明确FTD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
- 相关产品

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Packet Tracer和Capture with Trace选项

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

本文档可以与以下硬件和软件版本配合使用：

- 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。

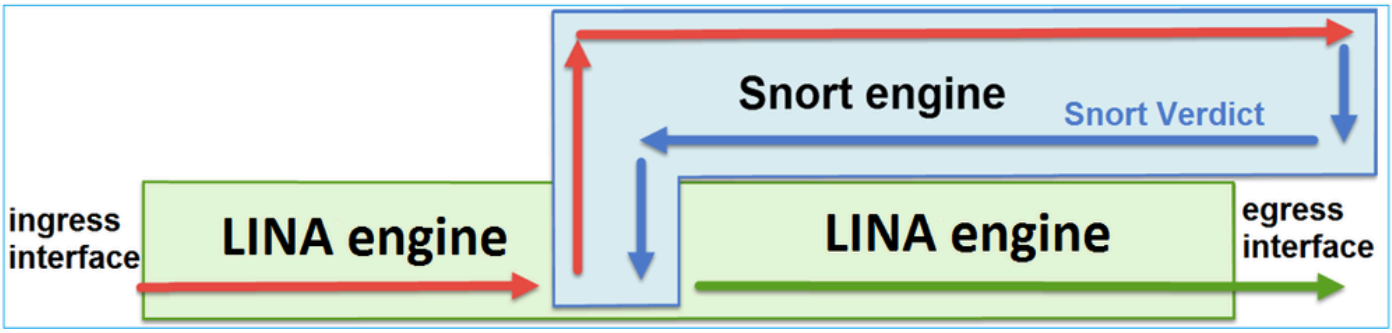
背景信息

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是一个统一的软件映像，包含两个主要引擎：

- LINA 引擎
- Snort 引擎

此图显示了两个引擎如何交互：



- 数据包进入入口接口并由 LINA 引擎处理.
- 如果FTD策略需要该数据包，则由Snort引擎检查该数据包。
- 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

当使用机外（远程）管理或使用本地Firepower设备管理器(FDM)时，FTD策略在FMC上配置。在这两种情况下，ACP 均部署为：

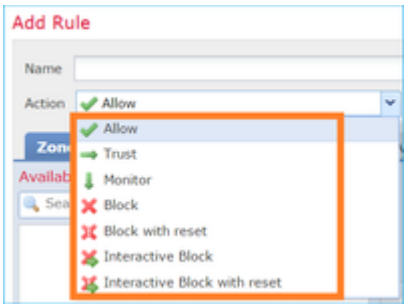
- FTD LINA引擎的名为CSM_FW_ACL_的全局访问控制列表(ACL)。
- FTD Snort 引擎的访问控制 (AC) 规则 ，位于 /ngfw/var/sf/detection_engines/<UUID>/ngfw.rules 文件中.

配置

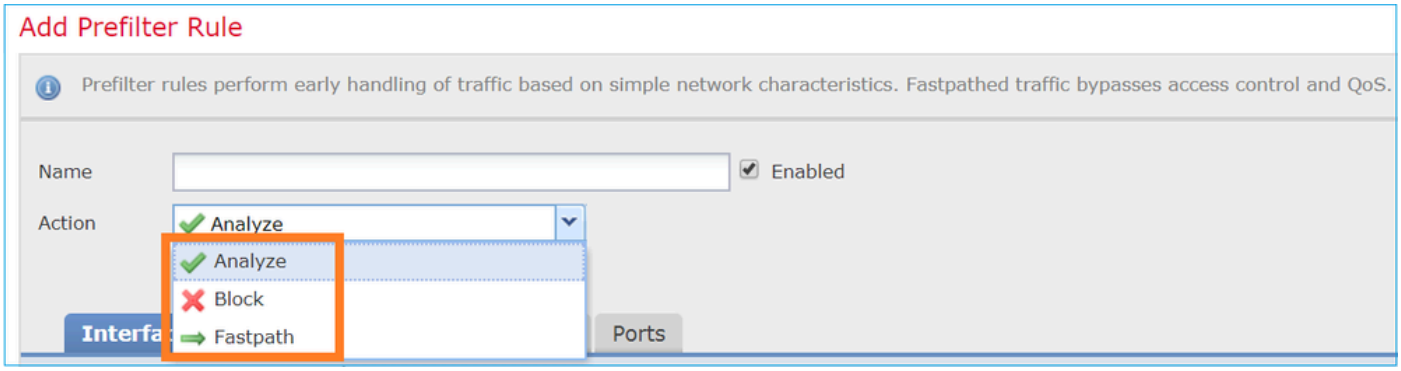
ACP 可用操作

FTD ACP包含一个或多个规则，并且每个规则可以具有下列操作之一：

- 允许
- 信任
- 监控
- 阻止
- 阻止并重置
- 交互式块
- 交互式阻止并重置



同样，预过滤器策略可以包含一个或多个规则和可能的操作：



ACP 和预过滤器策略如何交互

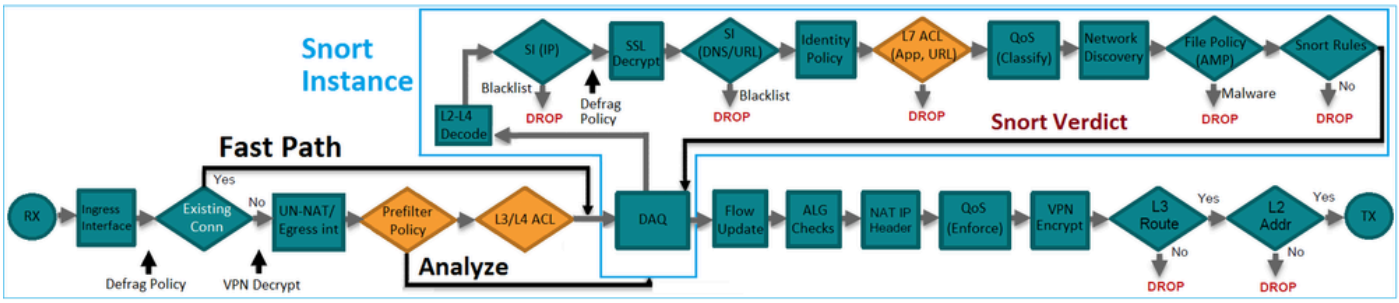
预过滤器策略在6.1版本中引入，主要用于两个目的：

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。更具体地说，对于隧道流量（例如GRE），预过滤器策略中的规则始终对外部报头起作用。而ACP中的规则始终适用于内部会话（内部报头）。

隧道流量是指以下协议：

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

早期访问控制(EAC)允许流量完全绕过Snort引擎：



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：

```
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
```

Prefilter Rules

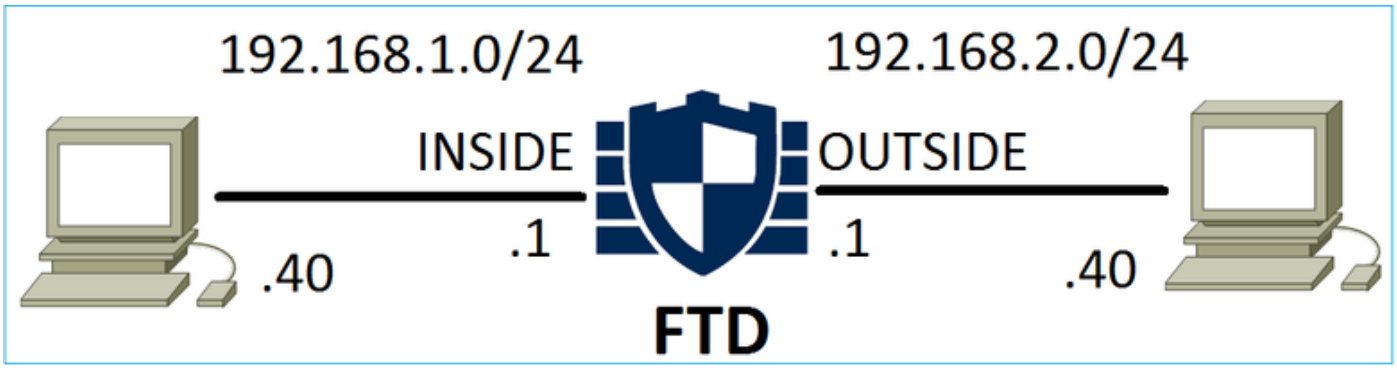
Tunnel Prefilter Rules

L3/L4 ACEs

注意：预过滤器v/s ACP规则=应用的第一个匹配项。

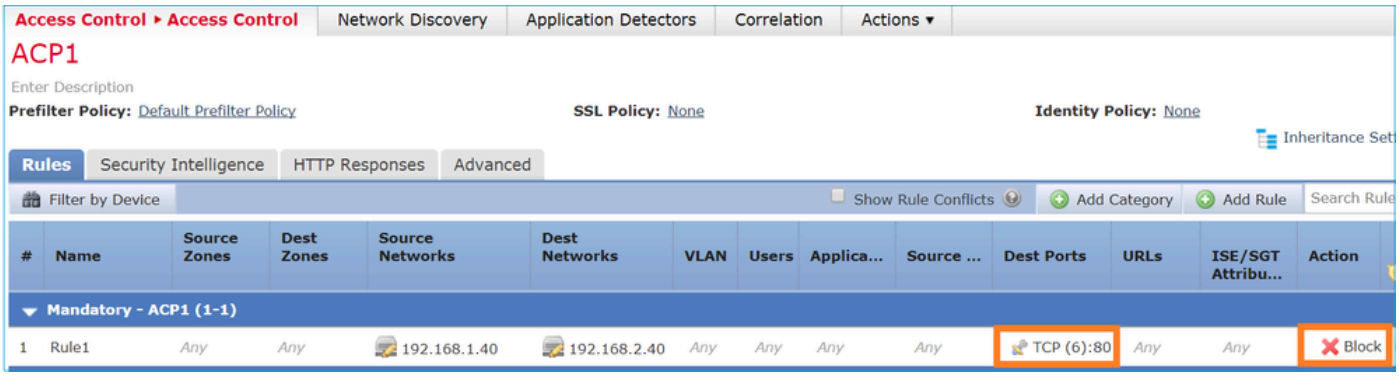
ACP 阻止操作

考虑拓扑：



场景 1. 提前 LINA 丢弃

ACP包含使用L4条件（目标端口TCP 80）的阻止规则：



Snort 中部署的策略：

<#root>

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，规则作为deny操作推送：

<#root>

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) 0x614

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，并且无法到达Snort引擎或目标：

<#root>

```
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
```

<#root>

```
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 1
   2: 11:08:12.672435  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1
   3: 11:08:18.672847  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1
   4: 11:08:30.673610  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1
```

