

# 明确Firepower威胁防御访问控制策略规则操作

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[ACP的部署方式](#)

[配置](#)

[ACP 可用操作](#)

[ACP 和预过滤器策略如何交互](#)

[ACP 阻止操作](#)

[场景 1. 提前 LINA 丢弃](#)

[场景 2：由于 Snort 判定而丢弃](#)

[ACP 阻止并重置操作](#)

[ACP 允许操作](#)

[场景 1. ACP 允许操作 \( L3/L4 条件 \)](#)

[场景 2：ACP 允许操作 \( L3-7 条件 \)](#)

[场景 3：Snort 快速转发判定 \( 使用“允许”规则 \)](#)

[ACP 信任操作](#)

[场景 1. ACP 信任操作](#)

[场景2. ACP信任操作 \( 无SI、QoS和身份策略 \)](#)

[预过滤器策略阻止操作](#)

[预过滤器策略快速路径操作](#)

[预过滤器策略快速路径操作 \( 内联集 \)](#)

[预过滤器策略快速路径操作 \( 带分路器的内联集 \)](#)

[预过滤器策略分析操作](#)

[场景 1. 使用 ACP 阻止规则进行预过滤器分析](#)

[场景 2：使用 ACP 允许规则进行过滤器分析](#)

[场景 3：使用 ACP 信任规则进行过滤器分析](#)

[场景 4：使用 ACP 信任规则进行过滤器分析](#)

[ACP 监控操作](#)

[ACP 交互式阻止操作](#)

[ACP 交互式阻止并重置操作](#)

[FTD 辅助连接和针孔](#)

[FTD 规则准则](#)

[摘要](#)

[相关信息](#)

## 简介

本文档介绍 Firepower Threat Defense (FTD) 访问控制策略 (ACP) 和预过滤器策略中可用的各种操作。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 流分流
- Firepower威胁防御设备上的数据包捕获
- FTD 设备上的数据包跟踪器和带有跟踪选项的 capture 命令

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科 Firepower 4110 威胁防御版本 6.4.0 ( 内部版本 113 ) 和 6.6.0 ( 内部版本 90 )
- Firepower 管理中心 (FMC) 版本 6.4.0 ( 内部版本 113 ) 和 6.6.0 ( 内部版本 90 )

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。

### 相关产品

本文档还可用于以下硬件和软件版本：

- ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X
- ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X
- FPR1000、FPR2100、FPR4100、FPR9300
- VMware (ESXi)、Amazon Web Services (AWS)、基于内核的虚拟机 (KVM)
- 集成多业务路由器 (ISR) 模块
- FTD 软件版本 6.1.x 及更高版本

**注意：**流分流仅在ASA和FTD应用的本地实例以及FPR4100和FPR9300平台上受支持。FTD容器实例不支持流量分流。

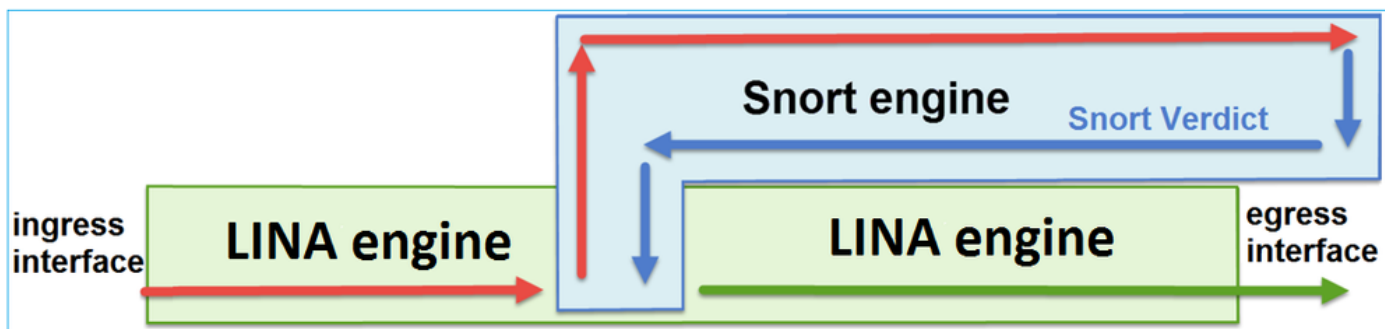
## 背景信息

检查每个操作的后台操作，以及它与其他功能 ( 如流量分流和打开辅助连接的协议 ) 的交互。

FTD 是由两个主要引擎组成的统一软件映像：

- LINA 引擎
- Snort 引擎

下图显示了这两个引擎的交互方式：



- 数据包进入入口接口并由 LINA 引擎处理
- 如果 FTD 策略要求，数据包将由 Snort 引擎检查
- Snort引擎返回数据包的判定（允许列表或阻止列表）
- LINA 引擎根据 Snort 的判定丢弃或转发数据包

## ACP的部署方式

使用机下（远程）管理时，在 FMC 上配置 FTD 策略；使用本地管理时，在 Firepower 设备管理器 (FDM) 上配置 FTD 策略。在这两种情况下，ACP 均部署为：

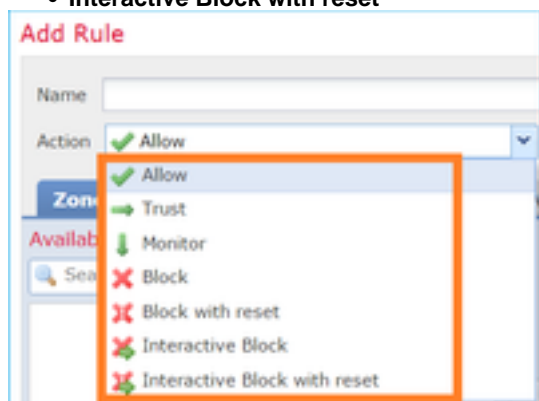
- FTD LINA引擎的名为CSM\_FW\_ACL\_的全局访问控制列表(ACL)
- /ngfw/var/sf/detection\_engines/<UUID>/ngfw.rules文件中的访问控制(AC)规则到FTD Snort引擎

## 配置

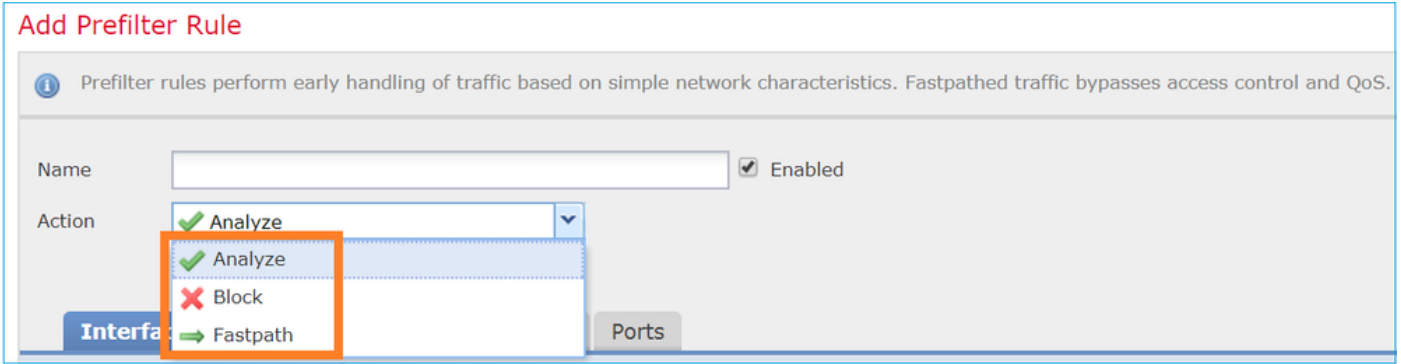
### ACP 可用操作

FTD ACP 包含一个或多个规则，每个规则可以具有以下任一操作，如图所示：

- Allow
- Trust
- Monitor
- Block
- Block with reset
- Interactive Block
- Interactive Block with reset



同样，预过滤器策略也可以包含一个或多个规则，可能的操作如下图所示：



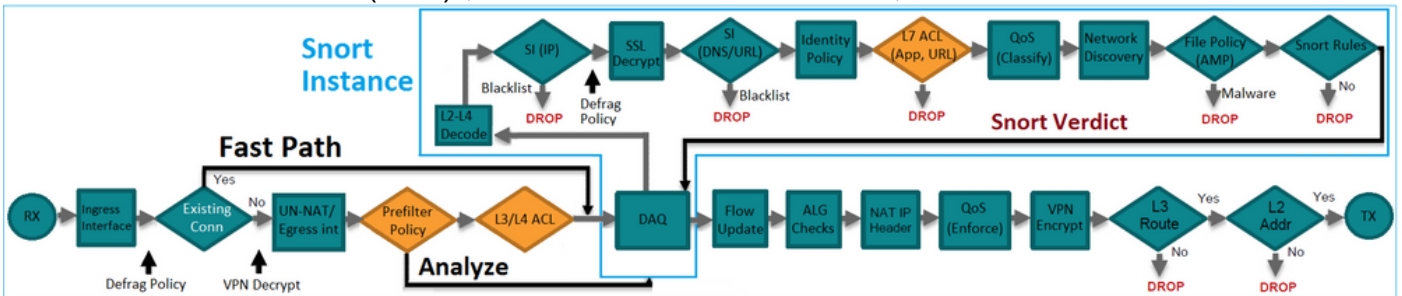
## ACP 和预过滤器策略如何交互

预过滤器策略在6.1版本中引入，主要用于2个目的：

1. 它允许检查隧道流量，其中 FTD LINA 引擎检查外部 IP 报头，而 Snort 引擎检查内部 IP 报头。具体而言，对于隧道流量（例如GRE），预过滤器策略中的规则始终在 **outer headers**，而 ACP 中的规则始终适用于内部会话 (**inner headers**)。隧道流量是指以下协议：

- GRE
- IP-in-IP
- IPv6-in-IP
- Teredo 端口 3544

2. 它提供早期访问控制(EAC)，允许流量完全绕过Snort引擎，如图所示。



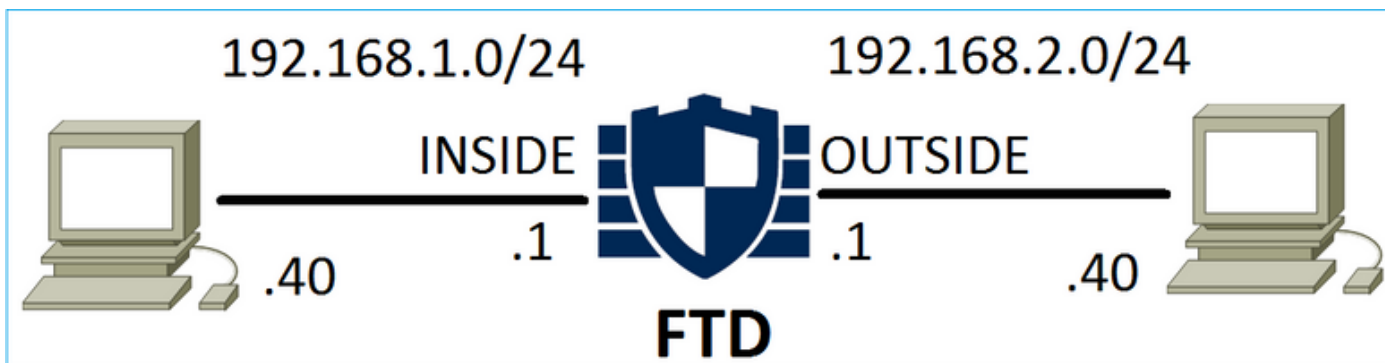
预过滤器规则在FTD上部署为L3/L4访问控制元素(ACE)，并在已配置的L3/L4 ACE之前，如图所示：

```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log both (hitcnt=0)
access-list CSM_FW_ACL_ line 4 remark rule-id 268434456: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268434456: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id 268434456 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268434456 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268434456 (hitcnt=2) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any any eq 3544 rule-id 268434456 (hitcnt=0) 0xcf6309bc
access-list CSM_FW_ACL_ line 10 remark rule-id 268434445: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ line 12 advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start (hitcnt=0) 0x8bf72c63
access-list CSM_FW_ACL_ line 14 remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 15 advanced permit ip any any rule-id 268434434 (hitcnt=410) 0xa1d3780e
```

注意：预过滤器v/s ACP规则=应用第一个匹配。

## ACP 阻止操作

请考虑下图所示的拓扑：



## 场景 1. 提前 LINA 丢弃

ACP 包含使用 L4 条件 ( 目的端口 TCP 80 ) 的阻止规则 , 如下图所示 :

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	TCP (6):80	Any	Any	Block

Snort 中部署的策略 :

```
268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

LINA 中部署的策略。请注意 , 规则推送为 deny 操作 :

```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 event-log flow-start (hitcnt=0) 0x6149c43c
```

验证行为 :

当主机A(192.168.1.40)尝试打开与主机B(192.168.2.40)的HTTP会话时 , TCP同步(SYN)数据包被 FTD LINA引擎丢弃 , 并且确实到达Snort引擎或目标 :

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing - 430 bytes]
  match ip host 192.168.1.40 any
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing - 0 bytes]
  match ip host 192.168.1.40 any
```

```
firepower# show capture CAPI
1: 11:08:09.672801 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
```

```

<mss 1460,sackOK,timestamp 4060517 0>
  2: 11:08:12.672435 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4063517 0>
  3: 11:08:18.672847 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4069517 0>
  4: 11:08:30.673610 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4081517 0>

```

firepower# show capture CAPI packet-number 1 trace

```

  1: 11:08:09.672801 192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920
<mss 1460,sackOK,timestamp 4060517 0>
...

