



CLI 手册 2: Cisco 安全防火墙 ASA 防火墙 CLI 配置指南, 9.23

上次修改日期: 2025 年 9 月 11 日

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 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 xxii

第 1 章

Cisco Secure Firewall ASA-防火墙服务 1

 如何实施防火墙服务 1

 基本访问控制 2

 URL 过滤 2

 威胁防范 2

 面向虚拟环境的防火墙服务 3

 网络地址转换 3

 应用检测 4

 应用场景：面向公众显示服务器 4

第 I 部分：

访问控制 7

第 2 章

访问控制的对象 9

 对象准则 9

 配置对象 10

 配置网络对象和组 10

 配置网络对象 10

 配置网络对象组 11

配置服务对象和服务组	12
配置服务对象	12
配置服务组	13
配置网络服务对象和组	15
网络服务对象的准则	15
配置受信任的 DNS 服务器	15
配置网络服务对象	17
配置网络服务对象组	18
配置本地用户组	20
配置安全组对象组	21
配置时间范围	22
监控对象	23
对象的历史记录	24

第 3 章

访问控制列表	27
关于 ACL	27
ACL 类型	27
ACL 名称	29
访问控制条目顺序	29
允许/拒绝与匹配/不匹配	29
访问控制隐式拒绝	29
使用 NAT 时用于扩展 ACL 的 IP 地址	30
基于时间的 ACE	31
访问控制列表的许可	31
ACL 准则	31
配置 ACL	32
基本 ACL 配置和管理选项	32
配置扩展 ACL	33
添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配	34
添加扩展 ACE 以执行基于端口的匹配	35
添加扩展 ACE 以执行基于 ICMP 的匹配	36

添加扩展 ACE 执行基于用户的匹配（身份防火墙）	37
添加扩展 ACE 执行基于安全组的匹配（思科 TrustSec）	38
扩展 ACL 的示例	38
将地址转换为扩展 ACL 对象的示例	39
配置标准 ACL	40
配置 Webtype ACL	41
添加 Webtype ACE 以执行 URL 匹配	41
添加 Webtype ACE 以执行 IP 地址匹配	42
Webtype ACL 的示例	43
配置 EtherType ACL	44
EtherType ACL 的示例	45
在隔离配置会话中编辑 ACL	46
监控 ACL	47
ACL 的历史记录	48

第 4 章

访问规则	51
控制网络访问	51
一般规则信息	52
接口访问规则和全局访问规则	52
入站和出站规则	52
规则顺序	53
隐式允许	53
隐式拒绝	54
NAT 和访问规则	54
相同安全级别的接口和访问规则	54
扩展访问规则	55
用于返回流量的扩展访问规则	55
允许广播和组播流量	55
管理访问规则	56
EtherType 规则	56
支持的 EtherType 和其他流量	56

返回流量的 EtherType 规则	56
允许 MPLS	57
面向访问规则的许可	57
访问控制准则	57
配置访问控制	58
配置访问组	58
配置 ICMP 访问规则	59
监控访问规则	61
评估访问规则的系统日志消息	62
允许或拒绝网络访问的配置示例	62
访问规则的历史记录	64

第 5 章

ASA 和思科 TrustSec	67
关于思科 TrustSec	67
关于思科 TrustSec 中的 SGT 和 SXP 支持	68
思科 TrustSec 功能中的角色	68
安全组策略实施	69
ASA 如何实施基于安全组的策略	70
更改 ISE 上安全组的效果	71
ASA 中的发言者和收听者	72
将 ASA 注册到 ISE	73
在 ISE 上创建安全组	73
生成 PAC 文件	74
思科 TrustSec 准则	74
将 ASA 配置为与思科 Trustsec 集成	77
配置 AAA 服务器以便与思科 TrustSec 集成	77
导入 PAC 文件	79
配置安全交换协议	80
添加 SXP 连接对等体	83
刷新环境数据	84
配置安全策略	84

配置第 2 层安全组标记实施	86
使用场合	86
在接口上配置安全组标记	87
手动配置 IP-SGT 绑定	89
故障排除提示	89
思科 TrustSec 示例	90
Secure Client VPN 支持思科 TrustSec	90
向远程访问 VPN 组策略和本地用户添加 SGT	91
监控 Cisco TrustSec	92
思科 TrustSec 的历史记录	93

第 6 章

思科 Umbrella	95
关于思科 Umbrella 连接器	95
思科 Umbrella 企业安全策略	95
思科 Umbrella 注册	96
从旧版 API 令牌切换到 API/密钥	96
思科 Umbrella 连接器的许可要求	97
思科 Umbrella 的准则和限制	97
配置思科 Umbrella 连接器	98
从思科 Umbrella 注册服务器安装 CA 证书	99
配置 Umbrella 连接器全局设置	100
在 DNS 检测策略映射中启用 Umbrella	103
验证 Umbrella 注册	104
Umbrella 连接器示例	105
示例：在全局 DNS 检测策略上启用 Umbrella	105
示例：在使用自定义检查策略的接口上启用 Umbrella	106
示例：从 Umbrella 全局排除某些主机或网络	106
监控 Umbrella 连接器	107
监控 Umbrella 服务策略统计信息	107
监控 Umbrella 系统日志消息	109
思科 Umbrella 连接器的历史记录	110

第 II 部分：	面向虚拟环境的防火墙服务	113
第 7 章	基于属性的访问控制	115
	基于属性的网络对象准则	115
	配置基于属性的访问控制	116
	配置 vCenter 虚拟机的属性	116
	配置虚拟机属性代理	118
	配置基于属性的网络对象	119
	使用基于属性的网络对象配置访问控制	121
	监控基于属性的网络对象	123
	基于属性的访问控制的历史记录	124
第 III 部分：	网络地址转换	125
第 8 章	网络地址转换 (NAT)	127
	为何使用 NAT?	127
	NAT 基础知识	128
	NAT 术语	128
	NAT 类型	128
	网络对象 NAT 和两次 NAT	129
	网络对象 NAT	129
	两次 NAT	129
	比较网络对象 NAT 和两次 NAT	129
	NAT 规则顺序	130
	NAT 接口	132
	NAT 准则	132
	NAT 防火墙模式准则	133
	IPv6 NAT 准则	133
	IPv6 NAT 最佳实践	133
	其他 NAT 准则	134

映射地址对象的网络对象 NAT 准则	136
用于实际与映射地址对象的两次 NAT 准则	137
FQDN 目的准则	138
实际和映射端口服务对象的两次 NAT 准则	139
动态 NAT	139
关于动态 NAT	139
动态 NAT 的优缺点	140
配置动态网络对象 NAT	141
配置静态两次 NAT	143
动态 PAT	146
关于动态 PAT	146
动态 PAT 的优缺点	147
PAT 池对象准则	147
配置动态网络对象 PAT	148
配置动态两次 NAT	150
使用端口块分配配置 PAT	153
配置每会话 PAT 或多会话 PAT	155
静态 NAT	157
关于静态 NAT	157
支持端口转换的静态 NAT	158
一对多静态 NAT	159
其他映射场景（不推荐）	160
配置静态网络对象 NAT 或支持端口转换的静态 NAT	161
配置静态两次 NAT 或支持端口转换的静态 NAT	164
身份 NAT	167
配置身份网络对象 PAT	167
配置身份两次 NAT	169
监控 NAT	171
NAT 的历史记录	171

网络对象 NAT 示例	177
为内部 Web 服务器提供访问（静态 NAT）	177
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）	178
具有多个映射地址的内部负载均衡器（静态 NAT，一对多）	180
用于 FTP、HTTP 和 SMTP（支持端口转换的静态 NAT）的单一地址	181
两次 NAT 的示例	182
根据目标进行不同的转换（动态两次 PAT）	182
根据目标地址和端口进行不同的转换（动态 PAT）	184
路由和透明防火墙模式下的 NAT	186
路由模式下的 NAT	186
透明模式下或桥接组内的 NAT	186
路由 NAT 数据包	188
映射地址和路由	188
地址与映射接口在相同的网络中	188
唯一网络中的地址	188
与实际地址相同的地址（身份 NAT）	189
远程网络的透明模式路由要求	190
确定出口接口	190
用于 VPN 的 NAT	191
NAT 和远程访问 VPN	191
NAT 和站点间 VPN	193
NAT 和 VPN 管理访问	196
NAT 和 VPN 故障排除	197
转换 IPv6 网络	197
NAT64/46：将 IPv6 地址转换为 IPv4 地址	198
NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网	198
NAT64/46 示例：包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络	199
NAT66：将 IPv6 地址转换为不同的 IPv6 地址	201
NAT66 示例：网络间的静态转换	201
NAT66 示例：简单 IPv6 接口 PAT	202
使用 NAT 重写 DNS 查询和响应	203

DNS 回复修改、外部接口上的 DNS 服务器	204
独立网络上的 DNS 应答修改、DNS 服务器、主机和服务	205
DNS 回复修改、主机网络上的 DNS 服务器	205
DNS64 应答修改	206
PTR 修改，主机网络上的 DNS 服务器	208

第 10 章

映射地址和端口 (MAP)	209
关于映射地址和端口 (MAP)	209
关于映射地址和端口转换 (MAP-T)	209
映射地址和端口 (MAP) 准则	210
配置 MAP-T 域	212
监控 MAP	213
验证 MAP 域配置	214
监控 MAP 系统日志消息	214
MAP 的历史记录	215

第 IV 部分：

服务策略和应用检测	217

第 11 章

服务策略	219
关于服务策略	219
服务策略的组件	219
使用服务策略配置的功能	221
功能方向性	222
服务策略中的功能匹配	222
多种功能操作的应用顺序	223
某些功能操作的不兼容性	224
多个服务策略的功能匹配	225
服务策略准则	225
服务策略默认设置	226
默认服务策略配置	227
默认类映射（流量类）	227

配置服务策略	228
身份流量（第 3/4 层类映射）	229
为通过流量创建第 3/4 层类映射	230
为管理流量创建第 3/4 层类映射	232
定义操作（第 3/4 层策略映射）	233
面向接口的应用操作（服务策略）	235
监控服务策略	235
服务策略（模块化策略框架）示例	236
向 HTTP 流量应用检测和 QoS 策略管制	236
对 HTTP 流量应用全局检测	236
向流入特定服务器的 HTTP 流量应用检测和连接限制	237
通过 NAT 对 HTTP 流量应用检测	238
服务策略的历史记录	238

第 12 章

应用层协议检测入门	241
应用层协议检测	241
何时使用应用协议检测	241
检测策略映射	242
更换正在使用的检测策略映射	242
如何处理多个流量类	242
应用检测准则	243
应用检测的默认设置	245
默认检测和 NAT 限制	245
默认检测策略映射	249
配置应用层协议检测	249
选择适合检测的流量类	254
配置正则表达式	255
创建正则表达式	255
创建正则表达式类映射	258
监控检测策略	258
应用检测的历史记录	259

第 13 章

基本互联网协议检测	261
DCERPC 检测	262
DCERPC 概述	262
配置 DCERPC 检测策略映射	262
DNS 检测	264
DNS 检测默认设置	265
配置 DNS 检测策略映射	265
FTP 检测	269
FTP 检测概述	269
严格 FTP	270
配置 FTP 检测策略映射	271
HTTP 检测	273
HTTP 检测概述	274
配置 HTTP 检测策略映射	274
ICMP 检查	278
ICMP 错误检测	278
ILS 检测	279
即时消息检测	279
IP 选项检测	282
IP 选项检测默认设置	282
配置 IP 选项检测策略映射	283
IPsec 穿透检测	284
IPsec 穿透检测概述	284
配置 IPsec 穿透检测策略映射	285
Ipv6 检测	286
IPv6 检测默认设置	286
配置 IPv6 检测策略映射	286
NetBIOS 检测	288
PPTP 检测	289
RSH 检测	289

SMTP 和扩展 SMTP 检测	289
SMTP 和 ESMTP 检测概述	290
ESMTP 检测默认设置	290
配置 ESMTP 检测策略映射	291
SNMP 检测	294
SQL*Net 检测	295
Sun RPC 检测	295
Sun RPC 检测概述	295
管理 Sun RPC 服务	295
TFTP 检测	297
XDMCP 检测	297
VXLAN 检测	297
基本互联网协议检测的历史记录	298

第 14 章

语音和视频协议检测	301
CTIQBE 检测	301
CTIQBE 检测的局限性	301
H.323 检测	302
H.323 检测概述	302
H.323 工作原理	302
H.245 消息中的 H.239 支持	303
H.323 检测的局限性	303
配置 H.323 检测策略映射	304
MGCP 检测	307
MGCP 检测概述	307
配置 MGCP 检测策略映射	308
RTSP 检测	310
RTSP 检测概述	310
RealPlayer 配置要求	310
RSTP 检测的局限性	310
配置 RTSP 检测策略映射	311

SIP 检测	313
SIP 检测概述	313
SIP 检查的限制	314
默认 SIP 检测	315
配置 SIP 检测策略映射	315
瘦客户端 (SCCP) 检测	318
SCCP 检测概述	319
支持思科 IP 电话	319
SCCP 检测的局限性	319
默认 SCCP 检测	320
配置瘦小客户端 (SCCP) 检测策略映射	320
STUN 检测	321
语音和视频协议检测的历史记录	322

第 15 章

移动网络检测	325
移动网络检测概述	325
GTP 检测概述	325
跟踪移动站位置更改	326
GTP 检测的局限性	326
流控制传输协议 (SCTP) 检测和访问控制	326
SCTP 状态检测	327
SCTP 访问控制	328
SCTP NAT	328
SCTP 应用层检测	328
SCTP 的局限性	328
Diameter 检测	329
M3UA 检测	330
M3UA 协议符合性	330
M3UA 检测的局限性	331
RADIUS 计费检测概述	331
移动网络协议检测的许可	331

GTP 检测默认设置	332
配置移动网络检测	333
配置 GTP 检测策略映射	333
配置 SCTP 检测策略映射	337
配置 Diameter 检测策略映射	339
创建自定义 Diameter 属性-值对 (AVP)	343
检查加密的 Diameter 会话	344
配置服务器与 Diameter 客户端的信任关系	345
使用静态客户端证书为 Diameter 检测配置完整 TLS 代理	347
为 Diameter 检测配置支持本地动态证书的完全 TLS 代理	350
为 Diameter 检测配置支持 TLS 分流的 TLS 代理	353
配置 M3UA 检测策略映射	355
配置移动网络检测服务策略	358
配置 RADIUS 计费检测	360
配置 RADIUS 计费检测策略映射	360
配置 RADIUS 计费检测服务策略	361
监控移动网络检测	363
监控 GTP 检测	363
监控 SCTP	364
监控 Diameter	365
监控 M3UA	366
移动网络检测的历史记录	367

第 V 部分：

连接管理和威胁检测 371

第 16 章

连接设置 373

什么是连接设置？	373
配置连接设置	374
配置全局超时	375
保护服务器不受 SYN 洪流 DoS 攻击 (TCP 拦截)	377
自定义异常 TCP 数据包处理 (TCP 映射、TCP 规范器)	380

绕过非对称路由的 TCP 状态检查（TCP 状态绕行）	383
非对称路由问题	383
有关 TCP 状态绕行的准则和限制	384
配置 TCP 状态绕行	385
禁用 TCP 序列随机化	386
分流大型数据流	388
数据流分流限制	388
配置数据流分流	390
IPsec 流分流	392
配置 IPsec 数据流分流	393
DTLS 加密加速	393
配置 DTLS 加密加速	393
监控 DTLS 加密加速	394
配置特定流量类的连接设置（所有服务）	395
配置 TCP 选项	400
监控连接	401
连接设置的历史记录	402

第 17 章

服务质量 407

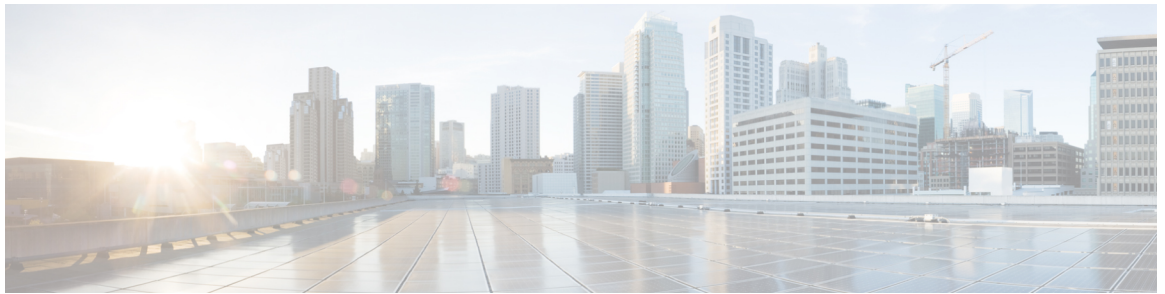
关于 QoS	407
支持的 QoS 功能	407
什么是令牌桶？	408
策略管制	408
优先级队列	408
如何交互使用 QoS 功能	408
DSCP (DiffServ) 保留	409
QoS 准则	409
配置 QoS	409
确定优先级队列的队列和传输环路限制	410
队列限制工作表	410
传输环路限制工作表	410

为接口配置优先级队列	411
为优先级排队和策略管制配置服务规则	412
监控 QoS	415
QoS 策略统计信息	415
QoS 优先级统计信息	415
QoS 优先级队列统计信息	416
优先级排队和策略管制的配置示例	416
VPN 流量的类映射示例	416
优先级和策略管制示例	417
QoS 的历史记录	418

第 18 章

威胁检测	419
检测威胁	419
基本威胁检测统计信息	420
高级威胁检测统计信息	420
扫描威胁检测	421
威胁检测准则	421
威胁检测的默认设置	422
配置威胁检测	423
配置基本威胁检测统计信息	423
配置高级威胁检测统计信息	424
配置扫描威胁检测	426
为 VPN 服务配置威胁检测	427
监控威胁检测	428
监控基本威胁检测统计信息	429
监控高级威胁检测统计信息	429
评估主机威胁检测统计信息	431
监控被避开的主机、攻击者和攻击目标	433
监控 VPN 服务的威胁检测	434
威胁检测 VPN 服务的系统日志监控	434
显示 VPN 服务威胁检测的监控命令	434

删除对 VPN 服务违规应用的规避次数	436
威胁检测示例	437
威胁检测的历史记录	437



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 xxii 页

文档目标

本指南旨在帮助您使用命令行界面来配置 Cisco Secure Firewall 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。

也可以使用自适应安全设备管理器 (ASDM) 这一基于 Web 的 GUI 应用来配置和监控 ASA。ASDM 提供配置向导指导您完成一些常见配置场景，并提供联机帮助以使您获得不常见场景的信息。

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。

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
boldface	命令、关键字、按钮标签、字段名称及用户输入的文本以 boldface 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。

约定	指示
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。注释部分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结果，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 DevNet](#)。
- 要获取一般网络、培训和认证主题相关的信息，请访问 [Cisco Press](#)。
- 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

Cisco Secure Firewall ASA-防火墙服务

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](#)
- [URL 过滤，第 2 页](#)
- [威胁防范，第 2 页](#)
- [面向虚拟环境的防火墙服务，第 3 页](#)
- [网络地址转换，第 3 页](#)
- [应用检测，第 4 页](#)
- [应用场景：面向公众显示服务器，第 4 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 URL 过滤。请参阅[URL 过滤，第 2 页](#)。
- 步骤 3** 实施威胁防范。请参阅[威胁防范，第 2 页](#)。
- 步骤 4** 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 3 页](#)。
- 步骤 5** 实施网络地址转换 (NAT)。请参阅[网络地址转换，第 3 页](#)。

步骤 6 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 4 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 51 页和[访问控制列表](#)，第 27 页。

可以通过对规则进行身份感知来扩充规则。要实施身份控制，请在单独的服务器上安装 Cisco Identity Services Engine (ISE)，以实施思科 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 67 页。

URL 过滤

URL 过滤根据目标站点的 URL 拒绝或允许流量。

要实施 URL 过滤，请订用 Cisco 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。该服务将为允许的域返回 FQDN 的真实 IP 地址。请参阅[思科 Umbrella](#)，第 95 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，但具有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 373 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 419 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 Virtual。

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 115 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 127 页
- [NAT 示例和参考](#)，第 177 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：

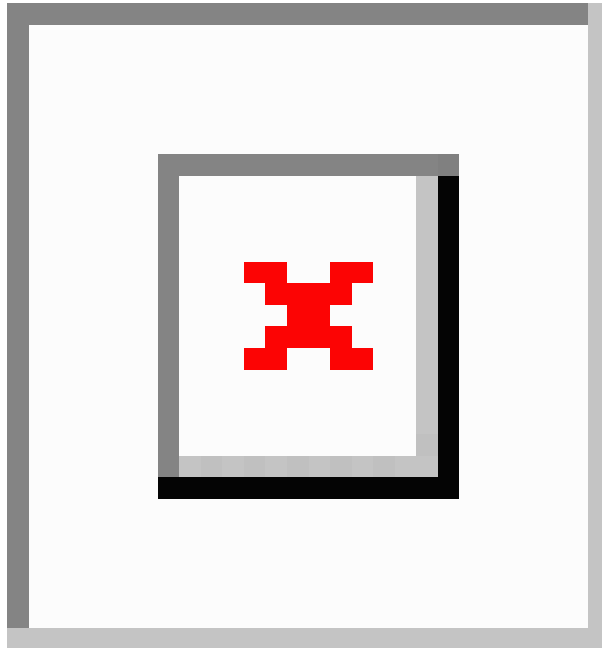
- [服务策略](#)，第 219 页
- [应用层协议检测入门](#)，第 241 页
- [基本互联网协议检测](#)，第 261 页
- [语音和视频协议检测](#)，第 301 页
- [移动网络检测](#)，第 325 页。

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

过程

步骤 1 为内部 Web 服务器创建网络对象。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 10.1.2.27
```

步骤 2 配置对象的静态 NAT：

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

步骤 3 向与外部接口关联的访问组添加访问规则，以允许对服务器进行 Web 访问。

```
hostname(config)# access-list outside_access_in line 1 extended
permit tcp any4 object myWebServ eq http
```

步骤 4 如果外部接口上没有访问组，请使用 `access-group` 命令应用该访问组：

```
hostname(config)# access-group outside_access_in in interface outside
```

■ 应用场景：面向公众显示服务器



第 I 部分

访问控制

- [访问控制的对象，第 9 页](#)
- [访问控制列表，第 27 页](#)
- [访问规则，第 51 页](#)
- [ASA 和思科 TrustSec，第 67 页](#)
- [思科 Umbrella，第 95 页](#)



第 2 章

访问控制的对象

对象指配置中可重用的组件。在 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。

- [对象准则，第 9 页](#)
- [配置对象，第 10 页](#)
- [监控对象，第 23 页](#)
- [对象的历史记录，第 24 页](#)

对象准则

IPv6 准则

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。
- 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。

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 127 页。

过程

步骤 1 使用对象名称创建或编辑网络对象：**object network object_name**

示例：

```
hostname(config)# object network email-server
```

步骤 2 使用以下命令之一将地址添加到对象。使用命令的 **no** 形式来删除对象。

- **host** {IPv4_address | IPv6_address} - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet** {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix} - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **range** start_address end_address - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。
- **fqdn** [v4 | v6] fully_qualified_domain_name - 完全限定域名，即主机的名称，例如 www.example.com。指定 **v4** 将地址限定于 IPv4，**v6** 将地址限定于 IPv6。如果未指定地址类型，则假定为 IPv4。

示例：

```
hostname(config-network-object)# host 10.2.2.2
```

步骤 3 （可选）添加说明：**description string**

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 使用对象名称创建或编辑网络对象组：**object-group network group_name**

示例：

```
hostname(config)# object-group network admin
```

步骤 2 使用以下一个或多个命令将对象和地址添加到网络对象组。使用命令的 **no** 形式来删除对象。

- **network-object host {IPv4_address|IPv6_address}** - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **network-object {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix}** - 网络或主机的地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **network-object object object_name** - 现有网络对象的名称。
- **group-object object_group_name** - 现有网络对象组的名称。

示例：

```
hostname(config-network-object-group)# network-object 10.1.1.0 255.255.255.0
hostname(config-network-object-group)# network-object 2001:db8:0:cd30::/60
hostname(config-network-object-group)# network-object host 10.1.1.1
hostname(config-network-object-group)# network-object host 2001:DB8::0DB8:800:200C:417A
hostname(config-network-object-group)# network-object object existing-object-1
hostname(config-network-object-group)# group-object existing-network-object-group
```

步骤 3 （可选）添加说明：**description string**

示例

要创建包含三个管理员 IP 地址的网络组，请输入以下命令：

```
hostname (config)# object-group network admins
hostname (config-protocol)# description Administrator Addresses
hostname (config-protocol)# network-object host 10.2.2.4
hostname (config-protocol)# network-object host 10.2.2.78
hostname (config-protocol)# network-object host 10.2.2.34
```

通过输入下列命令，为来自各部门的特权用户创建网络对象组：

```
hostname (config)# object-group network eng
hostname (config-network)# network-object host 10.1.1.5
hostname (config-network)# network-object host 10.1.1.9
hostname (config-network)# network-object host 10.1.1.89

hostname (config)# object-group network hr
hostname (config-network)# network-object host 10.1.2.8
hostname (config-network)# network-object host 10.1.2.12

hostname (config)# object-group network finance
hostname (config-network)# network-object host 10.1.4.89
hostname (config-network)# network-object host 10.1.4.100
```

然后按下述方法对所有三个组进行嵌套：

```
hostname (config)# object-group network admin
hostname (config-network)# group-object eng
hostname (config-network)# group-object hr
hostname (config-network)# group-object finance
```

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 使用对象名称创建或编辑服务对象：**object service object_name**

示例：

```
hostname (config)# object service web
```

步骤 2 使用以下命令之一将服务添加到对象。使用命令的 **no** 形式来删除对象。

- **service protocol** - IP 协议的名称或编号 (0-255)。指定 **ip** 以应用于所有协议。
- **service {icmp | icmp6} [icmp-type [icmp_code]]** - 适用于 ICMP 或 ICMP 版本 6 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。
- **service {tcp | udp | sctp} [source operator port] [destination operator port]** - 适用于 TCP、UDP 或 SCTP。或者，可以指定源端口、目标端口或两者。可以按名称或编号指定端口。操作符可以是以下任意一项：

- **lt** - 小于。
- **gt** - 大于。
- **eq** - 等于。
- **neq** - 不等于。
- **range** - 值的范围（包括边界值）。使用该操作符时，请指定两个端口编号，例如，**range 100 200**。

示例：

```
hostname(config-service-object)# service tcp destination eq http
```

步骤 3 （可选）添加说明：**description string**

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组对象的类型。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 使用对象名称创建或编辑服务对象组：**object-group service object_name**

示例：

```
hostname(config)# object-group service general-services
```

步骤 2 使用以下一个或多个命令将对象和服务添加到服务对象组。使用命令的 **no** 形式来删除对象。

- **service-object protocol** - IP 协议的名称或编号 (0-255)。指定 **ip** 以应用于所有协议。
- **service-object {icmp | icmp6} [icmp-type [icmp_code]]** - 适用于 ICMP 或 ICMP 版本 6 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。

- **service-object** {**tcp** | **udp** | **tcp-udp** | **sctp**} [**source operator port**] [**destination operator port**] - 适用于 TCP、UDP 或两者或适用于 SCTP。或者，可以指定源端口、目标端口或两者。可以按名称或编号指定端口。操作符可以是以下任意一项：

- **lt** - 小于。
- **gt** - 大于。
- **eq** - 等于。
- **neq** - 不等于。
- **range** - 值的范围（包括边界值）。使用该操作符时，请指定两个端口编号，例如，**range 100 200**。

- **service-object object object_name** - 现有服务对象的名称。
- **group-object object_group_name** - 现有服务对象组的名称。

示例：

```
hostname(config-service-object-group)# service-object ipsec
hostname(config-service-object-group)# service-object tcp destination eq domain
hostname(config-service-object-group)# service-object icmp echo
hostname(config-service-object-group)# service-object object my-service
hostname(config-service-object-group)# group-object Engineering_groups
```

步骤 3 （可选）添加说明： **description string**

示例

以下示例显示如何将 TCP 和 UDP 服务添加到服务对象组：

```
hostname(config)# object-group service CommonApps
hostname(config-service-object-group)# service-object tcp destination eq ftp
hostname(config-service-object-group)# service-object tcp-udp destination eq www
hostname(config-service-object-group)# service-object tcp destination eq h323
hostname(config-service-object-group)# service-object tcp destination eq https
hostname(config-service-object-group)# service-object udp destination eq ntp
```

以下示例显示如何将多个服务对象添加到服务对象组：

```
hostname(config)# object service SSH
hostname(config-service-object)# service tcp destination eq ssh
hostname(config)# object service EIGRP
hostname(config-service-object)# service eigrp
hostname(config)# object service HTTPS
hostname(config-service-object)# service tcp source range 1 1024 destination eq https
hostname(config)# object-group service Group1
hostname(config-service-object-group)# service-object object SSH
hostname(config-service-object-group)# service-object object EIGRP
```

```
hostname(config-service-object-group)# service-object object HTTPS
```

配置网络服务对象和组

网络服务对象或组定义了一个应用。应用可以由 DNS 域名（如 `example.com`）、IP 子网以及协议和端口（如 `TCP/80`）组成。因此，网络服务对象或组可以将不同网络和服务对象的内容合并为一个对象。

您可以在扩展 ACL 中使用网络服务对象组，以便与路由映射（在基于策略的路由选择中）、访问控制规则和 VPN 过滤器一起使用。请注意，不能在 ACL 中直接使用网络服务对象（而不是组）：必须先将对象放入组对象中，然后才能使用组对象。

使用域名规范时，系统会使用 DNS 监听来获取 IP 地址，这些 IP 地址是在连接开始前通过用户的 DNS 请求获得的。这样可以确保在连接开始时就有 IP 地址，以便路由映射和访问控制规则从第一个数据包开始就能正确处理连接。

网络服务对象的准则

- 如果在网络服务对象中包含 DNS 域名规范，则需要进行 DNS 检测。默认情况下，DNS 检测已启用。如果使用网络服务对象，请勿禁用它。
- DNS 监听只针对 UDP DNS 数据包，不针对 TCP 或 HTTP DNS 数据包。与完全限定域名对象不同，即使不在访问列表中使用该对象，也会立即监听网络服务域名规范。
- 不能在 DNS 检测策略映射中启用 `dnsCrypt`；它与 DNS 监听不兼容，而 DNS 监听是为网络服务对象中使用的域获取 IP 地址所必需的。任何包含域规范的网络服务对象都将无法操作，相关的访问控制条目也将无法匹配。
- 您最多可以定义 1024 个网络服务组。但是，身份防火墙本地用户组也共享这一限制。每定义一个网络服务组，就可以少创建 2 个用户组。
- 网络服务组的内容可以重叠，但不能创建网络服务组的完整副本。
- 如果 ACL 中使用了网络服务对象或组，删除该对象只需清除对象内容即可。对象本身仍在配置中定义。
- **dynamic** 关键字意味着对象不会保存到运行配置，它将仅显示在 `show object` 输出中。请勿直接配置此关键字。关键字主要供外部设备管理器使用。
- 该编号是思科为特定应用分配的唯一编号，范围为 1-4294967295。**app-id** 请勿直接配置此命令。此命令主要供外部设备管理器使用。

配置受信任的 DNS 服务器

如果在网络服务对象中配置域名，系统就会监听 DNS 请求/响应流量，以收集 DNS 域名的 IP 地址，并缓存结果。任何 DNS 请求/响应都可以被监听。

监听的记录包括 A、AAAA 和 MX。每个已解析名称的生存时间 (TTL) 都在一定范围内：最小 TTL 为 2 分钟，最大为 24 小时。这样可以确保缓存不会过时。

出于安全考虑，可以通过定义哪些 DNS 服务器应受信任来限制 DNS 监听的范围。指向非信任 DNS 服务器的任何 DNS 流量都会被忽略，也不会用于获取网络服务对象的映射。默认情况下，所有已配置和已学习的 DNS 服务器都是受信任的；只有在要限制受信任列表时才需要更改。



注释 关键在于您要将客户端使用的 DNS 服务器定义为受信任服务器。

开始之前

DNS 监听依赖于 DNS 检查，默认情况下已启用。确保没有禁用检测。此外，DNS 监听与 **dnsCrypt** 功能不兼容，因此请勿在 DNS 检测策略映射中启用该命令。

过程

步骤 1 使用 **show dns trusted-source detail** 命令确定已下载到数据路径以用于网络服务对象域解析的当前受信任服务器。

默认情况下，信任任何在 DNS 组中配置的 DNS 服务器，或通过 DHCP 客户端/服务器或中继配置的 DNS 服务器。此命令显示当前设置和受信任的服务器。

示例：

```
ciscoasa# show dns trusted-source detail
DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
  DNS Server Configured: 10.163.47.11: management : N/A
  DNS Server Configured: 10.37.137.85: management : N/A
  DNS Server Configured: 10.37.142.73: management : N/A
Data-Path DNS Trusted Source (count 3): <ip>/<refcnt>; Trust-any disabled
  10.37.142.73/1
  10.37.137.85/1
  10.163.47.11/1
```

步骤 2 （可选。）添加或删除显式配置的受信任 DNS 服务器：

dns trusted-source ip_list

ip_list 是应信任的 DNS 服务器 IP 地址的列表，以空格分隔。您最多可以列出 12 个 IPv4 和 IPv6 地址。指定 **any** 以涵盖所有 DNS 服务器。使用命令的 **no** 形式来删除服务器。

步骤 3 （可选。）指定是否信任 DNS 服务器组中配置的服务器。

dns trusted-source configured-servers

配置的服务器是 DNS 组或 **name-server** 命令中指定的任何服务器。默认情况下，此选项已启用。要将其禁用，请使用这些命令的 **no** 形式。

步骤 4 （可选。）指定是否要信任 DHCP 池中为通过设备接口上运行的 DHCP 服务器获取地址的客户端配置的 DNS 服务器。

dns trusted-source dhcp-pools

这些是使用 **dhcpd dns** 命令配置的服务器，因此仅为 IPv4。默认情况下，此选项已启用。要将其禁用，请使用这些命令的 **no** 形式。

步骤 5 （可选。）指定通过 DHCP 客户端和 DHCP 服务器之间的 DHCP 中继消息监听所了解到的服务器是否被视为受信任的 DNS 服务器。

dns trusted-source dhcp-relay

默认情况下，此选项已启用。要将其禁用，请使用这些命令的 **no** 形式。

步骤 6 （可选。）指定通过 DHCP 客户端和 DHCP 服务器之间的消息监听所了解到的服务器是否被视为受信任的 DNS 服务器。

dns trusted-source dhcp-client

该选项适用于配置 **dhcpd auto_config** 命令时，使用从通过 DHCP 客户端获取 IP 地址的设备接口上获得的信息在内部接口上配置 DHCP 服务器。默认情况下，此选项已启用。要将其禁用，请使用这些命令的 **no** 形式。

配置网络服务对象

网络服务对象定义了一个应用。它通过子网规范或更常见的 DNS 域名来定义应用的位置。您也可以选择包括协议和端口，以缩小应用的范围。

只能在网络服务组对象中使用这些对象；不能在访问控制列表条目 (ACE) 中直接使用网络服务对象。

过程

步骤 1 使用对象名称创建或编辑网络服务对象：

object network-service object_name

名称最多可包含 128 个字符，并且可以包含空格。如果包含空格，则必须用双引号将名称引起来。

示例：

```
ciscoasa(config)# object network-service webex
```

步骤 2 使用以下命令之一向对象添加一个或多个应用程序位置和可选服务。使用命令的 **no** 形式来删除对象。您可以多次输入这些命令。

- **domain domain_name [service]** - DNS 名称，最多 253 个字符。名称可以是完全限定的（例如 **www.example.com**）或部分名称（例如 **example.com**），在后一种情况下，对象会匹配所有子域，即使用部分名称的服务器（如 **www.example.com**、**www1.example.com**、

long.server.name.example.com 等)。如果存在完全匹配的名称, 则将根据最长名称对连接进行匹配。域名可以解析到多个 IP 地址。

- **subnet** {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix} [service] - 网络地址。对于 IPv4 子网, 请在空格后添加掩码, 例如, 10.0.0.0 255.0.0.0。对于 IPv6, 请将地址和前缀作为一个整体 (不带空格), 例如 2001:DB8:0:CD30::/60。

这些命令的服务规范相同。只有当您想限制匹配的连接范围时, 才指定服务。默认情况下, 与已解析 IP 地址的任何连接都与对象相匹配。

protocol [operator port]

其中:

- *protocol* 是连接中使用的协议, 例如 tcp、udp、ip 等。使用 ? 查看协议列表。
- (仅限 TCP/UDP。) *operator* 为以下选项之一:
 - **eq** 等于指定的端口号。
 - **lt** 表示小于指定端口号的任何端口。
 - **gt** 表示大于指定端口号的任何端口。
 - **range** 表示两个指定端口之间的任何端口。
- (仅限 TCP/UDP。) *port* 是端口号 1-65535 或助记符, 例如 www。使用 ? 查看助记符。对于范围, 必须指定两个端口, 并且第一个端口号要小于第二个端口号。

步骤 3 (可选) 添加说明 (最多 200 个字符): **description string**

示例

```
object network-service outlook365
  description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

配置网络服务对象组

网络服务组可以包含网络服务对象和明确的子网或域规范。您可以在访问控制列表条目 (ACE) 中使用网络服务对象, 以实现基于策略的路由选择、访问控制和 VPN 过滤。

使用 **network-service groups** 可定义应以相同方式处理的应用的类别。例如, 您可以创建一个组, 定义其流量应导向互联网而不是指向企业中心的站点间 VPN 通道的应用程序。

对于网络服务对象组中包含的应用程序数量, 没有任何限制, 无论是显式还是通过引用网络服务对象。

过程

步骤 1 使用组名创建或编辑网络服务对象组：

object-group network-service *group_name*

名称最多可包含 128 个字符，并且可以包含空格。如果包含空格，则必须用双引号将名称引起来。

示例：

```
ciscoasa(config)# object-group network-service SaaS_Applications
```

步骤 2 使用以下命令之一向对象添加一个或多个应用程序位置和可选服务。使用命令的 **no** 形式来删除对象。您可以多次输入这些命令。

- **network-service-member** *object_name* - 组中包含的网络服务对象的名称。如果名称中有空格，请用双引号括起来。
- **domain** *domain_name* [*service*] - DNS 名称，最多 253 个字符。名称可以是完全限定的（例如 `www.example.com`）或部分名称（例如 `example.com`），在后一种情况下，对象会匹配所有子域，即使用部分名称的服务器（如 `www.example.com`、`www1.example.com`、`long.server.name.example.com` 等）。如果存在完全匹配的名称，则将根据最长名称对连接进行匹配。域名可以解析到多个 IP 地址。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*] - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，`10.0.0.0 255.0.0.0`。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 `2001:DB8:0:CD30::/60`。

这些命令的服务规范相同。只有当您想限制匹配的连接范围时，才指定服务。默认情况下，与已解析 IP 地址的任何连接都与对象相匹配。

protocol [*operator port*]

其中：

- *protocol* 是连接中使用的协议，例如 `tcp`、`udp`、`ip` 等。使用 ? 查看协议列表。
- （仅限 TCP/UDP。）*operator* 为以下选项之一：
 - **eq** 等于指定的端口号。
 - **lt** 表示小于指定端口号的任何端口。
 - **gt** 表示大于指定端口号的任何端口。
 - **range** 表示两个指定端口之间的任何端口。
- （仅限 TCP/UDP。）*port* 是端口号 1-65535 或助记符，例如 `www`。使用 ? 查看助记符。对于范围，必须指定两个端口，并且第一个端口号要小于第二个端口号。

步骤 3 （可选）添加说明（最多 200 个字符）：**description string****示例**

使用之前定义的网络服务对象配置一组 SaaS 应用。

```
object-group network-service SaaS_Applications
  description This group includes relevant 'Software as a Service' applications
  network-service-member "outlook 365"
  network-service-member webex
  network-service-member box
```

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或用户组。

过程**步骤 1** 使用对象名称创建或编辑用户对象组：**object-group user group_name**

示例：

```
hostname(config)# object-group user admins
```

步骤 2 使用以下一个或多个命令将用户和组添加到用户对象组。使用命令的 **no** 形式来删除对象。

- **user [domain_NETBIOS_name\]username** - 用户名。如果域名或用户名中有空格，必须用引号将域名和用户名引起来。域名可以是 LOCAL（适用于本地数据库中定义的用户）或 **user-identity domain domain_NetBIOS_name aaa-server aaa_server_group_tag** 命令中指定的 Active Directory (AD) 域名。添加 AD 域中定义的用户时，**user_name** 必须是 Active Directory sAMAccountName（唯一），而非公用名(cn）（可能不唯一）。如果未指定域名，则使用默认域名，即 LOCAL 或 **user-identity default-domain** 命令中定义的域名。

- **user-group** *[domain_NETBIOS_name\\]username* - 用户组。如果域名或组名中有空格，必须用引号将域名和组名引起来。请注意分隔域名和组名的双反斜杠 \\。
- **group-object** *object_group_name* - 现有用户对象组的名称。

示例:

```
hostname(config-user-object-group)# user EXAMPLE\admin
hostname(config-user-object-group)# user-group EXAMPLE\managers
hostname(config-user-object-group)# group-object local-admins
```

步骤 3 (可选) 添加说明: **description string**

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 使用对象名称来创建或编辑安全组对象组: **object-group security group_name**

示例:

```
hostname(config)# object-group security mktg-sg
```

步骤 2 使用以下一个或多个命令将对象添加到服务组对象组。使用命令的 **no** 形式来删除对象。

- **security-group** {tag *sgt_number* | name *sg_name*} - 安全组标签 (SGT) 或名称。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。
- **group-object** *object_group_name* - 现有安全组对象组的名称。

示例：

```
hostname(config-security-object-group)# security-group tag 1
hostname(config-security-object-group)# security-group name mgkt
hostname(config-security-object-group)# group-object local-sg
```

步骤 3 （可选）添加说明：**description string**

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 创建时间范围：**time-range name**

步骤 2 （可选。）为时间范围添加起始时间或结束时间（或两者）。

absolute [*start time date*] [*end time date*]

如果未指定起始时间，则默认当前时间为起始时间。

time 采用 24 小时格式 *hh:mm*。例如，8:00 表示上午 8:00，20:00 表示晚上 8:00。

date 的格式为：*day month year*，例如 **1 January 2014**。

步骤 3 （可选。）添加循环时间周期。

periodic *days-of-the-week time to* [*days-of-the-week*] *time*

可以为 *days-of-the-week* 指定以下值。请注意，只有为第一个参数指定了某一天时，才可以指定一个星期中的第二天。

- **Monday、Tuesday、Wednesday、Thursday、Friday、Saturday 或 Sunday**。可以为第一个 *days-of-the-week* 参数指定上述其中多个值（用空格隔开）。
- **daily**
- **weekdays**
- **weekend**

time 采用 24 小时格式 *hh:mm*。例如，8:00 表示上午 8:00，20:00 表示晚上 8:00。

可以重复该命令来配置多个循环时间段。

示例

以下示例表示从 2006 年 1 月 1 日上午 8:00 开始的绝对时间范围。由于未指定结束时间和日期，因此该时间范围无限期有效。

```
hostname(config)# time-range for2006
hostname(config-time-range)# absolute start 8:00 1 january 2006
```

以下示例表示工作日从上午 8:00 到下午 6:00 的每周定期时间范围：

```
hostname(config)# time-range workinghours
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
```

以下示例确定时间范围的结束日期，且设置从上午 8 点到下午 5 点的工作日时间段，以及星期一、星期三和星期五与星期二和星期四不同的下午 5 点之后的时间。

```
asa4(config)# time-range contract-A-access
asa4(config-time-range)# absolute end 12:00 1 September 2025
asa4(config-time-range)# periodic weekdays 08:00 to 17:00
asa4(config-time-range)# periodic Monday Wednesday Friday 18:00 to 20:00
asa4(config-time-range)# periodic Tuesday Thursday 17:30 to 18:30
```

监控对象

要监控对象和组，请输入以下命令：

- **show access-list**

显示访问列表条目。包括对象的条目也会基于对象内容展开显示单个条目。

- **show running-config object [id object_id]**

显示当前所有的对象。使用 **id** 关键字按名称查看单个对象。

- **show running-config object *object_type***

按类型（**network** 或 **service**）显示当前对象。

- **show running-config object-group [*id group_id*]**

显示当前所有的对象组。使用 **id** 关键字按名称查看单个对象组。

- **show running-config object-group *grp_type***

按组类型显示当前对象组。

对象的历史记录

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。 引入或修改了以下命令： object-group protocol 、 object-group network 、 object-group service 、 object-group icmp_type 。
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。 引入或修改了以下命令： object-network 、 object-service 、 object-group network 、 object-group service 、 network object 、 access-list extended 、 access-list webtype 、 access-list remark 。
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。 引入了以下命令： object-network user 、 user 。
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 引入了以下命令： object-network security 、 security 。
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。 修改了以下命令： object-group network 。

功能名称	平台 版本	说明
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。 引入或修改了以下命令： access-list extended 、 service-object 、 service 。
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。 修改了以下命令： service-object 、 service 。
网络服务对象及其在基于策略的路由和访问控制中的使用。	9.17(1)	您可以配置网络服务对象并将其用于扩展访问控制列表，以便在基于策略的路由映射和访问控制组中使用。网络服务对象包括 IP 子网或 DNS 域名规范，以及（可选）协议和端口规范，它们实质上结合了网络和服务对象。此功能还包括定义受信任 DNS 服务器的功能，以确保任何 DNS 域名解析都从受信任来源获取 IP 地址。 添加或修改了以下命令： access-list extended 、 app-id 、 clear configure object network-service 、 clear configure object-group network-service 、 clear dns ip-cache 、 clear object 、 clear object-group 、 debug network-service 、 description 、 dns trusted-source 、 domain 、 network-service-member 、 network-service reload 、 object-group network-service 、 object network-service 、 policy-route cost 、 set adaptive-interface cost 、 show asp table classify 、 show asp table network-service 、 show dns trusted-source 、 show dns ip-cache 、 show object 、 show object-group 、 show running-config 、 subnet 。
网络服务组支持	9.19(1)	您现在最多可以定义 1024 个网络服务组。



第 3 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 51 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 27 页
- [访问控制列表的许可](#)，第 31 页
- [ACL 准则](#)，第 31 页
- [配置 ACL](#)，第 32 页
- [在隔离配置会话中编辑 ACL](#)，第 46 页
- [监控 ACL](#)，第 47 页
- [ACL 的历史记录](#)，第 48 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。请参阅[配置扩展 ACL](#)，第 33 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 ACL](#)，第 44 页。

- Webtype ACL - Webtype 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 Webtype ACL](#)，第 41 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 40 页。

下表列出 ACL 的一些常见用途及使用的类型。

表 1: 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间 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	Webtype	可以配置 Webtype ACL 以过滤 URL 和目标。

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。

在扩展 ACL 中，使用 `access-list` 命令上的 `line number` 参数将规则插入正确位置。使用 `show access-list name` 命令查看 ACL 条目及其行号以帮助确定要使用的正确行号。对于其他类型的 ACL，必须重新创建 ACL（或最好使用 ASDM）以更改 ACE 的顺序。

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。

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)。

```
hostname(config)# object network server1
hostname(config-network-object)# host 10.1.1.5
hostname(config-network-object)# nat (inside,outside) static 209.165.201.5

hostname(config)# access-list OUTSIDE extended permit tcp any host 10.1.1.5 eq www
hostname(config)# access-group OUTSIDE in interface outside
```

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 准则

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。

故障转移和集群

配置会话未在故障转移或集群设备间同步。在会话中进行更改时，将在故障转移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。

其他准则

- 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）。
- （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 ACL。请阅读有关 ACL 基本信息的章节以了解总体情况，然后阅读有关特定类型 ACL 的章节了解详细信息。

基本 ACL 配置和管理选项

ACL 由一个或多个具有相同 ACL ID 或名称的访问控制条目 (ACE) 组成。要创建新的 ACL，只需使用新的 ACL 名称创建 ACE 即可，该 ACE 将成为新 ACL 中的第一条规则。

使用 ACL 时，可执行下列操作：

检查 ACL 内容并确定行号和命中计数

使用 **show access-list name** 命令查看 ACL 的内容。每一行是一个 ACE，并且包括行号，如果要将新条目插入扩展 ACL 中，则需要了解这些信息。信息还包括每个 ACE 的命中次数，即为流量匹配规则的次数。例如：

```
hostname# show access-list outside_access_in
access-list outside_access_in; 3 elements; name hash: 0x6892a938
access-list outside_access_in line 1 extended permit ip 10.2.2.0 255.255.255.0 any
(hitcnt=0) 0xcc48b55c
access-list outside_access_in line 2 extended permit ip host
2001:DB8::0DB8:800:200C:417A any (hitcnt=0) 0x79797f94
access-list outside_access_in line 3 extended permit ip user-group
LOCAL\\usergroup any any (hitcnt=0) 0xb0f5b1e1
```

添加 ACE

添加 ACE 的命令为 **access-list name [line line-num] type parameters**。行号参数仅适用于扩展 ACL。如果在命令中包含行号，ACE 将插入 ACL 中的该位置，而且该位置的 ACE 及其余 ACE 将向

下移动（即，在行号处插入 ACE 不会取代该行上的旧 ACE）。如果不包含行号，ACE 将被添加到 ACL 末尾。可用参数因 ACL 类型而异；请参阅每个 ACL 类型的特定主题以了解详细信息。

向 ACL 中添加注释（除 webtype 之外的所有类型）

使用 **access-list name [line line-num] remark text** 命令向 ACL 中添加备注，以帮助说明 ACE 的用途。最佳实践是在 ACE 之前插入备注；如果在 ASDM 中查看配置，备注将与备注后面的 ACE 关联。可以在 ACE 之前输入多个备注以包含一个扩展注释。每条备注限制在 100 个字符以内。可以包含前导空格以帮助引出备注。如果不包含行号，备注将被添加到 ACL 末尾。例如，可以在添加每个 ACE 之前添加备注：

```
hostname(config)# access-list OUT remark - this is the inside admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT remark - this is the hr admin address
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any
```

编辑或移动 ACE 或备注

无法编辑或移动 ACE 或备注。相反，必须使用所需的值在正确位置创建新的 ACE 或备注（使用行号），然后删除旧的 ACE 或备注。由于只能将 ACE 插入扩展 ACL，如果需要编辑或移动 ACE，则需要重新建立标准 ACL、Webtype ACL 或 EtherType ACL。使用 ASDM 能更容易地重新组织较长的 ACL。

删除 ACE 或备注

使用 **no access-list parameters** 命令删除 ACE 或备注。使用 **show access-list** 命令查看您必须输入的参数字符串：字符串必须完全匹配 ACE 或备注才能将其删除，**line line-num** 参数除外，该参数对于 **no access-list** 命令为可选参数。

删除整个 ACL，包括备注

使用 **clear configure access-list name** 命令。务必要谨慎使用该命令！该命令不会要求您进行确认。如果未包含名称，ASA 中的每个访问列表都会被删除。

重命名 ACL

使用 **access-list name rename new_name** 命令。

将 ACL 应用到策略

创建一个 ACL，就其本身不对流量执行任何操作。必须将 ACL 应用到策略。例如，可以使用 **access-group** 命令将扩展 ACL 应用到接口，从而拒绝或允许通过接口的流量。

配置扩展 ACL

扩展 ACL 由具有相同 ACL ID 或名称的所有 ACE 组成。扩展 ACL 是最复杂且功能丰富的一类 ACL，可以用于许多功能。扩展 ACL 最显著用途是作为访问组被全局应用或应用到接口，以确定将被拒绝或允许通过设备的流量。但是，扩展 ACL 还可用于确定要向其提供其他服务的流量。

由于扩展 ACL 非常复杂，以下各节集中描述创建 ACE 以提供特定类型的流量匹配。前几节介绍关于基于地址的基本 ACE 以及 TCP/UDP ACE 的基本信息，为其余各节提供了基础。

添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配

基本的扩展 ACE 基于源地址和目标地址（包括 IPv4 和 IPv6 地址及完全限定域名 (FQDN)，如 `www.example.com`）来匹配流量。事实上，每种类型的扩展 ACE 都必须包含源地址和目标地址的一些规格，因此，本主题介绍最基本的扩展 ACE。



提示 提示：若要基于 FQDN 匹配流量，必须为每个 FQDN 创建一个网络对象。

要添加 ACE 以进行 IP 地址或 FQDN 匹配，请使用以下命令：

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
source_address_argument dest_address_argument [log [[level] [interval secs] | disable |
default]] [time-range time_range_name] [inactive]
```

示例：

```
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-list ACL_IN extended permit object service-obj-http any any
```

选项有：

- *access_list_name* - 新的或现有 ACL 的名称。
- 行号 - **line** *line_number* 选项指定插入 ACE 的行号，否则 ACE 将被添加到 ACL 的末尾。
- Permit 或 Deny - 如果条件匹配，**deny** 关键字可拒绝或排除数据包。如果条件匹配，**permit** 关键字可允许或添加数据包。
- 协议 - *protocol_argument* 指定 IP 协议。如果使用指定协议和端口的网络服务对象，则应在此参数中指定 **ip**。
 - *name* 或 *number* - 指定协议名称或编号。指定 **ip** 以应用于所有协议。
 - **object-group** *protocol_grp_id* 指定使用 **object-group protocol** 命令创建的协议对象组。
 - **object** *service_grp_id* - 指定使用命令创建的服务 **object service** 对象。如果需要，该对象可以包含端口或 ICMP 类型和代码规范。
 - **object-group** *service_grp_id* - 指定使用 **object-group service** 命令创建的服务对象组。
- Source Address、Destination Address - *source_address_argument* 指定将从其发送数据包的 IP 地址或 FQDN，*dest_address_argument* 指定将向其发送数据包的 IP 地址或 FQDN：
 - **host** *ip_address* - 指定 IPv4 主机地址。host
 - *ip_address mask* - 指定 IPv4 网络地址和子网掩码，例如 10.100.10.0 255.255.255.0。
 - *ipv6-address/prefix-length* - 指定 IPv6 主机或网络地址和前缀。
 - **any**, **any4**, **any6**—**any** 指定 IPv4 和 IPv6 流量；**any4** 仅指定 IPv4 流量；**any6** 仅指定 IPv6 流量。

- **interface** *interface_name* - 指定 ASA 接口的名称。使用接口名称（而非 IP 地址）基于接口是流量的源还是目标来匹配流量。
- **object** *nw_obj_id* - 指定使用 **object network** 命令创建的网络对象。
- **object-group** *nw_grp_id* - 指定使用 **object-group network** 命令创建的网络对象组。
- **object-group-network-service** 名称 - 指定网络服务对象的名称。
- **Logging - log** 参数设置 ACE 与网络访问连接匹配时的日志记录选项（使用 **access-group** 命令 **access-group** 应用的 ACL）。如果未在 **log** 选项中输入任何参数，则将以默认间隔（300 秒）启用默认级别 (6) 的系统日志消息 106100。日志选项是：
 - **level** - 在 0 和 7 之间的严重级别。默认值为 6（信息性）。如果为活动 ACE 更改此级别，则新级别应用于新连接；现有连接继续记录在原来的级别中。
 - **interval** *secs* - 系统日志消息之间的时间间隔，范围为 1 至 600（单位：秒）。默认值为 300。此值也用作从用于收集丢弃统计信息的缓存中删除非活动的流的超时值。
 - **disable** - 禁用所有 ACE 日志记录。
 - **default** - 为被拒绝的数据包启用消息 106023 日志记录。此设置与不包括 **log** 选项相同。
- **时间范围 - time-range** *time_range_name* 选项指定时间范围对象，可以确定 ACE 在一天中某些时间或一周中某些天处于活动状态。如果不包括时间范围，则 ACE 始终为活动状态。
- **Activation** - 使用 **inactive** 选项，在不删除 ACE 的情况下禁用 ACE。要重新启用 ACE，请输入完整的 ACE，无需含 **inactive** 关键字。

添加扩展 ACE 以执行基于端口的匹配

如果在 ACE 中指定服务对象，则服务对象可包含符合端口规范的协议，例如 TCP/80。或者，也可以直接在 ACE 中指定端口。对于基于端口的匹配，您可以将基于端口的协议的特定类型的流量作为匹配目标，而不是将该协议的所有流量作为匹配目标。



注释 如果使用指定协议和端口的网络服务对象，则不应按本主题所述指定端口。指定 **ip** 作为协议，以便可以匹配对象中定义的协议/端口。

如果协议为 **tcp**、**udp** 或 **sctp**，基于端口的扩展 ACE 只是基本的地址匹配 ACE。若要添加端口规范，请使用以下命令：

```
access-list access_list_name [ line line_number ] extended { deny | permit } { tcp | udp | sctp }
source_address_argument [ port_argument ] dest_address_argument [ port_argument ] [ log [ level ] ] [ interval
secs ] | disable | default ] [ time-range time-range-name ] [ inactive ]
```

示例：

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
```

port_argument 选项指定源端口或目标端口。如果不指定端口，则与所有端口匹配。可用参数包括：

- *operator port - port* 可以是整数或端口名称。操作符可以是以下任意一项：
 - **lt** - 小于
 - **gt** - 大于
 - **eq** - 等于
 - **neq** - 不等于
 - **range** - 值的范围（包括边界值）。使用该操作符时，请指定两个端口编号，例如，**range 100 200**。



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。

- **object-group service_grp_id** - 指定使用 **object-group service {tcp | udp | tcp-udp}** 命令创建的服务对象组。请注意，建议不要再使用这些对象类型。

无法指定建议的通用服务对象，其中协议和端口在对象内定义为端口参数。您可以将这些对象指定为协议参数的一部分，如[添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配](#)，第 34 页中所述。

有关其他关键字的说明以及如何使用服务对象指定协议和端口，请参阅[添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配](#)，第 34 页。

添加扩展 ACE 以执行基于 ICMP 的匹配

要匹配 ICMP 流量，请使用 ICMP 协议关键字之一：**icmp** 或 **icmp6**。**icmp** 协议仅匹配 IPv4 地址，而 **icmp6** 协议仅匹配 IPv6 地址。确保网络地址与所选的协议相匹配，否则 ACE 将无法匹配任何连接。

如果在 ACE 中指定服务对象，则服务对象可包含 ICMP/ICMP6 协议 ICMP 类型和代码规格。或者，也可以直接在 ACE 中指定 ICMP 类型和代码。例如，可以将 ICMP 回应请求流量 (ping) 作为目标。

ICMP 扩展 ACE 只是基本的地址匹配 ACE，其中协议为 **icmp** 或 **icmp6**。由于这些协议具有类型和代码值，可以将类型和代码规格添加到 ACE。

要添加 ACE 以进行 IP 地址或 FQDN 匹配（其中协议为 ICMP 或 ICMP6），请使用以下命令：

```
access-list access_list_name [line line_number] extended {deny | permit} {icmp | icmp6}
source_address_argument dest_address_argument [icmp_argument] [log [[level] [interval secs] | disable |
default]] [time-range time_range_name] [inactive]
```

示例：


```
hostname(config)# access-list abc extended permit icmp any any object-group obj_icmp_1
hostname(config)# access-list abc extended permit icmp any any echo
```

icmp_argument 选项指定 ICMP 类型和代码。

- *icmp_type* [*icmp_code*] - 按名称或编号指定 ICMP 类型，以及用于该类型的可选 ICMP 代码。如果不指定代码，则使用所有代码。
- **object-group** *icmp_grp_id*- 为使用（已弃用）**object-group icmp-type** 命令创建的 ICMP/ICMP6 指定对象组。

无法指定建议的通用服务对象，其中协议和端口在对象内定义为 ICMP 参数。您可以将这些对象指定为协议参数的一部分，如[添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配](#)，第 34 页中所述。

有关其他关键字的说明，请参阅[添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配](#)，第 34 页。

添加扩展 ACE 执行基于用户的匹配（身份防火墙）

基于用户的扩展 ACE 只是基本的地址匹配 ACE，可以在源匹配条件中包含用户名或用户组。通过基于用户身份创建规则，可以避免将规则与静态主机或网络地址相关联。例如，如果为 *user1* 定义规则，且身份防火墙功能将该用户映射到某一天分配 10.100.10.3 但下一天分配 192.168.1.5 的主机，则基于用户的规则将仍然适用。

由于仍必须提供源地址和目标地址，因此请扩展源地址以包含将分配给用户（通常通过 DHCP）的可能地址。例如，无论分配什么 IP 地址，用户“LOCAL\user1 any”都将匹配 LOCAL\user1 用户，而“LOCAL\user1 10.100.1.0 255.255.255.0”仅在地址处于 10.100.1.0/24 网络上时匹配该用户。

通过使用组名称，可以基于整个类别的用户（如学生、教师、管理人员、工程师等）定义规则。

要添加 ACE 以进行用户或组匹配，请使用以下命令：

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument [user_argument]
source_address_argument [port_argument] dest_address_argument [port_argument] [log [[level]]] [interval
secs] [disable | default]] [time-range time_range_name] [inactive]
```

示例：

```
hostname(config)# access-list v1 extended permit ip user LOCAL\idfw
any 10.0.0.0 255.255.255.0
```

user_argument 选项指定除源地址之外还要为其匹配流量的用户或组。可用参数包括以下各项：

- **object-group-user** *user_obj_grp_id* - 指定使用 **object-group user** 命令创建的用户对象组。
- **user** {[*domain_nickname*]*name* | **any** | **none**} - 指定用户名。指定 **any** 以将所有用户与用户凭证匹配，或指定 **none** 以匹配未映射到用户名的地址。这些选项对于将 **access-group** 与 **aaa authentication match** 策略结合特别有用。
- **user-group** [*domain_nickname*]*user_group_name* - 指定用户组名称。请注意分隔域名和组名的双斜号 \。

有关其他关键字的说明，请参阅[添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配](#)，第 34 页。



提示 可以在给定 ACE 中同时包含用户和思科 TrustSec 安全组。

添加扩展 ACE 执行基于安全组的匹配（思科 TrustSec）

安全组（思科 TrustSec）扩展 ACE 只是基本的地址匹配 ACE，可以在源或目标匹配条件中包含安全组或标签。通过基于安全组创建规则，可以避免将规则与静态主机或网络地址相关联。由于您仍必须提供源地址和目标地址，因此请扩展地址以包含将分配给用户（通常通过 DHCP）的可能地址。



提示 在添加这种类型的 ACE 之前，请配置思科 TrustSec。

要添加 ACE 以进行安全组匹配，请使用以下命令：

```
access-list access_list_name [line line_number] extended {deny | permit} protocol_argument
[security_group_argument] source_address_argument [port_argument] [security_group_argument]
dest_address_argument [port_argument] [log [[level] [interval secs] | disable | default]] [inactive | time-range
time_range_name]
```

示例：

```
hostname(config)# access-list INSIDE_IN extended permit ip
security-group name my-group any any
```

security_group_argument 选项指定除源地址或目标地址之外还要为其匹配流量的安全组。可用参数包括以下各项：

- **object-group-security** *security_obj_grp_id* - 指定使用 **object-group security** 命令创建的安全对象组。
- **security-group** {**name** *security_grp_id* | **tag** *security_grp_tag*} - 指定安全组名称或标签。

有关其他关键字的说明，请参阅[添加扩展 ACE 以执行基于 IP 地址或完全限定域名的匹配](#)，第 34 页。



提示 可以在给定 ACE 中同时包含用户和思科 TrustSec 安全组。

扩展 ACL 的示例

以下 ACL 允许所有主机（将 ACL 应用到的接口）通过 ASA：

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

以下 ACL 阻止 192.168.1.0/24 上的主机访问 209.165.201.0/27 网络以获取基于 TCP 的流量。允许所有其他地址。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

如果要仅限制对选定主机的访问，则输入一个受限制的允许 ACE。默认情况下，除非明确允许，否则拒绝所有其他流量。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

以下 ACL 限制所有主机（将 ACL 应用到的接口）访问地址为 209.165.201.29 的网站。允许所有其他流量。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

以下使用对象组的 ACL 限制内部网络中的多台主机访问多台 Web 服务器。允许所有其他流量。

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

以下示例会临时禁用允许流量从一个网络对象组 (A) 流向另一个网络对象组 (B) 的 ACL：

