釐清 Firepower Threat Defense 存取控制原則規則動作

目錄

簡介

本文件說明 Firepower Threat Defense (FTD) 存取控制原則 (ACP) 和預先過濾原則上可用的不同動作。

必要條件

需求

思科建議您瞭解以下主題：

- 流量卸載
- Firepower威脅防禦裝置上的資料包捕獲
- FTD 設備上具有追蹤軌跡選項的 Packet Tracer 和擷取

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco Firepower 4110 Threat Defense 版本 6.4.0（組建 113）和 6.6.0（組建 90）
- Firepower Management Center (FMC) 版本 6.4.0（組建 113）和 6.6.0（組建 90）

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

相關產品

本文件也適用於以下硬體和軟體版本：

- 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)、核心式虛擬機器 (KVM)
- 整合式服務路由器 (ISR) 模組
- FTD 軟體 6.1.x 和更新版本

> **附註**：流解除安裝僅在ASA和FTD應用的本機例項以及FPR4100和FPR9300平台上受支援。FTD容器例項不支援流量解除安裝。

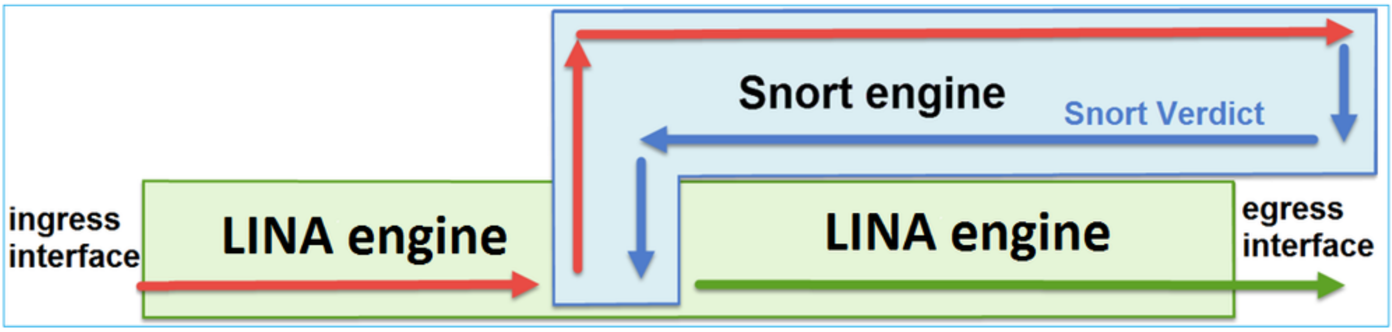
背景資訊

檢查每個操作的後台操作，以及它與其他功能（如流量分流和開啟輔助連線的協定）的互動。

FTD 是一個整合的軟體映像，其中包括 2 個主引擎：

- LINA 引擎
- Snort 引擎

本圖顯示 2 個引擎如何互動：



- 封包進入輸入介面，並由 LINA 引擎處理
- 如果 FTD 原則需要該封包，則 Snort 引擎會對其進行檢查
- Snort引擎傳回封包的判定結果（允許清單或封鎖清單）
- LINA 引擎根據 Snort 的判定結果捨棄或轉送封包

ACP 部署方式

使用機下（遠端）管理時，系統會在 FMC 上設定 FTD 原則；或使用本機管理時，系統會在 FMC 上設定 Firepower Device Manager (FDM)。在兩種案例下，ACP 會顯示為：

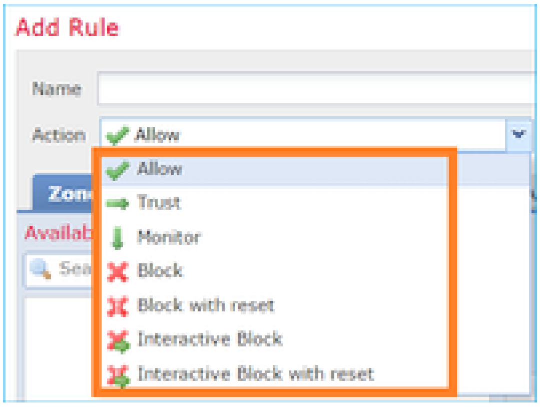
- FTD LINA引擎的命名為CSM_FW_ACL_的全域存取控制清單(ACL)
- FTD Snort 引擎之 /ngfw/var/sf/detection_engines/<UUID>/ngfw.rules 檔案中的存取控制 (AC) 規則