```

Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: DROP

Config:

access-group CSM\_FW\_ACL\_ global

**access-list CSM\_FW\_ACL\_ advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id 268435461 event-log flow-start**

access-list CSM\_FW\_ACL\_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory

access-list CSM\_FW\_ACL\_ remark rule-id 268435461: L4 RULE: Rule1

**Additional Information:**

<- No Additional Information = No Snort Inspection

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

output-line-status: up

Action: drop

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

## 场景 2：由于 Snort 判定而丢弃

ACP 包含使用 L7 条件 ( 应用 HTTP ) 的阻止规则，如下图所示：

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	HTTP	Any	Any	Any	Any	Block

Snort 中部署的策略：

268435461 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any (appid 676:1)

Appid 676:1 = HTTP

LINA 中部署的策略。

**注意：**规则推送为 **permit** 操作，因为LINA无法确定会话使用HTTP。在FTD上，应用检测机制位于Snort引擎中。

```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 (hitcnt=0) 0xb788b786
```

对于使用 **Application** 作为条件，实际数据包的跟踪显示，由于Snort引擎判定，会话被LINA丢弃。

**注意：**为了使Snort引擎确定应用，它必须检查几个数据包（通常为3-10，这取决于应用解码器）。因此，一些数据包允许通过FTD并到达目的地。允许的数据包仍会根据以下内容接受入侵策略检查：**Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** 选项。

**验证行为：**

当主机 A (192.168.1.40) 尝试与主机 B (192.168.2.40) 建立 HTTP 会话时，LINA 入口捕获显示：

```
firepower# show capture CAPI

8 packets captured

  1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
  2: 11:31:19.826403 192.168.2.40.80 > 192.168.1.40.32790: S 1283931030:1283931030(0) ack
357753152 win 2896 <mss 1380,sackOK,timestamp 5449236 5450579>
  3: 11:31:19.826556 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>
  4: 11:31:20.026899 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450781 5449236>
  5: 11:31:20.428887 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5451183 5449236>
...
```

**出口捕获显示：**

```
firepower# show capture CAPO

5 packets captured

  1: 11:31:19.825869 192.168.1.40.32790 > 192.168.2.40.80: S 1163713179:1163713179(0) win 2920
<mss 1380,sackOK,timestamp 5450579 0>
  2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
  3: 11:31:23.426049 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5452836 5450579>
  4: 11:31:29.426430 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5458836 5450579>
  5: 11:31:41.427208 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
```

1163713180 win 2896 <mss 1460,sackOK,timestamp 5470836 5450579>

跟踪表明，由于尚未达到应用检测判定，Snort允许第一个数据包(TCP SYN):

```
firepower# show capture CAPI packet-number 1 trace
  1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80: S 357753151:357753151(0) win 2920
<mss 1460,sackOK,timestamp 5450579 0>
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435461
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268435461: L7 RULE: Rule1
Additional Information:
  This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 23194, packet dispatched to next module
...
Phase: 12
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 357753151
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 0, icmpCode 0
Firewall: pending rule-matching, id 268435461, pending AppID
NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

TCP SYN/ACK 数据包也是如此：

```
firepower# show capture CAPO packet-number 2 trace
  2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack
1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
...
```



Phase: 3  
Type: FLOW-LOOKUP  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
**Found flow with id 23194, using existing flow**  
...

Phase: 5  
Type: SNORT  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Snort Trace:  
Packet: TCP, SYN, ACK, seq 1283931030, ack 357753152  
AppID: service unknown (0), application unknown (0)  
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,  
icmpType 0, icmpCode 0  
**Firewall: pending rule-matching, id 268435461, pending AppID**  
NAP id 1, IPS id 0, Verdict PASS  
**Snort Verdict: (pass-packet) allow this packet**

Result:  
input-interface: INSIDE  
input-status: up  
input-line-status: up  
output-interface: INSIDE  
output-status: up  
output-line-status: up  
**Action: allow**

完成第三个数据包的检测后，Snort会返回DROP判定：

```
firepower# show capture CAPI packet-number 3 trace
  3: 11:31:19.826556 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack
1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>
```

Phase: 3  
Type: FLOW-LOOKUP  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
**Found flow with id 23194, using existing flow**

Phase: 5  
Type: SNORT  
Subtype:  
**Result: DROP**  
Config:  
Additional Information:  
Snort Trace:  
Packet: TCP, ACK, seq 357753152, ack 1283931031  
**AppID: service HTTP (676), application unknown (0)**  
Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0, vlan 0, sgt 65535, user 9999997,  
url http://192.168.2.40/128k.html  
**Firewall: block rule, id 268435461, drop**  
Snort: processed decoder alerts or actions queue, drop  
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall  
**Snort Verdict: (block-list) block list this flow**

```
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

您还可以运行命令 `system support trace` 从FTD CLISH模式。此工具提供2个功能：

- 显示每个数据包发送到数据采集库(DAQ)时的Snort判定，在LINA中可见该判定。DAQ 是位于FTD LINA 引擎和 Snort 引擎之间的组件
- 允许运行 `system support firewall-engine-debug` 同时了解Snort引擎本身的情况

以下是输出：

```
> system support trace
```

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages
```

```
Tracing enabled by Lina
```

```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, seq 2620409313
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 New session
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS
```

```
Tracing enabled by Lina
```

```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, SYN, ACK, seq 3700371680, ack 2620409314
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0 -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc 0,
payload 0, client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 ->
0, vlan 0, sgt 65535, user 9999997, icmpType 0, icmpCode 0
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: pending rule-matching, 'Rule1', pending AppID
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTS
```

```
Tracing enabled by Lina
```

```
192.168.2.40-80 - 192.168.1.40-32791 6 Packet: TCP, ACK, seq 2620409314, ack 3700371681
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone
first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, inline sgt tag: untagged, ISE sgt id: 0, svc
676, payload 0, client 686, misc 0, user 9999997, url http://192.168.2.40/128k.html, xff
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0)
-> 0, vlan 0, sgt 65535, user 9999997, url http://192.168.2.40/128k.html
```

```

192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 match rule order 2, 'Rule1', action Block
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 deny action
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: block rule, 'Rule1', drop
192.168.1.40-32791 > 192.168.2.40-80 6 Snort: processed decoder alerts or actions queue, drop
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Deleting session
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict BLOCKLIST
192.168.1.40-32791 > 192.168.2.40-80 6 ==> Blocked by Firewall

```

## 摘要

- ACP 阻止操作在 LINA 中部署为许可或拒绝规则，具体取决于规则条件
- 如果条件为 L3/L4，则 LINA 会阻止数据包。对于TCP，第一个数据包(TCP SYN)被阻止
- 如果条件为 L7，则数据包将被转发到 Snort 引擎以进行进一步检查。如果使用 TCP，则在 Snort 作出判定之前，会允许一些数据包通过 FTD。允许的数据包仍会根据以下内容接受入侵策略检查：**Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** 选项。

## ACP 阻止并重置操作

在 FMC UI 上配置的“阻止并重置”规则：

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action	
▼ Mandatory - ACP1 (1-4)														
1	Block-RST-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Block with reset
2	Block-RST_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Block with reset

Block with reset规则在FTD LINA引擎上部署为 permit 和Snort引擎 reset 规则：

```

firepower# show access-list
...
access-list CSM_FW_ACL_line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=0) 0xba785fc0
access-list CSM_FW_ACL_line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_line 12 remark rule-id 268438865: L7 RULE: Block-RST_Rule2
access-list CSM_FW_ACL_line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0

```

Snort 引擎：

```

admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
...
# Start of AC rule.
268438864 reset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 reset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865

```

当数据包与Block with reset规则匹配时，FTD发送 TCP Reset 数据包或 ICMP Type 3 Code 13 目标无法到达 (管理性过滤) 消息：

```

root@kali:~/tests# wget 192.168.11.50/file1.zip

```

```
--2020-06-20 22:48:10-- http://192.168.11.50/file1.zip
Connecting to 192.168.11.50:80... failed: Connection refused.
```

以下是在 FTD 入口接口上执行的捕获：

