



适用于 **Firepower** 设备管理器的思科 **Firepower** 威胁防御配置指南，版本 **6.3.0**

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: [www.cisco.com go trademarks](http://www.cisco.com/go/trademarks). 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)

© 2015 - 2018 Cisco Systems, Inc. 保留所有权利。



目录

第 1 章

使用入门 1

本指南适用对象 1

Firepower 设备管理器/FTD6.3.0 版本中的新增功能 2

登录系统 5

用户角色决定用户的访问及操作权限 5

登录 Firepower 设备管理器 6

登录命令行界面 (CLI) 7

更改密码 7

设置用户配置文件首选项 8

设置系统 8

连接接口 9

ASA 5508-X 和 5516-X 的布线 9

ASA 5515-X、5525-X、5545-X 和 5555-X 的布线 10

Firepower 2100 的布线 11

Firepower 威胁防御虚拟的虚拟布线 11

ISA 3000 的布线 13

完成初始配置 14

如果未获取外部接口的 IP 地址，该怎么做？ 16

进行初始设置之前的默认配置 17

进行初始设置之后的配置 18

配置基本信息 20

配置设备 20

配置安全策略 22

部署更改 23

重启检测引擎的配置更改	24
查看接口状态和管理状态	25
查看系统任务状态	26
使用 CLI 控制台监控和测试配置	27
搭配使用 Firepower 设备管理器和 REST API	28

第 2 章**Firepower 威胁防御使用案例 29**

如何在 Firepower 设备管理器中配置设备	29
如何深入了解您的网络流量	34
如何阻止威胁	41
如何阻止恶意软件	47
如何实施可接受使用策略（URL 过滤）	50
如何控制应用使用情况	54
如何添加子网	57
如何被动监控网络上的流量	62
更多示例	67

第 3 章**为系统授权许可 69**

Firepower 系统的智能许可	69
思科智能软件管理器	69
与许可证颁发机构的定期通信	70
智能许可证类型	70
可选许可证过期或被禁用的影响	71
管理智能许可证	72
注册设备	73
启用或禁用可选许可证	74
与思科智能软件管理器同步	74
注销设备	75

第 I 部分：**系统监控 77**

第 4 章**监控设备 79**

- 启用日志记录以获取流量统计信息 79
 - 事件类型 79
 - 可配置的连接日志记录 80
 - 自动连接日志记录 81
 - 连接日志记录的提示 81
 - 将事件发送至外部系统日志服务器 81
- 监控流量和系统控制面板 82
- 使用命令行监控更多统计信息 84
- 查看事件 85
 - 配置自定义视图 86
 - 过滤事件 87
 - 事件字段说明 88

第 5 章**思科 ISA 3000 的报警 97**

- 关于报警 97
 - 报警输入接口 97
 - 报警输出接口 98
 - 系统日志报警 98
 - SNMP 陷阱报警 99
- 报警默认值 99
- 为 ISA 3000 配置报警 100
 - 配置报警输入触点 100
 - 配置电源报警 102
 - 配置温度报警 103
- 监控报警 105
 - 监控报警状态 105
 - 监控报警系统日志消息 105
 - 关闭外部报警 106

第 11 部分：	可重用对象	107
----------	--------------	------------

第 6 章	对象	109
	对象类型	109
	管理对象	111
	配置网络对象和组	112
	配置端口对象和组	113
	配置安全区	114
	配置应用过滤器对象	115
	配置 URL 对象和组	117
	配置地理位置对象	118
	配置系统日志服务器	119

第 7 章	证书	121
	关于证书	121
	公钥加密	122
	功能使用的证书类型	122
	示例：使用 OpenSSL 生成内部证书	123
	配置证书	124
	上传内部和内部 CA 证书	124
	生成自签名的内部和内部 CA 证书	126
	上传受信任的 CA 证书	127

第 8 章	身份源	129
	关于身份源	129
	Active Directory (AD) 身份领域	130
	支持的目录服务器	130
	对用户数量的限制	131
	确定目录基准标识名	131
	配置 AD 身份领域	132

故障排除目录服务器连接	134
RADIUS 服务器和组	135
配置 RADIUS 服务器	135
配置 RADIUS 服务器组	136
RADIUS 服务器和组故障排除	137
身份服务引擎 (ISE)	138
ISE 的指南和限制	138
配置身份服务引擎	139
ISE/ISE-PIC 身份源故障排除	140
本地用户	141
配置本地用户	141

第 III 部分：

基本操作 143

第 9 章

高可用性（故障切换） 145

关于高可用性（故障切换）	145
关于主用/备用故障切换	145
主/辅助角色和主用/备用状态	146
启动时的主用设备确定	146
故障切换事件	146
故障切换和状态故障切换链路	147
故障切换链路	147
状态故障切换链路	148
用于故障切换和状态链路的接口	148
连接故障切换和状态故障切换接口	148
避免中断故障切换和数据链路	149
状态故障切换如何影响用户连接	150
支持的功能	150
不支持的功能	152
备用设备上允许的配置更改和操作	152
高可用性的系统要求	153

高可用性的硬件要求	153
高可用性的软件要求	153
高可用性的许可证要求	154
高可用性指南	154
配置高可用性	155
准备两台用于高可用性的设备	156
配置高可用的主要设备	157
配置高可用的辅助设备	159
配置故障切换运行状况监控条件	160
配置对等设备运行状况监控故障切换条件	161
配置接口运行状况监控故障切换条件	162
系统如何测试接口运行状况	164
配置备用 IP 地址和 MAC 地址	164
验证高可用性配置	165
管理高可用性	166
暂停或恢复高可用性	167
中断高可用性	168
切换主用和备用对等设备（强制故障切换）	169
在故障切换后保留未部署的配置更改	170
在高可用性模式下更改许可证和注册	170
编辑 HA IPsec 加密密钥或 HA 配置	171
将故障设备标记为运行状况正常	171
在高可用性设备上安装软件升级	171
升级 HA 设备时部署更改	173
更换高可用性对中的设备	173
监控高可用性	174
监控常规故障切换状态和历史记录	174
监控高可用性监控接口的状态	175
监控与高可用性相关的系统日志消息	176
在对等设备上远程执行 CLI 命令	176
高可用性故障排除（故障切换）	176

- 设备故障状态故障排除 178
- 高可用性应用同步失败故障排除 179

第 10 章

接口 183

- 关于 FTD 接口 183
 - 接口模式 184
 - 管理/诊断接口 184
 - 配置单独管理网络的建议 185
 - 单独的管理网络的管理/诊断接口配置的限制性 185
 - 安全区域 185
 - IPv6 编址 186
 - Auto-MDI/MDIX 功能 186
- 接口的准则与限制 186
 - 接口配置的限制性 186
 - 各设备型号的最大 VLAN 子接口数量 187
- 配置物理接口 188
- 配置桥接组 191
- 配置 VLAN 子接口和 802.1Q 中继 195
- 配置被动接口 199
 - 为什么使用被动接口? 199
 - 被动接口的限制 199
 - 为硬件 Firepower 威胁设备被动接口配置交换机 200
 - 为 Firepower 威胁防御虚拟被动接口配置 VLAN 201
 - 将物理接口配置为被动模式 201
- 配置高级接口选项 202
 - 关于 MAC 地址 202
 - 关于 MTU 203
 - 路径 MTU 发现 203
 - MTU 和分段 203
 - MTU 和巨帧 203
 - 配置高级选项 203

添加接口到虚拟 Firepower 威胁防御	206
监控接口	207
接口示例	208

第 11 章

路由	209
路由概述	209
路由类型	209
路由表和路由选择	210
路由表的填充方式	210
如何制定转发决策	212
管理流量的路由表	212
等价多路径 (ECMP) 路由	213
静态路由	213
关于静态路由和默认路由	213
默认路由	214
静态路由	214
静态路由指南	214
配置静态路由	214
监控路由	216

第 IV 部分：

安全策略	217
-------------	------------

第 12 章

SSL 解密	219
关于 SSL 解密	219
为什么要实施 SSL 解密？	219
可应用于加密流量的操作	220
解密重签名	220
解密已知密钥	221
不解密	221
阻止	221
自动生成的 SSL 解密规则	222

处理不可解密流量	222
SSL 解密许可证要求	222
SSL 解密指南	222
如何实施和维护 SSL 解密策略	223
配置 SSL 解密策略	224
启用 SSL 解密策略	226
配置默认 SSL 解密操作	226
配置 SSL 解密规则	227
SSL 解密规则的源/目标标准	229
SSL 解密规则的应用标准	231
SSL 解密规则的 URL 标准	231
SSL 解密规则的用户标准	232
SSL 解密规则的高级标准	233
为已知密钥和重签解密配置证书	233
为解密重签名规则下载 CA 证书	234
示例：从网络阻止较旧的 SSL/TLS 版本	236
监控和故障排除 SSL 解密	237
监控 SSL 解密	237
处理解密重签名适用于浏览器而非应用的的 Web 站点（SSL 或证书授权锁定）	238

第 13 章

身份策略 241

身份策略概述	241
通过被动身份验证确定用户身份	242
通过主动身份验证确定用户身份	242
处理未知用户	242
如何实施身份策略	243
配置身份策略	244
配置身份策略设置	244
配置身份策略默认操作	246
配置身份规则	246
启用透明用户身份验证	249

透明身份验证的要求	250
配置 Internet Explorer 以进行透明身份验证	250
配置 Firefox 以进行透明身份验证	251
监控身份策略	252
身份策略示例	252

第 14 章**安全情报 253**

关于安全情报	253
黑名单例外	254
安全情报源类别	254
安全情报许可证要求	254
配置安全情报	255
监控安全情报	256
安全情报示例	256

第 15 章**访问控制 257**

访问控制概述	257
访问控制规则和默认操作	257
应用过滤	258
已加密和已解密流量的应用控制	258
应用过滤最佳实践	258
URL 过滤	259
按照类别和信誉过滤 URL	259
查找 URL 的类别和信誉	259
手动 URL 过滤	260
过滤 HTTPS 流量	260
比较 URL 和应用过滤	261
有效 URL 过滤的最佳实践	262
阻止网站时用户看到的内容	262
入侵、文件和恶意软件检测	263
访问控制规则顺序最佳实践	263

NAT 和访问规则	264
其他安全策略如何影响访问控制	264
访问控制许可证要求	264
访问控制策略的准则与限制	264
配置访问控制策略	266
配置默认操作	266
配置访问控制规则	267
源/目标条件	268
应用条件	270
URL 标准	271
用户条件	272
入侵策略设置	273
文件策略设置	273
日志记录设置	274
监控访问控制策略	275
在控制面板中监控访问控制统计信息	275
监控访问控制系统日志消息	276
在 CLI 中监控访问控制策略	276
访问控制示例	276

第 16 章

入侵策略 279

关于入侵和网络分析策略	279
系统定义的网络分析和入侵策略	279
入侵和预处理器规则	280
入侵规则属性	280
默认入侵变量集	281
生成器标识符	282
网络分析策略	284
系统如何使用 NAP 规则选择网络分析策略	284
关于应用入侵策略优化 NAP 处理的最佳实践	285
入侵策略的许可证要求	286

管理入侵策略	286
在访问控制规则中应用入侵策略	286
更改入侵规则操作	287
为入侵事件配置系统日志	288
监控入侵策略	289
入侵策略示例	289

第 17 章

网络地址转换 (NAT)	291
为何使用 NAT?	291
NAT 基础知识	292
NAT 术语	292
NAT 类型	292
路由模式下的 NAT	293
自动 NAT 和 手动 NAT	293
自动 NAT	294
手动 NAT	294
比较 自动 NAT 和 手动 NAT	294
NAT 规则顺序	295
NAT 接口	296
为 NAT 配置路由	297
地址与映射接口在相同的网络中	297
唯一网络中的地址	297
与实际地址相同的地址 (身份 NAT)	297
NAT 指南	297
接口指导原则	297
IPv6 NAT 指南	298
IPv6 NAT 最佳实践	298
对检测到的协议的 NAT 支持	299
其他 NAT 指南	300
配置 NAT	301
动态 NAT	302

关于动态 NAT	302
动态 NAT 不足和优势	303
配置动态自动 NAT	304
配置动态手动 NAT	305
动态 PAT	307
关于动态 PAT	307
动态 PAT 不足和优势	307
配置动态自动 PAT	308
配置动态手动 PAT	309
静态 NAT	311
关于静态 NAT	311
配置静态自动 NAT	315
配置静态手动 NAT	316
身份 NAT	319
配置身份自动 NAT	319
配置身份手动 NAT	320
Firepower 威胁防御的 NAT 规则属性	322
自动 NAT 的数据包转换属性	323
手动 NAT 的数据包转换属性 (Packet Translation Properties for Manual NAT)	324
高级 NAT 属性	325
转换 IPv6 网络	326
NAT64/46: 将 IPv6 地址转换为 IPv4 地址	326
NAT64/46 示例: 内部 IPv6 网络与外部 IPv4 互联网	327
NAT64/46 示例: 包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络	329
NAT66: 将 IPv6 地址转换为不同的 IPv6 地址	334
NAT66 示例: 网络间的静态转换	334
NAT66 示例: 简单 IPv6 接口 PAT	337
监控 NAT	340
NAT 示例	341
提供对内部 Web 服务器的访问权限 (静态自动 NAT)	341
FTP、HTTP 和 SMTP 的单个地址 (具有端口转换的静态自动 NAT)	343

- 转换因目的而异（动态手动 PAT） 349
- 转换因目的地址和端口而异（动态手动 PAT） 355
- 使用 NAT 重写 DNS 查询和响应 361
 - DNS 64 回复修改 362
 - DNS 应答修改，外部接口上的 DNS 服务器 368
 - DNS 应答修改，主机网络上的 DNS 服务器 371

第 V 部分：**虚拟专用网络 (VPN) 375**

第 18 章 **站点间 VPN 377**

- VPN 基础知识 377
 - 互联网密钥交换 (IKE) 378
 - VPN 连接应具有多高的安全性？ 378
 - 决定使用哪个加密算法 379
 - 决定使用哪些散列算法 379
 - 决定要使用的 Diffie-Hellman 模数组 380
 - VPN 拓扑 381
 - 管理站点间 VPN 381
 - 配置站点间 VPN 连接 382
 - 允许流量通过站点间 VPN 384
 - 配置全局 IKE 策略 384
 - 配置 IKEv1 策略 385
 - 配置 IKEv2 策略 387
 - 配置 IPsec 提议 388
 - 为 IKEv1 配置 IPsec 提议 389
 - 为 IKEv2 配置 IPsec 提议 390
 - 验证站点间 VPN 连接 390
 - 监控站点间 VPN 393
 - 站点间 VPN 示例 394
 - 使站点间 VPN 流量豁免 NAT 394
 - 如何在外部接口上为外部站点间 VPN 用户提供互联网访问（发夹方法） 399

第 19 章**远程接入 VPN 407**

远程接入 VPN 概述 407

各设备型号的最大并发 VPN 会话数量 407

下载 AnyConnect 客户端软件 408

用户如何安装 AnyConnect 软件 408

远程接入 VPN 的许可要求 409

远程接入 VPN 的准则与限制 409

配置远程接入 VPN 410

配置并上传客户端配置文件 411

配置远程接入 VPN 连接 412

允许流量通过远程接入 VPN 415

控制远程接入 VPN 组对资源的访问 416

验证远程接入 VPN 配置 417

监控远程接入 VPN 419

远程接入 VPN 故障排除 419

SSL 连接问题故障排除 419

AnyConnect 下载和安装问题故障排除 419

AnyConnect 连接问题故障排除 420

RA VPN 流量问题故障排除 420

远程接入 VPN 示例 421

如何在外部接口上为远程接入 VPN 用户提供互联网访问权限（发夹方法） 421

如何通过远程接入 VPN 使用外部网络上的目录服务器 428

第 VI 部分：**系统管理 445**

第 20 章**系统设置 447**

配置管理访问列表 447

配置诊断日志记录 449

严重性级别 449

配置 DHCP 服务器 450

- 配置 DNS 452
 - 配置 DNS 组 452
 - 为数据和管理接口配置 DNS 453
 - 常规 DNS 问题故障排除 454
- 配置管理接口 455
- 配置设备主机名 457
- 配置网络时间协议 (NTP) 457
- 配置URL 过滤首选项 458
- 配置云服务 458
 - 配置云管理（思科防御协调器） 458
 - 连接到思科成功网络 459
 - 禁用思科云服务注册 460
 - 启用或禁用网络分析 461

第 21 章

- 系统管理 463**
 - 安装软件更新 463
 - 更新系统数据库和源 463
 - 系统数据库和源更新概述 463
 - 更新系统数据库 464
 - 更新思科安全情报源 465
 - 升级 Firepower 威胁防御软件 466
 - 重新映像设备 468
- 备份和恢复系统 468
 - 立即备份系统 469
 - 在预定时间备份系统 469
 - 设置周期性备份计划 470
 - 恢复备份 471
 - 更换 ISA 3000 设备 472
 - 管理备份文件 472
- 审核与变更管理 472
 - 审核事件 473

查看和分析审核日志	474
过滤审核日志	475
检查部署和实体更改历史记录	476
放弃所有待处理更改	477
导出设备配置	478
管理 FDM 和 FTD 用户访问权限	478
为 FDM (HTTPS) 用户配置外部授权 (AAA)	479
管理 Firepower 设备管理器用户会话	480
启用备用 HA 设备上的外部用户 FDM 访问权限	480
为 FTD CLI 创建本地用户账户	481
重新启动系统	482
系统故障排除	483
用于测试连接的 Ping 命令	483
跟踪主机路由	485
设置 Firepower 威胁防御设备显示在跟踪路由上	486
排除 NTP 故障	488
为管理接口排除 DNS 故障	489
分析 CPU 和内存使用情况	492
查看日志	492
创建故障排除文件	494
不常见的管理任务	494
在本地和远程管理之间切换	494
更改防火墙模式	497
重置配置	499

附录 A:

高级配置	501
关于 Smart CLI 和 FlexConfig	501
Smart CLI 和 FlexConfig 的建议用法	502
Smart CLI 和 FlexConfig 对象中的 CLI 命令	502
软件升级如何影响 FlexConfig 策略	503
确定 ASA 软件版本和当前 CLI 配置	503

禁止的 CLI 命令	503
Smart CLI 模板	509
Smart CLI 和 FlexConfig 的准则与限制	509
配置 Smart CLI 对象	510
配置 FlexConfig 策略	511
配置 FlexConfig 对象	513
在 FlexConfig 对象中创建变量	514
引用 FlexConfig 变量和检索值	516
变量引用: <code>{{variable}}</code> 或 <code>{{{variable}}}</code>	516
部分 <code>{#key}</code> <code>{{/key}}</code> 和反向部分 <code>{{^key}}</code> <code>{{/key}}</code>	518
在 FlexConfig 对象中引用 Smart CLI 对象	520
配置密钥对象	521
FlexConfig 策略故障排除	522
FlexConfig 示例	523
如何启用和禁用默认全局检测	523
如何撤消 FlexConfig 更改	529
如何启用唯一流量类检测	530
如何在 ISA 3000 上启用硬件绕行	534



第 1 章

使用入门

以下主题介绍如何开始配置 Firepower 威胁防御。

- [本指南适用对象，第 1 页](#)
- [Firepower 设备管理器/FTD6.3.0 版本中的新增功能，第 2 页](#)
- [登录系统，第 5 页](#)
- [设置系统，第 8 页](#)
- [配置基本信息，第 20 页](#)

本指南适用对象

本指南介绍如何使用 Firepower 威胁防御设备自带的、基于 Web 的 Firepower 设备管理器配置界面配置 Firepower 威胁防御。

通过 Firepower 设备管理器，可以配置小型或中型网络最常用软件的基本功能。此产品专为包括一台或几台设备的网络而设计，在这种网络中，无需使用高功率多设备管理器来控制包含许多 Firepower 威胁防御设备的大型网络。

如果要管理大量设备或要使用 Firepower 威胁防御支持的更复杂的功能和配置，请使用 Firepower 管理中心（而不是集成的 Firepower 设备管理器）来配置您的设备。

您可以在以下设备上使用 Firepower 设备管理器。

表 1: Firepower 设备管理器支持的型号

设备型号	Firepower 威胁防御软件最低版本
Firepower 2110、2120、2130、2140	6.2.1
Firepower 威胁防御虚拟 适用于 VMware	6.2.2
Firepower 威胁防御虚拟 适用于基于内核的虚拟机 (KVM) 监控程序	6.2.3
ASA 5508-X、5516-X	6.1

设备型号	Firepower 威胁防御软件最低版本
ASA 5525-X、5545-X、5555-X	6.1
ASA 5506-、5506H-X、5506W-X、5512-X、-X 注释 支持以 6.2.3 结尾的型号，此版本是允许的最新版本。 不能在這些型号上安装版本 6.3 或更高版本。	6.1
ASA 5515-X	6.1
ISA 3000（思科 3000 系列工业安全设备）	6.2.3

Firepower 设备管理器/FTD6.3.0 版本中的新增功能

发布日期：2018 年 12 月 3 日

下表列出了在使用 Firepower 设备管理器进行配置时 FTD 6.3.0 中可用的新功能：

功能	说明
高可用性配置。	您可以将两台设备配置为主用/备用高可用性对。高可用性或故障切换设置可以将两台设备相关联，这样，当主设备发生故障时，辅助设备可以接管其任务。这有助于您在设备发生故障时保持网络运行。设备必须为相同型号，具有相同数量和类型的接口，且必须运行相同的软件版本。您可以从 设备 页面配置高可用性。
针对被动用户身份获取的支持。	可以配置身份策略，查看被动身份验证。被动身份验证在收集用户身份信息时不提示用户输入用户名和密码。系统将从您指定的身份源（可以是思科身份服务引擎 (ISE) /思科身份服务引擎被动身份连接器 (ISE PIC)）获取映射，或从远程接入 VPN 用户获取登录。 更改包括支持 策略 > 身份 中的被动身份验证规则和 对象 > 身份源 中的 ISE 配置。
针对远程接入 VPN 和用户身份的本地用户支持。	您现在可以直接通过 Firepower 设备管理器创建用户。然后可以使用这些本地用户账户对远程接入 VPN 的连接进行身份验证。可以使用本地用户数据库作为主要或回退身份验证源。此外，还可以在身份策略中配置被动身份验证规则，以便将本地用户名反映在控制面板中，并在策略中使用这些用户名匹配流量。 添加了 对象 > 用户 页面，更新了远程接入 VPN 向导，在向导中添加了回退选项。

功能	说明
更改了访问控制策略中 VPN 流量处理的默认操作 (sysopt connection permit-vpn)。	访问控制策略中 VPN 流量的默认处理操作已更改。从 6.3 版开始，默认操作为所有 VPN 流量均由访问控制策略处理。这样一来，您便可以对 VPN 流量应用 URL 过滤、入侵防护和文件策略等高级检测。您必须配置访问控制规则允许 VPN 流量通过。或者，您可以使用 FlexConfig 配置 sysopt connection permit-vpn 命令，指示系统允许 VPN 终止流量绕过访问控制策略（和任何高级检测）。
针对基于 FQDN 的网络对象的支持以及针对 DNS 查询的数据接口支持。	<p>您现在可以创建通过完全限定域名 (FQDN) 而非静态 IP 地址指定主机的网络对象（和组）。系统会定期查找 FQDN 到 IP 地址映射，寻找访问控制规则中使用的任何 FQDN 对象。只能在访问控制规则中使用这些对象。</p> <p>对象页面添加了 DNS 组对象，更改了系统设置 > DNS 服务器页面，允许组分配到数据接口，并允许访问控制规则支持 FQDN 网络对象选择。此外，管理接口的 DNS 配置现在使用 DNS 组，而不是 DNS 服务器地址列表。</p>
针对 TCP 系统日志的支持，以及通过管理接口发送诊断系统日志消息的功能。	<p>在以前的版本中，诊断系统日志消息（相对于连接和入侵消息）始终使用数据接口。您现在可以配置系统日志，以便所有消息都使用管理接口。最终的源 IP 地址取决于是否使用数据接口作为管理接口网关，其中 IP 地址来自数据接口。您还可以配置系统日志使用 TCP 而不是 UDP 作为协议。</p> <p>从对象 > 系统日志服务器更改了系统日志服务器的“添加/编辑”对话框。</p>
对 Firepower 设备管理器用户使用 RADIUS 的外部身份验证和授权。	<p>您可以使用外部 RADIUS 服务器对登录到 Firepower 设备管理器的用户进行身份验证和授权。您可以为外部用户提供管理、读写或只读权限。Firepower 设备管理器可以支持 5 个同时登录；第六个会话会自动注销时间最早的会话。您可以强制结束 Firepower 设备管理器用户会话，如有必要。</p> <p>在对象 > 身份源页面添加了用于配置对象的 RADIUS 服务器和 RADIUS 服务器组对象。为设备 > 系统设置 > 管理访问添加了 AAA 配置选项卡，以便可以使用服务器组。此外，监控 > 会话页面将列出活动用户，并允许管理用户终止会话。</p>
待处理更改视图和部署改进。	部署窗口已更改，能够更清晰直观地展示即将部署的待处理更改。此外，您现在可以选择放弃更改、将更改复制到剪贴板，并以 YAML 格式的文件下载更改。您还可以为部署作业命名，在审核日志中查找这类作业更方便。
审核日志。	您可以查看记录部署、系统任务、配置更改以及管理用户登录和注销等事件的审核日志。添加了设备 > 设备管理 > 审核日志页面。

功能	说明
导出配置的功能。	您可以下载设备配置副本，以便在本地备案。但是，您不能将此配置导入设备。此功能并不取代备份/恢复。添加了 设备 > 设备管理 > 下载配置 页面。
针对未知 URL 的 URL 过滤改进功能。	如果您在访问控制规则中执行基于类别的 URL 过滤，用户可能会访问 URL 数据库中未定义其类别和信誉的 URL。以前，您需要从思科综合安全情报 (CSI) 手动启用相应选项，查找这类 URL 的类别和信誉。现在，此选项已默认启用。此外，现在可以设置查询结果的生存时间 (TTL)，以便系统可以刷新每个未知 URL 的类别/信誉。更新了 设备 > 系统设置 > URL 过滤 首选项页面。
默认情况下启用安全情报日志记录。	6.2.3 版本引入了安全情报策略，默认情况下日志记录处于禁用状态。从 6.3.0 版本开始，日志记录在默认情况下处于启用状态。如果您是从 6.2.3 版本进行升级，则会保留您的日志记录设置，可能是启用或禁用。如果您想要查看策略实施结果，则可以启用日志记录。
被动模式接口	<p>您可以将接口配置为被动模式。在被动模式下工作时，接口仅监控交换机自身（针对硬件设备）或混合 VLAN（针对 Firepower 威胁防御虚拟）配置的监控会话中来自源端口的流量。</p> <p>您可以使用被动模式评估 Firepower 威胁防御虚拟 被部署为活动防火墙时会如何表现。如果您需要 IDS（入侵检测系统）服务，还可以将被动接口用于想要了解威胁、但不希望设备主动阻止威胁的生产网络。编辑物理接口和创建安全区域时，您可以选择被动模式。</p>
适用于 OSPF 的 Smart CLI 增强功能和针对 BGP 的支持。	增强了 Smart CLI OSPF 配置，添加了适用于标准和扩展 ACL 的新 Smart CLI 对象类型，路由映射、AS 路径对象、IPv4 和 IPv6 前缀列表、策略列表以及标准和扩展社区列表。此外，您现在可以使用 Smart CLI 配置 BGP 路由。可以在 设备 > 高级配置 页面找到这些功能。
适用于 ISA 3000 设备的增强功能。	您现在可以为 ISA 3000 配置以下功能：报警、硬件绕行以及使用 SD 卡备份和恢复。使用 FlexConfig 配置报警和硬件绕行。对于 SD 卡，我们更新了 Firepower 设备管理器中的备份/恢复页面。
自 FTD 6.3 起，删除了对 ASA 5506-X、5506w-x、5506h-x 以及 5512-X 的支持。	不能在 ASA 5506-X、5506w-x、5506h-x 和 5512-X 上安装 Firepower 威胁防御 6.3 或后续版本。这些平台的最终支持 FTD 版本是 6.2.3。

功能	说明
FTD REST API version 2 (v2)。	软件版本 6.3 的 FTD REST API 已增加到第 2 版。必须将 API URL 中的第 1 版替换为第 2 版。第 2 版 API 包括许多涵盖软件版本 6.3 添加的所有功能的新资源。请重新评估所有现有的调用，因为正在使用的资源型号可能已发生更改。要打开 API Explorer（您可以在其中查看资源），登录后请将 Firepower 设备管理器 URL 的末尾改为 <code>/#/api-explorer</code> 。
用于向思科提供产品使用情况信息的网络分析。	您可以启用网络分析，根据页面点击量向思科提供匿名产品使用情况信息。此信息可帮助思科确定功能使用模式，帮助思科改进产品。所有使用情况数据均为匿名数据，且不会传输敏感数据。默认启用网络分析。 在 设备 > 系统设置 > 云服务 页面添加了网络分析。
安装漏洞数据库 (VDB) 更新不会再重新启动 Snort。	安装 VDB 更新时，安装过程本身不再重新启动 Snort。但是，下一步配置部署期间仍会重新启动 Snort。
部署入侵规则 (SRU) 数据库更新不再重新启动 Snort。	安装入侵规则 (SRU) 更新后，您必须部署配置以激活新的规则。部署 SRU 更新不会再导致重新启动 Snort。

登录系统

有两个 Firepower 威胁防御设备接口：

Firepower 设备管理器 Web 界面

Firepower 设备管理器在网络浏览器中运行的 Firepower 设备管理器。使用该界面可配置、管理和监控系统。

命令行界面 (CLI、控制台)

可以使用 CLI 进行故障排除。另外，也可以使用它来代替 Firepower 设备管理器进行初始设置。

以下主题介绍如何登录这些界面和管理您的用户账户。

用户角色决定用户的访问及操作权限

用户名分配了角色，而角色决定用户能够在 Firepower 设备管理器中查看哪些内容，或执行哪些操作。本地定义的 **admin** 用户拥有所有权限，但如果使用不同的账户登录，享有的权限可能会减少。

Firepower 设备管理器窗口的右上角将显示您的用户名和权限级别。

admin
Administrator 

权限：

- **管理员** - 可以查看和使用所有功能。
- **读写用户** - 可以执行只读用户可以执行的任何操作，还可以编辑和部署配置。唯一的限制是无法执行关键系统操作，包括安装升级、创建和恢复备份、查看审核日志以及中止其他 Firepower 设备管理器用户的会话。
- **只读用户** - 可以查看控制面板和配置，但不能进行任何更改。如果尝试进行更改，错误消息会解释由于缺乏权限出错。

这些权限与 CLI 用户可享受的权限不相关。

登录 Firepower 设备管理器

使用 Firepower 设备管理器可配置、管理和监控系统。配置功能可通过浏览器实现，但无法通过命令行界面 (CLI) 执行，即：必须使用 Web 界面实施安全策略。

使用 Firefox、Chrome、Safari、Edge 或 Internet Explorer 的当前版本。



注释 如果输入错误的密码且连续 3 次尝试登录失败，账户将锁定 5 分钟。必须待锁定时间结束后方可尝试重新登录。

开始之前

最初，您只能使用 **admin** 用户名登录 Firepower 设备管理器。但是，您可以稍后为外部 AAA 服务器中定义的其他用户配置授权，如[管理 FDM 和 FTD 用户访问权限](#)，第 478 页中所述。

过程

步骤 1 使用浏览器打开系统主页，例如 <https://ftd.example.com>。

您可以使用以下地址中的任何一个。如果已配置了 IPv4 或 IPv6 地址或 DNS 名称，可以使用。

- **管理地址**。默认情况下，这在管理/诊断接口上为 192.168.45.45。
- **您为 HTTPS 访问打开的数据接口的地址**。默认情况下（在硬件平台上），“inside”接口允许 HTTPS 访问，因此可以连接到默认的内部地址 192.168.1.1。在内部接口为桥接组的设备型号上，可以通过任何桥接组成员接口连接到此地址。

提示 如果浏览器未配置为识别服务器证书，系统会显示一条有关证书不受信任的警告。将证书作为一种例外接受，或者将证书放到受信任的根证书存储库中。

步骤 2 输入为设备定义的用户名和密码，然后点击**登录**。

您可以使用“**admin**”用户名，这是预定义的用户。默认管理员密码为 Admin123。

如果会话连续 30 分钟处于非活动状态，就会过期，系统将提示您重新登录。从页面右上角的用户图标下拉菜单中选择**注销**。



登录命令行界面 (CLI)

使用命令行界面 (CLI) 可设置系统以及对系统进行基本的故障排除。无法通过 CLI 会话配置策略。要登录到 CLI，请执行以下一项操作：

- 使用设备随附的控制台电缆将您的 PC 连接到使用终端仿真器的控制台，终端仿真器的设置为 9600 波特、8 个数据位、无奇偶校验、1 个停止位、无流量控制。有关控制台电缆的详细信息，请参阅设备的硬件指南。



注释 在 Firepower 2100 设备上，控制台端口上的 CLI 是 FXOS。可以使用 **connect ftd** 命令进入 FTD CLI。仅将 FXOS CLI 用于机箱级故障排除。使用 FTD CLI 进行基本配置、监控和正常的系统故障排除。有关 FXOS 命令的信息，请参阅 FXOS 文档。

- 对于 Firepower 威胁防御虚拟，请打开虚拟控制台。
- 使用 SSH 客户端连接到管理 IP 地址。如果您为 SSH 连接打开某个数据接口，也可以连接到该接口上的地址（请参阅[配置管理访问列表](#)，第 447 页）。默认情况下，禁用 SSH 数据接口访问。使用 **admin** 用户名（默认密码为 **Admin123**）或其他 CLI 用户账户登录。

提示

- 登录后，如需了解 CLI 中可用命令的相关信息，请输入 **help** 或 **?**。有关使用信息，请参阅 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html 中的 [思科 Firepower 威胁防御命令参考](#)。
- 您可以使用 **configure user add** 命令创建可登录 CLI 的本地用户账户。但这些用户只能登录 CLI，无法登录到 Firepower 设备管理器 Web 界面。

更改密码

密码应定期更改。以下步骤程序介绍了登录到 Firepower 设备管理器时如何更改密码。



注释 如果已登录到 CLI，可使用 **configure password** 命令更改密码。您可以使用 **configure user password username** 命令为不同的 CLI 用户更改密码。

开始之前

此步骤仅适用于本地用户。如果用户账户是在外部 AAA 服务器上定义的，必须通过该服务器更改密码。

过程

步骤 1 从菜单右上角的用户图标下拉列表中选择**配置文件**。



步骤 2 点击**密码**选项卡。

步骤 3 输入您当前的密码。

步骤 4 输入新密码，然后进行确认。

步骤 5 点击**更改**。

设置用户配置文件首选项

您可以设置用户界面的首选项并更改密码。

过程

步骤 1 从菜单右上角的用户图标下拉列表中选择**配置文件**。



步骤 2 在**配置文件**选项卡中配置以下选项，然后点击**保存**。

- **安排任务的时区** - 选择安排备份和更新等任务要使用的时区。如果此处设置了不同的时区，将对控制面板和事件使用浏览器时区。
- **颜色主题** - 选择用户界面中要使用的颜色主题。

步骤 3 在**密码**选项卡中，可以输入新密码并点击**更改**。

设置系统

只有完成初始配置，系统才能在网络中正常运行。成功部署包括正确连接电缆和配置将设备插入网络所需的地址，以及将设备连接到互联网或其他上游路由器。以下程序介绍了相关过程。

开始之前

在开始初始设置之前，设备中包括了一些默认设置。有关详细信息，请参阅[进行初始设置之前的默认配置](#)，第 17 页。

过程

步骤 1 [连接接口](#)，第 9 页

步骤 2 [完成初始配置](#)，第 14 页

有关生成的配置的信息，请参阅[进行初始设置之后的配置](#)，第 18 页。

连接接口

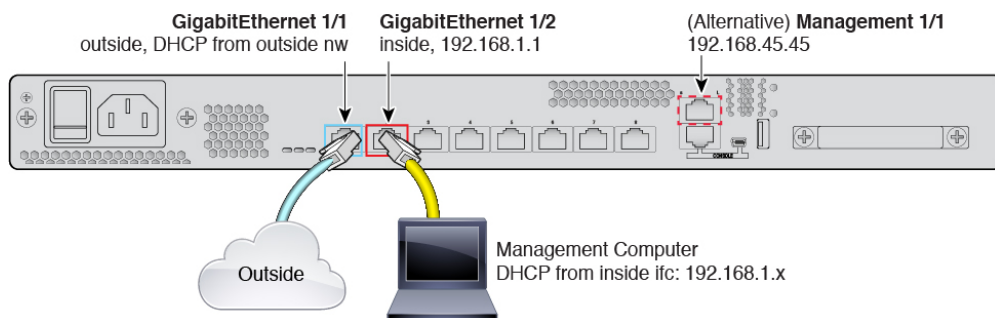
默认配置假定某些接口用于内部和外部网络。如果基于上述预期将网线连接至接口，初始配置将变得更易于完成。

硬件型号的默认配置旨在让您将工作站直接连接到内部接口。对于内部接口为桥接组的设备型号，您可以连接到任意成员接口。或者，您也可以直接将工作站连接到管理端口。通过 DHCP 在正确的网络上获取地址。接口位于不同的网络上，因此不要尝试将任何内部接口和管理端口连接到同一网络。

不要将任何内部接口或管理接口连接到具有活动 DHCP 服务器的网络。这将与已在内部端口和管理端口上运行的 DHCP 服务器冲突。如果要使用其他 DHCP 网络服务器，只需将工作站直接连接到管理端口，完成初始配置，然后禁用不需要的 DHCP 服务器。然后，您就可以将设备连接到网络。

以下主题介绍了在使用内部接口配置设备时，如何为该拓扑进行系统布线。

ASA 5508-X 和 5516-X 的布线

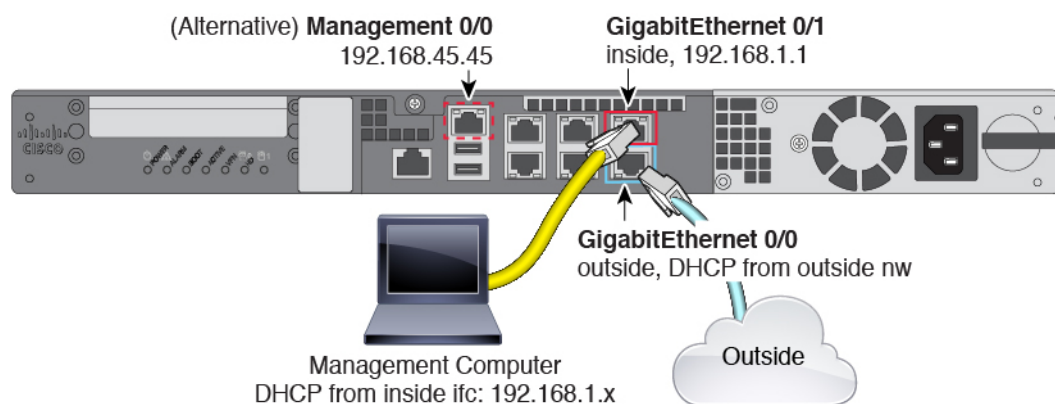


- 将 GigabitEthernet 1/1 连接到 ISP/WAN 调制解调器或其他外部设备。默认情况下，使用 DHCP 获取 IP 地址，但可以在初始配置期间设置静态地址。
- 将 GigabitEthernet 1/2 连接到您的工作站，即您将用来配置设备的工作站。将工作站配置为通过 DHCP 来获取 IP 地址。工作站将获得 192.168.1.0/24 网络中的地址。



注释 连接管理工作站还有几种其他选择。您也可以直接将其连接到管理端口。工作站将通过 DHCP 获得 192.168.45.0/24 网络中的地址。另一个方法是将工作站连接到交换机，并将该交换机连接到 GigabitEthernet1/2。不过，必须确保该交换机的网络中没有其他设备运行 DHCP 服务器，否则就会与内部接口 192.168.1.1 上运行的 DHCP 服务器冲突。

ASA 5515-X、5525-X、5545-X 和 5555-X 的布线

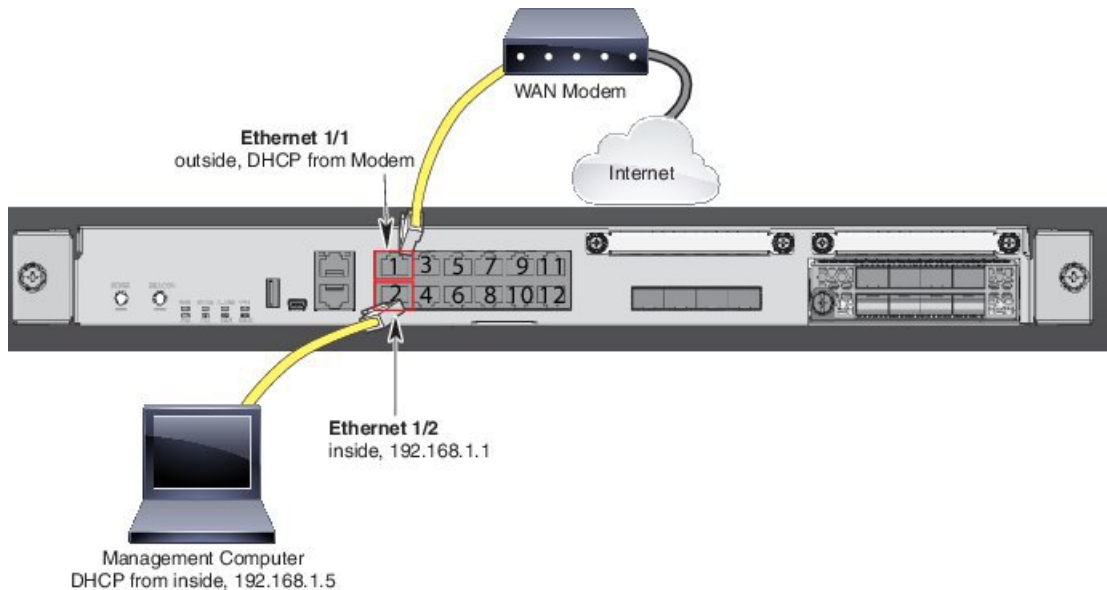


- 将 GigabitEthernet 0/0 连接到 ISP/WAN 调制解调器或其他外部设备。默认情况下，使用 DHCP 获取 IP 地址，但可以在初始配置期间设置静态地址。
- 将 GigabitEthernet 0/1 连接到准备用于配置设备的工作站。将工作站配置为通过 DHCP 来获取 IP 地址。工作站将获得 192.168.1.0/24 网络中的地址。



注释 连接管理工作站还有几种其他选择。您也可以直接将其连接到管理端口。工作站将通过 DHCP 获得 192.168.45.0/24 网络中的地址。另一个选择是仍将工作站连接到一台交换机，并将该交换机连接到 GigabitEthernet0/1。不过，必须确保该交换机的网络中没有其他设备运行 DHCP 服务器，否则就会与内部接口 192.168.1.1 上运行的 DHCP 服务器冲突。

Firepower 2100 的布线



- 将以太网 1/1 连接到 ISP/WAN 调制解调器或其他外部设备。默认情况下，使用 DHCP 获取 IP 地址，但可以在初始配置期间设置静态地址。
- 将以太网 1/2 连接到您将用来配置设备的那个工作站。将工作站配置为通过 DHCP 来获取 IP 地址。工作站将获得 192.168.1.0/24 网络中的地址。



注释 连接管理工作站还有几种其他选择。您也可以直接将其连接到管理端口。工作站将通过 DHCP 获得 192.168.45.0/24 网络中的地址。另一个方法是将工作站连接到交换机，并将该交换机连接到以太网 1/2。但是，您必须确保交换机的网络上没有其他设备正在运行 DHCP 服务器，否则它会与在以太网 1/2 192.168.1.1 上运行的设备冲突。

Firepower 威胁防御虚拟的虚拟布线

要安装虚拟 Firepower 威胁防御，请前往 <http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/products-installation-guides-list.html>，参阅用于您的虚拟平台的《思科虚拟 Firepower 威胁防御快速入门指南》。以下虚拟平台支持 Firepower 设备管理器：VMware、KVM。

虚拟 Firepower 威胁防御默认配置将管理接口和内部接口置于同一子网上。您的管理接口必须具有互联网连接，才能使用智能许可并获取系统数据库的更新。

因此，默认配置的设计使您可以将 Management0/0 和 GigabitEthernet0/1（内部）两个接口都连接到虚拟交换机上的同一网络。默认管理地址使用内部 IP 地址作为网关。因此，管理接口路由通过内部接口，然后通过外部接口连通互联网。

您还可以选择将 Management0/0 连接到与用于内部接口的子网不同的子网，只要使用具有互联网接入的网络即可。确保为网络正确配置管理接口 IP 地址和网关。

请注意，管理接口 IP 配置在设备 > 系统设置 > 管理接口上定义。它与设备 > 接口 > 视图配置中列出的 Management0/0（诊断）接口的 IP 地址不同。

VMware 网络适配器和接口如何映射到 Firepower 威胁防御物理接口

您可以为 VMware Firepower 威胁防御虚拟设备配置最多 10 个接口。您必须配置至少 4 个接口。

确保 Management0-0 源网络关联到可以访问互联网的 VM 网络。这是必需的，以便系统可以与思科智能软件管理器通信并下载系统数据库更新。

安装 OVF 时分配网络。只要您配置一个接口，稍后便可以通过 VMware 客户端更改虚拟网络。然而，如果需要添加新接口，此过程更麻烦，如[添加接口到虚拟 Firepower 威胁防御](#)，第 206 页中所述。

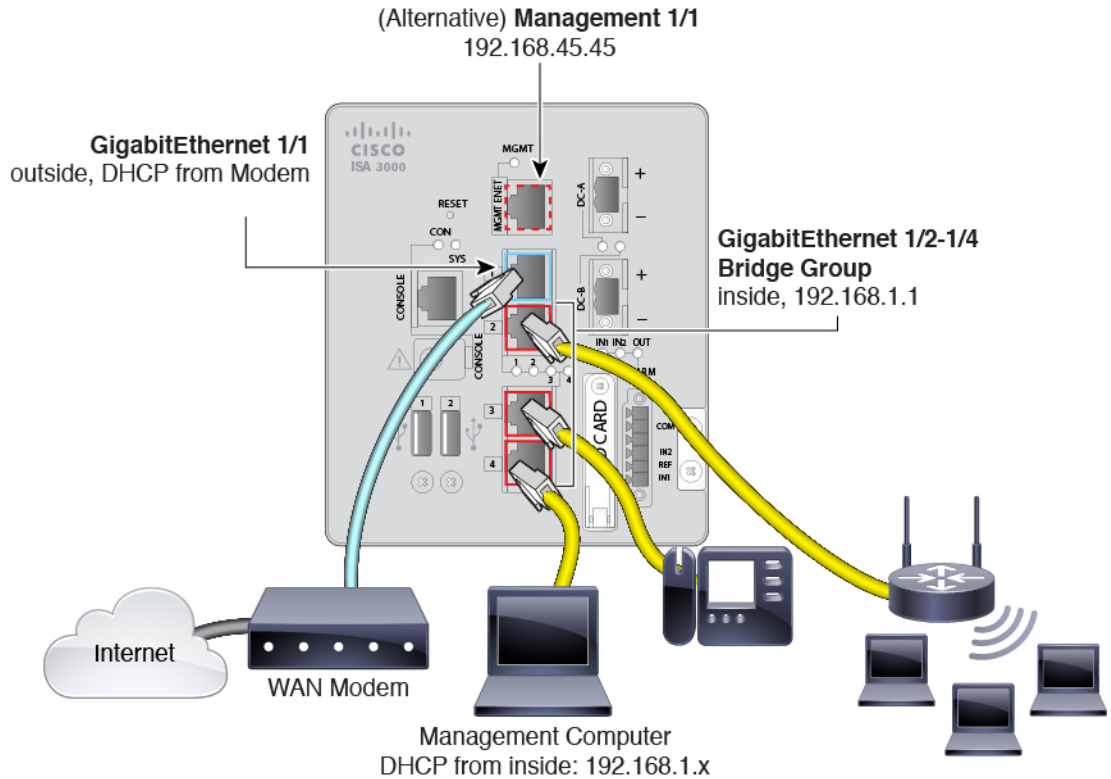
下表介绍 VMware 网络适配器和源接口如何映射到 Firepower 威胁防御虚拟物理接口名称。对其他接口命名遵循相同的模式，并将相关数字增加一。所有其他接口都是数据接口。有关将虚拟网络分配到虚拟机的详细信息，请参阅 VMware 在线帮助。

表 2: 源网络与目标网络的映射

网络适配器	源网络	目的网络（物理接口名称）	功能
网络适配器 1	Management0-0	Diagnostic0/0	管理与诊断
网络适配器 2	GigabitEthernet0-0	GigabitEthernet0/0	内部数据
网络适配器 3	GigabitEthernet0-1	GigabitEthernet0/1	外部数据
网络适配器 4	GigabitEthernet0-2	GigabitEthernet0/2	数据流量
网络适配器 5	GigabitEthernet0-3	GigabitEthernet0/3	数据流量
网络适配器 6	GigabitEthernet0-4	GigabitEthernet0/4	数据流量
网络适配器 7	GigabitEthernet0-5	GigabitEthernet0/5	数据流量
网络适配器 8	GigabitEthernet0-6	GigabitEthernet0/6	数据流量
网络适配器 9	GigabitEthernet0-7	GigabitEthernet0/7	数据流量
网络适配器 10	GigabitEthernet0-8	GigabitEthernet0/8	数据流量

ISA 3000 的布线

图 1: ISA 3000



- 将 GigabitEthernet 1/1 连接到 ISP/WAN 调制解调器或其他外部设备。默认情况下，使用 DHCP 获取 IP 地址，但可以在初始配置期间设置静态地址。
- 将 GigabitEthernet 1/2（或另一个内部桥接组成员端口）连接到您的工作站，您将用它来配置设备。将工作站配置为通过 DHCP 来获取 IP 地址。工作站将获得 192.168.1.0/24 网络中的地址。



注释 连接管理工作站还有几种其他选择。您也可以直接将其连接到管理端口。工作站将通过 DHCP 获得 192.168.45.0/24 网络中的地址。另一个方法是将工作站连接到一台交换机，并将该交换机连接到一个内部端口（例如 GigabitEthernet1/2）。但是，您必须确保交换机的网络上没有正在运行 DHCP 服务器的其他设备，否则它会与在内部桥接组 192.168.1.1 上运行的设备冲突。

- 或者，将其他终端或交换机连接到内部桥接组中的其他端口。您最好是等到完成初始设备设置后再添加终端。如果添加交换机，请确保没有其他 DHCP 服务器在这些网络上运行，否则会与在内部桥接组上运行的 DHCP 服务器冲突。

完成初始配置

在首次登录 Firepower 设备管理器时，系统会通过设备设置向导指导您完成初始系统配置。

如果您计划在高可用性配置中使用设备，请阅读[准备两台用于高可用性的设备](#)，第 156 页。

开始之前

确保将数据接口连接到网关设备（例如电缆调制解调器或路由器）。对于边缘部署，网关设备可能是面向互联网的网关。对于数据中心部署，可能是主干路由器。使用您的设备型号的默认“外部”接口（请参阅[连接接口](#)，第 9 页和[进行初始设置之前的默认配置](#)，第 17 页）。

然后，将您的工作站连接到硬件型号的“内部”接口。对于内部接口是桥接组的型号，可以连接到任意桥接组成员接口，即除外部接口之外的任意数据端口。或者，您可以连接到管理/诊断物理接口。对于 Firepower 威胁防御虚拟，只需确保连接到管理 IP 地址。

（除 Firepower 威胁防御虚拟之外，该项需要从管理 IP 地址连接到互联网。）管理/诊断物理接口不需要连接到网络。默认情况下，系统通过连接到互联网的数据接口（通常为外部接口），获取系统许可授权和数据库以及其他更新。如果想使用单独的管理网络，则可以在完成初始设置后，将管理/诊断接口连接到网络并配置单独的管理网关。

过程

步骤 1 登录 Firepower 设备管理器。

a) 假如您未在 CLI 中进行初始配置，请在 <https://ip-address>（其中地址为以下任意一个地址）打开 Firepower 设备管理器。

- 如果您已连接到内部接口，或具有默认内部桥接组的型号的一个内部桥接组数据接口：
<https://192.168.1.1>。
- （Firepower 威胁防御虚拟必需。）如果连接到管理物理接口，则地址为：
<https://192.168.45.45>。

b) 使用用户名 **admin** 和密码 **Admin123** 登录。

步骤 2 如果是首次登录系统，而且您未使用过 CLI 安装向导，系统将提示您阅读并接受“最终用户许可协议”以及更改管理员密码。

只有完成这些步骤，才能继续。

步骤 3 为外部接口和管理接口配置以下选项，然后单击 **Next**。

注意 单击 **Next** 后，您的设置将部署到设备中。该接口将命名为“outside”，并添加到“outside_zone”安全区。确保您的设置正确。

外部接口

- **Configure IPv4** - 外部接口的 Ipv4 地址。可以使用 DHCP，也可以手动输入静态 IP 地址、子网掩码和网关。另外，也可以选择 **Off**，不配置 IPv4 地址。不管是通过静态方式还是通过 DHCP，

都不要在与默认内部地址相同的子网上配置IP地址（请参阅[进行初始设置之前的默认配置](#)，第 17 页）。

- **Configure IPv6** - 外部接口的 Ipv6 地址可以使用 DHCP，也可以手动输入静态 IP 地址、前缀和网关。另外，也可以选择 **Off**，不配置 IPv6 地址。

Management Interface

- **DNS Servers** - 系统管理地址的 DNS 服务器。输入 DNS 服务器的一个或多个地址以解析名称。默认值为 OpenDNS 公共 DNS 服务器。如果您编辑字段并想要恢复默认值，请单击 **Use OpenDNS** 以重新将合适的 IP 地址加载到字段。您的 ISP 可能会要求您使用特定的 DNS 服务器。如果您在完成向导后发现无法进行 DNS 解析，请参阅[为管理接口排除 DNS 故障](#)，第 489 页。
- **防火墙主机名** - 系统管理地址的主机名。

步骤 4 配置系统时间设置，然后单击 **Next**。

- **Time Zone** - 选择系统时区。
- **NTP Time Server** - 选择使用默认 NTP 服务器，还是手动输入 NTP 服务器的地址。可以添加多个服务器来提供备份。

步骤 5 为系统配置智能许可证。

只有具有智能许可证账户，才能获取和应用系统需要的许可证。最初，可以使用为期90天的评估许可证，以后再设置智能许可。

要立即注册设备，请点击链接登录您的智能软件管理器账户，生成新的令牌，并将该令牌复制到编辑框。

如果您还不想注册设备，请选择评估模式选项。评估期长达90天。若要在以后注册设备并获取智能许可证，请点击 **设备**，然后点击**智能许可证组**中的链接。

步骤 6 点击**完成**。

下一步做什么

- 如果要使用可选许可证涵盖的功能（例如基于类别的 URL 过滤、入侵检测或恶意软件防御），请启用所需的许可证。请参阅[启用或禁用可选许可证](#)，第 74 页。
- 如果这是新系统，则具有默认内部桥接组的设备型号上的其他接口可以用作内部桥接组的成员。您可以将终端直接连接到接口。对于具有单个默认物理接口的型号，可以将其他数据接口连接到不同的网络并配置接口。对于桥接组成员接口，您可以从桥接组移除它们并配置额外的唯一网络。有关配置接口的信息，请参阅[如何添加子网](#)，第 57 页和[接口](#)，第 183 页。
- 如果通过内部接口或桥接组成员接口管理设备，并且想通过内部接口打开 CLI 会话，请打开内部接口或 SSH 连接的桥接组。请参阅[配置管理访问列表](#)，第 447 页。
- 查看使用案例以了解如何使用产品。请参阅[Firepower 威胁防御使用案例](#)，第 29 页。

如果未获取外部接口的 IP 地址，该怎么做？

默认设备配置包括一个用于内部接口的静态 IPv4 地址。此时无法通过初始设备设置向导更改该地址，但随后可以进行更改。

默认的内部 IP 地址可能与连接到设备的其他网络冲突。如果在外部接口上使用 DHCP，从互联网服务提供商 (ISP) 处获取地址，尤其如此。有些 ISP 使用与内部网络相同的子网作为地址池。由于无法在同一个子网上使用两个带有地址的数据接口，因此无法在外部接口上配置来自 ISP 的冲突地址。

如果内部静态 IP 地址与外部接口上 DHCP 提供的地址存在冲突，则连接图应将外部接口显示为管理 UP，但没有 IPv4 地址。


在这种情况下，设置向导将会成功完成，并且系统将配置所有默认 NAT、访问以及其他策略和设置。只需按照下列程序消除冲突即可。

开始之前

验证 ISP 连接是否正常。尽管子网冲突会阻碍您获取外部接口上的地址，但如果根本没有连接 ISP，也将无法获取地址。

过程

步骤 1 点击设备，然后点击接口摘要中的链接。

步骤 2 将鼠标悬停在内部接口中的操作列中，然后点击编辑图标 ()。

步骤 3 在 IPv4 地址选项卡中，输入唯一子网上的静态地址，例如 192.168.2.1/24 或 192.168.46.1/24。请注意，默认管理地址是 192.168.45.45/24，因此不使用该子网。

如果已有 DHCP 服务器在内部网络上运行，那么您还可以选择使用 DHCP。但是，首先必须在为此接口定义 DHCP 服务器组中点击删除，从接口中删除 DHCP 服务器。

步骤 4 在为此接口定义 DHCP 服务器区域中，点击编辑并将 DHCP 池更改为新子网上的某个范围（例如 192.168.2.5-192.168.2.254）。

步骤 5 点击确定，保存接口更改。

步骤 6 点击菜单中的部署按钮以部署更改。



步骤 7 点击立即部署。

部署完成后，连接图应显示外部接口此时已有一个 IP 地址。使用内部网络中的客户端验证是否已连接到互联网或其他上游网络。

进行初始设置之前的默认配置

在使用本地管理器（Firepower 设备管理器）对 Firepower 威胁防御设备进行初始配置之前，设备包括以下默认配置。

对于许多型号，此配置假定您通过内部接口打开 Firepower 设备管理器，通常是计算机直接插入接口，并使用内部接口上定义的 DHCP 服务器为计算机提供 IP 地址。或者，也可以将计算机插入管理/诊断物理接口，并通过 DHCP 获取地址。但是，某些型号具有不同的默认配置和管理要求。有关详细信息，请参阅下表。

默认配置设置

设置	默认	是否可在初始配置期间更改？
Admin 用户的密码。	Admin123	是。必须更改默认密码。
管理 IP 地址。	192.168.45.45	编号
管理网关。	设备上的数据接口。通常外部接口会成为通往互联网的路由。此网关仅适用于关联设备流量。 Firepower 威胁防御虚拟：192.168.45.1	编号
管理接口上的 DHCP 服务器。	启用，使用地址池 192.168.45.46 - 192.168.45.254。 Firepower 威胁防御虚拟：未启用 DHCP 服务器。	否。
管理接口的 DNS 服务器。	OpenDNS 公共 DNS 服务器，208.67.220.220 和 208.67.222.222。	是
内部接口 IP 地址。	192.168.1.1/24 Firepower 威胁防御虚拟：192.168.45.1/24	否。
内部客户端的 DHCP 服务器。	在内部接口上运行，地址池为 192.168.1.5 - 192.168.1.254。 Firepower 威胁防御虚拟：内部接口上的地址池为 192.168.45.46 - 192.168.45.254。	否。
内部客户端的 DHCP 自动配置。（自动配置为客户端提供 WINS 和 DNS 服务器的地址。）	在外部接口上启用。	是的，但属于间接更改。如果为外部接口配置的是静态 IPv4 地址，则禁用 DHCP 服务器自动配置。
外部接口 IP 地址。	通过 DHCP 从互联网服务提供商 (ISP) 或上游路由器获取。	是。

各个设备型号的默认接口

在初始配置期间不能选择不同的内部接口和外部接口。若要在配置后更改接口分配，请编辑接口和 DHCP 设置。您必须从桥接组中删除一个接口，然后才能将其配置为非交换接口。

Firepower 威胁防御设备	外部接口	内部接口
ASA 5508-X ASA 5516-X	GigabitEthernet1/1	GigabitEthernet1/2
ASA 5515-X ASA 5525-X ASA 5545-X ASA 5555-X	GigabitEthernet0/0	GigabitEthernet0/1
Firepower 2100 系列	以太网接口 1/1	以太网接口 1/2
Firepower 威胁防御虚拟	GigabitEthernet0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet1/1	BVI1, 包含除外部接口以外的所有其他数据接口。

进行初始设置之后的配置

在完成安装向导后，设备配置将包括以下设置。下表显示某项特定设置是否为您明示选择的项目，或者它们是否基于您的其他选项而定义。请验证任何“默示”配置，如果它们不符合您的需求，对其进行编辑。

设置	配置	明示、默示或默认配置
Admin 用户的密码。	您输入的任何信息。	明示。
管理 IP 地址。	192.168.45.45	默认值。
管理网关。	设备上的数据接口。通常外部接口会成为通往互联网的路由。管理网关仅适用于关联设备流量。 Firepower 威胁防御虚拟：192.168.45.1	默认值。
管理接口上的 DHCP 服务器。	启用，使用地址池 192.168.45.46 - 192.168.45.254。 Firepower 威胁防御虚拟：未启用 DHCP 服务器。	默认值。
管理接口的 DNS 服务器。	您输入的任何信息。	明示。
管理主机名。	firepower 或您输入的任何信息。	明示。

设置	配置	明示、默示或默认配置
通过数据接口进行管理访问。	数据接口管理访问列表规则允许通过内部接口进行 HTTPS 访问。对于具有内部桥接组的型号，这涵盖了内部桥接组的所有成员接口。不允许 SSH 连接。允许 IPv4 和 IPv6 连接。 Firepower 威胁防御虚拟：任何数据接口均无默认管理访问规则。	默示。
系统时间。	您所选的时区和 NTP 服务器。	明示。
智能许可证。	注册的基本许可证或激活的评估期，以您的选择为准。 未启用订阅许可证。如需启用它们，请转到智能许可页面。	明示。
内部接口 IP 地址。	192.168.1.1/24 Firepower 威胁防御虚拟：192.168.45.1/24	默认值。
内部客户端的 DHCP 服务器。	在内部接口上运行，地址池为 192.168.1.5 - 192.168.1.254。 Firepower 威胁防御虚拟：内部接口上的地址池为 192.168.45.46 - 192.168.45.254。	默认值。
内部客户端的 DHCP 自动配置。（自动配置为客户端提供 WINS 和 DNS 服务器的地址。）	如果使用 DHCP 来获取外部接口 IPv4 地址，则在外部接口上启用。 如果使用静态寻址，则禁用 DHCP 自动配置。	明示，但属于间接配置。
数据接口配置。	<ul style="list-style-type: none"> ISA 3000 - 除外部接口之外的所有数据接口（如 GigabitEthernet1/2）均启用，并且作为内部桥接组的一部分。可以将终端或交换机插入这些端口，并从内部接口的 DHCP 服务器获取地址。这些接口被命名为 inside_1、inside_2，以此类推。 所有其他型号 - 外部和内部接口是唯一配置和启用的接口。所有其他数据接口均禁用。 	默认值。
外部物理接口和 IP 地址。	基于设备型号的默认外部端口。请参阅 进行初始设置之前的默认配置，第 17 页 。 通过 DHCP 获取 IP 地址，或者是输入的静态地址 (IPv4、IPv6 或两者)。	接口是默认值。 寻址为显式的。
静态路由。	如果为外部接口配置的是静态 IPv4 或 IPv6 地址，则会为 IPv4/IPv6 配置相应的静态默认路由，指向您为该地址类型定义的网关。如果选择 DHCP，则从 DHCP 服务器获取默认路由。 另外，也会为网关和“任意”地址创建网络对象，即为 IPv4 创建 0.0.0.0/0，为 IPv6 创建 ::/0。	默示。

设置	配置	明示、默示或默认配置
安全区。	<p>inside_zone, 包含内部接口。对于具有内部桥接组的型号, 该区域包含内部桥接组接口的所有成员。</p> <p>outside_zone, 包含外部接。</p> <p>(您可以编辑这些区域以添加其他接口, 也可以自己创建区域)。</p>	默示。
访问控制策略。	<p>信任从 inside_zone 到 outside_zone 之间所有流量的规则。这样则允许用户的所有流量从网络内部传至外部, 并允许这些连接返回所有流量, 无需进行检查。</p> <p>对于具有内部桥接组的型号, 第二个规则信任 inside_zone 中的接口之间的所有流量。这可在不进行检查的情况下, 允许您的内部网络上的用户之间的所有流量。</p> <p>对于任何其他流量, 默认操作是阻止。这样可防止外部发起的任何流量进入网络。</p>	默示。
NAT	<p>(没有内部桥接组的型号。) 接口动态 PAT 规则可将发往外部接口的任何 IPv4 流量的源地址转换为外部接口 IP 地址上的唯一端口。</p> <p>(具有内部桥接组的型号。) 对于内部桥接组的每个成员, 接口动态 PAT 规则可将发往外部接口的任何 IPv4 流量的源地址转换为外部接口 IP 地址上的唯一端口。这些将显示在 NAT 规则表中, 稍后您可以视需要进行编辑。</p> <p>还有一些隐藏的 PAT 规则, 允许通过内部接口进行 HTTPS 访问, 并通过管理地址的数据接口进行路由。这些不会显示在 NAT 表中, 但如果您在 CLI 中使用 show nat 命令, 就会看到它们。</p>	默示。

配置基本信息

以下主题介绍配置设备的基本方法。

配置设备

首次登录 Firepower 设备管理器时, 系统将通过安装向导来帮助您配置基本设置。完成该向导后, 请使用以下方法来配置其他功能和管理设备配置。

如果难以从视觉上区分项目, 请在用户配置文件中选择不同的配色方案。从页面右上角的用户图标下拉菜单中选择配置文件。



过程

步骤 1 点击设备访问设备摘要。

该控制面板直观地显示了设备的状态，包括所启用的接口以及关键设置（绿色）已配置或还需继续配置。有关详细信息，请参阅[查看接口状态和管理状态](#)，第 25 页。

状态图像的上方是设备型号、软件版本、VDB（系统和漏洞数据库）版本及入侵规则最后更新时间的摘要。此区域还显示高可用性状态，包括配置该功能的链接；请参阅[高可用性（故障切换）](#)，第 145 页。

图像下方是您可以配置的各种功能分组、每组的配置摘要以及管理系统配置可执行的操作。

步骤 2 点击每组中的链接可配置设置或执行操作。

下面是各组的摘要：

- **接口** - 除了管理接口外，至少应配置两个数据接口。请参阅[接口](#)，第 183 页。
- **路由** - 路由配置。必须定义默认路由。根据您的配置，也可能需要其他路由。请参阅[路由](#)，第 209 页。
- **更新** - 地理位置、入侵规则和漏洞数据库更新，以及系统软件升级。如果使用这些功能，请设置定期更新计划，以确保您拥有最新的数据库更新。另外，如需在执行定期计划更新之前下载更新，也可以访问此页面。请参阅[更新系统数据库和源](#)，第 463 页。
- **系统设置** - 此组包括多种设置。有些设置是在初始设置设备时配置的基本设置，很少更改。请参阅[系统设置](#)，第 447 页。
- **智能许可证** - 显示系统许可证的当前状态。必须安装适当的许可证，才能使用该系统。某些功能需要额外的许可证。请参阅[为系统授权许可](#)，第 69 页。
- **备份和恢复** - 备份系统配置或恢复先前的备份。请参阅[备份和恢复系统](#)，第 468 页。
- **故障排除** - 应思科技术支持中心的要求生成故障排除文件。请参阅[创建故障排除文件](#)，第 494 页。
- **站点间 VPN** - 本设备与远程设备之间的站点间虚拟专用网络 (VPN) 连接。请参阅[管理站点间 VPN](#)，第 381 页。
- **远程接入 VPN** - 允许外部客户端连接到内部网络的远程接入虚拟专用网 (VPN) 配置。请参阅[配置远程接入 VPN](#)，第 410 页。
- **高级配置** - 使用 FlexConfig 和智能 CLI 配置使用 Firepower 设备管理器无法配置的功能。请参阅[高级配置](#)，第 501 页。
- **设备管理** - 查看审核日志或导出配置副本。请参阅[审核与变更管理](#)，第 472 页。

步骤 3 点击菜单中的部署按钮以部署更改。



只有将更改部署至设备，更改才会生效。请参阅[部署更改](#)，第 23 页。

下一步做什么

在主菜单中点击[策略](#)，并为系统配置安全策略。另外，也可以点击[对象 \(Objects\)](#)配置这些策略中所需的对象。

配置安全策略

使用安全策略实施组织可接受的使用策略并保护网络免受入侵或其他威胁。

过程

步骤 1 点击策略。

“安全策略”页面显示通过系统实现连接的常规流程以及安全策略的应用顺序。

步骤 2 点击策略的名称并对其进行配置。

虽然必须始终拥有访问控制策略，但可能不需要配置每个策略类型。以下是策略摘要：

- **SSL Decryption** - 如果要检查加密连接（例如 HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。请参阅[配置 SSL 解密策略](#)，第 224 页。
- **身份** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。请参阅[配置身份策略](#)，第 244 页。
- **Security Intelligence** - 使用安全情报策略快速丢弃进出列入黑名单的 IP 地址或 URL 的连接。将已知恶意站点列入黑名单后，在访问控制策略中即可无需考虑这些站点。思科提供定期更新的已知恶意地址和 URL 源，可使安全情报黑名单实现动态更新。使用情报源，无需通过编辑策略来添加或删除黑名单中的项目。请参阅[配置安全情报](#)，第 255 页。
- **NAT**（网络地址转换）- 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。请参阅[配置 NAT](#)，第 301 页。
- **Access Control** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。请参阅[配置访问控制策略](#)，第 266 页。
- **Intrusion** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。请参阅[管理入侵策略](#)，第 286 页。

步骤 3 点击菜单中的部署按钮以部署更改。



只有将更改部署至设备，更改才会生效。请参阅[部署更改](#)，第 23 页。

部署更改

在更新策略或设置时，更改不会立即应用到设备中。更改配置的过程分为两步：

1. 进行更改。
2. 部署更改。

通过此过程，您可以执行一组相关的更改，而不必在进行“部分配置”的情况下运行设备。在大多数情况下，仅会部署您做出的更改。但是，如有必要，系统将重新应用整个配置，这可能会造成您的网络中断。此外，有些更改需要重新启动检测引擎，在重启过程中会丢弃流量。因此，当系统中断带来的影响很小时，可以考虑部署更改。

完成要进行的更改后，请按照以下程序将它们部署到设备中。



注意 如果检测引擎由于软件资源问题而处于繁忙状态，或由于某个配置要求引擎在配置部署期间重新启动而出现故障，使用 Firepower 设备管理器的 Firepower 威胁防御设备将丢弃流量。有关需要重新启动的更改的详细信息，请参阅[重启检测引擎的配置更改](#)，第 24 页。

过程

步骤 1 点击网页右上角的部署更改图标。

若有未部署的更改，系统会用圆点高亮显示。



“待处理更改”窗口显示配置的部署版本与待处理更改之间的对比信息。这些更改进行了颜色编码，表示出删除、添加或编辑的元素。有关每种颜色的解释，请参阅窗口中的说明。

如果部署要求重新启动检测引擎，则该页面包含一条消息，其中提供要求重新启动的更改的详细信息。如果此时无法接受瞬时流量丢失，请关闭该对话框，等待最佳的部署更改时机。

如果图标未高亮显示，仍可以点击图标查看上一个成功部署作业的日期和时间。窗口中还包含显示部署历史记录链接，点击此链接可访问已经过过滤仅显示部署作业的审核页面。



步骤 2 如果您对所做的更改比较满意，可以点击**立即部署**立即启动作业。

窗口将显示部署正在进行。您可以关闭窗口，或等待部署完成。如果您在部署过程中关闭窗口，作业不会停止。您可以在任务列表或审核日志中查看结果。如果将窗口保持打开状态，请点击[部署历史记录](#)链接查看结果。

或者，您现在可以执行以下操作：

- **为作业命名** - 要对部署作业命名，请点击**立即部署**按钮上的下拉箭头，然后选择**为部署作业命名**。输入一个名称，然后点击**部署**。名称将会连同作业一块显示在审核和部署历史记录中，更便于您查找作业。

例如，如果将作业命名为“DMZ Interface Configuration”，成功的部署将被命名为“Deployment Completed: DMZ Interface Configuration”。此外，在与部署作业相关的“任务已开始”和“任务已结束”事件中，作业名称将用作事件名称。

- **放弃更改** - 要放弃所有待处理更改，请依次点击**更多选项** > **全部放弃**。系统将要求您进行确认。
- **复制更改** - 要将更改列表复制到剪贴板，请依次点击**更多选项** > **复制到剪贴板**。仅当更改不超过 500 项时，才选项才可用。
- **下载更改** - 要以文件形式下载更改列表，请依次点击**更多选项** > **以文本形式下载**。系统将提示将文件保存到工作站。文件采用 YAML 格式。如果您没有专门支持 YAML 格式的编辑器，可以使用文本编辑器查看。

重启检测引擎的配置更改

在部署配置更改时，以下任意配置或操作都会重新启动检测引擎。



注意

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。另外，部署某些配置需要检测引擎重新启动，这样会中断流量检测并丢弃流量。

部署

部分更改需要重新启动检测引擎，这将导致瞬时流量丢失。以下更改需要重新启动检测引擎：

- 启用或禁用 SSL 解密策略。
- 更改一个或多个物理接口（但不是子接口）上的 MTU。
- 在访问控制规则上添加或删除文件策略。
- VDB 已更新。
- 创建或中断高可用性配置。

此外，如果 Snort 进程繁忙、总 CPU 使用率超过 60%，部署期间可能会丢弃部分数据包。可以使用 **show asp inspect-dp snort** 命令，检查 Snort 当前的 CPU 使用率。

系统数据库更新

如要将更新下载到规则数据库或 VDB，则必须部署该更新，使其处于活动状态。此部署可能会重新启动检测引擎。手动下载更新或计划更新时，可以指明下载完成后是否应自动部署更改。如果没有

将系统设置为自动部署更新，则系统将在下一次部署更改时应用更新，此时检测引擎可能会重新启动。

系统更新

安装不重新启动系统和包括二进制更改的系统更新或补丁，需要检测引擎重新启动。二进制更改可能包括对检测引擎、预处理器、漏洞数据库 (VDB) 或共享对象规则的更改。另请注意，不包括二进制更改的补丁有时需要 Snort 重新启动。

查看接口状态和管理状态

“设备摘要”包括设备的图形视图和管理地址的选定设置。要打开“设备摘要”，请点击**设备**。

此图中要素的颜色根据该要素的状态而变化。将鼠标悬停在要素的上方，有时会显示更多信息。使用此图可监控以下项目。



注释 此图的接口部分（包括接口状态信息）也会显示于**接口**页面和**监控 > 系统控制面板**中。

接口状态

将鼠标悬停在端口上方可查看其 IP 地址、启用状态和链路状态。IP 地址可静态分配，也可以使用 DHCP 获取。将鼠标悬停于网桥虚拟接口 (BVI) 的上方也会显示成员接口列表。

接口端口使用以下颜色代码：

- 绿色 - 接口已配置和启用，链路为运行状态。
- 灰色 - 接口未启用。
- 橙色/红色 - 接口已配置和启用，但链路中断。如果该接口已连接电缆，则此状态表示有错误需要更正。如果该接口未连接电缆，则此状态为预期状态。

内部、外部网络连接

图中指出了在以下条件下连接到外部（或上游）和内部网络的端口。

- 内部网络 - 仅对名为“内部”的接口显示内部网络的端口。如有其他内部网络，则不显示它们。如果未命名任何没有名为“内部”的接口为“内部”，则不会将任何端口标记为内部端口。
- 外部网络 - 仅对名为“外部”的接口显示外部网络的端口。同内部网络一样，此名称是必需的，否则不会将任何端口标记为外部端口。

管理设置状态

图中显示是否为管理地址配置了网关、DNS 服务器、NTP 服务器和智能许可，以及这些设置是否正常运行。

绿色表示该功能已配置且运行正常，灰色表示未配置或无法正常运行。例如，如果无法连接服务器，则 DNS 框显示灰色。将鼠标悬停在各个要素上可查看详细信息。

如果发现问题，请按以下步骤更正它们：

- 管理端口和网关 - 依次选择系统设置 > 管理接口。
- DNS 服务器 - 依次选择系统设置 > DNS 服务器。
- NTP 服务器 - 依次选择系统设置 > NTP。另请参阅[排除 NTP 故障](#)，第 488 页。
- 智能许可证 - 点击“智能许可证”组下的[查看配置链接](#)。

查看系统任务状态

系统任务包括无需直接参与而进行的各种操作，例如检索和应用各种数据库更新。您可以查看这些任务的列表及其状态，以确认系统任务是否成功完成。

任务列表将显示系统任务和部署作业的综合状态。审核日志位于设备 > 设备管理 > 审核日志下方，其中包含更多详细信息。例如，审核日志将任务开始和任务结束显示为单独的事件，而任务列表将这些事件合并为一个条目。此外，部署作业的审核日志条目包括有关已部署变更的详细信息。

过程

步骤 1 点击主菜单中的任务列表按钮。



此时将打开任务列表，其中显示系统任务的状态和详细信息。

步骤 2 评估任务状态。

如果发现持续性的问题，可能需要修复设备配置。例如，如果一直无法获取数据库更新，则可能是设备的管理 IP 地址无法访问互联网造成。对于任务说明中指出的某些问题，您可能需要联系思科技术支持中心 (TAC)。

针对任务列表可以执行以下操作：

- 点击成功或失败按钮，可依据这些状态过滤列表。
 - 点击任务的删除图标 (🗑️)，可将其从列表中移除。
 - 点击删除所有完成的任务可清空已结束的所有任务的列表。
-

使用 CLI 控制台监控和测试配置

FTD 设备包括一个可用于监控和故障排除的命令行界面 (CLI)。虽然可以打开 SSH 会话访问所有系统命令，但也可以在 Firepower 设备管理器中打开 CLI 控制台使用只读命令，例如各种 **show** 命令以及 **ping**、**traceroute** 和 **packet-tracer**。

从一个页面移动到另一个页面时，可以使 CLI 控制台保持打开状态，并配置和部署功能。例如，在部署新的静态路由之后，可以在 CLI 控制台中使用 **ping** 验证是否可以访问目标网络。

CLI 控制台使用基本的 FTD CLI。不能使用 CLI 控制台进入诊断 CLI、专家模式、FXOS CLI（在使用 FXOS 的型号上）。如果需要进入其他 CLI 模式，请使用 SSH。

有关命令的详细信息，请参阅思科 Firepower 威胁防御命令参考，https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html。

注：

- 尽管 CLI 控制台支持 **ping**，但不支持 **ping system** 命令。
- 系统最多可以处理 2 个并发命令。因此，如果其他用户发出命令（例如，使用 REST API），您可能需要等待其他命令完成后才能输入命令。如果此问题持续存在，请使用 SSH 会话，而非 CLI 控制台。
- 命令会根据已部署的配置来返回信息。如果在 FDM 中更改配置而不进行部署，则不会在命令输出中看到所做更改的结果。例如，如果创建一个新静态路由，但不部署该路由，则该路由不会显示在 **show route** 输出中。

过程

步骤 1 点击网页右上角的 CLI 控制台图标。







步骤 2 在出现提示时键入命令，然后按 **Enter** 键。

有些命令需要更长时间生成输出，请耐心等待。如果收到命令执行超时的消息，请重试。如果输入需要交互响应的命令（例如 **show perfstats**），也会出现超时错误。如果问题仍然存在，您可能需要使用 SSH 客户端而不是 CLI 控制台。

以下是有关如何使用该窗口的一些提示。

- 按 **Tab** 键，在键入部分命令时系统会自动补全。此外，此时按 **Tab** 键，系统还会列出命令中可用的参数。**Tab** 可列出三级关键字。三级之后，需要使用命令参考来获取更多信息。
- 按 **Ctrl+C** 可以停止命令执行。
- 要移动窗口，请点击并按住报头的任意位置，然后将窗口拖到所需位置。
- 点击展开 (☰) 或收起 (☷) 按钮放大或缩小窗口。

- 点击**取消停靠，以独立窗口显示**（）按钮，将窗口从网页分离出去，在独立的浏览器窗口中显示。要再次停靠，请点击**停靠到主窗口**（）按钮。
- 点击并拖动以突出显示文本，然后按 **Ctrl+C** 将输出复制到剪贴板。
- 点击**清除 CLI**（）按钮，清除所有输出。
- 点击**复制最后一个输出**（）按钮，将您输入的最后一个命令的输出内容复制到剪贴板上。

步骤 3 完成后，只需关闭控制台窗口即可。请勿使用 **exit** 命令。

尽管用于登录 Firepower 设备管理器的凭证可验证您对 CLI 的访问权限，但使用控制台时，实际上从来无需登录 CLI。

搭配使用 Firepower 设备管理器和 REST API

在本地管理模式下设置设备时，您可以使用 Firepower 设备管理器和 Firepower 威胁防御 REST API 配置设备。实际上，Firepower 设备管理器使用 REST API 配置设备。

但请注意，REST API 可提供除通过 Firepower 设备管理器提供的功能之外的其他功能。因此，对于任何给定的功能，您可以使用 REST API 配置通过 Firepower 设备管理器查看配置时不能显示的设置。

如果配置了在 REST API 中可用、但在 Firepower 设备管理器中不可用的功能设置，使用 Firepower 设备管理器更改全局功能（例如远程接入 VPN）时，该设置可能会被撤消。是否保留仅 API 设置可能会有所不同，并且在许多情况下，通过 FDM 编辑会保留对 FDM 中不可用设置的 API 更改。对于任何给定功能，应验证所作更改是否已保留。

一般而言，应避免对任何给定功能同时使用 Firepower 设备管理器和 REST API。相反，配置设备时，应从两者中选择一种方法，逐一配置每项功能。



第 2 章

Firepower 威胁防御使用案例

以下主题介绍了您可能希望使用 Firepower 设备管理器，通过 Firepower 威胁防御完成的一些常见任务。这些使用案例假定您已完成设备配置向导，并保留了此初始配置。即使修改了初始配置，也应该能够使用这些示例了解产品的使用方法。

- [如何在 Firepower 设备管理器中配置设备，第 29 页](#)
- [如何深入了解您的网络流量，第 34 页](#)
- [如何阻止威胁，第 41 页](#)
- [如何阻止恶意软件，第 47 页](#)
- [如何实施可接受使用策略（URL 过滤），第 50 页](#)
- [如何控制应用使用情况，第 54 页](#)
- [如何添加子网，第 57 页](#)
- [如何被动监控网络上的流量，第 62 页](#)
- [更多示例，第 67 页](#)

如何在 Firepower 设备管理器中配置设备

完成设置向导后，您的设备应该会正常工作并应部署了下列基本策略：

- （ISA 3000 除外）外部接口和内部接口。其他数据接口则未配置。
- （仅限 ISA 3000。）外部接口以及包含所有其他数据接口的内部桥接组。
- 内部和外部接口的安全区域。
- 信任所有内部到外部流量的访问规则。
- 接口 NAT 规则，用于将所有内部到外部流量转换到外部接口 IP 地址上的唯一端口。
- 在内部接口或桥接组上运行的 DHCP 服务器。

以下步骤概述了可能需要配置的其他功能。请点击页面上的帮助按钮(?)，获取有关每个步骤的详细信息。

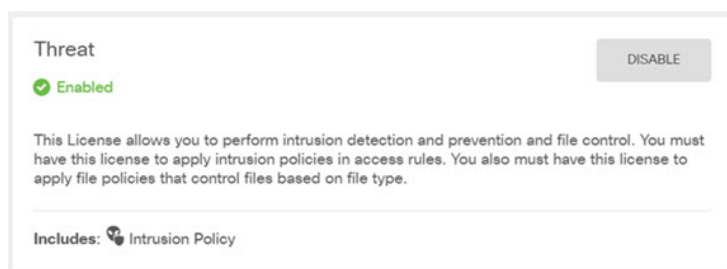
过程

步骤 1 选择 **设备**，然后点击**智能许可证组**中的**查看配置**。

对于您想要使用的可选许可证（威胁、恶意软件、URL），单击 **Enable**。如果不确定是否需要使用某个许可证，请参阅该许可证的说明。

如果尚未注册，可以从该页面执行该操作。依次点击**注册设备**，并按照说明执行操作。请在评估版许可证到期前进行注册。

例如，以下是启用的威胁许可证：



步骤 2 如果连接其他接口，请选择**设备**，然后点击**接口摘要**中的链路。

- 由于 ISA 3000 预先配置了包含所有非外部数据接口的桥接组，因此无需配置这些接口。如果要拆分该桥接组，可以对其进行编辑，删除要单独处理的接口。然后，可以将这些接口配置为承载单独的网络。

对于其他型号，可以为其他接口创建桥接组或配置单独的网络，或同时采用这两种方法。

点击每个接口的编辑图标 (🔗)，定义 IP 地址和其他设置。

以下示例将一个接口配置为“隔离区” (DMZ)，可以将可公开访问的资产（例如 Web 服务器）放在该区域中。完成后单击 **Save**。

Edit Physical Interface

Interface Name: Mode: Status:

Most features work with named interfaces only, although some require unnamed interfaces. [Learn More](#)

Description:

IPv4 Address | IPv6 Address | Advanced Options

Type:

IP Address and Subnet Mask: /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

步骤 3 如果已配置新接口，请选择 **Objects**，然后从目录中选择 **Security Zones**。

根据需要编辑或创建新区域。每个接口都必须属于一个区域，因为需要根据安全区域而不是接口来配置策略。配置接口时不能将其放在区域中，因此每当创建新接口或更改现有接口的用途之后，都必须编辑区域对象。

以下示例显示如何为 DMZ 接口创建一个新的 DMZ 区域。

Add Security Zone

Name:

Description:

Mode: Routed Passive

Interfaces:

dmz

步骤 4 如果希望内部客户端使用 DHCP 从设备中获取 IP 地址，请选择 **设备**，然后依次选择 **系统设置 > DHCP 服务器**。选择 **DHCP 服务器** 选项卡。

内部接口已配置了 DHCP 服务器，但可以编辑地址池或甚至将其删除。如果配置了其他内部接口，则在这些接口上设置 DHCP 服务器是非常典型的做法。点击 +，为每个内部接口配置服务器和地址池。

此外，还可以在配置选项卡中对为客户端提供的 WINS 和 DNS 列表进行微调。

以下示例显示如何在 inside2 接口（地址池为 192.168.4.50-192.168.4.240）上设置 DHCP 服务器。

步骤 5 选择设备，然后点击路由组中的查看配置（或创建第一个静态路由），并配置一个默认路由。

默认路由通常指向位于外部接口之外的上游或 ISP 路由器。默认的 IPv4 路由适用于 any-ipv4 (0.0.0.0/0)，而默认的 IPv6 路由适用于 any-ipv6 (:::0/0)。为所使用的每个 IP 版本创建路由。如果使用 DHCP 获取外部接口的地址，则可能已经拥有所需的默认路由。

此页面上定义的路由仅适用于数据接口，而不会影响管理接口。在系统设置 > 管理接口上设置管理网关。

以下示例显示 IPv4 的默认路由。在此示例中，isp-gateway 是用于标识 ISP 网关 IP 地址的网络对象（必须从 ISP 中获取地址）。可以通过单击 Gateway 下拉菜单底部的 Create New Network，来创建该对象。

步骤 6 选择 Policies，为网络配置安全策略。

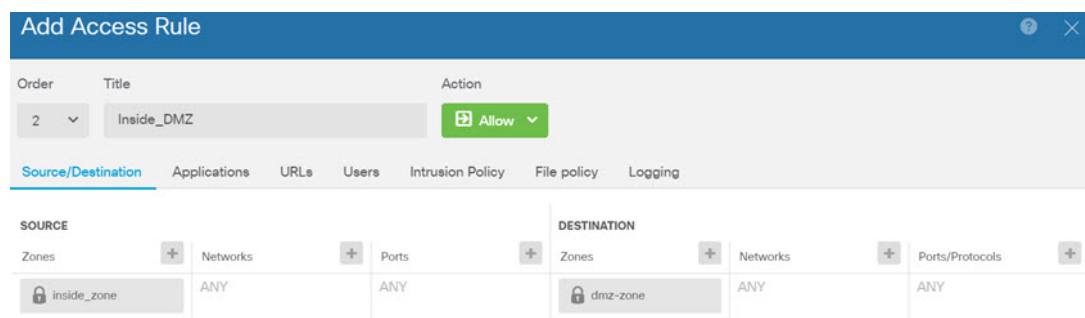
设备安装向导设置允许内部区域与外部区域之间存在流量流动，并对所有接口上流向外部接口的流量启用网络地址转换 (NAT)。即使配置了新接口，如果将其添加到内部区域对象中，访问控制规则也将自动应用于这些接口。

但是，如果有多个内部接口，则需要一条访问控制规则来允许内部区域之间的流量。如要添加其他安全区域，则需要规则来允许这些区域之间的流量。这是您需要进行的最低限度的更改。

此外，您还可配置其他策略以提供附加服务，并对 NAT 和访问规则进行精细调整，以实现组织需要的结果。您可以配置以下策略：

- **SSL Decryption** - 如果要检查加密连接（例如 HTTPS）是否存在入侵、恶意软件等，则必须解密连接。使用 SSL 解密策略确定需要解密的连接。系统检查连接后，会将其重新加密。
- **Identity** - 如果要将网络活动与各个用户相关联，或根据用户或用户组成员身份控制网络访问，请使用身份策略确定与给定源 IP 地址关联的用户。
- **Security Intelligence** - 使用安全情报策略快速丢弃进出列入黑名单的 IP 地址或 URL 的连接。将已知恶意站点列入黑名单后，在访问控制策略中即可无需考虑这些站点。思科提供定期更新的已知恶意地址和 URL 源，可使安全情报黑名单实现动态更新。使用情报源，无需通过编辑策略来添加或删除黑名单中的项目。
- **NAT**（网络地址转换）- 使用 NAT 策略将内部 IP 地址转换为外部可路由地址。
- **Access Control** - 使用访问控制策略确定网络上允许的连接。您可以按安全区域、IP 地址、协议、端口、应用、URL、用户或用户组进行过滤。您还可以使用访问控制规则来应用入侵策略和文件（恶意软件）策略。使用此策略实施 URL 过滤。
- **Intrusion** - 使用入侵策略检测已知威胁。即使使用访问控制规则应用入侵策略，也仍可以编辑入侵策略，以选择性地启用或禁用特定的入侵规则。

以下示例显示如何在访问控制策略中允许内部区域与 DMZ 区域之间的流量。在此示例中，除 **Logging** 中的 **At End of Connection** 选项外，任何其他选项卡上均未设置任何选项。



步骤 7 确认您的更改。

- a) 点击网页右上角的部署更改图标。



b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

如何深入了解您的网络流量

在完成初始设备设置后，您将获得一项访问控制策略，该策略允许所有内部流量访问互联网或其他上游网络，以及一项会阻止所有其他流量的默认操作。在创建其他访问控制规则之前，您可能会发现深入了解网络中实际发生的流量非常有益。

您可以使用 Firepower 设备管理器的监控功能来分析网络流量。Firepower 设备管理器报告可帮助您解答以下问题：

- 我的网络的用途是什么？
- 哪些用户使用的网络流量最多？
- 我的用户会访问哪些站点？
- 他们使用的是什么设备？
- 哪些访问控制规则（策略）的使用次数最多？

初始访问规则可提供一些信息帮助您深入了解流量，包括策略、目的和安全区。但要获取用户信息，您需要配置一项要求用户验证自己（身份）的身份策略。要获取网络中所使用应用的信息，您需要进行一些其他调整。

以下步骤程序介绍了如何设置 Firepower 威胁防御设备以监控流量，并概述了配置和监控策略的端到端流程。



注释

通过此步骤程序无法了解用户所访问站点的网站类别和信誉，因此在 URL 类别控制面板中看不到有用的信息。只有实施基于类别的 URL 过滤并启用 URL 许可证，才能获取类别和信誉数据。如果只想获取这些信息，可以添加一个新访问控制规则，以允许访问可接受的类别（例如金融服务），并将其设为访问控制策略的第一个规则。有关实施 URL 过滤的详细信息，请参阅[如何实施可接受使用策略（URL 过滤）](#)，第 50 页。

过程

步骤 1 要了解用户行为，您需要配置身份策略以确保可以识别与连接关联的用户。

通过启用身份策略，可以收集有关网络用户以及他们所使用资源的信息。在用户监控控制面板中可获取这些信息。另外，也可以获取事件查看器中所示的连接事件的用户信息。

在本示例中，我们将实施主动身份验证以获取用户身份。使用主动身份验证时，设备将提示用户输入用户名和密码。只有用户使用支持 HTTP 连接的 Web 浏览器时，才会对他们进行身份验证。

如果用户未通过身份验证，其仍可进行 Web 连接。这仅仅意味着，您不会获取连接的用户身份信息。如果需要，可以创建一项访问控制规则，以丢弃身份验证失败的用户流量。

- a) 在主菜单中点击**策略**，然后点击**身份**。

身份策略最初处于禁用状态。使用主动身份验证时，身份策略使用您的 Active Directory 服务器对用户进行身份验证，并将他们与其使用的工作站的 IP 地址关联。随后，系统会将该 IP 地址的流量标识为该用户的流量。

- b) 点击**启用身份策略**。

- c) 点击**创建身份规则按钮**或**+**按钮，创建规则以要求进行主动身份验证。

在本示例中，我们假设您要对每个用户都执行身份验证。

- d) 为规则输入**名称**，可以是您选择的任何内容，例如 `Require_Authentication`。

- e) 在**源/目标**选项卡上，保留默认设置，此设置应用于任何条件。

您可以根据需要将该策略限制为更具体的流量集。但是，主动身份验证仅适用于 HTTP 流量，因此非 HTTP 流量与源/目的条件匹配并不重要。有关身份策略属性的详细信息，请参阅[配置身份规则](#)，第 246 页

- f) 对于**操作**，请选择**主动身份验证**。

假设您尚未配置身份策略设置，由于存在一些未定义的设置，系统将打开“身份策略配置”对话框。


- g) 配置主动身份验证所需的强制网络门户和 SSL 解密设置。

如果身份规则要求对用户进行主动身份验证，则该用户将重定向到连接该用户所通过的界面上的强制网络门户，然后系统会提示用户进行身份验证。强制网络门户需要使用 SSL 解密规则，系统将自动生成这些规则，但您必须选择要用于 SSL 解密规则的证书。

- **服务器证书** - 选择在主动身份验证期间提供给用户的内部证书。您可以选择预定义的自签名 `DefaultInternalCertificate`，也可以点击**创建新的内部证书**并上传您的浏览器已信任的证书。

如果用户不上传其浏览器已经信任的证书，则必须接受该证书。

- **端口** - 强制网络门户端口。默认端口是 885 (TCP)。如果配置了其他端口，则该端口必须在 1025-65535 的范围内。
- **解密重签证书** - 选择内部 CA 证书，以用于使用重签名证书实施解密的规则。您可以使用预定义的 `NGFW-Default-InternalCA` 证书（默认证书），也可以使用创建或上传的证书。如果尚无证书，请点击**创建内部 CA**进行创建。（仅当您尚未启用 SSL 解密策略时，系统才会提示您提供解密重签名证书。）

如果尚未在客户端浏览器中安装证书，请点击**下载按钮**  获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅[解密重签名规则下载 CA 证书](#)，第 234 页。

示例：

“身份策略配置”对话框现在应如下所示。

- h) 点击**保存**以保存主动身份验证设置。

“主动身份验证”选项卡现在显示在“操作”设置下方。

- i) 在**主动身份验证**选项卡上，选择 **HTTP 协商**。

这样则允许浏览器和目录服务器按顺序协商最安全的身份验证协议，先是NTLM，然后是HTTP基本验证。

注释 对于 HTTP Basic、HTTP Response Page 和 NTLM 身份验证方法，通过接口的 IP 地址可将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.AD-domain-name* 进行重定向。如果想要使用 HTTP Negotiate，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。如果无法或不想更新 DNS 服务器，请选择其他某种身份验证方法。

- j) 对于 **AD 身份源**，请点击**创建新身份领域**。

如果您已创建领域服务器对象，只需选中它并跳过配置服务器的步骤。

填写以下字段，然后点击**确定**。

- **名称** - 目录领域的名称。
- **类型**- 目录服务器的类型。Active Directory 是唯一支持的类型，所以无法更改此字段。
- **目录用户名、目录密码** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

注释 系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=adminisntrator、cn=users、dc=example、dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准 DN (Base DN)** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如 dc=example,dc=com。有关查找基准 DN 的信息，请参阅[确定目录基准标识名](#)，第 131 页。
- **AD 主域** - 设备应加入的 Active Directory 完全限定域名。例如 example.com。
- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。
- **加密** - 要使用加密连接下载用户和组信息，请选择所需的方法 **STARTTLS** 或 **LDAPS**。系统默认为无，也就是说以明文形式下载用户和组信息。
 - **STARTTLS** 将会协商加密方法，并使用目录服务器支持的最强方法。使用端口 389。如果将领域用于远程接入 VPN，则不支持此选项。
 - **LDAPS** 需要基于 SSL 的 LDAP。使用端口 636。
- **受信任的 CA 证书** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

示例:

例如，下图显示了如何为 ad.example.com 服务器创建未加密的连接。主域为 example.com，目录用户名为 Administrator@ad.example.com。所有用户和组信息均位于标识名 (DN) ou=user,dc=example,dc=com 的下方。

Name	Type
AD	Active Directory (AD) ▼
Directory Username	Directory Password
Administrator@ad.example.com
<i>e.g. user@example.com</i>	
Base DN	AD Primary Domain
ou=user,dc=example,dc=com	example.com
<i>e.g. ou=user, dc=example, dc=com</i>	<i>e.g. example.com</i>

Directory Server Configuration

Hostname / IP Address	Port
ad.example.com	389
<i>e.g. ad.example.com</i>	
Encryption	Trusted CA certificate
NONE ▼	Please select a certificate ▼

- k) 对于 **AD 身份源**，请选择您刚刚创建的对象。

规则应类似于以下内容：

Order	Title	AD Identity Source	Action
1 ▼	Require_Authentication	AD ▼	Active Auth ▼

Source / Destination [Active authentication](#)

Type	ACTIVE AUTHENTICATION
HTTP Negotiate ▼	For HTTP connections only, pre-specified identity source to obtain connections, even non-HTTP, is prompted to authenticate again access. You must configure the
Fall Back as Guest <input type="checkbox"/>	Type - Select the authenticat

- l) 点击**确定**以添加规则。

如果查看窗口的右上角，可以看到**部署**图标现在带有一个圆点，表示存在未部署的更改。在用户界面进行更改还不足以获取在设备上配置的更改，还必须部署更改。因此，您可以执行一组相关更改，然后再部署它们，这样就不会出现仅在设备上配置了部分更改的情况。在此步骤程序后面，将要部署更改。



步骤 2 将 `Inside_Outside_Rule` 访问控制规则上的操作更改为 **允许**。

`Inside_Outside_Rule` 访问规则创建为信任规则。但由于不检测到受信任的流量，所以在匹配条件的流量不含应用或区域、IP 地址和端口之外的其他条件时，系统则无法了解受信任流量（例如应用）的某些特征。如果将该规则更改为允许非受信任的流量，系统会全面检测流量。

注释 （ISA 3000。）还要考虑将 `Inside_Inside_Rule` 从“信任”更改为“允许”。此规则涵盖了内部接口之间的流量。

- a) 点击策略页面上的访问控制。
- b) 将鼠标悬停在 `Inside_Outside_Rule` 行右侧的操作单元格上将显示编辑和删除图标，然后点击编辑图标 (🔗) 以打开该规则。
- c) 针对操作选择允许。

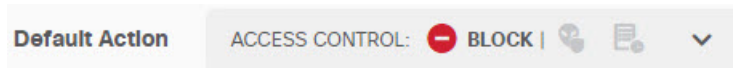
Order	Title	Action
1	Inside_Outside_Rule	Allow

- d) 点击确定以保存更改。

步骤 3 基于访问控制策略默认操作启用日志记录。

控制面板仅包含与启用连接日志记录的访问控制规则匹配的连接的信息。`Inside_Outside_Rule` 规则启用日志记录，但默认操作为禁用日志记录。因此，控制面板仅显示 `Inside_Outside_Rule` 的信息，而不反映与任何规则皆不匹配的连接。

- a) 点击“访问控制策略”页面底部默认操作的任意位置。



- b) 选择选择日志操作 > 连接开始和结束时。
- c) 点击确定。

步骤 4 设置漏洞数据库 (VDB) 的更新计划。

思科会定期发布 VDB 更新，其中包括可识别连接中所用应用的应用检测器。您应定期更新 VDB。您可以手动下载更新，也可以设置定期更新计划。以下步骤程序介绍了如何设置计划。默认情况下，VDB 更新处于禁用状态，所以您需要采取措施来获取 VDB 更新。

- a) 点击设备。
- b) 点击“更新”组中的查看配置。

Updates

[View Configuration](#) >

- c) 点击 VDB 组中的配置。

VDB 265.0

Configure
Set recurring VDB updates

UPDATE NOW

- d) 定义更新计划。

选择不会影响网络的时间和频率。另外，请注意系统在下载更新后会自动执行部署。激活新的检测器需要执行此操作。因此，也会部署您已进行和保存，但尚未部署的任何配置更改。

例如，以下计划会在每周星期日上午 12:00（使用 24 小时制表示法）更新一次 VDB。

Set recurring VDB Update

Frequency

Weekly

Days of Week

Sundays *

Time

at 00 : 00

(-07:00) America/Los_Angeles

- e) 点击保存。

步骤 5 确认您的更改。

- a) 点击网页右上角的部署更改图标。



- b) 点击立即部署按钮。

您可以等待部署完成，也可以点击确定，稍后再检查任务列表或部署历史记录。

下一步做什么

这时，监控控制面板和事件应开始显示用户和应用的相关信息。您可以评估这些信息是否存在不需要的模式，并制定新的访问规则来限制不可接受的用途。

如果要开始收集入侵和恶意软件的相关信息，您需要针对一个或多个访问规则启用入侵和文件策略。另外，您还需要对这些功能启用许可证。

如果要开始收集 URL 类别的相关信息，则必须实施 URL 过滤。

如何阻止威胁

通过将入侵策略添加到访问控制规则中，可以实施下一代入侵防御系统 (IPS) 过滤。入侵策略可分析网络流量，根据已知威胁比较流量内容。如果某个连接与您正在监控的威胁匹配，系统将丢弃该连接，从而阻止攻击。

处理所有其他流量后，才会检验网络流量中是否存在入侵。通过将入侵策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略检测流量。

您只能对允许流量的规则配置入侵策略。对于设置为信任或阻止流量的规则，系统不会执行检测。另外，如果默认操作是允许，您可以将入侵策略配置为默认操作的一部分。

思科通过 Firepower 系统提供多种入侵策略。这些策略由思科 Talos 情报小组 (Talos) 设计，其设定了入侵和预处理器规则的状态和高级设置。

除了检查允许的流量是否存在潜在入侵之外，您还可以使用安全情报策略来预先阻止所有传送到或来自已知不良 IP 地址，或传送到已知不良 URL 的流量。

过程

步骤 1 如果尚未启用威胁许可证，请启用该许可证。

必须启用威胁许可证，才能使用入侵策略和安全情报。如果您当前使用的是评估许可证，将启用该许可证的评估版本。如果已注册设备，则必须购买所需的许可证，并将其添加到您在 Cisco.com 的智能软件管理器账户。

- a) 点击设备。
- b) 点击“智能许可证”组中的查看配置。



- c) 点击威胁组中的启用。

系统则会将该许可证注册到您的账户，或激活相应的评估许可证。该组应指示许可证已启用，且按钮将改为显示“禁用”。



步骤 2 针对一个或多个访问规则选择入侵策略。

确定哪些规则包括应该扫描威胁的流量。在本示例中，我们会将入侵检测添加到 `Inside_Outside_Rule` 中。

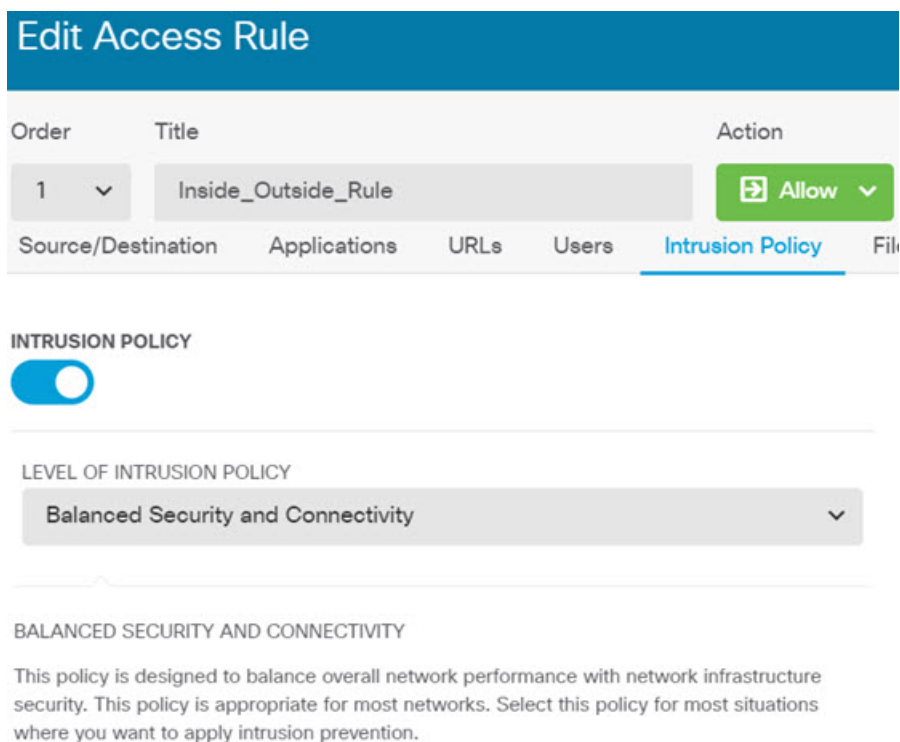
- a) 在主菜单中点击**策略**。
确保系统显示**访问控制策略**。
- b) 将鼠标悬停在 `Inside_Outside_Rule` 行右侧的**操作**单元格上将显示编辑和删除图标，然后点击编辑图标 (🔗) 以打开该规则。
- c) 如果尚未针对**操作**选择**允许**，请进行此选择。

Order	Title	Action
1	Inside_Outside_Rule	Allow

- d) 点击**入侵策略**选项卡。
- e) 点击**入侵策略**开关启用该选项，然后选择入侵策略。

策略将按安全性由低到高列出。对于大多数网络，合适的策略是**平衡安全和连接策略**。它提供良好的入侵防御，而不会过度激进，有可能会丢弃可能不想被丢弃的流量。如果您确定要丢弃很多流量，可以选择**连接优先于安全**以放宽策略。

如果您需要积极关注安全性，请尝试**安全优先于连接策略**。**最大检测策略**更加重视网络基础设施的安全性，有可能对操作造成更大的影响。



f) 点击**确定**以保存更改。

步骤 3 设置入侵规则数据库的更新计划。

思科会定期发布入侵规则数据库更新，入侵策略使用入侵规则数据库来确定是否应丢弃连接。您应定期更新规则数据库。您可以手动下载更新，也可以设置定期更新计划。以下步骤程序介绍了如何设置计划。默认情况下，数据库更新处于禁用状态，所以您需要采取措施来获取更新的规则。

- a) 点击 **设备**。
- b) 点击“更新”组中的**查看配置**。

Updates

[View Configuration](#) >

- c) 点击“规则”组中的**配置**。

Rule 2016-03-28-001-vrt

Configure
Set recurring Rule updates

UPDATE NOW



d) 定义更新计划。

选择不会影响网络的时间和频率。另外，请注意系统在下载更新后会自动执行部署。激活新规则需要执行此操作。因此，也会部署您已进行和保存，但尚未部署的任何配置更改。

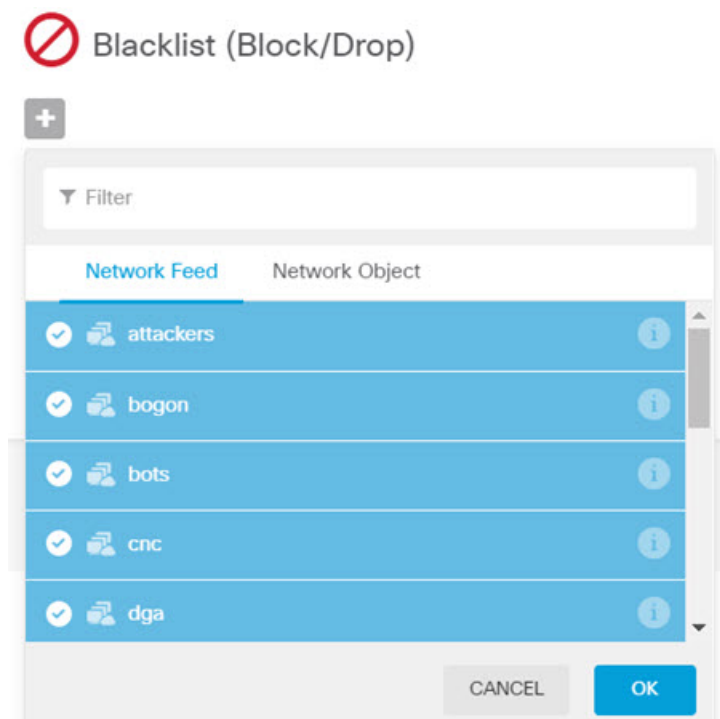
例如，以下计划会在每周星期一上午 12:00（使用 24 小时制表示法）更新一次规则数据库。

e) 点击保存。

步骤 4 配置安全情报策略预先丢弃主机和站点已知不良的连接。

通过使用安全情报阻止连接属于已知威胁的主机或站点，为系统留出执行深度数据包检测，以识别每个连接中的威胁所需的时间。安全情报可提早阻止不必要的流量，为系统留出更多的时间来处理您真正关心的流量。

- 点击**设备**，然后点击**更新组**中的**查看配置**。
- 点击安全情报源组中的**立即更新**。
- 此外，点击**配置**为源设置定期更新。默认情况下，**每小时**适合大多数网络，但如有必要，可以降低频率。
- 点击**策略**，然后点击**安全情报策略**。
- 点击**启用安全情报**，如果尚未启用该策略。
- 在**网络**选项卡上，点击**黑名单**下的 **+**，并选择**网络源**选项卡上的所有源。您可以点击源旁边的 **i** 按钮，阅读每个源的说明。



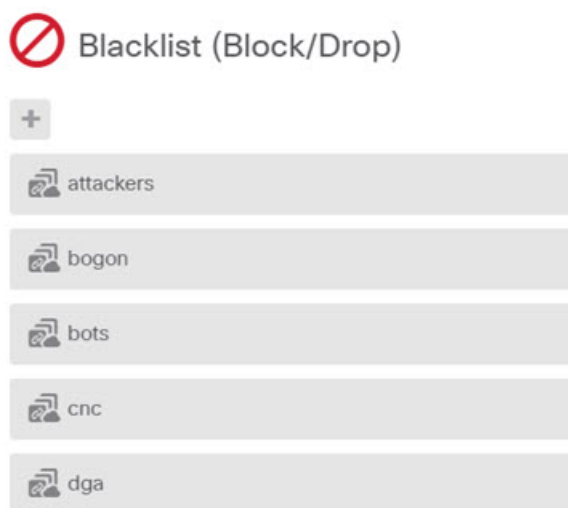
如果您看到指出尚不存在任何源的消息，请稍后重试。源下载尚未完成。如果此问题仍然存在，请确保管理 IP 地址和互联网之间存在路径。

- g) 点击**确定**添加选定的源。

如果您知道存在其他不良 IP 地址，可以依次点击+> **网络对象**，添加包含这些地址的对象。您可以点击列表底部的**创建新网络对象**立即添加这些对象。

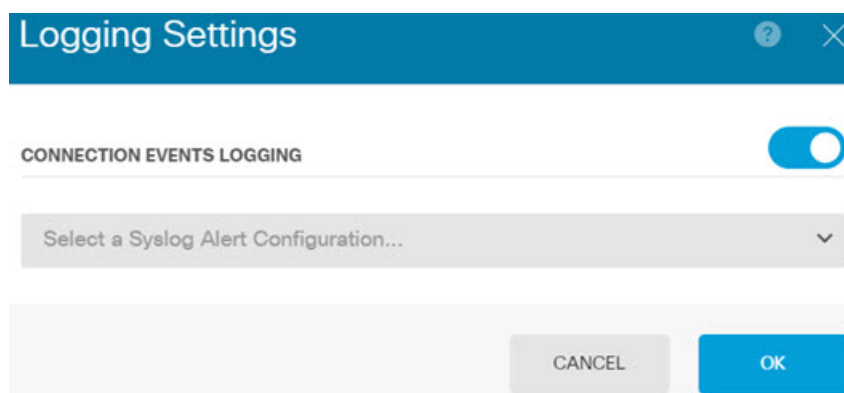
- h) 点击 **URL** 选项卡，然后依次点击**黑名单**下面的 +> **URL 源**，选择所有 URL 源。点击**确定**将其添加到黑名单。

与网络列表类似，您可以将自己的 URL 对象添加到黑名单，以阻止源中不存在的其他站点。依次点击 +> **URL 对象**。您可以通过点击列表末尾的**创建新 URL 对象**添加新对象。



- i) 点击齿轮图标，并启用**连接事件**日志记录，以便策略能够为匹配的连接生成安全情报事件。点击 **OK**，保存更改。

如果您不启用连接日志记录，您将没有数据来评估策略的表现是否达到预期。如果定义了外部系统日志服务器，现在即可选择此服务器，以便将事件同时发送到该服务器上。



- j) 根据需要，您可以在每个选项卡的**不阻止**列表中添加网络或 URL 对象，创建黑名单例外。

不阻止列表不是真正的白名单。它们是例外列表。如果例外列表中的地址或 URL 也出现在黑名单中，允许该地址或 URL 的连接传递到访问控制策略。通过这种方式，您可以阻止源，但如果您后期发现所需的地址或站点被阻止，可以使用例外列表来覆盖阻止，而不需要彻底删除源。注意，这些连接随后由访问控制和入侵策略（如果已配置）评估。因此，如果任何连接包含威胁，这些连接将在入侵检查过程中被识别和阻止。

使用“访问和 SI 规则”控制面板和事件查看器中的“安全情报”视图，判断哪些流量实际上被策略丢弃，以及您是否需要在**不阻止**列表中添加地址或 URL。

步骤 5 确认您的更改。

- a) 点击网页右上角的**部署更改**图标。



b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

如果已识别任何入侵，这时监控控制面板和事件应开始显示攻击者、目标和威胁的相关信息。您可以评估这些信息来确定，您的网络是否需要更多安全预防措施，或是否需要降低使用的入侵策略级别。

对于安全情报，您可以在“访问和 SI 规则”控制面板上查看策略使用情况。您还可以在事件查看器中查看安全情报事件。安全情报数据块不反映在入侵威胁信息中，因为流量在可检测之前已被阻止。

如何阻止恶意软件

用户不断面临着经由互联网站点或其他通信方法（例如邮件）而感染恶意软件的风险。即使受信任的网站，也可能遭受劫持，让信任该网站的用户遭受恶意软件的肆意攻击。网页可能包含来自不同来源的对象。这些对象可能包含图像、可执行文件、JavaScript、广告等等。受感染的网站通常会植入外部源中托管的对象。实际安全性意味着，逐个查看每个对象，而不只是初始请求。

使用文件策略，借助适用于 Firepower 的高级恶意软件保护（适用于 Firepower 的 AMP）检测恶意软件。另外，您还可以使用文件策略执行文件控制，以允许控制特定类型的所有文件，而不考虑文件中是否包含恶意软件。

适用于 Firepower 的 AMP 使用 AMP 云为网络流量中检测到的恶意软件检索处置。管理接口必须可连接互联网，以便访问 AMP 云并搜索恶意软件。当设备检测到符合条件的文件时，它将使用该文件的 SHA-256 散列值来查询 AMP 云中是否存在该文件的处置。可能的处置可以是**正常**、**恶意软件**或**未知**（没有明确判定）。如果无法连接 AMP 云，则处置为**未知**。

通过将文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要检测连接中的任何文件。

您只能对**允许**流量的规则配置文件策略。对于设置为**信任**或**阻止**流量的规则，系统不会执行检测。

过程

步骤 1 如果尚未启用**恶意软件**许可证，请启用该许可证。

只有启用**恶意软件**许可证，才能使用文件策略执行**恶意软件**控制。如果您当前使用的是**评估**许可证，将启用该许可证的**评估**版本。如果已注册设备，则必须购买所需的许可证，并将其添加到您在 Cisco.com 的智能软件管理器账户。

a) 点击**设备**。

- b) 点击“智能许可证”组中的**查看配置**。



- c) 点击恶意软件组中的**启用**。

系统则会将该许可证注册到您的账户，或激活相应的评估许可证。该组应指示许可证已启用，且按钮将改为显示“禁用”。



步骤 2 针对一个或多个访问规则选择文件策略。

确定哪些规则包括应该扫描恶意软件的流量。在本示例中，我们会将文件检测添加到 Inside_Outside_Rule 中。

- a) 在主菜单中点击**策略**。

确保系统显示**访问控制策略**。

- b) 将鼠标悬停在 Inside_Outside_Rule 行右侧的**操作**单元格上将显示编辑和删除图标，然后点击编辑图标 (🔗) 以打开该规则。

- c) 如果尚未针对**操作**选择**允许**，请进行此选择。

Order	Title	Action
1	Inside_Outside_Rule	Allow

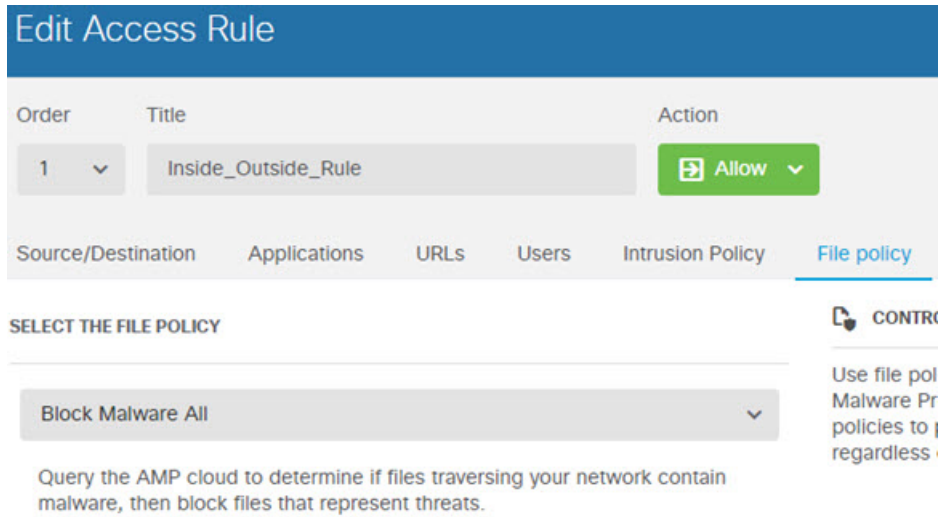
- d) 点击**文件策略**选项卡。

- e) 点击要使用的文件策略。

您的主要选择为**阻止所有恶意软件**或**全部执行云查找**，前者将丢弃被视为恶意软件的任何文件，后者将查询 AMP 云以确定文件处置，但不执行阻止。如果您想先查看文件评估的方式，请使用云查找。如果对文件的评估方式感到满意，稍后可以切换到阻止策略。

使用其他策略也可以阻止恶意软件。这些策略搭配文件控制，可阻止上传 Microsoft Office（或 Office）和 PDF 文档。也就是说，除了阻止恶意软件，这些策略还可阻止用户向其他网络发送这些类型的文件。如果它们符合您的需求，您可以选择这些策略。

对于本示例，请选择**阻止所有恶意软件**。



- f) 点击日志记录选项卡，并确认是否已选中“文件事件”下的日志文件。

默认情况下，无论何时选择文件策略，文件日志记录均已启用。只有启用文件日志记录，才能获得事件和控制面板中的文件和恶意软件信息。

FILE EVENTS

Log Files

- g) 点击**确定**以保存更改。

步骤 3 确认您的更改。

- a) 点击网页右上角的**部署更改**图标。



- b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

如果已传输任何文件或恶意软件，这时监控控制面板和事件应开始显示文件类型、文件和恶意软件的相关信息。您可以评估这些信息，以确定您的网络在文件传输方面是否需要更多安全预防措施。

如何实施可接受使用策略（URL 过滤）

您的网络可能设有可接受使用策略。可接受使用策略可区分适合您所在组织的网络活动和认为不合适的活动。这些策略通常专注于互联网使用情况，旨在保持工作效率，避免法律责任（例如，维护非敌对工作空间）以及总体控制 Web 网络流量。

您可以使用 URL 过滤来定义访问策略的可接受使用策略。您可以基于各种类别（例如赌博）过滤，这样则无需识别应阻止的每个单独的网站。对于类别匹配，您还可以指定要允许或阻止的站点的相对信誉。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止。

使用类别和信誉数据还会简化策略创建和管理。此方法可保证系统将按预期控制网络流量。最后，由于思科的威胁情报会不断更新有关新 URL 以及现有 URL 的新类别和新风险的信息，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁（如恶意软件、垃圾邮件、僵尸网络和钓鱼）的恶意站点出现和消失的速度可能比您更新和部署新策略的速度要快。

以下程序介绍了如何使用 URL 过滤实施可接受使用策略。在本例中，我们将阻止某些类别的任何信誉的站点、存在风险的社交网站和未分类站点 `badsite.example.com`。

过程

步骤 1 如果尚未执行此操作，请启用 URL 许可证。

只有启用 URL 许可证，才能使用 URL 类别和信誉信息，或查看控制面板和事件中的信息。如果您当前使用的是评估许可证，将启用该许可证的评估版本。如果已注册设备，则必须购买所需的许可证，并将其添加到您在 `Cisco.com` 的智能软件管理器账户。

- 点击设备。
- 点击“智能许可证”组中的查看配置。



- 点击 URL 许可证组中的启用。

系统则会将该许可证注册到您的账户，或激活相应的评估许可证。该组应指示许可证已启用，且按钮将改为显示“禁用”。



步骤 2 创建 URL 过滤访问控制规则。

您可能想要先查看用户访问的站点的类别，再实施阻止规则。对于这种情况，您可以创建一项规则，对可接受的类别（例如金融服务）执行“允许”操作。由于必须检测所有网络连接来确定 URL 是否属于此类别，所以即便是非金融服务站点，您也会收到相关的类别信息。

但是，可能存在您已知要阻止的 URL 类别。阻止策略还会强制执行检测，所以您会获得非阻止类别连接的类别信息，而不只是受阻止的类别。

a) 在主菜单中点击策略。

确保系统显示访问控制策略。

b) 点击 + 可添加新规则。

c) 配置顺序、标题和操作。

- **顺序** - 默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目的及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一条规则，即该规则是连接在表中匹配的第一条规则）。对于该规则，我们将使用与初始设备配置期间创建的 `Inside_Outside_Rule` 相同的源/目的。您可能也已经创建了其他规则。为了最大限度地提高访问控制效率，最好是尽早设置特定规则，以确保快速决定允许还是丢弃某个连接。对于此示例，请选择 **1** 作为规则顺序。

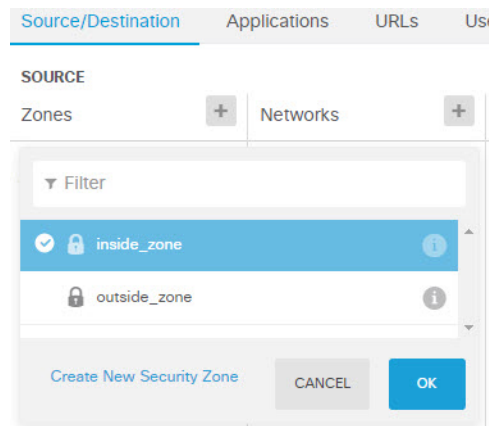
- **标题** - 为该规则指定一个有意义的名称，例如 `Block_Web_Sites`。

- **操作** - 选择阻止。

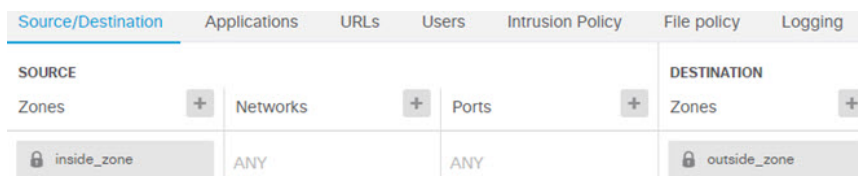
Order	Title	Action
1	Block_Web_Sites	Block

d) 在源/目的选项卡上，点击 + 以打开源 > 区域，然后选择 `inside_zone`，再在区域对话框中点击确定。

添加任何标准的方式与此相同。点击+打开一个小对话框，从中点击您要添加的项目。可以点击多个项目，点击已选项目将取消选择该项目（选中标记表示所选项目）。选择项目后，点击确定按钮才能将它们添加到策略中，只是选中项目并不能将项目添加到策略中。

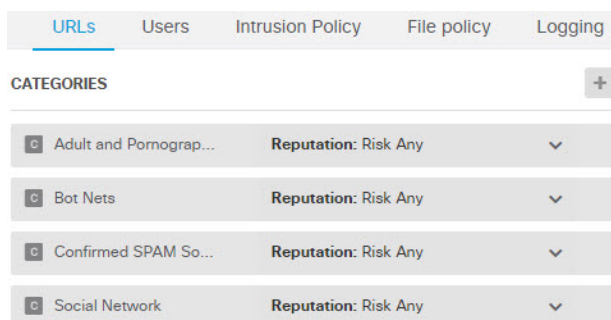


e) 按照相同的方法，为目的 > 区域选择 `outside_zone`。

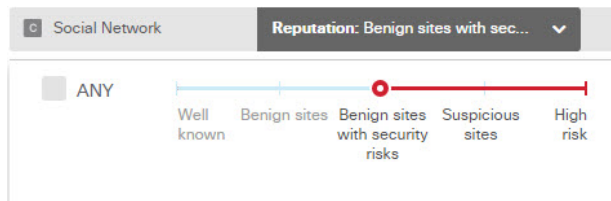


- f) 点击 **URL** 选项卡。
- g) 点击类别的 **+**，然后选择要完全或部分阻止的类别。

在本例中，选择“成人和色情”、“僵尸网络”、“确认的垃圾邮件源”和“社交网络”。您可能还希望阻止其他类别。



- h) 要对“社交网络”类别按信誉敏感性实施阻止，请点击该类别的信誉：任何风险，取消选择任何，然后将滑块移到存在安全风险的良性站点。点击远离滑块的位置将其关闭。



信誉滑块的左侧指示要允许的站点，右侧是要阻止的站点。在这种情况下，只会阻止信誉为“可疑站点”和属于“高风险”范围的社交网站。因此，您的用户应该能够访问风险较低的常用社交网站。

使用信誉，您可以选择性地阻止要允许的某个类别内的某些站点。

- i) 点击类别列表左侧 **URL** 列表旁边的 **+**。
- j) 在弹出对话框的底部，点击**创建新 URL** 链接。
- k) 对于名称和 URL，请输入 **badsite.example.com**，然后依次点击**确定**以创建对象。

您可以为该对象指定与 URL 相同的名称，也可以为其指定不同的名称。对于 URL，请勿包含 URL 的协议部分，只添加服务器名称。

New URL Object

Name
badsite.example.com

Description

URL
badsite.example.com

- l) 选择该新对象，然后点击**确定**。

在编辑策略时添加该新对象，即可方便地将该对象添加到列表中。新对象不会自动选中。

Order	Title	Action
1	Block_Web_Sites	Block

Source/Destination Applications **URLs** Users Intrusion Policy File policy Logging

URLS CATEGORIES

badsite.example.com	Adult and Pornograp... Reputation: Risk Any
	Bot Nets Reputation: Risk Any
	Confirmed SPAM So... Reputation: Risk Any
	Social Network Reputation: Benign sites with sec...

