配置并运行FTD预过滤器策略

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- 预过滤器策略使用案例1
- 要点
- 预过滤器策略使用案例2

任务 1：验证默认预过滤器策略

- 任务要求
- 解决方案
- CLI(LINA)验证

任务 2：使用标记阻止隧道流量

- 任务要求
- 解决方案

确认

任务 3：使用快速路径预过滤器规则绕过Snort引擎

- 任务要求
- 解决方案

验证

故障排除

相关信息

简介

本文档介绍Firepower威胁防御(FTD)预过滤器策略的配置和操作。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行FTD代码6.1.0-195的ASA5506X
- 两台运行15.2映像的3925 Cisco IOS®路由器
- 运行6.1.0-195的FireSIGHT管理中心(FMC)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

预过滤器策略是版本6.1中引入的一项功能，主要有三个用途：

1. 根据内部报头和外部报头匹配流量。
2. 提供早期访问控制，允许流量完全绕过Snort引擎。
3. 用作从自适应安全设备(ASA)迁移工具迁移的访问控制条目(ACE)的占位符。

配置

预过滤器策略使用案例1

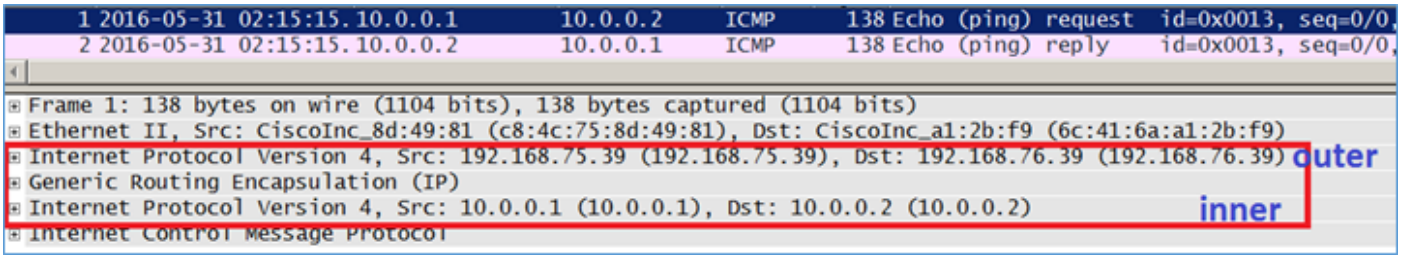
预过滤器策略可以使用允许FTD根据内部和/或外部IP报头隧道流量进行过滤的隧道规则类型。在撰写本文时，隧道流量是指：

- IP-in-IP
- IPv6-in-IP
- Teredo 端口 3544
- 通用路由封装 (GRE)

考虑如图所示的GRE隧道：



当您使用GRE隧道从R1 ping R2时，流量会通过防火墙：



如果防火墙是ASA设备，它会检查外部IP报头：

L2 Header	Outer IP Header src=192.168.75.39 dst=192.168.76.39	GRE Header	Inner IP Header src=10.0.0.1 dst=10.0.0.2	L7

<#root>

ASA#

show conn

GRE OUTSIDE 192.168.76.39:0 INSIDE 192.168.75.39:0

, idle 0:00:17, bytes 520, flags

如果防火墙是FirePOWER设备，它会检查内部IP报头：

L2 Header	Outer IP Header src=192.168.75.39 dst=192.168.76.39	GRE Header	Inner IP Header src=10.0.0.1 dst=10.0.0.2	L7

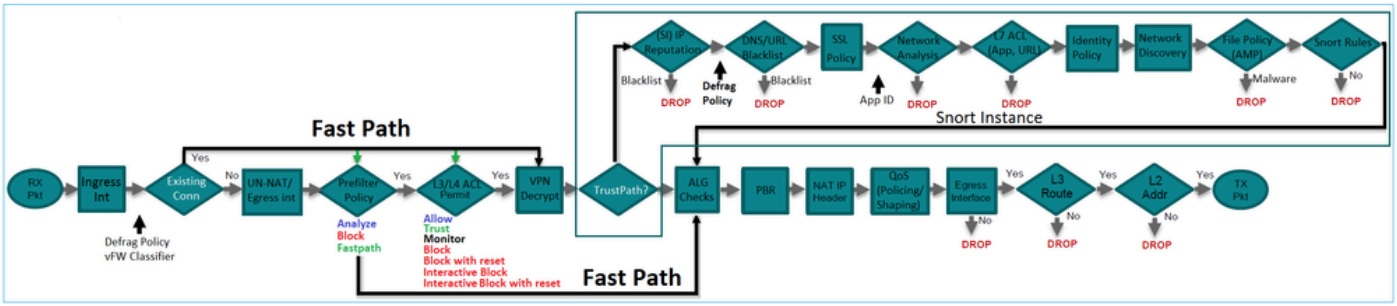
使用预过滤器策略，FTD设备可以根据内部报头和外部报头匹配流量。

要点

设备	检查
ASA	外部IP
Snort	内部IP
FTD	外部（预过滤器）+内部IP(访问控制策略(ACP))