<#root>

```
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 e

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

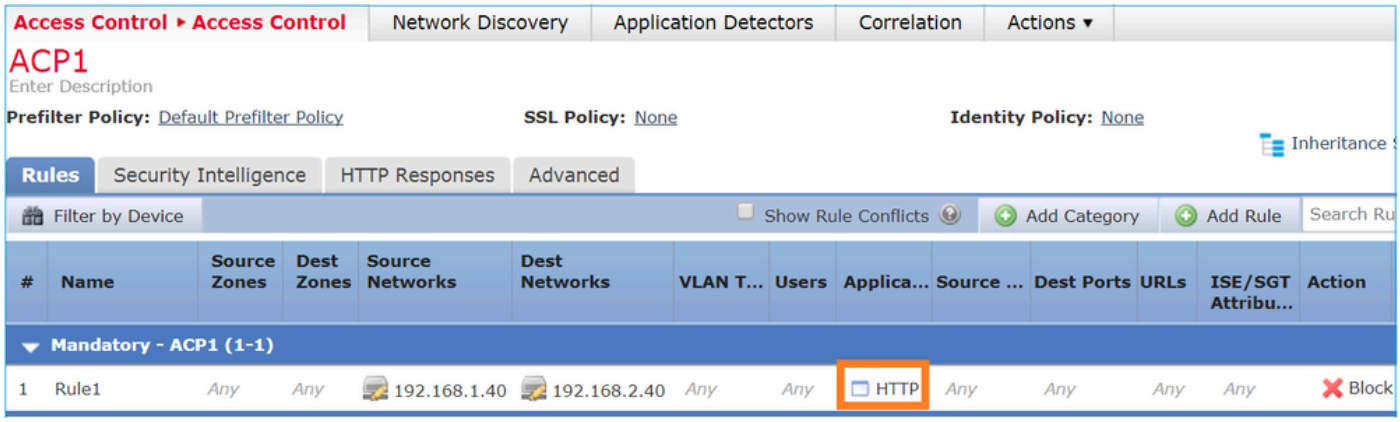


Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop

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：



Snort 中部署的策略：

<#root>

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

在LINA中部署的策略：

注意：由于LINA引擎无法确定会话使用HTTP，因此将该规则作为permit操作推送。在FTD上，应用检测机制位于Snort引擎中。

<#root>

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作为条件的块规则，实际数据包的跟踪显示，由于Snort引擎判定，会话被LINA引擎丢弃。

注意：为了让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，少数数据包可以通过FTD并传输到目的地。根据Access Policy > Advanced > Intrusion Policy used before Access Control rule is determined选项，允许的数据包仍会接受入侵策略检查。

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：

```
<#root>
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
   5: 11:31:20.428887  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack 1283931031
 ...
```

出口捕获显示：

```
<#root>

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 1
   2: 11:31:19.826312  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack 1163713180 wi
   3: 11:31:23.426049  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack 1163713180 wi
   4: 11:31:29.426430  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack 1163713180 wi
   5: 11:31:41.427208  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack 1163713180 wi
```

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

```
<#root>

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
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：

```
<#root>

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

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：

<#root>

```
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 ht

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
```

您也可以从FTD CLISH模式运行system support trace命令。此工具提供两个功能：

- 它显示每个数据包在发送到数据采集库(DAQ)时的Snort判定，在LINA中可以看到。DAQ 是位于 FTD LINA 引擎和 Snort 引擎之间的组件.
- 它允许您同时运行system support firewall-engine-debug，以查看Snort引擎本身发生的情况。

⚠ 警告：您必须在Cisco支持的指导下使用system support命令，但system support ssl-client-hello-commands指南中记录的命令除外，该指南一般使用。

此外，请始终使用适当的过滤器，不要让命令无限期地运行，因为它可能会影响设备性能。

以下为示例输出：

```
<#root>

>

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 wit
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vla
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 wit
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vla
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 wit
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0,

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 ===>
```

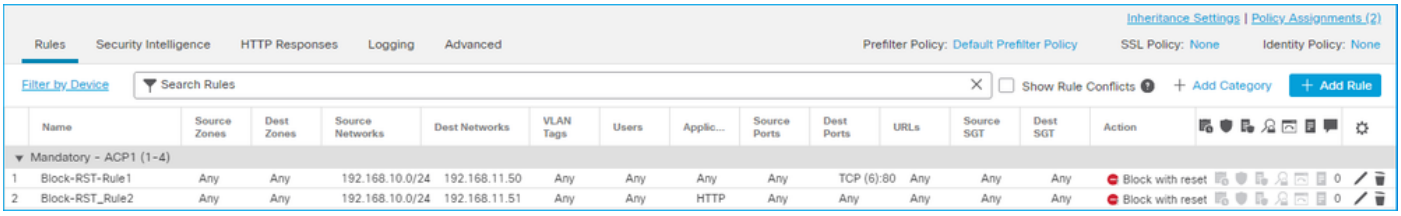
Blocked by Firewall

摘要:

- ACP阻止操作在LINA引擎中部署为允许或拒绝规则，具体取决于规则条件。
- 如果条件是L3/L4，则LINA引擎会阻止数据包。对于TCP，第一个数据包(TCP SYN)被阻止。
- 如果条件是L7，则将数据包转发到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。根据Access Policy > Advanced > Intrusion Policy used before Access Control rule is determined选项，允许的数据包仍会接受入侵策略检查。

ACP 阻止并重置操作

在 FMC UI 上配置的“阻止并重置”规则：



带重置规则的块作为permit部署在FTD LINA引擎上，作为reset规则部署到Snort引擎：

<#root>

```
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：

<#root>

```
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
```

当数据包匹配具有重置规则的块时，FTD会发送TCP Reset数据包或ICMP Type 3 Code 13 Destination Unreachable(Administratively filtered)消息：

<#root>

```
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.

请参阅FTD入口接口上捕获的流量：

```
firepower# show capture CAPI
2 packets captured
1: 21:01:00.977259 802.1Q vlan#202 P0 192.168.10.50.41986 > 192.168.11.50.80: S 3120295488:3120295488(0)
2: 21:01:00.978114 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.41986: R 0:0(0) ack 3120295489 w
```

系统支持跟踪输出，在本例中，它显示由于Snort判定而丢弃数据包：

```
<#root>

>

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 (
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',
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 = 0x
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,
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操作相同，但它会立即终止连接。

⚠ 警告：您必须在Cisco支持的指导下使用system support命令，但system support ssl-client-hello-commands指南中记录的命令除外，该指南一般使用。

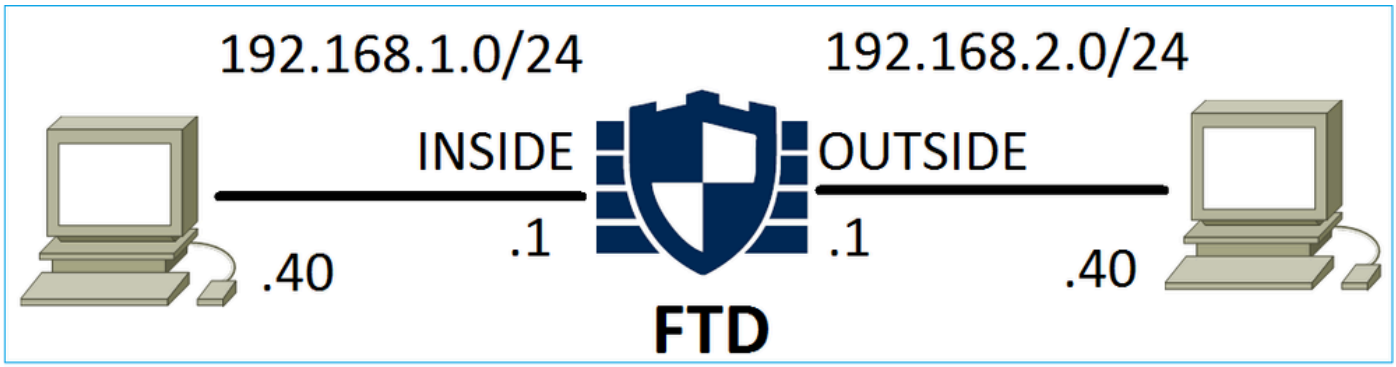
此外，请始终使用适当的过滤器，不要让命令无限期地运行，因为它可能会影响设备性能。

ACP 允许操作

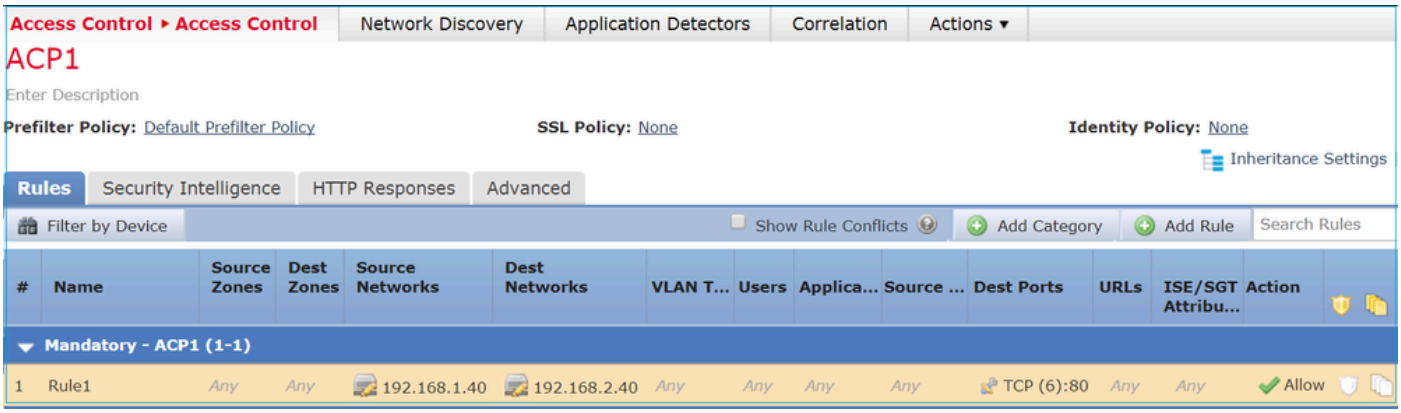
场景 1. ACP 允许操作（L3/L4 条件）

通常，您正在配置Allow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。

请思考以下拓扑：



应用此策略：



Snort 中部署的策略。请注意，该规则作为允许操作部署：

<#root>

```
# Start of AC rule.
268435461
```

allow

```
 any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

LINA引擎中的策略：

注意：规则部署为permit操作，这意味着它重定向到Snort以进行进一步检查。

<#root>

