 같은 DHCP 임대 상태입니다. • Initial - 디바이스에서 리스를 획득하는 프로세스를 시작한 초기화 상태입니다. 리스가 끝나거나 리스 협상에 실패한 경우에도 이 상태가 표시됩니다. • Selecting - 디바이스가 하나 이상의 DHCP 서버에서 DHCPOFFER 메시지를 받아 하나를 선택할 수 있도록 기다리고 있습니다. • Requesting - 디바이스가 요청을 전송한 서버에서 다시 수신되기를 기다리고 있습니다. • Purging - 클라이언트가 IP 주소를 다시 반납했거나 다른 오류가 발생하여 디바이스에서 리스를 제거하는 중입니다. • Bound - 디바이스에 유효한 리스가 있으며 정상적으로 작동하고 있습니다. • Renewing - 디바이스가 리스를 갱신하려고 시도 중입니다. 디바이스가 DHCPREQUEST 메시지를 정기적으로 현재 DHCP 서버로 전송하여 응답을 기다립니다. • Rebinding - 디바이스가 원래 서버에서 리스를 갱신하지 못해 임의의 서버에서 응답을 받거나 리스가끝날 때까지 DHCPREQUEST 메시지를 보냅니다. • Holddown - 디바이스가 리스를 제거하는 프로세스를 시작했습니다. • Releasing - 디바이스에서 IP 주소가 더 이상 필요하지 않음을 나타내는 해제 메시지를 서버에 보냅니다.
DHCP transaction id	클라이언트와 서버에서 요청 메시지를 연결하는 데 사용하기 위해 클라이언트에서 선택한 난수입니다.
Lease	인터페이스에서 이 IP 주소를 사용할 수 있는 기간으로, DHCP 서버에서 지정합니다.
Renewal	인터페이스에서 이 임대를 자동으로 갱신할 때까지의 기간입니다.

필드	설명
Rebind	Firepower Threat Defense 디바이스가 DHCP 서버에 다시 바인딩할 때까지의 기간입니다. 리바인딩은 디바이스가 원래 DHCP 서버와 통신할 수 없고 리스 시간의 87.5%가 만료된 경우에 발생합니다. 그런 다음 디바이스는 DHCP 요청을 브로드캐스트하여 사용 가능한 DHCP 서버에 연결하려고 시도합니다.
Temp default-gateway addr	DHCP 서버에서 제공하는 기본 게이트웨이 주소입니다.
Temp ip static route0	기본 고정 경로입니다.
Next timer fires after	내부 타이머가 트리거되는 시간(초)입니다.
재시도 횟수	Firepower Threat Defense 디바이스에서 리스를 설정하려고 시도하면 이 필드에 디바이스에서 DHCP 메시지를 보내려고 시도한 횟수가 표시됩니다. 예를 들어 디바이스의 상태가 Selecting이면 디바이스에서 검색 메시지를 보낸 횟수가 이 값에 표시됩니다. 디바이스의 상태가 Requesting이면 디바이스에서 요청 메시지를 보낸 횟수가 이 값에 표시됩니다.
Client-ID	서버와의 모든 통신에 사용되는 클라이언트 ID입니다.
Proxy	이 인터페이스가 VPN 클라이언트에 대한 프록시 DHCP 클라이언트인지 여부를 참 또는 거짓으로 지정합니다.
Proxy Network	요청받은 네트워크입니다.
Hostname	클라이언트 호스트 이름입니다.

다음은 **show ip address dhcp server** 명령의 샘플 출력입니다.

```
> show ip address outside dhcp server
   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

다음 표는 각 필드에 대해 설명합니다.

표 ***38: show ip address dhcp server*** 필드

필드	설명
DHCP server	이 인터페이스가 리스를 얻은 DHCP 서버 주소입니다. 상위 항목(“ANY”)은 기본 서버이며 항상 존재합니다.
Leases	서버에서 얻은 대여 수입니다. 예를 들어 임대 수는 일반적으로 1입니다. 서버에서 VPN용 프록시를 실행 중인 인터페이스에 대한 주소를 제공하는 경우 임대가 여러 개 있을 것입니다.
Offers	서버의 제안 수입니다.
Requests	서버로 전송된 요청 수입니다.
Acks	서버에서 받은 확인 응답 수입니다.
Naks	서버에서 받은 부정적인 확인 응답 수입니다.
Declines	서버에서 받은 거부 수입니다.
릴리스s	서버로 전송된 임대 수입니다.
Bad	서버에서 받은 불량 패킷 수입니다.
DNS0	DHCP 서버에서 받은 기본 DNS 서버 주소입니다.
DNS1	DHCP 서버에서 받은 보조 DNS 서버 주소입니다.
WINS0	DHCP 서버에서 받은 기본 WINS 서버 주소입니다.
WINS1	DHCP 서버에서 받은 보조 WINS 서버 주소입니다.
Subnet	DHCP 서버에서 받은 서브넷 주소입니다.
DNS Domain	DHCP 서버에서 받은 도메인입니다.

명령	설명
show interface ip brief	인터페이스 IP 주소 및 상태를 표시합니다.
show ip address	인터페이스의 IP 주소를 표시합니다.

show ip address pppoe

PPPoE 연결에 대한 자세한 정보를 보려면 **show ip address pppoe** 명령을 사용합니다.

show ip address {*physical_interface*[**.***subinterface*] | *interface_name* | } **pppoe**

interface_name	인터페이스 이름을 식별합니다.
physical_interface	인터페이스 ID(예: **gigabitethernet0/1**)를 식별합니다.
subinterface	논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

명령	설명
show interface ip brief	인터페이스 IP 주소 및 상태를 표시합니다.
show ip address	인터페이스의 IP 주소를 표시합니다.

show ip audit count

이 명령을 사용하지 마십시오. 이 명령은 Firepower Threat Defense에서 지원하지 않는 기능과 관련이 있습니다.

show ip verify statistics

유니캐스트 RPF 기능 때문에 드롭된 패킷 수를 표시하려면 **show ip verify statistics** 명령을 사용합니다.

show ip verify statistics [**interface** *interface_name*]

interface*interface_name*	(선택 사항) 특정 인터페이스에 대한 통계를 보여줍니다.

이 명령은 모든 인터페이스에 대한 통계를 보여줍니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ip verify statistics** 명령의 샘플 출력입니다.

```
> show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

명령	설명
clear ip verify statistics	유니캐스트 RPF 통계를 지웁니다.
show running-config ip verify reverse-path	**ip verify reverse-path** 컨피그레이션을 표시합니다.

show ipsec sa

IPsec SA(보안 연결)의 목록을 표시하려면 **show ipsec sa** 명령을 사용합니다. 이 명령어의 대체 양식인 **show crypto ipsec sa**를 사용해도 됩니다.

show ipsec sa [**assigned-address** *hostname_or_IP_address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr* | **spi** *spi-num*] [**detail**]

assigned-address *hostname_or_IP_address*	(선택 사항) 지정된 호스트 이름 또는 IP 주소에 대한 IPsec SA를 표시합니다.
detail	(선택 사항) 표시된 항목에 대한 자세한 오류 정보를 표시합니다.
entry	(선택 사항) 피어 주소별로 정렬된 IPsec SA를 표시합니다.
ID	(선택 사항) ESP를 포함하지 않고 ID별로 정렬된 IPsec SA를 표시합니다. 이는 축소된 형식입니다.
inactive	(선택 사항) 트래픽을 전달할 수 없는 IPsec SA를 표시합니다.
map *map-name*	(선택 사항) 지정된 암호화 맵에 대한 IPsec SA를 표시합니다.
peer *peer-addr*	(선택 사항) 지정된 피어 IP 주소에 대한 IPsec SA를 표시합니다.
spi *spi-num*	(선택 사항) SPI에 대한 IPsec SA를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 할당된 IPv6 주소와 전송 모드 및 GRE 캡슐화 표시를 포함하여 IPsec SA를 표시합니다.

```
> show ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
```

```
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 4

     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624

    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

다음 예는 터널을 OSPFv3으로 식별하는 데 사용 중인 설정을 포함하여 IPsec SA를 표시합니다.

```
> show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3),}
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
```

```
        transform: esp-3des esp-md5-hmac
        in use settings ={L2L, Transport, Manual key (OSPFv3), }
        slot: 0, conn_id: 3, crypto-map: def
        sa timing: remaining key lifetime (sec): 548
        IV size: 8 bytes
        replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

참고 조각화 통계는 IPsec SA 정책에 IPsec 처리 전 조각화가 발생하도록 규정된 경우 사전 조각화 통계입니다. 사후 조각화 통계는 SA 정책에 IPsec 처리 후 조각화가 발생하도록 규정된 경우에 표시됩니다.

글로벌 구성 모드에서 입력된 다음 예에서는 def라는 암호화 맵에 대한 IPsec SA를 표시합니다.

```
> show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
```

```
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
```

다음 예에서는 키워드 **entry**에 대한 IPsec SA를 보여줍니다.

```
> show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
```

```
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
```

다음 예에서는 키워드 **entry detail**에 대한 IPsec SA를 보여줍니다.

```
> show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17
```

```
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
>
```

다음 예에서는 키워드 **identity**에 대한 IPsec SA를 보여줍니다.

```
> show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
```

```
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

다음 예에서는 키워드 **identity** 및 **detail**에 대한 IPsec SA를 보여줍니다.

```
> show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

다음 예에서는 IPv6 할당 주소를 기반으로 IPSec SA를 표시합니다.

```
> show ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23

      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
```

```
  dynamic allocated peer ip(ipv6): 2001:1000::10

  #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
  #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
  #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 35

  local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
  path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: D9C00FC2
  current inbound spi : 4FCB6624

inbound esp sas:
  spi: 0x4FCB6624 (1338730020)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
  spi: 0xD9C00FC2 (3653242818)
     transform: esp-3des esp-sha-hmac no compression
     in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
     slot: 0, conn_id: 8192, crypto-map: def
     sa timing: remaining key lifetime (sec): 28108
     IV size: 8 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x00000001
```

명령	설명
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 ISAKMP 구성을 표시합니다.

show ipsec sa summary

IPsec SA의 요약을 표시하려면 **show ipsec sa summary** 명령을 사용합니다.

show ipsec sa summary

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 아래의 연결 유형별로 IPsec SA의 요약을 표시합니다.

- IPSec
- IPsec over UDP
- IPsec over NAT-T
- IPsec over TCP
- IPsec VPN load balancing

```
> show ipsec sa summary
Current IPsec SA's:           Peak IPsec SA's:
IPsec              :     2      Peak Concurrent SA  :    14
IPsec over UDP     :     2      Peak Concurrent L2L :     0
IPsec over NAT-T   :     4      Peak Concurrent RA  :    14
IPsec over TCP     :     6
IPsec VPN LB       :     0
Total              :    14
```

명령	설명
clear ipsec sa	IPsec SA를 모두 제거하거나 특정 파라미터를 기반으로 제거합니다.
show ipsec sa	IPsec SA 목록을 표시합니다.
show ipsec stats	IPsec 통계 목록을 표시합니다.

show ipsec stats

IPsec 통계의 목록을 표시하려면 **show ipsec stats** 명령을 사용합니다.

show ipsec stats

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

다음 테이블에는 출력 항목의 의미가 설명되어 있습니다.

출력(계속됨)	설명(계속됨)
IPsec Global Statistics	이 섹션은 Firepower Threat Defense 디바이스에서 지원하는 총 IPsec 터널 수와 관계가 있습니다.
Active tunnels	현재 연결된 IPsec 터널 수 입니다.
Previous tunnels	활성 상태인 터널을 포함하여 연결된 IPsec 터널의 수입니다.
Inbound	이 섹션은 IPsec 터널을 통해 받은 인바운드 암호화 트래픽과 관계가 있습니다.
Bytes	수신된 암호화 트래픽의 바이트 수입니다.
Decompressed bytes	해당하는 경우 압축을 해제한 후에 수신된 암호화 트래픽의 바이트 수입니다. 압축이 활성화되지 않은 경우에는 이 바이트 수가 이전 바이트 수와 항상 같아야 합니다.
Packets	수신된 암호화 IPsec 패킷의 수입니다.
Dropped packets	수신되었지만 오류 때문에 끊어진 암호화 IPsec 패킷의 수입니다.
Replay failures	수신된 암호화 IPsec 패킷에서 감지된 재전송 방지 실패 횟수입니다.
Authentications	수신된 암호화 IPsec 패킷에서 성공적으로 수행된 인증 횟수입니다.

출력(계속됨)	설명(계속됨)
Authentication failures	수신된 암호화 IPsec 패킷에서 감지된 인증 실패 횟수입니다.
Decryptions	수신된 암호화 IPsec 패킷에서 성공적으로 수행된 암호 해독 횟수입니다.
Decryption failures	수신된 암호화 IPsec 패킷에서 감지된 암호 해독 실패 횟수입니다.
Decapsulated fragments needing reassembly	다시 어셈블할 IP 조각이 포함된 암호 해독 IPsec 패킷의 수입니다.
Outbound	이 섹션은 IPsec 트래픽을 통해 전송할 아웃바운드 일반 텍스트 트래픽과 관계가 있습니다.
Bytes	암호화하여 IPsec 터널을 통해 전송할 일반 텍스트 트래픽의 바이트 수입니다.
Uncompressed bytes	암호화하여 IPsec 터널을 통해 전송할 압축되지 않은 일반 텍스트 트래픽의 바이트 수입니다. 압축이 활성화되지 않은 경우에는 이 바이트 수가 이전 바이트 수와 항상 같아야 합니다.
Packets	암호화하여 IPsec 터널을 통해 전송할 일반 패킷의 수입니다.
Dropped packets	오류 때문에 끊어였으며 암호화하여 IPsec 터널을 통해 전송할 일반 텍스트 패킷의 수입니다.
Authentications	IPsec 터널을 통해 전송할 패킷에서 수행된 인증 횟수입니다.
Authentication failures	IPsec 터널을 통해 전송할 패킷에서 감지된 인증 실패 횟수입니다.
Encryptions	IPsec 터널을 통해 전송할 패킷에서 수행된 암호화 횟수입니다.
Encryption failures	IPsec 터널을 통해 전송할 패킷에서 감지된 암호화 실패 횟수입니다.
Fragmentation successes	아웃바운드 IPsec 패킷 전송 작업의 일부로 수행된 조각화 작업 횟수입니다.
Pre-fragmentation successes	아웃바운드 IPsec 패킷 전송 작업의 일부로 수행된 사전 조각화 작업 횟수입니다. 사전 조각화는 일반 텍스트 패킷이 암호화되어 하나 이상의 IPsec패킷으로 캡슐화되기 전에 발생합니다.

출력(계속됨)	설명(계속됨)
Post-fragmentation successes	아웃바운드 IPsec 패킷 전송 작업의 일부로 수행된 사전 조각화 작업 횟수입니다. 사후 조각화는 일반 텍스트 패킷이 암호화되어 IPsec 패킷으로 캡슐화된 후에 발생하며, 그 결과로 여러 IP 조각이 생깁니다. 암호 해독하려면 이러한 조각을 다시 어셈블해야 합니다.
Fragmentation failures	아웃바운드 IPsec 패킷 변형 중에 발생한 조각화 실패 횟수입니다.
Pre-fragmentation failures	아웃바운드 IPsec 패킷 변형 중에 발생한 사전 조각화 실패 횟수입니다. 사전 조각화는 일반 텍스트 패킷이 암호화되어 하나 이상의 IPsec패킷으로 캡슐화되기 전에 발생합니다.
Post-fragmentation failure	아웃바운드 IPsec 패킷 변형 중에 발생한 사후 조각화 실패 횟수입니다. 사후 조각화는 일반 텍스트 패킷이 암호화되어 IPsec 패킷으로 캡슐화된 후에 발생하며, 그 결과로 여러 IP 조각이 생깁니다. 암호 해독하려면 이러한 조각을 다시 어셈블해야 합니다.
Fragments created	IPsec 변형의 일부로 생성된 조각의 수입니다.
PMTUs sent	IPsec 시스템에서 보낸 경로 MTU 메시지의 수입니다. IPsec에서는 너무 커서 캡슐화 후에 IPsec 터널을 통해 전송할 수 없는 패킷을 보내는 내부 호스트에 PMTU 메시지를 보냅니다. PMTU 메시지는 IPsec 터널을 통해 전송할 수 있도록 호스트에 MTU를 낮추고 더 작은 패킷을 보내라는 요청입니다.
PMTUs recvd	IPsec 시스템에서 받은 경로 MTU 메시지의 수입니다. 터널을 통해 보내는 패킷이 너무 커서 해당 네트워크 요소를 우회할 수 없는 경우 IPsec이 다운스트림 네트워크 요소로부터 경로 MTU 메시지를 수신합니다. 경로 MTU 메시지를 받으면 IPsec은 일반적으로 터널 MTU를 낮춥니다.
Protocol failures	수신된 IPsec 패킷 중 형식이 잘못된 패킷의 수입니다.
Missing SA failures	요청된 IPsec 작업 중 지정된 IPsec 보안 연계가 없는 IPsec 작업의 수입니다.
System capacity failures	IPsec 시스템 용량이 데이터 속도를 지원할 만큼 높지 않아서 완료할 수 없는 IPsec 작업의 수입니다.

글로벌 컨피그레이션 모드에서 입력된 다음 예에서는 IPsec 통계를 표시합니다.

```
> show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
```

명령	설명
clear ipsec sa	지정된 파라미터를 기반으로 IPsec SA 또는 카운터를 지웁니다.
show ipsec sa	지정된 파라미터를 기반으로 IPsec SA를 표시합니다.
show ipsec sa summary	IPsec SA 요약을 표시합니다.

show ipv6 access-list

이 명령은 Firepower Threat Defense에서 지원하지 않는 기능을 위한 것입니다. IPv6 액세스 제어는 표준 액세스 제어 정책에 통합됩니다. 관리자에서 정책을 보거나 다음 명령을 사용합니다.

- **show access-list**
- **show access-control-config**

show ipv6 dhcprelay binding

릴레이 에이전트가 생성한 릴레이 바인딩 항목을 표시하려면 **show ipv6 dhcprelay binding** 명령을 사용합니다.

show ipv6 dhcprelay binding

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 dhcprelay binding** 명령의 샘플 출력입니다.

```
> show ipv6 dhcprelay binding
1 in use, 2 most used

Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds

Above binding is created for client with link local address of fe80::204:23ff:febb:b094 on
the inside interface using DHCPv6 id of 000100010f9a59d1000423bbb094, and will timeout in
60 seconds.

There will be limit of 1000 bindings for each context.
```

명령	설명
show ipv6 dhcprelay statistics	IPv6 DHCP 릴레이 에이전트 정보를 표시합니다.

show ipv6 dhcprelay statistics

IPv6 DHCP 릴레이 에이전트 통계를 표시하려면 **show ipv6 dhcprelay statistics** 명령을 사용합니다.

show ipv6 dhcprelay statistics

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 dhcprelay statistics** 명령의 샘플 출력입니다.

```
> show ipv6 dhcprelay statistics
Relay Messages:
  SOLICIT                                   1
  ADVERTISE                                 2
  REQUEST                                   1
  CONFIRM                                   1
  RENEW                                   496
  REBIND                                    0
  REPLY                                   498
  RELEASE                                   0
  DECLINE                                   0
  RECONFIGURE                               0
  INFORMATION-REQUEST                       0
  RELAY-FORWARD                           499
  RELAY-REPLY                             500

Relay Errors:
  Malformed message:                        0
  Block allocation/duplication failures:    0
  Hop count limit exceeded:                 0
  Forward binding creation failures:        0
  Reply binding lookup failures:            0
  No output route:                          0
  Conflict relay server route:              0
  Failed to add server NP rule:             0
  Unit or context is not active:            0

Total Relay Bindings Created:             498
```

명령	설명
show ipv6 dhcprelay binding	릴레이 에이전트가 생성한 릴레이 바인딩 항목을 표시합니다.

show ipv6 general-prefix

IPv6 일반 접두사를 표시하려면 **show ipv6 general-prefix** 명령을 사용합니다.

show ipv6 general-prefix

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

IPv6 일반 접두사에 대한 정보를 확인하려면 **show ipv6 general-prefix** 명령을 사용합니다.

다음은 **show ipv6 general-prefix** 명령의 샘플 출력입니다.

```
> show ipv6 general-prefix
IPv6 Prefix my-prefix, acquired via 6to4
2002:B0B:B0B::/48
 Loopback42 (Address command)
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 icmp

모든 인터페이스에 구성된 ICMPv6 액세스 규칙을 표시하려면 **show ipv6 icmp** 명령을 사용합니다.

show ipv6 icmp

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

ICMPv6 규칙은 디바이스 인터페이스에 대한 ICMPv6 트래픽을 제어합니다. 이 규칙은 through-the-box 트래픽은 제어하지 않습니다. 이 규칙을 사용하여 어떤 주소에서 인터페이스(예: 핑)에 ICMPv6 명령을 전송할 수 있는지와 어떤 ICMPv6 명령 유형이 전송될 수 있는지 제어할 수 있습니다. 이 규칙을 보려면 **show ipv6 icmp** 명령을 사용합니다.

다음은 **show ipv6 icmp** 명령의 샘플 출력입니다.

```
> show ipv6 icmp
ipv6 icmp permit any inside
```

show ipv6 interface

IPv6에 대해 구성된 인터페이스의 상태를 표시하려면 **show ipv6 interface** 명령을 사용합니다.

show ipv6 interface [**brief**] [*if_name* [**prefix**]]

brief	각 인터페이스의 IPv6 상태 및 컨피그레이션에 대한 간략한 요약을 표시합니다.
if_name	(선택 사항) 내부 또는 외부 인터페이스 이름입니다. 지정된 인터페이스에 대해서만 상태 및 컨피그레이션이 표시됩니다. 모든 인터페이스를 표시하는 경우, 시스템 통신에 사용된 내부 인터페이스에 대한 정보도 참조하십시오. 내부 인터페이스는 사용자가 구성할 수 없으며, 정보는 디버깅용으로만 제공됩니다.
prefix	(선택 사항) 로컬 IPv6 접두사 풀에서 생성된 접두사입니다. 접두사는 IPv6 주소의 네트워크 부분입니다.

모든 IPv6 인터페이스를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show ipv6 interface 명령은 IPv6에 특정하다는 점을 제외하고는 **show interface** 명령과 유사한 출력을 제공합니다. 인터페이스 하드웨어를 사용할 수 있는 경우 인터페이스가 up으로 표시됩니다. 인터페이스에서 양방향 통신을 제공할 수 있는 경우 회선 프로토콜이 up으로 표시됩니다.

인터페이스 이름을 지정하지 않으면 모든 IPv6 인터페이스에 대한 정보가 표시됩니다. 인터페이스 이름을 지정하면 지정된 인터페이스에 대한 정보가 표시됩니다.

다음은 **show ipv6 interface** 명령의 샘플 출력입니다.

```
> show ipv6 interface outside
```

```
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

다음은 **show ipv6 interface** 명령의 샘플 출력입니다(**brief** 키워드와 함께 입력된 경우).

```
> show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

다음은 **show ipv6 interface** 명령의 샘플 출력입니다. 주소에서 접두사를 생성한 인터페이스의 특성을 표시합니다.

```
> show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 local pool

IPv6 주소 풀 정보를 표시하려면 **show ipv6 local pool** 명령을 사용합니다.

show ipv6 local pool [*poolname*]

poolname	(선택 사항) 로컬 주소 풀의 사용자 정의 이름입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

풀 이름을 생략할 경우, 이 명령은 모든 정의된 주소 풀과 이 풀에 속하는 IP 주소의 일반 목록을 표시합니다. 풀 이름을 지정하는 경우, 명령은 해당 풀에 대한 세부 정보를 표시합니다.

다음은 **show ipv6 local pool** 명령의 샘플 출력입니다.

```
> show ipv6 local pool
Pool Prefix Free In use
mypool 2001:0DB8::/29 65516 20
>
> show ipv6 local pool mypool
Prefix is 1234::/48 assign /64 prefix
20 entries in use, 65516 available, 0 rejected
0 entries cached, 1000 maximum
User Prefix Interface
user1-72b 1234::/64 Vi1.21
user1-72b 1234:0:0:1::/64 Vi1.22
user1-72b 1234:0:0:2::/64 Vi1.23
user1-72b 1234:0:0:3::/64 Vi1.24
user1-72b 1234:0:0:4::/64 Vi1.25
user1-72b 1234:0:0:5::/64 Vi1.26
user1-72b 1234:0:0:6::/64 Vi1.27
user1-72b 1234:0:0:7::/64 Vi1.28
user1-72b 1234:0:0:8::/64 Vi1.29
user1-72b 1234:0:0:9::/64 Vi1.30
user1-72b 1234:0:0:A::/64 Vi1.31
user1-72b 1234:0:0:B::/64 Vi1.32
user1-72b 1234:0:0:C::/64 Vi1.33
user1-72b 1234:0:0:D::/64 Vi1.34
user1-72b 1234:0:0:E::/64 Vi1.35
user1-72b 1234:0:0:F::/64 Vi1.36
user1-72b 1234:0:0:10::/64 Vi1.37
user1-72b 1234:0:0:11::/64 Vi1.38
```

```
user1-72b 1234:0:0:12::/64 Vi1.39
user1-72b 1234:0:0:13::/64 Vi1.40
```

show ipv6 mld traffic

MLD(Multicast Listener Discovery) 트래픽 카운터 정보를 표시하려면 **show ipv6 mld traffic** 명령을 사용합니다.

show ipv6 mld traffic

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show ipv6 mld traffic 명령을 사용하면 필요한 개수의 MLD 메시지가 수신 및 전송되었는지 확인할 수 있습니다. **show ipv6 mld traffic** 명령에서 제공되는 정보는 다음과 같습니다.

- Elapsed time since counters cleared - 카운터가 지워진 후 경과한 시간입니다.
- Valid MLD Packets - 수신 및 전송된 유효한 MLD 패킷 수입니다.
- Queries - 수신 및 전송된 유효한 쿼리 수입니다.
- Reports - 수신 및 전송된 유효한 보고서 수입니다.
- Leaves - 수신 및 전송된 유효한 리프 수입니다.
- Mtrace packets - 수신 및 전송된 멀티캐스트 추적 패킷 수입니다.
- Errors - 발생한 오류의 유형 및 개수입니다.

다음은 **show ipv6 mld traffic** 명령의 샘플 출력입니다.

```
> show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
                   Received          Sent
Valid MLD Packets  1                 3
Queries            1                 0
Reports            0                 3
Leaves             0                 0
Mtrace packets     0                 0
Errors:
Malformed Packets  0
Martian source     0
```

```
Non link-local source 0
Hop limit is not equal to 1 0
```

명령	설명
clear ipv6 mld traffic	모든 MLD 트래픽 카운터를 재설정합니다.

show ipv6 neighbor

IPv6 인접 검색 캐시 정보를 표시하려면 **show ipv6 neighbor** 명령을 사용합니다.

show ipv6 neighbor [*if_name* | *address*]

address	(선택 사항) 제공된 IPv6 주소에 대한 인접 검색 캐시 정보만 표시합니다.
if_name	(선택 사항) 제공된 인터페이스 이름에 대한 캐시 정보를 표시합니다. 모든 인터페이스를 표시하는 경우, 시스템 통신에 사용된 내부 인터페이스에 대한 정보도 참조하십시오. 내부 인터페이스는 사용자가 구성할 수 없으며, 정보는 디버깅용으로만 제공됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show ipv6 neighbor 명령에서 제공되는 정보는 다음과 같습니다.

- IPv6 Address - 인접 항목 또는 인터페이스의 IPv6 주소입니다.
- Age - 주소가 연결할 수 있는 것으로 확인된 이후에 경과한 시간(분)입니다. 하이픈(-)은 정적 항목을 나타냅니다.
- Link-layer Addr - MAC 주소입니다. 주소를 알 수 없는 경우 하이픈(-)이 표시됩니다.
- State - 인접 캐시 항목의 상태입니다.

참고 연결 가능성 감지는 IPv6 인접 검색 캐시의 정적 항목에는 적용되지 않습니다. 따라서 INCMP(불완전) 및 REACH(연결 가능) 상태의 설명이 동적 캐시 항목과 정적 항목에 대해 서로 다릅니다.

다음은 IPv6 인접 검색 캐시의 동적 항목에 대한 가능한 상태입니다.

  - INCMP - (불완전) 항목에 대한 주소 확인을 수행하는 중입니다. 인접 요청 메시지가 대상의 요청된 노드 멀티캐스트 주소로 전송되었지만 해당 인접 알림 메시지가 아직 수신되지 않았습니다.

- REACH - (연결 가능) 지난 ReachableTime 밀리초 이내에 인접 항목의 정방향 경로가 올바르게 작동한다는 긍정적인 확인이 수신되었습니다. REACH 상태에 있는 동안 디바이스는 패킷이 전송될 때 특별한 작업을 수행하지 않습니다.
- STALE - 정방향 경로가 올바르게 작동한다는 긍정적인 확인이 마지막으로 수신된 후 ReachableTime 밀리초보다 많은 시간이 경과했습니다. STALE 상태에 있는 동안 디바이스는 패킷이 전송될 때까지 아무 작업도 수행하지 않습니다.
- DELAY - 정방향 경로가 올바르게 작동한다는 긍정적인 확인이 마지막으로 수신된 후 ReachableTime 밀리초보다 많은 시간이 경과했습니다. 패킷이 지난 DELAY_FIRST_PROBE_TIME 초 이내에 전송되었습니다. DELAY 상태로 전환된 후 DELAY_FIRST_PROBE_TIME 초 이내에 연결 가능성 확인이 수신되지 않으면 인접 요청 메시지를 보내고 상태를 PROBE로 변경하십시오.
- PROBE - 연결 가능성 확인이 수신될 때까지 RetransTimer 밀리초마다 인접 요청 메시지를 다시 보내 연결 가능성 확인을 적극적으로 요청합니다.
- ???? - 알 수 없는 상태입니다.

다음은 IPv6 인접 검색 캐시의 정적 항목에 대한 가능한 상태입니다.

- INCMP - (불완전) 이 항목에 대한 인터페이스의 작동이 중지되었습니다.
- REACH - (연결 가능) 이 항목에 대한 인터페이스가 작동합니다.

• 인터페이스

주소에 연결할 수 있는 인터페이스입니다.

다음은 인터페이스와 함께 입력한 경우 **show ipv6 neighbor** 명령의 샘플 출력입니다.

```
> show ipv6 neighbor inside
IPv6 Address                             Age Link-layer Addr State Interface
2000:0:0:4::2                              0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                   0 0003.a0d6.141e  REACH inside
3001:1::45a                                - 0002.7d1a.9472  REACH inside
```

다음은 IPv6 주소와 함께 입력한 경우 **show ipv6 neighbor** 명령의 샘플 출력입니다.

```
> show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                             Age Link-layer Addr State Interface
2000:0:0:4::2                              0 0003.a0d6.141e  REACH inside
```

명령	설명
clear ipv6 neighbors	IPv6 인접 검색 캐시에서 정적 항목을 제외한 모든 항목을 삭제합니다.

show ipv6 ospf

OSPFv3 라우팅 프로세스에 대한 일반 정보를 표시하려면 **show ipv6 ospf** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*]

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPFv3 라우팅 프로세스를 사용하는 경우 관리자에 의해 할당되는 번호입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 ospf** 명령의 샘플 출력입니다.

```
> show ipv6 ospf
Routing Process "ospfv3 1" with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
```

명령	설명
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.
show ipv6 ospf database	특정 라우터의 OSPFv3 데이터베이스와 관련된 정보 목록을 표시합니다.

show ipv6 ospf border-routers

ABR(area border router) 및 ASBR(autonomous system boundary router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시하려면 **show ipv6 ospf border-routers** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **border-routers**

process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPFv3 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show ipv6 ospf border-routers 명령은 다음 설정을 나열합니다.

- 영역 간 경로
- 영역 내 경로
- IPv6 주소
- 인터페이스 유형
- 영역 ID
- SPF 번호

다음은 **show ipv6 ospf border-routers** 명령의 샘플 출력입니다.

```
> show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
```

```
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf database	특정 라우터의 OSPFv3 데이터베이스와 관련된 정보 목록을 표시합니다.

show ipv6 ospf database

특정 라우터의 OSPFv3 데이터베이스와 관련된 정보 목록을 표시하려면 **show ipv6 ospf database** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **database** [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]

adv-router*router-id*	(선택 사항) 알리는 라우터의 모든 LSA를 표시합니다. 라우터 ID는 RFC 2740에 문서화된 형식이어야 합니다. 즉, 콜론으로 구분된 16비트 값을 사용하여 16진수로 주소를 지정해야 합니다.
area	(선택 사항) 영역 LSA에 대한 정보만 표시합니다.
area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
as	(선택 사항) 알 수 없는 AS(자동 시스템) LSA를 필터링합니다.
database-summary	(선택 사항) 데이터베이스의 각 영역에 대해 존재하는 유형별 LSA 수와 총 LSA 수를 표시합니다.
destination-router-id	(선택 사항) 지정된 대상 라우터에 대한 정보만 표시합니다.
external	(선택 사항) 외부 LSA에 대한 정보만 표시합니다.
interface	(선택 사항) 인터페이스 상황으로 필터링된 LSA에 대한 정보를 표시합니다.
interface-name	(선택 사항) LSA 인터페이스 이름을 지정합니다.
internal	(선택 사항) 내부 LSA에 대한 정보만 표시합니다.
inter-area prefix	(선택 사항) inter-area 접두사를 기반으로 하는 LSA에 대한 정보만 표시합니다.
inter-area router	(선택 사항) 영역 내 라우터 LSA를 기반으로 하는 LSA에 대한 정보만 표시합니다.
링크	(선택 사항) 링크 LSA에 대한 정보를 표시합니다. **unknown** 키워드 뒤에 사용된 경우 **link** 키워드는 링크 범위 LSA를 필터링합니다.
link-state-id	(선택 사항) LSA를 구분하는 데 사용되는 정수를 지정합니다. 네트워크 및 링크 LSA에서 링크 상태 ID는 인터페이스 인덱스와 일치합니다.

네트워크	(선택 사항) 네트워크 LSA에 대한 정보를 표시합니다.
nssa-external	(선택 사항) NSSA(Not So Stubby Area) 외부 LSA에 대한 정보만 표시합니다.
prefix*ipv6-prefix*	(선택 사항) 네이버의 링크-로컬 IPv6 주소를 표시합니다. IPv6 접두사는 RFC 2373에 문서화된 형식이어야 합니다. 즉, 콜론으로 구분된 16비트 값을 사용하여 16진수로 주소를 지정해야 합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.
ref-lsa	(선택 사항) 접두사 LSA 유형을 추가로 필터링합니다.
라우터	(선택 사항) 라우터 LSA에 대한 정보를 표시합니다.
self-originate	(선택 사항) 로컬 라우터에서 자체 시작되는 LSA만 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

다양한 형식의 명령에서 서로 다른 OSPFv3 LSA에 대한 정보를 제공합니다.

다음은 **show ipv6 ospf database** 명령의 샘플 출력입니다.