预过滤器策略使用案例2

预过滤器策略可以使用可以提供早期访问控制并允许流完全绕过Snort引擎的预过滤器规则类型：



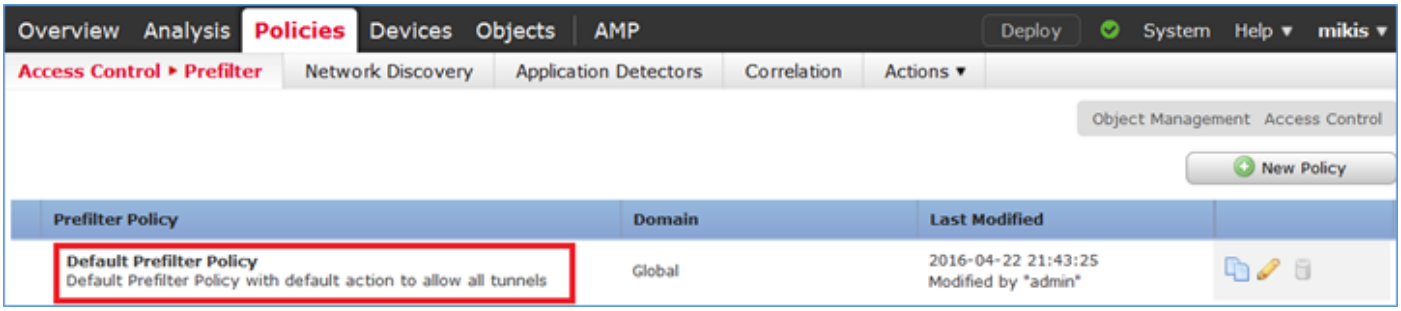
任务 1：验证默认预过滤器策略

任务要求

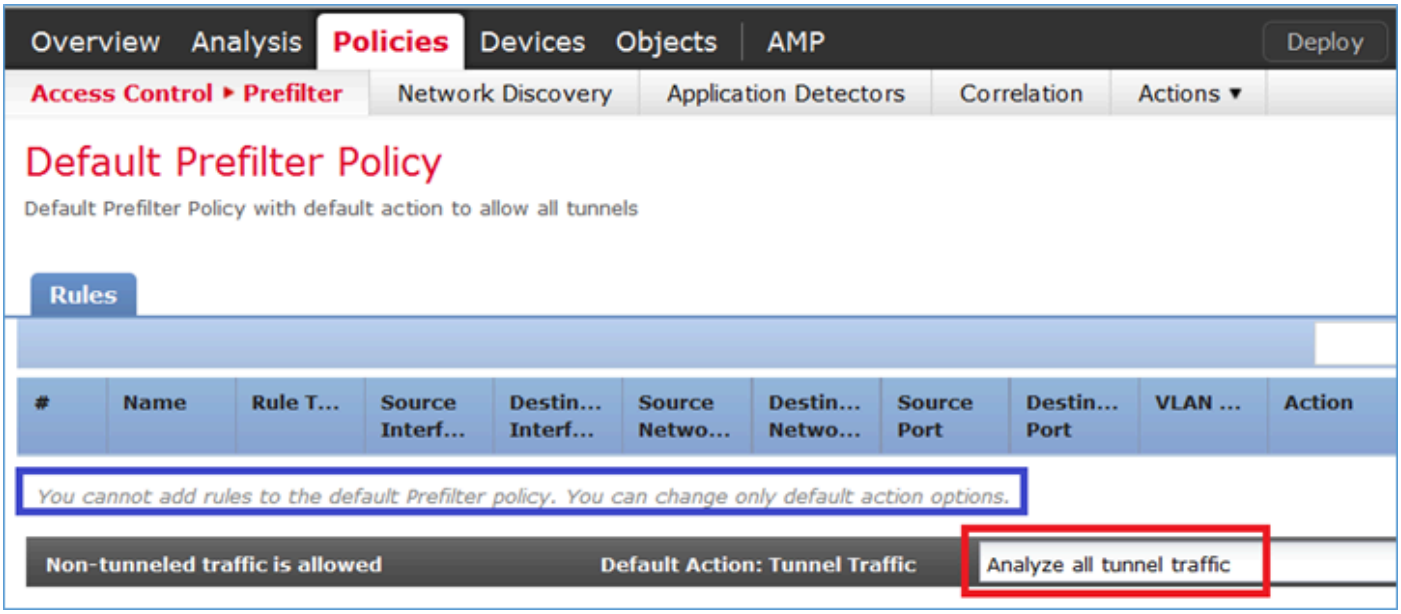
验证默认预过滤器策略。

解决方案

1.定位至策略>访问控制>预过滤器。在本示例中，默认预过滤器策略已存在：



2.选择Edit以查看策略设置：



3.预过滤器策略已附加到访问控制策略：



CLI(LINA)验证

预过滤器规则添加在ACL的顶部：

<#root>

```
firepower#

show access-list

access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list CSM_FW_ACL_; 5 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998:

PREFILTER POLICY:

 Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=5) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any any eq 3544 rule-id 9998 (hitcnt=0) 0xcf6309bc
```

任务 2：使用标记阻止隧道流量

任务要求

阻止GRE隧道内通过隧道传输的ICMP流量。

解决方案

1.如果应用这些ACP，您可以看到Internet控制消息协议(ICMP)流量被阻止，即使它是否通过GRE隧道也是如此：



<#root>

R1#

ping 192.168.76.39

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:

.....