```
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
```

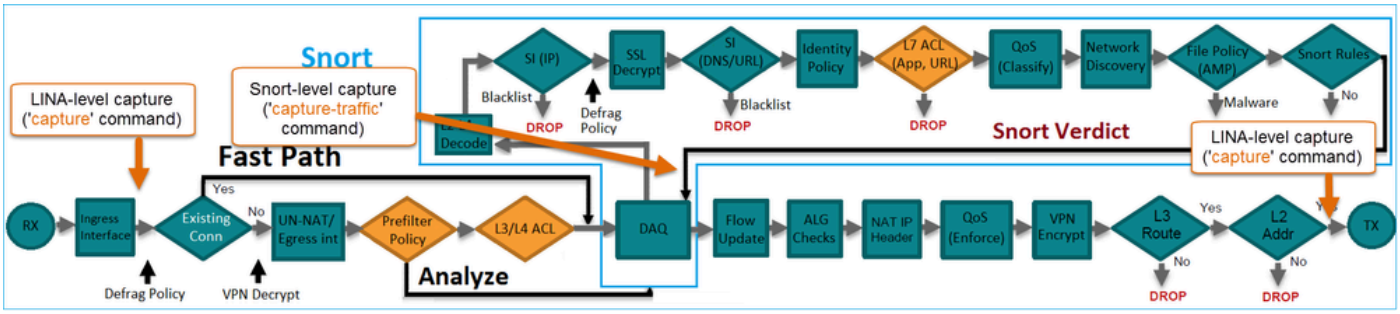
permit

```
 tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id 268435461 (hitcnt=1) 0x641a20c3
```

要查看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
- 使用系统支持跟踪CLISH工具
- 通过在LINA引擎中使用捕获和trace选项，您可以在Snort引擎中选择使用capture-traffic

LINA capture 命令与 Snort capture-traffic 命令：



验证行为

清除Snort统计信息并启用从CLISH的system support trace，然后启动从主机A(192.168.1.40)到主机B(192.168.2.40)的HTTP流。 所有数据包都转发到Snort引擎并接收Snort引擎的PASS判定：

<#root>

```
firepower#
```

clear snort statistics

⚠ 警告：您必须在Cisco支持的指导下使用system support命令，但system support ssl-client-hello-commands指南中记录的命令除外，该指南一般使用。

此外，请始终使用适当的过滤器，不要让命令无限期地运行，因为它可能会影响设备性能。

<#root>

```
>

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
```

Pass Packets计数器增加：

<#root>

```
>
```

```
show snort statistics


Packet Counters:

  Passed Packets                                   54


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

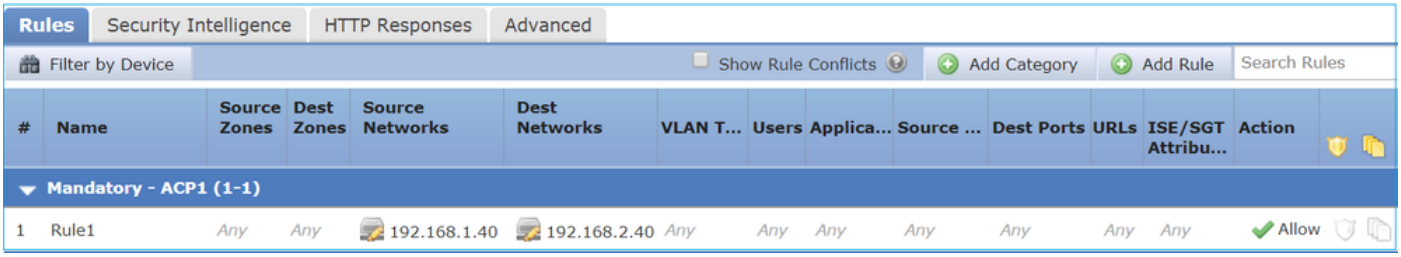
Flow Counters:
  Fast-Forwarded Flows                              0
  Blocklisted Flows                                 0
...
```

Passed Packets = Snort引擎检查

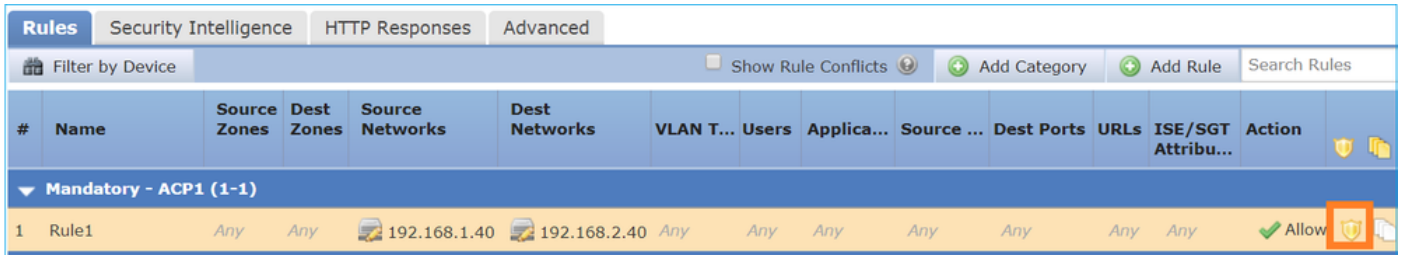
场景 2： ACP 允许操作（L3-7 条件）

部署Allow规则时会出现类似行为。

只有L3/L4条件：

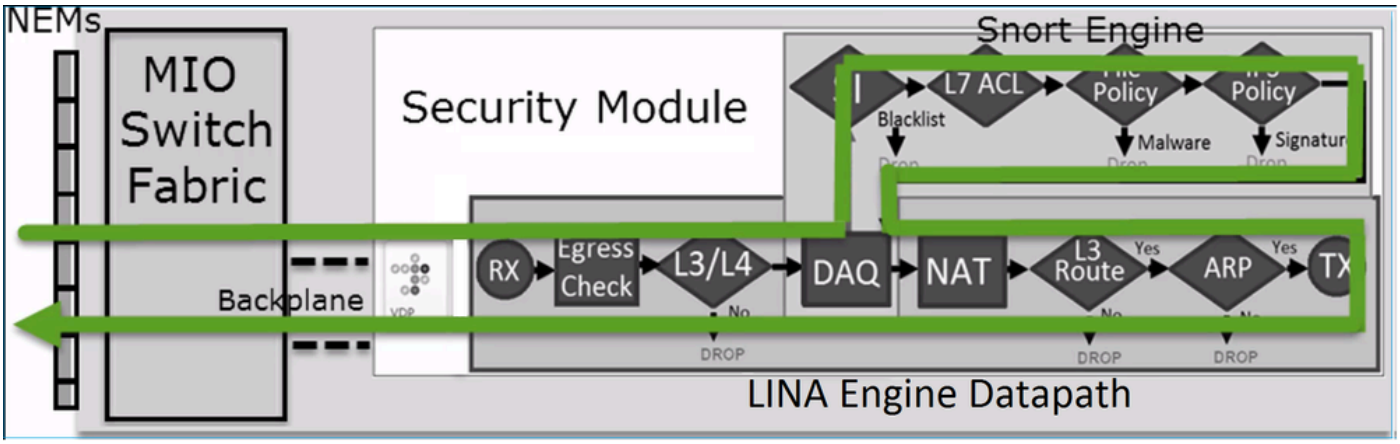


L7条件（例如，入侵策略、文件策略、应用）：



摘要

总之，当Allow规则匹配时，这是部署在FP4100/9300上的FTD处理流量的方式：



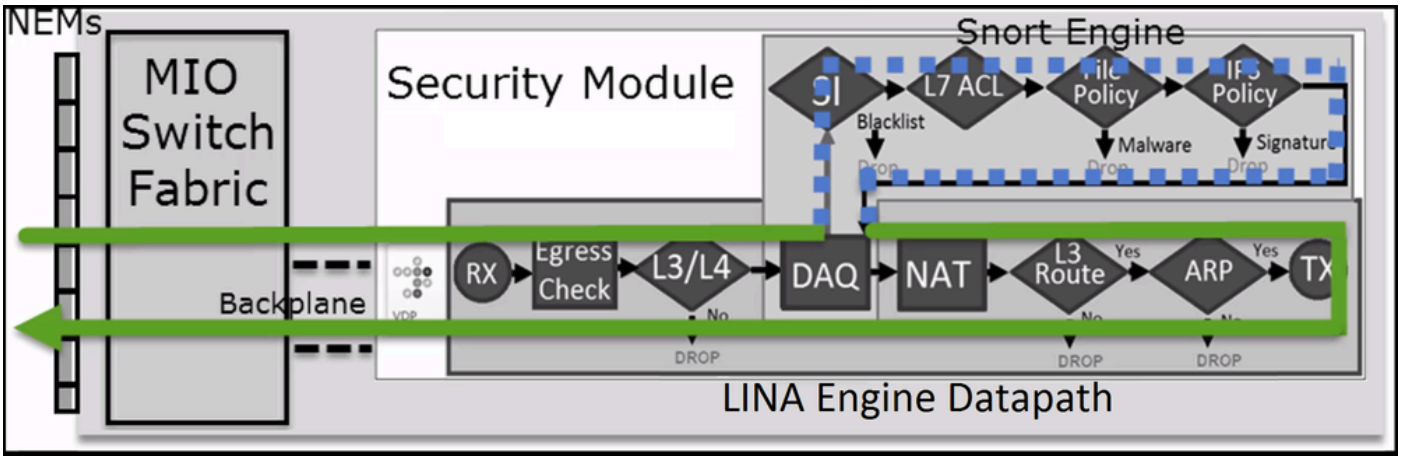
注意：管理输入输出 (MIO) 是 Firepower 机箱的管理引擎。

场景 3： Snort 快速转发判定（使用“允许”规则）

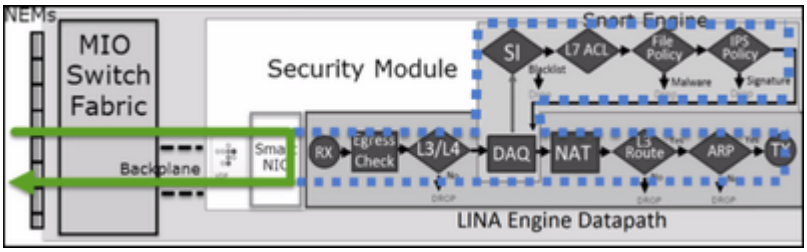
在某些特定情况下，FTD Snort引擎会提供PERMITLIST判定（快速转发），剩余流量会卸载到LINA引擎（在某些情况下，会卸载到HW加速器 — SmartNIC）。 即：

- 未配置 SSL 策略的 SSL 流量
- 智能应用旁路(IAB)

请参阅数据包路径的可视化表示：



在某些情况下：



要点

- 允许规则在Snort中部署为allow，在LINA引擎中部署为permit。
- 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

仅当需要Snort引擎进行L7检测时，才配置Allow规则，例如：

- 入侵策略
- 文件策略

ACP 信任操作

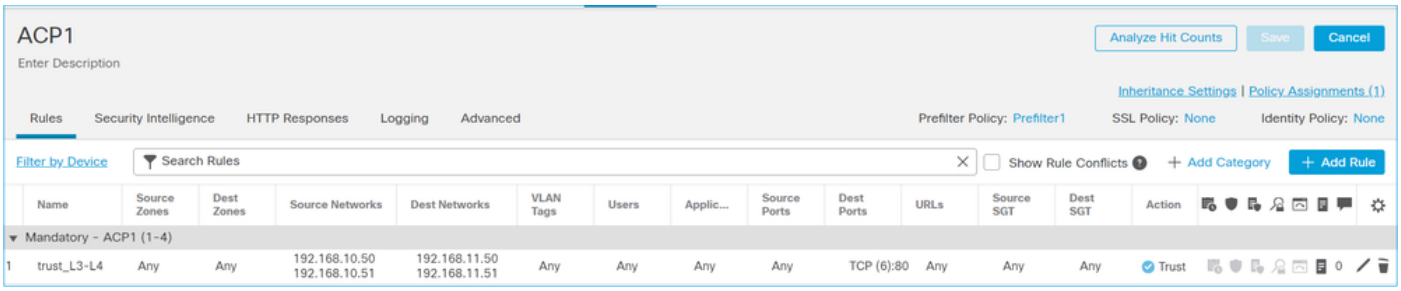
场景 1. ACP 信任操作

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 Action。

拓扑：



已配置的策略：



在部署到FTD Snort引擎时，请参阅信任规则：

<#root>