```
> show ipv6 ospf database

            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)

                Router Link States (Area 0)

ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B

            Inter Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
```

```
172.16.6.6         82          0x80000001  FEC0::/32

            Inter Area Router Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3

            Link (Type-8) Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0

            Intra Area Prefix Link States (Area 0)

ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf events

OSPFv3 내부 이벤트 정보를 표시하려면 **show ipv6 ospf events** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **events**

process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 ospf events** 명령의 샘플 출력입니다.

```
> show ipv6 ospf events

OSPFv3 Router with ID (10.1.3.2) (Process ID 10)

   1 Jul 9  18:49:34.071: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
   2 Jul 9  18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2,

Seq# 80000008, Age 1, Area 10
   3 Jul 9  18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004,
Age    0, Area 10
   4 Jul 9  18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005,

Age 0, Area 10
   5 Jul 9  18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
   6 Jul 9  18:41:18.902: Starting External processing in area 10
   7 Jul 9  18:41:18.902: Starting External processing
   8 Jul 9  18:41:18.902: Starting Inter-Area SPF in area 10
   9 Jul 9  18:41:18.902: Generic:  post_spf_intra  0x0
  10 Jul 9  18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
  11 Jul 9  18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
  12 Jul 9  18:41:18.902: Starting Intra-Area SPF in Area 10
  13 Jul 9  18:41:18.903: Starting SPF, wait-interval 5000ms
  14 Jul 9  18:41:16.403: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
  15 Jul 9  18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0,
Adv-Rtr   50.100.168.192
```

```
  16 Jul 9  18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,
Seq# 80000003, Age 1, Area 10
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf flood-list

인터페이스로 플러딩되기를 기다리는 OSPFv3 LSA 목록을 표시하려면 **show ipv6 ospf flood-list** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **flood-list** *interface-type interface-number*

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
interface-number	LSA가 플러딩되는 인터페이스 번호를 지정합니다.
interface-type	LSA가 플러딩되는 인터페이스 유형을 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPFv3 라우팅 프로세스가 사용 설정된 경우 관리자에 의해 할당되는 번호입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령을 사용하여 OSPFv3 패킷 속도 정보를 표시할 수 있습니다.

다음은 **show ipv6 ospf flood-list** 명령의 샘플 출력입니다.

```
> show ipv6 ospf flood-list

OSPFv3 Router with ID (172.16.6.6) (Process ID 1)

 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971

 Interface FastEthernet0/0, Queue length 0
```

```
Interface ATM3/0, Queue length 0
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf graceful-restart

OSPFv3 정상 재시작에 대한 정보를 표시하려면 **show ipv6 ospf graceful-restart** 명령을 사용합니다.

show ipv6 ospf graceful-restart

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 ospf graceful-restart** 명령의 샘플 출력입니다.

```
> show ipv6 ospf graceful-restart
Routing Process "ospfv3 10"
  Graceful Restart enabled
    restart-interval limit: 240 sec
    Clustering is not configured in spanned etherchannel mode
  Graceful Restart helper support enabled
    Number of neighbors performing Graceful Restart is 0
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.

show ipv6 ospf interface

OSPFv3 관련 인터페이스 정보를 표시하려면 **show ipv6 ospf interface** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **interface** [*type-number*] [**brief**]

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
brief	(선택 사항) OSPFv3 인터페이스, 상태, 주소 및 마스크, 라우터의 영역에 대한 간략한 개요 정보를 표시합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.
type-number	(선택 사항) 인터페이스 유형 및 번호를 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령을 OSPFv3 인터페이스, 상태, 주소 및 마스크, 라우터의 영역에 대한 개요 정보를 표시할 수 있습니다.

다음은 **show ipv6 ospf interface** 명령의 샘플 출력입니다.

```
> show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
```

```
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf request-list

라우터에서 요청된 모든 LSA 목록을 표시하려면 **show ipv6 ospf request-list** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
interface	(선택 사항) 이 인터페이스의 라우터가 요청한 모든 LSA 목록을 지정합니다.
interface-neighbor	(선택 사항) 이 네이버에서 이 인터페이스의 라우터가 요청한 모든 LSA 목록을 지정합니다.
neighbor	(선택 사항) 이 네이버에서 라우터가 요청한 모든 LSA 목록을 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 ospf request-list** 명령의 샘플 출력입니다.

```
> show ipv6 ospf request-list

            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)

 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600

 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0         192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0         192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0         192.168.255.1   0x800000C5  1      0x008CD1
```

```
2       0.0.0.3         192.168.255.3   0x800000A9  774     0x0058C0
2       0.0.0.2         192.168.255.3   0x800000B7  1       0x003A63
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf retransmission-list

재전송을 대기 중인 모든 LSA 목록을 표시하려면 **show ipv6 ospf retransmission-list** 명령을 사용합니다.

show ipv6 ospf [*process_id*] [*area_id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

area_id	(선택 사항) 지정된 영역에 대한 정보만 표시합니다.
interface	(선택 사항) 이 인터페이스에서 재전송을 대기 중인 모든 LSA 목록을 지정합니다.
interface-neighbor	(선택 사항) 이 네이버에서 이 인터페이스에 대해 재전송을 대기 중인 모든 LSA 목록을 지정합니다.
neighbor	(선택 사항) 이 네이버에 대해 재전송을 대기 중인 모든 LSA 목록을 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 ospf retransmission-list** 명령의 샘플 출력입니다.

```
> show ipv6 ospf retransmission-list

       OSPFv3 Router with ID (192.168.255.2) (Process ID 1)

Neighbor 192.168.255.1, interface Ethernet0/0
Link state retransmission due in 3759 msec, Queue length 1
```

```
Type    LS ID           ADV RTR         Seq NO      Age    Checksum
0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf statistic

SPF가 실행된 횟수, 이유 및 지속 시간 같이 다양한 OSPFv3 통계를 표시하려면 **show ipv6 ospf statistic** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **statistic** [**detail**]

detail	(선택 사항) 트리거 지점을 포함하여 자세한 SPF 정보를 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 ospf statistic** 명령의 샘플 출력입니다.

```
> show ipv6 ospf 10 statistic detail
Area 10: SPF algorithm executed 6 times

SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
              0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)

SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
              0             0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
  50.100.168.192/2(N)
```

show ipv6 ospf summary-prefix

OSPFv3 프로세스 중에 구성된 모든 요약 주소 재배포 정보 목록을 표시하려면 **show ipv6 ospf summary-prefix** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **summary-prefix**

process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 ospf summary-prefix** 명령의 샘플 출력입니다.

```
> show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf timers

OSPFv3 타이머 정보를 표시하려면 **show ipv6 ospf timers** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **timers** [**lsa-group** | **rate-limit**]

lsa-group	(선택 사항) OSPFv3 LSA 그룹 정보를 지정합니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 사용 설정된 경우 관리자에 의해 할당되는 번호입니다.
rate-limit	(선택 사항) OSPFv3 LSA 속도 제한 정보를 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 ospf timers lsa-group** 명령의 샘플 출력입니다.

```
> show ipv6 ospf timers lsa-group

OSPFv3 Router with ID (10.10.13.101) (Process ID 1)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:13
Current time 96532
Index 0 Timestamp 96546
Index 1 Timestamp 96788
Index 2 Timestamp 97048
Index 3 Timestamp 97293
Index 4 Timestamp 97548

Failure Head 0, Last 0 LSA group failure logged

            OSPFv3 Router with ID (10.10.10.102) (Process ID 5709)

Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:22
Current time 96532
Index 0 Timestamp 96555
Index 1 Timestamp 96801
Index 2 Timestamp 97041
Index 3 Timestamp 97287
Index 4 Timestamp 97546

Failure Head 0, Last 0 LSA group failure logged
```

show ipv6 ospf traffic

현재 사용 가능한 인터페이스에 대한 OSPFv3 트래픽 관련 통계를 표시하려면 **show ipv6 ospf traffic** 명령을 사용합니다.

show ipv6 ospf [*process_id*] **traffic** [*interface_name*]

interface_name	(선택 사항) 인터페이스의 이름을 지정합니다. 이 옵션을 사용하여 트래픽을 특정 인터페이스로 분리할 수 있습니다.
process_id	(선택 사항) 로컬로 할당된 내부 ID(임의의 양의 정수일 수 있음)를 지정합니다. 이 ID는 OSPF 라우팅 프로세스가 활성화된 경우 관리자에 의해 할당되는 번호입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 ospf traffic** 명령의 샘플 출력입니다.

```
> show ipv6 ospf 10 traffic inside
Interface inside

Last clearing of interface traffic counters never

OSPFv3 packets received/sent
  Type          Packets               Bytes
  RX Invalid                      0 0
  RX Hello                     1232 53132
  RX DB des                      27 896
  RX LS req                       3 216
  RX LS upd                      28 2436
  RX LS ack                      14 1064
  RX Total                     1304 57744

  TX Failed                       0 0
  TX Hello                      753 32072
  TX DB des                      27 1056
  TX LS req                       2 92
  TX LS upd                       9 1128
```

```
TX LS ack                        15 900
TX Total                        806 35248
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 ospf virtual-links

OSPFv3 가상 링크의 파라미터 및 현재 상태를 표시하려면 **show ipv6 ospf virtual-links** 명령을 사용합니다.

show ipv6 ospf virtual-links

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ipv6 ospf virtual-links** 명령의 샘플 출력입니다.

```
> show ipv6 ospf virtual-links

Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

명령	설명
show ipv6 ospf	OSPFv3 라우팅 프로세스의 모든 IPv6 설정을 표시합니다.
show ipv6 ospf border-routers	ABR(Area Border Router) 및 ASBR(Autonomous System Boundary Router)에 대한 내부 OSPFv3 라우팅 테이블 항목을 표시합니다.

show ipv6 route

IPv6 라우팅 테이블의 내용을 표시하려면 **show ipv6 route** 명령을 사용합니다.

show ipv6 route [**management-only**] [**failover**] [**cluster**] [**interface** *name*] [**ospf**] [**summary**]

managment-only	IPv6 관리 라우팅 테이블에서의 경로를 표시합니다.
클러스터	(선택 사항) 클러스터의 IPv6 라우팅 테이블 시퀀스 번호, IPv6 재수렴 타이머 상태 및 IPv6 라우팅 항목 시퀀스 번호를 표시합니다.
페일오버	(선택 사항) IPv6 라우팅 테이블 시퀀스 번호, IPv6 재수렴 타이머 상태 및 IPv6 라우팅 항목 시퀀스 번호를 표시합니다.
interface*name*	(선택 사항) IPv6 인터페이스 관련 경로를 표시합니다.
ospf	(선택 사항) OSPFv3 경로를 표시합니다.
요약	(선택 사항) IPv6 경로 요약을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show ipv6 route 명령은 정보가 IPv6에 특정하다는 점을 제외하고는 **show route** 명령과 유사한 출력을 제공합니다.

IPv6 라우팅 테이블에 표시되는 정보는 다음과 같습니다.

- Codes - 경로를 파생한 프로토콜을 나타냅니다. 값은 다음과 같습니다.
  - C - 연결됨
  - L - 로컬
  - S - 정적
  - R - RIP 파생됨
  - B - BGP 파생됨

  - I1—ISIS L1 - 통합 IS-IS 수준 1 파생됨
  - I2—ISIS L2 - 통합 IS-IS 수준 2 파생됨
  - IA—ISIS interarea - 통합 IS-IS 영역 내 파생됨

- fe80::/10 - 원격 네트워크의 IPv6 접두사를 나타냅니다.
- [0/0] - 대괄호 안의 첫 번째 숫자는 정보 소스의 관리 영역이고, 두 번째 숫자는 경로에 대한 메트릭입니다.
- via :: - 원격 네트워크에 대한 다음 라우터의 주소를 지정합니다.
- inside - 지정된 네트워크의 다음 라우터에 연결할 수 있는 인터페이스를 지정합니다.

다음은 **show ipv6 route** 명령의 샘플 출력입니다.

```
> show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

다음은 **show ipv6 route failover** 명령의 샘플 출력입니다.

```
> show ipv6 route failover

IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
           ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired

O   2009::1/128 [110/10]
     via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
     via fe80::217:94ff:fe85:4401, inside seq 0
S   4001::1/128 [0/0]
     via 4001::2, inside seq 0
C   7001::1/128 [0/0]
     via ::, outside seq 0
L   fe80::/10 [0/0]
     via ::, inside seq 0
```

```
     via ::, outside seq 0
L   ff00::/8 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
```

다음은 마스터 유닛에서 실행된 **how ipv6 route cluster** 명령의 샘플 출력입니다.

```
> show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 2
IPv6 Reconvergence timer expired

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

다음은 역할 변경 중 슬레이브 유닛에서 실행된 **show ipv6 route cluster** 명령의 샘플 출력입니다.

```
> cluster master
INFO: Wait for existing master to quit. Use "show cluster info"
to check status. Use "cluster remove unit <name>" to force
master unit out of the cluster if for some reason it refuses
to quit within reasonable time
> show ipv6 route cluster

IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 3
IPv6 Reconvergence timer expires in 61 secs

OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

명령	설명
debug ipv6 route	IPv6 라우팅 테이블 업데이트 및 경로 캐시 업데이트에 대한 디버깅 메시지를 표시합니다.
ipv6 route	IPv6 라우팅 테이블에 정적 항목을 추가합니다.

show ipv6 routers

연결된(on-link) 라우터에서 받은 IPv6 라우터 알림 정보를 표시하려면 **show ipv6 routers** 명령을 사용합니다.

show ipv6 routers [*if_name*]

if_name	(선택 사항) 정보를 표시할 내부 또는 외부 인터페이스 이름입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

인터페이스 이름을 지정하지 않으면 모든 IPv6 인터페이스에 대한 정보가 표시됩니다. 인터페이스 이름을 지정하면 지정된 인터페이스에 대한 정보가 표시됩니다.

다음은 인터페이스 이름 없이 입력한 경우 **show ipv6 routers** 명령의 샘플 출력입니다.

```
> show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

명령	설명
ipv6 route	IPv6 라우팅 테이블에 고정 항목을 추가합니다.

show ipv6 traffic

IPv6 트래픽에 대한 통계를 표시하려면 **show ipv6 traffic** 명령을 사용합니다.

show ipv6 traffic

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

트래픽 카운터를 지우려면 **clear ipv6 traffic** 명령을 사용합니다.

다음은 **show ipv6 traffic** 명령의 샘플 출력입니다.

```
> show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output
```

```
TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

명령	설명
clear ipv6 traffic	IPv6 트래픽 카운터를 지웁니다.

show isakmp sa

IKE 런타임 SA 데이터베이스를 표시하려면 **show isakmp sa** 명령을 사용합니다.

show isakmp sa [**detail**]

detail	SA 데이터베이스에 대한 자세한 출력을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 SA 데이터베이스에 대한 세부 정보를 표시합니다.

```
> show isakmp sa detail

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
```

명령	설명
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 ISAKMP 구성을 표시합니다.

show isakmp stats

런타임 통계를 표시하려면 **show isakmp stats** 명령을 사용합니다.

show isakmp stats

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

자용 가이드라인

각 카운터는 연결된 cikePhase1GW 카운터에 매핑됩니다. 각 카운터에 대한 자세한 내용은 CISCO-IPSEC-FLOW-MONITOR-MIB.my를 참조하십시오.

- Active/Standby Tunnels - cikePhase1GWActiveTunnels
- Previous Tunnels - cikePhase1GWPreviousTunnels
- In Octets - cikePhase1GWInOctets
- In Packets - cikePhase1GWInPkts
- In Drop Packets - cikePhase1GWInDropPkts
- In Notifys - cikePhase1GWInNotifys
- In P2 Exchanges - cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids - cikePhase1GWInP2ExchgInvalids
- In P2 Exchange Rejects - cikePhase1GWInP2ExchgRejects
- In P2 Sa Delete Requests - cikePhase1GWInP2SaDelRequests
- Out Octets - cikePhase1GWOutOctets
- Out Packets - cikePhase1GWOutPkts
- Out Drop Packets - cikePhase1GWOutDropPkts
- Out Notifys - cikePhase1GWOutNotifys
- Out P2 Exchanges - cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids - cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects - cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests - cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels - cikePhase1GWInitTunnels
- Initiator Fails - cikePhase1GWInitTunnelFails

- Responder Fails - cikePhase1GWRespTunnelFails
- System Capacity Fails - cikePhase1GWSysCapFails
- Auth Fails - cikePhase1GWAuthFails
- Decrypt Fails - cikePhase1GWDecryptFails
- Hash Valid Fails - cikePhase1GWHashValidFails
- No Sa Fails - cikePhase1GWNoSaFails

다음 예는 ISAKMP 통계를 표시합니다.

```
> show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
```

명령	설명
clear isakmp sa	IKE 런타임 SA 데이터베이스를 지웁니다.
show running-config isakmp	모든 활성 ISAKMP 컨피그레이션을 표시합니다.

show j - show o

show jumbo-frame reservation

점보 프레임이 모든 인터페이스에 대해 사용 설정되어 있는지 여부를 보려면 **show jumbo-frame reservation** 명령을 사용합니다.

show jumbo-frame reservation

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

점보 프레임 예약은 1500개 이상의 인터페이스에 대한 MTU를 증가시킬 경우 항상 사용 설정됩니다. 이 기능은 모든 MTU를 1500 이하로 되돌릴 경우 자동으로 사용 해제됩니다.

다음은 점보 프레임 지원이 사용 설정된 경우의 **show jumbo-frame reservation** 명령의 샘플 출력입니다.

```
> show jumbo-frame-reservation
Jumbo Frame Support is currently enabled
```

show kernel

Linux brctl 유틸리티에서 제공하는 디버깅에 사용할 수 있는 정보를 표시하려면 **show kernel** 명령을 사용합니다.

show kernel {**process** | **bridge** [**mac-address** *bridge_name*] | **cgroup-controller** [**cpu** | **cpuset** | **memory**] [**detail**] | **ifconfig** | **module**}

bridge [**mac-address***bridge_name*]	Linux 탭 브리지, 해당 멤버 포트 및 디버깅에 사용할 수 있는 각 포트에서 학습된 MAC 주소(원격 MAC 주소 포함)를 표시합니다. 특정 브리지에 대한 MAC 주소 세부 정보를 확인하기 위해 **mac-address** 키워드를 사용할 수 있습니다. br0 같이 사용 가능한 브리지 이름을 확인하려면 키워드 없이 이 명령을 사용합니다.
cgroup-controller [**cpu** | **cpuset** | **memory**] [**detail**]	cgroup-controller 통계를 표시합니다. **cpu**, **cpuset** 및 **memory** 키워드는 요구 사항에 따라 cgroup-controller 통계를 필터링할 수 있습니다. 추가 정보를 보려면 detail 키워드를 사용합니다.
ifconfig	탭 및 브리지 인터페이스 통계를 표시합니다.
모듈	설치되고 실행되는 모듈을 표시합니다.
프로세스	디바이스에서 실행되는 활성 커널 프로세스의 현재 상태를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 커널에서 실행되는 여러 프로세스에 대한 통계를 표시합니다.

다음 예에서는 **show kernel process** 명령의 출력을 표시합니다.

```
> show kernel process
PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
```

```
  4     1  20 -5          0        0 3725736671    S         0 khelper
  5     1  20 -5          0        0 3725736671    S         0 kthread
  7     5  10 -5          0        0 3725736671    S         0 kblockd/0
  8     5  20 -5          0        0 3726794334    S         0 kseriod
 66     5  20  0          0        0 3725811768    S         0 pdflush
 67     5  15  0          0        0 3725811768    S         0 pdflush
 68     1  15  0          0        0 3725824451    S         2 kswapd0
 69     5  20 -5          0        0 3725736671    S         0 aio/0
171     1  16  0     991232       80 3725684979    S         0 init
172   171  19  0     983040      268 3725684979    S         0 rcS
201   172  21  0    1351680      344 3725712932    S         0 lina_monitor
202   201  16  0 1017602048   899932 3725716348    S       212 lina
203   202  16  0 1017602048   899932          0    S         0 lina
204   203  15  0 1017602048   899932          0    S         0 lina
205   203  15  0 1017602048   899932 3725712932    S         6 lina
206   203  25  0 1017602048   899932          0    R 13069390 lina
>
```

다음 표는 각 필드에 대해 설명합니다.

표 ***39: show kernel process*** 필드

필드	설명
PID	프로세스 ID입니다.
PPID	상위 프로세스 ID입니다.
PRI	프로세스의 우선순위입니다.
NI	우선순위 계산에 사용되는 nice 값입니다. 값 범위는 19(nicest)~19(not nice to others)입니다.
VSIZE	가상 메모리 크기(바이트)입니다.
RSS	프로세스의 상주 집합 크기(킬로바이트)입니다.
WCHAN	프로세스가 대기하는 채널입니다.
STAT	프로세스의 상태입니다. • R - 실행 중 • S - 중단 가능한 상태로 대기 중 • D - 중단할 수 없는 디스크 절전 상태로 대기 중 • Z - 좀비 • T - 추적되거나 중지됨(신호에서) • P - 페이징
RUNTIME	프로세스가 사용자 모드 및 커널 모드에서 예약된 지피(Jiffy) 수입니다. 런타임은 utime과 stime의 합계입니다.

필드	설명
명령	프로세스 이름입니다.

다음 예에서는 **show kernel module** 명령의 출력을 표시합니다.

```
> show kernel module

Module                  Size  Used by    Tainted: P
cpp_base              861808  2
kvm_intel              44104  8
kvm                   174304  1 kvm_intel
msrif                   4180  0
tscsync                 3852  0
```

다음 예에서는 **show kernel ifconfig** 명령의 출력을 표시합니다.

```
> show kernel ifconfig

br0       Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1708 (1.6 KiB)  TX bytes:0 (0.0 B)

br1       Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap0      Link encap:Ethernet  HWaddr 6A:0C:48:32:FE:F4
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:13 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:10320 (10.0 KiB)  TX bytes:12452 (12.1 KiB)

tap1      Link encap:Ethernet  HWaddr 8E:E7:61:CF:E9:BD
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:19368 (18.9 KiB)  TX bytes:14638 (14.2 KiB)

tap2      Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap3      Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:187 errors:0 dropped:0 overruns:0 frame:0
```

```
          TX packets:256 errors:0 dropped:3 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:14638 (14.2 KiB)  TX bytes:19202 (18.7 KiB)

tap4      Link encap:Ethernet  HWaddr 6A:5C:60:BC:9C:ED
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

다음 예에서는 **show kernel bridge** 명령의 출력을 표시합니다.

```
> show kernel bridge

bridge name     bridge id               STP enabled     interfaces
br0             8000.000000040001       no              tap1
                                                        tap3
br1             8000.84b261b192bd       no              tap2
                                                        tap4
                                                        tap5
```

다음 예에서는 **show kernel bridge mac-address** 명령의 출력을 표시합니다.

```
> show kernel bridge mac-address br1

port no    mac addr       is local?   ageing timer
 1    00:21:d8:cb:dc:f7    no          12.93
 3    00:22:bd:d8:7d:da    no          12.93
 2    26:d2:9f:51:a4:90    yes          0.00
 1    4e:a4:e0:73:1f:ab    yes          0.00
 3    52:04:38:3d:79:c0    yes          0.00
```

명령	설명
show module	디바이스에 설치된 모듈에 대한 정보를 표시합니다.

show lacp

트래픽 통계, 시스템 식별자 및 네이버 정보와 같은 EtherChannel LACP 정보를 표시하려면 이 명령을 입력합니다.

show lacp {*channel_group_number* {**counters** | **internal** [**detail**] | **neighbor** [**detail**]} | **neighbor** [**detail**] | **sys-id**}

channel_group_number	EtherChannel 채널 그룹 번호(1~48)를 지정하고, 이 채널 그룹에 대한 정보만 표시합니다.
카운터	보내고 받은 LACPDU 및 마커 수에 대한 카운터를 표시합니다.
detail	항목에 대한 추가 세부 정보를 표시합니다.
internal	내부 정보를 표시합니다.
neighbor	네이버 정보를 표시합니다.
sys-id	LACP 시스템 ID를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show lacp sys-id** 명령의 샘플 출력입니다.

```
> show lacp sys-id
32768,001c.c4e5.cfee
```

다음은 **show lacp counters** 명령의 샘플 출력입니다.

```
> show lacp counters

              LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv    Sent    Recv      Pkts Err
--------------------------------------------------------------------
Channel group: 1
Gi3/1      736    728      0      0       0       0         0
Gi3/2      739    730      0      0       0       0         0
Gi3/3      739    732      0      0       0       0         0
```

다음은 **show lacp internal** 명령의 샘플 출력입니다.

```
> show lacp internal

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d
```

다음은 **show lacp neighbor** 명령의 샘플 출력입니다.

```
> show lacp neighbor

Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1 neighbors

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

명령	설명
show port-channel	EtherChannel 정보를 자세한 형식 및 한 줄짜리 요약 형식으로 표시합니다. 이 명령은 포트 및 포트-채널 정보도 표시합니다.
show port-channel load-balance	정해진 매개변수 집합에 대해 선택한 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보를 표시합니다.

show lacp cluster

cLACP 시스템 MAC 및 ID를 표시하려면 **show lacp cluster** 명령을 사용합니다.

show lacp cluster {**system-mac** | **system-id**}

system-mac	시스템 ID와 해당 ID가 자동으로 생성되었는지 또는 수동으로 입력되었는지 표시합니다.
system-id	시스템 ID와 우선순위를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show lacp cluster system-mac** 명령의 샘플 출력입니다.

```
> show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

다음은 **show lacp cluster system-id** 명령의 샘플 출력입니다.

```
> show lacp cluster system-id
5    ,a300.010a.010a
```

show lisp eid

EID 테이블을 보려면 **show lisp eid** 명령을 사용합니다.

show lisp eid [**site-id** *id*]

site-id*id*	특정 사이트의 EID만 확인합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스가 EID 및 사이트 ID를 상호 연결하는 EID 테이블을 유지 관리합니다.

다음은 **show lisp eid** 명령의 샘플 출력입니다.

```
> show lisp eid
LISP EID       Site ID
10.44.33.105        2
10.44.33.201        2
192.168.11.1        4
192.168.11.2        4
```

명령	설명
clear cluster info flow-mobility counters	플로우 모빌리티 카운터를 지웁니다.
clear lisp eid	ASA EID 테이블에서 EID를 제거합니다.
show cluster info flow-mobility counters	플로우 모빌리티 카운터를 표시합니다.
show conn	LISP 플로우 모빌리티에 대한 트래픽 제목을 표시합니다.
show service-policy	서비스 정책을 표시합니다.

show local-host

로컬 호스트의 네트워크 상태를 표시하려면 **show local-host** 명령을 사용합니다.

show local-host [*hostname* | *ip_address*] [**detail**] [**all**] [**brief**] [**connection** {**sctp** | **tcp** | **udp** | **embryonic**} *start*[*-end*]] [**zone**]

all	(선택 사항) 디바이스에 연결된 로컬 호스트와 디바이스에서 연결된 로컬 호스트를 포함합니다.
brief	(선택 사항) 로컬 호스트에 대한 간략한 정보를 표시합니다.
connection {**sctp** | **tcp** | **udp** | **embryonic**} *start*[*-end*]	(선택 사항) 번호 및 연결 유형에 따라 필터를 적용합니다. 원시, TCP, UDP 또는 SCTP. 시작 숫자는 해당 유형 연결의 최소 개수를 표시합니다. 10-100 같은 범위를 지정하려면 -end 숫자를 포함시킵니다. 이러한 필터를 개별적으로 사용하거나 함께 사용할 수 있습니다.
detail	(선택 사항) 활성 xlate 및 네트워크 연결에 대한 자세한 정보를 포함하여 로컬 호스트 정보의 자세한 네트워크 상태를 표시합니다.
hostname | *ip_address*	(선택 사항) 로컬 호스트 이름 또는 IPv4/IPv6 주소를 지정합니다.
zone	(선택 사항) 이 키워드는 Firepower Threat Defense에서 사용되지 않습니다. 이는 보안 영역과 연결되지 않습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show local-host 명령을 사용하여 로컬 호스트의 네트워크 상태를 표시할 수 있습니다. 로컬 호스트는 Firepower Threat Defense 디바이스로 트래픽을 전달하거나 Firepower Threat Defense 디바이스를 통해 트래픽을 전달하는 모든 호스트에 대해 생성됩니다.

이 명령을 사용하여 로컬 호스트에 대한 변환 및 연결 슬롯을 표시할 수 있습니다. 변환 정보가 호스트에 할당된 모든 PAT 포트 블록을 포함합니다.

또한 연결 제한 값도 표시합니다. 연결 제한이 설정되지 않은 경우에는 값이 0으로 표시되고 제한이 적용되지 않습니다.

SYN 공격(TCP 가로채기가 구성됨) 시 **show local-host** 명령 출력에는 가로채기된 연결 수가 사용 개수에 포함됩니다. 이 필드에는 일반적으로 완전히 열려 있는 연결만 표시됩니다.

show local-host 명령 출력에서 **TCP embryonic count to host counter**는 고정 연결을 사용하는 호스트에 대해 최대 원시 제한(TCP 가로채기 워터마크)이 구성된 경우에 사용됩니다. 이 카운터는 다른 호스트에서 호스트에 연결한 총 원시 연결 수를 보여 줍니다. 이 합계가 구성된 최대 제한을 초과하면 호스트에 대한 새 연결에 TCP 가로채기가 적용됩니다.

다음은 **show local-host** 명령의 샘플 출력입니다.

```
> show local-host

Interface mgmt: 2 active, 2 maximum active, 0 denied
local host: <10.24.250.191>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
local host: <10.44.64.65>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 1
    TCP intercept watermark = unlimited
    UDP flow count/limit = 5/unlimited
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
Interface any: 0 active, 0 maximum active, 0 denied
```

다음 예에서는 로컬 호스트의 네트워크 상태를 보여 줍니다.

```
> show local-host all

Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
```

```
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
```

다음 예에서는 특정한 호스트에 대한 정보를 보여준 다음 해당 호스트에 대한 상세한 정보를 보여줍니다.

```
> show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

> show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active,
1 maximum active, 0 denied
```

다음 예에서는 최소 4개의 UDP 연결이 있고 TCP 동시 연결 수가 1~10개인 모든 호스트를 보여 줍니다.

```
> show local-host connection udp 4 tcp 1-10
Interface mng: 0 active, 3 maximum active, 0 denied
Interface INSIDE: 4 active, 5 maximum active, 0 denied
local host: <10.1.1.11>,
       TCP flow count/limit = 1/unlimited TCP embryonic count to host = 0 TCP intercept
       watermark = unlimited UDP flow count/limit = 4/unlimited
Xlate:
       Global 192.168.1.24 Local 10.1.1.11 Conn: UDP out 192.168.1.10:80 in
       10.1.1.11:1730 idle 0:00:21 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1729 idle 0:00:22 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1728 idle 0:00:23 bytes 0 flags - UDP out 192.168.1.10:80 in
       10.1.1.11:1727 idle 0:00:24 bytes 0 flags - TCP out 192.168.1.10:22 in
       10.1.1.11:27337 idle 0:01:55 bytes 2641 flags UIO Interface OUTSIDE: 3 active, 5
```

```
maximum active, 0 denied
```

명령	설명
clear local-host	**show local-host** 명령에서 표시하는 로컬 호스트에서 네트워크 연결을 해제합니다.

show log-events-to-ramdisk

RAM 디스크에 대한 연결 이벤트 로깅의 상태를 표시하려면 **show log-events-to-ramdisk** 명령을 사용합니다.

show log-events-to-ramdisk

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 연결 이벤트를 RAM 디스크 또는 SSD(Solid State Drive)에 로깅하고 있는지를 보여줍니다. RAM 디스크 로깅은 모든 하드웨어 모델에서 지원되지는 않습니다. **configure log-events-to-ramdisk** 명령을 사용하여 RAM 디스크 로깅을 구성합니다.

다음 예에서는 RAM 디스크에 대한 로깅이 이 하드웨어 모델에서 지원되지 않음을 보여줍니다.

```
> show log-events-to-ramdisk
This command is not available on this platform.
```

명령	설명
configure log-events-to-ramdisk	RAM 디스크에 대한 연결 이벤트 로깅을 활성화하거나 비활성화합니다.

show logging

버퍼의 로그 또는 기타 기록 설정을 표시하려면 **show logging** 명령을 사용합니다.

show logging [**message** [*syslog_id* | **all**] | **asdm** | **flow-export-syslogs** | **host** | **queue** | **setting**]

all	(선택 사항) 모든 syslog 메시지 ID를 사용 여부와 함께 표시합니다.
asdm	(선택 사항) 이 키워드는 Firepower Device Manager에서 작동하지 않습니다. 이는 ASA 소프트웨어 디바이스를 구성하는 ASDM에 연결됩니다.
flow-export-syslogs	(선택 사항) 해당 정보는 NetFlow에서 정보가 캡처되는 syslog 메시지를 모두 표시합니다.
host	(선택 사항) Syslog 서버 정보를 표시합니다.
message [*syslog_id* | **all**]	(선택 사항) syslog ID 또는 모두를 지정하지 않으면 이 키워드는 기준이 아닌 수준의 메시지를 표시합니다. 또한 ID별로 메시지를 표시하거나 모든 syslog 메시지에 대한 정보를 참조하십시오.
queue	(선택 사항) syslog 메시지 대기열을 표시합니다.
setting	(선택 사항) 기록 버퍼를 표시하지 않고 기록 설정을 표시합니다.
syslog_id	(선택 사항) 표시할 메시지 수를 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

내부 버퍼에 대한 로깅을 활성화한 경우 키워드 없는 **show logging** 명령은 현재 메시지 버퍼 및 현재 설정을 표시합니다.

show logging queue 명령을 사용하여 다음을 표시할 수 있습니다.

- 대기열의 메시지 수
- 대기열에 있는 기록된 최대 메시지 수

- 블록 메모리를 사용하여 처리할 수 없어 삭제된 메시지 수
- 트랩과 다른 syslog 메시지에 대한 별도의 대기열

참고 0은 구성된 대기열 크기에 사용할 수 있는 숫자이며, 허용되는 최대 대기열 크기를 나타냅니다. 구성된 대기열 크기가 0인 경우 **show logging queue** 명령의 출력에는 실제 대기열 크기가 표시됩니다.

show logging flow-export-syslogs 명령은 다음 syslog가 활성화 또는 비활성화되는지 여부를 표시합니다. Netflow를 사용 중인 경우, syslog가 중복되므로 이 syslog를 비활성화하는 옵션이 있습니다.

Syslog 메시지	설명
106015	첫 번째 패킷이 SYN 패킷이 아니므로 TCP 플로우가 거부됨
106023	인터페이스에 연결된 인그레스 ACL 또는 이그레스 ACL에서 거부하는 흐름.
106100	ACL에서 허용 또는 거부하는 흐름.
302013 및 302014	TCP 연결 및 삭제.
302015 및 302016	UDP 연결 및 삭제.
302017 및 302018	GRE 연결 및 삭제.
302020 및 302021	ICMP 연결 및 삭제.
313001	Firepower Threat Defense 디바이스에 대한 ICMP 패킷이 거부됨
313008	Firepower Threat Defense 디바이스에 대한 ICMPv6 패킷이 거부됨
710003	Firepower Threat Defense에 대한 연결 시도가 거부됨

다음은 **show logging** 명령의 샘플 출력입니다.

```
> show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging:disabled
    Debug-trace logging: disabled
    Console logging: level informational, 3962 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, facility 20, 20549 messages logged
        Logging to inside 10.2.5.3 tcp/50001 connected
```

```
    Permit-hostdown state
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

참고 Syslog 로깅의 가능한 값은 enabled, disabled, disabled-blocking 및 disabled-not blocking입니다.

다음은 보안 syslog 서버가 구성된 경우 **show logging** 명령의 샘플 출력입니다.

```
> show logging
Syslog logging: disabled
    Facility:
    Timestamp logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: level debugging, 135 messages logged
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: list show _syslog, facility, 20, 21 messages logged
        Logging to inside 10.0.0.1 tcp/1500 SECURE
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging disabled
```

다음은 **show logging queue** 명령의 샘플 출력입니다.

```
> show logging queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

다음은 **show logging message all** 명령의 샘플 출력입니다.

```
> show logging message all
syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

show mac-address-table

MAC 주소 테이블을 표시하려면 **show mac-address-table** 명령을 사용합니다.

show mac-address-table[*interface_name*| **count** | **static**]

count	(선택 사항) 동적 및 고정 항목의 총 개수를 나열합니다.
interface_name	(선택 사항) MAC 주소 테이블 항목을 확인할 인터페이스 이름을 식별합니다.
static	(선택 사항) 고정 항목만 나열합니다.