Success rate is 0 percent (0/5)

<#root>

R1#

ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)

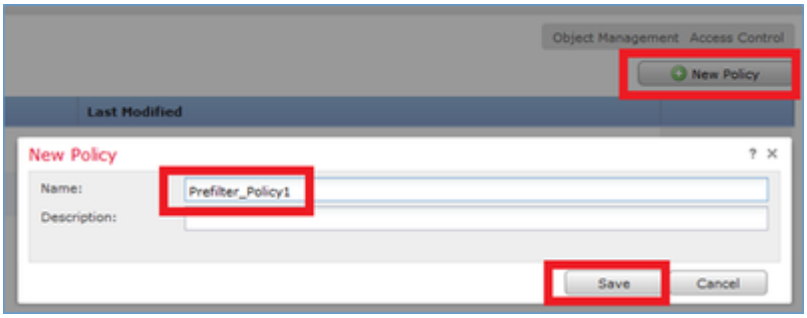
在本例中，您可以使用预过滤器策略满足任务要求。其逻辑如下：

- 标记封装在GRE中的所有数据包。
- 创建与标记的数据包匹配并阻止ICMP的访问控制策略。

从架构角度来看，根据LInux Natively(LINA)预过滤器规则检查数据包，然后Snort预过滤器规则和ACP，最后Snort指示LINA丢弃。第一个数据包通过FTD设备。

1.定义隧道流量的标记。

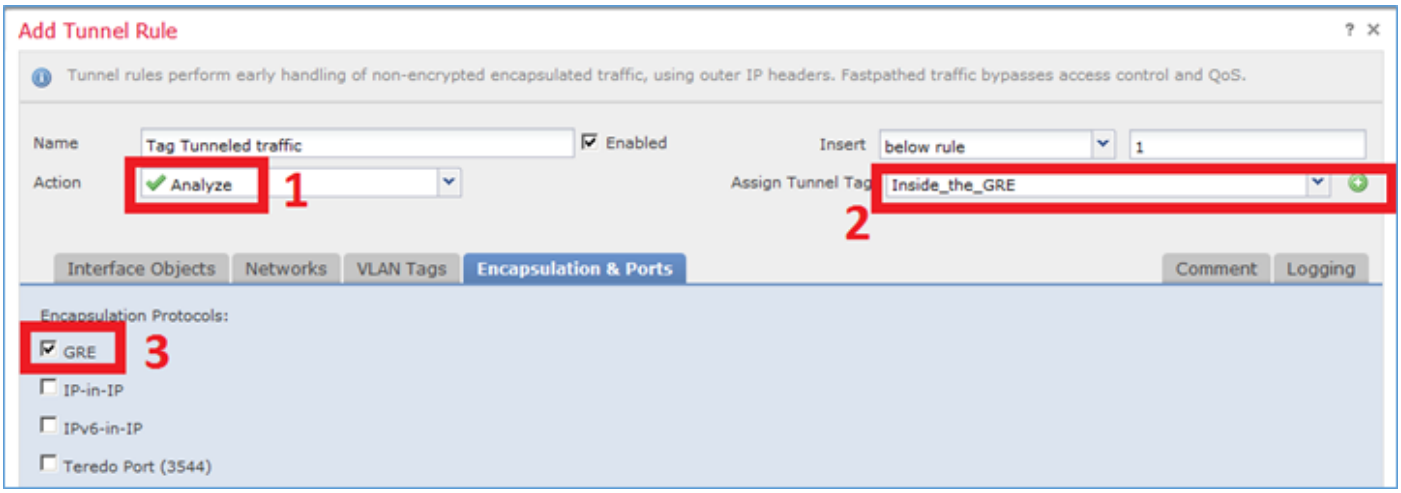
2.定位至策略>访问控制>预过滤器，然后创建新的预过滤器策略。请记住，默认预过滤器策略无法编辑：



在预过滤器策略中，定义两种类型的规则：

- 隧道规则
- 预过滤器规则

可以将这两个功能视为可在预过滤器策略中配置的完全不同的功能。对于此任务，需要定义隧道规则：。

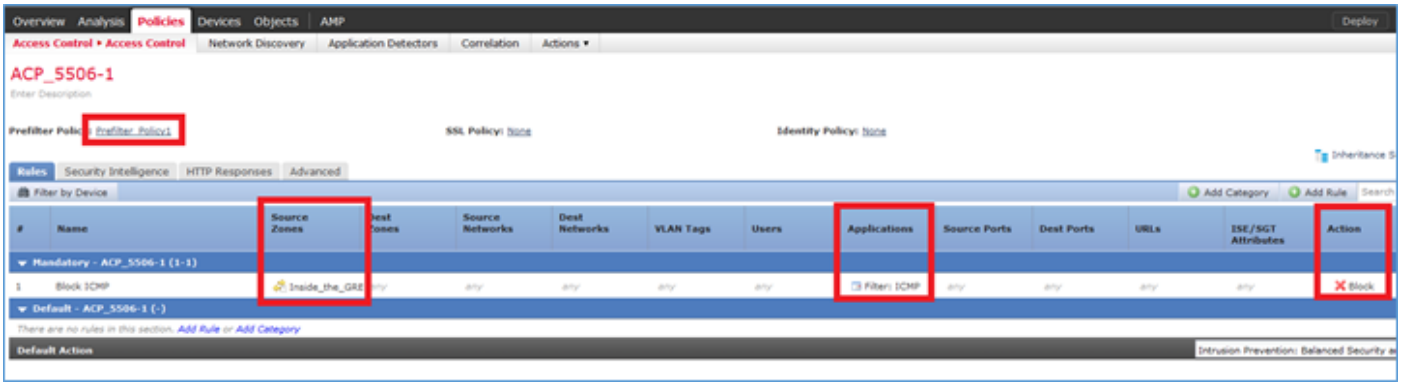


此表定义了操作，并提供了每个操作的简短说明：

操作	描述
分析	在LINA之后，Snort引擎会检查流量。或者，隧道标记可以分配给隧道流量。
阻止	流被LINA阻止。将检查外部报头。
快速路径	该流程仅由LINA处理，无需使用Snort引擎。

2.定义已标记流量的访问控制策略

- 虽然一开始并不十分直观，但隧道标记可由访问控制策略规则用作源区域。导航到Policies > Access Control并创建阻止标记流量的ICMP的规则：