```
hostname(config)# access-list 104 permit ip host object-group A object-group B inactive
```

要实施基于时间的 ACE，请使用 **time-range** 命令来定义一周和一天中的特定时间。然后，使用 **access-list extended** 命令将该时间范围绑定到 ACE。以下示例将 “Sales” ACL 中的 ACE 绑定到名为 “New_York_Minute” 的时间范围。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
```

以下示例显示同时包含 IPv4 和 IPv6 的 ACL：

```
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 10.2.2.0
255.255.255.0
hostname(config)# access-list demoacl extended permit ip 2001:DB8:1::/64 2001:DB8:2::/64
hostname(config)# access-list demoacl extended permit ip host 10.3.3.3 host 10.4.4.4
```

将地址转换为扩展 ACL 对象的示例

以下未使用对象组的正常 ACL 限制内部网络上的多台主机访问若干 Web 服务器。允许所有其他流量。

```

hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.29
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.16
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.4 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.78 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended deny tcp host 10.1.1.89 host 209.165.201.78
eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside

```

如果创建两个网络对象组，一个用于内部主机，另一个用于 Web 服务器，则可以简化并轻松地修改配置来添加更多主机：

```

hostname(config)# object-group network denied
hostname(config-network)# network-object host 10.1.1.4
hostname(config-network)# network-object host 10.1.1.78
hostname(config-network)# network-object host 10.1.1.89

hostname(config-network)# object-group network web
hostname(config-network)# network-object host 209.165.201.29
hostname(config-network)# network-object host 209.165.201.16
hostname(config-network)# network-object host 209.165.201.78

hostname(config)# access-list ACL_IN extended deny tcp object-group denied object-group
web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside

```

配置标准 ACL

标准 ACL 由具有相同 ACL ID 或名称的所有 ACE 组成。标准 ACL 用于有限数量的功能，例如路由映射或 VPN 过滤器。标准 ACL 仅使用 IPv4 地址，并且仅定义目标地址。

要添加标准访问列表条目，请使用以下命令：

access-list *access_list_name* standard {deny | permit} {any4 | host *ip_address* | *ip_address mask*}

示例：

```
hostname(config)# access-list OSPF standard permit 192.168.1.0 255.255.255.0
```

选项有：

- 名称 - *access_list_name* 参数指定 ACL 的编号名称。标准 ACL 的传统编号是 1 - 99 或 1300 - 1999，但可以使用任意名称或编号。如果 ACL 不存在，则创建新的 ACL，否则，将条目添加到 ACL 末尾。
- Permit 或 Deny - 如果条件匹配，**deny** 关键字可拒绝或排除数据包。如果条件匹配，**permit** 关键字可允许或添加数据包。
- 目的地址 - **any4** 关键字与所有 IPv4 地址匹配。**host ip_address** 参数与主机 IPv4 地址匹配。**ip_address ip_mask** 参数与 IPv4 子网匹配，例如 10.1.1.0 255.255.255.0。

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 由具有相同 ACL ID 或名称的所有 ACE 组成。

通过 Webtype ACL，可以基于 URL 或目标地址来匹配流量。单个 ACE 不能混用这些规格。以下各节介绍每种类型的 ACE。

添加 Webtype ACE 以执行 URL 匹配

要基于用户正尝试访问的 URL 匹配流量，请使用以下命令：

```
access-list access_list_name webtype {deny | permit} url {url_string | any} [log [[level] [interval secs] | disable | default]] [time_range time_range_name] [inactive]
```

示例：

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

选项有：

- *access_list_name* - 新的或现有 ACL 的名称。如果 ACL 已经存在，则 ACE 将添加到 ACL 末尾。
- Permit 或 Deny - 如果条件匹配，**deny** 关键字可拒绝或排除数据包。如果条件匹配，**permit** 关键字可允许或添加数据包。
- URL - 关键字 **url** 指定要匹配的 URL。使用 **url any** 与所有基于 URL 的流量匹配。否则，请输入 URL 字符串，它可以包括通配符。以下是指定 URL 时的一些提示和限制：
 - 指定 **any** 将匹配所有 URL。
 - “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]/`。
- **Logging - log** 参数可设置当 ACE 匹配数据包时的日志记录选项。如果未在 **log** 选项中输入任何参数，则将以默认间隔（300 秒）启用默认级别 (6) 的系统日志消息 106102。日志选项是：
 - **level** - 在 0 和 7 之间的严重级别。默认值为 6。
 - **interval secs** - 各系统日志消息之间的时间间隔（以秒为单位），从 1 到 600。默认值为 300。
 - **disable** - 禁用所有 ACL 日志记录。
 - **default** - 对消息 106103 启用日志记录。此设置与不包括 **log** 选项相同。
- **Time Range - time-range time_range_name** 选项指定时间范围对象，可以确定 ACE 在一天中某些时间或一周中某些天处于活动状态。如果不包括时间范围，则 ACE 始终为活动状态。
- **Activation** - 使用 **inactive** 选项，在不删除 ACE 的情况下禁用 ACE。要重新启用 ACE，请输入完整的 ACE，无需含 **inactive** 关键字。

添加 Webtype ACE 以执行 IP 地址匹配

可以基于用户正尝试访问的目标地址来匹配流量。除了 URL 规格之外，Webtype ACL 可以同时包含 IPv4 和 IPv6 地址。

要添加 Webtype ACE 以进行 IP 地址匹配，请使用以下命令：

```
access-list access_list_name webtype {deny | permit} tcp dest_address_argument [operator port] [log  
[[level] [interval secs] | disable | default]] [time_range time_range_name]] [inactive]]
```

示例：

```
hostname(config)# access-list acl_company webtype permit tcp any
```

有关此处未说明的关键字的说明，请参阅[添加 Webtype ACE 以执行 URL 匹配，第 41 页](#)。此类型 ACE 的特定关键字和参数包括以下各项：

- **tcp** - TCP 协议。Webtype ACL 仅匹配 TCP 流量。
- **Destination Address - dest_address_argument** 指定将向其发送数据包的 IP 地址。

- **host ip_address** - 指定 IPv4 主机地址。
- **dest_ip_address mask** - 指定 IPv4 网络地址和子网掩码，例如 10.100.10.0 255.255.255.0。
- **ipv6-address/prefix-length** - 指定 IPv6 主机或网络地址和前缀。
- **any**、**any4** 和 **any6** - **any** 指定 IPv4 和 IPv6 流量；**any4** 仅指定 IPv4 流量；**any6** 仅指定 IPv6 流量。
- **operator port** - 目标端口。如果不指定端口，则与所有端口匹配。**port** 可以是表示 TCP 端口号的整数或端口名称。**operator** 可以是以下任意一项：
 - **lt** - 小于
 - **gt** - 大于
 - **eq** - 等于
 - **neq** - 不等于
 - **range** - 值的范围（包括边界值）。使用该操作符时，请指定两个端口编号，例如，**range 100 200**。

Webtype ACL 的示例

以下示例展示如何拒绝对特定公司 URL 的访问：

```
hostname(config)# access-list acl_company webtype deny url http://*.example.com
```

以下示例显示如何拒绝对特定网页的访问：

```
hostname(config)# access-list acl_file webtype deny url https://www.example.com/dir/file.html
```

以下示例显示如何拒绝通过端口 8080 对特定服务器上任何 URL 的 HTTP 访问：

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

以下示例显示如何在 webtype ACL 中使用通配符。

- 以下示例匹配 `http://www.example.com/layouts/1033` 等 URL：

```
access-list VPN-Group webtype permit url http://www.example.com/*
```

- 以下示例匹配 `http://www.example.com/` 和 `http://www.example.net/` 等 URL：

```
access-list test webtype permit url http://www.example.*
```

- 以下示例匹配 `http://www.example.com` 和 `ftp://wwz.example.com` 等 URL：

```
access-list test webtype permit url *://ww?.e*co*/
```

- 以下示例匹配 `http://www.cisco.com:80` 和 `https://www.cisco.com:81` 等 URL：

```
access-list test webtype permit url *://ww?.c*co*:8[01]/
```

上一个示例中的范围操作符 “[]” 指定在该位置可能出现 **0** 或 **1**。

- 以下示例匹配 `http://www.example.com` 和 `http://www.example.net` 等 URL：

```
access-list test webtype permit url http://www.[a-z]xample?*/
```

上一个示例中的范围操作符 “[]” 指定该范围（从 **a** 到 **z**）内的任何字符都可能出现。

- 以下示例匹配文件名或路径中包含 “**cgi**” 的 `http` 或 `https` URL。

```
access-list test webtype permit url htt*:///*/*cgi?*
```



注释 要匹配任意 `http` URL，必须输入 **`http:///*/*`**，而非 `http://*`。

以下示例显示如何强制 Webtype ACL 禁用对特定 CIFS 共享的访问。

在此场景中，我们有一个包含名为 “**Marketing_Reports**” 和 “**Sales_Reports**” 的两个子文件夹的 “**shares**” 根文件夹。我们希望明确拒绝访问 “**shares/Marketing_Reports**” 文件夹。

```
access-list CIFS_Avoid webtype deny url cifs://172.16.10.40/shares/Marketing_Reports.
```

但是，由于 ACL 末尾的隐式 “**deny all**”，上述 ACL 使所有子文件夹 变得都不可访问（“**shares/Sales_Reports**” 和 “**shares/Marketing_Reports**”），包括根文件夹（“**shares**”）。

要解决此问题，请添加一个新的 ACL 来 允许访问根文件夹和其余的子文件夹：

```
access-list CIFS_Allow webtype permit url cifs://172.16.10.40/shares*
```

配置 EtherType ACL

EtherType ACL 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。使用 EtherType ACL，可以控制非 IP 流量跨桥接组的流动。请注意，802.3 格式的帧不是由 ACL 处理，因为这些帧使用的是长度字段，而非类型字段。

要添加 EtherType ACE，请使用以下命令：

```
access-list access_list_name ethertype {deny | permit} {any | bpdu | dsap {hex_address | bpdu | ipx | isis | raw-ipx} | eii-ipx | ipx | isis | mpls-multicast | mpls-unicast | hex_number}
```


示例：

```
hostname(config)# access-list ETHER ethertype deny mpls-multicast
```

选项有：

- **access_list_name** - 新的或现有 ACL 的名称。如果 ACL 已经存在，则 ACE 将添加到 ACL 末尾。
- **Permit 或 Deny** - 如果条件匹配，**deny** 关键字可拒绝数据包。如果条件匹配，**permit** 关键字可允许数据包。
- **Traffic Matching Criteria** - 可以使用以下选项匹配流量：
 - **any** - 匹配所有第 2 层流量。
 - **bpdu** - 默认允许的桥接协议数据单元 (dsap 0x42)。此关键字将转换为 **dsap bpdu**。
 - **dsap {hex_address | bpdu | ipx | isis | raw-ipx}** - IEEE 802.2 逻辑链路控制 (LLC) 数据包的目的服务无线接入点地址。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。也可以使用以下关键字来为通用值创建规则：
 - **bpdu** 对于 0x42，桥接协议数据单元。
 - **ipx** 对于 0xe0，互联网数据包交换 (IPX) 802.2 LLC。
 - **isis** 对于 0xfe，中间系统到中间系统 (IS-IS)。
 - **raw-ipx** 对于 0xff，原始 IPX 802.3 格式。
 - **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。
 - **isis** - 中间系统到中间系统 (IS-IS)。此关键字将转换为 **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。

EtherType ACL 的示例

以下示例显示如何配置 EtherType ACL，包括如何将 ACL 应用到接口。

例如，以下示例 ACL 允许源自内部接口的常见 EtherType 流量：

```
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
```

```
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

以下示例通过 ASA 允许一些 EtherType，但会拒绝所有其他 EtherType：

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

以下示例将拒绝 EtherType 0x1256 的流量，但允许两个接口上的所有其他流量：

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

在隔离配置会话中编辑 ACL

在编辑用于访问规则或任何其他用途的 ACL 时，更改会立即实施并影响流量。通过访问规则，可以启用事务性提交模型，以确保新规则仅在规则编译完成后变为活动状态，但编译发生在编辑的每个 ACE 之后。

如果想进一步隔离编辑 ACL 的影响，可在“configuration session”中进行更改，这是一种独立模式，在该模式下允许在明确提交更改前编辑多个 ACE 和对象，这样可确保更改设备行为前完成预期的所有更改。

开始之前

- 可以编辑由 access-group 命令引用的 ACL，但无法编辑由任何其他命令引用的 ACL。也可以编辑未引用的 ACL 或创建新的 ACL。
- 可以创建或编辑对象和对象组，但如果在会话中创建一个对象或对象组，则无法在同一会话中进行编辑。如果对象未按预期方式定义，则必须提交更改，然后编辑对象，或丢弃整个会话并重新开始。
- 编辑由 access-group 命令（访问规则）引用的 ACL 时，在提交会话时使用事务性提交模型。因此，ACL 将在新的 ACL 替换旧版本之前被完全编译。

过程

步骤 1 启动会话。

```
hostname#configure session session_name
hostname(config-s)#
```

如果 `session_name` 已存在，将打开该会话。否则，将创建一个新的会话。

使用 **show configuration session** 命令查看现有会话。一次最多可让 3 个会话处于活动状态。如果需要删除旧的未使用的会话，请使用 **clear configuration session session_name** 命令。

如果因为现有会话正在别处进行编辑而无法打开，则可以清除指示会话正在进行编辑的标记。该操作仅在确定会话实际上并未进行编辑时执行。使用 **clear session session_name access** 命令重置标记。

步骤 2（仅限未提交的会话。）进行更改。可以将以下基本命令与其任一参数配合使用：

- **access-list**
- **object**
- **object-group**

步骤 3 决定如何处理会话。可用的命令取决于之前是否已提交会话。可能的命令如下：

- **exit** - 简单地退出会话而不提交或放弃更改，以便稍后返回。
- **commit [noconfirm [revert-save | config-save]]** -（仅限未提交的会话。）可提交更改。系统将询问您是否要保存会话。可以保存复原会话 (**revert-save**)，其可以让您使用 **revert** 命令撤消更改，或者可以保存配置会话 (**config-save**)，其包括在会话中所做的所有更改（允许您根据需要重新提交相同的更改）。如果保存复原或配置会话，将提交更改，但会话保持活动状态。可以打开会话，复原或重新提交更改。可以通过选中 **noconfirm** 选项（也可同时选中所需的保存选项）避免提示。
- **abort** -（仅限未提交的会话。）可放弃更改并删除会话。如果要保持会话，请退出会话并使用 **clear session session_name configuration** 命令，该命令清空会话而不删除会话。
- **revert** -（仅限已提交的会话。）取消所做更改，将配置返回到提交会话前的状态并删除会话。
- **show configuration session [session_name]** - 可显示会话中所做的更改。

监控 ACL

要监控 ACL，请输入以下其中一个命令：

- **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 的历史记录

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。 引入了以下命令：access-list extended、access-list standard、access-list webtype 和 access-list ethertype。
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。 修改了以下命令：access-list extended。
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。 修改了以下命令：access-list ethertype {permit deny} isis。
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。 修改了以下命令：access-list extended。
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。 修改了以下命令：access-list extended、access-list webtype。 删除了以下命令：ipv6 access-list、ipv6 access-list webtype 和 ipv6-vpn-filter。
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。 引入或修改了以下命令：access-list extended、service-object、service。

功能名称	版本	说明
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。 引入了 clear configuration session 、 clear session 、 configure session 、 forward-reference 和 show configuration session 命令。
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。 修改了以下命令： access-list extended 。
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。 修改了以下命令： access-list ethertype
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)	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。 修改了以下命令： access-group 、 access-list ethertype 。
EtherType 访问控制列表更改。	9.9(1)	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。 修改了以下命令： access-list ethertype 添加了新的关键字 eii-ipx 和 dsap {bpdu ipx isis raw-ipx} ； capture ethernet-type 不再支持关键字 ipx 。
支持扩展 ACL 中的网络服务对象。	9.17(1)	您可以在扩展 ACL 和访问控制规则中使用网络服务对象作为源和目标条件。 我们更改了以下命令： access-list extended 。

功能名称	版本	说明
始终启用 ACL 和对象的转发引用。此外，默认情况下，为访问控制启用对象组搜索。	9.18(1)	在配置访问组或访问规则时，可以引用尚不存在的 ACL 或网络对象。 此外，默认情况下，为 新 部署的访问控制启用对象组搜索。升级设备将继续禁用此命令。如果要启用它（推荐），必须手动执行此操作。 我们删除了 forward-reference enable 命令，并将 object-group-search access-control 的默认设置更改为启用。



第 4 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 51 页](#)
- [面向访问规则的许可，第 57 页](#)
- [访问控制准则，第 57 页](#)
- [配置访问控制，第 58 页](#)
- [监控访问规则，第 61 页](#)
- [允许或拒绝网络访问的配置示例，第 62 页](#)
- [访问规则的历史记录，第 64 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：

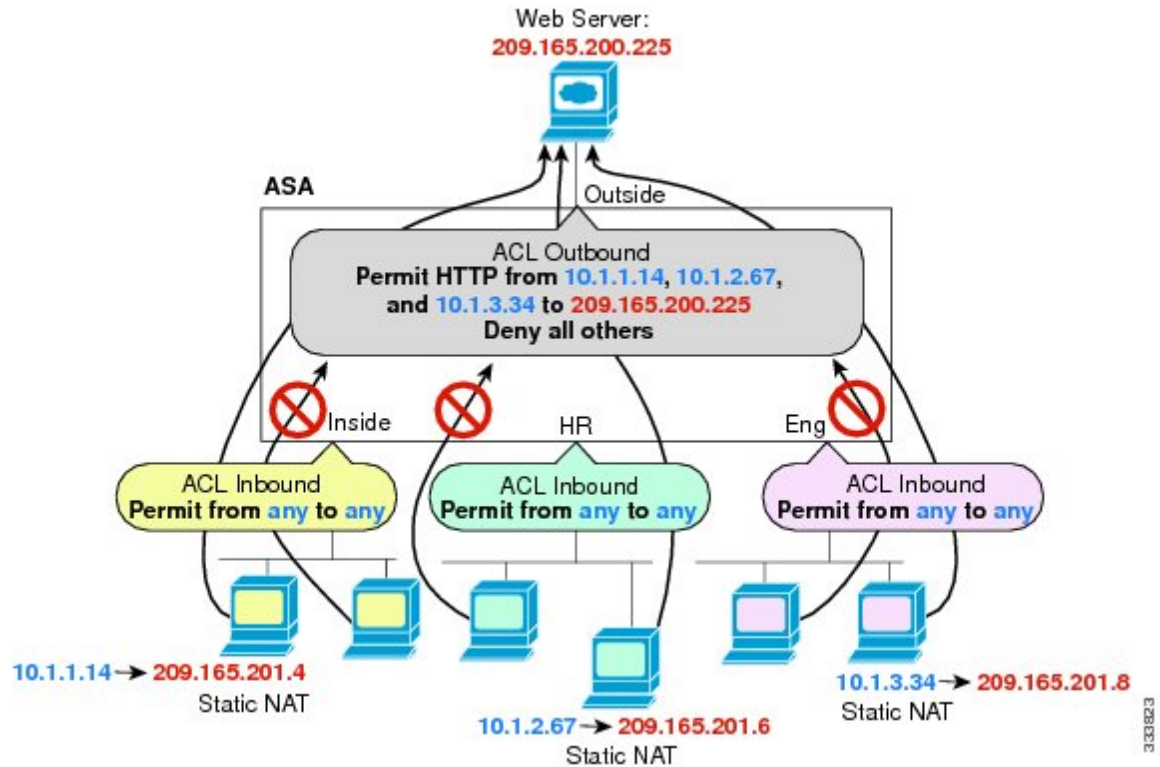
- 入站 - 入站访问规则在流量进入接口时应用于流量。全局访问规则和管理访问规则始终为入站规则。
- 出站 - 出站规则在流量离开接口时应用于流量。



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



请见以下适用于本示例的命令：

```
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.1.14 host 209.165.200.225
eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.2.67 host 209.165.200.225
eq www
hostname(config)# access-list OUTSIDE extended permit tcp host 10.1.3.34 host 209.165.200.225
eq www
hostname(config)# access-group OUTSIDE out interface outside
```

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 BPDUs 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 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)。

相同安全级别的接口和访问规则

每个接口都有一个安全级别，在考虑访问规则之前要进行安全级别检查。因此，即使您在访问规则中允许某个连接，它也可能因接口级的同一安全级别检查而被阻止。您可能需要确保您的配置允许相同安全级别的连接，以便在做出允许/拒绝决定时始终考虑您的访问规则。

- 相同安全级别的入口和出口接口之间的连接要接受相同安全流量接口间检查。

要允许这些连接，请输入 **same-security-traffic permit inter-interface** 命令。

要允许这些连接，依次选择配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces)，然后选择启用两个或多个配置了相同安全级别的接口之间的流量

(Enable traffic between two or more interfaces which are configured with the same security levels) 选项。

- 具有相同入口和出口接口的连接要接受相同安全流量的接口间检查。

要允许这些连接，请输入 **same-security-traffic permit intra-interface** 命令。

要允许这些连接，依次选择配置 (Configuration) > 设备设置 (Device Setup) > 接口设置 (Interface Settings) > 接口 (Interfaces)，然后选择启用连接到同一接口的两台或多台主机之间的流量 (**Enable traffic between two or more hosts connected to the same interface**) 选项。

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 2: 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	—

流量类型	协议或端口	说明
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（由 **http**、**ssh** 或 **telnet** 等命令定义）的优先级高于使用 **control-plane** 选项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。

访问控制准则

IPv6 准则

支持 IPv6。源和目标地址可能包括 IPv4 和 IPv6 地址的任意混合。

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

- 随着时间的推移，访问规则列表可能会增长到包含许多过时的规则。最终，访问组的 ACL 可能会非常大，以至于影响整体系统性能。如果您发现系统在发送系统日志消息、进行故障转移同步通信、建立和维护 SSH/HTTPS 管理访问连接等方面遇到问题，可能需要修剪访问规则。通常，您应主动维护规则列表，以删除过时的规则、永远不会命中的规则、无法再解析的 FQDN 对象等。另请考虑实施对象组搜索。
- 新部署默认启用对象组搜索。

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。可以使用 **object-group-search access-control** 命令设置此选项。

可以使用 **object-group-search threshold** 命令启用阈值，以有助于防止性能下降。使用阈值运行时，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。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。但是，如果使用 FQDN 对象来处理解析经常变化的主机名，则不建议使用事务提交，因为访问组编译可能永远无法完全解析。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。使用 **asp rule-engine transactional-commit access-group** 命令。
- 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。
- 要将完全限定域名 (FQDN) 网络对象用作源或目标条件，您还必须配置适用于数据接口的 DNS。

请注意，通过 FQDN 控制访问是尽力而为机制。考虑以下几点：

- 由于 DNS 回复可能具有欺骗性，因此只能使用完全受信任的内部 DNS 服务器。
- 有些 FQDN，特别是非常受欢迎的服务器，可能有成百上千个 IP 地址，而且这些地址经常都会变化。由于系统使用的是缓存的 DNS 查询结果，用户可能会获得尚未在缓存中的地址，因此他们的连接将与 FQDN 规则不匹配。使用 FQDN 网络对象的规则只对解析为 100 个以内地址的名称有效。

建议您不要为解析为超过 100 个地址的 FQDN 创建网络对象规则，因为连接中的地址是设备 DNS 缓存中已解析和可用地址的可能性很低。

- 对于受欢迎的 FQDN，不同的 DNS 服务器可以返回一组不同的 IP 地址。因此，如果您的用户使用的 DNS 服务器与您所配置的不同，基于 FQDN 的访问控制规则可能不适用于客户端对于该站点使用的所有 IP 地址，而您的规则也不会实现预期结果。
- 一些 FQDN DNS 条目的生存时间 (TTL) 值非常小。这会导致查询表频繁地进行重新编译，从而可能会影响总体系统性能。

配置访问控制

以下主题解释如何配置访问控制。

配置访问组

应先创建 ACL，然后才能创建访问组。

要将 ACL 绑定至接口，或将其全局应用，请使用以下命令：

```
access-group access_list { {in | out} interface interface_name [per-user-override | control-plane] | global}
```

对接口特定的访问组：

- 指定扩展或 EtherType ACL 名称。可为每个 ACL 类型、每个接口、每个方向配置一个 **access-group** 命令，并配置一个控制平面 ACL。控制平面 ACL 必须是扩展 ACL。EtherType ACL 仅可用于网桥组成员接口。对于路由模式下的网桥组，可为网桥虚拟接口 (BVI) 和每个网桥组成员接口上的每个方向指定扩展 ACL。
- **in** 关键字会将 ACL 应用于入站流量。**out** 关键字会将 ACL 应用于出站流量。
- 指定 **interface** 名称。
- **Per-user-override** 关键字（仅适用于入站扩展 ACL）允许为用户授权下载的动态用户 ACL 覆盖分配给该接口的 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。

默认情况下，将不针对接口 ACL 匹配 VPN 远程访问流量。但是，如果使用 **no sysopt connection permit-vpn** 命令关闭此旁路，则该行为取决于是否存在应用于组策略的 **vpn-filter**，以及是否设置 **per-user-override** 选项：

- **No per-user-override, no vpn-filter** - 针对接口 ACL 匹配流量。
- **No per-user-override, vpn-filter** - 依次针对接口 ACL 和 VPN 过滤器匹配流量。
- **per-user-override、vpn-filter** - 仅针对 VPN 过滤器匹配流量。
- **control-plane** 关键字指定扩展 ACL 是否适用于传入流量。

与正则访问规则不同，接口的管理（控制平面）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。

对于全局访问组，指定 **global** 关键字，以将扩展 ACL 应用于所有接口的入站方向流量。

示例

以下示例展示如何使用 **access-group** 命令：

```
hostname(config)# access-list outside_access permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group outside_access in interface outside
```

access-list 命令允许任何主机使用端口 80 访问主机地址。**access-group** 命令指定 **access-list** 命令适用于传入外部接口的流量。

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 创建适用于 ICMP 流量的规则。

icmp {permit | deny} {host ip_address | ip_address mask | any} [icmp_type] interface_name

如果未指定 *icmp_type*，该规则将适用于所有类型。可输入编号或名称。要控制 ping 操作，请指定 echo-reply (0) (ASA-to-host) 或 echo (8) (host-to-ASA)。

对于地址，可将规则应用于 **any** 地址、单个 **host** 或某个网络 (*ip_address mask*)。

步骤 2 创建适用于 ICMPv6 (IPv6) 流量的规则。

ipv6 icmp {permit | deny} {host ipv6_address | ipv6-network/prefix-length | any} [icmp_type] interface_name

如果未指定 *icmp_type*，该规则将适用于所有类型。

对于地址，可将规则应用于 **any** 地址、单个 **host** 或某个网络 (*ipv6-network/prefix-length*)。

步骤 3 （可选。）设置对 ICMP Unreachable 消息的速率限制，以便 ASA 显示在跟踪路由输出中。

icmp unreachable rate-limit rate burst-size size

速率限制可为 1-100，1 为默认值。突发大小可以是 1-10。发送的回复数量为突发大小，但在达到速率限制之前不会发送后续回复。

示例：

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 **set connection decrement-ttl** 命令。例如，以下策略可增加速率限制并减小通过 ASA 的所有流量的生存时间 (TTL) 值。

```
icmp unreachable rate-limit 50 burst-size 10
class-map global-class
  match any
policy-map global_policy
  class global-class
```



```
set connection decrement-ttl
```

示例

以下示例展示，如何允许除处于 10.1.1.15 的主机之外的所有主机使用 ICMP 流量侦测内部接口：

```
hostname(config)# icmp deny host 10.1.1.15 inside  
hostname(config)# icmp permit any inside
```

以下示例显示如何允许地址为 10.1.1.15 的主机仅使用 ping 连接内部接口：

```
hostname(config)# icmp permit host 10.1.1.15 inside
```

以下示例显示如何在外部接口上拒绝所有 ping 请求并允许所有数据包太大的消息（以支持路径 MTU 发现）：

```
hostname(config)# ipv6 icmp deny any echo-reply outside  
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

以下示例显示如何允许主机 2000:0:0:4::2 或前缀 2001::/64 的主机使用 ping 连接外部接口：

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside  
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside  
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

监控访问规则

要监控网络访问，请输入以下命令：

- **clear access-list id counters**

清除访问列表的命中计数。

- **show access-list [name]**

显示访问列表，包括每个 ACE 的行号和命中次数。纳入 ACL 名称，否则将看到所有访问列表。

- **show running-config access-group**

显示与接口绑定的当前 ACL。

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。

当您为消息 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

当您为消息 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。可使用 **access-list alert-interval secs** 命令控制发出此消息的频率，并使用 **access-list deny-flow-max number** 命令控制缓存的拒绝流的最大数量。

允许或拒绝网络访问的配置示例

以下是一些允许或拒绝网络访问的典型配置示例。

扩展 ACL 示例

以下示例为内部服务器 1 添加网络对象，为服务器执行静态 NAT 以及为内部服务器 1 启用来自外部的访问。

```
hostname(config)# object network inside-server1
hostname(config)# host 10.1.1.1
hostname(config)# nat (inside,outside) static 209.165.201.12
```

```
hostname(config)# access-list outside_access extended permit tcp any object inside-server1
eq www
hostname(config)# access-group outside_access in interface outside
```

以下示例允许所有主机在 **inside** 和 **hr** 网络之间进行通信，但仅允许特定主机访问外部网络：

```
hostname(config)# access-list ANY extended permit ip any any
hostname(config)# access-list OUT extended permit ip host 209.168.200.3 any
hostname(config)# access-list OUT extended permit ip host 209.168.200.4 any

hostname(config)# access-group ANY in interface inside
hostname(config)# access-group ANY in interface hr
hostname(config)# access-group OUT out interface outside
```

以下示例使用对象组来允许内部接口上的特定流量：

```
!
hostname (config)# object-group service myaclog
hostname (config-service)# service-object tcp source range 2000 3000
hostname (config-service)# service-object tcp source range 3000 3010 destination$
hostname (config-service)# service-object ipsec
hostname (config-service)# service-object udp destination range 1002 1006
hostname (config-service)# service-object icmp echo

hostname(config)# access-list outsideacl extended permit object-group myaclog interface
inside any
```

EtherType 示例

例如，以下示例 ACL 允许源自内部接口的常见 EtherType 流量：

```
hostname(config)# access-list ETHER ethertype permit ipx
INFO: ethertype ipx is saved to config as ethertype eii-ipx
INFO: ethertype ipx is saved to config as ethertype dsap ipx
INFO: ethertype ipx is saved to config as ethertype dsap raw-ipx
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

以下示例通过 ASA 允许一些 EtherType，但会拒绝所有其他 EtherType：

```
hostname(config)# access-list ETHER ethertype permit 0x1234
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
hostname(config)# access-group ETHER in interface outside
```

以下示例将拒绝 EtherType 0x1256 的流量，但允许两个接口上的所有其他流量：

```
hostname(config)# access-list nonIP ethertype deny 1256
hostname(config)# access-list nonIP ethertype permit any
hostname(config)# access-group nonIP in interface inside
hostname(config)# access-group nonIP in interface outside
```

访问规则的历史记录

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。 引入了以下命令： access-group 。
全局访问规则	8.3(1)	引入了全局访问规则。 修改了以下命令： access-group 。
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。 修改了以下命令： access-list extended 。
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。 修改了以下命令： access-list ethertype {permit deny} isis 。
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。 修改了以下命令： access-list extended 。
适用于 IPv4 和 IPv6 的统一 ACL	9.0(1)	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。 修改了以下命令： access-list extended 、 access-list webtype 。 删除了以下命令： ipv6 access-list 、 ipv6 access-list webtype 、 ipv6-vpn-filter
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。 引入或修改了以下命令： access-list extended 、 service-object 、 service 。
基于访问组规则引擎的事务提交模型	9.1(5)	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。 引入了以下命令： asp rule-engine transactional-commit 、 show running-config asp rule-engine transactional-commit 、 clear configure asp rule-engine transactional-commit 。

功能名称	平台版本	说明
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。 引入了 clear config-session 、 clear session 、 configure session 、 forward-reference 和 show config-session 命令。
流控制传输协议 (SCTP) 的访问规则支持	9.5(2)	现在，您可以使用 sctp 协议（包括端口规范）创建访问规则。 修改了以下命令： access-list extended 。
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。 修改了以下命令： access-list ethertype
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)	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。 修改了以下命令： access-group 、 access-list ethertype 。
EtherType 访问控制列表更改。	9.9(1)	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。 修改了以下命令： access-list ethertype 添加了新的关键字 eii-ipx 和 dsap {bpdu ipx isis raw-ipx} ； capture ethernet-type 不再支持关键字 ipx 。
现在，对象组搜索阈值将默认禁用。	9.12(1)	在以前，如果您启用对象组搜索功能，此功能将受阈值限制，这是为了防止性能出现下降。该阈值现在默认将被禁用。您可以使用 object-group-search threshold 命令启用该阈值。 添加了以下命令： object-group-search threshold 。

功能名称	平台版本	说明
始终启用 ACL 和对象的转发引用。此外，默认情况下，为访问控制启用对象组搜索。	9.18(1)	在配置访问组或访问规则时，可以引用尚不存在的 ACL 或网络对象。 此外，默认情况下，为 新 部署的访问控制启用对象组搜索。升级设备将继续禁用此命令。如果要启用它（推荐），必须手动执行此操作。 我们删除了 forward-reference enable 命令，并将 object-group-search access-control 的默认设置更改为启用。
对象组搜索优化。	9.22(1)	对象组搜索功能得到了增强，可在评估访问控制规则以匹配连接时减少对象查找时间，并减少 CPU 开销。配置对象组搜索没有任何变化，优化行为会自动进行。 我们在设备 CLI 或增强的命令输出中添加了以下命令：clear asp table network-object、debug ac logs、packet-tracer、show access-list、show asp table network-group、show object-group。



第 5 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 67 页](#)
- [思科 TrustSec 准则，第 74 页](#)
- [将 ASA 配置为与思科 TrustSec 集成，第 77 页](#)
- [思科 TrustSec 示例，第 90 页](#)
- [Secure Client VPN 支持思科 TrustSec，第 90 页](#)
- [监控 Cisco TrustSec，第 92 页](#)
- [思科 TrustSec 的历史记录，第 93 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保护的安全要求也显著提高。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：
 - 面向企业的 Cisco TrustSec 系统和架构的说明。
<http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html>
 - 有关在企业中部署 Cisco TrustSec 解决方案的说明，包含组件设计指南的链接。
http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-security/landing_DesignZone_TrustSec.html
 - 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/collateral/enterprise-networks/trustsec/solution_overview_c22-591771.pdf
 - 思科 TrustSec 平台支持矩阵，其中列出支持 Cisco TrustSec 解决方案的思科产品。
http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html

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 TCP 64999 端口启动连接。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、DACL 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。

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

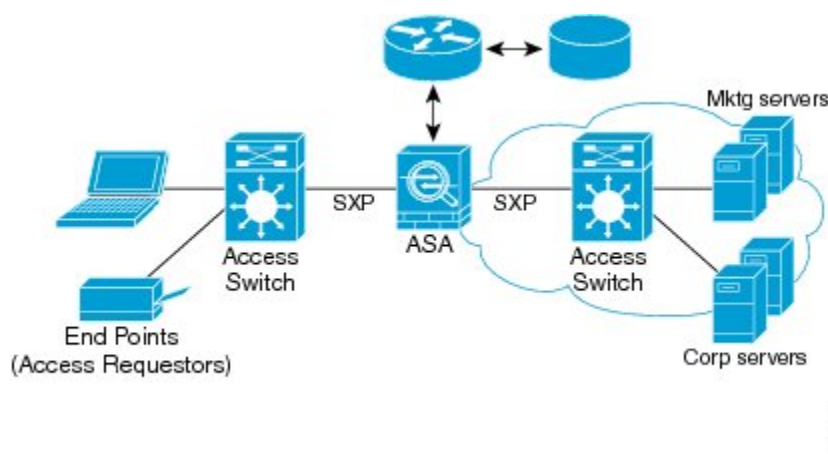
安全策略实施基于安全组名称进行。终端设备尝试访问数据中心中的资源。与在防火墙上配置的基于 IP 的传统策略相比，基于身份的策略基于用户和设备身份配置。例如，允许市场营销承包商访问市场营销服务器；允许市场营销公司用户访问市场营销服务器和公司服务器。

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 3: 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。

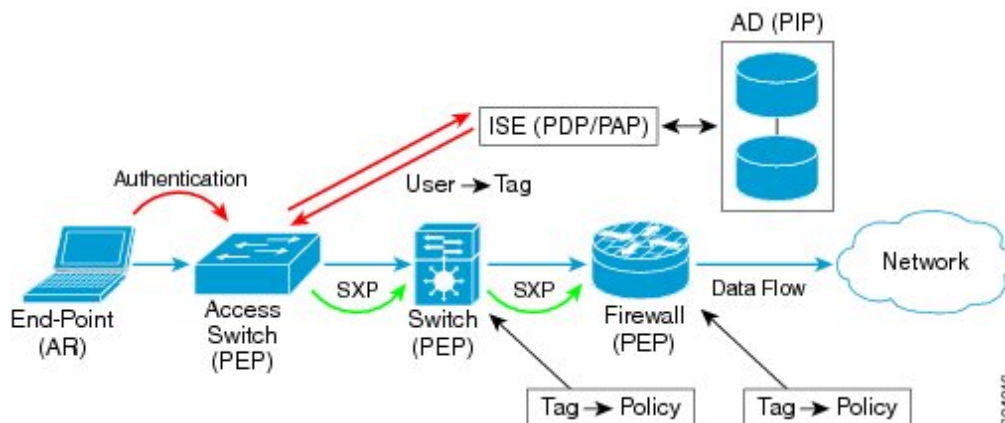
要将 ASA 配置为与思科 TrustSec 协同运行，必须从 ISE 导入受保护的访问凭证 (PAC) 文件。

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 4: 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 准则

本节包括在配置思科 TrustSec 之前应查看的准则和限制。

故障转移

- 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。
- 如果故障转移配置中涉及 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

- 如果故障转移配置中涉及 ASA，则必须将 PAC 文件导入控制单元。
- 如果故障转移配置中涉及 ASA，则必须刷新控制单元上的环境数据。

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、子接口、和 EtherChannel 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。
- 不支持故障转移链路。
- 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。
- Firepower 1010 交换机端口和 VLAN 接口不支持第 2 层安全组标记实施。

其他准则

- 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。
- 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 73 页](#)
- [在 ISE 上创建安全组，第 73 页](#)
- [生成 PAC 文件，第 74 页](#)

过程

步骤 1 [配置 AAA 服务器以便与思科 TrustSec 集成，第 77 页](#)

步骤 2 [导入 PAC 文件，第 79 页](#)

步骤 3 [配置安全交换协议，第 80 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 83 页](#)

步骤 5 [刷新环境数据，第 84 页](#)

请根据需要执行任务。

步骤 6 [配置安全策略，第 84 页](#)

步骤 7 [配置第 2 层安全组标记实施，第 86 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 为 ASA 创建 AAA 服务器组并配置 AAA 服务器参数，以便与 ISE 服务器通信。

aaa-server server-tag protocol radius

示例：

```
ciscoasa(config)# aaa-server ISEserver protocol radius
```

server-tag 参数指定服务器组名称。

步骤 2 从 aaa 服务器组配置模式中退出。

exit

示例：

```
ciscoasa(config-aaa-server-group)# exit
```

步骤 3 将 AAA 服务器配置为 AAA 服务器组的一部分，设置主机特定连接数据。

```
ciscoasa(config)# aaa-server server-tag(interface-name) host server-ip
```

示例：

```
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
```

interface-name 参数指定 ISE 所驻留的网络接口。需要在此参数中使用圆括号。*server-tag* 参数是 AAA 服务器组的名称。*server-ip* 参数指定 ISE 服务器的 IP 地址。

步骤 4 指定向 ISE 服务器验证 ASA 的服务器密钥值。

key key

示例：

```
ciscoasa(config-aaa-server-host)# key myexclusivekey
```

key 参数为字母数字关键字，最长为 127 个字符。

如果也使用 ISE 进行用户验证，请输入将 ASA 注册到 ISE 时在 ISE 上输入的共享密钥。

步骤 5 从 AAA 服务器主机配置模式中退出。

exit

示例:

```
ciscoasa(config-aaa-server-host)# exit
```

步骤 6 标识被 Cisco TrustSec 用于环境数据检索的 AAA 服务器组。

```
cts server-group AAA-server-group-name
```

示例:

```
ciscoasa(config)# cts server-group ISEserver
```

AAA-server-group-name 参数为您在步骤 1 中在 *server-tag* 参数中指定的 AAA 服务器组的名称。

注释

您可以在 ASA 上只为思科 TrustSec 配置一个服务器组实例。

以下示例显示如何为思科 TrustSec 集成配置 ASA 以便与 ISE 服务器通信:

```
ciscoasa(config)#aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

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。
- 导入后，PAC 文件会驻留在 NVRAM 中。在 HA 模式下运行时，如果正确配置故障转移和有状态链路，将 PAC 文件导入活动单元后，就会复制到辅助单元。由于导入的文件驻留在 NVRAM 中，因此每当设备重启时，例如软件升级后，必须再次导入文件。
- 设备使用单个 PAC 文件。如果导入多个 PAC 文件，则每个导入的 PAC 文件都会替换之前导入的文件。
- 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。

过程

导入 Cisco TrustSec PAC 文件。

cts import-pac *filepath* password *value*

示例:

```
ciscoasa(config)# cts import-pac disk0:/xyz.pac password IDFW-pac99
```

value 参数指定用于加密 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。输入 *filepath* 参数作为下列选项之一:

单模式

- **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

以下示例显示如何将 PAC 文件导入 ASA:

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme  
PAC file successfully imported
```

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 在 ASA 上启用 SXP。默认情况下，SXP 被禁用。

cts sxp enable

示例：

```
ciscoasa(config)# cts sxp enable
```

步骤 2 （可选，不推荐。）为 SXP 连接配置默认源 IP 地址。

cts sxp default source-ip ipaddress

示例：

```
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
```

ipaddress 参数是 IPv4 或 IPv6 地址。

当为 SXP 配置默认源 IP 地址时，必须指定与 ASA 出站接口相同的地址。如果源 IP 地址不匹配出站接口的地址，SXP 连接将失败。

如果未配置 SXP 连接的源 IP 地址，ASA 将执行路由/ARP 查询来确定 SXP 连接的出站接口。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 3 （可选。）配置用于对 SXP 对等体进行 TCP MD5 身份验证的默认密码。默认情况下，SXP 连接无密码。

cts sxp default password [0 | 8] 密码

示例：

```
ciscoasa(config)# cts sxp default password 8 IDFW-TrustSec-99
```

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。

密码的长度取决于解密级别，如果未指定，则默认为 0：

- 0- 未加密的明文形式。密码最长为 80 个字符。
- 8- 加密的文本。密码最长为 162 个字符。

步骤 4（可选。）指定 ASA 尝试在 SXP 对等体之间设置新 SXP 连接的时间间隔。

cts sxp retry period *timervalue*

示例：

```
ciscoasa(config)# cts sxp retry period 60
```

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 5（可选。）指定调和计时器的值。

cts sxp reconciliation period *timervalue*

示例：

```
ciscoasa(config)# cts sxp reconciliation period 60
```

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 6（可选。）配置在 SXP 对等体终止其 SXP 连接后从某个对等体获知的 IP-SGT 映射的删除抑制计时器。

cts sxp delete-hold-down period *timervalue*

计时器的值指定了在删除从非活动状态的 SXP 连接获知的 IP-SGT 映射之前将其保留的秒数 (120-64000)。

示例：

```
ciscoasa(config)# cts sxp delete-hold-down period 240
```

每个 SXP 连接都与一个删除抑制计时器相关联。当侦听程序端的 SXP 连接不活动时，就会触发此计时器。从该 SXP 连接获知的 IP SGT 映射不会被立即删除。相反，它们将被保留，直到删除抑制计时器到期。此计时器到期时删除该映射。

步骤 7（可选。）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。

cts sxp mapping network-map *maximum_hosts*

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。

添加 SXP 连接对等体

如要添加 SXP 连接对等体，请执行以下步骤：

过程

建立与 SXP 对等体的 SXP 连接。

```
cts sxp connection peer peer_ip_address [source source_ip_address] password {default | none} [mode {local | peer}] {speaker | listener}
```

示例：

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default mode peer speaker
```

SXP 连接按 IP 地址设置：一个设备对可以服务于多个 SXP 连接。

peer_ip_address 参数为 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。

source_ip_ad 参数是 SXP 连接的本地 IPv4 或 IPv6 地址。源 IP 地址必须与 ASA 出站接口相同，否则连接将失败。

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。

指示是否使用 SXP 连接的身份验证密钥：

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

指示 SXP 连接模式：

- **local** - 使用本地 SXP 设备。
- **peer** - 使用对等 SXP 设备。

指示 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。

以下示例显示如何在 ASA 上配置 SXP 对等体：

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100 password default
```

```
mode peer speaker
ciscoasa(config)# cts sxp connection peer 192.168.1.101 password default
mode peer speaker
```

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

刷新来自 ISE 的环境数据，将协调计时器重置为已配置的默认值。

```
cts refresh environment-data
```

示例：

```
ciscoasa(config)# cts refresh environment-data
```

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。

- 要配置扩展 ACL，请参阅[添加扩展 ACE 执行基于安全组的匹配（思科 TrustSec）](#)，第 38 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 21 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。

以下示例显示如何创建一个使用在本地定义的安全对象组的 ACL：

```
object-group security objgrp-it-admin
  security-group name it-admin-sg-name
  security-group tag 1
object-group security objgrp-hr-admin
  security-group name hr-admin-sg-name // single sg_name
  group-object it-admin // locally defined object-group as nested object
object-group security objgrp-hr-servers
  security-group name hr-servers-sg-name
object-group security objgrp-hr-network
  security-group tag 2
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
```

通过配置访问组或模块化策略框架，可激活上一个示例中配置的 ACL。

其他示例：

```
!match src hr-admin-sg-name from any network to dst host 172.23.59.53
access-list idw-acl permit ip security-group name hr-admin-sg-name any host 172.23.59.53

!match src hr-admin-sg-name from host 10.1.1.1 to dst any
access-list idfw-acl permit ip security-group name hr-admin-sg-name host 10.1.1.1 any

!match src tag 22 from any network to dst hr-servers-sg-name any network
access-list idfw-acl permit ip security-group tag 22 any security-group
name hr-servers-sg-name any

!match src user mary from any host to dst hr-servers-sg-name any network
access-list idfw-acl permit ip user CSC0\mary any security-group
name hr-servers-sg-name any

!match src objgrp-hr-admin from any network to dst objgrp-hr-servers any network
access-list idfw-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers any

!match src user Jack from objgrp-hr-network and ip subnet 10.1.1.0/24
! to dst objgrp-hr-servers any network
access-list idfw-acl permit ip user CSC0\Jack object-group-security
objgrp-hr-network 10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any

!match src user Tom from security-group mktg any google.com
object network net-google
fqdn google.com
access-list sgacl permit ip sec name mktg any object net-google

! If user Tom or object_group security objgrp-hr-admin needs to be matched,
! multiple ACEs can be defined as follows:
```

```
access-list idfw-acl2 permit ip user CSCO\Tom 10.1.1.0 255.255.255.0
object-group-security objgrp-hr-servers any
access-list idfw-acl2 permit ip object-group-security objgrp-hr-admin
10.1.1.0 255.255.255.0 object-group-security objgrp-hr-servers any
```

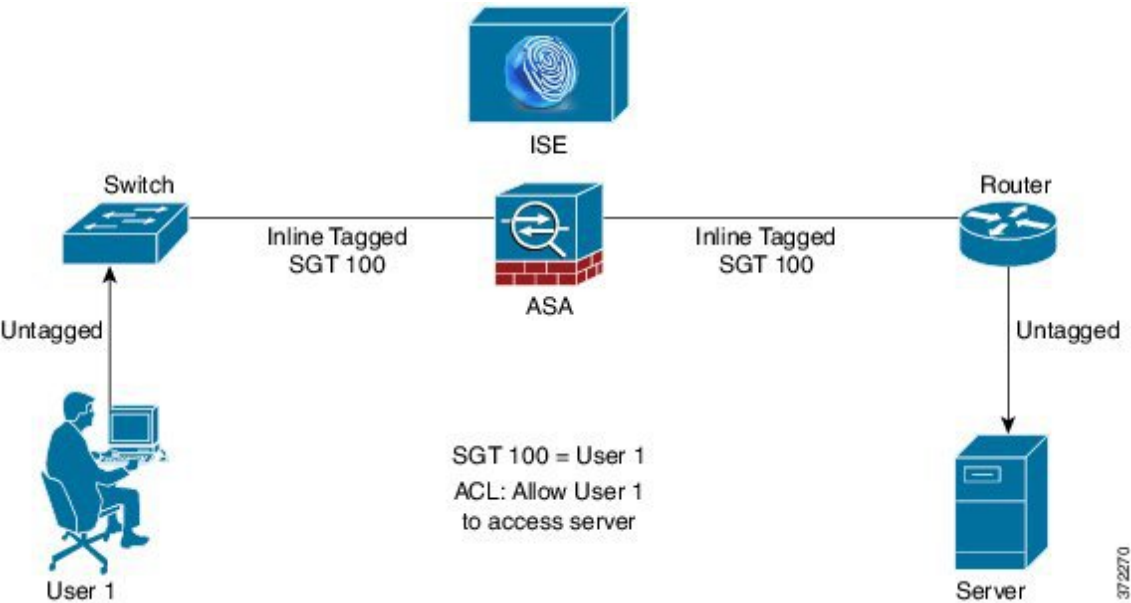
配置第 2 层安全组标记实施

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 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。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 5: 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 3: 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。

接口配置	收到的已标记数据包	收到的未标记数据包
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 4: 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 5: 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。
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 指定接口并输入接口配置模式。

interface *id*

示例:

```
ciscoasa(config)# interface gigabitethernet 0/0
```

步骤 2 启用第 2 层 SGT 实施，然后进入 cts 手动接口配置模式。

cts manual

示例:

```
ciscoasa(config-if)# cts manual
```

步骤 3 在接口上启用安全组标记传送。默认情况下，传送被启用。

propagate sgt

示例:

```
ciscoasa(config-if-cts-manual)# propagate sgt
```

步骤 4 将策略应用于手动配置的 CTS 链路中。

policy static sgt *sgt_number* [**trusted**]

示例:

```
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

static 关键字指定应用到链路上的传入流量的 SGT 策略。

sgt *sgt_number* 关键字参数对指定要应用于来自对等体的传入流量的 SGT 号。有效值为 2 到 65519。

trusted 关键字指明接口上具有在命令中指定的 SGT 的进口流量不应使其 SGT 被覆盖。默认设置为 Untrusted。

以下示例为第 2 层 SGT 实施启用接口并定义此接口是否可信:

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)# propagate sgt
ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

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

手动配置 IP-SGT 绑定。

cts role-based sgt-map {IPv4_addr[/mask] | IPv6_addr[/prefix]} sgt sgt_value

示例：

```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```

可以指定 IPv4 或 IPv6 主机地址。另外，也可以通过包含子网掩码或前缀值（对于 IPv6）指定网络地址，例如 10.100.10.0/24。*sgt_value* 是 SGT 编号，范围介于 2 到 65519 之间。

故障排除提示

使用 **packet-tracer** 命令确定为何特定会话被允许或被拒绝，正在使用哪个 SGT 值（来自数据包中的 SGT，来自 IP-SGT 管理器，或来自在接口上配置的 **policy static sgt** 命令），以及应用了哪些基于安全组的安全策略。

以下示例显示 **packet-tracer** 命令的输出，以显示到 IP 地址的安全组标记映射：

```
ciscoasa# packet-tracer input inside tcp inline-tag 100
security-group name alpha 30 security-group tag 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.

Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
-----More-----
```

使用 **capture capture-name type inline-tag tag** 命令仅捕获带或不带特定 SGT 值的思科 CMD 数据包 (EtherType 0x8909)。

以下示例显示 **show capture** 命令针对指定的 SGT 值的输出：

```
ciscoasa# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 10.0.101.100: icmp: echo request
4: 11:34:43.933164 INLINE-TAG 48 10.0.101.100 > 10.0.101.22: icmp: echo reply
```

思科 TrustSec 示例

以下示例显示如何配置 ASA 以使用思科 TrustSec:

```
// Import an encrypted CTS PAC file
cts import-pac asa.pac password Cisco
// Configure ISE for environment data download
aaa-server cts-server-list protocol radius
aaa-server cts-server-list host 10.1.1.100 cisco123
cts server-group cts-server-list
// Configure SXP peers
cts sxp enable
cts sxp connection peer 192.168.1.100 password default mode peer speaker
//Configure security-group based policies
object-group security objgrp-it-admin
  security-group name it-admin-sg-name
  security-group tag 1
object-group security objgrp-hr-admin
  security-group name hr-admin-sg-name
group-object it-admin
object-group security objgrp-hr-servers
  security-group name hr-servers-sg-name
access-list hr-acl permit ip object-group-security objgrp-hr-admin any
object-group-security objgrp-hr-servers
//Configure security group tagging plus Ethernet tagging
  interface gi0/1
    cts manual
    propagate sgt
    policy static sgt 100 trusted
    cts role-based sgt-map 10.1.1.100 sgt 50
```

Secure Client VPN 支持思科 TrustSec

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) 进入组策略配置模式：

group-policy *name*

示例：

```
ciscoasa(config)# group policy Grpolicy1
```

b) 为组策略配置 SGT。

security-group-tag {none | value *sgt*}

如果使用 **value** 设置标记，该标记的范围可介于 2 到 65519 之间。指定 **none** 可设置无 SGT。

示例：

```
ciscoasa(config-group-policy)# security-group-tag value 101
```

步骤 2 要为 LOCAL 数据库中的用户配置 SGT，请执行以下操作：

a) 如果需要，请创建用户。

username *name* {nopassword | password *password* [encrypted]} [privilege *priv_level*]

示例：

```
ciscoasa(config)# username newuser password changeme encrypted privilege 15
```

b) 进入用户名配置模式。

username *name* **attributes**

示例：

```
asa3(config)# username newuser attributes
```

```
asa3(config-username)#
```

c) 为用户配置 SGT。

security-group-tag {none | value sgt}

如果使用 **value** 设置标记，该标记的范围可介于 2 到 65519 之间。指定 **none** 可设置无 SGT。

示例：

```
ciscoasa(config-username)# security-group-tag value 101
```

监控 Cisco TrustSec

请参阅以下 commands 来监控思科 TrustSec：

- **show running-config cts**

- **show running-config [all] cts role-based [sgt-map]**

此命令显示用户定义的 IP-SGT 绑定表条目。

- **show cts sxp connections**

此命令显示使用多情景模式时，ASA 上特定用户情景的 SXP 连接。

- **show conn security-group**

显示所有 SXP 连接的数据。

- **show cts environment-data**

显示 ASA 上安全组表中包含的思科 TrustSec 环境信息。

- **show cts sgt-map**

显示控制路径中的 IP 地址安全组表管理器条目。

- **show asp table cts sgt-map**

此命令显示数据路径内维护的 IP 地址安全组表映射数据库中的 IP 地址安全组表映射条目。

- **show cts 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 的历史记录

表 6: 思科 TrustSec 的历史记录

功能名称	平台版本	说明
思科 TrustSec	9.0(1)	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。 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。 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。 引入或修改了以下命令：access-list extended、cts sxp enable、cts server-group、cts sxp default、cts sxp retry period、cts sxp reconciliation period、cts sxp connection peer、cts import-pac、cts refresh environment-data、object-group security、security-group、show running-config cts、show running-config object-group、clear configure cts、clear configure object-group、show cts pac、show cts environment-data、show cts environment-data sg-table、show cts sxp connections、show object-group、show configure security-group、clear cts environment-data、debug cts，和 packet-tracer。
第 2 层安全组标记实施	9.3(1)	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。 引入或修改了以下命令：cts manual、policy static sgt、propagate sgt、cts role-based sgt-map、show cts sgt-map、packet-tracer、capture、show capture、show asp drop、show asp table classify、show running-config all、clear configure all 和 write memory。
思科 Trustsec 支持安全交换协议 (SXP) 版本 3。	9.6(1)	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。 引入或修改了以下命令：cts sxp mapping network-map、cts role-based sgt-map、show cts sgt-map、show cts sxp sgt-map、show asp table cts sgt-map。

功能名称	平台版本	说明
Trustsec SXP 连接可配置删除抑制计时器	9.8(3)	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。 新增/修改的命令：cts sxp delete-hold-down period、show cts sxp connection brief 和 show cts sxp connections



第 6 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 95 页](#)
- [思科 Umbrella 连接器的许可要求，第 97 页](#)
- [思科 Umbrella 的准则和限制，第 97 页](#)
- [配置思科 Umbrella 连接器，第 98 页](#)
- [Umbrella 连接器示例，第 105 页](#)
- [监控 Umbrella 连接器，第 107 页](#)
- [思科 Umbrella 连接器的历史记录，第 110 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。这样，Cisco Umbrella 就能识别对未经允许或有问题的域名的请求，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 Cisco 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 信誉以及这些条件来控制访问。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：

- 允许 - 如果对某个 FQDN 未设置阻止规则，并且 Cisco 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。

- 代理 - 如果对某个 FQDN 未设置阻止规则，并且 Cisco 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 Cisco Umbrella 控制面板（安全设置 (Security Setting) > 启用智能代理 (Enable Intelligent Proxy)）启用智能代理。
- 阻止 - 如果明确阻止 FQDN，或 Cisco 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。

从旧版 API 令牌切换到 API/密钥

从 ASA 9.23(1) 开始，Umbrella 将 API 注册机制从 API 令牌更改为 API 密钥和秘密。如果使用的是旧版令牌，则可通过执行以下操作从旧版 API 切换到 API/密钥 API。详细步骤请参见相关程序。

过程

-
- 步骤 1 导入新 API 的证书。您需要安装 ISRG Root X1 自签名证书。
 - 步骤 2 禁用 Umbrella。
 - 步骤 3 删除现有的令牌注册。
 - 步骤 4 配置新的 API 和密钥。
 - 步骤 5 重新启用 Umbrella。
-

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 的准则和限制

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。

故障转移

- 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

- 集群控制单元在 Cisco 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。

其他准则

- 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，阻止和代理操作才有效，因为返回的 IP 地址是针对网站的。非 HTTP/HTTPS 连接的任何列入阻止和代理地址的操作将失败或以误导性方式完成。例如，针对列入阻止 FQDN 执行 ping 操作会导致对托管 Cisco Umbrella 云阻止页面的服务器执行 ping 操作。



注释

Cisco Umbrella 试图智能地识别可能是非 HTTP/HTTPS 的 FQDN，并且对于代理域名的 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，DNSCrypt 会加密 IPv4 和 IPv6 流量。
- 必须有一个 IPv4 路由可到达互联网 api.umbrella.com 和 api.opendns.com（注册仅使用 IPv4）。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。系统会指示系统使用的默认服务器；通过在 Umbrella 全局设置中配置解析器，可以使用其他服务器。
 - 208.67.220.220（IPv4 的系统默认值）
 - 208.67.222.222
 - 2620:119:53::53（IPv6 的系统默认值）
 - 2620:119:35::35
- 系统不支持 Umbrella FamilyShield 服务。如果配置 FamilyShield 解析器，则可能会出现意外结果。
- 当评估是否在故障时打开时，系统会判断 Umbrella 解析器是否关闭，或干预设备是否根据发送 DNS 请求后等待的时间长度来丢弃 DNS 请求或响应。系统不考虑其他因素，例如没有到 Umbrella 解析器的路由。
- 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 99 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。

可以使用自己的服务器，或配置思科 Umbrella 服务器。即使配置其他服务器，DNS 检测也会自动重定向到思科 Umbrella 解析器。

- 208.67.220.220
- 208.67.222.222
- 2620:119:53::53
- 2620:119:35::35

示例：

```
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220
```

步骤 4 配置 Umbrella 连接器全局设置，第 100 页。

步骤 5 在 DNS 检测策略映射中启用 Umbrella，第 103 页。

步骤 6 验证 Umbrella 注册，第 104 页。

从思科 Umbrella 注册服务器安装 CA 证书

必须导入根证书，才能与思科 Umbrella 注册服务器建立 HTTPS 连接。注册设备时，系统使用 HTTPS 连接。在 Cisco Umbrella 中，依次选择 **部署 (Deployments)** > **配置 (Configuration)** > **根证书 (Root Certificate)** 并下载证书。

使用 API 和密钥注册 Umbrella 时，需要安装 ISRG Root X1 自签名证书 pem 文件。您可以从 <https://letsencrypt.org/certs/isrgrootx1.pem> 获取此证书。

开始之前

如果 Umbrella 更新了证书，则您需要下载新证书。根证书也可能发生变化。确保上传了正确的根证书。

更新证书时，必须先禁用 Umbrella，然后再启用，这样系统才能接收新证书并正确注册 Umbrella。

过程

步骤 1 为思科 Umbrella 注册服务器创建信任点。

crypto ca trustpoint name

可以使用您希望使用的任何名称命名信任点（最多 128 个字符），例如 ctx1 或 umbrella_server。

示例：

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)#
```

步骤 2 指出您想要通过粘贴证书手动注册。

enrollment terminal

示例：

```
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)#
```

步骤 3 导入证书。

crypto ca authenticate name

输入为此证书创建的信任点的名称。根据提示操作并粘贴 Base-64 编码证书。不要包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。

```
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

配置 Umbrella 连接器全局设置

Umbrella 全局设置主要定义在 Cisco Umbrella 注册设备所需的 API 和密钥或旧版 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 103 页 所述。

开始之前

- 登录 Umbrella 控制面板并生成 API 密钥和秘密。在 Umbrella 中从管理员 (Admin) > API 密钥 (API Keys) 生成密钥。生成密钥时，必须确保复制并保存 API 和密钥，因为以后无法检索密钥。密钥的范围必须是读/写。
- (旧版，不推荐。) 登录 Cisco Umbrella 网络设备控制面板 (<https://login.umbrella.com/>)，获取适用于您的组织的旧版网络设备 API 令牌。此令牌是十六进制字符串，例如 AABBA59A0BDE1485C912AFE。从 Umbrella 控制面板生成旧版网络设备 API 密钥。
- 安装思科 Umbrella 注册服务器证书。

过程

步骤 1 进入 Umbrella 配置模式。

umbrella-global

示例:

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)#
```

步骤 2 配置向 Cisco Umbrella 注册所需的 API 密钥和秘密。

token-request-credential api-key key_value secret secret_value

请注意，密钥会过期，您需要禁用 Umbrella，添加新密钥/秘密，并在应用新密钥时重新启用 Umbrella。

示例:

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token-request-credential
api-key f817feb474d94c56b3448bcd08edc11 secret 4afe58df5c454161a10a172145cb1456
```

步骤 3 (旧版，不推荐。) 配置在思科 Umbrella 中注册时所需的 API 令牌。

仅当不配置 API 密钥和秘密时，才能配置令牌。

token api_token

示例:

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
```

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，则使用当前分布分发的默认公钥进行验证。

public-key *hex_key*

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

要恢复使用默认公钥，请输入 **no public-key**。可以省略所配置的密钥，或将其包含在 **no** 版本命令中。

示例：

```
ciscoasa(config-umbrella)# public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
```

步骤 5（可选。）配置当服务器没有响应时，在删除从客户端至 Umbrella 服务器的连接之前的空闲超时。

timeout edns *hh:mm:ss*

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）。

示例：

```
ciscoasa(config-umbrella)# timeout edns 00:01:00
```

步骤 6（可选。）配置应绕过 Umbrella 的本地域名。

可以识别 DNS 请求应绕过思科 Umbrella 直接转至所配置的 DNS 服务器的本地域。例如，假设允许所有内部连接，可以借助内部 DNS 服务器解析组织域名的所有名称。