인터페이스를 지정하지 않으면 모든 인터페이스 MAC 주소 항목이 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 추가되었습니다.
6.2	Cisco는 IRB(Integrated Routing and Bridging) 사용 시 라우팅 방화벽 모드에서 지원을 추가했습니다.

다음은 **show mac-address-table** 명령의 샘플 출력입니다.

```
> show mac-address-table
interface    mac address     type      Time Left
-----------------------------------------------------
outside      0009.7cbe.2100  static    -
inside       0010.7cbe.6101  static    -
inside       0009.7cbe.5101  dynamic   10
```

다음은 **show mac-address-table count** 명령의 샘플 출력입니다.

```
> show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

show mac-learn

MAC 학습이 각 인터페이스에 대해 사용 설정 또는 사용 해제되었는지 여부를 표시하려면 **show mac-learn** 명령을 사용합니다.

show mac-learn

릴리스	수정 사항
6.1	이 명령이 추가되었습니다.
6.2	Cisco는 통합 라우팅 및 브리징 사용 시 라우팅 방화벽 모드에서 지원을 추가했습니다.

사용 가이드라인

기본적으로 각 인터페이스에서는 들어오는 트래픽의 MAC 주소를 자동으로 알게 되며, 시스템에서는 해당 항목을 MAC 주소 테이블에 추가합니다. 인터페이스당 MAC 학습을 사용 해제할 수 있습니다.

다음은 **show mac-learn** 명령의 샘플 출력입니다.

```
> show mac-learn
no mac-learn flood
interface                          mac learn
-----------------------------------------
 outside                             enabled
 inside1_2                           enabled
 inside1_3                           enabled
 inside1_4                           enabled
 inside1_5                           enabled
 inside1_6                           enabled
 inside1_7                           enabled
 inside1_8                           enabled
 diagnostic                          enabled
 inside                              enabled
```

show managers

디바이스 구성을 관리하는 현재 관리자를 표시하려면 **show managers** 명령을 사용합니다.

show managers

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

어느 애플리케이션이 디바이스 구성 관리에 대해 정의되어 있는지 확인하려면 **show managers** 명령을 사용합니다. 그런 다음 웹 브라우저를 사용하여 관리자로 로그인할 수 있습니다.

configure manager add 명령을 사용하여 원격 관리자, Firepower Management Center를 디바이스에 대해 구성할 경우, 출력은 호스트 이름 및 등록 상태를 보여줍니다. 등록이 보류 중이면 등록 키와 NAT ID만 표시됩니다. 디바이스가 고가용성 쌍에 등록되면 관리하는 두 Management Center에 대한 정보가 표시됩니다. 디바이스가 스태킹된 구성에서 보조 디바이스로 구성된 경우, 관리하는 Management Center 및 기본 디바이스 모두에 대한 정보가 표시됩니다.

다음 예에서는 Firepower Management Center 원격 관리자에게 완료된 등록을 보여줍니다.

```
> show managers
Type                      : Manager
Host                      : 10.83.57.41
Registration              : Completed
```

다음 예에서는 로컬 관리자, Firepower Device Manager가 사용 설정되어 있는지를 보여줍니다.

```
> show managers
Managed locally.
```

다음 예에서는 관리자가 현재 구성되어 있지 않음을 보여줍니다. 디바이스를 구성하려면 먼저 사용하기 위해 configure manager add 또는 configure manager local 명령을 사용해야 합니다.

```
> show managers
No managers configured.
```

명령	설명
configure manager add	원격 관리자, Firepower Management Center를 추가합니다.

명령	설명
configure manager delete	현재 관리자를 삭제하고 관리자 없음 모드를 시작합니다.
configure manager local	로컬 관리자, Firepower Device Manager를 활성화합니다.

show memory

운영 체제에 사용 가능한 최대 실제 메모리 및 현재 사용 가능한 메모리에 대한 요약을 표시하려면 **show memory** 명령을 사용합니다.

show memory [**api** | **app-cache** | **binsize** *size* | **caller-address** | **detail** | **region** | **system** | **top-usage** [*num*]]

api	(선택 사항) 이 명령은 시스템에 등록된 malloc 스택 API를 표시합니다. 메모리 디버깅 기능(즉, delay-free-poisoner, memory logger, memory tracker 또는 memory profiler)이 켜진 경우 해당 API가 출력에 표시됩니다.
app-cache	(선택 사항) 애플리케이션별로 메모리 사용량을 표시합니다.
binsize*size*	(선택 사항) 특정 휴지통 크기에 할당된 청크(메모리 블록)에 대한 요약 정보를 표시합니다. 휴지통 크기는 **show memory detail** 명령 출력의 "fragment size" 열에 표시됩니다.
caller-address	**memory caller-address** 컨피그레이션과 관련된 정보를 표시합니다.
detail	(선택 사항) 사용 가능한 시스템 메모리와 할당된 시스템 메모리에 대한 자세한 보기를 표시합니다.
region	프로세스 맵을 처리합니다.
system	디바이스에 대한 총 메모리, 사용 중인 메모리 및 사용 가능한 메모리를 표시합니다.
top-usage [*num*]	**show memory detail** 명령에서 할당된 조각 크기의 최대 수를 표시합니다. 나열할 휴지통 크기의 수(1-64)를 선택적으로 지정할 수 있습니다. 기본값은 10입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show memory 명령을 사용하여 운영 체제에 사용 가능한 최대 실제 메모리 및 현재 사용 가능한 메모리에 대한 요약을 표시할 수 있습니다. 메모리는 필요에 따라 할당됩니다.

또한 SNMP를 사용하여 **show memory** 명령에서 정보를 표시할 수 있습니다.

show memory detail 출력을 **show memory binsize** 명령과 함께 사용하여 메모리 누수를 디버그할 수 있습니다.

show memory detail 명령 출력은 세 개의 섹션(Summary, DMA Memory 및 HEAP Memory)으로 분할될 수 있습니다. 요약에는 할당된 총 메모리가 표시됩니다. DMA에 연결되거나 예약되지 않은 메모리는 HEAP으로 간주됩니다. Free Memory 값은 HEAP에서 사용되지 않은 메모리입니다. Allocated memory in use 값은 할당된 HEAP 양입니다. HEAP 할당의 분석 결과는 출력의 뒷부분에 표시됩니다. Reserved memory 및 DMA Reserved memory는 서로 다른 시스템 프로세스에서 사용되며, 주로 VPN 서비스에서 사용됩니다.

Free memory는 Free memory heap과 Free memory system의 두 부분으로 나누어집니다. Free memory heap은 glibc heap의 사용 가능한 메모리 양입니다. glibc heap이 요청에 따라 증가 및 감소할 때 free heap memory 양은 시스템에 남아 있는 총 메모리를 나타내지 않습니다. Free memory system은 ASA에 사용 가능한 여유 메모리 양을 나타냅니다.

Reserved memory(DMA)는 DMA 풀용으로 예약된 메모리 양입니다. Memory overhead는 실행 중인 여러 프로세스의 glibc 오버헤드 및 프로세스 오버헤드입니다.

allocated memory statistics total (bytes) 열에 표시된 값은 **show memory detail** 명령 출력의 실제 값(MEMPOOL_GLOBAL_SHARED POOL STATS)을 반영하지 않습니다.

참고 MEMPOOL_GLOBAL_SHARED가 부팅 중 모든 시스템 메모리를 사용하지는 않지만 필요할 때마다 메모리를 위해 기본 운영 체제를 요청합니다. 마찬가지로, 상당한 양의 메모리가 지워진 경우 시스템에 메모리를 반환합니다. 그 결과, MEMPOOL_GLOBAL_SHARED의 크기는 요구 사항에 따라 증가하거나 축소되게 나타납니다. 할당 속도를 높이기 위해 MEMPOOL_GLOBAL_SHARED에 최소 여유 메모리가 남아 있습니다.

출력에는 크기가 49,152인 블록이 할당된 다음 사용 가능한 풀로 반환되고 크기가 131,072인 다른 블록이 할당된 것으로 표시됩니다. 이 경우 사용 가능한 메모리가 131,072-49,152=81,920바이트 감소한 것으로 생각할 수 있지만 실제로는 100,000바이트 감소한 것입니다(Free memory 줄 참고).

```
> show memory detail
MEMPOOL_GLOBAL_SHARED POOL STATS:            MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated =   1862270976   Non-mmapped bytes allocated =   1862270976
Number of free chunks       =           99   Number of free chunks       =          100
Number of mmapped regions   =            0   Number of mmapped regions   =            0
Mmapped bytes allocated     =            0   Mmapped bytes allocated     =            0
Max memory footprint        =   1862270976   Max memory footprint        =   1862270976
Keepcost                    =   1762019304   Keepcost                    =   1761869256
Max contiguous free mem     =   1762019304   Max contiguous free mem     =   1761869256
Allocated memory in use     =    100133944   Allocated memory in use     =    100233944
Free memory                 =   1762137032   Free memory                 =   1762037032
----- fragmented memory statistics -----     ----- fragmented memory statistics -----
 fragment size       count          total      fragment size       count          total
    (bytes)                       (bytes)         (bytes)                       (bytes)
---------------  ----------  -------------- ---------------  ----------  --------------
        32768             1          33176          32768             1          33176
                                                    49152             1          50048
   1762019304             1     1762019304*     1761869256             1     1761869256*
----- allocated memory statistics -----      ----- allocated memory statistics -----
 fragment size       count          total      fragment size       count          total
    (bytes)                       (bytes)         (bytes)                       (bytes)
---------------  ----------  -------------- ---------------  ----------  --------------
        49152            10         491520          49152             9         442368
```

```
        65536          125        8192000          65536          125        8192000
        98304            3         294912          98304            3         294912
       131072           18        2359296         131072           19        2490368
```

다음 출력에서는 크기가 131,072인 블록 대신 크기가 150,000인 블록이 할당되었음을 확인합니다.

```
> show memory binsize 131072
MEMPOOL_DMA pool bin stats:
MEMPOOL_GLOBAL_SHARED pool bin stats:
pc = 0x8eda524, size = 150000   , count = 1
pc = 0x8f08054, size = 163904   , count = 1
pc = 0x846e477, size = 139264   , count = 1
pc = 0x8068691, size = 393216   , count = 3
pc = 0x8eea09b, size = 131072   , count = 1
pc = 0x88ca830, size = 141212   , count = 1
pc = 0x9589e93, size = 593580   , count = 4
pc = 0x9589bd2, size = 616004   , count = 4
pc = 0x8f2e060, size = 327808   , count = 2
pc = 0x8068284, size = 182000   , count = 1

0x8eda524 <logger_buffer_init_int+148 at syslog/main.c:403>
```

show memory detail 명령 출력에 대략적인 총 바이트 수가 표시되는 것은 설계에 따른 것입니다. 여기에는 두 가지 이유가 있습니다.

- 각 프래그먼트 크기에 대해 모든 프래그먼트의 합계를 구해야 하는 경우 단일 프래그먼트 크기에 대한 할당이 너무 많고 정확한 값을 얻으려면 수천 개의 청크를 확인해야 하기 때문에 성능이 저하될 수 있습니다.
- 각 휴지통 크기의 경우 이중 링크된 할당 목록을 확인해야 하며 많은 할당이 있을 수 있습니다. 이 경우 연장된 기간 동안 CPU를 사용할 수 없으므로 할당을 주기적으로 일시 중단해야 합니다. 할당을 다시 시작한 후에는 다른 프로세스에 메모리가 할당되거나 할당 취소되고 메모리 상태가 변경될 수 있습니다. 따라서 total bytes 열에 실제 값 대신 근사값이 제공됩니다.

다음은 **show memory** 명령의 샘플 출력입니다.

```
> show memory
Free memory:        845044716 bytes (79%)
Used memory:        228697108 bytes (21%)
-------------      ----------------
Total memory:      1073741824 bytes (100%)
```

다음 예는 시스템 레벨 메모리 사용량이 표시되는 방법을 보여줍니다.

```
> show memory system
             total       used       free     shared    buffers     cached
Mem:       3982640    3014544     240200          0     159932     567964
-/+ buffers/cache:    3014544     968096
Swap:      3998716     137704    3861012
```

다음은 **show memory detail** 명령의 샘플 출력입니다.

```
> show memory detail
Free memory heap:                   36502064 bytes ( 2%)
Free memory system:                977607394 bytes (46%)
Used memory:
     Allocated memory in use:      285386128 bytes (13%)
     Reserved memory (DMA):        169869312 bytes ( 8%)
     Memory overhead:              678118749 bytes (32%)
```

```
------------------------------   ------------------
Total memory:                     2147483647 bytes (100%)

Least free memory:       1682870271 bytes (78%)
Most used memory:         464613376 bytes (22%)

MEMPOOL_HEAPCACHE_0 POOL STATS:
Non-mmapped bytes allocated =    314572800
Number of free chunks       =          518
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    314572800
Keepcost                    =     27897792
Max contiguous free mem     =     27897792
Allocated memory in use     =    278070512
Free memory                 =     36502288

----- fragmented memory statistics -----

(...Remaining output truncated...)
```

다음 예는 휴지통 크기 8192에 할당된 청크를 보여줍니다.

```
> show memory binsize 8192
MEMPOOL_HEAPCACHE_0 pool bin stats:
pc = 0x7efc3f80e508, size = 773406   , count = 92
pc = 0x7efc3e3c5013, size = 189152   , count = 23
pc = 0x7efc405df64f, size = 287036   , count = 32
pc = 0x7efc3f9ef622, size = 8128     , count = 1
pc = 0x7efc3f4fd5f5, size = 871744   , count = 106
pc = 0x7efc3f4fd8b7, size = 82240    , count = 10
pc = 0x7efc3f18c3e6, size = 20272    , count = 2
pc = 0x7efc3f557139, size = 8192     , count = 1
pc = 0x7efc3e3f1697, size = 8344     , count = 1
pc = 0x7efc3e0506f6, size = 8192     , count = 1
MEMPOOL_DMA pool bin stats:
pc = 0x7efc3e1cca68, size = 10240    , count = 1
MEMPOOL_GLOBAL_SHARED pool bin stats:
```

다음은 **show memory api** 명령의 샘플 출력입니다. 메모리 추적기 delayed-free-poisoner 메모리 기능이 활성화되었음을 보여줍니다.

```
> show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

다음 예는 시스템 레벨 메모리 사용량이 표시되는 방법을 보여줍니다.

```
> show memory system
             total       used       free     shared    buffers     cached
Mem:       3982640    3014544     240200          0     159932     567964
-/+ buffers/cache:    3014544     968096
Swap:      3998716     137704    3861012
```

명령	설명
show memory profile	Firepower Threat Defense의 메모리 사용량(프로파일링)에 대한 정보를 표시합니다.
show memory binsize	특정 휴지통 크기에 할당된 청크에 대한 요약 정보를 표시합니다.

show memory delayed-free-poisoner

memory delayed-free-poisoner 대기열 사용에 대한 요약을 표시하려면 **show memory delayed-free-poisoner** 명령을 사용합니다.

show memory delayed-free-poisoner

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

기능을 활성화하려면 **memory delayed-free-poisoner enable** 명령을 사용합니다. **clear memory delayed-free-poisoner** 명령을 사용하여 대기열 및 통계를 지울 수 있습니다.

다음은 **show memory delayed-free-poisoner** 명령의 샘플 출력입니다.

```
> memory delayed-free-poisoner enable
> show memory delayed-free-poisoner
delayed-free-poisoner settings:
 delayed-free-poisoner threshold 100
 delayed-free-poisoner desired-fragment-size 102400
 delayed-free-poisoner desired-fragment-count 16
 delayed-free-poisoner watchdog-percent 50
delayed-free-poisoner statistics:
                  136064:  current memory in queue
                     500:  current queue length
                       0:  frees dequeued
                     280:  frees not queued for size
                       0:  frees not queued for locking
                       0:  successful validate runs
                       0:  aborted validate runs
                   never:  time of last validate
                       0:  threshold defragment operations
                       0:  size and/or count defragment operations
                       0:  watchdog-aborts
```

show memory logging

메모리 사용량 로깅을 표시하려면 **show memory logging** 명령을 사용합니다.

show memory logging [**wrap** | **brief** | **include** [*option*]]

brief	(선택 사항) 요약된 메모리 사용량 로깅을 표시합니다.
include*option*	(선택 사항) 출력에서 지정된 필드만 포함합니다. 필드의 키워드를 지정할 때는 특별한 순서가 없지만 항상 다음 순서로 나타납니다. 옵션을 포함하지 않는 경우, 출력은 **brief**를 지정하는 경우(**include** 대신)와 동일합니다. • **process** • **time** • **operator**(free/malloc/etc.) • **address** • **size** • **callers** 출력 형식은 다음과 같습니다. process=[XXX] time=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX 최대 4개의 발신자 주소가 나타납니다. 작업의 유형이 예시된 출력(Number of...)에 나와 있습니다.
wrap	(선택 사항) 메모리 사용량 로깅 래핑 데이터를 표시합니다. 이 데이터는 중복 데이터가 나타나지 않고 저장되지도 않도록 이 명령을 입력한 후에 제거됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

메모리 로그 정보를 보려면 **show memory logging** 명령을 사용합니다. **memory logging** 명령을 사용하여 이 로깅을 먼저 활성화해야 합니다.

다음은 **show memory logging** 명령의 샘플 출력입니다.

```
> memory logging 1024
> show memory logging
Number of free                          203989
Number of calloc                        83703
Number of malloc                        120286
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 407978
Buffer size: 1024 (73816 x2 bytes)
process=[cli_xml_server] time=[19:23:42.030] oper=[malloc] addr=0x00007efc358373c0 size=72

@ 0x00007efc3f8e9404 0x00007efc3f80e508 0x00007efc3f4d3cea 0x00007efc3e037f0c
process=[cli_xml_server] time=[19:23:42.030] oper=[free] addr=0x00007efc358373c0 size=72
@ 0x00007efc3f80e9c0 0x00007efc3f4d3fb8 0x00007efc3e037fb0 0x00007efc3f4d537d
(...Remaining output truncated...)
```

다음은 **show memory logging brief** 명령의 샘플 출력입니다.

```
> show memory logging brief
Number of free                          223195
Number of calloc                        91624
Number of malloc                        131572
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 446391
Buffer size: 1024 (73816 x2 bytes)
```

명령	설명
memory logging	메모리 로깅을 활성화합니다.

show memory profile

Firepower Threat Defense 디바이스의 메모리 사용량(프로파일링)에 대한 정보를 표시하려면 **show memory profile** 명령을 사용합니다.

show memory profile [**status** | **peak** [**detail** | **collated**]]

collated	(선택 사항) 표시된 메모리 정보를 대조합니다.
detail	(선택 사항) 자세한 메모리 정보를 표시합니다.
peak	(선택 사항) "사용 중인" 버퍼가 아니라 피크 캡처 버퍼를 표시합니다.
status	(선택 사항) 메모리 프로파일링의 현재 상태 및 피크 캡처 버퍼를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show memory profile 명령을 사용하여 메모리 사용량 수준 및 메모리 누수 문제를 해결할 수 있습니다. 프로파일링이 중지된 경우에도 프로파일 버퍼 내용을 볼 수 있습니다. 프로파일링을 시작하면 버퍼가 자동으로 지워집니다.

참고 Firepower Threat Defense 디바이스에서는 메모리 프로파일링이 활성화된 경우 성능이 일시적으로 저하될 수 있습니다.

다음은 **show memory profile** 명령의 샘플 출력입니다.

```
> show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

show memory profile detail 명령의 출력은 맨 왼쪽부터 6개의 데이터 열과 1개의 헤더 열로 나누어집니다. 첫 번째 데이터 열에 해당하는 메모리 버킷 주소는 헤더 열에 제공됩니다(16진수 숫자). 데이터 자체는 버킷 주소에 속한 텍스트/코드에서 유지되는 바이트 수입니다. 데이터 열의 마침표(.)는 이 버킷의 텍스트에서 유지되는 메모리가 없음을 의미합니다. 행의 다른 열은 이전 열의 증분 양보다 큰 버킷 주소에 해당합니다. 예를 들어 첫 번째 행에 있는 첫 번째 데이터 열의 주소 버킷은 0x001069e0이고, 첫 번째 행에 있는 두 번째 데이터 열의 주소 버킷은 0x001069e4입니다. 일반적으로 헤더 열 주소는 다음 버킷 주소입니다. 즉, 이전 행의 마지막 데이터 열 주소에 증분값을 더한 값입니다. 사용량이 없는 모든 행은 표시되지 않습니다. 헤더 열에 3개의 마침표(...)를 표시하여 이러한 인접 행을 두 개 이상 표시하지 않을 수 있습니다.

다음은 피크 캡처 버퍼 및 해당 버킷 주소에 속한 텍스트/코드에서 유지되는 바이트 수를 보여 주는 **show memory profile peak detail** 명령의 샘플 출력입니다.

```
> show memory profile peak detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
(...output truncated...)
```

다음은 **show memory profile peak collated** 명령의 샘플 출력입니다.

```
> show memory profile peak collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<More>
```

다음은 피크 캡처 버퍼를 보여주는 **show memory profile peak** 명령의 샘플 출력입니다.

```
> show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

다음은 메모리 프로파일링의 현재 상태 및 피크 캡처 버퍼를 보여 주는 **show memory profile status** 명령의 샘플 출력입니다.

```
> show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
```

```
Profile:
0x00100020-0x00bfc3a8(00000004)
```

명령	설명
memory profile enable	메모리 사용량(메모리 프로파일링)의 모니터링을 활성화합니다.
memory profile text	프로파일링할 메모리의 프로그램 텍스트 범위를 구성합니다.
clear memory profile	메모리 프로파일링 기능에서 유지되는 메모리 버퍼를 지웁니다.

show memory tracking

툴에서 추적한 현재 할당된 메모리를 표시하려면 **show memory tracking** 명령을 사용합니다.

show memory tracking [**address** | **detail** | **dump** *tracked_address*]

address	(선택 사항) 주소를 통한 메모리 추적을 표시합니다.
detail	(선택 사항) 내부 메모리 추적 상태를 표시합니다.
dump*tracked_address*	(선택 사항) 지정된 메모리 추적 주소(0-4294967295)의 덤프를 보여줍니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

자용 가이드라인

show memory tracking 명령을 사용하여 툴에서 추적한 현재 할당된 메모리를 표시할 수 있습니다. 이 정보를 확인하려면 먼저 **memory tracking enable**을 사용해야 합니다.

다음은 **show memory tracking** 명령의 샘플 출력입니다.

```
> show memory tracking
memory tracking by caller:
  bytes-threshold:        0
  allocates-by-threshold: 0
         65406 bytes from    49 allocates by 0x00007efc3f80e508
          3000 bytes from     1 allocates by 0x00007efc3f4e1278
           159 bytes from     1 allocates by 0x00007efc3fe9ee13
            17 bytes from     1 allocates by 0x00007efc3fe9ef4e
```

다음은 **show memory tracking address** 명령의 샘플 출력입니다.

```
> show memory tracking address
memory tracking by caller:
  bytes-threshold:        0
  allocates-by-threshold: 0
         58918 bytes from    49 allocates by 0x00007efc3f80e508
          3000 bytes from     1 allocates by 0x00007efc3f4e1278
           167 bytes from     1 allocates by 0x00007efc3fe9ee13
            17 bytes from     1 allocates by 0x00007efc3fe9ef4e
memory tracking address pool:
            32 byte region @ 0x00007efc358a06e0 allocated by 0x00007efc3f80e508
```

```
  96 byte region @ 0x00007efc351d0880 allocated by 0x00007efc3f80e508
 896 byte region @ 0x00007efc35f121c0 allocated by 0x00007efc3f80e508
8192 byte region @ 0x00007efc35832e20 allocated by 0x00007efc3f80e508
  96 byte region @ 0x00007efc30483910 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc359e3960 allocated by 0x00007efc3f80e508
1036 byte region @ 0x00007efc35f04680 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc36024890 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc35fd48a0 allocated by 0x00007efc3f80e508
  32 byte region @ 0x00007efc35f04ad0 allocated by 0x00007efc3f80e508
  34 byte region @ 0x00007efc35e54e00 allocated by 0x00007efc3f80e508
8192 byte region @ 0x00007efc35834e70 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc36005cc0 allocated by 0x00007efc3f80e508
  11 byte region @ 0x00007efc360061e0 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc357a6dd0 allocated by 0x00007efc3f80e508
1024 byte region @ 0x00007efc358574f0 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc365b7ef0 allocated by 0x00007efc3f80e508
  56 byte region @ 0x00007efc365b7f90 allocated by 0x00007efc3f80e508
 168 byte region @ 0x00007efc365b8210 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc365b8300 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc365b83c0 allocated by 0x00007efc3f80e508
  16 byte region @ 0x00007efc365b8560 allocated by 0x00007efc3f80e508
 167 byte region @ 0x00007efc365b85c0 allocated by 0x00007efc3fe9ee13
2048 byte region @ 0x00007efc357a8610 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc35728be0 allocated by 0x00007efc3f80e508
  88 byte region @ 0x00007efc357a8e60 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc35fe90c0 allocated by 0x00007efc3f80e508
  17 byte region @ 0x00007efc365b95a0 allocated by 0x00007efc3fe9ef4e
  72 byte region @ 0x00007efc365b9600 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc365b9690 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc365b9720 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc365b97b0 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc365b9820 allocated by 0x00007efc3f80e508
   2 byte region @ 0x00007efc365b9880 allocated by 0x00007efc3f80e508
  76 byte region @ 0x00007efc35ff9aa0 allocated by 0x00007efc3f80e508
 776 byte region @ 0x00007efc35f19df0 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc3585a0a0 allocated by 0x00007efc3f80e508
 936 byte region @ 0x00007efc357aaea0 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc357ab290 allocated by 0x00007efc3f80e508
 568 byte region @ 0x00007efc3592bc40 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc35e5c8a0 allocated by 0x00007efc3f80e508
  40 byte region @ 0x00007efc35f2cae0 allocated by 0x00007efc3f80e508
1665 byte region @ 0x00007efc359fcda0 allocated by 0x00007efc3f80e508
 168 byte region @ 0x00007efc34fccf60 allocated by 0x00007efc3f80e508
 112 byte region @ 0x00007efc35ffd0e0 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc356bd340 allocated by 0x00007efc3f80e508
8208 byte region @ 0x00007efc3643d3e0 allocated by 0x00007efc3f80e508
 386 byte region @ 0x00007efc359fd470 allocated by 0x00007efc3f80e508
  72 byte region @ 0x00007efc35e4d570 allocated by 0x00007efc3f80e508
8208 byte region @ 0x00007efc359fd840 allocated by 0x00007efc3f80e508
4112 byte region @ 0x00007efc3592ded0 allocated by 0x00007efc3f80e508
3000 byte region @ 0x00007efc357ee5c0 allocated by 0x00007efc3f4e1278
  32 byte region @ 0x00007efc351be6d0 allocated by 0x00007efc3f80e508
  16 byte region @ 0x00007efc359de790 allocated by 0x00007efc3f80e508
1036 byte region @ 0x00007efc3524f080 allocated by 0x00007efc3f80e508
 512 byte region @ 0x00007efc357ff290 allocated by 0x00007efc3f80e508
 360 byte region @ 0x00007efc357ef360 allocated by 0x00007efc3f80e508
  24 byte region @ 0x00007efc357ff4e0 allocated by 0x00007efc3f80e508
```

명령	설명
clear memory tracking	현재 수집된 모든 정보를 지웁니다.
memory tracking	메모리 추적을 사용합니다.

show memory webvpn

WebVPN에 대한 메모리 사용량 통계를 생성하려면 **show memory webvpn** 명령을 사용합니다.

show memory webvpn [**allobjects** | **blocks** | **dumpstate** *filename* | **pools** | **usedobjects**]

show memory webvpn profile [**clear** | **dump** *filename* | **start** | **stop**]

allobjects	풀에 대한 WebVPN 메모리 소비 정보, 블록, 사용된 모든 개체 및 사용 가능한 모든 개체를 표시합니다.
blocks	메모리 블록에 대한 WebVPN 메모리 소비 정보를 표시합니다.
clear	WebVPN 메모리 프로필을 지웁니다.
dump*filename*	WebVPN 메모리 프로필을 지정된 파일에 저장합니다. 파일 이름은 disk0:, disk1:, flash:, ftp:, tftp:일 수 있는 위치를 포함해야 합니다.
dumpstate*filename*	WebVPN 메모리 상태를 지정된 파일에 저장합니다. 파일 이름은 disk0:, disk1:, flash:, ftp:, tftp:일 수 있는 위치를 포함해야 합니다.
풀	메모리 풀에 대한 WebVPN 메모리 소비 정보를 표시합니다.
profile	WebVPN 메모리 프로필을 가져와 파일에 배치합니다.
start	WebVPN 메모리 프로필 수집을 시작합니다.
stop	WebVPN 메모리 프로필 가져오기를 중지합니다.
usedobjects	사용된 개체에 대한 WebVPN 메모리 소비 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show memory webvpn allobjects** 명령의 샘플 출력입니다.

```
> show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
```

```
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

show mfib

Multicast Forwarding Information Base에서 정보를 표시하려면 **show mfib** 명령을 사용합니다.

show mfib [*source_or_group* [*group*]] [**cluster** | **count** | **verbose**]

show mfib [**active** [*kbps*] | **cluster-stats** | **interface** | **status** | **summary**]

show mfib reserved [**active** [*kbps*] | **cluster** | **count** | **verbose**]

[**active** [*kbps*]	(선택 사항) 활성 멀티캐스트 소스를 표시합니다. 이 값보다 크거나 같은 멀티캐스트 스트림을 표시하려면 초당 킬로비트 제한을 지정할 수 있습니다. 기본값은 4이며 범위는 0-4294967295입니다.
클러스터	(선택 사항) MFIB epoch 수 및 현재 타이머 값을 표시합니다. 소스 및 그룹을 모두 지정할 경우 **cluster**를 지정할 수 없습니다.
cluster-stats	(선택 사항) MFIB 클러스터 동기화 통계를 표시합니다.
count	(선택 사항) MFIB 경로 및 패킷 수 데이터를 표시합니다. 이 명령은 패킷 삭제 통계를 표시합니다.
interface	(선택 사항) MFIB 프로세스와 관련된 인터페이스에 대한 패킷 통계를 표시합니다.
reserved	(선택 사항) 224.0.0.0 - 224.0.0.225의 범위에서 예약된 그룹에 대한 MFIB 항목을 표시합니다.
source_or_group [*group*]	(선택 사항) 소스 또는 그룹 IPv4, IPv6 또는 이름입니다. 두 가지를 모두 지정하는 경우, 소스를 처음에 지정합니다. 소스 주소는 유니캐스트 주소입니다.
status	(선택 사항) 일반 MFIB 컨피그레이션 및 운영 상태를 표시합니다.
요약	(선택 사항) MFIB 항목 및 인터페이스 수에 대한 요약 정보를 표시합니다.
verbose	(선택 사항) 전달 항목 및 인터페이스에 대한 자세한 정보를 표시합니다.

선택적 인수 없이 모든 그룹에 대한 정보가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show mfib** 명령의 샘플 출력입니다.

```
> show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

다음은 **show mfib verbose** 명령의 샘플 출력입니다.

```
> show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

다음은 **show mfib count** 명령의 샘플 출력입니다.

```
> show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

다음은 **show mfib active** 명령의 샘플 출력입니다. 출력은 PPS 비율의 양수 또는 음수 중 하나를 표시합니다. RPF 패킷이 실패하거나 라우터에서 인터페이스 출력(OIF) 목록이 있는 RPF 패킷을 발견한

경우에는 이 명령에서 음수를 표시합니다. 이 활동 유형은 멀티캐스트 라우팅 문제를 나타낼 수 있습니다.

```
> show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

다음 예는 **show mfib interface** 명령의 샘플 출력입니다.

```
> show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

다음은 **show mfib status** 명령의 샘플 출력입니다.

```
> show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

다음은 **show mfib summary** 명령의 샘플 출력입니다.

```
> show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

다음은 **show mfib reserved** 명령의 샘플 출력입니다.

```
> show mfib reserved
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
```

```
dmz Flags: IC
inside Flags: IC
```

명령	설명
clear mfib counters	MFIB 라우터 패킷 카운터를 지웁니다.
show mroute active	활성 멀티캐스트 스트림을 표시합니다.
show mroute count	멀티캐스트 경로 카운터를 표시합니다.
show mroute summary	멀티캐스트 라우팅 테이블 요약 정보를 표시합니다.

show mode

시스템에 대한 보안 상황 모드를 표시하려면 **show mode** 명령을 사용합니다.

show mode

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

Firepower Threat Defense 디바이스는 단일 상황만 지원합니다. 다중 상황 모드는 지원되지 않습니다.

다음 예에서는 보안 상황 모드를 표시하는 방법을 보여줍니다.

```
> show mode
Security context mode: single
```

show model

디바이스의 하드웨어 모델을 표시하려면 **show model** 명령을 사용합니다.

show model

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 디바이스 모델을 보여줍니다.

```
> show model
Cisco ASA5516-X Threat Defense
```

명령	설명
show serial-number	디바이스 일련 번호를 표시합니다.
show version	소프트웨어 및 기타 디바이스 버전 정보를 표시합니다.

show module

Firepower Threat Defense 디바이스에 설치된 모듈에 대한 정보를 표시하려면 사용자 EXEC 모드에서 **show module** 명령을 사용합니다.

show module [*id* [**details** | **recover** | **log console**]] | **all**]

all	(기본값) 모든 모듈에 대한 정보를 표시합니다. 이는 기본값입니다.
details	(선택 사항) 모듈에 대한 원격 관리 컨피그레이션을 비롯한 추가 정보를 표시합니다.
id	모듈 ID를 지정합니다. 사용 가능한 슬롯 번호(일반적으로 0과 1)를 보려면 파라미터 없이 show module 명령을 사용합니다.
log console	(선택 사항) 모듈에 대한 로그 정보를 표시합니다. 이 옵션은 모든 모듈에서 유효하지는 않을 수 있습니다.
recover	(선택 사항) 모듈 복구를 위한 설정을 표시합니다.

기본적으로 모든 모듈에 대한 정보가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 Firepower Threat Defense 디바이스에 설치된 모듈에 대한 정보를 표시합니다. Firepower Threat Defense 자체도 화면(슬롯 0)에 모듈로 나타납니다. 디바이스 지원 추가 모듈이 디바이스 모델에 따라 다른지 여부입니다.

show module details 명령의 출력은 설치된 모듈에 따라 다릅니다.

소프트웨어 모듈을 구성할 수 있는 모델의 경우 **show module** 명령은 가능한 모든 모듈을 나열합니다. 상태 정보는 그 중 하나가 설치되어 있는지 여부를 나타냅니다.

다음 샘플 출력은 ASA 5516-X를 실행하는 Firepower Threat Defense 소프트웨어에 사용됩니다. 이 디바이스의 경우, Firepower Threat Defense가 모든 소프트웨어 모듈을 지원하지는 않으므로, 슬롯 1을 알 수 없는 경우가 일반적입니다.

```
> show module

Mod  Card Type                                    Model              Serial No.
---- ------------------------------------------- ------------------ -----------
   0 ASA 5516-X with FirePOWER services, 8GE, AC, ASA5516            JAD1939056I
   1 Unknown                                     N/A                JAD1939056I

Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 84b2.61b1.92be to 84b2.61b1.92c6  1.0          1.1.3        97.1(0)60
   1 84b2.61b1.92bd to 84b2.61b1.92bd  N/A          N/A

Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- ------------------------
   1 Unknown                        No Image Present Not Applicable

Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
   1 Unresponsive       Not Applicable
```

다음 표에서 출력에 나열된 각 필드에 대한 설명이 나와 있습니다.

