



ASDM 手册 2: 思科 ASA 系列防火墙 ASDM 配置指南, 7.10

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

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 报头压缩是加州大学伯克利分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。© 1981，加州大学董事会。

无论本手册中是否有任何其他保证，这些供应商的所有文档文件和软件均按“原样”提供，并可能包含缺陷。思科和上面所提及的提供商拒绝所有明示或暗示保证，包括（但不限于）适销性、特定用途适用性和无侵权保证，或者因买卖或使用以及商业惯例所引发的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏，思科及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

本文档中使用的任何互联网协议 (IP) 地址和电话号码并非实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

本文档的所有打印副本和复制的电子副本均视为非受控副本。有关最新版本，请参阅当前在线版本。

思科在全球设有 200 多个办事处。思科网站 www.cisco.com/go/offices 上列出了各办事处的地址和电话号码。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请访问此 URL：[www.cisco.com go trademarks](http://www.cisco.com/go/trademarks)。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1721R)

© 2019 Cisco Systems, Inc. 保留所有权利。



目录

序言：	关于本指南 xxi
	文档目标 xxi
	相关文档 xxi
	文档约定 xxi
	通信、服务和其他信息 xxiii

第 1 章	思科 ASA 防火墙服务简介 1
	如何实施防火墙服务 1
	基本访问控制 2
	应用程序过滤 2
	URL 过滤 2
	威胁防范 3
	面向虚拟环境的防火墙服务 4
	网络地址转换 4
	应用检测 5
	应用场景：面向公众显示服务器 5

第 1 部分：	访问控制 9
---------	----------------------

第 2 章	访问规则 11
	控制网络访问 11
	一般规则信息 12
	接口访问规则和全局访问规则 12
	入站和出站规则 12

规则顺序	13
隐式允许	13
隐式拒绝	14
NAT 和访问规则	14
扩展访问规则	14
用于返回流量的扩展访问规则	14
允许广播和组播流量	14
管理访问规则	15
EtherType 规则	15
支持的 EtherType 和其他流量	15
返回流量的 EtherType 规则	16
允许 MPLS	16
面向访问规则的许可	16
访问控制指南	16
配置访问控制	17
配置访问规则	17
访问规则属性	18
配置访问规则的高级选项	20
配置管理访问规则	22
配置 EtherType 规则	23
配置 ICMP 访问规则	24
监控访问规则	25
评估访问规则的系统日志消息	25
访问规则的历史	26

第 3 章

访问控制的对象	29
对象指南	29
配置对象	30
配置网络对象和组	30
配置网络对象	30
配置网络对象组	31

配置服务对象和服务组	31
配置服务对象	31
配置服务组	32
配置本地用户组	33
配置安全组对象组	34
配置时间范围	35
监控对象	36
对象的历史	36

第 4 章

访问控制列表	39
关于 ACL	39
ACL 类型	39
ACL 管理器	40
ACL 名称	41
访问控制条目顺序	41
允许/拒绝与匹配/不匹配	42
访问控制隐式拒绝	42
使用 NAT 时用于扩展 ACL 的 IP 地址	42
基于时间的 ACE	43
访问控制列表的许可	43
ACL 指南	43
配置 ACL	44
配置扩展 ACL	45
扩展 ACE 属性	45
扩展 ACE 中的服务规范	47
配置标准 ACL	48
配置 Webtype ACL	49
Webtype ACE 属性	50
Webtype ACL 的示例	51
监控 ACL	52
ACL 的历史	52

第 5 章

身份防火墙 55

- 关于身份防火墙 55
 - 身份防火墙部署的架构 56
 - 身份防火墙的功能 57
 - 部署方案 58
- 身份防火墙指南 61
- 身份防火墙的前提条件 63
- 配置身份防火墙 64
 - 配置 Active Directory 域 64
 - 配置 Active Directory 服务器组 65
 - 配置 Active Directory 代理 66
 - 配置 Active Directory 代理组 66
 - 配置身份选项 67
 - 配置基于身份的安全策略 69
- 监控身份防火墙 70
- 身份防火墙的历史 70

第 6 章

ASA 和思科 TrustSec 71

- 关于思科 TrustSec 71
 - 关于思科 TrustSec 中的 SGT 和 SXP 支持 72
 - 思科 TrustSec 功能中的角色 72
 - 安全组策略实施 73
 - ASA 如何实施基于安全组的策略 74
 - 更改 ISE 上安全组的效果 75
 - ASA 中的发言者和收听者 76
 - 将 ASA 注册到 ISE 77
 - 在 ISE 上创建安全组 77
 - 生成 PAC 文件 78
- 思科 TrustSec 指南 78
- 将 ASA 配置为与思科 Trustsec 集成 81

配置 AAA 服务器以便与思科 TrustSec 集成	81
导入 PAC 文件	82
配置安全交换协议	84
添加 SXP 连接对等体	85
刷新环境数据	86
配置安全策略	86
配置第 2 层安全组标记实施	87
使用场合	87
在接口上配置安全组标记	89
手动配置 IP-SGT 绑定	89
思科 TrustSec 的 AnyConnect VPN 支持	90
向远程访问 VPN 组策略和本地用户添加 SGT	90
监控 Cisco TrustSec	91
思科 TrustSec 的历史	92

第 7 章

ASA FirePOWER 模块 93

关于 ASA FirePOWER 模块	93
ASA FirePOWER 模块如何与 ASA 协同运行	93
ASA FirePOWER 内联模式	94
ASA FirePOWER 内联分路仪监控模式	95
ASA FirePOWER 被动仪监控流量转发模式	95
ASA FirePOWER 管理	96
与 ASA 功能的兼容性	96
如果 ASA FirePOWER 模块无法过滤 URL，应该怎么办	96
ASA FirePOWER 模块的许可要求	97
ASA FirePOWER 指南	97
ASA FirePOWER 默认设置	99
执行初始 ASA FirePOWER 设置	99
在网络中部署 ASA FirePOWER 模块	99
路由模式	99
透明模式	101

将 ASA FirePOWER 模块注册到管理中心	103
访问 ASA FirePOWER CLI	104
配置 ASA FirePOWER 基本设置	104
为 ASDM 管理配置 ASA FirePOWER 模块	106
配置 ASA FirePOWER 模块	108
在 ASA FirePOWER 模块上配置安全策略	108
将流量重定向到 ASA FirePOWER 模块	108
配置内联模式或内联分路仅监控模式	108
配置被动流量转发	109
启用强制网络门户以执行主动身份验证	110
管理 ASA FirePOWER 模块	111
安装或重新映像模块	111
安装或重新映像软件模块	111
重新映像 5585-X ASA FirePOWER 硬件模块	114
重置密码	116
重新加载或重置模块	117
关闭模块	117
卸载软件模块映像	118
从 ASA 向软件模块发起会话	119
升级系统软件	119
监控 ASA FirePOWER 模块	120
显示模块状态	120
显示模块统计信息	120
分析操作行为 (ASDM 管理)	120
监控模块连接	120
ASA FirePOWER 模块的历史	122
<hr/>	
第 8 章	思科 Umbrella 125
关于思科 Umbrella 连接器	125
思科 Umbrella 企业安全策略	125
思科 Umbrella 注册	126

思科 Umbrella 连接器的许可要求	126
思科 Umbrella 的使用指南和限制	126
配置思科 Umbrella 连接器	128
从思科 Umbrella 注册服务器安装 CA 证书	129
配置 Umbrella 连接器全局设置	130
在 DNS 检测策略映射中启用 Umbrella	131
验证 Umbrella 注册	131
监控 Umbrella 连接器	132
监控 Umbrella 服务策略统计信息	132
监控 Umbrella 系统日志消息	134
思科 Umbrella 连接器的历史记录	135

第 9 章

ASA 和思科 Cloud Web Security	137
思科 Cloud Web Security 相关信息	137
用户身份和云网络安全	137
身份验证密钥	138
ScanCenter 策略	138
目录组	138
自定义组	139
组和身份验证密钥如何互通	139
从主用代理服务器故障切换到备用代理服务器	140
思科 Cloud Web Security 的许可要求	140
云网络安全指南	141
配置思科 Cloud Web Security	142
配置与云网络安全代理服务器的通信	142
列入身份白名单的流量	143
配置向云网络安全发送流量的服务策略	145
配置用户身份监控功能	150
配置云网络安全策略	151
监控云网络安全	151
思科云网络安全示例	152

云网络安全的服务策略示例	152
思科云网络安全的历史	157

第 II 部分：	面向虚拟环境的防火墙服务	159
----------	--------------	-----

第 10 章	基于属性的访问控制	161
	基于属性的网络对象指南	161
	配置基于属性的访问控制	162
	配置 vCenter 虚拟机的属性	162
	配置虚拟机属性代理	164
	配置基于属性的网络对象	165
	使用基于属性的网络对象配置访问规则	166
	监控基于属性的网络对象	166
	基于属性的访问控制的历史	167

第 III 部分：	网络地址转换	169
-----------	--------	-----

第 11 章	网络地址转换 (NAT)	171
	为何使用 NAT?	171
	NAT 基础知识	172
	NAT 术语	172
	NAT 类型	172
	网络对象 NAT 和 两次 NAT	173
	网络对象 NAT	173
	两次 NAT	173
	比较 网络对象 NAT 和 两次 NAT	173
	NAT 规则排序	174
	NAT 接口	176
	NAT 指南	176
	NAT 防火墙模式指南	176
	IPv6 NAT 指导原则	177

IPv6 NAT 建议	177
其他 NAT 指南	177
映射地址对象的网络对象 NAT 指南	179
用于实际与映射地址对象的两次 NAT 准则	180
实际和映射端口服务对象的两次 NAT 指南	181
动态 NAT	182
关于动态 NAT	182
动态 NAT 不足和优势	183
配置动态网络对象 NAT	183
配置静态两次 NAT	185
动态 PAT	190
关于动态 PAT	190
动态 PAT 不足和优势	190
PAT 池对象指南	191
配置动态网络对象 PAT (隐藏)	192
使用 PAT 池配置动态网络对象 PAT	194
配置静态两次 PAT (隐藏)	196
使用 PAT 池配置动态两次 PAT	201
使用端口块分配配置 PAT	206
配置每会话 PAT 或多会话 PAT (版本 9.0(1) 及更高版本)	208
静态 NAT	209
关于静态 NAT	209
支持端口转换的静态 NAT	209
一对多静态 NAT	211
其他映射场景 (不推荐)	212
配置静态网络对象 NAT 或支持端口转换的静态 NAT	213
配置静态两次 NAT 或支持端口转换的静态 NAT	215
身份 NAT	220
配置身份网络对象 PAT	220
配置身份两次 NAT	222
监控 NAT	226

NAT 的历史 227

第 12 章

NAT 示例和参考 231

网络对象 NAT 示例 231

为内部 Web 服务器提供访问（静态 NAT） 231

面向内部主机的 NAT（动态 NAT）和面向外部 Web 服务器的 NAT（静态 NAT） 234

具有多个映射地址的内部负载均衡器（静态 NAT，一对多） 238

用于 FTP、HTTP 和 SMTP（支持端口转换的静态 NAT）的单一地址 240

两次 NAT 的示例 244

根据目标进行不同的转换（动态两次 PAT） 244

根据目标地址和端口进行不同的转换（动态 PAT） 250

示例：支持目标地址转换的两次 NAT 257

路由和透明防火墙模式下的 NAT 258

路由模式下的 NAT 258

透明模式下或桥接组内的 NAT 259

路由 NAT 数据包 260

映射地址和路由 261

地址与映射接口在相同的网络中 261

唯一网络中的地址 261

与实际地址相同的地址（身份 NAT） 261

远程网络的透明模式路由要求 263

确定出口接口 263

用于 VPN 的 NAT 263

NAT 和远程访问 VPN 264

NAT 和站点到站点 VPN 265

NAT 和 VPN 管理访问 268

NAT 和 VPN 故障排除 269

转换 IPv6 网络 269

NAT64/46：将 IPv6 地址转换为 IPv4 地址 270

NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网 270

NAT66：将 IPv6 地址转换为不同的 IPv6 地址 273

	NAT66 示例：网络间的静态转换	274
	NAT66 示例：简单 IPv6 接口 PAT	275
	使用 NAT 重写 DNS 查询和响应	277
	DNS 应答修改，外部接口上的 DNS 服务器	278
	独立网络上的 DNS 应答修改、DNS 服务器、主机和服务	280
	DNS 应答修改，主机网络上的 DNS 服务器	281
	DNS64 应答修改	283
	PTR 修改，主机网络上的 DNS 服务器	289
<hr/>		
第 IV 部分：	服务策略和应用检测	291
<hr/>		
第 13 章	服务策略	293
	关于服务策略	293
	服务策略的组件	293
	使用服务策略配置的功能	295
	功能方向性	296
	服务策略中的功能匹配	297
	多种功能操作的应用顺序	297
	某些功能操作的不兼容性	298
	多个服务策略的功能匹配	299
	服务策略指南	299
	服务策略默认设置	300
	默认服务策略配置	300
	默认类映射（流量类）	301
	配置服务策略	302
	为直通流量添加服务策略规则	302
	为管理流量添加服务策略规则	305
	管理服务策略规则的顺序	307
	服务策略的历史	308
<hr/>		
第 14 章	应用层协议检测入门	309

应用层协议检测	309
何时使用应用协议检测	309
检测策略映射	310
更换正在使用的检测策略映射	310
如何处理多个流量类	310
应用检测指南	311
应用检测的默认设置	312
默认检测和 NAT 限制	312
默认检测策略映射	316
配置应用层协议检测	316
配置正则表达式	320
创建正则表达式	320
创建正则表达式类映射	324
监控检测策略	324
应用检测的历史	325

第 15 章

基本互联网协议检测	327
DCERPC 检测	328
DCERPC 概述	328
配置 DCERPC 检测策略映射	328
DNS 检测	330
DNS 检测默认设置	330
配置 DNS 检测策略映射	330
FTP 检测	333
FTP 检测概述	333
严格 FTP	334
配置 FTP 检测策略映射	335
HTTP 检测	337
HTTP 检测概述	338
配置 HTTP 检测策略映射	338
ICMP 检测	341

ICMP 错误检测	341
ILS 检测	342
即时消息检测	342
IP 选项检测	344
IP 选项检测默认设置	345
配置 IP 选项检测策略映射	345
IPsec 穿透检测	346
IPsec 穿透检测概述	346
配置 IPsec 穿透检测策略映射	346
IPv6 检测	347
IPv6 检测默认设置	347
配置 IPv6 检测策略映射	348
NetBIOS 检测	349
PPTP 检测	349
RSH 检测	350
SMTP 和扩展 SMTP 检测	350
SMTP 和 ESMTP 检测概述	350
ESMTP 检测默认设置	351
配置 ESMTP 检测策略映射	352
SNMP 检测	354
SQL*Net 检测	354
Sun RPC 检测	355
Sun RPC 检测概述	355
管理 Sun RPC 服务	355
TFTP 检测	356
XDMCP 检测	356
VXLAN 检测	357
基本互联网协议检测的历史	357

语音和视频协议检测	359
CTIQBE 检测	359

CTIQBE 检测的局限性	359
H.323 检测	360
H.323 检测概述	360
H.323 工作原理	360
H.245 消息中的 H.239 支持	361
H.323 检测的局限性	361
配置 H.323 检测策略映射	362
MGCP 检测	364
MGCP 检测概述	364
配置 MGCP 检测策略映射	365
RTSP 检测	366
RTSP 检测概述	366
RealPlayer 配置要求	367
RSTP 检测的局限性	367
配置 RTSP 检测策略映射	367
SIP 检测	369
SIP 检测概述	369
SIP 检查的限制	370
默认 SIP 检测	370
配置 SIP 检测策略映射	371
瘦客户端控制协议 (SCCP) 检测	373
SCCP 检测概述	373
支持思科 IP 电话	374
SCCP 检测的局限性	374
默认 SCCP 检测	374
配置瘦小客户端 (SCCP) 检测策略映射	375
STUN 检测	376
语音和视频协议检测的历史	376

GTP 检测概述	379
GTP 检测的局限性	380
流控制传输协议 (SCTP) 检测和访问控制	380
SCTP 状态检测	381
SCTP 访问控制	381
SCTP NAT	381
SCTP 应用层检测	382
SCTP 的局限性	382
Diameter 检测	383
M3UA 检测	383
M3UA 协议符合性	384
M3UA 检测的局限性	384
RADIUS 计费检测概述	385
移动网络协议检测的许可	385
GTP 检测默认设置	386
配置移动网络检测	386
配置 GTP 检测策略映射	387
配置 SCTP 检测策略映射	390
配置 Diameter 检测策略映射	391
创建自定义 Diameter 属性-值对 (AVP)	394
检查加密的 Diameter 会话	395
配置服务器与 Diameter 客户端的信任关系	396
使用静态客户端证书为 Diameter 检测配置完整 TLS 代理	397
为 Diameter 检测配置支持本地动态证书的完全 TLS 代理	398
为 Diameter 检测配置支持 TLS 分流的 TLS 代理	400
配置 M3UA 检测策略映射	401
配置移动网络检测服务策略	404
配置 RADIUS 计费检测	405
配置 RADIUS 计费检测策略映射	405
配置 RADIUS 计费检测服务策略	406
监控移动网络检测	407

监控 GTP 检测	407
监控 SCTP	408
监控 Diameter	409
监控 M3UA	410
移动网络检测的历史	411

第 V 部分：**连接管理和威胁检测 413**

第 18 章 **连接设置 415**

什么是连接设置？	415
配置连接设置	416
配置全局超时	416
保护服务器不受 SYN 洪流 DoS 攻击（TCP 拦截）	419
自定义异常 TCP 数据包处理（TCP 映射、TCP 规范器）	420
绕过面向异步路由的 TCP 状态检查（TCP 状态绕行）	423
异步路由问题	423
有关 TCP 状态绕行的准则和限制	424
配置 TCP 状态绕行	424
禁用 TCP 序列随机化	425
分流大型数据流	426
数据流分流限制	426
配置数据流分流	427
配置特定流量类的连接设置（所有服务）	429
监控连接	431
连接设置的历史	432

第 19 章 **服务质量 435**

关于 QoS	435
支持的 QoS 功能	435
什么是令牌桶？	436
策略管制	436

优先级队列	436
如何交互使用 QoS 功能	436
DSCP (DiffServ) 保留	437
QoS 指南	437
配置 QoS	438
确定优先级队列的队列和传输环路限制	438
队列限制工作表	438
传输环路限制工作表	439
为接口配置优先级队列	439
为优先级排队和策略管制配置服务规则	440
监控 QoS	442
QoS 策略统计信息	442
QoS 优先级统计信息	442
QoS 优先级队列统计信息	443
QoS 的历史	443

第 20 章

威胁检测	445
检测威胁	445
基本威胁检测统计信息	446
高级威胁检测统计信息	446
扫描威胁检测	446
威胁检测指南	447
威胁检测的默认设置	447
配置威胁检测	448
配置基本威胁检测统计信息	449
配置高级威胁检测统计信息	449
配置扫描威胁检测	450
监控威胁检测	451
监控基本威胁检测统计信息	451
监控高级威胁检测统计信息	451
威胁检测的历史	452



关于本指南

以下主题介绍如何使用本指南。

- 文档目标，第 **xxi** 页
- 相关文档，第 **xxi** 页
- 文档约定，第 **xxi** 页
- 通信、服务和其他信息，第 **xxiii** 页

文档目标

本指南旨在帮助您使用自适应安全设备管理器 (ASDM) 来配置思科 ASA 系列的防火墙功能。本指南仅介绍最常见的一些配置场景，并未涵盖所有功能。

在本指南中，除非有专门指定，否则术语“ASA”一般适用于受支持的模型。



注释

ASDM 支持许多 ASA 版本。ASDM 文档和在线帮助包括 ASA 支持的所有最新功能。如果您运行的是旧版 ASA 软件，本文档可能包含您的版本中不支持的功能。请参阅每章的功能历史记录表以确定功能的添加时间。有关每个 ASA 版本所支持的 ASDM 最低版本，请参阅[思科 ASA 系列兼容性](#)。

相关文档

有关详细信息，请参阅思科 ASA 系列文档一览，网址：<http://www.cisco.com/go/asadocs>。

文档约定

本文档遵循以下文本、显示和警报约定。

文本约定

约定	指示
黑体字	命令、关键字、按钮标签、字段名称及用户输入的文本以黑体字字体显示。对于基于菜单的命令，显示指向该命令的完整路径。
斜体	为其赋值的变量以斜体字体显示。 斜体字体还用于文档标题和一般强调。
等宽字体	系统显示的终端会话和信息以等宽字体格式显示。
{x y z}	必需的备选关键字集中在大括号内，以竖线分隔。
[]	方括号中的元素是可选项。
[x y z]	可选的备选关键字集中在方括号内，以竖线分隔。
[]	对于系统提示符的默认响应也位于方括号内。
<>	非打印字符（例如密码）位于尖括号内。
!, #	一行代码开头带有叹号 (!) 或星号 (#) 表示这是注释行。

读者提示

本文档采用以下格式的读者提示：



注释 表示读者需要注意的地方。“注”中包含有用的建议或本文档未涵盖材料的引用信息。



提示 表示以下信息可帮助您解决问题。



注意 表示读者应当小心处理。在这种情况下，您的操作可能会导致设备损坏或数据丢失。



便捷程序 表示所述操作可以节省时间。按照该段落中的说明执行操作，有助于节省时间。



警告 表示读者需要注意。在这种情况下，操作可能会造成人身伤害。

通信、服务和其他信息

- 要及时从思科收到相关信息，请注册[思科配置文件管理器](#)。
- 要使用重要技术实现您期望实现的业务影响，请访问[思科服务](#)。
- 要提交服务请求，请访问[思科支持](#)。
- 要了解并浏览安全且经过验证的企业级应用、产品、解决方案和服务，请访问[思科Marketplace](#)。
- 要获取一般网络、培训和认证主题相关的信息，请访问[思科出版社](#)。
- 要查找有关特定产品或产品系列的保修信息，请访问[思科保修服务查找工具](#)。

思科漏洞搜索工具

[思科漏洞搜索工具 \(BST\)](#) 是一款基于 Web 的工具，用作思科漏洞跟踪系统的网关，该系统包含一个关于思科产品和软件的缺陷和漏洞的综合列表。BST 提供关于您的产品和软件的详细漏洞信息。



第 1 章

思科 ASA 防火墙服务简介

防火墙服务是指专注于控制网络访问的 ASA 功能，包括阻止流量的服务和在内外部网络之间启用流量数据流的服务。这些服务包括保护网络免受威胁（例如拒绝服务 [DoS] 及其他攻击）的服务。

以下主题概括介绍防火墙服务。

- [如何实施防火墙服务，第 1 页](#)
- [基本访问控制，第 2 页](#)
- [应用程序过滤，第 2 页](#)
- [URL 过滤，第 2 页](#)
- [威胁防范，第 3 页](#)
- [面向虚拟环境的防火墙服务，第 4 页](#)
- [网络地址转换，第 4 页](#)
- [应用检测，第 5 页](#)
- [应用场景：面向公众显示服务器，第 5 页](#)

如何实施防火墙服务

以下操作步骤介绍实施防火墙服务的通用顺序。但每个步骤都是可选步骤，只有在您要为网络提供该服务时才需要使用。

开始之前

根据一般操作配置指南配置 ASA，包括最低基本设置、接口配置、路由和管理访问。

过程

- 步骤 1** 实施网络访问控制。请参阅[基本访问控制，第 2 页](#)。
- 步骤 2** 实施应用过滤。请参阅[应用程序过滤，第 2 页](#)。
- 步骤 3** 实施 URL 过滤。请参阅[URL 过滤，第 2 页](#)。
- 步骤 4** 实施威胁防范。请参阅[威胁防范，第 3 页](#)。
- 步骤 5** 实施为虚拟环境定制的防火墙服务。请参阅[面向虚拟环境的防火墙服务，第 4 页](#)。

步骤 6 实施网络地址转换 (NAT)。请参阅[网络地址转换](#)，第 4 页。

步骤 7 实施应用检测（如果默认设置不能满足网络要求）。请参阅[应用检测](#)，第 5 页。

基本访问控制

访问规则是第一道防线，按接口或全局进行应用。可以在特定类型的流量进入后丢弃该流量，或者丢弃流出（或流入）特定主机或网络的流量。默认情况下，ASA 允许流量从内部网络（较高安全性级别）自由流向外部网络（较低安全性级别）。

可以应用访问规则，以限制从内部到外部的流量，或者允许从外部到内部的流量。

基本访问规则使用“5 元组”的源地址和端口、目标地址和端口以及协议控制流量。请参阅[访问规则](#)，第 11 页和[访问控制列表](#)，第 39 页。

可以通过对规则进行身份感知来扩充规则。这样便可以根据用户身份或组成员身份配置规则。要实施身份控制，请执行以下操作的任意组合：

- 在一台单独的服务器上安装 Cisco Context Directory Agent (CDA)，也称为 AD 代理，用于收集 Active Directory (AD) 服务器中已定义的用户和组信息。然后，配置 ASA 来获取这些信息并向访问规则中添加用户或组条件。请参阅[身份防火墙](#)，第 55 页。
- 在一台单独的服务器上安装思科身份服务引擎 (ISE)，用于实施 Cisco Trustsec。然后，可以向访问规则添加安全组条件。请参阅[ASA 和思科 TrustSec](#)，第 71 页。
- 在 ASA 上安装 ASA FirePOWER 模块，并实施该模块中的身份策略。ASA FirePOWER 中的身份感知型访问策略会应用于重定向到该模块的任何流量。请参阅[ASA FirePOWER 模块](#)，第 93 页。

应用程序过滤

随着基于 Web 的应用的广泛使用，大量流量通过 HTTP 或 HTTPS 协议进行传输。使用传统的 5 元组访问规则，可以允许或禁止所有 HTTP/HTTPS 流量。这可能需要对网络流量进行更精细的控制。

可以在 ASA 上安装模块，以提供应用过滤，从而根据所使用的应用选择性地允许 HTTP 或其他流量，因此无需对 HTTP 执行一揽子允许操作。可以查看流量的内部情况，阻止网络不接受的应用（例如，不适当的文件共享）。当为应用过滤添加模块时，请勿在 ASA 上配置 HTTP 检测。

要实施应用过滤，请在 ASA 上安装 ASA FirePOWER 模块，并使用 ASA FirePOWER 访问规则中的应用过滤条件。这些策略将应用于重定向到该模块的所有流量。请参阅[ASA FirePOWER 模块](#)，第 93 页。

URL 过滤

URL 过滤根据目标站点的 URL 拒绝或允许流量。

URL 过滤的目的主要是完全阻止或允许对某个网站的访问。虽然可以将单个页面作为目标，但通常是指定主机名（例如 `www.example.com`）或 URL 类别，从而定义提供特定类型服务（如赌博）的主机名列表。

当尝试决定是为 HTTP/HTTPS 流量使用 URL 过滤还是应用过滤时，请考虑是否要创建应用于定向至某个网站的所有流量的策略。如果打算以相同的方式处理所有此类流量（拒绝或允许），请使用 URL 过滤。如果打算选择性地阻止或允许流向网站的流量，请使用应用过滤。

要实施 URL 过滤，请执行以下操作之一：

- 在 ASA 上安装 ASA FirePOWER 模块，并在 ASA FirePOWER 访问规则中使用应用过滤条件。这些策略将应用于重定向到该模块的所有流量。请参阅 [ASA FirePOWER 模块，第 93 页](#)。
- 订用思科 Umbrella 服务，您将在其中配置企业安全策略基于完全限定域名 (FQDN) 来阻止恶意站点。对于被视为可疑的 FQDN，您可以将用户连接重定向至执行 URL 过滤的思科 Umbrella 智能代理。Umbrella 服务通过处理用户的 DNS 查询请求，返回阻止页面的 IP 地址或智能代理的 IP 地址发挥作用。该服务将为列入白名单的域返回 FQDN 的真实 IP 地址。请参阅 [思科 Umbrella，第 125 页](#)。
- 订用云网络安全服务，其中在 ScanCenter 中配置过滤策略，然后将 ASA 配置为向您的云网络安全账户发送流量。请参阅 [ASA 和思科 Cloud Web Security，第 137 页](#)

威胁防范

可以执行许多措施，来防御扫描、拒绝服务 (DoS) 及其他攻击。许多 ASA 功能可通过应用连接限制和丢弃异常 TCP 数据包来帮助防御攻击。某些功能是自动功能，某些功能可配置，但在大多数情况下适用的默认设置，而其他功能则完全可选，如果要使用这些可选功能，必须进行配置。

下面是 ASA 中可用的威胁防范服务。

- IP 数据包分段保护 - ASA 完全重组所有 ICMP 错误消息，并虚拟重组通过 ASA 路由的剩余 IP 网段，丢弃未通过安全检查和网段。无需进行配置。
- 连接限制、TCP 规范化及其他连接相关的功能 - 配置连接相关的服务，例如 TCP 和 UDP 连接限制与超时、TCP 序列号随机化、TCP 规范化以及 TCP 状态绕行。TCP 规范化旨在丢弃出现异常的数据包。请参阅 [连接设置，第 415 页](#)。

例如，可以限制 TCP 和 UDP 连接及初期连接（源与目标之间尚未完成必要握手的连接请求）。限制连接和半开连接的数量可防止遭受 DoS 攻击。ASA 通过限制初期连接的数量来触发 TCP 拦截，从而防止内部系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。

- 威胁检测 - 在 ASA 上实施威胁检测，以便收集统计信息来帮助识别攻击。默认情况下启用基本威胁检测，但您可以实施高级统计和扫描威胁检测功能。可以避开标识为扫描威胁的主机。请参阅 [威胁检测，第 445 页](#)。
- 下一代 IPS - 在 ASA 上安装 ASA FirePOWER 模块并在 ASA FirePOWER 中实施下一代 IPS 入侵规则。这些策略会应用于重定向到 ASA FirePOWER 的任何流量。请参阅 [ASA FirePOWER 模块，第 93 页](#)。

面向虚拟环境的防火墙服务

虚拟环境将服务器部署为虚拟机，例如在 VMware ESXi 中。虚拟环境中的防火墙可以是传统硬件设备，也可以是虚拟机防火墙，例如 ASA v。

传统和下一代防火墙服务应用于虚拟环境的方式与其应用于不使用虚拟机服务器的环境的方式相同。不过，因为在虚拟环境下易于创建和断开服务器，虚拟环境可提供更多挑战。

此外，数据中心内服务器之间的流量可能同数据中心与外部用户之间的流量需要相同程度的保护。例如，如果攻击者控制了数据中心内的某台服务器，则可能会对该数据中心的其他服务器发起攻击。

虚拟环境的防火墙服务添加了专门面向虚拟机应用防火墙保护的功能。下面是可用于虚拟环境的防火墙服务：

- 基于属性的访问控制 - 您可以将网络对象配置为基于属性匹配流量，并在访问控制规则中使用这些对象。这样便可以从网络拓扑中将防火墙规则分离出来。例如，您可以允许具有 Engineering 属性的所有主机访问具有 Lab Server 属性的主机。然后，可以添加/删除具有这些属性的主机并自动应用防火墙策略，而无需更新访问规则。有关详细信息，请参阅[基于属性的访问控制](#)，第 161 页。

网络地址转换

网络地址转换 (NAT) 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法可路由地址。通过这种方式，NAT 即可保存公用地址，因为您至少可以为整个网络向外部网络通告一个公用地址。

NAT 的其他功能包括：

- 安全 - 隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案 - 使用 NAT 时不会出现重叠 IP 地址。
- 灵活性 - 可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。
- 在 IPv4 和 IPv6 之间转换（仅路由模式） - 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。

不需要 NAT。如果不为一组给定流量配置 NAT，将不转换这些流量，但会正常应用所有安全策略。

请参阅：

- [网络地址转换 \(NAT\)](#)，第 171 页
- [NAT 示例和参考](#)，第 231 页

应用检测

对于在用户数据包中嵌入 IP 寻址信息的服务或在动态分配端口上打开辅助信道的服务，需要使用应用检测引擎。这些协议需要 ASA 执行深度数据包检测，以便打开所需的针孔及应用网络地址转换 (NAT)。

默认 ASA 策略已对许多常见协议（例如 DNS、FTP、SIP、ESMTP、TFTP 等）全局应用检测。默认检测可能满足您对网络的所有需求。

但是，您可能需要启用其他协议的检测，或者优化检测。许多检测都包含详细的选项，您可以根据这些选项的内容来控制数据包。如果非常熟悉某个协议，可以对该流量应用精细控制。

使用服务策略配置应用检测。可以配置全局服务策略，还可以向每个接口应用服务策略，或者同时使用这两种方式。

请参阅：

- [服务策略，第 293 页](#)
- [应用层协议检测入门，第 309 页](#)
- [基本互联网协议检测，第 327 页](#)
- [语音和视频协议检测，第 359 页](#)
- [移动网络检测，第 379 页。](#)

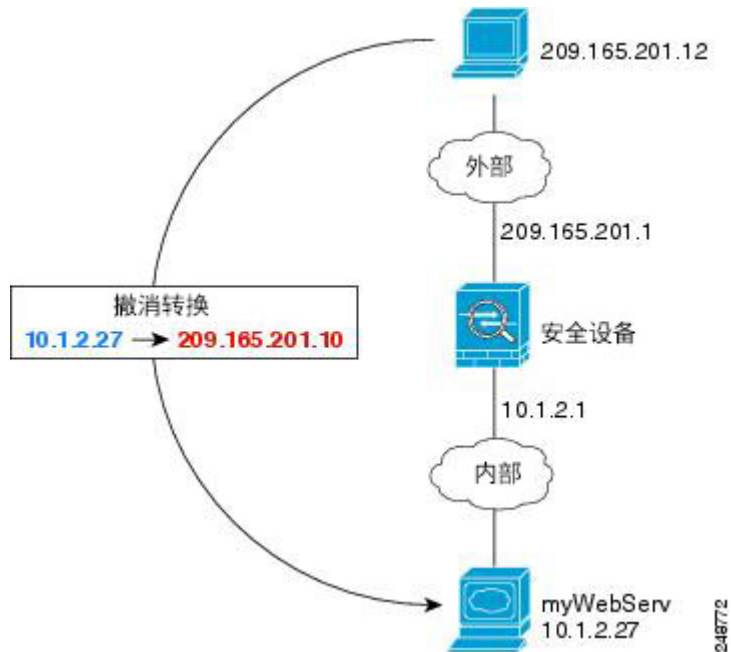
应用场景：面向公众显示服务器

可以在公共网络上显示服务器上的某些应用服务。例如，可以开放 Web 服务器，以便用户可以连接到网页，但不与服务器建立任何其他连接。

要在公共网络上开放服务器，通常需要创建允许连接和 NAT 规则的访问规则，以在服务器的内部 IP 地址与公共网络可以使用的外部地址之间转换。此外，如果不希望外部开放的服务使用与内部服务器相同的端口，可以使用端口地址转换 (PAT) 将内部端口映射到外部端口。例如，如果内部 Web 服务器不在 TCP/80 上运行，可以将其映射到 TCP/80，以方便外部用户进行连接。

以下示例实现了内部专用网络上某台 Web 服务器的公共访问。

图 1: 面向内部 Web 服务器的静态 NAT



ASDM 包括配置所需访问和 NAT 规则的快捷方式，简化了在公共网络上显示内部服务器上的服务的过程。

过程

步骤 1 依次选择配置 > 防火墙 > 公共服务器。

步骤 2 点击 Add。

步骤 3 定义要开放服务的专用特性和公共特性。

- **Private Interface** - 与实际服务器连接的接口。在本示例中为 “inside”。
- **Private IP Address** - 定义服务器的实际 IPv4 地址的主机网络对象。无法指定 IPv6 地址。如果没有包含地址的对象，请点击 “...” 按钮，然后点击 **Add**，以此创建一个对象。在本示例中，对象名称是 MyWebServ，将包含 10.1.2.27 主机地址。
- **Private Service** - 在实际服务器上运行的实际服务。可以使用预定义的服务或服务对象。还可以使用服务对象组，除非您还指定了映射专用服务的公共服务。

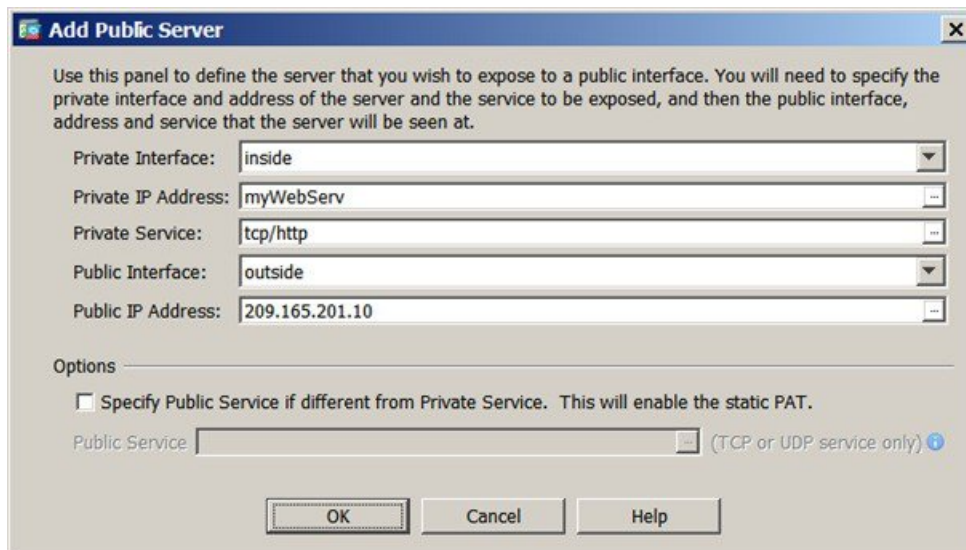
可以开放各种服务；但是，如果指定了公共服务，所有端口均映射到相同的公共端口。

在本示例中，端口是 **tcp/http**。

- **Public Interface** - 外部用户访问实际服务器所通过的接口。在本示例中为 “outside”。
- **Public Address** - 外部用户所看到的 IPv4 地址。可以直接指定地址，也可以使用主机网络对象。在本示例中，外部地址是 209.165.201.10。

- **Specify Public Service if different from private service, Public Service** - 在转换地址上运行的服务。只有当公共服务与专用服务不同时，才指定公共服务。例如，如果专用 Web 服务器在 TCP/80 上运行，要为外部用户使用同一端口，则不需要指定公共服务。如果指定公共服务，必须使用预定义的 TCP 或 UDP 服务。本示例不使用端口转换，因此不选择此选项。

下面显示对话框的外观。



Use this panel to define the server that you wish to expose to a public interface. You will need to specify the private interface and address of the server and the service to be exposed, and then the public interface, address and service that the server will be seen at.

Private Interface: inside

Private IP Address: myWebServ

Private Service: tcp/http

Public Interface: outside

Public IP Address: 209.165.201.10

Options

Specify Public Service if different from Private Service. This will enable the static PAT.

Public Service (TCP or UDP service only)

OK Cancel Help

步骤 4 点击 **OK**，然后点击 **Apply**。

■ 应用场景：面向公众显示服务器



第 I 部分

访问控制

- [访问规则](#)，第 11 页
- [访问控制的对象](#)，第 29 页
- [访问控制列表](#)，第 39 页
- [身份防火墙](#)，第 55 页
- [ASA 和思科 TrustSec](#)，第 71 页
- [ASA FirePOWER 模块](#)，第 93 页
- [思科 Umbrella](#)，第 125 页
- [ASA 和思科 Cloud Web Security](#)，第 137 页



第 2 章

访问规则

本章介绍如何使用访问规则控制通过或流向 ASA 的网络访问。在路由和透明防火墙模式下均可使用访问规则控制网络访问。在透明模式下，可同时使用访问规则（适用于第 3 层流量）和 EtherType 规则（适用于第 2 层流量）。



注释

要访问 ASA 接口进行访问管理，亦无需允许主机 IP 地址的访问规则。只需根据一般操作配置指南配置管理访问即可。

- [控制网络访问，第 11 页](#)
- [面向访问规则的许可，第 16 页](#)
- [访问控制指南，第 16 页](#)
- [配置访问控制，第 17 页](#)
- [监控访问规则，第 25 页](#)
- [访问规则的历史，第 26 页](#)

控制网络访问

访问规则决定允许哪些流量通过 ASA。有多个不同的规则层，这些规则层共同实施访问控制策略：

- 分配至接口的扩展访问规则（第 3+ 层流量） - 可于入站和出站方向应用单独的规则集 (ACL)。扩展访问规则根据源和目标流量条件允许或拒绝流量。
- 分配至桥接虚拟接口（BVI、路由模式）的扩展访问规则（第 3+ 层流量） - 如果命名了 BVI，可以在入站和出站方向应用单独的规则集，也可以向桥接组成员接口应用规则集。当 BVI 和成员接口都有访问规则时，处理顺序取决于方向。入站时，首先评估成员访问规则，然后是 BVI 访问规则。出站时，首先考虑 BVI 规则，然后是成员接口规则。
- 全局分配的扩展访问规则 - 可创建用作默认访问控制的单个全局规则集。全局规则在接口规则之后应用。
- 管理访问规则（第 3+ 层流量） - 可应用单个规则集以覆盖接口处定向的流量，这通常是管理流量。在 CLI 中，这些是“控制平面”访问组。对于在设备处定向的 ICMP 流量，也可配置 ICMP 规则。

- 分配至接口（仅限桥接组成员接口）的 EtherType 规则（第 2 层流量）- 可以在入站和出站方向应用单独的规则集。EtherType 规则控制针对非 IP 流量的网络访问。EtherType 规则根据 EtherType 允许或拒绝流量。此外，还可以对桥接组成员接口应用扩展访问规则来控制第 3+ 层流量。

一般规则信息

以下主题提供有关访问规则和 EtherType 规则的一般信息。

接口访问规则和全局访问规则

可将访问规则应用于特定接口，也可将访问规则全局应用于所有接口。可结合接口访问规则配置全局访问规则，在此情况下，特定入站接口访问规则始终在通用全局访问规则之前得以处理。全局访问规则仅适用于入站流量。

入站和出站规则

可根据流量的方向配置访问规则：

- 入站 - 入站访问规则在流量进入接口时应用于流量。全局访问规则和管理访问规则始终为入站规则。
- 出站 - 出站规则在流量离开接口时应用于流量。

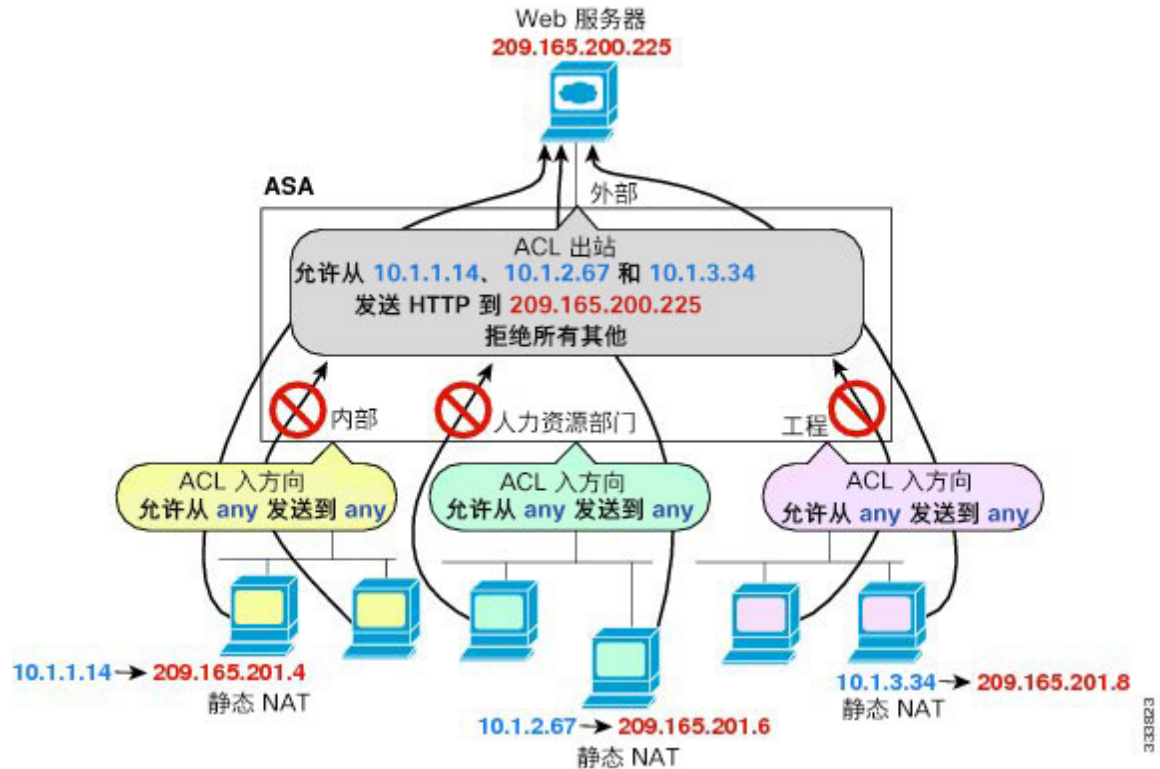


注释

“入站”和“出站”指在接口上对通过接口进入 ASA 或离开 ASA 的流量应用 ACL。这些术语不是指流量从较低安全性接口至较高安全性接口的移动（通常称为入站），或者流量从较高安全性接口至较低安全性接口的移动（通常称为出站）。

出站 ACL 非常有用，例如，如果您想要仅允许内部网络上的某些主机访问外部网络上的某个网络服务器，可创建仅允许指定主机的单个出站 ACL，而不是创建多个入站 ACL 以限制访问。（请参阅下图。）出站 ACL 会阻止任何其他主机到达外部网络。

图 2: 出站 ACL



规则顺序

规则顺序非常重要。当 ASA 决定转发数据包还是丢弃数据包时，ASA 会按适用 ACL 中列出规则的顺序对照每个规则检测数据包。发现某个匹配后，将不再检查其他规则。例如，如在起始处创建的访问规则显式允许某接口的所有流量，系统将不检查更多的规则。

隐式允许

默认情况下，允许从较高安全性接口流向较低安全性接口的单播 IPv4 和 IPv6 流量。其中，包括路由模式下标准路由接口与桥接虚拟接口 (BVI) 之间的流量。

对于桥接组成员接口，这种从较高安全性接口到较低安全性接口之间的隐式允许仅适用于同一桥接组内的接口。桥接组成员接口与路由接口或不同桥接组的成员之间不存在隐式允许。

默认情况下，桥接组成员接口（路由或透明模式）还允许以下流量：

- 两个方向上的 ARP 流量。（可使用 ARP 检测控制 ARP 流量，但不能通过访问规则控制该流量。）
- 两个方向上的 BPDU 流量。（您可以使用 EtherType 规则控制这些流量。）

对于其他流量，需要使用扩展访问规则 (IPv4 和 IPv6) 或 EtherType 规则 (非 IP)。

隐式拒绝

ACL 列表的末尾有隐式拒绝，因此，除非您显式允许流量，否则流量无法通过。例如，如果除特定地址以外，要允许其他所有用户通过 ASA 访问网络，则需要拒绝这些特定地址，再允许所有其他地址。

对于用来控制传入流量的管理（控制平面）ACL，接口的管理规则集的末尾没有任何隐式拒绝。相反，与管理访问规则不匹配的任何连接都通过正则访问控制规则进行评估。

对于 EtherType ACL，ACL 末尾处的隐式拒绝不会影响 IP 流量或 ARP 流量；例如，如果您允许 EtherType 8037，则 ACL 末尾处的隐式拒绝此时将不阻止您先前使用扩展 ACL 允许的任何 IP 流量（或者隐式允许的从较高安全性接口流向较低安全性接口的 IP 流量）。然而，如果您使用 EtherType 规则显式拒绝所有流量，则将拒绝 IP 和 ARP 流量，仅物理协议流量（如自动协商流量）仍得以允许。

如果配置全局访问规则，则全局规则之后的隐式拒绝得以处理。请参阅以下操作顺序：

1. 接口访问规则。
2. 对于网桥组成员接口，网桥虚拟接口 (BVI) 访问规则。
3. 全局访问规则。
4. 隐式拒绝。

NAT 和访问规则

在确定访问规则匹配时，访问规则始终将使用真实 IP 地址，即使您已配置 NAT。例如，如果已为内部服务器 (10.1.1.5) 配置 NAT，以使该服务器在外部拥有公共可路由的 IP 地址 209.165.201.5，则用于允许外部流量访问内部服务器的访问规则需要引用该服务器的真实 IP 地址 (10.1.1.5)，而非映射地址 (209.165.201.5)。

扩展访问规则

本节介绍有关扩展访问规则的信息。

用于返回流量的扩展访问规则

对于路由和透明模式下的 TCP、UDP 和 SCTP 连接，ASA 允许建立的双向连接的所有返回流量，无需使用访问规则来允许返回流量。

不过，对于 ICMP 等无连接协议，ASA 会建立单向会话，所以您需要使用访问规则来允许两个方向的 ICMP（通过向源接口和目标接口应用 ACL），或者需要启用 ICMP 检测引擎。ICMP 检测引擎将 ICMP 会话视为双向连接。例如，要控制 ping 操作，请指定 **echo-reply (0)**（ASA 到主机）或 **echo (8)**（主机到 ASA）。

允许广播和组播流量

在路由防火墙模式下，即便访问规则（包括不支持的动态路由协议和 DHCP）中允许广播和组播流量，它们也会受到阻拦。必须配置动态路由协议或 DHCP 中继，才能允许这些流量。

对于在透明或路由防火墙模式下属于同一桥接组成员的接口，可以使用访问规则允许任何 IP 流量通过。



注释 由于这些特殊类型的流量无传输连接，所以需要向入站和出站接口应用访问规则，才能允许返回流量通过。

下表列出了在同一桥接组成员的接口之间可使用访问规则允许的常见流量类型。

表 1: 在同一个桥接组成员之间应用访问规则的特殊流量

流量类型	协议或端口	说明
DHCP	UDP 端口 67 和 68	如果启用 DHCP 服务器，则 ASA 不会传送 DHCP 数据包。
EIGRP	协议 88	—
OSPF	协议 89	—
组播流	UDP 端口因应用而异。	组播流始终以 D 类地址为目标（224.0.0.0 至 239.x.x.x）。
RIP (v1 或 v2)	UDP 端口 520	—

管理访问规则

您可以配置访问规则来控制流向 ASA 的管理流量。传入管理流量的访问控制规则（例如与接口的 HTTP、Telnet 和 SSH 连接）的优先级高于应用的管理访问规则。因此，系统允许此类允许的管理流量传入，即使被所有传入 ACL 明确拒绝。

与正则访问规则不同，接口的管理规则集末尾没有隐式拒绝。而是由正则访问控制规则对任何未匹配管理访问规则的连接进行评估。

或者，可使用 ICMP 规则控制流向设备的 ICMP 流量。使用正则扩展访问规则可控制通过设备的 ICMP 流量。

EtherType 规则

本节介绍 EtherType 规则。

支持的 EtherType 和其他流量

EtherType 规则控制以下方面：

- 一个 16 位十六进制数字标识的 EtherType，包括常见类型 IPX 和 MPLS 单播或组播。
- 以太网 V2 帧。

- 默认情况下允许的 BPDU。BPDU 采用 SNAP 封装，ASA 专用于处理 BPDU。
- 中继端口（思科专有）BPDU。中继 BPDU 在负载内包含 VLAN 信息，因此，如果允许 BPDU，ASA 将使用出站 VLAN 修改负载。
- 中间系统到中间系统 (IS-IS)。
- IEEE 802.2 逻辑链路控制数据包。可以根据目标服务无线接入点地址来控制访问。

不支持以下类型的流量：

- 802.3 格式化帧 - 规则将不处理这些帧，因为它们使用长度字段而不是类型字段。

返回流量的 EtherType 规则

因为 EtherType 是无连接的，所以，如果想要在两个方向上允许流量通过，则需要在两个接口上都应用规则。

允许 MPLS

如果允许 MPLS，请确保已通过 ASA 建立标签分发协议和标记分发协议 TCP 连接，方法是将两个连接到 ASA 的 MPLS 路由器配置为使用 ASA 接口上的 IP 地址作为 LDP 或 TDP 会话的路由器 ID。

（LDP 和 TDP 允许 MPLS 路由器协商用于转发数据包的标签（地址）。）

在思科 IOS 路由器上，输入协议、LDP 或 TDP 的相应命令。*interface* 为连接到 ASA 的接口。

mpls ldp router-id interface force

或

tag-switching tdp router-id interface force

面向访问规则的许可

访问控制规则无需专用许可证。

但是，要使用 **sctp** 作为规则中的协议，您必须拥有运营商许可证。

访问控制指南

IPv6 准则

支持 IPv6。（9.0 及更高版本）源和目标地址可能包括 IPv4 和 IPv6 地址的任意混合。对于 9.0 之前的版本，您必须创建单独的 IPv6 访问规则。

每用户 ACL 准则

- 每用户 ACL 使用 **timeout uauth** 命令中的值，但该值可被 AAA 每用户会话超时值覆盖。

- 如果由于每用户 ACL 而拒绝流量，则将记录系统日志消息 109025。如果允许流量，则将不生成系统日志消息。每用户 ACL 中的 **log** 选项将不产生影响。

其他准则和限制

- 通过启用对象组搜索可降低搜索访问规则所需的内存，但此规则会影响查询性能及增加 CPU 使用量。已启用的对象组搜索不会展开网络或服务对象，而是根据这些组定义搜索匹配的访问规则。可以点击访问规则表下方的 **Advanced** 按钮设置此选项。

对于每个连接，将根据网络对象匹配源和目标 IP 地址。如果将源地址匹配的对象数乘以目标地址匹配的对象数结果超过 10,000，则丢弃连接。此检查是为了防止性能降低。配置规则以防止过多的匹配项。



注释 对象组搜索仅适用于网络和服务对象。它不适用于安全组或用户对象。如果 ACL 包括安全组，请勿启用此功能。结果可能是非活动的 ACL 或其他意外行为。

- 可使用访问组的事务提交模型，从而提高系统性能和可靠性。有关详细信息，请参阅常规操作配置指南中的基本设置章节。该选项位于 **配置 > 设备管理 > 高级 > 规则引擎** 下。
- 在 ASDM 中，规则描述基于出现在 ACL 中规则之前的访问列表注释，对于在 ASDM 中创建的新规则，任何描述均将配置为相关规则之前的注释。然而，ASDM 中的数据包跟踪器匹配在 CLI 中在匹配规则之后配置的注释。
- 如果在源地址或目标地址或者源服务或目标服务中输入不止一个项目，ASDM 将使用前缀 **DM_INLINE** 为其自动创建对象组。在规则表视图中，这些对象会自动扩展至其组件部分，但如果在 **Tools > Preferences** 中取消选择 **Auto-expand network and service objects with specified prefix** 规则表首选项，可以看到对象名称。
- 通常情况下，无法引用在 ACL 或对象组中不存在的对象或对象组，或删除当前被引用的对象或对象组。也无法引用在 **access-group** 命令中不存在的 ACL（以应用访问规则）。但是，可以更改此默认行为，以便可在创建对象或 ACL 之前进行“向前引用”。在创建对象或 ACL 之前，任何引用它们的规则或访问组都将被忽略。要启用向前引用，请选择访问规则高级设置中的选项；依次选择 **配置 > 访问规则**，然后点击高级按钮。

配置访问控制

以下主题解释如何配置访问控制。

配置访问规则

要应用访问规则，请执行以下步骤。

过程

步骤 1 依次选择 **Configuration > Firewall > Access Rules**。

规则按接口和方向排列，全局规则另行分组。如果配置管理访问规则，则它们将在此页面上重复出现。这些分组等同于已创建并分配至接口或作为访问组全局性分配的扩展 ACL。这些 ACL 也显示在 ACL Manager 页面上。

步骤 2 执行以下任一操作：

- 要添加新规则，请依次选择 **Add > Add Access Rule**。
- 要在容器内的特定位置插入规则，请选择现有规则，并依次选择 **Add > Insert** 以便在该规则上方添加规则，或依次选择 **Add > Insert After**。
- 要编辑规则，请选择规则并点击 **Edit**。

步骤 3 填写规则属性。可选择的主要选项如下：

- **Interface** - 要应用规则的接口。选择 Any 以创建全局规则。对于路由模式下的桥接组，可以为网桥虚拟接口 (BVI) 和每个桥接组成员接口创建访问规则。
- **Action: Permit/Deny** - 是允许所述流量还是拒绝（丢弃）所述流量。
- **Source/Destination criteria** - 源（原始地址）和目标（流量的目标地址）的定义。通常要配置主机或子网的 IPv4 或 IPv6 地址，可以使用网络或网络对象组进行表示。还可以为源指定用户或用户组名称。此外，如果要将规则限制在比所有 IP 流量更窄的范围，则可以使用 Service 字段识别特定类型的流量。如果实施 Trustsec，则可使用安全组定义源和目标地址。

有关所有可用选项的详细信息，请参阅 [访问规则属性](#)，第 18 页。

定义规则完毕，请点击 **OK** 以将规则添加至表。

步骤 4 点击 **Apply**，以将访问规则保存至配置。

访问规则属性

添加或编辑访问规则时，可配置以下属性。在很多字段中，可以点击编辑方框右侧的“...”按钮，选择、创建或编辑字段可用的对象。

接口

将规则应用到的接口。选择 Any 以创建全局规则。对于路由模式下的桥接组，可以选择网桥虚拟接口 (BVI) 或桥接组成员接口。

操作：允许/拒绝

许可（允许）所述的流量或者拒绝（丢弃）它们。

源条件

尝试匹配的流量的始发器特征。必须配置 **Source**，但其他属性可选。

来源

源的 IPv4 或 IPv6 地址。默认值为 **any**，该值会匹配所有 IPv4 或 IPv6 地址；可以使用 **any4** 以只将 IPv4 作为目标，或使用 **any6** 以只将 IPv6 作为目标。可指定单个主机地址（如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）、子网（采用 0.100.10.0/24 或 10.100.10.0/255.255.255.0 格式，或者对于 IPv6，采用 2001:DB8:0:CD30::/60 格式）、网络对象或网络对象组的名称，或者接口的名称。

用户

如果启用身份防火墙，可以指定用户或用户组作为流量源。用户当前使用的 IP 地址将匹配规则。可以指定用户名 (DOMAIN\user)、用户组 (DOMAIN\group，注意 \ 表示组名称) 或用户对象组。对于此字段，点击“...”，从 AAA 服务器组中选择名称比直接键入名称更方便。

Security Group

如果启用思科 Trustsec，可以指定安全组名称或标记 (1-65533) 或安全组对象。

More Options > Source Service

如果指定 TCP、UDP 或 SCTP 作为目标服务，可以选择性地为 TCP、UDP、TCP-UDP 或 SCTP 指定预定义的服务对象，或者使用自己的对象。通常，只需定义目标服务，而无需定义源服务。请注意，如果定义源服务，则目标服务协议必须与其匹配（例如，带或不带端口定义的 TCP）。

目标条件

尝试匹配的流量的目标特征。必须配置 **Destination**，但其他属性可选。

目标

目标的 IPv4 或 IPv6 地址。默认值为 **any**，该值会匹配所有 IPv4 或 IPv6 地址；可以使用 **any4** 以只将 IPv4 作为目标，或使用 **any6** 以只将 IPv6 作为目标。可指定单个主机地址（如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）、子网（采用 0.100.10.0/24 或 10.100.10.0/255.255.255.0 格式，或者对于 IPv6，采用 2001:DB8:0:CD30::/60 格式）、网络对象或网络对象组的名称，或者接口的名称。

Security Group

如果启用思科 Trustsec，可以指定安全组名称或标记 (1-65533) 或安全组对象。

服务

流量的协议（例如 IP、TCP、UDP）以及 TCP、UDP 或 SCTP 的可选端口。默认值为 IP，但可以选择更具体的协议以将更精细的流量作为目标。通常，可以选择某些类型的服务对象。对于 TCP、UDP 和 SCTP，可以指定端口，例如 tcp/80、tcp/http、tcp/10-20（用于端口范围）、tcp-udp/80（匹配端口 80 上的任意 TCP 或 UDP 流量）、sctp/diameter 等等。

说明

规则的用途说明，每行最多 100 个字符。可输入多行；每行均在 CLI 中作为注释添加，注释将放置在规则之前。



注释 如果将含非英文字符的备注添加到一个平台（如 Windows）上，然后尝试从另一个平台（如 Linux）将这些备注删除，则可能无法编辑或删除这些备注，因为原特征可能无法被正确识别。此限制由底层平台依赖性所导致，其以不同方式对不同语言进行编码。

Enable Logging、Logging Level、More Options > Logging Interval

日志记录选项定义如何为规则生成系统日志消息。可以实施以下日志记录选项：

取消选择 Enable Logging

此操作将为规则禁用日志记录。对于匹配此规则的连接，不会发出任何类型的系统日志消息。

选择 Enable Logging，设置 Logging Level = Default

此操作为规则提供默认日志记录。对于每个被拒绝的连接发出系统日志消息 106023。如果设备受到攻击，发出此消息的频率可能会影响服务。

选择 Enable Logging，使用非默认日志记录级别

此操作提供一条汇总系统日志消息 106100，而不是 106023。在第一次命中后，系统将发出消息 106100，然后在 **More Options > Logging Interval** 中配置的每个间隔（默认值为每隔 300 秒，可以指定 1 - 600 秒）后再次发出消息，显示在间隔过程中的命中次数。建议的日志记录级别为 **Informational**。

汇总拒绝消息可以减少攻击的影响，并且有可能方便您分析消息。如果受到拒绝服务攻击，则可能会看到消息 106101，表示用于为消息 106100 生成命中次数的缓存拒绝流的数量已超过某个间隔内的最大值。此时，设备将在下一个间隔前停止收集统计信息以减轻攻击。

More Options > Traffic Direction

规则适用于 **In** 还是 **Out** 方向。**In** 是默认值，对于全局和管理访问规则，它是唯一选项。

More Options > Enable Rule

规则在设备上是否处于活动状态。已禁用的规则在规则表中显示为带删除线的文本。禁用规则可以让您在不删除规则的情况下停止将其应用到流量，以便可以在以后需要时重新启用。

More Options > Time Range

定义规则应在一周中的哪几天以及一天中的哪些时段处于活动状态的时间范围对象的名称。如果不指定时间范围，规则将始终处于活动状态。

配置访问规则的高级选项

高级访问规则选项可供您自定义规则行为的某些方面，但这些选项拥有适用于大多数情况的默认值。

过程

步骤 1 依次选择配置 > 防火墙 > 访问规则。

步骤 2 点击规则表下方的 **Advanced** 按钮。

步骤 3 根据需要配置以下选项：

- **Advanced Logging Settings** - 如果配置非默认日志记录，则系统将缓存拒绝流，以便生成消息 106100 的统计信息，如[评估访问规则的系统日志消息](#)，第 25 页中所述。为了防止无限制地占用内存和 CPU 资源，ASA 会限制并行拒绝流数，因为它们可能指示攻击。到达该限制时，将会发布消息 106101。可控制与消息 106101 相关的以下方面。
 - **Maximum Deny-flows** - 在 ASA 停止缓存流之前允许的最大拒绝流数，该值介于 1 到 4096 之间。默认值为 4096。
 - **Alert Interval** - 发布系统日志消息 106101 的间隔时长（1-3600 秒），该消息指示已达到拒绝流的最大数量。默认值为 300 秒。

- **Per User Override table** - 对于从 RADIUS 服务器下载用于用户授权的动态用户 ACL，是否允许其覆盖已分配至接口的 ACL。例如，如果接口 ACL 拒绝来自 10.0.0.0 的所有流量，但动态 ACL 允许来自 10.0.0.0 的所有流量，则动态 ACL 将覆盖该用户的接口 ACL。对于应允许用户覆盖的每个接口（仅入站方向），请选择 **Per User Override** 复选框。如已禁用每用户覆盖功能，则 RADIUS 服务器提供的访问规则将与在该接口上配置的访问规则相组合。

默认情况下，将不针对接口 ACL 匹配 VPN 远程访问流量。不过，如果取消选择 Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles 窗格中的 **Enable inbound VPN sessions to bypass interface access lists** 设置，行为将取决于组策略中是否应用了 VPN 过滤器（请参阅 Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add/Edit > General > More Options > Filter 字段）以及是否设置了 Per User Override 选项：

- **No Per User Override, no VPN filter** - 根据接口 ACL 匹配流量。
 - **No Per User Override, VPN filter** - 先根据接口 ACL 匹配流量，再根据 VPN 过滤器匹配流量。
 - **Per User Override, VPN filter** - 仅根据 VPN 过滤器匹配流量。
- **Object Group Search Setting** - 通过选择 **Enable Object Group Search Algorithm**，可减少搜索使用了对象组的访问规则所需的内存，但这将以降低规则查找性能为代价。已启用的对象组搜索将不展开网络对象，而是根据这些组定义搜索匹配的访问规则。

注释 对象组搜索仅适用于网络和服务对象。它不适用于安全组对象。如果 ACL 包括安全组，请勿启用此功能。结果可能是非活动的 ACL 或其他意外行为。

- **Forward Reference Setting** - 通常，不能在 ACL 或对象组中引用不存在的对象或对象组，也不能删除目前已引用的对象或对象组。也无法引用在 **access-group** 命令中不存在的 ACL（以应用访问规则）。但是，可以更改此默认行为，以便可在创建对象或 ACL 之前进行“向前引用”。在创建对象或 ACL 之前，任何引用它们的规则或访问组都将被忽略。请选择 **Enable the forward**

reference of objects and object-groups 以便启用前向引用。请注意，如果启用向前引用，ASDM 则无法明确对现有对象的错误引用与向前引用之间的差别。

步骤 4 点击确定。

配置管理访问规则

您可以配置接口 ACL 来控制从特定对等体（或对等体集）到 ASA 的传入管理流量。在一种情况下，此类型 ACL 非常有用，即当您想要阻止 IKE 拒绝服务攻击时。

与正则访问规则不同，接口的管理规则集末尾没有隐式拒绝。而是由正则访问控制规则对任何未匹配管理访问规则的连接进行评估。

过程

步骤 1 依次选择 **Configuration > Device Management > Management Access > Management Access Rules**。

规则将按接口进行排列。每个分组等同于作为控制平面 ACL 创建并分配至接口的扩展 ACL。这些 ACL 也将显示在 Access Rules 和 ACL Manager 页面上。

步骤 2 执行以下任一操作：

- 要添加新规则，请依次选择 **Add > Add Management Access Rule**。
- 要在容器内的特定位置插入规则，请选择现有规则，并依次选择 **Add > Insert** 以便在该规则上方添加规则，或依次选择 **Add > Insert After**。
- 要编辑规则，请选择规则并点击 **Edit**。

步骤 3 填写规则属性。可选择的主要选项如下：

- **Interface** - 要应用规则的接口。对于路由模式下的桥接组，可以为网桥虚拟接口 (BVI) 和每个桥接组成员接口创建访问规则。
- **Action: Permit/Deny** - 是允许所述流量还是拒绝（丢弃）所述流量。
- **Source/Destination criteria** - 源（原始地址）和目标（流量的目标地址）的定义。通常要配置主机或子网的 IPv4 或 IPv6 地址，可以使用网络或网络对象组进行表示。还可以为源指定用户或用户组名称。此外，如果要将规则限制在比所有 IP 流量更窄的范围，则可以使用 Service 字段识别特定类型的流量。如果实施 Trustsec，则可使用安全组定义源和目标地址。

有关所有可用选项的详细信息，请参阅 [访问规则属性](#)，第 18 页。

定义规则完毕，请点击 **OK** 以将规则添加至表。

步骤 4 点击 **Apply**，以将规则保存至配置。

配置 EtherType 规则

EtherType 规则适用于网桥组成员接口上的非 IP 第 2 层流量（在路由或透明防火墙模式下）。可以使用这些规则，根据第 2 层数据包中的 EtherType 值允许或丢弃流量。使用 EtherType 规则，可以控制非 IP 流量跨 ASA 的流动。

对于桥接组成员接口，可同时应用扩展和 EtherType 访问规则。EtherType 规则优先于扩展访问规则。

过程

步骤 1 依次选择 **Configuration > Firewall > EtherType Rules**。

规则按接口和方向排列。每个分组等同于已创建并分配至接口的 EtherType ACL。

步骤 2 执行以下任一操作：

- 要添加新规则，请依次选择添加 > 添加 **EtherType** 规则。
- 要在容器内的特定位置插入规则，请选择一条现有规则，并依次选择添加 > 插入，以便在该规则上方添加规则，或依次选择添加 > 插入其后。
- 要编辑规则，请选择规则并点击 **Edit**。

步骤 3 填写规则属性。可选择的主要选项如下：

- **Interface** - 要应用规则的接口。
- **Action: Permit/Deny** - 是允许所述流量还是拒绝（丢弃）所述流量。
- **EtherType** - 可使用以下选项来匹配流量：
 - **any** - 匹配所有流量。
 - **bpdu** - 默认允许的桥接协议数据单位。当您应用配置时，此关键字将转换为设备上的 **dsap bpdu**。
 - **dsap** - IEEE 802.2 逻辑链路控制数据包的目标服务无线接入点地址。此外，还需要在 **DSAP Value** 中包括要允许或拒绝的十六进制格式地址，范围介于 0x01 到 0xff 之间。以下是一些通用地址的值：
 - **0X42** - 桥接协议数据单元 (BPDU)。当您应用配置时，这将转换为设备上的 **dsap bpdu**。
 - **0xc0** - 互联网数据包交换 (IPX) 802.2 LLC。当您应用配置时，这将转换为设备上的 **dsap ipx**。
 - **0xfe** - 中间系统到中间系统 (IS-IS)。当您应用配置时，这将转换为设备上的 **dsap isis**。
 - **0xff** - 原始 IPX 802.3 格式。当您应用配置时，这将转换为设备上的 **dsap raw-ipx**。
 - **eii-ipx** - 以太网 II IPX 格式，EtherType 0x8137。

- **ipx** - 互联网数据包交换 (IPX)。此关键字是为 **dsap ipx**、**dsap raw-ipx** 和 **eii-ipx** 配置三条单独规则的快捷方式。在您将配置应用于设备时进行转换。
- **isis** - 中间系统到中间系统 (IS-IS)。当您应用配置时，此关键字将转换为设备上的 **dsap isis**。
- **Mpls-multicast** - MPLS 组播。
- **mpls-unicast** - MPLS 单播。
- **hex_number** - 16 位十六进制数字 (0x600 到 0xffff) 可识别的任何 EtherType。请参阅 <http://www.ietf.org/rfc/rfc1700.txt> 上的 RFC 1700 “分配的编号”，以获取 EtherType 列表。
- **Description** - 规则用途的解释，每行最多 100 个字符。可输入多行；每行均在 CLI 中作为注释添加，注释将放置在规则之前。
- **更多选项 > 方向** - 规则用于传入还是传出方向。**In** 为默认值。

定义规则完毕，请点击 **OK** 以将规则添加至表。

步骤 4 点击 **Apply**，以将规则保存至配置。

配置 ICMP 访问规则

默认情况下，您可以使用 IPv4 或 IPv6 将 ICMP 数据包发送到任何接口，以下情况例外：

- ASA 不响应定向至广播地址的 ICMP 回显请求。
- ASA 仅响应发送至流量进入的接口的 ICMP 流量；不能通过某个接口将 ICMP 流量发送至远端接口。

为了保护设备免受攻击，您可以使用 ICMP 规则将接口的 ICMP 访问限制为特定主机、网络或 ICMP 类型。ICMP 规则的工作原理与访问规则类似，将对规则进行排序，与数据包匹配的第一条规则将定义操作。

如为某个接口配置任何 ICMP 规则，则将隐式拒绝 ICMP 规则添加至 ICMP 规则列表的末尾，从而更改默认行为。因此，如果想要仅拒绝几种消息类型，则须在 ICMP 规则列表的末尾纳入一条允许任何消息类型的规则，以便允许剩余的消息类型。

我们建议，始终为 ICMP 不可到达消息类型（类型 3）授予权限。拒绝 ICMP 不可达消息会禁用 ICMP 路径 MTU 发现，从而可能阻止 IPsec 和 PPTP 流量。此外，IPv6 中的 ICMP 数据包用于 IPv6 邻居发现进程。

过程

步骤 1 依次选择配置 > 设备管理 > 管理访问 > ICMP。

步骤 2 配置 ICMP 规则：

- a) 添加规则（**Add > Rule**、**Add > IPv6 Rule** 或 **Add > Insert**），或者选择并编辑一条规则。

- b) 选择要控制的 ICMP 类型，或选择 **any** 以应用于所有类型。
- c) 选择要将规则应用至的接口。必须为每个接口创建单独的规则。
- d) 选择是允许还是拒绝匹配流量的访问。
- e) 选择 **Any Address**，以将规则应用于所有流量。或者，输入您正尝试控制的主机或网络的地址与掩码（适用于 IPv4），或地址与前缀长度（适用于 IPv6）。
- f) 点击 **OK**。

步骤 3（可选）要设置 ICMP 无法到达的消息限制，请设置以下选项。要允许跟踪路由通过 ASA（作为其中一跳显示 ASA），需要增加速率限制并在服务策略中启用 **Decrement time to live for a connection** 选项（在 Configuration > Firewall > Service Policy Rules > Rule Actions > Connection Settings 对话框中）。

- 速率限制 - 设置不可达消息的速率限制，该限制介于每秒 1 至 100 条消息之间。默认值为每秒 1 条消息。
- 突发大小 - 设置突发速率，其值介于 1 至 10 之间。系统当前未使用此值。

步骤 4 点击 **Apply**。

监控访问规则

Access Rules 页面包含每条规则的命中计数。将鼠标指针悬停在命中计数之上，即可查看计数的更新时间和间隔。要重置命中计数，右键单击规则，然后选择 **Clear Hit Count**，但请注意，这将清除应用至相同接口相同方向的所有规则的计数。

评估访问规则的系统日志消息

使用系统日志事件查看器，如 ASDM 中的查看器，查看与访问规则相关的消息。

如果使用默认日志记录，则只会看到与显式拒绝的流对应的系统日志消息 106023。将不记录与规则列表末尾的“隐式拒绝”条目匹配的流量。

如果已连接 ASA，则拒绝数据包的系统日志消息数可能非常大。我们建议您转而启用使用系统日志消息 106100 的日志记录，该记录提供每条规则（包括允许规则）的统计信息，且可使您限制所生成的系统日志消息的数量。或者，可禁用给定规则的所有日志记录。

当您对消息 106100 启用日志记录时，如果数据包与某个 ACE 匹配，ASA 会创建一个流条目来跟踪特定间隔内收到的数据包数。ASA 会在首次计数和每个间隔结束时都生成一条系统日志消息，标识该间隔内计数的总数以及最后一次计数的时间戳。在每个间隔结束时，ASA 会将计数数额重置为 0。如果在一个间隔内没有数据包匹配，ASA 将删除该流条目。为规则配置日志记录时，可控制间隔，甚至可控制每条规则的日志消息的严重性级别。

流是按源与目标 IP 地址、协议和端口定义的。由于对于相同两台主机之间的新连接而言源端口可能不同，且为该连接创建了新的流，因此，可能看不到相同的流递增。

不需要针对 ACL 检查属于已建立连接的已允许数据包；仅初始数据包将得以记录并纳入命中计数中。对于无连接的协议（如 ICMP），所有数据包均得以记录，即使它们是被允许的数据包，且所有已拒绝数据包均得以记录。

有关这些消息的详细信息，请参阅系统日志消息指南。



提示 当您对消息 106100 启用日志记录时，如果数据包与某个 ACE 匹配，ASA 会创建一个流条目来跟踪特定间隔内收到的数据包数。ASA 包含的 ACE 日志记录流最大为 32 K。在任何时间点，都可能有大量的流同时存在。为了防止无限制地占用内存和 CPU 资源，ASA 会限制并发拒绝流的数量；由于拒绝流可能意味着正在发生攻击，所以该限制仅应用于拒绝流（不应用于允许流）。达到该限制时，ASA 在现有流到期前不会对日志记录创建新的拒绝流，并会发出消息 106101。可在高级设置中控制发出该消息的频率和缓存的拒绝流的最大数量；请参阅[配置访问规则的高级选项](#)，第 20 页。

访问规则的历史

功能名称	平台版本	说明
接口访问规则	7.0(1)	使用 ACL 通过 ASA 控制网络访问。 引入了以下屏幕：Configuration > Firewall > Access Rules。
全局访问规则	8.3(1)	引入了全局访问规则。 修改了以下屏幕：Configuration > Firewall > Access Rules。
标识防火墙的支持	8.4(2)	现在可以将身份防火墙用户和组用于源和目标。可以将身份防火墙 ACL 与访问规则、AAA 规则配合使用，并可将其用于 VPN 身份验证。
IS-IS 流量的 EtherType ACL 支持	8.4(5)、9.1(2)	在透明防火墙模式下，ASA 现在可使用 EtherType ACL 传输 IS-IS 流量。 修改了以下屏幕：Configuration > Device Management > Management Access > EtherType Rules。
对 TrustSec 的支持	9.0(1)	现可将 TrustSec 安全组用于源和目标。可以将身份防火墙 ACL 与访问规则配合使用。

功能名称	平台版本	说明
适用于 IPv4 和 IPv6 的统一 ACL	9.0(1)	<p>ACL 现支持 IPv4 和 IPv6 地址。甚至可以为源和目标同时指定 IPv4 和 IPv6 地址。更改了 any 关键字以表示 IPv4 和 IPv6 流量。添加了 any4 和 any6 关键字以分别表示纯 IPv4 和纯 IPv6 流量。特定于 IPv6 的 ACL 已弃用。现有 IPv6 ACL 已迁移到扩展 ACL。有关迁移的详细信息，请参阅版本说明。</p> <p>修改了以下屏幕：</p> <p>Configuration > Firewall > Access Rules Configuration > Remote Access VPN > Network (Client) Access > Group Policies > General > More Options</p>
用于按 ICMP 代码过滤 ICMP 流量的扩展 ACL 和对象增强	9.0(1)	<p>现在可以根据 ICMP 代码允许/拒绝 ICMP 流量。</p> <p>引入或修改了以下菜单项：</p> <p>Configuration > Firewall > Objects > Service Objects/Groups Configuration > Firewall > Access Rule</p>
基于访问组规则引擎的事务提交模型	9.1(5)	<p>一经启用，规则更新在规则编译完成后即可得以应用；不会影响规则匹配性能。</p> <p>引入了以下屏幕：Configuration > Device Management > Advanced > Rule Engine。</p>
用于编辑 ACL 和对象的配置会话。向前引用访问规则中的对象和 ACL。	9.3(2)	<p>现在，可以在单独的配置会话中编辑 ACL 和对象。还可以向前引用对象和 ACL，也就是说，可以为尚未存在的对象或 ACL 配置规则和访问组。</p>
流控制传输协议 (SCTP) 的访问规则支持	9.5(2)	<p>现在，您可以使用 sctp 协议（包括端口规范）创建访问规则。</p> <p>在 Configuration > Firewall > Access Rules 页面上修改了访问规则的添加/编辑对话框。</p>
对 IEEE 802.2 逻辑链路控制数据包的目标服务无线接入点地址的 Ethertype 规则支持。	9.6(2)	<p>现在，您可以为 IEEE 802.2 逻辑链路控制数据包的目标服务访问点地址编写 Ethertype 访问控制规则。添加此支持后，bpdu 关键字与预期流量不再匹配。我们重写了 dsap 0x42 的 bpdu 规则。</p> <p>修改了以下菜单项：配置 > 防火墙 > EtherType 规则。</p>
在路由模式下，桥接组成员接口上支持 Ethertype 规则，桥接组虚拟接口 (BVI) 上支持扩展访问规则。	9.7(1)	<p>现在，您可以创建 Ethertype ACL，并在路由模式下将它们应用于桥接组成员接口。除成员接口之外，您还可以向桥接虚拟接口 (BVI) 应用扩展访问规则。</p> <p>修改了以下屏幕：Configuration > Firewall > Access Rules、Configuration > Firewall > Ethertype Rules。</p>

功能名称	平台版本	说明
EtherType 访问控制列表更改。	9.9(1)	<p>EtherType 访问控制列表现在支持以太网 II IPX (EII IPX)。此外，在 DSAP 关键字中增加了新关键字，以支持通用 DSAP 值：BPDU (0x42)、IPX (0xE0)、Raw IPX (0xFF) 和 ISIS (0xFE)。因此，现有的使用 BPDU 或 ISIS 关键字的 EtherType 访问控制条目将被自动转换为使用 DSAP 规范，并且 IPX 的规则将被转换为 3 条规则（DSAP IPX、DSAP Raw IPX 和 EII IPX）。此外，使用 IPX 作为 EtherType 值的数据包捕获已被弃用，因为 IPX 对应于 3 个单独的 EtherType。</p> <p>修改了以下菜单项：配置 > 防火墙 > Ethertype 规则。</p>



第 3 章

访问控制的对象

对象指配置中可重用的组件。在思科 ASA 配置中可以定义和使用它们来代替内联 IP 地址、服务、名称等。可以使用对象轻松维护配置，因为只需要修改某一位置的对象，便可以使该对象在引用该对象的所有其他位置显示出来。如未使用对象，必要时必须逐一修改每项功能的参数，而不是一次性修改完成。例如，如果网络对象定义了 IP 地址和子网掩码，当要更改地址时，只需要在对象定义中进行更改，而无需在引用该 IP 地址的各项功能中逐一更改。

- [对象指南，第 29 页](#)
- [配置对象，第 30 页](#)
- [监控对象，第 36 页](#)
- [对象的历史，第 36 页](#)

对象指南

IPv6 指导原则

在以下限制条件下支持 IPv6:

- 可以在网络对象组中混合 IPv4 和 IPv6 条目，但不能将混合的对象组用于 NAT。

其他准则和限制

- 由于对象和对象组共享同一命名空间，对象名称必须唯一。当可能想要创建名为“Engineering”的网络对象组以及名为“Engineering”的服务对象组时，需要在至少其中一个对象组名称的末尾添加一个标识符（或“标签”），使其名称唯一。例如，可以使用名称“Engineering_admins”和“Engineering_hosts”，使对象组名称保持唯一，同时有助于进行识别。
- 如果在 ACL 或访问规则的源地址或目标地址或者源服务或目标服务中输入不止一个项目，ASDM 将自动使用前缀 DM_INLINE 为其创建对象组。这些对象不会显示在对象页面中，但它们是在设备上定义的。
- 对象名称限于 64 个字符，包括字母、数字和如下字符：.!@#%^&()-_{}。对象名称区分大小写。

- 如果在命令中使用对象，则无法将对象删除或留空，除非启用前向引用（在访问规则高级设置中）。

配置对象

以下各节介绍如何配置主要用于访问控制的对象。

配置网络对象和组

网络对象和组可以识别 IP 地址或主机名。可以使用访问控制列表中的这些对象来简化规则。

配置网络对象

网络对象可以包含主机、网络 IP 地址、IP 地址范围或完全限定域名 (FQDN)。

也可以启用对象的 NAT 规则（FQDN 对象除外）。有关配置对象 NAT 的详细信息，请参阅[网络地址转换 \(NAT\)](#)，第 171 页。

过程

步骤 1 依次选择 **Configuration > Firewall > Objects > Network Objects/Group**。

步骤 2 执行以下操作之一：

- 依次选择 **Add > Network Object**，添加新的对象。输入名称和说明（后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3 基于对象 **Type** 和 **IP version** 字段配置对象的地址。

- **Host** - 单个主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **Network** - 网络的地址。对于 IPv4，请添加掩码，例如，**IP address** = 10.0.0.0 **Netmask** = 255.0.0.0。对于 IPv6，请添加前缀，例如 **IP Address** = 2001:DB8:0:CD30:: **Prefix Length** = 60。
- **Range** - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。
- **FQDN** - 完全限定域名，即主机的名称，例如 www.example.com。

步骤 4 点击 **OK**，然后点击 **Apply**。

现在即可使用该网络对象来创建规则。如果编辑对象，则使用该对象的任何规则都将自动继承更改。

配置网络对象组

网络对象组可以包含多个网络对象以及内联网络或主机。网络对象组可以同时包含 IPv4 和 IPv6 地址。

但是，无法使用包含 IPv4 和 IPv6 的混合对象组进行 NAT，也无法使用包含 FQDN 对象的对象组。

过程

步骤 1 依次选择 **Configuration > Firewall > Objects > Network Objects/Groups**。

步骤 2 执行以下操作之一：

- 依次选择 **Add > Network Object Group**，添加新的对象。输入名称和说明（后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3 使用以下方法的任意组合将网络对象添加到组：

- **Existing Network Objects/Groups** - 选择已定义的任何网络对象或组，然后点击 **Add** 将其添加到组。
- **Create New Network Object Member** - 输入适用于新网络对象的条件，然后点击 **Add**。如果为对象命名，则在应用更改时，会创建新的对象并添加到组中。添加主机或网络时，名称为可选项。

步骤 4 添加所有成员对象之后，点击 **OK**，然后点击 **Apply**。

现在即可在创建规则时使用该网络对象组。对于已编辑的对象组，使用该组的任何规则都将自动继承更改。

配置服务对象和服务组

服务对象和组可标识协议和端口。可以使用访问控制列表中的这些对象来简化规则。

配置服务对象

服务对象可以包含单个协议规范。

过程

步骤 1 依次选择 **配置 > 防火墙 > 对象 > 服务对象/组**。

步骤 2 执行以下操作之一：

- 依次选择 **Add > Service Object**，添加新的对象。输入名称和说明（后者为可选项）。

- 选择现有的对象，然后点击 **Edit**。

步骤 3 选择服务类型，并按需填写详细信息：

- Protocol - 介于 0 到 255 之间的数字，或已知名称，如 **ip**、**tcp**、**udp**、**gre** 等等。
- ICMP、ICMP6 - 可以将消息类型和代码字段留空，以匹配任何 ICMP/ICMP 第 6 版消息。或者，可以按名称或编号 (0-255) 指定 ICMP 类型，以便将对象限于该消息类型。如果指定类型，则可以选择性地为该类型指定一个 ICMP 代码 (1-255)。如果不指定代码，则使用所有代码。
- TCP、UDP、SCTP - 可以选择性地指定源和/或目标的端口。可以按名称或编号指定端口。可以添加以下操作符：
 - < - 小于。例如，<80。
 - > - 大于。例如，>80。
 - != - 不等于。例如，!=80。
 - - (连字号) - 值的范围（含两端）。例如，100-200。

步骤 4 点击 **OK**，然后点击 **Apply**。

配置服务组

服务对象组包括各种协议的组合，如果需要，包括使用协议的可选源端口和目标端口以及 ICMP 类型和代码。

开始之前

可以使用通用服务对象组来建立所有服务的模型（如本节所介绍）。不过，仍然可以配置 ASA 8.3(1) 版本之前可用的服务对象组的类型。上述旧版对象包括 TCP/UDP/TCP-UDP 端口组、协议组和 ICMP 组。这些组的内容与通用服务对象组（ICMP 组除外）中的关联配置等效，因为这些组不支持 ICMP6 或 ICMP 代码。如果仍希望使用这些旧版对象，请参阅 Cisco.com 命令参考中的 **object-service** 命令说明，获取详细的使用说明。

过程

步骤 1 依次选择 **Configuration > Firewall > Objects > Service Objects/Groups**。

步骤 2 执行以下操作之一：

- 依次选择 **Add > Service Group** 以添加新对象。输入名称和说明（后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3 使用以下方法的任意组合将服务对象添加到组：

- **Existing Service/Service Group** - 选择任何已定义的服务、服务对象或组，然后点击 **Add** 将它们添加到组中。
- **Create New Member** - 输入新服务对象的条件，然后点击 **Add**。如果为对象命名，则在应用更改时，会创建新的对象并添加到组；否则，未命名的对象仅为该组的成员。无法为 TCP-UDP 对象命名；这些对象仅为组的成员。

步骤 4 添加所有成员对象之后，点击 **OK**，然后点击 **Apply**。

现在即可在创建规则时使用该服务对象。对于已编辑的对象组，使用该组的任何规则都将自动继承更改。

配置本地用户组

可以创建本地用户组，通过将组列入扩展 ACL 中，在支持身份防火墙的功能中使用本地用户组，进而用于访问规则等。

对于 Active Directory 域控制器中全局定义的用户组，ASA 将向 Active Directory 服务器发送 LDAP 查询。ASA 为基于身份的规则导入这些组。不过，ASA 可能包含未全局定义的本地化网络资源，需要使用支持本地化安全策略的本地用户组。本地用户组可包含从 Active Directory 导入的嵌套组 and 用户组。ASA 可整合本地组和 Active Directory 组。

用户可以属于本地用户组和从 Active Directory 导入的用户组。

由于能够在 ACL 中直接使用用户名和用户组，因此只有在以下情况下才需配置本地用户组：

- 要创建 LOCAL 数据库中定义的一组用户。
- 要创建在 AD 服务器上所定义的单一用户组中未捕获的一组用户 or 用户组。

过程

步骤 1 依次选择 **Configuration > Firewall > Objects > Local User Groups**。

步骤 2 执行以下操作之一：

- 选择 **Add**，添加新对象。输入名称和说明（后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3 使用下列任意一种方法，将用户或组添加到对象：

- **Select existing users or groups** - 选择包含用户或组的域，从列表中选择用户名或组名，然后点击 **Add**。对于长列表，可以使用 Find 框方便查找用户。这些名称从服务器中提取出来，用于所选域。

- **Manually type user names** - 可以简单地在底部编辑框中键入用户名或组名，然后点击 **Add**。使用此方法时，如果未指定域，所选域名会被忽略，并且将使用默认域。对于用户名，格式为 `domain_name\username`；对于组名，则带双反斜杠 `\\`，格式为 `domain_name\\group_name`。

步骤 4 添加所有成员对象之后，点击 **OK**，然后点击 **Apply**。

现在即可在创建规则时使用该用户对象组。对于已编辑的对象组，使用该组的任何规则都将自动继承更改。

配置安全组对象组

例如，通过在扩展 ACL 中包含组，可以创建用于支持 Cisco TrustSec 的功能的安全组对象组，然后该组又可用于访问规则等。

将 ASA 与思科 TrustSec 集成时，ASA 可从 ISE 中下载安全组信息。ISE 可以提供思科 TrustSec 标签到用户的身份映射以及思科 TrustSec 标签到服务器的资源映射，从而充当身份储存库。可以在 ISE 上集中调配和管理安全组 ACL。

不过，ASA 可能包含未全局定义的本地化网络资源，需要使用支持本地化安全策略的本地安全组。本地安全组可以包含下载自 ISE 的嵌套安全组。ASA 可整合本地和中心安全组。

要在 ASA 上创建本地安全组，需要创建本地安全对象组。本地安全对象组可以包含一个或多个嵌套的安全对象组或安全 ID 或安全组名称。另外，也可以创建 ASA 上不存在的新的安全 ID 或安全组名称。

可以使用您在 ASA 上创建的安全对象组来控制对网络资源的访问。可以将安全对象组用作访问组或服务策略的一部分。



提示 如果创建的组包含 ASA 未知的标签或名称，使用该组的任何规则都将处于非活动状态，直到这些标签或名称在 ISE 中得到解析。

过程

步骤 1 依次选择 **Configuration > Firewall > Objects > Security Group Object Groups**。

步骤 2 执行以下操作之一：

- 选择 **Add**，添加新对象。输入名称和说明（后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3 使用下列任意一种方法，将安全组添加到对象：

- **Select existing local security group object groups** - 从已定义的对象列表中选择，然后点击 **Add**。对于长列表，可以使用 Find 框方便查找对象。

- **Select security groups discovered from ISE** - 从现有组列表中选择组，然后点击 **Add**。
- **Manually add security tags or names** - 可以简单地在底部编辑框中键入标签号或安全组名称，然后点击 **Add**。标签为一个介于 1 和 65533 之间的数字，由 ISE 通过 IEEE 802.1X 身份验证、Web 身份验证或 MAC 身份验证绕行 (MAB) 分配给设备。安全组名称在 ISE 上创建，为安全组提供用户友好的名称。此安全组表将 SGT 映射到安全组名称。有关有效标签和名称，请查阅 ISE 配置。

步骤 4 添加所有成员对象之后，点击 **OK**，然后点击 **Apply**。

现在即可在创建规则时使用该安全组对象组。对于已编辑的对象组，使用该组的任何规则都将自动继承更改。

配置时间范围

时间范围对象定义了由起始时间、结束时间和可选循环条目组成的特定时间。可以将这些对象用于 ACL 规则，从而对特定功能或资产提供基于时间的访问。例如，可以创建一条仅允许在工作时间内对特定服务器进行访问的访问规则。



注释 可以在时间范围对象中列入多个定期条目。如果为时间范围规定指定了绝对值和周期值，则只有在达到绝对起始时间后才开始评估周期值，而且在绝对结束时间到达后便不再对其进行评估。

创建时间范围并不会限制对设备的访问。该操作步骤仅定义时间范围。随后必须在访问控制规则中使用该对象。

过程

步骤 1 依次选择 **配置 > 防火墙 > 对象 > 时间范围**。

步骤 2 执行以下操作之一：

- 选择 **Add**，添加新的时间范围。输入名称和说明（后者为可选项）。
- 选择现有的时间范围，然后点击 **Edit**。

步骤 3 选择总体起始和结束时间。

默认为立即开始且永不结束，但是可以设置特定日期和时间。输入的时间包含在时间范围内。

步骤 4 （可选）配置总体活动时间内的循环时间段，例如时间范围将在一周内的某些日期或每周循环间隔内处于活动状态。

- a) 点击 **Add**，或选择现有时间段并点击 **Edit**。
- b) 执行以下操作之一：

- 点击 **Specify days of the week and times on which this recurring range will be active**，并从列表中选择日期和时间。
- 点击 **Specify a weekly interval when this recurring range will be active**，并从列表中选择日期和时间。

c) 点击 **OK**。

步骤 5 点击 **OK**，然后点击 **Apply**。

监控对象

对于网络、服务和安全组对象，可以分析单个对象的使用情况。在 **Configuration > Firewall > Objects** 文件夹中，找到对象所在页面，然后点击 **Where Used** 按钮。

对于网络对象，也可以点击 **Not Used** 按钮，查找在任何规则以及其他对象中都未使用的对象。该屏幕提供一个删除这些未使用对象的快捷方式。

对象的历史

功能名称	平台版本	说明
对象组	7.0(1)	对象组可简化 ACL 的创建和维护。
正则表达式和策略映射	7.2(1)	引入了正则表达式和策略映射，将其用于检查策略映射下。引入了以下命令： class-map type regex、regex、match regex 。
对象	8.3(1)	引入了对象支持功能。
用于身份防火墙的用户对象组	8.4(2)	引入了用于身份防火墙的用户对象组。
用于 Cisco TrustSec 的安全组对象组	8.4(2)	引入了用于 Cisco TrustSec 的安全组对象组
IPv4 和 IPv6 混合网络对象组	9.0(1)	以前，网络对象组只能包含所有 IPv4 地址或所有 IPv6 地址。现在，网络对象组可以同时包含 IPv4 和 IPv6 地址。 注释 不能使用混合对象组进行 NAT。
用于按 ICMP 代码过滤 ICMP 流量的扩展 ACL 和对象增强	9.0(1)	现在可以根据 ICMP 代码允许/拒绝 ICMP 流量。 引入或修改了以下菜单项： Configuration > Firewall > Objects > Service Objects/Groups; Configuration > Firewall > Access Rule

功能名称	平台版本	说明
流控制传输协议 (SCTP) 的服务对象支持	9.5(2)	现在可以创建服务对象和组合特定 SCTP 端口。 在配置 > 防火墙 > 对象 > 服务对象/组页面上修改了服务对象和组的添加/编辑对话框。



第 4 章

访问控制列表

访问控制列表 (ACL) 在许多不同的功能中使用。作为访问规则应用到接口或全局应用时，这些列表可允许或拒绝通过设备的流量。对于其他功能，ACL 可选择功能所适用的流量，执行匹配服务而非控制服务。

以下各节介绍 ACL 的基本信息以及如何配置和监控 ACL。[访问规则](#)，第 11 页中将更加详细地介绍访问规则、全局应用或应用到接口的 ACL。

- [关于 ACL](#)，第 39 页
- [访问控制列表的许可](#)，第 43 页
- [ACL 指南](#)，第 43 页
- [配置 ACL](#)，第 44 页
- [监控 ACL](#)，第 52 页
- [ACL 的历史](#)，第 52 页

关于 ACL

访问控制列表 (ACL) 通过一个或多个特征识别流量，包括源和目标 IP 地址、IP 协议、端口、EtherType 及其他参数，视 ACL 类型而定。ACL 可用于各种功能。ACL 由一个或多个访问控制条目 (ACE) 组成。

ACL 类型

ASA 使用以下类型的 ACL：

- **扩展 ACL** - 扩展 ACL 是您将使用的主要类型。这些 ACL 用于访问规则以允许和拒绝通过设备的流量，并在许多功能中用于流量匹配，包括服务策略、AAA 规则、WCCP、僵尸网络流量过滤器、VPN 组和 DAP 策略。在 ASDM 中，这些功能大部分都有各自的规则页面，并且无法使用您在 ACL 管理器中定义的扩展 ACL，但 ACL 管理器将显示在这些页面上创建的 ACL。请参阅[配置扩展 ACL](#)，第 45 页。
- **EtherType ACL** - EtherType ACL 仅适用于桥接组成员接口上的非 IP 第 2 层流量。可以使用这些规则，根据第 2 层数据包中的 EtherType 值允许或丢弃流量。通过 EtherType ACL，可以控制设备上的非 IP 流量。请参阅[配置 EtherType 规则](#)，第 23 页。

- Webytype ACL - Webytype ACL 用于过滤无客户端 SSL VPN 流量。这些 ACL 可基于 URL 或目标地址拒绝访问。请参阅[配置 Webytype ACL](#)，第 49 页。
- 标准 ACL - 标准 ACL 只能基于目标地址识别流量。使用这种 ACL 的功能较少：路由映射和 VPN 过滤器。由于 VPN 过滤器还允许扩展访问列表，限制将标准 ACL 用于路由映射。请参阅[配置标准 ACL](#)，第 48 页。

下表列出 ACL 的一些常见用途及使用的类型。

表 2: ACL 类型和常见用途

ACL 用途	ACL 类型	说明
控制 IP 流量的网络接入（路由和透明模式）	扩展	ASA 不允许任何流量从较低安全性接口传送到较高安全性接口，除非流量经扩展 ACL 显式许可。在路由模式下，必须使用 ACL 来允许桥接组成员接口与同一个桥接组外部接口之间的流量。 注释 要接入 ASA 接口执行管理访问，也无需允许主机 IP 地址的 ACL。只需根据一般操作配置指南配置管理访问即可。
识别 AAA 规则的流量	扩展	AAA 规则使用 ACL 识别流量。
为给定用户增强 IP 流量的网络接入控制	扩展，按用户从 AAA 服务器下载	可以配置 RADIUS 服务器来下载要应用于用户的动态 ACL，或者服务器可以发送 ASA 上已配置的 ACL 的名称。
VPN 访问和过滤	扩展 标准	用于远程访问和站点到站点 VPN 的组策略使用标准或扩展 ACL 进行过滤。远程访问 VPN 还将扩展 ACL 用于客户端防火墙配置和动态访问策略。
识别用于模块化策略框架的流量类映射的流量。	扩展	可使用 ACL 来识别类映射中的流量，该类映射用于支持模块化策略框架的功能。支持模块化策略框架的功能包括 TCP 和一般连接设置及检测。
对于桥接组成员接口，控制非 IP 流量的网络接入	EtherType	可配置 ACL，以便基于属于桥接组成员的任何接口的 EtherType 来控制流量。
识别路由过滤和重分布	标准 扩展	各种路由协议将标准 ACL 用于 IPv4 地址（扩展 ACL 用于 IPv6 地址）的路由过滤和重分布（通过路由映射）。
无客户端 SSL VPN 过滤	Webytype	可以配置 Webytype ACL 以过滤 URL 和目标。

ACL 管理器

ACL 管理器有两种显示方式：

- 例如，在主窗口中依次选择 **Configuration > Firewall > Advanced > ACL Manager**。在这种情况下，ACL 管理器仅显示扩展 ACL。此类 ACL 包括您在 Access Rules、Service Policy Rules 和 AAA Rules 页面创建的规则所生成的 ACL。请注意，在 ACL 管理器中进行的编辑不会对这些规则造成负面影响；在此处进行的更改将在其他页面上反映。
- 在要求 ACL 的策略上，通过点击字段旁边的 **Manage** 按钮显示。在这种情况下，ACL 管理器可以为标准 ACL 和扩展 ACL 提供单独的选项卡，前提是策略允许任一类型的 ACL。否则，视图将被过滤为仅显示标准、扩展或 Webtype ACL。ACL 管理器绝不会显示 EtherType ACL。

标准 ACL 和 Webtype ACL 具有单独的页面，因此，可以在主窗口中配置这些 ACL。这些页面在功能上相当于不含名称的 ACL 管理器：

- 标准 ACL - **Configuration > Firewall > Advanced > Standard ACL**。
- Webtype ACL - **Configuration > Remote Access VPN > Clientless SSL VPN Access > Advanced > Web ACLs**。

ACL 名称

每个 ACL 都有一个名称或数字 ID，如 `outside_in`、`OUTSIDE_IN` 或 `101`。名称限于不超过 241 个字符。请考虑全部使用大写字母，以便在查看运行配置时更方便地查找名称。

制定一个可帮助您识别 ACL 的预期用途的命名约定。例如，ASDM 使用约定 `interface-name_purpose_direction`，如 `“outside_access_in”`，用于在入站方向应用于“外部”接口的 ACL。

一般来说，ACL ID 为数字。标准 ACL 的范围曾为 1 - 99 或 1300 - 1999。扩展 ACL 的范围曾为 100-199 或 2000-2699。ASA 不会执行这些范围，但若使用编号，您可能希望遵循这些规则，以便与运行 IOS 软件的路由器保持一致。

访问控制条目顺序

ACL 由一个或多个 ACE 组成。除非明确将 ACE 插入给定行，否则为给定 ACL 名称输入的所有 ACE 都将附加到 ACL 的末尾。

ACE 的顺序非常重要。当 ASA 决定转发数据包还是丢包时，ASA 会按条目的列出顺序对照每个 ACE 检测数据包。找到匹配项后，不再检查更多 ACE。

因此，如果将一条更具体的规则放在一条更通用的规则之后，则该更具体的规则可能永远不会被命中。例如，如果要允许网络 `10.1.1.0/24`，但要丢弃该子网上来自主机 `10.1.1.15` 的流量，则拒绝 `10.1.1.15` 的 ACE 必须排在允许 `10.1.1.0/24` 的 ACE 之前。如果允许 `10.1.1.0/24` 的 ACE 排在前面，则将允许 `10.1.1.15`，并且用以拒绝的 ACE 将永远不会被匹配。

根据需要，使用 Up 和 Down 按钮重新排列规则。

允许/拒绝与匹配/不匹配

访问控制条目“允许”或“拒绝”与规则匹配的流量。向用来决定允许流量通过 ASA 还是将其丢弃的功能应用 ACL（例如全局和接口访问规则）时，“允许”和“拒绝”是名副其实的“允许”和“拒绝”。

对于其他功能（例如服务策略规则），“允许”和“拒绝”实际上表示“匹配”或“不匹配”。在这些情况下，ACL 选择的是应接收该功能服务的流量，例如，应用检查或重定向到服务模块。“被拒绝的”流量即为不匹配 ACL 的流量，因而将不会接收该服务。（例如，在 ASDM 中，服务策略规则实际上使用“匹配/不匹配”，AAA 规则使用“验证/不验证”，但在 CLI 中，始终是“允许/拒绝”。）

访问控制隐式拒绝

用于通过型访问规则的 ACL 在末尾有隐式拒绝语句。因此，对于那些应用于接口的流量控制 ACL，如果未明确允许某个类型的流量，则该流量将被丢弃。例如，如果除一个或多个特定地址以外，要允许所有用户通过 ASA 访问网络，则需要拒绝这些特定地址，再允许所有其他地址。

对于控制传入流量的管理（控制平面）ACL，接口的管理规则集末尾没有隐式拒绝。而是由正则访问控制规则对任何未匹配管理访问规则的连接进行评估。

对于用于为某项服务选择流量的 ACL，必须明确“允许”流量；对于该服务，任何未“被允许的”流量都不会被匹配接受服务；“被拒绝的”流量将绕过该服务。

对于 EtherType ACL，ACL 末尾处的隐式拒绝不会影响 IP 流量或 ARP 流量；例如，如果您允许 EtherType 8037，则 ACL 末尾处的隐式拒绝此时将不阻止您先前使用扩展 ACL 允许的任何 IP 流量（或者隐式允许的从较高安全性接口流向较低安全性接口的 IP 流量）。但是，如果通过 EtherType ACE 明确拒绝所有流量，则 IP 和 ARP 流量将被拒绝；仅仍然允许物理协议流量，如自动协商。

使用 NAT 时用于扩展 ACL 的 IP 地址

使用 NAT 或 PAT 时，您将转换地址或端口，通常是在内部和外部地址之间进行映射。如果需要创建适用于已转换的地址或端口的扩展 ACL，则需要确定是要使用实际（未转换）地址或端口，还是要使用已映射地址或端口。具体要求因功能而异。

使用实际地址和端口意味着，如果 NAT 配置更改，则无需更改 ACL。

使用实际 IP 地址的功能

以下命令和功能可以在 ACL 中使用实际 IP 地址，即使接口上所示的地址是映射地址：

- 访问规则（由 **access-group** 命令引用的扩展 ACL）
- 服务策略规则（模块化策略框架 **match access-list** 命令）
- 僵尸网络流量过滤器流量分类（**dynamic-filter enable classify-list** 命令）
- AAA 规则（**aaa ... match** 命令）
- WCCP（**wccp redirect-list group-list** 命令）

例如，如果已为内部服务器 (10.1.1.5) 配置 NAT，以使该服务器在外部拥有公共可路由的 IP 地址 209.165.201.5，则用于允许外部流量访问内部服务器的访问规则需要引用该服务器的真实 IP 地址 (10.1.1.5)，而非映射地址 (209.165.201.5)。

使用映射的 IP 地址的功能

以下功能使用 ACL，但是这些 ACL 使用接口上可见的映射值：

- IPsec ACL
- `capture` 命令 ACL
- 每用户 ACL
- 路由协议 ACL
- 所有其他功能 ACL。

基于时间的 ACE

可以将时间范围对象应用到扩展 ACE 和 Webtype ACE，以便规则仅在特定期限内处于活动状态。通过这些类型的规则，可以区分在一天中某些时间点可接受但在其他时间点不可接受的活动。例如，可以在工作时间内提供附加限制，而在下班后或在午餐时间则不限制。相反，基本上可以在非工作时间关闭网络。

您无法创建具有完全相同的协议、源、目标的基于时间的规则，以及不包含时间范围对象的规则服务条件。非基于时间的规则始终会覆盖重复的基于时间的规则，因为它们是冗余。



注释 用户可能会在指定结束时间后遇到约 80 至 100 秒的延迟，以使 ACL 处于非活动状态。例如，如果指定的结束时间是 3:50，因为结束时间包含在内，所以将在 3:51:00 与 3:51:59 之间的任何时间点选取命令。选取命令后，ASA 将完成当前正在运行的所有任务，然后使用该命令来停用 ACL。

访问控制列表的许可

访问控制列表不需要特殊许可证。

但是，要使用 `sctp` 作为条目中的协议，必须拥有运营商许可证。

ACL 指南

防火墙模式

- 扩展 ACL 和标准 ACL 均支持路由和透明防火墙模式。

- Webtype ACL 仅支持路由模式。
- EtherType ACL 仅支持路由和透明模式下的桥接组成员接口。

故障切换和集群

配置会话未在故障切换或集群设备间同步。在会话中进行更改时，将在故障切换和集群设备中正常地进行更改。

IPv6

- 扩展 ACL 和 Webtype ACL 允许 IPv4 和 IPv6 地址混合使用。
- 标准 ACL 不允许 IPv6 地址。
- EtherType ACL 不包含 IP 地址。

其他指导原则

- 指定网络掩码时，方法与思科 IOS 软件 **access-list** 命令不同。ASA 使用网络掩码（例如使用 255.255.255.0 作为 C 类掩码）。思科 IOS 掩码使用通配符位（例如 0.0.0.255）。
- 通常情况下，无法引用在 ACL 或对象组中不存在的对象或对象组，或删除当前被引用的对象或对象组。也无法引用在 **access-group** 命令中不存在的 ACL（以应用访问规则）。但是，可以更改此默认行为，以便可在创建对象或 ACL 之前进行“向前引用”。在创建对象或 ACL 之前，任何引用它们的规则或访问组都将被忽略。要启用向前引用，请选择访问规则高级设置中的选项；依次选择 **Configuration > Access Rules**，然后点击 **Advanced** 按钮。
- 如果在源地址或目标地址或者源服务或目标服务中输入不止一个项目，ASDM 将使用前缀 DM_INLINE 为其自动创建对象组。在规则表视图中，这些对象会自动扩展至其组件部分，但如果在 **Tools > Preferences** 中取消选择 **Auto-expand network and service objects with specified prefix** 规则表首选项，可以看到对象名称。
- （仅限扩展 ACL）以下功能使用 ACL，但无法接受带有身份防火墙（指定用户或组名称）、FQDN（完全限定域名）或思科 TrustSec 值的 ACL：
 - VPN **crypto map** 命令
 - VPN **group-policy** 命令，**vpn-filter** 除外
 - WCCP
 - DAP

配置 ACL

以下各节介绍如何配置各种类型的通用 ACL，用作访问规则（包括 EtherType）、服务策略规则、AAA 规则和其他用途（其中 ASDM 为基于规则的策略提供专用页面）的 ACL 除外。

配置扩展 ACL

扩展 ACL 被表示为 ACE 的命名容器。要创建新的 ACL，必须先创建一个容器。之后，可以添加 ACE，编辑现有 ACE 并使用 ACL 管理器中的表将 ACE 重新排序。

扩展 ACL 可以同时包含 IPv4 和 IPv6 地址。

过程

步骤 1 依次选择 **Configuration > Firewall > Advanced > ACL Manager**。

步骤 2 如果要创建新的 ACL，请依次选择 **添加 > 添加 ACL**，并填写名称，然后点击 **确定**。

ACL 容器将被添加到表中。可以稍后对 ACL 容器重命名，只需选择该容器并点击 **Edit** 即可。

步骤 3 执行以下任一操作：

- 要将 ACE 添加到 ACL 末尾，请选择 ACL 名称或其中的任意 ACE 并依次选择 **Add > Add ACE**。
- 要将 ACE 插入特定位置，请选择现有的 ACE 并依次选择 **Add > Insert**，以将 ACE 添加到规则上方，或依次选择 **Add > Insert After**。
- 要编辑规则，请选择规则并点击 **Edit**。

步骤 4 填写 ACE 属性。可选择的主要选项如下：

- **Action: Permit/Deny** - 是否允许（选择）或拒绝（取消选择，不匹配）所述流量。
- **Source/Destination criteria** - 源（原始地址）和目标（流量的目标地址）的定义。通常要配置主机或子网的 IPv4 或 IPv6 地址，可以使用网络或网络对象组进行表示。还可以为源指定用户或用户组名称。此外，如果要限制规则在比所有 IP 流量更窄的范围，则可以使用 Service 字段识别特定类型的流量。如果实施思科 TrustSec，则可以使用安全组定义源和目标。

有关所有可用选项的详细信息，请参阅[扩展 ACE 属性，第 45 页](#)。

ACE 定义完成后，请点击 **OK**，将规则添加到表中。

步骤 5 点击 **Apply**。

扩展 ACE 属性

将 ACE 添加到扩展 ACL 或进行编辑时，可以配置以下属性。在很多字段中，可以点击编辑方框右侧的“...”按钮，选择、创建或编辑字段可用的对象。

Action: Permit/Deny

允许（选择）还是拒绝（取消选择、不匹配）所述的流量。

源条件

尝试匹配的流量的始发器特征。必须配置 Source，但其他属性可选。

来源

源的 IPv4 或 IPv6 地址。默认值为 **any**，该值会匹配所有 IPv4 或 IPv6 地址；可以使用 **any4** 以只将 IPv4 作为目标，或使用 **any6** 以只将 IPv6 作为目标。可指定单个主机地址（如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）、子网（采用 0.100.10.0/24 或 10.100.10.0/255.255.255.0 格式，或者对于 IPv6，采用 2001:DB8:0:CD30::/60 格式）、网络对象或网络对象组的名称，或者接口的名称。

用户

如果启用身份防火墙，可以指定用户或用户组作为流量源。用户当前使用的 IP 地址将匹配规则。可以指定用户名 (DOMAIN\user)、用户组 (DOMAIN\group，注意 \ 表示组名称) 或用户对象组。对于此字段，点击“...”，从 AAA 服务器组中选择名称比直接键入名称更方便。

Security Group

如果启用思科 Trustsec，可以指定安全组名称或标记 (1-65533) 或安全组对象。

More Options > Source Service

如果指定 TCP、UDP 或 SCTP 作为目标服务，可以选择性地为 TCP、UDP、TCP-UDP 或 SCTP 指定预定义的服务对象，或者使用自己的对象。通常，只需定义目标服务，而无需定义源服务。请注意，如果定义源服务，则目标服务协议必须与其匹配（例如，带或不带端口定义的 TCP）。

目标条件

尝试匹配的流量的目标特征。必须配置 Destination，但其他属性可选。

目标

目标的 IPv4 或 IPv6 地址。默认值为 **any**，该值会匹配所有 IPv4 或 IPv6 地址；可以使用 **any4** 以只将 IPv4 作为目标，或使用 **any6** 以只将 IPv6 作为目标。可指定单个主机地址（如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）、子网（采用 0.100.10.0/24 或 10.100.10.0/255.255.255.0 格式，或者对于 IPv6，采用 2001:DB8:0:CD30::/60 格式）、网络对象或网络对象组的名称，或者接口的名称。

Security Group

如果启用思科 Trustsec，可以指定安全组名称或标记 (1-65533) 或安全组对象。

服务

流量的协议（例如 IP、TCP、UDP）以及 TCP、UDP 或 SCTP 的可选端口。默认值为 IP，但可以选择更具体的协议以将更精细的流量作为目标。通常，可以选择某些类型的服务对象。对于 TCP、UDP 和 SCTP，可以指定端口，例如 tcp/80、tcp/http、tcp/10-20（用于端口范围）、tcp-udp/80（匹配端口 80 上的任意 TCP 或 UDP 流量）、sctp/diameter 等等。有关指定服务的详细信息，请参阅[扩展 ACE 中的服务规范](#)，第 47 页。

说明

ACE 的用途说明，每行最多 100 个字符。可以输入多行；每一行将作为备注添加到 CLI 中，并且备注放在 ACE 之前。



注释 如果将含非英文字符的备注添加到一个平台（如 Windows）上，然后尝试从另一个平台（如 Linux）将这些备注删除，则可能无法编辑或删除这些备注，因为原特征可能无法被正确识别。此限制由底层平台依赖性所导致，其以不同方式对不同语言进行编码。

Enable Logging; Logging Level; More Options > Logging Interval

日志记录选项定义如何为规则生成系统日志消息。这些选项仅适用于被用作访问规则的 ACL，即连接到接口或全局应用的 ACL。对于用于其他功能的 ACL，这些选项将被忽略。可以实施以下日志记录选项：

取消选择 **Enable Logging**

此操作将为规则禁用日志记录。对于匹配此规则的连接，不会发出任何类型的系统日志消息。

选择 **Enable Logging**，设置 **Logging Level = Default**

此操作为规则提供默认日志记录。对于每个被拒绝的连接发出系统日志消息 106023。如果设备受到攻击，发出此消息的频率可能会影响服务。

选择 **Enable Logging**，使用非默认日志记录级别

此操作提供一条汇总系统日志消息 106100，而不是 106023。在第一次命中后，系统将发出消息 106100，然后在 **More Options > Logging Interval** 中配置的每个间隔（默认值为每隔 300 秒，可以指定 1 - 600 秒）后再次发出消息，显示在间隔过程中的命中次数。建议的日志记录级别为 **Informational**。

汇总拒绝消息可以减少攻击的影响，并且有可能方便您分析消息。如果受到拒绝服务攻击，则可能会看到消息 106101，表示用于为消息 106100 生成命中次数的缓存拒绝流的数量已超过某个间隔内的最大值。此时，设备将在下一个间隔前停止收集统计信息以减轻攻击。

More Options > Enable Rule

规则在设备上是否处于活动状态。已禁用的规则在规则表中显示为带删除线的文本。禁用规则可以让您在不删除规则的情况下停止将其应用到流量，以便可以在以后需要时重新启用。

More Options > Time Range

定义规则应在一周中的哪几天以及一天中的哪些时段处于活动状态的时间范围对象的名称。如果不指定时间范围，规则将始终处于活动状态。

扩展 ACE 中的服务规范

对于扩展 ACE 中的目标服务，可以指定以下任一条件。选项都相似，但对于源服务，具有更多的限制，即限于 TCP、UDP、TCP-UDP 或 SCTP 条件。

对象名称

任何类型的服务对象或服务对象组的名称。这些对象可以包含以下所述的大部分规格，您可以轻松地在 ACL 中重用服务定义。存在许多预定义的对象，因此，您也许可以找到所需的对象，而无需手动键入规格或创建对象。

协议

介于 1-255 之间的数字或已知名称（例如 **ip**、**tcp**、**udp**、**gre** 等）。

TCP、UDP、TCP-UDP、SCTP 端口

可以在 **tcp**、**udp**、**tcp-udp** 和 **sctp** 关键字中包括端口规格。可以通过 **tcp-udp** 关键字同时为两个协议定义端口，而不必单独指定。可以使用以下方法指定端口：

- 单个端口 - **tcp/80**、**udp/80**、**tcp-udp/80**、**sctp/3868** 或已知服务名称，如 **tcp/www**、**udp/snmp** 或 **sctp/diameter**。
- 端口范围 - **tcp/1-100**、**udp/1-100**、**tcp-udp/1-100**、**sctp/1-100**，匹配端口 1-100（含）。
- 不等于端口号 - 将 **!=** 添加到规格的开头，例如，**!=tcp/80** 表示匹配任意 TCP 流量，TCP 端口 80 (HTTP) 除外。
- 小于端口号 - 添加 **<**，例如，**<tcp/150** 表示匹配任何端口号小于 150 的 TCP 流量。
- 大于端口号 - 添加 **>**，例如，**>tcp150** 表示匹配任何端口号大于 150 的 TCP 流量。



注释 DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC 和 Talk 都需要一个对 TCP 的定义和一个对 UDP 的定义。TACACS+ 需要一个对 TCP 上的端口 49 的定义。

ICMP、ICMP6 消息

可以将特定消息（例如 ping 回应请求和应答消息）甚至消息代码作为目标。存在许多涵盖 ICMP（适用于 IPv4）和 ICMP6（适用于 IPv6）的预定义对象，因此也许不需要手动定义标准。格式如下：

icmp/*icmp_message_type*[/*icmp_message_code*]

icmp6/*icmp6_message_type*[/*icmp6_message_code*]

其中消息类型为 1-255 或已知名称，代码为 0-255。确保选择的数字与实际类型/代码相匹配，否则 ACE 将永远不会被匹配。

配置标准 ACL

标准 ACL 用 ACE 的命名容器表示。要创建新的 ACL，必须先创建一个容器。之后，可以添加 ACE，编辑现有 ACE 并使用标准 ACL 表对 ACE 重新排序。如果在配置使用 ACL 的策略的同时配置 ACL，该表格可以在 ACL 管理器中显示为一个选项卡，在这种情况下，除了到达窗口的方式不同外，操作步骤基本相同。

标准 ACL 仅使用 IPv4 地址，并且仅定义目标地址。

过程

步骤 1 依次选择 **Configuration > Firewall > Advanced > Standard ACL**。

步骤 2 如果要创建新的 ACL，请依次选择添加 > 添加 ACL，并填写名称，然后点击确定。

ACL 容器将被添加到表中。无法重命名标准 ACL。

步骤 3 执行以下任一操作：

- 要将 ACE 添加到 ACL 末尾，请选择 ACL 名称或其中的任意 ACE 并依次选择 **Add > Add ACE**。
- 要将 ACE 插入特定位置，请选择现有的 ACE 并依次选择 **Add > Insert**，以将 ACE 添加到规则上方，或依次选择 **Add > Insert After**。
- 要编辑规则，请选择规则并点击 **Edit**。

步骤 4 填写 ACE 属性。选项有：

- **Action: Permit/Deny** - 是否允许（选择）或拒绝（取消选择，不匹配）所述流量。
- **Address** - 定义流量的目标地址。可以指定主机地址（如 10.100.1.1）、网络（10.100.1.0/24 或 10.100.1.0/255.255.255.0 格式），或可以选择网络对象（只需将对象的内容加载到 Address 字段即可）。
- **Description** - ACE 用途的说明，每行最多 100 个字符。可以输入多行；每一行将作为备注添加到 CLI 中，并且备注放在 ACE 之前。

注释 如果将含非英文字符的备注添加到一个平台（如 Windows）上，然后尝试从另一个平台（如 Linux）将这些备注删除，则可能无法编辑或删除这些备注，因为原特征可能无法被正确识别。此限制由底层平台依赖性所导致，其以不同方式对不同语言进行编码。

ACE 定义完成后，请点击 **OK**，将规则添加到表中。

步骤 5 点击应用。

配置 Webtype ACL

Webtype ACL 用于过滤无客户端 SSL VPN 流量，限制用户对特定网络、子网、主机和 Web 服务器的访问。如果不定义过滤器，将允许所有连接。Webtype ACL 用 ACE 的命名容器表示。要创建新的 ACL，必须先创建一个容器。之后，可以添加 ACE，编辑现有 ACE 并使用 Web ACL 表对 ACE 重新排序。如果在配置使用 Webtype ACL 的策略的同时配置 Webtype ACL，该表格可以显示为 ACL 管理器，在这种情况下，除了到达窗口的方式不同外，操作步骤基本相同。

除了 URL 规格之外，Webtype ACL 可以同时包含 IPv4 和 IPv6 地址。

过程

步骤 1 依次选择配置 > 远程接入 VPN > 无客户端 SSL VPN 接入 > 高级 > Web > ACL。

步骤 2 如果要创建新的 ACL，请依次选择添加 > 添加 ACL，并填写名称，然后点击确定。

ACL 容器将被添加到表中。可以稍后对 ACL 容器重命名，只需选择该容器并点击 **Edit** 即可。

步骤 3 执行以下任一操作：

- 要将 ACE 添加到 ACL 末尾，请选择 ACL 名称或其中的任意 ACE 并依次选择 **Add > Add ACE**。
- 要将 ACE 插入特定位置，请选择现有的 ACE 并依次选择 **Add > Insert**，以将 ACE 添加到规则上方，或依次选择 **Add > Insert After**。
- 要编辑规则，请选择规则并点击 **Edit**。

步骤 4 填写 ACE 属性。可选择的主要选项如下：

- **Action: Permit/Deny** - 是否允许（选择）或拒绝（取消选择，不匹配）所述流量。
- **Filter** - 基于目标的流量匹配条件。可以通过选择协议并输入服务器名称和路径及文件名（后面两者可选）来指定 URL，或可以指定目标 IPv4 或 IPv6 地址和 TCP 服务。

有关所有可用选项的详细信息，请参阅 [Webtype ACE 属性，第 50 页](#)。

ACE 定义完成后，请点击 **OK**，将规则添加到表中。

步骤 5 点击 **Apply**。

Webtype ACE 属性

将 ACE 添加到 Webtype ACL 或进行编辑时，可以配置以下属性。在很多字段中，可以点击编辑方框右侧的“...”按钮，选择、创建或编辑字段可用的对象。

对于给定的 ACE，可以基于 URL 或 Address 进行过滤，但不能同时基于两者进行过滤。

- **Action: Permit/Deny** - 是否允许（选择）或拒绝（取消选择，不匹配）所述流量。
- **Filter on URL** - 基于目标 URL 匹配流量。选择协议并输入服务器名称和路径和文件名（后面两者可选）。例如，`http://www.example.com`，或者要涵盖所有服务器，请输入 `http://*.example.com`。以下是指定 URL 时的一些提示和限制：
 - 选择 **any** 与所有 URL 匹配。
 - “Permit url any” 会允许具有格式 `protocol://server-ip/path` 的所有 URL，并会阻止与此模式不匹配的流量，例如端口转发。应该有一个 ACE 允许连接至所需端口（如果是 Citrix，为端口 1494），从而避免发生隐式拒绝。
 - 具有“permit url any”的 ACL 不影响智能隧道和 ICA 插件，因为它们仅与 `smart-tunnel://` 和 `ica://` 类型匹配。
 - 可以使用这些协议：`cifs://`、`citrix://`、`citrixs://`、`ftp://`、`http://`、`https://`、`imap4://`、`nfs://`、`pop3://`、`smart-tunnel://` 和 `smtp://`。也可以在协议中使用通配符；例如，`htt*` 与 `http` 和 `https` 匹配，星号（*）与所有协议匹配。例如，`*://*.example.com` 与传输到 `example.com` 网络的基于 URL 的任何类型的流量匹配。
 - 如果指定 `smart-tunnel://URL`，则可以仅包括服务器名称。URL 无法包含路径。例如，`smart-tunnel://www.example.com` 可接受，但是不接受 `smart-tunnel://www.example.com/index.html`。