可以直接输入本地域名。或者，可以创建定义该域名的正则表达式，然后创建正则表达式类映射并在以下命令中指定：

local-domain-bypass {*regular_expression* | **regex class** *regex_classmap*}

示例：

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# local-domain-bypass example.com
```

步骤 7（可选。）配置您想要用于解析 DNS 请求的非默认思科 Umbrella DNS 服务器的地址。

resolver {*ipv4* | *ipv6*} *ip_address*

可以单独输入命令，以定义非默认 Umbrella 解析器的 IPv4 和 IPv6 地址。

示例：

```
ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222
ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```

步骤 8 选择向 Umbrella 注册时要使用的方法

- 令牌（旧版本，不推荐）- 在令牌 (Token) 字段中输入 API 令牌。
- 令牌请求凭证 - 配置以下内容：
 - API 密钥 - 输入从 Umbrella 生成的 API 密钥。
 - 密钥 - 输入为 API 密钥提供的密钥。

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 265 页](#)。

过程

步骤 1 编辑 `preset_dns_map` 检测策略映射，并进入参数配置模式。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)#
```

步骤 2 启用思科 Umbrella 并选择性地指定要应用于设备的思科 Umbrella 策略的名称。

umbrella [**tag umbrella_policy**] [**fail-open**]

该标签为思科 Umbrella 中所定义策略的名称。注册期间，思科 Umbrella 会将策略分配到设备（如果存在策略名称）。如果未指定策略，系统将应用默认策略。

如果希望 DNS 解析在 Umbrella DNS 服务器不可用条件下运行，则请包含 **fail-open** 关键字。故障时打开的情况下，如果思科 Umbrella DNS 服务器不可用，则 Umbrella 会在该策略映射上自动禁用，并允许向系统上配置的其他 DNS 服务器发送 DNS 请求（若有）。当 DNS 服务器恢复可用状态时，策略映射会恢复使用它们。如果未包含该选项，则 DNS 请求会继续发送至无法访问的 Umbrella 解析器，因此这些请求不会收到任何回复。

示例：

```
ciscoasa(config-pmap-p)# umbrella fail-open
```

步骤 3（可选。）启用 DNScrypt 以加密设备与思科 Umbrella 之间的连接。

dnscrypt

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。

示例：

```
ciscoasa(config-pmap-p)# dnscrypt
```

示例

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella fail-open
ciscoasa(config-pmap-p)# dnscrypt
```

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。

首先，检查服务策略统计信息，查询思科 Umbrella 注册行。这应显示 Cisco Umbrella 应用的策略（标签）、连接的 HTTP 状态和设备 ID。

状态应为 200 成功。错误代码指示以下内容：401 表示 API 令牌不正确，403 表示密钥的范围不是读/写（阻止访问），405 表示 API 密钥已过期，409 表示设备已存在在 Cisco Umbrella 中部署。

如果状态为 UNKNOWN，请检查系统日志消息。信息 339011：“Umbrella API 令牌请求未收到任何响应” (Umbrella API token request received no responses) 表明在访问 api.umbrella.com 时出现了路由问题，或者您没有上传所需的证书。

请注意，Umbrella 解析器行不应指示解析器无响应。如果解析器无响应，则验证是否在访问控制策略中打开了与这些 IP 地址的 DNS 通信。这可能是临时情况，也可能表示存在路由问题。

```
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: mode: fail-open tag: default, status: 200 success, device-id:
```

```

010a13b8fbdfc9aa
    Umbrella ipv4 resolver: 208.67.220.220
    Umbrella ipv6 resolver: 2620:119:53::53
    Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0 local-domain-bypass
10
    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。

```

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

```

Umbrella 连接器示例

以下主题提供 Umbrella 连接器的配置示例。

示例： 在全局 DNS 检测策略上启用 Umbrella

以下示例显示如何全局启用 Umbrella。配置使用默认公钥启用 DNScrypt。它会分配默认思科 Umbrella 企业安全策略。密钥和秘密仅为示例；您必须从 Umbrella 生成自己的有效密钥/秘密对。

此示例假设您已上传 Umbrella 注册所需的相应证书。确保下载 Umbrella 站点使用的最新根证书，因为正确的证书会随时间变化。

```

ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token-request-credential
api-key f817feb474d94c56b3448bcbd08edc11 secret 4afe58df5c454161a10a172145cb1456

ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt

```

示例： 在使用自定义检查策略的接口上启用 Umbrella

以下示例显示如何针对特定流量类启用 Umbrella。在仅适用于 DNS/UDP 流量的内部接口上启用 Umbrella。因为我们正在启用 DNSCrypt，UDP/443 必须包含在流量类中。应用名为 mypolicy（在思科 Umbrella 中定义）的企业安全策略。密钥和秘密仅为示例；您必须从 Umbrella 生成自己的有效密钥/秘密对。

此示例假设您已上传 Umbrella 注册所需的相应证书。确保下载 Umbrella 站点使用的最新根证书，因为正确的证书会随时间变化。

```
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token-request-credential
api-key f817feb474d94c56b3448bcbd08edc11 secret 4afe58df5c454161a10a172145cb1456

ciscoasa(config)# policy-map type inspect dns umbrella-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella tag mypolicy
ciscoasa(config-pmap-p)# dnscrypt

ciscoasa(config)# object-group service umbrella-service-object
ciscoasa(config-service-object-group)# service-object udp destination eq domain
ciscoasa(config-service-object-group)# service-object udp destination eq 443

ciscoasa(config)# access-list umbrella-acl extended permit
object-group umbrella-service-object any any

ciscoasa(config)# class-map dns-umbrella
ciscoasa(config-cmap)# match access-list umbrella-acl

ciscoasa(config)# policy-map inside-policy
ciscoasa(config-pmap)# class dns-umbrella
ciscoasa(config-pmap-c)# inspect dns umbrella-policy

ciscoasa(config)# service-policy inside-policy interface inside
```

示例： 从 Umbrella 全局排除某些主机或网络

如果需要排除某些主机或网络使用 Umbrella，而且选择是全局性的而不是基于接口的，可以移除全局 DNS 检查，并创建单独的类来排除或包括 Umbrella 检查。

以下示例修改了全局检查策略，使 192.168.1.0/24 网络无法使用 Umbrella。

开始之前

本示例假定您已启用 DNS 并配置了 Umbrella 全局设置。

过程

步骤 1 删除全局默认 DNS 检查。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# no inspect dns
```

步骤 2 创建可启用 Umbrella 的 DNS 策略映射。

在本示例中，策略映射命名为 umbrella-policy。

```
ciscoasa(config)# policy-map type inspect dns umbrella-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella tag mypolicy
```

步骤 3 为排除在外的流量创建流量类别。

以下示例使用 ACL 来识别来自 192.168.1.0/24 网络的 UDP/53 流量。

```
ciscoasa(config)# access-list Umb_Exclude permit udp 192.168.1.0 255.255.255.0 any eq 53
ciscoasa(config)# class-map Umbrella_Exclude
ciscoasa(config-cmap)# match access-list Umb_Exclude
```

步骤 4 为应该使用 Umbrella 的主机创建流量类别。

以下示例匹配来自任何源的 UDP/53 流量。

```
ciscoasa(config)# class-map Umbrella_Include
ciscoasa(config-cmap)# match port udp eq 53
```

步骤 5 更新全局检测策略，使用适当的 DNS 策略映射为流量类别启用 DNS 检测。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class Umbrella_Exclude
ciscoasa(config-pmap-c)# inspect dns
ciscoasa(config-pmap)# class Umbrella_Include
ciscoasa(config-pmap-c)# inspect dns umbrella-policy
```

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。

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。

解析器行表示正在使用的 Umbrella 服务器。这些行将指出服务器是否无响应，或系统当前是否正在探测服务器以确定服务器是否可用。如果模式为故障时打开模式，系统将允许 DNS 请求转至其他 DNS 服务器（如果配置）；否则，只要 Umbrella 服务器无响应，DNS 请求就不会收到任何响应。

```
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: mode: fail-open tag: default, status: 200 success, device-id:
010a13b8fbd9c9aa
      Umbrella ipv4 resolver: 208.67.220.220
      Umbrella ipv6 resolver: 2620:119:53::53
      Umbrella: bypass 0, req inject 0 - sent 0, res rcv 0 - inject 0 local-domain-bypass
10
      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: dnsencrypt30000
      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: mode: fail-open tag: default, status: 200 SUCCESS, device-id:
010af97abf89abc3, retry 0
      Umbrella ipv4 resolver: 208.67.220.220
      Umbrella ipv6 resolver: 2620:119:53::53
      Umbrella: bypass 0, req inject 6 - sent 6, res rcv 6 - inject 6 local-domain-bypass
10
      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。
- %ASA-3-339006: 无法访问 Umbrella 解析器 *IP_address*，已恢复 Umbrella 重定向。
此消息表明，系统已恢复到正常运行状态。无需任何操作。
- %ASA-3-339007: Umbrella 解析器 *IP_address* 无响应，已使用故障关闭模式，启动对解析器的探测。
由于您正在使用故障关闭模式，因此在 Umbrella DNS 服务器重新上线前，用户不会收到有关其 DNS 请求的响应。如果问题仍然存在，请验证是否存在从系统到 Umbrella 服务器的路由，以及在访问控制策略中是否允许 DNS 流量流向服务器。
- 与 API 密钥/密钥注册相关的消息：
 - %ASA-6-339010: Umbrella API 令牌请求成功
 - %ASA-3-339011: Umbrella API 令牌请求未收到响应
 - %ASA-3-339012: Umbrella API 令牌请求失败，错误代码为 %d
 - %ASA-3-339013: Umbrella API 令牌请求在响应处理过程中失败
 - %ASA-3-339014: Umbrella API 令牌请求在 %d 次重试后失败；中止注册

思科 Umbrella 连接器的历史记录

功能名称	平台版本	说明
思科 Umbrella 支持。	9.10(1)	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。 关键字，所以您可以显示有关特定 GTP 版本的信息：umbrella、umbrella-global、token、public-key、timeout edns、dnscrypt、show service-policy inspect dns detail。

功能名称	平台版本	说明
思科 Umbrella 增强功能。	9.12(1)	您现在可以标识需要绕过思科 Umbrella 的本地域名。发向这些域的 DNS 请求将直接流向 DNS 服务器，而不经 Umbrella 处理。此外，您还可以标识用于解析 DNS 请求的 Umbrella 服务器。最后，您可以定义 Umbrella 检测策略以实现故障时自动开放，以确保 Umbrella 服务器不可用时，DNS 请求不会被阻止。 添加或更改了以下命令：local-domain-bypass、resolver、umbrella fail-open。
新的 Umbrella API。	9.23(1)	您现在可以使用 Umbrella 开放 API 来配置 Umbrella，该 API 使用带密钥的 API 密钥。 添加了以下命令：token-request-credential



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 115 页



第 7 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 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 Virtual 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准则，第 115 页](#)
- [配置基于属性的访问控制，第 116 页](#)
- [监控基于属性的网络对象，第 123 页](#)
- [基于属性的访问控制的历史记录，第 124 页](#)

基于属性的网络对象准则

IPv6 准则

- 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。

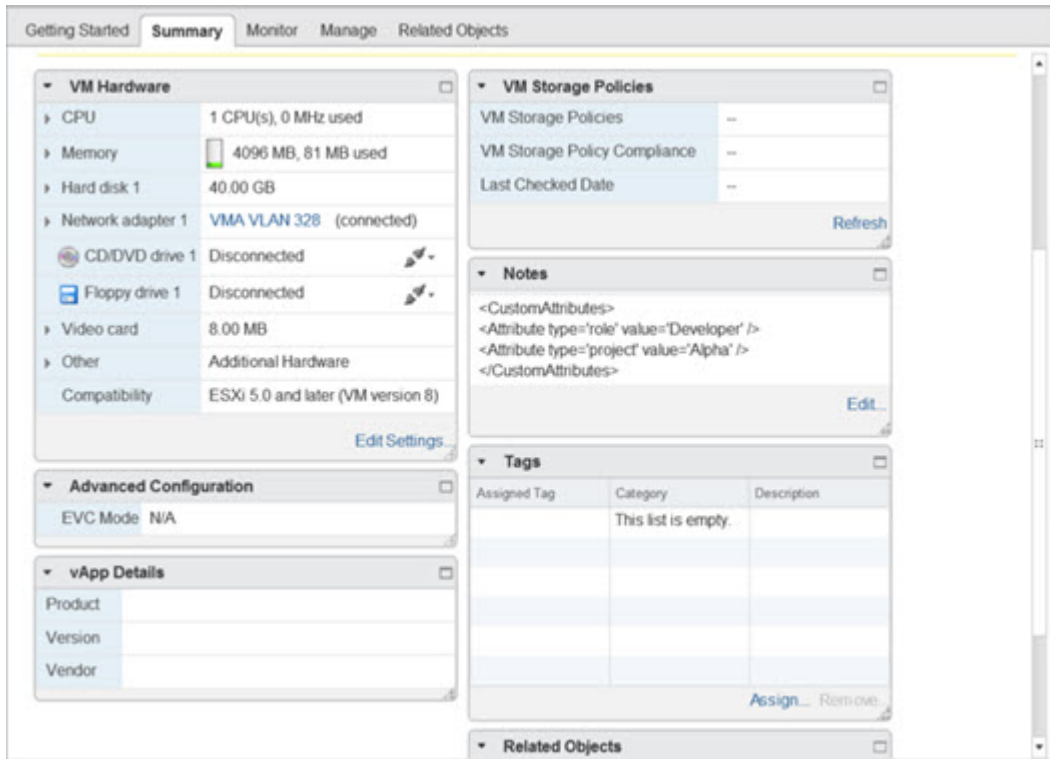
过程

-
- 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 116 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 118 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 119 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控制](#)，第 121 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 6: 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 点击确定 (OK)。

示例

以下示例显示格式正确的 XML 文件文件，该文件用于为可应用于虚拟机的对象 “role” 和 “project” 定义自定义属性：

```
<CustomAttributes>
<Attribute type='role' value='Developer' />
<Attribute type='project' value='Alpha' />
</CustomAttributes>
```

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 创建与 vCenter 通信的虚拟机属性代理：**attribute source-group agent-name type agent-type**

示例:

```
hostname(config)# attribute source-group VMagent type esxi
```

agent-name 参数指定虚拟机属性代理名称。*type* 参数是属性代理的类型。

注释

目前，ESXi 是唯一受支持的代理类型。

步骤 2 配置您的 vCenter 主机凭证：**host ip-address username ESXi-username password ESXi-password**

示例：

```
hostname(config-attr)# host 10.122.202.217 user admin password Cisco123
```

步骤 3 配置 vCenter 通信的保持连接设置：**keepalive retry-interval interval retry-count count**

示例：

```
hostname(config-attr)# keepalive retry-timer 10 retry-count 3
```

默认保持连接计时器值为间隔 30 秒进行 3 次重试。

步骤 4 检查虚拟机属性代理配置：**show attribute source-group agent-name**

示例：

```
hostname(config-attr)# sh attribute source-group VMagent

Attribute agent VMagent
Agent type: ESXi
Agent state: Inactive
Connection state: Connected
Host Address: 10.122.202.217
Retry interval: 30 seconds
Retry count: 3
```

Agent State 将保持非活动状态，直到您配置网络对象并指定与该对象关联的属性。

步骤 5 退出属性配置模式：**exit**

示例：

```
hostname(config-attr)# exit
```

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 启用对象组搜索： **object-group-search access-control**

示例：

```
hostname(config)# object-group-search access-control
```

必须启用对象组搜索，才能配置基于属性的网络对象。

步骤 2 使用对象名称创建或编辑基于属性的网络对象： **object network object-id**

示例：

```
hostname(config)# object network dev
```

步骤 3 指定与对象关联的代理、属性类型和属性值： **attribute agent-name attribute-type attribute-value**

示例：

```
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

agent-name 指定 VM 属性代理，请参阅 <XREF>。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“无可用证书”状态，直到使用 **host** 子命令提供主机证书。

attribute-type 和 *attribute-value* 对一起可定义唯一的属性。*attribute-type* 是随机字符串，并且必须包含 **custom.** 前缀。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。

示例

以下示例为开发组创建基于属性的网络对象 *dev*，其角色为“Developer”。VM 属性代理与 vCenter 通信并返回匹配属性 *custom.role* 的所有虚拟机绑定：

```
hostname(config)# object network dev
hostname(config-network-object)# attribute VMAgent custom.role Developer
```

以下示例为测试组创建基于属性的网络对象 *test*，其角色为“Automation”。VM 属性代理与 vCenter 通信并返回匹配属性 *custom.role* 的所有虚拟机绑定。请注意，本例使用的虚拟机列表与上一个示例相同：

```
hostname(config)# object network test
hostname(config-network-object)# attribute VMAgent custom.role Automation
```

以下示例为项目组创建基于属性的网络对象 *project*，其角色为“Alpha”。VM 属性代理与 vCenter 通信并返回匹配属性 *custom.project* 的所有虚拟机绑定。请注意，某些计算机的多个属性重叠：

```
hostname(config)# object network project
hostname(config-network-object)# attribute VMAgent custom.project Alpha
```

以下示例显示具有待定属性请求、处于活动状态的 VM 属性代理：

```
hostname(config-attr)# show attribute source-group VMAgent

Attribute agent VMAgent
Agent type: ESXi
Agent state: Active
Connection state: Connected
Host Address: 10.122.202.217
Retry interval: 30 seconds
Retry count: 3
Attribute requests pending:
    'custom.project'
    'custom.role'
```

使用基于属性的网络对象配置访问控制

在对来自共享一个或多个属性的虚拟机组的流量定义访问控制列表 (ACL) 时，可以使用基于属性的网络对象。访问列表包含一个或多个访问控制条目 (ACE)。一个 ACE 指访问列表中的一个条目，指定允许或拒绝规则（转发或丢弃数据包）。通常，允许或拒绝规则应用于协议、源与目标 IP 地址或网络，也可以选择性地应用于源与目标端口。

使用基于属性的网络对象时，可以使用这些对象替换源和/或目标 IP 地址。在部署、移动或废弃虚拟机时，可更新虚拟机上的属性，同时分配的访问控制策略可保持有效，不进行配置更改。

有关 ACL 所有可用选项的完整信息，请参阅[配置 ACL](#)，第 32 页。

过程

步骤 1 使用基于属性的网络对象创建和配置扩展 ACL 条目 (ACE): **access-list access_list_name extended {deny | permit} protocol_argument object source_object_name object dest_object_name**

示例：

```
hostname(config)# access-list lab-access extended permit ip object dev object test
```

注释

根据需要，为您的策略重复上述操作。

选项有:

- **access_list_name** - 新的或现有 ACL 的名称。
- **Permit 或 Deny** - 如果条件匹配, **deny** 关键字可拒绝或排除数据包。如果条件匹配, **permit** 关键字可允许或添加数据包。
- **Protocol - protocol_argument** 指定 IP 协议:
 - **name 或 number** - 指定协议名称或编号。指定 **ip** 以应用于所有协议。
 - **object-group protocol_grp_id** - 指定使用 **object-group protocol** 命令创建的协议对象组。
- **Source Object - object** 指定使用 **object network** 命令创建的基于属性的网络对象。
source_object_name 指定发送数据包的对象。
- **Destination Object - object** 指定使用 **object network** 命令创建的基于属性的网络对象。
dest_object_name 指定将数据包发送到的对象。

步骤 2 将 ACL 绑定到接口或全局应用该 ACL: **access-group access_list_name {in interface interface_name | global}**

示例:

```
hostname(config)# access-group lab-access in interface inside
```

对接口特定的访问组:

- 指定扩展 ACL 名称。可以为每个接口上的每种 ACL 类型配置一个 **access-group** 命令。
- **in** 关键字会将 ACL 应用于入站流量。
- 指定 **interface** 名称。

对于全局访问组, 指定 **global** 关键字, 以将扩展 ACL 应用于所有接口的入站方向流量。

示例

以下示例显示如何全局应用基于属性的扩展 ACL:

```
hostname(config)# access-list lab-access extended permit ip object dev object test
hostname(config)# access-group lab-access global
hostname(config)# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
      alert-interval 300
access-list lab-access; 1 elements; name hash: 0x62b4790b
access-list lab-access line 1 extended permit ip object dev object test (hitcnt=0) 0x64a1be76

      access-list lab-access line 1 extended permit ip object dev(2) object test(3) (hitcnt=0)
      0x64a1be76
```

监控基于属性的网络对象

要监控基于属性的网络对象，请输入以下命令：

- **show attribute host-map**

显示特定属性的代理、类型和值的属性绑定。

- **show attribute object-map**

显示对象到属性的绑定。

- **show attribute source-group**

显示配置的 VM 属性代理。

示例

以下示例显示主机到属性绑定的映射：

```
hostname# show attribute host-map /all
IP Address-Attribute Bindings Information
```

Source/Attribute	Value
=====	=====
VMAgent.custom.project	'Alpha'
10.15.28.34	
10.15.28.32	
10.15.28.31	
10.15.28.33	
VMAgent.custom.role	'Automation'
10.15.27.133	
10.15.27.135	
10.15.27.134	
VMAgent.custom.role	'Developer'
10.15.28.34	
10.15.28.12	
10.15.28.31	
10.15.28.13	

以下示例显示对象到属性的绑定：

```
hostname# show attribute object-map /all
Network Object-Attribute Bindings Information
```

Object	Source/Attribute	Value
=====	=====	=====
dev		
	VMAgent.custom.role	'Developer'
test		
	VMAgent.custom.role	'Automation'
project		
	VMAgent.custom.project	'Alpha'

以下示例显示属性代理配置：

```
hostname# show attribute source-group
Attribute agent VMAgent
Agent type: ESXi
Agent state: Active
Connection state: Connected
Host Address: 10.122.202.217
Retry interval: 30 seconds
Retry count: 3
Attributes being monitored:
    'custom.role' (2)
```

基于属性的访问控制的历史记录

功能名称	平台版本	说明
基于属性的网络对象的支持	9.7.(1)	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。 引入了以下命令： object network attribute attribute agent-name attribute-type attribute-value attribute source-group agent-name type agent-type host ip-address username ESXi-username password ESXi-password keepalive retry-interval interval retry-count count
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 127 页
- [NAT 示例和参考](#)，第 177 页
- [映射地址和端口 \(MAP\)](#)，第 209 页



第 8 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 127 页](#)
- [NAT 基础知识 ， 第 128 页](#)
- [NAT 准则 ， 第 132 页](#)
- [动态 NAT ， 第 139 页](#)
- [动态 PAT ， 第 146 页](#)
- [静态 NAT ， 第 157 页](#)
- [身份 NAT ， 第 167 页](#)
- [监控 NAT ， 第 171 页](#)
- [NAT 的历史记录 ， 第 171 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） - 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 地址和目标 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“目标”，即便是给定的连接，也可能源自“目标”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 139 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 146 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 157 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，但又想豁免一小部分地址时，可能就要这样配置 NAT。请参阅[身份 NAT](#)，第 167 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标地址。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。同时指定源和目标地址，可以让您指定源 A/目的 A 有不同于源 A/目的 B 的转换。



注释 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“目标”，即便是给定的连接，也可能源自“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。

目标地址是可选的。如果指定目标地址，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，一条用于目标 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 规则顺序

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。



注释 还有一个第 0 部分，其中包含系统创建供自己使用的任何 NAT 规则。这些规则优先于所有其他规则。系统会自动创建这些规则并根据需要清除 `xlate`。您不能在第 0 部分中添加、编辑或修改规则。

表 7: 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，所以必须确保具体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。 “具体规则优先”是指： - 静态规则应放在动态规则前面。 - 包含目的地转换的规则应仅放在具有源转换的规则前面。 如果无法消除重叠规则（其中可能有多个规则基于源或目标地址而应用），请特别注意遵循这些建议。
第 2 部分	网络对象 NAT	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： - 静态规则。 - 动态规则。 在每个规则类型中，遵循以下排序准则： - 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。 - 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。 - 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	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。

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：

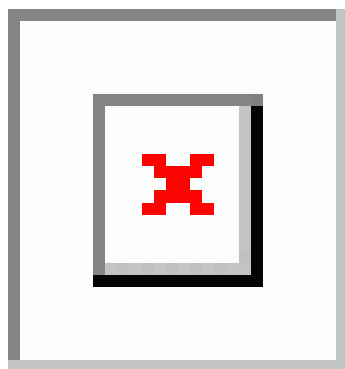
- 192.168.1.1/32（静态）
- 10.1.1.0/24（静态）
- 192.168.1.0/24（静态）
- 172.16.1.0/24（动态）（对象 abc）
- 172.16.1.0/24（动态）（对象 def）
- 192.168.1.0/24（动态）

NAT 接口

除了网桥组成员接口，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 7: 指定任何接口



然而，“任何”接口的概念不适用于网桥组成员接口。当指定“任何”接口时，NAT 将排除所有网桥组成员接口。因此，要将NAT应用于网桥组成员，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 准则

以下主题提供有关实施 NAT 的详细准则。

NAT 防火墙模式准则

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：

- 为网桥组的成员配置 NAT 时，需要指定成员接口。您不能为网桥组接口 (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。
- 当源接口和目标接口是同一网桥组的成员时，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，您可以在不同网桥组的成员之间，或在网桥组成员（源接口）和标准路由接口（目标接口）之间执行 NAT64/46。

IPv6 NAT 准则

NAT 支持 IPv6，但有以下准则和限制。

- 对于标准路由模式接口，您还可以在 IPv4 和 IPv6 之间进行转换。
- 对于同一个网桥组的成员接口，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成员或一个接口为网桥组成员，另一个为标准路由接口的情况。
- 在同属一个网桥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成员或一个接口为网桥组成员，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 最佳实践

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。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 准则

- NAT 规则仅适用于通过设备流量，不适用于由设备发起的流量，例如 RADIUS 身份验证。
- 对于作为网桥组成员的接口，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。
- 您不能为站点间 VPN 中使用的虚拟隧道接口 (VTI) 编写 NAT 规则。为 VTI 的源接口编写规则不会将 NAT 应用于 VPN 隧道。要编写应用于 VTI 上通过隧道传输的 VPN 流量的 NAT 规则，您必须使用“任何”作为接口，而不能明确指定接口名称。
- （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。例如，**对象网络 obj-10.10.10.1-01**、**对象网络 obj-10.10.10.1-02** 等。
- 如果在接口上定义了 VPN，则接口上的入站 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。

如果创建应用于现有连接（例如 VPN 隧道）的新 NAT 规则，则需要使用 **clear conn** 来终止连接。然后，尝试重新建立连接应符合 NAT 规则，且连接应正确进行 NAT。



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** 或 **clear conn** 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 关联的目标部分的拓扑未知。
- 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，“任何”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；借助此前提条件，ASA 可确定 NAT 规则中的 **any** 的值。例如，如果配置从“任何”到 IPv6 服务器的规则，且该服务器已从 IPv4 地址映射，则任何指“任何 IPv6 流量”。如果配置从“任何”到“任何”的规则，并且将源映射至接口 IPv4 地址，则任何指“任何 IPv4 流量”，因为映射的接口地址意味着目标也是 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“任何”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。
 - 故障转移接口 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。
- 无法在 NAT 规则的源地址和远程访问 VPN 地址池中使用重叠地址。
- 有关 NAT 或 PAT 的应用检测限制，请参阅[默认检测和 NAT 限制](#)，第 245 页。
- 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 188 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。要解决这个问题，请指定映射接口。
- 如果在规则中指定目标接口，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。
- 如果对用于连接 NFS 服务器的 Sun RPC 流量使用 PAT，请注意，在通过 PAT 方式转换的端口号大于 1024 时，NFS 服务器可能会拒绝连接。NFS 服务器的默认配置是拒绝来自端口号大于 1024 的连接。错误通常为“权限被拒”。如果在较小范围内的端口不可用时选择“扁平范围”选项来使用更高的端口号，则可能会映射编号大于 1024 的端口，尤其是在未选择将较小范围包含在扁平范围内的选项时。如果不选择将保留端口 (1-1023) 包括在 PAT 池的端口范围内的选项，则系统会映射高于 1024 的端口。您可以通过将 NFS 服务器配置更改为允许所有端口号来避免此问题。
- NAT 仅适用于直通流量。系统生成的流量不进行 NAT。

- 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。使用 **asp rule-engine transactional-commit nat** 命令。
- 请不要使用大写或小写字母的任意组合来命名网络对象或组 **pat-pool**。
- 单向选项主要用于测试目的，可能不适用于所有协议。例如，SIP 要求执行协议检查以使用 NAT 转换 SIP 报头，但如果将转换设为单向，则不会发生这种情况。
- 不能在协议无关组播 (PIM) 寄存器的内部负载上使用 NAT。
- (两次 NAT) 为双 ISP 接口设置（使用路由配置中的服务级别协议的主接口和备用接口）编写 NAT 规则时，请勿在规则中指定目标条件。确保主接口的规则在备用接口的规则之前。这允许设备在主 ISP 不可用时根据当前路由状态选择正确的 NAT 目的接口。如果指定目标对象，NAT 规则将始终为其他规则选择主接口。
- 如果您收到不应与为接口定义的 NAT 规则匹配的流量的 ASP drop reason nat-no-xlate-to-pat-pool，请为受影响的流量配置身份 NAT 规则，以便流量可以不经转换地通过。
- 如果为 GRE 隧道终端配置 NAT，则您必须在终端上禁用保持连接，否则将无法建立隧道。终端将保持连接发送到原始地址。
- DHCP 和 BOOTP 共享端口 UDP/67-68。由于 BOOTP 已经过时，如果同时运行 DHCP，为 bootps 端口编写 NAT 规则可能会导致端口分配问题。请考虑使用 DHCP 中继来传输网段之间的 DHCP 请求。

映射地址对象的网络对象 NAT 准则

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。使用 **object network** 和 **object-group network** 命令创建对象。

为映射地址创建对象时，请注意以下准则。

- 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 准则](#)，第 134 页。
- 请不要使用大写或小写字母的任意组合来命名网络对象或组 **pat-pool**。
- 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。使用 **object network** 和 **object-group network** 命令创建对象。

为两次 NAT 创建对象时，请注意以下准则。

- 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 准则](#)，第 134 页。
- 请不要使用大写或小写字母的任意组合来命名网络对象或组 pat-pool。
- 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 129 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。
 - 您可以使用完全限定域名作为转换（映射）目标，例如 `www.example.com`。有关详细信息，请参阅[FQDN 目的准则](#)，第 138 页。

FQDN 目的准则

您可以使用完全限定域名 (FQDN) 网络对象而不是 IP 地址在两次 NAT 规则中指定转换（映射）目的。例如，您可以基于发往 `www.example.com` Web 服务器的流量创建规则。

使用 FQDN 时，系统基于返回的地址获取 DNS 解析并编写 NAT 规则。如果使用多个 DNS 服务器组，则系统会使用过滤器域，并根据过滤器从相应的组请求地址。如果从 DNS 服务器获取多个地址，则使用的地址基于以下条件：

- 如果某个地址与指定接口位于相同的子网上，则使用该地址。如果没有地址位于相同的子网上，则使用返回的第一个地址。
- 转换后的源和转换后的目的的 IP 类型必须匹配。例如，如果转换后的源地址为 IPv6，则 FQDN 对象必须指定 IPv6 作为地址类型。如果转换后的源为 IPv4，则 FQDN 对象必须指定 IPv4 作为地址类型。

不能在用于手动 NAT 目的的网络组中包含 FQDN 对象。在 NAT 中，必须单独使用 FQDN 对象，因为只有单个目的主机才适用于此类 NAT 规则。

如果 FQDN 无法解析为 IP 地址，则在获得 DNS 解析之前该规则不起作用。

实际和映射端口服务对象的两次 NAT 准则

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

使用 **object service** 命令创建对象。

为两次 NAT 创建对象时，请注意以下准则。

- 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。当您转换的主机访问目标网络时，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，目标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。远程主机的成功连接可重置连接的空闲计时器。

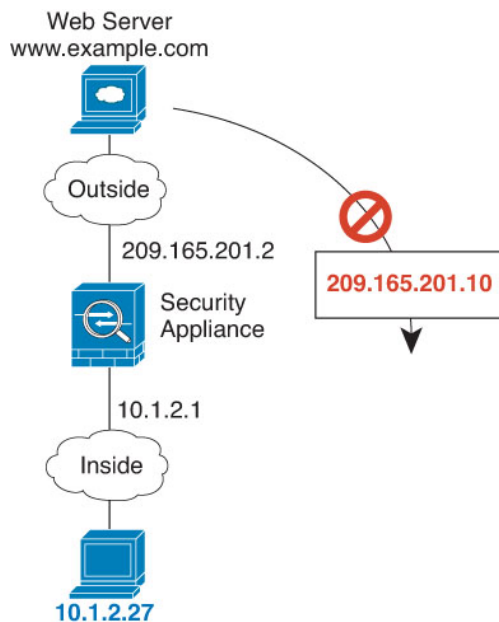
下图显示典型的动态 NAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。

图 8: 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 9: 远程主机尝试向映射地址发起连接



动态 NAT 的优缺点

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。

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 为映射地址创建主机或范围网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。

- 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。

步骤 2 创建或编辑要为其配置 NAT 的网络对象：**object network obj_name**

示例：

```
hostname(config)# object network my-host-obj1
```

步骤 3 （编辑具有正确地址的对象时，请跳过此步骤。）定义要转换的实际 IPv4 或 IPv6 地址。

- **host {IPv4_address | IPv6_address}** - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix}** - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **range start_address end_address** - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。

示例：

```
hostname(config-network-object)# host 10.2.2.2
```

步骤 4 为对象 IP 地址配置动态 NAT。只能为给定对象定义单一 NAT 规则。

```
nat [(real_ifc,mapped_ifc)] dynamic mapped_obj [interface [ipv6]] [dns]
```

其中：

- **Interfaces** - （对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any,outside），但 **any** 不适用于桥接组成员接口。
- **Mapped IP address** - 指定包括映射的 IP 地址的网络对象或网络对象组。
- **Interface PAT fallback** - （可选）**interface** 关键字启用接口 PAT 回退。在用尽映射 IP 地址后，使用映射接口的 IP 地址。如果指定 **ipv6**，则将使用接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）
- **DNS** - （可选）**dns** 关键字可以转换 DNS 应答。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 203 页。

示例：

```
hostname(config-network-object)# nat (inside,outside) dynamic MAPPED_IPS interface
```

示例

以下示例配置动态 NAT，将 192.168.2.0 网络隐藏在外地址 10.2.2.1 到 10.2.2.10 的范围后面：

```
hostname(config)# object network my-range-obj
hostname(config-network-object)# range 10.2.2.1 10.2.2.10
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

以下示例使用动态 PAT 备份配置 动态 NAT。内部网络 10.76.11.0 中的主机首先映射到 nat-range 1 池 (10.10.10.10-10.10.10.20)。分配 nat-range1 池中的所有地址之后，使用 pat-ip1 地址 (10.10.10.21) 执行动态 PAT。PAT 转换也用尽的可能性不大，即使发生这种情况，也可以使用外部接口地址执行动态 PAT。

```
hostname(config)# object network nat-range1
hostname(config-network-object)# range 10.10.10.10 10.10.10.20

hostname(config-network-object)# object network pat-ip1
hostname(config-network-object)# host 10.10.10.21
```

```
hostname(config-network-object)# object-group network nat-pat-grp
hostname(config-network-object)# network-object object nat-range1
hostname(config-network-object)# network-object object pat-ip1

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 10.76.11.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

以下示例使用动态 PAT 备份配置动态 NAT，将 IPv6 主机转换为 IPv4 主机。内部网络 2001:DB8::/96 上的主机首先映射到 IPv4_NAT_RANGE 池（209.165.201.1 到 209.165.201.30）。分配 IPv4_NAT_RANGE 池中的所有地址之后，使用 IPv4_PAT 地址（209.165.201.31）执行动态 PAT。在 PAT 转换也被用完的情况下，使用外部接口地址执行动态 PAT。

```
hostname(config)# object network IPv4_NAT_RANGE
hostname(config-network-object)# range 209.165.201.1 209.165.201.30

hostname(config-network-object)# object network IPv4_PAT
hostname(config-network-object)# host 209.165.201.31

hostname(config-network-object)# object-group network IPv4_GROUP
hostname(config-network-object)# network-object object IPv4_NAT_RANGE
hostname(config-network-object)# network-object object IPv4_PAT

hostname(config-network-object)# object network my_net_obj5
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

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 为源实际地址、源映射地址、目标实际地址和目标映射地址创建主机或范围网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。还可以将 FQDN 网络对象用于目标映射地址。

- 如果要转换所有源流量，则跳过为源实际地址添加对象，转而在 **nat** 命令中指定 **any** 关键字。
- 如果要配置仅支持端口转换的静态接口 NAT，则可跳过为目标映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。

如果创建对象，请注意以下准则：

- 通常要配置将较大实际地址组映射至较小的组。
- 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。

步骤 2（可选。）为目标实际端口和目标映射端口创建服务对象。

对于动态 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。

步骤 3 配置动态 NAT。

```
nat [(real_ifc,mapped_ifc)] [line | {after-auto [line]}] source dynamic {real_obj | any} {mapped_obj
[interface [ipv6]]} [destination static {mapped_obj | interface [ipv6]} real_obj] [service
mapped_dest_svc_obj real_dest_svc_obj] [dns] [unidirectional] [inactive] [description desc]
```

其中：

- **Interfaces** -（对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any、outside），但 **any** 不适用于桥接组成员接口。
- **Section and Line** -（可选。）默认情况下，NAT 规则将添加至 NAT 表的第 1 部分的末尾（请参阅 [NAT 规则顺序](#)，第 130 页）。如果要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。可以使用 *line* 参数在适用部分的任意位置插入规则。
- **源地址**：
 - **Real** - 指定网络对象、组或 **any** 关键字。
 - **Mapped** - 指定不同的网络对象或组。或者您可以选择配置以下回退方法：
 - **Interface PAT fallback** -（可选。）**interface** 关键字启用接口 PAT 回退。在用尽映射 IP 地址后，使用映射接口的 IP 地址。如果指定 **ipv6**，则将使用接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。（当映射接口为桥接组成员时，无法指定 **interface**）。
- **目标地址（可选）**：
 - **Mapped** - 指定网络对象或组，或对于仅支持端口转换的静态接口 NAT，指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如指定 **interface**，请务必也配置 **service** 关键字。对于此选项，必须为 *real_ifc* 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 158 页。
 - **Real** - 指定网络对象或组。对于身份 NAT，只需将相同的对象或组同时用于实际和映射地址。
- **Destination port** -（可选。）指定 **service** 关键字以及映射和实际服务对象。对于身份端口转换，只需相同的服务对象同时用于实际和映射端口。

- **DNS** - (可选; 适用于源专用规则。) **dns** 关键字转换 DNS 应答。确保启用 DNS 检测 (默认情况下启用)。如配置 **destination** 地址, 则无法配置 **dns** 关键字。有关详细信息, 请参阅 [使用 NAT 重写 DNS 查询和响应](#), 第 203 页。
- **Unidirectional** - (可选。) 指定 **unidirectional**, 以使目标地址无法发起流向源地址的流量。
- **Inactive** - (可选。) 要使此规则变为非活动状态而不必删除命令, 请使用 **inactive** 关键字。要将其重新激活, 请重新输入没有 **inactive** 关键字的整个命令。
- **Description** - (可选。) 使用 **description** 关键字可提供最多 200 个字符的说明。

示例:

```
hostname(config)# nat (inside,outside) source dynamic MyInsNet NAT_POOL
destination static Server1_mapped Server1 service MAPPED_SVC REAL_SVC
```

示例

以下示例在访问 209.165.201.1/27 网络上的服务器以及 203.0.113.0/24 网络上的服务器时为内部网络 10.1.1.0/24 配置动态 NAT。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
destination static SERVERS_2 SERVERS_2
```

以下示例在访问 IPv4 209.165.201.1/27 网络上的服务器以及 203.0.113.0/24 网络上的服务器时为 IPv6 内部网络 2001:DB8:AAAA::/96 配置动态 NAT:

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_1
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network MAPPED_2
hostname(config-network-object)# range 209.165.202.129 209.165.200.158
```

```

hostname(config)# object network SERVERS_1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224

hostname(config)# object network SERVERS_2
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1
destination static SERVERS_1 SERVERS_1
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2
destination static SERVERS_2 SERVERS_2

```

动态 PAT

以下主题介绍动态 PAT。

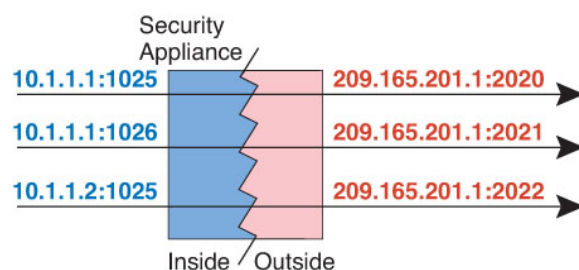
关于动态 PAT

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。

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 10: 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，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 的优缺点

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。

在同属一个网桥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成员或一个接口为网桥组成员，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。

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这种情况。

PAT 池对象准则

当为 PAT 池创建网络对象时，请遵守以下准则。

对于 PAT 池

- 端口会映射到 1024 到 65535 范围内的可用端口。您可以选择包含保留的端口，即 1024 以下的端口，以便让整个端口范围可用于转换。

在集群中运行时，每个地址的 512 个端口块会被分配给集群成员，并在这些端口块内进行映射。如果还启用块分配，则会根据块分配大小（其默认值也是 512）来分配端口。如果更改集群设备限制（集群大小），请确保清除转换或重新启动设备，以便将 PAT 池适当地重新分配到集群设备。

- 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) 的应用会获得 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，则另一条规则也必须指定扩展 PAT。
- 如果主机拥有现有连接，则来自该主机的后续连接会使用相同的 PAT IP 地址。如果没有可用的端口，这可能会阻止连接。使用轮询选项可避免此问题。
- 为获得最佳性能，请将 PAT 池中的 IP 地址数量限制为 10,000。

对于 PAT 池的扩展 PAT

- 许多应用检测不支持扩展 PAT。
- 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。

- 您不能在集群中的设备上使用扩展 PAT。
- 扩展 PAT 会增加设备上的内存使用率。

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”不能超越故障转移。如果该设备执行故障转移，来自主机的后续连接可能会使用初始 IP 地址。
- 如果在同一接口上混合使用 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

本节介绍如何为动态 PAT 配置网络对象 NAT。

过程

步骤 1 （可选。）为映射地址创建一个主机或范围网络对象（**object network** 命令）或网络对象组（**object-group network** 命令）。

- 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，对象或组不能包含子网；对象必须定义主机，或者对于 PAT 池，必须定义范围；组（对于 PAT 池）可以包含主机和范围。

步骤 2 创建或编辑要为其配置 NAT 的网络对象：**object network obj_name**

示例：

```
hostname(config)# object network my-host-obj1
```

步骤 3 （编辑具有正确地址的对象时，请跳过此步骤。）定义要转换的实际 IPv4 或 IPv6 地址。

- **host** {IPv4_address | IPv6_address} - 单一主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet** {IPv4_address IPv4_mask | IPv6_address / IPv6_prefix} - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。

- **rangestart_address end_address** - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。

示例:

```
hostname(config-network-object)# range 10.1.1.1 10.1.1.90
```

步骤 4 为对象 IP 地址配置 **dynamic PAT**。只能为给定对象定义单一 NAT 规则。

```
nat [(real_ifc,mapped_ifc)] dynamic {mapped_inline_host_ip | mapped_obj | pat-pool mapped-obj  
[round-robin] [extended] [include-reserve] [block-allocation] | interface [ipv6]} [interface [ipv6]]
```

其中:

- **Interfaces** - (对于桥接组成员接口需要填入。)指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下, 如果没有指定实际接口和映射接口, 则将使用所有接口。您也可以为一个或两个接口指定关键字 **any** (例如 any,outside), 但 **any** 不适用于桥接组成员接口。
- **Mapped IP address** - 可以将映射 IP 地址指定为:
 - *mapped_inline_host_ip* - 内联主机地址。
 - *mapped_obj* - 定义为主机地址的网络对象。
 - **pat-pool mapped-obj** - 包含多个地址的网络对象或组。
 - **interface [ipv6]** - 使用映射接口的 IP 地址作为映射地址。如果指定 **ipv6**, 则稍后使用该接口的 IPv6 地址。对于此选项, 必须为 *mapped_ifc* 配置一个特定接口。(当映射接口为桥接组成员时, 无法指定 **interface**。)要使用接口 IP 地址时, 必须使用此关键字; 不能内联输入或作为对象输入。
- 对于 PAT 池, 可以指定以下一个或多个选项:
 - **round-robin**- 为 PAT 池启用轮询地址分配。不使用轮询时, 默认情况下, 在使用下一个 PAT 地址前, 将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的地址/端口, 然后才返回再次使用第一个地址, 接着是第二个地址, 以此类推。
 - **extended**- 启用扩展 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。
 - **include-reserve** - 包括保留的端口 1-1023, 属于可用于地址转换的端口范围。如果不指定此选项, 地址将仅被转换为 1024-65535 范围内的端口。
 - **block-allocation**- 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 **round-robin** 兼容，但无法使用 **extended** 选项。也无法使用接口 PAT 回退。

- **Interface PAT fallback** - (可选。) 在主 PAT 地址后输入了 **interface [ipv6]** 关键字时，该关键字将启用接口 PAT 回退。主要 PAT 地址用尽后，接着将使用映射接口的 IP 地址。如果指定 **ipv6**，则稍后使用该接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置一个特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）

示例：

```
hostname(config-network-object)# nat (any,outside) dynamic interface
```

示例

以下示例配置动态 PAT，将 192.168.2.0 网络隐藏在地址 10.2.2.2 后面：

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 10.2.2.2
```

以下示例配置动态 PAT，将 192.168.2.0 网络隐藏在外部接口地址后面：

```
hostname(config)# object network my-inside-net
hostname(config-network-object)# subnet 192.168.2.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic interface
```

以下示例配置动态 PAT，使用 PAT 池将内部 IPv6 网络转换为外部 IPv4 网络：

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 203.0.113.1 203.0.113.254
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

配置动态两次 NAT

本节介绍如何为动态 PAT 配置两次 NAT。

过程

- 步骤 1** 为源实际地址、源映射地址、目的实际地址和目的映射地址创建主机或范围网络对象（**object network** 命令）或网络对象组（**object-group network** 命令）。还可以将 FQDN 网络对象用于目标映射地址。

- 如果要转换所有源流量，可以跳过为源实际地址添加对象，转而在 **nat** 命令中指定 **any** 关键字。
- 如果要使用接口地址作为映射地址，可以跳过为源映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。
- 如果要配置仅支持端口转换的静态接口 NAT，则可跳过为目的映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。

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。

步骤 2 （可选。）为目标实际端口和目标映射端口创建服务对象。

对于动态 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。

步骤 3 配置动态 PAT。

```
nat [(real_ifc,mapped_ifc)] [line | after-auto [line]] source dynamic {real_obj | any} {mapped_obj [interface [ipv6]] | pat-pool mapped_obj [round-robin] [extended] [include-reserve] [block-allocation] [interface [ipv6]] | interface [ipv6]} [destination static {mapped_obj | interface [ipv6]} real_obj] [service mapped_dest_svc_obj real_dest_svc_obj] [unidirectional] [inactive] [description description]
```

其中：

- Interfaces - （对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any** （例如 any,outside），但 **any** 不适用于桥接组成员接口。
- Section and Line - （可选。）默认情况下，NAT 规则将添加至 NAT 表的第 1 部分的末尾（请参阅 [NAT 规则顺序，第 130 页](#)）。如果要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。可以使用 *line* 参数在适用部分的任意位置插入规则。
- 源地址：
 - Real - 网络对象、组或 **any** 关键字。如果要转换从实际接口流向映射接口的所有流量，请使用 **any** 关键字。
 - Mapped - 配置以下其中一项：
 - Network object - 包含主机地址的网络对象。
 - **pat-pool mapped_obj** - 包含多个地址的网络对象或组。
 - **interface [ipv6]** - （仅路由模式。）使用映射接口的 IP 地址作为映射地址（接口 PAT）。如果指定 **ipv6**，则稍后使用该接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置一个特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）如果使用 PAT 池或网络对象指定此关键字，则会启用接口 PAT 回退。PAT IP 地址用尽后，接着将使用映射接口的 IP 地址。

对于 PAT 池，可以指定以下一个或多个选项：

- **round-robin**- 为 PAT 池启用轮询地址分配。不使用轮询时，默认情况下，在使用下一个 PAT 地址前，将分配 PAT 地址的所有端口。轮询方法分配来自池中每个 PAT 地址的地址/端口，然后才返回再次使用第一个地址，接着是第二个地址，以此类推。
 - **extended**- 启用扩展 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。
 - **include-reserve**- 包括保留的端口 1-1023，属于可用于地址转换的端口范围。如果不指定此选项，地址将仅被转换为 1024-65535 范围内的端口。
 - **block-allocation**- 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 **round-robin** 兼容，但无法使用 **extended** 选项。也无法使用接口 PAT 回退。
- 目标地址（可选）：
- **Mapped** - 指定网络对象或组，或对于仅支持端口转换的静态接口 NAT（仅限非桥接组成员接口），指定 **interface** 关键字。如果指定 **ipv6**，则稍后使用该接口的 IPv6 地址。如指定 **interface**，请务必也配置 **service** 关键字。对于此选项，必须为 **real_ifc** 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 158 页。
 - **Real** - 指定网络对象或组。对于身份 NAT，只需将相同的对象或组同时用于实际和映射地址。
- **Destination port** - （可选。）指定 **service** 关键字以及映射和实际服务对象。对于身份端口转换，只需相同的服务对象同时用于实际和映射端口。
- **Unidirectional** - （可选。）指定 **unidirectional**，以使目标地址无法发起流向源地址的流量。
- **Inactive** - （可选。）要使此规则变为非活动状态而不必删除命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。
- **Description** - （可选。）使用 **description** 关键字可提供最多 200 个字符的说明。

示例：

```
hostname(config)# nat (inside,outside) source dynamic MyInsNet interface
destination static Server1 Server1
description Interface PAT for inside addresses when going to server 1
```

示例

以下示例为内部网络 192.168.1.0/24 配置访问外部 Telnet 服务器 209.165.201.23 时的接口 PAT，以及访问 203.0.113.0/24 网络上任何服务器时使用 PAT 池的动态 PAT。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 209.165.200.225 209.165.200.254

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 209.165.201.23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 203.0.113.0 255.255.255.0

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface
destination static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

以下示例为内部网络 192.168.1.0/24 配置访问外部 IPv6 Telnet 服务器 2001:DB8::23 时的接口 PAT，以及访问 2001:DB8:AAAA::/96 网络上任何服务器时使用 PAT 池的动态 PAT。

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0

hostname(config)# object network PAT_POOL
hostname(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200

hostname(config)# object network TELNET_SVR
hostname(config-network-object)# host 2001:DB8::23

hostname(config)# object service TELNET
hostname(config-service-object)# service tcp destination eq 23

hostname(config)# object network SERVERS
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6
destination static TELNET_SVR TELNET_SVR service TELNET TELNET
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

使用端口块分配配置 PAT

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）。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。TCP、UDP 和 ICMP 连接有单独的数据块，并且这些数据块可以重叠。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) 的应用会获得 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：

- 可以包括 **round-robin** 关键字，但不能包括 **extended**、**include-reserve** 或 **interface**（用于接口 PAT 回退）。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。但是，在集群中运行时，必须重新加载集群，以便设备可以正确分发块。



注释 如果要在常规 PAT 和块分配 PAT 规则之间切换，您必须先删除规则，然后再清除转换。然后，您可以创建新的对象 NAT 规则。否则，您将在 **show asp drop** 输出中看到 **pat-port-block-state-mismatch** 丢弃。

- 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（可选。）配置块分配大小，即每个块中的端口数。

xlate block-allocation size value

范围为 32-4096。默认值为 512。使用 “no” 形式可恢复默认值。

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。

步骤 2（可选。）配置每个主机可分配的最大块数。

xlate block-allocation maximum-per-host number

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。使用 “no” 形式可恢复默认值。

步骤 3（可选。）启用临时系统日志生成。

xlate block-allocation pba-interim-logging seconds

默认情况下，系统会在端口块创建和删除操作发生时生成系统日志消息。如果启用临时日志记录，系统会按您指定的时间间隔生成以下消息。这些消息会报告消息生成时所有已分配的活动端口块，包括协议（ICMP、TCP、UDP、源和目标接口与 IP 地址，以及端口块。可以指定 21600 至 604800 秒（6 小时至 7 天）的时间间隔。

%ASA-6-305017: Pba-interim-logging: Active *protocol* block of ports for translation from *real_interface:real_host_ip* to *mapped_interface:mapped_ip_address/start_port_num-end_port_num*

示例：

```
ciscoasa(config)# xlate block-allocation pba-interim-logging 21600
```

步骤 4 添加使用 PAT 池块分配的 NAT 规则。

- 对象 PAT。

nat [(*real_ifc*,*mapped_ifc*)] dynamic pat-pool *mapped-obj* block-allocation

示例：

```
object network mapped-pat-pool
  range 10.100.10.1 10.100.10.2
object network src_host
  host 10.111.10.15
object network src_host
  nat (inside,outside) dynamic
pat-pool mapped-pat-pool block-allocation
```

- 两次 PAT。

nat [(*real_ifc*,*mapped_ifc*)] [*line* | **after-auto [*line*]] source dynamic *real_obj* pat-pool*mapped-obj* block-allocation**

示例：

```
object network mapped-pat-pool
  range 10.100.10.1 10.100.10.2
object network src_network
  subnet 10.100.10.0 255.255.255.0
nat (inside,outside) 1 source dynamic src_network
pat-pool mapped-pat-pool block-allocation
```

配置每会话 PAT 或多会话 PAT

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控制单元所有。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：

```
xlate per-session permit tcp any4 any4
xlate per-session permit tcp any4 any6
xlate per-session permit tcp any6 any4
xlate per-session permit tcp any6 any6
xlate per-session permit udp any4 any4 eq domain
xlate per-session permit udp any4 any6 eq domain
xlate per-session permit udp any6 any4 eq domain
xlate per-session permit udp any6 any6 eq domain
```

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：

```
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
```

过程

创建允许或拒绝每会话 PAT 规则。此规则置于默认规则上方，但在任何其他手动创建的规则下方。确保按照所需的应用顺序创建规则。

xlate per-session {permit | deny} {tcp | udp} source_ip [operator src_port] destination_ip [operator dest_port]

对于源 IP 地址和目标 IP 地址，可以配置以下选项：

- **host ip_address** - 指定 IPv4 或 IPv6 主机地址。
- **ip_address mask** - 指定 IPv4 网络地址和子网掩码。
- **ipv6-address/prefix-length** - 指定 IPv6 网络地址和前缀。
- **any4** 和 **any6** - **any4** 指定纯 IPv4 流量；**any6** 则指定 any6 流量。

运算符与源或目标使用的端口号相匹配。默认为所有端口。允许的运算符如下所示：

- **lt** - 小于
- **gt** - 大于
- **eq** - 等于
- **neq** - 不等于
- **range** - 值的范围（包括边界值）。使用该操作符时，请指定两个端口编号，例如，**range 100 200**。

示例

以下示例为 H.323 流量创建拒绝规则，以便它使用多会话 PAT：

```
hostname(config)# xlate per-session deny tcp any4 209.165.201.7 eq 1720
hostname(config)# xlate per-session deny udp any4 209.165.201.7 range 1718 1719
```

以下示例通过允许将每会话 PAT 用于 SIP UDP 端口，启用了跨集群成员分配 SIP。每会话 PAT 是 SIP TCP 端口的默认值，因此除非您更改了默认规则，否则无需 TCP 规则。

```
hostname(config)# xlate per-session permit udp any4 any4 eq sip
```

静态 NAT

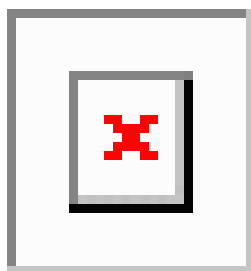
以下主题介绍静态 NAT 以及如何实施静态 NAT。

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 11: 静态 NAT



注释 如果需要，可以禁用双向性。

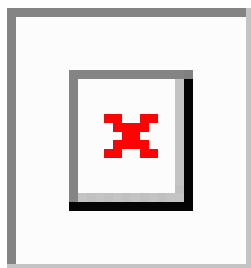
支持端口转换的静态 NAT

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 12: 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 181 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

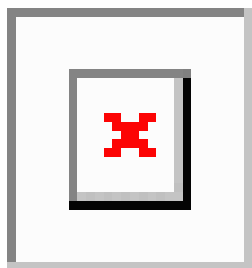
可以配置静态 NAT，以将一个实际地址映射到一个接口地址/端口组合。例如，如果要将对设备外部接口的 Telnet 访问重定向至内部主机，则可以将内部主机 IP 地址/端口 23 映射到外部接口地址/端口 23。

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。

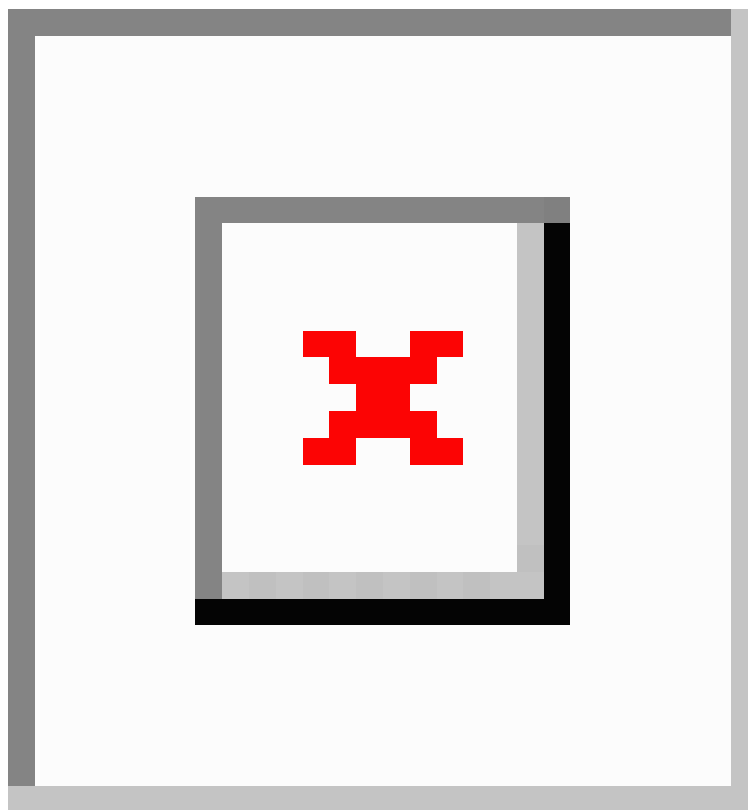
下图显示典型的一对多静态 NAT 场景。由于实际主机进行的发起的流量始终使用第一个映射地址，因此从技术上说，实际主机 IP/第一个映射 IP 的转换是唯一的单向转换。

图 13: 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 180 页。

图 14: 一对多静态 NAT 示例



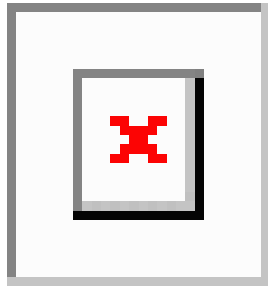
其他映射场景（不推荐）

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，依此类推，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 15: 少对多静态 NAT



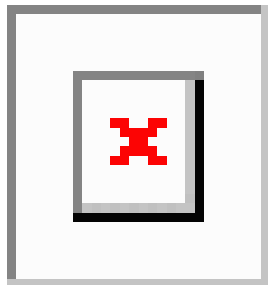
对于实际地址多于映射地址的多对少或多对一配置，映射地址会在实际地址用尽之前先用尽。仅最低实际 IP 地址和映射池之间的映射可以导致双向发起。剩余的更高的实际地址可以发起流量，但不能将流量发起到这些地址（由于五元组 [源 IP、目标 IP、源端口、目标端口、协议] 的唯一性，连接的返回流量会定向到正确的实际地址）。



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 16: 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 （可选。）为映射地址创建网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。

- 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。

步骤 2 创建或编辑要为其配置 NAT 的网络对象：**object network obj_name**

示例：

```
hostname(config)# object network my-host-obj1
```

步骤 3 （编辑具有正确地址的对象时，请跳过此步骤。）定义要转换的实际 IPv4 或 IPv6 地址。

- **host** {IPv4_address | IPv6_address} - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet** {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix} - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **range** start_address end_address - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。

示例：

```
hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0
```

步骤 4 为对象 IP 地址配置静态 NAT。只能为给定对象定义单一 NAT 规则。

```
nat [(real_ifc,mapped_ifc)] static {mapped_inline_host_ip | mapped_obj} [interface [ipv6]] [net-to-net]
[dns | service {tcp | udp | sctp} real_port mapped_port] [no-proxy-arp]
```

其中：

- **Interfaces** - （对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any,outside），但 **any** 不适用于桥接组成员接口。
- **Mapped IP address** - 可以将映射 IP 地址指定为以下任一地址：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。请参阅[静态 NAT，第 157 页](#)。
 - **mapped_inline_host_ip** - 内联主机 IP 地址。此项为主机对象提供一对一映射。对于子网对象，内联主机地址使用的是相同的掩码，而映射的内联主机子网中的地址则是一一对应的。对于范围对象，映射地址包括范围对象中相同数量的主机，从映射主机地址开始。例如，如果实际地址定义为 10.1.1.1 到 10.1.1.6 的范围，并且将 172.20.1.1 指定为映射地址，则映射范围将包括 172.20.1.1 到 172.20.1.6。对于 NAT46 或 NAT66 转换，此项可以是 IPv6 网络地址。
 - **mapped_obj** - 现有网络对象或组。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。

- **interface** - (仅限支持端口转换的静态 NAT。)映射接口的 IP 地址用作映射地址。如果指定 **ipv6**，则将使用接口的 IPv6 地址。对于此选项，必须为 *mapped_ifc* 配置特定接口。(当映射接口为桥接组成员时，无法指定 **interface**。)要使用接口 IP 地址时，必须使用此关键字；不能内联输入或作为对象输入。另请确保配置 **service** 关键字。
- **Net-to-net** - (可选。)对于 NAT 46，指定 **net-to-net** 以将第一个 IPv4 地址转换为第一个 IPv6 地址，第二个 IPv4 地址转换为第二个 IPv6 地址，以此类推。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。
- **DNS** - (可选)。**dns** 关键字转换 DNS 应答。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 203 页](#)。
- **Port translation** - (仅带端口转换的静态 NAT。)指定具有所需端口关键字的 **service** 以及实际与映射端口。可以输入端口号或已知的端口名称（例如 **http**）。
- **No Proxy ARP** - (可选。)指定 **no-proxy-arp**，为映射 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 188 页](#)。

示例:

```
hostname(config-network-object)#  
nat (inside,outside) static MAPPED_IPS service tcp 80 8080
```

示例

以下示例为内部的实际主机 10.1.1.1 到外部的 10.2.2.2 配置静态 NAT，启用 DNS 重写。

```
hostname(config)# object network my-host-obj1  
hostname(config-network-object)# host 10.1.1.1  
hostname(config-network-object)# nat (inside,outside) static 10.2.2.2 dns
```

以下示例为内部的实际主机 10.1.1.1 到外部的 10.2.2.2 配置使用映射对象的静态 NAT。

```
hostname(config)# object network my-mapped-obj  
hostname(config-network-object)# host 10.2.2.2  
  
hostname(config-network-object)# object network my-host-obj1  
hostname(config-network-object)# host 10.1.1.1  
hostname(config-network-object)# nat (inside,outside) static my-mapped-obj
```

以下示例为 TCP 端口 21 上的 10.1.1.1 到端口 2121 上的外部接口配置支持端口转换的静态 NAT。

```
hostname(config)# object network my-ftp-server  
hostname(config-network-object)# host 10.1.1.1  
hostname(config-network-object)# nat (inside,outside) static interface service tcp 21 2121
```

以下示例将内部 IPv4 网络映射到外部 IPv6 网络。

```
hostname(config)# object network inside_v4_v6
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

以下示例将内部 IPv6 网络映射到外部 IPv6 网络。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96
hostname(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

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 为源实际地址、源映射地址、目标实际地址和目标映射地址创建主机或范围网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。还可以将 FQDN 网络对象用于目标映射地址。

- 如果仅要配置支持端口转换的源静态接口 NAT，则可跳过为源映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。
- 如果要配置仅支持端口转换的静态接口 NAT，则可跳过为目标映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。