```
# 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：

<#root>

```
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-g
  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：

启用 system support trace，然后发起从主机 A (192.168.10.50) 到主机 B (192.168.11.50) 的 HTTP 会话。

⚠ 警告：您必须在Cisco支持的指导下使用system support命令，但system support ssl-client-hello-commands指南中记录的命令除外，该指南一般使用。

此外，请始终使用适当的过滤器，不要让命令无限期地运行，因为它可能会影响设备性能。

有三个数据包转发到Snort引擎。Snort引擎发送到LINA，PERMITLIST判定将剩余流卸载到LINA引擎：

<#root>

```
>
```

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 (
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', act
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', all
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 (
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-L4', all
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 (
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-L4', all
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

一旦连接终止，Snort引擎将从LINA引擎接收元数据信息并删除会话：

<#root>

```
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 =
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
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleted snort session using 0 bytes; pro
```

Snort引擎捕获显示到达Snort引擎的三个数据包：

<#root>

```
>
```

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, option
```

```
10:26:16.525928 IP 192.168.11.50.80 > 192.168.10.50.42144: Flags [S.], seq 3581351172, ack 3065553466, w
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [.], ack 1, win 229, options [nop,nop,T
```

LINA引擎捕获显示了经过它的流量：

```
<#root>

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 2459891187:24598911
   2: 09:51:19.431648  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: S 2860907367:28609073
   3: 09:51:19.431847  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: . ack 2860907368 win
   4: 09:51:19.431953  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: P 2459891188:24598913
   5: 09:51:19.444816  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: . 2860907368:28609087
   6: 09:51:19.444831  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: . 2860908736:28609101

…
```

来自LINA的数据包跟踪是查看Snort判定的另一种方法。第一个数据包收到了PASS判定：

```
<#root>

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

OUTSIDE接口上TCP SYN/ACK数据包的跟踪：

<#root>

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收到允许列表判定：

<#root>

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

请参阅Snort判定(数据包#3)的完整输出：

```
<#root>

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
```

第四个数据包不会转发到Snort引擎，因为LINA引擎会缓存判定：

```
<#root>

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 164375589:1643
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统计信息证实这一点：

```
<#root>

firepower#

show snort statistics


Packet Counters:


Passed Packets                                                2

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

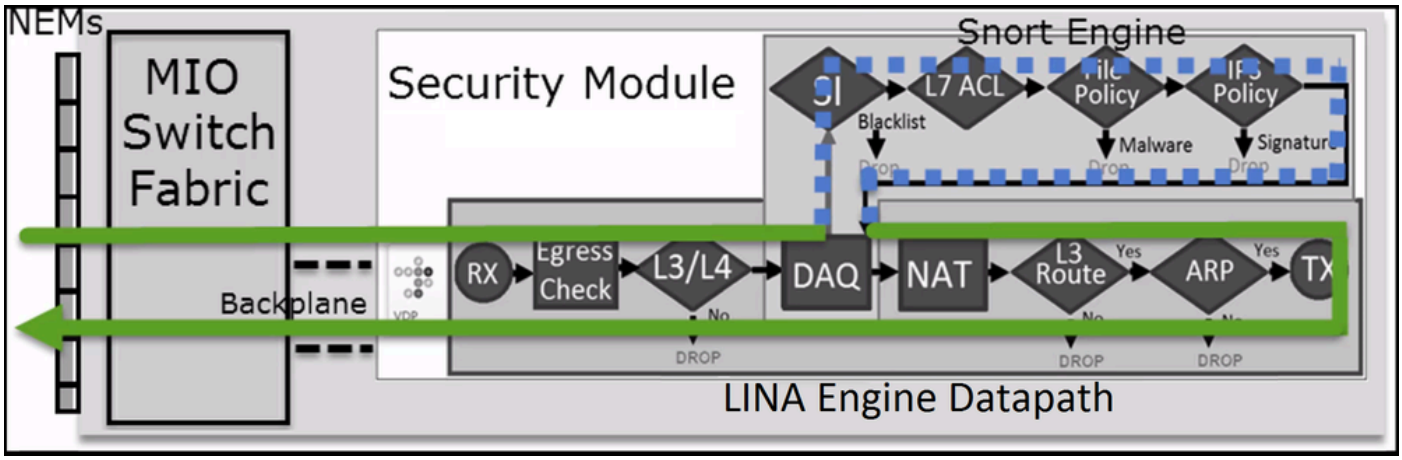
Flow Counters:


Fast-Forwarded Flows                                          1
```

```
  Blacklisted Flows                                                0

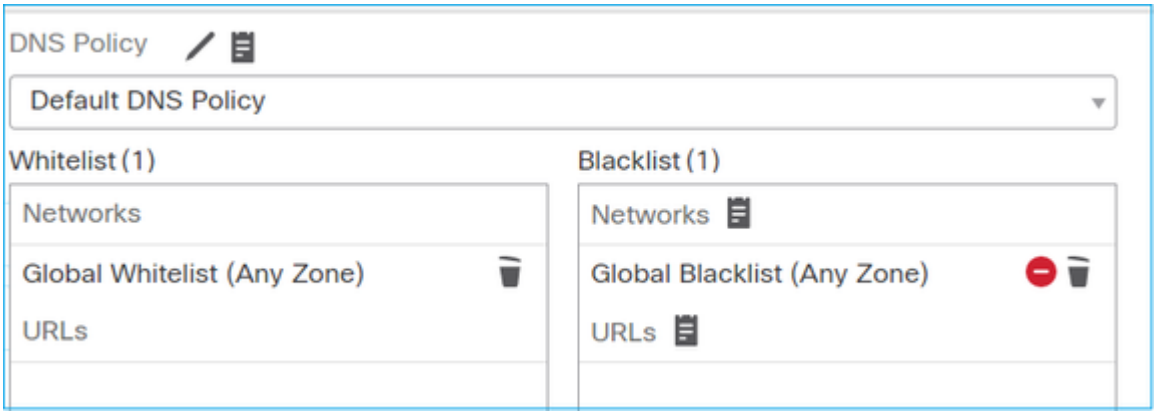
Miscellaneous Counters:
  Start-of-Flow events                                             0
  End-of-Flow events                                               1
  Denied flow events                                               0
  Frames forwarded to Snort before drop                            0
  Inject packets dropped                                           0
```

请参阅具有信任规则的数据包流。Snort引擎会检查一些数据包，其余数据包则通过LINA进行检查：



场景2. ACP信任操作（无SI、QoS和身份策略）

如果希望FTD将安全情报(SI)检查应用于所有流，SI已在ACP级别启用，您可以指定SI源（TALOS、源、列表）。 另一方面，如果要禁用它，可以全局禁用每个ACP的网络的SI、URL的SI和DNS的SI。网络的SI和URL已禁用：



在本例中，“信任”规则作为信任操作部署到 LINA：

<#root>

```
>

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
```

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

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，请注意以下情况：

- 某些数据包通过FTD LINA引擎转发，而剩余流量被分流到SmartNIC（硬件加速器）。
- 不会将数据包转发到Snort引擎。

FTD LINA连接表显示标志"**o**"，表示流已卸载到硬件。另请注意，没有“N”标志。这意味着“no Snort redirection”：

```
<#root>

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 UIO

o
```

Snort统计信息仅显示会话开始和结束时的日志记录事件：

```
<#root>

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                                  1
  End-of-Flow events                                    1
```