- m) 点击**日志记录**选项卡，然后依次选择**选择日志操作 > 连接开始和结束时**。
只有启用日志记录才能将类别和信誉信息记入 Web 类别控制面板和连接事件。
- n) 点击**确定**以保存该规则。

步骤 3（可选。）设置 URL 过滤的首选项。

在启用 URL 许可证时，系统会自动启用对 Web 类别数据库的更新。系统每 30 分钟检查一次更新，不过数据通常每天更新一次。如果您由于某种原因不想更新，可以关闭这些更新。

另外，还可以选择将未分类的 URL 发送给思科进行分析。因此，如果安装的 URL 数据库没有进行站点分类，思科 CSI 可能会进行分类。思科 CSI 返回类别和信誉，基于类别的规则随后可以正确应用至 URL 请求。对因内存限制而安装较小 URL 数据库的低端系统而言，选择此选项非常重要。您可以设置查找结果的生存时间：默认值为“从不”，这意味着永远不会刷新查找结果。

- 点击 **设备**。
- 依次点击**系统设置 > 流量设置 > URL 过滤首选项**。
- 选择**针对未知 URL 查询思科 CSI (Query Cisco CSI for Unknown URLs)**。
- 选择合理的 **URL 生存时间**，例如 24 小时。

e) 点击**保存**。

步骤 4 确认您的更改。

a) 点击网页右上角的**部署更改**图标。



b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

此时，监控控制面板和事件应开始显示 URL 类别和信誉及被丢弃连接的相关信息。您可以评估此信息以确定您的 URL 过滤要丢弃这些不符合条件的站点，还是您需要针对特定类别降低信誉设置。

请考虑事先通知用户，您会基于网站的分类和信誉阻止对网站的访问。

如何控制应用使用情况

Web 已成为企业交付应用（无论是基于浏览器的应用平台，还是使用 Web 协议传入和传出企业网络的富媒体应用）普遍使用的平台。

Firepower 威胁防御通过检查连接确定使用的应用。这样即可写入针对应用的访问控制规则，而不只是针对特定的 TCP/UDP 端口。因此，即使使用相同的端口，也可以选择性地阻止或允许基于 Web 的应用。

虽然可以选择要允许或阻止的特定应用，但也可以基于类型、类别、标记、风险或业务相关性写入规则。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

在此使用案例中，我们将阻止属于**匿名程序/代理**类别的任何应用。

开始之前

此使用案例假定您已完成使用案例[如何深入了解您的网络流量](#)，第 34 页。该使用案例介绍了如何收集应用使用信息，您可以在“应用”控制面板中分析这些信息。了解实际使用的应用可帮助您基于应用设计有效的规则。另外，该使用案例还介绍了如何安排 VDB 更新，我们在此不再重复。请务必必要定期更新 VDB，以便可正确识别应用。

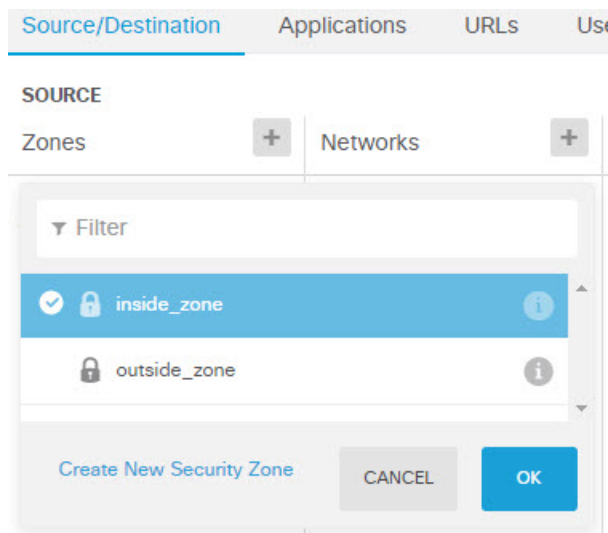
过程

步骤 1 创建基于应用的访问控制规则。

- a) 在主菜单中点击**策略**。
确保系统显示**访问控制策略**。
- b) 点击 **+** 可添加新规则。
- c) 配置顺序、标题和操作。
 - **顺序** - 默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目的及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一条规则，即该规则是连接在表中匹配的第一条规则）。对于该规则，我们将使用与初始设备配置期间创建的 **Inside_Outside_Rule** 相同的源/目的。您可能也已经创建了其他规则。为了最大限度地提高访问控制效率，最好是尽早设置特定规则，以确保快速决定允许还是丢弃某个连接。对于此示例，请选择 **1** 作为规则顺序。
 - **标题** - 为该规则指定一个有意义的名称，例如 **Block_Anonymizers**。
 - **操作** - 选择**阻止**。

Order	Title	Action
1	Block_Anonymizers	Block

- d) 在**源/目的**的选项卡上，点击 **+** 以打开**源 > 区域**，然后选择 **inside_zone**，再在区域对话框中点击**确定**。



- e) 按照相同的方法，为**目的 > 区域**选择 **outside_zone**。

Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy	Logging
SOURCE			DESTINATION			
Zones	+	Networks	+	Ports	+	Zones
inside_zone		ANY		ANY		outside_zone

- f) 点击 **Applications** (应用) 选项卡。
- g) 针对应用点击 +, 然后点击弹出对话框底部的高级过滤器链接。

虽然可以事先创建应用过滤器对象, 再在此处从“应用过滤器”列表中选择它们, 但也可以直接在访问控制规则中指定标准, 再选择将该标准另存为过滤器对象。除非为单个应用写入规则, 否则使用“高级过滤器”对话框查找应用和构建适当的标准更方便。

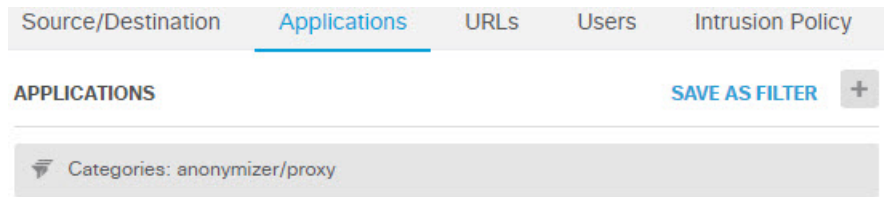
在选择标准时, 对话框底部的“应用”列表将准确显示符合标准的应用。您要编写的规则将应用到这些应用中。

仔细查看此列表。例如, 您可能会希望阻止风险极高的所有应用。但是, 在撰写本文时, Facebook 和 TFPT 则属于风险极高类别。而大多数组织不想阻止这些应用。请花些时间测试各种过滤条件, 以查看哪些应用符合您的选择。请注意, 这些列表可能随着每次 VDB 更新而变化。

在本例中, 从“类别”列表中选择“匿名程序/代理”。

The screenshot shows the 'Filter Applications' interface. It has three main filter sections: Risks, Categories, and Tags. Under Risks, three dropdown menus are set to 'Any'. Under Categories, 'anonymizer/proxy' is selected. Under Tags, five items are selected. Below these filters, a search bar and a list of 33 applications are shown. The list has columns for 'Application' and 'Description'. The first few items are ASProxy, After School, Avocent, and Avoidr.

- h) 在“高级过滤器”对话框中点击添加。
“应用” (Applications) 选项卡中将添加并显示该过滤器。



- i) 点击日志记录选项卡，然后依次选择选择日志操作 > 连接开始和结束时。
您必须启用日志记录选项卡才能获取与此规则阻止的任何连接相关的信息
- j) 点击确定以保存该规则。

步骤 2 确认您的更改。

- a) 点击网页右上角的部署更改图标。



- b) 点击立即部署按钮。

您可以等待部署完成，也可以点击确定，稍后再检查任务列表或部署历史记录。

步骤 3 点击监控并评估结果。

现在，您可能会在网络概况控制面板中看到“应用”构件中丢弃的连接。使用所有/已拒绝/已允许下拉选项可仅关注被丢弃的应用。

此外，还可以在 Web 应用控制面板上查找应用的相关信息。应用控制面板显示与协议相关的结果。假定您启用了身份策略并要求身份验证，当有人尝试使用这些应用，则该应用可以与尝试连接的用户相关联。

如何添加子网

如果您的设备有一个可用接口，则可以将其连接到交换机（或其他路由器）为其他子网提供服务。

添加子网的潜在原因很多。对于此使用案例，我们将处理以下典型场景。

- 子网是内部网络，使用专用网络 192.168.2.0/24。
- 该网络的接口使用静态地址 192.168.2.1。在本例中，网络使用的是物理接口。另一种选项是使用已连线的接口，并为新网络创建一个子接口。
- 设备将使用 DHCP 为网络中的工作站提供地址，使用的地址池为 192.168.2.2 - 192.168.2.254。
- 允许网络访问其他内部网络和外部网络。传至外部网络的流量将使用 NAT 获取公共地址。



注释 此示例假定未使用的接口不是桥接组的一部分。如果它当前是桥接组成员，则必须首先将其从桥接组中删除，然后再执行此步骤过程。

开始之前

将网络电缆物理连接到新子网的接口和交换机。

过程

步骤 1 配置接口。

- 点击 **设备**，然后点击接口摘要中的链接。
- 将鼠标悬停在您连线的接口行右侧的操作单元格上方，然后点击编辑图标 (✎)。
- 配置基本接口属性。
 - **名称** - 接口的名称。在本例中为 **inside_2**。
 - **模式** - 选择路由。
 - **状态** - 点击状态开关启用该接口。
 - **IPv4 地址**选项卡 - 针对**类型**选择**静态**，然后输入 **192.168.2.1/24**。

Edit Physical Interface

Interface Name	Mode	Status
<input type="text" value="inside_2"/>	<input style="border: none; background-color: #ccc; padding: 2px 10px; font-size: small; font-weight: normal; color: #000; text-decoration: none; border-bottom: 1px solid #000; border-top: 1px solid #000; border-left: 1px solid #000; border-right: 1px solid #000; vertical-align: middle;" type="text" value="Routed"/> ▼	<input checked="" type="checkbox"/>
<i>Most features work with named interfaces only, although some require unnamed interfaces. Learn More</i>		
Description		
<div style="display: flex; justify-content: space-between; font-size: x-small; color: #0070c0; border-bottom: 1px solid #ccc; margin-bottom: 5px;"> IPv4 Address IPv6 Address Advanced Options </div> <p>Type</p> <input style="border: none; background-color: #ccc; padding: 2px 10px; font-size: small; font-weight: normal; color: #000; text-decoration: none; border-bottom: 1px solid #000; border-top: 1px solid #000; border-left: 1px solid #000; border-right: 1px solid #000; vertical-align: middle;" type="text" value="Static"/> ▼		
IP Address and Subnet Mask		
<input style="border: none; background-color: #ccc; padding: 2px 10px; font-size: small; font-weight: normal; color: #000; text-decoration: none; border-bottom: 1px solid #000; border-top: 1px solid #000; border-left: 1px solid #000; border-right: 1px solid #000; vertical-align: middle;" type="text" value="192.168.2.1"/> / <input style="border: none; background-color: #ccc; padding: 2px 10px; font-size: small; font-weight: normal; color: #000; text-decoration: none; border-bottom: 1px solid #000; border-top: 1px solid #000; border-left: 1px solid #000; border-right: 1px solid #000; vertical-align: middle;" type="text" value="24"/>		
<i>e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0</i>		

- 点击**保存**。

接口列表将显示更新的接口状态和配置的 IP 地址。

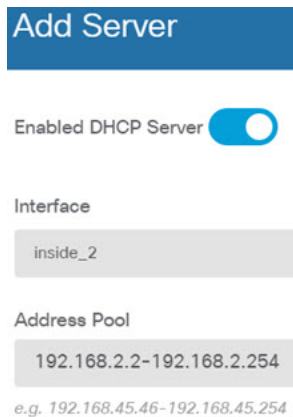


步骤 2 针对该接口配置 DHCP 服务器。

- a) 点击 **设备**。
- b) 点击 **系统设置 > DHCP 服务器**。
- c) 点击 **DHCP 服务器** 选项卡。

下表列出了所有现有 DHCP 服务器。如果使用默认配置，列表中包含内部接口的一个 DHCP 服务器。

- d) 点击表格上方的 **+**。
- e) 配置服务器属性。
 - **启用 DHCP 服务器** - 点击此开关启用该服务器。
 - **接口** - 选择您提供 DHCP 服务所使用的接口。在本例中，选择 `inside_2`。
 - **地址池** - 服务器可以为网络中设备提供的地址。输入 `192.168.2.2-192.168.2.254`。确保未包含网络地址 (.0)、接口地址 (.1) 或广播地址 (.255)。另外，如果网络中的任何设备需要使用静态地址，请从池中排除这些地址。池必须是一系列连续地址，所以请从该范围的开头或末尾选择静态地址。



- f) 点击 **添加**。

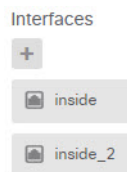
#	INTERFACE	ENABLED DHCP SERVER	ADDRESS POOL
1	inside	Enabled	192.168.1.5-192.168.1.254
2	inside_2	Enabled	192.168.2.2-192.168.2.254

步骤 3 将该接口添加到内部安全区。

要在接口上编写策略，该接口必须属于安全区。您需要针对安全区编写策略。因此，您在区域中添加和删除接口时，会自动更改应用于接口的策略。

- a) 在主菜单中点击 **对象**。

- b) 从对象目录中选择安全区。
- c) 将鼠标悬停在 **inside_zone** 对象行右侧的操作单元格上方，然后点击编辑图标 (🔗)。
- d) 点击接口下的 +，选择 **inside_2** 接口，然后点击接口列表中的确定。



- e) 点击保存。

Security Zones

3 objects

#	NAME	MODE	INTERFACES
1	inside_zone	Routed	inside, inside_2
2	outside_zone	Routed	outside

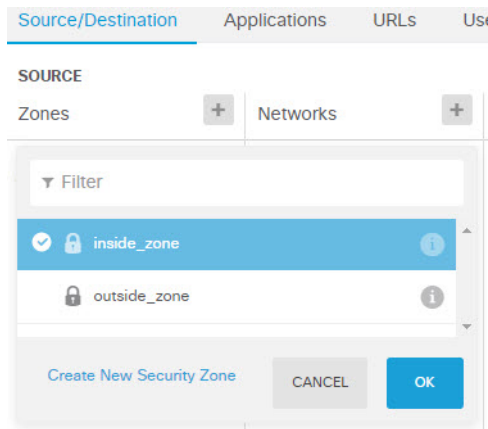
步骤 4 创建一条允许在内部网络之间传输流量的访问控制规则。

不会自动允许任何接口之间的流量。必须创建访问控制规则，才能允许所需的流量。唯一例外情况是，允许访问控制规则默认操作中的流量。在本例中，我们假定您保留了设备安装向导配置的阻止默认操作。因此，您需要创建一条规则，以允许内部接口之间的流量。如果已经创建这样的规则，请跳过此步骤。

- a) 在主菜单中点击策略。
 - 确保系统显示访问控制策略。
- b) 点击 + 可添加新规则。
- c) 配置顺序、标题和操作。
 - **顺序** - 默认将新规则添加到访问控制策略的末尾。但是，您必须将此规则放在符合相同源/目的及其他条件的任何规则之前（上方），否则该规则将无法获得匹配（一个连接仅匹配一条规则，即该规则是连接在表中匹配的第一条规则）。对于该规则，我们将使用唯一“源/目的”条件，所以可以将该规则添加到列表的末尾。
 - **标题** - 为该规则指定一个有意义的名称，例如 Allow_Inside_Inside。
 - **操作** - 选择允许。

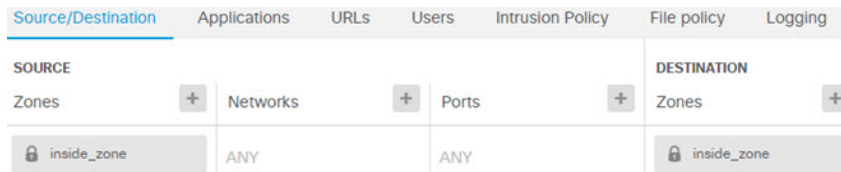
Order	Title	Action
4	Allow_Inside_Inside	Allow

- d) 在源/目的选项卡上，点击 + 以打开源 > 区域，然后选择 **inside_zone**，再在区域对话框中点击确定。



- e) 按照相同的方法，为目的 > 区域选择 **inside_zone**。

安全区必须至少包含两个接口，以便为源和目标选择同一区域。



- f) (可选。) 配置入侵和恶意软件检测。

虽然内部接口位于受信任区域，但用户通常会将笔记本电脑连接到网络。因此，用户可能不知道会将外部网络或 Wi-Fi 热点的威胁带入网络内部。因此，您可能希望扫描内部网络之间的流量中是否存在入侵和恶意软件。

请考虑执行以下操作。

- 点击**入侵策略**选项卡，启用入侵策略，并使用滑块选择“平衡安全性和连接”策略。
- 点击**文件策略**选项卡，然后选择“阻止所有恶意软件”策略。

- g) 点击**日志记录**选项卡，然后依次选择**选择日志操作 > 连接开始和结束时**。

只有启用日志记录，才能获得符合该规则的任何连接的相关信息。日志记录会向控制面板中添加统计信息，并会显示事件查看器中的事件。

- h) 点击**确定**以保存该规则。

步骤 5 确认是否已为新子网定义所需的策略。

通过将该接口添加到 **inside_zone** 安全区，**inside_zone** 的任何现有策略将自动应用到新子网。但是，请花些时间来检查您的策略，确保未遗漏任何其他策略。

如果已完成初始配置，即可应用以下策略。

- **访问控制 - Inside_Outside_Rule** 应允许新子网和外部网络之间的所有流量。如果您按照前面使用案例执行了操作，该策略则还会提供入侵和恶意软件检测。必须有一条规则允许新网络和外部网络之间的某些流量，否则用户将无法访问互联网或其他外部网络。

- **NAT - InsideOutsideNATrule** 适用于传至外部接口的任何接口，并会应用于接口 PAT。如果保留了此规则，则从新网络传至外部网络的流量会将 IP 地址转换为外部接口 IP 地址上的唯一端口。如果在传至外部接口时没有应用于所有接口或 `inside_zone` 接口的规则，则可能需要立即创建一条规则。
- **身份** - 没有默认的身份策略。但是，如果您按照前面使用案例执行了操作，则可能已有需要对新网络进行身份验证的身份策略。如果没有适用的身份策略，但希望掌握新网络的用户信息，请立即创建一条策略。

步骤 6 确认您的更改。

- a) 点击网页右上角的**部署更改**图标。



- b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

下一步做什么

确认新子网中的工作站是否使用 DHCP 获取 IP 地址，以及它们是否可访问其他内部网络和外部网络。使用监控控制面板和事件查看器评估网络使用情况。

如何被动监控网络上的流量

Firepower 威胁防御设备通常部署为主动防火墙和 IPS（入侵防御系统）安全设备。设备的核心功能是提供主动网络保护，丢弃不需要的连接和威胁。

但是，您还可以在被动模式下部署系统，使设备只分析受监控交换机端口上的流量。此模式主要用于演示或测试目的，以便您可以在将设备部署为主动防火墙之前熟悉设备。使用被动部署，您可以监控网络上的各种威胁、用户浏览的 URL 类别，等等。

虽然被动模式通常用于演示或测试目的，但也可以在生产环境中使用，如果它可提供所需的服务，例如 IDS（入侵检测系统，而无需防御）。您可以搭配使用被动接口和主动防火墙路由接口，以提供组织所需的确切服务组合。

以下过程介绍如何被动部署系统来分析通过有限数量的交换机端口传递的流量。



注释

本示例适用于硬件 Firepower 威胁防御设备。您还可以对 Firepower 威胁防御虚拟使用被动模式，但网络设置是不同的。有关详细信息，请参阅[Firepower 威胁防御虚拟被动接口配置 VLAN](#)，第 201 页。否则，此步骤也适用于 Firepower 威胁防御虚拟。

开始之前

此过程假定您已连接内部和外部接口，并完成初始设备设置向导。即使在被动部署中，您也需要连接到互联网下载系统数据库更新。您还需要能够连接到管理接口以打开 Firepower 设备管理器（可通过到内部或管理端口的直接连接实现）。

过程

步骤 1 将交换机端口配置为 SPAN（交换端口分析器）端口，并为源接口配置监控会话。

以下示例为 Cisco Nexus 5000 系列交换机上的两个源接口设置 SPAN 端口和监控会话。如果您使用不同类型的交换机，所需的命令可能会有所不同。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)# exit
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

验证：


```
switch# show monitor session 1 brief
      session 1
-----
type           : local
state          : up
source intf    :
  rx           : Eth1/7      Eth1/8
  tx           : Eth1/7      Eth1/8
  both        : Eth1/7      Eth1/8
source VSANs   :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```


步骤 2 将 Firepower 威胁防御接口连接到交换机的 SPAN 端口。

最好选择 Firepower 威胁防御设备上当前未使用的端口。根据示例交换机配置，将电缆连接到交换机的以太网 1/48。这是监控会话的目标接口。

步骤 3 将 Firepower 威胁防御接口配置为被动模式。

- a) 点击**设备**，然后点击**接口摘要**。
- b) 点击要编辑的物理接口的编辑图标 。

选择当前未使用的接口。如果您要将使用中的接口转换为被动接口，需要先从任何安全区中删除该接口，并删除使用该接口的所有其他配置。

- c) 将**状态滑块**设置为已启用设置 。
- d) 进行以下配置：

- 接口名称 - 接口名称，最多 48 个字符。字母字符必须为小写。例如，**monitor**。
- 模式 - 选择被动。

Interface Name	Mode	Status
<input type="text" value="monitor"/>	<input type="text" value="Passive"/>	<input checked="" type="checkbox"/>

e) 点击确定。

步骤 4 为接口创建被动安全区。

- 选择对象，然后从目录中选择安全区。
- 点击 + 按钮。
- 输入对象的名称和描述（后者为可选项）。例如，**passive_zone**。
- 对于模式，请选择被动。
- 点击 +，然后选择被动接口。

Name
<input type="text" value="passive_zone"/>
Description
<input type="text"/>
Mode
<input type="radio"/> Routed <input checked="" type="radio"/> Passive
Interfaces
<input type="button" value="+"/>
<input type="button" value="monitor"/>

f) 点击确定。

步骤 5 为被动安全区配置一个或多个访问控制规则。

创建的规则数量和类型取决于您想要收集的信息。例如，如果您要将系统配置为 IDS（入侵检测系统），需要至少一个分配有入侵策略的允许规则。如果您想要收集 URL 类别数据，需要至少一个具有 URL 类别规范的规则。

您可以创建阻止规则，以确定系统本可阻止主动路由接口上的哪些连接。这些连接实际上并没有被阻止，因为接口是被动接口，但您将清楚地看到系统会如何整理网络上的流量。

以下使用案例介绍访问控制规则的主要用途。这些规则也适用于被动接口。只需选择被动安全区作为所创建规则的源区域。

- [如何阻止威胁，第 41 页](#)

- 如何阻止恶意软件，第 47 页
- 如何实施可接受使用策略（URL 过滤），第 50 页
- 如何控制应用使用情况，第 54 页

以下过程创建两条允许规则来应用入侵策略并收集 URL 类别数据。

- 依次选择策略 > 访问控制。
- 点击 + 添加允许所有流量、但应用入侵策略的规则。
- 选择 **1** 作为规则顺序。此规则比默认规则更具体，但并不与之重叠。如果您已有自定义规则，请为这些规则选择适当的位置，以便传递到被动接口的流量不匹配这些规则。
- 输入规则的名称，例如 **Passive_IDS**。
- 对操作选择允许。
- 在源/目标选项卡上，选择源 > 区域下的被动区。不要配置选项卡上的任何其他选项。

在评估模式运行时，此阶段的规则应为：

Order	Title	Action
1	Passive_IDS	Allow

Source/Destination	Applications	URLs	Users	Intrusion Policy						
<p>SOURCE</p> <table border="1"> <thead> <tr> <th>Zones</th> <th>Networks</th> <th>Ports</th> </tr> </thead> <tbody> <tr> <td>passive_zone</td> <td>ANY</td> <td>ANY</td> </tr> </tbody> </table>	Zones	Networks	Ports	passive_zone	ANY	ANY				
Zones	Networks	Ports								
passive_zone	ANY	ANY								

- 点击入侵策略选项卡，将滑块滑动至打开，并选择 **Balanced Security and Connectivity** 入侵策略（建议将此策略应用于大多数网络）。

INTRUSION POLICY

LEVEL OF INTRUSION POLICY

Balanced Security and Connectivity

- 点击日志记录选项卡，并选择在连接结束时作为日志记录选项。

SELECT LOG ACTION

- At Beginning and End of Connection
 At End of Connection
 No Connection Logging

- i) 点击**确定**。
- j) 点击 + 添加要求系统执行深度检查以确定所有 HTTP 请求的 URL 和类别的规则。
通过此规则，您可以在控制面板中查看 URL 类别信息。为节省处理时间并提高性能，系统仅在至少有一个指定 URL 类别条件的访问控制规则时确定 URL 类别。
- k) 选择**1**作为规则顺序。这样可将规则放置在上一个规则(Passive_IDS)上方。如果您将其放置在该规则（适用于所有流量）后面，流量将永远不会匹配您现在创建的规则。
- l) 输入规则的名称，例如 **Determine_URL_Category**。
- m) 对操作选择**允许**。
或者，您可以选择**阻止**。上述任一操作都可以实现此规则的目的。
- n) 在源/目标选项卡上，选择源 > 区域下的被动区。不要配置选项卡上的任何其他选项。

Order	Title	Action
1	Determine_URL_Category	Allow

[Source/Destination](#)
[Applications](#)
[URLs](#)
[Users](#)
[Intrusion Policy](#)

SOURCE		
Zones	Networks	Ports
passive_zone	ANY	ANY

- o) 点击 **URL** 选项卡，点击**类别**标题旁边的 +，然后选择任何类别。例如，**互联网门户**。或者，可以选择信誉级别，或保留默认值“任何”。

CATEGORIES	
Internet Portals	Reputation: Risk Any

- p) 点击**入侵策略**选项卡，将滑块滑动至打开，并选择您为第一个规则选择的同一入侵策略。
- q) 点击**日志记录**选项卡，并选择在**连接结束时**作为日志记录选项。

但是，如果您选择**阻止**操作，请选择在**连接开始和结束时**。由于被阻止的连接不会自行终止，只能在连接开始时获取日志信息。

r) 点击**确定**。

步骤 6 (可选。)配置其他安全策略。

您还可以配置以下安全策略，了解它们对流量的影响：

- **身份** - 收集用户信息。您可以在身份策略中配置规则，以确保识别与源 IP 地址关联的用户。为被动接口实施身份策略的过程与为路由接口实施身份策略的过程相同。请按照[如何深入了解您的网络流量](#)，第 34 页所述的使用案例操作。
- **安全情报** - 阻止已知不良 IP 地址和 URL。有关详细信息，请参阅[如何阻止威胁](#)，第 41 页。

注释 被动接口上的所有加密流量均划分为无法解密类别，因此 SSL 解密规则无效，不会应用于被动接口。

步骤 7 确认您的更改。

a) 点击网页右上角的**部署更改**图标。



b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 8 使用监控控制面板分析来自整个网络的流量和威胁类型。如果您确定要让 Firepower 威胁防御设备主动丢弃不需要的连接，请重新部署设备，以便您可以配置用于为监控网络提供防火墙保护的主动路由接口。

更多示例

除了使用案例一章中的示例之外，某些解释特定服务的章节中还包括示例配置。您可能对下面的示例感兴趣。

网络地址转换 (NAT)

IPv4 地址的 NAT

- [提供对内部 Web 服务器的访问权限（静态自动 NAT）](#)，第 341 页
- [FTP、HTTP 和 SMTP 的单个地址（具有端口转换的静态自动 NAT）](#)，第 343 页
- [转换因目的而异（动态手动 PAT）](#)，第 349 页
- [转换因目的地址和端口而异（动态手动 PAT）](#)，第 355 页
- [DNS 应答修改，外部接口上的 DNS 服务器](#)，第 368 页
- [DNS 应答修改，主机网络上的 DNS 服务器](#)，第 371 页
- [使站点间 VPN 流量豁免 NAT](#)，第 394 页

IPv6 地址的 NAT

- [NAT64/46 示例：内部 IPv6 网络与外部 IPv4 互联网](#)，第 327 页
- [NAT64/46 示例：包含外部 IPv4 互联网和 DNS 转换的内部 IPv6 网络](#)，第 329 页
- [NAT66 示例：网络间的静态转换](#)，第 334 页
- [NAT66 示例：简单 IPv6 接口 PAT](#)，第 337 页
- [DNS 64 回复修改](#)，第 362 页

远程接入虚拟专用网络 (RA VPN)

- [如何在外部接口上为远程接入 VPN 用户提供互联网访问权限（发夹方法）](#)，第 421 页
- [如何通过远程接入 VPN 使用外部网络上的目录服务器](#)，第 428 页

站点间虚拟专用网络 (VPN)

- [使站点间 VPN 流量豁免 NAT](#)，第 394 页
- [如何在外部接口上为外部站点间 VPN 用户提供互联网访问（发夹方法）](#)，第 399 页

SSL/TLS 解密

- [示例：从网络阻止较旧的 SSL/TLS 版本](#)，第 236 页

FlexConfig 策略

- [如何启用和禁用默认全局检测](#)，第 523 页
- [如何撤消 FlexConfig 更改](#)，第 529 页
- [如何启用唯一流量类检测](#)，第 530 页
- [如何在 ISA 3000 上启用硬件绕行](#)，第 534 页



第 3 章

为系统授权许可

以下主题介绍如何向 Firepower 威胁防御设备授予许可证。

- [Firepower 系统的智能许可](#)，第 69 页
- [管理智能许可证](#)，第 72 页

Firepower 系统的智能许可

通过思科智能许可，您可以集中购买和管理许可证池。与产品授权密钥 (PAK) 许可证不同，智能许可证未绑定到特定序列号或许可证密钥。通过智能许可，您可以直观地评估许可证使用情况和需求。

此外，智能许可不会阻止您使用尚未购买的产品功能。只要您向思科智能软件管理器进行了注册，即可立即开始使用许可证，并在以后购买该许可证。这使您能够部署和使用功能，并避免由于采购订单审批造成延迟。

思科智能软件管理器

在为 Firepower 威胁防御设备购买一个或多个许可证时，可以在思科智能软件管理器中对其进行管理：<https://software.cisco.com/#SmartLicensing-Inventory>。通过思科智能软件管理器，您可以为组织创建一个主账户。

默认情况下，许可证分配给主账户下的默认虚拟账户。作为账户管理员，您可以创建其他虚拟账户；例如，为区域、部门或子公司创建账户。使用多个虚拟账户有助于管理大量许可证和设备。

许可证和设备按虚拟账户进行管理；只有该虚拟账户的设备可以使用分配给该账户的许可证。如果您需要其他许可证，则可以从另一个虚拟账户传输未使用的许可证。您还可以在虚拟账户之间传输设备。

当您向思科智能软件管理器注册某个设备时，会在管理器中创建一个产品实例注册令牌，然后将其输入 Firepower 设备管理器。注册的设备将基于使用的令牌与某个虚拟账户相关联。

有关思科智能软件管理器的详细信息，请参阅该管理器的在线帮助。

与许可证颁发机构的定期通信

使用产品实例注册令牌注册 Firepower 威胁防御设备时，设备会向思科许可证颁发机构注册。许可证颁发机构会为该设备与许可证颁发机构之间的通信颁发 ID 证书。此证书有效期为 1 年，但需要每 6 个月续签一次。如果 ID 证书到期（通常在九个月或一年内未通信），设备将恢复撤销注册状态，许可的功能将被暂停使用。

设备定期与许可证颁发机构进行通信。如果您在思科智能软件管理器中进行更改，则可以刷新设备上的授权，以使更改立即生效。另外，也可以等待设备按计划通信。常规许可证通信每 30 天进行一次，但如果设备具有宽限期，则会最多运行 90 天，而不会进行自动通报。您必须在 90 天截止前与许可证颁发机构联系。

智能许可证类型

下表介绍了 Firepower 威胁防御设备可用的许可证。

购买 Firepower 威胁防御设备会自动附带基本许可证。其他所有许可证均是可选的。



注释 无法购买 ISA 3000 设备的恶意软件或 URL 过滤许可证。

表 3: 智能许可证类型

许可证	持续时间	授予的功能
基础（自动包含）	永久	<p>可选期限的许可证中未包括的所有功能。</p> <p>您还必须指定是否在使用此令牌注册的产品上允许出口控制功能。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。</p>
威胁	基于期限	<p>入侵检测和防御 - 入侵策略用于分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。</p> <p>文件控制 - 文件策略用于检测和选择性地阻止用户上传（发送）或下载（接收）特定类型的文件。通过面向 Firepower 的 AMP（需要恶意软件许可证），您可以检查和阻止包含恶意软件的文件。必须拥有威胁许可证才可使用任何类型的文件策略。</p> <p>安全情报过滤 - 将选定流量丢弃后，通过访问控制规则对流量进行分析。动态源可用于根据最新情报立即丢弃连接。</p>

许可证	持续时间	授予的功能
恶意软件	基于期限	检查恶意软件的文件策略，将思科高级恶意软件保护 (AMP) 与适用于 Firepower 的 AMP（基于网络的高级恶意软件保护）和思科 Threat Grid 结合使用。 文件策略可以检测和阻止通过网络传输的文件中的恶意软件。
URL 过滤	基于期限	基于类别和信誉的 URL 过滤。 您可以对单个 URL 执行 URL 过滤，而不使用此许可证。
远程接入 RA VPN： <ul style="list-style-type: none"> • AnyConnect Plus • AnyConnect Apex • AnyConnect VPN Only 	基于期限或永久，取决于许可证类型。	远程接入 VPN 配置。您的基础许可证必须允许出口控制功能，以便配置远程接入 RA VPN。在注册设备时，您需要选择是否满足出口要求。 Firepower 设备管理器可以使用任何有效的 AnyConnect 许可证。可用功能不因许可证类型不同而不同。如果尚未购买，请参阅 远程接入 VPN 的许可要求，第 409 页 。 另请参阅《思科 AnyConnect 订购指南》 http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf 。

可选许可证过期或被禁用的影响

如果可选许可证过期，您可以继续使用需要该许可证的功能。但是，该许可证将被标记为不合规，您需要购买许可证并将其添加到您的账户，才能使该许可证恢复合规状态。

如果禁用了某个可选许可证，系统将做出如下反应：

- **恶意软件许可证** - 系统会停止查询 AMP 云，还会停止确认从 AMP 云发送的追溯性事件。如果现有访问控制策略包括的文件策略会应用恶意软件检测，则无法重新部署现有访问控制策略。请注意，在禁用恶意软件许可证后的很短时间内，系统可以使用现有缓存文件处置情况。在时间窗过期后，系统将向这些文件分配不可用的处置情况。
- **威胁** - 系统将不再应用入侵或文件控制策略。对于安全情报策略，系统不再应用策略并停止下载情报源更新。您无法重新部署需要该许可证的现有策略。
- **URL 过滤** - 带有 URL 类别条件的访问控制规则会立即停止过滤 URL，且系统不再会下载对 URL 数据的更新。如果现有访问控制策略包含的规则带有基于类别和信誉的 URL 标准，则不能重新部署现有的访问控制策略。
- **RA VPN** - 您不能编辑远程接入 VPN 配置，但可以将其删除。用户仍可使用 RA VPN 配置进行连接。但是，如果您更改设备注册，致使系统不再符合导出规定，则远程接入 VPN 配置会立即停止，且所有远程用户都无法通过 VPN 进行连接。

管理智能许可证

使用“智能许可证”页面可查看系统当前的许可证状态。系统必须获得许可。

该页面显示您使用的是90天评估许可证，还是已注册到思科智能软件管理器。注册后，您可以查看与思科智能软件管理器的连接状态，以及各类许可证的状态。

使用授权标识智能许可证代理状态：

- 已授权（“已连接”、“足够的许可证”）-设备已成功联系许可证颁发机构并向其注册，该机构已向设备授予许可证授权。设备现在处于合规状态。
- 不合规 - 设备没有可用的许可证授权。许可功能可继续工作。但您必须购买或释放其他授权，才能变为合规状态。
- 授权已过期 - 设备已连续90天或更长时间未与许可颁发机构通信。许可功能可继续工作。在此状态下，智能许可证代理将重试其授权申请。如果重试成功，代理将进入“不合规”或“已授权”状态，并开始新的授权期限。尝试手动同步设备。



注释 点击智能许可证状态旁边的 **i** 按钮，可查看虚拟账户、出口管制功能，并可获链接来打开思科智能软件管理器。出口控制的功能控制软件受国家安全、外交政策和反恐怖主义法律和法规约束。

以下步骤程序概述了如何管理系统的许可证。

过程

步骤 1 点击 **设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 注册该设备。

只有注册到思科智能软件管理器，才能分配可选许可证。在评估期结束前进行注册。

请参阅[注册设备](#)，第 73 页。

注释 注册时，选择是否向思科发送使用数据。可以通过点击齿轮图标旁边的[转到思科成功网络链接](#)更改选择。

步骤 3 申请和管理可选功能许可证。

只有注册可选许可证后，才能使用该许可证控制的功能。请参阅[启用或禁用可选许可证](#)，第 74 页。

步骤 4 维护系统许可。

您可以执行以下任务：

- [与思科智能软件管理器同步](#)，第 74 页

- [注销设备，第 75 页](#)

注册设备

购买 Firepower 威胁防御设备会自动附带基本许可证。基本许可证涵盖可选许可证未覆盖的所有功能。它是一种永久许可证。

在初始系统设置期间，系统会提示您将设备注册到思科智能软件管理器。如果您选择使用 90 天的评估许可证，必须在评估期结束前注册设备。

注册设备时，您的虚拟账户会向设备分配许可证。注册设备也会注册已启用的任何可选许可证。

开始之前

注册设备时，仅该设备被注册。如果设备已配置为高可用性，您必须登录到高可用性对的另一台设备注册该设备。

过程

步骤 1 点击 **设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 依次点击**注册设备**，并按照说明执行操作。

- a) 点击链接以打开**思科智能软件管理器**，然后登录您的账户或创建一个新账户（如果需要）。
- b) 生成新的令牌。

在创建令牌时，指定该令牌的有效使用期限。建议的过期期限为 30 天。此期限定义令牌本身的过期日期，不会影响您使用该令牌注册的设备。如果令牌在使用前过期，只需生成一个新令牌即可。

您还必须指定是否**在使用此令牌注册的产品上允许出口控制功能**。仅在您的国家/地区满足出口控制标准时，才可以选择此选项。此选项控制您对高级加密和需要高级加密的功能的使用。

- c) 复制该令牌，并将其粘贴到 Smart License Registration 对话框的编辑框中。
- d) 决定是否向思科发送使用数据。

阅读“思科成功网络”步骤中的信息，单击 **Sample Data** 链接查看收集到的实际数据，然后决定是否选中 **Enable Cisco Success Network** 选项。虽然您未启用连接，但已向思科云服务服务器注册，因此可以根据需要启用云服务。

- e) 依次点击**注册设备**。

启用或禁用可选许可证

您可以启用（注册）或禁用（解除）可选许可证。只有启用许可证后，才能使用该许可证控制的功能。

如果您不想再使用某个可选期限许可证包含的功能，可以禁用该许可证。禁用许可证会在思科智能软件管理器账户中将其释放，以便可将其应用到其他设备。

另外，在评估模式下运行时，还可启用这些许可证的评估版本。在评估模式下，只有注册设备，许可证才会注册到思科智能软件管理器。但是，您不能在评估模式下启用远程接入 RA VPN 许可证。

开始之前

在禁用许可证之前，请确保它不在使用中。重写或删除需要该许可证的任何策略。

对于在高可用性配置中运行的设备，只需在主用设备上启用或禁用许可证。备用设备请求（或释放）必要许可证时，更改会在下一次部署配置时反映在备用设备上。启用许可证时，必须确保思科智能软件管理器账户具有足够的许可证，否则可能会造成一台设备合规，而另一台设备不合规。

过程

步骤 1 点击 **设备**，然后点击“智能许可证”摘要中的**查看配置**。

步骤 2 根据需要，单击每个可选许可证的 **Enable/Disable** 控件。

- **Enable** - 将许可证注册到您的思科智能软件管理器帐户，并启用控制的功能。现在，您可以配置和部署该许可证控制的策略了。
- **Disable** - 取消许可证向思科智能软件管理器帐户的注册，并禁用控制的功能。新策略中无法配置这些功能，也不能再部署使用该功能的策略。

步骤 3 如果启用 RA VPN 许可证，请选择您账户中可用的许可证类型。

您可以使用以下任意 AnyConnect 许可证：**Plus**、**Apex** 或 **VPN Only**。如果你有 **Plus** 和 **Apex**，并想同时使用这两个许可证，则可以两个都选择。

与思科智能软件管理器同步

系统定期与思科智能软件管理器同步许可证信息。常规许可证通信每30天进行一次，但如果设备具有宽限期，则最多运行 90 天，而不会进行自动通报。

不过，如果您在思科智能软件管理器中进行更改，可以刷新设备上的授权，以使更改立即生效。

同步可获取许可证的当前状态，并更新授权和 ID 证书。

过程

- 步骤 1** 单击 **设备**，然后单击“智能许可证”摘要中的**查看配置**。
 - 步骤 2** 从齿轮下拉列表中选择**重新同步连接**。
-

注销设备

如果您不想再使用设备，可以从思科智能软件管理器中将其注销。注销后，您的虚拟账户将释放与该设备关联的基本许可证和所有可选许可证。可选许可证可以分配给其他设备。

注销设备后，该设备中的当前配置和策略将继续按原样运行，但无法进行或部署任何更改。

开始之前

当注销一台设备时，只有该设备被注销。如果该设备已配置高可用性，那么您必须登录到高可用性对的另一台设备才能注销该设备。

过程

- 步骤 1** 单击 **设备**，然后单击 Smart License 摘要中的 **View Configuration**。
 - 步骤 2** 从齿轮下拉列表中选择 **Unregister Device**。
 - 步骤 3** 如果确实要注销设备，请阅读警告并单击**注销**。
-



第 **I** 部分

系统监控

- [监控设备，第 79 页](#)
- [思科 ISA 3000 的报警，第 97 页](#)



第 4 章

监控设备

系统包括控制面板和事件查看器，通过它们可监控设备和通过设备传递的流量。

- [启用日志记录以获取流量统计信息，第 79 页](#)
- [监控流量和系统控制面板，第 82 页](#)
- [使用命令行监控更多统计信息，第 84 页](#)
- [查看事件，第 85 页](#)

启用日志记录以获取流量统计信息

使用监控控制面板和事件查看器，可以监控各种流量统计信息。但是，必须启用日志记录才能告诉系统要收集哪些统计信息。日志记录生成各种类型的事件，有助于深入了解通过系统的连接。

以下主题详细介绍事件及其所提供信息，并特别强调连接日志记录。

事件类型

系统可以生成以下类型的事件。只有生成这些事件，才能在监控控制面板中查看相关统计信息。

连接事件

您可以在用户生成通过系统传递的流量时生成连接事件。启用访问规则连接日志记录以生成这些事件。还可启用安全情报策略和 SSL 解密规则日志记录，以生成连接事件。

连接事件包括有关连接的各种信息，包括源和目的 IP 地址及端口、使用的 URL 和应用，以及传输的字节数或数据包数。另外，还包括执行的操作（例如，允许或阻止连接）和应用于连接的策略的信息。

入侵事件

系统检查网络上传输的数据包是否存在可能影响主机及其数据的可用性、完整性和机密性的恶意活动。如果系统识别出潜在的入侵，会生成入侵事件；入侵事件是有关攻击源和攻击目标的日期、时间、攻击程序类型以及情境信息的记录。无论调用访问控制规则的日志记录配置如何，系统均会生成设为阻止或提醒的入侵规则的入侵事件。

文件事件

文件事件表示系统基于文件策略在网络流量中检测到或者被阻止的文件。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。

无论调用访问控制规则采用何种日志记录配置，在系统生成文件事件时，都会记录相关连接的终止。

恶意软件事件

作为整体访问控制配置的一部分，系统可在网络流量内检测恶意软件。适用于 Firepower 的 AMP 可以生成恶意软件事件，其中包含生成事件的处置，有关检测该恶意软件的方式、位置和时间的情境数据。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。

文件的处置可能发生变化，例如，从安全变为恶意软件或从恶意软件变为安全。如果适用于 Firepower 的 AMP 向 AMP 云查询文件，且云决定在查询一周内更改处置，系统即会生成追溯性恶意软件事件。

安全情报事件

安全情报事件是由安全情报策略为该策略列入黑名单（阻止）或监控的连接生成的一种连接事件。所有安全情报事件都有一个由系统填充的“安全情报类别”字段。

对于各事件，都有一个相应的“常规”连接事件。由于评估安全情报策略后才会评估许多其他安全策略（包括访问控制），所以当安全情报阻止连接时，所生成事件不含系统从后续评估中收集的信息（如用户身份）。

可配置的连接日志记录

您应该根据贵组织的安全和合规性需求记录连接。如果您的目标是限制所生成事件的数量和提高性能，则只能启用对分析至关重要的连接的日志记录。然而，如果出于分析目的，您想要广泛了解网络流量，则可启用其他连接的日志记录。

由于系统可能会因为多种原因记录连接，因此禁用某一处的日志记录不能确保匹配连接不会被记录。

可在以下位置配置连接日志记录。

- 访问控制规则和默认操作 - 连接结束时的日志记录可提供有关连接的大多数信息。另外，您还可以记录连接开始信息，但这些事件的信息不完整。连接日志记录默认处于禁用状态，因此必须针对所要跟踪的流量的每个规则（和默认操作）启用该日志记录。
- 安全情报策略 - 可启用日志记录，为已列入黑名单的各连接生成安全情报事件。当系统由于安全情报过滤而记录连接事件时，它也会记录匹配的安全情报事件（这是一种您可以单独查看和分析的特殊类型连接事件）。
- SSL 解密规则和默认操作 - 可在连接结束时配置日志记录。对于受阻连接，系统会立即结束会话并生成事件。对于受监控连接以及您将其传递到访问控制规则的连接，系统会在会话结束时生成事件。

自动连接日志记录

系统自动保存以下连接结束事件，而不管其他日志记录配置如何。

- 除非通过访问控制策略的默认操作来处理连接，否则系统会自动记录与入侵事件关联的连接。您必须在默认操作上启用日志记录以获取匹配流量的入侵事件。
- 系统会自动记录与文件和恶意软件事件关联的连接。这仅适用于连接操作：您可以选择禁用生成文件和恶意软件事件。

连接日志记录的提示

在考虑日志记录配置和评估相关统计信息时，请记住以下提示：

- 当您通过访问控制规则允许流量时，可以使用关联的入侵或文件策略（或同时使用这两种策略），在流量到达其最终目的地前进一步检测流量并阻止入侵、禁止文件和恶意软件。不过请注意，对于加密负载，文件和入侵检测已默认禁用。如果入侵或文件策略需要阻止连接，系统将立即记录连接结束事件，而不考虑连接日志设置。允许日志记录的连接提供有关网络流量的大多数统计信息。
- 受信任连接是由信任访问控制规则或访问控制策略中的默认操作所处理的连接。但是，不会检测受信任连接中是否存在发现数据、入侵、禁止文件和恶意软件。因此，受信任连接的连接事件包含的信息有限。
- 对于阻止流量的访问控制规则和访问控制策略默认操作，系统将记录连接开始事件。匹配流量会被拒绝，无需进一步检测。
- 在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。在对 Block 规则启用日志记录之前，请考虑该规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口上的流量。

将事件发送至外部系统日志服务器

除了通过 Firepower 设备管理器（其事件存储容量有限）查看事件外，还可以选择配置规则和策略以将事件发送至外部系统日志服务器。然后，可使用所选系统日志服务器平台的功能和附加存储查看和分析事件数据。

要将事件发送至外部系统日志服务器，请编辑启用连接日志记录的各项规则、默认操作或策略，并在日志设置中选择系统日志服务器对象。要将入侵事件发送到系统日志服务器，请在入侵策略设置中配置服务器。

有关更多信息，请参阅各规则和策略类型的帮助，另请参阅[配置系统日志服务器](#)，第 119 页。

监控流量和系统控制面板

系统包括多个控制面板，它们可用来分析通过设备传递的流量和安全策略的结果。使用这些信息可评估您的配置的总体效率，识别和解决网络问题。

高可用性组中设备的控制面板仅显示该设备的统计信息。统计信息不会在设备之间同步。



注释

流量相关的控制面板中使用的数据基于访问控制规则进行收集，该规则实现连接或文件日志记录以及允许日志记录的其他安全策略。控制面板不会反映匹配未启用日志记录的规则的流量。请确保配置规则以记录对您重要的信息。另外，只有配置了身份规则来收集用户身份，才能获得用户信息。最后，只有拥有入侵、文件、恶意软件和 URL 类别功能的许可证，并配置了使用这些功能的规则，才能获得这些功能的相关信息。

过程

步骤 1 在主菜单中点击**监控**，打开“控制面板”页面。

您可以选择预定义的时间范围（例如前一小时或上周），也可以使用特定开始和结束时间自定义时间范围，以便控制控制面板图形和表格中所示的数据。

流量相关的控制面板包括以下显示类型：

- 前 5 个条形图 - 这些图形显示在**网络概况**控制面板中，以及点击控制面板表中的项目时看到的各项的摘要控制面板中。您可以在**事务数**或**数据使用量**（收发的总字节数）之间切换信息。另外，还可以切换显示屏以显示所有事务、允许的事务或拒绝的事务。点击**查看更多**链接可查看与该图相关的表格。
- 表格 - 表格显示特定类型的项目（例如，应用或 URL 类别）及该项目的事务总数、允许的事务、阻止的事务、数据使用量和收发的字节数。您可以在**原始值**和**百分比**之间切换数字，并显示前 10、100 或 1000 个条目。如果项目是链接，点击该链接可查看摘要控制面板及更多详细信息。

步骤 2 点击目录中的**控制面板**链接，可查看以下数据的控制面板：

- **网络概况** - 显示有关网络流量的摘要信息，包括匹配的访问规则（策略）、发起流量的用户、连接中使用的应用、匹配的入侵威胁（签名）、所访问 URL 的 URL 类别和连接最常访问的目标。
- **用户** - 显示网络的热门用户。只有配置身份策略，才能查看用户信息。如果没有用户身份，则包含源 IP 地址。您可能会看到以下特殊实体：
 - **身份验证失败** - 系统提示用户进行身份验证，但用户未在允许的最大尝试次数内输入有效的用户名/密码对。身份验证失败本身不会阻止用户访问网络，但您可以写入访问规则来限制这些用户访问网络。

- **访客** - “访客”用户与“身份验证失败”用户类似，只是您的身份规则配置为将这些用户称为“访客”。系统提示“访客”(Guest)用户进行身份验证，但他们在最大尝试次数内未成功通过身份验证。
- **无需身份验证** - 系统不提示用户进行身份验证，因为该类用户的连接与指定不进行身份验证的身份规则匹配。
- **未知** - 没有用户的 IP 地址映射，也没有身份验证失败的记录。通常，这意味着尚无来自该地址的 HTTP 流量。
- **应用** - 显示网络中使用的热门应用，例如 Facebook。只有检测连接，才能获得这些信息。只有连接匹配“允许”规则或使用区域、地址和端口之外条件的“阻止”规则时，才会对它们进行检测。因此，在触发需要检测的任何规则之前，如果该连接受信任或被阻止，则无法获得应用信息。
- **Web 应用** - 显示网络中使用的热门 Web 应用，例如 Google。收集 Web 应用信息的条件与“应用”控制面板的条件相同。
- **URL 类别** - 基于所访问网站的分类，显示网络中使用的热门网站类别，例如博彩或教育机构。要获得这些信息，必须至少设置一条以 URL 类别为流量匹配条件的访问控制规则。对于匹配该规则的流量，或必须检测以确定是否匹配该规则的流量，可以获得此方面的相关信息。而对于匹配第一个 Web 类别访问控制规则之前规则的连接，则不会看到它们的类别（或信誉）信息。
- **访问和 SI 规则** - 显示热门访问规则和安全情报规则（与网络流量匹配的对应项目）。
- **区域** - 显示用于进出设备的流量的热门安全区域对。
- **目的** - 显示网络流量排名靠前的目的。
- **攻击者** - 显示排名靠前的攻击者，即触发入侵事件的连接源。只有在访问规则中配置入侵策略，才能查看这些信息。
- **目标** - 显示入侵事件排名靠前的目标，即攻击的受害者。只有在访问规则中配置入侵策略，才能查看这些信息。
- **威胁** - 显示已触发的排名靠前的入侵规则。只有在访问规则中配置入侵策略，才能查看这些信息。
- **文件日志** - 显示网络流量中发现的排名靠前的文件类型。只有在访问规则中配置文件策略，才能查看这些信息。
- **恶意软件** - 显示热门恶意软件操作和处置组合。您可以详细了解相关文件类型的信息。只有在访问规则中配置文件策略，才能查看这些信息。
 - 可能的操作包括：恶意软件云查找、阻止、存档阻止（加密）、检测、自定义检测、云查找超时、恶意软件白名单、恶意软件阻止、存档阻止（已超出深度）、自定义检测阻止、TID 阻止、存档阻止（检测失败）。
 - 可能的处置包括：恶意软件、未知、安全、自定义检测、不可用。

- **SSL 解密** - 显示通过设备的加密与纯文本流量的细分以及根据 SSL 解密规则解密加密流量方法的细分。
- **系统** - 显示整个系统视图，包括接口及其状态（将鼠标悬停在接口上，查看其 IP 地址）、总平均系统吞吐量（一小时内的时间以 5 分钟存储桶为单位，一小时以上的时间以一小时存储桶为单位）、有关系统事件以及 CPU、内存和磁盘的使用情况的摘要信息。您可以将吞吐量图形限制为显示特定接口（而非所有接口）的吞吐量。与接口相关的统计信息（如吞吐量）不包括子接口。

注释 “系统”控制面板所示的信息为整个系统的相关信息。如果登录到设备 CLI，您可以使用各种命令来查看更多详细信息。例如，**show cpu** 和 **show memory** 命令包括用于显示其他详细信息的参数，而这些控制面板显示来自 **show cpu system** 和 **show memory system** 命令的数据。

步骤 3 另外，您还可以点击目录中的这些链接：

- **事件** - 查看发生的事件。只有在各个访问规则中启用连接日志记录，才能查看与这些规则相关的连接事件。此外，在安全情报策略和 SSL 解密规则中启用日志记录，以查看安全情报事件和其他连接事件数据。这些事件可以帮助您解决用户的连接问题。
- **会话** - 查看和管理 Firepower 设备管理器用户会话。有关详细信息，请参阅[管理 Firepower 设备管理器用户会话](#)，第 480 页。

使用命令行监控更多统计信息

Firepower 设备管理器控制面板提供与通过设备的流量和一般系统使用情况相关的各种统计信息。但是，您可以使用 CLI 控制面板或登录设备 CLI 获取控制面板未涵盖方面的其他信息（请参阅[登录命令行界面 \(CLI\)](#)，第 7 页）。

CLI 包含各种 **show** 命令，可用来提供这些统计信息。您还可以使用 CLI 进行常规故障排除，包括 **ping** 和 **traceroute** 等命令。大多数 **show** 命令都与 **clear** 命令结合使用，用于将统计信息重置为 0。（无法从 CLI 控制台清除统计信息。）

您可以在[思科 Firepower 威胁防御命令参考](http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html)中查找有关这些命令的文档：http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html。

例如，您会发现以下较常用的命令。

- **show nat** 显示您的 NAT 规则的命中计数点击数。
- **show xlate** 显示处于活动状态的实际 NAT 转换。
- **show conn** 提供当前通过设备的连接的相关信息。
- **show dhcpd** 提供您在接口上配置的 DHCP 服务器的相关信息。
- **show interface** 提供每个接口的使用统计信息。

查看事件

您可以查看启用日志记录的安全策略中生成的事件。另外，也可为触发的入侵策略和文件策略生成事件。

事件查看器表格可实时显示生成的事件。有新事件生成时，旧事件将退出表格。

开始之前

除了连接匹配相关策略外，是否会生成特定类型的事件还取决于以下事件：

- 连接事件 - 访问规则必须启用连接日志记录。此外还可以在安全情报策略和 SSL 解密规则中启用连接日志记录。
- 入侵事件 - 访问规则必须应用入侵策略。
- 文件和恶意软件事件 - 访问规则必须执行文件策略并启用文件日志记录。
- 安全情报事件 - 必须启用和配置安全情报策略，并启用日志记录。

过程

步骤 1 点击主菜单中的**监控**。

步骤 2 从目录中选择**事件**。

事件查看器将基于事件类型在选项卡中组织事件。有关详细信息，请参阅[事件类型](#)，第 79 页。

步骤 3 点击显示您要查看的事件类型的选项卡。

您可以对事件列表执行以下操作：

- 点击**暂停**以停止添加新事件，这样即可更加轻松地查找和分析事件。点击**继续**以允许显示新事件。
- 选择不同的刷新率（5 秒、10 秒、20 秒或 60 秒）以控制新事件的显示速度。
- 创建包含所需列的自定义视图。要创建自定义视图，请点击选项卡栏中的 **+** 按钮，或点击**添加/删除列**。无法更改预设的选项卡，所以添加或删除列将会创建新视图。有关详细信息，请参阅[配置自定义视图](#)，第 86 页。
- 要更改列的宽度，请点击列标题并将列标题分隔符拖动至所需的宽度。
- 将鼠标悬停在某个事件上方，点击**查看详细信息**可查看该事件的完整信息。有关事件中各个字段的描述，请参阅[事件字段说明](#)，第 88 页。

步骤 4 如果需要，对表格应用过滤器，以协助您基于各种事件属性找到所需的事件。

要创建新过滤器，请通过从下拉列表中选择原子元素，手动键入过滤器；也可以点击事件表格中包括要基于其过滤的值的单元格，构建一个过滤器。您可以点击同一列中的多个单元格，在这些值之

间创建 OR 条件；也可以点击不同列的单元格，在列之间创建 AND 条件。如果通过点击单元格构建过滤器，还可以编辑生成的过滤器对其微调。有关创建过滤器规则的详细信息，请参阅[过滤事件](#)，第 87 页。

在构建过滤器后，执行以下任一操作：

- 要应用过滤器和更新表格以仅显示匹配过滤器的事件，请点击[过滤器](#) 按钮。
- 要清除您应用的整个过滤器并使表返回未过滤状态，请点击[过滤器框](#)中的[重置过滤器](#)。
- 要清除过滤器中的某个原子元素，请将鼠标悬停在该元素上方，并点击该元素的 **X**。然后，点击[过滤器](#)按钮。

配置自定义视图

您可以创建自己的自定义视图，这样即可在查看事件时轻松地查看所需的列。另外，还可以编辑或删除自定义视图，但无法编辑或删除预定义的视图。

过程

步骤 1 依次选择[监控](#) > [事件](#)。

步骤 2 执行以下操作之一：

- 要基于现有自定义（或预定义）视图创建新视图，请点击该视图的选项卡，然后点击选项卡左侧的 **+** 按钮。
- 要编辑现有的自定义视图，请点击该视图的选项卡。

注释 要删除自定义视图，只需点击该视图选项卡中的 **X** 即可。删除无法撤消。

步骤 3 点击右侧事件表上方的[添加/删除列](#)链接，选择或取消选择列，直到选定列表中仅包含要包含在视图中的列为止。

点击列，并在可用（但未使用）列表和选定列表之间拖动它们。另外，您还可以点击和拖动选定列表中的列，以更改表格中从左至右的列顺序。有关列的描述，请参阅[事件字段说明](#)，第 88 页。

完成后，点击[确定](#)以保存列更改。

注释 如果在查看预定义视图时更改列选项，将会创建一个新视图。

步骤 4 如果需要，点击和拖动列分隔符可更改列宽。

过滤事件

您可以创建复杂过滤器，将事件表格限制为您当前感兴趣的事件。您可以单独或组合使用以下方法来构建过滤器：

点击列

要构建过滤器，最简单的方法就是点击事件表格中包含要基于其过滤的值的单元格。点击单元格会为该值和字段组合正确设定的规则更新**过滤器**字段。但是，使用此方法要求现有的事件列表中包含所需的值。

不能基于所有列执行过滤。如果可基于某个单元格的内容过滤，将鼠标悬停在该单元格上方时，它将显示下划线。

选择原子元素

另外，您还可以构建过滤器，具体方法为：点击**过滤器**字段，从下拉列表中选择所需的原子元素，然后再键入匹配值。这些元素包括在事件表格中未作为列显示的事件字段。另外，还包括定义您键入的值和要显示的事件之间关系的操作符。而点击列总会生成“equals (=)”过滤器，在选择元素时，还可以对数值字段选择“大于 (>)”或“小于 (<)”。

无论采用何种方式在**过滤器**字段中添加元素，均可通过在该字段中键入信息来调整运算符或值。点击**过滤器**可将过滤器应用于表格。

事件过滤器的操作符

在事件过滤器中可以使用以下操作符：

=	等于。该事件与指定值匹配。不能使用通配符。
!=	不等于。该事件与指定值不匹配。要构建不等表达式，必须键入！（感叹号）。
>	大于。该事件包含大于指定值的值。此操作符仅可用于数值，例如端口和IP地址。
<	小于。该事件包含小于指定值的值。此操作符仅可用于数值。

复杂事件过滤器的规则

在构建包含多个原子元素的复杂过滤器时，请记住以下规则：

- 相同类型的元素在该类型的所有值之间具有 OR 关系。例如，“包括发起方 IP=10.100.10.10”和“发起方 IP=10.100.10.11”与包含其中任一地址作为流量源的事件匹配。
- 不同类型的元素之间为 AND 关系。例如，“包括发起方 IP=10.100.10.10”和“目的地端口/ICMP 类型=80”与仅包含此源地址 AND 目的地端口的事件匹配。不显示从 10.100.10.10 传至不同目的地端口的事件。
- 数值元素（包括 IPv4 和 IPv6 地址）可以指定范围。例如，您可以指定“目的地端口=50-80”，以捕获此范围内端口的所有流量。使用连字符分隔开始和结束编号。并不是所有数值字段均可使用范围，例如在源元素中无法指定 IP 地址范围。
- 不能使用通配符或正则表达式。

事件字段说明

事件可包含以下信息。在查看事件详细信息时可以看到这些信息。另外，您还可以向事件查看器表格中添加列，以显示您最感兴趣的信息。

下面是可用字段的完整列表。并不是每个字段都适用于每种事件类型。请记住，任何单独事件的可用信息视系统记录连接的方式、原因和时间而异。

操作

对于连接或安全情报事件，与记录连接的访问控制规则关联的操作或默认操作：

允许

明确允许的连接。

信任

受信任的连接。信任规则在第一个数据包上检测到的 TCP 连接仅生成连接结束事件。系统将在最终会话数据包发送完毕 1 小时后生成事件。

阻止

阻止的连接。在以下条件下，阻止操作可与“允许”访问规则相关联：

- 某个攻击程序漏洞被入侵策略阻止的连接。
- 某个文件被文件策略阻止的连接。
- 被安全情报列入黑名单的连接。
- 被 SSL 策略阻止的连接。

默认操作

连接按默认操作处理。

对于文件或恶意文件事件，与文件所匹配规则的规则操作相关联的文件规则操作，以及任何关联的文件规则操作选项。

允许的连接

系统是否允许事件的流量通过。

应用

在连接中检测到的应用。

应用业务相关性

与连接中检测到的应用流量关联的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。

应用类别、应用标记

展示了应用特征的条件标准，协助您了解应用功能。

应用风险

与连接中检测到的应用流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。

阻止类型

在与事件中的流量匹配的访问控制规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

客户端应用、客户端版本

在连接中检测到的客户端应用及版本。

客户端业务相关性

与连接中检测到的客户端流量关联的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类客户端都有相关的业务相关性；该字段显示级别最低（最不相关）的业务相关性。

客户端类别、客户端标记

展示了应用特征的条件标准，协助您了解应用功能。

客户端风险

与连接中检测到的客户端流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类客户端都有一个相关风险；该字段显示最高风险。

连接

内部产生的流量的唯一 ID。

连接阻止类型指示器

在与事件中的流量匹配的访问控制规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

连接字节数

连接的总字节数。

连接时间

连接开始的时间。

连接时间戳

检测到连接的时间。

拒绝的连接

系统是否已拒绝事件的流量通过。

目标国家/地区和大洲

接收主机的国家/地区和大洲。

目标 IP

入侵、文件或恶意软件事件中的接收主机使用的 IP 地址。

目的目标端口/ICMP 代码；目的目标端口；目的目标 Icode

会话响应方使用的端口或 ICMP 代码。

方向

文件传输的方向。

处置

文件的处置：

恶意软件

表示 AMP 云将文件归类为恶意软件，或文件威胁评分超过文件策略定义的恶意软件阈值。本地恶意软件分析还可以将文件标记为恶意软件。

清洁

表示 AMP 云将文件分类为干净，或用户将文件添加到干净的列表。

未知

表示系统已查询 AMP 云，但文件尚未被分配处置情况；换句话说，AMP 云尚未对文件进行分类。

不可用

表示系统无法查询 AMP 云。您可能看到很少一部分事件为此处置；这是预期行为。

不适用

表示“检测文件”或“阻止文件”规则处理了文件，系统未查询 AMP 云。

传出接口、传出安全区

连接离开设备所通过的接口和区域。

事件、事件类型

事件的类型。

事件秒数、事件微秒数

检测到事件的时间（秒或微秒）。

文件类别

文件类型的一般类别，例如：Office 文档、存档、多媒体、可执行文件、PDF 文件、编码文件、图形或系统文件。

文件事件时间戳

文件或恶意软件文件的创建时间和日期。

文件名

文件名称。

文件规则操作

检测文件的文件策略规则的相关操作以及任何相关文件规则操作选项。

文件 SHA-256

文件的 SHA-256 散列值。

文件大小 (KB)

文件大小（千字节）。如果文件在完全接收前被系统阻止，文件大小可以为空。

文件类型

文件类型，例如 HTML 或 MSEXE。

文件/恶意软件策略

与事件生成相关的文件策略。

文件日志阻止类型指示器

在与事件中的流量匹配的文件规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

防火墙策略规则、防火墙规则

处理连接的访问控制规则或默认操作。

首个数据包

查看会话的第一个数据包的日期和时间。

HTTP 来源地址

HTTP 来源地址，表示在连接中检测到的 HTTP 流量的请求 URL 来源地址（例如提供到另一个 URL 的链接或从其导入链接的网站）。

HTTP 响应 (HTTP Response)

发送的 HTTP 状态码用于响应客户端通过连接的 HTTP 请求。

IDS 分类

生成事件的规则所属的分类。

传入接口、传入安全区

连接进入设备所通过的接口和区域。

发起方字节、发起方数据包

会话发起方发送的总字节数或数据包总数。

发起方国家/地区和大洲

发起会话的主机的国家/地区和大洲。只有发起方的 IP 地址可路由，方可用。

发起方 IP

在连接或安全情报事件中发起会话的主机 IP 地址（以及主机名，如果已启用 DNS 解析）。

内联结果

系统是否丢弃或本可丢弃触发入侵事件的数据包（如果即使运行在内联模式下操作）。空白表示触发的规则未被设置为“丢弃并生成事件”

入侵策略

启用了生成事件的规则的入侵策略。

IPS 阻止类型指示器

与事件中的流量匹配的入侵规则的操作。

最后一个数据包 (Last Packet)

查看会话的最后一个数据包的日期和时间。

MPLS 标记 (MPLS Label)

与触发此入侵事件的数据包相关的多协议标记交换标记。

恶意软件阻止类型指示器

在与事件中的流量匹配的文件规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

消息

对于入侵事件，事件的解释性文本。对于恶意软件或文件事件而言，与恶意软件事件相关的任何其他信息。

NetBIOS 域

会话中使用的 NetBIOS 域。

原始客户端国家/地区和大洲

发起会话的原始客户端的国家/地区和大洲。只有原始客户端的 IP 地址可路由，方可用。

原始客户端 IP

发起 HTTP 连接的客户端的原始 IP 地址。此地址由 X-Forwarded-For (XFF) 或 True-Client-IP HTTP 标头报头字段或其对应项目派生。

策略、策略版本

访问控制策略及其版本，包括与事件相关的访问（防火墙）规则。

优先级

事件优先级确定为思科 Talos 情报小组 (Talos)：高、中或低。

协议

连接中使用的传输协议。

原因

各种情况下的连接记录原因如下表所述。否则该字段为空。

原因	说明
文件阻止	连接中包含系统禁止传输的文件或恶意软件文件。“文件阻止”原因始终与“阻止”操作匹配。
文件监控	系统在连接中检测到特定类型的文件。
允许继续传输文件	文件传输最初被“阻止文件”或“阻止恶意软件”文件规则阻止。在部署允许该文件的新访问控制策略之后，将自动继续 HTTP 会话。
阻止继续传输文件	“检测文件”或“恶意软件云查找”文件规则最初允许文件传输。在新访问控制策略阻止文件部署之后，会自动停止 HTTP 会话。
入侵阻止	系统阻止或本可阻止在连接中检测到的漏洞（入侵策略违规）。“入侵阻止”原因与用于阻止漏洞的“阻止”操作和用于本可阻止漏洞的“允许”操作匹配。
入侵监控	系统检测到但并未阻止连接中检测到的漏洞。当触发的入侵规则状态设置为“生成事件”时，即会发生这种情况。
IP 阻止	系统未经检查就根据 IP 地址和安全情报数据拒绝连接。“IP 阻止”原因始终与“阻止”操作匹配。
SSL 阻止	系统基于 SSL 检查配置阻止加密连接。“SSL 阻止”原因始终与“阻止”操作匹配。
URL 阻止	系统未经检查就根据 URL 和安全情报数据拒绝连接。“URL 阻止”原因始终与“阻止”操作匹配。

接收时间

事件生成的日期和时间。

引用的主机 (Referenced Host)

如果连接中的协议是 HTTP 或 HTTPS，此字段显示各自协议使用的主机名。

响应方字节、响应方数据包

会话响应方发送的总字节数或数据包总数。

响应方国家/地区和大洲

响应会话的主机的国家/地区和大洲。只有响应方的 IP 地址可路由，方可用。

响应方 IP

在连接或安全情报事件中的会话响应者主机 IP 地址（以及主机名，如果已启用 DNS 解析）。

SI 类别 ID（安全情报类别）

含列入黑名单项的对象的名称，例如网络或 URL 对象名称，或情报源类别名称。

签名

文件/恶意软件事件的签名 ID。

源国家/地区和大洲

发送主机的国家/地区和大洲。只有源 IP 地址可路由，方可用。

源 IP

入侵、文件或恶意软件事件中的发送主机使用的 IP 地址。

源端口/ICMP 类型；源端口；源端口 Itype

会话发起方使用的端口或 ICMP 类型。

SSL 实际操作

系统应用于连接的实际操作。此操作可能与预期操作不同。例如，连接可能与应用解密的规则匹配，但出于某些原因不能被解密。

操作	说明
阻止/阻止并重置	表示阻止的加密连接。
解密（重新签名）	表示使用重新签名的服务器证书解密的传出连接。
解密（替换密钥）	表示使用具有替代公钥的自签名服务器证书解密的传出连接。
解密（已知密钥）	表示使用已知私钥解密的传入连接。
默认操作	表示连接采用默认操作处理。
不解密	表示系统未解密的连接。

SSL 证书指纹

用于验证证书的 SHA 哈希值。

SSL 证书状态

仅在配置了证书状态规则条件时，此字段才适用。如果加密流量与 SSL 规则匹配，则此字段显示以下一个或多个服务器证书状态值：

- 自签名
- 有效
- 无效签名
- 无效颁发者
- 已到期

- 未知
- 无效
- 已撤销

如果无法解密的流量与 SSL 规则相匹配，则此字段显示“未检查”。

SSL 加密套件

连接中使用的加密套件。

SSL 预期操作

连接匹配的 SSL 规则中指定的操作。

SSL 流标志

已加密连接的前十大调试级别标记。

SSL 流信息

在 SSL 握手期间客户端与服务器之间交换的 SSL/TLS 消息，例如 HELLO_REQUEST 和 CLIENT_HELLO。有关 TLS 连接中交换的消息的详细信息，请参阅 <http://tools.ietf.org/html/rfc5246>。

SSL 策略

应用于连接的 SSL 解密策略的名称。

SSL 规则

应用于连接的 SSL 解密规则的名称。

SSL 会话 ID

在 SSL 握手期间，在客户端与服务器之间协商的十六进制会话 ID。

SSL 通知单 ID

在 SSL 握手期间发送的会话单信息的一个十六进制哈希值。

SSL URL 类别

SSL 解密处理过程中确定的目标 Web 服务器的 URL 类别。

SSL 版本

连接中使用的 SSL/TLS 版本。

TCP 标志

在连接中检测到的 TCP 标记。

数据包总数

在=连接中传输的数据包总数，即发起方数据包 + 响应方数据包。

URL、URL 类别、URL 信誉、URL 信誉评分

会话期间受控主机请求的 URL 以及 URL 类别、信誉和信誉评分（如有）。

如果系统识别或阻止 SSL 应用，而请求的 URL 位于加密流量中，系统会基于 SSL 证书识别流量。因此，对于 SSL 应用，URL 表示包含在证书中的通用名称。

用户

与发起方 IP 地址关联的用户。

VLAN

与触发事件的数据包相关的最内部的 VLAN ID。

Web 应用业务相关性

与连接中检测到的 Web 应用流量相关的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类网络应用都有相关的业务相关性；该字段显示级别最低（最不相关）的业务相关性。

Web 应用类别、Web 应用标记

展示了 Web 应用特征的条件标准，协助您了解 Web 应用功能。

Web 应用风险

与连接中检测到的 Web 应用流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类 Web 应用都有一个相关风险；该字段显示最高风险。

Web 应用

表示连接中检测到的 HTTP 流量内容或请求的 URL 的 Web 应用。

如果 Web 应用不匹配事件的 URL，该流量大概是推荐流量，例如广告流量。如果系统检测到推荐流量，则会存储该推荐应用（如有），并将该应用列为 Web 应用。



第 5 章

思科 ISA 3000 的报警

您可以配置思科 ISA 3000 设备上的报警系统，以便在出现不正常情况时发出警告。

- [关于报警，第 97 页](#)
- [报警默认值，第 99 页](#)
- [为 ISA 3000 配置报警，第 100 页](#)
- [监控报警，第 105 页](#)

关于报警

您可以将 ISA 3000 配置为在多种条件下发出报警。如果有任何条件与配置的设置不匹配，系统会触发报警，报警的报告方式为 LED、系统日志消息、SNMP 陷阱以及连接到报警输出接口的外部设备。默认情况下，触发的报警仅会发出系统日志消息。

您可以将报警系统配置为监控以下对象：

- 电源。
- 主温度传感器和辅助温度传感器。
- 报警输入接口。

ISA 3000 具有内部传感器、2 个报警输入接口以及 1 个报警输出接口。您可以将外部传感器（如门禁传感器）连接到报警输入接口，将外部报警设备（如蜂鸣器或指示灯）连接到报警输出接口。

报警输出接口是一个中继装置。根据报警条件，中继处于连接或断开状态。当处于连接状态时，连接至该接口的任何设备都将被激活。当中继处于断开状态时，会导致连接的任何设备都处于非活动状态。只要触发了报警，中继就会保持连接状态。

有关连接外部传感器和报警中继装置的信息，请参阅[思科 ISA 3000 工业安全设备硬件安装指南](#)。

报警输入接口

您可以将报警输入接口（或触点）连接到外部传感器，例如检测门是否打开的传感器。

每个报警输入接口都有一个对应的 LED。这些 LED 负责传达每个报警输入的报警状态。您可以为每个报警输入配置触发器和严重性。除了 LED，您还可以配置触点来触发输出中继（用于激活外部报警），以发送系统日志消息和 SNMP 陷阱。

下表介绍与报警输入的报警条件所对应的 LED 状态。表中还介绍了启用这些报警输入响应时输出中继、系统日志消息和 SNMP 陷阱的行为。

报警状态	LED	输出中继	系统日志	SNMP 陷阱
未配置报警	关闭	—	—	—
未触发任何报警	绿灯常亮	—	—	—
已激活报警	次要报警 - 红色长亮 重大报警 - 红色闪烁	中继已通电	生成系统日志	发送 SNMP 陷阱
报警结束	绿灯常亮	继电器断电	生成系统日志	—

报警输出接口

您可以将外部报警（如蜂鸣器或灯光）连接到报警输出接口。

报警输出接口充当一个中继，并且还有一个对应的 LED，用于传达连接到输入接口的外部传感器以及内部传感器（例如双电源和温度传感器）的报警状态。请配置哪些报警应该激活输出中继（如果有）。

下表介绍与报警条件对应的 LED 和输出中继的状态。表中还介绍了启用这些报警响应时系统日志消息和 SNMP 陷阱的行为。

报警状态	LED	输出中继	系统日志	SNMP 陷阱
未配置报警	关闭	—	—	—
未触发任何报警	绿灯常亮	—	—	—
已激活报警	红色常亮	中继已通电	生成系统日志	发送 SNMP 陷阱
报警结束	绿灯常亮	继电器断电	生成系统日志	—

系统日志报警

默认情况下，触发任何报警时，系统都会发送系统日志消息。如果您不希望收到这些消息，可以禁用系统日志消息传递。

要使系统日志报警正常工作，您还必须在 **设备 > 系统设置 > 日志记录设置** 上启用诊断日志记录。配置系统日志服务器并启用 **系统日志过滤器**，或启用 **控制台日志记录**，或同时配置这两项。

如果未启用诊断日志记录的目标，报警系统不清楚向何处发送系统日志消息。

SNMP 陷阱报警

您可以选择配置报警，将 SNMP 陷阱发送到 SNMP 服务器。要让 SNMP 陷阱报警正常使用，您还必须配置 SNMP 设置。

使用 FlexConfig 配置 SNMP。例如，要启用到 192.168.1.25 位置 SNMP 服务器（可通过内部接口访问）的 SNMP 连接，并使用 SNMP 服务器仅接收陷阱，请创建 FlexConfig 对象以发出以下命令。将社区字符串替换为 SNMP 服务器上配置的字符串。

```
snmp-server host inside 192.168.1.25 trap
snmp-server community your-string
```

取消模板为：

```
no snmp-server host inside 192.168.1.25 trap
no snmp-server community your-string
```

创建对象后，将其添加到 FlexConfig 策略（设备 > 高级配置 > FlexConfig 策略）并将配置部署。

这是最简单的示例，适用于 SNMP 版本 1 和 2c。有关配置 SNMP 的完整信息，包括如何配置 SNMP 第 3 版，请参阅最新 ASA 软件版本的《CLI 手册 1：思科 ASA 系列常规操作 CLI 配置指南》中的 SNMP 章节。指南位置为 <https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html>。

报警默认值

下表指定了报警输入接口（触点）、冗余电源和温度的默认值。

	警报	触发	严重性	SNMP 陷阱	输出中继	系统日志消息
报警触点 1	启用	关闭状态	次要	禁用	禁用	启用
报警触点 2	启用	关闭状态	次要	禁用	禁用	启用
冗余电源（在启用时）	启用	—	—	禁用	禁用	启用
温度	为主温度报警启用（高阈值和低阈值的默认值分别为 92°C 和 -40°C） 为辅助报警禁用。	—	—	为主温度报警启用	为主温度报警启用	为主温度报警启用

为 ISA 3000 配置报警

请使用 FlexConfig 为 ISA 3000 配置报警。以下主题介绍如何配置不同类型的报警。

配置报警输入触点

如果您将报警输入触点（接口）连接到外部传感器，可以配置触点基于传感器的输入发出报警。事实上，默认启用触点，以便在关闭触点时发送系统日志消息，也即在电流停止流经触点时发送。只有当默认设置不符合您的要求时，才需要配置触点。

报警触点的编号分别是 1 和 2，您需要了解如何连接物理引脚以配置正确的设置。单独配置每个触点。

过程

步骤 1 在设备 > 高级配置中点击查看配置。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig > FlexConfig** 对象。

步骤 3 点击 + 按钮以创建新的对象。

步骤 4 为对象输入名称。例如，**Enable_Alarm_Contact**。

步骤 5 在模板编辑器中，输入配置触点所需的命令。

a) 配置报警触点的说明。

alarm contact {1 | 2} description string

例如，要将触点 1 的说明设置为“Door Open”，输入以下信息：

```
alarm contact 1 description Door Open
```

b) 配置报警触点的严重性。

alarm contact {1 | 2 | any} severity {major | minor | none}

您可以指定 **any** 更改所有触点的严重性，而不是配置一个触点。严重性控制与触点关联的 LED 指示灯的行为。

- **major**- LED 指示灯红色闪烁。
- **minor**- LED 指示灯红色长亮。这是默认值。
- **none**- LED 指示灯熄灭。

例如，要将触点 1 的严重级别设置为“Major”，可输入以下信息：

```
alarm contact 1 severity major
```

c) 配置报警触点的触发器。

alarm contact {1 | 2 | any} trigger {open | closed}

您可以指定 **any** 更改所有触点的触发器，而不是配置一个触点。触发器决定发出报警信号的电气条件。

- **open**- 触点的正常状态为关闭，即电流流经触点。如果触点变成打开状态，即电流停止流动，会触发警报。
- **closed**- 触点的正常状态为打开，即电流不通过触点。如果触点变成关闭状态，即电流开始流经触点，会触发警报。这是默认值。

例如，将门禁传感器连接到报警输入触点 1，该触点的正常状态为没有电流流经报警触点（即打开）。如果门被打开，触点会变成关闭状态，电流将流经报警触点。您应将报警触发器设为关闭，以便当电流开始流动时，警报响起。

```
alarm contact 1 trigger closed
```

d) 配置触发报警触点时采取的操作。

alarm facility input-alarm {1 | 2} {relay | syslog | notifies}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。默认情况下，此选项已启用。
- **通知** - 发送 SNMP 陷阱。

例如，要启用报警输入触点 1 的所有操作，请输入以下命令：

```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

步骤 6 在取消模板编辑器中，输入撤消此配置所需的命令。

所有这些命令采用 **no** 形式来将其禁用并恢复默认设置。例如，如果您的模板包含此过程中所示的所有命令示例，取消模板如下：

```
no alarm contact 1 description Door Open
no alarm contact 1 severity major
no alarm contact 1 trigger closed
no alarm facility input-alarm 1 relay
no alarm facility input-alarm 1 syslog
no alarm facility input-alarm 1 notifies
```

步骤 7 点击**确定**保存对象。

步骤 8 将对象添加到 FlexConfig 策略中。

- 点击目录中的 **FlexConfig** 策略。
- 在组列表中点击 +。
- 选择 Enable_Alarm_Contact 对象，然后点击**确定**。

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

d) 点击**保存**。

您现在可以部署策略。

步骤 9 部署完成后，在 CLI 控制台或 SSH 会话中使用 **show running-config** 命令，验证对运行配置的更改是否正确。测试外部传感器，验证是否可以触发警报。

配置电源报警

ISA 3000 包含两个电源。默认情况下，系统在单电源模式下运行。但是，您可以配置系统在双电源模式下运行，其中第二个电源会在主电源发生故障时自动供电。启用双电源模式时，自动启用电源警报来发送系统日志警报，但您可以完全禁用警报，或同时启用 SNMP 陷阱或警报硬件中继。

以下过程说明如何启用双电源模式下，以及如何配置电源报警。

过程

步骤 1 在设备 > 高级配置中点击**查看配置**。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig > FlexConfig** 对象。

步骤 3 点击 + 按钮以创建新的对象。

步骤 4 为对象输入名称。例如，**Enable_Power_Supply_Alarm**。

步骤 5 在模板编辑器中，输入配置电源警报所需的命令。

a) 启用双电源模式。

power-supply dual

例如：

```
power-supply dual
```

b) 配置触发电源警报时要采取的操作。

alarm facility power-supply rps {relay | syslog | notifies | disable}

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。默认情况下，此选项已启用。
- **通知** - 发送 SNMP 陷阱。
- **禁用** - 禁用电源报警。为电源报警配置的任何其他操作都无法运行。

例如，要启用电源警报的所有操作，请输入以下命令：

```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

步骤 6 在取消模板编辑器中，输入撤消此配置所需的命令。

所有这些命令采用 **no** 形式来将其禁用并恢复默认设置。例如，如果您的模板包含此过程中所示的所有命令示例，取消模板如下：

```
no power-supply dual
no alarm facility power-supply rps relay
no alarm facility power-supply rps syslog
no alarm facility power-supply rps notifies
```

步骤 7 点击确定保存对象。

步骤 8 将对象添加到 FlexConfig 策略中。

- a) 点击目录中的 **FlexConfig** 策略。
- b) 在组列表中点击 +。
- c) 选择 **Enable_Power_Supply_Alarm** 对象，然后点击确定。

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

- d) 点击保存。

您现在可以部署策略。

步骤 9 部署完成后，在 CLI 控制台或 SSH 会话中使用 **show running-config** 命令，验证对运行配置的更改是否正确。

配置温度报警

您可以配置基于设备中 CPU 卡温度的警报。

您可以设置主要和辅助温度范围。如果温度低于低阈值，或超过高阈值，则触发警报。

默认对所有报警操作启用主温度报警：输出中继、系统日志和 SNMP。主要温度范围的默认设置为 -40°C 至 92°C。

默认情况下，禁用辅助温度警报。您可以将辅助温度范围设置为 -35°C 至 85°C。

由于辅助温度范围比主范围更严格，如果您设置辅助低温度或高温度，该设置将禁用对应的主要设置，即使您为主设置配置非默认值。您不能启用两个单独的高温度报警和两个单独的低温度报警。

因此，在实践中，您应为高温度和低温度仅配置主要设置或仅配置辅助设置。

过程

步骤 1 在设备 > 高级配置中点击查看配置。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig > FlexConfig** 对象。

步骤 3 点击 + 按钮以创建新的对象。

步骤 4 为对象输入名称。例如，**Enable_Temperature_Alarm**。

步骤 5 在模板编辑器中，输入配置温度报警所需的命令。

a) 配置可接受的温度范围。

```
alarm facility temperature {primary | secondary} {low | high} temperature
```

温度单位为摄氏度。主要报警的允许范围为 -40 至 92，这也是默认的范围。辅助报警的允许范围是 85 到 -35。低值必须小于高值。

例如，要设置更严格的 -20 至 80 温度范围（在辅助报警的允许范围内），请按如下所示配置辅助报警：

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

b) 配置触发温度警报时要采取的操作。

```
alarm facility temperature {primary | secondary} {relay | syslog | notifies}
```

您可以配置多个操作。例如，您可以配置设备以激活外部报警，发送系统日志消息，以及发送 SNMP 陷阱。

- **中继** - 启动报警输出中继，激活连接的蜂鸣器或闪烁灯等外部警报。输出 LED 指示灯也会变成红色。
- **系统日志** - 发送系统日志消息。
- **通知** - 发送 SNMP 陷阱。

例如，要启用辅助温度报警的所有操作，请输入以下命令：

```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

步骤 6 在取消模板编辑器中，输入撤消此配置所需的命令。

所有这些命令采用 **no** 形式来恢复默认设置（针对主要报警）或将其禁用（针对辅助警报）。例如，如果您的模板包含此过程中所示的所有命令示例，取消模板如下：

```
no alarm facility temperature secondary low -20
no alarm facility temperature secondary high 80
no alarm facility temperature secondary relay
no alarm facility temperature secondary syslog
no alarm facility temperature secondary notifies
```

步骤 7 点击确定保存对象。

步骤 8 将对象添加到 FlexConfig 策略中。

- a) 点击目录中的 **FlexConfig 策略**。
- b) 在组列表中点击 +。
- c) 选择 `Enable_Temperature_Alarm` 对象，然后点击**确定**。

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

- d) 点击**保存**。

您现在可以部署策略。

步骤 9 部署完成后，在 CLI 控制台或 SSH 会话中使用 `show running-config` 命令，验证对运行配置的更改是否正确。

监控报警

以下主题介绍如何监控和管理报警。

监控报警状态

您可以在 CLI 中使用以下命令监控报警。

- **show alarm settings**

显示每个可能的报警的当前配置。

- **show environment alarm-contact**

显示输入报警触点的物理状态信息。

- **show facility-alarm relay**

显示有关已触发输出中继的警报信息。

- **show facility-alarm status [info | major | minor]**

显示所有已触发警报的信息。您可以通过过滤 **major** 或 **minor** 状态来限制视图。**info** 关键字提供与不使用关键字时相同的视图。

监控报警系统日志消息

根据您的报警类型，您可能会看到以下系统日志消息。

双电源报警

- %FTD-1-735005: 电源设备冗余正常
- %FTD-1-735006: 电源设备冗余丢失

温度报警

在这些报警中，*Celsius* 将替换为设备上检测到的温度，以摄氏为单位。

- %FTD-6-806001: 主警报 CPU 温度高 *Celsius*
- %FTD-6-806002: CPU 高温主警报已清除
- %FTD-6-806003: 主警报 CPU 温度低 *Celsius*
- %FTD-6-806004: CPU 低温主警报已清除
- %FTD-6-806005: 辅助警报 CPU 温度高 *Celsius*
- %FTD-6-806006: CPU 高温辅助警报已清除
- %FTD-6-806007: 辅助警报 CPU 温度低 *Celsius*
- %FTD-6-806008: CPU 低温辅助警报已清除

报警输入触点警报

在这些警报中，*description* 是您所配置触点的说明。

- %FTD-6-806009: 与 *ALARM_IN_1 alarm_1_description* 对应的警报已确定
- %FTD-6-806010: 与 *ALARM_IN_1 alarm_1_description* 对应的警报已清除
- %FTD-6-806011: 与 *ALARM_IN_2 alarm_2_description* 对应的警报已确定
- %FTD-6-806012: 与 *ALARM_IN_2 alarm_2_description* 对应的警报已清除

关闭外部报警

如果您使用连接到警报输出的外部报警，并触发了报警，可以使用 **clear facility-alarm output** 命令从设备 CLI 关闭外部报警。此命令会断开输出引脚，同时关闭输出 LED。



第 II 部分

可重用对象

- [对象](#)，第 109 页
- [证书](#)，第 121 页
- [身份源](#)，第 129 页



第 6 章

对象

对象是可重用容器，用于定义在策略或其他设置中要使用的条件。例如，网络对象定义主机和子网地址。

对象允许您定义条件，这样即可在不同策略中重新使用相同的条件。在更新对象时，将自动更新使用该对象的所有策略。

- [对象类型](#)，第 109 页
- [管理对象](#)，第 111 页

对象类型

可以创建以下类型的对象。在大多数情况下，如果策略或设置允许使用对象，则必须使用对象。

对象类型	主要用途	说明
AnyConnect 客户端配置文件	远程接入 VPN。	AnyConnect 客户端配置文件随 AnyConnect 客户端软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及是否允许终端用户更改 AnyConnect 客户端首选项和高级设置中的选项。 请参阅 配置并上传客户端配置文件 ，第 411 页。
应用过滤器	访问控制规则。	应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。 请参阅 配置应用过滤器对象 ，第 115 页。
证书	身份策略。 远程接入 VPN。 SSL 解密规则。	数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。 请参阅 配置证书 ，第 124 页。

对象类型	主要用途	说明
DNS 组	管理和数据接口的 DNS 设置。	DNS 组定义 DNS 服务器列表和某些相关联的属性。需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 <code>www.example.com</code> 。 请参阅 配置 DNS 组 ，第 452 页。
地理位置	安全策略。	地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。 请参阅 配置地理位置对象 ，第 118 页。
身份源	身份策略。 远程接入 VPN。 Firepower 设备管理器访问。	身份源是定义用户账户的服务器和数据库。身份源信息具有多种用途，例如提供与 IP 地址关联的用户身份，或是对远程接入 VPN 连接或到 Firepower 设备管理器的访问进行身份验证。 请参阅 身份源 ，第 129 页。
IKE 策略	VPN。	互联网密钥交换 (IKE) 策略对象定义用于对 IPsec 对等体进行身份验证、协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的 IKE 提议。IKEv1 和 IKEv2 有单独的对象。 请参阅 配置全局 IKE 策略 ，第 384 页。
IPsec 提议	VPN。	IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。IKEv1 和 IKEv2 有单独的对象。 请参阅 配置 IPsec 提议 ，第 388 页。
网络	安全策略和各种设备设置。	网络组和网络对象（统称为“网络对象”）定义主机或网络的地址。 请参阅 配置网络对象和组 ，第 112 页。
端口	安全策略。	端口组和端口对象（统称为“端口对象”）定义流量的协议、端口或 ICMP 服务。 请参阅 配置端口对象和组 ，第 113 页。
密钥	Smart CLI 和 FlexConfig 策略。	密钥对象定义要加密和隐藏的密码或其他身份验证字符串。 请参阅 配置密钥对象 ，第 521 页。
安全区	安全策略。	安全区是一组接口。区域将网络划分网段，帮助您管理流量以及对流量进行分类。 请参阅 配置安全区 ，第 114 页。

对象类型	主要用途	说明
系统日志服务器	访问控制规则。 诊断日志记录。 安全情报策略。 SSL 解密规则。 入侵策略。	系统日志服务器对象标识可接收面向连接的消息或诊断系统日志（系统日志）消息的服务器。 请参阅 配置系统日志服务器 ，第 119 页。
URL	访问控制规则。 安全情报策略。	URL 对象和组（统称为“URL 对象”）定义网络请求的 URL 或 IP 地址。 请参阅 配置 URL 对象和组 ，第 117 页。
用户	远程接入 VPN。	您可以直接在设备上创建与远程接入 VPN 搭配使用的用户账户。您可以使用本地用户账户代替外部身份验证源，或与后者搭配使用。 请参阅 配置本地用户 ，第 141 页。

管理对象

您可以直接通过“对象”页面配置对象，也可以在编辑策略时进行配置。两种方法得到的结果相同：新对象或更新的对象，所以请使用当下符合您需求的方法。

以下程序介绍如何直接通过“对象”页面创建和管理对象。





注释 在编辑策略或设置时，如果属性需要对象，系统将会为您显示已定义的对象列表，从中您可以选择适当的对象。如果所需的对象不存在，只需点击列表中所显示的[创建新对象](#)链接即可。

过程

步骤 1 选择对象。

“对象”页面由一个目录，其中列出了可用的对象类型。在选择对象类型时，您会看到现有对象的列表，并可在此处创建新对象。另外，还可看到对象内容和类型。

步骤 2 从目录中选择对象类型，并执行以下任一操作：

- 要创建对象，请点击 + 按钮。对象的内容视类型而异；有关每个对象类型的信息，请参阅配置主题。
- 要创建组对象，请点击添加组 () 按钮。组对象包含多个项目。
- 要编辑对象，请点击该对象的编辑图标 ()。无法编辑预定义对象的内容。

- 要删除对象，请点击该对象的删除图标 (🗑️)。如果某个策略或其他对象目前正在使用对象，或者对象为预定义对象，则无法将其删除。

配置网络对象和组

使用网络组和网络对象（统称为“网络对象”）可定义主机或网络的地址。然后，您可以在安全策略中使用这些对象来定义流量匹配条件，或在设置中使用它们来定义服务器或其他资源的地址。

网络对象定义单个主机或网络地址，而网络组对象可以定义多个地址。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在编辑地址属性时，点击对象列表中所示的**创建新网络**链接来创建网络对象。

过程

步骤 1 选择对象，然后从目录中选择网络。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要创建组，请点击添加组 (📁) 按钮。
- 要编辑对象或组，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 输入对象的名称和描述（后者为可选项），并定义对象内容。

我们建议不要单独使用 IP 地址作为名称，以便您可以轻松地从对象内容或独立 IP 地址中识别对象名称。如果您想要在名称中使用 IP 地址，请添加一个有意义的前缀，例如 host-192.168.1.2 或 network-192.168.1.0。如果您使用 IP 地址作为名称，系统将添加一条竖线作为前缀，例如 |192.168.1.2。FDM 不会在对象选择器中显示这条竖线，但如果您在 CLI 中使用 **show running-config** 命令检查运行配置，您将看到此命名标准。

步骤 4 配置对象的内容。

网络对象

选择对象类型并配置内容：

- **网络** - 使用以下格式之一输入网络地址：
 - IPv4 网络（包含子网掩码），例如 10.100.10.0/24 或 10.100.10.0/255.255.255.0。
 - IPv6 网络（包括前缀），例如 2001:DB8:0:CD30::/60。
- **主机** - 使用以下格式之一输入主机 IP 地址：
 - IPv4 主机地址，例如 10.100.10.10。

- IPv6 主机地址，例如 2001:DB8::0DB8:800:200C:417A 或 2001:DB8:0:0:0DB8:800:200C:417A。
- **FQDN** - 输入完全限定域名，例如 www.example.com。不能使用通配符。此外，请选择 **DNS 解析** 确定是否要将 IPv4 地址、IPv6 地址，或这两个地址与 FQDN 关联。默认值为 IPv4 和 IPv6 这两个地址。只能在访问控制规则中使用这些对象。规则匹配通过 DNS 查找获取的 FQDN IP 地址。

网络组

点击 + 按钮，以选择要添加到组中的网络对象。另外，也可以创建新对象。

步骤 5 点击 **OK**，保存更改。

配置端口对象和组

使用端口组和端口对象（统称为“端口对象”）可定义流量的协议、端口或 ICMP 服务。然后，可以在安全策略中使用这些对象来定义流量匹配条件，例如使用访问规则来允许流量传送至特定 TCP 端口。

端口对象定义单一协议、TCP/UDP 端口、端口范围或 ICMP 服务，而端口组对象可定义多项服务。

该系统中包括多个针对通用服务的预定义对象。您可以在策略中使用这些对象，但无法编辑或删除系统定义的对象。



注释 在创建端口组对象时，请确保合理组合对象。例如，如果在访问规则中使用某个对象指定源端口和目的端口，则不能在该对象中混合使用多个协议。在编辑已使用的对象时请务必小心，否则可能导致使用该对象的策略无效（和被禁用）。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在编辑服务属性时，点击对象列表中所示的 **创建新端口** 链接来创建端口对象。

过程

步骤 1 选择对象，然后从目录中选择端口。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要创建组，请点击 **添加组** (📁) 按钮。
- 要编辑对象或组，请点击该对象的编辑图标 (🔍)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 输入对象的名称和描述（后者为可选项），并定义对象内容。

端口对象

选择协议，然后按以下所示配置该协议：

- **TCP、UDP** - 输入单一端口或端口范围编号，例如 80（适用于 HTTP）或 1-65535（涵盖所有端口）。
- **ICMP、IPv6-ICMP** - 选择 ICMP 类型和代码（可选）。选择 **Any** 类型可应用于所有 ICMP 消息。有关类型和代码的信息，请参阅以下页面：
 - ICMP - <http://www.iana.org/assignments/icmp-parameters/icmp-parameters.xml>
 - ICMPv6 - <http://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xml>
- **其他** - 选择所需协议。

端口组

点击 + 按钮，以选择要添加至该组的端口对象。另外，也可以创建新对象。

步骤 4 点击 **OK**，保存更改。

配置安全区

安全区是一组接口。区域将网络划分网段，帮助您管理流量以及对流量进行分类。您可以定义多个区域，但一个给定接口只能位于一个区域中。

系统将在初始配置期间创建以下区域。您可以编辑这些区域以添加或移除接口；如果不再使用这些区域，也可以删除它们。

- **inside_zone** - 包括内部接口。如果内部接口为桥接组，则此区域包括所有桥接组成员接口，而不是内部网桥虚拟接口 (BVI)。此区域用于表示内部网络。
- **outside_zone** - 包括外部接口。此区域用于表示在您控制之外的网络，例如互联网。

通常，按接口在网络中扮演的角色对它们分组。例如，可将连接至互联网的接口放在 **outside_zone** 安全区，并将内部网络的所有接口放在 **inside_zone** 安全区。然后，可以对来自外部区域和传至内部区域的流量应用访问控制规则。

在创建区域之前，请考虑要应用至网络的访问规则和其他策略。例如，无需将所有内部接口都放到同一个区域。如果您有 4 个内部网络，并希望将其中一个与另外三个区别对待，则可以创建两个区域（而不是一个区域）。如果有一个接口需允许外部访问公共 Web 服务器，您可能希望对该接口使用单独的区域。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在编辑安全区属性时，点击对象列表中所示的**创建新安全区**链接来创建安全区。

过程

步骤 1 选择对象，然后从目录中选择安全区。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 输入对象的名称和描述（后者为可选项）。

步骤 4 选择区域的模式。

此模式与接口模式直接关联，可以是路由或被动模式。区域可以包含一种类型的接口。对于直通流量的普通区域，请选择路由。

步骤 5 在接口列表中，点击 + 并选择要添加到该区域的接口。

列表中 will 显示当前不在该区域的所有已命名接口。只有配置接口并为其指定了名称，才能将其添加到该区域。

如果所有已命名接口均已在该区域内，则列表为空。如果要尝试将某个接口移到其他区域，则首先必须将其从当前区域中删除。

注释 您不能将桥接组接口 (BVI) 添加到某个区域，而只能添加成员接口。您可以将成员接口放到不同的区域中。

步骤 6 点击 **OK**，保存更改。

配置应用过滤器对象

应用过滤器对象定义 IP 连接中使用的应用，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。您可以在策略中使用这些对象而不是使用端口规格来控制流量。

虽然您可以指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

您可以直接在策略中选择应用和应用过滤器，而不使用应用过滤器对象。但是，如果要为同一组应用或过滤器创建多个策略，使用对象则非常方便。该系统包括多个预定义的应用过滤器，您不能编辑或删除它们。



注释 思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在编辑访问控制规则时，在向“应用”选项卡中添加应用条件后点击**另存为过滤器**链接来创建应用过滤器对象。

开始之前

编辑过滤器时，如果所选应用已由 VDB 更新删除，则会在应用名称后显示“(Deprecated)”。必须从过滤器中删除这些应用，否则将阻止后续部署和系统软件升级。

过程

步骤 1 选择对象，然后从目录中选择应用过滤器。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 输入对象的名称和描述（后者为可选项）。

步骤 4 在应用列表中，点击**添加 +** 并选择要添加到该对象的应用和过滤器。

初始列表将在连续滚动的列表中显示应用。点击**高级过滤器**可查看过滤器选项，可更加方便地查看和选择应用。完成选择后，点击**添加**。您可以重复该过程，以添加更多应用或过滤器。

注释 单个过滤器条件中的多个选项具有 OR 关系。例如，风险高 OR 非常高。过滤器之间的关系是 AND，因此是风险高 OR 非常高，AND 业务相关性低 OR 非常低。在选择过滤器时，显示屏中的应用列表更新，只显示符合条件标准的应用。您可以使用这些过滤器来帮助查找要单独添加的应用，或确认是否要选择所需的过滤器以添加到规则中。

风险

应用所用的用途可能违反组织安全策略的可能性，从非常低到非常高。

业务相关性

在组织的业务运营环境下使用应用的可能性，与娱乐相对，从非常低到非常高。

类型

应用类型：

- **应用协议** - 应用协议（例如 HTTP 和 SSH），代表主机之间的通信。
- **客户端协议** - 客户端（例如 Web 浏览器和邮件客户端），代表主机上运行的软件。
- **Web 应用** - Web 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL。

类别

说明应用的最基本功能的应用通用分类。

标记

关于应用的其他信息，与类别类似。

对于加密流量，系统可以仅使用标记有 **SSL 协议** 的应用识别和过滤流量。只有在未加密或已解密的流量中才能检测到没有此标记的应用。此外，系统仅将**已解密的流量**标记分配给可在已解密的流量中检测到的应用，而不会将它们分配给加密或未加密的流量中检测到的应用。

应用列表（显示屏底部）

在从列表上方的选项中选择过滤器时，此列表将进行更新，所以您可查看当前符合过滤器的应用。在计划将过滤器条件添加到规则中时，使用此列表可确认您的过滤器是否针对所需的应用。如果您计划添加特定应用，请从此列表中选择它们。

步骤 5 点击 **OK**，保存更改。

配置 URL 对象和组

使用 URL 对象和组（统称为“URL 对象”）可定义 Web 请求的 URL 或 IP 地址。可以使用这些对象在访问控制策略中执行手动 URL 过滤，或在安全情报策略中进行阻止。

URL 对象定义单个 URL 或 IP 地址，而 URL 组对象可以定义多个 URL 或地址。

在创建 URL 对象时，请记住以下要点：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果主机名位于 `://` 分隔符之后，或在主机名中的任何点之后，则认为该主机名匹配。例如，`ign.com` 匹配 `ign.com` 和 `www.ign.com`，但不匹配 `verisign.com`。
- 如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配，其中包括服务器名称、路径和任何查询参数。但是，我们建议您不要使用手动 URL 过滤阻止或允许个别网页或部分网站，因为这样可能会重组服务器并将页面移至新路径。子字符串匹配还可能导致意外匹配，其中 URL 对象中包含的字符串也与非预期服务器上的路径或查询参数中的字符串匹配。
- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 `example.com` 而不是 `http://example.com`。
- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的主题公用名创建该对象。此外，系统会忽略在主题公用名中的子域，因此，不包括子域信息。例如，使用 `example.com` 而不是 `www.example.com`。

但请注意，证书中的使用者公用名可能与网站的域名完全无关。例如，`youtube.com` 证书中的使用者公用名是 `*.google.com`（当然，这可能会随时更改）。如果使用 SSL 解密策略解密 HTTPS 流量以便 URL 过滤规则可用于解密策略，则可能获得更一致的结果。



注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能得到不一致的 HTTPS 连接结果。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在编辑 URL 属性时，点击对象列表中所显示的**创建新 URL** 链接来创建 URL 对象。

过程

步骤 1 选择对象，然后从目录中选择 URL。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要创建组，请点击**添加组** (📁) 按钮。
- 要编辑对象或组，请点击该对象的编辑图标 (✎)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 输入对象的名称和描述（后者为可选项）。

步骤 4 定义对象内容。

URL 对象

在 URL 框中输入 URL 或 IP 地址。在 URL 中不能使用通配符。

URL 组

点击 + 按钮选择要添加到组中的 URL 对象。另外，也可以创建新对象。

步骤 5 点击 **OK**，保存更改。

配置地理位置对象

地理位置对象定义托管设备（流量的源或目的）的国家/地区和大洲。您可以在策略中使用这些对象而不是使用 IP 地址来控制流量。例如，使用地理位置可以很容易地将访问权限限制为特定国家/地区，而无需知道此处使用的所有潜在 IP 地址。

通常，可以直接在策略中选择地理位置，而无需使用地理位置对象。但是，如果要为同一组国家/地区或大洲创建多个策略，使用对象则非常方便。



注释 为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在编辑网络属性时，点击对象列表中所示的[创建新地理位置](#)链接来创建地理位置对象。

过程

步骤 1 选择对象，然后从目录中选择地理位置。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 输入对象的名称和描述（后者为可选项）。

步骤 4 在大洲/国家/地区列表中，点击添加 + 并选择要添加到该对象的大洲和国家/地区。

选择大陆将会选择该大陆内的所有国家/地区。

步骤 5 点击 **OK**，保存更改。

配置系统日志服务器

系统日志服务器对象标识可接收面向连接的消息或诊断系统日志（系统日志）消息的服务器。如果已为日志收集和分析设置一台系统日志服务器，请创建对象以进行定义并在相关策略中使用这些对象。

可以将下列类型的事件发送至系统日志服务器：

- 连接事件。根据下列策略类型配置系统日志服务器对象：访问控制规则和默认操作、SSL 解密规则和默认操作、安全情报策略。
- 入侵事件。根据入侵策略配置系统日志服务器对象。
- 诊断事件。请参阅[配置诊断日志记录](#)，第 449 页。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。此外，也可以在编辑系统日志服务器属性时，点击对象列表中所示的[添加系统日志服务器](#)链接来创建系统日志服务器对象。

过程

步骤 1 选择对象，然后从目录中选择系统日志服务器。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。

- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 配置系统日志服务器的属性：

- **IP 地址** - 输入系统日志服务器的 IP 地址。
- **协议类型、端口号** - 选择用于系统日志的协议并输入端口号。默认值为 UDP/514。如果您选择 **TCP**，系统可以识别何时系统日志服务器不可用，并停止发送事件，直至服务器再次可用。默认 UDP 端口为 514，默认 TCP 端口为 1470。如果您更改默认值，端口范围必须介于 1025 至 65535 之间。
- **用于设备日志的接口** - 选择应使用哪个接口发送诊断系统日志消息。以下类型的事件始终使用管理接口：连接、入侵。接口选择决定与系统日志消息关联的 IP 地址。选择以下选项之一：
 - **数据接口** - 选择用于诊断系统日志消息的数据接口。如果可以通过桥接组成员接口访问该服务器，请改而选择该桥接组接口 (BVI)。如果通过诊断接口（物理管理接口）访问，我们建议您选择**管理接口**，而不是此选项。您不能选择被动接口。
对于连接和入侵系统日志消息，源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。
 - **管理接口** - 对所有类型的系统日志消息使用虚拟管理接口。源 IP 地址是管理接口的地址；如果您通过数据接口进行路由，则是网关接口的地址。

步骤 4 点击 **OK**，保存更改。



第 7 章

证书

数字证书是一种用于身份验证的数字识别方式。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。以下主题介绍如何创建和管理证书。

- [关于证书，第 121 页](#)
- [配置证书，第 124 页](#)

关于证书

数字证书是一种用于身份验证的数字识别方式。数字证书包括用于识别设备或用户的信息，例如名称、序列号、公司、部门或 IP 地址。数字证书还包括用户或设备的公钥副本。证书用于 SSL（安全套接字层）、TLS（传输层安全）和 DTLS（数据报 TLS）连接，例如 HTTPS 和 LDAPS。

您可以创建以下类型的证书：

- **内部证书** - 内部身份证书是用于特定系统或主机的证书。您可以使用 **OpenSSL** 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名证书。
- **内部证书颁发机构 (CA) 证书** - 内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。您可以使用 **OpenSSL** 工具包自己生成这些证书，也可以从证书颁发机构获取这些证书。此外，您还可以生成自签名的内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。
- **可信证书颁发机构 (CA) 证书** - 可信的 CA 证书可用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

证书颁发机构 (CA) 是指“签署”证书以确认其真实性，从而确保设备或用户的身份的可信颁发机构。CA 在 PKI（使用公钥或私钥加密以确保安全性）的情景下颁发数字证书。CA 可以是可信的第三方（例如 **VeriSign**），也可以是组织内建立的私有（内部）CA。CA 负责管理证书请求和颁发数字证书。有关详细信息，请参阅 [公钥加密，第 122 页](#)。

公钥加密

在 RSA 加密系统等公钥加密中，每位用户都有一个包含公钥和私钥的密钥对。这一对密钥相互补充，用其中一个密钥加密的任何内容都可用另一个密钥解密。

简言之，使用私钥加密数据时会形成一个签名。此签名附加在数据中并发送给接收者。接收者对数据应用发送者的公钥。如果随数据一起发送的签名与对数据应用公钥的结果一致，就会确立消息的有效性。

此过程的前提是接收者拥有发送者的公钥副本而且非常确定此密钥属于发送者，而不是伪装成发送者的其他人。

获取发送方公钥通常是在外部处理或通过安装时执行的操作处理。例如，默认情况下，大多数 Web 浏览器都使用若干 CA 的根证书进行配置。

您可以通过 opendss.org、维基百科或其他来源了解有关数字证书和公钥加密的更多信息。充分了解 SSL/TLS 加密有助于您为自己的设备建立安全连接。

功能使用的证书类型

您需要为每个功能创建正确类型的证书。以下功能需要证书。

身份策略（强制网络门户） - 内部证书

（可选。）强制网络门户用于身份策略中。在向设备进行身份验证时，为了标识自己的身份并获得与其用户名关联的 IP 地址，用户必须接受此证书。如果不提供证书，设备将使用自动生成的证书。

身份领域（身份策略和远程接入 VPN） - 受信任的 CA 证书

（可选。）如果对目录服务器进行加密连接，则必须接受证书才能在目录服务器上执行身份验证。当系统按身份和远程接入 VPN 策略提示用户进行身份验证时，用户必须进行身份验证。如果不对目录服务器使用加密，则不需要证书。

远程接入 VPN - 内部证书

（必需。）内部证书用于外部接口，在 AnyConnect 客户端与设备进行连接时确定客户端的设备身份。客户端必须接受此证书。

SSL 解密策略 - 内部、内部 CA 和受信任 CA 证书

（必需。）SSL 解密策略将证书用于以下目的：

- 内部证书用于已知的密钥解密规则。
- 在客户端和 FTD 设备之间创建会话时，内部 CA 证书用于解密重签名规则。
- 在 FTD 设备和服务器之间创建会话时，受信任 CA 证书直接用于解密重签名规则。与其他证书不同，这些证书不能直接在 SSL 解密策略中配置，而是需要上传到系统。系统包括大量受信任 CA 证书，因此，您无需上传任何其他证书。

示例：使用 OpenSSL 生成内部证书

以下示例使用 OpenSSL 命令生成内部服务器证书。您可以从 [openssl.org](https://www.openssl.org) 获取 OpenSSL。有关具体信息，请查阅 OpenSSL 文档。此示例中使用的命令可能会更改，您还可以使用其他您可能想要使用的可用选项。

此程序旨在让您了解如何获取要上传到 FTD 的证书。



注释 这里显示的 OpenSSL 命令仅作为示例。调整参数以满足您的安全要求。

过程

步骤 1 生成密钥。

```
openssl genrsa -out server.key 4096
```

步骤 2 生成证书签名请求 (CSR)。

```
openssl req -new -key server.key -out server.csr
```

步骤 3 使用密钥和 CSR 生成自签证书。

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

由于 Firepower 设备管理器不支持加密的密钥，请尝试在生成自签证书时按回车键跳过质询密码。

步骤 4 在 Firepower 设备管理器中创建内部证书对象时，将文件上传到相应的字段。

您还可以复制/粘贴文件内容。示例命令创建以下文件：

- `server.crt` - 将内容上传或粘贴到“服务器证书”字段中。
- `server.key` - 将内容上传或粘贴到“证书密钥”字段中。如果您在生成密钥时提供了密码，则可以使用以下命令对其进行解密。输出发送到 `stdout`，您可以从其中复制它。

```
openssl rsa -in server.key -check
```

配置证书

FTD支持 PEM 或 DER 格式的 X509 证书。如果需要，可使用 OpenSSL 生成证书、从受信任的证书颁发机构获取证书或创建自签名证书。

有关证书的详细信息，请参阅[关于证书](#)，第 121 页。

有关每项功能所用证书类型的信息，请参阅[功能使用的证书类型](#)，第 122 页。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。此外，也可以在编辑证书属性时，点击对象列表中所示的[创建新证书](#)链接来创建证书对象。

过程

步骤 1 选择对象，然后从目录中选择证书。

系统提供以下预定义证书（您可以按原样使用或替换更换它们）。

- DefaultInternalCertificate
- NGFW-Default-InternalCA

此外，系统还包括许多从第三方证书颁发机构获取的受信任的 CA 证书。SSL 解密策略可使用这些证书执行解密重新签署操作。

步骤 2 执行以下操作之一：

- 要创建新的证书对象，请使用 + 菜单中适合证书类型的命令。
- 要查看或编辑证书，请点击证书的编辑图标 (🔗) 或视图图标 (📄)。
- 要删除未引用的证书，请点击证书的垃圾桶图标 (🗑️)。

有关创建或编辑证书的详细信息，请参阅下列主题：

- [上传内部和内部 CA 证书](#)，第 124 页
- [生成自签名的内部和内部 CA 证书](#)，第 126 页
- [上传受信任的 CA 证书](#)，第 127 页

上传内部和内部 CA 证书

内部身份证书是特定系统或主机的证书。

内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。

您可以使用 OpenSSL 工具包自行生成这些证书，也可以从证书颁发机构获取证书，然后再按照以下步骤程序上传证书。有关生成密钥的示例，请参阅[示例：使用 OpenSSL 生成内部证书，第 123 页](#)。

此外，您还可以生成自签名的内部身份和内部 CA 证书。如果配置自签名的内部 CA 证书，该 CA 将在设备自身上运行。有关创建自签名证书的信息，请参阅[生成自签名的内部和内部 CA 证书，第 126 页](#)。

有关使用这些证书的功能的信息，请参阅[功能使用的证书类型，第 122 页](#)。

过程

步骤 1 选择对象，然后从目录中选择证书。

步骤 2 执行以下操作之一：

- 依次点击 + > 添加内部证书，然后点击上传证书和密钥。
- 依次点击 + > 添加内部 CA 证书，然后点击上传证书和密钥。
- 要编辑或查看证书，请点击信息图标 (i)。对话框中将显示证书主题、颁发者和有效时间范围。点击“替换证书”即可上传新的证书和密钥。此外，您还可以在对话框中粘贴证书和密钥。

步骤 3 键入证书的名称。

该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 4 点击上传证书（或在编辑时点击替换证书），并选择证书文件（例如 *.cert）。允许的文件扩展名有 .pem、.cert、.cer、.crt 和 .der。或者，粘贴证书。

该证书必须为 PEM 或 DER 格式的 X509 证书。

您粘贴的证书必须包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。例如：

```
-----BEGIN CERTIFICATE-----
MIICMTCCAZoCCQDdUV3NGK/cUjANBgkqhkiG9w0BAQsFADBdMQswCQYDVQQGEwJV
UzETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYYSW50ZXJuzXQgV2lkZ210
(...5 lines removed...)
shGJDRERYJQqilhHZrYTWZAYTrD7NQPhtK+ZiJng67cPgnNDuXEn55UwMOQoHBp
HMUwmhiGZlzM8BpX2Js2yQ3ms30pr8rO+gPCPMCAwEAATANBgkqhkiG9w0BAQsF
AAOBgQC02CebA6YjJCGr2CJZrQSeUwSveRBpmOuoqm98o2Z+5gJM5CkqgfxcUn
RV7LRfQGfYd76V/5uor4Wx2ZCjy6+zuQEm4ZxWNSZpA9UBixFXJCs9MBO4qkG5D
v1k3WYJfcgyJ10h4E4b0W2xiixBU+xoOTLRATnbKY36EWAG5cw==
-----END CERTIFICATE-----
```