표 ***40: show module*** 출력 필드

필드	설명
Mod	모듈 번호(0 또는 1)입니다.
Card Type	카드 유형입니다. 모듈 0에 표시된 디바이스의 유형은 플랫폼 모델입니다. 슬롯 1의 경우, 추가 모듈이 될 수 있습니다(있는 경우).
Model	이 모듈의 모델 번호입니다.
반납 제품의	일련 번호입니다.
MAC Address Range	이 모듈의 인터페이스에 대한 MAC 주소 범위입니다.
Hw Version	하드웨어 버전입니다.
Fw Version	펌웨어 버전입니다.
Sw Version	소프트웨어 버전입니다. 이는 Firepower Threat Defense 버전이 아닙니다. 대신, Firepower Threat Defense 소프트웨어의 구성 요소인 ASA 소프트웨어 버전입니다. Firepower Threat Defense 버전을 보려면 **show version** 명령을 사용합니다.

필드	설명
SSM Application Name	보안 서비스 모듈에서 실행되는 애플리케이션의 이름입니다.
SSM Application Version	보안 서비스 모듈에서 실행되는 애플리케이션의 버전입니다.
상태	모듈 0에 있는 디바이스의 경우 상태는 Up Sys입니다. 슬롯 1에 있는 모듈의 상태는 다음 중 하나일 수 있습니다. • Initializing - 모듈을 감지하는 중이며, 디바이스에서 제어 통신을 초기화하는 중입니다. • Up - 모듈에서 디바이스에 의한 초기화를 완료했습니다. • Unresponsive - 이 모듈과 통신하는 동안 디바이스에서 오류가 발생했습니다. • Reloading - 모듈을 다시 로드하는 중입니다. • Shutting Down - 모듈을 종료하는 중입니다. • Down - 모듈이 종료되었습니다. • Recover - 모듈에서 복구 이미지를 다운로드하는 중입니다. • No Image Present - 모듈 소프트웨어가 설치되어 있지 않습니다.
Data Plane Status	데이터 평면의 현재 상태입니다.
호환성	나머지 디바이스에 상대적인 모듈의 호환성입니다.

show monitor-interface

장애 조치를 위해 모니터링되는 인터페이스에 대한 정보를 표시하려면 **show monitor-interface** 명령을 사용합니다.

show monitor-interface

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

인터페이스에 둘 이상의 IPv6 주소가 구성되어 있을 수 있으므로 링크-로컬 주소만 **show monitor-interface** 명령에 표시됩니다. 인터페이스에 IPv4 주소와 IPv6 주소가 둘 다 구성된 경우 두 주소 모두 출력에 표시됩니다. 인터페이스에 구성된 IPv4 주소가 없는 경우 IPv4 주소는 출력에 0.0.0.0으로 표시됩니다. 인터페이스에 구성된 IPv6 주소가 없는 경우 이 주소는 출력에서 생략됩니다.

모니터링되는 대체작동 인터페이스의 상태는 다음과 같습니다.

- Unknown - 초기 상태입니다. 이 상태는 상태를 확인할 수 없음을 의미할 수도 있습니다.
- Normal - 인터페이스를 트래픽을 받는 중입니다.
- Normal (Waiting) - 인터페이스가 작동하지만 피어 디바이스의 해당 인터페이스에서 hello 패킷을 아직 받지 않았습니다. 인터페이스에 대해 대기 IP 주소가 구성되어 있는지, 그리고 두 인터페이스가 연결되어 있는지 확인하십시오.
- Testing - 다섯 번의 폴링 시간 동안 인터페이스에 Hello 메시지가 수신되지 않았습니다.
- Link Down - 관리자가 인터페이스 또는 VLAN을 중단했습니다.
- No Link - 인터페이스에 대한 물리적 링크가 중단되었습니다.
- Failed - 인터페이스에 수신된 트래픽이 없지만 피어 인터페이스에는 트래픽이 수신되었습니다.

다음은 **show monitor-interface** 명령의 샘플 출력입니다.

```
> show monitor-interface

This host: Primary - Active
                Interface outside (10.86.94.88): Normal (Waiting)
                Interface management (192.168.1.1): Normal (Waiting)
                Interface failif (0.0.0.0/fe80::223:4ff:fe77:fed): Normal (Waiting)
        Other host: Secondary - Failed
                Interface outside (0.0.0.0): Unknown (Waiting)
```

```
Interface management (0.0.0.0): Unknown (Waiting)
Interface failif (0.0.0.0): Unknown (Waiting)
```

show mrib client

MRIB 클라이언트 연결에 대한 정보를 표시하려면 **show mrib client** 명령을 사용합니다.

show mrib client [**filter**] [**name** *client_name*]

필터	(선택 사항) 클라이언트 필터를 표시합니다. 각 클라이언트에서 소유한 MRIB 플래그 및 각 클라이언트와 관련된 플래그에 대한 정보를 보는 데 사용됩니다.
name*client_name*	(선택 사항) MRIB의 클라이언트로 작동하는 멀티캐스트 라우팅 프로토콜(PIM 또는 IGMP)의 이름입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

filter 옵션은 여러 MRIB 클라이언트에서 등록한 경로 및 인터페이스 수준 플래그 변경 사항을 표시하는 데 사용됩니다. 또한 이 명령 옵션은 MRIB 클라이언트가 소유한 플래그도 표시합니다.

다음은 **show mrib client** 명령(**filter** 키워드 사용)의 샘플 출력입니다.

```
> show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
```

```
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

명령	설명
show mrib route	MRIB 테이블 항목을 표시합니다.

show mrib route

MRIB 테이블을 표시하려면 **show mrib route** 명령을 사용합니다.

show mrib route [[[*source* | *****] [*group*[/*prefix-length*]]] | **summary**]

*	(선택 사항) 공유 트리 항목을 표시합니다.
/*prefix-length*	(선택 사항) MRIB 경로의 접두사 길이입니다. 접두사(주소의 네트워크 부분)를 구성하는 상위 연속 비트 수를 나타내는 10진수 값입니다. 10진수 값 앞에 슬래시가 표시되어야 합니다.
group	(선택 사항) 그룹의 IP 주소 또는 이름입니다.
source	(선택 사항) 경로 소스의 IP 주소 또는 이름입니다.
요약	MRIB 테이블 항목에 대한 요약을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

MFIB 테이블에는 MRIB에서 업데이트된 항목 및 플래그의 하위 집합이 유지됩니다. 플래그는 멀티캐스트 패킷에 대한 전달 규칙 집합에 따라 전달 및 신호 처리 동작을 결정합니다.

인터페이스 및 플래그 목록 외에 각 경로 항목에 여러 카운터가 표시됩니다. 바이트 수는 전달된 총 바이트 수입니다. 패킷 수는 이 항목에 대해 수신된 패킷 수입니다. **show mfib count** 명령은 경로에 독립적인 전역 카운터를 표시합니다.

다음은 **show mrib route** 명령의 샘플 출력입니다.

```
> show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
```

```
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

명령	설명
show mfib count	MFIB 테이블의 경로 및 패킷 수 데이터를 표시합니다.

show mroute

IPv4 멀티캐스트 라우팅 테이블을 표시하려면 **show mroute** 명령을 사용합니다.

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

active*rate*	(선택 사항) 활성 멀티캐스트 소스만 표시합니다. 활성 소스는 지정된 *rate* 이상으로 전송하는 소스입니다. *rate*를 지정하지 않은 경우에는 4kbps 이상의 속도로 전송하는 소스가 활성 소스입니다.
count	(선택 사항) 패킷 수, 초당 패킷 수, 평균 패킷 크기, 초당 비트 수 등 그룹 및 소스에 대한 통계를 표시합니다.
group	(선택 사항) DNS 호스트 테이블에 정의된 멀티캐스트 그룹의 IP 주소 또는 이름입니다.
pruned	(선택 사항) 정리된 경로를 표시합니다.
reserved	(선택 사항) 예약된 그룹을 표시합니다.
source	(선택 사항) 소스 호스트 이름 또는 IP 주소입니다.
summary	(선택 사항) 멀티캐스트 라우팅 테이블의 각 항목에 대한 한 줄로 요약된 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show mroute 명령은 멀티캐스트 라우팅 테이블의 내용을 표시합니다. 디바이스는 PIM 프로토콜 메시지, IGMP 보고서 및 트래픽을 기반으로 (S,G) 및 (*,G) 항목을 생성하여 멀티캐스트 라우팅 테이블을 채웁니다. 별표(*)는 모든 소스 주소를 나타내고, "S"는 단일 소스 주소를 나타내며, "G"는 대상 멀티캐스트 그룹 주소입니다. (S, G) 항목을 생성할 때 소프트웨어는 유니캐스트 라우팅 테이블에서 발견한(RPF를 통해) 해당 대상 그룹에 대한 최상의 경로를 사용합니다.

실행 중인 컨피그레이션에서 **mroute** 명령을 보려면 **show running-config mroute** 명령을 사용합니다.

다음은 **show mroute** 명령의 샘플 출력입니다.

```
> show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

다음 필드가 **show mroute** 출력에 표시됩니다.

- Flags - 항목에 대한 정보를 제공합니다.
  - D-Dense. 항목이 덴스 모드로 작동하는 중입니다.
  - S-Sparse. 항목이 스파스 모드로 작동하는 중입니다.
  - B-Bidir Group. 멀티캐스트 그룹이 양방향 모드로 작동 중임을 나타냅니다.
  - s-SSM Group. 멀티캐스트 그룹이 IP 주소의 SSM 범위 내에 있음을 나타냅니다. 이 플래그는 SSM 범위가 변경되면 재설정됩니다.
  - C-Connected. 멀티캐스트 그룹의 멤버가 직접 연결된 인터페이스에 있습니다.
  - L-Local. 디바이스 자체가 멀티캐스트 그룹의 멤버입니다. 그룹은 igmp join-group 명령을 통해 로컬로 조인됩니다(구성된 그룹의 경우).
  - I-Received Source Specific Host Report. (S, G) 항목이 (S, G) 보고서에 의해 생성되었음을 나타냅니다. 이 (S, G) 보고서는 IGMP에 의해 생성되었을 수 있습니다. 이 플래그는 DR에서만 설정됩니다.
  - P-Pruned. 경로가 정리되었습니다. 소프트웨어는 다운스트림 멤버가 소스에 조인할 수 있도록 이 정보를 유지합니다.
  - R-RP-bit set. (S, G) 항목이 RP 쪽을 가리키고 있음을 나타냅니다.
  - F-Register flag. 소프트웨어가 멀티캐스트 소스에 등록 중임을 나타냅니다.
  - T-SPT-bit set. 패킷이 최단 경로 소스 트리에 수신되었음을 나타냅니다.

◦ J-Join SPT. (*, G) 항목의 경우 공유 트리 아래에 흐르는 트래픽 속도가 그룹에 대해 설정된 SPT-Threshold를 초과함을 나타냅니다. (기본 SPT-Threshold 설정은 0kbps임) J - Join shortest path tree(SPT) 플래그가 설정된 경우 공유 트리 아래에 수신된 다음 (S, G) 패킷이 소스 방향으로 (S, G) 조인을 트리거하여 디바이스가 소스 트리에 조인하도록 합니다.

(S, G) 항목의 경우 그룹에 대한 SPT-Threshold를 초과하여 항목이 생성되었음을 나타냅니다. J - Join SPT 플래그가 (S, G) 항목에 설정된 경우 디바이스는 소스 트리에서 트래픽 속도를 모니터링하여 소스 트리의 트래픽 속도가 그룹에 대해 설정된 SPT-Threshold보다 1분 이상 낮게 유지되는 경우 이 소스에 대한 공유 트리로 다시 전환합니다.

참고 디바이스는 공유 트리에서 트래픽 속도를 측정하여 측정된 속도를 1초에 한 번씩 그룹의 SPT-Threshold와 비교합니다. 트래픽 속도가 SPT-Threshold를 초과하는 경우에는 다음에 트래픽 속도를 측정할 때까지 J - Join SPT 플래그가 (*, G) 항목에 설정되어 있습니다. 다음 패킷이 공유 트리에 도착하고 새 특정 간격이 시작되면 플래그가 지워집니다.

기본 SPT-Threshold 값인 0kbps가 그룹에 사용되는 경우에는 J - Join SPT 플래그가 항상 (*, G) 항목에 설정되고 지워지지 않습니다. 기본 SPT-Threshold 값이 사용되는 경우 디바이스는 새 소스의 트래픽이 수신될 때 최단 경로 소스 트리로 즉시 전환됩니다.

- Timers:Uptime/Expires - Uptime은 인터페이스별로 항목이 IP 멀티캐스트 라우팅 테이블에 유지된 기간(시간, 분, 초)을 나타냅니다. Expires는 인터페이스별로 항목이 IP 멀티캐스트 라우팅 테이블에서 제거될 때까지의 기간(시간, 분, 초)을 나타냅니다.
- Interface state - 들어오거나 나가는 인터페이스의 상태를 나타냅니다.
  - Interface - 들어오거나 나가는 인터페이스 목록에 나열된 인터페이스 이름입니다.
  - State - 액세스 목록 또는 TTL(Time to Live) 임계값으로 인한 제한이 있는지 여부에 따라 패킷이 전달 또는 정리되거나 인터페이스에서 null로 유지됨을 나타냅니다.
- (*, 239.1.1.40) 및 (* , 239.2.2.1) - IP 멀티캐스트 라우팅 테이블의 항목입니다. 항목은 소스의 IP 주소와 그 뒤에 오는 멀티캐스트 그룹의 IP 주소로 구성됩니다. 소스 위치의 별표(*)는 모든 소스를 나타냅니다.
- RP - RP의 주소입니다. 스파스 모드에서 작동하는 라우터 및 액세스 서버의 경우 이 주소는 항상 224.0.0.0입니다.
- Incoming interface - 소스의 멀티캐스트 패킷에 필요한 인터페이스입니다. 이 인터페이스에 수신되지 않은 패킷은 삭제됩니다.
- RPF nbr - 소스에 대한 업스트림 라우터의 IP 주소입니다.

• Outgoing interface list - 전달되는 패킷이 통과하는 인터페이스입니다.

명령	설명
show running-config mroute	구성된 멀티캐스트 경로를 표시합니다.

show nameif

인터페이스의 논리적 이름을 보려면 **show nameif** 명령을 사용합니다.

show nameif [*physical_interface*[**.***subinterface*] | **zone**]

physical_interface	(선택 사항) 인터페이스 ID(예: **gigabitethernet0/1**)를 식별합니다.
subinterface	(선택 사항) 논리적 하위 인터페이스를 지정하는 1에서 4294967293 사이의 정수를 식별합니다.
zone	(선택 사항) 영역 이름을 표시합니다. 이 정보는 Firepower Threat Defense에 대해 유효하지 않습니다.

인터페이스를 지정하지 않은 경우 이 명령에서 모든 인터페이스 이름을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

인터페이스에 할당된 이름을 표시하려면 이 명령을 사용합니다. 인터페이스는 임의의 구성 설정 내에서 사용하도록 이름이 지정되어야 합니다.

명령은 보안 레벨을 표시하고 선택적으로 영역 정보를 표시하지만 둘 다 Firepower Threat Defense에 대해 유효하지 않습니다. 보안 레벨은 항상 0이며 영역 정보는 항상 비어 있습니다. 어떤 보안 영역이 각 인터페이스를 포함하는지 확인하려면 디바이스 관리자를 사용합니다.

다음은 **show nameif** 명령의 샘플 출력입니다.

```
> show nameif
Interface                  Name                       Security
GigabitEthernet1/1         outside                      0
GigabitEthernet1/2         inside1_2                    0
GigabitEthernet1/3         inside1_3                    0
GigabitEthernet1/4         inside1_4                    0
GigabitEthernet1/5         inside1_5                    0
GigabitEthernet1/6         inside1_6                    0
```

```
GigabitEthernet1/7       inside1_7                 0
GigabitEthernet1/8       inside1_8                 0
Management1/1            diagnostic                0
BVI1                     inside                    0
```

show nat

NAT 정책의 통계를 표시하려면 **show nat** 명령을 사용합니다.

show nat [**interface** *name*] [*ip_addr* [*mask*] | {**object** | **object-group**} *name*] [**translated** [**interface** *name*] {*ip_addr* [*mask*] | {**object** | **object-group**} *name*}] [**detail**]

detail	(선택 사항) 개체 필드의 자세한 정보 표시 확장을 포함합니다.
interface*name*	(선택 사항) 소스 인터페이스를 지정합니다.
ip_addr [*mask*]	(선택 사항) IP 주소 및 서브넷 마스크를 지정합니다.
object*name*	(선택 사항) 네트워크 개체 또는 서비스 개체를 지정합니다.
object-group*name*	(선택 사항) 네트워크 개체 그룹을 지정합니다.
translated	(선택 사항) 변환된 파라미터를 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show nat 명령을 사용하여 NAT 정책의 런타임 표현을 표시할 수 있습니다. **detail** 선택적 키워드를 사용하여 개체를 확장하고 개체 값을 확인할 수 있습니다. 추가 선택기 필드를 사용하여 **show nat** 명령 출력을 제한할 수 있습니다.

출력은 모든 NAT 명령, 숨겨진 명령을 보여줍니다. 예를 들어, 데이터 인터페이스를 게이트웨이로 사용하기 위해 관리 인터페이스를 구성하는 경우, 관리 인터페이스와 각 데이터 인터페이스 간의 통신을 활성화하기 위해 숨겨진 NAT 규칙이 숨겨진 가상 인터페이스(예를 들어, nlp_int_tap)용으로 구성됩니다. 이 규칙은 Firepower Device Manager에 있는 NAT 테이블에 반영되지 않습니다. 또한 데이터 인터페이스에 대한 관리 연결을 허용하는 HTTPS/SSH 관리 액세스 규칙에 대해 숨겨진 규칙을 확

인할 수 있습니다. 이 규칙은 Firepower Device Manager의 관리 액세스 테이블에는 반영되지만 NAT 테이블에는 반영되지 않습니다.

다음은 **show nat** 명령의 샘플 출력입니다.

```
> show nat
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0

> show nat detail
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.2/32, Mapped: 2.2.2.3/32
       Destination - Real: 10.10.10.0/24, Mapped: 20.20.20.0/24

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.1/32, Mapped: 2.2.2.2/32

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 11.11.11.10-11.11.11.11, Mapped: 192.168.10.10/32
       Destination - Real: 192.168.1.0/24, Mapped: 10.75.1.0/24
       Service - Real: tcp source eq 10 destination eq ftp-data , Mapped: tcp source eq
       100 destination eq 200
```

다음은 IPv6와 IPv4 사이의 **show nat detail** 명령의 샘플 출력입니다.

```
> show nat detail
1 (in) to (outside) source dynamic inside_nw outside_map destination static inside_map any
translate_hits = 0, untranslate_hits = 0
Source - Origin: 2001::/96, Translated: 192.168.102.200-192.168.102.210
Destination - Origin: 2001::/96, Translated: 0.0.0.0/0
```

명령	설명
clear nat counters	NAT 정책 카운터를 지웁니다.

show nat divert-table

NAT 전환 테이블의 통계를 표시하려면 **show nat divert-table** 명령을 사용합니다.

show nat divert-table [**ipv6**] [**interface** *interface_name*]

divert-table	NAT 전환 테이블을 표시합니다.
ipv6	(선택 사항) 전환 테이블에서 IPv6 항목을 표시합니다.
interface*interface_name*	(선택 사항) 지정된 소스 인터페이스로 출력을 제한합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show nat divert-table 명령을 사용하여 NAT 전환 테이블의 런타임 표현을 표시할 수 있습니다. **ipv6** 선택적 키워드를 사용하여 전환 테이블에서 IPv6 항목을 확인할 수 있습니다. **interface** 선택적 키워드를 사용하여 특정 소스 인터페이스에 대한 NAT 전환 테이블을 확인할 수 있습니다.

전환 테이블은 숨겨진 명령을 포함하여 모든 NAT 명령을 보여줍니다. 예를 들어, 데이터 인터페이스를 게이트웨이로 사용하기 위해 관리 인터페이스를 구성하는 경우, 관리 인터페이스와 각 데이터 인터페이스 간의 통신을 활성화하기 위해 숨겨진 NAT 규칙이 숨겨진 가상 인터페이스(예를 들어, nlp_int_tap)용으로 구성됩니다. 이 규칙은 Firepower Device Manager에 있는 NAT 테이블에 반영되지 않습니다.

다음은 **show nat divert-table** 명령의 샘플 출력입니다.

```
> show nat divert-table
Divert Table
id=0xad1521b8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.119.255, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1523a8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.116.0, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
```

```
id=0xad1865c0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad1867b0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.0.0, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad257bf8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.255, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
id=0xad257db8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.0, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
```

다음은 **show nat divert ipv6** 명령의 샘플 출력입니다.

```
> show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

명령	설명
clear nat counters	NAT 정책 카운터를 지웁니다.
show nat	NAT 정책의 런타임 표현을 표시합니다.

show nat pool

NAT 풀 사용 통계를 표시하려면 **show nat pool** 명령을 사용합니다.

show nat pool [**cluster**]

cluster	(선택 사항) 클러스터링이 활성화된 경우 소유자 유닛 및 백업 유닛에 대한 현재 PAT 주소 할당을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

NAT 풀은 매핑된 각 프로토콜/IP 주소/포트 범위에 대해 생성됩니다. 여기서 포트 범위는 기본적으로 1~511, 512~1023 및 1024~65535입니다. 포트의 균일한 범위를 사용하기 위해 PAT 풀을 구성하는 경우, 더 적은 수의 큰 범위를 볼 수 있습니다.

각 NAT 풀은 마지막으로 사용한 후 최소 10분간 존재합니다. **clear xlate**를 사용하여 변환을 지운 경우 10분 유지 타이머가 취소됩니다.

다음은 **show running-config object network** 명령을 통해 표시되는 동적 PAT 규칙에 의해 생성된 NAT 풀의 샘플 출력입니다.

```
> show running-config object network
object network myhost
 host 10.10.10.10
 nat (pppoe2,inside) dynamic 10.76.11.25

> show nat pool
TCP inside, address 10.76.11.25, range 1-511, allocated 0
TCP inside, address 10.76.11.25, range 512-1023, allocated 0
TCP inside, address 10.76.11.25, range 1024-65535, allocated 1
```

다음은 **show nat pool** 명령의 샘플 출력으로, PAT 풀 **flat** 옵션 사용을 보여줍니다. **include-reserve** 키워드가 없으면 두 개의 범위가 표시됩니다. 둘 중 낮은 범위는 1024 미만의 소스 포트가 동일한 포트에 매핑된 경우에 사용됩니다.

```
> show nat pool
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
```

```
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
```

다음은 **show nat pool** 명령의 샘플 출력으로, PAT 풀 **flatinclude-reserve** 옵션 사용을 보여줍니다.

```
> show nat pool
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
```

다음은 **show nat pool** 명령의 샘플 출력으로, PAT 풀 **extended flat include-reserve** 옵션 사용을 보여줍니다. 중요한 항목은 괄호 안의 주소입니다. 이는 PAT를 확장하는 데 사용되는 목적지 주소입니다.

```
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
TCP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
UDP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535,
allocated 1
TCP PAT pool outside:dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535,
allocated 2
UDP PAT pool outside:dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
```

명령	설명
show nat	NAT 정책 통계를 표시합니다.

show nat proxy-arp

NAT 프록시 ARP 테이블을 표시하려면 **show nat proxy-arp** 명령을 사용합니다.

show nat proxy-arp [**ipv6**] [**interface** *name*]

ipv6	(선택 사항) 프록시 ARP 테이블에서 IPv6 항목을 표시합니다.
interface*name*	(선택 사항) 지정된 소스 인터페이스로 출력을 제한합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show nat proxy-arp 명령을 사용하여 NAT 프록시 ARP 테이블의 런타임 표현을 표시할 수 있습니다.

프록시 ARP 테이블은 숨겨진 명령을 포함하여 모든 NAT 명령을 보여줍니다. 예를 들어, 데이터 인터페이스를 게이트웨이로 사용하기 위해 관리 인터페이스를 구성하는 경우, 관리 인터페이스와 각 데이터 인터페이스 간의 통신을 활성화하기 위해 숨겨진 NAT 규칙이 숨겨진 가상 인터페이스(예를 들어, nlp_int_tap)용으로 구성됩니다. 이 규칙은 Firepower Device Manager에 있는 NAT 테이블에 반영되지 않습니다.

다음은 **show nat proxy-arp** 명령의 샘플 출력입니다.

```
> show nat proxy-arp
Nat Proxy-arp Table
id=0x00007f4ce491a010, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_8) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc6138d0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_7) to (outside) source dynamic any-ipv4 interface
id=0x00007f4ce491d2e0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_6) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc618a10, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_5) to (outside) source dynamic any-ipv4 interface
id=0x00007f4d019c9e70, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_4) to (outside) source dynamic any-ipv4 interface
id=0x00007f4cdc61b300, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_3) to (outside) source dynamic any-ipv4 interface
```

```
id=0x00007f4ce49261f0, ip/id=0.0.0.0, mask=255.255.255.255 ifc=outside
        config:(inside1_2) to (outside) source dynamic any-ipv4 interface
```

명령	설명
clear nat counters	NAT 정책 카운터를 지웁니다.
show nat	NAT 정책의 런타임은 표현을 표시합니다.

show network

관리 인터페이스의 속성을 표시하려면 **show network** 명령을 사용합니다.

show network

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

사용자가 **configure network** 명령을 사용하여 설정한 관리 인터페이스 속성을 표시하려면 이 명령을 사용합니다.

데이터 인터페이스를 게이트웨이로 사용하기 위해 관리 주소를 구성하는 경우 게이트웨이는 "data-interface"로 표시됩니다.

다음은 **show network** 명령의 샘플 출력입니다.

```
> show network
===============[ System Information ]===============
Hostname                  : 5516-x-1
Domains                   : example.com
DNS Servers               : 10.163.47.11
Management port           : 8305
IPv4 Default route
  Gateway                 : 192.168.0.254

======================[ br1 ]=======================
State                     : Enabled
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 84:B2:61:B1:92:BD
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 192.168.0.166
Netmask                   : 255.255.255.0
Broadcast                 : 192.168.0.255
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled
```

show network-dhcp-server

관리 인터페이스에서 DHCP 서버의 상태를 표시하려면 **show network-dhcp-server** 명령을 사용합니다.

show network-dhcp-server

릴리스	수정 사항
6.2	이 명령이 도입되었습니다.

사용 가이드라인

관리 인터페이스에 대한 선택적인 DHCP 서버의 상태를 확인하려면 이 명령을 사용합니다. DHCP 서버를 구성하려면 **configure network ipv4 dhcp-server-enable** 명령을 사용합니다.

출력은 DHCP 서버가 활성화 또는 비활성화될지 여부를 보여줍니다. 출력이 활성화된 경우, 주소 풀을 보여줍니다.

다음 예에서는 DHCP 서버를 구성하는 방법과 서버의 상태를 보여줍니다.

```
> show network-dhcp-server
DHCP Server Disabled
> configure network ipv4 dhcp-server-enable 192.168.45.46 192.168.45.254
DHCP Server Enabled
> show network-dhcp-server
DHCP Server Enabled
192.168.45.46-192.168.45.254
```

명령	설명
configure network ipv4 dhcp-server-enable	관리 인터페이스에서 DHCP 서버를 구성합니다.
configure network ipv4 dhcp-server-disable	관리 인터페이스에서 DHCP 서버를 비활성화합니다.

show network-static-routes

관리 인터페이스에 대해 구성된 고정 경로를 표시하려면 **show network-static-routes** 명령을 사용합니다.

show network-static-routes

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

관리 인터페이스에 대한 고정 경로는 여러 관리 인터페이스를 구성할 때 사용됩니다. 이 경로는 기본 게이트웨이를 포함하지 않습니다. 단일 관리 인터페이스를 사용할 경우, 일반적으로 추가 고정 경로가 없습니다.

이 명령으로 표시되는 경로는 관리 인터페이스에만 적용됩니다. 이 경로는 데이터 인터페이스에는 사용되지 않습니다. 이 경로는 through-the-box 트래픽에는 사용되지 않습니다.

다음 예는 관리 인터페이스에 대한 추가 고정 경로가 없는 경우를 보여줍니다. 기본 게이트웨이는 고유한 경로입니다.

```
> show network-static-routes
No static routes currently configured.
```

다음 예는 고정 경로를 보여줍니다.

```
> show network-static-routes
---------------[ IPv4 Static Routes ]---------------
Interface                : br1
Destination              : 10.1.1.0
Gateway                  : 192.168.0.254
Netmask                  : 255.255.255.0
```

명령	설명
configure network static-routes	관리 인터페이스에 대한 고정 경로를 구성합니다.

show ntp

현재 NTP(Network Time Protocol) 서버 및 컨피그레이션을 표시하려면 **show ntp** 명령을 사용합니다.

show ntp

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 NTP 컨피그레이션을 표시하는 방법을 보여줍니다.

```
> show ntp
NTP Server                : 209.208.79.69
Status                    : Available
Offset                    : -1.614 (milliseconds)
Last Update               : 578 (seconds)

NTP Server                : 45.127.112.2  (clocka.ntpjs.org)
Status                    : Available
Offset                    : -1.355 (milliseconds)
Last Update               : 874 (seconds)

NTP Server                : 198.58.105.63  (ha81.smatwebdesign.com)
Status                    : Not Available
Offset                    : -4.942 (milliseconds)
Last Update               : 369 (seconds)

NTP Server                : 204.9.54.119  (ntp.your.org)
Status                    : Being Used
Offset                    : 0.312 (milliseconds)
Last Update               : 962 (seconds)
```

명령	설명
system support ntp	NTP에 대한 자세한 문제 해결 정보를 표시합니다.

show object-group

개체 그룹 정보 및 관련 적중 횟수(개체 그룹이 네트워크 object-group 유형인 경우)를 표시하려면 **show object-group** 명령을 사용합니다.

show object-group [**network** | **service** | **id** *name*]

id*name*	(선택 사항) 개체 그룹을 이름별로 식별합니다.
network	(선택 사항) 네트워크 유형 개체입니다.
service	(선택 사항) 서비스 유형 개체입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show object-group** 명령의 샘플 출력으로, "Anet"이라는 네트워크 개체 그룹에 대한 정보를 표시합니다.

```
> show object-group id Anet
Object-group network Anet (hitcnt=10)
   Description OBJ SEARCH ALG APPLIED
   network-object 1.1.1.0 255.255.255.0 (hitcnt=4)
   network-object 2.2.2.0 255.255.255.0 (hitcnt=6)
```

다음은 **show object-group** 명령의 샘플 출력으로, 서비스 그룹에 대한 정보를 표시합니다.

```
> show object-group service
object-group service B-Serobj
   description its a service group
   service-object tcp eq bgp
```

명령	설명
clear object-group	지정된 개체 그룹에 대한 네트워크 개체 적중 횟수를 지웁니다.
show access-list	모든 액세스 목록, 관련 확장 액세스 목록 항목 및 적중 횟수를 표시합니다.

show ospf

OSPF 라우팅 프로세스에 대한 일반적인 정보를 표시하려면 **show ospf** 명령을 사용합니다.

show ospf [*pid* [*area_id*]]

area_id	(선택 사항) OSPF 주소 범위와 연계된 영역의 ID입니다.
pid	(선택 사항) OSPF 프로세스의 ID입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ospf** 명령의 샘플 출력으로, 특정 OSPF 라우팅 프로세스에 대한 일반적인 정보를 표시하는 방법을 보여줍니다.

```
> show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

다음은 **show ospf** 명령의 샘플 출력으로, 모든 OSPF 라우팅 프로세스에 대한 일반적인 정보를 표시하는 방법을 보여줍니다.

```
> show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0

 Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
```

```
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

show ospf border-routers

ABR 및 ASBR에 대한 내부 OSPF 라우팅 테이블 항목을 표시하려면 **show ospf border-routers** 명령을 사용합니다.

show ospf border-routers

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ospf border-routers** 명령의 샘플 출력입니다.

```
> show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

show ospf database

OSPF 토폴로지 데이터베이스에 포함된 정보를 표시하려면 **show ospf database** 명령을 사용합니다.

show ospf [*pid* [*area_id*]] **database** [**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**] [*lsid*] [**internal**] [**self-originate** | **adv-router** *addr*]

show ospf [*pid* [*area_id*]] **database database-summary**

addr	(선택 사항) 라우터 주소입니다.
adv-router	(선택 사항) 알림이 전송된 라우터입니다.
area_id	(선택 사항) OSPF 주소 범위와 연계된 영역의 ID입니다.
asbr-summary	(선택 사항) ASBR 목록 요약을 표시합니다.
database	데이터베이스 정보를 표시합니다.
database-summary	(선택 사항) 전체 데이터베이스 요약 목록을 표시합니다.
external	(선택 사항) 지정된 자동 시스템의 외부 경로를 표시합니다.
internal	(선택 사항) 지정된 자동 시스템의 내부 경로입니다.
lsid	(선택 사항) LSA ID입니다.
network	(선택 사항) 네트워크에 대한 OSPF 데이터베이스 정보를 표시합니다.
nssa-external	(선택 사항) 외부 NSSA(Not-So-Stubby-Area) 목록을 표시합니다.
pid	(선택 사항) OSPF 프로세스의 ID입니다.
router	(선택 사항) 라우터를 표시합니다.
self-originate	(선택 사항) 지정된 자동 시스템에 대한 정보를 표시합니다.
summary	(선택 사항) 목록에 대한 요약을 표시합니다.

릴리스	수정 사항
6.1	이 명령을 도입했습니다.

다음은 **show ospf database** 명령의 샘플 출력입니다.

```
> show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

다음은 **show ospf database asbr-summary** 명령의 샘플 출력입니다.

```
> show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

다음은 **show ospf database router** 명령의 샘플 출력입니다.

```
> show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

다음은 **show ospf database network** 명령의 샘플 출력입니다.

```
> show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

다음은 **show ospf database summary** 명령의 샘플 출력입니다.

```
> show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

다음은 **show ospf database external** 명령의 샘플 출력입니다.

```
> show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

show ospf flood-list

인터페이스로 플러딩되기를 기다리는 OSPF LSA 목록을 표시하려면 **show ospf flood-list** 명령을 사용합니다.

show ospf flood-list *interface_name*

interface_name	네이버 정보를 표시할 인터페이스의 이름입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ospf flood-list** 명령의 샘플 출력입니다.

```
> show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

show ospf interface

OSPF 관련 인터페이스 정보를 표시하려면 **show ospf interface** 명령을 사용합니다.

show ospf interface [*interface_name*]

interface_name	(선택 사항) OSPF 관련 정보를 표시할 인터페이스의 이름입니다.

인터페이스를 지정하지 않으면 모든 인터페이스에 대한 OSPF 정보가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ospf interface** 명령의 샘플 출력입니다.

```
> show ospf interface outside
out is up, line protocol is up
  Internet Address 10.0.3.4 mask 255.255.255.0, Area 0
  Process ID 2, Router ID 10.0.3.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 5 msec
    Wait time before Designated router selection 0:00:11
  Index 1/1, flood queue length 0
  Next 0x00000000(0)/0x00000000(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

show ospf neighbor

인터페이스별로 OSPF 인접 항목 정보를 표시하려면 **show ospf neighbor** 명령을 사용합니다.

show ospf neighbor [**detail** | *interface_name* [*nbr_router_id*]]

detail	(선택 사항) 지정된 라우터에 대한 세부사항을 나열합니다.
interface_name	(선택 사항) 네이버 정보를 표시할 인터페이스의 이름입니다.
nbr_router_id	(선택 사항) 인접 라우터의 라우터 ID입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ospf neighbor** 명령의 샘플 출력입니다. 인터페이스별로 OSPF 네이버 정보를 표시하는 방법을 보여 줍니다.