```
firepower# show capture CAPI
2 packets captured
1: 21:01:00.977259 802.1Q vlan#202 PO 192.168.10.50.41986 > 192.168.11.50.80: S
3120295488:3120295488(0) win 29200 <mss 1460,sackOK,timestamp 3740873275 0,nop,wscale 7>
2: 21:01:00.978114 802.1Q vlan#202 PO 192.168.11.50.80 > 192.168.10.50.41986: R 0:0(0) ack
3120295489 win 0 2 packets shown
```

**System support trace** 在本例中，输出显示由于Snort判定而丢弃数据包：

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.50
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages

192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3387496622
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 new firewall session
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 using HW or preset rule order 2, 'Block-RST-
Rule1', action Reset and prefilter rule 0
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 HitCount data sent for rule id: 268438864,
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 reset action
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 deleting firewall session flags = 0x0,
fwFlags = 0x0
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: block w/ reset rule, 'Block-RST-
Rule1', drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 9, NAP id 1, IPS id 0, Verdict
BLOCKLIST
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

## 使用案例

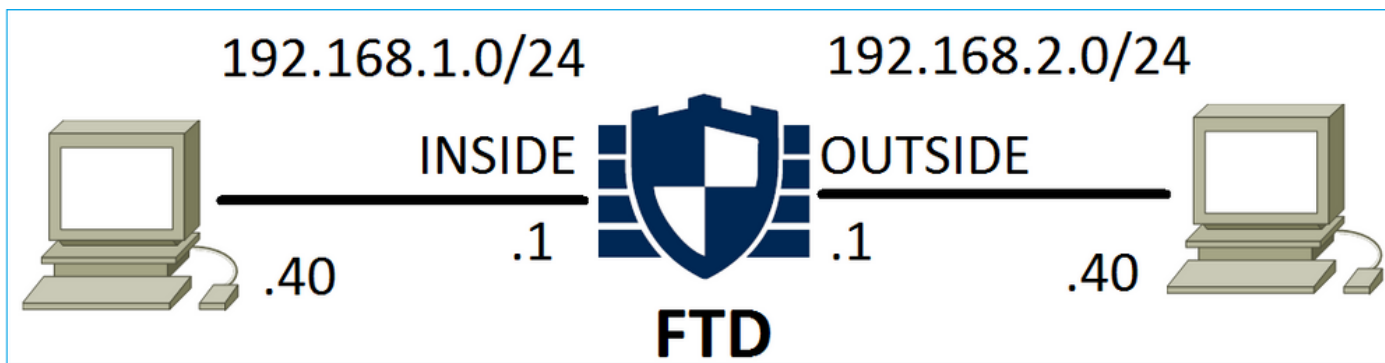
与 **Block** 操作，但立即终止连接。

## ACP 允许操作

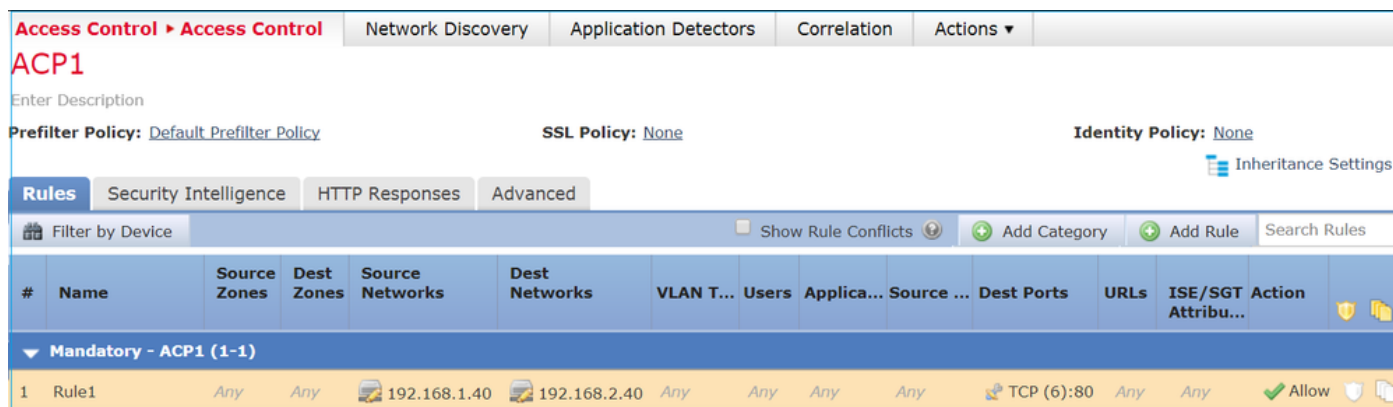
### 场景 1. ACP 允许操作 ( L3/L4 条件 )

通常，您会配置允许规则以指定其他检查，如入侵策略和/或文件策略。第一个场景演示应用 L3/L4条件时Allow规则的操作。

考虑下图所示的拓扑：



应用此策略如图所示：



Snort 中部署的策略。请注意，规则部署为 **allow** 操作：

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

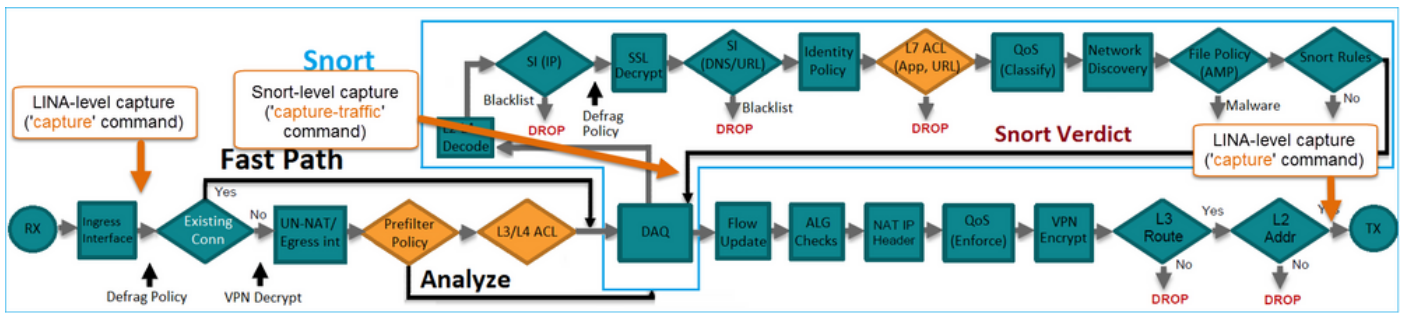
LINA 中的策略。

**注意：**规则部署为 **permit** 操作，本质上意味着重定向到Snort以进行进一步检查。

```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268435461 (hitcnt=1) 0x641a20c3
```

为了查看FTD如何处理与Allow规则匹配的流，有以下几种方法：

- 验证 Snort 统计信息
  - 使用 system support trace CLISH 工具
  - 在 LINA 中使用带有跟踪选项的 capture 命令，或者在 Snort 引擎中使用 capture-traffic 命令
- LINA capture 命令与 Snort capture-traffic 命令：



## 验证行为：

清除Snort统计信息，启用 **system support trace** from CLISH, and initiate an HTTP flow from host-A (192.168.1.40) to host-B (192.168.2.40). All the packets are forwarded to the Snort engine and get the PASS verdict by the Snort:

```
firepower# clear snort statistics
```

```
> system support trace
```

```
Please specify an IP protocol:
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]:
Monitoring packet tracer debug messages
```

Tracing enabled by Lina

```
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, seq 361134402
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTs
```

Tracing enabled by Lina

```
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, ACK, seq 1591434735, ack 361134403
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
Trace buffer and verdict reason are sent to DAQ's PDTs
```

Tracing enabled by Lina

```
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, ACK, seq 361134403, ack 1591434736
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0, Verdict PASS
```

## 传递数据包计数器增加：

```
> show snort statistics
```

Packet Counters:

<b>Passed Packets</b>	<b>54</b>
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

Flow Counters:

Fast-Forwarded Flows 0  
 Blocklisted Flows 0

Passed Packets = Snort引擎检查

### 场景 2：ACP 允许操作 ( L3-7 条件 )

当按如下方式部署Allow规则时，会看到类似行为。

只有第3/第4层情况，如图所示：

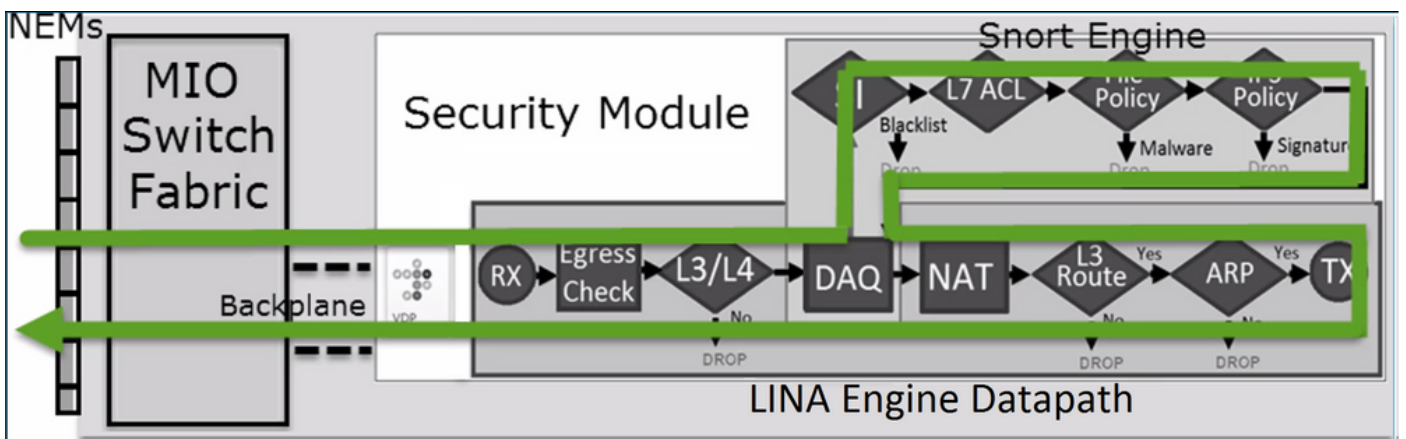
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

L7条件 ( 例如，入侵策略、文件策略、应用等 ) 显示在图像中：

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applica...	Source ...	Dest Ports	URLs	ISE/SGT Attribu...	Action
Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	Allow

### 摘要

总而言之，以上介绍了 FP4100/9300 上部署的 FTD 如何处理匹配“允许”规则的流，如下图所示：



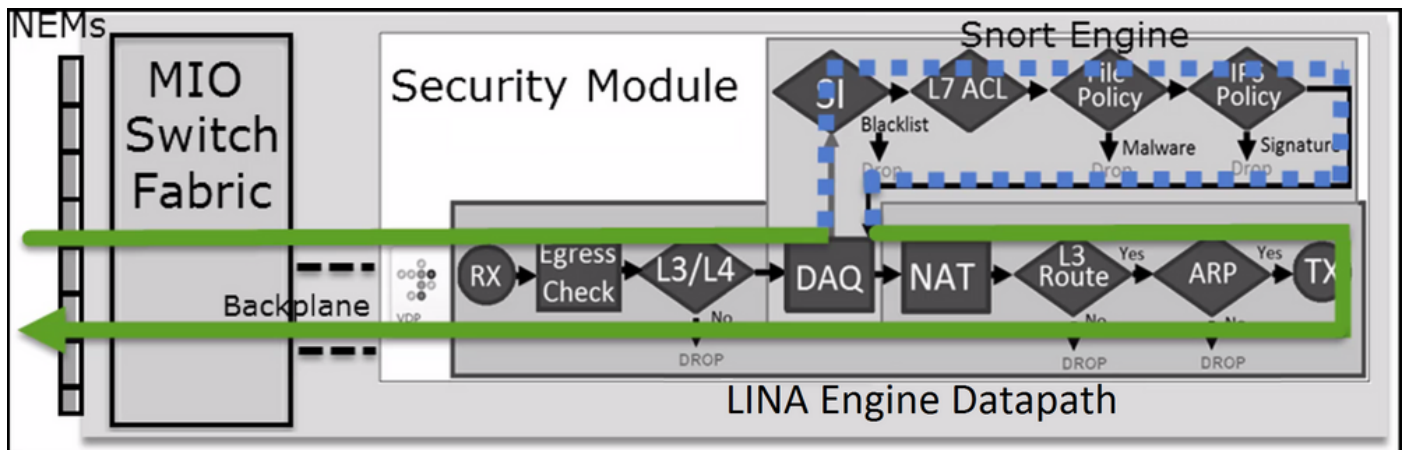
注意：管理输入输出 (MIO) 是 Firepower 机箱的管理引擎。

### 场景 3：Snort 快速转发判定 ( 使用“允许”规则 )

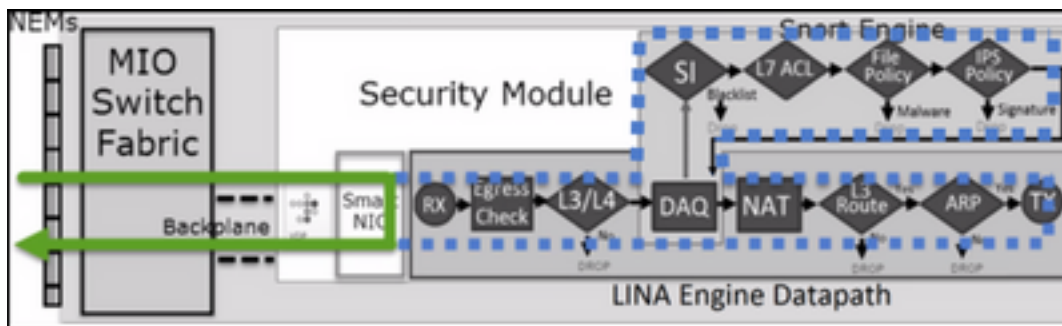
在某些特定情况下，FTD Snort引擎会提供PERMITLIST判定 ( 快速转发 )，而流的其余部分会卸载到LINA引擎 ( 在某些情况下，然后卸载到HW加速器 — SmartNIC )。即：

1. 未配置 SSL 策略的 SSL 流量
2. 智能应用旁路(IAB)

这是数据包路径的可视表示：



在某些情况下：



## 要点

- 允许规则部署为 `allow` 在Snort和 `permit` 在LINA
- 在大多数情况下，会话的所有数据包都会转发到Snort引擎进行其他检查

## 使用案例

当需要Snort引擎进行L7检测时，应配置允许规则，例如：

- 入侵策略
- 文件策略

## ACP 信任操作

### 场景 1. ACP 信任操作

如果您不想在Snort级别应用高级L7检测（例如，入侵策略、文件策略、网络发现），但仍希望使用安全情报(SI)、身份策略、QoS等功能，则建议在规则中使用Trust操作。

拓扑：





已配置的策略：

ACP1															Analyze Hit Counts	Save	Cancel			
Enter Description															<a href="#">Inheritance Settings</a>   <a href="#">Policy Assignments (1)</a>					
Rules	Security Intelligence	HTTP Responses	Logging	Advanced	Prefilter Policy: Prefilter1					SSL Policy: None		Identity Policy: None								
Filter by Device															Search Rules	Show Rule Conflicts	Add Category	Add Rule		
Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action							
Mandatory - ACP1 (1-4)																				
1	trust_L3-L4	Any	Any	192.168.10.50 192.168.10.51	192.168.11.50 192.168.11.51	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Trust						

FTD Snort 引擎中部署的“信任”规则：