- 星号 (*) 与零个字符或任何数量的字符匹配。要与任何 http URL 匹配，请输入 `http://*/*`。
 - 问号 (?) 完全匹配任意字符。
 - 方括号 ([]) 是范围运算符，与范围中的任何字符匹配。例如，要与 `http://www.cisco.com:80/` 和 `http://www.cisco.com:81/` 匹配，请输入 `http://www.cisco.com:8[01]/`。
- **Filter on Address and Service** - 基于目标地址和服务匹配流量。
 - **Address** - 目标的 IPv4 或 IPv6 地址。要匹配所有地址，可以使用 **any**，将匹配所有 IPv4 或 IPv6 地址；使用 **any4** 仅匹配 IPv4，或使用 **any6** 仅匹配 IPv6。可以指定单个主机地址（如 10.100.10.5 或 2001:DB8::0DB8:800:200C:417A）、子网（10.100.10.0/24 或 10.100.10.0/255.255.255.0 格式，或对于 IPv6 为 2001:DB8:0:CD30::/60 格式），或选择网络对象，该网络对象将使用对象内容填写字段。
 - **Service** - 一种 TCP 服务规格。默认为无端口的 **tcp**，但可以指定单个端口（如 `tcp/80` 或 `tcp/www`）或端口范围（如 `tcp/1-100`）。可以包含运算符；例如，`!=tcp/80` 排除端口 80；`<tcp/80` 是端口号小于 80 的所有端口；`>tcp/80` 是端口号大于 80 的所有端口。
 - **Enable Logging; Logging Level; More Options > Logging Interval** - 日志记录选项定义如何为实际拒绝流量的规则生成系统日志消息。可以实施以下日志记录选项：
 - **Deselect Enable Logging** - 这将禁用规则的日志记录。系统将不会为该规则所拒绝的流量发出任何类型的系统日志消息。
 - **Select Enable Logging with Logging Level = Default** - 这将为规则提供默认的日志记录。系统将为每个被拒绝的数据包发布系统日志消息 106103。如果设备受到攻击，发出此消息的频率可能会影响服务。
 - **Select Enable Logging with Non-Default Logging Level** - 提供一条汇总系统日志消息 106102，而非 106103。在第一次命中后，系统将发出消息 106102，然后在 **More Options > Logging Interval** 中配置的每个间隔（默认值为每隔 300 秒，可以指定 1-600 秒）后再次发出消息，显示在间隔过程中的命中次数。建议的日志记录级别为 **Informational**。
 - **More Options > Time Range** - 时间范围对象的名称，该对象定义在一周的哪些天、一天的哪些时间该规则应处于活动状态。如果不指定时间范围，规则将始终处于活动状态。

Webtype ACL 的示例

以下是一些用于 Webtype ACL 的基于 URL 的规则示例。

	过滤	效果
拒绝	<code>url http://*.yahoo.com/</code>	拒绝访问所有 Yahoo!
拒绝	<code>url cifs://fileserver/share/directory</code>	拒绝访问指定位置中的所有文件。

	过滤	效果
拒绝	url https://www.example.com/ directory/file.html	拒绝访问指定文件。
允许	url https://www.example.com/directory	允许访问指定位置。
拒绝	url http://*:8080/	拒绝通过端口 8080 以 HTTPS 方式访问任何位置。
拒绝	url http://10.10.10.10	拒绝以 HTTPS 方式访问 10.10.10.10。
允许	url any	允许访问任意 URL。通常用于拒绝 URL 访问的 ACL 之后。

监控 ACL

ACL 管理器、标准 ACL、Web ACL 和 EtherType ACL 表格可以显示 ACL 的合并视图。但要准确了解设备上的配置，请使用以下命令。依次选择 **Tools > Command Line Interface**，输入命令。

- **show access-list [name]** - 显示访问列表，包括每个 ACE 的行号和匹配数。纳入 ACL 名称，否则将看到所有访问列表。
- **show running-config access-list [name]** - 显示当前运行的访问列表配置。纳入 ACL 名称，否则将看到所有访问列表。

ACL 的历史

功能名称	版本	说明
扩展 ACL、标准 ACL、Webtype ACL	7.0(1)	将 ACL 用于控制网络接入或指定供许多功能操作的流量。扩展访问控制列表用于通过设备的访问控制和其他几种功能。标准 ACL 用于路由映射和 VPN 过滤器。Webtype ACL 用于无客户端 SSL VPN 过滤。EtherType ACL 控制第 2 层非 IP 流量。 添加了 ACL 管理器和其他页面，用于配置 ACL。
扩展 ACL 中的实际 IP 地址	8.3(1)	使用 NAT 或 PAT 时，对于几种功能，ACL 中不再使用映射地址和端口。必须为这些功能使用实际、未转换的地址和端口。使用实际地址和端口意味着，如果 NAT 配置更改，则无需更改 ACL。
支持在扩展 ACL 中使用身份防火墙	8.4(2)	现在可以将身份防火墙用户和组用于源和目标。可以将身份防火墙 ACL 与访问规则、AAA 规则配合使用，并可将其用于 VPN 身份验证。

功能名称	版本	说明
IS-IS 流量的 EtherType ACL 支持	8.4(5)、9.1(2)	在透明防火墙模式下，ASA 现在可使用 EtherType ACL 控制 IS-IS 流量。 修改了以下屏幕：Configuration > Device Management > Management Access > EtherType Rules。
支持在扩展 ACL 中使用思科 TrustSec	9.0(1)	现在可以将思科 TrustSec 安全组用于源和目标。可以将身份防火墙 ACL 与访问规则配合使用。
为 IPv4 和 IPv6 统一扩展 ACL 和 Webtype ACL	9.0(1)	扩展 ACL 和 Webtype ACL 现在支持 IPv4 和 IPv6 地址。甚至可以为源和目标同时指定 IPv4 和 IPv6 地址。更改了 any 关键字以表示 IPv4 和 IPv6 流量。添加了 any4 和 any6 关键字以分别表示纯 IPv4 和纯 IPv6 流量。特定于 IPv6 的 ACL 已弃用。现有 IPv6 ACL 已迁移到扩展 ACL。有关迁移的详细信息，请参阅版本说明。 修改了以下菜单项： Configuration > Firewall > Access Rules Configuration > Remote Access VPN > Network (Client) Access > Group Policies > General > More Options
用于按 ICMP 代码过滤 ICMP 流量的扩展 ACL 和对对象增强	9.0(1)	现在可以根据 ICMP 代码允许/拒绝 ICMP 流量。 引入或修改了以下菜单项： Configuration > Firewall > Objects > Service Objects/Groups Configuration > Firewall > Access Rule
用于编辑 ACL 和对象的配置会话。向前引用访问规则中的对象和 ACL。	9.3(2)	现在，可以在单独的配置会话中编辑 ACL 和对象。还可以向前引用对象和 ACL，也就是说，可以为尚未存在的对象或 ACL 配置规则和访问组。 修改了访问规则的 Advanced 设置。
流控制传输协议 (SCTP) 的 ACL 支持	9.5(2)	现在，您可以使用 sctp 协议（包括端口规范）创建 ACL 规则。 在 Configuration > Firewall > Advanced > ACL Manager 页面上修改了访问控制条目的添加/编辑对话框。
对 IEEE 802.2 逻辑链路控制数据包的目标服务无线接入点地址的 Ethertype 规则支持。	9.6(2)	现在，您可以为 IEEE 802.2 逻辑链路控制数据包的目标服务访问点地址编写 Ethertype 访问控制规则。添加此支持后， bpdu 关键字与预期流量不再匹配。我们重写了 dsap 0x42 的 bpdu 规则。 修改了以下菜单项：配置 > 防火墙 > EtherType 规则。

功能名称	版本	说明
在路由模式下，桥接组成员接口上支持 EtherType 规则，桥接组虚拟接口 (BVI) 上支持扩展访问规则。	9.7(1)	<p>现在，您可以创建 EtherType ACL，并在路由模式下将它们应用于桥接组成员接口。除成员接口之外，您还可以向桥接虚拟接口 (BVI) 应用扩展访问规则。</p> <p>修改了以下屏幕：Configuration > Firewall > Access Rules、Configuration > Firewall > EtherType Rules。</p>
EtherType 访问控制列表更改。	9.9(1)	<p>EtherType 访问控制列表现在支持以太网 II IPX (EII IPX)。此外，在 DSAP 关键字中增加了新关键字，以支持通用 DSAP 值：BPDU (0x42)、IPX (0xE0)、Raw IPX (0xFF) 和 ISIS (0xFE)。因此，现有的使用 BPDU 或 ISIS 关键字的 EtherType 访问控制条目将被自动转换为使用 DSAP 规范，并且 IPX 的规则将被转换为 3 条规则 (DSAP IPX、DSAP Raw IPX 和 EII IPX)。此外，使用 IPX 作为 EtherType 值的数据包捕获已被弃用，因为 IPX 对应于 3 个单独的 EtherType。</p> <p>修改了以下菜单项：配置 > 防火墙 > EtherType 规则。</p>



第 5 章

身份防火墙

本章介绍如何为身份防火墙配置 ASA。

- [关于身份防火墙，第 55 页](#)
- [身份防火墙指南，第 61 页](#)
- [身份防火墙的前提条件，第 63 页](#)
- [配置身份防火墙，第 64 页](#)
- [监控身份防火墙，第 70 页](#)
- [身份防火墙的历史，第 70 页](#)

关于身份防火墙

在企业中，用户通常需要访问一个或多个服务器资源。通常，防火墙不知道用户的身份，因此也就无法基于身份应用安全策略。要配置每个用户的访问策略，则您必须配置用户身份验证代理，其要求用户交互（用户名/密码查询）。

ASA 中的身份防火墙可基于用户身份提供更加精细的访问控制。可以基于用户名和用户组名，而不是通过源 IP 地址配置访问规则和安全策略。ASA 会基于 IP 地址与 Windows Active Directory 登录信息的关联应用安全策略，并基于映射的用户名（而不是网络 IP 地址）报告事件。

身份防火墙与提供实际身份映射的外部 Active Directory (AD) 代理配合，与 Microsoft Active Directory 相集成。ASA 以 Windows Active Directory 为源来检索特定 IP 地址的当前用户身份信息，并允许对 Active Directory 用户透明地进行身份验证。

通过允许指定用户或组来代替源 IP 地址，基于身份的身份防火墙服务增强现有访问控制和安全策略机制。基于身份的安全策略可以交错，无传统的基于 IP 地址的规则之间的限制。

身份防火墙的主要优点包括：

- 将网络拓扑从安全策略解耦
- 简化安全策略创建
- 能够轻松识别用户在网络资源上的活动
- 简化用户活动监控

身份防火墙部署的架构

身份防火墙与提供实际身份映射的外部 Active Directory (AD) 代理配合，与 Window Active Directory 相集成。

身份防火墙由三个组件组成：

- ASA
- Microsoft Active Directory

虽然 Active Directory 在 ASA 中是身份防火墙的一部分，但 Active Directory 管理员仍可对其进行管理。数据可靠性和准确性取决于 Active Directory 中的数据。

支持的版本包括 Windows Server 2003、Windows Server 2008 和 Windows Server 2008 R2 服务器。

- Active Directory (AD) 代理

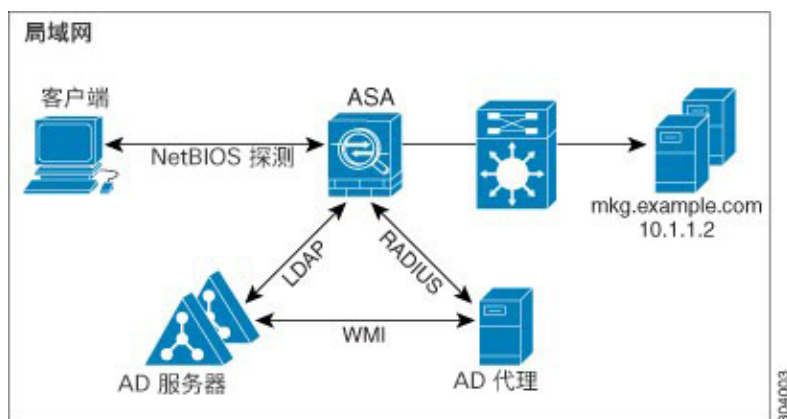
AD 代理在 Windows 服务器上运行。支持的 Windows 服务器包括 Windows 2003、Windows 2008 和 Windows 2008 R2。



注释 对于 AD 代理服务器来说，不支持 Windows 2003 R2。

下图显示身份防火墙的组件。随后的表格介绍这些组件的角色，以及它们如何互相通信。

图 3: 身份防火墙组件



1	<p>在 ASA 上：管理员配置本地用户组和身份防火墙策略。</p>	4	<p>客户端 <-> ASA：客户端通过 Microsoft Active Directory 登录网络。AD 服务器对用户进行身份验证并生成用户登录安全日志。</p> <p>或者，客户端可以通过直接转发代理或 VPN 登录网络。</p>
2	<p>ASA <-> AD 服务器：ASA 为 AD 服务器中配置的 Active Directory 组发送 LDAP 查询。</p> <p>ASA 会整合本地与 Active Directory 组，并基于用户身份应用访问规则和模块化策略框架安全策略。</p>	5	<p>ASA <-> 客户端：根据 ASA 上配置的策略，允许或拒绝访问客户端。</p> <p>如果配置此项，ASA 将探测客户端的 NetBIOS 来传送不活动和未响应的用户。</p>
3	<p>ASA <-> AD 代理：根据身份防火墙配置，ASA 将下载 IP-用户数据库或向寻求用户 IP 地址的 AD 代理发送 RADIUS 请求。</p> <p>ASA 会将通过 Web 身份验证和 VPN 会话获悉的新映射条目转发到 AD 代理。</p>	6	<p>AD 代理 <-> AD 服务器：AD 代理维护用户 ID 和 IP 地址映射条目的缓存，并通知 ASA 它们的变更情况。</p> <p>AD 代理向系统日志服务器发送日志。</p>

身份防火墙的功能

身份防火墙包括以下主要功能。

灵活性

- 通过查询每个新 IP 地址的 AD 代理或维护完整用户身份和 IP 地址数据库的本地副本，ASA 可从 AD 代理中检索用户身份和 IP 地址映射。
- 支持用户身份策略目标的主机组、子网或 IP 地址。
- 支持用户身份策略源和目标的完全限定域名 (FQDN)。
- 支持基于 ID 策略的五元组策略组合。基于身份的功能与现有五元组解决方案配套使用。

- 支持使用 IPS 和应用检查策略。
- 从远程访问 VPN、AnyConnect VPN、L2TP VPN 和直接转发代理检索用户身份信息。检索到的所有用户会被填入连接到 AD 代理的所有 ASA。

可扩展性

- 每个 AD 代理都支持 100 ASA。多个 ASA 可以与单一 AD 代理通信，以便在较大规模的网络部署中提供扩展性。
- 假如 IP 地址在所有域中保持唯一，则支持 30 个 Active Directory 服务器。
- 在域中的每个用户身份可以包含多达 8 个 IP 地址。
- ASA 5500 系列型号的活动策略中最多支持 64,000 个用户身份-IP 地址映射条目。此限制控制了策略的用户最大数量。用户总数是在所有不同情景中配置的所有用户合计数量。
- 活动 ASA 策略最多支持 512 个用户组。
- 单个访问规则可以包含一个或多个用户组或用户。
- 支持多个域。

可用性

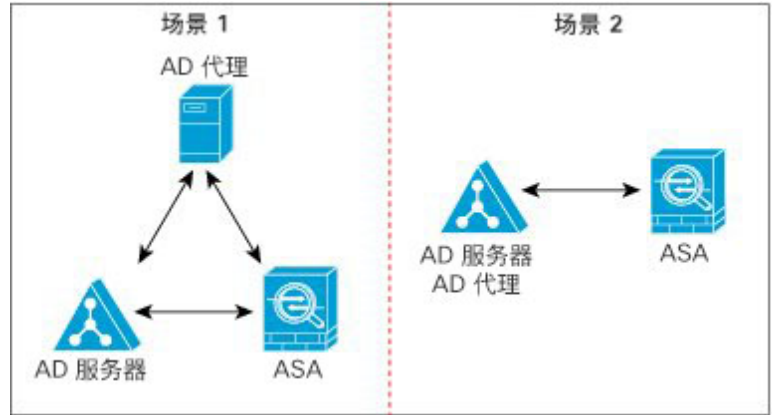
- 当 AD 代理无法将源 IP 地址映射到用户身份时，ASA 将从 Active Directory 检索组信息，并回退到对 IP 地址执行 Web 身份验证。
- 如有任何 Active Directory 服务器或 ASA 未响应，AD 代理将继续工作。
- 支持在 ASA 上配置主 AD 代理和辅助 AD 代理。如果主 AD 代理停止响应，ASA 可切换到辅助 AD 代理。
- 如果 AD 代理不可用，ASA 可回退到现有身份源，例如直接转发代理和 VPN 身份验证。
- AD 代理运行监视器进程，在服务关闭时自动重新启动服务。
- 允许在 ASA 之间使用分布式 IP 地址/用户映射数据库。

部署方案

根据环境要求，您能够以下列方式部署身份防火墙组件。

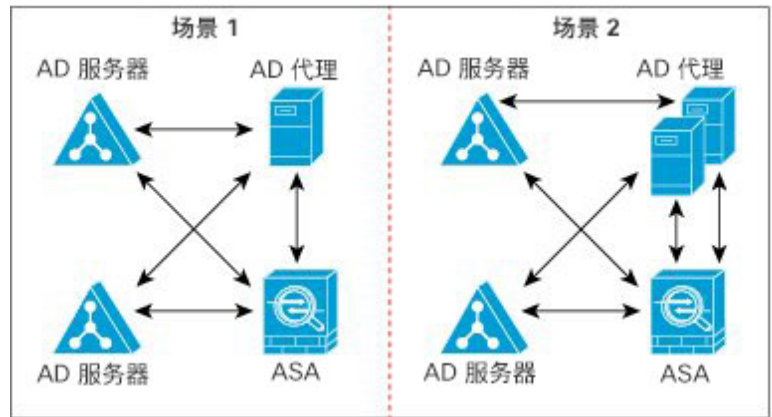
下图显示如何部署身份防火墙组件以允许冗余。方案 1 显示无组件冗余的简单安装。方案 2 也显示无冗余的简单安装。但是，在此部署方案中，Active Directory 服务器和 AD 代理共同位于同一 Windows 服务器上。

图 4: 无冗余部署方案



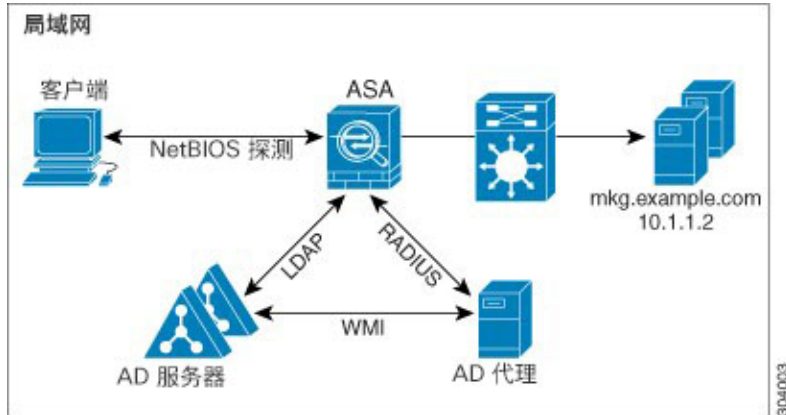
下图显示可以如何部署身份防火墙组件以支持冗余。方案 1 显示一种部署，其中有多于一个 Active Directory 服务器和单个安装在单独 Windows 服务器上的 AD 代理。方案 2 显示一个部署，其中有多于一个 Active Directory 服务器和多个安装在单独 Windows 服务器上的 AD 代理。

图 5: 具有冗余组件的部署方案



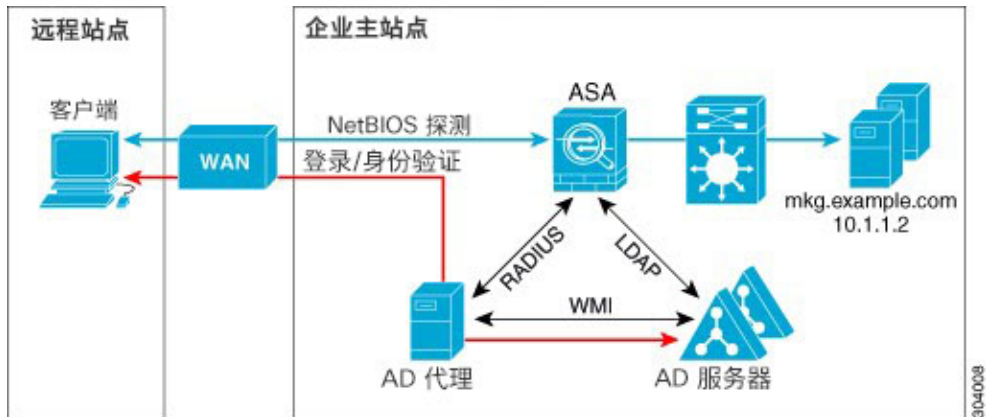
下图显示所有身份防火墙组件（Active Directory 服务器、AD 代理和客户端）如何进行安装以及如何在局域网上进行通信。

图 6: 基于 LAN 的部署



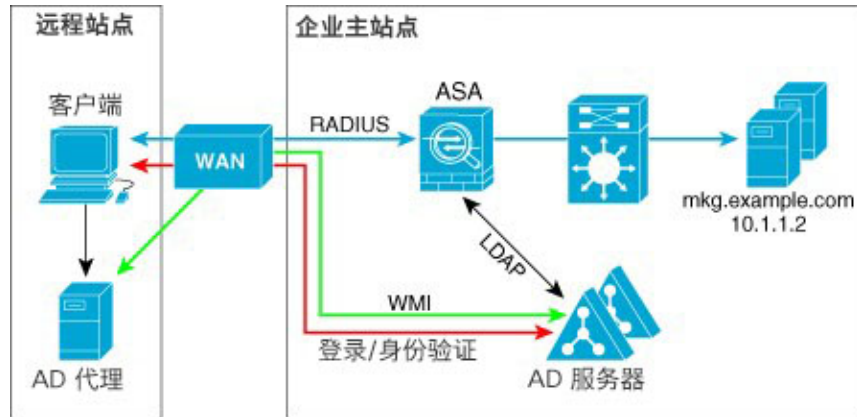
下图显示用于支持远程站点的基于广域网的部署。Active Directory 服务器和 AD 代理安装在主站点局域网中。客户端位于远程站点，并通过广域网连接至身份防火墙组件。

图 7: 基于广域网的部署



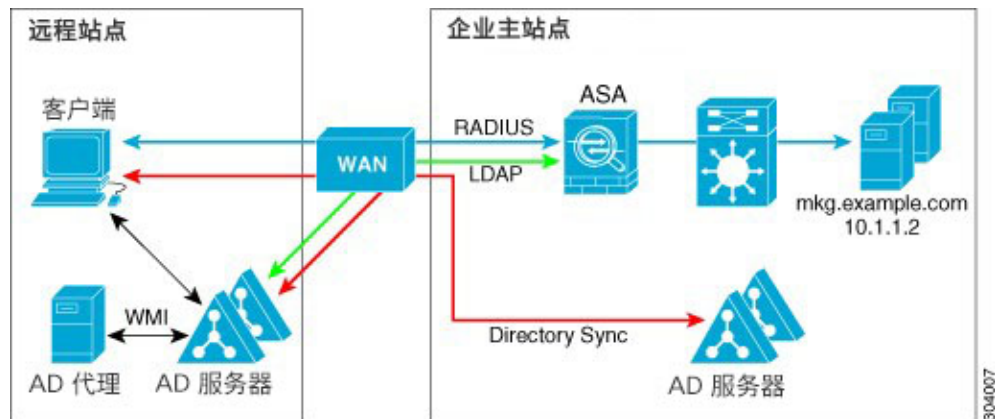
下图也显示用于支持远程站点的基于广域网的部署。Active Directory 服务器安装在主站点局域网中。但是，AD 代理通过远程站点的客户端进行安装和访问。远程客户端通过广域网连接至主站点的 Active Directory 服务器。

图 8: 具有远程 AD 代理的基于广域网的部署



下图显示扩展的远程站点安装。AD 代理和 Active Directory 服务器安装在远程站点。客户端登录位于主站点的网络资源时，在本地访问这些组件。远程 Active Directory 服务器必须与位于主站点的中央 Active Directory 服务器同步其数据。

图 9: 具有远程 AD 代理和 AD 服务器的基于广域网的部署



身份防火墙指南

本节介绍在配置身份防火墙之前应检查的指导原则和限制。

故障切换

- 当启用状态故障切换时，身份防火墙支持从主用设备到备用设备的用户身份-IP 地址映射和 AD 代理状态复制。但是，仅复制用户身份-IP 地址映射、AD 代理状态和域状态。不会将用户和用户组记录复制到备用 ASA。
- 在配置故障切换时，还必须将备用 ASA 配置为直接连接到 AD 代理，以便检索用户组。备用 ASA 不会向客户端发送 NetBIOS 数据包，即便已为身份防火墙配置了 NetBIOS 探测选项。

- 当活动 ASA 确定某个客户端未处于活动状态后，会将信息传送到备用 ASA。不会向备用 ASA 传送用户统计信息。
- 如果已配置故障切换，则必须配置 AD 代理，才能与活动 ASA 和备用 ASA 通信。有关在 AD 代理服务器上配置 ASA 的步骤，请参阅 *Active Directory* 代理安装和设置指南。

IPv6

- AD 代理支持具有 IPv6 地址的终端。它可以接收日志事件中的 IPv6 地址，将其置于缓存中，并通过 RADIUS 消息进行发送。AAA 服务器必须使用 IPv4 地址。
- 不支持 NetBIOS over IPv6。

其他指导原则

- 不支持将完整 URL 用作目标地址。
- 要执行 NetBIOS 探测功能，ASA、AD 代理和客户端之间的网络必须支持 UDP 封装 NetBIOS 流量。
- 当存在干预路由器时，身份防火墙的 MAC 地址检查不起作用。登录同一路由器之后的客户端的用户具有相同的 MAC 地址。实施这些设置后，来自同一路由器的所有数据包均可通过检查，因为 ASA 无法确定路由器之后的实际 MAC 地址。
- 虽然可以在 VPN 过滤器 ACL 中使用用户说明，但基于用户的规则解释是单向的，而并非像 VPN 过滤器一样通常是双向运行的。也就是说，您可以基于用户发起的流量过滤，但过滤器不适用于从目标返回用户的流量。例如，您可以包括一项规则，允许特定用户 ping 连接服务器，但该规则将不允许服务器 ping 连接用户。
- 以下 ASA 功能不支持在扩展 ACL 中使用基于身份的对象和 FQDN：
 - 加密映射
 - WCCP
 - NAT
 - 组策略（除 VPN 过滤器外）
 - DAP
- 可以使用 **user-identity update active-user-database** 命令主动从 AD 代理发起用户-IP 地址下载。根据设计，如果以前的下载会话已完成，ASA 将不允许再次发出此命令。因此，如果用户-IP 数据库非常庞大，以前的下载会话尚未完成，而您又发出了一个 **user-identity update active-user-database** 命令，系统将显示以下错误消息：

“ERROR: one update active-user-database is already in progress.”

您需要等待以前的会话彻底完成后，才能发出其他 **user-identity update active-user-database** 命令。

此行为另一个示例的发生是由于从 AD 代理到 ASA 的数据包丢失。

在发出 **user-identity update active-user-database** 命令时，ASA 会请求提供要下载的用户-IP 映射条目总数。然后，AD 代理发起与 ASA 的 UDP 连接，并发送授权请求数据包的更改信息。

如果由于某种原因导致数据包丢失，ASA 也就无法识别这一点。因此，如果已发出了 **user-identity update active-user-database** 命令，ASA 将使该会话保持 4-5 分钟，在该段时间内系统会不断显示此错误消息。

- 将思科 Context Directory Agent (CDA) 与 ASA 或思科 Ironport 网络安全设备 (WSA) 协同使用时，请确保打开以下端口：
 - UDP 身份验证端口 - 1645
 - UDP 记账端口 - 1646
 - UDP 侦听端口 - 3799侦听端口用于将来自 CDA 的授权变更请求发送到 ASA 或 WSA。
- 如果配置了 **user-identity action domain-controller-down domain_name disable user-identity-rule** 命令且指定的域关闭，或者配置了 **user-identity action ad-agent-down disable user-identity-rule** 命令且 AD 代理关闭，则所有已登录用户都会处于被禁用状态。
- 对于域名，以下字符无效：\:*?"<>|。
- 对于用户名，以下字符无效：\[]:;=,+*?"<>|@。
- 对于用户组名，以下字符无效：\[]:;=,+*?"<>|。
- 如何配置身份防火墙以从 AD 代理检索用户信息会影响功能所使用的内存量。指定 ASA 使用按需检索还是完全下载检索。选择按需检索的优点是使用较少的内存，因为只查询和存储接收的数据包的用户。

身份防火墙的前提条件

本节列出配置身份防火墙的必备条件。

AD 代理

- 必须在可访问 ASA 的 Windows 服务器上安装 AD 代理。此外，必须将 AD 代理配置为从 Active Directory 服务器获取信息并可与 ASA 通信。
- 支持的 Windows 服务器包括 Windows 2003、Windows 2008 和 Windows 2008 R2。



注释 对于 AD 代理服务器来说，不支持 Windows 2003 R2。

- 关于安装和配置 AD 代理的步骤，请参阅《Active Directory 代理安装和设置指南》。
- 在 ASA 中配置 AD 代理前，获取 AD 代理和 ASA 用于通信的密钥值。AD 代理和 ASA 中的此值必须匹配。

Microsoft Active Directory

- Microsoft Active Directory 必须安装在 Windows 服务器上，并且可供 ASA 访问。支持的版本包括 Windows 2003、2008 和 2008 R2 服务器。
- 在 ASA 中配置 Active Directory 服务器之前，请在 Active Directory 中为 ASA 创建一个用户账户。
- 此外，ASA 会使用通过 LDAP 启用的 SSL 向 Active Directory 服务器发送加密的登录信息。在 Active Directory 服务器上必须启用 SSL。有关如何启用 Active Directory 的 SSL，请参阅 Microsoft Active Directory 的文档。



注释 在运行 AD 代理安装程序之前，必须在 AD 代理监控的每个 Microsoft Active Directory 服务器上安装 *README First for the Cisco Active Directory Agent* 中列出的补丁。即使当 AD 代理直接安装在域控制器服务器上时，这些补丁也是必需的。

配置身份防火墙

要配置身份防火墙，请执行以下任务：

过程

- 步骤 1** 在 ASA 中配置 Active Directory 域。
- 步骤 2** 在 ASA 中配置 AD 代理。
- 步骤 3** 配置身份选项。
- 步骤 4** 配置基于身份的安全策略。在配置 AD 域和 AD 代理后，可以创建将用在许多功能中的基于身份的对象组和 ACL。

配置 Active Directory 域

在接收来自 AD 代理的 IP-用户映射时，需要在 ASA 上配置 Active Directory，ASA 才能下载 Active Directory 组并接受来自特定域的用户身份。

开始之前

- Active Directory 服务器 IP 地址
 - LDAP 基础 DN 的可分辨名称
 - 身份防火墙用于连接 Active Directory 域控制器的 Active Directory 用户的可分辨名称和密码
- 要配置 Active Directory 域，请执行以下步骤：

过程

步骤 1 依次选择 **Configuration > Firewall > Identity Options**。

步骤 2 选中 **Enable User Identity** 复选框启用用户身份。

步骤 3 点击 **Add**。

系统将显示 **Domain** 对话框。

步骤 4 输入最多 32 个字符的域名，可包含 [a-z]、[A-Z]、[0-9]、[!@#%&()-_+[]{};,.]，第一个字符不能是 “.” 和 “ ”。如果域名包含空格，则必须用引号将该空格字符引起来。域名不区分大小写。

在编辑现有域名时，与现有用户和用户组相关的域名不会更改。

步骤 5 选择与该域相关联的 Active Directory 服务器，或点击 **Manage** 以将新服务器组添加到列表中。

步骤 6 点击 **OK** 保存域设置并关闭该对话框。

配置 Active Directory 服务器组

要配置 Active Directory 服务器组，请执行以下步骤：

过程

步骤 1 依次选择 **Configuration > Firewall > Identity Options > Add > Manage**。

系统将显示 **Configure Active Directory Server Groups** 对话框。

步骤 2 点击 **Add**。

系统将显示 **Add Active Directory Server Group** 对话框。

步骤 3 要将服务器添加到 Active Directory 服务器组，请从 **Active Directory Server Groups** 列表中选择该组，然后点击 **Add**。

系统将显示 **Add Active Directory Server** 对话框。

步骤 4 点击 **OK** 保存设置并关闭该对话框。

配置 Active Directory 代理

开始之前

- AD 代理 IP 地址
- ASA 与 AD 代理之间的共享密钥

要配置 AD 代理，请执行以下步骤：

过程

步骤 1 依次选择 **Configuration > Firewall > Identity Options**。

步骤 2 选中 **Enable User Identity** 复选框启用此功能。

步骤 3 在 **Active Directory Agent** 部分，点击 **Manage**。

系统显示 **Configure Active Directory Agents** 对话框。

步骤 4 点击 **Add** 按钮。

步骤 5 点击 **OK** 保存更改并关闭该对话框。

配置 Active Directory 代理组

配置 AD 代理服务器组的主 AD 代理和辅助 AD 代理。如果 ASA 检测到主 AD 代理未响应并指定了辅助代理，则 ASA 会切换到辅助 AD 代理。AD 代理的 Active Directory 服务器使用 RADIUS 作为通信协议；因此，应为 ASA 与 AD 代理之间的共享密钥指定一个 key 属性。

要配置 AD 代理组，请执行以下步骤：

过程

步骤 1 从 **Configure Active Directory Agents** 对话框，点击 **Add**。

系统将显示 **Add Active Directory Agent Group** 对话框。

步骤 2 输入 AD 代理组名称。

步骤 3 指定 ASA 用来侦听来自 AD 代理服务器的流量的接口，并在 **Primary Active Directory Agent** 部分输入服务器的 FQDN 或 IP 地址。

步骤 4 在 **Primary Active Directory Agent** 部分输入超时时间以及 AD 代理未响应时，ASA 尝试继续联系 AD 代理的重试间隔。

步骤 5 输入主 AD 代理与 ASA 之间使用的共享密钥。

步骤 6 指定 ASA 用来侦听来自 AD 代理服务器的流量的接口，并在 **Secondary Active Directory Agent** 部分输入服务器的 FQDN 或 IP 地址。

- 步骤 7** 在 **Secondary Active Directory Agent** 部分输入超时间隔以及 AD 代理未响应时，ASA 将执行尝试以继续联系 AD 代理的重试间隔。
- 步骤 8** 输入辅助 AD 代理与 ASA 之间使用的共享密钥。
- 步骤 9** 点击 **OK** 保存更改并关闭该对话框。

配置身份选项

要配置身份防火墙的身份选项，请执行以下步骤：

过程

- 步骤 1** 依次选择 **Configuration > Firewall > Identity Options**。
- 步骤 2** 选中 **Enable User Identity** 复选框。
- 步骤 3** 要为身份防火墙添加一个域，请点击 **Add** 以显示 **Add Domain** 对话框。
- 步骤 4** 对于已添加到 **Domains** 列表中的域，选中当域因为 Active Directory 域控制器未响应而关闭时是否禁用规则。
- 当域关闭且为该域选中了此选项时，ASA 将禁用与该域中用户关联的用户身份规则。另外，**监控 > 属性 > 身份 > 用户** 窗格中会将该域所有用户 IP 地址的状态标记为已禁用。
- 步骤 5** 选择身份防火墙的默认域。
- 当没有为所有用户或用户组明确配置域时，所有用户和用户组都使用默认域。未指定默认域时，用户和组的默认域为 LOCAL。
- 此外，身份防火墙为所有本地定义的用户组或本地定义的用户（通过使用 VPN 或网络门户登录和进行身份验证的用户）使用 LOCAL 域。
- 注释** 选择的默认域名必须与在 Active Directory 域控制器上配置的 NetBIOS 域名相匹配。如果域名不匹配，在配置 ASA 时，AD 代理会误将用户-IP 映射与您输入的域名关联。要查看 NetBIOS 域名，请在任意文本编辑器中打开 Active Directory 用户事件安全日志。
- 对于多情景模式，可以为每个情景以及在系统执行空间中设置一个默认域名。
- 步骤 6** 从下拉列表中选择 AD 代理组。点击 **Manage** 添加 AD 代理组。
- 步骤 7** 在 **Hello Timer** 字段中输入一个 10 至 65535 秒之间的数值。
- ASA 与 AD 代理之间的问候计时器定义 ASA 交换问候数据包的频率。ASA 使用问候数据包以获得 ASA 复制状态（同步或不同步）和域状态（运行或关闭）。如果 ASA 没有收到来自 AD 代理的响应，它会在指定间隔后重新发送问候数据包。
- 指定 ASA 会继续向 AD 代理发送问候数据包的次数。默认情况下，秒数设置为 30 秒，重试次数设置为 5 次。
- 步骤 8** 选中 **Enable Event Timestamp** 复选框启用 ASA，可跟踪其对于每个标识符接收的最后事件时间戳，如果事件时间戳至少比 ASA 时钟早 5 分钟或其时间戳早于最后事件的时间戳，则丢弃任何消息。

对于新启动的不了解最后事件时间戳的ASA，ASA会对比事件时间戳与自己的时钟。如果该事件已过去至少5分钟，ASA则不接受该消息。

我们建议您使用NTP配置ASA、Active Directory和Active Directory代理，使它们的时钟彼此同步。

- 步骤 9** 在ASA用于查询DNS服务以解析完全限定域名(FQDN)的**Poll Group Timer**字段中输入小时数。默认情况下，轮询计时器设置为4小时。
- 步骤 10** 在**Retrieve User Information**部分，从列表中选择相应选项：
- **On Demand** - 指定ASA在收到需要新连接的数据包且其源IP地址的用户不在用户身份数据库中时，从AD代理检索该IP地址的用户映射信息。
 - **Full Download** - 指定ASA在启动时向AD代理发送请求以下载完整的IP-用户映射表，然后在用户登录和注销时接收递增的IP-用户映射。
- 注释 选择**On Demand**的优点是使用较少的内存，因为只查询和存储接收到的数据包的用户。
- 步骤 11** 选择在AD代理未响应时是否禁用规则。
- 当AD代理关闭且选择了此选项时，ASA将禁用与该域中用户关联的用户身份规则。另外，**监控 > 属性 > 身份 > 用户**窗格中会将该域所有用户IP地址的状态标记为已禁用。
- 步骤 12** 选择当NetBIOS探测失败时是否删除用户的IP地址。
- 选择此选项可指定当到用户的NetBIOS探测阻塞（例如，用户客户端不响应NetBIOS探测）时的操作。该客户端的网络连接可能已被阻止或客户端处于不活动状态。当选择此选项时，ASA将禁用与该用户的IP地址关联的身份规则。
- 步骤 13** 选择当用户的MAC地址与ASA当前映射到该MAC地址的IP地址不一致时是否删除该MAC地址。当选择此选项时，ASA将禁用与该特定用户关联的用户身份规则。
- 步骤 14** 选择是否跟踪未发现的用户。
- 步骤 15** 选择**Idle Timeout**选项并输入一个时间（以分钟为单位，范围从1到65535分钟）。默认情况下，空闲超时设置为60分钟。
- 启用此选项将在活动用户被视为空闲时配置一个计时器，这意味着ASA未收到来自该用户IP地址的流量的时间已超过指定时间。当计时器过期后，该用户的IP地址将被标记为不活动并从本地缓存的IP-用户数据库中删除，而且ASA不再通知AD代理该IP地址的情况。现有的流量仍允许通过。启用**Idle Timeout**选项时，即便已配置NetBIOS注销探测，ASA仍会运行不活动的计时器。
- 注释 **Idle Timeout**选项不适用于VPN或直接转发代理用户。
- 步骤 16** 启用NetBIOS探测并设置探测到用户IP地址前的探测计时器（1到65535分钟）和重试探测之间的重试间隔（1到256次重试）。
- 启用此选项可配置ASA为了确定用户客户端是否仍处于活动状态而探测用户主机的频率。为了最大限度地减少NetBIOS数据包，ASA仅在用户的空闲时间超出**Idle Timeout minutes**字段中指定的分钟数时向客户端发送一次NetBIOS探测。
- 步骤 17** 从**User Name**列表选择相应选项：

- **Match Any** - 只要来自主机的 NetBIOS 响应包含分配到 IP 地址的用户的用户名，用户身份就被视为有效。指定此选项要求主机启用 Messenger 服务并配置 WINS 服务器。
- **Exact Match** - 分配到 IP 地址的用户的用户名在 NetBIOS 响应中必须唯一。否则，该 IP 地址的用户身份将被视为无效。指定此选项要求主机启用 Messenger 服务并配置 WINS 服务器。
- **User Not Needed** - 只要 ASA 收到来自主机的 NetBIOS 响应，用户身份就被视为有效。

步骤 18 点击 **Apply** 保存身份防火墙配置。

配置基于身份的安全策略

可以在许多 ASA 功能中加入基于身份的策略。任何使用扩展 ACL（除非在“指南”部分列为不支持）的功能都能够利用身份防火墙。现在，可以将用户身份参数添加到扩展 ACL 中，并添加基于网络的参数。

可以使用身份的功能包括以下内容：

- 访问规则 - 访问规则利用网络信息允许或拒绝接口上的流量。借助身份防火墙，可以基于用户身份控制访问。
- AAA 规则 - 身份验证规则（也称为直接转发代理）基于用户控制网络访问。由于此功能非常类似于访问规则加上身份防火墙，因此 AAA 规则现在可以用作用户 AD 登录超时情况下的身份验证备份方法。例如，对于无有效登录的任何用户，可以触发 AAA 规则。要确保 AAA 规则仅对无有效登录的用户触发，可以在用于访问规则和 AAA 规则的扩展 ACL 中指定特殊用户名：None（无有效登录的用户）和 Any（有有效登录的用户）。在访问规则中，请照常为用户和组配置策略，但是，包括允许所有 None 用户的 AAA 规则；必须允许这些用户，以便他们以后可以触发 AAA 规则。然后，配置拒绝 Any 用户的 AAA 规则（这些用户将不受 AAA 规则的限制，并已由访问规则处理），但是 AAA 规则允许所有 None 用户。例如：

```
access-list 100 ex permit ip user CISCO\xyz any any
access-list 100 ex deny ip user CISCO\abc any any
access-list 100 ex permit ip user NONE any any
access-list 100 ex deny any any
access-group 100 in interface inside

access-list 200 ex deny ip user ANY any any
access-list 200 ex permit user NONE any any
aaa authenticate match 200 inside user-identity
```

有关详细信息，请参阅旧版功能指南。

- 云网络安全 - 可以控制将哪些用户发送给云网络安全代理服务器。另外，可以在 Cloud Web Security ScanCenter 上配置基于发送给云网络安全的 ASA 流量信头中包含的用户组的策略。
- VPN 过滤器 - 虽然 VPN 通常不支持身份防火墙 ACL，但可以配置 ASA 来强制对 VPN 流量实施基于身份的访问规则。默认情况下，VPN 流量不受访问规则限制。可以强制 VPN 客户端遵守使用身份防火墙 ACL 的访问规则（使用 **no sysopt connection permit-vpn** 命令）。还可以使

用具有 VPN 过滤器功能的身份防火墙 ACL；VPN 过滤器一般通过允许访问规则实现相似的效果。

监控身份防火墙

如需监控身份防火墙状态，请参阅以下屏幕：

- **监控 > 属性 > 身份 > AD 代理**
此窗格显示 AD 代理和域的状态以及 AD 代理的统计信息。
- **监控 > 属性 > 身份 > 内存使用率**
此窗格显示身份防火墙在 ASA 上使用的内存量。
- **监控 > 属性 > 身份 > 用户**
此窗格显示身份防火墙使用的 IP 用户映射数据库中包含的所有用户的相关信息。
- **监控 > 属性 > 身份 > 组**
此窗格显示为身份防火墙配置的用户组列表。
- **工具 > 命令行界面**
您可以在此窗格中发出各种非交互式命令并查看结果。

身份防火墙的历史

表 3: 身份防火墙的历史

功能名称	版本	说明
身份防火墙	8.4(2)	引入了身份防火墙功能。 引入或修改了以下菜单项： 配置 > 防火墙 > 身份选项 配置 > 防火墙 > 对象 > 本地用户组 Monitoring > Properties > Identity。



第 6 章

ASA 和思科 TrustSec

本章介绍如何为 ASA 实施思科 TrustSec。

- [关于思科 TrustSec，第 71 页](#)
- [思科 TrustSec 指南，第 78 页](#)
- [将 ASA 配置为与思科 TrustSec 集成，第 81 页](#)
- [思科 TrustSec 的 AnyConnect VPN 支持，第 90 页](#)
- [监控 Cisco TrustSec，第 91 页](#)
- [思科 TrustSec 的历史，第 92 页](#)

关于思科 TrustSec

以往，防火墙等安全功能根据预定义的 IP 地址、子网和协议执行访问控制。然而，随着企业不断向无边界网络过渡，用于连接人员和组织的技术取得了长足的进步，同时对数据保护和网络安全的要求也显著提高。同时，终端变得越来越具流动性，而且用户通常利用各种终端（例如，笔记本电脑（而非台式机）、智能手机或平板电脑），这样用户属性结合终端属性一起提供了关键特征（除了现有的基于 6 元组的规则以外），带防火墙功能的交换机和路由器或专用防火墙等实施设备能够可靠地利用这些关键特征制定访问控制决策。

因此，对于支持跨客户网络、在网络的接入层、分发层和核心层以及在数据中心实现安全性，终端属性或客户端身份属性的可用性和传送性已经成为越来越重要的要求。

思科 TrustSec 可以提供基于现有的身份感知基础设施的访问控制，确保网络设备之间的数据保密性，并集成平台上的安全访问服务。在思科 TrustSec 功能中，实施设备结合用户属性和终端属性制定基于角色和基于身份的访问控制决策。此信息的可用性和传送性支持在网络的接入层、分发层和核心层实现跨网络安全性。

在环境中实施思科 TrustSec 具备以下优势：

- 提供不断增加的移动和复杂劳动力，他们能够从任何设备进行适当和更安全的访问。
- 针对正在连接有线或无线网络的人员和设备，提供全面的可视性，降低安全风险
- 针对访问物理或云计算型的 IT 资源的网络用户的活动提供优越控制
- 通过高度安全的集中式访问策略管理和可扩展策略实施机制来降低总拥有成本

- 有关详细信息，请访问以下 URL：

参考	说明
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html	介绍面向企业的 Cisco TrustSec 系统和架构。
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html	提供有关在企业中部署 Cisco TrustSec 解决方案的指导说明，包含组件设计指南的链接。
http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf	提供搭配 ASA、交换机、无线 LAN (WLAN) 控制器和路由器使用的思科 TrustSec 解决方案概述。
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html	提供 Cisco TrustSec 平台支持矩阵，其中列出支持 Cisco TrustSec 解决方案的思科产品。

关于思科 TrustSec 中的 SGT 和 SXP 支持

在 Cisco TrustSec 功能中，安全组访问可以将拓扑感知网络转换为基于角色的网络，支持在基于角色的访问控制 (RBAC) 的基础上实施端到端策略。在身份验证期间获得的设备和用户凭证用于按安全组对数据包进行分类。每个进入 Cisco TrustSec 云的数据包都被标记有安全组标记 (SGT)。这种标记有助于可信的中间设备确定数据包的源身份，沿着数据路径实施安全策略。当使用 SGT 定义安全组 ACL 时，SGT 可以指明域上的权限级别。

SGT 通过 IEEE 802.1X 身份验证、Web 身份验证或 MAC 身份验证绕行 (MAB) 分配到设备，被分配的同时带有 RADIUS 供应商特定属性。SGT 可以被静态地分配给特定 IP 地址或交换机接口。在成功进行身份验证之后，SGT 可以被动态地传送到交换机或访问点。

安全组交换协议 (SXP) 是一种为 Cisco TrustSec 开发的协议，用以在不具有（支持 SGT 的）硬件支持的网络设备上将 IP 到 SGT 的映射数据库传送到支持 SGT 和安全组 ACL 的硬件。SXP 为一种控制层面协议，可以将 IP-SGT 映射从身份验证点（例如，旧版接入层交换机）传送到网络中的上游设备。

SXP 连接为点到点的连接，使用 TCP 作为底层传输协议。SXP 使用众所周知的 TCP 端口号 64999 发起连接。此外，SXP 连接唯一可通过源 IP 地址和目标 IP 地址被标识。

思科 TrustSec 功能中的角色

为了提供基于身份和策略的访问实施，思科 TrustSec 功能包含以下角色：

- 访问请求者 (AR) - 访问请求者指的是请求访问网络中受保护资源的终端设备。它们是架构的主要主体，其访问权限视身份凭证而定。

访问请求者包括终端设备，例如计算机、笔记本电脑、移动电话、打印机、摄像机和支持 MACsec 功能的 IP 电话。

- 策略决定点 (PDP) - 策略决定点负责制定访问控制决策。PDP 可以提供 802.1x、MAB 和 Web 身份验证等功能。PDP 通过 VLAN、DAACL 和安全组访问 (SGACL/SXP/SGT) 支持身份验证和实施。

在思科 TrustSec 功能中，思科身份服务引擎 (ISE) 可充当 PDP。思科 ISE 提供身份和访问控制策略功能。

- 策略信息点 (PIP) - 策略信息点是向策略决策点提供外部信息（例如，信誉、位置和 LDAP 属性）的源。

策略信息点包括 Session Directory、Sensor IPS 和通信管理器等设备。

- 策略管理点 (PAP) - 策略管理点定义策略并将策略插入授权系统。PAP 提供思科 TrustSec 标记到用户身份映射和思科 TrustSec 标记到服务器资源映射，充当一个身份资源库。

在思科 TrustSec 功能中，思科安全访问控制系统（带集成式 802.1x 和 SGT 支持的策略服务器）充当 PAP。

- 策略实施点 (PEP) - 策略实施点是实施 PDP 为每个 AR 制定的决策（策略规则和操作）的实体。PEP 设备通过网络上的主要通信路径获悉身份信息。PEP 设备从多个来源获悉每个 AR 的身份属性，例如终端代理、授权服务器、对等实施设备和网络流量。反过来，PEP 设备使用 SXP 将 IP-SGT 映射传送到网络上相互信任的对等设备。

策略实施点包括 Catalyst 交换机、路由器、防火墙（特别是 ASA）、服务器、VPN 设备和 SAN 设备等网络设备。

思科 ASA 在身份架构中充当 PEP 角色。使用 SXP，ASA 可直接从身份验证点获悉身份信息并使用它们来实施基于身份的策略。

安全组策略实施

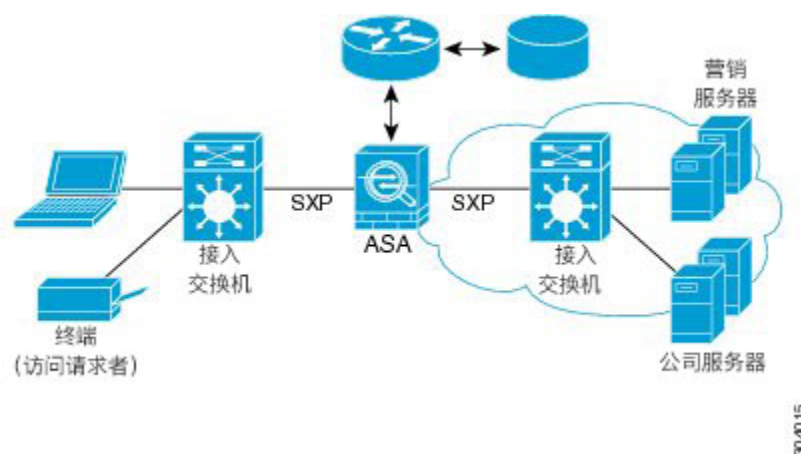
安全策略实施基于安全组名称进行。终端设备尝试访问数据中心中的资源。与在防火墙上配置的基于 IP 的传统策略相比，基于身份的策略基于用户和设备身份配置。例如，允许市场营销承包商访问市场营销服务器；允许市场营销公司用户访问市场营销服务器和公司服务器。

此类部署的优点包括：

- 使用单一对象 (SGT) 简化策略管理定义和实施用户组与资源。
- 在支持思科 TrustSec 的交换机基础设施中保留用户身份和资源身份。

下图显示基于安全组名称的策略实施的部署。

图 10: 基于安全组名称的策略实施部署



通过实施思科 TrustSec，可以配置支持服务器分类的安全策略，并且实现以下功能：

- 可以将 SGT 分配给服务器池，以简化策略管理。
- SGT 信息保留在支持思科 TrustSec 的交换机的基础设施中。
- ASA 可使用 IP-SGT 映射跨思科 TrustSec 域执行策略实施。
- 服务器强制要求 802.1x 授权，由此可能简化部署。

ASA 如何实施基于安全组的策略



注释 基于用户的安全策略和基于安全组的策略在 ASA 中可以共存。网络属性、基于用户的属性和基于安全组的属性的任意组合都能够在安全策略中配置。

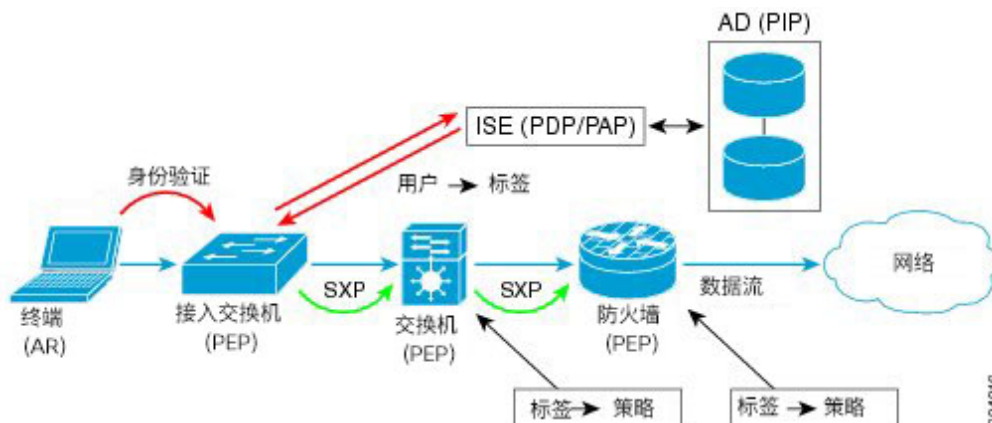
要将 ASA 配置为与思科 TrustSec 协同运行，必须从 ISE 导入受保护的访问凭证 (PAC) 文件。

将 PAC 文件导入到 ASA 会与 ISE 建立安全的通信通道。建立通道后，ASA 会使用 ISE 启动 PAC 安全 RADIUS 事务并下载思科 TrustSec 环境数据（即安全组表）。此安全组表将 SGT 映射到安全组名称。安全组名称在 ISE 上创建，为安全组提供用户友好的名称。

ASA 第一次下载安全组表时会浏览表中的所有条目，并解析在其中配置的安全策略中包含的所有安全组名称；然后，ASA 将在本地激活这些安全策略。如果 ASA 无法解析安全组名称，则会对未知安全组名称生成系统日志消息。

下图显示如何在 Cisco TrustSec 实施安全策略。

图 11: 安全策略实施



1. 终端设备直接或通过远程访问连接到接入层设备，并使用思科 TrustSec 进行身份验证。
2. 通过使用 802.1X 或 Web 身份验证等身份验证方法，接入层设备可以利用 ISE 对终端设备进行身份验证。终端设备传送角色和组成员信息，将此设备划分至相应的安全组。
3. 接入层设备使用 SXP，将 IP-SGT 映射传送到上游设备。
4. ASA 接收数据包并使用 SXP 传送的 IP-SGT 映射查询源与目标 IP 地址的 SGT。

如果该映射为新映射，ASA 将在其本地 IP-SGT 管理器数据库中记录该映射。IP-SGT 管理器数据库在控制层面中运行，为每个 IPv4 或 IPv6 地址跟踪 IP-SGT 映射。此数据库记录映射被获悉的源。SXP 连接的对等 IP 地址可用作映射源。每个 IP-SGT 映射条目都可以有多个源。

如果 ASA 被配置为发言者，ASA 会将所有 IP-SGT 映射条目传输到其 SXP 对等体。

5. 如果在 ASA 上配置了包含 SGT 或安全组名称的安全策略，ASA 将实施该策略。（您可以在 ASA 上创建包含 SGT 或安全组名称的安全策略。要基于安全组名称实施策略，ASA 需要使用安全组表将安全组名称映射到 SGT。）

如果 ASA 在安全组表中找不到安全组名称，但安全策略中包含安全组名称，ASA 会将安全组名称视为未知并生成一条系统日志消息。在 ASA 从 ISE 刷新安全组表并获得安全组名称后，ASA 将生成一条系统日志消息，指示安全组名称已知。

更改 ISE 上安全组的效果

ASA 通过从 ISE 下载更新表定期刷新安全组表。在不同的下载之间，ISE 上的安全组会发生更改。在刷新安全组表之前，ASA 中不会反映这些更改。



提示

我们建议您在维护时段安排在 ISE 上进行策略配置更改，然后手动刷新 ASA 上的安全组表，以确保执行安全组更改。

按这种方式处理策略配置更改，可以最大限度增加安全组名称获得解析和安全策略立即进入活动状态的几率。

当环境数据计时器过期时，系统会自动刷新安全组表。也可以按需触发安全组表刷新。

如果进行 ISE 中的安全组更改，当 ASA 刷新安全组表时会发生以下事件：

- 只有使用安全组名称配置的安全组策略才需要通过安全组表进行解析。包含安全组标记的策略始终处于活动状态。
- 当安全组表首次可用时，浏览所有包含安全组名称的策略，解析安全组名称，激活策略。浏览所有包含标记的策略，并为未知标记生成系统日志。
- 如果安全组表已过期，将继续根据最新下载的安全组表实施策略，直到您清楚或有新表变得可用为止。
- 当 ASA 上已解析的安全组名称变成未知时，安全策略将被禁用；不过，该安全策略仍然存在于 ASA 运行配置中。
- 如果在 PAP 上删除现有安全组，以前已知的安全组标记会变成未知，但在 ASA 上不会发生策略状态更改。以前已知的安全组名称会变成未解析，然后策略被停用。如果安全组名称被重用，则使用新标记重新编译策略。
- 如果在 PAP 上添加新安全组，以前未知的安全组标记会变成已知，会生成系统日志消息，但策略状态不会发生更改。以前未知的安全组名称变成已解析，然后相关联的策略被激活。
- 如果已在 PAP 上重命名标记，使用标记配置的策略会显示新的标记名称，策略状态不会发生更改。使用此新标记值重新编译使用安全组名称配置的策略。

ASA 中的发言者和收听者

ASA 支持通过 SXP 发送和接收进出其他网络设备的 IP-SGT 映射条目。SXP 允许安全设备和防火墙从访问交换机获悉身份信息，无需硬件升级或更改。SXP 还能够用来将上游设备（例如，数据中心设备）的 IP-SGT 映射条目重新传送到下游设备。ASA 可接受来自上游和下游方向的信息。

在 ASA 上配置 SXP 到 SXP 对等体的连接时，您必须将 ASA 指定为该连接的发言者或收听者，这样才能交换身份信息：

- 发言者模式 - 配置 ASA，使其可以将 ASA 中收集的所有活动 IP-SGT 映射条目转发到上游设备进行策略实施。
- 收听者模式 - 配置 ASA，使其可以接收来自下游设备（支持 SGT 的交换机）的 IP-SGT 映射条目，并可使用该信息创建策略定义。

如果将 SXP 连接的一端配置为说话者，必须将另一端配置为收听者，反之亦然。如果位于 SXP 连接两端的两个设备均配置为同一角色（同为发言者或同为收听者），则 SXP 连接失败，ASA 将生成一条系统日志消息。

多个 SXP 连接能够获悉已从 IP-SGT 映射数据库下载的 IP-SGT 映射条目。在 ASA 上建立 SXP 到 SXP 对等体的连接后，收听者将从发言者下载完整的 IP-SGT 映射数据库。此后发生的所有更改仅在网络上出现新设备时被发送。因此，SXP 信息流速率与终端主机对网络进行身份验证的速率成比例。

已通过 SXP 连接获悉的 IP-SGT 映射条目在 SXP IP-SGT 映射数据库中进行维护。可以通过不同 SXP 连接获悉相同映射条目。此映射数据库为每个已获悉的映射条目维护一个副本。同一 IP-SGT 映射值

的多个映射条目按获悉映射的连接的对等 IP 地址进行标识。SXP 请求 IP-SGT 管理器在首次获悉新映射时添加映射条目，并在删除 SXP 数据库中的最后副本时删除映射条目。

无论 SXP 连接何时被配置为说话者，SXP 都请求 IP-SGT 管理器将在设备上收集的所有映射条目转发给对等体。当在本地获悉新映射时，IP-SGT 管理器请求 SXP 通过已配置为说话者的连接转发此映射。

将 ASA 同时配置为 SXP 连接的发言者和收听者可能会导致形成 SXP 循环，这意味着最初传输 SXP 数据的 SXP 对等体可以接收这些数据。

将 ASA 注册到 ISE

在 ISE 中，必须首先将 ASA 配置为认可的思科 TrustSec 网络设备，ASA 才能成功导入 PAC 文件。要将 ASA 注册到 ISE，请执行以下步骤：

过程

步骤 1 登录 ISE。

步骤 2 依次选择 **Administration > Network Devices > Network Devices**。

步骤 3 点击 **Add**。

步骤 4 输入 ASA 的 IP 地址。

步骤 5 当 ISE 用于进行用户身份验证时，请在 **Authentication Settings** 区域输入一个共享密钥。

在 ASA 上配置 AAA 服务器时，需提供您此时在 ISE 上创建的共享密钥。ASA 上的 AAA 服务器要与 ISE 通信需使用此共享密钥。

步骤 6 为 ASA 指定设备名称、设备 ID、密码和下载间隔。有关如何执行这些任务的详细信息，请参阅 ISE 文档。

在 ISE 上创建安全组

在配置 ASA 以便与 ISE 通信时，需指定 AAA 服务器。在 ASA 上配置 AAA 服务器时，必须指定服务器组。必须配置安全组，使其使用 RADIUS 协议。要在 ISE 上创建安全组，请执行以下步骤：

过程

步骤 1 登录 ISE。

步骤 2 依次选择 **Policy > Policy Elements > Results > Security Group Access > Security Group**。

步骤 3 为 ASA 添加安全组。（安全组是全局性的，并非 ASA 特定的。）

ISE 在 **Security Groups** 下创建带有标记的条目。

步骤 4 在 Security Group Access 区域，为 ASA 配置设备 ID 凭证和密码。

生成 PAC 文件

要生成 PAC 文件，请执行以下步骤。



注释 PAC 文件包括允许 ASA 和 ISE 保护两者之间进行的 RADIUS 交易的共享密钥。因此，请确保将其安全地存储于 ASA 中。

过程

步骤 1 登录 ISE。

步骤 2 依次选择 **Administration > Network Resources > Network Devices**。

步骤 3 从设备列表中选择 ASA。

步骤 4 在 Security Group Access (SGA) 下方点击 **Generate PAC**。

步骤 5 要加密 PAC 文件，请输入密码。

为加密 PAC 文件而输入的密码（或加密密钥）独立于在 ISE 上被配置为设备凭证的一部分的密码。

ISE 生成 PAC 文件。ASA 可通过 TFTP、FTP、HTTP、HTTPS 或 SMB 从闪存或远程服务器导入 PAC 文件。（导入 PAC 文件之前，不必一定将其置于 ASA 闪存中。）

思科 TrustSec 指南

本节包括在配置思科 TrustSec 之前应查看的指导原则和限制。

故障切换

- 在主/主和主/备配置下，您可以在 ASA 上配置基于安全组的策略。
- 如果故障切换配置中涉及 ASA，则必须将 PAC 文件导入主 ASA 设备。另外，还必须刷新主设备上的环境数据。
- ASA 可与为实现高可用性 (HA) 而配置的 ISE 通信。
- 您可以在 ASA 上配置多个 ISE 服务器，如果无法连接第一个服务器，会继续连接下一个服务器，以此类推。然而，如果服务器列表被下载为 Cisco TrustSec 环境数据的一部分，它将被忽略。

- 如果 ASA 中从 ISE 下载的安全组表到期且无法下载更新的安全组表，ASA 将继续基于上次下载的安全组表实施安全策略，直到 ASA 下载更新的表。

集群

- 如果故障切换配置中涉及 ASA，则必须将 PAC 文件导入主设备。
- 如果故障切换配置中涉及 ASA，则必须刷新主设备上的环境数据。

IPv6

对于 IPv6 和支持 IPv6 的网络设备，ASA 支持 SXP。AAA 服务器必须使用 IPv4 地址。

第 2 层 SGT 实施

- 仅支持物理接口、VLAN 接口、端口通道接口和冗余接口。
- 不支持逻辑接口或虚拟接口，例如 BVI。
- 不支持采用 SAP 协商和 MACsec 的链路加密。
- 不支持故障切换链路。
- 不支持集群控制链路。
- 如果 SGT 更改，ASA 不会对现有的流量重新分类。任何根据以前 SGT 指定的策略决定对流量寿命依然有效。不过，ASA 可立即反映传出数据包上的 SGT 更改，即便数据包所属的流量是基于以前的 SGT 进行分类。
- ASA 5585-X 的硬件架构旨在以最佳方式均衡普通数据包的负载，但包含第 2 层安全组标记拼版 (Layer 2 Security Group Tagging Imposition) 的内联标记数据包并非如此。ASA 5585-X 在处理传入内联标记数据包时，性能可能会大幅下降。其他 ASA 平台上的内联标记数据包以及 ASA 5585-X 上的非标记数据包不会出现此问题。一种解决方法是卸载访问策略，以便最大限度地减少传入 ASA 5585-X 的内联标记数据包，从而允许使用交换机来处理标记的策略实施。另一种解决方法是使用 SXP，以便 ASA 5585-X 可将 IP 地址映射到安全组标记，而无需接收标记的数据包。
- ASM 不支持第 2 层安全组标记拼版 (Security Group Tagging Imposition)。

其他规定

- ASA 支持 SXP 版本 3。ASA 与支持 SXP 的不同网络设备协商 SXP 版本。
- 您可以将 ASA 配置为在 SXP 调和计时器到期时刷新安全组表，也可以根据需要下载安全组表。从 ISE 更新 ASA 中的安全组表时，更改也会反映到相应的安全策略中。
- Cisco TrustSec 在单一情景和多情景模式中支持 Smart Call Home 功能，但在系统情景模式中不支持此功能。
- 只能将 ASA 配置为在单一思科 TrustSec 域中实现互通。

- ASA 不支持设备中 SGT-名称映射的静态配置。
- SXP 消息不支持 NAT。
- SXP 在网络中将 IP-SGT 映射传送到实施点。如果接入层交换机与实施点分属不同的 NAT 域，该交换机上传的 IP-SGT 映射则无效，而且在实施设备上进行的 IP-SGT 映射数据库查找不会显示有效的结果。因此，ASA 无法在实施设备上应用安全组感知型安全策略。
- 您可以为 ASA 配置默认密码以用于 SXP 连接，也可以选择不使用密码；不过 SXP 对等体不支持使用特定于连接的密码。配置的默认 SXP 密码应当在部署网络中保持一致。如果配置连接特定密码，连接可能会失败，并且显示警告消息。如果使用默认密码配置连接，但未配置默认密码，则结果与不使用密码配置连接时的结果相同。
- 可以将 ASA 配置为 SXP 发言者或收听者，或者同时配置为两者。但是，当某台设备与对等体之间存在双向连接，或是设备属于单向连接设备链的一部分时，可能会形成 SXP 连接循环。
(ASA 可从数据中心的接入层获悉资源的 IP-SGT 映射。ASA 可能需要将这些标记传送到下游设备。) SXP 连接环路会导致 SXP 消息传输出现意外行为。如果 ASA 被配置为发言者和收听者，可能会形成 SXP 连接循环，导致最初发送 SXP 数据的对等体接收这些数据。
- 在更改 ASA 本地 IP 地址时，必须确保所有 SXP 对等体均已更新其对等体列表。另外，如果 SXP 对等体更改其 IP 地址，必须确保这些更改反映到 ASA 中。
- 不支持自动 PAC 文件调配。ASA 管理员必须从 ISE 管理界面请求 PAC 文件，再将其导入 ASA。
- PAC 文件有过期日期。在当前的 PAC 文件到期前必须导入更新的 PAC 文件，否则 ASA 将无法检索环境数据更新。如果 ASA 中从 ISE 下载的 PAC 文件到期且无法下载更新的安全组表，ASA 将继续基于上次下载的安全组表实施安全策略，直到 ASA 下载更新的表。
- 如果 ISE 中的安全组发生更改（例如被重命名或删除），ASA 不会更改包含与已更改安全组相关联的 SGT 或安全组名称的任何 ASA 安全策略之状态；但 ASA 会生成一条系统日志消息，指示这些安全策略已更改。
- 在 ISE 1.0 中不支持组播类型。
- SXP 连接在通过 ASA 互连的两个 SXP 对等体之间处于正在初始化的状态，如下例所示：

```
(SXP peer A) - - - - (ASA) - - - (SXP peer B)
```

因此，在将 ASA 配置为与思科 TrustSec 集成时，必须在 ASA 中启用 no-NAT、no-SEQ-RAND 和 MD5-AUTHENTICATION TCP 选项以便配置 SXP 连接。为 SXP 对等体之间以 SXP 端口 TCP 64999 为目标的流量创建 TCP 状态绕行策略。然后，在相应的接口上应用该策略。

例如，以下命令集显示如何为 TCP 状态绕行策略配置 ASA：

```
access-list SXP-MD5-ACL extended permit tcp host peerA host peerB eq 64999
access-list SXP-MD5-ACL extended permit tcp host peerB host peerA eq 64999

tcp-map SXP-MD5-OPTION-ALLOW
tcp-options range 19 19 allow

class-map SXP-MD5-CLASSMAP
match access-list SXP-MD5-ACL
```



```
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
policy-map global_policy
class SXP-MD5-CLASSMAP
  set connection random-sequence-number disable
  set connection advanced-options SXP-MD5-OPTION-ALLOW
  set connection advanced-options tcp-state-bypass
service-policy global_policy global
```

将 ASA 配置为与思科 Trustsec 集成

要配置 ASA 与思科 TrustSec 集成，请执行以下任务。

开始之前

在配置 ASA 与思科 TrustSec 集成之前，必须在 ISE 中完成以下任务：

- [将 ASA 注册到 ISE，第 77 页](#)
- [在 ISE 上创建安全组，第 77 页](#)
- [生成 PAC 文件，第 78 页](#)

过程

步骤 1 [配置 AAA 服务器以便与思科 TrustSec 集成，第 81 页](#)

步骤 2 [导入 PAC 文件，第 82 页](#)

步骤 3 [配置安全交换协议，第 84 页](#)

此任务会为 SXP 启用和设置默认值。

步骤 4 [添加 SXP 连接对等体，第 85 页](#)

步骤 5 [刷新环境数据，第 86 页](#)

请根据需要执行任务。

步骤 6 [配置安全策略，第 86 页](#)

步骤 7 [配置第 2 层安全组标记实施，第 87 页](#)

配置 AAA 服务器以便与思科 TrustSec 集成

本节介绍如何为 Cisco TrustSec 集成 AAA 服务器。要在 ASA 上配置 AAA 服务器组以便与 ISE 通信，请执行以下步骤。

开始之前

- 引用的服务器组必须配置为使用 RADIUS 协议。如果向 ASA 中添加非 RADIUS 服务器，配置将会失败。
- 如果也使用 ISE 进行用户验证，请获取将 ASA 注册到 ISE 时在 ISE 上输入的共享密钥。请联系 ISE 管理员，以获取此信息。

过程

-
- 步骤 1** 依次选择 **Configuration > Firewall > Identity By TrustSec**。
 - 步骤 2** 点击 **Manage** 以向 ASA 中添加服务器组。
系统将显示 **Configure AAA Server Group** 对话框。
 - 步骤 3** 输入在 ISE 上为 ASA 创建的安全组的名称。
您在此指定的服务器组名称必须与在 ISE 上为 ASA 创建的安全组名称匹配。如果这两个组名称不匹配，则 ASA 无法与 ISE 匹配。请联系 ISE 管理员，以获取此信息。
 - 步骤 4** 从 **Protocol** 下拉列表中选择 **RADIUS**。
要完成 **AAA Server Group** 对话框中剩余的字段，请参阅一般操作配置指南的“RADIUS”一章。
 - 步骤 5** 点击 **OK**。
 - 步骤 6** 选择刚刚创建的 AAA 服务器组，然后在 **Servers in the Selected Group** 区域点击 **Add** 以向组中添加服务器。
系统将显示 **Add AAA Server** 对话框。
 - 步骤 7** 选择 ISE 服务器所在的网络接口。
 - 步骤 8** 输入 ISE 服务器的 IP 地址。
要完成 **AAA Server** 对话框中剩余的字段，请参阅一般操作配置指南的“RADIUS”一章。
 - 步骤 9** 点击 **OK**。
 - 步骤 10** 点击 **Apply** 以将更改保存到运行配置。
-

导入 PAC 文件

本节介绍如何导入 PAC 文件。

开始之前

- ASA 在 ISE 中必须被配置为认可的思科 TrustSec 网络设备，才能生成 PAC 文件。
- 在 ISE 上生成 PAC 文件时，请获取用于加密此文件的密码。ASA 需要使用此密码来导入和解密 PAC 文件。

- ASA 需要访问 ISE 生成的 PAC 文件。ASA 可通过 TFTP、FTP、HTTP、HTTPS 或 SMB 从闪存或远程服务器导入 PAC 文件。（导入 PAC 文件之前，无需将其置于 ASA 闪存中。）
- 系统已为 ASA 配置服务器组。

如要导入 PAC 文件，请执行以下步骤：

过程

步骤 1 依次选择 **Configuration > Firewall > Identity By TrustSec**。

步骤 2 选中 **Enable Security Exchange Protocol** 复选框，以启用 SXP。

步骤 3 点击 **Import PAC** 以显示 **Import PAC** 对话框。

步骤 4 按以下格式之一输入 PAC 文件的路径和文件名：

- **disk0**: disk0 上的路径和文件名
- **disk1**: disk1 上的路径和文件名
- **flash**: 闪存上的路径和文件名
- **ftp**: FTP 上的路径和文件名
- **http**: HTTP 上的路径和文件名
- **https**: HTTPS 上的路径和文件名
- **smb**: SMB 上的路径和文件名
- **tftp**: TFTP 上的路径和文件名

多模式

- **http**: HTTP 上的路径和文件名
- **https**: HTTPS 上的路径和文件名
- **smb**: SMB 上的路径和文件名
- **tftp**: TFTP 上的路径和文件名

步骤 5 输入用于加密 PAC 文件的密码。此密码与 ISE 上配置为设备凭证一部分的密码无关。

步骤 6 重新输入密码以进行确认。

步骤 7 点击 **Import**。

步骤 8 点击 **Apply** 以将更改保存到运行配置。

在导入 PAC 文件时，该文件将被转换为 ASCII HEX 格式并由系统在非交互模式下发送到 ASA。

配置安全交换协议

您需要启用和配置安全交换协议 (SXP)，才能使用思科 Trustsec。

开始之前

至少必须有一个接口处于 UP/UP 状态。如果启用 SXP 时所有接口均处于关闭状态，ASA 不会显示消息来表示该 SXP 没有运行或无法启用。如果通过输入 **show running-config** 命令来检查配置，此命令输出则显示以下消息：

```
“WARNING: SXP configuration in process, please wait for a few moments and try again.”
```

过程

步骤 1 依次选择 **Configuration > Firewall > Identity By TrustSec**。

步骤 2 选中 **Enable Security Exchange Protocol** 复选框，以启用 SXP。默认情况下，SXP 被禁用。

步骤 3 （可选，不推荐。）为 SXP 连接输入默认本地 IP 地址。此 IP 地址可以是一个 IPv4 或 IPv6 地址。

注释 ASA 确定使用 SXP 连接的本地 IP 地址作为对等体 IP 地址可访问的传出接口 IP 地址。如果配置的本地地址与传出接口 IP 地址不同，则 ASA 无法连接到 SXP 对等体并会生成一条系统日志消息。我们建议您不要为 SXP 连接配置默认源 IP 地址，并允许 ASA 执行路由/ARP 查询来确定 SXP 连接的源 IP 地址。

步骤 4 （可选。）输入用于对 SXP 对等体进行 TCP MD5 身份验证的默认密码。默认情况下，SXP 连接未设置密码。

当且仅当配置 SXP 连接对等体来使用默认密码时配置一个默认密码。密码最长为 80 个字符。它没有加密。

步骤 5 （可选。）在 **Retry Timer** 字段，更改 ASA 尝试在 SXP 对等体之间设置新 SXP 连接的时间间隔。

ASA 将继续尝试进行连接，直到成功建立连接，尝试失败后则等待重试之前的重试间隔。您可以指定重试期间，范围介于 0 到 64000 秒之间。默认值为 120 秒。如果指定 0 秒，ASA 则不会尝试连接到 SXP 对等体。

我们建议您将重试计时器配置为不同于其 SXP 对等体的值。

步骤 6 （可选。）更改调和计时器值。

在 SXP 对等体终止其 SXP 连接后，ASA 将启动抑制计时器。如果 SXP 在抑制计时器运行时进行连接，ASA 将启动调和计时器；然后，ASA 将更新 SXP 映射数据库来获取最新映射。

在调和计时器过期后，ASA 将扫描 SXP 映射以识别过时的映射条目（以前的连接会话获取的内容）。ASA 会将这些连接标记为过时。在调和计时器过期后，ASA 将从 SXP 映射数据中删除过时的条目。

您可以指定调和期间，范围介于 1 到 64000 秒之间。默认值为 120 秒。

步骤 7（可选。）在 **Network Map** 中，配置 IPv4 子网在充当使用 SXPv2 或更低版本的对等体的发言者时的扩展深度。

如果对等体使用 SXPv2 或更低版本，则该对等体无法将 SGT 扩展至子网绑定。ASA 可以将 IPv4 子网绑定扩展到各个主机绑定（IPv6 绑定不进行扩展）。此命令指定一个子网绑定可生成的最大主机绑定数。

您可以指定最大数量，范围介于 0 到 65535 之间。默认值为 0，意味着子网绑定未扩展至主机绑定。

步骤 8 点击 **Apply** 以将更改保存到运行配置。

添加 SXP 连接对等体

若要添加 SXP 连接对等体，请执行以下步骤：

过程

步骤 1 依次选择 **Configuration > Firewall > Identity By TrustSec**。

步骤 2 点击 **Add** 显示 **Add Connection** 对话框。

步骤 3 输入 SXP 对等体的 IPv4 或 IPv6 地址。对等体 IP 地址必须可从 ASA 传出接口访问。

步骤 4 通过选择以下值之一指示是否对 SXP 连接使用身份验证密钥：

- **Default** - 使用为 SXP 连接配置的默认密码。
- **None** - 对 SXP 连接不使用密码。

步骤 5（可选）通过选择以下值之一指定 SXP 连接的模式：

- **Local** - 使用本地 SXP 设备。
- **Peer** - 使用对等 SXP 设备。

步骤 6 指定 ASA 是作为 SXP 连接的发言者还是收听者：

- **Speaker** - ASA 可将 IP-SGT 映射转发到上游设备。
- **Listener** - ASA 可接收来自下游设备的 IP-SGT 映射。

步骤 7（可选）点击 **Advanced**，并输入 SXP 连接的本地 IPv4 或 IPv6 地址。

ASA 使用路由查询来确定正确的接口。如果指定地址，则该地址必须与出站接口的路由查询接口地址匹配。我们建议您不要为 SXP 连接配置源 IP 地址，并允许 ASA 执行路由/ARP 查询来确定 SXP 连接的源 IP 地址。

步骤 8 点击 **OK**。

步骤 9 点击 **Apply** 以将设置保存到运行配置。

刷新环境数据

ASA 从 ISE 下载环境数据，ISE 中包括安全组标记 (SGT) 名称表。在 ASA 上完成以下任务后，ASA 将自动刷新从 ISE 获取的环境数据：

- 将 AAA 服务器配置为与 ISE 通信。
- 从 ISE 导入 PAC 文件。
- 标识 ASA 用于检索思科 TrustSec 环境数据的 AAA 服务器组。

通常，无需手动刷新来自 ISE 的环境数据；然而，安全组会在 ISE 上发生更改。在刷新 AAA 安全组表中的数据之前，这些更改不会反映到 ASA 上，所以在 ASA 上刷新数据可确保将在 ISE 上进行的任何安全组更改都反映到 ASA 上。



注释 我们建议您在 ISE 上安排策略配置更改，并于维护期间在 ASA 上手动刷新数据。按这种方式处理策略配置更改，可尽可能地提高安全组名称被解析以及安全策略在 ASA 上立即处于活动状态的可能性。

要刷新环境数据，请执行以下步骤：

过程

步骤 1 依次选择 **Configuration > Firewall > Identity By TrustSec**。

步骤 2 依次点击**服务器组设置区域**的**刷新环境 > 数据**。

ASA 将刷新来自 ISE 的思科 TrustSec 环境数据，并将调和计时器重置为配置的默认值。

配置安全策略

可以在许多 ASA 功能中加入思科 TrustSec 策略。任何使用扩展 ACL（除非在本章列为不支持）的功能都能够利用思科 TrustSec。可以将安全组参数添加到扩展 ACL 以及基于网络的传统参数中。

- 要配置访问规则，请参阅[配置访问规则](#)，第 17 页。有关其他扩展 ACL，请参阅[配置扩展 ACL](#)，第 45 页。
- 要配置可在 ACL 中使用的安全组对象组，请参阅[配置安全组对象组](#)，第 34 页。

例如，访问规则通过网络信息允许或拒绝接口上的流量。通过思科 TrustSec，可以根据安全组控制访问。例如，可以为 sample_securitygroup1 10.0.0.0 255.0.0.0 创建访问规则，这意味着，安全组可以拥有 10.0.0.0/8 子网上的任何 IP 地址。

可以根据安全组名称（服务器、用户、非受管设备等等）、基于用户的属性和基于 IP 地址的传统对象（IP 地址、Active Directory 对象和 FQDN）构成的组合配置安全策略。安全组成员能够扩展到角色以外，将设备和位置属性包含在内，并且不受用户组成员约束。

配置第 2 层安全组标记实施

Cisco TrustSec 可以对每个网络用户和资源进行标识和身份验证，并分配一个称为安全组标记 (SGT) 的 16 位数字。转而，此标识符会传送到网络跃点之间，从而允许 ASA、交换机和路由器等中间设备基于此身份标记实施策略。

SGT 以太网标记（也称为第 2 层 SGT 实施）使 ASA 能够使用思科专有的以太网帧 (EtherType 0x8909)（允许向纯文本以太网帧中插入源安全组标记）在以太网接口上收发安全组标记。ASA 可基于手动每接口配置在传出数据包中插入安全组标记，并处理传入数据包中的安全组标记。此功能允许跨网络设备对终端身份进行内联逐跳传送，在每个跃点之间提供无缝的第 2 层 SGT 实施。

下图显示第 2 层 SGT 实施的典型示例。

图 12: 第 2 层 SGT 实施



使用场合

下表介绍配置此功能时入口流量的预期行为。

表 4: 入口流量

接口配置	收到的已标记数据包	收到的未标记数据包
未发出命令。	数据包被丢弃。	SGT 值来自 IP-SGT 管理器。
发出 cts manual 命令。	SGT 值来自 IP-SGT 管理器。	SGT 值来自 IP-SGT 管理器。
同时发出 cts manual 命令和 policy static sgt sgt_number 命令。	SGT 值来自 policy static sgt sgt_number 命令。	SGT 值来自 policy static sgt sgt_number 命令。
同时发出 cts manual 命令和 policy static sgt sgt_number trusted 命令。	SGT 值来自数据包中的内联 SGT。	SGT 值来自 policy static sgt sgt_number 命令。



注释 如果没有来自 IP-SGT 管理器的匹配 IP-SGT 映射，则为“Unknown”使用预留 SGT 值“0x0”。

下表介绍配置此功能时出口流量的预期行为。

表 5: 出口流量

接口配置	发送的已标记或未标记数据包
未发出命令。	未标记
发出 cts manual 命令。	已标记
同时发出 cts manual 命令和 propagate sgt 命令。	已标记
同时发出 cts manual 命令和 no propagate sgt 命令。	未标记

下表介绍配置此功能时流向设备的流量和流出设备的流量的预期行为。

表 6: 传入和传出流量

接口配置	接收的已标记或未标记数据包
未在进口接口上为流向设备的流量发出命令。	数据包被丢弃。
在进口接口上为流向设备的流量发出 cts manual 命令。	数据包已被接受，但没有策略实施或 SGT 传送。
未发出 cts manual 命令，或者在出口接口上为流出设备的流量同时发出 cts manual 命令和 no propagate sgt 命令。	未标记数据包被发送，但没有策略实施。SGT 号来自 IP-SGT 管理器。

接口配置	接收的已标记或未标记数据包
已发出 cts manual 命令，或者在出口接口上为流出设备的流量发出 cts manual 命令和 propagate sgt 命令。	已标记数据包被发送。SGT 号来自 IP-SGT 管理器。



注释 如果没有来自 IP-SGT 管理器的匹配 IP-SGT 映射，则为“Unknown”使用预留 SGT 值“0x0”。

在接口上配置安全组标记

要在接口上配置安全组标记，请执行以下步骤：

过程

步骤 1 选择以下选项之一：

- 配置 > 设备设置 > 接口 > 添加接口 > 高级
- 配置 > 设备设置 > 接口 > 添加冗余接口 > 高级
- 配置 > 设备设置 > 接口 > 添加以太网接口 > 高级

步骤 2 选中 **Enable secure group tagging for Cisco TrustSec** 复选框。

步骤 3 选中 **Tag egress packets with service group tags** 复选框。

步骤 4 选中 **Add a static secure group tag to all ingress packets** 复选框。

步骤 5 输入安全组标记号。有效值范围为 2 到 65519。

步骤 6 选中这是可信接口。请勿覆盖现有安全组标记复选框。

步骤 7 点击 **OK** 保存设置。

手动配置 IP-SGT 绑定

要手动配置 IP-SGT 绑定，请执行以下步骤：

过程

步骤 1 依次选择配置 > 按 **TrustSec** 配置防火墙身份。

步骤 2 在 **SGT Map** 区域点击 **Add**，或选择 SGT 映射，然后点击 **Edit**。

步骤 3 在 SGT Map 对话框中，输入 SGT 映射 IP 地址，并在相应字段中输入 SGT 值。

SGT 编号的范围介于 2 到 65519 之间。

要将网络映射到 SGT，请选中 **Prefix** 复选框并输入子网或 IPv6 前缀。例如，输入 24 来映射 10.100.10.0/24。

步骤 4 点击 **OK**，然后点击 **Apply** 以保存设置。

思科 TrustSec 的 AnyConnect VPN 支持

ASA 支持对 VPN 会话应用安全组标记。可以使用外部 AAA 服务器向 VPN 会话分配安全组标记 (SGT)，也可以通过为本地用户或 VPN 组策略配置安全组标记来向 VPN 会话分配安全组标记。然后，可以在第 2 层以太网上通过思科 TrustSec 系统传送此标记。安全组标记适用于组策略，当 AAA 服务器无法提供 SGT 时可用于本地用户。

以下是向 VPN 用户分配 SGT 的典型步骤：

1. 用户连接到使用 AAA 服务器组（包含 ISE 服务器）的远程访问 VPN。
2. ASA 从 ISE 请求可能包括 SGT 的 AAA 信息。ASA 也为用户通过隧道传输的流量分配 IP 地址。
3. ASA 使用 AAA 信息对用户进行身份验证，并创建隧道。
4. ASA 使用 AAA 信息中的 SGT 和分配的 IP 地址向第 2 层报头中添加一个 SGT。
5. 包含 SGT 的数据包传递到 Cisco TrustSec 网络中的下一个对等设备。

如果来自 AAA 服务器的属性中没有可分配给 VPN 用户的 SGT，ASA 将使用组策略中的 SGT。如果组策略中也没有 SGT，则会分配标记 0x0。



注释 此外，您也可以通过 ISE 授权变更 (CoA) 将 ISE 用于策略实施。有关如何配置策略实施的信息，请参阅 VPN 配置指南。

向远程访问 VPN 组策略和本地用户添加 SGT

要在远程访问 VPN 组策略中配置 SGT 属性，或在 VPN 策略中为 LOCAL 用户数据库中定义的用户配置 SGT 属性，请执行以下步骤。

没有用于组策略或本地用户的默认 SGT。

过程

步骤 1 要在远程访问 VPN 组策略上配置 SGT，请执行以下操作：

- a) 依次选择配置 > 远程接入 VPN > 网络（客户端）访问 > 组策略。
- b) 点击 **General** 选项卡，然后点击 **More Options**。
- c) 在 **Security Group Tag (STG)** 字段输入一个值，范围介于 2 到 65519 之间。

此外，也可以选择 None 来设置无 SGT。

d) 点击 **OK**。

步骤 2 要为 LOCAL 数据库中的用户配置 SGT，请执行以下操作：

- a) 依次选择 **Configuration > Remote Access VPN > AAA/Local Users > Local Users**。
- b) 选择一个用户，然后点击 **Edit**。
- c) 点击 **VPN Policy**。
- d) 在 **Security Group Tag (STG)** 字段输入一个值，范围介于 2 到 65519 之间。

此外，也可以选择 None 来设置无 SGT。

e) 点击 **OK**。

监控 Cisco TrustSec

请参阅以下屏幕来监控思科 TrustSec：

- **Monitoring > Properties > Identity By TrustSec > SXP Connections**

显示为 Cisco TrustSec 基础设施和 SXP 命令配置的默认值。

- **Monitoring > Properties > Connections**

过滤 IP 地址安全组表映射条目，以便您能够按安全组表值、安全组名称或 IP 地址查看数据。

- **Monitoring > Properties > Identity By TrustSec > Environment Data**

显示 ASA 上安全组表中包含的思科 TrustSec 环境信息。

- **Monitoring > Properties > Identity By TrustSec > IP Mapping**

过滤 IP 地址安全组表映射条目，以便您能够按安全组表值、安全组名称或 IP 地址查看数据。

点击 **Where Used**，显示已选中安全组对象在 ACL 中的使用位置，或者嵌入到另一个安全组对象中的位置。

- **Monitoring > Properties > Identity By TrustSec > PAC**

显示从 ISE 导入到 ASA 的 PAC 文件的相关信息，并包括 PAC 文件已过期或 30 天内即将过期的警告消息。

思科 TrustSec 的历史

表 7: 思科 TrustSec 的历史

功能名称	平台版本	说明
思科 TrustSec	9.0(1)	<p>Cisco TrustSec 可以提供基于现有的身份感知基础设施的访问控制，确保网络设备之间的数据保密性，并将集成平台上的安全访问服务集成在一个平台上。在思科 TrustSec 功能中，实施设备结合用户属性和终端属性制定基于角色和基于身份的访问控制决策。</p> <p>在此版本中，ASA 与思科 TrustSec 集成提供基于安全组的策略实施。Cisco TrustSec 域中的访问策略不受拓扑影响，基于源和目标设备的角色，而非基于网络 IP 地址。</p> <p>ASA 可对其他类型的基于安全组的策略（例如应用检测）使用思科 TrustSec，例如可配置包含基于安全组的访问策略的类映射。</p> <p>引入或修改了以下菜单项：</p> <p>Configuration > Firewall > Identity By TrustSecConfiguration > Firewall > Objects > Security Groups Object GroupsConfiguration > Firewall > Access Rules > Add Access RulesMonitoring > Properties > Identity By Tag.</p>
第 2 层安全组标记实施	9.3(1)	<p>现在，可以使用结合了以太网标记的安全组标记来实施策略。SGT 加以太网标记（也称为第 2 层 SGT 实施）使 ASA 能够使用思科专有的以太网帧 (EtherType 0x8909)（允许向纯文本以太网帧中插入源安全组标记）在以太网接口上收发安全组标记。</p> <p>修改了以下屏幕：</p> <p>Configuration > Device Setup > Interfaces > Add Interface > Advanced Configuration > Device Setup > Interfaces > Add Redundant Interface > Advanced Configuration > Device Setup > Add Ethernet Interface > Advanced.</p>
思科 Trustsec 支持安全交换协议 (SXP) 版本 3。	9.6(1)	<p>ASA 上的思科 Trustsec 现在实施 SXPv3，其中启用了比主机绑定更加高效的 SGT 到子网绑定。</p> <p>修改了以下菜单项：配置 > 防火墙 > 按 TrustSec 标识和 SGT 映射设置对话框。</p>
Trustsec SXP 连接可配置删除抑制计时器	9.8(3)	<p>默认 SXP 连接抑制计时器为 120 秒。现在，您可以配置此计时器，范围介于 120 到 64000 秒之间。</p> <p>新增/修改的命令：cts sxp delete-hold-down period、show cts sxp connection brief 和 show cts sxp connections。</p> <p>无 ASDM 支持。</p>



第 7 章

ASA FirePOWER 模块

以下主题介绍如何配置 ASA 上运行的 ASA FirePOWER 模块。

- [关于 ASA FirePOWER 模块，第 93 页](#)
- [ASA FirePOWER 模块的许可要求，第 97 页](#)
- [ASA FirePOWER 指南，第 97 页](#)
- [ASA FirePOWER 默认设置，第 99 页](#)
- [执行初始 ASA FirePOWER 设置，第 99 页](#)
- [配置 ASA FirePOWER 模块，第 108 页](#)
- [管理 ASA FirePOWER 模块，第 111 页](#)
- [监控 ASA FirePOWER 模块，第 120 页](#)
- [ASA FirePOWER 模块的历史，第 122 页](#)

关于 ASA FirePOWER 模块

ASA FirePOWER 模块提供下一代防火墙服务，包括下一代入侵防御系统 (NGIPS)、应用可见性与可控性 (AVC)、URL 过滤及高级恶意软件保护 (AMP)。

ASA FirePOWER 模块从 ASA 运行独立应用。此模块可以是一个硬件模块（仅在 ASA 5585-X 上），也可以是一个软件模块（其他所有型号）。

ASA FirePOWER 模块如何与 ASA 协同运行

您可以使用下列一种部署模式来配置 ASA FirePOWER 模块：

- **内联模式** - 在内联部署中，实际流量被发送到 ASA FirePOWER 模块，该模块的策略会影响对流量采取的操作。在丢弃不需要的流量并执行由策略应用的任何其他操作后，流量返回至 ASA，以供进一步处理和最终传输。
- **内联分路仅监控模式 (ASA 内联)** - 在内联分路仅监控部署中，流量副本被发送到 ASA FirePOWER 模块，但不会返回 ASA。通过内联分路模式，可以查看 ASA FirePOWER 模块会对流量采取的操作，并且可以评估流量内容，而不会影响网络。但是，在这种模式下，ASA 不会对流量应用其策略，所以流量可能会由于访问规则、TCP 规范化等原因被丢弃。

- 被动仅监控（流量转发）模式 - 如果想要杜绝 ASA 与 FirePOWER 服务设备协同运行影响流量的任何可能性，可以配置一个流量转发接口并将其连接到交换机上的 SPAN 端口。在此模式下，流量会直接被发送到 ASA FirePOWER 模块，不经过 ASA 处理。这种流量称为“black holed”（黑洞），因为该模块不会返回任何内容，ASA 也不会将该流量传出任何接口。您必须在单情景透明模式下运行 ASA，才能配置流量转发。

请务必在 ASA 和 ASA FirePOWER 上配置一致的策略。两种策略均应反映流量的内联或仅监控模式。

以下各节对这些模式进行更详细地说明。

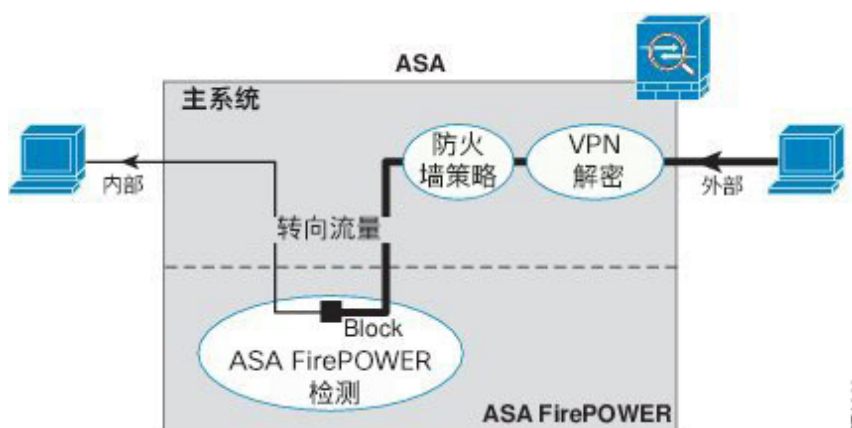
ASA FirePOWER 内联模式

在内联模式下，流量先经过防火墙检查，才会被转发到 ASA FirePOWER 模块。在 ASA 上识别要进行 ASA FirePOWER 检测的流量后，流量将按以下方式通过 ASA 和模块：

1. 流量进入 ASA。
2. 解密流入 VPN 的流量。
3. 应用防火墙策略。
4. 流量被发送到 ASA FirePOWER 模块。
5. ASA FirePOWER 模块向流量应用其安全策略，并采取适当的操作。
6. 有效流量传回 ASA；ASA FirePOWER 模块可能会根据其安全策略阻止一些流量，这些流量不能通过。
7. 加密流出 VPN 的流量。
8. 流量退出 ASA。

下图显示在内联模式下使用 ASA FirePOWER 模块时的流量数据流。在此示例中，模块阻止不允许某个应用使用的流量。所有其他流量均通过 ASA 转发。

图 13: ASA 中的 ASA FirePOWER 模块流量数据流





注释 如果在两个 ASA 接口上的主机之间建立了连接，并且仅为其中一个接口配置了 ASA FirePOWER 服务策略，则这些主机之间的所有流量均会被发送到 ASA FirePOWER 模块，包括非 ASA FirePOWER 接口上始发的流量（因为该功能是双向的）。

ASA FirePOWER 内联分路仅监控模式

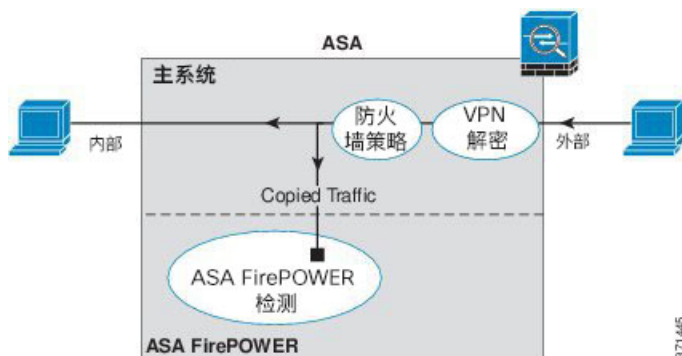
此模式仅会向 ASA FirePOWER 模块发送流量流副本，以用于监控。此模块向流量应用安全策略，并告知您其在内联模式下运行时将会执行的处理，例如流量可能会在事件中被标记为“应丢弃”。可以使用这些信息来分析流量，帮助您确定内联模式是否合适。



注释 无法在 ASA 上同时配置内联分路仅监控模式和正常内联模式。只允许一种类型的服务策略规则。在多情景模式下，对某些情景无法配置内联分路仅监控模式，对另一些情景则无法配置正常内联模式。

下图显示在内联分路模式下运行时的流量。

图 14: ASA FirePOWER 内联分路仅监控模式



ASA FirePOWER 被动仅监控流量转发模式

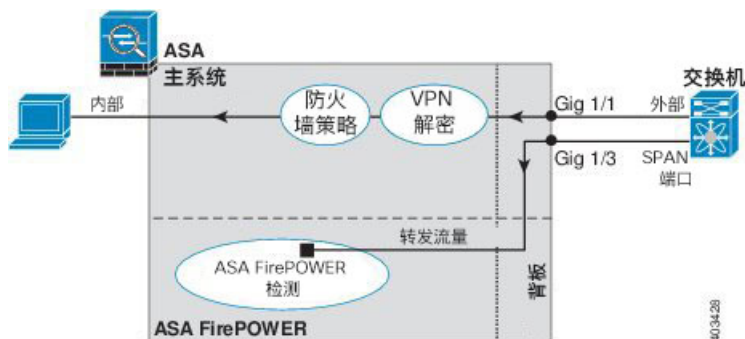
若要单纯作为入侵检测系统 (IDS) 运行 ASA FirePOWER 模块，而不对流量造成任何影响，您可以配置一个流量转发接口。流量转发接口可将收到的所有流量直接发送到 ASA FirePOWER 模块，不作任何 ASA 处理。

此模块向流量应用安全策略，并告知您其在内联模式下运行时将会执行的处理，例如流量可能会在事件中被标记为“应丢弃”。可以使用这些信息来分析流量，帮助您确定内联模式是否合适。

此设置中的流量从不会被转发：无论模块还是 ASA，均不会将流量发送到其最终目标。您必须在单一情景和透明模式下运行 ASA，才能使用此配置。

下图显示配置为进行流量转发的接口。该接口连接到交换机 SPAN 端口，以便 ASA FirePOWER 模块可检测所有网络流量。通常另一个接口通过防火墙发送流量。

图 15: ASA FirePOWER 被动仅监控，流量转发模式



ASA FirePOWER 管理

此模块拥有仅用于初始配置和故障排除的基本命令行界面 (CLI)。在 ASA FirePOWER 模块上可使用以下方法之一配置安全策略：

- Firepower/FireSIGHT 管理中心 - 可在单独的管理中心设备上托管，或作为虚拟设备托管。自版本 6 起，管理中心应用称为 Firepower。之前的版本中称之为 FireSIGHT。
- ASDM（检查与您的型号/版本的兼容性）- 您可使用内部 ASDM 同时管理 ASA 和该模块。

与 ASA 功能的兼容性

ASA 包括许多高级应用检测功能，包括 HTTP 检测。不过，ASA FirePOWER 模块还提供比 ASA 更高级的 HTTP 检测，以及更多适合其他应用的功能，包括监控和控制应用使用情况。

您必须遵守以下有关 ASA 的配置限制：

- 不对发送到 ASA FirePOWER 模块的 HTTP 流量配置 ASA 检测。
- 不对发送到 ASA FirePOWER 模块的流量配置云网络安全 (ScanSafe) 检测。如果流量同时匹配云网络安全和 ASA FirePOWER 服务策略，则流量仅被转发到 ASA FirePOWER 模块。如果要实施两种服务，请确保每种服务的流量匹配条件之间没有重叠。
- 不能启用移动用户安全 (MUS) 服务器，它与 ASA FirePOWER 模块不兼容。

ASA 上的其他应用检测与 ASA FirePOWER 模块兼容，包括默认检测。

如果 ASA FirePOWER 模块无法过滤 URL，应该怎么办

ASA FirePOWER 模块通过管理 Firepower 管理中心 HTTP 上的流量获取其 URL 过滤数据。如果该模块无法下载此数据库，则无法执行 URL 过滤。

如果 ASA FirePOWER 模块与 Firepower 管理中心（执行 ASA HTTP 检测或使用 ASA CX 模块执行 HTTP 检测）之间存在设备，检测可能会冻结 ASA FirePOWER 模块发往 Firepower 管理中心的 HTTP

GET 请求。如果在托管 ASA FirePOWER 模块的 ASA 上配置 HTTP 检测（属于错误配置），也会出现这种问题。

要解决问题，请执行以下任何适合您的情况的操作：

- 如果在托管 ASA FirePOWER 模块的 ASA 上配置了 HTTP 检测，请删除 HTTP 检测配置。ASA FirePOWER 检测与 ASA HTTP 检测不兼容。
- 如果存在执行 ASA HTTP 检测的干预设备，请从 HTTP 检测策略映射中删除丢弃协议违规操作：

```
policy-map type inspect http http_inspection_policy
  parameters
    no protocol-violation action drop-connection
```

- 如果存在干预性 ASA CX 模块，请绕过该 CX 模块以便在 ASA FirePOWER 模块和 Firepower 管理中心的管理 IP 地址之间建立连接。

ASA FirePOWER 模块的许可要求

ASA FirePOWER 模块的某些功能领域可能需要其他许可证。

对于 Firepower/FireSIGHT 管理中心管理的 ASA FirePOWER 模块，请使用管理中心在该模块上启用许可证。有关详细信息，请参阅 *FireSIGHT* 系统用户指南 5.4 的“许可”一章、*Firepower* 管理中心配置指南 6.0 或“FireSIGHT 管理中心”联机帮助。

对于使用 ASDM 管理的 ASA FirePOWER 模块，请在该模块中使用 ASDM 中的 FirePOWER 模块配置启用许可证。有关详细信息，请参阅 *ASA FirePOWER* 模块用户指南 5.4、*ASA FirePOWER* 服务本地管理配置指南 6.0 或 ASDM 中的模块联机帮助。

ASA 本身不需要任何额外许可证。

ASA FirePOWER 指南

故障切换准则

不支持直接进行故障切换；当 ASA 进行故障切换时，现有的任何 ASA FirePOWER 数据流都会被传送到新的 ASA。新 ASA 中的 ASA FirePOWER 模块将开始检测来自该点转发的流量；不传递旧检测状态。

您需负责在高可用性 ASA 对的 ASA FirePOWER 模块上维持一致的策略，以确保故障切换的行为一致。



注释 请在配置 ASA FirePOWER 模块之前先创建故障切换对。如果已在两个设备上配置这些模块，请首先清除备用设备上的接口配置，再创建高可用性对。在备用设备的 CLI 中，输入 **clear configure interface** 命令。

ASA 集群指导原则

不支持直接集群，但可在集群中使用这些模块。您需负责在集群的 ASA FirePOWER 模块上保持一致的策略。



注释 请在配置 ASA FirePOWER 模块之前先创建集群。如果已在从属设备上配置这些模块，请首先清除这些设备上的接口配置，再将它们添加到集群。在 CLI 中，输入 **clear configure interface** 命令。

型号规定

- 有关 ASA 型号软硬件与 ASA FirePOWER 模块的兼容性，请参阅[思科 ASA 兼容性](#)。
- 对于 ASA 5515-X 至 ASA 5555-X，必须安装思科固态硬盘 (SSD)。有关详细信息，请参阅《ASA 5500-X 硬件指南》。(5508-X 和 5516-X 上标配 SSD。)
- 无法更改 ASA 5585-X 硬件模块上已安装的软件类型。如果购买 ASA FirePOWER 模块，以后则无法在该模块上安装其他软件。
- 在模块重新启动期间（包括软件升级期间的重新启动），ASA 5585-X ASA FirePOWER 硬件模块上的接口将丢弃长达 30 秒内的流量。

ASDM 管理 ASA FirePOWER 的准则

- ASDM 管理支持的 ASA、ASDM 和 ASA FirePOWER 版本因型号而异。有关支持的组合，请参阅[思科 ASA 兼容性](#)。
- 如果在托管该模块的 ASA 上启用命令授权，必须使用具有 15 级权限的用户名登录，才能查看 **ASA FirePOWER** 主页、配置和监控页面。不支持以状态页面之外的只读或仅监控方式访问 **ASA FirePOWER** 页面。
- 如果使用的是 Java 7 更新 51 至 Java 8，需要同时为 ASA 和 ASA FirePOWER 模块配置身份证书。请参阅[安装用于 ASDM 的身份证书](#)。
- 您可能从不会同时使用 ASDM 和 Firepower/FireSIGHT 管理中心，但在两者之间要必选其一。

其他指导原则和限制

- 请参阅[与 ASA 功能的兼容性](#)，第 96 页。

- 无法在 ASA 上同时配置正常内联模式和内联分路仅监控模式。只允许一种类型的服务策略规则。在多情景模式下，对某些情景无法配置内联分路仅监控模式，对另一些情景则无法配置正常内联模式。

ASA FirePOWER 默认设置

下表列出了 ASA FirePOWER 模块的默认设置。

表 8: ASA FirePOWER 默认网络参数

参数	默认设置
管理 IP 地址	系统软件映像: 192.168.45.45/24 启动映像: 192.168.8.8/24
网关	系统软件映像: 无 启动映像: 192.168.8.1/24
SSH 或会话用户名	admin
密码	系统软件映像: <ul style="list-style-type: none"> • 版本 6.0 及更高版本: Admin123 • 早于 6.0 的版本: Sourcefire 启动映像: Admin123

执行初始 ASA FirePOWER 设置

在网络中部署 ASA FirePOWER 模块，然后选择管理方法。

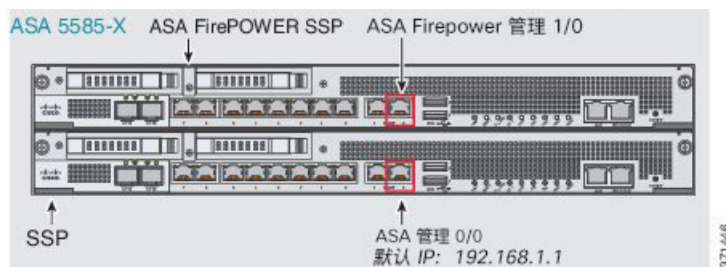
在网络中部署 ASA FirePOWER 模块

要确定如何将 ASA FirePOWER 模块管理接口连接到您的网络，请参阅防火墙模式和 ASA 型号部分。

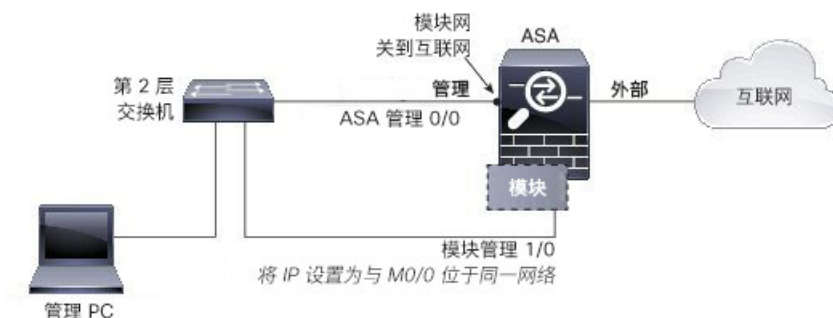
路由模式

路由模式下的 **ASA 5585-X**（硬件模块）

ASA FirePOWER 模块包括 ASA 中的独立管理接口。



进出 ASA FirePOWER 模块的所有管理流量必须进入和离开管理 1/0 或 1/1 接口。ASA FirePOWER 模块还需要访问互联网。由于管理 1/x 接口不是 ASA 数据接口，所以流量无法经由背板通过 ASA，因此需要通过电缆将管理接口实际连接到 ASA 接口。若要允许 ASA FirePOWER 通过 ASA 管理接口访问互联网，请参阅以下典型布线设置（您也可以使用数据接口）。也可以选择其他方法，具体取决于要连接网络的方式；例如，可以将管理接口 1/0 作为外部接口；如果有内部路由器，也可以在管理 1/0 接口和另一个 ASA 接口之间进行路由。



路由模式下的 ASA 5508-X 至 ASA 5555-X (软件模块)

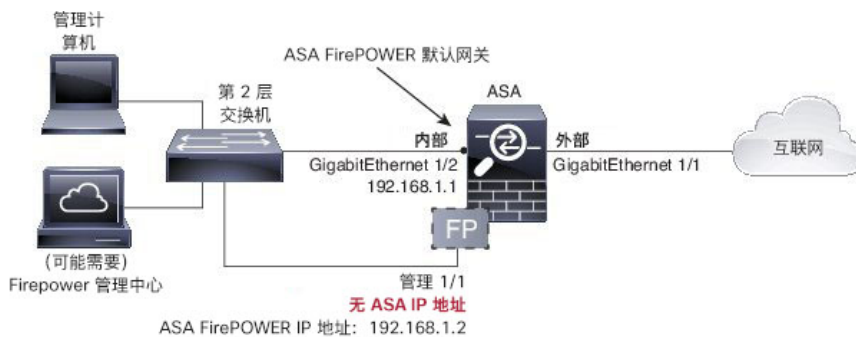
这些模块将 ASA FirePOWER 模块作为软件模块来运行，而且 ASA FirePOWER 模块与 ASA 共享管理 0/0 或管理 1/1 接口（取决于您的型号）。

进出 ASA FirePOWER 模块的所有管理流量必须进入和离开管理接口。ASA FirePOWER 模块还需要访问互联网。管理流量无法经由背板通过 ASA，因此需要通过电缆将管理接口实际连接到 ASA 接口，才能连接互联网。

如果在 ASA 配置中未配置管理接口的名称和 IP 地址，则该接口仅属于该模块。在这种情况下，管理接口并非普通 ASA 接口，您可以：

1. 将 ASA FirePOWER IP 地址配置为与普通 ASA 数据接口位于同一网络。
2. 将数据接口指定为 ASA FirePOWER 网关。
3. 将管理接口直接连接到数据接口（使用第 2 层交换机）。

若要允许 ASA FirePOWER 通过 ASA 内部接口访问互联网，请参阅以下典型布线设置。



对于 ASA 5508-X 和 5516-X，默认配置会启用上述网络部署，您唯一需要更改的是将模块 IP 地址设置为与 ASA 内部接口位于同一网络，并配置模块网关 IP 地址。

对于其他型号，必须删除 ASA 为管理 0/0 或 1/1 配置的名称和 IP 地址，再按以上所示配置其他接口。



注释 若有额外接口可分配到内部桥接组来配置“软交换机”，可避免使用外部交换机。请务必将所有桥接组接口设置为同一安全级别、允许相同的安全通信，并为每个桥接组成员配置 NAT。有关更多信息，请参阅“ASA 接口配置指南”一章。

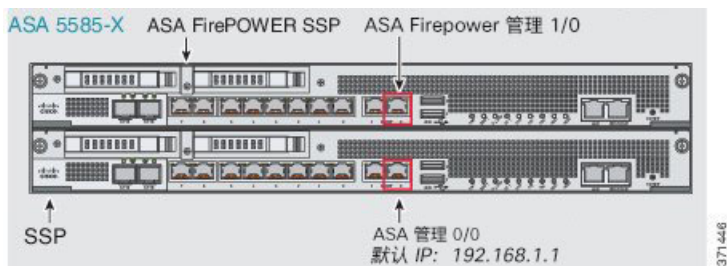


注释 如果要在内部网络上部署单独的路由器，则可以在管理接口和内部接口之间进行路由。在这种情况下，您可以通过适当地更改配置在管理接口上同时管理 ASA 和 ASA FirePOWER 模块，包括为管理接口配置 ASA 名称和 IP 地址（与 ASA FirePOWER 模块地址位于相同网络）。

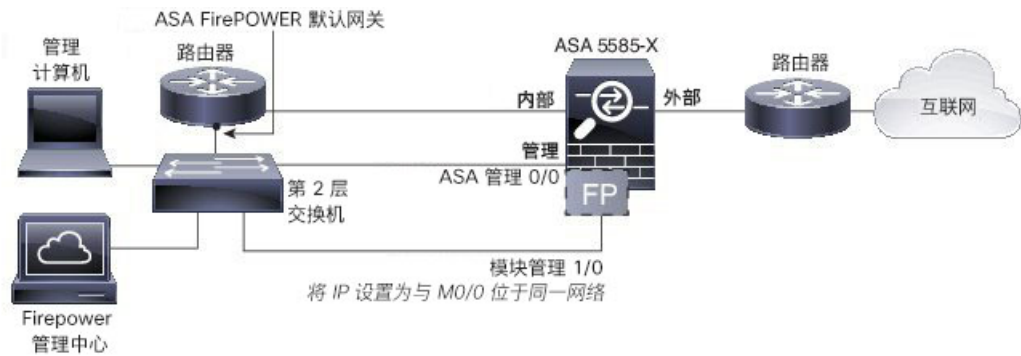
透明模式

透明模式下的 ASA 5585-X（硬件模块）

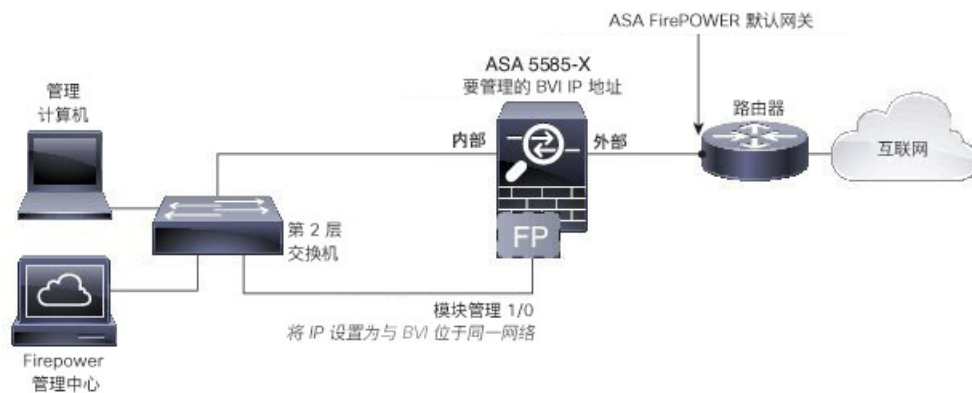
ASA FirePOWER 模块包括 ASA 中的独立管理接口。



进出 ASA FirePOWER 模块的所有管理流量必须进入和离开管理 1/0 或 1/1 接口。ASA FirePOWER 模块还需要访问互联网。由于此接口不是 ASA 数据接口，所以流量无法经由背板通过 ASA，因此需要通过电缆将管理接口实际连接到 ASA 接口。若要允许 ASA FirePOWER 通过 ASA 内部接口访问互联网，请参阅以下典型布线设置。



如果不使用内部路由器，可通过内部接口（使用 BVI IP 地址）管理 ASA，而不使用管理 0/0 接口进行管理：



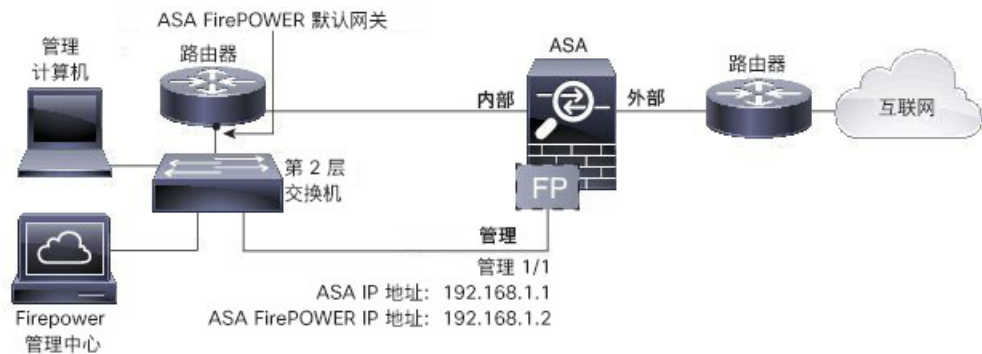
注释 若有额外接口可分配到内部桥接组来配置“软交换机”，可避免使用外部交换机。请务必将所有桥接组接口设置为同一安全级别、允许相同的安全通信，并为每个桥接组成员配置 NAT。有关更多信息，请参阅“ASA 接口配置指南”一章。

透明模式下的 ASA 5508-X 至 ASA 5555-X、ISA 3000（软件模块）

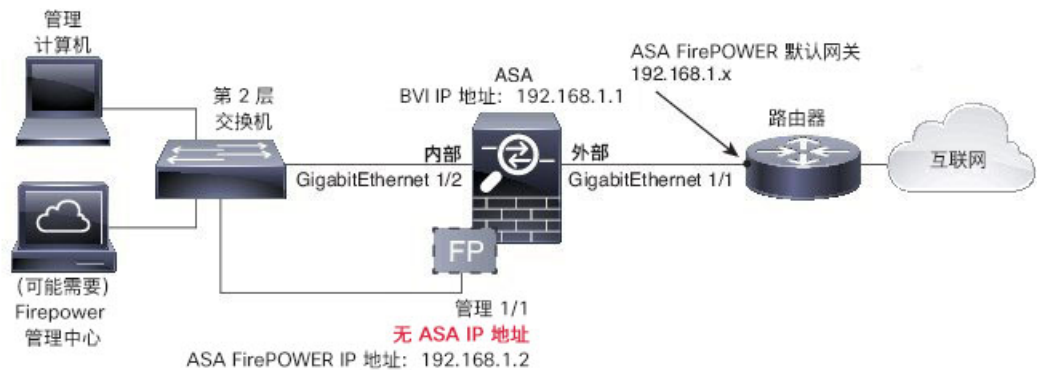
这些模块将 ASA FirePOWER 模块作为软件模块来运行，而且 ASA FirePOWER 模块与 ASA 共享管理 0/0 或管理 1/1 接口（取决于您的型号）。

进出 ASA FirePOWER 模块的所有管理流量必须进入和离开管理接口。ASA FirePOWER 模块还需要访问互联网。

下图显示针对配备 ASA FirePOWER 模块的 ASA 5500-X 或 ISA 3000 的建议网络部署：



如果不使用内部路由器，可通过内部接口（使用 BVI IP 地址）管理 ASA，而不使用管理接口进行 ASA 管理：



注释 若有额外接口可分配到内部桥接组来配置“软交换机”，可避免使用外部交换机。请务必将所有桥接组接口设置为同一安全级别、允许相同的安全通信，并为每个桥接组成员配置 NAT。有关更多信息，请参阅“ASA 接口配置指南”一章。

将 ASA FirePOWER 模块注册到管理中心

要将模块注册到 Firepower/FireSIGHT 管理中心，必须访问 ASA FirePOWER 模块 CLI。首次访问 CLI 时，系统会提示您输入基本配置参数。此外，还必须将模块添加到管理中心。

注：

- 如果希望使用 ASDM 来管理模块，请跳过此部分并参阅 [为 ASDM 管理配置 ASA FirePOWER 模块，第 106 页](#)。
- 如果您需要将模块管理从一个管理中心移到另一个，请首先从管理中心的资产中删除该设备。然后，使用 `configure manager add` 命令，以指向新的管理中心。然后您可以从新的管理中心完成注册。此过程可确保明确的交接。

访问 ASA FirePOWER CLI

要访问 ASA FirePOWER CLI，可以使用以下方法之一。

过程

步骤 1 控制台端口：

- ASA 5585-X - 此型号包括适用于 ASA FirePOWER 模块的专用控制台端口。需要使用随附的 DB-9 至 RJ-45 串行电缆和/或自备的 USB 串口适配器。
- 所有其他型号 - 使用随附的 DB-9 至 RJ-45 串行电缆和/或自备的 USB 串行适配器连接到 ASA 控制台。ASA 5508-X/5516-X 还配备微型 USB 控制台端口。有关使用 USB 控制台端口的说明，请参阅[硬件指南](#)。

在 ASA CLI，发起与 ASA FirePOWER 模块的会话：

```
session sfr
```

另请参阅[从 ASA 向软件模块发起会话](#)，第 119 页。

步骤 2 SSH：

您可以连接到模块默认 IP 地址（请参阅[ASA FirePOWER 默认设置](#)，第 99 页），也可以使用 ASA 上的 ASDM 来更改管理 IP 地址，再使用 SSH 进行连接：

在 ASDM 中，依次选择 **Wizards > Startup Wizard**，然后按照向导逐步转到 **ASA FirePOWER Basic Configuration**，在此可设置 IP 地址、掩码和默认网关。

配置 ASA FirePOWER 基本设置

首次访问 ASA FirePOWER 模块 CLI 时，系统会提示您设置基本配置参数。如果您使用的不是 ASDM，还必须将该模块添加到 Firepower/FireSIGHT 管理中心。

开始之前

根据[访问 ASA FirePOWER CLI](#)，第 104 页访问模块 CLI。

过程

步骤 1 在 ASA FirePOWER CLI，使用用户名 **admin** 进行登录。

如果这是您首次登录，请使用默认密码。请参阅[ASA FirePOWER 默认设置](#)，第 99 页。

步骤 2 根据提示完成系统配置。

将以下网络设置用于推荐网络部署的 ASA FirePOWER 模块 ([在网络中部署 ASA FirePOWER 模块](#)，第 99 页)：

- 管理接口: 192.168.1.2
- 管理子网掩码: 255.255.255.0
- 网关 IP: 192.168.1.1

示例:

```
System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat password>
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(Wait for the system to reconfigure itself.)
```

This sensor must be managed by a Defense Center. A unique alphanumeric registration key is always required. In most cases, to register a sensor to a Defense Center, you must provide the hostname or the IP address along with the registration key.

```
'configure manager add [hostname | ip address ] [registration key ]'
```

However, if the sensor and the Defense Center are separated by a NAT device, you must enter a unique NAT ID, along with the unique registration key.

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Defense Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Defense Center.