```
> show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

다음은 **show ospf neighbor detail** 명령의 샘플 출력입니다. 지정된 OSPF 네이버에 대한 자세한 정보를 표시하는 방법을 보여 줍니다.

```
> show ospf neighbor detail

Neighbor 25.1.1.60, interface address 15.1.1.60
    In the area 0 via interface inside
    Neighbor priority is 1, State is FULL, 46 state changes
    DR is 15.1.1.62 BDR is 15.1.1.60
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR), last OOB-Resync 00:03:07 ago
    Dead timer due in 0:00:24
```

```
Neighbor is up for 01:42:15
Index 5/5, retransmission queue length 0, number of retransmission 0
First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
```

show ospf nsf

OSPFv2 관련 NSF 정보를 표시하려면 **show ospf nsf** 명령을 사용합니다.

show ospf nsf

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ospf nsf** 명령의 샘플 출력입니다.

```
> show ospf nsf
Routing Process "ospf 10"
Non-Stop Forwarding enabled
    Clustering is not configured in spanned etherchannel mode
IETF NSF helper support enabled
Cisco NSF helper support enabled
    OSPF restart state is
    Handle 1, Router ID 25.1.1.60, checkpoint Router ID 0.0.0.0
    Config wait timer interval 10, timer not running
    Dbase wait timer interval 120, timer not running
```

show ospf request-list

라우터에서 요청한 모든 LSA 목록을 표시하려면 **show ospf request-list** 명령을 사용합니다.

show ospf request-list *nbr_router_id interface_name*

interface_name	네이버 정보를 표시할 인터페이스의 이름입니다. 이 인터페이스에서 라우터가 요청한 모든 LSA 목록을 표시합니다.
nbr_router_id	인접 라우터의 라우터 ID입니다. 이 인접 항목에서 라우터가 요청한 모든 LSA 목록을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ospf request-list** 명령의 샘플 출력입니다.

```
> show ospf request-list 192.168.1.12 inside

         OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

명령	설명
show ospf retransmission-list	재전송 대기 중인 모든 LSA 목록을 표시합니다.

show ospf retransmission-list

특정 네이버 및 인터페이스에 대해 재전송 대기할 모든 LSA 목록을 표시하려면 **show ospf retransmission-list** 명령을 사용합니다.

show ospf retransmission-list *nbr_router_id interface_name*

interface_name	네이버 정보를 표시할 인터페이스의 이름입니다.
nbr_router_id	네이버 라우터의 라우터 ID입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 외부 인터페이스에 있는 192.168.1.11 네이버 라우터에 대한 **show ospf retransmission-list** 명령의 샘플 출력입니다.

```
> show ospf retransmission-list 192.168.1.11 outside

         OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11

  Link state retransmission due in 3764 msec, Queue length 2
  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

명령	설명
show ospf request-list	라우터에서 요청한 모든 LSA 목록을 표시합니다.

show ospf summary-address

OSPF 프로세스 중에 구성된 모든 요약 주소 재배포 정보 목록을 표시하려면 **show ospf summary-address** 명령을 사용합니다.

show ospf summary-address

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ospf summary-address** 명령의 샘플 출력을 보여줍니다. OSPF 프로세스에 대한 요약 주소를 구성하기 전에 ID 5를 사용하여 모든 요약 주소 재배포 정보 목록을 표시하는 방법을 보여 줍니다.

```
> show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

show ospf traffic

특정 OSPF 인스턴스에서 처리된(보내거나 받은) 여러 유형의 패킷 목록을 표시하려면 **show ospf traffic** 명령을 사용합니다.

show ospf traffic

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령을 사용하면 디버깅을 사용하지 않고 처리 중인 여러 유형의 OSPF 패킷에 대한 스냅샷을 가져올 수 있습니다. 두 개의 OSPF 인스턴스가 구성된 경우 **show ospf traffic** 명령은 각 인스턴스의 프로세스 ID를 사용하여 두 인스턴스 모두에 대한 통계를 표시합니다. **show ospf***process_id***traffic** 명령을 사용하여 단일 인스턴스에 대한 통계를 표시할 수도 있습니다.

다음은 **show ospf traffic** 명령의 샘플 출력을 보여줍니다.

```
> show ospf traffic

OSPF statistics (Process ID 70):

       Rcvd: 244 total, 0 checksum errors
             234 hello, 4 database desc, 1 link state req
             3 link state updates, 2 link state acks
       Sent: 485 total
             472 hello, 7 database desc, 1 link state req
             3 link state updates, 2 link state acks
```

명령	설명
show ospf virtual-links	OSPF 가상 링크의 파라미터 및 현재 상태를 표시합니다.

show ospf virtual-links

OSPF 가상 링크의 파라미터 및 현재 상태를 표시하려면 **show ospf virtual-links** 명령을 사용합니다.

show ospf virtual-links

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show ospf virtual-links** 명령의 샘플 출력입니다.

```
> show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

show p - show r

show pager

CLI 세션에 대한 현재 페이지 길이 즉, -- 자세히 보기 -- 표시가 있어 출력이 일시 중지되기 전에 표시된 라인 수에 대한 현재 페이지 길이를 표시하려면 **show pager** 명령을 사용합니다.

show pager

참고 Firepower Threat Defense CLI의 페이지 길이를 설정할 수 없습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show pager** 명령의 샘플 출력입니다. Firepower Threat Defense CLI에서 페이지 길이를 설정할 수 없으므로, 출력은 페이저가 없음을 나타냅니다.

```
> show pager
no pager
```

show parser dump

show parser dump 명령은 내부 또는 Cisco Technical Support에 사용하기 위한 것입니다.

show password encryption

비밀번호 암호화 컨피그레이션 설정을 표시하려면 **show password encryption** 명령을 사용합니다.

show password encryption

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

Firepower Threat Defense에서는 마스터 비밀번호 암호화를 구성할 수 없으므로 이 명령은 항상 비밀번호 암호화가 사용 해제되었으며 마스터 키 해시가 설정되지 않았음을 표시해야 합니다.

키가 저장된 경우 키 해시 옆에 “saved”가 표시됩니다. 키가 없거나 실행 중인 구성에서 키를 제거한 경우 해시 값 대신 “Not set”이 표시됩니다.

다음은 **show password encryption** 명령의 샘플 출력입니다.

```
> show password encryption
Password Encryption: Disabled
Master key hash: Not set(saved)
```

show pclu

show pclu 명령은 내부 또는 Cisco Technical Support에 사용하기 위한 것입니다.

show perfmon

디바이스의 성능에 대한 정보를 표시하려면 **show perfmon** 명령을 사용합니다.

show perfmon [**detail**]

detail	(선택 사항) 추가 통계를 표시합니다. 이러한 통계는 Cisco Unified Firewall MIB의 전역 연결 개체 및 프로토콜별 연결 개체에서 생성된 통계와 일치합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

perfmon 명령은 정의된 간격으로 성능 통계를 지속적으로 표시합니다. **show perfmon** 명령을 사용하면 정보를 즉시 표시할 수 있습니다.

다음은 **show perfmon detail** 명령의 샘플 출력입니다.

```
> show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept        0/s          0/s
SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
```

```
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

명령	설명
perfmon	정의된 간격으로 자세한 성능 모니터링 정보를 표시합니다.

show perfstats

디바이스에 대한 성능 통계를 표시하려면 **show perfstats** 명령을 사용합니다.

show perfstats

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show perfstats 명령은 탐지 엔진에 대한 성능 정보를 보여줍니다. 이 명령은 사용 가능한 엔진 목록을 보여주며 사용자는 확인하고 싶은 통계에 대한 목록을 선택할 수 있습니다. 그런 다음 프로파일 번호가 표시되면 확인하고 싶은 내용에 대한 프로파일을 선택합니다.

이 파일은 Firepower Management Center에서 원격으로 관리하는 시스템인 경우 유효합니다. 이 파일은 일반적으로 로컬 관리자인 Firepower Device Manager를 사용하여 관리하는 시스템에 대한 내용을 포함하지 않습니다.

전체 파일을 확인하고 싶지 않은 경우, Crtl+C를 사용하여 표시를 중지합니다. 파일 내용은 길 수 있습니다.

```
> show perfstats
Available DEs:
  1 - Primary Detection Engine (703006f4-8ff6-11e6-bb6e-8f2d5febf243)
  0 - Cancel and return to CLI

Select a DE to profile: 1
Available now files:
  1 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-13
  2 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-16
  3 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-11
  4 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-15
  5 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-14
  6 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/2016-10-12
  7 - /var/sf/detection_engines/f24ce56c-8ff6-11e6-b914-515e5febf243/instance-1/now
  0 - Cancel and return to DE selection

Select a now file: 7
Mon Oct 17 00:05:00 2016
                 Pkts Recv: 162
                 Pkts Drop: 0
            Block Verdicts: 0
                 Mbits/Sec: 0.001
                 Drop Rate: 0%
                Alerts/Sec: 0
          Total Alerts/Sec: 0
(...remaining content truncated...)
```

show pim bsr-router

BSR(bootstrap router) 정보를 표시하려면 **show pim bsr-router** 명령을 사용합니다.

show pim bsr-router

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show pim bsr-router** 명령의 샘플 출력입니다.

```
> show pim bsr-router
PIMv2 Bootstrap information
This system is a candidate BSR
  Candidate BSR interface GigabitEthernet0/0 is down - BSR messages not originated
  Candidate RP: 4.4.4.1(GigabitEthernet0/0), GigabitEthernet0/0 is down - not advertised
```

show pim df

RP(랑데부 지점) 또는 인터페이스에 대한 양방향 DF "winner"를 표시하려면 **show pim df** 명령을 사용합니다.

show pim df [**winner**] [*rp_address* | *interface_name*]

rp_address	다음 중 하나일 수 있습니다. • DNS(Domain Name System) 호스트 테이블에 정의된 RP의 이름. • RP의 IP 주소. 이는 네 부분의 점으로 구분된 10진수 형식 표기법의 멀티캐스트 IP 주소입니다.
interface_name	물리적 또는 논리적 인터페이스 이름입니다.
winner	(선택 사항) 각 RP의 인터페이스별로 선택된 DF를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 RP 쪽 적용 메트릭도 표시합니다.

다음은 **show pim df** 명령의 샘플 출력입니다.

```
> show pim df
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

그룹-프로토콜 매핑 테이블을 표시하려면 **show pim group-map** 명령을 사용합니다.

show pim group-map [**info-source** | **rp-timers**] [*group*]

group	(선택 사항) 다음 중 하나일 수 있습니다. • DNS 호스트 테이블에 정의된 멀티캐스트 그룹의 이름. • 멀티캐스트 그룹의 IPv4 또는 IPv6 주소.
info-source	(선택 사항) 그룹 범위 정보 소스를 표시합니다.
rp-timers	(선택 사항) 그룹-RP 매핑의 가동 시간 및 만료 타이머를 표시합니다.

모든 그룹에 대한 그룹-프로토콜 매핑을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 RP에 대한 모든 그룹 프로토콜 주소 매핑을 표시합니다. 매핑은 다른 클라이언트를 통해 디바이스에서 학습됩니다.

디바이스의 PIM 구현에는 매핑 테이블에 여러 특수 항목이 있습니다. Auto-rp 그룹 범위는 특별히 sparse-mode 그룹 범위에서 거부됩니다. 또한 SSM 그룹 범위는 sparse-mode에 속하지 않습니다. Link Local 멀티캐스트 그룹(224.0.0.0/24에 의해 정의된 대로 224.0.0.0~224.0.0.225)도 sparse-mode 그룹 범위에서 거부됩니다. 마지막 항목은 지정된 RP를 사용하는 Sparse-Mode의 나머지 모든 그룹을 표시합니다.

다음은 **show pim group-map** 명령의 샘플 출력입니다.

```
> show pim group-map
Group Range      Proto   Client Groups   RP address   Info
```

```
224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

첫 번째 및 두 번째 줄에서 Auto-RP 그룹 범위는 특별히 sparse mode 그룹 범위에서 거부됩니다.

세 번째 줄에서 link-local 멀티캐스트 그룹(224.0.0.0/24에 의해 정의된 대로 224.0.0.0~224.0.0.225)도 sparse mode 그룹 범위에서 거부됩니다.

네 번째 줄에서 PIM-SSM(PIM 소스별 멀티캐스트) 그룹 범위는 232.0.0.0/8에 매핑됩니다.

마지막 항목은 나머지 모든 그룹이 RP 10.10.3.2에 매핑된 sparse mode에 있음을 보여 줍니다.

show pim interface

PIM에 대한 인터페이스 특정 정보를 표시하려면 **show pim interface** 명령을 사용합니다.

show pim interface [*interface_name* | **state-off** | **state-on**]

interface_name	(선택 사항) 인터페이스의 이름입니다. 이 인수를 포함하면 표시되는 정보가 지정된 인터페이스로 제한됩니다.
state-off	(선택 사항) PIM이 사용 해제된 인터페이스를 표시합니다.
state-on	(선택 사항) PIM이 활성화된 인터페이스를 표시합니다.

인터페이스를 지정하지 않으면 모든 인터페이스에 대한 PIM 정보가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

Firepower Threat Defense 디바이스가 PIM 네이버입니다. 따라서 이 명령 출력의 neighbor count 열에 실제 네이버 수보다 하나 많은 값이 표시됩니다.

다음 예에서는 내부 인터페이스에 대한 PIM 정보를 표시합니다.

```
> show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR     DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1      172.16.1.4
```

show pim join-prune statistic

PIM join/prune 어그리게이션 통계를 표시하려면 **show pim join-prune statistic** 명령을 사용합니다.

show pim join-prune statistic [*interface_name*]

interface_name	(선택 사항) 인터페이스의 이름입니다. 이 인수를 포함하면 표시되는 정보가 지정된 인터페이스로 제한됩니다.

인터페이스를 지정하지 않으면 모든 인터페이스에 대한 join/prune 통계가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

clear pim counters 명령을 사용하여 PIM join/prune 통계를 지웁니다.

다음은 **show pim join-prune statistic** 명령의 샘플 출력입니다.

```
> show pim join-prune statistic
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface         Transmitted             Received
             inside   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
          Ethernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet3   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet2   0 /    0 /    0         0 /    0 /    0
```

명령	설명
clear pim counters	PIM 트래픽 카운터를 지웁니다.

show pim neighbor

PIM 인접 테이블에 있는 항목을 표시하려면 **show pim neighbor** 명령을 사용합니다.

show pim neighbor [**count** | **detail**] [*interface*]

interface	(선택 사항) 인터페이스의 이름입니다. 이 인수를 포함하면 표시되는 정보가 지정된 인터페이스로 제한됩니다.
count	(선택 사항) 총 PIM 네이버 수 및 각 인터페이스의 PIM 네이버 수를 표시합니다.
detail	(선택 사항) upstream-detection hello 옵션을 통해 학습된 네이버의 추가 주소를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

자용가이드라인

이 명령은 PIM hello 메시지를 통해 이 라우터에 알려진 PIM 네이버를 확인하는 데 사용됩니다. 또한 이 명령은 인터페이스가 DR(지정된 라우터)임을 나타내고, 인접 항목이 양방향 작업을 수행할 수 있는 경우를 알려 줍니다.

Firepower Threat Defense 디바이스가 PIM 인접 항목입니다. 따라서 Firepower Threat Defense 인터페이스가 이 명령의 출력에 표시됩니다. Firepower Threat Defense 디바이스의 IP 주소는 주소 옆에 별표로 표시됩니다.

다음은 **show pim neighbor** 명령의 샘플 출력입니다.

```
> show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

show pim range-list

PIM에 대한 범위 목록 정보를 표시하려면 **show pim range-list** 명령을 사용합니다.

show pim range-list [**config**] [*rp_address*]

config	PIM CLI 범위 목록 정보를 표시합니다.
rp_address	다음 중 하나일 수 있습니다. • DNS(Domain Name System) 호스트 테이블에 정의된 Rp(랑데부 지점)의 이름. • RP의 IP 주소. 이는 네 부분의 점으로 구분된 10진수 형식 표기법의 멀티캐스트 IP 주소입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 그룹 매핑에 대한 멀티캐스트 전달 모드를 확인하는 데 사용됩니다. 출력에는 범위의 RP(랑데부 지점) 주소(해당되는 경우)도 표시됩니다.

다음은 **show pim range-list** 명령의 샘플 출력입니다.

```
> show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
```

```
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

명령	설명
show pim group-map	그룹-PIM 모드 매핑 및 활성 RP 정보를 표시합니다.

show pim topology

PIM 토폴로지 테이블 정보를 표시하려면 **show pim topology** 명령을 사용합니다.

show pim topology [**reserved** | **route-count** [**detail**] | *group* [*source*]]

reserved	예약된 그룹에 대한 PIM 토폴로지 테이블 정보를 표시합니다.
route-count	PIM 토폴로지 테이블의 경로 수를 표시합니다.
detail	(선택 사항) 그룹별로 보다 자세한 개수 정보를 표시합니다.
group	(선택 사항) 다음 중 하나일 수 있습니다. • DNS 호스트 테이블에 정의된 멀티캐스트 그룹의 이름. • 멀티캐스트 그룹의 IPv4 또는 IPv6 주소.
source	(선택 사항) 다음 중 하나일 수 있습니다. • DNS 호스트 테이블에 정의된 멀티캐스트 소스의 이름. • 멀티캐스트 소스의 IPv4 또는 IPv6 주소.

모든 그룹 및 소스에 대한 토폴로지 정보가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

PIM 토폴로지 테이블을 사용하여 각각 자체 인터페이스 목록이 있는 지정된 그룹 (*, G), (S, G) 및 (S, G)RPT에 대한 여러 항목을 표시할 수 있습니다.

PIM은 멀티캐스트 라우팅 프로토콜(예: PIM), 로컬 멤버십 프로토콜(예: IGMP(Internet Group Management Protocol)) 및 시스템의 멀티캐스트 포워딩 엔진 간의 통신을 중개하는 MRIB를 통해 이러한 항목의 내용을 전달합니다.

MRIB는 지정된 (S, G) 항목에 대해 데이터 패킷을 허용해야 하는 인터페이스 및 데이터 패킷을 전달해야 하는 인터페이스에 표시됩니다. 또한 MFIB(Multicast Forwarding Information Base) 테이블은 전달 중 패킷별 전달 작업을 결정하는 데 사용됩니다.

참고 전달 정보에는 **show mfib route** 명령을 사용합니다.

다음은 **show pim topology** 명령의 샘플 출력입니다.

```
> show pim topology
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

다음은 **show pim topology reserved** 명령의 샘플 출력입니다.

```
> show pim topology reserved
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside            00:02:26  off II

(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside             00:00:48  off II
```

다음은 **show pim topology route-count** 명령의 샘플 출력입니다.

```
> show pim topology route-count
PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
```

```
No. of (S,G) routes = 0
No. of (S,G)RPT routes = 0
```

명령	설명
show mrib route	MRIB 테이블을 표시합니다.

show pim traffic

PIM 트래픽 카운터를 표시하려면 **show pim traffic** 명령을 사용합니다.

show pim traffic

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

자용 가이드라인

clear pim counters 명령을 사용하여 PIM 트래픽 카운터를 지웁니다.

다음은 **show pim traffic** 명령의 샘플 출력입니다.

```
> show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                      0        9485
Hello                                  0        9485
Join-Prune                             0           0
Register                               0           0
Register Stop                          0           0
Assert                                 0           0
Bidir DF Election                      0           0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Send Errors                                        0
Packet Sent on Loopback Errors                     0
Packets Received on PIM-disabled Interface         0
Packets Received with Unknown PIM Version          0
```

명령	설명
clear pim counters	PIM 트래픽 카운터를 지웁니다.

show pim tunnel

PIM 터널 인터페이스에 대한 정보를 표시하려면 **show pim tunnel** 명령을 사용합니다.

show pim tunnel [*interface_name*]

interface_name	(선택 사항) 인터페이스의 이름입니다. 이 인수를 포함하면 표시되는 정보가 지정된 인터페이스로 제한됩니다.

인터페이스를 지정하지 않으면 모든 인터페이스에 대한 PIM 터널 정보가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

PIM 등록 패킷은 가상 캡슐화 터널 인터페이스를 통해 소스의 첫 번째 홉 DR 라우터에서 RP(rendezvous point)로 전송됩니다. RP에서는 가상 역캡슐화 터널을 사용하여 PIM 등록 패킷의 수신 인터페이스를 표시합니다. 이 명령은 두 유형의 인터페이스 모두에 대한 터널 정보를 표시합니다.

등록 터널은 공유 트리를 통해 배포되도록 소스에서 RP로 전송되는 캡슐화된(PIM 등록 메시지에서) 멀티캐스트 패킷입니다. 등록은 SM에만 적용되며, SSM 및 양방향 PIM에는 적용되지 않습니다.

다음은 **show pim tunnel** 명령의 샘플 출력입니다.

```
> show pim tunnel

Interface     RP Address    Source Address

Encapstunne   l0 10.1.1.1   10.1.1.1
Decapstunne   l0 10.1.1.1   -
```

명령	설명
show pim topology	PIM 토폴로지 테이블을 표시합니다.

show policy-list

구성된 정책 목록 및 정책 목록 항목에 대한 정보를 표시하려면 **show policy-list** 명령을 사용합니다.

show policy-list [*policy_list_name*]

policy_list_name	(선택 사항) IP 정책 목록 이름입니다. 지정된 정책 목록에 관한 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

정책 목록은 BGP 라우팅에 사용됩니다.

다음은 **show policy-list** 명령의 샘플 출력입니다.

```
> show policy-list
policy-list POLICY-LIST-NAME-1 permit
  Match clauses:
    metric 20
policy-list POLICY-LIST-NAME-2 permit
  Match clauses:
    as-path (as-path filter): 1
```

show policy-route

정책 기반 라우팅 컨피그레이션을 표시하려면 **show policy-route** 명령을 사용합니다.

show policy-route

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show policy-route** 명령의 샘플 출력입니다.

```
> show policy-route
Interface Route map
GigabitEthernet0/0   equal-access
```

show port-channel

자세한 EtherChannel 정보 및 한 줄 요약 정보를 표시하거나 포트 및 포트 채널 정보를 표시하려면 **show port-channel** 명령을 사용합니다.

show port-channel [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

brief	(기본값) 간략한 정보를 표시합니다.
channel_group_number	(선택 사항) EtherChannel 채널 그룹 번호(1~48)를 지정하고, 이 채널 그룹에 대한 정보만 표시합니다.
detail	(선택 사항) 자세한 정보를 표시합니다.
port	(선택 사항) 각 인터페이스에 대한 정보를 표시합니다.
protocol	(선택 사항) 활성화된 경우 LACP와 같은 EtherChannel 프로토콜을 표시합니다.
summary	(선택 사항) 포트 채널에 대한 요약을 표시합니다.

기본값은 **brief**입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show port-channel** 명령의 샘플 출력입니다.

```
> show port-channel
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
```

```
Load balance: src-dst-ip
```

다음은 **show port-channel summary** 명령의 샘플 출력입니다.

```
> show port-channel summary

Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1             LACP    Gi3/1   Gi3/2   Gi3/3
```

다음은 **show port-channel detail** 명령의 샘플 출력입니다.

```
> show port-channel detail
        Channel-group listing:
        ----------------------

Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip

       Ports in the group:
       -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl      32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d

Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl      32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
--------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
```

```
Port: Gi3/3
-----------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

다음은 **show port-channel port** 명령의 샘플 출력입니다.

```
> show port-channel port
        Channel-group listing:
        ----------------------

Group: 1
----------
       Ports in the group:
       -------------------
Port: Gi3/1
-----------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d

Port: Gi3/2
-----------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
```

```
Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                            LACP port     Admin     Oper    Port        Port
Port      Flags   State     Priority      Key       Key     Number      State
-------------------------------------------------------------------------------
Gi3/3     SA      bndl      32768         0x1       0x1     0x304       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-------------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

다음은 **show port-channel protocol** 명령의 샘플 출력입니다.

```
> show port-channel protocol
        Channel-group listing:
        ----------------------
Group: 1
----------
Protocol: LACP
```

명령	설명
show lacp	트래픽 통계, 시스템 식별자 및 네이버 정보와 같은 LACP 정보를 표시합니다.
show port-channel load-balance	정해진 파라미터 집합에 대해 선택한 해시 결과 및 멤버 인터페이스와 함께 포트 채널 로드 밸런싱 정보를 표시합니다.

show port-channel load-balance

EtherChannel에 대해 현재 포트 채널 로드 밸런스 알고리즘을 표시하고, 선택적으로 지정된 파라미터 집합에 대해 선택된 멤버 인터페이스를 확인하려면 **show port-channel load-balance** 명령을 사용합니다.

show port-channel *channel_group_number* **load-balance** [**hash-result** {{**ip** | **ipv6** | **mac** | **l4port** | **mixed**} *parameters* | **vlan-only** *number*}]

channel_group_number	EtherChannel 채널 그룹 번호(1~48)를 지정합니다.
hash-result	(선택 사항) 현재 로드 밸런싱 알고리즘에 대한 해싱 값을 입력한 후에 선택한 멤버 인터페이스를 표시합니다.
ip	(선택 사항) IPv4 패킷 파라미터를 지정합니다.
ipv6	(선택 사항) IPv6 패킷 파라미터를 지정합니다.
l4port	(선택 사항) 포트 패킷 파라미터를 지정합니다.
mac	(선택 사항) MAC 주소 패킷 파라미터를 지정합니다.
mixed	(선택 사항) 포트 및/또는 VLAN ID와 함께 IP 또는 IPv6 파라미터의 조합을 지정합니다.
parameters	(선택 사항) 유형에 따른 패킷 파라미터입니다. 예를 들어 ip의 경우 소스 IP 주소, 대상 IP 주소 및/또는 VLAN ID를 지정할 수 있습니다.
vlan-only*number*	(선택 사항) 패킷에 대한 VLAN ID(0-4095)를 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

기본적으로 디바이스는 패킷의 소스 및 대상 IP 주소(**src-dst-ip**)에 따라 인터페이스에서 패킷 로드 밸런싱을 수행합니다.

이 명령을 사용하여 현재 로드 밸런싱 알고리즘을 볼 수 있지만 **hash-result** 키워드를 사용하면 지정된 파라미터로 패킷에 대해 선택할 멤버 인터페이스를 테스트할 수도 있습니다. 이 명령은 현재 로드 밸런싱 알고리즘에 대해서만 테스트합니다. 예를 들어 알고리즘이 src-dst-ip인 경우 IPv4 또는 IPv6 소스 및 대상 IP 주소를 입력합니다. 현재 알고리즘에서 사용되지 않는 다른 인수를 입력하면 해당 인수가 무시되고 알고리즘에서 실제로 사용되는 입력되지 않은 값이 기본적으로 0으로 설정됩니다. 예를 들어 알고리즘이 vlan-src-ip인 경우 다음을 입력합니다.

```
show port-channel 1 load-balance hash-result ip source 10.1.1.1 vlan 5
```

다음을 입력하면 vlan-src-ip 알고리즘이 소스 IP 주소 0.0.0.0 및 VLAN 0을 가정하고, 입력한 값을 무시합니다.

```
show port-channel 1 load-balance hash-result l4port source 90 destination 100
```

다음은 **show port-channel 1 load-balance** 명령의 샘플 출력입니다.

```
> show port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
       src-dst-ip

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
 IPv4: Source XOR Destination IP address
 IPv6: Source XOR Destination IP address
```

다음은 입력한 파라미터가 현재 알고리즘(src-dst-ip)과 일치하는 경우 **show port-channel 1 load-balance hash-result** 명령의 샘플 출력입니다.

```
> show port-channel 1 load-balance hash-result ip source 10.1.1.1 destination 10.5.5.5
Would select GigabitEthernet2/1 based on algorithm src-dst-ip
```

다음은 입력한 파라미터가 현재 알고리즘(src-dst-ip)과 일치하지 않고 해시에서 0 값을 사용하는 경우 **show port-channel 1 load-balance hash-result** 명령의 샘플 출력입니다.

```
> show port-channel 1 load-balance hash-result l4port source 5
Would select GigabitEthernet3/2 of Port-channel1 based on algorithm src-dst-ip
```

명령	설명
show lacp	트래픽 통계, 시스템 식별자, 인접 디바이스 세부사항 같은 LACP 정보가 표시됩니다.
show port-channel	EtherChannel 정보를 자세한 형식 및 한 줄짜리 요약 형식으로 표시합니다. 이 명령은 포트 및 포트-채널 정보도 표시합니다.

show prefix-list

트래픽과 일치하도록 구성된 IP 접두사를 나열하려면 **show prefix-list** 명령을 사용합니다.

show prefix-list [**detail**| **summary**] [*prefix_list_name* [**seq** *sequence_number* | *network/length* [**longer** | **first-match**]]]

detail	접두사 목록에 대한 세부 사항을 표시합니다.
summary	접두사 목록의 요약을 표시합니다.
prefix_list_name	접두사 목록의 이름입니다.
seq*sequence_number*	(선택 사항) 지정된 접두사 목록에서 지정된 시퀀스 번호가 있는 접두사 목록 항목만 표시합니다.
network/length	(선택 사항) 이 네트워크 주소 및 넷마스크 길이(비트)를 사용하는 지정된 접두사 목록의 모든 항목을 표시합니다. 네트워크 마스크 길이는 0~32입니다.
longer	(선택 사항) 지정된 network/length와 일치하거나 더 구체적으로 지정된 접두사 목록의 모든 항목을 표시합니다.
first-match	(선택 사항) 지정된 network/length와 일치하는 지정된 접두사 목록의 첫 번째 항목을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 "test"라고 명명된 접두사 목록과 함께 표시된 **show prefix-list** 명령의 샘플 출력입니다.

```
> show prefix-list detail test
show prefix-list detail test
ip prefix-list test:
Description: test-list
```

```
count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

명령	설명
clear prefix-list	IP 접두사 목록에서의 적중 횟수를 재설정합니다.
show bgp prefix-list	Border Gateway Protocol의 상황에서 접두사 목록 또는 접두사 목록 항목에 대한 정보를 표시합니다.

show processes

디바이스에서 실행되는 프로세스 목록을 표시하려면 **show processes** 명령을 사용합니다.

show processes [**cpu-hog** | **cpu-usage** [**non-zero**] [**sorted**] | **internals** | **memory** | **system**]

cpu-hog	CPU를 호그(즉, 100밀리초 넘게 CPU를 사용)하고 있는 프로세스 수 및 세부 정보를 표시합니다.
cpu-usage	지난 5초, 1분 및 5분 동안 각 프로세스에서 사용한 CPU의 백분율을 표시합니다.
internals	각 프로세스에 대한 내부 세부 정보를 표시합니다.
memory	각 프로세스의 메모리 할당을 표시합니다.
non-zero	(선택 사항) CPU 사용량이 0이 아닌 프로세스를 표시합니다.
sorted	(선택 사항) 프로세스에 대한 정렬된 CPU 사용량을 표시합니다.
system	(선택 사항) 현재 시스템에서 실행 중인 프로세스에 대한 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

프로세스가 몇 가지 명령만 필요한 경량 스레드입니다. **show processes** 명령은 디바이스에서 실행 중인 프로세스 목록을 다음과 같이 표시합니다.

Command(명령)	표시되는 데이터	설명
show processes	PC	프로그램 카운터입니다.
show processes	SP	스택 포인터입니다.
show processes	주	스레드 대기열의 주소입니다.

Command(명령)	표시되는 데이터	설명
show processes	가동 시간	스레드가 실행된 밀리초입니다(CPU 클럭 주기 기반). 정확도는 클럭 틱(10ms 해상도) 대신 CPU 클럭 주기(<10ns 해상도)를 기반으로 프로세스 CPU 사용량을 완전하고 정확하게 계산하는 데 1밀리초 이내가 소요됩니다.
show processes	SBASE	스택 기본 주소입니다.
show processes	Stack	현재 사용 중인 바이트 수 및 스택의 총 크기입니다.
show processes	프로세스	스레드의 기능입니다.
show processes cpu-usage	MAXHOG	최대 CPU 호그 런타임(밀리초)입니다.
show processes cpu-usage	NUMHOG	CPU 호그 실행 횟수입니다.
show processes cpu-usage	LASTHOG	마지막 CPU 호그 런타임(밀리초)입니다.
show processes cpu-usage	PC	CPU 호깅 프로세스의 명령 포인터입니다.
show processes cpu-usage	Traceback	CPU 호깅 프로세스의 스택 추적입니다. Traceback에는 최대 14개의 주소가 있을 수 있습니다.
show processes internals	Invoked Calls	스케줄러에서 프로세스를 실행한 횟수입니다.
show processes internals	Giveups	프로세스에서 스케줄러로 CPU를 다시 양보한 횟수입니다.

show processes cpu-usage 명령을 사용하여 디바이스에서 CPU를 사용 중일 수 있는 특정 프로세스로 범위를 좁힐 수 있습니다. **sorted** 및 **non-zero** 명령을 사용하여 **show processes cpu-usage** 명령의 출력을 추가로 사용자 지정할 수 있습니다.

scheduler 및 total summary 줄에서 **show proccesses** 명령을 두 번 연속으로 실행하고 출력을 비교하여 다음을 확인할 수 있습니다.

- CPU의 100% 소비
- 각 스레드에서 사용하는 CPU 백분율 - 스레드의 런타임 델타와 총 런타임 델타를 비교하여 확인

디바이스가 다른 여러 스레드 실행을 통해 단일 프로세스로 실행됩니다. 이 명령의 출력은 실제로 스레드당 기준으로 메모리 할당 및 여유 메모리를 보여줍니다. 이러한 스레드가 디바이스의 작업과 관련된 데이터 흐름 및 다른 작업에서의 협업에서 작동하므로 다른 스레드가 메모리를 사용하지 않는 동안 하나의 스레드가 메모리 블록을 할당할 수 있습니다. 출력의 마지막 행은 모든 스레드의 총 개

수를 포함합니다. 이 행만 사용하여 할당 및 여유 메모리 간의 차이를 모니터링하여 잠재적인 메모리 누수를 추적할 수 있습니다.

다음 예에서는 실행 중인 프로세스 목록을 표시하는 방법을 보여 줍니다. 명령 출력 래핑.

```
> show processes
    PC                 SP                 STATE                 Runtime              SBASE

Stack Process TID
Mwe 0x00007f9ae994881e 0x00007f9acb9d6e18 0x00007f9b027e1340          0 0x00007f9acb9cf030
32000/32768 zone_background_idb 140
Mwe 0x00007f9ae91d64ae 0x00007f9ae7659cd8 0x00007f9b027e1340          0 0x00007f9ae7652030
27568/32768 WebVPN KCD Process 14
Msi 0x00007f9aea3f8c04 0x00007f9acba86e48 0x00007f9b027e1340       2917 0x00007f9acba7f030
29944/32768 vpnlb_timer_thread 131
```

다음 예에서는 시스템 프로세스를 나열하는 방법을 보여 줍니다.

```
> show processes system
  PID USER      PR  NI  VIRT  RES  SHR S %CPU %MEM    TIME+  COMMAND
23302 root       0 -20 1896m 558m 101m S  198  7.1  16939:07 lina
 8330 admin     20   0 15240 1188  852 R    2  0.0   0:00.01 top
23148 root      20   0 29780 2876 1268 S    2  0.0  41:27.25 UEChanneld
(...output truncated...)
```

다음 예에서는 각 프로세스에서 사용하는 CPU 백분율을 표시하는 방법을 보여 줍니다.

```
> show processes cpu-usage non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x00007f9ae8abcc76   0x00007f9ad04cf7a0     0.2%     0.0%     0.0%   Environment Monitor
Process
```

다음 예에서는 CPU를 호그 중인 프로세스 수 및 세부 정보를 표시하는 방법을 보여 줍니다.