```
# Start of AC rule.
268438858 fastpath any 192.168.10.50 31 any any 192.168.11.50 31 80 any 6 (log dcforward
flowend)
```

**注意：**数字 6 是协议 (TCP)。

FTD LINA 中的规则：

```
firepower# show access-list | i 268438858
access-list CSM_FW_ACL_ line 17 remark rule-id 268438858: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 18 remark rule-id 268438858: L7 RULE: trust_L3-L4
access-list CSM_FW_ACL_ line 19 advanced permit tcp object-group FMC_INLINE_src_rule_268438858
object-group FMC_INLINE_dst_rule_268438858 eq www rule-id 268438858 (hitcnt=19) 0x29588b4f
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=19) 0x9d442895
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.50 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0xd026252b
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.50 eq
www rule-id 268438858 (hitcnt=0) 0x0d785cc4
access-list CSM_FW_ACL_ line 19 advanced permit tcp host 192.168.10.51 host 192.168.11.51 eq
www rule-id 268438858 (hitcnt=0) 0x3b3234f1
```

**验证：**

enable system support trace 并从主机A(192.168.10.50)发起到主机B(192.168.11.50)的HTTP会话。有 3 个数据包转发到 Snort 引擎。Snort引擎向LINA发送PERMITLIST判定，该判定实质上会将流的其余部分卸载到LINA引擎：

> **system support trace**

Enable firewall-engine-debug too? [n]: **y**  
Please specify an IP protocol: **tcp**  
**Please** specify a client IP address: **192.168.10.50**  
Please specify a client port:  
Please specify a server IP address: **192.168.11.50**  
Please specify a server port: **80**  
Monitoring packet tracer and firewall debug messages

```
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 453426648
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 new firewall session
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 using HW or preset rule order 5, 'trust_L3-
L4', action Trust and prefilter rule 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 HitCount data sent for rule id: 268438858,
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2820426532, ack
453426649
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PASS

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 453426649, ack
2820426533
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-
L4', allow
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0, Verdict
PERMITLIST
```

连接终止后，Snort 引擎会从 LINA 引擎获取元数据信息并删除会话：

```
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Got end of flow event from hardware with
flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 3
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Logging EOF for event from hardware with
rule_id = 268438858 ruleAction = 3 ruleReason = 0
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 : Received EOF, deleting the snort session.

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleting snort session, reason:
timeout
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 deleting firewall session flags = 0x10003,
fwFlags = 0x1115
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleted snort session using 0
bytes; protocol id:(-1) : LWstate 0xf LWFlags 0x6007
```

Snort捕获显示到达Snort引擎的3个数据包：

> **capture-traffic**

Please choose domain to capture traffic from:

- 0 - management0
- 1 - management1
- 2 - Global

Selection? **2**

Please specify tcpdump options desired.

(or enter '?' for a list of supported options)

Options: **-n vlan and (host 192.168.10.50 and host 192.168.11.50)**

10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [S], seq 3065553465, win 29200, options [mss 1380,sackOK,TS val 3789188468 ecr 0,nop,wscale 7], length 0

10:26:16.525928 IP 192.168.11.50.80 > 192.168.10.50.42144: Flags [S.], seq 3581351172, ack 3065553466, win 8192, options [mss 1380,nop,wscale 8,sackOK,TS val 57650410 ecr 3789188468], length 0

10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [.], ack 1, win 229, options [nop,nop,TS val 3789188470 ecr 57650410], length 0

**LINA capture 命令显示通过它的流量 :**

```
firepower# show capture CAPI
```

437 packets captured

```
1: 09:51:19.431007 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: S
2459891187:2459891187(0) win 29200 <mss 1460,sackOK,timestamp 3787091387 0,nop,wscale 7>
```

```
2: 09:51:19.431648 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: S
2860907367:2860907367(0) ack 2459891188 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
57440579 3787091387>
```

```
3: 09:51:19.431847 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: . ack
2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
```

```
4: 09:51:19.431953 802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: P
2459891188:2459891337(149) ack 2860907368 win 229 <nop,nop,timestamp 3787091388 57440579>
```

```
5: 09:51:19.444816 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860907368:2860908736(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>
```

```
6: 09:51:19.444831 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: .
2860908736:2860910104(1368) ack 2459891337 win 256 <nop,nop,timestamp 57440580 3787091388>
```

...

跟踪来自 LINA 的数据包是查看 Snort 判定的另一种方式。第一个数据包得到PASS判定 :

```
firepower# show capture CAPI packet-number 1 trace | i Type|Verdict
```

Type: CAPTURE

Type: ACCESS-LIST

Type: ROUTE-LOOKUP

Type: ACCESS-LIST

Type: CONN-SETTINGS

Type: NAT

Type: NAT

Type: IP-OPTIONS

Type: CAPTURE

Type: CAPTURE

Type: NAT

Type: CAPTURE

Type: NAT

Type: IP-OPTIONS

Type: CAPTURE

Type: FLOW-CREATION

```
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

跟踪外部接口上的TCP SYN/ACK数据包：

```
firepower# show capture CAPO packet-number 2 trace | i Type|Verdict
Type: CAPTURE
Type: ACCESS-LIST
Type: FLOW-LOOKUP
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

TCP ACK获取PERMITLIST判定：

```
firepower# show capture CAPI packet-number 3 trace | i Type|Verdict
Type: CAPTURE
Type: ACCESS-LIST
Type: FLOW-LOOKUP
Type: EXTERNAL-INSPECT
Type: SNORT
Snort id 22, NAP id 2, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
Type: CAPTURE
```

以下是 Snort 判定的完整输出 (数据包 3)

```
firepower# show capture CAPI packet-number 3 trace | b Type: SNORT
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 687485179, ack 1029625865
AppID: service unknown (0), application unknown (0)
Firewall: trust/fastpath rule, id 268438858, allow
Snort id 31, NAP id 2, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
```

第4个数据包不会转发到Snort引擎，因为判定由LINA引擎缓存：

```
firepower# show capture CAPI packet-number 4 trace
```

```
441 packets captured
```

```
4: 10:34:02.741523      802.1Q vlan#202 P0 192.168.10.50.42158 > 192.168.11.50.80: P
```

164375589:164375738(149) ack 3008397532 win 229 <nop,nop,timestamp 3789654678 57697031>

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 1254, using existing flow**

**Phase: 4**

**Type: SNORT**

**Subtype:**

**Result: ALLOW**

**Config:**

**Additional Information:**

**Snort Verdict: (fast-forward) fast forward this flow**

Result:

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

Action: allow

1 packet shown

Snort 统计信息证实了这一点：

firepower# **show snort statistics**

Packet Counters:

<b>Passed Packets</b>	<b>2</b>
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

Flow Counters:

<b>Fast-Forwarded Flows</b>	<b>1</b>
Blacklisted Flows	0

Miscellaneous Counters:

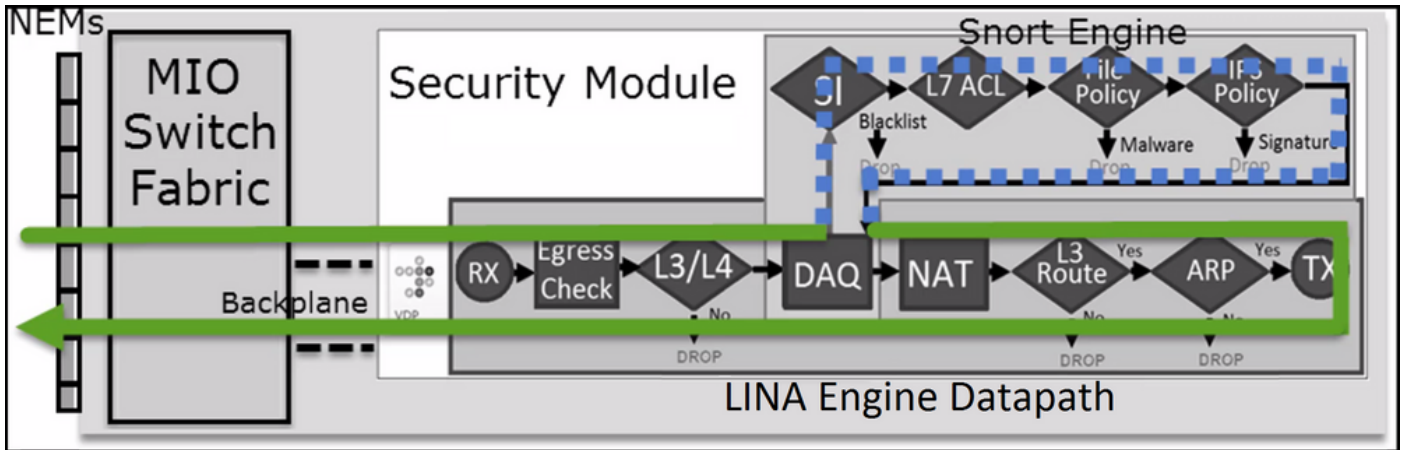
Start-of-Flow events	0
End-of-Flow events	1
Denied flow events	0

```

Frames forwarded to Snort before drop           0
Inject packets dropped                          0

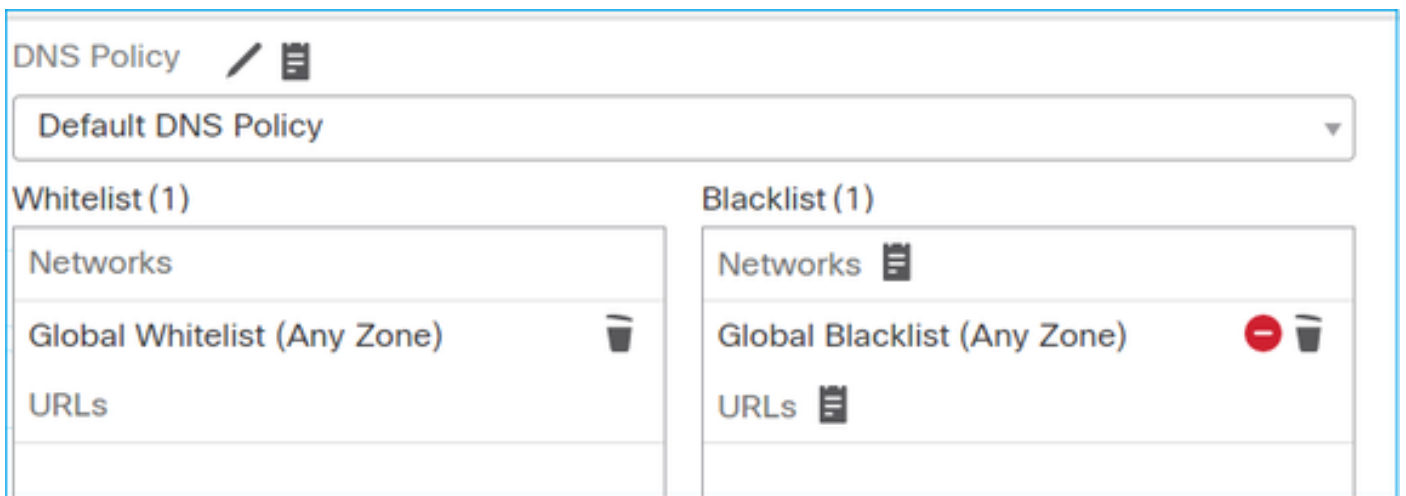
```

使用“信任”规则的数据包流。Snort会检查一些数据包，其余数据包由LINA检查：



## 场景2. ACP信任操作 (无SI、QoS和身份策略)

如果您希望FTD对所有流应用安全情报(SI)检查，SI已在ACP级别启用，您可以指定SI源 (TALOS、源、列表等)。另一方面，如果要禁用SI，您可以为每个ACP全局禁用网络的SI并禁用URL的SI和DNS的SI。网络和URL的SI已禁用，如下图所示：



在本例中，“信任”规则作为信任操作部署到LINA：

```

> show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6

```

**注意：**自6.2.2起，FTD支持TID。TID的工作方式与SI类似，但如果SI被禁用，FTD不会“强制”将数据包重定向到Snort引擎以进行TID检查。

## 验证行为

从主机A(192.168.1.40)向主机B(192.168.2.40)发起HTTP会话。由于这是FP4100并支持硬件中的

流量分流，因此会发生以下情况：

- 一些数据包通过FTD LINA引擎转发，其余的数据流被分流到SmartNIC（硬件加速器）
- 没有数据包转发到Snort引擎

FTD LINA连接表显示标志“o”这意味着流已卸载到HW。另请注意，没有“N”标志。这实质上意味着“无Snort重定向”：