FTD LINA日志显示每个会话有两个分流到硬件上的流（每个方向一个）：

```
<#root>

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 (
Sep 27 2017 20:16:05: %ASA-6-805001:

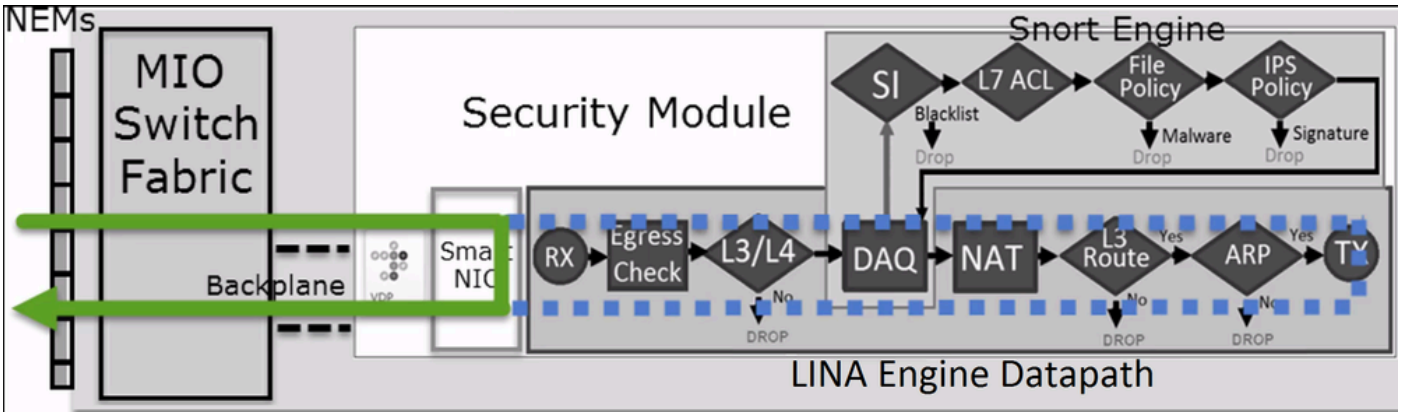
Offloaded TCP Flow for connection 25384 from INSIDE

: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:
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from INSIDE:1
Sep 27 2017 20:16:05: %ASA-6-302014: Teardown TCP connection 25384 for INSIDE:192.168.1.40/32809 to OUT
Sep 27 2017 20:16:05: %ASA-7-609002: Teardown local-host INSIDE:192.168.1.40 duration 0:00:00
```

在LINA中将信任规则部署为信任操作的数据包流。LINA会检查一些数据包，其余数据包被卸载到SmartNIC(FP4100/FP9300):

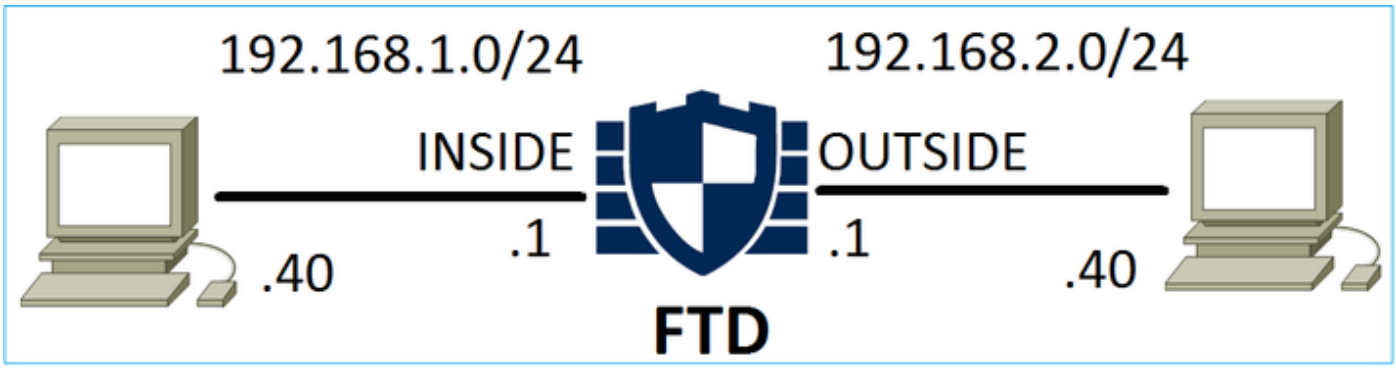


使用案例

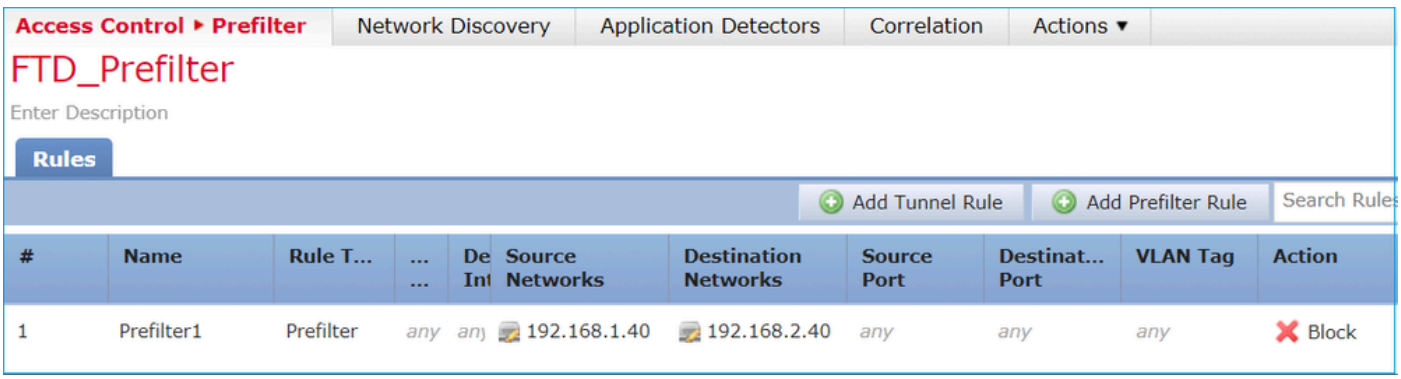
- 当仅需要由Snort引擎检查几个数据包（例如，应用检测、SI检查）且剩余流已卸载到LINA引擎时，必须使用Trust操作。
- 如果在FP4100/9300上使用FTD并希望流量完全绕过Snort检测。然后考虑带有Fastpath操作的预过滤器规则（请参阅本文档的相关部分）。

预过滤器策略阻止操作

考虑拓扑：



请参阅FTD预过滤器策略：



FTD Snort引擎（ngfw.rules文件）中部署的策略：

```
<#root>

# 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：

```
<#root>

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丢弃且从未转发到Snort:

```
<#root>

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
```

```
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：

```
<#root>

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：

```
<#root>
```

```
firepower#

show asp drop

Frame drop:

Flow is denied by configured rule (acl-drop)

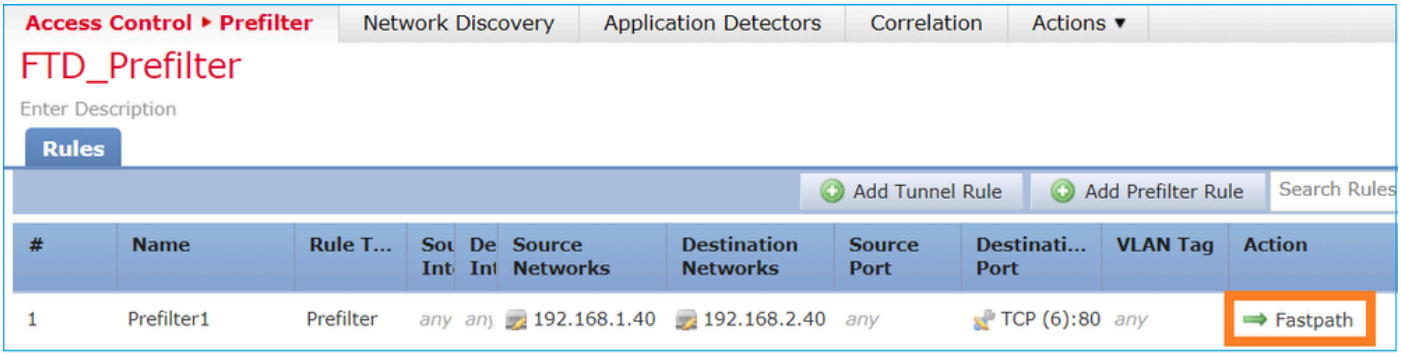
1
```

使用案例

当您想要根据L3/L4条件阻止流量，而不对流量进行额外的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

考虑预过滤器策略规则：



FTD Snort引擎中部署的策略：

```
<#root>

268437506

fastpath

 any any any any any any any any (log dcforward flowend) (tunnel -1)
```

FTD LINA 中部署的策略：

```
<#root>

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) 0xf3410
```

验证行为

当主机A(192.168.1.40)尝试打开到主机B(192.168.2.40)的HTTP会话时，一些数据包通过LINA，其余数据包被卸载到SmartNIC。在本例中，启用firewall-engine-debug的系统支持跟踪显示：

```
<#root>

>

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
```

⚠ 警告：您必须在Cisco支持的指导下使用system support命令，但system support ssl-client-hello-commands指南中记录的命令除外，这些命令用于一般用途。

此外，请始终使用适当的过滤器，不要让命令无限期地运行，因为它可能会影响设备性能。

LINA日志显示卸载的流量：

<#root>

```
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 (19
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捕获显示八个数据包的处理方式：

<#root>

```
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
```

<#root>

```
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 1
   2: 14:45:32.700372  192.168.2.40.80 > 192.168.1.40.32842: S 184794124:184794124(0) ack 3195173119 wi
   3: 14:45:32.700540  192.168.1.40.32842 > 192.168.2.40.80: P 3195173119:3195173317(198) ack 184794125
   4: 14:45:32.700876  192.168.2.40.80 > 192.168.1.40.32842: . 184794125:184795493(1368) ack 3195173317
   5: 14:45:32.700922  192.168.2.40.80 > 192.168.1.40.32842: P 184795493:184796861(1368) ack 3195173317
   6: 14:45:32.701425  192.168.2.40.80 > 192.168.1.40.32842: FP 184810541:184810851(310) ack 3195173317
   7: 14:45:32.701532  192.168.1.40.32842 > 192.168.2.40.80: F 3195173317:3195173317(0) ack 184810852 w
   8: 14:45:32.701639  192.168.2.40.80 > 192.168.1.40.32842: . ack 3195173318 win 2697 <nop,nop,timesta
```

FTD 流分流统计信息显示 22 个数据包分流到硬件：