注意：新的预过滤器策略已附加到访问控制策略。

确认

在LINA和CLISH上启用捕获：

<#root>

```
firepower#

show capture

capture CAPI type raw-data trace interface inside [Capturing - 152 bytes]
capture CAPO type raw-data trace interface outside [Capturing - 152 bytes]
```

<#root>

```
>

capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection?

1


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:

-n
```

从R1，尝试ping远程GRE隧道终端；ping失败：

<#root>

```
R1#

ping 10.0.0.2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)
```

CLISH捕获显示第一个通过FTD的回应请求，且应答被阻止：

<#root>

```
Options: -n
18:21:07.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo

18:21:07.759939 IP 192.168.76.39 > 192.168.75.39: GREv0, length 104: IP 10.0.0.2 > 10.0.0.1: ICMP echo r

18:21:09.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
18:21:11.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2: ICMP echo
```

LINA捕获证实了这一点：

<#root>

```
>

show capture CAPI | include ip-proto-47

 102: 18:21:07.767523  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 107: 18:21:09.763739  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 111: 18:21:11.763769  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 115: 18:21:13.763784  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 120: 18:21:15.763830  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
>
>

show capture CAPO | include ip-proto-47

  93: 18:21:07.768133  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104

  94: 18:21:07.768438  192.168.76.39 > 192.168.75.39:  ip-proto-47, length 104
```

启用CLISH firewall-engine-debug，清除LINA ASP丢弃计数器并完成相同测试。CLISH调试显示

，对于Echo-Request，您已匹配预过滤器规则，对于Echo-Reply，则显示ACP规则：

```
<#root>

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

New session

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

uses prefilter rule 268434441 with tunnel zone 1

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1, 

icmpType 8, icmpCode 0

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 pending rule order 3, 'Block ICMP', AppId
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

uses prefilter rule 268434441 with tunnel zone 1

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1 -> -1, 

icmpType 0, icmpCode 0

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0

match rule order 3, 'Block ICMP', action Block

10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 deny action
```

ASP丢弃显示Snort丢弃了数据包：

```
<#root>

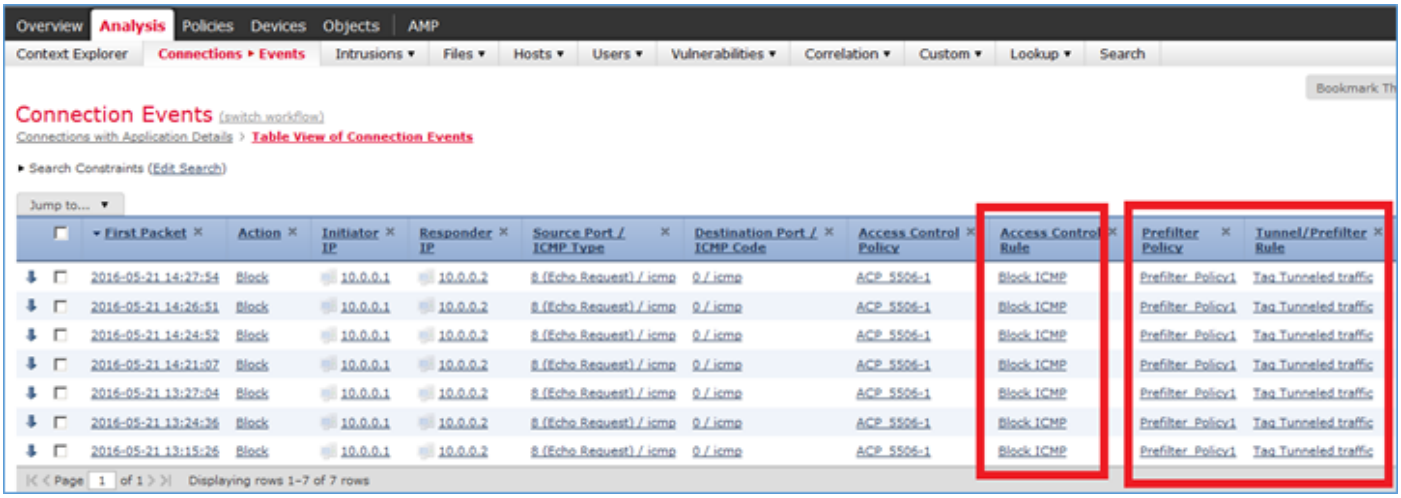
>

show asp drop


Frame drop:
  No route to host (no-route)                                   366
  Reverse-path verify failed (rpf-violated)                       2
  Flow is denied by configured rule (acl-drop)                    2

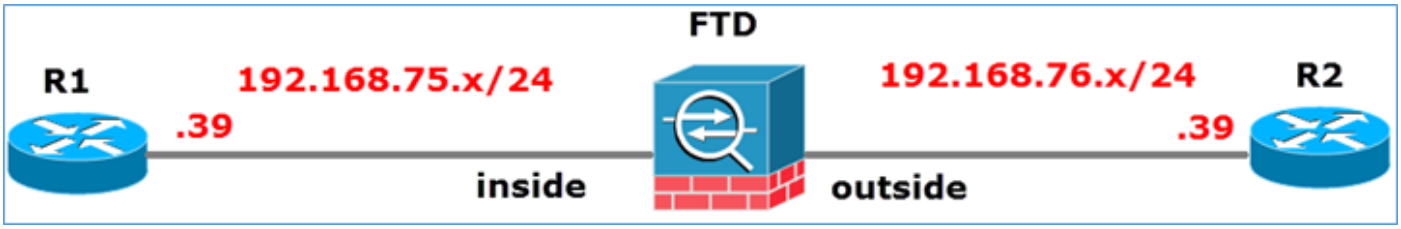

 Snort requested to drop the frame (snort-drop)                   5
```