步骤 3 将 ASA FirePOWER 模块注册到管理中心:

```
> configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key [nat_id]
```

其中:

- {hostname | IPv4_address | IPv6_address | DONTRESOLVE} 指定管理中心的完全限定主机名或 IP 地址。如果不能直接对管理中心寻址, 请使用 DONTRESOLVE。
- reg_key 是将 ASA FirePOWER 模块注册到管理中心所需的唯一字母数字注册密钥。
- nat_id 是注册过程中管理中心与 ASA FirePOWER 模块之间使用的可选字母数字字符串。如果主机名设置为 DONTRESOLVE, 此项为必填项。

步骤 4 关闭控制台连接。对于软件模块, 请输入:

```
> exit
```

为 ASDM 管理配置 ASA FirePOWER 模块

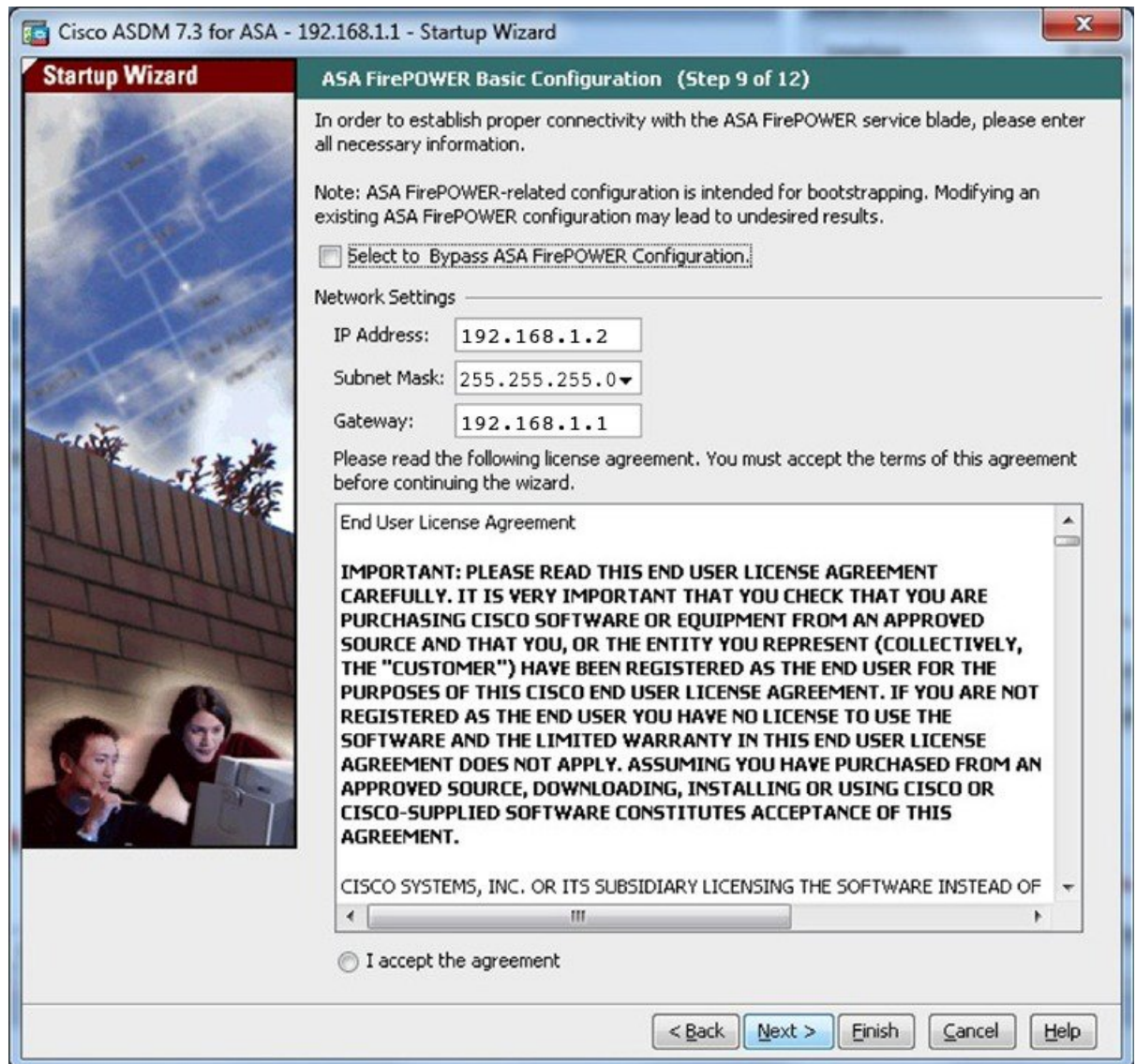
并非所有版本/型号组合都支持；请核实与您的型号和版本的[兼容性](#)。

ASDM 可在 ASA 背板上更改 ASA FirePOWER 模块 IP 地址，但所有进一步管理都需要在 ASDM 接口和可访问该模块的管理接口之间进行网络访问。

要使用 ASDM 管理该模块，请启动 ASDM 并运行启动向导。

过程

- 步骤 1** 在连接到 ASA 的计算机上，启动网络浏览器。
- 步骤 2** 在 Address 字段中输入以下 URL：<https://192.168.1.1/admin>。此时将出现思科 ASDM 网页。
- 步骤 3** 点击以下可用选项之一：**安装 ASDM 启动程序 (Install ASDM Launcher)**、**运行 ASDM (Run ASDM)** 或 **运行启动向导 (Run Startup Wizard)**。
- 步骤 4** 根据您选择的选项，按照屏幕上的说明启动 ASDM。系统将显示思科 ASDM-IDM 启动程序。
注释 如果点击 ASDM 安装启动程序，有些情况下需要根据[为 ASDM 安装身份证书](#)为 ASA 安装身份证书并为 ASA FirePOWER 模块安装单独的证书。
- 步骤 5** 将用户名和密码字段留空，然后点击**确定 (OK)**。系统将显示 ASDM 主窗口。
- 步骤 6** 若系统提示您提供已安装 ASA Firepower 模块的 IP 地址，请取消对话框。您首先必须使用启动向导 (Startup Wizard) 设置正确的模块 IP 地址。
- 步骤 7** 依次选择 **Wizards > Startup Wizard**。
- 步骤 8** 根据需要配置其他 ASA 设置或跳过屏幕，直到到达 **ASA Firepower Basic Configuration** 屏幕。



使用默认配置设置如下值:

- IP 地址 (IP Address) - 192.168.1.2
- 子网掩码 (Subnet Mask) - 255.255.255.0
- 网关 (Gateway) - 192.168.1.1

步骤 9 点击 I accept the agreement, 然后点击 **Next** 或 **Finish** 完成向导。

步骤 10 退出 ASDM, 然后重新启动。在 **Home** 页面上应可以看到 **ASA Firepower** 选项卡。

配置 ASA FirePOWER 模块

在 ASA FirePOWER 模块中配置安全策略，然后配置 ASA 以便向该模块发送流量。

在 ASA FirePOWER 模块上配置安全策略

安全策略控制模块提供的服务，如下一代 IPS 过滤和应用过滤。可以在 ASA FirePOWER 模块上使用以下任一方法配置安全策略。

FireSIGHT 管理中心

使用 Web 浏览器打开 https://DC_address，其中 *DC_address* 是在 [配置 ASA FirePOWER 基本设置，第 104 页](#) 中定义的管理器的 DNS 名称或 IP 地址。例如，<https://dc.example.com>。

或者，在 ASDM 中依次选择 **Home > ASA FirePOWER Status**，然后点击控制面板底部的链接。

有关 ASA FirePOWER 配置的详细信息，请参阅管理中心联机帮助、*FireSIGHT* 系统用户指南 5.4 或 *Firepower* 管理中心配置指南 6.0（可通过<http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html>获取）。

ASDM

在 ASDM 中，依次选择 **Configuration > ASA FirePOWER Configuration**。

有关 ASA FirePOWER 配置的详细信息，请参阅 ASDM 中该模块的联机帮助、*ASA FirePOWER* 模块用户指南 5.4 或 *ASA FirePOWER* 本地管理配置指南 6.0（可通过<http://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html>获取）。

将流量重定向到 ASA FirePOWER 模块

对于内联模式和内联分路（仅监控）模式，应将服务策略配置为将流量重定向至此模块。如果希望使用被动仅监控模式，可配置流量重定向接口来绕过 ASA 策略。

以下主题介绍如何配置这些模式。

配置内联模式或内联分路仅监控模式

通过创建标识要发送的特定流量的服务策略，将流量重定向到 ASA FirePOWER 模块。在此模式下，在流量被重定向至此模块之前，系统会向流量应用访问规则等 ASA 策略。

开始之前

- 如果有活动的服务策略正在将流量重定向到 IPS 或 CX 模块（已替换为 ASA FirePOWER），则在配置 ASA FirePOWER 服务策略之前必须删除该策略。
- 请务必在 ASA 和 ASA FirePOWER 模块上配置一致的策略。两种策略均应反映流量的内联模式或内联分路模式。

- 在多情景模式下，请在每个安全情景中执行此操作步骤。

过程

步骤 1 依次选择配置 > 防火墙 > 服务策略规则。

步骤 2 依次选择添加 > 添加服务策略规则。

步骤 3 选择是向特定接口应用此策略还是全局应用此策略，并点击 **Next**。

步骤 4 配置流量匹配。例如，可以匹配 **Any Traffic**，以便将通过入站访问规则的所有流量重定向到模块。或者，也可以基于端口、ACL（源和目标条件）或现有流量类定义更严格的条件。其他选项对于此策略的用处不大。完成流量类定义后，点击下一步 (**Next**)。

步骤 5 在“规则操作”页面上，点击 **ASA FirePOWER 检测** 选项卡。

步骤 6 选中为此流量启用 **ASA FirePOWER** 复选框。

步骤 7 在 If ASA FirePOWER Card Fails 区域中，点击以下选项之一：

- **Permit traffic** - 设定 ASA 在模块不可用时允许所有流量通过，不进行检测。
- **Close traffic** - 设定 ASA 在模块不可用时阻拦所有流量。

步骤 8 （可选）选中 **Monitor-only** 以将流量的只读副本发送到模块（内联分路模式）。

默认情况下，流量在内联模式下进行发送。请务必在 ASA 和 ASA FirePOWER 上配置一致的策略。两种策略均应反映流量的内联或仅监控模式。

步骤 9 点击 **Finish**，然后点击 **Apply**。

请重复此操作步骤，以根据需要配置其他流量。

配置被动流量转发

如果要在被动仅监控模式下使用模块，使模块获得流量副本且该模块或 ASA 都不会影响网络，请配置一个流量转发接口并将该接口连接到交换机上的 SPAN。有关详细信息，请参阅 [ASA FirePOWER 被动仅监控流量转发模式](#)，第 95 页。

以下指导原则说明此部署模式的要求：

- ASA 必须处于单情景和透明模式下。
- 可将最多 4 个接口配置为流量转发接口。其他 ASA 接口可正常使用。
- 流量转发接口必须是物理接口，而不能是 VLAN 或 BVI。物理接口也不能关联任何 VLAN。
- 不能对 ASA 流量使用流量转发接口；无法对它们命名或无法为 ASA 功能（包括故障切换或仅管理）配置它们。
- 无法同时为 ASA FirePOWER 流量配置流量转发接口和服务策略。

过程

步骤 1 为要用于流量转发的物理接口输入接口配置模式。

interface physical_interface

示例:

```
hostname(config)# interface gigabitethernet 0/5
```

步骤 2 删除为该接口配置的所有名称。如有任何 ASA 配置正在使用此接口，该配置将被删除。无法在已命名的接口上配置流量转发。

no nameif

步骤 3 启用流量转发。

traffic-forward sfr monitor-only

注释 可以忽略关于仅用于演示目的的流量转发的所有警告。这是支持的生产模式。

步骤 4 启用接口。

no shutdown

对任意其他接口重复此操作步骤。

示例

以下示例将 GigabitEthernet 0/5 设为流量转发接口:

```
interface gigabitethernet 0/5
  no nameif
  traffic-forward sfr monitor-only
  no shutdown
```

启用强制网络门户以执行主动身份验证

ASA FirePOWER 包括允许您收集用户 ID 信息的身份策略。通过收集用户身份信息，可以为特定用户或用户组定制访问控制规则，从而基于用户选择性地允许和禁止访问。此外，还可以基于用户身份分析流量。

对于 HTTP/HTTPS 连接，可以定义通过主动身份验证收集用户 ID 的身份规则。如果要实施主动身份验证身份规则，必须在 ASA 上启用强制网络门户充当身份验证代理端口。当连接匹配请求主动身份验证的身份规则时，ASA FirePOWER 模块会将身份验证请求重定向到 ASA 接口 IP 地址/强制网络门户。默认端口为 885，可以对此进行更改。

如果未对身份验证代理启用强制网络门户，则只能使用被动身份验证。

开始之前

- 此功能仅可在路由模式下使用，并且仅可用于 ASA FirePOWER 6.0+。
- 在多情景模式下，请在每个安全情景中执行此操作步骤。

过程

步骤 1 依次选择 **Tools > Command Line Tool**。

步骤 2 启用强制网络门户。

```
captive-portal {global | interface name} [port number]
```

其中：

- **global** 对于所有接口全局启用强制网络门户。
- **interface name** 仅对指定接口启用强制网络门户。您可以多次输入该命令，以便在多个接口上启用该命令。如果仅将一个接口子集的流量重定向到 ASA FirePOWER 模块，可以使用此方法。
- **port number** 选择性地指定身份验证端口。如果未包含该关键字，则使用端口 885。如果包括该关键字，则端口号必须为 1025 或更高。

示例：

例如，要在端口 885 上全局启用强制网络门户，请输入以下信息：

```
ciscoasa(config)# captive-portal global  
ciscoasa(config)#
```

步骤 3 在 ASA FirePOWER 身份策略中，请确保主动身份验证设置指定的端口与您为强制网络门户配置的端口相同，并配置启用主动身份验证所需的其他设置。

管理 ASA FirePOWER 模块

本节包括帮助您管理模块的操作步骤。

安装或重新映像模块

本节介绍如何安装或重新映像软件或硬件模块。

安装或重新映像软件模块

如果购买的 ASA 配备 ASA FirePOWER 模块，则已预安装模块软件和所需的固态硬盘 (SSD)，可以进行配置。如果要向现有的 ASA 中添加 ASA FirePOWER 软件模块或需要更换 SSD，您需要根据此操作步骤安装 ASA FirePOWER 启动软件，对 SSD 分区，并安装系统软件。

重新映像模块的操作步骤与此相同，但应首先卸载 ASA FirePOWER 模块。如果更换 SSD，需要重新映像系统。

有关如何实际安装 SSD 的信息，请参阅 ASA 硬件指南。

开始之前

- 除去启动软件所占空间外，闪存 (disk0) 上的可用空间至少应为 3GB。
- 在多情景模式下，请在系统执行空间中执行此操作步骤。
- 您必须关闭可能运行的任何其他软件模块；ASA 每次可运行一个软件模块。必须从 ASA CLI 执行此操作。例如，以下命令关闭并卸载 IPS 软件模块，然后重新加载 ASA；用于删除 CX 模块的命令也是一样的，除非使用 **cxsc** 关键字代替 **ips**。

sw-module module ips shutdown sw-module module ips uninstall reload

在重新映像 ASA FirePOWER 模块时，请使用相同的关闭和卸载命令来删除旧映像。例如 `sw-module module sfr uninstall`。

- 如果有活动服务策略将流量重定向至 IPS 或 CX 模块，则必须删除该策略。例如，如果策略为全局策略，则使用 **no service-policy ips_policy global**。如果服务策略包括其他要维护的规则，只需从相关的策略映射删除重定向命令；或者，如果重定向是类的唯一操作，则从整个流量类删除。可以使用 CLI 或 ASDM 删除策略。
- 从 Cisco.com 获取 ASA FirePOWER 启动映像和系统软件包。

过程

步骤 1 将启动映像下载到 ASA。请勿传输系统软件；系统软件稍后会下载到 SSD。您有以下选择：

- ASDM - 首先，将启动映像下载至工作站，或将其放在 FTP、TFTP、HTTP、HTTPS、SMB 或 SCP 服务器上。然后，在 ASDM 中，依次选择 **Tools > File Management**，然后选择适当的 **File Transfer** 命令，可以是 **Between Local PC and Flash** 或 **Between Remote Server and Flash**。将启动软件传输到 ASA 中的 disk0。
- ASA CLI - 首先，将启动映像放在 TFTP、FTP、HTTP 或 HTTPS 服务器上，然后使用 **copy** 命令将其下载至闪存。以下示例使用 TFTP。

```
ciscoasa# copy tftp://10.1.1.89/asasfr-5500x-boot-5.4.1-58.img
disk0:/asasfr-5500x-boot-5.4.1-58.img
```

步骤 2 从 Cisco.com 下载 ASA FirePOWER 系统软件，将它们保存到 ASA FirePOWER 管理接口可访问的 HTTP、HTTPS 或 FTP 服务器。请勿将其下载到 ASA 上的 disk0。

步骤 3 通过输入以下命令设置 ASA FirePOWER 模块启动映像在 ASA disk0 中的位置：

```
sw-module module sfr recover configure image disk0: file_path
```

示例：


```
hostname# sw-module module sfr recover configure image disk0:asasfr-5500x-boot-5.4.1-58.img
```

如果看到“ERROR: Another service (cxsc) is running, only one service is allowed to run at any time”（错误：正在运行其他服务(cxsc)，无论何时只能运行一个服务）之类的消息，则表示您已配置了不同的软件模块。必须将其关闭并删除，以安装以上“先决条件”一节所述的新模块。

步骤 4 加载 ASA FirePOWER 启动映像：

```
sw-module module sfr recover boot
```

步骤 5 等待约 5-15 分钟，直到 ASA FirePOWER 模块启动，然后打开正在运行的 ASA FirePOWER 启动映像的控制台会话。发起会话后，可能需要按 Enter 键显示登录提示符。默认用户名是 **admin**，默认密码是 **Admin123**。

```
hostname# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

如果模块启动未完成，**session** 命令将失败并提示无法通过 ttyS1 进行连接。请稍后重试。

步骤 6 配置系统，以便可以安装系统软件包：

```
asasfr-boot> setup
```

示例：

```
asasfr-boot> setup
```

```
Welcome to SFR Setup
[hit Ctrl-C to abort]
Default values are inside []
```

系统将提示输入以下信息。请注意，管理地址和网关以及 DNS 信息是要配置的主要设置。

- 主机名 - 最多可达 65 个字母数字字符，不能包含空格。允许使用连字符。
- 网络地址 - 可设置静态 IPv4 或 IPv6 地址，或使用 DHCP（适用于 IPv4）或 IPv6 无状态自动配置。
- DNS 信息 - 必须至少确定一个 DNS 服务器，还可设置域名和搜索域。
- NTP 信息 - 可启用 NTP 并配置 NTP 服务器，以便设置系统时间。

步骤 7 安装系统软件映像：

```
asasfr-boot> system install [noconfirm] url
```

如果不想响应确认消息，请在命令中添加 **noconfirm** 选项。使用 HTTP、HTTPS 或 FTP URL；如果需要用户名和密码，系统将提示您提供这些信息。

安装完成后，系统将重新启动。安装应用组件所需的时间以及启动 ASA FirePOWER 服务所需的时间差别极为明显：高端平台可能需要 10 分钟或更长时间，但低端平台可能需要 60-80 分钟或更长时间。（**show module sfr** 输出应将所有进程状态显示为 Up。）

例如：

```

asasfr-boot> system install http://upgrades.example.com/packages/asasfr-sys-5.4.1-58.pkg
Verifying
Downloading
Extracting
Package Detail
      Description:          Cisco ASA-FirePOWER 5.4.1-58 System Install
      Requires reboot:      Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
(press Enter)
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2014):

The system is going down for reboot NOW!
Console session with module sfr terminated.

```

步骤 8 打开 ASA FirePOWER 模块的会话。因为登录的是全功能模块，系统将会显示不同的登录提示。

ciscoasa# session sfr console

示例：

```

ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Sourcefire ASA5555 v5.4.1 (build 58)
Sourcefire3D login:

```

步骤 9 请参阅 [配置 ASA FirePOWER 基本设置](#)，第 104 页以完成设置。

重新映像 5585-X ASA FirePOWER 硬件模块

如果出于任何原因需要重新映像 ASA 5585-X 中的 ASA FirePOWER 硬件模块，需要按先启动映像再系统软件包的顺序安装它们。必须安装这两个软件包，系统才能正常运行。在正常情况下，不需要重新映像系统即可安装升级软件包。

要安装启动映像，需要登录模块的控制台端口从 ASA FirePOWER SSP 的端口 0 对启动映像执行 TFTP 启动。因为管理 0 端口位于第一个插槽的一个 SSP 上，所以也称为管理 1/0 端口；但是，ROMMON 将其识别为管理 0 或管理 0/1 端口。



注释 在模块重新启动期间（包括模块重新映像期间的重新启动），ASA 5585-X ASA FirePOWER 硬件模块上的接口将丢弃长达 30 秒内的流量。

开始之前

要完成 TFTP 启动，必须执行以下操作：

- 将启动映像和系统软件包放到 TFTP 服务器上，通过 ASA FirePOWER 模块上的管理 1/0 接口可以访问该服务器。
- 将管理 1/0 接口连接至网络。必须使用此接口对启动映像执行 TFTP 启动。

过程

步骤 1 连接至模块控制台端口。

步骤 2 重新加载系统：

system reboot

步骤 3 系统提示时，按 Esc 键中断启动。如果看到 GRUB 多操作系统启动程序开始启动系统，则表明等待时间过长。

这样，您就可以看到 ROMMON 提示符。

步骤 4 在 ROMMON 提示符处输入：

set

配置以下参数：

- ADDRESS - 模块的管理 IP 地址。
- SERVER - TFTP 服务器的 IP 地址。
- GATEWAY - TFTP 服务器的网关地址。如果 TFTP 服务器直接连接至 Management1/0，请使用 TFTP 服务器的 IP 地址。如果 TFTP 服务器和管理地址位于同一子网，则请勿配置网关，否则 TFTP 启动将失败。
- IMAGE - TFTP 服务器上的启动映像路径和映像名称。例如，如果在 TFTP 服务器上将文件放在 tftpboot/images/filename.img 中，则 IMAGE 值为 images/filename.img。

示例：

```
ADDRESS=10.5.190.199
SERVER=10.5.11.170
```

```
GATEWAY=10.5.1.1  
IMAGE=asasfrboot-5.4.1-58.img
```

步骤 5 保存设置：

```
sync
```

步骤 6 发起下载和启动流程：

```
tftp
```

您将看到指示进度的 ! 符号。几分钟后启动完成时，将看到登录提示符。

步骤 7 以 **admin** 身份使用密码 **Admin123** 登录。

步骤 8 配置系统，以便可以安装系统软件包：

```
setup
```

系统将提示输入以下信息。请注意，管理地址和网关以及 DNS 信息是要配置的主要设置。

- 主机名 - 最多可达 65 个字母数字字符，不能包含空格。允许使用连字符。
- 网络地址 - 可设置静态 IPv4 或 IPv6 地址，或使用 DHCP（适用于 IPv4）或 IPv6 无状态自动配置。
- DNS 信息 - 必须至少确定一个 DNS 服务器，还可设置域名和搜索域。
- NTP 信息 - 可启用 NTP 并配置 NTP 服务器，以便设置系统时间。

步骤 9 安装系统软件映像：

```
system install [noconfirm] url
```

示例：

```
asasfr-boot> system install http://upgrades.example.com/packages/asasfr-sys-5.4.1-58.pkg
```

如果不想响应确认消息，请在命令中添加 **noconfirm** 选项。

安装完成后，系统将重新启动。应用组件安装和 ASA FirePOWER 服务启动约需十几分钟。

步骤 10 启动完成后，请以 **admin** 身份使用默认密码登录。请参阅 [ASA FirePOWER 默认设置，第 99 页](#)。

步骤 11 请参阅 [配置 ASA FirePOWER 基本设置，第 104 页](#) 以完成设置。

重置密码

如果忘记管理员用户的密码，则拥有 CLI 配置权限的其他用户可登录并更改该密码。

如果其他用户没有所需的权限，可从 ASA 重置管理员密码。默认密码因软件版本而异；请参阅 [ASA FirePOWER 默认设置，第 99 页](#)。

开始之前

- 在多情景模式下，请在系统执行空间中执行本程序。
- ASA `hw-module` 和 `sw-module` 命令中的 `password-reset` 选项不适用于 ASA FirePOWER。

过程

将用户 `admin` 的模块密码重置为默认值：

session {1 | sfr} do password-reset

对硬件模块使用 `1`，对软件模块使用 `sfr`。

重新加载或重置模块

可从 ASA 重新加载模块，或先对其重置再重新加载。

开始之前

在多情景模式下，请在系统执行空间中执行本程序。

过程

输入以下命令之一：

- 硬件模块 (ASA 5585-X):

hw-module module 1 {reload | reset}

注释 在模块重新启动期间（包括软件升级期间的重新启动），ASA 5585-X ASA FirePOWER 硬件模块上的接口将丢弃长达 30 秒内的流量。

- 软件模块（所有其他型号）：

sw-module module sfr {reload | reset}

关闭模块

关闭模块软件使得模块可以安全断电而不会丢失配置数据。

开始之前

- 在多情景模式下，请在系统执行空间中执行本程序。

- 如果重新加载 ASA，模块不会自动关闭，所以我们建议您先关闭模块再重新加载 ASA。

过程

输入以下命令之一：

- 硬件模块 (ASA 5585-X):
hw-module module 1 shutdown
 - 软件模块（所有其他型号）：
sw-module module sfr shutdown
-

卸载软件模块映像

可卸载软件模块映像及其相关配置。

开始之前

在多情景模式下，请在系统执行空间中执行本程序。

过程

步骤 1 卸载软件模块映像以及关联配置。

sw-module module sfr uninstall

示例：

```
ciscoasa# sw-module module sfr uninstall

Module sfr will be uninstalled. This will completely remove the disk image
associated with the sw-module including any configuration that existed within it.

Uninstall module sfr? [confirm]
```

步骤 2 重新加载 ASA。

reload

您必须重新加载 ASA，才能安装新模块。

从 ASA 向软件模块发起会话

使用 ASA FirePOWER CLI 可配置基本网络设置和排除模块故障。

要从 ASA 访问 ASA FirePOWER 软件模块 CLI，可从 ASA 发起会话。（无法向 5585-X 上运行的硬件模块发起会话。）

可向模块发起会话（使用 Telnet），也可创建虚拟控制台会话。如果控制面板已关闭且无法建立 Telnet 会话，则控制台会话可能有用。在多情景模式下，从系统执行空间发起会话。

在 Telnet 或控制台会话中，会提示您输入用户名和密码。您可以使用 ASA FirePOWER 中配置的任何用户名进行登录。最初，**admin** 用户名是已配置的唯一用户名（且始终可用）。根据映像类型（完整映像或引导映像）和软件版本，初始默认密码有所不同；请参阅[ASA FirePOWER 默认设置](#)，第 99 页。

- Telnet 会话：

session sfr

要退出 ASA FirePOWER CLI 并返回 ASA CLI，请输入可从模块注销的任何命令，例如 **logout** 或 **exit**，或者按 **Ctrl-Shift-6** 和 **x**。

- 控制台会话：

session sfr console

退出控制台会话的唯一途径为同时按 **Ctrl-Shift-6** 和 **x**。从模块注销后，您就可以看到模块登录提示符。



注释

请勿将 **session sfr console** 命令与终端服务器结合使用，其中 **Ctrl-Shift-6** 和 **x** 是用于返回到终端服务器提示符的转义序列。要退出 ASA FirePOWER 控制台并返回 ASA 提示符，也可以使用 **Ctrl-Shift-6** 和 **x** 序列。因此，在此情景下若要退出 ASA FirePOWER 控制台，会一直退出到终端服务器提示符。如果将终端服务器重新连接到 ASA，ASA FirePOWER 控制台会话仍处于活动状态；您永远不会退出到 ASA 提示符。必须使用直接串行连接将控制台返回到 ASA 提示符。出现此情况时，请使用 **session sfr** 命令，而不要使用控制台命令。

升级系统软件

在应用升级之前，请确保 ASA 运行的是新版本所需的最低版本；可能需要先升级 ASA，然后才能升级模块。有关应用升级的详细信息，请参阅管理中心联机帮助：[FireSIGHT 系统用户指南 5.4](#) 或 [Firepower 管理中心配置指南 6.0](#)。

有关 ASDM 管理，可使用 **Configuration > ASA FirePOWER Configuration > Updates** 应用对系统软件和组件的升级。有关详细信息，请在 Updates 页面上点击 **Help**。

监控 ASA FirePOWER 模块

以下主题提供有关监控模块的指南。有关与 ASA FirePOWER 相关的系统日志消息，请参阅系统日志消息指南。ASA FirePOWER 系统日志消息以消息编号 434001 开头。

依次选择 **Tools > Command Line Interface** 以使用监控命令。

显示模块状态

从 Home 页面，可选择 **ASA FirePOWER Status** 选项卡以查看有关模块的信息。这包括模块信息（如型号、序列号、软件版本）和模块状态（如应用名称和状态、数据平面状态和总体状态）。如果已将模块注册到管理中心，可以点击链接打开应用和进一步执行分析和模块配置。

使用 ASDM 管理模块时，还可以使用 **Home > ASA FirePOWER Dashboard** 页面查看有关模块上运行的软件的概要信息、产品更新、许可、系统负载、磁盘使用情况、系统时间以及接口状态。

显示模块统计信息

使用 `show service-policy sfr` 命令来显示包括 `sfr` 命令的每个服务策略的统计信息和状态。可以使用 `clear service-policy` 命令清除计数器。

以下示例显示 ASA FirePOWER 服务策略和当前的统计信息以及模块状态。在仅监控模式下，输入计数器保持为零。

```
ciscoasa# show service-policy sfr

Global policy:
  Service-policy: global_policy
  Class-map: my-sfr-class
    SFR: card status Up, mode fail-close
        packet input 2626422041, packet output 2626877967, drop 0, reset-drop 0, proxied 0
```

分析操作行为（ASDM 管理）

使用 ASA 管理 ASA FirePOWER 模块时，可通过以下页面查看该模块的操作信息：

- **Home > ASA FirePOWER Reporting** - 报告页面提供用于各种模块统计信息的前 10 个控制面板，例如通过该模块的流量的 Web 类别、用户、源和目标。
- **Monitoring > ASA FirePOWER Monitoring** - 这些页面用于监控模块，包括系统日志、任务状态、模块统计信息和实时事件查看器。

监控模块连接

要通过 ASA FirePOWER 模块显示连接，请输入下列命令之一：

- **show asp table classify domain sfr**

显示用于将流量发送到 ASA FirePOWER 模块的 NP 规则。

- **show asp drop**

显示丢弃的数据包。丢弃类型说明如下。

- **show conn**

通过显示“X - inspected by service module”标记表明连接是否正在被转发到模块。

show asp drop 命令可包括以下与 ASA FirePOWER 模块相关的丢弃原因。

丢帧：

- **sfr-bad-tlv-received** - 当 ASA 从 FirePOWER 收到没有 Policy ID TLV 的数据包时发生此情况。如果此 TLV 没有在操作字段中设置的备用/主用位，则必须出现于非控数据包中。
- **sfr-request** - 此帧由 FirePOWER 根据 FirePOWER 上的一条策略请求丢弃，其中 FirePOWER 将操作设置为 Deny Source、Deny Destination 或 Deny Pkt。如果不该丢弃该帧，请查看拒绝流量的模块上的策略。
- **sfr-fail-close** - 数据包已丢弃，因为卡未正常工作且配置的策略为“fail-close”（而不是“fail-open”，该策略即使在卡出现故障的情况下也允许数据包通过）。检查卡状态并尝试重新启动服务或重新启动卡。
- 已为现有流量删除 FirePOWER 配置且无法通过将丢弃现有流量的 FirePOWER 对其进行处理。这种情况十分罕见。
- **sfr-malformed-packet** - 来自 FirePOWER 的数据包包含无效的报头。例如，报头长度可能不正确。
- **sfr-ha-request** - 当安全设备收到 FirePOWER HA 请求数据包但无法对其进行处理，且数据包已丢弃时，此计数器递增。
- **sfr-invalid-encap** - 当安全设备收到具有无效消息报头的 FirePOWER 数据包，且数据包已丢弃时，此计数器递增。
- **sfr-bad-handle-received** - 在来自 FirePOWER 模块的数据包中收到错误的流量句柄，因此丢弃流量。此计数器递增，FirePOWER 流量的句柄在流量持续时间期间已更改，因此在 ASA 上丢弃流量和数据包。
- **sfr-rx-monitor-only** - 当安全设备在仅监控模式下收到 FirePOWER 数据包，且数据包已丢弃时，此计数器递增。

流量丢弃：

- **sfr-request** - FirePOWER 请求终止流量。设置了操作位 0。
- **reset-by-sfr** - FirePOWER 请求终止并重置流量。设置了操作位 1。
- **sfr-fail-close** - 流量已终止，因为卡出现故障且配置的策略为“fail-close”。

ASA FirePOWER 模块的历史

功能	平台版本	描述
<p>ASA 5585-X（所有型号）支持匹配的 ASA FirePOWER SSP 硬件模块。</p> <p>ASA 5512-X 到 ASA 5555-X 支持 ASA FirePOWER 软件模块。</p>	<p>ASA 9.2(2.4)</p> <p>ASA FirePOWER 5.3.1</p>	<p>ASA FirePOWER 模块提供下一代防火墙服务，包括下一代 IPS (NGIPS)、应用可见性与可控性 (AVC)、URL 过滤及高级恶意软件保护 (AMP)。您可以在单情景或多情景模式以及路由或透明模式下使用该模块。</p> <p>引入了以下菜单项：</p> <p>Home > ASA FirePOWER Status Wizards > Startup Wizard > ASA FirePOWER Basic Configuration Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > ASA FirePOWER Inspection</p>
<p>ASA 5506-X 支持 ASA FirePOWER 软件模块，包括支持在 ASDM 中配置该模块</p>	<p>ASA 9.3(2)</p> <p>ASDM 7.3(3)</p> <p>ASA FirePOWER 5.4.1</p>	<p>可以在 ASA 5506-X 上运行 ASA FirePOWER 软件模块。可以使用 FireSIGHT 管理中心管理该模块，也可以使用 ASDM 进行管理。</p> <p>引入了以下屏幕：</p> <p>Home > ASA FirePOWER Dashboard、Home > ASA FirePOWER Reporting、Configuration > ASA FirePOWER Configuration（包括子页面）、Monitoring > ASA FirePOWER Monitoring（包括子页面）。</p>
<p>使用流量重定向接口的 ASA FirePOWER 被动仅监控模式</p>	<p>ASA 9.3(2)</p> <p>ASA FirePOWER 5.4.1</p>	<p>现在可以将流量转发接口配置为向模块发送流量，以代替使用服务策略。在这种模块下，模块和 ASA 都不会影响流量。</p> <p>完全支持了以下命令：traffic-forward sfr monitor-only。仅可在 CLI 中进行此配置。</p>
<p>支持通过 ASDM 管理 5506H-X、5506W-X、5508-X 和 5516-X 的模块。</p>	<p>ASA 9.4(1)</p> <p>ASDM 7.4(1)</p> <p>ASA FirePOWER 5.4.1</p>	<p>您可以使用 ASDM，而不是 FireSIGHT 管理中心来管理模块。</p> <p>无新增菜单项或命令。</p>
<p>支持通过 ASDM 管理 5512-X 到 5585-X 的模块。</p>	<p>ASA 9.5.(1.5)</p> <p>ASDM 7.5(1.112)</p> <p>ASA FirePOWER 6.0</p>	<p>您可以使用 ASDM，而不是 Firepower 管理中心（以前称为 FireSIGHT 管理中心）来管理模块。</p> <p>无新增菜单项或命令。</p>

功能	平台版本	描述
ASA FirePOWER 6.0 中使用强制网络门户的主动身份验证。	ASA 9.5.(2) ASA FirePOWER 6.0	从 ASA FirePOWER 6.0 开始，要使用身份策略启用主动身份验证，需使用强制网络门户功能。 引入或修改了以下命令： captive-portal 、 clear configure captive-portal 和 show running-config captive-portal 。
ASA 5506-X 和 ASA 5512-X 系列不支持 9.10(1) 版本的 ASA FirePOWER 模块	9.10(1)	由于内存限制，ASA 5506-X 和 5512-X 系列不再支持 9.10(1) 及更高版本的 ASA FirePOWER 模块。您必须保持 9.9(x) 或更低版本以继续使用该模块。仍然支持其他模块类型。如果升级到 9.10(1)，则将流量发送到 FirePOWER 模块的 ASA 配置将被清除；请确保在升级之前备份配置。SSD 上的 FirePOWER 映像及其配置保持不变。如果想要降级，可以从备份复制 ASA 配置以恢复功能。



第 8 章

思科 Umbrella

您可以配置设备将 DNS 请求重定向至思科 Umbrella，以便将您在思科 Umbrella 中定义的 FQDN 策略应用于用户连接。以下主题介绍如何配置 Umbrella 连接器将设备与思科 Umbrella 进行集成。

- [关于思科 Umbrella 连接器，第 125 页](#)
- [思科 Umbrella 连接器的许可要求，第 126 页](#)
- [思科 Umbrella 的使用指南和限制，第 126 页](#)
- [配置思科 Umbrella 连接器，第 128 页](#)
- [监控 Umbrella 连接器，第 132 页](#)
- [思科 Umbrella 连接器的历史记录，第 135 页](#)

关于思科 Umbrella 连接器

如果使用思科 Umbrella，可以配置思科 Umbrella 连接器，将 DNS 查询重定向到思科 Umbrella。这允许思科 Umbrella 识别对黑或灰名单域名的请求，并应用基于 DNS 的安全策略。

Umbrella 连接器是系统 DNS 检测的一部分。如果现有 DNS 检测策略映射决定根据 DNS 检测设置阻止或丢弃请求，则该请求不会转发至思科 Umbrella。因此，有两条保护防线：本地 DNS 检测策略和思科 Umbrella 基于云的策略。

将 DNS 查询请求重定向到思科 Umbrella 时，Umbrella 连接器会添加 EDNS（DNS 扩展机制）记录。EDNS 记录包括设备标识符信息、组织 ID 和客户端 IP 地址。基于云的策略可以使用 FQDN 信誉以及这些标准来控制访问。还可以选择使用 DNSCrypt 加密 DNS 请求，以确保用户名和内部 IP 地址的隐私性。

思科 Umbrella 企业安全策略

在基于云的思科 Umbrella 企业安全策略中，可以基于 DNS 查询请求中的完全限定域名 (FQDN) 的信誉来控制访问。企业安全策略可以强制执行以下操作之一：

- 白名单 - 如果对某个 FQDN 未设置阻止规则，并且思科 Umbrella 确定其属于非恶意站点，则系统会返回该站点的实际 IP 地址。这是正常的 DNS 查询行为。

- 灰名单 - 如果对某个 FQDN 未设置阻止规则，并且思科 Umbrella 确定其属于恶意站点，则 DNS 应答会返回 Umbrella 智能代理的 IP 地址。然后，该代理可以检查 HTTP 连接，并应用 URL 过滤。必须确保从思科 Umbrella 控制面板（安全设置 > 启用智能代理）启用智能代理。
- 黑名单 - 如果明确阻止 FQDN，或思科 Umbrella 确定其属于恶意站点，则 DNS 应答会返回已阻止连接的 Umbrella 云登录页面的 IP 地址。

思科 Umbrella 注册

在设备上配置 Umbrella 连接器时，它会在云中向思科 Umbrella 注册。在注册流程中，分配设备 ID，用于确定以下任一项：

- 单情景模式下的一个独立设备。
- 单情景模式下的一个高可用性对。
- 单情景模式下的一个集群。
- 多情景独立设备中的一个安全情景。
- 高可用性对的一个安全情景。
- 集群的一个安全情景。

注册后，设备详细信息将显示在思科 Umbrella 控制面板上。然后，可以更改向设备附加的策略。在注册期间，使用配置中指定的策略，或者分配默认策略。可以向多个设备分配同一 Umbrella 策略。指定策略后收到的设备 ID 不同于未指定策略情况下收到的设备 ID。

思科 Umbrella 连接器的许可要求

要使用思科 Umbrella 连接器，必须拥有 3DES 许可证。如果正在使用智能许可，必须启用账户的导出控制功能。

思科 Umbrella 门户具有单独的许可要求。

思科 Umbrella 的使用指南和限制

情景模式

- 在多情景模式下，可在每个情景下配置 Umbrella 连接器。每个情景都有单独的设备 ID，并且在思科 Umbrella 连接器控制面板中被表示为独立设备。设备名称是在情景中配置的主机名，再加上硬件型号和情景名称。例如，CiscoASA-ASA5515-Context1。

故障切换

- 高可用性对中的主用设备向思科 Umbrella 将此高可用性对注册为单一设备。两个对等体使用根据其序列号形成的同一设备 ID: *primary-serial-number_secondary-serial-number*。对于多情景模式，安全情景的每一对都被视为单一设备。启用思科 Umbrella 前，必须配置高可用性，并且设备必须成功建立高可用性组（即使备用设备目前处于故障状态），否则注册将以失败告终。

集群

- 集群主装置在思科 Umbrella 中作为单一设备注册该集群。所有对等体使用同一设备 ID。对于多情景模式，该集群中的安全情景在所有对等体中均被视为单一设备。

其他规定

- 仅直通流量中的 DNS 请求重定向到思科 Umbrella。系统自身发起的 DNS 请求永远不会重定向到思科 Umbrella。例如，基于 FQDN 的访问控制规则以及其他命令或配置设置中使用的任何 FQDN 永远无法根据 Umbrella 策略解析。
- 思科 Umbrella 连接器适用于直通流量中任何 DNS 请求。然而，只有 DNS 响应用于 HTTP/HTTPS 连接时，黑名单和灰名单操作才有效，因为返回的 IP 地址是针对网站的。非 HTTP/HTTPS 连接的任何列入黑名单或灰名单的地址的操作将失败或以误导性方式完成。例如，针对列入黑名单的 FQDN 执行 ping 操作会导致对托管思科 Umbrella 云阻止页面的服务器执行 ping 操作。



注释 思科 Umbrella 试图智能地识别可能是非 HTTP/HTTPS 的 FQDN，并且对于列入灰名单的域名的 FQDN，不向智能代理返回 IP 地址。

- 系统仅向思科 Umbrella 发送 DNS/UDP 流量。如果启用 DNS/TCP 检测，则系统不会向思科 Umbrella 发送任何 DNS/TCP 请求。然而，DNS/TCP 请求不会增加 Umbrella 旁路计数器的读数。
- 如果启用 Umbrella DNSCrypt 检测，则系统会使用 UDP/443 进行加密会话。必须将 UDP/443 和 UDP/53 包含在为思科 Umbrella 应用 DNS 检测的类映射中，以确保 DNSCrypt 正常运行。UDP/443 和 UDP/53 均包含在 DNS 的默认检测类中，但如果创建一个自定义类，请确保所定义的 ACL 将这两个端口都包含到匹配类中。
- DNSCrypt 仅对证书更新握手使用 IPv4。但是，DNSscrypt 会加密 IPv4 和 IPv6 流量。
- 对于给定连接，思科 Umbrella 和 ASA FirePOWER 处理不兼容。如果想要同时使用这两种服务，则必须从 ASA FirePOWER 处理中排除 UDP/53 和 UDP/443。例如，如果目前正在将所有流量重定向到 ASA FirePOWER 模块，必须更新类以使用访问列表匹配。访问列表应首先拒绝目的端口 UDP/53 和 UDP/443 上的 Umbrella 服务器的任何连接，然后允许任何源流向到任何目的地。ACL 和匹配语句应与以下内容类似：

```
access-list sfr extended deny udp any host 208.67.220.220 eq domain
access-list sfr extended deny udp any host 208.67.220.220 eq 443
access-list sfr extended permit ip any any
```

```
class-map sfr
  match access-list sfr
  policy-map global_policy
    class sfr
      sfr fail-open
```

- 必须有到可访问 api.opendns.com（注册仅使用 IPv4）的互联网的 IPv4 路由。同时，还必须要有到以下 DNS 解析器的路由，且访问规则必须允许流向这些主机的 DNS 流量。这些路由可以经过数据接口或管理接口；任何有效路由均适用于注册和 DNS 解析。
 - 208.67.220.220
 - 2620:119:53::53
- 要取消注册设备，请先删除 Umbrella 配置，然后从思科 Umbrella 控制面板中删除设备。
- 使用 IP 地址而不使用 FQDN 的任何 Web 请求均会绕过思科 Umbrella。此外，如果漫游客户端从不同于通过启用 Umbrella 的设备的 WAN 连接获取 DNS 解析，则使用这些解析的连接将绕过思科 Umbrella。
- 如果用户具有 HTTP 代理，则该代理可能会执行 DNS 解析，并且解析不会通过思科 Umbrella。
- 不支持 NAT DNS46 和 DNS64。无法在 IPv4 与 IPv6 寻址之间转换 DNS 请求。
- EDNS 记录将同时包括 IPv4 和 IPv6 主机地址。
- 如果客户端使用基于 HTTPS 的 DNS，云安全服务将不会检测 DNS 和 HTTP/HTTPS 流量。

配置思科 Umbrella 连接器

可以配置设备，以与云中的思科 Umbrella 交互。系统将 DNS 查询请求重定向到思科 Umbrella，由后者应用基于云的企业级安全性完全限定域名 (FQDN) 策略。对于恶意或可疑流量，可以从站点阻止用户或将其重定向至可以根据基于云的策略执行 URL 过滤的智能代理。

以下程序介绍用于配置思科 Umbrella 连接器的端到端流程。

开始之前

在多情景模式下，请在应使用思科 Umbrella 的每个安全情景中执行此程序。

过程

步骤 1 在思科 Umbrella（地址：<https://umbrella.cisco.com>）上建立账户。

步骤 2 从思科 Umbrella 注册服务器安装 CA 证书，第 129 页。

设备注册使用 HTTPS，这要求安装根证书。

步骤 3 如果尚未启用，则配置 DNS 服务器，并在接口上启用 DNS 查询。

在 **配置 > 设备管理 > DNS > DNS 客户端页面配置设置**。

步骤 3 输入信任点名称，例如 `ctx1` 或 `umbrella_server`。

步骤 4 选择粘贴 PEM 格式的证书，然后将证书粘贴到框中。

如果包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行，这就无关紧要了。

步骤 5 点击 **Install Certificate**。

在设备上创建证书。需要刷新视图以查看列出的信任点。

配置 Umbrella 连接器全局设置

Umbrella 全局设置主要定义在思科 Umbrella 中注册设备时所需的 API 令牌。全局设置不足以启用 Umbrella。您还必须在 DNS 检测策略映射中启用 Umbrella，如在 [DNS 检测策略映射中启用 Umbrella](#)，第 131 页 所述。

开始之前

- 登录思科 Umbrella 网络设备控制面板 (<https://login.umbrella.com/>)，获取适用于您的组织的网络设备 API 令牌。此令牌是十六进制字符串，例如 `AABBA59A0BDE1485C912AFE`。在 Umbrella 中，可以通过选择 **部署 > 核心身份 > 网络设备** 找到。如果 API 令牌尚未显示在页面上，请点击页面右上角的 **API 令牌** 按钮。
- 安装思科 Umbrella 注册服务器证书。

过程

步骤 1 依次选择 **配置 > 防火墙 > 对象 > Umbrella**。

步骤 2 选择启用 **Umbrella**。

步骤 3 在令牌字段中输入 API 令牌。

步骤 4（可选。）如果想要在 DNS 检测策略映射中启用 DNSCrypt DNS，则可以选择配置用于证书验证的 DNSCrypt 提供商公钥。如果未配置密钥，则使用当前默认分布式公共密钥进行验证。

密钥是一个 32 字节的十六进制值。在 ASCII 中输入十六进制值，每个 2 字节使用一个冒号分隔符。密钥长度为 79 个字节。从思科 Umbrella 获取此密钥。

默认密钥为：

```
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
```

要恢复为使用默认公钥，请从公钥字段删除该密钥。

步骤 5（可选。）当服务器没有响应时，选择 **EDNS 超时** 并更改在删除从客户端至 Umbrella 服务器的连接之前的空闲超时。

超时采用时:分:秒的格式，可以介于 0:0:0 到 1193:0:0 之间。默认值为 0:02:00（2 分钟）。

在 DNS 检测策略映射中启用 Umbrella

配置全局 Umbrella 设置不足以注册设备和启用 DNS 查询重定向。必须添加 Umbrella 作为活动 DNS 检测的一部分。

可以通过将 Umbrella 添加到 `preset_dns_map` DNS 检测策略映射中实现全局启用 Umbrella。

但是，如果已自定义 DNS 检测并对不同流量类应用不同的检测策略映射，则必须在想要获取服务的每个类上启用 Umbrella。

以下程序说明如何全局实施 Umbrella。如果已自定义 DNS 策略映射，请参阅 [配置 DNS 检测策略映射](#)，第 330 页。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > DNS。

步骤 2 双击 `preset_dns_map` 检测映射，以对其进行编辑。

步骤 3 点击 **Umbrella 连接** 选项卡，并在云中启用与思科 Umbrella 的连接。

- **Umbrella - 启用思科 Umbrella。** 可以选择在 **Umbrella 标记** 字段中指定要应用于设备的思科 Umbrella 策略的名称。如果未指定策略，系统将应用默认策略。注册后，Umbrella 设备 ID 会显示在标签旁边。
- **启用 Dnscrypt - 启用 DNSCrypt，** 为设备和思科 Umbrella 之间的连接加密。启用 DNSCrypt 将使用 Umbrella 解析器启动密钥交换线程。密钥交换线程每小时执行与解析器的握手，并使用新密钥来更新设备。由于 DNSCrypt 使用 UDP/443，您必须确保用于 DNS 检测的类映射包含该端口。请注意，默认检测类已在 DNS 检测中包括 UDP/443。

步骤 4 点击 **OK**。

验证 Umbrella 注册

在您配置全局 Umbrella 设置并在 DNS 检测中启用 Umbrella 后，设备应与思科 Umbrella 通信并进行注册。可以通过检查思科 Umbrella 是否提供了设备 ID 来检查注册是否成功。

使用 **工具 > 命令行界面** 或 SSH 会话输入这些命令。

首先，检查服务策略统计信息，查询思科 Umbrella 注册行。这应指示思科 Umbrella 应用的策略（标签）、HTTP 连接状态（401 表示 API 令牌不正确，409 表示思科 Umbrella 中已存在该设备）和设备 ID。

```
asa(config)# show service-policy inspect dns
Interface inside:
  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
      message-length maximum client auto, drop 0
```

```

message-length maximum 512, drop 0
dns-guard, count 0
protocol-enforcement, drop 0
nat-rewrite, count 0
umbrella registration: tag: default, status: 200 success, device-id: 010a13b8fbdfc9aa

Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0
DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
DNScrypt: Certificate Update: completion 10, failure 1

```

您还可以验证运行配置（在策略映射上执行过滤）。策略映射中的 Umbrella 命令更新以显示设备 ID。当启用此命令时，无法直接配置设备 ID。以下示例编辑输出，以显示相关信息。您还可以通过编辑用于 Umbrella 的 DNS 检测映射来查看 ASDM 中的设备 ID；ID 显示在 **Umbrella 连接** 选项卡上。

```

ciscoasa(config)# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  dnscrypt
  umbrella device-id 010a3e5760fdd6d3
  no tcp-inspection
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map

```

监控 Umbrella 连接器

以下主题介绍如何监控 Umbrella 连接器。

监控 Umbrella 服务策略统计信息

可以在启用 Umbrella 的情况下查看 DNS 检测的概述和详细统计信息。

使用 **工具 > 命令行界面** 或 SSH 会话输入这些命令。

show service-policy inspect dns [detail]

查看所有主 DNS 检测计数器和 Umbrella 配置信息，而无需 **detail** 关键字。状态字段提供系统尝试在思科 Umbrella 中注册使用的 HTTP 状态代码。

```

asa(config)# show service-policy inspect dns
Interface inside:
  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
  message-length maximum client auto, drop 0
  message-length maximum 512, drop 0
  dns-guard, count 0
  protocol-enforcement, drop 0

```

```

nat-rewrite, count 0
umbrella registration: tag: default, status: 200 success, device-id: 010a13b8fbdfc9aa

Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0
DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
DNScrypt: Certificate Update: completion 10, failure 1

```

详细输出显示 DNScrypt 统计信息和使用的密钥。

```

asa(config)# show service-policy inspect dns detail
Global policy:
  Service-policy: global_policy
  Class-map: inspection_default
  Class-map: dnscrypt30000
    Inspect: dns dns_umbrella, packet 12, lock fail 0, drop 0, reset-drop 0,
      5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
      message-length maximum client auto, drop 0
      message-length maximum 1500, drop 0
      dns-guard, count 3
      protocol-enforcement, drop 0
      nat-rewrite, count 0
    Umbrella registration: tag: default, status: 200 SUCCESS, device-id: 010af97abf89abc3,
retry 0
  Umbrella: bypass 0, req inject 6 - sent 6, res recv 6 - inject 6
  Umbrella app-id fail, count 0
  Umbrella flow alloc fail, count 0
  Umbrella block alloc fail, count 0
  Umbrella client flow expired, count 0
  Umbrella server flow expired, count 0
  Umbrella request drop, count 0
  Umbrella response drop, count 0
  DNScrypt egress: rcvd 6, encrypt 6, bypass 0, inject 6
  DNScrypt ingress: rcvd 18, decrypt 6, bypass 12, inject 6
  DNScrypt length error, count 0
  DNScrypt add padding error, count 0
  DNScrypt encryption error, count 0
  DNScrypt magic_mismatch error, count 0
  DNScrypt disabled, count 0
  DNScrypt flow error, count 0
  DNScrypt nonce error, count 0
  DNScrypt: Certificate Update: completion 1, failure 1
  DNScrypt Receive internal drop count 0
  DNScrypt Receive on wrong channel drop count 0
  DNScrypt Receive cannot queue drop count 0
  DNScrypt No memory to create channel count 0
  DNScrypt Send no output interface count 1
  DNScrypt Send open channel failed count 0
  DNScrypt Send no handle count 0
  DNScrypt Send dupb failure count 0
  DNScrypt Create cert update no memory count 0
  DNScrypt Store cert no memory count 0
  DNScrypt Certificate invalid length count 0
  DNScrypt Certificate invalid magic count 0
  DNScrypt Certificate invalid major version count 0
  DNScrypt Certificate invalid minor version count 0
  DNScrypt Certificate invalid signature count 0
  Last Successful: 01:42:29 UTC May 2 2018, Last Failed: None
  Magic DNSC, Major Version 0x0001, Minor Version 0x0000,
  Query Magic 0x714e7a696d657555, Serial Number 1517943461,
  Start Time 1517943461 (18:57:41 UTC Feb 6 2018)
  End Time 1549479461 (18:57:41 UTC Feb 6 2019)
  Server Public Key

```

```
240B:11B7:AD02:FAC0:6285:1E88:6EAA:44E7:AE5B:AD2F:921F:9577:514D:E226:D552:6836
Client Secret Key Hash
48DD:E6D3:C058:D063:1098:C6B4:BA6F:D8A7:F0F8:0754:40B0:AFB3:CB31:2B22:A7A4:9CEE
Client Public key
6CB9:FA4B:4273:E10A:8A67:BA66:76A3:BFF5:2FB9:5004:CD3B:B3F2:86C1:A7EC:A0B6:1A58
NM key Hash
9182:9F42:6C01:003C:9939:7741:1734:D199:22DF:511E:E8C9:206B:D0A3:8181:CE57:8020
```

监控 Umbrella 系统日志消息

可以监控以下 Umbrella 相关系统日志消息：

- %ASA-3-339001: DNSCRYPT certificate update failed for *number* tries.

检查是否存在到 Umbrella 服务器的路由，以及出口接口是否启动且正常运行。此外，检查配置用于 DNSCrypt 的公钥是否正确。可能需要从思科 Umbrella 获取新密钥。

- %ASA-3-339002: Umbrella 设备注册失败，错误代码为 *error_code*。

错误代码具有以下含义：

- 400 - 存在请求格式或内容问题。令牌可能过短或已损坏。验证令牌与 Umbrella 控制面板上的令牌是否匹配。
- 401 - API 令牌未授权。请尝试重新配置该令牌。如果在 Umbrella 控制面板上刷新了令牌，然后必须确保使用新令牌。
- 409 - 设备 ID 与另一个组织存在冲突。请与 Umbrella 管理员合作检查，了解可能存在的问题。
- 500 - 内部服务器错误。与 Umbrella 管理员合作检查，了解可能存在的问题。

- %ASA-6-339003: Umbrella 设备注册成功。

- %ASA-3-339004: 由于缺失令牌，Umbrella 设备注册失败。

必须从思科 Umbrella 获取 API 令牌并将全局 Umbrella 设置中配置该令牌。

- %ASA-3-339005: 经过 *number* 次尝试，Umbrella 设备注册失败。

检查系统日志 339002 消息，以确定需要修复的错误。

思科 Umbrella 连接器的历史记录

功能名称	平台版本	描述
思科 Umbrella 支持。	9.10(1)	<p>您可以配置设备将 DNS 请求重定向至思科 Umbrella，以便将您在思科 Umbrella 中定义的企业安全策略应用于用户连接。您可以允许或阻止基于 FQDN 的连接，或者，对于可疑的 FQDN，您可以将用户重定向至思科 Umbrella 智能代理，该代理可以执行 URL 筛选。Umbrella 配置是 DNS 检测策略的一部分。</p> <p>我们添加或修改了以下屏幕：配置 > 防火墙 > 对象 > Umbrella、配置 > 防火墙 > 对象 > 检测映射 > DNS。</p>



第 9 章

ASA 和思科 Cloud Web Security

思科 Cloud Web Security（亦称为 ScanSafe）通过软件即服务 (SaaS) 模式提供 Web 安全和 Web 过滤服务。如果企业的网络中配备 ASA，不必额外安装硬件即可使用云网络安全服务。

- [思科 Cloud Web Security 相关信息，第 137 页](#)
- [思科 Cloud Web Security 的许可要求，第 140 页](#)
- [云网络安全指南，第 141 页](#)
- [配置思科 Cloud Web Security，第 142 页](#)
- [监控云网络安全，第 151 页](#)
- [思科云网络安全示例，第 152 页](#)
- [思科云网络安全的历史，第 157 页](#)

思科 Cloud Web Security 相关信息

在 ASA 上启用云网络安全时，ASA 将基于服务策略规则将所选的 HTTP 和 HTTPS 流量透明地重定向到云网络安全代理服务器。然后，云网络安全代理服务器将扫描内容，并基于思科 ScanCenter 中配置的策略允许、阻止流量或发送警告，以便强制执行可接受的使用及保护用户不受恶意软件侵害。

ASA 可选择性地使用身份防火墙和 AAA 规则进行身份验证并识别用户。ASA 可对其重定向到云网络安全的流量加密，并在其中包含用户凭证（包括用户名和用户组）。然后，云网络安全服务将使用用户凭证来匹配流量与策略。此外，该服务还将这些凭证用于基于用户的报告。如果不进行用户验证，ASA 可提供（可选）默认用户名和组，但用户名和组并非云网络安全服务应用策略的必需条件。

在创建服务策略规则时，可以自定义要发送到云网络安全的流量。此外，也可以配置“白名单”，以使匹配服务策略规则的 Web 流量子集改为直接流入初始请求的 Web 服务器，且不经过云网络安全扫描。

可以配置主用和备用云网络安全代理服务器，ASA 会定期轮询它们以检查其可用性。

用户身份和云网络安全

可以使用用户身份在云网络安全中应用策略。此外，用户身份对于云网络安全报告也非常有用。使用云网络安全并不要求使用用户身份。还存在其他为云网络安全策略标识流量的方法。

可以使用以下方法确定用户身份或提供默认身份：

- 身份防火墙 - 当 ASA 配合 Active Directory (AD) 使用身份防火墙时，系统会从 AD 代理中检索用户名和组。将用户和组用于访问规则等功能中的 ACL 或用于服务策略中时，系统会检索这些用户和组，也可以通过将用户身份监控配置为直接下载用户身份信息检索这些用户和组。
- AAA 规则 - 当 ASA 使用 AAA 规则执行用户身份验证时，系统会从 AAA 服务器或本地数据库中检索用户名。来自 AAA 规则的身份不包含组信息。如果配置一个默认组，这些用户会与该默认组关联。有关配置 AAA 规则的信息，请参阅旧版功能指南。
- 默认用户名和组 - 对于没有关联用户名或组的流量，可以配置可选默认用户名和组名。这些默认配置适用于与云网络安全服务策略规则匹配的所有用户。

身份验证密钥

每个 ASA 必须使用您从云网络安全获取的身份验证密钥。通过身份验证密钥，云网络安全可识别与 Web 请求相关的公司，并确保 ASA 与有效客户相关联。

可以为 ASA 使用两种身份验证密钥类型之一：公司密钥或组密钥。

- **公司身份验证密钥** - 可以在同一公司内的多个 ASA 上使用公司身份验证密钥。此密钥仅为您的 ASA 启用云网络安全服务。
- **组身份验证密钥** - 组身份验证密钥是特定于执行两种功能的每个 ASA 的特殊密钥：
 - 为 ASA 启用云网络安全服务。
 - 识别 ASA 的所有流量，以便可以为每个 ASA 创建 ScanCenter 策略。

您可在 ScanCenter (<https://scancenter.scansafe.com/portal/admin/login.jsp>) 中生成这些密钥。有关详细信息，请参阅云网络安全文档：

<http://www.cisco.com/c/en/us/support/security/cloud-web-security/products-installation-and-configuration-guides-list.html>

ScanCenter 策略

在 ScanCenter 中，流量按顺序匹配策略规则，直到匹配某个规则为止。然后云网络安全为规则应用已配置的操作，允许或阻止流量，或警告用户。即使出现警告，用户仍可以选择继续进入网站。

您可以在 ScanCenter（而不是 ASA）中配置 URL 过滤策略。

但是，策略的某些部分仅适用于策略的应用对象。用户流量可以根据以下组关联匹配 ScanCenter 中的策略规则：目录组或自定义组。组信息包含在从 ASA 重定向的请求中，所以您需要了解可以从 ASA 中获得哪些组信息。

目录组

目录组定义流量所属的组。当使用身份防火墙时，如果已有组，则其包含在客户端的 HTTP 请求中。如果未使用身份防火墙，可以为匹配云网络安全检测的 ASA 规则的流量配置默认组。

在 ScanCenter 中，当配置策略中的目录组时，必须正确输入组名。

- 身份防火墙组名按以下格式发送：

domain-name\group-name

请注意，在 ASA 中的格式为 *domain-name\group-name*。但是，ASA 可将名称修改为仅使用一个反斜线 (\)，以便在将组包含在重定向 HTTP 请求中时符合常见的 ScanCenter 注释法。

- 默认组名称按以下格式发送：

[domain\]group-name

在 ASA 中，需要配置可选域名，后跟 2 个反斜线 (\)；但是，ASA 可将名称修改为仅使用一个反斜线 (\)，以符合常见的 ScanCenter 注释法。例如，如果指定 “Cisco\\Boulder1”，则 ASA 可将该组名修改为 “Cisco\Boulder1”，在将该组名发送到云网络安全时仅使用一个反斜线 (\)。

自定义组

使用以下一个或多个条件定义自定义组：

- ScanCenter 组身份验证密钥 - 可以为自定义组生成一个组身份验证密钥。然后，如果在配置 ASA 时标识此组密钥，则来自 ASA 的所有流量都将带有组密钥标记。
- 源 IP 地址 - 可以在自定义组中确定源 IP 地址。请注意，ASA 服务策略基于源 IP 地址，所以可能需要改为在 ASA 上配置任何基于 IP 地址的策略。
- 用户名 - 可以在自定义组中确定用户名。

- 身份防火墙用户名按以下格式发送：

domain-name\username

- 使用 RADIUS 或 TACACS+ 时，AAA 用户名按以下格式发送：

LOCAL\username

- 使用 LDAP 时，AAA 用户名按以下格式发送：

domain-name\username

- 默认用户名按以下格式发送：

[domain-name\]username

例如，如果将默认用户名配置为 “Guest”，则 ASA 将发送 “Guest”。如果将默认用户名配置为 “Cisco\Guest”，则 ASA 将发送 “Cisco\Guest”。

组和身份验证密钥如何互通

除非需要自定义组及组密钥提供的每 ASA 策略，否则可能会使用公司密钥。请注意，并非所有的自定义组都与组密钥相关联。可以使用非加密自定义组标识 IP 地址或用户名，然后将这些 IP 地址或用户名与使用目录组的规则一起用于策略中。

即使的确需要每 ASA 策略并且正在使用组密钥，也可以使用目录组和非加密自定义组提供的匹配功能。在这种情况下，您可能需要基于 ASA 的策略，但基于组关系、IP 地址或用户名的一些情况例外。例如，如果要排除所有 ASA 中 America\Management 组内的用户：

1. 为 America/Management 添加目录组。
2. 为此组添加免除规则。
3. 在排除规则后添加用于每个自定义组及组密钥的规则，以便应用每 ASA 策略。
4. 来自 America\Management 中用户的流量将匹配排除规则，而所有其他流量将匹配其始发 ASA 的规则。

可以将诸多密钥、组和策略规则进行组合。

从主用代理服务器故障切换到备用代理服务器

您订用思科 Cloud Web Security 服务后，系统会为您分配主用云网络安全代理服务器和备用代理服务器。

如有任何客户端无法访问主用服务器，ASA 将开始轮询信号塔以确定可用性。（如果没有客户端活动，ASA 将每隔 15 分钟轮询一次。）如果在重试次数达到所配置的次数（默认设置为 5 次；此设置可配置）之后代理服务器不可用，则系统会宣布该服务器无法访问，并且备用代理服务器进入活动状态。ASA 根据服务器能否完成 TCP 三向握手来确定可用性。

故障切换到备用服务器后，ASA 将继续轮询主用服务器。如果主用服务器可以访问，ASA 将恢复使用主用服务器。

您可以通过检查云网络安全应用的运行状况，进一步优化故障切换。有时，服务器可以完成 TCP 三向握手，然而服务器上的云网络安全应用无法正常运行。如果启用应用运行状况检查，即使完成三向握手，但如果该应用本身未响应，系统也可故障切换到备用服务器。这样可提供更可靠的故障切换设置。

运行状况检查涉及向云网络安全应用发送包含测试 URL 的 GET 请求。如果服务器未能在配置的超时和重试限制内响应，则会被标记为关闭，并且系统将发起故障切换。此外，在将备用服务器标记为活动服务器之前，还会对备用服务器进行测试，以确保其正常运行。在故障切换后，系统每隔 30 秒便会重新测试一次主用服务器上的应用，直到其恢复联机且可被重新标记为活动服务器。

您可以在 ASA 既不能访问主用云网络安全代理服务器，也不能访问备用代理服务器时选择如何处理 Web 流量。可以阻止或允许所有网络流量。默认情况下，阻止网络流量。

思科 Cloud Web Security 的许可要求

型号	许可证要求
ASAv	标准许可证或高级许可证。
所有其他型号	严格加密 (3DES/AES) 许可证，用于加密 ASA 与云网络安全服务器之间的流量。

在云网络安全方面，必须购买思科 Cloud Web Security 许可证并确定 ASA 要处理的用户数。然后，登录 ScanCenter，生成身份验证密钥。

云网络安全指南

故障切换准则

在故障切换配置中受支持。不过，在活动/活动故障切换中，仅在主设备上配置策略。云网络安全连接器仅可跟踪从主设备到塔的连接情况；辅助设备总是报告塔无法接通。执行故障切换时，当辅助设备变为主设备时，辅助设备可以跟踪塔的连接情况。

情景模式准则

支持单一和多情景模式。

在多情景模式中，仅允许在系统情景中进行服务器配置，并且仅允许在安全情景中进行服务器策略规则配置。云网络安全连接器仅可跟踪从主管理情景到塔的连接情况。

如果需要的话，每个情景都可以拥有各自的身份验证密钥。

防火墙模式指导原则

仅支持路由防火墙模式。不支持透明防火墙模式。

IPv6 指导原则

不支持 IPv6。云网络安全目前仅支持 IPv4 地址。如果内部使用的是 IPv6，对于需要发送到云网络安全的任何 IPv6 流量，请使用 NAT 64 将 IPv6 地址转换为 IPv4 地址。

其他规定

- ASA 集群不支持云网络安全。
- 对于重定向到也可以执行 URL 过滤的模块（例如 ASA CX 和 ASA FirePOWER）的相同流量，不能使用云网络安全。流量只会发送到这些模块，而不是发送到云网络安全服务器。
- 云网络安全不支持无客户端 SSL VPN；云网络安全的 ASA 服务策略不得包含任何无客户端 SSL VPN 流量。
- 当云网络安全代理服务器的接口断开时，**show scansafe server** 命令的输出会显示两个服务器均已正常运行约 15-25 分钟。发生这种情况的原因是，轮询机制基于活动连接，而且由于接口发生故障而显示零连接，因此采用了轮询时间最长的方法。
- 对于同一流量，云网络安全检测兼容 HTTP 检测。
- 云网络安全不支持使用扩展 PAT 或任何可能使用同一源端口和 IP 地址进行不同连接的应用。例如，如果两个不同的连接（定位于不同的服务器）使用扩展 PAT，ASA 可能会重用同一源 IP 和源端口对两者执行连接转换，因为它们因目标不同而异。当 ASA 将这些连接重定向到云网络安全服务器时，会将目标替换为云网络安全服务器 IP 地址和端口（默认为 8080）。结果，两个

连接现在看起来属于同一流量（相同源 IP/端口和目标 IP/端口），导致返回流量无法被适当地反向转换。

- 默认检测流量类不包含云网络安全检测的默认端口（80 和 443）。

配置思科 Cloud Web Security

在配置云网络安全之前，请获取要使用的代理服务器的许可证和地址。此外，请生成身份验证密钥。有关更多信息，请参阅云网络安全网页 (<http://www.cisco.com/go/cloudwebsecurity>)。

请按照以下过程配置 ASA，将 Web 流量重定向到云网络安全。

开始之前

若要将用户身份信息发送到云网络安全，请在 ASA 上配置下列项目之一：

- 身份防火墙（用户名和组）。
- AAA 规则（仅用户名）- 请参阅旧版功能指南。

若要使用完全限定域名 (FQDN)，例如 `www.example.com`，必须为 ASA 配置 DNS 服务器。

过程

-
- 步骤 1 配置与云网络安全代理服务器的通信，第 142 页。
 - 步骤 2（可选。）列入身份白名单的流量，第 143 页。
 - 步骤 3 配置向云网络安全发送流量的服务策略，第 145 页。
 - 步骤 4（可选。）配置用户身份监控功能，第 150 页
 - 步骤 5 配置云网络安全策略，第 151 页。
-

配置与云网络安全代理服务器的通信

必须标识云网络安全代理服务器，以便可正确重定向用户 Web 请求。

在多情景模式下，必须在系统情景中配置代理服务器，然后为每个情景启用云网络安全。因此，在某些情景中可以使用该服务，而在其余情景中无法使用。

开始之前

- 必须为 ASA 配置 DNS 服务器才可以将完全限定域名用于代理服务器。
- （多情景模式。）必须同时在系统情景和特定情景下配置指向云网络安全代理服务器的路由。这样可确保云网络安全代理服务器在活动/活动故障切换情景下仍然可以访问。

过程

步骤 1 依次选择配置 > 设备管理 > 云网络安全。在多情景模式下，请在系统情景中执行此操作。

步骤 2 通过 IP 地址或完全限定域名标识主用和备用服务器。

当您订阅思科 Cloud Web Security 服务时，系统会为您分配主用和备用云网络安全代理服务器。

默认情况下，云网络安全代理服务器使用端口 8080 传输 HTTP 和 HTTPS 流量；除非明确要求，否则请勿更改此值。

步骤 3 （可选。）在 **Health Check** 组中，启用应用运行状况检查以改进故障切换处理。

如果要确定服务器的运行状况是否正常，可以配置思科 Cloud Web Security 来检查云网络安全应用的运行状况。通过检查应用运行状况，系统可以在主服务器响应 TCP 三向握手但无法处理请求时，故障切换到备用服务器。这可确保系统更加可靠。

配置以下选项：

- **Application URL** - 轮询系统来确定应用是否可响应时使用的 URL。要使用默认 URL，请输入 `http://gs.scansafe.net/goldStandard?type=text&size=10`。如果已不再需要该 URL，请指定思科 Cloud Web Security 为您提供的新 URL。
- **Application Timeout** - 超时确定 ASA 在发送 GET 请求后等待多长时间，运行状况检查 URL 才会获得响应。ASA 在超时后会重试该请求，直至达到轮询服务器的重试上限，然后才会将该服务器标记为关闭并启动故障切换。默认值为 15 秒，范围介于 5-120 秒之间。

步骤 4 在 **Other** 组中输入以下信息：

- **Retry Counter** - 在确定云网络安全代理服务器无法访问之前连续轮询该服务器的失败次数。每 30 秒执行一次轮询。有效值介于 2 和 100 之间，默认值为 5。
- **License Key**、**Confirm License Key** - ASA 发送到云网络安全代理服务器的身份验证密钥，用于指明发送请求的组织。身份验证密钥是一个 16 字节的十六进制数。该密钥可以是公司或组密钥。

步骤 5 点击 **Apply**。

步骤 6 （仅多情景模式。）切换到要使用该服务的每个情景并启用该服务。

可以选择为每个情景输入单独的身份验证密钥。如果不在其中包括身份验证密钥，则系统使用为系统情景配置的身份验证密钥。

列入身份白名单的流量

如果使用身份防火墙或 AAA 规则，可以配置 ASA，使来自匹配服务策略规则的特定用户或组的 Web 流量不会被重定向到云网络安全代理服务器进行扫描。此过程被称作将流量“列入白名单”。

您应在 ScanSafe 检测类映射中配置白名单。可以使用从身份防火墙和 AAA 规则派生的用户名和组名。无法根据 IP 地址或目标 URL 将流量列入白名单。

当配置云网络安全服务策略规则时，应在策略中引用类映射。尽管在服务策略规则中配置流量匹配条件（使用 ACL）时实现的结果与根据用户或组免除流量实现的结果相同，但您可能发现，使用白名单更简单。

过程

步骤 1 依次选择 **配置 > 防火墙 > 对象 > 类映射 > 云网络安全**。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新的类映射。输入映射名称（长度不超过 40 个字符），说明可选。
- 选择映射并点击 **Edit**。

步骤 3 选择匹配选项：**Match All** 或 **Match Any**。

Match All 是默认选项，指定流量必须与所有条件匹配才算是与类映射匹配。**Match Any** 表示流量只要与至少一个条件匹配，即为与类映射匹配。

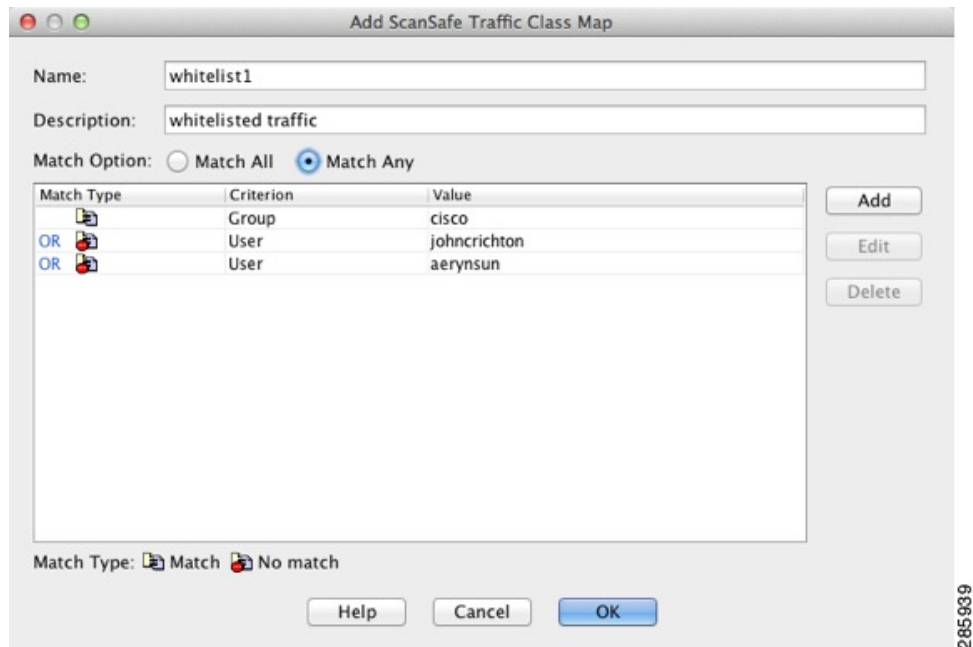
步骤 4 可通过在匹配表中添加或编辑条目来配置匹配条件。可以任意添加所需的条目来定义目标流量。

a) 选择条件的匹配类型：**Match** 或 **No Match**。

- **Match** - 指定要列入白名单的用户或组。
- **No Match** - 指定不想列入白名单的用户或组；例如，如果将组“cisco”列入白名单，但要扫描来自用户“johnrichton”和“aerynsun”的流量，则可以为这两个用户指定 **No Match**。

b) 选择是否要定义用户和/或组，然后输入用户或组的名称。

c) 点击 **OK**。重复此过程，直到已添加所有白名单条件。



步骤 5 点击 **OK**，添加类映射。

步骤 6 点击 **Apply**。

现在，就可以在云网络安全服务策略中使用白名单。

配置向云网络安全发送流量的服务策略

服务策略包括多条服务策略规则，这些规则被全局应用或者应用到单个接口。每条服务策略规则都可以将流量发送到云网络安全 (Match) 或免除来自云网络安全的流量 (Do Not Match)。

为以互联网为目标的流量创建规则。这些规则的顺序非常重要。当ASA决定转发数据包还是免于转发数据包时，ASA会按规则的列出顺序对照每个规则检测数据包。发现某个匹配后，将不再检查其他规则。例如，如果在明确匹配所有流量的策略的开头创建规则，将不检查更多语句。

开始之前

(可选) 如果需要使用白名单，使某些流量免于发送到云网络安全，则首先创建白名单，以便在服务策略规则中引用此白名单。

过程

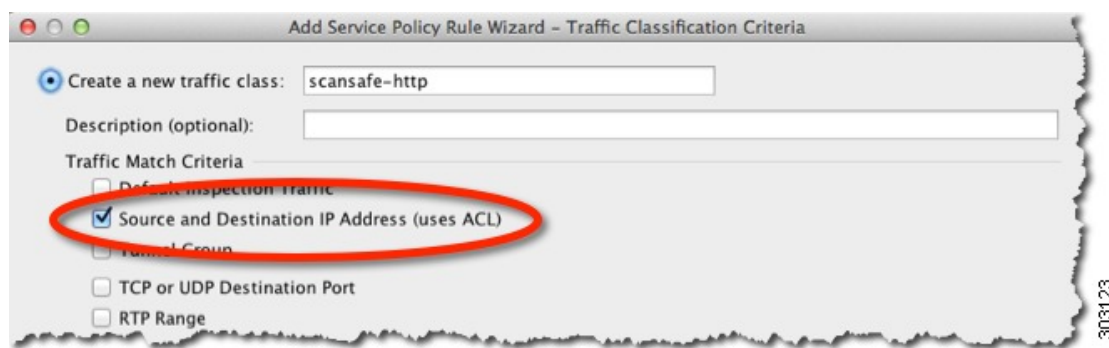
步骤 1 依次选择配置 > 防火墙 > 服务策略，并打开规则。

- 要创建新规则，请依次点击 **Add > Add Service Policy Rule**。当添加策略时，可以将策略应用到特定接口或全局应用到所有接口。如果已有全局策略或用于接口的策略，则可以向现有策略添加规则。可以命名新规则。点击 **Next** 继续操作。
- 如果有 ScanSafe 检测规则，或者有要添加 ScanSafe 检测的规则，请选择该规则并点击 **Edit**。请注意，Global 文件夹中的“inspection_default”规则不包含 HTTP 和 HTTPS 端口，所以无法向该规则添加 ScanSafe 检测。

步骤 2 在 Traffic Classification Criteria 页面，选择以下选项之一，指定要应用策略操作的流量，然后点击 **Next**。当创建新类时，请为类提供一个有意义的名称。另请注意，必须为 HTTP 和 HTTPS 流量创建单独的类。

- **Create a new traffic class > Source and Destination IP Address (uses ACL)** - 如果云网络安全中尚未包含流量类，我们建议使用此选项，因为 ACL 匹配是最灵活的类定义方式。

创建此类型的新流量类时，最初只能指定一个访问控制条目 (ACE)。完成添加规则之后，可以通过向同一接口或全局策略添加一条新规则，然后指定 **Add rule to existing traffic class**，添加其他 ACE。



- **Create a new traffic class > TCP or UDP Port** - 如果不希望区分 Web 流量，请使用此选项。点击 **Next** 之后，请指定一个端口，可以是 **TCP http** 或 **TCP https**。
- **Add rule to existing traffic class** - 如果已为思科云网络安全检测启动 ACL，并且正在向现有策略中添加规则，请选择此选项并选择流量类。

步骤 3 (ACL 匹配。) 根据源和目标条件定义流量类时，请为此规则填写 ACL 属性。

a) 点击 **Match** 或 **Do Not Match**。

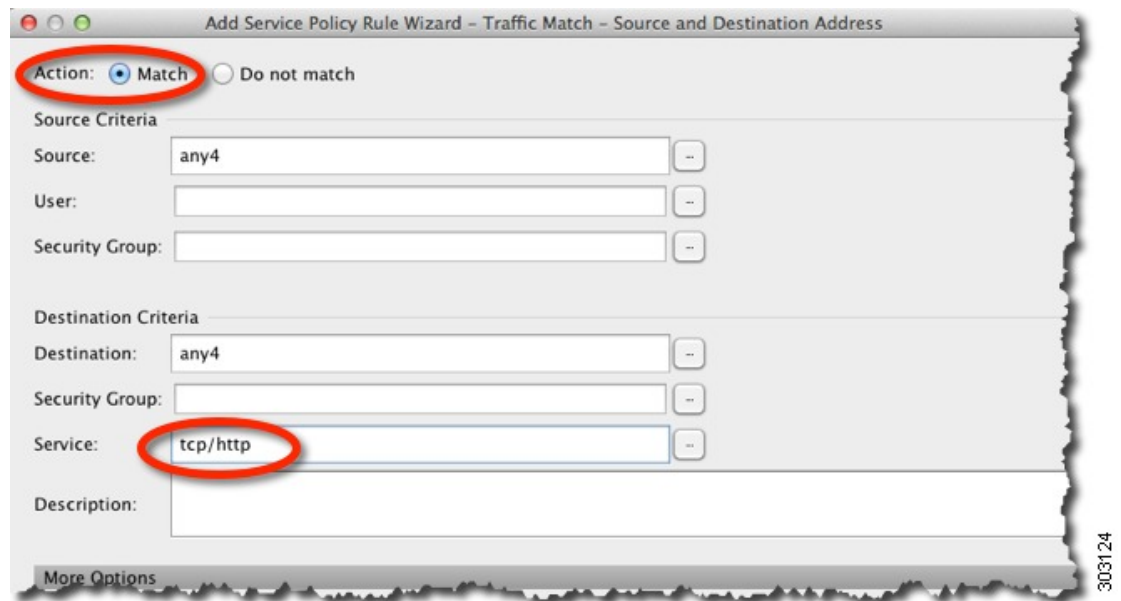
Match 指定将匹配源和目标的流量发送到云网络安全。**Do Not Match** 使匹配的流量免于发送到云网络安全。稍后可以添加其他规则，以匹配或不匹配其他流量。

创建规则时，请考虑如何匹配以互联网为目标的相应流量，但不匹配以其他内部网络为目标的流量。例如，当目标为 DMZ 上的内部服务器时，为阻止将内部流量发送到云网络安全，请务必将 deny ACE 添加到 ACL，使流量免于发送到 DMZ。

b) 在 Source Criteria 区域，输入或浏览源 IP 地址或网络对象。还可以使用身份防火墙用户参数和思科 TrustSec 安全组帮助标识流量。请注意，系统不会将 Trustsec 安全组信息发送到云网络安全；不能基于安全组定义策略。

- c) 在 Destination Criteria 区域，输入或浏览目标 IP 地址或网络对象，以及可选的 TrustSec 安全组。在匹配流量或使流量免于发送到特定服务器时，FQDN 网络对象可能比较有用。
- d) 在 Service 字段中，输入 **http** 或 **https**，然后点击 **Next**。

注释 云网络安全只能在 HTTP 和 HTTPS 流量上运行。ASA 将单独处理每种类型的流量。因此，需要创建仅 HTTP 规则和仅 HTTPS 规则。



- 步骤 4** 在 Rule Actions 页面的 **Protocol Inspection** 选项卡上，选中 **Cloud Web Security** 复选框。



- 步骤 5** 点击 **Configure** 设置流量操作，并添加检测策略映射。

检测策略映射可以为规则配置基本参数，或者也可以标识白名单。对于要发送到云网络安全的每个流量类，都要求检测策略映射。也可以通过依次选择 **Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security** 预配置检测策略映射。

- a) 对于 Cloud Web Security Traffic Action，请选择以下某一项：
- **Fail Close** - 如果云网络安全服务器不可用，丢弃所有流量。

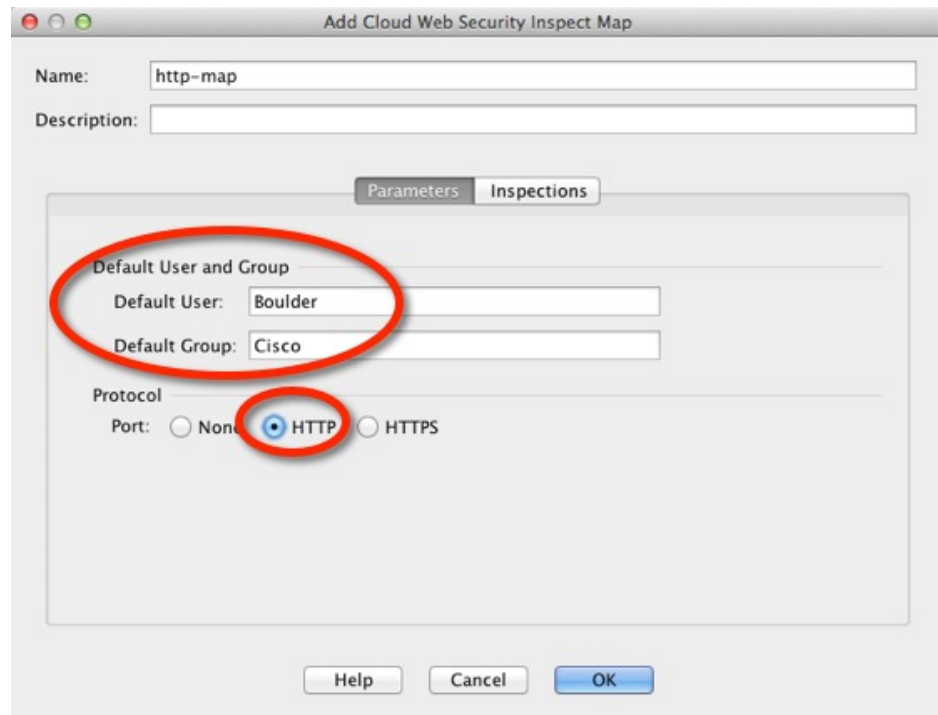
- **Fail Open** - 如果云网络安全服务器不可用，允许流量通过 ASA。

b) 选择现有检测策略映射，或点击 **Add** 添加新映射。



c) (仅新映射。) 在 Cloud Web Security Inspection Map 对话框中，为映射输入名称并配置以下属性。完成后点击 **OK**。

- **Default User and Group** - (可选)。默认用户名和/或组名。如果 ASA 无法确定传入 ASA 的用户的身份，则发送到云网络安全的 HTTP 请求中包括默认用户和组。可以在 ScanCenter 中为此用户名或组名定义策略。
- **Protocol** - 根据在流量类中选择的服务选择 **HTTP** 或 **HTTPS**。这些选择必须匹配。云网络安全单独处理每种类型的流量。



- **Inspections** 选项卡 - (可选) 要标识白名单, 请点击 **Inspections** 选项卡上的 **Add**, 并选择用于白名单的类映射。此时还可以通过点击 **Manage** 添加白名单。确保选择 **Whitelist** 作为操作, 然后点击 **OK**。可以添加其他白名单。

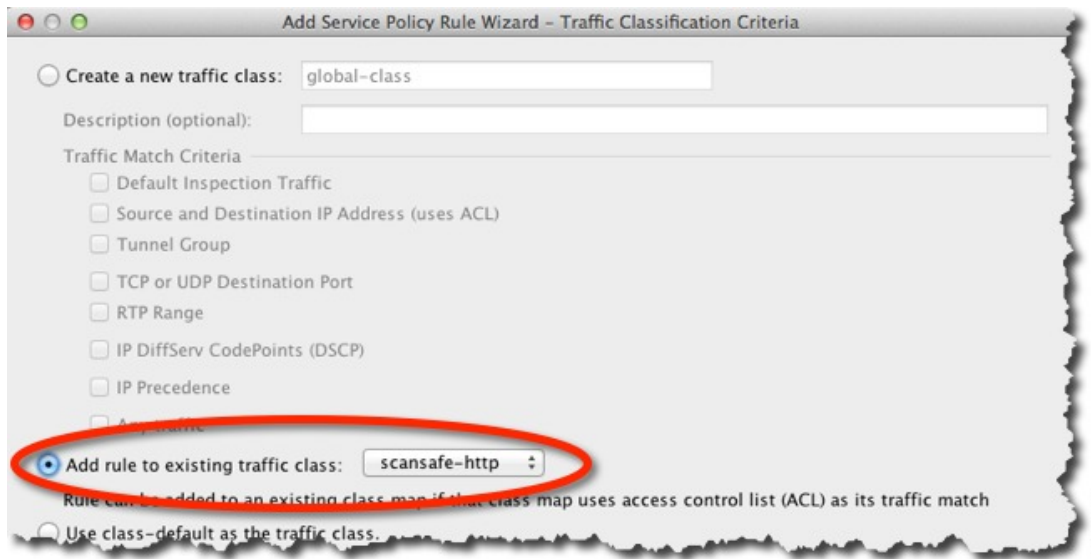
d) 在 **Select Cloud Web Security Inspect Map** 对话框中点击 **OK**。

步骤 6 点击 **Finish**。规则已添加到 **Service Policy Rules** 表。

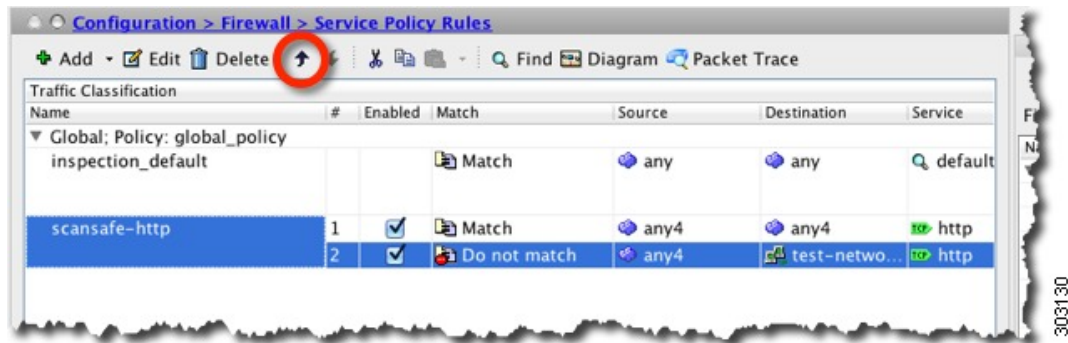
步骤 7 要为此流量类添加其他子规则 (ACE) 以及匹配或免除其他流量, 请选择相同的接口或全局策略, 重复此过程。当配置流量类时, 请选择 **Add rule to existing traffic class** 选项, 并选择 **Cloud Web Security** 类。

当配置新 ACE 时, 请确保在类中指定其他规则使用的相同服务, 可以是 **HTTP** 或 **HTTPS**。

请勿对 **Rule Actions** 页面进行更改。规则配置完成后点击 **Finish**。



- 步骤 8** 完整重复此操作步骤，为其他协议（例如为 HTTPS 流量）创建流量类（假定您已从 HTTP 流量类开始创建）。可以按需创建多项规则和子规则。
- 步骤 9** 在 Service Policy Rules 窗格中，安排云网络安全规则和子规则的顺序。选择要移动的规则并点击向上或向下按钮。确保特定规则排列在一般规则之前。



- 步骤 10** 点击 **Apply**。

配置用户身份监控功能

当使用身份防火墙时，ASA 仅会从 AD 服务器为活动 ACL 中包括的用户和组下载用户身份信息。在访问规则、AAA 规则、服务策略规则或视为活动状态的其他功能中必须使用 ACL。

例如，尽管可以将云网络安全服务策略规则配置为将 ACL 与用户和组配合使用，从而激活任何相关组，但这并非强制操作。可以使用完全基于 IP 地址 ACL。

由于云网络安全可将其 ScanCenter 策略基于用户身份，您可能需要下载并非活动 ACL 一部分的组，以获得所有用户的完全身份防火墙覆盖。用户身份监控功能使您可以从 AD 代理直接下载组信息。



注释 ASA 最多只能监控 512 个组，包括为用户身份监控功能配置的组和通过活动 ACL 监控的组。

过程

- 步骤 1** 依次选择 **Configuration > Firewall > Identity Options**，滚动到 Cloud Web Security Configuration 部分。
- 步骤 2** 点击 **Add**。
- 步骤 3** 选择包含该组的域并在用户组列表中双击该组，然后点击 **OK** 以添加该组。重复此过程以添加更多组。
 - 如果有大量的组，请使用 **Find** 框过滤列表。ASA 从 AD 为指定的域下载名称。
 - 还可以直接以 `domain_name\group_name` 格式键入组名。
 - 如有必要，可以通过点击 **Manage** 按钮添加新域。
- 步骤 4** 添加要监控的所有组后，点击 **Apply**。

配置云网络安全策略

在配置 ASA 服务策略规则后，启动 ScanCenter 门户以配置 Web 内容扫描、过滤、恶意软件保护服务和报告。

请访问：<https://scancenter.scansafe.com/portal/admin/login.jsp>。

有关详细信息，请参阅《思科 ScanSafe 云网络安全配置指南》：

http://www.cisco.com/en/US/products/ps11720/products_installation_and_configuration_guides_list.html

监控云网络安全

要监控云网络安全，请依次选择 **Monitoring > Properties > Cloud Web Security**。此页面显示代理服务器状态和重定向的 HTTP/HTTPS 连接的统计信息。在多情景模式下，仅在一个情景中显示统计信息。

可以通过从客户端计算机访问以下 URL 确定用户的流量是否被重定向到代理服务器。此页面将显示一条信息，用于指示用户当前是否正在使用该服务。

<http://Whoami.scansafe.net>

思科云网络安全示例

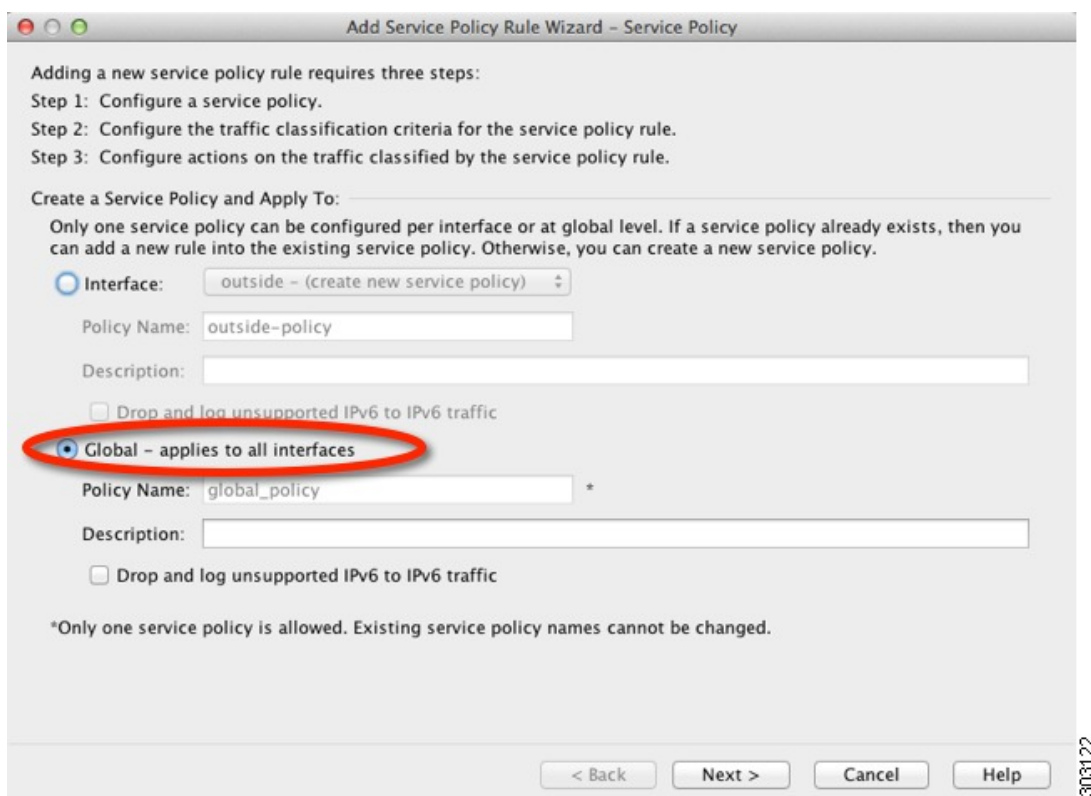
以下是配置云网络安全的一些示例。

云网络安全的服务策略示例

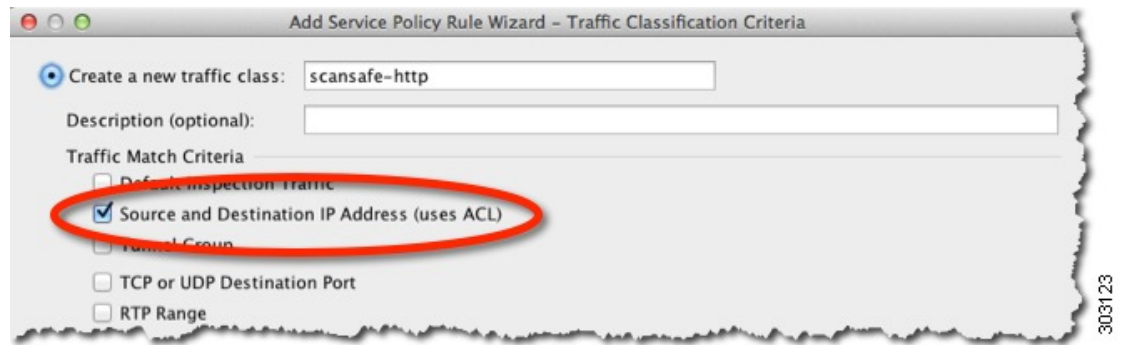
以下示例使所有 IPv4 HTTP 和 HTTPS 流量免于被发送到 10.6.6.0/24 网络，将所有其他 HTTPS 和 HTTPS 流量发送到云网络安全，并将该服务策略规则作为现有全局策略的一部分应用到所有接口。如果无法访问云网络安全服务器，ASA 将丢弃所有匹配流量 (fail close)。如果用户没有用户身份信息，则使用默认用户 Boulder 和组 Cisco。

过程

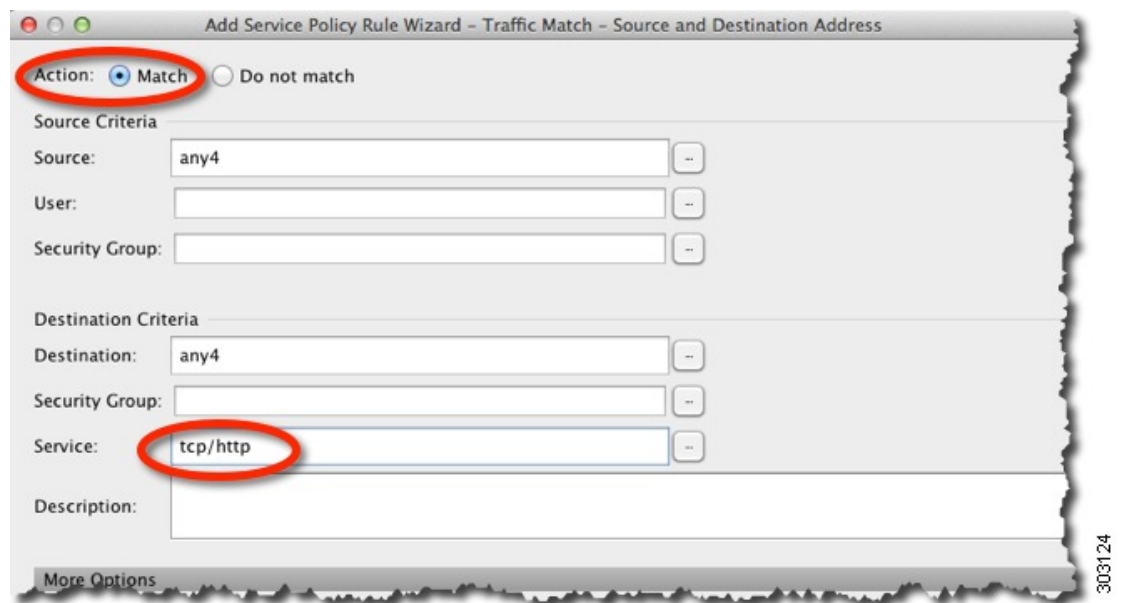
- 步骤 1** 依次选择配置 > 防火墙 > 服务策略规则，然后依次点击添加 > 服务器策略规则。将该规则添加到默认 global_policy 中。点击 **Next**。



- 步骤 2** 添加被称作“scansafe-http”的新流量类，并指定用于流量匹配的 ACL。点击 **Next**。



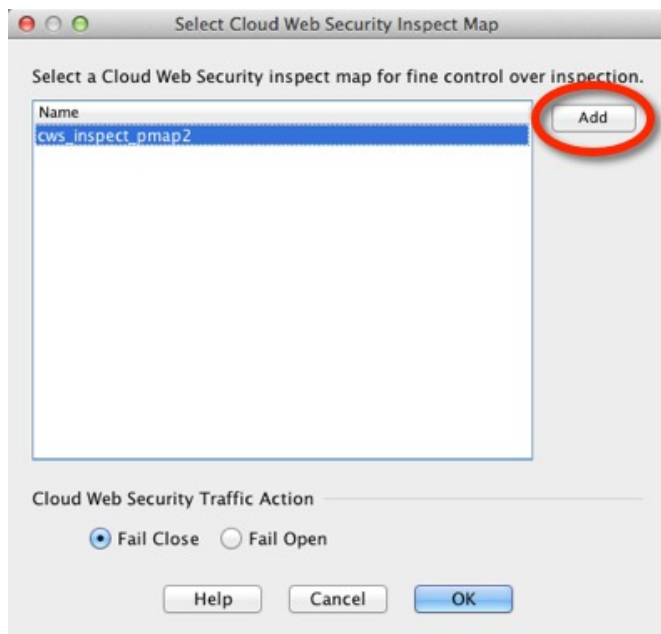
步骤 3 选择 **Match**，并将 Source 和 Destination 指定为 **any4**。将 Service 指定为 **tcp/http**。点击 **Next**。



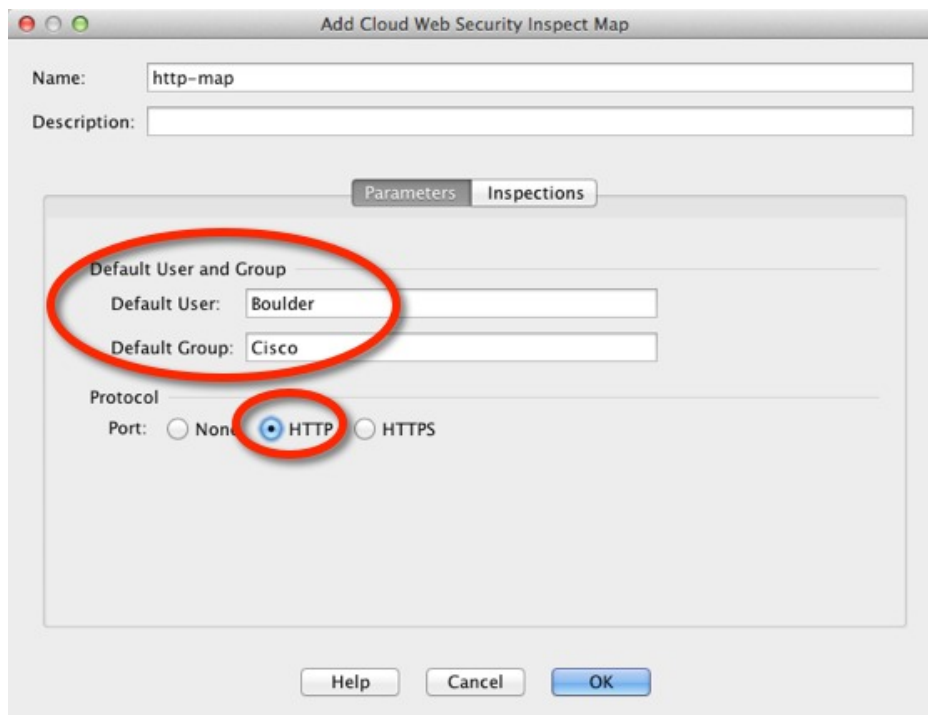
步骤 4 在 Protocol Inspection 选项卡上选中 **Cloud Web Security**，然后点击 **Configure**。



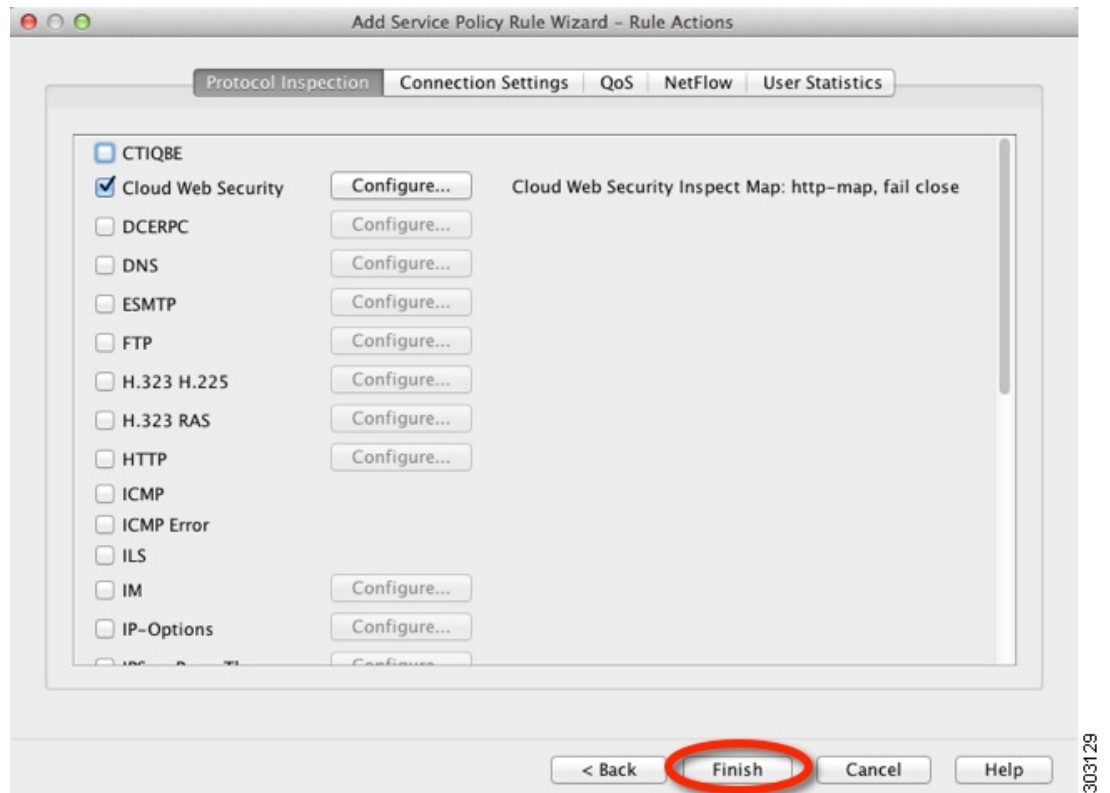
步骤 5 接受默认 Fail Close 操作，然后点击 **Add**。



步骤 6 将检测策略映射命名为“http-map”，将 Default User 设置为 Boulder，将 Default Group 设置为 Cisco。选择 HTTP。

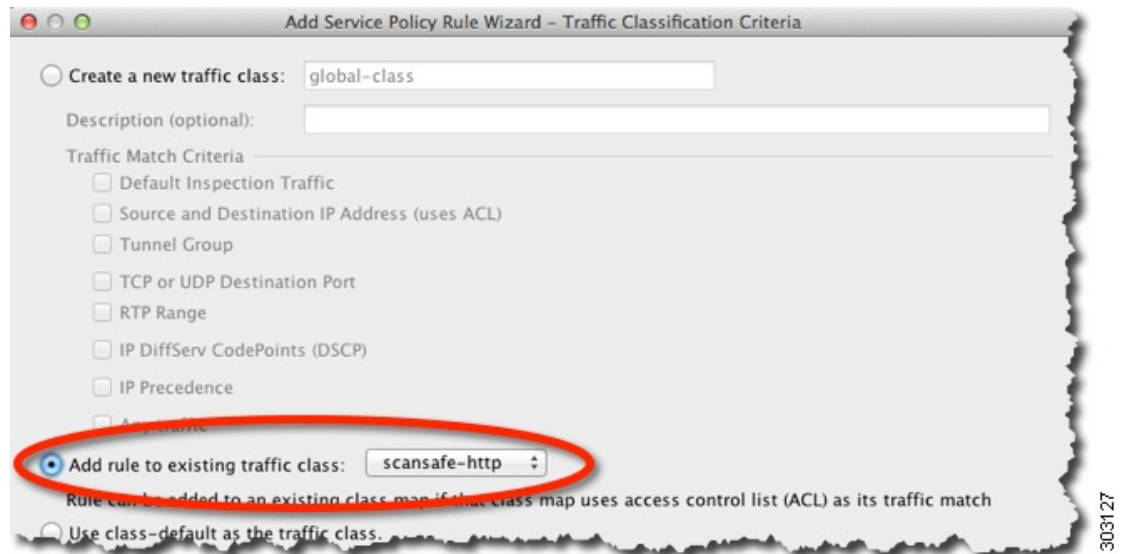


步骤 7 依次点击 **OK** 和 **OK**，然后点击 **Finish**。规则已添加到 Service Policy Rules 表。

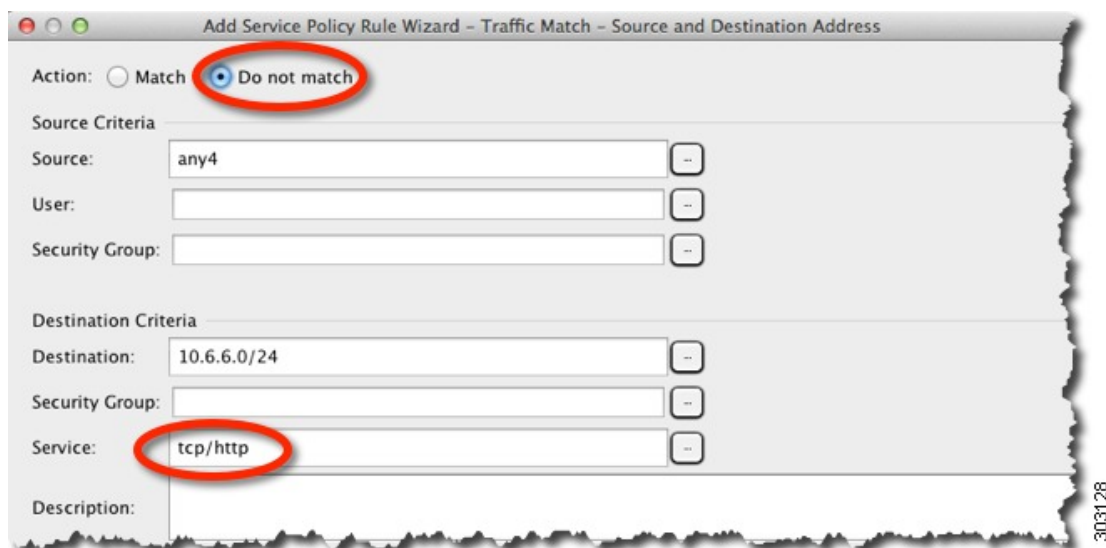


步骤 8 依次选择配置 > 防火墙 > 服务策略规则，然后依次点击添加 > 服务器策略规则。将新规则添加到默认 global_policy 中，然后点击 Next。

步骤 9 点击 Add rule to existing traffic class，然后选择 scansafe-http。

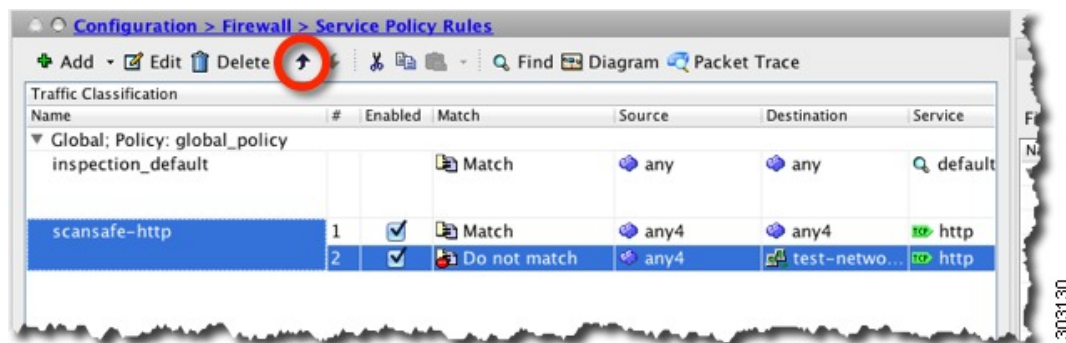


步骤 10 选择 Do not match，将 Source 设置为 any4，将 Destination 设置为 10.6.6.0/24。将 Service 设置为 tcp/http。点击 Next。



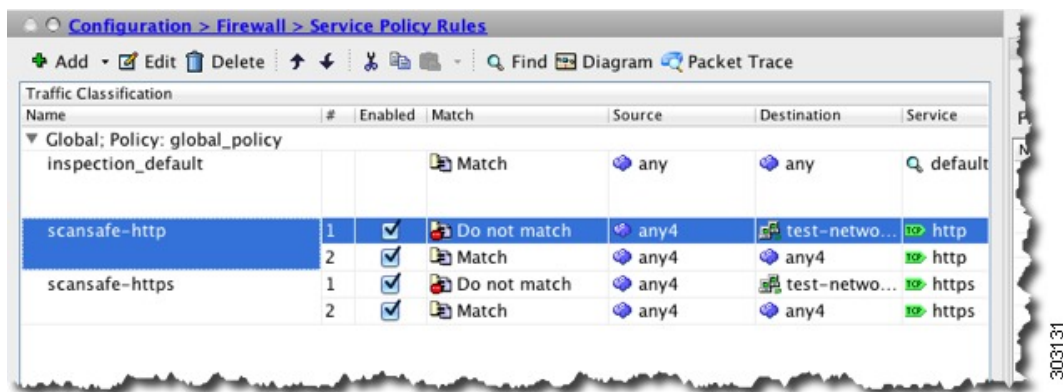
步骤 11 点击 **Finish**。

步骤 12 重新排列规则，使 **Do not match** 规则位于 **Match** 规则上方。



按顺序比较用户流量和这些规则；如果此 **Match** 规则是列表中的第一条规则，则所有流量（包括发送到测试网络的流量）仅匹配此规则，**Do not match** 规则将永远不会被匹配。如果将 **Do not match** 规则移到 **Match** 规则上方，则发送到测试网络的流量将匹配 **Do not match** 规则，所有其他流量将匹配 **Match** 规则。

步骤 13 重复上述步骤并做出以下更改：添加被称作“scansafe-https”的新流量类，为检测策略映射选择 **HTTPS**。



步骤 14 点击 **Apply**。

思科云网络安全的历史

功能名称	平台版本	功能信息
云网络安全	9.0(1)	<p>引入了此功能。</p> <p>思科云网络安全为 Web 流量提供内容扫描及其他恶意软件保护服务。还能够根据用户身份重定向网络流量和提交相关报告。</p> <p>引入或修改了以下菜单项：</p> <p>Configuration > Device Management > Cloud Web Security Configuration > Firewall > Objects > Class Maps > Cloud Web Security Configuration > Firewall > Objects > Inspect Maps > Cloud Web Security Configuration > Firewall > Identity Options Configuration > Firewall > Service Policy Rules Monitoring > Properties > Cloud Web Security</p>
思科云网络安全的应用层运行状况检查。	9.6(2)	<p>现在，您可以配置思科云 Web 安全以在确定服务器是否正常时检查云 Web 安全应用的运行状况。通过检查应用运行状况，系统可以在主服务器响应 TCP 三向握手但无法处理请求时，故障切换到备用服务器。这可确保系统更加可靠。</p> <p>修改了以下屏幕：Configuration > Device Management > Cloud Web Security。</p>



第 II 部分

面向虚拟环境的防火墙服务

• [基于属性的访问控制](#)，第 161 页



第 10 章

基于属性的访问控制

属性是配置中使用的自定义网络对象。您可以在思科 ASA 配置中定义和使用它们来过滤与 VMware ESXi 环境（由 VMware vCenter 管理）下的一个或多个虚拟机相关的流量。通过属性，您可以定义访问控制列表 (ACL) 为来自共享一个或多个属性的虚拟机组的流量分配策略。可向 ESXi 环境内的虚拟机分配属性并配置属性代理，属性代理使用 HTTPS 连接到 vCenter 或单个 ESXi 主机。然后，代理将请求和检索一个或多个绑定，从而将特定属性与虚拟机的主 IP 地址关联起来。

所有硬件平台以及 ESXi、KVM 或 HyperV 虚拟机监控程序上运行的所有 ASA 平台均支持基于属性的访问控制。只能从 ESXi 虚拟机监控程序上运行的虚拟机中检索属性。

- [基于属性的网络对象指南，第 161 页](#)
- [配置基于属性的访问控制，第 162 页](#)
- [监控基于属性的网络对象，第 166 页](#)
- [基于属性的访问控制的历史，第 167 页](#)

基于属性的网络对象指南

IPv6 规定

- vCenter 不支持使用 IPv6 地址作为主机凭证。
- IPv6 支持虚拟机绑定，其中虚拟机的主 IP 地址是 IPv6 地址。

其他准则和限制

- 不支持多情景模式。基于属性的网络对象仅支持单情景模式。
- 基于属性的网络对象仅支持绑定到虚拟机的主地址。不支持绑定到单一虚拟机的多个 vNIC。
- 只能为用于访问组的对象配置基于属性的网络对象。不支持为其他功能（NAT 等）配置网络对象。
- 虚拟机必须运行 VMware Tools，才能向 vCenter 报告主 IP 地址。不会通知 ASA 属性变更情况，除非 vCenter 知道虚拟机的 IP 地址。这是 vCenter 的限制。
- Amazon Web Services (AWS) 或 Microsoft Azure 公共云环境不支持基于属性的网络对象。

配置基于属性的访问控制

以下操作步骤介绍在 VMware ESXi 环境下，在托管的虚拟机上实施基于属性的访问控制的通用顺序。

过程

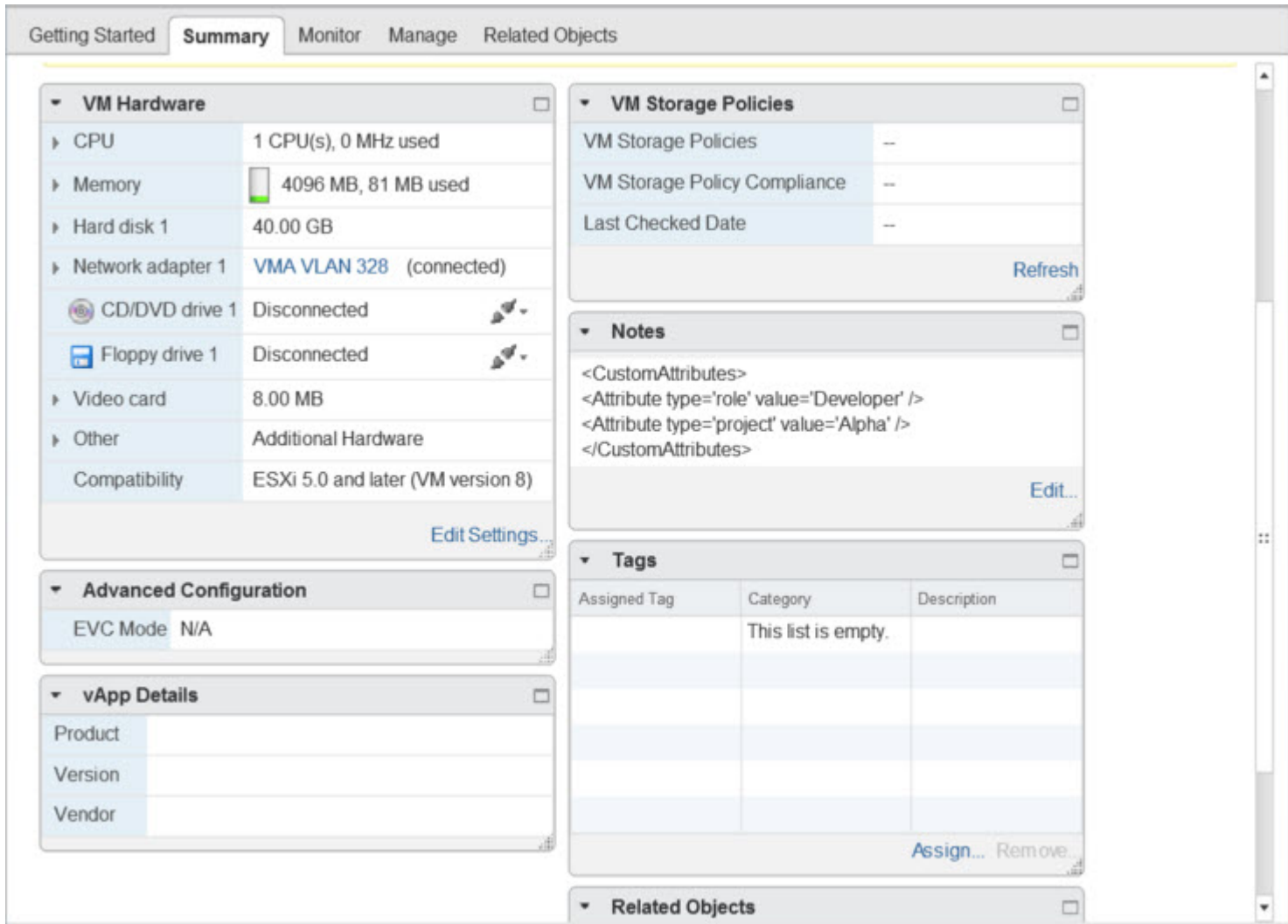
-
- 步骤 1** 为托管的虚拟机分配自定义属性类型和值。请参阅[配置 vCenter 虚拟机的属性](#)，第 162 页。
 - 步骤 2** 配置一个属性代理，以连接到您的 vCenter 服务器或 ESXi 主机。请参阅[配置虚拟机属性代理](#)，第 164 页。
 - 步骤 3** 配置部署方案所需的基于属性的网络对象。请参阅[配置基于属性的网络对象](#)，第 165 页。
 - 步骤 4** 配置访问控制列表和规则。请参阅[使用基于属性的网络对象配置访问规则](#)，第 166 页。
-

配置 vCenter 虚拟机的属性

您可以为虚拟机分配自定义属性类型和值，并将这些属性与网络对象相关联。然后，即可使用这些基于属性的网络对象向一组具有通用用户定义特征的虚拟机应用 ACL。例如，可以隔离开发人员构建设备和测试设备，或按项目和/或位置组合虚拟机。要使 ASA 基于属性监控虚拟机，需要使 vCenter 可通过管理的虚拟机使用这些属性。为此，可向 vCenter 中虚拟机 Summary 页面的 Notes 字段插入一个格式化的文本文件。

在下图中可以看到 Notes 字段。

图 16: vCenter 中虚拟机的 Summary 选项卡



要指定自定义属性，需将格式正确的 XML 文件复制到虚拟机的 Notes 字段。该文件的格式为：

```
<CustomAttributes>
<Attribute type='attribute-type' value='attribute-value' />
...
</CustomAttributes>
```

单个虚拟机可通过重复以上第二行定义多个属性。请注意，每行必须标识唯一的属性类型。如果为多个属性值定义的属性类型相同，则每次该属性类型的绑定更新都会覆盖上一次更新的值。

对于字符串属性值，与对象定义关联的值必须与虚拟机向 vCenter 报告的值完全匹配。例如，在虚拟机上，属性值 *Build Machine* 与注记值 *build machine* 不匹配。对于此属性，不会将绑定添加到主机映射。

在单个文件中可以定义多个唯一的属性类型。

过程

步骤 1 从 vCenter 清单中选择虚拟机。

步骤 2 点击虚拟机的 **Summary** 选项卡。

步骤 3 在 **Notes** 字段中，点击 **Edit** 链接。

步骤 4 将自定义属性文本文件粘贴到 **Edit Notes** 框中。该文本文件应遵循 XML 模板格式：

示例：