如果创建对象，请注意以下准则：

- 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。有关详细信息，请参阅[静态 NAT，第 157 页](#)。

步骤 2 （可选。）为以下端口创建服务对象：

- 源或目标实际端口
- 源或目标映射端口

服务对象可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。

步骤 3 配置静态 NAT。


```
nat [(real_ifc,mapped_ifc)] [line | {after-object [line]}] source static real_ob [mapped_obj | interface [ipv6]]
[destination static {mapped_obj | interface [ipv6]} real_obj] [service real_src_mapped_dest_svc_obj
mapped_src_real_dest_svc_obj] [net-to-net] [dns] [unidirectional | no-proxy-arp] [inactive] [description
desc]
```

其中：

- **Interfaces** - （对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any、outside），但 **any** 不适用于桥接组成员接口。
- **Section and Line** - （可选。）默认情况下，NAT 规则将添加至 NAT 表的第 1 部分的末尾（请参阅 [NAT 规则顺序，第 130 页](#)）。如果要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。可以使用 *line* 参数在适用部分的任意位置插入规则。
- **源地址**：
 - **Real** - 指定网络对象或组。请勿使用 **any** 关键字，此关键字用于身份 NAT。
 - **Mapped** - 指定不同的网络对象或组。仅可为支持端口转换的静态接口 NAT 指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如果指定 **interface**，请务必也配置 **service** 关键字（在此情况下，服务对象应仅包括源端口）。对于此选项，必须为 *mapped_ifc* 配置特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）有关详细信息，请参阅 [支持端口转换的静态 NAT，第 158 页](#)。
- **目标地址（可选）**：
 - **Mapped** - 指定网络对象或组，或对于仅支持端口转换的静态接口 NAT，指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如果指定 **interface**，请务必也配置 **service** 关键字（在此情况下，服务对象应仅包括目标端口）。对于此选项，必须为 *real_ifc* 配置特定接口。（当映射接口为桥接组成员时，无法指定 **interface**。）
 - **Real** - 指定网络对象或组。对于身份 NAT，只需将相同的对象或组同时用于实际和映射地址。
- **Ports** - （可选。）指定 **service** 关键字以及实际和映射服务对象。对于源端口转换，对象必须指定源服务。对于源端口转换，命令中服务对象的顺序为 **service real_obj mapped_obj**。对于目标端口转换，对象必须指定目标服务。对于目标端口转换，服务对象的顺序为 **service mapped_obj real_obj**。在极少数的情况下，会在对象中同时指定源和目标端口，第一个服务对象包含实际源端口/映射目标端口；第二个服务对象包含映射源端口/实际目标端口。对于身份端口转换，只需将相同的服务对象同时用于实际和映射端口（源和/或目标端口，具体取决于配置）。
- **Net-to-net** - （可选。）对于 NAT 46，指定 **net-to-net** 以将第一个 IPv4 地址转换为第一个 IPv6 地址，第二个 IPv4 地址转换为第二个 IPv6 地址，以此类推。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。
- **DNS** - （可选；适用于源专用规则。）**dns** 关键字转换 DNS 应答。确保启用 DNS 检测（默认情况下启用）。如配置 **destination** 地址，则无法配置 **dns** 关键字。有关详细信息，请参阅 [使用 NAT 重写 DNS 查询和响应，第 203 页](#)。

- Unidirectional - (可选。)指定 **unidirectional**，以使目标地址无法发起流向源地址的流量。
- No Proxy ARP - (可选。)指定 **no-proxy-arp**，为映射 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 188 页。
- Inactive - (可选。)要使此规则变为非活动状态而不必删除命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。
- Description - (可选。)使用 **description** 关键字可提供最多 200 个字符的说明。

示例：

```
hostname(config)# nat (inside,dmz) source static MyInsNet MyInsNet_mapped
destination static Server1 Server1 service REAL_SRC_SVC MAPPED_SRC_SVC
```

示例

以下示例展示支持端口转换的静态接口 NAT 的用途。外部主机通过目标端口 65000 至 65004 连接至外部接口 IP 地址，从而访问内部 FTP 服务器。流量通过 65004 未经转换地发送至位于 192.168.10.100:6500 的内部 FTP 服务器。请注意，应在服务对象中指定源端口范围（而不是指定目标端口），因为要在命令中将源地址和端口转换为已标识状态；目标端口为“any”。由于静态 NAT 是双向的，“源”和“目标”主要指命令关键字；数据包中的实际源和目标地址与端口取决于发送数据包的主机。在此示例中，连接源自外部，通向内部，因此，FTP 服务器的“源”地址和端口实际是源数据包中的目标地址和端口。

```
hostname(config)# object service FTP_PASV_PORT_RANGE
hostname(config-service-object)# service tcp source range 65000 65004

hostname(config)# object network HOST_FTP_SERVER
hostname(config-network-object)# host 192.168.10.100

hostname(config)# nat (inside,outside) source static HOST_FTP_SERVER interface
service FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

以下示例显示访问 IPv6 网络时从一个 IPv6 网络到另一个 IPv6 的静态转换，以及访问 IPv4 网络时到 IPv4 PAT 池的动态 PAT 转换：

```
hostname(config)# object network INSIDE_NW
hostname(config-network-object)# subnet 2001:DB8:AAAA::/96

hostname(config)# object network MAPPED_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:BBBB::/96

hostname(config)# object network OUTSIDE_IPv6_NW
hostname(config-network-object)# subnet 2001:DB8:CCCC::/96

hostname(config)# object network OUTSIDE_IPv4_NW
hostname(config-network-object)# subnet 10.1.1.0 255.255.255.0

hostname(config)# object network MAPPED_IPv4_POOL
hostname(config-network-object)# range 10.1.2.1 10.1.2.254
```

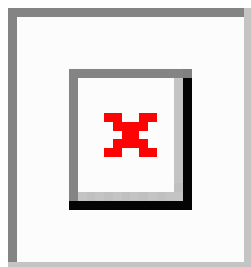
```
hostname(config)# nat (inside,outside) source static INSIDE_NW MAPPED_IPv6_NW
destination static OUTSIDE_IPv6_NW OUTSIDE_IPv6_NW
hostname(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool MAPPED_IPv4_POOL
destination static OUTSIDE_IPv4_NW OUTSIDE_IPv4_NW
```

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 是远程访问访问 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 17: 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 （可选。）为映射地址创建网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。

- 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。

步骤 2 创建或编辑要为其配置 NAT 的网络对象：**object network *obj_name***

对象必须不同于用于映射地址的对象，虽然每个对象中的内容必须相同。

示例：

```
hostname(config)# object network my-host-obj1
```

步骤 3 （编辑具有正确地址的对象时，请跳过此步骤。）定义要转换的实际 IPv4 或 IPv6 地址。

- **host** {IPv4_address | IPv6_address} - 单台主机的 IPv4 或 IPv6 地址。例如，10.1.1.1 或 2001:DB8::0DB8:800:200C:417A。
- **subnet** {IPv4_address IPv4_mask | IPv6_address/IPv6_prefix} - 网络地址。对于 IPv4 子网，请在空格后添加掩码，例如，10.0.0.0 255.0.0.0。对于 IPv6，请将地址和前缀作为一个整体（不带空格），例如 2001:DB8:0:CD30::/60。
- **range** start_address end_address - 地址的范围。可以指定 IPv4 或 IPv6 范围。请勿包含掩码或前缀。

示例：

```
hostname(config-network-object)# subnet 10.2.1.0 255.255.255.0
```

步骤 4 为对象 IP 地址配置身份 NAT。只能为给定对象定义单一 NAT 规则。

nat [(real_ifc,mapped_ifc)] **static** {mapped_inline_host_ip | mapped_obj} [**no-proxy-arp**] [**route-lookup**]

其中：

- **Interfaces** - （对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 any、outside），但 **any** 不适用于桥接组成员接口。
- **Mapped IP addresses** - 确保为映射地址和实际地址配置相同的 IP 地址。使用以下选项之一：
 - *mapped_inline_host_ip* - 内联主机 IP 地址。对于主机对象，请指定相同的地址。对于范围对象，请指定实际范围中的第一个地址（将使用范围中的相同地址数量）。对于子网对象，请指定实际子网中的任何地址（将使用子网中的所有地址）。
 - *mapped_obj* - 包含与实际对象相同地址的网络对象或组。
- **No Proxy ARP** - （可选。）指定 **no-proxy-arp**，为映射 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 188 页。
- **Route lookup** - （仅路由模式；已指定接口。）指定 **route-lookup** 以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 190 页。

示例：

```
hostname(config-network-object)# nat (inside,outside) static MAPPED_IPS
```

示例

以下示例使用内联映射地址将主机地址映射到它本身：

```
hostname(config)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static 10.1.1.1
```

以下示例使用网络对象 将主机地址映射到它本身：

```
hostname(config)# object network my-host-obj1-identity
hostname(config-network-object)# host 10.1.1.1

hostname(config-network-object)# object network my-host-obj1
hostname(config-network-object)# host 10.1.1.1
hostname(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

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 为源实际地址（通常应为源映射地址使用相同对象）、目标实际地址和目标映射地址创建主机或范围网络对象（使用 **object network** 命令）或网络对象组（使用 **object-group network** 命令）。还可以将 FQDN 网络对象用于目标映射地址。

- 如果要为所有地址执行身份 NAT，则可跳过为源实际地址创建对象，转而在 **nat** 命令中使用关键字 **any any**。
- 如果要配置仅支持端口转换的静态接口 NAT，则可跳过为目标映射地址添加对象，转而在 **nat** 命令中指定 **interface** 关键字。

如果创建对象，请注意以下准则：

- 映射对象或组可能包含主机、范围或子网。
- 实际源对象和映射源对象必须匹配。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。

步骤 2 （可选。）为以下端口创建服务对象：

- 源或目标实际端口
- 源或目标映射端口

服务对象可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。

步骤 3 配置身份 NAT。

```
nat [(real_ifc,mapped_ifc)] [line | {after-object [line]}] source static {nw_obj nw_obj | any any} [destination
static {mapped_obj | interface [ipv6]} real_obj] [service real_src_mapped_dest_svc_obj
mapped_src_real_dest_svc_obj] [no-proxy-arp] [route-lookup] [inactive] [description desc]
```

其中：

- **Interfaces** - （对于桥接组成员接口需要填入。）指定实际 (*real_ifc*) 接口和映射 (*mapped_ifc*) 接口。确保包含圆括号。在路由模式下，如果没有指定实际接口和映射接口，则将使用所有接口。您也可以为一个或两个接口指定关键字 **any**（例如 *any*、*outside*），但 **any** 不适用于桥接组成员接口。
- **Section and Line** - （可选。）默认情况下，NAT 规则将添加至 NAT 表的第 1 部分的末尾（请参阅 [NAT 规则顺序，第 130 页](#)）。如果要转而将规则添加至第 3 部分（位于网络对象 NAT 规则之后），则可使用 **after-auto** 关键字。可以使用 *line* 参数在适用部分的任意位置插入规则。
- **Source addresses** - 同时为实际和映射地址指定网络对象、组或 **any** 关键字。
- **目标地址（可选）**：
 - **Mapped** - 指定网络对象或组，或对于仅支持端口转换的静态接口 NAT，指定 **interface** 关键字。如果指定 **ipv6**，则将使用接口的 IPv6 地址。如果指定 **interface**，请务必也配置 **service** 关键字（在此情况下，服务对象应仅包括目标端口）。对于此选项，必须为 *real_ifc* 配置特定接口。（当实际接口为桥接组成员时，无法指定 **interface**。）
 - **Real** - 指定网络对象或组。对于身份 NAT，只需将相同的对象或组同时用于实际和映射地址。
- **Ports** - （可选。）指定 **service** 关键字以及实际和映射服务对象。对于源端口转换，对象必须指定源服务。对于源端口转换，命令中服务对象的顺序为 **service real_obj mapped_obj**。对于目标端口转换，对象必须指定目标服务。对于目标端口转换，服务对象的顺序为 **service mapped_obj real_obj**。在极少数的情况下，会在对象中同时指定源和目标端口，第一个服务对象包含实际源端口/映射目标端口；第二个服务对象包含映射源端口/实际目标端口。对于身份端口转换，只需将相同的服务对象同时用于实际和映射端口（源和/或目标端口，具体取决于配置）。
- **No Proxy ARP** - （可选。）指定 **no-proxy-arp**，为映射 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 188 页](#)。
- **Route lookup** - （可选、仅路由模式、已指定接口。）指定 **route-lookup** 以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 190 页](#)。
- **Inactive** - （可选。）要使此规则变为非活动状态而不必删除命令，请使用 **inactive** 关键字。要将其重新激活，请重新输入没有 **inactive** 关键字的整个命令。
- **Description** - （可选。）使用 **description** 关键字可提供最多 200 个字符的说明。

示例：

```
hostname(config)# nat (inside,outside) source static MyInsNet MyInsNet
destination static Server1 Server1
```

监控 NAT

要监控 NAT，请使用以下命令：

- **show nat**

显示 NAT 统计信息，包括每条 NAT 规则的命中信息。

- **show nat pool**

显示 NAT 池统计信息，包括已分配的地址和端口，及其分配次数。

- **show running-config nat**

显示 NAT 配置。不能使用 **show running-config object** 查看对象 NAT 规则。当使用无修饰符的 **show running-config** 命令时，包含 NAT 规则的对象会显示两次，第一次随基本地址配置一起显示，然后在使用 NAT 规则的对象配置中显示一次。完整的对象不与地址和 NAT 规则作为整体一起显示。

- **show xlate**

显示当前 NAT 会话信息。

NAT 的历史记录

功能名称	平台版本	说明
网络对象 NAT	8.3(1)	为网络对象 IP 地址配置 NAT。 引入或修改了以下命令： nat （对象网络配置模式）、 show nat 、 show xlate 、 show nat pool 。
两次 NAT	8.3(1)	两次 NAT 可供您在单一规则中同时标识源和目标地址。 修改或引入了以下命令： nat 、 show nat 、 show xlate 、 show nat pool 。

功能名称	平台版本	说明
身份 NAT 可配置代理 ARP 和路由查找	8.4(2)/8.5(1)	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。 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。 修改了以下命令：nat static [no-proxy-arp] [route-lookup]。
PAT 池和轮询地址分配	8.4(2)/8.5(1)	现在，您可以指定 PAT 地址池，而不是单一地址。或者还可以启用 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。 修改了以下命令：nat dynamic [pat-pool mapped_object [round-robin]] 和 nat source dynamic [pat-pool mapped_object [round-robin]]。
轮询 PAT 池分配技术使用现有主机的相同 IP 地址	8.4(3)	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。 未修改任何命令。 此功能在 8.5(1) 或 8.6(1) 中不可用。

功能名称	平台版本	说明
用于 PAT 池的不分段 PAT 端口范围	8.4(3)	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。 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。 修改了以下命令：nat dynamic [pat-pool mapped_object [flat [include-reserve]]] 和 nat source dynamic [pat-pool mapped_object [flat [include-reserve]]]。 此功能在 8.5(1) 或 8.6(1) 中不可用。
用于 PAT 池的扩展 PAT	8.4(3)	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。 修改了以下命令：nat dynamic [pat-pool mapped_object [extended]] 和 nat source dynamic [pat-pool mapped_object [extended]]。 此功能在 8.5(1) 或 8.6(1) 中不可用。

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)	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。 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。 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： • 仅支持 Cisco IPsec 和 Secure 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）。 引入了以下命令：nat-assigned-to-public-ip interface（tunnel-group general-attributes 配置模式）。
NAT 支持 IPv6	9.0(1)	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。 修改了以下命令：nat（全局和对象网络配置模式）、show nat、show nat pool、show xlate。
NAT 支持反向 DNS 查找	9.0(1)	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。

功能名称	平台版本	说明
每会话 PAT	9.0(1)	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控制单元所有。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。 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。 引入了以下命令：xlate per-session、show nat pool。
NAT 规则引擎上的事务提交模式	9.3(1)	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。 我们已将 nat 关键字添加至以下命令：asp rule-engine transactional-commit、show running-config asp rule-engine transactional-commit、clear configure asp rule-engine transactional-commit。 我们向以下屏幕中添加了 NAT：Configuration > Device Management > Advanced > Rule Engine。
对运营商级 NAT 的改进	9.5(1)	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）。 添加了以下命令：xlate block-allocation size、xlate block-allocation maximum-per-host。向 nat 命令中添加了 block-allocation 关键词。
SCTP 的 NAT 支持	9.5(2)	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。 修改了以下命令：nat static (object)。

功能名称	平台版本	说明
NAT 端口块分配的临时日志。	9.12(1)	当对 NAT 启用端口块分配功能后，系统会在端口块创建和删除操作发生时生成系统日志消息。如果启用临时日志，系统会按您指定的时间间隔生成消息 305017。这些消息会报告消息生成时所有已分配的活动端口块，包括协议（ICMP、TCP、UDP、源和目标接口与 IP 地址，以及端口块。 添加了以下命令：xlate block-allocation pba-interim-logging seconds。
集群中对PAT地址分配的更改。PAT 池 flat 选项现在已默认启用，并且不可配置。	9.15(1)	更改PAT地址分配给集群成员的方式。以前，地址是分配给集群成员的，因此您的PAT池每个集群成员至少需要一个地址。现在，控制设备改为将每个PAT池地址划分为大小相等的端口块，并在集群成员之间分配它们。每个成员都有相同 PAT 地址的端口块。因此，您可以根据通常需要 PAT 的连接数量，将 PAT 池的大小减小到一个 IP 地址。能在 1024-65535 范围内，在 512 端口块中分配端口块。配置 PAT 池规则时，可以选择在此块分配中包含保留端口 1-1023。例如，在4节点集群中，每个节点获得32个数据块，与每个PAT池IP地址处理65535个连接的单个节点相比，它能够处理每个PAT池IP地址16384个连接。 作为此更改的一部分，所有系统的PAT池（无论是独立系统还是在集群中运行）现在都使用1023-65535的平面端口范围。以前，您可以通过在 PAT 池 flat 规则中包含关键字，选择性地使用平面范围。不再支持 flat 关键字：PAT 池现在始终为平面。include-reserve 关键字以前是 flat 的子关键字，现在则是 PAT 池配置中的独立关键字。使用此选项，您可以在 PAT 池中包括 1-1023 端口范围。 请注意，如果配置端口块分配（block-allocation PAT 池选项），则会使用块分配大小，而不是默认的 512 端口块。此外，不能为集群中的系统的PAT池配置扩展PAT。 新增/修改的命令：nat、show nat pool
新增的系统定义的 NAT 规则的第 0 部分。	9.16 (1)	向 NAT 规则表添加了新的第 0 部分。此部分专门供系统使用。系统正常运行所需的任何 NAT 规则都添加到此部分，这些规则优先于您创建的任何规则。以前，系统定义的规则添加到第 1 部分，用户定义的规则可能会干扰系统的正常运行。您无法添加、编辑或删除第 0 部分中的规则，但您会在 show nat detail 命令输出中看到这些规则。
两次 NAT 支持完全限定域名 (FQDN) 对象作为转换（映像）目的。	9.17(1)	您可以使用 FQDN 网络对象（例如指定 www.example.com 的网络对象）作为二次 NAT 规则中的转换（映射）目标地址。系统根据 DNS 服务器返回的 IP 地址配置规则。



第 9 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 177 页](#)
- [两次 NAT 的示例，第 182 页](#)
- [路由和透明防火墙模式下的 NAT，第 186 页](#)
- [路由 NAT 数据包，第 188 页](#)
- [用于 VPN 的 NAT，第 191 页](#)
- [转换 IPv6 网络，第 197 页](#)
- [使用 NAT 重写 DNS 查询和响应，第 203 页](#)

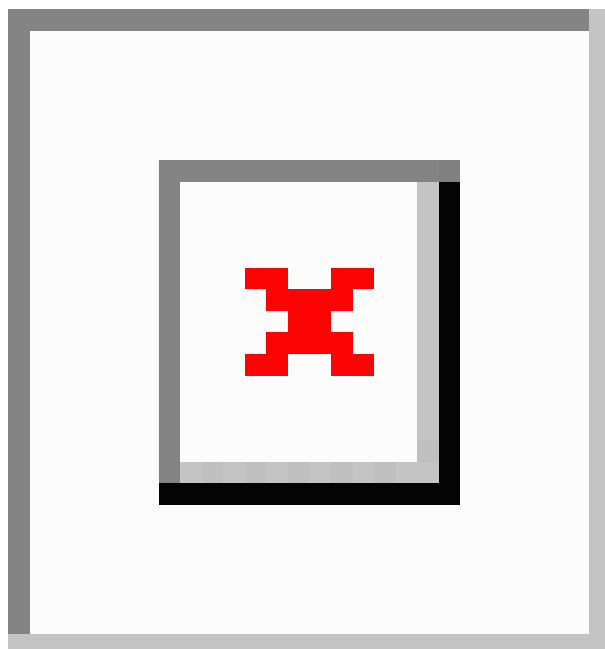
网络对象 NAT 示例

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 18: 面向内部 Web 服务器的静态 NAT



过程

步骤 1 为内部 Web 服务器创建网络对象。

```
hostname(config)# object network myWebServ  
hostname(config-network-object)# host 10.1.2.27
```

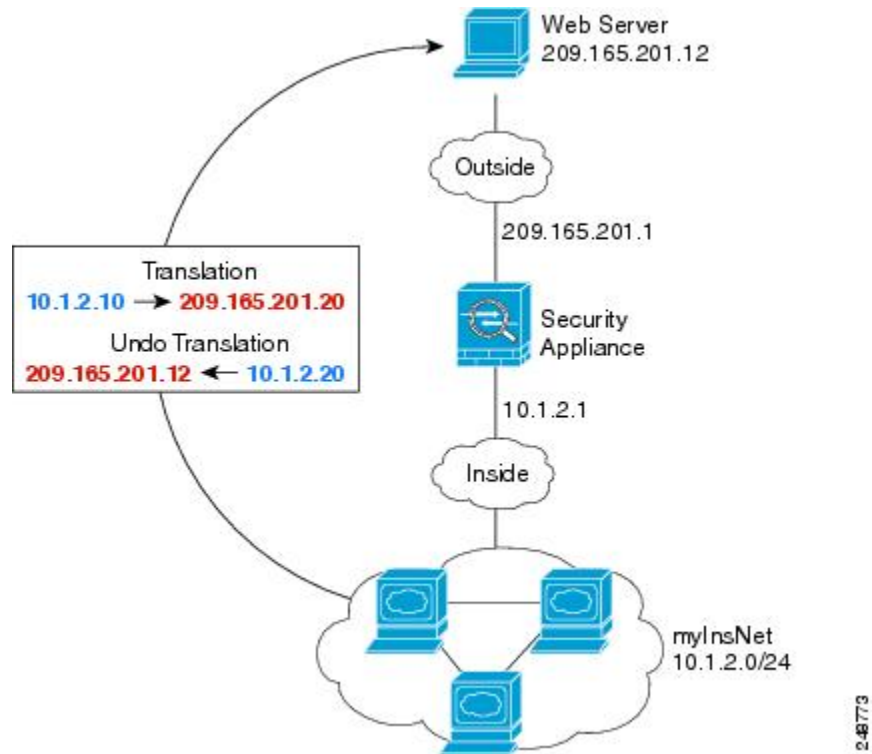
步骤 2 配置对象的静态 NAT:

```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10
```

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 19: 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 为要向其转换内部地址的动态 NAT 池创建一个网络对象。

```
hostname(config)# object network myNatPool
hostname(config-network-object)# range 209.165.201.20 209.165.201.30
```

步骤 2 为内部网络创建网络对象。

```
hostname(config)# object network myInsNet
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

步骤 3 使用动态 NAT 池对象为内部网络启用动态 NAT。

```
hostname(config-network-object)# nat (inside,outside) dynamic myNatPool
```

步骤 4 为外部 Web 服务器创建网络对象。

```
hostname(config)# object network myWebServ
hostname(config-network-object)# host 209.165.201.12
```

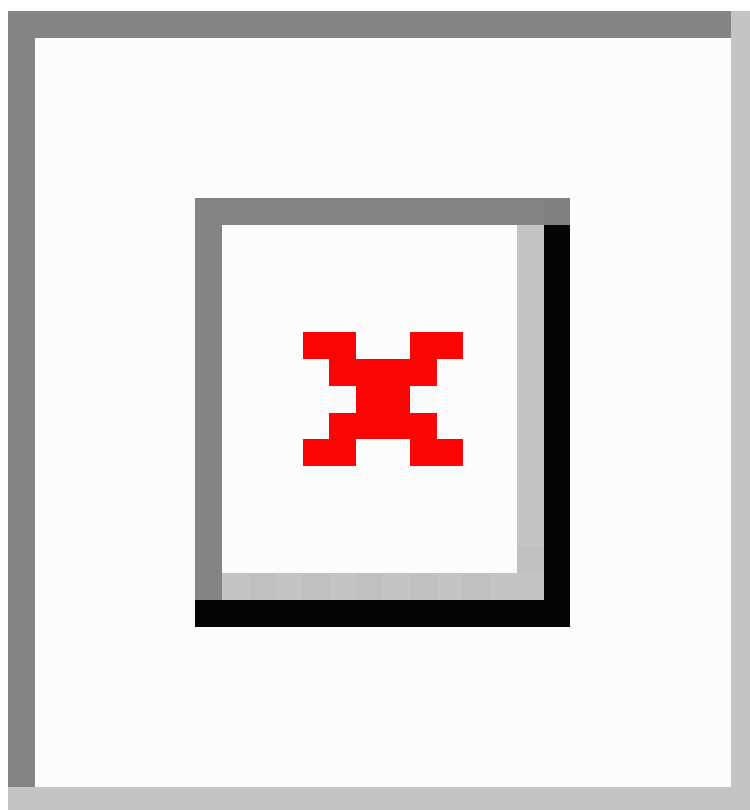
步骤 5 为 Web 服务器配置静态 NAT。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.20
```

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 20: 内部负载均衡器的一对多静态 NAT



过程

步骤 1 为要向其映射负载均衡器的地址创建网络对象。

```
hostname(config)# object network myPublicIPs
hostname(config-network-object)# range 209.165.201.3 209.265.201.8
```


步骤 2 为负载均衡器创建网络对象。

```
hostname(config)# object network myLBHost  
hostname(config-network-object)# host 10.1.2.27
```

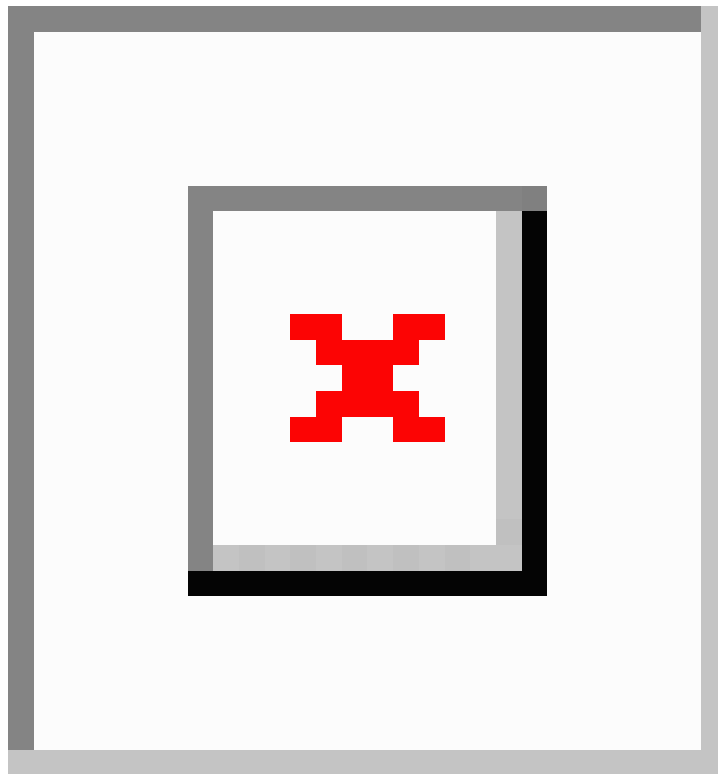
步骤 3 为应用范围对象的负载均衡器配置静态 NAT。

```
hostname(config-network-object)# nat (inside,outside) static myPublicIPs
```

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 21: 支持端口转换的静态 NAT



过程

步骤 1 为 FTP 服务器创建网络对象，并配置支持端口转换的静态 NAT，将 FTP 端口映射到其本身。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.2.27
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp ftp
ftp
```

步骤 2 为 HTTP 服务器创建网络对象，并配置支持端口转换的静态 NAT，将 HTTP 端口映射到其本身。

```
hostname(config)# object network HTTP_SERVER
hostname(config-network-object)# host 10.1.2.28
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp http
http
```

步骤 3 为 SMTP 服务器创建网络对象，并配置支持端口转换的静态 NAT，将 SMTP 端口映射到其本身。

```
hostname(config)# object network SMTP_SERVER
hostname(config-network-object)# host 10.1.2.29
hostname(config-network-object)# nat (inside,outside) static 209.165.201.3 service tcp smtp
smtp
```

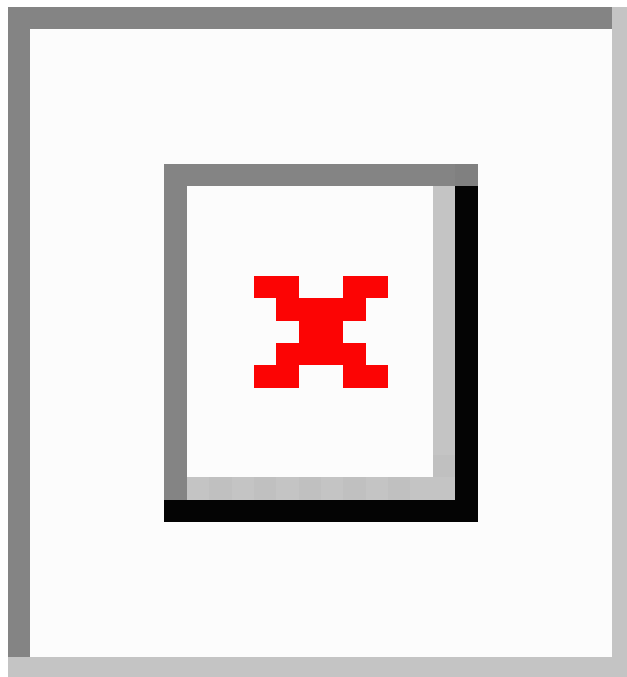
两次 NAT 的示例

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:port。

图 22: 使用不同目标地址的两次 NAT



过程

步骤 1 为内部网络添加网络对象：

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

步骤 2 为 DMZ 网络 1 添加网络对象：

```
hostname(config)# object network DMZnetwork1
hostname(config-network-object)# subnet 209.165.201.0 255.255.255.224
```

步骤 3 为 PAT 地址添加网络对象：

```
hostname(config)# object network PATaddress1
hostname(config-network-object)# host 209.165.202.129
```

步骤 4 配置第一条两次 NAT 规则：

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1
destination static DMZnetwork1 DMZnetwork1
```

由于不希望转换目标地址，所以需要为实际和映射目标地址指定同一地址来为其配置身份 NAT。

步骤 5 为 DMZ 网络 2 添加网络对象：

```
hostname(config)# object network DMZnetwork2
hostname(config-network-object)# subnet 209.165.200.224 255.255.255.224
```

步骤 6 为 PAT 地址添加网络对象：

```
hostname(config)# object network PATaddress2
hostname(config-network-object)# host 209.165.202.130
```

步骤 7 配置第二条两次 NAT 规则：

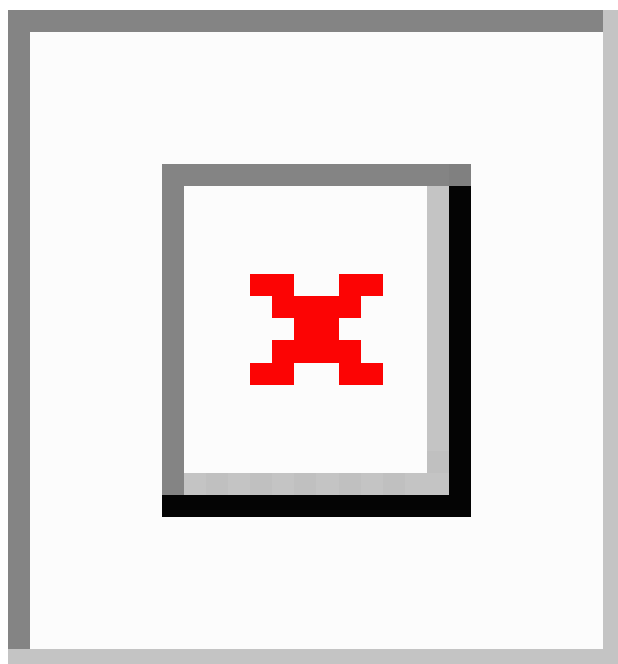
示例：

```
hostname(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2
destination static DMZnetwork2 DMZnetwork2
```

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标端口的使用情况。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。当主机进行网络服务访问相同服务器时，真实地址将转换为 209.165.202.130:port。

图 23: 使用不同目标端口的两次 NAT



过程

步骤 1 为内部网络添加网络对象：

```
hostname(config)# object network myInsideNetwork
hostname(config-network-object)# subnet 10.1.2.0 255.255.255.0
```

步骤 2 为 Telnet/Web 服务器添加网络对象：

```
hostname(config)# object network TelnetWebServer
hostname(config-network-object)# host 209.165.201.11
```

步骤 3 使用 Telnet 时为 PAT 地址添加网络对象：

```
hostname(config)# object network PATAddress1
hostname(config-network-object)# host 209.165.202.129
```

步骤 4 为 Telnet 添加服务对象：

```
hostname(config)# object service TelnetObj
hostname(config-network-object)# service tcp destination eq telnet
```

步骤 5 配置第一条两次 NAT 规则：

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATAddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
```

由于不希望转换目标地址或端口，所以需要为实际和映射目标地址指定同一地址并为实际和映射服务指定同一端口来为它们配置身份 NAT。

步骤 6 使用 HTTP 时为 PAT 地址添加网络对象：

```
hostname(config)# object network PATAddress2
hostname(config-network-object)# host 209.165.202.130
```

步骤 7 为 HTTP 添加服务对象：

```
hostname(config)# object service HTTPObj
hostname(config-network-object)# service tcp destination eq http
```

步骤 8 配置第二条两次 NAT 规则：

```
hostname(config)# nat (inside,outside) source dynamic myInsideNetwork PATAddress2
```

```
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

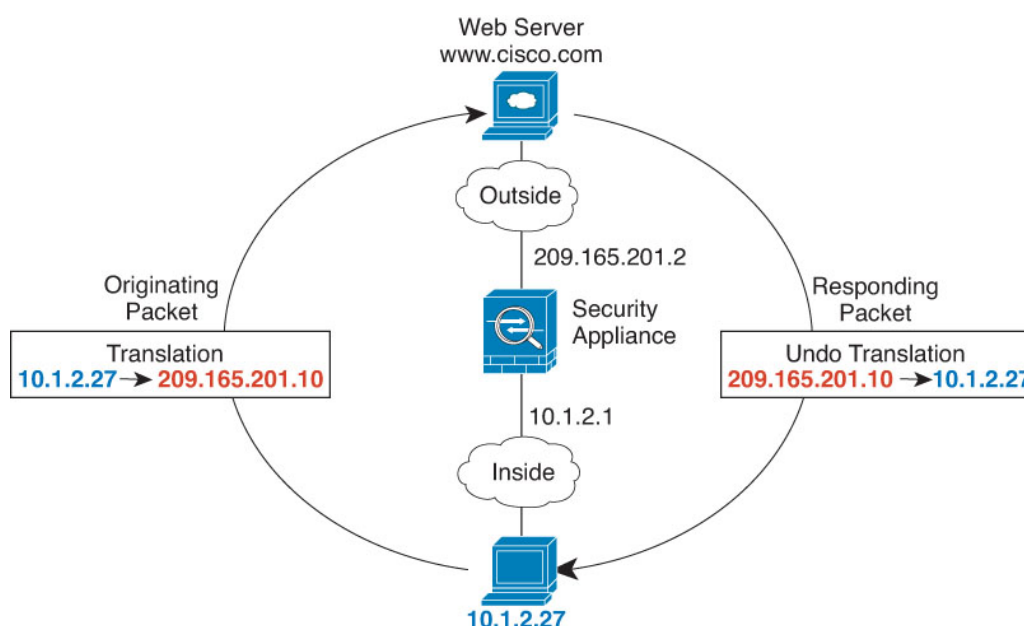
路由和透明防火墙模式下的 NAT

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 24: 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

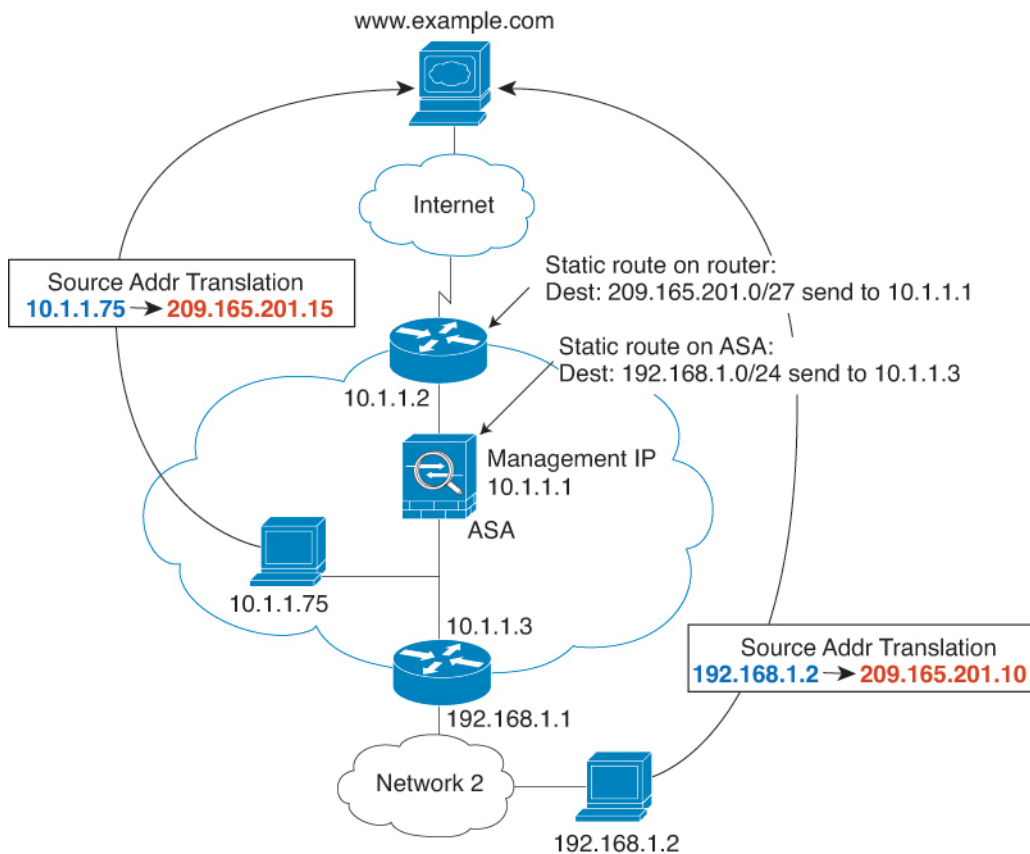
在透明模式下使用 NAT 可以消除上游或下游路由器为其网络执行 NAT 的需求。在路由模式下，NAT 可以执行与桥接组内类似的功能。

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 25: 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。

- 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标。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 准则](#)，第 134 页，了解有关映射 IP 地址的其他准则。

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

如果使用与目标（映射）接口在同一网络中的地址，ASA 使用代理 ARP 应答映射地址的任何 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，则需要在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。使用 **arp** 命令配置 ARP。

唯一网络中的地址

如果需要比目标（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
```

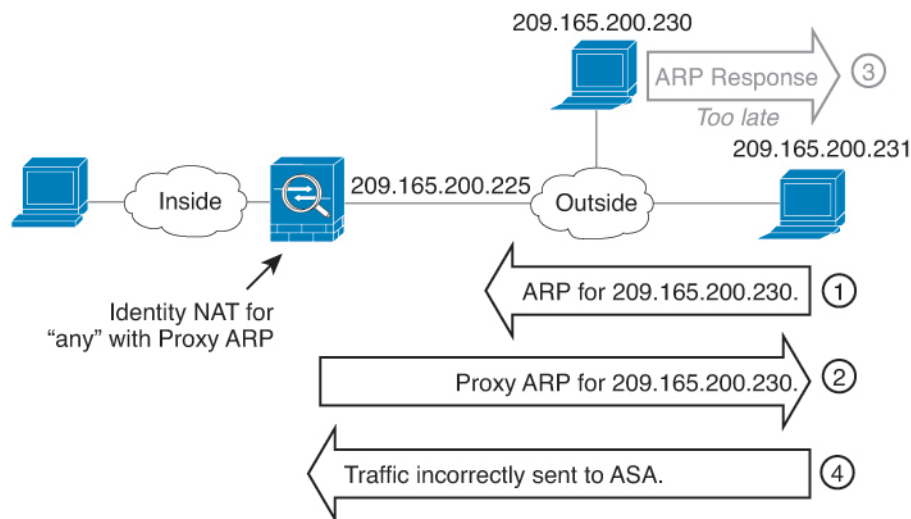

对于透明模式，如果直接连接实际主机，则将上游路由器的静态路由配置为指向 ASA：，指定桥接组 IP 地址。对于透明模式下的远程主机，在上游路由器上的静态路由中，您也可以指定下游路由器 IP 地址。

与实际地址相同的地址（身份 NAT）

身份 NAT 的默认行为已启用代理 ARP，并且与其他静态 NAT 规则匹配。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。

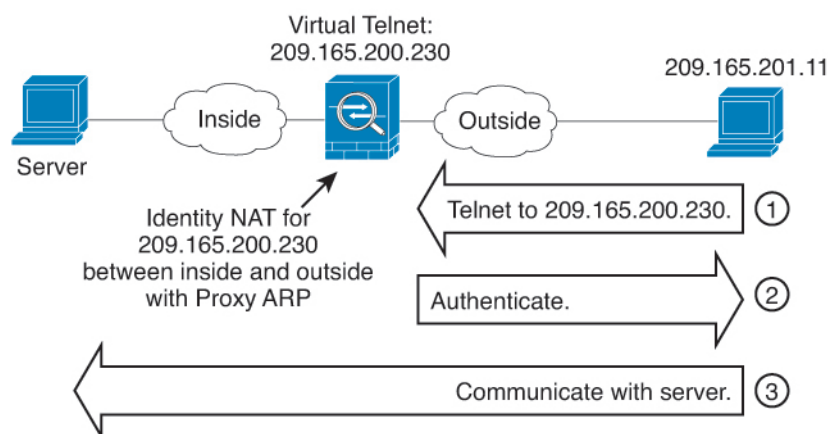
通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。例如，如果为“任何”IP 地址配置一条大体的身份 NAT 规则，则使代理 ARP 保持启用状态会给直接连接到映射接口的网络上的主机造成问题。在这种情况下，当映射网络上的主机要与同一网络上的其他主机通信时，ARP 请求中的地址匹配 NAT 规则（匹配“任何”地址）。然后，ASA 将代理地址的 ARP，即使数据包实际上不以 ASA 为目标。（请注意，即便已设置两次 NAT 规则，也会造成此问题；虽然 NAT 规则必须匹配源地址和目标地址，但仅会根据“源”地址作出代理 ARP 决定）。如果在实际主机 ARP 响应之前收到 ASA ARP 响应，则流量会错误地发送到 ASA。

图 26: 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 27: 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。

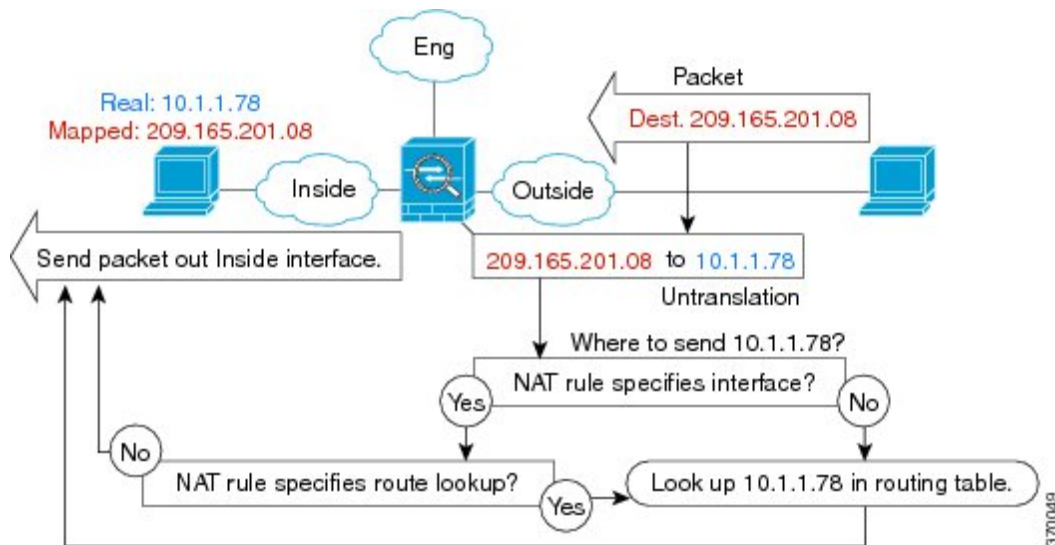
确定出口接口

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。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 28: 含 NAT 的路由模式出口接口选择



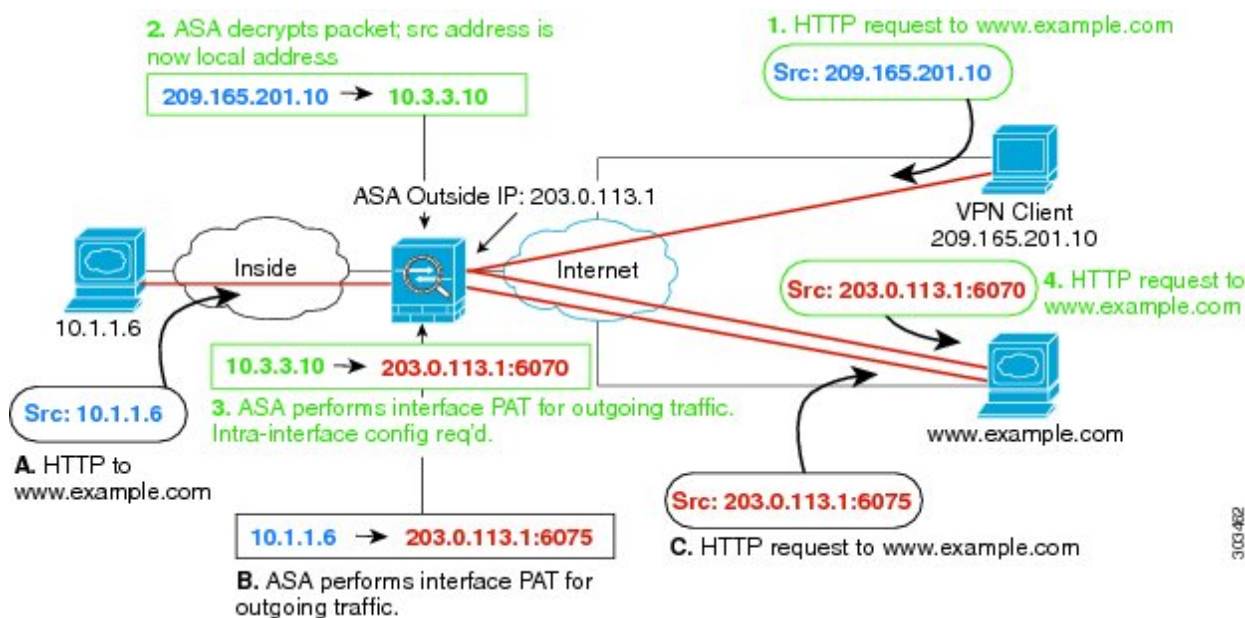
用于 VPN 的 NAT

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

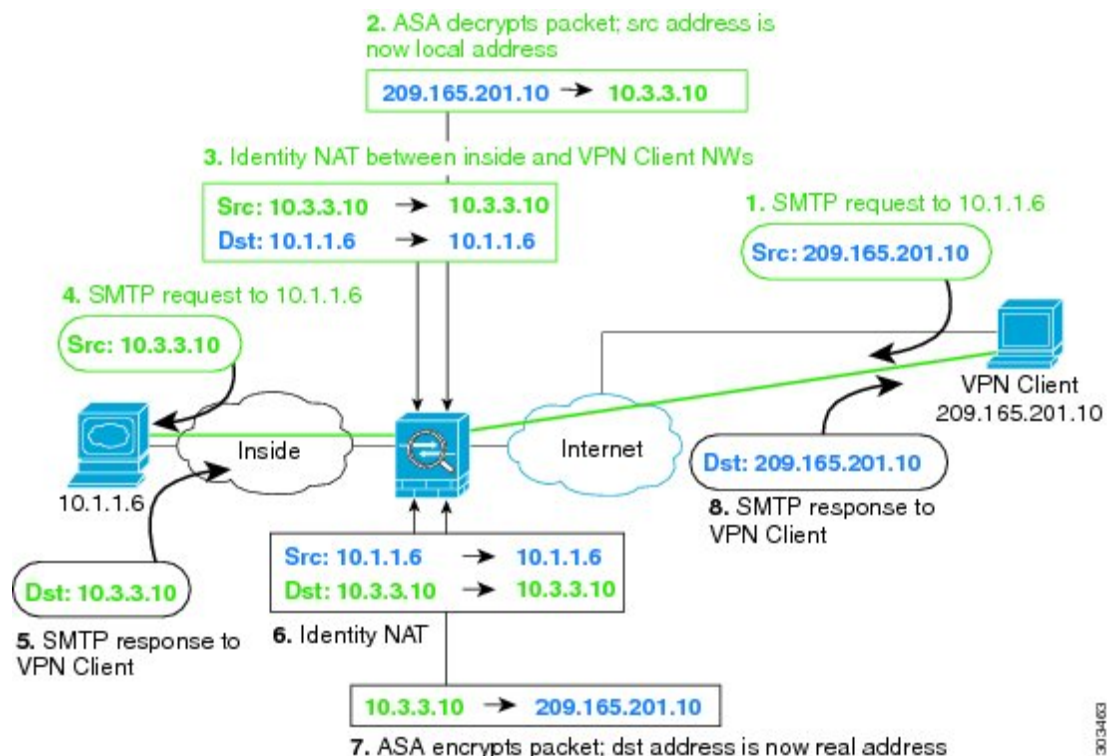
下图显示访问互联网的内部服务器 (10.1.1.6) 和 VPN 客户端 (209.165.201.10)。除非为 VPN 客户端配置拆分隧道（只有指定流量会流经 VPN 隧道），否则互联网绑定的 VPN 流量还必须流经 ASA。当 VPN 流量传入 ASA 时，ASA 会解密数据包；生成的数据包会将 VPN 客户端本地地址 (10.3.3.10) 作为源。对于内部和 VPN 客户端本地网络，需要使用 NAT 提供的公用 IP 地址访问互联网。以下示例使用接口 PAT 规则。为使 VPN 流量可以退出其已进入的相同接口，还需要启用接口内通信（也称为“发夹”网络）。

图 29: 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 30: 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

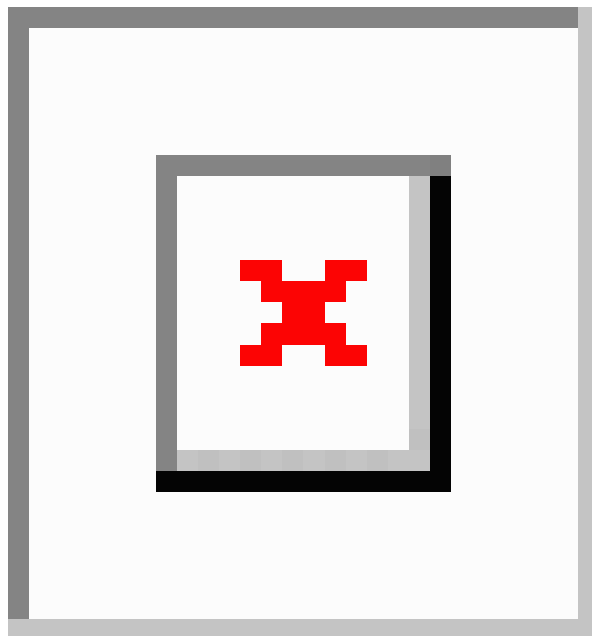
! Use twice NAT to pass traffic between the inside network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static inside_nw inside_nw destination static vpn_local vpn_local
```

NAT 和站点间 VPN

下图显示连接博尔德办公室和圣荷西办公室的站点间隧道。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

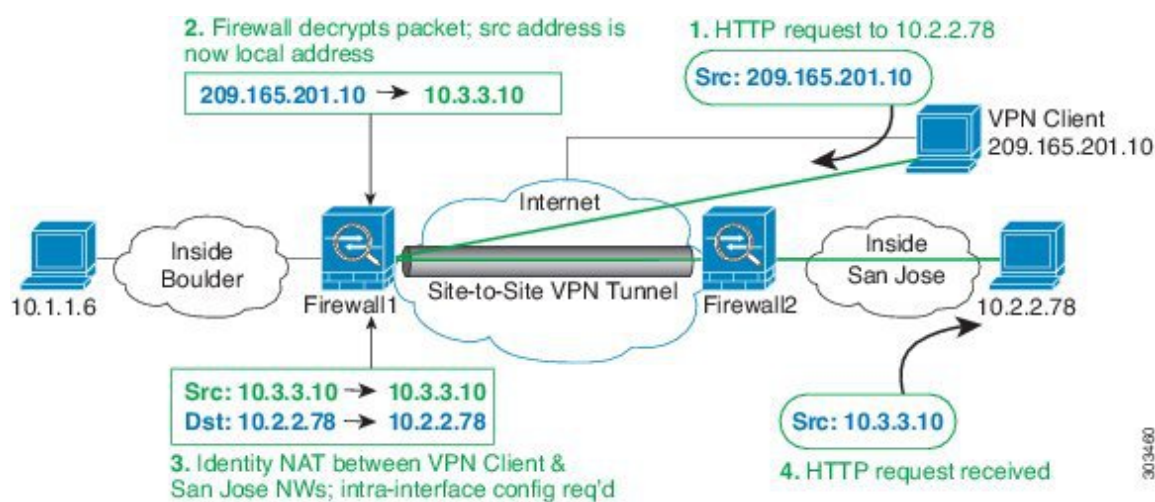
10.1.1.6 到圣荷西办公室中的 10.2.2.78），您不想执行 NAT；您需要通过创建身份 NAT 规则来豁免此流量。身份 NAT 只能将地址转换为其相同的地址。

图 31: 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）之间的站点间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 32: VPN 客户端访问站点间 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

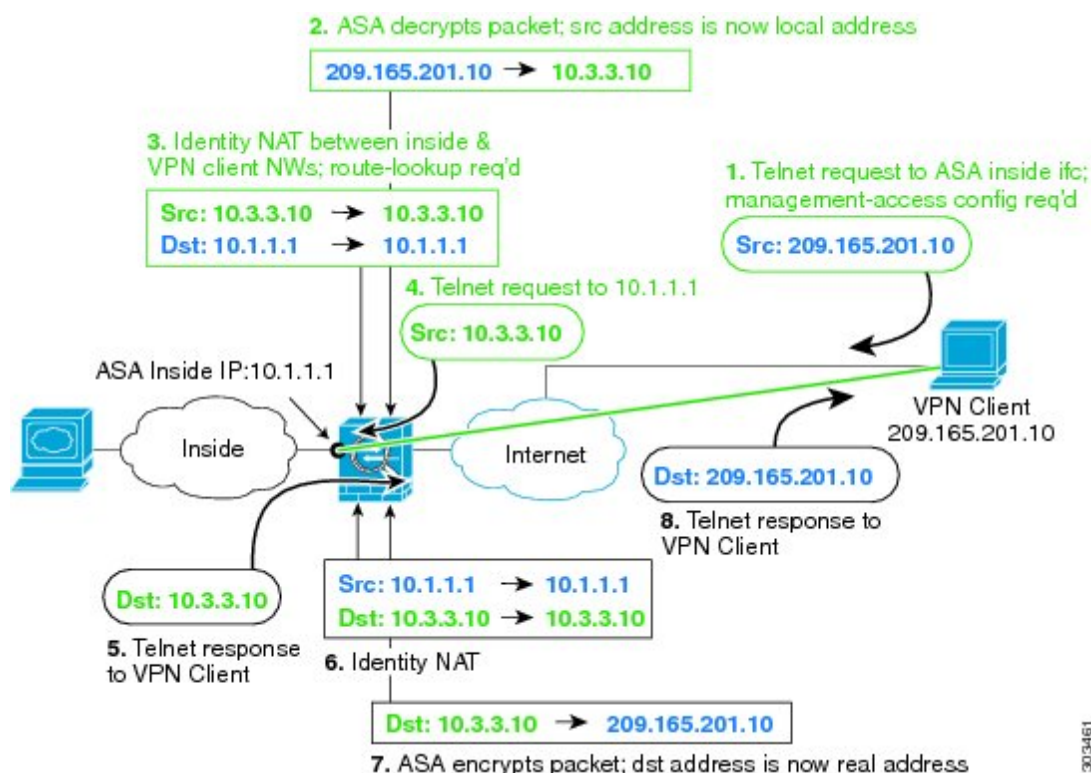
! Use twice NAT to pass traffic between the San Jose network and the VPN client without
! address translation (identity NAT):
nat (inside,outside) source static sanjose_inside sanjose_inside
destination static vpn_local vpn_local
```


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（请参阅 **management-access** 命令）。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 191 页或 [NAT 和站点间 VPN](#)，第 193 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 190 页。

图 33: 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 可在路由接口和网桥组成员接口上使用。

NAT64/46: 将 IPv6 地址转换为 IPv4 地址

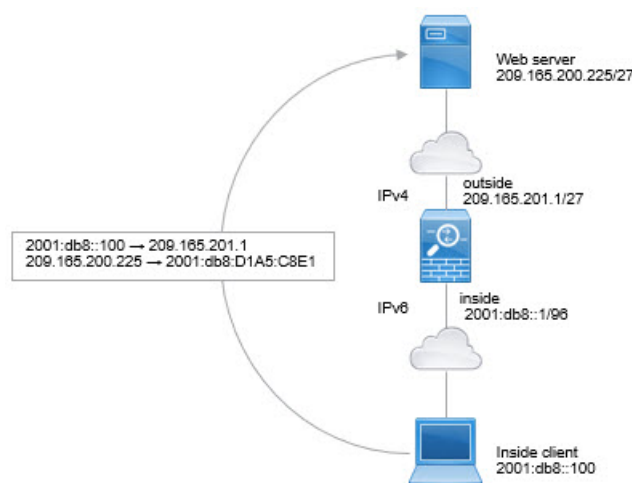
当流量从 IPv6 网络进入仅 IPv4 网络时，您需要将 IPv6 地址转换为 IPv4 地址，并将流量从 IPv4 返回 IPv6。您需要定义两个地址池，一个 IPv4 地址池用于绑定 IPv4 网络中的 IPv6 地址，另一个 IPv6 地址池用于绑定 IPv6 网络中的 IPv4 地址。

- 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，一个用于目标 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

以下是一个非常简单的示例，假设您具有仅包含 IPv6 的内部网络，且您希望将发送到互联网的流量转换为 IPv4。此示例假定您无需 DNS 转换，以便可以在单个两次 NAT 规则中执行 NAT64 和 NAT46 转换。



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。

过程

步骤 1 创建用于内部 IPv6 网络的网络对象。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
```

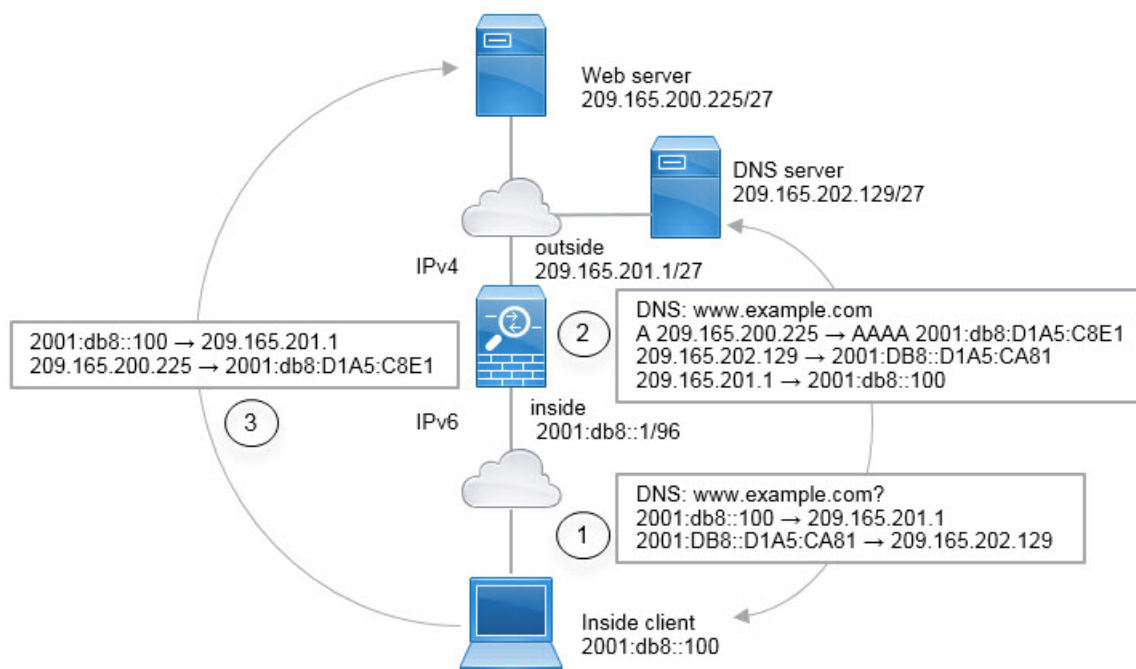
步骤 2 创建两次 NAT 规则以将 IPv6 网络转换为 IPv4 并再次返回。

```
hostname(config)# nat (inside,outside) source dynamic inside_v6 interface
destination static inside_v6 any
```

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。相反，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。

NAT64/46 示例：包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络

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 请求中的源和目的进行转换：
 - 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 为内部 IPv6 网络创建一个网络对象，并添加 NAT64 规则。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface
```

使用此规则，从内部接口的 2001:db8::/96 子网到外部接口的任何流量均会使用外部接口的 IPv4 地址获得 NAT64 PAT 转换。

步骤 2 为外部 IPv4 网络转换的 IPv6 网络创建一个网络对象，并添加 NAT46 规则。