```
firepower# show conn
1 in use, 15 most used
```

```
TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:32809, idle 0:00:00, bytes 949584, flags UIOo
```

Snort 统计信息仅显示会话开始和结束时的日志记录事件：

```
firepower# show snort statistics
```

Packet Counters:

Passed Packets	0
Blocked Packets	0
Injected Packets	0
Packets bypassed (Snort Down)	0
Packets bypassed (Snort Busy)	0

Flow Counters:

Fast-Forwarded Flows	0
Blacklisted Flows	0

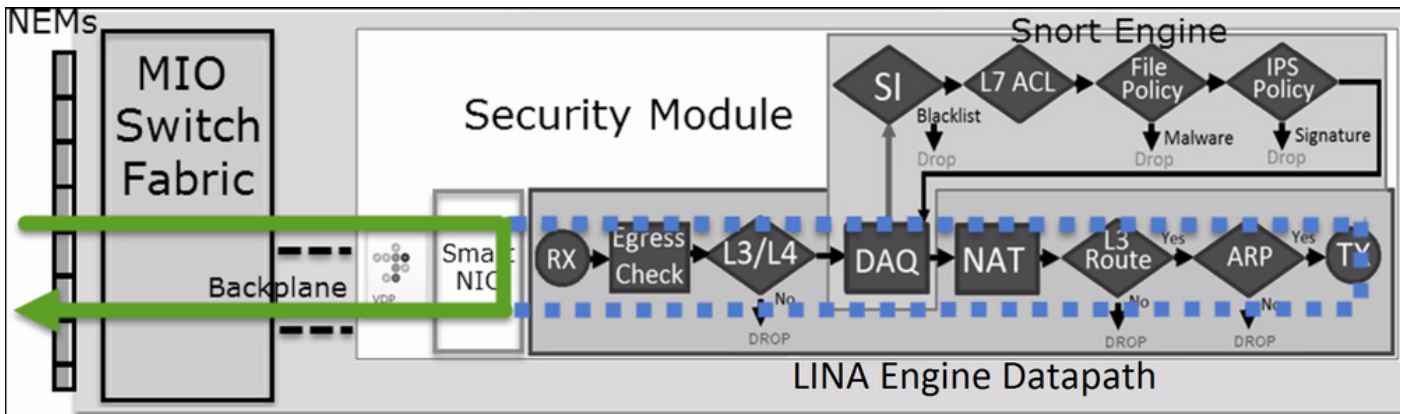
Miscellaneous Counters:

<b>Start-of-Flow events</b>	<b>1</b>
<b>End-of-Flow events</b>	<b>1</b>

FTD LINA 日志显示，每个会话有 2 个流（每个方向一个）分流到硬件：

```
Sep 27 2017 20:16:05: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Sep 27 2017 20:16:05: %ASA-6-302013: Built inbound TCP connection 25384 for
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001: Offloaded TCP Flow for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from
INSIDE:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-302014: Teardown TCP connection 25384 for INSIDE:192.168.1.40/32809
to OUTSIDE:192.168.2.40/80 duration 0:00:00 bytes 1055048 TCP FINs
Sep 27 2017 20:16:05: %ASA-7-609002: Teardown local-host INSIDE:192.168.1.40 duration 0:00:00
```

将信任规则部署为 trust 在LINA采取行动。LINA会检查一些数据包，其余数据包被卸载到SmartNIC(FP4100/FP9300):

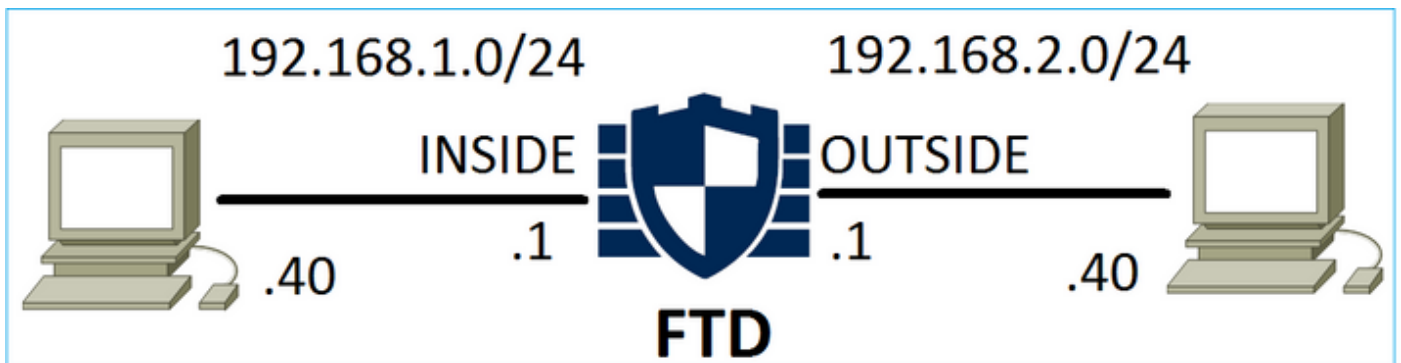


## 使用案例

- 您必须使用 `Trust` 当您仅希望由Snort引擎检查几个数据包（例如，应用检测、SI检查）并将流的其余部分卸载到LINA引擎时执行的操作
- 如果在FP4100/9300上使用FTD并希望流完全绕过Snort检测，则考虑预过滤器规则以 `Fastpath` 操作（请参阅本文档中的相关部分）

## 预过滤器策略阻止操作

考虑下图所示的拓扑：



另请考虑下图所示的策略：

Access Control > Prefilter									
FTD_Prefilter									
Enter Description									
Rules									
<span>+</span> Add Tunnel Rule <span>+</span> Add Prefilter Rule    Search Rules									
#	Name	Rule T...	...	De Source Int Networks	Destination Networks	Source Port	Destinat... Port	VLAN Tag	Action
1	Prefilter1	Prefilter	any any	192.168.1.40	192.168.2.40	any	any	any	Block

这是FTD Snort引擎（`ngfw.rules`文件）中部署的策略：

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268437506 deny any 192.168.1.40 32 any any 192.168.2.40 32 any any any (tunnel -1
```



## LINA 中部署的策略：

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id
268437506 event-log flow-start (hitcnt=0) 0x76476240
```

当您跟踪虚拟数据包时，它显示数据包被LINA丢弃，并且从不转发到Snort:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id 268437506
event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ remark rule-id 268437506: RULE: Prefilter1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

## Snort 统计信息显示：

```
firepower# show snort statistics
```

```
Packet Counters:
  Passed Packets                                0
  Blocked Packets                               0
  Injected Packets                              0
  Packets bypassed (Snort Down)                 0
  Packets bypassed (Snort Busy)                 0

Flow Counters:
  Fast-Forwarded Flows                          0
  Blacklisted Flows                             0

Miscellaneous Counters:
  Start-of-Flow events                          0
  End-of-Flow events                            0
  Denied flow events                            1
```

## LINA ASP 丢包显示：

```
firepower# show asp drop
```

Frame drop:

Flow is denied by configured rule (acl-drop)

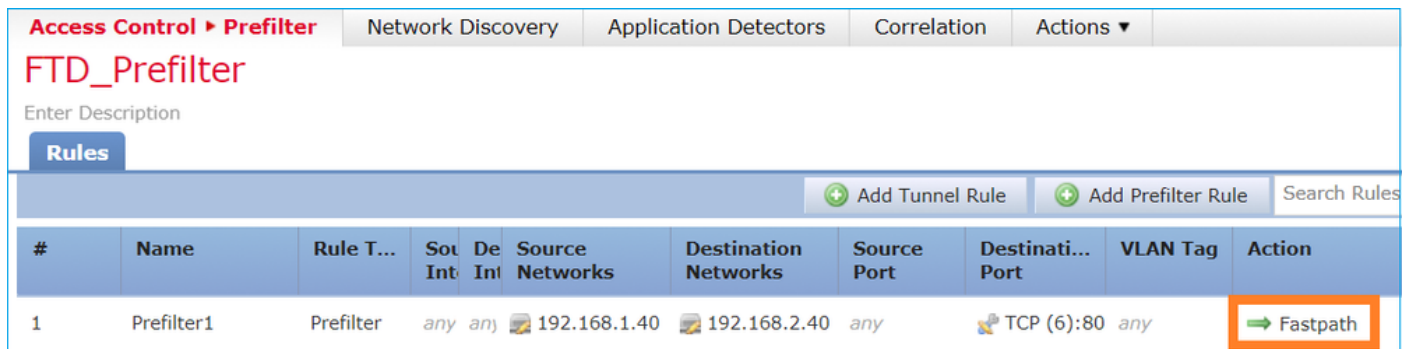
1

## 使用案例

当您想要根据L3/L4条件阻止流量，而无需对流量执行任何Snort检测时，可以使用预过滤器阻止规则。

## 预过滤器策略快速路径操作

考虑下图所示的预过滤器策略规则：



#	Name	Rule T...	Sot Int	De Int	Source Networks	Destination Networks	Source Port	Destinati...	VLAN Tag	Action
1	Prefilter1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	TCP (6):80	any	→ Fastpath

这是FTD Snort引擎中部署的策略：

```
268437506 fastpath any any any any any any (log dcfoward flowend) (tunnel -1)
```

FTD LINA 中部署的策略：

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced trust tcp host 192.168.1.40 host 192.168.2.40 eq www
rule-id 268437506 event-log flow-end (hitcnt=0) 0xf3410b6f
```

## 验证行为

当主机 A (192.168.1.40) 尝试打开与主机 B (192.168.2.40) 的 HTTP 会话时，少量数据包会通过 LINA，而其余数据包会分流到 SmartNIC。在这种情况下 system support trace 与 firewall-engine-debug enabled 显示：

```
> system support trace
```

```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages
```

```
192.168.1.40-32840 > 192.168.2.40-80 6 AS 1 I 8 Got end of flow event from hardware with flags
04000000
```

## LINA 日志显示已分流的流：

```
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host OUTSIDE:192.168.2.40
Oct 01 2017 14:36:51: %ASA-6-302013: Built inbound TCP connection 966 for
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
INSIDE:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001: Offloaded TCP Flow for connection 966 from
OUTSIDE:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32840 (192.168.1.40/32840)
```

## LINA捕获show 8个数据包通过：

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
3908 bytes]
  match ip host 192.168.1.40 host 192.168.2.40
```

```
firepower# show capture CAPI
```

### 8 packets captured

```
  1: 14:45:32.700021 192.168.1.40.32842 > 192.168.2.40.80: S 3195173118:3195173118(0) win 2920
<mss 1460,sackOK,timestamp 332569060 0>
  2: 14:45:32.700372 192.168.2.40.80 > 192.168.1.40.32842: S 184794124:184794124(0) ack
3195173119 win 2896 <mss 1380,sackOK,timestamp 332567732 332569060>
  3: 14:45:32.700540 192.168.1.40.32842 > 192.168.2.40.80: P 3195173119:3195173317(198) ack
184794125 win 2920 <nop,nop,timestamp 332569060 332567732>
  4: 14:45:32.700876 192.168.2.40.80 > 192.168.1.40.32842: . 184794125:184795493(1368) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
  5: 14:45:32.700922 192.168.2.40.80 > 192.168.1.40.32842: P 184795493:184796861(1368) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569060>
  6: 14:45:32.701425 192.168.2.40.80 > 192.168.1.40.32842: FP 184810541:184810851(310) ack
3195173317 win 2698 <nop,nop,timestamp 332567733 332569061>
  7: 14:45:32.701532 192.168.1.40.32842 > 192.168.2.40.80: F 3195173317:3195173317(0) ack
184810852 win 2736 <nop,nop,timestamp 332569061 332567733>
  8: 14:45:32.701639 192.168.2.40.80 > 192.168.1.40.32842: . ack 3195173318 win 2697
<nop,nop,timestamp 332567734 332569061>
```

## FTD 流分流统计信息显示 22 个数据包分流到硬件：

```
firepower# show flow-offload statistics
```

```
Packet stats of port : 0
```

<b>Tx Packet count</b>	:	<b>22</b>
<b>Rx Packet count</b>	:	<b>22</b>
Dropped Packet count	:	0
VNIC transmitted packet	:	22
VNIC transmitted bytes	:	15308
VNIC Dropped packets	:	0
VNIC erroneous received	:	0