```
<CustomAttributes>
<Attribute type='attribute-type' value='attribute-value' />
...
</CustomAttributes>
```

步骤 5 点击 **OK**。

配置虚拟机属性代理

配置虚拟机属性代理可实现与 vCenter 或单个 ESXi 主机的通信。当您向 VMware 环境下的虚拟机分配属性时，属性代理会向 vCenter 发送一条消息，指明已配置哪些属性；而 vCenter 的响应是绑定更新配置的属性类型匹配的每个虚拟机。

虚拟机属性代理和 vCenter 交换绑定更新的方式如下：

- 如果代理发出获取新属性类型的请求，vCenter 的响应是绑定更新已配置该属性类型的每个虚拟机。在此之后，vCenter 仅在添加或更改属性值时才会发出新绑定。
- 如果一个或多个虚拟机的受控属性发生变化，则会收到绑定更新消息。根据报告该属性值的虚拟机的 IP 地址标识每个绑定消息。
- 如果多个属性由单一代理监控，则单一绑定更新包含每个虚拟机所有受监控的属性的当前值。
- 如果虚拟机中并未配置代理监控的某个特定属性，则绑定中对于该虚拟机包含一个空属性值。
- 如果尚未对虚拟机配置任何受监控的属性，则 vCenter 不会发送绑定更新。

每个属性代理仅与一个 vCenter 或 ESXi 主机通信。可以为单个 ASA 定义多个属性代理，每个属性代理与不同的 vCenter 进行通信，或者一个或多个属性代理与同一个 vCenter 进行通信。

过程

步骤 1 依次选择 **Configuration > Firewall > VM Attribute Agent**。

步骤 2 点击 **Add**。

步骤 3 在 Host Information 区域：

- a) 选择是否启用 IP 地址和身份验证证书。
- b) 输入 DNS 主机名或 IP 地址。

- c) 输入用户名。
- d) 选择密码类型：**Clear Text**、**UnEncrypted** 或 **Encrypted**。
- e) 输入密码。

步骤 4 在 **Keepalive Information** 区域：

- a) 输入 **Retry Interval**。输入 1 到 65535 之间的值。默认值为 30。
- b) 输入 **Retry Count**。输入 1 到 32 之间的值。默认值为 3。

步骤 5 点击 **OK**。

配置基于属性的网络对象

基于属性的网络对象可根据与 VMware ESXi 环境下一个或多个虚拟机相关的属性过滤流量。您可以通过定义访问控制列表 (ACL) 为来自共享一个或多个属性的虚拟机组的流量分配策略。

例如，可以配置允许具有 *engineering* 属性的计算机访问具有 *eng_lab* 属性的计算机的访问规则。网络管理员可添加或删除 *engineering* 计算机和 *lab* 服务器，安全管理员管理的安全策略会自动应用，而无需手动更新访问规则。

过程

步骤 1 依次选择 **Configuration > Firewall > Access Rules > Advanced Options**。

步骤 2 选中 **Enable Object Group Search Algorithm** 复选框。

必须启用对象组搜索，才能配置 VM 属性。

步骤 3 依次选择 **Configuration > Firewall > Objects > Network Objects/Groups**。

步骤 4 执行以下操作之一：

- 依次选择 **Add > Network Object Attributes**，添加一个新的基于属性的网络对象。输入名称和说明（后者为可选项）。
- 选择现有的基于属性的网络对象，并点击 **Edit**。

步骤 5 对于新的基于属性的网络对象，输入以下字段的值：

- a) **Agent Name** - 点击浏览按钮，并选择一个 VM 属性代理（或定义一个新代理）；请参阅 [配置虚拟机属性代理](#)。

如果将基于属性的网络对象配置为使用尚未配置的属性代理，则系统会自动创建一个无证书、无默认保持连接值的占位符代理。此代理将保持“无可用的证书”状态，直到提供了主机证书。

- b) **Attribute Type** - 此字符串定义属性类型，并且必须包含 **custom.** 前缀。例如 *custom.role*。
- c) **Attribute Value** - 使用此字符串条目将值与属性类型相关联。

Attribute Type 和 *Attribute Value* 对一起可定义唯一的属性。这使您可以定义适合特定部署方案的多个属性。如果使用多个属性值对同一属性类型定义了多次，则最后定义的值将覆盖以前的值。

步骤 6 点击 **OK**。

使用基于属性的网络对象配置访问规则

要使用基于属性的网络对象应用访问规则，请执行以下步骤。

过程

步骤 1 依次选择 **Configuration > Firewall > Access Rules**。

规则按接口和方向排列，全局规则另行分组。如果配置管理访问规则，则它们将在此页面上重复出现。这些分组等同于已创建并分配至接口或作为访问组全局性分配的扩展 ACL。这些 ACL 也显示在 **ACL Manager** 页面上。

步骤 2 执行以下任一操作：

- 要添加新规则，请依次选择 **Add > Add Access Rule**。
- 要在容器内的特定位置插入规则，请选择现有规则，并依次选择 **Add > Insert** 以便在该规则上方添加规则，或依次选择 **Add > Insert After**。
- 要编辑规则，请选择规则并点击 **Edit**。

步骤 3 填写规则属性。可选择的主要选项如下：

- **Interface** - 要应用规则的接口。选择 **Any** 以创建全局规则。对于路由模式下的桥接组，可以为网桥虚拟接口 (BVI) 和每个桥接组成员接口创建访问规则。
- **Action: Permit/Deny** - 是允许所述流量还是拒绝（丢弃）所述流量。
- **Source/Destination criteria** - 选择基于源属性的网络对象（始发对象）和基于目标属性的网络对象（流量流的目标对象）。还可以为源指定用户或用户组名称。此外，如果要将规则限制在比所有 IP 流量更窄的范围，则可以使用 **Service** 字段识别特定类型的流量。如果实施 **Trustsec**，则可使用安全组定义源和目标地址。

有关所有可用选项的详细信息，请参阅 [访问规则属性](#)，第 18 页。

定义规则完毕，请点击 **OK** 以将规则添加至表。

步骤 4 点击 **Apply**，以将访问规则保存至配置。

监控基于属性的网络对象

对于基于属性的网络对象，可以分析各个对象的使用情况。在 **Configuration > Firewall > Objects > Network Objects/Groups** 文件夹的相应页面，点击 **Where Used** 按钮。

对于基于属性的网络对象，还可以点击 **Not Used** 按钮来查找未用于任何规则的对象。该屏幕提供一个删除这些未使用对象的快捷方式。

基于属性的访问控制的历史

功能名称	平台版本	描述
基于属性的网络对象的支持	9.7(1)	<p>现在，除 IP 地址、协议和端口等传统网络特征之外，您还可以使用虚拟机属性控制网络访问。虚拟机必须位于 VMware ESXi 环境之下。</p> <p>引入或修改了以下屏幕：</p> <p>Configuration > Firewall > Objects > Network Object Attributes。</p> <p>引入了以下屏幕：Configuration > Firewall > VM Attribute Agent。</p>
从 ASA 5506-X（所有型号）、5508-X、5512-X 和 5516-X 中删除了对基于虚拟机属性的网络对象的支持。	9.10(1)	您无法再在以下平台上使用基于虚拟机属性的网络对象：ASA 5506-X（所有型号）、5508-X、5512-X、5516-X。



第 III 部分

网络地址转换

- [网络地址转换 \(NAT\)](#)，第 171 页
- [NAT 示例和参考](#)，第 231 页



第 11 章

网络地址转换 (NAT)

以下主题介绍网络地址转换 (NAT) 及其配置方法。

- [为何使用 NAT? ， 第 171 页](#)
- [NAT 基础知识 ， 第 172 页](#)
- [NAT 指南 ， 第 176 页](#)
- [动态 NAT ， 第 182 页](#)
- [动态 PAT ， 第 190 页](#)
- [静态 NAT ， 第 209 页](#)
- [身份 NAT ， 第 220 页](#)
- [监控 NAT ， 第 226 页](#)
- [NAT 的历史 ， 第 227 页](#)

为何使用 NAT?

IP 网络中的每台计算机和设备都分配了标识主机的唯一 IP 地址。因为缺乏公用 IPv4 地址，所以这些 IP 地址中的大多数都是专用地址，在专用公司网络以外的任何地方都不可路由。RFC 1918 定义可以在内部使用但不应通告的专用 IP 地址：

- 10.0.0.0 到 10.255.255.255
- 172.16.0.0 至 172.31.255.255
- 192.168.0.0 到 192.168.255.255

NAT 的主要功能之一是使专用 IP 网络可以连接到互联网。NAT 用公用 IP 地址替换专用 IP 地址，将内部专用网络中的专用地址转换为可在公用互联网上使用的合法可路由地址。NAT 以此方式保存公用地址，因为它可配置为至少仅将整个网络的一个公用地址向外界通告。

NAT 的其他功能包括：

- 安全 - 隐藏内部 IP 地址可以阻止直接攻击。
- IP 路由解决方案 - 使用 NAT 时不会出现重叠 IP 地址。

- 灵活性 - 可以更改内部 IP 寻址方案，而不影响外部的可用公用地址；例如，对于可以访问互联网的服务器，可以维护供互联网使用的固定 IP 地址，但在内部，可以更改服务器地址。
- 在 IPv4 和 IPv6 之间转换（仅路由模式）（9.0(1) 及更高版本） - 如果想将 IPv6 网络连接到 IPv4 网络，可以利用 NAT 在两种类型的地址之间转换。



注释 不需要 NAT。如果不为一组给定流量配置 NAT，将不转换这些流量，但会正常应用所有安全策略。

NAT 基础知识

以下主题介绍一些 NAT 基础知识。

NAT 术语

本文档使用以下术语：

- 实际地址/主机/网络/接口 - 实际地址是指在主机上定义的转换前地址。在内部网络访问外部网络时，要转换内部网络的典型 NAT 场景中，内部网络会成为“实际”网络。请注意，您可以转换连接到设备的任何网络，而不是只在网络内部转换。因此，如果配置 NAT 以转换外部地址，“实际”可以是指访问内部网络时的外部网络。
- 映射地址/主机/网络/接口 - 映射地址是指实际地址转换而成的地址。在内部网络访问外部网络时，要转换内部网络的典型 NAT 场景中，外部网络会成为“映射”网络。



注释 在地址转换过程中，不会转换为设备接口配置的 IP 地址。

- 双向发起 - 静态 NAT 允许双向发起连接，意味着可发起到主机的连接和从主机发起连接。
- 源 NAT 和目的 NAT - 对于任何给定数据包，将源 IP 地址和目的地 IP 地址与 NAT 规则进行比较，转换/不转换一个或两个地址。对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目的地”，即便是给定的连接，也可能源自“目的地”地址。

NAT 类型

可以使用以下方法实施 NAT：

- 动态 NAT - 按先到先得的方式，将一组实际 IP 地址映射到一组映射 IP 地址（通常较小）。仅实际主机可以发起流量。请参阅[动态 NAT](#)，第 182 页。
- 动态端口地址转换 (PAT) - 使用 IP 地址的唯一源端口，将一组实际 IP 地址映射到单一 IP 地址。请参阅[动态 PAT](#)，第 190 页。

- 静态 NAT - 实际 IP 地址和映射 IP 地址之间的一致映射。允许发起双向流量。请参阅[静态 NAT](#)，第 209 页。
- 身份 NAT - 系统将实际地址静态转换为其本身，基本绕过 NAT。当您想转换一大组地址，但又想免除一小部分地址时，可能就要这样配置 NAT。请参阅[身份 NAT](#)，第 220 页。

网络对象 NAT 和 两次 NAT

可以通过以下两种方法实施地址转换：网络对象 NAT 和 两次 NAT。

我们建议使用网络对象 NAT，除非您需要两次 NAT 提供的额外功能。网络对象 NAT 更容易配置，而且可能对应用（例如 IP 语音 [VoIP]）更加可靠。（对于 VoIP，对不属于规则中使用的任何对象的间接地址进行转换可能会失败。）

网络对象 NAT

配置为网络对象参数的所有 NAT 规则都被视为网络对象 NAT 规则。这是一种为网络对象配置 NAT 的快捷方法。但是，您无法为对象组创建这些规则。

配置网络对象之后，可以接着将该对象的映射地址标识为内联地址或者另一个网络对象或网络对象组。

当数据包进入接口时，系统会根据网络对象 NAT 规则来检查源和目标 IP 地址。如果进行独立匹配，可根据独立规则转换数据包中的源地址和目的地地址。这些规则互不牵连，可以根据流量使用不同的规则组合。

因为规则从未配对，所以不能指定源 A/目的 A 应当有不同于源 A/目的 B 的转换。两次 NAT 用于实现这样的功能：您可以识别单个规则中的源和目标地址。

两次 NAT

两次 NAT 供您在单个规则中同时标识源和目标地址。同时指定源和目的的目标地址，可以让您指定源 A/目的目标 A 有不同于源 A/目的目标 B 的转换。



注释

对于静态 NAT，规则是双向的，因此请注意，本指南各处的命令和说明中使用了“源”和“目的目标”这两个词，即便给定连接可能源自“目的目标”地址。例如，如果配置支持端口地址转换的静态 NAT，然后将源地址指定为某台 Telnet 服务器，并且希望进入该 Telnet 服务器的所有流量都将端口从 2323 转换为 23，那么您就必须指定要转换的源端口（实际端口：23，映射端口：2323）。必须指定源端口是因为您已将 Telnet 服务器地址指定为源地址。

目的目标地址是可选的。如果指定目的目标地址，可以将其映射到其本身（身份 NAT），也可以将其映射到不同的地址。目的目标映射始终是静态映射。

比较 网络对象 NAT 和 两次 NAT

这两类 NAT 之间的主要差异是：

- 定义实际地址的方法。
 - 网络对象 NAT - 将 NAT 定义为网络对象的参数。网络对象命名 IP 主机、范围或子网，以便能在 NAT 配置中使用对象，而不是实际 IP 地址。网络对象 IP 地址用作实际地址。通过此方法，可以轻松将 NAT 添加到可能已在配置的其他部分使用的网络对象。
 - 两次 NAT- 标识实际地址和映射地址的网络对象或网络对象组。在这种情况下，NAT 不是网络对象的参数；网络对象或组是 NAT 配置的参数。能够使用实际地址的网络对象组意味着两次 NAT 更具可扩展性。
- 实施源和目标 NAT 的方法。
 - 网络对象 NAT- 每个规则都可应用到数据包的源或目标。因此，可能使用两条规则，一条用于源 IP 地址，一条用于目的 IP 地址。这两条规则不能绑在一起对源/目的组合进行特定转换。
 - 两次 NAT- 单一规则可以同时转换源和目标。数据包仅匹配一条规则，且不再检查其他规则。即使您不配置可选目标地址，匹配的数据包仍仅匹配一个两次 NAT 规则。源和目的绑在一起，使您可以根据源/目的组合进行不同的转换。例如，源 A/目的 A 可以有不同于源 A/目的 B 的转换。
- NAT 规则顺序。
 - 网络对象 NAT- 在 NAT 表中自动排序。
 - 两次 NAT - 在 NAT 表中手动排序（在网络对象 NAT 规则之前或之后）。

NAT 规则排序

网络对象 NAT 和两次 NAT 规则存储在分为三个部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

表 9: NAT 规则表

表部分	规则类型	部分中的规则顺序
第 1 部分	两次 NAT	系统按照在配置中出现的顺序应用第一个匹配的规则。因为会应用第一个匹配规则，所以必须确保特定规则位于更加通用的规则前面，否则无法按预期应用特定规则。默认情况下，两次 NAT 规则会添加到第 1 部分。

表部分	规则类型	部分中的规则顺序
第 2 部分	网络对象 NAT	<p>如果在第 1 部分未找到匹配项，则会按照以下顺序应用第 2 部分的规则：</p> <ol style="list-style-type: none"> 1. 静态规则。 2. 动态规则。 <p>在每个规则类型中，遵循以下排序指导原则：</p> <ol style="list-style-type: none"> 1. 实际 IP 地址数量 - 从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。 2. 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。 3. 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，abracadabra 在 catwoman 之前进行评估。
第 3 部分	两次 NAT	<p>如果仍未找到匹配项，则按照在配置中出现的顺序，应用第三部分规则的第一个匹配项。此部分应当包含最通用的规则。还必须确保此部分的特定规则位于通用规则之前，否则会应用通用规则。</p>

例如，对于第二部分规则，在网络对象中定义以下 IP 地址：

- 192.168.1.0/24（静态）
- 192.168.1.0/24（动态）
- 10.1.1.0/24（静态）
- 192.168.1.1/32（静态）
- 172.16.1.0/24（动态）（对象 def）
- 172.16.1.0/24（动态）（对象 abc）

结果排序可能是：

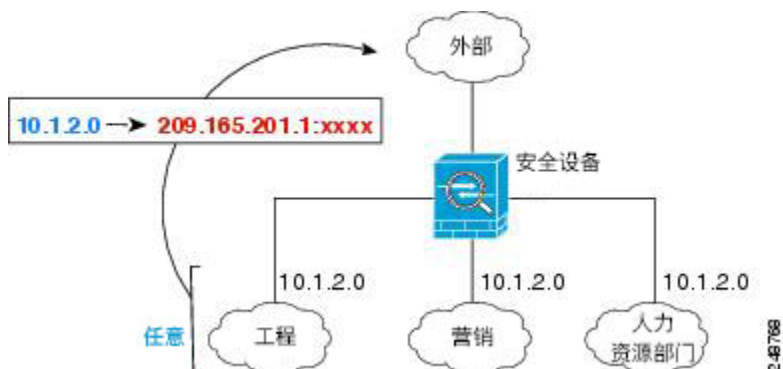
- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 abc）
- 172.16.1.0/24（动态）（对象 def）
- 192.168.1.0/24（动态）

NAT 接口

除了桥接组成员接口，您可以将 NAT 规则配置为应用到任何接口（也就是，所有接口），或者也可以标识特定的实际接口和映射接口。还可以为实际地址指定任何接口，为映射地址指定特定接口，反之亦然。

例如，如果在多个接口上使用相同的专用地址，并且在访问外部接口时要将这些地址全部转换到同一全局池，则可能要为实际地址指定任何接口，并且为映射地址指定外部接口。

图 17: 指定任意接口



然而，“任意”接口的概念不适用于桥接组成员接口。当指定“任意”接口时，NAT 将排除所有桥接组成员接口。因此，要将 NAT 应用于桥接组成员，必须指定成员接口。这样可能导致有许多只有一个接口不同的类似规则。您不能为桥接虚拟接口 (BVI) 本身配置 NAT，只能为成员接口配置 NAT。

NAT 指南

以下主题提供有关实施 NAT 的详细指导原则。

NAT 防火墙模式指南

在路由和透明防火墙模式下支持 NAT。

不过，在桥接组成员接口（属于桥接组虚拟接口 [BVI] 的接口）上配置 NAT 具有以下局限性：

- 为桥接组的成员配置 NAT 时，需要指定成员接口。您不能为桥接组接口 (BVI) 本身配置 NAT。
- 在桥接组成员接口之间执行 NAT 时，必须指定实际地址和映射地址。不能指定“任意”作为接口。
- 当映射地址是桥接组成员接口时，不能配置接口 PAT，因为没有 IP 地址连接到该接口。
- 当源接口和目的地接口是同一桥接组的成员时，不能在 IPv4 和 IPv6 网络 (NAT64/46) 之间进行转换。静态 NAT/PAT 44/66、动态 NAT44/66 和动态 PAT44 是唯一允许的方法；不支持动态 PAT66。但是，您可以在不同桥接组的成员之间，或在桥接组成员（源接口）和标准路由接口（目的地接口）之间执行 NAT64/46。

IPv6 NAT 指导原则

NAT 支持 IPv6，但有以下指导原则和限制。

- 对于标准路由模式接口，您还可以在 IPv4 和 IPv6 之间进行转换。
- 对于同一个桥接组的成员接口，不能在 IPv4 和 IPv6 之间进行转换，而只能在两个 IPv6 或两个 IPv4 网络之间进行转换。此限制不适用于接口为不同网桥组桥接组成员或一个接口为网桥组桥接组成员，另一个为标准路由接口的情况。
- 在同属一个桥接组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于接口为不同网桥组桥接组成员或一个接口为网桥组桥接组成员，另一个为标准路由接口的情况。
- 对于静态 NAT，可以指定一个最大 /64 的 IPv6 子网。不支持更大的子网。
- 将 FTP 和 NAT46 配合使用时，当 IPv4 FTP 客户端连接到 IPv6 FTP 服务器时，客户端必须使用扩展被动模式 (EPSV) 或扩展端口模式 (EPRT)；在使用 IPv6 时，不支持 PASV 和 PORT 命令。

IPv6 NAT 建议

可以使用 NAT 在 IPv6 网络之间转换，以及在 IPv4 和 IPv6 网络之间转换（仅路由模式）。我们推荐以下最佳实践：

- NAT66 (IPv6 对 IPv6) - 我们建议使用静态 NAT。尽管您可以使用动态 NAT 或 PAT，但鉴于 IPv6 地址供应量巨大，因此您不必使用动态 NAT。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限于两次 NAT）。
- NAT46 (IPv4 对 IPv6) - 我们建议使用静态 NAT。因为 IPv6 地址空间远远大于 IPv4 地址空间，所以可以轻松满足静态转换需求。如果不想允许返回流量，您可以启用单向静态 NAT 规则（仅限于两次 NAT）。转换为 IPv6 子网 (/96 或更低) 时，默认情况下，生成的映射地址为有嵌入 IPv4 的 IPv6 地址，其中 32 位 IPv4 地址嵌入在 IPv6 前缀后面。例如，如果 IPv6 前缀为 /96 前缀，则 IPv4 地址附在最后的 32 位地址中。例如，如果将 192.168.1.0/24 映射到 201b::0/96，则 192.168.1.4 将被映射到 201b::0.192.168.1.4（通过混合表示法显示）。如果前缀较小（例如 /64），则 IPv4 地址附在前缀的后面，后缀 0 附在 IPv4 地址后面。或者，还能够以网络对网络的方式转换地址，其中第一个 IPv4 地址映射到第一个 IPv6 地址，第二个 IPv4 地址映射到第二个 IPv6，依次类推。
- NAT64 (IPv6 到 IPv4) - 可能没有足够的 IPv4 地址来容纳大量的 IPv6 地址。我们建议使用动态 PAT 池提供大量的 IPv4 转换。

其他 NAT 指南

- 对于作为桥接组成员的接口，您需要为成员接口编写 NAT 规则。您无法为桥接虚拟接口 (BVI) 本身编写 NAT 规则。
- （仅限于网络对象 NAT。）您仅可为给定对象定义单个 NAT 规则，如果要为某个对象配置多个 NAT 规则，则需要创建通过不同名称指定同一 IP 地址的多个对象。

- 如果在接口上定义了 VPN，则接口上的进站 ESP 流量不受 NAT 规则的约束。系统仅允许已建立的 VPN 隧道的 ESP 流量，而丢弃与现有隧道不相关的流量。此限制适用于 ESP 和 UDP 端口 500 和 4500。
- 如果在应用动态 PAT 设备之后的某设备上定义站点间 VPN，以便 UDP 端口 500 和 4500 不是实际使用的端口，必须从 PAT 设备之后的设备发起连接。响应方无法发起安全关联 (SA)，因为不知道正确的端口号。
- 如果更改 NAT 配置，并且不想等待现有转换超时后再使用新 NAT 配置，则可以在设备 CLI 中使用 **clear xlate** 命令清除转换表。然而，清除转换表将断开使用转换的当前所有连接。



注释 如果删除动态 NAT 或 PAT 规则，然后使用与已删除规则中地址重叠的映射地址添加新规则，则系统将不使用新规则，直至与已删除规则关联的所有连接超时，或已使用 **clear xlate** 命令将这些连接清除。此保护措施确保相同的地址将不分配至多个主机。

- 转换 SCTP 流量时，仅使用静态网络对象 NAT。系统不允许动态 NAT/PAT。虽然您可以配置静态两次 NAT，但不建议这样做，因为 SCTP 关联的目的地部分的拓扑未知。
- NAT 中使用的对象和对象组不能是未定义的，它们必须包含 IP 地址。
- 不能使用同时包含 IPv4 和 IPv6 地址的对象组，对象组只能包括一种类型的地址。
- （仅限于两次 NAT。）在 NAT 规则中使用 **any** 作为源地址时，“any”流量（IPv4 与 IPv6）的定义取决于规则。只有数据包为 IPv6 至 IPv6 或 IPv4 至 IPv4，ASA 才能对数据包执行 NAT；借助此先决条件，ASA 可确定 NAT 规则中的 **any** 的值。例如，如果配置从“any”到 IPv6 服务器的规则，且该服务器已从 IPv4 地址映射，则 **any** 指“任意 IPv6 流量”。如果配置从“any”到“any”的规则，并且将源映射至接口 IPv4 地址，则 **any** 指“任意 IPv4 流量”，因为映射的接口地址意味着目的地也是 IPv4。
- 可以在多条 NAT 规则中使用同一映射对象或组。
- 映射 IP 地址池不能包括：
 - 映射接口的 IP 地址。如果为该规则指定“any”接口，则禁止所有接口 IP 地址。对于接口 PAT（仅路由模式），指定接口名称而不是接口地址。
 - 故障切换接口 IP 地址。
 - （透明模式。）管理 IP 地址。
 - （动态 NAT。）启用 VPN 时的备用接口 IP 地址。
 - 现有的 VPN 池地址。
- 避免在静态和动态 NAT 策略中使用重叠地址。例如，使用重叠地址，如果 PPTP 的辅助连接命中静态而非动态 xlate，将无法建立 PPTP 连接。
- 有关 NAT 或 PAT 的应用检测限制，请参阅[默认检测和 NAT 限制](#)，第 312 页。

- (8.3(1)、8.3(2)和8.4(1)) 用于身份 NAT 的默认行为已禁用代理 ARP。无法配置此设置。(8.4(2)及更高版本) 用于身份 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。如果需要，可以禁用代理 ARP。有关详细信息，请参阅[路由 NAT 数据包](#)，第 260 页。
- 启用 **arp permit-nonconnected** 命令时，如果映射地址不是任何已连接子网的一部分，并且没有在 NAT 规则中指定映射接口（即，指定“任何”接口），系统不会响应 ARP 请求。要解决此问题，请指定映射接口。
- 如果在规则中指定目的地接口，则该接口用作出口接口，而不是在路由表中查找路由。但是，对于身份 NAT，您可以选择改为使用路由查找。在 8.3 (1) 到 8.4 (1) 中，身份 NAT 总是使用路由表。
- 可使用 NAT 的事务提交模式提高系统性能和可靠性。有关详细信息，请参阅常规操作配置指南中的基本设置章节。该选项位于 **配置 > 设备管理 > 高级 > 规则引擎** 下。

映射地址对象的网络对象 NAT 指南

对于动态 NAT，必须为映射地址使用一个对象或组。对于其他 NAT 类型，可以使用对象或组，或者选择使用内联地址。在使用不连续的 IP 地址范围、多个主机或子网创建映射地址池时，网络对象组特别有用。

为映射地址创建对象时，请注意以下指导原则。

- 网络对象组可以包含多个对象或 IPv4 或 IPv6 地址的内联地址。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。
- 有关不允许的映射 IP 地址的详细信息，请参阅[其他 NAT 指南](#)，第 177 页。
- 动态 NAT：
 - 不能使用内联地址；必须配置一个网络对象或组。
 - 对象或组不能包含子网；对象必须定义一个范围；组可以包含主机和范围。
 - 如果映射网络对象同时包含范围和主机 IP 地址，则范围可用于动态 NAT，主机 IP 地址可用作 PAT 回退。
- 动态 PAT（隐藏）：
 - 如果不使用对象，可以选择配置内联主机地址或指定接口地址。
 - 如果使用对象，则对象或组不可以包含子网。对象必须定义主机，对于 PAT 池，则必须定义范围。组（对于 PAT 池）可以包含主机和范围。
- 静态 NAT 或支持端口转换的静态 NAT：
 - 如果不使用对象，可以配置内联地址，或者指定接口地址（对于带端口转换的静态 NAT）。
 - 如果使用对象，对象或组可以包含主机、范围或子网。
- 身份 NAT

- 如果不使用对象，可以配置内联地址。
- 如果使用对象，对象必须匹配要转换的实际地址。

用于实际与映射地址对象的两次 NAT 准则

对于每条 NAT 规则，均可为以下地址配置最多四个网络对象或组：

- 源实际地址
- 源映射地址
- 目标实际地址
- 目标映射地址

除非以内联方式指定 **any** 关键字来代表所有流量，或对于某些类型的 NAT，指定 **interface** 关键字来代表接口地址，否则需要配置对象。在使用不连续的 IP 地址范围、多个主机或子网创建映射地址池时，网络对象组特别有用。

为两次 NAT 创建对象时，请注意以下指导原则。

- 网络对象组可以包含多个对象或 IPv4 或 IPv6 地址的内联地址。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。
- 有关不允许的映射 IP 地址的详细信息，请参阅[其他 NAT 指南](#)，第 177 页。
- 源动态 NAT：
 - 通常要配置将较大实际地址组映射至较小的组。
 - 映射对象或组不能包含子网；对象必须定义一个范围；组可以包含主机和范围。
 - 如果映射网络对象同时包含范围和主机 IP 地址，则范围可用于动态 NAT，主机 IP 地址可用作 PAT 回退。
- 源动态 PAT（隐藏）：
 - 如果使用对象，则对象或组不可以包含子网。对象必须定义主机，对于 PAT 池，则必须定义范围。组（对于 PAT 池）可以包含主机和范围。
- 源静态 NAT 或支持端口转换的静态 NAT：
 - 映射对象或组可能包含主机、范围或子网。
 - 静态映射通常为一对一，因此实际地址的数量与映射地址相同。然而，如果需要，可拥有不同的数量。
- 源身份 NAT
 - 实际对象和映射对象必须匹配。可以为这二者使用相同对象，也可以单独创建包含相同 IP 地址的对象。

- 目标静态 NAT 或支持端口转换的静态 NAT（目标转换始终为静态）：
 - 尽管两次 NAT 的主要功能是纳入目标 IP 地址，但目标地址是可选的。如果确实指定目标地址，则可为该地址配置静态转换，或只将身份 NAT 用于该地址。可能需要配置没有目标地址的两次 NAT，以利用两次 NAT 的一些其他特性，包括使用实际地址的网络对象组或对规则手动排序。有关详细信息，请参阅[比较网络对象 NAT 和 两次 NAT](#)，第 173 页。
 - 对于身份 NAT，实际对象和映射对象必须匹配。可以为这二者使用相同对象，也可以单独创建包含相同 IP 地址的对象。
 - 静态映射通常为一对一，因此实际地址的数量与映射地址相同。然而，如果需要，可拥有不同的数量。
 - 对于支持端口转换的静态接口 NAT（仅路由模式），可指定 **interface** 关键字，而不是映射地址的网络对象/组。

实际和映射端口服务对象的两次 NAT 指南

可以选择为以下端口配置服务对象：

- 源实际端口（仅静态）或目标实际端口
- 源映射端口（仅静态）或目标映射端口

为两次 NAT 创建对象时，请注意以下指导原则。

- NAT 仅支持 TCP、UDP 和 SCTP。在转换端口时，请确保实际服务对象与映射服务对象中的协议完全相同（例如，同为 TCP）。虽然可以使用 SCTP 端口说明配置静态两次 NAT 规则，但建议不要这样操作，因为 SCTP 关联的目标端口的拓扑未知。请使用静态对象 NAT 代替 SCTP。
- 不支持“不等于”(**neq**)运算符。
- 对于身份端口转换，可将相同的服务对象同时用于实际和映射端口。
- 源动态 NAT - 源动态 NAT 不支持端口转换。
- 源动态 PAT（隐藏）- 源动态 PAT 不支持端口转换。
- 源静态 NAT、支持端口转换的静态 NAT，或身份 NAT - 服务对象可能同时包含源和目标端口；然而，应为两个服务对象指定源或目标端口。如果应用使用固定的源端口（如某些 DNS 服务器），则您只能同时指定源和目标端口；然而，很少使用固定源端口。例如，如果要转换源主机的端口，则请配置源服务。
- 目标静态 NAT 或支持端口转换的静态 NAT（目标转换始终为静态）- 对于非静态源 NAT，只能对目标执行端口转换。服务对象可能同时包含源和目标端口，但在此情况下，将仅使用目标端口。系统将忽略您指定的源端口。

动态 NAT

以下主题介绍动态 NAT 以及如何配置动态 NAT。

关于动态 NAT

动态 NAT 将一个实际地址组转换为一个可在目标目的网络上路由的映射地址池。映射池通常包含少于实际地址组的地址。当您要转换的主机访问目标目的网络时，NAT 会从映射池中为该主机分配 IP 地址。仅在实际主机发起连接时创建转换。转换仅在连接期间发生，而且转换超时后，给定用户不保持同一 IP 地址。因此，目的网络上的用户不能向使用动态 NAT 的主机发起可靠连接，即使访问规则允许该连接。

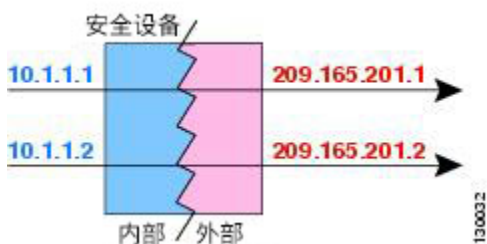


注释

在转换期间，如果访问规则允许连接转换后主机，远程主机可以发起这种连接。因为地址不可预测，所以与主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。

下图显示典型的动态 NAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。

图 18: 动态 NAT



下图显示一台远程主机尝试发起到映射地址的连接。该地址当前不在转换表中；因此，会丢弃数据包。

图 19: 远程主机尝试向映射地址发起连接



动态 NAT 不足和优势

动态 NAT 有以下缺点：

- 如果映射池的地址少于实际组，并且流量数量大于预期，地址可能会用尽。
如果经常发生这种情况，请使用 PAT 或 PAT 回退方法，因为 PAT 可以使用单一地址的端口提供超过 64,000 次转换。
- 不得不利用映射池中的大量可路由地址，而且可能没有大量的可路由地址可用。

动态 NAT 的优点在于，某些协议不能使用 PAT。PAT 不适用于以下项：

- 没有超载端口的 IP 协议，例如 GRE 0 版本。
- 某些多媒体应用，它们在一个端口上有数据流，在另一个端口上有控制路径，并且不是开放标准。

有关 NAT 和 PAT 支持的详细信息，请参阅[默认检测和 NAT 限制](#)，第 312 页。

配置动态网络对象 NAT

本节介绍如何为动态 NAT 配置网络对象 NAT。

过程

步骤 1 将 NAT 添加到新的或现有的网络对象中：

- 要添加新的网络对象，请依次选择 **Configuration > Firewall > NAT Rules**，然后依次点击 **Add > Add Network Object NAT Rule**。
- 要将 NAT 添加到现有的网络对象中，请依次选择 **Configuration > Firewall > Objects > Network Objects/Groups**，然后编辑网络对象。

步骤 2 对于新对象，请为以下字段输入值：

- Name** - 对象名称。使用字符 a 到 z、A 到 Z、0 到 9、句号、破折号、逗号或下划线。名称不得超过 64 个字符。
- Type** - 主机、网络或范围。
- IP Addresses** - IPv4 或 IPv6 地址、主机的单一地址、范围的开始和结束地址，以及子网的 IPv4 网络地址和掩码（例如 10.100.10.0 255.255.255.0）或 IPv6 地址和前缀长度（例如 2001:DB8:0:CD30::/60）。

步骤 3 如果 NAT 部分隐藏，请点击 **NAT** 展开此部分。

步骤 4 选中 **Add Automatic Translation Rules** 复选框。

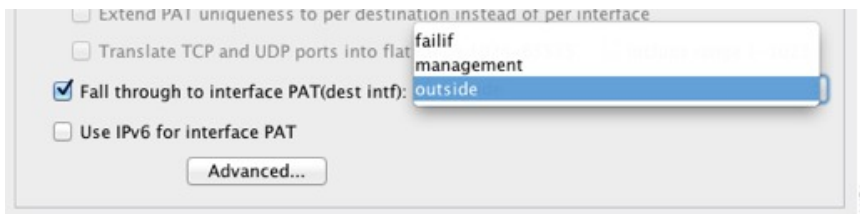
步骤 5 从 **Type** 下拉列表中选择 **Dynamic**。

步骤 6 在 **Translated Addr** 字段右侧，点击浏览按钮并选择包含映射地址的网络对象或网络对象组。

如有必要，可以创建新对象。

对象或组不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。

步骤 7 (可选, 仅限映射接口不是网桥组成员时。) 当其他映射地址已被分配时, 要使用接口 IP 地址作为备份方法, 请选中 **Fall through to interface PAT (dest intf)** 复选框, 并从下拉列表中选择接口。要使用接口的 IPv6 地址, 另请选中 **Use IPv6 for interface PAT** 复选框。



步骤 8 (可选) 点击 **Advanced**, 在 Advanced NAT Settings 对话框中配置以下选项, 然后点击 **OK**。

- **Translate DNS replies for rule** - 转换 DNS 应答中的 IP 地址。确保启用 DNS 检测 (默认情况下启用)。有关详细信息, 请参阅 [使用 NAT 重写 DNS 查询和响应](#), 第 277 页。
- (对于桥接组成员接口需要填入。) **Interface** - 指定应用此 NAT 规则时的实际接口 (源) 和映射接口 (目标)。默认情况下, 该规则将应用于所有接口, 桥接组成员除外。

步骤 9 点击 **OK**, 然后点击 **Apply**。

配置静态两次 NAT

本节介绍如何为动态 NAT 配置两次 NAT。

过程

步骤 1 依次选择配置 > 防火墙 > NAT 规则, 然后执行下列操作之一:

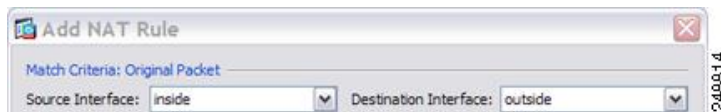
- 点击 **Add**, 或依次点击 **Add > Add NAT Rule Before Network Object NAT Rules**。
- 点击 **Add > Add NAT Rule After Network Object NAT Rules**。
- 选择一条两次 NAT 规则, 然后点击 **Edit**。

系统将显示 Add NAT Rule 对话框。

步骤 2 (对于桥接组成员接口需要填入。) 设置源和目标接口。

在路由模式下，默认源和目标均采用 any 接口。可以为一个或两个选项选择特定接口。但是，必须在为桥接组成员接口写入规则时选择接口；“any”不包括这些接口。

- 从 **Match Criteria: Original Packet > Source Interface** 下拉列表中选择源接口。
- 从 **Match Criteria: Original Packet > Destination Interface** 下拉列表中选择目标接口。

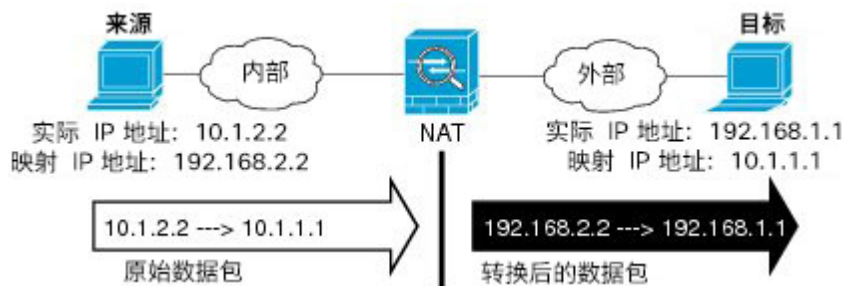


步骤 3 从操作：转换后的数据包 > 源 NAT 类型下拉列表中选择 动态。

该设置仅应用于源地址；目标转换始终为静态。



步骤 4 确定原始数据包地址 (IPv4 或 IPv6 地址)；即源接口网络上显示的数据包地址 (实际源地址和映射目标地址)。请参阅下图，了解原始数据包与转换后数据包的示例。



- a) 对于 **Match Criteria: Original Packet > Source Address**，从 Browse Original Source Address 对话框，点击浏览按钮，并选择现有网络对象或组，或创建新的对象或组。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。默认设置为 **any**。
- b) （可选。）对于 **Match Criteria: Original Packet > Destination Address**，点击浏览按钮选择现有的网络对象、组或接口，或在 Browse Original Destination Address 对话框中创建新对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。

尽管两次 NAT 的主要功能是纳入目标 IP 地址，但目标地址是可选的。如果确实指定目标地址，则可为该地址配置静态转换，或只将身份 NAT 用于该地址。可能需要配置没有目标地址的两次 NAT，以利用两次 NAT 的一些其他特性，包括使用实际地址的网络对象组或对规则手动排序。有关详细信息，请参阅[比较网络对象 NAT 和 两次 NAT](#)，第 173 页。

对于仅支持端口转换的静态接口 NAT，请从 Browse 对话框选择接口。务必同时配置服务转换。对于此选项，必须为 Source Interface 配置特定接口。有关详细信息，请参阅[支持端口转换的静态 NAT](#)，第 209 页。

步骤 5 确定转换后的数据包地址（IPv4 或 IPv6 地址）；即目标接口网络上显示的数据包地址（映射源地址和实际目标地址）。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- a) 对于 **Action: Translated Packet > Source Address**，从 Browse Translated Source Address 对话框，点击浏览按钮，并选择现有网络对象或组，或创建新的对象或组。

对于动态 NAT，通常会配置将较大源地址组映射至较小的组。

注释 对象或组不能包含子网。

- b) 对于 **Action: Translated Packet > Destination Address**，从 Browse Translated Destination Address 对话框，点击浏览按钮并选择现有网络对象或组，或创建新的对象或组。

对于用于目标地址的身份 NAT，只需将相同的对象或组同时用于实际和映射地址。

如果要转换目标地址，则静态映射通常为一对一，因此实际地址的数量与映射地址相同。然而，如果需要，可拥有不同的数量。有关详细信息，请参阅[静态 NAT](#)，第 209 页。有关不允许的映射 IP 地址的详细信息，请参阅[其他 NAT 指南](#)，第 177 页。

步骤 6 （可选。）为服务转换确定目标服务端口。

- 确定原始数据包端口（映射目标端口）。对于 **Match Criteria: Original Packet > Service**，从 Browse Original Service 对话框，点击浏览按钮并选择指定 TCP 或 UDP 端口的现有服务对象，或创建新的对象。

- 确定转换后的数据包端口（实际目标端口）。对于 **Action: Translated Packet > Service**，从 **Browse Translated Service** 对话框，点击浏览按钮并选择指定 TCP 或 UDP 端口的现有服务对象，或创建新的对象。

动态 NAT 不支持端口转换。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。服务对象可能同时包含源和目标端口，但在此情况下，将仅使用目标端口。系统将忽略您指定的源端口。NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。不支持“不等于”(!=) 运算符。

例如：

The screenshot shows the 'Add Service Object' dialog box with the following fields:

- Name: web
- Service Type: tcp
- Destination Port/Range: 80
- Source Port/Range: (empty)
- Description: (empty)

Buttons: Help, Cancel, OK

The screenshot shows the 'Match Criteria: Original Packet' dialog box with the following fields:

- Source Interface: inside
- Destination Interface: outside
- Source Address: obj-192.168.251.164
- Destination Address: obj-172.25.23.32
- Service: web

The screenshot shows the 'Add Service Object' dialog box with the following fields:

- Name: web_map
- Service Type: tcp
- Destination Port/Range: 8080
- Source Port/Range: (empty)
- Description: (empty)

Buttons: Help, Cancel, OK

步骤 7 (可选, 仅限映射接口不是桥接组成员时。) 如果其他映射源地址已分配, 要将接口 IP 地址用作备份方法, 则请选中 **Fall through to interface PAT** 复选框。要使用 IPv6 接口地址, 另请选中 **Use IPv6 for interface PAT** 复选框。

将使用目标接口 IP 地址。只有配置特定目标接口, 此选项才可用。

步骤 8 (可选。) 在 Options 区域中配置 NAT 选项

- **Enable rule** - 启用此 NAT 规则。该规则默认启用。
- (对于源专用规则) **Translate DNS replies that match this rule** - 在 DNS 应答中重写 DNS A 记录。确保启用 DNS 检测 (默认情况下启用)。如果配置目标地址, 则无法配置 DNS 修改。有关详细信息, 请参阅 [使用 NAT 重写 DNS 查询和响应](#), 第 277 页。
- **Description** - 添加规则的相关说明, 最长 200 个字符。

步骤 9 点击 **OK**, 然后点击 **Apply**。

动态 PAT

以下主题介绍动态 PAT。

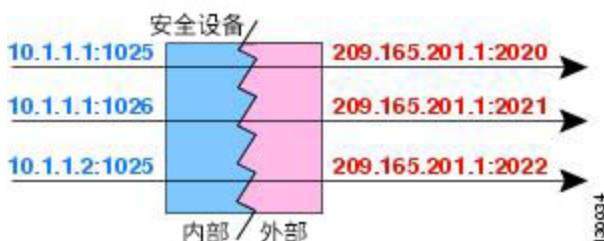
关于动态 PAT

通过将实际地址和源端口转换为映射地址和唯一端口，动态 PAT 可以将多个实际地址转换为单一映射地址。如果可用，实际源端口号将用于映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。如果大量流量使用较小的端口范围，则可以指定使用以下不分段端口范围，代替三个分段大小不等的端口范围。

每个连接都需要单独的转换会话，因为每个连接的源端口都不同。例如，10.1.1.1:1025 需要来自 10.1.1.1:1026 的单独的转换。

下图显示一个典型的动态 PAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。映射地址对于每次转换都是相同的，但端口需要动态分配。

图 20: 动态 PAT



对于转换持续时间，如果访问规则允许，目标网络上的远程主机可以发起到转换后主机的连接。因为端口地址（实际和映射）不可预测，所以到该主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。

在连接过期后，端口转换也将过期。对于多会话 PAT，使用 PAT 超时，默认情况下为 30 秒。对于每会话 PAT（9.0(1) 及更高版本），会立即删除 xlate。



注释 建议每个接口使用不同的 PAT 池。如果多个接口使用同一池，尤其是用于“任何”接口时，该池将被快速耗尽，且没有端口可用于新的转换。

动态 PAT 不足和优势

通过动态 PAT，可以使用单一映射地址，从而保存可路由地址。甚至可以将 ASA 接口 IP 地址用作 PAT 地址。

在同属一个桥接组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于接口为不同网桥组桥接组成员或一个接口为网桥组桥接组成员，另一个为标准路由接口的情况。

动态 PAT 不适用于某些数据流不同于控制路径的多媒体应用。有关 NAT 和 PAT 支持的详细信息，请参阅[默认检测和 NAT 限制](#)，第 312 页。

动态 PAT 还可以创建大量显示为来自单一 IP 地址的连接，服务器可能将此流量解释为 DoS 攻击。可以配置一个 PAT 地址池，使用 PAT 地址轮询分配来避免出现这种情况。

PAT 池对象指南

当为 PAT 池创建网络对象时，请遵守以下指导原则。

对于 PAT 池

- 如果可用，实际源端口号将用于映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。如果使用较小端口范围的流量庞大，可以指定使用不分段的端口范围来代替三个大小不等的分层：1024 至 65535 或 1 至 65535。
- 如果对 PAT 池启用块分配，则仅在 1024-65535 范围内分配端口块。因此，如果应用需要较低的端口号 (1-1023)，它可能不起作用。例如，请求端口 22 (SSH) 的应用将获得 1024-65535 范围内和分配到主机的块范围内的映射端口。
- 如在两个不同的规则中使用相同的 PAT 池对象，则请确保为每条规则指定相同的选项。例如，如果一条规则指定扩展 PAT 和不分段范围，则另一条规则也必须指定扩展 PAT 和无层次的范围。

对于 PAT 池的扩展 PAT

- 许多应用检测不支持扩展 PAT。有关不支持的检测的完整列表，请参阅[默认检测和 NAT 限制](#)，第 312 页。
- 如为动态 PAT 规则启用扩展 PAT，则不能在支持端口转换规则的另一静态 NAT 中使用 PAT 池中的地址作为 PAT 地址。例如，如果 PAT 池包括 10.1.1.1，则无法将 10.1.1.1 作为 PAT 地址创建带端口转换规则的静态 NAT。
- 如使用 PAT 池，并为回退指定接口，则无法指定扩展 PAT。
- 对于使用 ICE 或 TURN 的 VoIP 部署，请勿使用扩展 PAT。ICE 和 TURN 依赖于 PAT 绑定才能对所有目标均保持相同。

对于 PAT 池的轮询

- 如果主机拥有现有连接，并且端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。不过，这种“粘性”不能超越故障切换。如果该设备执行故障切换，来自主机的后续连接可能会使用初始 IP 地址。
- 如果在同一接口混合使用 PAT 池/轮询规则和接口 PAT 规则，IP 地址“粘性”也会受到影响。对于任何给定接口，请选择 PAT 池或接口 PAT；请勿创建竞争 PAT 规则。

- 轮询可能会消耗大量的内存，在与扩展 PAT 组合使用时尤其如此。由于将为每一个映射协议/IP 地址/端口范围创建 NAT 池，因此，轮询会导致大量并发 NAT 池，从而消耗内存。扩展 PAT 甚至将导致更多数量的并发 NAT 池。

配置动态网络对象 PAT（隐藏）

本节介绍如何为动态 PAT（隐藏）配置网络对象 NAT，该 PAT 使用单个地址而不是 PAT 池进行转换。

过程

步骤 1 将 NAT 添加到新的或现有的网络对象中：

- 要添加新的网络对象，请依次选择 **Configuration > Firewall > NAT Rules**，然后依次点击 **Add > Add Network Object NAT Rule**。
- 要将 NAT 添加到现有的网络对象中，请依次选择 **Configuration > Firewall > Objects > Network Objects/Groups**，然后编辑网络对象。

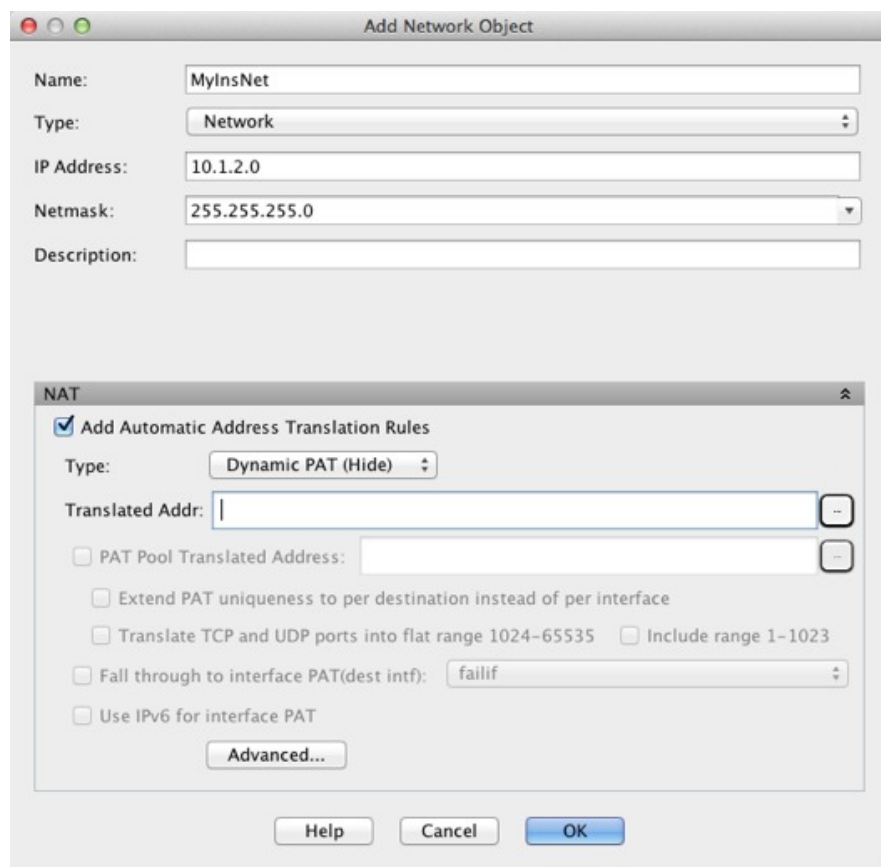
步骤 2 对于新对象，请为以下字段输入值：

- a) **Name** - 对象名称。使用字符 a 到 z、A 到 Z、0 到 9、句号、破折号、逗号或下划线。名称不得超过 64 个字符。
- b) **Type** - 主机、网络或范围。
- c) **IP Addresses** - IPv4 或 IPv6 地址、主机的单一地址、范围的开始和结束地址，以及子网的 IPv4 网络地址和掩码（例如 10.100.10.0 255.255.255.0）或 IPv6 地址和前缀长度（例如 2001:DB8:0:CD30::/60）。

步骤 3 如果 NAT 部分隐藏，请点击 **NAT** 展开此部分。

步骤 4 选中 **Add Automatic Translation Rules** 复选框。

步骤 5 从 Type 下拉列表中选择 **Dynamic PAT (Hide)**。



步骤 6 指定单一映射地址。通过执行以下任一操作，在 Translated Addr. 字段中指定映射 IP 地址：

- 键入主机 IP 地址。
- 点击浏览按钮并选择主机网络对象（或创建一个新的主机网络对象）。
- （仅限非网桥组成员接口。）键入接口名称或点击浏览按钮，从 Browse Translated Addr 对话框中选择一个接口。



如果指定一个接口名称，则可以启用 *interface PAT*，其中指定的接口 IP 地址用作映射地址。要使用 IPv6 接口地址，还必须选中 **Use IPv6 for interface PAT** 复选框。使用接口 PAT 时，NAT 规则将应用于指定的映射接口，不包括桥接组成员。（如果不使用接口 PAT，则默认将规则应用于所有接口。）不能在透明模式下指定接口。

步骤 7 （可选。）点击 **Advanced**，在 Advanced NAT Settings 对话框中配置以下选项，然后点击 **OK**。

- （对于桥接组成员接口需要填入。）**Interface** - 指定应用此 NAT 规则时的实际接口（源）和映射接口（目标）。默认情况下，该规则将应用于所有接口，桥接组成员除外。

步骤 8 点击 **OK**，然后点击 **Apply**。

使用 PAT 池配置动态网络对象 PAT

本节介绍如何使用 PAT 池为动态 PAT 配置网络对象 NAT。

过程

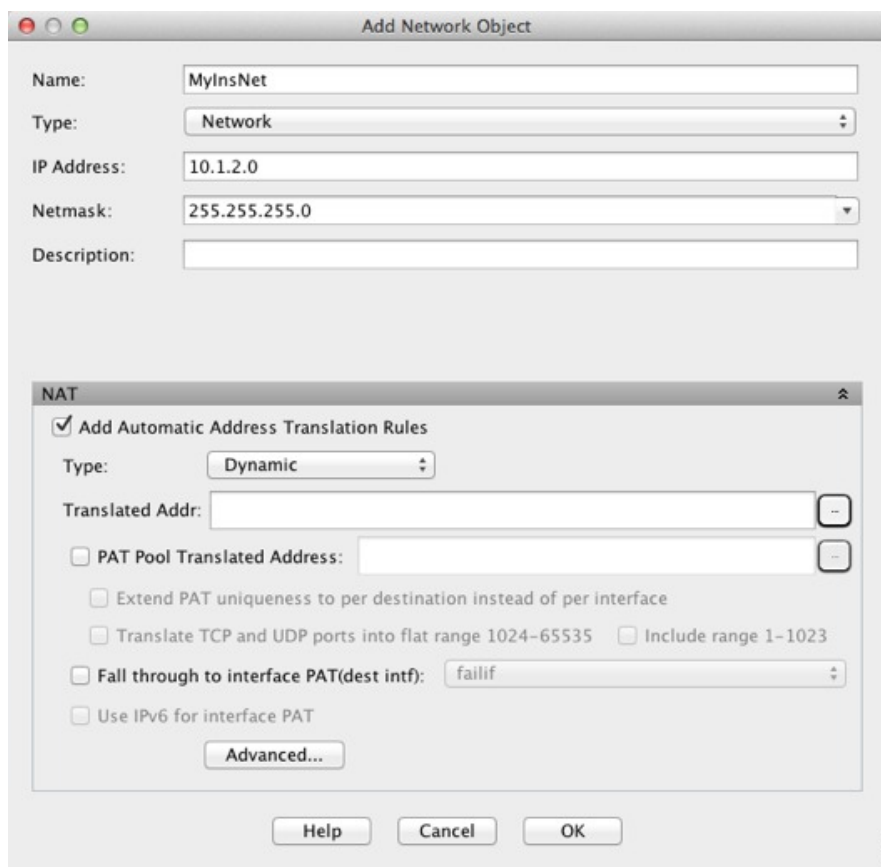
步骤 1 将 NAT 添加到新的或现有的网络对象中：

- 要添加新的网络对象 NAT 规则，请依次选择 **Configuration > Firewall > NAT Rules**，然后点击 **Add > Add Network Object NAT Rule**。
- 要向现有网络对象中添加 NAT，请依次选择 **Configuration > Firewall > Objects > Network Objects/Groups**，然后编辑网络对象。

步骤 2 对于新对象，请为以下字段输入值：

- a) **Name** - 对象名称。使用字符 a 到 z、A 到 Z、0 到 9、句号、破折号、逗号或下划线。名称不得超过 64 个字符。
- b) **Type** - 主机、网络或范围。
- c) **IP Addresses** - IPv4 或 IPv6 地址、主机的单一地址、范围的开始和结束地址，以及子网的 IPv4 网络地址和掩码（例如 10.100.10.0 255.255.255.0）或 IPv6 地址和前缀长度（例如 2001:DB8:0:CD30::/60）。

步骤 3 如果 NAT 部分隐藏，请点击 **NAT** 展开此部分。



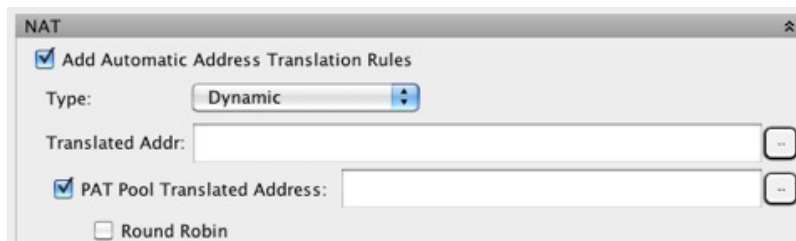
步骤 4 选中 **Add Automatic Translation Rules** 复选框。

步骤 5 从 Type 下拉列表中选择 **Dynamic**，即使正在使用 PAT 池配置动态 PAT 也是如此。

步骤 6 要配置 PAT 池，请执行以下步骤：

- a) 请勿为 Translated Addr. 字段输入值；将此字段留空。
- b) 选中 **PAT Pool Translated Address** 复选框，然后点击浏览按钮并选择包含 PAT 池地址的网络对象或组。或者，从 Browse Translated PAT Pool Address 对话框中创建一个新对象。

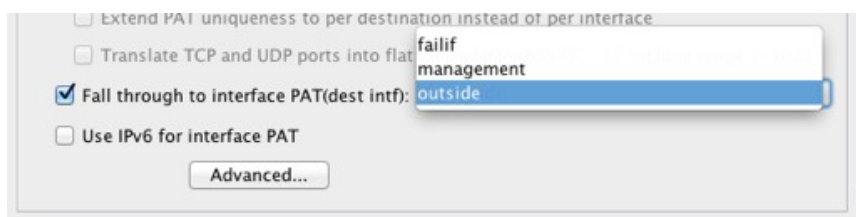
注释 PAT 池对象或组不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。



- c) (可选) 根据需要选择以下选项：

- **Round Robin** - 以轮询方式分配地址和端口。默认情况下，如果不采用轮询，在使用下一个 PAT 地址之前，将分配 PAT 地址的所有端口。在返回再次使用第一个地址、第二个地址等等之前，轮询方法可以从池中的每个 PAT 地址分配一个地址/端口。
- **Extend PAT uniqueness to per destination instead of per interface** (8.4(3) 及更高版本，不包含 8.5(1) 或 8.6(1)) - 使用扩展 PAT。通过将目的地地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。通常，创建 PAT 转换时，不考虑目的地端口和地址，因此限制为每个 PAT 地址 65535 个端口。例如，通过扩展 PAT，您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换，以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。
- **Translate TCP or UDP ports into flat range (1024-65535)** (8.4(3) 及更高版本，不包括 8.5(1) 后 8.6(1)) - 在分配端口时使用 1024 至 65535 端口范围作为单一不分段范围。当选择要转换的映射端口号时，ASA 将使用实际源端口号（如果可用）。然而，如果不使用此选项，则当实际端口不可用时，将默认从与实际端口号相同的端口范围选择映射端口：1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口，请配置此设置。要使用 1 至 65535 的整个范围，请也选择 **Include range 1 to 1023** 复选框。
- **Enable Block Allocation** (9.5.1 及更高版本) - 启用端口块分配。对于运营商级或大规模 PAT，可以为每个主机分配一个端口块，而非由 NAT 每次分配一个端口转换。如果分配端口块，来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中，可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与轮询兼容，但无法将其与扩展 PAT 或不分段端口范围选项一起使用。也无法使用接口 PAT 回退。

步骤 7（可选，仅限映射接口不是桥接组成员时。）当其他映射源地址已被分配时，要使用接口 IP 地址作为备份方法，请选中 **Fall through to interface PAT** 复选框，并从下拉列表中选择接口。要使用该接口的 IPv6 地址，另请选中 **Use IPv6 for interface PAT** 复选框。



步骤 8（可选）点击 **Advanced**，在 Advanced NAT Settings 对话框中配置以下选项，然后点击 **OK**。

- （对于桥接组成员接口需要填入。）**Interface** - 指定应用此 NAT 规则时的实际接口（源）和映射接口（目标）。默认情况下，该规则将应用于所有接口，桥接组成员除外。

步骤 9 点击 **OK**，然后点击 **Apply**。

配置静态两次 PAT（隐藏）

本节介绍如何为动态 PAT（隐藏）配置两次 NAT，使用单个地址而不是 PAT 池进行转换。

过程

步骤 1 依次选择配置 > 防火墙 > NAT 规则，然后执行下列操作之一：

- 点击 **Add**，或依次点击 **Add > Add NAT Rule Before Network Object NAT Rules**。
- 点击 **Add > Add NAT Rule After Network Object NAT Rules**。
- 选择一条两次 NAT 规则，然后点击 **Edit**。

系统将显示 Add NAT Rule 对话框。

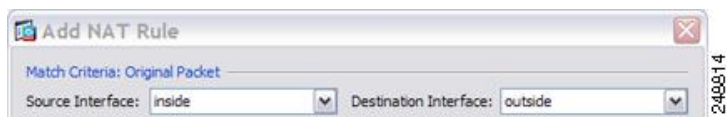
The screenshot shows the 'Add NAT Rule' dialog box with the following configuration:

- Match Criteria: Original Packet**
 - Source Interface: -- Any --
 - Destination Interface: -- Any --
 - Source Address: any
 - Destination Address: any
 - Service: any
- Action: Translated Packet**
 - Source NAT Type: Static
 - Source Address: -- Original --
 - Destination Address: -- Original --
 - Use one-to-one address translation:
 - PAT Pool Translated Address:
 - Round Robin:
 - Extend PAT uniqueness to per destination instead of per interface:
 - Translate TCP and UDP ports into flat range 1024-65535:
 - Include range 1-1023:
 - Fall through to interface PAT:
 - Use IPv6 for interface PAT:
- Options**
 - Enable rule:
 - Translate DNS replies that match this rule:
 - Disable Proxy ARP on egress interface:
 - Lookup route table to locate egress interface:
- Direction: Both
- Description: (empty field)

步骤 2 (对于桥接组成员接口需要填入。) 设置源和目标接口。

在路由模式下，默认源和目标均采用 any 接口。可以为一个或两个选项选择特定接口。但是，必须在为桥接组成员接口写入规则时选择接口；“any”不包括这些接口。

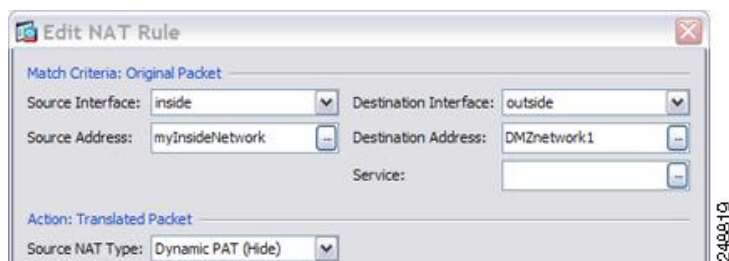
- a) 从 **Match Criteria: Original Packet > Source Interface** 下拉列表中选择源接口。
- b) 从 **Match Criteria: Original Packet > Destination Interface** 下拉列表中选择目标接口。



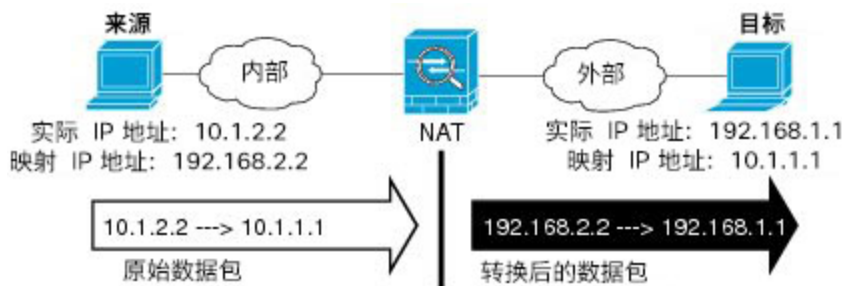
步骤 3 从操作：转换后的数据包 > 源 NAT 类型下拉列表中选择动态 PAT（隐藏）。

该设置仅应用于源地址；目标转换始终为静态。

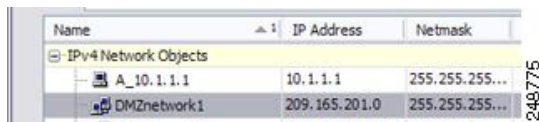
注释 要使用 PAT 池配置动态 PAT，请选择 **Dynamic**，而不是 Dynamic PAT (Hide)，详见[使用 PAT 池配置动态两次 PAT](#)，第 201 页。



步骤 4 确定原始数据包地址（IPv4 或 IPv6 地址）；即源接口网络上显示的数据包地址（实际源地址和映射目标地址）。请参阅下图，了解原始数据包与转换后数据包的示例。



- a) 对于 **Match Criteria: Original Packet > Source Address**，从 Browse Original Source Address 对话框，点击浏览按钮，并选择现有网络对象或组，或创建新的对象或组。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。默认设置为 **any**。



- b) （可选）对于 **Match Criteria: Original Packet > Destination Address**，从 Browse Original Destination Address 对话框，点击浏览按钮并选择现有网络对象、组或接口（仅限非桥接组成员接口），或创建新的对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。

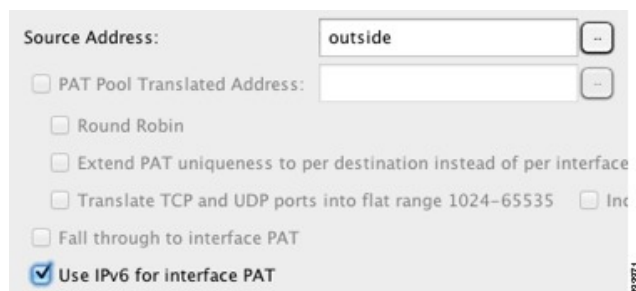
尽管两次 NAT 的主要功能是纳入目标 IP 地址，但目标地址是可选的。如果确实指定目标地址，则可为该地址配置静态转换，或只将身份 NAT 用于该地址。可能需要配置没有目标地址的两次 NAT，以利用两次 NAT 的一些其他特性，包括使用实际地址的网络对象组或对规则手动排序。有关详细信息，请参阅[比较网络对象 NAT 和两次 NAT](#)，第 173 页。

对于仅支持端口转换的静态接口 NAT，请从 **Browse** 对话框选择接口。务必同时配置服务转换。对于此选项，必须为 **Source Interface** 配置特定接口。有关详细信息，请参阅[支持端口转换的静态 NAT](#)，第 209 页。

步骤 5 确定转换后的数据包地址（IPv4 或 IPv6 地址）；即目标接口网络上显示的数据包地址（映射源地址和实际目标地址）。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- a) 对于 **Action: Translated Packet > Source Address**，从 **Browse Translated Source Address** 对话框，点击浏览按钮并选择定义主机地址的现有网络对象或接口，或者创建新的对象。该接口不能是桥接组成员。

要使用接口的 IPv6 地址，请选中 **Use IPv6 for interface PAT** 复选框。



- b) (可选。)对于 **Action: Translated Packet > Destination Address**，从 **Browse Translated Destination Address** 对话框，点击浏览按钮并选择现有网络对象或组，或创建新的对象或组。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。

对于用于目标地址的身份 NAT，只需将相同的对象或组同时用于实际和映射地址。

如果要转换目标地址，则静态映射通常为一对一，因此实际地址的数量与映射地址相同。然而，如果需要，可拥有不同的数量。有关详细信息，请参阅[静态 NAT](#)，第 209 页。有关不允许的映射 IP 地址的详细信息，请参阅[NAT 指南](#)，第 176 页。

步骤 6 (可选。)为服务转换确定目标服务端口。

- 确定原始数据包端口（映射目标端口）。对于 **Match Criteria: Original Packet > Service**，从 **Browse Original Service** 对话框，点击浏览按钮并选择指定 TCP 或 UDP 端口的现有服务对象，或创建新的对象。
- 确定转换后的数据包端口（实际目标端口）。对于 **Action: Translated Packet > Service**，从 **Browse Translated Service** 对话框，点击浏览按钮并选择指定 TCP 或 UDP 端口的现有服务对象，或创建新的对象。

动态 NAT 不支持端口转换。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。服务对象可能同时包含源和目标端口，但在此情况下，将仅使用目标端口。系统将忽略您指定的源端口。NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。不支持“不等于”(!=) 运算符。

例如：

Add Service Object

Name: web

Service Type: tcp

Destination Port/Range: 80

Source Port/Range:

Description:

Help Cancel OK

Match Criteria: Original Packet

Source Interface: inside Destination Interface: outside

Source Address: obj-192.168.251.164 Destination Address: obj-172.25.23.32

Service: web

Add Service Object

Name: web_map

Service Type: tcp

Destination Port/Range: 8080

Source Port/Range:

Description:

Help Cancel OK

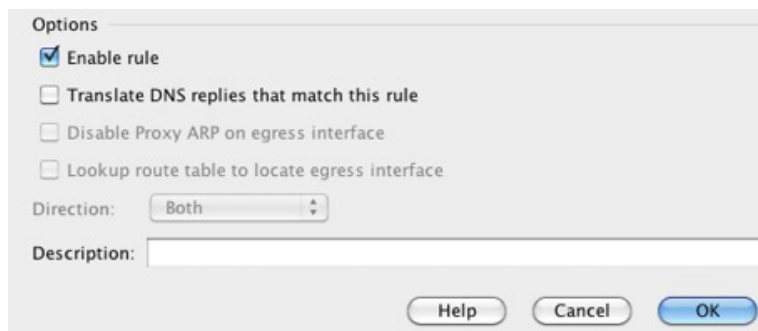
Action: Translated Packet

Source NAT Type: Static

Source Address: obj-192.168.252.128 Destination Address: obj-172.25.23.32

PAT Pool Translated Address: Service: web_map

步骤 7 (可选) 在 Options 区域中配置 NAT 选项。



Options

- Enable rule
- Translate DNS replies that match this rule
- Disable Proxy ARP on egress interface
- Lookup route table to locate egress interface

Direction: Both

Description:

Help Cancel OK

- **Enable rule** - 启用此 NAT 规则。该规则默认启用。
- **Description** - 添加规则的相关说明，最长 200 个字符。

步骤 8 点击 **OK**，然后点击 **Apply**。

使用 PAT 池配置动态两次 PAT

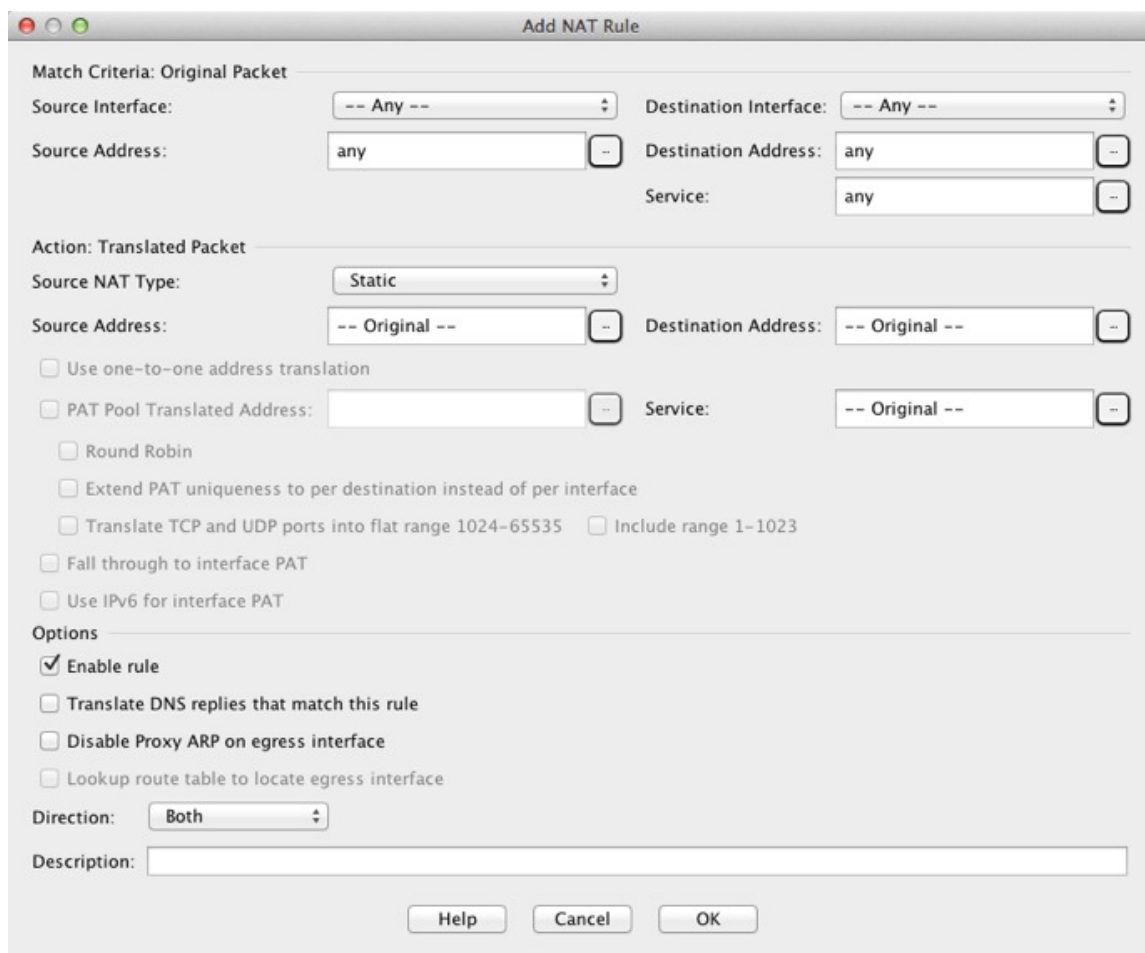
本节介绍如何使用 PAT 池为动态 PAT 配置两次 NAT。

过程

步骤 1 依次选择配置 > 防火墙 > NAT 规则，然后执行下列操作之一：

- 点击 **Add**，或依次点击 **Add > Add NAT Rule Before Network Object NAT Rules**。
- 依次点击 **Add > Add NAT Rule After Network Object NAT Rules**。
- 选择一条两次 NAT 规则，然后点击 **Edit**。

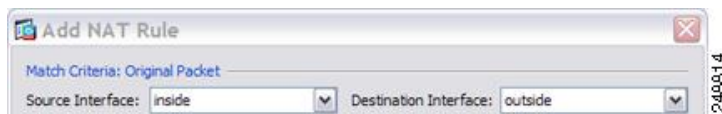
系统将显示 Add NAT Rule 对话框。



步骤 2 (对于桥接组成员接口需要填入。) 设置源和目标接口。

在路由模式下，默认源和目标均采用 any 接口。可以为一个或两个选项选择特定接口。但是，必须在为桥接组成员接口写入规则时选择接口；“any”不包括这些接口。

- 从 **Match Criteria: Original Packet > Source Interface** 下拉列表中选择源接口。
- 从 **Match Criteria: Original Packet > Destination Interface** 下拉列表中选择目标接口。

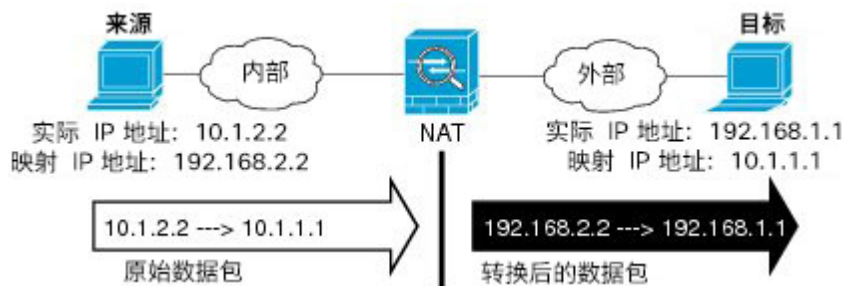


步骤 3 从操作：转换后的数据包 > 源 NAT 类型下拉列表中选择 动态。

该设置仅应用于源地址；目标转换始终为静态。



步骤 4 确定原始数据包地址（IPv4 或 IPv6 地址）；即源接口网络上显示的数据包地址（实际源地址和映射目标地址）。请参阅下图，了解原始数据包与转换后数据包的示例。



- a) 对于 **Match Criteria: Original Packet > Source Address**，从 Browse Original Source Address 对话框，点击浏览按钮并选择现有网络对象或组，或创建新的对象或组。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。默认设置为 **any**。
- b) （可选。）对于 **Match Criteria: Original Packet > Destination Address**，从 Browse Original Destination Address 对话框，点击浏览按钮并选择现有网络对象、组或接口（仅限非桥接组成员接口），或创建新的对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。

尽管两次 NAT 的主要功能是纳入目标 IP 地址，但目标地址是可选的。如果确实指定目标地址，则可为该地址配置静态转换，或只将身份 NAT 用于该地址。可能需要配置没有目标地址的两次 NAT，以利用两次 NAT 的一些其他特性，包括使用实际地址的网络对象组或对规则手动排序。有关详细信息，请参阅[比较网络对象 NAT 和两次 NAT](#)，第 173 页。

对于仅支持端口转换的静态接口 NAT，请从 Browse 对话框选择接口。务必同时配置服务转换。对于此选项，必须为 Source Interface 配置特定接口。有关详细信息，请参阅[支持端口转换的静态 NAT](#)，第 209 页。

步骤 5 确定转换后的数据包地址（IPv4 或 IPv6 地址）；即目标接口网络上显示的数据包地址（映射源地址和实际目标地址）。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- a) 选中 **PAT Pool Translated Address** 复选框，然后从 Browse Translated PAT Pool Address 对话框，点击浏览按钮并选择现有网络对象或组，或创建新的对象或组。**注意：**将 Source Address 字段留空。

Action: Translated Packet

Source NAT Type: Dynamic

Source Address: -- Original -- -- Destination Address: --

PAT Pool Translated Address: -- Service: --

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023

Fall through to interface PAT

注释 对象或组不能包含子网。

- b) （可选。）对于操作：**转换后的数据包 > 目标地址**，点击浏览按钮并选择现有网络对象或组，或在“浏览转换后的目标地址”对话框中创建一个新对象或组。

对于用于目标地址的身份 NAT，只需将相同的对象或组同时用于实际和映射地址。

如果要转换目标地址，则静态映射通常为一对一，因此实际地址的数量与映射地址相同。然而，如果需要，可拥有不同的数量。有关详细信息，请参阅[静态 NAT，第 209 页](#)。有关不允许的映射 IP 地址的详细信息，请参阅[NAT 指南，第 176 页](#)。

步骤 6 (可选。) 为服务转换确定目标服务端口。

- 确定原始数据包端口（映射目标端口）。对于**匹配条件：原始数据包 > 服务**，点击浏览按钮并选择指定 TCP 或 UDP 端口的现有服务对象或在“浏览原始服务”对话框中创建一个新对象。
- 确定转换后的数据包端口（实际目标端口）。对于**Action: Translated Packet > Service**，从 Browse Translated Service 对话框，点击浏览按钮并选择指定 TCP 或 UDP 端口的现有服务对象，或创建新的对象。

动态 NAT 不支持端口转换。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。服务对象可能同时包含源和目标端口，但在此情况下，将仅使用目标端口。系统将忽略您指定的源端口。NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。不支持“不等于”(!=) 运算符。

例如：

The screenshot shows the 'Add Service Object' dialog box with the following fields:

- Name: web
- Service Type: tcp
- Destination Port/Range: 80
- Source Port/Range: (empty)
- Description: (empty)

Buttons: Help, Cancel, OK

The screenshot shows the 'Match Criteria: Original Packet' dialog box with the following fields:

- Source Interface: inside
- Destination Interface: outside
- Source Address: obj-192.168.251.164
- Destination Address: obj-172.25.23.32
- Service: web

步骤 7 (可选。) 对于 PAT 池,请根据需要配置以下选项:

- **轮询** - 按轮询方式分配地址/端口。默认情况下, 如果不采用轮询, 在使用下一个 PAT 地址之前, 将分配 PAT 地址的所有端口。在返回再次使用第一个地址、第二个地址等等之前, 轮询方法可以从池中的每个 PAT 地址分配一个地址/端口。
- **Extend PAT uniqueness to per destination instead of per interface** (8.4(3) 及更高版本, 不包含 8.5(1) 或 8.6(1)。) - 使用扩展 PAT。通过将目的地地址和端口纳入转换信息, 相对于按 IP 地址, 扩展 PAT 将按服务使用 65535 个端口。通常, 创建 PAT 转换时, 不考虑目的地端口和地址, 因此限制为每个 PAT 地址 65535 个端口。例如, 通过扩展 PAT, 您可以创建在访问 192.168.1.7:23 时转到 10.1.1.1:1027 的转换, 以及在访问 192.168.1.7:80 时转到 10.1.1.1:1027 的转换。
- **Translate TCP or UDP ports into flat range (1024-65535)** (8.4(3) 及更高版本, 不包括 8.5(1) 后 8.6(1)。) - 在分配端口时使用 1024 至 65535 端口范围作为单一不分段范围。当选择要转换的映射端口号时, ASA 将使用实际源端口号 (如果可用)。然而, 如果不使用此选项, 则当实际端口不可用时, 将默认从与实际端口号相同的端口范围选择映射端口: 1 到 511、512 到 1023 以及 1024 到 65535。为了避免用尽低端口号范围的端口, 请配置此设置。要使用 1 至 65535 的整个范围, 请也选择 **Include range 1 to 1023** 复选框。
- **Enable Block Allocation** (9.5.1 及更高版本。) - 启用端口块分配。对于运营高级或大规模 PAT, 可以为每个主机分配一个端口块, 而非由 NAT 每次分配一个端口转换。如果分配端口块, 来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中, 可根据需要分配更多块。只能在 1024-65535 范围内分配端口块。端口块分配与轮询兼容, 但无法将其与扩展 PAT 或不分段端口范围选项一起使用。也无法使用接口 PAT 回退。

步骤 8 (可选, 仅限映射接口不是桥接组成员时。) 如果其他映射源地址已被分配, 要使用接口 IP 地址作为备份方法, 请选中 **Fall through to interface PAT** 复选框。要使用 IPv6 接口地址, 另请选中 **Use IPv6 for interface PAT** 复选框。

将使用目标接口 IP 地址。只有配置特定目标接口, 此选项才可用。

Action: Translated Packet

Source NAT Type: Dynamic

Source Address: group1

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535

Fall through to interface PAT

Use IPv6 for interface PAT

步骤 9 (可选。) 在 Options 区域中配置 NAT 选项

Options

Enable rule

Translate DNS replies that match this rule

Disable Proxy ARP on egress interface

Lookup route table to locate egress interface

Direction: Both

Description:

Help Cancel OK

- **Enable rule** - 启用此 NAT 规则。该规则默认启用。
- **Description** - 添加规则的相关说明, 最长 200 个字符。

步骤 10 点击 **OK**, 然后点击 **Apply**。

使用端口块分配配置 PAT

对于运营商级或大规模 PAT, 您可以为每台主机分配端口块, 而无需通过 NAT 一次分配一个端口转换 (请参阅 RFC 6888)。如果分配端口块, 来自该主机的后续连接将使用该块中随机选定的新端口。如果主机将所有端口的活动连接置于基元块中, 可根据需要分配更多块。当使用块中端口的最后一个转换被删除时, 系统将释放该块。

分配端口块的主要原因是为了减少日志记录。记录端口块分配, 记录连接, 但不会记录在端口块中创建的转换。另一方面, 这样会使日志分析变得更加复杂。

只能在 1024-65535 范围内分配端口块。因此, 如果应用需要较低的端口号 (1-1023), 它可能不起作用。例如, 请求端口 22 (SSH) 的应用将获得 1024-65535 范围内和分配到主机的块范围内的映射端

口。您可以创建一个单独的 NAT 规则，对于使用低端口号的应用不应用块分配；对于两次 NAT，请确保该规则位于块分配规则之前。

开始之前

NAT 规则的使用说明：

- 可以添加 **Round Robin** 选项，但不添加扩展 PAT 唯一性、使用宽范围或后退至接口 PAT 的选项。此外，还允许其他源/目标地址和端口信息。
- 同所有 NAT 变更一样，如果要替换现有的规则，必须清除与被替换规则相关的转换，新规则才会生效。可以显式清除它们，也可以静待它们超时。
- 对于特定 PAT 池，必须为使用该池的所有规则指定（或不指定）块分配。不能在一个规则中分配块，而在另一个规则中不分配块。重叠的 PAT 池也不能混合块分配设置。此外，该池的静态 NAT 不能与端口转换规则重叠。

过程

步骤 1 依次选择 **Configuration > Firewall > Advanced > PAT Port Block Allocation**，并配置以下设置：

- **Size of the block** - 每个块中的端口数。范围为 32-4096。默认值为 512。
如果不使用默认值，请确保 64,512 能被您所选的大小整除（1024-65535 范围中的端口数）。否则，会出现无法使用的端口。例如，如果指定 100，会有 12 个未使用端口。
- **Maximum block allocation per host** - 每个主机可分配的最大块数。限制是针对每个协议，因此限制为 4 表示每个主机最多 4 个 UDP 块、4 个 TCP 块和 4 个 ICMP 块。范围为 1-8，默认值为 4。

步骤 2 添加使用 PAT 池块分配的 NAT 规则。

- 依次选择 **Configuration > Firewall > NAT Rules**。
- 添加或编辑对象 NAT 或两次 NAT 规则。
- 至少配置以下选项：
 - （两次 NAT。）在 **Original Packet > Source Address** 中，选择定义源地址的对象。
 - **Type = Dynamic**。
 - **Pat Pool Translated Address**。选择定义 pat 池网络的网络对象。
 - **Enable Block Allocation**。
- 点击 **OK**。

配置每会话 PAT 或多会话 PAT（版本 9.0(1) 及更高版本）

默认情况下，所有 TCP PAT 流量和所有 UDP DNS 流量均使用每会话 PAT。要将多会话 PAT 用于流量，可配置每会话 PAT 规则：一条允许规则使用每会话 PAT，一条拒绝规则使用多会话 PAT。

每会话 PAT 可以提高 PAT 的可扩展性，对于集群，允许每个成员单元拥有自己的 PAT 连接；多会话 PAT 连接必须转发到主单元并且归主单元所有。在每会话 PAT 会话结束时，ASA 将发送一条重置消息并立即删除转换。此重置会使结束节点立即释放连接，避免 TIME_WAIT 状态。另一方面，多会话 PAT 使用 PAT 超时，默认为 30 秒。

对于“命中并运行”流量，例如 HTTP 或 HTTPS，每会话 PAT 可以显著增加一个地址支持的连接速率。不使用每会话 PAT，IP 协议的一个地址的最大连接速率大约为每秒 2000。使用每会话 PAT，IP 协议的一个地址的连接速率为 65535/平均生命周期。

对于可受益于多会话 PAT 的流量（例如 H.323、SIP 或 Skinny），可以创建每会话拒绝规则来禁用每会话 PAT。但是，如果还想将每会话 PAT 用于这些协议所用的 UDP 端口，您必须为这些端口创建允许规则。

开始之前

默认情况下，已安装以下规则：

- 允许从任何（IPv4 和 IPv6）到任何（IPv4 和 IPv6）的 TCP。
- 允许从任何（IPv4 和 IPv6）到域端口的 UDP。

这些规则不会显示在表中。

这些规则无法删除，无论手动创建什么规则，它们始终存在。因为会按顺序评估规则，所以可以忽略默认规则。例如，要完全忽略这些规则，可以添加以下规则：

- 拒绝从任何（IPv4 和 IPv6）到任何（IPv4 和 IPv6）的 TCP。
- 拒绝从任何（IPv4 和 IPv6）到域端口的 UDP。

过程

步骤 1 依次选择配置 > 防火墙 > 高级 > 每会话 NAT 规则。

步骤 2 执行以下操作之一：

- 依次选择 **Add > Add Per-Session NAT Rule**。
- 选择一条规则，然后点击 **Edit**。

步骤 3 配置规则：

- **Action** - 点击 **Permit** 或 **Deny**。允许规则使用每会话 PAT；拒绝规则使用多会话 PAT。

- **Source**-通过键入一个地址，或者点击 ... 按钮来选择一个对象，从而指定源地址。对于该服务，请选择 UDP 或 TCP。也可以指定源端口，尽管通常仅指定目标端口。在 UDP/port 或 TCP/port 中键入，或者点击 ... 按钮选择一个通用值或对象。
- **Destination**-通过键入一个地址，或者点击 ... 按钮来选择一个对象，从而指定目标地址。对于该服务，请选择 UDP 或 TCP；此选项必须与源服务匹配。或者，可以指定目标端口。在 UDP/port 或 TCP/port 中键入，或者点击 ... 按钮选择一个通用值或对象。可以使用运算符 !=（不等于）、>（大于）、<（小于），或使用连字符指定范围（例如 100-200）。

步骤 4 点击 **OK**，然后点击 **Apply**。

静态 NAT

以下主题介绍静态 NAT 以及如何实施静态 NAT。

关于静态 NAT

静态 NAT 创建实际地址到映射地址的固定转换。因为映射地址对于每个连续连接都是相同的，所以静态 NAT 允许双向连接发起，即到主机发起和从主机发起（如果有允许这样做的访问规则）。另一方面，通过动态 NAT 和 PAT，每台主机为每次后续转换使用不同的地址或端口，因此，不支持双向发起。

下图显示典型的静态 NAT 场景。转换始终处于活动状态，所以，实际主机和远程主机可以发起连接。

图 21: 静态 NAT



注释 如果需要，可以禁用双向性。

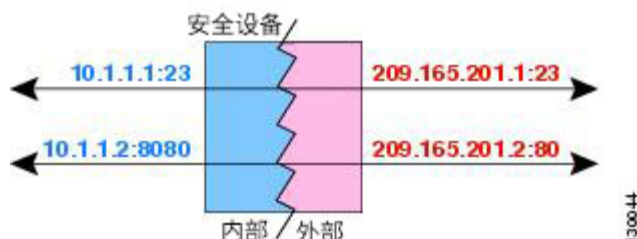
支持端口转换的静态 NAT

支持端口转换的静态 NAT 让您指定实际和映射协议及端口。

指定带静态 NAT 的端口时，可以选择将端口和/或 IP 地址映射到同一值或不同值。

下图显示支持端口转换的典型静态 NAT 场景，其中显示映射到本身的端口和映射到不同值的端口；在这两种情况下，IP 地址映射到不同值。转换始终处于活动状态，所以，转换后主机和远程主机可以发起连接。

图 22: 支持端口转换的典型静态 NAT 场景



支持端口转换的静态 NAT 规则支持仅访问指定端口的目标 IP 地址。如果您尝试访问其他端口上 NAT 规则未涵盖的目标 IP 地址，连接将被阻止。此外，对于两次 NAT，如果流量与 NAT 规则的源 IP 地址不匹配，但与目标 IP 地址匹配，流量将被丢弃，不管目标端口为何。因此，您必须为允许发送到目标 IP 地址的所有其他流量添加额外规则。例如，您可以为 IP 地址配置静态 NAT 规则（不含端口规范），并将其放置在端口转换规则后面。



注释 对于需要对辅助信道执行应用检查的应用（例如 FTP 和 VoIP），NAT 会自动转换辅助端口。

下面是使用支持端口转换的静态 NAT 的其他情况。

具有身份端口转换的静态 NAT

可以简化对内部资源的外部访问。例如，如果您有在不同端口上提供服务（例如 FTP、HTTP 和 SMTP）的三个单独的服务器，可以为外部用户提供单个 IP 地址以访问这些服务。然后，可以配置具有身份端口转换的静态 NAT，从而根据尝试访问的端口将单个外部 IP 地址映射到实际服务器的正确 IP 地址。您无需更改端口，因为服务器使用的是标准端口（分别是 21、80 和 25）。有关如何配置此示例的详细信息，请参阅[用于 FTP、HTTP 和 SMTP（支持端口转换的静态 NAT）的单一地址](#)，第 240 页。

对非标准端口进行端口转换的静态 NAT

还可以利用支持端口转换的静态 NAT 将一个公认端口转换为一个非标准端口，反之亦然。例如，如果内部 Web 服务器使用端口 8080，可以允许外部用户连接到端口 80，然后取消转换到原始端口 8080。同样，要进一步提高安全性，可以告知 Web 用户连接到非标准端口 6785，然后取消转换到端口 80。

具有端口转换的静态接口 NAT

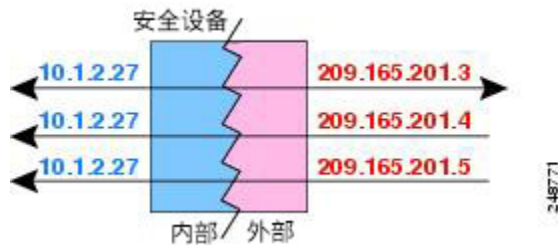
可以配置静态 NAT，以将一个实际地址映射到一个接口地址/端口组合。例如，如果要将对设备外部接口的 Telnet 访问重定向至内部主机，则可以将内部主机 IP 地址/端口 23 映射到外部接口地址/端口 23。

一对多静态 NAT

通常，配置带一对一映射的静态 NAT。然而，在某些情况下，可能要将单一实际地址配置到多个映射地址（一对多）。配置一对多静态 NAT 时，当实际主机发起流量时，它始终使用第一个映射地址。然而，对于发起到主机的流量，可以发起到任何映射地址的流量，并且不将它们转换为单一实际地址。

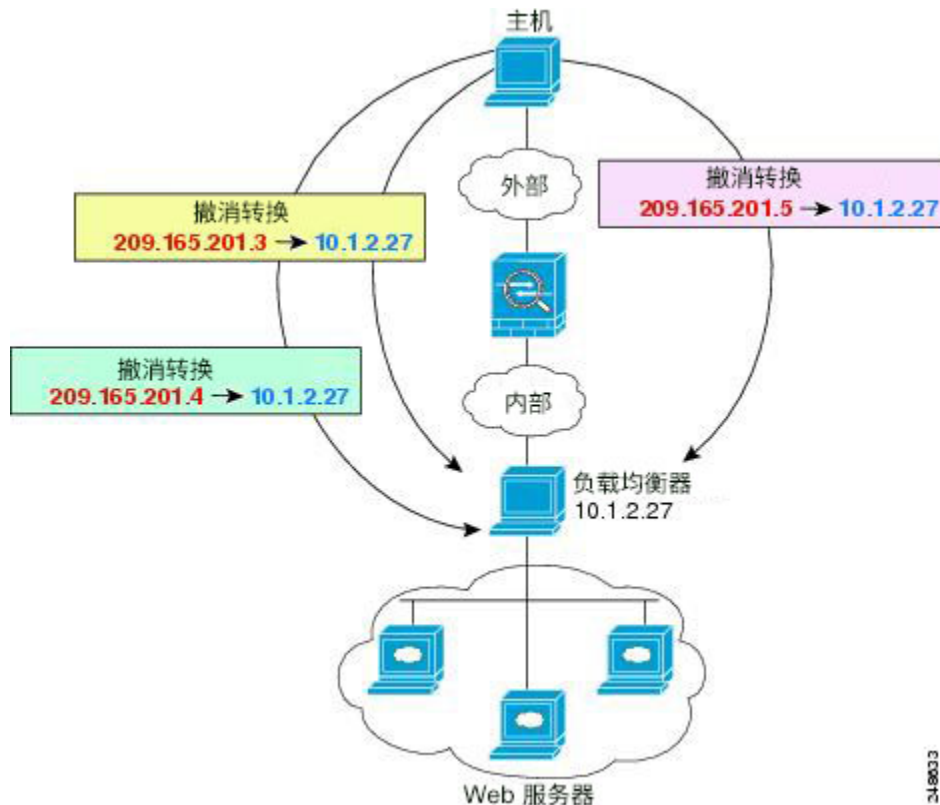
下图显示典型的一对多静态 NAT 场景。由于实际主机进行的发起的流量始终使用第一个映射地址，因此从技术上说，实际主机 IP/第一个映射 IP 的转换是唯一的双向转换。

图 23: 一对多静态 NAT



例如，在 10.1.2.27 上有一个负载均衡器。根据请求的 URL，它会将流量重新定向到正确的 Web 服务器。有关如何配置此示例的详细信息，请参阅[具有多个映射地址的内部负载均衡器（静态 NAT，一对多）](#)，第 238 页。

图 24: 一对多静态 NAT 示例



其他映射场景（不推荐）

NAT 具有很高的灵活性，允许任何类型的静态映射场景：不仅包括一对一、一对多，还包括少对多、多对少和多对一映射。我们推荐仅使用一对一或一对多映射。其他映射选项可能会导致意外后果。

在功能上，少对多与一对多相同；但是，因为此配置更加复杂，而且实际映射可能不会一目了然，所以我们建议为每个需要一对多配置的实际地址创建该配置。例如，对于少对多场景，少量的实际地址会按顺序映射到多个映射地址（A 到 1、B 到 2、C 到 3）。当映射所有实际地址时，下一个映射地址会映射到第一个实际地址，等等，直到映射了所有映射地址为止（A 到 4、B 到 5、C 到 6）。这将导致每个实际地址有多个映射地址。就像一对多配置一样，仅第一个映射是双向的；后续映射可以将流量发起到实际主机，但所有从实际主机发起的流量仅将第一个映射地址用于源。

下图显示典型的少对多静态 NAT 场景。

图 25: 少对多静态 NAT



对于实际地址多于映射地址的多对少或多对一配置，映射地址会在实际地址用尽之前先用尽。仅最低实际 IP 地址和映射池之间的映射可以导致双向发起。剩余的更高的实际地址可以发起流量，但不能将流量发起到这些地址（由于五元组 [源 IP、目的目标 IP、源端口、目的目标端口、协议] 的唯一性，连接的返回流量会定向到正确的实际地址）。



注释 多对少或多对一 NAT 不是 PAT。如果两台实际主机使用同一源端口号，连接到同一外部服务器和同一 TCP 目的目标端口，并且两台主机转换到同一 IP 地址，那么由于地址冲突（五元组不唯一），将重置两个连接。

下图显示一个典型的多对少静态 NAT 场景。

图 26: 多对少静态 NAT



我们建议不要这样使用静态规则，而是为需要双向发起的流量创建一对一规则，为其他地址创建动态规则。

配置静态网络对象 NAT 或支持端口转换的静态 NAT

本节介绍如何使用网络对象 NAT 配置静态 NAT 规则。

过程

步骤 1 将 NAT 添加到新的或现有的网络对象中：

- 要添加新的网络对象，请依次选择 **Configuration > Firewall > NAT Rules**，然后依次点击 **Add > Add Network Object NAT Rule**。
- 要将 NAT 添加到现有的网络对象中，请依次选择 **Configuration > Firewall > Objects > Network Objects/Groups**，然后编辑网络对象。

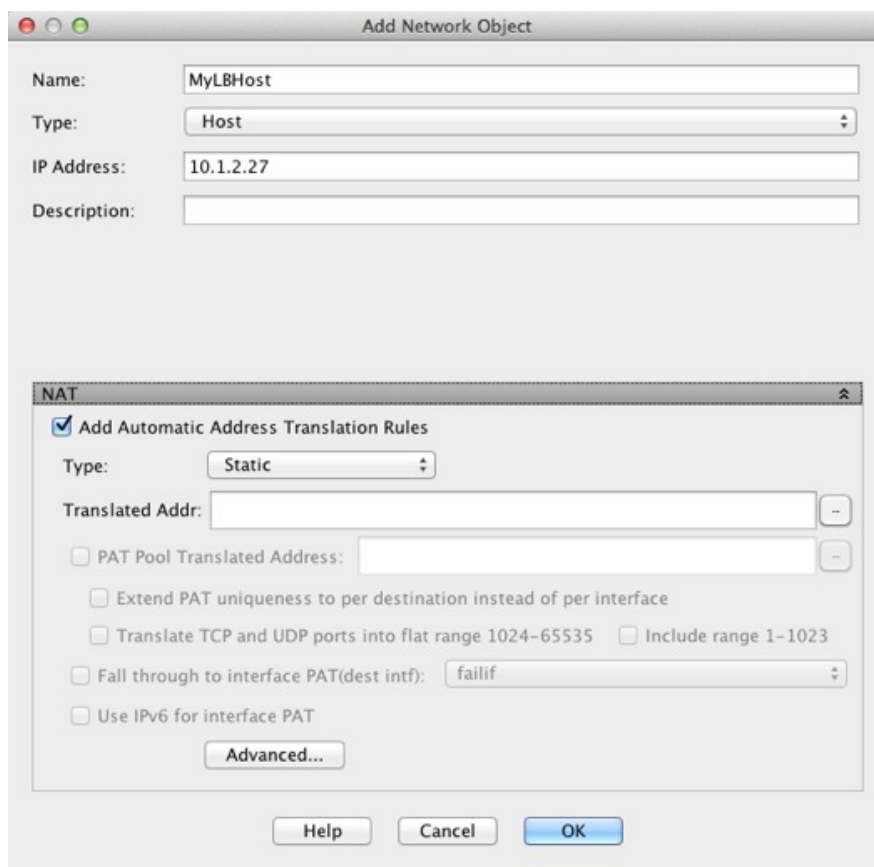
步骤 2 对于新对象，请为以下字段输入值：

- **Name** - 对象名称。使用字符 a 到 z、A 到 Z、0 到 9、句号、破折号、逗号或下划线。名称不得超过 64 个字符。
- **Type** - 主机、网络或范围。
- **IP Addresses** - IPv4 或 IPv6 地址、主机的单一地址、范围的开始和结束地址，以及子网的 IPv4 网络地址和掩码（例如 10.100.10.0 255.255.255.0）或 IPv6 地址和前缀长度（例如 2001:DB8:0:CD30::/60）。

步骤 3 如果 NAT 部分隐藏，请点击 **NAT** 展开此部分。

步骤 4 选中 **Add Automatic Translation Rules** 复选框。

步骤 5 从 Type 下拉列表中选择 **Static**。



步骤 6 在 Translated Addr. 字段中，将映射 IP 地址指定为以下任一选项。通常，配置相同数量的映射地址和实际地址，以便进行一对一映射。然而，地址数量可以不匹配。有关详细信息，请参阅[静态 NAT](#)，第 209 页。

- 键入主机 IP 地址。此项仅为主机对象提供一对一映射。否则，您将获得多对一映射。对于 NAT46 或 NAT66 转换，此项可以是 IPv6 网络地址。
- 点击浏览按钮并选择网络对象（或创建一个新的网络对象）。要为一组 IP 地址执行一对一映射，请选择包含具有相同地址数量的范围的对象。
- （仅限支持端口转换的静态 NAT。）键入接口名称或点击浏览按钮，从 Browse Translated Addr 对话框中选择一个接口。无法选择桥接组成员接口。



要使用 IPv6 接口地址，还必须选中 **Use IPv6 for interface PAT** 复选框。另请确保点击 **Advanced** 并配置服务端口的转换。（不能在透明模式下指定接口。）

步骤 7 （可选。）对于 NAT46，选中 **Use one-to-one address translation**。对于 NAT 46，指定一对一转换，将第一个 IPv4 地址转换为第一个 IPv6 地址，将第二个 IPv4 地址转换为第二个 IPv6 地址，依次类推。如不使用此选项，则将使用 IPv4 嵌入式方法。对于一对一转换，必须使用此关键字。

步骤 8 (可选) 点击 **Advanced**，在 Advanced NAT Settings 对话框中配置以下选项，然后点击 **OK**。

- **Translate DNS replies for rule** - 转换 DNS 应答中的 IP 地址。确保启用 DNS 检测（默认情况下启用）。有关详细信息，请参阅 [使用 NAT 重写 DNS 查询和响应](#)，第 277 页。
- **Disable Proxy ARP on egress interface** 对映射 IP 地址的传入数据包禁用代理 ARP。有关可能需要禁用代理 ARP 的情况的信息，请参阅 [映射地址和路由](#)，第 261 页。
- (对于桥接组成员接口需要填入。) **Interface** - 指定应用此 NAT 规则时的实际接口（源）和映射接口（目标）。默认情况下，该规则将应用于所有接口，桥接组成员除外。
- **Service** - 配置带端口转换的静态 NAT。选择协议，然后输入实际端口和映射端口。可以使用端口号或已知的端口名称（例如 http）。

步骤 9 点击 **OK**，然后点击 **Apply**。

因为静态规则是双向的（允许启动到实际主机或从实际主机发起），所以 NAT Rules 表为每条静态规则显示两行，每个方向显示一行。

#	Match Criteria: Original Packet					Action: Translated Packet		
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service
1	inside	outside	static1	HTTP_SERVER	service1	static2 (S)	HTTP_SERVER	service1
	outside	inside	HTTP_SERVER	static2	service1	HTTP_SERVER (S)	static1	service1
"Network Object" NAT (Rule 2)								
2	inside	outside	HTTP_SERVER	any	http	209.165.201.3 (S)	-- Original --	http
	outside	inside	any	209.165.201.3	http	-- Original --	HTTP_SERVER	http

配置静态两次 NAT 或支持端口转换的静态 NAT

本节介绍如何使用两次 NAT 配置静态 NAT 规则。

过程

步骤 1 依次选择配置 > 防火墙 > NAT 规则，然后执行下列操作之一：

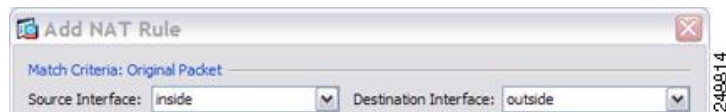
- 点击 **Add**，或依次点击 **Add > Add NAT Rule Before Network Object NAT Rules**。
- 点击 **Add > Add NAT Rule After Network Object NAT Rules**。
- 选择一条两次 NAT 规则，然后点击 **Edit**。

系统将显示 Add NAT Rule 对话框。

步骤 2 (对于桥接组成员接口需要填入。) 设置源和目标接口。

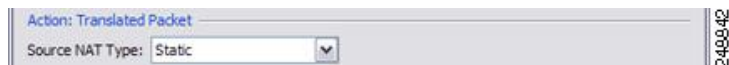
在路由模式下，默认源和目标均采用 any 接口。可以为一个或两个选项选择特定接口。但是，必须在为桥接组成员接口写入规则时选择接口；“any”不包括这些接口。

- 从 **Match Criteria: Original Packet > Source Interface** 下拉列表中选择源接口。
- 从 **Match Criteria: Original Packet > Destination Interface** 下拉列表中选择目标接口。

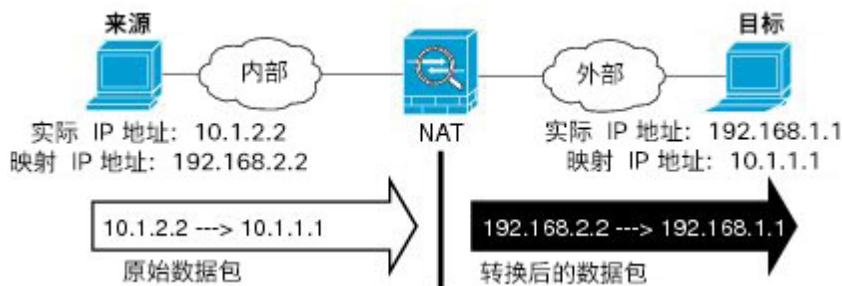


步骤 3 从操作：转换后的数据包 > 源 NAT 类型下拉列表中选择静态。Static 为默认设置。

该设置仅应用于源地址；目标转换始终为静态。



步骤 4 确定原始数据包地址（IPv4 或 IPv6 地址）；即源接口网络上显示的数据包地址（实际源地址和映射目标地址）。请参阅下图，了解原始数据包与转换后数据包的示例。



- a) 对于 **Match Criteria: Original Packet > Source Address**，从 Browse Original Source Address 对话框，点击浏览按钮，并选择现有网络对象或组，或创建新的对象或组。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。默认设置为 **any**，但除身份 NAT 外，请勿使用此选项。

Name	IP Address	Netmask
IPv4 Network Objects		
A_10.1.1.1	10.1.1.1	255.255.255...
DMZnetwork1	209.165.201.0	255.255.255...

- b) (可选) 对于 **Match Criteria: Original Packet > Destination Address**，从 Browse Original Destination Address 对话框，点击浏览按钮并选择现有网络对象、组或接口，或创建新的对象或组。

尽管两次 NAT 的主要功能是纳入目标 IP 地址，但目标地址是可选的。如果确实指定目标地址，则可为该地址配置静态转换，或只将身份 NAT 用于该地址。可能需要配置没有目标地址的两次 NAT，以利用两次 NAT 的一些其他特性，包括使用实际地址的网络对象组或对规则手动排序。有关详细信息，请参阅[比较网络对象 NAT 和两次 NAT](#)，第 173 页。

步骤 5 确定转换后的数据包地址 (IPv4 或 IPv6 地址)；即目标接口网络上显示的数据包地址 (映射源地址和实际目标地址)。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- a) 对于 **Action: Translated Packet > Source Address**，从 Browse Translated Source Address 对话框，点击浏览按钮，并选择现有网络对象或组，或创建新的对象或组。

对于静态 NAT，映射通常是一对一的，因此实际地址与映射地址的数量相同。然而，如果需要，可拥有不同的数量。

对于支持端口转换的静态接口 NAT，可为映射地址指定接口而非网络对象/组。要使用接口的 IPv6 地址，请选中 **Use IPv6 for interface PAT** 复选框。无法选择桥接组成员接口。

Source Address:

PAT Pool Translated Address:

Round Robin

Extend PAT uniqueness to per destination instead of per interface

Translate TCP and UDP ports into flat range 1024-65535 Inc

Fall through to interface PAT

Use IPv6 for interface PAT

有关详细信息，请参阅[支持端口转换的静态 NAT](#)，第 209 页。有关不允许的映射 IP 地址的详细信息，请参阅[NAT 指南](#)，第 176 页。

- b) (可选。)对于 **Action: Translated Packet > Destination Address**，从 Browse Translated Destination Address 对话框，点击浏览按钮并选择现有网络对象或组，或创建新的对象或组。

步骤 6 (可选。)为服务转换确定源或目标服务端口。

- 确定原始数据包源或目标端口（实际源端口或映射目标端口）。对于 **Match Criteria: Original Packet > Service**，从 Browse Original Service 对话框，点击浏览按钮并选择指定端口的现有服务对象，或创建新的对象。
- 确定转换后数据包源或目标端口（映射源端口或实际目标端口）。对于 **Action: Translated Packet > Service**，从 Browse Translated Service 对话框，点击浏览按钮并选择指定端口的现有服务对象，或创建新的对象。

服务对象可能同时包含源和目标端口。应同时为实际和映射服务对象指定源或目标端口。如果应用使用固定的源端口（如某些 DNS 服务器），则您只能同时指定源和目标端口；然而，很少使用固定源端口。在极少数情况下，会在对象中同时指定源和目标端口，原始数据包服务对象包含实际源端口/映射目标端口；转换后的数据包服务对象包含映射源端口/实际目标端口。在转换端口时，请确保实际服务对象与映射服务对象中的协议完全相同（例如，同为 TCP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。不支持“不等于”(!=) 运算符。

例如：

The screenshot shows the 'Add Service Object' dialog box with the following fields:

- Name: web
- Service Type: tcp
- Destination Port/Range: 80
- Source Port/Range: (empty)
- Description: (empty)

The screenshot shows the 'Match Criteria: Original Packet' configuration section with the following fields:

- Source Interface: inside
- Destination Interface: outside
- Source Address: obj-192.168.251.164
- Destination Address: obj-172.25.23.32
- Service: web

步骤 7 (可选。)对于 NAT46, 选中 **Use one-to-one address translation** 复选框。对于 NAT46, 指定一对一转换, 将第一个 IPv4 地址转换为第一个 IPv6 地址, 将第二个 IPv4 地址转换为第二个 IPv6 地址, 依次类推。如不使用此选项, 则将使用 IPv4 嵌入式方法。对于一对一转换, 必须使用此关键字。

步骤 8 (可选。)在 Options 区域中配置 NAT 选项

- **Enable rule** - 启用此 NAT 规则。该规则默认启用。
- (适用于源专用规则。) **Translate DNS replies that match this rule** - 在 DNS 应答中重写 DNS A 记录。确保启用 DNS 检测 (默认情况下启用)。如果配置目标地址, 则无法配置 DNS 修改。有关详细信息, 请参阅 [使用 NAT 重写 DNS 查询和响应](#), 第 277 页。
- **Disable Proxy ARP on egress interface** 对映射 IP 地址的传入数据包禁用代理 ARP。有关详细信息, 请参阅 [映射地址和路由](#), 第 261 页。
- **Direction** - 要使规则成为单向, 请选择 **Unidirectional**。默认设置为 Both。将该规则设为单向可防止始发连接的目标地址变成实际地址。
- **Description** - 添加规则的相关说明, 最长 200 个字符。

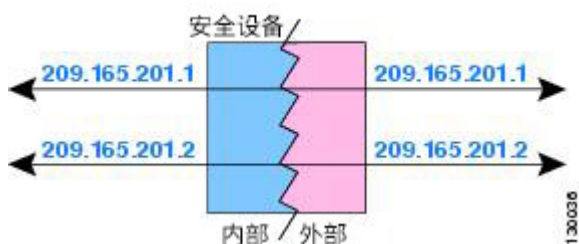
步骤 9 点击 **OK**，然后点击 **Apply**。

身份 NAT

可能有一个 NAT 配置，在其中需要将 IP 地址转换为其本身。例如，如果创建一条将 NAT 应用于每个网络的大体的规则，但想使一个网络免于 NAT，则可以创建一条静态 NAT 规则，以将地址转换为其本身。身份 NAT 是远程接入访问 VPN 所必需的，需要使客户端流量免于 NAT。

下图显示典型的身份 NAT 场景。

图 27: 身份 NAT



以下主题介绍如何配置身份 NAT

配置身份网络对象 PAT

本节介绍如何使用网络对象 NAT 配置身份 NAT 规则。

过程

步骤 1 将 NAT 添加到新的或现有的网络对象中：

- 要添加新的网络对象，请依次选择 **Configuration > Firewall > NAT Rules**，然后依次点击 **Add > Add Network Object NAT Rule**。
- 要将 NAT 添加到现有的网络对象中，请依次选择 **Configuration > Firewall > Objects > Network Objects/Groups**，然后编辑网络对象。

步骤 2 对于新对象，请为以下字段输入值：

- **Name** - 对象名称。使用字符 a 到 z、A 到 Z、0 到 9、句号、破折号、逗号或下划线。名称不得超过 64 个字符。
- **Type** - 主机、网络或范围。

- **IP Addresses** - IPv4 或 IPv6 地址、主机的单一地址、范围的开始和结束地址，以及子网的 IPv4 网络地址和掩码（例如 10.100.10.0 255.255.255.0）或 IPv6 地址和前缀长度（例如 2001:DB8:0:CD30::/60）。

步骤 3 如果 NAT 部分隐藏，请点击 **NAT** 展开此部分。

步骤 4 选中 **Add Automatic Translation Rules** 复选框。

步骤 5 从 Type 下拉列表中选择 **Static**。

步骤 6 在 Translated Addr. 字段中，执行以下操作之一：

- 键入用于实际地址的相同 IP 地址。对于身份 NAT，此选项仅适用于主机对象。
- 点击浏览按钮并选择网络对象（或创建一个新的网络对象）。当为一个地址范围配置身份 NAT 时，请使用此选项。

步骤 7（可选）点击 **Advanced**，在 Advanced NAT Settings 对话框中配置以下选项，然后点击 **OK**。

- **Translate DNS replies for rule** - 请勿为身份 NAT 配置此选项。
- **Disable Proxy ARP on egress interface** 对映射 IP 地址的传入数据包禁用代理 ARP。有关可能需要禁用代理 ARP 的情况的信息，请参阅[映射地址和路由](#)，第 261 页。

- (路由模式; 已指定接口。) **Lookup route table to locate egress interface** - 使用路由查找而不使用 NAT 命令中指定的接口确定出口接口。有关详细信息, 请参阅[确定出口接口](#), 第 263 页。
- (对于桥接组成员接口需要填入。) **Interface** - 指定应用此 NAT 规则时的实际接口 (源) 和映射接口 (目标)。默认情况下, 该规则将应用于所有接口, 桥接组成员除外。
- **Service** - 请勿为身份 NAT 配置此选项。

步骤 8 点击 **OK**, 然后点击 **Apply**。

因为静态规则是双向的 (允许启动到实际主机或从实际主机启动), 所以 NAT Rules 表为每条静态规则显示两行, 每个方向显示一行, 除非选择路由查找选项。

#	Match Criteria: Original Packet					Action: Translated Packet		
	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service
1	inside	outside	static1	HTTP_SERVER	service1	static2 (S)	HTTP_SERVER	service1
	outside	inside	HTTP_SERVER	static2	service1	HTTP_SERVER (S)	static1	service1
"Network Object" NAT (Rule 2)								
2	inside	outside	HTTP_SERVER	any	http	209.165.201.3 (S)	-- Original --	http
	outside	inside	any	209.165.201.3	http	-- Original --	HTTP_SERVER	http

配置身份两次 NAT

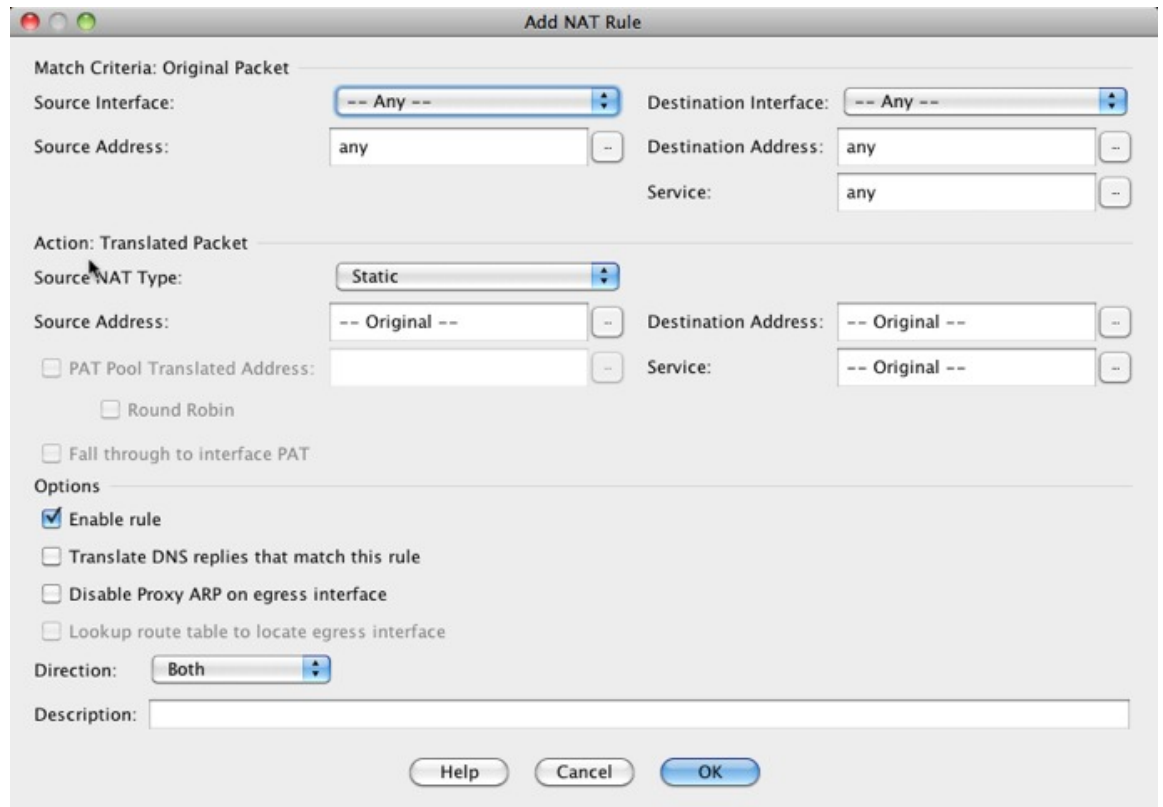
本节介绍如何使用两次 NAT 配置身份 NAT 规则。

过程

步骤 1 依次选择配置 > 防火墙 > NAT 规则, 然后执行下列操作之一:

- 点击 **Add**, 或依次点击 **Add > Add NAT Rule Before Network Object NAT Rules**。
- 点击 **Add > Add NAT Rule After Network Object NAT Rules**。
- 选择一条两次 NAT 规则, 然后点击 **Edit**。

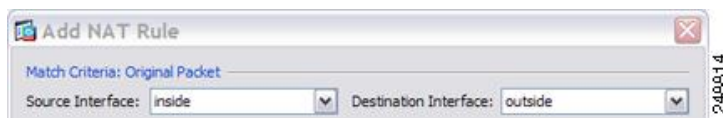
系统将显示 Add NAT Rule 对话框。



步骤 2 (对于桥接组成员接口需要填入。) 设置源和目标接口。

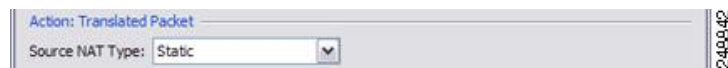
在路由模式下，默认源和目标均采用 any 接口。可以为一个或两个选项选择特定接口。但是，必须在为桥接组成员接口写入规则时选择接口；“any”不包括这些接口。

- a) 从 **Match Criteria: Original Packet > Source Interface** 下拉列表中选择源接口。
- b) 从 **Match Criteria: Original Packet > Destination Interface** 下拉列表中选择目标接口。

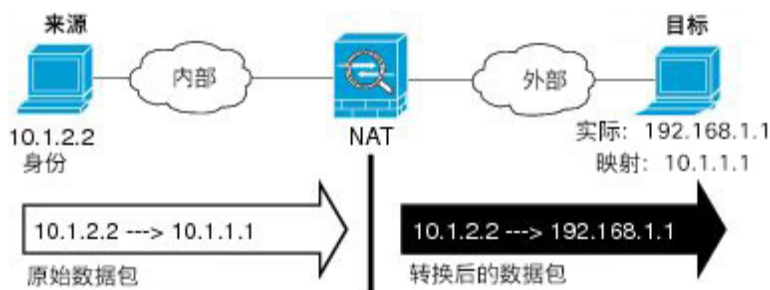


步骤 3 从操作：转换后的数据包 > 源 NAT 类型下拉列表中选择静态。Static 为默认设置。

该设置仅应用于源地址；目标转换始终为静态。



步骤 4 确定原始数据包地址 (IPv4 或 IPv6 地址)；即源接口网络上显示的数据包地址 (实际源地址和映射目标地址)。请参阅下图，了解原始数据包与转换后数据包的示例，其中在内部主机上执行身份 NAT，但转换外部主机。



- a) 对于 **Match Criteria: Original Packet > Source Address**，从 Browse Original Source Address 对话框，点击浏览按钮，并选择现有网络对象或组，或创建新的对象或组。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。默认设置为 **any**；只有也将映射地址设置为 **any** 时才能使用此选项。

Name	IP Address	Netmask
IPv4 Network Objects		
A_10.1.1.1	10.1.1.1	255.255.255...
DMZnetwork1	209.165.201.0	255.255.255...

- b) (可选。) 对于 **Match Criteria: Original Packet > Destination Address**，从 Browse Original Destination Address 对话框，点击浏览按钮并选择现有网络对象、组或接口，或创建新的对象或组。

尽管两次 NAT 的主要功能是纳入目标 IP 地址，但目标地址是可选的。如果确实指定目标地址，则可为该地址配置静态转换，或只将身份 NAT 用于该地址。可能需要配置没有目标地址的两次 NAT，以利用两次 NAT 的一些其他特性，包括使用实际地址的网络对象组或对规则手动排序。有关详细信息，请参阅[比较网络对象 NAT 和两次 NAT](#)，第 173 页。

对于仅支持端口转换的静态接口 NAT，请选择接口。如果指定了接口，请务必同时配置服务转换。有关详细信息，请参阅[支持端口转换的静态 NAT](#)，第 209 页。

步骤 5 确定转换后的数据包地址；即目标接口网络上显示的数据包地址（映射源地址和实际目标地址）。

- a) 对于 **Action: Translated Packet > Source Address**，从选择实际源地址的 Browse Translated Source Address 对话框，点击浏览按钮，并选择相同的网络对象或组。如已为实际地址指定 **any**，则请使用 **any**。
- b) 对于 **Match Criteria: Translated Packet > Destination Address**，从 Browse Translated Destination Address 对话框，点击浏览按钮并选择现有网络对象或组，或创建新的对象或组。

对于用于目标地址的身份 NAT，只需将相同的对象或组同时用于实际和映射地址。

如果要转换目标地址，则静态映射通常为一对一，因此实际地址的数量与映射地址相同。然而，如果需要，可拥有不同的数量。有关详细信息，请参阅[静态 NAT](#)，第 209 页。有关不允许的映射 IP 地址的详细信息，请参阅[NAT 指南](#)，第 176 页。

步骤 6 (可选。) 为服务转换确定源或目标服务端口。

- 确定原始数据包源或目标端口（实际源端口或映射目标端口）。对于 **Match Criteria: Original Packet > Service**，从 Browse Original Service 对话框，点击浏览按钮并选择指定端口的现有服务对象，或创建新的对象。

- 确定转换后数据包源或目标端口（映射源端口或实际目标端口）。对于 **Action: Translated Packet > Service**，从 Browse Translated Service 对话框，点击浏览按钮并选择指定端口的现有服务对象，或创建新的对象。

服务对象可能同时包含源和目标端口。应同时为实际和映射服务对象指定源或目标端口。如果应用使用固定的源端口（如某些 DNS 服务器），则您只能同时指定源和目标端口；然而，很少使用固定源端口。在极少数情况下，会在对象中同时指定源和目标端口，原始数据包服务对象包含实际源端口/映射目标端口；转换后的数据包服务对象包含映射源端口/实际目标端口。在转换端口时，请确保实际服务对象与映射服务对象中的协议完全相同（例如，同为 TCP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。不支持“不等于”(!=) 运算符。

例如：

Add Service Object

Name: web

Service Type: tcp

Destination Port/Range: 80

Source Port/Range:

Description:

Help Cancel OK

Match Criteria: Original Packet

Source Interface: inside Destination Interface: outside

Source Address: obj-192.168.251.164 Destination Address: obj-172.25.23.32

Service: web

Add Service Object

Name: web_map

Service Type: tcp

Destination Port/Range: 8080

Source Port/Range:

Description:

Help Cancel OK

Action: Translated Packet
 Source NAT Type:
 Source Address: Destination Address:
 PAT Pool Translated Address: Service:

步骤 7 (可选) 在 Options 区域中配置 NAT 选项。

Options
 Enable rule
 Translate DNS replies that match this rule
 Disable Proxy ARP on egress interface
 Lookup route table to locate egress interface
 Direction:
 Description:

- **Enable rule** - 启用此 NAT 规则。该规则默认启用。
- (适用于源专用规则。) **Translate DNS replies that match this rule** - 尽管此选项可用，但如果未配置目标地址，则此选项不适用于身份 NAT，因为您是将地址转换为其自身，所以此 DNS 应答不需要修改。
- **Disable Proxy ARP on egress interface** 对映射 IP 地址的传入数据包禁用代理 ARP。有关详细信息，请参阅[映射地址和路由](#)，第 261 页。
- (路由模式；已指定接口。) **Lookup route table to locate egress interface** - 使用路由查找而不使用 NAT 命令中指定的接口确定出口接口。有关详细信息，请参阅[确定出口接口](#)，第 263 页。
- **Direction** - 要使规则成为单向，请选择 **Unidirectional**。默认设置为 Both。使规则成为单向可防止流量发起通向实际地址的连接。可能要将此设置用于测试目的。
- **Description** - 添加规则的相关说明，最长 200 个字符。

步骤 8 点击 OK，然后点击 Apply。

监控 NAT

可以从以下页面查看 NAT 相关图表：

- **Monitoring > Properties > Connection Graphs > Xlates** - 选择 Xlate Utilization 图表，查看使用中和使用最多的转换。此操作等同于 **show xlate** 命令。
- **Monitoring > Properties > Connection Graphs > Perfmon** - 选择 Xlate Perfmon 图表，查看 NAT 性能信息。此操作等同于 **show perfmon** 命令提供的 xlate 信息。

NAT 的历史

功能名称	平台版本	说明
网络对象 NAT	8.3(1)	<p>为网络对象 IP 地址配置 NAT。</p> <p>引入或修改了以下屏幕： Configuration > Firewall > NAT Rules Configuration > Firewall > Objects > Network Objects/Groups</p>
两次 NAT	8.3(1)	<p>两次 NAT 可供您在单一规则中同时标识源和目标地址。</p> <p>修改了以下屏幕： Configuration > Firewall > NAT Rules。</p>
身份 NAT 可配置代理 ARP 和路由查找	8.4(2)/8.5(1)	<p>在身份 NAT 的更早版本中，代理 ARP 被禁用，始终使用路由查找确定出口接口。无法配置这些设置。在 8.4(2) 及更高版本中，身份 NAT 的默认行为已更改为匹配其他静态 NAT 配置的行为：在默认情况下，代理 ARP 已启用，并且 NAT 配置确定出口接口（如已指定）。您可以原样保留这些设置，或者单独启用或禁用这些设置。请注意，现在您也可以为常规静态 NAT 禁用代理 ARP。</p> <p>对于 8.3 之前版本的配置，NAT 免除规则（nat 0 access-list 命令）至 8.4(2) 及更高版本的迁移现包含以下关键字，以禁用代理 ARP 并使用路由查找：no-proxy-arp 和 route-lookup。用于迁移至 8.3(2) 和 8.4(1) 的 unidirectional 关键字不再用于迁移。从 8.3(1)、8.3(2) 和 8.4(1) 升级至 8.4(2) 时，所有身份 NAT 配置现包含 no-proxy-arp 和 route-lookup 关键字，以便维持现有功能。unidirectional 关键字已删除。</p> <p>修改了以下屏幕： Configuration > Firewall > NAT Rules > Add/Edit Network Object > Advanced NAT Settings; Configuration > Firewall > NAT Rules > Add/Edit NAT Rule。</p>
PAT 池和轮询地址分配	8.4(2)/8.5(1)	<p>现在，您可以指定 PAT 地址池，而不是单一地址。您还可以启用 PAT 地址的轮询分配，而不是先使用 PAT 地址上的所有端口，然后再使用池中的下一个地址。这些功能有助于防止来自单一 PAT 地址的大量连接显示为 DoS 攻击的一部分，并使大量 PAT 地址的配置过程更轻松。</p> <p>修改了以下屏幕： Configuration > Firewall > NAT Rules > Add/Edit Network Object; Configuration > Firewall > NAT Rules > Add/Edit NAT Rule。</p>

功能名称	平台版本	说明
轮询 PAT 池分配技术使用现有主机的相同 IP 地址	8.4(3)	<p>组合使用 PAT 池与轮询分配时，如果主机拥有现有连接，且有端口可用，则来自该主机的后续连接将使用相同的 PAT IP 地址。</p> <p>未修改任何菜单项。</p> <p>此功能在 8.5(1) 或 8.6(1) 中不可用。</p>
用于 PAT 池的不分段 PAT 端口范围	8.4(3)	<p>如果可用，实际源端口号将用于映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，1024 以下的端口只有一个小 PAT 池。</p> <p>如果大量流量使用较小的端口范围，在使用 PAT 池时，现可指定使用以下不分段端口范围，代替三个分段大小不等的端口范围：1024 至 65535，或 1 至 65535。</p> <p>修改了以下屏幕：Configuration > Firewall > NAT Rules > Add/Edit Network Object; Configuration > Firewall > NAT Rules > Add/Edit NAT Rule。</p> <p>此功能在 8.5(1) 或 8.6(1) 中不可用。</p>
用于 PAT 池的扩展 PAT	8.4(3)	<p>每个 PAT IP 地址允许最多 65535 个端口。如果 65535 个端口不能提供足够的转换，则现可启用适合 PAT 池的扩展 PAT。通过将目标地址和端口纳入转换信息，相对于按 IP 地址，扩展 PAT 将按服务使用 65535 个端口。</p> <p>修改了以下屏幕：Configuration > Firewall > NAT Rules > Add/Edit Network Object; Configuration > Firewall > NAT Rules > Add/Edit NAT Rule。</p> <p>此功能在 8.5(1) 或 8.6(1) 中不可用。</p>

功能名称	平台版本	说明
自动 NAT 规则，可将 VPN 对等体的本地 IP 地址转换回对等体的实际 IP 地址	8.4(3)	<p>在极少数情况下，您可能要在内部网络上使用 VPN 对等体的实际 IP 地址，而非已分配的本地 IP 地址。通常在使用 VPN 的情况下，对等体会获得分配的本地 IP 地址以访问内部网络。但是，例如在内部服务器和网络安全基于对等体的实际 IP 地址情况下，可能要将本地 IP 地址重新转换为对等体的实际公有 IP 地址。</p> <p>可以在每个隧道组一个接口的基础上启用此功能。当 VPN 会话已建立或断开连接时，动态添加或删除对象 NAT 规则。可使用 show nat 命令查看这些规则。</p> <p>由于路由问题，我们不建议使用此功能，除非您知道自己需要此功能；请联系思科 TAC 确认网络的功能兼容性。请参阅以下限制：</p> <ul style="list-style-type: none"> • 仅支持思科 IPsec 和 AnyConnect Client。 • 流向公共 IP 地址的返回流量必须路由回 ASA，以便应用 NAT 策略和 VPN 策略。 • 不支持负载均衡（由于路由问题）。 • 不支持漫游（公共 IP 更改）。 <p>ASDM 不支持该命令，请使用命令行工具输入该命令。</p>
NAT 支持 IPv6	9.0(1)	<p>NAT 现在支持 IPv6 流量，以及 IPv4 和 IPv6 之间的转换。在透明模式下，不支持 IPv4 和 IPv6 之间的转换。</p> <p>修改了以下屏幕：Configuration > Firewall > Objects > Network Objects/Group；Configuration > Firewall > NAT Rules。</p>
NAT 支持反向 DNS 查找	9.0(1)	<p>在为 NAT 规则启用了 DNS 检测的情况下使用 IPv4 NAT、IPv6 NAT 和 NAT64 时，NAT 现支持为反向 DNS 查找转换 DNS PTR 记录。</p>

功能名称	平台版本	说明
每会话 PAT	9.0(1)	<p>每会话 PAT 功能可以提高 PAT 的可扩展性，对于集群，允许每个成员单元拥有自己的 PAT 连接；多会话 PAT 连接必须转发到主单元并且归主单元所有。在每会话 PAT 会话结束时，ASA 将发送一条重置消息并立即删除转换。此重置会使结束节点立即释放连接，避免 TIME_WAIT 状态。另一方面，多会话 PAT 使用 PAT 超时，默认为 30 秒。对于“命中并运行”的数据流，例如 HTTP 或 HTTPS，每会话功能可以显著提高一个地址支持的连接速度。不使用每会话功能时，一个用于 IP 协议的地址的最大连接速率约为每秒 2000。在使用每会话功能的情况下，对于 IP 协议，一个地址的连接速率为 $65535/average-lifetime$。</p> <p>默认情况下，所有 TCP 流量和 UDP DNS 流量都使用每会话 PAT xlate。对于需要多会话 PAT 的流量，如 H.323、SIP 或 Skinny，可通过创建每会话拒绝规则来禁用每会话 PAT。</p> <p>引入了以下屏幕：Configuration > Firewall > Advanced > Per-Session NAT Rules。</p>
NAT 规则引擎上的事务提交模式	9.3(1)	<p>启用时，NAT 规则更新将在规则编译完成后应用，而不影响规则匹配性能。</p> <p>我们向以下屏幕中添加了 NAT：Configuration > Device Management > Advanced > Rule Engine。</p>
对运营级 NAT 的改进	9.5(1)	<p>对于运营级或大规模 PAT，您可以为每台主机分配端口块，而无需通过 NAT 一次分配一个端口转换（请参阅 RFC 6888）。</p> <p>添加了以下命令：Configuration > Firewall > Advanced > PAT Port Block Allocation。我们添加了对对象 NAT 启用端口块分配 (Enable Block Allocation) 并两次添加了 NAT 对话框。</p>
SCTP 的 NAT 支持	9.5(2)	<p>现在，可以在静态网络对象 NAT 规则中指定 SCTP 端口。建议不要在静态两次 NAT 中使用 SCTP。动态 NAT/PAT 不支持 SCTP。</p> <p>修改了以下屏幕：Configuration > Firewall > NAT 添加/编辑静态网络对象 NAT 规则、Advanced NAT Settings 对话框。</p>



第 12 章

NAT 示例和参考

以下主题介绍有关配置 NAT 的示例，以及有关高级配置和故障排除的信息。

- [网络对象 NAT 示例，第 231 页](#)
- [两次 NAT 的示例，第 244 页](#)
- [路由和透明防火墙模式下的 NAT，第 258 页](#)
- [路由 NAT 数据包，第 260 页](#)
- [用于 VPN 的 NAT，第 263 页](#)
- [转换 IPv6 网络，第 269 页](#)
- [使用 NAT 重写 DNS 查询和响应，第 277 页](#)

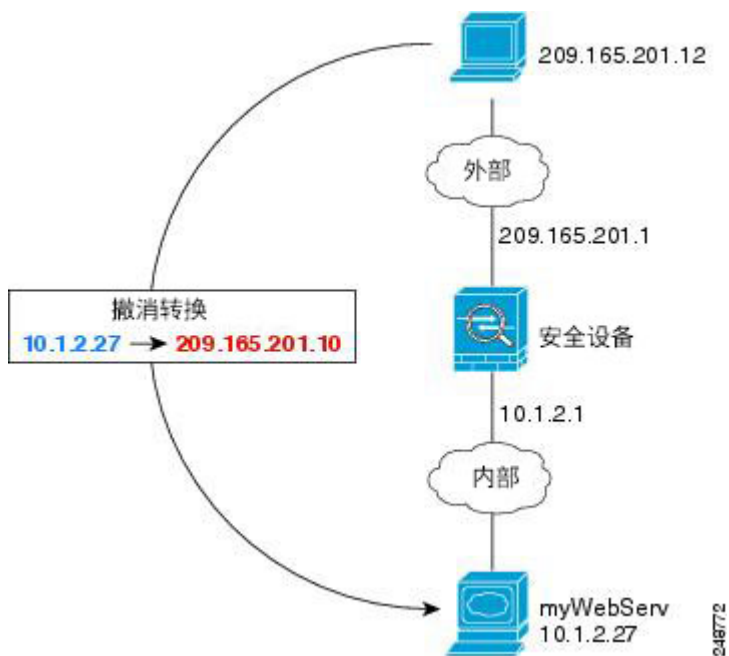
网络对象 NAT 示例

以下是网络对象 NAT 的一些配置示例。

为内部 Web 服务器提供访问（静态 NAT）

以下示例为内部 Web 服务器执行静态 NAT。实际地址位于专用网络上，因此公共地址是必需的。需要静态 NAT，以便主机能够在固定地址发起到 Web 服务器的流量。

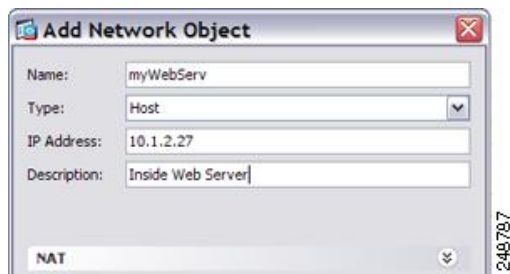
图 28: 面向内部 Web 服务器的静态 NAT



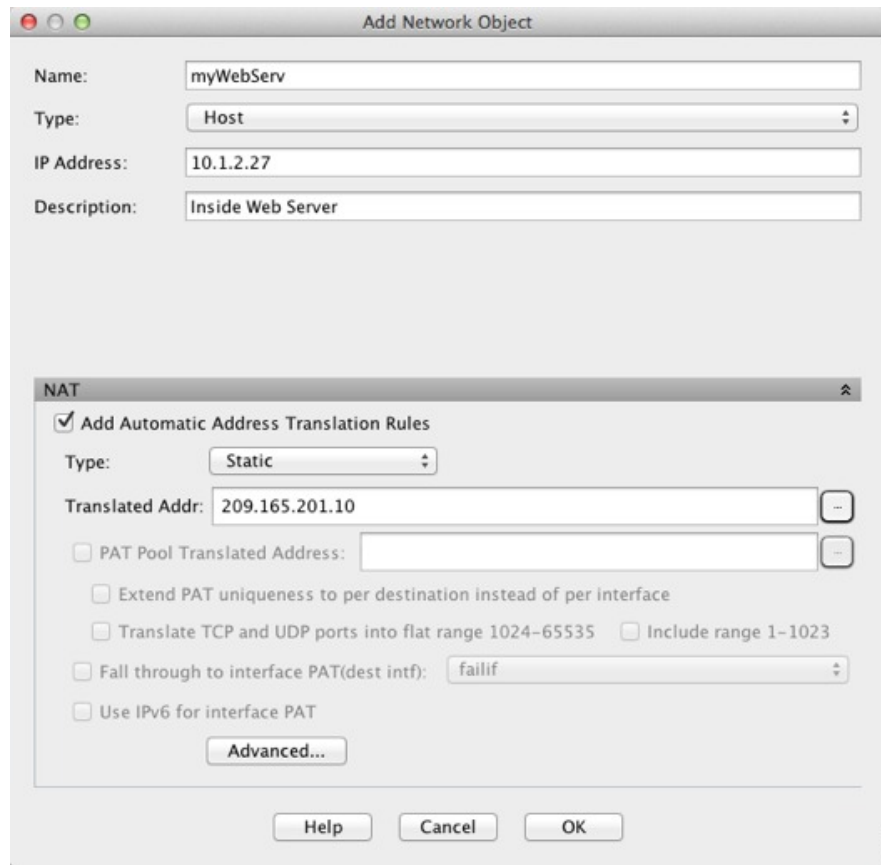
过程

步骤 1 依次选择配置 > 防火墙 > NAT。

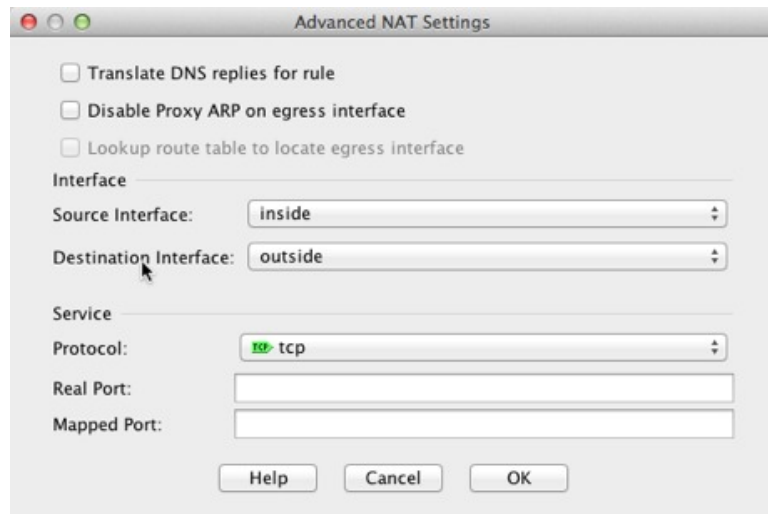
步骤 2 依次选择添加 > 网络对象 NAT 规则，为新的网络对象命名，然后定义 Web 服务器主机地址。



步骤 3 配置对象的静态 NAT。



步骤 4 点击 **Advanced** 并配置实际接口和映射接口。

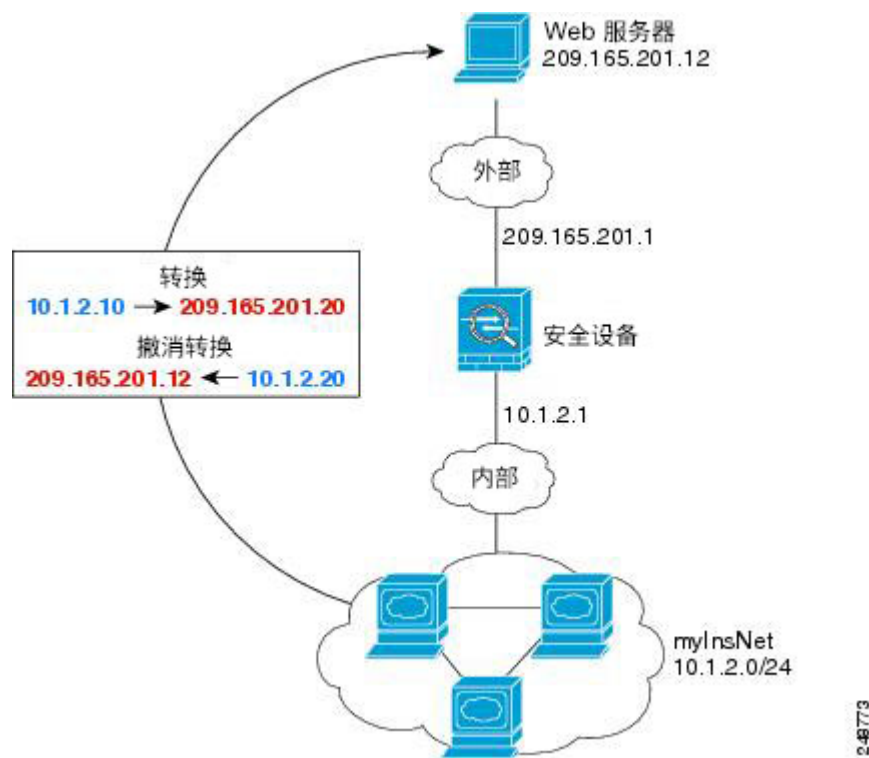


步骤 5 点击 **OK** 返回到 Edit Network Object 对话框，再次点击 **OK**，然后点击 **Apply**。

面向内部主机的 NAT（动态 NAT）和面向外部 Web 服务器的 NAT（静态 NAT）

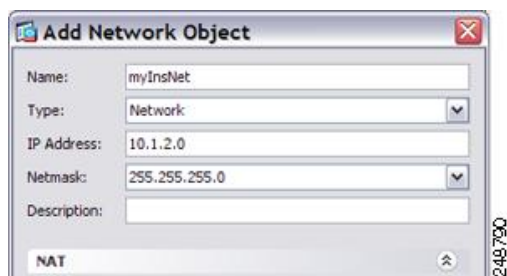
当专用网络上的内部用户访问外部 Web 服务器时，以下示例为这些用户配置动态 NAT。此外，当内部用户连接到外部 Web 服务器时，该 Web 服务器地址被转换为显示在内部网络上的地址。

图 29: 面向内部 Web 服务器的动态 NAT, 面向外部 Web 服务器的静态 NAT

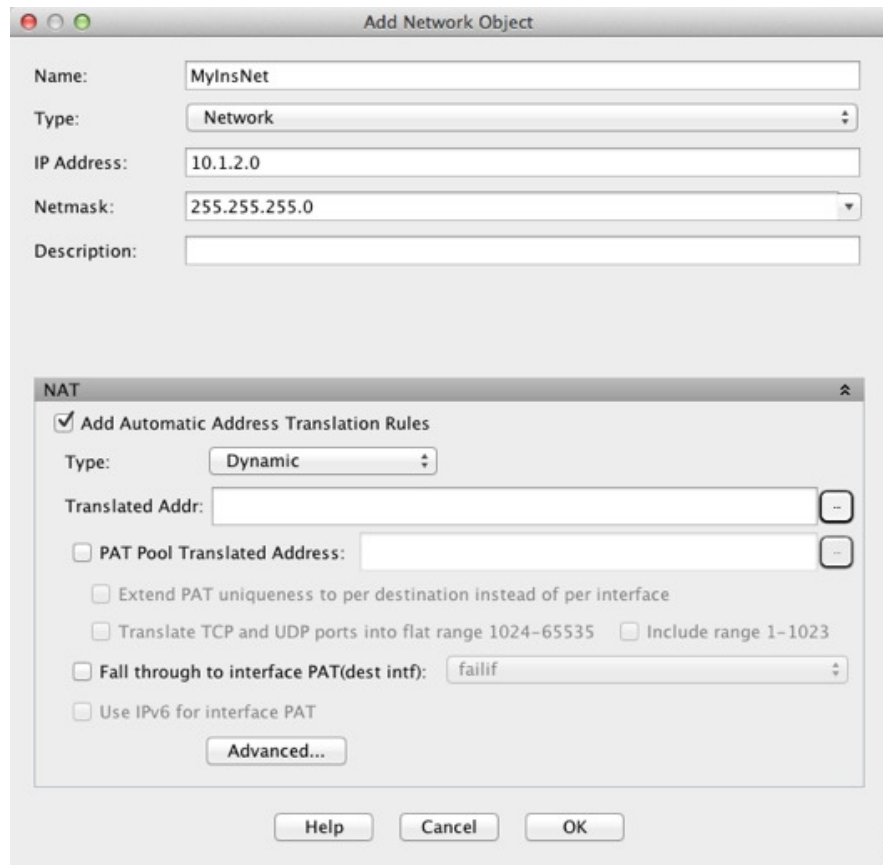


过程

- 步骤 1 依次选择配置 > 防火墙 > NAT。
- 步骤 2 依次选择添加 > 网络对象 NAT 规则，为新的网络对象命名，然后定义内部网络。

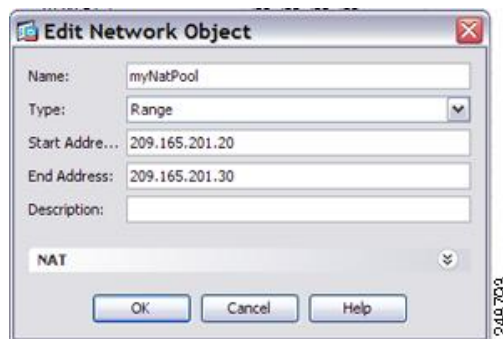


- 步骤 3 为内部网络启用动态 NAT。



步骤 4 对于 Translated Addr 字段，点击浏览按钮，为要向其转换内部地址的动态 NAT 池添加新网络对象。

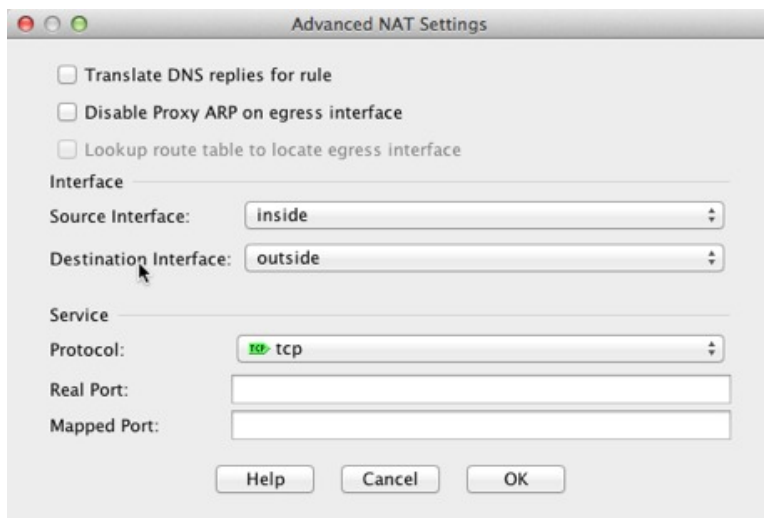
a) 依次选择 **Add > Network Object**，为新对象命名，在 NAT 池中定义地址范围，然后点击 **OK**。



b) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。

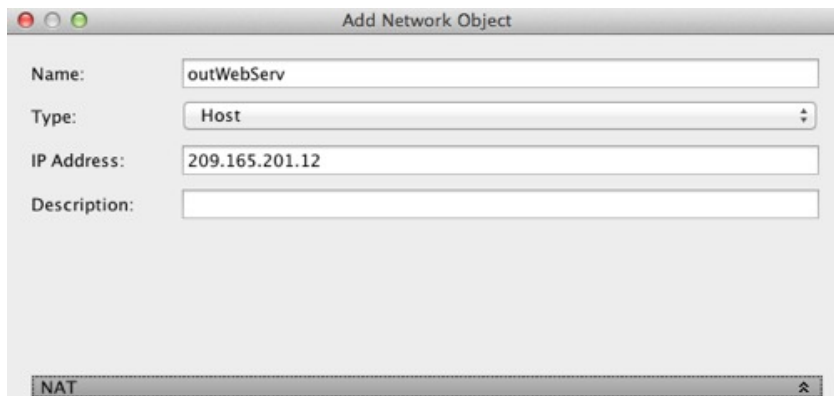


步骤 5 点击 **Advanced** 并配置实际接口和映射接口。

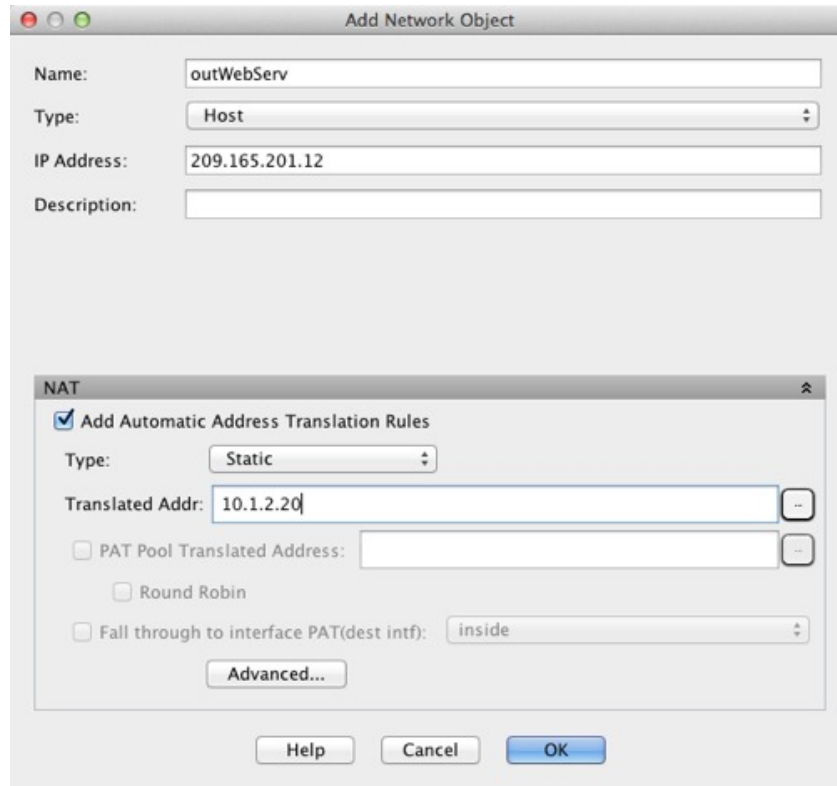


步骤 6 点击 **OK** 返回到 Edit Network Object 对话框，然后再次点击 **OK** 返回到 NAT Rules 表。

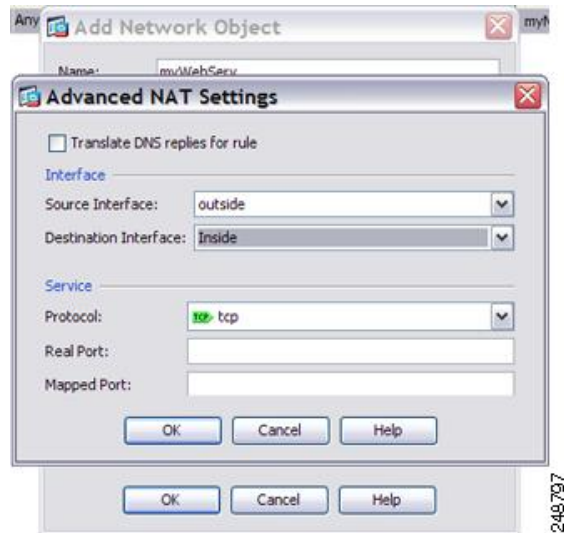
步骤 7 依次选择添加 > 网络对象 NAT 规则，并为外部 Web 服务器创建对象。



步骤 8 为 Web 服务器配置静态 NAT。



步骤 9 点击 **Advanced** 并配置实际接口和映射接口。

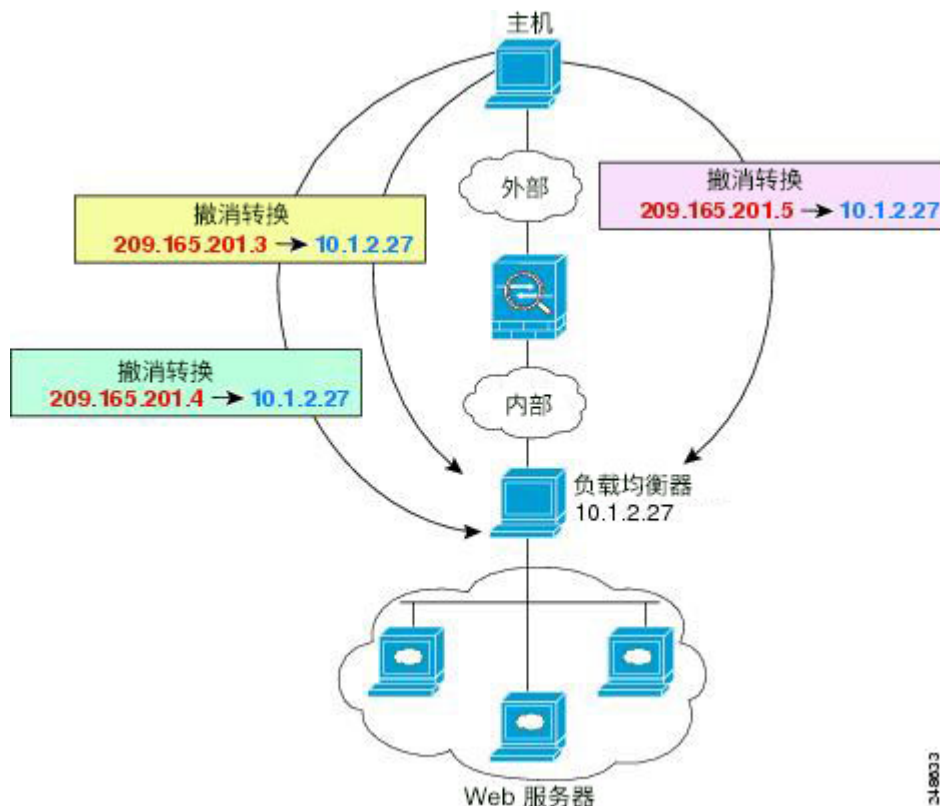


步骤 10 点击 **OK** 返回到 Edit Network Object 对话框，再次点击 **OK**，然后点击 **Apply**。

具有多个映射地址的内部负载均衡器（静态 NAT，一对多）

以下示例显示转换为多个 IP 地址的内部负载均衡器。当外部主机访问其中一个映射 IP 地址时，将该地址反向转换为单一负载均衡器地址。根据请求的 URL，它会将流量重新定向到正确的 Web 服务器。

图 30: 内部负载均衡器的一对多静态 NAT



过程

步骤 1 依次选择配置 > 防火墙 > NAT。

步骤 2 依次选择添加 > 网络对象 NAT 规则，为新网络对象命名并定义负载均衡器地址。

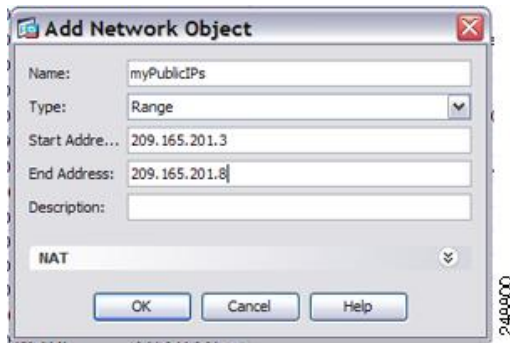


步骤 3 为负载均衡器启用静态 NAT:



步骤 4 对于 Translated Addr 字段，点击浏览按钮，为要向其转换负载均衡器地址的静态 NAT 地址组添加新网络对象。

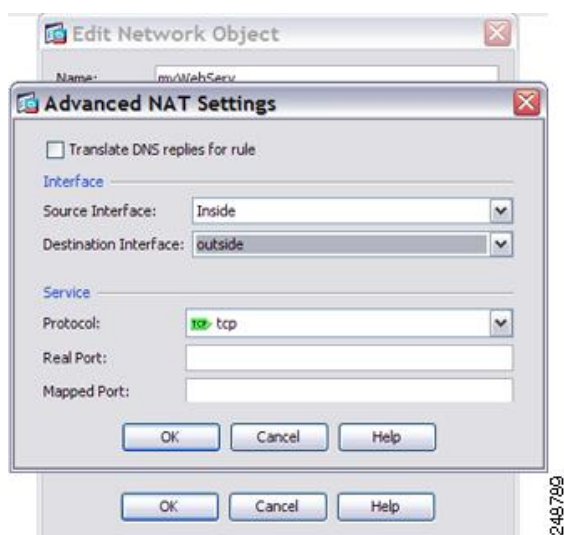
- a) 依次选择 **Add > Network Object**，为新对象命名，定义地址范围，然后点击 **OK**。



- b) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。



步骤 5 点击 **Advanced** 并配置实际接口和映射接口。

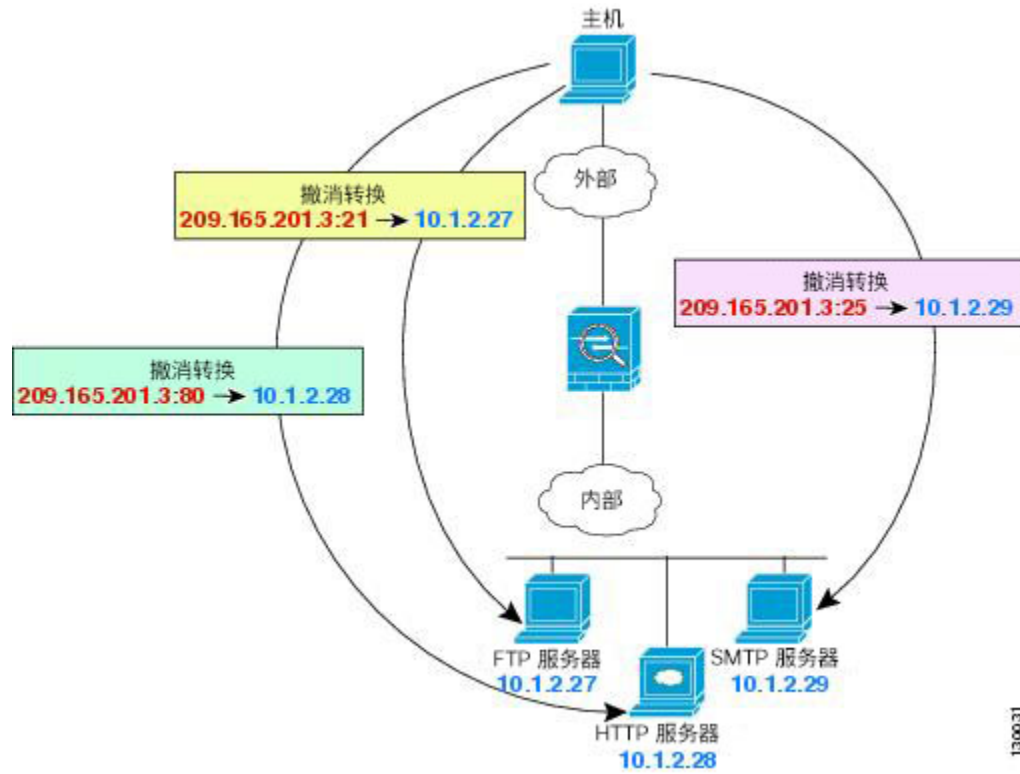


步骤 6 点击 **OK** 返回到 Edit Network Object 对话框，再次点击 **OK**，然后点击 **Apply**。

用于 FTP、HTTP 和 SMTP（支持端口转换的静态 NAT）的单一地址

以下支持端口转换的静态 NAT 示例为远程用户访问 FTP、HTTP 和 SMTP 提供单一地址。实际上，这些服务器是实际网络上的不同设备，但对于每台服务器，可以指定采用端口转换规则的静态 NAT，这些规则使用同一映射 IP 地址和不同端口。

图 31: 支持端口转换的静态 NAT



130031

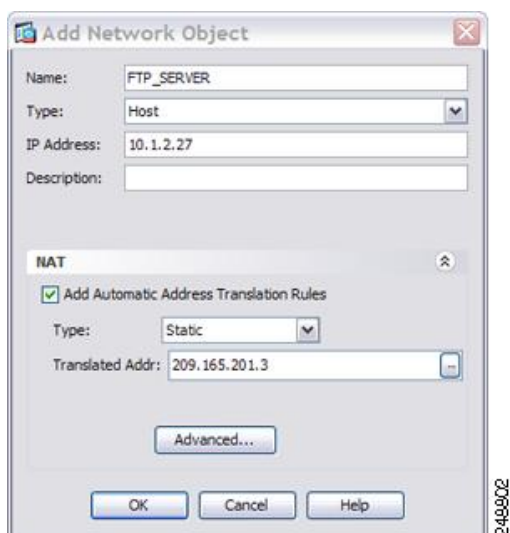
过程

步骤 1 依次选择配置 > 防火墙 > NAT。

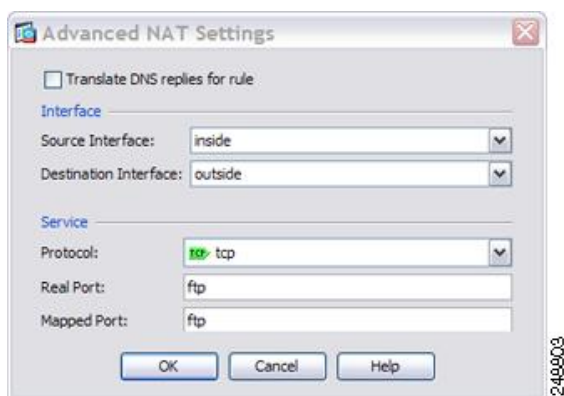
步骤 2 为 FTP 服务器配置支持端口转换规则的静态网络对象 NAT。

- a) 依次选择添加 > 网络对象 NAT 规则。
- b) 为新网络对象命名，定义 FTP 服务器地址，启用静态 NAT，并输入转换地址。

用于 FTP、HTTP 和 SMTP（支持端口转换的静态 NAT）的单一地址



- c) 点击 **Advanced**，为 FTP 配置实际接口和映射接口以及端口转换，将 FTP 端口映射到其本身。



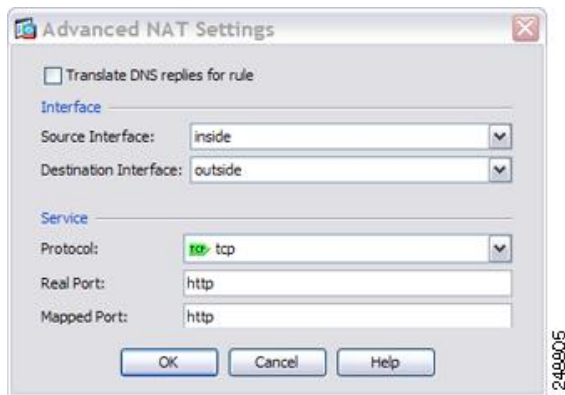
- d) 点击 **OK**，然后再次点击 **OK**，以保存规则并返回 NAT 页面。

步骤 3 为 HTTP 服务器配置支持端口转换规则的静态网络对象 NAT。

- a) 依次选择添加 > 网络对象 NAT 规则。
- b) 为新网络对象命名，定义 HTTP 服务器地址，启用静态 NAT，并输入转换地址。



- c) 点击 **Advanced**，为 HTTP 配置实际接口和映射接口以及端口转换，将 HTTP 端口映射到其本身。



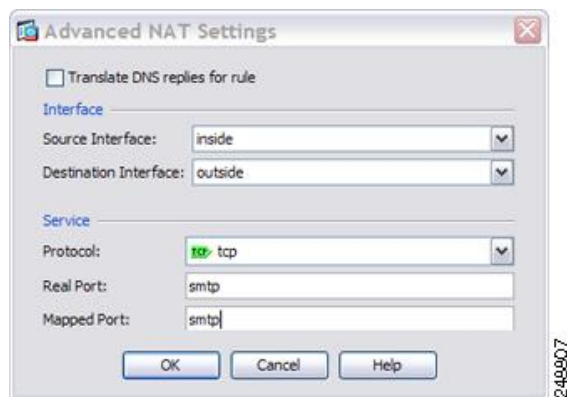
- d) 点击 **OK**，然后再次点击 **OK**，以保存规则并返回 NAT 页面。

步骤 4 为 SMTP 服务器配置支持端口转换规则的静态网络对象 NAT。

- a) 依次选择添加 > 网络对象 NAT 规则。
- b) 为新网络对象命名，定义 SMTP 服务器地址，启用静态 NAT，并输入转换地址。



- c) 点击 **Advanced**，为 SMTP 配置实际接口和映射接口以及端口转换，将 SMTP 端口映射到其本身。



- d) 点击 **OK** 返回到 Edit Network Object 对话框，再次点击 **OK**，然后点击 **Apply**。

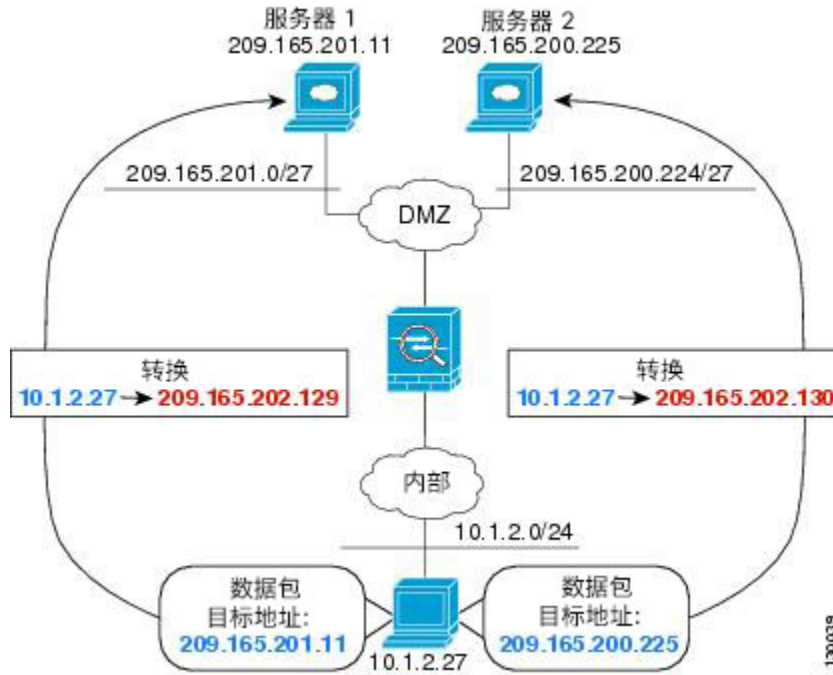
两次 NAT 的示例

本节包括以下配置示例：

根据目标进行不同的转换（动态两次 PAT）

下图显示 10.1.2.0/24 网络上的一台主机正在访问两台不同的服务器。当主机访问位于 209.165.201.11 的服务器时，实际地址将转换为 209.165.202.129:port。当主机访问位于 209.165.200.225 的服务器时，实际地址将转换为 209.165.202.130:端口。

图 32: 使用不同目标地址的两次 NAT

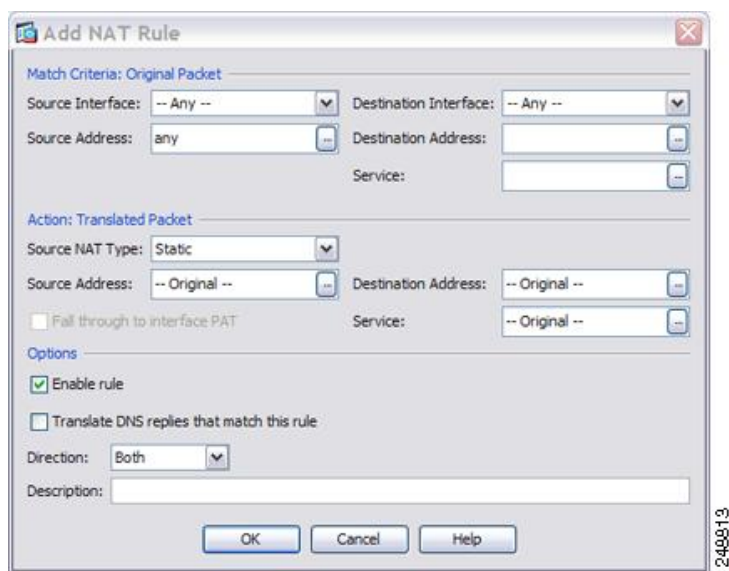


过程

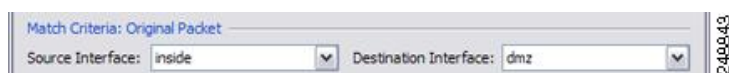
步骤 1 在配置 > 防火墙 > NAT 规则页面上，依次点击添加 > 在网络对象 NAT 规则之前添加 NAT 规则添加用于从内部网络传送到 DMZ 网络 1 的流量的 NAT 规则。

如果想要将 NAT 规则添加至网络对象 NAT 规则之后的第 3 部分，请选择 **Add NAT Rule After Network Object NAT Rules**。

系统将显示 Add NAT Rule 对话框。



步骤 2 设置源和目标接口。

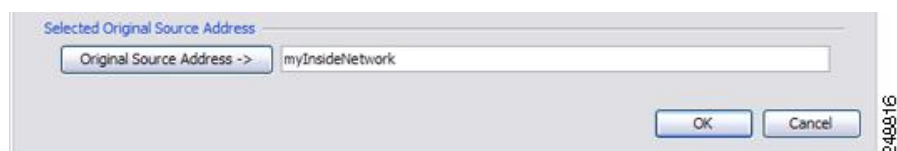


步骤 3 对于 Original Source Address，在 Browse Original Source Address 对话框中，点击浏览按钮以便为内部网络添加新网络对象。

- a) 依次选择 **Add > Network Object**。
- b) 定义内部网络地址，并点击 **OK**。



c) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。



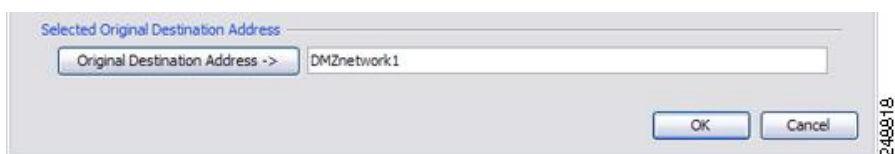
步骤 4 对于 Original Destination Address，在 Browse Original Destination Address 对话框中，点击浏览按钮以便为 DMZ 网络 1 添加新网络对象。

- a) 依次选择 **Add > Network Object**。

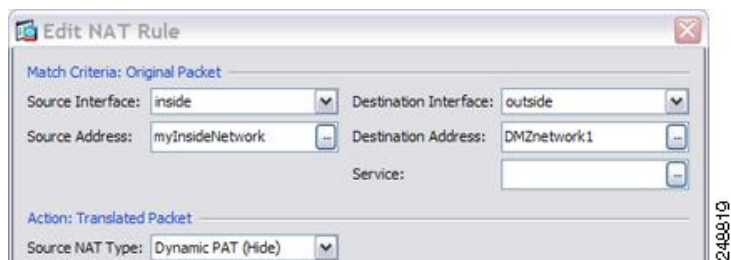
- b) 定义 DMZ 网络 1 地址，并点击 **OK**。



- c) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。



- 步骤 5** 将 NAT Type 设置为 **Dynamic PAT (Hide)**:

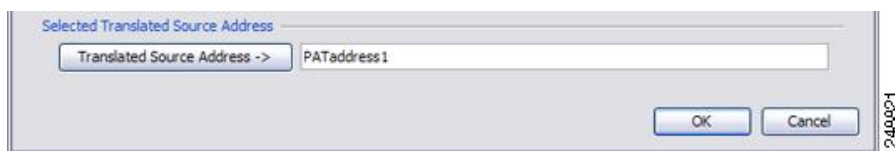


- 步骤 6** 对于 Translated Source Address，在 Browse Translated Source Address 对话框中，点击浏览按钮以便为 PAT 地址添加新网络对象。

- a) 依次选择 **Add > Network Object**。
b) 定义 PAT 地址，并点击 **OK**。

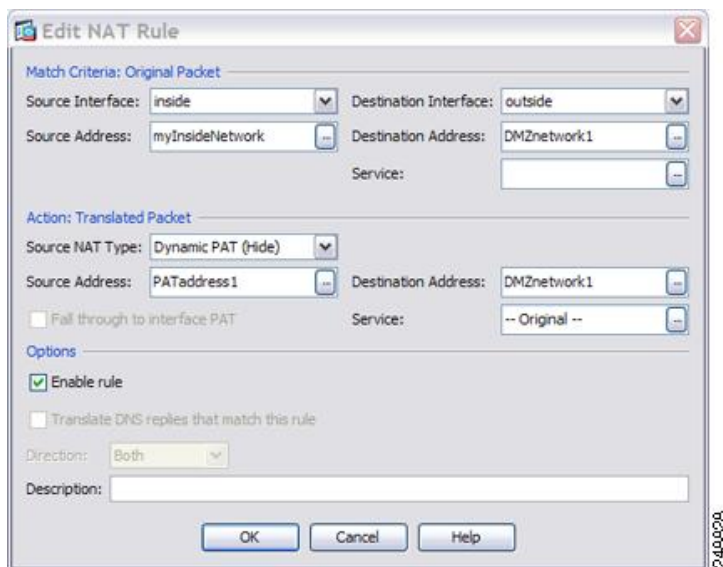


- c) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。



步骤 7 对于 Translated Destination Address，键入 Original Destination Address 的名称 (DMZnetwork1)，或者点击浏览按钮选择该地址。

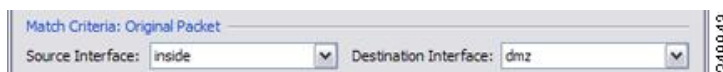
由于您不想转换目标地址，需要为其配置身份 NAT，只需为原始和转换后的目标地址指定相同的地址。



步骤 8 点击 **OK**，以将规则添加至 NAT 表。

步骤 9 依次点击添加 > 在网络对象 NAT 规则之前添加 NAT 规则或在网络对象 NAT 规则之后添加 NAT 规则，添加用于从内部网络传送到 DMZ 网络 2 的流量的 NAT 规则。

步骤 10 设置源和目标接口。



步骤 11 对于 Original Source Address，键入内部网络对象的名称 (myInsideNetwork)，或者点击浏览按钮选择该名称。

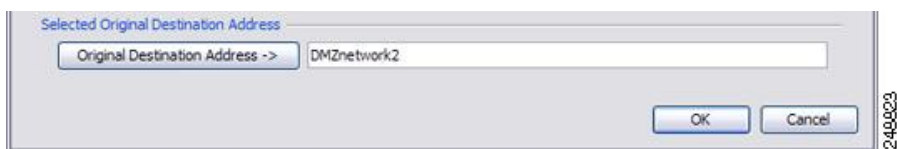
步骤 12 对于 Original Destination Address，在 Browse Original Destination Address 对话框中，点击浏览按钮以便为 DMZ 网络 2 添加新网络对象。

a) 依次选择 **Add > Network Object**。

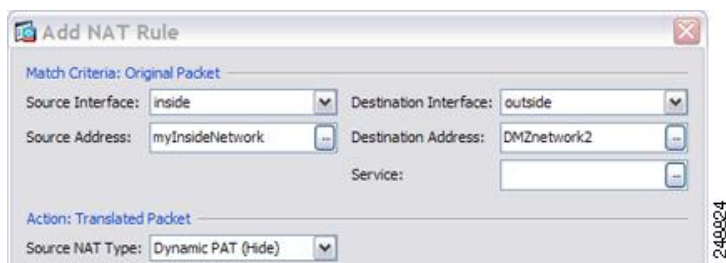
b) 定义 DMZ 网络 2 地址，并点击 **OK**。



- c) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。

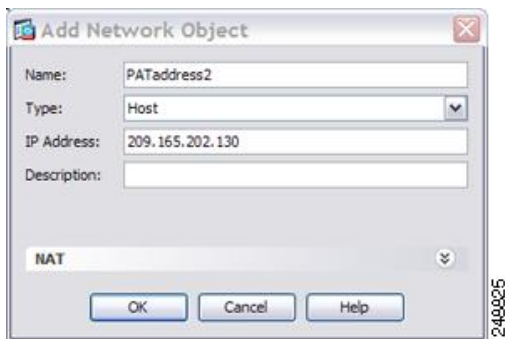


步骤 13 将 NAT Type 设置为 **Dynamic PAT (Hide)**:

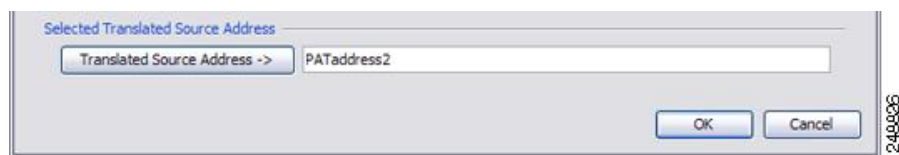


步骤 14 对于 Translated Source Address, 在 Browse Translated Source Address 对话框中, 点击浏览按钮以便为 PAT 地址添加新网络对象。

- a) 依次选择 **Add > Network Object**。
- b) 定义 PAT 地址, 并点击 **OK**。

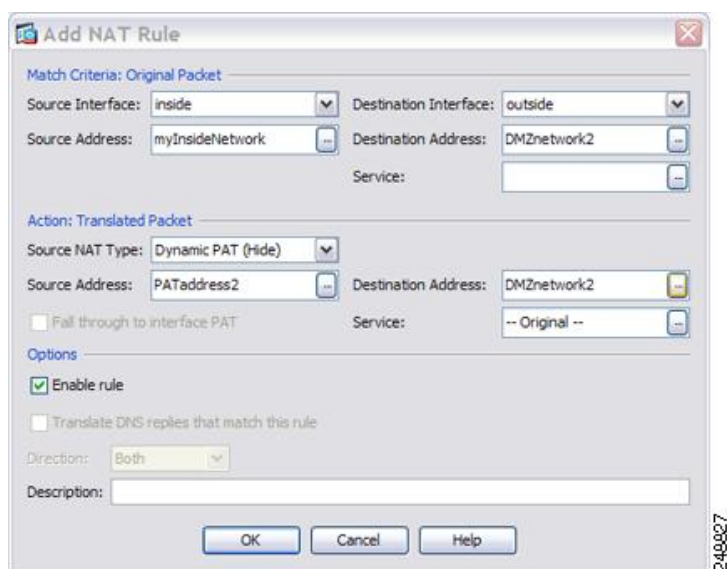


- c) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。



步骤 15 对于 Translated Destination Address，键入 Original Destination Address 的名称 (DMZnetwork2)，或者点击浏览按钮选择该地址。

由于您不想转换目标地址，需要为其配置身份 NAT，只需为原始和转换后的目标地址指定相同的地址。



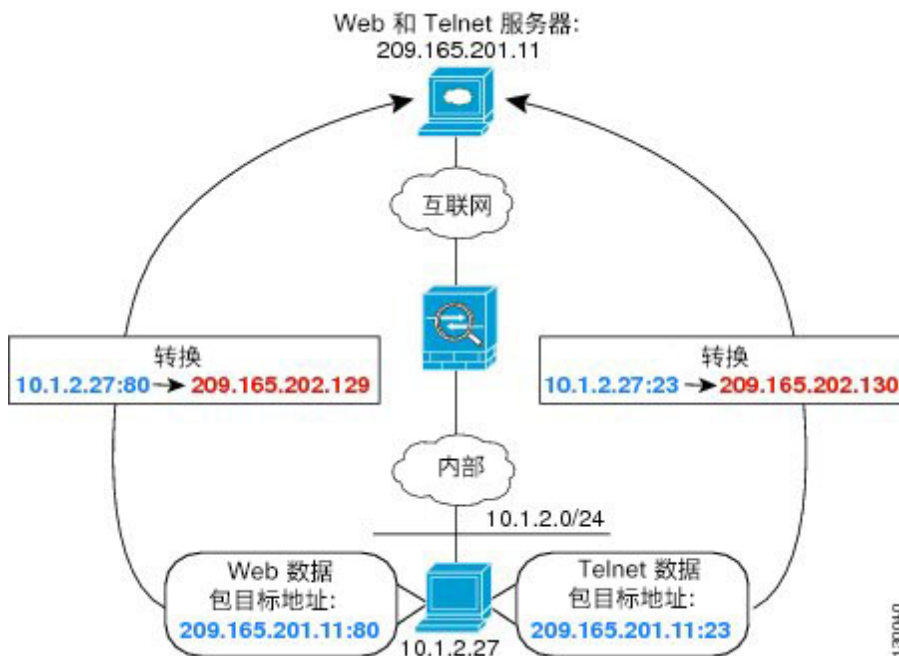
步骤 16 点击 **OK**，以将规则添加至 NAT 表。

步骤 17 点击 **Apply**。

根据目标地址和端口进行不同的转换（动态 PAT）

下图显示源端口和目的端口的使用情况。10.1.2.0/24 网络上的主机同时因为网络服务和 Telnet 服务访问单个主机。当主机进行 Telnet 服务访问服务器时，实际地址将转换为 209.165.202.129:port。当主机访问同一服务器以实现 Web 服务时，真实地址将转换为 209.165.202.130:port。

图 33: 使用不同目标端口的两次 NAT



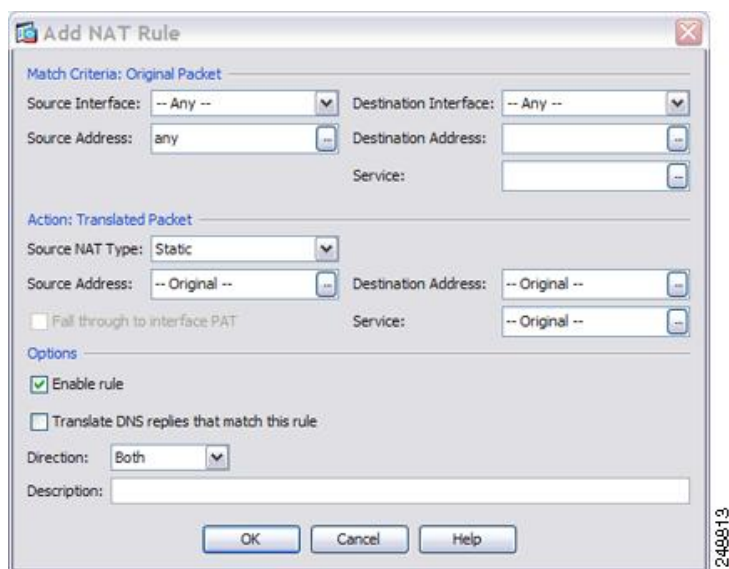
过程

步骤 1 在配置 > 防火墙 > NAT 规则页面上，依次点击添加 > 在网络对象 NAT 规则之前添加 NAT 规则添加用于从内部网络传送到 Telnet 服务器的流量的 NAT 规则。

如果想要将 NAT 规则添加至网络对象 NAT 规则之后的第 3 部分，请选择 **Add NAT Rule After Network Object NAT Rules**。

系统将显示 Add NAT Rule 对话框。

根据目标地址和端口进行不同的转换（动态 PAT）

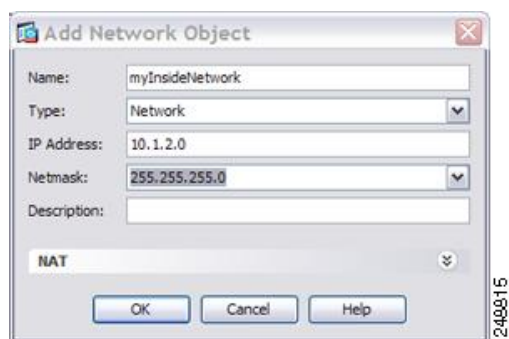


步骤 2 设置源和目标接口。

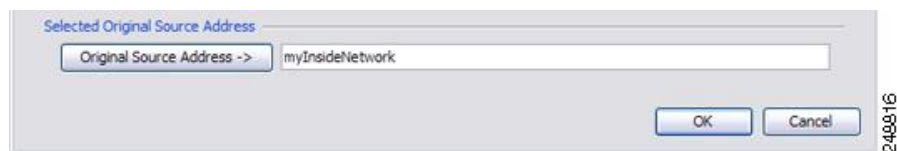


步骤 3 对于 Original Source Address，在 Browse Original Source Address 对话框中，点击浏览按钮以便为内部网络添加新网络对象。

- a) 依次选择 **Add > Network Object**。
- b) 定义内部网络地址，并点击 **OK**。



- c) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。

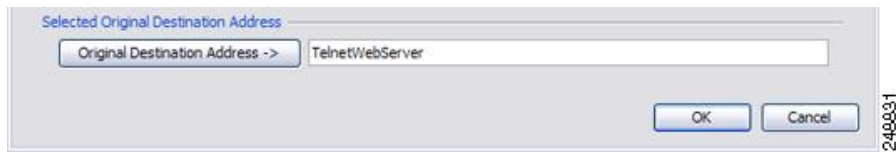


步骤 4 对于 Original Destination Address，在 Browse Original Destination Address 对话框中，点击浏览按钮以便为 Telnet/Web 服务器添加网络对象。

- a) 依次选择 **Add > Network Object**。
- b) 定义服务器地址，并点击 **OK**。

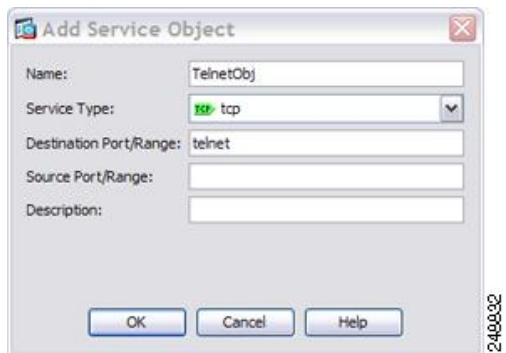


- c) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。

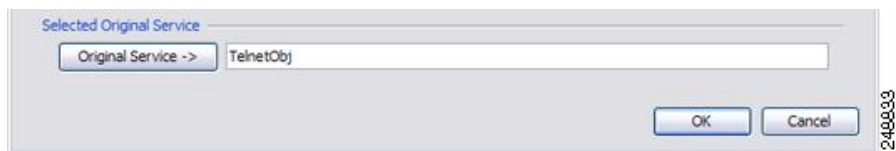


步骤 5 对于 Original Service，在 Browse Original Service 对话框中，点击浏览按钮，以便为 Telnet 添加新服务对象。

- a) 依次选择 **Add > Service Object**。
- b) 定义协议和端口，并点击 **OK**。

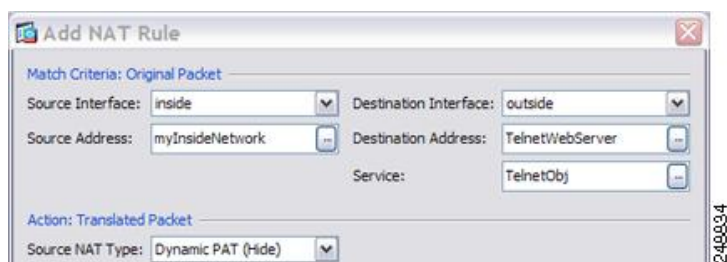


- c) 双击新服务对象将其选中。点击 **OK** 返回到 NAT 配置。



步骤 6 将 NAT Type 设置为 **Dynamic PAT (Hide)**:

根据目标地址和端口进行不同的转换（动态 PAT）

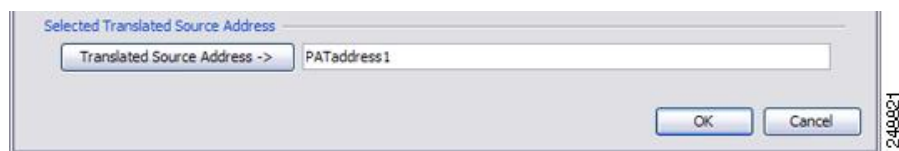


步骤 7 对于 Translated Source Address, 在 Browse Translated Source Address 对话框中, 点击浏览按钮以便为 PAT 地址添加新网络对象。

- a) 依次选择 **Add > Network Object**。
- b) 定义 PAT 地址, 并点击 **OK**。

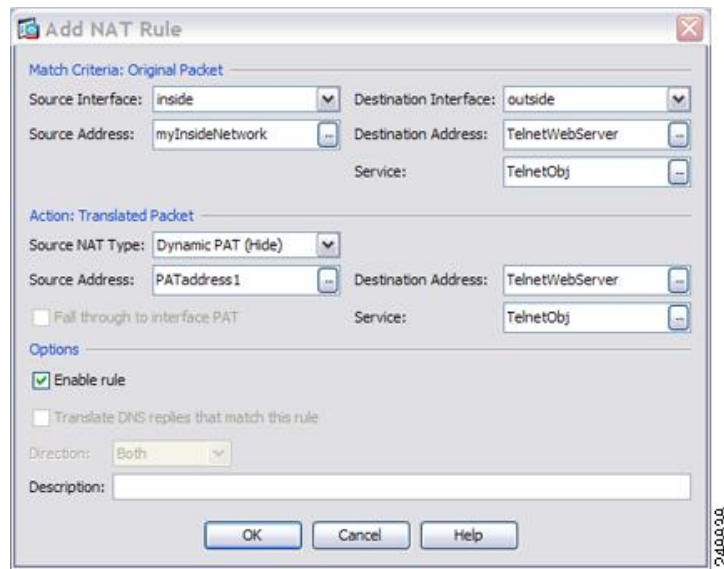


- c) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。



步骤 8 对于 Translated Destination Address, 键入 Original Destination Address 的名称 (TelnetWebServer), 或者点击浏览按钮选择该地址。

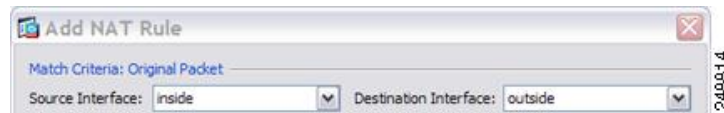
由于您不想转换目标地址, 需要为其配置身份 NAT, 只需为原始和转换后的目标地址指定相同的地址。



步骤 9 点击 **OK**，以将规则添加至 NAT 表。

步骤 10 依次点击添加 > 在网络对象 NAT 规则之前添加 NAT 规则或在网络对象 NAT 规则之后添加 NAT 规则，添加用于从内部网络传送到 Web 服务器的流量的 NAT 规则。

步骤 11 设置实际和映射接口。

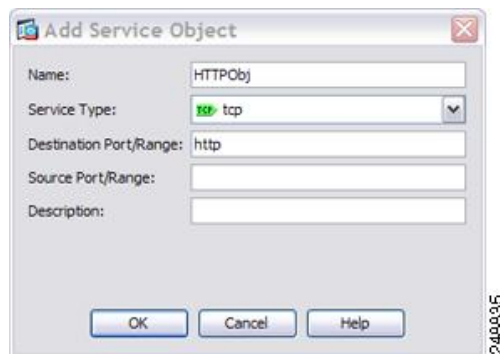


步骤 12 对于 Original Source Address，键入内部网络对象的名称 (myInsideNetwork)，或者点击浏览按钮选择该名称。

步骤 13 对于 Original Destination Address，键入 Telnet/Web 服务器网络对象的名称 (TelnetWebServer)，或者点击浏览按钮选择该名称。

步骤 14 对于 Original Service，在 Browse Original Service 对话框中，点击浏览按钮，以便为 HTTP 添加新服务对象。

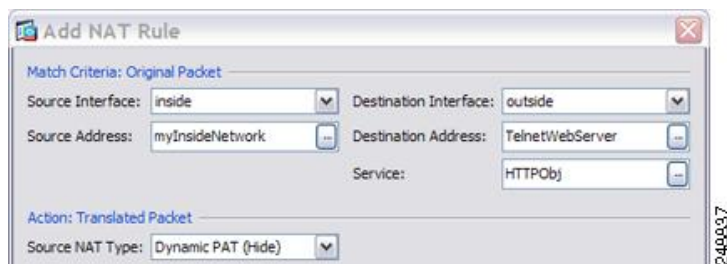
- a) 依次选择 **Add > Service Object**。
- b) 定义协议和端口，并点击 **OK**。



- c) 双击新服务对象将其选中。点击 **OK** 返回到 NAT 配置。



- 步骤 15 将 NAT Type 设置为 **Dynamic PAT (Hide)**:

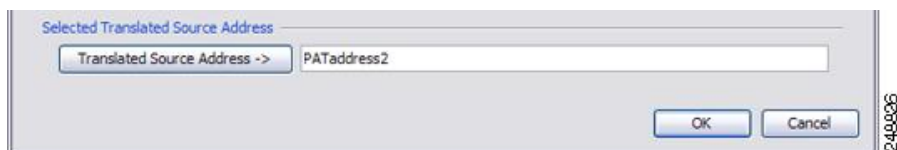


- 步骤 16 对于 Translated Source Address, 在 Browse Translated Source Address 对话框中, 点击浏览按钮以便为 PAT 地址添加新网络对象。

- a) 依次选择 **Add > Network Object**。
b) 定义 PAT 地址, 并点击 **OK**。

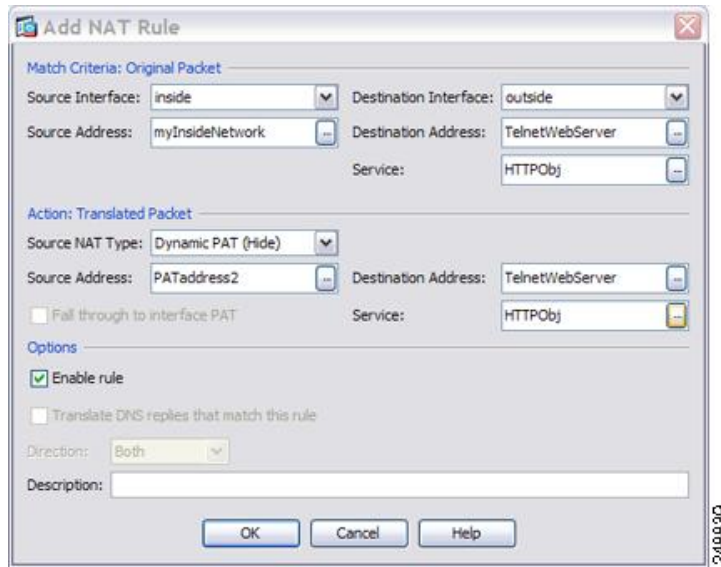


- c) 双击新网络对象将其选中。点击 **OK** 返回到 NAT 配置。



- 步骤 17 对于 Translated Destination Address, 键入 Original Destination Address 的名称 (TelnetWebServer), 或者点击浏览按钮选择该地址。

由于您不想转换目标地址, 需要为其配置身份 NAT, 只需为原始和转换后的目标地址指定相同的地址。



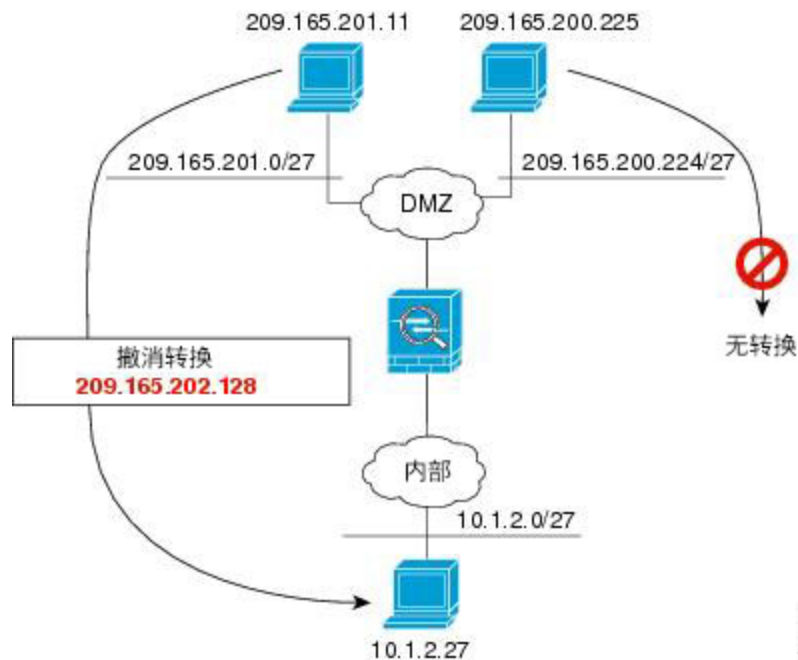
步骤 18 点击 **OK**，以将规则添加至 NAT 表。

步骤 19 点击 **Apply**。

示例：支持目标地址转换的两次 NAT

下图显示一台连接到映射主机的远程主机。映射主机有一个两次静态 NAT 转换，将仅面向流量的实际地址转换到 209.165.201.0/27 网络或从 209.165.201.0/27 网络转换。不存在面向 209.165.200.224/27 网络的转换，因此转换主机不能连接到该网络，该网络上的主机也不能连接到转换主机。

图 34: 支持目标地址转换的两次静态 NAT



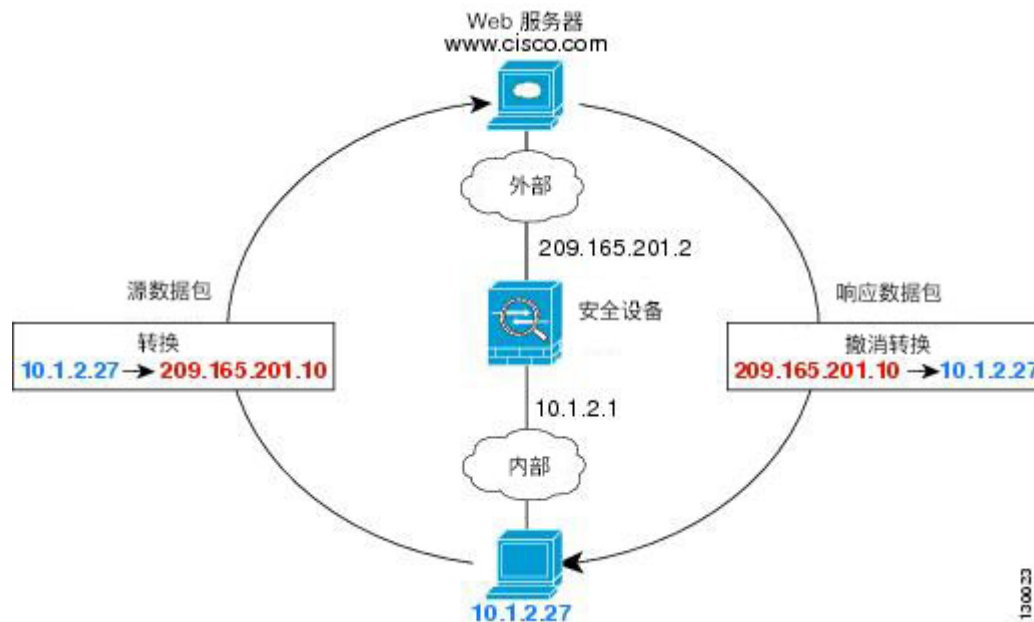
路由和透明防火墙模式下的 NAT

可以在路由和透明防火墙模式下配置 NAT。以下部分介绍每种防火墙模式的典型用法。

路由模式下的 NAT

下图显示路由模式下的一个典型 NAT 示例，专用网络位于内部。

图 35: NAT 示例: 路由模式



1. 当位于 10.1.2.27 的内部主机向 Web 服务器发送数据包时，数据包的实际源地址 10.1.2.27 会转换为映射地址 209.165.201.10。
2. 当服务器响应时，它会将响应发送到映射地址 209.165.201.10，ASA 接收数据包，因为 ASA 执行代理 ARP 以认领数据包。
3. 接下来，ASA 变更从映射地址 209.165.201.10 回到实际地址 10.1.2.27 的转换，然后再发送到主机。

透明模式下或桥接组内的 NAT

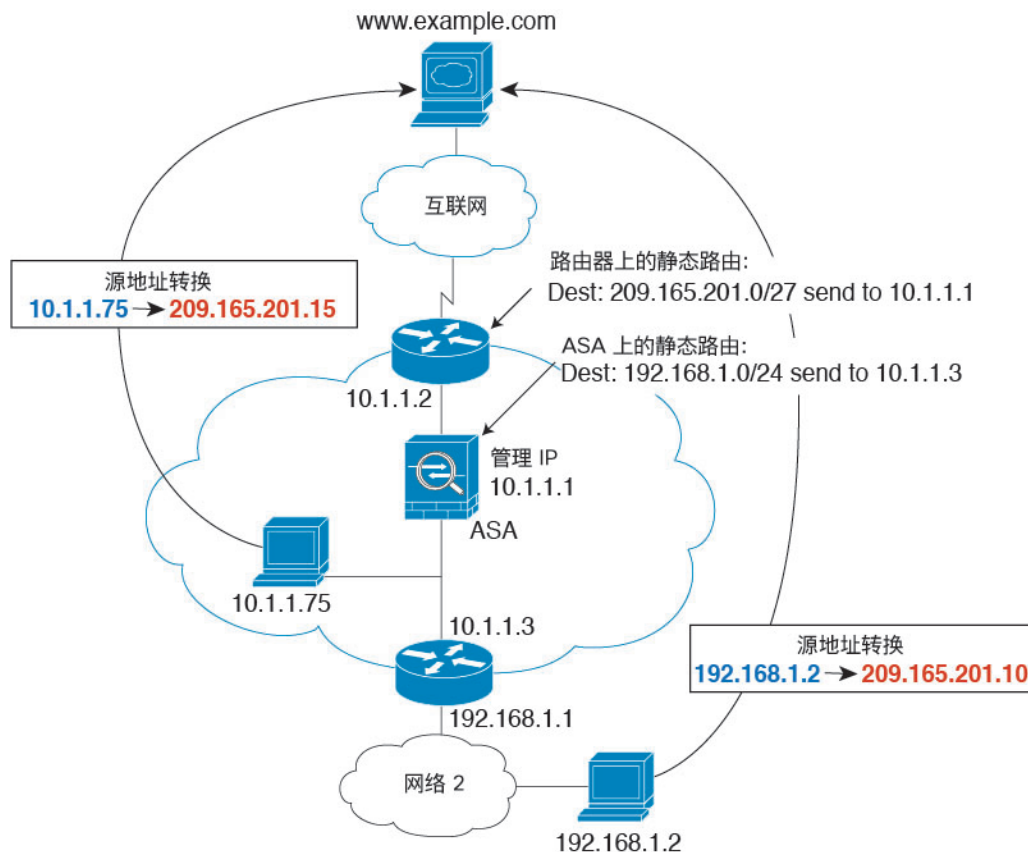
在透明模式下使用 NAT 可以消除上游或下游路由器为其网络执行 NAT 的需求。在路由模式下，NAT 可以执行与桥接组内类似的功能。

透明模式下的 NAT 或在路由模式下同一桥接组的成员之间具有以下要求和局限性：

- 当映射地址是桥接组成员接口时，不能配置接口 PAT，因为没有 IP 地址连接到该接口。
- 不支持 ARP 检测。此外，如果由于某种原因，ASA 一端的主机向 ASA 另一端的主机发送 ARP 请求，而且发起主机实际地址被映射到同一子网的不同地址，则实际地址在 ARP 请求中依然可见。
- 不支持在 IPv4 和 IPv6 网络之间进行转换。支持在两个 IPv6 网络之间或两个 IPv4 网络之间进行转换。

下图显示透明模式下的典型 NAT 场景，内部接口和外部接口上的网络相同。在此场景中，透明防火墙执行 NAT 服务，因此上游路由器不必执行 NAT。

图 36: NAT 示例: 透明模式



1. 当位于 10.1.1.75 的内部主机将数据包发送到 Web 服务器时，数据包的实际源地址 10.1.1.75 被更改为映射地址 209.165.201.15。
2. 当服务器响应时，它将响应发送到映射地址 209.165.201.15，ASA 接收数据包，因为上游路由器将此映射网络包含在定向到 ASA 管理 IP 地址的静态路由中。
3. 然后，ASA 取消映射地址 209.165.201.15 回到实际地址 10.1.1.1.75 的转换。因为实际地址是直接连接的，所以 ASA 将实际地址直接发送到主机。
4. 对于主机 192.168.1.2，发生相同流程，但返回流量除外，ASA 在其路由表中查询路由，根据 192.168.1.0/24 的 ASA 静态路由，将数据包发送到位于 10.1.1.3 的下游路由器。

路由 NAT 数据包

ASA 需要是发送到映射地址的任何数据包的目的地。此外，ASA 还需要为它收到的以映射地址为目标的数据包确定出口接口。本节介绍 ASA 如何处理通过 NAT 接受和交付数据包。

映射地址和路由

将实际地址转换为映射地址时，如果需要，您选择的映射地址将确定如何为映射地址配置路由。

请参阅[其他 NAT 指南](#)，第 177 页，了解有关映射 IP 地址的其他指导原则。

以下主题介绍映射地址类型。

地址与映射接口在相同的网络中

如果使用与目的地（映射）接口在同一网络中的地址，ASA 使用代理 ARP 应答任何对映射地址的 ARP 请求，从而拦截发往映射地址的流量。此解决方案可以简化路由，因为 ASA 不必成为任何其他网络的网关。如果外部网络包含足够多的空闲地址，并且您正在使用 1:1 转换（例如动态 NAT 或静态 NAT），此解决方案是理想选择。动态 PAT 可显著增加您可以通过少量地址实现的转换数量，因此即使外部网络中的可用地址较少，依然可以使用此方法。对于 PAT，甚至可以使用映射接口的 IP 地址。



注释

如果将映射接口配置为任何接口，而且在与其中一个映射接口相同的网络中指定映射地址，那么如果从其他接口传入对此映射地址的 ARP 请求，则需要为入口接口上为该网络手动配置 ARP 条目，并指定其 MAC 地址。通常，如果该映射接口指定任何接口，则将唯一网络用于此映射地址，避免此类情况发生。依次选择配置 > 设备管理 > 高级 > ARP > ARP 静态表来配置 ARP。

唯一网络中的地址

如果需要比目的地（映射）接口网络上提供的地址更多的地址，则可以识别其他子网中的地址。上游路由器需要对指向 ASA 的映射地址进行静态路由。

或者，对于路由模式，可以将目标网络上的任何 IP 地址用作网关，为映射地址配置 ASA 上的静态路由，然后使用路由协议重新分配路由。例如，如果您将 NAT 用于内部网络 (10.1.1.0/24)，并且使用映射 IP 地址 209.165.201.5，则可以为 10.1.1.99 网关配置 209.165.201.5 255.255.255.255（主机地址）的可重新分发静态路由。