步骤 5 点击上传密钥（或在编辑时点击替换密钥），并选择证书文件（例如 *.key）。文件扩展名必须为 .key。或者，粘贴证书的密钥。

密钥不能加密。

例如：

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC1SulBknrMjzw/5FZ9YgdMLDUGJlbYgkN7mVrkjyLQx2TYsem
r8iTiKB6iyTKbuS4iPeyEYkNF5FglCqKWEdmthNZkKhOsPslA8e60r5mImeDrtw+
```

```
Cc005cSfnlTAW5CgcGkcxTCaGIzmXmkzwGlfYmzbJDeazfSmvys76A8I8wIDAQAB
AoGAUVDgEX8vXE0m9cOubPZ54pZo64KW/OJzUKP0TwxdlqGw/h39XFpkEXiIgmDL
(...5 lines removed...)
DSWvzeKRDH83dmP66+MIbWePhbhty+D1OxbiuVuHV0/ZhxOhCG8tig3R8QJBAJmj
fId05+1dNI4tGbWv6hHh/H/dTP2STlZ3jERMZd29fjIRuJ9jpfC2lIDjvs8YGeAe
0YHkfSOULJn8/jOCf6kCQQDIJiHfGF/31Dk/8/5MGrg+3zau6oKXiuv6db8Rh+7l
MU0x09tvbBUy9REJq1YJWTKpeKD+E0QL+FX0bqvz4tHA
-----END RSA PRIVATE KEY-----
```

步骤 6 单击 **OK**。

生成自签名的内部和内部 CA 证书

内部身份证书是特定系统或主机的证书。

内部 CA 证书是系统可用于签署其他证书的证书。这些证书与内部身份证书的区别在于基本限制条件扩展和 CA 标记方面，CA 证书启用了这些功能，而身份证书中则禁用了这些功能。

您可以生成自签名的内部身份和内部 CA 证书，即这些证书由设备自身签署。如果配置自签名的内部 CA 证书，该 CA 将在设备上运行。系统会生成证书和密钥。

此外，还可以使用 OpenSSL 创建证书或从受信任的 CA 获取证书，再上传它们。有关详细信息，请参阅[上传内部和内部 CA 证书](#)，第 124 页。

有关使用这些证书的功能的信息，请参阅[功能使用的证书类型](#)，第 122 页。



注释 新的自签名证书生成的有效期为 5 年。请务必在证书过期前进行更换。

过程

步骤 1 选择对象，然后从目录中选择证书。

步骤 2 执行以下操作之一：

- 依次点击 +> 添加内部证书，然后点击自签名证书。
- 依次点击 +> 添加内部 CA 证书，然后点击自签名证书。

注释 要编辑或查看证书，请点击信息图标 (i)。对话框中将显示证书主题、颁发者和有效时间范围。点击[替换证书](#)，可上传新的证书和密钥。替换证书后，不能重新执行以下步骤中介绍的自签名特性设置。相反，您必须粘贴或上传新的证书，如[上传内部和内部 CA 证书](#)，第 124 页中所述。其余步骤仅适用于新的自签名证书。

步骤 3 键入证书的名称。

该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 4 为证书主题和颁发机构信息至少配置以下一项。

- **国家/地区 (C)** - 证书中包括的双字符 ISO 3166 国家/地区代码。例如，美国的国家/地区代码是 US。从下拉列表中选择国家/地区代码。
- **州或省 (ST)** - 证书中包括的州或省。
- **地区或城市 (L)** - 证书中包括的地区，例如城市名称。
- **组织 (O)** - 证书中包括的组织或公司名称。
- **组织单位 (部门) (OU)** - 证书中包含的组织单位名称（例如部门名称）。
- **通用名称 (CN)** - 证书中包括的 X.500 通用名称。它们可能是设备、网站或其他文本字符串的名称。通常需要有此元素，才能成功进行连接。例如，用于远程接入 VPN 的内部证书中必须包括 CN。

步骤 5 点击保存。

上传受信任的 CA 证书

受信任证书颁发机构 (CA) 证书用于签署其他证书。它是自签名证书，也称为根证书。由另一个 CA 证书颁发的证书称为从属证书。

有关使用这些证书的功能的信息，请参阅[功能使用的证书类型](#)，第 122 页。

受信任 CA 证书可从外部证书颁发机构获取，也可以使用自己的内部 CA 创建（例如通过 OpenSSL 工具生成证书）。然后，使用以下步骤程序上传证书。

过程

步骤 1 选择对象，然后从目录中选择证书。

步骤 2 执行以下操作之一：

- 依次点击 + > 添加受信任 CA 证书。
- 要编辑证书，请点击证书的编辑图标 (🔗)。

步骤 3 键入证书的名称。

该名称仅在配置中用作对象名称，不会成为证书本身的一部分。

步骤 4 点击上传证书（或在编辑时点击替换证书），然后选择受信任 CA 证书文件（例如 *.pem）。允许的文件扩展名有 .pem、.cert、.cer、.crt 和 .der。或者，粘贴到受信任 CA 证书中。

证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

该证书必须为 PEM 或 DER 格式的 X509 证书。



第 8 章

身份源

身份源是定义用户账户的服务器和数据库。身份源信息具有多种用途，例如提供与 IP 地址关联的用户身份，或是对远程接入 VPN 连接到 Firepower 设备管理器的访问进行身份验证。

以下主题介绍如何定义身份源。后期配置需要使用身份源的服务时，可以使用这些对象。

- [关于身份源，第 129 页](#)
- [Active Directory \(AD\) 身份领域，第 130 页](#)
- [RADIUS 服务器和组，第 135 页](#)
- [身份服务引擎 \(ISE\)，第 138 页](#)
- [本地用户，第 141 页](#)

关于身份源

身份源是为组织内的人员定义用户账户的 AAA 服务器和数据库。身份源信息具有多种用途，例如提供与 IP 地址关联的用户身份，或是对远程接入 VPN 连接到 Firepower 设备管理器的访问进行身份验证。

使用 **对象 > 身份源** 页面可以创建和管理您的源。后期在配置需要身份源的服务时，会用到这些对象。

以下是受支持的身份源及其用途：

Active Directory (AD) 身份领域

Active Directory 可提供用户账户和身份验证信息。请参阅 [Active Directory \(AD\) 身份领域，第 130 页](#)。

您可以将此源用于以下目的：

- 远程接入 VPN，作为主要身份源。
- 身份策略，用于主动身份验证，并作为用户身份源用于被动身份验证。

思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE-PIC)

如果使用 ISE，可以将 Firepower 威胁防御设备与您的 ISE 部署集成。请参阅 [身份服务引擎 \(ISE\)，第 138 页](#)。

您可以将此源用于以下目的：

- 身份策略，作为被动身份源来从 ISE 收集用户身份信息。

RADIUS 服务器，RADIUS 服务器组

如果您使用 RADIUS 服务器，还可以将其与 Firepower 设备管理器搭配使用。必须将每个服务器定义为单独的对象，然后将其归入服务器组（其中，指定组中的服务器是彼此的副本）。为服务器组分配功能，但不为单个服务器分配功能。请参阅 [RADIUS 服务器和组](#)，第 135 页。

您可以将此源用于以下目的：

- 对 FDM 管理用户进行外部身份验证。可以支持具有不同授权级别的多个管理用户。这些用户可以登录到系统进行设备配置和监控。

LocalIdentitySource

这是本地用户数据库，其中包括您在 Firepower 设备管理器中定义的用户。选择 **对象 > 用户管理** 此数据库中的用户账户。请参阅 [本地用户](#)，第 141 页。



注释 本地身份源数据库不包含您在 CLI 中配置（使用 `configure user add` 命令）以进行 CLI 访问的用户。CLI 用户与您在 Firepower 设备管理器中创建的用户是完全独立的。

您可以将此源用于以下目的：

- 远程接入 VPN，作为主要身份源或回退身份源。
- 身份策略，作为被动身份源来从远程接入 VPN 登录收集用户身份信息。

Active Directory (AD) 身份领域

Microsoft Active Directory (AD) 定义用户账户。您可以为 Active Directory 域创建 AD 身份领域。以下主题介绍如何定义 AD 身份领域。

支持的目录服务器

可以使用 Windows Server 2008 和 2012 上的 Microsoft Active Directory (AD)。

请注意以下有关服务器配置的信息：

- 如果要对用户组或组内用户执行用户控制，则必须在目录服务器上配置用户组。如果服务器按照基本对象层次结构组织用户，系统无法执行用户组控制。
- 目录服务器必须使用下表中列出的字段名称，以便系统从该域的服务器中检索用户元数据。

元数据	Active Directory 字段
LDAP user name	samaccountname

元数据	Active Directory 字段
first name	givenname
last name	sn
email address	mail Userprincipalname (如果 mail 没有值)
department	department distinguishedname (如果 department 没有值)
telephone number	telephonenumber

对用户数量的限制

Firepower 设备管理器可以从目录服务器下载多达 2000 个用户的信息。

如果您的目录服务器上有超过 2000 个用户账户，则在访问规则中选择用户时或查看基于用户的控制面板信息时，您不会看到所有可能的名称。您仅可以对已下载的名称编写规则。

此限制也适用于与组相关联的名称。如果组成员超过 2000 个，则只能将下载的 2000 个名称与组成员身份进行匹配。

如果您有 2000 多个用户，请考虑使用 Firepower 管理中心（远程管理器）而非 Firepower 设备管理器。Firepower 管理中心支持的用户数量要多很多。

确定目录基准标识名

配置目录属性时，需要为用户和组指定公共基准标识名(DN)。基准在您的目录服务器中定义，并且会因网络而不同。您必须进入正确的基准，身份策略才能正常使用。如果基准错误，则系统无法确定用户名或组名，进而导致基于身份的策略无法使用。



提示 要获得正确的基准，请咨询目录服务器的管理员。

对于 Active Directory，您可以用域管理员的身份登录 Active Directory 服务器，并按照如下所示在命令提示符后输入 **dsquery** 命令来确定正确的基准：

用户搜索库

输入 **dsquery user** 命令时加上已知用户名（部分或完整），以确定基准标识名。例如，以下命令使用部分名称“John*”返回以“John.”开头的所有用户的信息。

```
C:\Users\Administrator>dsquery user -name "John*"
"CN=John Doe,CN=Users,DC=csc-lab,DC=example,DC=com"
```

基准 DN 为 “DC=csc-lab,DC=example,DC=com”。

组搜索基准

输入 `dsquery group` 命令时加上已知用户名，以确定基准标识名。例如，以下命令使用组名称 `Employees` 返回标识名名称：

```
C:\>dsquery group -name "Employees"
"CN=Employees,CN=Users,DC=csc-lab,DC=example,DC=com"
```

组基准标识名为 “DC=csc-lab,DC=example,DC=com”。

此外，还可以使用 ADSI Edit 程序浏览 Active Directory 结构（开始 > 运行 > `adsiedit.msc`）。在 ADSI Edit 中，右键单击任意对象，例如组织单位 (OU)、组或用户，然后选择属性查看标识名。然后，可以复制 DC 值的字符串作为基准。

要验证您是否获得了正确的基准，请执行以下操作：

1. 单击目录属性中的“测试连接”按钮验证连接。解决所有问题后，保存目录属性。
2. 提交对设备的更改。
3. 创建访问规则，选择用户选项卡，并尝试从目录添加已知的用户和组名称。在您键入内容时，系统会自动填充建议，以匹配包含该目录的领域中的用户和组。如果这些建议显示在一个下拉列表中，则说明系统可以成功查询目录。如果您没有看到建议，而且确定您键入的字符串应显示在用户或组名称中，则需要更正相应的搜索基准。

配置 AD 身份领域

身份领域是目录服务器加上提供身份验证服务所需的其他属性。目录服务器包含有权访问您网络的用户和用户组的相关信息。

对于 Active Directory，领域就等于 Active Directory 域。

领域用于以下策略中：

- 身份 - 领域提供用户身份和组成员身份信息，然后您可将这些信息用于访问控制规则。系统每天都会在当天的最后一个小时 (UTC) 下载有关所有用户和组更新后的相关信息。必须能够从管理接口访问目录服务器。
- 远程接入 VPN - 领域提供身份验证服务，用于确定是否允许接入某个连接。必须能够从 RA VPN 外部接口访问目录服务器。

与您的目录管理员一起获取配置目录服务器属性所需的值。



注释 如果目录服务器不在相连的网络中或无法通过默认路由使用，请为该服务器创建静态路由。依次选择 **设备 > 路由 > 查看配置**，创建静态路由。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。此外，也可以在编辑领域属性时，点击对象列表中所显示的[创建新身份领域](#)链接来创建身份领域对象。


开始之前

确保目录服务器、Firepower 威胁防御设备和客户端之间的时间设置一致。这些设备间的时间偏差可能会导致用户身份验证操作失败。“一致”说明您可以使用不同的时区，但时间相对于这些时区应是相同的；例如，10 AM PST = 1 PM EST。

过程

步骤 1 选择对象，然后从目录中选择身份源。

步骤 2 执行以下操作之一：

- 要创建 AD 领域，请点击 + > **AD**。最多只能创建一个领域。
- 要编辑领域，请点击此领域的编辑图标 ()。

一旦创建某个领域，就无法将其删除。要停止使用该领域，请禁用已配置使用该领域的功能。

步骤 3 配置基本领域属性。

- **名称** - 目录领域的名称。
- **类型** - 目录服务器的类型。Active Directory 是唯一支持的类型，所以无法更改此字段。
- **目录用户名、目录密码** - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

注释 系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=admin administrator,cn=users,dc=example,dc=com。请注意，cn = users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- **基准 DN (Base DN)** - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如，cn=users、dc=example、dc=com。有关查找基准 DN 的信息，请参阅[确定目录基准标识名](#)，第 131 页。
- **AD 主域** - 设备应加入的 Active Directory 完全限定域名。例如 example.com。

步骤 4 配置目录服务器属性。

- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。

- **加密** - 要使用加密连接下载用户和组信息，请选择所需的方法 **STARTTLS** 或 **LDAPS**。系统默认为无，也就是说以明文形式下载用户和组信息。
 - **STARTTLS** 将会协商加密方法，并使用目录服务器支持的最强方法。使用端口 389。如果将领域用于远程接入 VPN，则不支持此选项。
 - **LDAPS** 需要基于 SSL 的 LDAP。使用端口 636。
- **受信任的 CA 证书** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 10.10.10.250 作为 IP 地址，但证书中的地址为 ad.example.com，则连接失败。

步骤 5 点击**测试**按钮验证系统是否可以与服务器通信。

系统使用单独的进程和接口访问服务器，因此您可能会收到错误通知，指出连接适用于一种用途而不适用于另一种用途，例如可用于身份策略，但不可用于远程接入 VPN。如果无法访问服务器，请确认 IP 地址和主机名正确、DNS 服务器具有该主机名的条目等。您可能需要为该服务器配置静态路由。有关详细信息，请参阅[故障排除目录服务器连接](#)，第 134 页。

步骤 6 单击 **OK**。

故障排除目录服务器连接

系统使用不同的进程与您的目录服务器通信，具体取决于服务器的功能。因此，身份策略的连接可以正常工作，而远程接入 VPN 的连接则失败。

这些进程使用不同的接口与目录服务器进行通信。您必须确保这些接口的连接性。

- 管理接口，用途：身份策略。
- 数据接口，用途：远程接入 VPN（外部接口）。

配置身份领域时，请使用 **Test** 按钮验证连接是否可以正常工作。失败消息应指示该功能存在连接问题。根据身份验证属性和路由/接口配置，以下是您可能会遇到的常规问题。

目录用户身份验证问题。

如果问题是系统因用户名或密码而无法登录目录服务器，请确保用户名和密码正确并在目录服务器上有效。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

此外，系统还会根据用户名和密码信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=admin, cn=users, dc=example, dc=com。请注意，cn=users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

目录服务器可通过数据接口进行访问。

如果目录服务器所在的网络直接连接到数据接口（例如千兆以太网接口）或是可从直连网络路由，那么您必须确保虚拟管理接口与目录服务器之间存在路由。

- 使用 **data-interfaces** 作为管理网关应该能够确保路由成功。
- 如果管理接口上有显式网关，则该网关路由器需要与目录服务器之间建立路由。
- 您不需要在**诊断**接口上配置 IP 地址，该接口是虚拟管理接口使用的物理接口。但是，如果您确实配置了地址，也不要配置会将流向目录服务器的流量重定向至**诊断**接口的静态路由（例如默认路由）。
- 如果直连网络与托管目录服务器的网络之间存在路由器，则为目录服务器配置静态路由 (**Device > Routing**)。
- 验证数据接口的 IP 地址和子网掩码是否正确。

目录服务器可通过管理物理接口进行访问。

如果目录服务器所在的网络直接连接到管理物理接口（例如 Management0/0）或是可从该网络路由，那么您必须执行以下操作：

- 在 **Device > Interfaces** 上为管理接口配置 IPv4 地址（使用逻辑名称 **diagnostic**）。该 IP 地址必须与虚拟管理地址 (**Device > System Settings > Management Interface**) 位于同一子网上。
- 如果目录服务器与管理接口之间存在路由器，则在**诊断**接口的 **Device > Routing** 上为目录服务器配置路由。
- 验证**诊断**接口和管理接口的 IP 地址和子网掩码是否正确。

目录服务器位于外部网络上。

如果目录服务器位于外部（上行链路）接口另一端的网络，您可能需要配置站点间 VPN 连接。有关详细程序，请参阅[如何通过远程接入 VPN 使用外部网络上的目录服务器](#)，第 428 页。

RADIUS 服务器和组

您可以使用 RADIUS 服务器对 FDM 管理用户进行身份验证和授权。例如，如果您还使用思科身份服务引擎 (ISE) 及其 RADIUS 服务器，可以将该服务器与 Firepower 设备管理器搭配使用。

配置要使用 RADIUS 服务器的功能时，您应选择 RADIUS 组而不是单个服务器。RADIUS 组所含 RADIUS 服务器是彼此副本的集合。如果一个组具有多个服务器，这些服务器可构成备份服务器链，在其中一台服务器不可用时提供冗余。但即使只有一台服务器，也必须创建包含一个成员的组，以配置功能的 RADIUS 支持。

以下主题介绍如何配置 RADIUS 服务器和组，以便它们可用于支持的功能。

配置 RADIUS 服务器

RADIUS 服务器提供 AAA（身份验证、授权和记帐）服务。如果您使用 RADIUS 服务器进行用户身份验证和授权，可以将这些服务器与 Firepower 设备管理器搭配使用。

为每个 RADIUS 服务器创建对象后，创建 RADIUS 服务器组，以包含每个重复服务器组。

过程

步骤 1 选择对象，然后从目录中选择身份源。

步骤 2 执行以下操作之一：

- 要创建对象，请依次点击 + > **RADIUS 服务器**。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 配置以下属性：

- **名称** - 对象的名称。这不需要与服务器上配置的任何内容匹配。
- **服务器名称或 IP 地址** - 服务器的完全限定主机名 (FQDN) 或 IP 地址。例如，radius.example.com 或 10.100.10.10。
- **身份验证端口** - 在其上执行 RADIUS 身份验证和授权的端口。默认值为 1812。
- **超时** - 系统将请求发送至下一服务器之前等待服务器响应的时长，1-300 秒之间的数值。默认值为 10 秒。
- **服务器密钥** - (可选。) 用于加密 Firepower 威胁防御设备和 RADIUS 服务器之间数据的共享密钥。该密钥是一个区分大小写的字母数字字符串，最多 64 个字符，且不含空格。密钥必须以字母数字字符或下划线开头，它可以包含特殊字符：\$ & - _ . + @。字符串必须匹配 RADIUS 服务器上配置的字符串。如果不配置密钥，则不加密连接。

步骤 4 (可选，仅编辑对象时) 点击**测试**检查系统是否可以连接到服务器。

系统会提示输入用户名和密码。测试确认是否可以连接服务器，如果可以连接，则确认是否可以对用户名进行身份验证。

步骤 5 单击 **OK**。

配置 RADIUS 服务器组

RADIUS 服务器组中包含一个或多个 RADIUS 服务器对象。组中的服务器必须是彼此的备份。这些服务器构成本地服务器链，因此，如果第一台服务器不可用，系统可以尝试列表中的下一个服务器。

在一项功能中配置 RADIUS 支持时，必须选择服务器组。因此，即使只有一台 RADIUS 服务器，也必须创建包含该服务器的组。

过程

步骤 1 选择对象，然后从目录中选择身份源。

步骤 2 执行以下操作之一：

- 要创建对象，请依次点击 + > **RADIUS 服务器组**。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 配置以下属性：

- **名称** - 对象的名称。这不需要与服务器上配置内容匹配。
- **断路时间** - 只要当所有服务器均发生故障时，才会重新激活故障服务器。断路时间是指最后一台服务器发生故障后，在重新激活所有服务器之前所等待的时间，其值为 0-1440 分钟。默认值为 10 分钟。
- **最大失败尝试次数** - 尝试组中下一个服务器之前发送到 RADIUS 服务器的失败 AAA 事务（即，未收到响应的请求）的数量。您可以指定 1 到 5 之间的数字，默认值为 3。超过最大失败尝试次数时，系统会将服务器标记为故障。

对于给定功能，如果您使用本地数据库配置回退方法，并且组中的所有服务器都无法响应，则会将该组视为无法响应，并将尝试回退方法。该服务器组会在断路时间内保持标记为无响应，以确保该时段内其他 AAA 请求不会尝试联系该服务器组，而是立即使用回退方法。

- **RADIUS 服务器列表** - 选择为该组定义服务器的最多 16 个 RADIUS 服务器对象。按优先级顺序添加这些对象。使用列表中的第一个服务器，直至此服务器无法响应。添加对象后，您可以通过拖放重新排列对象。如果所需的对象尚不存在，请点击**创建新的 RADIUS 服务器**立即添加对象。

您也可以点击**测试**链接，验证系统是否可以连接到服务器。系统会提示输入用户名和密码。测试确认是否可以连接服务器，如果可以连接，则确认是否可以对用户名进行身份验证。

步骤 4（可选。）点击**测试所有服务器**按钮，检查到组中每台服务器的连接。

系统会提示输入用户名和密码。系统会检查是否可以连接每个服务器，以及用户名是否可在每台服务器上身份验证。

步骤 5 单击 **OK**。

RADIUS 服务器和组故障排除

当外部授权无法使用时，您可以检查以下事项。

- 使用 RADIUS 服务器和服务器组对象中的**测试**按钮，验证是否可以从设备连接到服务器。务必在测试之前保存对象。如果测试失败：
 - 请注意，测试会忽略为服务器配置的接口，且始终使用管理接口。如果未将 RADIUS 身份验证代理配置为响应来自管理 IP 地址的请求，则测试预期失败。
 - 验证您在测试期间是否输入了正确的用户名/密码组合。如果用户名/密码组合不正确，您将收到凭证错误消息。

- 验证服务器的加密密钥、端口和 IP 地址。如果使用主机名，验证是否为管理接口配置了 DNS。考虑在 RADIUS 服务器上，而不是在设备配置中是否会更改密钥。
- 如果测试仍然失败，您可能需要配置到 RADIUS 服务器的静态路由。请尝试从 CLI 控制台或 SSH 会话对服务器执行 ping 操作，检查是否可以访问服务器。
- 如果外部身份验证一直都在工作，却停止了工作，请考虑是否会出现所有服务器均处于空载时间的情况。组内的所有 RADIUS 服务器都发生故障时，空载时间是系统在再次尝试连接第一个服务器之前等待的分钟数。默认时间为 10 分钟，不过您可以配置最长 1440 分钟。
- 如果 HTTPS 外部身份验证对一部分用户适用，对另一部分用户不适用，请评估 RADIUS 服务器中为每个用户账户定义的 cisco-av-pair 属性。此属性可能未正确配置。属性缺失或不正确将阻止对该用户账户的所有 HTTPS 访问。

身份服务引擎 (ISE)

您可以将思科身份服务引擎 (ISE) 或 ISE 被动身份连接器 (ISE-PIC) 部署与 Firepower 威胁防御设备相集成，以使用 ISE/ISE-PIC 进行被动身份验证。

ISE/ISE-PIC 是一个授权身份源，并为使用 Active Directory (AD)、LDAP、RADIUS 或 RSA 进行身份验证的用户提供用户感知数据。但是，对于 Firepower 威胁防御，您只能将 ISE 与 AD 配合使用，以获悉用户身份。除查看各种监控控制面板和事件中的用户信息之外，还可以将用户身份用作访问控制和 SSL 解密策略中的匹配条件。

有关思科 ISE/ISE-PIC 的更多信息，请参阅《思科身份服务引擎管理员指南》(<https://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html>) 和《身份服务引擎被动身份连接器 (ISE-PIC) 安装和管理员指南》(<https://www.cisco.com/c/en/us/support/security/ise-passive-identity-connector/tsd-products-support-series-home.html>)。

ISE 的指南和限制

- 由于系统不将设备身份验证与用户关联，因此 Firepower System 不支持与 Active Directory 身份验证同时进行 802.1x 设备身份验证。如果使用 802.1x 主动登录，则将 ISE 配置为仅报告 802.1x 主动登录（设备和用户）。这样，仅向系统报告一次设备登录。
- ISE/ISE-PIC 不报告 ISE 访客服务用户的活动。
- 同步 ISE/ISE-PIC 服务器和设备上的时间。否则，系统可能会以意外间隔执行用户超时。
- 如果将 ISE/ISE-PIC 配置为监控大量用户组，则由于内存限制，系统可能会根据组丢弃用户映射。因此，带有领域或用户条件的规则可能不会按预期执行。
- 有关与此版本的系统兼容的 ISE/ISE-PIC 的特定版本，请参阅思科 *Firepower* 兼容性指南 (<https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-device-support-tables-list.html>)。
- 使用 ISE 服务器的 IPv4 地址，除非您确认您的 ISE 版本支持 IPv6。

配置身份服务引擎

要使用思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE PIC) 作为被动身份源，您必须配置与 ISE 平台交换网络 (pxGrid) 服务器的连接。

开始之前

- 从 ISE 中导出 pxGrid 和 MNT 服务器证书。例如，在 ISE PIC 2.2 上，可在 **证书 > 证书管理 > 系统证书** 页面找到这些证书。MNT（监控和故障排除节点）在证书列表的“使用者”列中显示为 Admin。您可以在 **对象 > 证书** 页面将他们上传为受信任的 CA 证书，也可以在以下过程中上传这些证书。这些节点可能使用相同的证书。
- 您还必须配置 AD 身份领域。系统从 AD 获取用户列表，从 ISE 获取用户到 IP 地址映射的信息。

过程

步骤 1 选择对象，然后从目录中选择身份源。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 **+ > ISE 对象**。可创建最多一个 ISE 对象。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 配置以下属性：

- **名称** - 对象的名称。
- **状态** - 点击开关以启用或禁用对象。禁用对象时，您不能将 ISE 用作身份规则中的身份源。
- **说明** - 对象的可选说明。
- **主节点主机名/IP 地址** - 主要 pxGrid ISE 服务器的主机名或 IP 地址。不要指定 IPv6 地址，除非确认您的 ISE 版本支持 IPv6。
- **pxGrid 服务器 CA 证书** - 受信任的 pxGrid 框架证书颁发机构证书。
- **MNT 服务器 CA 证书** - 执行批量下载时 ISE 证书的受信任的证书颁发机构证书。如果您的 MNT（监控和故障排除）服务器不是单独的服务器，此证书可能与 pxGrid 服务器证书相同。
- **服务器证书** - 连接 ISE 或执行批量下载时，Firepower 威胁防御设备必须向 ISE 提供的内部身份证书。
- **ISE 网络过滤器** - 可设置用来限制 ISE 向系统报告的数据的可选过滤器。如果提供网络过滤器，ISE 会仅报告网络上符合过滤器要求的数据。点击 +，选择标识网络的网络对象，然后点击确定。如果您需要创建对象，点击 **创建新网络**。仅配置 IPv4 网络对象。

步骤 4 点击测试按钮，验证系统是否可以连接到 ISE 服务器。

如果测试失败，请点击[查看日志](#)链接了解详细的错误消息。例如，以下消息表示系统无法在规定端口连接到服务器。存在的问题可能是，没有路由到主机（即 ISE 服务器未使用预期端口），或访问控制规则阻止这类连接。

```
Captured Jabberwerx log:2018-05-11T16:10:30 [ ERROR]: connection timed out while  
trying to test connection to host=10.88.127.142:ip=10.88.127.142:port=5222
```

步骤 5 点击确定保存对象。

下一步做什么

配置 ISE 后，启用身份策略，配置被动身份验证规则，并部署配置。然后，您必须转到 ISE/ISE PIC 并接受设备作为订阅方。如果您配置 ISE/ISE PIC 自动接受订阅方，无需手动接受订用。

ISE/ISE-PIC 身份源故障排除

ISE/ISE-PIC 连接

如果您遇到 ISE 或 ISE-PIC 连接问题，请检查以下事项：

- 必须启用 ISE 中的 pxGrid 身份映射功能，才能将 ISE 与 Firepower 威胁防御设备成功集成。
- 在 ISE 服务器与 Firepower 威胁防御设备成功建立连接之前，您必须手动在 ISE 中批准客户端。
或者，您可以在 ISE 中启用[自动审批新账户](#)，具体操作请参照《思科身份服务引擎管理员指南》中有关管理用户和外部身份源的章节。
- Firepower 威胁防御设备（服务器）证书必须包含 **clientAuth** 扩展密钥用法值，否则不能包含任何扩展密钥用法值。如果设置了 **clientAuth** 扩展密钥用法，还必须选择不设置密钥用法，或设置数字签名密钥用法值。使用 Firepower 设备管理器创建的自签名身份证书满足这些要求。
- ISE 服务器上的时间必须与 Firepower 威胁防御上的时间同步。如果设备不同步，系统可能会以非预期时间间隔执行用户超时。

ISE/ISE-PIC 用户数据

如果您遇到 ISE 或 ISE-PIC 报告的用户数据问题，请注意以下事项：

- 系统检测到其数据尚未在数据库中的 ISE 用户的活动后，会从服务器检索其相关信息。ISE 用户发现的活动并非由访问控制规则处理，而且在系统于用户下载中成功检索到这些活动的相关信息之前，活动不会显示在控制面板中。
- 不能对由 LDAP、RADIUS 或 RSA 域控制器进行身份验证的 ISE 用户执行用户控制。
- 系统不会收到 ISE 访客服务用户的用户数据。

本地用户

本地用户数据库 (LocalIdentitySource) 包括您在 Firepower 设备管理器中定义的用户。

您可以将本地定义的用户用于以下目的：

- 远程接入 VPN，作为主要身份源或回退身份源。
- 管理访问权限，作为 Firepower 设备管理器用户的主要或辅助源。

admin 用户是系统定义的本地用户。但是，管理员用户无法登录远程接入 VPN。您不能创建额外的本地管理用户。

如果您定义管理访问的外部身份验证，登录到设备的外部用户将显示在本地用户列表中。

- 作为被动身份源，身份策略间接从远程接入 VPN 登录收集用户身份。

以下主题介绍如何配置本地用户。

配置本地用户

您可以直接在设备上创建与远程接入 VPN 搭配使用的用户账户。您可以使用本地用户账户代替外部身份验证源，或与后者搭配使用。

如果您使用本地用户数据库作为远程接入 VPN 的回退身份验证方式，请确保在本地数据库中配置与外部数据库中的名称相同的用户名/密码。否则，回退机制将无效。

此处定义的用户无法登录设备 CLI。

过程

步骤 1 依次选择对象 > 用户。

列表将显示用户名和服务类型，可以是：

- **MGMT** - 针对可以登录到 Firepower 设备管理器的管理用户。始终定义管理员用户，并且无法将其删除。也不能配置其他 MGMT 用户。但是，如果您定义管理访问的外部身份验证，登录到设备的外部用户将作为 MGMT 用户显示在本地用户列表中。
- **远程接入 VPN** - 针对可以登录到设备上配置的远程接入 VPN 的用户。您还必须选择主要或辅助（回退）源的本地数据库。

步骤 2 执行以下操作之一：

- 要添加用户，请点击 +。
- 要编辑用户，请点击该用户的编辑图标 (🔗)。

如果您不再需要特定用户账户，请点击该用户的删除图标 (🗑️)。

步骤 3 配置用户属性:

用户名和密码可以包含除空格和问号之外的任何可打印 ASCII 字母数字或特殊字符。可打印的字符为 ASCII 代码 33-126。

- **名称** - 用于登录远程接入 VPN 的用户名。名称可以是 4 至 64 个字符，但不能包含空格。例如，johndoe。
- **密码、确认密码** - 输入账户的密码。密码长度必须介于 8 到 16 个字符之间。它不能包含相同的连续字母。它还必须包含至少一个以下各项：数字、大写和小写字符，以及特殊字符。

注释 用户无法更改其密码。告诉他们密码，需要更改密码时，必须编辑用户账户。此外，不要更新外部 MGMT 用户的密码：密码由外部 AAA 服务器控制。

步骤 4 单击 **OK**。



第 III 部分

基本操作

- [高可用性（故障切换），第 145 页](#)
- [接口，第 183 页](#)
- [路由，第 209 页](#)



第 9 章

高可用性（故障切换）

以下主题介绍如何配置和管理主用/备用设备故障切换，以实现 Firepower 威胁防御系统的高可用性。

- [关于高可用性（故障切换），第 145 页](#)
- [高可用性的系统要求，第 153 页](#)
- [高可用性指南，第 154 页](#)
- [配置高可用性，第 155 页](#)
- [管理高可用性，第 166 页](#)
- [监控高可用性，第 174 页](#)
- [高可用性故障排除（故障切换），第 176 页](#)

关于高可用性（故障切换）

高可用性或故障切换设置可以将两台设备相关联，这样，当主设备发生故障时，辅助设备可以接管其任务。这有助于您在设备发生故障时保持网络运行。

配置高可用性需要两台相同的 Firepower 威胁防御设备，二者之间通过专用故障切换链路和（可选）状态链路彼此互连。这两台设备不断通过故障切换链路进行通信，以便确定每台设备的运行状态并同步已部署的配置更改。系统使用状态链路将连接状态信息传递到备用设备，因此如果发生故障切换，用户连接将得以保留。

这两台设备构成一对主用/备用设备，其中一台设备是主用设备并传递流量。备用设备不会主动传递流量，但会使配置和其他状态信息与主用设备同步。

系统会对主用设备的运行状况（硬件、接口、软件以及环境状态）进行监控，以便确定是否符合特定的故障切换条件。如果符合条件，主用设备将故障切换至备用设备，届时备用设备将变成主用设备。

关于主用/备用故障切换

主用/备用故障切换允许您使用备用 Firepower 威胁防御设备来接管故障设备的功能。当主用设备发生故障时，备用设备将变为主用设备。

主/辅助角色和主用/备用状态

在故障切换对中这两台设备之间的主要区别是哪台是主用设备，哪台是备用设备，即要使用哪些 IP 地址以及哪台设备积极传递流量。

但是，设备之间还存在一些取决于哪一设备为主设备（在配置中指定），哪一设备为辅助设备的差别：

- 如果两台设备同一时间启动（并且运行状况相同），则主设备总是会成为主用设备。
- 主设备 MAC 地址始终与主用 IP 地址相匹配。此规则的例外是，当辅助设备成为主用设备并且无法通过故障切换链路获取主设备 MAC 时。在这种情况下，会使用辅助设备的 MAC 地址。

启动时的主用设备确定

主用设备按以下方式确定：

- 如果某台设备启动，并检测到对等体已作为主用设备运行，则该设备会成为备用设备。
- 如果某台设备启动，并且未检测到对等体，则该设备会成为主用设备。
- 如果两台设备同时启动，则主设备成为主用设备，辅助设备成为备用设备。

故障切换事件

在主用/备用故障切换中，故障切换会在设备级别进行。

下表显示了每个故障事件的故障切换操作。对于每种故障事件，该表显示了故障切换策略（故障切换或禁用故障切换）、主用设备执行的操作、备用设备执行的操作，以及有关故障切换条件和操作的所有特别说明。

表 4: 故障切换事件

故障事件	策略	主用组操作	备用组操作	备注
主用设备发生故障（电源或硬件）	故障切换	不适用	成为主用设备 将主用设备标记为发生故障	在任何受监控接口或故障切换链路上，均未收到 Hello 消息。
以前的主用设备恢复	禁用故障切换	成为备用设备	无需操作	无。
备用设备发生故障（电源或硬件）	禁用故障切换	将备用设备标记为发生故障	不适用	备用设备被标记为发生故障后，主用设备不会尝试进行故障切换，即使超过接口故障阈值也是如此。

故障事件	策略	主用组操作	备用组操作	备注
故障切换链路在运行过程中发生故障	禁用故障切换	将故障切换链路标记为发生故障	将故障切换链路标记为发生故障	您应尽快恢复故障切换链路，因为当故障切换链路发生故障时，设备无法故障切换到备用设备。
故障切换链路在启动时发生故障	禁用故障切换	将故障切换链路标记为发生故障	成为主用设备	如果故障切换链路在启动时发生故障，则两台设备都会成为主用设备。
状态链路发生故障	禁用故障切换	无需操作	无需操作	如果发生故障切换，状态信息会过时，而且会话会被终止。
主用设备上的接口故障超过阈值	故障切换	将主用设备标记为发生故障	成为主用设备	无。
备用设备上的接口故障超过阈值	禁用故障切换	无需操作	将备用设备标记为发生故障	备用设备被标记为发生故障后，主用设备不会尝试进行故障切换，即使超过接口故障阈值也是如此。

故障切换和状态故障切换链路

故障切换链路是两台设备之间的专用连接。状态故障切换链路也是专用连接，不过，您可以使用一个故障切换链路作为组合的故障切换/状态链路，也可以创建单独的专用状态链路。如果仅使用故障切换链路，状态信息也会通过该链路：状态故障切换功能不会受到影响。

默认情况下，故障切换和状态故障切换链路上的通信是纯文本通信（不加密）。为了增强安全性，您可以通过配置 IPsec 加密密钥对通信加密。

以下主题更加详细地介绍了这些接口，并就如何连接设备以获得最佳效果给出了建议。

故障切换链路

故障切换对中的两台设备会不断地通过故障切换链路进行通信，以确定每台设备的运行状态和同步配置更改。

以下信息将通过故障切换链路传输：

- 设备状态（主用或备用）。
- Hello 消息 (keep-alives)。
- 网络链路状态。

- MAC 地址交换。
- 配置复制和同步。
- 系统数据库更新，包括 VDB 和规则，但不包括地理位置和安全情报数据库。每个系统会单独下载地理位置和安全情报更新。如果您创建更新计划，这些更新应保持同步。但是，如果您在主用设备上执行手动地理位置或安全情报更新，那么也应在备用设备上执行同样的操作。



注释 事件、报告和审核日志数据不会同步。事件查看器和控制面板仅显示与特定设备相关的数据。此外，部署历史记录、任务历史记录和其他审核日志事件不会同步。

状态故障切换链路

系统使用状态链路将连接状态信息传送到备用设备。此信息可在发生故障切换时帮助备用设备保留现有连接。

对故障切换和状态故障切换链路使用一条链路能够最大程度地节省接口。但是，如果您有一个大型配置和高流量网络，必须考虑对状态链路和故障切换链路使用专用接口。

思科建议状态故障切换链路的带宽应匹配设备上数据接口的最大带宽。

用于故障切换和状态链路的接口

可以使用未使用但已启用的数据接口（物理接口接口）作为故障切换链路；但无法指定当前配置了名称的接口。故障切换链路接口不会配置为常规网络接口；该接口仅会因为故障切换而存在。该接口只能用于故障切换链路（还用于状态链路）。无法使用管理接口或子接口进行故障切换。

FTD 用户数据和故障切换链路之间共享接口。

连接故障切换和状态故障切换接口

您可以将任何未使用的数据物理接口用作故障切换链路和可选的专用状态链路。但是，您不能选择当前已配置名称或具有子接口的接口。故障切换和状态故障切换链路接口不会被配置为通常的网络接口。这些接口只是为了进行故障切换通信，不能用于直通流量或管理访问。

此配置在设备之间是同步的，因此您必须为链路的两端选择相同的端口号。例如，用于故障切换链路的两台设备都使用 GigabitEthernet1/3。

使用以下两种方法中的一种连接故障切换链路和专用状态链路（如已使用）：

- 使用不与任何其他设备处于相同网段（广播域或 VLAN）的交换机作为 Firepower 威胁防御设备的故障切换接口。专用状态链路的要求与故障切换链路相同，只是必须与故障切换链路位于不同的网段上。



注释 使用交换机的优点是，如果设备的其中一个接口发生故障，可以轻松确定哪一个接口出现故障。如果使用直连电缆连接，那么当一个接口发生故障时，链路将在两个对等设备上断开，这样将难以确定哪台设备出现故障。

- 使用以太网电缆直接连接设备，无需外部交换机。Firepower 威胁防御设备在其铜缆以太网端口上支持自动 MDI/MDIX，因此您可以使用交叉电缆或直通电缆。如果使用的是直通电缆，接口会自动检测该电缆，并将其中一个发送/接收对交换为 MDIX。

使用长距离故障切换时，为实现最佳性能，状态链路的延迟应低于 10 毫秒且不超过 250 毫秒。如果延迟超过 10 毫秒，重新传输故障切换消息会导致一些性能降级。

避免中断故障切换和数据链路

我们建议，让故障切换链路和数据接口使用不同的路径，以便降低所有接口同时发生故障的可能性。如果故障切换链路发生故障，Firepower 威胁防御设备可使用数据接口来确定是否需要进行故障切换。随后，故障切换操作会被暂停，直到故障切换链路恢复正常。

请参阅以下连接情景，以设计具有弹性的故障切换网络。

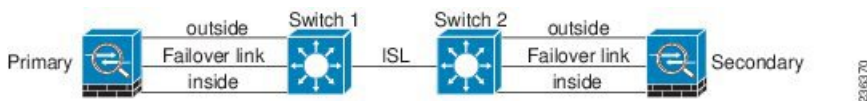
情景 1 - 不推荐

如果单台交换机或一组交换机用于连接两台 Firepower 威胁防御设备之间的故障切换和数据接口，则交换机或交换机间链路发生故障时，两台 Firepower 威胁防御设备都将处于主用状态。因此，建议不要使用下图中显示的 2 种连接方法。

图 2: 使用单交换机连接 - 不推荐



图 3: 使用双交换机连接 - 不推荐



情景 2 - 推荐

我们建议不要让故障切换链路和数据接口使用相同的交换机，而是应使用不同的交换机或使用直连电缆来连接故障切换链路，如下图所示。

图 4: 使用其他交换机连接

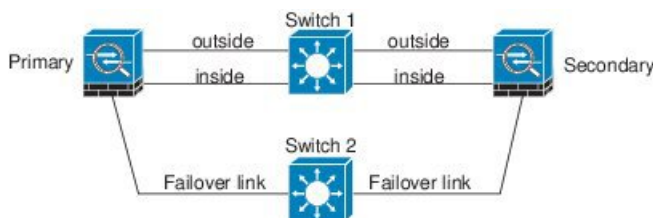
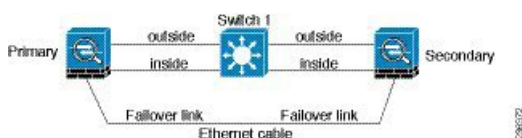


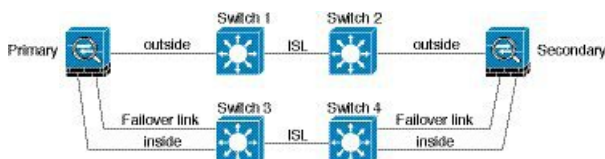
图 5: 通过电缆连接



情景 3 - 推荐

如果 Firepower 威胁防御数据接口连接到多台交换机，则故障切换链路可以连接到其中一台交换机，最好是处于网络的安全一侧（内部）的交换机，如下图所示。

图 6: 使用安全交换机连接



状态故障切换如何影响用户连接

主用设备与备用设备共享连接状态信息。这意味着，备用设备可以保持某些类型的连接，而不会影响用户。

但是，有一些类型的连接不支持状态故障切换。对于这些连接，如果发生故障切换，用户需要重新建立连接。通常，连接会根据连接中所用协议的行为自动进行。

以下主题介绍状态故障切换支持或不支持的功能。

支持的功能

对于状态故障切换，以下状态信息会传送至备用 Firepower 威胁防御设备：

- NAT 转换表。
- TCP 和 UDP 连接和状态，包括 HTTP 连接状态。其他类型的 IP 协议和 ICMP 不会通过主用设备解析，因为它们是在新数据包到达时在新的主用设备上建立的。
- Snort 连接状态、检查结果和引脚信息，包括严格 TCP 实施。
- ARP 表

- 第 2 层网桥表（适用于桥接组）
- ISAKMP 和 IPsec SA 表
- GTP PDP 连接数据库
- SIP 信令会话和引脚。
- 静态和动态路由表 - 状态故障切换会参与动态路由协议（如 OSPF 和 EIGRP），因此通过主用设备上的动态路由协议获悉的路由，将会保留在备用设备的路由信息库 (RIB) 表中。发生故障切换事件时，数据包可以正常传输，并且只会对流量产生极小的影响，因为主用辅助设备一开始就具有镜像主设备的规则。进行故障切换后，新的主用设备上的重新融合计时器会立即启动。随后 RIB 表中的代编号将会增加。在重新融合期间，OSPF 和 EIGRP 路由将使用新的代编号进行更新。计时器到期后，过时的路由条目（由代编号确定）将从表中删除。于是 RIB 将包含新主用设备上的最新的路由协议转发信息。



注释 路由仅会因为主用设备上的链路打开或关闭事件而同步。如果备用设备上的链路打开或关闭，从主用设备发出的动态路由可能会丢失。这是预期的正常行为。

- DHCP 服务器 - 不会复制 DHCP 地址租用。但是，在接口上配置的 DHCP 服务器将发送 ping 命令，以确保在向 DHCP 客户端授予地址前不使用地址，使得服务不会受到影响。对于 DHCP 中继代理或 DDNS，状态信息不相关。
- 访问控制策略决策 - 在故障切换期间，会保留与流量匹配（包括 URL、URL 类别、地理位置等）、入侵检测、恶意软件和文件类型相关的决策。但是，对于在故障切换时评估的连接，有以下注意事项：
 - AVC - 系统会复制 App-ID 裁定，而不是检测状态。只要 App-ID 裁定是完整的，并且在发生故障切换之前完成同步，即可实现正确的同步。
 - 入侵检测状态 - 进行故障切换时，一旦出现拾取中间流的情况，新检测既已完成，但旧状态会丢失。
 - 文件恶意软件阻止 - 文件处置必须在故障切换之前变为可用。
 - 文件类型检测和阻止 - 文件类型必须在故障切换之前加以识别。如果在原始主用设备识别文件时发生故障切换，则文件类型不同步。即使文件策略阻止该文件类型，新的主用设备也会下载该文件。
- 来自身份策略的被动用户身份决策，并非通过主动身份验证和通过强制网络门户收集的决策。
- 安全情报决策。
- RA VPN - 故障切换后，远程接入 VPN 终端用户不必对 VPN 会话重新进行身份验证，也不必重新连接。但是，在 VPN 连接上运行的应用，在故障切换过程中可能会丢失数据包，并且无法从数据包丢失中恢复。

不支持的功能

对于状态故障切换，以下状态信息不会传送到备用 Firepower 威胁防御设备：

- 纯文本隧道（例如 GRE 或 IP-in-IP 隧道）内的会话。不会复制隧道内部的会话，并且新的主动节点不能重复使用现有检测判定来匹配正确的策略规则。
- 由 SSL 解密策略解密的连接 - 解密状态不同步，且重置后当前已解密的连接将被阻止。新连接将正常工作。未解密的连接（它们匹配不解密规则）不受影响，并会像其他任何 TCP 连接一样正确进行复制。
- 组播路由。

备用设备上允许的配置更改和操作

当设备在高可用性模式下运行时，仅需要对主用设备进行配置更改。部署配置时，新的更改也会传输到备用设备。

但某些属性是备用设备所特有的。您可以在备用设备上更改以下属性：

- 管理 IP 地址和网关。
- （仅限于 CLI。）管理员用户账户的密码。此更改只能在 CLI 中进行，不能在 FDM 中进行。

此外，您还可以在备用设备上执行以下操作。

- 高可用性操作（例如暂停、恢复、重置和中断 HA）以及在主用设备和备用设备之间进行模式切换。
- 每个设备的控制面板和事件数据是唯一的，并且是不同步的。这包括事件查看器中的自定义视图。
- 每个设备的审核日志信息是唯一的。
- 智能许可注册。前提是，您必须启用或禁用主用设备上的可选许可证，并且该操作是与备用设备同步的，用于请求或释放相应的许可证。
- 备份，但不进行恢复。要恢复备份，您必须中断设备上的 HA。如果备份包括 HA 配置，设备将重新加入高可用性组。
- 软件升级安装。
- 生成故障排除日志。
- 手动更新地理位置或安全情报数据库。这些数据库在设备之间不同步。如果您创建更新计划，设备可以独立地保持一致。
- 您可以从 **监控 > 会话** 页面查看活动 Firepower 设备管理器用户会话，并删除会话。

高可用性的系统要求

以下主题介绍整合高可用性配置中的两台设备之前必须满足的要求。

高可用性的硬件要求

要将高可用性配置中的两台设备链接在一起，必须满足以下硬件要求。

- 设备的硬件型号必须完全相同。
- 设备接口的数量和类型必须相同。
- 设备安装的模块必须相同。例如，如果具有可选的网络接口模块，则必须在另一台设备中安装相同的模块。

高可用性的软件要求

要将两台设备链接到高可用性配置，必须满足以下软件要求。

- 设备必须运行完全相同的软件版本，也即，版本号的大（第一个）、小（第二个）以及维护（第三个）数字均必须相同。您可以在 Firepower 设备管理器的设备页面或者 CLI 中使用 **show version** 命令找到版本信息。允许连接具有不同版本的设备，但配置不会导入备用设备且故障切换无法使用，直到您将设备升级到同一软件版本。
- 两台设备必须在本地管理器模式下运行，也即，使用 Firepower 设备管理器配置设备。如果您可以在两个系统上登录 Firepower 设备管理器，则表示这两台设备是本地管理器模式。您还可以在 CLI 中使用 **show managers** 命令进行验证。
- 必须在每台设备中完成初始设置向导。
- 每台设备都必须有自己的管理 IP 地址。管理接口的配置在两台设备之间未同步。
- 设备必须具有相同的 NTP 配置。
- 不能配置任何接口使用 DHCP 获取地址。也就是说，所有接口都必须有静态 IP 地址。
- 两台设备必须具有与思科防御协调器相同的注册状态：要么均注册，要么均未注册。
- 对于以下云服务，必须启用主设备和辅助设备，或在辅助设备启用后禁用主设备（辅助设备在 HA 加入后将被禁用）。
 - 思科成功网络
- 在配置高可用性之前，必须先部署任何待处理更改。

高可用性的许可证要求

在配置高可用性之前，设备必须处于相同的状态：两台设备均注册基本许可证，或均处于评估模式。如果设备已注册，可以将其注册到不同的思科智能软件管理器账户，但这些账户的出口控制功能设置的状态必须相同，要么都启用这类设置，要么都禁用。但是，如果您已在设备上启用不同的可选许可证，上述设置便不再重要。

在运行过程中，高可用性对中的设备必须具有相同的许可证。在部署过程中，主用设备进行的任何许可证更改都会在备用设备上重复进行。

高可用性配置需要两种智能许可证权利；对中的每个设备各一个。您必须确保您的账户中有足够的许可证，可应用到每个设备。如果没有足够的许可证，可能会出现一台设备合规，另一台设备不合规的情况。

例如，如果主用设备具有基本许可证和威胁许可证，而备用设备只有基本许可证，备用设备将与思科智能软件管理器通信，以从您的账户获取可用威胁许可证。如果您的智能许可证账户没有足够的已购授权，您的账户将不合规（且备用设备也将不合规，即使主用设备合规），直到您购买正确数量的许可证。



注释

如果将用户注册到存在不同导出受控功能设置的账户，或者尝试创建一个 HA 对，注册其中的一台设备，而将另外一台设备设置为评估模式，则 HA 加入可能会失败。对于受出口控制的功能，如果您使用不一致的设置配置 IPSec 加密密钥，当您激活 HA 后，两个设备都将变为主用状态。这会受影响支持网段上的路由，且您必须手动断开辅助设备上的 HA 才能消除影响。

高可用性指南

其他规定

- 169.254.0.0/16 和 fd00:0:0::*:/64 是内部使用的子网，不能用于故障切换或状态链路。
- 当您在主用设备上运行部署作业时，主用设备的配置会同步到备用设备。但是，在您部署更改之前，某些更改不会显示在待处理更改中，即使它们还未同步到备用设备上。如果您更改以下任一项，所做的更改将会被隐藏，且您必须运行部署作业才能使它们配置在备用设备上。如果您需要立即应用更改，您将需要进行一些其他更改，这些更改会显示在待处理更改中。隐藏的更改包括对以下项目的编辑：规则计划、空间数据库、安全情报或 VDB 更新；备份计划；NTP；管理界面 DNS；许可证授权；云服务选项；URL 过滤选项。
- 您应在主设备和辅助设备上执行备份。要恢复备份，您必须首先中断高可用性。不要在两台设备上恢复相同备份，因为这两台设备都会变成活动状态。相反，您要在想要首先恢复活动状态的设备上恢复备份，然后在另一台设备上恢复等效备份。
- 适用于各种身份源的测试按钮仅在主用设备上可用。如果您需要测试备用设备的身份源连接，必须先切换模式，使备用对等设备变成主用对等设备。

- 创建或中断高可用性配置会在部署配置更改后重新启动两台设备上的 Snort 检测过程。这可能会导致直通流量中断，直到进程完全重新启动。
- 最初配置高可用性时，如果辅助设备上的安全情报和地理位置数据库的版本与主设备上的版本不同，请在辅助设备上安排作业来更新数据库。下一次部署时，从主用设备运行这些作业。即使高可用性加入失败，这些作业仍将保留，并将在下一次部署时执行。
- 如果您通过外部身份源进行身份验证（也即，您不是本地 **admin** 用户），可能无法登录到备用设备。您必须至少登录主用设备一次，并部署配置，之后才能够登录备用设备。此限制不适用于本地 **admin** 用户。
- 当主用设备故障切换到备用设备时，所连接的运行生成树协议 (STP) 的交换机端口在感知到拓扑变化时，会进入阻塞状态 30 秒至 50 秒。当端口处于阻塞状态时，为避免流量丢失，您可以根据交换机启用 STP PortFast 功能：

interface interface_id spanning-tree portfast

此解决方法适用于连接到路由模式和桥接组接口的交换机。链路打开时，PortFast 功能会立即使端口转换到 STP 转发模式。该端口仍会参与 STP。因此，如果端口是环路的一部分，则端口最终会转换为 STP 阻塞模式。

- 发生故障切换事件时，在连接到高可用性对的交换机上配置端口安全性，可能会导致通信问题。一个安全端口上配置或获悉的安全 MAC 地址移至另一安全端口，交换机端口安全功能标记违例时，会发生此问题。
- 对于主用/备用高可用性和 VPN IPSec 隧道，无法使用 SNMP 通过 VPN 隧道监控主用设备和备用设备。备用设备没有有效的 VPN 隧道，将丢弃发往网络管理系统 (NMS) 的流量。您可以改为使用具有加密功能的 SNMPv3，因此不需要 IPsec 隧道。

配置高可用性

使用高可用性设置确保网络连接，即使设备发生故障。设置主用/备用高可用性时，两台设备将链接到一起。如果主用设备发生故障，备用设备会接管相应的角色，因此用户几乎察觉不到连接问题。

以下过程介绍设置主用/备用高可用性 (HA) 对的端到端流程。

过程

- 步骤 1** 准备两台用于高可用性的设备，第 156 页。
- 步骤 2** 配置高可用性的主要设备，第 157 页。
- 步骤 3** 配置高可用性的辅助设备，第 159 页。
- 步骤 4** 配置故障切换运行状况监控条件，第 160 页。

条件包括对等设备监控和接口监控。虽然所有故障切换条件都有默认设置，您至少应检查这些设置，验证是否适用于您的网络。

- 配置对等设备运行状况监控故障切换条件，第 161 页。

- [配置接口运行状况监控故障切换条件](#)，第 162 页。

有关接口测试的信息，请参阅[系统如何测试接口运行状况](#)，第 164 页。

步骤 5（推荐的可选项目。）[配置备用 IP 地址和 MAC 地址](#)，第 164 页。

步骤 6（可选。）[验证高可用性配置](#)，第 165 页。

准备两台用于高可用性的设备

要成功配置高可用性，您需要正确做好多项准备。

过程

步骤 1 确保设备满足[高可用性的硬件要求](#)，第 153 页中列出的要求。

步骤 2 确定使用一个故障切换链路，还是使用单独的故障切换和状态故障切换链路，并确定您将使用的端口。

必须在每台设备上为每个链路使用相同的端口号。例如，在两台设备上均对故障切换链路使用 GigabitEthernet 1/3。确定您要使用哪些端口，避免将其意外用于其他用途。有关详细信息，请参阅[故障切换和状态故障切换链路](#)，第 147 页。

步骤 3 安装设备，将其连接到网络，并在每个设备上完成初始设置向导。

- a) 查看[避免中断故障切换和数据链路](#)，第 149 页中的建议网络设计。
- b) 必须至少连接外部接口，如[连接接口](#)，第 9 页中所述。

您还可以连接其他接口，但是必须确保在每个设备上使用相同的端口连接到指定子网。由于设备将共享相同的配置，必须将它们以并行方式连接到网络中。

注释 安装向导不允许更改管理和内部接口上的 IP 地址。因此，如果您将主要设备上的这些接口连接到网络，不要同时连接辅助设备上的同类接口，否则 IP 地址会发生冲突。您可以直接将工作站连接到其中一个接口并通过 DHCP 获取地址，以便您可以连接到 Firepower 设备管理器并配置设备。

- c) 在每台设备上完成初始设置向导。确保指定外部接口的静态 IP 地址。此外，配置相同的 NTP 服务器。有关详细信息，请参阅[完成初始配置](#)，第 14 页。

为设备选择相同的许可和思科成功网络选项。例如，为每个设备选择评估模式或注册设备。

- d) 在辅助设备上，依次选择**设备 > 系统设置 > 管理接口**并配置唯一的 IP 地址，更改网关（如有必要），并更改或禁用 DHCP 服务器设置，以满足您的需求。
- e) 在辅助设备上，依次选择**设备 > 接口**并编辑内部接口。删除或更改 IP 地址。此外，删除为接口定义的 DHCP 服务器，因为不能在同一网络上有两个 DHCP 服务器。
- f) 在辅助设备上部署配置。
- g) 根据您的网络拓扑要求，登录到主设备，更改管理地址、网关与 DHCP 服务器设置以及内部接口 IP 地址与 DHCP 服务器设置。如果您进行任何更改，请部署配置。

h) 如果您未连接内部接口或管理接口（如果您使用单独的管理网络），现在可以将其连接到交换机。

步骤 4 验证设备是否具有完全相同的软件版本，也即，版本号的大（第一个）、小（第二个）以及维护（第三个）数字均必须相同。您可以在 Firepower 设备管理器的“设备”页面，或者可以在 CLI 中使用 **show version** 命令找到版本。

如果设备未运行相同的软件版本，从 Cisco.com 获取首选的软件版本并将其安装在每台设备上。有关详细信息，请参阅[升级 Firepower 威胁防御软件](#)，第 466 页。

步骤 5 连接和配置故障切换和状态故障切换链路。

- a) 按照您的首选网络设计（从[避免中断故障切换和数据链路](#)，第 149 页选择），酌情将每台设备的故障切换接口连接到交换机或直接互连。
- b) 如果使用单独的状态链路，也请相应地连接每台设备的状态故障切换接口。
- c) 依次登录到每台设备，然后转至**设备 > 接口**。编辑每个接口，并验证没有配置接口名称或 IP 地址。

如果为接口配置了名称，您可能需要从安全区域中删除这些接口和其他配置，然后才能删除名称。如果删除名称失败，检查错误消息以确定需要进行哪些其他更改。

步骤 6 在主设备上，连接剩余的数据接口并配置设备。

- a) 选择**设备 > 接口**，编辑用于直通流量的每个接口和配置主要静态 IP 地址。
- b) 将接口添加到安全区域，并配置处理已连接网络上的流量所需的基本策略。有关示例配置，请参阅[Firepower 威胁防御使用案例](#)，第 29 页中列出的主题。
- c) 部署配置。

步骤 7 验证您是否达到[高可用性的软件要求](#)，第 153 页中所述的所有要求。

步骤 8 确认您有一致的许可（注册或评估模式）。有关详细信息，请参阅[高可用性的许可证要求](#)，第 154 页。

步骤 9 在辅助设备上，将其余数据接口连接到主要设备上对等接口连接的网络。不要配置接口。

步骤 10 在每台设备上，依次选择**设备 > 系统设置 > 云服务**，确认思科威胁协调器和其他云服务（如思科成功网络等）的设置相同。

现在您即可在主设备上配置高可用性。

配置高可用性的主要设备

要设置主用/备用高可用性对，必须先配置主要设备。主设备是您打算在正常情况下应该处于主用模式的设备。辅助设备保持备用模式，直到主设备不可用。

选择您要当做主设备的设备，然后在该设备上登录 Firepower 设备管理器并按照此程序操作。



注释

创建高可用性对后，必须拆分对，才能够按照此过程中的说明编辑配置。

开始之前

确保您为故障切换和状态故障切换链路配置的接口尚未命名。如果当前接口已命名，您必须从使用这些接口的任何策略（包括安全区对象）中将其删除，然后编辑接口以删除名称。接口还必须处于路由模式，而不是被动模式。这些接口必须专用于高可用性配置：不能将其用于任何其他用途。

如果存在任何待处理的更改，必须先部署这些更改，然后才能配置高可用性。

过程

步骤 1 点击 **Device**。

步骤 2 在设备摘要的右侧，点击高可用性组旁边的**配置**。

如果您在设备上第一次配置高可用性，该组将如下所示。



步骤 3 在“高可用性”页面上，点击**主设备框**。

如果已配置辅助设备，并已将配置复制到剪贴板，您可以点击**从剪贴板粘贴**按钮并粘贴配置。这将使用适当的值更新字段，稍后，您可以验证这些值。

步骤 4 配置故障切换链路属性。

故障切换对中的两台设备会不断地通过故障切换链路进行通信，以确定每台设备的运行状态和同步配置更改。有关详细信息，请参阅[故障切换链路](#)，第 147 页。

- **物理接口** - 选择连接到辅助设备用作故障切换链路的接口。此接口必须是未命名的接口。
- **类型** - 选择是否对接口使用 IPv4 或 IPv6 地址。只能配置一种类型的地址。
- **主 IP** - 为此设备上的接口输入 IP 地址。例如：192.168.10.1。对于 IPv6 地址，您必须采用标准表示法添加前缀长度，例如 2001:a0a:b00::a0a:b70/64。
- **辅助 IP** - 输入应在链路的另一端为辅助设备上的接口配置的 IP 地址。地址必须与主地址位于同一子网，且必须与主地址不同。例如，192.168.10.2 或 2001:a0a:b00::a0a:b71/64。
- **子网掩码**（仅限 IPv4）- 输入主/辅助 IP 地址的子网掩码。

步骤 5 配置状态故障切换链路属性。

系统使用状态链路将连接状态信息传送到备用设备。此信息可在发生故障切换时帮助备用设备保留现有连接。您可以使用同一链路作为故障切换链路，也可以配置一个单独的链路。

- **使用相同的接口作为故障切换链路** - 如果您想对故障切换和状态故障切换通信使用单一链路，请选择此选项。如果选择此选项，请继续执行下一步。
- **物理接口** - 如果您想要使用单独的状态故障切换链路，请选择连接到辅助设备的接口，以用作状态故障切换链路。此接口必须是未命名的接口。然后，配置以下属性：
 - **类型** - 选择是否对接口使用 IPv4 或 IPv6 地址。只能配置一种类型的地址。

- **主 IP** - 为此设备上的接口输入 IP 地址。地址必须与用于故障切换链路的地址位于不同子网。例如：192.168.11.1。对于 IPv6 地址，您必须采用标准表示法添加前缀长度，例如 2001:a0a:b00:a::a0a:b70/64。
- **辅助 IP** - 输入应在链路的另一端为辅助设备上的接口配置的 IP 地址。地址必须与主地址位于同一子网，且必须与主地址不同。例如，192.168.11.2 或 2001:a0a:b00:a::a0a:b71/64。
- **子网掩码**（仅限 IPv4） - 输入主/辅助 IP 地址的子网掩码。

步骤 6（可选。）如果您希望对设备对中两台设备之间的通信加密，请输入 **IPsec 加密密钥** 字符串。

必须在辅助节点上配置完全相同的密钥，因此请记住您输入的字符串。

如果您不输入密钥，故障切换和状态故障切换链路上的所有通信都是纯文本。如果您未在接口之间使用直连电缆连接，可能会引发安全问题。



步骤 7 点击**激活高可用性**。

系统立即将配置部署到设备。不需要启动部署作业。如果您没有看到指出配置已保存和部署正在进行的消息，请滚动至页面顶部，查看错误消息。

配置也会被复制到剪贴板。您可以使用 `copy` 命令快速配置辅助设备。为提高安全性，加密密钥不包含在剪贴板复制内容中。

配置完成后，您会收到介绍后续操作的消息。阅读信息后，点击**明白**。

此时，您应转至“高可用性”页面，且设备状态应为“协商”。此状态应在配置对等设备之前切换为“主用”，且对等设备应显示为“故障”，直至开始配置此设备。

PRIMARY DEVICE
Current Device Mode: **Active**  Peer: **Failed** 

现在，您可以配置辅助设备。请参阅[配置高可用性的辅助设备](#)，第 159 页。

注释 所选的接口不直接配置。但是，如果您在 CLI 中输入 `show interface`，您将看到接口正在使用指定的 IP 地址、如果您配置了单独的状态链路，接口被命名为“failover-link”和“stateful-failover-link”。

配置高可用性的辅助设备

为主用/备用高可用性配置主设备后，必须再配置辅助设备。在此设备上登录 Firepower 设备管理器并按照此过程操作。



注释 如果您尚未执行此操作，请将高可用性配置从主设备复制到剪贴板。使用复制/粘贴配置辅助设备比手动输入数据更容易。

过程

步骤 1 点击 **Device**。

步骤 2 在设备摘要的右侧，点击高可用性组旁边的**配置**。

如果您在设备上第一次配置高可用性，该组将如下所示。



步骤 3 在“高可用性”页面上，点击**辅助设备框**。

步骤 4 执行以下操作之一：

- **简单方法** - 点击**从剪贴板粘贴**按钮，粘贴配置并点击**确定**。这将使用适当的值更新字段，稍后，您可以验证这些值。
- **手动方法** - 直接配置故障切换和状态故障切换链路。在辅助设备上输入与主设备完全相同的设置。


步骤 5 如果在主设备上配置了 **IPSec 加密密钥**，请在辅助设备上输入完全相同的密钥。

步骤 6 点击**激活高可用性**。

系统立即将配置部署到设备。不需要启动部署作业。如果您没有看到指出配置已保存和部署正在进行的消息，请滚动至页面顶部，查看错误消息。

配置完成后，您将收到说明已配置高可用性的消息。点击**明白**关闭该消息。

此时，您应转至“高可用性”页面，且设备状态应指明此设备为辅助设备。如果与主要设备连接成功，设备将与主要设备同步，且最终模式应为备用、对等设备应为主用模式。

SECONDARY DEVICE
Current Device Mode: **Standby**  Peer Device: **Active**

注释 所选的接口不直接配置。但是，如果您在 CLI 中输入 **show interface**，您将看到接口正在使用指定的 IP 地址、如果您配置了单独的状态链路，接口被命名为“failover-link”和“stateful-failover-link”。

配置故障切换运行状况监控条件

采用高可用性配置的设备会监控自身的整体运行状况和接口运行状况。

故障切换条件定义运行状况监控指标，以此确定对等设备是否发生故障。如果主用对等设备违反了故障切换条件，会触发故障切换，切换到备用设备。如果备用对等设备违反了故障切换条件，它将被标记为故障，且无法进行故障切换。

您可以仅在主用设备上配置故障切换条件。

下表列出了故障切换触发事件及关联的故障检测时间。

表 5: 基于故障切换条件的故障切换时间

故障触发事件	最小	默认	最大
主用设备断电或停止正常工作。	800 毫秒	15 秒	45 秒
主用设备接口物理链路关闭。	500 毫秒	5 秒	15 秒
主用设备接口正常运行，但是连接问题引发了接口测试。	5 秒	25 秒	75 秒

以下主题介绍如何自定义故障切换运行状况监控条件以及系统如何测试接口。

配置对等设备运行状况监控故障切换条件

高可用性配置中的每个对等设备均通过使用 hello 消息监控故障切换链路判断另一个对等设备的运行状况。当设备在故障切换链路上没有收到三条连续的 Hello 消息时，设备会在每个数据接口（包括故障切换链路）上发送 LANTEST 消息，以验证对等设备是否响应。设备采取的操作取决于另一台设备的响应。

- 如果设备在故障切换链路上收到响应，则不会进行故障切换。
- 如果设备在故障切换链路上未收到响应，但在数据接口上收到响应，设备不会进行故障切换。故障切换链路会标记为发生故障。您应尽快恢复故障切换链路，因为当故障切换发生故障时，设备无法故障切换到备用设备。
- 如果设备未在任何接口上收到响应，则备用设备会切换至主用模式，并将另一台设备分类为故障设备。

您可以配置 hello 消息的轮询和保持时间。

过程

步骤 1 在主用设备上，点击设备。

步骤 2 点击设备摘要右侧的高可用性链接。

故障切换条件将在“高可用性”页面的右侧列中列出。

步骤 3 定义对等设备时间配置。

这些设置决定主用设备可以在多短的时间内故障切换至备用设备。设置的轮询时间越快，设备便可越快检测到故障并触发故障切换。但是，当网络临时堵塞时，更快的检测会导致不必要的切换。默认设置适用于大多数情况。

如果设备在一个轮询周期内未收到故障切换接口上的呼叫数据包，则会通过其余接口进行其他的测试。如果在保持时间内，仍未收到来自对等设备的响应，该设备会被视为发生故障，如果故障设备为主用设备，则备用设备会进行接管，成为主用设备。

- **轮询时间** - hello 消息之间的等待时间。输入 1-15 秒或 200 到 999 毫秒。默认值为 1 秒。
- **保持时间** - 设备必须在故障切换链路上收到 hello 消息的时间，超出此时间仍未收到，则宣布对等设备发生故障。保持时间必须至少是轮询时间的 3 倍。输入 1 到 45 秒或 800 到 999 毫秒。默认值为 15 秒。

步骤 4 点击保存。

配置接口运行状况监控故障切换条件

您可以监控最多 211 个接口，具体取决于您的设备型号。您应监控重要的接口。例如，确保重要网络之间吞吐量的接口。仅当您为其配置备用 IP 地址且接口应始终开启时，才监控接口。

当设备在 2 个轮询期内，未在受监控的接口上收到 Hello 消息，将运行接口测试。如果对于某个接口，所有接口测试均失败，但在另一设备上的此接口继续成功传送流量，则此接口会被视为发生故障。如果达到故障接口的阈值，则会进行故障切换。如果另一设备的接口在所有网络测试中也全部失败，则这两个接口会进入“Unknown”状态，并且不会计入故障切换限制。

如果接口收到任何流量，则该接口会再次变为正常工作状态。如果不再满足接口故障阈值，发生故障的设备会回到备用模式。

您可以使用 **show monitor-interface** 命令，从 CLI 或 CLI 控制台监控接口 HA 状态。有关详细信息，请参阅 [监控高可用性监控接口的状态](#)，第 175 页。



注释 接口关闭时，为了进行故障切换，该接口仍被视为是设备问题。如果设备检测到接口已关闭，将立即发生故障切换（如果您保留 1 个接口的默认阈值），而不等待接口保持时间。仅当设备将接口状态视为 OK 时，接口保持时间才有用，尽管设备并不从对等设备接收呼叫数据包。

开始之前

默认情况下，所有已命名的物理接口均进行高可用性监控。因此，您应禁止监控不重要的物理接口。对于子接口或桥接组，您必须手动启用监控。

要完全禁用接口监控并防止因接口故障导致的故障切换，只需确保未对接口启用高可用性监控。

过程

步骤 1 在主用设备上，点击**设备**。

步骤 2 点击设备摘要右侧的高可用性链接。

故障切换条件将在“高可用性”页面的右侧列中列出。

步骤 3 定义接口故障阈值。

如果故障接口的数量达到阈值，设备会将自身标记为发生故障。如果设备是主用设备，它会故障切换到备用设备。如果设备是备用设备，通过将自身标记为发生故障，主用设备会将此设备视为不可用于故障切换。

设置此条件时，请考虑您要监控多少个接口。例如，如果您仅在 2 个接口上启用监控，则永远不会达到 10 个接口的阈值。编辑接口属性时，通过选择高级选项选项卡上的启用高可用性监控选项，配置接口监控。

默认情况下，如果其中一个监控接口发生故障，设备会将自身标记为故障。

您可以通过选择以下故障切换条件选项之一设置接口故障阈值：

- **超出故障接口数** - 输入接口的原始值。默认值为 1。最大值实际上取决于设备型号，可能不尽相同，但您不能输入超过 211 个。如果您使用此条件，如果您输入的数字超过设备支持，将出现部署错误。请尝试较小的数字或改为使用百分比。
- **超出故障接口的百分比** - 输入 1 到 100 之间的数字。例如，如果您输入 50%，且您正在监控 10 个接口，那么如果 5 个接口发生故障，设备会将自身标记为故障。

步骤 4 定义接口时间配置。

这些设置决定了主用设备能够以多快的速度确定接口是否发生故障。设置的轮询时间越快，设备便可越快检测到接口故障。但是，更快的检测速度可能也会导致繁忙的接口在实际状况良好时被标记为故障，从而造成不必要的频繁故障切换。默认设置适用于大多数情况。

如果接口链路关闭，则不会执行接口测试，如果发生故障的接口数达到或超出配置的接口故障切换阈值，备用设备可能仅在一个接口轮询周期内就会变为主用状态。

- **轮询时间** - 在数据接口上发出呼叫数据包的频率。输入 1-15 秒或 500 到 999 毫秒。默认值为 5 秒。
- **保持时间** - 保持时间确定，从一个呼叫数据包丢失到接口被标记故障的时长。输入 5 - 75 秒。输入的保持时间不得短于设备轮询时间的 5 倍。

步骤 5 点击保存。

步骤 6 对您想要监控的每个接口启用高可用性监控。

a) 选择设备 > 接口。

如果接口被监控，高可用性列的监视器将指示“已启用”。

b) 对要更改监控状态的接口，点击编辑图标 。

您无法编辑故障切换或状态故障切换接口。接口监控不适用于这些接口。

c) 点击高级选项选项卡。

d) 根据需要，选择或取消选择启用高可用性监控复选框。

e) 点击确定。

步骤 7 (可选，但不推荐。) 为监控的接口配置备用 IP 地址和 MAC 地址。请参阅[配置备用 IP 地址和 MAC 地址](#)，第 164 页。

系统如何测试接口运行状况

系统将持续测试监控的接口，确保高可用性正常。用于测试接口的地址取决于配置的地址类型：

- 如果接口上配置了 IPv4 和 IPv6 地址，设备会使用 IPv4 地址执行运行状况监控。
- 如果接口上仅配置了 IPv6 地址，设备会使用 IPv6 邻居发现，而不是 ARP 来执行运行状况监控测试。对于广播 Ping 测试，设备会使用所有的 IPv6 节点地址 (FE02::1)。

系统将在每台设备上执行以下测试：

1. 链路打开/关闭测试 - 一种接口状态测试。如果链路打开/关闭测试指示接口关闭，则视为设备测试失败。如果状态为打开，则设备执行网络活动测试。
2. 网络活动测试 - 接收的网络活动测试。此测试旨在使用 LANTEST 消息生成网络流量，以确定发生故障的设备（如有）。测试开始时，每台设备会清除其接口的收到的数据包计数。在测试期间（最多 5 秒），一旦设备收到数据包，则接口会被视为正常运行。如果一台设备收到流量，另一设备未收到，则未收到流量的设备会被视为已发生故障。如果两台设备均未收到流量，则设备开始进行 ARP 测试。
3. ARP 测试 - 读取设备 ARP 缓存，以获取 2 个最近获得的条目。设备会逐一向这些设备发送 ARP 请求，从而尝试激发网络流量。在每次请求之后，设备会对最多 5 秒内收到的所有流量进行计数。如果收到流量，接口会被视为正常工作。如果未收到任何流量，系统会将 ARP 请求发送到下一台设备。如果到达列表末尾，也没有设备收到流量，设备开始进行 ping 测试。
4. Broadcast Ping 测试 - 包括发出广播 ping 请求的 ping 测试。随后设备会对最多 5 秒内收到的所有数据包进行计数。如果在此时间间隔内的任意时刻收到任何数据包，接口会被认为正常工作，并且会停止测试。如果未收到任何流量，测试将通过 ARP 测试再次开始。

配置备用 IP 地址和 MAC 地址

当您配置接口时，可以在相同网络上指定一个主用 IP 地址和一个备用 IP 地址。虽然建议指定备用 IP 地址，但它并不是必需的。如果没有备用 IP 地址，则主用设备无法执行用于检查备用接口运行状况的网络测试；它只能跟踪链路状态。此外，您也无法出于管理目的，连接到该接口上的备用设备。

1. 当主设备进行故障切换时，辅助设备会使用主设备的 IP 地址和 MAC 地址，并开始传送流量。
2. 此时处于备用状态的设备会接管备用 IP 地址和 MAC 地址。

由于网络设备不会发现 MAC 与 IP 地址配对的变化，网络上的任意位置都不会发生 ARP 条目变化或超时。

如果辅助设备启动时未检测到主设备，辅助设备将成为主用设备，并使用其自己的 MAC 地址，因为它不知道主设备的 MAC 地址。不过，当主设备可用时，辅助（主用）设备会将 MAC 地址更改为主设备的 MAC 地址，这可能会导致网络流量中断。同样，如果您用新硬件替换主设备，将使用新 MAC 地址。

使用虚拟 MAC 地址可防范这种中断，因为对于启动时的辅助设备，主用 MAC 地址是已知的，并在采用新的主设备硬件时保持不变。您可以手动配置虚拟 MAC 地址。

如果您没有配置虚拟 MAC 地址，则可能需要清除连接的路由器上的 ARP 表，以便恢复流量。Firepower 威胁防御设备在 MAC 地址变化时，不会为静态 NAT 地址发送无故 ARP，因此连接的路由器不会知道这些地址的 MAC 地址变化。

过程

步骤 1 选择设备 > 接口。

您至少应为进行高可用性监控的接口配置备用 IP 和 MAC 地址。如果接口被监控，高可用性列的监视器将指示“已启用”。

步骤 2 对要配置备用地址的接口，点击编辑图标 (🔗)。

您无法编辑故障切换或状态故障切换接口。配置高可用性时，您可以为这些接口设置 IP 地址。

步骤 3 在 IPv4 地址和 IPv6 地址选项卡上配置备用 IP 地址。

此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。为要使用的每个 IP 版本配置备用地址。

步骤 4 点击高级选项选项卡，配置 MAC 地址。

默认情况下，系统对接口使用预烧到网络接口卡(NIC)的MAC地址。因此，该接口上的所有子接口都使用相同的MAC地址，也因此您可能想要为每个子接口创建唯一地址。如果您配置高可用性，建议手动配置主用/备用MAC地址。定义MAC地址有助于在故障切换时保持网络中的一致性。

- **MAC 地址** - 采用 H.H.H 格式的介质访问控制地址，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。
- **备用 MAC 地址** - 用于高可用性。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 5 单击 OK。

验证高可用性配置

完成高可用性配置后，验证设备的状态是否表明两台设备均运行正常并处于主用/备用模式。

PRIMARY DEVICE
Current Device Mode: **Active** 🔄 Peer Device: **Standby**

您可以通过以下程序验证高可用性配置是否在工作。

过程

步骤 1 测试您的主用设备是否在通过使用 FTP（例如）来在不同接口上的主机之间发送文件，从而如预期传送流量。

至少应测试从一个工作站到连接到每个已配置的接口系统的连接。

步骤 2 可以通过执行以下任一操作，切换模式，使主用设备立即变成备用设备：

- 在 Firepower 设备管理器上，从 **设备 > 高可用性** 页面的齿轮菜单上选择 **切换模式**。
- 在主用设备的 CLI 中，输入 **no failover active**。

步骤 3 重复连接测试，以验证可以通过高可用性对中的另一台设备进行相同的连接。

如果测试不成功，请验证是否已将设备的接口与另一台设备上的对等接口连接到相同的网络上。

您可以从“高可用性”页面查看 HA 状态。您还可以使用设备的 CLI 或 CLI 控制台，输入 **show failover** 命令检查故障切换状态。此外，使用 **show interface** 命令，验证任何失败的连接测试中所用接口的接口配置。

如果这些操作找不到问题的症结所在，您可以尝试其他操作。请参阅 [高可用性故障排除（故障切换）](#)，第 176 页。

步骤 4 完成后，可以切换模式，使最初处于主用状态的设备恢复主用状态。

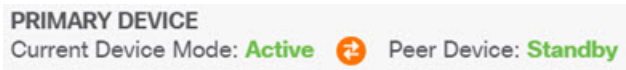
管理高可用性

您可以通过点击 **设备摘要** 页面上的 **高可用性** 链接，管理高可用性对。




“高可用性”页面包括以下内容：

- **角色和模式状态** - 左侧的状态区域显示设备是组中的主要设备还是辅助设备。模式表示此设备处于主用模式还是备用模式，或者高可用性已被暂停还是设备正在等待加入对等设备。它还显示对等设备的状态，可以是主用、备用、暂停或失败状态。例如，当您登录主要设备，并且该设备也是主用设备时，如果辅助设备正常并可在必要时用于故障切换，那么状态将如下所示。您可以点击对等设备之间的图标获取设备之间的配置同步状态信息。



- **故障切换历史记录链路** - 点击此链接可查看高可用性对中设备状态的详细历史记录。系统将打开 CLI 控制台并执行 **show failover history details** 命令。
- **部署历史记录链接** - 点击此链接可转至审核日志，其中事件已过滤为仅显示部署作业。

- **齿轮按钮**  - 点击此按钮可在设备上执行操作。
 - **暂停高可用性/恢复高可用性** - 暂停高可用性会让设备停止作为高可用性对，但不删除高可用性配置。您可以随后在设备上恢复，也即重新启用高可用性。有关详细信息，请参阅[暂停或恢复高可用性，第 167 页](#)。
 - **中断高可用性** - 中断高可用性将从两台设备删除高可用性配置，并将它们恢复为独立设备。有关详细信息，请参阅[中断高可用性，第 168 页](#)。
 - **切换模式** - 切换模式将强制主用设备变成备用设备，或备用设备变为主用设备，具体取决于您在哪台设备上执行操作。有关详细信息，请参阅[切换主用和备用对等设备（强制故障切换），第 169 页](#)。
- **高可用性配置** - 此面板会显示故障切换对对的配置。点击**复制到剪贴板**按钮将信息加载到剪贴板，从其中您可以将其粘贴到辅助设备的配置中。您也可以将其复制到另一个文件中做记录之用。此信息并不显示您是否已定义 IPsec 加密密钥。



注释 高可用性的接口配置不会反映在接口页面上（**设备 > 接口**）。您无法编辑高可用性配置中使用的接口。

- **故障切换条件** - 此面板包含在评估主用设备是否已出现故障、备用设备应变成主用设备时确定运行状况条件使用的设置。调整这些条件，以便您可以获得网络所需的故障切换性能。有关详细信息，请参阅[配置故障切换运行状况监控条件，第 160 页](#)。

以下主题介绍与高可用性配置相关的各种管理任务。

暂停或恢复高可用性

可以暂停高可用性对中的设备。此功能适用于以下情形：

- 两台设备都在主用-主用情况下，且修复故障切换链路上的通信不能更正问题。
- 希望对主用或备用设备进行故障排除，并且不希望设备在此期间发生故障切换。
- 您想要在备用设备上安装软件升级期间阻止故障切换。

暂停高可用性时，停止将设备对用作故障切换设备。当前主用设备保持活动状态，并处理所有用户连接。但是，不会再监控故障切换条件，并且系统永远不会故障切换到现在的伪备用设备。备用设备将保留其配置，但将保持非活动状态。

暂停 HA 和中断 HA 之间的主要区别是，在暂停的 HA 设备上将保留高可用性配置。如果中断 HA，则会清除配置。因此，您可以选择在暂停系统上恢复高可用性，这样可启用现有配置并再次将两台设备设置为故障切换对。

如果您从主用设备暂停高可用性，配置将在主用和备用设备上暂停。如果从备用设备暂停，配置仅在备用设备上暂停，但主用设备不会尝试故障切换至暂停的设备。

只能恢复处于暂停状态的设备。该设备将与对等设备协商主用/备用状态。



注释 如有必要，可以输入 `configure high-availability suspend` 命令从 CLI 暂停 HA。要恢复 HA，请输入 `configure high-availability resume`。

开始之前

如果您通过 Firepower 设备管理器暂停高可用性，高可用性将一直暂停直至您进行恢复，即使您重新加载设备亦如此。但是，如果您通过 CLI 暂停，这样是一种临时状态，重新加载后，设备自动恢复高可用性配置，并与对等设备协商主用/备用状态。

如果您在备用设备上暂停高可用性，请检查主用设备当前是否正在运行部署作业。如果在部署作业进行期间切换模式，部署作业将失败，配置更改也会丢失。

过程

步骤 1 点击 **Device**。

步骤 2 点击设备摘要右侧的高可用性链接。

步骤 3 从齿轮图标 (⚙️) 选择适当的命令。

- **暂停高可用性** - 系统会提示您确认操作。阅读消息，并点击**确定**。高可用性状态应显示设备处于暂停模式。
- **恢复高可用性** - 系统会提示您确认该操作。阅读消息，并点击**确定**。设备与对等设备进行协商后，高可用性状态应恢复正常，或为主用或为备用状态。

中断高可用性

如果您不想让两台设备继续以高可用性对方式运行，可以中断高可用性配置。中断高可用性后，设备会变成独立设备。设备配置将发生如下变化：

- 主用设备保留中断高可用性之前的完整配置，删除高可用性配置。
- 备用设备删除所有接口配置以及高可用性配置。所有物理接口均被禁用，但不会禁用子接口。管理接口保持活动状态，因此您可以登录到设备并重新配置。

中断实际上会如何影响设备取决于执行中断时每台设备的状态。

- 如果设备处于运行状况正常的主用/备用状态，从主用设备中断高可用性。这将从高可用性对的两台设备删除高可用性配置。如果您仅想在备用设备上中断高可用性，您必须登录该设备，先暂停高可用性，然后再中断高可用性。
- 如果备用设备处于暂停或故障状态，从主用设备中断高可用性将仅删除主用设备上的高可用性配置。必须登录备用设备，同时在该设备上中断高可用性。

- 如果对等设备仍协商高可用性或同步其配置，无法中断高可用性。等待协商或同步完成或超时。如果您认为系统会停留在这种状态，您可以暂停高可用性，然后中断高可用性。



注释 使用 Firepower 设备管理器时，不能使用 **configure high-availability disable** 命令从 CLI 中断 HA。

开始之前

要获得理想结果，请将设备置于正常的主用/备用状态，然后从主用设备执行此操作。

过程

步骤 1 点击 **Device**。

步骤 2 点击设备摘要右侧的高可用性链接。

步骤 3 从齿轮图标 (⚙️)，选择中断高可用性。

步骤 4 阅读确认消息，决定是否选择该选项以禁用接口，然后点击**确定**。

如果您从备用设备中断高可用性，必须选择该选项以禁用接口。

系统将立即在此设备和对等设备上部署所做的更改（如果可能）。在每个设备上完成部署，并让每台设备都变成独立设备可能需要几分钟的时间。

切换主用和备用对等设备（强制故障切换）

您可以对正常运行的高可用性对切换主用/备用模式，即一个对等设备处于主用状态，另一个是备用状态。例如，如果您要安装软件升级，可以将主用设备切换为备用设备，以便升级不会影响用户流量。

您可以从主用或备用设备切换模式，但从另一台设备的角度来看，对等设备必须正在运行。如果任何设备被暂停（必须先恢复高可用性）或发生故障，则无法切换模式。



注释 如有必要，可以从 CLI 在主用和备用模式之间切换。从备用设备，输入 **failover active** 命令。从主用设备，输入 **no failover active** 命令。

开始之前

在切换模式之前，验证主用设备没有在执行部署作业。等待部署完成后再切换模式。

如果主用设备包含待处理的未部署更改，请在切换模式之前部署这些更改。否则，如果您从新主用设备运行部署作业，这些更改会丢失。

过程

- 步骤 1 点击 **Device**。
- 步骤 2 点击设备摘要右侧的高可用性链接。
- 步骤 3 从齿轮图标 (⚙️) 中选择切换模式。
- 步骤 4 阅读确认消息，并点击**确定**。

系统将强制进行故障切换，以便主用设备成为备用设备，备用设备成为新的主用设备。

在故障切换后保留未部署的配置更改

对高可用性对中的设备进行配置更改时，需要在主用设备上编辑配置。然后部署更改，即可使用新配置同时更新主用和备用设备。主用设备是主设备还是辅助设备并不重要。

但是，未部署的更改不会在设备之间同步。任何未部署的更改仅在您做出这些更改的设备上可用。

因此，如果在有未部署更改的情况下进行故障切换，这些更改在新主用设备上不可用。但是，这些更改仍保留在现为备用状态的设备上。

要检索未部署的更改，您必须切换模式以强制进行故障切换，将另一台设备恢复为主用状态。当您登录到新主用设备时，未部署的更改可用，可以部署这些更改。从**高可用性**设置齿轮菜单 (⚙️) 使用**模式切换**命令。

记住以下几点：

- 如果从主用设备部署更改时备用设备上存在未部署的更改，备用设备上未部署的更改将被清除。这些更改无法检索。
- 当备用设备加入高可用性对时，备用设备上任何未部署的更改将被清除。每当设备加入或重新加入高可用性对时，都会同步配置。
- 如果包含未部署更改的设备发生灾难性的故障，并且您必须更换或重新映像该设备，未部署的更改会永久丢失。

在高可用性模式下更改许可证和注册

高可用性对中的设备必须具有相同的许可证和注册状态。要进行更改，请执行以下操作：

- 启用或禁用主用设备上的可选许可证。然后，部署配置，备用设备会请求（或释放）必要的许可证。启用许可证时，必须确保思科智能软件管理器账户具有足够的许可证，否则可能会造成一台设备合规，而另一台设备不合规。
- 单独注册或取消注册设备。两台设备必须均处于评估模式，或均已注册，才能正常使用。可以将设备注册到不同的思科智能软件管理器账户，但这些账户的出口控制功能设置的状态必须相同，要么都为启用，要么都为禁用。如果设备的注册状态不一致，将无法部署配置更改。

编辑 HA IPsec 加密密钥或 HA 配置

您可以通过登录到主用设备、进行更改并部署更改来更改任何故障切换条件。

但如果需要更改故障切换链路上使用的 IPsec 加密密钥，或更改故障切换链路或状态故障切换链路的接口或 IP 地址，则必须先中断 HA 配置。然后，可以使用新的加密密钥或故障切换/状态故障切换链路设置重新配置主设备和辅助设备。

将故障设备标记为运行状况正常

在常规运行状况监控过程中，高可用性配置中的设备可能会被标记为发生故障。如果设备运行状况正常，再次满足运行状况监控要求时，设备将恢复正常状态。如果您发现运行状况正常的设备频繁发生故障，您可能需要增加对等设备超时，停止监控相对不重要的特定接口，或更改接口监控超时。

可以从 CLI 输入 **failover reset** 命令，强制将故障设备视为正常设备。我们建议您在主用设备上输入此命令，重置备用设备的状态。可以使用 **show failover** 或 **show failover state** 命令显示设备的故障切换状态。

将故障设备恢复到非故障状态不会自动将其设为主用设备。恢复后的设备仍处于备用状态，直到由于故障切换（强制或自然）变成主用设备。

重置设备状态不能解决导致设备被标记为故障设备的问题。如果您没有解决问题，或放宽监控超时，设备可能会被再次标记为故障设备。

在高可用性设备上安装软件升级

您可以升级高可用性对设备上运行的系统软件，不中断网络中的流量。通常，升级备用设备，以便主用设备可以继续处理流量。升级完成后，切换角色，并再次升级备用设备。

当高可用性组中的设备运行不同的软件版本时，无法实现故障切换。在正常情况下，设备必须运行相同的软件版本。只有当您安装软件升级时，两台设备才能运行不同的版本。

此过程总结了升级流程。有关详细信息，请参阅[升级 Firepower 威胁防御软件](#)，第 466 页。

开始之前

确保在开始升级流程之前从主用节点部署待处理更改。升级设备过程中，在升级一台设备后但未升级另一台设备的间隙，不要进行任何配置更改或启动任何部署，否则部署会失败并可能会丢失更改。

查看任务列表，并确认没有任务正在运行。等所有任务（例如数据库更新）均完成后再安装升级。此外，检查是否有任何已计划的任务。任何计划任务都不得与升级任务重叠。

执行更新前，请确保应用过滤器、访问规则或 SSL 解密规则中不存在已弃用应用。这些应用的应用名称后面带有“(Deprecated)”。虽然无法将已弃用应用添加至这些对象，但后续 VDB 更新可能会使先前有效应用变为弃用应用。如果发生这种情况，则升级将失败，导致设备处于不可用状态。

登录 [Cisco.com](#)，下载升级映像。

- 确保获得适当的升级文件（文件类型为 REL.tar）。请勿下载系统软件包或引导映像。
- 请勿对更新文件重命名。系统将重命名的文件视为无效。

- 您无法降级或卸载补丁。
- 确认您是否正在运行升级所需的基准映像。有关兼容性信息，请参阅《思科 *Firepower* 兼容性指南》，网址是：
<http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html>。
- 阅读有关新版本的版本说明。您可以在 <http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html> 找到发行说明。

过程

步骤 1 登录到备用设备并安装升级。

- a) 选择设备，然后点击“更新”摘要中的**查看配置**。
- b) 通过点击**系统升级组**中的**浏览或上传其他文件**，上传映像。
- c) 点击**安装**开始安装过程。

等待安装完成后，您可以重新登录并验证系统是否运行正常。

注释 如果检查高可用性状态，您可能会看到应用程序同步失败。只有从主用设备部署更改，同时备用设备在升级软件时才会发生这种情况。

步骤 2 在备用设备上，依次点击**设备 > 高可用性**，然后从齿轮菜单 (⚙) 选择**切换模式**。

此操作将强制执行故障切换，将登录设备变成主用设备。等待设备的状态更改为主用。

继续操作之前，您可以选择性地测试网络，确保流量流经设备连接的网络。

步骤 3 登录到新的备用设备，即原来的主用设备，并安装升级。

流程与上面介绍的流程相同。必须上传软件升级；升级不会从另一台设备复制。

安装完成后，重新登录到备用设备，验证安装成功，且设备恢复为正常主用/备用状态。此设备不会自动恢复主用状态。

注释 如果检查高可用性状态，应看不到应用程序同步失败。设备现在运行相同的软件版本，因此应该能够从主用设备导入配置。如果自动部署失败，或者如果设备不会以其他方式进入备用就绪状态，请点击齿轮菜单中的**恢复 HA**。

步骤 4 登录到当前处于主用状态的设备。如果有任何待处理更改，部署这些更改并等待部署成功完成。

步骤 5 （可选。）如果您希望当前的备用设备恢复主用状态，请依次点击**设备 > 高可用性**，然后从任一设备的齿轮菜单中选择**切换模式**。

例如，如果主设备在开始此过程时为主用设备，而且您也希望保留这种设置，可切换模式。

升级 HA 设备时部署更改

如果正处于在高可用性组中的设备上升级系统软件的过程中，则有时备用设备运行高于主用设备的软件版本。正常情况下，此时切换模式，使备用设备成为主设备，然后升级第二台设备。

但是，若升级一半时发现必须更改主设备配置，则必须执行以下步骤以便能够部署更改。

过程

- 步骤 1** 在备用设备（运行较新软件版本的设备）上，从“高可用性”页面上的齿轮菜单(⚙️)中选择**挂起 HA**。
- 步骤 2** 在主用设备上，部署更改。等待部署成功完成。
- 步骤 3** 在挂起的备用设备上，从“高可用性”页面上的齿轮菜单(⚙️)中选择**恢复 HA**。设备将从主用设备同步其配置，并获取最新更改。
- 步骤 4** 在恢复的备用设备上，从高可用性页面上的齿轮菜单(⚙️)中选择**切换模式**。这会使备用设备成为主用设备，而且可以继续升级。请参阅[在高可用性设备上安装软件升级](#)，第 171 页。

更换高可用性对中的设备

如有必要，您可以更换高可用性组中的一个设备，而不中断网络流量。

过程

- 步骤 1** 如果要更换的设备能够正常使用，请确保故障切换至对等设备，然后从该设备 CLI 使用 **shutdown** 命令正常关闭设备。如果设备不能使用，确认对等设备在主用模式下运行。
- 步骤 2** 从网络中删除设备。
- 步骤 3** 安装替换设备并重新连接接口。
- 步骤 4** 在替换设备上完成设备安装向导。
- 步骤 5** 在对等设备上，转到“高可用性”页面，并将配置复制到剪贴板。请注意，设备是主设备还是辅助设备。

如果有任何待处理更改，请现在部署这些更改并等待部署完成后再继续。

- 步骤 6** 在替换设备上，点击**高可用性**中的**配置**，然后选择与对等设备相反的设备类型。也即，如果对等设备为主设备，选择**辅助**，如果对等设备为辅助设备，选择**主**。
- 步骤 7** 从对等设备粘贴高可用性配置，然后输入 IPsec 密钥，如果您在使用。点击**激活高可用性**。

部署完成后，设备将与对等设备通信并加入高可用性组。系统随即导入主用对等设备的配置，且根据您的选择替换设备可以在组中充当主要或辅助设备。您现在可以验证高可用性运行是否正常，而且如果需要，可切换模式使新设备变成主用设备。

监控高可用性

以下主题介绍如何监控高可用性。

请注意，事件查看器和控制面板仅显示与您所登录设备相关的数据。它们不会显示两台设备的合并信息。

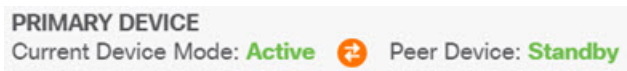
监控常规故障切换状态和历史记录

您可以使用以下方法监控常规高可用性状态和历史记录：

- 在“设备摘要”上（点击设备），高可用性组会显示设备状态。



- 在“高可用性”页面上（依次点击设备 > 高可用性），您可以看到两台设备的状态。点击两台设备之间的同步图标了解更多状态。



- 从“高可用性”页面，点击状态旁边的故障切换历史记录链接。系统将打开 CLI 控制台并执行 `show failover history details` 命令。您还可以直接在 CLI 或 CLI 控制台中输入此命令。

CLI 命令

从 CLI 或 CLI 控制台中，您可以使用以下命令：

- **show failover**

显示有关设备的故障切换状态的信息。

- **show failover history [details]**

显示过去的故障切换状态更改和状态变化的原因。添加 **details** 关键字可显示对等设备的故障切换历史记录。此信息可帮助进行故障排除。

- **show failover state**

显示两个设备的故障切换状态。信息包括设备的主要或辅助状态、设备的主用/备用状态以及最新报告的故障切换原因。

- **show failover statistics**

显示故障切换接口传输和接收的数据包计数。例如，如果输出接口显示设备发送数据包，但未收到任何数据包，那么链路可能出现故障。这可能是电缆问题、对等设备上配置的 IP 地址，或可能是设备将故障切换接口连接到不同的子网。

```
> show failover statistics
```



```
tx:320875
rx:0
```

• show failover interface

显示故障切换和状态故障切换链路的配置。例如：

```
> show failover interface
  interface failover-link GigabitEthernet1/3
    System IP Address: 192.168.10.1 255.255.255.0
    My IP Address    : 192.168.10.1
    Other IP Address : 192.168.10.2
  interface stateful-failover-link GigabitEthernet1/4
    System IP Address: 192.168.11.1 255.255.255.0
    My IP Address    : 192.168.11.1
    Other IP Address : 192.168.11.2
```

• show monitor-interface

显示为高可用性监控的接口的相关信息。有关详细信息，请参阅[监控高可用性监控接口的状态](#)，第 175 页。

• show running-config failover

显示运行配置中的故障切换命令。以下是配置高可用性的命令。

监控高可用性监控接口的状态

如果对任何接口启用了高可用性监控，您可以使用 **show monitor-interface** 命令在 CLI 或 CLI 控制台中查看受监控接口的状态。

```
> show monitor-interface
This host: Primary - Active
  Interface inside (192.168.1.13): Normal (Monitored)
  Interface outside (192.168.2.13): Normal (Monitored)
Other host: Secondary - Standby Ready
  Interface inside (192.168.1.14): Normal (Monitored)
  Interface outside (192.168.2.14): Normal (Monitored)
```

受监控接口可以具有以下状态：

- (Waiting) 并显示任何其他状态（例如 Unknown）(Waiting) - 接口尚未从对等设备上的相应接口收到呼叫数据包。
- Unknown - 初始状态。此状态也可能意味着状态无法确定。
- Normal - 接口正在接收流量。
- Testing - 接口上有 5 个轮询时间未收听到 Hello 消息。
- Link Down - 接口或 VLAN 通过管理方式关闭。
- No Link - 接口的物理链路关闭。

- Failed - 在接口上没有收到流量，但在对等体接口上收听到流量。

监控与高可用性相关的系统日志消息

系统在优先级别 2 发出大量与故障切换有关的系统日志消息，级别 2 表示一种关键情况。与故障切换关联的消息 ID 的范围是：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx 和 727xxx。例如，105032 和 105043 表示故障切换链路存在问题。有关系统日志消息的说明，请参阅思科 *Firepower* 威胁防御系统日志消息指南 (https://www.cisco.com/c/en/us/td/docs/security/firepower/Syslogs/b_fptd_syslog_guide.html)。



注释 故障切换期间，系统按照逻辑先关闭接口，再启动接口，从而生成日志消息 411001 和 411002。这是正常活动。

必须先先在 **设备 > 日志记录设置** 上配置诊断日志记录，才能查看系统日志消息。设置外部系统日志服务器，以便您可以稳定持续地监控消息。

在对等设备上远程执行 CLI 命令

在 CLI 中，您可以使用 `failover exec` 命令在对等设备上输入 `show` 命令，无需登录到对等设备。

failover exec {active | standby | mate} 命令

必须指明哪一台设备应执行命令，主用设备还是备用设备，或输入 **mate**，如果您想要另一台设备而非您登录的设备响应。

例如，如果您想要查看对等设备的接口配置和统计信息，可以输入：

```
> failover exec mate show interface
```

您不能输入 **configure** 命令。此功能与 **show** 命令搭配使用。



注释 如果您登录到主用设备，可以使用 **failover reload-standby** 命令重新加载备用设备。

不能通过 Firepower 设备管理器 CLI 控制台输入这些命令。

高可用性故障排除（故障切换）

如果高可用性组中设备的表现未能达到预期，请考虑以下步骤排除配置故障。

如果主用设备显示对等设备出现故障，请参阅 **设备故障状态故障排除**，第 178 页。

过程

步骤 1 从每个设备（主要和辅助设备）：

- 对故障切换链路的另一设备的 IP 地址执行 ping 操作。
- 如果您使用单独的链接，对状态故障切换链路的另一设备的 IP 地址执行 ping 操作。

如果 ping 操作失败，请确保每个设备上的接口都连接到同一网段。如果您使用直连电缆连接，请检查电缆。

步骤 2 进行以下一般检查：

- 检查主要和辅助设备上是否存在重复的管理 IP 地址。
- 检查两台设备上是否存在重复的故障切换和状态故障切 IP 地址。
- 检查每台设备上的等效接口端口是否连接到同一网段。

步骤 3 检查备用设备上的任务列表或审核日志。主用设备上每次部署成功后，您都应该看到“从活动节点导入配置”任务。如果任务失败，请检查故障切换链路，并再次尝试部署。

注释 如果任务列表指示存在失败的部署任务，则可能是在部署作业期间发生了故障切换。如果启动部署任务时备用设备是主用设备，但在任务期间发生了故障切换，则部署将失效。要解决此问题，请切换模式，使备用设备再次成为主用设备，然后重新部署配置更改。

步骤 4 使用 **show failover history** 命令获取有关设备上状态更改的详细信息。

查找以下情况：

- 应用同步失败：

```
12:41:24 UTC Dec 6 2017
App Sync      Disabled      HA state progression failed due to APP SYNC timeout
```

在应用同步阶段，将配置从主用设备传输到备用设备。应用同步失败会导致设备被禁用，使设备无法再被设置为主用设备。

如果设备因应用同步问题被禁用，您可能需要对故障切换和状态故障切换链路的端点使用设备上的其他接口。必须对链路的两端使用相同的端口号。

如果 **show failover** 命令显示辅助设备处于伪备用状态，这可能意味着您在辅助设备上为故障切换链路配置的 IP 地址与您在主设备上配置的地址不同。确保在两台设备为故障切换链路使用相同的主要/辅助 IP 地址。

伪备用状态也可能表示您在主设备和辅助设备上配置的 IPsec 密钥不同。

有关其他应用同步问题，请参阅[高可用性应用同步失败故障排除](#)，第 179 页。

- （从主用转到备用，然后再切换）的异常频繁地故障切换可能意味着故障切换链路出现问题。最坏的情况是，两台设备可能都变为主用状态，导致流经的流量中断。对链路的两端执行 ping 操作以验证连接性。您还可以使用 **show arp** 检查故障切换 IP 地址和 ARP 映射是否正确。

如果故障切换链路正常，并配置正确，请考虑增加对等设备轮询和保持时间、接口轮询和保持时间，减少高可用性监控的接口数量，或增加接口阈值。

- 接口检查导致的故障。接口检查原因包括被视为故障的接口列表。检查这些接口，以确保它们配置正确，并且不存在硬件问题。验证链路另一端的交换机配置没有问题。如果没有任何问题，请考虑在这些接口上禁用高可用性监控，或者增加接口故障阈值或时间。

06:17:51 UTC Jan 15 2017

```
Active      Failed      Interface check

                This Host:3

                admin: inside

                ctx-1: ctx1-1

                ctx-2: ctx2-1

                Other Host:0
```

步骤 5 如果无法检测到备用设备，而且您找不到具体原因（例如，故障切换链路路上的 LAN 错误或电缆连接出错等），请尝试以下步骤。

- 在备用设备上登录 CLI 并输入 **failover reset** 命令。此命令应将设备从故障状态更改为无故障状态。现在，检查主用设备上的高可用性状态。如果现在可检测到备用对等设备，则问题解决。
- 在主用设备上登录 CLI 并输入 **failover reset** 命令。这会重置主用和备用设备上的高可用性状态。理想情况下，它将重新建立设备之间的链路。检查高可用性状态。如果状态仍然不正确，请继续。
- 在主用设备的 CLI 或从 Firepower 设备管理器首先暂停高可用性，然后恢复高可用性。CLI 命令是 **configure high-availability suspend** 和 **configure high-availability resume**。
- 如果这些操作失败，请对备用设备执行 **reboot** 命令。

设备故障状态故障排除

如果一台设备在对等设备的高可用性状态中被标记为故障设备（在设备或设备 > 高可用性页），可能有如下原因，假设设备 A 是主用设备，设备 B 是出现故障的对等设备。

- 如果设备 B 尚未配置高可用性（仍然是单机模式），设备 A 显示设备 B 为故障设备。
- 如果在设备 B 上暂停高可用性，设备 A 将显示设备 B 为故障设备。
- 如果重新启动设备 B，设备 A 将显示设备 B 为故障设备，直至 B 完成重新启动并通过故障切换链路恢复通信。

- 如果应用同步 (App Sync) 在设备 B 上失败，设备 A 将显示设备 B 为故障设备。请参阅[高可用性应用同步失败故障排除](#)，第 179 页。
- 如果设备 B 在设备或接口运行状况监控中表现不合格，设备 A 将其标记为故障设备。检查设备 B 是否出现系统性问题。请尝试重启设备。如果设备大体运行状况正常，请考虑放宽设备或接口运行状况监控设置。**show failover history** 输出应提供有关接口运行状况检查失败的信息，
- 如果两台设备都变为主用状态，那么每台设备都会将对等设备显示为故障设备。这通常表示故障切换链路出现问题。

还可以指出与许可相关的问题。设备必须有一致的许可，要么均处于评估模式，要么都已注册。如果已注册，使用的智能许可证账户可以不同，但两个账户的导出受控功能设置必须相同，均为启用或禁用。对于受出口控制的功能，如果您使用不一致的设置配置 IPSec 加密密钥，当您激活 HA 后，两个设备都将变为主用状态。这会影响受支持网段上的路由，且您必须手动断开辅助设备上的 HA 才能消除影响。

高可用性应用同步失败故障排除

如果对等设备无法加入高可用性组，或在您从主用设备部署更改时发生故障，请登录发生故障的设备，转至[高可用性](#)页面，然后点击[故障切换历史记录](#)链接。如果 **show failover history** 输出指出应用同步失败，即表示在 HA 验证阶段（在此过程中，系统检查设备是否可以作为高可用性组正常运行）出现问题。

这种故障可能会如下所示：

```

=====
From State           To State           Reason
=====
16:19:34 UTC May 9 2018
Not Detected        Disabled           No Error

17:08:25 UTC May 9 2018
Disabled            Negotiation       Set by the config command

17:09:10 UTC May 9 2018
Negotiation         Cold Standby      Detected an Active mate

17:09:11 UTC May 9 2018
Cold Standby        App Sync          Detected an Active mate