```
hostname(config)# object network outside_v4_any
hostname(config-network-object)# subnet 0.0.0.0 0.0.0.0
hostname(config-network-object)# nat(outside,inside) static 2001:db8::/96 dns
```

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。

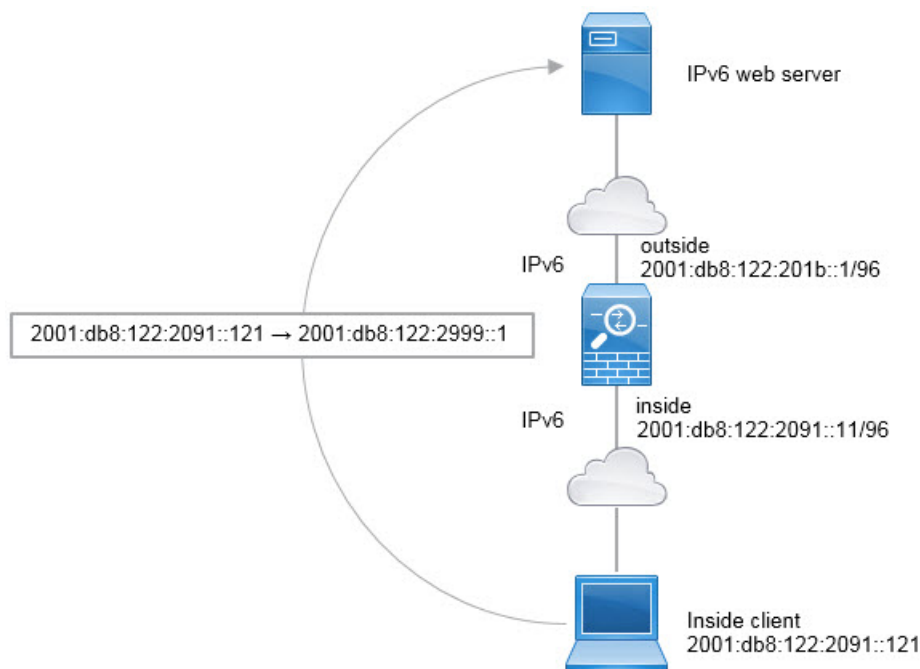
NAT66: 将 IPv6 地址转换为不同的 IPv6 地址

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

为内部 IPv6 网络创建网络对象并添加静态 NAT 规则。

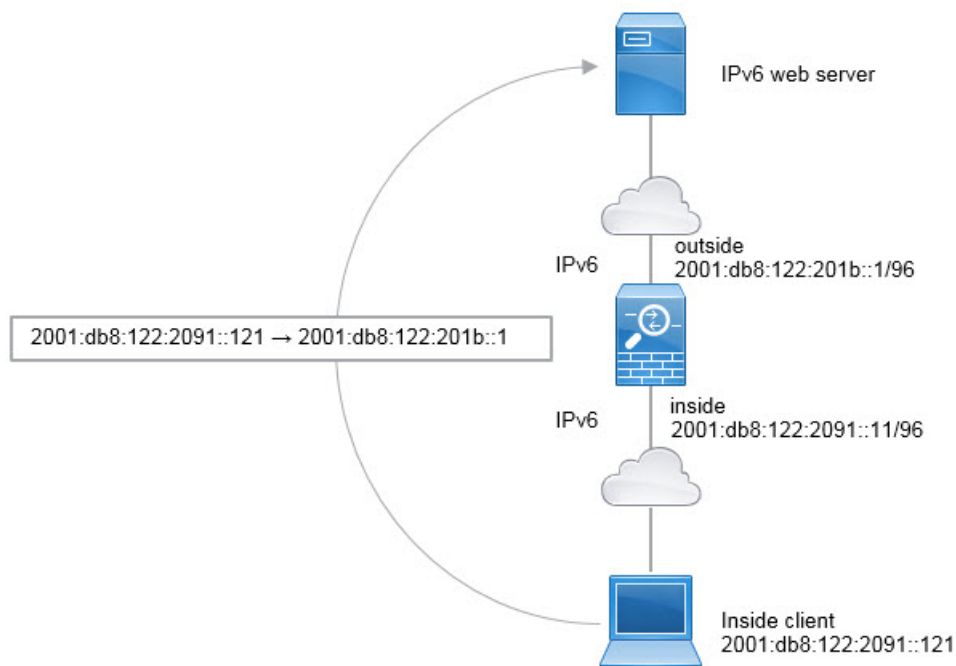
```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) static 2001:db8:122:2999::/96
```

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通过静态 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

为内部 IPv6 网络创建网络对象并添加动态 PAT 规则。

```
hostname(config)# object network inside_v6
hostname(config-network-object)# subnet 2001:db8:122:2091::/96
hostname(config-network-object)# nat(inside,outside) dynamic interface ipv6
```

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。此功能适用于 NAT44、NAT 66、NAT46 和 NAT64。

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，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）。

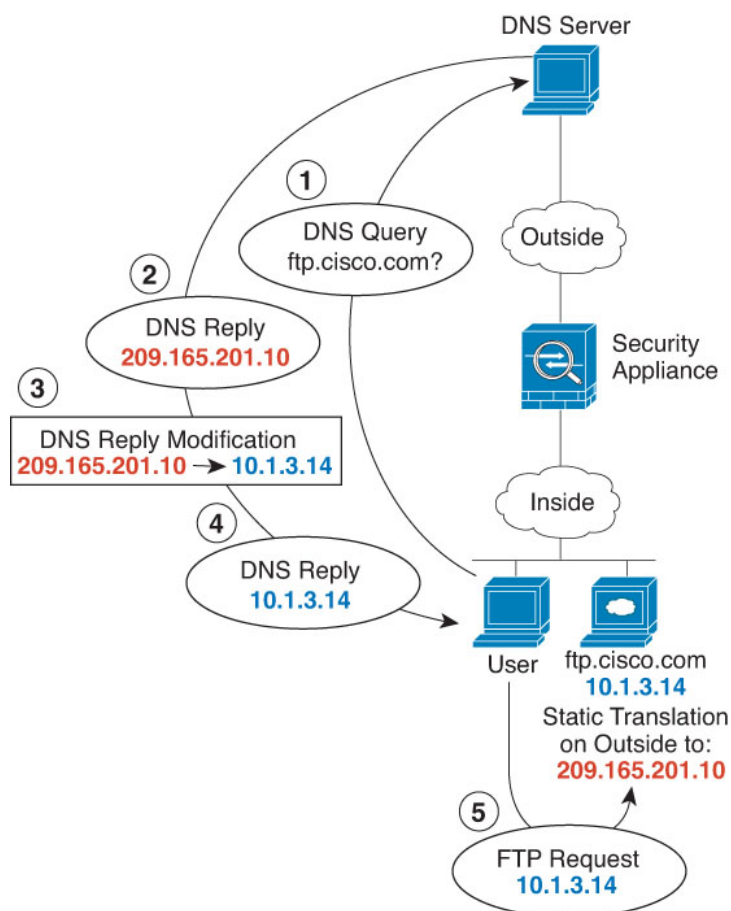
以下主题提供了 NAT 规则中 DNS 重写的示例。

DNS 回复修改、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 回复修改，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。



过程

步骤 1 为 FTP 服务器创建网络对象。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 10.1.3.14
```


步骤 2 配置支持 DNS 修改的静态 NAT。

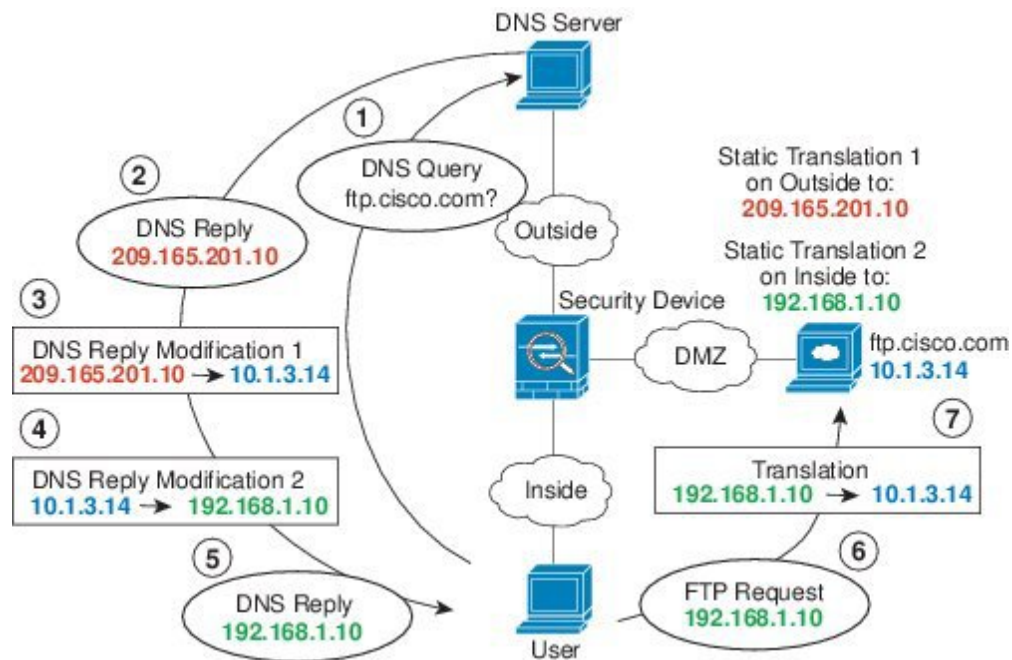
```
hostname(config-network-object)# nat (inside,outside) static 209.165.201.10 dns
```

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。

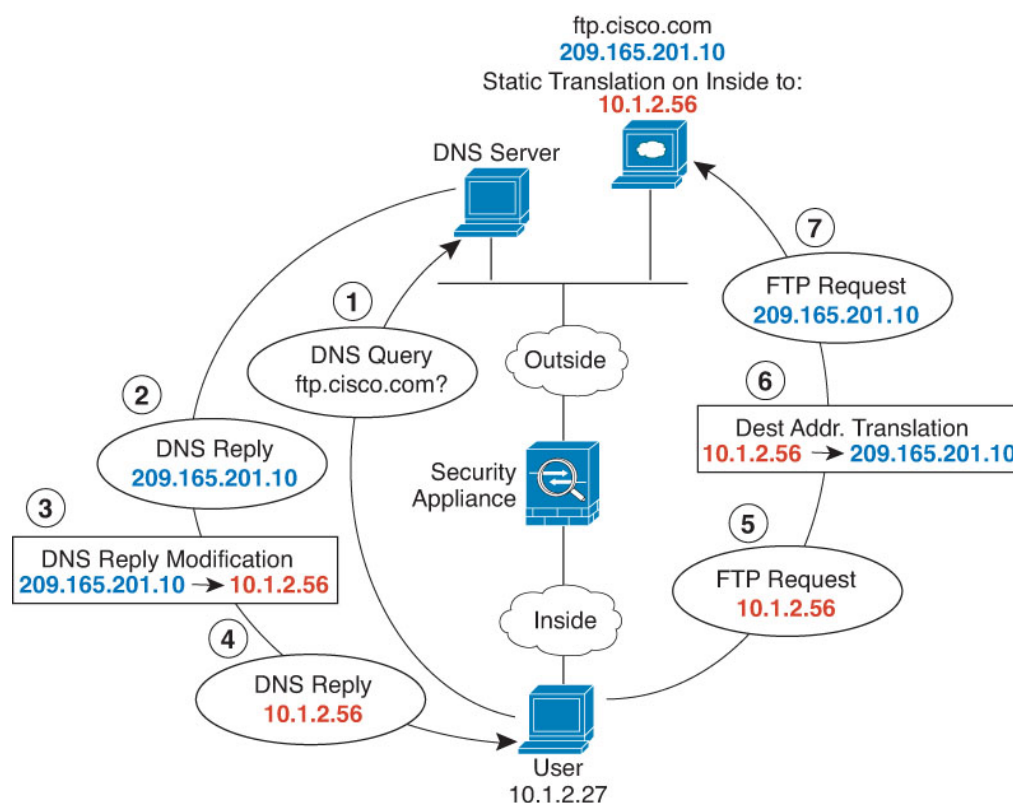
如果用户需要使用实际地址访问 ftp.cisco.com，则无需更多配置。如果内部网络和 DMZ 网络之间也有静态规则，还需要在此规则上启用 DNS 应答修改。然后，修改 DNS 应答两次。这种情况下，ASA 会根据内部和 DMZ 之间的静态规则将 DNS 应答内的地址重新转换为 192.168.1.10。

图 34: 独立网络上的 DNS 应答修改、DNS 服务器、主机和服务



DNS 回复修改、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 为 FTP 服务器创建网络对象。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.201.10
```

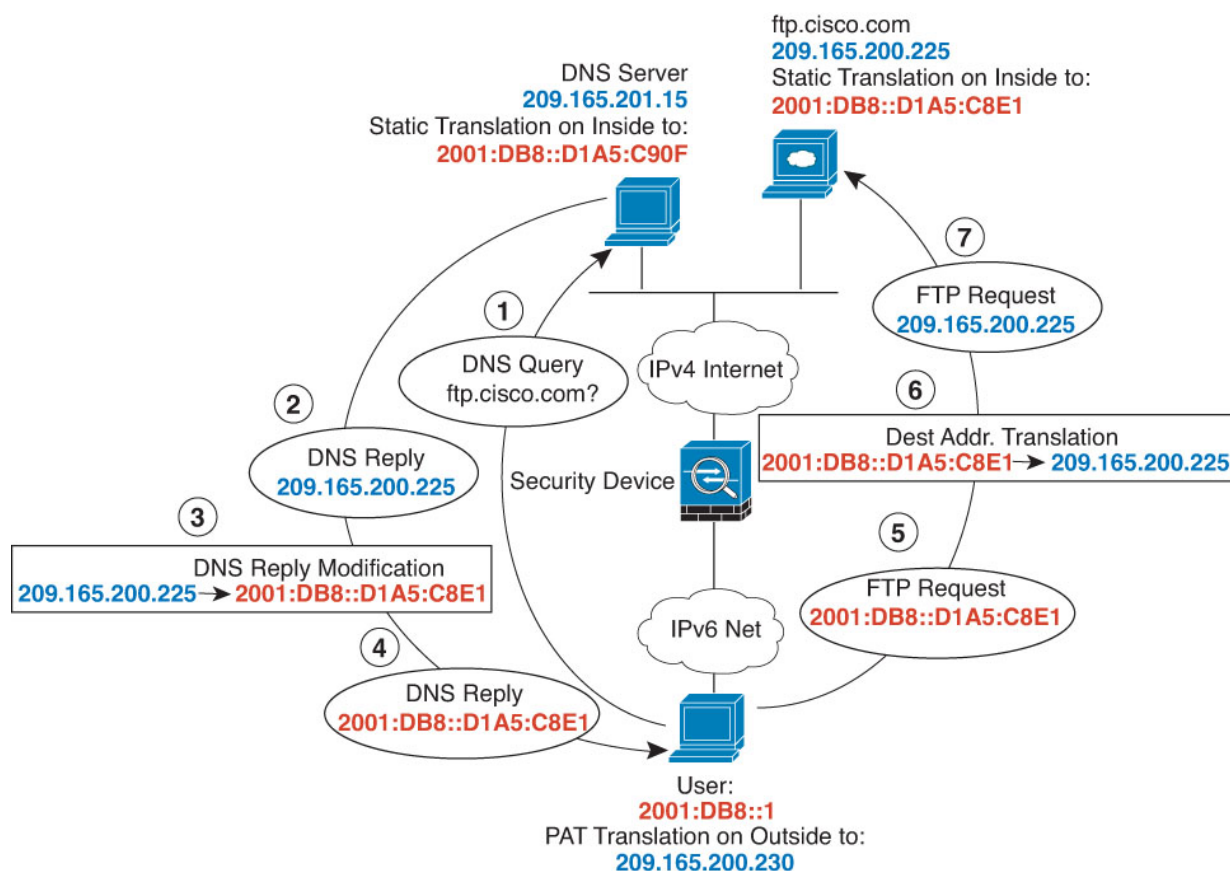
步骤 2 配置支持 DNS 修改的静态 NAT。

```
hostname(config-network-object)# nat (outside,inside) static 10.1.2.56 dns
```

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 为 FTP 服务器创建网络对象并配置支持 DNS 修改的静态 NAT。由于这是一对一的转换，请为 NAT46 包含 **net-to-net** 选项。

```
hostname(config)# object network FTP_SERVER
hostname(config-network-object)# host 209.165.200.225
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C8E1/128
net-to-net dns
```

步骤 2 为 DNS 服务器创建网络对象并配置静态 NAT。为 NAT46 包含 **net-to-net** 选项。

```
hostname(config)# object network DNS_SERVER
hostname(config-network-object)# host 209.165.201.15
hostname(config-network-object)# nat (outside,inside) static 2001:DB8::D1A5:C90F/128
net-to-net
```

步骤 3 配置 IPv4 PAT 池, 以转换内部 IPv6 网络。

示例:

```
hostname(config)# object network IPv4_POOL
hostname(config-network-object)# range 209.165.200.230 209.165.200.235
```

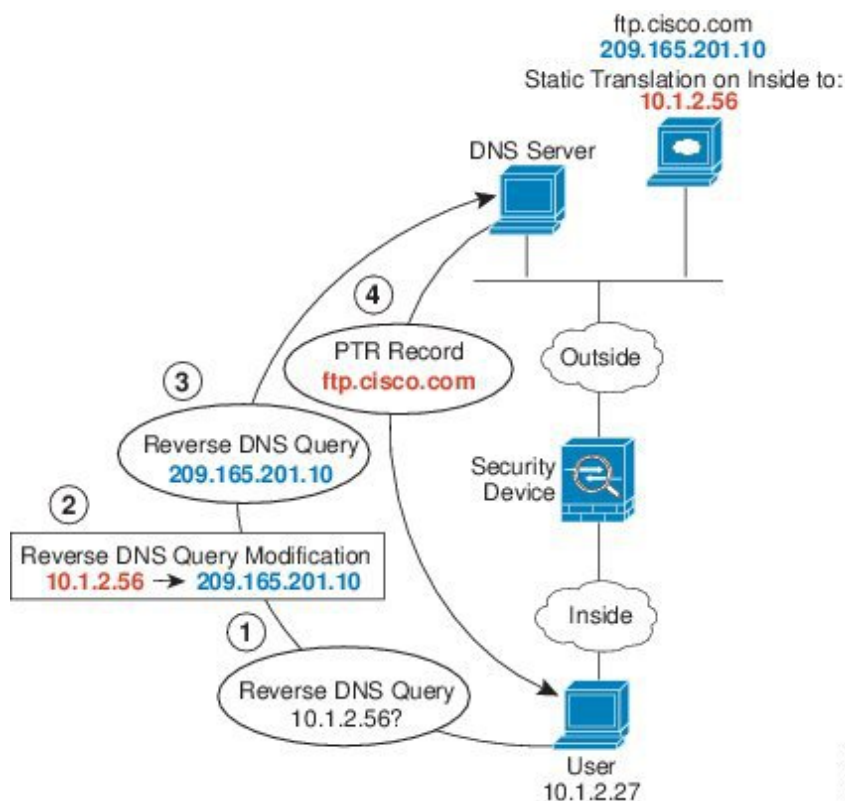
步骤 4 为内部 IPv6 网络创建网络对象, 并配置带 PAT 池的动态 NAT。

```
hostname(config)# object network IPv6_INSIDE
hostname(config-network-object)# subnet 2001:DB8::/96
hostname(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

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 35: PTR 修改, 主机网络上的 DNS 服务器



304002



第 10 章

映射地址和端口 (MAP)

映射地址和端口 (MAP) 是将 IPv4 地址转换为 IPv6 的运营商级功能，因此流量可以通过服务提供商的 IPv6 网络发送，然后在服务提供商边缘转换回 IPv4。

- [关于映射地址和端口 \(MAP\)，第 209 页](#)
- [映射地址和端口 \(MAP\) 准则，第 210 页](#)
- [配置 MAP-T 域，第 212 页](#)
- [监控 MAP，第 213 页](#)
- [MAP 的历史记录，第 215 页](#)

关于映射地址和端口 (MAP)

映射地址和端口（映射）主要是在服务提供商（SP）网络中使用的一项功能。服务提供商可以运行 IPv6 网络、映射域，同时支持 IPv4 用户，以及与公共互联网上的 IPv4 站点通信的需要。映射在 RFC7597、RFC7598 和 RFC7599 中定义。

对于 MAP 域内的服务提供商来说，MAP 相对于 NAT46 的优势在于，用 IPv6 地址替换用户的 IPv4 地址（在 SP 网络边缘再返回到 IPv4）是无状态的。与 NAT46 相比，这提高了 SP 网络的效率。

有两种 MAP 技术：MAP 转换 (MAP-T) 和 MAP 封装 (MAP-E)。ASA 支持 MAP-T；不支持 MAP-E。

关于映射地址和端口转换 (MAP-T)

通过 MAP-T，用户的 IPv4 地址首先被转换为服务器提供商 (SP) 的公共 IPv4 地址，这可以是一对一的地址映射，也可以是与前缀或共享地址的映射。然后，该 IPv4 地址被转换为 MAP 域内的 IPv6 地址，数据包通过 SP IPv6 网络传输。在网络边缘，SP 的边界中继负责将 IPv6 地址转换回 SP 的 IPv4 地址，然后将数据包路由到公共 IPv4 网络。从公共 IPv4 网络到用户的流量则完全相反。

图 36: MAP-T 网络



通过使用 MAP-T，您可以将 SP 网络过渡到纯 IPv6 架构，同时允许用户继续使用 IPv4 并与纯 IPv4 互联网或 SP 网络外的其他站点通信。

MAP-T 的行为类似于 NAT64 转换，但它使用的不是内嵌 IPv4 地址的 IPv6 地址，而是同时包含端口的编码方案。因此，MAP-T 提供了一种限制设备使用端口范围的方法。

MAP-T 系统包括以下内容：

- **客户边缘 (CE) 设备** - CE 是家庭网关（无线路由器、带路由器的电缆调制解调器等）。CE 提供 IPv4/IPv6 转换和本地 IPv6 转发功能。它有一个面向提供商的 IPv6 地址广域网接口和一个或多个使用专用 IPv4 地址寻址的局域网接口。您将配置一个或多个 MAP 域，供 CE 用于将 IPv4 数据包转换为 IPv6，反之亦然。
- **边界中继 (BR) 设备** - 可将 ASA 安装为边界中继。BR 是 MAP 域边缘的提供方组件，支持 IPv4/IPv6 转换。BR 至少有一个支持 IPv6 的接口和一个连接 IPv4 网络的 IPv4 接口。您将配置一个或多个 MAP 域，供 BR 用于将 IPv4 数据包转换为 IPv6，反之亦然。必须使用相同的 MAP 域规则配置 CE 和 BR。
- **MAP 域** - MAP 域是一种机制，用于将一组 MAP-T CE 设备与一组 MAP-T BR 设备进行分组。域是分配给域的 BR 和 CE 设备之间共享的一组参数。在每个 BR 和 CE 设备上配置相同的域和相同的参数。

映射地址和端口 (MAP) 准则

防火墙模式准则

只能在路由模式下配置 MAP。不支持透明模式。

其他准则

- ASA 在网状模式下不参与数据包转发。因此，不能在 MAP 域中配置转发映射规则 (FMR)。
- MAP 不支持隧道 VPN、组播或任播流量。
- 不能在给定连接上同时使用 NAT 和 MAP。确保 NAT 和 MAP 规则不重叠。如果有重叠的规则，则会出现意外结果。
- 以下检测不支持 MAP 转换。不会转换进行这些检测的数据包。
 - CTIQBE

- DCERPC
- Diameter
- WINS 名称解析
- GTP
- H.323 和 H.225 和 H.245 和 RAS
- ILS (LDAP)
- 即时消息
- IP 选项 (RFC 791、2113)
- IPSec 穿透
- LISP
- M3UA
- MGCP
- MMP
- NetBIOS
- PPTP
- RADIUS 记账
- RSH
- RTSP
- SIP
- SKINNY
- SMTP 和 ESMTP
- SNMP
- SQL*Net
- STUN
- Sun RPC
- TFTP
- WAAS
- XDMCP
- 活动 FTP

配置 MAP-T 域

要配置 MAP-T，您需要创建一个或多个域。在客户边缘 (CE) 和边界中继 (BR) 设备上配置 MAP-T 时，请确保将参与每个域的每台设备使用相同的参数。

您最多可以配置 25 个 MAP-T 域。在多情景模式下，您最多可以在每个情景中配置 25 个域。

过程

步骤 1 创建（或编辑）MAP 域。

map-domain 名称

其中，名称为最多 48 个字符的字母数字字符串。该名称还可以包含以下特殊字符：句点 (.)、斜线 (/) 和冒号 (:)。

示例：

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)#
```

步骤 2 配置默认映射规则。

default-mapping-rule *ipv6_prefix/prefix_length*

根据 RFC 6052，指定用于嵌入 IPv4 目标地址的 IPv6 前缀。前缀长度通常为 64，但允许的值为 32、40、48、56、64 或 96。嵌入式 IPv4 地址后的任何尾部位都将设置为 0。

边界中继 (BR) 设备使用此规则将 MAP 域外的所有 IPv4 地址转换为 MAP 域内的 IPv6 地址。

示例：

```
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
```

步骤 3 配置基本映射规则。

客户边缘 (CE) 设备使用基本映射规则确定其专用 IPv4 寻址或共享地址和端口集分配。CE 设备首先将系统的 IPv4 地址转换为池前缀和端口范围内的 IPv4 地址和端口（使用 NAT44），然后 MAP 将新的 IPv4 地址转换为由规则的 IPv6 前缀定义的池内的 IPv6 地址。然后，数据包就可以通过服务提供商的纯 IPv6 网络传输到边界中继 (BR) 设备。

a) 进入基本映射规则配置模式。

basic-mapping-rule

b) 配置 IPv4 前缀。

ipv4-prefix *ipv4_network_address netmask*

IPv4 前缀定义客户边缘 (CE) 设备的 IPv4 地址池。CE 设备首先将其 IPv4 地址转换为 IPv4 前缀定义的池中的地址（和端口号）。然后，MAP 会使用默认映射规则中的前缀将新地址转换为 IPv6 地址。

指定网络地址和子网掩码，例如 192.168.3.0 255.255.255.0。不能在不同 MAP 域中使用相同的 IPv4 前缀。

- c) 配置 IPv6 前缀。

ipv6-prefix *ipv6_prefix/prefix_length*

IPv6 前缀定义 CE 设备 IPv6 地址的地址池。只有当数据包的目标地址具有该前缀，源地址具有默认映射规则中定义的 IPv6 前缀，且在正确的端口范围内时，MAP 才会将 IPv6 数据包翻译回 IPv4。任何从其他地址发送到 CE 设备的 IPv6 数据包都会被简单地作为 IPv6 流量处理，而不会进行 MAP 转换。来自 MAP 源/目的池但端口超出范围的数据包会被直接丢弃。

指定 IPv6 前缀和前缀长度，通常为 64，但不能小于 8。不能在不同 MAP 域中使用相同的 IPv6 前缀。

- d) 配置起始端口。

start-port 数字

转换地址的端口池中的第一个端口。指定的端口必须是 2 的次幂，范围是 1-32768，例如 1、2、4、8 等。如果要排除知名端口，请从 1024 或更高的端口开始。

- e) 配置端口比率，该比率决定端口池中有多少个端口。

share-ratio 数字

指定池中应包含的端口数。数字必须是 2 的幂，范围为 1-65536，例如 1、2、4、8 等。

示例：

```
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

示例

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

监控 MAP

以下主题介绍如何监控 MAP 配置和活动。

验证 MAP 域配置

您可以查看映射域及其状态，以验证配置是否正确。

show map-domain 命令显示 MAP 配置（类似于 **show running-config map-domain** 命令），但也可指示域配置是否有效。在以下示例中，有两个域：1 和 2。输出结果说明 MAP 域 2 不完整，因此未激活。

```
MAP Domain 1
  Default Mapping Rule
    IPv6 prefix 2001:db8:cafe:cafe::/64
  Basic Mapping Rule
    IPv6 prefix 2001:cafe:cafe:1::/64
    IPv4 prefix 192.168.3.0 255.255.255.0
    share ratio 16
    start port 1024
    PSID length 4
    PSID offset 6
    Rule EA-bit length 12

MAP Domain 2
  Default Mapping Rule
    IPv6 prefix 2001:db8:1234:1234::/64

Warning: map-domain 2 configuration is incomplete and not in effect.
```

监控 MAP 系统日志消息

如果启用了系统日志，则可以通过以下系统日志消息监控 MAP 行为：

- 305018：从接口名称：源 IP 地址/源端口-目标 IP 地址/目标端口到接口名称的 MAP 转换：转换后的源 IP 地址/转换后的源端口-转换后的目标 IP 地址/转换后的目标端口进行了新的 MAP 转换。消息中会显示原始的和转换后的源及目标。
- 305019：MAP 节点地址 IP 地址/端口的端口集 ID 编码不一致
数据包中的地址与 MAP 基本映射规则相匹配（意味着需要转换），但地址中编码的端口集 ID 不一致（根据 RFC7599）。这可能意味着该数据包所在的 MAP 节点出现了软件故障。
- 305020：地址 IP 地址的 MAP 节点不允许使用端口端口
数据包中的地址与 MAP 基本映射规则相匹配（意味着它需要转换），但关联端口不在分配给此地址的范围内。这可能意味着发起此数据包的 MAP 节点配置有误。

MAP 的历史记录

功能名称	平台版本	说明
映射地址和端口转换(MAP-T)	9.13(1)	映射地址和端口（映射）主要是在服务提供商（SP）网络中使用的一项功能。服务提供商可以运行 IPv6 网络、映射域，同时支持 IPv4 用户，以及与公共互联网上的 IPv4 站点通信的需要。映射在 RFC7597、RFC7598 和 RFC7599 中定义。 引入或修改了以下命令：basic-mapping-rule、default-mapping-rule、ipv4-prefix、ipv6-prefix、map-domain、share-ratio、show map-domain、start-port。



第 **IV** 部分

服务策略和应用检测

- [服务策略，第 219 页](#)
- [应用层协议检测入门，第 241 页](#)
- [基本互联网协议检测，第 261 页](#)
- [语音和视频协议检测，第 301 页](#)
- [移动网络检测，第 325 页](#)



第 11 章

服务策略

使用模块化策略框架的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 219 页](#)
- [服务策略准则，第 225 页](#)
- [服务策略默认设置，第 226 页](#)
- [配置服务策略，第 228 页](#)
- [监控服务策略，第 235 页](#)
- [服务策略（模块化策略框架）示例，第 236 页](#)
- [服务策略的历史记录，第 238 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：

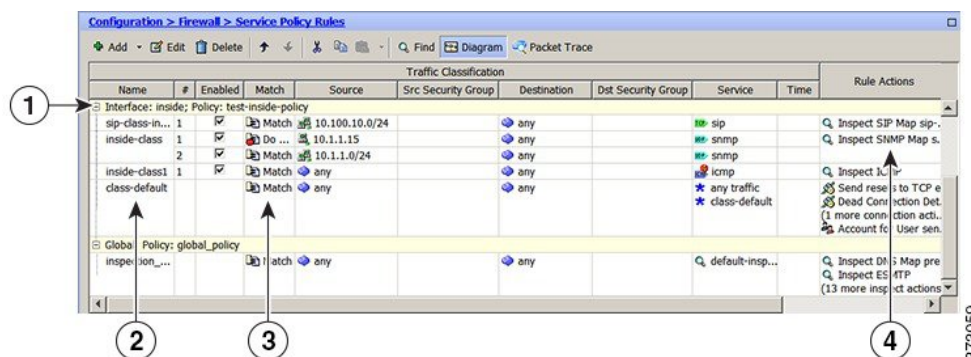
1. 服务策略映射。这是一组按顺序排列的规则集，根据 **service-policy** 命令命名。在 ASDM 中，策略映射表示为 Service Policy Rules 页面上的一个文件夹。

- 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 8: 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	- 应用层协议检测入门, 第 241 页。 - 基本互联网协议检测, 第 261 页。 - 语音和视频协议检测, 第 301 页。 - 移动网络检测, 第 325 页。
NetFlow 安全事件记录过滤	是	是	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 407 页。
QoS 标准优先级队列	是	否	服务质量, 第 407 页。
TCP 和 UDP 连接限制与超时, 以及 TCP 序列号随机化	是	是	连接设置, 第 373 页。
TCP 规范化	是	否	连接设置, 第 373 页。

功能	适用于直通流量？	适用于管理流量？	请参阅：
TCP 状态绕行	是	否	连接设置 ，第 373 页。
身份防火墙用户统计信息	是	是	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 9: 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
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
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映射中的类映射：

1. 对于每个功能类型，数据包只能与策略映射中的一个类映射匹配。
2. 在数据包匹配某个功能类型的类映射后，ASA 不会再尝试将其与该功能类型的任何后续类映射匹配。
3. 但是，如果该数据包与其他功能类型的后续类映射匹配，则 ASA 也会应用适用于该后续类映射的操作（如果支持）。请参阅[某些功能操作的不兼容性](#)，第 224 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类映射匹配，还与应用检测的类映射匹配，则会同时应用两项操作。
- 如果数据包不仅与 HTTP 检测的类映射匹配，还与包含 HTTP 检测的另一个类映射匹配，则不会应用第二项类映射操作。
- 如果数据包不仅与 HTTP 检测的类映射匹配，还与包含 FTP 检测的另一个类映射匹配，则不会应用第二项类映射操作，因为 HTTP 和 FTP 检测无法合并。
- 如果数据包不仅与 HTTP 检测的类映射匹配，还与包含 IPv6 检测的另一个类映射匹配，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

不同类型的操作在策略映射中的执行顺序独立于操作在策略映射中的显示顺序。

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 224 页。
5. QoS 输出策略管制
6. 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。[多种功能操作的应用顺序](#)，第 223 页 中列出了其他例外情况。



注释 默认全局策略中使用的 **match default-inspection-traffic** 命令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命令时，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。

错误配置示例：在同一策略映射中配置多个检测，并且不使用 **default-inspection-traffic** 快捷方式。在第一个示例中，误为 FTP 和 HTTP 检测都配置了流向端口 21 的流量。在第二个示例中，误为 FTP 和 HTTP 检测都配置了流向端口 80 的流量。在这两种错误配置示例的情况下，系统仅会应用 FTP 检测，因为按照应用检测的顺序，FTP 先于 HTTP。

示例 1：FTP 数据包错误配置：也配置了 HTTP 检测

```
class-map ftp
  match port tcp eq 21
class-map http
  match port tcp eq 21 [it should be 80]
policy-map test
  class ftp
    inspect ftp
  class http
    inspect http
```

示例 2: HTTP 数据包错误配置: 也配置了 FTP 检测

```
class-map ftp
  match port tcp eq 80 [it should be 21]
class-map http
  match port tcp eq 80
policy-map test
  class ftp
    inspect ftp
  class http
    inspect http
```

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。

服务策略准则

检测准则

本文以有单独的主题详细介绍用于应用检测服务策略的准则。请参阅[应用检测准则](#)，第 243 页。

IPv6 准则

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[应用检测准则](#)，第 243 页。
- 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 序列号随机化
- 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）准则

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。

策略映射准则

请参阅下列有关使用策略映射的准则：

- 对于每个接口，只能分配一个策略映射。对于低端防火墙，最多可在配置中创建 64 个策略映射；对于功能更强大的防火墙，最多可创建 128 个策略映射。
- 可以将同一策略映射应用到多个接口。
- 可以在第 3/4 层映射中识别多达 63 个第 3/4 层类映射。
- 对于每个类映射，在支持的情况下，可以从一种或多种功能类型分配多项操作。请参阅[某些功能操作的不兼容性](#)，第 224 页。

服务策略准则

- 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
- 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 `default-inspection-traffic`）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。

```
class-map inspection default
  match default-inspection-traffic
```

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。此类映射显示在所有第 3/4 层策略映射的末尾，基本上是告知 ASA 不要对任何其他流量执行任何操作。如果需要，您可以使用 **class-default** 类，而不是使用 Any 流量类建立自己的 **match any** 类映射。实际上，有些功能仅适用于 **class-default**。

```
class-map class-default
match any
```

配置服务策略

要使用模块化策略框架配置服务策略，请执行以下步骤：

过程

步骤 1 按照身份流量（第 3/4 层类映射），第 229 页中所述，通过创建第 3/4 层类映射标识要对其执行操作的流量。

例如，您可能希望对通过 ASA 的所有流量执行操作，也可能希望仅对从 10.1.1.0/24 到任何目标地址的流量执行某些操作。



步骤 2 或者，在某些检测流量上执行其他操作。

如果要执行的操作之一是应用检测，并想在某些检测流量上执行附加操作，请创建检测策略映射。检测策略映射可以识别流量并指定对流量执行的操作。

例如，您可能想丢弃所有正文长度大于 1000 字节的 HTTP 请求。

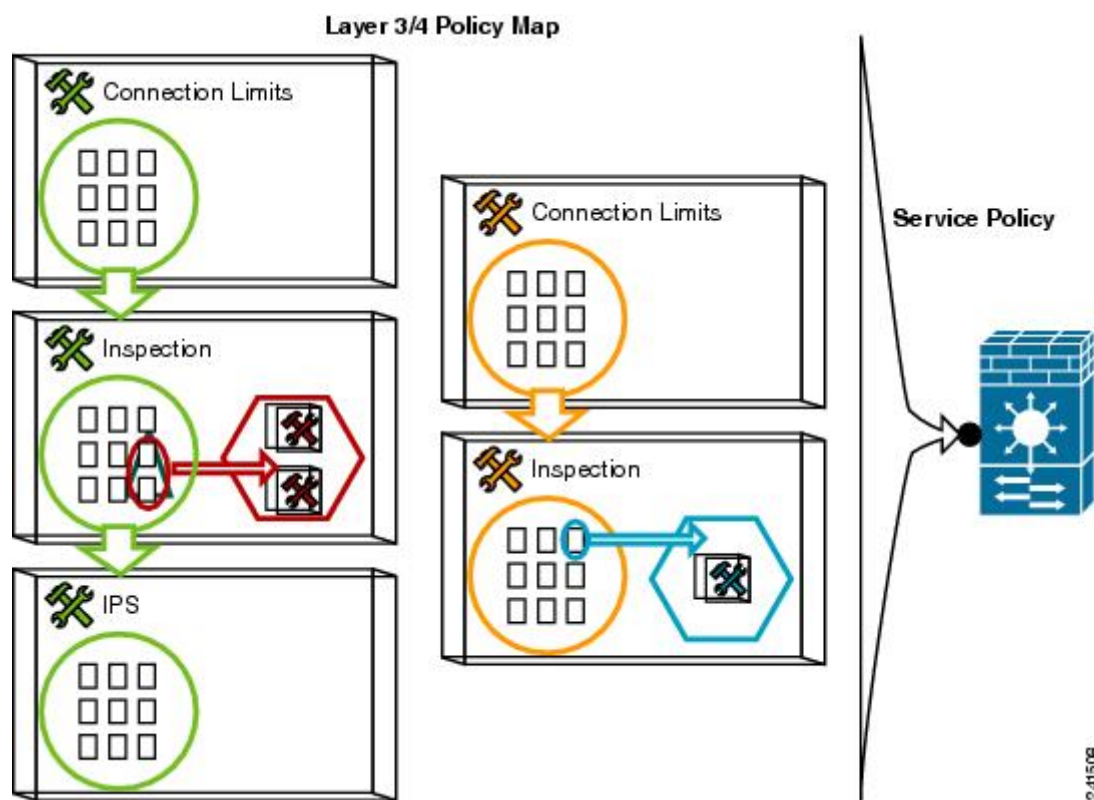


可以创建一个独立检测策略映射，该映射直接使用 **match** 命令识别流量；或者，创建一个可重复使用或进行更复杂匹配的检测类映射。例如，可以使用一个正则表达式或一组正则表达式（一个正则表达式类映射）匹配被检测数据包中的文本，并基于更小的条件范围指定操作。例如，可能想丢弃所有 URL 中包含 “example.com” 文本的 HTTP 请求。



请参阅[配置应用层协议检测](#)，第 249 页。

步骤 3 创建第 3/4 层策略映射，定义要在每个第 3/4 层类映射上执行的操作，如[定义操作（第 3/4 层策略映射）](#)，第 233 页中所述。



步骤 4 确定要应用策略映射的接口，或者全局应用策略映射，如[面向接口的应用操作（服务策略）](#)，第 235 页中所述。

身份流量（第 3/4 层类映射）

第 3/4 层类映射标识要应用操作的第 3 层和第 4 层流量。可以为每个第 3/4 层策略映射创建多个第 3/4 层类映射。

为通过流量创建第 3/4 层类映射

第 3/4 层类映射根据协议、端口、IP 地址和其他第 3 或 4 层属性匹配流量。



提示 我们建议您仅检测期待其中应用流量的端口上的流量；如果检测所有流量（例如使用 **match any**），ASA 的性能可能会受到影响。

过程

步骤 1 创建第 3/4 层类映射：**class-map** *class_map_name*

其中，*class_map_name* 是最多可包含 40 个字符的字符串。

保留名称 “class-default”。所有类型的类映射都使用同一命名空间，因此无法重复使用已被另一类型的类映射使用的名称。CLI 进入类映射配置模式。

示例：

```
hostname(config)# class-map all_udp
```

步骤 2 （可选）向类映射添加说明。

description *string*

示例：

```
hostname(config-cmap)# description All UDP traffic
```

步骤 3 使用以下某个命令匹配流量。除非另有规定，否则只能在类映射中包含一条 **match** 命令。

- **match any** - 匹配所有流量。

```
hostname(config-cmap)# match any
```

- **match access-list** *access_list_name* - 匹配扩展 ACL 指定的流量。

```
hostname(config-cmap)# match access-list udp
```

- **match port** {**tcp** | **udp** | **sctp**} {**eq** *port_num* | **range** *port_num* *port_num*} - 匹配指示协议的目标端口，可以是单一端口或连续的端口范围。对于使用多个非连续端口的应用，请使用 **match access-list** 命令并定义 ACE 来匹配每个端口。

```
hostname(config-cmap)# match tcp eq 80
```

- **match default-inspection-traffic** - 匹配默认检测流量：ASA 可检测的所有应用使用的默认 TCP 和 UDP 端口。

```
hostname(config-cmap)# match default-inspection-traffic
```

默认全局策略中使用的此命令在用于策略映射中时是一种特殊 CLI 快捷方式，可确保根据流量的目标端口对每个数据包应用正确的检测。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。因此仅在这种情况下，可以为同一类映射配置多个检测（WAAS 检测除外，该检测可以通过其他检测配置。请参阅[某些功能操作的不兼容性](#)，第 224 页，了解有关整合操作的详细信息）。通常，ASA 不会使用端口号来确定应用的检测，因此您可以灵活地对非标准端口等应用检测。

请参阅[默认检测和 NAT 限制](#)，第 245 页，查看默认端口列表。默认情况下，不是端口包含在 **match default-inspection-traffic** 命令中的所有应用都在策略映射中启用。

可以指定 **match access-list** 命令连同 **match default-inspection-traffic** 命令来缩小匹配的流量范围。由于 **match default-inspection-traffic** 命令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。

- **match dscp value1 [value2] [...] [value8]** - 匹配 IP 报头中的 DSCP 值，最多 8 个 DSCP 值。

```
hostname(config-cmap)# match dscp af43 cs1 ef
```

- **match precedence value1 [value2] [value3] [value4]** - 最多匹配 IP 报头中以 TOS 字节表示的四个优先级值，优先级值可以是 0 到 7。

```
hostname(config-cmap)# match precedence 1 4
```

- **match rtp starting_port range** - 匹配 RTP 流量，其中 *starting_port* 指定介于 2000 和 65534 之间的偶数 UDP 目标端口。*range* 指定要匹配上述 *starting_port* 的额外 UDP 端口的数量，介于 0 和 16383 之间。

```
hostname(config-cmap)# match rtp 4004 100
```

- **match tunnel-group name** - 匹配要应用 QoS 的 VPN 隧道组流量。

还可以指定另一个 **match** 命令，细化流量匹配。可以指定上述命令中除 **match any**、**match access-list** 或 **match default-inspection-traffic** 之外的任意命令。或者，还可以输入 **match flow ip destination-address** 命令，匹配隧道组中流向每个 IP 地址的流。

```
hostname(config-cmap)# match tunnel-group group1
hostname(config-cmap)# match flow ip destination-address
```

示例

以下是 **class-map** 命令的示例：

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

为管理流量创建第 3/4 层类映射

对于流入 ASA 的管理流量，您可能希望执行特定于此类流量的操作。可以指定能够匹配 ACL、TCP 或 UDP 端口的管理类映射。可用于策略映射中的管理类映射的操作类型专用于管理流量。

过程

步骤 1 创建管理类映射：**class-map type management class_map_name**

其中，*class_map_name* 是最多可包含 40 个字符的字符串。

保留名称 “class-default”。所有类型的类映射都使用同一命名空间，因此无法重复使用已被另一类型的类映射使用的名称。CLI 进入类映射配置模式。

示例：

```
hostname(config)# class-map management all_udp
```

步骤 2 （可选）向类映射添加说明。

description string

示例：

```
hostname(config-cmap)# description All UDP traffic
```

步骤 3 使用以下某个命令匹配流量。

- **match access-list** *access_list_name* - 匹配扩展 ACL 指定的流量。

```
hostname(config-cmap)# match access-list udp
```

- **match port** {**tcp** | **udp** | **sctp**} {**eq** *port_num* | **range** *port_num* *port_num*} - 匹配指示协议的目标端口，可以是单一端口或连续的端口范围。对于使用多个非连续端口的应用，请使用 **match access-list** 命令并定义 ACE 来匹配每个端口。

```
hostname(config-cmap)# match tcp eq 80
```

定义操作（第 3/4 层策略映射）

配置第 3/4 层类映射识别流量之后，使用第 3/4 层策略映射将操作与这些类关联起来。



提示 策略映射最大数量为 64 个，但每个接口只能应用一个策略映射。

过程

步骤 1 添加策略映射：**policy-map** *policy_map_name*

其中 *policy_map_name* 为策略映射的名称，最长包括 40 个字符。所有类型的策略映射都使用同一命名空间，因此无法重复使用已被另一类型的策略映射使用的名称。CLI 将进入策略映射配置模式。

示例：

```
hostname(config)# policy-map global_policy
```

步骤 2 指定以前配置的第 3/4 层类映射：**class** *class_map_name*

其中，*class_map_name* 是类映射的名称。

请参阅[身份流量（第 3/4 层类映射）](#)，第 229 页，添加类映射。

示例：

```
hostname(config-pmap)# class all_http
```

步骤 3 为该类映射指定一项或多项操作。

请参阅[使用服务策略配置的功能](#)，第 221 页。

注释

如果类映射中不存在 **match default-inspection-traffic** 命令，则允许在该类下最多配置一个 **inspect** 命令。

步骤 4 为想添加到策略映射中的每个类映射重复此过程。

示例

以下是用于连接策略的 **policy-map** 命令的示例。它限制了允许到达 Web 服务器 10.1.1.1 的连接数：

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

以下示例显示多匹配在策略映射中如何运行：

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout idle 0:10:0
```

以下示例显示流量如何与第一个可用的类映射匹配而不匹配同一功能域中指定操作的任何后续类映射：

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout idle 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout idle 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout idle 2:0:0
```

```
hostname(config-pmap-c)# set connection conn-max 2000
```

当发起 Telnet 连接时，它将与 **class telnet_traffic** 匹配。同样，如果启动 FTP 连接，则它会与 **class ftp_traffic** 进行匹配。对于除 Telnet 和 FTP 外的任何 TCP 连接，它将与 **class tcp_traffic** 进行匹配。虽然 Telnet 或 FTP 连接可与 **class tcp_traffic** 匹配，但由于它们之前已与其他类匹配，所以 ASA 不会进行此匹配。

面向接口的应用操作（服务策略）

要激活第 3/4 层策略映射，请创建一项将其应用到一个或多个接口或将其全局应用到所有接口的服务策略。使用以下命令：

```
service-policy policy_map_name {global | interface interface_name} [fail-close]
```

其中：

- **policy_map_name** 是策略映射的名称。
- **global** 可以创建一项应用于所有没有特定策略的接口的服务策略。

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。默认情况下，配置包括与所有默认应用检测流量匹配的全局策略，并且将检测全局应用到流量。默认服务策略包含以下命令：**service-policy global_policy global**。

- **interface interface_name** 通过将策略映射与接口相关联，创建服务策略。
- **fail-close** 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。

示例

例如，以下命令可以在外部接口上启用 **inbound_policy** 策略映射：

```
hostname(config)# service-policy inbound_policy interface outside
```

以下命令可禁用默认全局策略，并启用一个名为 **new_global_policy** 的新策略

```
hostname(config)# no service-policy global_policy global  
hostname(config)# service-policy new_global_policy global
```

监控服务策略

要监控服务策略，请输入以下命令：

- **show service-policy**

显示服务策略统计信息。

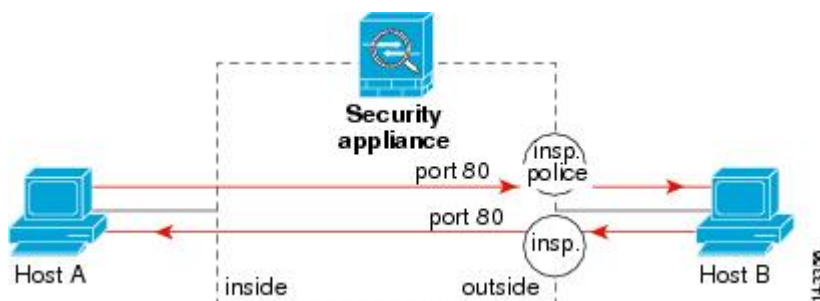
服务策略（模块化策略框架）示例

本节包括若干模块化策略框架示例。

向 HTTP 流量应用检测和 QoS 策略管制

在本例中，任何通过外部接口进出 ASA 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测进行分类。任何流出外部接口的 HTTP 流量针对策略管制进行分类。

图 37: HTTP 检测和 QoS 策略管制



请见以下适用于本示例的命令：

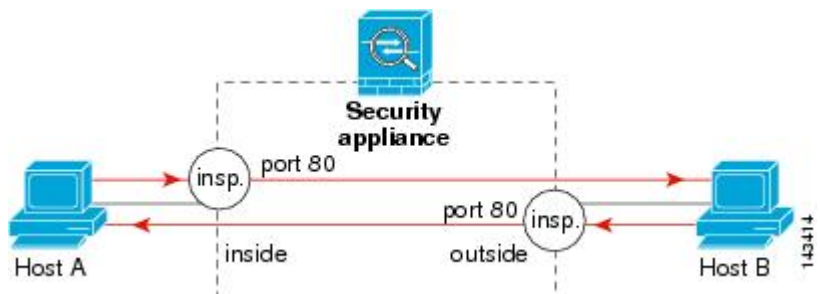
```
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# police output 250000
hostname(config)# service-policy http_traffic_policy interface outside
```

对 HTTP 流量应用全局检测

在本例中，任何通过 any 接口进入 ASA 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测进行分类。由于采用了全局策略，检测仅在流量流入每个接口时发生。

图 38: 全局 HTTP 检测



请见以下适用于本示例的命令：


```

hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map http_traffic_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# inspect http
hostname(config)# service-policy http_traffic_policy global

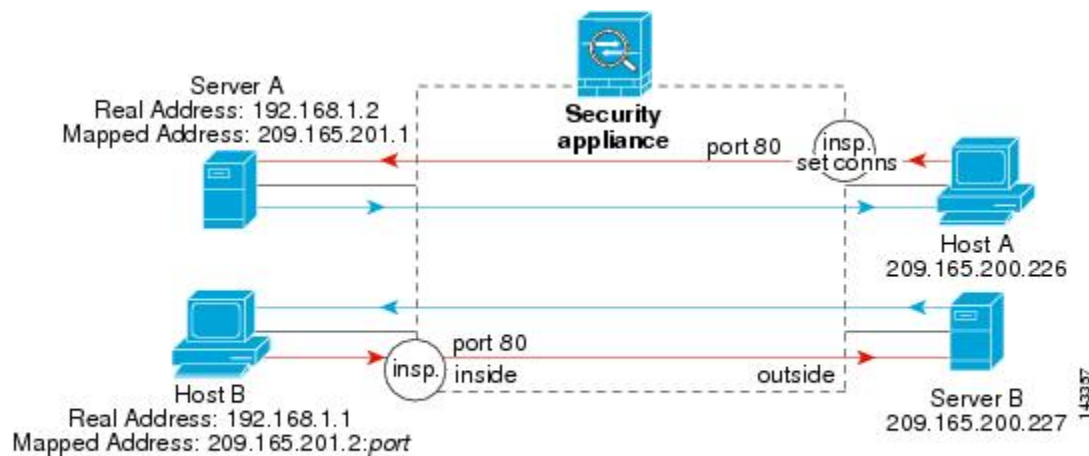
```

向流入特定服务器的 HTTP 流量应用检测和连接限制

在本例中，任何通过外部接口进入 ASA 流入服务器 A 的 HTTP 连接（端口 80 上的 TCP 流量）都针对 HTTP 检测和最大连接限制进行分类。从服务器 A 发起到主机 A 的连接不匹配类映射中的 ACL，因此这些连接不会受到影响。

任何通过内部接口进入 ASA 流入服务器 B 的 HTTP 连接都针对 HTTP 检测进行分类。从服务器 B 发起到主机 B 的连接不匹配类映射中的 ACL，因此这些连接不会受到影响。

图 39: 对于特定服务器的 HTTP 检测和连接限制



请见以下适用于本示例的命令：

```

hostname(config)# object network obj-192.168.1.2
hostname(config-network-object)# host 192.168.1.2
hostname(config-network-object)# nat (inside,outside) static 209.165.201.1
hostname(config)# object network obj-192.168.1.0
hostname(config-network-object)# subnet 192.168.1.0 255.255.255.0
hostname(config-network-object)# nat (inside,outside) dynamic 209.165.201.2
hostname(config)# access-list serverA extended permit tcp any host 209.165.201.1 eq 80
hostname(config)# access-list ServerB extended permit tcp any host 209.165.200.227 eq 80

hostname(config)# class-map http_serverA
hostname(config-cmap)# match access-list serverA
hostname(config)# class-map http_serverB
hostname(config-cmap)# match access-list serverB

hostname(config)# policy-map policy_serverA
hostname(config-pmap)# class http_serverA

```

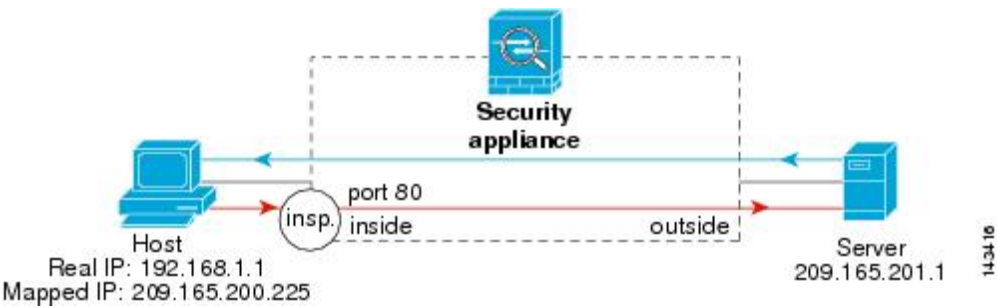
```
hostname(config-pmap-c)# inspect http
hostname(config-pmap-c)# set connection conn-max 100
hostname(config)# policy-map policy_serverB
hostname(config-pmap)# class http_serverB
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy policy_serverB interface inside
hostname(config)# service-policy policy_serverA interface outside
```

通过 NAT 对 HTTP 流量应用检测

在本例中，内部网络上的主机有两个地址：一个是实际地址 192.168.1.1，另一个是在外部网络上使用的映射 IP 地址 209.165.200.225。在类映射中的 ACL 中，必须使用实际 IP 地址。如果已将其应用到外部接口，也可以使用实际地址。

图 40: 通过 NAT 进行的 HTTP 检测



请见以下适用于本示例的命令：

```
hostname(config)# object network obj-192.168.1.1
hostname(config-network-object)# host 192.168.1.1
hostname(config-network-object)# nat (VM1,outside) static 209.165.200.225

hostname(config)# access-list http_client extended permit tcp host 192.168.1.1 any eq 80

hostname(config)# class-map http_client
hostname(config-cmap)# match access-list http_client

hostname(config)# policy-map http_client
hostname(config-pmap)# class http_client
hostname(config-pmap-c)# inspect http

hostname(config)# service-policy http_client interface inside
```

服务策略的历史记录

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。

功能名称	版本	说明
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 12 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 241 页
- [配置应用层协议检测](#)，第 249 页
- [配置正则表达式](#)，第 255 页
- [监控检测策略](#)，第 258 页
- [应用检测的历史记录](#)，第 259 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。

其他应用需要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，必须删除该检测。然后，为策略映射提供新的名称，再将其重新添加到策略中。

例如，要将 SIP 检测中的 sip-map1 替换为 sip-map2，请使用以下命令序列：

```
hostname(config)# policy-map test
hostname(config-pmap)# class sip
hostname(config-pmap-c)# no inspect sip sip-map1
hostname(config-pmap-c)# inspect sip sip-map2
```

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。例如，以下匹配命令可以按任意顺序输入，但首先匹配的是 **match request method get** 命令。

```
match request header host length gt 100
reset
match request method get
log
```

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。例如，如果一个数据包的报头长度为 1001，则该数据包匹配以下第一个命令，执行记录，然后再匹配第二个命令并进行重置。如果颠倒两个 **match** 命令的顺序，则该数据包在匹配第二个 **match** 命令之前会被丢弃并重置连接，而不会进行日志记录。

```
match request header length gt 100
  log
match request header length gt 1000
  reset
```

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。例如，以下三个类映射包含两类 **match** 命令：**match request-cmd**（优先级较高）和 **match filename**（优先级较低）。ftp3 类映射包括这两种命令，但它们根据最低优先级命令 **match filename** 排序。ftp1 类映射包括最高优先级命令，所以首先进行匹配，不考虑它在策略映射中的顺序。ftp3 类映射的排序优先级与同样包含 **match filename** 命令的 ftp2 类映射相同。它们按照在策略映射中所处的顺序进行匹配：ftp3 先于 ftp2。

```
class-map type inspect ftp match-all ftp1
  match request-cmd get
class-map type inspect ftp match-all ftp2
  match filename regex abc
class-map type inspect ftp match-all ftp3
  match request-cmd get
  match filename regex abc

policy-map type inspect ftp ftp
  class ftp3
    log
  class ftp2
    log
  class ftp1
    log
```

应用检测准则

故障转移

需要检测的多媒体会话的状态信息不通过用于状态故障转移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，才能执行状态故障转移。

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

其他准则

- 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 245 页。
- 对于所有应用检测，ASA 允许同时活动的数据连接数限为 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 10: 支持的应用检测引擎

应用	默认协议、端口	NAT 限制	标准	备注
CTIQBE	TCP/2748	无扩展 PAT。 无 NAT64。 (集群) 无静态 PAT。	—	—
DCERPC	TCP/135	无 NAT64。	—	—

应用	默认协议、端口	NAT 限制	标准	备注
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、H.225.0、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。
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	—

应用	默认协议、端口	NAT 限制	标准	备注
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	—
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。
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。

应用	默认协议、端口	NAT 限制	标准	备注
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 同样运行 Cisco Secure Firewall eXtensible 操作系统 (FXOS) 的平台上的 UDP/4161。	无 NAT 或 PAT。	RFC 1155、1157、1212、1213、1215	v.2 RFC 1902-1908; v.3 RFC 2570-2580。 在 FXOS 平台上，如果配置了 SNMP，则会自动启用该检测功能，且无法禁用。
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	—
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。	—	—

应用	默认协议、端口	NAT 限制	标准	备注
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 ESMTTP 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 245 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 除非是向现有类映射中添加检测，否则可创建一个 L3/L4 类映射来标识要应用该检测的流量。

```
class-map name
match parameter
```

示例:

```
hostname(config)# class-map dns_class_map
hostname(config-cmap)# match access-list dns
```

在默认全局策略中，`inspection_default` 类映射是包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。只有 `inspection_default` 类可以有多项检测，而且可能需要简单地编辑应用检测默认操作的现有全局策略。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。有关选择哪种类映射的详细信息，请参阅[选择适合检测的流量类](#)，第 254 页。

有关匹配语句的信息，请参阅[为通过流量创建第 3/4 层类映射](#)，第 230 页。有关使用管理层 3/4 类的 RADIUS 计费检测，请参阅[配置 RADIUS 计费检测](#)，第 360 页。

步骤 2 添加或编辑第 3/4 层策略映射，以用于设置要对类映射流量执行的操作：**policy-map name**

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，`global_policy` 策略映射会全局性分配到所有接口。如果要编辑 `global_policy`，请输入 `global_policy` 作为策略名称。

步骤 3 标识正在用于检测的第 3/4 层类映射：**class name**

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 `inspection_default` 类映射，请将 *name* 指定为 **inspection_default**。否则，将会指定在前面的操作步骤中创建的类。

必要时可以将多个类映射合并在同一策略中，因此可以创建一个类映射来匹配某些流量，创建另一个类映射来匹配不同流量。但是，如果流量匹配包含检测命令的某个类映射，然后匹配也包含检测命令的另一个类映射，将会仅使用第一个匹配的类。例如，SNMP 匹配 `inspection_default` 类映射。要启用 SNMP 检测，请启用默认类的 SNMP 检测。请勿添加另一个匹配 SNMP 的类。

步骤 4 启用应用检测：**inspect protocol**

protocol 是以下其中一个值：

表 11: 检测协议关键字

关键字	注
ctiqbe	请参阅 CTIQBE 检测 ，第 301 页。
dcerpc [<i>map_name</i>]	请参阅 DCERPC 检测，第 262 页。 如果已按照配置 DCERPC 检测策略映射，第 262 页中所述添加了 DCERPC 检测策略映射，请在此命令中识别映射名称。

关键字	注
diameter [<i>map_name</i>] [tls-proxy <i>proxy_name</i>]	请参阅Diameter 检测，第 329 页。 如果已按照配置 Diameter 检测策略映射，第 339 页中所述添加了 Diameter 检测策略映射，请在此命令中识别映射名称。 tls-proxy proxy_name 标识用于此检测的 TLS 代理。仅在要启用加密流量检测时，才需要 TLS 代理。
dns [<i>map_name</i>] [dynamic-filter-snoop]	请参阅 DNS 检测，第 264 页。 如果已按照配置 DNS 检测策略映射，第 265 页中所述添加了 DNS 检测策略映射，请在此命令中识别映射名称。默认 DNS 检测策略映射名称为 “<code>preset_dns_map</code>”。 dynamic-filter-snoop 启用僵尸网络流量过滤器专用的动态过滤器监听。应仅在使用僵尸网络流量过滤时包含此关键字。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。
esmtpt [<i>map_name</i>]	请参阅 SMTP 和扩展 SMTP 检测，第 289 页。 如果已按照配置 ESMTP 检测策略映射，第 291 页中所述添加了 ESMTP 检测策略映射，请在此命令中识别映射名称。
ftp [strict [<i>map_name</i>]]	请参阅 FTP 检测，第 269 页。 使用 strict 关键字防止网络浏览器在 FTP 请求中发送嵌入式命令，从而提高受保护网络的安全。有关详细信息，请参阅严格 FTP，第 270 页。 如果已按照配置 FTP 检测策略映射，第 271 页中所述添加了 FTP 检测策略映射，请在此命令中识别映射名称。
gtp [<i>map_name</i>]	请参阅 GTP 检测概述，第 325 页。 如果已按照配置 GTP 检测策略映射，第 333 页中所述添加了 GTP 检测策略映射，请在此命令中识别映射名称。
h323 h225 [<i>map_name</i>]	请参阅 H.323 检测，第 302 页。 如果已按照配置 H.323 检测策略映射，第 304 页中所述添加了 H323 检测策略映射，请在此命令中识别映射名称。
h323 ras [<i>map_name</i>]	请参阅 H.323 检测，第 302 页。 如果已按照配置 H.323 检测策略映射，第 304 页中所述添加了 H323 检测策略映射，请在此命令中识别映射名称。

关键字	注
http [<i>map_name</i>]	请参阅 HTTP 检测 ，第 273 页。 如果已按照 配置 HTTP 检测策略映射 ，第 274 页中所述添加了 HTTP 检测策略映射，请在此命令中识别映射名称。
ICMP	请参阅 ICMP 检查 ，第 278 页。
icmp error	请参阅 ICMP 错误检测 ，第 278 页。
ils	请参阅 ILS 检测 ，第 279 页。
im [<i>map_name</i>]	请参阅 即时消息检测 ，第 279 页。 如果添加了即时消息检测策略映射，请在此命令中识别映射名称。
ip-options [<i>map_name</i>]	请参阅 IP 选项检测 ，第 282 页。 如果已按照 配置 IP 选项检测策略映射 ，第 283 页中所述添加了 IP 选项检测策略映射，请在此命令中识别映射名称。
ipsec-pass-thru [<i>map_name</i>]	请参阅 IPsec 穿透检测 ，第 284 页。 如果已按照 配置 IPsec 穿透检测策略映射 ，第 285 页中所述添加了 IPsec 直通检测策略映射，请在此命令中识别映射名称。
ipv6 [<i>map_name</i>]	请参阅 Ipv6 检测 ，第 286 页。 如果已按照 配置 IPv6 检测策略映射 ，第 286 页中所述添加了 IPv6 检测策略映射，请在此命令中识别映射名称。
lisp [<i>map_name</i>]	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。 如果添加了 LISP 检测策略映射，请在此命令中识别映射名称。
m3ua [<i>map_name</i>]	请参阅 M3UA 检测 ，第 330 页。 如果已按照 配置 M3UA 检测策略映射 ，第 355 页中所述添加了 M3UA 检测策略映射，请在此命令中识别映射名称。
mgcp [<i>map_name</i>]	请参阅 MGCP 检测 ，第 307 页。 如果已按照 配置 MGCP 检测策略映射 ，第 308 页中所述添加了 MGCP 检测策略映射，请在此命令中识别映射名称。
netbios [<i>map_name</i>]	请参阅 NetBIOS 检测 ，第 288 页。 如果添加了 NetBIOS 检测策略映射，请在此命令中识别映射名称。
pptp	请参阅 PPTP 检测 ，第 289 页。