在连接事件中，您可以看到匹配的预过滤器策略和规则：



任务 3：使用快速路径预过滤器规则旁路Snort引擎

网络图

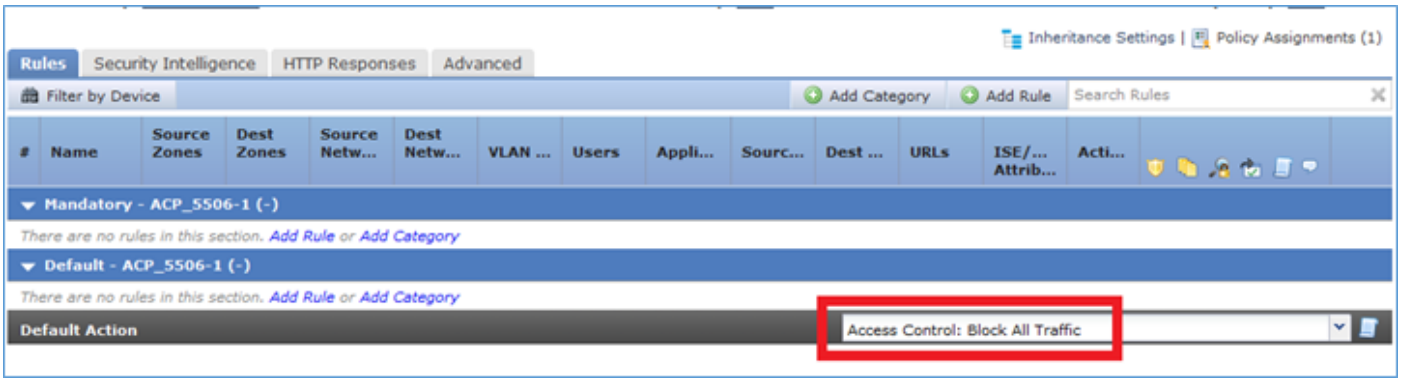


任务要求

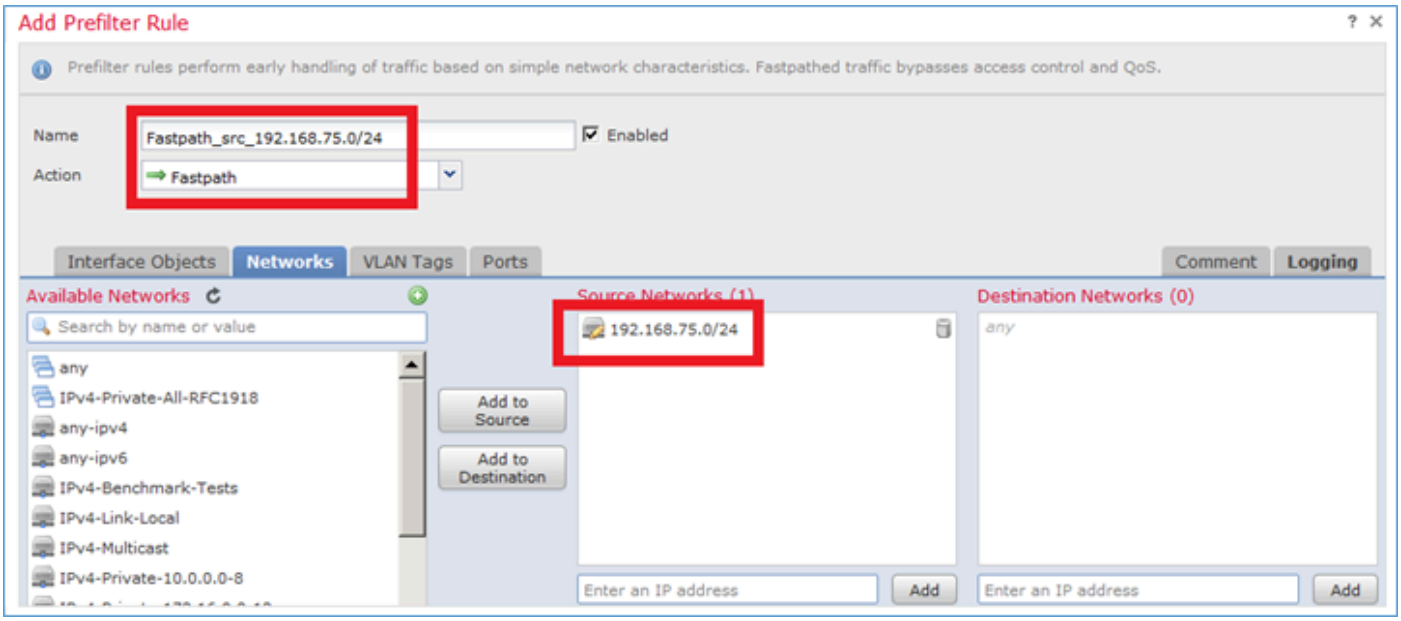
1. 删除当前的访问控制策略规则并添加阻止所有流量的访问控制策略规则。
2. 为来自192.168.75.0/24网络的流量配置绕过Snort引擎的预过滤器策略规则。