17:13:07 UTC May 9 2018
App Sync            Disabled          CD App Sync error is
High Availability State Link Interface Mismatch between Primary and Secondary Node

```

理想情况下，当 From State 为 App Sync 时，您希望收到的消息是 “All validation passed”，并且节点的状态变为 Standby Ready。任何验证失败都会将对等设备的状态转换成 Disabled (Failed)。您必须解决这些问题，使对等设备能够再次用作高可用性组。请注意，如果通过对主用设备进行更改来修复应用同步错误，则必须先对其进行部署，然后再恢复高可用性以使对等节点加入。

以下消息表示发生了故障，并介绍如何解决问题。这些错误可能发生在节点加入和每次后续部署时。节点加入期间，系统会对主用设备上的最新部署配置执行检查。

- 主要和辅助节点之间的许可证注册模式不匹配。

许可证错误指出，一台对等设备已注册，而另一台对等设备处于评估模式。对等设备必须同时为注册状态或同处于评估模式，才能加入高可用性组。由于无法将注册设备恢复为评估模式，必须从**设备 > 智能许可证**页面注册另一台对等设备。

如果您注册的设备为主用设备，请在注册设备后执行部署。部署将强制设备刷新并同步配置，从而允许辅助设备正确加入高可用性组。

- 主要和辅助节点之间的许可证导出合规性不匹配。

许可证合规性错误表示，设备注册到不同的思科智能软件管理器账户，并且其中一个账户启用了出口控制功能，而另一个账户没有启用。必须使用具有相同出口控制功能设置（启用或禁用）的账户注册设备。在**设备 > 智能许可证**页面上更改设备注册。

- 主要和辅助节点之间的软件版本不匹配。

软件不匹配错误表示，对等设备运行不同版本的Firepower威胁防御软件。一次在一台设备上安装软件升级时，系统仅临时允许不匹配。但是，您无法在升级对等设备的过程中部署配置更改。要解决此问题，请升级对等设备，然后重新部署。

- 主要和辅助节点之间的物理接口计数不匹配。

高可用性组中的设备必须具有相同数量和类型的物理接口。此错误表示，设备上的接口不相同。您必须要么选择不同的对等设备，要么在缺少接口模块的对等设备上安装这些模块。

- 主要和辅助节点之间的故障切换链路接口不匹配。

将每台设备的故障切换物理接口连接到网络时，必须选择相同的物理接口。例如，每台设备上的GigabitEthernet1/8接口。此错误表示您使用不同的接口。要解决错误，请更正对等设备上的电缆。

- 主要和辅助节点之间的状态故障切换链路接口不匹配。

如果您使用单独的状态故障切换链路，将每台设备的状态故障切换物理接口连接到网络时，必须选择相同的物理接口。例如，每台设备上的GigabitEthernet1/7接口。此错误表示您使用不同的接口。要解决错误，请更正对等设备上的电缆。

- 主要和辅助节点之间的设备型号不匹配。

加入高可用性组的对等设备必须是型号完全相同的设备。此错误消息表示，对等设备的设备型号不相同。必须选择不同的对等设备来配置高可用性。

- 发生未知错误，请重试。

应用同步期间出现问题，但系统无法识别该问题。再次尝试部署配置。

- 规则数据包损坏。请更新规则数据包，并重试。

入侵规则数据库出现问题。在发生故障的对等设备上，请转至**设备 > 更新**，然后点击规则组中的**立即更新**。等待更新完成，然后部署更改。然后，您可以从主用设备重试部署。

- 思科成功网络在主用设备上启用，但未在备用设备上启用。

为处于评估模式的设备配置高可用性时，必须在对等设备上选择相同的思科成功网络参与选项。要解决此错误，请转至**设备 > 系统设置 > 云服务**，并启用**思科成功网络**。

- 思科 Defense Orchestrator 在主用设备上启用，但未在备用设备上启用。

为处于评估模式的设备配置高可用性时，必须在对等设备上选择相同的思科 Defense Orchestrator 选项。要么都选择注册选项，要么都不选择。要解决此错误，请转至**设备 > 系统设置 > 云服务**，将设备注册到**思科威胁协调器组**。

- 部署数据包损坏。请重试。

这是一个系统错误。再次尝试部署，应该能解决此问题。



第 10 章

接口

以下主题介绍如何在 FTD 设备上配置接口。

- [关于 FTD 接口，第 183 页](#)
- [接口的准则与限制，第 186 页](#)
- [配置物理接口，第 188 页](#)
- [配置桥接组，第 191 页](#)
- [配置 VLAN 子接口和 802.1Q 中继，第 195 页](#)
- [配置被动接口，第 199 页](#)
- [配置高级接口选项，第 202 页](#)
- [添加接口到虚拟 Firepower 威胁防御，第 206 页](#)
- [监控接口，第 207 页](#)
- [接口示例，第 208 页](#)

关于 FTD 接口

FTD 包括数据接口和管理/诊断接口。

将电缆（以物理方式或虚拟方式）连接到接口接头时，您需要配置该接口。至少需要命名并启用该接口，该接口才会传输流量。如果该接口是桥接组的成员，此配置就已足够。对于非桥接组成员，您还需要为该接口指定一个 IP 地址。如果要在特定端口上创建 VLAN 子接口（而非单一物理接口），通常要在该子接口（而不是物理接口）上配置 IP 地址。通过 VLAN 子接口，可以将一个物理接口拆分为多个标记有不同 VLANID 的逻辑接口，这一点在您连接到交换机的中继端口时非常有用。请勿在被动接口上配置 IP 地址。

接口列表列出了可用的接口、接口名称、地址、模式以及状态。您可以直接在接口列表中更改接口的状态，打开接口或将其关闭。列表将基于您的配置显示接口特征。使用桥接组接口上的开/关箭头可查看成员接口，这些成员接口也会显示于列表中。有关如何将这些接口映射到虚拟接口和网络适配器的信息，请参阅 [VMware 网络适配器和接口如何映射到 Firepower 威胁防御物理接口，第 12 页](#)。

以下主题介绍了通过 Firepower 设备管理器配置接口的局限性及其他接口管理概念。

接口模式

可以为每个接口配置下列其中一种模式：

路由

每个第 3 层路由接口都需要唯一子网上的一个 IP 地址。通常会将这些接口与交换机、另一个路由器上的端口或 ISP/WAN 网关连接。

被动

被动接口使用交换机 SPAN（交换端口分析器）或镜像端口监控在网络中传输的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。

BridgeGroupMember

桥接组是指 FTD 网桥（而非路由）的接口组。所有接口位于同一网络上。桥接组由在网桥网络上有 IP 地址的桥接虚拟接口 (BVI) 表示。

如果指定 BVI，您可以在路由接口和 BVI 之间路由。在这种情况下，BVI 充当成员接口和路由接口之间的网关。如果不指定 BVI，桥接组成员接口上的流量不能离开桥接组。通常，可以指定该接口，以便将成员接口路由到互联网。

在路由模式下，桥接组的一个用途是在 Firepower 威胁防御设备上使用额外接口，而不使用外部交换机。您可以将终端直接连接到桥接组成员接口。您还可以连接交换机，以将更多终端添加到与 BVI 相同的网络。

管理/诊断接口

标记为“管理”的物理端口（对于 Firepower 威胁防御虚拟，则为 Management0/0 虚拟接口）实际上有两个与其关联的单独接口。

- 管理虚拟接口 - 此 IP 地址用于系统通信。这是系统用于进行智能许可和检索数据库更新的地址。您可以打开它的管理会话（Firepower 设备管理器和 CLI）。您必须配置一个管理地址，该地址在 **系统设置 > 管理界面** 上定义。
- 诊断物理接口 - 此物理管理端口的实际名称为“诊断”。您可以使用此接口将系统日志消息发送到外部系统日志服务器。为诊断物理接口配置 IP 地址是可选项。配置该接口的唯一原因是您需要将它用于系统日志。此接口显示在 **设备 > 接口** 页面上，并可在此页面上进行配置。诊断物理接口只允许管理流量，而不允许穿越流量。

（硬件设备。）建议配置管理/诊断接口时，不要将物理端口连接到网络。而是仅配置管理 IP 地址，并把它配置为将数据接口用作从互联网获取更新的网关。然后，打开 HTTPS/SSH 流量（默认情况下启用 HTTPS）的内部接口，并使用内部 IP 地址打开 Firepower 设备管理器（请参阅 [配置管理访问列表](#)，第 447 页）。

对于 Firepower 威胁防御虚拟，建议的配置是将 Management0/0 连接到与内部接口相同的网络，并将内部接口用作网关。不要为诊断接口配置单独的地址。

配置单独管理网络的建议

（硬件设备。）如果要使用单独管理网络，请将物理管理/诊断接口连接到交换机或路由器。

对于 Firepower 威胁防御虚拟，请将 Management0/0 连接到不同于任何数据接口的独立网络。如果仍然使用默认 IP 地址，则需要更改管理 IP 地址或内部接口 IP 地址（因为它们在同一子网上），

然后，进行以下配置：

- 依次选择**设备 > 系统设置 > 管理接口**，并配置所连接网络上的 IPv4 或 IPv6 地址（或两者）。如果需要，可以配置 DHCP 服务器以便能向网络上的其他终端提供 IPv4 地址。如果路由器在管理网络上有到互联网的路由，则可将其作为网关来使用。如果没有，请使用数据接口作为网关。
- 仅当您打算通过该接口向系统日志服务器发送系统日志消息时，才需要为诊断接口配置地址（在**设备 > 接口**上）。否则，不要为诊断接口配置地址，因为不需要。您配置的任何 IP 地址必须与管理 IP 地址在同一子网上，并且不能在 DHCP 服务器池中。例如，默认配置使用 192.168.45.45 作为管理地址，192.168.45.46 至 192.168.45.254 作为 DHCP 池，因此您可以使用从 192.168.45.1 到 192.168.45.44 的任何地址配置诊断接口。

单独的管理网络的管理/诊断接口配置的限制性

如果连接物理管理接口，或对于 Firepower 威胁防御虚拟，将 Management0/0 连接到单独的网络，请确保遵循以下限制：

- 如果需要一台位于管理网络中的 DHCP 服务器，请在管理接口上配置该服务器（**设备 > 系统设置 > 管理接口**）。不能在诊断（物理）接口上配置 DHCP 服务器。
- 如果管理网络中存在另一台 DHCP 服务器，请禁用该服务器或管理接口上运行的 DHCP 服务器。通常而言，一个给定子网中的 DHCP 服务器不应超过一台。
- 如果同时为管理接口和诊断接口配置地址，请确保其位于同一子网中。
- （仅硬件设备。）您可以使用数据接口作为管理网关，即便为诊断接口配置了 IP 地址。但是，诊断接口不会使用该数据接口作为网关。如果需从诊断接口通往其他网络的路径，则需要由位于管理网络中的另一台路由器来路由源于诊断 IP 地址的流量。如有必要，请为诊断接口配置静态路由（依次选择**设备 > 路由**）。

安全区域

可为每个接口分配一个安全区域。然后根据区域应用您的安全策略。例如，您可以将内部接口分配到内部区域，而将外部接口分配到外部区域。例如，可以配置访问控制策略，允许流量从内部传到外部，但不允许从外部传入内部。

每个区域都有一个模式，路由或被动模式。该模式与接口模式直接关联。您可以仅向同一模式安全区添加路由和被动接口。

对于桥接组，可将成员接口添加到区域，但不能添加桥接虚拟接口 (BVI)。

不能将诊断/管理接口包括在区域中。区域只适用于数据接口。

可在**对象**页面创建安全区域。

IPv6 编址

您可以为 IPv6 配置两种类型的单播地址：

- 全局 - 全局地址是可在公用网络上使用的公用地址。对于桥接组，需要在桥接虚拟接口 (BVI) 上而非每个成员接口上配置全局地址。不能将以下任何地址指定为全局地址。
 - 内部保留的 IPv6 地址：fd00::/56 (fd00:: 至 fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
 - 未指定的地址，例如 ::/128
 - 环回地址 ::1/128
 - 组播地址 ff00::/8
 - 链路本地地址 fe80::/10
- 链路本地 - 链路本地地址是只能在直连网络上使用的专用地址。路由器不使用链路本地地址转发数据包；它们仅用于在特定物理网段上通信。链路本地地址可用于地址配置或网络发现功能，例如地址解析和邻居发现。在桥接组中，对 BVI 启用 IPv6 将为每个桥接组成员接口自动配置链路本地地址。每个接口必须有自己的地址，因为链路本地地址仅在网段中可用，并且会与接口 MAC 地址绑定。

至少需要配置链路本地地址，IPv6 才会起作用。如果配置全局地址，则接口上会自动配置链路本地地址，因此无需另外专门配置链路本地地址。如果不配置全局地址，则需要自动或手动配置链路本地地址。

Auto-MDI/MDIX 功能

对于 RJ-45 接口，默认的自动协商设置还包括 Auto-MDI/MDIX 功能。Auto-MDI/MDIX 在自动协商阶段检测直通电缆时执行内部交叉，从而消除交叉布线的需要。如要启用接口的 Auto-MDI/MDIX，必须将速度或双工设置为自动协商。如果将速度和双工明确设置为固定值，从而禁用了两种设置的自动协商，则 Auto-MDI/MDIX 也将被禁用。对于千兆以太网，当速度和双工被设置为 1000 和全值时，接口始终会自动协商；因此，Auto-MDI/MDIX 始终会启用，且您无法禁用它。

接口的准则与限制

以下主题介绍接口的局限性。

接口配置的局限性

使用 Firepower 设备管理器配置设备时，接口配置存在许多局限性。如果您需要以下任意功能，则必须使用 Firepower 管理中心来配置设备。

- 仅支持路由防火墙模式。无法配置透明防火墙模式的接口。
- 可以配置被动接口，但不能配置 ERSPAN 接口。

- 不能将接口配置为内联（在内联集内）或内联分路，用于仅 IPS 的处理。仅 IPS 模式的接口将绕过许多防火墙检查，仅支持 IPS 安全策略。相比之下，防火墙模式接口需要对流量执行防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组和 TCP 规范化。另外，您还可以根据安全策略，选择配置该防火墙模式接口的 IPS 功能。
- 无法配置 EtherChannel 或冗余接口。
- 仅可添加一个桥接组。
- 无法为 IPv4 配置 PPPoE。如果将互联网接口连接到 DSL、电缆调制解调器或 ISP 的其他连接，且 ISP 使用 PPPoE 为您提供 IP 地址，则您必须使用 Firepower 管理中心来配置这些设置。
- 对于 ASA 5515-X、5525-X、5545-X 和 5555-X 以及 Firepower 2100 系列，可安装可选网络接口模块。仅在引导程序期间（即初始安装或重新映像，或在本地/远程管理之间切换时），才会发现网络接口模块。Firepower 设备管理器为这些接口设置正确的速度和双工默认值。如果将可选网络接口模块替换为更改接口速度/双工选项的模块，而不更改可用接口的总数，则重新启动设备，以便系统识别替换接口的正确速度/双工值。在与设备的 SSH 或控制台会话中，输入 **reboot** 命令。然后，在 Firepower 设备管理器中，编辑能够更改的各物理接口，并选择有效的速度和双工选项，因为系统不会自动更正您的原始设置。立即部署更改，确保系统行为正确无误。



注释 将模块更换为更改接口总数的模块，或移除其他对象引用的接口，均可能导致意外问题。如果需要进行此类更改，请先删除待移除接口的所有引用，如安全区成员资格、VPN 连接等。此外，建议您在更改前进行备份。

- 对于 Firepower 威胁防御虚拟设备，仅在重新初始化设备（如[添加接口到虚拟 Firepower 威胁防御](#)，第 206 页所述）后才可添加或删除接口。但是，如果仅将接口替换为速度/双工能力不同的接口，请重启设备，以便系统识别新的速度/双工值。在 CLI 控制台中，输入 **reboot** 命令。然后，在 Firepower 设备管理器中，编辑能够更改的各接口，并选择有效的速度和双工选项，因为系统不会自动更正您的原始设置。立即部署更改，确保系统行为正确无误。

各设备型号的最大 VLAN 子接口数量

设备型号限制可配置的最大 VLAN 子接口数量。请注意，仅可在数据接口上而不可在管理接口上配置子接口。

下表介绍各设备型号的限制。

型号	最大 VLAN 子接口数量
Firepower 2100	1024
Firepower 威胁防御虚拟	50
ASA 5508-X	50
ASA 5515-X	100

型号	最大 VLAN 子接口数量
ASA 5516-X	100
ASA 5525-X	200
ASA 5545-X	300
ASA 5555-X	500
ISA 3000	25

配置物理接口

要使用启用物理接口，至少必须启用它。。通常，您还需要为它命名并配置 IP 寻址。如果要创建 VLAN 子接口，或者配置被动模式接口，或者要将接口添加到桥接组，无需配置 IP 寻址。



注释 要将物理接口配置为被动接口，请参阅[将物理接口配置为被动模式](#)，第 201 页。

您可以禁用接口，以临时阻止在相连网络中的传输。无需删除该接口的配置。

过程

步骤 1 点击 **设备**，然后点击**接口摘要**中的链接。

接口列表将显示可用的接口及其名称、地址和状态。

步骤 2 点击要编辑的物理接口的编辑图标 (🔗)。

不能编辑在高可用性配置中用作故障切换或状态故障切换链路的接口。

步骤 3 进行以下设置：

Ethernet1/2
Edit Physical Interface

Interface Name: Mode: Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

IPv4 Address | IPv6 Address | Advanced

Type:

IP Address and Subnet Mask: /
e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask: /
e.g. 192.168.5.16

a) 设置接口名称。


设置接口名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。如果没有名称，将忽略其余的接口配置。除非配置子接口，否则接口应有名称。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

b) 选择模式。

- **路由** - 路由模式接口需要对流量执行所有防火墙功能，例如维持流量、跟踪 IP 和 TCP 层的流量状态、IP 分片重组、TCP 规范化以及防火墙策略。这是正常接口模式。
- **被动** - 被动接口使用交换机 SPAN 或镜像端口监控网络中流经的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。如果在被动部署中配置系统，系统将不能执行某些操作，例如，阻止流量或流量整形。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。如果您选择此模式，无需执行此过程的其余部分。参阅[将物理接口配置为被动模式](#)，第 201 页。请注意，无法在被动接口上配置 IP 地址。

如果稍后将此接口添加至桥接组，则模式将自动更改为 **BridgeGroupMember**。请注意，无法在桥接组成员接口上配置 IP 地址。

- c) 将状态滑块设置为已启用设置 ()。

如果要为此物理接口配置子接口，则可能已完成。点击**保存并继续配置 VLAN 子接口和 802.1Q 中继**，第 195 页。否则，请继续。

注释 即使在配置子接口时，为接口命名和提供 IP 地址也有效。这不是常规设置，但如果确定符合您的需求，则可以进行配置。

- d) (可选) 设置说明。

一行说明最多可包含 200 个字符（不包括回车符）。

步骤 4 点击 **IPv4 地址** 选项卡，并配置 IPv4 地址。

从**类型**字段中选择以下任一选项：

- **动态 (DHCP)** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
 - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
 - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。
- **静态** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

注释 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅**配置 DHCP 服务器**，第 450 页。

步骤 5 (可选。) 点击 **IPv6 地址** 选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择**已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

注释 禁用 IPv6 不会禁用接口上使用明示 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置** - 选择此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但 FTD 设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA** 可抑制消息，遵从 RFC 要求。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 [IPv6 编址](#)，第 186 页。

如果仅使用本地链路地址，请选择**本地链路**选项。本地链路地址在本地网络之外无法访问。在桥接组接口上无法配置本地链路地址。

注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feec:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。Firepower 威胁防御设备可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望 FTD 设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 6 （可选。）[配置高级选项](#)，第 203 页。

高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 7 点击**确定**。

下一步做什么

- 将接口添加至相应的安全区域。请参阅[配置安全区](#)，第 114 页。

配置桥接组

桥接组是将一个或多个接口分组的虚拟接口。对接口分组的主要原因是创建一组交换接口。如此，就可以将工作站或其他终端设备直接连接到桥接组中所包含的接口。您不需要通过单独的物理交换机来连接这些设备，尽管您也可以将一台交换机连接到某个桥接组成员。

组成员没有 IP 地址。相反，所有成员接口共用桥接虚拟接口 (BVI) 的 IP 地址。如果在 BVI 上启用 IPv6，系统会自动为成员接口分配唯一的链路本地地址。

单独启用和禁用成员接口。这样就可以禁用任何未使用的接口，而无需将其从桥接组删除。桥接组本身始终处于启用状态。

通常会在桥接组接口 (BVI) 上配置 DHCP 服务器，为通过成员接口连接的任何终端提供 IP 地址。不过，如果愿意的话，您也可以在连接到成员接口的终端上配置静态地址。桥接组中的所有终端都必须具有与桥接组 IP 地址位于同一子网的 IP 地址。

规定和限制

- 可以添加一个桥接组。
- 在 Firepower 2100 系列或 Firepower 威胁防御虚拟设备上不能配置桥接组。
- 对于 ISA 3000，设备预配置名 **inside** 的桥接组 BVI1，其中包括除 **outside** 接口以外的所有数据接口。因此，设备已经预配置了一个端口用于连接到互联网或其他上游网络，而所有其他端口已启用并可用于直接连接终端。如果要将某个内部接口用于新的子网，必须先从 BVI1 删除所需接口。

开始之前

指定将成为桥接组成员的接口。具体而言，每个成员接口都必须满足以下要求：

- 该接口必须具有名称。
- 该接口不能有任何已定义的 IPv4 或 IPv6 地址，无论是静态分配的还是通过 DHCP 获得的。如果需从当前正在使用的某个接口删除地址，则可能还需要删除该接口的其他配置，例如静态路由、DHCP 服务器或 NAT 规则，具体视具有地址的接口而定。
- 必须将该接口从所属安全区域中删除（如果它在某个区域中），并删除该接口的所有 NAT 规则，然后才能将其添加到桥接组。

过程

步骤 1 点击设备，然后点击接口摘要中的链接。

接口列表将显示可用的接口及其名称、地址和状态。如果已有桥接组，此处将显示文件夹。点击开/关箭头可查看成员接口。成员接口也单独显示于列表中。

步骤 2 执行以下操作之一：

- 点击 BVI1 桥接组的编辑图标 (🔗)。
- 从齿轮下拉列表中选择**添加桥接组接口**创建新组。

注释 桥接组只能有一个。如果已经定义了一个桥接组，则应编辑该组而非尝试创建新组。如果需要创建新的桥接组，则必须先删除现有桥接组。

- 如果不再需要某个桥接组，点击该桥接组的删除图标 (🗑️)。删除桥接组时，其成员将变成标准路由接口，并且所有 NAT 规则或安全区域成员身份保持不变。可以编辑这些接口为其提供 IP 地址。如果要将其添加到新的桥接组，需要先删除 NAT 规则并将接口从所属安全区域中删除。

步骤 3 进行以下配置：

a) (可选) 设置接口名称。

设置桥接组的名称，最多 48 个字符。字母字符必须为小写。例如 **inside** 或 **outside**。如果希望此 BVI 参与其与其他命名接口之间的路由，请设置名称。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

b) (可选) 设置说明。

一行说明最多可包含 200 个字符（不包括回车符）。

c) 编辑桥接组成员列表。

最多可向一个桥接组添加 64 个接口或子接口。

- 添加接口 - 点击加号图标 (+)，点击一个或多个接口，然后点击确定。
- 移除接口 - 将鼠标悬停于接口上方，然后点击右侧的 x。

步骤 4 点击 **IPv4 地址** 选项卡，并配置 IPv4 地址。

从类型字段中选择以下任一选项：

- **静态** - 如果希望分配固定的地址，请选择此选项。键入桥接组的 IP 地址和子网掩码。所有连接的终端都将位于此网络中。对于预配置了桥接组的型号而言，BVI1 “inside” 网络的默认值为 192.168.1.1/24（如 255.255.255.0）。确保该地址尚未在网络中使用。

如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

注释 如果为接口配置了 DHCP 服务器，您会看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅[配置 DHCP 服务器](#)，第 450 页。

- **动态 (DHCP)** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。桥接组通常不会使用此选项，但是您可以根据需要如此配置。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
 - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
 - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。

步骤 5 (可选。) 点击 **IPv6 地址** 选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择 **已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

注释 禁用 IPv6 不会禁用接口上使用明示 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅[IPv6 编址](#)，第 186 页。

如果仅使用本地链路地址，请选择 **本地链路** 选项。本地链路地址在本地网络之外无法访问。在桥接组接口上无法配置本地链路地址。

注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feec:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。Firepower 威胁防御设备可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望 FTD 设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 6 (可选。) [配置高级选项](#)，第 203 页。

请对桥接组成员接口配置大多数高级选项，不过其中一些选项可用于桥接组接口。高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 7 点击确定。

下一步做什么

- 确保已启用您打算使用的所有成员接口。
- 为桥接组配置 DHCP 服务器。请参阅[配置 DHCP 服务器](#)，第 450 页。
- 将成员接口添加到相应的安全区域。请参阅[配置安全区](#)，第 114 页。
- 确保各项策略（例如身份、NAT 和访问策略）可为桥接组和成员接口提供所需的服务。

配置 VLAN 子接口和 802.1Q 中继

通过 VLAN 子接口，可将一个物理接口划分成多个标记有不同 VLAN ID 的逻辑接口。带有一个或多个 VLAN 子接口的接口将自动配置为 802.1Q 中继。由于 VLAN 允许您在特定物理接口上将流量分开，所以您可以增加网络中可用的接口数量，而无需增加物理接口或设备。

如果您将物理接口连接到交换机的中继端口，请创建子接口。为交换机中继端口上显示的每个 VLAN 创建子接口。如果您将物理接口连接到交换机的接入端口，创建子接口将没有意义。

规定和限制

- 防止物理接口上的未标记数据包 - 如果使用子接口，则通常表明也不希望物理接口传递流量，因为物理接口会传递未标记的数据包。由于必须启用物理接口，才能允许子接口传递流量，所以请确保物理接口不会通过未命名接口传递流量。如果要允许物理接口传递未标记数据包，可以照常命名接口。
- 您不能在桥接组成员接口上配置 IP 地址，但是可以根据需要修改高级设置。
- 同一父接口上的所有子接口必须为桥接组成员或路由接口；您无法混合搭配。
- FTD 不支持动态中继协议 (DTP)，因此您必须无条件地将连接的交换机端口配置到中继上。
- 您可能想要为 FTD 上定义的子接口分配唯一 MAC 地址，因为它们使用父接口上相同的固化 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 FTD 上特定实例内发生流量中断。

过程

步骤 1 点击 **设备**，然后点击**接口摘要**中的链接。

接口列表将显示可用的接口及其名称、地址和状态。

步骤 2 执行以下操作之一：

- 从齿轮下拉列表中选择添加子接口，以创建新的子接口。
- 点击要编辑的子接口的编辑图标 (🔗)。

如果不再需要某个子接口，请点击该子接口对应的删除图标 (🗑️) 将其删除。

步骤 3 将状态滑块设置为已启用设置 (🔘)。

步骤 4 配置父接口、名称和描述：

Add Subinterface

Parent Interface: Ethernet1/1

Subinterface Name: engineering

Mode: Routed

Status:

Most features work with named interfaces only, although some require unnamed interfaces.

Description:

VLAN ID: 200

Subinterface ID: 200

1 - 4094

IPv4 Address | IPv6 Address | Advanced

Type: Static

IP Address and Subnet Mask: 10.10.10.1 / 24

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask: 10.10.10.2 / 24

e.g. 192.168.5.16

CANCEL OK

a) 选择父接口。

父接口是将子接口添加至其中的物理接口。创建子接口后，父接口则无法更改。

b) 设置子接口名称，最多 48 个字符。

字母字符必须为小写。例如 **inside** 或 **outside**。如果没有名称，将忽略其余的接口配置。

注释 如果更改名称，更改将自动反映到使用旧名称的所有位置，包括安全区、系统日志服务器对象和 DHCP 服务器定义。但无法删除名称，除非首先删除使用该名称的所有配置，这是因为对于任何策略或设置通常无法使用未命名的接口。

c) 将模式设置为路由。

如果稍后将此接口添加到桥接组，则该模式将自动更改为 **BridgeGroupMember**。请注意，无法在桥接组成员接口上配置 IP 地址。

d) （可选）设置说明。

一行说明最多可包含 200 个字符（不包括回车符）。

e) 设置 VLAN ID。

输入 VLAN ID，介于 1 和 4094 之间，用于标记该子接口上的数据包。

f) 设置子接口 ID。

以整数形式输入介于 1 和 4294967295 之间的子接口 ID。此 ID 附加至接口 ID；例如 Ethernet1/1.100。方便起见，您可以匹配 VLAN ID，但这不是必需的。创建子接口后，则无法更改该 ID。

步骤 5 点击 **IPv4 地址** 选项卡，并配置 IPv4 地址。

从 **类型** 字段中选择以下任一选项：

- **动态 (DHCP)** - 如果应从网络中的 DHCP 服务器获取地址，请选择此选项。如果您配置高可用性，将不能使用此选项。如有需要，更改以下选项：
 - **路由指标** - 如果从 DHCP 服务器获取默认路由，则此选项是指与获知路由的管理距离，其值介于 1 到 255 之间。默认值为 1。
 - **获取默认路由** - 是否从 DHCP 服务器获取默认路由。您通常会选择此选项，该选项是默认值。
- **静态** - 如果希望分配固定的地址，请选择此选项。对于连接到接口的网络，键入接口的 IP 地址和子网掩码。例如，如果您连接的是 10.100.10.0/24 网络，则可以输入 10.100.10.1/24。确保该地址尚未在网络中使用。

如果您配置了高可用性，并要监控此接口的高可用性，则还要在同一子网上配置一个备用 IP 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。

注释 如果为接口配置了 DHCP 服务器，您将看到该配置。您可以编辑或删除 DHCP 地址池。如果将接口 IP 地址更改为不同的子网，必须先删除 DHCP 服务器或在新子网上配置地址池，才能保存接口更改。请参阅 [配置 DHCP 服务器](#)，第 450 页。

步骤 6 （可选。）点击 **IPv6 地址** 选项卡，并配置 IPv6 地址。

- **状态** - 在不想配置全局地址时，要启用 IPv6 处理并自动配置本地链路地址，请选择 **已启用**。本地链路地址基于接口的 MAC 地址（修改的 EUI-64 格式）生成。

注释 禁用 IPv6 不会禁用接口上使用明示 IPv6 地址配置或启用自动配置的 IPv6 处理。

- **地址自动配置** - 选择此选项可自动配置地址。只有设备所在链路中的路由器配置为提供 IPv6 服务（包括通告 IPv6 全局前缀以用于该链路），IPv6 无状态自动配置才会生成全局 IPv6 地址。如果该链路中的 IPv6 路由服务不可用，则只能获得本地链路 IPv6 地址，无法访问设备直接的网络链路之外的服务。本地链路地址以修改的 EUI-64 接口 ID 为基础。

虽然 RFC 4862 规定为无状态自动配置所配置的主机不发送路由器通告消息，但 FTD 设备在这种情况下确实会发送路由器通告消息。选择**抑制 RA**可抑制消息，遵从 RFC 要求。

- **静态地址/前缀** - 如果不使用无状态自动配置，请输入完整的静态全局 IPv6 地址和网络前缀。例如，2001:0DB8::BA98:0:3210/48。有关 IPv6 寻址的详细信息，请参阅 [IPv6 编址](#)，第 186 页。

如果仅使用本地链路地址，请选择**本地链路**选项。本地链路地址在本地网络之外无法访问。在桥接组接口上无法配置本地链路地址。

注释 链路本地地址应以 FE8、FE9、FEA 或 FEB 开头，例如 fe80::20d:88ff:feec:6a82。请注意，我们建议根据修改的 EUI-64 格式自动分配链路本地地址。例如，如果其他设备强制使用修改的 EUI-64 格式，则手动分配的链路本地地址可能导致丢弃数据包。

- **备用 IP 地址** - 如果您配置了高可用性，并为高可用性监控此接口，请在同一子网上配置备用 IPv6 地址。此接口在备用设备上使用备用地址。如果未设置备用 IP 地址，则主用设备无法使用网络测试监控备用接口，只能跟踪链路状态。
- **抑制 RA** - 是否抑制路由器通告。Firepower 威胁防御设备可以参与路由器通告，以便邻居设备可以动态获悉默认路由器地址。默认情况下，每个配置 IPv6 的接口定期发送路由器通告消息（ICMPv6 类型 134）

也会发送路由器通告，以响应路由器请求消息（ICMPv6 类型 133）。路由器请求消息由主机在系统启动时发送，以便主机可以立即自动配置，而无需等待下一条预定路由器通告消息。

对于不希望 FTD 设备提供 IPv6 前缀的任何接口（例如外部接口），您可能希望抑制接口上的这些消息。

步骤 7（可选。）[配置高级选项](#)，第 203 页。

高级设置的默认值适用于大多数网络。只有在需要解决网络问题时，再进行编辑。

步骤 8 点击确定。

下一步做什么

- 将子接口添加至相应的安全区域。请参阅[配置安全区](#)，第 114 页。

配置被动接口

被动接口使用交换机 SPAN（交换端口分析器）或镜像端口监控在网络中传输的流量。SPAN 或镜像端口允许从交换机的其他端口复制流量。此功能可以提供网络内的系统可视性，而不会影响网络流量。

如果系统是在被动部署中配置的，则无法执行某些操作，例如阻止流量。被动接口无条件接收所有流量，这些接口不会重传接收到的流量。

使用被动接口监控网络上的流量，以收集流量相关的信息。例如，您可以应用入侵策略来识别攻击网络的威胁类型，或了解用户正在发出的 Web 请求的 URL 类别。您可以实施各种安全策略和规则，了解系统在主动部署的情况下会执行哪些操作，以便可以根据访问控制和其他规则丢弃流量。

但是，由于被动接口无法影响流量，因此存在很多配置限制。这些接口只是让系统知悉有流量通过：进入被动接口的数据包不会从设备流出。

以下主题更加详细地介绍了被动接口及其配置方法。

为什么使用被动接口？

被动接口的主要目的是提供一种简单的演示模式。您可以设置交换机监控单个源端口，然后使用工作站发送通过被动接口监控的测试流量。由此，可以了解 Firepower 威胁防御系统如何评估连接、识别威胁等。系统性能满足要求后，可以将其主动部署在网络中，并删除被动接口配置。

不过，您也可以在生产环境中使用被动接口，以提供以下服务：

- 纯 ID 部署 - 如果您不想使用系统作为防火墙或 IPS（入侵防御系统），可以将其被动部署为 IDS（入侵检测系统）。在此部署方法中，您将使用访问控制规则将入侵策略应用于所有流量。您还必须设置系统监控交换机上的多个源端口。然后，您将可以使用控制面板监控网络上发现的威胁。但是，在此模式下，系统不会执行任何操作来阻止这些威胁。
- 混合部署 - 您可以在同一系统上搭配使用主动路由接口和被动接口。因此，在某些网络中，您可以将 Firepower 威胁防御设备部署为防火墙，同时配置一个或多个被动接口监控其他网络中的流量。

被动接口的限制

定义为被动模式接口的任何物理接口具有以下限制：

- 无法为被动接口配置子接口。
- 不能将被动接口添加到桥接组。
- 不能在被动接口上配置 IPv4 或 IPv6 地址。
- 不能对被动接口选择“仅管理”选项。
- 只能将接口添加到被动模式安全区，不能将其添加到路由安全区。

- 可以将被动安全区添加到访问控制或身份规则的源条件中。不能在目标条件中使用被动区域。同时，也不能在同一规则中搭配使用被动和路由区域。
- 不能为被动接口配置管理访问规则（HTTPS 或 SSH）。
- 不能在 NAT 规则中使用被动接口。
- 不能为被动接口配置静态路由。也不能在路由协议配置中使用被动接口。
- 不能在被动接口上配置 DHCP 服务器。也不能使用被动接口通过自动配置获取 DHCP 设置。
- 不能在系统日志服务器配置中使用被动接口。
- 不能在被动接口上配置任何类型的 VPN。

为硬件 Firepower 威胁设备被动接口配置交换机

只有当网络交换机配置正确时，硬件 Firepower 威胁防御设备上的被动接口才能使用。以下过程基于思科 Nexus 5000 系列交换机。如果您有不同类型的交换机，所用的命令可能会有所不同。

其基本思路是，配置 SPAN（交换端口分析器）或镜像端口，将被动接口连接到该端口，在交换机上配置监控会话以将流量副本从一个或多个源端口发送到 SPAN 或镜像端口。

过程

步骤 1 将交换机上的端口配置为监控（SPAN 或镜像）端口。

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

步骤 2 定义监控会话以识别要监控的端口。

确保您将 SPAN 或镜像端口定义为目标端口。在以下示例中，监控两个源端口。

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

步骤 3（可选。）使用 `show monitor session` 命令验证配置。

以下示例显示会话 1 的简要输出。

```
switch# show monitor session 1 brief
  session 1
-----
type           : local
state          : up
source intf    :
```



```
rx          : Eth1/7      Eth1/8
tx          : Eth1/7      Eth1/8
both        : Eth1/7      Eth1/8
source VSANs :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

步骤 4 以物理方式将电缆从 Firepower 威胁防御虚拟被动接口连接到交换机的目标端口。

可以在进行物理连接前后，将接口配置为被动模式。请参阅[将物理接口配置为被动模式](#)，第 201 页。

为 Firepower 威胁防御虚拟被动接口配置 VLAN

只有在虚拟网络上正确配置了 VLAN 时，Firepower 威胁防御虚拟设备的被动接口才可以正常工作。请确保执行以下操作：

- 将 Firepower 威胁防御虚拟接口连接到已在混杂模式下配置的 VLAN。然后，按照[将物理接口配置为被动模式](#)，第 201 页中的说明配置接口。被动接口会看到混合 VLAN 上所有流量的副本。
- 将一个或多个终端设备（例如虚拟 Windows 系统）连接到同一 VLAN。如果 VLAN 已连接到互联网，可以使用单台设备。否则，需要至少两台设备，才可以在两者之间传递流量。要想获取 URL 类别数据，需要建立互联网连接。

将物理接口配置为被动模式

您可以将接口配置为被动模式。在被动模式下工作时，接口仅监控交换机自身（针对硬件设备）或混合 VLAN（针对 Firepower 威胁防御虚拟）配置的监控会话中来自源端口的流量。有关需要在交换机或虚拟网络中配置哪些对象的详细信息，请参阅以下主题：

- [为硬件 Firepower 威胁设备被动接口配置交换机](#)，第 200 页
- [为 Firepower 威胁防御虚拟被动接口配置 VLAN](#)，第 201 页

当您想要分析通过受监控交换机端口传入的流量，而不影响这些流量时，可使用被动模式。有关使用被动模式的端到端示例，请参阅[如何被动监控网络上的流量](#)，第 62 页。


过程

步骤 1 点击 **设备**，然后点击**接口摘要**中的链接。

接口列表将显示可用的接口及其名称、地址和状态。

步骤 2 点击要编辑的物理接口的编辑图标 (🔗)。

选择当前未使用的接口。如果您要将使用中的接口转换为被动接口，需要先从任何安全区中删除该接口，并删除使用该接口的所有其他配置。

步骤 3 将状态滑块设置为已启用设置 ()。

步骤 4 进行以下配置：

- **接口名称** - 接口名称，最多 48 个字符。字母字符必须为小写。例如，monitor。
- **模式** - 选择被动。
- **(可选。) 说明** - 说明最多为 200 个字符，单行，不能使用回车。

注释 无法配置 IPv4 或 IPv6 地址。在“高级”选项卡中，仅可以更改 MTU、双工和速度设置。

步骤 5 点击确定。

下一步做什么

创建被动接口并不会在控制面板上填充接口上所发现流量的相关信息。您还必须执行以下操作：使用案例会介绍这些步骤。请参阅[如何被动监控网络上的流量](#)，第 62 页。

- 创建被动安全区并向其添加接口。请参阅[配置安全区](#)，第 114 页。
- 创建将被动安全区用作源区域的访问控制规则。通常，您将在这些规则中应用入侵策略以实施 IDS（入侵检测系统）监控。请参阅[配置访问控制策略](#)，第 266 页。
- 或者，为被动安全区创建 SSL 解密和身份规则，并启用安全情报策略。

配置高级接口选项

高级选项包括设置 MTU、硬件设置、仅管理、MAC 地址和其他设置。

关于 MAC 地址

您可以手动配置介质访问控制 (MAC) 地址来覆盖默认地址。

对于高可用性配置，您可以同时配置接口的主用和备用 MAC 地址。如果主用设备进行故障切换，并且备用设备成为主用设备，则新的主用设备会开始使用主用 MAC 地址，以最大限度地减少网络中断。

默认 MAC 地址

默认 MAC 地址分配取决于接口类型。

- **物理接口** - 物理接口使用已刻录的 MAC 地址。
- **子接口** - 物理接口的所有子接口都使用同一个烧录 MAC 地址。您可能想为子接口分配唯一的 MAC 地址。例如，您的运营商可能根据 MAC 地址执行访问控制。此外，由于 IPv6 链路本地地址是基于 MAC 地址生成的，因此将唯一 MAC 地址分配给子接口会允许使用唯一 IPv6 链路本地地址，这能够避免 FTD 上特定实例内发生流量中断。

关于 MTU

MTU 指定 Firepower 威胁防御设备可在给定以太网接口上传输的最大帧负载大小。MTU 值是没有以太网报头、VLAN 标记或其他系统开销情况下的帧大小。例如，将 MTU 设置为 1500 时，预期帧大小为 1518 字节（含报头）或 1522 字节（使用 VLAN）。请勿为容纳这些报头而将 MTU 的值设得过高。

路径 MTU 发现

Firepower 威胁防御设备支持路径 MTU 发现（如 RFC 1191 中所定义），从而使两个主机之间的网络路径中的所有设备均可协调 MTU，以便它们可以标准化路径中的最低 MTU。

MTU 和分段

对于 IPv4，如果传出 IP 数据包大于指定 MTU，则该数据包将分为 2 帧或更多帧。片段在目标处（有时在中间跃点处）重组，而分片可能会导致性能下降。对于 IPv6，通常不允许对数据包进行分段。因此，IP 数据包大小应在 MTU 大小范围内，以避免分片。

对于 UDP 或 ICMP，应用应将 MTU 考虑在内，以避免分段。



注释 只要有内存空间，Firepower 威胁防御设备就可接收大于所配置的 MTU 的帧。

MTU 和巨帧

MTU 越大，您能发送的数据包越大。加大数据包可能有利于提高网络效率。请参阅以下准则：

- 与流量路径上的 MTU 相匹配 - 我们建议将所有 FTD 接口以及流量路径的其他设备接口上的 MTU 设为相同。匹配 MTU 可防止中间设备对数据包进行分片。
- 容纳巨帧 - 巨帧是指大于标准最大值 1522 字节（包括第 2 层报头和 VLAN 报头）的以太网数据包，最大为 9216 字节。MTU 最大可设置为 9198 字节，以容纳巨帧。Firepower 威胁防御虚拟的最大值为 9184。



注释 加大 MTU 会为巨帧分配更多内存，这样可能会限制其他功能（例如访问规则）的最大使用量。如果在 ASA 5500-X 系列设备或 Firepower 威胁防御虚拟上将 MTU 增加到默认值 1500 以上，则必须重新启动系统。如果设备已为高可用性，还须重新启动备用设备。无需重新启动 Firepower 型号，因为巨帧支持在该型号上始终启用。

配置高级选项

高级接口选项的默认设置适用于大多数网络。只有当您解决网络问题或配置高可用性时，才需要进行配置。

以下步骤程序假定已定义接口。另外，您还可以在初始编辑或创建接口时编辑这些设置。

限制

- 对于桥接组，您可以在成员接口上配置大多数这些选项。除用于 DAD 尝试和高可用性监控之外，这些选项不适用于桥接虚拟接口 (BVI)。
- 您无法在 Firepower 2100 设备上设置管理接口的 MTU、双工或速度。
- 对于被动接口，您只能设置 MTU、双工以及速度。不能将接口仅用于管理。

过程

步骤 1 点击 **设备**，然后点击**接口摘要**中的链接。

接口列表将显示可用的接口及其名称、地址和状态。

步骤 2 点击要编辑的接口的编辑图标 (🔗)。

步骤 3 点击**高级选项**。

步骤 4 如果您想让系统在决定是否故障切换到高可用性配置中的对等设备时考虑接口的运行状况，请选择**对高可用性监控启用**。

如果不配置高可用性，可忽略此选项。如果不配置接口的名称，也可以忽略此选项。

步骤 5 要将数据接口仅用于管理，请选择**仅管理**。

仅管理接口不允许直通流量，所以将数据接口设置为仅管理的价值微乎其微。不能更改管理/诊断接口的此项设置，它们始终为仅管理。

步骤 6 将 **MTU**（最大传输单位）更改为所需的值。

默认 MTU 为 1500 字节。您可以指定介于 64 - 9198（或 9000，适用于 Firepower 威胁防御虚拟）之间的值。如果通常在网络中使用巨帧，请设置一个较大的值。

注释 如果在 ASA 5500-X 系列设备、ISA 3000 系列设备或 Firepower 威胁防御虚拟上将 MTU 提高到 1500 以上，则必须重新启动设备。登录 CLI 并使用 **reboot** 命令。如果设备已为高可用性，还须重新启动备用设备。无需重新启动 Firepower 型号，因为巨帧支持在该型号上始终启用。

步骤 7 （仅限物理接口）。修改速度和双工设置。

默认设置为该接口与线路另一端的接口协商最佳双工和速度，但如有必要，您可以强制实施特定的双工或速度。所列的选项仅为接口支持的设置。在网络模块上设置这些选项之前，请阅读[接口配置的限制性](#)，第 186 页。

- **双工** - 选择**自动**、**半双工**、**全双工**或**默认**。当接口支持时，自动为默认值。例如，您不能为 Firepower 2100 系列设备上的 SFP 接口选择“自动”。

选择**默认**表示 Firepower 设备管理器不应尝试配置设置。任何现有配置将保持不变。

- **速度** - 选择**自动**可使接口协商速度（默认值）或选取特定速度：**10 Mbps**、**100 Mbps**、**1000 Mbps**、**10000 Mbps**。此外，您还可以选择以下特殊选项：
 - **不协商** - 对于光纤接口，请将速度设置为 1000 Mbps，并且不协商链路参数。这是这些接口上配置的默认配置。
 - **默认** - 表示 Firepower 设备管理器不应尝试配置设置。任何现有配置将保持不变。

接口类型限制了您可以选择的选项。例如，Firepower 2100 系列设备上的 SFP+ 接口仅支持 1000 (1 Gbps) 和 10000 (10 Gbps)，SFP 接口仅支持 1000 (1 Gbps)，而千兆以太网端口不支持 10000 (10 Gbps)。其他设备上的 SPF 接口可能需要设置**不协商**。有关接口所支持的选项的信息，请参阅硬件文档。

步骤 8 修改 IPv6 配置设置。

- **启用 DHCP 以获取 IPv6 地址配置** - 是否在 IPv6 路由器通告数据包中设置“托管地址配置”标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 来获取相关地址以及派生的无状态自动配置地址。
- **启用 DHCP 以获取 IPv6 非地址配置** - 是否在 IPv6 路由器通告数据包中设置“其他地址配置”标志。此标志通知 IPv6 自动配置客户端应使用 DHCPv6 从 DHCPv6 获取其他信息，如 DNS 服务器地址。
- **DAD 尝试** - 接口执行重复地址检测 (DAD) 的频率，介于 0 - 600 之间。默认值为 1。在无状态自动配置过程中，DAD 会验证新单播 IPv6 地址的唯一性，再将地址分配给接口。如果重复地址是接口的链路本地地址，则在接口上禁用 IPv6 数据包处理。如果重复地址是全局地址，则将不使用该地址。接口将使用邻居的询求消息来执行重复地址检测。将该值设置为 0 可禁用重复地址检测 (DAD) 流程。

步骤 9 （可选，建议为子接口和高可用性设备配置。）配置 MAC 地址。

默认情况下，系统对接口使用预烧到网络接口卡 (NIC) 的 MAC 地址。因此，该接口上的所有子接口都使用相同的 MAC 地址，也因此您可能想要为每个子接口创建唯一地址。如果您配置高可用性，建议手动配置主用/备用 MAC 地址。定义 MAC 地址有助于在故障切换时保持网络中的一致性。

- **MAC 地址** - 采用 H.H.H 格式的介质访问控制，其中 H 是 16 位十六进制数字。例如，您可以将 MAC 地址 00-0C-F1-42-4C-DE 输入为 000C.F142.4CDE。MAC 地址不能设置组播位，即左起第二个十六进制数字不能是奇数。
- **备用 MAC 地址** - 用于高可用性。如果主用设备发生故障切换，备用设备变为主用设备，则新的主用设备开始使用主用 MAC 地址，以最大限度地减少网络中断，而原来的主用设备使用备用地址。

步骤 10 单击 **OK**。

添加接口到虚拟 Firepower 威胁防御

部署 FTDv 时，可以将接口分配给虚拟机。然后，在 FDM 中，使用与配置硬件设备相同的方法配置这些接口。

但是，您无法给虚拟机添加更多虚拟接口，然后让 FDM 来自动识别它们。如果您需要为 FTDv 配置更多物理接口对等体，那基本上需要重新执行该流程。您可以部署新的虚拟机，也可以使用以下程序。



注意 要给虚拟机添加接口，您需要完全清除 FTDv 配置。配置中唯一保留不变的部分是管理地址和网关设置。

开始之前

在中 FDM 执行以下操作：

- 检查 FTDv 配置并记下要在新虚拟机中复制的设置。
- 依次选择 **设备 > 智能许可证 > 查看配置并禁用所有功能许可证**。

过程

步骤 1 关闭 FTDv 的电源。

步骤 2 使用虚拟机软件，将接口添加至 FTDv。

对于 VMware，默认情况下，虚拟设备使用 e1000（1 千兆位/秒）接口。您还可以使用 vmxnet3 或 ixgbe（10 千兆位/秒）接口。

步骤 3 打开 FTDv 的电源。

步骤 4 打开 FTDv 控制台，删除本地管理器，然后启用本地管理器。

删除本地管理器，然后启用本地管理器，重置设备配置，并让系统识别新接口。管理接口配置不会重置。以下 SSH 会话会显示相应命令。

```
> show managers
Managed locally.
```

```
> configure manager delete
```

```
If you enabled any feature licenses, you must disable them in Firepower Device Manager
before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
DCHP Server Disabled
```

```
> show managers
No managers configured.
```

```
> configure manager local  
>
```

步骤 5 打开浏览器并连接到 Firepower 设备管理器，完成设备安装向导，并配置设备。请参阅[完成初始配置](#)，第 14 页。

监控接口

可在以下区域查看有关接口的一些基本信息：

- **设备**。使用端口图可监控接口的当前状态。将鼠标悬停在端口上方可查看其 IP 地址启用状态和链路状态。IP 地址可静态分配，也可以使用 DHCP 获取。

接口端口使用以下颜色代码：

- 绿色 - 接口已配置和启用，链路为运行状态。
 - 灰色 - 接口未启用。
 - 橙色/红色 - 接口已配置和启用，但链路中断。如果该接口已连接电缆，则此状态表示有错误需要更正。如果该接口未连接电缆，则此状态为预期状态。
- **监控 > 系统**。吞吐量控制面板显示有关流经系统的流量的信息。您可以查看所有接口的信息，也可以选择特定接口查看其信息。
 - **监控 > 区域**。该控制面板显示基于安全区域的统计信息，这些安全区域由接口组成。您可以深入分析此信息以了解更多详情。

在 CLI 中监控接口

您还可以打开 CLI 控制台或登录设备 CLI，使用以下命令获取有关接口相关行为与统计信息的更详细信息。

- **show interface** 显示接口统计信息和配置信息。此命令有许多关键字，可用于获取所需的信息。使用 ? 作为关键字可查看可用选项。
- **show ipv6 interface** 显示有关接口的 IPv6 配置信息。
- **show bridge-group** 显示网桥虚拟接口 (BVI) 的相关信息，包括成员信息和 IP 地址。
- **show conn** 显示当前通过接口建立的连接的相关信息。
- **show traffic** 显示流过每个接口的流量的相关统计信息。
- **show ipv6 traffic** 显示流过设备的 IPv6 流量的相关统计信息。
- **show dhcpd** 显示接口上的 DHCP 使用统计信息及其他信息，特别是接口上配置的 DHCP 服务器的相关信息。

接口示例

使用案例章节涵盖以下与接口相关的示例：

- [如何在 Firepower 设备管理器中配置设备，第 29 页](#)
- [如何添加子网，第 57 页](#)
- [如何被动监控网络上的流量，第 62 页](#)



第 11 章

路由

系统使用路由表来确定进入系统的数据包的传出接口。以下主题介绍路由的基本信息以及如何在设备上配置路由。

- [路由概述](#)，第 209 页
- [静态路由](#)，第 213 页
- [监控路由](#)，第 216 页

路由概述

以下主题介绍路由在 FTD 设备中的运行方式。所谓路由是指通过网络将信息从源发送到目的地的活动。在途中通常会经过至少一个中间节点。路由涉及两个基本活动：确定最佳路由路径和通过网络传输数据包。

路由类型

主要有两种类型的路由：静态路由或动态路由。

静态路由是明确定义的路由。它们相对稳定且通常具有高优先级，用于确保将发往路由目标的流量发送到正确的接口。例如，您可以创建一个默认静态路由，用于覆盖尚未被任何其他路由覆盖的所有流量，即 IPv4 的 0.0.0.0/0 或 IPv6 的 ::/。另一个示例是指向您经常使用的内部系统日志服务器的静态路由。

动态路由是从路由协议（如 OSPF、BGP、EIGRP、IS-IS 或 RIP）的操作中习得的路由协议，您不用直接定义这类路由。相反，您配置路由协议，然后系统与邻居路由器进行通信，传输并接收路由更新。

动态路由协议通过分析收到的路由更新消息调整路由表，使其适应不断变化的网络环境。如果有消息表明网络发生更改，则系统会重新计算路由并发出新的路由更新消息。这些消息会渗入网络，促使路由器重新运行其算法并相应地更改其路由表。

静态路由非常简单，发挥基本路由的作用，在网络流量相对可预测且网络设计相对简单的环境中十分适用。但是，静态路由不能更改（除非您编辑它们），因此它们不能应对网络中的更改。

除非您有一个小型网络，否则您通常会将静态路由和一个或多个动态路由协议搭配使用。您将定义至少一个静态路由，作为不匹配显式路由的流量的默认路由。



注释 可以使用 Smart CLI 配置以下路由协议：OSPF、BGP。使用 FlexConfig 配置 ASA 软件支持的其他路由协议。

路由表和路由选择

如果 NAT 转换 (xlates) 和规则无法确定传出接口，系统将使用路由表来确定数据包的路径。

路由表中的路由包括一个名为“管理距离”的指标，提供相对于既定路由的优先级。如果某个数据包与多个路由条目匹配，则使用距离最短的路由。直连网络（在接口上定义的网络）的距离为 0，因此始终首选使用此网络。静态路由的默认距离为 1，但您可以使用 1-254 之间的任意距离创建默认距离。

标识具体目的地的路由优先于默认路由（即目的地为 0.0.0.0/0 或 ::/0 的路由）。

路由表的填充方式

FTD 路由表可以通过静态定义的路由、直连路由以及动态路由协议发现的路由来填充。由于 FTD 除具有路由表中的静态路由和已连接路由外，还可以运行多条路由协议，因此可通过多种方式发现或输入同一路由。当在路由表中放入同一目标的两条路由时，将按如下确定保留在路由表中的路由：

- 如果两个路由具有不同的网络前缀长度（网络掩码），则会将两个路由都视为唯一并输入到路由表中。然后，由数据包转发逻辑确定使用哪一条路由。

例如，如果 RIP 和 OSPF 进程发现以下路由：

- RIP: 192.168.32.0/24
- OSPF: 192.168.32.0/19

即使 OSPF 路由具有更好的管理距离，但由于两条路由具有不同的前缀长度（子网掩码），因此均会安装在路由表中。这两条路由被视为不同目标，数据包转发逻辑会确定使用哪条路由。

- 如果 FTD 从单个路由协议（例如 RIP）获悉通向同一目标的多条路径，则会在路由表中输入具有更佳指标的路由（由路由协议确定）。

指标是与特定路由关联的值，从最高优先到最低优先进行排序。用于确定指标的参数根据路由协议而异。具有最低指标的路径选择作为最佳路径并安装在路由表中。如果有多个指标相等的通向同一目标的路径，则会在这些等价路径上进行负载均衡。

- 如果 FTD 从多个路由协议获悉目标，则会比较路由的管理距离，并在路由表中输入管理距离较短的路由。

路由的管理距离

您可以更改由路由协议发现或重分发到路由协议中的路由的管理距离。如果来自两个不同路由协议的两条路由具有相同的管理距离，则会将具有较短默认管理距离的路由输入到路由表中。对于 EIGRP 和 OSPF 路由，如果 EIGRP 路由和 OSPF 路由具有相同的管理距离，则默认选择 EIGRP 路由。

管理距离是 Firepower 威胁防御设备在有两个或多个通向同一目标（来自两个不同路由协议）的路由时，用于选择最佳路径的路由参数。由于路由协议具有基于不同于其他协议的算法的指标，因此并非总能够确定通向由不同路由协议生成的同一目标的两条路由的最佳路径。

每个路由协议使用管理距离值划分优先级。下表显示 Firepower 威胁防御设备支持的路由协议的默认管理距离值。

表 6: 受支持的路由协议的默认管理距离

路由源	默认管理距离
已连接的接口	0
静态路由	1
EIGRP 汇总路由	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部路由	170
内部和本地 BGP	200
未知	255

管理距离值越小，协议的优先等级越高。例如，如果 Firepower 威胁防御设备从 OSPF 路由进程（默认管理距离 - 110）和 RIP 路由进程（默认管理距离 - 120）均收到通向特定网络的路由，则 Firepower 威胁防御设备会选择 OSPF 路由，因为 OSPF 具有更高的优先级。在这种情况下，路由器会将 OSPF 版本的路由添加到路由表。

在本示例中，如果 OSPF 派生路由的源丢失（例如，由于电源关闭），则 Firepower 威胁防御设备会使用 RIP 派生路由，直至 OSPF 派生路由再次出现。

管理距离是一项本地设置。例如，如果您更改通过 OSPF 获取的路由的管理距离，则该更改仅会影响输入了该命令的 Firepower 威胁防御设备上的路由表。在路由更新中不会通告管理距离。

管理距离不影响路由进程。路由进程仅通告路由进程已发现或重分发到路由进程中的路由。例如，即使在路由表中使用 OSPF 路由进程发现的路由，RIP 路由进程也会通告 RIP 路由。

备份动态和浮动静态路由

当由于安装另一条路由而导致初始尝试将路由安装在路由表中失败时，系统会注册备用路由。如果安装在路由表中的路由失败，则路由表维护进程会呼叫已注册备用路由的每个路由协议进程，并请求它们重新在路由表中安装此路由。如果有多个协议为失败路由注册了备用路由，则根据管理距离选择优先路由。

鉴于以上过程，当动态路由协议发现的路由失败时，您可以创建安装在路由表中的浮动静态路由。浮动静态路由仅仅是配置有比 Firepower 威胁防御设备上运行的动态路由协议更大的管理距离的静态路由。当动态路由进程发现的对应路由失败时，会在路由表中安装静态路由。

如何制定转发决策

系统按如下制定转发决策：

- 如果目的目标不匹配路由表中的条目，则通过为默认路由指定的接口转发数据包。如果尚未配置默认路由，则会丢弃数据包。
- 如果目的目标匹配路由表中的单个条目，则通过与该路由关联的接口转发数据包。
- 如果目的目标匹配路由表中的多个条目，则通过与具有较长网络前缀的路由相关联的接口转发数据包。

例如，发往 192.168.32.1 的数据包到达在路由表中拥有以下路由的接口：

- 192.168.32.0/24 网关 10.1.1.2
- 192.168.32.0/19 网关 10.1.1.3

在这种情况下，发往 192.168.32.1 的数据包直接发送到 10.1.1.2，因为 192.168.32.1 属于 192.168.32.0/24 网络。它也属于路由表中的其他路由，但 192.168.32.0/24 在路由表中的前缀最长（24 位对比 19 位）。在转发数据包时，较长前缀始终优先于较短的前缀。



注释 即便新的相似连接将因路由中的变化而导致不同行为，现有连接也将继续使用其已建立的接口。

管理流量的路由表

作为一项标准安全实践，在将管理流量与数据流量分开与隔离时，通常会需要它。要实现这种隔离，FTD 为管理专用流量和数据流量使用单独的路由表。单独的路由表意味着您也可以创建用于数据和管理单独默认路由。

关联设备流量始终使用数据路由表。

设备流量（根据类型）在默认情况下使用管理路由表或数据路由表。如果在默认路由表中找不到匹配项，则会检查其他路由表。

关联设备管理表包括使用 HTTP、SCP、TFTP、等打开远程文件的功能。

关联设备流量数据表包括所有其他功能，如 ping、DNS、DHCP 等。

如果您需要传出流量退出默认路由表中不存在的接口，则您可能需要在配置接口时指定接口，而不是依赖于回到另一个表。FTD 检查用于该接口路由的正确路由表。例如，如果需要 ping 命令来退出管理专用接口，请在 ping 函数中指定该接口。否则，如果数据路由表中具有默认路由，则将匹配默认路由且绝不回到管理路由表。

管理路由表支持独立于数据接口路由表的动态路由。给定的动态路由进程必须在管理专用接口或数据接口上运行；不能将两种类型混用。

管理专用接口包括所有“管理 x/x”（名为“诊断”）接口以及您配置为管理专用的所有接口。



注释 此路由表不影响其用于与 FMC 通信的特殊 FTD 管理逻辑接口；该接口具有自身的路由表。另一方面，诊断逻辑接口使用本节所述的管理专用路由表。



注释 此路由表不影响其用于与许可服务器通信或数据库更新的特殊 FTD 管理虚拟接口；该接口具有自身的路由表。另一方面，诊断物理接口使用本节所述的管理专用路由表。

等价多路径 (ECMP) 路由

Firepower 威胁防御设备支持等价多路径 (ECMP) 路由。

每个接口最多支持 3 个等价静态或动态路由。例如，您可以在外部接口上配置多个默认路由，指定不同的网关：

```
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.2
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.3
route for 0.0.0.0 0.0.0.0 through outside to 10.1.1.4
```

在这种情况下，流量在外部接口上的 10.1.1.2、10.1.1.3 和 10.1.1.4 之间进行负载均衡。流量基于散列源和目标 IP 地址、传入接口、协议、源与目标端口的算法在指定网关之间进行分发。

不支持跨多个接口执行 ECMP，因此您不能在不同接口上定义到同一目标的路由。使用上述任一路由配置时，不允许使用以下路由：

```
route for 0.0.0.0 0.0.0.0 through outside2 to 10.2.1.1
```

静态路由

您可以创建静态路由，以提供网络基本路由。

关于静态路由和默认路由

要将流量路由到非连接的主机或网络，必须使用静态路由或动态路由定义到主机或网络的路由。通常，您必须配置至少一个静态路由：所有流量的默认路由（不是通过其他方式路由到默认网络网关），通常是指下一跳路由器。

默认路由

最简单的方法是配置一个默认静态路由，将所有流量都发送到上游路由器，从而依靠该路由器来为您路由流量。默认路由对网关 IP 地址进行标识，FTD 设备 将所有不具有已获悉或静态路由的数据包发送到该网关地址。默认静态路由是以 0.0.0.0/0 (IPv4) 或 ::/0 (IPv6) 作为目标 IP 地址的静态路由。

应始终定义一个默认路由。

由于 FTD 使用用于数据流量和管理流量的单独路由表，所以，您可以选择配置数据流量的默认路由和管理流量的另一默认路由。请注意，关联设备流量默认使用管理或数据路由表，具体取决于类型（请参阅[管理流量的路由表](#)，第 212 页），但如果未找到路由，则会退回至其他路由表。默认路由将始终匹配流量，并将阻止退回至其他路由表。在这种情况下，如果接口不在默认路由表中，则必须指定要用于出口流量的接口。

静态路由

在以下情况下，您可能希望使用静态路由：

- 您的网络使用不受支持的路由器发现协议。
- 网络规模较小，并且可以轻松管理静态路由。
- 不希望流量或 CPU 开销与路由协议相关联。
- 在某些情况下，仅使用默认路由并不足够。默认网关可能无法到达目标网络，因此还必须配置更具体的静态路由。例如，如果默认网关在外部，则默认路由无法将直接流量定向到未直接与 FTD 设备 连接的任何内部网络。
- 您使用的是不支持动态路由协议的功能。

静态路由指南

桥接组

- 在路由模式下，必须指定 BVI 作为网关；不能指定成员接口。
- 对于源自 Firepower 威胁防御设备（例如系统日志或 SNMP）且通过桥接组成员接口为非直接连接网络定义的流量，需要配置默认路由或静态路由，以使 Firepower 威胁防御设备了解通过哪个桥接组成员接口发出流量。如果存在无法通过单个默认路由进行访问的服务器，则必须配置静态路由。

配置静态路由

定义静态路由，以告知系统从何处发送的数据包不会绑定至直连到系统接口的网络。

对于网络 0.0.0.0/0，至少需要一个静态路由，即默认路由。如果数据包的传出接口无法由现有 NAT xlate（转换）、静态 NAT 规则或其他静态路由确定，则此路由为所发送的数据包定义目的。

如果无法使用默认网关到达所有网络，则可能需要其他静态路由。例如，默认路由通常是外部接口上的上游路由器。如果还有其他未直连到设备的内部网络，并且通过默认网关无法访问它们，则需要对每个此类内部网络使用静态路由。

对于直连到系统接口的网络，无法定义静态路由。系统自动创建这些路由。

过程

步骤 1 点击**设备**，然后点击**路由摘要**中的链路。

步骤 2 在**静态路由**页面中，执行以下某项操作：

- 要添加新路由，请点击 **+**。
- 点击要编辑的路由的编辑图标 (✎)。

如果不再需要路由，请点击该路由的垃圾桶图标将其删除。

步骤 3 配置路由属性。

名称

路由的显示名称。

说明

路由目的的可选说明。

接口

选择要通过其发送流量的接口。通过此接口需能够访问网关地址。

对于桥接组，您应为桥接组接口 (BVI)，而不是为成员接口，配置路由。

协议

选择路由是用于 **IPv4** 还是 **IPv6** 地址。

网络 (Networks)

选择标识目的网络或主机（应使用此路由中的网关）的网络对象。

要定义默认路由，请使用预定义的 **any-ipv4** 或 **any-ipv6** 网络对象，或创建一个适用于 **0.0.0.0/0 (IPv4)** 或 **::/0 (IPv6)** 网络的对象。

网关

选择标识网关 IP 地址的主机网络对象。流量将发送至此地址。您无法将同一个网关用于多个接口上的路由。

指标

路由的管理距离，该值介于 1 和 254 之间。静态路由的默认值为 1。如果接口和网关之间还有其他路由器，请输入跳数作为管理距离。

管理距离是用于比较路由的参数。数字越小，为该路由指定的优先级越高。连接的路由（直连到设备接口的网络）始终优先于静态路由。

步骤 4 单击 **OK**。

监控路由

要监控和故障排除路由，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。

- **show route** 显示数据接口的路由表，包括直连网络的路由。
- **show ipv6 route** 显示数据接口的 IPv6 路由表，包括直连网络的路由。
- **show network** 显示虚拟管理接口的配置，包括管理网关。通过虚拟接口路由不由数据接口路由表处理，除非您指定数据接口作为管理网关。
- **show network-static-routes** 显示使用 **configure network static-routes** 命令为虚拟管理接口配置的静态路由。通常不会有任何静态路由，因为在大多数情况下，管理网关足以支持管理路由。这些路由不可用于数据接口上的流量。该命令在 CLI 控制台中不可用。



第 **IV** 部分

安全策略

- [SSL 解密](#)，第 219 页
- [身份策略](#)，第 241 页
- [安全情报](#)，第 253 页
- [访问控制](#)，第 257 页
- [入侵策略](#)，第 279 页
- [网络地址转换 \(NAT\)](#)，第 291 页



第 12 章

SSL 解密

某些协议（如 HTTPS）使用安全套接字层 (SSL) 或其后续版本传输层安全性 (TLS) 来加密流量以进行安全传输。由于系统无法检查加密连接，因此，如果要应用可考虑借助更高层流量特性进行访问决策的访问规则，则必须将其解密。

- [关于 SSL 解密，第 219 页](#)
- [SSL 解密许可证要求，第 222 页](#)
- [SSL 解密指南，第 222 页](#)
- [如何实施和维护 SSL 解密策略，第 223 页](#)
- [配置 SSL 解密策略，第 224 页](#)
- [示例：从网络阻止较旧的 SSL/TLS 版本，第 236 页](#)
- [监控和故障排除 SSL 解密，第 237 页](#)

关于 SSL 解密

通常情况下，访问控制策略会评估连接以确定是允许还是阻止相应连接。但是，如果启用 SSL 解密策略，则连接将首先被发送至 SSL 解密策略，以确定应将其解密还是阻止。然后，访问控制策略评估所有未阻止连接（无论是否解密），作出最终的允许/阻止决策。



注释 您必须启用 SSL 解密策略，才能在身份策略中实施有效的身份验证规则。如果您启用 SSL 解密来启用身份策略，但不想另外实施 SSL 解密，请选择“不解密”作为默认操作，并且不要创建其他 SSL 解密规则身份策略会自动生成所需的任何规则。

以下主题更详细地介绍了加密流量管理和解密。

为什么要实施 SSL 解密？

无法检查 HTTPS 连接等加密流量。

许多连接均是合法加密的连接，比如与银行和其他金融机构的连接。许多网站使用加密保护隐私或敏感数据。例如，加密与 Firepower 设备管理器的连接。

但是，用户也可能会隐藏加密连接中的不良流量。

通过实施 SSL 解密，可解密和检查连接，确保不含威胁或其他不良流量，然后重新加密后再允许继续连接。（解密流量通过访问控制策略，并根据检查的加密连接特征而不是加密特征匹配规则。）这平衡了应用访问控制策略的需求与用户保护敏感信息的需求。

还可以配置 SSL 解密规则，阻止明确不想要允许其进入网络的加密流量类型。

请记住，解密并重新加密流量会增加设备的处理负载，从而降低整体系统性能。

可应用于加密流量的操作

配置 SSL 解密规则时，可应用以下主题中所述的操作。这些操作也可用于默认操作（适用于与显示规则不匹配的任何流量）。



注释

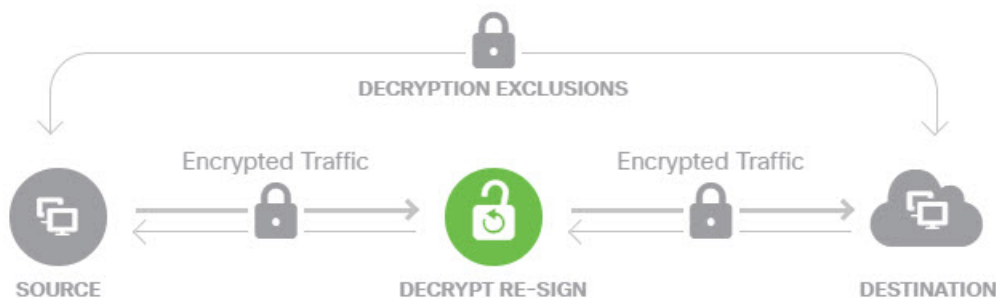
通过 SSL 解密策略的任何流量均必须通过访问控制策略。除了 SSL 解密策略中丢弃的流量外，最终的允许或丢弃决定还取决于访问控制策略。

解密重签名

如果选择解密或重签流量，系统将扮演中间人的角色。

例如，用户在浏览器中键入 `https://www.cisco.com`。流量到达 FTD 设备，然后设备使用规则中指定的 CA 证书与用户进行协商，并在用户和 FTD 设备之间建立 SSL 隧道。同时，设备连接至 `https://www.cisco.com`，并在服务器和 FTD 设备之间建立 SSL 隧道。

因此，用户将看到配置用于 SSL 解密规则的 CA 证书，而不是来自 `www.cisco.com` 的证书。用户必须信任该证书才能完成连接。FTD 设备随后对用户和目标服务器之间的流量执行双向解密/重新加密。



注释

如果客户端不信任用于对服务器证书重新签名的 CA，则会警告用户不应信任该证书。为了避免此情况，请将 CA 证书导入到客户端信任的 CA 库。或者，如果组织拥有专用 PKI，则可以颁发由根 CA（自动受组织中的所有客户端信任）签名的中级 CA 证书，然后将该 CA 证书上传到设备。

如果使用解密重签名操作配置规则，则除了已配置的任何规则条件之外，该规则会根据所引用的内部 CA 证书的签名算法类型来匹配流量。由于您可以选择用于 SSL 解密策略的单个重签证书，因此可以限制匹配重签规则的流量。

例如，仅当重签证书是基于 EC 的 CA 证书时，使用椭圆曲线 (EC) 算法加密的出站流量才能匹配解密重签名规则。同样，仅当全局重签证书为 RSA 时，使用 RSA 算法加密的流量才可与解密重签名规则匹配；即使所有其他配置的规则条件匹配，使用 EC 算法加密的出站流量也与规则不匹配。

解密已知密钥

如果您拥有目标服务器，则可使用已知密钥实现解密。在这种情况下，用户打开 <https://www.cisco.com> 的连接后，用户会看到 www.cisco.com 的实际证书，即使出示证书的是 FTD 设备。



您的组织必须是域和证书的所有者。以 [cisco.com](https://www.cisco.com) 为例，让最终用户查看思科证书的唯一可能方式是，您实际拥有域 [cisco.com](https://www.cisco.com)（即您是思科系统公司）并拥有由公共 CA 签名的 [cisco.com](https://www.cisco.com) 证书。您仅可使用已知密钥对您的组织拥有的站点进行解密。

使用已知密钥进行解密的主要目的是对通往 HTTPS 服务器的流量进行解密，以保护服务器免受外部攻击。如要检查流向外部 HTTPS 站点的客户端流量，由于您不是服务器所有者，所以必须使用解密重签名。



注释

要使用已知密钥解密，必须将服务器证书和密钥上传为内部身份证书，再在 SSL 解密策略设置中将其添加至已知密钥证书。然后，可编写已知密钥解密规则，其中服务器地址为目标地址。有关将证书添加至 SSL 解密策略的信息，请参阅[为已知密钥和重签解密配置证书](#)，第 233 页。

不解密

如果选择绕行某些类型的流量的解密，则不会对流量进行任何处理。系统会使加密流量继续进入访问控制策略，根据流量所匹配的访问控制规则对其执行允许或丢弃操作。

阻止

您可以简单地阻止匹配 SSL 解密规则的加密流量。阻止 SSL 解密策略可防止连接到访问控制策略。

阻止 HTTPS 连接后，用户看不到系统默认阻止响应页面。相反，用户会看到浏览器显示安全连接故障的默认页面。错误消息不会指明该站点由于策略而被阻止。相反，错误可能显示为没有通用的加密算法。据此消息，无法明确看出是您有意阻止了该连接。

自动生成的 SSL 解密规则

无论您是否启用 SSL 解密策略，系统都会自动为实施主动身份验证的各身份策略规则生成解密重签名规则。这是为 HTTPS 连接启用主动身份验证的必然要求。

启用 SSL 解密策略后，您可以在“身份策略主动身份验证规则”标题下看到这些规则。这些规则归入 SSL 解密策略顶部。这些规则为只读格式。仅可通过更改身份策略进行更改。

处理不可解密流量

有几个特点使得连接不可解密。如果连接具有以下任何特征，则默认操作将应用于该连接，而不管该连接本可能会与哪个规则匹配。如果将“阻止”选作默认操作（而不是“不解密”），则可能会出问题，包括过度丢弃合法流量的问题。

- 压缩会话 - 数据压缩应用于连接。
- SSLv2 会话 - 支持的最低 SSL 版本是 SSLv3。
- 未知密码套件 - 系统无法识别连接的密码套件。
- 不受支持的密码套件 - 系统不支持根据检测到的密码套件进行解密。
- 会话未缓存 - SSL 会话已启用会话重复使用，客户端和服务器使用会话标识符重新建立了该会话，并且系统未缓存该会话标识符。
- 握手错误 - SSL 握手协商期间出错。
- 解密错误 - 解密操作期间出错。
- 被动接口流量 - 被动接口（被动安全区域）上的所有流量均无法解密。

SSL 解密许可证要求

使用 SSL 解密策略无需特殊许可证。

但需要 [URL 过滤许可证](#) 创建将 URL 类别和信誉作为匹配标准的规则。有关配置许可证的信息，请参阅 [启用或禁用可选许可证](#)，第 74 页。

SSL 解密指南

配置和监控 SSL 解密策略时，请注意以下事项：

- 对匹配设置进行信任或阻止的访问控制规则的连接绕过 SSL 解密策略，如果这些规则满足以下条件：
 - 将安全区、网络、地理位置和端口仅用作流量匹配条件。

- 排在任何要求检测的其他规则之前，例如，基于应用或 URL 匹配连接的规则，或允许应用入侵或文件检测的规则。
- 使用 URL 类别匹配时，请注意，有时候站点登录页的类别与站点本身的类别不同。例如，Gmail 的类别是“基于网页的邮件”，而登录页的类别是“互联网门户网站”。要对到这些站点的连接解密，必须在规则中添加这两个类别。
- 如果漏洞数据库 (VDB) 更新删除（弃用）应用，则必须对使用已删除应用的任何 SSL 解密规则或应用过滤器进行更改。修复这些规则前，您无法部署更改。此外，您无法在解决问题之前安装系统软件更新。在“应用过滤器对象”页面上或规则的“应用”选项卡上，这些应用在其名称后显示“(Deprecated)”。
- 如果您有任何主动身份验证规则，将无法禁用 SSL 解密策略。要禁用 SSL 解密策略，您必须禁用身份策略，或者删除任何使用主动身份验证的身份规则。

如何实施和维护 SSL 解密策略

您可以使用 SSL 解密策略将加密流量转换为纯文本流量，以便可应用 URL 过滤、入侵和恶意软件控制以及其他需要深度数据包检测的服务。如果策略允许流量通过，则流量在离开设备前会被重新加密。

SSL 解密策略仅适用于加密流量。系统不会根据 SSL 解密规则评估未加密连接。

与其他一些安全策略不同的是，您需要监控并积极维护 SSL 解密策略，这是因为目标服务器上的证书可能会过期甚至发生变更。此外，客户端软件的变更可能会改变解密某些连接的能力，这是因为解密重签名操作无法与中间人攻击区分开来。

以下程序介绍了实施和维护 SSL 解密策略的端到端流程。

过程

步骤 1 如果要实施解密重签名规则，请创建所需的内部 CA 证书。

必须使用内部证书颁发机构 (CA) 证书。有以下选项可供选择。由于用户必须信任证书，因此应上传客户端浏览器已配置为可信任的证书，或确保所上传的证书已添加到浏览器信任存储区。

- 创建由设备自身签署的自签名内部 CA 证书。请参阅[生成自签名的内部和内部 CA 证书](#)，第 126 页。
- 上传由外部受信任 CA 或组织内部 CA 签署的内部 CA 证书和密钥。请参阅[上传内部和内部 CA 证书](#)，第 124 页。

步骤 2 如果要实施解密已知密钥规则，请从各内部服务器收集证书和密钥。

只可将解密已知密钥用于您所控制的服务器，这是因为必须从服务器中获取证书和密钥。上传这些证书和密钥，作为内部证书（而不是内部 CA 证书）。请参阅[上传内部和内部 CA 证书](#)，第 124 页。

步骤 3 启用 SSL 解密策略，第 226 页。

启用该策略时，还需要配置一些基本设置。

步骤 4 配置默认 SSL 解密操作，第 226 页。

如有疑问，请选择**不解密**作为默认操作。在适当的情况下，访问控制策略仍然可以丢弃与默认 SSL 解密规则匹配的流量。

步骤 5 配置 SSL 解密规则，第 227 页。

标识要解密的流量以及要应用的解密类型。

步骤 6 如要配置已知密钥解密，请编辑 SSL 解密策略设置，以加入这些证书。请参阅[为已知密钥和重签解密配置证书，第 233 页](#)。

步骤 7 如有需要，下载用于解密重签名规则的 CA 证书并将其上传到客户端工作站上的浏览器。

有关下载证书并将其分发给客户端的信息，请参阅[为解密重签名规则下载 CA 证书，第 234 页](#)。

步骤 8 定期更新重新和已知密钥证书。

- 重签证书 - 在证书过期之前更新此证书。如果通过 Firepower 设备管理器生成证书，则有效期为 5 年。要检查证书的有效期，请依次选择**对象 > 证书**，在列表中查找该证书，然后在“操作”列中点击证书的信息图标 (i)。“信息”对话框显示有效期和一些其他属性。此外，也可从此页面上替换证书。
- 已知密钥证书 - 对于任何已知密钥解密规则，需要确保已上传目标服务器的当前证书和密钥。只要所支持的服务器上的证书和密钥发生更改，就必须上传新的证书和密钥（作为内部证书）并更新 SSL 解密设置，以使用新证书。

步骤 9 上传外部服务器缺失的受信任 CA 证书。

系统包含各种由第三方颁发的受信任根证书和中间证书。为解密重签名规则协商 FTD 和目标服务器之间的连接时，需要这些证书。

将根 CA 的信任链中的所有证书都上传到受信任 CA 证书列表中，包括根 CA 证书和所有中间 CA 证书。否则，更难以检测由中间 CA 颁发的受信任证书。在**对象 > 证书**页面上上传证书。请参阅[上传受信任的 CA 证书，第 127 页](#)。

配置 SSL 解密策略

您可以使用 SSL 解密策略将加密流量转换为纯文本流量，以便可应用 URL 过滤、入侵和恶意软件控制以及其他需要深度数据包检测的服务。如果策略允许流量通过，则流量在离设备前会被重新加密。

SSL 解密策略仅适用于加密流量。系统不会根据 SSL 解密规则评估未加密连接。



注释 VPN 隧道在 SSL 解密策略评估之前已解密，因此该策略永远不适用于隧道本身。但是，隧道内的任何加密连接都要通过 SSL 解密策略进行评估。

以下程序介绍了如何配置 SSL 解密策略。有关创建和管理 SSL 解密的端到端流程说明，请参阅[如何实施和维护 SSL 解密策略](#)，第 223 页。

开始之前

SSL 解密规则表包含两个部分：

- **身份策略主动身份验证规则** - 如果启用身份策略并创建使用主动身份验证的规则，系统将自动创建使这些策略生效所需的 SSL 解密规则。这些规则始终在您自己创建的 SSL 解密规则之前进行评估。只可通过更改身份策略来间接更改这些规则。
- **SSL 本机规则** - 这些是已经配置的规则。只能将规则添加到此部分。

过程

步骤 1 依次选择策略 > SSL 解密。

如果尚未启用该策略，请点击[启用 SSL 解密](#)并按[启用 SSL 解密策略](#)，第 226 页中的说明配置策略设置。

步骤 2 配置策略的默认操作。

最安全的选择是**不解密**。有关详细信息，请参阅[配置默认 SSL 解密操作](#)，第 226 页。

步骤 3 管理 SSL 解密策略。

在配置 SSL 解密设置后，此页面将按顺序列出所有规则。规则依据流量按照从上到下的顺序进行匹配，由第一个匹配项确定要应用的操作。从此页面中可以执行以下操作：

- 要禁用该策略，请点击 **SSL 解密策略** 开关。可以通过点击[启用 SSL 解密](#)重新启用该策略。
- 要编辑策略设置（包括策略中使用的证书列表），请点击 **SSL 解密设置按钮** (⚙️)。此外，还可以下载与解密重签名规则一起使用的证书，以便将其分发给客户端。请参阅以下主题：
 - [为已知密钥和重签解密配置证书](#)，第 233 页
 - [为解密重签名规则下载 CA 证书](#)，第 234 页
- 要配置规则，请执行以下操作：
 - 要创建新规则，请点击 + 按钮。请参阅[配置 SSL 解密规则](#)，第 227 页。
 - 要编辑现有规则，请点击该规则的编辑图标 (🔗)（在“操作”列中）。也可以选择表中点击某编辑属性来编辑该属性。
 - 要删除不再需要的规则，请点击该规则的删除图标 (🗑️)（在“操作”列中）。

- 要移动规则，请编辑规则并从**顺序**下拉列表中选择新位置。

启用 SSL 解密策略

在可以配置 SSL 解密规则之前，必须启用该策略并配置一些基本设置。以下程序介绍了如何直接启用该策略。此外，还可在启用身份策略时启用该策略。身份策略要求启用 SSL 解密策略。

开始之前

如果从未设置 SSL 解密策略的版本进行升级，但已使用主动身份验证规则配置身份策略，则 SSL 解密策略已启用。确保已选择要使用的解密重签名证书，并且可以选择启用预定义规则。

过程

步骤 1 依次选择**策略 > SSL 解密**。

步骤 2 点击**启用 SSL 解密配置策略设置**。

- 如果是第一次启动该策略，系统将打开“SSL 解密配置”对话框。继续进行后续步骤。
- 如果已对策略进行过一次配置然后禁用了策略，则只需使用之前的设置和规则即可再次启动该策略。可以点击**SSL 解密设置按钮** (⚙️) 并按照[为已知密钥和重签解密配置证书](#)，第 233 页中所述的方式配置设置。

步骤 3 在**解密重签名证书**中，选择相应内部 CA 证书，以用于利用重签证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击**创建内部 CA** 进行创建。

如果尚未在客户端浏览器中安装证书，请点击**下载按钮** (↓) 获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅[为解密重签名规则下载 CA 证书](#)，第 234 页。

步骤 4 选择初始 SSL 解密规则。

系统包含可能对您有用的下列预定义规则：

- **Sensitive_Data** - 该规则不对与金融服务和医疗 URL 类别（包括银行、医疗服务等）网站匹配的流量进行解密。必须启用 URL 许可证才能实现该规则。

步骤 5 点击**启用**。

配置默认 SSL 解密操作

如果加密连接没有匹配特定 SSL 解密规则，则由 SSL 解密策略的默认操作来处理。

过程

步骤 1 依次选择策略 > SSL 解密。

步骤 2 点击默认操作字段的任意位置。

步骤 3 选择应用于匹配流量的操作。

- **不解密** - 允许加密连接。然后，访问控制策略将评估加密连接，并根据访问控制规则丢弃或允许该连接。
- **阻止** - 立即丢弃连接。连接将不传递到访问控制策略。

步骤 4 (可选。) 针对默认操作配置日志记录。

要在控制面板数据或事件查看器中包括匹配默认操作的流量，必须对匹配默认操作的流量启用日志记录。从以下选项中选择：

- **连接结束时** - 在连接结束时生成事件。
- **将连接事件发送到** - 如果要将事件副本发送至外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建新系统日志服务器**，并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择任何）。

由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

- **无日志记录** - 不生成任何事件。

步骤 5 点击保存。

配置 SSL 解密规则

使用 SSL 解密规则确定如何处理加密连接。SSL 解密策略中的规则按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件标准的第一个规则。

只可在“SSL 本机规则”部分创建和编辑规则。



注释

在 SSL 解密策略评估连接之前，系统将对 VPN 连接（站点间和远程访问）流量进行解密。因此，SSL 解密规则永远不会应用于 VPN 连接，且在创建这些规则时不需要考虑 VPN 连接。但是，系统会对 VPN 隧道中使用的所有加密连接进行评估。例如，SSL 解密规则将对通过 RA VPN 连接到内部服务器的 HTTPS 连接进行评估，即使 RA VPN 隧道本身没有接受评估（原因在于其已解密）。

开始之前

如要创建解密已知密钥规则，请确保上传目标服务器的证书和密钥（作为内部证书），并编辑 SSL 解密策略设置，以使用该证书。已知密钥规则通常在该规则目标网络条件中指定目标服务器。有关详细信息，请参阅[为已知密钥和重签解密配置证书](#)，第 233 页。

过程

步骤 1 依次选择策略 > SSL 解密。

如果未配置任何 SSL 解密规则（不是为主动身份验证的身份规则自动生成的规则），可以点击[添加预定义规则](#)来添加预定义规则。系统将提示您选择所需的规则。

步骤 2 执行以下任一操作：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 (🔗)。

要删除不再需要的规则，请点击该规则的删除图标 (🗑️)。

步骤 3 在顺序中，选择要将该规则插入在已排序有序规则列表插入该规则的位置。

只可将规则插入 **SSL 本机规则** 部分。身份策略主动身份验证规则将根据身份策略自动生成并且为只读形式。

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 4 在名称中输入规则的名称。

名称不能包含空格。可以使用字母数字字符和以下特殊字符：+ . _ -

步骤 5 选择应用于匹配流量的操作。

有关每个选项的详细讨论，请参阅下列内容：

- [解密重签名](#)，第 220 页
- [解密已知密钥](#)，第 221 页
- [不解密](#)，第 221 页
- [阻止](#)，第 221 页

步骤 6 使用以下选项卡的任意组合，定义流量匹配标准：

- [源/目标](#) - 流量通过的安全区域（接口）、IP 地址或该 IP 地址的国家/地区或大陆（地理位置）或者流量中使用的 TCP 端口。默认设置为任何区域、地址、地理位置和 TCP 端口。请参阅[SSL 解密规则的源/目标标准](#)，第 229 页。

- **应用** - 应用或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何加密应用。请参阅 [SSL 解密规则的应用标准](#)，第 231 页。
- **URL** - Web 请求的 URL 类别。默认情况下，进行匹配时不考虑 URL 类别和信誉。请参阅 [SSL 解密规则的 URL 标准](#)，第 231 页。
- **用户** - 用户或用户组。身份策略决定了用户和组的信息是否可用于流量匹配。只有配置身份策略，才能使用此条件标准。请参阅 [SSL 解密规则的用户标准](#)，第 232 页。
- **高级** - 从连接中使用的证书派生的特性，例如 SSL/TLS 版本和证书状态。请参阅 [SSL 解密规则的高级标准](#)，第 233 页。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后在弹出对话框中点击**确定**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的 **x**，可将其从策略中移除。

向 SSL 解密规则中添加条件时，请考虑以下提示：

- 您可以为每个规则配置多个条件。要使规则应用于流量，流量必须匹配该规则中的所有条件。例如，可以使用单一规则来基于 URL 类别对流量进行解密。
- 最多可以为规则中的每个条件添加 50 个标准。匹配某个条件所有条件标准的流量满足该条件。例如，您可以使用单一规则为最多 50 个应用或应用过滤器执行应用控制。因此，单一条件中的项目之间为 OR 关系，但不同条件类型之间（例如，源/目的目标和应用之间）为 AND 关系。
- 匹配 URL 类别需要 URL 过滤许可证。

步骤 7 （可选。）针对规则配置日志记录。

对于与控制面板或事件查看器中包括的规则匹配的流量，必须为其启用日志记录。从以下选项中选择：

- **连接结束时** - 在连接结束时生成事件。
 - **将连接事件发送到** - 如果要将事件副本发送至外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建新系统日志服务器**，并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择“任何”）。
- 由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

- **无日志记录** - 不生成任何事件。

步骤 8 单击 **OK**。

SSL 解密规则的源/目标标准

SSL 解密规则的源/目标条件定义了流量通过的安全区（接口）、IP 地址或该 IP 地址所在的国家/地区或大洲（地理位置）或是流量中所用的 TCP 端口。默认设置为任何区域、地址、地理位置、协议和任何 TCP 端口。TCP 是与 SSL 解密规则匹配的唯一协议。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后点击**确定**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的 **x**，可将其从策略中移除。

您可以通过以下标准来标识规则中要匹配的源和目的地。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至**目标区域**。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至**源区域**。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保从外部主机到内部主机的所有流量均被解密，则应将外部区域选为**源区域**，并将内部区域选为**目标区域**。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置**源网络**。
- 要匹配流向 IP 地址或地理位置的流量，请配置**目标网络**。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目的 IP 地址的网络对象或组。



注释 对于解密已知密钥规则，请选择使用目标服务器 IP 地址的对象（该对象使用您上传的证书和密钥）。

- **地理位置** - 选择要基于流量的源或目的国家/地区或大陆控制流量的地理位置。选择大陆将会选择该大陆内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

源端口、目标端口/协议

定义流量中所用协议的端口对象。仅可指定用于 SSL 解密规则的 TCP 协议和端口。

- 要匹配来自 TCP 端口的流量，请配置**源端口**。
- 要匹配流向 TCP 端口的流量，请配置**目标端口/协议**。

- 要同时匹配来自特定 TCP 端口的流量和流向特定 TCP 端口的流量，请配置源端口和目标端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

SSL 解密规则的应用标准

SSL 解密规则的应用标准定义 IP 连接中使用的应用，或定义按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认为任何具有 SSL 协议标记的应用。您无法将 SSL 解密规则与任何未加密应用相匹配。

虽然您可以在规则中指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条 SSL 解密规则，用于解密或阻止所有业务关联性较低的高风险应用。如果用户尝试使用这些应用中的任意一个，系统会解密或阻止会话。

另外，思科会通过系统和漏洞数据库 (VDB) 更新频繁更新和添加其他应用检测器。因此，高风险应用规则可自动应用到新应用中，而无需您手动更新规则。

您可以直接在规则指定应用和过滤器，也可以创建定义这些特征的应用过滤器对象。规格相当，尽管如果要创建复杂规则，使用对象可便于遵守每个条件 50 个项目的系统限制。

要修改应用和过滤器列表，请点击该条件内的 + 按钮，选择在单独选项卡中列出的相应应用或应用过滤器对象，然后在弹出对话框中点击**确定**。在任一选项卡中，您可以点击**高级过滤器**选择过滤器条件或帮助您搜索特定应用。点击应用、过滤器或对象的 **x**，可将其从策略中移除。点击**另存为过滤器链接**，可将尚不是对象的组合条件另存为新应用过滤器对象。

有关应用标准以及如何配置高级过滤器和选择应用的更多信息，请参阅[配置应用过滤器对象](#)，第 115 页。

在 SSL 解密规则中使用应用标准时，请考虑以下提示。

- 系统可以识别使用 StartTLS 进行加密的未加密应用。这包括诸如 SMTPS、POPS、FTPS、TelnetS 和 IMAPS 之类的应用。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书使用者可分辨名称值来识别某些加密应用。
- 仅在服务器证书交换后，系统才可识别使用。如果在 SSL 握手期间交换的流量与包含应用条件的 SSL 规则中的所有其他条件相匹配，但是识别未完成，则 SSL 策略允许数据包通过。此行为允许完成握手，以便可以识别应用。在系统完成其识别后，系统将 SSL 规则操作应用于与其应用条件相匹配的剩余会话流量。
- 如果所选应用已由 VDB 更新删除，则会在应用名称后显示“(Deprecated)”。必须从过滤器中删除这些应用，否则将阻止后续部署和系统软件升级。

SSL 解密规则的 URL 标准

SSL 解密规则的 URL 标准定义了 Web 请求中的 URL 所属的类别。还可以指定要解密、阻止或允许不解密的站点的相对信誉。默认不基于 URL 类别匹配连接。

例如，您可以阻止所有加密的赌博网站，或解密高风险社交网站。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止或解密。有关 URL 类别匹配的详细信息，请参阅[按照类别和信誉过滤 URL](#)，第 259 页。

“类别”选项卡

点击 +，选择所需的类别，然后点击**确定**。点击类别或对象的 **x**，可将其从策略中删除。

默认为将规则应用于每个选定类别的所有 URL，不考虑信誉。要根据信誉限制规则，请点击每个类别的向下箭头，取消选中任何复选框，然后使用**信誉**滑块选择信誉级别。信誉滑块的左侧指明待允许而不解密的站点，右侧是要解密或阻止的站点。如何使用信誉取决于规则操作：

- 如果该规则解密或阻止连接，则选择某个信誉级别也会选择高于该级别的所有信誉。例如，如果配置规则以解密或阻止**可疑站点**（第 2 级），系统还会自动解密或阻止**高风险**（第 1 级）站点。
- 如果规则允许连接而不解密（不解密），则选择某个信誉级别也会选择低于该级别的所有信誉。例如，如果配置规则不解密**良性站点**（第 4 级），该规则还会自动不解密**知名**（第 5 级）站点。

SSL 解密规则的用户标准

SSL 解密规则的“用户”条件对 IP 连接的用户或用户组进行了定义。只有配置身份策略和相关联的目录服务器，才能在规则中包括用户或用户组条件。

您的身份策略决定是否收集某个特定连接的用户身份。如果建立了身份，则主机的 IP 地址与所识别的用户相关联。因此，源 IP 地址映射到用户的流量将被视为来自该用户。IP 数据包本身不包含用户身份信息，所以此 IP 地址到用户的映射是最接近的近似值。

由于最多可以向规则中添加 50 个用户或群组，所以选择群组比选择单个用户通常更有意义。例如，您可以创建规则，对从外部网络发往工程组的流量进行解密，并单独创建一个不会对从该组传出的流量进行解密的规则。然后，要将该规则应用于新工程师，您只需添加将工程师添加到目录服务器的“工程”组即可。

要修改用户列表，请点击该条件内的 + 按钮，并使用以下任一方法选择所需的用户或用户组。点击用户或组对应的 **x**，或将其从策略中移除。

- **用户和组**选项卡 - 选择所需的用户或用户组。只有在目录服务器中配置了群组，才能使用群组。如果您选择了某个群组，规则将应用于该群组的所有成员，包括子组。如果要区别对待某个子组，您需要针对该子组创建一条单独的访问规则，并将其置于访问控制策略中适用于父组的规则之上。
- **特殊实体**选项卡 - 从以下项目中选择：
 - **身份验证失败** - 系统提示用户进行身份验证，但用户未在允许的最大尝试次数内输入有效的用户名/密码对。身份验证失败本身不会阻止用户访问网络，但您可以写入访问规则来限制这些用户访问网络。
 - **访客** - “访客”用户与“身份验证失败”用户类似，只是您的身份规则配置为将这些用户称为“访客”。系统提示“访客”(Guest) 用户进行身份验证，但他们在最大尝试次数内未成功通过身份验证。
 - **无需身份验证** - 系统不提示用户进行身份验证，因为该类用户的连接与指定不进行身份验证的身份规则匹配。

- 未知 - 没有用户的 IP 地址映射，也没有身份验证失败的记录。通常，这意味着尚无来自该地址的 HTTP 流量。

SSL 解密规则的高级标准

高级流量匹配标准与根据连接中使用的证书派生的属性有关。您可以配置以下任何或全部选项。

证书属性

如果流量与任何选定属性匹配，则它与相应规则的证书属性选项匹配。您可以配置以下内容：

证书状态

证书无效还是有效。如果您不关心证书状态，请选择任意（默认）。

如果满足以下所有条件，证书即视为有效，否则视为无效：

- 策略信任颁发证书的 CA。
- 可根据证书的内容对证书的签名进行适当的验证。
- 颁发者 CA 证书存储在策略的受信任 CA 证书列表中。
- 策略的受信任 CA 未撤销证书
- 当前日期介于证书的有效期开始日期和有效期结束日期之间。

自签名

服务器证书是否包含相同的使用者和颁发者可分辨名称。选择以下一个选项：

- 自签名 - 服务器证书自签名。
- CA 签名 - 服务器证书由证书颁发机构签名。也就是说，颁发者和使用者不同。
- 任意 - 不考虑按照匹配标准，证书是否为自签名。

支持的版本

要匹配的 SSL/TLS 版本。该规则适用于仅使用任何选定版本的流量。默认设置是所有版本。可以选择以下版本：**SSLv3.0**、**TLSv1.0**、**TLSv1.1** 和 **TLSv1.2**。

例如，如果仅希望允许 TLSv1.2 连接，则可创建用于非 TLSv1.2 版本的阻止规则。

使用任何未列出版本（例如 SSL v2.0）的流量均由 SSL 解密策略的默认操作处理。

为已知密钥和重签解密配置证书

如果通过重签或使用已知密钥实施解密，则需要确定 SSL 解密规则可以使用的证书。确保所有证书均有效且未过期。

特别是对于已知密钥的解密，需要确保系统拥有要解密连接的各目标服务器的当前证书和密钥。通过解密已知密钥规则，可以使用目标服务器的实际证书和密钥进行解密。因此，必须确保 FTD 设备始终拥有当前证书和密钥，否则将无法成功解密。

只要在已知密钥规则中更改目标服务器上的证书或密钥，就要上传新的内部证书和密钥。将上述证书作为内部证书（而不是内部 CA 证书）上传。可以在下列程序中上传证书，也可以转到**对象 > 证书**页面并在此页面中上传。

过程

步骤 1 依次选择**策略 > SSL 解密**。

步骤 2 点击**SSL 解密设置按钮** (⚙️)。

步骤 3 在**解密重签名证书**中，选择相应内部 CA 证书，以用于利用重签证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击**创建内部 CA** 进行创建。

如果尚未在客户端浏览器中安装证书，请点击**下载按钮** (↓) 获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅**为解密重签名规则下载 CA 证书**，第 234 页。

步骤 4 对于使用已知密钥解密的每条规则，上传目标服务器的内部证书和密钥。

- a) 点击**解密已知密钥证书**下的 +。
- b) 选择内部身份证书，或点击**创建新的内部证书**以便立即上传。
- c) 单击 **OK**。

步骤 5 点击**保存**。

为解密重签名规则下载 CA 证书

如果决定对流量进行解密，则用户必须拥有加密流程中使用的内部 CA 证书，该证书为使用 TLS/SSL 的应用中被定义为受信任根证书颁发机构所颁发。通常，如果生成证书，这些应用会尚未将其定义为受信任证书，有时候即使导入证书也会如此。默认情况下，在大多数 Web 浏览器中，当用户发送 HTTPS 请求时，他们将看到一条来自客户端应用的警告消息，告知他们网站的安全证书有问题。通常，错误消息表明网站的安全证书并非由受信任证书颁发机构所颁发或网站由未知机构所认证，但该警告可能还表明可能存在中间人攻击。一些其他客户端应用程序不会向用户显示此警告消息，也不允许用户接受无法识别的证书。

可以通过以下方式为用户提供所需的证书：

通知用户接受根证书

可以通知贵组织中的用户，告知其公司的新策略并指示其接受组织提供的根证书作为受信任来源。用户应接受该证书并将其保存在受信任根证书颁发机构存储区，以确保在下次访问该站点时系统不会再次提示。



注释 用户需要接受并信任创建替换证书的 CA 证书。如果仅信任替换服务器证书，用户访问各个不同 HTTPS 站点时将看到警告。

将根证书添加到客户端设备

能够以受信任根证书颁发机构身份将根证书添加到网络上的所有客户端设备。这样，客户端应用将自动接受包含根证书的事务。

可以通过以下方式向用户提供证书：通过邮件发送或将其放在共享站点上，将证书整合到企业工作站映像中并使用应用更新工具将其自动分发给用户。

以下程序介绍了如何下载内部 CA 证书并将其安装在 Windows 客户端上。

过程

步骤 1 从 Firepower 设备管理器中下载证书。

- a) 依次选择**策略 > SSL 解密**。
- b) 点击**SSL 解密设置按钮** (⚙️)。
- c) 点击**下载按钮** (📄)。
- d) 选择一个下载位置，或者更改文件名（但是不要更改扩展名），然后点击**保存**。

此时可以取消“SSL 解密设置”对话框。

步骤 2 在客户端系统上，在 Web 浏览器的受信任根证书颁发机构存储区安装证书，或向客户端提供证书，以便用户自行安装。

该流程因操作系统和浏览器类型的不同而不同。例如，对于 Windows 上运行的 Internet Explorer 和 Chrome 浏览器，可以采用以下流程。（对于 Firefox，请依次选择**工具 > 选项 > 高级页面**，进行安装。）

- a) 从**开始菜单**中，依次选择**控制面板 > Internet 选项**。
- b) 选择**内容选项卡**。
- c) 点击**证书按钮**，打开“证书”对话框。
- d) 选择**受信任根证书颁发机构选项卡**。
- e) 点击**导入**，然后根据向导找到并选择下载的文件 (<uuid>_internalCA.crt) 并将其添加到受信任根证书颁发机构存储区。
- f) 点击**完成**。

系统应显示消息，指示已成功导入。您可能会看到一个中间对话框，警告：如果生成自签名证书而不是从知名第三方证书颁发机构获取证书，则 Windows 无法验证该证书。

此时，可以关闭“证书”和“Internet 选项”对话框。

示例：从网络阻止较旧的 SSL/TLS 版本

某些组织需要通过政府法规或公司策略来阻止使用较旧版本的 SSL 或 TLS。可以使用 SSL 解密策略来阻止使用您禁止的 SSL/TLS 版本的流量。请考虑将此规则置于 SSL 解密策略的顶部，以确保立即捕获禁止的流量。

以下示例阻止所有 SSL 3.0 和 TLS 1.0 连接。

开始之前

此过程假定已启用 SSL 解密策略，如中[启用 SSL 解密策略](#)，第 226 页所述。

过程

步骤 1 依次选择策略 > SSL 解密。

步骤 2 点击 + 按钮创建新规则。

步骤 3 按顺序选择 1 将规则置于策略的顶部，或选择最适合您网络的数字。

默认情况下，会将该规则添加到策略的末尾。

步骤 4 在标题中，输入规则名称，例如，Block_SSL3.0_and_TLS1.0。

步骤 5 在操作中，选择阻止。这将立即丢弃与该规则匹配的任何流量。

步骤 6 保留以下选项卡上所有选项的默认值：源/目标、应用、URL 和 用户。

步骤 7 点击高级选项卡，并在受支持版本下，选择 SSL3.0 和 TLS1.0，但取消选中 TLS1.1 和 TLS1.2。

策略应如下所示：

Add SSL Decryption Rule

Order	Title	Action
1	Block_SSL3.0_and_TLS1.0	Block

Source / Destination Applications URLs ¹ Users ¹ **Advanced** Logging

CERTIFICATES

Certificate Status	Self Signed	Certificate Pro
Any	Any	These options whether the ce option of the ru

SUPPORTED VERSION

SSL/TLS Version	Supported Ver
<input checked="" type="checkbox"/> SSL 3.0	The SSL/TLS v selected versio
<input checked="" type="checkbox"/> TLS 1.0	
<input type="checkbox"/> TLS 1.1	
<input type="checkbox"/> TLS 1.2	

步骤 8（可选）如果希望控制面板和事件反映阻止连接，请点击**日志记录**选项卡并选择在**连接结束时**。如果正在使用外部系统日志服务器，还可以选择该服务器。

步骤 9 点击**确定**。

您现在可以部署策略。部署后，通过系统的任何 SSL 3.0 或 TLS 1.0 连接均将弃用。

注释 SSL 2.0 连接由策略的默认操作处理。如果要确保已弃用这些，请将默认操作更改为阻止。

下一步做什么

如果实施此规则，我们具有以下建议：

- 对于任何类型的解密规则，请包括“高级”选项卡的默认设置，其中，所有 SSL/TLS 选项均已选中。通过应用至所有版本，可以简化握手过程。但是，您的初始阻止规则仍将阻止 SSL 3.0 和 TLS 1.0 连接。
- 通常建议使用“不解密”作为策略的默认操作。但是，由于 SSL 2.0 连接始终由默认操作处理，因此您可能希望改用“阻止”。但是，如果要将“不解密”应用为所有可解密流量的默认操作，请在策略末尾创建“不解密”规则，其中，您接受所有流量匹配条件的默认值。此规则将匹配与表中的较早规则不匹配的任何受支持 TLS 连接，并作为这些 TLS 版本的默认值。

监控和故障排除 SSL 解密

以下主题介绍如何监控和故障排除 SSL 解密策略。

监控 SSL 解密

您可以在控制面板和事件中查看有关匹配日志记录已启用的规则（或默认操作）的流量解密信息。

SSL 解密控制面板

要评估整体解密统计信息，请查看**监控 > SSL 解密**控制面板。控制面板显示以下信息：

- 加密流量与纯文本流量百分比。
- 按照 SSL 规则的流量解密百分比。

事件

除了控制面板，事件查看器（**监控 > 事件**）包括加密流量 SSL 信息。以下是评估事件的一些提示：

- 对于因匹配阻止匹配流量的 SSL 规则（或默认操作）而被丢弃的连接，操作应为“阻止”，原因应指示“SSL 阻止”。

- **SSL 实际操作**字段指示系统应用于连接的实际操作。这可能与 **SSL 预期操作**有所不同，SSL 预期操作指示在匹配规则上定义的操作。例如，连接可能与应用解密的规则匹配，但出于某些原因不能被解密。

处理解密重签名适用于浏览器而非应用的 Web 站点（SSL 或证书授权锁定）

智能手机和其他设备的某些应用使用 SSL（或证书授权）锁定技术。SSL 锁定技术将原始服务器证书的散列值嵌入到应用本身内部。因此，当应用收到来自 Firepower 威胁防御设备的重签证书时，散列验证会失败并中止连接。

主要表现是，用户使用站点应用无法连接到网站，但可以使用网络浏览器连接，即使在应用无法正常工作的同一台设备上使用浏览器也可以连接。例如，用户不能使用 Facebook iOS 或 Android 应用，但可以通过 <https://www.facebook.com> 转至 Safari 或 Chrome，进行成功连接。

由于 SSL 锁定专用于避免中间人攻击，因此此问题无法解决。必须从以下选项中选择一项：

- 支持应用用户，在这种情况下无法解密流向网站的任何流量。为站点应用创建“Do Not Decrypt”规则（在 SSL 解密规则的“应用”选项卡上），并确保该规则排在应用于连接的任何解密重签名规则前面。
- 强制用户只使用浏览器。如果必须解密流向网站的流量，需要向用户说明，通过您的网络连接时，他们无法使用站点应用，必须只能使用浏览器。

更多详细信息

如果站点在浏览器中可用，但不能在同一设备的应用中使用，几乎可以肯定这是一个 SSL 锁定实例。但是，如果您想要更深入地挖掘，除了浏览器测试之外，还可以使用连接事件确定 SSL 锁定。

应用可能会通过两种方式处理散列验证失败：

- 第 1 组应用，例如 Facebook，从服务器收到 SH、CERT、SHD 消息后立即发送 SSL 警告消息。警告通常是一个表示 SSL 锁定的“Unknown CA (48)”警告。紧接着警告消息发送 TCP 重置。在事件详细信息中，您应看到以下现象：
 - SSL 流标志包括 ALERT_SEEN。
 - SSL 流标志不包括 APP_DATA_C2S 或 APP_DATA_S2C。
 - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE。
- 第 2 组应用，例如 Dropbox，不会发送任何警告。而是，等到完成握手后发送 TCP 重置。在事件中，您应看到以下现象：
 - SSL 流标志不包括 ALERT_SEEN、APP_DATA_C2S 或 APP_DATA_S2C。
 - SSL 流消息通常是：CLIENT_HELLO、SERVER_HELLO、SERVER_CERTIFICATE、SERVER_KEY_EXCHANGE、SERVER_HELLO_DONE、CLIENT_KEY_EXCHANGE、

CLIENT_CHANGE_CIPHER_SPEC、CLIENT_FINISHED、
SERVER_CHANGE_CIPHER_SPEC、SERVER_FINISHED。

处理解密重签名适用于浏览器而非应用的 **Web** 站点（**SSL** 或证书授权锁定）



第 13 章

身份策略

您可以使用身份策略从连接中收集用户身份信息。然后，可以在控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。

- [身份策略概述，第 241 页](#)
- [如何实施身份策略，第 243 页](#)
- [配置身份策略，第 244 页](#)
- [启用透明用户身份验证，第 249 页](#)
- [监控身份策略，第 252 页](#)
- [身份策略示例，第 252 页](#)

身份策略概述

您可以使用身份策略检测与连接关联的用户。通过识别用户身份，可以将威胁、终端和网络智能与用户身份信息关联。通过将网络行为、流量和事件直接与单个用户相关联，系统可帮助您确定策略违规、攻击或网络漏洞的来源。

例如，可以确定入侵事件所攻击的主机的所有人是谁，并确定是谁发起了内部攻击或端口扫描。此外，还可以确定高带宽用户，以及正在访问不良网站或应用的用户。

用户检测不仅仅是收集数据进行分析，您也可以基于用户名或用户组名编写访问规则，根据用户身份选择性允许或阻止到资源的访问。

可以使用以下方法获取用户身份：

- 被动身份验证 - 对所有类型的连接，从其他身份验证服务获取用户身份而不提示输入用户名和密码。
- 主动身份验证 - 提示输入用户名和密码，并根据指定身份源进行身份验证，获取源 IP 地址的用户身份（仅限于 HTTP 连接）。

以下主题提供了有关用户身份的详细信息。

通过被动身份验证确定用户身份

被动身份验证在收集用户身份信息时不提示用户输入用户名和密码。系统会从您指定的身份源获取映射。

您可以从以下源被动获取用户到 IP 地址的映射：

- 远程接入 VPN 登录。被动身份支持以下用户类型：
 - 在外部验证服务器中定义的用户账户。
 - 在 Firepower 设备管理器中定义的本地用户账户。
- 思科身份服务引擎 (ISE)；思科身份服务引擎被动身份连接器 (ISE-PIC)。

如果给定用户是通过多个源所识别，则 RA VPN 身份占优先地位。

通过主动身份验证确定用户身份

身份验证是确认用户身份的行为。

如果 HTTP 流量来自系统没有其用户身份映射的 IP 地址，通过主动身份验证，您可以决定是否针对为系统配置的目录对发起该流量的用户进行身份验证。如果身份验证成功，该 IP 地址则被视为具有该通过身份验证的用户的身份。

如身份验证不成功，用户对网络的访问并不会受阻。为这些用户提供哪些访问权限最终由访问规则决定。

处理未知用户

当您为身份策略配置目录服务器后，系统会从目录服务器下载用户和组成员信息。此信息每 24 小时在午夜刷新一次，或在每次您编辑和保存目录配置时刷新（即使您未进行任何更改）。

如果某用户在活动身份验证身份规则提示时成功进行了身份验证，但该用户的名称不在下载的用户身份信息中，则该用户会被标记为“未知”。您不会在与身份相关的控制面板中看到该用户的 ID，该用户也不会匹配组规则。

但是，系统将应用面向未知用户的任何访问控制规则。例如，如果您阻止未知用户的连接，那么即使这些用户成功进行了身份验证（即目录服务器可识别用户并且密码有效），他们也会被阻止。

因此，当您对目录服务器进行更改（例如添加或删除用户，或更改组成员身份）时，直到系统从目录下载更新之后这些更改才会反映在策略实施中。

如果您不希望每天都等到午夜进行更新，可以通过编辑目录领域信息（依次选择**对象 > 身份源**，然后编辑领域）强制进行更新。点击**保存**，然后部署更改。系统随即会下载更新。



注释 您可以依次转至**策略 > 访问控制**，点击**添加规则 (+)** 按钮，并在**用户**选项卡上查看用户列表，从而检查系统上是否有新的或已删除的用户信息。如果找不到新用户，或者还是可以找到已删除的用户，则系统的信息未更新。

如何实施身份策略

要启用用户身份采集，以便得知与 IP 地址与关联的用户，您需要配置多个项目。正确配置后，您将能够看到监控控制面板和事件中的用户名。您还将能够在访问控制和 SSL 解密规则中使用用户身份作为流量匹配条件。

以下过程概述您必须配置哪些内容才能正常使用身份策略。

过程

步骤 1 配置 AD 身份领域。

不论您是主动（提示进行用户验证）使用用户身份，还是被动使用，都需要配置包含用户身份信息的 Active Directory (AD) 服务器。请参阅[配置 AD 身份领域](#)，第 132 页。

步骤 2 如果您想要使用被动身份验证身份规则，请配置被动身份源。

根据您要在设备中实现的服务和网络中可用的服务，您可以配置任何以下内容。

- 远程接入 VPN - 如果您要支持到设备的远程接入 VPN 连接，用户登录可以提供基于 AD 服务器或本地用户（Firepower 设备管理器中定义的用户）的身份。有关配置远程接入 VPN 的信息，请参阅[配置远程接入 VPN](#)，第 410 页。
- 思科身份服务引擎 (ISE) 或思科身份服务引擎被动身份连接器 (ISE PIC) - 如果您使用这些产品，您可以将设备配置为 pxGrid 订阅方，并从 ISE 获取用户身份。请参阅[配置身份服务引擎](#)，第 139 页。

步骤 3 依次选择**策略 > 身份**，并启用身份策略。请参阅[配置身份策略](#)，第 244 页。

步骤 4 [配置身份策略设置](#)，第 244 页。

基于您在系统中配置的源，自动选择被动身份源。如果您想要配置主动身份验证，您必须为强制网络门户和 SSL 重签解密（如果尚未启用 SSL 解密策略）配置证书。

步骤 5 [配置身份策略默认操作](#)，第 246 页。

如果您打算仅使用被动身份验证，您可以将默认操作设置为被动身份验证，无需创建特定规则。

步骤 6 [配置身份规则](#)，第 246 页。

创建将从相关网络收集被动或主动用户身份的规则。

配置身份策略

您可以使用身份策略从连接中收集用户身份信息。然后，可以在控制面板中基于用户身份查看使用情况，并根据用户或用户组配置访问控制。

下文概述了如何配置通过身份策略获取用户身份所需的元素。

过程

步骤 1 依次选择策略 > 身份。

如果尚未定义身份策略，请点击[启用身份策略](#)并按[配置身份策略设置](#)，第 244 页中的说明配置设置。

步骤 2 管理身份策略。

在配置身份设置后，此页面将按顺序列出所有规则。规则依据流量按照从上到下的顺序进行匹配，由第一个匹配项确定要应用的操作。从此页面中可以执行以下操作：

- 要启用或禁用身份策略，请点击[身份策略开关](#)。
- 要更改身份策略设置，请点击[身份策略配置按钮](#) ()。
- 要更改[默认操作](#)，请点击操作并选择所需的操作。请参阅[配置身份策略默认操作](#)，第 246 页。
- 要移动规则，请编辑规则并从[顺序](#)下拉列表中选择新位置。
- 要配置规则，请执行以下操作：
 - 要创建新规则，请点击 + 按钮。
 - 要编辑现有规则，请点击该规则的编辑图标 ()（在“操作”列中）。也可以选择表中点击某编辑属性来编辑该属性。
 - 要删除不再需要的规则，请点击该规则的删除图标 ()（在“操作”列中）。

有关创建和编辑身份策略的更多信息，请参阅[配置身份规则](#)，第 246 页。

配置身份策略设置

要正常使用身份策略，必须配置提供用户身份信息的源。必须配置的设置因配置的规则类型而异，而规则类型可以是被动和/或主动的。

这些设置显示在设置对话框的不同部分。您可以看到两个部分，也可以看到一个部分，具体取决于如何访问对话框。如果您尝试创建身份验证类型的规则，而没有事先配置所需的设置，系统将自动显示对话框。


以下过程介绍完整对话框。

开始之前

确保目录服务器、Firepower 威胁防御设备和客户端之间的时间设置一致。这些设备间的时间偏差可能会导致用户身份验证操作失败。“一致”说明您可以使用不同的时区，但时间相对于这些时区应是相同的；例如，10 AM PST = 1 PM EST。

过程

步骤 1 依次选择策略 > 身份。

步骤 2 点击身份策略配置按钮 ()。

步骤 3 配置被动身份验证选项。

对话框显示已经配置的被动身份验证源。

如有必要，您可以通过此对话框配置 ISE。如果您尚未配置 ISE 对象，可以点击集成 ISE 链接，立即创建对象。如果对象存在，将显示对象及其状态（已启用或已禁用）。

必须配置至少一个已启用被动身份源，才能创建被动身份验证规则。

步骤 4 配置主动身份验证选项。

如果身份规则要求对用户进行主动身份验证，则该用户将重定向到连接该用户所通过的界面上的强制网络门户，然后系统会提示用户进行身份验证。

服务器证书

选择在主动身份验证期间提供给用户的 CA 证书。如果尚未创建所需的证书，请点击下拉列表底部的创建新的内部证书。

如果用户不上传其浏览器已经信任的证书，则必须接受该证书。


端口

强制网络门户端口。默认端口是 885 (TCP)。如果配置了其他端口，则该端口必须 1025-65535 的范围内。

注释 对于 HTTP Basic、HTTP Response Page 和 NTLM 身份验证方法，通过接口的 IP 地址可将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 *firewall-hostname.AD-domain-name* 进行重定向。如果想要使用 HTTP Negotiate，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。

步骤 5 （仅主动身份验证。）在解密重签名证书中，选择相应内部 CA 证书，以用于利用重签证书实施解密的规则。

您可以使用预定义的 NGFW-Default-InternalCA 证书，也可以使用您创建或上传的证书。如果尚无证书，请点击创建内部 CA 进行创建。

如果尚未在客户端浏览器中安装证书，请点击下载按钮 () 获取副本。有关如何安装证书的信息，请参阅各浏览器文档。另请参阅[为解密重签名规则下载 CA 证书](#)，第 234 页。

注释 只有在未配置 SSL 解密策略的情况下，系统才会提示您进行 SSL 解密设置。要在启用身份策略之后更改这些设置，请编辑 SSL 解密策略设置。

步骤 6 点击保存。

配置身份策略默认操作

身份策略对不匹配任何身份规则的连接实施默认操作。

实际上，不设置规则是策略的有效配置。如果想在所有流量源上使用被动身份验证，只需将被动身份验证配置为默认操作。

过程

步骤 1 依次选择策略 > 身份。

步骤 2 点击默认操作，并从以下选项中选择一个：

- **被动身份验证(任何身份源)**-通过对不匹配任何身份规则的连接使用所有配置的被动身份源，确定用户身份。如果不配置任何被动身份源，使用被动身份验证作为默认选择等同于使用“不进行身份验证”。
- **不进行身份验证(不需要身份验证)**-不对不匹配任何身份规则的连接确定用户身份。

配置身份规则

身份规则确定是否应收集用户身份信息以匹配流量。如果您不想获取用户身份信息以匹配流量，则可以配置“无身份验证”(No Authentication)。

请记住，无论规则配置如何，都仅对 HTTP 流量进行主动身份验证。因此，无需创建规则将非 HTTP 流量从主动身份验证中排除。如果您希望获取所有 HTTP 流量的用户身份信息，只需将主动身份验证规则应用于所有源和目的。



注释 而且请记住，身份验证失败对网络访问没有影响。身份策略仅收集用户身份信息。如果要阻止无法进行身份验证的用户访问网络，则必须使用访问规则。

过程

步骤 1 依次选择策略 > 身份。

步骤 2 执行以下任一操作：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 (🔗)。

要删除不再需要的规则，请点击该规则的删除图标 (🗑️)。

步骤 3 在顺序中，选择要将该规则插入在已排序有序规则列表插入该规则的位置。

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 4 在名称中输入规则的名称。

步骤 5 选择操作，如有必要，还要选择 **AD 身份源**。

您必须选择包括用于被动和主动身份验证规则的用户账户的 **AD 身份领域**。

- **被动身份验证** - 使用被动身份验证确定用户身份。系统将会显示所有已配置的身份源。此规则会自动使用所有已配置的源。
- **主动身份验证** - 使用主动身份验证确定用户身份。主动身份验证仅适用于 HTTP 流量。如果任何其他类型的流量与要求或允许主动身份验证的身份策略匹配，则不会尝试进行主动身份验证。
- **无身份验证** - 不获取用户身份。基于身份的访问规则不会应用于此流量。这些用户将标记为无需身份验证。

步骤 6 (仅主动身份验证。) 选择您的目录服务器支持的身份验证方法 (类型)。

- **HTTP 基本身份验证** - 使用未加密的 HTTP 基本身份验证 (BA) 连接对用户进行身份验证。用户通过其浏览器的默认身份验证弹出窗口登录网络。这是默认值。
- **NTLM** - 使用 NT LAN Manager (NTLM) 连接对用户进行身份验证。仅当选择了一个 AD 领域时，此选项才可用。用户使用其浏览器的默认身份验证弹出窗口登录网络，不过您可以将 IE 和 Firefox 浏览器配置为使用其 Windows 登录域信息以透明方式进行身份验证(请参阅[启用透明用户身份验证](#)，第 249 页)。
- **HTTP 协商** - 允许设备协商用于用户代理 (用户发起流量流所用的应用) 和 Active Directory 服务器之间的方法。协商有助于使用广受支持的最强方法，顺序为先 NTLM，然后是 Basic 方法。用户通过其浏览器的默认身份验证弹出窗口登录网络。
- **HTTP 响应页面** - 提示用户使用系统提供的网页进行身份验证。这是一种 HTTP Basic 身份验证方法。

注释 对于 HTTP Basic、HTTP Response Page 和 NTLM 身份验证方法，通过接口的 IP 地址可将用户重定向到强制网络门户。但对于 HTTP 协商，用户将使用完全限定 DNS 名称 `firewall-hostname.AD-domain-name` 进行重定向。如果想要使用 HTTP Negotiate，还必须更新 DNS 服务器以将此名称映射到您需要进行主动身份验证的所有内部接口的 IP 地址。否则，将无法进行重定向，用户也无法进行身份验证。

步骤 7 (仅主动身份验证。) 依次选择以**访客身份回退** > **开/关**，确定是否将未通过主动身份验证的用户标记为访客用户。

用户有三次机会成功进行身份验证。如果仍不成功，选择此选项可以确定是否标记用户。您可以根据这些值编写访问规则。

- 以访客身份回退 > 开 - 系统将用户标记为访客。
- 以访客身份回退 > 关 - 系统将用户标记为未通过身份验证。

步骤 8 在源/目的选项卡上定义流量匹配条件。

请记住，仅在使用 HTTP 流量时才会尝试进行主动身份验证。因此，无需为非 HTTP 流量配置无身份验证规则，也无需为任何非 HTTP 流量创建主动身份验证规则。但是，被动身份验证适用于任何类型的流量。

身份规则的源/目的条件定义了流量通过的安全区（接口）、IP 地址或该 IP 地址所在的国家/地区或大洲（地理位置）或是流量中所用的协议和端口。默认设置为任何区域、地址、地理位置、协议和端口。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后在弹出对话框中点击确定。如果条件需要对象，而所需的对象不存在，您可以点击创建新对象。点击对象或元素对应的 x，可将其从策略中移除。

可以配置以下流量匹配条件。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至目标区域。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至源区域。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保从源自内部网络的所有流量收集用户身份，请选择内部区域作为源区域，同时将目的区域留空。

注释 不能在同一规则中搭配使用被动和路由安全区域。此外，被动安全区域只能被指定为源区域，不能作为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置源网络。
- 要匹配流向 IP 地址或地理位置的流量，请配置目标网络。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目的 IP 地址的网络对象或组。

- **地理位置** - 选择要基于流量的源或目的国家/地区或大陆控制流量的地理位置。选择大陆将会选择该大陆内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。

注释 为了确保使用最新地理位置数据过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

源端口、目标端口/协议

定义流量中所用协议的端口对象。对于 TCP/UDP，这可能包括端口。

- 要匹配来自协议或端口的流量，请配置**源端口**。源端口只能为 TCP/UDP。
- 要匹配流向协议或端口的流量，请配置**目标端口/协议**。
- 要同时匹配来自特定 TCP/UDP 端口的流量和流向特定 TCP/UDP 端口的流量，请配置源端口和目标端口。如果同时将源和目的端口添加至条件，则只能添加共享单一传输协议 (TCP 或 UDP) 的端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

步骤 9 单击 **OK**。

启用透明用户身份验证

如果将身份策略配置为允许进行主动身份验证，可以使用以下身份验证方法获取用户身份：

HTTP Basic

使用 HTTP Basic 身份验证时，系统会始终提示用户使用其目录用户名和密码进行身份验证。密码以明文形式传输。因此，Basic 身份验证不是一种安全的身份验证。

Basic 身份验证方法是默认的身份验证机制。

HTTP Response Page

这是一种 HTTP Basic 身份验证类型，使用时，用户会看到登录浏览器页面。

NTLM、HTTP Negotiate（适用于 Active Directory 的集成 Windows 身份验证）

使用集成的 Windows 身份验证，用户可以登录到域来使用其工作站。访问服务器（包括主动身份验证期间的 Firepower 威胁防御强制网络门户）时，浏览器将尝试使用此域登录。密码不进行传输。如果身份验证成功，则以透明方式对用户进行身份验证；用户不了解存在或解决的任何身份验证挑战。

如果浏览器使用域登录凭证无法满足某个身份验证请求，则系统会提示用户提供用户名和密码，这与 Basic 身份验证的用户体验是相同的。因此，如果配置集成的 Windows 身份验证，用户无需在访问同一域内的网络或服务时提供凭证。

请注意，HTTP Negotiate 会选择 Active Directory 服务器和用户代理支持的最强方法。如果协商选择 HTTP Basic 作为身份验证方法，则不会获取透明身份验证。强度顺序依次为 NTLM、Basic。协商必须选择 NTLM，才能进行透明身份验证。

您必须将客户端浏览器配置为支持集成的 Windows 身份验证才能进行透明身份验证。以下部分介绍了支持集成的 Windows 身份验证的一些常用浏览器的集成 Windows 身份验证常规要求和基本配置。有关更详细的信息，用户应参阅其浏览器（或其他用户代理）的帮助，因为各方法可能会因软件版本而不同。



提示 并非所有浏览器都支持集成的 Windows 身份验证，例如 Chrome 和 Safari（基于编写本文档时可用版本）。系统会提示用户提供用户名和密码。请参阅浏览器的文档确定您使用的版本是否支持。

透明身份验证的要求

用户必须将其浏览器或用户代理配置为实施透明身份验证。用户可以单独执行此操作，您也可以代其进行配置，并使用软件分发工具将此配置推送至客户端工作站。如果您选择让用户自己执行此操作，请确保提供适用于您的网络的特定配置参数。

无论是浏览器还是用户代理，您都必须实施以下常规配置：

- 将用户连接网络所采用的 Firepower 威胁防御接口添加到“受信任站点”列表。可以使用 IP 地址，也可以使用完全限定域名（如果可用，例如，inside.example.com）。也可以使用通配符或部分地址创建一个通用的受信任站点。例如，使用 *.example.com 或只是 example.com 通常可以覆盖所有内部站点，从而信任您网络中的所有服务器（使用您自己的域名）。如果添加接口的物理地址，可能需要将多个地址添加到受信任站点，从而涵盖用户对网络的所有接入点。
- 集成的 Windows 身份验证不通过代理服务器工作。因此，您要么不使用代理，要么必须将 Firepower 威胁防御接口添加到被排除在外而无法通过该代理的地址中。如果您决定必须使用代理，系统会提示用户进行身份验证，即使使用 NTLM 亦是如此。



提示 配置透明身份验证不是必须的，却可为终端用户提供方便。如果不配置透明身份验证，系统会向用户显示所有身份验证方法的登录挑战。

配置 Internet Explorer 以进行透明身份验证

要配置 Internet Explorer 以进行 NTLM 透明身份验证，请执行以下操作：

过程

步骤 1 依次选择工具 (Tools) > Internet 选项 (Internet Options)。

步骤 2 依次选择安全选项卡和本地 Intranet 区域，然后执行以下操作：

- a) 点击站点按钮，打开受信任站点列表。
- b) 确保至少选择以下其中一个选项：
 - 自动检测 Intranet 网络。如果选择此选项，系统将禁用其他所有选项。

- 包括所有不使用代理服务器的站点。

c) 点击高级打开“本地 Intranet 站点”对话框，然后将您要信任的站点添加到添加站点框中，然后点击添加。

如果您有多个 URL，请重复该过程。使用通配符指定部分 URL，例如 `http://*.example.com` 或只是 `*.example.com`。

关闭对话框返回到“Internet 选项” (Internet Options) 对话框。

d) 在本地 Intranet 仍处于选中状态的情况下，点击自定义级别打开“安全设置”对话框。找到用户身份验证 > 登录设置，然后选择只在 Intranet 区域自动登录。点击确定。

步骤 3 在“Internet 选项”对话框中，点击连接选项卡，然后点击 LAN 设置。

如果选中为 LAN 使用代理服务器，您需要确保 Firepower 威胁防御接口绕过该代理。适当执行以下任一操作：

- 选择对于本地地址不使用代理服务器。
- 点击高级并将地址输入对于以下列字符开头的地址不使用代理服务器框。您可以使用通配符，例如 `*.example.com`。

配置 Firefox 以进行透明身份验证

要配置 Firefox 进行 NTLM 透明身份验证，请执行以下操作：

过程

步骤 1 打开 `about:config`。借助过滤器栏找到您需要修改的首选项。

步骤 2 要支持 NTLM，请修改以下首选项（在 `network.automatic` 上过滤）：

- **network.automatic-ntlm-auth.trusted-uris** - 双击首选项，输入 URL，然后点击确定。您可以通过将 URL 以逗号分隔来输入多个 URL；包括该协议是可选的。例如：

```
http://host.example.com, http://hostname, myhost.example.com
```

您也可以使用部分 URL。Firefox 匹配该字符串的末尾，而不是一个随机子字符串。因此，您可以仅指定域名来包括您的整个内部网络。例如：

```
example.com
```

- **network.automatic-ntlm-auth.allow-proxies** - 确保值为 `true`，这是默认值。如果值当前为 `false`，请双击以更改该值。

步骤 3 检查 HTTP 代理设置。可以通过选择 **工具 > 选项**，然后点击“选项”对话框中的 **网络** 选项卡来查找这些设置。点击“连接”组中的 **设置** 按钮。

- 如果选择 **无代理**，则无需进行任何配置。
- 如果选择 **使用系统代理设置**，则需要修改 `about:config` 中的 `network.proxy.no_proxies_on` 属性，以添加您在 `network.automatic-ntlm-auth.trusted-uris` 中包括的可信赖 URI。
- 如果选择 **手动代理配置**，则更新 **无代理对象** 列表以包括这些可信赖的 URI。
- 如果选择其他某个选项，请确保用于这些配置的属不包括这些可信赖的 URI。

监控身份策略

如果要求身份验证的身份策略正常工作，您应该会在 **监控 > 用户** 控制面板和其他有用户信息的控制面板上看到用户信息。

此外，**监控 > 事件** 中显示的事件应该有用户信息。

如果没有看到任何用户信息，请验证目录服务器是否在正常运行。使用目录服务器配置对话框中的 **测试** 按钮验证连接。

如果目录服务器在正常运行并且可用，请验证要求主动身份验证的身份规则的流量匹配条件是否是以与您的用户匹配的方式编写的。例如，请确保源区域有用户流量进入设备的接口。主动身份验证身份规则仅与 **HTTP** 流量匹配，因此用户必须通过设备发送该类型的流量。

对于被动身份验证，使用 **ISE** 对象中的 **测试** 按钮，如果您在使用该源。如果您使用远程接入 **VPN**，请验证服务正常运行，并且用户可以进行 **VPN** 连接。有关识别和解决问题的更多详细信息，请参阅这些功能的故障排除主题。

身份策略示例

使用案例章节涵盖实施身份策略的示例。请参阅 [如何深入了解您的网络流量](#)，第 34 页。



第 14 章

安全情报

通过安全情报策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。以下主题介绍如何实施安全情报。

- [关于安全情报](#)，第 253 页
- [安全情报许可证要求](#)，第 254 页
- [配置安全情报](#)，第 255 页
- [监控安全情报](#)，第 256 页
- [安全情报示例](#)，第 256 页

关于安全情报

通过安全情报策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。在使用访问控制策略评估列入黑名单的流量前，系统会将其丢弃，从而减少系统资源的使用量。

您可以基于以下内容将流量列入黑名单：

- **思科 Talos 情报小组 (Talos) 源** - Talos 提供对定期更新的安全情报源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。系统定期下载情报源更新，从而提供新的威胁情报，而无需重新部署配置。



注释 Talos 默认情况下，源每小时更新一次。您可以从 **设备 > 更新** 页面更改更新频率，甚至根据需要更新情报源。

- **网络和 URL 对象** - 如果您知道要阻止的特定 IP 地址或 URL，则可为其创建对象并将其添加到黑名单（或例外列表，也称为白名单）。

创建用于 IP 地址（网络）和 URL 的单独黑名单。

黑名单例外

对于各黑名单，可创建关联的例外列表，也称之为白名单。例外列表的唯一目的是免除阻止出现在黑名单中的 IP 地址或 URL。也就是说，如果发现需使用且已知安全的地址或 URL 位于在黑名单上配置的情报源中，则可免除该网络/URL，而无需从黑名单中完全删除该类别。