```

VNIC CRC errors          : 0
VNIC transmit failed    : 0
VNIC multicast received  : 0

```

您还可以使用 `show flow-offload flow` 命令查看与卸载流相关的其他信息。示例如下：

```

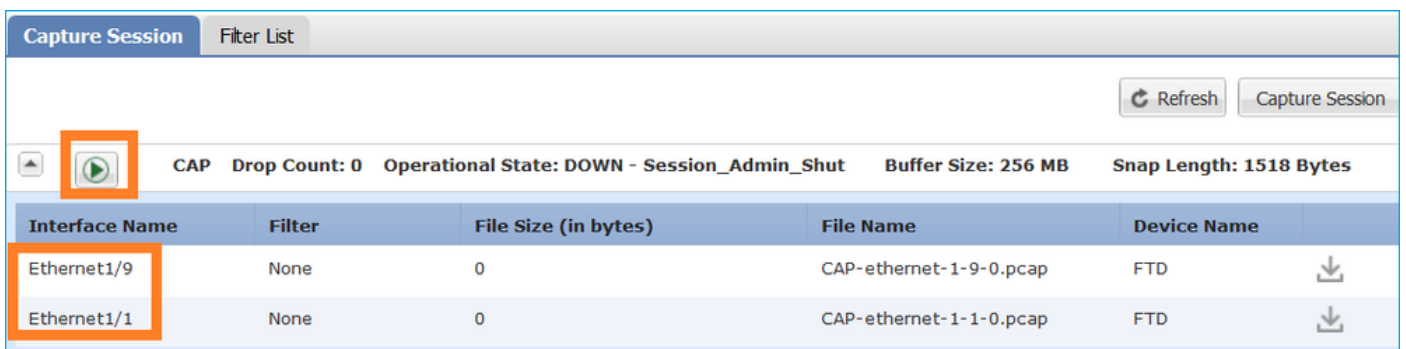
firepower# show flow-offload flow
Total offloaded flow stats: 2 in use, 4 most used, 20% offloaded, 0 collisions
TCP intf 103 src 192.168.1.40:39301 dest 192.168.2.40:20, static, timestamp 616063741, packets
33240, bytes 2326800
TCP intf 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 616063760, packets
249140, bytes 358263320
firepower# show conn
5 in use, 5 most used
Inspect Snort:
  preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 0 most in effect

TCP OUTSIDE 192.168.2.40:21 INSIDE 192.168.1.40:40988, idle 0:00:00, bytes 723, flags UIO
TCP OUTSIDE 192.168.2.40:21 INSIDE 192.168.1.40:40980, idle 0:02:40, bytes 1086, flags UIO
TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:49442, idle 0:00:00, bytes 86348310, flags UIO
N1
TCP OUTSIDE 192.168.2.40:20 INSIDE 192.168.1.40:39301, idle 0:00:00, bytes 485268628, flags Uo
<- offloaded flow
TCP OUTSIDE 192.168.2.40:20 INSIDE 192.168.1.40:34713, idle 0:02:40, bytes 821799360, flags
UFRIO

```

- 百分比基于“show conn”输出。例如，如果总共5个连接通过FTD LINA引擎，其中1个被分流，则报告20%被分流
- 卸载会话的最大限制取决于软件版本(例如，ASA 9.8.3和FTD 6.2.3支持400万个双向 (或800万个单向) 卸载流)
- 如果卸载流的数量达到限制 (例如400万个双向流)，则不会卸载任何新连接，直到从卸载表中删除当前连接

要查看 FP4100/9300 上通过 FTD (分流 + LINA) 的所有数据包，需要在机箱级别启用捕获，如下图所示：



机箱背板捕获显示两个方向。由于 FXOS 捕获架构 (每个方向 2 个捕获点)，每个数据包显示两次，如下图所示：

数据包统计信息：

- 通过 FTD 的数据包总数：30
- 通过 FTD LINA 的数据包数：8
- 分流到 SmartNIC 硬件加速器的数据包数：22

在平台不同于FP4100/FP9300的情况下，所有数据包都由LINA引擎处理，因为不支持流量分流(注

意没有o标志):

```
FP2100-6# show conn addr 192.168.1.40
33 in use, 123 most used
Inspect Snort:
    preserve-connection: 0 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP OUTSIDE 192.168.2.40:80 INSIDE 192.168.1.40:50890, idle 0:00:09, bytes 175, flags UxIO
```

LINA 系统日志仅显示连接建立和连接终止事件：

```
FP2100-6# show log | i 192.168.2.40
Jun 21 2020 14:29:44: %FTD-6-302013: Built inbound TCP connection 6914 for
INSIDE:192.168.1.40/50900 (192.168.11.101/50900) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Jun 21 2020 14:30:30: %FTD-6-302014: Teardown TCP connection 6914 for INSIDE:192.168.1.40/50900
to OUTSIDE:192.168.2.40/80 duration 0:00:46 bytes 565 TCP FINs from OUTSIDE
```

## 使用案例

- 使用 **Prefilter Fastpath** 当您希望完全绕过Snort检测时执行操作。您通常希望对您信任的大数据流（如备份、数据库传输等）执行此操作
- 在FP4100/9300设备上 **Fastpath** 操作会触发flow-offload，只有少数数据包通过FTD LINA引擎。其余数据包由 SmartNIC 处理，从而减少延迟

## 预过滤器策略快速路径操作（内联集）

如果Prefilter Policy Fastpath操作应用于通过内联集（NGIPS接口）的流量，则必须考虑以下几点：

- 规则应用到LINA引擎作为 **trust** 动作
- Snort 引擎不检查流
- 由于流分流不适用于 NGIPS 接口，因此不会发生流分流（硬件加速）

以下是在内联集上应用Prefilter Fastpath操作时数据包跟踪的示例：

```
firepower# packet-tracer input inside tcp 192.168.1.40 12345 192.168.1.50 80 detailed

Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
Forward Flow based lookup yields rule:
in id=0x2ad7ac48b330, priority=501, domain=ips-mode, deny=false
hits=2, user_data=0x2ad80d54abd0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype: log
```

Result: ALLOW

Config:

```
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip object 192.168.1.0 object 192.168.1.0 rule-id
268438531 event-log flow-end
access-list CSM_FW_ACL_ remark rule-id 268438531: PREFILTER POLICY: PF1
access-list CSM_FW_ACL_ remark rule-id 268438531: RULE: 1
```

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x2ad9f9f8a7f0, priority=12, domain=permit, trust
hits=1, user_data=0x2ad9b23c5d40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any
dst ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any
```

Phase: 3

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

Ingress interface inside is in NGIPS inline mode.

Egress interface outside is determined by inline-set configuration

Phase: 4

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 7, packet dispatched to next module

Module information for forward flow ...

```
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat
```

Module information for reverse flow ...

```
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat
```

Result:

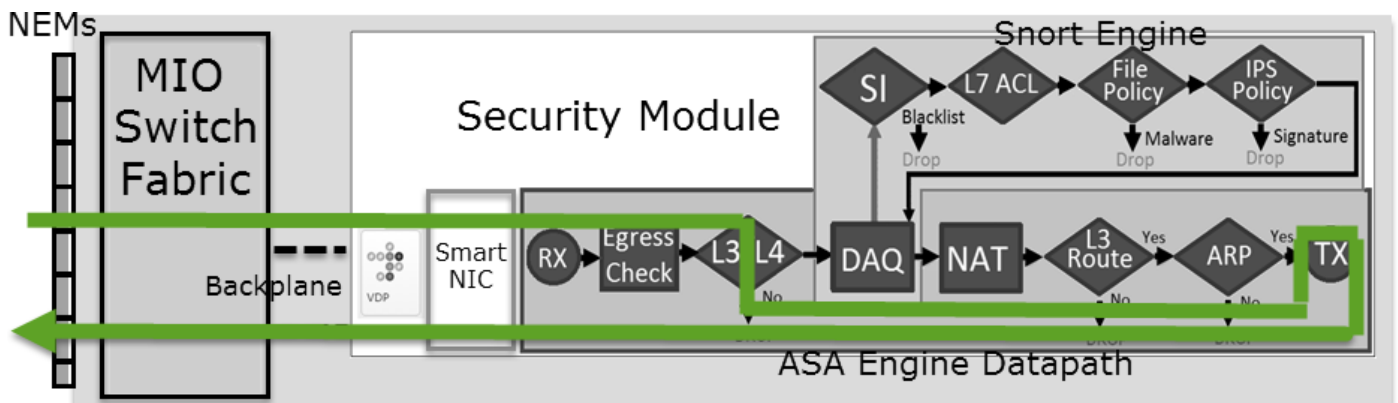
input-interface: inside

input-status: up

input-line-status: up

Action: allow

这是数据包路径的可视表示：



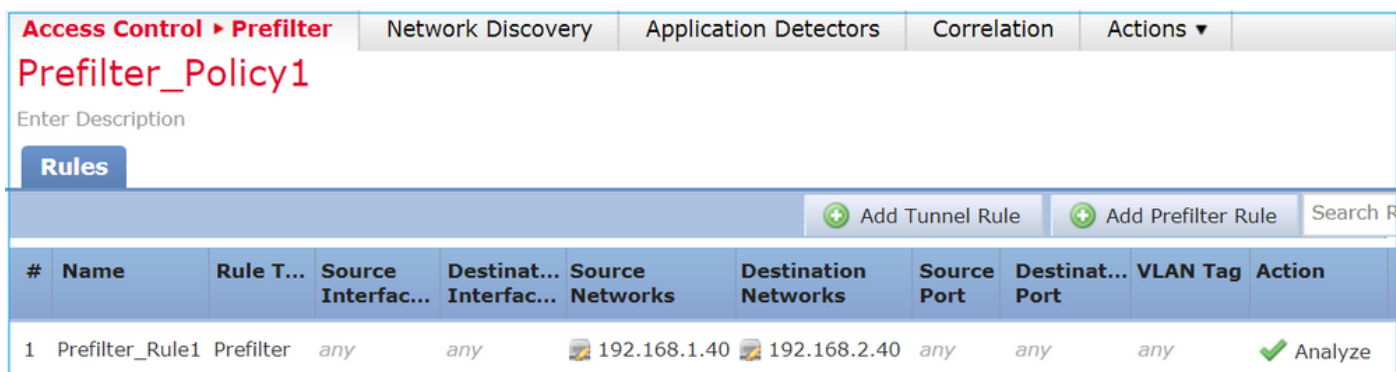
## 预过滤器策略快速路径操作 (带分路器的内联集)

与内联集情况相同

## 预过滤器策略分析操作

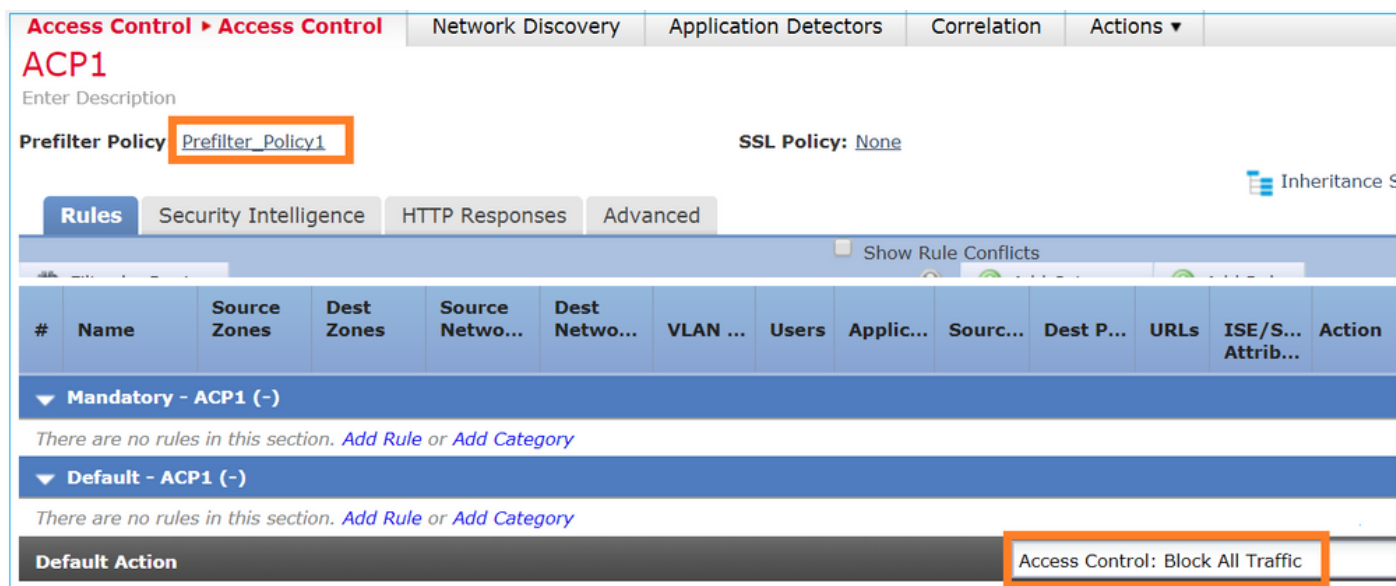
### 场景 1. 使用 ACP 阻止规则进行预过滤器分析

考虑包含分析规则的预过滤器策略，如下图所示：



#	Name	Rule T...	Source Interfac...	Destinat...	Source Networks	Destination Networks	Source Port	Destinat...	VLAN Tag	Action
1	Prefilter_Rule1	Prefilter	any	any	192.168.1.40	192.168.2.40	any	any	any	Analyze