关键字	注
radius-accounting <i>map_name</i>	请参阅 RADIUS 计费检测概述，第 331 页。 radius-accounting 关键字仅适用于管理类映射。必须指定 RADIUS 记账检测策略映射；请参阅配置 RADIUS 计费检测策略映射，第 360 页。
rsh	请参阅 RSH 检测 ，第 289 页。
rtsp [<i>map_name</i>]	请参阅 RTSP 检测，第 310 页。 如果已按照配置 RTSP 检测策略映射，第 311 页中所述添加了 RTSP 检测策略映射，请在此命令中识别映射名称。
sctp [<i>map_name</i>]	请参阅SCTP 应用层检测，第 328 页。 如果已按照配置 SCTP 检测策略映射，第 337 页中所述添加了 SCTP 检测策略映射，请在此命令中识别映射名称。
sip [<i>map_name</i>] [tls-proxy <i>proxy_name</i>]	请参阅 SIP 检测，第 313 页。 如果已按照配置 SIP 检测策略映射，第 315 页中所述添加了 SIP 检测策略映射，请在此命令中识别映射名称。 tls-proxy <i>proxy_name</i> 标识用于这项检测的 TLS 代理。仅在要启用加密流量检测时，才需要 TLS 代理。
skinny [<i>map_name</i>]	请参阅瘦客户端 (SCCP) 检测，第 318 页。 如果已按照配置瘦小客户端 (SCCP) 检测策略映射，第 320 页中所述添加了瘦客户端检测策略映射，请在此命令中识别映射名称。
snmp [<i>map_name</i>]	请参阅 SNMP 检测，第 294 页。 如果添加了 SNMP 检测策略映射，请在此命令中识别映射名称。
sqlnet	请参阅 SQL*Net 检测 ，第 295 页。
stun	请参阅 STUN 检测 ，第 321 页。
sunrpc	请参阅 Sun RPC 检测，第 295 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 inspect sunrpc 命令。
tftp	请参阅 TFTP 检测 ，第 297 页。
waas	启用 TCP 选项 33 解析。部署思科广域应用服务产品时使用。
xdmcp	请参阅 XDMCP 检测 ，第 297 页。
vxlan	请参阅 VXLAN 检测 ，第 297 页。

注释

如果要编辑默认全局策略（或任何使用中的策略）来使用不同的检测策略映射，必须使用 **no inspect protocol** 命令删除旧的检测，然后为其提供新的检测策略映射名称并重新添加这项检测。

示例：

```
hostname(config-class)# no inspect sip
hostname(config-class)# inspect sip sip-map
```

步骤 5 如果是编辑现有服务策略（例如，称为 `global_policy` 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *polycymap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

选择适合检测的流量类

直通流量的默认第 3/4 层类映射称为 “`inspection_default`”。该类映射与使用特殊 **match** 命令 **match default-inspection-traffic** 的流量匹配，以便匹配每个应用协议的默认协议和端口。此流量类（以及通常不用于检测的 **match any**）匹配支持 IPv6 检测的 IPv4 和 IPv6 流量。有关支持 IPv6 的检测的列表，请参阅[应用检测准则](#)，第 243 页。

可以指定 **match access-list** 命令连同 **match default-inspection-traffic** 命令来缩小流向特定 IP 地址的匹配流量范围。由于 **match default-inspection-traffic** 命令指定了要匹配的端口和协议，所以 ACL 中的任何端口将被忽略。



提示 我们建议您仅检测期待其中应用流量的端口上的流量；如果检测所有流量（例如使用 **match any**），ASA 的性能可能会受到影响。

如果要匹配非标准端口，请创建适用于非标准端口的新的类映射。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 245 页。必要时可以将多个类映射合并到同一策略中，因此可以创建一个类映射来匹配某些流量，创建另一个类映射来匹配不同流量。但是，如果流量匹配包含检测命令的某个类映射，然后匹配也包含检测命令的另一个类映射，将会仅使用第一个匹配的类。例如，SNMP 匹配 `inspection_default` 类。要启用 SNMP 检测，请启用默认类的 SNMP 检测。请勿添加另一个匹配 SNMP 的类。

例如，要使用默认类映射将检测限制为针对从 10.1.1.0 到 192.168.1.0 的流量，请输入以下命令：

```
hostname(config)# access-list inspect extended permit ip 10.1.1.0 255.255.255.0
192.168.1.0 255.255.255.0
hostname(config)# class-map inspection_default
hostname(config-cmap)# match access-list inspect
```

使用以下命令可查看整个类映射：

```
hostname(config-cmap)# show running-config class-map inspection_default
!
class-map inspection_default
  match default-inspection-traffic
  match access-list inspect
!
```

要检测端口 21 和 1056（非标准端口）上的 FTP 流量，请创建指定端口的 ACL，并将其分配给一个新的类映射：

```
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 21
hostname(config)# access-list ftp_inspect extended permit tcp any any eq 1056
hostname(config)# class-map new_inspection
hostname(config-cmap)# match access-list ftp_inspect
```

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

使用 **Ctrl+V** 对 CLI 中的所有特殊字符进行转义，例如问号 (?) 或制表符。例如，键入 **d[Ctrl+V]?g** 以在配置中输入 **d?g**。

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 12: 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 。
(exp)	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 。
{x} 或 {x,}	最小重复限定符	至少重复 x 次。例如， ab(xy){2}z 匹配 abxyxyz 、 abxyxyxyz 等等。
[abc]	字符类	匹配方括号中的任意字符。例如， [abc] 匹配 a 、 b 或 c 。
[^abc]	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。
[a-c]	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。

字符	说明	注
\	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。
\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 测试正则表达式，以确保其匹配内容与您的预期相符：**test regex *input_text* *regular_expression***

其中 *input_text* 参数为使用正则表达式要匹配的字符串，最长为 201 个字符。*regular_expression* 参数最多可包含 100 个字符。

使用 **Ctrl+V** 可转义 CLI 中的所有特殊字符。例如，要在 **test regex** 命令的输入文本中输入制表符，必须输入 **test regex "test[Ctrl+V Tab]" "test\t"**。

如果正则表达式匹配输入文本，您将看到以下消息：

```
INFO: Regular expression match succeeded.
```

如果正则表达式不匹配输入文本，您将看到以下消息：

```
INFO: Regular expression match failed.
```

步骤 2 若在测试后要添加正则表达式，请输入以下命令：**regex *name* *regular_expression***

其中，*name* 参数最多可包含 40 个字符。*regular_expression* 参数最多可包含 100 个字符。

示例

以下示例创建两个用于检测策略映射的正则表达式：

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

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 创建正则表达式类映射：**class-map type regex match-any class_map_name**

其中，*class_map_name* 是最多可包含 40 个字符的字符串。保留名称 “class-default”。所有类型的类映射都使用同一命名空间，因此无法重复使用已被另一类型的类映射使用的名称。

match-any 关键字指明如果流量至少匹配类映射中的一个正则表达式，那么它匹配类映射。

步骤 2 （可选）向类映射添加说明：**description string**

步骤 3 通过为每个正则表达式输入以下命令标识要包括的正则表达式：**match regex regex_name**

示例

以下示例创建两个正则表达式，并将它们添加到正则表达式类映射。如果流量包含字符串 “example.com” 或 “example2.com”，则其匹配该类映射。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex url_example
hostname(config-cmap)# match regex url_example2
```

监控检测策略

要监控检测服务策略，请输入以下命令。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 ctique**

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。

应用检测的历史记录

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 。

功能名称	版本	说明
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 13 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 241 页。

- [DCERPC 检测](#)，第 262 页
- [DNS 检测](#)，第 264 页
- [FTP 检测](#)，第 269 页
- [HTTP 检测](#)，第 273 页
- [ICMP 检查](#)，第 278 页
- [ICMP 错误检测](#)，第 278 页
- [ILS 检测](#)，第 279 页
- [即时消息检测](#)，第 279 页
- [IP 选项检测](#)，第 282 页
- [IPsec 穿透检测](#)，第 284 页
- [Ipv6 检测](#)，第 286 页
- [NetBIOS 检测](#)，第 288 页
- [PPTP 检测](#)，第 289 页
- [RSH 检测](#)，第 289 页
- [SMTP 和扩展 SMTP 检测](#)，第 289 页
- [SNMP 检测](#)，第 294 页
- [SQL*Net 检测](#)，第 295 页
- [Sun RPC 检测](#)，第 295 页
- [TFTP 检测](#)，第 297 页
- [XDMCP 检测](#)，第 297 页
- [VXLAN 检测](#)，第 297 页
- [基本互联网协议检测的历史记录](#)，第 298 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端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。客户端和服务端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。

过程

步骤 1 （可选）创建 DCERPC 检测类映射。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect dcerpc [match-all | match-any] class_map_name**

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。**match-any** 关键字指定只要流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 进入类映射配置模式。

b) 指定要使用以下 **match** 命令对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] uuid type** - 匹配 DCERPC 消息的通用唯一标识符 (UUID)。type 可以是下列项目之一：
 - **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。

c) 输入 **exit** 退出类映射配置模式。**步骤 2** 创建 DCERPC 检测策略映射：**policy-map type inspect dcerpc policy_map_name**

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 （可选）添加策略映射说明：**description string****步骤 4** 要对匹配的流量应用操作，请执行以下步骤。

a) 使用以下其中一种方法指定要对其执行操作的流量：

- 如果您已创建 DCERPC 类映射，请输入以下命令对其进行指定：**class class_map_name**
- 使用介绍用于 DCERPC 类映射的 **match** 命令之一，直接在策略映射中指定流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **reset [log]** - 丢弃数据包、关闭连接并向服务器和/或客户端发送 TCP 重置。
- **log**- 发送系统日志消息。您可以单独使用此选项，也可以与其他某项操作一起使用。

可以在策略映射中指定多个 **class** 或 **match** 命令。

示例：

```
hostname(config)# policy-map type inspect dcerpc dcerpc-map
hostname(config-pmap)# match uuid ms-rpc-epm
hostname(config-pmap-c)# log
```

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **timeout pinhole hh:mm:ss** - 为 DCERPC 针孔配置超时，并覆盖全局系统针孔超时：2 分钟。超时可以是 00:00:01 到 119:00:00。
- **endpoint-mapper [epm-service-only] [lookup-operation [timeout hh:mm:ss]]** - 配置用于终端映射器流量的选项。在绑定期间，**epm-service-only** 关键字将实施终端映射器服务，以便仅处理其服务流量。**lookup-operation** 关键字将启用终端映射器服务的查找操作。可以配置查找操作生成的针孔超时。如果没有为查找操作配置超时，将会使用针孔超时命令或默认值。

示例

以下示例显示如何使用为 DCERPC 针孔配置的超时定义 DCERPC 检测策略映射。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc-map

hostname(config)# service-policy global-policy global
```

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 249 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）。

请参阅以下默认 DNS 检测命令：

```
class-map inspection default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
! ...
service-policy global_policy global
```

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。

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 （可选）执行以下步骤创建 DNS 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略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。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串 “example.com”，则包含 “example.com” 的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect dns [match-all | match-any] class_map_name**

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。**match-any** 关键字指定只要流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b) （可选）向类映射添加说明：**description string**

其中，*string* 是对类映射的说明（最多可包含 200 个字符）。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] header-flag [eq] {f_name [f_name...] | f_value}** - 匹配 DNS 标志。*f_name* 参数是以下 DNS 标志名称之一：**AA**（授权应答）、**QR**（查询）、**RA**（可用递归）、**RD**（所需递归）、**TC**（截断）。*f_value* 参数是以 0x 开头的十六进制的 16 位值，范围是 0x0 到 0xffff。**Eq** 关键字指定精确匹配（完全匹配）；如果没有 **eq** 关键字，数据包只需匹配指定的报头之一（任意匹配）。例如，**match header-flag AA QR**。
- **match [not] dns-type {eq {t_name | t_value} | range t_value1 t_value2}** - 匹配 DNS 类型。*t_name* 参数是以下 DNS 类型名称之一：**A**（IPv4 地址）、**AXFR**（完整区域传送）、**CNAME**（规范名称）、**IXFR**（增量区域传输）、**NS**（授权域名服务器）、**SOA**（授权区域起始）或 **TSIG**（事务数字签名）。*t_value* 参数为 DNS 类型字段中的任意值 (0-65535)。**range** 关键字指定范围，**eq** 关键字指定精确匹配。例如：**match dns-type eq A**。
- **match [not] dns-class {eq {in | c_value} | range c_value1 c_value2}** - 匹配 DNS 类。该类为 **in**（对于互联网）或 **c_value**（DNS 类字段中的任意值，范围介于 0 到 65535 之间）。**range** 关键字指定范围，**eq** 关键字指定精确匹配。例如：**match dns-class eq in**。
- **match [not] {question | resource-record {answer | authority | additional}}** - 匹配 DNS 问题或资源记录。**question** 关键字指定 DNS 消息的问题部分。**Resource-record** 关键字指定资源记录的以下部分之一：**answer**、**authority** 或 **additional**。例如：**match resource-record answer**。
- **match [not] domain-name regex {regex_name | class class_name}** - 根据指定的正则表达式或正则表达式类匹配 DNS 消息域名列表。

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 DNS 检测策略映射：**policy-map type inspect dns policy_map_name**

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 （可选）添加策略映射说明：**description string**

步骤 4 要对匹配的流量应用操作，请执行以下步骤。

a) 使用以下其中一种方法指定要对其执行操作的流量：

- 如果您已创建 DNS 类映射，请输入以下命令对其进行指定：**class class_map_name**
- 要直接在策略映射中指定流量，请对 DNS 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop [log]** - 丢弃匹配的所有数据包。
- **drop-connection [log]** - 丢弃数据包并关闭连接。
- **mask [log]** - 掩蔽数据包的匹配部分。此操作仅适用于报头标志匹配项。
- **log** - 发送系统日志消息。您可以单独使用此选项，也可以与其他某项操作一起使用。
- **enforce-tsig [drop] [log]** - 强制消息中包含 TSIG 资源记录。可以丢弃数据包但不丢弃 TSIG 资源记录，可以记录数据包，也可以丢弃并记录数据包。可以将此选项与针对报头标志匹配项的掩蔽操作结合使用；否则，此操作与其他操作相互排斥。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅[如何处理多个流量类，第 242 页](#)。

示例：

```
hostname(config)# policy-map type inspect dns dns-map
hostname(config-pmap)# class dns-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match header-flag eq aa
hostname(config-pmap-c)# drop log
```

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项。

- **dnsencrypt** - 启用 DNSCrypt 以加密设备与思科 Umbrella 之间的连接。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。
- **dns-guard** - 启用 DNS 保护。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。
- **id-mismatch count number duration seconds action log** - 为过多的 DNS ID 不匹配启用日志记录，其中 **count number duration seconds** 参数指定在发送系统消息日志之前允许的最大每秒不匹配实例数量。
- **id-randomization** - 随机化 DNS 查询的 DNS 标识符。

- **message-length maximum** {*length* | **client** {*length* | **auto**} | **server** {*length* | **auto**}} - 设置最大 DNS 消息长度（512 至 65535 字节）。还可以设置客户端或服务器消息的最大长度。**auto** 关键字将最大长度设置为资源记录中的值。
- **nat-rewrite** - 根据 NAT 配置转换 DNS 记录。
- **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）。
- **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。
- **tsig enforced action** {[**drop**] [**log**]} - 要求必须有 TSIG 资源记录。可以丢弃和/或记录不符合要求的数据包。
- **umbrella** [**tag** *umbrella_policy*] [**fail-open**] - 启用思科 Umbrella 并选择性地指定要应用于设备的思科 Umbrella 策略的名称 (**tag**)。如果未指定策略，则会应用默认策略。有关详细信息，请参阅[思科 Umbrella，第 95 页](#)。

如果希望 DNS 解析在 Umbrella DNS 服务器不可用条件下运行，则请包含 **fail-open** 关键字。故障时打开的情况下，如果思科 Umbrella DNS 服务器不可用，则 Umbrella 会在该策略映射上自动禁用，并允许向系统上配置的其他 DNS 服务器发送 DNS 请求（若有）。当 DNS 服务器恢复可用状态时，策略映射会恢复使用它们。如果未包含该选项，则 DNS 请求会继续发送至无法访问的 Umbrella 解析器，因此这些请求不会收到任何回复。

示例：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
hostname(config-pmap-p)# message-length maximum 1024
hostname(config-pmap-p)# nat-rewrite
hostname(config-pmap-p)# protocol-enforcement
```

示例

以下示例显示如何在全局默认配置中使用新的检测策略映射：

```
regex domain_example "example\.com"
regex domain_foo "foo\.com"

! define the domain names that the server serves
class-map type inspect regex match-any my_domains
  match regex domain_example
  match regex domain_foo

! Define a DNS map for query only
class-map type inspect dns match-all pub_server_map
  match not header-flag QR
  match question
  match not domain-name regex class my_domains
```



```
policy-map type inspect dns new_dns_map
  class pub_server_map
    drop log
  match header-flag RD
  mask log
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite

policy-map global_policy
  class inspection_default
    no inspect dns preset_dns_map
    inspect dns new_dns_map
  service-policy global_policy global
```

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 249 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 **inspect ftp** 命令中包含 **strict** 选项。

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。此外，您必须确保只对 FTP 端口进行检查（TCP/21 是正常的 FTP 端口）。对非 FTP 流量进行严格的 FTP 检查可能会导致意外的流量损失，尤其是 HTTP 流量。

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。

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 （可选）执行以下步骤创建 FTP 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略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。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串“example.com”，则包含“example.com”的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect ftp [match-all | match-any] class_map_name**

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。**match-any** 关键字指定只要流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b) （可选）向类映射添加说明：**description string**

其中，*string* 是对类映射的说明（最多可包含 200 个字符）。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] filename regex {regex_name | class class_name}** - 将 FTP 传输中的文件名与指定的正则表达式或正则表达式类进行匹配。
- **match [not] filetype regex {regex_name | class class_name}** - 将 FTP 传输中的文件类型与指定的正则表达式或正则表达式类进行匹配。

- **match [not] request-command** *ftp_command* [*ftp_command...*] - 匹配以下一个或多个 FTP 命令：
 - **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。
- **match [not] server regex** {*regex_name* | **class** *class_name*} - 将 FTP 服务器名称与指定的正则表达式或正则表达式类进行匹配。
- **match [not] username regex** {*regex_name* | **class** *class_name*} - 将 FTP 用户名与指定的正则表达式或正则表达式类进行匹配。

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 FTP 检测策略映射：**policy-map type inspect ftp** *policy_map_name*

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 （可选）添加策略映射说明：**description** *string*

步骤 4 要对匹配的流量应用操作，请执行以下步骤。

a) 使用以下其中一种方法指定要对其执行操作的流量：

- 如果您已创建 FTP 类映射，请输入以下命令对其进行指定：**class** *class_map_name*
- 要直接在策略映射中指定流量，请对 FTP 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 输入下列命令，以指定要对匹配流量执行的操作：

- **reset [log]** - 丢弃数据包、关闭连接并向服务器和/或客户端发送 TCP 重置。添加 **log** 关键字以发送系统日志消息。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅[如何处理多个流量类，第 242 页](#)。

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **mask-banner** - 遮蔽来自 FTP 服务器的问候横幅。
- **mask-syst-reply** 遮蔽对 **syst** 命令的应答。

示例

提交用户名和密码之前，所有 FTP 用户均可以看到问候横幅。默认情况下，该横幅包含对于试图发现系统缺陷的黑客来说很有用的版本信息。以下示例显示如何遮蔽该横幅：

```
hostname(config)# policy-map type inspect ftp mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner

hostname(config)# class-map match-all ftp-traffic
hostname(config-cmap)# match port tcp eq ftp

hostname(config)# policy-map ftp-policy
hostname(config-pmap)# class ftp-traffic
hostname(config-pmap-c)# inspect ftp strict mymap

hostname(config)# service-policy ftp-policy interface inside
```

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 249 页](#)。

HTTP 检测

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。

以下各节介绍 HTTP 检测引擎。

HTTP 检测概述

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。

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 （可选）执行以下步骤创建 HTTP 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略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。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串“example.com”，则包含“example.com”的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect http [match-all | match-any] class_map_name**

其中, *class_map_name* 是类映射的名称。**match-all** 关键字为默认值, 指定流量必须匹配所有条件, 才能匹配类映射。**match-any** 关键字指定只要流量至少与一个 **match** 语句匹配, 即为与类映射匹配。CLI 将进入类映射配置模式, 可以在该模式下输入一个或多个 **match** 命令。

b) (可选) 向类映射添加说明: **description string**

其中, *string* 是对类映射的说明 (最多可包含 200 个字符)。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令, 将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] req-resp content-type mismatch** - 匹配 HTTP 响应中的 content-type 字段与相应 HTTP 请求消息中的接受字段不匹配的流量。
- **match [not] request args regex {regex_name | class class_name}** - 将在 HTTP 请求消息参数中找到的文本与指定的正则表达式或正则表达式类进行匹配。
- **match [not] request body {regex {regex_name | class class_name} | length gt bytes}** - 将在 HTTP 请求消息正文中找到的文本与指定的正则表达式或正则表达式类进行匹配, 或者匹配请求正文长度大于指定长度的消息。
- **match [not] request header {field | regex regex_name} regex {regex_name | class class_name}** - 将 HTTP 请求消息报头中字段的内容与指定的正则表达式或正则表达式类进行匹配。可以明确指定字段名称, 或者将字段名称与正则表达式进行匹配。字段名称包括: 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。
- **match [not] request header {field | regex {regex_name | class class_name}} {length gt bytes | count gt number}** - 匹配 HTTP 请求消息报头中指定字段的长度或报头中的总字段数 (数量)。可以明确指定字段名称, 或者将字段名称与正则表达式或正则表达式类进行匹配。上一要点中列出了字段名称。
- **match [not] request header {length gt bytes | count gt number | non-ascii}** - 匹配 HTTP 请求消息报头的总长度、报头中的总字段数 (数量) 或包含非 ASCII 字符的报头。
- **match [not] request method {method | regex {regex_name | class class_name}}** - 匹配 HTTP 请求方法。可以明确指定方法, 或者将方法与正则表达式进行匹配。方法包括: 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、revlabel、revlog、revnum、save、search、setattribute、startrev、stoprev、subscribe、trace、unedit、unlock、unsubscribe。
- **match [not] request uri {regex {regex_name | class class_name} | length gt bytes}** - 将 HTTP 请求消息 URI 中找到的文本与指定的正则表达式或正则表达式类进行匹配, 或者匹配请求 URI 长度大于指定长度的消息。

- **match [not] response body {active-x | java-applet | regex {regex_name | class class_name}}** - 将 HTTP 响应消息正文中找到的文本与指定的正则表达式或正则表达式类进行匹配，或者注释掉 Java 小应用程序和 Active X 对象标签以便对其进行过滤。
- **match [not] response body length gt bytes** - 匹配正文长度大于指定长度的 HTTP 响应消息。
- **match [not] response header {field | regex regex_name} regex {regex_name | class class_name}** - 将 HTTP 响应消息报头中字段的內容与指定的正则表达式或正则表达式类进行匹配。可以明确指定字段名称，或者将字段名称与正则表达式进行匹配。字段名称包括：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。
- **match [not] response header {field | regex {regex_name | class class_name}} {length gt bytes | count gt number}** - 匹配 HTTP 响应消息报头中指定字段的长度或报头中的总字段数（数量）。可以明确指定字段名称，或者将字段名称与正则表达式或正则表达式类进行匹配。上一要点中列出了字段名称。
- **match [not] response header {length gt bytes | count gt number | non-ascii}** - 匹配 HTTP 响应消息报头的总长度、报头中的总字段数（数量）或包含非 ASCII 字符的报头。
- **match [not] response status-line regex {regex_name | class class_name}** - 将 HTTP 响应消息状态行中找到的文本与指定的正则表达式或正则表达式类进行匹配。

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 HTTP 检测策略映射：**policy-map type inspect http policy_map_name**

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 （可选）添加策略映射说明：**description string**

步骤 4 要对匹配的流量应用操作，请执行以下步骤。

a) 使用以下其中一种方法指定要对其执行操作的流量：

- 如果您已创建 HTTP 类映射，请输入以下命令对其进行指定：**class class_map_name**
- 要直接在策略映射中指定流量，请对 HTTP 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop-connection [log]** - 丢弃数据包并关闭连接。
- **reset [log]** - 丢弃数据包、关闭连接并向服务器和/或客户端发送 TCP 重置。
- **log** - 发送系统日志消息。您可以单独使用此选项，也可以与其他某项操作一起使用。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅[如何处理多个流量类，第 242 页](#)。

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **body-match-maximum number** - 设置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。
- **protocol-violation action {drop-connection [log] | reset [log] | log}** - 检查 HTTP 协议违规情况。必须选择要对违规情况执行的操作（断开连接、重置连接或记录连接）以及是否启用或禁用日志记录。
- **spooof-server string** - 替代服务器报头字段的字符串。WebVPN 流不受 spoof-server 命令影响。

示例

以下示例显示如何定义如下 HTTP 检测策略映射：允许并记录使用“GET”或“PUT”方法尝试访问“www.xyz.com/*.asp”或“www.xyz[0-9][0-9].com”的任何 HTTP 连接。默认允许 URL/方法的所有其他组合。

```
hostname(config)# regex url1 "www\.xyz\.com/.*\.asp"
hostname(config)# regex url2 "www\.xyz[0-9][0-9]\.com"
hostname(config)# regex get "GET"
hostname(config)# regex put "PUT"

hostname(config)# class-map type regex match-any url_to_log
hostname(config-cmap)# match regex url1
hostname(config-cmap)# match regex url2
hostname(config-cmap)# exit

hostname(config)# class-map type regex match-any methods_to_log
hostname(config-cmap)# match regex get
hostname(config-cmap)# match regex put
hostname(config-cmap)# exit

hostname(config)# class-map type inspect http http_url_policy
hostname(config-cmap)# match request uri regex class url_to_log
hostname(config-cmap)# match request method regex class methods_to_log
hostname(config-cmap)# exit

hostname(config)# policy-map type inspect http http_policy
hostname(config-pmap)# class http_url_policy
hostname(config-pmap-c)# log
```

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 249 页。

ICMP 检查

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。



注释 即使禁用了 ICMP 检查，NAT 也会在转换数据包时使用 ICMP 检测。

有关启用 ICMP 检测的信息，请参阅[配置应用层协议检测](#)，第 249 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 traceroute 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。



注释 如果有可能对 ICMP 数据包使用 NAT，则应始终启用 ICMP 错误检测。由于 NAT 会自动使用 ICMP 检测 ICMP 数据包，因此即使您禁用了 ICMP 检测，使用映射的目标地址作为源地址也会让人觉得扫描仪正在检查您的网络。例如，在未启用 ICMP 错误检测的情况下，如果回应请求数据包的目标已被转换，那么当它被嵌入到 ICMP 超时响应中时，超时请求的外层报头就会使用被转换的目标作为源地址。如果启用 ICMP 错误检测，超时源地址将被设置为正确值。

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 249 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。这就需要提供的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 249 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。

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 （可选）执行以下步骤创建 IM 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略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。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串 “example.com”，则包含 “example.com” 的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect im [match-all | match-any] class_map_name**

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。**match-any** 关键字指定只要流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b) （可选）向类映射添加说明：**description string**

其中，*string* 是对类映射的说明（最多可包含 200 个字符）。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] protocol {im-yahoo | im-msn}** - 匹配特定 IM 协议（Yahoo 或 MSN）。
- **match [not] service {chat | file-transfer | webcam | voice-chat | conference | games}** - 匹配特定 IM 服务。
- **match [not] login-name regex {regex_name | class class_name}** - 将 IM 消息的源客户端登录名与指定的正则表达式或正则表达式类进行匹配。
- **match [not] peer-login-name regex {regex_name | class class_name}** - 将 IM 消息的目标对等体登录名与指定的正则表达式或正则表达式类进行匹配。
- **match [not] ip-address ip_address mask** - 匹配 IM 消息的源 IP 地址和掩码。
- **match [not] peer-ip-address ip_address mask** - 匹配 IM 消息的目标 IP 地址和掩码。
- **match [not] version regex {regex_name | class class_name}** - 将 IM 消息的版本与指定的正则表达式或正则表达式类进行匹配。
- **match [not] filename regex {regex_name | class class_name}** - 将 IM 消息的文件名与指定的正则表达式或正则表达式类进行匹配。MSN IM 协议不支持这种匹配。

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 IM 检测策略映射：**policy-map type inspect im policy_map_name**

其中, *policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 (可选) 添加策略映射说明: **description string**

步骤 4 要对匹配的流量应用操作, 请执行以下步骤。

a) 使用以下其中一种方法指定要对其执行操作的流量:

- 如果您已创建 IM 类映射, 请输入以下命令对其进行指定: **class class_map_name**
- 要直接在策略映射中指定流量, 请对 IM 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令, 将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 输入下列命令, 以指定要对匹配流量执行的操作:

- **drop-connection [log]** - 丢弃数据包并关闭连接。
- **reset [log]** - 丢弃数据包、关闭连接并向服务器和/或客户端发送 TCP 重置。
- **log** - 发送系统日志消息。您可以单独使用此选项, 也可以与其他某项操作一起使用。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息, 请参阅 [如何处理多个流量类, 第 242 页](#)。

示例

以下示例显示如何定义 IM 检测策略映射。

```
hostname(config)# regex loginname1 "ying@yahoo.com"
hostname(config)# regex loginname2 "Kevin@yahoo.com"
hostname(config)# regex loginname3 "rahul@yahoo.com"
hostname(config)# regex loginname4 "darshant@yahoo.com"
hostname(config)# regex yahoo_version_regex "1\\.0"
hostname(config)# regex gif_files "\\.gif"
hostname(config)# regex exe_files "\\.exe"

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4

hostname(config)# class-map type inspect im match-any yahoo_file_block_list
hostname(config-cmap)# match filename regex gif_files
hostname(config-cmap)# match filename regex exe_files

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yahoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex

hostname(config)# class-map type inspect im match-all yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex
```

```
hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map type inspect im im_policy_all
hostname(config-pmap)# class yahoo_file_block_list
hostname(config-pmap-c)# match service file-transfer
hostname(config-pmap)# class yahoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yahoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspect_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

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 249 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。

以下是策略映射配置：

```
policy-map type inspect ip-options _default_ip_options_map
description Default IP-OPTIONS policy-map
parameters
router-alert action allow
```

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。

过程

步骤 1 创建 IM 检测策略映射：**policy-map type inspect ip-options *policy_map_name***

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description *string***

步骤 3 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

步骤 4 标识希望允许的选项。

可以检测以下选项。在所有情况下，**allow** 操作允许包含指定选项且未经过修改的数据包；**clear** 操作允许包含指定选项的数据包，但会从报头中删除该选项。

使用命令的 **no** 形式可从映射中删除该选项。任何包含映射中未包括的选项的数据包都会被丢弃，即使数据包中包含其他允许或清除的选项。

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>)。

- **default action {allow | clear}** - 为映射中未显式包括的任何选项设置默认操作。如果未设置默认操作 allow 或 clear，包含不允许的选项的数据包将被丢弃
- **basic-security action {allow | clear}** - 允许或清除“安全”(SEC) 选项。
- **commercial-security action {allow | clear}** - 允许或清除“商业安全”(CIPSO) 选项。
- **ool action {allow | clear}** - 允许或清除“选项列表末尾”选项。
- **exp-flow-control action {allow | clear}** - 允许或清除“实验流控制”(FINN) 选项。

- **exp-measurement action {allow | clear}** - 允许或清除“实验测量值”(ZSU) 选项。
- **extended-security action {allow | clear}** - 允许或清除“扩展安全”(E-SEC) 选项。
- **imi-traffic-descriptor action {allow | clear}** - 允许或清除“IMI 流量描述符”(IMITD) 选项。
- **nop action {allow | clear}** - 允许或清除“未运行”选项。
- **quick-start action {allow | clear}** - 允许或清除“快速启动”(QS) 选项。
- **record-route action {allow | clear}** - 允许或清除“记录路由”(RR) 选项。
- **router-alert action {allow | clear}** - 允许或清除“路由器警报”(RTRALT) 选项。
- **timestamp action {allow | clear}** - 允许或清除“时间戳”(TS) 选项。
- **{0-255} action {allow | clear}** - 允许或清除根据选项类型编号标识的选项。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>)。

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 249 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。

过程

步骤 1 创建 IPsec 穿透检测策略映射：**`policy-map type inspect ipsec-pass-thru policy_map_name`**

其中，`policy_map_name` 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**`description string`**

步骤 3 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **`no`** 形式可禁用该选项：

- **`esp per-client-max number timeout time`** - 允许 ESP 隧道并设置每个客户端的最大允许连接数和空闲超时（格式为 hh:mm:ss）。要允许无限连接数，请指定 0。
- **`ah per-client-max number timeout time`** - 允许 AH 隧道。这些参数的含义与 `esp` 命令的含义相同。

示例

以下示例显示如何使用 ACL 来标识 IKE 流量、定义 IPsec 穿透参数映射、定义策略以及将策略应用于外部接口：

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

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 Pw6 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。

以下是策略映射配置：

```
policy-map type inspect ipv6 _default_ipv6_map
  description Default IPV6 policy-map
  parameters
    verify-header type
    verify-header order
  match header routing-type range 0 255
  drop log
```

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 创建 IPv6 检测策略映射：**policy-map type inspect ipv6 policy_map_name**

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description string**

步骤 3 （可选）根据 IPv6 消息中的报头丢弃或记录流量。

a) 根据 IPv6 报头标识流量：**match header type**

其中 *type* 是下列项目之一：

- **ah** - 匹配 IPv6 身份验证扩展报头。
- **count gt number** - 指定 IPv6 扩展报头的最大数量（0 至 255）。

- **destination-option** - 匹配 IPv6 目标选项扩展报头。
- **esp** - 匹配 IPv6 封装安全负载 (ESP) 扩展报头。
- **fragment** - 匹配 IPv6 分片扩展报头。
- **hop-by-hop** - 匹配 IPv6 逐跳扩展报头。
- **routing-address count gt number** - 设置 IPv6 路由报头类型 0 地址的最大数量（大于 0 至 255 之间的值）。
- **routing-type {eq | range} number** - 匹配 IPv6 路由报头类型（0 至 255）。对于范围，请用空格将各个值隔开，例如，**30 40**。

b) 指定要对匹配的数据包执行的操作。可以丢弃数据包和（可选）记录数据包，或者只记录数据包。如果未输入操作，将会记录数据包。

- **drop [log]** - 丢弃匹配的所有数据包。
- **log** - 发送系统日志消息。您可以单独使用此选项，也可以与其他某项操作一起使用。

c) 重复以上步骤，直至标识出所有要丢弃或记录的报头。

步骤 4 配置影响检测引擎的参数。

a) 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **verify-header type** - 仅允许已知的 IPv6 扩展报头。
- **verify-header order** - 按照 RFC 2460 的规定实施 IPv6 扩展报头顺序。

示例

以下示例创建的检测策略将会丢弃并记录带有逐跳报头、目标选项报头、路由地址报头和路由类型 0 报头的所有 IPv6 数据包。此示例还强制报头顺序和类型。

```
policy-map type inspect ipv6 ipv6-pm
parameters
  verify-header type
  verify-header order
match header hop-by-hop
  drop log
match header destination-option
  drop log
match header routing-address count gt 0
  drop log
```

```

match header routing-type eq 0
  drop log

policy-map global_policy
  class class-default
    inspect ipv6 ipv6-pm
  !
service-policy global_policy global

```

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 249 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 创建 NetBIOS 检测策略映射：**policy-map type inspect netbios *policy_map_name***

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description *string***

步骤 3 进入参数配置模式。

```

hostname(config-pmap)# parameters
hostname(config-pmap-p)#

```

步骤 4 指定要对 NETBIOS 协议违规采取的操作：**protocol-violation action {drop [log] | log}**

其中，**drop** 操作丢弃数据包。如果策略映射与流量匹配，**log** 操作将会发送系统日志消息。

示例

```

hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop log

hostname(config)# policy-map netbios_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# no inspect netbios

```

```
hostname(config-pmap-c)# inspect netbios netbios_map
```

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 249 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 249 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。客户端和服务端协商出 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 249 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。

以下是策略映射配置：

```
policy-map type inspect esmtp _default_esmtp_map
description Default ESMTP policy-map
parameters
mask-banner
no mail-relay
no special-character
allow-tls
match cmd line length gt 512
drop-connection log
match cmd RCPT count gt 100
drop-connection log
match body line length gt 998
log
match header line length gt 998
drop-connection log
match sender-address length gt 320
drop-connection log
match MIME filename length gt 255
drop-connection log
match ehlo-reply-parameter others
mask
```

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 创建 ESMTP 检测策略映射：**policy-map type inspect esmtp policy_map_name**

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description string**

步骤 3 要对匹配的流量应用操作，请执行以下步骤。

a) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] body {length | line length} gt bytes** - 匹配 ESMTP 消息正文长度或其行长度大于指定字节数的消息。
- **match [not] cmd verb verb1 [verb2...]** - 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、etrn、helo、help、mail、noop、quit、rcpt、rset、saml、sowl、vrfy。
- **match [not] cmd line length gt bytes** - 匹配命令谓词中一行的长度大于指定字节数的消息。
- **match [not] cmd rcpt count gt count** - 匹配收件人数量大于指定数量的消息。
- **match [not] ehlo-reply-parameter parameter [parameter2...]** - 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、etrn、others、pipelining、size、vrfy。
- **match [not] header {length | line length} gt bytes** - 匹配 ESMTP 报头长度或其行长度大于指定字节数的消息。
- **match [not] header to-fields count gt count** - 匹配报头中 To 字段数量大于指定数量的消息。
- **match [not] invalid-recipients count gt number** - 匹配无效收件人数量大于指定数量的消息。
- **match [not] mime filetype regex {regex_name | class class_name}** - 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。
- **match [not] mime filename length gt bytes** - 匹配文件名长度大于指定字节数的消息。
- **match [not] mime encoding type [type2...]** - 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。
- **match [not] sender-address regex {regex_name | class class_name}** - 根据指定的正则表达式或正则表达式类匹配发件人邮件地址。
- **match [not] sender-address length gt bytes** - 匹配发件人地址长度大于指定字节数的消息。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop-connection [log]** - 丢弃数据包并关闭连接。
- **mask [log]** - 掩蔽数据包的匹配部分。此操作仅适用于 **ehlo-reply-parameter** 和 **cmd verb**。

- **reset [log]** - 丢弃数据包、关闭连接并向服务器和/或客户端发送 TCP 重置。
- **log** - 发送系统日志消息。您可以单独使用此选项，也可以与其他某项操作一起使用。
- **rate-limit message_rate** - 限制数据包中每秒的消息速率。此选项仅适用于 **cmd verb**，其中可以将此选项用作唯一操作，也可以将其与 **mask** 操作一起使用。

可以在策略映射中指定多个 **match** 命令。有关 **match** 命令顺序的信息，请参阅[如何处理多个流量类](#)，第 242 页。

步骤 4 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **mail-relay domain-name action {drop-connection [log] | log}** - 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。
- **mask-banner** - 掩蔽来自 ESMTP 服务器的横幅。
- **special-character action {drop-connection [log] | log}** - 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。
- **allow-tls [action log]** - 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。如果指定 **no allow-tls**，系统会从会话连接中去除 STARTTLS 指示符并强制执行纯文本连接。

示例

以下示例显示如何定义 ESMTP 检测策略映射。

```
hostname(config)# regex user1 "user1@cisco.com"
hostname(config)# regex user2 "user2@cisco.com"
hostname(config)# regex user3 "user3@cisco.com"
hostname(config)# class-map type regex senders_black_list
hostname(config-cmap)# description "Regular expressions to filter out undesired senders"
hostname(config-cmap)# match regex user1
hostname(config-cmap)# match regex user2
hostname(config-cmap)# match regex user3

hostname(config)# policy-map type inspect esmtp advanced esmtp_map
hostname(config-pmap)# match sender-address regex class senders_black_list
hostname(config-pmap-c)# drop-connection log

hostname(config)# policy-map outside_policy
```

```
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect esmtp advanced_esmtp_map

hostname(config)# service-policy outside_policy interface outside
```

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 249 页。

SNMP 检测

SNMP 应用检测同时适用于通过设备和通过设备的流量。如果您配置的 SNMP v3 将用户限制在特定 SNMP 主机上，则必须进行此检测。如果未检测，定义的 v3 用户可以从任何允许的主机轮询设备。默认端口已启用 SNMP 检测，因此只有在使用非默认端口时才需要进行配置。默认端口为 UDP/161、162（适用于所有设备类型），对于同时运行 FXOS 的设备，默认端口为 UDP/4161，因为 FXOS 监听 UDP/161。

默认情况下，SNMP 检测会将轮询限制为配置的版本。



注释 如果在同时运行 FXOS 的设备上配置 SNMP，则 SNMP 检测是强制性的，如果禁用，则会重新启用。在包含端口 UDP/4161 的流量类别映射上启用 SNMP 检测。

您还可以选择将 SNMP 流量进一步限制为特定版本的 SNMP。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。系统可能会拒绝 SNMP 1、2、2c 或 3 版本。如下所述，可以创建 SNMP 映射来控制允许的版本。如果不需要控制版本，只需启用 SNMP 检查，无需地图。

过程

创建 SNMP 映射。

使用 **snmp-map map_name** 命令创建映射，进入 SNMP 映射配置模式，然后使用 **deny version version** 命令标识不允许的版本。版本可能是 1、2、2c 或 3。

示例：

以下示例拒绝 SNMP 1 和 2 版本：

```
hostname(config)# snmp-map sample_map
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# deny version 2
```

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 249 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。

在以下情况下禁用 SQL*Net 检测：

- SQL 数据传输端口与 SQL 控制 TCP 1521 端口相同。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。
- 对高速 SQL 流量的检查会导致 CPU 使用率出现不可接受的峰值。

禁用 SQL*Net 检测后，使用 **clear conn port 1521** 命令，以便可以在不进行检测的情况下重建连接。

有关启用 SQL*Net 检测的信息，请参阅[配置应用层协议检测](#)，第 249 页。

Sun RPC 检测

本节介绍 Sun RPC 应用检测。

Sun RPC 检测概述

SunRPC 协议检测默认启用。只需管理 SunRPC 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流程执行此操作，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，而端口映射程序流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，指定端口映射程序流程识别的端口。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 配置 Sun RPC 服务属性。

```
sunrpc-server interface_name ip_address mask service service_type protocol {tcp | udp} port[-port]
timeout hh:mm:ss
```

其中：

- *interface_name* - 流量流向服务器数据流所通过的接口。
- *ip_address mask* - Sun RPC 服务器的地址。
- **service service_type** - 服务器上的服务类型，即特定服务类型与用于服务的端口号之间的映射。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。
- **protocol {tcp | udp}** - 服务使用 TCP 还是 UDP。
- *port[-port]* - 服务使用的端口或端口范围。要指定端口范围，请使用连字符分隔范围中起始端口号和结束端口号（例如，111-113）。
- **timeout hh:mm:ss** - Sun RPC 检测为连接打开的针孔的空闲超时。

示例：

例如，要为使用 IP 地址 192.168.100.2 的 Sun RPC 服务器创建 30 分钟的超时，请输入以下命令。在此示例中，Sun RPC 服务器位于使用 TCP 端口 111 的内部接口上。

```
hostname(config)# sunrpc-server inside 192.168.100.2 255.255.255.255
service 100003 protocol tcp 111 timeout 00:30:00
```

步骤 2 （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。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 249 页。

XDMCP 检测

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 249 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 包头格式符合标准，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记录

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。 未修改任何命令。
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。 引入了以下命令： inspect vxlan 。
TLS 会话默认行为中的 ESMTP 检测变化。	9.4(1)	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。 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)。
改进了 IP 选项检测。	9.5(1)	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。 添加了以下命令： basic-security 、 commercial-security 、 default 、 exp-flow-control 、 exp-measure 、 extended-security 、 imi-traffic-description 、 quick-start 、 record-route 、 timestamp 和 {0-255} （指示 IP 选项类型编号）。
DCERPC 检测改进和 UUID 过滤	9.5(2)	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。 引入了以下命令： match [not] uuid 。修改了以下命令： class-map type inspect 。

功能名称	版本	功能信息
通过 TCP 的 DNS 检测。	9.6(2)	现在，您可以检查通过 TCP 的 DNS 流量 (TCP/53)。 添加了以下命令： tcp-inspection 。
思科 Umbrella 支持。	9.10(1)	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。 添加或修改了以下命令： umbrella (global and policy-map parameters configuration modes)、 token 、 public-key 、 timeout edns 、 dnsencrypt 、 show service-policy inspect dns detail 。
思科 Umbrella 增强功能。	9.12(1)	您现在可以标识需要绕过思科 Umbrella 的本地域名。发向这些域的 DNS 请求将直接流向 DNS 服务器，而不经 Umbrella 处理。此外，您还可以标识用于解析 DNS 请求的 Umbrella 服务器。最后，您可以定义 Umbrella 检测策略以实现故障时自动开放，以确保 Umbrella 服务器不可用时，DNS 请求不会被阻止。 添加或更改了以下命令： local-domain-bypass 、 resolver 、 umbrella fail-open 。
XDMCP 检测在新安装中默认为禁用。	9.15(1)	以前，所有流量默认情况下都启用 XDMCP 检测。现在，在新安装（包括新系统和重新映像的系统）上，XDMCP 则默认处于关闭状态。如果需要这一检测功能，请启用它。请注意，升级时，您的 XDMCP 检测当前设置会保留，即使您只是通过默认检测设置启用了该设置。



第 14 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 241 页。

- [CTIQBE 检测](#)，第 301 页
- [H.323 检测](#)，第 302 页
- [MGCP 检测](#)，第 307 页
- [RTSP 检测](#)，第 310 页
- [SIP 检测](#)，第 313 页
- [瘦客户端 \(SCCP\) 检测](#)，第 318 页
- [STUN 检测](#)，第 321 页
- [语音和视频协议检测的历史记录](#)，第 322 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 249 页。

CTIQBE 检测的局限性

不支持 CTIQBE 呼叫状态故障转移。

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、T.38 传真和音频/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，且每个连接均按照使用 **timeout** 命令配置的 H.323 超时值设置超时值。



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。要在 H.323 终端之间启用呼叫建立，请在创建 H.323 检测策略映射时在参数配置模式期间输入 **ras-rcf-pinholes enable** 命令。

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。

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 （可选）执行以下步骤创建 H.323 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略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。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串“example.com”，则包含“example.com”的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect h323 [match-all | match-any] class_map_name**

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。**match-any** 关键字指定如果流量匹配至少一个条件，则匹配类映射。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b) （可选）向类映射添加说明：**description string**

其中，*string* 是对类映射的说明（最多可包含 200 个字符）。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] called-party regex {regex_name | class class_name}** - 将被叫方与指定的正则表达式或正则表达式类进行匹配。

- **match [not] calling-party regex** {*regex_name* | **class** *class_name*} - 将主叫方与指定的正则表达式或正则表达式类进行匹配。
- **match [not] media-type** {**audio** | **data** | **video**} - 匹配媒体类型。

步骤 2 创建 H.323 检测策略映射：**policy-map type inspect h323** *policy_map_name*

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 （可选）添加策略映射说明：**description** *string*

步骤 4 要对匹配的流量应用操作，请执行以下步骤。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅[如何处理多个流量类](#)，第 242 页。

a) 使用以下其中一种方法指定要对其执行操作的流量：

- 如果您已创建 H.323 类映射，请输入以下命令对其进行指定：**class** *class_map_name*
- 对 H.323 类映射使用上述 **match** 命令之一，以直接在策略映射中指定流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop [log]** - 丢弃数据包。对于媒体类型匹配，可以包括 **log** 关键字以发送系统日志消息。
- **drop-connection** - 丢弃数据包并关闭连接。此选项适用于被叫方匹配或主叫方匹配。
- **reset** - 丢弃数据包、关闭连接并向服务器和/或客户端发送 TCP 重置。此选项适用于被叫方匹配或主叫方匹配。

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **ras-rcf-pinholes enable** - 启用 H.323 终端之间的呼叫建立。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。
- **timeout users time** - 设置 H.323 呼叫持续时间限制（格式为 hh:mm:ss）。如果不想设置超时，请指定 00:00:00。超时范围是 0:0:0 到 1193:0:0。
- **call-party-number** - 在呼叫建立过程中强制发送主叫方号码。
- **h245-tunnel-block action** {**drop-connection** | **log**} - 强制阻止 H.245 隧道。指定是要断开连接还是仅记录连接。

- **rtp-conformance [enforce-payloadtype]** - 检查流经针孔的 RTP 数据包的协议符合性。可选的 **enforce-payloadtype** 关键字基于信令交换将负载类型限制为音频或视频。
- **state-checking {h225 | ras}** - 启用状态检查验证。可以分别为 H.225 和 RAS 输入此命令来启用状态检查。
- **early-message message_type** - 是否允许指定类型的 H.225 消息在 H.225 SETUP 消息之前到达可以按照 H.460.18 允许 **facility** 消息提前到达。

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），请使用此命令允许消息提前到达。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）。

步骤 6 可以在仍处于参数配置模式下时配置 HSI 组。

- a) 定义 HSI 组并进入 HSI 组配置模式：**hsi-group id**

其中 *id* 为 HSI 组 ID。范围为 0 至 2147483647。

- b) 使用以下 IP 地址向 HSI 组中添加 HSI：**hsi ip_address**

每个 HSI 组最多可以添加 5 台主机。

- c) 向 HSI 组中添加终端：**endpoint ip_address if_name**

其中 *ip_address* 为要添加的终端，*if_name* 为终端连接到 ASA 使用的接口。每个 HSI 组最多可以添加 10 个终端。

示例

以下示例显示如何配置电话号码过滤：

```
hostname(config)# regex caller 1 "5551234567"
hostname(config)# regex caller 2 "5552345678"
hostname(config)# regex caller 3 "5553456789"

hostname(config)# class-map type inspect h323 match-all h323_traffic
hostname(config-pmap-c)# match called-party regex caller1
hostname(config-pmap-c)# match calling-party regex caller2

hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# class h323_traffic
hostname(config-pmap-c)# drop
```

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 249 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。

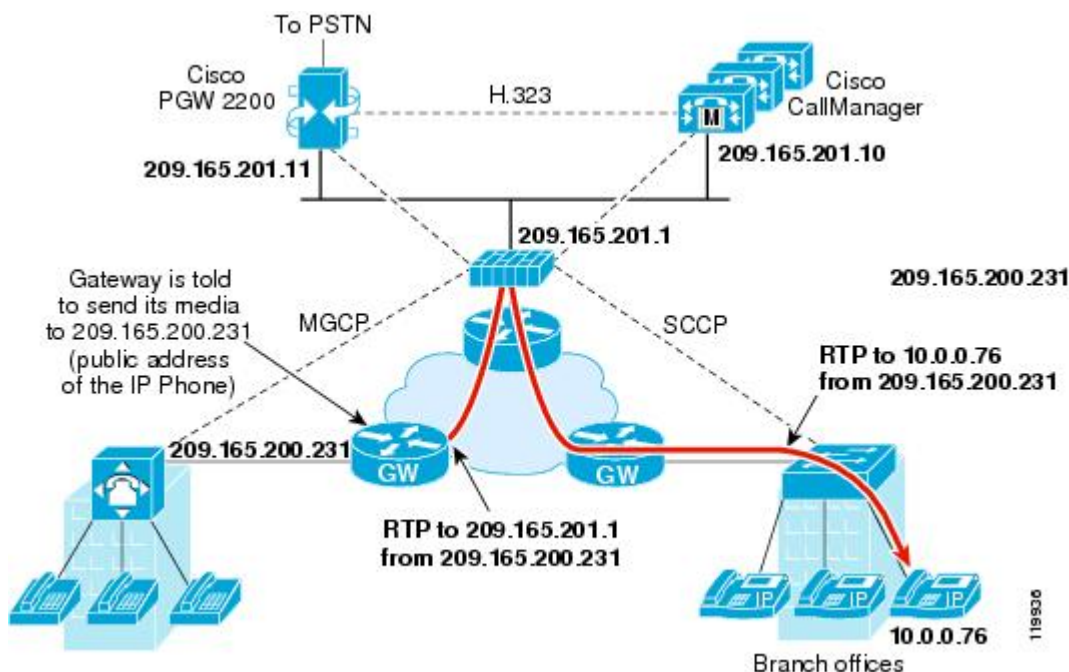
MGCP 检测概述

MGCP 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 41: 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 创建 MGCP 检测策略映射：**policy-map type inspect mgcp policy_map_name**

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description string**

步骤 3 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

步骤 4 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项。

- **call-agent ip_address group_id** - 配置可以管理一个或多个网关的呼叫代理组。呼叫代理组信息用于为组内的呼叫代理打开连接（而不是只为网关向其发送命令的那个呼叫代理打开连接），以使任何呼叫代理都可以发送响应。具有相同 **group_id** 的呼叫代理属于同一个组。一个呼叫代理可以同时属于多个组。**group_id** 是一个编号，范围介于 0 到 4294967295 之间。**ip_address** 选项指定呼叫代理的 IP 地址。

注释

MGCP 呼叫代理发送 AUEP 消息，以确定 MGCP 终端是否存在。这样将通过 ASA 建立一个数据流，并允许 MGCP 终端注册到呼叫代理。

- **gateway ip_address group_id** - 标识哪个呼叫代理组在管理特定网关。使用 **ip_address** 选项指定网关的 IP 地址。**group_id** 选项是一个介于 0 到 4294967295 之间的编号，必须与管理网关的呼叫代理的 **group_id** 相对应。一个网关可能只属于一个组。
- **command-queue command_limit** - 设置 MGCP 命令队列允许的最大命令数，范围是 1 到 2147483647。默认值为 200。

示例

以下示例显示如何定义 MGCP 映射：

```
hostname(config)# policy-map type inspect mgcp sample_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-agent 10.10.11.5 101
hostname(config-pmap-p)# call-agent 10.10.11.6 101
hostname(config-pmap-p)# call-agent 10.10.11.7 102
hostname(config-pmap-p)# call-agent 10.10.11.8 102
hostname(config-pmap-p)# gateway 10.10.10.115 101
hostname(config-pmap-p)# gateway 10.10.10.116 102
hostname(config-pmap-p)# gateway 10.10.10.117 102
hostname(config-pmap-p)# command-queue 150
```

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 249 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-rdt、x-real-rdt/udp 和 x-pn-tng/udp。

ASA 使用状态代码 200 解析建立响应消息。如果响应消息要入站，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。

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 （可选）执行以下步骤创建 RTSP 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略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。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串“example.com”，则包含“example.com”的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect rtsp [match-all | match-any] class_map_name**

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。**match-any** 关键字指定如果流量匹配至少一个条件，则匹配类映射。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b) （可选）向类映射添加说明：**description string**

其中，*string* 是对类映射的说明（最多可包含 200 个字符）。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] request-method method** - 匹配 RTSP 请求方法。这些方法包括：announce、describe、get_parameter、options、pause、play、record、redirect、setup、set_parameter、teardown。

- **match [not] url-filter regex** {*regex_name* | **class** *class_name*} - 将 URL 与指定的正则表达式或正则表达式类进行匹配。

步骤 2 要创建 RTSP 检测策略映射：**policy-map type inspect rtsp** *policy_map_name*

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 （可选）添加策略映射说明：**description** *string*

步骤 4 要对匹配的流量应用操作，请执行以下步骤。

a) 使用以下其中一种方法指定要对其执行操作的流量：

- 如果您已创建 RTSP 类映射，请输入以下命令对其进行指定：**class** *class_map_name*
- 要直接在策略映射中指定流量，请对 RTSP 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop-connection** [**log**] - 丢弃数据包，关闭连接，并选择性地发送系统日志消息。此选项适用于 URL 匹配。
- **log** - 发送系统日志消息。
- **rate-limit** *message_rate* - 限制每秒发生消息的速率。此选项适用于请求方法匹配。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅[如何处理多个流量类](#)，第 242 页。

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **reserve-port-protect** - 在媒体协商期间限制保留端口的使用。
- **url-length-limit** *bytes* - 设置消息中使用的 URL 的长度限制（0 到 6000 字节）。

示例

以下示例显示如何定义 RTSP 检测策略映射。

```
hostname(config)# regex badurl1 www.url1.com/rtsp.avi
hostname(config)# regex badurl2 www.url2.com/rtsp.rm
hostname(config)# regex badurl3 www.url3.com/rtsp.asp
```

```

hostname(config)# class-map type regex match-any badurl-list
hostname(config-cmap)# match regex badurl1
hostname(config-cmap)# match regex badurl2
hostname(config-cmap)# match regex badurl3

hostname(config)# policy-map type inspect rtsp rtsp-filter-map
hostname(config-pmap)# match url-filter regex class badurl-list
hostname(config-pmap-p)# drop-connection

hostname(config)# class-map rtsp-traffic-class
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map rtsp-traffic-policy
hostname(config-pmap)# class rtsp-traffic-class
hostname(config-pmap-c)# inspect rtsp rtsp-filter-map

hostname(config)# service-policy rtsp-traffic-policy global

```

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 249 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 应用检测会在消息信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。

如果发现 SIP 电话无法连接到呼叫管理器，可以尝试使用以下命令在 CLI 中增加未处理 TCP 网段的最大数量：**sysopt connection tcp-max-unprocessed-seg 6-24**。默认值为 6，请尝试更高的值。

SIP 检查不支持 T.38 MIME 互联网传真协议 (IFP)。SIP 检测会放弃使用 T.38 MIME 音频子类型的 SIP 邀请。如果需要允许这种类型，请禁用 SIP 检测并编写允许 RTP 流的访问控制规则。

SIP 检测的 NAT 限制

- 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。
- 如果为目标流量类（即非 `inspection_default` 流量类）配置 SIP 检测，请确保使用双向 ACL，并仅指定 5060 目的地端口。否则，您可能会遇到 NAT 问题，即使 IP 数据包已正确转换，但 SIP 报头中的 IP 地址仍无法转换。
- 如果在 SIP 邀请的 VIA 标头中硬编码映射地址，则不要启用 SIP 检测。如果使用静态 NAT 转换客户端源地址，而默认路由的接口与客户端使用的连接路由的接口不同，就会出现这个问题。

SIP 检测的 PAT 限制

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，具体如下：

- SIP 即时消息 (IM) 扩展：已启用。
- SIP 端口的非 SIP 流量：丢弃 (Dropped)。
- 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。

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 （可选）执行以下步骤创建 SIP 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略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。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串“example.com”，则包含“example.com”的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect sip [match-all | match-any] class_map_name**

其中，*class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。**match-any** 关键字指定只要流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b) （可选）向类映射添加说明：**description string**

其中，*string* 是对类映射的说明（最多可包含 200 个字符）。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] called-party regex {regex_name | class class_name}** - 将 To 报头中指定的被叫方与指定的正则表达式或正则表达式类进行匹配。
- **match [not] calling-party regex {regex_name | class class_name}** - 将 From 报头中指定的主叫方与指定的正则表达式或正则表达式类进行匹配。
- **match [not] content length gt bytes** - 匹配在 SIP 报头中的内容长度大于指定字节数（0 到 65536）的消息。
- **match [not] content type {sdp | regex {regex_name | class class_name}}** - 将内容类型匹配为 SDP 或者与指定的正则表达式或正则表达式类进行匹配。
- **match [not] im-subscriber regex {regex_name | class class_name}** - 将 SIP IM 用户与指定的正则表达式或正则表达式类进行匹配。
- **match [not] message-path regex {regex_name | class class_name}** - 将 SIP Via 报头与指定的正则表达式或正则表达式类进行匹配。
- **match [not] request-method method** - 匹配 SIP 请求方法：ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update。
- **match [not] third-party-registration regex {regex_name | class class_name}** - 将第三方注册的请求方与指定的正则表达式或正则表达式类进行匹配。
- **match [not] uri {sip | tel} length gt bytes** - 匹配长度大于指定长度（0 到 65536 字节）的选定类型（SIP 或 TEL）的 SIP 报头 URI。

d) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 SIP 检测策略映射：**policy-map type inspect sip policy_map_name**

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 （可选）添加策略映射说明：**description string**

步骤 4 要对匹配的流量应用操作，请执行以下步骤。

a) 使用以下其中一种方法指定要对其执行操作的流量：

- 如果您已创建 SIP 类映射，请输入以下命令对其进行指定：**class class_map_name**

- 要直接在策略映射中指定流量，请对 SIP 类映射使用上述 **match** 命令之一。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop** - 丢弃匹配的所有数据包。
- **drop-connection** - 丢弃数据包并关闭连接。
- **reset** - 丢弃数据包、关闭连接并向服务器和/或客户端发送 TCP 重置。
- **log** - 发送系统日志消息。您可以单独使用此选项，也可以与其他某项操作一起使用。
- **rate-limit message_rate** - 限制发出消息的速率。速率限制仅适用于匹配“invite”和“register”的请求方法。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息，请参阅[如何处理多个流量类，第 242 页](#)。

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap) # parameters
hostname(config-pmap-p) #
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **im** - 启用即时消息。
- **ip-address-privacy** - 启用 IP 地址隐私（即，隐藏服务器和终端的 IP 地址）。
- **max-forwards-validation action {drop | drop-connection | reset | log} [log]** - 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。
- **rtp-conformance [enforce-payloadtype]** - 检查流经针孔的 RTP 数据包的协议符合性。可选的 **enforce-payloadtype** 关键字基于信令交换将负载类型限制为音频或视频。
- **software-version action {mask [log] | log}** - 使用 Server 和 User-Agent（终端）报头字段标识软件版本。可以在 SIP 消息中掩蔽软件版本以及（可选）进行有关记录，或者仅进行有关记录。
- **state-checking action {drop | drop-connection | reset | log} [log]** - 启用状态转换检查。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。
- **strict-header-validation action {drop | drop-connection | reset | log} [log]** - 根据 RFC 3261 对 SIP 消息中的报头字段启用严格验证。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。
- **traffic-non-sip** - 允许已知 SIP 信令端口上出现非 SIP 流量。

- **trust-verification-server ip ip_address** - 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）。最多可以输入命令四次来标识四台服务器。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。
- **trust-verification-server port number** - 标识信任验证服务端口。默认端口是 2445，因此，请仅在服务器使用其他端口的情况下使用此命令。允许的端口范围是 1026 到 32768。
- **uri-non-sip action {mask [log] | log}** - 标识在 Alert-Info 和 Call-Info 报头字段中出现的非 SIP URI。可以在 SIP 消息中掩蔽这部分信息以及（可选）进行有关记录，或者仅进行有关记录。

示例

以下示例显示如何禁用采用 SIP 的即时消息：

```
hostname(config)# policy-map type inspect sip mymap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# no im

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect sip mymap

hostname(config)# service-policy global_policy global
```

以下示例显示如何标识四个信任验证服务服务器。

```
hostname(config)# policy-map type inspect sip sample_sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.1
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.2
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.3
hostname(config-pmap-p)# trust-verification-server ip 10.1.1.4
hostname(config-pmap-p)# trust-verification-server port 2445
```

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 249 页。

瘦客户端 (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 呼叫的状态故障转移，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。

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 创建 SCCP 检测策略映射：**policy-map type inspect skinny policy_map_name**