随后通过访问控制策略评估被排除或列入白名单的流量。有关允许或丢弃连接的最终决定基于连接匹配的访问控制规则。访问规则还会决定恶意软件检查是否应用于连接。

安全情报源类别

下表介绍思科 Talos 情报小组 (Talos)源中的可用类别。这些类别可用于网络和 URL 黑名单。

表 7: Talos 源类别

类别	说明
攻击者	出站恶意活动已知的活动扫描工具和列入黑名单的主机。
bogon	Bogon 网络和未分配的 IP 地址。
僵尸	托管二进制恶意软件丢弃程序的站点。
CnC	托管僵尸网络的命令和控制服务器的站点。
dga	用于生成作为与命令和控制服务器的交汇点的大量域名的恶意软件算法。
exploitkit	指定用于识别客户端中的软件漏洞的软件包。
恶意软件	托管恶意软件二进制或漏洞包的站点。
open_proxy	允许匿名 Web 浏览的开放代理。
open_relay	已知用于垃圾邮件的开放邮件中继。
网络钓鱼	托管网络钓鱼页面的站点。
效率低下	主动参与恶意或可疑活动的 IP 地址和 URL。
垃圾邮件	已知用于发送垃圾邮件的邮件主机。
可疑	看似可疑并具有类似于已知恶意软件的特征的文件。
tor_exit_node	Tor 出口节点。

安全情报许可证要求

必须启用威胁许可证，才能使用安全情报。请参阅[启用或禁用可选许可证](#)，第 74 页。

配置安全情报

通过安全情报策略能够根据源/目标 IP 地址或目标 URL 提前丢弃非必要流量。所有允许的连接仍会通过访问控制策略进行评估，并且最终可能会被丢弃。必须启用威胁许可证，才能使用安全情报。

过程

步骤 1 依次选择策略 > 安全情报。

步骤 2 如果未启用策略，请点击启用安全情报按钮。

您可以通过点击安全情报开关切换到关闭随时禁用策略。配置将被保留，因此，当您再次启用该策略时，无需重新配置。

步骤 3 配置安全情报。

网络（IP 地址）和 URL 有单独的黑名单。

- a) 点击**网络**或**URL**选项卡显示要配置的黑名单。
- b) 在**黑名单**中，点击 +，选择要立即丢弃其连接的对象或情报源。

对象选择器按类型对单独选项卡上的对象和情报源进行分门别类。如果所需的对象尚不存在，请点击列表底部的**创建新对象**链接，立即创建对象。有关思科 Talos 情报小组 (Talos) 源的说明，请点击源旁边的 **i** 按钮。另请参阅[安全情报源类别](#)，第 254 页。

注释 安全情报会忽略使用 /0 掩码的 IP 地址块。这包括 any-ipv4 和 any-ipv6 网络对象。不得选择这些对象用于网络黑名单。

- c) 在**不阻止**列表中，点击 + 并选择黑名单的任何例外。

配置该列表的唯一原因是对黑名单中的 IP 地址或 URL 进行例外处理。被免除的连接随后将通过访问控制策略进行评估，且仍然可能会被丢弃。

- d) 重复此过程以配置其他黑名单。

步骤 4 （可选。）点击**编辑日志记录设置**按钮 (⚙️) 来配置日志记录。

如果启用了日志记录，系统会记录与黑名单条目的任意匹配项。系统不记录例外条目的匹配项，但如果被免除的连接与启用日志记录的访问控制规则匹配，您会收到日志消息。

配置以下设置：

- **连接事件日志记录** - 点击开关以启用或禁用日志记录。
- **系统日志** - 如果要将事件副本发送到外部系统日志服务器，请选择该选项并选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**添加系统日志服务器**并创建对象。

由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

监控安全情报

如果启用安全情报策略的日志记录，则系统生成各黑名单连接的安全情报事件。这些连接已有匹配的连接事件。

已丢弃黑名单连接的统计信息显示在“监控”页面上的各控制面板中。

监控 > 访问和 SI 规则控制面板显示排名靠前的访问规则及匹配流量的安全情报等效对象。

此外，可依次选择**监控 > 事件**，然后选择**安全情报**视图，查看安全情报事件以及**连接**选项卡上的相关连接事件。

- 事件中的 **SI 类别 ID** 字段指示黑名单中匹配的对象，如网络或 URL 对象或源。
- 连接事件中的“原因”字段解释为什么应用了事件中显示的操作。例如，与“IP阻止”或“URL阻止”等原因配对的“阻止”操作表示某连接已被安全情报列入黑名单并已被丢弃。

安全情报示例

使用案例章节涵盖实施安全情报策略的示例。请参阅[如何阻止威胁](#)，第 41 页。



第 15 章

访问控制

以下主题介绍访问控制规则。这些规则控制允许通过设备传递的流量，并会对流量应用入侵检测等高级服务。

- [访问控制概述，第 257 页](#)
- [访问控制许可证要求，第 264 页](#)
- [访问控制策略的准则与限制，第 264 页](#)
- [配置访问控制策略，第 266 页](#)
- [监控访问控制策略，第 275 页](#)
- [访问控制示例，第 276 页](#)

访问控制概述

以下主题介绍访问控制策略。

访问控制规则和默认操作

使用访问控制策略允许或阻止对网络资源的访问。该策略包含一系列有序的规则，按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件标准的第一个规则。

您可以根据以下条件控制访问：

- 传统网络特征，例如源和目的 IP 地址、协议、端口和接口（以安全区形式）。
- 源或目标（以网络对象形式）的完全限定域名 (FQDN)。流量匹配基于从 DNS 查询为该名称返回的 IP 地址。
- 正在使用的应用。您可以基于特定应用控制访问，也可以创建涵盖应用类别、标记特定特征的应用、应用类型（客户端、服务器、Web）或应用风险或业务相关性评级的规则。
- Web 请求的目的 URL，包括 URL 的通用类别。您可以基于目标站点的公共信誉优化类别匹配。
- 发出请求的用户或用户所属的用户组。

对于您允许的未加密流量，可以应用 IPS 检测来检查威胁并阻止看似攻击的流量。另外，您还可以使用文件策略来检查是否存在禁止文件或恶意软件。

与访问规则不匹配的流量由访问控制默认操作处理。默认情况下，如果允许流量，则可以对流量应用入侵检测。但您不能对默认操作处理的流量执行文件或恶意软件检测。

应用过滤

您可以使用访问控制规则基于连接中使用的应用过滤流量。系统会识别各种各样的应用，因此您不需要弄明白如何在阻止所有 Web 应用的情况下阻止某个 Web 应用。

对于一些常用的应用，您可以根据应用的不同方面进行过滤。例如，您可以创建一个阻止 Facebook 游戏但不阻止所有 Facebook 功能的规则。

您还可以基于一般应用特点创建规则，通过选择风险或业务关联性、类型、类别或标记来阻止或允许整组应用。但是，在应用过滤器中选择类别时，请查看匹配的应用列表，确保不包含非预期应用。有关可能分组的详细说明，请参阅[应用条件](#)，第 270 页。

已加密和已解密流量的应用控制

如果应用使用加密，系统可能无法识别该应用。

系统可以检测使用 StartTLS 加密的应用流量，包括 SMTPS、POP、FTPS、TelnetS 和 IMAPS。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书中的主题专有名称值来识别某些加密应用。

请使用应用过滤器对话框通过选择以下标记来确定应用是否需要解密，然后检查应用列表。

- **SSL 协议** - 不需要解密标记为“SSL 协议”的流量。系统可以识别此流量并应用您的访问控制操作。用于所列应用的访问控制规则应与预期的连接匹配。
- **解密流量** - 只有先解密流量，系统才能识别此流量。配置用于此流量的 SSL 解密规则。

应用过滤最佳实践

设计应用过滤访问控制规则时，请牢记以下建议。

- 要处理网络服务器所推荐的流量（例如广告流量），请匹配被推荐的应用（而非推荐应用）。
- 避免将应用与 URL 标准组合在同一规则中，尤其是对于加密流量。
- 如果要为标记为解密流量的流量编写规则，请确保具有解密匹配流量的 SSL 解密规则。仅可在解密连接中识别这些应用。
- 系统可以检测多个类型的 Skype 应用流量。要控制 Skype 流量，请从应用过滤器列表中选择 Skype 标记（而不是选择个别应用）。这确保系统可以相同方式检测和控制所有 Skype 流量。
- 要控制 Zoho 邮件访问，请选择 Zoho 和 Zoho 邮件应用。

URL 过滤

您可以使用访问控制规则基于 HTTP 或 HTTPS 连接中使用的 URL 过滤流量。请注意，HTTP 的 URL 过滤比 HTTPS 更直接，因为 HTTPS 会被加密。

您可以使用以下方法实施 URL 过滤：

- 基于类别和信誉的 URL 过滤 - 使用 URL 过滤许可证，您可以根据 URL 的一般分类（类别）和风险级别（信誉）控制对网站的访问。这是迄今为止阻止非必要网站的最简单、最有效的方法。
- 手动 URL 过滤 - 使用任何许可证均可手动指定各个 URL 和 URL 组，以便对网络流量实现精细的自定义控制。手动过滤的主要目的是创建基于类别的阻止规则的例外，但可以将手动规则用于其他目的。

以下主题提供了有关 URL 过滤的详细信息。

按照类别和信誉过滤 URL

通过 URL 过滤许可证，您可以基于所请求 URL 的类别和信誉控制对网站的访问：

- 类别 - URL 的一般分类。例如，[ebay.com](#) 属于“拍卖”类别，而 [monster.com](#) 属于“职位搜索”类别。URL 可以属于多个类别。
- 信誉 - URL 被用于可能违反组织安全策略之目的的可能性。范围可从“高风险”（第 1 级）到“知名”（第 5 级）。

URL 类别和信誉可帮助您快速配置 URL 过滤。例如，您可以使用访问规则阻止“滥用药物”类别中的高风险 URL。

使用类别和信誉数据还会简化策略创建和管理。代表安全威胁的站点或提供不良内容的站点的出现和消失速度，可能比您更新和部署新策略的速度要快。由于思科使用新站点、已更改分类与信誉更新 URL 数据库，因此，规则会自动调整以适应新信息。无需为新站点编辑规则。

如果启用常规 URL 数据库更新，则可确保系统使用最新信息进行 URL 过滤。还可启用与思科 综合安全情报 (CSI) 的通信，获取类别和信誉已知的 URL 的最新威胁情报。有关详细信息，请参阅[配置 URL 过滤首选项](#)，第 458 页。



注释 要查看事件和应用详细信息中的 URL 类别和信誉信息，必须至少创建一条具有 URL 标准的规则。

查找 URL 的类别和信誉

您可以通过以下网站检查特定 URL 的类别和信誉。您可以使用此信息，帮助您查看基于类别和信誉的 URL 过滤规则的表现。

<https://www.brightcloud.com/tools/url-ip-lookup.php>

手动 URL 过滤

您可以通过手动过滤各个 URL 或 URL 组，补充或选择性地覆盖基于类别和信誉的 URL 过滤。您可以在没有特殊许可证的情况下执行此类 URL 过滤。

例如，您可以使用访问控制阻止不适合于您组织的某类网站。但是，如果该类别包含适合的网站，且要为其提供访问权限，则可以为该站点创建手动“允许”规则，并将该规则置于适用于该类别的“阻止”规则前。

要配置手动 URL 过滤，请使用目标 URL 创建一个 URL 对象。基于如下规则解释该 URL：

- 如果不包含路径（即 URL 中无 / 字符），则匹配仅基于服务器主机名。如果主机名位于 `://` 分隔符之后，或在主机名中的任何点之后，则认为该主机名匹配。例如，`ign.com` 匹配 `ign.com` 和 `www.ign.com`，但不匹配 `verisign.com`。
- 如果包含一个或多个 / 字符，则整个 URL 字符串将用于子字符串匹配，其中包括服务器名称、路径和任何查询参数。但是，我们建议您不要使用手动 URL 过滤阻止或允许个别网页或部分网站，因为这样可能会重组服务器并将页面移至新路径。子字符串匹配还可能导致意外匹配，其中 URL 对象中包含的字符串也与非预期服务器上的路径或查询参数中的字符串匹配。
- 系统忽略加密协议（HTTP 与 HTTPS）。换句话说，如果阻止网站，系统将阻止发往该网站的 HTTP 和 HTTPS 流量，除非您使用一个应用条件指定特定协议。在创建 URL 对象时，您不需要指定创建对象时的协议。例如，使用 `example.com` 而不是 `http://example.com`。
- 如果您计划使用 URL 对象匹配访问控制规则中的 HTTPS 流量，请使用加密流量时所使用的公钥中的主题公用名创建该对象。此外，系统会忽略在主题公用名中的子域，因此，不包括子域信息。例如，使用 `example.com` 而不是 `www.example.com`。

但请注意，证书中的使用者公用名可能与网站的域名完全无关。例如，`youtube.com` 证书中的使用者公用名是 `*.google.com`（当然，这可能会随时更改）。如果使用 SSL 解密策略解密 HTTPS 流量以便 URL 过滤规则可用于解密策略，则可能获得更一致的结果。



注释 如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

过滤 HTTPS 流量

由于 HTTPS 流量加密，所以直接对 HTTPS 流量执行 URL 过滤并不像对 HTTP 流量执行 URL 过滤那样直接。因此，应考虑使用 SSL 解密策略解密想要过滤的所有 HTTPS 流量。这样，URL 过滤访问控制策略可有效用于解密流量，并会获得与常规 HTTP 流量相同的结果。

但是，如果打算允许某些 HTTPS 流量在未加密情况下通过访问控制策略，则需了解规则匹配 HTTPS 流量与匹配 HTTP 流量的方式不同。要过滤加密流量，系统将根据 SSL 握手期间传递的信息确定请求的 URL：用于加密流量的公钥证书中的主题公用名称。URL 中的网站主机名与使用者公用名之间可能没有多大关系。

HTTPS 过滤与 HTTP 过滤不同，它不考虑使用者公用名内的子域。手动过滤 HTTPS URL 时，请勿包含子域信息。例如，使用 `example.com` 而不是 `www.example.com`。此外，请查看站点所使用的证书内容，以确保使用者公用名中使用的域名正确，且该名称不会与其他规则冲突（例如，想要阻止的站点名称可能与想要允许的站点名称重叠）。例如，`youtube.com` 证书中的使用者公用名是 `*.google.com`（当然，这可能会随时更改）。



注释

如果由于证书信息不再可用，浏览器恢复 TLS 会话，则 URL 对象将不匹配 HTTPS 流量。因此，即使精心配置 URL 对象，也可能会得到不一致的 HTTPS 连接结果。

按加密协议控制流量

在执行 URL 过滤时，系统会忽略加密协议（HTTP 和 HTTPS）。对于手动 URL 标准和基于信誉的 URL 标准均会发生此情况。换句话说，URL 过滤以相同方式处理发送到以下网站的流量：

- `http://example.com`
- `https://example.com`

要配置仅匹配 HTTP 流量或 HTTPS 流量（而不是同时匹配这两种流量）的规则，请在“目标”条件中指定 TCP 端口或在规则中添加应用条件。例如，可以通过构造两个访问控制规则（各规则具有 TCP 端口或应用和 URL 标准）来允许对某个站点进行 HTTP 访问，同时禁止 HTTP 访问。

第一个规则允许 HTTPS 流量到达网站：

操作：允许
TCP 端口或应用：HTTPS（TCP 端口 443）
URL：example.com

第二个规则阻止对同一网站进行 HTTP 访问：

操作：阻止
TCP 端口或应用：HTTP（TCP 端口 80）
URL：example.com

比较 URL 和应用过滤

URL 和应用过滤具有许多相似之处。但应将其用于明显不同的目的：

- URL 过滤最好用于阻止或允许访问整个 Web 服务器。例如，如果不希望在网络上进行任何类型的赌博，则可创建用于阻止赌博类别的 URL 过滤规则。通过该规则，用户无法访问该类别内所有 Web 服务器上的任何页面。
- 应用过滤适用于阻止特定应用（无论托管站点如何），或阻止在其他方面受允许的其他网站的特定功能。例如，可以在不阻止所有 Facebook 功能的情况下阻止 Facebook 游戏应用。

由于组合应用与 URL 标准可能会导致非预期结果，尤其是对于加密流量，因此，分别创建用于 URL 和应用标准的单独规则是个好方法。如果需要将应用与 URL 标准合并到单个规则中，应将这些规则

直接置于仅应用或仅 URL 规则后，除非应用+URL 规则作为更一般的仅应用或仅 URL 规则的例外。由于 URL 过滤阻止规则比应用过滤阻止规则更广泛，因此，您应将其置于仅应用规则之上。

如果将应用标准与 URL 标准组合在一起，则可能需要更仔细地监控网络，以确保不允许访问不必要的站点和应用。

有效 URL 过滤的最佳实践

设计 URL 过滤访问控制规则时，请牢记以下建议。

- 尽可能使用类别和信誉阻止。这可以确保在将新站点添加到类别时自动将其阻止，且如果站点的信誉变得更佳（或更劣），则根据信誉对阻止情况进行调整。
- 使用 URL 类别匹配时，请注意，有时候站点登录页的类别与站点本身的类别不同。例如，Gmail 属于“基于 Web 的邮件”类别，而登录页面属于互联网门户类别。如果您为类别制定了包含不同操作的不同规则，可能会出现意想不到的结果。
- 使用 URL 对象定位整个网站，并对类别阻止规则进行例外处理。也就是说，允许特定网站（否则，该网站会被阻止于某个类别规则中）。
- 如果要手动阻止 Web 服务器（使用 URL 对象），则在安全情报策略中这样做更有效。评估访问控制规则前，安全情报策略丢弃连接，以便可获得更快、更有效的阻止。
- 为对 HTTPS 连接进行最有效的过滤，请使用 SSL 解密规则解密正在为其编写访问控制规则的流量。任何解密的 HTTPS 连接均会在访问控制策略中作为 HTTP 连接予以过滤，以避免 HTTPS 过滤的所有限制。
- 将 URL 阻止规则置于任何应用过滤规则前，因为 URL 过滤阻止整个 Web 服务器，而应用过滤将针对特定的应用使用，而不考虑 Web 服务器。

阻止网站时用户看到的内容

使用 URL 过滤规则阻止网站时，用户所看到的内容视该站点是否加密而异。

- HTTP 连接 - 用户会看到系统默认阻止响应页面，而不是为超时或重置连接而正常显示的浏览器页面。此页面将明确指示，您有意阻止了该连接。
- HTTPS（已加密）连接 - 用户不会看到系统默认阻止响应页面。相反，用户会看到浏览器显示安全连接故障的默认页面。错误消息不会指明该站点由于策略而被阻止。相反，错误可能显示为没有通用的加密算法。据此消息，无法明确看出是您有意阻止了该连接。

此外，网站可能是被属于非明示 URL 过滤规则的其他访问控制规则，甚至是被默认操作而阻止。例如，如果阻止整个网络或地理位置，也会阻止该网络或该地理位置的任何网站。受这些规则阻止的用户可能（也可能不能）得到以下限制中所述的响应页面。

如果实施 URL 过滤，请考虑向最终用户说明他们在站点被有意阻止时可能会看到的内容，以及您将阻止的站点类型。否则，他们可能会花费大量时间来解决受阻止的连接故障。

HTTP 响应页面的限制

当系统阻止网络流量时，并不总是显示 HTTP 响应页面。

- 如果网络流量由于提升的访问控制规则（放在前面的仅包含简单网络条件的阻止规则）被阻止，系统则不显示响应页面。
- 如果网络流量在系统识别请求的 URL 之前被阻止，则系统不显示响应页面。
- 对于被访问控制规则阻止的已加密连接，系统不会显示响应页面。

入侵、文件和恶意软件检测

入侵策略和文件策略共同发挥作用，作为允许流量到达其目的地之前的最后一道防线。

- 入侵策略监管系统的入侵防御功能。
- 文件策略监管系统的文件控制和适用于 Firepower 的 AMP 功能。

处理所有其他流量后，才会检验网络流量中是否存在入侵、禁止文件和恶意软件。通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。

您只能对允许流量的规则配置入侵策略和文件策略。对于设置为信任或阻止流量的规则，系统不会执行检测。此外，如果访问控制策略的默认操作是允许，则您可以配置入侵策略，但不能配置文件策略。

对由访问控制规则处理的任何单个连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检测。



注释

默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。检测仅适用于未加密的流量。

访问控制规则顺序最佳实践

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。请考虑以下建议：

- 特定规则应在一般规则之前，特别当特定规则是一般规则的例外时。
- 仅基于第 3/4 层标准丢弃流量的任何规则（如 IP 地址、安全区域和端口号）应尽早出现。我们建议这些规则应在需要检查的任何规则前，如具有应用或 URL 标准的规则，因为可快速评估第 3/4 层标准而无需检查。当然，这些规则的任何例外必须置于这些规则之上。
- 尽可能将特定丢弃规则置于策略顶部附近。这确保了对非预期流量尽可能做出最早的决定。
- 包括应用和 URL 标准的任何规则应直接位于仅应用或仅 URL 规则前，除非应用+URL 规则作为更一般仅应用或仅 URL 规则的例外。组合应用和 URL 标准可能会导致非预期结果，尤其是对于加密流量，因此，我们建议您尽可能创建单独的 URL 和应用过滤规则。

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)。

其他安全策略如何影响访问控制

其他安全策略可能影响访问控制规则的运行和对连接的匹配。配置访问规则时，请记住以下几点：

- **SSL 解密策略** - 访问控制前评估 SSL 解密规则。因此，如果加密连接与应用某类型解密的 SSL 解密规则相匹配，则该连接为通过访问控制策略评估的纯文本（解密）连接。访问规则无法查看加密版本的连接。此外，访问控制策略绝不会看到任何与丢弃流量的 SSL 解密规则相匹配的连接。最后，匹配“不解密”规则的任何加密连接将以其加密状态接受评估。
- **身份策略** - 仅当存在用于源 IP 地址的用户映射时，连接才与用户（以及用户组）匹配。侧重于用户或组成员关系的访问规则可能仅匹配身份策略成功收集的用户身份的那些连接。
- **安全情报策略** - 访问控制策略绝不会看到任何被列入黑名单和丢弃的连接。
- **VPN（站点间或远程访问）** - 始终根据访问控制策略对 VPN 流量进行评估，并根据匹配规则允许或丢弃连接。但在评估访问控制策略前，VPN 隧道本身将被解密。访问控制策略评估嵌入 VPN 隧道中的连接，而不是隧道本身。

访问控制许可证要求

使用访问控制策略无需特殊许可证。

但若使用访问控制策略中的特定功能，则需以下许可证。有关配置许可证的信息，请参阅[启用或禁用可选许可证](#)，第 74 页。

- **URL 过滤许可证** - 创建将 URL 类别和信誉作为匹配标准的规则。
- **威胁许可证** - 为访问规则或默认操作配置入侵策略。还需此许可证才可使用文件策略。
- **恶意软件许可证** - 在用于恶意软件控制的访问规则上配置文件策略。

访问控制策略的准则与限制

以下是访问控制的一些其他限制。请在评估是否会从规则中获取预期结果时考虑这些内容。

- **Firepower 设备管理器** 可以从目录服务器下载多达 2000 个用户的信息。如果您的目录服务器上有超过 2000 个用户账户，则在访问规则中选择用户时或查看基于用户的控制面板信息时，您不会看到所有可能的名称。您仅可以对已下载的名称编写规则。

此 2000 个用户的限制也适用于与组相关联的名称。如果组成员超过 2000 个，则只能将下载的 2000 个名称与组成员身份进行匹配。

- 如果漏洞数据库 (VDB) 更新删除 (弃用) 应用，则必须对使用已删除应用的任何访问控制规则或应用过滤器进行更改。修复这些规则前，您无法部署更改。此外，您无法在解决问题之前安装系统软件更新。在“应用过滤器对象”页面上或规则的“应用”选项卡上，这些应用应用名称后显示“(Deprecated)”。
- 要将完全限定域名 (FQDN) 网络对象用作源或目标条件，您还必须在 **设备 > 系统设置 > DNS 服务器** 上配置适用于数据接口的 DNS。系统不使用管理 DNS 服务器设置查找访问控制规则中使用的 FQDN 对象。有关排除 FQDN 解析问题的信息，请参阅 [常规 DNS 问题故障排除](#)，第 454 页。

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 应答可能具有欺骗性，因此只能使用完全受信任的内部 DNS 服务器。
- 某些 FQDN (尤其是对于非常受欢迎的服务器) 可以有多个且经常更改的 IP 地址。由于系统使用缓存 DNS 查询结果，用户可能会获得缓存中尚不存在的新地址。因此，通过 FQDN 阻止受欢迎站点可能会导致不一致的结果。
- 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。
- 如果编辑的规则正在使用中，所做的更改不会应用于 Snort 不再检查的已建连接。此新规则用于根据未来的连接进行匹配。此外，如果 Snort 当前正在检查连接，它可以将更改的匹配或操作条件应用于现有连接。如果您需要确保将所做的更改应用于当前的所有连接，您可以登录设备 CLI 并使用 **clear conn** 命令终止已建连接，但前提是，连接源稍后将尝试重新建立连接，并根据新规则进行相应匹配。
- 系统需要 3 至 5 个数据包才能识别连接中的应用或 URL。因此，正确的访问控制规则可能不会立即匹配给定连接。但是，一旦应用/URL 已知，系统会根据匹配规则处理连接。对于加密连接，这发生于 SSL 握手过程中的服务器证书交换之后。
- 对于在用于应用识别的连接中没有负载的数据包，系统会应用默认策略操作。
- 尽可能将匹配条件留空，尤其是安全区域、网络对象和端口对象的匹配条件。例如，如果仅将安全区域条件留空，而不是创建包含所有接口的区域，则系统可以更有效地匹配所有接口的流量。指定多个条件时，系统必须匹配您指定的条件内容的各组合。
- 由于内存限制，某些设备型号会使用一系列较小、欠精细的类别和信誉执行大部分 URL 过滤。例如，如果父 URL 的子站点具有不同的 URL 类别和信誉，某些设备可能仅存储父 URL 的数据。对于这些设备处理的 Web 网络流量，系统可能会执行云查找来确定本地数据库中不存在的站点的类别和信誉。内存较低的设备包括以下 ASA 型号：5508-X、5515-X、5516-X 以及 5525-X。

配置访问控制策略

使用访问控制策略可监控对网络资源的访问。该策略包含一系列有序的规则，按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件标准的第一个规则。如果没有匹配流量的规则，则应用页面底部显示的默认操作。

要配置访问控制策略，请依次选择**策略 > 访问控制**。

访问控制表将按顺序列出所有规则。对于每条规则：

- 点击最左列规则编号旁边的>按钮，可打开规则图表。图表可帮助您查看规则控制流量的方式。再次点击该按钮可关闭图表。
- 大多数单元格允许行内编辑。例如，您可以点击操作选择不同的操作，或者点击某个源网络对象以添加或更改源条件标准。
- 要移动规则，请将鼠标悬停在规则上，直到显示移动图标 (📏)，然后点击规则并将其拖放到新位置。您还可以通过编辑规则并在**顺序**列表中选择新位置来移动规则。一定要按您想要处理它们的顺序排列这些规则。特定规则应该靠近顶部，特别是定义一般规则例外情况的规则
- 最右列包含规则的操作按钮；将鼠标悬停在该单元格上可查看按钮。您可以编辑 (🔧) 或删除 (🗑️) 规则。

以下主题介绍如何配置策略。

配置默认操作

如果连接未匹配特定访问规则，则由访问控制策略的默认操作来处理该连接。

过程

步骤 1 依次选择**策略 > 访问控制**。

步骤 2 点击**默认操作**字段的任意位置。

步骤 3 选择应用于匹配流量的操作。

- **信任** - 允许流量，而无需进行任何类型的进一步检测。
- **允许** - 允许流量接受入侵策略检测。
- **阻止** - 无条件地丢弃流量。不检测流量。

步骤 4 如果操作为**允许**，请选择一条入侵策略。

有关策略选项的说明，请查看[入侵策略设置](#)，第 273 页。

步骤 5 (可选。) 针对默认操作配置日志记录。

要在控制面板数据或事件查看器中包括匹配默认操作的流量，必须对匹配默认操作的流量启用日志记录。请参阅[日志记录设置](#)，第 274 页。

步骤 6 单击 **OK**。

配置访问控制规则

使用访问控制规则可监控对网络资源的访问。访问控制策略中的规则按从上到下的顺序进行评估。对流量应用的规则是符合所有流量条件标准的第一个规则。

过程

步骤 1 依次选择策略 > 访问控制。

步骤 2 执行以下任一操作：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 (🔗)。

要删除不再需要的规则，请点击该规则的删除图标 (🗑️)。

步骤 3 在顺序中，选择要将该规则插入在已排序有序规则列表插入该规则的位置。

先匹配的规则先应用，所以您必须确保流量匹配条件标准较具体的规则显示在次之用来匹配流量的较通用条件标准的策略上方。

默认将规则添加到列表的末尾。如果以后要更改规则的位置，请编辑此选项。

步骤 4 在名称中输入规则的名称。

名称不能包含空格。可以使用字母数字字符和以下特殊字符：+ . _ -

步骤 5 选择应用于匹配流量的操作。

- 信任 - 允许流量，而无需进行任何类型的进一步检测。
- 允许 - 允许流量，不受策略中的入侵及其他检测设置约束。
- 阻止 - 无条件地丢弃流量。不检测流量。

步骤 6 使用以下选项卡的任意组合，定义流量匹配标准：

- 源/目标 - 通过其传输流量的安全区域（接口）、IP 地址或该 IP 地址的国家/地区或大陆（地理位置）或者流量中使用的协议和端口。默认设置为任何区域、地址、地理位置、协议和端口。请参阅[源/目标条件](#)，第 268 页。
- 应用 - 应用或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何应用。请参阅[应用条件](#)，第 270 页。
- URL - Web 请求的 URL 或 URL 类别。默认设置为任何 URL。请参阅[URL 标准](#)，第 271 页。
- 用户 - 用户或用户组。身份策略决定了用户和组的信息是否可用于流量匹配。只有配置身份策略，才能使用此条件标准。请参阅[用户条件](#)，第 272 页。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后在弹出对话框中点击**确定**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的 **x**，可将其从策略中移除。

向访问控制规则中添加条件时，请考虑以下提示：

- 您可以为每个规则配置多个条件。要使规则应用于流量，流量必须匹配该规则中的所有条件。例如，可以使用单一规则对特定主机或网络执行 URL 过滤。
- 最多可以为规则中的每个条件添加 50 个标准。匹配某个条件所有条件标准的流量满足该条件。例如，您可以使用单一规则为最多 50 个应用或应用过滤器执行应用控制。因此，单一条件中的项目之间为 OR 关系，但不同条件类型之间（例如，源/目的目标和应用之间）为 AND 关系。
- 有些功能需要您启用适当的许可证。

步骤 7（可选。）对于使用“允许”操作的策略，可以对未加密流量配置进一步的检测。点击以下任一链接：

- **入侵策略** - 依次选择**入侵策略 > 开**，然后选择入侵检测策略，可检测流量中是否存在入侵和漏洞。请参阅[入侵策略设置，第 273 页](#)。
- **文件策略** - 选择文件策略可检测流量中是否存在包含恶意软件的文件和应被阻止的文件。请参阅[文件策略设置，第 273 页](#)。

步骤 8（可选。）针对规则配置日志记录。

默认情况下，对于匹配规则的流量不会生成连接事件，但如果选择了文件策略，则默认生成文件事件。您可以更改此行为。要在控制面板数据或事件查看器中包括匹配策略的流量，必须对匹配策略的流量启用日志记录。请参阅[日志记录设置，第 274 页](#)。

无论匹配访问规则的日志记录配置如何，系统始终为设置为丢弃或发送警报的入侵规则生成入侵事件。

步骤 9 单击 **OK**。

源/目标条件

访问规则的“源/目标”标准定义通过其传递流量的安全区（接口）、IP 地址或 IP 地址的国家/地区或大洲（地理位置）或流量中使用的协议和端口。默认设置为任何区域、地址、地理位置、协议和端口。

要修改条件，请点击该条件内的 + 按钮，选择所需的对象或元素，然后点击**确定**。如果条件需要对象，而所需的对象不存在，您可以点击**创建新对象**。点击对象或元素对应的 **x**，可将其从策略中移除。

您可以通过以下标准来标识规则中要匹配的源和目的地。

源区域、目标区域

安全区对象，定义通过其传递流量的接口。可以定义一个或两个条件，也可以不定义任何条件：未指定的任何条件都将应用到任何接口上的流量。

- 要匹配从区域中的接口离开设备的流量，请将该区域添加至**目标区域**。
- 要匹配从区域中的接口进入设备的流量，请将该区域添加至**源区域**。
- 如果同时向一条规则添加源区域和目标区域条件，匹配流量必须源自其中一个指定源区域并通过其中一个目标区域流出。

如果应基于流量进入或离开设备的位置来应用规则，请使用此条件。例如，如果要确保到达内部主机的所有流量均进行入侵检测，则应将内部区域选为**目标区域**，同时将源区域保留为空。要在规则中实施入侵过滤，则规则操作必须为**允许**，并且必须在该规则中选择入侵策略。



注释 不能在同一规则中搭配使用被动和路由安全区域。此外，被动安全区域只能被指定为源区域，不能作为目标区域。

源网络、目标网络

定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请配置**源网络**。
- 要匹配流向 IP 地址或地理位置的流量，请配置**目标网络**。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目的 IP 地址的网络对象或组。您可以使用通过完全限定域名 (FQDN) 定义地址的对象；通过 DNS 查询确定地址。
- **地理位置** - 选择要基于流量的源或目的国家/地区或大陆控制流量的地理位置。选择大陆将会选择该大陆内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。



注释 为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

源端口、目标端口/协议

定义流量中所用协议的端口对象。对于 TCP/UDP，这可能包括端口。对于 ICMP，可包括代码和类型。

- 要匹配来自协议或端口的流量，请配置**源端口**。源端口只能为 TCP/UDP。
- 要匹配流向协议或端口的流量，请配置**目标端口/协议**。如果仅将目的地端口添加至条件，则可以添加使用不同传输协议的端口。ICMP 和其他非 TCP/UDP 规格仅可用于目的地端口，不允许用于源端口。

- 要同时匹配来自特定 TCP/UDP 端口的流量和流向特定 TCP/UDP 端口的流量，请配置源端口和目标端口。如果同时将源和目的端口添加至条件，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，您可以匹配从端口 TCP/80 流至端口 TCP/8080 的流量。

应用条件

访问规则的“应用”条件对 IP 连接中使用的应用进行定义，或按类型、类别、标记、风险或业务相关性定义应用的过滤器。默认设置为任何应用。

虽然您可以在规则中指定个别应用，但应用过滤器可简化策略创建和管理。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

另外，思科会通过系统和漏洞数据库 (VDB) 更新频繁更新和添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

您可以直接在规则指定应用和过滤器，也可以创建定义这些特征的应用过滤器对象。规格相当，尽管如果要创建复杂规则，使用对象可便于遵守每个条件 50 个项目的系统限制。

要修改应用和过滤器列表，请点击该条件内的 + 按钮，选择在单独选项卡中列出的相应应用或应用过滤器对象，然后在弹出对话框中点击**确定**。在任一选项卡中，您可以点击**高级过滤器**选择过滤器条件或帮助您搜索特定应用。点击应用、过滤器或对象的 **x**，可将其从策略中移除。点击**另存为过滤器**链接，可将尚不是对象的组合条件另存为新应用过滤器对象。



注释 如果所选应用已由 VDB 更新删除，则会在应用名称后显示“(Deprecated)”。必须从过滤器中删除这些应用，否则将阻止后续部署和系统软件升级。

您可以使用以下**高级过滤器**条件来标识规则中要匹配的应用或过滤器。这些元素与应用过滤器对象中使用的元素相同。



注释 单个过滤器条件中的多个选项具有 OR 关系。例如，风险高 OR 非常高。过滤器之间的关系是 AND，因此是风险高 OR 非常高，AND 业务相关性低 OR 非常低。在选择过滤器时，显示屏中的应用列表更新，只显示符合条件标准的应用。您可以使用这些过滤器来帮助查找要单独添加的应用，或确认是否要选择所需的过滤器以添加到规则中。

风险

应用所用的用途可能违反组织安全策略的可能性，从非常低到非常高。

业务相关性

在组织的业务运营环境下使用应用的可能性，与娱乐相对，从非常低到非常高。

类型

应用类型：

- **应用协议** - 应用协议（例如 HTTP 和 SSH），代表主机之间的通信。

- **客户端协议** - 客户端（例如 Web 浏览器和邮件客户端），代表主机上运行的软件。
- **Web 应用** - Web 应用（例如 MPEG 视频和 Facebook），代表 HTTP 流量的内容或请求的 URL。

类别

说明应用的最基本功能的应用通用分类。

标记

关于应用的其他信息，与类别类似。

对于加密流量，系统可以仅使用标记有 **SSL 协议** 的应用识别和过滤流量。只有在未加密或已解密的流量中才能检测到没有此标记的应用。此外，系统仅将 **已解密** 的流量标记分配给可在已解密的流量中检测到的应用，而不会将它们分配给加密或未加密的流量中检测到的应用。

应用列表（显示屏底部）

在从列表上方的选项中选择过滤器时，此列表将进行更新，所以您可查看当前符合过滤器的应用。在计划将过滤器条件添加到规则中时，使用此列表可确认您的过滤器是否针对所需的应用。如果您计划添加特定应用，请从此列表中选择它们。

URL 标准

访问规则中的 URL 标准对 Web 请求中使用的 URL 或请求的 URL 所属的类别进行定义。对于类别匹配，您还可以指定要允许或阻止的站点的相对信誉。默认设置为允许所有 URL。

URL 类别和信誉可供您快速创建访问控制规则的 URL 标准。例如，您可阻止所有赌博网站或高风险的社交网站。如果用户尝试浏览至任何包含该类别和信誉组合的 URL，会话将被阻止。

使用类别和信誉数据还会简化策略创建和管理。此方法可保证系统将按预期控制网络流量。最后，由于思科的威胁情报会不断更新有关新 URL 以及现有 URL 的新类别和新风险的信息，因此可以确保系统使用最新信息来过滤所请求的 URL。代表安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的恶意站点出现和消失的速度可能比您更新和部署新策略的速度要快。

要修改 URL 列表，请点击该条件内的 + 按钮，使用以下任一方法选择所需的类别或 URL。点击类别或对象的 **x**，可将其从策略中删除。

URL 选项卡

点击 +，选择 URL 对象或组，然后点击 **确定**。如果所需的对象不存在，可以点击 **创建新 URL**。



注释 在配置特定目标站点的 URL 对象之前，请仔细阅读有关手动 URL 过滤的信息。

“类别”选项卡

点击 +，选择所需的类别，然后点击 **确定**。

默认为将规则应用于每个选定类别的所有 URL，不考虑信誉。要根据信誉限制规则，请点击每个类别的向下箭头，取消选中任何复选框，然后使用 **信誉滑块** 选择信誉级别。信誉滑块的左侧指示要允许的站点，右侧是要阻止的站点。如何使用信誉取决于规则操作：

- 如果该规则阻止或监控网络访问，则选择某个信誉级别也会选择高于该级别的所有信誉。例如，如果将规则配置为阻止或监控**可疑站点**（第 2 级），该规则还会自动阻止或监控**高风险**（第 1 级）站点。
- 如果该规则允许网络访问，则选择某个信誉级别也会选择低于该级别的所有信誉。例如，如果您将规则配置为允许**良性站点**（第 4 级），该规则还会自动允许**已知**（第 5 级）站点。

用户条件

访问规则的“用户”条件对 IP 连接的用户或用户组进行了定义。只有配置身份策略和相关联的目录服务器，才能在访问规则中包括用户或用户组条件。

您的身份策略决定是否收集某个特定连接的用户身份。如果建立了身份，则主机的 IP 地址与所识别的用户相关联。因此，源 IP 地址映射到用户的流量将被视为来自该用户。IP 数据包本身不包含用户身份信息，所以此 IP 地址到用户的映射是最接近的近似值。

由于最多可以向规则中添加 50 个用户或群组，所以选择群组比选择单个用户通常更有意义。例如，您可以创建一条规则允许“工程”组访问开发网络，并创建一条后续规则拒绝对该网络的所有其他访问。然后，要将该规则应用于新工程师，您只需添加将工程师添加到目录服务器的“工程”组即可。

要修改用户列表，请点击该条件内的 + 按钮，并使用以下任一方法选择所需的身份。点击身份对应的 **x**，可将其从策略中删除。

- **用户和组**选项卡 - 选择所需的用户或用户组。只有在目录服务器中配置了群组，才能使用群组。如果您选择了某个群组，规则将应用于该群组的所有成员，包括子组。如果要区别对待某个子组，您需要针对该子组创建一条单独的访问规则，并将其置于访问控制策略中适用于父组的规则之上。
- **特殊实体**选项卡 - 从以下项目中选择：
 - **身份验证失败** - 系统提示用户进行身份验证，但用户未在允许的最大尝试次数内输入有效的用户名/密码对。身份验证失败本身不会阻止用户访问网络，但您可以写入访问规则来限制这些用户访问网络。
 - **访客** - “访客”用户与“身份验证失败”用户类似，只是您的身份规则配置为将这些用户称为“访客”。系统提示“访客”(Guest) 用户进行身份验证，但他们在最大尝试次数内未成功通过身份验证。
 - **无需身份验证** - 系统不提示用户进行身份验证，因为该类用户的连接与指定不进行身份验证的身份规则匹配。
 - **未知** - 没有用户的 IP 地址映射，也没有身份验证失败的记录。通常，这意味着尚无来自该地址的 HTTP 流量。

入侵策略设置

思科通过 Firepower 系统提供多种入侵策略。这些策略由思科 Talos 情报小组 (Talos) 设计，其设定了入侵和预处理器规则的状态和高级设置。您不能修改这些策略。不过，您可以更改要对给定规则执行的操作，如[更改入侵规则操作](#)，第 287 页中所述。

对于允许流量的访问控制规则，您可以选择以下任一入侵策略来检测流量中是否存在入侵和攻击程序。入侵策略根据模式检查已解码数据包中是否存在攻击，并且可以阻止或修改恶意流量。

要启用入侵检测，请选择**入侵策略 > 开**，然后选择所需策略。策略将按安全性由低到高列出。

- **连接优先于安全性** - 此策略适用于连接（即确保能够获取所有资源）优先于网络基础设施安全性的组织。此入侵策略启用的规则远远少于“安全性优先于连接”策略中启用的规则。仅会启用阻止流量的最重要规则。如果要应用某些入侵保护，但对网络的安全性相当自信，可选择此策略。
- **平衡安全和连接** - 此策略用于平衡整体网络性能和网络基础设施安全性。此策略适合大多数网络。对于要应用入侵防御的大多数情况，可选择此策略。
- **安全性优先于连接** - 此策略适用于网络基础设施安全性优先于用户便利性的组织。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。如果安全性至上或针对高风险流量，可选择此策略。
- **最大检测** - 此策略适用于网络基础设施安全性比在“安全性优先于连接”策略中还要重要、有可能产生更大运营影响的组织。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。如果选择此策略，请仔细评估是否要丢弃过多的合法流量。

文件策略设置

借助适用于 Firepower 的高级恶意软件保护（适用于 Firepower 的 AMP），可使用文件策略检测恶意软件（或恶意软件）。另外，您还可以使用文件策略执行文件控制，以允许控制特定类型的所有文件，而不考虑文件中是否包含恶意软件。

适用于 Firepower 的 AMP 使用 AMP 云检索网络流量中检测到的潜在恶意软件的处置，并获取本地恶意软件分析和文件预分类更新。管理接口必须可连接互联网，以便访问 AMP 云并搜索恶意软件。当设备检测到符合条件的文件时，它将使用该文件的 SHA-256 散列值来查询 AMP 云中是否存在该文件的处置。可能的处置包括：

- **恶意软件** - AMP 云将文件归类为恶意软件。如果其中的任何文件为恶意软件，存档文件（例如 zip 文件）会被标记为恶意软件。
- **安全** - AMP 云将文件归类为安全，不含恶意软件。如果其中的所有文件都安全，存档文件将会标记为安全。
- **未知** - AMP 云尚未指定该文件的处置。如果其中的任何文件属于未知状态，存档文件会被标记为未知。
- **不可用** - 系统无法通过查询 AMP 云来确定文件的处置。您可能看到很少一部分事件为此处置；这是预期行为。如果您连续看到许多“不可用”事件，请确保管理地址的互联网连接正常运行。

可用的文件策略

您可以选择下列文件策略之一：

- **无** - 不评估传输的文件中是否存在恶意软件，且不止特定的文件。对于文件传输受信任或不可能传输文件的规则或您相信自己的应用或URL过滤可适当保护网络的规则，请选择此选项。
- **阻止所有恶意软件** - 查询 AMP 云以确定通过网络传输的文件是否包含恶意软件，然后阻止存在威胁的文件。
- **全部执行云查找** - 查询 AMP 云以获取和记录通过网络传输的文件的处置，同时仍允许文件传输。
- **阻止 Office 文档和 PDF 上传、阻止其他恶意软件** - 阻止用户上传 Microsoft Office 文档和 PDF。此外，查询 AMP 云以确定遍历网络的文件是否包含恶意软件，然后阻止存在威胁的文件。
- **阻止 Office 文档上传、阻止其他恶意软件** - 阻止用户上传 Microsoft Office 文档。此外，查询 AMP 云以确定遍历网络的文件是否包含恶意软件，然后阻止存在威胁的文件。

日志记录设置

访问规则的日志记录设置确定是否对匹配规则的流量发出连接事件。只有启用日志记录，才能在事件查看器中查看与该规则相关的事件。另外，您还必须启用日志记录，才能使匹配流量反映到可用于监控系统的各种控制面板中。

您应该根据贵组织的安全和合规性需求记录连接。如果您的目标是限制所生成事件的数量和提高性能，则只能启用对分析至关重要的连接的日志记录。然而，如果出于分析目的，您想要广泛了解网络流量，则可启用其他连接的日志记录。



注意

在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。在对“阻止”规则启用日志记录之前，请考虑该规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口。

您可以配置以下日志记录操作。

选择日志操作

可以选择下列操作之一：

- **在连接开始和结束时记录** - 在连接开始和结束时发出事件。由于连接结束事件包含连接开始事件所含的一切，以及连接期间可能收集的所有信息，所以思科建议不要对允许的流量选择此选项。记录两种事件可能会影响系统性能。但是，这是针对阻止的流量唯一允许的选项。
- **在连接结束时记录** - 如果要在连接结束时启用连接日志记录（建议对允许或受信任的流量执行此操作），请选择此选项。
- **在连接时不执行日志记录** - 选择此选项，可对规则禁用日志记录。这是默认值。



注释 当访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，系统会在发生入侵的位置自动记录连接终止，无论该规则的日志记录配置如何。对于入侵受阻的连接，连接日志中的连接操作作为**阻止**，原因为**入侵阻止**，即使执行入侵检测，也必须使用“允许”规则。

文件事件

如果要对禁止文件或恶意软件事件启用日志记录，请选择**日志文件**。只有在规则中选择了文件策略，才能配置此选项。如果对规则选择了文件策略，则该选项默认处于启用状态。思科建议您将此选项保留为已启用。

当系统检测到受禁文件时，它会自动记录以下类型的事件之一：

- 文件事件，代表检测到或阻止的文件，包括恶意软件文件。
- 恶意软件事件，仅代表检测到或阻止的恶意软件文件。
- 可追溯的恶意软件事件，在之前检测到的文件的恶意软件处置变更时生成。

对于文件受阻的连接，连接记录中的连接操作为**Block**，即便要执行文件和恶意软件检测，也必须使用“允许”规则。连接原因是**文件监控**（检测到某种文件类型或恶意软件）或者是**恶意软件阻止**或**文件阻止**（文件被阻止）。

将连接事件发送到

如果要将事件副本发送到外部系统日志服务器，请选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建新系统日志服务器**，并创建对象。（要对系统日志服务器禁用日志记录，请从服务器列表中选择任何）。

由于设备中的事件存储受限，所以将事件发送至外部系统日志服务器可供长期存储，并增强您的事件分析。

监控访问控制策略

以下主题介绍如何监控访问控制策略。

在控制面板中监控访问控制统计信息

监控控制面板上的大多数数据与您的访问控制策略直接相关。请参阅[监控流量和系统控制面板](#)，第 82 页。

- **监控 > 访问和 SI 规则** 显示点击量最高的访问规则及安全情报规则等效对象和相关统计信息。
- 可以在**网络概述**、**目标**和**区域**控制面板找到常规统计信息。
- 可以在**URL 类别**和**目标**控制面板找到 URL 过滤结果。必须至少有一个 URL 过滤策略，才可在**URL 类别**控制面板看到任何信息。
- 可以在**应用**和**Web 应用**控制面板找到应用过滤结果。

- 还可以在用户控制面板找到基于用户的统计信息。只有实施身份策略才能收集用户信息。
- 可以在攻击者和目标控制面板找到入侵策略统计信息。必须将入侵策略应用于至少一个访问控制规则，才能在這些控制面板上看到任何信息。
- 可以在文件日志和恶意软件控制面板找到文件策略和恶意软件过滤统计信息。必须将文件策略应用于至少一个访问控制规则，才能在這些控制面板上看到任何信息。
- 监控 > 事件还显示与访问控制规则相关的连接和数据的事件。

监控访问控制系统日志消息

除了在事件查看器中查看事件外，您还可以配置访问控制规则、入侵策略、和安全情报策略，以将事件发送到系统日志服务器。事件使用以下消息 ID：

- 430001 - 入侵事件。
- 430002 - 连接开始时记录的连接事件。
- 430003 - 在连接结束时记录的连接事件。

在 CLI 中监控访问控制策略

您还可以打开 CLI 控制台或登录设备 CLI，使用以下命令获取有关访问控制策略和统计信息的更多详细信息。

- **show access-control-config** 显示访问控制规则的摘要信息以及每个规则的命中计数点击数。
- **show access-list** 显示基于访问控制规则生成的访问控制列表 (ACL)。ACL 提供初始过滤器并尝试尽可能提供快速决策，以使应丢弃的连接不需要接受检测（从而避免不必要的资源消耗）。此信息包括命中计数。
- **show snort statistics** 显示 Snort 检测引擎（主要检测程序）的相关信息。Snort 实施应用过滤、URL 过滤、入侵防护以及文件和恶意软件过滤。
- **show conn** 显示当前通过接口建立的连接的相关信息。
- **show traffic** 显示流过每个接口的流量的相关统计信息。
- **show ipv6 traffic** 显示流过设备的 IPv6 流量的相关统计信息。

访问控制示例

使用案例章节涵盖多个实施访问控制规则的示例。请参阅下面的示例：

- [如何深入了解您的网络流量](#)，第 34 页。此示例展示收集整体的连接和用户信息的一些基本概念。

- [如何阻止威胁，第 41 页](#)。此示例展示如何应用入侵策略。
- [如何阻止恶意软件，第 47 页](#)。此示例展示如何应用文件策略。
- [如何实施可接受使用策略（URL 过滤），第 50 页](#)。此示例展示如何执行 URL 过滤。
- [如何控制应用使用情况，第 54 页](#)。此示例展示如何执行应用过滤。
- [如何添加子网，第 57 页](#)。此示例展示如何将新的子网集成到整个网络，包括允许流量所需的访问规则。
- [如何被动监控网络上的流量，第 62 页](#)



第 16 章

入侵策略

以下主题说明了入侵策略和密切相关的网络分析策略 (NAP)。入侵策略包括用于检查流量中的威胁并阻止看似为攻击的流量的规则。网络分析策略控制流量预处理，通过规范化流量和识别协议异常来准备要进一步检查的流量。

由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略必须相互补充。

- [关于入侵和网络分析策略，第 279 页](#)
- [入侵策略的许可证要求，第 286 页](#)
- [管理入侵策略，第 286 页](#)
- [监控入侵策略，第 289 页](#)
- [入侵策略示例，第 289 页](#)

关于入侵和网络分析策略

网络分析和入侵策略协同工作检测和防止入侵威胁。

- 网络分析策略 (NAP) 监管流量如何解码和预处理，以便可以进一步对其进行评估，尤其是对于可能指示入侵尝试的异常流量。
- 入侵策略使用入侵和预处理器规则（统称为入侵规则），根据模式检测已解码数据包是否存在攻击。入侵规则可防止（丢弃）有威胁的流量并生成事件，或直接检测（警告）有威胁流量并仅生成事件。

在系统分析流量时，进行解码和预处理的网络分析阶段发生在入侵防御阶段之前并与其分隔开来。网络分析和入侵策略共同提供广泛且深入的数据包检测。它们可以帮助您检测、提醒和防范可能威胁主机及其数据的可用性、完整性和保密性的网络流量。

系统定义的网络分析和入侵策略

系统包括几对相辅相成的同名网络分析和入侵策略。例如，名称同为“平衡安全和连接”的 NAP 策略和入侵策略要一起使用。系统提供的策略由思科 Talos 情报小组 (Talos) 配置。对于这些策略，Talos 设置入侵和预处理器规则状态，并提供预处理器和其他高级设置的初始配置。

随着新的漏洞被发现，Talos 会发布入侵规则更新。这些规则更新可以修改系统提供的任何网络分析或入侵策略，并且可以提供新的和已更新的入侵规则及预处理器规则、现有规则的已修改状态，以及已修改的默认策略设置。规则更新还可以从系统提供的策略中删除规则，并且提供新规则类别，以及修改默认变量集。

您可以手动更新规则数据库，或配置定期更新计划。更新必须部署，才能生效。有关更新系统数据库的更多信息，请参阅[更新系统数据库](#)，第 464 页。

以下是系统提供的策略：

“平衡安全和连接”网络分析和入侵策略

这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数网络和部署类型的良好起点。系统默认使用“平衡安全和连接”网络分析策略。

“连接优先于安全”网络分析和入侵策略

这些策略专为连接性（能够获取所有资源）优先于网络基础设施安全性的网络而构建。此入侵策略启用的规则远远少于“安全性优先于连接”策略中启用的规则。仅会启用阻止流量的最重要规则。

“安全优先于连接”网络分析和入侵策略

这些策略专为网络基础设施安全优先于用户便利性的网络而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。

“最大检测” (Maximum Detection) 网络分析和入侵策略

此类策略适用于网络基础设施安全比在“安全优先于连接”策略中还要重要、且有可能产生更大运行影响的网络。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。

入侵和预处理器规则

入侵规则是系统用于检测利用网络漏洞企图的一组指定关键字和参数。当系统分析网络流量时，它将数据包与每个规则中指定的条件相比较，并在数据包满足规则中指定的所有条件的情况下触发规则。

系统包含思科 Talos 情报小组 (Talos) 创建的以下类型的规则：

- 入侵规则，可细分为共享对象规则和标准文本规则
- 预处理器规则，是指与网络分析策略中的预处理器和数据包解码器检测选项关联的规则。默认情况下禁用大多数预处理器规则。

以下主题更深入地介绍入侵规则。

入侵规则属性

依次选择**策略 > 入侵**，可看到的用于识别威胁的所有入侵规则列表。在表的上方，可以点击入侵策略的名称来查看每个策略的规则。

各策略的规则列表仅显示设置为发出警报或丢弃的规则以及显式禁用的规则，不显示默认禁用的规则。虽然有3万多条规则，但您只会看到所有可能的规则的子集。但即使对于最小的已启用规则集，滚动列表也需要时间。滚动时会显示规则。

以下是定义每个规则的属性：

> (签名说明)

点击左列的 > 按钮可打开签名说明。说明内容是 Snort 检测引擎用来根据规则匹配流量的实际代码。代码介绍不在本文范围之内，有关详细信息，请参阅《Firepower 管理中心配置指南》；请从 <http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html> 中选择适合您的软件版本的书籍。查找入侵规则编辑的相关信息。

签名包含某些项目的变量。有关详细信息，请参阅默认入侵变量集，第 281 页。

GID

生成器标识符 (ID)。此数字指示评估规则并生成事件的系统组件。1 表示标准文本入侵规则，3 表示共享对象入侵规则。（对于 Firepower 设备管理器用户，这些规则类型差异没有意义）。这些是在配置入侵策略时主要关注的规则。有关其他 GID 的信息，请参阅生成器标识符，第 282 页。

SID

Snort 标识符 (ID)，也称为签名 ID。低于 1000000 的 Snort ID 由思科 Talos 情报小组 (Talos) 创建。

操作

此规则在所选入侵策略中的状态。此策略内每个规则的默认操作后面会添加“（默认）”。要使规则返回其默认设置，请选择此操作。可能的操作包括：

- **警报** - 当此规则与流量匹配时，创建一个事件但不丢弃连接。
- **丢弃** - 当此规则与流量匹配时，创建一个事件同时丢弃连接。
- **禁用** - 不针对此规则匹配流量。不生成事件。

状态

如果更改规则的默认操作，此列将显示“已覆盖”。否则，该列为空。

消息

这是规则的名称，规则触发的事件中也会显示该名称。消息通常标识签名匹配的威胁。通过互联网可搜索每个威胁的详细信息。

默认入侵变量集

入侵规则签名包含某些项目的变量。以下是这些变量的默认值，其中最常用的变量是 \$HOME_NET 和 \$EXTERNAL_NET。请注意，协议与端口号分开指定，所以端口变量只是数字。

- \$AIM_SERVERS = 网络或主机的 20 个地址：64.12.24.0/23、64.12.28.0/23、64.12.31.136、64.12.46.140、64.12.161.0/24、64.12.163.0/24、64.12.186.85、64.12.200.0/24、205.188.1.132、

205.188.3.0/24、205.188.5.0/24、205.188.7.0/24、205.188.9.0/24、205.188.11.228、205.188.11.253、205.188.11.254、205.188.153.0/24、205.188.179.0/24、205.188.210.203、205.188.248.0/24。

- \$DNS_SERVERS = \$HOME_NET（表示任何 IP 地址）。
- \$EXTERNAL_NET = 任何 IP 地址。
- \$FILE_DATA_PORTS = \$HTTP_PORTS、143、110。
- \$FTP_PORTS = 21、2100、3535。
- \$GTP_PORTS = 3386、2123、2152。
- \$HOME_NET = 任何 IP 地址。
- \$HTTP_PORTS = 144 个端口号：36、80-90、311、383、443、555、591、593、631、666、801、808、818、901、972、1158、1212、1220、1414、1422、1533、1741、1830、1942、2231、2301、2381、2578、2809、2980、3029、3037、3057、3128、3443、3507、3702、4000、4343、4848、5000、5117、5222、5250、5450、5600、5814、6080、6173、6767、6988、7000、7001、7005、7071、7080、7144、7145、7510、7770、7777-7779、8000、8001、8008、8014、8015、8020、8028、8040、8060、8080-8082、8085、8088、8118、8123、8161、8180-8182、8222、8243、8280、8300、8333、8344、8400、8443、8500、8509、8787、8800、8888、8899、8983、9000、9002、9060、9080、9090、9091、9111、9290、9443、9447、9710、9788、9999、10000、11371、12601、13014、15489、19980、23472、29991、33300、34412、34443、34444、40007、41080、44449、50000、50002、51423、53331、55252、55555、56712。
- \$HTTP_SERVERS = \$HOME_NET（表示任何 IP 地址）。
- \$ORACLE_PORTS = 任意
- \$SHELLCODE_PORTS = 180。
- \$SIP_PORTS = 5060、5061、5600
- \$SIP_SERVERS = \$HOME_NET（表示任何 IP 地址）。
- \$SMTP_SERVERS = \$HOME_NET（表示任何 IP 地址）。
- \$SNMP_SERVERS = \$HOME_NET（表示任何 IP 地址）。
- \$SQL_SERVERS = \$HOME_NET（表示任何 IP 地址）。
- \$SSH_PORTS = 22。
- \$SSH_SERVERS = \$HOME_NET（表示任何 IP 地址）。
- \$TELNET_SERVERS = \$HOME_NET（表示任何 IP 地址）。

生成器标识符

生成器标识符 (GID) 标识评估入侵规则并生成事件的子系统。标准文本入侵规则的生成器 ID 为 1，共享对象入侵规则的生成器 ID 为 3。对于各种预处理器也有几套规则。下表解释了 GID。

表 8: 生成器 ID

ID	组件
1	标准文本规则。
2	标记的数据包。 (标记生成器规则, 根据标记会话生成数据包。)
3	共享对象规则。
102	HTTP 解码器。
105	Back Orifice 检测器。
106	RPC 解码器。
116	数据包解码器。
119、120	HTTP 检查预处理器。 (GID 120 规则与服务器特定 HTTP 流量相关。)
122	Portscan 检测器。
123	IP 分片重组器。
124	SMTP 解码器。 (针对 SMTP 动词的攻击)
125	FTP 解码器。
126	Telnet 解码器。
128	SSH 预处理器。
129	流预处理器。
131	DNS 预处理器。
133	DCE/RPC 预处理器。
134	规则延迟, 数据包延迟。 (规则延迟暂停 (SID 1) 或重新启用 (SID 2) 一组入侵规则, 或系统由于超出数据包延迟阈值 (SID 3) 而停止检查数据包时, 生成这些规则的事件。)
135	基于速率的攻击检测器。 (与网络上主机的连接过多。)
137	SSL 预处理器。

ID	组件
138、139	敏感数据预处理器。
140	SIP 预处理器。
141	IMAP 预处理器。
142	POP 预处理器。
143	GTP 预处理器。
144 个	Modbus 预处理器。
145	DNP3 预处理器。

网络分析策略

网络分析策略控制流量预处理。预处理器通过规范化流量和标识协议异常，准备要进行进一步检查的流量。网络分析相关预处理发生在安全情报黑名单和 SSL 解密之后进行，但在访问控制和入侵或文件检查开始之前进行。

默认情况下，系统使用“平衡安全和连接”网络分析策略预处理器由访问控制策略处理的所有流量。但是，系统根据您在访问控制规则中选择的入侵策略应用不同的网络分析策略。

系统尝试匹配入侵和网络分析策略，以便获得最佳处理。但是，网络分析策略 (NAP) 规则不具有访问控制规则中可用的相同流量匹配标准，因此，如果不遵循建议的准则，则可能得到不匹配的策略。

系统如何使用 NAP 规则选择网络分析策略

无法直接分配网络分析策略。相反，系统根据在访问控制规则中分配的入侵策略自动生成 NAP 规则。

NAP 规则仅基于安全区域和网络规范。因此，对于包含入侵策略的各访问控制规则，系统创建将同名网络分析策略应用于源/目标安全区域和网络的 NAP 规则。忽略端口、URL、用户和应用标准。

这是一个重要区别：虽然可根据第 4 层或第 7 层标准（如端口、应用或 URL）应用不同入侵策略，但这些较高层次的条件对于网络分析策略的选择并无影响。

系统会按照与访问控制规则相同的顺序排列 NAP 规则。系统使用第一个匹配 NAP 规则确定要应用的网络分析策略。

因此，如果有多个访问控制规则允许相同源/目标区域和网络对象组合的流量，但在其他流量匹配标准上有所不同，则系统生成多个重叠的 NAP 规则，但第二个和随后的重复规则绝不会匹配流量。如果将不同入侵策略应用于这些“重叠”规则，则至少有一些流量会不匹配入侵策略和网络分析策略。

例如，请考虑以下规则：

1. 访问规则 1

操作：允许

源区域: `inside_zone`
源网络: 任何
目的区域: `outside_zone`
目的网络: 任何
URL 类别: 社交网络
入侵策略: 安全优先于连接

2. 访问规则 2

操作: 允许
源区域: `inside_zone`
源网络: 任何
目的区域: `outside_zone`
目的网络: 任何
入侵策略: 平衡安全和连接

在这种情况下, 将会有两个 NAP 规则:

1. NAP 规则 1

源区域: `inside_zone`
源网络: 任何
目的区域: `outside_zone`
目的网络: 任何
网络分析策略: 安全优先于连接

2. NAP 规则 2

源区域: `inside_zone`
源网络: 任何
目的区域: `outside_zone`
目的网络: 任何
网络分析策略: 平衡安全和连接

由于两个 NAP 规则具有相同的匹配标准, 系统会将“安全优先于连接”网络分析策略应用于与访问控制规则 1 或 2 匹配的任何流量。但是, 大多数流量将匹配访问控制规则 2, 并使用“平衡”入侵策略。因此, 任何匹配访问控制规则 2 的流量将会不匹配 NAP 和入侵策略。



注释

如果在访问控制策略中使用单一入侵策略, 则系统仅将同名的网络分析策略设为默认策略, 且不会生成 NAP 规则。否则, 系统会将“平衡”策略设为默认的网络分析策略。无其他 NAP 规则适用时, 默认策略适用, 这通常适用于尚未为其分配入侵策略的区域和网络组合。

关于应用入侵策略优化 NAP 处理的最佳实践

决定如何分配策略以确保获取匹配的网络分析策略时, 请考虑以下建议:

- 如果始终使用相同的入侵策略，则将同名网络分析策略设为默认策略，并始终获得匹配的入侵和网络分析策略。
- 如果确定需将不同入侵策略用于特定流量，请始终将相同的入侵策略用于相同的源/目标安全区域和网络对象组合。这将确保 NAP 规则为所有相关联的访问控制规则分配同名的网络分析策略。

例如，如果确定需将“安全优先于连接”策略用于 `network_one` 的某些 `inside_zone` 至 `outside_zone` 流量，请将“安全优先于连接”策略分配给具有相同源/目标区域和网络规范的各访问控制规则。

入侵策略的许可证要求

只有启用**威胁**许可证，才能在访问控制规则中应用入侵策略。有关配置许可证的信息，请参阅[启用或禁用可选许可证](#)，第 74 页。

网络分析策略无需额外的许可证。

管理入侵策略

使用 Firepower 设备管理器，您可以应用预定义的任何入侵策略。其中每个策略包含相同的入侵规则（也称为签名）列表，但针对每个规则所采取的操作有所不同。例如，一条规则在某个策略中可能处于活动状态，但在另一个策略中可能被禁用。

如果您发现某个特定规则为您提供的误报过多，在这种情况下该规则会阻止您不希望阻止的流量，可以禁用该规则而不必切换到安全性较低的入侵策略。也可将其更改为匹配警告，而不丢弃流量。

但是，如果在入侵策略中默认禁用规则，则无法将其更改为丢弃或警告匹配的流量。仅可在已启用或先前禁用的策略上更改操作。

使用与入侵相关的控制面板和事件查看器（两者均在[监控](#)页面）可评估入侵规则对流量的影响。请记住，仅将匹配入侵规则的流量设为警告或丢弃时，才会看到入侵事件和入侵数据；系统不评估禁用的规则。

以下主题详细介绍入侵策略和规则调整。

在访问控制规则中应用入侵策略

要将入侵策略应用于网络流量，请在允许流量的访问控制规则中选择该策略。不得直接分配入侵策略。

可以根据所保护网络的相对风险分配不同的入侵策略，以提供可变的入侵保护。例如，可以对内部网络与外部网络之间的流量使用更严格的“安全优先于连接”策略。另一方面，可以对内部网络之间的流量应用更宽松的“连接优于安全”策略。

此外，还可以通过对所有网络使用相同的策略来简化配置。例如，“平衡安全和连接”策略用于提供良好的保护，且不会对连接产生过多的影响。

如果您决定对不同的网络使用不同的策略，则在使用相同源/目标安全区域和网络对象匹配条件的所有规则中应用相同的策略，将获得最佳效果。有关详细信息，请参阅[关于应用入侵策略优化NAP处理的最佳实践](#)，第 285 页。

过程

步骤 1 依次选择策略 > 访问控制。

步骤 2 创建新规则或编辑允许流量的现有规则。

如果允许默认操作，还可在默认操作中指定入侵策略。

步骤 3 点击入侵策略选项卡。

步骤 4 依次选择入侵策略 > 开，然后选择要在匹配流量中使用的入侵检测策略。

更改入侵规则操作

每个预定义的入侵策略包含相同的规则。不同的是针对每个规则所采取的操作因策略而异。

在给定策略中，仅可更改已启用规则（即，设置为发出警报或丢弃）的默认操作。通过更改默认操作，可以禁用为您提供过多误报的规则，也可以将规则更改为针对匹配流量发出警报或丢弃该流量。



注释 如果将规则从默认操作改为其他操作，则下一次更新入侵规则数据库时，系统会将规则的默认操作重置为所选的操作。此时，您的选择将成为新的默认操作，且该操作的状态不再显示为“已覆盖”。

过程

步骤 1 依次选择策略 > 入侵。

步骤 2 点击您要更改其规则操作的“入侵策略”选项卡。

预定义的策略包括：

- 连接优先于安全
- 平衡安全和连接
- 安全优先于连接
- 最大检测数

步骤 3 查找您要更改其操作的规则。

这些规则首先根据所列的已覆盖规则进行排序，并在已覆盖规则组中根据操作进行排序。否则，这些规则将先后根据 GID 和 SID 进行排序。

各策略的规则列表仅显示设置为发出警报或丢弃的规则以及显式禁用的规则，不显示默认禁用的规则。

使用搜索框查找希望更改的规则。如果您正在与思科技术支持部门合力解决某个问题，最好可以从事件中或通过该部门获取 Snort 标识符 (SID) 和生成器标识符 (ID)。

有关每个规则的元素的信息，请参阅[入侵规则属性，第 280 页](#)。

要搜索列表，请执行以下操作：

- a) 点击**搜索框**，打开“搜索属性”对话框。
- b) 输入生成器 ID 的组合 (**GID**)、Snort ID (**SID**) 或规则操作，然后点击**搜索**。

例如，您可以选择**操作=丢弃**来查看丢弃匹配连接的策略中的所有规则。搜索框旁边的文本表示与您的条件匹配的规则数量，例如“找到 9416 条规则中的 8937 条”。

要清除搜索条件，请点击搜索框中条件的 **x**。

步骤 4 点击规则的操作列，选择所需的操作：

- **警报** - 当此规则与流量匹配时，创建一个事件但不丢弃连接。
- **丢弃** - 当此规则与流量匹配时，创建一个事件同时丢弃连接。
- **禁用** - 不针对此规则匹配流量。不生成事件。

规则的默认操作后面附加“(默认)”表示。如果更改了默认设置，状态列会针对该规则指示“已覆盖”。

为入侵事件配置系统日志

可以为入侵策略配置外部系统日志服务器，从而将入侵事件发送至系统日志服务器。必须根据入侵策略配置系统日志服务器，从而将入侵事件发送到服务器。根据访问规则配置系统日志服务器只可将连接事件（而不是入侵事件）发送到系统日志服务器。

入侵事件的消息 ID 为 430001。

过程

步骤 1 依次选择**策略 > 入侵**。

步骤 2 点击**编辑日志记录设置按钮** (⚙️) 来配置日志记录。

步骤 3 点击**将连接事件发送到**字段，然后选择定义系统日志服务器的服务器对象。如果所需的对象尚不存在，请点击**创建新系统日志服务器**，并创建对象。

步骤 4 单击 **OK**。

监控入侵策略

可以在**监控**页面上的**攻击者**和**模板**控制面板找到入侵策略统计信息。必须将入侵策略应用于至少一个访问控制规则，才能在這些控制面板上看到任何信息。请参阅[监控流量和系统控制面板](#)，第 82 页。

要查看入侵事件，请依次选择**监控 > 事件**，然后点击**入侵**选项卡。将鼠标悬停在某个事件上方，点击[查看详细信息](#)链接以获取更多信息。在“详细信息”页面中，点击[查看 IPS 规则](#)转至相关入侵策略中的规则（您可以在此页面更改规则操作）。如果规则阻止过多安全连接，则可通过将操作从丢弃更改为警告减少误报带来的影响。相反，如果对于某条规则看到的是大量攻击流量，则可将警告规则更改为丢弃规则。

如果为入侵策略配置系统日志服务器，入侵事件的消息 ID 则为 430001。

入侵策略示例

使用案例章节涵盖以下实施入侵策略的示例。

- [如何阻止威胁](#)，第 41 页
- [如何被动监控网络上的流量](#)，第 62 页



第 17 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 291 页](#)
- [NAT 基础知识 ， 第 292 页](#)
- [NAT 指南 ， 第 297 页](#)
- [配置 NAT ， 第 301 页](#)
- [转换 IPv6 网络 ， 第 326 页](#)
- [监控 NAT ， 第 340 页](#)
- [NAT 示例 ， 第 341 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 地址和目的地 IP 地址与 NAT 规则进行比较，转换/不转换一个或两个地址。对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目的地”，即便是给定的连接，也可能源自“目的地”地址。

NAT 类型

可以使用以下方法实施 NAT：

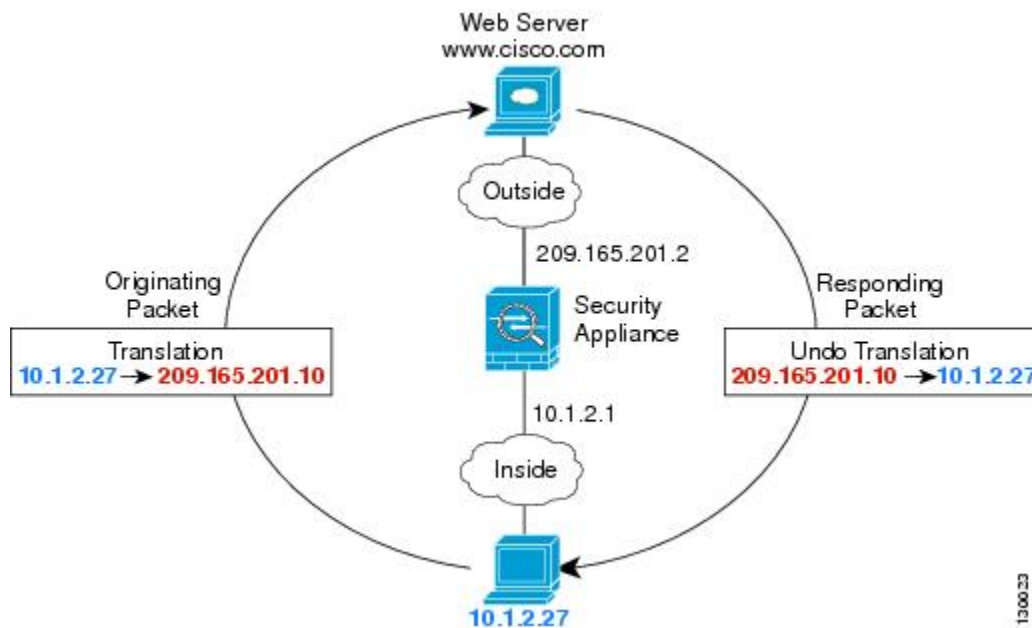
- 动态 NAT - 按先到先得的方式，将一组实际 IP 地址映射到一组映射 IP 地址（通常较小）。仅实际主机可以发起流量。请参阅[动态 NAT](#)，第 302 页。
- 动态端口地址转换 (PAT) - 使用 IP 地址的唯一源端口，将一组实际 IP 地址映射到单一 IP 地址。请参阅[动态 PAT](#)，第 307 页。
- 静态 NAT - 实际 IP 地址和映射 IP 地址之间的一致映射。允许发起双向流量。请参阅[静态 NAT](#)，第 311 页。

- 身份 NAT - 系统将实际地址静态转换为其本身，基本绕过 NAT。当您想转换一大组地址，但又想免除一小部分地址时，可能就要这样配置 NAT。请参阅[身份 NAT](#)，第 319 页。

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 7: 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，Firepower 威胁防御设备接收数据包，因为 Firepower 威胁防御设备执行代理 ARP 以认领数据包。
3. 接下来，Firepower 威胁防御设备变更从映射地址 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。

自动 NAT 和手动 NAT

可以通过以下两种方法实施地址转换：自动 NAT 和手动 NAT。

我们建议使用自动 NAT，除非您需要手动 NAT 提供的额外功能。自动 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。）

自动 NAT

配置为网络对象参数的所有 NAT 规则都被视为自动 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。

尽管这些规则配置为对象的一部分，但是您通过对象管理器无法看到对象定义中的 NAT 配置。

当数据包进入接口时，系统会根据自动 NAT 规则来检查源和目标 IP 地址。如果进行独立匹配，可根据独立规则转换数据包中的源地址和目的地地址。这些规则互不牵连，可以根据流量使用不同的规则组合。

因为规则从未配对，所以不能指定源 A/目的 A 应当有不同于源 A/目的 B 的转换。手动 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。

手动 NAT

手动 NAT 供您在单个规则中同时标识源和目标地址。同时指定源和目的目标地址，可以让您指定源 A/目的目标 A 有不同于源 A/目的目标 B 的转换。



注释

对于静态 NAT，规则是双向的，因此，请注意，这整个指南中命令和说明中使用的“源”和“目的地”，即便是给定的连接，也可能源自“目的地”地址。例如，如果配置支持端口地址转换的静态 NAT，然后将源地址指定为某台 Telnet 服务器，并且希望进入该 Telnet 服务器的所有流量都将端口从 2323 转换为 23，那么您就必须指定要转换的源端口（实际端口：23，映射端口：2323）。必须指定源端口是因为您已将 Telnet 服务器地址指定为源地址。

目的目标地址是可选的。如果指定目的目标地址，可以将其映射到其本身（身份 NAT），也可以将其映射到不同的地址。目的目标映射始终是静态映射。

比较自动 NAT 和手动 NAT

这两类 NAT 之间的主要差异是：

- 定义实际地址的方法。
 - 自动 NAT - NAT 规则成为网络对象的参数。网络对象 IP 地址用作原始（实际）地址。
 - 手动 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手动 NAT 更具可扩展性。
- 实施源和目标 NAT 的方法。
 - 自动 NAT- 每个规则都可应用到数据包的源或目标。因此，可能使用两条规则，一条用于源 IP 地址，一条用于目的 IP 地址。这两条规则不能绑在一起对源/目的组合进行特定转换。
 - 手动 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手动 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。
 - 自动 NAT- 在 NAT 表中自动排序。
 - 手动 NAT - 在 NAT 表中手动排序（在自动 NAT 规则之前或之后）。

NAT 规则顺序

自动 NAT 和手动 NAT 规则存储在分为三个部分的单个表中。首先应用第一部分规则，其次是第二部分，最后是第三部分，直到找到匹配项为止。例如，如果在第一部分找到匹配项，则不评估第二部分和第三部分。下表显示每个部分的规则顺序。

表 9: NAT 规则表

表部分	规则类型	部分中的规则顺序
第 1 部分	手动 NAT	系统按照在配置中出现的顺序应用第一个匹配的规则。因为会应用第一个匹配规则，所以必须确保特定规则位于更加通用的规则前面，否则无法按预期应用特定规则。默认情况下，手动 NAT 规则会添加到第 1 部分。
第 2 部分	自动 NAT	<p>如果在第 1 部分未找到匹配项，则会按照以下顺序应用第 2 部分的规则：</p> <ol style="list-style-type: none"> 1. 静态规则。 2. 动态规则。 <p>在每个规则类型中，遵循以下排序指导原则：</p> <ol style="list-style-type: none"> 1. 实际 IP 地址数量 - 从最小到最大。例如，带一个地址的对象将在带 10 个地址的对象之前进行评估。 2. 如果数量相同，则按从最低到最高的顺序使用 IP 地址编号。例如，10.1.1.0 在 11.1.1.0 之前进行评估。 3. 如果使用同一 IP 地址，则按字母数字顺序使用网络对象名称。例如，abracadabra 在 catwoman 之前进行评估。
第 3 部分	手动 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:

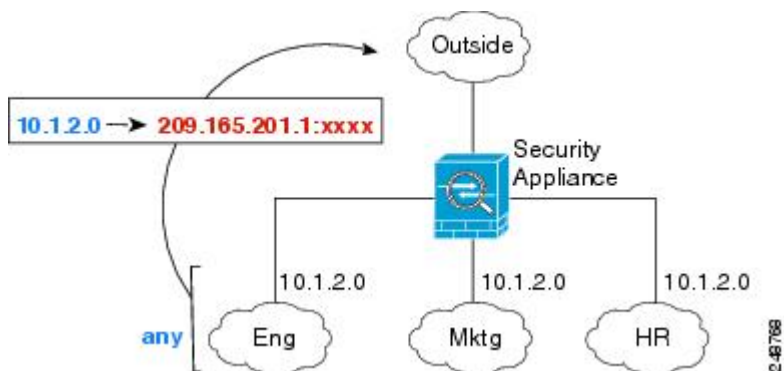
- 192.168.1.1/32 (静态)
- 10.1.1.0/24 (静态)
- 192.168.1.0/24 (静态)
- 172.16.1.0/24 (动态) (对象 abc)
- 172.16.1.0/24 (动态) (对象 def)
- 192.168.1.0/24 (动态)

NAT 接口

除了桥接组成员接口，您可以将 NAT 规则配置为应用到任何接口（也就是，所有接口），或者也可以标识特定的实际接口和映射接口。还可以为实际地址指定任何接口，为映射地址指定特定接口，反之亦然。

例如，如果在多个接口上使用相同的专用地址，并且在访问外部接口时要将这些地址全部转换到同一全局池，则可能要为实际地址指定任何接口，并且为映射地址指定外部接口。

图 8: 指定任何接口



然而，“任何”接口的概念不适用于桥接组成员接口。当指定“任何”接口时，NAT 将排除所有桥接组成员接口。因此，要将 NAT 应用于桥接组成员，必须指定成员接口。这样可能导致有许多只有一个接口不同的类似规则。您不能为桥接虚拟接口 (BVI) 本身配置 NAT，只能为成员接口配置 NAT。

不能为被动接口配置 NAT。

为 NAT 配置路由

FTD 设备需要成为发送到转换（映射）地址的所有数据包的目的地。

在发送数据包时，设备使用目的地接口（如果指定了接口）或路由表查找（如果未指定接口）来确定出口接口。对于身份 NAT，即使指定了目的地接口，您也可以选择使用路由查找。

所需的路由配置类型取决于映射地址的类型，以下主题对此进行了说明。

地址与映射接口在相同的网络中

如果使用与目的地（映射）接口在同一网络中的地址，Firepower 威胁防御设备使用代理 ARP 应答任何对映射地址的 ARP 请求，从而拦截发往映射地址的流量。此解决方案可以简化路由，因为 Firepower 威胁防御设备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。

唯一网络中的地址

如果需要比目的地（映射）接口网络上提供的地址更多的地址，则可以识别其他子网中的地址。上游路由器需要对指向 Firepower 威胁防御设备的映射地址进行静态路由。

与实际地址相同的地址（身份 NAT）

用于身份 NAT 的默认行为已启用代理 ARP，匹配其他静态 NAT 规则。如果需要，可以禁用代理 ARP。如果需要，还可以为常规静态 NAT 禁用代理 ARP，在这种情况下，需要确保上游路由器上有适当的路由。

通常，对于身份 NAT，是不需要代理 ARP 的，而且在某些情况下，会造成连接问题。例如，如果为“任何”IP 地址配置一条大体的身份 NAT 规则，则使代理 ARP 保持启用状态会给直接连接到映射接口的网络上的主机造成问题。在这种情况下，当映射网络上的主机要与同一网络上的其他主机通信时，ARP 请求中的地址匹配 NAT 规则（匹配“任何”地址）。然后，Firepower 威胁防御设备将代理地址的 ARP，即使数据包实际上不以 Firepower 威胁防御设备为目标。（请注意，即便已设置手动 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 Firepower 威胁防御设备 ARP 响应，则流量会错误地发送到 Firepower 威胁防御设备。

NAT 指南

以下主题提供有关实施 NAT 的详细指导原则。

接口指导原则

标准路由物理接口或子接口都支持 NAT

但是，在桥接组成员接口（作为桥接虚拟接口或 BVI 一部分的接口）上配置 NAT 有以下限制：

- 为桥接组的成员配置 NAT 时，需要指定成员接口。您不能为桥接组接口 (BVI) 本身配置 NAT。
- 在桥接组成员接口之间执行 NAT 时，必须指定源接口和目的地接口。不能指定“任意”作为接口。
- 当目的地接口为桥接组成员接口时，不能配置接口 PAT，因为没有连接到该接口的 IP 地址。
- 当源接口和目的地接口是同一桥接组的成员时，不能在 IPv4 和 IPv6 网络 (NAT64/46) 之间进行转换。静态 NAT/PAT 44/66、动态 NAT44/66 和动态 PAT44 是唯一允许的方法；不支持动态 PAT66。

IPv6 NAT 指南

NAT 支持 IPv6，但有以下指导原则和限制。

- 对于标准路由模式接口，您还可以在 IPv4 和 IPv6 之间进行转换。
- 对于同一个桥接组的成员接口，不能在 IPv4 和 IPv6 之间进行转换，而只能在两个 IPv6 或两个 IPv4 网络之间进行转换。此限制不适用于一个接口为桥接组成员，另一个为标准路由接口的情况。
- 在同属一个桥接组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于一个接口为桥接组成员，另一个为标准路由接口的情况。
- 对于静态 NAT，可以指定一个最大 /64 的 IPv6 子网。不支持更大的子网。
- 将 FTP 和 NAT46 配合使用时，当 IPv4 FTP 客户端连接到 IPv6 FTP 服务器时，客户端必须使用扩展被动模式 (EPSV) 或扩展端口模式 (EPRT)；在使用 IPv6 时，不支持 PASV 和 PORT 命令。

IPv6 NAT 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（仅限于手动 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（仅限于手动 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。
- 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。

对检测到的协议的 NAT 支持

检测打开辅助连接或者在数据包中嵌入 IP 地址的一些应用层协议，以提供以下服务：

- 创建小孔 - 一些应用协议在标准端口或协商的端口上打开辅助 TCP 或 UDP 连接。检测会为这些辅助端口打开小孔，使您无需创建访问控制规则予以允许。
- NAT 重写 - 诸如 FTP 等协议会在数据包数据中嵌入用于辅助连接的 IP 地址和端口，作为协议的一部分。如果 NAT 转换涉及到任一终端，则检测引擎会重写数据包数据以反映嵌入式地址和端口的 NAT 转换。在没有 NAT 重写的情况下，辅助连接不起作用。
- 协议实施 - 一些检测会为检测到的协议实施某种程度的 RFC 一致性。

下表列出了应用 NAT 重写及其 NAT 限制的检测到的协议。当写入包括这些协议的 NAT 规则时，请记住这些限制。此处未列出的协议不应用 NAT 重写。这些检测包括 GTP、HTTP、IMAP、POP、SMAP、SSH 和 SSL。



注释 仅列出的端口支持 NAT 重写。如果在非标准端口上使用这些协议，请勿对连接使用 NAT。

表 10: NAT 支持的应用检测

应用	检测到的协议、端口	NAT 限制	创建的小孔
DCERPC	TCP/135	无 NAT64。	是
DNS over UDP	UDP/53	无可用于通过 WINS 进行名称解析的 NAT 支持。	否
ESMTP	TCP/25	无 NAT64。	否
FTP	TCP/21	没有限制。	是
H.323 H.225 (呼叫信令) H.323 RAS	TCP/1720 UDP/1718 对于 RAS, 则为 UDP/1718-1719	无 NAT64。	是
ICMP ICMP 错误	ICMP (从不会对定向到设备接口的 ICMP 流量进行检测。)	没有限制。	否
IP 选项	RSVP	无 NAT64。	否
NetBIOS Name Server over IP	UDP/137、138 (源端口)	无 NAT64。	否

应用	检测到的协议、端口	NAT 限制	创建的小孔
RSH	TCP/514	无 PAT。 无 NAT64。	是
RTSP	TCP/554 (对于 HTTP 隐藏没有任何处理。)	无 NAT64。	是
SIP	TCP/5060 UDP/5060	无扩展 PAT。 无 NAT64 或 NAT46。	是
Skinny (SCCP)	TCP/2000	无 NAT64、NAT46 或 NAT66。	是
SQL*Net (版本 1、2)	TCP/1521	无 NAT64。	是
Sun RPC	TCP/111 UDP/111	无 NAT64。	是
TFTP	UDP/69	无 NAT64。 不转换负载 IP 地址。	是
XDMCP	UDP/177	无 NAT64。	是

其他 NAT 指南

- 对于作为桥接组成员的接口，您需要为成员接口编写 NAT 规则。您无法为桥接虚拟接口 (BVI) 本身编写 NAT 规则。
- (仅限于自动 NAT。) 您仅可为给定对象定义单个 NAT 规则，如果要为某个对象配置多个 NAT 规则，则需要创建通过不同名称指定同一 IP 地址的多个对象。
- 如果在接口上定义了 VPN，则接口上的进站 ESP 流量不受 NAT 规则的约束。系统仅允许已建立的 VPN 隧道的 ESP 流量，而丢弃与现有隧道不相关的流量。此限制适用于 ESP 和 UDP 端口 500 和 4500。
- 如果在应用动态 PAT 设备之后的某设备上定义站点间 VPN，以便 UDP 端口 500 和 4500 不是实际使用的端口，必须从 PAT 设备之后的设备发起连接。响应方无法发起安全关联 (SA)，因为不知道正确的端口号。
- 如果更改 NAT 配置，并且不想等待现有转换超时后再使用新 NAT 配置，则可以在设备 CLI 中使用 **clear xlate** 命令清除转换表。然而，清除转换表将断开使用转换的当前所有连接。



注释 如果删除动态 NAT 或 PAT 规则，然后使用与已删除规则中地址重叠的映射地址添加新规则，则系统将不使用新规则，直至与已删除规则关联的所有连接超时，或已使用 **clear xlate** 命令将这些连接清除。此保护措施确保相同的地址将不分配至多个主机。

- 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。
- （仅限于手动 NAT。）在 NAT 规则中使用 **any** 作为源地址时，“any”流量（IPv4 与 IPv6）的定义取决于规则。只有数据包为 IPv6 至 IPv6 或 IPv4 至 IPv4，Firepower 威胁防御设备才能对数据包执行 NAT；借助此先决条件，Firepower 威胁防御设备可确定 NAT 规则中的 **any** 的值。例如，如果配置从“any”到 IPv6 服务器的规则，且该服务器已从 IPv4 地址映射，则 **any** 指“任意 IPv6 流量”。如果配置从“any”到“any”的规则，并且将源映射至接口 IPv4 地址，则 **any** 指“任意 IPv4 流量”，因为映射的接口地址意味着目的地也是 IPv4。
- 可以在多条 NAT 规则中使用同一映射对象或组。
- 映射 IP 地址池不能包括：
 - 映射接口的 IP 地址。如果为该规则指定“any”接口，则禁止所有接口 IP 地址。对于接口 PAT（仅路由模式），指定接口名称而不是接口地址。
 - 故障切换接口 IP 地址。
 - （动态 NAT。）启用 VPN 时的备用接口 IP 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接入 VPN 地址池中使用重叠地址。
- 如果在规则中指定目的地接口，则该接口用作出口接口，而不是在路由表中查找路由。但是，对于身份 NAT，您可以选择改为使用路由查找。
- NAT 仅适用于直通流量。系统生成的流量不进行 NAT。

配置 NAT

网络地址转换可能非常复杂。我们建议规则应尽可能保持简单，以避免出现转换问题和难以进行故障排除的情况。在实施 NAT 之前仔细规划，这非常重要。以下程序说明了规划的基本方法。

过程

- 步骤 1** 依次选择 **策略 > NAT**。
- 步骤 2** 决定您需要哪些类型的规则。

可以创建动态 NAT、动态 PAT、静态 NAT 和身份 NAT 规则。有关概述，请参阅 [NAT 类型](#)，第 292 页。

步骤 3 决定应将哪些规则作为手动或自动 NAT 来实施。



有关这两种实施选项的比较，请参阅 [自动 NAT 和手动 NAT](#)，第 293 页。

步骤 4 遵循以下部分中的说明创建规则。

- [动态 NAT](#)，第 302 页
- [动态 PAT](#)，第 307 页
- [静态 NAT](#)，第 311 页
- [身份 NAT](#)，第 319 页

步骤 5 管理 NAT 策略和规则。

您可以执行以下操作来管理策略及其规则。

- 要编辑规则，请点击规则的编辑图标 ()。
- 要删除某条规则，请点击该规则的删除图标 ()。

动态 NAT

以下主题介绍动态 NAT 以及如何配置动态 NAT。

关于动态 NAT

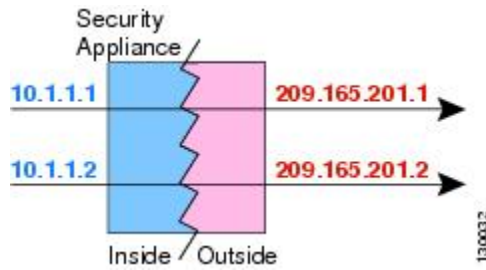
动态 NAT 将一个实际地址组转换为一个可在目标目的网络上路由的映射地址池。映射池通常包含少于实际地址组的地址。当您要转换的主机访问目标目的的网络时，NAT 会从映射池中为该主机分配 IP 地址。仅在实际主机发起连接时创建转换。转换仅在连接期间发生，而且转换超时后，给定用户不保持同一 IP 地址。因此，目的网络上的用户不能向使用动态 NAT 的主机发起可靠连接，即使访问规则允许该连接。



注释 在转换期间，如果访问规则允许连接转换后主机，远程主机可以发起这种连接。因为地址不可预测，所以与主机的连接不可能发生。然而，在这种情况下，可以依靠访问规则的安全性。

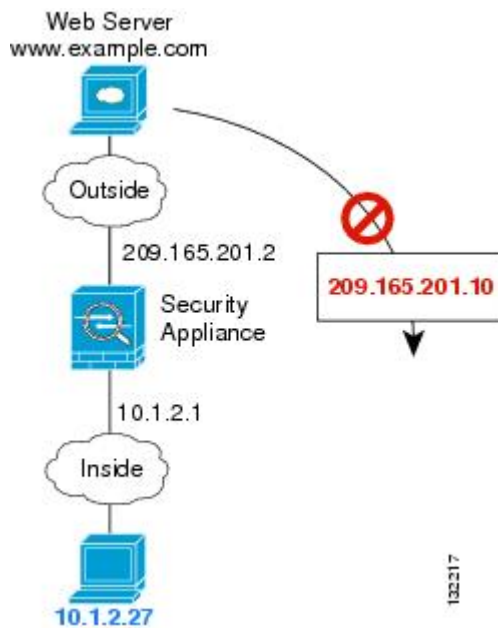
下图显示典型的动态 NAT 场景。仅实际主机可以创建 NAT 会话，允许返回响应流量。

图 9: 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 10: 远程主机尝试向映射地址发起连接



动态 NAT 不足和优势

动态 NAT 有以下缺点：

- 如果映射池的地址少于实际组，并且流量数量大于预期，地址可能会用尽。
如果经常发生这种情况，请使用 PAT 或 PAT 回退方法，因为 PAT 可以使用单一地址的端口提供超过 64,000 次转换。
- 不得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。

配置动态自动 NAT

使用动态自动 NAT 规则将地址转换为可在目标网络中路由的其他 IP 地址。

开始之前

选择对象并创建规则中所需的网络对象或组。或者，您可以在定义 NAT 规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机或子网。
- **转换后的地址** - 该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。

过程

步骤 1 依次选择 **策略 > NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 (✎)。

(要删除不再需要的规则，请点击该规则的垃圾桶图标。)

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于 (Create Rule For)** - 选择 **自动 NAT (Auto NAT)**。
- **类型** - 选择 **动态**。

步骤 4 配置以下数据包转换选项：

- **源接口、目标接口** - (桥接组成员接口的必选项。) 应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口 (**任意**)。
- **原始地址 (Original Address)** - 包含您要转换的地址的网络对象。
- **转换后的地址** - 包含映射地址的网络对象或组。

步骤 5 (可选。) 点击 **高级选项 (Advanced Options)** 链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址 (IPv4 A 或 IPv6 AAAA) 记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换 (其中重写也会在 A 和 AAAA 记录之间转换) 需要使用此选项。有关详细信息，请参阅 [使用 NAT 重写 DNS 查询和响应](#)，第 361 页。

- 跳转到接口 **PAT**（目标接口） - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 **PAT** 回退）。仅当您选择不是桥接组成员的目的地接口时，此选项才可用。

步骤 6 单击 **OK**。

配置动态手动 NAT

当自动 NAT 不能满足您的需求时，请使用动态手动 NAT 规则。例如，如果您要根据目的进行不同的转换。动态 NAT 会将地址转换为可在目标目的网络中路由的其他 IP 地址。

开始之前

选择对象并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- 原始源地址 - 地址可以是网络对象或组，而且它可以包含主机或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定任何 (**Any**)。
- 转换后的源地址 - 此选项可以是网络对象或组，但不能包含在子网中。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。

如果您要在规则中为原始目标地址 (**Original Destination Address**) 和转换后的目标地址 (**Translated Destination Address**) 配置静态转换，还可以为这些地址创建网络对象。

对于动态 NAT，您还可以对目标执行端口转换。在对象管理器中，请确保有可用于原始目标端口和转换后的目标端口的端口对象。系统将忽略您指定的源端口。

过程

步骤 1 依次选择 **策略 > NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 (✎)。

(要删除不再需要的规则，请点击该规则的垃圾桶图标。)

步骤 3 配置基本规则选项：

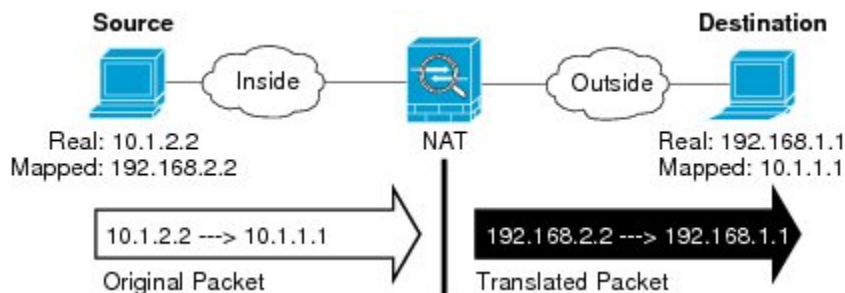
- 标题 - 为规则输入名称。
- 为创建规则 - 选择 **手动 NAT**。
- 规则位置 - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。
- 类型 - 选择 **动态**。该设置仅应用于源地址。如果为目的的目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口、目标接口** - (桥接组成员接口的必选项。) 应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口 (**任意**)。

步骤 5 确定原始数据包地址 (IPv4 或 IPv6 地址)；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** - (可选。) 包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

可以依次选择**接口**以使原始目标基于源接口 (不能为“任意”)。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址 (IPv4 或 IPv6 地址)；例如，显示在目标目的接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址** - 包含映射地址的网络对象或组。
- **转换后的目标地址** - (可选。) 包含已转换的数据包中使用的目的目标地址的网络对象或组。如果为**原始目标地址**选择了一个对象，则可以通过选择相同的对象设置身份 NAT (即无转换)。

步骤 7 (可选。) 确定用于服务转换的目标服务端口：**原始目标端口**、**转换后的目标端口**。

动态 NAT 不支持端口转换，因此，请将**原始源端口**和**已转换源端口**字段保留为空。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同 (同为 TCP 或同为 UDP)。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

步骤 8 (可选。) 点击**高级选项 (Advanced Options)** 链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址 (IPv4 A 或 IPv6 AAAA) 记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换 (其中重写也会在 A 和 AAAA 记录之间转换) 需要使用此选项。有关详细信息，请参阅[使用 NAT 重写 DNS 查询和响应](#)，第 361 页。

- 跳转到接口 PAT（目标接口） - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是桥接组成员的目的地接口时，此选项才可用。

步骤 9 单击 **OK**。

动态 PAT

以下主题介绍动态 PAT。

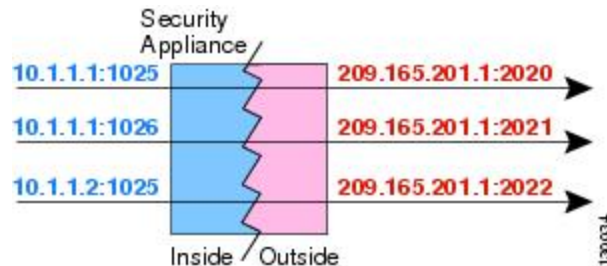
关于动态 PAT

通过将实际地址和源端口转换为映射地址和唯一端口，动态 PAT 可以将多个实际地址转换为单一映射地址。如果可用，实际源端口号将用于映射端口。然而，如果实际端口不可用，将默认从与实际端口号相同的端口范围选择映射端口：0 至 511、512 至 1023 以及 1024 至 65535。因此，低于 1024 的端口仅拥有很小的可用 PAT 池。

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 11: 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。



注释 建议每个接口使用不同的 PAT 池。如果多个接口使用同一池，尤其是用于“任何”接口时，该池将被快速耗尽，且没有端口可用于新的转换。

动态 PAT 不足和优势

通过动态 PAT，可以使用单一映射地址，从而保存可路由地址。甚至可以将 Firepower 威胁防御设备接口 IP 地址用作 PAT 地址。但是，不能将接口 PAT 用于接口上的 IPv6 地址。

在同属一个桥接组的接口之间进行转换时，不能将动态 PAT 用于 IPv6 (NAT66)。此限制不适用于一个接口为桥接组成员，另一个为标准路由接口的情况。

动态 PAT 不适用于某些数据流不同于控制路径的多媒体应用。有关详细信息，请参阅[对检测到的协议的 NAT 支持](#)，第 299 页。

动态 PAT 还可以创建大量显示为来自单一 IP 地址的连接，服务器可能将此流量解释为 DoS 攻击。

配置动态自动 PAT

使用动态自动 PAT 规则可将地址转换为唯一的 IP 地址/端口组合，而不是仅转换为多个 IP 地址。可以转换为单个地址，即目标目的接口的地址或其他地址。

开始之前

选择对象并创建规则中所需的网络对象或组。或者，您可以在定义 NAT 规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机或子网。
- **转换后的地址** - 可以通过以下选项指定 PAT 地址：
 - **目标接口 (Destination Interface)** - 要使用目标接口 IPv4 地址，不需要网络对象。您不能将接口 PAT 用于 IPv6。
 - **单个 PAT 地址** - 创建包含单个主机的网络对象。

过程

步骤 1 依次选择 **策略 > NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 (✎)。

(要删除不再需要的规则，请点击该规则的垃圾桶图标。)

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于 (Create Rule For)** - 选择 **自动 NAT (Auto NAT)**。
- **类型** - 选择 **动态**。

步骤 4 配置以下数据包转换选项：

- **源接口、目标接口** - (桥接组成员接口的必选项。) 应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口 (**任意**)。
- **原始地址 (Original Address)** - 包含您要转换的地址的网络对象。

- **转换后的地址 (Translated Address)** - 以下项之一：
 - (接口 PAT。)要使用目的接口的 IPv4 地址，请选择接口。您还必须选择具体的目的接口，该接口不能是桥接组成员接口。您不能将接口 PAT 用于 IPv6。
 - 要使用目的目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。

步骤 5 (可选。) 点击 **高级选项 (Advanced Options)** 链接并选择所需的选项：

- **跳转到接口 PAT (目标接口)** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法 (接口 PAT 回退)。仅当您选择不是桥接组成员的目的地接口时，此选项才可用。如果已配置接口 PAT 作为转换后的地址，则不能选择此选项。您也不能将此选项用于 IPv6 网络。

步骤 6 单击 **OK**。

配置动态手动 PAT

当自动 PAT 不能满足您的需求时，请使用动态手动 PAT 规则。例如，如果您要根据目的进行不同的转换。动态 PAT 可将地址转换为唯一的 IP 地址/端口组合，而不是仅转换为多个 IP 地址。可以转换为单个地址，即目标目的接口的地址或其他地址。

开始之前

选择对象并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源地址** - 地址可以是网络对象或组，而且它可以包含主机或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定任何 (**Any**)。
- **转换后的源地址** - 您可通过以下选项指定 PAT 地址：
 - **目标接口 (Destination Interface)** - 要使用目标接口 IPv4 地址，不需要网络对象。您不能将接口 PAT 用于 IPv6。
 - **单个 PAT 地址** - 创建包含单个主机的网络对象。

如果您要在规则中为原始目标地址 (**Original Destination Address**) 和转换后的目标地址 (**Translated Destination Address**) 配置静态转换，还可以为这些地址创建网络对象。

对于动态 PAT，您还可以对目标执行端口转换。在对象管理器中，请确保有可用于原始目标端口和转换后的目标端口的端口对象。系统将忽略您指定的源端口。

过程

步骤 1 依次选择 **策略 > NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。

- 要编辑现有规则，请点击规则的编辑图标 (✎)。
- (要删除不再需要的规则，请点击该规则的垃圾桶图标。)

步骤 3 配置基本规则选项：

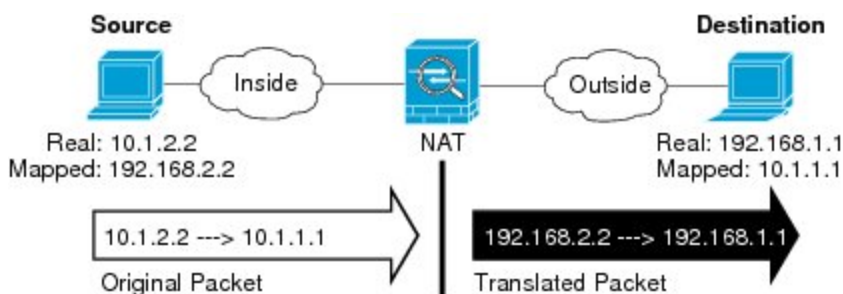
- **标题** - 为规则输入名称。
- 为创建规则 - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。
- **类型** - 选择**动态**。该设置仅应用于源地址。如果为目的的目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口、目标接口** - （桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（**任意**）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** - （可选。）包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

可以依次选择**接口**以使原始目标基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标目的接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址 (Translated Source Address)** - 以下项之一：
 - （接口 PAT。）要使用目的接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目的接口，该接口不能是桥接组成员接口。您不能将接口 PAT 用于 IPv6。
 - 要使用目的目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。

- **转换后的目标地址** - (可选。) 包含已转换的数据包中使用的目的目标地址的网络对象或组。如果为**原始目的目标** 选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 (可选。) 确定用于服务转换的目标服务端口：**原始目标端口**、**转换后的目标端口**。

动态 NAT 不支持端口转换，因此，请将**原始源端口**和**已转换源端口**字段保留为空。然而，由于目标转换始终为静态，因此可为目标端口执行端口转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

步骤 8 (可选。) 点击**高级选项 (Advanced Options)** 链接并选择所需的选项：

- **跳转到接口 PAT (目标接口)** - 当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是桥接组成员的目的地接口时，此选项才可用。如果已配置接口 PAT 作为转换后的地址，则不能选择此选项。您也不能将此选项用于 IPv6 网络。

步骤 9 单击 **OK**。

静态 NAT

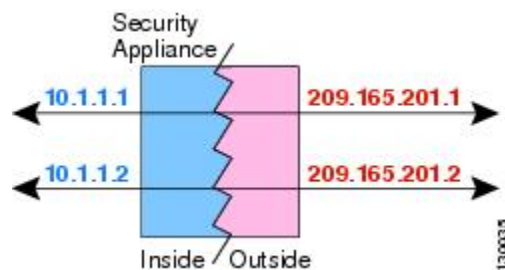
以下主题介绍静态 NAT 以及如何实施静态 NAT。

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 12: 静态 NAT



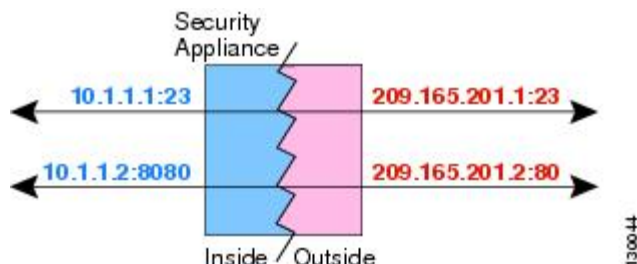
支持端口转换的静态 NAT

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 13: 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，对于手动 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）。

对非标准端口进行端口转换的静态 NAT

还可以利用支持端口转换的静态 NAT 将一个公认端口转换为一个非标准端口，反之亦然。例如，如果内部 Web 服务器使用端口 8080，可以允许外部用户连接到端口 80，然后取消转换到原始端口 8080。同样，要进一步提高安全性，可以告知 Web 用户连接到非标准端口 6785，然后取消转换到端口 80。

具有端口转换的静态接口 NAT

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

一对多静态 NAT

通常，配置带一对一映射的静态 NAT。然而，在某些情况下，可能要将单一实际地址配置到多个映射地址（一对多）。配置一对多静态 NAT 时，当实际主机发起流量时，它始终使用第一个映射地

址。然而，对于发起到主机的流量，可以发起到任何映射地址的流量，并且不将它们转换为单一实际地址。

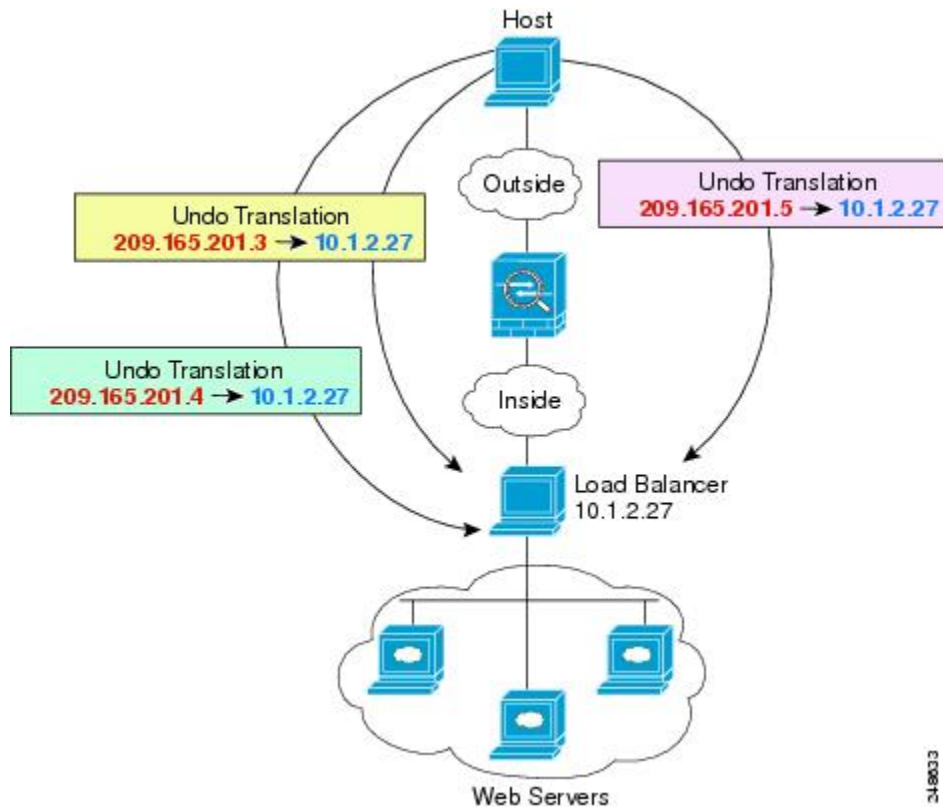
下图显示典型的一对多静态 NAT 场景。由于实际主机进行的发起的流量始终使用第一个映射地址，因此从技术上说，实际主机 IP/第一个映射 IP 的转换是唯一的双向转换。

图 14: 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。

图 15: 一对多静态 NAT 示例



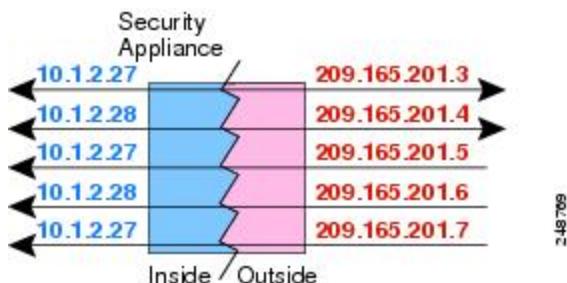
其他映射场景（不推荐）

NAT 具有很高的灵活性，允许任何类型的静态映射场景：不仅包括一对一、一对多，还包括少对多、多对少和多对一映射。我们推荐仅使用一对一或一对多映射。其他映射选项可能会导致意外后果。

在功能上，少对多与一对多相同；但是，因为此配置更加复杂，而且实际映射可能不会一目了然，所以我们建议为每个需要一对多配置的实际地址创建该配置。例如，对于少对多场景，少量的实际地址会按顺序映射到多个映射地址（A 到 1、B 到 2、C 到 3）。当映射所有实际地址时，下一个映射地址会映射到第一个实际地址，等等，直到映射了所有映射地址为止（A 到 4、B 到 5、C 到 6）。这将导致每个实际地址有多个映射地址。就像一对多配置一样，仅第一个映射是双向的；后续映射可以将流量发起到实际主机，但所有从实际主机发起的流量仅将第一个映射地址用于源。

下图显示典型的少对多静态 NAT 场景。

图 16: 少对多静态 NAT



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



注释 多对少或多对一 NAT 不是 PAT。如果两台实际主机使用同一源端口号，连接到同一外部服务器和同一 TCP 目的目标端口，并且两台主机转换到同一 IP 地址，那么由于地址冲突（五元组不唯一），将重置两个连接。

下图显示一个典型的多对少静态 NAT 场景。

图 17: 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。

配置静态自动 NAT

使用静态自动 NAT 规则将地址转换为可在目标目的网络中路由的其他 IP 地址。您还可以通过静态 NAT 规则执行端口转换。

开始之前


选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义 NAT 规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机或子网。
- **转换后的地址 (Translated Address)** - 您可以通过以下选项指定转换后的地址：
 - **目标接口 (Destination Interface)** - 要使用目标接口 IPv4 地址，不需要网络对象。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。
 - **地址** - 创建包含主机或子网的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。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。

过程

步骤 1 依次选择 **策略 > NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 。

（要删除不再需要的规则，请点击该规则的垃圾桶图标。）

步骤 3 配置基本规则选项：

- **标题** - 为规则输入名称。
- **创建规则用于 (Create Rule For)** - 选择 **自动 NAT (Auto NAT)**。
- **类型 (Type)** - 选择 **静态 (Static)**。

步骤 4 配置以下数据包转换选项：

- **源接口、目标接口** - （桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（任意）。
- **原始地址 (Original Address)** - 包含您要转换的地址的网络对象。
- **转换后的地址 (Translated Address)** - 以下项之一：

- 要使用一组地址，请选择包含映射地址的网络对象或组。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。
- （具有端口转换的静态接口 NAT。）要使用目的地接口的地址，请选择**接口**。您还必须选择具体的目的接口，该接口不能是桥接组成员接口。您不能将接口 PAT 用于 IPv6。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。
- （可选。）**原始端口 (Original Port)、转换后的端口 (Translated Port)** - 如果需要转换 TCP 或 UDP 端口，请选择定义原始端口和转换后的端口的端口对象。对象必须用于相同的协议。如果对象不存在，请点击**创建新对象 (Create New Object)** 链接。例如，如有必要，可以将 TCP/80 转换为 TCP/8080。

步骤 5 （可选。）点击**高级选项 (Advanced Options)** 链接并选择所需的选项：

- **转换与此规则相匹配的 DNS 应答** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅[使用 NAT 重写 DNS 查询和响应，第 361 页](#)。如果您在进行端口转换，则此选项不可用。
- **请勿在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。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。

步骤 6 单击 **OK**。

配置静态手动 NAT

当自动 NAT 不能满足您的需求时，请使用静态手动 NAT 规则。例如，如果您要根据目的进行不同的转换。静态 NAT 会将地址转换为可在目的网络中路由的其他 IP 地址。您还可以通过静态 NAT 规则执行端口转换。

开始之前

选择**对象**并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- **原始源地址** - 地址可以是网络对象或组，而且它可以包含主机或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定**任何 (Any)**。
- **转换后的源地址 (Translated Source Address)** - 可以通过以下选项指定转换后的地址：
 - **目标接口 (Destination Interface)** - 要使用目标接口 IPv4 地址，不需要网络对象。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。

- **地址** - 创建包含主机或子网的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；其只能包含一种类型。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。

如果您要在规则中为原始目标地址 (**Original Destination Address**) 和转换后的目标地址 (**Translated Destination Address**) 配置静态转换，还可以为这些地址创建网络对象。如果只需要配置支持端口转换的目的静态接口 NAT，则可以跳过为目的映射地址添加对象的过程，并在规则中指定接口。

您还可以对源和/或目的执行端口转换。在对象管理器中，确保有可以用于原始端口和转换后的端口的端口对象。

过程

步骤 1 依次选择 **策略 > NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 + 按钮。
- 要编辑现有规则，请点击规则的编辑图标 (✎)。

(要删除不再需要的规则，请点击该规则的垃圾桶图标。)

步骤 3 配置基本规则选项：

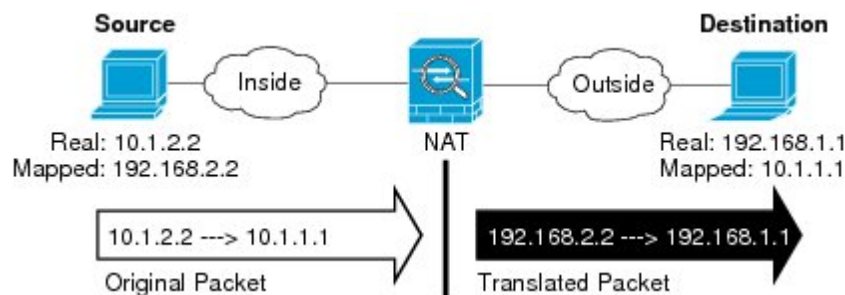
- **标题** - 为规则输入名称。
- 为创建规则 - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。
- **类型 (Type)** - 选择**静态 (Static)**。该设置仅应用于源地址。如果为目的的目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口、目标接口** - （桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（任意）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** - (可选。) 包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

可以依次选择**接口**以使原始目标基于源接口（不能为“任意”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标目的接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址 (Translated Source Address)** - 以下项之一：
 - 要使用一组地址，请选择包含映射地址的网络对象或组。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。
 - (具有端口转换的静态接口 NAT。) 要使用目的接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目的接口，该接口不能是桥接组成员接口。该选项配置具有端口转换的静态接口 NAT：源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。
- **转换后的目标地址** - (可选。) 包含已转换的数据包中使用的目的目标地址的网络对象或组。如果为**原始目的目标** 选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

步骤 7 (可选。) 为服务转换确定源或目的服务端口。

如果要配置支持端口转换的静态 NAT，可以为源和/或目的转换端口。例如，可以在 TCP/80 和 TCP/8080 之间进行转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

- **原始源端口 (Original Source Port)、转换后的源端口 (Translated Source Port)** - 定义源地址的端口转换。
- **原始目标端口、转换后的目标端口** - 定义目标地址的端口转换。

步骤 8 (可选。) 点击高级选项 (**Advanced Options**) 链接并选择所需的选项：

- **转换与此规则相匹配的 DNS 应答** - 是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址 (IPv4 A 或 IPv6 AAAA) 记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅[使用 NAT 重写 DNS 查询和响应](#)，第 361 页。如果您在进行端口转换，则此选项不可用。
- **请勿在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。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。

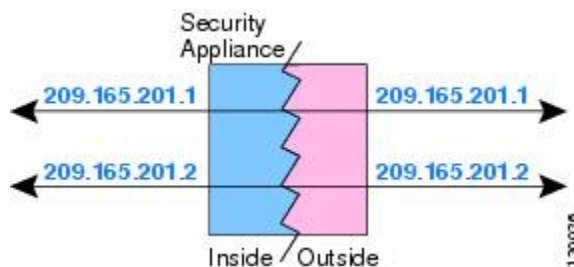
步骤 9 单击 **OK**。

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。

下图显示典型的身份 NAT 场景。

图 18: 身份 NAT



以下主题介绍如何配置身份 NAT

配置身份自动 NAT

使用静态身份自动 NAT 规则可防止地址转换。即，防止将地址转换为自身。

开始之前

选择**对象**并创建规则中所需的网络对象或组。或者，您可以在定义 NAT 规则时创建对象。对象必须满足以下要求：

- **原始地址** - 该地址必须是网络对象（而非组），而且它可以是主机或子网。
- **转换后的地址** - 其内容与原始源对象完全相同的网络对象或组。您可以使用相同的对象。

过程

步骤 1 依次选择 **策略 > NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 **+** 按钮。
- 要编辑现有规则，请点击规则的编辑图标 (✎)。

(要删除不再需要的规则，请点击该规则的垃圾桶图标。)

步骤 3 配置基本规则选项：

- 标题 - 为规则输入名称。
- 创建规则用于 (**Create Rule For**) - 选择自动 NAT (**Auto NAT**)。
- 类型 (**Type**) - 选择静态 (**Static**)。

步骤 4 配置以下数据包转换选项：

- 源接口、目标接口 - (桥接组成员接口的必选项。) 应用此 NAT 规则的接口。源是实际接口，流量通过该接口进入设备。目标是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口 (任意)。
- 原始地址 (**Original Address**) - 包含您要转换的地址的网络对象。
- 转换后的地址 - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

不要为身份 NAT 配置原始端口和转换后的端口选项。

步骤 5 (可选。) 点击高级选项 (**Advanced Options**) 链接并选择所需的选项：

- 转换与此规则匹配的 DNS 回复 - 请勿为身份 NAT 配置此选项。
- 请勿在目标接口上使用代理 ARP - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。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。
- 对目标接口执行路由查找 - 如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在 NAT 规则中配置的目标接口来确定目标接口。

步骤 6 单击 **OK**。

配置身份手动 NAT

当自动 NAT 不能满足您的需求时，请使用静态身份手动 NAT 规则。例如，如果您要根据目的进行不同的转换。使用静态身份 NAT 规则可防止地址转换。即，防止将地址转换为自身。

开始之前

选择对象并创建规则中所需的网络对象或组。组不能同时包含 IPv4 和 IPv6 地址；只能包含一种类型。或者，您可以在定义 NAT 规则时创建对象。对象还必须满足以下要求：

- 原始源地址 - 地址可以是网络对象或组，而且它可以包含主机或子网。如果要转换所有原始源流量，可以跳过此步骤并在规则中指定任何 (**Any**)。
- 转换后的源地址 - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

如果您要在规则中为原始目标地址 (**Original Destination Address**) 和转换后的目标地址 (**Translated Destination Address**) 配置静态转换，还可以为这些地址创建网络对象。如果只需要配置支持端口转换的目的静态接口 NAT，则可以跳过为目的映射地址添加对象的过程，并在规则中指定接口。

您还可以对源和/或目的执行端口转换。在对象管理器中，确保有可以用于原始端口和转换后的端口的端口对象。您可以为身份 NAT 使用相同的对象。

过程

步骤 1 依次选择 **策略 > NAT**。

步骤 2 执行以下操作之一：

- 要创建新规则，请点击 + 按钮。
 - 要编辑现有规则，请点击规则的编辑图标 (✎)。
- (要删除不再需要的规则，请点击该规则的垃圾桶图标。)