解决方案

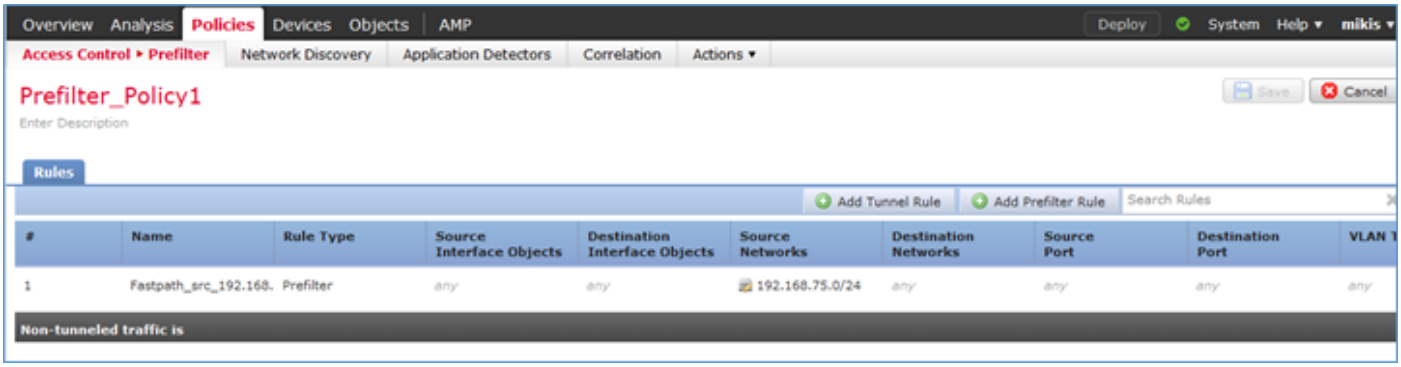
1.阻止所有流量的访问控制策略：



2.添加一个预过滤器规则，将Fastpath作为源网络192.168.75.0/24的操作：



3.结果显示在下一幅图像中：



4.保存和部署。

在两个FTD接口上启用带有跟踪的捕获：

<#root>

```
firepower#

capture CAPI int inside trace match icmp any any

firepower#

capture CAPO int outsid trace match icmp any any
```

尝试通过FTD从R1(192.168.75.39)ping R2(192.168.76.39);ping失败：

<#root>

```
R1#

ping 192.168.76.39

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:

.....
Success rate is 0 percent (0/5)
```

内部接口上的捕获显示：

<#root>

```
firepower#

show capture CAPI

5 packets captured

   1: 23:35:07.281738   192.168.75.39 > 192.168.76.39: icmp: echo request
   2: 23:35:09.278641   192.168.75.39 > 192.168.76.39: icmp: echo request
   3: 23:35:11.279251   192.168.75.39 > 192.168.76.39: icmp: echo request
```

```
   4: 23:35:13.278778   192.168.75.39 > 192.168.76.39: icmp: echo request
   5: 23:35:15.279282   192.168.75.39 > 192.168.76.39: icmp: echo request
5 packets shown
```

第一个数据包(echo-request)的跟踪显示（重要点突出显示）：

Spoiler（突出显示以便阅读）

firepower# show capture CAPI packet-number 1 trace

捕获了5个数据包

1:23:35:07.281738 192.168.75.39 > 192.168.76.39:icmp:回应请求

阶段：1

type：捕获

子类型：

结果：允许

Config :

其它信息：

MAC访问列表

阶段：2

type：访问列表

子类型：

结果：允许

Config :

隐式规则

其它信息：

MAC访问列表

阶段：3

type：路由查找

子类型：解析出口接口

结果：允许

Config :

其它信息：

发现下一跳192.168.76.39使用出口ifc outside

阶段：4

type：访问列表

子类型：日志

结果：允许

Config :

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log both

access-list CSM_FW_ACL_ remark rule-id 268434448:预过滤器策略：Prefilter_Policy1

access-list CSM_FW_ACL_ remark rule-id 268434448:规则：Fastpath_src_192.168.75.0/24

其它信息：

阶段：5

type：CONN设置

子类型：

结果：允许

Config :

class-map class-default

 match any

policy-map global_policy

 class class-default

  set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

其它信息：

阶段：6

type：NAT

子类型：每会话

结果：允许

Config :

其它信息：

阶段：7

type：IP选项

子类型：

结果：允许

Config :

其它信息：

阶段：8

type：检查

子类型：np-inspect

结果：允许

Config :

class-map inspection_default

 match default-inspection-traffic

policy-map global_policy

 class inspection_default

  inspect icmp

service-policy global_policy global

其它信息：

阶段：9

type：检查

子类型：np-inspect

结果：允许

Config :

其它信息：

阶段：10

type：NAT

子类型：每会话

结果：允许

Config :

其它信息：

阶段：11

type：IP选项

子类型：

结果：允许

Config :

其它信息：

阶段：12

type：流创建

子类型：

结果：允许

Config :

其它信息：

使用ID 52创建新流，将数据包分派到下一个模块

阶段：13

type：访问列表

子类型：日志

结果：允许

Config :

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log both

access-list CSM_FW_ACL_ remark rule-id 268434448:预过滤器策略：Prefilter_Policy1

access-list CSM_FW_ACL_ remark rule-id 268434448:规则：Fastpath_src_192.168.75.0/24

其它信息：

阶段：14

type：CONN设置

子类型：

结果：允许

Config :

class-map class-default

 match any

policy-map global_policy

 class class-default

  set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

其它信息：

阶段：15

type：NAT

子类型：每会话

结果：允许

Config :

其它信息：

阶段：16

type：IP选项

子类型：

结果：允许

Config :

其它信息：

阶段：17

type：路由查找

子类型：解析出口接口

结果：允许

Config :

其它信息：

发现下一跳192.168.76.39使用出口ifc outside

阶段：18

type：ADJACENCY-LOOKUP

子类型：下一跳和邻接关系

结果：允许

Config :