```
> show processes cpu-hog
Process:      cli_xml_server, NUMHOG: 12, MAXHOG: 30, LASTHOG: 2
LASTHOG At:   17:37:08 UTC Oct 28 2016
PC:           0x00007f9ae9b11539 (suspend)
Call stack:   0x00007f9ae9b11539  0x00007f9ae9caf084  0x00007f9ae9caf9d0
              0x00007f9ae8736425  0x00007f9ae9b13346  0x00007f9ae9b15ab4
              0x00007f9ae8730ead  0x00007f9ae87663ec  0x00007f9ae6eccde0
              0x00007f9ac4a46120  0x31223d646920696c
(...output truncated...)
```

다음 예에서는 각 프로세스에 대한 메모리 할당을 표시하는 방법을 보여 줍니다.

```
> show processes memory

-------------------------------------------------------------------------------
Allocs      Allocated             Frees       Freed                 Process
             (bytes)                           (bytes)
-------------------------------------------------------------------------------
0           0                     0           0                     *System Main*
0           0                     0           0                     QoS Support Module
0           0                     0           0                     SSL
0           0                     0           0                     vpnfol_thread_sync
22          8636                  78          3728                  DHCP Network Scope
Monitor
7           40459                 0           0                     Integrity FW Task
0           0                     0           0                     uauth_urlb clean
2           64                    0           0                     arp_timer
8450        233220                0           0                     HDD Health Monitor
```

```
14638       1659384              14509       1570750              PTHREAD-23518
0           0                    6           1926                 DHCP Client
(...output truncated...)
```

다음 예에서는 각 프로세스의 내부 정보를 표시하는 방법을 보여 줍니다.

```
> show processes internals
     Invoked      Giveups  Max_Runtime  Process
           1            0        0.002  zone_background_idb
           2            0        0.163  WebVPN KCD Process
      507512            0        0.060  vpnlb_timer_thread
           2            0        0.057  vpnlb_thread
     2029820            0        0.130  vpnfol_thread_unsent
      507455            0        0.137  vpnfol_thread_timer
(...output truncated...)
```

show process-tree

트리 관계에서 시스템 프로세스를 표시하려면 **show process-tree** 명령을 사용합니다.

show process-tree

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령의 출력은 Cisco 기술 지원의 주요 관심사입니다.

다음은 프로세스 트리를 보여주는 예입니다.

```
> show process-tree
init(1)-+-acpid(23138)
        |-agetty(23726)
        |-crond(23141)
        |-dbus-daemon(23119)
        |-login(23727)---clish(6394)
        |-nscd(14445)-+-{nscd}(14448)
        |             |-{nscd}(14449)
        |             |-{nscd}(14450)
        |             |-{nscd}(14451)
        |             |-{nscd}(14452)
        |             `-{nscd}(14453)
(...remaining output truncated...)
```

show quota

현재 세션에 대한 할당량 통계를 표시하려면 **show quota** 명령을 사용합니다.

show quota [**management-session**]

management-session	현재 관리 세션의 통계를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

Firepower Threat Defense에서 관리 세션 할당량을 구성할 수 없습니다. 이 명령은 항상 제한이 없음(no limits)을 표시해야 합니다.

다음 예는 할당량 통계를 보여줍니다.

```
> show quota
quota management-session limit 0
quota management-session warning level 0
quota management-session level 0
quota management-session high water 0
quota management-session errors 0
quota management-session warnings 0
```

show resource types

디바이스에서 사용량을 추적하는 리소스 유형을 표시하려면 **show resource types** 명령을 사용합니다.

show resource types

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 샘플 표시는 리소스 유형을 보여 줍니다.

```
> show resource types
Rate limited resource types:
  Conns                     Connections/sec
  Inspects                  Inspects/sec
  Syslogs                   Syslogs/sec

Absolute limit types:
  Conns                     Connections
  Hosts                     Hosts
  IPSec                     IPSec Mgmt Tunnels
  Mac-addresses             MAC Address table entries
  ASDM                      ASDM Connections
  SSH Client                SSH Client Sessions
  SSH Server                SSH Server Sessions
  Storage                   Storage Limit Size of context directory in MB
  Telnet                    Telnet Sessions
  Xlates                    XLATE Objects
  Routes                    Routing Table Entries
  All                       All Resources
  Other VPN Sessions        Other VPN Sessions
  Other VPN Burst           Allowable burst for Other VPN Sessions
  AnyConnect                AnyConnect Premium licensed sessions
  AnyConnect Burst          Allowable burst for AnyConnect Premium licensed sessions
  IKEv1 in-negotiation      Allowable in negotiation IKEv1 SAs
```

명령	설명
clear resource usage	리소스 사용 통계를 지웁니다.
show resource usage	디바이스의 리소스 사용량을 표시합니다.

show resource usage

디바이스의 리소스 사용을 표시하려면 **show resource usage** 명령을 사용합니다.

show resource usage [**all** | **detail**] [**resource** {[**rate**] *resource_name* | **all**}] [**counter** *counter_name* [*count_threshold*]]

all	모든 유형입니다.
count_threshold	표시되는 리소스 수의 하한을 설정합니다. 기본값은 1입니다. 리소스 사용량이 설정된 값보다 적을 경우 리소스가 표시되지 않습니다. 카운터 이름에 대해 all을 지정한 경우 카운트 임계값은 현재 사용량에 적용됩니다. 모든 리소스를 표시하려면 카운트 임계값을 0으로 설정합니다.
counter*counter_name*	다음 카운터 유형의 개수를 표시합니다. • **current** - 액티브 동시 인스턴스 또는 리소스의 현재 비율을 표시합니다. • **peak - clear resource usage** 명령 또는 디바이스 재부팅으로 인해 통계가 마지막으로 지워진 이후의 피크 동시 인스턴스 또는 리소스의 피크 비율을 표시합니다. • **denied** - Limit 열에 표시된 리소스 제한을 초과했기 때문에 거부된 인스턴스 수를 표시합니다. • **all** - (기본 설정) 모든 통계를 표시합니다.
detail	관리할 수 없는 리소스를 포함하여 모든 리소스의 사용량을 표시합니다. 예를 들어, TCP 인터셉트의 수를 볼 수 있습니다.
resource {[**rate**] *resource_name* | **all**}	특정 리소스의 사용량을 표시합니다. 모든 리소스에 대해 **all**을 지정합니다. 리소스 사용률을 표시하려면 rate를 지정합니다. 비율로 측정되는 리소스에는 **conns**, **inspects** 및 **syslogs** 등이 있습니다. 이러한 리소스 유형에는 **rate** 키워드를 지정해야 합니다. **conns** 리소스는 동시 연결 수로도 측정되지만 초당 연결 수를 보려면 rate 키워드를 사용해야 합니다. 리소스 이름 목록은 사용 지침 섹션을 참고하십시오.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

resource 키워드를 사용하는 경우 리소스에 다음 유형이 포함됩니다.

- **asdm** - 이 키워드와 관련된 기능은 Firepower Threat Defense에서 지원되지 않습니다.
- **conns** - 호스트 하나와 여러 다른 호스트 간의 연결을 포함하여 두 호스트 간의 TCP 또는 UDP 연결입니다.
- **hosts** - Firepower Threat Defense 디바이스를 통해 연결할 수 있는 호스트입니다.
- **ipsec** - IPSec 관리 터널
- **mac-addresses** - 투명 방화벽 모드의 경우 MAC 주소 테이블에서 허용되는 MAC 주소의 수.
- **rate** - 속도가 측정된 리소스. **conns**, **inspects** 또는 **syslogs**를 지정합니다.
- **routes** - 라우팅 테이블 엔트리.
- **ssh** - SSH 세션.
- **storage** - 스토리지 제한 크기입니다(MB 단위).
- **telnet** - 텔넷 세션.
- **vpn** - VPN 리소스.
- **vpn anyconnect** - AnyConnect Premium 라이선스 제한.
- **vpn ikev1 in-negotiation** - 협상에 포함될 수 있는 IKEv1 세션의 수입니다.
- **VPN Other** - Site-to-Site VPN 세션입니다.
- **VPN Burst Other** - Site-to-Site VPN 버스트 세션입니다.
- **xlates** - NAT 변환.

다음은 **show resource usage** 명령의 샘플 출력입니다. 여기서는 모든 리소스의 리소스 사용량을 보여줍니다. 디바이스는 단일 상황 모드에 있으므로 상황이 시스템으로 표시됩니다.

```
> show resource usage
Resource                Current         Peak      Limit        Denied Context
Syslogs [rate]                0          144        N/A             0 System
Conns                         0            5     100000             0 System
Xlates                        0            5        N/A             0 System
Hosts                         0            8        N/A             0 System
Conns [rate]                  0            1        N/A             0 System
Inspects [rate]               0            3        N/A             0 System
```

```
Mac-addresses                 0           4      16384            0 System
Routes                        9           9  unlimited            0 System
```

명령	설명
clear resource usage	리소스 사용 통계를 지웁니다.
show resource types	리소스 유형의 목록을 표시합니다.

show rip database

RIP 토폴로지 데이터베이스에 저장된 정보를 표시하려면 **show rip database** 명령을 사용합니다.

show rip database [*ip_addr* [*mask*]]

ip_addr	(선택 사항) 지정된 네트워크 주소에 대한 표시 경로를 제한합니다.
mask	(선택 사항) 선택적 네트워크 주소에 대한 네트워크 마스크를 지정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

RIP 데이터베이스에는 RIP를 통해 학습된 모든 경로가 포함되어 있습니다. 이 데이터베이스에 표시된 경로는 라우팅 테이블에 나타나지 않을 수도 있습니다.

다음은 **show rip database** 명령의 샘플 출력입니다.

```
> show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

다음은 네트워크 주소 및 마스크가 포함된 **show rip database** 명령의 샘플 출력입니다.

```
> show rip database 172.19.86.0 255.255.255.0
172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

show route

라우팅 테이블을 표시하려면 **show route** 명령을 사용합니다.

show route [**cluster** | **failover** | *ip_address* [*mask*] [**longer-prefixes**] | **bgp** [*as_number*] | **connected** | **eigrp** [*process_id*] | **ospf** [*process_id*] | **rip** | **static** | **summary** | **zone**]

bgp*as_number*	(선택 사항) BGP 경로에 대한 RIB(Routing Information Base) 에포크 번호(시퀀스 번호), 현재 타이머 값 및 네트워크 설명자 블록 에포크 번호(시퀀스 번호)를 표시합니다. AS 번호는 지정된 AS 번호를 사용하는 경로 항목으로 표시를 제한합니다.
cluster	(선택 사항) RIB(Routing Information Base) 에포크 번호(시퀀스 번호), 현재 타이머 값 및 네트워크 설명자 블록 에포크 번호(시퀀스 번호)를 표시합니다.
connected	(선택 사항) 연결된 경로를 표시합니다.
eigrp*process_id*	(선택 사항) EIGRP 경로를 표시합니다. 단, Firepower Threat Defense는 EIGRP를 지원하지 않습니다.
failover	(선택 사항) 라우팅 테이블의 현재 시퀀스 번호 및 페일오버가발생한 후의 라우팅 항목을 표시하며, 스탠바이 유닛이 액티브 유닛이 됩니다.
interface_name	(선택 사항) 지정된 인터페이스를 사용하는 라우팅 항목을 표시합니다.
ip_address mask	(선택 사항) 지정된 대상에 대한 경로를 표시합니다.
longer-prefixes	(선택 사항) 지정된 ip_address/마스크 쌍과 일치하는 경로만 표시합니다.
ospf*process_id*	(선택 사항) OSPF 경로를 표시합니다.
rip	(선택 사항) RIP 경로를 표시합니다.
static	(선택 사항) 고정 경로를 표시합니다.
summary	(옵션) 라우팅 테이블의 현재 상태를 표시합니다.
zone	(선택 사항) 영역 인터페이스의 경로를 표시합니다. Firepower Threat Defense는 이 기능을 지원하지 않습니다. 이는 보안 영역과 동일하지 않습니다.

릴리스	수정
6.1	이 명령이 추가되었습니다.

사용 가이드라인

show route 명령은 정보가 IPv4에 특정하다는 점을 제외하고는 **show ipv6 route** 명령과 유사한 출력을 제공합니다.

참고 **clustering** 및 **failover** 키워드는 이러한 기능이 Firepower Threat Defense 디바이스에 구성되지 않은 한 표시되지 않습니다.

show route 명령은 새 연결에 대한 "최상의" 경로를 나열합니다. 허용된 TCP SYN을 백업 인터페이스로 전송한 경우 Firepower Threat Defense 디바이스는 동일한 인터페이스를 통해서만 응답할 수 있습니다. 해당 인터페이스의 RIB에 기본 경로가 없는 경우 디바이스는 인접성이 없기 때문에 패킷을 드롭합니다. **show running-config route** 명령에 표시된 대로 구성된 모든 항목은 특정 데이터 구조로 시스템에서 유지됩니다.

show asp table routing 명령을 사용하여 백엔드 인터페이스별 라우팅 테이블을 확인할 수 있습니다. 이 설계는 프로토콜별 경로 데이터베이스가 "최상의" 경로만 표시하는 전역 라우팅 테이블과 동일하지 않다는 점에서 OSPF 또는 EIGRP와 유사합니다. 이 동작은 설계에 따른 것입니다.

다음은 **show route** 명령의 샘플 출력입니다.

```
> show route

Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

다음은 페일오버 후 OSPF 및 EIGRP 경로와 스탠바이 유닛의 동기화를 보여주는 **show route failover** 명령의 샘플 출력입니다.

```
> show route failover
```

```
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0
Routing table sequence number 1
Reconvergence timer 00.20 (Running)

S    10.10.10.0 255.0.0.0 [1/0] via 10.10.10.1, mgmt, seq 1
                        [1/0] via 10.10.10.2, mgmt, seq 1
D    209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 1

O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 0

D   10.65.68.220 255.255.255.255 [1/0] via 10.76.11.1, mgmt, seq 1
```

다음은 **show route cluster** 명령의 샘플 출력입니다.

```
> show route cluster
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

Routing table seq num 2
Reconvergence timer expires in 52 secs

C    70.0.0.0 255.255.255.0 is directly connected, cluster, seq 1
C    172.23.0.0 255.255.0.0 is directly connected, tftp, seq 1
C    200.165.200.0 255.255.255.0 is directly connected, outside, seq 1
C    198.51.100.0 255.255.255.0 is directly connected, inside, seq 1
O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 2
D   209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 2
```

다음은 **show route summary** 명령의 샘플 출력입니다.

```
> show route summary

IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          1           0           0           88          288
bgp 2           0           0           0           0           0
  External: 0 Internal: 0 Local: 0
internal        1                                               408
Total           2           2           0           264         1272
```

show route-map

경로 맵 정보를 표시하려면 **show route-map** 명령을 사용합니다.

show route-map [**all** | **dynamic** [**application** [*application*] | **detail**| *route_map*] | *route_map*]

all	고정 및 동적 경로 맵에 대한 정보를 표시합니다.
dynamic	동적 경로 맵에 대한 정보만 표시합니다.
application*application*	경로 맵을 생성한 애플리케이션입니다.
route_map	경로 맵의 이름입니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show route-map dynamic** 명령의 샘플 출력입니다.

```
> show route-map dynamic
route-map MIP-10/24/06-05:23:46.091-1-MPATH_1, permit, sequence 0, identifier 54943520
  Match clauses:
    ip address (access-lists): VOICE
  Set clauses:
    interface Tunnel0
  Policy routing matches: 0 packets, 0 bytes
 Current active dynamic routemaps = 1
```

show running-config

현재 디바이스에서 실행 중인 컨피그레이션을 표시하려면 **show running-config** 명령을 사용합니다.

show running-config [**all**] [*command*]

all	기본 컨피그레이션을 비롯하여 작동 중인 전체 컨피그레이션을 표시합니다.
command	특정 명령과 관련된 컨피그레이션을 표시합니다. 사용 가능한 명령은 **show running-config ?**를 사용하여 CLI 도움말을 참고하십시오. 참고 Firepower Threat Defense는 CLI 도움말에 나열되어 있는 각 명령을 직접 지원하지는 않습니다. 지정된 옵션에 대한 컨피그레이션이 있을 수 있습니다. 일부 옵션은 Firepower Management Center에서 FlexConfig를 사용하는 경우에만 구성할 수 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show running-config 명령은 디바이스에 있는 메모리의 활성 컨피그레이션(저장된 컨피그레이션 변경 사항 포함)을 표시합니다. 직접 이 명령을 구성할 수 없습니다. 대신, 이 명령은 디바이스를 제어하는 관리자를 통해 구성할 수 있습니다. 예를 들어, Firepower Management Center 또는 Firepower Device Manager가 있습니다.

그러나, 이것은 부분적인 컨피그레이션입니다. 이것은 ASA 소프트웨어 컨피그레이션 명령만 사용하여 구성될 수 있는 경우를 보여줍니다. 단, 일부 명령은 Firepower Threat Defense에 특정할 수 있습니다. 이 명령은 Firepower Threat Defense로 복사됩니다. 따라서, 문제 해결로만 실행 중인 컨피그레이션 정보를 사용해야 합니다. 디바이스 컨피그레이션을 분석하기 위한 기본 방법으로 디바이스 관리자를 사용합니다.

다음은 **show running-config** 명령의 샘플 출력입니다.

```
> show running-config
: Saved
```

```
:
: Serial Number: XXXXXXXXXXX
: Hardware:   ASA5512, 4096 MB RAM, CPU Clarkdale 2793 MHz, 1 CPU (2 cores)
:
NGFW Version 6.1.0
!
hostname firepower
enable password $sha512$5000$Col980QPR9VVq/VYoAkGJw==$ZvzuZDNpcvvEP/DGbBqytA== pbkdf2
strong-encryption-disable
names

!
interface GigabitEthernet0/0
 nameif outside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.10.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/1
 shutdown
 nameif inside
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.1.1 255.255.255.0
 ipv6 enable
!
interface GigabitEthernet0/2
 shutdown
 nameif dmz
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
 ip address 192.168.2.1 255.255.255.0
 ipv6 enable
!
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
 management-only
 no nameif
 no security-level
 no ip address
!
ftp mode passive
ngips conn-match vlan-id
access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority
 Policy
access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998
access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998
```

```
access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998
access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: Initial AC Policy - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434432
access-list CSM_IPSEC_ACL_1 extended permit ip any6 any6
!
tcp-map UM_STATIC_TCP_MAP
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options md5 clear
  urgent-flag allow
!
no pager
logging enable
logging buffered informational
logging flash-minimum-free 1024
logging flash-maximum-allocation 3076
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 106100
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
no monitor-interface service-module
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
arp rate-limit 8192
access-group CSM_FW_ACL_ global
as-path access-list 2 deny 100$
as-path access-list 2 permit 200$
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:00:30
timeout floating-conn 0:00:00
timeout conn-holddown 0:00:15
aaa proxy-limit disable
no snmp-server location
no snmp-server contact
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
no sysopt connection permit-vpn
crypto ipsec ikev1 transform-set CSM_TS_1 esp-des esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map CSM_outside_map 1 match address CSM_IPSEC_ACL_1
crypto map CSM_outside_map 1 set peer 10.10.10.10
crypto map CSM_outside_map 1 set ikev1 transform-set CSM_TS_1
crypto map CSM_outside_map 1 set reverse-route
crypto map CSM_outside_map interface outside
crypto ca trustpool policy
crypto ikev1 enable outside
crypto ikev1 policy 160
 authentication pre-share
 encryption des
 hash sha
```

```
 group 5
 lifetime 86400
telnet timeout 5
console timeout 0
dynamic-access-policy-record DfltAccessPolicy
tunnel-group 10.10.10.10 type ipsec-l2l
tunnel-group 10.10.10.10 ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:167911f11cbf1140edeffcb0f9b17f01
: end
>
```

명령	설명
show access-control-config	액세스 제어 정책에 대한 요약 정보를 표시합니다.

show s - sz

show sctp

현재 SCTP(Stream Control Transmission Protocol) 쿠키 및 연결을 표시하려면 **show sctp** 명령을 사용합니다.

show sctp [**detail**]

detail	SCTP 연결에 대한 자세한 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show sctp 명령은 SCTP 쿠키 및 연결에 대한 정보를 표시합니다.

Firepower Management Center에서 FlexConfig를 사용하여 SCTP 검사를 활성화한 경우, 이 명령은 SCTP 정보를 표시할 수 있습니다.

다음은 **show sctp** 명령의 샘플 출력입니다.

```
> show sctp

AssocID: 2279da7a
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40174 (ESTABLISHED)

AssocID: 4924f520
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40200 (ESTABLISHED)
```

다음은 **show sctp detail** 명령의 샘플 출력입니다.

```
> show sctp detail

AssocID: 8b7e3ffb
Local:  192.168.100.56/3868 (ESTABLISHED)
    Receiver Window: 48000
    Cumulative TSN: 5cb6cd9b
    Next TSN: 5cb6cd9c
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
Remote: 192.168.200.78/3868 (ESTABLISHED)
    Receiver Window: 114688
```

```
Cumulative TSN: 5cb6cd98
Next TSN: 0
Earliest Outstanding TSN: 5cb6cd9c
Out-of-Order Packet Count: 0
```

명령	설명
show local-host	인터페이스당 디바이스를 통해 연결하는 호스트에 대한 정보를 표시합니다.
show service-policy inspect sctp	SCTP 검사 통계를 표시합니다.
show traffic	인터페이스당 연결 및 검사 통계를 표시합니다.

show serial-number

섀시 일련 번호를 표시하려면 **show serial-number** 명령을 사용합니다. 가상 디바이스에서는 이 명령을 이용할 수 없습니다.

show serial-number

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

디바이스의 일련 번호를 보려면 **show serial-number** 명령을 사용합니다. 이 정보는 **show version system** 및 **show running-config** 출력에서도 표시됩니다.

다음 예는 일련 번호를 표시하는 방법을 보여줍니다. 이 예의 숫자는 유효하지 않은 숫자로 변경되었습니다.

```
> show serial-number
XXX175078X5
```

show service-policy

서비스 정책 통계를 표시하려면 **show service-policy** 명령을 사용합니다.

show service-policy [**global** | **interface** *intf*] [**cluster flow-mobility** | **inspect** *inspection* [*arguments*] | **police** | **priority** | **set connection** [**details**] | **sfr** | **shape** | **user-statistics**]

show service-policy [**global** | **interface** *intf*] [**flow** *protocol* {**host** *src_host* | *src_ip src_mask*} [**eq** *src_port*] {**host** *dest_host* | *dest_ip dest_mask*} [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

cluster flow-mobility	(선택 사항) Firepower Threat Defense 클러스터에서 플로우 모빌리티에 대한 상태 정보를 표시합니다.
dest_ip dest_mask	**flow** 키워드를 사용할 경우 트래픽 플로우의 대상 IP 주소 및 넷마스크입니다.
details	(선택 사항) **set connection** 키워드를 사용할 경우 클라이언트별 연결 제한이 활성화된 경우 클라이언트별 연결 정보를 표시합니다.
eq*dest_port*	(선택 사항) **flow** 키워드를 사용할 경우 플로우의 대상 포트와 같습니다.
eq*src_port*	(선택 사항) **flow** 키워드를 사용할 경우 플로우의 소스 포트와 같습니다.
flow*protocol*	(선택 사항) 5튜블(프로토콜, 소스 IP 주소, 소스 포트, 대상 IP 주소, 대상 포트)로 식별되는 특정 플로우와 일치하는 정책을 표시합니다. 이 명령을 사용하여 서비스 정책 컨피그레이션이 특정 연결에 대한 원하는 서비스를 제공하는지 확인할 수 있습니다.
global	(선택 사항) 전역 정책으로 출력을 제한합니다.
host*dest_host*	**flow** 키워드를 사용할 경우 트래픽 흐름의 호스트 대상 IP 주소입니다.
host*src_host*	**flow** 키워드를 사용할 경우 트래픽 플로우의 호스트 소스 IP 주소입니다.
icmp_control_message	(선택 사항) **flow** 키워드를 사용할 때 ICMP를 프로토콜로 지정하는 경우 트래픽 플로우의 ICMP 제어 메시지를 지정합니다.
icmp_number	(선택 사항) **flow** 키워드를 사용할 때 ICMP를 프로토콜로 지정하는 경우 트래픽 플로우의 ICMP 프로토콜 수를 지정합니다.
inspect*inspection* [*arguments*]	(선택 사항) **inspect** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다. 일부 **inspect** 명령은 세부 출력이 지원되지 않습니다. 모든 검사를 보려면 **show service-policy inspect ?** 명령을 사용하십시오. 검사마다 사용할 수 있는 인수가 다릅니다. 자세한 내용은 CLI 도움말을 참고하십시오.

interface*intf*	(선택 사항) *intf* 인수로 지정된 인터페이스에 적용되는 정책을 표시합니다. 여기서 *intf*는 인터페이스 이름입니다.
police	(선택 사항) **police** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
priority	(선택 사항) **priority** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
set connection	(선택 사항) **set connection** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
sfr	(선택 사항) ASA FirePOWER 모듈의 정책에 대한 자세한 정보를 표시합니다. 이 키워드는 Firepower Threat Defense에 대해 유효하지 않습니다.
shape	(선택 사항) **shape** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다.
src_ip src_mask	**flow** 키워드를 사용할 경우 트래픽 플로우의 소스 IP 주소 및 넷마스크입니다.
user-statistics	(선택 사항) **user-statistics** 명령이 포함된 정책에 대한 자세한 정보를 표시합니다. 이 키워드는 Firepower Threat Defense에 대해 유효하지 않습니다.

인수를 지정하지 않으면 모든 전역 및 인터페이스 정책이 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show service-policy 명령 출력에 표시되는 원시 연결 수는 트래픽 클래스에 정의된 것과 일치하는 트래픽에 대해 인터페이스에 현재 연결된 원시 연결 수를 나타냅니다. "embryonic-conn-max" 필드는 트래픽 클래스에 대해 구성된 최대 원시 제한을 표시합니다. 표시된 현재 원시 연결 수가 최대값과 같거나 최대값을 초과하는 경우 트래픽과 일치하는 새 TCP 연결에 TCP 가로채기가 적용됩니다.

서비스 정책 변경 사항을 컨피그레이션에 적용하면 모든 새 연결에서 새로운 서비스 정책을 사용합니다. 기존 연결에서는 연결 설정 당시에 구성된 정책을 계속 사용합니다. **show** 명령 출력에는 이전 연결에 대한 데이터가 포함되지 않습니다. 모든 연결에서 새 정책을 사용하려면 새 정책을 사용하여 다시 연결할 수 있도록 현재 연결을 해제해야 합니다. 자세한 내용은 **clear conn** 또는 **clear local-host** 명령을 참고하십시오.

Firepower Management Center 또는 Firepower Device Manager를 사용하여 직접 서비스 정책을 구성할 수 없습니다. 다양한 연결 설정을 수정하거나 QoS 정책을 구성할 때 간접적으로 일부 내용이 변경됩니다. 또한 **configure inspection** 명령을 사용하여 어떤 기본 검사를 활성화할지 조정할 수 있습니다. 서비스 정책을 구성하려면 Firepower Management Center에서 FlexConfig를 사용하는 경우, 이 명령은 컨피그레이션과 관련된 통계를 표시합니다.

참고 **inspect icmp** 및 **inspect icmp error** 정책의 경우에는 패킷 수에 에코 요청 및 응답 패킷만 포함됩니다.

다음은 **show service-policy** 명령의 샘플 출력입니다.

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: esmtp _default_esmtp_map, packet 0, lock fail 0, drop 0, reset-drop 0,
5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: skinny , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: xdmcp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: netbios, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0
pkts/sec, v6-fail-close 0 sctp-drop-override 0
      Inspect: ip-options UM_STATIC_IP_OPTIONS_MAP, packet 0, lock fail 0, drop 0,
reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
    Class-map: class-default
      Default Queueing      Set connection policy:         drop 0
      Set connection advanced-options: UM_STATIC_TCP_MAP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
```

```
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

여러 CPU 코어가 있는 디바이스의 경우 잠금 실패에 대한 카운터가 있습니다. 잠금 메커니즘은 여러 코어에서 사용될 수 있으므로 공유된 데이터 구조와 변수를 보호하는 데 사용됩니다. 코어가 잠금을 획득하지 못할 경우, 다시 잠금을 시도합니다. 잠금 실패 카운터가 실패한 시도마다 증가합니다.

```
> show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      ...
      Inspect: esmtp _default_esmtp_map, packet 96716502, lock fail 7, drop 25,
reset-drop 0
      Inspect: sqlnet, packet 2526511491, lock fail 21, drop 2362, reset-drop 0
```

다음 명령에서는 GTP 검사 통계를 보여줍니다. 이 출력은 예 다음에 오는 표에 설명되어 있습니다.

```
> show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support               0     msg_too_short             0
  unknown_msg                       0     unexpected_sig_msg        0
  unexpected_data_msg               0     ie_duplicated             0
  mandatory_ie_missing              0     mandatory_ie_incorrect    0
  optional_ie_incorrect             0     ie_unknown                0
  ie_out_of_order                   0     ie_unexpected             0
  total_forwarded                  67     total_dropped             1
  signalling_msg_dropped            1     data_msg_dropped          0
  signalling_msg_forwarded         67     data_msg_forwarded        0
  total created_pdp                33     total deleted_pdp         32
  total created_pdpmcb             31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo             0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo            0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                  1
```

표 ***41: GPRS GTP*** 통계

열 머리글	설명
version_not_support	지원되지 않는 GTP 버전 필드가 있는 패킷을 표시합니다.
msg_too_short	길이가 8바이트 미만인 패킷을 표시합니다.
unknown_msg	알 수 없는 유형의 메시지를 표시합니다.
unexpected_sig_msg	예상치 못한 신호 메시지를 표시합니다.
unexpected_data_msg	예상치 못한 데이터 메시지를 표시합니다.
mandatory_ie_missing	필수 IE(Information Element)가 없는 메시지를 표시합니다.
mandatory_ie_incorrect	필수 IE(Information Element)의 형식이 잘못된 메시지를 표시합니다.

열 머리글	설명
optional_ie_incorrect	유효하지 않은 선택적 IE(Information Element)를 지닌 메시지를 표시합니다.
ie_unknown	알 수 없는 IE(Information Element)가 있는 메시지를 표시합니다.
ie_out_of_order	시퀀스가 잘못된 IE(Information Element)가 있는 메시지를 표시합니다.
ie_unexpected	예상치 못한 IE(Information Element)가 있는 메시지를 표시합니다.
ie_duplicated	중복된 IE(Information Element)가 있는 메시지를 표시합니다.
optional_ie_incorrect	선택적 IE(Information Element)의 형식이 잘못된 메시지를 표시합니다.
total_dropped	삭제된 총 메시지 수를 표시합니다.
signalling_msg_dropped	삭제된 신호 처리 메시지 수를 표시합니다.
data_msg_dropped	삭제된 데이터 메시지 수를 표시합니다.
total_forwarded	전달된 총 메시지 수를 표시합니다.
signalling_msg_forwarded	전달된 신호 처리 메시지 수를 표시합니다.
data_msg_forwarded	전달된 데이터 메시지 수를 표시합니다.
total created_pdp	생성된 총 PDP(Packet Data Protocol) 또는 전달자(bearer) 상황 수를 표시합니다.
total deleted_pdp	삭제된 총 PDP(Packet Data Protocol) 또는 전달자(bearer) 상황 수를 표시합니다.
total created_pdpmcb total deleted_pdpmcb total dup_sig_mcbinfo total dup_data_mcbinfo no_new_sgw_sig_mcbinfo no_new_sgw_data_mcbinfo	이 필드는 구현 기능인 PDP 마스터 제어 블록의 사용과 관련이 있습니다. 이 카운터는 문제 해결을 위해 Cisco Technical Support에서 사용되며 엔 유저와 직접적인 관련이 없습니다.
pdp_non_existent	존재하지 않는 PDP 상황에 대해 수신된 메시지를 표시합니다.

다음 명령은 PDP 상황에 대한 정보를 표시합니다.

```
> show service-policy inspect gtp pdp-context
4 in use, 5 most used
Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146
```

다음 표에는 **show service-policy inspect gtp pdp-context** 명령 출력에 대한 설명이 나와 있습니다.

표 ***42: PDP*** 상황

열 머리글	설명
버전	GTP 버전을 표시합니다.
TID	터널 식별자를 표시합니다.
MS Addr	모바일 스테이션 주소를 표시합니다.
SGSN Addr SGW Addr	SGSN(serving gateway service node) 또는 SGW(serving gateway)를 표시합니다.
Idle	PDP 또는 전달자(bearer) 상황이 사용되지 않은 시간을 표시합니다.
APN	액세스 포인트 이름을 표시합니다.

명령	설명
clear service-policy	모든 서비스 정책 통계를 지웁니다.
configure inspection	기본 검사를 활성 또는 비활성화합니다.
show running-config service-policy	실행 중인 컨피그레이션에 구성된 서비스 정책을 표시합니다.

show shun

차단 정보를 표시하려면 **show shun** 명령을 사용합니다.

show shun [*src_ip* | **statistics**]

src_ip	(선택 사항) 해당 주소에 대한 정보를 표시합니다.
statistics	(선택 사항) 인터페이스 차단 통계를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show shun** 명령의 샘플 출력입니다.

```
> show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

명령	설명
clear shun	현재 사용 설정된 모든 shun을 사용 해제하고 shun 통계를 지웁니다.
shun	새 연결을 방지하고 모든 기존 연결의 패킷을 거부하여 공격 호스트에 대한 동적 응답을 사용합니다.

show sip

SIP 세션을 표시하려면 **show sip** 명령을 사용합니다.

show sip

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show sip 명령은 Firepower Threat Defense 디바이스에 설정된 SIP 세션의 정보를 표시합니다.

다음은 **show sip** 명령의 샘플 출력입니다.

```
> show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 | state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 | state Active, idle 0:00:06
```

이 샘플에서는 Firepower Threat Defense 디바이스에 있는 2개의 활성 SIP 세션을 보여줍니다(Total 필드에 표시됨). 각 call-id는 통화를 나타냅니다.

첫 번째 세션(call-id c3943000-960ca-2e43-228f@10.130.56.44)은 Call Init 상태인데, 이는 세션이 아직 통화 설정 중임을 의미합니다. 통화 설정은 ACK가 표시된 경우에만 완료됩니다. 이 세션은 1 초 동안 유휴 상태였습니다.

두 번째 세션은 Active 상태인데, 이는 통화 설정이 완료되었고 엔드포인트가 미디어를 교환 중임을 의미합니다. 이 세션은 6초 동안 유휴 상태였습니다.

명령	설명
show conn	여러 연결 유형에 대한 연결 상태를 표시합니다.

show skinny

SCCP(Skinny) 세션에 대한 정보를 표시하려면 **show skinny** 명령을 사용합니다.

show skinny [**audio** | **video**]

audio	SCCP 오디오 세션을 표시합니다.
비디오	SCCP 비디오 세션을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 아래 조건에 따른 **show skinny** 명령의 샘플 출력입니다. 두 개의 활성 Skinny 세션이 디바이스에 설정되어 있습니다. 첫 번째 세션은 내부 Cisco IP Phone(로컬 주소 10.0.0.11)과 외부 Cisco Unified Communications Manager(172.18.1.33) 간에 설정되었습니다. TCP 포트 2000은 Cisco Unified Communications Manager입니다. 두 번째 세션은 다른 내부 Cisco IP Phone(로컬 주소 10.0.0.22)과 Cisco Unified Communications Manager 간에 설정되었습니다.

```
> show skinny
MEDIA 10.0.0.22/20798         172.18.1.11/22948
LOCAL                     FOREIGN                 STATE
-----------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000                1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000                1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

이 출력은 두 개의 내부 Cisco IP Phone 모두 간에 통화가 설정되었음을 나타냅니다. 첫 번째 전화와 두 번째 전화의 RTP 수신 대기 포트는 각각 UDP 22948 및 20798입니다.