步骤 3 配置基本规则选项：

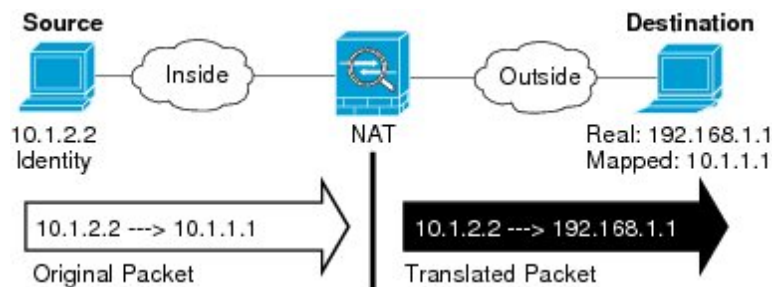
- **标题** - 为规则输入名称。
- **为创建规则** - 选择**手动 NAT**。
- **规则位置** - 要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。
- **类型 (Type)** - 选择**静态 (Static)**。该设置仅应用于源地址。如果为目的的目标地址定义转换，则该转换始终为静态。

步骤 4 配置以下接口选项：

- **源接口、目标接口** - （桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（任意）。

步骤 5 确定原始数据包地址（IPv4 或 IPv6 地址）；例如，显示在原始数据包中的数据包地址。

请参阅下图，了解原始数据包与转换后数据包的示例，其中在内部主机上执行身份 NAT，但转换外部主机。



- **原始源地址** - 包含将要转换的地址的网络对象或组。
- **原始目标地址** - （可选。）包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用身份 NAT 用于该地址。

您可以选择**接口**以使原始目的目标基于源接口（不能为“任何”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

步骤 6 确定已转换的数据包地址（IPv4 或 IPv6 地址）；例如，显示在目标目的接口网络中的数据包地址。如果需要，可在 IPv4 与 IPv6 之间进行转换。

- **转换后的源地址** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。
- **转换后的目标地址** - （可选。）包含已转换的数据包中使用的目的目标地址的网络对象或组。如果为**原始目标地址** 选择了一个对象，则可以通过选择相同的对象设置身份 NAT（即无转换）。

步骤 7 （可选。）为服务转换确定源或目的服务端口。

如果要配置支持端口转换的静态 NAT，可以为源和/或目的转换端口。例如，可以在 TCP/80 和 TCP/8080 之间进行转换。

NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，可将相同的服务对象同时用于实际和映射端口。

- **原始源端口 (Original Source Port)、转换后的源端口 (Translated Source Port)** - 定义源地址的端口转换。
- **原始目标端口、转换后的目标端口** - 定义目标地址的端口转换。

步骤 8 （可选。）点击高级选项 (**Advanced Options**) 链接并选择所需的选项：

- **转换与此规则匹配的 DNS 回复** - 请勿为身份 NAT 配置此选项。
- **请勿在目标接口上使用代理 ARP** - 为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。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。
- **对目标接口执行路由查找** - 如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在 NAT 规则中配置的目标接口来确定目标接口。

步骤 9 单击 **OK**。

Firepower 威胁防御的 NAT 规则属性

使用网络地址转换 (NAT) 规则将 IP 地址转换为其他 IP 地址。通常使用 NAT 规则将私有地址转换为可公开路由的地址。该转换可以从一个地址到另一个地址，或者您可以使用端口地址转换 (PAT) 将许多地址转换为一个地址，并且使用端口号区分源地址。

NAT 规则包括以下基本属性。自动 NAT 和手动 NAT 规则的属性相同，除非另行指明。

职位

为规则输入名称。名称不能包含空格。

创建规则用于

转换规则是**自动 NAT**还是**手动 NAT**。自动 NAT 比手动 NAT 简单，但是手动 NAT 允许根据目的地地址为源地址创建单独的转换。

状态

您希望该规则有效还是被禁用。

位置（仅手动 NAT。）

要添加规则的位置。可以将其插入类别中（在自动 NAT 规则之前或之后），或者所选规则的上方或下方。

Type

转换规则是**动态**还是**静态**。在实施 PAT 时，动态转换会自动从地址池中选择映射的地址或地址/端口组合。如果要精确定义映射的地址/端口，请使用静态转换。

以下主题介绍了其余的 NAT 规则属性。

自动 NAT 的数据包转换属性

使用**数据包转换**选项定义源地址和映射的转换后地址。以下属性仅适用于自动 NAT。

源接口、目的地接口

（桥接组成员接口的必选项。）应用此 NAT 规则的接口。**源**是实际接口，流量通过该接口进入设备。**目标**是映射接口，流量通过该接口离开设备。默认情况下，此规则应用于除桥接组成员接口之外的所有接口（任意）。

原始地址（始终为必填项）。

包含您要转换的源地址的网络对象。该地址必须是网络对象（而非组），而且可以是主机、或子网。

转换后的地址（通常为必填项）。

您要转换到的映射地址。您在此处选择的选项取决于定义的转换规则类型。

- **动态 NAT** - 包含映射地址的网络对象或组。该地址可以是网络对象或组，但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址，它只能包含一种类型的地址。
- **动态 PAT** - 以下项之一：
 - （接口 PAT。）要使用目的接口的 IPv4 地址，请选择**接口**。您还必须选择具体的目的接口，该接口不能是桥接组成员接口。您不能将接口 PAT 用于 IPv6。
 - 要使用目的目标接口地址以外的单个地址，请选择为此用途创建的主机网络对象。
- **静态 NAT** - 以下项之一：
 - 要使用一组地址，请选择包含映射地址的网络对象或组。该对象或组可以包含主机或子网。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。

- (具有端口转换的静态接口 NAT。) 要使用目的地接口的地址, 请选择**接口**。您还必须选择具体的目的接口, 该接口不能是桥接组成员接口。该选项配置具有端口转换的静态接口 NAT: 源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。
- **身份 NAT** - 与原始源相同的对象。或者, 您可以选择内容完全相同的其他对象。

原始端口、转换后的端口 (仅静态 NAT)。

如果需要转换 TCP 或 UDP 端口, 请选择定义原始端口和转换后的端口的端口对象。对象必须用于相同的协议。例如, 如有必要, 可以将 TCP/80 转换为 TCP/8080。

手动 NAT 的数据包转换属性 (Packet Translation Properties for Manual NAT)

使用**数据包转换**选项定义源地址和映射的转换后地址。以下属性仅适用于手动 NAT。所有选项均为可选, 除非另行指明。

源接口、目的地接口

(桥接组成员接口的必选项。) 应用此 NAT 规则的接口。**源**是实际接口, 流量通过该接口进入设备。**目标**是映射接口, 流量通过该接口离开设备。默认情况下, 此规则应用于除桥接组成员接口之外的所有接口 (任意)。

原始源地址 (始终为必填项)。

包含您要转换的地址的网络对象或组。该地址可以是网络对象或组, 而且它可以包含主机或子网。如果要转换所有原始源流量, 可以在规则中指定**任何**。

转换后的源地址 (通常为必填项。)

您要转换到的映射地址。您在此处选择的选项取决于定义的转换规则类型。

- **动态 NAT** - 包含映射地址的网络对象或组。该地址可以是网络对象或组, 但是它不能包含子网。组不能同时包含 IPv4 和 IPv6 地址, 它只能包含一种类型的地址。
- **动态 PAT** - 以下项之一:
 - (接口 PAT。) 要使用目的地接口的地址, 请选择**接口**。您还必须选择具体的目的接口, 该接口不能是桥接组成员接口。您不能将接口 PAT 用于 IPv6。
 - 要使用目的目标接口地址以外的单个地址, 请选择为此用途创建的主机网络对象。
- **静态 NAT** - 以下项之一:
 - 要使用一组地址, 请选择包含映射地址的网络对象或组。该对象或组可以包含主机或子网。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。
 - (具有端口转换的静态接口 NAT。) 要使用目的地接口的地址, 请选择**接口**。您还必须选择具体的目的接口, 该接口不能是桥接组成员接口。该选项配置具有端口转换的静态接口 NAT: 源地址/端口转换为接口的地址和相同的端口号。您不能将接口 PAT 用于 IPv6。

- **身份 NAT** - 与原始源相同的对象。或者，您可以选择内容完全相同的其他对象。

原始目的目标地址

包含目的目标地址的网络对象。如果将此留空，则无论目的目标为何都将应用源地址转换。如果指定目标目的地址，可以为该地址配置静态转换或只是为其使用将身份 NAT 用于该地址。

您可以选择**接口**以使原始目的目标基于源接口（不能为“任何”）。如果选择此选项，则还必须选择一个已转换后的目的目标对象。要为目的目标地址实施带端口转换的静态接口 NAT，请选择此选项，并为目的目标端口选择适当的端口对象。

已转换后的目的目标地址

包含已转换的数据包中使用的目的目标地址的网络对象或组。如果为**原始目的目标**选择了一个对象，则可以通过选择相同的对象确定 NAT（即无转换）。

原始源端口、转换后的源端口、原始目标端口、转换后的目标端口

为原始和已转换后的数据包定义源和目标目的服务的端口对象。您可以转换端口，或者选择同一对象以便在没有转换端口的情况下使规则敏感察觉到该服务。在配置服务时请记住以下规则：

- （动态 NAT 或 PAT。）不能对**原始源端口**和**转换后的源端口**进行转换。您可以仅对目的目标端口进行转换。
- NAT 仅支持 TCP 或 UDP。转换端口时，请确保实际和映射服务对象中的协议相同（同为 TCP 或同为 UDP）。对于身份 NAT，您可以将同一对象用于实际端口和映射端口。

高级 NAT 属性

在配置 NAT 时，可以在高级选项中配置提供专业化服务的属性。所有这些属性都是可选的：仅当需要服务时才对其进行配置。

转换与此规则匹配的 DNS 回复

是否转换 DNS 应答中的 IP 地址。对于从映射接口传输到实际接口的 DNS 回复，地址（IPv4 A 或 IPv6 AAAA）记录会从映射值重写为实际值。相反，对于从实际接口传输到映射接口的 DNS 回复，该记录会从实际值重写为映射值。此选项用于特定情况，有时 NAT64/46 转换（其中重写也会在 A 和 AAAA 记录之间转换）需要使用此选项。有关详细信息，请参阅[使用 NAT 重写 DNS 查询和响应](#)，第 361 页。如果在静态 NAT 规则中进行端口转换，则此选项不可用。

贯穿到接口 PAT（目标接口）（仅动态 NAT。）

当已分配其他映射地址后，是否将目标接口的 IP 地址用作备份方法（接口 PAT 回退）。仅当您选择不是桥接组成员的目的地接口时，此选项才可用。如果已配置了接口 PAT 配置作为转换的地址，则不能选择此选项。您不能将此选项用于 IPv6 网络。

不在目标接口上使用代理 ARP (Do not proxy ARP on Destination Interface)（仅静态 NAT。）

为映射 IP 地址的传入数据包禁用代理 ARP。如果使用与映射接口相同的网络中的地址，则系统会使用代理 ARP 来应答映射地址的任何 ARP 请求，从而拦截以映射地址为目的地的流量。此解决方案可以简化路由，因为设备不必是任何其他网络的网关。如果需要，可以禁用代理 ARP，在此情况下需要确保在上游路由器上具有正确的路由。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。

对目的目标接口执行路由查找（仅静态身份 NAT。仅路由模式。）

如果在为原始源地址和已转换源地址选择同一对象时选择源接口和目标接口，则可以选择此选项，以使系统根据路由表而不是使用在 NAT 规则中配置的目标接口来确定目标接口。

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手动 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，无法在手动 NAT 规则中启用 DNS 重写，所以最好创建两个自动 NAT 规则。



注释 NAT46 仅支持静态映射。

- NAT66 - 将 IPv6 数据包转换为不同的 IPv6 地址。我们建议使用静态 NAT。尽管可以使用 NAT 或 PAT，但由于 IPv6 地址大量供应，因此不必使用动态 NAT。



注释 NAT64 和 NAT 46 仅可以在标准路由接口上使用。NAT66 可在路由接口和桥接组成员接口上使用。

NAT64/46：将 IPv6 地址转换为 IPv4 地址

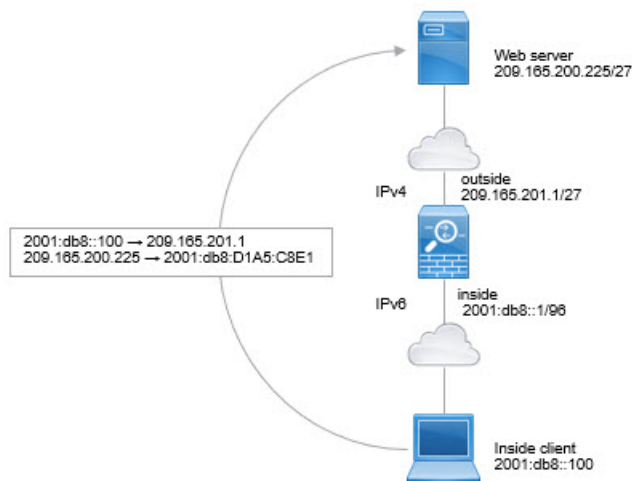
当流量从 IPv6 网络进入仅 IPv4 网络时，您需要将 IPv6 地址转换为 IPv4 地址，并将流量从 IPv4 返回 IPv6。您需要定义两个地址池，一个 IPv4 地址池用于绑定 IPv4 网络中的 IPv6 地址，另一个 IPv6 地址池用于绑定 IPv6 网络中的 IPv4 地址。

- NAT64 规则的 IPv4 地址池一般较小，通常可能没有足够的地址与 IPv6 客户端地址一对一映射。与动态或静态 NAT 相比，动态 PAT 可以更容易满足可能的大量 IPv6 客户端地址需要。
- NAT46 规则的 IPv6 地址池可以等于或大于要映射的 IPv4 地址数。这允许每个 IPv4 地址映射到不同的 IPv6 地址。NAT46 仅支持静态映射，因此您不能使用动态 PAT。

您需要定义两个策略，一个用于源 IPv6 网络，一个用于目的地 IPv4 网络。虽然您可以使用单一手动 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，无法在手动 NAT 规则中启用 DNS 重写，所以最好创建两个自动 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，以便可以在单个手动 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。

- a) 选择对象 (Objects)。
- b) 从目录中选择网络，然后点击 +。
- c) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），选择网络，然后输入网络地址 2001:db8::/96。

Add Network Object

Name
inside_v6

Description

Type
 Network Host

Network
2001:DB8::/96

d) 点击确定。

步骤 2 创建手动 NAT 规则以将 IPv6 网络转换为 IPv4 并再次返回。

- a) 依次选择 **策略 > NAT**。
- b) 点击 **+** 按钮。
- c) 配置以下属性：
 - 标题 = PAT64Rule（或您选择的其他名称）。
 - 创建规则的对象 = 手动 NAT。
 - 位置 = 自动 NAT 规则之前
 - 类型 = 动态。
 - 源接口 = 内部。
 - 目的接口 = 外部。
 - 原始数据包源地址 = inside_v6 网络对象。
 - 转换后数据包源地址 = 接口。此选项使用目的接口的 IPv4 地址作为 PAT 地址。
 - 原始数据包目的地址 = inside_v6 网络对象。
 - 转换后数据包目的地址 = any-ipv4 网络对象。

Title	Create Rule for	Status
PAT64Rule	Manual NAT	<input checked="" type="checkbox"/>

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement	Type
Before Auto NAT Rules	Dynamic

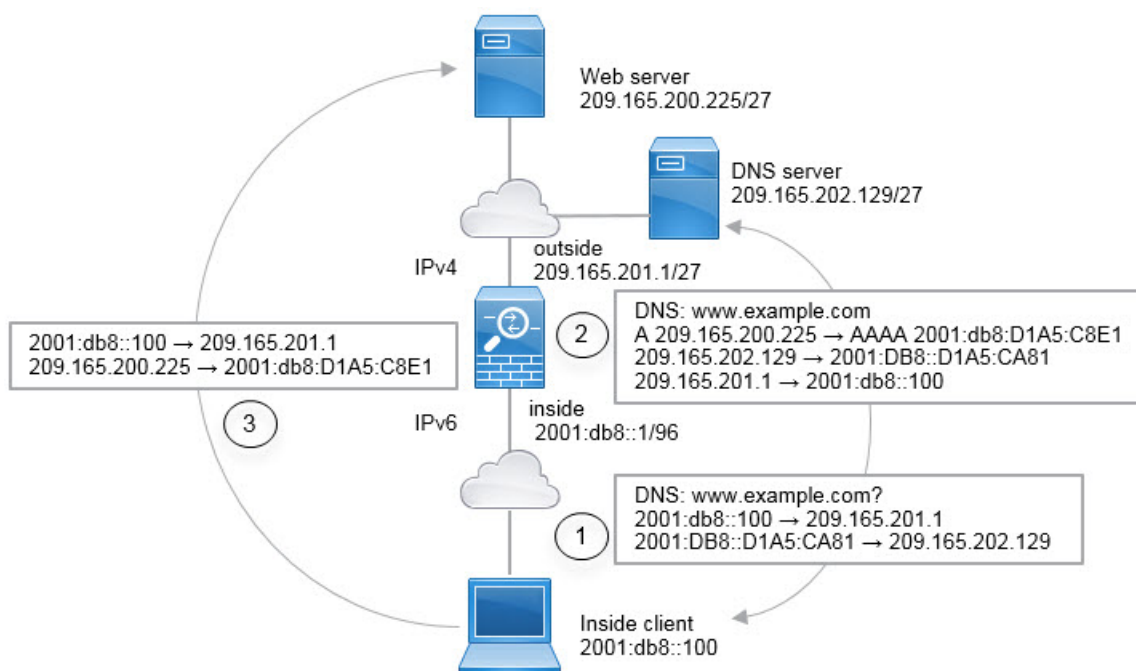
Packet Translation		Advanced Options	
ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	Source Address	Destination Interface	Source Address
inside	inside_v6	outside	Interface
Source Port	Destination Address	Source Port	Destination Port
Any	inside_v6	Any	any-ipv4
Destination Port		Destination Port	
Any		Any	

d) 点击**确定**。

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 请求中的源和目的如下转换：
 - 2001:DB8::100 转换为 209.156.101.54 上的唯一端口（NAT64 接口 PAT 规则。）

- 2001:db8:D1A5:C8E1 转换为 209.165.200.225（NAT46 规则。）

以下步骤程序介绍了如何配置此示例。

过程

步骤 1 创建定义内部 IPv6 网络和外部 IPv4 网络的网络对象。

- a) 选择对象 (**Objects**)。
- b) 从目录中选择**网络**，然后点击 +。
- c) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:db8::/96。

Add Network Object

Name
inside_v6

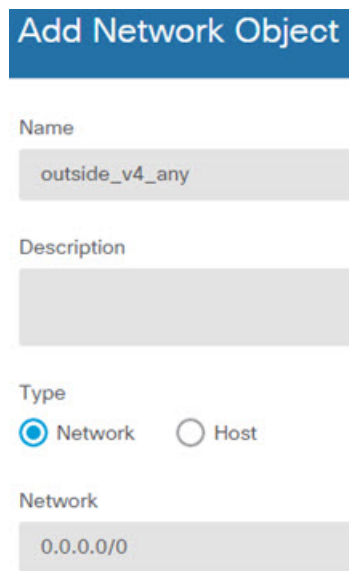
Description

Type
 Network Host

Network
2001:DB8::/96

- d) 点击**确定**。
- e) 点击 + 并定义外部 IPv4 网络。

为网络对象命名（例如，outside_v4_any），选择**网络**，然后输入网络地址 0.0.0.0/0。



Add Network Object

Name
outside_v4_any

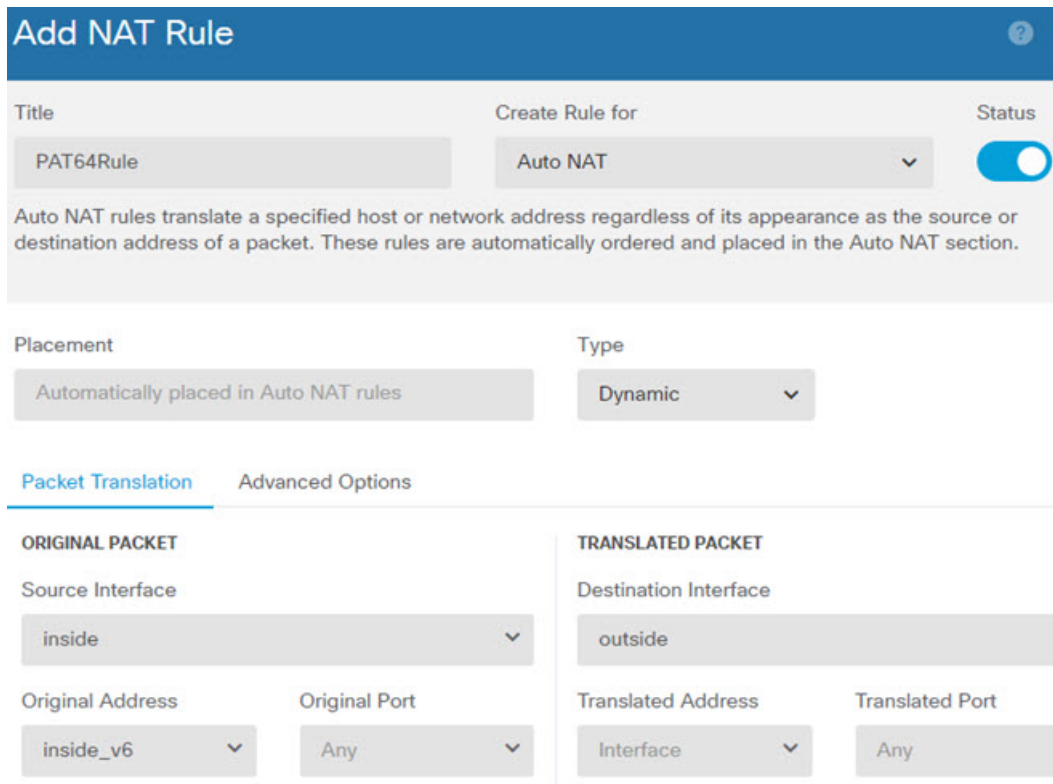
Description

Type
 Network Host

Network
0.0.0.0/0

步骤 2 为内部 IPv6 网络配置 NAT64 动态 PAT 规则。

- a) 依次选择 **策略 > NAT**。
- b) 点击 **+** 按钮。
- c) 配置以下属性：
 - 标题 = PAT64Rule（或您选择的其他名称）。
 - 创建规则的对象 = 自动 NAT。
 - 类型 = 动态。
 - 源接口 = 内部。
 - 目的接口 = 外部。
 - 原始地址 = inside_v6 网络对象。
 - 转换后的地址 = 接口。此选项使用目的接口的 IPv4 地址作为 PAT 地址。



Add NAT Rule

Title: PAT64Rule Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Dynamic

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	inside	Destination Interface	outside
Original Address	inside_v6	Translated Address	Interface
Original Port	Any	Translated Port	Any

d) 点击确定。

使用此规则时，从内部接口上的 2001:db8::/96 子网流向外部接口的任何流量都将接受使用外部接口 IPv4 地址进行的 NAT64 PAT 转换。

步骤 3 为外部 IPv4 网络配置静态 NAT46 规则。

a) 点击 + 按钮。

b) 配置以下属性：

- 标题 = NAT46Rule（或您选择的其他名称）。
- 创建规则的对象 = 自动 NAT。
- 类型 = 静态。
- 源接口 = 外部。
- 目的接口 = 内部。
- 原始地址 = outside_v4_any 网络对象。
- 转换后的地址 = inside_v6 网络对象。
- 在高级选项选项卡中，选择转换与此规则匹配的 DNS 回复。

c) 点击确定。

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。

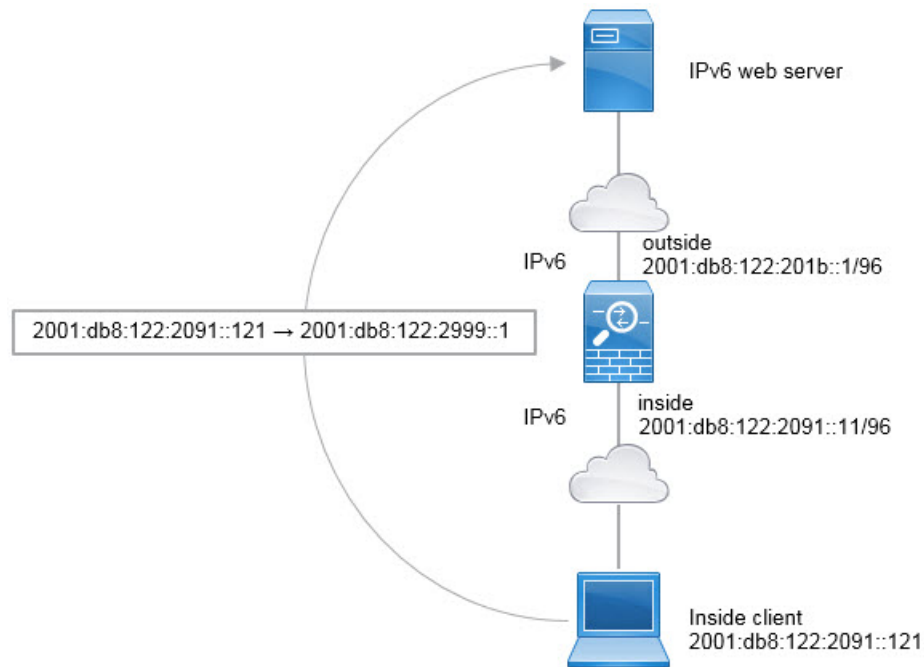
NAT66: 将 IPv6 地址转换为不同的 IPv6 地址

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。使用自动 NAT 可轻松地对这些规则建模。但是，如果不想允许返回流量，您可以仅使用手动 NAT 将静态 NAT 规则设为单向。

NAT66 示例：网络间的静态转换

您可以使用自动 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。



注释 此示例假定，内部接口不是桥接组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

步骤 1 创建定义内部 IPv6 网络和外部 IPv6 NAT 网络的网络对象。

- a) 选择对象 (**Objects**)。
- b) 从目录中选择**网络**，然后点击 +。
- c) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:db8:122:2091::/96。

Add Network Object

Name
inside_v6

Description

Type
 Network Host

Network
2001:db8:122:2091::/96

- d) 点击**确定**。
- e) 点击**+** 并定义外部 IPv6 NAT 网络。

为网络对象命名（例如，outside_nat_v6），选择**网络**，然后输入网络地址 2001:db8:122:2999::/96。

Add Network Object

Name
outside_nat_v6

Description

Type
 Network Host

Network
2001:db8:122:2999::/96

步骤 2 为内部 IPv6 网络配置静态 NAT 规则。

- a) 依次选择 **策略 > NAT**。
- b) 点击 **+** 按钮。
- c) 配置以下属性：
 - 标题 = NAT66Rule（或您选择的其他名称）。
 - 创建规则的对象 = 自动 NAT。

- 类型 = 静态。
- 源接口 = 内部。
- 目的接口 = 外部。
- 原始地址 = inside_v6 网络对象。
- 转换后的地址 = outside_nat_v6 网络对象。

Add NAT Rule ?

Title NAT66Rule	Create Rule for Auto NAT	Status <input checked="" type="checkbox"/>
--------------------	-----------------------------	---

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement Automatically placed in Auto NAT rules	Type Static
---	----------------

Packet Translation

Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface inside	Destination Interface outside	Translated Address outside_nat_v6	Translated Port Any
Original Address inside_v6	Original Port Any		

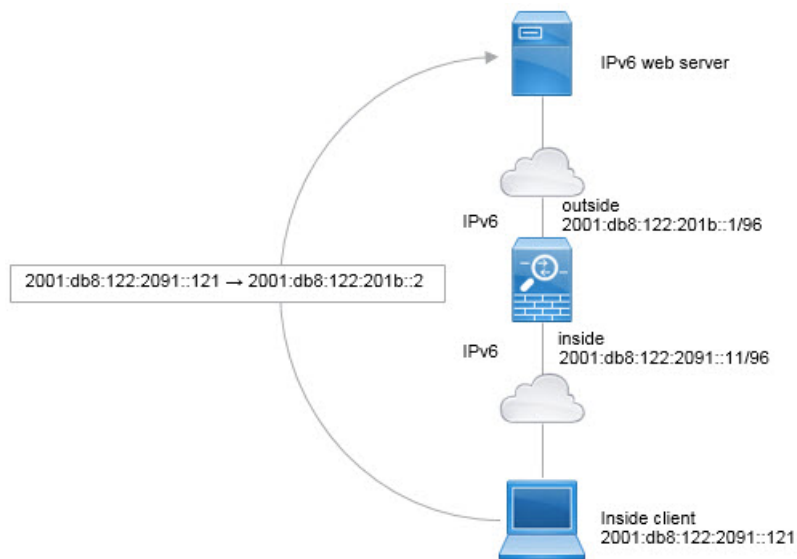
d) 点击确定。

使用此规则，从内部接口上的 2001:db8:122:2091::/96 子网到外部接口的任何流量都会经静态 NAT66 转换为 2001:db8:122:2999::/96 网络上的地址。

NAT66 示例：简单 IPv6 接口 PAT

实施 NAT66 的一个简单方法是将内部地址动态分配给外部接口 IPv6 地址上的不同端口。

不过，无法通过 Firepower 设备管理器使用接口的 IPv6 地址配置接口 PAT。相反，要使用同一网络中的一个空闲地址作为动态 PAT 池。



注释 此示例假定，内部接口不是桥接组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

步骤 1 创建定义内部 IPv6 网络和 IPv6 PAT 地址的网络对象。

- a) 选择对象 (Objects)。
- b) 从目录中选择网络，然后点击 +。
- c) 定义内部 IPv6 网络。

为网络对象命名（例如，inside_v6），选择网络，然后输入网络地址 2001:db8:122:2091::/96。

Add Network Object

Name
inside_v6

Description

Type
 Network Host

Network
2001:db8:122:2091::/96

- d) 点击**确定**。
- e) 点击**+** 并定义外部 IPv6 PAT 地址。
为网络对象命名（例如，ipv6_pat），选择**主机**，然后输入主机地址 2001:db8:122:201b::2。

Add Network Object

Name
ipv6_pat

Description

Type
 Network Host

Host
2001:db8:122:201b::2

步骤 2 为内部 IPv6 网络配置动态 PAT 规则。

- 依次选择 **策略 > NAT**。
- 点击 **+** 按钮。
- 配置以下属性：
 - 标题 = PAT66Rule（或您选择的其他名称）。
 - 创建规则的对象 = 自动 NAT。

- 类型 = 动态。
- 源接口 = 内部。
- 目的接口 = 外部。
- 原始地址 = inside_v6 网络对象。
- 转换后的地址 = ipv6_pat 网络对象。

Add NAT Rule ?

Title	Create Rule for	Status
PAT66Rule	Auto NAT ▼	<input checked="" type="checkbox"/>

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Dynamic ▼

Packet Translation

Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	Destination Interface		
inside ▼	outside		
Original Address	Original Port	Translated Address	Translated Port
inside_v6 ▼	Any ▼	ipv6_pat ▼	Any

d) 点击确定。

使用此规则，从内部接口上的 2001:db8:122:2091::/96 子网到外部接口的任何流量都会经动态 PAT66 转换为 2001:db8:122:201b::2 上的端口。

监控 NAT

要监控和故障排除 NAT 连接，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。

- **show nat** 显示 NAT 规则和每个规则的命中计数点击数。还有其他关键字可用于显示 NAT 的其他方面信息。
- **show xlate** 显示当前处于活动状态的实际 NAT 转换。

- **clear xlate** 允许删除处于活动状态的 NAT 转换。如果更改 NAT 规则，您可能需要删除活动的转换，因为现有连接继续使用旧的转换槽，直到连接结束。清除转换允许系统根据您的新规则，在客户端的下一连接尝试中为客户端构建新的转换。（您无法在 CLI 控制台中使用此命令。）

NAT 示例

以下主题提供了在威胁防御设备上配置 NAT 的示例。

提供对内部 Web 服务器的访问权限（静态自动 NAT）

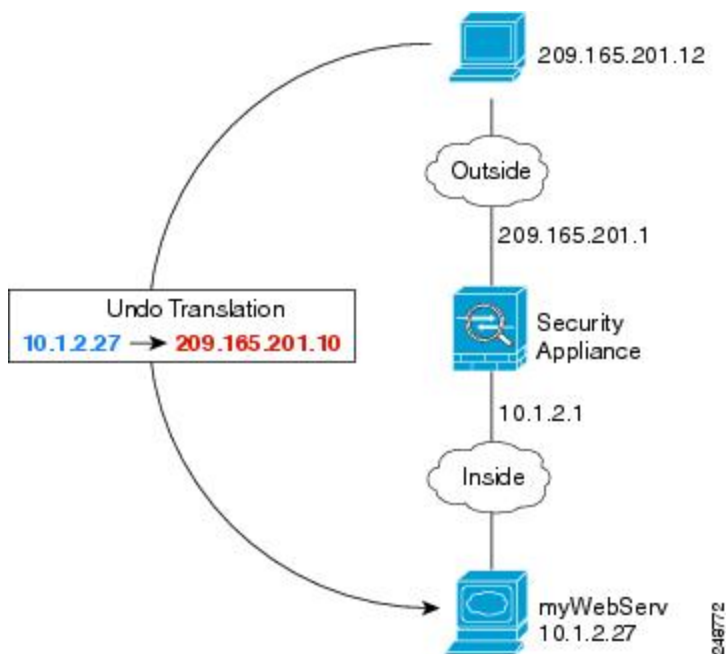
以下示例为内部 Web 服务器执行静态 NAT。实际地址位于专用网络上，因此公共地址是必需的。需要静态 NAT，以便主机能够在固定地址发起到 Web 服务器的流量。



注释

此示例假定，内部接口不是桥接组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，请选择 Web 服务器连接到的具体桥接组成员接口，例如 `inside1_3`。

图 19: 面向内部 Web 服务器的静态 NAT



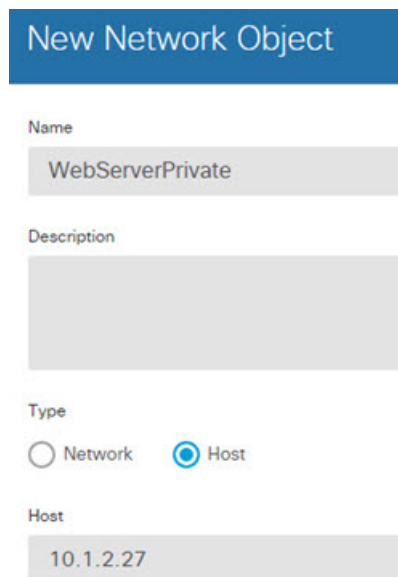
过程

步骤 1 创建定义服务器私有和公共主机地址的网络对象。

a) 选择对象 (Objects)。

- b) 从目录中选择网络，然后单击 +。
- c) 定义 Web 服务器的私有地址。

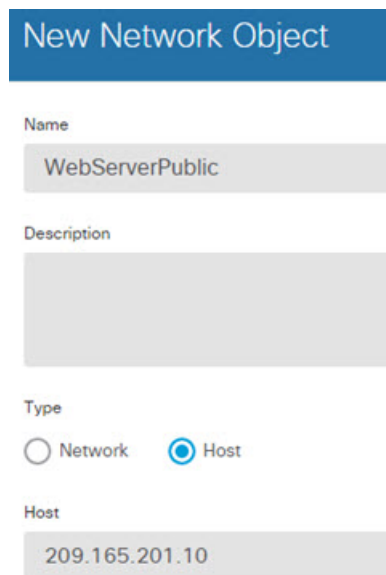
为网络对象命名（例如，WebServerPrivate），选择主机 (Host)，然后输入实际主机 IP 地址 10.1.2.27。



The screenshot shows the 'New Network Object' configuration form. The 'Name' field contains 'WebServerPrivate'. The 'Description' field is empty. Under the 'Type' section, the 'Host' radio button is selected. The 'Host' field contains the IP address '10.1.2.27'.

- d) 单击确定。
- e) 单击 + 并定义公共地址。

为网络对象命名（例如，WebServerPublic），选择主机，然后输入实际主机地址 209.165.201.10。



The screenshot shows the 'New Network Object' configuration form. The 'Name' field contains 'WebServerPublic'. The 'Description' field is empty. Under the 'Type' section, the 'Host' radio button is selected. The 'Host' field contains the IP address '209.165.201.10'.

- f) 单击确定。

步骤 2 配置对象的静态 NAT。

- a) 依次选择 策略 > NAT。
- b) 点击 + 按钮。
- c) 配置以下属性：
 - 标题 = WebServer（或您选择的其他名称）。
 - 创建规则的对象 = 自动 NAT。
 - 类型 = 静态。
 - 源接口 = 内部。
 - 目的接口 = 外部。
 - 原始地址 = WebServerPrivate 网络对象。
 - 转换后的地址 = WebServerPublic 网络对象。

Add NAT Rule

Title: WebServer

Create Rule for: Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules

Type: Static

Packet Translation | Advanced Options

Original Packet

Source Interface: inside

Original Address: WebServerPrivat

Original Port: Any

Translated Packet

Destination Interface: outside

Translated Address: WebServerPublic

Translated Port: Any

- d) 单击 **OK**。

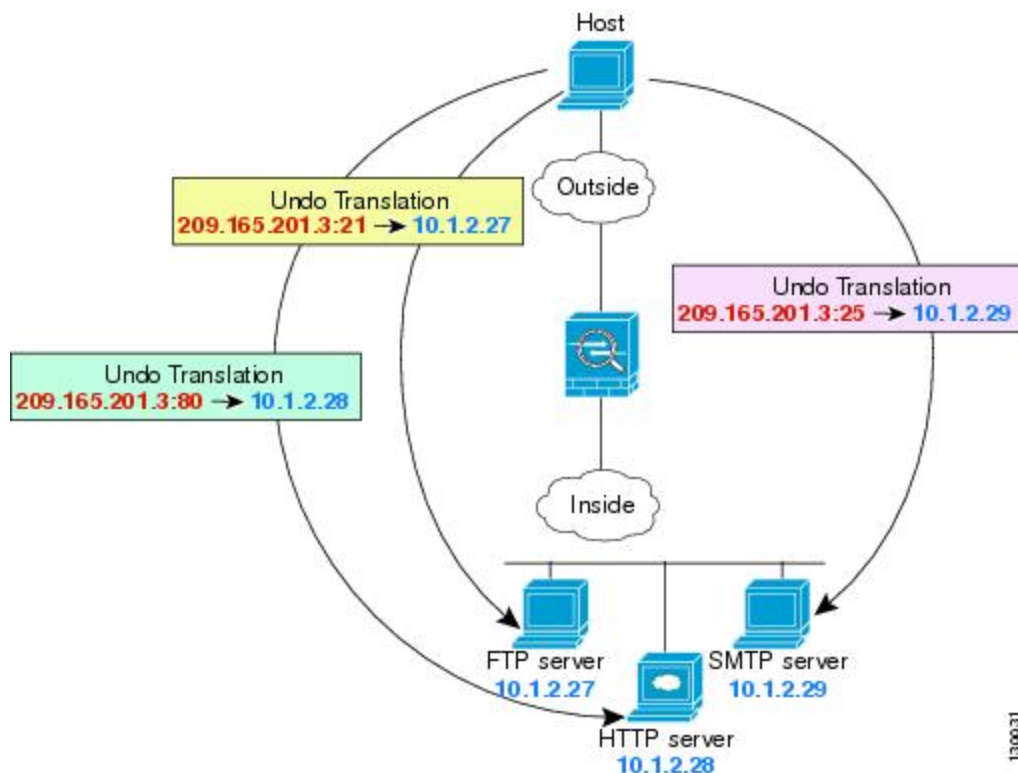
FTP、HTTP 和 SMTP 的单个地址（具有端口转换的静态自动 NAT）

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。



注释 此示例假设内部接口是连接到交换机的标准路由接口，其中服务器连接到交换机。如果您的内部接口是桥接组接口 (BVI)，并且服务器连接到单独的桥接组成员接口，请选择对于相应规则，每个服务器连接的特定成员接口。例如，规则的源接口可能有 inside1_2、inside1_3 和 inside1_4，而不是 inside。

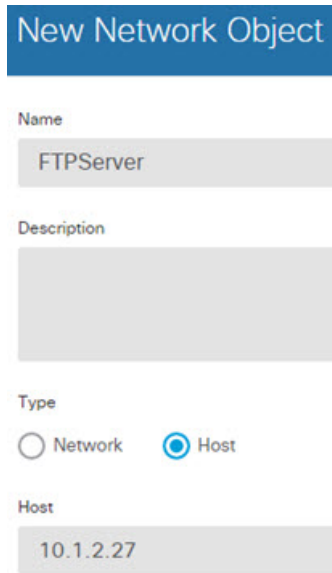
图 20: 支持端口转换的静态 NAT



过程

步骤 1 为 FTP 服务器创建网络对象。

- a) 选择对象 (Objects)。
- b) 从目录中选择网络，然后点击 +。
- c) 为网络对象命名（例如，FTPserver），选择主机 (Host)，然后输入 FTP 服务器的实际 IP 地址 10.1.2.27。



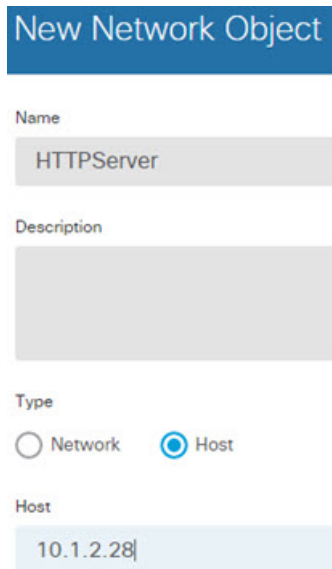
The screenshot shows the 'New Network Object' configuration form. The 'Name' field contains 'FTPServer'. The 'Description' field is empty. Under the 'Type' section, the 'Host' radio button is selected. The 'Host' field contains the IP address '10.1.2.27'.

d) 点击确定。

步骤 2 为 HTTP 服务器创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，HTTPserver），选择主机，然后输入实际主机地址 10.1.2.28。



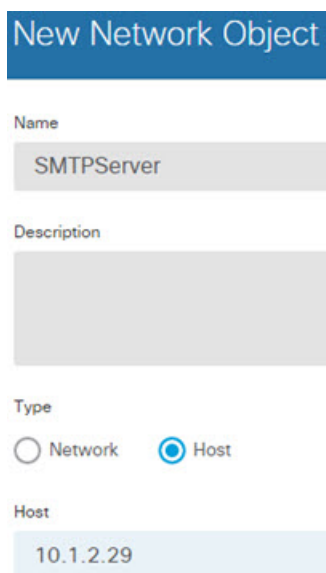
The screenshot shows the 'New Network Object' configuration form. The 'Name' field contains 'HTTPServer'. The 'Description' field is empty. Under the 'Type' section, the 'Host' radio button is selected. The 'Host' field contains the IP address '10.1.2.28'.

c) 点击确定。

步骤 3 为 SMTP 服务器创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，SMTPserver），选择主机，然后输入实际主机地址 10.1.2.29。



New Network Object

Name
SMTPServer

Description

Type
 Network Host

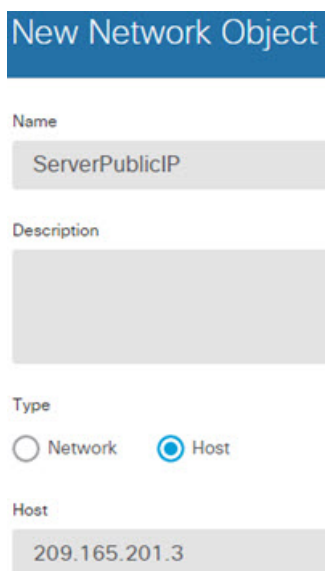
Host
10.1.2.29

c) 点击确定。

步骤 4 为用于三台服务器的公共 IP 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，ServerPublicIP），选择主机，然后输入实际主机地址 209.165.201.3。



New Network Object

Name
ServerPublicIP

Description

Type
 Network Host

Host
209.165.201.3

c) 点击确定。

步骤 5 为 FTP 服务器配置具有端口转换的静态 NAT，并将 FTP 端口映射到其自身。

a) 依次选择 策略 > NAT。

b) 点击 + 按钮。

c) 配置以下属性：

- 标题 = FTPServer（或您选择的其他名称）。
- 创建规则的对象 = 自动 NAT。
- 类型 = 静态。
- 源接口 = 内部。
- 目的接口 = 外部。
- 原始地址 = FTPserver 网络对象。
- 转换后的地址 = ServerPublicIP 网络对象。
- 原始端口 = FTP 端口对象。
- 转换后的端口 = FTP 端口对象。

Add NAT Rule

Title: FTPServer

Create Rule for: Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules

Type: Static

Packet Translation | Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	outside
Original Address	FTPServer	Translated Address	ServerPublicIP
Original Port	FTP	Translated Port	FTP

d) 点击确定。

步骤 6 为 HTTP 服务器配置支持端口转换的静态 NAT，并将 HTTP 端口映射到其自身。

- 点击 + 按钮。
- 配置以下属性：
 - 标题 = HTTPServer（或您选择的其他名称）。
 - 创建规则的对象 = 自动 NAT。
 - 类型 = 静态。

- 源接口 = 内部。
- 目的接口 = 外部。
- 原始地址 = HTTPserver 网络对象。
- 转换后的地址 = ServerPublicIP 网络对象。
- 原始端口 = HTTP 端口对象。
- 转换后的端口 = HTTP 端口对象。

Add NAT Rule

Title: HTTPServer Create Rule for: Auto NAT

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

Packet Translation Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	outside
Original Address	HTTPServer	Translated Address	ServerPublicIP
Original Port	HTTP	Translated Port	HTTP

c) 点击确定。

步骤 7 为 SMTP 服务器配置支持端口转换的静态 NAT，并将 SMTP 端口映射到其自身。

a) 点击 + 按钮。

b) 配置以下属性：

- 标题 = SMTPServer（或您选择的其他名称）。
- 创建规则的对象 = 自动 NAT。
- 类型 = 静态。
- 源接口 = 内部。
- 目的接口 = 外部。
- 原始地址 = SMTPserver 网络对象。

- 转换后的地址 = ServerPublicIP 网络对象。
- 原始端口 = SMTP 端口对象。
- 转换后的端口 = SMTP 端口对象。

c) 单击 **OK**。

转换因目的而异（动态手动 PAT）

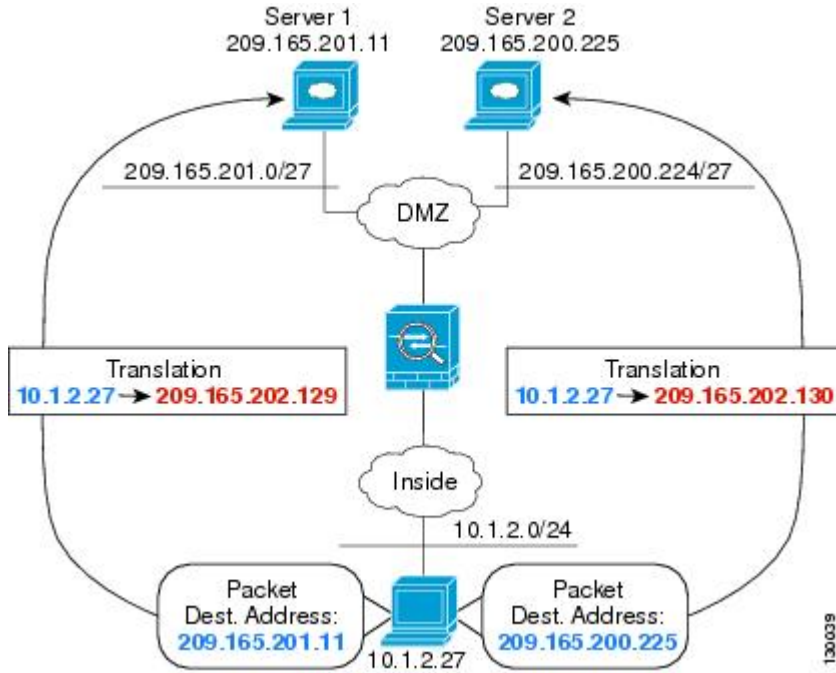
下图显示 10.1.2.0/24 网络上的一台主机正在访问两台不同的服务器。当主机访问位于 209.165.201.11 的服务器时，实际地址将转换为 209.165.202.129:port。当主机访问位于 209.165.200.225 的服务器时，实际地址将转换为 209.165.202.130:port。



注释

此示例假设内部接口是连接到交换机的标准路由接口，其中服务器连接到交换机。如果您的内部接口是桥接组接口 (BVI)，并且服务器连接到单独的桥接组成员接口，请选择对于相应规则，每个服务器连接的特定成员接口。例如，对于源接口而言，规则可能有 `inside1_2` 和 `inside1_3`，而非 `inside`。

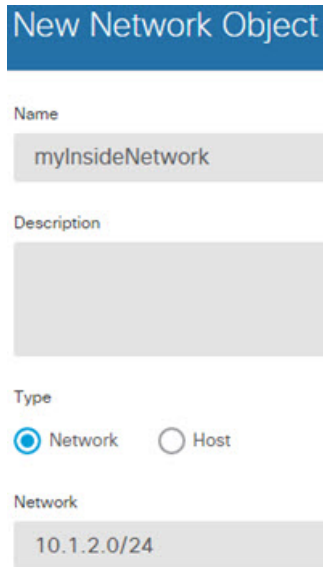
图 21: 具有不同目标地址的手动 NAT



过程

步骤 1 为内部网络创建网络对象。

- a) 选择对象 (**Objects**)。
- b) 从目录中选择网络，然后点击 +。
- c) 为网络对象命名（例如，myInsideNetwork），选择网络 (**Network**)，然后输入实际网络地址 10.1.2.0/24。



New Network Object

Name
myInsideNetwork

Description

Type
 Network Host

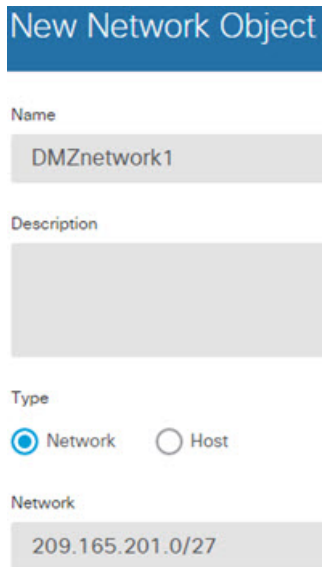
Network
10.1.2.0/24

d) 点击**确定**。

步骤 2 为 DMZ 网络 1 创建网络对象。

a) 点击**+**。

b) 为网络对象命名（例如，DMZnetwork1），选择**网络**，然后输入网络地址 209.165.201.0/27（子网掩码为 255.255.255.224）。



New Network Object

Name
DMZnetwork1

Description

Type
 Network Host

Network
209.165.201.0/27

c) 点击**确定**。

步骤 3 为 DMZ 网络 1 的 PAT 地址创建网络对象。

a) 点击**+**。

b) 为网络对象命名（例如，PATaddress1），选择**主机**，然后输入主机地址 209.165.202.129。

New Network Object

Name

PATaddress1

Description

Type

 Network Host

Host

209.165.202.129

c) 点击确定。

步骤 4 为 DMZ 网络 2 创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，DMZnetwork2），选择网络，然后输入网络地址 209.165.200.224/27（子网掩码为 255.255.255.224）。

New Network Object

Name

DMZnetwork2

Description

Type

 Network Host

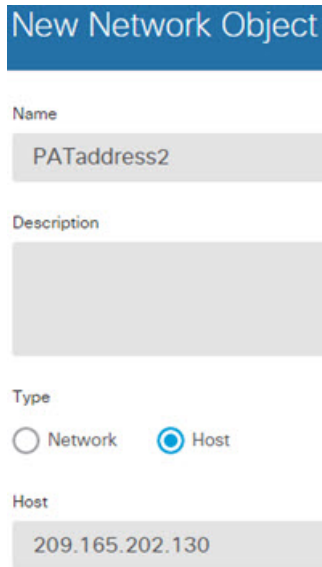
Network

209.165.200.224/27

c) 点击确定。

步骤 5 为 DMZ 网络 2 的 PAT 地址创建网络对象。

- a) 点击 +。
- b) 为网络对象命名（例如，PATaddress2），选择主机，然后输入主机地址 209.165.202.130。



New Network Object

Name
PATaddress2

Description

Type
 Network Host

Host
209.165.202.130

- c) 点击确定。

步骤 6 为 DMZ 网络 1 配置动态手动 PAT。

- a) 依次选择 **策略 > NAT**。
- b) 点击 + 按钮。
- c) 配置以下属性：
 - 标题 = DMZNetwork1（或您选择的其他名称）。
 - 创建规则的对象 = 手动 NAT。
 - 类型 = 动态。
 - 源接口 = 内部。
 - 目的接口 = dmz。
 - 原始源地址 = myInsideNetwork 网络对象。
 - 转换后的源地址 = PATaddress1 网络对象。
 - 原始目标地址 = DMZnetwork1 网络对象。
 - 转换后的目标地址 = DMZnetwork1 网络对象。

注释 由于您不需要转换目的地址，因此需要通过为原始目的地址和转换后的目的地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。

Add NAT Rule

Title: DMZNetwork1 Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules Type: Dynamic

Packet Translation Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATaddress1
Source Port	Any	Source Port	Any
Destination Address	DMZnetwork1	Destination Address	DMZnetwork1
Destination Port	Any	Destination Port	Any

d) 点击确定。

步骤 7 为 DMZ 网络 2 配置动态手动 PAT。

a) 点击 + 按钮。

b) 配置以下属性：

- 标题 = DMZNetwork2（或您选择的其他名称）。
- 创建规则的对象 = 手动 NAT。
- 类型 = 动态。
- 源接口 = 内部。
- 目的接口 = dmz。
- 原始源地址 = myInsideNetwork 网络对象。
- 转换后的源地址 = PATaddress2 网络对象。
- 原始目标地址 = DMZnetwork2 网络对象。
- 转换后的目标地址 = DMZnetwork2 网络对象。

Add NAT Rule

Title: DMZNetwork2

Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules

Type: Dynamic

Packet Translation | Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATaddress2
Source Port	Any	Source Port	Any
Destination Address	DMZnetwork2	Destination Address	DMZnetwork2
Destination Port	Any	Destination Port	Any

c) 单击 **OK**。

转换因目的地址和端口而异（动态手动 PAT）

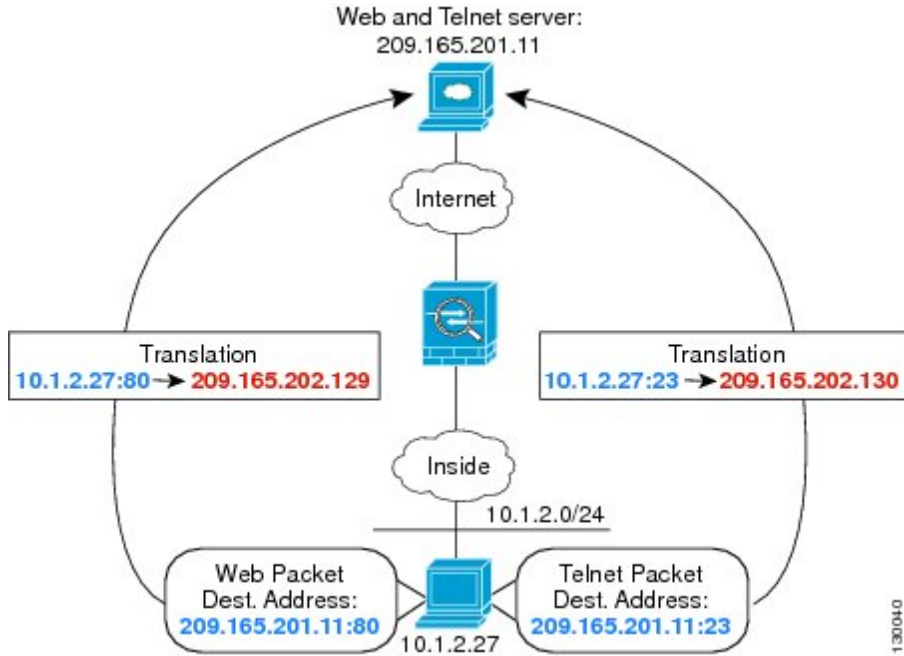
下图显示源端口和目的端口的使用情况。10.1.2.0/24 网络上的主机同时因为网络服务和 Telnet 服务访问单个主机。当主机进行 Telnet 服务访问服务器时，实际地址将转换为 209.165.202.129:port。当主机进行网络服务访问相同服务器时，真实地址将转换为 209.165.202.130:port。



注释

此示例假设内部接口是连接到交换机的标准路由接口，其中服务器连接到交换机。如果内部接口是桥接组接口 (BVI) 而服务器连接到某个桥接组成员接口，请选择服务器连接到的具体成员接口。例如，该规则可能以 inside1_2 而非“内部”作为源接口。

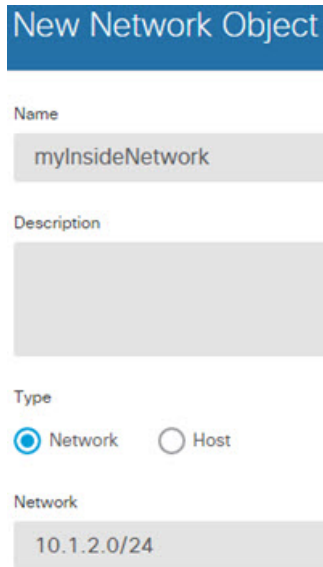
图 22: 具有不同目标端口的手动 NAT



过程

步骤 1 为内部网络创建网络对象。

- 选择对象 (Objects)。
- 从目录中选择网络，然后点击 +。
- 为网络对象命名（例如，myInsideNetwork），选择网络 (Network)，然后输入实际网络地址 10.1.2.0/24。



New Network Object

Name
myInsideNetwork

Description

Type
 Network Host

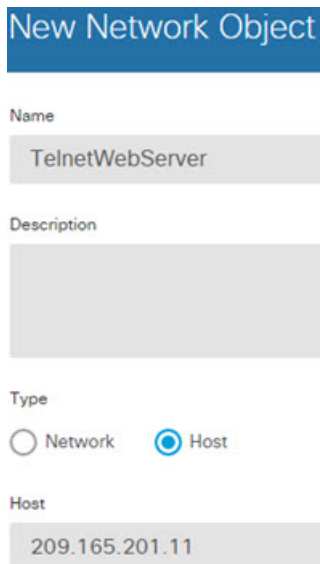
Network
10.1.2.0/24

d) 点击确定。

步骤 2 为 Telnet/Web 服务器创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，TelnetWebServer），选择主机，然后输入实际主机地址 209.165.201.11。



New Network Object

Name
TelnetWebServer

Description

Type
 Network Host

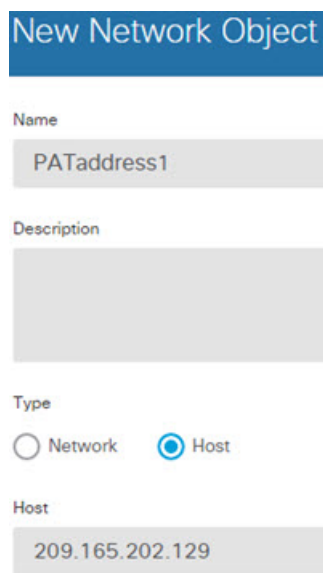
Host
209.165.201.11

c) 点击确定。

步骤 3 使用 Telnet 时为 PAT 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，PATaddress1），选择主机，然后输入主机地址 209.165.202.129。



New Network Object

Name
PATAddress1

Description

Type
 Network Host

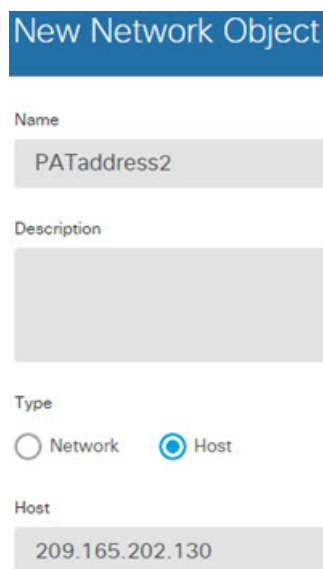
Host
209.165.202.129

c) 点击确定。

步骤 4 使用 HTTP 时为 PAT 地址创建网络对象。

a) 点击 +。

b) 为网络对象命名（例如，PATAddress2），选择主机，然后输入主机地址 209.165.202.130。



New Network Object

Name
PATAddress2

Description

Type
 Network Host

Host
209.165.202.130

c) 点击确定。

步骤 5 为 Telnet 访问创建动态手动 PAT。

a) 依次选择 **策略 > NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- 标题 = TelnetServer（或您选择的其他名称）。
- 创建规则的对象 = 手动 NAT。
- 类型 = 动态。
- 源接口 = 内部。
- 目的接口 = dmz。
- 原始源地址 = myInsideNetwork 网络对象。
- 转换后的源地址 (**Translated Source Address**) = PATAddress1 网络对象。
- 原始目标地址 = TelnetWebServer 网络对象。
- 转换后的目标地址 = TelnetWebServer 网络对象。
- 原始目的端口 = TELNET 端口对象。
- 转换后的目的端口 = TELNET 端口对象。

注释 由于您不需要转换目标地址或端口，因此需要通过为原始目标地址和转换后的目标地址指定相同的地址，以及为原始端口和转换后的端口指定相同的端口，从而为它们配置身份 NAT。

Add NAT Rule

Title: TelnetServer

Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules

Type: Dynamic

Packet Translation | Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATAddress1
Source Port	Any	Source Port	Any
Destination Address	TelnetWebServe	Destination Address	TelnetWebServe
Destination Port	TELNET	Destination Port	TELNET

d) 点击确定。

步骤 6 为 Web 访问创建动态手动 PAT。

a) 点击 + 按钮。

b) 配置以下属性：

- 标题 = WebServer（或您选择的其他名称）。
- 创建规则的对象 = 手动 NAT。
- 类型 = 动态。
- 源接口 = 内部。
- 目的接口 = dmz。
- 原始源地址 = myInsideNetwork 网络对象。
- 转换后的源地址 = PATaddress2 网络对象。
- 原始目标地址 = TelnetWebServer 网络对象。
- 转换后的目标地址 = TelnetWebServer 网络对象。
- 原始目的端口 = HTTP 端口对象。
- 转换后的目的端口 = HTTP 端口对象。

Add NAT Rule

Title: WebServer

Create Rule for: Manual NAT

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules

Type: Dynamic

Packet Translation | Advanced Options

Original Packet		Translated Packet	
Source Interface	inside	Destination Interface	dmz
Source Address	myInsideNetwork	Source Address	PATAddress2
Source Port	Any	Source Port	Any
Destination Address	TelnetWebServe	Destination Address	TelnetWebServe
Destination Port	HTTP	Destination Port	HTTP

c) 单击 **OK**。

使用 NAT 重写 DNS 查询和响应

可能需要配置 Firepower 威胁防御设备以修改 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，适用于反向 DNS 查询的 PTR 记录）。对于从映射接口穿越到任何其他接口的 DNS 应答，记录会从映射值被重写为实际值。相反，对于从任何接口穿越到映射接口的 DNS 应答，记录会从实际值被重写为映射值。

以下是需要在 NAT 规则上配置 DNS 重写的几种主要情况。

- 规则为 NAT64 或 NAT46，并且 DNS 服务器位于外部网络上。您需要进行 DNS 重写以实现 DNS A 记录（适用于 IPv4）和 AAAA 记录（适用于 IPv6）之间的转换。
- DNS 服务器在外部，客户端在内部，并且客户端使用的一些完全限定域名解析到其他内部主机。
- DNS 服务器在内部并以专用 IP 地址进行响应，客户端在外部，并且客户端访问指向内部托管的服务器的完全限定域名。

DNS 重写限制

以下是 DNS 重写的某些限制：

- DNS 重写不适用于 PAT，因为多条 PAT 规则适用于每个 A 或 AAAA 记录，而要使用的 PAT 规则不确定。
- 如果您配置了手动 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，Firepower 威胁防御设备将精确匹配 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。
- 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 64 回复修改

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。

Add Network Object

Name

ftp_server

Description

Type

Network Host

Host

209.165.200.225

- d) 点击**确定**。
- e) 点击 **+** 并定义 DNS 服务器的实际地址。
为网络对象命名（例如，dns_server），选择**主机**，然后输入主机地址 209.165.201.15。

Add Network Object

Name

dns_server

Description

Type

Network Host

Host

209.165.201.15

- f) 点击**确定**。
- g) 点击 **+** 并定义内部 IPv6 网络。
为网络对象命名（例如，inside_v6），选择**网络**，然后输入网络地址 2001:DB8::/96。

Add Network Object

Name
inside_v6

Description

Type
 Network Host

Network
2001:DB8::/96

- h) 点击**确定**。
- i) 点击 **+** 并为内部 IPv6 网络定义 IPv4 PAT 地址。
为网络对象命名（例如，ipv4_pat），选择**主机**，然后输入主机地址 209.165.200.230。

Add Network Object

Name
ipv4_pat

Description

Type
 Network Host

Host
209.165.200.230

- j) 点击**确定**。

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

- a) 依次选择 **策略 > NAT**。
- b) 点击 **+** 按钮。
- c) 配置以下属性：
- **标题** = FTPServer（或您选择的其他名称）。

- 创建规则的对象 = 自动 NAT。
- 类型 = 静态。
- 源接口 = 外部。
- 目的接口 = 内部。
- 原始地址 = ftp_server 网络对象。
- 转换后的地址 = inside_v6 网络对象。由于在将 IPv4 转换为 IPv6 地址时使用 IPv4 嵌入地址方法，因此系统将 209.165.200.225 转换为 IPv6 对等的 D1A5:C8E1，并添加网络前缀以获取完整地址 2001:DB8::D1A5:C8E1。
- 在高级选项选项卡中，选择转换与此规则匹配的 DNS 回复。

Add NAT Rule

Title: FTPServer Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	outside	Destination Interface	inside
Original Address	ftp_server	Translated Address	inside_v6
Original Port	Any	Translated Port	Any

d) 点击确定。

步骤 3 为 DNS 服务器配置静态 NAT 规则。

- 依次选择 **策略 > NAT**。
- 点击 **+** 按钮。
- 配置以下属性：
 - 标题 = DNSServer（或您选择的其他名称）。
 - 创建规则的对象 = 自动 NAT。

- 类型 = 静态。
- 源接口 = 外部。
- 目的接口 = 内部。
- 原始地址 = dns_server 网络对象。
- 转换后的地址 = inside_v6 网络对象。由于在将 IPv4 转换为 IPv6 地址时使用 IPv4 嵌入地址方法，因此系统将 209.165.201.15 转换为 IPv6 对等的 D1A5:C90F，并添加网络前缀以获取完整地址 2001:DB8::D1A5:C90F。

d) 点击确定。

步骤 4 为内部 IPv6 网络配置动态 PAT 规则。

- 依次选择 策略 > NAT。
- 点击 + 按钮。
- 配置以下属性：
 - 标题 = PAT64Rule（或您选择的其他名称）。
 - 创建规则的对象 = 自动 NAT。
 - 类型 = 动态。
 - 源接口 = 内部。

- 目的接口 = 外部。
- 原始地址 = inside_v6 网络对象。
- 转换后的地址 = ipv4_pat 网络对象。

Add NAT Rule

Title: PAT64Rule Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Dynamic

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	inside	Destination Interface	outside
Original Address	inside_v6	Translated Address	ipv4_pat
Original Port	Any	Translated Port	Any

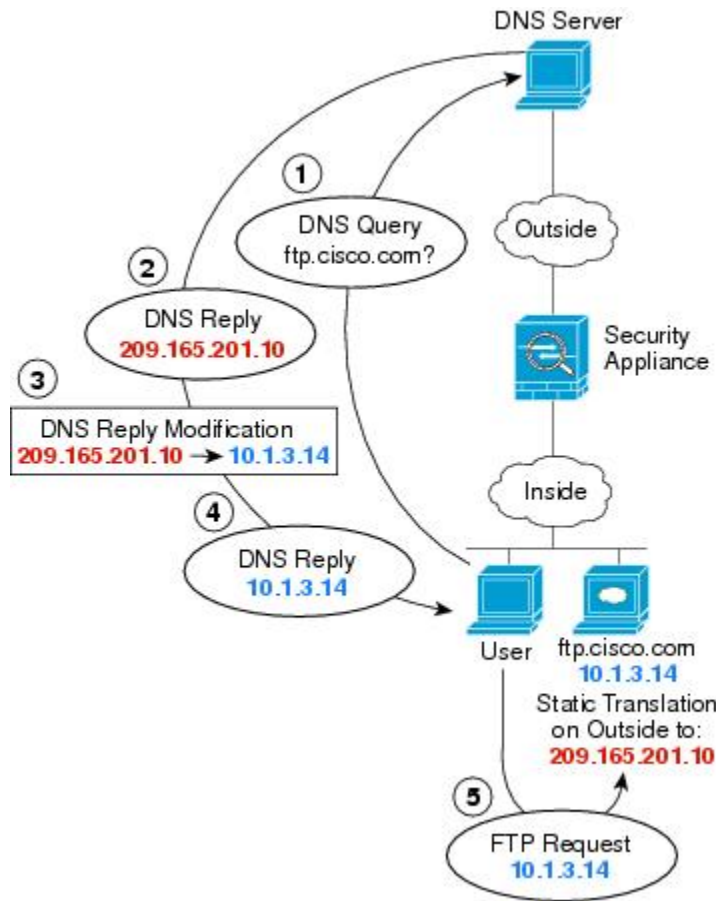
d) 单击 **OK**。

DNS 应答修改，外部接口上的 DNS 服务器

下图显示可从外部接口访问的 DNS 服务器。服务器 `ftp.cisco.com` 在内部接口上。将 NAT 配置为将 `ftp.cisco.com` 实际地址 (10.1.3.14) 静态转换为在外部网络上可见的映射地址 (209.165.201.10)。

在这种情况下，您要在此静态规则上启用 DNS 回复修改，以便使用实际地址访问 `ftp.cisco.com` 的内部用户可以接收来自 DNS 服务器的实际地址，而不是映射地址。

当内部主机发送对 `ftp.cisco.com` 的地址的 DNS 请求时，DNS 服务器将以映射地址 (209.165.201.10) 作为回复。系统引用内部服务器的静态规则，并将 DNS 回复中的地址转换为 10.1.3.14。如果不启用 DNS 应答修改，则内部主机尝试将流量发送到 209.165.201.10，而不是直接访问 `ftp.cisco.com`。



注释 此示例假定，内部接口不是桥接组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

步骤 1 为 FTP 服务器创建网络对象。

- a) 选择对象 (**Objects**)。
- b) 从目录中选择**网络**，然后点击 +。
- c) 定义实际 FTP 服务器地址。

为网络对象命名（例如，ftp_server），选择主机，然后输入实际主机 IP 地址 10.1.3.14。

Add Network Object

Name
ftp_server

Description

Type
 Network Host

Host
10.1.3.14

- d) 点击确定。
- e) 点击 +，然后定义 FTP 服务器的转换后的地址。
为网络对象命名（例如，ftp_server_outside），选择主机，然后输入主机地址 209.165.201.10。

Add Network Object

Name
ftp_server_outside

Description

Type
 Network Host

Host
209.165.201.10

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

- a) 依次选择 **策略 > NAT**。
- b) 点击 + 按钮。
- c) 配置以下属性：
- 标题 = FTPServer（或您选择的其他名称）。
 - 创建规则的对象 = 自动 NAT。

- 类型 = 静态。
- 源接口 = 内部。
- 目的接口 = 外部。
- 原始地址 = ftp_server 网络对象。
- 转换后的地址 = ftp_server_outside 网络对象。
- 在高级选项选项卡中，选择转换与此规则匹配的 DNS 回复。

Add NAT Rule

Title: FTPServer Create Rule for: Auto NAT Status:

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement: Automatically placed in Auto NAT rules Type: Static

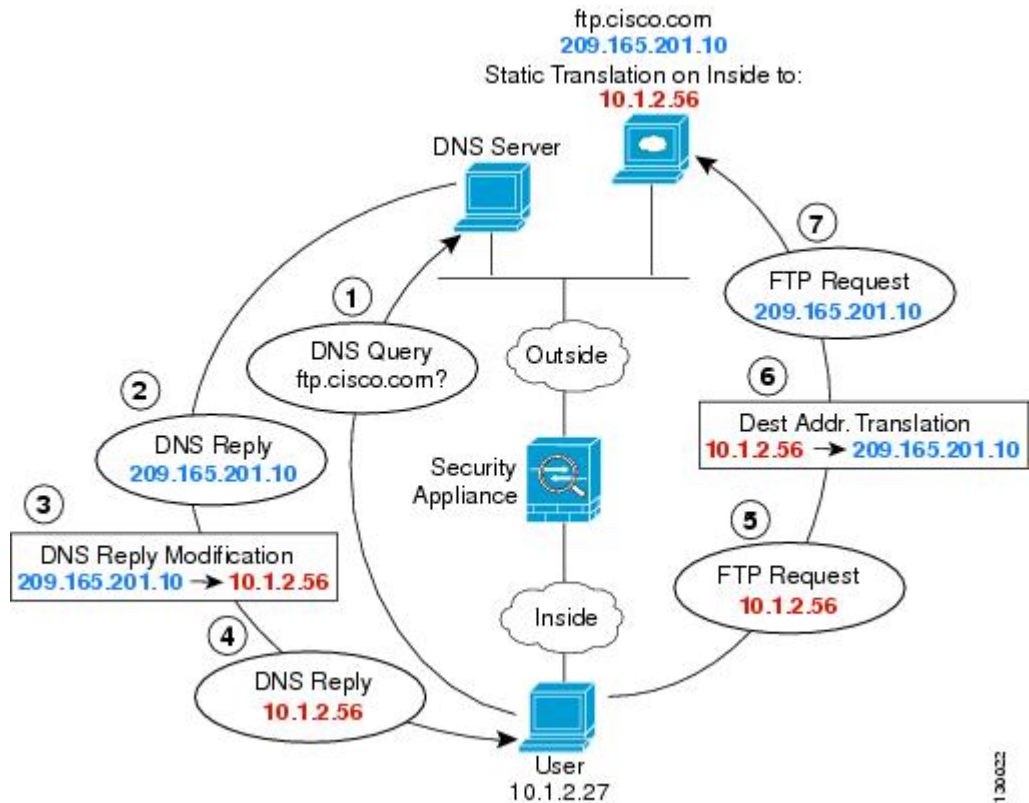
Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	inside	Destination Interface	outside
Original Address	ftp_server	Translated Address	ftp_server_outside
Original Port	Any	Translated Port	Any

d) 单击 **OK**。

DNS 应答修改，主机网络上的 DNS 服务器

下图显示外部网络上的 FTP 服务器和 DNS 服务器。系统有面向外部服务器的静态转换。在这种情况下，当内部用户从 DNS 服务器请求 ftp.cisco.com 的地址时，DNS 服务器将以实际地址 209.165.20.10 作为响应。由于您希望内部用户使用 ftp.cisco.com 的映射地址 (10.1.2.56)，因此需要配置 DNS 回复修改以进行静态转换。



注释 此示例假定，内部接口不是桥接组接口 (BVI)，而是标准路由接口。如果内部接口是 BVI，您需要为每个成员接口复制规则。

过程

步骤 1 为 FTP 服务器创建网络对象。

- a) 选择对象 (Objects)。
- b) 从目录中选择网络，然后点击 +。
- c) 定义实际 FTP 服务器地址。

为网络对象命名（例如，ftp_server），选择主机，然后输入实际主机 IP 地址 209.165.201.10。

Add Network Object

Name
ftp_server

Description

Type
 Network Host

Host
209.165.201.10

- d) 点击**确定**。
e) 点击**+**，然后定义 FTP 服务器的转换后的地址。

为网络对象命名（例如，ftp_server_translated），选择**主机**，然后输入主机地址 10.1.2.56。

Add Network Object

Name
ftp_server_translated

Description

Type
 Network Host

Host
10.1.2.56

步骤 2 为 FTP 服务器配置带 DNS 修改的静态 NAT 规则。

- a) 依次选择 **策略 > NAT**。
b) 点击 **+** 按钮。
c) 配置以下属性：
- 标题 = FTPServer（或您选择的其他名称）。
 - 创建规则的对象 = 自动 NAT。

- 类型 = 静态。
- 源接口 = 外部。
- 目的接口 = 内部。
- 原始地址 = ftp_server 网络对象。
- 转换后的地址 = ftp_server_translated 网络对象。
- 在高级选项选项卡中，选择转换与此规则匹配的 DNS 回复。

Add NAT Rule ?

Title	Create Rule for	Status
FTPServer	Auto NAT ▼	<input checked="" type="checkbox"/>

Auto NAT rules translate a specified host or network address regardless of its appearance as the source or destination address of a packet. These rules are automatically ordered and placed in the Auto NAT section.

Placement	Type
Automatically placed in Auto NAT rules	Static ▼

Packet Translation Advanced Options

ORIGINAL PACKET		TRANSLATED PACKET	
Source Interface	outside ▼	Destination Interface	inside
Original Address	ftp_server ▼	Translated Address	ftp_server_transla ▼
Original Port	Any ▼	Translated Port	Any

d) 单击 **OK**。



第 **V** 部分

虚拟专用网络 (VPN)

- [站点间 VPN，第 377 页](#)
- [远程接入 VPN，第 407 页](#)



第 18 章

站点间 VPN

虚拟专用网络 (VPN) 是一种网络连接，通过诸如互联网或其他网络之类的公共资源在远程对等体之间建立安全隧道。VPN 使用隧道来封装正常 IP 数据包内的数据包，以在基于 IP 的网络上转发。它们使用加密来确保隐私和身份验证，以确保数据的完整性。

- [VPN 基础知识，第 377 页](#)
- [管理站点间 VPN，第 381 页](#)
- [监控站点间 VPN，第 393 页](#)
- [站点间 VPN 示例，第 394 页](#)

VPN 基础知识

借助隧道，可以使用互联网等公共 TCP/IP 网络在远程用户与企业专用网络之间创建安全连接。每个安全连接都称为一个隧道。

基于 IPSec 的 VPN 技术通过互联网安全关联和密钥管理协议 (ISAKMP 或 IKE) 以及 IPSec 隧道标准来建立和管理隧道。ISAKMP 和 IPSec 将完成以下操作：

- 协商隧道参数。
- 建立隧道。
- 验证用户和数据。
- 管理安全密钥。
- 加密和解密数据。
- 管理隧道中的数据传输。
- 作为隧道终端或路由器管理入站和出站数据传输。

VPN 中的设备可用作双向隧道终端。它可以从专用网络接收明文数据包，将其封装，创建隧道，然后发送到隧道的另一端，随后解封并发送到最终目的地。它也会从公用网络接收封装数据包，将其解封，然后发送给其在专用网络上的最终目的地。

建立站点间 VPN 连接之后，本地网关后的主机可通过安全 VPN 隧道连接至远程网关后的主机。一个连接由以下部分组成：这两个网关的 IP 地址和主机名、这两个网关后的子网，以及这两个网关用来进行相互身份验证的方法。

互联网密钥交换 (IKE)

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时均使用方案。

IKE 策略是一组算法，供两个对等体用于保护它们之间的 IKE 协商。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数保护后续 IKE 协商。对于 IKE 版本 1 (IKEv1)，IKE 策略包含单个算法集和模数组。与 IKEv1 不同，在 IKEv2 策略中，您可以选择多个算法和模数组，对等体可以在第 1 阶段协商期间从中进行选择。可创建单个 IKE 策略，尽管您可能需要不同的策略来向最需要的选项赋予更高优先级。对于站点间 VPN，您可以创建单个 IKE 策略。

要定义 IKE 策略，请指定：

- 唯一优先级（1 至 65,543，其中 1 为最高优先级）。
- 一种 IKE 协商加密方法，用于保护数据并确保隐私。
- 散列消息身份验证代码 (HMAC) 方法（在 IKEv2 中称为完整性算法），用于确保发送人身份，以及确保消息在传输过程中未被修改。
- 对于 IKEv2，使用单独的伪随机函数 (PRF) 作为派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法。这些选项与用于散列算法的选项相同。
- Diffie-Hellman 群，用于确定 encryption-key-determination 算法的强度。设备使用此算法派生加密密钥和散列密钥。
- 身份验证方法，用于确保对等体的身份。
- 在更换加密密钥前，设备可使用该加密密钥的时间限制。

当 IKE 协商开始时，发起协商的对等体将其启用的所有策略发送到远程对等体，然后远程对等体按优先级顺序搜索其自己的策略的匹配项。如果 IKE 策略具有相同的加密、散列（完整性和用于 IKEv2 的 PRF）、身份验证和 Diffie-Hellman 值，而且 SA 生命周期小于或等于发送的策略中的生命周期，则它们之间存在匹配。如果生命周期不同，则会应用较短的生命周期（来自远程对等体）。默认情况下，使用 DES 的简单 IKE 策略是唯一启用的策略。您可以启用更高优先级的其他 IKE 策略来协商更强的加密标准，但 DES 策略应确保成功协商。

VPN 连接应具有多高的安全性？

由于 VPN 隧道通常流经公共网络（最可能是互联网），因此您需要对连接进行加密以保护流量。可以使用 IKE 策略和 IPsec 提议定义要应用的加密和其他安全技术。

如果您的设备许可证允许应用较强的加密，则有大量的加密和散列算法以及 Diffie-Hellman 组供您选择。然而，通常情况下，应用于隧道的加密越强，系统性能越差。您要在安全性和性能之间实现平衡，在提供充分保护的同时不牺牲效率。

我们无法就选择哪些选项提供具体指导。如果您在大型公司或其他组织执行运营，可能已有需要满足的指定标准。如果没有，请花些时间研究各个选项。

下面的主题介绍了几个可用选项。

决定使用哪个加密算法

在决定用于 IKE 策略或 IPsec 提议的加密算法时，您的选择仅限于 VPN 中的设备所支持的算法。

对于 IKEv2，您可以配置多个加密算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

对于 IPsec 提议，该算法用于封装安全协议 (ESP)，该协议提供身份验证、加密和防重放服务。ESP 为 IP 协议类型 50。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀。

如果设备许可证符合强加密要求，可以从以下加密算法中选择。如果不符合强加密要求，则只能选择 DES。

- AES-GCM - (仅 IKEv2。) Galois/Counter 模式中的高级加密标准是提供机密性和数据源身份验证的分组加密操作模式，并且提供比 AES 更高的安全性。AES-GCM 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。GCM 是支持 NSA Suite B 所需的 AES 模式。NSA Suite B 是一套加密算法，设备必须支持这套算法才能满足密码强度的联邦标准。
- AES-GMAC - (仅 IKEv2 IPsec 提议。) 高级加密标准 Galois 消息身份验证代码是仅提供数据源身份验证的分组加密操作模式。它是 AES-GCM 的一个变体，允许在不加密数据的情况下进行数据身份验证。AES-GMAC 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。
- AES - 高级加密标准是一种对称密码算法，提供比 DES 更高的安全性，在计算上比 3DES 更高效。AES 提供三种不同的密钥强度：128 位、192 位和 256 位密钥。密钥越长，其提供的安全性就越高，但性能会随之降低。
- 3DES - 三重 DES，使用 56 位密钥加密三次，比 DES 更加安全，因其使用不同密钥对每个数据块处理三次。不过，此算法比 DES 使用的系统资源更多且速度更慢。
- DES - 数据加密标准，使用 56 位密钥进行加密，是一种对称密钥块算法。如果您的许可证账户不符合导出控制要求，这将是您唯一的选择。此算法比 3DES 快且使用的系统资源更少，但安全性也较低。如果不需要很强的数据保密性，并且系统资源或速度存在问题，请选择 DES。
- 空 - 空加密算法提供不加密的身份验证。这通常仅用于测试目的。

决定使用哪些散列算法

在 IKE 策略中，散列算法创建消息摘要，用于确保消息的完整性。在 IKEv2 中，散列算法分成两个选项，一个用于完整性算法，一个用于伪随机函数 (PRF)。

在 IPsec 提议中，散列算法由封装安全协议 (ESP) 用于身份验证。在 IKEv2 IPsec 提议中，这称为完整性散列。在 IKEv1 IPsec 提议中，算法名称以 ESP- 为前缀，并且还有 -HMAC 后缀（代表“散列方法身份验证代码”）。

对于 IKEv2，您可以配置多个散列算法。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

您可以选择以下散列算法：

- SHA（安全散列算法）- 生成 160 位摘要的标准 SHA (SHA1)。SHA 抗暴力攻击的能力高于 MD5。但是，它也会比 MD5 占用更多的资源。对于需要最高级别安全性的实施，请使用 SHA 散列算法。

以下 SHA-2 选项更加安全，可用于 IKEv2 配置。如果要实施 NSA Suite B 加密规范，请选择以下选项之一。

- SHA256 - 指定具有 256 位摘要的安全散列算法 SHA 2。
- SHA384 - 指定具有 384 位摘要的安全散列算法 SHA 2。
- SHA512 - 指定具有 512 位摘要的安全散列算法 SHA 2。
- MD5（消息摘要 5）- 生成 128 位的摘要。MD5 能使用更少的处理时间实现比 SHA 更快的整体性能，但 MD5 被认为安全性低于 SHA。
- 空或无（NULL、ESP-NONE）-（仅限 IPsec 提议。）空散列算法；这通常仅用于测试目的。但是，如果选择 AES-GCM/GMAC 选项之一作为加密算法，则应选择空完整性算法。即使选择非空选项，这些加密标准也会忽略完整性散列。

决定要使用的 Diffie-Hellman 模数组

您可以使用以下 Diffie-Hellman 密钥导出算法生成 IPsec 安全关联 (SA) 密钥。每组具有不同的长度模数。模数越大，安全性越高，但需要的处理时间更长。两个对等体上必须具有一个匹配的模数组。

如果选择 AES 加密，要支持 AES 所需的大型密钥长度，应使用 Diffie-Hellman (DH) 组 5 或更高组。IKEv1 策略不支持下面列出的所有组。

要实施 NSA Suite B 加密规范，请使用 IKEv2 并选择椭圆曲线 Diffie-Hellman (ECDH) 的一个选项：19、20 或 21。使用 2048 位模数的椭圆曲线选项和组较少遭受 Logjam 等攻击。

对于 IKEv2，您可以配置多个组。系统将按安全性从高到低的顺序对设置进行排序，并使用该顺序与对等体进行协商。对于 IKEv1，仅可以选择一个选项。

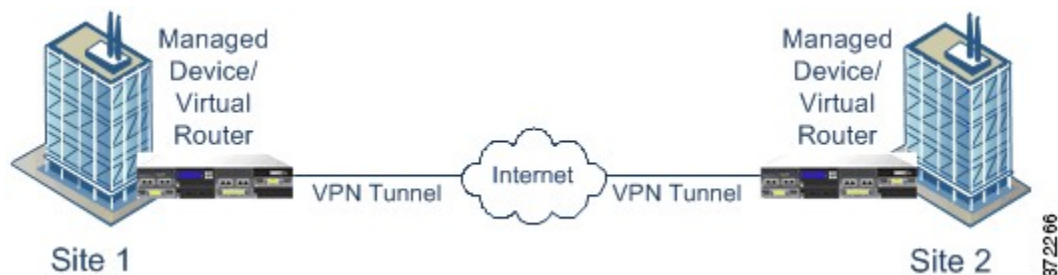
- 1 - Diffie-Hellman 组 1：768 位模数。DH 组 1 被视为不安全，请不要使用。
- 2 - Diffie-Hellman 组 2：1024 位模数算法 (MODP) 组。此选项不再是一种良好的保护措施。
- 5 - Diffie-Hellman 组 5：1536 位 MODP 组。曾经被认为可以良好地保护 128 位密钥，如今却不再是一种良好的保护措施。
- 14 - Diffie-Hellman 组 14：2048 位模数算法 (MODP) 组。被认为可以良好地保护 192 位密钥。
- 19 - Diffie-Hellman 组 19：美国国家标准与技术研究所 (NIST) 256 位椭圆曲线取素数 (ECP) 组。

- 20 - Diffie-Hellman 组 20: NIST 384 位 ECP 组。
- 21 - Diffie-Hellman 组 21: NIST 521 位 ECP 组。
- 24 - Diffie-Hellman 组 24: 带 256 位素数阶子组的 2048 位 MODP 组。我们不再建议采用此选项。

VPN 拓扑

使用 Firepower 设备管理器仅尽可能可以配置点对点 VPN 连接。虽然所有连接都是点对点的，但您可以通过定义设备参与的每个隧道，链接到更大的中心辐射型或网状 VPN。

下图显示了典型的点对点 VPN 拓扑。在点对点 VPN 拓扑中，两个终端彼此直接通信。将两个终端配置为对等设备，任一设备均可启动安全连接。



管理站点间 VPN

虚拟专用网络 (VPN) 是一种网络连接，通过诸如互联网或其他网络之类的公共资源在远程对等体之间建立安全隧道。VPN 使用隧道来封装正常 IP 数据包内的数据包，以在基于 IP 的网络上转发。它们使用加密来确保隐私和身份验证，以确保数据的完整性。

您可以与对等设备创建 VPN 连接。所有连接都是点对点连接，但您可以通过配置所有相关连接，将设备连接到更大的中心辐射型或网格 VPN 中。






注释 VPN 连接使用加密技术保护网络隐私。您可以使用的加密算法取决于您的基本许可证是否允许强加密。而控制这一点的，则是您在向思科智能许可证管理器注册时是否选择了允许在设备上使用出口控制功能的选项。如果您使用的是评估许可证，或者您没有启用受到出口管制的功能，则无法使用强加密。

过程

步骤 1 点击设备，然后点击站点间 VPN 组中的查看配置。

此操作将打开“站点间 VPN”页面，其中列出了您已配置的所有连接。

步骤 2 执行以下任一操作。

- 要创建新的站点间 VPN 连接，请点击 + 按钮。请参阅[配置站点间 VPN 连接，第 382 页](#)。
如果尚无连接，也可以点击[创建站点间连接按钮](#)。
- 要编辑现有连接，请点击该连接的编辑图标 ()。请参阅[配置站点间 VPN 连接，第 382 页](#)。
- 要将连接配置的摘要复制到剪贴板，请点击该连接的复制图标 ()。您可以将此信息粘贴到文档中发送给远程设备的管理员，帮助完成连接另一端的配置。
- 要删除不再需要的连接，请点击该连接的删除图标 ()。

配置站点间 VPN 连接

假定获得了远程设备所有者的合作与权限，您可以创建点对点 VPN 连接，将您的设备链接到另一台设备。虽然所有连接都是点对点的，但您可以通过定义设备参与的每个隧道，链接到更大的中心辐射型或网状 VPN。





注释 您可以为每个本地网络/远程网络组合创建单个 VPN 连接。但是，如果远程网络在每个连接配置文件中是唯一的，则可以为本地网络创建多个连接。

过程

步骤 1 点击**设备**，然后点击**站点间 VPN 组**中的**查看配置**。

步骤 2 执行以下任一操作：

- 要创建新的站点间 VPN 连接，请点击 + 按钮。
如果尚无连接，也可以点击[创建站点间连接按钮](#)。
- 要编辑现有连接，请点击该连接的编辑图标 ()。

要删除不再需要的连接，请点击该连接的删除图标 ()。

步骤 3 定义点对点 VPN 连接的终端。

- **连接配置文件名称** - 此连接的名称，最多 64 个字符，不含空格。例如，MainOffice。不能将 IP 地址用作名称。
- **本地站点** - 这些选项定义本地终端。
 - **本地 VPN 访问接口** - 选择远程对等体可连接的接口。这通常是外部接口。该接口不能是桥接组的成员。

- **本地网络** - 点击 + 并选择标识应参与 VPN 连接的本地网络的网络对象。这些网络上的用户将能够通过该连接访问远程网络。

注释 您可以为这些网络使用 IPv4 或 IPv6 地址，但必须在连接的每一侧都具有匹配的地址类型。例如，本地 IPv4 网络的 VPN 连接必须至少有一个远程 IPv4 网络。您可以在单个连接的两端结合 IPv4 和 IPv6。终端受保护的网路不能重叠。

- **远程站点** - 这些选项定义远程终端。
 - **远程 IP 地址** - 输入将用于托管 VPN 连接的远程 VPN 对等体接口的 IP 地址。
 - **远程网络** - 点击 + 并选择标识应参与 VPN 连接的远程网络的网络对象。这些网络上的用户将能够通过连接访问本地网络。

步骤 4 点击下一步。

步骤 5 定义 VPN 的隐私配置。

注释 您的许可证决定您可以选择哪些加密协议。您必须符合强加密的条件，即满足出口管制条件，才能并只能选择最基本的选项。

- **IKE 版本 2, IKE 版本 1** - 选择在互联网密钥交换 (IKE) 协商期间使用的 IKE 版本。根据需要选择一个或两个选项。当设备尝试与另一个对等体协商连接时，它使用您允许且该对等体接受的任何版本。如果这两个版本都允许，而对于最初选择的版本的协商不成功，则设备将自动回退到另一个版本。如果配置了 IKEv2，则系统将始终首先尝试它。两个对等体必须都支持 IKEv2 才能在协商中使用它。
- **IKE 策略** - 互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。这是一个全局策略：您启用的对象应用于所有 VPN。点击 **编辑** 以检查每个 IKE 版本当前全局启用的策略，并启用和创建新的策略。有关详细信息，请参阅 [配置全局 IKE 策略，第 384 页](#)。
- **IPsec 提议** - IPsec 提议定义确保 IPsec 隧道中流量安全的安全协议和算法的组合。点击 **编辑** 并为每个 IKE 版本选择提议。选择要允许的所有提议。点击 **设置默认值** 以简单选择系统默认值，这根据您的出口合规性而有所不同。系统与对等体协商，从最强到最弱的提议，直到约定一个匹配项。有关详细信息，请参阅 [配置 IPsec 提议，第 388 页](#)。
- **(IKEv2) 本地预共享密钥, 远程对等预共享密钥** - 此设备和远程设备上为 VPN 连接定义的密钥。这些密钥在 IKEv2 中可能不同。该密钥可以有 1 至 127 个字母数字字符。
- **(IKEv1) 预共享密钥** - 本地和远程设备上均定义的密钥。该密钥可以有 1 至 127 个字母数字字符。
- **NAT 免除** - 是否从本地 VPN 访问接口的 NAT 策略中免除 VPN 流量。如果不想将 NAT 规则应用于本地网络，请选择托管本地网络的接口。此选项仅在本地网络驻留在单个路由接口（而非桥接组成员）后时有用。如果本地网络位于多个路由接口或一个或多个桥接组成员之后，则必须手动创建 NAT 免除规则。有关手动创建所需规则的信息，请参阅 [使站点间 VPN 流量豁免 NAT，第 394 页](#)。

- **完美前向保密的 Diffie-Hellman 组** - 是否使用完美前向保密 (PFS) 为每个加密交换生成和使用唯一会话密钥。唯一会话密钥可保护交换免于后续解密，即使整个交换已被记录且攻击者已经获得终端设备使用的预共享密钥或私钥。要启用完美前向保密，请选择在模数组列表中生成 PFS 会话密钥时使用的 Diffie-Hellman 密钥导出算法。如果同时启用 IKEv1 和 IKEv2，则选项仅限于 IKEv1 支持的那些。有关选项的说明，请查看[决定要使用的 Diffie-Hellman 模数组](#)，第 380 页。

步骤 6 点击下一步。

步骤 7 查看摘要并点击完成。

摘要信息将复制到剪贴板。您可以将这些信息粘贴到文档中，并使用它来帮助配置远程对等体，或将其发送到负责配置对等体的一方。

您必须执行一些附加步骤，才能允许 VPN 隧道中的流量，如[允许流量通过站点间 VPN](#)，第 384 页中所述。

部署配置后，登录到设备 CLI 并使用 `show ipsec sa` 命令确认终端是否建立了安全关联。请参阅[验证站点间 VPN 连接](#)，第 390 页。

允许流量通过站点间 VPN

创建站点间连接尚无法使系统通过 VPN 隧道发送流量。还必须配置以下其中一个设置：

- 配置 `sysopt connection permit-vpn` 命令，此命令会使匹配 VPN 连接的流量免受访问控制策略的限制。此命令的默认值是 `no sysopt connection permit-vpn`，这意味着 VPN 流量还必须获得访问控制策略的允许，

由于外部用户无法在远程受保护网络中伪造 IP 地址，因此这是一种允许流量通过 VPN 的较为安全的方法。但它的缺点是，VPN 流量得不到检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。

使用 FlexConfig 配置此命令。

- 创建访问控制规则以允许来自远程网络的连接。此方法可确保对 VPN 流量进行检测，并将高级服务应用于连接。但它的缺点是，有可能造成外部用户伪造 IP 地址，进而获得访问内部网络的权限。

配置全局 IKE 策略

互联网密钥交换 (IKE) 是用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA) 的密钥管理协议。

IKE 协商包含两个阶段。第 1 阶段协商两个 IKE 对等体之间的安全关联，使对等体能够在第 2 阶段中安全通信。在第 2 阶段协商期间，IKE 为其他应用建立 SA，例如 IPsec。两个阶段在协商连接时

均使用方案。IKE 方案是一组两个对等体用于保护其之间的协商的算法。在各对等体商定公共（共享）IKE 策略后，即开始 IKE 协商。此策略声明哪些安全参数用于保护后续 IKE 协商。

IKE 策略对象为这些协商定义 IKE 提议。您启用的对象是对等体协商 VPN 连接时使用的对象：不能为每个连接指定不同的 IKE 策略。每个对象的相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。如果协商无法找到两个对等体全都支持的策略，则不建立连接。

要定义全局 IKE 策略，需要为每个 IKE 版本选择启用哪些对象。如果预定义的对象不能满足您的要求，请创建新的策略来执行您的安全策略。

以下步骤说明如何通过“对象”页面配置全局策略。在编辑 VPN 连接时，您还可以点击 IKE 策略设置的**编辑**，来启用、禁用和创建策略。

过程

步骤 1 从目录中选择对象，然后选择 **IKE 策略**。

IKEv1 和 IKEv2 的策略显示在不同列表中。

步骤 2 为每个 IKE 版本启用您希望允许的 IKE 策略。

- a) 在对象表上方选择 **IKEv1** 或 **IKEv2**，以显示该版本的策略。
- b) 点击**状态**开关以启用适当的对象并禁用不符合要求的对象。

如果您的一些安全要求没有反映在现有对象中，请定义新的对象以实施您的要求。有关详情，请参阅以下主题：

- [配置 IKEv1 策略，第 385 页](#)
- [配置 IKEv2 策略，第 387 页](#)

- c) 验证相对优先级是否符合您的要求。

如果您需要更改策略的优先级，请进行编辑。如果策略为预定义的系统策略，则需要创建您自己的策略版本来更改优先级。

优先级是相对的，而非绝对的。例如，优先级 80 高于 160。如果 80 是您启用的最高优先级对象，则它将成为您的首选策略。但如果您随后启用了优先级为 25 的策略，那它将成为您的首选策略。

- d) 如果同时使用两个 IKE 版本，使用另一个版本时，请重复相同的过程。

配置 IKEv1 策略

互联网密钥交换 (IKE) 版本 1 策略对象包含定义 VPN 连接时 IKEv1 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义 IKEv1 策略有多个。如果哪个符合您的需求，只需点击**状态**旋钮便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在 VPN 连接中编辑 IKEv1 设置时，点击对象列表中所示的**创建新 IKE 策略**链接来创建 IKEv1 策略对象。

过程


步骤 1 从目录中选择对象，然后选择 **IKE 策略**。


步骤 2 选择对象表上方的 **IKEv1**，以显示 IKEv1 策略。

步骤 3 如果任何系统定义的策略符合您的要求，请点击**状态**旋钮以启用它们。

也可使用**状态**开关禁用不需要的策略。相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。

步骤 4 执行以下操作之一：

- 要创建对象，请点击 **+** 按钮。
- 要编辑对象，请点击该对象的编辑图标 ()。

要删除未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 5 配置 IKEv1 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **名称** - 对象的名称，最多 128 个字符。
- **状态** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **身份验证** - 在两个对等体之间使用的身份验证方法。
 - **预共享密钥** - 使用在每个设备上定义的预共享密钥。在身份验证阶段，此类密钥允许密钥在两个对等体之间共享并由 IKE 使用。如果未使用同一预共享密钥配置对等体，则无法建立 IKE SA。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。有关选项的说明，请查看[决定使用哪个加密算法](#)，第 379 页。
- **Diffie-Hellman 组** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。有关选项的说明，请查看[决定要使用的 Diffie-Hellman 模数组](#)，第 380 页。
- **散列** - 用于创建消息摘要的散列算法，以确保消息的完整性。有关选项的说明，请查看[决定使用哪些散列算法](#)，第 379 页。
- **使用时间** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某

种程度上)，IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 6 点击 **OK**，保存更改。

配置 IKEv2 策略

互联网密钥交换 (IKE) 版本 2 策略对象包含定义 VPN 连接时 IKEv2 策略所需的参数。IKE 是一种密钥管理协议，有助于管理基于 IPsec 的通信。它用于对 IPsec 对等体进行身份验证，协商和分发 IPsec 加密密钥以及自动建立 IPsec 安全关联 (SA)。

预定义的 IKEv2 策略有多个。如果哪个符合您的需求，只需点击状态旋钮便可启用它们。您还可以创建新策略来实施其他安全设置组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在编辑 VPN 连接中的 IKEv2 设置时，点击对象列表中所示的**创建新 IKE 策略**链接来创建 IKEv2 策略。

过程

步骤 1 从目录中选择对象，然后选择 **IKE 策略**。

步骤 2 选择对象表上方的 **IKEv2** 以显示 IKEv2 策略。

步骤 3 如果任何系统定义的策略符合您的要求，请点击状态旋钮以启用它们。

也可使用状态开关禁用不需要的策略。相对优先级确定首先尝试这些策略中的哪一个，数字越小优先级越高。

步骤 4 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 5 配置 IKEv2 属性。

- **优先级** - IKE 策略的相对优先级，从 1 到 65,535。当尝试查找常见安全关联 (SA) 时，优先级可确定两个协商对等体比较的 IKE 策略顺序。如果远程 IPsec 对等体不支持在您的最高优先级策略中选定的参数，它会尝试使用下一个优先级中定义的参数。数值越低，优先级越高。
- **名称** - 对象的名称，最多 128 个字符。
- **状态** - IKE 策略是启用还是禁用状态。点击开关以更改状态。在 IKE 协商期间仅使用启用的策略。
- **加密** - 用于建立第 1 阶段安全关联 (SA)（用于保护第 2 阶段协商）的加密算法。选择要允许的所有算法，但不能在同一策略中同时包括混合模式 (AES-GCM) 和正常模式选项。（正常模式要

求选择完整性散列，而混合模式禁止选择单独的完整性散列。)系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请查看[决定使用哪个加密算法](#)，第 379 页。

- **Diffie-Hellman 组** - 用于在两个 IPsec 对等体之间派生共享密钥而不将其相互传输的 Diffie-Hellman 组。模数更大则安全性越高，但需要更多的处理时间。两个对等体必须具有匹配的模数组。选择要允许的所有算法。系统与对等体协商，从最强到最弱组，直到达成匹配。有关选项的说明，请查看[决定要使用的 Diffie-Hellman 模数组](#)，第 380 页。
- **完整性散列** - 用于创建消息摘要的散列算法的完整性部分，用于确保消息完整性。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。完整性散列不与 AES-GCM 加密选项一起使用。有关选项的说明，请查看[决定使用哪些散列算法](#)，第 379 页。
- **伪随机函数 (PRF) 散列** - 散列算法中用作派生 IKEv2 隧道加密所要求的密钥内容和散列运算的算法的伪随机函数 (PRF) 部分。在 IKEv1 中，完整性和 PRF 算法不分开，但在 IKEv2 中，可以为这些元素指定不同的算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请查看[决定使用哪些散列算法](#)，第 379 页。
- **使用时间** - 安全关联 (SA) 的生命周期（以秒为单位）范围为 120 到 2147483647，也可以将其留空。当超过生命周期时，SA 到期且必须在两个对等体之间重新协商。通常，生命周期越短（某种程度上），IKE 协商越安全。但是，生命周期越长，将来设置 IPsec 安全关联的速度比生命周期较短时更快。默认值为 86400。要指定无限生命周期，请不要输入任何值（将此字段留空）。

步骤 6 点击 **OK**，保存更改。

配置 IPsec 提议

IPsec 是设置 VPN 的最安全方法之一。IPsec 在 IP 数据包级别提供数据加密，提供一种基于标准的强大的安全解决方案。使用 IPsec，数据通过隧道在公共网络上传输。隧道是两个对等体之间安全的逻辑通信路径。进入 IPsec 隧道的流量由称为转换集的安全协议和算法组合保护。在 IPsec 安全关联 (SA) 协商期间，对等体搜索在两个对等体处相同的转换集。

根据 IKE 版本 (IKEv1 或 IKEv2)，存在不同的 IPsec 方案对象：

- 当创建 IKEv1 IPsec 提议时，可以选择 IPsec 运行的模式，并定义所需的加密和身份验证类型。您可以为算法选择单一选项。如果要在 VPN 中支持多个组合，请创建和选择多个 IKEv1 IPsec 提议对象。
- 当创建 IKEv2 IPsec 提议时，可以选择 VPN 中允许的所有加密和散列算法。系统将按安全性从高到低的顺序对设置进行排序，并与对等体进行协商，直到找到匹配。利用这种排序，您可以发送单个提议来传达所有允许的组合，而无需像 IKEv1 一样逐一发送每个允许的组合。

IKEv1 和 IKEv2 IPsec 提议都使用封装安全协议 (ESP)。它可以提供身份验证、加密和反重播服务。ESP 为 IP 协议类型 50。



注释 我们建议对 IPsec 隧道使用加密和身份验证。

以下主题介绍如何为每个 IKE 版本配置 IPsec 提议。

为 IKEv1 配置 IPsec 提议

使用 IKEv1 IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

有几个预定义的 IKEv1 IPsec 提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv1 IPsec 设置时，点击对象列表中所示的**创建新 IPsec 提议**链接来创建 IKEv1 IPsec 提议对象。

过程

步骤 1 选择对象，然后从目录中选择 IPsec 提议。

步骤 2 选择对象表上方的 **IKEv1** 显示 IKEv1 IPsec 提议。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 4 配置 IKEv1 IPsec 提议属性。

- **名称** - 对象的名称，最多 128 个字符。
- **模式** - IPsec 隧道的运行模式。
 - **隧道模式** 封装整个 IP 数据包。IPsec 报头被添加到原始 IP 报头和新的 IP 报头之间。这是默认值。当防火墙对出入位于防火墙后的主机的流量进行保护时，请使用隧道模式。在通过不可信网络（例如互联网）连接的两个防火墙（或其他安全网关）之间，通常采用隧道模式实施常规 IPsec。
 - **传输模式** 只封装 IP 数据包的上层协议。IPsec 报头被插入到 IP 报头和上层协议报头（例如 TCP）之间。传输模式要求源和目的主机都支持 IPsec，并且只有在隧道的目的对等体是 IP 数据包的最目的时才可使用。通常只有在保护第 2 层或第 3 层隧道协议（例如 GRE、L2TP 和 DLSW）时，才会使用传输模式。
- **ESP 加密** - 此提议的封装安全协议 (ESP) 加密算法。有关选项的说明，请查看[决定使用哪个加密算法](#)，第 379 页。
- **ESP 散列** - 要用于身份验证的散列或完整性算法。有关选项的说明，请查看[决定使用哪些散列算法](#)，第 379 页。

步骤 5 点击 **OK**，保存更改。

为 IKEv2 配置 IPsec 提议

使用 IKEv2 IPsec 提议对象配置 IKE 第 2 阶段协商期间使用的 IPsec 提议。IPsec 提议定义在 IPsec 隧道中保护流量的安全协议和算法的组合。

有几个预定义的 IKEv2 IPsec 提议。您也可以创建新的提议，用于实施安全设置的其他组合。但您无法编辑或删除系统定义的对象。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。此外，也可以在编辑 VPN 连接中的 IKEv2 IPsec 设置时，点击对象列表中所示的**创建新 IPsec 提议**链接来创建 IKEv2 IPsec 提议对象。

过程

步骤 1 选择对象，然后从目录中选择 **IPsec 提议**。

步骤 2 选择对象表上方的 **IKEv2** 显示 IKEv2 IPsec 提议。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 4 配置 IKEv2 IPsec 提议属性。

- **名称** - 对象的名称，最多 128 个字符。
- **加密** - 此提议的封装安全协议 (ESP) 加密算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请查看[决定使用哪个加密算法](#)，第 379 页。
- **完整性散列** - 要用于身份验证的散列或完整性算法。选择要允许的所有算法。系统与对等体协商，从最强算法到最弱算法，直到达成匹配。有关选项的说明，请查看[决定使用哪些散列算法](#)，第 379 页。

注释 如果选择其中一个 AES-GCM/GMAC 选项作为加密算法，则应该选择空完整性算法。即使您选择非空选项，这些加密标准也不会使用完整性散列算法。

步骤 5 点击 **OK**，保存更改。

验证站点间 VPN 连接

在配置站点间 VPN 连接并将该配置部署到设备后，请确认系统是否与远程设备建立了安全关联。

如果无法建立连接，请在设备 CLI 中使用 **ping interface interface_name remote_ip_address** 命令，以确保路径通过 VPN 接口连接到远程设备。如果没有连接通过配置的接口，可停用 **interface interface_name** 关键字并确定连接是否通过其他接口。您可能选错了用于连接的接口：必须选择面对远程设备的接口，而不是面对受保护网络的接口。

如果存在网络路径，请检查两个终端配置和支持的 IKE 版本和密钥，并根据需要调整 VPN 连接。确保没有访问控制规则或 NAT 规则会阻止连接。

过程

步骤 1 登录到设备 CLI，如[登录命令行界面 \(CLI\)](#)，第 7 页中所述。

步骤 2 使用 **show ipsec sa** 命令可确认是否建立了 IPsec 安全关联。

您应可看到设备（本地地址）与远程对等体（**current_peer**）之间建立了 VPN 连接。随着您通过该连接发送流量，数据包 (pkts) 计数应会增加。访问列表应显示该连接的本地和远程网络。

例如，以下输出显示 IKEv2 连接。

```
> show ipsec sa
interface: site-a-outside
  Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

  access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
  local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
  current_peer: 192.168.4.6

  #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
  #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
  #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #send errors: 0, #recv errors: 0

  local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
  path mtu 1500, ipsec overhead 55(36), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: CD22739C
  current inbound spi : 52D2F1E4

inbound esp sas:
  spi: 0x52D2F1E4 (1389556196)
    SA State: active
    transform: esp-aes-gcm-256 esp-null-hmac no compression
    in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
    slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
    sa timing: remaining key lifetime (kB/sec): (4285434/28730)
    IV size: 8 bytes
    replay detection support: Y
  Anti replay bitmap:
    0xFFFFFFFF 0xFFFFFFFF
```

```

outbound esp sas:
 spi: 0xCD22739C (3441587100)
  SA State: active
  transform: esp-aes-gcm-256 esp-null-hmac no compression
  in use settings =(L2L, Tunnel, PFS Group 19, IKEv2, )
  slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
  sa timing: remaining key lifetime (kB/sec): (4055034/28730)
  IV size: 8 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001

```

以下输出显示 IKEv1 连接。

```

> show ipsec sa
interface: site-a-outside
  Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

  access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
current_peer: 192.168.4.6

#pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
#pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 077D72C9
current inbound spi : AC146DEC

inbound esp sas:
 spi: 0xAC146DEC (2887020012)
  SA State: active
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings =(L2L, Tunnel, PFS Group 5, IKEv1, )
  slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
  sa timing: remaining key lifetime (kB/sec): (3914999/28567)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x000007FF
outbound esp sas:
 spi: 0x077D72C9 (125661897)
  SA State: active
  transform: esp-aes-256 esp-sha-hmac no compression
  in use settings =(L2L, Tunnel, PFS Group 5, IKEv1, )
  slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
  sa timing: remaining key lifetime (kB/sec): (3914999/28567)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:

```



```
0x00000000 0x00000001
```

步骤 3 使用 **show isakmp sa** 命令可验证 IKE 安全关联。

您可以使用不带 **sa** 关键字的命令（或改用 **stats** 关键字）查看 IKE 统计信息。

例如，以下输出显示 IKEv2 安全关联。

```
> show isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
592216161 192.168.2.15/500 192.168.4.6/500 READY INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector 192.168.1.0/0 - 192.168.1.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

以下输出显示 IKEv1 安全关联。

```
> show isakmp sa

IKEv1 SAs:

  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 192.168.4.6
   Type    : L2L           Role    : initiator
   Rekey   : no           State   : MM_ACTIVE