```
route inside 209.165.201.5 255.255.255.255 10.1.1.99
```

对于透明模式，如果直接连接实际主机，则将上游路由器的静态路由配置为指向 ASA：在 8.3 中，指定全局管理 IP 地址；在 8.4(1) 及更高版本中，指定桥接组 IP 地址。对于透明模式下的远程主机，在上游路由器上的静态路由中，您也可以指定下游路由器 IP 地址。

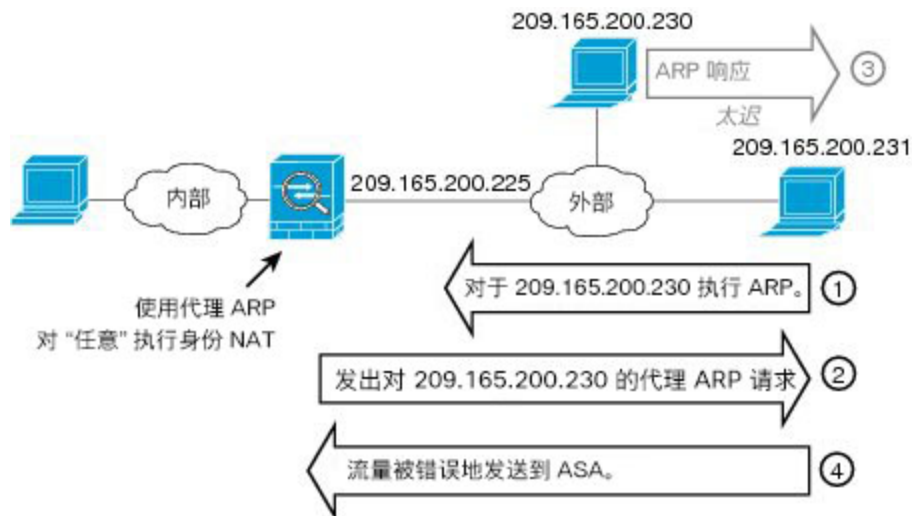
与实际地址相同的地址（身份 NAT）

（8.3(1)、8.3(2) 和 8.4(1)）用于身份 NAT 的默认行为已禁用代理 ARP。无法配置此设置。

（8.4(2) 及更高版本）用于身份 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。如果需要，可以禁用代理 ARP。如果需要，还可以为常规静态 NAT 禁用代理 ARP，在这种情况下，需要确保上游路由器上有适当的路由。

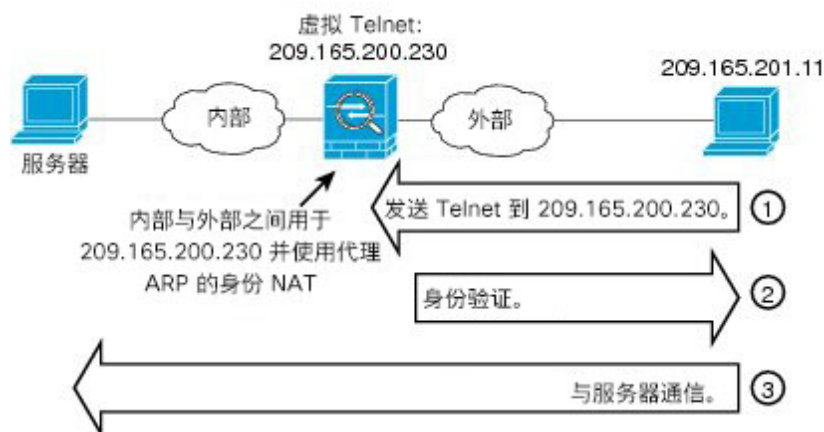
通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。例如，如果为“任何”IP 地址配置一条大体的身份 NAT 规则，则使代理 ARP 保持启用状态会给直接连接到映射接口的网络上的主机造成问题。在这种情况下，当映射网络上的主机要与同一网络上的其他主机通信时，ARP 请求中的地址匹配 NAT 规则（匹配“任何”地址）。然后，ASA 将代理地址的 ARP，即使数据包实际上不以 ASA 为目标。（请注意，即便已设置两次 NAT 规则，也会造成此问题；虽然 NAT 规则必须匹配源地址和目标地址，但仅会根据“源”地址作出代理 ARP 决定）。如果在实际主机 ARP 响应之前收到 ASA ARP 响应，则流量会错误地发送到 ASA。

图 37: 身份 NAT 的代理 ARP 问题



在极少数情况下，需要面向身份 NAT 的代理 ARP；例如，对于虚拟 Telnet。将 AAA 用于网络访问时，主机需要先利用 Telnet 等服务对 ASA 进行身份验证，然后才能让任何其他流量通过。您可以在 ASA 上配置虚拟 Telnet 服务器，以提供必需的登录。从外部访问虚拟 Telnet 地址时，必需为此地址配置身份 NAT 规则，尤其是对于代理 ARP 功能而言。由于虚拟 Telnet 的内部流程，代理 ARP 允许 ASA 保留以虚拟 Telnet 地址为目的的流量，而不是根据 NAT 规则将流量发送到源接口外部。（请见下图。）

图 38: 代理 ARP 和虚拟 Telnet



远程网络的透明模式路由要求

在透明模式下使用 NAT 时，某些类型的流量要求静态路由。有关更多信息，请参阅一般操作配置指南。

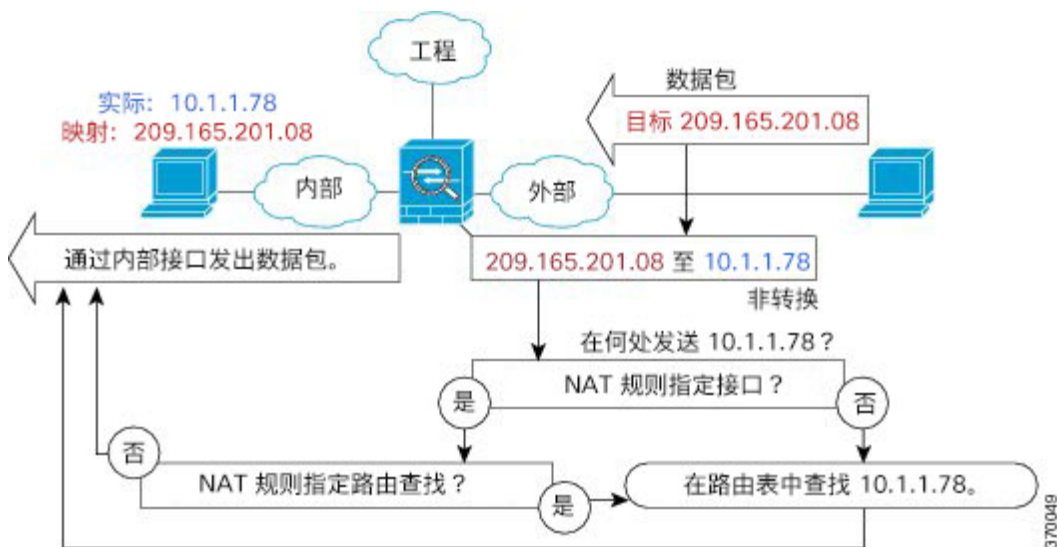
确定出口接口

当使用 NAT 且 ASA 接收映射地址的流量时，ASA 根据 NAT 规则取消转换目标地址，然后将数据包发送到实际地址。ASA 按照以下方式数据包确定出口接口：

- 透明模式或路由模式下的网桥组接口 - ASA 使用 NAT 规则，为实际地址确定出口接口；您必须在 NAT 规则中指定源和目标网桥组成员接口。
- 路由模式下的常规接口 - ASA 按照以下其中一种方式确定出口接口：
 - 在 NAT 规则中配置接口 - ASA 使用 NAT 规则确定出口接口。（8.3(1) 到 8.4(1)）唯一的例外是面向身份 NAT，其中该身份 NAT 始终使用路由查询，无论 NAT 配置如何。（8.4(2) 及更高版本）对于身份 NAT，默认行为是要使用 NAT 配置。然而，您可以选择始终使用路由查询。在某些情景下，必须使用路由查找覆盖。
 - 不在 NAT 规则中配置接口 - ASA 使用路由查询确定出口接口。

下图显示路由模式下的出口接口选择方法。几乎在所有情况下，路由查询都等同于 NAT 规则接口，但在某些配置中，这两种方法可能不同。

图 39: 含 NAT 的路由模式出口接口选择



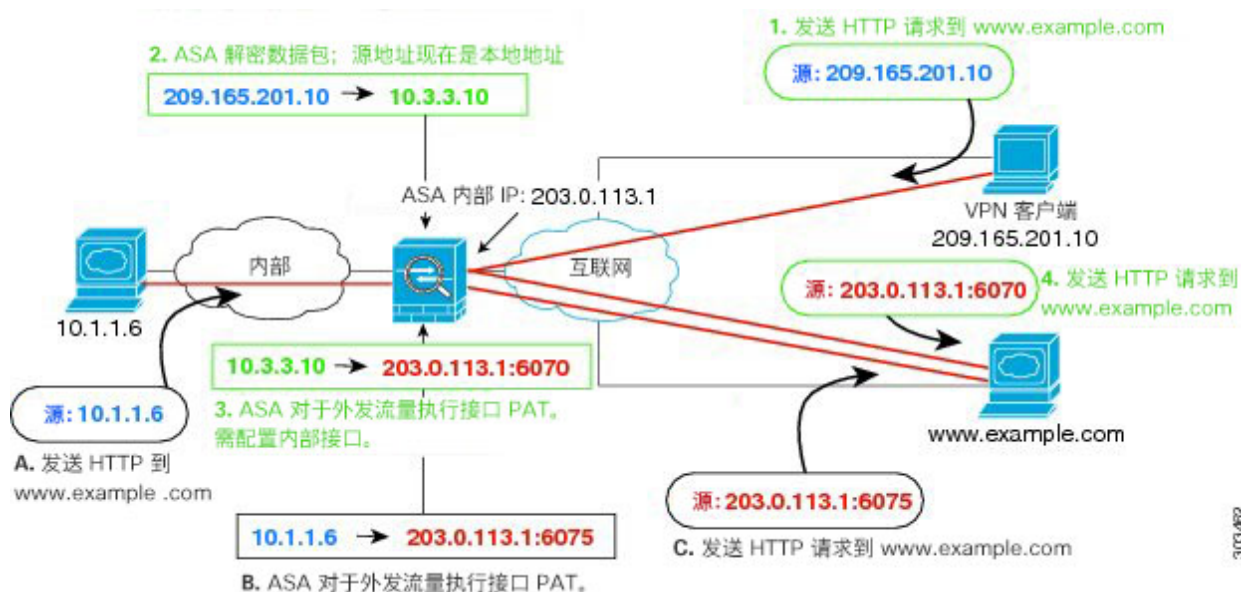
用于 VPN 的 NAT

以下主题借助各种类型的 VPN 来介绍 NAT 用途。

NAT 和远程访问 VPN

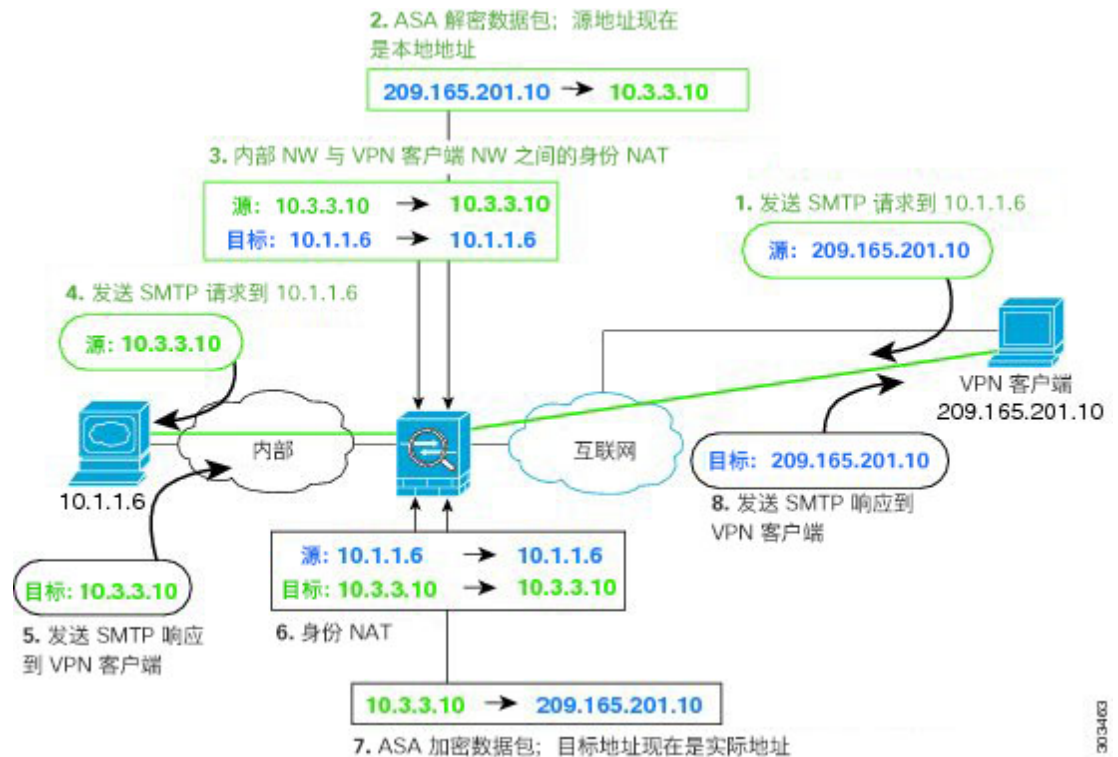
下图显示访问互联网的内部服务器 (10.1.1.6) 和 VPN 客户端 (209.165.201.10)。除非为 VPN 客户端配置拆分隧道（只有指定流量会流经 VPN 隧道），否则互联网绑定的 VPN 流量还必须流经 ASA。当 VPN 流量传入 ASA 时，ASA 会解密数据包；生成的数据包会将 VPN 客户端本地地址 (10.3.3.10) 作为源。对于内部和 VPN 客户端本地网络，需要使用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口 PAT 规则。为使 VPN 流量可以退出其已进入的相同接口，还需要启用接口内通信（也称为“发夹”网络）。

图 40: 面向互联网绑定 VPN 流量的接口 PAT（接口内）



下图显示要访问内部邮件服务器的 VPN 客户端。由于 ASA 预计内部网络与任何外部网络之间的流量与您为互联网访问设置的 PAT 规则匹配，所以从 VPN 客户端 (10.3.3.10) 流向 SMTP 服务器 (10.1.1.6) 的流量会由于反向路径失败而被丢弃：从 10.3.3.10 流向 10.1.1.6 的流量与 NAT 规则不匹配，但从 10.1.1.6 返回 10.3.3.10 的流量应与外发流量的接口 PAT 规则匹配。由于转发流和反向流不匹配，ASA 在收到数据包时会将其丢弃。为避免这种故障，需要在那些网络之间使用身份 NAT 规则，使内部到 VPN 客户端流量免于应用接口 PAT 规则。身份 NAT 只能将地址转换为其相同的地址。

图 41: 面向 VPN 客户端的身份 NAT



请参阅以下用于上述网络的 NAT 配置示例:

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

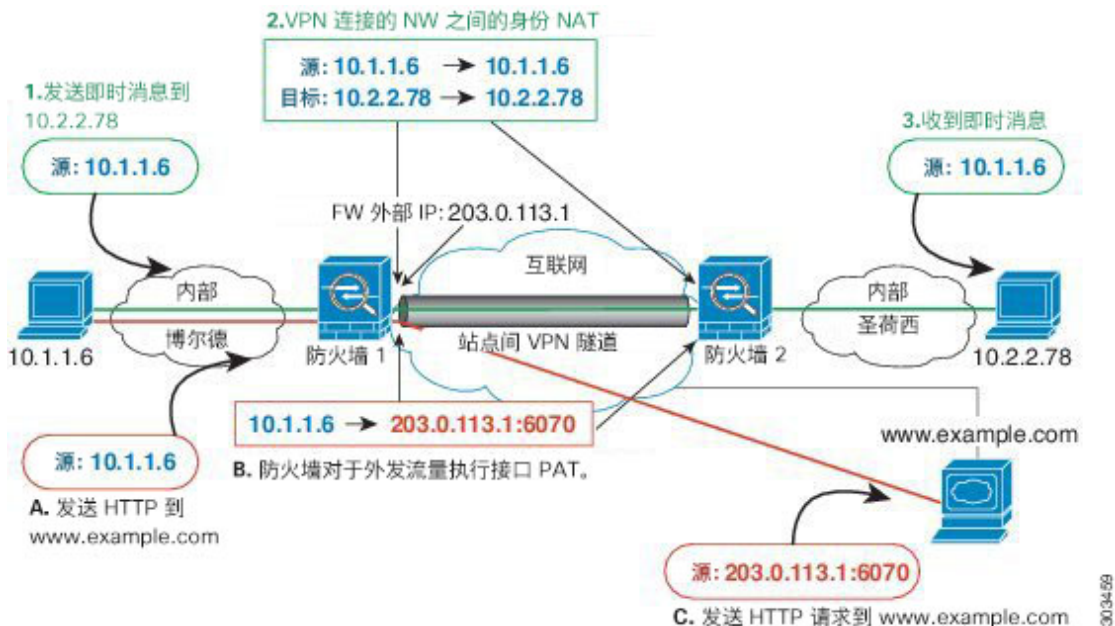
! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local vpn_local
```

NAT 和站点到站点 VPN

下图显示连接博尔德办公室和圣荷西办公室的站点到站点隧道。对于要发送到互联网的流量（例如，从博尔德办公室中的 10.1.1.6 到 www.example.com），需要利用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口 PAT 规则。然而，对于要穿过 VPN 隧道的流量（例如，从博尔德办公室中

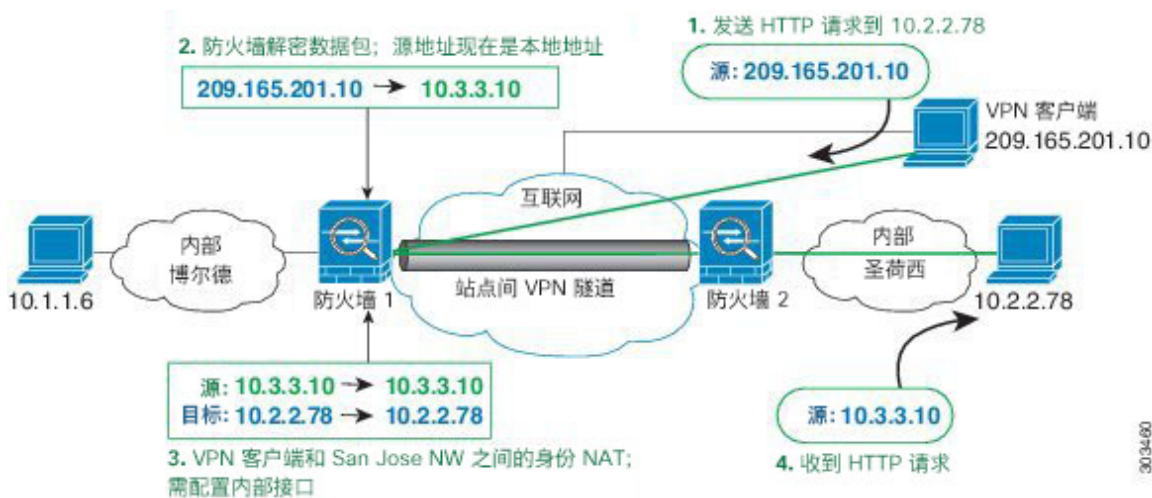
的 10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份 NAT 规则来豁免此流量。身份 NAT 只能将地址转换为其相同的地址。

图 42: 用于站点间 VPN 的接口 PAT 和身份 NAT



下图显示连接到 Firewall1（博尔德）的 VPN 客户端以及对通过 Firewall1 与 Firewall2（圣荷西）之间的站点到站点隧道可访问的服务器（10.2.2.78）的 Telnet 请求。因为这是一种发夹连接，所以您需要启用接口内通信，这也是来自 VPN 客户端的非拆分隧道互联网绑定流量所必需的。还需要在 VPN 客户端以及博尔德和圣荷西网络之间配置身份 NAT，就像在 VPN 连接的任何网络之间一样配置，使此流量免于应用出站 NAT 规则。

图 43: VPN 客户端访问站点到站点 VPN



对于第二个示例，请参阅以下针对 Firewall1（博尔德）的 NAT 配置示例：

```

! Enable hairpin for VPN client traffic:
same-security-traffic permit intra-interface

! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside Boulder network, & perform object interface PAT when going to Internet:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside San Jose network for use in twice NAT rule:
object network sanjose_inside
subnet 10.2.2.0 255.255.255.0

! Use twice NAT to pass traffic between the Boulder network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static vpn_local vpn_local

! Use twice NAT to pass traffic between the Boulder network and San Jose without
! address translation (identity NAT):
nat (inside,outside) source static boulder_inside boulder_inside
destination static sanjose_inside sanjose_inside

! Use twice NAT to pass traffic between the VPN client and San Jose without
! address translation (identity NAT):
nat (outside,outside) source static vpn_local vpn_local
destination static sanjose_inside sanjose_inside

```

请参阅以下针对 Firewall2（圣荷西）的 NAT 配置示例：

```

! Identify inside San Jose network, & perform object interface PAT when going to Internet:
object network sanjose_inside
subnet 10.2.2.0 255.255.255.0
nat (inside,outside) dynamic interface

! Identify inside Boulder network for use in twice NAT rule:
object network boulder_inside
subnet 10.1.1.0 255.255.255.0

! Identify local VPN network for use in twice NAT rule:
object network vpn_local
subnet 10.3.3.0 255.255.255.0

! Use twice NAT to pass traffic between the San Jose network and Boulder without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static boulder_inside boulder_inside

! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static vpn_local vpn_local

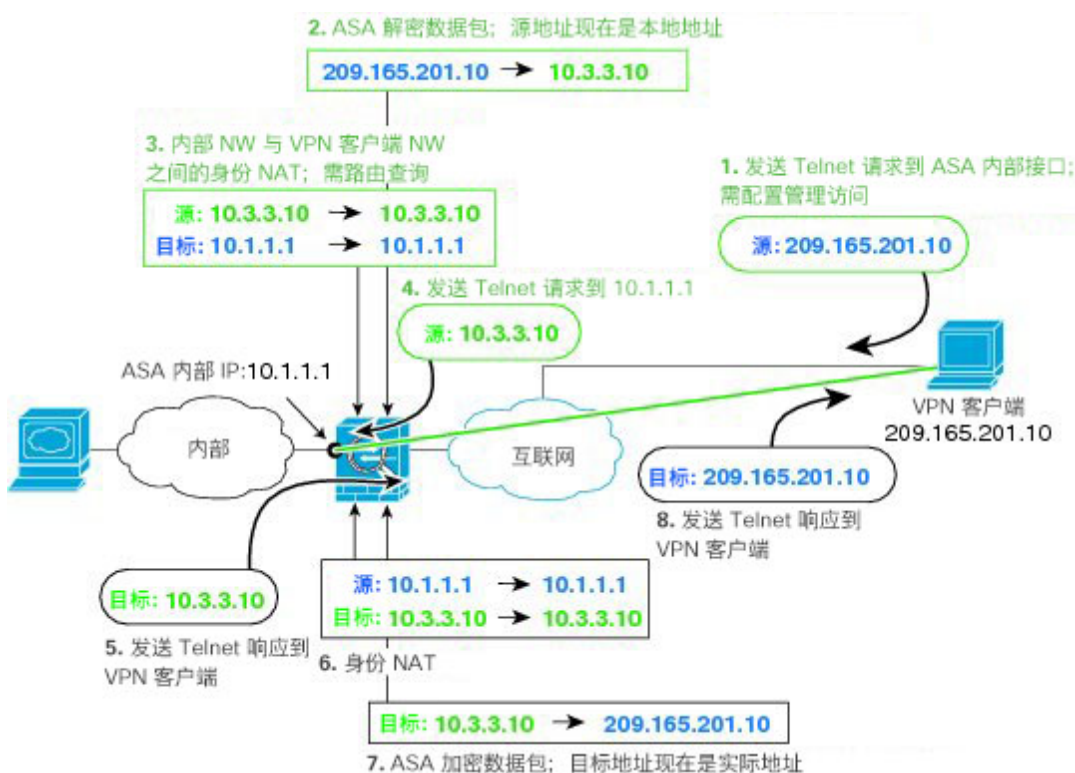
```

NAT 和 VPN 管理访问

使用 VPN 时，可允许管理访问连接到与您进入 ASA 所用接口不同的接口。例如，如果您从外部接口进入 ASA，则管理访问功能允许您使用 ASDM、SSH、Telnet 或 SNMP 连接到内部接口；或者可以 ping 连接内部接口。

下图显示使用 Telnet 连接到 ASA 内部接口的 VPN 客户端。当使用管理访问接口，并且根据 [NAT 和远程访问 VPN](#)，第 264 页或 [NAT 和站点到站点 VPN](#)，第 265 页配置身份 NAT 时，必须为 NAT 配置路由查询选项。如果未配置路由查询，ASA 会将流量传出 NAT 命令中指定的接口，不考虑路由表规则；在以下示例中，出口接口为内部接口。您不希望 ASA 将管理流量发送到内部网络，否则它们将再不会回到内部接口 IP 地址。路由查询选项允许 ASA 将流量直接发送到内部接口 IP 地址，而不是流入内部网络。对于从 VPN 客户端到内部网络上的主机的流量，路由查询选项仍将导致正确的出口接口（内部），因此，正常业务流不会受到影响。有关路由查询选项的详细信息，请参阅 [确定出口接口](#)，第 263 页。

图 44: VPN 管理访问



请参阅以下用于上述网络的 NAT 配置示例：

```
! Enable hairpin for non-split-tunneled VPN client traffic:
same-security-traffic permit intra-interface
```

```
! Enable management access on inside ifc:
management-access inside
```

```
! Identify local VPN network, & perform object interface PAT when going to Internet:
object network vpn_local
```

```
subnet 10.3.3.0 255.255.255.0
nat (outside,outside) dynamic interface

! Identify inside network, & perform object interface PAT when going to Internet:
object network inside_nw
subnet 10.1.1.0 255.255.255.0
nat (inside,outside) dynamic interface

! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT), w/route-lookup:
nat (outside,inside) source static vpn_local vpn_local
destination static inside_nw inside_nw route-lookup
```

NAT 和 VPN 故障排除

请参阅以下用于排除 VPN 中 NAT 问题的监控工具：

- 数据包跟踪器 - 正确使用时，数据包跟踪器显示数据包命中了哪些 NAT 规则。
- **show nat detail** - 显示给定 NAT 规则的命中数和未转换流量。
- **show conn all** - 让您查看活动连接，包括流向设备的流量和通过设备的流量。

要让自己熟悉非工作配置和工作配置，可以执行以下步骤：

1. 配置无身份 NAT 的 VPN。
2. 输入 **show nat detail** 和 **show conn all**。
3. 添加身份 NAT 配置。
4. 重复 **show nat detail** 和 **show conn all**。

转换 IPv6 网络

当需要在仅 IPv6 网络和仅 IPv4 网络之间传递流量时，需要使用 NAT 在地址类型之间进行转换。即使两个都是 IPv6 网络，您可能也需要对外部网络隐藏内部地址。

对于 IPv6 网络，您可以使用以下转换类型：

- NAT64、NAT46 - 将 IPv6 数据包转换成 IPv4 数据包，反之亦然。您需要定义两个策略，一个用于 IPv6 向 IPv4 的转换，另一个用于 IPv4 向 IPv6 的转换。虽然您可以使用单一两次 NAT 规则完成此任务，但如果 DNS 服务器位于外部网络，则可能需要重写 DNS 响应。由于在指定了目标的情况下，无法在两次 NAT 规则中启用 DNS 重写，所以最好创建两个网络对象 NAT 规则。



注释 NAT46 仅支持静态映射。

- NAT66 - 将 IPv6 数据包转换为不同的 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。



注释 NAT64 和 NAT 46 仅可以在标准路由接口上使用。NAT66 可在路由接口和桥接组成员接口上使用。

NAT64/46: 将 IPv6 地址转换为 IPv4 地址

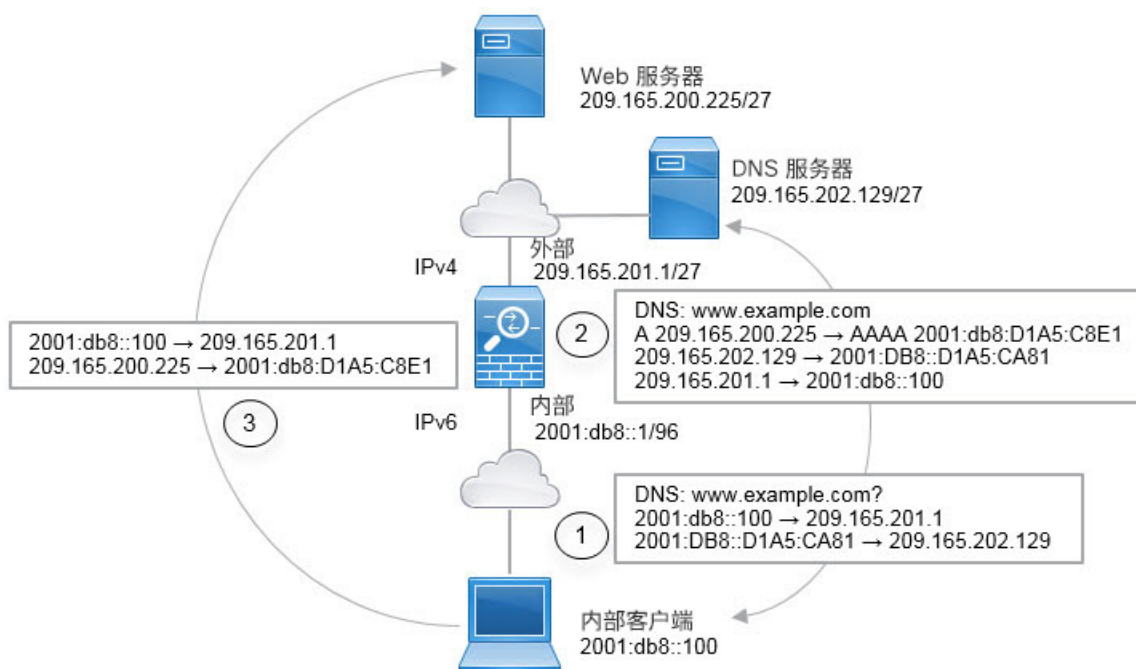
当流量从 IPv6 网络进入仅 IPv4 网络时，您需要将 IPv6 地址转换为 IPv4 地址，并将流量从 IPv4 返回 IPv6。您需要定义两个地址池，一个 IPv4 地址池用于绑定 IPv4 网络中的 IPv6 地址，另一个 IPv6 地址池用于绑定 IPv6 网络中的 IPv4 地址。

- NAT64 规则的 IPv4 地址池一般较小，通常可能没有足够的地址与 IPv6 客户端地址一对一映射。与动态或静态 NAT 相比，动态 PAT 可以更容易满足可能的大量 IPv6 客户端地址需要。
- NAT46 规则的 IPv6 地址池可以等于或大于要映射的 IPv4 地址数。这允许每个 IPv4 地址映射到不同的 IPv6 地址。NAT46 仅支持静态映射，因此您不能使用动态 PAT。

您需要定义两个策略，一个用于源 IPv6 网络，一个用于目的地 IPv4 网络。虽然您可以使用单一两次 NAT 规则完成此任务，但如果 DNS 服务器位于外部网络，则可能需要重写 DNS 响应。由于在指定了目标的情况下，无法在两次 NAT 规则中启用 DNS 重写，所以最好创建两个网络对象 NAT 规则。

NAT64/46 示例: 内部 IPv6 网络与外部 IPv4 互联网

下面是一个典型的示例：内部网络只支持 IPv6 但外部互联网上有一些内部用户所需的服务只支持 IPv4。



在本例中，借助外部接口的 IP 地址，使用动态接口 PAT 将内部 IPv6 网络转换为 IPv4。将外部 IPv4 流量静态转换为 2001:db8::/96 网络中的地址，允许在内部网络中传输。对 NAT46 规则启用 DNS 重写，使外部 DNS 服务器的回复可以从 A (IPv4) 记录转换为 AAAA (IPv6) 记录，地址也能从 IPv4 地址转换为 IPv6 地址。

当内部 IPv6 网络中地址为 2001:DB8::100 的客户端尝试打开 www.example.com 时，此 Web 请求的典型顺序如下。

1. 客户端的计算机向地址为 2001:DB8::D1A5:CA81 的 DNS 服务器发送 DNS 请求。NAT 规则对 DNS 请求中的源和目的进行以下转换：
 - 2001:DB8::100 转换为 209.165.201.1 上的唯一端口（NAT64 接口 PAT 规则。）
 - 2001:DB8::D1A5:CA81 转换为 209.165.202.129（NAT46 规则。） D1A5:CA81 是 209.165.202.129 的 IPv6 对应物。）
2. DNS 服务器以 A 记录进行响应，指出 www.example.com 位于 209.165.200.225。NAT46 规则（已启用 DNS 重写）将 A 记录转换为 IPv6 对应物 AAAA 记录，并在 AAAA 记录中将 209.165.200.225 转换为 2001:db8:D1A5:C8E1。此外，DNS 响应中的源地址和目标地址未转换：
 - 209.165.202.129 转换为 2001:DB8::D1A5:CA81
 - 209.165.201.1 转换为 2001:db8::100
3. IPv6 客户端现在有 Web 服务器的 IP 地址，于是向位于 2001:db8:D1A5:C8E1 的 www.example.com 发出 HTTP 请求。（D1A5:C8E1 是 209.165.200.225 的 IPv6 对应物。）HTTP 请求中的源和目的如下转换：
 - 2001:DB8::100 转换为 209.156.101.54 上的唯一端口（NAT64 接口 PAT 规则。）
 - 2001:db8:D1A5:C8E1 转换为 209.165.200.225（NAT46 规则。）

以下步骤程序介绍了如何配置此示例。

过程

步骤 1 依次选择 **Configuration > Firewall > NAT Rules**。

步骤 2 为内部 IPv6 网络配置 NAT64 动态 PAT 规则。

a) 依次选择 **Add > Network Object NAT Rule**。

b) 配置基本对象属性：

- **Name** - 例如 **inside_v6**。
- **Type** - 选择 **Network**。
- **IP Version** - 选择 **IPv6**。
- **IP Address** - 输入 **2001:db8::**。
- **Prefix Length** - 输入 **96**。

- c) 对于 NAT 类型，选择 **Dynamic** 或 **Dynamic PAT (Hide)**。
- d) 对于 **Translated Address**，点击浏览按钮并选择“outside”接口。

- e) 点击 **Advanced** 按钮，并配置以下选项：
 - **Source Interface** - 选择“inside”。
 - **Destination Interface** - 应已选择“outside”接口。
- f) 点击 **OK** 以保存高级设置。
- g) 点击 **OK** 以添加 NAT 规则。

使用此规则时，从内部接口上的 2001:db8::/96 子网流向外部接口的任何流量都将接受使用外部接口 IPv4 地址进行的 NAT64 PAT 转换。

步骤 3 为外部 IPv4 网络配置静态 NAT46 规则。

- a) 依次选择 **Add > Network Object NAT Rule**。
- b) 配置基本对象属性：
 - **Name** - 例如 **outside_v4_any**。
 - **Type** - 选择 **Network**。
 - **IP Version** - 选择 **IPv4**。
 - **IP Address** - 输入 **0.0.0.0**。
 - **Netmask** - 输入 **0.0.0.0**。
- c) 配置 NAT 属性：
 - **NAT Type** - 选择 **Static**。
 - **Translated Address** - 输入 **2001:db8::/96**。

- d) 点击 **Advanced** 按钮，并配置以下选项：
- **Translate DNS Replies for Rule** - 选择此选项。
 - **Source Interface** - 选择“outside”。
 - **Destination Interface** - 选择“inside”。

- e) 点击 **OK** 以保存高级设置。
f) 点击 **OK** 以添加 NAT 规则。

使用此规则时，外部网络中的任何 IPv4 地址到达内部接口，都将使用嵌入式 IPv4 地址方法转换为 2001:db8::/96 网络中的一个地址。此外，DNS 响应从 A (IPv4) 记录转换为 AAAA (IPv6) 记录，其地址也从 IPv4 地址转换为 IPv6 地址。

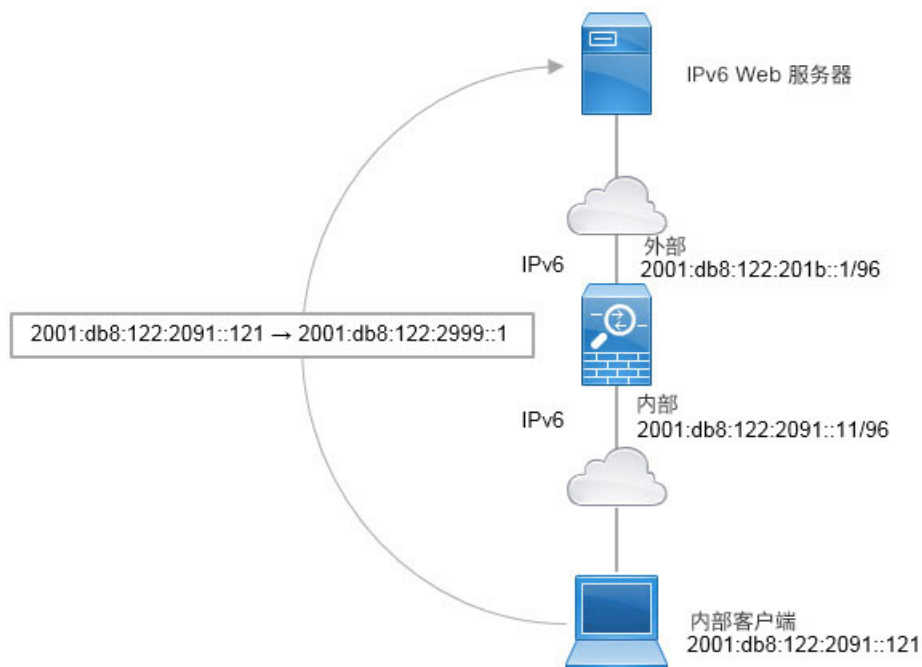
NAT66: 将 IPv6 地址转换为不同的 IPv6 地址

当从一个 IPv6 网络进入另一个 IPv6 网络时，您可以将地址转换为外部网络上的不同 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。