其它信息：

活动邻接关系

下一跳mac地址0004.deab.681b命中140372416161507

阶段：19

type：捕获

子类型：

结果：允许

Config :

其它信息：

MAC访问列表

结果：

输入接口：外部

输入状态： up

input-line-status: up

output-interface:外部

输出状态： up

output-line-status: up

操作：允许

1个数据包显示

firepower#

firepower# show capture CAPI packet-number 1 trace 5 packets captured 1:23:35:07.281738 192.168.75.39 > 192.168.76.39:icmp:回应请求阶段：1类型：捕获子类型：结果：允许配置：其它信息：MAC访问列表阶段：2类型：ACCESS-LIST子类型：结果：允许配置：隐式规则其他信息：MAC访问列表阶段：3类型：ROUTE-LOOKUP子类型：解析出口接口结果：允许配置：其它信息：发现下一跳192.168.76.39在阶段外使用出口ifc:4类型：ACCESS-LIST子类型：日志结果：允许配置：access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log both access-list CSM_FW_ACL_ remark rule-id 268434448:预过滤器策略：Prefilter_Policy1 access-list CSM_FW_ACL_remark rule-id 268434448:规则：Fastpath_src_192.168.75.0/24其他信息： 阶段：5类型：CONN-SETTINGS子类型：结果：允许配置：class-map class-default match any policy-map global_policy class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global其他信息： 阶段：6类型：NAT子类型：每会话结果：允许配置：其它信息： 阶段：7类型：IP-OPTIONS子类型：结果：允许配置：其它信息： 阶段：8类型：INSPECT子类型：np-inspect结果：允许配置：class-map inspection_default match default-inspection-traffic policy-map global_policy class inspection_default inspect icmp service-policy global_policy global其他信息：阶段：9类型：INSPECT子类型：np-inspect结果：允许配置：其它信息： 阶段：10类型：NAT子类型：每会话结果：允许配置：其它信息： 阶段：11类型：IP-OPTIONS子类型：结果：允许配置：其它信息： 阶段：12类型：FLOW-CREATION子类型：结果：允许配置：其它信息：使用ID 52创建新流，将数据包分派到下一模块阶段：13类型：ACCESS-LIST子类型：日志结果：允许配置：access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip 192.168.75.0 255.255.255.0 any rule-id 268434448 event-log both access-list CSM_FW_ACL_ remark rule-id 268434448:预过滤器策略：Prefilter_Policy1 access-list CSM_FW_ACL_remark rule-id 268434448:规则：Fastpath_src_192.168.75.0/24其他信息： 阶段：14类型：CONN-SETTINGS子类型：结果：允许配置：class-map class-default match any policy-map global_policy class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global其他信息： 阶段：15类型：NAT子类型：每会话结果：允许配置：其它信息： 阶段：16类型：IP-OPTIONS子类型：结果：允许配置：其它信息： 阶段：17类型：ROUTE-LOOKUP子类型：解析出口接口结果：允许配置：其它信息：发现下一跳192.168.76.39在阶段外使用出口ifc:18类型：ADJACENCY-LOOKUP子类型下一跳和邻接结果：允许配置：其它信息：邻接活动下一跳mac地址0004.deab.681b命中140372416161507阶段：19类型：捕获子类型：结果：允许配置：其它信息：MAC访问列表结果：输入接口：outside input-status:up input-line-status:up output-interface:outside output-status:up output-line-status:up操作：允许1个显示为firepower#的数据包

外部接口上的捕获显示：

```
<#root>

firepower#

show capture CAPO


10 packets captured

   1: 23:35:07.282044   192.168.75.39 > 192.168.76.39: icmp: echo request
   2: 23:35:07.282227   192.168.76.39 > 192.168.75.39: icmp: echo reply
   3: 23:35:09.278717   192.168.75.39 > 192.168.76.39: icmp: echo request
   4: 23:35:09.278962   192.168.76.39 > 192.168.75.39: icmp: echo reply
   5: 23:35:11.279343   192.168.75.39 > 192.168.76.39: icmp: echo request
   6: 23:35:11.279541   192.168.76.39 > 192.168.75.39: icmp: echo reply
   7: 23:35:13.278870   192.168.75.39 > 192.168.76.39: icmp: echo request
   8: 23:35:13.279023   192.168.76.39 > 192.168.75.39: icmp: echo reply
   9: 23:35:15.279373   192.168.75.39 > 192.168.76.39: icmp: echo request
  10: 23:35:15.279541   192.168.76.39 > 192.168.75.39: icmp: echo reply
10 packets shown
```