ACP仅包含设置为的默认规则 Block All Traffic 如图所示:



#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S...	Action
Mandatory - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action												Access Control: Block All Traffic	

这是FTD Snort引擎 (ngfw.rules文件) 中部署的策略：

```
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268435460 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any (tunnel -1)
268435459 allow any any 1025-65535 any any 3544 any 17 (tunnel -1)
268435459 allow any any 3544 any any 1025-65535 any 17 (tunnel -1)
268435459 allow any any any any any any any any 47 (tunnel -1)
268435459 allow any any any any any any any any 41 (tunnel -1)
268435459 allow any any any any any any any any 4 (tunnel -1)
# End of tunnel and priority rules.
# Start of AC rule.
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

以下是 FTD LINA 引擎中部署的策略：

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460 (hitcnt=0) 0xb788b786
```

验证行为

Packet Tracer显示LINA允许该数据包，将其转发到Snort引擎(由于 permit action)和Snort Engine返回 Block 判定是因为AC的默认操作已匹配。

**注意：** Snort 不根据隧道规则评估流量

当跟踪数据包时，会显示相同的信息：

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

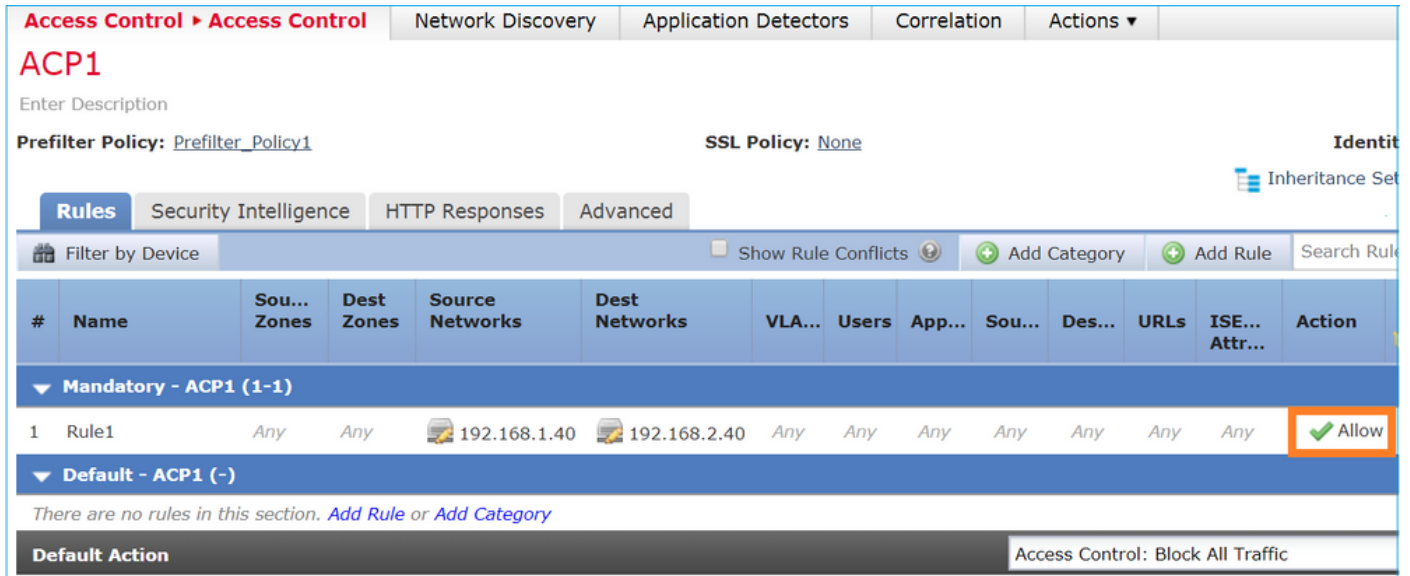
...
Phase: 14
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: block rule, id 268435458, drop
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0, Verdict BLOCKLIST, Blocked by Firewall
Snort Verdict: (block-list) block list this flow

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (firewall) Blocked by the firewall preprocessor
```

**场景 2：使用 ACP 允许规则进行过滤器分析**



如果目标是允许数据包通过 FTD，则需要在 ACP 中添加规则。操作可以是允许或信任，具体取决于目标（例如，如果您要应用必须使用的 L7 检测）Allow 操作），如图所示：



FTD Snort 引擎中部署的策略：

```
# Start of AC rule.
268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any any (log dcfoward flowstart)
# End of AC rule.
```

LINA 引擎中部署的策略：

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=1) 0xb788b786
```

### 验证行为

Packet Tracer显示数据包匹配规则 268435460 和 268435461 在Snort引擎中：

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
  This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```

Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: allow rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
...
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow

```

### 场景 3：使用 ACP 信任规则进行过滤器分析

如果 ACP 包含信任规则，则情况如下图所示：

Snort:

```

# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.

```

LINA :

```

access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=2) 0xb788b786

```

请记住，由于默认情况下已启用SI，因此信任规则部署为 **permit** 在LINA上执行操作，以便至少将几个数据包重定向到Snort引擎进行检查。

验证行为

Packet Tracer显示Snort引擎允许该数据包，并基本上将剩余流量分流到LINA:

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: trust/fastpath rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
...
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

#### 场景 4：使用 ACP 信任规则进行过滤器分析

在此场景中，SI被手动禁用。

在 Snort 中，规则部署如下：

```
# Start of AC rule.
268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any any any any any any any any (log dcforward flowstart)
# End of AC rule.
```

在 LINA 中，该规则部署为“信任”规则。与Analyze Prefilter规则所部署的允许规则（请参阅ACE命中计数）匹配的数据包，且数据包由Snort引擎进行检查：

```
access-list CSM_FW_ACL_ line 3 advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id
268435460 (hitcnt=3) 0xb788b786
```

```
...
access-list CSM_FW_ACL_ line 13 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id
268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
...
access-list CSM_FW_ACL_ line 16 advanced deny ip any any rule-id 268435458 event-log flow-start
(hitcnt=0) 0x97aa021a
```

## 验证行为

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997,
icmpType 8, icmpCode 0
Firewall: trust/fastpath rule, id 268435461, allow
NAP id 1, IPS id 0, Verdict PERMITLIST
Snort Verdict: (fast-forward) fast forward this flow
...
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow
```

## 要点

- 此 **Analyze** 操作在LINA引擎中部署为允许规则。这会影响到转发到Snort引擎进行检查的数据包
- 此 **Analyze** 操作不会在Snort引擎中部署任何规则，因此您需要确保在ACP中配置与Snort匹配的规则
- 这取决于Snort引擎中部署的ACP规则(**block** 与 **allow** 与 **fastpath**)Snort不允许、也不允许全部或少数数据包

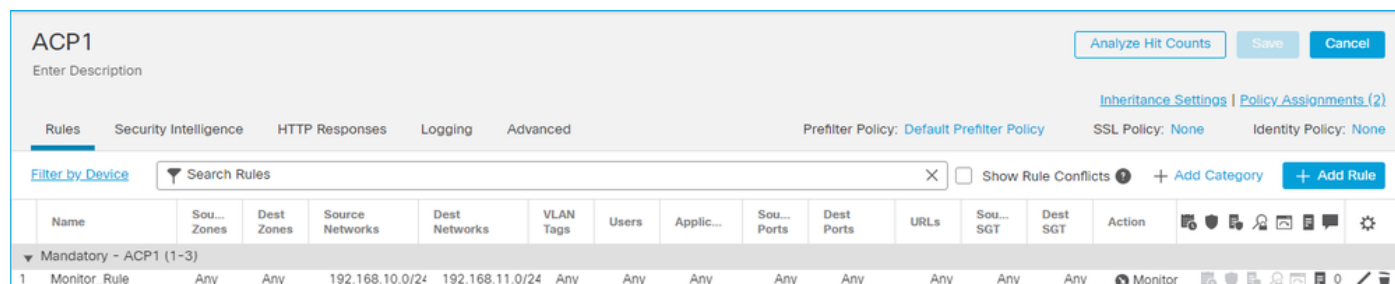
## 使用案例

- 使用案例 **Analyze** 操作是当您在预过滤器策略中有广泛的Fastpath规则，并且希望为特定流放置

一些例外以便由Snort检查它们时

## ACP 监控操作

在 FMC UI 上配置的监控规则：



监控规则在FTD LINA引擎上部署为 **permit** 操作和Snort引擎作为 **audit** 动作。

```
firepower# show access-list
```

```
...
access-list CSM_FW_ACL_ line 10 advanced permit ip 192.168.10.0 255.255.255.0 192.168.11.0
255.255.255.0 rule-id 268438863 (hitcnt=0) 0x61bbaf0c
```

Snort 规则：

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
...
# Start of AC rule.
268438863 audit any 192.168.10.0 24 any any 192.168.11.0 24 any any any (log dcfoward flowend)
# End rule 268438863
```

## 要点

- 监控规则不丢弃或允许流量，但生成连接事件。根据后续规则检查数据包，允许或丢弃该数据包
- FMC Connection Events显示数据包与2条规则匹配：



System support trace 输出显示数据包同时符合两个规则：

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
```

Please specify a client IP address: **192.168.10.50**  
 Please specify a client port:  
 Please specify a server IP address: **192.168.11.50**  
 Please specify a server port:  
 Monitoring packet tracer and firewall debug messages

```
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 419031630
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 new firewall session
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 Starting AC with minimum 2, 'Monitor_Rule',
and IPPProto first with zone          s -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0,          svc 0, payload 0,
client 0, misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 2, 'Monitor_Rule', action
Audit
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 match rule order 3, 'trust_L3-L4', action
Trust
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 MidRecovery data sent for rule id:
268438858,rule_action:3, rev id:1078          02206, rule_match flag:0x2
```

## 使用案例

用于监控网络活动并生成连接事件

## ACP 交互式阻止操作

在 FMC UI 上配置的交互式阻止规则：

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action
▼ Mandatory - ACP1 (1-4)													
1	Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block
2	Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Interactive Block

交互式阻止规则在FTD LINA引擎上部署为 **permit** 作为旁路规则对Snort引擎执行操作：

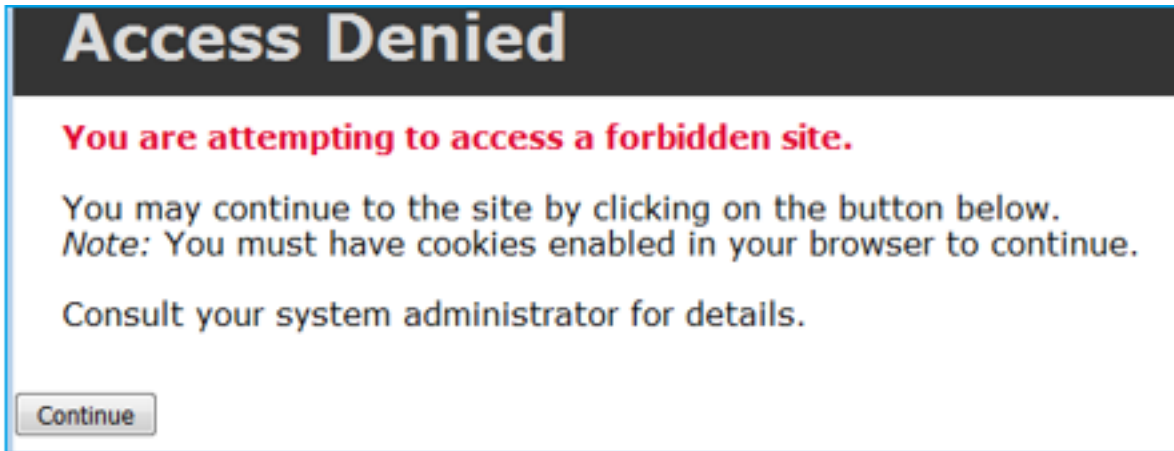
```
firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=3) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0
```