因为您不是在不同的地址类型之间转换，所以您需要一个单一的 NAT66 转换规则。使用网络对象 NAT 可轻松地对这些规则建模。但是，如果不想允许返回流量，您可以仅使用两次 NAT 将静态 NAT 规则设为单向。

NAT66 示例：网络间的静态转换

您可以使用网络对象 NAT 在 IPv6 地址池之间配置静态转换。以下示例说明如何将 2001:db8:122:2091::/96 网络中的内部地址转换为 2001:db8:122:2999::/96 网络中的外部地址。



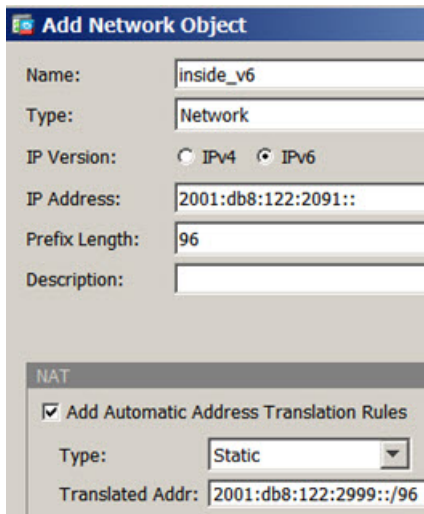
过程

步骤 1 依次选择 **Configuration > Firewall > NAT Rules**。

步骤 2 为内部 IPv6 网络配置静态 NAT 规则。

- a) 依次选择 **Add > Network Object NAT Rule**。
- b) 配置基本对象属性：
 - **Name** - 例如 **inside_v6**。
 - **Type** - 选择 **Network**。
 - **IP Version** - 选择 **IPv6**。
 - **IP Address** - 输入 **2001:db8:122:2091::**。
 - **Prefix Length** - 输入 **96**。
- c) 对于 NAT 类型选择 **Static**。

- d) 对于 **Translated Address**，输入 **2001:db8:122:2999::/96**。



- e) 点击 **Advanced** 按钮，并配置以下选项：
- **Source Interface** - 选择 “inside” 。
 - **Destination Interface** - 选择 “outside” 。

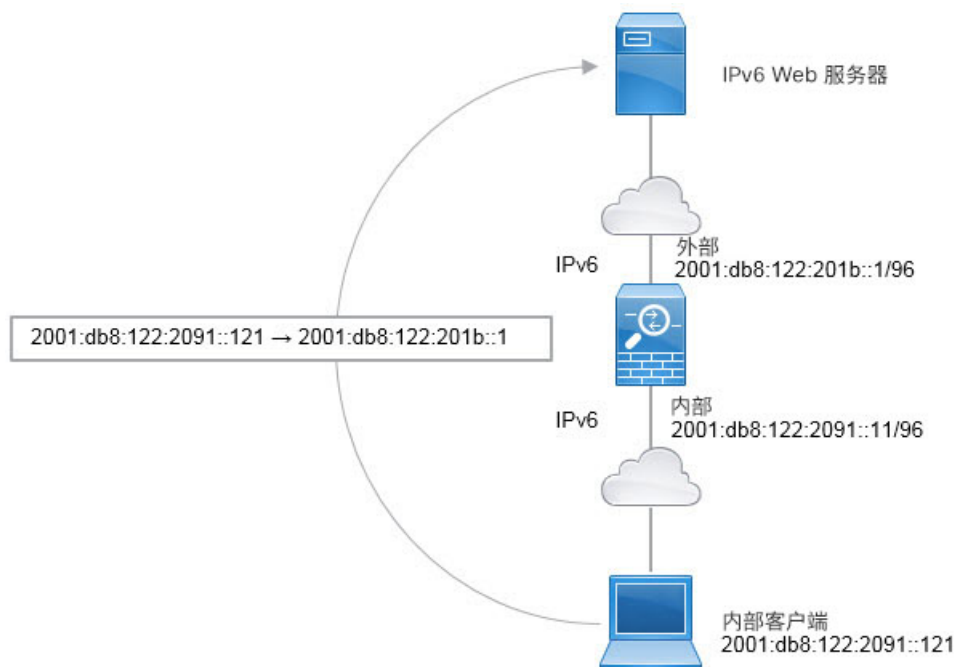
- f) 点击 **OK** 以保存高级设置。
g) 点击 **OK** 以添加 NAT 规则。

使用此规则，从内部接口上的 2001:db8:122:2091::/96 子网到外部接口的任何流量都会经静态 NAT66 转换为 2001:db8:122:2999::/96 网络上的地址。

NAT66 示例：简单 IPv6 接口 PAT

实施 NAT66 的一个简单方法是将内部地址动态分配给外部接口 IPv6 地址上的不同端口。

为 NAT66 配置接口 PAT 规则时，该接口上配置的所有全局地址均用于 PAT 映射。该接口的链路本地地址或站点本地地址不用于 PAT。

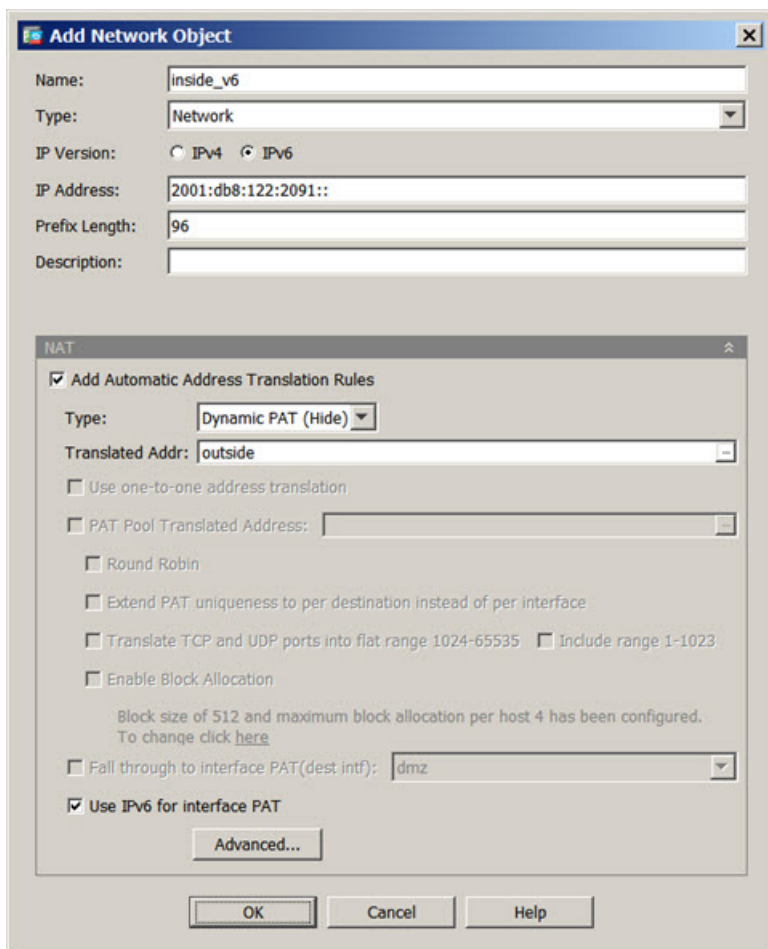


过程

步骤 1 依次选择 **Configuration > Firewall > NAT Rules**。

步骤 2 为内部 IPv6 网络配置动态 PAT 规则。

- a) 依次选择 **Add > Network Object NAT Rule**。
- b) 配置基本对象属性：
 - **Name** - 例如 `inside_v6`。
 - **Type** - 选择 **Network**。
 - **IP Version** - 选择 **IPv6**。
 - **IP Address** - 输入 `2001:db8:122:2091::`。
 - **Prefix Length** - 输入 `96`。
- c) 对于 NAT 类型，选择 **Dynamic** 或 **Dynamic PAT (Hide)**。
- d) 对于 **Translated Address**，点击浏览按钮并选择“outside”接口。
- e) 选择 **Use IPv6 for Interface PAT** 选项。



f) 点击 **Advanced** 按钮，并配置以下选项：

- **Source Interface** - 选择“inside”。
- **Destination Interface** - 应已选择“outside”接口。

g) 点击 **OK** 以保存高级设置。

h) 点击 **OK** 以添加 NAT 规则。

使用此规则，从内部接口的 2001:db8:122:2091::/96 子网到外部接口的任何流量均会通过 NAT66 PAT 转换为为外部接口配置的 IPv6 全局地址之一。

使用 NAT 重写 DNS 查询和响应

可能需要配置 ASA 以修改 DNS 应答，方法是用匹配 NAT 配置的地址替换应答中的地址。配置每条转换规则时，可以配置 DNS 修改。DNS 修改也称为“DNS Doctoring”。

此功能可以重写匹配 NAT 规则的 DNS 查询和应答中的地址（例如，适用于 IPv4 的 A 记录；适用于 IPv6 的 AAAA 记录；或者，适用于逆向 DNS 查询的 PTR 记录）。对于从映射接口穿越到任何其他接口的 DNS 应答，记录会从映射值被重写为实际值。相反，对于从任何接口穿越到映射接口的 DNS 应答，记录会从实际值被重写为映射值。

以下是需要在 NAT 规则上配置 DNS 重写的几种主要情况。

- 规则为 NAT64 或 NAT46，并且 DNS 服务器位于外部网络上。您需要进行 DNS 重写以实现 DNS A 记录（适用于 IPv4）和 AAAA 记录（适用于 IPv6）之间的转换。
- DNS 服务器在外部，客户端在内部，并且客户端使用的一些完全限定域名解析到其他内部主机。
- DNS 服务器在内部并以专用 IP 地址进行响应，客户端在外部，并且客户端访问指向内部托管的服务器的完全限定域名。

DNS 重写限制

以下是 DNS 重写的某些限制：

- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 或 AAAA 记录，而要使用的 PAT 规则不确定。
- 如果您配置了两次 NAT 规则，当指定了目的地址和源地址时，不能配置 DNS 修改。当流向 A 与 B 时，这类规则可能会有单个地址的不同转换。因此，ASA 将精确匹配 DNS 应答中的 IP 地址与正确的两次 NAT 规则相匹配；DNS 应答不包含有关哪个源地址/目标地址组合位于提示 DNS 请求的数据包中的信息。
- 要重写 DNS 查询和响应，您必须启用针对 NAT 规则启用了 DNS NAT 重写的 DNS 应用检查。默认情况下，启用了 DNS NAT 重写的 DNS 检查会全局应用，因此可能无需更改检查配置。
- 实际上，DNS 重写在 xlate 条目而非 NAT 规则上完成。因此，如果没有面向动态规则的 xlate，则不能正确完成重写。静态 NAT 也会出现相同的问题。
- DNS 重写不会重写 DNS 动态更新消息（操作码为 5）。

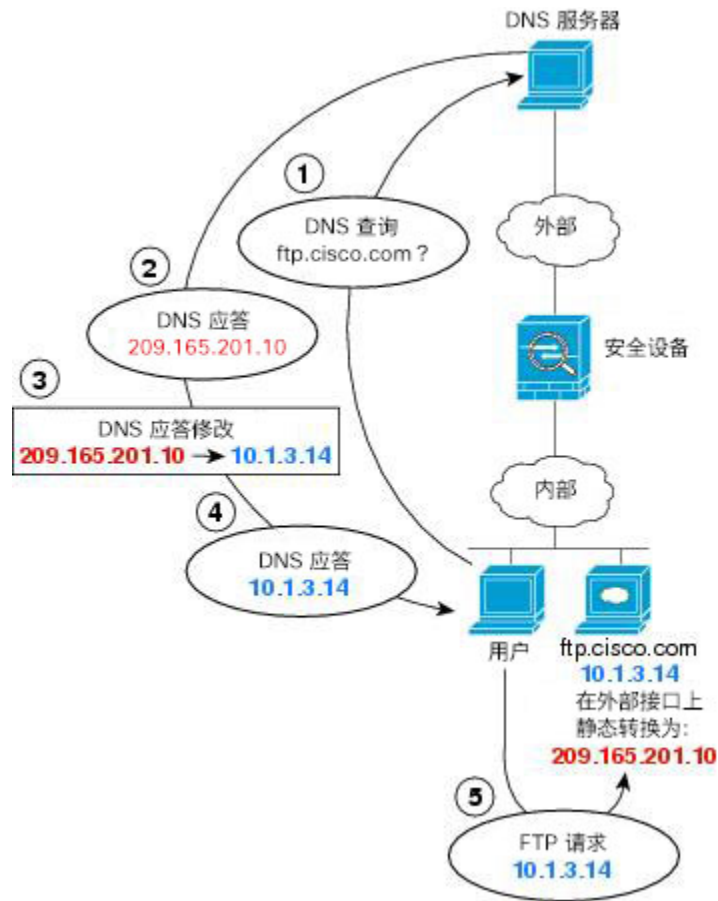
以下主题提供了 NAT 规则中 DNS 重写的示例。

DNS 应答修改，外部接口上的 DNS 服务器

下图显示可从外部接口访问的 DNS 服务器。服务器 ftp.cisco.com 在内部接口上。将 NAT 配置为将 ftp.cisco.com 实际地址 (10.1.3.14) 静态转换为在外部网络上可见的映射地址 (209.165.201.10)。

在这种情况下，您要在此静态规则上启用 DNS 回复修改，以便使用实际地址访问 ftp.cisco.com 的内部用户可以接收来自 DNS 服务器的实际地址，而不是映射地址。

当内部主机发送对 ftp.cisco.com 的地址的 DNS 请求时，DNS 服务器将以映射地址 (209.165.201.10) 作为回复。系统引用内部服务器的静态规则，并将 DNS 回复中的地址转换为 10.1.3.14。如果不启用 DNS 应答修改，则内部主机尝试将流量发送到 209.165.201.10，而不是直接访问 ftp.cisco.com。



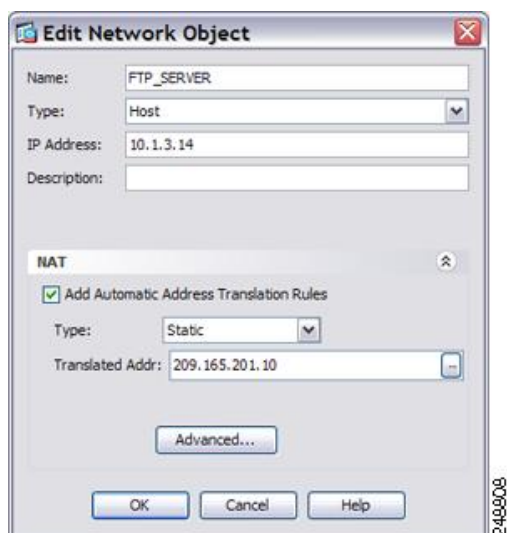
130021

过程

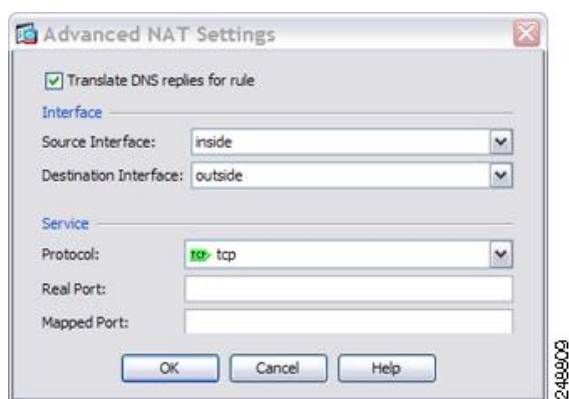
步骤 1 依次选择配置 > 防火墙 > NAT。

步骤 2 依次选择添加 > 网络对象 NAT 规则。

步骤 3 为新网络对象命名，定义 FTP 服务器地址，启用静态 NAT，并输入转换地址。



步骤 4 点击 **Advanced** 并配置实际接口和映射接口以及 DNS 修改。



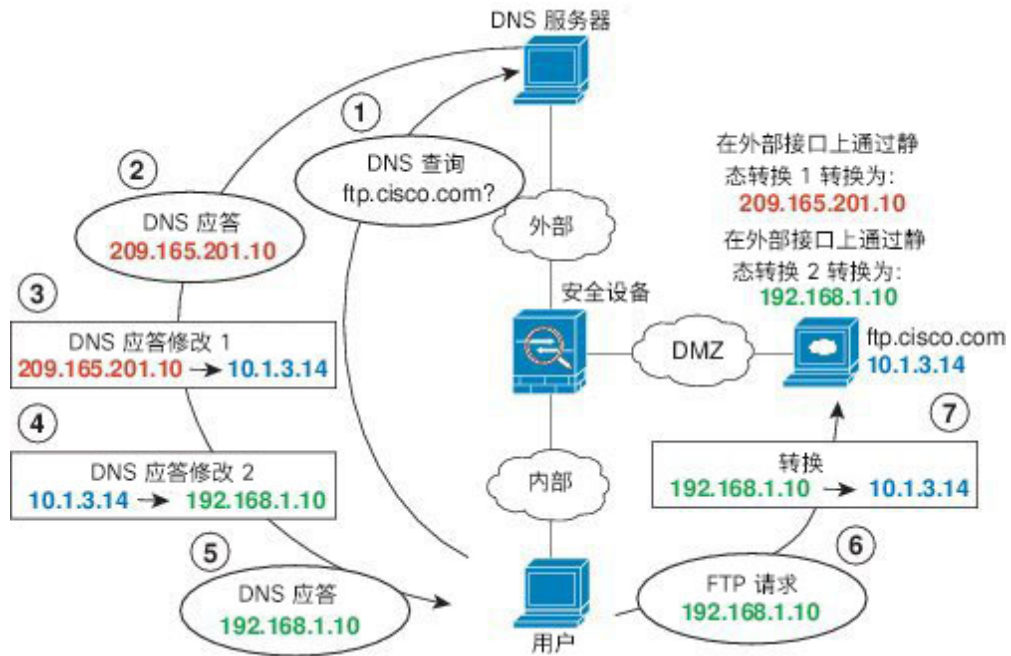
步骤 5 点击 **OK** 返回到 Edit Network Object 对话框，再次点击 **OK**，然后点击 **Apply**。

独立网络上的 DNS 应答修改、DNS 服务器、主机和服务

下图显示一个内部网络的用户正在从外部 DNS 服务器请求 DMZ 网络上的 ftp.cisco.com 的 IP 地址。DNS 服务器根据外部网络和 DMZ 网络之间的静态规则，以映射地址 (209.165.201.10) 作为应答，即使该用户不在 DMZ 网络中。ASA 将 DNS 应答内的地址转换为 10.1.3.14。

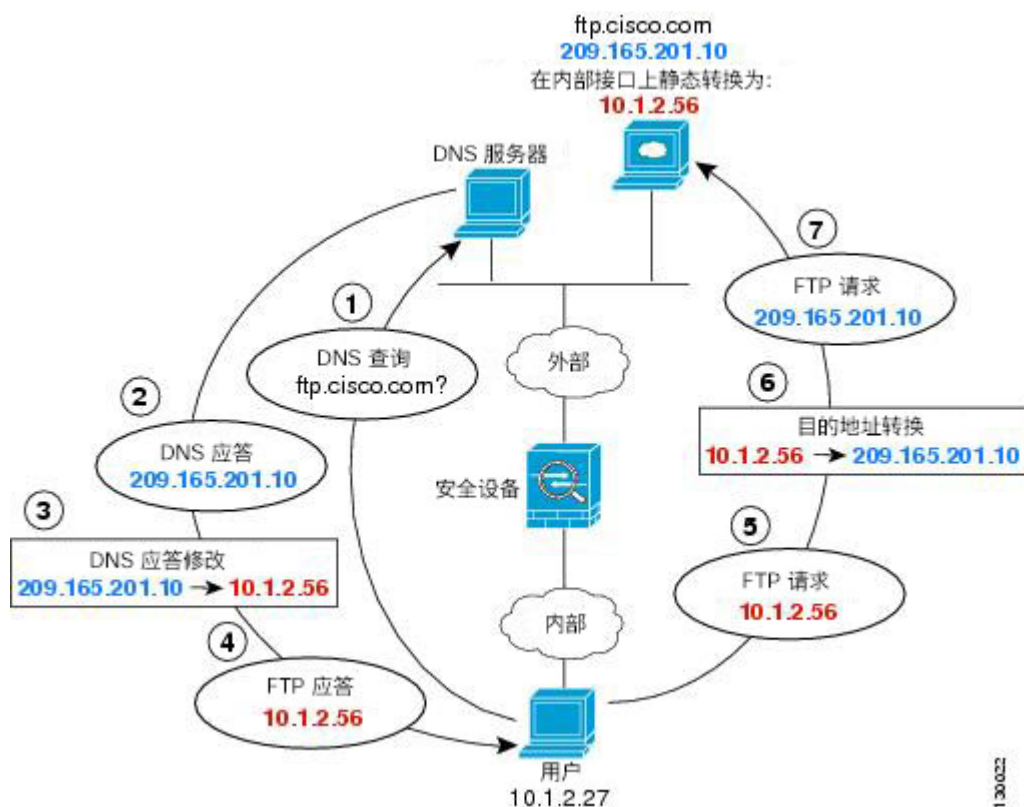
如果用户需要使用实际地址访问 ftp.cisco.com，则无需更多配置。如果内部网络和 DMZ 网络之间也有静态规则，还需要在此规则上启用 DNS 应答修改。然后，修改 DNS 应答两次。这种情况下，ASA 会根据内部和 DMZ 之间的静态规则将 DNS 应答内的地址重新转换为 192.168.1.10。

图 45: 独立网络上的 DNS 应答修改、DNS 服务器、主机和服务器



DNS 应答修改，主机网络上的 DNS 服务器

下图显示外部网络上的 FTP 服务器和 DNS 服务器。系统有面向外部服务器的静态转换。在这种情况下，当内部用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.20.10 作为响应。由于您希望内部用户使用 ftp.cisco.com 的映射地址 (10.1.2.56)，因此需要配置 DNS 回复修改以进行静态转换。

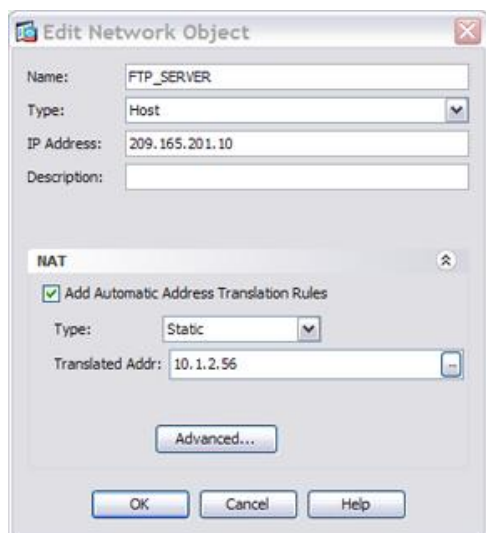


过程

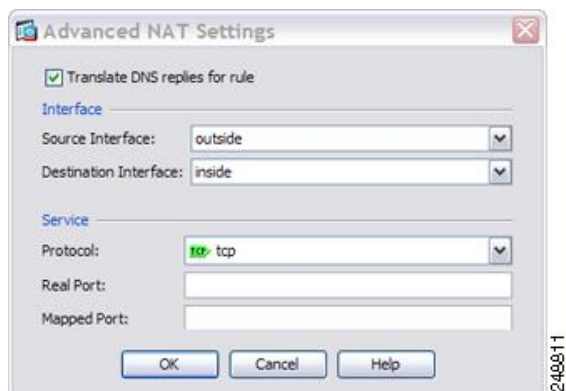
步骤 1 依次选择配置 > 防火墙 > NAT。

步骤 2 依次选择添加 > 网络对象 NAT 规则。

步骤 3 为新网络对象命名，定义 FTP 服务器地址，启用静态 NAT，并输入转换地址。



步骤 4 点击 **Advanced** 并配置实际接口和映射接口以及 DNS 修改。

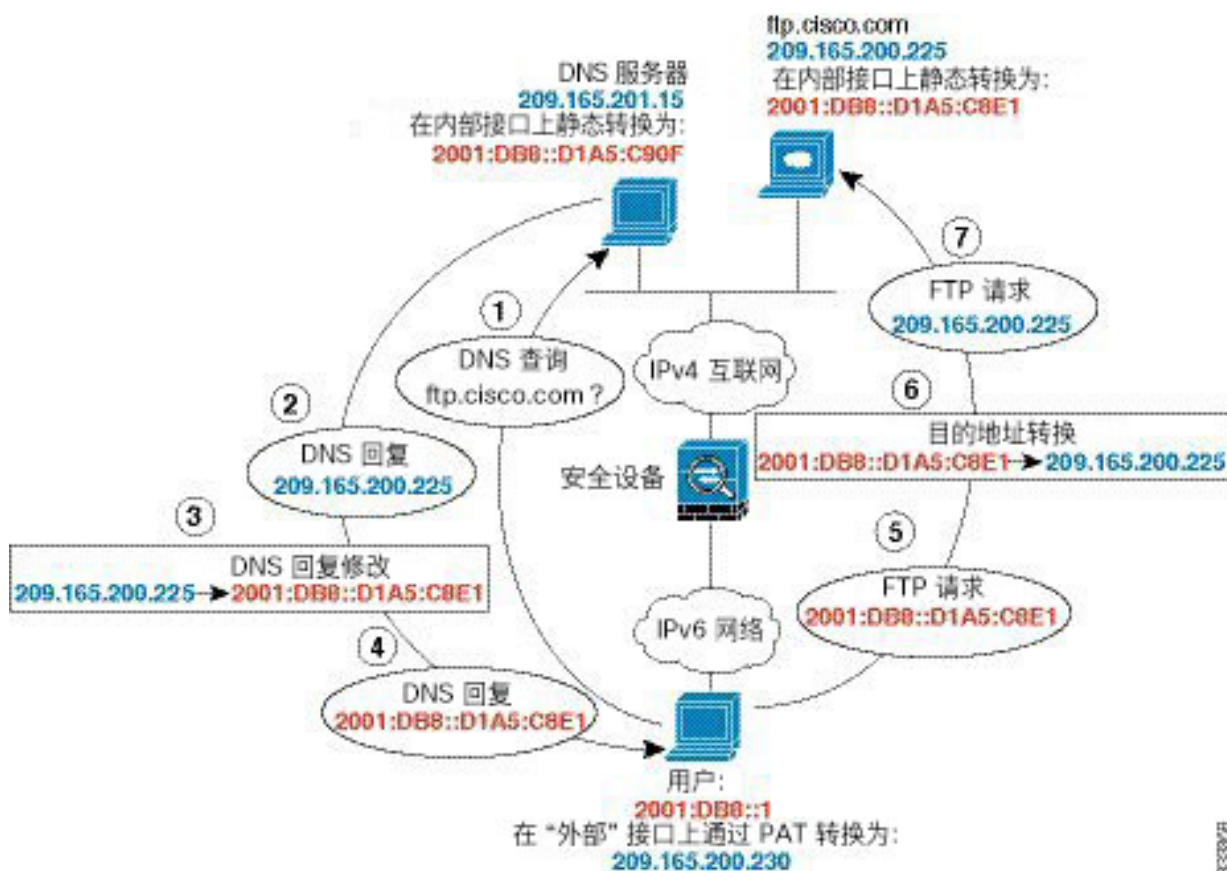


步骤 5 点击 **OK** 返回到 Edit Network Object 对话框，再次点击 **OK**，然后点击 **Apply**。

DNS64 应答修改

下图显示外部 IPv4 网络上的 FTP 服务器和 DNS 服务器。系统有面向外部服务器的静态转换。在这种情况下，当内部 IPv6 用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.200.225 作为响应。

由于您希望内部用户使用 ftp.cisco.com 的映射地址（2001:DB8::D1A5:C8E1，其中 D1A5:C8E1 是 209.165.200.225 的 IPv6 对应物），因此需要配置 DNS 回复修改以进行静态转换。本示例还包括面向 DNS 服务器的静态 NAT 转换和面向内部 IPv6 主机的 PAT 规则。

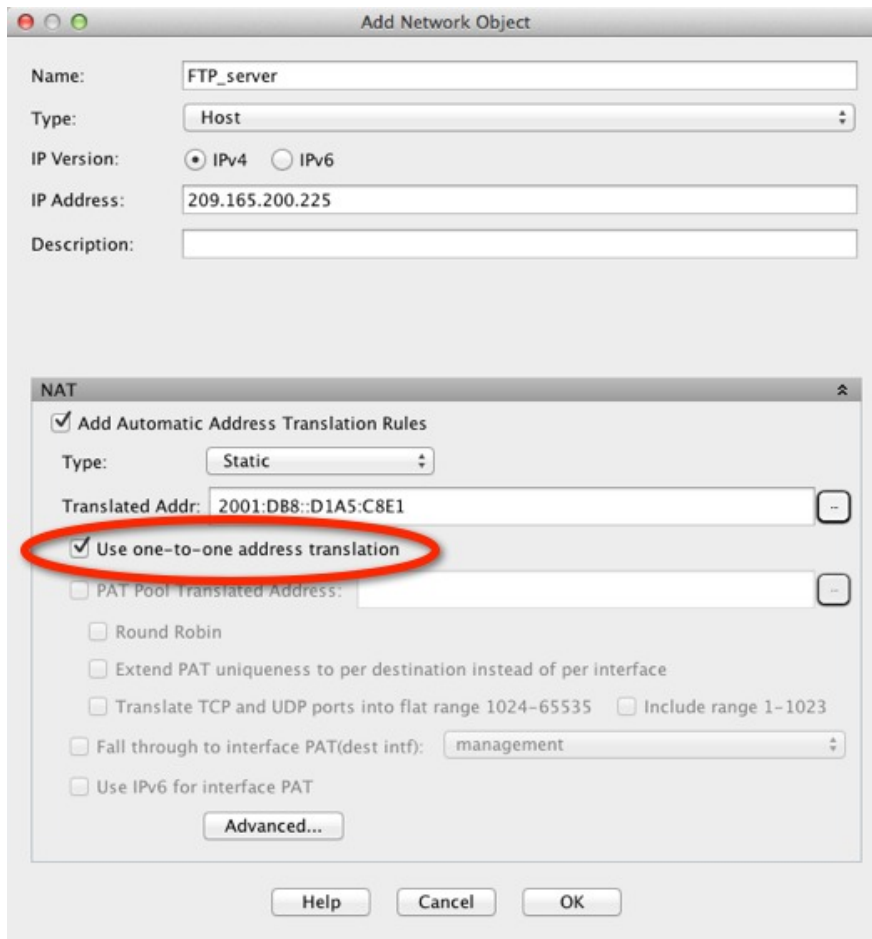


过程

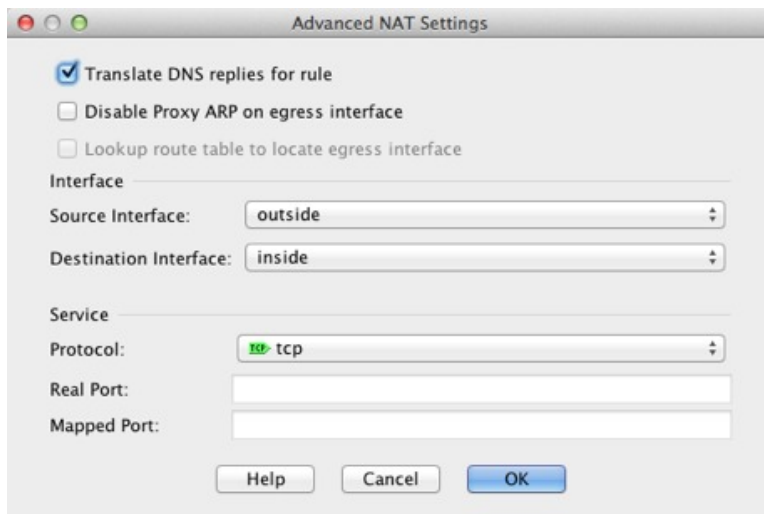
步骤 1 依次选择配置 > 防火墙 > NAT。

步骤 2 为 FTP 服务器配置支持 DNS 修改的静态网络对象 NAT。

- 依次选择 **Add > Network Object NAT Rule**。
- 为新网络对象命名，定义 FTP 服务器地址，启用静态 NAT，并输入转换地址。由于这是 NAT46 的一对一转换，请选择 **Use one-to-one address translation**。



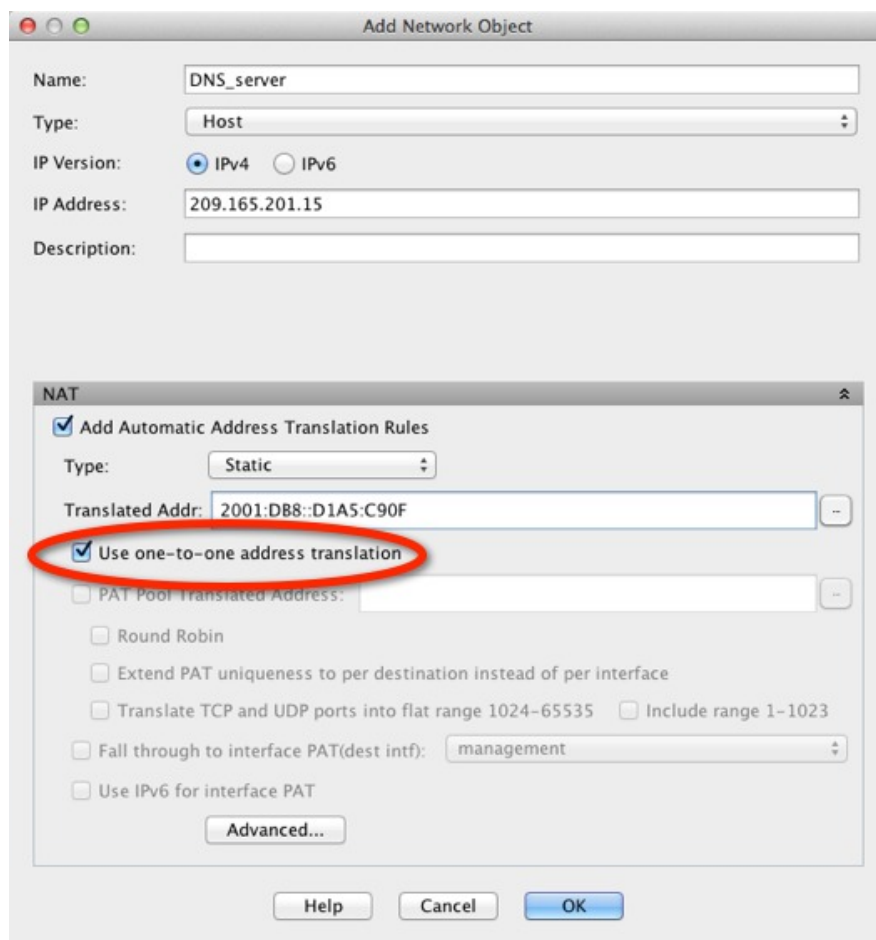
c) 点击 **Advanced** 配置实际接口和映射接口以及 DNS 修改。



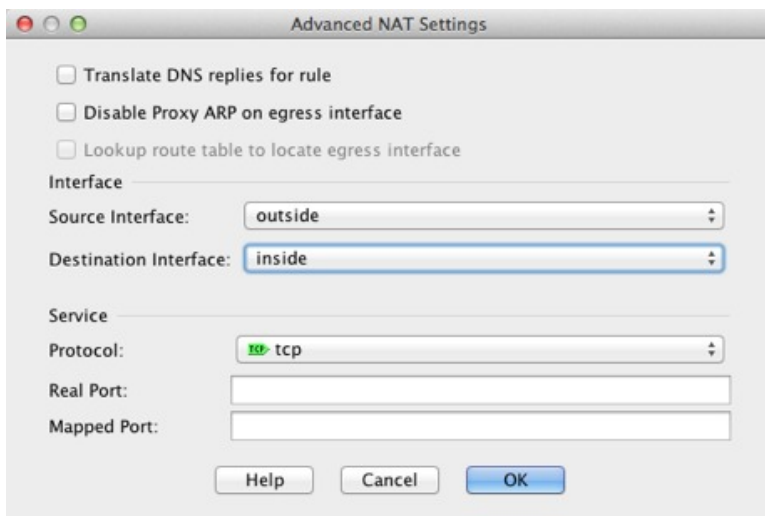
d) 点击 **OK** 返回到 Network Object 对话框，然后再次点击 **OK** 以保存规则。

步骤 3 为 DNS 服务器配置静态网络对象 NAT。

- a) 依次选择 **Add > Network Object NAT Rule**。
- b) 为新网络对象命名，定义 DNS 服务器地址，启用静态 NAT，并输入转换地址。由于这是 NAT46 的一对一转换，请选择 **Use one-to-one address translation**。



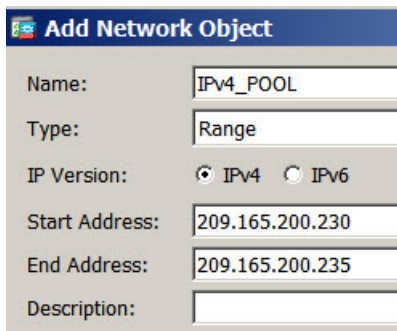
- c) 点击 **Advanced** 配置实际接口和映射接口。



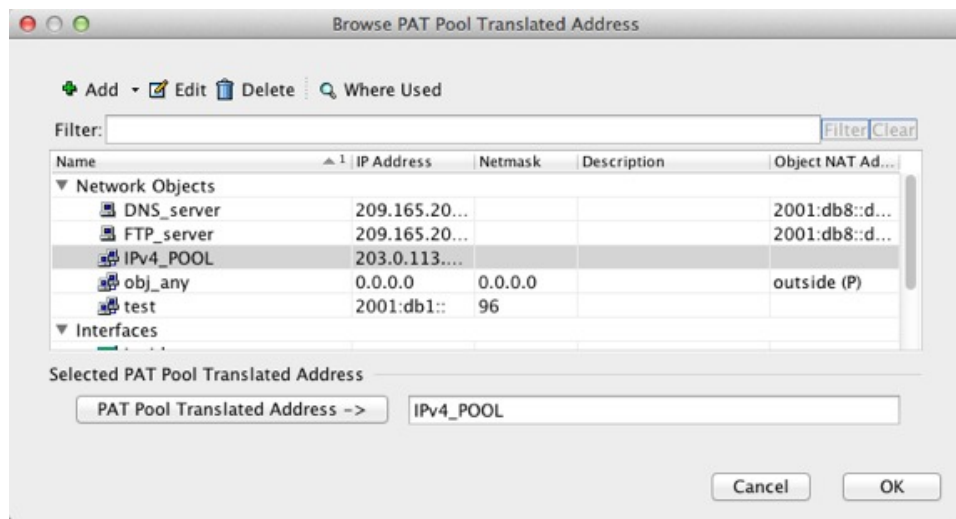
d) 点击 **OK** 返回到 Network Object 对话框，然后再次点击 **OK** 以保存规则。

步骤 4 为内部 IPv6 网络配置 PAT。

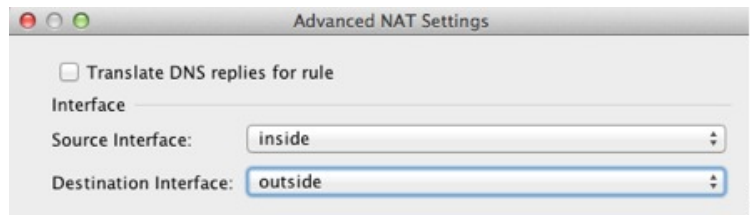
- a) 依次选择 **Add > Network Object NAT Rule**。
- b) 为新网络对象命名，定义 IPv6 网络地址，并选择 **Dynamic NAT**。
- c) 选择 **PAT Pool Translated Address**，然后点击 ...（浏览）按钮以创建 PAT 池对象。
- d) 在 Browse PAT Pool Translated Address 对话框中，依次选择 **Add > Network Object**。为新对象命名，输入 PAT 池的地址范围，然后点击 **OK**。



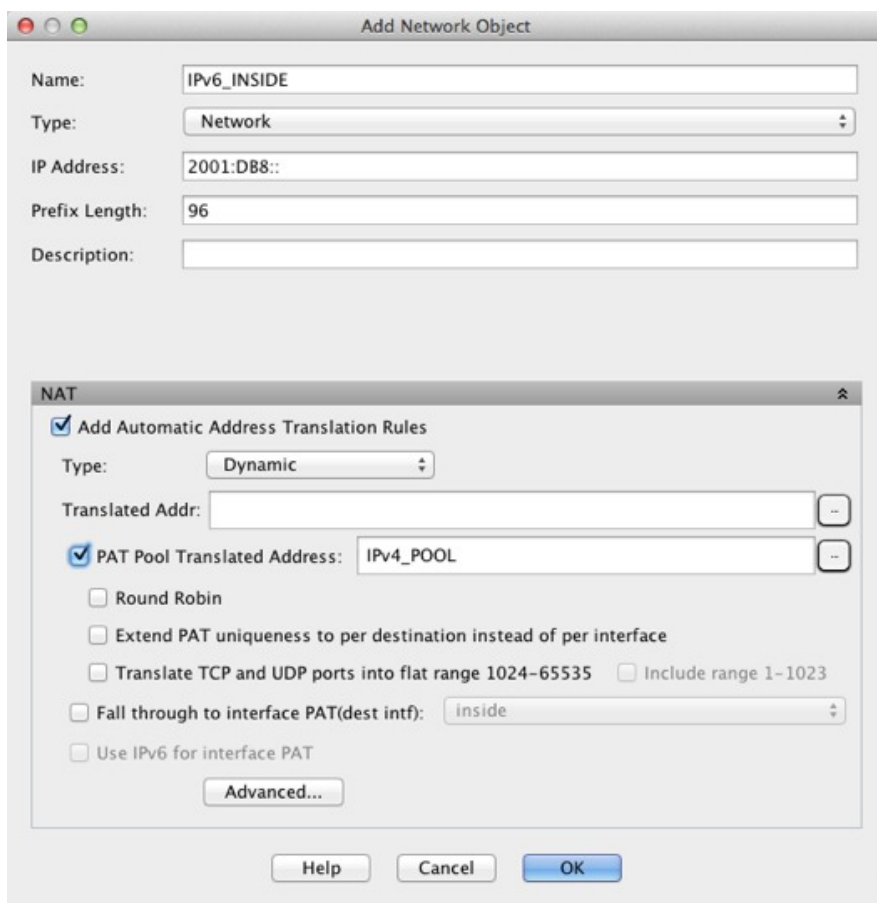
e) 在 Browse PAT Pool Translated Address 对话框中，双击所创建的 PAT 池对象将其选中，然后点击 **OK**。



f) 点击 **Advanced** 配置实际接口和映射接口。



g) 点击 **OK** 返回到 Network Object 对话框。

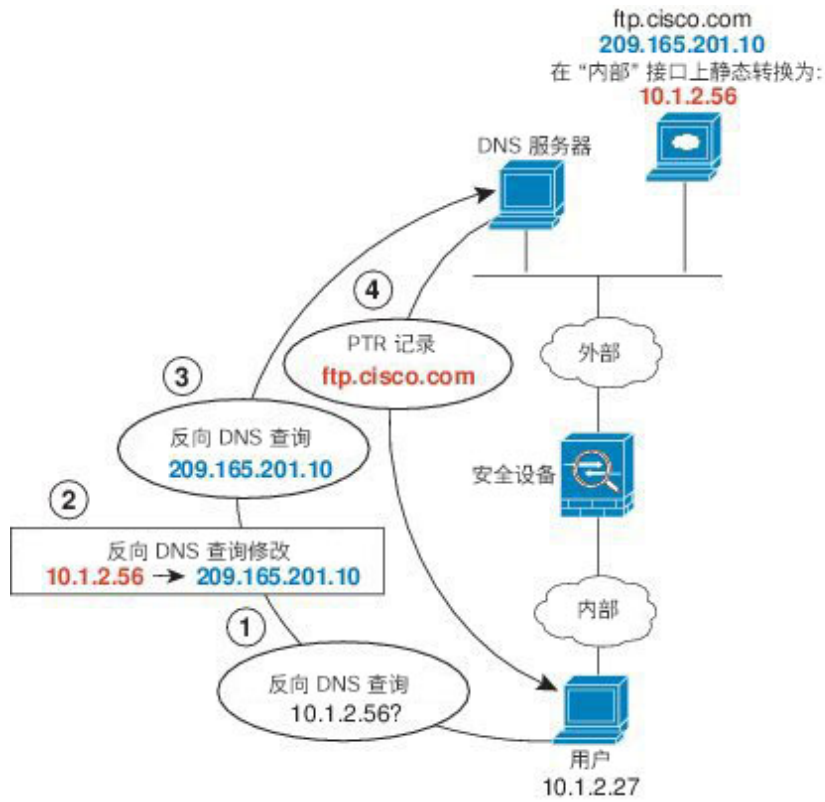


步骤 5 点击 **OK**，然后点击 **Apply**。

PTR 修改，主机网络上的 DNS 服务器

下图显示外部网络上的 FTP 服务器和 DNS 服务器。ASA 包含用于外部服务器的静态转换。在这种情况下，当内部用户为 10.1.2.56 执行逆向 DNS 查询时，ASA 将使用实际地址修改逆向 DNS 查询，而 DNS 服务器将使用服务器名称 ftp.cisco.com 提供响应。

图 46: PTR 修改, 主机网络上的 DNS 服务器





第 **IV** 部分

服务策略和应用检测

- [服务策略](#)，第 293 页
- [应用层协议检测入门](#)，第 309 页
- [基本互联网协议检测](#)，第 327 页
- [语音和视频协议检测](#)，第 359 页
- [移动网络检测](#)，第 379 页



第 13 章

服务策略

服务策略提供一致而灵活的配置 ASA 功能的方式。例如，可以使用服务策略创建特定于某项 TCP 应用而非应用于所有 TCP 应用的超时配置。服务策略由多个应用于某个接口或全局应用的操作或规则组成。

- [关于服务策略，第 293 页](#)
- [服务策略指南，第 299 页](#)
- [服务策略默认设置，第 300 页](#)
- [配置服务策略，第 302 页](#)
- [服务策略的历史，第 308 页](#)

关于服务策略

以下主题介绍服务策略的工作原理。

服务策略的组件

服务策略的关键意义在于，将高级服务应用于允许的流量。任何被访问规则允许的流量都可以应用服务策略，从而接受特殊处理，例如被重定向到服务模块，或者实施应用检测。

提供有以下类型的服务策略：

- 一项应用到所有接口的全局策略。
- 一项应用到单个接口的服务策略。该策略可以通过设备的流量类和在 ASA 接口上定向而非通过的管理流量类的混合。

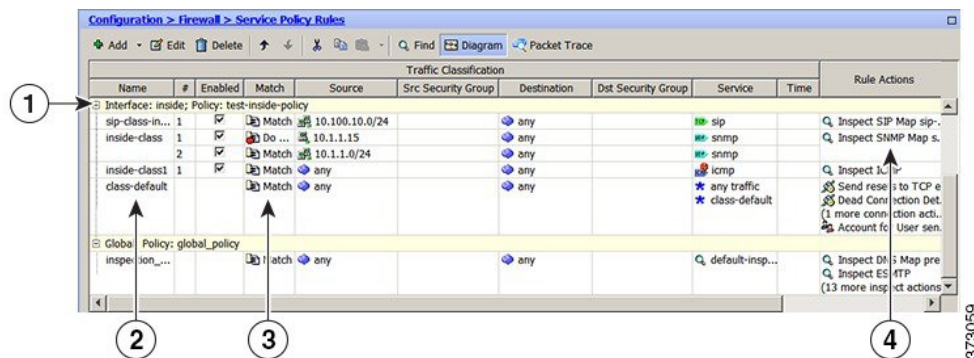
每项服务策略都由以下要素组成：

1. 服务策略映射。这是一组按顺序排列的规则集，根据 **service-policy** 命令命名。在 ASDM 中，策略映射表示为 **Service Policy Rules** 页面上的一个文件夹。
2. 规则。每条规则都是服务策略映射中的 **class** 命令，以及与 **class** 命令相关联的命令。在 ASDM 中，每条规则都显示于不同的行，规则名称为类名称。

class 命令定义匹配规则条件的流量。

与类相关联的命令（例如 **inspect** 和 **set connection timeout**），定义应用于匹配流量的服务和限制。请注意，检测命令可以指向检测策略映射，以此定义应用于被检测流量的操作。请记住，检测策略映射不同于服务策略映射。

以下示例将服务策略在 CLI 中的显示方式与在 ASDM 中的显示方式进行了对比。请注意，图中编号和 CLI 中的行之间没有一对一映射关系。



以下 CLI 由上图中显示的规则生成。

```

: Access lists used in class maps.
: In ASDM, these map to call-out 3, from the Match to the Time fields.
access-list inside_mpc line 1 extended permit tcp 10.100.10.0 255.255.255.0 any eq sip
access-list inside_mpc_1 line 1 extended deny udp host 10.1.1.15 any eq snmp
access-list inside_mpc_1 line 2 extended permit udp 10.1.1.0 255.255.255.0 any eq snmp
access-list inside_mpc_2 line 1 extended permit icmp any any
: SNMP map for SNMP inspection. Denies all but v3.
: In ASDM, this maps to call-out 4, rule actions, for the class-inside policy.
snmp-map snmp-v3only
  deny version 1
  deny version 2
  deny version 2c
: Inspection policy map to define SIP behavior.
: The sip-high inspection policy map must be referred to by an inspect sip command
: in the service policy map.
: In ASDM, this maps to call-out 4, rule actions, for the sip-class-inside policy.
policy-map type inspect sip sip-high
  parameters
    rtp-conformance enforce-payloadtype
    no traffic-non-sip
    software-version action mask log
    uri-non-sip action mask log
    state-checking action drop-connection log
    max-forwards-validation action drop log
    strict-header-validation action drop log
: Class map to define traffic matching for the inside-class rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class
  match access-list inside_mpc_1
: Class map to define traffic matching for the sip-class-inside rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map sip-class-inside
  match access-list inside_mpc
: Class map to define traffic matching for the inside-class1 rule.
: In ASDM, this maps to call-out 3, from the Match to the Time fields.
class-map inside-class1
  match access-list inside_mpc_2

```

```

: Policy map that actually defines the service policy rule set named test-inside-policy.
: In ASDM, this corresponds to the folder at call-out 1.
policy-map test-inside-policy
: First rule in test-inside-policy, named sip-class-inside. Inspects SIP traffic.
: The sip-class-inside rule applies the sip-high inspection policy map to SIP inspection.
: In ASDM, each rule corresponds to call-out 2.
  class sip-class-inside
    inspect sip sip-high
: Second rule, inside-class. Applies SNMP inspection using an SNMP map.
  class inside-class
    inspect snmp snmp-v3only
: Third rule, inside-class1. Applies ICMP inspection.
  class inside-class1
    inspect icmp
: Fourth rule, class-default. Applies connection settings and enables user statistics.
  class class-default
    set connection timeout embryonic 0:00:30 half-closed 0:10:00 idle 1:00:00
  reset dcd 0:15:00 5
    user-statistics accounting
: The service-policy command applies the policy map rule set to the inside interface.
: This command activates the policies.
service-policy test-inside-policy interface inside

```

使用服务策略配置的功能

下表列出了使用服务策略配置的功能。

表 10: 使用服务策略配置的功能

功能	适用于直通流量?	适用于管理流量?	请参阅:
应用检测 (多种类型)	全部, 除 RADIUS 记账以外	仅限 RADIUS 记账	<ul style="list-style-type: none"> • 应用层协议检测入门, 第 309 页。 • 基本互联网协议检测, 第 327 页。 • 语音和视频协议检测, 第 359 页。 • 移动网络检测, 第 379 页。 • ASA 和思科 Cloud Web Security, 第 137 页。
ASA IPS	是	否	请参阅 ASA IPS 快速入门指南 。
ASA CX	是	否	请参阅 ASA CX 快速入门指南 。
ASA FirePOWER (ASA SFR)	是	否	ASA FirePOWER 模块 , 第 93 页。
NetFlow 安全事件记录过滤	支持	支持	请参阅 NetFlow 实施指南 。
QoS 输入和输出策略管制	是	否	服务质量 , 第 435 页。
QoS 标准优先级队列	是	否	服务质量 , 第 435 页。

功能	适用于直通流量？	适用于管理流量？	请参阅：
TCP 和 UDP 连接限制与超时，以及 TCP 序列号随机化	支持	支持	连接设置，第 415 页。
TCP 规范化	是	否	连接设置，第 415 页。
TCP 状态绕行	是	否	连接设置，第 415 页。
身份防火墙用户统计信息	支持	支持	请参阅命令参考中的 user-statistics 命令。

功能方向性

可以操作将双向或单向应用到流量，具体情况视功能而定。对于双向应用的功能，如果流量在两个方向上都匹配类映射，所有流入或流出应用了策略映射的接口的流量都会受到影响。



注释 当使用全局策略时，所有功能都是单向的；通常在应用到单一接口时为双向的功能，在全局应用时仅应用到每个接口的入口。因为策略应用到所有接口，策略将在两个方向上应用，因此在这种情况下，双向性是多余的。

对于单向应用的功能（例如 QoS 优先级队列），仅流入（或流出，具体取决于功能）应用了策略映射的接口的流量会受到影响。请参见下表，了解每项功能的方向性。

表 11: 功能方向性

功能	单一接口方向	全局方向
应用检测（多种类型）	双向	入口
ASA CX	双向	入口
ASA CX 身份验证代理	入口	入口
ASA FirePOWER (ASA SFR)	双向	入口
ASA IPS	双向	入口
NetFlow 安全事件记录过滤	N/A	入口
QoS 输入策略管制	入口	入口
QoS 输出策略管制	出口	出口
QoS 标准优先级队列	出口	出口

功能	单一接口方向	全局方向
TCP 和 UDP 连接限制与超时，以及 TCP 序列号随机化	双向	入口
TCP 规范化	双向	入口
TCP 状态绕行	双向	入口
身份防火墙用户统计信息	双向	入口

服务策略中的功能匹配

数据包根据以下规则，匹配给定接口的策略中的规则：

1. 对于每个功能类型，数据包只能与接口的一个规则匹配。
2. 在数据包匹配某个功能类型的规则后，ASA 不会再尝试将其与该功能类型的任何后续规则匹配。
3. 但是，如果该数据包与其他功能类型的后续规则匹配，则 ASA 也会应用适用于该后续规则的操作（如果支持）。请参阅[某些功能操作的不兼容性](#)，第 298 页，了解有关不受支持的组合的详细信息。



注释

应用检测包括多种检测类型，大部分类型都相互排斥。对于可以组合在一起的检测，每项检测都被视为一项独立功能。

数据包匹配示例

例如：

- 如果数据包不仅与连接限制的规则匹配，还与应用检测的规则匹配，则会同时应用两项操作。
- 如果数据包不仅与 HTTP 检测的规则匹配，还与包含 HTTP 检测的另一个规则匹配，则不会应用第二项规则操作。
- 如果数据包不仅与 HTTP 检测的规则匹配，还与包含 FTP 检测的另一个规则匹配，则不会应用第二项规则操作，因为 HTTP 和 FTP 检测无法合并。
- 如果数据包不仅与 HTTP 检测的规则匹配，还与包含 IPv6 检测的另一个规则匹配，则会同时应用两项操作，因为 IPv6 检测可与任何类型的检测合并。

多种功能操作的应用顺序

不同类型的操作在服务策略中的执行顺序独立于操作在表中的显示顺序。

按以下顺序执行操作：

1. QoS 输入策略管制
2. TCP 规范化、TCP 和 UDP 连接限制与超时、TCP 序列号随机化以及 TCP 状态绕行。



注释 当 ASA 执行代理服务（例如 AAA 或 CSC）或修改 TCP 负载（例如 FTP 检测）时，TCP 规范器在双重模式下运行，即于代理或负载修改服务之前和之后进行应用。

3. 可以与其他检测合并在一起的应用检测：
 1. IPv6
 2. IP 选项
 3. WAAS
4. 无法与其他检测合并在一起的应用检测。有关详细信息，请参阅[某些功能操作的不兼容性](#)，第 298 页。
5. ASA IPS
6. ASA CX
7. ASA FirePOWER (ASA SFR)
8. QoS 输出策略管制
9. QoS 标准优先级队列



注释 NetFlow 安全事件记录过滤和身份防火墙用户统计信息与顺序无关。

某些功能操作的不兼容性

某些功能对于同一流量互不兼容。下表可能不包含所有不兼容性；有关每项功能兼容性的详细信息，请参阅功能对应的章节：

- 无法对同一组的流量配置优先级队列和策略管制。
- 大多数检测不应与其他检测整合使用，所以当为相同流量配置了多种检测时，ASA 仅应用一种检测。HTTP 检测可以与云网络安全检测整合在一起。其他例外已在[多种功能操作的应用顺序](#)，第 297 页中列出。
- 无法配置即将发送到多个模块（例如 ASA CX 和 ASA IPS）的流量。
- HTTP 检测与 ASA CX 或 ASA FirePOWER 不兼容。
- 云网络安全与 ASA CX 或 ASA FirePOWER 不兼容。

**注释**

默认全局策略中使用的默认检测 Traffic 流量类是用来匹配所有检测的默认端口的特殊 CLI 快捷方式。在策略映射中使用该流量类时，该类映射可以根据流量的目标端口确保应用到每个数据包的检测都正确。例如，当端口 69 的 UDP 流量到达 ASA 时，ASA 会应用 TFTP 检测；当端口 21 的 TCP 流量到达时，ASA 会应用 FTP 检测。因此只有在这种情况下，才能为同一类映射配置多项检测。通常，ASA 不会使用端口号来确定应用哪种检测，因此您可以灵活地对非标准端口等应用检测。

该流量类不包含云网络安全检测的默认端口（80 和 443）。

多个服务策略的功能匹配

对于 TCP 和 UDP 流量（以及启用状态性 ICMP 检测时的 ICMP），服务策略不仅在单个数据包上运行，还在流量上运行。如果流量为现有连接的一部分且该现有连接匹配一个接口上的策略中的某项功能，那么该流量无法匹配另一个接口上的策略中的同一项功能；仅使用第一项策略。

例如，如果 HTTP 流量匹配内部接口上的检查 HTTP 流量的策略，而且在 HTTP 检测的外部接口上有独立策略，该流量不会同时在外部接口的出口被检测。同样，该连接的返回流量不会被外部接口的入口策略检测，也不会被内部接口的出口策略检测。

对于未被当作流量处理的流量，例如，不启用状态性 ICMP 检测时的 ICMP，返回流量可以匹配返回接口上的另一个策略映射。例如，如果在内部和外部接口上配置 IPS，但内部策略使用虚拟传感器 1，同时外部策略使用虚拟传感器 2，则非状态性 Ping 将匹配出站虚拟传感器 1，以及匹配入站虚拟传感器 2。

服务策略指南

检测指南

本文以有单独的主题详细介绍用于应用检测服务策略的指南。请参阅[应用检测指南](#)，第 311 页。

IPv6 规定

支持在以下功能中使用 IPv6：

- 服务器（但并非所有）、协议的应用检测。有关详细信息，请参阅[应用检测指南](#)，第 311 页。
- ASA IPS
- ASA CX
- ASA FirePOWER
- NetFlow 安全事件记录过滤
- SCTP 状态绕行
- TCP 和 UDP 连接限制与超时，TCP 系列号随机化

- TCP 规范化
- TCP 状态绕行
- 身份防火墙用户统计信息

类映射（流量类）指导原则

所有类型的最大类映射（流量类）数量在单一模式下为 255，在多模式下视情景而定。类映射包括下列类型：

- 第 3/4 层类映射（对于直通流量和管理流量）。
- 检测类映射
- 正则表达式类映射
- **match** 直接在检测策略映射下使用的命令

该限制还包括所有类型的默认类映射，将用户配置的类映射限制为大约 235 个。

服务策略指导原则

- 对于给定功能，入口接口上的接口服务策略优先级高于全局服务策略。例如，如果有 FTP 检测全局策略和 TCP 规范化接口策略，则系统将 FTP 检测和 TCP 规范化应用到接口。不过，如果有 FTP 检测全局策略和 FTP 检测入口接口策略，则仅向该接口应用入口接口策略 FTP 检测。如果没有入口或全局策略来实施功能，则应用出口接口上指定该功能的接口服务策略。
- 只能应用一项全局策略。例如，无法创建一个包含功能集 1 的全局策略和另一个包含功能集 2 的全局策略。所有功能都必须包含在单一策略中。
- 当对配置进行服务策略更改后，所有新连接都将使用新的服务策略。现有连接将继续使用在连接建立时配置的策略。**show** 命令输出不包含有关旧连接的数据。

例如，如果从接口中删除 QoS 服务策略，再添加修改的版本，则 **show service-policy** 命令仅显示与匹配新服务策略的新连接相关的 QoS 计数器；命令输出中不再显示旧策略上的现有连接。

要确保所有连接都使用新策略，需要断开当前连接，以便使用新策略重新连接。使用 **clear conn** 或 **clear local-host** 命令。

服务策略默认设置

以下主题介绍服务策略和模块化策略框架的默认设置。

默认服务策略配置

默认情况下，配置包含一项策略（全局策略），该策略匹配所有默认应用检测流量并将某些检测应用到所有接口上的流量。并非所有检测都默认被启用。仅能应用一个全局策略，因此如果想要改变

全局策略，则需要编辑默认策略或禁用默认策略并应用新策略。（对于某项特定功能，接口策略覆盖全局策略。）

默认策略包括以下应用检测：

- DNS
- FTP
- H323 (H225)
- H323 (RAS)
- RSH
- RTSP
- ESMTTP
- SQLnet
- Skinny (SCCP)
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP
- IP Options

默认类映射（流量类）

该配置包括 ASA 在默认全局策略（称为默认检测流量）中使用的默认第 3/4 层类映射（流量类）；它与默认检测流量匹配。该类在默认全局策略中使用，是一个用来匹配所有检测的默认端口的特殊快捷方式。

在策略中使用时，该类可以根据流量的目标端口，确保应用到每个数据包的检测都正确。例如，当端口 69 的 UDP 流量到达 ASA 时，ASA 会应用 TFTP 检测；当端口 21 的 TCP 流量到达时，ASA 会应用 FTP 检测。因此只有在这种情况下，才能为同一类映射配置多项检测。通常，ASA 不会使用端口号来确定应用哪种检测，因此您可以灵活地对非标准端口等应用检测。

默认配置中存在的另一种类映射是 `class-default`，它与所有流量均匹配。如果需要，您可以使用 `class-default` 类，而不是。实际上，有些功能仅适用于 `class-default`。

配置服务策略

配置服务策略包括为每个接口或全局策略添加一项或多项服务策略。ASDM 使用向导来执行创建服务策略的过程。对于每条规则，可以识别以下要素：

1. 要应用规则的接口或全局策略。
2. 要应用操作的流量。可以识别第 3 层和第 4 层流量。
3. 应用到流量类的操作。可以为每个流量类应用多项互不冲突的操作。

创建策略后，可以添加规则，移动、编辑或删除规则或策略。以下主题介绍如何配置服务策略。

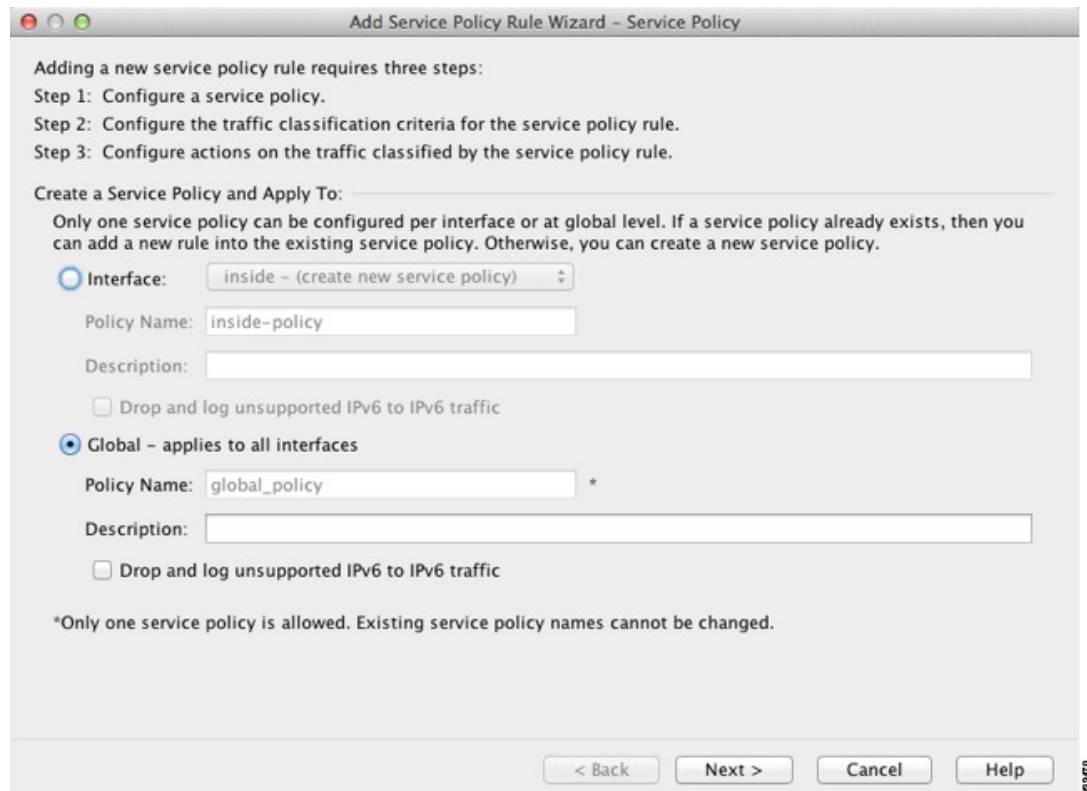
为直通流量添加服务策略规则

要为直通流量添加服务策略规则，请使用 Add Service Policy Rule 向导。系统将要求您为某个特定接口或全局选择策略范围：

- 对于指定的功能，接口服务策略优先于全局服务策略。例如，如果有 FTP 检测全局策略和 TCP 连接限制接口策略，则系统将 FTP 检测和 TCP 连接限制应用到接口。然而，如果有 FTP 检测全局策略和 FTP 检测接口策略，则系统仅会将接口策略 FTP 检测应用到接口。
- 全局服务策略可以为所有接口提供默认服务。除非被接口特定策略覆盖，否则将应用全局服务。默认情况下，存在一项全局策略，包括适用于默认应用检测的服务策略规则。可以使用向导向全局策略添加规则。

过程

步骤 1 依次选择 **配置 > 防火墙 > 服务策略规则**，然后点击 **添加或添加** 添加服务策略规则。



步骤 2 在 **Create a Service Policy and Apply To** 区域:

- a) 选择 **Interface** 将策略应用到某个特定接口，或者选择 **Global** 应用到所有接口。
- b) 如果选择 **Interface**，请选择接口名称。如果接口已有策略，可以向现有策略添加规则。
- c) 如果接口没有服务策略，请输入新策略的名称。
- d) （可选）输入策略说明。
- e) （可选）选中 **Drop and log unsupported IPv6 to IPv6 traffic** 选项，为不支持 IPv6 流量的应用检测丢弃的 IPv6 流量生成系统日志 (767001)。默认情况下不生成系统日志。
- f) 点击 **Next**。

步骤 3 在 **Traffic Classification Criteria** 页面，选择以下选项之一，指定要应用策略操作的流量，然后点击 **Next**。

- **Create a new traffic class**。输入流量类名称和可选说明。

使用以下某个条件识别流量:

- **Default Inspection Traffic** - 该类匹配 ASA 可检测的所有应用使用的默认 TCP 和 UDP 端口。当点击 **Next** 时，系统将显示该类定义的服务和端口。

该选项在默认全局策略中使用，在规则中使用，是一个特殊的快捷方式，可以根据流量的目标端口确保应用到每个数据包的检测都正确。有关详细信息，请参阅[默认类映射（流量类）](#)，第 301 页。

请参阅[默认检测和 NAT 限制](#)，第 312 页，查看默认端口列表。ASA 包括匹配默认检测流量的默认全局策略，并会对所有接口上的流量应用常规检测。并非端口包含在 Default Inspection Traffic 类中的所有应用都在策略映射中被默认启用。

可以指定 Source and Destination IP Address 类（使用 ACL）以及 Default Inspection Traffic 类，缩小被匹配的流量的范围。由于 Default Inspection Traffic 类指定了要匹配的端口和协议，ACL 中的任意端口和协议都将被忽略。

- **Source and Destination IP Address (uses ACL)** - 该类匹配扩展 ACL 指定的流量。当点击 **Next** 时，系统会提示您输入访问控制条目的属性，然后向导将构建 ACL。或者，您可以选择现有 ACL。

定义 ACE 时，Match 选项创建一条规则，使操作应用于匹配这些地址的流量。Do Not Match 选项可以免于向流量应用指定的操作。例如，要匹配 10.1.1.0/24 中的所有流量，并应用连接限制，但 10.1.1.25 除外。在这种情况下，创建两条规则，使用 Match 选项为 10.1.1.0/24 创建一条，使用 Do Not Match 为 10.1.1.25 创建一条。请务必安排这些规则，使 Do Not Match 规则优先于 Match 规则，否则 10.1.1.25 将首先匹配 Match 规则。

注释 创建此类型的新流量类时，最初只能指定一个访问控制条目 (ACE)。完成添加该规则后，即可添加更多 ACE，方法是向同一个接口或全局策略中添加一条新规则，然后指定 **Add rule to existing traffic class**（请参阅以下内容）。

- **Tunnel Group** - 该类匹配想要应用 QoS 的隧道组流量（连接配置文件）。还可以指定另一个流量匹配选项，以优化流量匹配，Any Traffic、Source and Destination IP Address (uses ACL) 或 Default Inspection Traffic 除外。

点击 **Next** 时，系统将提示您选择隧道组（如果需要，可以创建一个新隧道组）。要对每个流进行策略管制，请选中 **Match flow destination IP address**。所有流向某唯一 IP 目标地址的流量都被视为流。

- **TCP or UDP or SCTP Destination Port** - 该类匹配单一端口或连续的端口范围。点击 **Next** 时，系统会提示您选择协议并输入端口号；点击 ... 可选择 ASDM 中已定义的某个协议。

提示 对于使用多个非连续端口的应用，请使用 Source and Destination IP Address (uses ACL) 匹配每个端口。

- **RTP Range** - 该类映射匹配 RTP 流量。点击 **Next** 时，系统将提示您输入一个 RTP 端口范围，介于 2000 和 65534 之间。此范围中的最大端口数量为 16383 个。
- **IP DiffServ CodePoints (DSCP)** - 该类最多匹配 IP 报头中的 8 个 DSCP 值。点击 **Next** 时，系统将提示您选择或输入所需要的值（将这些值移至 Match on DSCP 列表）。
- **IP Precedence** - 该类映射最多匹配 4 个优先级值，用 IP 报头中的 TOS 字节表示。点击 **Next** 时，系统将提示您设置数值。
- **Any Traffic** - 匹配所有流量。

- **Add rule to existing traffic class**。如果同一接口上已有服务策略规则，或者正在向全局服务策略添加规则，可以通过此选项向现有 ACL 添加 ACE。可以将 ACE 添加到之前在为该接口上的服务策略规则选择 Source and Destination IP Address (uses ACL) 选项时创建的任意 ACL。对于该流

量类，即使添加多个 ACE，也只能有一组规则操作。可以重复这一完整操作步骤，将多个 ACE 添加到同一流量类。点击 **Next** 时，系统将提示您设置访问控制条目的属性。

- **Use an existing traffic class.** 如果创建了被不同接口上的规则使用的流量类，可以重复使用该规则的流量类定义。请注意，如果更改某条规则的流量类，该更改将被所有使用该流量类的规则继承。如果配置包含在 CLI 上输入的任何 **class-map** 命令，则那些流量类名称也可用（尽管需要创建规则，以查看流量类的定义）。
- **Use class default as the traffic class.** 该选项使用 class-default 类，该类匹配所有流量。class-default 类由 ASA 自动创建并被置于策略末尾。如果不对其应用任何操作，ASA 仍会创建该类，但仅供内部使用。如果需要，可以对该类应用操作，这可能比创建一个匹配所有流量的新流量类更方便。只能使用 class-default 类为该服务策略创建一条规则，因为每个流量类只能与一项策略的单一规则相关联。

步骤 4 如果选择了要求附加配置的流量匹配条件，请输入所需的参数并点击 **Next**。

步骤 5 在 Rule Actions 页面，配置一项或多项规则操作。请参阅 [使用服务策略配置的功能](#)，第 295 页，了解可以应用的功能和操作列表，以及到其他详细信息的指针。

步骤 6 点击 **Finish**。

为管理流量添加服务策略规则

要为定向到 ASA 的流量添加服务策略规则以进行管理，请使用 Add Service Policy Rule 向导。系统将要求您为某个特定接口或全局选择策略范围：

- 对于指定的功能，接口服务策略优先于全局服务策略。例如，如果有 RADIUS 记账检测全局策略和连接限制接口策略，则系统将 RADIUS 记账和连接限制应用到接口。然而，如果有 RADIUS 记账到接口。
- 全局服务策略可以为所有接口提供默认服务。除非被接口特定策略覆盖，否则将应用全局服务。默认情况下，存在一项全局策略，包括适用于默认应用检测的服务策略规则。可以使用向导向全局策略添加规则。

过程

步骤 1 依次选择 **配置 > 防火墙 > 服务策略规则**，然后点击 **添加或添加 > 添加管理服务策略规则**。

步骤 2 在 Create a Service Policy and Apply To 区域：

- a) 选择 **Interface** 将策略应用到某个特定接口，或者选择 **Global** 应用到所有接口。
- b) 如果选择 **Interface**，请选择接口名称。如果接口已有策略，可以向现有策略添加规则。
- c) 如果接口没有服务策略，请输入新策略的名称。
- d) （可选）输入策略说明。
- e) 点击 **Next**。

步骤 3 在 Traffic Classification Criteria 页面，选择以下选项之一，指定要应用策略操作的流量，然后点击 **Next**。

- **Create a new traffic class**。输入流量类名称和可选说明。

使用以下某个条件识别流量：

- **Source and Destination IP Address (uses ACL)** - 该类匹配扩展 ACL 指定的流量。当点击 **Next** 时，系统会提示您输入访问控制条目的属性，然后向导将构建 ACL。或者，您可以选择现有 ACL。

定义 ACE 时，Match 选项创建一条规则，使操作应用于匹配这些地址的流量。Do Not Match 选项可以免于向流量应用指定的操作。例如，要匹配 10.1.1.0/24 中的所有流量，并应用连接限制，但 10.1.1.25 除外。在这种情况下，创建两条规则，使用 Match 选项为 10.1.1.0/24 创建一条，使用 Do Not Match 为 10.1.1.25 创建一条。请务必安排这些规则，使 Do Not Match 规则优先于 Match 规则，否则 10.1.1.25 将首先匹配 Match 规则。

- **TCP or UDP or SCTP Destination Port** - 该类匹配单一端口或连续的端口范围。点击 **Next** 时，系统会提示您选择协议并输入端口号；点击 ... 可选择 ASDM 中已定义的某个协议。

提示 对于使用多个非连续端口的应用，请使用 Source and Destination IP Address (uses ACL) 匹配每个端口。

- **Add rule to existing traffic class**。如果同一接口上已有服务策略规则，或者正在向全局服务策略添加规则，可以通过此选项向现有 ACL 添加 ACE。可以将 ACE 添加到之前在为该接口上的服务策略规则选择 Source and Destination IP Address (uses ACL) 选项时创建的任意 ACL。对于该流量类，即使添加多个 ACE，也只能有一组规则操作。可以重复这一完整操作步骤，将多个 ACE 添加到同一流量类。点击 **Next** 时，系统将提示您设置访问控制条目的属性。
- **Use an existing traffic class**。如果创建了被不同接口上的规则使用的流量类，可以重复使用该规则的流量类定义。请注意，如果更改某条规则的流量类，该更改将被所有使用该流量类的规则继承。如果配置包含在 CLI 上输入的任何 **class-map** 命令，则那些流量类名称也可用（尽管需要创建规则，以查看流量类的定义）。

步骤 4 如果选择了要求附加配置的流量匹配条件，请输入所需的参数并点击 **Next**。

步骤 5 在 Rule Actions 页面，配置一项或多项规则操作。

- 要配置 RADIUS 记账检测，请从 RADIUS Accounting Map 下拉列表选择检测映射，或者点击 **Configure** 添加映射。有关详细信息，请参阅 [使用服务策略配置的功能](#)，第 295 页。
- 要配置连接设置，请参阅 [配置特定流量类的连接设置（所有服务）](#)，第 429 页。

步骤 6 点击 **Finish**。

管理服务策略规则的顺序

接口上或全局策略中的服务策略规则的顺序会影响将操作应用到流量的方式。请参阅以下指导原则，了解数据包如何匹配服务策略中的规则：

- 数据包只能匹配每个功能类型的服务策略中的一条规则。
- 在数据包匹配包含某个功能类型的操作的规则后，ASA 不会再尝试将其与包含该功能类型的任何后续规则匹配。
- 但是，如果该数据包与其他功能类型的后续规则匹配，则 ASA 也会应用适用于该后续规则的操作。

例如，如果数据包既匹配连接限制规则，也匹配应用检查规则，则系统会应用这两项规则的操作。

如果数据包匹配应用检测规则，但也匹配另一条包含应用检测的规则，则系统不会应用第二条规则的操作。

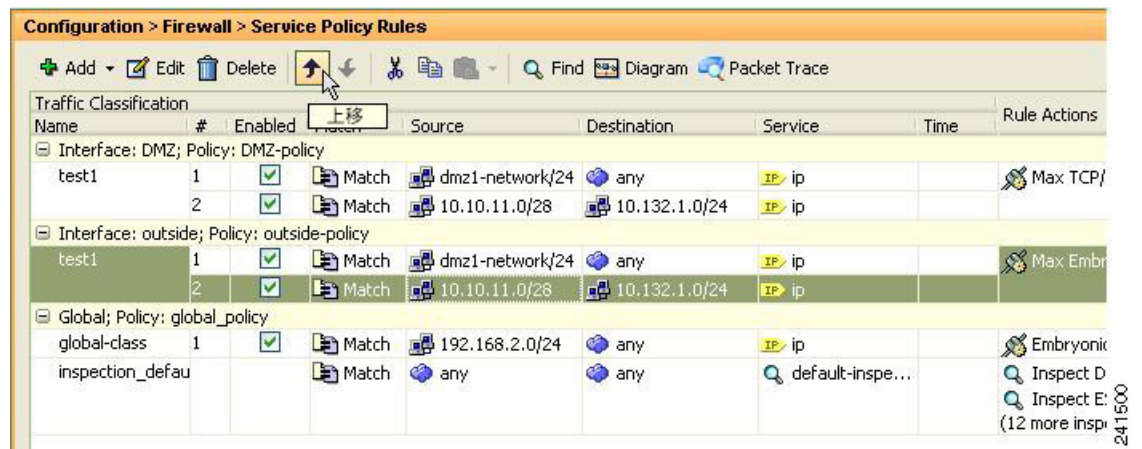
如果规则包含一个带多个 ACE 的 ACL，ACE 的顺序也会影响数据包流。ASA 会按照条目列出的顺序对照每个 ACE 检测数据包。找到匹配项后，不再检查更多 ACE。例如，如果在 ACL 的开头创建一个明确允许所有流量的 ACE，则不进一步检查其他语句。

要更改规则顺序或规则中 ACE 的顺序，请执行以下步骤：

过程

步骤 1 在 **Configuration > Firewall > Service Policy Rules** 页面上，选择希望上下移动的规则或 ACE。

步骤 2 点击 **Move Up** 或 **Move Down** 按钮。



注释 如果在多个服务策略中使用的 ACL 中重新排列 ACE，该更改将在所有服务策略中被继承。

步骤 3 重新排列规则或 ACE 后，点击 **Apply**。

服务策略的历史

功能名称	版本	说明
模块化策略框架	7.0(1)	引入了模块化策略框架。
与 RADIUS 记账流量一起使用的管理类映射	7.2(1)	引入了管理类映射，与 RADIUS 记账流量一起使用。引入了以下命令： class-map type management 和 inspect radius-accounting 。
检测策略映射	7.2(1)	引入了检测策略映射。引入了以下命令： class-map type inspect 。
正则表达式和策略映射	7.2(1)	引入了正则表达式和策略映射，将其用于检查策略映射下。引入了以下命令： class-map type regex 、 regex 、 match regex 。
检测策略映射的 match any	8.0(2)	引入了关键字 match any ，与检测策略映射一起使用：流量可以匹配一个或多个条件以匹配类映射。过去，仅 match all 可用。



第 14 章

应用层协议检测入门

以下主题介绍如何配置应用层协议检测。

- [应用层协议检测](#)，第 309 页
- [配置应用层协议检测](#)，第 316 页
- [配置正则表达式](#)，第 320 页
- [监控检测策略](#)，第 324 页
- [应用检测的历史](#)，第 325 页

应用层协议检测

针对在用户数据包内嵌入 IP 寻址信息的服务或在动态分配端口上打开辅助信道的服务，需要使用检测引擎。这些协议需要 ASA 执行深度数据包检测，而不是通过快速路径传递数据包。因此，检测引擎可能会影响整体吞吐量。默认情况下，ASA 上启用了几个常见检测引擎，但您可能需要根据您的网络启用其他检测引擎。

以下主题详细说明应用检测。

何时使用应用协议检测

当用户建立连接时，ASA 会对照 ACL 检查数据包、创建地址转换并为快速路径中的会话创建条目，以便后续数据包可绕过耗时的检查。但是，快速路径依赖于可预测的端口号，且不在数据包内执行地址转换。

许多协议开放辅助 TCP 或 UDP 端口。已知端口上的初始会话用于协商动态分配的端口号。

其他应用在需要与源地址匹配的数据包中嵌入 IP 地址，源地址通常在通过 ASA 时被转换。

如果使用类似的应用，需要启用应用检测。

当您对嵌入 IP 地址的服务启用应用检测时，ASA 转换嵌入的地址并更新受转换影响的所有校验和其他字段。

当您对使用动态分配的端口的服务启用应用检测时，ASA 监控会话以标识动态端口分配并允许特定会话期间在这些端口上进行数据交换。

检测策略映射

可以使用检测策略映射为许多应用检测配置特殊操作。这些映射是可选的：无需配置映射，即可为支持检测策略映射的协议启用检测。仅在需要执行非默认检测操作的情况下，才需要这些映射。

检测策略映射由下列一个或多个要素组成。检测策略映射的确切可用选项视应用而定。

- 流量匹配条件 - 将应用流量与特定于应用的条件进行匹配（例如 URL 字符串，随后可以对这些条件启用操作）。

对于某些流量匹配条件，可使用正则表达式来匹配数据包中的文本。请务必在配置策略映射之前，在正则表达式类映射中单独或集中创建和测试正则表达式。

- 检测类映射 - 某些检测策略映射可以实现使用检测类映射包含多个流量匹配条件。然后，可以在检测策略映射中识别检测类映射，并整体启用用于类的操作。创建类映射和直接在检测策略映射中定义流量匹配的差别在于，您可以创建更复杂的匹配条件和重复使用类映射。然而，您无法为不同的匹配设置不同操作。

- 参数 - 参数会影响检测引擎的行为。

以下主题提供更多详细信息。

更换正在使用的检测策略映射

如果在服务策略中已启用使用某一策略映射的检测，则更换策略映射需要分两步进行。首先，必须从服务策略中删除该检测并应用更改。然后重新添加该检测，选择新的策略映射名称，并重新应用更改。

如何处理多个流量类

在检测策略映射中可以指定多个检测类映射或直接匹配。

如果一个数据包匹配不同的类或直接匹配，则 ASA 应用操作的顺序由内部 ASA 规则决定，而不是按操作添加到检测策略映射的顺序应用应用。内部规则由应用类型和解析数据包的逻辑顺序确定，并且不可由用户配置。例如，对于 HTTP 流量，解析 Request Method 字段优先于解析 Header Host Length 字段；Request Method 字段的操作早于 Header Host Length 字段的操作。

如果操作丢弃数据包，则在检测策略映射中将不会执行进一步操作。例如，如果第一个操作是重置连接，将不会匹配任何进一步的匹配条件。如果第一个操作是记录数据包，则会发生第二个操作，例如，重置连接。

如果一个数据包匹配多个相同的匹配条件，则按策略映射中显示匹配条件的顺序匹配它们。

根据类映射中的最低优先级匹配选项（优先级以内部规则为准），确定一个类映射与另一个类映射的类型相同或直接匹配。如果某个类映射具有与另一个类映射相同的最低优先级匹配选项类型，则根据类映射添加到策略映射的顺序来匹配类映射。如果每个类映射的最低优先级匹配选项不同，则首先匹配具有较高优先级匹配选项的类映射。

应用检测指南

故障切换

需要检测的多媒体会话的状态信息不通过用于状态故障切换的状态链路进行传递。但通过状态链路进行复制的 GTP、M3UA, 和 SIP 例外。您必须在 M3UA 检测中配置严格应用服务器进程 (ASP) 状态检查, 才能执行状态故障切换。

集群

集群中不支持以下检测:

- CTIQBE
- H323、H225 和 RAS
- IPsec 穿透
- MGCP
- MMP
- RTSP
- SCCP (瘦客户端)
- WAAS

IPv6

以下检测中支持 IPv6:

- Diameter
- DNS over UDP
- FTP
- GTP
- HTTP
- ICMP
- IPsec 直通
- IPv6
- M3UA
- SCCP (瘦客户端)
- SCTP
- SIP

- SMTP
- VXLAN

以下检测中支持 NAT64:

- DNS over UDP
- FTP
- HTTP
- ICMP
- SCTP

其他指导原则

- 某些检测引擎不支持 PAT、NAT、外部 NAT 或相同安全接口之间的 NAT。有关 NAT 支持的详细信息，请参阅[默认检测和 NAT 限制](#)，第 312 页。
- 对于所有应用检测，ASA 允许同时活动的数据连接数限于 200 个连接。例如，如果 FTP 客户端打开多个辅助连接，FTP 检测引擎只允许 200 个活动连接，第 201 个连接将被丢弃，并且自适应安全设备将生成系统错误消息。
- 检测的协议受制于高级 TCP 状态跟踪，这些连接的 TCP 状态不会自动复制。如果这些连接复制到备用设备，将会尽力尝试重新建立 TCP 状态。
- 如果系统确定 TCP 连接需要检测，系统在检测之前，将会清除除关于数据包的 MSS 和选择性确认 (SACK) 选项以外的所有 TCP 选项。其他选项将被清除，即使您在应用于连接的 TCP 映射中允许这些选项。
- 默认检测定向到 ASA（流向接口）的 TCP/UDP 流量。但是，即使启用 ICMP 检测，也不会检测流向接口的 ICMP 流量。因此，到接口的 ping（回应请求）可能会在特定情况下失败，例如，如果回应请求来自 ASA 可以通过备用默认路由到达的源。

应用检测的默认设置

以下主题介绍应用检测的默认操作。

默认检测和 NAT 限制

默认情况下，配置包括会匹配所有默认应用检测流量并对所有接口的流量应用检测的策略（全局策略）。默认应用检测流量包括流向各个协议的默认端口的流量。只能应用一个全局策略，因此如果要改变全局策略（例如，要对非标准端口应用检测，或者要添加默认情况下未启用的检测），需要编辑默认策略或者禁用默认策略并应用新策略。

下表列出了所有支持的检测、用于默认类映射的默认端口和默认打开的检测引擎（以粗体显示）。该表中还对任何 NAT 限制作了备注。在该表中：

- 默认情况下为默认端口启用的检测引擎以粗体显示。

- ASA 符合指示的标准，但它不会对要检测的数据包执行合规性。例如，FTP 命令应采用特定的顺序，但 ASA 不执行该顺序。

表 12: 支持的应用检测引擎

应用	默认协议、端口	NAT 限制	标准	注释
CTIQBE	TCP/2748	无扩展 PAT。 无 NAT64。 (集群) 无静态 PAT。	—	—
DCERPC	TCP/135	无 NAT64。	—	—
Diameter	TCP/3868 TCP/5868 (用于 TCP/TLS) SCTP/3868	无 NAT/PAT。	RFC 6733	需要 Carrier 许可证。
DNS over UDP DNS over TCP	UDP/53 UDP/443 TCP/53	无可用于通过 WINS 进行名称解析的 NAT 支持。	RFC 1123	要检测 DNS over TCP，必须在 DNS 检测策略映射中启用 DNS/TCP 检测。 UDP/443 仅用于思科 Umbrella DNScrypt 会话。
FTP	TCP/21	(集群) 无静态 PAT。	RFC 959	—
GTP	UDP/3386 (GTPv0) UDP/2123 (GTPv1+)	无扩展 PAT。 无 NAT。	—	需要 Carrier 许可证。
H.323 H.225 和 RAS	TCP/1720 UDP/1718 UDP (RAS) 1718-1719	(集群) 无静态 PAT。 无扩展 PAT。 不支持对同类安全接口执行 NAT。 无 NAT64。	ITU-T H.323、 H.245、 H225.0、 Q.931、Q.932	—
HTTP	TCP/80	—	RFC 2616	请注意，MTU 限制会去除 ActiveX 和 Java。如果 MTU 因为太小而不允许在一个数据包中包含 Java 或 ActiveX 标记，可能不会出现去除操作。

应用	默认协议、端口	NAT 限制	标准	注释
ICMP	ICMP	—	—	不会检测流向 ASA 接口的 ICMP 流量。
ICMP 错误	ICMP	—	—	—
ILS (LDAP)	TCP/389	无扩展 PAT。 无 NAT64。	—	—
即时消息 (IM)	因客户端而异	无扩展 PAT。 无 NAT64。	RFC 3860	—
IP 选项	RSVP	无 NAT64。	RFC 791、RFC 2113	—
IPSec 穿透	UDP/500	无 PAT。 无 NAT64。	—	—
IPv6	—	无 NAT64。	RFC 2460	—
LISP	—	无 NAT 或 PAT。	—	—
M3UA	SCTP/2905	无面向嵌入式地址的 NAT 或 PAT。	RFC 4666	需要 Carrier 许可证。
MGCP	UDP/2427、 2727	无扩展 PAT。 无 NAT64。 (集群) 无静态 PAT。	RFC 2705bis-05	—
MMP	TCP/5443	无扩展 PAT。 无 NAT64。	—	—
基于 IP 的 NetBIOS 名称服 务器	UDP/137、138 (源端口)	无扩展 PAT。 无 NAT64。	—	通过执行 NBNS UDP 端口 137 和 NBDS UDP 端口 138 的数据包 NAT 来支持 NetBIOS。
PPTP	TCP/1723	无 NAT64。 (集群) 无静态 PAT。	RFC 2637	—
RADIUS 记账	UDP/1646	无 NAT64。	RFC 2865	—
RSH	TCP/514	无 PAT。 无 NAT64。 (集群) 无静态 PAT。	Berkeley UNIX	—

应用	默认协议、端口	NAT 限制	标准	注释
RTSP	TCP/554	无扩展 PAT。 无 NAT64。 (集群) 无静态 PAT。	RFC 2326、 2327、1889	无 HTTP 掩蔽处理。
ScanSafe (云网络安全)	TCP/80 TCP/443	—	—	这些端口未包含在适用于 ScanSafe 检测的 default-inspection-traffic 类中。
SCTP	SCTP	—	RFC 4960	需要 Carrier 许可证。 虽然可以对 SCTP 流量执行静态网络对象 NAT (无动态 NAT/PAT)，但检测引擎不用于 NAT。
SIP	TCP/5060 UDP/5060	在安全级别相同或低于较高安全级别的接口上无 NAT/PAT。 无扩展 PAT。 无 NAT64 或 NAT46。 (集群) 无静态 PAT。	RFC 2543	某些情况下不处理 TFTP 上传的思科 IP 电话配置。
瘦客户端 (SCCP)	TCP/2000	不支持对同类安全接口执行 NAT。 无扩展 PAT。 无 NAT64、NAT46 或 NAT66。 (集群) 无静态 PAT。	—	某些情况下不处理 TFTP 上传的思科 IP 电话配置。
SMTP 和 ESMTP	TCP/25	无 NAT64。	RFC 821、1123	—
SNMP	UDP/161、162	无 NAT 或 PAT。	RFC 1155、 1157、1212、 1213、1215	v.2 RFC 1902-1908; v.3 RFC 2570-2580。
SQL*Net	TCP/1521	无扩展 PAT。 无 NAT64。 (集群) 无静态 PAT。	—	v.1 和 v.2。
STUN	TCP/3478 UDP/3478	(WebRTC) 仅静态 NAT/PAT44。 (思科 Spark) 静态 NAT/PAT44 和 64; 动态 NAT/PAT。	RFC 5245、5389	—

应用	默认协议、端口	NAT 限制	标准	注释
Sun RPC	TCP/111 UDP/111	无扩展 PAT。 无 NAT64。	—	—
TFTP	UDP/69	无 NAT64。 (集群) 无静态 PAT。	RFC 1350	不转换负载 IP 地址。
WAAS	TCP/1 - 65535	无扩展 PAT。 无 NAT64。	—	—
XDMCP	UDP/177	无扩展 PAT。 无 NAT64。 (集群) 无静态 PAT。	—	—
VXLAN	UDP/4789	不适用	RFC 7348	虚拟可扩展局域网。

默认检测策略映射

某些检测类型使用隐藏的默认策略映射。例如，如果启用 ESMTP 检测但不指定映射，将会使用 `_default_esmtp_map`。

说明每种检测类型的各节中介绍了默认检测。可以使用 `show running-config all policy-map` 命令；使用 **工具 > 命令行界面** 查看这些默认映射。

DNS 检测是唯一一种采用明确配置的默认映射 `preset_dns_map` 的检测。

配置应用层协议检测

应用检测在服务策略中进行配置。

某些使用标准端口和协议的应用，默认已在所有接口上全局启用检测。有关默认检测的详细信息，请参阅 [默认检测和 NAT 限制](#)，第 312 页。自定义检测配置的一种常用方法是自定义默认全局策略。或者，可以创建所需的新服务策略，例如，接口特定策略。

开始之前

对于某些应用，在配置检测策略映射来启用检测时，可以执行特殊操作。此操作步骤后面的表显示了哪些协议允许检测策略映射，还提供了指向相关配置说明的链接。如果希望配置这些高级功能，请首先创建映射，再配置检测。

过程

步骤 1 依次选择 **配置 > 防火墙 > 服务策略规则**。

步骤 2 打开一个规则。

- 要编辑默认全局策略，请在 Global 文件夹中选择“inspection_default”规则，然后点击 **Edit**。
- 要创建新规则，请依次点击 **Add > Add Service Policy Rule**。继续运行向导，转到 Rules 页面。
- 如果有其他检测规则或有要添加检测的规则，请选择该规则并点击 **Edit**。

如果要匹配非标准端口，请创建适用于非标准端口的新规则。有关每个检测引擎的标准端口，请参阅[默认检测和 NAT 限制](#)，第 312 页。

必要时可以将多个规则整合在同一服务策略中，因此可以创建一个规则来匹配某些流量，创建另一个规则来匹配不同流量。但是，如果流量匹配包含检测操作的某个规则，然后匹配也包含检测操作的另一个规则，将会仅使用第一个匹配的规则。

如果实施的是 RADIUS 计费检测，请改为创建一个管理服务策略规则。请参阅[配置 RADIUS 计费检测](#)，第 405 页。

步骤 3 在 Rule Actions 向导页面或选项卡上，选择 **Protocol Inspection** 选项卡。**步骤 4** （要更改使用中的策略）如果要编辑任何使用中的策略来使用不同的检测策略映射，必须禁用原有检测，然后为其提供新的检测策略映射名称并重新启用这项检测：

- 取消选中相应协议的复选框。
- 点击 **OK**。
- 点击 **Apply**。
- 重复这些步骤以返回到 **Protocol Inspections** 选项卡。

步骤 5 选择要应用的检测类型。

只能对默认检测流量类选择多个选项。

某些检测引擎允许您在对流量应用检测时控制其他参数。点击检测类型的 **Configure**，可配置检测策略映射及其他选项。可以选择现有映射，或者创建新的映射。可以从 **Configuration > Firewall > Objects > Inspect Maps** 列表预定义检测策略映射。

下表列出了可检测的协议，指明这些协议是允许检测策略映射还是检测类映射，还提供了指向相关配置详细信息的链接。

表 13: 检测协议

协议	支持检测策略映射	支持检测类映射	注
CTIQBE	否	否	请参阅 CTIQBE 检测 ，第 359 页。
云网络安全	支持	支持	如果要启用 ScanSafe（云网络安全），请执行以下主题中介绍的操作步骤而不要执行此步骤： 配置向云网络安全发送流量的服务策略 ，第 145 页。列出的该操作步骤说明了全面策略配置，包括如何配置策略检测映射。
DCERPC	是	支持	请参阅 DCERPC 检测 ，第 328 页。

协议	支持检测策略映射	支持检测类映射	注
Diameter	支持	支持	请参阅 Diameter 检测 ，第 383 页。 如果要检测加密的 Diameter 流量，请选择 Enable encrypted traffic inspection 并选择 TLS 代理（如有需要，可点击 Manage 创建一个 TLS 代理）。
DNS	支持	支持	请参阅 DNS 检测 ，第 330 页。 如果使用僵尸网络流量过滤器，请选择 Enable DNS snooping 。我们建议仅在外部 DNS 请求经过的接口上启用 DNS 监听。在所有 UDP DNS 流量（包括流向内部 DNS 服务器的流量）上启用 DNS 监听会为 ASA 形成不必要的负载。例如，如果 DNS 服务器位于某个外部接口，应该对该外部接口的所有 UDP DNS 流量启用具有监听功能的 DNS 检测。
ESMTP	是	否	请参阅 SMTP 和扩展 SMTP 检测 ，第 350 页。
FTP	支持	支持	请参阅 FTP 检测 ，第 333 页。 选择 Use Strict FTP 以选择检测策略映射。严格 FTP 可防止 Web 浏览器在 FTP 请求中发送嵌入式命令，从而提高受保护网络的安全。
GTP	是	否	请参阅 GTP 检测概述 ，第 379 页。
H.323 H.225	支持	支持	请参阅 H.323 检测 ，第 360 页。
H.323 RAS	支持	支持	请参阅 H.323 检测 ，第 360 页。
HTTP	支持	支持	请参阅 HTTP 检测 ，第 337 页。
ICMP	否	否	请参阅 ICMP 检测 ，第 341 页。
ICMP 错误	否	否	请参阅 ICMP 错误检测 ，第 341 页。
ILS	否	否	请参阅 ILS 检测 ，第 342 页。
IM	支持	支持	请参阅 即时消息检测 ，第 342 页。
IP 选项	是	否	请参阅 IP 选项检测 ，第 344 页。
IPSec 直通	是	否	请参阅 IPsec 穿透检测 ，第 346 页。
IPv6	是	否	请参阅 Ipv6 检测 ，第 347 页。

协议	支持检测策略映射	支持检测类映射	注
LISP	是	否	有关配置 LISP 的详细信息（包括检测），请参阅一般配置指南中的“集群”一章。
M3UA	是	否	请参阅 M3UA 检测 ，第 383 页。
MGCP	是	否	请参阅 MGCP 检测 ，第 364 页。
NetBIOS	是	否	请参阅 NetBIOS 检测 ，第 349 页。
PPTP	否	否	请参阅 PPTP 检测 ，第 349 页。
RADIUS 记账	是	否	请参阅 RADIUS 计费检测概述 ，第 385 页。 RADIUS 记账检测仅适用于管理服务策略。必须选择一个策略映射来实施这项检测。
RSH	否	否	请参阅 RSH 检测 ，第 350 页。
RTSP	是	否	请参阅 RTSP 检测 ，第 366 页。
SCCP（瘦客户端）	是	否	请参阅 瘦客户端控制协议 (SCCP) 检测 ，第 373 页。 如果要检测加密 SCCP 流量，请选择 Enable encrypted traffic inspection 并选择 TLS 代理（如有必要，点击 Manage 创建 TLS 代理）。
SCTP	是	否	请参阅 SCTP 应用层检测 ，第 382 页。
SIP	支持	支持	请参阅 SIP 检测 ，第 369 页。 如果要检测加密 SIP 流量，请选择 Enable encrypted traffic inspection 并选择 TLS 代理（如有必要，点击 Manage 创建 TLS 代理）。
SNMP	是	否	请参阅 SNMP 检测 ，第 354 页。
SQLNET	否	否	请参阅 SQL*Net 检测 ，第 354 页。
STUN	否	否	请参阅 STUN 检测 ，第 376 页。
SUNRPC	否	否	请参阅 Sun RPC 检测 ，第 355 页。 默认类映射包括 UDP 端口 111；如果要为 TCP 端口 111 启用 Sun RPC 检测，需要创建一个匹配 TCP 端口 111 的新类映射，将该类添加到策略中，再向该类应用 SUNRPC 检测。
TFTP	否	否	请参阅 TFTP 检测 ，第 356 页。

协议	支持检测策略映射	支持检测类映射	注
WAAS	否	否	启用 TCP 选项 33 解析。部署思科广域应用服务产品时使用。
XDMCP	否	否	请参阅 XDMCP 检测 ，第 356 页。
VXLAN	否	否	请参阅 VXLAN 检测 ，第 357 页。

步骤 6 点击 **OK** 或 **Finish** 以保存服务策略规则。

配置正则表达式

正则表达式定义文本字符串的模式匹配。可以在某些协议检测映射中使用这些表达式根据字符串（例如，URL 或特定报头字段的内容）来匹配数据包。

创建正则表达式

正则表达式可逐字地完全匹配文本字符串，或者，可以使用 *metacharacters* 来匹配文本字符串的多个变体。可以使用正则表达式匹配某些应用流量的内容，例如，可以匹配 HTTP 数据包中的 URL 字符串。

开始之前

有关将正则表达式匹配数据包时对性能造成影响的信息，请参阅命令参考中的 **regex** 命令。一般来说，匹配长输入字符串或尝试匹配大量的正则表达式将会降低系统性能。



注释 为了优化性能，ASA 可在去模糊化的 URL 中搜索。去模糊化处理将多个正斜杠 (/) 压缩为一个斜杠。对于通常使用双斜杠的字符串（例如“http://”），请务必搜索“http:/”。

下表列出了有特殊意义的元字符。

表 14: 正则表达式元字符

字符	说明	注
.	点	匹配任何单个字符。例如， d.g 匹配 dog、dag、dtg 以及任何含有这些字符的单词，如 doggonnit。

字符	说明	注
<i>(exp)</i>	子表达式	子表达式将字符与其周围的字符分隔开，从而可以在子表达式上使用其他元字符。例如， d(o a)g 匹配 dog 和 dag ，但是， do ag 匹配 do 和 ag 。子表达式还可以与重复限定符配合使用，以区分意味着重复的字符。例如， ab(xy){3}z 匹配 abxyxyxyz 。
	交替	匹配其分隔的任意一个表达式。例如， dog cat 匹配 dog 或 cat 。
?	问号	一个限定符，表示前面有 0 个或 1 个表达式。例如， lo?se 匹配 lse 或 lose 。
*	星号	一个限定符，表示前面有 0 个、1 个或任意数量的表达式。例如， lo*se 匹配 lse 、 lose 、 loose 等等。
+	加号	一个限定符，表示前面至少有 1 个表达式。例如， lo+se 匹配 lose 和 loose ，但不匹配 lse 。
{ <i>x</i> } 或 { <i>x</i> ,}	最小重复限定符	至少重复 <i>x</i> 次。例如， ab(xy){2,}z 匹配 abxyxyz 、 abxyxyxyz 等等。
[<i>abc</i>]	字符类	匹配方括号中的任意字符。例如， [abc] 匹配 a 、 b 或 c 。
[^ <i>abc</i>]	求反字符类	匹配不包含在方括号中的单个字符。例如， [^abc] 匹配 a 、 b 或 c 以外的任意字符。 [^A-Z] 匹配非大写字母形式的任意单个字符。
[<i>a-c</i>]	字符范围类	匹配范围内的任意字符。 [a-z] 匹配任意小写字母。可以混合使用字符和字符范围： [abcq-z] 匹配 a 、 b 、 c 、 q 、 r 、 s 、 t 、 u 、 v 、 w 、 x 、 y 和 z ， [a-cq-z] 也是匹配这些字符。 破折号(-)字符仅在是在括号中的最后一个或第一个字符时，才是原义字符：例如， [abc-] 或 [-abc] 。
“ ”	引号	保留字符串中的尾随空格或前导空格。例如， " test" 在查找匹配时会保留前导空格。
^	脱字号	指定行首。
\	转义字符	当与元字符一起使用时，可以匹配原义字符。例如， \[匹配左方括号。
<i>char</i>	字符	当字符不是元字符时，匹配原义字符。

字符	说明	注
\r	回车符	匹配回车符 0x0d。
\n	换行符	匹配换行符 0x0a。
\t	Tab	匹配制表符 0x09。
\f	换页符	匹配换页符 0x0c。
\xNN	转义的十六进制数字	匹配十六进制的 ASCII 字符（必须是两位数）。
\NNN	转义的八进制数字	匹配八进制的 ASCII 字符（必须是三位数）。例如，字符 040 代表空格。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 正则表达式。

步骤 2 在 Regular Expressions 区域，执行以下操作之一：

- 选择 **Add**，添加新对象。输入名称和说明（后者为可选项）。
- 选择现有的对象，然后点击 **Edit**。

步骤 3 在 **Value** 字段中输入正则表达式，或者点击 **Build** 获取有关创建表达式的帮助。

正则表达式最多可包含 100 个字符。

如果点击 **Build**，请按照以下过程创建表达式：

- 在 **Build Snippet** 区域，使用以下选项创建表达式的组成部分。在本节末尾的 **Snippet Preview** 区域可查看正在构建的表达式。
 - **Starts at the beginning of the line (^)** - 使用脱字号 (^) 元字符指明代码片断应该始于行首。请务必使用此选项在正则表达式开头插入任意代码片断。
 - **Specify Character String** - 如果尝试匹配特定字符串（例如字词或短语），请输入字符串。
如果文本字符串中有您想用作原义字符的任何元字符，请选择 **Escape Special Characters**，在这些元字符前面添加反斜杠 (\) 转义字符。例如，如果输入 “example.com”，此选项会将其转换为 “example\.com”。
如果要匹配大写和小写字母，请选择 **Ignore Case**。例如，“cats” 将被转换为 “[cC][aA][tT][sS]”。
 - **Specify Character** - 如果尝试匹配特定类型的字符或字符集，而不是匹配特定短语，请选择此选项并使用以下选项对字符进行识别：
 - **Negate the character** - 指明不要匹配识别的字符。

- **Any character (.)** - 插入句点 (.) 元字符以匹配任意字符。例如，**d.g** 匹配 dog、dag、dtg 以及任何含有这些字符的单词，如 doggonnit。
 - **Character set** - 插入字符集。文本可匹配字符集中的任意字符。例如，如果指定 **[0-9A-Za-z]**，该代码片断会匹配 A 到 Z（不区分大小写）之间的任意字符或 0 到 9 之间的任意数字。**[\n\r\t]** 字符集匹配换行符、换页符、回车符或制表符。
 - **Special character** - 插入需要转义的字符，包括 \、?、*、+、|、.、[、(或 ^。转义字符为反斜杠 (\)；如果选择此选项，会自动输入转义字符。
 - **Whitespace character** - 空白字符包括 \n（换行符）、\f（换页符）、\r（回车符）或 \t（制表符）。
 - **Three digit octal number** - 匹配八进制的 ASCII 字符（最多可以是三位数）。例如，字符 \040 代表空格。反斜杠 (\) 是自动输入的。
 - **Two digit hexadecimal number** - 匹配十六进制的 ASCII 字符（必须是两位数）。反斜杠 (\) 是自动输入的。
 - **Specified character** - 输入任意单个字符。
- b) 使用以下按钮之一将代码片断添加到正则表达式框中。请注意，也可以直接键入正则表达式。
- **Append Snippet** - 将代码片断添加到正则表达式结尾。
 - **Append Snippet as Alternate** - 将代码片断添加到正则表达式结尾，代码片段与表达式之间用竖线 (|) 分隔（这将会匹配竖线分隔的任何一个表达式）。例如，**dog|cat** 匹配 dog 或 cat。
 - **Insert Snippet at Cursor** - 在光标处插入代码片断。
- c) 继续按照上一个步骤添加代码片段，直至表达式完整。
- d) （可选。）在 **Selection Occurrences** 中，选择表达式或其中一部分必须匹配被视为匹配的文本的频率。选择 Regular Expression 字段中的文本，点击以下选项之一，然后点击 **Apply to Selection**。例如，如果正则表达式是 “test me”，而您选择 “me” 并应用 **One or more times**，正则表达式将更改为 “test (me)+”。
- **Zero or one times (?)** - 前面有 0 个或 1 个表达式。例如，**lo?se** 匹配 lse 或 lose。
 - **One or more times (+)** - 前面至少有 1 个表达式。例如，**lo+se** 匹配 lose 和 loose，但不匹配 lse。
 - **Any number of times (*)** - 前面有 0 个、1 个或任意数量的表达式。例如，**lo*se** 匹配 lse、lose、loose 等等。
 - **At least** - 至少重复 x 次。例如，**ab(xy){2,}z** 匹配 abxyxyz、abxyxyxyz 等等。
 - **Exactly** - 准确重复 x 次。例如，**ab(xy){3}z** 匹配 abxyxyxyz。
- e) 点击 **Test** 验证表达式是否匹配预期的文本。如果测试不成功，可以尝试在测试对话框中编辑表达式，或者返回到表达式构建器。如果在文本对话中编辑表达式并点击 **OK**，将会保存所做的编辑并反映在表达式构建器中。

f) 点击 **OK**。

创建正则表达式类映射

正则表达式类映射识别一个或多个正则表达式，是正则表达式对象的集合。在很多情况下，可以使用正则表达式类映射代替正则表达式对象。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 正则表达式。

步骤 2 在 Regular Expressions Classes 区域，执行以下操作之一：

- 选择 **Add**，添加新的类映射。输入名称和说明（后者为可选项）。
- 选择现有的类映射，然后点击 **Edit**。

步骤 3 在映射中选择所需的表达式，然后点击 **Add**。删除不想要的任何类映射。

步骤 4 点击 **OK**。

监控检测策略

要监控检测服务策略，请输入以下命令。依次选择工具 > 命令行界面输入以下命令。有关详细的语法和示例，请参阅 Cisco.com 上的命令参考。

- **show service-policy inspect protocol**

显示检测服务策略的统计信息。*protocol* 指来自检测命令的协议，例如 **dns**。但是，并非所有检测协议的统计信息均通过此命令显示。例如：

```
asa# show service-policy inspect dns

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
    message-length maximum client auto, drop 0
    message-length maximum 512, drop 0
    dns-guard, count 0
    protocol-enforcement, drop 0
    nat-rewrite, count 0
asa#
```

- **show conn**

显示流经设备的流量的当前连接。此命令包括各种关键字，让您可获取有关各种协议的信息。

- 用于特定检测协议的其他命令：
 - **show ctiqbe**
显示 CTIQBE 检测引擎所分配媒体连接的相关信息。
 - **show h225**
显示 H.225 会话的相关信息。
 - **show h245**
显示终端使用慢启动 (slow start) 建立的 H.245 会话的相关信息。
 - **show h323 ras**
显示网守与其 H.323 终端之间建立的 H.323 RAS 会话的连接信息。
 - **show mgcp {commands |sessions }**
显示命令队列中的 MGCP 命令数量或现有的 MGCP 会话数量。
 - **show sip**
显示 SIP 会话的相关信息。
 - **show skinny**
显示瘦小客户端控制协议 (SCCP) 会话的信息。
 - **show sunrpc-server active**
显示为 Sun RPC 服务打开的针孔。

应用检测的历史

功能名称	版本	说明
检测策略映射	7.2(1)	引入了检测策略映射。引入了以下命令： class-map type inspect 。
正则表达式和策略映射	7.2(1)	引入了正则表达式和策略映射，将其用于检查策略映射下。引入了以下命令： class-map type regex、regex、match regex 。
检测策略映射的 match any	8.0(2)	引入了关键字 match any ，与检测策略映射一起使用：流量可以匹配一个或多个条件以匹配类映射。过去，仅 match all 可用。



第 15 章

基本互联网协议检测

以下主题介绍基本互联网协议的应用检测。有关为何需要对某些协议进行检测以及应用检测的总体方法的信息，请参阅[应用层协议检测入门](#)，第 309 页。

- [DCERPC 检测](#)，第 328 页
- [DNS 检测](#)，第 330 页
- [FTP 检测](#)，第 333 页
- [HTTP 检测](#)，第 337 页
- [ICMP 检测](#)，第 341 页
- [ICMP 错误检测](#)，第 341 页
- [ILS 检测](#)，第 342 页
- [即时消息检测](#)，第 342 页
- [IP 选项检测](#)，第 344 页
- [IPsec 穿透检测](#)，第 346 页
- [Ipv6 检测](#)，第 347 页
- [NetBIOS 检测](#)，第 349 页
- [PPTP 检测](#)，第 349 页
- [RSH 检测](#)，第 350 页
- [SMTP 和扩展 SMTP 检测](#)，第 350 页
- [SNMP 检测](#)，第 354 页
- [SQL*Net 检测](#)，第 354 页
- [Sun RPC 检测](#)，第 355 页
- [TFTP 检测](#)，第 356 页
- [XDMCP 检测](#)，第 356 页
- [VXLAN 检测](#)，第 357 页
- [基本互联网协议检测的历史](#)，第 357 页

DCERPC 检测

DCERPC 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用这项检测。可以简单地编辑默认全局检测策略来添加 DCERPC 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

以下各节介绍 DCERPC 检测引擎。

DCERPC 概述

Microsoft 远程过程调用 (MSRPC) 基于 DCERPC，是 Microsoft 分布式客户端和服务器应用广泛使用的协议，允许软件客户端在服务器上远程执行程序。

这通常涉及查询称为终端映射器的服务器（用于侦听已知端口号，以获取所需服务的动态分配网络信息）的客户端。然后，客户端建立与提供服务的服务器实例之间的辅助连接。安全设备允许相应的端口号以及网络地址，如有必要，还会为辅助连接应用 NAT。

DCERPC 检测引擎在已知 TCP 端口 135 上检测 EPM 与客户端之间的本地 TCP 通信。支持客户端的 EPM 映射和查找操作。客户端和服务器可位于任何安全区域。从适用的 EPM 响应消息接收嵌入式服务器 IP 地址和端口号。由于客户端可能尝试多次连接到 EPM 返回的服务器端口，因此，允许使用可配置超时的多个针孔。

DCE 检测支持以下通用唯一标识符 (UUID) 和消息：

- 终端映射器 (EPM) UUID。支持所有 EPM 消息。
- ISystemMapper UUID（非 EPM）。支持的消息如下：
 - RemoteCreateInstance opnum4
 - RemoteGetClassObject opnum3
- OxidResolver UUID（非 EPM）支持的消息如下：
 - ServerAlive2 opnum5
- 不包含 IP 地址或端口信息的任何消息，因为这些消息不需要检测。

配置 DCERPC 检测策略映射

要指定其他 DCERPC 检测参数，请创建 DCERPC 检测策略映射。然后，可以在启用 DCERPC 检测时应用所创建的检测策略映射。

在定义流量匹配条件时，可以创建类映射或者直接在策略映射中包括匹配语句。创建类映射与直接在检测策略映射中定义流量匹配的差别在于，可以重复使用类映射。以下程序介绍检测策略映射，但也说明了类映射中可用的流量匹配条件。要创建类映射，请依次选择配置 > 防火墙 > 对象 > 类映射 > DCERPC。



提示 除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > DCERPC。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射以查看映射内容。可以直接更改安全级别，或者点击 **Customize** 编辑映射。此操作过程的剩余步骤假设要自定义或添加映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 在 DCERPC Inspect Map 对话框的 **Security Level** 视图中，选择最符合所需配置的级别。

如果预设级别之一符合要求，执行到这一步即可。只需点击 **OK**，跳过此操作过程的剩余步骤，并将映射用于服务策略规则中以执行 DCERPC 检测。

如需进一步自定义设置，请点击 **Details** 并继续执行该程序。

提示 使用 **UUID Filtering** 按钮，可快捷地配置消息过滤，本程序后面将介绍相关内容。

步骤 5 配置所需选项。

- **Pinhole Timeout** - 设置针孔超时。由于客户端可将终端映射器返回的服务器信息用于多个连接，因此，超时值可根据客户端应用环境进行配置。超时范围是 0:0:1 到 1193:0:0。
- **Enforce endpoint-mapper service** - 是否在捆绑期间执行终端映射器服务，从而仅处理其服务流量。
- **Enable endpoint-mapper service lookup** - 是否启用终端映射器服务的查找操作。还可以执行服务查找的超时。如果未配置超时，将会使用针孔超时。

步骤 6 （可选。）点击 **Inspections** 选项卡，并定义要针对特定消息类型采取的操作。

您可以通过基于 DCERPC 类映射或直接在检测映射中配置匹配的方式定义流量匹配条件。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

b) 选择 **Single Match** 直接定义条件，或选择 **Multiple Match**，在后者情况下可选择定义条件的 DCERPC 类映射。

- c) 如果在这里定义条件，请选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。然后，选择所需的 UUID：
- **ms-rpc-epm-** 匹配 Microsoft RPC EPM 消息。
 - **ms-rpc-isystemactivator-** 匹配 ISystemMapper 消息。
 - **ms-rpc-oxidresolver-** 匹配 OxidResolver 消息。
- d) 选择是 **Reset** 还是 **Log** 连接。如果选择重置连接，您也可以启用日志记录。重置连接将丢弃数据包、关闭连接并向服务器或客户端发送 TCP 重置。
- e) 点击 **OK** 添加该条件。根据需要重复上述步骤。

步骤 7 点击 **OK**。

这样即可将检测映射用于 DCERPC 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

DNS 检测

默认情况下，DNS 检测已启用。仅在需要非默认处理的情况下，才需要配置这项检测。以下各节介绍 DNS 应用检测。

DNS 检测默认设置

默认情况下，启用 DNS 检测，使用 `preset_dns_map` 检测类映射：

- 最大 DNS 消息长度为 512 字节。
- 禁用通过 TCP 的 DNS 检测。
- 最大客户端 DNS 消息长度是自动设置的，以与资源记录匹配。
- DNS Guard 已启用，因此 ASA 在转发 DNS 应答后立即终止与 DNS 查询相关的 DNS 会话。另外，ASA 还会监控消息交换，以确保 DNS 应答的 ID 与 DNS 查询的 ID 匹配。
- 根据 NAT 配置的 DNS 记录转换已启用。
- 协议执行已启用，使得可以进行 DNS 消息格式检查（具体检查内容包括：域名长度不得超过 255 个字符，标签长度不得超过 63 个字符，压缩检查和循环指针检查）。

配置 DNS 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 DNS 检测策略映射来自定义 DNS 检测操作。

或者可以创建 DNS 检测类映射来定义 DNS 检测的流量类。另一种方法是，直接在 DNS 检测策略映射中定义流量类。创建类映射与直接在检测映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。虽然此过程介绍了检测映射，但类映射中使用的匹配条件与 **Inspection** 选项卡相关步骤中介绍的匹配条件相同。您可以通过以下两种方法来配置 DNS 类映射：依次选择配置 > 防火墙 > 对象 > 类映射 > DNS；或在配置检测映射时创建它们。



提示 除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > DNS。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射以查看映射内容。可以直接更改安全级别，或者点击 **Customize** 编辑映射。此操作过程的剩余步骤假设要自定义或添加映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 在 DNS Inspect Map 对话框的 **Security Level** 视图中，选择最符合所需配置的级别。默认级别为 Low。

如果预设级别之一符合要求，执行到这一步即可。只需点击 **OK**，跳过此操作过程的剩余步骤，并将映射用于服务策略规则中以执行 DNS 检测。

如果需要进一步自定义设置，请点击 **Details** 并继续执行此操作步骤。

步骤 5 点击 **Protocol Conformance** 选项卡并选择所需的选项：

- **Enable DNS guard function** - 使用 DNS Guard，ASA 可在转发 DNS 应答后立即清除与 DNS 查询相关的 DNS 会话。另外，ASA 还会监控消息交换，以确保 DNS 应答的 ID 与 DNS 查询的 ID 匹配。
- **Enable NAT re-write function** - 根据 NAT 配置转换 DNS 记录。
- **Enable protocol enforcement** - 启用 DNS 消息格式检查（具体检查内容包括：域名长度不得超过 255 个字符，标签长度不得超过 63 个字符，压缩检查和循环指针检查）。
- **Randomize the DNS identifier for DNS query.**
- **Enable TCP inspection** - 启用 TCP 上的 DNS 流量检测。确保 DNS/TCP 端口 53 流量是要应用 DNS 检测的类的一部分。该检测的默认类包括 TCP/53。

- **Enforce TSIG resource record to be present in DNS message** - 可以丢弃或记录不符合要求的数据包，或者还可以记录丢弃的数据包。

步骤 6 点击 **Filtering** 选项卡并选择所需的选项。

- **Global Settings** - 选择是否丢弃超过指定最大长度（512 至 65535 字节）的数据包，无论数据包是来自客户端还是服务器的数据包。
- **Server Settings - Drop packets that exceed specified maximum length 和 Drop packets sent to server that exceed length indicated by the RR** - 设置最大服务器 DNS 消息长度（512 至 65535 字节），或者将最大长度设置为资源记录中的值。如果启用这两个设置，将使用较小的值。
- **Client Settings - Drop packets that exceed specified maximum length 和 Drop packets sent to server that exceed length indicated by the RR** - 设置最大客户端 DNS 消息长度（512 至 65535 字节），或者将最大长度设置为资源记录中的值。如果启用这两个设置，将使用较小的值。

步骤 7 点击**不匹配率**选项卡，并选择在 DNS ID 不匹配率超过指定阈值时是否启用日志记录。例如，可以将阈值设置为每 3 秒 30 次不匹配。

步骤 8 点击 **Inspections** 选项卡，并定义要基于流量特性实施的特定检测。

可以根据 DNS 类映射定义流量匹配条件，或者直接在检测映射中配置匹配，还可以同时使用这两种方法。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

b) 选择 **Single Match** 直接定义条件，或选择 **Multiple Match**，在后者情况下可选择 DNS 类映射来定义条件。

c) 如果在这里定义条件，请选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。例如，如果对字符串“example.com”选择了 No Match，将会从类映射排除任何包含“example.com”的流量。然后，按如下方式配置条件：

- **Header Flag** - 选择标志是否应等于或包含指定值，然后选择报头标志名称或输入报头的十六进制值（0x0 至 0xffff）。如果选择多个报头值，“equals”要求数据包中存在所有标志，“contains”要求数据包中存在任意一个标志。报头标志名称是 **AA**（授权应答）、**QR**（查询）、**RA**（可用递归）、**RD**（所需递归）、**TC**（截断）。
- **Type** - 数据包中 DNS Type 字段的名称或值。字段名称是 **A**（IPv4 地址）、**AXFR**（完整区域传送）、**CNAME**（规范名称）、**IXFR**（增量区域传送）、**NS**（授权域名服务器）、**SOA**（授权区域起始）或 **TSIG**（事务数字签名）。DNS Type 字段中的值是 0 到 65535 之间的任意数字：可输入具体值或值范围。
- **Class** - 数据包中 DNS Class 字段的名称或值。“互联网”是唯一可用于此字段的名称。DNS Class 字段中的值是 0 到 65535 之间的任意数字：可输入具体值或值范围。
- **Question** - DNS 消息的问题部分。

- Resource Record - DNS 资源记录。选择是否匹配资源记录的 additional、answer 或 authority 部分。

- d) 选择要对匹配的流量执行的主要操作：丢弃数据包，断开连接，掩蔽（仅适用于报头标志匹配项）或者不执行任何操作。
- e) 选择是启用还是禁用日志记录。如果要强制 TSIG，必须禁用日志记录。
- f) 选择是否强制要求必须有 TSIG 资源记录。可以丢弃数据包，记录数据包或者丢弃并记录数据包。要强制 TSIG，通常必须选择 **Primary Action: None** 和 **Log: Disable**。但是，对于报头标志匹配项，可以将 TSIG 强制与掩蔽主要操作配合使用。
- g) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 9 点击 **Umbrella 连接** 选项卡，并在云中启用与思科 Umbrella 的连接。

仅当您在 **配置 > 防火墙 > 对象 > Umbrella** 页面上配置了思科 Umbrella 连接时，此选项卡上的选项才起作用。然后，您必须配置此选项卡上的选项，让设备注册思科 Umbrella，以便设备能够将 DNS 查询重定向至思科 Umbrella。然后，思科 Umbrella 可以应用基于 FQDN 的安全策略。有关详细信息，请参阅 [思科 Umbrella](#)，第 125 页。

- **Umbrella** - 启用思科 Umbrella。可以选择在 **Umbrella 标记** 字段中指定要应用于设备的思科 Umbrella 策略的名称。如果未指定策略，系统将应用默认策略。注册后，Umbrella 设备 ID 会显示在标签旁边。
- **启用 Dnscrypt** - 启用 DNSCrypt，为设备和思科 Umbrella 之间的连接加密。启用 DNSCrypt 将使用 Umbrella 解析器启动密钥交换线程。密钥交换线程每小时执行与解析器的握手，并使用新密钥来更新设备。由于 DNSCrypt 使用 UDP/443，您必须确保用于 DNS 检测的类映射包含该端口。请注意，默认检测类已在 DNS 检测中包括 UDP/443。