There are no IKEv2 SAs
```

监控站点间 VPN

要监控和故障排除站点间 VPN 连接，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。

- **show ipsec sa** 显示 VPN 会话（安全关联）。您可以使用 **clear ipsec sa counters** 命令重置这些统计信息。
- **show ipsec keyword** 显示的是 IPsec 运行数据和统计信息。输入 **show ipsec ?** 查看可用关键字。
- **show isakmp** 显示 ISAKMP 运行数据和统计信息。

站点间 VPN 示例

以下是配置站点间 VPN 的示例。

使站点间 VPN 流量豁免 NAT

当您在某个接口上定义了站点间 VPN 连接并且还对该接口实施了 NAT 规则时，可以选择使该 VPN 上的流量豁免 NAT 规则。如果 VPN 连接的远端可以处理您的内部地址，则可能要执行此操作。

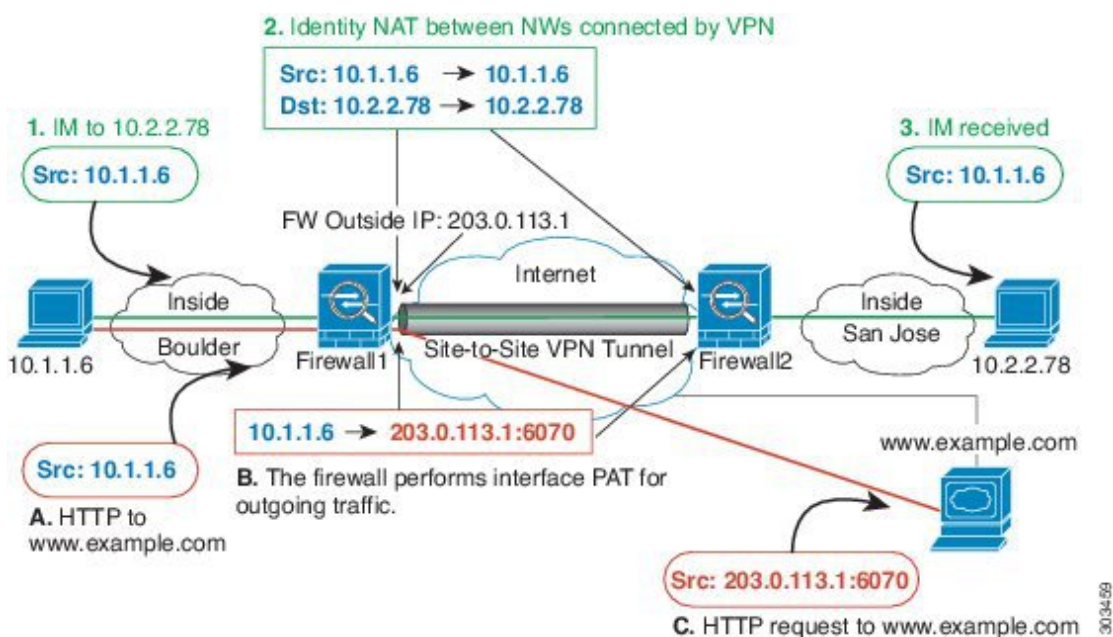
创建 VPN 连接时，可以选择 **NAT 豁免** 选项自动创建 NAT 豁免规则。不过，此操作仅在通过单个路由接口（而非桥接组成员）连接本地受保护网络时才奏效。相反，如果该连接中的本地网络位于两个或多个路由接口之后或者一个或多个桥接组成员之后，则需要手动配置 NAT 豁免规则。

要使 VPN 流量豁免 NAT 规则，需要为目的是远程网络时的本地流量创建身份手动 NAT 规则。然后，将 NAT 应用于目的是其他网络（例如互联网）时的流量。如果本地网络有多个接口，请为每个接口分别创建规则。也可以考虑以下建议：

- 如果连接中有多个本地网络，请创建一个网络对象组用于容纳定义这些网络的对象。
- 如果 VPN 中同时包括 IPv4 和 IPv6 网络，请为其各创建一个单独的身份 NAT 规则。

下例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 23: 用于站点间 VPN 的接口 PAT 和身份 NAT



以下示例说明 Firewall1（博尔德办公室）的配置。该示例假定内部接口是桥接组，因此需要为每个成员接口编写规则。如果有一个或多个路由内部接口，其过程相同。



注释 此示例假定只包括 IPv4 网络。如果该 VPN 还包括 IPv6 网络，请为 IPv6 创建并行规则。请注意，由于无法实施 IPv6 接口 PAT，因此需要使用唯一 IPv6 地址创建主机对象用于 PAT。

过程

步骤 1 创建对象来定义各种网络。

- a) 选择对象 (**Objects**)。
- b) 从目录中选择**网络**，然后点击 +。
- c) 找到博尔德办公室内部网络。

为网络对象命名（例如，boulder-network），选择**网络**，然后输入网络地址 10.1.1.0/24。

Add Network Object

Name
boulder-network

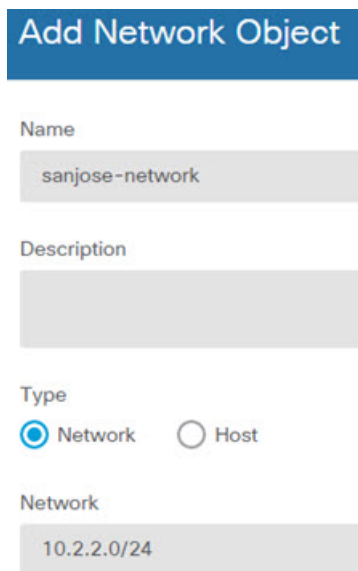
Description

Type
 Network Host

Network
10.1.1.0/24

- d) 点击**确定**。
- e) 点击 + 并定义内部圣荷西办公室网络。

为网络对象命名（例如，sanjose-network），选择**网络**，然后输入网络地址 10.2.2.0/24。



Add Network Object

Name
sanjose-network

Description

Type
 Network Host

Network
10.2.2.0/24

f) 点击确定。

步骤 2 在 Firewall1（博尔德办公室）上，为博尔德办公室网络配置经过 VPN 连接到圣荷西办公室时的手动身份 NAT。

a) 依次选择 **策略 > NAT**。

b) 点击 + 按钮。

c) 配置以下属性：

- 标题 = NAT Exempt 1_2 Boulder San Jose VPN（或您选择的其他名称）。
- 创建规则的对象 = 手动 NAT。
- 位置 = 特定规则之上，然后在“手动 NAT 在自动 NAT 之前”部分选择第一条规则。需要确保此规则在目的接口的任何常规接口 PAT 规则之前。否则，该规则可能不会应用于正确的流量。
- 类型 = 静态。
- 源接口 = inside1_2。
- 目的接口 = 外部。
- 原始源地址 = boulder-network 网络对象。
- 转换后的源地址 = boulder-network 网络对象。
- 原始目标地址 = sanjose-network 网络对象。
- 转换后的目标地址 = sanjose-network 网络对象。

注释 由于您不需要转换目的地址，因此需要通过为原始目的地址和转换后的目的地址指定相同的地址，从而为其配置身份 NAT。将所有端口字段留空。此规则为源和目的配置身份 NAT。

- d) 在高级选项卡中，选择不在目的接口上使用代理 ARP。
- e) 点击确定。
- f) 重复此过程，为每个其他内部接口创建相应规则。

步骤 3 在 Firewall1（博尔德办公室）上，为内部博尔德办公室网络配置接入互联网时的手动动态接口 PAT。

注释 内部接口可能已经配置了将所有 IPv4 流量包括在内的动态接口 PAT 规则，因为初始配置过程中会默认创建这些规则。不过，为完整起见，此处仍显示了这些配置。完成这些步骤之前，请检查是否已经存在将内部接口和网络包括在内的规则，如有则跳过此步骤。

- a) 点击 + 按钮。
- b) 配置以下属性：
 - 标题 = inside1_2 接口 PAT（或您选择的其他名称）。
 - 创建规则的对象 = 手动 NAT。
 - 位置 = 特定规则之下，然后在“手动 NAT 在自动 NAT 之前”部分选择您在上面对此接口创建的规则。由于此规则将应用于所有目标地址，使用 sanjose-network 作为目标的规则必须在此规则之前，否则 sanjose-network 规则永远没有匹配项。默认设置是将新的手动 NAT 规则放到“NAT 规则在自动 NAT 之前”部分的末尾，此设置也已足够。
 - 类型 = 动态。

- 源接口 = inside1_2。
- 目的接口 = 外部。
- 原始源地址 = boulder-network 网络对象。
- 转换后的源地址 = 接口。此选项配置使用目的接口的接口 PAT。
- 原始目标地址 = 任意。
- 转换后的目标地址 = 任意。

- 点击确定。
- 重复此过程，为每个其他内部接口创建相应规则。

步骤 4 确认您的更改。

- 点击网页右上角的部署更改图标。



- 点击立即部署按钮。

您可以等待部署完成，也可以点击确定，稍后再检查任务列表或部署历史记录。

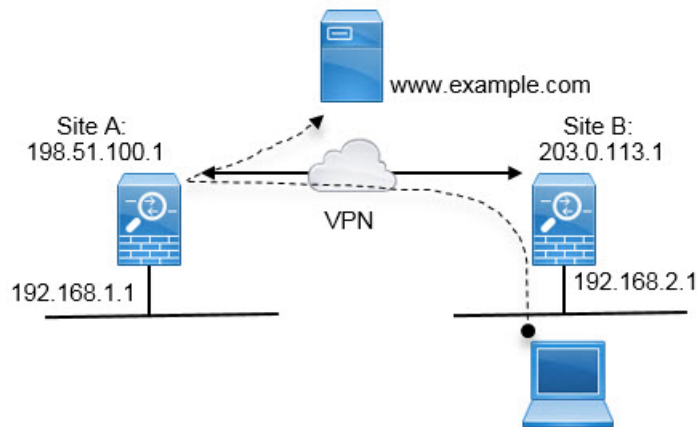
步骤 5 如果您也管理着 Firewall2（圣荷西办公室），您可以为该设备配置类似的规则。

- 当目的是 boulder-network 时，手动身份 NAT 规则将用于 sanjose-network。为 Firewall2 内部和外部网络创建新的接口对象。
- 当目的是“任意”时，手动动态接口 PAT 规则将用于 sanjose-network。

如何在外部接口上为外部站点间 VPN 用户提供互联网访问（发夹方法）

在站点间 VPN 中，您可能希望远程网络用户通过您的设备访问互联网。不过，这些远程用户进入设备所用的接口与访问互联网所用的接口（外部接口）相同，因此需要使互联网流量从外部接口退出。这种技术有时候称为发夹方法。

下图展示了一个示例。在 198.51.100.1（在主站点上，站点 A）与 203.0.113.1（远程站点，站点 B）之间配置了一个站点间 VPN 隧道。从网络内部的远程站点 192.168.2.0/24 流出的所有用户流量均通过此 VPN 隧道。因此，如果该网络上的用户想要访问互联网上的某个服务器（例如 www.example.com），连接会首先通过此 VPN 隧道，然后从 198.51.100.1 接口路由回到互联网。



以下程序介绍如何配置此服务。首先，需要配置 VPN 隧道的两个终端。

开始之前

此程序假定您使用了允许 VPN 流量的默认设置，使 VPN 流量受访问控制策略的限制。在运行配置中，这由 `no sysopt connection permit-vpn` 命令表示。如果您通过 FlexConfig 中选择为已解密的流量绕过访问控制策略选项启用了 `sysopt connection permit-vpn`，则无需执行这些步骤来配置访问控制规则。

过程

步骤 1（站点 A，主站点。）配置到远程站点 B 的站点间 VPN 连接。

- a) 点击设备，然后点击站点间 VPN 组中的查看配置。

- b) 点击 + 添加新连接。
- c) 按如下所述定义终端，然后点击下一步：
- **连接配置文件名称** - 为连接指定一个有意义的名称，例如 Site-A-to-Site-B。
 - **本地 VPN 接入接口** - 选择外部接口。
 - **本地网络** - 保留默认值“任何”。
 - **远程 IP 地址** - 输入远程对等设备外部接口的 IP 地址。在本示例中，此地址为 203.0.113.1。
 - **远程网络** - 点击 +，然后选择定义远程对等设备的受保护网络的网络对象。在本示例中，此对象为 192.168.2.0/24。可以点击**创建新网络**立即创建对象。

下图展示了第一步操作对应的界面。

Connection Profile Name

Site-A-to-Site-B

LOCAL SITE	REMOTE SITE
Local VPN Access Interface	Remote IP Address
outside	203.0.113.1
Local Network	Remote Network
+ ANY	+ Site-B-Network

- d) 定义隐私配置，然后点击下一步。
- **IKE 策略** - IKE 设置对发夹方法没有影响。选择满足安全需求的 IKE 版本、策略和提议即可。请记住您输入的本地和远程预共享密钥：配置远程对等设备时会用到这些信息。
 - **NAT 免除** - 选择内部接口。

Additional Options

NAT Exempt

inside

- **完美前向保密的 Diffie-Hellman 组** - 此设置对发夹方法没有影响。可以根据需要配置此设置。

- e) 点击完成。

连接摘要信息将会复制到剪贴板。您可以将这些信息粘贴到文本文件或其他文档，帮助您配置远程对等设备。


步骤 2（站点 A，主站点。）将 NAT 规则配置为将外部接口发出的所有连接转换到外部 IP 地址上的端口（接口 PAT）。

完成初始设备配置后，系统将创建名为 `InsideOutsideNatRule` 的 NAT 规则。此规则将接口 PAT 应用于任意接口上通过外部接口流出设备的 IPv4 流量。由于外部接口包含在“任何”源接口中，因此，此规则已经存在，除非您对所需的规则进行编辑或将其删除。

以下程序介绍如何创建所需的规则。

a) 依次点击**策略 > NAT**。

b) 执行以下操作之一：

- 要编辑 `InsideOutsideNatRule`，请将鼠标指针悬停在**操作**列上，然后点击编辑图标 。
- 要创建新规则，请点击 **+**。

c) 配置规则的以下属性：

- **名称** - 为新规则输入一个有意义且不含空格名称。例如，`OutsideInterfacePAT`。
- **创建规则的对象** - **手动 NAT**。
- **位置** - **自动 NAT 规则之前**（默认）。
- **类型** - **动态**。
- **原始数据包** - 对于源地址，请选择“任何”或 `any-ipv4`。对于源接口，请确保选择“任何”（默认值）。对于所有其他“原始数据包”选项，请保留默认值“任何”。
- **已转换的数据包** - 对于目标接口，请选择外部接口。对于已转换的地址，请选择接口。对于所有其他“已转换的数据包”选项，请保留默认值“任何”。

下图展示了选择“任何”作为源地址时的简单情况。

The screenshot shows the configuration for a Manual NAT rule. Key settings highlighted with red circles include:

- Create Rule for:** Manual NAT
- Placement:** Before Auto NAT Rules
- Type:** Dynamic
- ORIGINAL PACKET Source Interface:** Any
- ORIGINAL PACKET Source Address:** Any
- TRANSLATED PACKET Destination Interface:** outside
- TRANSLATED PACKET Source Address:** Interface

d) 点击确定。

步骤 3（站点 A，主站点。）配置访问控制规则，以允许访问站点 B 上的受保护网络。

仅仅创建 VPN 连接不会自动允许通过 VPN 上的流量。还需要确保您的访问控制策略允许流量通过远程网络。

以下程序展示了如何添加远程网络专用的规则。是否需要其他规则取决于您现有的规则。

- 依次点击策略 > 访问控制。
- 点击 + 创建新规则。
- 配置规则的以下属性：

- **顺序** - 在策略中选择一个位置，此位置应位于可能会匹配并阻止这些连接的任何其他规则之前。默认情况下，会将该规则添加到策略的末尾。如果稍后需要重新调整规则的位置，可以编辑此选项，也可以直接将规则拖放到表格中相应的位置。
- **名称** - 输入一个有意义且不含空格的名词。例如，Site-B-Network。
- **操作** - 允许。如果不希望对此流量执行协议违规检测或入侵检测，可以选择“信任”。
- **源/目标选项卡** - 对于目标 > 网络，请选择您在 VPN 连接配置文件中用于远程网络的同一对象。对于所有其他“源”和“目标”选项，请保留默认值“任何”。

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
ANY	ANY	ANY	ANY	Site-B-Network	ANY

- 应用、URL 和用户选项卡 - 保留这些选项卡的默认设置，即不做任何选择。
- 入侵、文件选项卡 -（可选）您可以选择入侵或文件策略，以进行威胁或恶意软件检测。
- 日志记录选项卡 -（可选）您可以选择启用连接日志记录。

d) 点击**确定**。

步骤 4（站点 A，主站点。）确认您的更改。

a) 点击网页右上角的**部署更改**图标。



b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。如果保持窗口打开，那么成功部署后，窗口中将指示没有待处理的更改。

步骤 5（站点 B，远程站点。）登录到远程站点设备，并配置到站点 A 的站点间 VPN 连接。

借助从站点 A 设备配置获取的连接摘要来配置连接的站点 B 端。

- 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。
- 点击**+ 添加新连接**。
- 按如下所述定义终端，然后点击**下一步**：
 - **连接配置文件名称** - 为连接指定一个有意义的名称，例如，Site-B-to-Site-A。
 - **本地 VPN 接入接口** - 选择外部接口。
 - **本地网络** - 点击 **+**，然后选择定义本地受保护网络的网络对象。在本示例中，此对象为 192.168.2.0/24。可以点击**创建新网络**立即创建对象。
 - **远程 IP 地址** - 输入主站点的外部接口的 IP 地址。在本示例中，此地址为 198.51.100.1。
 - **远程网络** - 保留默认值“任何”。请忽略警告；此警告与本使用案例无关。

下图展示了第一步操作对应的界面。

Connection Profile Name

Site-B-to-Site-A

LOCAL SITE	REMOTE SITE
Local VPN Access Interface	Remote IP Address
outside	198.51.100.1
Local Network	Remote Network
ProtectedNetwork	<p>We don't recommend to use "ANY" for this option.</p> <p>ANY</p>

d) 定义隐私配置，然后点击下一步。

- **IKE 策略** - IKE 设置对发夹方法没有影响。配置与 VPN 连接的站点 A 端相同或兼容的选项。必须正确配置预共享密钥：按照站点 A 设备上的配置交换本地和远程密钥（适用于 IKEv2）。对于 IKEv1，只有一个密钥，此密钥在两个对等设备上必须相同。
- **NAT 免除** - 选择内部接口。

Additional Options

NAT Exempt

inside

- **完美前向保密的 Diffie-Hellman 组** - 此设置对发夹方法没有影响。匹配 VPN 连接的站点 A 端使用的设置。

e) 点击完成。

步骤 6（站点 B，远程站点。）删除受保护网络的所有 NAT 规则，以便离开此站点的所有流量都必须流经 VPN 隧道。

由于站点 A 设备会执行地址转换，因此无需在此设备上执行 NAT。但还是请根据自己的具体情况具体分析。如果您有多个内部网络，而且不是所有这些网络都参与此 VPN 连接，则请勿删除这些网络所需的 NAT 规则。

- 依次点击策略 > NAT。
- 执行以下操作之一：

- 要删除规则，请将鼠标指针悬停在“操作”列上，然后点击删除图标 (🗑️)。

- 要编辑规则，使其不再应用于受保护的网路，请将鼠标指针悬停在“操作”列上，然后点击编辑图标 (🔗)。

步骤 7（站点 B，远程站点。）配置访问控制规则，以允许从受保护网路访问互联网。

以下示例允许受保护网路中的流量通过任何目标。您可以根据自己的具体要求调整此选项。也可以在此规则之前添加阻止规则，过滤掉不必要的流量。还有另外一种方法，就是在站点 A 设备上配置阻止规则。

a) 依次点击**策略 > 访问控制**。

b) 点击 **+** 创建新规则。

c) 配置规则的以下属性：

- **顺序** - 在策略中选择一个位置，此位置应位于可能会匹配并阻止这些连接的任何其他规则之前。默认情况下，会将该规则添加到策略的末尾。如果稍后需要重新调整规则的位置，可以编辑此选项，也可以直接将规则拖放到表格中相应的位置。
- **名称** - 输入一个有意义且不含空格名称。例如，**Protected-Network-to-Any**。
- **操作** - **允许**。如果不希望对此流量执行协议违规检测或入侵检测，可以选择“信任”。
- **源/目标选项卡** - 对于**源 > 网路**，请选择在 VPN 连接配置文件中用于本地网路的同一对象。对于所有其他“源”和“目标”选项，请保留默认值“任何”。

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
ANY	ProtectedNetwork	ANY	ANY	ANY	ANY

- **应用、URL 和用户选项卡** - 保留这些选项卡的默认设置，即不做任何选择。
- **入侵、文件选项卡** -（可选）您可以选择入侵或文件策略，以进行威胁或恶意软件检测。
- **日志记录选项卡** -（可选）您可以选择启用连接日志记录。

d) 点击**确定**。

步骤 8（站点 B，远程站点。）确认您的更改。

a) 点击网页右上角的**部署更改**图标。



b) 点击**立即部署**按钮，并等待部署完成。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。如果保持窗口打开，那么成功部署后，窗口中将指示没有待处理的更改。

如何在外部接口上为外部站点间 VPN 用户提供互联网访问（发夹方法）



第 19 章

远程接入 VPN

远程接入虚拟专用网络 (VPN) 允许个人用户使用连接到互联网的计算机或其他受支持的 iOS 或 Android 设备，从远程位置连接到您的网络。这样，移动员工就可以从家庭网络或公共 Wi-Fi 网络进行连接。

以下主题介绍如何为您的网络配置远程接入 VPN。

- [远程接入 VPN 概述](#)，第 407 页
- [远程接入 VPN 的许可要求](#)，第 409 页
- [远程接入 VPN 的准则与限制](#)，第 409 页
- [配置远程接入 VPN](#)，第 410 页
- [监控远程接入 VPN](#)，第 419 页
- [远程接入 VPN 故障排除](#)，第 419 页
- [远程接入 VPN 示例](#)，第 421 页

远程接入 VPN 概述

您可以使用 Firepower 设备管理器，配置通过 SSL 借助 AnyConnect 客户端软件实现的远程接入 VPN。

AnyConnect 客户端与 Firepower 威胁防御设备协商 SSL VPN 连接时，会使用传输层安全 (TLS) 或数据报传输层安全 (DTLS) 进行连接。DTLS 可避免与某些 SSL 连接关联的延迟和带宽问题，并可提高对于数据包延迟敏感的实时应用的性能。客户端与 Firepower 威胁防御设备会协商要使用的 TLS/DTLS 版本。如果客户端支持 DTLS，则使用 DTLS。

各设备型号的最大并发 VPN 会话数量

根据设备型号，设备上允许的并发远程接入 VPN 会话数量有最大值限制。此限制用于确保系统性能不会降低到不可接受的水平。请使用这些限制进行容量规划。

设备型号	最大并发远程接入 VPN 会话数
ASA 5508-X	100
、ASA 5515-X	250
ASA 5516-X	300

设备型号	最大并发远程接入 VPN 会话数
ASA 5525-X	750
ASA 5545-X	2500
ASA 5555-X	5000
Firepower 2110	1500
Firepower 2120	3500
Firepower 2130	7500
Firepower 2140	10,000
Firepower 威胁防御虚拟	250
ISA 3000	25

下载 AnyConnect 客户端软件

在配置远程接入 VPN 之前，必须将 AnyConnect 软件下载到您的工作站。定义 VPN 时，您需要上传这些软件包。

您应该下载最新的 AnyConnect 版本，以确保获得最新的功能、漏洞修复和安全补丁。请定期更新 Firepower 威胁防御设备上的软件包。



注释 可以为以下每个操作系统上传一个 AnyConnect 软件包：Windows、Mac 和 Linux。无法为特定操作系统类型上传多个版本。

从 software.cisco.com 上的 AnyConnect 安全移动客户端类别中获取 AnyConnect 软件包。您需要下载客户端的“完全安装软件包”版本。

用户如何安装 AnyConnect 软件

要完成 VPN 连接，您的用户必须安装 AnyConnect 客户端软件。可以使用现有的软件分发方法直接安装该软件。或者，用户直接从 Firepower 威胁防御设备安装 AnyConnect 客户端。

用户必须对其工作站具有管理员权限才能安装软件。

安装 AnyConnect 客户端后，如果您将新的 AnyConnect 版本上传到系统，AnyConnect 客户端将在用户进行下一个 VPN 连接时检测到新版本。系统将自动提示用户下载并安装更新的客户端软件。这种自动化可为您和您的客户端简化软件分发。

如果您决定让用户一开始从 Firepower 威胁防御设备安装软件，请告诉用户执行以下步骤。



注释 Android 和 iOS 用户应从相应的应用商店下载 AnyConnect。

过程

步骤 1 使用 Web 浏览器，打开 <https://ravpn-address>，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。

您在配置远程接入 VPN 时确定此接口。系统提示用户登录。

步骤 2 登录到网站。

用户使用为远程接入 VPN 配置的目录服务器进行身份验证。登录成功后可继续操作。

如果登录成功，系统将确定用户是否已具有所需的 AnyConnect 客户端版本。如果用户的计算机上没有 AnyConnect 客户端，或者客户端的版本较低，系统将自动开始安装 AnyConnect 软件。

安装后，AnyConnect 会完成远程接入 VPN 连接。

远程接入 VPN 的许可要求

您的基本设备许可证必须满足出口要求，您才能配置远程接入 VPN。注册设备时，必须使用启用了出口管制功能的智能软件管理器账户。您也不能使用评估许可证配置该功能。

此外，您需要购买并启用远程接入 VPN 许可证，请选择以下任一项：AnyConnect Plus、AnyConnect Apex 或仅 AnyConnect VPN。即使这些许可证被设计为在与基于 ASA 软件的头端一起使用时允许不同的功能集，它们对于 Firepower 威胁防御设备都同等处理。

要启用许可证，请依次选择设备 > 智能许可证 > 查看配置，然后在远程接入 RA VPN 许可证组中选择正确的许可证。您需要在智能软件管理器账户中提供许可证。有关启用许可证的详细信息，请参阅 [启用或禁用可选许可证](#)，第 74 页。

有关详细信息，请参阅《思科 AnyConnect 订购指南》<http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf>。另外，<http://www.cisco.com/c/en/us/products/security/anyconnect-secure-mobility-client/datasheet-listing.html> 中还提供了其他数据表。

远程接入 VPN 的准则与限制

配置 RA VPN 时，请时刻注意以下准则和限制。

- 对于同一个 TCP 端口，无法在同一接口上同时配置 Firepower 设备管理器访问（管理访问列表中的 HTTPS 访问）和 AnyConnect 远程访问 SSL VPN。例如，如果在外部接口上配置远程访问

SSL VPN，则也无法在端口 443 上打开 HTTPS 连接的外部接口。因为无法在 Firepower 设备管理器中配置这些功能所使用的端口，所以无法在同一接口上配置这两项功能。

- 无法在 NAT 规则的源地址和远程接入 VPN 地址池中使用重叠地址。
- （仅限 REST API 配置。）如果您使用 RADIUS 和 RSA 令牌配置双因素身份验证，则在大多数情况下，12 秒的默认身份验证超时太短，无法实现成功的身份验证。您可以通过创建自定义 AnyConnect 客户端配置文件并将其应用到 RA VPN 连接配置文件，来增加身份验证超时值，如 [配置并上传客户端配置文件](#)，第 411 页中所述。建议身份验证超时时间最短为 60 秒，以使用户有足够的时间进行身份验证并粘贴 RSA 令牌，以及进行令牌往返验证。

配置远程接入 VPN

要为客户端启用远程接入 VPN，需要配置许多单独的项目。以下步骤程序介绍了端到端流程。

过程

步骤 1 配置许可证。

需要启用两个许可证：

- 注册设备时，必须使用启用了出口管制功能的智能软件管理器账户。基本许可证必须符合出口管制要求，然后才能配置远程接入 VPN。您也不能使用评估许可证配置该功能。有关注册设备的步骤程序，请参阅[注册设备](#)，第 73 页。
- 远程接入 VPN 许可证。有关详细信息，请参阅[远程接入 VPN 的许可要求](#)，第 409 页。要启用该许可证，请参阅[启用或禁用可选许可证](#)，第 74 页。

步骤 2 配置证书。

对客户端与设备之间的 SSL 连接进行身份验证需要使用证书。您可以将预定义的 DefaultInternalCertificate 用于 VPN，也可以自行创建证书。

如果对用于身份验证的目录领域使用加密连接，则必须上传受信任的 CA 证书。

有关证书及其上传方法的详细信息，请参阅[配置证书](#)，第 124 页。

步骤 3 （可选。）配置并上传客户端配置文件，第 411 页。

步骤 4 配置用于对远程用户进行身份验证的身份源。

您可以对允许登录远程接入 VPN 的用户账户使用以下源。

- Active Directory 身份领域 - 作为主要身份验证源。在 Active Directory AD 服务器中定义用户账户。请参阅[配置 AD 身份领域](#)，第 132 页。
- LocalIdentitySource（本地用户数据库）- 作为主要或回退源。您可以直接在设备上定义用户，不使用外部服务器。如果您使用本地数据库作为回退源，请确保您定义与外部服务器中定义的同用户名/密码。请参阅[配置本地用户](#)，第 141 页。

步骤 5 配置远程接入 VPN 连接，第 412 页。

步骤 6 允许流量通过远程接入 VPN，第 415 页。

步骤 7 (可选。) 控制远程接入 VPN 组对资源的访问，第 416 页。

如果您不希望所有远程接入用户访问所有内部资源的权限都相同，可以应用访问控制规则以根据用户组成员关系允许或阻止访问。

步骤 8 验证远程接入 VPN 配置，第 417 页。

如果在完成连接时遇到问题，请参阅[远程接入 VPN 故障排除](#)，第 419 页。

步骤 9 (可选。) 启用身份策略并配置被动身份验证规则。

如果启用被动用户验证，通过远程接入 VPN 登录的用户将显示在控制面板上，他们也可以用作策略中的流量匹配条件。如果不启用被动身份验证，只有当远程接入 VPN 用户匹配主动身份验证策略时，这些用户才可用。必须启用身份策略以在控制面板中获取任何用户名信息，或将其用于流量匹配。

配置并上传客户端配置文件

AnyConnect 客户端配置文件随 AnyConnect 客户端软件一起下载到客户端。这些配置文件定义与客户端相关的诸多选项，例如启动时自动连接和自动重新连接，以及是否允许终端用户更改 AnyConnect 客户端首选项和高级设置中的选项。

如果在配置远程接入 VPN 连接时为外部接口配置完全限定主机名 (FQDN)，系统将为您创建一个客户端配置文件。此配置文件启用默认设置。只有在需要非默认行为时，才需要创建和上传客户端配置文件。请注意，客户端配置文件是可选的：如果您不上传，AnyConnect 客户端将对所有配置文件控制选项使用默认设置。



注释 必须将 Firepower 威胁防御设备的外部接口添加到 VPN 配置文件的服务器列表中，以便 AnyConnect 客户端在第一次连接时显示所有用户可控的设置。如果您不将地址或 FQDN 添加为配置文件中的主机条目，则系统不会向会话应用过滤器。例如，如果您创建了一个证书匹配，且证书与条件正确匹配，但您未将设备添加为该配置文件中的主机条目，那么证书匹配将被忽略。

以下程序介绍了如何通过“对象”页面直接创建和编辑对象。另外，您还可以在编辑配置文件属性时，点击对象列表中所示的[创建新 AnyConnect 客户端配置文件](#)链接来创建 AnyConnect 客户端配置文件对象。

开始之前

在上传客户端配置文件之前，必须先执行以下操作。

- 下载并安装独立版 AnyConnect “配置文件编辑器 - Windows/独立版安装程序 (MSI)”。此安装文件仅适用于 Windows，文件名为 anyconnect-profileeditor-win-`<version>`-k9.msi，其中 `<version>` 指 AnyConnect 版本。例如，anyconnect-profileeditor-win-4.3.04027-k9.msi。您还必须在安装配

置文件编辑器之前安装 Java JRE 1.6（或更高版本）。从 software.cisco.com，在“AnyConnect 安全移动客户端”类别中，获取 AnyConnect 配置文件编辑器。

- 使用配置文件编辑器创建所需的配置文件。您应在配置文件中指定外部接口的主机名或 IP 地址。有关详细信息，请参阅编辑器的在线帮助。

过程

步骤 1 选择对象，然后从目录中选择 **AnyConnect 客户端配置文件**。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。
- 要下载与对象关联的配置文件，请点击对象的下载图标 (📄)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 为对象输入名称和（可选）说明。

步骤 4 点击上传并选择使用配置文件编辑器创建的文件。

步骤 5 点击打开上传配置文件。

步骤 6 点击确定添加对象。

配置远程接入 VPN 连接

您可以创建远程接入 VPN 连接，以允许用户在外部网络（例如其家庭网络）上时连接到您的内部网络。

开始之前

在配置远程接入 (RA) VPN 连接之前：

- 从 software.cisco.com 将所需的 AnyConnect 软件包下载到您的工作站。
- 或者，使用 AnyConnect 配置文件编辑器创建客户端配置文件。如果为外部接口指定了完全限定域名，系统将为您创建一个默认配置文件。客户端配置文件是可选的，仅当您想要自定义由配置文件控制的功能时才需要创建。
- 外部接口（作为远程接入 VPN 连接终端的那个外部接口）也不能具有允许 HTTPS 连接的管理访问列表。在配置 RA VPN 之前，从外部接口删除所有 HTTPS 规则。请参阅[配置管理访问列表](#)，第 447 页。

过程

步骤 1 点击**设备**，然后点击“远程接入 VPN”组中的**设置连接配置文件**。

您可以配置一个远程接入 VPN。如果已经配置了它，点击**查看配置**可打开现有的 VPN；点击**编辑**按钮可进行更改。

如果要删除该配置，请点击**清除配置**。

步骤 2 定义 AnyConnect 客户端配置。

- **连接配置文件名称** - 此连接的名称，最多 50 个字符，不能含空格。例如，MainOffice。不能将 IP 地址用作名称。

注释 您在此输入的名称将是用户在 AnyConnect 客户端的连接列表中看到的名称。选择一个对您的用户来说有意义的名称。

- **用户身份验证的身份源** - 用于对远程用户进行身份验证的主要身份源。必须在此源或可选的回退源中定义终端用户，才能完成 VPN 连接。选择以下一个选项：
 - **Active Directory (AD) 身份领域**。
 - **LocalIdentitySource**（本地用户数据库）- 您可以直接在设备上定义用户，而不使用外部服务器。
- **回退本地身份源** - 如果主要源是一个外部服务器，您可以选择 LocalIdentitySource 作为回退源，以防主服务器不可用。如果使用本地数据库作为回退源，请确保您定义的本地用户名/密码与外部服务器中的定义的用户名/密码相同。
- **AnyConnect 软件包** - 您将在此 VPN 连接上支持的 AnyConnect 完整安装软件映像。对于每个软件包，文件名（包括扩展名）不能超过 60 个字符。可以为 Windows、Mac 和 Linux 终端上传单独的软件包。

从 software.cisco.com 下载该软件包。如果终端尚未安装正确的软件包，系统会提示用户在用户验证后下载并安装软件包。

步骤 3 点击**下一步**。

步骤 4 定义设备身份和客户端寻址配置。

- **设备身份证书** - 选择用于建立设备身份的内部证书。客户端必须接受此证书才能完成安全的 VPN 连接。如果您还没有证书，请点击下拉列表中的**创建新内部证书**。您必须配置证书。
- **外部接口** - 用户在进行远程接入 VPN 连接时连接的接口。请选择您使用此连接配置文件支持的设备与终端用户之间的任何接口，虽然这通常是外部（面向互联网的）接口。
- **外部接口的完全限定域名** - 接口的名称，例如 ravpn.example.com。如果指定名称，系统可以为您创建一个客户端配置文件。

注释 您要确保 VPN 中和客户端使用的 DNS 服务器可以将此名称解析为外部接口的 IP 地址。将 FQDN 添加到相关 DNS 服务器。

- **IPv4、IPv6 地址池** - 这些选项为远程终端定义地址池。根据客户端用于建立 VPN 连接的 IP 版本，从这些池为客户端分配地址。选择一个网络对象，定义要支持的每个 IP 类型的子网。如果不想支持该 IP 版本，则选择无（或留空）。例如，可以将 IPv4 池定义为 10.100.10.0/24。地址池不能与外部接口的 IP 地址位于同一子网。
- **主要、辅助 DNS 服务器** - 当连接到 VPN 时，DNS 服务器客户端应用于域名解析。点击 **OpenDNS** 按钮以使用 OpenDNS 公共 DNS 服务器加载这些字段。或者，输入 DNS 服务器的 IP 地址。
- **域搜索名称** - 为您的网络输入域名，例如 example.com。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。

步骤 5 点击下一步。

步骤 6 定义连接设置以自定义 AnyConnect 客户端行为。

- **适用于通过身份验证的客户端的 banner 文本** -（可选）输入要在 VPN 会话开始时向用户显示的任何消息。例如，关于适当使用的法律免责声明和警告。Banner 最多可包含 500 个字符，但不能包含分号 (;) 或 HTML 标记。
- **最长连接时间** - 在不注销和重新连接的情况下，允许用户持续连接到 VPN 的最大时间长度（以分钟为单位），范围为 1 到 4473924 或留空。默认值为无限（留空），但空闲超时仍适用。
- **空闲超时** - VPN 连接在自动关闭之前可以闲置的时间长度（以分钟为单位），范围为 1 到 35791394。默认值为 30 分钟。
- **VPN 会话期间的浏览器代理** - 是否在 Windows 客户端设备上的 Internet Explorer Web 浏览器的 VPN 会话期间使用代理。从以下选项中进行选择：
 - **终端设置无变化** - 允许用户配置（或不配置）浏览器代理，并在已配置的情况下使用代理。
 - **禁用浏览器代理** - 不使用为浏览器定义的代理（如有）。浏览器连接不会通过该代理。
 - **自动检测设置** - 允许在浏览器中使用自动代理服务器检测。
 - **使用自定义设置** - 为客户端浏览器配置代理。输入 HTTP 代理服务器的 IP 地址和（可选）端口（主机和端口加起来不能超过 100 个字符）。如果要免除特定 Web 服务器通过代理的请求，也可以点击 **添加代理例外**（在例外列表中指定端口为可选项）。整个代理例外列表（包括所有地址和端口）不能超过 255 个字符。
- **分离隧道** - 启用分离隧道以允许用户在使用安全 VPN 隧道的同时直接访问本地网络或互联网。保持禁用分离隧道功能以确保 VPN 连接更安全。如果启用分离隧道，还必须选择代表远程用户将在 **内部网络** 列表中访问的内部网络的网络对象。网络列表必须包含与您支持的地址池相同的 IP 类型。对于指定的网络之外的任何网络，用户的 ISP 网关用于传输流量。
- **NAT 免除** - 启用 NAT 免除，使进出远程接入 VPN 终端的流量免于执行 NAT 转换。如果不免除 VPN 流量执行 NAT，请确保外部和内部接口的现有 NAT 规则不适用于 RA VPN 地址池。NAT 免除规则是给定源/目的接口和网络组合的手动静态身份 NAT 规则，但它们不会反映在 NAT 策略中，它们是隐藏起来的。如果启用 NAT 免除，还必须进行以下配置。
 - **内部接口** - 选择远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。

- **内部网络** - 选择代表远程用户将访问的内部网络的网络对象。网络列表必须包含与您支持的地址池相同的 IP 类型。
- **AnyConnect 客户端配置文件** - (可选。) 如果为外部接口配置的是完全限定域名，则系统将会为您创建默认配置文件。或者，您可上传您自己的客户端配置文件。使用独立的 AnyConnect 配置文件编辑器创建这些配置文件，您可以从 software.cisco.com 下载和安装该编辑器。如果不选择客户端配置文件，AnyConnect 客户端将为所有选项使用默认值。此列表中的项目是 AnyConnect 客户端配置文件对象，而不是配置文件本身。您可以通过点击下拉列表中的 **创建新的 AnyConnect 客户端配置文件**，创建 (和上传) 新配置文件。

步骤 7 点击下一步。

步骤 8 审核摘要。

首先，验证摘要是否正确。

然后，点击 **说明** 查看终端用户初步安装 AnyConnect 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击 **复制** 将这些说明复制到剪贴板，然后分发给您的用户。

步骤 9 点击完成。

下一步做什么

确保 VPN 隧道中允许流量，如 [允许流量通过远程接入 VPN](#)，第 415 页中所述。

默认情况下，VPN 终止流量会绕过访问控制策略，包括该策略中定义的任何高级检测，例如 URL 过滤、入侵保护或文件策略。如果想要访问控制策略评估并检测 VPN 流量，请使用 FlexConfig 配置 **no sysopt connection permit-vpn** 命令。然后，您可以配置访问控制规则以允许地址池和内部网络之间的流量从外部接口传输到内部接口。使用访问控制策略对 VPN 流量进行评估之前，系统会先将其解密，因此您可以应用入侵防御、URL 过滤等。

允许流量通过远程接入 VPN

创建远程接入 VPN 连接无法使系统通过 VPN 隧道发送流量。还必须配置以下其中一个设置：

- 配置 **sysopt connection permit-vpn** 命令，此命令会使匹配 VPN 连接的流量免受访问控制策略的限制。此命令的默认值是 **no sysopt connection permit-vpn**，这意味着 VPN 流量还必须获得访问控制策略的允许，

外部用户无法在远程接入 VPN 地址池中伪造 IP 地址，因此这种允许 VPN 流量的方法较为安全。但它的缺点是，VPN 流量得不到检测，也就是说不会对流量应用入侵和文件保护、URL 过滤或其他高级功能。同时，系统不会生成有关此流量的任何连接事件，且统计控制面板不会反映 VPN 连接。

使用 FlexConfig 配置此命令。

- 创建访问控制规则以允许来自远程接入 VPN 地址池的连接。此方法可确保对 VPN 流量进行检测，并将高级服务应用于连接。但它的缺点是，有可能造成外部用户伪造 IP 地址，进而获得访问内部网络的权限。

如果您希望基于用户组控制访问，则必须使用此选项，如[控制远程接入 VPN 组对资源的访问](#)，第 416 页中所述。

控制远程接入 VPN 组对资源的访问

如果您熟悉如何在 ASA 上配置远程接入 VPN 或在 FTD 设备上使用 Firepower 设备管理器配置远程接入 VPN，则您可能熟悉根据远程接入 VPN 组控制对网络中各种资源的访问。

在 Firepower 设备管理器中，您可以使用单个组策略配置单个连接配置文件。不过，通过直接实施身份策略和基于用户组的访问控制，也可以根据用户组控制访问。

以下流程程序介绍配置方式。

开始之前

此步骤程序假定您已配置远程接入 VPN (RA VPN) 和所需的身份领域。不过，您可以首先配置身份和访问控制策略，再配置 RA VPN。

此配置要求 VPN 流量受到访问控制策略的限制。在 CLI 中，使用 `show running-config` 命令来检查 `no sysopt connection permit-vpn` 命令是否已显示。如果不是在运行配置中，请使用 FlexConfig 配置此命令。

过程

步骤 1 在目录服务器中配置所需的用户组。

目录服务器必须包含用户组，而这些组必须包含符合要部署的策略的正确用户。例如，如果要区分工程用户和营销用户，并允许组成员访问不同的资源，则必须在目录服务器中定义这些用户的组。

不能直接在 FTD 设备上创建用户组。

有关创建用户组的信息，请参阅目录服务器文档。

步骤 2 依次选择 **策略 > 身份**，启用身份策略，然后创建一条规则以对 RA VPN 用户执行被动身份验证。

被动身份验证规则与 RA VPN 连接使用相同的领域。至少，必须设置一条身份策略，要求对包含 RA VPN 外部接口的区域的 RA VPN 地址池中的 IP 地址执行被动身份验证。

如果您有一揽子身份策略要求对所有地址和所有区域执行被动身份验证，则无需任何其他规则。

有关启用此策略和创建规则的信息，请参阅[配置身份策略](#)，第 244 页。

由于只有通过身份策略身份验证收集的名称才能用于基于用户的访问控制策略，所以必须配置身份规则。访问控制策略不能使用仅从 RA VPN 连接获取的、没有关联身份规则的用户名。请注意，覆盖远程接入 VPN 用户的主动身份验证规则也足以收集所需的用户身份信息。

步骤 3 点击菜单中的 **部署** 按钮，然后点击 **立即部署** 按钮以部署更改。



系统需要建立与目录服务器的连接并下载用户和用户组。部署配置从下载用户/组开始。如果不部署，则不可在访问控制规则中选择用户和组。

步骤 4 依次选择**策略 > 访问控制**，并创建基于组的访问控制规则。

现在，您即可创建访问控制规则来区分 RA VPN 用户的目录领域组。您可以创建常用的规则，也可以创建有针对性的具体规则。有关创建访问控制规则的信息，请参阅[配置访问控制规则](#)，第 267 页。

例如，根据“添加/编辑访问规则”对话框中的选项卡，针对特定 RA VPN 用户组的规则可能使用以下条件：

- **源/目标、区域** - 源区域应包括 RA VPN 外部接口。目标区域可以包括任何相关的内部接口。
- **源/目标、网络和端口** - 选择 RA VPN 地址池网络对象作为源网络，并选择定义受控资源的网络（或端口）对象作为目标网络/端口。如果应用或 URL 更适合您的要求，您可以不选择目标网络/端口，而使用应用或 URL 选项卡来定义目标资源。
- **用户** - 在此选项卡上选择特定目录组。这是提供基于组的访问控制的标准。
- **应用、URL** - 除源/目标选项卡上的目标网络/端口标准之外，您也可以使用这些标准。例如，您可以选择网络对象将规则限制为特定子网，然后选择应用来控制对目标网络上这些应用的访问。
- **入侵策略、文件策略** - 选择符合您要求的选项。这些选项可控制威胁，但不能控制对特定资源的访问。
- **日志记录** - 选择符合您要求的选项。您必须启用日志记录，才能查看监控控制面板中的任何结果或事件查看器中的连接事件。

验证远程接入 VPN 配置

在配置远程接入 VPN 并将该配置部署到设备后，请确认是否可以进行远程连接。

如果遇到问题，请阅读故障排除主题以帮助隔离和更正问题。请参阅[远程接入 VPN 故障排除](#)，第 419 页。

过程

步骤 1 在外部网络中，使用 AnyConnect 客户端建立 VPN 连接。

使用 Web 浏览器，打开 <https://ravpn-address>，其中 *ravpn-address* 是您允许 VPN 连接的外部接口的 IP 地址或主机名。如有必要，安装客户端软件并完成连接。请参阅[用户如何安装 AnyConnect 软件](#)，第 408 页。

步骤 2 登录到设备 CLI，如[登录命令行界面 \(CLI\)](#)，第 7 页中所述。或者，打开 CLI 控制台。

步骤 3 使用 `show vpn-sessiondb` 命令查看有关当前 VPN 会话的摘要信息。

统计信息应显示您的活动 AnyConnect 客户端会话以及有关累积会话、峰值并发会话数量和非活动会话的信息。以下是该命令的输出示例。

```

> show vpn-sessiondb
-----
VPN Session Summary
-----
Active : Cumulative : Peak Concur : Inactive
-----
AnyConnect Client      : 1 : 49 : 3 : 0
  SSL/TLS/DTLS        : 1 : 49 : 3 : 0
Clientless VPN        : 0 : 1 : 1 : 0
  Browser              : 0 : 1 : 1 : 0
-----
Total Active and Inactive : 1          Total Cumulative : 50
Device Total VPN Capacity : 10000
Device Load               : 0%
-----

Tunnels Summary
-----
Active : Cumulative : Peak Concurrent
-----
Clientless      : 0 : 1 : 1
AnyConnect-Parent : 1 : 49 : 3
SSL-Tunnel     : 1 : 46 : 3
DTLS-Tunnel    : 1 : 46 : 3
-----
Totals         : 3 : 142
-----

IPv6 Usage Summary
-----
Active : Cumulative : Peak Concurrent
-----
AnyConnect SSL/TLS/DTLS :  :  : 
  Tunneled IPv6         : 1 : 20 : 2
-----

```

步骤 4 使用 `show vpn-sessiondb anyconnect` 命令查看有关当前 AnyConnect VPN 会话的详细信息。

详细信息包括使用的加密方式、传输和接收的字节数及其他统计信息。如果使用 VPN 连接，随着您重新发出命令，您应可看到传输/接收的字节数会变化。

```

> show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username      : priya                Index      : 4820
Assigned IP   : 172.18.0.1           Public IP   : 192.168.2.20
Assigned IPv6 : 2009::1
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 27731                Bytes Rx    : 14427
Group Policy  : MyRaVpn|Policy       Tunnel Group : MyRaVpn
Login Time    : 21:58:10 UTC Mon Apr 10 2017
Duration      : 0h:51m:13s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                 VLAN        : none
Audt Sess ID  : c0a800fd012d400058ebffff2

```

Security Grp : none

Tunnel Zone : 0

监控远程接入 VPN

要监控和故障排除远程接入 VPN，请打开 CLI 控制台或登录设备 CLI 并使用以下命令。

- **show vpn-sessiondb** 显示有关 VPN 会话的信息。您可以使用 **clear vpn-sessiondb** 命令重置这些统计信息。
- **show webvpn keyword** 显示的是远程接入 VPN 配置相关信息，包括统计信息和安装的 AnyConnect 映像。输入 **show webvpn ?** 查看可用关键字。
- **show aaa-server** 可显示用于远程接入 VPN 的目录服务器的统计信息。

远程接入 VPN 故障排除

远程接入 VPN 连接问题可能源自客户端或 Firepower 威胁防御设备配置。以下主题介绍您可能会遇到的主要故障排除问题。

SSL 连接问题故障排除

如果用户无法对外部 IP 地址进行初始非 AnyConnect SSL 连接以下载 AnyConnect 客户端，请执行以下操作：

1. 从客户端工作站，验证能否对外部接口的 IP 地址执行 ping 命令。如果不能，请确定从用户工作站到该地址无路由的原因。
2. 从客户端工作站，验证能否对外部接口（即远程接入 [RA] VPN 连接配置文件中定义的接口）的完全限定域名 (FQDN) 执行 ping 操作。如果能够 ping 通 IP 地址但 ping 不通 FQDN，则需要更新客户端和 RA VPN 连接配置文件使用的 DNS 服务器，添加该 FQDN 到 IP 地址的映射。
3. 验证用户是否接受外部接口提供的证书。用户应该永久接受该证书。
4. 检查 RA VPN 连接配置，并验证您是否选择了正确的外部接口。一个常见错误是选择了面向内部网络的内部接口，而不是面向 RA VPN 用户的外部接口。
5. 如果正确配置了 SSL 加密，请使用外部嗅探器来验证 TCP 三次握手是否成功。

AnyConnect 下载和安装问题故障排除

如果用户可以与外部接口建立 SSL 连接，但无法下载和安装 AnyConnect 软件包，请考虑以下方面：

- 确保您已上传客户端操作系统适用的 AnyConnect 软件包。例如，如果用户的工作站运行的是 Linux，但您没有上传 Linux AnyConnect 映像，就没有可安装的软件包。
- 对于 Windows 客户端，用户必须获有管理员权限才能安装软件。
- 对于 Windows 客户端，工作站必须启用 ActiveX 或安装 Java JRE 1.5 或更高版本，推荐使用 JRE 7。
- 对于 Safari 浏览器，必须启用 Java。
- 请尝试不同的浏览器，一种浏览器失败不意味着其他浏览器也会失败。

AnyConnect 连接问题故障排除

如果用户能够连接到外部接口、下载并安装 AnyConnect 客户端，然后却无法使用 AnyConnect 完成连接，请考虑以下方面：

- 如果身份验证失败，请检验用户输入的用户名和密码是否正确，该用户名在身份验证服务器中的定义是否正确。身份验证服务器还必须可以通过一个数据接口使用。



注释 如果身份验证服务器在外部网络，则需要配置与该外部网络的站点间 VPN 连接，并将远程接入 VPN 接口地址包括在 VPN 中。有关详细信息，请参阅[如何通过远程接入 VPN 使用外部网络上的目录服务器](#)，第 428 页。

- 如果在远程接入 (RA) VPN 连接配置文件中为外部接口配置了完全限定域名 (FQDN)，请验证能否从客户端设备 ping 通该 FQDN。如果能够 ping 通 IP 地址但 ping 不通 FQDN，则需要更新客户端和 RA VPN 连接配置文件使用的 DNS 服务器，添加该 FQDN 到 IP 地址的映射。如果使用的是为外部接口指定 FQDN 时生成的默认 AnyConnect 客户端配置文件，用户需要编辑服务器地址才能使用 IP 地址，直到 DNS 被更新。
- 验证用户是否接受外部接口提供的证书。用户应该永久接受该证书。
- 如果用户的 AnyConnect 客户端包括多个连接配置文件，请检验其选择的连接配置文件是否正确。
- 如果客户端似乎一切正常，请与 Firepower 威胁防御设备建立 SSH 连接，并输入 `debug webvpn` 命令。检查尝试连接期间发出的消息。

RA VPN 流量问题故障排除

如果用户可以进行安全远程接入 (RA) VPN 连接，但无法发送和接收流量，请执行以下操作：

1. 使客户端断开连接，然后重新连接。有时此方法会消除问题。
2. 在 AnyConnect 客户端中，请检查流量统计信息以确定发送和接收的数据包计数器是否在增加。如果接收的数据包计数保持为零，则 Firepower 威胁防御设备未返回任何流量。这种情况下，Firepower 威胁防御配置可能存在问题。常见问题包括：

- 访问规则在阻止流量。检查访问控制策略是否包含阻止内部网络与 RA VPN 地址池之间传递流量的规则。如果您的默认操作是阻止流量，则可能需要创建一个显式“允许”规则。
 - RA VPN 流量没有绕过 NAT 规则。确保为每个内部接口的 RA VPN 连接配置 NAT 免除。或者，确保 NAT 规则不会阻止内部网络和接口与 RA VPN 地址池和外部接口之间的通信。
 - 路由配置错误。确保定义的所有路由有效并在正常工作。例如，如果您为外部接口定义了静态 IP 地址，请确保路由表包含默认路由（对于 0.0.0.0/0 和 ::/0）。
 - 确保为 RA VPN 配置的 DNS 服务器和域名正确，并且客户端系统使用的是正确的 DNS 服务器和域名。验证 DNS 服务器是否可访问。
 - 如果在 RA VPN 中启用分割隧道，请检查到指定内部网络的流量是否通过该隧道，而所有其他流量则绕过该隧道（以使 Firepower 威胁防御设备不可见）。
3. 与 Firepower 威胁防御设备建立 SSH 连接，并验证是否在为远程接入 VPN 发送和接收流量。使用以下命令。
- **show webvpn anyconnect**
 - **show vpn-sessiondb**

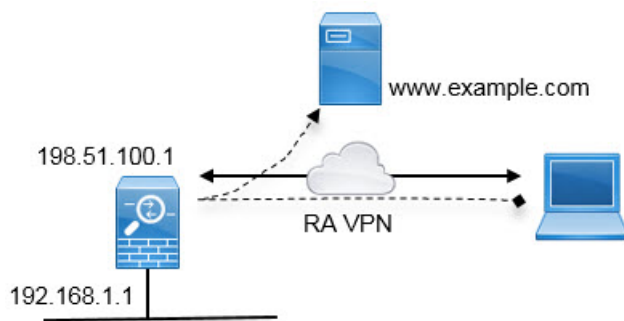
远程接入 VPN 示例

以下是配置远程接入 VPN 的示例。

如何在外部接口上为远程接入 VPN 用户提供互联网访问权限（发夹方法）

在远程接入 VPN 中，您可能希望远程网络用户通过您的设备访问互联网。不过，这些远程用户进入设备所用的接口与访问互联网所用的接口（外部接口）相同，因此需要使互联网流量从外部接口退出。这种技术有时候称为发夹方法。

下图展示了一个示例。外部接口 198.51.100.1 上配置了一个远程接入 VPN。您想要拆分远程用户的 VPN 隧道，以使退出的互联网流量重新回到外部接口，而流向内部网络的流量仍然流经设备。因此，如果远程用户想要访问互联网上的某个服务器（例如 www.example.com），连接会首先通过 VPN，然后从 198.51.100.1 接口路由回到互联网。



以下程序介绍如何配置此服务。

开始之前

此示例假定您已经注册设备、应用远程接入 VPN 许可证并上传 AnyConnect 客户端映像，同时还假定您已配置身份领域，并且此领域也用于身份策略。

此外，此程序假定您使用了允许 VPN 流量的默认设置，使 VPN 流量受访问控制策略的限制。在运行配置中，这由 `no sysopt connection permit-vpn` 命令表示。如果通过 FlexConfig 启用 `sysopt connection permit-vpn`，则无需执行这些步骤来配置访问控制规则。

过程

步骤 1 配置远程接入 VPN 连接配置文件。

- a) 点击设备，然后点击“远程接入 VPN”组中的设置连接配置文件。（如果已对配置文件进行配置，请点击查看配置）。

对于现有连接，点击编辑可修改配置文件。

- b) 配置连接配置文件设置：

- 连接配置文件名称 - 输入名称，例如 Corporate-RAVPN。
- 用于用户身份验证的身份源 - 选择用于远程用户身份验证的身份领域。如果尚未配置身份领域，请点击下拉列表底部的创建新身份领域立即创建。或者，可以使用 LocalIdentitySource 作为主要源或回退源。
- AnyConnect 软件包 - 上传适用于要支持的各个操作系统的 AnyConnect 客户端。等待上传完成，然后再继续。

连接配置文件设置应类似于以下内容：

Connection Profile Name

Corporate-RAVPN

Identity Source for User Authentication

AD

Fallback Local Identity Source


Note

If you want to use remote access user identity dashboards, you must enable the identity policy action to remote access VPN connections. [Er](#)

LocalIdentitySource

AnyConnect Packages

Windows

 anyconnect-win-4.4.00243-webdeploy-k9.pkg

Upload New

Choose another package to upload

c) 点击下一步，然后配置设备身份属性：

- **设备身份证书** - 选择用于建立设备身份的内部证书。客户端必须接受此证书才能完成安全的 VPN 连接。如果您没有自己的证书，可以使用 `DefaultInternalCertificate`。
- **外部接口** - 选择远程用户将要连接到的外部接口。通常，此接口名为“outside”。
- **外部接口的完全限定域名** - 如果外部接口有 DNS 名称，请在此输入。例如，`corporate-vpn.example.com`。

页面的设备身份部分可能如下所示：

Certificate of Device Identity

DefaultInternalCertificate

Outside Interface

AnyConnect clients connect to this interface

outside

Fully-qualified Domain Name for the Outside Interface

corporate-vpn.example.com

e.g. ad.example.com

- d) 继续向下浏览页面，配置 IPv4 地址池和（可选）IPv6 地址池。

选择用于标识网络的对象。系统将从该池为远程接入 VPN 用户分配地址。例如，指定 10.1.10.0/24 的网络对象。如果对象尚不存在，请点击列表底部的“创建新网络”。如果您支持这些地址，还要为 IPv6 配置池。

IPv4 Address Pool

Endpoints are provided an address from this pool

ravpn-pool

IPv6 Address Pool

Endpoints are provided an address from this pool

Please select

- e) 向下滚动页面，并配置远程连接的 DNS 设置。

输入所用 DNS 服务器的 IP 地址以及您的本地域名，例如 example.com。您可以点击 OpenDNS 以使用开放式 DNS 服务器。

Primary DNS IP Address

208.67.222.222

Secondary DNS IP Address

208.67.220.220

Domain Search Name

example.com

- f) 点击下一步，向下滚动，并配置“公司资源”选项。
(您还可以配置横幅、连接时间与超时以及代理设置，但这些设置与发夹方法没有直接关系。)

以下设置对于远程接入 VPN 中能否使用发夹方法至关重要。

- **拆分隧道** - 禁用此功能。您希望所有流量都通过 VPN 网关，而拆分隧道这种方法允许远程客户端直接访问 VPN 外部的本地或互联网站点。
- **NAT 免除** - 启用此功能。选择内部接口，然后选择定义内部网络的网络对象。在本示例中，该对象应指定 192.168.1.0/24。流向内部网络的 RA VPN 流量不会进行地址转换。但是，应用发夹方法的流量通过外部接口传出，因此这些流量仍会进行 NAT，因为 NAT 免除仅适用于内部接口。

Split Tunneling



NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



inside

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



local-network

- g) (可选) 选择 **AnyConnect** 客户端配置文件，然后点击下一步。
h) 查看远程接入 VPN 配置，然后点击完成。

步骤 2 将 NAT 规则配置为将外部接口发出的所有连接转换到外部 IP 地址上的端口（接口 PAT）。

完成初始设备配置后，系统将创建名为 `InsideOutsideNatRule` 的 NAT 规则。此规则将接口 PAT 应用于任意接口上通过外部接口流出设备的 IPv4 流量。由于外部接口包含在“任何”源接口中，因此，此规则已经存在，除非您对所需的规则进行编辑或将其删除。

以下程序介绍如何创建所需的规则。

- a) 依次点击**策略 > NAT**。
- b) 执行以下操作之一：
 - 要编辑 `InsideOutsideNatRule`，请将鼠标指针悬停在**操作**列上，然后点击编辑图标 (🔗)。
 - 要创建新规则，请点击 **+**。
- c) 配置规则的以下属性：
 - **名称** - 为新规则输入一个有意义且不含空格的名称。例如，`OutsideInterfacePAT`。
 - **创建规则的对象** - **手动 NAT**。
 - **位置** - **自动 NAT 规则之前**（默认）。
 - **类型** - **动态**。
 - **原始数据包** - 对于**源地址**，请选择“任何”或 `any-ipv4`。对于**源接口**，请确保选择“任何”（默认值）。对于所有其他“原始数据包”选项，请保留默认值“任何”。
 - **已转换的数据包** - 对于**目标接口**，请选择外部接口。对于**已转换的地址**，请选择接口。对于所有其他“已转换的数据包”选项，请保留默认值“任何”。

下图展示了选择“任何”作为源地址时的简单情况。

The screenshot shows the configuration for a Manual NAT rule. Key elements highlighted with red circles include:

- Title:** Create Rule for (Manual NAT)
- Placement:** Before Auto NAT Rules
- Type:** Dynamic
- ORIGINAL PACKET:** Source Interface: Any
- TRANSLATED PACKET:** Destination Interface: outside
- ORIGINAL PACKET:** Source Address: Any
- TRANSLATED PACKET:** Source Address: Interface

d) 点击确定。

步骤 3 配置访问控制规则，以允许从远程接入 VPN 地址池进行访问。

在以下示例中，允许来自地址池的流量流至任何目标。您可以根据自己的具体要求调整此选项。也可以在此规则之前添加阻止规则，过滤掉不必要的流量。

- 依次点击策略 > 访问控制。
- 点击 + 创建新规则。
- 配置规则的以下属性：

- **顺序** - 在策略中选择一个位置，此位置应位于可能会匹配并阻止这些连接的任何其他规则之前。默认情况下，会将该规则添加到策略的末尾。如果稍后需要重新调整规则的位置，可以编辑此选项，也可以直接将规则拖放到表格中相应的位置。
- **名称** - 输入一个有意义且不含空格的名词。例如，RAVPN-address-pool。
- **操作** - 允许。如果不希望对此流量执行协议违规检测或入侵检测，可以选择“信任”。
- **源/目标选项卡** - 对于源 > 网络，请选择在远程接入 VPN 连接配置文件中用于地址池的同一对象。对于所有其他“源”和“目标”选项，请保留默认值“任何”。

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
ANY	ravpn-pool	ANY	ANY	ANY	ANY

- 应用、URL 和用户选项卡 - 保留这些选项卡的默认设置，即不做任何选择。
- 入侵、文件选项卡 - (可选) 您可以选择入侵或文件策略，以进行威胁或恶意软件检测。
- 日志记录选项卡 - (可选) 您可以选择启用连接日志记录。

d) 单击 **OK**。

步骤 4 确认您的更改。

a) 点击网页右上角的部署更改图标。



b) 点击立即部署按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

如何通过远程接入 VPN 使用外部网络上的目录服务器

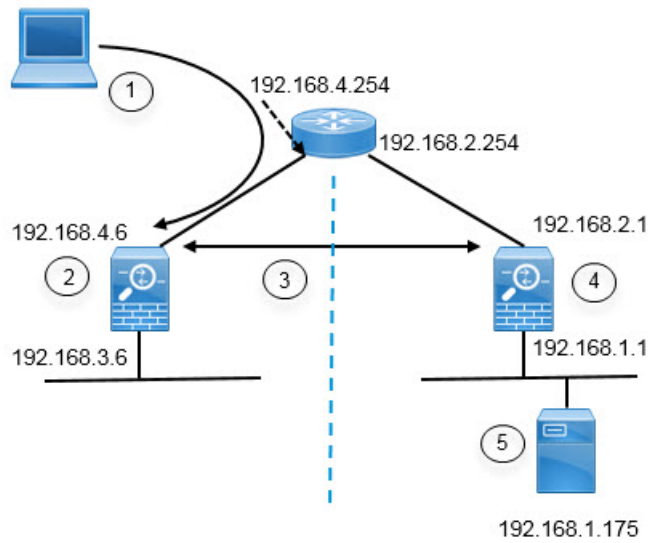
您可以配置远程接入 VPN，以便移动员工和远程办公人员安全地连接到内部网络。此连接的安全性取决于您的目录服务器，该目录服务器对用户连接进行身份验证，以确保仅授权用户才能登录。

如果您的目录服务器位于外部网络而非内部网络上，则需要配置从外部接口到包含目录服务器的网络的站点间 VPN 连接。站点间 VPN 配置有一个诀窍：您必须将远程接入 VPN 设备的外部接口地址包括在站点间 VPN 连接的“内部”网络内，还必须将其包括在目录服务器所在设备的远程网络中。后续程序会对此加以说明。



注释 如果使用数据接口作为虚拟管理接口的网关，此配置还允许将目录用于身份策略。如果不使用数据接口作为管理网关，请确保存在从管理网络到参与站点间 VPN 连接的内部网络的路由。

此使用案例实施以下网络场景。



图中标注	说明
1	与 192.168.4.6 建立 VPN 连接的远程访问主机。客户端将在 172.18.1.0/24 地址池中获得一个地址。
2	站点 A，托管远程接入 VPN。
3	站点 A 和站点 B FTD 设备的外部接口之间的站点间 VPN 隧道。
4	站点 B，托管目录服务器。
5	目录服务器，位于站点 B 的内部网络上。

开始之前

此使用案例假定您按照设备安装向导进行了正常的基准配置。具体包括：

- 有一条 Inside_Outside_Rule 访问控制规则，允许（或信任）从 inside_zone 到 outside_zone 的流量。
- inside_zone 和 outside_zone 安全区（分别）包含内部和外部接口。
- 有一个 InsideOutsideNATRule，对从内部接口到外部接口的所有流量执行接口 PAT。对于默认情况下使用内部桥接组的设备，可能存在多个接口 PAT 规则。
- 存在 0.0.0.0/0 的一条静态 IPv4 路由，指向外部接口。此示例假定您对外部接口使用静态 IP 地址，但也可以使用 DHCP 动态获取静态路由。在本示例中，我们假定采用以下静态路由：
 - 站点 A：外部接口，网关为 192.168.4.254。
 - 站点 B：外部接口，网关为 192.168.2.254。

过程

步骤 1 配置站点 B（托管目录服务器）上的站点间 VPN 连接。

- a) 点击设备，然后点击站点间 VPN 组中的查看配置。
- b) 点击 + 按钮。
- c) 为终端设置配置以下选项。
 - 连接配置文件名称 - 输入名称，例如 SiteA（表示连接到站点 A）。
 - 本地站点 - 这些选项定义本地终端。
 - 本地 VPN 访问接口 - 选择外部接口（图表中地址为 192.168.2.1 的那一个接口）。
 - 本地网络 - 点击 + 并选择标识应参与 VPN 连接的本地网络的网络对象。由于目录服务器在此网络上，因此可以参与站点间 VPN。假定该对象尚不存在，点击创建新网络并为 192.168.1.0/24 网络配置对象。在保存对象后，在下拉列表中选择它并点击确定。

Add Network Object

Name

Network192.168.1.0

Description

Type

Network Host

Network

192.168.1.0/24

- 远程站点 - 这些选项定义远程终端。
 - 远程 IP 地址 - 输入 192.168.4.6，这是将托管 VPN 连接的远程 VPN 对等体接口的 IP 地址。
 - 远程网络 - 点击 + 并选择标识应参与 VPN 连接的远程网络的网络对象。点击创建新网络，配置以下对象，然后在列表中选择它们。
 1. SiteAInside, 网络, 192.168.3.0/24。

Add Network Object

Name

SiteAInside

Description

Type

Network Host

Network

192.168.3.0/24

2. SiteAInterface, 主机, 192.168.4.6。这是关键：您必须将远程接入 VPN 连接点地址作为站点间 VPN 连接的远程网络的一部分，以便该接口上托管的 RA VPN 可以使用目录服务器。

Add Network Object

Name

SiteAInterface

Description

Type

Network Host

Host

192.168.4.6

完成后，终端设置应如下所示：

Connection Profile Name

SiteA

LOCAL SITE	REMOTE SITE
Local VPN Access Interface	Remote IP Address
outside	192.168.4.6
Local Network	Remote Network
+ Network192.168.1.0	+ SiteAInside SiteAInterface

- d) 点击下一步。
- e) 定义 VPN 的隐私配置。

在本使用案例中，我们假定您符合出口控制功能的要求，允许使用强加密。调整这些示例设置以满足您的需求和许可证合规性。

- **IKE 版本 2、IKE 版本 1** - 保留默认设置，启用 **IKE 版本 2**，禁用 **IKE 版本 1**。
- **IKE 策略** - 点击**编辑**并启用 **AES-GCM-NUL-LSHA** 和 **AES-SHA-SHA**，禁用 **DES-SHA-SHA**。
- **IPsec 提议** - 点击**编辑**。在“选择 IPsec 提议”对话框中，点击**+**，然后点击**设置默认值**以选择默认 AES-GCM 提议。
- **本地预共享密钥、远程对等体预共享密钥** - 输入此设备和远程设备上为 VPN 连接定义的密钥。这些密钥在 IKEv2 中可能不同。该密钥可以有 1 至 127 个字母数字字符。记住这些密钥，因为在站点 A 设备上创建站点间 VPN 连接时，必须配置相同的字符串。

IKE 策略应如下所示：

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE connections.

IKE VERSION 2



IKE VERSION 1



IKE Policy

Globally applied

EDIT...

IPSec Proposal

Default set selected

EDIT...

Local Pre-shared Key

●●●●●●●●

Remote Peer Pre-shared Key

●●●●●●●●

f) 配置其他选项。

- **NAT 免除** - 选择托管内部网络的接口，在本示例中为内部接口。通常，您不希望站点间 VPN 隧道中的流量转换其 IP 地址。此选项仅在本地网络驻留在单个路由接口（而非桥接组成员）后时有用。如果本地网络位于多个路由接口或一个或多个桥接组成员之后，则必须手动创建 NAT 免除规则。有关手动创建所需规则的信息，请参阅[使站点间 VPN 流量豁免 NAT](#)，第 394 页。
- **完美前向保密的 Diffie-Hellman 组** - 选择第 19 组。此选项决定是否使用完美前向保密 (PFS) 为每个加密交换生成和使用唯一会话密钥。唯一会话密钥可保护交换免于后续解密，即使整个交换已被记录且攻击者已经获得终端设备使用的预共享密钥或私钥。有关选项的说明，请查看[决定要使用的 Diffie-Hellman 模数组](#)，第 380 页。

该选项应如下所示：

Additional Options

NAT Exempt

inside



Diffie-Hellman Group for Perfect Forward Secrecy

19



- g) 点击下一步。
- h) 查看摘要并点击**完成**。

摘要信息将复制到剪贴板。您可以将这些信息粘贴到文档中，并使用它来帮助您配置远程对等体，或将其发送到负责配置对等体的一方。

- i) 点击网页右上角的**部署更改**图标。



- j) 点击**立即部署**按钮，并等待部署成功完成。

现在，站点 B 设备已准备好托管站点间 VPN 连接的一端。

步骤 2 注销站点 B 设备并登录站点 A 设备。

步骤 3 配置站点 A（托管远程接入 VPN）上的站点间 VPN 连接。

- a) 点击**设备**，然后点击站点间 VPN 组中的**查看配置**。
- b) 点击 **+** 按钮。
- c) 为**终端设置**配置以下选项。
 - **连接配置文件名称** - 输入名称，例如 SiteB（表示连接到站点 B）。
 - **本地站点** - 这些选项定义本地终端。
 - **本地 VPN 接入接口** - 选择外部接口（图表中地址为 192.168.4.6 的那一个接口）。
 - **本地网络** - 点击 **+** 并选择标识应参与 VPN 连接的本地网络的网络对象。点击**创建新网络**，配置以下对象，然后在列表中选择它们。注意，您已在站点 B 设备中创建相同的对象，但是您必须在站点 A 设备中重新创建它们。
 1. SiteAInside，网络，192.168.3.0/24。

Add Network Object

Name

SiteAInside

Description

Type

Network Host

Network

192.168.3.0/24

2. SiteAInterface, 主机, 192.168.4.6。这是关键：您必须将远程接入 VPN 连接点地址作为站点间 VPN 连接的内部网络的一部分，以便该接口上托管的 RA VPN 可以使用远程网络上的目录服务器。

Add Network Object

Name

SiteAInterface

Description

Type

Network Host

Host

192.168.4.6

- 远程站点 - 这些选项定义远程终端。
 - 远程 IP 地址 - 输入 192.168.2.1，这是将托管 VPN 连接的远程 VPN 对等体接口的 IP 地址。

- **远程网络** - 点击 + 并选择标识应该参与 VPN 连接的远程网络的网络对象（包含目录服务器的 VPN 连接）。点击**创建新网络**并为 192.168.1.0/24 网络配置对象。在保存对象后，在下拉列表中选择它并点击**确定**。注意，您已在**站点 B** 设备中创建相同的对象，但是您必须在**站点 A** 设备中重新创建它。

Add Network Object

Name

Network192.168.1.0

Description

Type

 Network
 Host

Network

192.168.1.0/24

完成后，终端设置应如下所示。请注意，与**站点 B** 设置相比，本地/远程网络是相反的。点对点连接的两端看起来应始终是这样的。

Connection Profile Name

SiteB

LOCAL SITE

Local VPN Access Interface

outside

REMOTE SITE

Remote IP Address

192.168.2.1

Local Network

+

SiteAInside

SiteAInterface

Remote Network

+

Network192.168.1.0

- 点击下一步。
- 定义 VPN 的隐私配置。

与站点 B 连接一样，配置相同的 IKE 版本、策略和 IPsec 提议，以及相同的预共享密钥，但请确保调换本地和远程预共享密钥。

IKE 策略应如下所示：

IKE Policy

i IKE policies are global, you cannot configure different policies per VPN. Any enabled IKE connections.

IKE VERSION 2 IKE VERSION 1

IKE Policy

Globally applied

IPSec Proposal

Default set selected

Local Pre-shared Key

●●●●●●●●

Remote Peer Pre-shared Key

●●●●●●●●

f) 配置其他选项。

- **NAT 免除** - 选择托管内部网络的接口，在本示例中为内部接口。通常，您不希望站点间 VPN 隧道中的流量转换其 IP 地址。此选项仅在本地网络驻留在单个路由接口（而非桥接组成员）后时有用。如果本地网络位于多个路由接口或一个或多个桥接组成员之后，则必须手动创建 NAT 免除规则。有关手动创建所需规则的信息，请参阅[使站点间 VPN 流量豁免 NAT](#)，第 394 页。
- **完美前向保密的 Diffie-Hellman 组** - 选择第 19 组。

该选项应如下所示：

Additional Options

NAT Exempt **i**

Diffie-Hellman Group for Perfect Forward Secrecy **i**

- g) 点击下一步。
- h) 查看摘要并点击完成。
- i) 点击网页右上角的部署更改图标。



- j) 点击立即部署按钮，并等待部署成功完成。

现在，站点 A 设备已准备好托管站点间 VPN 连接的另一端。由于站点 B 已经配置了兼容设置，因此两台设备应该协商 VPN 连接。

您可以登录设备 CLI 并对目录服务器进行 ping 测试，从而确认连接。您也可以使用 `show ipsec sa` 命令查看会话信息。

步骤 4 在站点 A 上配置目录服务器。点击测试验证是否有连接。

- a) 选择对象，然后从目录中选择身份源。
- b) 点击 + > AD。
- c) 配置基本领域属性。
 - 名称 - 目录领域的名称。例如，AD。
 - 类型 - 目录服务器的类型。Active Directory 是唯一支持的类型，所以无法更改此字段。
 - 目录用户名、目录密码 - 用户的标识名称和密码，该用户具备访问您要检索的用户信息的适当权限。对于 Active Directory，用户不需要更高的权限。您可以在域中指定任何用户。用户名必须是完全限定的；例如，Administrator@example.com（而不仅仅是 Administrator）。

注释 系统使用此信息生成 ldap-login-dn 和 ldap-login-password。例如，Administrator@example.com 被转换为 cn=adminisntrator、cn=users、dc=example、dc=com。请注意，cn=users 始终是此转换的一部分，因此您必须在公用名“users”文件夹下配置此处指定的用户。

- 基准 DN (Base DN) - 用于搜索或查询用户和组信息的目录树，即用户和组的公共父项。例如，cn=users、dc=example、dc=com。有关查找基准 DN 的信息，请参阅[确定目录基准标识名](#)，第 131 页。
- AD 主域 - 设备应加入的 Active Directory 完全限定域名。例如 example.com。

Name	Type
AD	Active Directory (AD)
Directory Username	Directory Password
Administrator@example.com
<small>e.g. user@example.com</small>	
Base DN	AD Primary Domain
cn=users,dc=example,dc=com	example.com
<small>e.g. ou=user, dc=example, dc=com</small>	<small>e.g. example.com</small>

d) 配置目录服务器属性。

- **主机名/IP 地址** - 目录服务器的主机名或 IP 地址。如果以加密方式连接到服务器，则必须输入完全限定域名，而非 IP 地址。在本例中，输入 192.168.1.175。
- **端口** - 用于与服务器通信的端口号。默认值为 389。如果选择 LDAPS 作为加密方法，请使用端口 636。在本例中，保留 389。
- **加密** - 使用加密连接下载用户和组信息。系统默认为无，也就是说以明文形式下载用户和组信息。对于 RA VPN，您可以使用 **LDAPS**，即基于 SSL 的 LDAP。如果选择此选项，则使用端口 636。RA VPN 不支持 STARTTLS。对于此示例，选择无。
- **受信任的 CA 证书** - 如果选择加密方法，请上传证书颁发机构 (CA) 证书以便在系统和目录服务器之间启用受信任的连接。如果要使用证书进行身份验证，则证书中的服务器名称必须与服务器主机名/IP 地址匹配。例如，如果使用 192.168.1.175 作为 IP 地址，但证书中的地址为 ad.example.com，则连接会失败。

Directory Server Configuration

Hostname / IP Address	Port
192.168.1.175	389
<small>e.g. ad.example.com</small>	
Encryption	Trusted CA certificate
NONE	Please select a certificate

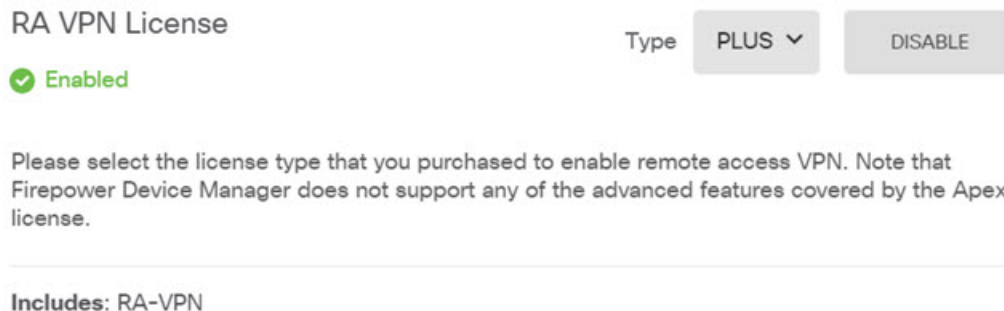
e) 点击测试按钮验证系统是否可以与服务器通信。

系统使用单独的进程访问服务器，因此您可能会收到错误通知，指出连接适用于一种用途而不适用于另一种用途，例如可用于身份策略，但不可用于远程接入 VPN。如果无法访问服务器，请确认 IP 地址和主机名正确、DNS 服务器具有该主机名的条目等。另外，验证站点间 VPN 连接是否正常工作，并且您在 VPN 中包含了站点 A 的外部接口地址，并且 NAT 不会转换目录服务器的流量。您可能还需要为服务器配置静态路由。

f) 点击确定。

步骤 5 依次点击设备 > 智能许可证 > 查看配置，然后启用 RA VPN 许可证。

启用 RA VPN 许可证时，请选择您购买的许可证类型：Plus、Apex（或两者）或仅 VPN。有关详细信息，请参阅[远程接入 VPN 的许可要求](#)，第 409 页。



步骤 6 在站点 A 上配置远程接入 VPN。

- a) 点击设备，然后点击“远程接入 VPN”组中的设置连接配置文件。
- b) 定义 AnyConnect 客户端配置。

- **连接配置文件名称** - 此连接的名称，最多 50 个字符，不能含空格。例如，MainOffice。不能将 IP 地址用作名称。

注释 您在此输入的名称将是用户在 AnyConnect 客户端的连接列表中看到的名称。选择一个对您的用户来说有意义的名称。

- **用户身份验证的身份源** - 选择目录领域。或者，您可以选择本地数据库作为回退身份源。
- **AnyConnect 软件包** - 您将在此 VPN 连接上支持的 AnyConnect 完整安装软件映像。对于每个软件包，文件名（包括扩展名）不能超过 60 个字符。可以为 Windows、Mac 和 Linux 终端上传单独的软件包。

从 software.cisco.com 下载软件包（页面底部右侧位置有链接）。如果终端尚未安装正确的软件包，系统会提示用户在用户验证后下载并安装软件包。

Connection Profile Name

MainOffice

Identity Source for User Authentication

AD

Fallback Local Identity Source

 Note

If you want to use remote access user identity dashboards, you must enable the identity policy action to remote access VPN connections. [Ena](#)

LocalIdentitySource

AnyConnect Packages

Windows

 anyconnect-win-4.4.00243-webdeploy-k9.pkg

Upload New

Choose another package to upload

- c) 点击下一步。
- d) 定义设备身份和客户端寻址配置。
 - 设备身份证书 - 选择 DefaultInternalCertificate。这是用于建立设备身份的内部证书。客户端必须接受此证书才能完成安全的 VPN 连接。如果您要使用其他证书，请在下拉列表中点击创建新的内部证书，并上传相应证书。
 - 外部接口 - 选择外部，即 IP 地址为 192.168.4.6 的接口。这是用户在远程接入 VPN 连接时要连接的接口。

Certificate of Device Identity

DefaultInternalCertificate

Outside Interface

AnyConnect clients connect to this interface

outside

- **外部接口的完全限定域名** - 接口的名称，例如 `ravpn.example.com`。如果指定名称，系统可以为您创建一个客户端配置文件。在本例中，我们将它留空。

注释 您要确保 VPN 中和客户端使用的 DNS 服务器可以将此名称解析为外部接口的 IP 地址。将 FQDN 添加到相关 DNS 服务器。

- **IPv4、IPv6 地址池** - 这些选项为远程终端定义地址池。对于本示例，在 IPv4 地址池中选择创建新的网络并为 `172.18.1.0/24` 网络创建一个对象，然后选择对象。从该地址池中为客户端分配地址。将 IPv6 池留空。地址池不能与外部接口的 IP 地址位于同一子网。

该对象应如下所示：

Name

ra-vpn-pool

Description

Type

Network

Network

172.18.1.0/24

该地址池规范应如下所示：

IPv4 Address Pool

Endpoints are provided an address from this pool

ra-vpn-pool

IPv6 Address Pool

Endpoints are provided an address from this pool

Please select

- **主要、辅助 DNS 服务器** - 在此示例中，点击 **OpenDNS** 按钮以使用 OpenDNS 公共 DNS 服务器加载这些字段。当连接 VPN 时，RA VPN 客户端使用这些 DNS 服务器客户端进行域名解析。或者，输入您的 DNS 服务器的 IP 地址。
- **域搜索名称** - 为您的网络输入域名，例如 `example.com`。此域将被添加到非完全限定的主机名，例如 `serverA` 而不是 `serverA.example.com`。

Primary DNS IP Address

208.67.222.222

Secondary DNS IP Address

208.67.220.220

Domain Search Name

example.com

- e) 点击下一步。
- f) 定义连接设置以自定义 AnyConnect 客户端行为。

保留所有选项的默认设置，因为它们适用于大多数网络。

由于选择了 **NAT 免除**，您需要配置以下选项：

- **内部接口** - 选择内部接口。这些是远程用户将要访问的内部网络的接口。所创建的 NAT 规则用于这些接口。
- **内部网络** - 选择 SiteAInside 网络对象。这些是代表远程用户将访问的内部网络的网络对象。

Split Tunneling



NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal network.



inside

Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions must match, either IPv4, IPv6, or both.



SiteAInside

- g) 点击下一步。
- h) 审核摘要。

首先，验证摘要是否正确。

然后，点击**说明**查看终端用户初步安装 AnyConnect 软件需要做什么，并测试他们是否可以完成 VPN 连接。点击**复制**以将这些说明复制到剪贴板，然后将它们粘贴在文本文件或邮件中。

i) 点击**完成**。

步骤 7 点击网页右上角的**部署更改**图标。



步骤 8 点击**立即部署**按钮，并等待部署成功完成。

现在，站点 A 设备已准备好接受 RA VPN 连接。让外部用户安装 AnyConnect 客户端并完成 VPN 连接。

您可以登录设备 CLI 并使用 **show vpn-sessiondb anyconnect** 命令查看会话信息，从而确认连接。



第 **VI** 部分

系统管理

- [系统设置](#)，第 447 页
- [系统管理](#)，第 463 页



第 20 章

系统设置

以下主题介绍如何配置一起划分到“系统设置”页面的各种系统设置。这些设置涵盖整个系统功能。

- [配置管理访问列表，第 447 页](#)
- [配置诊断日志记录，第 449 页](#)
- [配置 DHCP 服务器，第 450 页](#)
- [配置 DNS，第 452 页](#)
- [配置管理接口，第 455 页](#)
- [配置设备主机名，第 457 页](#)
- [配置网络时间协议 \(NTP\)，第 457 页](#)
- [配置 URL 过滤首选项，第 458 页](#)
- [配置云服务，第 458 页](#)

配置管理访问列表

默认情况下，您可以从任何 IP 地址的管理地址访问设备的 Firepower 设备管理器 Web 或 CLI 界面。系统访问仅受用户名/密码的保护。但是，您可以配置访问列表以仅允许来自特定 IP 地址或子网的连接，以进一步加强保护。

您还可以开放数据接口，允许建立 Firepower 设备管理器连接或与 CLI 建立 SSH 连接。然后，无需使用管理地址即可管理设备。例如，您可以允许对外部接口进行管理访问，这样就能远程配置设备。用户名/密码可防止不希望看到的连接。默认情况下，对数据接口的 HTTPS 管理访问会在内部接口上启用而在外部接口上禁用。对于具有默认“内部”桥接组的设备型号，这意味着可以通过桥接组中的任意数据接口，与桥接组 IP 地址（默认值为 192.168.1.1）建立 Firepower 设备管理器连接。您可以只在进入设备所通过的接口上开放管理连接。



注意

如果只允许访问特定地址，那么您可能很容易将自己锁定在系统之外。如果删除对当前所用 IP 地址的访问，并且没有“任意”地址条目，则在部署策略时将丢失对系统的访问。如果决定配置访问列表，必须非常小心。

开始之前

不可在同一个 TCP 端口的同一个接口上配置 Firepower 设备管理器访问（HTTPS 访问）和 AnyConnect 远程访问 SSL VPN。例如，如果在外部接口上配置远程访问 SSL VPN，则也无法在端口 443 上打开 HTTPS 连接的外部接口。因为无法在 Firepower 设备管理器中配置这些功能所使用的端口，所以无法在同一接口上配置这两项功能。

过程

步骤 1 点击 **设备**，然后点击 **系统设置 > 管理访问** 链接。

如果您已位于“系统设置”页面，只需依次点击目录中的 **管理访问**。


您还可以在此页面上配置 AAA，允许外部 AAA 服务器中定义的用户进行管理访问。有关详细信息，请参阅 [管理 FDM 和 FTD 用户访问权限](#)，第 478 页。

步骤 2 要为管理地址创建规则，请执行以下操作：

a) 选择 **管理接口** 选项卡。

规则列表定义了允许哪些地址访问指定的端口：对于 Firepower 设备管理器（HTTPS Web 界面）而言，该端口为 443；对于 SSH CLI 而言，该端口为 22。

规则不是一个有序列表。如果一个 IP 地址与请求的端口的任意规则匹配，则用户可以尝试登录设备。

注释 要删除规则，请点击该规则的垃圾桶图标 。如果删除了某个协议的所有规则，则没有人可以使用该协议访问该接口上的设备。

b) 点击 **+** 并填写以下选项：

- **协议** - 选择规则是用于 HTTPS（端口 443）还是 SSH（端口 22）。
- **IP 地址** - 选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4 (0.0.0.0/0)** 和 **any-ipv6 (:::0)**。


c) 点击 **确定**。

步骤 3 要为数据接口创建规则，请执行以下操作：

a) 选择 **数据接口** 选项卡。

规则列表定义允许访问接口上专用端口的地址：443 用于 Firepower 设备管理器（HTTPS 网络接口），22 用于 SSH CLI。

规则不是一个有序列表。如果一个 IP 地址与请求的端口的任意规则匹配，则用户可以尝试登录设备。

注释 要删除规则，请点击该规则的垃圾桶图标 。如果删除了某个协议的所有规则，则没有人可以使用该协议访问该接口上的设备。

b) 点击 **+** 并填写以下选项：

- **接口** - 选择要在其上允许管理访问的接口。
- **协议** - 选择规则是用于 HTTPS（端口 443）、SSH（端口 22）还是二者。不能为远程接入 VPN 连接配置文件中使用的外部接口配置 HTTPS 规则。
- **允许的网络** - 选择定义应该能够访问系统的 IPv4 或 IPv6 网络或主机的网络对象。要指定“任何”地址，请选择 **any-ipv4** (0.0.0.0/0) 和 **any-ipv6** (::/0)。

c) 单击 **OK**。

配置诊断日志记录

诊断日志记录可为与连接不相关的事件提供系统日志消息。可以在各个访问控制规则内配置连接日志记录。以下步骤介绍如何配置诊断消息的日志记录。

过程

步骤 1 点击 **设备**，然后点击 **系统设置 > 日志记录设置** 链接。

如果已经位于“系统设置”页面中，只需点击目录中的 **日志记录设置**

步骤 2 点击 **诊断日志设置 > 开**。

即使配置了本页的剩余字段，只要未开启此设置，就不会生成诊断日志消息。

步骤 3 针对您要查看诊断日志消息的每个位置，将滑块转至 **开** 的位置，然后选择一个最低严重性级别。

可以将日志消息记录到以下位置：

- **控制台** - 当在控制台端口上登录 CLI 时会显示这些消息。使用 **show console-output** 命令也可以在其他界面（包括管理地址）的 SSH 会话中看到这些日志。此外，从主 CLI 中输入 **system support diagnostic-cli** 即可在诊断 CLI 中实时看到这些消息。
- **系统日志** - 这些消息将发送到您指定的外部系统日志服务器。点击 **+**，选择系统日志服务器对象，然后在弹出对话框中点击 **确定**。如果服务器对象尚不存在，请点击 **添加系统日志服务器** 创建对象。

步骤 4 点击 **保存**。

严重性级别

下表列出系统日志消息严重性级别。

表 11: 系统日志消息严重级别

级别号	严重性级别	说明
0	紧急	系统不可用。
1	警报	需要立即采取措施。
2	严重	严重情况。
3	错误	错误情况。
4	警告	警告情况。
5	通知	正常但重大的情况。
6	信息性	消息仅供参考。
7	调试	消息仅供调试。



注释 Firepower 威胁防御 不会生成严重性级别为零（紧急）的系统日志消息。

配置 DHCP 服务器

DHCP 服务器可为 DHCP 客户端提供网络配置参数，例如 IP 地址。您可以在接口上配置 DHCP 服务器，为连接的网络上的 DHCP 客户端提供配置参数。

IPv4 DHCP 客户端使用广播而非组播地址到达服务器。DHCP 客户端侦听 UDP 端口 68 上的消息；DHCP 服务器侦听 UDP 端口 67 上的消息。DHCP 服务器不支持 BOOTP 请求。

DHCP 客户端必须与启用了服务器的接口位于同一网络内。即服务器和客户端之间不能有干预路由器，但可以有交换机。



注释 不要在已经有 DHCP 服务器运行的网络上配置 DHCP 服务器。这两个服务器将发生冲突，结果不可预测。

过程

步骤 1 点击设备，然后点击系统设置 > DHCP 服务器链接。

如果已经位于“系统设置”页面中，只需点击目录中的 **DHCP 服务器**

该页有两个选项卡。一开始，配置选项卡显示全局参数。

DHCP 服务器选项卡显示已在其上配置 DHCP 服务器的接口、服务器启用情况以及服务器的地址池。

步骤 2 在**配置**选项卡上，配置自动配置和全局设置。

DHCP 自动配置使 DHCP 服务器能为 DHCP 客户端提供从运行于指定接口上的 DHCP 客户端获得的 DNS 服务器、域名和 WINS 服务器信息。通常，如果您是在使用 DHCP 获取地址，则会使用自动配置，但您可以选择通过 DHCP 获取其地址的任何接口。如果无法使用自动配置，可以手动定义所需的选项。

- a) 如果要使用自动配置，请点击**启用自动配置**>**开**（滑块应位于右侧），然后在**源接口**中选择正在通过 DHCP 获取其地址的接口。
- b) 如果不启用自动配置，或者如果要覆盖任何一个自动配置的设置，请配置以下全局选项。这些设置将发送到托管 DHCP 服务器的所有接口上的 DHCP 客户端。
 - **主 WINS IP 地址、辅助 WINS IP 地址** - Windows Internet Name Service (WINS) 服务器客户端应该用于 NetBIOS 域名解析的地址。
 - **主 DNS IP 地址、辅助 DNS IP 地址** - 客户端应该用于域名解析的域名系统 (DNS) 服务器的地址。如果要配置 OpenDNS 公共 DNS 服务器，请点击**使用 OpenDNS**。点击该按钮会将正确的 IP 地址加载到字段中。
- c) 点击**保存**。

步骤 3 点击**DHCP 服务器**选项卡并配置服务器。

- a) 执行以下操作之一：
 - 要为尚未列出的接口配置 DHCP 服务器，请点击 **+**。
 - 要编辑现有的 DHCP 服务器，请点击该服务器的编辑图标 (🔗)。要删除服务器，请点击该服务器的垃圾桶图标 (🗑️)。
- b) 配置服务器属性：
 - **启用 DHCP 服务器** - 是否启用服务器。您可以配置服务器，但在做好准备开始使用之前，要一直将其禁用。
 - **接口** - 选择您为客户端提供 DHCP 地址的接口。接口必须拥有静态 IP 地址；如果要在接口上运行 DHCP 服务器，则不能使用 DHCP 获取接口。对于桥接组，在网桥虚拟接口 (BVI) 上（而不是成员接口上）配置 DHCP 服务器，并且服务器在所有成员接口上运行。
您不能在诊断接口上配置 DHCP 服务器，而应在管理接口上配置，它位于**设备**>**系统设置**>**管理接口**页面。
 - **地址池** - 允许服务器为请求地址的客户端提供的 IP 地址的范围（最低至最高）。指定该池的开始和结束地址，用连字符隔开。例如 10.100.10.12-10.100.10.250。
该 IP 地址范围必须与所选接口位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。

FTD设备上地址池的大小不得超过每个池 256 个地址。如果地址池范围大于 253 个地址，则 FTD接口的网络掩码不能为 C 类地址（例如 255.255.255.0）且需要成为更大的地址，例如 255.255.254.0。

c) 单击 **OK**。

配置 DNS

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。DNS 服务器的配置在初始系统设置期间执行，并且这些服务器将应用于数据和管理接口。您可以在设置完成后对其进行更改，并对数据和管理接口使用单独的一组服务器。

至少，必须要为管理接口配置 DNS。如果您想要使用基于 FQDN 的访问控制规则，或想要在 CLI 命令（如 **ping**）中使用主机名，那么还必须要为数据接口配置 DNS。

DNS 的配置分两步完成：配置 DNS 组，然后在接口上配置 DNS。

以下主题更详细地介绍了这一过程。

配置 DNS 组

DNS 组定义 DNS 服务器列表和某些相关联的属性。您可以在管理和数据接口上单独配置 DNS。需要使用 DNS 服务器将完全限定域名 (FQDN) 解析为 IP 地址，例如 `www.example.com`。



完成设备设置向导后，您将有一个或两个系统定义的以下 DNS 组：


- **CiscoUmbrellaDNSServerGroup** - 此组包括思科 Umbrella 所搭配 DNS 服务器的 IP 地址。如果您在初始设置期间选择了这些服务器，此组便是系统定义的唯一组。您无法更改此组中的名称或服务器列表，但您可以编辑其他属性。
- **CustomDNSServerGroup** - 如果您不在设备设置期间选择 Umbrella 服务器，系统将使用您的服务器列表创建此组。您可以编辑此组中的任何属性。

过程

步骤 1 选择对象，然后从目录中选择 **DNS 组**。

步骤 2 执行以下操作之一：

- 要创建组，请点击 **添加组** () 按钮。
- 要编辑组，请点击该组的编辑图标 ()。

要删除未引用的对象，请点击该对象的垃圾桶图标 ()。

步骤 3 配置以下属性：

- **名称** - DNS 服务器组的名称。保留 DefaultDNS 名称：不能使用该名称。
- **DNS IP 地址** - 输入 DNS 服务器的 IP 地址。点击添加另一个 **DNS IP 地址** 配置多个服务器。如果您想要删除服务器地址，请点击该地址的删除图标 (🗑️)。

列表采用优先顺序：始终使用列表中的第一个服务器，只有当从前面的服务器收不到响应时，才使用后面的服务器。您最多可以配置 6 个服务器。但是，仅数据接口上支持 6 个服务器。管理接口仅使用前面的 3 个服务器。

- **域搜索名称** - 为您的网络输入域名，例如 example.com。此域将被添加到非完全限定的主机名，例如 serverA 而不是 serverA.example.com。名称必须不能超过 63 个字符以使用数据接口组。
- **重试次数** - 系统接收不到响应时，重试 DNS 服务器列表的次数，介于 0 和 10 次之间。默认值为 2。此设置仅适用于数据接口上使用的 DNS 组。
- **超时 (Timeout)** - 尝试下一个 DNS 服务器之前要等待的秒数，介于 1 和 30 秒之间。默认值为 2 秒。每次系统重试服务器列表，此超时将加倍。此设置仅适用于数据接口上使用的 DNS 组。

步骤 4 单击 **OK**。

为数据和管理接口配置 DNS

域名系统 (DNS) 服务器用来将主机名解析到 IP 地址。最初，数据和管理 DNS 配置基于设备设置向导中配置的 DNS 服务器。可以使用以下过程更改默认设置。

您还可以在 CLI 中使用 **configure network dns servers** 和 **configure network dns searchdomains** 命令更改 DNS 配置。如果数据和管理接口使用相同的 DNS 组，组将更新，且所做的更改也会在下一个部署中应用到数据接口。

如果您无法进行 DNS 解析，请参阅：

- [常规 DNS 问题故障排除，第 454 页](#)
- [为管理接口排除 DNS 故障，第 489 页](#)

过程

步骤 1 点击设备，然后点击系统设置 > DNS 服务器链接。

如果已经位于“系统设置”页面中，只需点击目录中的 **DNS 服务器**。

步骤 2 为数据接口配置 DNS。

a) (可选。) 点击 + 并选择要用来执行 DNS 查找的接口。

默认和推荐的值为任何，以便（基于路由表）在所有接口上进行查找。请仅在您知道应通过这些接口访问的 DNS 服务器时，选择特定接口。请仅在您为其配置了 IP 地址时，选择诊断接口。如果现有路由不足以将流量定向到服务器，您可能需要为 DNS 服务器配置静态路由。

- b) 选择定义在数据接口上使用的服务器的 **DNS 组**。如果组尚不存在，请点击**创建新的 DNS 组**立即创建组。如果您想要阻止在数据接口上进行查找，请选择**无**。
- c) （可选。）如果在访问控制规则中使用 FQDN 网络对象，配置 **FQDN DNS 设置**。

仅解析 FQDN 对象时使用这些选项，任何其他类型的 DNS 解析都将忽略这些选项。

- **轮询时间** - 将 FQDN 网络对象解析为 IP 地址的轮询周期，以分钟为单位。仅在访问控制策略中使用 FQDN 对象时，解析这些对象。计时器决定两次解析之间的最长时间；DNS 条目的生存时间 (TTL) 值也用于确定更新 IP 地址解析的时间，因此，解析单个 FQDN 的频率可能大于轮询周期。默认设置为 240（4 个小时）。范围为 1 至 65535 分钟。
- **过期** - DNS 条目过期（即，超出从 DNS 服务器获得的 TTL）后，从 DNS 查找表中删除该条目前等待的分钟数。删除条目要求重新编译表，使频繁删除能够增加设备上的处理负载。因为某些 DNS 条目可以有非常短的 TTL（短至 3 秒），所以您能够使用此设置实际上延长 TTL。默认设置为 1 分钟（即，TTL 过去后 1 分钟，会删除条目）。范围为 1 至 65535 分钟。

- d) 点击**保存**。您还必须部署配置，将更改应用到设备。

步骤 3 为管理接口配置 DNS。

- a) 选择定义在管理接口上使用的服务器的 **DNS 组**。如果组尚不存在，请点击**创建新的 DNS 组**立即创建组。
- b) 点击**保存**。所做的更改会立即应用到设备。不需要运行部署作业来应用此更改。

常规 DNS 问题故障排除

必须为管理和数据接口单独配置 DNS 服务器。某些功能通过这两类接口中的其中一类接口，而不是这两类接口，解析域名。有时，给定的功能将使用不同的解析方法，具体取决于您如何使用该功能。

例如，**ping hostname** 和 **ping interface interface_name hostname** 命令使用数据接口 DNS 服务器解析域名，而 **ping system hostname** 命令使用管理接口 DNS 服务器。这使您可以通过特定接口和路由表测试连接。

故障排除主机名查找问题时，请记住这一点。

有关排除管理接口 DNS 故障的信息，另请参阅[为管理接口排除 DNS 故障](#)，第 489 页。

未发生域名解析

如果根本没有发生域名解析，可参照以下故障排除提示。

- 验证您是否已为管理和数据接口均配置 DNS 服务器。对于数据接口，对接口使用“任何”设置。仅当可以通过这些接口访问 DNS 服务器时，明确指定接口。
- 如果您在数据接口上将诊断接口用于查找，请确认您在此接口上配置了 IP 地址。查找需要此接口具备 IP 地址。

- 执行 **ping** 操作，以验证是否可访问每个 DNS 服务器的 IP 地址。使用 **system** 和 **interface** 关键字测试特定接口。如果 **ping** 操作不成功，请检查您的静态路由和网关。您可能需要为服务器添加静态路由。
- 如果 **ping** 操作成功，但域名解析失败，请检查访问控制规则。验证您是否允许连接服务器的接口的 DNS 流量 (UDP/53)。此流量也可能被系统和 DNS 服务器之间的设备阻止，因此您可能需要使用不同的 DNS 服务器。
- 如果 **ping** 操作成功、路由充足，并且访问控制规则不是症结所在，请考虑 DNS 服务器是否存在 FQDN 映射。您可能需要使用不同的服务器。

域名解析错误

如果进行了域名解析，但名称的 IP 地址不是最新地址，可能存在缓存问题。此问题仅影响基于数据接口的功能，例如访问控制规则中使用的 FQDN 网络对象。

系统有从前期查找中获得的 DNS 信息的本地缓存。需要新的查询时，系统首先在本地缓存中查找。如果本地缓存中有该信息，则将返回生成的 IP 地址。如果本地缓存无法解析该请求，则将 DNS 查询发送至 DNS 服务器。如果外部 DNS 服务器解析请求，则生成的 IP 地址与其相应的主机名一起存储在本地缓存中。

每个查找都有一个生存时间值，该值由 DNS 服务器定义并自动从缓存到期。此外，系统会为访问控制规则中使用的 FQDN 定期刷新该值。至少，系统会按照轮询时间间隔（默认情况下，每 4 小时一次）刷新，不过可根据该条目的生存时间值，增加刷新频率。

使用 **show dns-hosts** 和 **show dns** 命令检查本地缓存。如果 FQDN 的 IP 地址错误，可以使用 **dns update [host hostname]** 命令强制系统刷新信息。如果在使用此命令时没有指定主机，系统会刷新所有主机名。

可以使用 **clear dns [host fqdn]** 和 **clear dns-hosts cache** 命令删除缓存的信息。

配置管理接口

管理接口是连接到物理管理端口的虚拟接口。该物理端口名为诊断接口，可在“接口”页面上使用其他物理端口进行配置。在 Firepower 威胁防御虚拟上，即使两个接口都是虚拟接口，这种双重性也保持不变。

管理接口有两种用途：

- 您可以与该 IP 地址建立 Web 连接和 SSH 连接，并通过该接口配置设备。
- 系统通过此 IP 地址获取智能许可和数据库更新。

如果使用 CLI 安装向导，则在初始系统配置期间，为设备配置管理地址和网关。如果使用 Firepower 设备管理器安装向导，管理地址和网关将保留默认值。

如果需要，可以通过 Firepower 设备管理器更改这些地址。您还可以在 CLI 中使用 **configure network ipv4 manual** 和 **configure network ipv6 manual** 命令更改管理地址和网关。

您可以定义静态地址，也可以在管理网络中有另一台设备用作 DHCP 服务器时，通过 DHCP 获取地址。默认情况下，管理地址是静态的，而且 DHCP 服务器通常在端口上运行（Firepower 威胁防御虚拟除外，它没有 DHCP 服务器）。因此，您可以将设备直接连接到管理端口并为工作站获取 DHCP 地址。这种方法可以十分方便地连接和配置设备。



注意 如果更改当前连接的地址，则当保存更改时，由于这些更改会立即应用，您将丢失对 Firepower 设备管理器（或 CL）的访问。您需要重新连接到设备。确保新地址有效且在管理网络中可用。

过程

步骤 1 点击**设备**，然后依次点击**系统设置 > 管理接口**链接。

如果已经位于“系统设置”页面中，只需点击目录中的**管理接口**

步骤 2 选择要如何定义管理网关。

网关确定系统如何访问互联网，以获取智能许可证、数据库更新（例如 VDB、规则、地理位置、URL）以及访问管理 DNS 和 NTP 服务器。从以下选项中选择：

- **使用数据接口作为网关** - 如果没有单独的管理网络连接物理管理接口，请选择此选项。流量根据路由表路由到互联网，通常经过外部接口。这是默认选项。但是，Firepower 威胁防御虚拟设备不支持此选项。
- **为管理接口使用独特网关** - 如果您有单独的管理网络连接管理接口，请为 IPv4 和 IPv6 指定独特网关（如下所示）。

步骤 3 配置管理地址、子网掩码或 IPv6 前缀，并根据需要配置 IPv4 和/或 IPv6 的网关。

必须配置至少一组属性。将一组设置留空将会禁用该寻址方法。

依次选择**类型 > DHCP**，通过 DHCP 或 IPv6 自动配置功能获取地址和网关。但是，如果使用数据接口作为网关，则不能使用 DHCP。在此情况下，必须使用静态地址。

步骤 4 （可选。）如果配置的是静态 IPv4 地址，请在该端口上配置 DHCP 服务器。

如果在管理端口上配置 DHCP 服务器，则直接连接的客户端或管理网络中的客户端可从 DHCP 池获取其地址。Firepower 威胁防御虚拟设备不支持此选项。

- a) 依次点击**启用 DHCP 服务器 > 开**。
- b) 输入服务器的**地址池**。

地址池是允许服务器为请求地址的客户端提供的 IP 地址的范围（最低至最高）。该 IP 地址范围必须与管理地址位于同一子网上，并且不能包括接口本身的 IP 地址、广播地址或子网地址。指定该池的开始和结束地址，用连字符隔开。例如 192.168.45.46-192.168.45.254。

步骤 5 点击**保存**，阅读警告，然后点击**确定**。

配置设备主机名

可以更改设备主机名。

您还可以在 CLI 中使用 **configure network hostname** 命令更改主机名。



注意 如果更改连接到系统所用的主机名，由于这些更改会立即应用，因此您将丢失对 Firepower 设备管理器的访问。您需要重新连接到设备。

过程

步骤 1 点击 **设备**，然后点击 **系统设置 > 主机名** 链接。

如果已经位于“系统设置”页面中，只需点击目录中的 **主机名**

步骤 2 输入新主机名。

步骤 3 点击 **保存**。

主机名更改随后立即应用到某些系统进程。但是，您必须部署更改以完成更新，以便所有系统进程都使用相同的名称。

配置网络时间协议 (NTP)

必须配置网络时间协议 (NTP) 服务器才能在系统上定义时间。NTP 服务器在初始系统设置期间配置，但您可以使用以下步骤程序对其进行更改。如果您无法连接到 NTP，请参阅 [排除 NTP 故障](#)，第 488 页。

过程

步骤 1 点击 **设备**，然后点击 **系统设置 > NTP** 链接。

如果已经位于“系统设置”页面中，只需点击目录中的 **NTP**

步骤 2 在 **NTP 时间服务器** 中，选择使用您自己的时间服务器还是思科时间服务器。

- **默认 NTP 时间服务器** - 如果选择此选项，服务器列表会显示用于 NTP 的服务器名称。
- **用户定义的 NTP 服务器** - 如果选择此选项，则输入您要使用的 NTP 服务器的完全限定域名或 IP 地址。例如 ntp1.example.com 或 10.100.10.10。如果您有多个 NTP 服务器，请点击 **添加另一个 NTP 时间服务器** 并输入地址。

步骤 3 点击保存。

配置URL 过滤首选项

系统从思科综合安全情报 (CSI) 获取 URL 类别和信誉数据库。这些首选项控制数据库更新和系统如何处理类别或信誉未知的 URL。必须启用 URL 过滤许可证，才能设置这些首选项。

过程

步骤 1 点击 **设备**，然后点击 **系统设置 > URL 过滤首选项** 链接。

如果已经位于“系统设置”页面中，只需依次点击目录中的 **URL 过滤首选项**

步骤 2 配置以下选项：

- **启用自动更新** - 允许系统自动检查和下载更新的 URL 数据，这些数据中包括类别和信誉信息。系统每 30 分钟检查一次更新，不过数据通常每天更新一次。默认会启用更新。如果取消选中该选项，并且在使用类别和信誉过滤，请定期启用该功能以获得新的 URL 数据。
- **通过思科 CSI 查询未知 URL** - 对在本地 URL 过滤数据库中不含类别和信誉数据的 URL，是否通过思科 CSI 查询其更新的信息。如果查询在合理的时间限制内返回此信息，则在根据 URL 标准选择访问规则是使用。否则，URL 将匹配未分类的类别。对因内存限制而安装较小 URL 数据库的低端系统而言，选择此选项非常重要。
- **URL 生存时间**（选择对未知 URL 查询思科 CSI 时可用）- 特定 URL 的类别和信誉查找值的缓存时间。生存时间到期时，下一个 URL 访问尝试将导致新的类别/信誉查找。更短的时间会产生更准确的 URL 过滤，较长的时间会给未知 URL 带来更好的表现。您可以将 TTL 设置为 2、4、8、12、24 或 48 小时、一周或从不（默认）。

步骤 3 点击保存。

配置云服务

使用“云服务”页面从设备端管理设备使用的基于云的服务。注册某些服务后，需从云端进行管理。

您可以点击页面顶部的 **云服务门户** 链接以转到思科云服务，并管理基于云的服务。

以下主题介绍云服务选项。

配置云管理（思科防御协调器）

您可以使用思科 Defense Orchestrator 基于云的门户来管理设备。使用思科 Defense Orchestrator，您可以通过以下方法来进行设备管理：

- 下载初始配置 - 在此方法中，您从思科 Defense Orchestrator 下载初始设备配置，但之后使用 Firepower 设备管理器在本地配置设备。



注释 使用 Firepower 设备管理器配置设备后，如果您决定要通过云管理设备，请确保在基于云的配置中复制本地更改。

- 通过云进行远程配置管理 - 在此方法中，您使用思科 Defense Orchestrator 创建和更新设备配置。使用此方法时，不要对配置进行本地更改，因为在每个云部署中，云中定义的配置将替换设备上的本地配置。如果进行了本地更改，请确保在基于云的配置中重复此配置以保存更改。

有关云管理原理的更多信息，请参阅思科 Defense Orchestrator 门户 (<http://www.cisco.com/go/cdo>) 或咨询您的经销商或合作伙伴。

开始之前

获取思科防御协调器的注册密钥。

如果您已向思科智能软件管理器 (CSSM) 注册该设备，我们强烈建议您首先从智能许可页面注销设备。您可以在使用令牌启用思科防御协调器后重新注册。

此外，请确保设备有到互联网的路由。



注释 如果您想要配置高可用性，则必须注册您要在高可用性组中使用的两台设备。

过程

步骤 1 点击**设备**，然后依次点击**系统设置** > **云服务**链接。

如果已经位于“系统设置”页面，只需点击目录中的**云服务**。

步骤 2 在思科 **Defense Orchestrator** 组中点击**开始**。

步骤 3 在注册密钥然后点击**连接**。

注册请求将发送到云门户。如果密钥有效，并且有通往互联网的路由，则设备会成功注册到门户。然后，您便可以开始使用门户来管理设备了。

如果您决定不想再使用云管理，可以点击**禁用**按钮。

连接到思科成功网络

注册设备时，需决定是否启用与思科成功网络之间的连接。请参阅[注册设备](#)，第 73 页。

通过启用思科成功网络，可以向思科提供使用信息和统计信息，这对思科为您提供技术支持至关重要。通过此信息，思科还可以改进产品，并使您获悉未使用的可用功能，以便您能够在网络中将产品的价值最大化。

启用连接时，设备将与思科云建立安全连接，以确保设备可以参与思科提供的其他服务（例如技术支持服务、云管理和监控服务）。您的设备将随时建立并维护此安全连接。有关从云完全断开连接的信息，请参阅[禁用思科云服务注册](#)，第 460 页。

注册设备后，可以更改思科成功网络设置。



注释 系统向思科发送数据时，任务列表会显示一项遥测作业。

开始之前

要启用思科成功网络，必须向云注册设备。要注册该设备，请使用思科智能软件管理器（在“智能许可”页面上）注册该设备，或者通过输入注册密钥使用思科 Defense Orchestrator 进行注册。



注释 如果您在高可用性组的主用设备上启用思科成功网络，也会在备用设备上启用该连接。

过程

步骤 1 点击设备，然后点击系统设置 > 云服务链接。

如果已经位于“系统设置”页面，只需点击目录中的云服务。

步骤 2 点击思科成功网络功能的启用/禁用控件，可以根据需要更改设置。

可以点击[样本数据](#)链接，查看发送给思科的信息类型。

启用该连接时，请阅读披露的信息并点击接受。

禁用思科云服务注册

向思科防御协调器注册设备后，请启用思科成功网络，或向思科智能软件管理器注册设备，设备会注册思科云服务。即使禁用所有云服务，设备仍会保持注册状态。

启用连接时，设备将与思科云服务建立安全连接，以确保设备可以参与思科提供的其他服务（例如技术支持服务、云管理和监控服务）。您的设备将随时建立并维护此安全连接。

您可能希望删除设备的思科云服务注册，以便可以在不同的智能许可账户下注册，或者从服务中删除设备。

过程

步骤 1 在**设备 > 系统设置 > 云服务**页面上禁用所有云服务。

步骤 2 从齿轮下拉列表中选择**设备 > 智能许可证**并选择**注销设备**。

步骤 3 如果要向云重新注册设备，请执行以下操作之一：

- 要使用思科安全账户，请选择**设备 > 系统设置 > 云服务**，并使用令牌向思科防御协调器重新注册。然后，可以转至**设备 > 智能许可证**并重新注册设备。
 - 要使用智能许可证账户，请在**设备 > 智能许可证**页面上注册设备。现在，可以返回至“云服务”页面并重新启用所需服务。
-

启用或禁用网络分析

启用网络分析可根据页面点击量向思科提供匿名产品使用情况信息。这类信息包括查看的页面、在页面上花费的时间、浏览器版本、产品版本、设备主机名等。此信息可帮助思科确定功能使用模式，帮助思科改进产品。所有使用情况数据均为匿名数据，且不会传输敏感数据。

默认启用网络分析。

过程

步骤 1 点击**设备**，然后点击**系统设置 > 云服务**链接。

如果已经位于“系统设置”页面，只需点击目录中的**云服务**。

步骤 2 点击**网络分析**功能的**启用/禁用**控件，根据需要更改设置。



第 21 章

系统管理

以下主题介绍如何执行系统管理任务，例如更新系统数据库及备份和恢复系统。

- [安装软件更新，第 463 页](#)
- [备份和恢复系统，第 468 页](#)
- [审核与变更管理，第 472 页](#)
- [导出设备配置，第 478 页](#)
- [管理 FDM 和 FTD 用户访问权限，第 478 页](#)
- [重新启动系统，第 482 页](#)
- [系统故障排除，第 483 页](#)
- [不常见的管理任务，第 494 页](#)

安装软件更新

您可以安装系统数据库和系统软件的更新。以下主题介绍如何安装这些更新。

更新系统数据库和源

系统使用许多个数据库和安全情报源来提供高级服务。思科会对这些数据库和源提供更新，以便您的安全策略采用可用的最新信息。

系统数据库和源更新概述

Firepower 威胁防御使用以下数据库和源提供高级服务。

入侵规则

随着新的漏洞被发现，思科 Talos 情报小组 (Talos) 会发布入侵规则更新，您可以导入更新的规则。这些更新会影响入侵规则、预处理器规则和使用这些规则的策略。

入侵规则更新提供全新和更新的入侵规则及预处理器规则、现有规则的修改状态和修改的默认入侵策略设置。另外，规则更新还可能删除规则，提供新规则类别和默认变量，并修改默认变量值。

要使入侵规则更新所做的更改生效，必须重新部署配置。

入侵规则更新可能很大，所以请在网络使用量低的环境下更新重要规则。在慢速网络中，更新尝试可能会失败，您将需要重试。

地理位置数据库 (GeoDB)

思科地理位置数据库 (GeoDB) 包含与可路由 IP 地址关联的地理数据（例如国家/地区、城市、坐标）和连接相关数据（例如互联网服务提供商、域名、连接类型）。

GeoDB 更新物理位置、连接类型等方面的更新信息，系统会将这些信息与所检测到的可路由 IP 地址相关联。您可以使用地理位置数据作为访问控制规则的条件。

更新 GeoDB 所需的时间取决于您的设备；安装通常需要 30-40 分钟。虽然 GeoDB 更新不会中断任何其他系统功能（包括正在进行的地理位置信息收集），但更新执行时确实会占用系统资源。制定更新计划时需要考虑这一点。

漏洞数据库 (VDB)

思科漏洞数据库 (VDB) 包含主机可能易受感染的已知漏洞，以及操作系统、客户端和应用程序指纹。Firepower 系统可将指纹与漏洞关联，帮助您确定某个特定主机是否会增加网络受攻击的风险。思科 Talos 情报小组 (Talos) 定期发布 VDB 更新。

更新漏洞映射所需的时间取决于网络映射中的主机数量。您可能希望在系统使用量低的期间安排更新，以尽可能地降低对任何系统停机的影响。一般说来，将网络中的主机数除以 1000，即可估算出执行更新所需的大致时间（分钟）。

在更新 VDB 后必须部署配置，才能使更新的应用检测器和操作系统指纹生效。

思科 Talos 情报小组 (Talos) 安全情报源

Talos 提供对安全情报策略中使用的定期更新情报源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。这些源包含已知威胁的地址和 URL。当系统更新源时，不必重新部署。新列表可用于评估后续连接。

URL 类别/信誉数据库

系统从思科综合安全情报 (CSI) 获取 URL 类别和信誉数据库。如果您配置过滤类别和信誉的 URL 过滤访问控制规则，请求的 URL 将根据数据库进行匹配。您可以在系统设置 > URL 过滤首选项上配置数据库更新和某些其他 URL 过滤首选项。您不能通过管理其他系统数据库更新的方式管理 URL 类别/信誉数据库更新。

更新系统数据库

您可以在方便之时，手动检索和执行系统数据库更新。从思科支持站点可检索更新。因此，系统的管理地址必须可连接互联网。

另外，您还可以设置计划来定期检索和应用数据库更新。由于这些更新可能很大，所以请将它们安排在网络活动少的时间进行更新。



注释 在更新数据库时，您可能会发现用户界面响应操作的速度迟缓。

开始之前

为了避免对进行的更改造成任何潜在影响，请先将配置部署到设备，再手动更新这些数据库。

请注意，VDB 和 URL 类别更新可删除应用或类别。您需要更新使用这些已弃用项目的任何访问控制或 SSL 解密规则，然后才能部署更改。

过程

步骤 1 点击 **设备**，然后点击“更新”摘要中的**查看配置**。

此时将打开“更新”页面。该页面上的信息显示每个数据库的当前版本，以及每个数据库的最后更新日期和时间。

步骤 2 要手动更新数据库，请点击该数据库的**立即更新**部分。

规则和 VDB 更新需要部署配置，使其处于活动状态。系统会询问是否要立即部署；点击**是**。如果点击**否**，请记住尽早启动部署作业。

步骤 3（可选）要设置定期数据库更新计划，请执行以下操作：

a) 点击所需数据库的**配置**链接部分。如果已有计划，请点击**编辑**。

数据库的更新计划是独立的。您必须单独定义计划。

b) 设置更新开始时间：

- 更新频率（每日、每周或每月）。
- 对于每周或每月更新，希望在星期几或每月几日执行更新。
- 希望开始更新的时间。您指定的时间已根据夏令时调整，因此当您所在地区的时间被调整时，它会向前或向后移动一小时。如果您想要在全年确保此时间准确无误，您必须在时间被更改时编辑计划。

c) 对于规则或 VDB 更新，如果希望系统在更新数据库时部署配置，请选中**自动部署更新**复选框。

更新在完成部署之前无效。自动部署还将部署尚未部署的任何其他配置更改。

d) 点击**保存**。

注释 如果要删除定期更新计划，请点击**编辑**链接打开计划对话框，然后点击**删除**按钮。

更新思科安全情报源

思科 Talos 情报小组 (Talos) 提供对定期更新的安全情报源的访问权限。具有安全威胁（如恶意软件、垃圾邮件、僵尸网络和网络钓鱼）的站点出现和消失的速度可能比您更新和部署自定义配置的速度要快。当系统更新源时，不必重新部署。新列表可用于评估后续连接。

如果要对系统从互联网更新源的时间进行严格控制，可以禁用该源的自动更新。但是，自动更新可确保获取最新的相关数据。

过程

步骤 1 点击设备，然后点击“更新”摘要中的**查看配置**。

此时将打开“更新”页面。页面上的信息显示**安全情报源**的当前版本以及其上次更新日期和时间。

步骤 2 要手动更新源，请点击**安全情报源**组中的**立即更新**。

如果您在高可用性组中的一台设备上手动更新源，也需要在另一台设备上手动进行此更新，以确保一致性。

步骤 3（可选。）要配置定期更新频率，请执行以下操作：

- a) 点击“思科源”部分中的**配置**链接。如果已有计划，请点击**编辑**。
- b) 选择所需的频率。

默认值为**每小时**。您还可以设置**每日更新**（指定具体时间）或**每周更新**（选择星期几和具体时间）。您指定的时间已根据夏令时调整，因此当您所在地区的时间被调整时，它会向前或向后移动一小时。如果您想要在全年确保此时间准确无误，您必须在时间被更改时编辑计划。

点击**删除**阻止自动更新。

- c) 单击 **OK**。
-

升级 Firepower 威胁防御软件

您可以在 Firepower 威胁防御软件升级可用时安装升级。以下程序假定您的系统已在运行 Firepower 威胁防御6.2.0 版或更高版本，并且它们运行正常。

升级有三种：热修补、次要升级和主要升级。热修补升级可能不需要重新启动系统，而次要和主要版本升级则的确需要重新启动。如果需要重新启动，系统会在安装后自动重新启动。安装任何更新都可能造成流量中断，因此请在非工作时间进行安装。

如果您要升级高可用性组中的设备，请升级备用设备，切换模式以交换主用/备用设备，然后在新的备用设备上安装升级。有关详细信息，请参阅[在高可用性设备上安装软件升级](#)，第 171 页。

使用此程序无法重新映像设备或从 ASA 软件迁移到 Firepower 威胁防御软件。



注释 如有任何等待完成的更改，请务必在安装更新前部署这些更改。此外，您还应该运行备份并下载备份副本。

开始之前

查看任务列表，并确认没有任务正在运行。等所有任务（例如数据库更新）均完成后再安装升级。此外，检查是否有任何已计划的任務。任何计划任务都不得与升级任务重叠。

执行更新前，请确保应用过滤器、访问规则或 SSL 解密规则中不存在已弃用应用。这些应用的应用名称后面带有“(Deprecated)”。虽然无法将已弃用应用添加至这些对象，但后续 VDB 更新可能会使先前有效应用变为弃用应用。如果发生这种情况，则升级将失败，导致设备处于不可用状态。

登录 Cisco.com，下载升级映像。

- 确保获得适当的升级文件（文件类型为 REL.tar）。请勿下载系统软件包或引导映像。
- 请勿对更新文件重命名。系统将重命名的文件视为无效。
- 您无法降级或卸载补丁。
- 确认您是否正在运行升级所需的基准映像。有关兼容性信息，请参阅《思科 Firepower 兼容性指南》，网址是：
<http://www.cisco.com/c/en/us/td/docs/security/firepower/compatibility/firepower-compatibility.html>。
- 阅读有关新版本的版本说明。您可以在 <http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-release-notes-list.html> 找到发行说明。

过程

步骤 1 选择设备，然后点击“更新”摘要中的**查看配置**。

系统升级部分将显示当前运行的软件版本和您已上传的任何更新。

步骤 2 上传升级文件。

- 如果尚未上传升级文件，请点击**浏览**并选择该文件。
- 如果已有上传的文件，但要上传与之不同的文件，请点击**上传其他文件**链接。只能上传一个文件。如果上传新文件，它将取代旧文件。
- 要删除该文件，请点击删除图标 (🗑️)。

步骤 3 点击**安装**开始安装过程。

图标旁的信息表示设备是否会在安装期间重新启动。您将从系统中自动注销。安装可能需要 30 分钟或更长时间。

请耐心等待，然后重新登录系统。“设备摘要”（或“系统监控”控制面板）应该显示新版本。

注释 不要只刷新浏览器窗口，而要从 URL 中删除所有路径，然后重新连接到主页。这可确保使用最新代码刷新缓存的信息。

步骤 4（可选。）更新系统数据库。

如果没有为地理位置、规则和漏洞数据库 (VDB) 配置自动更新作业，现在正是对其进行更新的好时机。

重新映像设备

重新映像设备包括擦除设备配置和安装新软件映像。重新映像是为了通过出厂默认配置实现安全安装。

在以下情况下，您可以重新映像设备：

- 要将系统从 ASA 软件转换为 Firepower 威胁防御 软件。无法将运行 ASA 映像的设备升级为运行 Firepower 威胁防御 映像的设备。
- 设备运行的是 6.1.0 版本之前的映像，而您要升级到 6.1 或更高版本的映像，并使用 Firepower 设备管理器配置设备。无法使用 Firepower 管理中心升级 6.1 版本之前的设备，然后再切换到本地管理。
- 设备无法正常工作，而修复配置的所有尝试均失败。

有关如何重新映像设备的信息，请参阅针对您的设备型号的编写的《重新映像思科 ASA 或 Firepower 威胁防御设备指南》或《Firepower 威胁防御快速入门指南》。如需查阅上述指南，请访问 <http://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-guides-list.html>。

备份和恢复系统

您可以备份系统配置，这样在配置因后续配置错误或物理故障而受损时即可恢复设备。

仅当两台设备的型号相同且运行相同版本的软件（包括内部版本号，而不仅仅是相同的发布版）时，才可将备份恢复到替换设备上。请勿使用备份和恢复过程在设备之间复制配置。备份文件包含唯一标识设备的信息，所以不能按此方式进行共享。



注释

备份不包括管理 IP 地址配置。因此，恢复备份文件时，不会从备份副本中替换管理地址。这可以确保保存对地址所做的任何更改，并且还可以在其他网段的其他设备上恢复配置。

备份仅包括配置，而不是系统软件。如果需要完全重新映像设备，您需要重新安装软件，然后才能上传备份和恢复配置。

在备份期间将锁定配置数据库。在备份期间不能更改配置，但可以查看策略、控制面板等。在恢复期间，系统完全不可用。

“备份和恢复” (Backup and Restore) 页面的表格将列出系统中可用的所有现有备份副本，包括备份的文件名、创建日期和时间及文件大小。备份类型（手动、预定或周期性）以您指示系统创建该备份副本的方式为基础。



提示

备份副本在系统中创建。您必须手动下载备份副本，并将它们存储到安全服务器上，以确保拥有执行灾难恢复所需的备份副本。

以下主题介绍如何管理备份和恢复操作。

立即备份系统

您可以根据需要随时开始备份。

过程

步骤 1 点击 **设备**，然后点击“备份和恢复”摘要中的**查看配置**。

点击后随即会打开“备份和恢复”页面。表格中将列出系统中可用的所有现有备份副本。

步骤 2 依次点击**手动备份 > 立即备份**。

步骤 3 输入备份名称和描述（后者为可选项）。

如果决定以后再进行备份（而不是立即进行），可以改为点击**计划**。

步骤 4（仅限于 ISA 3000）选择**备份文件的位置**。

您可以在**本地硬盘**或**SD 卡**上创建备份。使用 SD 卡的好处是，您可以使用卡将配置恢复到替换设备。

步骤 5 点击**立即备份**。

系统将开始备份过程。备份完成后，备份文件将显示在表格中。然后，您即可将备份副本下载到系统并存储到其他位置（如需）。

初始化备份后，即可离开“备份和恢复”页面。但是，系统可能会非常缓慢，您应考虑暂停您的工作以让备份完成。

此外，系统将在部分或所有备份期间获取配置数据库上的锁，这可能会阻止您在备份过程的持续时间内进行更改。

在预定时间备份系统

您可以设置预定备份，以便在将来的某个特定日期和时间备份系统。预定备份是一次性事件。如果要创建备份计划以定期创建备份，请配置周期性备份，而不是预定备份。



注释 如果要删除将来备份计划，请编辑该计划并点击**删除**。

过程

步骤 1 点击 **设备**，然后点击“备份和恢复”摘要中的**查看配置**。

步骤 2 依次点击**预定备份 > 计划备份**。

如果您已经有计划备份，请点击**预定备份 > 编辑**。

步骤 3 输入备份名称和描述（后者为可选项）。

步骤 4 选择备份的日期和时间。

步骤 5（仅限于 ISA 3000）选择备份文件的位置。

您可以在**本地硬盘**或**SD 卡**上创建备份。使用 SD 卡的好处是，您可以使用卡将配置恢复到替换设备。

步骤 6 点击计划。

当选择的日期和时间到达时，系统将执行备份。完成后，备份将在备份表格中列出。

设置周期性备份计划

您可以设置周期性备份来定期备份系统。例如，您可以在每个周五的午夜执行备份。周期性备份计划有助于确保您始终拥有一组最近的备份。



注释 如果要删除周期性计划，请编辑该计划并点击删除。

过程

步骤 1 点击 **设备**，然后点击“备份和恢复”摘要中的**查看配置**。

步骤 2 依次点击**周期性备份 > 配置**。

如果您已配置周期性备份，请依次点击**周期性备份 > 编辑**。

步骤 3 输入备份名称和描述（后者为可选项）。

步骤 4 选择频率和相关计划：

- **每日** - 选择一天的时间。系统每天在预定时间执行备份。
- **每周** - 选择星期几和当日的的时间。系统将在您所选的每天的预定时间执行备份。例如，您可将备份安排在每个星期一、星期三和星期五的 23:00（晚上 11 点）进行。
- **每月** - 选择每月的日期和当日的的时间。系统将在您所选的每天的预定时间执行备份。例如，您可将备份安排在每月一 (1) 日、十五 (15) 日和二十八 (28) 日的 23:00（晚上 11 点）进行。

您指定的时间已根据夏令时调整，因此当您所在地区的时间被调整时，它会向前或向后移动一小时。如果您想要在全年确保此时间准确无误，您必须在时间被更改时编辑计划。

步骤 5（仅限于 ISA 3000）选择备份文件的位置。

您可以在**本地硬盘**或**SD 卡**上创建备份。使用 SD 卡的好处是，您可以使用卡将配置恢复到替换设备。

步骤 6 点击保存。

到所选日期及时间时，系统执行备份。完成后，备份将在备份表格中列出。
周期性计划将持续执行备份，直到您更改或删除该计划为止。

恢复备份

只要设备运行的软件版本（包括内部版本号）与备份时相同，即可根据需要还原备份。只有两台设备的型号相同且运行相同版本的软件（包括内部版本号），才能将备份恢复到替换设备上。

不过，当设备属于高可用性对的一部分时，您无法恢复备份。您必须首先从**设备 > 高可用性**页面中断高可用性，然后才能恢复备份。如果备份包括高可用性配置，设备将重新加入高可用性组。不要在两台设备上恢复相同备份，因为这两台设备都会变成活动状态。相反，您要在想要首先恢复活动状态的设备上恢复备份，然后在另一台设备上恢复等效备份。

如果设备中没有要恢复的备份副本，必须先上传该备份，才能进行恢复。
在恢复期间，系统完全不可用。



注释 备份不包括管理 IP 地址配置。因此，恢复备份文件时，不会从备份副本中替换管理地址。这可以确保保存对地址所做的任何更改，并且还可以在其他网段的其他设备上恢复配置。

过程

步骤 1 点击 **设备**，然后点击“备份和恢复”摘要中的**查看配置**。

点击后随即会打开“备份和恢复”页面。表格中将列出系统中可用的所有现有备份副本。

步骤 2 如果可用的备份列表中没有要恢复的备份副本，请依次点击**上传 > 浏览**，并上传该备份副本。

步骤 3 点击该文件的恢复图标 (🔄)。

您需要确认恢复。默认情况下，恢复后系统将删除备份副本，但您可以事先选择**恢复后不删除备份**以保留备份副本，然后再继续进行恢复。

恢复完成后，系统会重新启动。

注释 系统重新启动后，会自动检查漏洞数据库 (VDB)、地理位置和规则数据库更新，并根据需要进行下载。由于这些更新可能很大，因此初始尝试可能会失败。请检查任务列表，如果下载失败，请手动下载更新，如[更新系统数据库](#)，第 464 页中所述。系统还会重新部署策略。在更新成功之前，任何后续部署都将失败。

步骤 4 如有必要，请依次点击**设备 > 智能许可证 > 查看配置**，重新注册该设备，并重新启用所需的可选许可证。

如果您将备份恢复到生成备份的设备，则许可状态将返回到备份时的状态。如果您进行了后续更改，例如启用或禁用许可证，则必须重新执行这些更改。

如果在不同设备上恢复备份，例如您要替换设备，则新设备是未注册的。您必须重新注册设备，并启用所需的可选许可证。如果备份包括高可用性配置，设备将不会尝试加入高可用性组。您必须先注册设备，然后手动部署配置。

更换 ISA 3000 设备

您可以移除 ISA 3000 的 SD 卡，将其插入另一台 ISA 3000 设备。如果您在 SD 卡上创建系统备份，可以使用此功能轻松更换设备。只需取出故障设备的 SD 卡，并插入新的设备。然后即可通过备份进行恢复。

要确保您有必要的备份，请配置备份作业以在 SD 卡上创建备份。

管理备份文件

在创建新备份时，备份文件将列在“备份和恢复”(Backup and Restore) 页面。备份副本不会无限期保留：当设备上的磁盘空间使用率达到最大阈值时，系统将删除较早的备份副本以便为较新的备份腾出空间。因此，您应定期管理备份文件，确保保存最希望保留的特定备份。

您可以执行以下操作来管理备份副本：

- 将文件下载到安全存储 - 要将备份文件下载到您的工作站，请点击该文件的下载图标 (📄)。然后，您就可以将该文件移到安全文件存储了。
- 将备份文件上传到系统 - 如果要恢复设备中不再可用的备份副本，请依次点击上传 > 浏览文件，并从工作站上传文件。然后即可执行恢复。



注释 可以重命名上传的文件，以便与原始文件名匹配。此外，如果系统中的备份副本已超过 10 个，系统将删除最早的备份副本，以便为上传的文件腾出空间。无法上传使用较早的软件版本创建的文件。

- 恢复备份 - 要恢复备份，请点击该文件的恢复图标 (🔄)。系统在恢复期间不可用，恢复完成后将重新启动。在系统正常运行后，您需要部署配置。
- 删除备份文件 - 如果不再需要某个特定备份，请点击该文件的删除图标 (🗑️)。您需要确认删除。删除后，则无法恢复备份文件。

审核与变更管理

您可以查看有关系统事件以及用户已执行操作的状态信息。此信息可以帮助您审核系统，并确保正确地管理系统。

依次点击**设备 > 设备管理 > 审核日志**可以查看审核日志。此外，您可以通过点击右上角的**任务列表**或**部署**图标按钮查找系统管理信息。

以下主题介绍系统审核和 变更管理的一些主要概念和任务。

审核事件

审核日志可包括以下类型的事件：

部署已完成，部署失败：作业名称或实体名称

这些事件表示部署作业已成功完成或失败。详细信息包括作业发起人以及与作业实体相关的信息。失败的作业包括与失败相关的错误消息。

详细信息还包括一个**差异视图**选项卡，其中显示了作业执行过程中部署到设备的更改。这里汇总了已部署实体的所有实体更改事件。

要过滤这些事件，只需点击**部署历史记录**预定义过滤器。请注意，这些事件的事件类型是部署事件，您无法仅过滤已完成或失败的事件。

事件名称包括用户定义的作业名称（如果进行了配置）或“用户（用户名）触发的部署”。其中还包括，在运行设备设置向导期间发生的“设备设置自动部署”和“设备设置自动部署（最后一步）”作业。

实体已创建、实体已更新、实体已删除：实体名称（实体类型）

这些事件表示对识别的实体或对象进行了更改。实体详细信息包括实施更改的人员以及实体名称、类型和ID。您可以过滤这些项目。详细信息还包括一个**差异视图**选项卡，其中显示了应用于对象的更改。

HA 操作事件

这些事件与有关高可用性配置的操作有关，它们可以是您发起的操作，也可以是系统发起的操作。HA 操作事件的类型为事件，但事件名称是以下项之一：

- **HA 已暂停** - 有意暂停系统上的 HA。
- **HA 已恢复** - 有意恢复系统上的 HA。
- **HA 已重置** - 有意重置系统上的 HA。
- **HA 故障切换：设备切换模式** - 有意切换模式，或系统由于运行状况指标违规而进行了故障切换。此消息表明，主用对等设备变为了备用设备，或备用对等设备变为了主用设备。

已放弃等待完成的更改

此事件表示已删除所有待完成的更改。此事件与先前的“部署已完成”事件之间由“实体已创建”、“实体已更新”以及“实体已删除”事件指明的所有更改均已删除，并且受影响对象的状态恢复到上一次部署的版本。

任务已开始，任务已完成，任务失败

任务事件表示系统或用户发起的的作业的开始和结束。这两个事件将会整合到任务列表中的一个任务中，您可以通过点击右上角的**任务列表**按钮进行查看。



任务包括部署作业以及手动或计划的数据库更新等操作。任务列表中的任何项目都将与审核日志中的两个任务事件对应，指示任务开始、成功完成或失败。

用户已登录、用户已注销：用户名

这些事件显示用户登录和注销 Firepower 设备管理器的时间和源 IP 地址。主动注销和因空闲时间超时而自动注销都会引发“用户已注销”事件。

这些事件无关于与设备建立连接的 RA VPN 用户。它们也不包含登录/注销设备 CLI。

查看和分析审核日志

审核日志包括有关系统发起和用户发起事件的相关信息，例如，部署作业、数据库更新和登录/注销 Firepower 设备管理器。

有关日志中可以显示的事件类型的说明，请参阅[审核事件](#)，第 473 页。

过程

步骤 1 点击设备，然后点击设备管理 > 查看配置链接。

步骤 2 点击目录中的审核日志（如果未将其选定）。

事件将按照日期分组，一天内的事件按时间分组，日期/时间最新的事件排在列表顶部。最初，所有事件都处于折叠状态，只能看到时间、事件名称、发起事件的用户以及该用户的源 IP 地址。如果用户和 IP 地址为“系统”，这意味着事件是由设备自身发起的。

可以执行以下操作：

- 点击事件名称旁边的 >，可事件打开并查看详细信息。再次点击该图标可关闭事件。很多事件具有一系列简单的事件属性，例如，事件类型、用户名、源 IP 地址等。但实体和部署事件包含两个选项卡：
 - **摘要**显示基本事件属性。
 - **差异视图**显示现有的“已部署”配置与事件过程中所发生变更的对比信息。如果是部署作业，此视图可能会很长，需要滚动鼠标才能完整查看。它将汇总部署作业过程中实体事件变更的所有差异。
- 从过滤器字段右侧的下拉列表中选择不同的时间范围。默认是查看过去 2 周的事件，但您可以更改范围，查看过去 24 小时、7 天、1 个月或 6 个月的事件。点击**自定义**可通过输入开始和结束日期与时间指定具体范围。
- 点击日志中的任意链接，为该条目添加搜索过滤器。列表会更新，仅显示包含该条目的事件。您也可以点击**过滤器框**，直接构建过滤器。此外，还可以点击过滤器框下方的预定义过滤器，加载相关的过滤条件。有关过滤事件的详细信息，请参阅[过滤审核日志](#)，第 475 页。

- 重新加载浏览器页面将会刷新日志，以显示最新事件。

过滤审核日志

您可以对审核日志应用过滤器，将视图显示范围缩小到仅显示特定类型的消息。过滤器中的每个元素都是一个准确、完全的匹配。例如，“User = admin”仅显示名为 **admin** 的用户发起的事件。

您可以单独或组合使用以下方法来构建过滤器：每次添加过滤器元素时，列表都会自动更新。

点击预定义过滤器

过滤器 字段下方是预定义的过滤器。点击链接即可加载过滤器。系统将要求您进行确认。如果您已应用过滤器，该过滤器会被替换，也不会添加该过滤器。

点击高亮显示的条目

要构建过滤器，最简单的方法是点击日志表或事件详细信息中包含作为过滤标准的值的条目。点击条目后，**过滤器** 字段将替换为该值和元素组合的格式设置正确的元素。但是，使用此方法要求现有的事件列表中包含所需的值。

如果可以为条目添加过滤器元素，当您将鼠标指针悬停在该条目上时，该条目会标有下划线，并显示命令 **点击添加到过滤器**。

选择原子元素

此外，您还可以通过以下方法创建过滤器：点击 **过滤器** 字段，从下拉列表中选择所需的原子元素，在等号后面键入匹配值，然后按 **Enter** 键。您可以过滤以下元素。请注意，对于每种类型的事件而言，并非所有元素都是相关的。

- **事件类型** - 事件类型通常与事件名称（不含实体名称或用户等变量限定符）相同，但并非总是这样。部署事件的事件类型是“部署事件”。有关事件类型的说明，请参阅 [审核事件](#)，第 473 页。
- **用户** - 发起事件的用户名称。系统用户采用字母全部大写的形式：SYSTEM。
- **源 IP** - 用户发起事件的源 IP 地址。系统发起事件的源 IP 地址是 SYSTEM。
- **实体 ID** - 实体或对象的 UUID，这是一种比较长且不可读的字符串，例如 8e7021b4-2e1e-11e8-9e5d-0fc002c5f931。通常，要使用此过滤器，您需要点击事件详细信息中的实体 ID，或使用 REST API 通过相关 GET 调用检索所需的 ID。
- **实体名称** - 实体或对象的名称。对于用户创建的实体，实体名称通常是您为对象指定的名称，例如，将网络对象命名为 InsideNetwork。对于系统生成的实体或（在某些情况下）用户定义的实体，实体名称是预定义但可识别的名称，例如，将没有明确命名的部署作业命名为 “User (admin) Triggered Deployment”。
- **实体类型** - 实体或对象的类型。这些是预定义但可识别的名称，例如 Network Object。您可以通过查看相关对象模型的 “type” 值，在 API Explorer 中查找实体类型。API 类型通常采用字母全部小写形式，且不含空格。如果您完全按照模型中所示输入类型，则按 **Enter** 键

时，字符串会变成可读性更强的格式。这两种输入方式都可以接受。要打开 API Explorer，请将浏览器中 URL 的最后部分改成 `/#/api-explorer`。

复杂审核日志过滤器的规则

在构建包含多个原子元素的复杂过滤器时，请记住以下规则：

- 相同类型的元素在该类型的所有值之间具有 OR 关系。例如，包括“User = admin”和“User = SYSTEM”将会匹配由任一用户发起的事件。
- 不同类型的元素之间为 AND 关系。例如，包括“Event Type = Entity Updated”和“User = SYSTEM”仅会显示由系统而非活动用户更新实体的事件。
- 您不能使用通配符、正则表达式、部分匹配或简单的文本字符串匹配。

检查部署和实体更改历史记录

部署和实体事件在事件详细信息中包括**差异视图**选项卡。此选项卡以彩色显示旧配置与更改之间的对比情况。

- 对于部署作业，此对比为部署之前设备上运行的配置与实际所部署更改之间的对比。
- 对于实体事件，这些是对之前版本的对象所做的配置更改。之前的版本可能是实际设备使用的版本，也可能是对象尚未部署的变化。

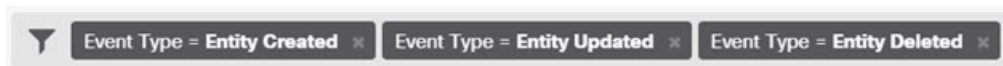
过程

步骤 1 点击**设备**，然后点击**设备管理 > 查看配置**链接。

步骤 2 点击目录中的**审核日志**（如果未将其选定）。

步骤 3（可选。）过滤消息：

- 部署事件 - 点击过滤器框下的**部署历史记录**预定义过滤器。
- 实体更改事件 - 使用事件类型元素为您感兴趣的更改类型手动创建过滤器。要查看所有实体更改，请选择**实体已创建**、**实体已更新**和**实体已删除**这三种规格。过滤器应如下所示：



步骤 4 打开事件，然后点击**差异视图**选项卡。

Deployment Completed: User (admin) Triggered Deployment

Summary Differences View

DEPLOYED VERSION	PENDING VERSION	Legend: Removed Added Edited
− Syslog Server Removed		
Entity ID: 4a1605df-311d-11e8-893d-c15d8f450fd9		
syslogServerIpAddress: 192.168.1.25	−	
portNumber: 514	−	
deviceInterface:		
inside	−	
+ Network Object Added		
Entity ID: b64f4101-311d-11e8-893d-a302db0bc31e		
−	subType: Network	
−	value: 10.1.10.0/24	
−	isSystemDefined: false	
−	name: RemoteNetwork	
⌚ Network Object Edited		
Entity ID: ddb608e9-311c-11e8-893d-5588b92854ca		
value: 192.168.2.0/24	192.168.1.0/24	

所做的更改会使用颜色编码，标题指示对象的类型以及对象是被添加（创建）、移除（删除）还是编辑（更新）。编辑的对象仅显示已更改或从该对象删除的属性。在部署作业中，每个更改的实体都有单独的标题。标题表明对象的实体类型。

放弃所有待处理更改

如果您对一套尚未部署的配置更改不满意，您可以放弃所有待处理的更改。此操作使所有功能均恢复到设备上存在的状态。之后，您可以再重新开始部署配置更改。

过程

步骤 1 点击网页右上角的部署更改图标。

如存在待处理的更改，系统会用圆点高亮显示。



步骤 2 依次点击更多选项 > 全部放弃。

步骤 3 点击确认对话框中的确定。

系统将放弃更改，操作完成后您会看到一条表示没有待处理更改的消息。系统会在审核日志中添加“已放弃待处理的更改”事件。

导出设备配置

可以 JSON 格式导出一份当前部署的配置。可以使用该文件进行归档或备案。密码和密钥等所有敏感数据均被屏蔽。

无法将文件导入此设备或其他设备。此功能不会取代系统备份。

必须至少完成一个成功的部署作业，才能下载配置。

过程

步骤 1 选择设备，然后点击设备管理组中的**查看配置**。

步骤 2 点击目录中的**下载配置**。

步骤 3 点击**获取设备配置**启动创建文件的作业。

如果您之前创建了一个文件，您将看到一个下载按钮和一条含文件创建日期的**文件可供下载**消息。

生成文件可能需要几分钟的时间，具体取决于配置的大小。检查任务列表或审核日志，或者定期返回到此页面，直到导出配置作业完成并生成文件。

步骤 4 生成文件后，返回到此页面并点击**下载配置文件按钮** (📄) 将文件保存到工作站。

管理 FDM 和 FTD 用户访问权限

您可以为登录到 Firepower 设备管理器的用户配置外部身份验证和授权源（HTTPS 访问）。您可以将外部服务器与本地用户数据库和系统定义的 **admin** 用户结合使用，或不使用后两者。请注意，您无法创建用于 FDM 访问的额外本地用户账户。

虽然您可以有多个可以更改配置的外部 FDM 用户账户，但用户不跟踪这些更改。当一个用户部署更改时，所有用户做出的更改均被部署。没有任何锁定：即，多个用户可能会尝试在同一时间更新同一对象，这将导致只有一个用户能够成功保存更改。您也无法基于用户丢弃更改。

Firepower 设备管理器允许 5 个并发用户会话。如果第六个用户登录，开始时间最早的用户会话会自动注销。还有空闲超时，非活动用户空闲 20 分钟后注销。

除 Firepower 设备管理器用户之外，您可以创建本地只使用 CLI 的用户。除 **admin** 用户之外，CLI 和 Firepower 设备管理器用户之间没有任何交叉：用户账户是完全独立的。



注释 使用外部服务器时，您可以通过设置单独的 RADIUS 服务器组，或在仅允许用户访问特定 FTD 设备 IP 地址的 RADIUS 服务器中创建身份验证/授权策略，来控制用户对您部分设备的访问。

以下主题介绍如何配置和管理 Firepower 设备管理器用户访问和 CLI 用户访问。

为 FDM (HTTPS) 用户配置外部授权 (AAA)

您可以从外部 RADIUS 服务器提供到 Firepower 设备管理器的 HTTPS 访问权限。通过启用 RADIUS 身份验证和授权，您可以提供不同级别的访问权限，使并非每个用户都通过本地 **admin** 账户登录。

这些外部用户还有权访问 Firepower 威胁防御 API 和 API Explorer。

要提供基于角色的访问控制 (RBAC)，请更新 RADIUS 服务器上的用户账户以定义 **cisco-av-pair** 属性（注意这是在 ISE 中，而在 Free RADIUS 中该属性拼写为 Cisco-AVPair；请检查系统的拼写是否正确）。必须在用户账户上正确定义此属性，否则系统会拒绝用户访问 Firepower 设备管理器。以下是受支持的 **cisco-av-pair** 属性值：

- **fdm.userrole.authority.admin** 提供完全管理员访问权限。这些用户可以执行本地 **admin** 用户可以执行的所有操作。
- **fdm.userrole.authority.rw** 提供读写访问权限。这些用户可以执行只读用户可以执行的任何操作，还可以编辑和部署配置。唯一的限制是无法执行关键系统操作，包括安装升级、创建和恢复备份、查看审核日志以及中止 Firepower 设备管理器用户的会话。
- **fdm.userrole.authority.ro** 提供只读访问权限。这些用户可以查看控制面板和配置，但无法进行任何更改。如果用户尝试进行更改，会显示错误消息，指明权限不足。

用户登录 Firepower 设备管理器后，页面右上角将显示用户名和角色：管理员、读写用户或只读用户。

在 RADIUS 服务器上正确设置账户后，您可以使用此程序启用账户，以进行管理访问。

过程

步骤 1 点击**设备**，然后依次点击**系统设置 > 管理访问**链接。

如果您已位于“系统设置”页面，只需点击目录中的**管理访问**。

步骤 2 点击**AAA 配置**选项卡，如果尚未选择此选项卡。

步骤 3 配置 **HTTPS 连接**选项：

- **管理/REST API 的服务器组** - 选择您想要用作主要身份验证源的 RADIUS 服务器组或本地用户数据库 (LocalIdentitySource)。必须选择要使用外部授权的 RADIUS 服务器组。

如果尚不存在服务器组，点击**创建新 RADIUS 服务器组**链接立即创建服务器组。您还需要为每个服务器创建 RADIUS 服务器对象，将这些对象添加到组（定义服务器组时可以执行此操作）。有关 RADIUS 的详细信息，请参阅 [RADIUS 服务器和组](#)，第 135 页。

- 使用本地身份源进行身份验证 - 如果您选择外部服务器组，可以指定如何使用包含本地 **admin** 用户账户的本地身份源。选择以下一个选项：
 - 在外部服务器之前 - 系统首先对照本地源检查用户名和密码。
 - 在外部服务器之后 - 仅当外部源不可用或在外部来源中找不到用户账户时，才检查本地源。
 - 从不 - (不推荐。) 从不使用本地源，因此不能以 **admin** 用户身份登录。

注意 如果您选择从不，将无法使用 **admin** 账户登录 Firepower 设备管理器。如果 RADIUS 服务器不可用，或者未在 RADIUS 服务器中配置账户，您将被锁定在系统外面。

步骤 4 点击保存。

管理 Firepower 设备管理器用户会话

依次选择**监控 > 会话**，查看当前登录到 Firepower 设备管理器的用户的列表。列表会显示当前会话每个用户登录的持续时间。

如果相同的用户名出现多次，则表示用户从不同的源地址打开会话。系统根据用户名和源地址单独跟踪会话，而且每个会话具有唯一时间戳。

系统允许 5 个并发用户会话。如果第六个用户登录，开始时间最早的当前会话会自动注销。此外，非活动状态长达 20 分钟的空闲用户会被自动注销。

如果 FDM 用户输入错误的密码且连续 3 次尝试登录失败，则该用户的账户将锁定 5 分钟。用户必须等待锁定时间结束后方可尝试重新登录。无法解锁 FDM 用户账户，也无法调整重试计数或锁定超时。（请注意，对于 SSH 用户，可以调整这些设置并解锁账户。）

如果有必要，您可以通过点击会话的删除图标 (🗑️) 终止用户会话。如果您删除您自己的会话，您也会被注销。结束会话没有锁定时段：用户可以立即重新登录。

启用备用 HA 设备上的外部用户 FDM 访问权限

如果为 FDM 用户配置了外部授权，则这些用户可以登录到高可用性对的主用和备用设备。但是，与登录主用设备相比，首次成功登录备用设备还需要执行一些额外操作。

外部用户首次登录到主用设备后，系统会创建一个对象，定义用户和用户的访问权限。随后，管理员或读写用户必须在主用设备上，为要在备用设备上显示的用户对象部署配置。

只有在部署和后续配置同步成功完成之后，外部用户才可登录到备用设备。

管理员和读写用户在登录到主用设备后可以部署更改。但是，只读用户无法部署配置，且必须请求拥有适当权限的用户部署配置。

为 FTD CLI 创建本地用户账户

您可以在 FTD 设备上为 CLI 访问创建用户。这些账户不允许访问管理应用，仅允许访问 CLI。CLI 对于故障排除和监控非常有用。

您不能一次性在多个设备上创建本地用户账户。每个设备都有自己的一组唯一本地用户 CLI 账户。

过程

步骤 1 使用具有配置权限的账户登录设备 CLI。

管理员用户账户具有所需的权限，但具有配置权限的任何账户都可以执行操作。您可以使用 SSH 会话或控制台端口。

对于某些设备型号，控制台端口会带您进入 FXOS CLI。使用 **connect ftd** 命令进入 FTD CLI。

步骤 2 创建用户账户。

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

您可以使用以下权限级别定义用户：

- **config**- 提供用户配置访问权限。此级别将赋予用户完整管理员权限，让其可以输入所有配置命令。
- **basic**- 提供用户基本访问权限。此级别不允许用户输入配置命令。

示例：

以下示例将添加一个名为 **joecool** 且具有配置访问权限的用户账户。在您键入密码时，密码不会显示。