Snort 引擎：

```
admin@firepower:~$ cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules
...
# Start of AC rule.
268438864 bypass any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
```

```
268438865 bypass any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

交互式阻止规则提示用户目的地已被禁止



默认情况下，防火墙允许绕过阻止 600 秒：

Rules	Security Intelligence	HTTP Responses	Logging	Advanced
<b>General Settings</b>				
Maximum URL characters to store in connection events				1024
Allow an Interactive Block to bypass blocking for (seconds)				600
Retry URL cache miss lookup				Yes
Enable Threat Intelligence Director				Yes
Inspect traffic during policy apply				Yes

如果 `system support trace` 输出可以看到防火墙最初阻止流量并显示阻止页面：

```
> system support trace
...
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 983273680, ack 2014879580
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application unknown (0)
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 Starting AC with minimum 2, 'Inter-Block-Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589, misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 match rule order 2, 'Inter-Block-Rule1',
action Interactive
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 bypass action sending HTTP interactive response of 1093 bytes
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-Block-Rule1', drop
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions queue, drop
```

```

192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 22, NAP id 1, IPS id 0, Verdict
BLACKLIST
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ

```

用户选择 **Continue** ( 或刷新浏览器页面 ) debug显示数据包被同一规则允许 , 该规则模仿并 **Allow** 操作 :

```

192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1357413630, ack
2607625293
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 match rule order 2, 'Inter-Block-Rule1',
action Interactive
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 bypass action interactive bypass
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 allow action
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 8, NAP id 1, IPS id 0, Verdict
PASS

```

## 使用案例

向 Web 用户显示警告页面并为他们提供继续的选项。

## ACP 交互式阻止并重置操作

在 FMC UI 上配置的“交互式阻止并重置”规则 :

Name	Sour... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Appli...	Sour... Ports	Dest Ports	URLs	Sour... SGT	Dest SGT	Action
1 Inter-Block-Rule1	Any	Any	192.168.10.0/24	192.168.11.50	Any	Any	Any	Any	TCP (6):80	Any	Any	Any	Interactive Block with reset
2 Inter-Block_Rule2	Any	Any	192.168.10.0/24	192.168.11.51	Any	Any	HTTP	Any	Any	Any	Any	Any	Interactive Block with reset

Interactive Block with reset规则在FTD LINA引擎上部署为 **permit** 作为重置规则对Snort引擎执行操作和操作 :

```

firepower# show access-list
...
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=13) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced permit ip 192.168.10.0 255.255.255.0 host 192.168.11.51
rule-id 268438865 (hitcnt=0) 0x622350d0

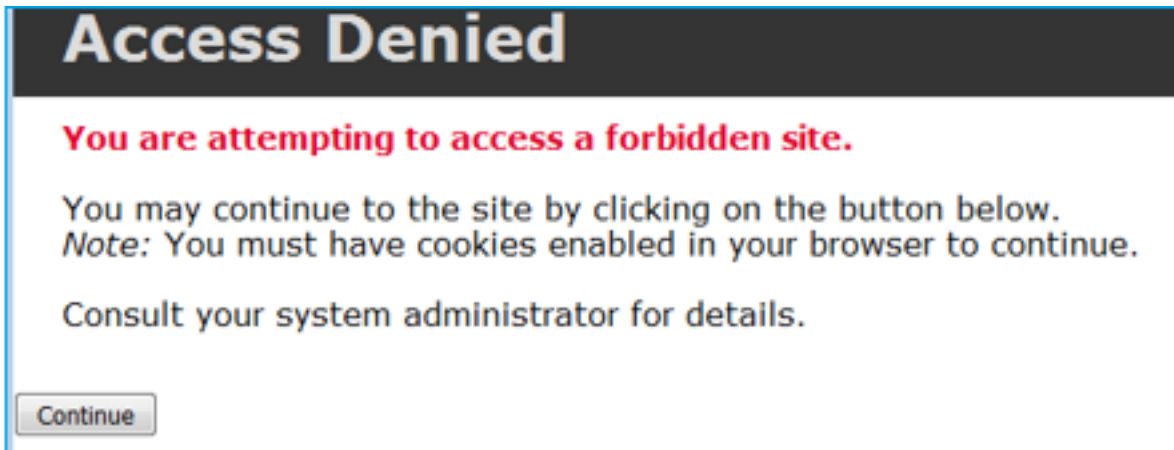
```



Snort 引擎：

```
# Start of AC rule.
268438864 intreset any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865 intreset any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1)
(ip_protos 6, 17)
# End rule 268438865
```

与Block with Reset类似，用户可以选择 **Continue** 选项：



在 Snort 调试中，交互式重置中显示的操作如下所示：

```
> system support trace
```

```
Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.52
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3232128039
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 new firewall session
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0 -> 0, vlan 0, source sgt type: 0, source
sgt tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest sgt tag: 0, svc 0, payload 0, client 0,
misc 0, user 9999997, icmpType 0, icmpCode 0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 MidRecovery data sent for rule id:
268438864,rule_action:8, rev id:1099034206, rule_match flag:0x0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 HitCount data sent for rule id: 268438864,
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS

192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2228213518, ack
3232128040
```

```
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
PASS
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack
2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 bypass action sending HTTP interactive
response of 1093 bytes
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-
Block-Rule1', drop
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions
queue, drop
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 deleting firewall session flags = 0x800,
fwFlags = 0x1002
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict
BLACKLIST
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 ==> Blocked by Firewall
Verdict reason is sent to DAQ
```

此时，阻止页面显示给最终用户。如果用户选择 **Continue** (或刷新网页) 与此次允许流量通过的规则匹配：

```
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1593478294, ack
3135589307
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 Starting AC with minimum 2, 'Inter-Block-
Rule1', and IPProto first with zones -1 -> -1, geo 0(0) -> 0, vlan 0, source sgt type: 0, sgt
tag: 0, ISE sgt id: 0, dest sgt type: 0, ISE dest_sgt_tag: 0, svc 676, payload 0, client 589,
misc 0, user 9999997, min url-cat-list 0-0-0, url http://192.168.11.50/, xff
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 match rule order 2, 'Inter-Block-Rule1',
action Interactive Reset
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 bypass action interactive bypass
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 allow action
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1',
allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-
Block-Rule1', allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict
PASS
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3135589307, ack
1593478786
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
```

```
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1', allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-Block-Rule1', allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0, Verdict PASS
```

“交互式阻止并重置”规则向非 Web 流量发送 TCP RST :

```
firepower# show cap CAPI | i 11.50
 2: 22:13:33.112954      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: S
3109534920:3109534920(0) win 29200 <mss 1460,sackOK,timestamp 3745225378 0,nop,wscale 7>
 3: 22:13:33.113626      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: S
3422362500:3422362500(0) ack 3109534921 win 8192 <mss 1380,nop,wscale 8,sackOK,timestamp
53252448 3745225378>
 4: 22:13:33.113824      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362501 win 229 <nop,nop,timestamp 3745225379 53252448>
 5: 22:13:33.114953      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362501:3422362543(42) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 6: 22:13:33.114984      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362543:3422362549(6) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 7: 22:13:33.114984      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P
3422362549:3422362570(21) ack 3109534921 win 256 <nop,nop,timestamp 53252448 3745225379>
 8: 22:13:33.115182      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362543 win 229 <nop,nop,timestamp 3745225381 53252448>
 9: 22:13:33.115411      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362549 win 229 <nop,nop,timestamp 3745225381 53252448>
10: 22:13:33.115426      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack
3422362570 win 229 <nop,nop,timestamp 3745225381 53252448>
12: 22:13:34.803699      802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: P
3109534921:3109534931(10) ack 3422362570 win 229 <nop,nop,timestamp 3745227069 53252448>
13: 22:13:34.804523      802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: R
3422362570:3422362570(0) ack 3109534931 win 0
```

## FTD辅助连接和 针孔

在旧版本 ( 例如6.2.2、6.2.3等 ) 中 , 如果您使用 Trust 动作.在最新版本中 , 此行为已更改 , 并且 Snort引擎会打开针孔 , 即使 Trust 动作.

## FTD 规则准则

- 对大型流使用预过滤器策略快速路径规则 , 以减少通过设备的延迟
  - 对基于 L3/L4 条件必须阻止的流量使用预过滤器阻止规则
  - 如果要绕过许多 Snort 检查 , 但仍要利用身份策略、QoS、SI、应用检测、URL 过滤等功能 , 可使用 ACP 信任规则
  - 使用以下准则将影响较少防火墙性能的规则置于访问控制策略的顶部 :
1. 块规则 ( 第1-4层 ) — 预过滤器块
  2. 允许规则 ( 第 1-4 层 ) - 预过滤器快速路径
  3. ACP 阻止规则 ( 第 1-4 层 )
  4. 信任规则 ( 第 1-4 层 )
  5. 阻止规则 ( 第 5-7 层 - 应用检测、URL 过滤 )
  6. 允许规则 ( 第 1-7 层 - 应用检测、URL 过滤、入侵策略/文件策略 )
  7. 阻止规则 ( 默认规则 )

- 避免过多日志记录 ( 在开始或结束时记录日志 , 避免同时在这两个时间记录日志 )
- 了解规则扩展 , 检查LINA中的规则数

```
firepower# show access-list | include elements
access-list CSM_FW_ACL; 7 elements; name hash: 0x4a69e3f3
```

## 摘要

### 预过滤器操作

Rule Action (FMC UI)	LINA Action	Snort Action	Notes
Fastpath	Trust	Fastpath	Static Flow Offload to SmartNIC (4100/9300). <b>No packets</b> are sent to Snort engine.
Analyze	Permit	-	The ACP rules are checked. <b>Few or all packets</b> are sent to Snort engine for inspection. Traffic is allowed or dropped based on Snort engine verdict
Block (Prefilter)	Deny	-	Early drop by FTD LINA <b>No packets</b> are sent to Snort engine

### ACP 操作

Rule Action (FMC UI)	Additional Conditions	LINA Action	Snort Action	Notes
Block	The rule matches L3/L4 conditions	Deny	Deny	
Block	The rule has L7 conditions	Permit	Deny	
Allow		Permit	Allow	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, or ID) enabled	Permit	Fastpath	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, and ID) disabled	Trust	Fastpath	Static Flow Offload (4100/9300)
Monitor		Permit	Audit	Monitor Rule doesn't drop or permit traffic, but it generates a Connection Event. The packet is checked against subsequent rules and it is either allowed or dropped
Block with reset		Permit	Reset	When a packet matches Block with reset rule FTD sends a TCP Reset packet or an ICMP Type 3 Code 13 Destination Unreachable (Administratively filtered) message
Interactive Block		Permit	Bypass	Interactive Block Rule prompts the user that the destination is forbidden If bypassed, by default, the firewall allows to bypass the block for 600 seconds
Interactive Block with reset		Permit	Intreset	Same as Interactive Block with the addition of a TCP RST in case of non-web traffic

**注意：**从6.3 FTD软件代码开始，动态流量分流可以分流满足其他条件的连接，例如需要Snort检查的可信数据包。有关详细信息，请参阅《Firepower 管理中心配置指南》中的“分流大型连接（流）”部分

## 相关信息

- [FTD 访问控制规则](#)

- [FTD 预过滤和预过滤器策略](#)
- [分析 Firepower 防火墙捕获以有效排除网络问题](#)
- [使用 Firepower 威胁防御 \(FTD\) 捕获和 packet-tracer](#)
- [通过 FMC 在 FTD 上配置日志记录](#)
- [技术支持和文档 - Cisco Systems](#)
- [分流大型连接](#)

## 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）。