명령	설명
show conn	여러 연결 유형에 대한 연결 상태를 표시합니다.

show sla monitor

IP SLA(Internet Protocol Service Level Agreement)에 대한 정보를 표시하려면 **show sla monitor** 명령을 사용합니다.

show sla monitor {**configuration** | **operational-state**} [*sla_id*]

구성	기본값을 포함하여 SLA 구성 값을 표시합니다.
operational-state	SLA 작업의 운영 상태를 표시합니다.
sla_id	(선택 사항) SLA 작업의 ID 번호입니다. 유효한 값은 1 ~ 2147483647입니다.

SLA ID를 지정하지 않으면 모든 SLA 작업에 대한 구성 값이 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show running-config sla monitor 명령을 사용하여 실행 중인 구성의 SLA 작업 명령을 확인할 수 있습니다.

다음은 **show sla monitor configuration** 명령의 샘플 출력입니다. SLA 작업 124에 대한 구성 값을 표시합니다. **show sla monitor configuration** 명령의 출력 뒤에는 동일한 SLA 작업에 대한 **show running-config sla monitor** 명령의 출력이 나와 있습니다.

```
> show sla monitor configuration 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
```

```
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

```
> show running-config sla monitor 124

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

다음은 **show sla monitor operational-state** 명령의 샘플 출력입니다.

```
> show sla monitor operational-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

명령	설명
show running-config sla monitor	실행 중인 구성의 SLA 작업 구성 명령을 표시합니다.

show snmp-server

디바이스에 구성된 SNMP 서버에 대한 정보를 표시하려면 **show snmp-server** 명령을 사용합니다.

show snmp-server {**engineID** | **group** | **host** | **statistics** | **user** [*username*]}

engineID	SNMP 엔진의 ID를 표시합니다.
group	구성된 SNMP 그룹의 이름, 사용 중인 보안 모델, 다양한 보기의 상태 및 각 그룹의 스토리지 유형을 표시합니다.
host	호스트 그룹에 속하는 구성된 SNMP 호스트의 이름, 사용되는 인터페이스, 사용되는 SNMP 버전을 표시합니다.
statistics	SNMP 서버 통계를 표시합니다.
user[*username*]	SNMP 사용자의 특성에 대한 정보를 표시합니다. 해당 사용자로 정보를 제한하려면 사용자 이름을 선택적으로 지정할 수 있습니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

SNMP 엔진은 로컬 디바이스에 상주할 수 있는 SNMP의 사본입니다. 엔진 ID는 각 SNMP 에이전트에 할당되는 고유한 값입니다. 엔진 ID는 구성할 수 없습니다. 엔진 ID는 25바이트이며 암호화된 비밀번호를 생성하는 데 사용됩니다. 대체작동 쌍에서는 엔진 ID가 피어와 동기화됩니다.

SNMP 사용자 및 그룹은 SNMP에 대한 VACM(보기 기반 액세스 제어 모델)에 따라 사용됩니다. SNMP 그룹에 따라 사용할 보안 모델이 결정됩니다. SNMP 사용자는 SNMP 그룹의 보안 모델과 일치해야 합니다. 각 SNMP 그룹 이름과 보안 수준 쌍은 고유해야 합니다.

다음은 **show snmp-server engineid** 명령의 샘플 출력입니다.

```
> show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

다음은 **show snmp-server group** 명령의 샘플 출력입니다.

```
> show snmp-server group
groupname: public                              security model:v1
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active

groupname: public                              security model:v2c
readview : <no readview specified>             writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active

groupname: privgroup                       security model:v3 priv
readview : def_read_view                   writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

다음은 **show snmp-server host** 명령의 샘플 출력이며 디바이스를 폴링하는 액티브 호스트만 표시합니다.

```
> show snmp-server host
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
```

다음은 **show snmp-server user** 명령의 샘플 출력입니다.

```
> show snmp-server user authuser
User name: authuser
Engine ID: 000000090200000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

이 출력은 다음 정보를 제공합니다.

- SNMP 사용자의 이름을 식별하는 문자열인 사용자 이름
- 디바이스에서 SNMP 사본을 식별하는 문자열인 엔진 ID
- 설정이 디바이스의 휘발성 또는 임시 메모리에 설정되었는지, 아니면 비휘발성 또는 영구 메모리에 설정(디바이스가 꺼졌다가 다시 켜진 후에도 설정이 그대로 유지됨)되었는지 여부를 나타내는 저장소 유형
- SNMP 사용자와 연계된 표준 IP 액세스 목록인 활성 액세스 목록
- 활성인지 또는 비활성인지 나타내는 행 상태
- 사용 중인 인증 프로토콜을 식별하는 인증 프로토콜(옵션은 MD5, SHA 또는 none). 소프트웨어 이미지에서 인증이 지원되지 않는 경우에는 이 필드가 표시되지 않습니다.
- DES 패킷 암호화가 활성화되었는지 여부를 나타내는 개인 정보 프로토콜. 소프트웨어 이미지에서 개인 정보가 지원되지 않는 경우에는 이 필드가 표시되지 않습니다.

- 사용자가 속한 SNMP 그룹을 나타내는 그룹 이름. SNMP 그룹은 VACM(보기 기반 액세스 제어 모델)에 따라 정의됨

명령	설명
clear snmp-server statistics	SNMP 패킷 입력 및 출력 카운터를 지웁니다.
show running-config snmp-server	SNMP 서버 구성을 표시합니다.

show snort statistics

Snort에서 트래픽이 검사될 경우 다양한 Snort 결정과 일치하는 패킷 수를 표시하려면 **show snort statistics** 명령을 사용합니다.

show snort statistics

릴리스	수정 사항
6.0.1	이 명령이 도입되었습니다.

사용 가이드라인

액세스 정책 및 침입 규칙 컨피그레이션의 Snort 검사 결과를 표시하려면 이 명령을 사용합니다. 일반적으로 이 명령은 예기치 않은 Snort 검사 동작을 디버깅할 때 사용됩니다.

다음 샘플 기록은 **show snort statistics** 명령을 통해 표시되는 정보를 보여줍니다.

```
> show snort statistics
Packet Counters:
  Passed Packets                                                6
  Blocked Packets                                               321
  Injected Packets                                              284
  Packets bypassed (Snort Down)                                 0
  Packets bypassed (Snort Busy)                                 0

Flow Counters:
  Fast-Forwarded Flows                                          0
  Blacklisted Flows                                             0

Miscellaneous Counters:
  Start-of-Flow events                                          0
  End-of-Flow events                                            0
  Denied flow events                                            0
  Frames forwarded to Snort before drop                         0
  Inject packets dropped                                        0
```

명령	설명
clear snort statistics	Snort 검사 통계를 지웁니다.

show software authenticity

소프트웨어 인증 정보를 표시하려면 **show software authenticity** 명령을 사용합니다.

show software authenticity {**development** | **file** *filename* | **keys** | **running**}

development	개발 키 서명 이미지의 로딩이 활성화 또는 비활성화될지 여부를 표시합니다.
file*filename*	특정 이미지 파일에 대한 소프트웨어 인증과 관련된 디지털 서명 정보를 표시합니다.
keys	SPI 플래시에 저장되는 릴리스 키 및 개발 키에 대한 정보를 표시합니다.
running	현재 실행 중인 이미지 파일에 대한 소프트웨어 인증과 관련된 디지털 서명 정보를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

파일 및 실행 중인 이미지의 출력은 다음 정보를 제공합니다.

- 메모리에 있는 파일의 이름인 파일 이름
- 표시되는 이미지의 유형인 이미지 유형
- 다음과 같은 서명 정보를 지정하는 서명자 정보
  - 소프트웨어 제조업체의 이름인 공통 이름
  - 소프트웨어 이미지가 배포된 하드웨어를 나타내는 조직 구성 단위
  - 소프트웨어 이미지의 소유자인 조직 이름
- 디지털 서명에 대한 인증서 일련 번호인 인증서 일련 번호
- 디지털 서명 확인에 사용되는 해시 알고리즘의 유형을 나타내는 해시 알고리즘
- 디지털 서명 확인에 사용되는 서명 알고리즘의 유형을 식별하는 서명 알고리즘

- 확인에 사용되는 키 버전을 나타내는 키 버전

다음은 **show software authenticity development** 명령의 샘플 출력입니다.

```
> show software authenticity development
Loading of development images is disabled
```

다음은 **show software authenticity file** 명령의 샘플 출력입니다. 이 예에서 파일은 개발 이미지입니다. 디바이스에서 현재 실행 중인 이미지 파일에 대한 정보는 **show software authenticity running**의 동일한 출력을 확인하십시오.

```
> show software authenticity file os.img
File Name                     : disk0:/os.img
Image type                    : Development
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 57F4610F
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

다음은 show software authenticity keys 명령의 샘플 출력입니다.

```
> show software authenticity keys
Public Key #1 Information
-------------------------
Key Type              : Release (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #2 Information
-------------------------
Key Type              : Development (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
```

```
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
Public Key #3 Information
--------------------------
Key Type              : Release (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #4 Information
--------------------------
Key Type              : Development (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
```

명령	설명
show version	소프트웨어 버전, 하드웨어 컨피그레이션, 라이센스 키 및 관련 가동 시간 데이터를 표시합니다.

show ssh-access-list

관리 인터페이스에 대한 SSH 액세스 목록 설정을 표시하려면 **show ssh-access-list** 명령을 사용합니다.

show ssh-access-list

릴리스	수정 사항
6.0.1	이 명령이 도입되었습니다.

사용 가이드라인

관리 인터페이스에 대한 SSH 액세스 목록 설정을 표시하려면 이 명령을 사용합니다. 액세스 목록은 어떤 IP 주소 사용자가 관리 IP 주소에 대한 SSH 연결을 시도할 수 있는지를 결정합니다. 이 목록은 데이터 인터페이스에 대한 SSH 액세스를 제어하지 않습니다.

다음 샘플은 **show ssh-access-list** 명령의 기본 출력입니다. 이 액세스 목록을 사용하면 임의의 IP 주소에서 관리 IP 주소로 SSH 연결이 가능합니다. 실제로 SSH 연결을 완료하려면 모든 사용자는 유효한 사용자 이름/비밀번호를 제공해야 합니다.

```
> show ssh-access-list
ACCEPT     tcp  --  anywhere             anywhere             state NEW tcp dpt:ssh
ACCEPT     tcp      anywhere             anywhere             state NEW tcp dpt:ssh
```

명령	설명
configure ssh-access-list	관리 인터페이스를 위한 SSH 액세스 목록을 구성합니다.

show ssl

활성 SSL 세션 및 사용 가능한 암호에 대한 정보를 표시하려면 **show ssl** 명령을 사용합니다.

show ssl [**cache** | **ciphers** [*level*] | **errors** [**trace**] | **mib** [**64**] | **objects**]

cache	(선택 사항) SSL 세션 캐시 통계를 표시합니다.
ciphers	(선택 사항) 사용할 수 있는 SSL 암호를 표시합니다. 암호 강도를 표시하는 특정 레벨에 사용 가능한 암호만 보려면 level 키워드를 포함합니다. 다음은 사용 가능한 레벨(강도 오름차순)입니다. • **all** • **low** • **medium**(레벨을 지정하지 않을 경우 기본값) • **fips** • **high**(TLSv1.2에만 적용됨)
errors [**trace**]	(선택 사항) SSL 오류를 표시합니다. 각 오류에 대한 추적 정보를 포함하도록 trace 키워드를 포함합니다.
mib [**64**]	(선택 사항) SSL MIB 통계를 표시합니다. 64비트 카운터 통계를 보려면 64 키워드를 포함합니다.
objects	(선택 사항) SSL 개체 통계를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 활성화된 암호 순서, 비활성화된 암호, 사용 중인 SSL 신뢰 지점, 인증서 인증 사용 여부 등 현재 SSLv3 이상 세션에 대한 정보를 표시합니다. 이 설정은 관리 인터페이스에서가 아니라 데이터 인터페이스에서의 SSL 연결에 사용됩니다.

다음은 **show ssl** 명령의 샘플 출력입니다.

```
> show ssl
Accept connections using SSLv3 or greater and negotiate to TLSv1 or greater
Start connections using TLSv1 and negotiate to TLSv1 or greater
SSL DH Group: group2 (1024-bit modulus)
SSL ECDH Group: group19 (256-bit EC)

SSL trust-points:
  Self-signed (RSA 2048 bits RSA-SHA256) certificate available
  Self-signed (EC 256 bits ecdsa-with-SHA256) certificate available
Certificate authentication is not enabled
```

다음은 **show ssl ciphers** 명령의 샘플 출력입니다.

```
> show ssl ciphers
Current cipher configuration:
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
```

```
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
  DES-CBC3-SHA
>
```

show ssl-policy-config

정책 설명, 기본 로깅 설명, 사용 설정된 모든 SSL 규칙 및 규칙 구성, 신뢰받는 CA 인증서, 해독 불가 트래픽 작업을 포함하여 현재 적용된 SSL 정책 구성을 표시하려면 **show ssl-policy-config** 명령을 사용합니다.

show ssl-policy-config

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

Firepower Management Center에서 SSL 정책을 구성하고 디바이스에 할당된 액세스 제어 정책에 연결합니다. 디바이스를 통과하는 트래픽에서 SSL 해독을 위해 구성된 작업에 대한 정보를 표시하기 위해 이 명령을 사용할 수 있습니다.

다음 예에서는 디바이스에 대한 SSL 정책을 구성하지 않은 경우 어떤 항목이 표시되는지 보여줍니다.

```
> show ssl-policy-config
SSL policy not yet applied.
```

다음 예에서는 구성된 SSL 정책을 보여줍니다.

```
> show ssl-policy-config
===============[ General SSL Policy ]===============

=================[ Default Action ]=================
Default Action            : Do Not Decrypt

======[ Category: admin_category (Built-in) ]=======

=====[ Category: standard_category (Built-in) ]=====

----------[ Block unwanted applications ]-----------
State                     : Enabled
Action                    : Block
Source Zones              : outside_zone
Destination Zones         : dmz_zone
Applications              : HTTP/SSL Tunnel (3860)

=======[ Category: root_category (Built-in) ]=======

============[ Trusted CA Certificates ]=============

Cisco-Trusted-Authorities (group)
                             thawte-Primary-Root-CA
                             UTN-DATACorp-SGC
```

```
                                Chambers-of-Commerce-Root-2008
                                Izenpe.com-1
                                A-Trust-Qual-02
                                A-Trust-nQual-03
                                Common-Policy
                                Starfield-Root-Certificate-Authority-G2
                                GeoTrust-Primary-Certification-Authority
                                Certum-Trusted-Network-CA
                                UTN-USERFirst-Object

C_US-O_VeriSign-Inc.-OU_Class-3-Public-Primary-Certification-Authority-G2-OU_
c-1998-VeriSign-Inc.-For-authorized-use-only-OU_VeriSign-Trust-Network
                                CA-Disig-Root-R1
                                C_US-O_Equifax-OU_Equifax-Secure-Certificate-Authority
                                Thawte-Server-CA-1
                                VeriSign-Class-3-Public-Primary-Certification-Authority-G3
                                COMODO-Certification-Authority
                                VeriSign-Class-3-Public-Primary-Certification-Authority-G5
                                UTN-USERFirst-Client-Authentication-and-Email
                                TC-TrustCenter-Universal-CA-III
                                Cisco-Root-CA-2048
                                Staat-der-Nederlanden-Root-CA-G2

(...Remaining trusted CA certificates removed...)

=============[ Undecryptable Actions ]==============
Unsupported Cipher Suite  : Inherit Default Action
Unknown Cipher Suite      : Inherit Default Action
Compressed Session        : Inherit Default Action
Uncached Session ID       : Inherit Default Action
SSLv2 Session             : Inherit Default Action
Handshake Error           : Inherit Default Action
Decryption Error          : Block
```

명령	설명
show access-policy-config	현재 구성된 액세스 제어 정책에 대한 정보를 표시합니다.

show ssl-protocol

로컬 디바이스 관리자(Firepower Device Manager)에 대한 HTTPS 액세스를 위해 현재 구성되어 있는 SSL 프로토콜을 표시하려면 **show ssl-protocol** 명령을 사용합니다.

show ssl-protocol

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

관리 인터페이스에 대해 구성된 SSL 프로토콜을 확인하려면 이 명령을 사용합니다. 이것은 HTTPS 연결을 위해 허용된 프로토콜로, 로컬 관리자인 Firepower Device Manager를 여는 데 사용됩니다. 이 프로토콜은 원격 관리자에는 사용되지 않습니다.

이 프로토콜을 구성하려면 **configure ssl-protocol** 명령을 사용합니다.

다음 예는 로컬 관리자를 사용할 때 현재 정의된 SSL 프로토콜을 확인하는 방법을 보여줍니다.

```
> show ssl-protocol
The supported ssl protocols are TLSv1.1 TLSv1.2
```

명령	설명
configure ssl-protocol	관리 인터페이스에 대한 HTTPS 액세스를 위해 SSL 프로토콜을 구성합니다.

show startup-config

시작 컨피그레이션 또는 시작 컨피그레이션 로드 시 오류를 표시하려면 **show startup-config** 명령을 사용합니다.

show startup-config [**errors**]

errors	(선택 사항) 시작 컨피그레이션을 로드할 때 생성된 모든 오류를 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show startup-config 명령은 시작 시스템 컨피그레이션을 표시합니다. 직접 이 명령을 구성할 수 없습니다. 대신, 이 명령은 디바이스를 제어하는 관리자를 통해 구성할 수 있습니다. 예를 들어, Firepower Management Center 또는 Firepower Device Manager가 있습니다.

그러나, 이것은 부분적인 컨피그레이션입니다. 이것은 ASA 소프트웨어 컨피그레이션 명령만 사용하여 구성될 수 있는 경우를 보여줍니다. 단, 일부 명령은 Firepower Threat Defense에 특정할 수 있습니다. 이 명령은 Firepower Threat Defense로 복사됩니다. 따라서, 문제 해결 지원용으로만 시작 컨피그레이션 정보를 사용해야 합니다. 디바이스 컨피그레이션을 분석하기 위한 기본 방법으로 디바이스 관리자를 사용합니다.

다음은 **show startup-config** 명령의 샘플 출력입니다.

```
> show startup-config
: Saved

:
: Serial Number: JAD192100RG
: Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores)
: Written by enable_1 at 20:39:10.749 UTC Tue Jun 28 2016
!
NGFW Version 6.1.0
!
hostname firepower
enable password 8Ry2YjIyt7RRXU24 encrypted
names
```

```
(...Output Truncated...)
```

명령	설명
show running-config	실행 중인 컨피그레이션을 표시합니다.

show summary

디바이스에 대한 가장 흔히 사용되는 정보(버전, 유형 UUID 등)의 요약을 표시하려면 **show summary** 명령을 사용합니다.

show summary

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

요약 정보는 기본 **show version** 출력과 적용된 정책 및 Snort 버전 정보의 목록을 포함합니다.

다음은 요약 정보를 보여주는 예입니다.

```
> show summary
--------[ ftd1.example.com ]---------
Model                     : Cisco ASA5512-X Threat Defense (75) Version 6.1.0 (Build 2007)
UUID                      : 703006f4-8ff6-11e6-bb6e-8f2d5febf243
Rules update version      : 2016-03-28-001-vrt
VDB version               : 271
-----------------------------------------------------

------------------[ policy info ]--------------------
Access Control Policy     : Initial AC Policy
Intrusion Policy          : Balanced Security and Connectivity

-----------------------------------------------------

---------------[ snort version info ]---------------
Snort Version             : 2.9.10 GRE (Build 20)
libpcap Version           : 1.1.1
PCRE Version              : 7.6 2008-01-28
ZLIB Version              : 1.2.8
-----------------------------------------------------
```

show sunrpc-server active

NFS 및 NIS 같이 Sun RPC 서비스에 대해 열려 있는 핀홀을 표시하려면 **show sunrpc-server active** 명령을 사용합니다.

show sunrpc-server active

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음은 **show sunrpc-server active** 명령의 샘플 출력입니다.

```
> show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        ------------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

LOCAL 열의 항목은 내부 인터페이스에 있는 클라이언트 또는 서버의 IP 주소를 보여주는 반면, FOREIGN 열의 값은 외부 인터페이스에 있는 클라이언트 또는 서버의 IP 주소를 보여줍니다.

명령	설명
clear sunrpc-server active	Sun RPC 서비스에 대해 열려 있는 핀홀(예: NFS 및 NIS)을 지웁니다.
show running-config sunrpc-server	SunRPC 서비스 컨피그레이션에 대한 정보를 표시합니다.

show tcpstat

TCP 스택의 상태 및 디바이스에서 종료되는 TCP 연결을 표시하려면(디버깅용) **show tcpstat** 명령을 사용합니다.

show tcpstat

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show tcpstat 명령을 사용하여 TCP 스택의 상태 및 디바이스에서 종료되는 TCP 연결을 표시할 수 있습니다. 표시되는 TCP 통계는 다음 표에 설명되어 있습니다.

표 ***43: show tcpstat*** 명령의 ***TCP*** 통계

통계	설명
tcb_cnt	TCP 사용자 수입니다.
proxy_cnt	TCP 프록시 수입니다. TCP 프록시는 사용자 권한 부여에서 사용됩니다.
tcp_xmt pkts	TCP 스택에서 전송된 패킷 수입니다.
tcp_rcv good pkts	TCP 스택에서 수신된 정상 패킷 수입니다.
tcp_rcv drop pkts	TCP 스택에서 삭제된 수신 패킷 수입니다.
tcp bad chksum	체크섬이 잘못된 수신 패킷 수입니다.
tcp user hash add	해시 테이블에 추가된 TCP 사용자 수입니다.
tcp user hash add dup	새 사용자를 추가하려고 할 때 TCP 사용자가 해시 테이블에 이미 존재한 횟수입니다.
tcp user srch hash hit	검색할 때 해시 테이블에서 TCP 사용자가 발견된 횟수입니다.
tcp user srch hash miss	검색할 때 해시 테이블에서 TCP 사용자가 발견되지 않은 횟수입니다.
tcp user hash delete	해시 테이블에서 TCP 사용자가 삭제된 횟수입니다.

통계	설명
tcp user hash delete miss	사용자를 삭제하려고 할 때 해시 테이블에서 TCP 사용자가 발견되지 않은 횟수입니다.
lip	TCP 사용자의 로컬 IP 주소입니다.
fip	TCP 사용자의 외부 IP 주소입니다.
lp	TCP 사용자의 로컬 포트입니다.
fp	TCP 사용자의 외부 포트입니다.
st	TCP 사용자의 상태입니다(RFC 793 참고). 가능한 값은 다음과 같습니다. 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	TCP 사용자의 재전송 대기열 기간입니다.
inqlen	TCP 사용자의 입력 대기열 기간입니다.
tw_timer	TCP 사용자의 time_wait 타이머 값(밀리초)입니다.
to_timer	TCP 사용자의 비활성 시간 제한 타이머 값(밀리초)입니다.
cl_timer	TCP 사용자의 닫기 요청 타이머 값(밀리초)입니다.
per_timer	TCP 사용자의 지속 타이머 값(밀리초)입니다.
rt_timer	TCP 사용자의 재전송 타이머 값(밀리초)입니다.
tries	TCP 사용자의 재전송 횟수입니다.

다음 예에서는 TCP 스택 상태를 표시하는 방법을 보여줍니다.

```
> show tcpstat
                 CURRENT MAX      TOTAL
tcb_cnt          2       12       320
```

```
proxy_cnt       0       0       160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 203.0.113.45 fip = 192.0.2.12 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
  rt_timer = 0 tries 0
```

명령	설명
show conn	사용된 연결 및 사용할 수 있는 연결을 표시합니다.

show tech-support

기술 지원 분석가가 진단에 사용하는 정보를 표시하려면 **show tech-support** 명령을 사용합니다.

show tech-support

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show tech-support 명령을 사용하여 기술 지원 분석가가 문제를 진단하는 데 필요한 정보를 나열할 수 있습니다.

다음 예에서는 기술 지원 분석가용으로 사용되는 정보를 표시하는 방법을 보여 줍니다. 출력은 처음 부분만 표시하도록 단축됩니다.

```
> show tech-support

-------------[ ftd1.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (B
uild 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
------------------------------------------------

Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 3 days 16 hours

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB
Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
(...Remaining output truncated...)
```

show time

디바이스에 대한 UTC 및 현지 시간과 날짜를 표시하려면 **show time** 명령을 사용합니다.

show time

릴리스	수정 사항
6.0.1	이 명령이 도입되었습니다.

다음은 **show time** 명령의 샘플 출력입니다.

```
> show time
UTC -       Wed Aug  3 17:04:06 UTC 2016
Localtime - Wed Aug 03 13:04:06 EDT 2016
```

show traffic

인터페이스 전송 및 수신 활동을 표시하려면 **show traffic** 명령을 사용합니다.

show traffic

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show traffic 명령은 **show traffic** 명령이 마지막으로 입력되거나 디바이스가 온라인 상태가 된 이후에 각 인터페이스를 통해 이동한 패킷 및 바이트 수를 나열합니다. 시간(초)은 디바이스가 마지막 재부팅 후 온라인 상태로 유지된 기간입니다(마지막 재부팅 후 **clear traffic** 명령이 입력되지 않은 경우). 마지막 재부팅 후 clear traffic 명령이 입력된 경우 시간(초)은 해당 명령이 입력된 이후의 기간입니다.

통계는 인터페이스 이름을 기준으로 첫 번째로 표시됩니다. 명명된 인터페이스 이후에 통계는 물리적 인터페이스를 기준으로 표시됩니다. 인터페이스는 내부 통신을 위해 시스템에서 사용된 숨겨진 가상 인터페이스를 포함할 수 있습니다.

다음은 단일 인터페이스의 통계를 표시하는 **show traffic** 명령의 축약된 샘플 출력입니다. 각 인터페이스는 동일한 통계를 보여줍니다.

```
> show traffic
...
diagnostic:
        received (in 102.080 secs):
                2048 packets     204295 bytes
                20 pkts/sec      2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets       204056 bytes
                20 pkts/sec      1998 bytes/sec
      1 minute input rate 122880 pkts/sec,  5775360 bytes/sec
      1 minute output rate 122887 pkts/sec,  5775389 bytes/sec
      1 minute drop rate, 3 pkts/sec
      5 minute input rate 118347 pkts/sec,  5562309 bytes/sec
      5 minute output rate 119221 pkts/sec,  5603387 bytes/sec
      5 minute drop rate, 11 pkts/sec
...
```

명령	설명
clear traffic	전송 및 수신 활동에 대한 카운터를 재설정합니다.

show uauth

이 명령을 사용하지 마십시오. 이 명령은 Firepower Threat Defense에서 지원하지 않는 기능과 관련이 있습니다.

show user

디바이스에서 CLI(Command Line Interface)에 액세스하기 위해 사용자 계정을 표시하려면 **show user** 명령을 사용합니다.

show user [*username1* [*usernam2*] [...]]

username1 [*usernam2*] [...]	(선택 사항) 하나 이상의 공백으로 구분된 사용자 이름. 이름을 지정하지 않으면 모든 사용자가 표시됩니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

다음 정보는 각 사용자에 대해 표시됩니다. **configure user add** 명령을 사용하여 사용자 계정을 생성합니다.

- Login - 로그인 이름
- UID - 숫자 사용자 ID.
- Auth - 사용자가 인증되는 방식(로컬 또는 원격(디렉토리 서버를 통해) 중 하나).
- Access - 사용자의 권한 수준(기본 또는 Config). 이 설정을 변경하려면 **configure user access** 명령을 사용합니다.
- Enabled - 사용자가 활성 상태인지 여부(활성화됨 또는 비활성화됨). 이 설정을 변경하려면 **configure user enable**/**disable** 명령을 사용합니다.
- Reset - 사용자가 다음 로그인 시 계정 비밀번호를 변경해야 하는지 여부(예 또는 아니요). 이 설정을 변경하려면 **configure user forcereset** 명령을 사용합니다.
- Exp - 사용자 비밀번호가 변경될 때까지의 일 수. 비밀번호가 만료되지 않음을 나타내지 않습니다. 이 설정을 변경하려면 **configure user aging** 명령을 사용합니다.
- Warn - 비밀번호가 만료되기 전에 비밀번호를 변경하도록 사용자에게 제공된 일수를 지정합니다. N/A는 경고를 적용할 수 없음을 나타냅니다. 이 설정을 변경하려면 **configure user aging** 명령을 사용합니다.

- Str - 사용자 비밀번호가 강도 검사 기준을 충족해야 하는지 여부(Dis - 비활성화 또는 Ena(활성화)). **configure user strengthcheck** 명령을 사용하여 이 옵션을 구성합니다.
- Lock - 너무 많은 로그인 실패 때문에 사용자 계정이 잠겼는지 여부(예 또는 아니요). **configure user unlock** 명령을 사용하여 사용자 계정의 잠금을 해제합니다.
- Max - 사용자 계정을 잠그기 전에 실패한 로그인의 최대 수. N/A는 계정을 잠글 수 없음을 나타냅니다. 이 설정을 변경하려면 configure user maxfailedlogins 명령을 사용합니다.

다음 예에서는 CLI 액세스에 대해 정의된 사용자를 표시하는 방법을 보여줍니다.

```
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
admin2            1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

명령	설명
configure user add	CLI 액세스를 위한 사용자 계정을 추가합니다.

show version

하드웨어 모델, 소프트웨어 버전, UUID, 침입 규칙 업데이트 버전 및 VDB 버전을 표시하려면 **show version** 명령을 사용합니다.

show version [**detail** | **system**]

detail	**show version** 및 **show version detail**은 동일한 정보를 표시합니다.
system	이 키워드는 **show version**을 사용하여 표시된 정보에 추가 시스템 정보를 추가합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show version 명령과 **show version detail** 명령은 동일한 기본 시스템 정보를 표시합니다. **show version system** 명령은 마지막 재부팅 이후 가동 시간과 특정한 하드웨어 추가 정보 같은 추가 시스템 정보를 표시합니다.

다음 예에서는 기본 **show version** 출력을 보여줍니다.

```
> show version
-------------[ example-sfr.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
------------------------------------------------------
```

show version system 명령의 다음 샘플 출력은 추가 정보와 함께 **show version** 명령과 동일한 출력을 추가합니다.

```
> show version system
-------------[ example-sfr.example.com ]--------------
Model                     : Cisco ASA5508-X Threat Defense (75) Version 6.1.0 (Build 226)
UUID                      : 43235986-2363-11e6-b278-aff0a43948fe
Rules update version      : 2016-03-28-001-vrt
VDB version               : 270
------------------------------------------------------
```

```
Cisco Adaptive Security Appliance Software Version 9.6(1)72

Compiled on Fri 20-May-16 13:36 PDT by builders
System image file is "disk0:/os.img"
Config file at boot was "startup-config"

firepower up 36 days 21 hours

Hardware:   ASA5508, 8192 MB RAM, CPU Atom C2000 series 2000 MHz, 1 CPU (8 cores
)
Internal ATA Compact Flash, 8192MB
BIOS Flash M25P64 @ 0xfed01000, 16384KB

Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1
)
                             Number of accelerators: 1

 1: Ext: GigabitEthernet1/1  : address is e865.49b8.97f2, irq 255
 2: Ext: GigabitEthernet1/2  : address is e865.49b8.97f3, irq 255
 3: Ext: GigabitEthernet1/3  : address is e865.49b8.97f4, irq 255
 4: Ext: GigabitEthernet1/4  : address is e865.49b8.97f5, irq 255
 5: Ext: GigabitEthernet1/5  : address is e865.49b8.97f6, irq 255
 6: Ext: GigabitEthernet1/6  : address is e865.49b8.97f7, irq 255
 7: Ext: GigabitEthernet1/7  : address is e865.49b8.97f8, irq 255
 8: Ext: GigabitEthernet1/8  : address is e865.49b8.97f9, irq 255
 9: Int: Internal-Data1/1    : address is e865.49b8.97f1, irq 255
10: Int: Internal-Data1/2    : address is 0000.0001.0002, irq 0
11: Int: Internal-Control1/1 : address is 0000.0001.0001, irq 0
12: Int: Internal-Data1/3    : address is 0000.0001.0003, irq 0
13: Ext: Management1/1       : address is e865.49b8.97f1, irq 0
14: Int: Internal-Data1/4    : address is 0000.0100.0001, irq 0

Serial Number: JAD192100RG
Configuration register is 0x1
Image type                : Release
Key Version               : A
Configuration last modified by enable_1 at 12:44:37.849 UTC Mon Jul 25 2016
```

show vlan

Firepower Threat Defense 디바이스에 구성된 모든 VLAN을 표시하려면 **show vlan** 명령을 사용합니다.

show vlan [**mapping** [*primary_id*]]

mapping	(선택 사항) 기본 VLAN에 매핑된 보조 VLAN을 표시합니다.
primary_id	(선택 사항) 특정한 기본 VLAN에 대한 보조 VLAN을 표시합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 구성된 VLAN을 표시합니다.

```
> show vlan
10-11,30,40,300
```

다음 예에서는 각각의 기본 VLAN에 매핑된 보조 VLAN을 표시합니다.

```
> show vlan mapping
Interface                   Secondary VLAN ID                   Mapped VLAN ID
0/1.100                     200                                            300
0/1.100                     201                                            300
0/2.500                     400                                            200
```

명령	설명
clear interface	**show interface** 명령에 대한 카운터를 지웁니다.
show interface	인터페이스의 런타임 상태 및 통계를 표시합니다.

show wccp

WCCP(Web Cache Communication Protocol)와 관련된 전역 통계를 표시하려면 **show wccp** 명령을 사용합니다.

show wccp {**web-cache** | *service_number*} [**buckets** | **detail** | **service** | **view** | **hash** *dest_addr source_addr dest_port source_port*]

show wccp [**interfaces** [**detail**]]

buckets	(선택 사항) 서비스 그룹 버킷 할당을 표시합니다.
detail	(선택 사항) 라우터 및 모든 웹 캐시에 대한 정보를 표시합니다.
hash*dest_addrsource_addr dest_port source_port*	(선택 사항) 지정된 연결에 대한 WCCP 해시를 표시합니다. • *dest_addr*은 대상 호스트의 IP 주소입니다. • *source_addr*은 소스 호스트의 IP 주소입니다. • *dest_port*는 대상 호스트의 포트입니다. • *source_port*는 소스 호스트의 포트입니다.
interfaces [**detail**]	(선택 사항) WCCP 리디렉션 인터페이스를 표시합니다. 인터페이스 구성에 대한 detail 키워드를 포함합니다.
service	(선택 사항) 서비스 그룹 정의 정보를 표시합니다.
service-number	캐시에서 제어되는 웹 캐시 서비스 그룹의 식별 번호입니다. 이 번호는 0에서 254 사이일 수 있습니다. Cisco Cache Engine을 사용하는 웹 캐시의 경우 역방향 프록시 서비스는 값 99로 표시됩니다.
보기	(선택 사항) 특정 서비스 그룹의 다른 멤버가 감지되거나 감지되지 않은지 여부를 표시합니다.
web-cache	웹 캐시 서비스에 대한 통계를 지정합니다.

릴리스	수정
6.2	이 명령이 추가되었습니다.

다음 예에서는 WCCP 정보를 표시하는 방법을 보여 줍니다.