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description string**

步骤 3 （可选）根据 SCCP 消息的站消息 ID 字段丢弃流量。

- 根据十六进制的站消息 ID 值（0x0 到 0xffff）标识流量。使用 **match [not] message-id** 命令可以指定单个 ID 或 ID 范围。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

match message-id {value | range start_value end_value}

示例：

```
hostname(config-pmap)# match message-id 0x181
hostname(config-pmap)# match message-id range 0x200 0xffff
```

- 指定要对匹配的数据包执行的操作。可以丢弃数据包和或者记录数据包：**drop [log]**
- 重复以上步骤，直至标识出所有要丢弃的消息 ID。

步骤 4 配置影响检测引擎的参数。

- 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **enforce-registration** - 要求必须进行注册才能发出呼叫。
- **message-ID max hex_value** - 设置允许的 SCCP 站消息 ID 的最大值。消息 ID 采用十六进制，默认最大值是 0x181。
- **rtp-conformance [enforce-payloadtype]** - 检查流经针孔的 RTP 数据包的协议符合性。可选的 **enforce-payloadtype** 关键字基于信令交换将负载类型限制为音频或视频。
- **sccp-prefix-len {max | min} length** - 设置允许的最大或最小 SCCP 前缀长度值。请输入此命令两次，以设置最小值和最大值。默认最小值是 4，没有默认最大值。
- **timeout {media | signaling} time** - 为媒体和信令连接设置超时（格式为 hh:mm:ss）。如果不想设置超时，请指定数字 0。默认的媒体超时是 5 分钟，默认的信令超时是 1 小时。

示例

以下示例显示如何定义 SCCP 检测策略映射。

```
hostname(config)# policy-map type inspect skinny skinny-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enforce-registration
hostname(config-pmap-p)# match message-id range 200 300
hostname(config-pmap-p)# drop log
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect skinny skinny-map
hostname(config)# service-policy global_policy global
```

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 249 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。

故障转移和集群模式支持 STUN 检查，因为针孔被复制。但是，节点之间不进行事务 ID 的复制。如果节点在收到 STUN 请求后发生故障，并且另一个节点收到 STUN 响应，则该 STUN 响应将被丢弃。



注释 STUN 检查使用事务 ID 来匹配请求和响应。如果使用调试来排除连接丢包，请注意，系统会更改调试输出的 ID 格式（字节序），因此它们与 pcap 中的 ID 无法直接比较。

有关启用 STUN 检测的信息，请参阅[配置应用层协议检测](#)，第 249 页。

语音和视频协议检测的历史记录

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。 未修改任何命令。
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。 添加了 trust-verification-server 参数命令。
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。 未修改任何命令。
ASA 集群中的 SIP 检查支持	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。 引入了以下命令： show cluster service-policy 。
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。 删除了以下命令： phone-proxy 和 uc-ime 。从 inspect sip 命令中删除了 phone-proxy 和 uc-ime 关键字。

功能名称	版本	功能信息
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。 引入了以下命令： early-message
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。 添加或修改了以下命令： inspect stun 、 show asp drop 、 show conn detail 、 show service-policy inspect stun 。
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。 修改了以下命令： client cipher-suite 。
已弃用用于 SCCP (Skinny) 检测的 TLS 代理。	9.13(1)	已弃用 tls-proxy 关键字以及对 SCCP/Skinny 加密检测的支持。在未来版本中，将从 inspect skinny 命令中删除该关键字。
SCCP (Skinny) 检查取消了 TLS 代理支持。	9.14(1)	已删除 tls-proxy 关键字，以及对 SCCP/Skinny 加密检测的支持。
默认 SIP 检测策略映射会丢弃非 SIP 流量。	9.16 (1)	对于 SIP 检查的流量，现在默认为丢弃非 SIP 流量。以前的默认设置是允许在检查 SIP 的端口上允许非 SIP 流量。 我们更改了默认 SIP 策略映射以包含 no traffic-non-sip 命令。



第 15 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 241 页。

- [移动网络检测概述](#)，第 325 页
- [移动网络协议检测的许可](#)，第 331 页
- [GTP 检测默认设置](#)，第 332 页
- [配置移动网络检测](#)，第 333 页
- [监控移动网络检测](#)，第 363 页
- [移动网络检测的历史记录](#)，第 367 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>。

跟踪移动站位置更改

可以使用 GTP 检测跟踪移动站位置更改。跟踪位置更改可能会帮助您识别欺诈漫游费用，例如，如果您看到移动站在不太可能的时间断内从一个位置移至另一个位置，例如在 30 分钟内从美国的一个小区移至欧洲的一个小区。

当您启用位置日志记录时，系统会生成每个国际移动用户身份 (IMSI) 新建或更改后位置的系统日志消息。

- 324010 表示创建新的 PDP 上下文，包括移动国家代码 (MCC)、移动网络代码 (MNC)、信息元素，以及可选的用户当前注册的小区 ID。单元 ID 从单元全局标识 (CGI) 或 E-UTRAN 单元全局标识符 (ECGI) 中提取。
- 324011 指示 IMSI 已从 PDP 情景创建过程中存储的位置移开。此消息显示上一个和当前的 MCC/MNC、信息元素以及可选的单元 ID。

默认情况下，系统日志消息不包含时间戳信息。如果您计划分析这些消息来识别不太可能漫游时，还必须启用时间戳。时间戳日志记录不作为 GTP 检测映射的一部分。使用 **logging timestamp** 命令。

有关启用位置日志记录的信息，请参阅 [配置 GTP 检测策略映射](#)，第 333 页。

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 V15.5.0。对于 GTPv1，最高支持 3GPP 29.060 V15.2.0。对于 GTPv0，最高支持版本 8。
- 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。
- 启用 GTP 检测后，使用 GTP-in-GTP 封装的连接始终会被丢弃。

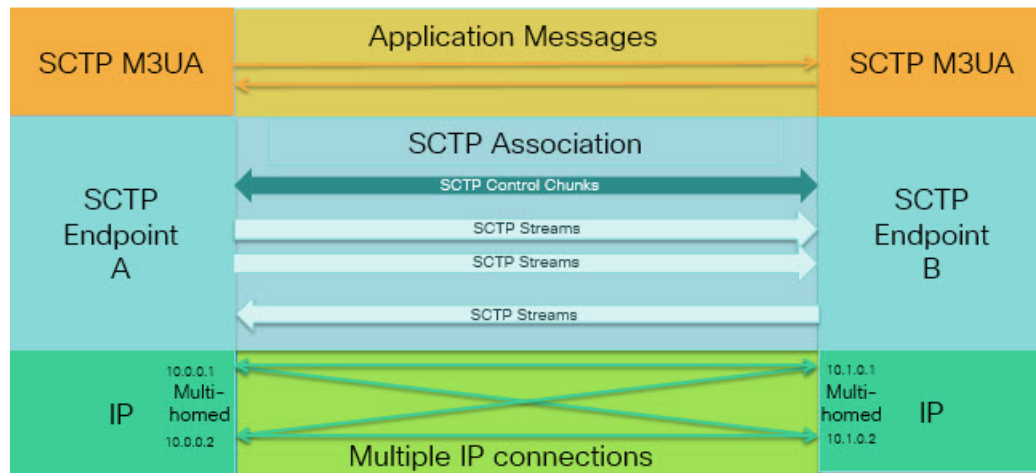
流控制传输协议 (SCTP) 检测和访问控制

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 42: 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 395 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 12 页
- [添加扩展 ACE 以执行基于端口的匹配](#)，第 35 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转移或在集群内操作，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转移或在集群内操作，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
ASA Virtual（所有型号）	Carrier 许可证（默认启用）
Cisco Secure Firewall 3100	运营商许可证
Firepower 4100	运营商许可证
Firepower 9300	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。
- 可以接受任何未知的消息 ID。可以配置 **match message v1/v2 id range** 命令来丢弃并记录不支持或想要允许的任何命令。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。

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 333 页。

步骤 2 （可选。）配置 SCTP 检测策略映射，第 337 页。

步骤 3 （可选。）配置 Diameter 检测策略映射，第 339 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 343 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 344 页

步骤 5 （可选。）配置 M3UA 检测策略映射，第 355 页

步骤 6 配置移动网络检测服务策略，第 358 页。

步骤 7 （可选。）配置 RADIUS 计费检测，第 360 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 创建 GTP 检测策略映射：**policy-map type inspect gtp policy_map_name**

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description string**

步骤 3 要对匹配的流量应用操作，请执行以下步骤。

- a) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] apn regex** {*regex_name* | **class** *class_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 (APN)。
- **match [not] message {v1 | v2} id** {*message_id* | **range** *message_id_1* *message_id_2*} - 匹配消息 ID，该值可介于 1 到 255 之间。可以指定单个 ID 或 ID 范围。必须指定该消息是否适用于 GTPv0/1 (**v1**) 或 GTPv2 (**v2**)。
- **match [not] message length min bytes max bytes** - 匹配 UDP 负载长度（GTP 报头加上消息其余部分）介于最小值和最大值（1 到 65536）之间的消息。
- **match [not] msisdn regex** {*regex_name* | **class** *class_name*} - 根据指定的正则表达式或正则表达式类来匹配“创建 PDP 情景”请求、“创建会话”请求和“修改载体响应”消息中的移动站国际用户目录号 (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。
- **match [not] selection-mode mode_value** - 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。
- **match [not] version** {*version_id* | **range** *version_id_1* *version_id_2*} - 匹配 GTP 版本（版本范围是 0 到 255）。可以指定单个版本或版本范围。

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop [log]** - 丢弃匹配的所有数据包。添加 **log** 关键字，以同时发送一条系统日志消息。
- **rate-limit** *Message_rate* - 限制消息的速率。此选项仅对 **message id** 可用。

可以在策略映射中指定多个 **match** 命令。有关 **match** 命令顺序的信息，请参阅[如何处理多个流量类](#)，第 242 页。

步骤 4 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **anti-replay [window_size]** - 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。如果未指定大小，您将获得默认值 512。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。

- **允许错误** - 允许无效 GTP 数据包或者那些无法解析并将被丢弃的数据包。根据在策略映射中定义的操作，仍然可以丢弃数据包。
- **request-queue *max_requests*** - 设置排队等待响应的最大 GTP 请求数。默认值为 200。达到限制后，如果有新请求到达，将会删除队列中等待时间最长的请求。错误提示、不支持的版本和 SGSN 情景确认消息不被视为请求，且不会进入请求队列中等待响应。
- **tunnel-limit *max_tunnels*** - 设置允许的最大活动 GTP 隧道数。该值相当于 PDP 情景或终端数量。默认值为 500。达到此命令指定的隧道数后，新请求将被丢弃。
- **timeout {*endpoint* | *pdp-context* | *request* | *signaling* | *t3-response* | *tunnel*} *time*** - 设置指定服务的空闲超时（采用“小时:分钟:秒”格式）。如果不想设置超时，请指定数字 0。为每个超时分别输入此命令。
 - **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。
 - **signaling**- 删除 GTP 信令之前允许处于非活动状态的最长时间。
 - **t3-response**- 删除连接前等待响应的最长时间。
 - **tunnel**- 终止 GTP 隧道之前允许处于非活动状态的最长时间。

步骤 5 仍在参数配置模式下，配置 GTP-U 检查 IP 数据包和反欺骗。

gtp-u-header-check [*anti-spoofing* [*gtpv2-dhcp-bypass* | *gtpv2-dhcp-drop*]]

不带关键字时，该命令会检查 GTP 数据包的内部负载是否是有效的 IP 数据包，如果包含非 IP 报头则将数据包丢弃。

如果包含 **anti-spoofing** 关键字，系统还会检查内部负载的 IP 报头中的移动用户 IP 地址是否与 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 GTP-U 消息丢弃。此检查支持 IPv4、IPv6、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 6 如有需要，可以在仍处于参数配置模式下时配置 IMSI 前缀过滤：

```
mcc country_code mnc network_code
```

```
drop mcc country_code mnc network_code
```

您可以根据需要多次输入命令，以指定所有目标 MCC/MNC 对，但策略映射中的所有命令都必须是 **mcc** 或 **drop mcc**。这些命令不能组合使用。

默认情况下，GTP 检测不检查移动国家/地区代码 (MCC)/移动网络代码 (MNC) 组合的有效性。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。然后，系统会根据命令采取以下行动之一：

- **mcc** 命令 - 如果数据包不匹配，则丢弃该数据包。
- **drop mcc** 命令 - 如果数据包匹配，则将其丢弃。

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。

添加您希望允许或放弃的所有 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 7 如有需要，可以在仍处于参数配置模式下时启用位置日志记录。

```
location-logging [cell-id]
```

记录用户的位置，以跟踪移动站的位置变化。跟踪位置更改有助于识别存在的欺诈性漫游费用。当您启用位置日志记录时，系统会生成每个国际移动用户身份 (IMSI) 新建位置（消息 324010）或更改后位置（消息 324011）的系统日志消息。

如果希望日志信息包括用户当前注册的单元 ID，请指定 **cell-id** 参数。单元 ID 从单元全局标识 (CGI) 或 E-UTRAN 单元全局标识符 (ECGI) 中提取。

步骤 8 如有需要，可以在仍处于参数配置模式下时配置 GSN 或 PGW 轮询：

```
permit-response to-object-group SGSN-SGW_name from-object-group GSN-PGW_pool
```

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 或 PGW 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。

要创建 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，并在 **from-object-group** 参数中指定该组。同样，为 SGSN/SBW 创建一个网络对象组并在 **to-object-group** 参数中选择该组。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/SBW 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。

示例：

以下是一个 GSN/PGW 轮询的示例。整个 C 类网络均被定义为 GSN/PGW 池，但您可以标识多个单独的 IP 地址，每个 **network-object** 命令标识一个，而不是标识整个网络。然后，此示例修改 GTP 检测映射，以允许响应从池传输到 SGSN/SgW。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.100.0 255.255.255.0
hostname(config)# object-group network sgsn32
hostname(config-network)# network-object host 192.168.50.100

hostname(config)# policy-map type inspect gtp gtp-policy
hostname(config-pmap)# parameters
hostname(config-pmap-p)# permit-response to-object-group sgsn32
from-object-group gsnpool32
```

示例

以下示例显示如何限制网络中隧道的数量：

```
hostname(config)# policy-map type inspect gtp gmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tunnel-limit 3000

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect gtp gmap

hostname(config)# service-policy global_policy global
```

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 358 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 创建 SCTP 检测策略映射：**policy-map type inspect sctp *policy_map_name***

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description string**

步骤 3 基于 SCTP 数据分块中的 PPID 丢弃、按速率限制或记录流量。

a) 基于 PPID 标识流量。

```
match [not] ppid ppid_1 [ppid_2]
```

其中 *ppid_1* 是 PPID 编号 (0-4294967295) 或名称（有关可用的名称，请参阅 CLI 帮助）。可以添加第二个（更高级别）PPID - *ppid_2*，用于指定 PPID 的范围。使用 **match not ppid** 来标识不匹配 PPID 或范围的流量。

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>。

b) 指定要对匹配的数据包执行的操作。

- **drop**- 丢弃并记录匹配的所有数据包。
- **log**- 发送系统日志消息。
- **rate-limit rate** - 限制消息的速率。速率单位为千位/秒 (Kbps)。

c) 重复该步骤，直到标识要选择性处理的所有 PPID。

示例

以下示例创建的检测策略映射将丢弃未分配的 PPID（写入此示例时未分配）、按速率限制 PPID 32-40，并记录 Diameter PPID。该服务策略会对向匹配所有 SCTP 流量的 *inspection_default* 类应用检测。

```
policy-map type inspect sctp sctp-pmap
  match ppid 58 4294967295
  drop
  match ppid 26
  drop
  match ppid 49
  drop
  match ppid 32 40
  rate-limit 1000
  match ppid diameter
  log

policy-map global_policy
  class inspection_default
    inspect sctp sctp-pmap
  !
service-policy global_policy global
```

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 358 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。

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 （可选）通过执行以下步骤创建 Diameter 检测类映射。

类映射可组合多个流量匹配。或者，您也可以直接在策略映射中标识 **match** 命令。创建类映射与直接在检测策略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。

要指定不应匹配类映射的流量，请使用 **match not** 命令。例如，如果 **match not** 命令指定了字符串“example.com”，则包含“example.com”的任何流量均与该类映射不匹配。

对于在此类映射中标识的流量，可以在检测策略映射中指定要对流量执行的操作。

如果要对每个 **match** 命令执行不同的操作，应该直接在策略映射中标识流量。

a) 创建类映射：**class-map type inspect diameter [match-all | match-any] class_map_name**

其中 *class_map_name* 是类映射的名称。**match-all** 关键字为默认值，指定流量必须匹配所有条件，才能匹配类映射。**match-any** 关键字指定只要流量至少与一个 **match** 语句匹配，即为与类映射匹配。CLI 将进入类映射配置模式，可以在该模式下输入一个或多个 **match** 命令。

b) （可选）向类映射添加说明：**description string**

其中，*string* 是对类映射的说明（最多可包含 200 个字符）。

c) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] application-id app_id [app_id_2]** - 匹配应用标识符，其中 *app_id* 为 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。有关应用名称的列表，请参阅 CLI 帮助。

- **3gpp-rx-ts29214** (16777236)
- **3gpp-s6a** (16777251)
- **3gpp-s9** (16777267)
- **common-message** (0)。这是基础 Diameter 协议。
- **match [not] command-code code [code_2]** - 匹配命令代码，其中 *code* 为 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，以下命令匹配“功能交换请求/应答”命令编码：

```
match command-code cer-cea
```

- 匹配属性-值对 (AVP)。

要仅按属性匹配 AVP，请使用以下命令：

```
match [not] avp code [code_2] [ vendor-id id_number]
```

要基于属性的值匹配 AVP，请使用以下命令：

```
match [not] avp code [ vendor-id id_number] value
```

其中：

- *code* - 属性-值对的名称或编号 (1-4294967295)。对于第一个代码，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。如果要匹配 AVP 的范围，请仅按编号指定第二个代码。如果要按值匹配 AVP，则无法指定第二个代码。有关 AVP 名称的列表，请参阅 CLI 帮助。
- **vendor-id id_number** - (可选。)也要一并匹配的供应商的 ID 编号，范围为 0-4294967295。例如，3GPP 供应商 ID 为 10415，IETF 为 0。
- *value* - AVP 的值部分。只有 AVP 的数据类型受支持，才能配置此项目。例如，可以为具有地址数据类型的 AVP 指定 IP 地址。下面是受支持的数据类型的值部分的特定语法：
 - Diameter Identity、Diameter URI、Octet String - 使用正则表达式或正则表达式类对象匹配这些数据类型。

```
{ regex regex_name | class regex_class }
```
 - 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。

```
date year month day time hh:mm:ss date year month day time hh:mm:ss
```

例如：


```
date 2015 feb 5 time 12:00:00 date 2015 mar 9 time 12:00:00
```

- **Numeric** - 指定编号的范围:

range *number_1 number_2*

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) 输入 **exit** 退出类映射配置模式。

步骤 2 创建 Diameter 检测策略映射: **policy-map type inspect diameter** *policy_map_name*

其中, *policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 3 (可选) 添加策略映射说明: **description** *string*

步骤 4 要对匹配的流量应用操作, 请执行以下步骤。

a) 使用以下其中一种方法指定要对其执行操作的流量:

- 如果您已创建 Diameter 类映射, 请输入以下命令对其进行指定: **class** *class_map_name*
- 使用为 Diameter 类映射而介绍的 **match** 命令之一, 直接在策略映射中指定流量。

b) 通过输入下列命令之一, 指定要对匹配的流量执行的操作:

- **drop**- 丢弃匹配的所有数据包。
- **drop-connection**- 丢弃数据包并关闭连接。
- **log**- 发送系统日志消息。

可以在策略映射中指定多个 **class** 或 **match** 命令。有关 **class** 和 **match** 命令顺序的信息, 请参阅[如何处理多个流量类, 第 242 页](#)。

示例:

```
hostname(config)# policy-map type inspect diameter diameter-map
hostname(config-pmap)# class diameter-class-map
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match command-code cer-cea
hostname(config-pmap-c)# log
```

步骤 5 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项。

- **unsupported {application-id | command-code | avp} action log** 针对不受支持的 Diameter 元素启用日志记录。这些选项指定该软件不直接支持的应用 ID、命令代码和 AVP。默认设置为允许这些元素而不对它们进行日志记录。您可以输入该命令三次以对所有元素启用日志记录。
- **strict-diameter {state | session}** - 启用符合 RFC 6733 要求的严格 Diameter 协议。默认情况下，检测可确保 Diameter 框架符合 RFC。您可以添加 **state** 机器验证或 **session** 相关的消息验证，或通过输入该命令两次来添加两种验证。

示例：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)# unsupported application-id action log
hostname(config-pmap-p)# unsupported command-code action log
hostname(config-pmap-p)# unsupported avp action log
hostname(config-pmap-p)# strict-diameter state
hostname(config-pmap-p)# strict-diameter session
```

示例

以下示例显示如何记录某些应用和阻止特定 IP 地址。

```
class-map type inspect diameter match-any log_app
  match application-id 3gpp-s6a
  match application-id 3gpp-s13

class-map type inspect diameter match-all block_ip
  match command-code cer-cea
  match avp host-ip-address 1.1.1.1

policy-map type inspect diameter diameter_map
  parameters
    unsupported application-id log
  class log_app
    log
  class block_ip
    drop-connection

policy-map global_policy
  class inspection_default
    inspect diameter diameter_map

service-policy global_policy global
```

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 358 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

创建自定义 Diameter AVP。

```
diameter avp name code value data-type type [vendor-id id_number] [description text]
```

其中：

- **name** - 要创建的自定义 AVP 的名称，最长为 32 个字符。在 Diameter 检测策略映射或类映射的 `match avp` 命令中可引用此名称。
- **code Value** - 自定义 AVP 代码值，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 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。
 - **address**- 适用于 IP 地址。
 - **diameter-identity**- Diameter 身份数据。
 - **diameter-uri**- Diameter 统一资源标识符 (URI)。
 - **float32**- 32 位浮点数值。
 - **float64**- 64 位浮点数值。
 - **int32**- 32 位整数。
 - **int64**- 64 位整数。
 - **octetstring**- 八位组字符串。
 - **time**- 时间值。
 - **uint32**- 32 位无符号整数。
 - **uint64**- 64 位无符号整数。
- **vendor-id id_number** - (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 Text** - （可选。）AVP 的说明，最长 80 个字符。如果包含空格，请将说明放在引号内。

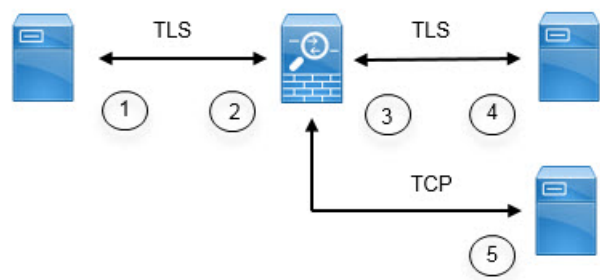
检查加密的 Diameter 会话

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 43: 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。

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。

a) 为 Diameter 客户端创建信任点。

在本例中，**enrollment terminal** 表示将证书粘贴到 CLI 中。该信任点称为 **diameter-clients**。

```
ciscoasa(config)# crypto ca trustpoint diameter-clients
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) 添加证书。

```
ciscoasa(config)# crypto ca authenticate diameter-clients
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcGP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

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) 导入 pkcs12 格式的证书。

在以下示例中，**tls-proxy-server-tp** 为信任点名称，“123”为解密密码。使用自己的信任点名称和密码。

```
ciscoasa (config)# crypto ca import tls-proxy-server-tp pkcs12 "123"

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[PKCS12 data omitted]

quit

INFO: Import PKCS12 operation completed successfully

ciscoasa (config)#
```

b) 配置信任点。

```
ciscoasa(config)# crypto ca trustpoint tls-proxy-server-tp
ciscoasa(ca-trustpoint)# revocation-check none
```

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 345 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 将用于对 Diameter 服务器证书签名的 CA 证书导入 ASA 信任点。

此步骤使 ASA 可以信任 Diameter 服务器。

a) 为 Diameter 服务器创建信任点。

在本例中，**enrollment terminal** 表示将证书粘贴到 CLI 中。此外，也可以使用注册 url 指定自动注册 (SCEP) 到 CA。该信任点称为 **diameter-server**。

```
ciscoasa(config)# crypto ca trustpoint diameter-server
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) 添加证书。

```
ciscoasa(config)# crypto ca authenticate diameter-server
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVCqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

步骤 2 导入证书，并为 ASA 代理客户端的身份证书和密钥对创建信任点。

此步骤使 Diameter 服务器可以信任 ASA。

a) 导入 pkcs12 格式的证书。

在以下示例中，**tls-proxy-client-tp** 为信任点名称，“123”为解密密码。使用自己的信任点名称和密码。

```
ciscoasa (config)# crypto ca import tls-proxy-client-tp pkcs12 "123"

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[PKCS12 data omitted]

quit

INFO: Import PKCS12 operation completed successfully

ciscoasa (config)#
```

b) 配置信任点。

```
ciscoasa(config)# crypto ca trustpoint tls-proxy-client-tp
ciscoasa(ca-trustpoint)# revocation-check none
```

步骤 3 配置 TLS 代理。

a) 为 TLS 代理命名，并进入 TLS 代理配置模式。

tls-proxy name

b) 标识 ASA 充当与 Diameter 客户端相关的代理服务器时使用的信任点。

server trust-point trustpoint_name

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 代理配置中添加 **no server authenticate-client** 命令。

c) 标识 ASA 充当与 Diameter 服务器相关的代理客户端时使用的信任点。

client trust-point name

d) （可选。）定义客户端可使用的密码。

client cipher-suite cipher-list

其中 *cipher-list* 可包括以下项目的任意组合：

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

使用空格隔开多个选项。

如果未定义 TLS 代理可使用的密码，代理服务器将使用 **ssl cipher** 命令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 **client cipher-suite** 命令。

要设置用于 ASA 上所有 SSL 客户端连接的最低 TLS 版本，请参阅 **ssl client-versionssl client-versionssl client-version** 命令。默认值为 TLS v1.0。

- e) （可选。）定义服务器可使用的密码。

server cipher-suite cipher-list

其中 *cipher-list* 可包括以下项目的任意组合：

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

使用空格隔开多个选项。

如果未定义 TLS 代理可使用的密码，代理服务器将使用 **ssl cipher** 命令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 **server cipher-suite** 命令。

要设置用于 ASA 上所有 SSL 服务器连接的最低 TLS 版本，请参阅 **ssl server-versionssl client-versionssl server-version** 命令。默认值为 TLS v1.0。

示例：

```
ciscoasa(config)# tls-proxy diameter-tls-static-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client trust-point tls-proxy-client-tp
```

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 358 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 345 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 347 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 将用于对 Diameter 服务器证书签名的 CA 证书导入 ASA 信任点。

此步骤使 ASA 可以信任 Diameter 服务器。

a) 为 Diameter 服务器创建信任点。

在本例中，**enrollment terminal** 表示将证书粘贴到 CLI 中。此外，也可以使用注册 url 指定自动注册 (SCEP) 到 CA。该信任点称为 **diameter-server**。

```
ciscoasa(config)# crypto ca trustpoint diameter-server
ciscoasa(ca-trustpoint)# revocation-check none
ciscoasa(ca-trustpoint)# enrollment terminal
```

b) 添加证书。

```
ciscoasa(config)# crypto ca authenticate diameter-server
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[certificate data omitted]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint: 24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

步骤 2 创建用于对本地动态证书 (LDC) 签名的本地 CA。

a) 为该信任点创建一个 RSA 密钥对。

在本例中，该密钥对名为 `ldc-signer-key`。

```
ciscoasa(config)# crypto key generate rsa label ldc-signer-key
INFO: The name for the keys will be: ldc-signer-key
Keypair generation process
ciscoasa(config)#
```

b) 创建 LDC 颁发机构信任点。

在本例中，该信任点名为 **ldc-server**，已使用上面创建的密钥对，已指定自签名注册（**enrollment self**，必需要求），并且 ASA 的通用名称被作为主题名称添加在内。检查 Diameter 应用对于主题名称是否具有特定要求。

proxy-ldc-issuer 命令为该信任点定义了本地 CA 角色，以便为 TLS 代理颁发动态证书。

```
ciscoasa(config)# crypto ca trustpoint ldc-server
ciscoasa(ca-trustpoint)# keypair ldc-signer-key
ciscoasa(ca-trustpoint)# subject-name CN=asa3
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# proxy-ldc-issuer
ciscoasa(ca-trustpoint)# exit
```

c) 注册该信任点。

```
ciscoasa(config)# crypto ca enroll ldc-server
```

步骤 3 配置 TLS 代理。

a) 为 TLS 代理命名，并进入 TLS 代理配置模式。

tls-proxy name

b) 标识 ASA 充当与 Diameter 客户端相关的服务器时使用的信任点。

server trust-point trustpoint_name

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 代理配置中添加 **no server authenticate-client** 命令。

c) 标识 ASA 颁发动态证书和充当与 Diameter 服务器相关的客户端时使用的信任点。

client ldc issuer name

d) 标识 LDC 密钥对。指定在 LDC 信任点定义的同密钥。

client ldc key-pair name

e) （可选。）定义客户端可使用的密码。

client cipher-suite cipher-list

其中 *cipher-list* 可包括以下项目的任意组合：

- 3des-sha1
- aes128-sha1
- aes256-sha1
- des-sha1
- null-sha1
- rc4-sha1

使用空格隔开多个选项。

如果未定义 TLS 代理可使用的密码，代理服务器将使用 **ssl cipher** 命令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 **client cipher-suite** 命令。

要设置用于 ASA 上所有 SSL 客户端连接的最低 TLS 版本，请参阅 **ssl client-version** 命令。默认值为 TLS v1.0。

- f) （可选。）定义服务器可使用的密码。

server cipher-suite *cipher-list*

其中 *cipher-list* 可包括以下项目的任意组合：

- 3des-sha1
- aes128-sha1
- aes256-sha1
- des-sha1
- null-sha1
- rc4-sha1

使用空格隔开多个选项。

如果未定义 TLS 代理可使用的密码，代理服务器将使用 **ssl cipher** 命令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 **server cipher-suite** 命令。

要设置用于 ASA 上所有 SSL 服务器连接的最低 TLS 版本，请参阅 **ssl server-version** 命令。默认值为 TLS v1.0。

示例：

```
ciscoasa(config)# tls-proxy diameter-tls-ldc-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client ldc issuer ldc-server
```

```
ciscoasa(config-tlsp)# client ldc key-pair ldc-signer-key
```

步骤 4 导出 LDC CA 证书，并将其导入到 Diameter 服务器。

a) 导出证书。

在以下示例中，LDC 信任点是 ldc-server；指定自己的 LDC 信任点名称。

```
ciscoasa(config)# crypto ca export ldc-server identity-certificate
-----BEGIN CERTIFICATE-----
MIIDbDCCAlSgAwIBAgIQfWOQvGFpj7hCCB49+kS4CjANBgkqhkiG9w0BAQUFADAT
MREwDwYDVQQDEwhIdW5ueUJlZTAeFw0xMzA2MjUwMTE5MzJaFw00ODA2MjUwMTI5
...[data omitted]...
1JZ48NoI64RqfGC/KHUsOQ==
-----END CERTIFICATE-----
```

b) 复制证书数据并将其保存到文件中。

现在即可将其导入到 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 358 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 345 页中的步骤。

过程

步骤 1 配置支持 TLS 分流的 TLS 代理。

a) 为 TLS 代理命名，并进入 TLS 代理配置模式。

```
tls-proxy name
```

b) 标识 ASA 充当与 Diameter 客户端相关的服务器时使用的信任点。

```
server trust-point trustpoint_name
```

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 代理配置中添加 **no server authenticate-client** 命令。

- c) (可选。) 定义服务器可使用的密码。

server cipher-suite cipher-list

其中 *cipher-list* 可包括以下项目的任意组合：

- **3des-sha1**
- **aes128-sha1**
- **aes256-sha1**
- **des-sha1**
- **null-sha1**
- **rc4-sha1**

使用空格隔开多个选项。

如果未定义 TLS 代理可使用的密码，代理服务器将使用 **ssl cipher** 命令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 **server cipher-suite** 命令。

要设置用于 ASA 上所有 SSL 服务器连接的最低 TLS 版本，请参阅 **ssl server-versionssl client-versionssl server-version** 命令。默认值为 TLS v1.0。

- d) 指定 ASA 与 Diameter 服务器之间的通信应为明文。在此关系中，ASA 充当 Diameter 服务器的客户端。

client clear-text

示例：

```
ciscoasa(config)# tls-proxy diameter-tls-offload-proxy
ciscoasa(config-tlsp)# server trust-point tls-proxy-server-tp
ciscoasa(config-tlsp)# client clear-text
```

步骤 2 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。每个规则应可以：

- 为 Diameter 服务器地址执行静态身份 NAT。即对象中的 IP 地址应与 NAT 规则中的转换地址相同。
- 将实际端口 3868（即默认 Diameter TCP 端口号）转换为 5868（默认 Diameter TLS 端口号）。
- 源接口是连接到 Diameter 服务器的接口，而目标接口是连接到 Diameter 客户端的接口。

以下示例将端口 3868 上从 10.29.29.29 Diameter 服务器传到外部接口的 TCP 流量转换到内部接口上的端口 5868。

```
ciscoasa(config)# object network diameter-client
ciscoasa(config-network-object)# host 10.29.29.29
ciscoasa(config-network-object)# nat (outside,inside) static 10.29.29.29
service tcp 3868 5868
```

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 358 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 创建 M3UA 检测策略映射：**policy-map type inspect m3ua policy_map_name**

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description string**

步骤 3 要对匹配的流量应用操作，请执行以下步骤。

a) 使用以下其中一个 **match** 命令指定要对其执行操作的流量。如果使用 **match not** 命令，将会对不匹配 **match not** 命令中的条件的所有流量应用操作。

- **match [not] message class class_id [id message_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

- **match [not] opc code** - 匹配数据消息中的始发点代码，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]。
- **match [not] dpc code** - 匹配数据消息中的目的点代码。点代码为 *zone-region-sp* 格式，如同所述的 **match opc** 相关内容。
- **match [not] service-indicator number** - 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

b) 通过输入下列命令之一，指定要对匹配的流量执行的操作：

- **drop [log]** - 丢弃匹配的所有数据包。或者，发送系统日志消息。
- **rate-limit Message_rate** - 限制消息的速率。此选项仅适用于 **match message class**。

可以在策略映射中指定多个 **match** 命令。有关 **match** 命令顺序的信息，请参阅[如何处理多个流量类，第 242 页](#)。

步骤 4 要配置影响检测引擎的参数，请执行以下步骤：

a) 进入参数配置模式：

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

b) 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项：

- **message-tag-validation {dupu | error | notify}** - 确保已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。
 - 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。
- **ss7 variant {ITU | ANSI | JAPAN | CHINA}** - 标识网络中使用的 SS7 的变量。此选项决定点编码的有效格式。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。
- **strict-asp-state** - 执行应用服务器进程 (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转移或在集群内操作，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。
- **timeout endpoint time** - 设置空闲超时，以便删除 M3UA 终端的统计信息；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)。
- **timeout session time** - 如果启用严格 ASP 状态验证，则设置空闲超时，以便删除 M3UA 会话，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。

示例

以下示例表示 M3UA 策略映射和服务策略。

```
hostname(config)# policy-map type inspect m3ua m3ua-map
hostname(config-pmap)# match message class 2 id 6
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match message class 9
```

```
hostname(config-pmap-c)# drop
hostname(config-pmap-c)# match dpc 1-5-1
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# ss7 variant ITU
hostname(config-pmap-p)# timeout endpoint 00:45:00

hostname(config)# policy-map global_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect m3ua m3ua-map

hostname(config)# service-policy global_policy global
```

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 358 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 如有必要，可创建 L3/L4 类映射来标识要应用检测的流量。

```
class-map name
    match parameter
```

示例：

```
hostname(config)# class-map mobile_class_map
hostname(config-cmap)# match access-list mobile
```

在默认全局策略中，`inspection_default` 类映射是一种特殊类映射，包括用于所有检测类型的默认端口的特殊类映射 (**match default-inspection-traffic**)。如果在默认策略或新的服务策略中使用该类映射，可以跳过此步骤。

有关匹配语句的信息，请参阅[为通过流量创建第 3/4 层类映射](#)，第 230 页。

步骤 2 添加或编辑策略映射，设置要对类映射流量采取的操作：**policy-map name**

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，`global_policy` 策略映射会全局性分配到所有接口。如果要编辑 `global_policy`，请输入 `global_policy` 作为策略名称。

步骤 3 标识正在用于检测的第 3/4 层类映射：**class name**

示例：

```
hostname(config-pmap)# class inspection_default
```

要编辑默认策略，或者在新策略中使用特殊的 `inspection_default` 类映射，请将 `name` 指定为 **inspection_default**。否则，将会指定在前面的操作步骤中创建的类。

步骤 4 启用检测。

在以下命令中，检测策略映射是可选的。如果您创建了其中任何映射来自定义检测，请在相应命令中指定它们的名称。对于 **Diameter**，也可以指定 TLS 代理来启用加密消息检测。

- **inspect gtp** [*map_name*] - 启用 GTP 检测。
- **inspect sctp** [*map_name*] - 启用 SCTP 检测。
- **inspect diameter** [*map_name*] [**tls-proxy** *proxy_name*] - 启用 Diameter 检测。

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。

- **inspect m3ua** [*map_name*] - 启用 M3UA 检测。

示例：

```
hostname(config-class)# inspect gtp
hostname(config-class)# inspect sctp
hostname(config-class)# inspect diameter
hostname(config-class)# inspect m3ua
```

注释

如果是编辑默认全局策略（或正在使用的任何策略）以使用不同的检测策略映射，必须使用命令的 **no inspect** 版本删除检测，然后再使用新的检测策略映射名称重新添加该检测。例如，要更改用于 GTP 的策略映射，请执行以下操作：

```
hostname(config-class)# no inspect gtp
hostname(config-class)# inspect gtp gtp-map
```

步骤 5 如果是编辑现有服务策略（例如，称为 `global_policy` 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *polycmap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

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 360 页。

步骤 2 配置 RADIUS 计费检测服务策略，第 361 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 创建 RADIUS 计费检测策略映射：**policy-map type inspect radius-accounting *policy_map_name***

其中，*policy_map_name* 是策略映射的名称。CLI 将进入策略映射配置模式。

步骤 2 （可选）添加策略映射说明：**description *string***

步骤 3 进入参数配置模式。

```
hostname(config-pmap)# parameters
hostname(config-pmap-p)#
```

步骤 4 设置一个或多个参数。可以设置以下选项；使用命令的 **no** 形式可禁用该选项。

- **send response** - 指示 ASA 向这些消息（**host** 命令中已标识）的发件人发送计费请求开始和停止消息。
- **enable gprs** - 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 *number*** - 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>。

- **host ip_address [key secret]** - 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。可以重复使用此命令来标识多个 RADIUS 和 GGSN 主机。ASA 收到来自这些主机的 RADIUS 计费消息副本。
- **timeout users time** - 设置用户空闲时间（格式为 hh:mm:ss）。如果不想设置超时，请指定 00:00:00。默认值为一小时。

示例

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
  class-map type management radius-class
    match port udp eq radius-acct
  policy-map global_policy
    class radius-class
      inspect radius-accounting radius-acct-pmap
```

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 创建 L3/L4 管理类映射，以标识要应用检测的流量并确定匹配流量。

```
class-map type management name
match {port | access-list} parameter
```

示例:

```
hostname(config)# class-map type management radius-class-map
```

```
hostname(config-cmap)# match port udp eq radius-acct
```

在本例中，匹配应用于 radius-acct UDP 端口，即 1646。可以指定其他端口或端口范围 (**match port udp range number1 number2**)，也可以使用 **match access-list acl_name** 和 ACL。

步骤 2 添加或编辑策略映射，设置要对类映射流量采取的操作：**policy-map name**

示例：

```
hostname(config)# policy-map global_policy
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。

步骤 3 标识正在用于 RADIUS 计费检测的第 3/4 层管理类映射：**class name**

示例：

```
hostname(config-pmap)# class radius-class-map
```

步骤 4 配置 RADIUS 计费检测：**inspect radius-accounting [radius-accounting_policy_map]**

其中，radius_accounting_policy_map 是在配置 RADIUS 计费检测策略映射，第 360 页中创建的 RADIUS 计费检测策略映射。

示例：

```
hostname(config-class)# no inspect radius-accounting
hostname(config-class)# inspect radius-accounting radius-class-map
```

注释

如果要编辑使用中的策略来使用不同的检测策略映射，必须使用 **no inspect radius-accounting** 命令删除 RADIUS 计费检测，然后为其提供新的检测策略映射名称并重新添加这项检测。

步骤 5 如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy policymap_name {global | interface interface_name}

示例：

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

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。

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 ssenauth146

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 ssenauth146
```

```

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。

- **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。

- **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。

- **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 :
      Forwarded      Dropped      Total Received
All Messages         21           5           26
DATA Messages         9           5           14
M3UA Endpoint Statistics for 10.0.0.110, Idle : 0:00:06 :
      Forwarded      Dropped      Total Received
All Messages         21           8           29
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记录

功能名称	版本	功能信息
GTPv2 检测和 GTPv0/1 检测的改进。	9.5(1)	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。 已将 match message id 命令更改为 match message {v1 v2} id message_id。已将 timeout gsn 命令替换为 timeout endpoint。从 clear/show service-policy inspect gtp statistics 命令中删除了 gsn 关键字；现在，只需输入终端 ID 即可查看或清除这些统计信息。现在，clear/show service-policy inspect gtp request 和 pdpmcb 命令包括 version 关键字，所以您可以显示有关特定 GTP 版本的信息。
SCTP 检测	9.5(2)	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。 关键字，所以您可以显示有关特定 GTP 版本的信息：clear conn protocol sctp、inspect sctp、match ppid、policy-map type inspect sctp、show conn protocol sctp、show local-host connection sctp、show service-policy inspect sctp。
Diameter 检测	9.5(2)	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。 添加或修改了以下命令：class-map type inspect diameter、diameter、inspect diameter、match application-id、match avp、match command-code、policy-map type inspect diameter、show conn detail、show diameter、show service-policy inspect diameter、unsupported。
Diameter 检测的改进	9.6(1)	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。 添加或修改了以下命令：client clear-text、inspect diameter、strict-diameter。
集群模式下的 SCTP 状态检测	9.6(1)	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。 我们未引入或更改任何命令。

功能名称	版本	功能信息
MTP3 用户适应 (M3UA) 检测。	9.6(2)	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。 添加或修改了以下命令：clear service-policy inspect m3ua {drops endpoint [IP_address]}、inspect m3ua、match dpc、match opc、match service-indicator、policy-map type inspect m3ua、show asp table classify domain inspect-m3ua、show conn detail、show service-policy inspect m3ua {drops endpoint [IP_address]}、ss7 variant、timeout endpoint。
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)	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。 修改了以下命令的输出：show sctp detail。
M3UA 检测有所改进。	9.7(1)	M3UA 检查现在支持状态化故障转移、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。对于状态故障转移和集群，需要使用严格 ASP 状态验证。 添加或修改了以下命令：clear service-policy inspect m3ua session [assocID id]、match port sctp、message-tag-validation、show service-policy inspect m3ua drop、show service-policy inspect m3ua endpoint、show service-policy inspect m3ua session、show service-policy inspect m3ua table、strict-asp-state、timeout session。
支持设置 TLS 代理服务器 SSL 加密套件。	9.8(1)	现在可在 ASA 作为 TLS 代理服务器时设置 SSL 密码套件。过去，您只能中使用 ssl cipher 命令为 ASA 设置全局设置。 引入了以下命令：server cipher-suite
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)	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。 添加了以下命令：anti-replay、gtp-u-header-check、match msisdn、match selection-mode。

功能名称	版本	功能信息
支持 GTPv1 版本 10.12。	9.12(1)	系统现在支持 GTPv1 版本 10.12。以前，系统支持版本 6.1。在支持新版本后，系统可以多识别 25 种 GTPv1 消息以及 66 种信息元素。 此外，系统行为也有所变化。现在，系统可以接受任何未知的消息 ID。而在过去，未知消息会被丢弃并记入日志。 未添加或更改任何命令。
移动站的位置日志记录（GTP 检测）。	9.13(1)	可以配置 GTP 检测以记录移动站的初始位置和该位置的后续更改。跟踪位置更改有助于识别可能存在的欺诈性漫游费用。 添加了以下命令：location-logging。
支持 GTPv2 和 GTPv1 版本 15。	9.13(1)	系统现在支持 GTPv2 3GPP 29.274 V15.5.0。对于 GTPv1，最高支持 3GPP 29.060 V15.2.0。在支持新版本后，系统可以多识别 2 种消息以及 53 种信息元素。 未添加或更改任何命令。
能够指定要在 GTP 检测中丢弃的 IMSI 前缀。	9.16 (1)	通过 GTP 检测，您可以配置 IMSI 前缀过滤，以识别允许的移动国家/地区代码/移动网络代码 (MCC/MNC) 组合。现在，您可以对要丢弃的 MCC/MNC 组合执行 IMSI 过滤。这样，您可以列出不需要的组合，并默认允许所有其他组合。 添加了以下命令：drop mcc。
Cisco Secure Firewall 3100 支持运营商许可证	9.18(1)	运营商许可证启用 Diameter、GTP/GPRS、SCTP 检测。 新增/修改的命令：feature carrier



第 **V** 部分

连接管理和威胁检测

- [连接设置](#)，第 373 页
- [服务质量](#)，第 407 页
- [威胁检测](#)，第 419 页



第 16 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 373 页
- [配置连接设置](#)，第 374 页
- [监控连接](#)，第 401 页
- [连接设置的历史记录](#)，第 402 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 便会探测连接的两端，了解两端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。您可以使用 **show conn detail** 命令获取有关发起方和响应方的信息，以及各自发送探测的频率。
- **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。但是，TCP 序列随机化有效地破坏了 TCP SACK（选

择性确认），因为客户端看到的序列号与服务器看到的序列号不同。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。
- **IPsec 流分流 (IPsec flow offload)** - 在初始设置 IPsec 站点间 VPN 或远程接入 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，而这应会提高设备性能。在支持此功能的平台上会默认启用此功能。

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。

开始之前

当数据包进入设备时，防火墙首先评估访问控制规则和 NAT，以确定是否需要创建连接条目。无论下一跳的 ARP 条目是否存在，都会创建一个连接条目。因此，连接的存在并不意味着连接范围内的任何数据包通过设备。空闲超时等连接设置可确保不需要的连接不会停滞不前，不会占用系统资源。

过程

-
- 步骤 1** [配置全局超时](#)，第 375 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 377 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 380 页。
 - 步骤 4** 如果有这种类型的路由环境，请[绕过非对称路由的 TCP 状态检查 \(TCP 状态绕行\)](#)，第 383 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 386 页。

步骤 6 分流大型数据流，第 388 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 395 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。

步骤 8 配置 TCP 选项，第 400 页（如果您需要强制重置或更改其他标准 TCP 行为）。

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。

对于没有特定可配置超时设置的协议（如 GRE），空闲超时为 2 分钟。

过程

使用 **timeout** 命令可设置全局超时。

所有超时值均采用 *hh:mm:ss* 格式，大多数情况下，最大持续时间为 1193:0:0。使用 **clear configure timeout** 命令将所有超时重置为其默认值。如果只想将一个计时器重置为默认值，请输入 **timeout** 命令，将该设置重置为默认值。

使用 **0** 值以禁用计时器。

可以配置以下全局超时。

- **timeout conn *hh:mm:ss*** - 连接关闭之前允许的空闲时间，该值介于 0:5:0 到 1193:0:0 之间。默认值为 1 小时 (1:0:0)。
- **timeout half-closed *hh:mm:ss*** - TCP 半闭连接关闭之前允许的空闲时间。如果同时收到 FIN 和 FIN-ACK，则连接会被认为是半关闭的。如果只看到了 FIN，则常规 **conn** 超时适用。最小值为 30 秒。默认值为 10 分钟。
- **timeout udp *hh:mm:ss*** - UDP 连接关闭之前允许的空闲时间。此持续时间必须为至少 1 分钟。默认值为 2 分钟。
- **timeout icmp *hh:mm:ss*** - ICMP 允许的空闲时间，该值介于 0:0:2 到 1193:0:0 之间。默认值为 2 秒 (0:0:2)。
- **timeout icmp-error *hh:mm:ss*** - 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 **timeout icmp** 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。

- **timeout sunrpc** *hh:mm:ss* - 释放 SunRPC 插槽之前允许的空闲时间。此持续时间必须为至少 1 分钟。默认值为 10 分钟。
- **timeout H323** *hh:mm:ss* - H.245 (TCP) 和 H.323 (UDP) 媒体连接关闭之前允许的空闲时间，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)。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。
- **timeout h225** *hh:mm:ss* - H.225 信令连接关闭之前允许的空闲时间。H.225 默认超时为 1 小时 (1:0:0)。要在所有呼叫清除之后立即关闭连接，建议将该值设置为 1 秒 (0:0:1)。
- **timeout mgcp** *hh:mm:ss* - 删除 MGCP 媒体连接之前允许的空闲时间，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)
- **timeout mgcp-pat** *hh:mm:ss* - 删除 MGCP PAT 转换之前允许的绝对间隔，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)。最短时间为 30 秒。
- **timeout sctp** *hh:mm:ss* - 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)。
- **timeout sip** *hh:mm:ss* - SIP 信令端口连接关闭之前允许的空闲时间，该值介于 0:5:0 到 1193:0:0 之间。默认值为 30 分钟 (0:30:0)。
- **timeout sip_media** *hh:mm:ss* - SIP 媒体端口连接关闭之前允许的空闲时间。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。
- **timeout sip-provisional-media** *hh:mm:ss* - SIP 临时媒体连接的超时值，该值介于 0:1:0 到 0:30:0 之间。默认值为 2 分钟。
- **timeout sip-invite** *hh:mm:ss* - 关闭 PROVISIONAL 响应和媒体转换的针孔之前允许的空闲时间，该值介于 0:1:0 到 00:30:0 之间。默认值为 3 分钟 (0:3:0)。
- **timeout sip-disconnect** *hh:mm:ss* - 在 CANCEL 或 BYE 消息未收到 200 OK 的情况下，删除 SIP 会话之前允许的空闲时间，该值介于 0:0:1 到 0:10:0 之间。默认值为 2 分钟 (0:2:0)。
- **timeout uauth** *hh:mm:ss* {**absolute** | **inactivity**} - 身份验证和授权缓存超时并且用户必须对下一连接重新进行身份验证之前经过的持续时间，该值介于 0:0:0 到 1193:0:0 之间。默认值为 5 分钟 (0:5:0)。默认计时器为 **absolute**；可以通过输入 **inactivity** 关键字设置在非活动状态持续了特定时间后发生超时。未经授权的持续时间必须比转换持续时间短。设置为 0 表示禁用缓存。如果连接使用被动 FTP 或使用虚拟 http 命令进行 Web 身份验证，请勿使用 0。
- **timeout xlate** *hh:mm:ss* - 释放转换插槽之前允许的空闲时间。此持续时间必须为至少 1 分钟。默认值为 3 小时。
- **timeout pat-xlate** *hh:mm:ss* - 释放 PAT 转换插槽之前允许的空闲时间，该值介于 0:0:30 到 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。
- **timeout tcp-proxy-reassembly** *hh:mm:ss* - 丢弃等待重组的缓冲数据包之前允许的空闲超时，该值介于 0:0:10 到 1193:0:0 之间。默认值为 1 分钟 (0:1:0)。

- **timeout floating-conn***hh:mm:ss* - 当多个具有不同指标的路由共存于一个网络时, ASA 在创建连接时使用指标最好的路由。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 (连接永不过时)。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。
- **timeout conn-holddown***hh:mm:ss* - 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。
- **timeout igp stale-route***hh:mm:ss* - 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。

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, 使该连接不加入到目标主机的 SYN 队列中。SYN Cookie 是在 SYN-ACK 中返回的初始序列号, 它由 MSS、时间戳和其他项目的数学散列构成, 用于创建密钥。如果在有效的时间窗口内 ASA 收到来自客户端的具有正确序列号的 ACK, 可以对实际客户端的真实性进行身份验证, 并且允许连接到服务器。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 创建 L3/L4 类映射以确定要保护的服务器。使用访问列表匹配。

```
class-map name
match parameter
```

示例:

```
hostname(config)# access-list servers extended permit tcp any host 10.1.1.5 eq http
hostname(config)# access-list servers extended permit tcp any host 10.1.1.6 eq http
hostname(config)# class-map protected-servers
hostname(config-cmap)# match access-list servers
```

步骤 2 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

```
policy-map name
class name
```

示例:

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class protected-servers
```

在默认配置中，`global_policy` 策略映射会全局性分配到所有接口。如果要编辑 `global_policy`，请输入 `global_policy` 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

步骤 3 设置初期连接限制。

- **set connection embryonic-conn-max** *n* - 允许的最大同时初期 TCP 连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。
- **set connection per-client-embryonic-max** *n* - 每个客户端允许的最大同步初期 TCP 连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。
- **set connection syn-cookie-mss** *n* - 在达到初期连接限制时为初期连接的 SYN-Cookie 设置服务器最大分段大小 (MSS)，范围为 48 到 65535。默认值为 1380。仅当配置 **set connection embryonic-conn-max** 或 **per-client-embryonic-max** 时，此设置才有意义。

示例:

```
hostname(config-pmap-c)# set connection embryonic-conn-max 1000
hostname(config-pmap-c)# set connection per-client-embryonic-max 50
```

步骤 4 如果编辑的是现有服务策略（例如，名为 `global_policy` 的默认全局策略），您即可跳过此步骤。否则，应在一个或多个接口上激活策略映射。

```
service-policy policymap_name {global | interface interface_name}
```

示例:

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

步骤 5 配置 TCP 拦截所拦截攻击的威胁检测统计信息。

```
threat-detection statistics tcp-intercept [ rate-interval minutes] [ burst-rate attacks_per_sec] [ average-rate attacks_per_sec]
```

其中:

- **rate-interval minutes** 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。在此间隔内，ASA 将对攻击数量抽样 30 次。
- **burst-rate attacks_per_sec** 设置生成系统日志消息的阈值，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-rate attacks_per_sec** 设置生成系统日志消息的平均速率阈值，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。

示例:

```
hostname(config)# threat-detection statistics tcp-intercept
```

步骤 6 可以使用以下命令监控结果:

- **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** 关键字显示历史记录采样数据。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。
- **clear threat-detection statistics tcp-intercept** - 清除 TCP 拦截统计信息。

示例:

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack Time)>
-----
1      10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2      10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

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。

默认配置包括以下设置：

```
no check-retransmission
no checksum-verification
exceed-mss allow
queue-limit 0 timeout 4
reserved-bits allow
syn-data allow
synack-data drop
invalid-ack drop
seq-past-window drop
tcp-options range 6 7 clear
tcp-options range 9 18 clear
tcp-options range 20 255 clear
tcp-options md5 allow
tcp-options mss allow
tcp-options selective-ack allow
tcp-options timestamp allow
tcp-options window-scale allow
ttl-evasion-protection
urgent-flag clear
window-variation allow-connection
```

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 创建 TCP 映射，以指定要查找的 TCP 规范化条件：**tcp-map tcp-map-name**

步骤 2 通过输入下列一个或多个命令配置 TCP 映射条件。系统对您未输入的所有命令使用默认设置。使用命令的 **no** 形式可禁用该设置。

- **check-retransmission** - 防止 TCP 重新传输出现不一致。此命令默认禁用。
- **checksum-verification** - 验证 TCP 校验和，丢弃验证失败的数据包。此命令默认禁用。
- **exceed-mss {allow | drop}** - 允许或丢弃数据长度超出 TCP 最大分段大小的数据包。默认为允许数据包。
- **invalid-ack {allow | drop}** - 允许或丢弃具有无效 ACK 的数据包。默认丢弃该类数据包，但 WAAS 连接除外，因为系统允许 WAAS 连接。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。

- **queue-limit** *pkt_num* [**timeout seconds**] - 设置 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 1 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 (**inspect** 命令)、和 TCP 检查重传 (TCP 映射 **check-retransmission** 命令) 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** 命令设置为 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。

timeout seconds 参数设置无序数据包可停留在缓冲区的最长时间, 介于 1 至 20 秒之间; 如果这些数据包在超时期间内未按顺序排列并通过, 则将被丢弃。默认值为 4 秒。如果 *pkt_num* 参数设置为 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, **timeout** 关键字才会生效。

- **reserved-bits** {**allow** | **clear** | **drop**} - 为 TCP 报头保留位设置操作。可以 **allow** 数据包 (不更改保留位), **clear** 保留位并允许数据包, 或者 **drop** 数据包。
- **seq-past-window** {**allow** | **drop**} - 为具有超出窗口序列号的数据包设置操作, 即已收到 TCP 数据包的序列号超出 TCP 接收窗口的右边。仅当 **queue-limit** 命令设置为 0 (禁用) 时, 才可以 **allow** 数据包。默认为丢弃数据包。
- **synack-data** {**allow** | **drop**} - 允许或丢弃含有数据的 TCP SYNACK 数据包。默认为丢弃数据包。
- **syn-data** {**allow** | **drop**} - 允许或丢弃含有数据的 SYN 数据包。默认为允许数据包。
- **tcp-options** {**md5** | **mss** | **selective-ack** | **timestamp** | **window-scale** | **range lower upper**} *action* - 设置包含 TCP 选项的数据包的操作。这些选项被命名为: **md5**、**mss**、**selective-ack** (选择性确认机制)、**timestamp** 和 **window-scale** (窗口缩放机制)。对于其他选项, 可按 **range** 关键字中的编号指定它们, 其中的范围限制为 6-7、9-18 和 20-255。要按编号定位单一选项, 请对范围下限和上限输入相同的编号。可以在映射中多次输入命令来定义完整的策略。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。可能的操作如下:
 - **allow** [**multiple**] - 允许包含单一此类型选项的数据包。这是所有已命名选项的默认设置。如果要允许数据包, 即便其中包含该选项的多个实例亦不例外, 请添加 **multiple** 关键字。 (**multiple** 关键字不适用于 **range**。)
 - **maximum limit** - 仅适用于 **mss**。将最大分段大小设置为所示的限制, 范围为 68-65535。默认 TCP MSS 在 **sysopt connection tcpmss** 命令中定义。
 - **clear** - 从报头中删除此类型的选项并允许该数据包。这是所有已编号选项的默认设置。请注意, 清除时间戳选项将禁用 PAWS 和 RTT。
 - **drop** - 丢弃包含此选项的数据包。此操作仅适用于 **md5** 和 **range**。

- **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。默认启用 TTL 逃逸防护，因此只需要输入此命令的 **no** 形式。

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。

- **urgent-flag {allow | clear}** - 为具有 URG 标志的数据包设置操作。可以 **allow** 数据包，或者 **clear** 标志并允许数据包。默认为清除标志。

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。

- **window-variation {allow | drop}** - 允许或丢弃意外更改其窗口大小的连接。默认为允许连接。

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”。检测到这种情况时，连接可能会断开。

步骤 3 使用服务策略将 TCP 映射应用到流量类。

- a) 使用 L3/L4 类映射定义流量类，并将该映射添加到策略映射中。

```
class-map name
match parameter
policy-map name
class name
```

示例:

```
hostname(config)# class-map normalization
hostname(config-cmap)# match any
hostname(config)# policy-map global_policy
hostname(config-pmap)# class normalization
```

在默认配置中，global_policy 策略映射会全局性分配到所有接口。如果要编辑 global_policy，请输入 global_policy 作为策略名称。有关类映射匹配语句的信息，请参阅[为通过流量创建第 3/4 层类映射，第 230 页](#)。

- b) 应用 TCP 映射: **set connection advanced-options tcp-map-name**

示例:

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

- c) 如果是编辑现有服务策略（例如，称为 global_policy 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *polycmap_name* {**global** | **interface** *interface_name*}

示例:

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

示例

例如，要允许所有流量的紧急标志和紧急偏移数据包发送到众所周知的 FTP 数据端口与 Telnet 端口之间的 TCP 端口范围，请输入以下命令：

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet
hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap
hostname(config-pmap-c)# service-policy pmap global
```

绕过非对称路由的 TCP 状态检查（TCP 状态绕行）

如果网络中有非对称路由环境，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，则需要在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。

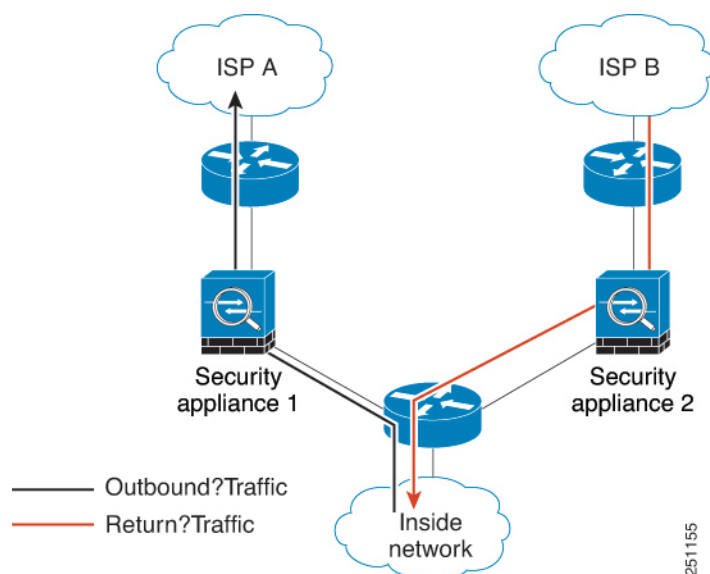
非对称路由问题

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 44: 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。
- 状态故障转移。

TCP 状态绕行 NAT 准则

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

要在非对称路由环境中绕过 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。您可以覆盖此默认值，将 **set connection timeout idle** 命令用于 TCP 状态绕行流量类。一般的 TCP 连接超时默认为 60 分钟后。

过程

步骤 1 创建 L3/L4 类映射以确定需要 TCP 状态绕行的主机。使用 **access-list match** 确定源主机和目标主机。

```
class-map name
match parameter
```

示例：

```
hostname(config)# access-list bypass extended permit tcp host 10.1.1.1 host 10.2.2.2
hostname(config)# class-map bypass-class
hostname(config-cmap)# match access-list bypass
```

步骤 2 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

```
policy-map name
class name
```

示例：

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class bypass-class
```

在默认配置中，**global_policy** 策略映射会全局性分配到所有接口。如果要编辑 **global_policy**，请输入 **global_policy** 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

步骤 3 在该类上启用 TCP 状态绕行：**set connection advanced-options tcp-state-bypass**

步骤 4 如果是编辑现有服务策略（例如，称为 **global_policy** 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

```
service-policy policymap_name {global | interface interface_name}
```

示例：

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

示例

以下是 TCP 状态绕行的示例配置：

```
hostname(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass

hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass

hostname(config-pmap-c)# service-policy tcp_bypass_policy interface outside
```

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。但是，TCP 序列随机化有效地破坏了 TCP SACK（选择性确认），因为客户端看到的序列号与服务器看到的序列号不同。

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。



注释

不建议您在使用集群时禁用 TCP 序列随机化。由于 SYN/ACK 数据包可能会被丢弃，因此少数情况下可能无法建立某些 TCP 会话。

过程

- 步骤 1** 创建 L3/L4 类映射以确定不应随机化 TCP 序列号的流量。应对 TCP 流量应用类匹配；可以识别特定的主机（使用 ACL）、执行 TCP 端口匹配或简单地匹配任何流量。

```
class-map name
match parameter
```

示例：

```
hostname(config)# access-list preserve-sq-no extended permit tcp any host 10.2.2.2
hostname(config)# class-map no-tcp-random
hostname(config-cmap)# match access-list preserve-sq-no
```

- 步骤 2** 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

```
policy-map name
class name
```

示例：

```
hostname(config)# policy-map global_policy
hostname(config-pmap)# class no-tcp-random
```

在默认配置中，`global_policy` 策略映射会全局性分配到所有接口。如果要编辑 `global_policy`，请输入 `global_policy` 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

- 步骤 3** 禁用类上的 TCP 序列号随机化：

```
set connection random-sequence-number disable
```