```
<#root>

firepower#

show flow-offload statistics

 Packet stats of port : 0

     Tx Packet count                 :              22



 Rx Packet count                 :              22

        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
```

您可以使用show flow-offload flow命令查看与分流流相关的其他信息。

```
<#root>

firepower#

show flow-offload flow


Total offloaded flow stats: 2 in use, 4 most used, 20% offloaded, 0 collisions
TCP intfc 103 src 192.168.1.40:39301 dest 192.168.2.40:20, static, timestamp 616063741, packets 33240,
TCP intfc 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 616063760, packets 249140,
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

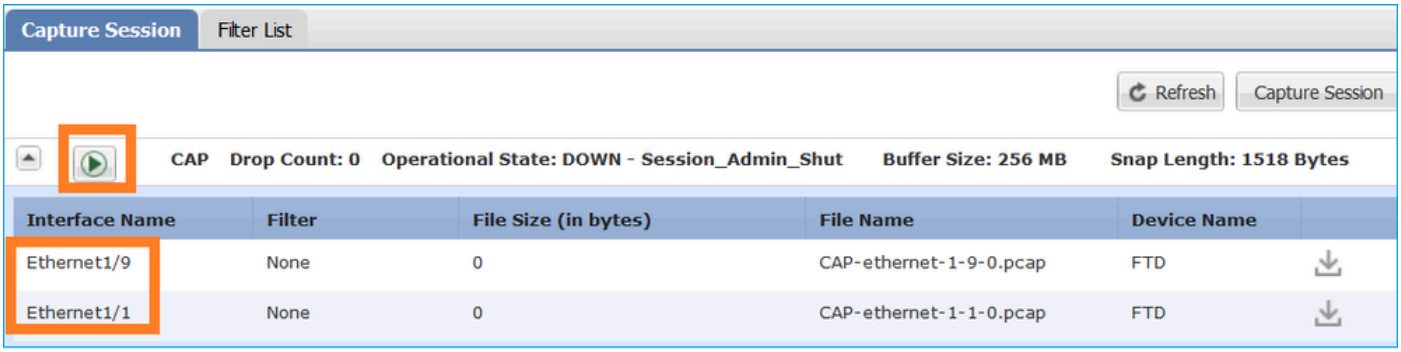
TCP OUTSIDE  192.168.2.40:21 INSIDE  192.168.1.40:40988, idle 0:00:00, bytes 723, flags UIO
TCP OUTSIDE  192.168.2.40:21 INSIDE  192.168.1.40:40980, idle 0:02:40, bytes 1086, flags UIO
TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:49442, idle 0:00:00, bytes 86348310, flags UIO N1
TCP OUTSIDE  192.168.2.40:20 INSIDE  192.168.1.40:39301, idle 0:00:00, bytes 485268628, flags U

o <- 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”输出计算。例如，如果通过FTD LINA引擎总共连接了5个，其中一个被分流，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）处理的所有数据包，必须在机箱级别启用捕获：



机箱背板捕获显示两个方向。由于FXOS捕获架构（每个方向两个捕获点），每个数据包显示两次:

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

如果平台与FP4100/FP9300不同，并且所有数据包都由LINA引擎处理，因为不支持流量分流(请注

意缺少o标志):

```
<#root>

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设置和连接终止事件：

```
<#root>

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 (192.1
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
```

使用案例

- 当您要完全绕过Snort检测时，请使用Prefilter Fastpath操作。您通常希望对备份或数据库传输等您信任的大数据流量执行此操作。
- 在FP4100/9300设备上，Fastpath操作会触发数据流分流，并且只有少数数据包通过FTD LINA引擎进行处理。其余部分由SmartNIC处理，从而减少延迟

预过滤器策略快速路径操作（内联集）

如果对通过内联集（NGIPS接口）的流量应用预过滤器策略快速路径操作，则必须考虑以下几点：

- 此规则作为trust操作应用于LINA引擎。
- Snort 引擎不检查流.
- 流量卸载（硬件加速）不会发生，因为流量卸载不适用于NGIPS接口。

如果对内联集应用了Prefilter Fastpath操作，请参阅数据包跟踪：

```
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
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

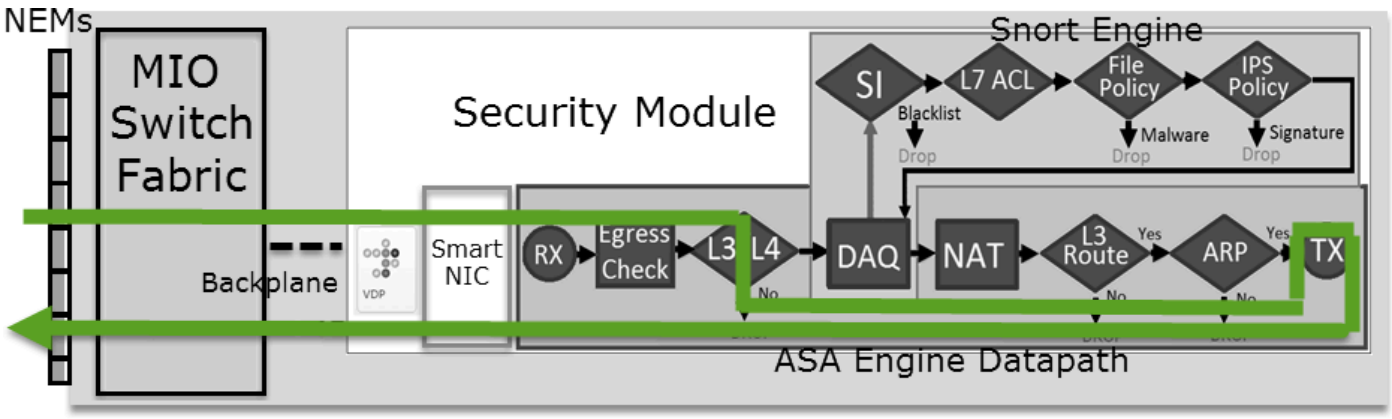
Phase: 4
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
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
```

数据包路径的可视表示图像：



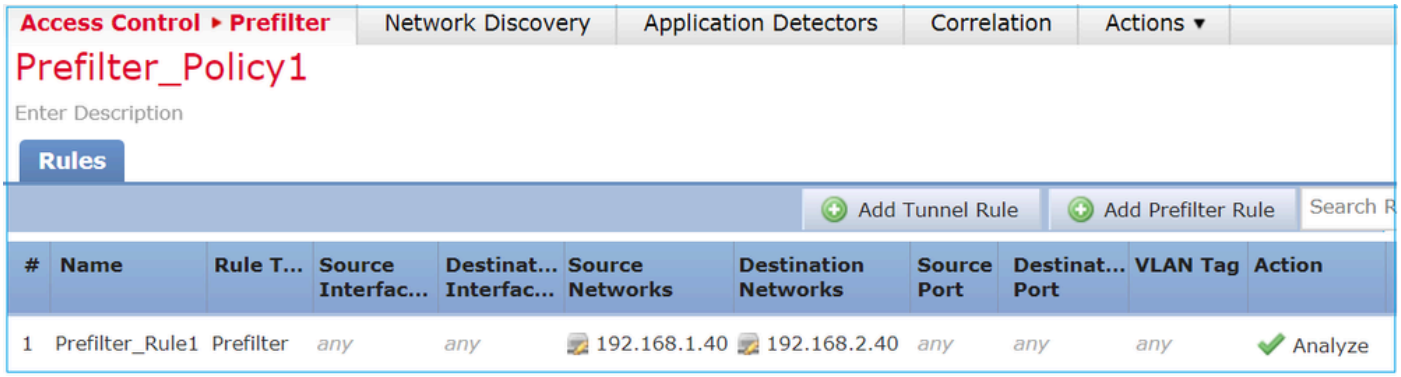
预过滤器策略快速路径操作（带分路器的内联集）

这与Inline-Set情况相同。

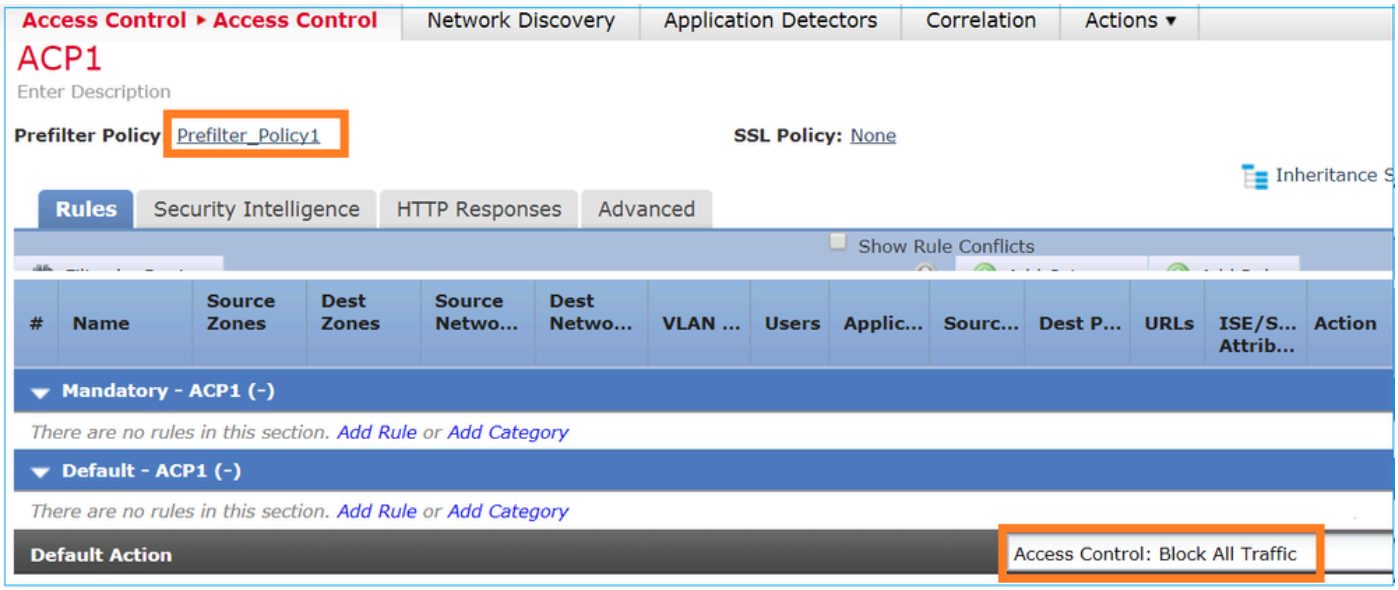
预过滤器策略分析操作

场景 1. 使用 ACP 阻止规则进行预过滤器分析

查看包含Analyze规则的预过滤器策略：



ACP仅包含设置为Block All Traffic的默认规则：



FTD Snort引擎（ngfw.rules文件）中部署的策略：

<#root>

```
# 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 47  (tunnel -1)
268435459 allow any any  any any any  any any 41  (tunnel -1)
268435459 allow 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  (log dcforward flowstart)
```

```
# End of AC rule.
```

在FTD LINA引擎中部署的策略：

<#root>

```
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允许的数据包，将其转发到Snort引擎(由于permit操作)，并且Snort引擎会返回block判定，因为来自AC的默认操作已匹配。

注意：Snort 不根据隧道规则评估流量.