步骤 10 在 DNS Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 DNS 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅 [配置应用层协议检测](#)，第 316 页。

FTP 检测

默认情况下，FTP 检测已启用。仅在需要非默认处理的情况下，才需要配置这项检测。以下各节介绍 FTP 检测引擎。

FTP 检测概述

FTP 应用检测用于检测 FTP 会话和执行四种任务：

- 为 FTP 数据传输准备动态辅助数据连接信道。这些信道的端口是通过 PORT 或 PASV 命令协商的。这些信道根据文件上传、文件下载或目录列表事件进行分配。
- 跟踪 FTP 命令响应序列。
- 生成审计追踪。
 - 为检索或上传的每个文件生成审核记录 303002。
 - 如果辅助动态信道准备因内存不足而失败，将会生成审核记录 201005。
- 转换嵌入式 IP 地址。



注释 如果禁用 FTP 检测，出站用户只能在被动模式下启动连接，而所有入站 FTP 将被禁用。

严格 FTP

严格 FTP 可防止 Web 浏览器在 FTP 请求中发送嵌入式命令，从而提高受保护网络的安全性。要启用严格 FTP，请在“配置”>“防火墙”>“服务策略规则”>“编辑服务策略规则”>“规则操作”>“协议检测”选项卡中点击 FTP 旁边的配置按钮。

在使用严格 FTP 时，您可以选择指定 FTP 检测策略映射来指定不允许通过 ASA 的 FTP 命令。

严格 FTP 检测将执行以下行为：

- 必须先确认 FTP 命令，然后 ASA 才允许使用新命令。
- ASA 丢弃发送嵌入式命令的连接。
- 检查 227 命令和 PORT 命令，以确保这些命令不显示在错误字符串中。



注意 使用严格 FTP 可能会导致没有严格遵从 FTP RFC 的 FTP 客户端故障。

使用严格 FTP 检测，系统会跟踪以下匿名活动的每个 FTP 命令和响应序列：

- 截断命令 - 检查 PORT 和 PASV 应答命令中逗号的数量是否是五个。如果不是五个，将会截断 PORT 命令并关闭 TCP 连接。
- 错误命令 - 检查 FTP 命令以确定它是否以 <CR><LF> 字符结尾（如 RFC 所要求）。如果不是，将会关闭连接。
- RETR 和 STOR 命令的大小 - 根据某个固定常数检查这些命令的大小。如果命令大小大于该固定常数，将会记录错误消息并关闭连接。
- 命令欺骗 - PORT 命令应始终从客户端发送。如果 PORT 命令是从服务器发送，将会拒绝 TCP 连接。

- 应答欺骗 - PASV 应答命令 (227) 应始终从服务器发送。如果 PASV 应答命令是从客户端发送，将会拒绝 TCP 连接。这样可防止用户执行 “227 xxxxx a1, a2, a3, a4, p1, p2.” 时出现安全漏洞
- TCP 流编辑 - 如果检测到 TCP 流编辑，ASA 将关闭连接。
- 无效的端口协商 - 检查协商的动态端口值是否小于 1024。由于 1 至 1024 范围内的端口号是为已知连接保留的，因此，如果协商的端口在这个范围内，将会释放 TCP 连接。
- 命令管道 - 将 PORT 和 PASV 应答命令中在端口号后显示的字符数与常数值 8 进行比较。如果该字符数大于 8，将会关闭 TCP 连接。
- ASA 将使用一系列 X 替代 FTP 服务器对 SYST 命令的响应，以防该服务器向 FTP 客户端泄露其系统类型。要覆盖此默认行为，请在 FTP 映射中使用 **no mask-syst-reply** 命令。

配置 FTP 检测策略映射

使用严格 FTP 检测可进行 FTP 命令过滤和安全检查，从而提高安全和加强控制。协议符合性包括数据包长度检查、分隔符和数据包格式检查、命令终止符检查以及命令验证。

也支持根据用户值阻止 FTP，这样，FTP 站点可以发布供下载的文件，但仅允许某些用户访问。可以根据文件类型、服务器名称及其他属性阻止 FTP 连接。如果进行检测后 FTP 连接被拒绝，将会生成系统消息日志。

如果希望 FTP 检测允许 FTP 服务器向 FTP 客户端显示其系统类型，并限制允许的 FTP 命令，可以创建并配置 FTP 检测策略映射。然后，可以在启用 FTP 检测时应用所创建的映射。

可以随意创建 FTP 检测类映射来定义 FTP 检测的流量类。另一种方法是，直接在 FTP 检测策略映射中定义流量类。创建类映射与直接在检测映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。虽然此过程介绍了检测映射，但类映射中使用的匹配条件与 **Inspection** 选项卡相关步骤中介绍的匹配条件相同。您可以通过以下两种方法来配置 DNS 类映射：依次选择配置 > 防火墙 > 对象 > 类映射 > **FTP**；或在配置检测映射时创建它们。



提示

除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > **FTP**。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。

- 选择映射以查看映射内容。可以直接更改安全级别，或者点击 **Customize** 编辑映射。此操作过程的剩余步骤假设要自定义或添加映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 在 FTP Inspect Map 对话框的 **Security Level** 视图中，选择最符合所需配置的级别。默认级别为 **High**。

如果预设级别之一符合要求，执行到这一步即可。只需点击 **OK**，跳过此操作过程的剩余步骤，并将映射用于服务策略规则中以执行 FTP 检测。

如果需要进一步自定义设置，请点击 **Details** 并继续执行此操作步骤。

提示 **File Type Filtering** 按钮是配置文件媒体或 MIME 类型检测的快捷方式（下面将会加以说明）。

步骤 5 点击 **Parameters** 选项卡，并选择是否掩蔽来自服务器的问候横幅或对 SYST 命令的应答。

掩蔽这些项目可防止客户端发现可能有助于攻击的服务器信息。

步骤 6 点击 **Inspections** 选项卡，并定义要基于流量特性实施的特定检测。

可以根据 FTP 类映射定义流量匹配条件，或者直接在检测映射中配置匹配，还可以同时使用这两种方法。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

b) 选择 **Single Match** 直接定义条件，或选择 **Multiple Match**，在后者情况下可选择 FTP 类映射来定义条件。

c) 如果在这里定义条件，请选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。例如，如果对字符串“example.com”选择了 **No Match**，将会从类映射排除任何包含“example.com”的流量。然后，按如下方式配置条件：

- **File Name** - 将正在传输的文件的名称与选定的正则表达式或正则表达式类进行匹配。
- **File Type** - 将正在传输的文件的 MIME 或媒体类型与选定的正则表达式或正则表达式类进行匹配。
- **Server** - 将 FTP 服务器名称与选定的正则表达式或正则表达式类进行匹配。
- **User** - 将已登录用户的名称与选定的正则表达式或正则表达式类进行匹配。
- **Request Command** - 数据包中使用的 FTP 命令，可以是以下命令的任意组合：
 - **APPE** - 附加到文件。
 - **CDUP** - 更改为当前工作目录的父目录。
 - **DELE** - 删除服务器上的文件。
 - **GET** - 从服务器获取文件。

- **HELP** - 提供帮助信息。
- **MKD** - 在服务器上创建目录。
- **PUT** - 向服务器发送文件。
- **RMD** - 在服务器上删除目录。
- **RNFR** - 指定“rename-from”文件名
- **RNTO** - 指定“rename-to”文件名
- **SITE** - 用于指定服务器特定命令。此命令通常用于远程管理。
- **STOU** - 用唯一文件名存储文件。

d) 选择是启用还是禁用日志记录。此操作必定会重置连接，从而导致丢弃数据包，关闭连接并向服务器或客户端发送 TCP 重置。

e) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 7 在 FTP Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 FTP 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

HTTP 检测

如果不使用专用模块（例如 ASA CX 或 ASA FirePOWER）来配置 HTTP 检测和应用过滤，可以手动在 ASA 上进行配置。

HTTP 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。但是，默认检测类包括默认 HTTP 端口，因此，只需简单地编辑默认全局检测策略即可添加 HTTP 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。



提示 请勿同时在服务模块和 ASA 上配置 HTTP 检测，因为两者中的检测不兼容。

以下各节介绍 HTTP 检测引擎。

HTTP 检测概述



提示 可以安装执行应用和 URL 过滤（包括 HTTP 检测）的服务模块，例如 ASA CX 或 ASA FirePOWER。ASA 上运行的 HTTP 检测与这些模块不兼容。请注意，使用专用模块配置应用过滤比尝试使用 HTTP 检测策略映射在 ASA 上手动配置要简单的多。

使用 HTTP 检测引擎可防御特定攻击以及与 HTTP 流量相关的其他威胁。

HTTP 应用检测扫描 HTTP 报头和正文，并对数据执行各种检查。这些检查可防止各种 HTTP 构造、内容类型、隧道协议和消息传送协议通过安全设备。

增强型 HTTP 检测功能（又称为应用防火墙，在配置 HTTP 检测策略映射时可使用此功能）有助于防止攻击者使用 HTTP 消息来避开网络安全策略。

HTTP 应用检测可阻止通过隧道传送的应用以及 HTTP 请求和响应中的非 ASCII 字符，从而防止恶意内容到达 Web 服务器。还支持对 HTTP 请求和响应报头中的各个元素进行大小限制、URL 拦截以及 HTTP 服务器报头类型欺骗。

增强型 HTTP 检测验证所有 HTTP 消息是否满足以下条件：

- 符合 RFC 2616 的要求
- 仅使用 RFC 定义的方法。
- 符合其他条件。

配置 HTTP 检测策略映射

要指定消息违反参数时要执行的操作，请创建 HTTP 检测策略映射。然后，可以在启用 HTTP 检测时应用所创建的检测策略映射。

或者可以创建 HTTP 检测类映射来定义 HTTP 检测的流量类。另一种方法是，直接在 HTTP 检测策略映射中定义流量类。创建类映射与直接在检测映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。虽然此过程介绍了检测映射，但类映射中使用的匹配条件与 **Inspection** 选项卡相关步骤中介绍的匹配条件相同。您可以通过以下两种方法来配置 HTTP 类映射：依次选择 **配置 > 防火墙 > 对象 > 类映射 > HTTP**；或在配置检测映射时创建它们。



提示 除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > HTTP。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射以查看映射内容。可以直接更改安全级别，或者点击 **Customize** 编辑映射。此操作过程的剩余步骤假设要自定义或添加映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 在 HTTP Inspect Map 对话框的 **Security Level** 视图中，选择最符合所需配置的级别。默认级别为 Low。

如果预设级别之一符合要求，执行到这一步即可。只需点击 **OK**，跳过此操作过程的剩余步骤，并将映射用于服务策略规则中以执行 HTTP 检测。

如果需要进一步自定义设置，请点击 **Details** 并继续执行此操作步骤。

提示 **URI Filtering** 按钮是配置请求 URI 检测的快捷方式（下面将会加以说明）。

步骤 5 点击 **Parameters** 选项卡并配置所需的选项。

- **Body Match Maximum** - 应在正文匹配中搜索的 HTTP 消息正文中的最大字符数。默认值为 200 字节。字符数量大将会对性能造成明显影响。
- **Check for protocol violations** - 是否验证数据包是否符合 HTTP 协议。对于违规情况，可以断开连接，重置连接或记录连接。断开或重置连接时，还可以启用日志记录。
- **Spoof server string** - 用指定的字符串（最多包含 82 个字符）替换服务器 HTTP 报头值。

步骤 6 点击 **Inspections** 选项卡，并定义要基于流量特性实施的特定检测。

可以根据 HTTP 类映射定义流量匹配条件，或者直接在检测映射中配置匹配，还可以同时使用这两种方法。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

b) 选择 **Single Match** 直接定义条件，或选择 **Multiple Match**，在后者情况下可选择 HTTP 类映射来定义条件。

c) 如果在这里定义条件，请选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。例如，如果对字符串“example.com”选择了 No Match，将会从类映射排除任何包含“example.com”的流量。然后，按如下方式配置条件：

- **Request/Response Content Type Mismatch** - 匹配响应中内容类型与请求的接受字段中 MIME 类型之一不匹配的数据包。

- Request Arguments - 将请求的参数与选定的正则表达式或正则表达式类进行匹配。
- Request Body Length - 匹配请求正文长度大于指定字节数的数据包。
- Request Body - 将请求的正文与选定的正则表达式或正则表达式类进行匹配。
- Request Header Field Count - 匹配请求中的报头字段数量大于指定数量的数据包。可以将字段报头类型与正则表达式或预定义类型进行匹配。预定义类型包括：accept、accept-charset、accept-encoding、accept-language、allow、authorization、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、cookie、date、expect、expires、from、host、if-match、if-modified-since、if-none-match、if-range、if-unmodified-since、last-modified、max-forwards、pragma、proxy-authorization、range、referer、te、trailer、transfer-encoding、upgrade、user-agent、via、warning。
- Request Header Field Length - 匹配请求中的报头字段长度大于指定字节数的数据包。可以将字段报头类型与正则表达式或预定义类型进行匹配。以上列出了适用于 Request Header Field Count 的预定义类型。
- Request Header Field - 将请求中选定报头字段的内容与选定的正则表达式或正则表达式类进行匹配。可以指定预定义报头类型，或者使用正则表达式选择报头。
- Request Header Count - 匹配请求中的报头数量大于指定数量的数据包。
- Request Header Length - 匹配请求中的报头长度大于指定字节数的数据包。
- Request Header Non-ASCII - 匹配请求中的报头包含非 ASCII 字符的数据包。
- Request Method - 匹配请求方法与预定义类型或选定的正则表达式或正则表达式类相匹配的数据包。预定义类型包括：bcopy、bdelete、bmove、bpropfind、bproppatch、connect、copy、delete、edit、get、getattribute、getattributenames、getproperties、head、index、lock、mkcol、mkdir、move、notify、options、poll、post、propfind、proppatch、put、revadd、relabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。
- Request URI Length - 匹配请求 URI 长度大于指定字节数的数据包。
- Request URI - 将请求 URI 的内容与选定的正则表达式或正则表达式类进行匹配。
- Request Body - 将请求正文与选定的正则表达式或正则表达式类或者与 ActiveX 或 Java 小应用程序内容进行匹配。
- Response Body Length - 匹配响应正文长度大于指定字节数的数据包。
- Response Header Field Count - 匹配响应中的报头字段数量大于指定数量的数据包。可以将字段报头类型与正则表达式或预定义类型进行匹配。预定义类型包括：accept-ranges、age、allow、cache-control、connection、content-encoding、content-language、content-length、content-location、content-md5、content-range、content-type、date、etag、expires、last-modified、location、pragma、proxy-authenticate、retry-after、server、set-cookie、trailer、transfer-encoding、upgrade、vary、via、warning、www-authenticate。

- **Response Header Field Length** - 匹配响应中的报头字段长度大于指定字节数的数据包。可以将字段报头类型与正则表达式或预定义类型进行匹配。以上列出了适用于 **Response Header Field Count** 的预定义类型。
- **Response Header Field** - 将响应中选定报头字段的内容与选定的正则表达式或正则表达式类进行匹配。可以指定预定义报头类型，或者使用正则表达式选择报头。
- **Response Header Count** - 匹配响应中的报头数量大于指定数量的数据包。
- **Response Header Length** - 匹配响应中的报头长度大于指定字节数的数据包。
- **Response Header Non-ASCII** - 匹配响应中的报头包含非 ASCII 字符的数据包。
- **Response Status Line** - 将响应状态的内容与选定的正则表达式或正则表达式类进行匹配。

- d) 选择是否断开连接、重置连接或记录连接。对于断开连接和重置连接这两种情况，可以启用或禁用日志记录。
- e) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 7 在 HTTP Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 HTTP 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

ICMP 检测

ICMP 检测引擎允许 ICMP 流量具有“会话”，这样可以像对 TCP 和 UDP 流量那样对这种流量进行检测。如果没有 ICMP 检测引擎，我们建议您在 ACL 中不要允许 ICMP 通过 ASA。如果不进行状态检测，ICMP 可能被用于攻击网络。ICMP 检测引擎确保每个请求只有一个响应，并确保序列号是正确的。

但是，即使已启用 ICMP 检测，也绝不会检测定向到 ASA 接口的 ICMP 流量。因此，到接口的 ping（回应请求）可能会在特定情况下失败，例如，如果回应请求来自 ASA 可以通过备用默认路由到达的源。

有关启用 ICMP 检测的信息，请参阅[配置应用层协议检测](#)，第 316 页。

ICMP 错误检测

当启用 ICMP 错误检测时，ASA 将基于 NAT 配置为发送 ICMP 错误消息的中间跃点创建转换会话。ASA 将使用转换的 IP 地址覆盖数据包。

禁用时，ASA 不会为生成 ICMP 错误消息的中间节点创建转换会话。内部主机与 ASA 之间的中间节点生成的 ICMP 错误消息将会到达外部主机，而不占用任何其他 NAT 资源。如果外部主机使用 `tracert` 命令来跟踪连接 ASA 内部目标的跃点，这种方式则不合适。当 ASA 不转换中间跃点时，显示的所有中间跃点将带有映射目标 IP 地址。

有关启用 ICMP 错误检测的信息，请参阅[配置应用层协议检测](#)，第 316 页。

ILS 检测

互联网定位器服务 (ILS) 检测引擎为使用 LDAP 与 ILS 服务器交换目录信息的 Microsoft NetMeeting、SiteServer 和 Active Directory 产品提供 NAT 支持。在 ILS 检测中不能使用 PAT，因为只有 LDAP 数据库会存储 IP 地址。

为了搜索响应，当 LDAP 服务器位于外部时，请考虑使用 NAT 以允许内部对等体在注册到外部 LDAP 服务器时进行本地通信。如果无需使用 NAT，我们建议您关闭检测引擎以提供更好的性能。

当 ILS 服务器位于 ASA 边界内时，可能需要进行其他配置。这就需要提供一个孔来让外部客户端在指定的端口（通常为 TCP 389）上访问 LDAP 服务器。



注释

由于 ILS 流量（H225 呼叫信号）仅出现在辅助 UDP 信道上，因此，过了 TCP 非活动间隔后，TCP 连接将断开。默认情况下，此间隔为 60 分钟，且可使用 `TCP timeout` 命令进行调整。在 ASDM 中，可在 **Configuration > Firewall > Advanced > Global Timeouts** 窗格上完成此操作。

ILS 检测存在如下局限性：

- 不支持推荐请求和响应。
- 多个目录中的用户不统一。
- NAT 无法标识多个目录中具有多个身份的单一用户。

有关启用 ILS 检测的信息，请参阅[配置应用层协议检测](#)，第 316 页。

即时消息检测

使用即时消息 (IM) 检测引擎可以控制 IM 的网络使用情况，以及阻止机密数据泄露、蠕虫传播和针对公司网络的其他威胁。

IM 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。但是，默认检测类包括默认 IM 端口，因此，只需简单地编辑默认全局检测策略即可添加 IM 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

如果决定实施 IM 检测，还可以配置 IM 检测策略映射来指定消息违反参数时采取的操作。以下操作步骤介绍 IM 检测策略映射。

或者可以创建 IM 检测类映射来定义 IM 检测的流量类。另一种方法是，直接在 IM 检测策略映射中定义流量类。创建类映射与直接在检测映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。以下操作步骤说明了检测映射；类映射与检测映射基本上是相同的，唯一不同之处在于，在类映射中，无需为匹配的流量指定操作。可以通过选择 **Configuration > Firewall > Objects > Class Maps > Instant Messaging (IM)** 配置 IM 类映射。



提示 除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 依次选择 **Configuration > Firewall > Objects > Inspect Maps > Instant Messaging (IM)**。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射并点击 **Edit**。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 定义要根据流量特性实施的特定检测。

可以根据 IM 类映射定义流量匹配条件，或者直接在检测映射中配置匹配，还可以同时使用这两种方法。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

b) 选择 **Single Match** 直接定义条件，或者选择 **Multiple Match**（如果选择后一个选项，需要选择定义条件的 IM 类映射）。点击 **Manage** 创建新的类映射。

c) 如果在这里定义条件，请选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。例如，如果对字符串“example.com”选择了 No Match，将会从类映射排除任何包含“example.com”的流量。然后，配置条件。

- Protocol - 匹配特定 IM 协议的流量，例如 Yahoo Messenger 或 MSN Messenger。
- Service - 匹配特定 IM 服务，例如聊天、文件传输、网络摄像头、语音聊天、会议或游戏。
- Version - 将 IM 消息的版本与选定的正则表达式或正则表达式类进行匹配。

- Client Login Name - 将 IM 消息的源客户端登录名与选定的正则表达式或正则表达式类进行匹配。
 - Client Peer Login Name - 将 IM 消息的目标对等体登录名与选定的正则表达式或正则表达式类进行匹配。
 - Source IP Address - 匹配源 IP 地址和掩码。
 - Destination IP Address - 匹配目标 IP 地址和掩码。
 - Filename - 将 IM 消息的文件名与选定的正则表达式或正则表达式类进行匹配。
- d) 选择是否断开连接、重置连接或记录连接。对于断开连接和重置连接这两种情况，可以启用或禁用日志记录。
- e) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 5 在 IM Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 IM 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

IP 选项检测

您可以配置 IP 选项检测，以便基于数据包信头 IP Options 字段的内容控制允许的 IP 数据包。您可以丢弃包含不需要选项的数据包、清除选项（并允许数据包）或者允许该数据包而不做任何更改。

IP 选项可提供某些情景下需要的控制功能，但在大多数常规通信中可能并不需要这些功能。特别是，IP 选项包括时间戳、安全性和特殊路由的调配。并非必须使用 IP 选项，此字段可能包括零个、一个或多个选项。

有关 IP 选项的列表以及相关 RFC 的参考，请参阅 IANA 页面 (<http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml>)。

默认情况下已启用 IP 选项检测，但仅限 RSVP 流量。仅当您需要允许默认映射所允许的选项之外的其他选项，或当您需要通过使用非默认检测流量类映射将其应用于其他类型的流量时，才需要配置它。



注释 IP 选项检测不适用于分段的数据包。例如，分段中的选项不会被清除。

以下部分介绍 IP 选项检测。

IP 选项检测默认设置

默认情况下，仅为 RSVP 流量启用 IP 选项检测，其中会使用 `_default_ip_options_map` 检测策略映射。

- 允许使用 Router Alert 选项。

此选项通知传输路由器检测数据包的内容，即使数据包未流向该路由器。实施 RSVP 以及实施需要路由器沿着数据包传送路径进行相对复杂的处理的类似协议时，这项检测很有用。丢弃包含 Router Alert 选项的 RSVP 数据包可能会导致 VoIP 的实施出现问题。

- 包含任何其他选项（包括不受支持的选项）的

每次数据包因检测而被丢弃时，都会发出系统日志 106012。该消息会显示是哪个选项导致数据包被丢弃。使用 `show service-policy inspect ip-options` 命令可查看每个选项的统计信息。

配置 IP 选项检测策略映射

如果要执行非默认 IP 选项检测，请创建一个 IP 选项检测策略映射来指定您希望如何处理每种选项类型。



提示 除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > IP 选项。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射并点击 **Edit**。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 选择要允许的选项，将它们从丢弃列表移到允许列表即可。

请注意以下提示：

- “default” 选项设置对映射中不包含的选项采取的默认行为。如果将其移至允许列表，则丢弃列表中显示的选项也将被允许。
- 对于允许的任何选项，在传输数据包前可以通过选中 **Clear** 框从数据包报头中删除该选项。
- 有些选项是按选项类型编号列出的。该编号是完整的选项类型，八位数（副本、类和选项编号），而不只是八位数的选项编号部分。这些选项类型可能不代表实际选项。非标准选项必须采用互联网协议 RFC 791 定义的预期 `type-length-value` 格式 (<http://tools.ietf.org/html/rfc791>)。

- 如果数据包包括多种类型的选项，只要对于其中一种类型的操作是丢弃数据包，该数据包将会被丢弃。

有关 IP 选项的列表以及相关 RFC 的参考，请参阅 IANA 页面 (<http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml>)。

步骤 5 点击 OK。

这样即可将检测映射用于 IP 选项检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

IPsec 穿透检测

IPsec 穿透检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。但是，默认检测类包括默认 IPsec 端口，因此，只需简单地编辑默认全局检测策略即可添加 IPsec 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

以下各节介绍 IPsec 穿透检测引擎。

IPsec 穿透检测概述

互联网协议安全 (IPsec) 是一个协议集，用于通过验证和加密数据流的每个 IP 数据包来保护 IP 通信。IPsec 还包括用于会话开始时在代理之间建立相互身份验证以及用于协商将在会话期间使用的加密密钥的协议。IPsec 可用于保护一对主机之间（例如，计算机用户或服务器）、一对安全网关之间（例如，路由器或防火墙）或安全网关与主机之间的数据流。

IPSec 穿透应用检测使得与 IKE UDP 端口 500 连接相关的 ESP (IP 协议 50) 和 AH (IP 协议 51) 流量可以轻松地通过。这项检测避免了为允许 ESP 和 AH 流量而需要进行冗长的 ACL 配置，并使用超时和最大连接数实现安全性。

可以为 IPsec 穿透检测配置策略映射，以指定 ESP 或 AH 流量的限制。可以为每个客户端设置最大连接数和空闲超时。

允许 NAT 流量和非 NAT 流量。但是，不支持 PAT。

配置 IPsec 穿透检测策略映射

通过 IPsec 穿透映射可以更改用于 IPSec 穿透应用检测的默认配置值。借助 IPsec 穿透映射，无需使用 ACL 即可允许某些数据流。

配置包括默认映射 `_default_ipsec_passthru_map`，该默认映射设置每个客户端的最大 ESP 连接数，并将 ESP 空闲超时设置为 10 分钟。仅在需要非默认值或者需要设置 AH 值的情况下，才需要配置检测策略映射。



提示 除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > **Ipsec 穿透**。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射以查看映射内容。可以直接更改安全级别，或者点击 **Customize** 编辑映射。此操作过程的剩余步骤假设要自定义或添加映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 在 IPsec Pass Through Inspect Map 对话框的 **Security Level** 视图中，选择最符合所需配置的级别。

如果预设级别之一符合要求，执行到这一步即可。只需点击 **OK**，跳过此操作过程的剩余步骤，并将映射用于服务策略规则中以执行 IPsec 穿透检测。

如果需要进一步自定义设置，请点击 **Details** 并继续执行此操作步骤。

步骤 5 选择是否允许 ESP 和 AH 隧道。

对于每个协议，还可以设置每个客户端的最大允许连接数和空闲超时。

步骤 6 点击 **OK**。

这样即可将检测映射用于 IPsec 穿透检测服务策略中。

IPv6 检测

IPv6 检测根据扩展报头有选择性地记录或丢弃 IPv6 流量。此外，IPv6 检测可以检查 Pv6 数据包中扩展报头的类型和顺序是否符合 RFC 2460 的要求。

IPv6 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用它。可以简单地编辑默认全局检测策略来添加 IPv6 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

IPv6 检测默认设置

如果启用 IPv6 检测但不指定检测策略映射，将会使用默认 IPv6 检测策略映射并执行以下操作：

- 仅允许已知的 IPv6 扩展报头。丢弃并记录不符合要求的数据包。
- 按照 RFC 2460 规范的规定实施 IPv6 扩展报头顺序。丢弃并记录不符合要求的数据包。

- 丢弃带有路由类型报头的任何数据包。

配置 IPv6 检测策略映射

要标识要丢弃或记录的扩展报头，或者要禁用数据包验证，请创建 IPv6 检测策略映射以用于服务策略。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > IPv6。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射并点击 **Edit**。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 点击 **Enforcement** 选项卡，并选择是仅允许已知的 IPv6 扩展报头还是按照 RFC 2460 的规定实施 IPv6 扩展报头顺序。丢弃并记录不符合要求的数据包。

步骤 5 （可选）点击 **Header Matches** 选项卡，可基于 IPv6 消息的报头标识要丢弃或记录的流量。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

b) 选择要匹配的 IPv6 扩展报头：

- 身份验证 (AH) 报头。
- 目标选项报头。
- 封装安全负载 (ESP) 报头。
- 分片报头。
- 逐跳选项检测。
- 路由报头 - 指定一个报头类型编号或编号范围。
- 报头数 - 指定在不丢弃或记录数据包的情况下允许的最大扩展报头数量。
- 路由报头地址数 - 指定在不丢弃或记录数据包的情况下允许类型 0 路由报头中存在的最大地址数量。

c) 选择是要丢弃数据包还是记录数据包。如果选择丢弃数据包，还可以启用日志记录。

d) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 6 在 IPv6 Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 IPv6 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

NetBIOS 检测

NetBIOS 应用检测对 NetBIOS 名称服务 (NBNS) 数据包和 NetBIOS 数据报服务数据包中嵌入的 IP 地址执行 NAT。这项检测还会检查各个数量字段和长度字段的一致性，从而强制执行协议符合性。

默认情况下，NetBIOS 检测已启用。或者可以创建策略映射以便丢弃或记录 NetBIOS 协议违规情况。以下操作步骤介绍如何配置 NetBIOS 检测策略映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > NetBIOS。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射并点击 **Edit**。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 选择 **Check for Protocol Violations**。如果不选择此选项，则没有理由创建映射。

步骤 5 选择要执行的操作（丢弃数据包或记录数据包）。如果选择丢弃数据包，还可以启用日志记录。

步骤 6 点击 **OK**。

这样即可将检测映射用于 NetBIOS 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

PPTP 检测

PPTP 是用于对 PPP 流量进行隧道传送的协议。PPTP 会话通常包括一个 TCP 信道和两个 PPTP GRE 隧道。TCP 信道是用于协商和管理 PPTP GRE 隧道的控制信道。GRE 隧道在两台主机之间传送 PPP 会话。

启用后，PPTP 应用检测会检查 PPTP 协议数据包，并动态创建允许 PPTP 流量所需的 GRE 连接和转换。

特别是，ASA 会检测 PPTP 版本通知和对外呼叫请求/响应序列。如 RFC 2637 所要求，仅检测 PPTP 版本 1。如果任一端公布的版本不是版本 1，将会禁用对 TCP 控制信道的进一步检测。此外，还会跟踪传出呼叫请求和应答序列。会根据需要动态分配连接和转换，以允许后续辅助 GRE 数据流量。

要以 PAT 方式转换 PPTP 流量，必须启用 PPTP 检测引擎。此外，仅对符合如下条件的 GRE 版本执行 PAT：经过修改的（如 RFC2637 所要求）；且是通过 TCP 控制信道协商的。不会对未经修改的 GRE 版本执行 PAT（如 RFC 1701 和 RFC 1702 所要求）。

有关启用 PPTP 检测的信息，请参阅[配置应用层协议检测](#)，第 316 页。

RSH 检测

默认情况下，RSH 检测已启用。RSH 协议在 TCP 端口 514 上使用从 RSH 客户端到 TCP RSH 服务器的连接。客户端和服务器协商出 TCP 端口号，客户端会在该端口上侦听 STDERR 输出流。如有必要，RSH 检测支持协商端口号的 NAT。

有关启用 RSH 检测的信息，请参阅[配置应用层协议检测](#)，第 316 页。

SMTP 和扩展 SMTP 检测

ESMTP 检测可检测垃圾邮件、网络钓鱼、变形邮件等攻击和缓冲流量上溢/下溢攻击。另外，它还支持应用安全和协议符合性（实施 ESMTP 消息合理性检查及冻结发件人/收件人）并可冻结邮件中继。

默认情况下，ESMTP 检测已启用。仅在希望实施的措施不同于默认检测映射提供的处理操作时，才需要配置该检测。

以下各节介绍 ESMTP 检测引擎。

SMTP 和 ESMTP 检测概述

扩展 SMTP (ESMTP) 应用检测通过限制可通过 ASA 的 SMTP 命令类型和添加监控功能，加强对基于 SMTP 的攻击的防御。ESMTP 是增强型 SMTP 协议，在大多数方面和 SMTP 类似。

ESMTP 应用检测可控制和减少用户可使用的命令数以及服务器返回的消息数。ESMTP 检测主要执行三种任务：

- 将 SMTP 请求限制为七个基本 SMTP 命令和八个扩展命令。支持的命令如下：
 - 扩展 SMTP - AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS 和 VRFY。
 - SMTP (RFC 821) - DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET。
- 监控 SMTP 命令-响应序列。

- 生成审核线索 - 邮件地址中嵌入的无效字符被替换时，会生成审核记录 108002。有关详细信息，请参阅 RFC 821。

ESMTP 检测可监控以下异常签名的命令和响应序列：

- 截断的命令。
- 命令终止错误（不是以 <CR><LR> 终止）。
- MAIL 和 RCPT 命令指定邮件的发件人和收件人。会扫描邮件地址以检测异常字符。竖线 (|) 将被删除（更改为空格）；“<”和“>”只能用于定义邮件地址（“>”前面必须有“<”）。
- SMTP 服务器执行的意外转换。
- 对于未知或不受支持的命令，检测引擎会将数据包中的所有字符更改为 X，它们将被内部服务器拒绝。这将会生成消息，例如“500 Command unknown: 'XXX'”。不完整的命令将被丢弃
- 不支持的 ESMTP 命令为 ATRN、ONEX、VERB、CHUNKING 和专用扩展名。
- TCP 数据流编辑。
- 命令管道。



注释 启用 ESMTP 检测后，如果未监测以下命令，用于交互式 SMTP 的 Telnet 会话将被挂起：SMTP 命令必须至少为四个字符；它们必须使用回车符和换行符终止；您必须先等待响应，再发出下一个应答。

ESMTP 检测默认设置

默认情况下，ESMTP 检测已启用，其中会使用 `_default_esmtp_map` 检测策略映射。

- 会掩蔽服务器横幅。ESMTP 检测引擎将服务器 SMTP 横幅中的字符更改为星号，但对“2”、“0”、“0”字符除外。会忽略回车符 (CR) 和换行符 (LF)。
- 会允许已加密连接，但不进行检测。
- 不会查找发件人和收件人地址中的特殊字符，不会执行任何操作。
- 会丢弃并记录命令行长度大于 512 的连接。
- 会丢弃并记录有多于 100 个收件人的连接。
- 会记录正文长度超过 998 字节的消息。
- 会丢弃并记录报头行长度大于 998 的连接。
- 会丢弃并记录 MIME 文件名超过 255 个字符的消息。
- 会掩蔽匹配“others”的 EHLO 应答参数。

配置 ESMTP 检测策略映射

要指定消息违反参数时要执行的操作，请创建 ESMTP 检测策略映射。然后，可以在启用 ESMTP 检测时应用所创建的检测策略映射。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > ESMTP。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射以查看映射内容。可以直接更改安全级别，或者点击 **Customize** 编辑映射。此操作过程的剩余步骤假设要自定义或添加映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 在 ESMTP Inspect Map 对话框的 **Security Level** 视图中，选择最符合所需配置的级别。

如果预设级别之一符合要求，执行到这一步即可。只需点击 **OK**，跳过此操作过程的剩余步骤，并将映射用于服务策略规则中以执行 ESMTP 检测。

如果需要进一步自定义设置，请点击 **Details** 并继续执行此操作步骤。

提示 **MIME File Type Filtering** 按钮是配置文件类型检测的快捷方式（此步骤的后续部分将会对其加以说明）。

步骤 5 点击 **Parameters** 选项卡并配置所需的选项。

- **Mask Server Banner** - 是否掩蔽来自 ESMTP 服务器的横幅。
- **Encrypted Packet Inspection** - 是否允许 ESMTP 在未经检测的情况下通过 TLS（加密连接）。如有需要，可以记录加密连接。默认设置为允许 TLS 会话，不进行检测。如果取消选择该选项，系统会从任何加密会话连接尝试中去掉 STARTTLS 指示符并强制执行纯文本连接。

步骤 6 点击 **Filtering** 选项卡并配置所需的选项。

- **Configure mail relay** - 标识用于邮件转发的域名。可以断开连接和（可选）记录连接，或者只记录连接。
- **Check for special characters** - 标识要对发件人或收件人邮件地址中包含特殊字符（竖线 (|)、反引号和空字符）的消息执行的操作。可以断开连接和（可选）记录连接，或者只记录连接。

步骤 7 点击 **Inspections** 选项卡，并定义要基于流量特性实施的特定检测。

- a) 执行以下任一操作：
- 点击 **Add** 添加新条件。
 - 选择现有条件并点击 **Edit**。
- b) 选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。例如，如果对字符串“example.com”选择了 No Match，将会从类映射排除任何包含“example.com”的流量。然后，配置条件：
- **Body Length** - 匹配 ESMTP 消息正文长度大于指定字节数的消息。
 - **Body Line Length** - 匹配 ESMTP 消息正文的行长度大于指定字节数的消息。
 - **Commands** - 匹配消息中的命令谓词。可以指定以下一个或多个命令：auth、data、ehlo、etrm、helo、help、mail、noop、quit、rcpt、rset、saml、sowl、vrfy。
 - **Command Recipient Count** - 匹配收件人数量大于指定数量的消息。
 - **Command Line Length** - 匹配命令谓词中行长度大于指定字节数的消息。
 - **EHLO Reply Parameters** - 匹配 ESMTP EHLO 应答参数。可以指定以下一个或多个参数：8bitmime、auth、binaryname、checkpoint、dsn、etrm、others、pipelining、size、vrfy。
 - **Header Length** - 匹配 ESMTP 报头长度大于指定字节数的消息。
 - **Header Line Length** - 匹配 ESMTP 报头的行长度大于指定字节数的消息。
 - **Header To: Fields Count** - 匹配报头中 To 字段数量大于指定数量的消息。
 - **Invalid Recipients Count** - 匹配无效收件人数量大于指定数量的消息。
 - **MIME File Type** - 将 MIME 或媒体文件类型与指定的正则表达式或正则表达式类进行匹配。
 - **MIME Filename Length** - 匹配文件名长度大于指定字节数的消息。
 - **MIME Encoding** - 匹配 MIME 编码类型。可以指定以下一个或多个类型：7bit、8bit、base64、binary、others、quoted-printable。
 - **Sender Address** - 将发件人邮件地址与指定的正则表达式或正则表达式类进行匹配。
 - **Sender Address Length** - 匹配发件人地址长度大于指定字节数的消息。
- c) 选择是否断开连接、重置连接或记录连接。对于断开连接和重置连接这两种情况，可以启用或禁用日志记录。对于命令匹配和 EHLO 应答参数匹配，还可以掩蔽此命令。对于命令匹配，还可以对数据包数应用每秒速率限制。
- d) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 8 在 ESMTP Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 ESMTP 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

SNMP 检测

通过 SNMP 应用检测可以将 SNMP 流量限制于特定 SNMP 版本。SNMP 早期版本的安全性较低；因此，安全策略可能要求拒绝使用某些 SNMP 版本。ASA 可拒绝 SNMP 版本 1、2、2c 或 3。可以创建 SNMP 映射来控制允许的版本。

SNMP 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用这项检测。可以简单地编辑默认全局检测策略来添加 SNMP 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > SNMP。

步骤 2 点击 **Add**，或者选择映射并点击 **Edit**。添加映射时，请输入映射名称。

步骤 3 选择不允许的 SNMP 版本。

步骤 4 点击 **OK**。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

SQL*Net 检测

系统已默认启用 SQL*Net 检测。检测引擎支持 SQL*Net 版本 1 和 2，但仅支持透明网络底层 (TNS) 格式。检测不支持表格数据流 (TDS) 格式。系统会扫描嵌入式地址和端口的 SQL*Net 消息，并在需要时应用 NAT 重写。

SQL*Net 的默认端口赋值为 1521。这是 Oracle 用于 SQL*Net 的值，但是，该值与结构化查询语言 (SQL) 的 IANA 端口赋值不符。如果您的应用使用其他端口，请对包含该端口的流量类应用 SQL*Net 检测。



注释

当与 SQL 控制 TCP 端口 1521 相同的端口上发生 SQL 数据传输时，请禁用 SQL*Net 检测。安全设备在启用 SQL*Net 检测之后充当代理，且将客户端窗口大小从 65000 缩小至大约 16000，从而导致数据传输问题。

有关启用 SQL*Net 检测的信息，请参阅[配置应用层协议检测](#)，第 316 页。

Sun RPC 检测

本节介绍 Sun RPC 应用检测。

Sun RPC 检测概述

Sun RPC 协议检测默认启用。只需管理 Sun RPC 服务器表，即可确定允许穿越防火墙的服务。但是，任何服务器的 NFS 针孔都会打开，即便没有服务器表配置。

Sun RPC 可供 NFS 和 NIS 使用。Sun RPC 服务可在任何端口上运行。当客户端尝试访问服务器上的 Sun RPC 服务时，必须获悉服务运行所在的端口。它通过查询端口映射程序进程执行此操作，通常为 `rpcbind`，位于公认端口 111。

客户端将发送服务的 Sun RPC 程序号，而端口映射程序进程将用服务的端口号进行响应。客户端发送其 Sun RPC 查询至服务器，指定端口映射程序进程识别的端口。当该服务器应答时，ASA 会拦截此数据包，并在该端口上同时打开初期 TCP 和 UDP 连接。

不支持 Sun RPC 负载信息的 NAT 或 PAT。

管理 Sun RPC 服务

使用 Sun RPC 服务表可基于建立的 Sun RPC 会话来控制 Sun RPC 流量。

过程

步骤 1 依次选择配置 > 防火墙 > 高级 > SUNRPC 服务器。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新服务器。
- 选择服务器并点击 **Edit**。

步骤 3 配置服务属性：

- **接口名称** - 流量流向服务器所流经的接口。
- **IP 地址/掩码** - Sun RPC 服务器的地址。
- **服务 ID** - 服务器上的服务类型。要确定服务类型（例如，100003），请在 Sun RPC 服务器计算机上的 UNIX 或 Linux 命令行处使用 `sunrpcinfo` 命令。
- **协议** - 服务使用 TCP 还是 UDP。
- **端口/端口范围** - 服务使用的端口或端口范围。
- **Timeout** - Sun RPC 检测为连接打开的针孔的空闲超时。

步骤 4 点击 **OK**。

步骤 5 （可选。）监控为这些服务创建的针孔。

要显示为 Sun RPC 服务打开的针孔，请输入 **show sunrpc-server active** 命令。依次选择工具 > 命令行界面输入命令。例如：

```
hostname# show sunrpc-server active
LOCAL FOREIGN SERVICE TIMEOUT
-----
1 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
2 209.165.200.5/0 192.168.100.2/2049 100003 0:30:00
3 209.165.200.5/0 192.168.100.2/647 100005 0:30:00
4 209.165.200.5/0 192.168.100.2/650 100005 0:30:00
```

LOCAL 列中的条目显示内部接口上客户端或服务器的 IP 地址，而 FOREIGN 列中的值则显示外部接口上客户端或服务器的 IP 地址。

如有必要，可使用清除这些服务 **clear sunrpc-server active**

TFTP 检测

默认情况下，TFTP 检测已启用。

如 RFC 1350 中所述，TFTP 是用于在 TFTP 服务器与客户端之间读取和写入文件的简单协议。

检测引擎检测 TFTP 读取请求 (RRQ)、写入请求 (WRQ) 和错误通知 (ERROR)，并且如有必要，还会动态创建连接和转换，从而允许在 TFTP 客户端和服务器之间传输文件。

如有必要，在接收有效的读取 (RRQ) 或写入 (WRQ) 请求时会分配动态辅助信道和 PAT 转换。随后，TFTP 会使用该辅助信道进行文件传输或错误通知。

只有 TFTP 服务器可以通过辅助信道发起流量；此外，TFTP 客户端与服务器之间最多只能有一个不完整的辅助信道。服务器发出的错误通知会致使辅助信道关闭。

如果使用静态 PAT 重定向 TFTP 流量，则必须启用 TFTP 检测。

有关启用 TFTP 检测的信息，请参阅[配置应用层协议检测](#)，第 316 页。

XDMCP 检测

XDMCP 检测默认已启用。XDMCP 是使用 UDP 端口 177 来协商 X 会话（建立后使用 TCP）的协议。

为了成功协商和启动 XWindows 会话，ASA 必须允许来自 Xhosted 计算机的 TCP 向后连接。要允许该向后连接，可以使用访问规则来允许 TCP 端口。或者，也可以在 ASA 上使用 **established** 命令。在 XDMCP 协商用于发送显示内容的端口后，系统将调用 **established** 命令来验证是否应允许此向后连接。

在 XWindows 会话期间，管理器将与已知端口 6000 | n 上的显示器 Xserver 通信。使用以下终端设置，每个显示器都会独立连接到 Xserver。

```
setenv DISPLAY Xserver:n
```

其中 n 为显示器编号。

使用 XDMCP 时，系统将使用 IP 地址协商显示，以便 ASA 可在需要时应用 NAT。XDMCP 检测不支持 PAT。

有关启用 XDMCP 检测的信息，请参阅[配置应用层协议检测](#)，第 316 页。

VXLAN 检测

虚拟可扩展局域网 (VXLAN) 检测适用于流经 ASA 的 VXLAN 封装流量。该检测可确保 VXLAN 报头格式符合标准，丢弃所有格式错误的数据包。系统对于将 ASA 用作 VXLAN 隧道终端 (VTEP) 或 VXLAN 网关的流量不执行 VXLAN 检测，因为在解除 VXLAN 数据包封装的正常环节中会执行那些检测。

VXLAN 数据包为 UDP，通常在端口 4789 上。此端口是默认检测流量类的一部分，因此只需将 VXLAN 检测添加到 inspection_default 服务策略规则中即可。或者，也可以使用端口或 ACL 匹配创建一个类。

基本互联网协议检测的历史

功能名称	版本	功能信息
DCERPC 检测支持 ISystemMapper UUID 消息 RemoteGetClassObject opnum3。	9.4(1)	ASA 从版本 8.3 开始支持非 EPM DCERPC 消息，支持 ISystemMapper UUID 消息 RemoteCreateInstance opnum4。此更改扩展了对 RemoteGetClassObject opnum3 消息的支持。 未修改任何 ASDM 菜单项。
VXLAN 数据包检测	9.4(1)	ASA 可检查 VXLAN 报头以强制遵守标准格式。 修改了以下屏幕： Configuration > Firewall > Service Policy Rules > Add Service Policy Rule > Rule Actions > Protocol Inspection 。

功能名称	版本	功能信息
TLS 会话默认行为中的 ESMTP 检测变化。	9.4(1)	<p>已将 ESMTP 检查的默认设置更改为允许 TLS 会话，这些会话不会被检查。不过，此默认设置适用于新的或重新映像的系统。如果您升级了包括 no allow-tls 的系统，则该命令不会更改。</p> <p>还在以下早期版本中进行了此默认行为更改：8.4(7.25)、8.5(1.23)、8.6(1.16)、8.7(1.15)、9.0(4.28)、9.1(6.1)、9.2(3.2)、9.3(1.2)、9.3(2.2)。</p>
改进了 IP 选项检测。	9.5(1)	<p>IP 选项检测现在支持所有可能的 IP 选项。您可以对检测进行调整以允许、清除或丢弃任何标准的或试验性选项，包括尚未定义的选项。还可以为 IP 选项检测图中尚未明确定义的选项设置默认行为。</p> <p>我们更改了 IP Options Inspect Map 对话框，添加了其他选项。现在，您可以选择要允许和（可选）清除的选项。</p>
DCERPC 检测改进和 UUID 过滤	9.5(2)	<p>DCERPC 检测现在支持 OxidResolver ServerAlive2 opnum5 消息的 NAT。现在您可根据 DCERPC 消息通用唯一标识 (UUID) 进行过滤，以便重置或记录特定消息类型。新 DCERPC 检测类映射可用于 UUID 过滤。</p> <p>添加了以下菜单项：配置 > 防火墙 > 对象 > 类映射 > DCERPC。修改了以下菜单项：配置 > 防火墙 > 对象 > 检测映射 > DCERPC。</p>
通过 TCP 的 DNS 检测。	9.6(2)	<p>现在，您可以检查通过 TCP 的 DNS 流量 (TCP/53)。</p> <p>修改了以下页面：Configuration > Firewall > Objects > Inspection Maps > DNS Add/Edit 对话框。</p>
思科 Umbrella 支持。	9.10(1)	<p>您可以配置设备将 DNS 请求重定向至思科 Umbrella，以便将您在思科 Umbrella 中定义的企业安全策略应用于用户连接。您可以允许或阻止基于 FQDN 的连接，或者，对于可疑的 FQDN，您可以将用户重定向至思科 Umbrella 智能代理，该代理可以执行 URL 筛选。Umbrella 配置是 DNS 检测策略的一部分。</p> <p>我们添加或修改了以下屏幕：配置 > 防火墙 > 对象 > Umbrella、配置 > 防火墙 > 对象 > 检测映射 > DNS。</p>



第 16 章

语音和视频协议检测

以下主题介绍针对语音和视频协议的应用检测。有关为何需要对某些协议进行检测以及应用检测的总体方法的基本信息，请参阅[应用层协议检测入门](#)，第 309 页。

- [CTIQBE 检测](#)，第 359 页
- [H.323 检测](#)，第 360 页
- [MGCP 检测](#)，第 364 页
- [RTSP 检测](#)，第 366 页
- [SIP 检测](#)，第 369 页
- [瘦客户端控制协议 \(SCCP\) 检测](#)，第 373 页
- [STUN 检测](#)，第 376 页
- [语音和视频协议检测的历史](#)，第 376 页

CTIQBE 检测

CTIQBE 协议检测支持 NAT、PAT 和双向 NAT。借此，思科 IP SoftPhone 及其他思科 TAPI/JTAPI 应用可协同思科 CallManager 在 ASA 范围内成功进行呼叫建立。

许多思科 VoIP 应用都使用 TAPI 和 JTAPI。思科 TSP 通过 CTIQBE 与 Cisco CallManager 通信。

有关启用 CTIQBE 检测的信息，请参阅[配置应用层协议检测](#)，第 316 页。

CTIQBE 检测的局限性

不支持 CTIQBE 呼叫状态故障切换。

下面总结了在特定情况下使用 CTIQBE 应用检测时的特殊注意事项：

- 如果两个思科 IP SoftPhone 注册到不同的思科 CallManager，且这两个思科 CallManager 连接到不同的 ASA 接口，则两个电话之间的呼叫将会失败。
- 当 Cisco CallManager 位于比 Cisco IP SoftPhone 更高的安全接口上时，如果 Cisco CallManager IP 地址必须执行 NAT 或外部 NAT，则映射必须为静态，因为 Cisco IP SoftPhone 需要在 PC 上的思科 TSP 配置中明确指定 Cisco CallManager IP 地址。

- 当使用 PAT 或外部 PAT 时，如果要转换 Cisco CallManager IP 地址，则必须将其 TCP 端口 2748 静态映射到 PAT（接口）地址的同一端口上，以便成功注册 Cisco IP SoftPhone。CTIQBE 侦听端口 (TCP 2748) 是固定的，用户不能在 Cisco CallManager、Cisco IP SoftPhone 或思科 TSP 上进行配置。

H.323 检测

H.323 检测支持 RAS、H.225 和 H.245，这项检测功能会转换所有嵌入式 IP 地址和端口。H.323 检测执行状态跟踪和过滤，并且可以激活很多检测功能。H.323 检测支持电话号码过滤、动态 T.120 控制、H.245 隧道控制、HSI 组、协议状态跟踪、H.323 呼叫持续时间限制和音频/视频控制。

默认情况下，H.323 检测已启用。仅在需要非默认处理的情况下，才需要配置这项检测。

以下各节介绍 H.323 应用检测。

H.323 检测概述

H.323 检测支持符合 H.323 规范的应用，例如思科 CallManager。H.323 是国际电信联盟制定的一套协议，用于通过 LAN 进行多媒体会议。ASA 最高支持 H.323 版本 6，其中包括 H.323 版本 3 “支持在一个呼叫信令通道上进行多个呼叫”的功能。

启用 H.323 检测后，ASA 支持在同一呼叫信令通道上进行多个呼叫（此功能在 H.323 版本 3 中引入）。此功能可缩短呼叫建立时间并减少 ASA 上端口的使用。

H.323 检测具有如下两个主要功能：

- 对 H.225 和 H.245 消息中必要的嵌入式 IPv4 地址进行 NAT 转换。由于 H.323 消息以 PER 编码格式编码，所以 ASA 使用 ASN.1 解码器来解码 H.323 消息。
- 动态分配协商的 H.245 和 RTP/RTCP 连接。使用 RAS 时，也可以动态分配 H.225 连接。

H.323 工作原理

H.323 协议集合总共最多可以使用两个 TCP 连接和四到八个 UDP 连接。FastConnect 仅使用一个 TCP 连接，且 RAS 使用单个 UDP 连接用于注册、准入和状态。

首先，H.323 客户端可以使用 TCP 端口 1720 与 H.323 服务器之间初步建立 TCP 连接，以请求建立 Q.931 呼叫。在呼叫建立过程中，H.323 终端向客户端提供用于 H.245 TCP 连接的端口号。在使用 H.323 网守的环境中，初始数据包使用 UDP 进行传输。

H.323 检测会监控 Q.931 TCP 连接，以确定 H.245 端口号。如果 H.323 终端使用的不是 FastConnect，ASA 将基于 H.225 消息的检测动态分配 H.245 连接。使用 RAS 时，也可以动态分配 H.225 连接。

在每个 H.245 消息中，H.323 终端交换用于后续 UDP 数据流的端口号。H.323 检测会检测 H.245 消息来标识这些端口，并动态创建用于媒体交换的连接。RTP 使用协商的端口号，而 RTCP 使用下一个更高的端口号。

H.323 控制信道处理 H.225、H.245 和 H.323 RAS。H.323 检测使用以下端口。

- 1718 - 网守发现 UDP 端口
- 1719 - RAS UDP 端口
- 1720 - TCP 控制端口

要实现 RAS 信令，必须允许已知 H.323 端口 1719 的流量。此外，要实现 H.225 呼叫信令，必须允许已知 H.323 端口 1720 的流量；但是，H.245 信令端口要在 H.225 信令中的终端之间协商。使用 H.323 网守时，ASA 将基于 ACF 和 RCF 消息的检测打开 H.225 连接。

检测 H.225 消息后，ASA 将打开 H.245 通道，然后也会检测通过 H.245 通道发送的流量。通过 ASA 传递的所有 H.245 消息均会接受 H.245 应用检测，即转换嵌入的 IP 地址并打开 H.245 消息中协商的媒体通道。

每个具有通过 H.323 检测的数据包的 UDP 连接都将被标记为 H.323 连接，这每个连接均按照 Configuration > Firewall > Advanced > Global Timeouts 窗格中的 H.323 超时配置超时。



注释 如果网守在网络内部，可以在 H.323 终端之间启用呼叫建立。ASA 包括基于 RegistrationRequest/RegistrationConfirm (RRQ/RCF) 消息打开呼叫针孔的选项。由于这些 RRQ/RCF 消息会进出网守，所以呼叫终端的 IP 地址未知且 ASA 会通过源 IP 地址/端口 0/0 打开针孔。默认情况下，此选项已禁用。

H.245 消息中的 H.239 支持

ASA 位于两个 H.323 终端之间。当两个 H.323 终端建立电话演示会话以便终端可收发数据演示（例如电子表格数据）时，ASA 可确保两个终端之间成功进行 H.239 协商。

H.239 是一项标准，使 H.300 系列终端能够在单个呼叫中打开另外一个视频信道。在呼叫中，终端（例如视频电话）会发送视频信道和数据演示信道。H.239 协商发生于 H.245 信道上。

ASA 可为更多媒体信道和媒体控制信道打开针孔。终端使用开放逻辑信道 (OLC) 消息来发出有关新信道创建的信息。消息扩展是 H.245 v13 的一部分。

默认情况下，电话演示会话的解码和编码已启用。H.239 的编码和解码由 ASN.1 编码器执行。

H.323 检测的局限性

H.323 检测已经过测试，受思科统一通信管理器 (CUCM) 7.0 支持。CUCM 8.0 及更高版本不支持这项检测。H.323 检测可能适用于其他版本和产品。

以下是 H.323 应用检测的某些已知问题和局限性：

- 支持 PAT，但扩展 PAT 或每会话 PAT 除外。
- 静态 PAT 可能无法正确转换 H.323 消息内嵌入到可选字段中的 IP 地址。如果遇到这种问题，请勿对 H.323 使用静态 PAT。
- 不支持同一安全级别接口之间的 NAT。

- 不支持 NAT64。
- 带有 H.323 检测的 NAT 直接在终端上执行时与 NAT 不兼容。如果在终端上执行 NAT，请禁用 H.323 检测。

配置 H.323 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 H.323 检测策略映射以自定义 H.323 检测操作。

或者，可以创建 H.323 检测类映射来定义 H.323 检测的流量类。另一种方法是，直接在 H.323 检测策略映射中定义流量类。创建类映射与直接在检测映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。虽然此过程介绍了检测映射，但类映射中使用的匹配条件与 **Inspection** 选项卡相关步骤中介绍的匹配条件相同。您可以通过以下两种方法来配置 H.323 类映射：依次选择配置 > 防火墙 > 对象 > 类映射 > **H.323**；或在配置检测映射时创建它们。



提示 除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > **H.323**。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射以查看映射内容。可以直接更改安全级别，或者点击 **Customize** 编辑映射。此操作过程的剩余步骤假设要自定义或添加映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 在 H.323 Inspect Map 对话框的 **Security Level** 视图中，选择最符合所需配置的级别。默认级别为 Low。

如果预设级别之一符合要求，执行到这一步即可。只需点击 **OK**，跳过此操作过程的剩余步骤，并将映射用于服务策略规则中以执行 H.323 检测。

提示 **Phone Number Filtering** 按钮是配置被叫方或主叫方检测的快捷方式（下面将会加以说明）。

步骤 5 如果需要进一步自定义设置，请点击 **Details** 并执行以下操作：

- a) 点击 **State Checking** 选项卡，选择是否启用 RAS 和 H.225 消息的状态转换检查。

还可以检查 RCF 消息并打开用于 RRQ 消息中存在的呼叫信号地址的针孔，这样，如果网守在网络内部，可以在 H.323 终端之间启用呼叫建立。使用此选项可根据 **RegistrationRequest/RegistrationConfirm (RRQ/RCF)** 消息为呼叫打开针孔。由于这些 RRQ/RCF 消息会进出网守，所以呼叫终端的 IP 地址未知且 ASA 会通过源 IP 地址/端口 0/0 打开针孔。默认情况下，此选项已禁用。

- b) 点击 **Call Attributes** 选项卡，选择是否实施呼叫持续时间限制（最长为 1193 小时）或是否在呼叫建立期间显示主叫方和被叫方。

此外，还可以根据 H.460.18 允许 H.225 FACILITY 消息在 H.225 SETUP 消息之前到达。如果遇到呼叫建立问题（使用 H.323/H.225 时连接会在完成之前被关闭），请使用此选项允许消息提前到达。此外，请确保为 H.323 RAS 和 H.225 启用检测（默认情况下，它们处于启用状态）。

- c) 点击 **Tunneling and Protocol Conformance** 选项卡，并选择是否检查 H.245 隧道；可以丢弃连接或记录连接。

还可以选择是否检查流经针孔的 RTP 数据包的协议符合性。如果检查符合性，还可以选择是否根据信令交换限制音频或视频的负载。

步骤 6 如有必要，请点击 **HSI Group Parameters** 选项卡并定义 HSI 组。

- a) 执行以下任一操作：

- 点击 **Add** 添加新组。
- 选择现有组并点击 **Edit**。

- b) 指定组 ID（0 到 2147483647）和 HSI 的 IP 地址。

- c) 要向 HSI 组添加终端，请输入 IP 地址，选择终端连接到 ASA 所通过的接口，然后点击 **Add>>**。可删除不再需要的任何终端。每个组最多可以有 10 个终端。

- d) 点击 **OK** 添加组。根据需要重复上述步骤。

步骤 7 点击 **Inspections** 选项卡，并定义要基于流量特性实施的特定检测。

可以根据 H.323 类映射定义流量匹配条件，或者直接在检测映射中配置匹配，还可以同时使用这两种方法。

- a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

- b) 选择 **Single Match** 直接定义条件，或选择 **Multiple Match**，在后者情况下可选择 H.323 类映射来定义条件。

- c) 如果在这里定义条件，请选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。然后，按如下方式配置条件：

- **Called Party** - 根据所选的正则表达式或正则表达式类匹配 H.323 被叫方。
- **Calling Party** - 根据所选的正则表达式或正则表达式类匹配 H.323 主叫方。

- **Media Type** - 匹配媒体类型：音频、视频或数据。

- d) 选择要对匹配的流量执行的操作。对于匹配的主叫方或被叫方，可以丢弃数据包，断开连接或重置连接。对于媒体类型匹配，操作始终是丢弃数据包；可以对此操作启用日志记录。
- e) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 8 在 H.323 Inspect Map 对话框中，点击 **OK**。

这样即可将检测映射用于 H.323 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

MGCP 检测

MGCP 检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用这项检测。但是，默认检测类确实包括默认 MGCP 端口，因此，只需简单地编辑默认全局检测策略，即可添加 MGCP 检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

以下各节介绍 MGCP 应用检测。

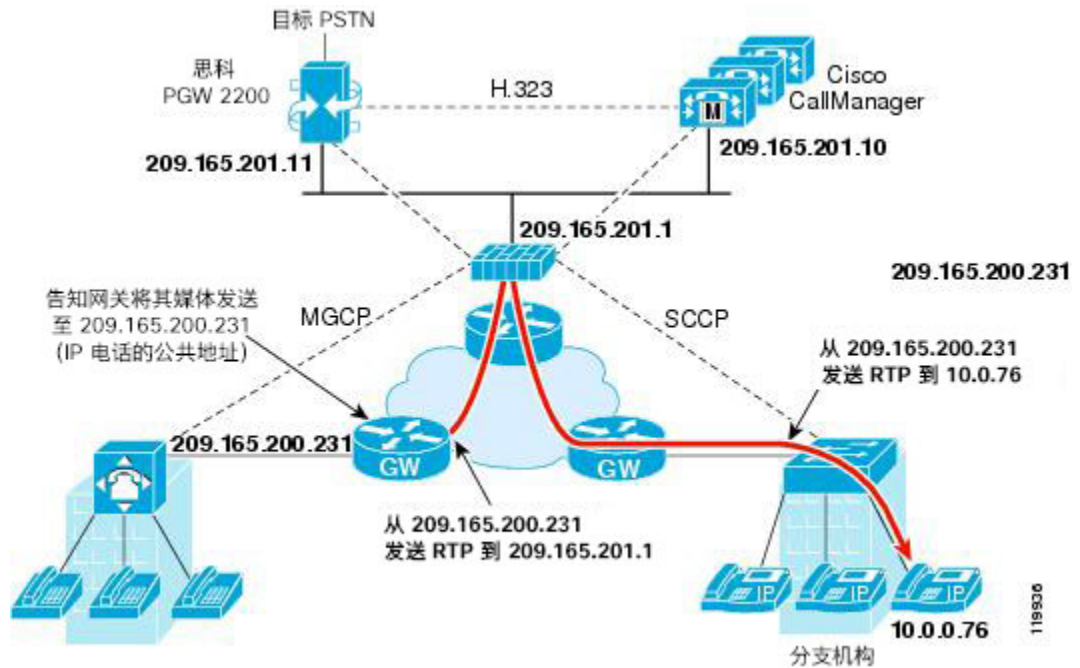
MGCP 检测概述

MGCP 是一个主/从协议，用于控制来自称为媒体网关控制器或呼叫代理的外部呼叫控制元件的媒体网关。媒体网关通常是一个网络元素，用于在电话电路上传送的音频信号和互联网上或其他数据包网络上传送的数据包之间提供转换。借助具有 MGCP 的 NAT 和 PAT，可以使用一组有限的外部（全局）地址来支持内部网络中的大量设备。媒体网关示例如下：

- 中继网关：用于在电话网络和 IP 语音网络之间建立连接。这种网关通常管理大量的数字电路。
- 家庭网关：提供用于连接到 IP 语音网络的传统模拟 (RJ11) 接口。电缆调制解调器/电缆机顶盒、xDSL 设备、宽带无线设备都是家庭网关示例。
- 业务网关：提供用于连接到 IP 语音网络的传统数字 PBX 接口或集成软 PBX 接口。

MGCP 消息通过 UDP 传输。响应会发送回命令的源地址（IP 地址和 UDP 端口号），但响应可能不会到达收到命令的同一地址。如果在同一故障转移配置中使用多个呼叫代理，且接收命令的呼叫代理已经将控制转交给备用呼叫代理，由备用呼叫代理来发送响应，可能会发生这种情况。下图说明如何配合使用 NAT 与 MGCP。

图 47: 配合使用 NAT 与 MGCP



MGCP 终端是数据的物理或虚拟源及目标。媒体网关包含终端，呼叫代理可以在这些终端上创建、修改和删除连接，从而建立并控制与其他多媒体终端之间的媒体会话。此外，呼叫代理可以指示终端检测某些事件和生成信号。终端会自动将服务状态变化情况告知呼叫代理。

- 网关通常会侦听 UDP 端口 2427 以接收来自呼叫代理的命令。
- 呼叫代理所在的端口接收来自网关的命令。呼叫代理通常会侦听 UDP 端口 2727 以接收来自网关的命令。



注释 MGCP 检测不支持对 MGCP 信令和 RTP 数据使用不同的 IP 地址。通常建议的做法是从弹性 IP 地址（例如回环或虚拟 IP 地址）发送 RTP 数据，但 ASA 要求 RTP 数据的发出地址与 MGCP 信令相同。

配置 MGCP 检测策略映射

如果网络中包含多个 ASA 必须为其打开针孔的呼叫代理和网关，请创建 MGCP 映射。然后，可以在启用 MGCP 检测时应用所创建的 MGCP 映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > MGCP。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射并点击 **Edit**。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 （可选）点击 **Command Queue** 选项卡，并指定 MGCP 命令队列允许的最大命令数。默认值为 200，允许的范围是 1 到 2147483647。

步骤 5 点击 **Gateways and Call Agents** 选项卡，并为映射配置网关组和呼叫代理组。

- 点击 **Add** 创建新组，或者选择组并点击 **Edit**。
- 在 **Group ID** 中输入呼叫代理组的组 ID。呼叫代理组将一个或多个呼叫代理与一个或多个 MGCP 媒体网关关联。有效范围为 0 到 2147483647。
- 要向组添加由关联的呼叫代理控制的媒体网关 IP 地址，请在 **Gateway to Be Added** 中输入这些地址并点击 **Add>>**。可删除不再使用的任何网关。

媒体网关通常是一个网络元素，用于在电话电路上传送的音频信号和互联网上或其他数据包网络上传送的数据包之间提供转换。通常，网关将命令发送到呼叫代理的默认 MGCP 端口 UDP 2727。

- 要添加控制 MGCP 媒体网关的呼叫代理的 IP 地址，请在 **Call Agent to Be Added** 中输入这些地址并点击 **Add>>**。可删除不再需要的任何代理。

通常，呼叫代理将命令发送到网关的默认 MGCP 端口 UDP 2427。

- 在 MGCP Group 对话框中点击 **OK**。根据需要重复上述步骤，添加其他组。

步骤 6 在 MGCP Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 MGCP 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

RTSP 检测

默认情况下，RTSP 检测已启用。仅在需要非默认处理的情况下，才需要配置这项检测。以下各节介绍 RTSP 应用检测。

RTSP 检测概述

RTSP 检测引擎允许 ASA 传送 RTSP 数据包。RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer 和思科 IP/TV 连接都使用 RTSP。



注释 对于思科 IP/TV，请使用 RTSP TCP 端口 554 和 8554。

RTSP 应用使用已知 TCP（很少用 UDP）端口 554 作为控制信道。根据 RFC 2326 要求，ASA 仅支持 TCP。该 TCP 控制信道用于根据客户端配置的传输模式协商用于传输音频/视频流量的数据信道。

支持如下 RDT 传输：rtp/avp、rtp/avp/udp、x-real-rtsp、x-real-rtsp/udp 和 x-pn-tng/udp。

ASA 使用状态代码 200 解析建立响应消息。如果响应消息要进站，服务器需相对于 ASA 处于外部，并需要为连接从服务器进入站内打开动态信道。如果响应消息要出站，则 ASA 无需打开动态信道。

RTSP 检测不支持 PAT 或双 NAT。另外，ASA 无法识别 HTTP 掩蔽，其中 RTSP 消息隐藏在 HTTP 消息中。

RealPlayer 配置要求

使用 RealPlayer 时，正确配置传输模式非常重要。对于 ASA，请将 **access-list** 命令从服务器添加到客户端，或者从客户端添加到服务器。对于 RealPlayer，依次点击 **Options>Preferences>Transport>RTSP Settings** 更改传输模式。

如果 RealPlayer 使用 TCP 模式，请选择 **Use TCP to Connect to Server** 和 **Attempt to use TCP for all content** 复选框。在 ASA 上无需配置检测引擎。

如果在 RealPlayer 上使用 UDP 模式，请勾选 **Use TCP to Connect to Server** 和 **Attempt to use UDP for static content** 复选框；对于无法通过组播获得的实时内容，也请勾选上述复选框。在 ASA 中添加 **inspect rtsp** 命令。

RSTP 检测的局限性

RSTP 检测有以下局限性。

- ASA 不支持通过 UDP 的组播 RTSP 或 RTSP 消息。
- ASA 无法识别 RTSP 消息隐藏在 HTTP 消息中的 HTTP 掩蔽技术。
- ASA 无法对 RTSP 消息执行 NAT，因为嵌入式 IP 地址作为 HTTP 或 RTSP 消息的一部分包含在 SDP 文件中。数据包可以分段，但 ASA 无法对分段的数据包执行 NAT。
- 对于思科 IP/TV，ASA 对消息 SDP 部分可执行的转换数与内容管理器中的程序列表数呈正比（每个程序列表至少可包含六个嵌入式 IP 地址）。
- 可以为 Apple QuickTime 4 或 RealPlayer 配置 NAT。如果查看器和内容管理器位于外部网络，而服务器位于内部网络，则思科 IP/TV 只能采用 NAT。

配置 RTSP 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 RTSP 检测策略映射来自定义 RTSP 检测操作。

或者，可以创建 RTSP 检测类映射来定义 RTSP 检测的流量类。另一种方法是，直接在 RTSP 检测策略映射中定义流量类。创建类映射与直接在检测映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。虽然此过程介绍了检测映射，但类映射中使用的匹配条件与 **Inspection** 选项卡相关步骤中介绍的匹配条件相同。您可以通过以下两种方法来

配置 RTSP 类映射：依次选择配置 > 防火墙 > 对象 > 类映射 > RTSP；或在配置检测映射时创建它们。



提示 除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > RTSP。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射并点击 **Edit**。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 点击 **Parameters** 选项卡并配置所需的选项：

- **Enforce Reserve Port Protection** - 在媒体端口协商期间是否限制使用预留端口。
- **Maximum URL Length** - 消息中允许的最大 URL 长度，范围介于 0 到 6000 之间。

步骤 5 点击 **Inspections** 选项卡，并定义要基于流量特性实施的特定检测。

可以根据 RTSP 类映射定义流量匹配条件，或者直接在检测映射中配置匹配，还可以同时使用这两种方法。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

b) 选择 **Single Match** 直接定义条件，或选择 **Multiple Match**，在后者情况下可选择 RTSP 类映射来定义条件。

c) 如果在这里定义条件，请选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。例如，如果对字符串“example.com”选择了 No Match，将会从类映射排除任何包含“example.com”的流量。然后，按如下方式配置条件：

- **URL Filter** - 根据所选的正则表达式或正则表达式类匹配 URL。

- **Request Method** - 匹配请求方法: announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameters、teardown。

- d) 选择要对匹配的流量执行的操作。对于 URL 匹配，可以断开连接或记录连接，而且可以对断开的连接启用日志记录。对于请求方法匹配，可以对数据包数应用每秒速率限制。
- e) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 6 在 RTSP Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 RTSP 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

SIP 检测

SIP 是一种广泛用于网络会议、电话、展示、事件通知和即时消息的协议。部分原因是 SIP 本质上是文本协议，部分原因是其具有灵活性，因此，SIP 网络面临大量安全威胁。

SIP 应用检测会在消息报头和正文中提供地址转换，会动态打开端口，还会执行基本健全性检查。SIP 应用检测还支持应用安全和协议符合性（此功能强制对 SIP 消息进行健全性检查，以及检测基于 SIP 的攻击）。

默认情况下，SIP 检测已启用。只有需要非默认处理时，或者要标识 TLS 代理来启用加密流量检测时，才需要配置这项检测。以下主题详细说明 SIP 检测。

SIP 检测概述

如 IETF 所定义，SIP 能够实现呼叫处理会话，特别是双方音频会议（又称为“通话”）。SIP 可与 SDP 配合使用来实现呼叫信令。SDP 指定用于媒体流的端口。使用 SIP，ASA 可支持任何 SIP VoIP 网关和 VoIP 代理服务器。SIP 和 SDP 在以下 RFC 中定义：

- SIP: 会话初始协议，RFC 3261
- SDP: 会话描述协议，RFC 2327

为了支持 SIP 呼叫通过 ASA，必须检测媒体连接地址、媒体端口和媒体初期连接的信令消息，因为在已知目标端口 (UDP/TCP 5060) 上发送信令时，系统会动态分配媒体流。此外，SIP 还会在 IP 数据包的用户数据部分嵌入 IP 地址。请注意，ASA 支持的最大 SIP 请求 URI 长度为 255。

即时消息 (IM) 应用也使用 SIP 扩展（定义见 RFC 3428）和 SIP 特定的事件通知 (RFC 3265)。用户发起聊天会话（注册/订用）之后，当用户相互聊天时，IM 应用会使用 MESSAGE/INFO 方法和 202 Accept 响应。例如，两个用户可以随时在线，但几个小时都不聊天。因此，SIP 检测引擎会根据配置的 SIP 超时值打开超时的针孔。该值必须配置为比订用持续时间至少长 5 分钟。订用持续时间在 Contact Expires 值中定义，通常是 30 分钟。

由于 MESSAGE/INFO 请求通常使用动态分配的端口（而不是端口 5060）发送，因此，这些请求必须通过 SIP 检测引擎。



注释 SIP 检测仅支持聊天功能。不支持白板、文件传输和应用共享。不支持 RTC Client 5.0。

SIP 检查的限制

SIP 检测已经过测试，受思科统一通信管理器 (CUCM) 7.0、8.0、8.6 和 10.5 支持。CUCM 8.5 或 9.x 不支持这项检测。SIP 检测可能适用于其他版本和产品。

SIP 检测适用于嵌入式 IP 地址的 NAT。但是，如果配置 NAT 来转换源地址和目标地址，将不会重写外部地址（“trying” 响应消息的 SIP 报头中的“from”）。因此，在处理 SIP 流量时应使用对象 NAT，从而避免转换目标地址。

请勿为安全级别相同、较低（源）或较高（目标）的接口配置 NAT 或 PAT。不支持此配置。

当与 SIP 结合使用 PAT 时，有以下限制和限定：

- 如果远程终端尝试在 ASA 保护的网络上注册 SIP 代理，在非常特殊的条件下注册会失败，如下所示：
 - 对远程终端配置了 PAT。
 - SIP 注册服务器位于外部网络。
 - 在终端发送给代理服务器的 REGISTER 消息中，联系人字段中的端口缺失。
- 如果在 SIP 设备传输数据包时，该数据包的 SDP 部分的所有者/创建者字段 (o=) 中的 IP 地址与连接字段 (c=) 中的 IP 地址不同，则可能未正确转换 o= 字段中的 IP 地址。这是 SIP 协议的如下局限性造成的：不在 o= 字段中提供端口值。由于 PAT 需要使用端口进行转换，所以转换会失败。
- 使用 PAT 时，任何包含无端口的内部 IP 地址的 SIP 报头字段都可能不会转换，因此，内部 IP 地址将向外泄漏。如果要避免这种泄漏，请配置 NAT 来代替 PAT。

默认 SIP 检测

默认情况下，SIP 检测已通过默认检测映射启用，具体以下：

- SIP 即时消息 (IM) 扩展：已启用。
- SIP 端口的非 SIP 流量：允许。
- 隐藏服务器和终端的 IP 地址：已禁用。
- 掩蔽软件版本和非 SIP URI：已禁用。
- 确保到目标的跳数大于 0：已启用。

- RTP 符合性：未执行。
- SIP 符合性：不执行状态检查和报头验证。

另请注意，加密流量检测未启用。要检测加密流量，必须配置 TLS 代理。

配置 SIP 检测策略映射

如果默认检测行为不能满足网络要求，可以创建 SIP 检测策略映射来自定义 SIP 检测操作。

可以选择创建 SIP 检测类映射来定义 SIP 检测的流量类。另一种方法是，直接在 SIP 检测策略映射中定义流量类。创建类映射与直接在检测映射中定义流量匹配之间的差别在于，前一种做法可以创建更复杂的匹配条件，并且可以重复使用类映射。虽然此过程介绍了检测映射，但类映射中使用的匹配条件与 **Inspection** 选项卡相关步骤中介绍的匹配条件相同。您可以通过以下两种方法来配置 SIP 类映射：依次选择配置 > 防火墙 > 对象 > 类映射 > SIP；或在配置检测映射时创建它们。



提示

除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > SIP。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射以查看映射内容。可以直接更改安全级别，或者点击 **Customize** 编辑映射。此操作过程的剩余步骤假设要自定义或添加映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 在 SIP Inspect Map 对话框的 **Security Level** 视图中，选择最符合所需配置的级别。默认级别为 Low。

如果预设级别之一符合要求，执行到这一步即可。只需点击 **OK**，跳过此操作过程的剩余步骤，并将映射用于服务策略规则中以执行 SIP 检测。

步骤 5 如果需要进一步自定义设置，请点击 **Details** 并执行以下操作：

- a) 点击 **Filtering** 选项卡，选择是要启用 SIP 即时消息 (IM) 扩展还是允许 SIP 端口上出现非 SIP 流量。
- b) 点击 **IP Address Privacy** 选项卡，并选择是否隐藏服务器和终端的 IP 地址。

- c) 点击 **Hop Count** 选项卡，并选择是否确保到目标的跳数大于 0。这样将会检查 Max-Forwards 报头值（在到达目标之前，此值不能为 0）。必须选择要对不符合要求的流量执行的操作（丢弃数据包、断开连接、重置连接或记录连接）以及是启用还是禁用日志记录。
- d) 点击 **RTP Conformance** 选项卡，并选择是否检查流经针孔的 RTP 数据包的协议符合性。如果检查符合性，还可以选择是否根据信令交换限制音频或视频的负载。
- e) 点击 **SIP Conformance** 选项卡，并选择是否启用状态转换检查和报头字段严格验证。对于所选的每个选项，应选择要对不符合要求的流量执行的操作（丢弃数据包、断开连接、重置连接或记录连接）以及是启用还是禁用日志记录。
- f) 点击 **Field Masking** 选项卡，并选择是否检测 Alert-Info 和 Call-Info 报头中的非 SIP URI 以及是否检测 User-Agent 和 Server 报头中的服务器和终端的软件版本。对于所选的每个选项，应选择要执行的操作（掩蔽或记录）以及是启用还是禁用日志记录。
- g) 点击 **TVS Server** 选项卡，并标识信任验证服务服务器（这些服务器使思科统一 IP 电话在 HTTPS 建立过程中可以对应用服务器进行身份验证）。最多可以标识四台服务器；可输入要标识的服务器的 IP 地址，以逗号分隔。SIP 检测会为每个已注册的电话打开用于连接到每台服务器的针孔，由电话确定使用哪个针孔。

可在 CUCM 服务器上配置信任验证服务服务器。如果配置使用非默认端口，请输入端口号（1026 到 32768）。默认端口为 2445。

步骤 6 点击 **Inspections** 选项卡，并定义要基于流量特性实施的特定检测。

可以根据 SIP 类映射定义流量匹配条件，或者直接在检测映射中配置匹配，还可以同时使用这两种方法。

- a) 执行以下任一操作：
 - 点击 **Add** 添加新条件。
 - 选择现有条件并点击 **Edit**。
- b) 选择 **Single Match** 直接定义条件，或选择 **Multiple Match**，在后者情况下可选择 SIP 类映射来定义条件。
- c) 如果在这里定义条件，请选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。例如，如果对字符串“example.com”选择了 No Match，将会从类映射排除任何包含“example.com”的流量。然后，按如下方式配置条件：
 - **Called Party** - 根据所选的正则表达式或正则表达式类匹配 To 报头中指定的被叫方。
 - **Calling Party** - 根据所选的正则表达式或正则表达式类匹配 From 报头中指定的主叫方。
 - **Content Length** - 匹配长度大于指定长度的 SIP 内容报头，该值介于 0 到 65536 字节之间。
 - **Content Type** - 匹配 SDP 类型或与所选正则表达式或正则表达式类匹配的类型的 Content Type 报头。
 - **IM Subscriber** - 根据所选的正则表达式或正则表达式类匹配 SIP IM 用户。
 - **Message Path** - 根据所选的正则表达式或正则表达式类通过报头匹配 SIP。
 - **Request Method** - 匹配 SIP 请求方法：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。

- **Third-Party Registration** - 根据所选的正则表达式或正则表达式类匹配第三方注册的请求者。
- **URI Length** - 匹配所选类型 (SIP 或 TEL) 的 SIP 报头中大于指定长度 (0 到 65536 字节之间) 的 URL。

- d) 选择要对匹配的流量执行的操作 (丢弃数据包、断开连接、重置连接或记录连接) 以及是启用还是禁用日志记录。对于匹配 “invite” 和 “register” 的请求方法, 还可以对数据包数应用每秒速率限制。
- e) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 7 在 SIP Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 SIP 检测服务策略中。

下一步做什么

现在, 您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#), 第 316 页。

瘦客户端控制协议 (SCCP) 检测

SCCP (瘦客户端) 应用检测对数据包数据中的嵌入式 IP 地址和端口号执行转换, 并会动态打开针孔。它还执行其他协议符合性检查和基本状态跟踪。

默认情况下, SCCP 检测已启用。只有需要非默认处理时, 或者要标识 TLS 代理来启用加密流量检测时, 才需要配置这项检测。

以下各节介绍 SCCP 应用检测。

SCCP 检测概述

瘦客户端 (SCCP) 是用于 VoIP 网络的简化协议。使用 SCCP 的思科 IP 电话可共存于 H.323 环境中。与 Cisco CallManager 一起使用时, SCCP 客户端可以与兼容 H.323 的终端进行互操作。

对于 SCCP, ASA 支持 PAT 和 NAT。如果要使用的 IP 电话多于 IP 电话可使用的全局 IP 地址, 必须进行 PAT。通过支持 SCCP 信令数据包的 NAT 和 PAT, 瘦应用检测可确保所有 SCCP 信令和媒体数据包均可通过 ASA。

Cisco CallManager 与思科 IP 电话之间的正常流量使用 SCCP, 这些流量由 SCCP 检测处理, 无需任何特殊配置。另外, ASA 还支持 DHCP 选项 150 和 66, 将 TFTP 服务器的位置发送到思科 IP 电话及其他 DHCP 客户端即可完成操作。思科 IP 电话可能在请求中还包含 DHCP 选项 3 (该选项用于设置默认路由)。



注释 ASA 支持检测来自运行 SCCP 协议版本 22 及更早版本的思科 IP 电话的流量。

支持思科 IP 电话

在思科 CallManager 位于思科 IP 电话较高安全性接口的拓扑中，如果需要对思科 CallManager IP 地址执行 NAT，则映射必须为静态，因为思科 IP 电话需要在其配置中显式指定思科 CallManager IP 地址。静态身份条目允许安全性较高的接口中的思科 CallManager 接受来自思科 IP 电话的注册。

思科 IP 电话需要访问 TFTP 服务器，以下载它们连接到 Cisco CallManager 服务器所需要的配置信息。

当思科 IP 电话位于比 TFTP 服务器低的安全接口上时，必须使用 ACL 来与 UDP 端口 69 上的受保护 TFTP 服务器连接。虽然需要对 TFTP 服务器使用静态条目，但该静态条目不一定必须是身份静态条目。使用 NAT 时，身份静态条目会映射到同一 IP 地址。使用 PAT 时，它会映射到同一 IP 地址和端口。

当思科 IP 电话位于比 TFTP 服务器和思科 CallManager 安全性更高的接口上时，无需 ACL 或静态条目即可允许思科 IP 电话发起连接。

SCCP 检测的局限性

SCCP 检测已经过测试，受思科统一通信管理器 (CUCM) 7.0、8.0、8.6 和 10.5 支持。CUCM 8.5 或 9.x 不支持这项检测。SCCP 检测可能适用于其他版本和产品。

如果为 NAT 或 PAT 配置的内部思科 CallManager 的地址为不同的 IP 地址或端口，则注册外部思科 IP 电话将会失败，因为 ASA 对于通过 TFTP 传输的文件内容不支持 NAT 或 PAT。虽然 ASA 支持 TFTP 消息的 NAT 并会为 TFTP 文件打开针孔，但在电话注册期间，ASA 无法转换通过 TFTP 传输的思科 IP 电话配置文件中嵌入的思科 CallManager IP 地址和端口。



注释 ASA 支持 SCCP 呼叫的状态故障切换，但呼叫建立过程中的呼叫除外。

默认 SCCP 检测

默认情况下，SCCP 检测已启用，默认设置如下：

- 注册：未执行。
- 最大消息 ID：0x181。
- 最小前缀长度：4
- 媒体超时：00:05:00
- 信令超时：01:00:00。
- RTP 符合性：未执行。

另请注意，加密流量检测未启用。要检测加密流量，必须配置 TLS 代理。

配置瘦小客户端 (SCCP) 检测策略映射

要指定消息违反参数时要执行的操作，请创建 SCCP 检测策略映射。然后，可以在启用 SCCP 检测时应用所创建的检测策略映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > SCCP（瘦小）。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射以查看映射内容。可以直接更改安全级别，或者点击 **Customize** 编辑映射。此操作过程的剩余步骤假设要自定义或添加映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 在 SCCP (Skinny) Inspect Map 对话框的 **Security Level** 视图中，选择最符合所需配置的级别。默认级别为 Low。

如果预设级别之一符合要求，执行到这一步即可。只需点击 **OK**，跳过此操作过程的剩余步骤，并将映射用于服务策略规则中以执行 SCCP 检测。

步骤 5 如果需要进一步自定义设置，请点击 **Details** 并执行以下操作：

a) 点击 **Parameters** 选项卡，根据需要选择以下选择：

- **Enforce endpoint registration** - 瘦终端是否必须注册后才能发出或接收呼叫。
- **Maximum Message ID** - 允许的最大 SCCP 站消息 ID。默认最大值是 0x181。十六进制数字可以是 0x0 到 0xffff。
- **SCCP Prefix Length** - 最大和最小 SCCP 前缀长度。默认最小值是 4；没有默认最大值。
- **Timeouts** - 是否设置媒体和信令连接超时以及这些超时的值。默认的媒体超时是 5 分钟，默认的信令超时是 1 小时。

b) 点击 **RTP Conformance** 选项卡，并选择是否检查流经针孔的 RTP 数据包的协议符合性。如果检查符合性，还可以选择是否根据信令交换限制音频或视频的负载。

步骤 6（可选）点击 **Message ID Filtering** 选项卡，以根据 SCCP 消息的站消息 ID 字段标识要丢弃的流量。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

b) 选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。

c) 在 **Value** 字段中，根据十六进制的站消息 ID 值（0x0 到 0xffff）标识流量。可以输入单个消息 ID 的值，或者输入 ID 范围的开始值和结束值。

- d) 选择是启用还是禁用日志记录。操作始终是丢弃数据包。
- e) 点击 **OK** 添加过滤器。根据需要重复上述步骤。

步骤 7 在 SCCP (Skinny) Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 SCCP 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置应用层协议检测](#)，第 316 页。

STUN 检测

WebRTC 客户端使用 RFC 5389 中定义的 NAT 会话穿越工具 (STUN) 进行基于浏览器的实时通信，因而不需要插件。WebRTC 客户端通常使用云 STUN 服务器获悉它们的公共 IP 地址和端口。WebRTC 使用交互式连接建立 (ICE, RFC 5245) 来验证客户端之间的连接。虽然这些客户端可以使用 TCP 或其他协议，但它们通常使用 UDP。

由于防火墙通常会阻止传出 UDP 流量，所以思科 Spark 等 WebRTC 产品在完成连接时可能会遇到问题。如果两端已确认连接检查，STUN 检测可为 STUN 终端打开针孔并实现基本的 STUN 和 ICE 合规，以便允许进行客户端通信。由此，可避免在访问规则中开放新端口来启用这些应用。

对于默认检测类启用 STUN 检测时，系统会监视 TCP/UDP 端口 3478 中的 STUN 流量。该检测仅支持 IPv4 地址和 TCP/UDP。

STUN 检测在 NAT 方面存在一些局限性。对于 WebRTC 流量，支持静态 NAT/PAT44。由于思科 Spark 不需要针孔，所以 Spark 可以支持其他类型的 NAT。另外，您还可以为思科 Spark 使用 NAT/PAT64，包括动态 NAT/PAT。

故障切换和集群模式支持 STUN 检查，因为针孔被复制。但是，设备之间不进行事务 ID 的复制。如果设备在收到 STUN 请求后发生故障，并且另一台设备收到 STUN 响应，则该 STUN 响应将被丢弃。

有关启用 STUN 检测的信息，请参阅[配置应用层协议检测](#)，第 316 页。

语音和视频协议检测的历史

功能名称	版本	功能信息
对 IPv6 的 SIP、SCCP 和 TLS 代理支持	9.3(1)	现在使用 SIP、SCCP 和 TLS 代理（使用 SIP 或 SCCP）时可检查 IPv6 流量。 未修改任何 ASDM 菜单项。

功能名称	版本	功能信息
适用于信任验证服务、NAT66、CUCM 10.5 和 8831 型号电话的 SIP 支持。	9.3(2)	现在，可以在 SIP 检测中配置信任验证服务服务器。还可以使用 NAT66。使用 CUCM 10.5 对 SIP 检测进行了测试。 向 SIP 检测策略映射添加了信任验证服务支持。
改进了多核心 ASA 上的 SIP 检测性能。	9.4(1)	如果有多条 SIP 信令流通过多核 ASA，表明 SIP 检查性能已经改进。但是，如果您使用的是 TLS、电话或 IME 代理，则不会看到性能改进。 未修改任何 ASDM 菜单项。
ASA 集群中的 SIP 检测支持	9.4(1)	您现在可以在 ASA 集群上配置 SIP 检查。控制流可以在任何设备上创建（由于负载均衡），但其子数据流必须驻留在同一设备上。不支持 TLS 代理配置。 未修改任何菜单项。
取消了对电话代理和 UC-IME 代理的 SIP 检查支持。	9.4(1)	配置 SIP 检查后，将无法再使用电话代理或 UC-IME 代理。使用 TLS 代理检查加密流量。 从 Select SIP Inspect Map 服务策略对话框删除了电话代理和 UC-IME 代理。
H.323 检测支持 H.255 FACILITY 消息先于 H.460.18 兼容性的 H.225 SETUP 消息到达。	9.6(1)	现在，当终端符合 H.460.18 的要求时，可将 H.323 检查策略映射配置为允许在 H.225 SETUP 消息之前发出 H.225 FACILITY 消息。 我们为 H.323 检查策略映射中的 Call Attributes 选项卡添加了一个选项。
NAT 会话穿透工具 (STUN) 检测。	9.6(2)	现在，您可以检测 WebRTC 应用程序的 STUN 流量，包括思科 Spark。检测会打开返回流量所需的针孔。 我们向 Add/Edit Service Policy 对话框的 Rule Actions > Protocol Inspection 选项卡中添加了一个选项。
在 TLS 代理和思科统一通信管理器 10.5.2 中支持 TLSv1.2。	9.7(1)	现在，您可以将包含 TLS 代理的 TLSv1.2 与思科 Unified Communications Manager 10.5.2 一起用于加密 SIP 或 SCCP 检查。TLS 代理支持作为 client cipher-suite 命令的一部分添加的附加 TLSv1.2 密码套件。 未修改任何菜单项。



第 17 章

移动网络检测

以下主题介绍用于 LTE 等移动网络协议的应用检测。这些检测需要使用 Carrier 许可证。有关为何需要对某些协议进行检测以及应用检测的总体方法的信息，请参阅[应用层协议检测入门](#)，第 309 页。

- [移动网络检测概述](#)，第 379 页
- [移动网络协议检测的许可](#)，第 385 页
- [GTP 检测默认设置](#)，第 386 页
- [配置移动网络检测](#)，第 386 页
- [监控移动网络检测](#)，第 407 页
- [移动网络检测的历史](#)，第 411 页

移动网络检测概述

以下主题介绍可用于 LTE 等移动网络协议的检测。除检测之外，还有可用于 SCTP 流量的其他服务。

GTP 检测概述

GPRS 隧道协议用于 GSM、UMTS 和 LTE 网络的通用分组无线服务 (GPRS) 流量。GTP 提供隧道控制和管理协议，通过创建、修改和删除隧道来为移动站提供 GPRS 网络接入。此外，GTP 还使用隧道机制来传送用户数据包。

服务提供商网络使用 GTP 通过终端之间的 GPRS 主干隧道传输多协议数据包。在 GTPv0-1 中，GTP 用于网关 GPRS 支持节点 (GGSN) 和服务 GPRS 支持节点 (SGSN) 之间的信令。在 GTPv2 中，信令位于数据包数据网络网关 (PGW) 和服务网关 (SGW) 以及其他终端之间。GGSN/PGW 是 GPRS 无线数据网络与其他网络之间的接口。SGSN/SGW 可执行移动、数据会话管理和数据压缩。

您可以使用 ASA 来防御欺诈漫游的合作伙伴。将设备放在主 GGSN/PGW 和被访问的 SGSN/SGW 终端之间，并对流量应用 GTP 检测。GTP 检测仅可在这些终端之间的流量上运行。在 GTPv2 中，这称为 S5/S8 接口。

GTP 和相关标准由 3GPP（第 3 代合作伙伴项目）定义。有关详细信息，请参阅<http://www.3gpp.org>。

GTP 检测的局限性

以下是 GTP 检测的一些局限性：

- 不支持 GTPv2 捎带消息。它们始终会被丢弃。
- 仅在包含 IMSI（国际移动用户识别码）时支持 GTPv2 紧急 UE 连接。
- GTP 检测不检查早期数据。即恰好在创建会话请求之后但在创建会话响应之前从 PGW 或 SGW 发送的数据。
- 对于 GTPv2，检测最高支持 3GPP 29.274 版本 10 第 13 版。对于 GTPv0/v1，最高支持 3GPP 29.060 版本 9。
- GTP 检测不支持 Inter SGSN 切换到辅助 PDP 情景。检测需要对主 PDP 情景和辅助 PDP 情景执行交接。

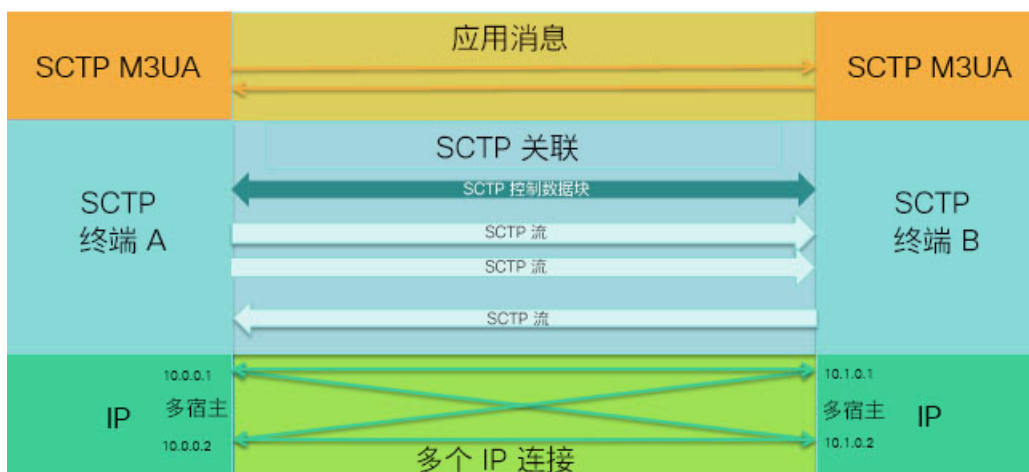
流控制传输协议 (SCTP) 检测和访问控制

RFC 4960 中介绍了 SCTP（流控制传输协议）。该协议支持基于 IP 的电话信令协议 SS7，也是适用于 4G LTE 移动网络架构中多个接口的传输协议。

SCTP 是在协议栈中基于 IP 运行的传输层协议，与 TCP 和 UDP 类似。但是，SCTP 可在基于一个或多个源或目标 IP 地址的两个终端节点之间创建一条逻辑通信通道，称为“关联”。这种行为称为多宿主。关联可在每个节点上定义一组 IP 地址（源和目标）和一个端口。该组中的任何 IP 地址均可作为与此关联相关的数据包的源或目标 IP 地址，从而形成多个连接。在每个连接中，可能存在多个发送消息的流。SCTP 中的流表示逻辑应用数据信道。

下图说明了关联与其流之间的关系。

图 48: SCTP 关联与流之间的关系



如果有 SCTP 流量通过 ASA，您可以基于 SCTP 端口控制访问，并实施应用层检测来启用连接和（可选）过滤负载协议 ID，以便选择性地丢弃应用、记录应用或限制应用速率。



注释 每个节点最多可包含三个 IP 地址。超过三个这一上限的任何地址都将被忽略，不会包含到关联中。此时，辅助 IP 地址的针孔会自动打开。您无需写入访问控制规则来启用它们。

以下部分更加详细地介绍可用于 SCTP 流量的服务。

SCTP 状态检测

SCTP 流量与 TCP 类似，由系统在第 4 层自动检测以确保流量的结构良好并符合具有限制性的 RFC 4960 实施要求。检测和实施以下协议元素：

- 数据块类型、标志和长度。
- 验证标志。
- 源端口和目标端口，以防止关联重定向攻击。
- 执行 ping 操作时没有任何问题。

SCTP 状态检测根据关联状态接受或拒绝数据包：

- 验证初始关联建立的 4 向打开和关闭序列。
- 验证关联和数据流内的 TSN 转发进阶。
- 当由于心跳故障看到 ABORT 数据库时终止关联。SCTP 终端可能发送 ABORT 数据块来响应炸弹攻击。

如果确定不希望执行这些实施检查，可以为特定流量类配置 SCTP 状态绕行，如[配置特定流量类的连接设置（所有服务）](#)，第 429 页中所述。

SCTP 访问控制

您可以为 SCTP 流量创建访问规则。这些规则与基于 TCP/UDP 端口的规则类似，您只需使用 `sctp` 作为协议，端口号为 SCTP 端口。您可以为 SCTP 创建服务对象或组，或者直接指定端口。请参阅以下主题。

- [配置服务对象和服务组](#)，第 31 页
- [配置扩展 ACL](#)，第 45 页
- [配置访问规则](#)，第 17 页

SCTP NAT

您可以向 SCTP 关联建立消息中的地址应用静态网络对象 NAT。虽然您可以配置静态两次 NAT，但不建议这样做，因为 SCTP 关联的目的地部分的拓扑未知。不能使用动态 NAT/PAT。

SCTP 的 NAT 依赖于 SCTP 状态检测，而不是 SCTP 应用层检测。因此，如果配置了 SCTP 状态绕行，则无法对流量应用 NAT。

SCTP 应用层检测

通过在 SCTP 应用上启用 SCTP 检测和过滤，可以进一步优化您的访问规则。您可以根据负载协议标识符 (PPID)，选择性地丢弃、记录或按速率限制 SCTP 流量类。

如果决定对 PPID 进行过滤，请记住以下几点：

- PPID 位于数据分块中，特定数据包可包含多个数据分块，甚至包含一个控制数据块。如果数据包包含一个控制数据块或多个数据分块，即便对其分配的操作为丢弃，该数据包也不会被丢弃。
- 如果使用 PPID 过滤来丢弃数据包或限制数据包速率，请注意发射器会重新发送被丢弃的任何数据包。虽然下次尝试时可能会让 PPID 速率受限制的数据包通过，但 PPID 丢弃的数据包仍会被丢弃。您可能需要评估网络中反复出现这些丢弃所带来的最终结果。

SCTP 的局限性

SCTP 支持包括以下局限性。

- 每个节点最多可包含三个 IP 地址。超过三个这一上限的任何地址都将被忽略，不会包含到关联中。此时，辅助 IP 地址的针孔会自动打开。您无需写入访问控制规则来启用它们。
- 未使用的针孔将在 5 分钟后超时。
- 不支持多宿主终端上的双堆栈 IPv4 和 IPv6 地址。
- 唯一支持的 NAT 类型是网络对象静态 NAT。此外，不支持 NAT46 和 NAT64。
- 仅对 Diameter、M3UA 和基于 SCTP PPID 的检测处理的流量完成 SCTP 数据包分段和重组。
- 不支持 SCTP 中用于动态添加或删除 IP 地址的 ASCONF 数据块。
- 不支持 INIT 和 INIT-ACK SCTP 消息中的主机名参数，它们用于指定可被解析为 IP 地址的主机名。
- 无论是在 ASA 上还是在网络中的其他位置配置，SCTP/M3UA 都不支持等价多路径路由 (ECMP)。利用 ECMP，可通过多个最佳路径将数据包路由至目标。但是，对单一目标的 SCTP/M3UA 数据包响应必须返回到所退出的同一接口。即使该响应可能来自任何 M3UA 服务器，但它必须始终返回到所退出的同一接口。此问题的症状是，SCTP INIT-ACK 数据包被丢弃，您可以在 **show asp drop flow sctp-chunk-init-timeout** 计数器中进行查看：

```
Flow drop:
SCTP INIT timed out (not receiving INIT ACK) (sctp-chunk-init-timeout)
```

如果您遇到此问题，可通过配置到 M3UA 服务器的静态路由，或通过配置基于策略的路由来实施能够确保该 INIT-ACK 数据包经过与 INIT 数据包相同的接口的网络设计，从而解决此问题。

Diameter 检测

Diameter 是用于下一代移动和固定电信网络（例如用于 LTE（长期演进）和 IMS（多媒体子系统）的 EPS（演进的数据包系统）的身份验证、授权和记账 (AAA) 协议。在这些网络中，该协议将取代 RADIUS 和 TACACS。

Diameter 使用 TCP 和 SCTP 作为传输层，并使用 TCP/TLS 和 SCTP/DTLS 保障通信安全。另外，它也可以选择性地提供数据对象加密。有关 Diameter 的详细信息，请参阅 RFC 6733。

Diameter 应用执行服务管理任务，例如决定用户权限、服务授权、服务质量和收费率。虽然 Diameter 应用可出现在 LTE 架构的许多不同控制面板接口上，但 ASA 仅检测以下接口的 Diameter 命令编码和属性-值对 (AVP)：

- S6a: 移动管理实体 (MME) - 家庭订用服务(HSS)。
- S9: PDN 网关 (PDG) - 3GPP AAA 代理/服务器。
- Rx: 策略收费规则功能 (PCRF) - 呼叫会话控制功能 (CSCF)。

Diameter 检测为 Diameter 终端打开针孔，以允许通信。该检测支持 3GPP 版本 12，并符合 RFC 6733 要求。您可以将其用于 TCP/TLS（通过在启用检测时指定 TLS 代理），但不能将其用于 SCTP。使用 Ipsec 可保障 SCTP Diameter 会话的安全。

您可以选择性地使用 Diameter 检测策略映射根据应用 ID、命令代码和 AVP 来过滤流量，以便应用特殊操作，例如丢弃数据包或连接或记录它们。可以为新注册的 Diameter 应用创建自定义 AVP。通过过滤，可以优化您在网络上允许的流量。



注释

默认情况下，允许其他接口上运行的应用的 Diameter 消息通过。虽然无法基于这些不支持应用的命令代码或 AVP 指定操作，但您可以配置 Diameter 检测策略映射，根据应用 ID 丢弃这些应用。

M3UA 检测

MTP3 User Adaptation (M3UA) 是客户端/服务器协议，为基于 IP 的应用提供连接 SS7 网络的网关，以便连接 SS7 消息传递部分 3 (MTP3) 层。使用 M3UA，可以通过 IP 网络运行 SS7 用户部分（例如 ISUP）。M3UA 在 RFC 4666 中定义。

M3UA 使用 SCTP 作为传输层。默认端口为 SCTP 端口 2905。

MTP3 层提供网络功能，例如路由和节点寻址，但使用点代码来识别节点。M3UA 层可交换源点码 (OPC) 和目标点码 (DPC)。这与 IP 使用 IP 地址识别节点的方式类似。

M3UA 检测提供的协议符合具有限制性。您可以选择性地地为特定消息实施严格应用服务器进程 (ASP) 状态检查和其他消息验证。如果要进行状态故障切换或在集群内操作，需要执行严格 ASP 状态检查。但是，严格 ASP 状态检查只能在覆盖模式下运行，如果在 Loadsharing 或广播模式下运行则不起作用（根据 RFC 4666）。该检测假设每个终端有一个且只有一个 ASP。

您可以基于点代码或服务指示符 (SI) 选择性地应用访问策略。此外，还可以基于消息类和类型应用速率限制。

M3UA 协议符合性

M3UA 检测提供以下具有限制性的协议执行。检测丢弃和记录不符合要求的数据包。

- 常见消息信头。检测验证常见信头中的所有字段。
 - 仅限版本 1。
 - 消息长度必须正确。
 - 禁止使用具有保留值的消息类型类。
 - 禁止在消息类内使用无效的消息 ID。
- 负载数据消息。
 - 对于特定类型只允许使用一个参数。
 - 禁止 SCTP 流 0 中存在数据消息。
- 以下消息中必须存在 **Affected Point Code** 字段，否则该消息将被丢弃：目标可用 (DAVA)、目标不可用 (DUNA)、目标状态审核 (DAUD)、信令拥塞 (SCON)、目标用户部分不可用 (DUPU)、目标受限 (DRST)。
- 如果为以下消息启用了消息标记验证，系统将检查和验证某些字段的内容。验证失败的消息将被丢弃。
 - 目标用户部分不可用 (DUPU) - User/Cause 字段必须存在，并且其中必须仅包含有效的原因和用户代码。
 - 错误 - 所有必填字段必须都存在，并且仅包含允许的值。每个错误消息都必须包含该错误代码的必填字段。
 - 通知 - 状态类型和状态信息字段必须仅包含允许的值。
- 如果启用了严格应用服务器进程 (ASP) 状态验证，系统将维护 M3UA 会话的 ASP 状态并基于验证结果允许或丢弃 ASP 消息。如果未启用严格 ASP 状态验证，系统将转发所有 ASP 消息而不进行检测。

M3UA 检测的局限性

以下是 M3UA 检测的一些局限性。

- 对于 M3UA 数据中嵌入的 IP 地址，不支持 NAT。
- M3UA 严格应用服务器进程 (ASP) 状态验证依赖于 SCTP 状态检测。不会对相同流量实施 SCTP 状态绕行和 M3UA 严格 ASP 验证。
- 如果要进行状态故障切换或在集群内操作，需要执行严格 ASP 状态检查。但是，严格 ASP 状态检查只能在覆盖模式下运行，如果在 Loadsharing 或广播模式下运行则不起作用（根据 RFC 4666）。该检测假设每个终端有一个且只有一个 ASP。

RADIUS 计费检测概述

RADIUS 计费检测是为了防止使用 RADIUS 服务器的 GPRS 网络上出现过度计费攻击。虽然实施 RADIUS 计费检测无需 Carrier 许可证，但它毫无意义，除非您正在实施 GTP 检测并已设置 GPRS。

GPRS 网络上的过度计费攻击会导致消费者为他们未使用的服务付费。在这种情况下，恶意攻击者会建立与服务器之间的连接，并从 SGSN 获取 IP 地址。即使攻击者结束呼叫，恶意服务器仍会向其发送数据包；虽然 GGSN 会丢弃这些数据包，但来自服务器的连接仍会保持活动状态。分配给恶意攻击者的 IP 地址将被释放，并重新分配给某个合法用户（该用户将需要为攻击者将会使用的服务付费）。

RADIUS 计费检测可确保流经 GGSN 的流量都是合法流量，从而防止此类攻击。正确配置 RADIUS 计费功能后，ASA 将基于 Radius 计费请求开始消息中的框架 IP 属性与 Radius 计费请求停止消息的匹配终止连接。如果发现停止消息包含框架 IP 属性中的匹配 IP 地址，ASA 将查找源与该 IP 地址匹配的所有连接。

您可以选择配置一个与 RADIUS 服务器预共享的密钥，以便 ASA 可验证消息。如果未配置共享密钥，ASA 则仅检查源 IP 地址是否为允许发送 RADIUS 消息的已配置地址之一。



注释

在启用 GPRS 的情形下使用 RADIUS 计费检测时，ASA 会检查计费请求 STOP 消息中的 3GPP-Session-Stop-Indicator，以便正确处理辅助 PDP 情景。特别是，ASA 要求计费请求 STOP 消息必须包含 3GPP-SGSN-Address 属性，才能终止用户会话和所有相关连接。默认情况下，某些第三方 GGSN 可能不发送此属性。

移动网络协议检测的许可

以下协议的检测需要下表中列出的许可证。

- GTP
- SCTP
- Diameter
- M3UA

型号	许可证要求
<ul style="list-style-type: none"> • ASA 5525-X • ASA 5545-X • ASA 5555-X • ASA 5585-X • ASASM 	Carrier 许可证

型号	许可证要求
ASAv（所有型号）	Carrier 许可证（默认启用）
Firepower 4100 上的 ASA	运营商许可证
Firepower 9300 上的 ASA	运营商许可证
所有其他型号	Carrier 许可证在其他型号上不可用。无法检查这些协议。

GTP 检测默认设置

默认情况下，GTP 检测未启用。但是，如果在未指定检测映射的情况下启用 GTP 检测，将会使用提供以下处理的默认映射。仅在需要不同值的情况下，才需要配置映射。

- 不允许错误。
- 最大请求数为 200。
- 最大隧道数为 500。此值相当于 PDP 情景（终端）的数量。
- GTP 终端超时为 30 分钟。终端包括 GSN（GTPv0、1）和 SGW/PGW（GTPv2）。
- PDP 情景超时是 30 分钟。在 GTPv2 中，此值为承载情景超时。
- 请求超时为 1 分钟。
- 信令超时是 30 分钟。
- 隧道超时为 1 小时。
- T3 响应超时为 20 秒。
- 丢弃并记录未知消息 ID。此行为限于 3GPP 为 S5S8 接口定义的消息。可能允许为其他 GPRS 接口定义的消息，最大程度地减少对它们应用的检测。

如果消息未定义或是在系统不支持的 GTP 版本中进行了定义，则会被视为未知消息。支持版本为 GTPv1 版本 6.1 和 GTPv2 版本 10.13。

配置移动网络检测

默认情况下，移动网络中使用的协议检测未启用。如果要支持移动网络，必须进行配置。

过程

步骤 1（可选。）配置 [GTP 检测策略映射](#)，第 387 页。

步骤 2（可选。）配置 [SCTP 检测策略映射](#)，第 390 页。

步骤 3 (可选。) [配置 Diameter 检测策略映射](#)，第 391 页。

如果要对软件中尚不支持的属性-值对 (AVP) 进行过滤，可以创建自定义 AVP 以用于 Diameter 检测策略映射。请参阅[创建自定义 Diameter 属性-值对 \(AVP\)](#)，第 394 页。

步骤 4 (可选。) 如果要检测加密的 Diameter TCP/TLS 流量，可按如下部分所述创建所需的 TLS 代理：[检查加密的 Diameter 会话](#)，第 395 页

步骤 5 (可选。) [配置 M3UA 检测策略映射](#)，第 401 页

步骤 6 [配置移动网络检测服务策略](#)，第 404 页。

步骤 7 (可选。) [配置 RADIUS 计费检测](#)，第 405 页。

RADIUS 会计检测可防止超额计费 (over-billing) 攻击。

配置 GTP 检测策略映射

如果要对 GTP 流量执行其他参数，而默认映射不能满足需求，则可以创建并配置 GTP 映射。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > GTP。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射以查看映射内容。点击 **Customize** 编辑映射。此操作过程的剩余步骤假设要自定义或添加映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 在 GTP Inspect Map 对话框的 **Security Level** 视图中，查看映射的当前配置。

该视图会指出使用的是默认映射还是自定义映射。如果需要进一步自定义设置，请点击 **Details** 并继续执行此操作步骤。

提示 **IMSI Prefix Filtering** 按钮是配置 IMSI 前缀过滤的快捷方式（下面将会加以说明）。

步骤 5 点击 **Permit Parameters** 选项卡并配置所需的选项。

- **Permit Response** - 当 ASA 执行 GTP 检测时，ASA 默认会丢弃来自 GSN 或 PGW 而 GTP 请求中未指定的 GTP 响应。在 GSN/PGW 终端池中使用负载均衡来提供 GPRS 的效率和扩展性时，会发生这种情况。

要配置 GSN/PGW 轮询以便支持负载均衡，请创建一个指定 GSN/PGW 终端的网络对象组，并为“**From Object Group**”选择该组。同样，为 SGSN/SGW 创建一个网络对象组，并为“**To Object Group**”选择该组。如果 GSN/PGW 响应与 GTP 请求被发送到的 GSN/PGW 属于同一个对象组，并且 SGSN/SGW 位于允许响应 GSN/PGW 向其发送 GTP 响应的对象组中，则 ASA 允许该响应。

网络对象组可通过主机地址或包含终端的子网标识它们。

- **Permit Errors** - 是否允许通过 ASA 发送无效数据包或检测期间遇到错误的数据包，而不是将它们丢弃。

步骤 6 点击 **General Parameters** 选项卡并配置所需的选项：

- **Maximum Number of Requests** - 排队等待响应的最大 GTP 请求数。
- **Maximum Number of Tunnels** - 允许的最大活动 GTP 隧道数。该值相当于 PDP 情景或终端数量。默认值为 500。达到最大隧道数后，新的请求将被丢弃。
- **Enforce Timeout** - 是否为以下行为执行空闲超时。超时格式为 hh:mm:ss。
 - **Endpoint** - 删除 GTP 终端之前允许处于非活动状态的最长时间。
 - **PDP-Context** - 删除 GTP 会话的 PDP 情景之前允许处于非活动状态的最长时间。在 GTPv2 中，这属于承载情景。
 - **Request** - 从请求队列中删除某个请求之前允许处于非活动状态的最长时间。对丢弃请求的任何后续响应也将被丢弃。
 - **信令** - 删除 GTP 信令之前允许处于非活动状态的最长时间。
 - **T3 响应超时** - 移除连接之前允许处于非活动状态的最长时间。
 - **Tunnel** - 终止 GTP 隧道之前允许处于非活动状态的最长时间。

步骤 7 如有需要，请点击 **IMSI Prefix Filtering** 选项卡并配置 IMSI 前缀过滤。

默认情况下，安全设备不检查有效的移动设备国家/地区代码 (MCC)/移动网络代码 (MNC) 组合。如果配置 IMSI 前缀过滤，接收到的数据包 IMSI 中的 MCC 和 MNC 将会与配置的 MCC/MNC 组合进行比较，如果不匹配，数据包将被丢弃。

移动设备国家/地区代码是非零的三位数值；应在一位或两位数值前添加零作为前缀。移动网络代码是两位或三位数值。

可添加所有允许的 MCC 和 MNC 组合。默认情况下，ASA 不会检查 MNC 和 MCC 组合的有效性，所以您必须验证配置组合的有效性。有关 MCC 和 MNC 代码的详细信息，请参阅 ITU E.212 建议《*Identification Plan for Land Mobile Stations*》（陆地移动站识别计划）。

步骤 8 点击 **Inspections** 选项卡，并定义要基于流量特性实施的特定检测。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。

- 选择现有条件并点击 **Edit**。
- b) 选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。然后，配置条件：
- **Access Point Name** - 根据指定的正则表达式或正则表达式类匹配接入点名称。默认情况下，会检测所有具有有效接入点名称的消息，且允有任何名称。
 - **Message ID** - 匹配消息 ID（范围是 1 到 255）。可以指定一个值或值范围。必须指定该消息适用于 GTPv1（包括 GTPv0）还是 GTPv2。默认情况下，允许所有有效的消息 ID。
 - **Message Length** - 匹配 UDP 负载长度介于指定的最小长度和最大长度之间的消息。
 - **Version** - 匹配 GTP 版本（范围是 0 到 255）。可以指定一个值或值范围。默认情况下，允许所有 GTP 版本。
 - **MSISDN** - 根据指定的正则表达式或正则表达式类，匹配创建 PDP 情景请求、创建会话请求和修改承载响应消息中的移动站点国际用户目录编号 (MSISDN) 信息元素。正则表达式可根据前 x 位数识别特定的 MSISDN 或 MSISDN 范围。MSISDN 过滤仅支持 GTPv1 和 GTPv2。
 - **选择模式** - 匹配创建 PDP 情景请求中的选择模式信息元素。选择模式指定消息中的无线接入点名称 (APN) 来源，可以是以下项目之一。选择模式过滤仅支持 GTPv1 和 GTPv2。
 - 0 - 已验证。由移动站点或网络提供 APN，并且已验证订用。
 - 1 - 移动站点。由移动站点提供 APN，并且已验证订用。
 - 2 - 网络。由网络提供 APN，并且已验证订用。
 - 3 - 保留，未使用。
- c) 对于消息 ID 匹配，请选择是要丢弃数据包还是要对数据包应用每秒速率限制。对于所有其他匹配，操作是丢弃数据包。对于所有匹配，可以选择是否启用日志记录。
- d) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 9 点击**防重放保护**选项卡并配置防重放选项。

- **启用数据包重放窗口** - 是否通过为 GTP-U 消息指定滑动窗口来启用防重放。滑动窗口的大小取决于消息的数量，可以为 128、256、512 或 1024。当有效消息出现时，窗口会移动到新的序列号。序列号在 0 至 65535 范围内，在其达到最大值时回卷，并且它们对每个 PDP 情景都是唯一的。如果消息的序列号在窗口以内，则视为有效消息。防重放有助于防范会话劫持或 DoS 攻击，在黑客捕获 GTP 数据包并进行重放时，可能发生这些攻击。

步骤 10 点击**用户欺骗**选项卡并配置防欺骗选项。

- **GTP 报头检查** - 是否检查 GTP 数据包的内部负载为有效的 IP 数据包，如果其包含非 IP 报头，则将数据包其丢弃。您必须选择此选项以实施防欺骗。
- **防欺骗** - 是否检查内部负载的 IP 报头中的移动用户 IP 地址与 GTP 控制消息（例如创建会话响应）中分配的 IP 地址匹配，如果 IP 地址不匹配，则将消息丢弃。黑客可以使用通过 GTP-C 分

配的 IP 地址之外的另一个 IP 地址来伪装（假冒）另外一个客户。防欺骗功能会检查所用的 GTP-U 地址是否确实是使用 GTP-C 分配的地址。该检查支持 IPv4、IPv6 和 IPv4v6 PDN 类型。

如果移动站点使用 DHCP 获取其地址，GTPv2 中的最终用户 IP 地址将为 0.0.0.0 (IPv4) 或 *prefix::0* (IPv6)，那么在这种情况下，系统将会使用在内部数据包中找到的第一个 IP 地址来更新最终用户 IP 地址。您可以使用以下关键字来更改 DHCP 获取的地址的默认行为：

- **GTPV2-DHCP-ByPass** - 不要更新 0.0.0.0 或 *prefix::0* 地址。而是允许最终用户 IP 地址为 0.0.0.0 或 *prefix::0* 的数据包。使用 DHCP 获取 IP 地址时，此选项会绕过防欺骗检查。
- **GTPV2-DHCP-DROP** - 不要更新 0.0.0.0 或 *prefix::0* 地址。而是丢弃最终用户 IP 地址为 0.0.0.0 或 *prefix::0* 的所有数据包。此选项可防止使用 DHCP 获取 IP 地址的用户访问。

步骤 11 在 GTP Inspect Map 对话框中点击 **OK**。

这样即可将检测映射用于 GTP 检测服务策略中。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置移动网络检测服务策略](#)，第 404 页。

配置 SCTP 检测策略映射

要基于速率限制等特定应用的负载协议标识符 (PPID) 将替代操作应用于 SCTP 流量，请创建服务策略要使用的 SCTP 检测策略映射。



注释 PPID 位于数据分块中，特定数据包可包含多个数据分块，甚至包含一个控制数据块。如果数据包包含一个控制数据块或多个数据分块，即便对其分配的操作为丢弃，该数据包也不会被丢弃。例如，如果将 SCTP 检测策略映射配置为丢弃 PPID 26，而 PPID 26 数据分块与包含 Diameter PPID 数据分块的数据包组合在一起，则该数据包不会被丢弃。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > SCTP。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射并点击 **Edit**。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 基于 SCTP 数据分块中的 PPID 丢弃、按速率限制或记录流量。

- a) 执行以下任一操作：
 - 点击 **Add** 添加新条件。
 - 选择现有条件并点击 **Edit**。
- b) 选择条件的匹配类型：**Match**（流量必须匹配 PPID）或 **No Match**（流量不必匹配 PPID）。
例如，如果在 Diameter PPID 中选择 No Match，则该类映射中将排除 Diameter 之外的所有 PPID。
- c) 选择 **Minimum Payload PID**，并且可选择要匹配的 **Maximum Payload PID**。
可以按名称或编号 (0-4294967295) 输入 PPID。点击每个字段中的 ... 按钮，可从 PPID 列表中选择项目。如果选择了最大 PPID，则该匹配适用于 PPID 的范围
您可以在以下网址查找当前的 SCTP PPID 列表：
<http://www.iana.org/assignments/sctp-parameters/sctp-parameters.xhtml#sctp-parameters-25>。
- d) 选择丢弃（并记录）、记录还是按速率限制（单位：千位/秒，Kbps）匹配的数据包。
- e) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 5 点击 SCTP Inspect Map 对话框中的 **OK**。

现在，您即可在 SCTP 检测服务策略中使用检测映射。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置移动网络检测服务策略](#)，第 404 页。

配置 Diameter 检测策略映射

您可以创建 Diameter 检测策略映射来过滤各种 Diameter 协议元素。然后，可以选择性地丢弃或记录连接。

要配置 Diameter 消息过滤，必须按照 RFC 和技术规范中的定义充分了解这些协议元素。例如，IETF 包含注册应用、命令代码和属性-值对的列表（网址：

<http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml>），但 Diameter 检测并非支持列出的所有项目。有关它们的技术规范，请参阅 3GPP 网站。

您可以选择创建 Diameter 检测类映射来定义 Diameter 检测的消息过滤条件。另一种选项是，直接在 Diameter 检测策略映射中定义过滤条件。创建类映射与直接在检测映射中定义过滤条件的差别在于，您可以创建更复杂的匹配条件，并且可以重复使用类映射。虽然此过程介绍了检测映射，但类映射中使用的匹配条件与 **Inspection** 选项卡相关步骤中介绍的匹配条件相同。您可以通过以下两种方法来配置 Diameter 类映射：依次选择 **配置 > 防火墙 > 对象 > 类映射 > Diameter**；或在配置检测映射时创建它们。



提示 除了以下所述的操作步骤外，还可以在创建服务策略时配置检测映射。无论采用哪种方法创建，映射的内容都相同。

开始之前

某些流量匹配选项使用正则表达式实现匹配。如果要使用这些方法之一，应首先创建正则表达式或正则表达式类映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > Diameter。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射，然后点击 **Edit** 查看其内容。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 点击 **Parameters** 选项卡，选择所需的选项。是否要记录包含不支持 Diameter 元素的消息。

- **Unsupported Parameters** - 是否要记录包含不支持 Diameter 元素的消息。您可以记录不受支持的 **Application ID**、**Command Code** 或 **Attribute Value Pair** 元素。
- **Strict Diameter Validation Parameters** - 启用符合 RFC 6733 要求的严格的 Diameter 协议。默认情况下，检测可确保 Diameter 框架符合 RFC。您可以添加会话相关的消息验证和状态机器验证。

步骤 5 点击 **Inspections** 选项卡，并定义要基于流量特性实施的特定检测。

您可以通过基于 Diameter 类映射和/或直接在检测映射中配置匹配的方式来定义流量匹配条件。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

b) 选择 **Single Match** 直接定义条件，或选择 **Multiple Match**，在后者情况下可选择定义条件的 Diameter 类映射。

c) 如果在这里定义条件，请选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。然后，按如下方式配置条件：

- **Application ID** - 输入 Diameter 应用名称或编号 (0-4294967295)。如果要匹配某个连续编号的应用范围，可以再添加一个 ID。您可以按应用名称或编号来定义范围，该范围将适用于第一个 ID 和第二个 ID 之间的所有编号。

这些应用会注册到 IANA。以下是支持的核心应用，但您可以对其他应用进行过滤。

- **3gpp-rx-ts29214** (16777236)
- **3gpp-s6a** (16777251)
- **3gpp-s9** (16777267)
- **common-message** (0)。这是基础 Diameter 协议。

- **Command Code** - 输入 Diameter 命令代码名称或编号 (0-4294967295)。如果要匹配某个连续编号的命令代码范围，可以再添加一个代码。您可以按命令代码名称或编号来定义范围，该范围将适用于第一个代码和第二个代码之间的所有编号。