如果以后确定要重新打开它，请将“disable”替换为 **enable**。

- 步骤 4** 如果是编辑现有服务策略（例如，称为 `global_policy` 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

```
service-policy policymap_name {global | interface interface_name}
```

示例：

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

分流大型数据流

如果在数据中心支持的设备上部署 ASA，就可以将选定的流量卸载到超快速路径上，在该路径上，流量在网卡本身进行切换。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服务策略规则。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：

设备限制

以下设备支持此功能：

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Firepower 4100/9300

无法分流的数据流

以下数据流类型无法分流。

- 任何不使用 IPv4 寻址的流，例如 IPv6 寻址。
- 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。
- 在设备上终止的 IPsec 和 TLS/DTLS VPN 连接。
- 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。
- TCP 状态绕过流。不能在同一流量的配置数据流分流和 TCP 状态绕行。
- AAA 直通代理流。
- Vpath、VXLAN 相关数据流。
- 使用安全组标记的数据流。
- Cisco Secure Firewall 4200 除外：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控制设备）。

其他限制

- 流分流与死连接检测 (DCD) 不兼容。不要在可分流的连接上配置 DCD。
- 如果多个与数据流分流条件匹配的数据流排队等待同时分流到硬件上的同一位置，则只会分流第一个数据流。其他数据流则会照常处理。这称为冲突。在 CLI 中使用 **show flow-offload flow** 命令显示此情况的统计信息。
- 虽然分流的数据流通过 FXOS 接口，但这些数据流的统计信息不会显示在逻辑设备接口上。因此，逻辑设备接口计数器和数据包速率不会反映分流流量。

集群重定向

当现有流的流量被发送到不同节点时，该流量会通过集群控制链路重定向到所有者节点。由于不对称流量会在集群控制链路上产生大量流量，因此分流这些流量可以提高性能，例如，对于分布式站点间 VPN 模式。此功能支持以下模式：

- Cisco Secure Firewall 4200
- 路由和透明模式
- 跨区以太网通道模式
- 多情景模式

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。对于 Firepower 4100/9300：初次启用该服务时，必须重新启动。流量分流默认为 Cisco Secure Firewall 3100/4200 启用。

过程

步骤 1 启用数据流分流服务。

flow-offload enable

流量分流默认为 Cisco Secure Firewall 3100/4200 启用。

对于 Firepower 4100/9300：初次启用该服务时，必须重新启动。

如果需要重新加载，则需要对集群或故障转移对进行特殊考虑，以实现无中断更改：

- 集群 - 首先在控制节点上输入命令，但不要立即重启控制节点。相反，首先重新启动该集群的每个节点，再返回控制节点并对其重新启动。然后，即可在控制节点上配置分流服务策略。
- 故障转移 - 首先在主用设备上输入该命令，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。

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。

示例：

```
ciscoasa(config)# flow-offload enable

WARNING: This command will take effect after the running-config is
saved and the system has been rebooted.

ciscoasa(config)# write memory
ciscoasa(config)# reload
```

步骤 2 （Cisco Secure Firewall 4200）启用集群重定向。

flow-offload cluster-redirect

默认情况下，启用集群重定向。此功能需要 **flow-offload enable** 命令，这也是默认情况下启用的。

对于不对称流，集群重定向允许转发节点将流量分流到硬件上。当现有流的流量被发送到不同节点时，该流量会通过集群控制链路重定向到所有者节点。由于不对称数据流会在集群控制链路上产生大量流量，因此由转发器分流这些数据流可提高性能。

步骤 3 创建用于识别符合分流条件的流量的服务策略规则。

- a) 创建一个 L3/L4 类映射，以识别符合数据流分流条件的流量。最常用的选项是按访问列表或端口匹配。

```
class-map name
match parameter
```

示例：

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
```

- b) 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

```
policy-map name
class name
```

示例：

```
hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload
```

在默认配置中，`global_policy` 策略映射会全局性分配到所有接口。如果要编辑 `global_policy`，请输入 `global_policy` 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

- c) 对于类启用数据流分流：**set connection advanced-options flow-offload**
d) 如果是编辑现有服务策略（例如，称为 `global_policy` 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

```
service-policy policymap_name {global | interface interface_name}
```

示例：

```
hostname(config)# service-policy offload_policy interface outside
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

示例

以下示例将来自 10.1.1.0/255.255.255.224 子网的所有 TCP 流量归为符合分流条件，并将该策略附加到外部接口。

```
hostname(config)# access-list offload permit tcp 10.1.1.0 255.255.255.224 any
hostname(config)# class-map flow_offload
hostname(config-cmap)# match access-list offload
hostname(config)# policy-map offload_policy
hostname(config-pmap)# class flow_offload
hostname(config-pmap-c)# set connection advanced-options flow-offload
hostname(config)# service-policy offload_policy interface outside
```

IPsec 流分流

您可以将支持的设备型号配置为使用 IPsec 数据流分流。初始设置 IPsec 站点间 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，这应该会提高设备性能。在 Cisco Secure Firewall 1200 系列上，IPsec 连接被分流到 Marvell 加密加速器 (CPT)，以提高设备性能。

分流操作特别涉及入口上的预解密和解密处理，以及出口上的预加密和加密处理。系统软件处理内部流以应用安全策略。

默认情况下启用 IPsec 数据流分流，并应用于以下设备类型：

- Cisco Secure Firewall 1200
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

启用设备的 VTI 环回接口时，也会使用 IPsec 数据流分流。

对于集群分布式站点间 VPN 模式中的不对称流量，IPsec 流分流现在可让流量所有者在硬件中解密通过集群控制链路转发的 IPsec 流量。此功能不可配置，启用 IPsec 流分流后始终可用。

IPsec 流分流的限制

不分流以下 IPsec 流：

- IKEv1 隧道。仅 IKEv2 隧道将被分流。IKEv2 支持更强的密码。
- 配置了基于卷的密钥更新的流。
- 已配置压缩的流。
- 传输模式流。仅会分流隧道模式流。
- AH 格式。仅支持 ESP/NAT-T 格式。
- 已配置后分段的流。

- 防重放窗口大小不是 64 位且防重放的流不会被禁用。
- 已启用防火墙过滤器的流。
- 多情景模式。

配置 IPsec 数据流分流

默认情况下，在支持该功能的硬件平台上启用 IPsec 数据流分流。但是，默认情况下并不启用出口优化功能，因此如果需要该功能，需要对其进行配置。

开始之前

IPsec 流分流是全局配置的。无法为选定流量进行配置。

要禁用这些功能，请使用这些命令的 **no** 形式。

要显示当前配置状态，请使用 **show flow-offload ipsec info** 命令。

过程

步骤 1 启用 IPsec 流分流。

flow-offload-ipsec

步骤 2 启用出口优化以优化数据路径，从而提高单个隧道流的性能。

flow-offload-ipsec egress-optimization

出口优化配置与流分流是分开的。但即使已启用，也只有在同时启用 IPsec 流分流的情况下才会有效。默认情况下不启用出口优化。

DTLS 加密加速

ASA 在 FPGA 和 Nitrox V 加密加速器的帮助下支持 DTLS 加密加速。

- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

此功能可提高 DTLS 加密和 DTLS 解密流量的吞吐量。支持 IPv4 和 IPv6 流量。

ASA 还会对出口加密数据包执行优化，以改善延迟。数据路径经过优化，可增强单个隧道流的性能。

默认情况下，这两项功能均已启用，并且仅适用于 DTLS 1.2。

配置 DTLS 加密加速

默认情况下，启用 DTLS 加密加速。如果需要，您可以禁用它。

在以下情况下，ASA 不会执行 DTLS 加密加速：

- 流使用 DTLS 1.0 或数据包压缩。
- 重新生成 DTLS 密钥。
- 集群或多情景模式。

过程

步骤 1 在设备上禁用 DTLS 加密加速。

no flow-offload-dtls

示例：

```
ciscoasa(config)# no flow-offload-dtls
```

要重新启用它，请使用 **flow-offload-dtls** 命令。

步骤 2 禁用出口加密数据包优化并改善延迟。

no flow-offload-dtls egress-optimization

示例：

```
ciscoasa(config)# flow-offload-dtls egress-optimization
```

要重新启用它，请使用 **flow-offload-dtls egress-optimization** 命令。

监控 DTLS 加密加速

在威胁防御设备上使用以下 CLI 命令验证并监控出口加密数据包的 DTLS 加密加速和优化。

- 要验证 DTLS 加密加速和出口加密数据包优化的状态，请使用以下命令：

```
ciscoasa# show flow-offload-dtls info
DTLS offload : Enabled
Egress Optimization: Enabled
```

- 要查看 DTLS 加密加速统计信息，请使用以下命令：

```
ciscoasa# show flow-offload-dtls statistics
Packet stats of Pipe 0
-----
Rx Packet count : 975638666
Tx Packet count : 975638666
Error Packet count : 0
Drop Packet count : 0

CAM stats of Pipe 0
```

```
-----
Option ID Table CAM Hit Count : 1145314723
Option ID Table CAM Miss Count : 0
Tunnel Table CAM Hit Count : 0
Tunnel Table CAM Miss Count : 0
6-Tuple CAM Hit Count : 975638666
6-Tuple CAM Miss Count : 169676057
NOTE: The counters displayed are cumulative counters
      for all offload applications and indicates the total packets
      offloaded
```

- 要查看设备的 Nitrox V 加密加速器统计信息，请使用以下命令：

```
ciscoasa# show crypto accelerator statistics

Crypto Accelerator Status
-----
<snip>
[Offloaded SSL Input statistics, Pipe 0]
  Input packets: 290593023
  Input bytes: 147049729714
  Decrypted packets: 290593023
  Decrypted bytes: 147049729714
[Offloaded SSL Output statistics, Pipe 0]
  Output packets: 254271808
  Output bytes: 136352952720
  Encrypted packets: 254271808
  Encrypted bytes: 136352952720
.
.
.
```

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。
- 为受不对称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（如 OSPF hello 数据包）的发送 TTL = 1，因此递减生存时间可能会给透明模式 ASA 设备带来意想不到的后果。当 ASA 以路由模式运行时，递减生存时间设置不会影响 OSPF 进程。

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。

下文将单独介绍各个参数的 **set connection** 命令（用于连接限制和序列标准化）和 **set connection timeout** 命令。但是，可以在一行中输入这两个命令，如果您分别输入，这些命令会在配置中显示为一个命令。

过程

步骤 1 创建 L3/L4 类映射，以确定要为其自定义连接设置的流量。

```
class-map name
match parameter
```

示例：

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
```

有关匹配语句的信息，请参阅[为通过流量创建第 3/4 层类映射](#)，第 230 页。

步骤 2 添加或编辑用于设置要对类映射流量执行的操作的策略映射，并确定类映射。

```
policy-map name
class name
```

示例：

```
hostname(config)# policy-map global_policy
```



```
hostname(config-pmap)# class CONNS
```

在默认配置中，`global_policy` 策略映射会全局性分配到所有接口。如果要编辑 `global_policy`，请输入 `global_policy` 作为策略名称。对于类映射，请指定在本程序前面部分中创建的类。

步骤 3 设置连接限制和 TCP 序列号随机化。（TCP 拦截。）

默认情况下，没有连接限制。如果实施了限制，系统就必须开始跟踪它们，这可能会增加 CPU 和内存的使用量，导致系统（尤其是集群中的系统）在负载较重的情况下出现运行问题。

- **set connection conn-max *n*** - (TCP、UDP、SCTP。) 整个类允许的最大同时连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。对于 TCP 连接，这仅适用于已建立的连接。
 - 如果有两台服务器被配置为允许同时连接，则连接限制单独适用于每个配置的服务器。
 - 由于限制适用于一个类，一台攻击主机可占用所有连接而且使其余所有主机无法与该类匹配。
- **set connection per-client-max *n*** - (TCP、UDP、SCTP。) 每个客户端允许的最大同时连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。此参数限制与类匹配的每台主机所允许的最大同步连接数。对于 TCP 连接，这包括已建立、半开和半闭的连接。
- **set connection embryonic-conn-max *n*** - 允许的最大同时初期 TCP 连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。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。
- **set connection per-client-embryonic-max *n*** - 每个客户端允许的最大同时初期 TCP 连接数，该值介于 0 到 2000000 之间。默认值为 0，允许无限制连接。
- **set connection syn-cookie-mss *n*** - 在达到初期连接限制时为初期连接的 SYN-Cookie 设置服务器最大分段大小 (MSS)，范围为 48 到 65535。默认值为 1380。仅当配置 **set connection embryonic-conn-max** 或 **per-client-embryonic-max** 时，此设置才有意义。
- **set connection random-sequence-number {enable | disable}** - 启用还是禁用 TCP 序列号随机化。默认情况下启用随机化。

示例：

```
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
```

步骤 4 设置连接超时和失效连接检测 (DCD)。

下述默认值假设未使用 **timeout** 命令更改这些行为的全局默认值；全局默认值覆盖此处所述的值。输入 **0** 禁用计时器，以便连接永不超时。

- **set connection timeout embryonic *hh:mm:ss*** - TCP 初期（半开）连接关闭之前的超时时间，该值介于 0:0:5 到 1193:00:00 之间。默认值为 0:0:30。

- **set connection timeout idle** *hh:mm:ss* [**reset**] - 空闲超时期间，该期间过后建立的任何协议连接均将关闭，该值介于 0:0:1 到 1193:0:0 之间。默认值为 1:0:0。对于 TCP 流量，在连接超时情况下，**reset** 关键字会向 TCP 终端发送重置消息。

默认 **udp** 空闲超时为 2 分钟。默认 **icmp** 空闲超时为 2 秒。默认 **esp** 和 **ha** 空闲超时为 30 秒。对于所有其他协议，默认空闲超时为 2 分钟。

- **set connection timeout half-closed** *hh:mm:ss* - 半闭连接关闭前的空闲超时期间，该值介于 0:5:0（适用于 9.1(1) 和更早版本）或 0:0:30（适用于 9.1(2) 和更高版本）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。

- **set connection timeout dcd** [*retry-interval* [*max_retries*]] - 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。在透明防火墙模式下运行，必须为终端配置静态路由。不能在同时分流的连接上配置 DCD，因此要确保 DCD 和流量分流流量类别不重叠。使用 **show conn detail** 命令跟踪发起方和响应方发送的 DCD 探测数量。

retry-interval 以 *hh:mm:ss* 格式设置每个未响应的 DCD 探测在发送另一个探测之前等待的时间段，该值介于 0:0:1 到 24:0:0 之间。默认值为 0:0:15。*max-retries* 设置 DCD 在宣称连接为失效连接之前可连续失败重试的次数。最小值为 1，最大值为 255。默认值为 5。

对于在集群或高可用性配置中运行的系统，我们建议您不要将间隔设置为小于一分钟 (0:1:0)。如果需要在系统之间移动连接，则所需的更改需要花费超过 30 秒，并且连接可能会在完成更改之前被删除。

示例：

```
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
half-closed 0:20:0 dcd
```

步骤 5 减少与类匹配的数据包的生存时间 (TTL)：set connection decrement-ttl

要允许跟踪路由通过 ASA（作为其中一跳显示 ASA），需要使用此命令连同 **icmp unreachable** 命令。

示例：

```
hostname(config)# class-map global-policy
hostname(config-cmap)# match any
hostname(config-cmap)# exit
hostname(config)# policy-map global_policy
hostname(config-pmap)# class global-policy
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp unreachable rate-limit 50 burst-size 6
```

步骤 6 设置高级连接选项。

高级选项指在正常情况下无需使用的专用配置。使用 **set connection advanced-options** 命令进行配置。

- **set connection advanced-options tcp_map_name** - 通过应用 TCP 映射自定义 TCP 规范器行为。有关详细信息，请参阅[自定义异常 TCP 数据包处理（TCP 映射、TCP 规范器）](#)，第 380 页。
- **set connection advanced-options tcp-state-bypass** - 实施 TCP 状态绕行。有关详细信息，请参阅[绕过非对称路由的 TCP 状态检查（TCP 状态绕行）](#)，第 383 页。
- **set connection advanced-options 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 327 页。
- **set connection advanced-options flow-offload** - （仅限 FXOS 1.1.3 或更高版本 Firepower 4100/9300 机箱中的 ASA。）实施流量卸载。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，还必须输入 **flow-offload enable** 命令，该命令不属于服务策略。

示例：

```
hostname(config-pmap-c)# set connection advanced-options tcp_map1
```

步骤 7 如果是编辑现有服务策略（例如，称为 `global_policy` 的默认全局策略），执行到这一步即可。否则，应在一个或多个接口上激活策略映射。

service-policy *polycmap_name* {**global** | **interface** *interface_name*}

示例：

```
hostname(config)# service-policy global_policy global
```

Global 关键字指示将策略映射应用于所有接口，而 **interface** 指示仅将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

示例

以下示例设置所有流量的连接限制和超时：

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection conn-max 1000 embryonic-conn-max 3000
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0
half-closed 0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

可以输入带多个参数的 **set connection** 命令，也可以作为单独命令输入每个参数。在运行配置中，ASA 会将这些命令组合成一行。例如，如果在类配置模式下输入了以下两个命令：

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map 命令的输出将在单一组合命令中显示两个命令的结果：

```
set connection conn-max 600 embryonic-conn-max 50
```

配置 TCP 选项

您可以配置选项，以控制 TCP 行为的某些方面。这些设置的默认值适合大多数网络。

过程

步骤 1 (CLI)。配置 TCP 重置行为。

```
service { resetinbound [ interface interface_name ] | resetoutbound [ interface interface_name ] | resetoutside }
```

- **resetinbound**。为所有试图通过 ASA 并被 ASA 根据访问列表或 AAA 设置拒绝的入站 TCP 会话发送 TCP 重置。ASA 还会对访问列表或 AAA 允许但不属于现有连接且被状态防火墙拒绝的数据包发送重置。相同安全级别接口之间的流量也会受到影响。不启用此选项时，ASA 会静默地丢弃被拒绝的数据包。如果未指定接口，则此设置适用于所有接口。
- **resetoutbound**。为所有试图通过 ASA 并被 ASA 根据访问列表或 AAA 设置拒绝的出站 TCP 会话发送 TCP 重置。ASA 还会对访问列表或 AAA 允许但不属于现有连接且被状态防火墙拒绝的数据包发送重置。相同安全级别接口之间的流量也会受到影响。不启用此选项时，ASA 会静默地丢弃被拒绝的数据包。默认情况下，此选项已启用。例如，您可能希望禁用出站重置，以减少流量风暴期间的 CPU 负载。
- **resetoutside**。对终止于安全性最低的接口且被 ASA 根据访问列表或 AAA 设置拒绝的 TCP 数据包启用重置。ASA 还会对访问列表或 AAA 允许但不属于现有连接且被状态防火墙拒绝的数据包发送重置。不启用此选项时，ASA 会静默地丢弃被拒绝的数据包。

建议您将此选项与接口 PAT 配合使用。此选项允许 ASA 终止来自外部 SMTP 或 FTP 服务器的 IDENT。主动重置这些连接可避免 30 秒的超时延迟。

步骤 2 设置 TCP MSS 可确保直通流量的最大 TCP 分段大小不超过您设置的值，且最大值不小于指定大小。

```
sysopt connection tcpmss [ minimum ] bytes
```

不带 **minimum** 关键字。以字节为单位设置 TCP 最大分片大小，范围在 48 和任何最大值之间。默认值为 1380 字节。您可以禁用此功能，只需将字节数设置为 0。

minimum。覆盖最大段大小，使其不小于指定字节，介于 48 和 65535 字节之间。默认情况下，此功能已禁用（设置为 0）。

步骤 3 设置 TCP 连接等待时间。

```
sysopt connection timewait
```

使用此命令可强制每个 TCP 连接在最后一个正常 TCP 关闭序列后处于缩短的 TIME_WAIT 状态（至少 15 秒）。如果终端主机应用默认的 TCP 终止序列是同时关闭，则可能需要使用此功能。

步骤 4 设置 TCP 未处理分段的最大数量。

sysopt connection tcp-max-unprocessed-seg 数据段

设置 TCP 未处理网段的最大数量，从 6 到 24 不等。默认值为 6。如果您发现 SIP 电话未连接到呼叫管理器，您可以尝试增加未处理的 TCP 分段的最大数量。

监控连接

可以使用以下命令监控连接：

- **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。

使用 **detail** 关键字时，您可以查看有关失效连接检测 (DCD) 探测的信息，这会显示发起方和响应方探测连接的频率。例如，对于启用 DCD 的连接，其连接详细信息如下所示：

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
    Locally received: 0 (0 byte/s)
  Traffic received at interface inside
    Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **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。



注释

在 ASA 配置中，初期连接（尚未完成三次握手过程的连接请求）会快速关闭，并且不会在主用设备和备用设备之间同步。此设计可确保高可用性系统的效率 and 安全性。因此，两台 ASA 设备上的连接数可能存在差异，这是预期行为。

连接设置的历史记录

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。 修改了以下命令： set connection timeout
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。 修改了以下命令： timeout floating-conn 。
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。 引入了以下命令： timeout pat-xlate 。 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。 修改了以下命令： set connection conn-max 、 set connection embryonic-conn-max 、 set connection per-client-embryonic-max 、 set connection per-client-max 。
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。 修改了以下命令： set connection timeout half-closed 、 timeout half-closed 。
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。 添加了以下命令： timeout conn-holddown 。

功能名称	平台版本	说明
SCTP 空闲超时和 SCTP 状态绕行	9.5(2)	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。 添加或修改了以下命令：timeout sctp、set connection advanced-options sctp-state-bypass。
Firepower 9300 上 ASA 的数据流分流。	9.5(2.1)	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。 此功能要求具有 FXOS 1.1.3 版本。 添加或修改了以下命令：clear flow-offload、flow-offload enable、set-connection advanced-options flow-offload、show conn detail 和 show flow-offload。
Firepower 4100 系列上 ASA 的数据流分流支持。	9.6(1)	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。 此功能需要 FXOS 1.1.4。 此功能没有新的命令或 ASDM 屏幕。
透明模式下组播连接的数据流分流支持。	9.6(2)	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。 对于此功能，没有新的命令或 ASDM 菜单项。
TCP 选项处理方式的变化。	9.6(2)	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。 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。 修改了以下命令：timeout igp stale-route。
内部网关协议过时路由超时	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。 添加了以下命令：timeout igp stale-route。

功能名称	平台版本	说明
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、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。 添加了以下命令：timeout icmp-error
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。
集群中的“死连接检测” (DCD) 支持的发起方和响应方信息。	9.13(1)	如果启用死连接检测(DCD)，则可以使用该 show conn detail 命令获取有关发起人和响应方的信息。通过死连接检测，您可以保持非活动连接，并且 show conn 输出会告诉您终端的探测频率。此外，在集群中现在还支持 DCD。 新增/修改的命令：show conn（仅输出）
配置初期连接的最大分段大小 (MSS)。	9.16 (1)	您可以配置服务策略，以在达到初期连接限制时为初期连接的 SYN-Cookie 设置服务器最大分段大小 (MSS)。这对于还设置初期连接最大值的服务策略非常重要。 新增的或更改的命令：set connection syn-cookie-mss。
IPsec 流分流。	9.18(1)	在 Cisco Secure Firewall 3100 上，默认情况下会分流 IPsec 流。初始设置 IPsec 站点间 VPN 或远程访问 VPN 安全关联 (SA) 后，IPsec 连接将被分流到设备中的现场可编程门阵列 (FPGA)，这应该会提高设备性能。 添加了以下命令：clear flow-offload-ipsec、flow-offload-ipsec、show flow-offload-ipsec
DTLS 加密加速	9.22(1)	Cisco Secure Firewall 4200 和 3100 系列支持 DTLS 加密加速。硬件执行 DTLS 加密和解密，并提高 DTLS 加密和 DTLS 解密流量的吞吐量。硬件还会对出口加密数据包执行优化，以改善延迟。 新增/修改的命令：flow-offload-dtls、flow-offload-dtls egress-optimization
Cisco Secure Firewall 3100/4200 默认启用流量分流	9.23(1)	流量分流现已默认启用。 添加/修改的命令：flow-offload enable。

功能名称	平台版本	说明
集群重定向：支持 Cisco Secure Firewall 4200 不对称集群流量的流分流	9.23(1)	对于不对称流，集群重定向允许转发节点将流量分流到硬件上。默认情况下启用此功能。 当现有流的流量被发送到不同节点时，该流量会通过集群控制链路重定向到所有者节点。由于不对称数据流会在集群控制链路上产生大量流量，因此由转发器分流这些数据流可提高性能。 添加/修改的命令：flow-offload cluster-redirect、show conn、show flow-offload flow、show flow-offload flow protocol、show flow-offload info。
在分布式站点间 VPN 模式下，对 Cisco Secure Firewall 4200 上的集群控制链路上的流量进行 IPsec 流分流	9.23(1)	对于分布式站点间 VPN 模式中的不对称流量，IPsec 流分流现在可让流量所有者在硬件中解密通过集群控制链路转发的 IPsec 流量。此功能不可配置，启用 IPsec 流分流后始终可用。 添加/修改的命令：flow-offload-ipsec、show crypto ipsec sa detail。



第 17 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。

以下主题介绍如何应用 QoS 策略。

- [关于 QoS，第 407 页](#)
- [QoS 准则，第 409 页](#)
- [配置 QoS，第 409 页](#)
- [监控 QoS，第 415 页](#)
- [优先级排队和策略管制的配置示例，第 416 页](#)
- [QoS 的历史记录，第 418 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 408 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 408 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 411 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 准则

情景模式准则

仅支持单情景模式。不支持多情景模式。

防火墙模式准则

仅支持路由防火墙模式。不支持透明防火墙模式。

IPv6 准则

不支持 IPv6。

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。
- 对于优先级排队，必须为某个物理接口配置优先级队列。
- 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 410 页。

步骤 2 为接口配置优先级队列，第 411 页。

步骤 3 为优先级排队和策略管制配置服务规则，第 412 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 411 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 13: 队列限制工作表

1	_____	Mbps	x	125	=	_____		
	出站带宽（单位为 Mbps 或 Kbps）	kbps	x	0.125	=	_____		
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 14: 传输环路限制工作表

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			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。

过程

步骤 1 创建接口的优先级队列。

priority-queue *interface_name*

示例：

```
hostname(config)# priority-queue inside
```

interface_name 参数指定要启用优先级队列的物理接口名称。

步骤 2 更改优先级队列的大小。

queue-limit *number_of_packets*

默认队列限制为 1024 个数据包。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）。以避免队列填充起来，您可以使用 **queue-limit** 命令以提高队列缓冲区大小。

用于 **queue-limit** 命令的值范围上限在运行时动态决定。要查看此限制，请在命令行中输入 **queue-limit?**。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。

示例：

```
hostname(config-priority-queue)# queue-limit 260
```

步骤 3 指定优先级队列的深度。

tx-ring-limit *number_of_packets*

默认 **tx-ring-limit** 是 511 个数据包。此命令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。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。

用于 **tx-ring-limit** 命令的值范围上限在运行时动态决定。要查看此限制，请在命令行中输入 **tx-ring-limit ?**。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 **tx-ring-limit** 会影响较高优先级低延迟队列和尽力而为队列。

示例：

```
hostname(config-priority-queue)# tx-ring-limit 3
```

示例

以下示例在接口“outside”（GigabitEthernet0/1 接口）建立优先级队列，默认值为 **queue-limit** 和 **tx-ring-limit**：

```
hostname(config)# priority-queue outside
```

以下示例在接口“outside”（GigabitEthernet0/1 接口）建立优先级队列，将 **queue-limit** 设置为 260 个数据包，并将 **tx-ring-limit** 设置为 3：

```
hostname(config)# priority-queue outside
hostname(config-priority-queue)# queue-limit 260
hostname(config-priority-queue)# tx-ring-limit 3
```

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 408 页](#)。

开始之前

- 对于优先级流量，无法使用 **class - default** 类映射。
- 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 创建一个 L3/L4 类映射，以标识要对其执行优先级排队的流量。

```
class-map name  
match parameter
```

示例:

```
hostname(config)# class-map priority_traffic  
hostname(config-cmap)# match access-list priority
```

有关详细信息，请参阅 [为通过流量创建第 3/4 层类映射](#)，第 230 页。

步骤 2 创建一个 L3/L4 类映射，以标识要对其执行优先级策略管制的流量。

```
class-map name  
match parameter
```

示例:

```
hostname(config)# class-map policing_traffic  
hostname(config-cmap)# match access-list policing
```

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 添加或编辑策略映射: **policy-map name**

示例:

```
hostname(config)# policy-map QoS_policy
```

步骤 4 标识您为应用优先级排列的流量创建的类映射，并为该类配置优先级排队。

```
class priority_map_name
priority
```

示例：

```
hostname(config-pmap)# class priority_class
hostname(config-pmap-c)# priority
```

步骤 5 标识您为应用策略管制的流量创建的类映射：**class name**

示例：

```
hostname(config-pmap)# class policing_class
```

步骤 6 配置类的策略管制。

```
police {output | input} conform-rate [conform-burst] [conform-action [drop | transmit]] [exceed-action
[drop | transmit]]
```

选项有：

- **output**- 为流向输出方向的流量启用策略管制。
- **input**- 为流向输入方向的流量启用策略管制。
- **conform-rate** - 为此流量类设置速率限制，范围从每秒 8000 位到 2000000000 位。例如，要将流量限制为 5Mbps，请输入 5000000。
- **conform-burst** - （可选。）指定控制到符合速率值之前连续突发中允许的最大即时字节数，该值介于 1000 到 512000000 字节之间。如果省略该变量，突发大小将按符合速率的 1/32 计算（以字节为单位）。例如，5Mbps 速率的突发大小为 156250。
- **conform-action** - （可选。）设置流量低于管制速率和突发大小时要执行的操作。可以丢弃或传输流量。默认为传输流量。
- **exceed-action** - （可选。）设置流量超过策略管制速率和突发大小时要执行的操作。可以丢弃或传输超过策略管制速率和突发大小的数据包。默认情况下会丢弃多余的数据包。

示例：

```
hostname(config-pmap-c)# police output 56000 10500
```

步骤 7 激活一个或多个接口上的策略映射。

```
service-policy policymap_name {global | interface interface_name}
```

示例：

```
hostname(config)# service-policy QoS_policy interface inside
```

global 选项将策略映射应用于所有接口，而 **interface** 选项将策略应用于一个接口。仅允许存在一个全局策略。可以通过向接口应用服务策略来覆盖该接口上的全局策略。每个接口只能应用一个策略映射。

监控 QoS

以下主题介绍如何监控 QoS。

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: TG1-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。

优先级排队和策略管制的配置示例

以下各节提供配置优先级排队和策略管制的示例。

VPN 流量的类映射示例

在以下示例中，**class-map** 命令采用一个名为 **tcp_traffic** 的 ACL 对所有不通过隧道传输的 TCP 流量进行分类：

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic
```

在以下示例中，使用其他更具体的匹配条件来分类与安全相关的特定隧道组的流量。这些具体匹配标准规定隧道组（在本示例中指先前定义的隧道组 1）上的匹配需要作为第一个匹配特征以对特定隧道的流量进行分类，并且此匹配允许一个附加匹配线对流量进行分类（IP 差分服务代码点，加速转发）。

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef
```

在以下示例中，**class-map** 命令根据流量类型对通过隧道传输和不通过隧道传输的流量分类：

```
hostname(config)# access-list tunneled extended permit ip 10.10.34.0 255.255.255.0
192.168.10.0 255.255.255.0
hostname(config)# access-list non-tunneled extended permit tcp any any
hostname(config)# tunnel-group tunnel-grp1 type IPsec_L2L

hostname(config)# class-map browse
hostname(config-cmap)# description "This class-map matches all non-tunneled tcp traffic."
hostname(config-cmap)# match access-list non-tunneled

hostname(config-cmap)# class-map TG1-voice
hostname(config-cmap)# description "This class-map matches all dscp ef traffic for
tunnel-grp 1."
hostname(config-cmap)# match dscp ef
hostname(config-cmap)# match tunnel-group tunnel-grp1

hostname(config-cmap)# class-map TG1-BestEffort
hostname(config-cmap)# description "This class-map matches all best-effort traffic for
tunnel-grp1."
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address
```

以下示例显示一种在隧道内对流量进行策略管制的方式，前提是分类的流量未被指定为隧道，而是经过隧道。在本示例中，192.168.10.10 是远程隧道的专用端上的主机地址，且 ACL 命名为“host-over-l2l”。通过创建类映射（名为“host-specific”），可在 LAN 到 LAN 连接实施隧道策略管制前对“host-specific”类进行策略管制。在本例中，在通过隧道传输前先对“host-specific”流量应用速率限制，再对隧道应用速率限制：

```
hostname(config)# access-list host-over-l2l extended permit ip any host 192.168.10.10
hostname(config)# class-map host-specific
hostname(config-cmap)# match access-list host-over-l2l
```

优先级和策略管制示例

以下示例构建在上节中开发的配置之上。在上述示例中，有两个命名的类映射：tcp_traffic 和 TG1-voice。

```
hostname(config)# class-map TG1-best-effort
hostname(config-cmap)# match tunnel-group Tunnel-Group-1
hostname(config-cmap)# match flow ip destination-address
```

添加第三个类映射可为定义通过隧道传输和不通过隧道传输的 QoS 策略建立基础，以下示例中为通过隧道传输和不通过隧道传输的流量创建了一个简单 QoS 策略，将 TGl-voice 类的数据包分配到低延迟队列，并设置了 tcp_traffic 和 TGl-best-effort 流量数据流上的速率限制。

在本示例中，tcp_traffic 类流量的最大速率为 56,000 位/秒，最大突发大小为 10,500 字节/秒。TC1-BestEffort 类的最大速率为 200,000 位/秒，最大突发大小为 37,500 字节/秒。TC1-voice 类流量的最大速度或突发速率不受策略管制，因为它们属于优先级类。

```
hostname(config)# access-list tcp_traffic permit tcp any any
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match access-list tcp_traffic

hostname(config)# class-map TGl-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config-cmap)# class-map TGl-BestEffort
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match flow ip destination-address

hostname(config)# policy-map qos
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# police output 56000 10500

hostname(config-pmap-c)# class TGl-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# class TGl-best-effort
hostname(config-pmap-c)# police output 200000 37500

hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)# police output 1000000 37500

hostname(config-pmap-c)# service-policy qos global
```

QoS 的历史记录

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。 引入了以下命令： priority-queue 、 queue-limit 、 tx-ring-limit 、 priority 、 police 、 show priority-queue statistics 、 show service-policy police 、 show service-policy priority 、 show running-config priority-queue 和 clear configure priority-queue 。
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。 引入了以下命令： shape 、 show service-policy shape 。
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 18 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 419 页](#)
- [威胁检测准则，第 421 页](#)
- [威胁检测的默认设置，第 422 页](#)
- [配置威胁检测，第 423 页](#)
- [监控威胁检测，第 428 页](#)
- [威胁检测示例，第 437 页](#)
- [威胁检测的历史记录，第 437 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。请参阅[基本威胁检测统计信息，第 420 页](#)。
- 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。请参阅[高级威胁检测统计信息，第 420 页](#)。
- 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。请参阅[扫描威胁检测，第 421 页](#)。

- VPN 服务的威胁检测，可用于防止来自 IPv4 地址的以下类型的 VPN 攻击：
 - 远程访问 VPN 验证尝试失败过多，例如用户名/密码暴力扫描。
 - 客户端启动攻击，即攻击者从一台主机发起但未完成与远程访问 VPN 头端的重复连接尝试。
 - 尝试访问无效的 VPN 服务，即仅供内部使用的服务。

这些攻击即使未能成功获取访问权，也会消耗计算资源，有时甚至会导致拒绝服务。请参阅[为 VPN 服务配置威胁检测，第 427 页](#)。

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 15: 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。

威胁检测准则

安全情景准则

除了高级威胁统计信息和VPN服务，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

- 统计时，只监控通过设备的流量，不监控传入流量。

- 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。
- 对于 VPN 服务，只监控来自 IPv4 地址的设备流量。

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。

对于 VPN 服务威胁检测，默认情况下禁用所有服务。

表 16: 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
• 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。

丢包原因	触发器设置	
	平均速率	突发速率
- 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 423 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 424 页。](#)

步骤 3 [配置扫描威胁检测，第 426 页。](#)

步骤 4 [为 VPN 服务配置威胁检测，第 427 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 启用基本威胁检测统计信息（如果以前已禁用）。

threat-detection basic-threat

示例：

```
hostname(config)# threat-detection basic-threat
```

默认情况下，启用基本威胁检测。使用 **no threat-detection basic-threat** 禁用此功能。

步骤 2（可选）更改一种或多种事件类型的默认设置。

```
threat-detection rate {acl-drop | bad-packet-drop | conn-limit-drop | dos-drop | fw-drop | icmp-drop |  
inspect-drop | interface-drop | scanning-threat | syn-attack} rate-interval rate_interval average-rate  
av_rate burst-rate burst_rate
```

有关每种事件类型的说明，请参阅第 8-1 页的“基本威胁检测统计信息”。

当您将此命令与 **scanning-threat** 关键字配合使用时，还可以在扫描威胁检测中使用此命令。如果不配置基本威胁检测，依然可以将此命令与 **scanning-threat** 关键字配合使用，以配置扫描威胁检测的速率限制。

可以为每种事件类型配置最多三个不同的速率间隔。

示例：

```
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate  
100
```

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（可选）启用全部统计信息。

```
threat-detection statistics
```

要仅启用某些统计信息，请为每个统计信息类型输入此命令（如此操作步骤后面所示），但不要输入不带任何选项的命令。可以输入 **threat-detection statistics**（不带任何选项），然后通过输入具有统计信息特定选项（例如，**threat-detection statistics host number-of-rate 2**）的命令自定义某些统计信息。如果输入 **threat-detection statistics**（不带任何选项），然后输入特定统计信息的命令，但不带任何统计信息特定选项，则该命令没有任何影响，因为命令已启用。

如果输入此命令的 **no** 形式，它会删除所有 **threat-detection statistics** 命令，包括默认情况下已启用的 **threat-detection statistics access-list** 命令。

示例：

```
hostname(config)# threat-detection statistics
```

步骤 2 （可选）启用 ACL 统计信息（如果以前被禁用）。

threat-detection statistics access-list

默认情况下，启用 ACL 统计信息。ACL 统计信息只能使用 **show threat-detection top access-list** 命令禁用。

示例：

```
hostname(config)# threat-detection statistics access-list
```

步骤 3 （可选）为主机（**host** 关键字）、TCP 和 UDP 端口（**port** 关键字）或者非 TCP/UDP IP 协议（**protocol** 关键字）配置统计信息。

threat-detection statistics {host | port | protocol} [number-of-rate {1 | 2 | 3}]

number-of-rate 关键字设置为统计信息维护的速率间隔数量。默认速率间隔数为 **1**，该值将保持较低的内存利用率。要查看更多速率间隔，请将该值设置为 **2** 或 **3**。例如，如果将该值设置为 **3**，则查看过去 1 小时、8 小时和 24 小时的数据。如果将此关键字设置为 **1**（默认值），则仅维护最短速率间隔的统计信息。如果将该值设置为 **2**，则维护最短的两个间隔。

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）。

示例：

```
hostname(config)# threat-detection statistics host number-of-rate 2
```

```
hostname(config)# threat-detection statistics port number-of-rate 2
```

```
hostname(config)# threat-detection statistics protocol number-of-rate 3
```

步骤 4 （可选）配置 TCP 拦截所拦截的攻击的统计信息。

threat-detection statistics tcp-intercept [rate-interval minutes] [burst-rate attacks_per_sec] [average-rate attacks_per_sec]

其中：

- **rate-interval** 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。在此间隔内，ASA 将对攻击数量抽样 30 次。
- **Burst-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-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。

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 377 页。

注释

此命令在多情景模式下可用，不同于其他威胁检测命令。

示例：

```
hostname(config)# threat-detection statistics tcp-intercept rate-interval 60
burst-rate 800 average-rate 600
```

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。

您可以将ASA配置为发送有关攻击者的系统日志消息，也可以自动避开主机。默认情况下，主机被标识为攻击者后，将生成系统日志消息 730101。当您预期主机将发送大量信息时，请确保将地址从规避中删除。例如，如果启用了 PIM 组播，则 PIM 路由器或 PIM 信息将被放弃。

过程

步骤 1 启用扫描威胁检测。

```
threat-detection scanning-threat [shun [except {ip-address ip_address mask | object-group
network_object_group_id}]]
```

默认情况下，主机被标识为攻击者后，将生成系统日志消息 733101。多次输入此命令以标识无需回避的多个 IP 地址或网络对象组。

示例：

```
hostname(config)# threat-detection scanning-threat shun except
ip-address 10.1.1.0 255.255.255.0
```

步骤 2 （可选）为攻击主机设置避开持续时间。

```
threat-detection scanning-threat shun duration seconds
```

示例：

```
hostname(config)# threat-detection scanning-threat shun duration 2000
```

步骤 3 （可选）更改 ASA 将主机标识为攻击者或目标时的默认事件限制。

```
threat-detection rate scanning-threat rate-interval rate_interval average-rate av_rate burst-rate burst_rate
```

如果在基本威胁检测配置过程中已配置了此命令，则那些设置将与扫描威胁检测功能共享；不能为基本和扫描威胁检测配置独立速率。如果不使用此命令设置速率，则将默认值用于扫描威胁检测功能和基本威胁检测功能。通过输入不同的命令，最多可配置三个不同的速率间隔。

示例：

```
hostname(config)# threat-detection rate scanning-threat rate-interval 1200
average-rate 10 burst-rate 20
```

```
hostname(config)# threat-detection rate scanning-threat rate-interval 2400
```

```
average-rate 10 burst-rate 20
```

为 VPN 服务配置威胁检测

您可以启用 VPN 服务威胁检测，以帮助防止来自 IPv4 地址的拒绝服务 (DoS) 攻击。针对以下类型的攻击，可提供单独的服务：

- 远程访问 VPN 登录身份验证。通过在密码泄露攻击中反复开始登录尝试，攻击者可以消耗用于身份验证尝试的资源，从而阻止真实用户登录 VPN。
- 客户端启动攻击，即攻击者从一台主机发起但未完成与远程访问 VPN 头端的重复连接尝试。与密码泄露攻击类似，这种攻击也会消耗资源，并阻止有效用户连接到 VPN。
- 尝试连接到无效的 VPN 服务，即服务仅供内部使用。尝试这种连接的 IP 地址会立即被避开。

启用这些服务后，系统会自动避开超过阈值的主机，以防止进一步的尝试。您可以使用地址的 **no shun** 命令来手动删除回避。

要手动将服务的计数器重置为 0，请使用 **clear threat-detection service** 命令。

开始之前

在决定适当的抑制值和阈值时，请考虑在您的环境中使用 NAT。如果使用 PAT，使许多请求来自同一 IP 地址，则应考虑提高身份验证失败和客户端启动服务的值，以确保有效用户有足够的时间完成连接。例如，在一家酒店，许多客户可能会在很短的时间内尝试连接。

过程

步骤 1 启用远程访问 VPN 身份验证失败的威胁检测。

```
threat-detection service remote-access-authentication hold-down minutes threshold count
```

其中：

- **hold-down minutes** 定义了从最后一次失败算起的抑制时间。攻击者的 IPv4 地址必须在前一次失败的抑制期内达到连续失败的阈值次数，才能触发回避。例如，如果抑制时间为 10 分钟，阈值为 20，并且来自单个 IPv4 地址的连续 20 次身份验证失败，且任何两次连续失败之间的时间间隔不超过 10 分钟，则将避开该源 IPv4 地址。可以指定介于 1 和 1440 分钟之间的时间。
- **threshold count** 定义在抑制期间必须发生的、会触发回避的失败尝试次数。可以指定 1 到 100 之间的阈值。

要禁用该服务，请使用以下命令：

```
no threat-detection service remote-access-authentication
```

示例：

下面的示例设置的指标是 20 分钟内发生 10 次故障。

```
ciscoasa(config)# threat-detection service remote-access-authentication
hold-down 10 threshold 20
```

步骤 2 启用远程访问 VPN 客户端启动时的威胁检测。

threat-detection service remote-access-client-initiations hold-down minutes threshold count

其中：

- **hold-down minutes** 定义了从最后一次启动算起的抑制时间。必须在上一次启动的抑制期内达到连续启动的阈值次数，才能触发对客户端 IPv4 地址的回避。例如，如果抑制时间为 10 分钟，阈值为 20，并且来自单个 IPv4 地址的连续启动次数为 20 次，且任何两次连续启动之间的时间间隔不超过 10 分钟，则将避开该源 IPv4 地址。可以指定介于 1 和 1440 分钟之间的时间。
- **threshold count** 定义在抑制期间必须发生的发起次数才能触发规避。可以指定 5 到 100 之间的阈值。

要禁用该服务，请使用以下命令：

no threat-detection service remote-access-client-initiations

示例：

下面的示例设置的指标是 20 分钟内启动 10 次。

```
ciscoasa(config)# threat-detection service remote-access-client-initiations
hold-down 10 threshold 20
```

步骤 3 对尝试连接无效 VPN 服务的行为启用威胁检测。

threat-detection service invalid-vpn-access

要禁用该服务，请使用以下命令：

no threat-detection service invalid-vpn-access

示例：

下面的示例启用了无效 VPN 访问服务。

```
ciscoasa(config)# threat-detection service invalid-vpn-access
```

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

要显示基本威胁检测统计信息，请使用以下命令：

```
show threat-detection rate [min-display-rate min_display_rate] [acl-drop | bad-packet-drop |  
conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop | interface-drop | scanning-threat |  
syn-attack]
```

min-display-rate *min_display_rate* 参数将显示内容限制为超出每秒最低事件显示速率的统计信息。可以将 *min_display_rate* 设置在 0 到 2147483647 之间。

其他参数可以让您将显示内容限制为特定类别。有关每种事件类型的说明，请参阅[基本威胁检测统计信息，第 420 页](#)。

输出显示两个固定时间段中的平均速率（单位：事件数/秒）：最后 10 分钟和最后 1 小时。它还显示：最后完成的突发间隔（平均速率间隔的 1/30 或 10 秒，以较大者为准）内当前突发速率（单位：事件数/秒）；超出（被触发）速率的次数；以及时间段中的事件总数。

对于完成的总共 30 个突发间隔，ASA 在每个突发期间的末尾存储计数。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。这种情况下，ASA 会计算过去 29 个完成间隔的总事件数再加上未完成突发间隔到目前的事件数。此例外可让您实时监控事件的大幅增加。

可以使用 **clear threat-detection rate** 命令清除统计信息。

以下是 **show threat-detection rate** 命令的输出示例：

```
hostname# show threat-detection rate
```

	Average (eps)	Current (eps)	Trigger	Total events
10-min ACL drop:	0	0	0	16
1-hour ACL drop:	0	0	0	112
1-hour SYN attck:	5	0	2	21438
10-min Scanning:	0	0	29	193
1-hour Scanning:	106	0	10	384776
1-hour Bad pkts:	76	0	2	274690
10-min Firewall:	0	0	3	22
1-hour Firewall:	76	0	2	274844
10-min DoS attck:	0	0	0	6
1-hour DoS attck:	0	0	0	42
10-min Interface:	0	0	0	204
1-hour Interface:	88	0	0	318225

监控高级威胁检测统计信息

要监控高级威胁检测统计信息，请使用下表中显示的命令。显示内容输出显示以下内容：

- 固定时间段内的平均速率（单位：事件数/秒）。
- 上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的当前突发速率（单位：事件数/秒）

- 超过速率的次数（仅适用于丢弃流量统计信息）
- 固定时间段内的事件总数。

对于完成的总共 30 个突发间隔，ASA 在每个突发期间的末尾存储计数。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 **show** 命令，则最后 5 秒不会包含在输出中。

此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。这种情况下，ASA 会计算过去 29 个完成间隔的总事件数再加上未完成突发间隔到目前的事件数。此例外可让您实时监控事件的大幅增加。

命令	目的
show threat-detection statistics [min-display-rate <i>min_display_rate</i>] top [[access-list host port-protocol] [rate-1 rate-2 rate-3] tcp-intercept [all] detail]]	显示前 10 条统计信息。如果不输入任何选项，将显示所有类别的前 10 条统计信息。 min-display-rate <i>min_display_rate</i> 参数将显示内容限制为超出每秒最低事件显示速率的统计信息。可以将 <i>min_display_rate</i> 设置在 0 到 2147483647 之间。 以下行将解释可选关键字。
show threat-detection statistics [min-display-rate <i>min_display_rate</i>] top access-list [rate-1 rate-2 rate-3]	要查看匹配数据包的前 10 个 ACE（包括允许和拒绝 ACE），请使用 access-list 关键字。允许和拒绝的流量在此显示内容中没有区别。如果使用 threat-detection basic-threat 命令启用基本威胁检测，则可以使用 show threat-detection rate acl-drop 命令跟踪 ACL 拒绝。 rate-1 关键字显示在显示内容中提供的最小固定速率间隔的统计信息；rate-2 显示第二大的速率间隔；如果定义了三个间隔，则 rate-3 显示最大的速率间隔。例如，显示内容显示最后 1 小时、8 小时和 24 小时的统计信息。如果设置为 rate-1 关键字，则 ASA 仅显示 1 小时的时间间隔。
show threat-detection statistics [min-display-rate <i>min_display_rate</i>] top host [rate-1 rate-2 rate-3]	要仅查看主机统计信息，请使用 host 关键字。注意：由于威胁检测算法，用作组合故障转移和状态链路的接口会在前 10 个主机中显示；这是预期行为，而且您可以在显示内容中忽略此 IP 地址。
show threat-detection statistics [min-display-rate <i>min_display_rate</i>] top port-protocol [rate-1 rate-2 rate-3]	要查看端口和协议统计信息，请使用 port-protocol 关键字。port-protocol 关键字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。
show threat-detection statistics [min-display-rate <i>min_display_rate</i>] top tcp-intercept [all] detail]]	要查看 TCP 拦截统计信息，请使用 tcp-intercept 关键字。显示内容包含受到攻击的前 10 台受保护服务器。all 关键字显示所有被跟踪服务器的历史数据。detail 关键字显示历史记录采样数据。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。

命令	目的
show threat-detection statistics [min-display-rate <i>min_display_rate</i>] host [<i>ip_address</i> [<i>mask</i>]]	显示所有主机或特定主机或子网的统计信息。
show threat-detection statistics [min-display-rate <i>min_display_rate</i>] port [<i>start_port</i> [- <i>end_port</i>]]	显示所有端口或特定端口或端口范围的统计信息。
show threat-detection statistics [min-display-rate <i>min_display_rate</i>] protocol [<i>protocol_number</i> <i>protocol</i>]	显示所有 IP 协议或特定协议的统计信息。 <i>protocol_number</i> 参数是介于 0 到 255 之间的整数。 <i>protocol</i> 参数可以是 ah 、 eigrp 、 esp 、 gre 、 icmp 、 icmp6 、 igmp 、 igrp 、 ip 、 ipinip 、 ipsec 、 nos 、 ospf 、 pcp 、 pim 、 pptp 、 snp 、 tcp 、 udp 中的一个。

评估主机威胁检测统计信息

以下是 **show threat-detection statistics host** 命令的输出示例：

```
hostname# show threat-detection statistics host

                                Average(eps)   Current(eps) Trigger                Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:                2938                0                0                10580308
  8-hour Sent byte:                 367                0                0                10580308
 24-hour Sent byte:                 122                0                0                10580308
  1-hour Sent pkts:                  28                0                0                104043
  8-hour Sent pkts:                   3                0                0                104043
 24-hour Sent pkts:                   1                0                0                104043
 20-min Sent drop:                   9                0                1                10851
  1-hour Sent drop:                   3                0                1                10851
  1-hour Recv byte:                2697                0                0                9712670
  8-hour Recv byte:                 337                0                0                9712670
 24-hour Recv byte:                 112                0                0                9712670
  1-hour Recv pkts:                  29                0                0                104846
  8-hour Recv pkts:                   3                0                0                104846
 24-hour Recv pkts:                   1                0                0                104846
 20-min Recv drop:                   42                0                3                50567
  1-hour Recv drop:                  14                0                1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                   0                0                0                 614
  8-hour Sent byte:                   0                0                0                 614
 24-hour Sent byte:                   0                0                0                 614
  1-hour Sent pkts:                   0                0                0                   6
  8-hour Sent pkts:                   0                0                0                   6
 24-hour Sent pkts:                   0                0                0                   6
 20-min Sent drop:                   0                0                0                   4
  1-hour Sent drop:                   0                0                0                   4
  1-hour Recv byte:                   0                0                0                706
  8-hour Recv byte:                   0                0                0                706
 24-hour Recv byte:                   0                0                0                706
  1-hour Recv pkts:                   0                0                0                   7
```

下表对输出进行了解释。

表 17: *show threat-detection statistics host*

字段	说明
Host	主机 IP 地址。
tot-ses	自主机添加到数据库后的该主机会话总数。
act-ses	主机当前参与的活动会话总数。
fw-drop	防火墙丢包数量。防火墙丢包是一个组合速率，其中包括在基本威胁检测中跟踪的与防火墙有关的所有丢包，包括 ACL 拒绝的数据包、错误数据包、超出连接限制的数据包、DoS 攻击数据包、可疑 ICMP 数据包、TCP SYN 攻击数据包以及无返回数据 UDP 会话攻击数据包。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。
insp-drop	因为数据包未通过应用检查而被丢弃的数据包的数量。
null-ses	空会话数量，空会话是指在 3 秒超时内未完成的 TCP SYN 会话，以及在会话开始后 3 秒内没有其服务器发送的任何数据的 UDP 会话。
bad-acc	对处于关闭状态的主机端口的不良访问尝试次数。当确定端口处于空会话中（请参阅 null-ses 字段说明）时，主机的端口状态被设为 HOST_PORT_CLOSE。任何访问该主机端口的客户端都会被立即分类为错误访问，无需等待超时。
Average(eps)	每个时间段内的平均速率（单位：事件数/秒）。 对于完成的总共 30 个突发间隔，ASA 在每个突发期间的末尾存储计数。当前进行的未完成突发间隔不包括在平均速率中。例如，如果平均速率间隔为 20 分钟，则突发间隔为 20 秒。如果上一个突发间隔为 3:00:00 至 3:00:20，并且您在 3:00:25 使用 show 命令，则最后 5 秒不会包含在输出中。 此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。这种情况下，ASA 会计算过去 29 个完成间隔的总事件数再加上未完成突发间隔到目前的事件数。此例外可让您实时监控事件的大幅增加。
Current(eps)	上一个完整突发间隔（平均速率间隔的 1/30 或 10 秒，两者中取较大的一个）内的当前突发速率（单位：事件数/秒）。对于 Average(eps) 说明中指定的示例，当前速率为 3:19:30 至 3:20:00 的速率
触发器	超出丢包速率限制的次数。对于发送和接收的字节和数据包行中标识的有效流量，此值始终为 0，因为对触发有效流量没有速率限制。
Total events	每个速率间隔内的事件总数。当前进行的未完成突发间隔不包括在事件总数中。此规则的唯一例外是，当计算总事件数时，未完成突发间隔内的事件数已超过最早突发间隔（30 个的第 1 个）内的事件数。这种情况下，ASA 会计算过去 29 个完成间隔的总事件数再加上未完成突发间隔到目前的事件数。此例外可让您实时监控事件的大幅增加。

字段	说明
20-min, 1-hour, 8-hour, and 24-hour	这些固定速率间隔的统计信息。对于每个间隔： • Sent byte - 从主机成功发送的字节数。 • Sent pkts - 从主机成功发送的数据包数。 • Sent drop - 已从主机发送但因为扫描攻击的一部分而被丢弃的数据包数。 • Recv byte - 主机成功接收的字节数。 • Recv pkts - 主机成功接收的数据包数。 • Recv drop - 主机已接收但因为扫描攻击的一部分而被丢弃的数据包数。

监控被避开的主机、攻击者和攻击目标

要监控和管理回避的主机和攻击者以及扫描威胁检测目标，请使用以下命令。这些命令仅用于扫描威胁检测，不适用于其他服务。

• **show threat-detection shun**

显示当前避开的主机。例如：

```
hostname# show threat-detection shun

Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

• **clear threat-detection shun [ip_address [mask]]**

释放回避的主机。如果不指定 IP 地址，所有主机都将从避开列表清除。

例如，要释放位于 10.1.1.6 的主机，请输入以下命令：

```
hostname# clear threat-detection shun 10.1.1.6
```

• **show threat-detection scanning-threat [attacker | target]**

显示 ASA 确定为攻击者的主机（包括避开列表中的主机），并显示成为攻击目标的主机。如果不输入选项，将显示攻击者和攻击目标主机。例如：

```
hostname# show threat-detection scanning-threat

Latest Target Host & Subnet List:
 192.168.1.0 (121)
 192.168.1.249 (121)
Latest Attacker Host & Subnet List:
 192.168.10.234 (outside)
```

```

192.168.10.0 (outside)
192.168.10.2 (outside)
192.168.10.3 (outside)
192.168.10.4 (outside)
192.168.10.5 (outside)
192.168.10.6 (outside)
192.168.10.7 (outside)
192.168.10.8 (outside)
192.168.10.9 (outside)

```

监控 VPN 服务的威胁检测

您可以使用 `syslog` 和 `show` 命令监控 VPN 服务的威胁检测，具体说明见以下主题。

威胁检测 VPN 服务的系统日志监控

您可能会看到以下与这些服务相关的系统日志消息：

- `%ASA-6-733200: 威胁检测信息: 消息`

此消息报告用于威胁检测的一般信息事件。

- `%ASA-4-733201:威胁检测: 服务[服务]对等体[对等体]: 已超过阈值阈的阈值。正在将回避添加到接口 interface。额外消息`

此消息显示，由于指定服务的可疑活动，威胁检测服务规避了某个 IP 地址。该消息可能包含其他信息。例如，对于 RA VPN 客户端发起尝试，附加信息可能是“SSL（或 IKEv2）：RA 客户端发起请求过多”。

您可以使用 `show shun` 命令来查看规避的主机列表。如果知道 IP 地址不是攻击者，则可以使用 `no shun` 命令移除回避。

显示 VPN 服务威胁检测的监控命令

要显示威胁检测 VPN 服务的统计数据，请使用以下命令：

show threat-detection service [*service*] [**entries** | **details**]

您可以选择将视图限制为特定服务（**remote-access-authentication**、**remote-access-client-initiations** 或 **invalid-vpn-access**）。您可以通过添加这些参数来进一步限制视图：

- **entries** - 仅显示正在跟踪的条目。例如，身份验证尝试失败的 IP 地址。
- **details** - 显示服务详细信息和服务条目。

根据所选选项，显示输出如下：

- 服务名称
- 服务状态：启用或禁用
- 服务抑制设置

- 服务阈值设置
- 服务操作统计信息
 - 失败 - 处理报告的事件时发生故障。
 - 阻止 - 报告的事件发生在抑制时间段内并且达到或超过阈值。因此，服务会自动安装回避以阻止恶意对等体。
 - 记录 - 报告的事件在抑制时间段之外，或者达到或超过阈值。因此，服务将记录发生的情况。
 - 不支持 - 报告的事件当前不支持自动避开。
 - 禁用 — 已报告事件；请参阅但服务已禁用。

示例

以下示例显示所有服务都已启用，远程访问身份验证服务正在跟踪潜在攻击者。

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
  State      : Enabled
  Hold-down  : 1 minutes
  Threshold  : 1
  Stats:
    failed      :          0
    blocking    :          0
    recording    :          0
    unsupported  :          0
    disabled    :          0
  Total entries: 0
Service: remote-access-authentication
  State      : Enabled
  Hold-down  : 10 minutes
  Threshold  : 20
  Stats:
    failed      :          0
    blocking    :          1
    recording    :          4
    unsupported  :          0
    disabled    :          0
  Total entries: 3
Name: remote-access-client-initiations
  State      : Enabled
  Hold-down  : 10 minutes
  Threshold  : 20
  Stats:
    failed      :          0
    blocking    :          0
    recording    :          0
    unsupported  :          0
    disabled    :          0
  Total entries: 0
```

以下是 **show threat-detection service entries** 命令的示例。

```
ciscoasa# show threat-detection service remote-access-authentication entries
```

删除对 VPN 服务违规应用的规避次数

```
Service: remote-access-authentication
Total entries: 2
```

Idx	Source	Interface	Count	Age	Hold-down
1	192.168.100.101/ 32	outside	1	721	0
2	192.168.100.102/ 32	outside	2	486	114

Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.

以下是 **show threat-detection service details** 命令的示例。

```
ciscoasa# show threat-detection service remote-access-authentication details
```

```
Service: remote-access-authentication
```

```
State : Enabled
```

```
Hold-down : 10 minutes
```

```
Threshold : 20
```

```
Stats:
```

```
failed : 0
```

```
blocking : 1
```

```
recording : 4
```

```
unsupported : 0
```

```
disabled : 0
```

```
Total entries: 2
```

Idx	Source	Interface	Count	Age	Hold-down
1	192.168.100.101/ 32	outside	1	721	0
2	192.168.100.102/ 32	outside	2	486	114

Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.

删除对 VPN 服务违规应用的规避次数

您可以使用以下命令监控为 VPN 服务申请的分区，并删除分区。请注意，威胁检测对 VPN 服务应用的规避不会显示在 **show threat-detection shun** 命令中，该命令仅适用于扫描威胁检测。

- **show shun [ip_address]**

显示规避的主机，包括通过 VPN 服务的威胁检测自动规避的主机，或使用 **shun** 命令手动规避的主机。您可以选择将视图限制到指定的 IP 地址。

- **no shun ip_address [interface if_name]**

仅从指定的 IP 地址删除回避。如果某个地址在多个接口上被避开，并且您想在某些接口上保留 shun，则可以选择性地为回避指定接口名称。

- **clear shun**

从所有 IP 地址中删除回避。

威胁检测示例

以下示例配置基本威胁检测统计信息，并且更改 DoS 攻击速率设置。启用所有高级威胁检测统计信息，速率间隔的主机统计信息数量低至 2。还自定义 TCP 拦截速率间隔。启用扫描威胁检测，自动避开除了 10.1.1.0/24 以外的所有地址。自定义扫描威胁速率间隔。

```
threat-detection basic-threat
threat-detection rate dos-drop rate-interval 600 average-rate 60 burst-rate 100
threat-detection statistics
threat-detection statistics host number-of-rate 2
threat-detection statistics tcp-intercept rate-interval 60 burst-rate 800 average-rate 600
threat-detection scanning-threat shun except ip-address 10.1.1.0 255.255.255.0
threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20
threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20
```

威胁检测的历史记录

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。 引入了以下命令： threat-detection basic-threat 、 threat-detection rate 、 show threat-detection rate 、 clear threat-detection rate 、 threat-detection statistics 、 show threat-detection statistics 、 threat-detection scanning-threat 、 threat-detection rate scanning-threat 、 show threat-detection scanning-threat 、 show threat-detection shun 、 clear threat-detection shun 。
避开持续时间	8.0(4)/8.1(2)	现在可以设置避开持续时间。 引入了以下命令： threat-detection scanning-threat shun duration 。
TCP 拦截统计信息	8.0(4)/8.1(2)	引入了 TCP 拦截统计信息。 引入或修改了以下命令： threat-detection statistics tcp-intercept 、 show threat-detection statistics top tcp-intercept 、 clear threat-detection statistics 。
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。 修改了以下命令： threat-detection statistics host number-of-rates 。

功能名称	平台版本	说明
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。 修改了以下命令：threat-detection statistics port number-of-rates、threat-detection statistics protocol number-of-rates。
提高了内存使用率	8.3(1)	提高了威胁检测的内存使用率。 引入了以下命令：show threat-detection memory。
适用于 VPN 服务的威胁检测	9.20(3)	您可以为 VPN 服务配置威胁检测，以防止来自 IPv4 地址的以下类型的 VPN 攻击： • 远程访问 VPN 验证尝试失败过多，例如用户名/密码暴力扫描。 • 客户端启动攻击，即攻击者从一台主机发起但未完成与远程访问 VPN 头端的重复连接尝试。 • 尝试访问无效的 VPN 服务，即仅供内部使用的服务。 这些攻击即使未能成功获取访问权，也会消耗计算资源，有时甚至会导致拒绝服务。 引入或更改了以下命令：clear threat-detection service、show threat-detection service、shun、threat-detection service。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。