当您跟踪数据包时，显示相同的结果：

<#root>

```
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

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:

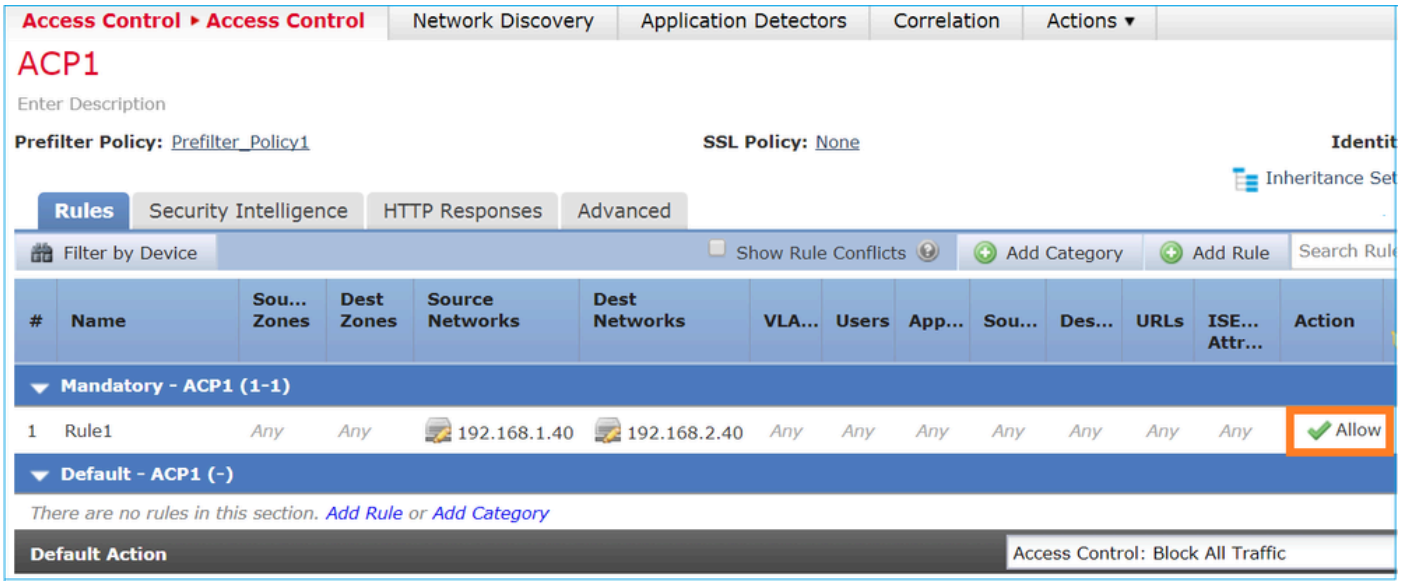
(block-list) block list this flow


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，则必须在ACP中添加规则。Action可以是Allow或Trust，这取决于目标(例如，如果要应用L7检测，必须使用Allow操作):



FTD Snort引擎中部署的策略：

<#root>

```
# 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  (log dcforward flowstart)
# End of AC rule.
```

在LINA引擎中：

<#root>

```
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在LINA中显示数据包匹配规则268435460，在Snort引擎中显示数据包匹配规则268435461:

<#root>

```
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
Firewall:

allow rule, id 268435461, allow

NAP id 1, IPS id 0,

Verdict PASS

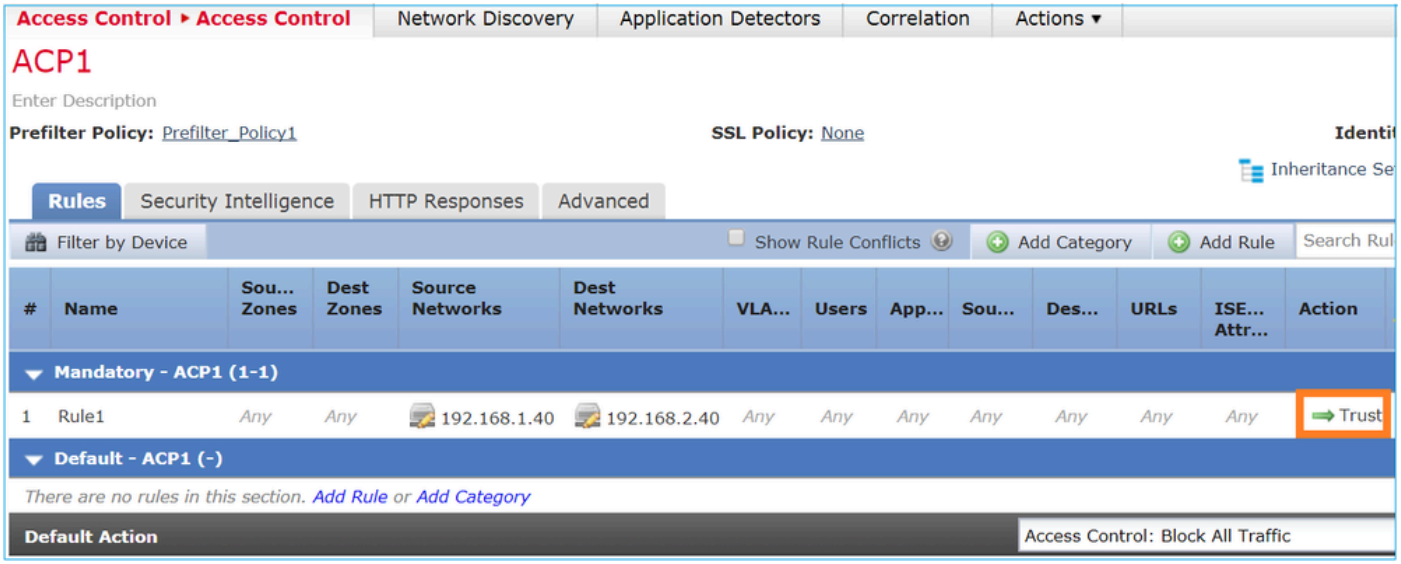
Snort Verdict: (pass-packet) allow this packet

…
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，请参阅预过滤器策略映像：



Snort:

<#root>

```
# 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  (log dcforward flowstart)
# End of AC rule.
```

LINA：

<#root>

```
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，因此信任规则在LINA上部署为permit操作；因此，将一些数据包重定向到Snort引擎进行检查。

验证行为

Packet-tracer显示Snort引擎的Permit列出数据包，并将剩余流量卸载到LINA:

<#root>

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
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。

规则在Snort中部署：

<#root>

```
# 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  (log dcforward flowstart)
# End of AC rule.
```

在LINA中，规则部署为信任。数据包与根据Analyze Prefilter规则部署的允许规则（检查ACE命中计数）匹配，并且数据包由Snort引擎进行检查：

<#root>

```
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

<#root>

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
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

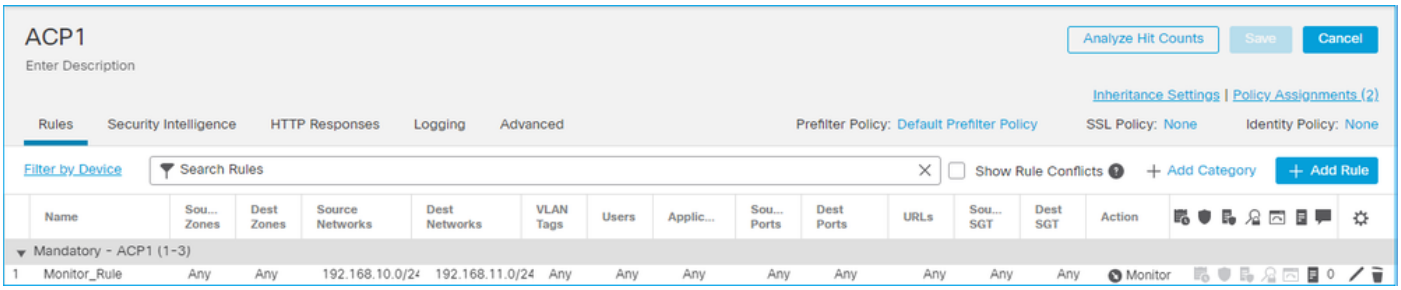
- Analyze操作在LINA引擎中部署为允许规则。这会影响要转发到Snort引擎进行检查的数据包。
- Analyze操作不会在Snort引擎中部署任何规则。您必须确保在ACP中配置在Snort中匹配的规则。
- 根据Snort中部署的ACP规则(block vs allow vs fastpath),Snort允许无、全部或少数数据包。

使用案例

- Analyze Action的一个使用案例是，您在Prefilter策略中具有宽泛的Fastpath规则，并且希望为特定流放置一些例外以便由Snort对其进行检查。

ACP 监控操作

在 FMC UI 上配置的监控规则：



监控规则作为permit操作部署在FTD LINA引擎上，作为audit操作部署到Snort引擎：

```
<#root>

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：

<#root>

```
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 dcforward flowend)
# End rule 268438863
```