```
> configure user add joecool config
Enter new password for user joecool: newpassword
Confirm new password for user joecool: newpassword
> show user
Login                UID   Auth Access  Enabled Reset   Exp Warn  Str Lock Max
admin                1000 Local Config Enabled  No   Never  N/A  Dis  No  N/A
joecool              1001 Local Config Enabled  No   Never  N/A  Dis  No   5
```

注释 告知用户他们可以使用 **configure password** 命令更改密码。

步骤 3 （可选。）根据安全要求调整该账户的特性。

您可以使用以下命令更改默认账户行为。

- **configure user aging** *username max_days warn_days*

设置用户密码的到期日。指定密码最大有效天数，以及密码到期前向用户发出密码即将到期警告的天数。两个值均介于 1 到 9999 之间，但是警告天数必须小于最大天数。当您创建账户时，密码没有到期日。

- **configure user forcereset** *username*

强制用户下次登录时更改密码。

- **configure user maxfailedlogins** *username number*

设置在锁定账户之前您允许的最大连续失败登录次数，该值介于 1 至 9999 之间。使用 **configure user unlock** 命令解锁账户。新账户的默认值为 5 次连续失败登录。

- **configure user minpasswdlen** *username number*

设置最小密码长度，此值介于 1 至 127 之间。

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

启用或禁用密码强度检查，此检查要求用户在更改密码时要满足特定的密码条件。如果用户密码到期或使用了 **configure user forcereset** 命令，则此要求会在用户下次登录时自动启用。

步骤 4 根据需要管理用户账户。

用户可能被锁定在账户之外了，也可能您需要删除账户或解决其他问题。使用以下命令管理系统中的用户账户。

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

更改用户账户的权限。

- **configure user delete** *username*

删除指定的账户。

- **configure user disable** *username*

禁用指定的账户，而不将其删除。用户无法登录，直到您启用该账户为止。

- **configure user enable** *username*

启用指定的账户。

- **configure user password** *username*

更改指定用户的密码。通常情况下，用户应使用 **configure password** 命令更改自己的密码。

- **configure user unlock** *username*

解锁因超出最大连续失败登录尝试次数而被锁定的用户账户。

重新启动系统

如果您认为系统运行不正确，而解决问题的其他操作均失败，您可以重新启动设备。您必须通过 CLI 重新启动设备；不能通过 Firepower 设备管理器重新启动设备。

过程

步骤 1 使用 SSH 客户端打开指向管理 IP 地址的连接，使用具有配置 CLI 访问权限的用户名登录设备 CLI。
例如 **admin** 用户名。

步骤 2 输入 **reboot** 命令。

示例：

```
> reboot
```

系统故障排除

以下主题介绍一些系统级故障排除任务和功能。有关对特定功能（如访问控制）进行故障排除的信息，请参阅相应功能的章节。

用于测试连接的 Ping 命令

ping 是一种简单命令，可用于确定特定地址是否处于活动状态以及是否会做出响应。这意味着基本连接正常工作。然而，在设备上运行的其他策略可能会阻止特定类型的流量成功通过设备。您可以通过 **ping** 打开 CLI 控制台或登录设备 CLI 使用。



注释

由于系统有多个接口，您可以控制用于 **ping** 地址的接口。必须确保使用正确的命令，以便测试重要的连接。例如，系统必须能够通过虚拟管理接口到达思科许可证服务器，因此您必须使用 **ping system** 命令测试连接。如果使用 **ping**，则测试的是能否通过数据接口访问地址，这可能不会得到相同的结果。

正常 **ping** 使用 ICMP 数据包测试连接。如果您的网络禁止 ICMP，可以换用 TCP **ping**（仅用于数据接口 **ping**）。

以下是 **ping** 网络地址的主要选项。

通过虚拟管理接口 ping 地址

使用 **ping system** 命令。

ping system host

主机可以是 IP 地址或完全限定域名 (FQDN)，例如 **www.example.com**。不同于通过数据接口进行 **ping** 操作，系统 **ping** 没有默认计数。**ping** 操作会持续执行，直到您使用 **Ctrl+c** 将其停止。例如：

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
```

```

64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>

```

使用路由表，通过数据接口 ping 地址

使用 **ping** 命令。测试的是系统一般能否找出通往主机的路由。因为这是系统正常路由流量的方式，所以您通常需要对此进行测试。

ping host

指定主机的 IP 地址。如果您仅知道 FQDN，可使用 **nslookup fqdn-name** 命令来确定 IP 地址。例如：

```

> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

```



注释 您可以指定超时、重复计数、数据包大小甚至发送时所用的数据模式。在 CLI 中使用帮助指示符？查看可用的选项。

通过特定数据接口 ping 地址

如果要通过特定数据接口测试连接性，可使用 **ping interface if_name** 命令。您还可以使用此命令指定诊断接口，但不能指定虚拟管理接口。

ping interface if_name host

指定主机的 IP 地址。如果您仅知道 FQDN，可使用 **nslookup fqdn-name** 命令来确定 IP 地址。例如：

```

> ping interface inside 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms

```

使用 TCP ping，通过数据接口 ping 地址

使用 **ping tcp** 命令。TCP ping 发送 SYN 数据包，如果目标发送了 SYN-ACK 数据包，则认为 ping 取得了成功。

ping tcp [interface if_name] host port

您必须指定主机和 TCP 端口。如果您仅知道 FQDN，可使用 **nslookup fqdn-name** 命令来确定 IP 地址。

您可以选择指定接口，即 ping 的源接口，而不是用于发送 ping 的接口。此类 ping 通常使用路由表。

TCP ping 发送 SYN 数据包，如果目标发送了 SYN-ACK 数据包，则认为 ping 取得了成功。例如：

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```



注释 您还可以指定 TCP ping 的超时、重复计数和源地址。在 CLI 中使用帮助指示符 ? 查看可用的选项。

跟踪主机路由

如果您向某个 IP 地址发送流量时遇到问题，可以跟踪主机路由以确定网络路径是否有问题。tracert 的工作方式是从无效端口向目的地发送 UDP 数据包或者向目的地发送 ICMPv6 回应。通往目的地沿途的路由器以 ICMP Time Exceeded 消息响应，并向 tracert 报告该错误。每个节点会收到三个数据包，因此对于每个节点，您有三次机会获得信息性结果。您可通过 tracert 打开 CLI 控制台或登录设备 CLI 使用。



注释 通过数据接口 (**tracert**) 或通过虚拟管理接口 (**tracert system**) 跟踪路由有单独的命令。请务必使用正确的命令。

下表说明了输出中显示的每个数据包的可能结果。

输出符号	说明
*	在超时期限内未收到对探测的响应。
nn msec	各节点指定探测数的往返时间（以毫秒为单位）。
!N.	无法访问 ICMP 网络。
!H	无法访问 ICMP 主机。
!P	ICMP 协议不可达。
!A	管理性禁止 ICMP。
?	未知 ICMP 错误。

通过虚拟管理接口跟踪路由

使用 **traceroute system** 命令。

traceroute system destination

主机可以是 IPv4/IPv6 地址或完全限定域名 (FQDN)，例如 `www.example.com`。例如：

```
> traceroute system www.example.com
traceroute to www.example.com (172.163.4.161), 30 hops max, 60 byte packets
 1 192.168.0.254 (192.168.0.254) 0.213 ms 0.310 ms 0.328 ms
 2 10.88.127.1 (10.88.127.1) 0.677 ms 0.739 ms 0.899 ms
 3 lab-gw1.example.com (10.89.128.25) 0.638 ms 0.856 ms 0.864 ms
 4 04-bb-gw1.example.com (10.152.240.65) 1.169 ms 1.355 ms 1.409 ms
 5 wan-gw1.example.com (10.152.240.33) 0.712 ms 0.722 ms 0.790 ms
 6 wag-gw1.example.com (10.152.240.73) 13.868 ms 10.760 ms 11.187 ms
 7 rbb-gw2.example.com (172.30.4.85) 7.202 ms 7.301 ms 7.101 ms
 8 rbb-gw1.example.com (172.30.4.77) 8.162 ms 8.225 ms 8.373 ms
 9 sbb-gw1.example.com (172.16.16.210) 7.396 ms 7.548 ms 7.653 ms
10 corp-gw2.example.com (172.16.16.58) 7.413 ms 7.310 ms 7.431 ms
11 dmzbb-gw2.example.com (172.16.0.78) 7.835 ms 7.705 ms 7.702 ms
12 dmzdcc-gw2.example.com (172.16.0.190) 8.126 ms 8.193 ms 11.559 ms
13 dcz05n-gw1.example.com (172.16.2.106) 11.729 ms 11.728 ms 11.939 ms
14 www1.example.com (172.16.4.161) 11.645 ms 7.958 ms 7.936 ms
```

通过数据接口跟踪路由

使用 **traceroute** 命令。

traceroute destination

指定主机的 IP 地址。如果您仅知道 FQDN，可使用 **nslookup fqdn-name** 命令来确定 IP 地址。例如：

```
> traceroute 209.165.200.225
Tracing the route to 209.165.200.225
 1 10.83.194.1 0 msec 10 msec 0 msec
 2 10.83.193.65 0 msec 0 msec 0 msec
 3 10.88.193.101 0 msec 10 msec 0 msec
 4 10.88.193.97 0 msec 0 msec 10 msec
 5 10.88.239.9 0 msec 10 msec 0 msec
 6 10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```



注释 您可以指定超时、生存时间、每个节点的数据包数量，乃至要用作 **traceroute** 源的 IP 地址或接口。在 CLI 中使用帮助指示符 `?` 查看可用的选项。

设置 Firepower 威胁防御设备显示在跟踪路由上

默认情况下，Firepower 威胁防御不会在跟踪路由上显示为跃点。要使其显示，您需要递减通过设备的数据包上的生存时间，并增加对 ICMP 不可达消息的速率限制。要实现此目的，您必须创建配置所需的服务策略规则和其他选项的 FlexConfig 对象。

有关服务策略和流量类别的详细讨论，请参阅《思科 ASA 系列防火墙配置指南》，网址为 <https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html>。



注释 如果减少生存时间，系统会丢弃 TTL 为 1 的数据包，但会为会话打开一个连接，前提是假设该连接可能包含具有更大 TTL 的数据包。请注意，某些数据包（例如 OSPF hello 数据包）发送时 TTL = 1，因此减去生存时间可能会导致意外后果。定义流量类时，请注意这些事项。

过程

步骤 1 在设备 > 高级配置中点击查看配置。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig** 对象。

步骤 3 创建减小 TTL 的对象。

- a) 点击 + 按钮以创建新的对象。
- b) 为对象输入名称。例如，**Decrement_TTL**。
- c) 在模板编辑器中，输入以下命令，包括缩进。

```
icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
  class class-default
    set connection decrement-ttl
```

- d) 在取消模板编辑器中，输入撤消此配置所需的命令。

正如要让命令启用模板需要添加父命令以进入正确的子模式那样，您也需要在取消模板中添加这些命令。

取消模板将在您从 FlexConfig 策略删除此对象（部署成功后删除）时，以及不成功的部署期间应用（将配置重置为之前的状态）。

因此，在本示例中，取消模板为：

```
no icmp unreachable rate-limit 50 burst-size 1
policy-map global_policy
  class class-default
    no set connection decrement-ttl
```

- e) 点击**确定**保存对象。

步骤 4 将对象添加到 FlexConfig 策略中。

仅部署在 FlexConfig 策略中选择的对象。

- a) 点击目录中的 **FlexConfig** 策略。
- b) 在组列表中点击 +。
- c) 选择 Decrement_TTL 对象，然后点击**确定**。

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

d) 点击保存。

您现在可以部署策略。

排除 NTP 故障

系统靠时间准确一致来正常运行，并确保事件和其他数据点得到准确处理。您必须配置至少一个（最好是三个）网络时间协议 (NTP) 服务器来确保系统始终能获得可靠的时间信息。

设备摘要连接图（在主菜单中点击设备）显示至 NTP 服务器的连接状态。如果状态为黄色或橙色，说明与配置的服务器存在连接问题。如果连接问题仍然存在（不仅仅是一个临时问题），请尝试以下操作。

- 首先，确保在设备 > 系统设置 > NTP 上配置至少三个 NTP 服务器。尽管不要求配置至少三个 NTP 服务器，但这样做可以大大提高可靠性。
- 确保管理接口 IP 地址（在设备 > 系统设置 > 管理接口中定义）与 NTP 服务器之间存在网络路径。
 - 当管理接口网关是数据接口时，如果默认路由不充足，则可以在设备 > 路由上配置到 NTP 服务器的静态路由。
 - 如果设置了显式管理接口网关，请登录设备 CLI，并使用 **ping system** 命令测试与每个 NTP 服务器之间是否存在网络路径。
- 登录设备 CLI，并使用以下命令检查 NTP 服务器的状态。
 - **show ntp**- 此命令显示 NTP 服务器的基本信息及其可用性。但是，Firepower 设备管理器中的连接状态使用其他信息指示其状态，所以此命令的显示以及连接状态图的显示可能存在不一致的地方。还可从 CLI 控制台发出此命令。
 - **system support ntp** - 此命令包括 **show ntp** 的输出以及标准 NTP 命令 **ntpq**（该命令记录在 NTP 协议中）的输出。如果需要确认 NTP 同步，请使用此命令。

查找“‘ntpq -pn’的结果”部分。例如，您可能会看到类似如下的内容：

```
Results of 'ntpq -pn'  
remote           : +216.229.0.50  
refid            : 129.7.1.66  
st               : 2  
t                : u  
when            : 704  
poll            : 1024  
reach           : 377  
delay           : 90.455  
offset          : 2.954  
jitter          : 2.473
```


在本例中，NTP 服务器地址前的 + 表示作为潜在候选者。此处的星号 * 表示当前的时间源对等体。

NTP 守护程序 (NTPD) 使用每个对等体中的八个示例的滑动窗口，并选出一个示例，然后根据时钟选择确定正确的报时器和错误的断续器。然后，NTPD 会确定往返距离（候补者的偏移不得超过往返延迟的一半）。如果连接延迟、丢包或服务器问题导致一个或全部候补者被拒绝，则同步中会出现较长的延迟。而且，该调整很长一段时间后会完成：时钟偏移和振荡器错误必须通过时钟训练算法解决，这可能会需要数小时的时间。



注释 如果 refid 是 .LOCL.，则表明对等体是一个未经训练的本地时钟，也即它只使用其本地时钟来设置时间。如果所选的对等体是 .LOCL.，则 Firepower 设备管理器始终将 NTP 连接标为黄色（未同步）。如果还有更好的证书，NTP 通常不会选择 .LOCL. 证书，这就是应配置至少三个服务器的原因所在。

为管理接口排除 DNS 故障

必须配置至少一个 DNS 服务器供管理接口使用。需要使用该服务器来云连接到智能许可、数据库更新（如 GeoDB、规则和 VDB）等服务，和处理其他需要域名解析的任何活动。

配置 DNS 服务器非常简单。只需在初始配置设备时输入所用 DNS 服务器的 IP 地址。随后可在 **设备 > 系统设置 > DNS 服务器** 页面进行更改。

但是，由于网络连接问题或 DNS 服务器本身的问题，系统可能会无法解析完全限定域名 (FQDN)。如果您发现系统无法使用您的 DNS 服务器，请考虑以下操作来识别和解决问题。另请参阅 [常规 DNS 问题故障排除](#)，第 454 页。

过程

步骤 1 确定是否存在问题。

- a) 使用 SSH 登录设备 CLI。
- b) 输入 **ping system www.cisco.com**。如果您获得类似于下文的“未知主机”消息，系统将无法解析域名。如果 ping 操作成功，问题得到解决：DNS 正常工作。（按 Ctrl+C 可停止 ping 命令。）

```
> ping system www.cisco.com
ping: unknown host www.cisco.com
```

注释 务必在 ping 命令中添加 **system** 关键字。**system** 关键字通过管理 IP 地址执行 ping 操作，该接口也是使用管理 DNS 服务器的唯一接口。访问 [www.cisco.com](#) 也是一个不错的选择，因为您需要到该服务器的路由以获得智能许可和更新。

步骤 2 验证管理接口的配置。

- a) 依次点击**设备 > 系统设置 > 管理接口**，并验证以下内容。如果您进行更改，点击**保存**后会立即应用所做的更改。如果您更改管理地址，需要重新连接并重新登录。
 - 管理网络的网关 IP 地址是正确的。如果您使用数据接口作为网关，后续步骤将验证该配置。
 - 如果您不使用数据接口作为网关，请验证管理 IP 地址/子网掩码和网关 IP 地址位于同一子网。
- b) 依次点击**设备 > 系统设置 > DNS 服务器**，并验证是否正确配置 DNS 服务器。
如果您在网络边缘部署设备，运营商可能会对您可以使用的 DNS 服务器提出特定要求。
- c) 如果您使用数据接口作为网关，确认您具有所需的路由。
您需要为 0.0.0.0 提供默认路由。如果 DNS 服务器不能使用默认路由的网关，您可能需要额外的路由。这种情况基本分为两类：
 - 如果您使用 DHCP 获取外部接口的地址且选择使用 **DHCP 获取默认路由** 选项，默认路由在 Firepower 设备管理器中不可见。从 SSH 输入 **show route** 验证是否存在适用于 0.0.0.0 的路由。由于这是外部接口的默认配置，您可能会遇到这样的情况。（请转至**设备 > 接口**查看外部接口的配置。）
 - 如果您在外部接口上使用静态 IP 地址或不从 DHCP 获取默认路由，则打开**设备 > 路由**。验证已为默认路由使用正确的网关。

如果无法通过默认路由访问 DNS 服务器，则必须在**路由**页面为其定义静态路由。请注意，不应为直连网络（即直接连接到系统任何数据接口的网络）添加路由，因为系统可以自动路由到这些网络。

此外，验证没有静态路由将发往服务器的流量错误引导至不正确的接口。

- d) 如果部署按钮指示存在未部署的更改，请现在部署这些更改并等待部署完成。



- e) 重新测试 **ping system www.cisco.com**。如果问题仍然存在，继续执行下一步。

步骤 3 在 SSH 会话中，输入 **nslookup www.cisco.com**。

- 如果 **nslookup** 指示可获取 DNS 服务器的响应，但服务器找不到名称，这意味着，DNS 已正确配置，但所用的 DNS 服务器没有适用于 FQDN 的地址。响应应类似于以下内容：

```
> nslookup www.cisco.com
Server:          10.163.47.11
Address:         10.163.47.11#53

** server can't find www.cisco.com: NXDOMAIN
```

解决方案：在这种情况下，您需要配置不同的 DNS 服务器，或获取已更新的服务器，使其能够解析需要解析的 FQDN。联系您的网络管理员或 ISP，获取可用于您网络的 DNS 服务器的 IP 地址。

- 如果您收到“连接已超时”消息，系统将无法访问 DNS 服务器，或所有 DNS 服务器目前均有故障，无法响应（不太可能出现这种情况）。继续进行下一步。

```
> nslookup www.cisco.com
; ; connection timed out; no servers could be reached
```

步骤 4 使用 `traceroute system DNS_server_ip_address` 命令追踪到 DNS 服务器的路由。

例如，如果 DNS 服务器 10.100.10.1，请输入：

```
> traceroute system 10.100.10.1
```

下文是可能出现的结果：

- 跟踪路由完成并到达 DNS 服务器。在这种情况下，实际上存在通向 DNS 服务器的路由，且系统可以访问该服务器。因此，没有任何路由问题。但是，由于某种原因，到此服务器的 DNS 请求没有获得响应。

解决方案：可能是因为沿该路径的路由器或防火墙丢弃 UDP/53 流量，这是用于 DNS 的端口。您可以沿其他网络路径尝试连接 DNS 服务器。这种问题比较棘手，因为您需要确定哪个节点阻止流量，并联系系统管理员才能更改访问规则。

- 跟踪路由连一个节点都无法访问，其响应如下所示：

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1 * * *
 2 * * *
 3 * * *
 (and so forth)
```

解决方案：在这种情况下，系统存在路由问题。尝试为网关 IP 地址执行 `ping system`。按照之前步骤中的介绍重新验证管理接口的配置，确保您已配置所需的网关和路由。

- 跟踪路由可以通过几个节点，之后便不再能够解析路由，其响应如下所示：

```
> traceroute system 10.100.10.1
traceroute to 10.100.10.1 (10.100.10.1), 30 hops max, 60 byte packets
 1 192.168.0.254 (192.168.0.254) 0.475 ms 0.532 ms 0.542 ms
 2 10.88.127.1 (10.88.127.1) 0.803 ms 1.434 ms 1.443 ms
 3 site04-lab-gwl.example.com (10.89.128.25) 1.390 ms 1.399 ms 1.435 ms
 4 * * *
 5 * * *
 6 * * *
```

解决方案：这种情况下，路由在最后一个节点出现问题。您可能需要联系系统管理员，以在该节点安装正确的路由。但是，如果有意地在该节点不设置通往 DNS 服务器的路由，您需要更改网关，或创建自己的静态路由，使其指向可以将流量路由到 DNS 服务器的路由器。

分析 CPU 和内存使用情况

要查看有关 CPU 和内存使用情况的系统级信息，请依次选择**监控 > 系统**，然后查找 CPU 和“内存”条形图。这些图表显示通过 CLI 使用 **show cpu system** 和 **show memory system** 命令收集的信息。

如果打开 CLI 控制台或登录 CLI，还可以使用这些命令的其他版本查看其他信息。通常，只有当使用情况存在长时间持续的问题时，或者奉思科技术支持中心 (TAC) 之命，才会查看此信息。其中许多详细信息比较复杂，需要 TAC 加以解释。

以下是您可以检查的一些要点。您可以在**思科 Firepower 威胁防御命令参考**（网址为 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html）中找到有关这些命令的更多详细信息。

- **show cpu** 显示数据平面 CPU 使用情况。
- **show cpu core** 分别显示每个 CPU 核心的使用情况。
- **show cpu detailed** 显示其他每个核心及总数据平面的 CPU 使用情况。
- **show memory** 显示数据平面内存使用情况。



注释 某些关键字（上文未提及）需要先使用 **cpu** 或 **memory** 命令设置分析或其他功能。这些功能只能奉 TAC 之命使用。

查看日志

系统会记录各种操作的信息。您可以使用 **system support view-files** 命令打开系统日志。请在配合思科技术支持中心 (TAC) 解决问题时使用此命令，以便他们帮助您解释输出内容并选择要查看的相应日志。

该命令将显示一个菜单供您选择日志。请使用以下命令在向导中导航：

- 要更改为子目录，请键入该目录的名称并按 Enter 键。
- 要选择欲查看的文件，请在提示符后输入 **s**。然后系统将提示您输入文件名。请键入完整名称，并注意区分大小写。文件列表会显示日志的大小，您最好考虑一下再打开非常大的日志。
- 看到 **--More--** 时，按空格键可查看下一页日志条目；按 Enter 键仅查看下一个日志条目。到达日志末尾后，即会转到主菜单。**--More--** 行会显示日志的大小和已查看部分的大小。如果不想翻阅整个日志，请使用 **Ctrl+C** 关闭日志并退出命令。
- 键入 **b** 返回菜单结构的上一级。

如果要保持日志打开以便及时看到添加的新消息，请使用 **tail-logs** 命令而非 **system support view-files**。

以下示例显示如何查看 **cisco/audit.log** 文件，该文件用于跟踪系统登录尝试。文件列表首先在顶部列出目录，然后列出当前目录下的文件。

```
> system support view-files

===View Logs===

=====
Directory: /ngfw/var/log
-----sub-dirs-----
cisco
mojo
removed_packages
setup
connector
sf
scripts
packages
removed_scripts
httpd
-----files-----
2016-10-14 18:12:04.514783 | 5371      | SMART_STATUS_sda.log
2016-10-14 18:12:04.524783 | 353      | SMART_STATUS_sdb.log
2016-10-11 21:32:23.848733 | 326517   | action_queue.log
2016-10-06 16:00:56.620019 | 1018     | br1.down.log

<list abbreviated>

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: cisco

=====
Directory: /ngfw/var/log/cisco
-----files-----
2017-02-13 22:44:42.394907 | 472      | audit.log
2017-02-13 23:40:30.858198 | 903615   | ev_stats.log.0
2017-02-09 18:14:26.870361 | 0        | ev_stats.log.0.lck
2017-02-13 05:24:00.682601 | 1024338  | ev_stats.log.1
2017-02-12 08:41:00.478103 | 1024338  | ev_stats.log.2
2017-02-11 11:58:00.260805 | 1024218  | ev_stats.log.3
2017-02-09 18:12:13.828607 | 95848    | firstboot.ngfw-onbox.log
2017-02-13 23:40:00.240359 | 6523160  | ngfw-onbox.log

([b] to go back or [s] to select a file to view, [Ctrl+C] to exit)
Type a sub-dir name to list its contents: s

Type the name of the file to view ([b] to go back, [Ctrl+C] to exit)
> audit.log
2017-02-09 18:59:26 - SubSystem:LOGIN, User:admin, IP:10.24.42.205, Message:Login successful,
2017-02-13 17:59:28 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,
2017-02-13 22:44:36 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login failed,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Login successful,
2017-02-13 22:44:42 - SubSystem:LOGIN, User:admin, IP:10.24.111.72, Message:Unlocked account.,

<remaining log truncated>
```

创建故障排除文件

在提交问题报告时，思科技术支持中心 (TAC) 人员可能要求您提交系统日志消息。这些信息可帮助他们诊断问题。您无需提交诊断文件，除非要求您这样做。

以下步骤程序介绍了如何创建和下载诊断文件。

过程

步骤 1 点击 **设备**。

步骤 2 在故障排除下，点击**请求创建文件或重新请求创建文件**（如果您之前已创建一份文件）。

系统将开始生成诊断文件。您可以转至其他页面，再返回此处检查状态。当该文件准备就绪后，会显示文件创建日期和时间及下载按钮。

步骤 3 当该文件准备就绪后，请点击**下载按钮**。

系统将使用浏览器的标准下载方法，将该文件下载到您的工作站。

不常见的管理任务

以下主题介绍您即便执行，也不会经常执行的操作。所有这些操作都可能清除您的设备配置。在进行这些更改之前，请确保设备当前没有向生产网络提供重要服务。

在本地和远程管理之间切换

您可以使用本地 Firepower 设备管理器（直接托管在设备上）配置和管理自己的设备，也可以使用 Firepower 管理中心 多设备管理器进行远程配置和管理。如果要配置不受 Firepower 设备管理器支持的功能，或需要 Firepower 管理中心提供的效能和分析功能，您可能要使用远程管理器。

另外，若要在透明防火墙模式下运行设备，也必须使用 Firepower 管理中心。

您可以在本地和远程管理之间切换，而无需重新安装软件。在从远程管理切换至本地管理之前，请确认 Firepower 设备管理器满足您的所有配置要求。



注意

切换管理器会清除设备配置，并会使系统恢复默认配置。但是，管理 IP 地址和主机名保留不变。

开始之前

如果已注册了设备，特别是如果启用了任何功能许可证，则必须通过 Firepower 设备管理器取消注册设备，然后才能切换到远程管理。取消注册设备会释放基本许可证和所有功能许可证。如果不取消注册设备，这些许可证将保持分配给思科智能软件管理器中的设备。请参阅[注销设备](#)，第 75 页。

如果设备已配置为高可用性，您必须首先使用设备管理器（如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 使用 SSH 客户端打开与管理 IP 地址的连接，使用具有配置 CLI 访问权限的用户名登录设备 CLI。例如 **admin** 用户名。

连接到管理 IP 地址时，请务必执行此过程。使用 Firepower 设备管理器时，您可以选择通过数据接口上的 IP 地址管理设备。但是，必须使用“管理”物理端口和管理 IP 地址来远程管理设备。

如果无法连接到管理 IP 地址，请解决以下问题：

- 确保管理物理端口连接到正常运行的网络。
- 确保为管理网络配置了管理 IP 地址和网关。在 Firepower 设备管理器中，在设备 > 系统设置 > 管理接口上配置地址和网关。（在 CLI 中，使用 **configure network ipv4/ipv6 manual** 命令。）

注释 确保使用外部网关作为管理 IP 地址。使用远程管理器时，不能将数据接口用作网关。

步骤 2 要从本地管理切换为远程管理，请执行以下操作：

a) 验证您当前处于本地管理模式之下。

```
> show managers
Managed locally.
```

b) 配置远程管理器

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

其中：

- {hostname | IPv4_address | IPv6_address | DONTRESOLVE} 指定管理此设备的 Firepower 管理中心的 DNS 主机名或 IP 地址（IPv4 或 IPv6）。如果 Firepower 管理中心无法直接寻址，请使用 **DONTRESOLVE**。如果使用 **DONTRESOLVE**，则需要使用 *nat_id*。
- *regkey* 是向 Firepower 管理中心注册设备所需的唯一字母数字注册密钥。
- *nat_id* 是在 Firepower 管理中心与设备之间的注册流程中使用的可选字母数字字符串。如果主机名设置为 **DONTRESOLVE**，此项为必填项。

例如，要在 192.168.0.123 处使用该管理器，注册密钥为 **secret**，请输入以下信息：

```
> configure manager add 192.168.0.123 secret
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before switching to remote management.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue [yes/no] yes
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.
```

```
> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status          :
```

注释 在执行注册期间，您可以使用 **configure manager delete** 删除该注册，然后使用 **configure manager local** 返回到本地管理。

- c) 登录 Firepower 管理中心并添加设备。

有关详细信息，请参见 Firepower 管理中心在线帮助。

步骤 3 要从远程管理切换为本地管理，请执行以下操作：

- a) 验证您当前处于远程管理模式之下。

```
> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status          :
```

- b) 删除远程管理器，进入无管理器模式。

无法直接从远程管理转至本地管理。使用 **configure manager delete** 命令可删除管理器。

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

- c) 配置本地管理器。

configure manager local

例如：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

现在，您可以使用 Web 浏览器在 **https://management-IP-address** 位置打开本地管理器。

更改防火墙模式

Firepower 威胁防御 防火墙可在路由模式或透明模式下运行。路由模式防火墙是指路由的跳跃，可作为连接到任一屏蔽子网的主机的默认网关。另一方面，透明防火墙是第 2 层防火墙，其作用相当于“网络嵌入式”或“隐形防火墙”，不会被视作路由器跳跃至相连设备。

本地 Firepower 设备管理器仅支持路由模式。不过，如果需要在透明模式下运行该设备，则可以更改防火墙模式，开始使用 Firepower 管理中心 管理设备。相反，您可以将透明模式设备转换为路由模式，然后选择使用本地管理器对其进行配置（也可以使用 Firepower 管理中心 管理路由模式设备）。

无论执行本地还是远程管理，都必须使用设备 CLI 更改模式。

以下步骤程序介绍了使用本地管理器或计划使用本地管理器时如何更改模式。



注意 更改防火墙模式会清除设备配置，并会使系统恢复默认配置。但是，管理 IP 地址和主机名保留不变。

开始之前

如果要转换为透明模式，请先安装 Firepower 管理中心，再更改防火墙模式。

如果启用了任何功能许可证，您必须首先在 Firepower 设备管理器中禁用它们，然后才能删除本地管理器和切换为远程管理。否则，这些许可证将仍旧分配给思科智能软件管理器中的设备。请参阅[启用或禁用可选许可证](#)，第 74 页。

如果设备已配置为高可用性，您必须首先使用设备管理器（如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 使用 SSH 客户端打开与管理 IP 地址的连接，使用具有配置 CLI 访问权限的用户名登录设备 CLI。例如 **admin** 用户名。

连接到管理 IP 地址时，请务必执行此过程。使用 Firepower 设备管理器时，您可以选择通过数据接口上的 IP 地址管理设备。但是，必须使用“管理”物理端口和管理 IP 地址来远程管理设备。

如果无法连接到管理 IP 地址，请解决以下问题：

- 确保管理物理端口连接到正常运行的网络。
- 确保为管理网络配置了管理 IP 地址和网关。在 Firepower 设备管理器中，在 **设备 > 系统设置 > 管理接口** 上配置地址和网关。（在 CLI 中，使用 **configure network ipv4/ipv6 manual** 命令。）

注释 确保使用外部网关作为管理 IP 地址。使用远程管理器时，不能将数据接口用作网关。

步骤 2 要从路由模式更改为透明模式，并且使用远程管理：

- a) 禁用本地管理，并进入无管理器模式。

若有活动管理器，则无法更改防火墙模式。使用 **configure manager delete** 命令可删除管理器。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

b) 将防火墙模式更改为透明。

configure firewall transparent

示例：

```
> configure firewall transparent
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

c) 配置远程管理器

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

其中：

- **{hostname | IPv4_address | IPv6_address | DONTRESOLVE}** 指定管理此设备的 Firepower 管理中心的 DNS 主机名或 IP 地址（IPv4 或 IPv6）。如果 Firepower 管理中心无法直接寻址，请使用 **DONTRESOLVE**。如果使用 **DONTRESOLVE**，则需要使用 *nat_id*。
- *regkey* 是向 Firepower 管理中心注册设备所需的唯一字母数字注册密钥。
- *nat_id* 是在 Firepower 管理中心与设备之间的注册流程中使用的可选字母数字字符串。如果主机名设置为 **DONTRESOLVE**，此项为必填项。

例如，要在 192.168.0.123 处使用该管理器，注册密钥为 **secret**，请输入以下信息：

```
> configure manager add 192.168.0.123 secret
Manager successfully configured.
Please make note of reg_key as this will be required while adding
Device in FMC.

> show managers
Host                : 192.168.0.123
Registration Key    : ****
Registration        : pending
RPC Status          :
```

d) 登录 Firepower 管理中心并添加设备。

有关详细信息，请参见 Firepower 管理中心在线帮助。

步骤 3 要从透明模式更改为路由模式并转换为本地管理，请执行以下操作：

- a) 从 FMC 注销设备。
- b) 访问 FTD 设备 CLI，首选使用控制台端口。

由于更改模式会清除配置，管理 IP 地址将恢复为默认值，所以更改模式后，您可能会丢失与管理 IP 地址的 SSH 连接。

- c) 将防火墙模式更改为路由。

configure firewall routed

示例：

```
> configure firewall routed
This will destroy the current interface configurations,
are you sure that you want to proceed? [y/N] y
The firewall mode was changed successfully.
```

- d) 启用本地管理器。

configure manager local

例如：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

现在，您可以使用 Web 浏览器在 <https://management-IP-address> 位置打开本地管理器。

重置配置

如果要重新开始，您可以将系统配置重置为出厂默认设置。虽然无法直接重置配置，但删除和添加管理器可清除配置。

如果您计划擦除配置，然后恢复备份，请确保您已下载要恢复的备份副本。重置系统后，您需要上传备份副本，然后才能执行恢复。

开始之前

如果启用了任何功能许可证，必须首先在 Firepower 设备管理器中禁用它们，然后才能删除本地管理器。否则，这些许可证将仍旧分配给思科智能软件管理器中的设备。请参阅[启用或禁用可选许可证](#)，第 74 页。

如果设备已配置为高可用性，您必须首先使用设备管理器（如果可能）或 **configure high-availability disable** 命令中断高可用性配置。理想情况下，应从主用设备中断高可用性。

过程

步骤 1 使用 SSH 客户端打开指向管理 IP 地址的连接，使用具有配置 CLI 访问权限的用户名登录设备 CLI。
例如 **admin** 用户名。

步骤 2 使用 **configure manager delete** 命令可删除管理器。

```
> configure manager delete
If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in Cisco
Smart Software Manager.
Do you want to continue[yes/no] yes
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

步骤 3 配置本地管理器。

configure manager local

例如：

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

现在，您可以使用 Web 浏览器在 <https://management-IP-address> 位置打开本地管理器。清除配置后，系统会提示您完成设备安装向导。



附录 A

高级配置

某些设备功能可使用 ASA 配置命令进行配置。虽然 Firepower 设备管理器可以配置很多基于命令的功能，但它并非支持所有功能。如果需要使用 Firepower 设备管理器本不支持的一些 ASA 功能，可以使用 Smart CLI 或 FlexConfig 手动配置这些功能。

以下主题详细说明这种类型的高级配置。

- [关于 Smart CLI 和 FlexConfig，第 501 页](#)
- [Smart CLI 和 FlexConfig 的准则与限制，第 509 页](#)
- [配置 Smart CLI 对象，第 510 页](#)
- [配置 FlexConfig 策略，第 511 页](#)
- [FlexConfig 策略故障排除，第 522 页](#)
- [FlexConfig 示例，第 523 页](#)

关于 Smart CLI 和 FlexConfig

Firepower 威胁防御使用 ASA 配置命令实现一些功能，但不是所有功能。没有唯一的一组 Firepower 威胁防御配置命令。

您可以借助以下方法使用 CLI 配置功能：

- **Smart CLI** - (首选方法。) Smart CLI 模板为用于特定功能的预定义模板，提供相应功能所需的所有命令，您只需选择变量值即可。系统会验证您的选择，以促进您正确配置具体功能。如果您所需的功能有对应的 Smart CLI 模板，则必须使用此方法。
- **FlexConfig** - FlexConfig 策略是 FlexConfig 对象的集合。FlexConfig 对象的形式比 Smart CLI 模板更自由，且系统不执行 CLI、变量或数据验证。您必须了解 ASA 配置命令，并按照 ASA 配置指南创建有效的命令序列。

Smart CLI 和 FlexConfig 的意义在于允许您配置不直接通过 Firepower 设备管理器策略和设置支持的功能。

**注意**

思科强烈声明，只建议具有较强 ASA 背景且自承风险的高级用户使用 Smart CLI 和 FlexConfig。您可配置任何未列入黑名单的命令。通过 Smart CLI 和 FlexConfig 启用功能可能会导致配置的其他功能出现意想不到的结果。

您可以联系思科技术支持中心获取有关您已配置的 Smart CLI 和 FlexConfig 对象的支持。思科技术支持中心不代表任何客户设计或编写自定义配置。思科不保证正确的操作或与其他 Firepower 威胁防御功能的互通性。Smart CLI 和 FlexConfig 功能可能随时被摒弃。为获得充分保证的功能支持，您必须等待 Firepower 设备管理器支持。如有疑问，请勿使用 Smart CLI 或 FlexConfig。

以下主题更详细地解释这些功能。

Smart CLI 和 FlexConfig 的建议用法

FlexConfig 有两大主要推荐用途：

- 您正在从 ASA 迁移至 FTD，并且存在您正在使用（且需继续使用）的 Firepower 设备管理器不直接支持的兼容功能。在这种情况下，请在 ASA 上使用 **show running-config** 命令来查看功能配置，并创建实现功能的 FlexConfig 对象。通过比较两个设备上的 **show running-config** 输入予以验证。
- 您正在使用 FTD，但有一个设置或功能需要配置，例如思科技术援助中心告诉您特定的设置应解决您遇到的特定问题。对于复杂功能，请使用实验室设备测试 FlexConfig，并验证您是否将得到预期行为。

尝试重新创建 ASA 配置前，请先确定是否可在标准策略中配置等效功能。例如，访问控制策略包括 ASA 使用单独功能实现的入侵检测和预防、HTTP 和其他类型的协议检查、URL 过滤、应用程序过滤和访问控制。由于许多功能并未使用 CLI 命令予以配置，因此，您不会看到各策略均显示在 **show running-config** 输出内。

**注释**

在任何时候，请记住 ASA 和 FTD 之间不存在一对一重叠关系。请勿尝试在 FTD 设备上完全重新创建 ASA 配置。您必须仔细测试使用 FlexConfig 配置的各项功能。

Smart CLI 和 FlexConfig 对象中的 CLI 命令

FTD 使用 ASA 配置命令配置某些功能。虽然并非所有的 ASA 功能均与 FTD 兼容，但仍存在可有效用于 FTD 却无法在 Firepower 设备管理器策略中进行配置的某些功能。您可以使用 Smart CLI 和 FlexConfig 对象指定配置这些功能所需的 CLI。

如果决定使用 Smart CLI 或 FlexConfig 手动配置功能，则需负责根据正确语法了解和执行这些命令。FlexConfig 不验证 CLI 命令语法。有关正确语法和配置 CLI 命令的更多信息，请使用以下 ASA 文档作为参考：

- ASA CLI 配置指南介绍了如何配置功能。指南位于：<http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html>
- ASA 命令参考提供按命令名称排序的附加信息。参考位于：<http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html>

以下主题介绍了有关配置命令的更多信息。

软件升级如何影响 FlexConfig 策略

每个新版本的 Firepower 威胁防御 软件都添加了对配置 Firepower 设备管理器中功能的支持。有时，这些新功能可能与您先前已使用 FlexConfig 配置的功能重叠。

升级后，您需要检查 FlexConfig 策略和对象。如果任何策略和对象包含因 Firepower 设备管理器或 Smart CLI 中添加的支持而被列入黑名单的命令，对象列表中的图标和消息会指出这一问题。请抽出时间重新进行配置。参考命令黑名单列表，帮助确定命令现在的部署位置。

系统不会阻止您部署更改，尽管连接到 FlexConfig 策略的 FlexConfig 对象包含新列入黑名单的命令。但是，您将无法创建新的 Smart CLI 对象，直到解决 FlexConfig 策略中提及的所有问题。

从 FlexConfig 策略中删除有问题的对象即可，因为限制仅适用于您主动部署到设备配置的对象。因此，您可以删除这些对象，创建相应的 Smart CLI 或集成 Firepower 设备管理器配置时再使用这些对象作参考。新配置达到要求后，删除对象即可。如果删除的对象包含一些未列入黑名单的元素，您可以编辑删除不受支持的命令，然后将其重新连接到 FlexConfig 策略。

确定 ASA 软件版本和当前 CLI 配置

由于系统使用 ASA 软件命令配置某些功能，因此需要确定在 FTD 设备上运行的软件中使用的当前 ASA 版本。此版本号指示用于指导配置功能的 ASA CLI 配置指南。此外，您还应检查当前基于 CLI 的配置，并将其与要实施的 ASA 配置进行比较。

注意，任何 ASA 配置都与 FTD 配置有着显著的差异。许多 FTD 策略都是在 CLI 之外配置的，因此查看这些命令看不到配置。请勿尝试在 ASA 和 FTD 配置之间创建一对一的对应关系。

要查看此信息，请在 Firepower 设备管理器中打开 CLI 控制台，或与设备管理接口建立 SSH 连接，然后发出以下命令：

- **show version system** 并查找思科自适应安全设备软件版本号。
- **show running-config** 查看当前的 CLI 配置。
- **show running-config all** 包括当前 CLI 配置中的所有默认命令。

禁止的 CLI 命令

Smart CLI 和 FlexConfig 的用途是配置在 ASA 设备上可用但无法使用 Firepower 设备管理器在 FTD 设备上配置的功能。

因此，您无法配置在 Firepower 设备管理器中具有等同功能的 ASA 功能。下表列出的是一些禁止的命令区。该列表包含许多进入配置模式的父命令。禁止父命令包括禁止子命令。还包括命令的 **no** 版本及其相关的 **clear** 命令。

FlexConfig 对象编辑器可防止将这些命令纳入对象中。此列表不适用于 Smart CLI 模板，因为这些模板仅包含可有效配置的命令。

禁止的 CLI 命令	备注
aaa	使用对象 > 身份源。
aaa-server	使用对象 > 身份源。
access-group	使用策略 > 访问控制，配置访问规则。
access-list	部分阻止。 <ul style="list-style-type: none"> • 可以创建 ethertype 访问列表。 • 不能创建 extended 和 standard 访问列表。使用智能 CLI 扩展访问列表或标准访问列表对象创建这些 ACL。然后，可以在按对象名称引用 ACL 且支持 FlexConfig 的命令中使用，例如带扩展 ACL 的 match access-list 用于服务策略流量类别。 • 无法创建 advanced 访问列表，系统将该访问列表与 access-group 命令一起使用。请使用策略 > 访问控制来配置访问规则。 • 不能创建 webtype 访问列表。
anyconnect-custom-data	使用设备 > 远程接入 VPN 配置 AnyConnect。
asdm	此功能不适用于 FTD 系统。
as-path	创建智能 CLI AS 路径对象，并将其用于智能 CLI BGP 对象，以配置自治系统路径过滤器。
attribute	—
auth-prompt	此功能不适用于 FTD 系统。
boot	—
call-home	—
captive-portal	使用策略 > 身份配置用于主动身份验证的强制网络门户。
clear	—
client-update	—
clock	使用设备 > 系统设置 > NTP 来配置系统时间。
cluster	—
command-alias	—

禁止的 CLI 命令	备注
community-list	创建智能 CLI 扩展社区列表或标准社区列表对象，并将其用于智能 CLI BGP 对象，以配置社区列表过滤器。
compression	—
configure	—
crypto	在对象页面上，使用证书、IKE 策略和 IPSec 提议。
dhcp-client	—
dhcpd	依次选择设备 > 系统设置 > DHCP 服务器。
dns	使用对象 > DNS 组配置 DNS 组，并使用设备 > 系统设置 > DNS 服务器分配这些组。
dns-group	使用对象 > DNS 组配置 DNS 组，并使用设备 > 系统设置 > DNS 服务器分配这些组。
domain-name	使用对象 > DNS 组配置 DNS 组，并使用设备 > 系统设置 > DNS 服务器分配这些组。
dynamic-access-policy-config	—
dynamic-access-policy-record	—
enable	—
event	—
failover	—
fips	—
firewall	Firepower 设备管理器仅支持路由防火墙模式。
hostname	依次选择设备 > 系统设置 > 主机名。
hpm	此功能不适用于 FTD 系统。
http	依次访问设备 > 系统设置 > 管理访问，使用数据接口选项卡。
inline-set	—

禁止的 CLI 命令	备注
interface 用于 BVI、管理、以太网、千兆以太网和子接口。	<p>部分阻止。</p> <p>在 设备 > 接口 页面上，配置物理接口、子接口和网桥虚拟接口。然后，可使用 FlexConfig 配置其他选项。</p> <p>但对于这些接口类型，禁止如下 interface 模式命令。</p> <p>cts ip address ip address dhcp ipv6 address ipv6 enable ipv6 nd dad ipv6 nd suppress-ra mode nameif security-level shutdown zone-member</p>
适用于 vni 、 redundant 、 tunnel 和 portchannel 的 interface	在 设备 > 接口 页面上配置接口。Firepower 设备管理器不支持这些类型的接口。
ip audit	此功能不适用于 FTD 系统。而应使用访问控制规则应用入侵策略。
ip-client	要将系统配置为使用数据接口作为管理网关，请使用 设备 > 系统设置 > 管理接口 。
ip local pool	使用 设备 > 远程接入 VPN ，配置地址池。
ipsec	—
ipv6	<p>可以配置 ipv6 ospf 和 ipv6 router ospf 命令，但所有其他 ipv6 命令均无法配置。</p> <p>创建智能 CLI IPv6 前缀列表对象，并将其用于智能 CLI BGP 对象，以配置 IPv6 前缀列表过滤。</p>
ipv6-vpn-addr-assign	使用 设备 > 远程接入 VPN ，配置地址池。
isakmp	使用 设备 > 站点间 VPN 。
jumbo-frame	如果将任何接口的 MTU 增至超出默认值 1500，系统将自动启用巨帧支持。
ldap	—
license-server	使用 设备 > 智能许可证 。

禁止的 CLI 命令	备注
logging	使用对象 > 系统日志服务器和设备 > 系统设置 > 日志记录设置。 但是，您可以在 FlexConfig 中配置 logging history 命令。
management-access	—
migrate	使用设备 > 远程接入 VPN 和设备 > 站点间 VPN 来启用 IKEv2 支持。
mode	Firepower 设备管理器仅支持单个上下文模式。
mount	—
mtu	在设备 > 接口上配置各接口的 MTU。
nat	使用策略 > NAT。
ngips	—
ntp	使用设备 > 系统设置 > NTP
object-group network object network	使用对象 > 网络。 无法在 FlexConfig 中创建网络对象或组，但可使用在模板内的对象管理器中定义的网络对象和组作为变量。
object service natorigsvc object service natmappedsvc	通常允许 object service 命令，但无法编辑名为 natorigsvc 或 natmappedsvc 的内部对象。在这些名称中，竖线是有意使用的，是限制对象名称的首个字符。
passwd password	—
password-policy	—
policy-list	创建智能 CLI 策略列表对象，并将其用于智能 CLI BGP 对象，以配置策略列表。
policy-map 子命令	不能在策略映射中配置以下命令。 priority police match tunnel-group
prefix-list	创建智能 CLI IPv4 前缀列表对象，并将其用于智能 CLI OSPF 或 BGP 对象，以配置 IPv4 前缀列表过滤。
priority-queue	—
privilege	—

禁止的 CLI 命令	备注
reload	不能安排重新加载。系统不使用 reload 命令重启系统，它使用的是 reboot 命令。
rest-api	此功能不适用于 FTD 系统。始终安装并启用 REST API。
route	使用 设备 > 路由 配置静态路由。
route-map	创建智能 CLI 路由映射对象，并将其用于智能 CLI OSPF 或 BGP 对象，以配置路由映射。
router bgp	使用适用于 BGP 的 Smart CLI 模板。
router ospf	使用适用于 OSPF 的 Smart CLI 模板。
scansafe	此功能不适用于 FTD 系统。请在访问控制规则中配置 URL 过滤。
setup	此功能不适用于 FTD 系统。
sla	—
ssh	依次访问 设备 > 系统设置 > 管理访问 ，使用 数据接口 选项卡。
ssl	—
telnet	FTD 不支持 Telnet 连接。使用 SSH 而不是 Telnet 访问设备 CLI。
time-range	—
tunnel-group	使用 设备 > 远程接入 VPN 和 设备 > 站点间 VPN 。
tunnel-group-map	使用 设备 > 远程接入 VPN 和 设备 > 站点间 VPN 。
user-identity	使用 策略 > 身份 。
username	要创建 CLI 用户，请打开 SSL 或设备控制台会话并使用 configure user 命令。
vpdn	—
vpn	—
vpn-addr-assign	—
vpnclient	—
vpn-sessiondb	—
vpnsetup	—
webvpn	—

禁止的 CLI 命令	备注
zone	—
zonelabs-integrity	此功能不适用于 FTD 系统。

Smart CLI 模板

下表介绍的是基于该功能的 Smart CLI 模板。

特性	模板	说明
对象：AS 路径	ASPath	创建用于路由协议对象的 ASPath 对象。
对象：访问列表	扩展访问列表 标准访问列表	创建用于路由对象的扩展或标准 ACL。您也可以从配置使用 ACL 的允许命令的 FlexConfig 对象按名称引用这些对象。
对象：社区列表	扩展社区列表 标准社区列表	创建用于路由对象的扩展或标准社区列表。
对象：前缀列表	IPV4 前缀列表 IPV6 前缀列表	创建用于路由对象的 IPV4 或 IPV6 前缀列表。
对象：策略列表	Policy List	创建用于路由对象的策略列表。
对象：路由映射	路由映射	创建用于路由对象的路由映射。
路由：BGP	BGP	使用 BGP 模板配置路由过程。
路由：OSPFv2	OSPF OSPF 接口设置	使用 OSPF 模板配置路由进程，使用接口模板配置各接口的 OSPF 行为。 提示： <ul style="list-style-type: none"> 如果打算从其他路由进程重新分配路由，则应首先配置这些过程。例如，配置 OSPF 以重新分配 EIGRP 路由前，请先创建和部署配置 EIGRP 的 FlexConfig 对象。 最多可配置 2 个 OSPF 进程。

Smart CLI 和 FlexConfig 的准则与限制

通过 Smart CLI 或 FlexConfig 配置功能时，请牢记以下几点。

- FlexConfig 对象中定义的命令应在通过 Firepower 设备管理器（包括 Smart CLI）定义的功能的所有命令之后进行部署。这样您就可以确保，在向设备发出这些命令前，配置好相应的对象和接口等。如果需要在 Smart CLI 模板中使用 FlexConfig 已部署的项目，请先创建和部署 FlexConfig，再创建和部署 Smart CLI 模板。例如，如果要使用 OSPF Smart CLI 模板重新分配 EIGRP 路由，请先使用 FlexConfig 配置 EIGRP，然后创建 OSPF Smart CLI 模板。
- 如果要删除通过 FlexConfig 配置的功能或功能的一部分，但 Smart CLI 模板引用该功能，则首先必须删除 Smart CLI 模板中使用该功能的命令。然后，部署配置，以便 Smart-CLI 配置功能不再引用它。然后，您可以从 FlexConfig 中删除该功能，并重新部署配置，最终完全清除该配置。

配置 Smart CLI 对象

Smart CLI 对象定义了无法在 Firepower 设备管理器中配置的功能。Smart CLI 对象为功能配置提供了一定程度的指导。对于给定的功能（模板），所有可能的命令均已预先加载且已验证所输入的变量。因此，尽管仍然使用 CLI 命令进行功能配置，但 Smart CLI 对象并不像 FlexConfig 对象一样具有自由的形式。

虽然 Smart CLI 模板确实提供了一定程度的指导，但仍然需要阅读 ASA 配置指南和命令参考，了解命令的用法，从而选择可以在您的网络环境下正确运行的值。最好已有可作为配置基础使用的 ASA 配置，只需在 Smart CLI 对象中构建相同的命令序列。

Smart CLI 对象根据功能区（如路由）进行分组。



注释 所定义的所有 Smart CLI 对象都将被部署。与 FlexConfig 不同的是，无法创建多个 Smart CLI 对象，然后再从中选择要部署的对象。只需为要配置的功能创建 Smart CLI 对象。

过程

步骤 1 在设备 > 高级配置中点击查看配置。

步骤 2 在“高级配置”目录中点击 **Smart CLI** 下的相应功能区。例如，**Smart CLI > 路由**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 4 输入对象的名称和描述（后者为可选项）。

步骤 5 为要配置的功能选择 **CLI 模板**。

系统会将命令模板加载到模板窗口中。最初，系统只显示模板所需的命令。这些命令表示模板所需的最低配置。

注释 某些功能需要多个模板。例如，要配置 OSPFv2，需要使用 **OSPF** 和 **接口** 模板创建两个 Smart CLI 对象。请注意，不能使用 OSPF 模板配置 OSPFv3。

步骤 6 填写变量并根据需要在模板中添加命令。

最好使用 ASA 或 Firepower 威胁防御设备（由 Firepower 管理中心负责管理）的现有配置。有了相应配置，只需确保模板符合配置要求，即可更改适合网络中该特定设备位置的变量（例如 IP 地址和接口名称）。

以下是填写模板的一些提示：

- 要选择变量值，请点击变量，然后键入适当的值或从列表中选择（在有枚举值的情况下）。将鼠标移动到需要键入的变量上，显示该选项的有效值（例如数字范围）。在某些情况下，系统会提供建议值。

例如，在 OSPF 模板中，所需的命令 **router ospf process-id** 在鼠标悬停于其上时显示“进程 ID (1-65535)”，点击 *process-id* 时，该字段会高亮显示。只需键入所需的数字即可。

- 选择变量选项时，如果有其他可能的命令可以配置该选项，则会自动显示并根据需要禁用或启用。注意这些附加命令。
- 使用模板上方的 **显示/隐藏禁用** 链接控制视图。系统不会配置禁用的命令，但您必须显示这些命令才能进行配置。要查看完整模板，请点击模板上方的 **显示禁用** 链接。如只查看将要配置的命令，请点击表上方的 **隐藏禁用** 链接。
- 要清除上次保存对象之后的所有编辑内容，请点击模板上方的 **重置** 链接。
- 要启用可选命令，请点击行号左侧的 + 按钮。
- 要禁用可选命令，请点击行号左侧的 - 按钮。如果已编辑该行，则不会删除编辑内容。
- 要复制命令，请点击“选项”... 按钮，然后选择 **复制**。只有在多次输入命令有效时，才允许复制命令。
- 要删除复制命令，请点击选项 ... 按钮，然后选择 **删除**。无法删除作为基本模板组成部分的命令。

步骤 7 单击 **OK**。

配置 FlexConfig 策略

FlexConfig 策略只是希望部署到设备配置中的 FlexConfig 对象列表。系统仅部署该策略中包含的对象，所有其他对象均只进行定义而不使用。

FlexConfig 对象中定义的命令应在通过 Firepower 设备管理器（包括 Smart CLI）定义的功能的所有命令之后进行部署。这样您就可以确保，在向设备发出这些命令前，配置好相应的对象和接口等。如果需要在 Smart CLI 模板中使用 FlexConfig 已部署的项目，请先创建和部署 FlexConfig，再创建和

部署 Smart CLI 模板。例如，如果要使用 OSPF Smart CLI 模板重新分配 EIGRP 路由，请先使用 FlexConfig 配置 EIGRP，然后创建 OSPF Smart CLI 模板。



注释 如有用于功能的 Smart CLI 模板，则不可使用 FlexConfig 进行配置。必须使用 Smart CLI 对象。

开始之前

创建 FlexConfig 对象。请参阅以下主题：

- [配置 FlexConfig 对象，第 513 页](#)
- [在 FlexConfig 对象中创建变量，第 514 页](#)
- [配置密钥对象，第 521 页](#)

过程

步骤 1 在设备 > 高级配置中点击[查看配置](#)。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 策略**。

步骤 3 管理组列表中的对象列表。

- 要添加对象，请点击 + 按钮。如果对象尚不存在，请点击[创建新的 FlexConfig 对象](#)来定义。
- 要删除对象，请点击对象条目右侧的 X 按钮。

注释 建议使每个对象都完全独立，而不依赖于任何其他 FlexConfig 对象中定义的配置。这样可以确保在不影响其他对象的情况下添加或删除对象。

步骤 4 在预览窗格中评估建议的命令。

可以点击[展开](#)按钮（随后点击[折叠](#)）加宽显示画面，以便更清晰地查看长命令。

预览将评估变量并生成将要发布的确切命令。请确保这些命令正确且有效。您必须确保这些命令不会导致错误或配置不当，否则会使设备无法使用。

注意 系统不验证命令。可以部署无效甚至可能有破坏性的命令。在部署更改之前，请仔细检查预览。

步骤 5 点击保存。

下一步做什么

编辑 FlexConfig 策略后，仔细检查下一部署的结果。如果出现错误，请更正对象中的 CLI。请参阅[FlexConfig 策略故障排除，第 522 页](#)。

配置 FlexConfig 对象

对于无法使用 Firepower 设备管理器进行配置的特定功能，FlexConfig 对象包含配置这类功能所需的 ASA 命令。您必须确保输入正确的命令序列，且无拼写错误。系统不验证 FlexConfig 对象的内容。

建议为要配置的每个常规功能创建单独的对象。例如，如要定义 banner 并配置 RIP 路由协议，请使用 2 个单独的对象。如果以单独的对象隔离各个功能，则可以更轻松地选择要部署的对象，而且更易于进行故障排除。



注释 请勿包括 **enable** 和 **configure terminal** 命令。系统将自动进入配置命令的正确模式。

过程

步骤 1 在设备 > 高级配置中点击查看配置。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig > FlexConfig 对象**。

步骤 3 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 4 输入对象的名称和描述（后者为可选项）。

步骤 5 在变量部分，创建要在对象正文中使用的所有变量。

唯一必须创建的变量是指向 Firepower 设备管理器中所定义对象的变量，具体而言即网络、端口和密钥变量类型，或指向指定接口的接口变量。对于其他变量类型，只需将值输入到对象正文中。

有关创建和使用变量的详细信息，请参阅[在 FlexConfig 对象中创建变量](#)，第 514 页。

步骤 6 在模板部分，键入配置该功能所需的 ASA 命令。

必须按正确的顺序输入命令，以便配置该功能。使用 ASA CLI 配置指南，了解如何输入命令。最好拥有 ASA 或其他 FTD 设备提供的经过预先测试的配置文件，以使用作参考。

此外，还可以使用 Mustache 表示法来引用和处理变量。有关详细信息，请参阅[引用 FlexConfig 变量和检索值](#)，第 516 页。

以下是创建对象正文的一些提示：

- 要添加行，请将光标放在行尾然后按 Enter 键。
- 要使用变量，请在双括号 `{{variable_name}}` 中键入变量名称。对于引用对象的变量，必须包括要检索其值的属性：`{{variable_name.attribute}}`。可用属性因对象类型而异。有关完整信息，请参阅[变量引用：{{variable}} 或 {{{variable}}}](#)，第 516 页。

- 要使用 Smart CLI 对象，请键入对象的名称。如果需要引用 Smart CLI 中配置的路由进程，请输入进程标识符。请参阅[在 FlexConfig 对象中引用 Smart CLI 对象](#)，第 520 页。
- 点击模板正文上方的[展开/折叠](#)链接，放大或缩小正文。
- 点击[重置](#)链接，清除自上次保存对象之后所做的任何更改。

步骤 7 在取消模板部分，输入删除或反向对象正文中已配置命令所需的命令

“取消”部分非常重要，有两个用途：

- 它简化了部署。在重新部署正文中的命令之前，系统将使用这些命令先清除或取消配置。这将确保一个干净的部署环境。
- 如果您决定通过从 FlexConfig 策略中删除对象的方式来删除该功能，系统将使用这些命令从设备中删除命令。

如果不提供在对象正文中取消或反向 CLI 所需的命令，则部署操作可能需要清除整个设备配置并重新部署所有策略，而不仅仅是对象中的命令。这将使部署时间更长，并且将造成流量中断。确保拥有撤消对象正文中所定义配置所需的所有命令，而且只有这些命令。虽然在模板中否定命令通常是命令的 **no** 或 **clear** 形式，如果真实关闭已启用的功能，“否定”命令实际上是命令的肯定形式，也即启用功能的形式。

使用 ASA 配置指南和命令参考确定相应的命令。有时，可以使用单个命令撤消配置。例如，在配置 RIP 的对象中，单个 **no router rip** 命令即可删除整个 **router rip** 配置，包括子命令。

同样，如果输入多个 **banner login** 命令创建多行横幅，则单个 **no banner login** 命令将取消整个登录横幅。

如果模板创建多个嵌套对象，取消模板需要按照反向顺序删除对象，即首先删除对象引用，然后再删除对象。例如，如果您先创建一个 ACL，接着在流量类中引用该 ACL，随后在策略映射中引用流量类，最后使用服务策略启用策略映射，那么取消模板必须依次删除服务策略、策略映射、流量类以及 ACL 来撤消配置。

步骤 8 点击确定。

下一步做什么

仅创建一个 FlexConfig 对象不足以完成部署。必须将该对象添加到 FlexConfig 策略中。仅 FlexConfig 策略中的对象可进行部署。这样可细化 FlexConfig 对象并为特殊用途做一些准备，而不会自动部署这些对象。请参阅[配置 FlexConfig 策略](#)，第 511 页。

在 FlexConfig 对象中创建变量

FlexConfig 对象中使用的变量在该对象中进行定义。没有单独的变量列表。因此，无法定义某个变量，然后在单独的 FlexConfig 对象中使用该变量。

变量提供以下主要好处：

- 可以指向使用 Firepower 设备管理器定义的对象。这包括网络、端口和密钥对象。
- 可以隔离可能会随对象正文变化的值。因此，如果需要更改值，只需编辑变量，而无需编辑对象正文。如果需要在多个命令行中引用对象，这会特别有用。


此程序说明向 FlexConfig 对象中添加变量的过程。


过程

步骤 1 从设备 > 高级配置页面中编辑或创建 FlexConfig 对象。

请参阅[配置 FlexConfig 对象](#)，第 513 页。

步骤 2 在变量部分执行下列操作之一：

- 要添加变量，请点击 + 按钮（如果尚未定义变量，请点击[添加变量](#)）。
- 要编辑变量，请点击该变量的编辑图标 ().

要删除变量，请点击该变量的垃圾桶 () 图标。确保从模板正文中删除变量的任何引用。

步骤 3 输入变量的名称和描述（后者为可选项）。

步骤 4 选择变量的数据类型，然后输入或选择相应值。

可以创建以下类型的变量。选择满足使用变量的命令数据要求的类型。

- **字符串** - 文本字符串。例如，主机名、用户名等。
- **数字** - 整数。不要使用逗号、小数、符号（如负号 -）或十六进制表示法。对于非整数数字，请使用字符串变量。
- **布尔值** - 逻辑真/假。选择真或假。
- **网络** - “对象”页面上定义的网络对象或组。选择网络对象或组。
- **端口** - “对象”页面上定义的 TCP 或 UDP 端口对象。选择端口对象。无法为其他协议选择组或对象。
- **接口** - “设备” > “接口”页面上定义的指定接口。选择接口。无法选择没有名称的接口。
- **IP** - 不带网络掩码或前缀长度的单个 IPv4 或 IPv6 IP 地址。
- **密钥** - 为 FlexConfig 定义的密钥对象。选择对象。有关创建密钥对象的详细信息，请参阅[配置密钥对象](#)，第 521 页。

步骤 5 在“变量”对话框中点击[添加](#)或[保存](#)。

此时，可以在 FlexConfig 对象正文中使用该变量。引用变量的方式根据变量类型的不同而有所不同。有关如何使用这些变量的详细信息，请参阅下列主题：

- [变量引用：{{variable}} 或 {{{variable}}}](#)，第 516 页

- 部分 `{{#key}}` `{{/key}}` 和反向部分 `{{^key}}` `{{/key}}`，第 518 页

步骤 6 在 FlexConfig “对象” 对话框中点击确定。

引用 FlexConfig 变量和检索值

FlexConfig 将 Mustache 作为模板语言，但支持仅限于以下各节中介绍的功能。使用这些功能引用变量、检索其值并予以处理。

变量引用：`{{variable}}` 或 `{{{variable}}}`

要引用在 FlexConfig 对象中定义的变量，请使用以下表示法：

```
{{variable_name}}
```

或：

```
{{{variable_name}}}
```

这足以用于为单值的简单变量，其中包括如下类型的变量：**数字、字符串、布尔值和 IP**。如果变量包含特殊字符（如 &），请使用三重大括号。或者，您可以始终对所有变量使用三重大括号。

但是，对于指向在配置数据库中建模为对象的元素的变量，必须使用点符号并纳入要检索的对象属性的名称。可通过检查相关对象类型的 API Explorer 中的模型查找这些属性名称。必须借助以下表示法使用以下类型的变量：**密钥、网络、端口和接口**。

```
{{variable_name.attribute}}
```

例如，要从名为 net-object1 的网络变量（指向网络对象，而不是网络组）检索地址，可使用：

```
{{net-object1.value}}
```

如果想要从对象内的对象中检索属性值，则需使用一系列带点符号的属性向下钻取所需值。例如，将接口的 IP 地址建模为名为 ipv4 和 ipv6 的接口对象子接口。因此，要检索名为 int-inside（指向内部接口）的接口变量的 IPv4 地址和子网掩码，可以使用：

```
{{int-inside.ipv4.ipAddress.ipAddress}} {{int-inside.ipv4.ipAddress.netmask}}
```



注释 要打开 API Explorer，请将浏览器中 URL 的最后一部分改成 `/#/api-explorer`。

下表列出的是变量类型、引用方式、API 模型名称及最可能使用的引用（对于对象）。

变量类型	参考模型	说明
布尔值 (简单变量)	<p>变量:</p> <pre>{{variable_name}}</pre> <p>部分:</p> <pre>{{#variable_name}} commands {{/variable_name}}</pre> <p>反向部分:</p> <pre>{{^variable_name}} commands {{/variable_name}}</pre>	<p>逻辑 true/false。布尔变量的主要用途是用于部分或反向部分。可以编辑布尔变量值打开或关闭一部分命令，例如，如果需要定期或在特殊情况下启用某项功能。</p> <p>一些对象在其模型中也具有布尔属性，可用于提供可选的部分处理。</p>
接口 (对象变量: API 模型是 Interface)	<p>变量:</p> <pre>{{variable_name.attribute}}</pre> <p>部分:</p> <pre>{{#variable_name.attribute}} commands {{/variable_name.attribute}}</pre> <p>反向部分:</p> <pre>{{^variable_name.attribute}} commands {{/variable_name.attribute}}</pre>	<p>在“设备” > “接口”页面上定义命名的接口。无法指向未命名接口。</p> <p>接口模型中有各种可用属性。此外，接口模型包括子对象，例如 IP 地址子对象。</p> <p>以下是您可能觉得有用的一些主要属性:</p> <ul style="list-style-type: none"> • variable_name.name 返回接口的逻辑名称。 • variable_name.hardwareName 返回接口端口名称，如 GigabitEthernet1/8。 • variable_name.managementOnly 是一个布尔值。TRUE 表示该接口被定义为仅限于管理。FALSE 表示该接口用于流经设备的流量。可以将此选项用作为部分密钥。 • variable_name.ipv4.ipAddress.ipAddress 返回接口的 IPv4 地址。 • variable_name.ipv4.ipAddress.netmask 返回接口的 IPv4 地址的子网掩码。
IP (简单变量)	<p>变量:</p> <pre>{{variable_name}}</pre>	<p>单个 IPv4 或 IPv6 IP 地址，无网络掩码或前缀长度。</p>

变量类型	参考模型	说明
网络 (对象变量: API 模型是 NetworkObject)	变量 (网络对象): <code>{{variable_name.attribute}}</code> 部分 (组对象): <code>{{#variable_name.objects}}</code> <code> commands referring to one of</code> <code> {{value}}</code> <code> {{name}}</code> <code>{{/variable_name.objects}}</code>	“对象”页面上定义的网络对象或组。可使用部分处理网络组。 以下是可能对您有用的主要属性: <ul style="list-style-type: none"> • <code>{{variable_name.name}}</code> 返回网络对象或组名称。 • <code>{{variable_name.value}}</code> 返回网络对象 (而非网络组) 的 IP 地址内容。确保将具有正确类型内容的网络对象用于给定命令, 例如使用主机地址而不是子网掩码地址。 • <code>{{variable_name.groups}}</code> 返回网络组中包含的网络对象的列表。仅与指向网络组的变量结合使用, 并在部分标记上使用以反复处理组内容。Use either <code>{{value}}</code> or <code>{{name}}</code> 依次检索各网络对象的内容。
数字 (简单变量)	变量: <code>{{variable_name}}</code>	整数。不要使用逗号、小数、符号 (如负号 -) 或十六进制表示法。对于非整数数字, 请使用字符串变量。
端口 (对象变量: API 模型是 PortObject、tcpports 或 udpports)	变量: <code>{{variable_name.attribute}}</code>	在“对象”页面定义的 TCP 或 UDP 端口对象。必须为端口对象, 而不是端口组。 以下是可能对您有用的主要属性: <ul style="list-style-type: none"> • <code>{{variable_name.port}}</code> 返回端口号。协议不包括在内。 • <code>{{variable_name.name}}</code> 返回端口对象名称。
密钥 (对象变量: API 模型是“密钥”)	变量: <code>{{variable_name.password}}</code> 或: <code>{{{variable_name.password}}}</code>	为 FlexConfig 定义的密钥对象。 应该进行的唯一引用是返回加密字符串的 password 属性。 如果密码包含特殊字符 (如 &), 请使用三重大括号。
字符串 (简单变量)	变量: <code>{{variable_name}}</code>	文本字符串。例如, 主机名、用户名等。

部分 `{{#key}}{/key}}` 和反向部分 `{{^key}}{/key}}`

部分或反向部分是部分开始和结束标记之间的命令块, 将密钥作为处理标准。该部分的处理方式视其为常规部分还是反向部分。

- 如果密钥为空或具有非空内容, 则处理常规部分 (或简称为部分)。如果密钥为 FALSE 或对象无内容, 则该部分中的命令不予配置。该部分被绕过了。

以下是常规部分的语法。

```

{{#key}}
one or more commands
{/key}

```

- 反向部分即部分的反面。如果密钥为 FALSE 或对象无内容，则处理反向部分。如果密钥为 TRUE 或对象具有内容，则绕过反向部分。

以下是反向部分的语法。唯一的区别是插入符号替换散列标记。

```

{{^key}}
one or more commands
{/key}

```

以下主题介绍部分和反向部分的主要用途。

如何处理多值变量

多值变量处理的一个主要示例是指向网络组的网络变量。由于该组包含多个对象（在 **objects** 属性下），可迭代地遍历网络组中的值以使用不同值多次配置相同命令。

例如，如果主机为 192.168.10.0、192.168.20.0 和 192.168.30.0 的网络组名称为 **net-group**，则可使用以下方法为各 RIP 路由地址配置网络命令。请注意，仅使用网络对象的 **value** 属性，而不指定整个 **net-group.objects.value** 引用，因为在该部分开始时使用的 **net-group.objects** 意味着要采用此用法（对于 FlexConfig 对象中的“value”属性，不需要创建单独的变量。）

```

router rip
{{#net-group.objects}}
  network {{value}}
{/net-group.objects}

```

系统将该部分结构转换为：

```

router rip
  network 192.168.10.0
  network 192.168.20.0
  network 192.168.30.0

```

如何基于布尔值或空对象执行可选处理

如果相应部分开始标记中的变量内容为 TRUE，或对象不为空，则处理该部分。如果布尔值为 FALSE 或空（例如空对象），则绕过该部分。

这里主要用于布尔值。例如，您可以创建布尔变量，并将命令置于变量所覆盖的节中。然后，如果需要启用或禁用 FlexConfig 对象中的一部分命令，则只需更改布尔变量的值，无需从代码中删除这些行。这使得启用或禁用功能很容易。

例如，如果使用 FlexConfig 启用 SNMP，则可能希望能够关闭 SNMP 陷阱。您可以创建名为 **enable-traps** 的布尔变量，且最初将其设为 TRUE。然后，如果需要关闭陷阱，只需编辑变量、将其更改为 FALSE、保存该对象，然后重新部署配置。命令序列可能如下所示：

```
snmp-server enable
snmp-server host inside 192.168.1.5
snmp-server community clearTextString
{{#enable-traps}}
snmp-server enable traps all
{{/enable-traps}}
```

还可根据对象内的布尔值执行此类处理。例如，您可以在接口上配置某些特性之前检查该接口是否仅限于管理。在下例中，`int-inside` 是指向名为 `inside` 的接口的接口变量。仅当并未将接口设为仅限于管理时，FlexConfig 才可在该接口上配置 EIGRP 相关接口选项。可使用反向部分，以便仅在布尔值为 `FALSE` 时才配置命令。

```
router eigrp 2
 network 192.168.1.0 255.255.255.0
 {{^int-inside.managementOnly}}
 interface {{int-inside.hardwareName}}
  hello interval eigrp 2 60
  delay 200
 {{/int-inside.managementOnly}}
```

在 FlexConfig 对象中引用 Smart CLI 对象

创建 FlexConfig 对象时，您可以使用变量指向可以在 Firepower 设备管理器中配置的对象。例如，您可以创建指向接口元素或网络对象的变量。

但是，不能以相同的方式指向智能 CLI 对象。

相反，如果您创建需要在 FlexConfig 策略中使用的 Smart CLI 对象，只需在适当的位置输入 Smart CLI 对象的名称。

例如，配置协议检测时，您可能想将扩展访问列表用作流量类。由于扩展访问列表具有 Smart CLI 对象，您需要使用 Smart CLI 对象来创建 ACL：不能在 FlexConfig 对象中使用 `access-list` 命令。

例如，如果您要在网络 192.168.1.0/24 和 192.168.2.0/24 之间全局启用 DCERPC 检测，应执行以下操作。

过程

步骤 1 为两个网络创建单独的网络对象。例如，`InsideNetwork` 和 `dmz-network`。

步骤 2 在 Smart CLI 扩展访问列表对象中使用这些对象。

Name	Description
dcerpc_class	

CLI Template

Extended Access List

Template

```

1  access-list dcerpc_class extended
2  configure access-list-entry permit
3  permit network source [ InsideNetworkx ] destination [ dmz-networkx ]
4  configure permit port any
5  permit port source ANY destination ANY
6  configure logging default
7  default log set log-level INFORMATIONAL log-interval 300

```

步骤 3 创建按名称指向 Smart CLI 对象的 FlexConfig 对象。

例如，如果为对象命名"dcerpc_class"，FlexConfig 对象应如下所示。请注意，在取消模板中，不对通过 Smart CLI 对象创建的访问列表求反，因为该对象实际上并非通过 FlexConfig 创建。

Template

```

1  class-map dcerpc_inspection
2  match access-list dcerpc_class
3  policy-map global_policy
4  class dcerpc_inspection
5  inspect dcerpc

```

Negate Template

```

1  policy-map global_policy
2  no class dcerpc_inspection
3  no class-map dcerpc_inspection

```

步骤 4 将对象添加到 FlexConfig 策略中。

配置密钥对象

密钥对象的重点在于隐藏密码或敏感字符串。如果不希望冒险让人看到 FlexConfig 对象或 Smart CLI 模板中使用的字符串，请为该字符串创建一个密钥对象。

过程

步骤 1 选择对象，然后从目录中选择密钥。

步骤 2 执行以下操作之一：

- 要创建对象，请点击 + 按钮。
- 要编辑对象，请点击该对象的编辑图标 (🔗)。

要删除未引用的对象，请点击该对象的垃圾桶图标 (🗑️)。

步骤 3 输入对象的名称和描述（后者为可选项）。

步骤 4 在密码字段和确认密码字段中输入密码或其他密钥字符串。

键入时系统会隐藏文本。

步骤 5 点击确定。

下一步做什么

- 如果是一个新对象，要在 FlexConfig 中使用该对象，请编辑 FlexConfig 对象，创建一个密钥类型变量，再选择该对象。然后，引用对象正文中的变量。有关详细信息，请参阅[在 FlexConfig 对象中创建变量](#)，第 514 页。
- 如要编辑作为 FlexConfig 策略一部分在 FlexConfig 对象中使用的现有对象，则需要部署配置，以使用新字符串更新设备。
- 在 Smart CLI 模板中，如果命令需要密钥，则在编辑相关属性时将会看到这些对象的列表。选择用于此用途的正确密钥。

FlexConfig 策略故障排除

编辑 FlexConfig 策略后，仔细检查下一部署的结果。如果您在“待处理更改”对话框中收到“上次部署失败”消息，请点击[查看详细信息](#)链接。链接将转至审核日志，您可以在其中找到失败的部署作业。打开作业，查找特定错误消息。

如果由于 FlexConfig 问题部署失败，则详细信息将提及带有错误命令的 FlexConfig 对象，并显示失败的命令。使用此信息更正对象并再次尝试部署。对象名称是一个链接，点击打开对象的编辑对话框。

例如，您可能需要配置最大 TCP 段大小 (TCP MSS)。您可以使用 `sysopt connection tcpmss` 命令控制此设置。通过 Firepower 设备管理器配置时，此选项的 Firepower 威胁防御默认值为 0，而 ASA 默认值为 1380。

ASA 默认值是在使用 1500 默认 MTU 的接口上运行 IPv4 VPN 时的最佳处理。系统需要 120 个字节用于 VPN 报头。对于 IPv6，系统需要 140 个字节。Firepower 威胁防御默认值为 0，仅允许终端协

商 MSS，这是正常流量的理想设置，尤其是在设备接口上使用不同 MTU（包括超过 1500 的 MTU）的情况下。由于 TCP MSS 是一个全局设置而不是根据接口，所以仅当流量中很大一部分通过 VPN，且获得过多分段时，才可对其进行更改。在这种情况下，可将 TCP MSS 设为 MTU - 120（适用于 IPv4）或 MTU - 140（适用于 IPv6），并将同一 MTU 用于所有接口。

为了说明这个问题，现在假设需要将 TCP MSS 设为 3 个字节。该命令需要取 48 个字节作为最小值，因此，您会得到类似于以下内容的部署错误：

Deployment Failed: User (admin) Triggered Deployment

- “Template” field of `sysopt-connection-tcpms` caused an error. ERROR: [3] is smaller than minimum allowed MSS of 48 by RFC 791 Config Error - `sysopt connection tcpms 3`

```
sysopt connection tcpms 3
```

错误由这些元素组成：

- 部署错误消息，其中包括导致错误的 FlexConfig 对象的名称。对象名称链接到编辑对话框，以便可快速打开对象更正错误。这是消息的第一句。
- 以“ERROR:”开头的文本是从设备返回的消息。在键入错误命令但不格式化 SSH 客户端的情况下，ASA 就会做出这种响应。在本例中，错误消息是“ERROR: [3] 小于 RFC 791 允许的最小 MSS 值 48”。以“Config Error”开头的文本会提及生成错误信息的特定行。
- 黑色文本是实际导致错误的 FlexConfig 对象行。必须修复此行。在本例中，如果尝试在 MTU 1500 接口上（常见情况）容纳 IPv4 VPN 流量，则应将 3 改为 1380。

修复本例时，可保持打开 CLI 控制台并使用 `show running-config all sysopt` 查看所有 `sysopt` 命令设置。多数 `sysopt` 命令均具有适用于多数用途的默认设置，因此，不会出现在运行配置中。`all` 关键字包括输出中的这些默认设置。

FlexConfig 示例

以下主题介绍使用 FlexConfig 配置功能的一些示例。

如何启用和禁用默认全局检测

某些协议在用户数据包中嵌入 IP 寻址信息，或在动态分配的端口上打开辅助信道。这些协议需要系统执行深度数据包检测，以便应用 NAT，并允许辅助信道。默认情况下，系统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或禁用默认检测。

要查看当前已启用的检测列表，请在 CLI 控制台或 SSH 会话中使用 `show running-config policy-map` 命令。以下是此命令在尚未更改检测配置的系统上运行的情况。在此输出中，输出末尾的 `inspect` 命令列表显示启用了哪些协议检测。上述命令在 `inspection_default` 流量类上启用这些检测（这是常规协议以及被检查协议的端口号，如果适用）。此类是 `global_policy` 策略映射的一部分，该映射使用未在输出中显示的服务策略命令将这些检测应用到所有接口。例如，在通过设备的所有 ICMP 流量上执行 ICMP 检查。

```
> show running-config policy-map
```

```

!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
    inspect ip-options
    inspect icmp
    inspect icmp error
!

```



注释 有关每个检测的讨论，请参阅《思科 ASA 系列防火墙配置指南》，网址为 <https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html>。

以下过程介绍如何启用或禁用此全局应用默认检测类中的检测。为便于解释，在本例中：

- 启用 PPTP（点对点隧道协议）。此协议用于在终端之间创建点对点连接。
- 禁用 SIP（会话发起协议）。通常仅当检测引发网络问题时，才会禁用 SIP。但是，如果禁用 SIP，必须确保访问控制策略允许 SIP 流量 (UDP/TCP 5060) 和任何动态分配的端口，而且，您无需为 SIP 连接提供 NAT 支持。通过标准页面而不是 FlexConfig 相应地调整访问控制和 NAT 策略。

开始之前

良好的规划可帮助您有效地使用 FlexConfig。在本示例中，我们要更改两个不同的不相关检测，尽管我们在同一流量类中进行更改。如果您需要更改这些策略，很可能需要单独执行此操作。

因此，我们建议在本示例中为每项检测创建单独的 FlexConfig 对象。通过这种方式，您可以轻松更改一项检测的设置，无需更改另一项检测的设置，也无需编辑 FlexConfig 对象。

过程

步骤 1 在设备 > 高级配置中点击查看配置。

步骤 2 在“高级配置”目录中依次点击 FlexConfig > FlexConfig 对象。

步骤 3 创建要启用 PPTP 检测的对象。

- a) 点击 + 按钮以创建新的对象。
- b) 为对象输入名称。例如，**Enable_PPTP_Global_Inspection**。
- c) 在模板编辑器中，输入以下命令，包括缩进。

```
policy-map global_policy
  class inspection_default
    inspect pptp
```

- d) 在取消模板编辑器中，输入撤消此配置所需的命令。

正如要让命令启用模板需要添加父命令以进入正确的子模式那样，您也需要在取消模板中添加这些命令。

取消模板将在您从 FlexConfig 策略删除此对象（部署成功后删除）时，以及不成功的部署期间应用（将配置重置为之前的状态）。

因此，在本示例中，取消模板为：

```
policy-map global_policy
  class inspection_default
    no inspect pptp
```

该对象应如下所示：

Name

Enable_PPTP_Global_Inspection

Description


Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

```
1 policy-map global_policy
2   class inspection_default
3     inspect pptp
```

Negate Template 

```
1 policy-map global_policy
2   class inspection_default
3     no inspect pptp
```

注释 由于 `inspection_default` 类启用了其他检测命令，您不想取消整个类。同样，`global_policy` 策略映射包括这些其他检测，而您也不想否定策略映射。

e) 点击**确定**保存对象。

步骤 4 创建要禁用 SIP 检查的对象。

- a) 点击 **+** 按钮以创建新的对象。
- b) 为对象输入名称。例如，**Disable_SIP_Global_Inspection**。
- c) 在**模板编辑器**中，输入以下命令，包括缩进。

```
policy-map global_policy
  class inspection_default
    no inspect sip
```

d) 在**取消模板编辑器**中，输入撤消此配置所需的命令。

禁用“no”命令的“否定”命令是启用功能的命令。因此，“取消”模板不仅仅是禁用某项功能的命令，它是“肯定”模板中所执行任何命令的反向命令。取消模板的实质是撤消所做的更改。

因此，在本示例中，取消模板为：

```
policy-map global_policy
  class inspection_default
    inspect sip
```

该对象应如下所示：

Name

Disable_SIP_Global_Inspection

Description

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

```

1  policy-map global_policy
2  class inspection_default
3    no inspect sip

```

Negate Template 

```

1  policy-map global_policy
2  class inspection_default
3    inspect sip

```

e) 点击**确定**保存对象。

步骤 5 将对象添加到 FlexConfig 策略中。


仅创建对象远远不够。仅当您将对象添加到 FlexConfig 策略（并保存所做的更改）时，才部署对象。这样，您可以在对象上试验（可部分完成），不必担心会在未完成的作业上失败。您可以通过添加和删除对象轻松打开或关闭功能：无需每次都重新创建对象。

- 点击目录中的 **FlexConfig 策略**。
- 在组列表中点击 +。
- 选择 Enable_PPTP_Global_Inspection 和 Disable_SIP_Global_Inspection 对象，然后点击**确定**。

组列表应如下所示：

FlexConfig Policy

Group List

+ 

> 1. Enable_PPTP_Global_Inspection

> 2. Disable_SIP_Global_Inspection

系统应随即使用模板中的命令更新预览。验证您是否看到预期的命令。

```
Preview
1 policy-map global_policy
2   class inspection_default
3     inspect pptp
4 policy-map global_policy
5   class inspection_default
6     no inspect sip
```

d) 点击保存。

您现在可以部署策略。

步骤 6 确认您的更改。

a) 点击网页右上角的部署更改图标。



b) 点击立即部署按钮。

您可以等待部署完成，也可以点击确定，稍后再检查任务列表或部署历史记录。

步骤 7 在 CLI 控制台或 SSH 会话中，使用 **show running-config policy-map** 命令并验证运行配置是否具有正确的更改。

请注意，在以下输出中，**inspect pptp** 已添加到 **inspection_default** 类的底部，而 **inspect sip** 在类中不再存在。这表示您已成功部署 FlexConfig 对象中定义的更改。

```
> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect netbios
    inspect tftp
    inspect ip-options
    inspect icmp
    inspect icmp error
```



```
inspect pptp
!
```

如何撤消 FlexConfig 更改

如果您在 FlexConfig 对象中输入正确的取消模板，删除使用该对象所做的更改非常简单。只需从 FlexConfig 策略中删除该对象，下一个部署时，系统即可使用取消模板撤消所做的更改。

您不需要创建新对象来撤消所做的更改。

以下示例展示如何重新启用全局 SIP 检测。该示例将恢复[如何启用和禁用默认全局检测](#)，第 523 页中所述的更改，此部分已禁用 SIP 检测。

开始之前

验证 FlexConfig 对象是否具有正确的取消模板。如果没有，请编辑对象更正取消模板。

过程

步骤 1 在设备 > 高级配置中点击查看配置。

步骤 2 在“高级配置”目录中依次点击 **FlexConfig** > **FlexConfig 策略**。

步骤 3 点击 FlexConfig 策略中 **Disable_SIP_Global_Inspection** 对象条目右侧的 **X**，将其从策略中删除。



预览中将删除该对象中的命令。取消命令不会添加到预览，而是在后台执行。

步骤 4 点击保存。

步骤 5 确认您的更改。

a) 点击网页右上角的部署更改图标。



b) 点击立即部署按钮。

您可以等待部署完成，也可以点击确定，稍后再检查任务列表或部署历史记录。

步骤 6 在 CLI 控制台或 SSH 会话中，使用 **show running-config policy-map** 命令并验证运行配置是否具有正确的更改。

请注意，在以下输出中，**inspect sip** 已添加到 **inspection_default** 类的底部。这表示已成功部署 FlexConfig 对象中定义的更改。（顺序在此类中不重要，因此，**inspect sip** 在末尾，而不在其原始位置并不重要。）

```

> show running-config policy-map
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    no tcp-inspection
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect rtsp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect netbios
    inspect tftp
    inspect ip-options
    inspect icmp
    inspect icmp error
    inspect pptp
    inspect sip
!

```

如何启用唯一流量类检测

在本示例中，我们将对特定接口上两个终端之间的流量启用 PPTP 检测。此检测仅面向两者之间配置点到点隧道的终端。

启用 2 个终端之间 PPTP 检测所需的 CLI 涉及以下要素：

1. 源和目标设置为终端主机 IP 地址的 ACL。
2. 引用此 ACL 的流量类。
3. 包含流量类，并在该流量类上启用 PPTP 检测的策略映射。
4. 将策略映射应用到所需接口的服务策略。此步骤实际上是激活策略并启用检测的操作。



注释 有关与检测相关的服务策略的详细讨论，请参阅《思科 ASA 系列防火墙配置指南》，网址为：
<https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html>。

过程

- 步骤 1 在设备 > 高级配置中点击查看配置。
- 步骤 2 在“高级配置”目录中依次点击 **FlexConfig > FlexConfig** 对象。
- 步骤 3 点击 + 按钮以创建新的对象。
- 步骤 4 为对象输入名称。例如，**Enable_PPTP_Inspection_on_Interface**。
- 步骤 5 为内部接口添加一个变量。
 - a) 点击变量列表上方的 +。
 - b) 输入变量的名称，例如 **pptp-if**。
 - c) 对于类型，请选择接口。
 - d) 对于值，请选择内部接口。

对话框应如下所示：

- e) 点击添加。

- 步骤 6 在模板编辑器中，输入以下命令，包括缩进。

```
access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
class-map MATCH_CMAP
  match access-list MATCH_ACL
policy-map PPTP_POLICY
  class MATCH_CMAP
    inspect pptp
service-policy PPTP_POLICY interface {{pptp-if.name}}
```

请注意，要使用变量，请在双括号中键入变量名称。此外，您还需要使用圆点表示法来选择您想要检索的属性，因为定义接口的对象具有许多属性。由于接口名称保存在“name”属性中，输入 **{{pptp-if.name}}** 将为接口检索分配给变量的名称属性的值如果您需要更改执行 PPTP 检测的接口，只需选择变量定义中的其他接口。

- 步骤 7 在取消模板编辑器中，输入撤消此配置所需的命令。

对于本示例中，我们将假设类映射、策略映射和服务策略仅用于应用 PPTP 检测目的。因此，在取消模板中，我们想要删除所有这些要素。

但是，如果您将 PPTP 检测实际添加到接口上的现有服务策略，不需要对策略映射或服务策略求反。您可以从策略映射对类求反，或仅在策略映射的类中关闭检测。您需要清楚了解您在其他 FlexConfig 对象中实施的策略，确保取消模板不会产生意外的后果。

删除嵌套项目时，您需要按照与项目创建顺序相反的顺序执行删除。因此，您需要先删除服务策略，最后再删除访问列表。否则，您将尝试删除正在使用的对象，而系统将返回错误，不允许您执行此操作。

```
no service-policy PPTP_POLICY interface {{pntp-if.name}}
no policy-map PPTP_POLICY
no class-map MATCH_CMAP
no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```


该对象应如下所示：

Name

Enable_PPTP_Inspection_on_Interface

Description

Variables +

NAME	TYPE	VALUE	DESCRIPTION	ACTIONS
pntp-if	Interface	 inside		

Template Expand | Reset

```

1 access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
2 class-map MATCH_CMAP
3   match access-list MATCH_ACL
4 policy-map PPTP_POLICY
5   class MATCH_CMAP
6   inspect pntp
7 service-policy PPTP_POLICY interface {{pntp-if.name}}
```

Negate Template Expand | Reset

```

1 no service-policy PPTP_POLICY interface {{pntp-if.name}}
2 no policy-map PPTP_POLICY
3 no class-map MATCH_CMAP
4 no access-list MATCH_ACL permit ip host 192.168.1.55 host 198.51.100.1
```

步骤 8 点击**确定**保存对象。

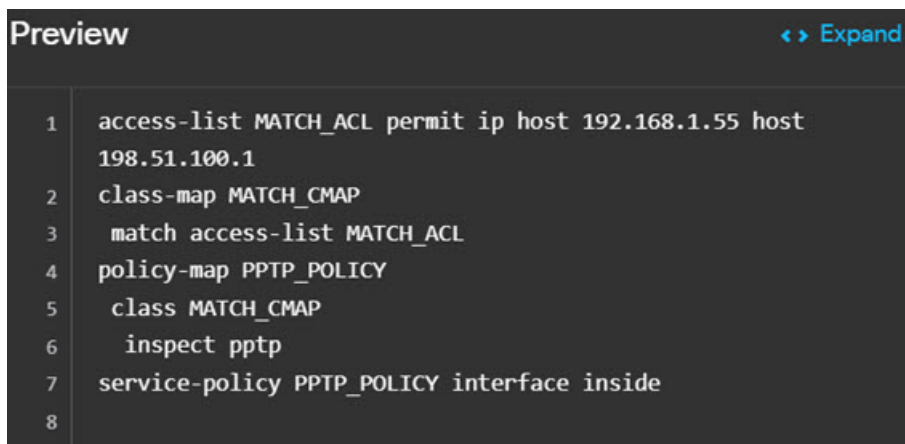
步骤 9 将对象添加到 FlexConfig 策略中。

- a) 点击目录中的 **FlexConfig 策略**。
- b) 在组列表中点击 **+**。
- c) 选择 **Enable_PPTP_Inspection_on_Interface** 对象，然后点击**确定**。

组列表应如下所示：



系统应随即使用模板中的命令更新预览。验证您是否看到下图所示的预期命令。请注意，接口变量在预览中解析为名称“inside”。需要特别注意变量：如果在预览中解析不正确，它们将不能正确部署。编辑 FlexConfig 对象，直到可以在预览中获得正确的变量转换。



- d) 点击**保存**。

您现在可以部署策略。

步骤 10 确认您的更改。

- a) 点击网页右上角的**部署更改**图标。



- b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 11 在 CLI 控制台或 SSH 会话中，使用 **show running-config** 命令的变体并验证运行配置是否具有正确的更改。

您可以输入 **show running-config** 检查整个 CLI 配置，也可以使用以下命令验证此配置的每个部分：

- **show running-config access-list MATCH_ACL** 验证 ACL。
- **show running-config class** 验证类映射。此命令将显示所有类映射。
- **show running-config policy-map PPTP_POLICY** 验证类和策略映射配置。
- **show running-config service-policy** 验证应用于接口的策略映射。这将显示所有服务策略。

以下输出显示该序列命令，您可以看到配置已正确应用。

```
> show running-config access-list MATCH_ACL
access-list MATCH_ACL extended permit ip host 192.168.1.55 host 198.51.100.1

> show running-config class
!
class-map MATCH_CMAP
  match access-list MATCH_ACL
class-map inspection_default
  match default-inspection-traffic
!

> show running-config policy-map PPTP_POLICY
!
policy-map PPTP_POLICY
  class MATCH_CMAP
    inspect pptp
!

> show running-config service-policy
service-policy global_policy global
service-policy PPTP_POLICY interface inside
```

如何在 ISA 3000 上启用硬件绕行

您可以启用硬件绕行，使流量在断电期间继续在接口对之间流动。支持的接口对为铜缆接口 GigabitEthernet 1/1 和 1/2 以及 GigabitEthernet 1/3 和 1/4。如果您使用的是光纤以太网型号，则只有铜缆以太网对（GigabitEthernet 1/1 和 1/2）支持硬件绕行。

启用硬件绕行时，流量将在这些接口对之间的第 1 层传递。在 FDM 和 FTD CLI 中都可以看到接口处于关闭状态。不使用防火墙功能，因此请确保您了解允许流量通过设备的风险。

此外，流量不会在任何其他接口对之间通过，且这些接口之间的任何现有连接被丢弃。

我们建议您禁用 TCP 序列号随机化（如本过程中所述）。默认情况下，ISA 3000 会将通过其的 TCP 连接的初始序列号 (ISN) 重写为随机编号。硬件绕行激活后，ISA 3000 不再位于数据路径中，也不再转换序列号。接收客户端会收到意外序列号，并丢弃连接，因此需要重新建立 TCP 会话。即便禁用 TCP 序列号随机化后，某些 TCP 连接将也需要重新建立，因为链路在切换期间会临时关闭。

开始之前

要使用硬件绕行：

- 必须将接口对放在同一桥接组内。
- 必须将接口连接到交换机的接入端口。不能将它们连接到中继端口。

以下过程介绍如何对电源故障设置自动硬件绕行。您也可以通过在 FlexConfig 策略中部署以下命令，手动启动硬件绕行：

hardware-bypass manual GigabitEthernet {1/1-1/2 | 1/3-1/4 }

然后，您需要部署命令的 **no** 形式禁用硬件旁路。

例如，要在 1/1-1/2 对上手动启动硬件绕行，并随后将其禁用，请单独部署以下命令：

```
hardware-bypass manual GigabitEthernet 1/1-1/2
no hardware-bypass manual GigabitEthernet 1/1-1/2
```

手动启用/禁用硬件绕行时，您将看到以下系统日志消息，其中对为 1/1-1/2 或 1/3-1/4。

- %Asa-6-803002: 系统不对通过 GigabitEthernet 对的流量提供保护
- %Asa-6-803003: 用户已手动在 GigabitEthernet 对上禁用绕行

过程

- 步骤 1** 在设备 > 高级配置中点击查看配置。
- 步骤 2** 在“高级配置”目录中依次点击 **FlexConfig > FlexConfig** 对象。
- 步骤 3** 点击 + 按钮以创建新的对象。
- 步骤 4** 为对象输入名称。例如，**Enable_Hardware_Bypass**。
- 步骤 5** 在模板编辑器中，启用硬件绕行。

hardware-bypass GigabitEthernet {1/1-1/2 | 1/3-1/4 } [sticky]

您可以输入命令两次，以在每个可能的接口上启用硬件绕行。例如：

```
hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4
```

可选的 **sticky** 关键字会在电源恢复和系统启动后使设备保持处于硬件旁路模式。在这种情况下，您需要在准备就绪后手动关闭硬件旁路。此选项允许您控制何时短暂中断流量。

- 步骤 6** （可选。）输入命令以禁用 TCP 序列号随机化。

命令是 **set connection random-sequence-number disable**，但您必须为策略映射中的特定类配置此命令。到目前为止，最简单的方法是全局禁用随机序列号，这需要以下命令：

```
policy-map global_policy
class default_class
set connection random-sequence-number disable
```

步骤 7 在取消模板编辑器中，输入撤消此配置所需的命令。

例如，如果您要在两个接口对上启用硬件绕行，同时全局禁用 TCP 序列号随机化，取消模板应为：

```
no hardware-bypass GigabitEthernet 1/1-1/2
no hardware-bypass GigabitEthernet 1/3-1/4
policy-map global_policy
 class default_class
  set connection random-sequence-number enable
```

步骤 8 点击**确定**保存对象。

步骤 9 将对象添加到 FlexConfig 策略中。

- a) 点击目录中的 **FlexConfig 策略**。
- b) 在组列表中点击 +。
- c) 选择 **Enable_Hardware_Bypass** 对象，然后点击**确定**。

系统应随即使使用模板中的命令更新预览。验证您是否看到预期的命令。

- d) 点击**保存**。

您现在可以部署策略。

步骤 10 确认您的更改。

- a) 点击网页右上角的**部署更改**图标。



- b) 点击**立即部署**按钮。

您可以等待部署完成，也可以点击**确定**，稍后再检查任务列表或部署历史记录。

步骤 11 在 CLI 控制台或 SSH 会话中，使用 **show running-config** 命令并验证运行配置是否具有正确的更改。

使用 **show hardware-bypass** 命令监控运行状态。