例如，要匹配“功能交换请求/应答”命令代码 CER/CEA，请输入 **cer-cea**。

- **Attribute Value Pair** - 您可以仅按属性、按 AVP 的范围或基于属性值的某个 AVP 匹配 AVP。对于 **AVP Begin Value**，您可以指定自定义 AVP 的名称或已在 RFC 或 3GPP 技术规范中注册且受该软件直接支持的某个 AVP 的名称。点击该字段的 ... 按钮可从列表中选择项目。

如果要匹配 AVP 的范围，请仅按编号指定 **AVP End Value**。如果要按 AVP 的值匹配 AVP，则无法指定第二个代码。

您可以指定可选的 **Vendor ID**（范围为 0-4294967295）来进一步优化匹配。例如，3GPP 供应商 ID 为 10415，IETF 为 0。

只有 AVP 的数据类型受支持，才能配置值匹配。例如，可以为具有地址数据类型的 AVP 指定 IP 地址。AVP 列表显示每项的数据类型。指定值的方式因 AVP 数据类型而异：

- **Diameter Identity**、**Diameter URI**、**Octet String** - 选择正则表达式或正则表达式类对象来匹配这些数据类型。
- **Address** - 指定要匹配的 IPv4 或 IPv6 地址。例如，10.100.10.10 或 2001:DB8::0DB8:800:200C:417A。
- **Time** - 指定开始和结束日期及时间。两者均为必填项目。时间采用 24 小时格式。
- **Numeric** - 指定编号的范围。有效的编号范围取决于数据类型：
 - **Integer32**: -2147483647 到 2147483647
 - **Integer64**: -9223372036854775807 到 9223372036854775807
 - **Unsigned32**: 0 到 4294967295
 - **Unsigned64**: 0 到 18446744073709551615
 - **Float32**: 小数点表示方式，精度为 8 位数
 - **Float64**: 小数点表示方式，精度为 16 位数

d) 选择要对匹配的流量执行的操作：丢包、断开连接或日志记录。

e) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 6 点击 Diameter Inspect Map 对话框中的 **OK**。

现在，您即可在 Diameter 检测服务策略中使用检测映射。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置移动网络检测服务策略](#)，第 404 页。

创建自定义 Diameter 属性-值对 (AVP)

定义和注册新属性-值对 (AVP) 后，即可创建自定义 Diameter AVP 在 Diameter 检测策略映射中定义和使用它们。通过 RFC 或定义 AVP 的其他来源可获得创建 AVP 所需的信息。

仅当希望在用于 AVP 匹配的 Diameter 检测策略映射或类映射中使用自定义 AVP 时创建它们。

过程

步骤 1 依次选择 **Configuration > Firewall > Objects > Inspect Maps > Diameter AVP**。

步骤 2 点击 **Add** 以创建新 AVP。

在编辑 AVP 时，只能更改说明。

步骤 3 配置以下选项：

- **Name** - 要创建的自定义 AVP 的名称，最长为 32 个字符。在定义属性-值对匹配时，可在 Diameter 检测策略映射或类映射中引用此名称。
- **Custom Code** - 自定义 AVP 代码值，范围介于 256-4294967295 之间。不能输入系统中已定义的代码和供应商 ID 组合。
- **Data Type** - AVP 的数据类型。可以定义以下类型的 AVP。如果新 AVP 的类型与之不同，则无法为其创建自定义 AVP。
 - 地址（用于 IP 地址）
 - Diameter 身份
 - Diameter 统一资源标识符 (URI)
 - 32 位浮点数值
 - 64 位浮点数值
 - 32 位整数
 - 64 位整数
 - 二进制八位数字符串
 - 时间
 - 32 位无符号整数
 - 64 位无符号整数
- **Vendor ID** - （可选。）定义 AVP 的供应商的 ID 编号，范围介于 0-4294967295 之间。例如，3GPP 供应商 ID 为 10415，IETF 为 0。
- **Description** - （可选。）AVP 的说明，最长 80 个字符。

步骤 4 点击确定。

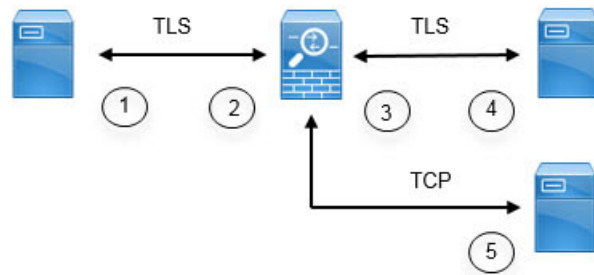
检查加密的 Diameter 会话

如果 Diameter 应用通过 TCP 使用加密数据，则检测功能看不到数据包的内部来实施消息过滤规则。因此，如果创建过滤规则和并希望也将它们应用于加密的 TCP 流量，必须配置 TLS 代理。另外，当希望对加密流量实施严格协议时，也需要代理。此配置不适用于 SCTP/DTLS 流量。

TLS 代理相当于中间人。它可以解密流量、进行检测、重新加密，再将其发送到预期目标。因此，连接的两端、Diameter 服务器和 Diameter 客户端必须信任 ASA，而且所有各方必须具有所需的证书。您必须全面了解实施 TLS 代理所需的数字证书。请阅读 ASA 常规配置指南中关于数字证书的一章。

下图显示 Diameter 客户端与服务器及 ASA 之间的关系以及建立证书所需的认证。在此模式中，Diameter 客户端是 MME（移动管理模块），而非最终用户。链路两端的 CA 证书分别用于对链路另一端的证书签名。例如，ASA 代理 TLS 服务器 CA 证书用于对 Diameter/TLS 客户端证书签名。

图 49: Diameter TLS 检测



1	Diameter TLS 客户端 (MME) • 客户端身份证书 • 用来对 ASA TLS 代理服务器身份证书签名的 CA 证书	2	ASA 代理 TLS 服务器 • 服务器身份证书 • 用来对 Diameter TLS 客户端身份证书签名的 CA 证书
3	ASA 代理 TLS 客户端 • 客户端身份（静态或 LDC）证书 • 用来对 Diameter TLS 服务器身份证书签名的 CA 证书	4	Diameter TLS 服务器（完全代理） • 服务器身份证书 • 用来对 ASA 代理 TLS 客户端身份证书签名的 CA 证书
5	Diameter TCP 服务器（TLS 卸载）。	—	—

您可以使用以下选项为 Diameter 检测配置 TLS 代理：

- 完全 TLS 代理 - 加密 ASA 与 Diameter 客户端以及 ASA 与 Diameter 服务器之间的流量。您可以使用以下选项建立与 TLS 服务器之间的信任关系：

- 使用静态代理客户端信任点。当与 Diameter 服务器通信时，ASA 会为每个 Diameter 客户端提供相同的证书。一方面，由于所有客户端看起来相同，所以 Diameter 服务器无法为每个客户端提供不同的服务。另一方面，此选项比 LDC 方法的速度更快。
- 使用本地动态证书 (LDC)。如果使用此选项，当与 Diameter 服务器通信时，ASA 会为每个 Diameter 客户端提供唯一证书。除公共密钥和来自 ASA 的新签名外，LDC 会保留收到的客户端身份证书的所有字段。使用这种方法，Diameter 服务器可更好地监控客户端流量，从而可以基于客户端证书特征提供不同的服务。
- TLS 卸载 - 加密 ASA 与 Diameter 客户端之间的流量，但在 ASA 与 Diameter 服务器之间使用明文连接。如果 Diameter 服务器与 ASA 位于同一数据中心，而您确定设备之间的流量不会离开受保护区域，则此选项是可行的。由于使用 TLS 卸载可减少所需的加密处理工作量，故可以提高性能。该方法应该是这些选项中速度最快的选项。Diameter 服务器只能基于客户端 IP 地址应用不同的服务。

以上三个选项对 ASA 与 Diameter 客户端之间的信任关系均采用相同的配置。



注释 TLS 代理使用 TLSv1.0 - 1.2。您可以配置 TLS 版本和加密套件。

以下主题介绍如何为 Diameter 检测配置 TLS 代理。

配置服务器与 Diameter 客户端的信任关系

ASA 相当于与 Diameter 客户端相关的 TLS 代理服务器。要建立互信关系，请执行以下操作：

- 需要将用于对 ASA 服务器证书签名的证书颁发机构 (CA) 证书导入到 Diameter 客户端。此证书可能位于客户端的 CA 证书存储中或客户端使用的某些其他位置。有关证书使用的具体详细信息，请参阅客户端文档。
- 需要导入用于对 Diameter TLS 客户端证书签名的 CA 证书，以便 ASA 可信任该客户端。

以下操作步骤介绍如何导入用于对 Diameter 客户端证书签名的 CA 证书，以及如何导入用于 ASA TLS 代理服务器的身份证书。您可以不导入身份证书，而是在 ASA 上创建自签名证书。或者，也可以在创建 TLS 代理时导入这些证书。

过程

步骤 1 将用于对 Diameter 客户端证书签名的 CA 证书导入到 ASA 信任点。

此步骤使 ASA 可以信任 Diameter 客户端。

- 依次选择 **Configuration > Firewall > Advanced > Certificate Management > CA Certificates**。
- 点击 **Add**，并为信任点输入一个名称。例如 **diameter-clients**。
- 添加证书。

可以从文件中导入证书，粘贴 PEM 格式的证书或使用 SCEP 导入证书。

d) 点击 **Install Certificate**。

步骤 2 导入证书，并为 ASA 代理服务器的身份证书和密钥对创建信任点。

此步骤使 Diameter 客户端可以信任 ASA。

- a) 依次选择 **Configuration > Firewall > Advanced > Certificate Management > Identity Certificates**。
- b) 点击 **Add**，并为信任点输入一个名称。例如 **tls-proxy-server-tp**。
- c) 选择 **Import the identity certificate from a file**，输入解密密码，并选择文件（pkcs12 格式）。
或者，您也可以创建一个新证书。
- d) 点击 **Add Certificate**。

使用静态客户端证书为 Diameter 检测配置完整 TLS 代理

如果 Diameter 服务器可接受所有客户端使用同一证书，您可以为 ASA 设置一个静态客户端证书，用来与 Diameter 服务器通信。

要实现此配置，需要在 ASA 与客户端（详见[配置服务器与 Diameter 客户端的信任关系](#)，第 396 页）以及 ASA 与 Diameter 服务器之间建立互信关系。以下是 ASA 和 Diameter 服务器的信任要求。

- 您需要导入用来对 Diameter 服务器身份证书签名的 CA 证书，以便 ASA 在 TLS 握手期间可验证该服务器的身份证书。
- 需要导入也受 Diameter 服务器信任的客户端证书。如果 Diameter 服务器尚不信任该证书，请将用于签名的 CA 证书导入该服务器。有关详细信息，请参阅 Diameter 服务器的文档。

过程

步骤 1 依次选择 **Configuration > Firewall > Unified Communications > TLS Proxy**。

步骤 2 点击 **Add**。

步骤 3 为 TLS 代理命名，例如 **diameter-tls-static-proxy**。点击 **Next**。

步骤 4 选择在[配置服务器与 Diameter 客户端的信任关系](#)，第 396 页中添加的 TLS 服务器代理身份证书。点击 **Next**。

如果尚未创建身份证书，可以点击 **Manage** 进行添加。此外，也可以点击 **Install TLS Server's Certificate** 安装 Diameter 客户端的 CA 证书。

或者，可以通过将算法从可用算法移到活动算法列表来定义服务器可使用的安全算法（密码）。如果未指定密码，则使用默认系统密码。

注释 为了便于测试，或者如果您确定可以信任 Diameter 客户端，可以跳过此步骤并在 TLS 代理配置中取消选择 **Enable client authentication during TLS Proxy handshake**。

步骤 5 选择 **Specify the proxy certificate for TLS client** 并执行以下操作：

- a) 选择用于 ASA TLS 代理客户端的证书。

如果尚未添加证书，请点击 **Manage** 立即添加。

- b) 如果尚未添加用于对 Diameter 服务器证书签名的 CA 证书，请点击 **Install TLS Client's Certificate** 进行添加。
- c) (可选。) 通过将算法从可用算法移到活动算法列表中，定义客户端可使用的安全算法（密码）。

如果未定义 TLS 代理可使用的密码，该代理将使用 **Configuration > Device Management > Advanced > SSL Settings** 加密设置定义的全局密码套件。默认情况下，全局密码等级为中等，这意味着除 NULL-SHA、DES-CBC-SHA 和 RC4-MD5 之外，所有密码均可用。仅在不希望使用 ASA 上通用的套件而使用其他套件时指定 TLS 特定代理密码。

- d) 点击 **Next**。

步骤 6 点击 **Finish**，然后点击 **Apply**。

下一步做什么

现在，您即可在 Diameter 检测中使用 TLS 代理。请参阅[配置移动网络检测服务策略](#)，第 404 页。

为 Diameter 检测配置支持本地动态证书的完全 TLS 代理

如果 Diameter 服务器对于每个客户端需要唯一的证书，可以配置 ASA 来生成本地动态证书 (LDC)。这些证书可在客户端连接持续时间内共存，然后则被删除。

要实现此配置，需要在 ASA 与客户端（详见[配置服务器与 Diameter 客户端的信任关系](#)，第 396 页）以及 ASA 与 Diameter 服务器之间建立互信关系。该配置与[使用静态客户端证书为 Diameter 检测配置完整 TLS 代理](#)，第 397 页中所述的配置类似，但不是导入 Diameter 客户端证书，而是在 ASA 上设置 LDC。以下是 ASA 和 Diameter 服务器的信任要求。

- 您需要导入用来对 Diameter 服务器身份证书签名的 CA 证书，以便 ASA 在 TLS 握手期间可验证该服务器的身份证书。
- 需要创建 LDC 信任点。需要导出 LDC 服务器的 CA 证书，并将其导入到 Diameter 服务器。导出步骤如下所述。有关导入证书的信息，请参阅 Diameter 服务器文档。

过程

步骤 1 依次选择 **Configuration > Firewall > Unified Communications > TLS Proxy**。

步骤 2 点击 **Add**。

步骤 3 为 TLS 代理命名，例如 **diameter-tls-ldc-proxy**。

步骤 4 选择在[配置服务器与 Diameter 客户端的信任关系](#)，第 396 页中添加的 TLS 服务器代理身份证书。点击 **Next**。

如果尚未创建身份证书，可以点击 **Manage** 进行添加。此外，也可以点击 **Install TLS Server's Certificate** 安装 Diameter 客户端的 CA 证书。

或者，可以通过将算法从可用算法移到活动算法列表来定义服务器可使用的安全算法（密码）。如果未指定密码，则使用默认系统密码。

注释 为了便于测试，或者如果您确定可以信任 Diameter 客户端，可以跳过此步骤并在 TLS 代理配置中取消选择 **Enable client authentication during TLS Proxy handshake**。

步骤 5 选择 **Specify the internal Certificate Authority to sign for local dynamic certificates**，并执行以下操作（忽略与 IP 电话相关的任何文本）。

此操作步骤假设您要创建新的证书和密钥。如果您已创建所需的证书和密钥，请选择它们并移至安全算法步骤。

- a) 对于 Local Dynamic Certificate Key Pair，点击 **New**。（您可能需要调整对话框大小，才能看到该按钮。）
- b) 使用新密钥对名称创建一个通用的 RSA 证书，例如 **ldc-signer-key**。点击 **Generate Now** 以创建密钥。

您将返回到 Manage Identity Certificates 对话框。

- c) 选择 **Certificate**，然后点击 **Manage** 为 ASA TLS 代理客户端创建证书和密钥。
- d) 点击 Manage Identity Certificates 对话框中的 **Add**。
- e) 为信任点命名，例如 **ldc-server**。
- f) 选择 **Add a new identity certificate**。
- g) 对于 **Key Pair**，选择您为本地动态证书密钥创建的同一密钥。
- h) 对于 **Certificate Subnet DN**，选择您所需的可区分名称属性。

设备通用名称采用默认值。检查 Diameter 应用对于主题名称是否具有特定要求。

- i) 选择 **Generate self-signed certificate**。这是必需要求。
- j) 选择 **Act as a local certificate authority and issue dynamic certificates to TLS Proxy**。此选项将使此证书变成 LDC 颁发机构。
- k) 点击 **Add Certificate**。

您将返回到 Manage Identity Certificates 对话框。

- l) 选择您刚才创建的证书，并点击 **Export**。

您需要导出该证书，才能将其导入到 Diameter 服务器。指定文件名和 PEM 格式，然后点击 **Export Certificate**。

您将返回到 Manage Identity Certificates 对话框。

- m) 仍然选择该证书，点击 **OK**。

您将返回到 TLS Proxy 向导。如果在 **Certificate** 字段未选择该证书，现在请选择该证书。

- n) （可选。）通过将算法从可用算法移到活动算法列表中，定义客户端可使用的安全算法（密码）。

如果未定义 TLS 代理可使用的密码，该代理将使用 **Configuration > Device Management > Advanced > SSL Settings** 加密设置定义的全局密码套件。默认情况下，全局密码等级为中等，

这意味着除 NULL-SHA、DES-CBC-SHA 和 RC4-MD5 之外，所有密码均可用。仅在不希望使用 ASA 上通用的套件而使用其他套件时指定 TLS 特定代理密码。

o) 点击 **Next**。

步骤 6 点击 **Finish**，然后点击 **Apply**。

步骤 7 现在即可将 LDC CA 证书导入到 Diameter 服务器。有关操作步骤，请参阅 Diameter 服务器文档。请注意，这些数据为 Base64 格式。如果您的服务器需要二进制或 DER 格式，需要使用 OpenSSL 工具来转换格式。

下一步做什么

现在，您即可在 Diameter 检测中使用 TLS 代理。请参阅[配置移动网络检测服务策略](#)，第 404 页。

为 Diameter 检测配置支持 TLS 分流的 TLS 代理

如果确定 ASA 与 Diameter 服务器之间的网络路径安全，可避免 ASA 与服务器之间加密数据的性能成本。使用 TLS 分流，TLS 代理可加密/解密 Diameter 客户端与 ASA 之间的会话，但对于 Diameter 服务器则使用明文。

要实现这种配置，只需在 ASA 与客户端之间建立互信关系，由此可简化配置。在执行以下步骤之前，请完成[配置服务器与 Diameter 客户端的信任关系](#)，第 396 页中的步骤。

过程

步骤 1 依次选择 **Configuration > Firewall > Unified Communications > TLS Proxy**。

步骤 2 点击 **Add**。

步骤 3 为 TLS 代理命名，例如 **diameter-tls-offload-proxy**。

步骤 4 选择在[配置服务器与 Diameter 客户端的信任关系](#)，第 396 页中添加的 TLS 服务器代理身份证书。点击 **Next**。

如果尚未创建身份证书，可以点击 **Manage** 进行添加。此外，也可以点击 **Install TLS Server's Certificate** 安装 Diameter 客户端的 CA 证书。

或者，可以通过将算法从可用算法移到活动算法列表来定义服务器可使用的安全算法（密码）。如果未指定密码，则使用默认系统密码。

注释 为了便于测试，或者如果您确定可以信任 Diameter 客户端，可以跳过此步骤并在 TLS 代理配置中取消选择 **Enable client authentication during TLS Proxy handshake**。

步骤 5 选择 **Configure the proxy client to use clear text to communicate with the remote TCP client**，然后点击 **Next**。

步骤 6 点击 **Finish**，然后点击 **Apply**。

步骤 7 由于 Diameter 端口与 TCP 和 TLS 不同，所以需配置一个 NAT 规则将 TCP 端口转换为 TLS 端口，以便流量从 Diameter 服务器流到客户端。

为每台 Diameter 服务器创建一个对象 NAT 规则。

- a) 依次选择 **Configuration > Firewall > NAT**。
- b) 依次点击 **Add > Object NAT Rule**。
- c) 配置基本属性：
 - **Name** - 对象名称，例如 DiameterServerA。
 - **Type**（对于对象）- 选择 **Host**。
 - **IP Version** - IPv4 或 IPv6，视具体情况而定。
 - **IP Address** - Diameter 服务器的 IP 地址，例如 10.100.10.10。
 - **Add Automatic Address Translation** - 确保选择此选项。
 - **Type**（对于 NAT 规则）- 选择 **Static**。
 - **Translated Addr** - Diameter 服务器端 IP 地址。此项与对象的 IP 地址相同，例如 10.100.10.10。
- d) 点击 **Advanced**，并配置以下 **Interface** 和 **Service** 选项：
 - **Source Interface** - 选择连接到 Diameter 服务器的接口。
 - **Destination Interface** - 选择连接到 Diameter 客户端的接口。
 - **Protocol** - 选择 **TCP**。
 - **Real Port** - 输入 3868，即默认 Diameter TCP 端口号。
 - **Mapped Port** - 输入 5868，即默认 Diameter TLS 端口号。
- e) 点击 **OK**，然后再次点击 Add Network Object 对话框中的 **OK**。

下一步做什么

现在，您即可在 Diameter 检测中使用 TLS 代理。请参阅[配置移动网络检测服务策略](#)，第 404 页。

配置 M3UA 检测策略映射

使用 M3UA 检测策略映射可基于点代码配置访问控制。此外，也可以按类和类型丢弃消息和对其应用速率限制。

默认点代码格式为 ITU。如果您使用其他格式，请在策略映射中指定所需的格式。

如果不希望基于点代码或消息类应用策略，则无需配置 M3UA 策略映射。可以启用不含映射的检测。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > M3UA。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射，然后点击 **Edit** 编辑该映射。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 点击 **Parameters** 选项卡并配置所需的选项：

- **SS7** - 网络中使用的 SS7 变量：ITU、ANSI、Japan、China。此选项决定编码的有效格式。配置该选项并部署 M3UA 策略后，无法再对其更改，除非首先删除该策略。默认变量为 ITU。
- **Enable M3UA Application Server Process (ASP) state validation** - 是否执行严格应用服务器进程 (ASP) 状态验证。系统将维护 M3UA 会话的 ASP 状态，并基于验证结果允许或丢弃 ASP 消息。如果未启用严格 ASP 状态验证，系统将转发所有 ASP 消息而不进行检测。如果要进行状态故障切换或在集群内操作，需要执行严格 ASP 状态检查。但是，严格 ASP 状态检查只能在覆盖模式下运行，如果在 Loadsharing 或广播模式下运行则不起作用（根据 RFC 4666）。该检测假设每个终端有一个且只有一个 ASP。
- **Enforce Timeout > Endpoint** - 删除 M3UA 终端统计信息之前的空闲超时，该值的格式为 hh:mm:ss。若不设置超时，请指定 0。默认值为 30 分钟 (00:30:00)。
- **Enforce Timeout > Session** - 如果启用严格 ASP 状态验证，则表示删除 M3UA 会话之前的空闲超时，该值的格式为 hh:mm:ss。若不设置超时，请指定 0。默认值为 30 分钟 (00:30:00)。禁用此超时可防止系统删除过时的会话。
- **Message Tag Validation** - 是否检查和验证指定消息类型的某些字段的内容。验证失败的消息将被丢弃。验证因消息类型而异。选择要验证的消息。
 - 目标用户部分不可用 (DUPU) - User/Cause 字段必须存在，并且其中必须仅包含有效的原因和用户代码。
 - 错误 - 所有必填字段必须都存在，并且仅包含允许的值。每个错误消息都必须包含该错误代码的必填字段。
 - 通知 - 状态类型和状态信息字段必须仅包含允许的值。

步骤 5 点击 **Inspections** 选项卡，并定义要基于流量特性实施的特定检测。

a) 执行以下任一操作：

- 点击 **Add** 添加新条件。
- 选择现有条件并点击 **Edit**。

b) 选择条件的匹配类型：**Match**（流量必须与条件匹配）或者 **No Match**（流量不得与条件匹配）。然后，配置条件：

- **Class ID** - 匹配 M3UA 消息类和类型。下表列出了可能的值。有关这些消息的详细信息，请参阅 M3UA RFC 和文档。

M3UA 消息类	消息 ID 类型
0 (管理消息)	0-1
1 (传输消息)	1
2 (SS7 信令网络管理消息)	1-6
3 (ASP 状态维护消息)	1-6
4 (ASP 流量维护消息)	1-4
9 (路由密钥管理消息)	1-4

- **OPC** - 匹配始发点代码，即流量源。点代码为 *zone-region-sp* 格式，其中每个元素可能的值取决于 SS7 变量：
 - **ITU**- 点代码为 14 位，格式为 3-8-3。值范围为 [0-7]-[0-255]-[0-7]。
 - **ANSI**- 点代码为 24 位，格式为 8-8-8。值范围为 [0-255]-[0-255]-[0-255]。
 - **Japan**- 点代码为 16 位，格式为 5-4-7。值范围为 [0-31]-[0-15]-[0-127]。
 - **China**- 点代码为 24 位，格式为 8-8-8。值范围为 [0-255]-[0-255]-[0-255]。
- **DPC** - 匹配目标点代码。点代码为 *zone-region-sp* 格式，如同所述的 **OPC** 相关内容。
- **Service Indicator** - 匹配服务指示符编号 0-15。下面是可用的服务指示符。有关这些服务指示符的详细信息，请参阅 M3UA RFC 和文档。
 - 0 - 信令网络管理消息
 - 1 - 信令网络测试和维护消息
 - 2 - 信令网络测试和维护特殊消息
 - 3 - SCCP
 - 4 - 电话用户部分
 - 5 - ISDN 用户部分
 - 6 - 数据用户部分（呼叫和电路相关消息）
 - 7 - 数据用户部分（设备注册和取消消息）
 - 8 - 预留用于 MTP 测试用户部分
 - 9 - 宽带 ISDN 用户部分
 - 10 - 卫星 ISDN 用户设备

- 11 - 预留
 - 12 - AAL 第 2 类信令
 - 13 - 承载独立呼叫控制
 - 14 - 网关控制协议
 - 15 - 预留
- c) 对于类 ID 匹配，选择是丢弃数据包还是应用每秒数据包速率限制。对于所有其他匹配，操作是丢弃数据包。对于所有匹配，可以选择是否启用日志记录。
- d) 点击 **OK** 添加检测。根据需要重复上述步骤。

步骤 6 点击 M3UA Inspect Map 对话框中的 **OK**。

现在，您即可在 M3UA 检测服务策略中使用检测映射。

下一步做什么

现在，您可以配置一个检测策略来使用该映射。请参阅[配置移动网络检测服务策略](#)，第 404 页。

配置移动网络检测服务策略

移动网络使用的协议检测在默认检测策略中未启用，所以如果需要这些检测，必须启用它们。可以简单地编辑默认全局检测策略来添加这些检测。或者，可以创建所需的新服务策略，例如，接口特定策略。

过程

步骤 1 依次选择配置 > 防火墙 > 服务策略，并打开规则。

- 要编辑默认全局策略，请在 Global 文件夹中选择“inspection_default”规则，然后点击 **Edit**。
- 要创建新规则，请点击 **Add > Add Service Policy Rule**。继续运行向导，转到 Rules 页面。
- 如果有移动网络检测规则或有要添加这些检测的规则，请选择该规则并点击 **Edit**。

步骤 2 在 Rule Actions 向导页面或选项卡上，选择 **Protocol Inspection** 选项卡。

步骤 3 （要更改使用中的策略。）如果是编辑任何使用中的策略来使用不同的检测策略映射，必须禁用这些检测，然后再为它们提供新的检测策略映射名称并重新启用它们。

- a) 取消选中已选的相关复选框：**GTP、SCTP、Diameter、M3UA**。
- b) 点击 **OK**。
- c) 点击 **Apply**。
- d) 重复这些步骤以返回到 Protocol Inspections 选项卡。

步骤 4 选择所需的移动网络协议：**GTP、SCTP、Diameter、M3UA**。

步骤 5 如果要对其中一个或多个协议执行非默认检测，请点击选项旁边的 **Configure**，并执行以下操作：

a) 选择使用默认映射还是已配置的检测策略映射。可在此时创建映射。

b) （仅限 Diameter。）要对加密消息启用 Diameter 检测，请选择 **Enable Encrypted Traffic Inspection**，然后选择用于解密的 TLS 代理。

注释 如果为 Diameter 检测指定 TLS 代理并对 Diameter 服务器流量应用 NAT 端口重定向（例如，将服务器流量从端口 5868 重定向到 3868），请配置全局检测或仅在传出接口上配置检测。如果对传出接口应用检测，则通过 NAT 连接的 Diameter 流量将绕过检测。

c) 点击 Select Inspect Map 对话框中的 **OK**。

步骤 6 点击 **OK** 或 **Finish** 以保存服务策略规则。

配置 RADIUS 计费检测

默认情况下，RADIUS 计费检测未启用。如果需要 RADIUS 计费检测，必须对其进行配置。

过程

步骤 1 配置 RADIUS 计费检测策略映射，第 405 页。

步骤 2 配置 RADIUS 计费检测服务策略，第 406 页。

配置 RADIUS 计费检测策略映射

要配置 RADIUS 计费检测所需的属性，必须创建 RADIUS 计费检测策略映射。

过程

步骤 1 依次选择配置 > 防火墙 > 对象 > 检测映射 > RADIUS 计费。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新映射。
- 选择映射并点击 **Edit**。

步骤 3 对于新的映射，请输入名称（最多可包含 40 个字符）和说明。编辑映射时，只可以更改说明。

步骤 4 点击 **Host Parameters** 选项卡，并添加各个 RADIUS 服务器或 GGSN 的 IP 地址。

您可以选择添加密钥，以便 ASA 可验证消息。如果没有密钥，则只检查 IP 地址。ASA 收到来自这些主机的 RADIUS 计费消息副本。

步骤 5 点击 **Other Parameters** 选项卡并配置所需的选项。

- **Send responses to the originator of the RADIUS accounting message** - 是否遮蔽来自 ESMTMP 服务器的横幅。
- **Enforce user timeout** - 是否实施用户空闲超时和超时值。默认值为一小时。
- **Enable detection of GPRS accounting** - 是否实施 GPRS 过度计费防护。ASA 检查计费请求停止和断开消息中的 3GPP VSA 26-10415 属性，以便正确处理辅助 PDP 情景。如果存在此属性，ASA 将终止其源 IP 与已配置接口上的用户 IP 地址匹配的所有连接。
- **Validate Attribute** - 接收 Accounting-Request Start 消息时用于构建用户账户表的其他条件。在 ASA 决定是否终止连接时，这些属性可提供帮助。

如果没有指定要验证的其他属性，ASA 将会以 Framed IP Address 属性中的 IP 地址作为唯一依据作出决定。如果配置了其他属性，并且 ASA 收到的开始计费消息包含当前正在跟踪的地址，但要验证的其他属性不同，则在已将 IP 地址重新分配给新用户的情况下，使用旧属性启动的所有连接都将被终止。

值范围是 1 到 191，而且可以多次输入命令。有关属性编号及其描述的列表，请访问 <http://www.iana.org/assignments/radius-types>。

步骤 6 点击 **OK**。

这样即可将检测映射用于 RADIUS 计费检测服务策略中。

配置 RADIUS 计费检测服务策略

RADIUS 计费检测在默认检测策略中未启用，如果需要进行这项检测，必须先启用这项检测。由于 RADIUS 计费检测应用于定向到 ASA 的流量，所以必须将其配置为管理检测规则，而不是标准规则。

过程

步骤 1 依次选择配置 > 防火墙 > 服务策略，并打开规则。

- 要创建新规则，请依次点击 **Add > Add Management Service Policy Rule**。继续运行向导，转到 Rules 页面。
- 如果有 RADIUS 计费检测规则，或者有要添加 RADIUS 计费检测的管理规则，请选择该规则并点击 **Edit**，然后点击 **Rule Actions** 选项卡。

步骤 2（要更改使用中的策略）如果要编辑任何使用中的策略来使用不同的检测策略映射，必须禁用 RADIUS 计费检测，然后为其提供新的检测策略映射名称并重新启用这项检测：

- a) 为 RADIUS 计费映射选择 **None**。
- b) 点击 **OK**。
- c) 点击 **Apply**。

d) 重复这些步骤以返回到 Protocol Inspections 选项卡。

步骤 3 从 **RADIUS Accounting Map** 选择所需的 RADIUS 计费映射。可在此时创建映射。有关详细信息，请参阅配置 **RADIUS 计费检测策略映射**，第 405 页。

步骤 4 点击 **OK** 或 **Finish** 以保存管理服务策略规则。

监控移动网络检测

以下主题介绍如何监控移动网络检测。

监控 GTP 检测

要显示 GTP 配置，请在特权 EXEC 模式下输入 **show service-policy inspect gtp** 命令。依次选择工具 > 命令行界面，输入命令。

使用 **show service - policy inspect gtp statistics** 命令显示 GTP 检测的统计信息。以下是输出示例：

```
firewall(config)# 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_pdpmbc         31     total_deleted_pdpmbc   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
```

通过在 **show service-policy inspect gtp statistics ip_address** 命令中输入 IP 地址，可获取特定 GTP 终端的统计信息。

```
firewall(config)# show service-policy inspect gtp statistics 10.9.9.9
1 in use, 1 most used, timeout 0:30:00
GTP GSN Statistics for 10.9.9.9, Idle 0:00:34, restart counter 0
  Tunnels Active                0
  Tunnels Created                1
  Tunnels Destroyed              0
  Total Messages Received        1
                                Signalling Messages      Data Messages
  total received                 1                          0
  dropped                         0                          0
  forwarded                       1                          0
```

可使用 **show service-policy inspect gtp pdp-context** 命令显示 PDP 情景相关信息。对于 GTPv2，这是承载情景。例如：

```

ciscoasa(config)# 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

ciscoasa(config)# show service-policy inspect gtp pdp-context detail
1 in use, 1 most used

Version v1, TID 050542012151705f, MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22, Idle 0:06:14, Timeout 3:00:00, APN ssenoauth146

    user_name (IMSI): 50502410121507    MS address: 2005:a00::250:56ff:fe96:eec
    nsapi: 5                            linked nsapi: 5
    primary pdp: Y                       sgsn is Remote
    sgsn_addr_signal: 10.0.203.22       sgsn_addr_data: 10.0.203.22
    ggsn_addr_signal: 10.0.202.22       ggsn_addr_data: 10.0.202.22
    sgsn control teid: 0x00000001      sgsn data teid: 0x000003e8
    ggsn control teid: 0x000f4240      ggsn data teid: 0x001e8480
    signal_sequence: 18                 state: Ready
...

```

PDP 或承载情景通过隧道 ID (TID) (IMSI 与 NSAPI (GTPv0-1) 或 IMSI 与 EBI (GTPv2) 值的组合) 标识。GTP 隧道由不同 GSN 或 SGW/PGW 节点中的两个关联情景来定义，并通过隧道 ID 标识。在外部数据包数据网络与移动用户 (MS) 之间转发数据包需要使用 GTP 隧道。

监控 SCTP

您可以使用以下命令来监控 SCTP。依次选择工具 > 命令行界面，输入以下命令。

- **show service-policy inspect sctp**

显示 Sctp 检测统计信息。PPID 每匹配一次丢弃操作，sctp-drop-override 计数器便递增一次，但数据包不会因为包含具有不同 PPID 的数据分块而被丢弃。例如：

```

ciscoasa# show service-policy inspect sctp
Global policy:
  Service-policy: global_policy
  Class-map: inspection_default
    Inspect: sctp sctp, packet 153302, lock fail 0, drop 20665, reset-drop 0,
  5-min-pkt-rate 0 pkts/sec, v6-fail-close 0, sctp-drop-override 4910
    Match ppid 30 35
      rate-limit 1000 kbps, chunk 2354, dropped 10, bytes 21408, dropped-bytes 958

    Match: ppid 40
      drop, chunk 5849
    Match: ppid 55
      log, chunk 9546

```


- **show sctp [detail]**

显示当前的 SCTP cookie 和关联。添加 **detail** 关键字，可查看有关 SCTP 关联的详细信息。详细视图还会显示有关多宿主、多流和分段重组的信息。

```
ciscoasa# show sctp

AssocID: 71adeb15
Local: 192.168.107.12/50001 (ESTABLISHED)
Remote: 192.168.108.122/2905 (ESTABLISHED)
Secondary Conn List:
  192.168.108.12(192.168.108.12):2905 to 192.168.107.122(192.168.107.122):50001
  192.168.107.122(192.168.107.122):50001 to 192.168.108.12(192.168.108.12):2905
  192.168.108.122(192.168.108.122):2905 to 192.168.107.122(192.168.107.122):50001
  192.168.107.122(192.168.107.122):50001 to 192.168.108.122(192.168.108.122):2905
  192.168.108.12(192.168.108.12):2905 to 192.168.107.12(192.168.107.12):50001
  192.168.107.12(192.168.107.12):50001 to 192.168.108.12(192.168.108.12):2905
```

- **show conn protocol sctp**

显示有关当前 SCTP 连接的信息。

- **show local-host [connection sctp start[-end]]**

显示主机上有关使 SCTP 连接在每个接口上通过 ASA 的信息。添加 **connection sctp** 关键字，可仅查看具有指定 SCTP 连接数量或范围的主机。

- **show traffic**

如果启用 **sysopt traffic detailed-statistics** 命令，则显示每个接口的 SCTP 连接和检测统计信息。

监控 Diameter

您可以使用以下命令来监控 Diameter。依次选择工具 > 命令行界面，输入以下命令。

- **show service-policy inspect diameter**

显示 Diameter 检测统计信息。例如：

```
ciscoasa# show service-policy inspect diameter
Global policy:
  Service-policy: global_policy
  Class-map: inspection_default
  Inspect: Diameter Diameter_map, packet 0, lock fail 0, drop 0, -drop 0,
  5-min-pkt-rate 0 pkts/sec, v6-fail-close 0
  Class-map: log_app
  Log: 5849
  Class-map: block_ip
  drop-connection: 2
```

- **show diameter**

显示每个 Diameter 连接的状态信息。例如：

```
ciscoasa# 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
...
```

- **show conn detail**

显示连接信息。Diameter 连接均标有 Q 标志。

- **show tls-proxy**

如果在 Diameter 检测中使用了 TLS 代理，则此命令显示 TLS 代理的相关信息。

监控 M3UA

您可以使用以下命令来监控 M3UA。依次选择工具 > 命令行界面输入以下命令。

- **show service-policy inspect m3ua drops**

显示有关 M3UA 检测的丢弃统计信息。

- **show service-policy inspect m3ua endpoint [IP_address]**

显示 M3UA 终端的统计信息。您可以指定终端 IP 地址来查看特定终端的信息。对于高可用性或集群系统，统计信息是相对于每台设备的，不同设备之间的统计数据并不同步。例如：

```
ciscoasa# sh service-policy inspect m3ua endpoint
M3UA Endpoint Statistics for 10.0.0.100, Idle : 0:00:06 :
All Messages      Forwarded      Dropped      Total Received
DATA Messages     9              5             14
M3UA Endpoint Statistics for 10.0.0.110, Idle : 0:00:06 :
All Messages      Forwarded      Dropped      Total Received
DATA Messages     9              8             17
```

- **show service-policy inspect m3ua session**

如果启用了强应用服务器进程 (ASP) 状态验证，则显示有关 M3UA 会话的信息。这些信息包括源关联 ID、会话是单一交换还是双重交换，以及在集群中会话是集群所有者会话还是备份会话。在包含 3 台或更多设备的集群中，如果某台设备离开集群然后又返回集群，您可能会看到过时的备份会话。这些过时会话在超时后将被删除，除非您已禁用会话超时。

```
Ciscoasa# show service-policy inspect m3ua session
0 in use, 0 most used
Flags: o - cluster owner session, b - cluster backup session
       d - double exchange      , s - single exchange
AssocID: cfc59fbe in Down state, idle:0:00:05, timeout:0:01:00, bd
AssocID: dac2e123 in Active state, idle:0:00:18, timeout:0:01:00, os
```

- **show service-policy inspect m3ua table**

显示运行时 M3UA 检测表，包括分类规则。

- **show conn detail**

显示连接信息。M3UA 连接标有 v 标志。

移动网络检测的历史

功能名称	版本	功能信息
GTPv2 检测和 GTPv0/1 检测的改进。	9.5(1)	<p>GTP 检测现在可以处理 GTPv2。此外，所有版本的 GTP 检测现在均支持 IPv6 地址。</p> <p>我们更改了 GTP Inspect Map > Inspections 对话框，允许您为 GTPv1 和 GTPv2 配置独立的消息 ID 匹配。在 General 参数选项卡上，GSN 超时现在为 Endpoint 超时。</p>
SCTP 检测	9.5(2)	<p>现在，您可以对流控制传输协议 (SCTP) 流量应用应用层检测，以便基于负载协议标识符 (PPID) 应用操作。</p> <p>我们添加或更改了以下屏幕：配置 > 防火墙 > 对象 > 检测映射 > SCTP；配置 > 防火墙 > 服务策略 添加/编辑向导的规则操作 > 协议检测选项卡。</p>
Diameter 检测	9.5(2)	<p>现在，您可以对 Diameter 流量应用应用层检测，也可以基于应用 ID、命令代码和属性值对 (AVP) 过滤应用操作。</p> <p>我们添加或更改了以下屏幕：配置 > 防火墙 > 对象 > 检测映射 > Diameter 和 Diameter AVP；配置 > 防火墙 > 服务策略 添加/编辑向导的规则操作 > 协议检测选项卡。</p>
Diameter 检测的改进	9.6(1)	<p>现在，您可以在集群模式下检测通过 TCP/TLS 的 Diameter 流量、应用严格协议符合性检查及检测通过 SCTP 的 Diameter 流量。</p> <p>添加或更改了以下菜单项：配置 > 防火墙 > 对象 > 检测映射 > Diameter；配置 > 防火墙 > 服务策略 添加/编辑向导的规则操作 > 协议检测选项卡。</p>
集群模式下的 SCTP 状态检测	9.6(1)	<p>SCTP 状态检查现在可在集群模式下进行。还可以在集群模式下配置 SCTP 状态检查旁路。</p> <p>我们未修改任何菜单项。</p>

功能名称	版本	功能信息
MTP3 用户适应 (M3UA) 检测。	9.6(2)	<p>现在，您可以检测 M3UA 流量并基于点编码、服务指标及消息类和类型应用操作。</p> <p>添加或修改了以下页面：Configuration > Firewall > Objects > Inspection Maps > M3UA；用于服务策略规则的 Rule Action > Protocol Inspection 选项卡。</p>
支持 SCTP 多流重新排序、重组和分段。支持 SCTP 多宿主，其中 SCTP 终端具有一个以上的 IP 地址。	9.7(1)	<p>现在，系统完全支持 SCTP 多流重新排序、重组和分段，由此改善了 SCTP 流量的 Diameter 和 M3UA 检测效果。该系统还支持 SCTP 多宿主，其中每个 SCTP 终端都有一个以上的 IP 地址。对于多宿主，该系统可以打开辅助地址的针孔，使您无需编写访问规则即可允许它们访问。必须将每个 SCTP 终端限制为 3 个 IP 地址。</p> <p>未修改任何 ASDM 屏幕。</p>
M3UA 检测有所改进。	9.7(1)	<p>M3UA 检查现在支持状态化故障切换、半分布式集群和多宿主。另外，您还可以配置严格应用服务器进程 (ASP) 状态验证和各种消息验证。对于状态故障切换和集群，需要使用严格 ASP 状态验证。</p> <p>修改了以下菜单项：配置 > 防火墙 > 对象 > 检测映射 > M3UA “添加/编辑”对话框。</p>
支持设置 TLS 代理服务器 SSL 加密套件。	9.8(1)	<p>现在可在 ASA 作为 TLS 代理服务器时设置 SSL 密码套件。过去，您只能在 配置 > 设备管理 > 高级 > SSL 设置 > 加密 页面中为 ASA 设置全局设置。</p> <p>修改了以下菜单项：配置 > 防火墙 > 统一通信 > TLS 代理、“添加/编辑”对话框、服务器配置 页面。</p>
MSISDN 的 GTP 检测增强功能和选择模式过滤、防重放以及用户欺骗保护。	9.10(1)	<p>您现在可以配置 GTP 检测基于移动站点国际用户目录编号 (MSISDN) 或选择模式丢弃创建 PDP 情景消息。您还可以实施防重放和用户防欺骗。</p> <p>修改了 配置 > 防火墙 > 对象 > 检测映射 > GTP > 添加/编辑 对话框。</p>



第 **V** 部分

连接管理和威胁检测

- [连接设置](#)，第 415 页
- [服务质量](#)，第 435 页
- [威胁检测](#)，第 445 页



第 18 章

连接设置

本章介绍如何配置通过 ASA 的连接或传至 ASA 的管理连接的连接设置。

- [什么是连接设置？](#)，第 415 页
- [配置连接设置](#)，第 416 页
- [监控连接](#)，第 431 页
- [连接设置的历史](#)，第 432 页

什么是连接设置？

连接设置包含与管理流量连接相关的各种功能，例如通过 ASA 的 TCP 流量。某些功能以组件命名，可以配置这些组件，以提供特定服务。

连接设置包括以下内容：

- **Global timeouts for various protocols** - 所有全局超时均具有默认值，因此，只有在遇到过早失去连接的情况下，才需要更改超时值。
- **Connection timeouts per traffic class** - 可以使用服务策略覆盖特定流量类型的全局超时。所有流量类超时均具有默认值，因此，无需设置这些超时。
- **Connection limits and TCP Intercept** - 默认情况下，对于可以通过（或到达）ASA 的连接数量没有限制。可以使用服务策略规则来设置对特定流量类的限制，以保护服务器免受拒绝服务 (DoS) 攻击。具体而言，可以设置对初期连接（未完成 TCP 握手的连接）的限制，防止 SYN 泛洪攻击。当超过初期限制时，TCP 拦截组件会参与代理连接并确保攻击受到限制。
- **Dead Connection Detection (DCD)** - 如果具有有效但经常空闲的持久连接，以至于这些连接因为超出空闲超时设置而关闭，就可以启用失效连接检测，以识别空闲但有效的连接并且（通过重置其空闲计时器）使之保持活动状态。每当超出空闲时间，DCD 便会探测连接的两侧，了解两侧是否均同意连接是有效的。`show service-policy` 命令输出中包含计数器，以显示来自 DCD 的活动量。
- **TCP 序列随机化** - 每个 TCP 连接都有两个初始序列号 (ISN)：一个由客户端生成，一个由服务器生成。默认情况下，ASA 随机化入站和出站方向的 TCP SYN 的 ISN。随机化可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。可以根据需要按流量类禁用随机化。

- **TCP Normalization** - TCP 规范器可防止异常数据包。可以按流量类配置处理某些数据包异常类型的方式。
- **TCP State Bypass** - 如果在网络中使用非对称路由，可以绕过 TCP 状态检查。
- **SCTP State Bypass** - 如果不希望进行 SCTP 协议验证，可以绕过流控制传输协议 (SCTP) 状态检测。
- **数据流分流** - 可以标识将要分流至超快路径的选定流量，在此路径中，数据流在 NIC 自身进行交换。分流可帮助您提高数据密集型应用（例如大型文件传输）的性能。

配置连接设置

连接限制、超时、TCP 规范化、TCP 序列随机化和减少生存时间 (TTL) 均具有适用于大多数网络的默认值。仅当有特殊要求、网络有特定的配置类型或遇到因过早空闲超时而导致的异常失去连接时，才需要配置这些连接设置。

其他连接相关的功能处于未启用状态。仅可在特定流量类上配置这些服务，并且不能配置为通用服务。这些功能包括以下内容：TCP 拦截、TCP 状态绕行、失效连接检测 (DCD)、SCTP 状态绕行、流量卸载。

以下常规操作步骤介绍所有可能的连接设置配置。请根据自己的需要选择要实施哪些设置。

过程

- 步骤 1** [配置全局超时](#)，第 416 页。这些设置为通过设备的所有流量更改各种协议的默认空闲超时。如果您在因过早超时而重置连接时遇到问题，请先尝试更改全局超时。
- 步骤 2** [保护服务器不受 SYN 洪流 DoS 攻击 \(TCP 拦截\)](#)，第 419 页。请使用此操作步骤配置 TCP 拦截。
- 步骤 3** 如果要更改特定流量类的默认 TCP 规范化行为，请[自定义异常 TCP 数据包处理 \(TCP 映射、TCP 规范器\)](#)，第 420 页。
- 步骤 4** 如果有这种类型的路由环境，请[绕过面向异步路由的 TCP 状态检查 \(TCP 状态绕行\)](#)，第 423 页。
- 步骤 5** 如果默认随机化加扰某些连接的数据，请[禁用 TCP 序列随机化](#)，第 425 页。
- 步骤 6** [分流大型数据流](#)，第 426 页（如果需要提升计算密集型数据中心的性能）。
- 步骤 7** [配置特定流量类的连接设置 \(所有服务\)](#)，第 429 页。这是连接设置的全部操作步骤。这些设置可以使用服务策略规则覆盖特定流量类的全局默认值。此外，您也可以使用这些规则自定义 TCP 规范器、更改 TCP 序列随机化、减少数据包生存时间和实施其他可选功能。

配置全局超时

可以设置各种协议的连接和转换插槽的全局空闲超时持续时间。如果插槽在指定的空闲时间内未使用，资源将返回到空闲池。

更改全局超时会设置新的默认超时，在某些情况下，可以通过服务策略为特定流量覆盖默认超时。

过程

步骤 1 依次选择配置 > 防火墙 > 高级 > 全局超时。

步骤 2 选中要更改的超时的复选框，输入新的超时值，以此配置超时时间。

所有持续时间均以 *hh:mm:ss* 格式显示，大多数情况下，最大持续时间为 1193:0:0。在所有情况下，除 **Authentication absolute** 和 **Authentication inactivity** 外，取消选中此复选框均会将超时恢复为默认值。在这两种情况下，清除此复选框表示对每个新连接重新进行身份验证。

输入 0 将禁用超时。

- **连接** - 连接插槽释放前的空闲时间。此持续时间必须为至少 5 分钟。默认值为 1 小时。
- **半封闭** - TCP 半闭合连接关闭前的空闲时间。最小值为 30 秒。默认值为 10 分钟。
- **UDP** - UDP 连接关闭前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。
- **ICMP** - 通用 ICMP 状态关闭前的空闲时间。默认值（及最小值）是 2 秒。
- **ICMP Error** - ASA 在收到 ICMP 回应应答数据包后删除 ICMP 连接之前允许的空闲时间，该值介于 0:0:0 到 0:1:0 之间；或者为 ICMP 超时值，以较低者为准。默认为 0（禁用）。如果禁用此超时并启用 ICMP 检测，ASA 将在收到回应应答后立即删除 ICMP 连接；因此，针对该（现已关闭）连接生成的任何 ICMP 错误都将被丢弃。此超时可延迟删除 ICMP 连接，以便您可以接收重要的 ICMP 错误。
- **H.323** - TH.245 (TCP) 和 H.323 (UDP) 媒体连接关闭前的空闲时间。默认值（和最小值）为 5 分钟。由于 H.245 和 H.323 媒体连接上设置的连接标志相同，因此 H.245 (TCP) 连接与 H.323 (RTP 和 RTCP) 媒体连接共享空闲超时。
- **H.225** - H.225 信令连接关闭前的空闲时间。默认值为 1 小时。若要在清除所有调用后立即关闭连接，建议使用超时值 1 秒 (0:0:1)。
- **MGCP**—删除 MGCP 媒体连接前的空闲时间。默认值为 5 分钟，但您可以将其设置为低至 1 秒。
- **MGCP PAT**-MGCP PAT 转换删除前的空闲时间。默认值为 5 分钟。最短时间为 30 秒。
- **TCP 代理重组** - 等待重组的缓冲数据包丢弃前的空闲时间，该值介于 0:0:10 到 1193:0:0 之间。默认值为 1 分钟 (0:1:0)。
- **Floating Connection** - 当某个网络存在具有不同指标的多个路由时，ASA 会使用连接创建时指标最佳的路由。如果有更好的路由变得可用，则此超时可让连接关闭，以便使用更好的路由重新建立连接。默认值为 0（连接永不超时）。为了可以使用更好的路由，请将超时设置为 0:0:30 至 1193:0:0 之间的值。
- **SCTP** - 流控制传输协议 (SCTP) 连接关闭之前允许的空闲时间，该值介于 0:1:0 到 1193:0:0 之间。默认值为 2 分钟 (0:2:0)。
- **Stale Routes** - 从路由器信息库中删除过时路由之前允许保留的时间长度。这些路由供内部网关协议（例如 OSPF）使用。默认值为 70 秒 (00:01:10)，范围介于 00:00:10 到 00:01:40 之间。

- **SUNRPC**—SunRPC 插槽释放前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 10 分钟。
- **SIP** - SIP 信令端口连接关闭前的空闲时间。此持续时间必须为至少 5 分钟。默认值为 30 分钟。
- **SIP 媒体** - SIP 媒体端口连接关闭前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。SIP 媒体计时器用于具有 SIP UDP 媒体数据包的 SIP RTP/RTCP，而不是 UDP 非活动超时。
- **SIP 临时媒体** - SIP 临时媒体连接的超时值，该值介于 1 至 30 分钟之间。默认值为 2 分钟。
- **SIP 邀请** - PROVISIONAL 响应和媒体转换的针孔关闭前的空闲时间，该值介于 0:1:0 至 00:30:0 之间。默认值为 3 分钟 (0:3:0)。
- **SIP 断开连接** - 在 CANCEL 或 BYE 消息未收到 200 OK 的情况下，SIP 会话删除之前的空闲时间，该值介于 0:0:1 至 00:10:0 之间。默认值为 2 分钟 (0:2:0)。
- **身份验证绝对值**-身份验证缓存超时且用户必须对新连接重新进行身份验证前的持续时间。此计时器仅用于直接转发代理，即 AAA 规则。此持续时间必须短于转换插槽超时。系统保持等待，直到用户开始新连接后，再次提示用户重新验证。在禁用缓存而对每个新连接强制执行身份验证前，请注意以下限制事项。
 - 如果在连接上使用被动 FTP，请勿将此值设置为 0。
 - 如果 Authentication Absolute 为 0，HTTPS 身份验证可能无法工作。如果浏览器在 HTTPS 身份验证之后发起多个 TCP 连接加载网页，第一个连接会被允许通过，但是后续连接会触发身份验证。因此，即使在身份验证成功后，系统也会不断地向用户显示身份验证页面。要解决该问题，请将身份验证绝对超时设置为 1 秒。此解决方法会打开 1 秒钟的窗口，可以允许未经身份验证的用户通过防火墙（如果这些用户来自相同源 IP 地址的话）。
- **身份验证非活动状态**-身份验证缓存超时且用户必须对新连接重新进行身份验证前的持续时间。此持续时间必须短于 Translation Slot 值。此超时默认处于禁用状态。此计时器仅用于直接转发代理，即 AAA 规则。
- **转换插槽** - NAT 转换插槽释放前的空闲时间。此持续时间必须为至少 1 分钟。默认值为 3 小时。
- **PAT 转换插槽**（8.4(3) 及更高版本，不包括 8.5(1) 和 8.6(1)）- PAT 转换插槽释放前的空闲时间，该值介于 0:0:30 至 0:5:0 之间。默认值为 30 秒。如果上游路由器拒绝使用释放的 PAT 端口的新连接，您可能会想要增加超时，因为以前的连接在上游设备中可能仍处于开放状态。
- **Connection Holddown** - 系统应在该连接使用的路由不再存在或处于非活动状态时维持连接的时间长度。如果在此等待期间内路由未处于活动状态，系统将释放该连接。配置连接等待计时器的目的是为了降低路由摆动的影响，其中路由可能会快速显示和断开。您可以减小等待计时器，以便更快地进行路由融合。默认值为 15 秒，范围介于 00:00:00 到 00:00:15 秒之间。

步骤 3 点击 **Apply**。

保护服务器不受 SYN 洪流 DoS 攻击 (TCP 拦截)

当攻击者将一系列 SYN 数据包发送到主机时，即表示发生 SYN 泛洪拒绝服务 (DoS) 攻击。这些数据包通常来自虚假 IP 地址。SYN 数据包的持续泛洪将使服务器 SYN 队列始终处于充满状态，而无法处理来自合法用户的连接请求。

可以限制初期连接的数量，这样有助于防止 SYN 泛洪攻击。半开连接是源与目标之间尚未完成必要握手的连接请求。

当超过连接的初期连接阈值时，ASA 将充当服务器代理，使用 SYN cookie 方法向客户端 SYN 请求生成 SYN-ACK 响应（有关 SYN cookie 的详细信息，请参阅维基百科）。如果 ASA 收到来自该客户端的 ACK 应答，则可以验证该客户端真实并允许连接到服务器。执行代理的组件称为 TCP 拦截。

保护服务器免受 SYN 泛洪攻击的端到端流程包括设置连接限制，启用 TCP 拦截统计信息，然后监控结果。

开始之前

- 请确保设置的初期连接限制低于要保护的服务器上的 TCP SYN 积压工作队列。否则，在 SYN 攻击期间，有效客户端将无法访问服务器。为了确定初期限制的合理值，请仔细分析服务器容量、网络和服务器的使用情况。
- 根据 ASA 型号中的 CPU 核心数，由于每个核心管理连接的方式不同，最大并发和初始连接数可超出配置的数量。在最坏的情形下，ASA 允许最多 $n-1$ 个额外连接和初始连接，其中 n 为核心数。例如，如果设备型号有 4 个核心，而配置了 6 个并发连接和 4 个初期连接，那么每个类型可能有 3 个额外连接。要确定型号的核心数量，请输入 `show cpu core` 命令。

过程

步骤 1 依次选择配置 > 防火墙 > 服务策略。

步骤 2 依次点击添加 > 添加服务策略规则。

或者，如果已为要保护的服务器设置了规则，请编辑规则。

步骤 3 选择是向特定接口应用此策略还是向所有接口全局应用此策略，然后点击 **Next**。

步骤 4 对于 Traffic Classification，请选择 **Source and Destination IP Addresses (uses ACL)**，然后点击 **Next**。

步骤 5 对于 ACL 规则，请在 **Destination** 中输入服务器的 IP 地址，然后为服务器指定协议。通常，会将 **any** 用于 **Source**。完成后，点击 **Next**。

例如，如果要保护 Web 服务器 10.1.1.5 和 10.1.1.6，请输入：

- Source = any
- Destination = 10.1.1.5, 10.1.1.6
- Destination Protocol = tcp/http

步骤 6 在 Rule Actions 页面上，点击 **Connection Settings** 选项卡并填写以下选项：

- **初期连接数** - 每个主机的最大初期 TCP 连接数，最大为 2000000。默认值为 **0**，表示允许的最大初期连接数。例如，可以将该值设置为 1000。
- **每个客户端的初期连接数** - 每个客户端的最大同步初期 TCP 连接数，最大为 2000000。如果客户端在已通过 ASA 打开每客户端最大初期连接数后请求新的连接，ASA 将阻止该连接。例如，可以将该值设置为 50。

步骤 7 点击 **Finish** 保存规则，然后点击 **Apply** 更新设备。

步骤 8 依次选择配置 > 防火墙 > 威胁检测，并至少在“威胁检测统计信息”组下启用 **TCP 拦截**。

可以启用所有统计数据，或者仅启用 TCP 拦截。也可以调整监控窗口和速率。

步骤 9 依次选择主页 > 防火墙控制面板，查看 SYN 攻击下前十大受保护的服务器控制面板以监控结果。

点击**详细信息**按钮以显示历史抽样数据。在该速率间隔内，ASA 会对攻击数量抽样 30 次，所以对于默认的 30 分钟期间，统计信息每 60 秒收集一次。

可以使用 **Tools > Command Line Interface**，输入 **clear threat-detection statistics tcp-intercept** 命令，以清除统计信息。

自定义异常 TCP 数据包处理 (TCP 映射、TCP 规范器)

TCP 规范器标识被检测到时可由 ASA 处理的异常数据包；例如，ASA 可允许、丢弃或删除这些数据包。TCP 规范化有助于防止 ASA 遭受攻击。TCP 规范化始终启用，但是，可以自定义某些功能的行为方式。

要自定义 TCP 规范器，请首先使用 TCP 映射定义设置。然后，可以使用服务策略将映射应用到所选的流量类。

过程

步骤 1 依次选择 **Configuration > Firewall > Objects > TCP Maps**。

步骤 2 执行以下操作之一：

- 点击 **Add** 添加新的 TCP 映射。输入映射名称。
- 选择映射并点击 **Edit**。

步骤 3 在 **Queue Limit** 字段中，输入 TCP 连接可缓冲并可按顺序排列的最大无序数据包数量，该值介于 0 到 250 个数据包之间。

默认值为 0，表示禁用此设置，而且使用的默认系统队列限制取决于流量类型：

- 对于用于应用检查、IPS 和 TCP 检查重传的连接，队列限制为 3 个数据包。如果 ASA 收到具有不同窗口大小的 TCP 数据包，则队列限制会动态变化以符合传送的设置。
- 对于其他 TCP 连接，无序数据包会按原样通过。

如果将 Queue Limit 设置为 1 或以上，则允许用于所有 TCP 流量的无序数据包的数量与此设置匹配。例如，对于应用检查、IPS 和 TCP 检查重发流量，来自 TCP 数据包的所有通告设置将被忽略，以支持 Queue Limit 设置。对于其他 TCP 流量，现在会缓冲无序数据包并将其按顺序排列，而不是按原样通过。

步骤 4 在 **Timeout** 字段中，设置无序数据包可以保留在缓冲区的最长时间，该值介于 1 到 20 秒之间。

如果这些数据包在超时期间未按顺序排列并通过，则会被丢弃。默认值为 4 秒。如果 Queue Limit 设置为 0，则不能更改任何流量的超时；需要将该限制设置为 1 或更大的值，超时才会生效。

步骤 5 对于 **Reserved Bits**，请选择如何处理 TCP 报头中包含预留位的数据包：**Clear and allow**（删除这些位后允许数据包）、**Allow only**（不更改这些位，默认设置）或 **Drop** 数据包。

步骤 6 选择下列任一选项：

- **Clear urgent flag** - 清除数据包中的 URG 标记，然后允许数据包。URG 标志用于指示数据包包含优先级高于流内其他数据的信息。TCP RFC 对 URG 标记的确切解释比较模糊，因此终端系统以不同的方式处理紧急偏移，这可能使终端系统容易受到攻击。
- **Drop connection on window variation** - 丢弃窗口大小意外变化的连接。窗口大小机制允许 TCP 通告一个大窗口，随后通告一个不接受过多数据的较小窗口。根据 TCP 规范，强烈反对“缩小窗口”。
- **Drop packets that exceed maximum segment size** - 丢弃超出对等体设置的 MSS 的数据包。
- **Check if transmitted data is the same as original** - 启用重新传输数据检查，防止 TCP 重新传输出现不一致。
- **Drop packets which have past-window sequence** - 丢弃具有超出窗口序列号的数据包，即收到的 TCP 数据包的序列号超出 TCP 接收窗口的右边。要允许这些数据包，请取消选择此选项并将 **Queue Limit** 设置为 0（禁用队列限制）。
- **Drop SYN Packets with data** - 丢弃包含数据的 SYN 数据包。
- **Enable TTL Evasion Protection** - 为连接设置最大 TTL 数，由初始数据包中的 TTL 确定。后续数据包的 TTL 可以减少，但不能增加。系统会将 TTL 重置为该连接之前看到过的最低 TTL。这样有助于防御 TTL 回避攻击。

例如，攻击者可能发送一个使用极短 TTL 通过策略的数据包。当 TTL 变为零时，ASA 与终端之间的路由器将丢弃该数据包。攻击者可能在此时发送包含长 TTL 的恶意数据包，在 ASA 看来则像是重新传输数据包并进行传送。但到达终端主机时，它是攻击者收到的第一个数据包。在这种情况下，攻击者可以成功绕过防范攻击的安全措施。
- **Verify TCP Checksum** - 验证 TCP 校验和，丢弃验证失败的数据包。
- **Drop SYNACK Packets with data** - 丢弃含有数据的 TCP SYNACK 数据包。
- **Drop packets with invalid ACK** - 丢弃具有无效 ACK 的数据包。可能会在以下实例中看到无效 ACK：
 - 在 TCP 连接 SYN-ACK 已接收状态下，如果已接收的 TCP 数据包的 ACK 号与正在发送的下一个 TCP 数据包的序列号不完全相同，则是无效 ACK。

- 如果已收到 TCP 数据包的 ACK 号大于发送的下一个 TCP 数据包的序列号，则为无效 ACK。

注释 对于 WAAS 连接，系统自动允许包含无效 ACK 的 TCP 数据包。

步骤 7 (可选。) 点击 **TCP 选项** 选项卡，并为包含 TCP 选项的数据包设置操作。

可以先清除选项再允许数据包；如果包含一个特定类型的选项，则允许数据包；或即便包含多个特定类型的选项，也允许数据包。默认为允许五个已命名的选项，只要每个数据包中出现的特定选项不超过一次即可（否则该数据包将被丢弃），同时清除所有其他选项。您还可以选择丢弃包含 MD5 或任何已编号选项的数据包。请注意，如果 TCP 连接已检测，则不论您的配置如何，都会清除除 MSS 和选择性确认 (SACK) 选项以外的所有选项。

- a) 选择用于 **Selective Acknowledgement**、**TCP Timestamp** 和 **Window Scale** 选项的操作。

清除时间戳选项将禁用 PAWS 和 RTT。

- b) 选择用于 **MSS** (最大分段大小) 选项的操作。

除正常允许、允许多个和清除操作之外，还可以选择指定最大值并输入最大分段大小，范围为 68-65535。默认 TCP MSS 在 **Configuration > Firewall > Advanced > TCP Options** 页面定义。

- c) 选择是否要允许具有 **MD5** 选项的数据包。

如果取消选择该复选框，包含 MD5 选项的数据包将被丢弃。如果选择该选项，可以应用正常的操作：允许、允许多个或清除。

- d) 按编号范围选择用于选项的操作。

默认清除编号为 6-7、9-18 和 20-255 的选项。可以改为允许这些选项或丢弃包含选项的数据包。可以为不同的选项范围指定不同的操作：只需输入范围的下限和上限编号，选择操作，然后点击 **Add**。要为单一选项配置操作，请对范围下限和上限输入相同的编号。

要删除已配置的范围，请选择该范围并点击删除。

步骤 8 依次点击 **OK** 和 **Apply**。

这样即可在服务策略中使用 TCP 映射。该映射仅在通过服务策略应用时影响流量。

步骤 9 使用服务策略将 TCP 映射应用到流量类。

- a) 依次选择 **Configuration > Firewall > Service Policy Rules**。
- b) 添加或编辑规则。可以全局应用规则，或者将规则应用到接口。例如，要自定义面向所有流量的异常数据包处理，请创建匹配所有流量的全局规则。继续操作，进入 **Rule Actions** 页面。
- c) 点击 **Connection Settings** 选项卡。
- d) 选择 **Use TCP Map**，然后选择创建的映射。
- e) 点击 **Finish** 或 **OK**，然后点击 **Apply**。

绕过面向异步路由的 TCP 状态检查 (TCP 状态绕行)

如果网络中有异步路由环境，其中，给定连接的出站和入站流量可以通过两个不同的 ASA 设备，则需要受影响的流量上实施 TCP 状态绕行。

但是，TCP 状态绕行会削弱网络安全性，因此应在非常具体的有限流量类上应用绕行。

以下主题详细介绍该问题和解决方案。

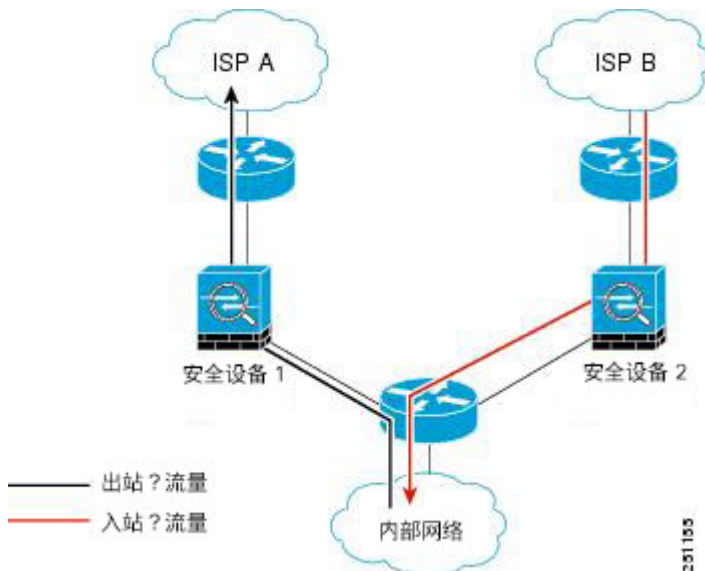
异步路由问题

默认情况下，所有经过 ASA 的流量都会使用自适应安全算法检查，并根据安全策略允许通过或予以丢弃。ASA 通过检查每个数据包的状态（新连接还是现有连接）并将其分配到会话管理路径（新连接 SYN 数据包）、快速路径（现有连接）或控制平面路径（高级检测），最大程度地提高防火墙性能。

匹配快速路径中现有连接的 TCP 数据包，不重新检查安全策略的每个方面即可通过 ASA。此功能可最大程度地提高性能。但是，使用 SYN 数据包在快速路径中建立会话的方法，以及在快速路径中进行的检查（例如 TCP 序列号），可能会阻碍非对称路由解决方案：出站和入站连接流必须通过同一 ASA。

例如，有一个新连接传入安全设备 1。SYN 数据包通过会话管理路径，而且连接的条目添加到快速路径表中。如果此连接的后续数据包通过安全设备 1，则这些数据包与快速路径中的该条目匹配，可以通过。但是，如果后续数据包传入安全设备 2，其中没有经过会话管理路径的 SYN 数据包，则快速路径中没有该连接的条目，数据包将被丢弃。下图显示一个不对称路由示例，其中，出站流量通过一个与入站流量不同的 ASA：

图 50: 非对称路由



如果在上游路由器中配置了不对称路由，且流量在两个 ASA 之间交替，则可以为特定流量配置 TCP 状态绕行。TCP 状态绕行将改变会话在快速路径中建立的方式，并且禁用快速路径检查。此功能按处理 UDP 连接的大致方式来处理 TCP 流量：当匹配指定网络的非 SYN 数据包进入 ASA 时，其中

没有快速路径条目，该数据包将通过会话管理路径在快速路径中建立该连接。流量到达快速路径后，将绕过快速路径检查。

有关 TCP 状态绕行的准则和限制

TCP 状态绕行不支持的功能

使用 TCP 状态绕行时不支持以下功能：

- 应用检测 - 检测要求入站和出站流量通过同一 ASA，因此不会对 TCP 状态绕行流量应用检测。
- 通过 AAA 身份验证的会话 - 如果用户通过一个 ASA 的身份验证，那么通过另一个 ASA 返回的流量将被拒绝，因为该用户未通过该 ASA 的身份验证。
- TCP 拦截、最大初期连接限制、TCP 序列号随机化 - ASA 不跟踪连接的状态，因此不会应用这些功能。
- TCP 标准化 - 禁用 TCP 规范器。
- 服务模块功能 - 无法使用 TCP 状态绕行及任何类型服务模块（例如 ASA FirePOWER）上运行的所有应用。
- 状态故障切换。

TCP 状态绕行 NAT 指南

由于转换会话是为每个 ASA 单独建立，请务必在两个设备上均为 TCP 状态绕行流量配置静态 NAT。如果使用动态 NAT，则在设备 1 上为会话选择的地址将与在设备 2 上为会话选择的地址不同。

配置 TCP 状态绕行

要在异步路由环境中绕过 TCP 状态检查，请仔细定义适用于受影响主机或仅适用于网络的流量类，然后使用服务策略在流量类上启用 TCP 状态绕行。由于绕行会降低网络安全性，请尽可能限制网络应用。

开始之前

如果指定的连接上在 2 分钟内没有流量，则连接超时。您可以通过更改 TCP 状态绕行流量类的空闲连接超时来覆盖此默认值。一般的 TCP 连接超时默认为 60 分钟后。

过程

步骤 1 依次选择配置 > 防火墙 > 服务策略。

步骤 2 依次点击添加 > 添加服务策略规则。

或者，如果已为主机设置了规则，请编辑规则。

步骤 3 选择是向特定接口应用此策略还是向所有接口全局应用此策略，然后点击 Next。

步骤 4 对于 Traffic Classification，请选择 **Source and Destination IP Addresses (uses ACL)**，然后点击 Next。

步骤 5 对于 ACL 规则，请在 **Source** 和 **Destination** 中输入路由两端主机的 IP 地址，并指定使用 TCP 协议。完成后，点击 **Next**。

例如，如果要绕过 10.1.1.1 与 10.2.2.2 之间的 TCP 状态检查，请输入：

- Source = 10.1.1.1
- Destination = 10.2.2.2
- Destination Protocol = tcp

步骤 6 在 Rule Actions 页面上，点击 **Connection Settings** 选项卡并选择 **TCP State Bypass**。

步骤 7 点击 **Finish** 保存规则，然后点击 **Apply** 更新设备。

禁用 TCP 序列随机化

每个 TCP 连接都有两个 ISN：一个由客户端生成，一个由服务器生成。ASA 会将入站和出站方向传送的 TCP SYN 的 ISN 随机化。

随机化受保护主机的 ISN 可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。

可以根据需要禁用 TCP 初始序列号随机化，例如，由于数据混乱。例如：

- 如果另一个在线防火墙也随机化初始序列号，则即使此操作不影响流量，两个防火墙也无需执行此操作。
- 如果通过 ASA 使用 eBGP 多跳，则 eBGP 对等体使用 MD5。随机化会中断 MD5 校验和。
- 使用要求 ASA 不对连接的序列号随机化的 WAAS 设备。
- 如果为 ISA 3000 启用硬件绕行，当 ISA 3000 不再是数据路径时的一部分时，TCP 连接将被丢弃。

过程

步骤 1 依次选择配置 > 防火墙 > 服务策略。

步骤 2 依次点击添加 > 添加服务策略规则。

或者，如果已为目标流量设置了规则，请编辑规则。

步骤 3 选择是向特定接口应用此策略还是向所有接口全局应用此策略，然后点击 **Next**。

步骤 4 对于 Traffic Classification，请确定流量匹配类型。类匹配应适用于 TCP 流量；可以确定让特定主机（带有 ACL）执行 TCP 端口匹配，或匹配所有流量。点击 **Next** 并在 ACL 中配置主机或定义端口，然后再次点击 **Next**。

例如，如果要为进入 10.2.2.2 的所有 TCP 流量禁用 TCP 序列号随机化，请输入：

- Source = any

- Destination = 10.2.2.2
- Destination Protocol = tcp

步骤 5 在 Rule Actions 页面上，点击 **Connection Settings** 选项卡并取消选中 **Randomize Sequence**。

步骤 6 点击 **Finish** 保存规则，然后点击 **Apply** 更新设备。

分流大型数据流

如果将 ASA 部署在数据中心的 Firepower 4100/9300 机箱（FXOS 1.1.3 或更高版本）上，则可以识别要分流到超快路径的特定流量，其中流量在 NIC 中进行交换。分流可帮助您提高数据密集型应用（例如大型文件传输）的性能。

- 高性能计算 (HPC) 研究站点，其中 ASA 部署在存储设施与高性能计算站之间。当一个研究站使用 NFS 上的 FTP 文件传输或文件同步备份时，庞大的数据流量会影响 ASA 上的所有情景。对 NFS 上的 FTP 文件传输或文件同步分流可降低对其他流量的影响。
- 高频交易 (HFT)，其中 ASA 部署在工作站与交易所之间，主要是出于合规目的。通常无需担心安全问题，但延迟是一个重大问题。

在分流之前，ASA 首先应用建立连接期间的正常安全处理，例如访问规则和检测。此外，ASA 还会终止会话。但建立连接后，如果流量符合分流的条件，则会在 NIC（而不是 ASA）中执行进一步的处理。

已分流的数据流会继续接受具有限制性的状态检测，例如基本 TCP 标记和选项检查以及校验和验证（如果已配置）。如有必要，系统可以有选择地将数据包上报至防火墙系统以进行进一步处理。

为了识别可分流的数据流，可以创建一项应用数据流分流服务的策略规则。如果数据流满足以下条件，则可进行分流：

- 仅有 IPv4 地址。
- 仅有 TCP、UDP 和 GRE。
- 仅有标准或 802.1Q 标记的以太网帧。
- （仅有透明模式。）包含两个且仅包含两个接口的桥接组的组播数据流。

已分流数据流的逆向数据流也会被分流。

数据流分流限制

并非所有数据流都可分流。即使在分流后，在某些情况下可取消对数据流的分流。以下是一些限制条件：

无法分流的数据流

以下数据流类型无法分流。

- 使用 IPv6 寻址的数据流。

- 除 TCP、UDP 和 GRE 之外的任意协议的数据流。



注释 无法分流 PPTP GRE 连接。

- 需要由检查的数据流。在某些情况下（例如 FTP），虽然无法分流控制通道，但可以分流次要数据通道。
- 通过另一个模块（例如 ASA Firepower）的数据流。
- IPsec 和 VPN 连接。
- 生存时间 (TTL) 值递减的数据流。
- 需要加密或解密的数据流。
- 路由模式下的组播数据流。
- 具备三个或更多接口的网桥组在透明模式下的组播数据流。
- TCP 拦截数据流。
- AAA 相关数据流。
- Vpath、VXLAN 相关数据流。
- URL 过滤。
- 跟踪器数据流。
- 使用安全组标记的数据流。
- 从不同集群节点转发来的逆向数据流（在集群中数据流不对称的情况下）。
- 集群中的集中数据流（如果数据流的所有者不是主设备）。

逆向分流的条件

对数据流分流后，如果数据流中的数据包符合以下条件，则将被返回到 ASA 接受进一步处理：

- 数据包包含时间戳以外的 TCP 选项。
- 数据包经过分段。
- 它们会进行等价多路径 (ECMP) 路由，并且入口数据包会从一个接口移至另一个接口。

配置数据流分流

要配置数据流分流，必须首先启用该服务，再创建服务策略来识别符合分流条件的流量。启用或禁用该服务需要重新启动。但添加或编辑服务策略不需要重新启动。

数据流分流只能用于 Firepower 4100/9300 机箱（FXOS 1.1.3 或更高版本）上的 ASA。



注释 有关设备支持的详细信息，请参阅
<http://www.cisco.com/c/en/us/td/docs/security/firepower/9300/compatibility/fxos-compatibility.html>。

过程

步骤 1 启用数据流分流服务。

无论何时启用或禁用此服务，都必须重新加载系统。

在多情景模式下，启用或禁用数据流分流将致使在所有情景下都启用或禁用它。每个情景无法进行不同设置。

如果需要无中断地更改，请特别考虑更改集群或故障切换对的模式：

- 集群 - 首先在主设备上启用该服务，但不立即重新启动主设备。相反，首先重新启动该集群的每个成员，再返回主设备并对其重新启动。然后，即可在主设备上配置分流服务策略。
- 故障切换 - 首先在主用设备上启用该服务，但不立即重新启动。相反，首先重新启动备用设备，再重新启动主用设备。然后，即可在主用设备上配置分流服务策略。

- a) 依次选择 **Configuration > Firewall > Advanced > Offload Engine**。
- b) 选择 **Enable Offload Engine**。
- c) 点击 **Apply**。
- d) 点击 **Save**，以便将更改保存到启动配置。
- e) 依次选择 **Tools > System Reload**，以重新启动该设备。

步骤 2 创建用于识别符合分流条件的流量的服务策略规则。

- a) 依次选择 **配置 > 防火墙 > 服务策略**。
- b) 依次点击 **添加 > 添加服务策略规则**。
或者，如果已为主机设置了规则，请编辑规则。
- c) 选择是向特定接口应用此策略还是向所有接口全局应用此策略，然后点击 **Next**。
- d) 对于 **Traffic Classification**，最常用的选项是按访问列表 (**Source and Destination IP Addresses (uses ACL)**) 或端口 (**TCP or UDP or SCTP Destination Port**) 匹配。选择一个映射，然后点击 **Next**。
- e) 输入 **ACL 或端口标准**。完成后，点击 **Next**。

例如，如果要使 10.1.1.0/255.255.255.224 子网上的所有 TCP 流量符合分流条件，请输入：

- Source = 10.1.1.0/255.255.255.224 (或 10.1.1.0/27)
- Destination = any
- Destination Protocol = tcp

- f) 在 **Rule Actions** 页面上，点击 **Connection Settings** 选项卡并选择 **Flow Offload**。

g) 点击 **Finish** 保存规则，然后点击 **Apply** 更新设备。

配置特定流量类的连接设置（所有服务）

可以使用服务策略配置特定流量类的不同连接设置。使用服务策略进行以下操作：

- 自定义用于防御 DoS 和 SYN 泛洪攻击的连接限制和超时。
- 实施失效连接检测，以便让有效但空闲的连接保持活动状态。
- 在不需要 TCP 序列号随机化的情况下将其禁用。
- 自定义 TCP 规范器如何防止异常 TCP 数据包。
- 为受异步路由限制的流量实施 TCP 状态绕行。绕行流量不受检查限制。
- 实施流控制传输协议 (SCTP) 状态绕行，以便关闭 SCTP 状态检测。
- 实施流量卸载，以提高受支持的硬件平台上的性能。
- 减少数据包的生存时间 (TTL)，以便 ASA 显示在跟踪路由输出中。



注释 如果减少生存时间，系统会丢弃 TTL 为 1 的数据包，但会为会话打开一个连接，前提是假设该连接可能包含具有更大 TTL 的数据包。请注意，某些数据包（例如 OSPF hello 数据包）发送时 TTL = 1，因此减去生存时间可能会导致意外后果。

可以为给定流量类配置这些设置的任意组合，但 TCP 状态绕行与 TCP 规范器自定义除外，因为这两者互相排斥。



提示 此过程显示用于通过 ASA 的流量的服务策略。还可以为管理（通过设备）流量配置最大连接数量和最大初期连接数量。

开始之前

如果要自定义 TCP 规范器，请先创建所需的 TCP 映射，再继续操作。

过程

步骤 1 依次选择 **配置 > 防火墙 > 服务策略**，并打开规则。

- 要创建新规则，请依次点击 **Add > Add Service Policy Rule**。继续运行向导，转到 **Rules** 页面。
- 如果有要更改连接设置的规则，请选择该规则，然后点击 **Edit**。

步骤 2 在 Rule Actions 向导页面或选项卡上，选择 **Connection Settings** 选项卡。

步骤 3 要设置最大连接数，请在 Maximum Connections 区域配置以下值：

- **Maximum TCP, UDP and SCTP Connections** - (TCP、UDP、SCTP。)流量类中所有客户端的最大同时连接数，最大为 2000000。默认值为 0，表示允许的最大可能连接数。对于 TCP 连接，这仅适用于现有连接。
- **Embryonic Connections** - 指定每个主机的最大初期 TCP 连接数，最大为 2000000。半开连接是源与目标之间尚未完成必要握手的连接请求。默认值为 0，表示允许的最大初期连接数。通过设置非零限制启用 TCP 拦截，从而防止内部系统受到 DoS 攻击（这种攻击使用 TCP SYN 数据包对接口发起泛洪攻击）。另外，请设置每客户端选项，以防止 SYN 泛洪。
- **Per Client Connections** - (TCP、UDP、SCTP。)指定每个客户端的最大同时连接数，最大为 2000000。如果客户端在已打开每客户端最大连接数后尝试新的连接，ASA 将拒绝该连接并丢弃数据包。对于 TCP 连接，这包括现有、半开和半闭连接。
- **Per Client Embryonic Connections** - 指定每个客户端的最大同步 TCP 初期连接数，最大为 2000000。如果客户端在已通过 ASA 打开每客户端最大初期连接数后请求新的连接，ASA 将阻止该连接。

步骤 4 要配置连接超时，请在 TCP Timeout 区域配置以下值：

- **Embryonic Connection Timeout** - 释放初期（半开）TCP 连接插槽之前的空闲时间。输入 0:0:0，以便禁用连接超时。默认值为 30 秒。
- **Half Closed Connection Timeout** - 半闭连接关闭之前经过的空闲超时时间，该值介于 0:5:0（适用于 9.1(1) 及更低版本）或 0:0:30（适用于 9.1(2) 及更高版本）到 1193:0:0 之间。默认值为 0:10:0。半闭连接不受 DCD 影响。另外，当半闭连接断开时，ASA 不会发送重置。
- **Idle Connection Timeout** - 释放连接插槽（任何协议，不只是 TCP）之前的空闲时间。输入 0:0:0，以便禁用连接超时。此持续时间必须为至少 5 分钟。默认值为 1 小时。
- **Send reset to TCP endpoints before timeout** - ASA 在释放连接插槽前释放应向连接终端发送 TCP 重置消息。
- **Dead Connection Detection (DCD)** - 是否启用失效连接检测 (DCD)。在空闲连接过期前，ASA 会探测终端主机来确定连接是否有效。如果两台主机均响应，系统会保留连接，否则会释放连接。设置重试次数（默认值为 5，范围为 1-255）和重试间隔，这是每个 DCD 探测器无响应之后发送另一个探测器之前的等待时间（介于 0:0:1 到 24:0:0 之间，默认值为 0:0:15）。在透明防火墙模式下运行，必须为终端配置静态路由。无法在集群中使用 DCD。

步骤 5 要禁用随机化序列号，请取消选中 **Randomize Sequence Number**。

随机化受保护主机的 ISN 可防止攻击者预测新连接的下一个 ISN 而潜在劫持新会话。

步骤 6 要自定义 TCP 规范器行为，请选中 **Use TCP Map**，然后从下拉列表（若有）选择一个现有 TCP 映射，或通过点击 **New** 添加一个新的 TCP 映射。

步骤 7 要减少与类匹配的数据包的生存时间 (TTL)，请选中 **Decrement time to live for a connection**。

要在跟踪路由中作为其中一跳显示 ASA，有必要减少 TTL。还必须在 **Configuration > Device Management > Management Access > ICMP** 上为 ICMP Unreachable 消息增加速率限制。

步骤 8 要启用 TCP 状态绕行，请选中 **TCP State Bypass**。

步骤 9 要启用 SCTP 状态绕行，请选中 **SCTP State Bypass**。

实施 SCTP 状态绕行，以便关闭 SCTP 状态检测。有关详细信息，请参阅 [SCTP 状态检测](#)，第 381 页。

步骤 10 （仅限 FXOS 1.1.3 或更高版本 Firepower 4100/9300 机箱中的 ASA。）要启用流量卸载，请选中 **Flow Offload**。

将符合条件的流量卸载到使用 NIC 本身交换流量的超快路径。此外，还必须启用卸载服务。依次选择 **Configuration > Firewall > Advanced > Offload Engine**。

步骤 11 点击 **OK** 或 **Finish**。

监控连接

使用以下页面监控连接：

- **Home > Firewall Dashboard**，并查看 **Top Ten Protected Servers under SYN Attack** 控制面板来监控 TCP 拦截。点击 **Detail** 按钮以显示历史抽样数据。在该速率间隔内，ASA 会对攻击数量抽样 30 次，所以对于默认的 30 分钟期间，统计信息每 60 秒收集一次。
- **Monitoring > Properties > Connections**，用于查看当前的连接。
- **Monitoring > Properties > Connection Graphs**，用于监控性能。

另外，可以使用 **Tools > Command Line Interface** 来输入以下命令。

- **show conn [detail]**

显示连接信息。详细信息使用标志来表示特殊连接特性。例如，“b”标志表示会对流量应用 TCP 状态绕行。

- **show flow-offload {info [detail] | cpu | flow [count | detail] | statistics}**

显示有关数据流分流的信息，包括常规状态信息、用于分流的 CPU 使用量、已分流的数据流数和详细信息，以及已分流的数据流统计信息。

- **show service-policy**

显示服务策略统计信息，包括失效连接检测 (DCD) 统计信息。

- **show threat-detection statistics top tcp-intercept [all | detail]**

查看遭受攻击的前 10 名受保护服务器。**all** 关键字显示所有被跟踪服务器的历史数据。**detail** 关键字显示历史采样数据。在该速率间隔内，ASA 会对攻击数量抽样 30 次，所以对于默认的 30 分钟期间，统计信息每 60 秒收集一次。

连接设置的历史

功能名称	平台版本	说明
TCP 状态绕行	8.2(1)	引入了此功能。引入了以下命令： set connection advanced-options tcp-state-bypass 。
所有协议的连接超时	8.2(2)	空闲超时已被更改为应用于所有协议，而不仅是 TCP 协议。 修改了以下屏幕：Configuration > Firewall > Service Policies > Rule Actions > Connection Settings。
使用备份静态路由的连接超时	8.2(5)/8.4(2)	当多个静态路由以不同的指标共存于一个网络时，ASA 将使用创建连接时指标最好的路由。如果有更好的路由变得可用，则此超时可让连接关闭，以便使用更好的路由重新建立连接。默认值为 0（连接永不超时）。要利用此功能，请将超时更改为新值。 修改了以下屏幕：Configuration > Firewall > Advanced > Global Timeouts。
可配置 PAT 转换超时	8.4(3)	如果 PAT 转换超时（默认为 30 秒后）且 ASA 使用该端口执行新的转换，因为以前的连接在上游设备中可能仍处于打开状态，有些上游路由器可能会拒绝该新连接。PAT 转换超时现在可配置为一个介于 30 秒到 5 分钟之间的值。 修改了以下屏幕：Configuration > Firewall > Advanced > Global Timeouts。 此功能在 8.5(1) 或 8.6(1) 中不可用。
服务策略规则增加的最大连接数限制	9.0(1)	服务策略规则的最大连接数从 65535 增加至 2000000。 修改了以下屏幕：Configuration > Firewall > Service Policy Rules > Connection Settings。
半闭超时最小值减小至 30 秒	9.1(2)	全局超时和连接超时的半闭超时最小值从 5 分钟缩短至 30 秒，以提供更好的 DoS 保护。 修改了以下菜单项： Configuration > Firewall > Service Policy Rules > Connection Settings； Configuration > Firewall > Advanced > Global Timeouts。
路由融合的连接等待超时。	9.4(3) 9.6(2)	现在，您可以配置在连接使用的路由不再存在或不活动时，系统应保持连接的时间。如果路由在此抑制期间未变为活动状态，连接将被释放。您可以减小抑制计时器，使路由汇聚更快速地进行。但是，默认值 15 秒适合大多数网络，可以防止路由摆动。 修改了以下菜单项：配置 > 防火墙 > 高级 > 全局超时。

功能名称	平台版本	说明
SCTP 空闲超时和 SCTP 状态绕行	9.5(2)	<p>您可以为 SCTP 连接设置空闲超时。另外，您还可以启用 SCTP 状态绕行，关闭某一类流量的 SCTP 状态检测。</p> <p>修改了以下屏幕：Configuration > Firewall > Advanced > Global Timeouts；Configuration > Firewall > Service Policy Rules 向导、Connection Settings 选项卡。</p>
Firepower 9300 上 ASA 的数据流分流。	9.5(2.1)	<p>您可以标识应从 ASA 中分流并直接在 NIC（在 Firepower 9300 上）中切换的流量。此功能可提升数据中心中的大数据流性能。</p> <p>此功能要求具有 FXOS 1.1.3 版本。</p> <p>在配置 > 防火墙 > 安全策略规则下添加或编辑规则时，添加或修改了以下菜单项：配置 > 防火墙 > 高级 > 分流引擎、规则行为 > 连接设置选项卡。</p>
Firepower 4100 系列上 ASA 的数据流分流支持。	9.6(1)	<p>您可以标识应从 ASA 中分流并直接在 Firepower 4100 系列的 NIC 中切换的流量。</p> <p>此功能需要 FXOS 1.1.4。</p> <p>此功能没有新的命令或 ASDM 屏幕。</p>
透明模式下组播连接的数据流分流支持。	9.6(2)	<p>现在，您可以卸载将在透明模式 Firepower 4100 和 9300 系列设备的网络接口卡中直接切换的组播连接。组播卸载仅适用于有且只有两个接口的网桥组。</p> <p>对于此功能，没有新的命令或 ASDM 菜单项。</p>
TCP 选项处理方式的变化。	9.6(2)	<p>现在，当配置 TCP 映射时，您可以在数据包的 TCP 报头中为 TCP MSS 和 MD5 选项指定操作。此外，对 MSS、timestamp、window-size 和 selective-ack 选项的默认处理已更改。以前，允许这些选项，即使报头中具有指定类型的多个选项也是如此。现在，默认情况下会丢弃包含指定类型的多个选项的数据包。例如，以前允许具有 2 个 timestamp 选项的数据包，而现在将丢弃该数据包。</p> <p>您可以配置 TCP 映射，以针对 MD5、MSS、selective-ack、timestamp 和 window-size 允许同一类型的多个选项。对于 MD5 选项，以前的默认设置为清除该选项，而现在的默认设置是允许它。您还可以丢弃包含 MD5 选项的数据包。对于 MSS 选项，您可以在 TCP 映射中设置最大分段大小（每个流量类）。所有其他 TCP 选项的默认设置均保持不变：被清除。</p> <p>修改了以下屏幕：Configuration > Firewall > Objects > TCP Maps Add/Edit对话框。</p>

功能名称	平台版本	说明
内部网关协议的过时路由超时	9.7(1)	现在您可以配置超时，用于删除内部网关协议（如 OSPF）的陈旧路由。 修改了以下菜单项： 配置 > 防火墙 > 高级 > 全局超时。
ICMP 全局超时错误	9.8(1)	现在可以设置 ASA 在接收 ICMP echo-reply 数据包后后、删除 ICMP 连接之前的空闲时间。如果禁用了此超时（默认），并且启用了 ICMP 检查，则 ASA 将在接收 echo-reply 后立即删除 ICMP 连接；因此将丢弃为该连接（现已关闭）生成的任何 ICMP 错误。此超时可以延迟删除 ICMP 连接，使您能够接收重要的 ICMP 错误。 修改了以下菜单项： 配置 > 防火墙 > 高级 > 全局超时。
TCP 状态绕行的默认空闲超时	9.10(1)	TCP 状态绕行连接的默认空闲超时现在为 2 分钟，而不是 1 小时。



第 19 章

服务质量

您是否曾用过使用卫星连接的长途电话？对话可能会不定期中断，出现短暂但可察觉的间隙。这些短暂间隙是在网络上传输的数据包到达之间的时间，即延迟。某些网络流量（例如语音和视频）不允许出现长时间延迟。通过服务质量 (QoS) 功能，您可以优先考虑重要流量、防止带宽占用及管理网络瓶颈，以防丢包。



注释 对于 ASASM，我们建议在交换机（而非 ASASM）上执行 QoS。交换机在此领域具有更多功能。通常，在网络路由器和交换机上执行 QoS 的效果最好，实现的功能常常比在 ASA 上还要广泛。

以下主题介绍如何应用 QoS 策略。

- [关于 QoS，第 435 页](#)
- [QoS 指南，第 437 页](#)
- [配置 QoS，第 438 页](#)
- [监控 QoS，第 442 页](#)
- [QoS 的历史，第 443 页](#)

关于 QoS

应考虑到，在不断变化的网络环境中，QoS 不是一次性部署，而是网络设计的持续必要的部分。

本节介绍 ASA 中可用的 QoS 功能。

支持的 QoS 功能

ASA 支持以下 QoS 功能：

- **策略管制** - 要防止分类流量占用网络带宽，可以限制每个类使用的最大带宽。有关详细信息，请参阅[策略管制，第 436 页](#)。
- **优先级排队** - 对于不允许出现延迟的关键流量（例如 IP 语音 [VoIP]），可以将此流量标记为低延迟排队 (LLQ) 的流量，以便其始终在其他流量之前传输。请参阅[优先级队列，第 436 页](#)。

什么是令牌桶？

令牌桶用于管理对流量中的数据进行管制的设备，例如流量监管器。令牌桶本身不具有丢弃或优先级策略。相反，如果流量超过管制器，令牌桶会丢弃令牌，并将管理传输队列的问题留给流量。

令牌桶是传输速率的正式定义。它包含三个组成部分：突发大小、平均速率和时间间隔。虽然平均速率通常表示为位/秒，但任意两个值可以通过以下关系从第三个值中推出：

平均速率 = 突发大小 / 时间间隔

以下是这些术语的部分定义：

- 平均速率 - 亦称承诺信息速率 (CIR)，指定单位时间平均发送或转发的数据量。
- 突发大小 - 亦称承诺突发 (Bc) 大小，以每次突发的字节为单位指定在给定的单位时间内可以发送而不引起调度问题的流量大小。
- 时间间隔 - 亦称测量间隔，以每次突发的秒为单位指定时间量。

在令牌桶比喻中，以一定速率将令牌添加到桶中。令牌桶本身有指定的容量。如果令牌桶容量已满，新到达的令牌会被丢弃。每个令牌允许源将一定数量的位发送到网络中。要发送数据包，管制器必须从令牌桶中删除与所代表的数据包大小相等的若干令牌。

如果令牌桶内没有足够的令牌来发送数据包，数据包会一直等，直到数据包被丢弃或被降级。如果令牌桶的令牌已满，传入的令牌会溢出而不能用于后续数据包。因此，在任何时刻，源能够发送到网络中的最大突发流量都大致与令牌桶的大小成正比。

策略管制

策略管制是一种通过确保流量不超过配置的最大速率（以位/秒为单位）以保证任何一个流量类都不会沿用全部资源的方式。如果流量超过最大速率，ASA 将丢弃超额的流量。策略管制还设定了允许的单个最大突发流量。

优先级队列

LLQ 优先级排队使您可以在处理其他流量之前优先处理某些流量（例如，像语音和视频之类的延迟敏感型流量）。优先级排队使用接口上的一个 LLQ 优先级队列（请参阅[为接口配置优先级队列](#)，第 439 页），而所有其他流量进入“尽力而为”队列。由于队列大小有限制，队列可以填满和溢出。如果队列已满，任何额外的数据包无法进入队列，并将丢弃。这称为尾部丢弃。要避免队列被填满，可以增加队列缓冲区的大小。还可以优化允许进入传输队列的数据包的最大数。这些选项使您能够控制优先级排队的延迟和稳定性。LLQ 队列中的数据包始终在“尽力而为”队列中的数据包之前传输。

如何交互使用 QoS 功能

如果需要，可以为 ASA 单独配置各种 QoS 功能。不过，ASA 上通常会配置多种 QoS 功能以便可以优先排列某些流量，并防止其他流量导致带宽问题。可以配置：

优先级排队（用于特定流量）+ 策略管制（用于其余流量）。

无法对同一组的流量配置优先级排队和策略管制。

DSCP (DiffServ) 保留

通过 ASA 的所有流量上都会保留 DSCP (DiffServ) 标记。ASA 不会在本地对任何分类流量进行标记/备注。例如，您可以切断每个数据包的快速转发 (EF) DSCP 位来确定该数据包是否需要“优先”处理，并让 ASA 将这些数据包定向到 LLQ。

QoS 指南

情景模式准则

仅支持单情景模式。不支持多情景模式。

防火墙模式指导原则

仅支持路由防火墙模式。不支持透明防火墙模式。

IPv6 指导原则

不支持 IPv6。

型号准则

- (ASA 5512-X 到 ASA 5555-X) 管理 0/0 接口不支持优先级排队。
- (ASASM) 仅支持策略管制。

其他准则和限制

- QoS 只能单向应用；只有流入（或流出，视 QoS 功能而定）应用了策略映射的接口的流量才会受到影响。
- 对于优先级流量，无法使用 **class-default** 类映射。
- 要执行优先级排队，必须为物理接口或 ASASM (VLAN) 配置优先级队列。
- 对于策略管制，不支持流向设备的流量。
- 对于策略管制，往返 VPN 隧道的流量会绕过接口策略管制。
- 对于策略管制，匹配隧道组类映射时，仅支持出站策略管制。

配置 QoS

按照以下顺序在 ASA 上实施 QoS。

过程

步骤 1 确定优先级队列的队列和传输环路限制，第 438 页。

步骤 2 为接口配置优先级队列，第 439 页。

步骤 3 为优先级排队和策略管制配置服务规则，第 440 页。

确定优先级队列的队列和传输环路限制

使用下列工作表确定优先级队列和传输环路限制。

队列限制工作表

下列工作表显示如何计算优先级队列大小。由于队列大小有限制，队列可以填满和溢出。当队列已满时，任何额外的数据包都无法进入队列并将被丢弃（称为尾部丢弃）。要避免队列被填满，可以根据[为接口配置优先级队列，第 439 页](#)调整队列缓冲区大小。

关于工作表的小提示：

- 出站带宽 - 例如，DSL 的上行链路速度可能为 768 Kbps。请与运营商核对。
- 平均数据包大小 - 通过编码解码器或采样量确定此值。例如，对于 VPN 上的 VoIP，可以使用 160 字节。如果不知道使用哪种大小，我们建议使用 256 字节。
- 延迟 - 延迟取决于应用。例如，VoIP 建议的最大延迟是 200 毫秒。如果不知道使用哪种延迟，我们建议使用 500 毫秒。

表 15: 队列限制工作表

1	_____	Mbps	x	125	=	_____		
	出站带宽 (单位为 <i>Mbps</i> 或 <i>Kbps</i>)					字节数/毫 秒		
		kbps	x	0.125	=	_____		
						字节数/毫 秒		

2	_____		÷	_____	x	_____	=	_____
	步骤 1 中的字节数/毫秒			平均数据包大小 (字节)		延迟 (毫秒)		队列限制 (数据包数)

传输环路限制工作表

下列工作表显示如何计算传输环路限制。此限制确定在以太网传输驱动器推回到接口的队列之前，允许进入驱动器的数据包的最大数量，以便缓冲数据包，直到堵塞消除为止。该设置确保基于硬件的传输环路对高优先级数据包施加有限数量的额外延迟。

关于工作表的小提示：

- 出站带宽 - 例如，DSL 的上行链路速度可能为 768 Kbps。请与运营商核对。
- 最大数据包大小 - 通常，最大数据包大小为 1538 字节（标记的以太网为 1542 字节）。如果允许超巨型帧（如果平台支持），则该数据包大小可能更大。
- 延迟 - 延迟取决于应用。例如，要控制 VoIP 的抖动，应使用 20 毫秒。

表 16: 传输环路限制工作表

1	_____	Mbps	x	125	=	_____		
	出站带宽 (单位为 Mbps 或 Kbps)	kbps	x	0.125	=	_____		
						字节数/毫秒		
						字节数/毫秒		
2	_____		÷	_____	x	_____	=	_____
	步骤 1 中的字节数/毫秒			最大数据包大小 (字节)		延迟 (毫秒)		传输环路限制 (数据包数)

为接口配置优先级队列

如果启用物理接口上流量的优先级排队，则需要每个接口上创建优先级队列。每个物理接口使用两个队列：一个用于优先级流量，另一个用于所有其他的流量。对于其他流量，可以选择配置策略管制。

开始之前

- (ASASM) ASASM 不支持优先级排队。

- (ASA 5512-X 到 ASA 5555-X) 管理 0/0 接口不支持优先级排队。

过程

步骤 1 依次选择配置 > 设备管理 > 高级 > 优先级队列，然后点击添加。

步骤 2 配置以下选项：

- **Interface** - 要在其上启用优先级队列的物理接口名称；对于 ASASM，为 VLAN 接口名称。
- **Queue Limit** -- 在500毫秒间隔内指定接口可传输的平均数，256字节数据包。范围为 0-2048，默认为 2048。

如果一个数据包在网络节点中停留时间超过 500 毫秒，可能会触发端到端应用的超时。各网络节点可以丢弃这类数据包。

由于队列大小有限制，队列可以填满和溢出。当队列已满时，任何额外的数据包都无法进入队列并将被丢弃（称为尾部丢弃）。要避免队列被填满，可以使用此选项增大队列缓冲区大小。

此选项数值范围的上限在运行时动态确定。关键决定因素是支持队列所需的内存和设备上可用的内存。

指定的 Queue Limit 对更高优先级的低延迟队列和“尽力而为”队列都有影响。

- **Transmission Ring Limit** - 优先级队列的深度，是指定接口在 10 毫秒时间间隔内可以传输的最大 1550 字节数据包的数量。范围为 3-511，默认为 511。

该设置确保基于硬件的传输环路对高优先级数据包的额外延迟不超过 10 毫秒。

此选项设定在以太网传输驱动器推回到接口上的队列之前，允许进入驱动器的低延迟或正常优先级数据包的最大数量，以便缓冲数据包，直到堵塞消除为止。

数值范围的上限在运行时动态确定。关键决定因素是支持队列所需的内存和设备上可用的内存。

您指定的传输环限制会影响较高优先级低延迟队列和尽力而为队列。

步骤 3 点击 OK，然后点击 Apply。

为优先级排队和策略管制配置服务规则

可以为同一策略映射中不同类映射配置优先级排队和策略管制。关于有效 QoS 配置的信息，请参阅[如何交互使用 QoS 功能，第 436 页](#)。

开始之前

- 对于优先级流量，无法使用 **class - default** 类映射。
- (ASASM) ASASM 仅支持策略管制。
- 对于策略管制，不支持流向设备的流量。

- 对于策略管制，往返 VPN 隧道的流量会绕过接口策略管制。
- 对于策略管制，匹配隧道组类映射时，仅支持出站策略管制。
- 对于优先级流量，仅识别延迟敏感型流量。
- 对于策略管制流量，可以选择对其他流量进行策略管制，也可以将流量限制到某些类型。

过程

步骤 1 依次选择配置 > 防火墙 > 服务策略，并打开规则。

可以将 QoS 配置为新的服务策略规则的一部分，或者编辑现有服务策略。

步骤 2 通过向导进入 Rules 页面，选择接口（或全局）以及相应的流量匹配条件。

对于策略管制流量，可以选择对不做优先级处理的所有流量进行策略管制，或者可以将流量限制到某些类型。

提示 如果使用 ACL 进行流量匹配，仅在 ACL 指定的方向上应用策略管制。即从源到目标的流量受到策略管制，但是从目标到源的流量则不受策略管制。

步骤 3 在 Rule Actions 对话框内，点击 **QoS** 选项卡。

步骤 4 选择 **Enable priority for this flow**。

如果服务策略规则适用于单个接口，ASDM 会自动为接口创建优先级队列（Configuration > Device Management > Advanced > Priority Queue；有关详细信息，请参阅[为接口配置优先级队列，第 439 页](#)）。如果此规则适用于全局策略，则需要在配置服务策略规则之前向一个或多个接口手动添加优先级队列。

步骤 5 选择 **Enable policing**，然后选中 **Input policing** 和/或 **Output policing** 复选框，以启用指定类型的流量策略管制。对于每类流量策略管制，请配置以下选项：

- **Committed Rate** - 此流量的速率限制；这是一个介于 8000 和 2000000000 之间的一个值，指定允许的最大速度（位/秒）。
- **Conform Action** - 在速率低于 conform-burst 值时待采取的操作。值为 transmit 或 drop。
- **Exceed Action** - 在速率介于 conform-rate 值和 conform-burst 值之间时采取的操作。值为 transmit 或 drop。
- **Burst Rate** - 介于 1000 和 512000000 之间的一个值，指定在减速到合格速率值之前持续突发中允许的最大短暂字节的数量。

步骤 6 点击 **Finish**，然后点击 **Apply**。

监控 QoS

以下主题介绍如何监控 QoS。

要监控 ASDM 中的 QoS，可以在命令行界面工具中输入命令。

QoS 策略统计信息

要查看流量策略管制的 QoS 统计信息，请使用 **show service-policy police** 命令。

```
hostname# show service-policy police

Global policy:
  Service-policy: global_fw_policy

Interface outside:
  Service-policy: qos
  Class-map: browse
    police Interface outside:
      cir 56000 bps, bc 10500 bytes
      conformed 10065 packets, 12621510 bytes; actions: transmit
      exceeded 499 packets, 625146 bytes; actions: drop
      conformed 5600 bps, exceed 5016 bps
  Class-map: cmap2
    police Interface outside:
      cir 200000 bps, bc 37500 bytes
      conformed 17179 packets, 20614800 bytes; actions: transmit
      exceeded 617 packets, 770718 bytes; actions: drop
      conformed 198785 bps, exceed 2303 bps
```

QoS 优先级统计信息

要查看实施 **priority** 命令的服务策略的统计信息，请使用 **show service-policy priority** 命令。

```
hostname# show service-policy priority

Global policy:
  Service-policy: global_fw_policy

Interface outside:
  Service-policy: qos
  Class-map: TGI-voice
  Priority:
    Interface outside: aggregate drop 0, aggregate transmit 9383
```

“Aggregate drop”表示此接口中的汇聚丢弃；“Aggregate transmit”表示此接口中已传输数据包的汇聚数量。

QoS 优先级队列统计信息

要显示某个接口的优先级队列统计信息，请使用 **show priority-queue statistics** 命令。结果将显示尽力而为 (BE) 队列和低延迟队列 (LLQ) 的统计信息。以下示例显示对名为 **test** 的接口应用 **show priority-queue statistics** 命令。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type           = BE
Packets Dropped      = 0
Packets Transmit     = 0
Packets Enqueued     = 0
Current Q Length     = 0
Max Q Length         = 0

Queue Type           = LLQ
Packets Dropped      = 0
Packets Transmit     = 0
Packets Enqueued     = 0
Current Q Length     = 0
Max Q Length         = 0
hostname#
```

在此统计报告中：

- “Packets Dropped” 表示此队列中已丢弃数据包的总数量。
- “Packets Transmit” 表示此队列中已传输数据包的总数量。
- “Packets Enqueued” 表示此队列中已排队数据包的总数量。
- “Current Q Length” 表示此队列当前的深度。
- “Max Q Length” 表示此队列曾发生过的最大深度。

QoS 的历史

功能名称	平台版本	说明
优先级排队和策略管制	7.0(1)	引入了 QoS 优先级排队和策略管制。 引入了以下屏幕： Configuration > Device Management > Advanced > Priority Queue Configuration > Firewall > Service Policy Rules
整形和分级式优先级排队	7.2(4)/8.0(4)	引入了 QoS 整形和分级式优先级排队。 修改了以下屏幕：Configuration > Firewall > Service Policy Rules。

功能名称	平台版本	说明
ASA 5585-X 标准优先级队列支持万兆以太网	8.2(3)/8.4(1)	我们为 ASA 5585-X 支持万兆以太网接口上的标准优先级队列。



第 20 章

威胁检测

以下主题介绍如何配置威胁检测统计信息和扫描威胁检测。

- [检测威胁，第 445 页](#)
- [威胁检测指南，第 447 页](#)
- [威胁检测的默认设置，第 447 页](#)
- [配置威胁检测，第 448 页](#)
- [监控威胁检测，第 451 页](#)
- [威胁检测的历史，第 452 页](#)

检测威胁

ASA 上的威胁检测是抵御攻击的第一道防线。威胁检测在第 3 层和第 4 层上工作，为设备上的流量制定基准，基于流量模式分析丢包统计信息，并累计“前面的”报告。相比之下，提供 IPS 或下一代 IPS 服务的模块可在 ASA 允许的流量中识别和减轻高达第 7 层的攻击媒介，但不能查看已被 ASA 丢弃的流量。因此，威胁检测和 IPS 能够协同工作，以提供更加全面的威胁防御。

威胁检测由以下要素组成：

- 为各种威胁收集的不同级别统计信息。

威胁检测统计信息可帮助您管理 ASA 面临的威胁，例如，如果启用扫描威胁检测，则查看统计信息可帮助您分析威胁。可以配置两种类型的威胁检测统计信息：

- 基本威胁检测统计信息 - 包括有关针对整个系统的攻击活动的信息。默认情况下启用基本威胁检测统计信息，并且不会对性能产生影响。
- 高级威胁检测统计信息 - 在对象级别跟踪活动，以便 ASA 可报告单个主机、端口、协议或 ACL 的活动。高级威胁检测统计信息会对性能产生重要影响，具体情况视收集的统计信息而定，因此，在默认情况下，仅启用 ACL 统计信息。
- 扫描威胁检测，其确定主机何时执行扫描。或者，可以避开任何被确定为扫描威胁的主机。

基本威胁检测统计信息

使用基本威胁检测统计信息，ASA 可监控由于以下原因被丢弃的数据包和安全事件的比率：

- 被 ACL 拒绝。
- 数据包格式错误（例如，invalid-ip-header 或 invalid-tcp-hdr-length）。
- 超出连接限制（系统范围的资源限制和在配置中设定的限制）。
- 检测到 DoS 攻击（例如，无效 SPI、状态防火墙检查故障）。
- 基本防火墙检查失败。此选项是一个组合比率，包含此列表中所有与防火墙有关的丢包。它不包括非防火墙相关丢弃，如接口过载、使应用检查失败的数据包以及检测到的扫描攻击。
- 检测到可疑的 ICMP 数据包。
- 数据包未通过应用检查。
- 接口过载。
- 检测到扫描攻击。此选项监控扫描攻击；例如，第一个 TCP 数据包并非 SYN 数据包，或者 TCP 连接未通过三方握手。例如，完整扫描威胁检测采用此扫描攻击频率信息，通过将主机分类为攻击者并自动避开这些主机，从而根据此信息采取行动。
- 不完整会话检测，例如检测到 TCP SYN 攻击或检测到无返回数据的 UDP 会话攻击。

当 ASA 检测到威胁时，会立即发送系统日志消息 (733100)。ASA 会跟踪两种速率类型：一段间隔的平均事件速率和较短突发间隔的突发事件速率。突发速率间隔为平均速率间隔的 1/30 或 10 秒，以较大者为准。对于收到的每个事件，ASA 会检查平均速率限制和突发速率限制；如果两种速率均超出限制，则 ASA 会发送两条单独的系统消息，对于每个突发期间的每种速率类型最多发送一条消息。

基本威胁检测仅当有丢包或潜在威胁时影响性能；即使在这种情况下，对性能的影响仍然可以忽略。

高级威胁检测统计信息

高级威胁检测统计信息显示单个对象（例如，主机、端口、协议或 ACL）允许和丢弃的流量速率。



注意

启用高级统计信息可能会影响 ASA 性能，具体取决于启用的统计信息类型。启用主机统计信息会严重影响性能；如果是高流量负载，可能要考虑临时启用这种统计信息类型。不过，端口统计信息造成的影响较小。

扫描威胁检测

典型的扫描攻击包含测试子网中每个 IP 地址可达性（通过扫描子网中的多台主机或扫描主机或子网中的多个端口）的主机。扫描威胁检测功能确定主机何时执行扫描。ASA 威胁检测扫描与基于流量

签名的 IPS 扫描检测不同，前者维护着广泛的数据库，其中包含可用来分析扫描活动的主机统计信息。

主机数据库跟踪可疑的活动（例如没有返回活动的连接、访问关闭的服务端口、如非随机 IPID 等易受攻击的 TCP 行为以及更多行为）。

如果超出扫描威胁速率，ASA 会发送系统日志消息 (733101) 并会选择性地避开攻击者。ASA 会跟踪两种速率类型：一段间隔的平均事件速率和较短突发间隔的突发事件速率。突发事件率为平均速率间隔的 1/30 或 10 秒，以较高者为准。对于检测到的被视为属于扫描攻击的每个事件，ASA 会检查平均速率限制和突发速率限制。如果从主机发送的流量超出任一速率，则该主机被视为攻击者。如果主机接收的流量超出任一速率，则该主机被视为目标。

下表列出扫描威胁检测的默认速率限制。

表 17: 扫描威胁检测的默认速率限制

平均速率	突发速率
在过去 600 秒内 5 个丢包/秒。	在过去 20 秒内 10 个丢包/秒。
在过去 3600 秒内 5 个丢包/秒。	在过去 120 秒内 10 个丢包/秒。



注意

扫描威胁检测功能可能会严重影响 ASA 的性能和内存，同时会创建和收集基于主机和子网的数据结构及信息。

威胁检测指南

安全情景指导原则

除了高级威胁统计信息，仅支持单一模式的威胁检测。在多模式下，仅支持 TCP 拦截统计信息。

监控的流量类型

- 仅监控通过设备的流量；流向设备的流量不包含在威胁检测中。
- ACL 拒绝的流量不会触发扫描威胁检测；只有允许通过 ASA 和创建数据流的流量才会受扫描威胁检测影响。

威胁检测的默认设置

默认情况下，启用基本威胁检测统计信息。

下表列出了默认的设置。可以使用 Tools > Command Line Interface 中的 **show running-config all threat-detection** 命令查看所有这些默认设置。

对于高级统计信息，默认情况下，启用 ACL 统计信息。

表 18: 基本的威胁检测默认设置

丢包原因	触发器设置	
	平均速率	突发速率
<ul style="list-style-type: none"> 检测到 DoS 攻击 数据包格式错误 超出连接限制 检测到可疑的 ICMP 数据包 	在过去 600 秒内 100 个丢包/秒。	在过去 20 秒内 400 个丢包/秒。
	在过去 3600 秒内 80 个丢包/秒。	在过去 120 秒内 320 个丢包/秒。
检测到扫描攻击	在过去 600 秒内 5 个丢包/秒。	在过去 20 秒内 10 个丢包/秒。
	在过去 3600 秒内 4 个丢包/秒。	在过去 120 秒内 8 个丢包/秒。
检测不完整会话，例如检测到 TCP SYN 攻击或检测到无返回数据的 UDP 会话攻击（组合）	在过去 600 秒内 100 个丢包/秒。	在过去 20 秒内 200 个丢包/秒。
	在过去 3600 秒内 80 个丢包/秒。	在过去 120 秒内 160 个丢包/秒。
被 ACL 拒绝	在过去 600 秒内 400 个丢包/秒。	在过去 20 秒内 800 个丢包/秒。
	在过去 3600 秒内 320 个丢包/秒。	在过去 120 秒内 640 个丢包/秒。
<ul style="list-style-type: none"> 基本防火墙检查失败 数据包未通过应用检查 	在过去 600 秒内 400 个丢包/秒。	在过去 20 秒内 1600 个丢包/秒。
	在过去 3600 秒内 320 个丢包/秒。	在过去 120 秒内 1280 个丢包/秒。
接口过载	在过去 600 秒内 2000 个丢包/秒。	在过去 20 秒内 8000 个丢包/秒。
	在过去 3600 秒内 1600 个丢包/秒。	在过去 120 秒内 6400 个丢包/秒。

配置威胁检测

默认情况下，启用基本威胁检测统计信息，而且您可能只需要威胁检测服务。如果要实施其他威胁检测服务，请使用以下操作步骤。

过程

步骤 1 配置基本威胁检测统计信息，第 449 页。

基本威胁检测统计信息包括可能与攻击（例如，DoS 攻击）有关的活动。

步骤 2 配置高级威胁检测统计信息，第 449 页。

步骤 3 配置扫描威胁检测，第 450 页。

配置基本威胁检测统计信息

默认情况下，启用基本威胁检测统计信息。可以禁用此功能，或者，如果已禁用，可以再次启用。

过程

步骤 1 依次选择配置 > 防火墙 > 威胁检测。

步骤 2 按需选择或取消选择 **Enable Basic Threat Detection**。

步骤 3 点击应用。

配置高级威胁检测统计信息

您可以将 ASA 配置为收集各种统计信息。默认情况下，启用 ACL 统计信息。要启用其他统计信息，请执行以下步骤。

过程

步骤 1 依次选择配置 > 防火墙 > 威胁检测。

步骤 2 在 Scanning Threat Statistics 区域，选择以下选项之一：

- **Enable All Statistic**。
- **Disable All Statistics**。
- **Enable Only Following Statistics**。

步骤 3 如果选择 **Enable Only Following Statistics**，则选择以下一个或多个选项：

- **Hosts** - 启用主机统计信息。只要主机处于活动状态并且位于扫描威胁主机数据库中，即可累积主机统计信息。处于非活动状态 10 分钟后，将从数据库中删除主机（并清除统计信息）。
- **Access Rules**（默认情况下启用）- 启用访问规则统计信息。

- **Port** - 启用 TCP 和 UDP 端口统计信息。
- **Protocol** - 启用非 TCP/UDP IP 协议统计信息。
- **TCP-Intercept** - 启用 TCP 拦截所拦截的攻击的统计信息（要启用 TCP 拦截，请参阅[保护服务器不受 SYN 洪流 DoS 攻击（TCP 拦截）](#)，第 419 页）。

步骤 4 对于主机、端口和协议统计信息，可以更改收集的速率间隔数量。在 **Rate Intervals** 区域，为每个统计信息类型选择 **1 hour**、**1 and 8 hours** 或 **1, 8 and 24 hours**。默认间隔为 **1 hour**，使内存使用率保持低位。

步骤 5 对于 TCP 拦截统计信息，可以在 **TCP Intercept Threat Detection** 区域设置以下选项：

- **Monitoring Window Size** - 设置历史监控窗口的大小，该值介于 1 到 1440 分钟之间。默认值为 30 分钟。在该速率间隔内，ASA 会对攻击数量抽样 30 次，所以对于默认的 30 分钟期间，统计信息每 60 秒收集一次。
- **Burst Threshold Rate** - 为系统日志消息生成设置阈值，该值介于 25 到 2147483647 之间。默认值为每秒 400 条消息。超出突发速率时，将生成系统日志消息 733104。
- **Average Threshold Rate** - 为系统日志消息生成设置平均速率阈值，该值介于 25 到 2147483647 之间。默认值为每秒 200 条消息。超出平均速率时，将生成系统日志消息 733105。

点击 **Set Default** 以恢复默认值。

步骤 6 点击应用。

配置扫描威胁检测

可以配置扫描威胁检测，以识别攻击者，或者避开攻击者。

过程

步骤 1 依次选择 **配置 > 防火墙 > 威胁检测**。

步骤 2 选择 **Enable Scanning Threat Detection**。

步骤 3 （可选）要在 ASA 将主机标识为攻击者时自动终止主机连接，请选择 **Shun Hosts detected by scanning threat**，并在需要时填入以下选项：

- 要使主机 IP 地址免于被避开，请在 **Networks excluded from shun** 字段中输入网络对象的地址或名称。可以输入多个地址或子网，用逗号分隔。要从 IP 地址对象列表中选择网络，请点击 **...** 按钮。
- 要为攻击主机设置避开持续时间，请选择 **Set Shun Duration**，并输入一个介于 10 到 2592000 秒之间的值。默认时长为 3600 秒（1 小时）。要恢复默认值，请点击 **Set Default**。

步骤 4 点击 **Apply**。

监控威胁检测

以下主题介绍如何监控威胁检测和查看流量统计信息。

监控基本威胁检测统计信息

依次选择 **Home > Firewall Dashboard > Traffic Overview**，以查看基本威胁检测统计信息。

监控高级威胁检测统计信息

可以使用以下控制面板监控高级威胁统计信息：

- **Home > Firewall Dashboard > Top 10 Access Rules** - 显示命中最多的访问规则。在此图形中不区分允许和拒绝。可以在 **Traffic Overview > Dropped Packets Rate** 图形中跟踪被拒绝的流量。
- **Home > Firewall Dashboard > Top Usage Statistics - Top 10 Sources** 和 **Top 10 Destinations** 选项卡显示主机统计信息。由于威胁检测算法，用作组合故障切换和状态链路的接口会在前 10 个主机中显示；这是预期行为，而且可以在显示内容中忽略此 IP 地址。
Top 10 Services 选项卡显示端口和协议统计信息（必须为显示内容启用两者），并且显示 TCP/UDP 端口和 IP 协议类型的组合统计信息。TCP（协议 6）和 UDP（协议 17）未包含在 IP 协议的显示内容中；但是，TCP 和 UDP 端口包含在端口的显示内容中。如果仅启用这些类型中一个类型（端口或协议）的统计信息，则只能查看启用的统计信息。
- **Home > Firewall Dashboard > Top Ten Protected Servers under SYN Attack** - 显示 TCP 拦截统计信息。点击**详细信息**按钮以显示历史抽样数据。在该速率间隔内，ASA 会对攻击数量抽样 30 次，所以对于默认的 30 分钟期间，统计信息每 60 秒收集一次。

威胁检测的历史

功能名称	平台版本	说明
基本和高级威胁检测统计信息、扫描威胁检测	8.0(2)	引入了基本和高级威胁检测统计信息、扫描威胁检测。 引入了以下屏幕： Configuration > Firewall > Threat Detection 、 Home > Firewall Dashboard > Traffic Overview 、 Home > Firewall Dashboard > Top 10 Access Rules 、 Home > Firewall Dashboard > Top Usage Status 、 Home > Firewall Dashboard > Top 10 Protected Servers Under SYN Attack 。
避开持续时间	8.0(4)/8.1(2)	现在可以设置避开持续时间。 修改了以下屏幕： Configuration > Firewall > Threat Detection 。
TCP 拦截统计信息	8.0(4)/8.1(2)	引入了 TCP 拦截统计信息。 引入或修改了以下屏幕： Configuration > Firewall > Threat Detection 、 Home > Firewall Dashboard > Top 10 Protected Servers Under SYN Attack 。
自定义主机统计信息速率间隔	8.1(2)	现在，可以自定义收集统计信息的速率间隔数。默认速率数已从 3 更改为 1。 修改了以下屏幕： Configuration > Firewall > Threat Detection 。
突发速率间隔已更改为平均速率的 1/30。	8.2(1)	在早期版本中，突发速率间隔为平均速率的 1/60。为最大限度利用内存，采样间隔已在平均速率中减少到 30 次。
自定义端口和协议统计信息速率间隔	8.3(1)	现在，可以自定义收集统计信息的速率间隔数。默认速率数已从 3 更改为 1。 修改了以下屏幕： Configuration > Firewall > Threat Detection 。
提高了内存使用率	8.3(1)	提高了威胁检测的内存使用率。