要点

- 监控规则不会丢弃或允许流量，但它会生成连接事件。根据后续规则检查数据包，允许或丢弃该数据包。
- FMC连接事件显示匹配两个规则的数据包：



System support trace输出显示数据包同时匹配两个规则：

<#root>

```
>
```

```
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 (
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 IP
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_
```

⚠ 警告：您必须在Cisco支持的指导下使用system support命令，但system support ssl-client-hello-commands指南中记录的命令除外，这些命令用于一般用途。

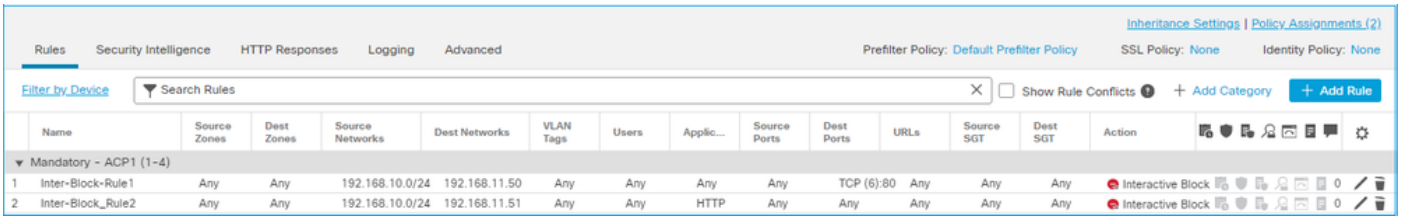
此外，请始终使用适当的过滤器，不要让命令无限期地运行，因为它可能会影响设备性能。

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：



交互式阻止规则作为permit操作部署在FTD LINA引擎上，并作为旁路规则部署到Snort引擎：

<#root>

```
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：

<#root>

```
admin@firepower:~$

cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules

…
# Start of AC rule.
268438864

bypass

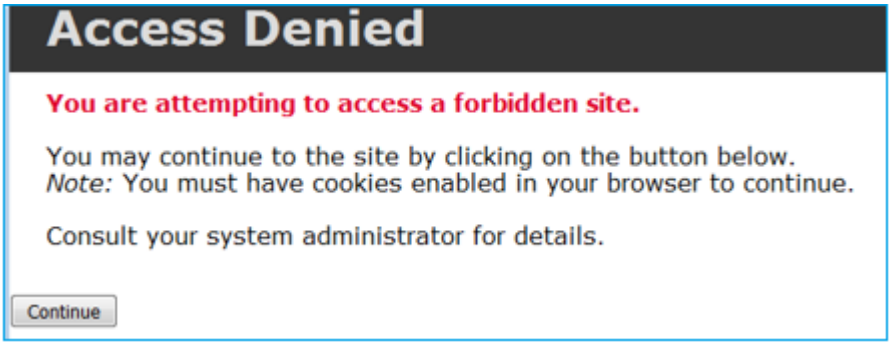
 any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
```

```
268438865
```

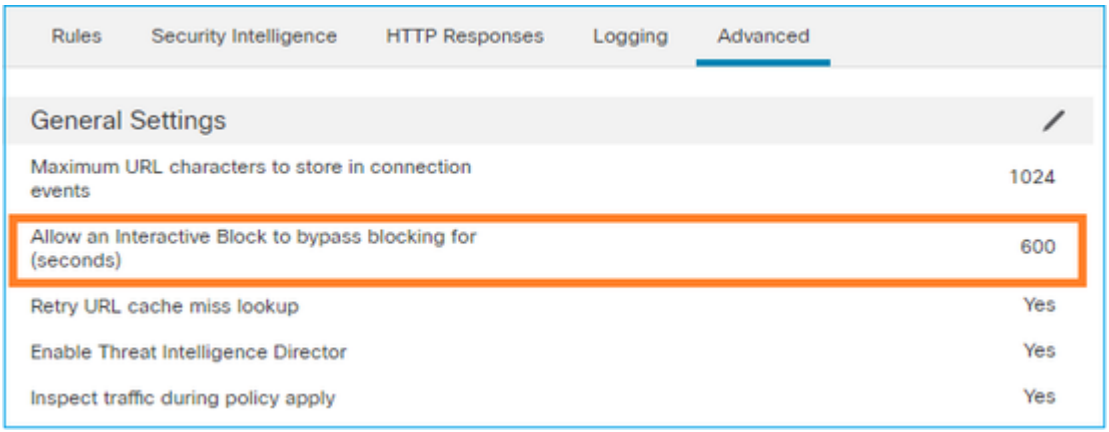
bypass

```
 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，防火墙允许您绕过阻止600秒：



在system support trace输出中，可以看到防火墙最初阻止流量并显示阻止页面：

<#root>

>

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', a
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-Ru
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions queue,
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 deleting firewall session flags = 0x800, fwFlags =
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）后，调试将显示相同规则允许的数据包，该规则模拟Allow操作：

<#root>

```
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', an
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-R
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
```

⚠ 警告：您必须在Cisco支持的指导下使用system support命令，但system support ssl-client-hello-commands指南中记录的命令除外，该指南一般使用。

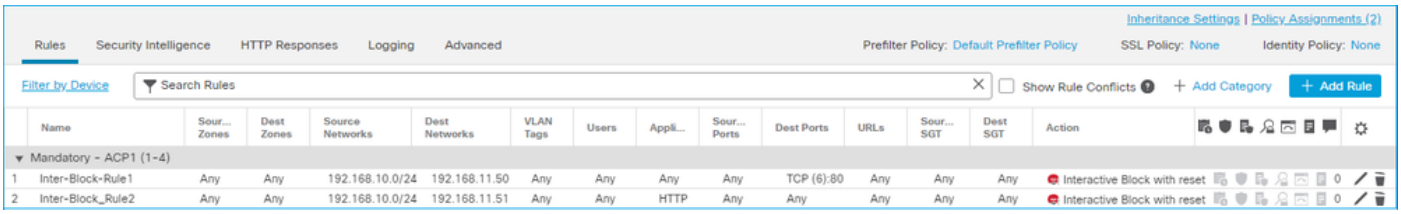
⚠ 此外，请始终使用适当的过滤器，不要让命令无限期地运行，因为它可能会影响设备性能。

使用案例

向Web用户显示警告页面，并向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：



带重置规则的交互式阻止作为permit操作部署在FTD LINA引擎上，作为intreset规则部署到Snort引擎上：

<#root>

```
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：

```
<#root>

# Start of AC rule.
268438864

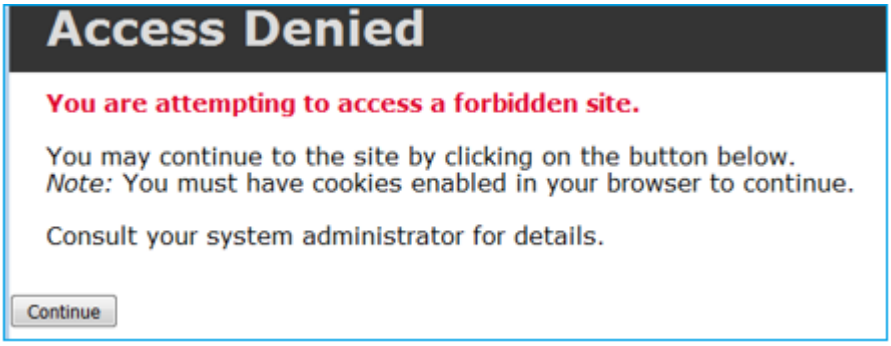
intreset

 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“阻止并重置”一样，用户可以选择继续选项：



在Snort调试中，Interactive Reset中显示的操作。

⚠ 警告：您必须在Cisco支持的指导下使用system support命令，但system support ssl-client-hello-commands指南中记录的命令除外，该指南一般使用。

此外，请始终使用适当的过滤器，不要让命令无限期地运行，因为它可能会影响设备性能。

```
<#root>

>

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 (
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', a
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1', action In
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 MidRecovery data sent for rule id: 268438864,rule_
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 323212
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 AppID: service unknown (0), application unknown (
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 (
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', a
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-Ru
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions queue,
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 deleting firewall session flags = 0x800, fwFlags =
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

向最终用户显示阻止页面。如果用户选择Continue（或刷新网页），则相同的规则匹配，允许流量通过：

```
<#root>

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', a
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-R
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-R
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：

```
<#root>

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 3109534920:310
   3: 22:13:33.113626       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: S 3422362500:342
   4: 22:13:33.113824       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack 3422362501
   5: 22:13:33.114953       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P 3422362501:342
   6: 22:13:33.114984       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P 3422362543:342
   7: 22:13:33.114984       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P 3422362549:342
   8: 22:13:33.115182       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack 3422362543
   9: 22:13:33.115411       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack 3422362549
  10: 22:13:33.115426       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack 3422362570
  12: 22:13:34.803699       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: P 3109534921:310
  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）中，Snort引擎不会为辅助连接（例如，FTD数据）或使用Trust操作时打开针孔。在最新版本中，此行为已更改，并且Snort引擎会打开针孔，即使使用Trust操作也是如此。

FTD 规则准则

- 对大流量流使用预过滤器策略快速路径规则，并减少整个设备的延迟。
- 对必须根据L3/L4条件阻止的流量使用预过滤器阻止规则。
- 使用ACP信任规则可绕过许多Snort检查，但仍可利用身份策略、QoS、SI、应用检测、URL过滤器等功能。
- 使用以下指导原则，将影响较差防火墙性能的规则置于访问控制策略的顶部：
    - 块规则（第1-4层） — 预过滤器块
    - 允许规则（第 1-4 层）- 预过滤器快速路径
    - ACP 阻止规则（第 1-4 层）
    - 信任规则（第 1-4 层）
    - 阻止规则（第 5-7 层 - 应用检测、URL 过滤）
    - 允许规则（第 1-7 层 - 应用检测、URL 过滤、入侵策略/文件策略）
    - 阻止规则（默认规则）

- 避免过多的日志记录(在开始时或结束时记录；同时避免这两种情况)
- 了解规则扩展，检查LINA中的规则数

<#root>

```
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). **No packets** are sent to Snort engine.
Analyze	Permit	-	The ACP rules are checked. **Few** or **all packets** 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 **No packets** 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：使用6.3 FTD软件代码，动态流量分流可以分流满足其他标准的连接；例如，需要Snort检测的可信数据包。有关详细信息，请查看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）。