```
> show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0
    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            0
        Redirect access-list:                foo
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   foobar
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
```

명령	설명
clear wccp	WCCP 통계를 지웁니다.

show xlate

NAT 세션(xlates 또는 변환)에 대한 정보를 표시하려면 **show xlate** 명령을 사용합니다.

show xlate [**global** *ip1*[*-ip2*] [**netmask** *mask*]] [**local** *ip1*[*-ip2*] [**netmask** *mask*]] [**gport** *port1*[*-port2*]] [**lport** *port1*[*-port2*]] [**interface** *if_name*] [**type** *type*]

show xlate count

count	변환 수를 표시합니다.
global*ip1*[*-ip2*]	(선택 사항) 매핑된 IP 주소 또는 주소 범위별 활성 변환을 표시합니다.
gport*port1*[*-port2*]	매핑된 포트 또는 포트 범위별 활성 변환을 표시합니다.
interface*if_name*	(선택 사항) 인터페이스별 활성 변환을 표시합니다.
local*ip1*[*-ip2*]	(선택 사항) 실제 IP 주소 또는 주소 범위별 활성 변환을 표시합니다.
lport*port1*[*-port2*]	실제 포트 또는 포트 범위별 활성 변환을 표시합니다.
netmask*mask*	(선택 사항) 매핑된 IP 주소 또는 실제 IP 주소를 정규화할 네트워크 마스크를 지정합니다.
type*type*	(선택 사항) 유형별 활성 변환을 표시합니다. 다음 유형 중 하나 이상을 입력할 수 있습니다. • **static** • **portmap** • 동적 • **twice-nat**(수동 NAT라고도 알려져 있음) 유형을 두 개 이상 지정할 경우 공백으로 구분합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

show xlate 명령은 변환 슬롯의 내용을 표시합니다. xlate는 내부 인터페이스에 대해 생성된 항목을 포함할 수 있으며 이것은 디바이스 관리자의 NAT 규칙 테이블에 나타나지 않습니다, 이것은 내부 프로세싱에 필요합니다.

VPN 클라이언트 컨피그레이션이 활성화되고 내부 호스트에서 DNS 요청을 전송하는 경우 **show xlate** 명령은 정적 변환에 대해 여러 xlate를 나열할 수 있습니다.

클러스터링 환경에서는 PAT 세션을 처리하기 위해 최대 3개의 xlate가 클러스터의 여러 노드에 복제될 수 있습니다. 하나는 연결을 소유한 디바이스에서 생성됩니다. 또 하나는 PAT 주소를 백업하기 위해 다른 유닛에서 생성됩니다. 마지막 하나는 흐름을 복제하는 디렉터에 존재합니다. 백업 및 디렉터가 같은 디바이스인 경우 3개 대신 2개의 xlate가 생성될 수 있습니다.

다음은 **show xlate** 명령의 샘플 출력입니다. nlp_int_tap의 초기 PAT xlate는 관리 인터페이스 주소 대신 192.168.1.1에 대한 Firepower Device Manager의 액세스를 허용하는 HTTPS 액세스 규칙과 관련이 있습니다. 이것은 해당 규칙이 디바이스 관리자의 NAT 테이블에 표시되지 않는 내부 NAT xlates입니다.

```
> show xlate
13 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_2:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_3:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_4:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_5:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_6:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
TCP PAT from nlp_int_tap:169.254.1.2 443-443 to inside1_7:192.168.1.1 443-443
    flags sr idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_8:0.0.0.0/0
    flags sIT idle 0:30:10 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_7:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_6:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_5:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_4:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_3:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
NAT from outside:0.0.0.0/0 to inside1_2:0.0.0.0/0
    flags sIT idle 124:39:20 timeout 0:00:00
```

다음은 IPv4에서 IPv6로의 변환을 표시하는 **show xlate** 명령의 샘플 출력입니다.

```
> show xlate
14 in use, 14 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
(...other entries removed...)
```

```
NAT from outside:0.0.0.0/0 to inside1_8:2001:db8::/96
    flags s idle 0:01:36 timeout 0:00:00
```

명령	설명
clear xlate	현재 변환 및 연결 정보를 지웁니다.
show conn	모든 활성 연결을 표시합니다.
show local-host	로컬 호스트 네트워크 정보를 표시합니다.

show zone

이 명령을 사용하지 마십시오. 이 명령은 Firepower Threat Defense에서 지원되지 않는 영역 기능과 관련이 있습니다. 이 명령은 보안 영역 컨피그레이션을 표시하지 않습니다.

shun

공격 호스트로부터 연결을 차단하려면 **shun** 명령을 사용합니다. shun을 사용 해제하려면 이 명령의 **no** 형식을 사용합니다.

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *source_ip* [**vlan** *vlan_id*]

dest_port	(선택 사항) 소스 IP 주소에 shun을 적용할 때, 연결을 끊고자 하는 현재 연결의 목적지 포트를 지정합니다.
dest_ip	(선택 사항) 소스 IP 주소에 shun을 적용할 때, 연결을 끊고자 하는 현재 연결의 목적지 주소를 지정합니다.
protocol	(선택 사항) UDP 또는 TCP와 같은 소스 IP 주소에 shun을 적용할 때 연결을 끊고자 하는 현재 연결의 IP 프로토콜을 지정합니다. 기본적으로 프로토콜은 0입니다(모든 프로토콜).
source_ip	공격 호스트의 주소를 지정합니다. 소스 IP 주소만 지정할 경우, 향후 이 주소에서의 모든 연결은 끊어지나 현재 연결은 그대로 유지됩니다. 현재 연결을 끊고 shun을 적용하려면 연결의 추가 파라미터를 지정합니다. 대상 파라미터에 상관없이 향후 소스 IP 주소의 모든 연결에 대해 shun이 유지됩니다.
source_port	(선택 사항) 소스 IP 주소에 shun을 적용할 때 연결을 끊고자 하는 현재 연결의 소스 포트를 지정합니다.
vlan*vlan_id*	(선택 사항) 소스 호스트가 상주하는 VLAN ID를 지정합니다.

기본 프로토콜은 0입니다(모든 프로토콜).

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

shun 명령을 사용하여 공격 호스트의 연결을 차단할 수 있습니다. 차단 기능을 수동으로 제거할 때까지 향후 이 소스 IP 주소의 모든 연결은 끊어지고 기록됩니다. **shun** 명령의 차단 기능은 지정된 호스트 주소와의 연결이 현재 활성 상태인지의 여부에 상관없이 적용됩니다.

목적지 주소와 소스 및 목적지 포트, 프로토콜을 지정한 경우 일치하는 연결을 삭제할 수 있을 뿐만 아니라 향후 해당 소스 IP 주소의 모든 연결에 shun을 적용할 수 있습니다. 그러면 특정 연결 파라미터와 일치하는 연결뿐만 아니라 이후의 모든 연결에 shun이 적용됩니다.

소스 IP 주소당 하나의 **shun** 명령만 적용 가능합니다.

shun 명령은 공격을 동적으로 차단하는 데 사용되기 때문에 Firepower Threat Defense 디바이스 구성에 표시되지 않습니다.

인터페이스 구성이 제거될 때마다 해당 인터페이스에 연결된 모든 shun도 제거됩니다.

다음 예에서 공격 호스트(10.1.1.27)가 TCP를 통해 대상(10.2.2.89)에 연결하는 것을 볼 수 있습니다. Firepower Threat Defense 디바이스 연결 테이블의 연결은 다음과 같이 읽을 수 있습니다.

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

다음 옵션을 사용하여 **shun** 명령을 적용합니다.

```
> shun 10.1.1.27 10.2.2.89 555 666 tcp
Shun 10.1.1.27 added in context: single_vf
Shun 10.1.1.27 successful
```

이 명령은 특정 현재 연결을 Firepower Threat Defense 연결 테이블에서 삭제하고, 향후 10.1.1.27의 모든 패킷이 Firepower Threat Defense 디바이스를 통해 이동하는 것을 방지합니다.

명령	설명
clear shun	현재 활성화된 모든 shun을 비활성화하고 shun 통계를 지웁니다.
show conn	모든 활성 연결을 표시합니다.
show shun	shun 정보를 표시합니다.

shutdown

디바이스를 종료하려면 **shutdown** 명령을 사용합니다.

shutdown

릴리스	수정 사항
6.0.1	이 명령이 도입되었습니다.

다음 예는 디바이스 종료 시 **shutdown** 명령의 샘플 출력입니다.

```
> shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': YES
```

명령	설명
reboot	디바이스를 재부팅합니다.

system access-control clear-rule-counts

액세스 제어 규칙의 적중 횟수를 0으로 재설정하려면 **system access-control clear-rule-counts** 명령을 사용합니다.

system access-control clear-rule-counts

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 **system access-control clear-rule-counts** 명령의 출력을 보여줍니다.

```
> system access-control clear-rule-counts
Are you sure that you want to clear the rule hit counters? (y/n): y
Clearing the rule hit counters.
Success.
```

명령	설명
show access-control-config	액세스 제어 정책 요약 및 적중 횟수를 보여줍니다.

system generate-troubleshoot

요청 받은 경우 Cisco Technical Support에서 제공하는 분석을 위해 문제 해결 데이터를 생성하려면 **system generate troubleshoot** 명령을 사용합니다.

system generate-troubleshoot *options*

options	표시를 생성하고 싶은 문제 해결 데이터의 유형. 하나 이상의 옵션을 입력할 수 있습니다. 여러 옵션을 구분하려면 공백을 사용합니다. • **ALL** — 다음 옵션 모두를 실행. • **SNT** — Snort 성능 및 컨피그레이션. • **PER** — 하드웨어 성능 및 로그. • **SYS** — 시스템 컨피그레이션, 정책 및 로그. • **DES** — 탐지 컨피그레이션, 정책 및 로그. • **NET** — 인터페이스 및 네트워크 관련 데이터. • **VDB** — 검색, 인식, VDB 데이터 및 로그. • **UPG** — 업그레이드 데이터 및 로그. • **DBO** — 모든 데이터베이스 데이터. • **LOG** — 모든 로그 데이터. • **NMP** — 네트워크 맵 정보.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예에서는 Snort 및 하드웨어 성능의 문제 해결 데이터를 생성하는 방법을 보여줍니다.

```
> system generate-troubleshoot SNT PER
Starting /usr/local/sf/bin/sf_troubleshoot.pl...
Please, be patient.  This may take several minutes.
the troubleshoot options codes specified are SNT,PER.
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/index]
getting filenames from [/ngfw/usr/local/sf/etc/db_updates/base-6.2.0]
```

```
Troubleshooting information successfully created at /ngfw/var/common/results-10-14-201
6--181112.tar.gz
```

명령	설명
copy	시스템에서 또는 시스템으로 파일을 복사합니다.
delete	시스템에서 파일을 삭제합니다.

system support 명령

대부분의 system support 명령은 Cisco Technical Assistance Center의 지원을 디버깅 및 문제 해결하는 데 사용됩니다. 일반적으로 사용되는 다음 명령을 제외하고 Cisco 지원의 지시에 따라 이 명령을 사용해야 합니다.

- system support diagnostic-cli, 859 페이지
- system support view-files, 861 페이지

system support diagnostic-cli

추가 show 및 기타 문제 해결 명령을 나타내는 진단 CLI를 시작하려면 **system support diagnostic-cli** 명령을 사용합니다.

system support diagnostic-cli

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

진단 CLI는 시스템의 문제를 해결하는 데 사용할 수 있는 다른 명령과 추가 show 명령을 포함합니다. 진단 CLI의 명령은 ASA 소프트웨어에서 가져온 것입니다. 일반 Firepower Threat Defense CLI는 동일한 명령을 다수 포함하므로 진단 CLI의 추가 명령이 필요하지 않을 수 있습니다.

진단 CLI를 시작할 때, 일반 Firepower Threat Defense CLI에서 별도의 세션에 있습니다.

프롬프트는 시스템 호스트 이름을 포함하도록 변경됩니다. 2가지 모드가 있으며, 이 프롬프트는 사용자의 현재 모드를 나타냅니다. User EXEC 모드의 경우, 프롬프트는 다음과 같습니다.

```
hostname>
```

Privileged EXEC 모드의 경우 Enable 모드로 알려져 있으며 프롬프트는 다음과 같습니다. Enable 명령을 사용하여 이 모드를 입력합니다. 비밀번호를 묻는 메시지가 표시되지만, Enter를 누르면 기본적으로 이 모드를 시작하는 데 비밀번호가 필요하지 않습니다.

```
hostname#
```

진단 CLI를 사용할 때 다음 정보를 기억하십시오.

- 진단 CLI를 종료하고 일반 CLI로 돌아가 Ctrl+a를 누른 다음 d를 누릅니다.
- Privileged EXEC 모드를 종료하려면 **exit** 명령을 사용합니다.

  각 모드에서 사용 가능한 명령은 다양합니다. Privileged EXEC 모드는 User EXEC 모드보다 훨씬 더 많은 명령을 포함합니다. 사용 가능한 명령을 보려면 **?**를 사용합니다. 다음의 ASA 소프트웨어 명령 참조에서 사용 정보를 찾을 수 있습니다.

  - Cisco ASA Series 명령 참조, A-H 명령 - http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/A-H/cmdref1.html)
  - Cisco ASA Series 명령 참조, I - R 명령 - http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/I-R/cmdref2.html

  - Cisco ASA Series 명령 참조, S 명령 - http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3.html
  - Cisco ASA Series 명령 참조, ASASM에 대한 T - Z 명령과 IOS 명령 - http://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/T-Z/cmdref4.html

- 진단 CLI는 Firepower Threat Defense에 대해 유효하지 않은 명령을 포함할 수 있습니다. 유효한 (또는 임의의) 정보를 제공하지 않는 명령을 시도할 경우, 관련된 기능은 Firepower Threat Defense에서 구성되거나 지원되지 않을 수 있습니다.
- 진단 CLI는 컨피그레이션 모드를 시작하도록 허용하지 않습니다. 디바이스를 구성하려면 CLI를 사용할 수 없습니다.
- 진단 CLI에서 분리할 경우, 이를 다음에 입력할 때 마지막으로 분리한 모드와 동일한 모드가 됩니다.
- ASA 5506W-X에서 무선 모듈에 대한 연결을 열려면 **session wlan** 명령을 사용할 수 있으며 액세스 포인트를 구성하려면 해당 CLI를 사용합니다. Privileged EXEC 모드에 있어야 합니다.

다음 예에서는 진단 CLI 및 Privileged EXEC 모드를 시작하는 방법을 보여줍니다. **enable** 명령을 입력한 후 비밀번호 프롬프트를 가져올 경우 Enter를 누릅니다. 기본적으로, Privileged EXEC 모드를 시작하는 비밀번호는 없습니다.

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> enable
Password: <press enter, do not enter a password>
firepower#
```

system support view-files

문제를 해결하기 위해 TAC(Cisco Technical Assistance Center) 작업 시 시스템 로그 내용을 보려면 **system support view-files** 명령을 사용합니다.

system support view-files

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

system support view-files 명령이 시스템 로그를 엽니다. Cisco TAC(Technical Assistance Center)와 작업할 때 이 명령을 사용하면 TAC에서 출력 해석을 지원할 수 있으며 확인해야 하는 적절한 로그를 선택할 수 있습니다.

이 명령을 실행하면 로그 선택을 위한 메뉴가 표시됩니다. 다음 명령을 사용하여 마법사를 탐색합니다.

- 보려는 파일을 선택하려면 프롬프트에서 **s**를 입력합니다. 그러면 파일 이름을 입력하라는 메시지가 표시됩니다. 대소문자를 구분하여 전체 이름을 입력해야 합니다. 파일 목록에는 로그의 크기가 표시됩니다. 매우 큰 로그의 경우 열기 전에 크기를 고려해야 합니다.
- --자세히--가 표시될 때 스페이스바를 누르면 다음 로그 항목 페이지가 표시되고 Enter 키를 누르면 다음 로그 항목만 표시됩니다. 로그의 끝에 도달하면 메인 메뉴로 이동됩니다. --자세히-- 줄에는 로그의 크기와 로그를 확인한 빈도가 표시됩니다. 전체 로그 페이지를 확인하지 않으려는 경우 **Ctrl+C**를 사용하여 로그를 닫고 명령을 종료합니다**.**
- 메뉴의 구조에서 한 레벨 위로 이동하려면 **b**를 입력합니다.

새로 추가되는 메시지를 확인할 수 있도록 로그를 열어 두려면 **tail-logs** 명령을 사용합니다.

다음 예에서는 ngfw.log 파일을 보는 방법을 보여줍니다. 파일 목록은 맨 위의 디렉토리에서 시작되며, 그 아래에는 현재 디렉토리의 파일 목록이 표시됩니다.

```
> system support view-files

===View Logs===

============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
```

```
setup
seshat
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>

2016-10-06 15:38:22.630001 | 9194       | ngfw.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> ngfw.log
2016-10-06 15:38:03 Starting Cisco Firepower Threat Defense ...
2016-10-06 15:38:03 Found USB flash drive /dev/sdb
2016-10-06 15:38:03 Found hard drive(s):  /dev/sda

<remaining log truncated>
```

명령	설명
tail-logs	로그를 열고 열린 상태로 유지합니다.

III 부

T - Z 명령

t - z

tail-logs

TAC(Cisco Technical Assistance Center)가 문제 해결 작업 시 작성한 메시지를 보기 위해 시스템 로그를 열려면 **tail-logs** 명령을 사용합니다.

tail-logs

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

tail-logs 명령은 쓰여질 시점의 메시지를 확인할 수 있는 시스템 로그를 엽니다. Cisco TAC(Technical Assistance Center)와 작업할 때 이 명령을 사용하면 TAC에서 출력 해석을 지원할 수 있으며 확인해야 하는 적절한 로그를 선택할 수 있습니다.

이 명령은 모든 사용 가능한 로그를 나열하는 메뉴를 표시합니다. 명령 프롬프트에 따라 로그를 선택합니다. 로그가 긴 경우, 추가 행을 살펴봅니다. 한 번에 한 줄씩 진행하려면 Enter를 누르고 한 번에 한 페이지씩 이동하려면 Space를 누릅니다. 로그 보기를 완료할 때 명령 프롬프트로 돌아가려면 Ctrl+C를 누릅니다.

다음 예에서는 ngfw.log 파일을 보는 방법을 보여줍니다. 파일 목록은 맨 위의 디렉터리에서 시작되며, 그 아래에는 현재 디렉터리의 파일 목록이 표시됩니다.

```
> tail-logs
===Tail Logs===
============================
Directory: /ngfw/var/log
----------sub-dirs----------
cisco
mojo
removed_packages
setup
seshat
connector
sf
scripts
packages
removed_scripts
httpd
-----------files------------
2016-10-14 18:12:04.514783 | 5371       | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353        | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517     | action_queue.log
2016-10-06 16:00:56.620019 | 1018       | br1.down.log

<list abbreviated>

2016-10-06 15:38:22.630001 | 9194       | ngfw.log
```

```
<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> ngfw.log
2016-10-06 15:38:22 Running [rm -rf /etc/logrotate-dmesg.conf /etc/logrotate.conf
/etc/logrotate.d
/etc/logrotate_ssp.conf /etc/logrotate_ssp.d] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate-size.conf /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate-size.d /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate.conf /etc/] ... success
2016-10-06 15:38:22 Running [ln -sf /ngfw/etc/logrotate.d /etc/] ... success
2016-10-06 15:38:22 Running [rm -f /usr/sbin/ntpd] ... success
```

명령	설명
system support view-files	로그 파일을 엽니다.

traceroute

데이터 인터페이스를 통해 패킷이 목적지에 도달하는 경로를 확인하려면 **traceroute** 명령을 사용합니다. 관리 IP 주소를 통과할 경우 패킷이 목적지에 도달하는 경로를 확인하려면 **traceroute system** 명령을 사용합니다.

traceroute *destination* [**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

traceroute system *destination*

destination	경로를 추적할 대상 호스트의 IPv4 또는 IPv6 주소 또는 호스트 이름입니다. 예를 들어, 10.100.10.10 또는 www.example.com입니다. 호스트 이름을 확인하려면 DNS 서버를 구성해야 합니다. 관리 주소에 대해 구성된 DNS 서버가 **traceroute system** 명령만으로 작동하기 때문에 데이터 인터페이스를 통과하는 호스트 이름을 추적하려면 먼저 **nslookup** 명령을 사용하여 호스트의 IP 주소를 확인한 다음 이 IP 주소를 대신 사용하십시오.
numeric	중간 게이트웨이의 IP 주소만 인쇄하도록 출력을 지정합니다. 이 키워드를 지정하지 않으면 traceroute에서 추적 중에 도달한 게이트웨이의 호스트 이름을 조회하려고 시도합니다.
port*port_value*	UDP(사용자 데이터그램 프로토콜) 프로브 메시지에서 사용하는 대상 포트입니다. 기본값은 33434입니다.
probe*probe_num*	각 TTL 수준에서 전송할 프로브 수입니다. 기본값은 3개입니다.
source {*source_ip* | *source_interface*}	추적 패킷의 소스로 사용될 IP 주소 또는 인터페이스를 지정합니다. 이 IP 주소는 데이터 인터페이스 중 하나의 IP 주소여야 합니다. 투명 모드에서는 이 IP 주소가 관리 IP 주소여야 합니다. 인터페이스 이름을 지정하면 인터페이스의 IP 주소가 사용됩니다.
system	traceroute가 데이터 인터페이스가 아니라 관리 인터페이스를 통과해야 함을 표시합니다.
timeout*timeout_value*	연결 시간이 초과되기 전에 응답을 대기할 기간(초)을 지정합니다. 기본값은 3초입니다.

ttl*min_ttl max_ttl*	프로브에서 사용할 TTL(Time To Live) 값의 범위를 지정합니다. • *min_ttl* - 첫 번째 프로브의 TTL 값입니다. 기본값은 1이지만 더 높은 값으로 설정하여 알려진 홉 표시를 무시할 수 있습니다. • *max-ttl* - 사용할 수 있는 최대 TTL 값입니다. 기본값은 30입니다. 이 명령은 traceroute 패킷이 대상에 도달하거나 값에 도달한 경우 종료됩니다.
use-icmp	UDP 프로브 패킷 대신 ICMP 프로브 패킷을 사용하도록 지정합니다.

릴리스	수정
6.1	이 명령이 추가되었습니다.

사용 가이드라인

traceroute 명령은 전송된 각 프로브의 결과를 인쇄합니다. 출력 화면의 각 줄은 TTL 값에 해당합니다(오름차순). 다음은 **traceroute** 명령에서 인쇄되는 출력 기호입니다.

출력 기호	설명
*	프로브에 대한 응답을 받지 못한 채 시간이 초과되었습니다.
nn msec	각 노드에서 지정된 수의 프로브가 왕복하는 데 걸린 시간(밀리초)입니다.
!N.	연결 불가한 ICMP 네트워크입니다.
!H	연결 불가한 ICMP 호스트입니다.
!P	ICMP 프로토콜에 연결할 수 없습니다.
!A	관리자가 ICMP를 금지했습니다.
?	알 수 없는 ICMP 오류입니다.

다음 예에서는 대상 IP 주소가 지정된 경우 traceroute의 출력 결과를 보여 줍니다.

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
```

```
 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

다음 예에서는 관리 인터페이스를 통과하는 traceroute를 호스트 이름에 대해 보여줍니다.

```
> traceroute system www.example.com
traceroute to www.example.com (72.163.4.161), 30 hops max, 60 byte packets
 1  192.168.0.254 (192.168.0.254)  0.213 ms  0.310 ms  0.328 ms
 2  10.88.127.1 (10.88.127.1)  0.677 ms  0.739 ms  0.899 ms
 3  lab-gw1.example.com (10.89.128.25)  0.638 ms  0.856 ms  0.864 ms
 4  04-bb-gw1.example.com (10.152.240.65)  1.169 ms  1.355 ms  1.409 ms
 5  wan-gw1.example.com (10.152.240.33)  0.712 ms  0.722 ms  0.790 ms
 6  wag-gw1.example.com (10.152.240.73)  13.868 ms  10.760 ms  11.187 ms
 7  rbb-gw2.example.com (172.30.4.85)  7.202 ms  7.301 ms  7.101 ms
 8  rbb-gw1.example.com (172.30.4.77)  8.162 ms  8.225 ms  8.373 ms
 9  sbb-gw1.example.com (172.16.16.210)  7.396 ms  7.548 ms  7.653 ms
10  corp-gw2.example.com (172.16.16.58)  7.413 ms  7.310 ms  7.431 ms
11  dmzbb-gw2.example.com (172.16.0.78)  7.835 ms  7.705 ms  7.702 ms
12  dmzdcc-gw2.example.com (172.16.0.190)  8.126 ms  8.193 ms  11.559 ms
13  dcz05n-gw1.example.com (172.16.2.106)  11.729 ms  11.728 ms  11.939 ms
14  www1.example.com (172.16.4.161)  11.645 ms  7.958 ms  7.936 ms
```

명령	설명
capture	추적 패킷을 포함한 패킷 정보를 캡처합니다.
show capture	옵션을 지정하지 않은 경우의 캡처 컨피그레이션을 표시합니다.
packet-tracer	패킷 추적 기능을 활성화합니다.

verify

파일의 체크섬을 확인하려면 **verify** 명령을 사용합니다.

verify [**sha-512** | **/signature**] *path*
verify/md5 *path* [*md5-value*]

/md5	(선택 사항) 지정된 소프트웨어 이미지의 MD5 값을 계산하고 표시합니다. 이 값을 Cisco.com에서 이 이미지에 사용할 수 있는 값과 비교합니다.
sha-512	(선택 사항) 지정된 소프트웨어 이미지의 SHA-512 값을 계산하고 표시합니다. 이 값을 Cisco.com에서 이 이미지에 사용할 수 있는 값과 비교합니다.
/signature	(선택 사항) 플래시에 저장된 이미지의 서명을 확인합니다.
md5-value	(선택 사항) 지정된 이미지에 대한 알려진 MD5 값입니다. MD5 값을 명령에 지정한 경우에는 시스템에서 지정된 이미지의 MD5 값을 계산하여 MD5 값이 일치하는지 또는 불일치가 있는지 확인하는 메시지를 표시합니다.

path

- *filename*

  현재 디렉토리에 있는 파일의 이름. 디렉토리 내용을 확인하려면 **dir**을 사용하고 디렉토리를 변경하려면 **cd**를 사용합니다.

- **disk0:**/[*path*/]*filename*

  이 옵션은 내부 플래시 메모리를 나타냅니다. 또한 **flash:**를 별칭이 지정된 **disk0** 대신 사용할 수도 있습니다.

- **disk1:**/[*path*/]*filename*

  이 옵션은 외부 플래시 메모리 카드를 나타냅니다.

- **flash:**/[*path*/]*filename*

  이 옵션은 내부 플래시 카드를 나타냅니다. ASA 5500 Series의 경우 **flash**는 **disk0:**의 별칭입니다.

- **ftp:**//[*user*[**:***password*]**@**]*server*[:*port*]/[*path*/]*filename*[**;type=***xx*]

  type은 다음 키워드 중 하나일 수 있습니다.

  - **ap** - ASCII 패시브 모드
  - **an** - ASCII 일반 모드
  - **ip** - (기본값) 이진 패시브 모드
  - **in** - 이진 일반 모드

- **http**[**s**]**:**//[*user*[:*password*] **@**]*server*[: *port*]/[*path*/]*filename*
- **tftp://**[*user*[:*password*]@]*server*[: *port*]/[*path*/]*filename*[**;int=***interface_name*]

  서버 주소의 경로를 재정의하려면 인터페이스 이름을 지정합니다. 경로 이름은 공백을 포함할 수 없습니다.

현재 플래시 디바이스가 기본 파일 시스템입니다.

참고 **/md5** 옵션을 지정한 경우 ftp, http, tftp 등의 네트워크 파일을 소스로 사용할 수 있습니다. **verify** 명령을 **/md5** 옵션 없이 사용하면 플래시의 로컬 이미지만 확인할 수 있습니다.

릴리스	수정 사항
6.1	이 명령이 추가되었습니다.

사용 가이드라인

verify 명령을 사용하여 파일을 사용하기 전에 해당 체크섬을 확인할 수 있습니다.

디스크에 분산되어 있는 각 소프트웨어 이미지는 전체 이미지에 단일 체크섬을 사용합니다. 이 체크섬은 이미지가 플래시 메모리에 복사된 경우에만 표시되며, 이미지 파일이 디스크 간에 복사된 경우에는 표시되지 않습니다.

이미지를 플래시 메모리 또는 서버에 복사할 때 체크섬을 확인하려면 새 이미지를 로드하거나 복제하기 전에 이미지의 체크섬 및 MD5 정보를 기록해야 합니다. 다양한 이미지 정보를 Cisco.com에서 사용할 수 있습니다.

플래시 메모리의 내용을 보려면 **show flash:** 명령을 사용합니다. 플래시 내용 목록에는 개별 파일의 체크섬이 포함되지 않습니다. 이미지를 플래시 메모리에 복사한 후 이미지 체크섬을 다시 계산하고 확인하려면 **verify** 명령을 사용합니다. 그러나 **verify** 명령은 파일 시스템 저장된 이후의 파일 무결성만 확인합니다. 손상된 이미지가 디바이스로 전송되어 탐지되지 않은 상태로 파일 시스템에 저장될 수 있습니다. 손상된 이미지가 디바이스로 전송된 경우 소프트웨어는 이미지가 손상되었음을 알려줄 수 없으므로 파일이 성공적으로 확인됩니다.

MD5(message-digest5) 해시 알고리즘을 사용하여 파일을 검증하려면 **verify** 명령을 **/md5** 옵션과 함께 사용합니다. MD5는 고유한 128비트 메시지 다이제스트를 생성하여 데이터 무결성을 확인하는 데 사용되는 알고리즘입니다(RFC 1321에 정의됨). **/md5** 옵션(**verify** 명령과 함께 사용)은 MD5 체크섬 값을 이미지에 대해 알려진 MD5 체크섬 값과 비교하여 보안 어플라이언스 소프트웨어 이미지의 무결성을 확인할 수 있도록 합니다. 이제 로컬 시스템 이미지 값과 비교할 수 있도록 모든 보안 어플라이언스 소프트웨어 이미지의 MD5 값을 Cisco.com에서 사용할 수 있습니다.

MD5 무결성 확인을 수행하려면 **verify** 명령(**/md5** 키워드를 사용)을 실행합니다. 예를 들어 **verify /md5 flash:cdisk.bin** 명령을 실행하면 소프트웨어 이미지의 MD5 값이 계산되고 표시됩니다. 이 값을 Cisco.com에서 이 이미지에 사용할 수 있는 값과 비교합니다.

또는 먼저 Cisco.com에서 MD5 값을 가져온 다음 명령 구문에서 이 값을 지정합니다. 예를 들어 **verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** 명령을 실행하면 MD5 값이 일치하는지 또는 불일치가 있는지 확인하는 메시지가 표시됩니다. MD5 값의 불일치는 이미지가 손상되었거나 잘못된 MD5 값이 입력되었음을 의미합니다.

다음 예에서는 이미지 파일을 확인합니다. 이는 **/signature** 키워드를 포함한 경우 확인할 수 있는 결과와 동일합니다.

```
> verify os.img
Verifying file integrity of disk0:/os.img
Computed Hash   SHA2: 4916c9b70ad368feb02a0597fbef798e
                      ca360037fc0bb596c78e7ef916c6c398
                      e238e2597eab213d5c48161df3e6f4a7
                      66e4ec15a7b327ee26963b2fd6e2b347
Embedded Hash   SHA2: 4916c9b70ad368feb02a0597fbef798e
                      ca360037fc0bb596c78e7ef916c6c398
                      e238e2597eab213d5c48161df3e6f4a7
                      66e4ec15a7b327ee26963b2fd6e2b347
Digital signature successfully validated
```

다음 예에서는 이미지에 대한 MD5 값을 계산합니다. 간략하게 하기 위해 대부분의 느낌표가 제거되었습니다.

```
> verify /md5 os.img
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!Done!
verify /MD5 (disk0:/os.img) = 0940c6c71d3d43b3ba495f7290f4f276
>
```

다음 예에서는 MD5 값을 계산하고 예상 값과 비교합니다. 이 경우 의사 결정이 확인(Verified)되며 계산 및 예상된 값이 일치합니다.

```
> verify /md5 os.img 0940c6c71d3d43b3ba495f7290f4f276
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Verified (disk0:/os.img) = 0940c6c71d3d43b3ba495f7290f4f276
>
```

다음 예에서는 이미지에 대한 SHA-512 값을 계산합니다.

```
> verify /sha-512 os.img
!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
verify /SHA-512 (disk0:/os.img) = 77421c0f6498976fbe5300e62bd8b7e8140b52a851f055265080
a392299848a77227d6047827192f34d969d36944abf2bddd215ec4127f9503173f82a2d6c7e2
```

명령	설명
copy	파일을 복사합니다.
dir	시스템의 파일을 나열합니다.

vpn-sessiondb logoff

모든 VPN 세션 또는 선택한 VPN 세션을 로그오프하려면 **vpn-sessiondb logoff** 명령을 사용합니다.

vpn-sessiondb logoff {**all** | **index** *index_number* | **ipaddress** *IPaddr* | **l2l** | **name** *username* | **protocol** *protocol-name* | **tunnel-group** *groupname* | **webvpn**} **noconfirm**

all	모든 VPN 세션을 로그오프합니다.
index*index_number*	인덱스 번호별로 단일 세션을 로그오프합니다. **show vpn-sessiondb detail** 명령을 사용하여 각 세션의 인덱스 번호를 확인할 수 있습니다.
ipaddress*IPaddr*	지정한 IP 주소에 대한 세션을 로그오프합니다.
l2l	모든 LAN-to-LAN 세션을 로그오프합니다.
name*username*	지정한 사용자 이름에 대한 세션을 로그오프합니다.
protocol*protocol-name*	지정한 프로토콜에 대한 세션을 로그오프합니다. 프로토콜은 다음과 같습니다. • **ikev1** — IKEv1(Internet Key Exchange version 1) 세션. • **ikev2** — IKEv2(Internet Key Exchange version 2) 세션. • **ipsec** — IKEv1 또는 IKEv2를 사용하는 IPsec 세션. • **ipseclan2lan** — IPsec LAN-to-LAN 세션. • **ipseclan2lanovernatt** — NAT-T를 통한 IPsec LAN-to-LAN 세션.
ra-ikev1-ipsec	모든 IPsec IKEv1 원격 액세스 세션을 로그오프합니다.
ra-ikev2-ipsec	모든 IPsec IKEv2 원격 액세스 세션을 로그오프합니다.
tunnel-group*groupname*	지정한 터널 그룹(연결 프로파일)에 대한 세션을 로그오프합니다.
webvpn	모든 클라이언트리스 SSL VPN 세션을 로그오프합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

다음 예는 기업 터널 그룹(연결 프로파일)의 세션에서 로그 오프하는 방법을 보여줍니다.

```
> vpn-sessiondb logoff tunnel-group Corporate noconfirm
INFO: Number of sessions from TunnelGroup "Corporate" logged off : 1
```

write net

실행 중인 구성을 TFTP 서버에 저장하려면 **write net** 명령을 사용합니다.

write net [**interface** *if_name*] *server***:**[*filename*]

:*filename*	경로 및 파일 이름을 지정합니다.
interface*if_name*	TFTP 서버에 도착하기 위해 통과할 인터페이스의 이름을 지정합니다.
*server***:**	TFTP 서버 IP 주소 또는 이름을 설정합니다.

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

실행 중인 컨피그레이션은 메모리에서 현재 실행 중인 구성입니다.

다음 예에서는 내부 인터페이스를 통해 TFTP 서버에 실행 중인 구성을 복사합니다.

```
> write net interface inside 10.1.1.1:/configs/contextbackup.cfg
```

명령	설명
show running-config	실행 중인 구성을 표시합니다.

write terminal

터미널에서 실행 중인 컨피그레이션을 표시하려면 **write terminal** 명령을 사용합니다.

write terminal

릴리스	수정 사항
6.1	이 명령이 도입되었습니다.

사용 가이드라인

이 명령은 **show running-config** 명령과 같습니다.

다음 예에서는 실행 중인 컨피그레이션을 터미널에 기록합니다.

```
> write terminal
: Saved
:
: Serial Number: XXXXXXXXXXX
: Hardware:   ASA5516, 8192 MB RAM, CPU Atom C2000 series 2416 MHz, 1 CPU (8 cores)
:
NGFW Version 6.2.0
!
hostname firepower
(...remaining output deleted...)
```