返回数据包的跟踪显示它与当前流(52)匹配，但被ACL阻止：

```
<#root>

firepower#

show capture CAPO packet-number 2 trace


10 packets captured



2: 23:35:07.282227       192.168.76.39 > 192.168.75.39: icmp: echo reply

Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
```

```
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:

Found flow with id 52, uses current flow


Phase: 4

Type: ACCESS-LIST

Subtype: log

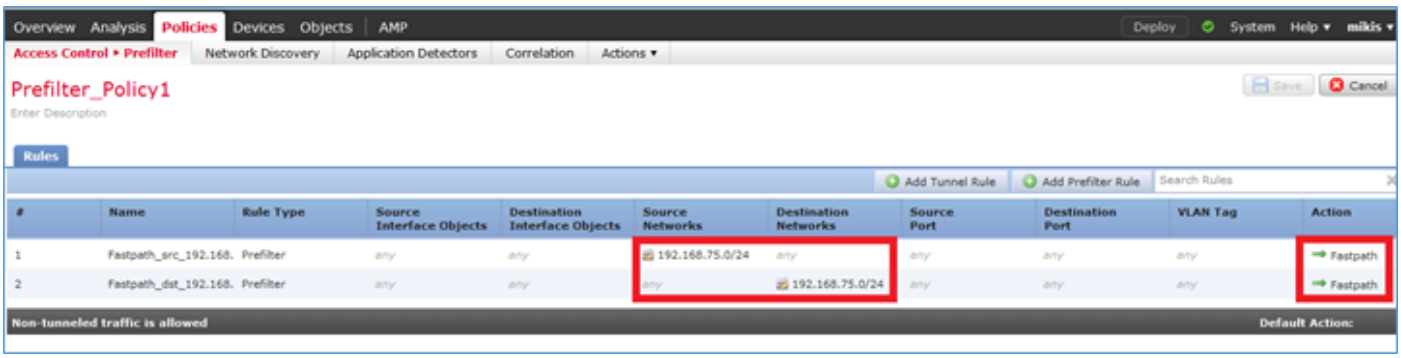
Result: DROP

Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268434432 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: ACP_5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule
```

5.为返回流量添加另一个预过滤器规则，下一图显示结果



现在跟踪您看到的返回数据包（重点突出显示）：

Spoiler（突出显示以便阅读）

firepower# show capture CAPO packet-number 2 trace

捕获了10个数据包

2:00:01:38.873123 192.168.76.39 > 192.168.75.39:icmp:回声应答

阶段：1

type：捕获

子类型：

结果：允许

Config :

其它信息：

MAC访问列表

阶段：2

type：访问列表

子类型：

结果：允许

Config :

隐式规则

其它信息：

MAC访问列表

阶段：3

type：流查找

子类型：

结果：允许

Config :

其它信息：

找到ID为62的流，使用当前流

阶段：4

type：访问列表

子类型：日志

结果：允许

Config :

access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced trust ip any 192.168.75.0 255.255.255.0 rule-id 268434450 event-log both

access-list CSM_FW_ACL_ remark rule-id 268434450:预过滤器策略：Prefilter_Policy1

access-list CSM_FW_ACL_ remark rule-id 268434450:规则：Fastpath_dst_192.168.75.0/24

其它信息：

阶段：5

type：CONN设置

子类型：

结果：允许

Config :

class-map class-default

 match any

policy-map global_policy

 class class-default

  set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

其它信息：

阶段：6

type：NAT

子类型：每会话

结果：允许

Config :

其它信息：

阶段：7

type：IP选项

子类型：

结果：允许

Config :

其它信息：

阶段：8

type：路由查找

子类型：解析出口接口

结果：允许

Config :

其它信息：

发现下一跳192.168.75.39在内部使用出口ifc

阶段：9

type：ADJACENCY-LOOKUP

子类型：下一跳和邻接关系

结果：允许

Config :

其它信息：

活动邻接关系

下一跳mac地址c84c.758d.4981命中140376711128802

阶段：10

type：捕获

子类型：

结果：允许

Config :

其它信息：

MAC访问列表

结果：

输入接口：内部

输入状态： up

input-line-status: up

output-interface:内部

输出状态： up

output-line-status: up

操作：允许

firepower# show capture CAPO packet-number 2 trace 10 packets captured 2:00:01:38.873123 192.168.76.39 > 192.168.75.39:icmp:回应应答阶段：1类型：捕获子类型：结果：允许配置：其它信息：MAC访问列表阶段：2类型：ACCESS-LIST子类型：结果：允许配置：隐式规则其他信息：MAC访问列表阶段：3类型：FLOW-LOOKUP子类型：结果：允许配置：其它信息：找到ID为62的流，使用当前流阶段：4类型：ACCESS-LIST子类型：日志结果：允许配置：access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip any 192.168.75.0 255.255.255.0 rule-id 268434450 event-log both access-list CSM_FW_ACL_ remark rule-id 268434450:预过滤器策略：Prefilter_Policy1 access-list CSM_FW_ACL_remark rule-id 268434450:规则：Fastpath_dst_192.168.75.0/24其他信息： 阶段：5类型：CONN-SETTINGS子类型：结果：允许配置：class-map class-default match any policy-map global_policy class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global其他信息： 阶段：6类型：NAT子类型：每会话结果：允许配置：其它信息： 阶段：7类型：IP-OPTIONS子类型：结果：允许配置：其它信息： 阶段：8类型：ROUTE-LOOKUP子类型：解析出口接口结果：允许配置：其它信息：发现下一跳192.168.75.39在阶段内使用出口ifc:9类型：ADJACENCY-LOOKUP子类型下一跳和邻接结果：允许配置：其它信息：邻接活动下一跳mac地址c84c.758d.4981命中140376711128802阶段：10类型：捕获子类型：结果：允许配置：其它信息：MAC访问列表结果：输入接口：inside input-status:up input-line-status:up output-interface:inside output-status:up output-line-status:up操作：允许

验证

使用此部分可以确认您的配置是否正常。验证已在各个任务部分中说明。

故障排除

当前没有故障排除此配置的特定可用资料。

相关信息

- 所有版本的Cisco Firepower管理中心配置指南都可以在思科安全防火墙威胁防御文档导航中找到
- 思科全球技术支持中心(TAC)强烈推荐此可视化指南，以了解有关Cisco Firepower下一代安全技术的深入实践知识，其中包括本文中提到的思科Firepower威胁防御(Cisco Firepower Threat Defense， FTD)下的知识
- 有关所有配置和故障排除技术说明，请参阅Cisco安全防火墙管理中心
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。