設定

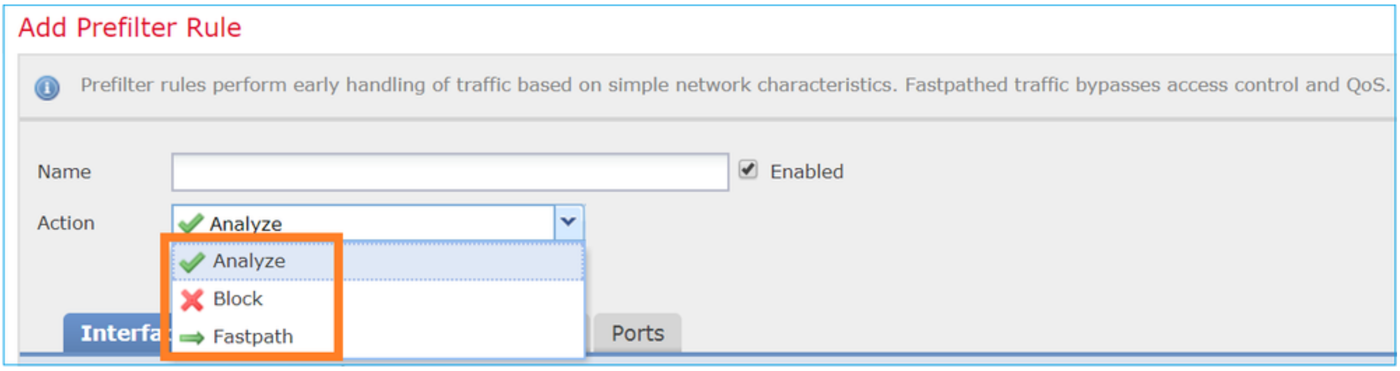
ACP 可用動作

FTD ACP 包含一或多個規則，而每個規則可具有下列其中一個動作，如圖所示：

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



同樣地，預先篩選原則可包含一或多個規則，而可能的動作如下圖所示：



Add Prefilter Rule

Prefilter rules perform early handling of traffic based on simple network characteristics. Fastpathed traffic bypasses access control and QoS.

Name ☑ Enabled

Action: Analyze

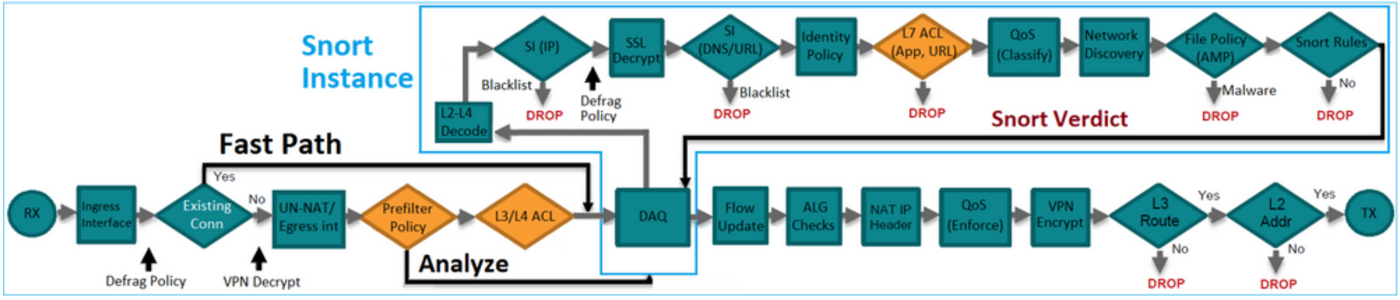
ACP 和預先篩選原則互動方式

預過濾器策略是在6.1版中引入的，主要有兩個用途：

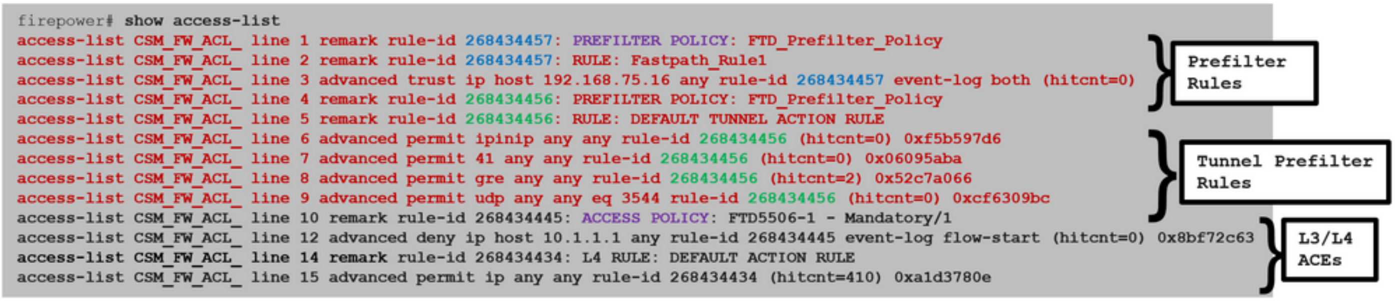
1. 此原則允許檢查通道流量，其中 FTD LINA 引擎會選取外部 IP 標頭，而 Snort 引擎會選取內部 IP 標頭。更具體地說，在隧道流量（例如GRE）的情況下，預過濾器策略中的規則始終在 **outer headers,** 而ACP中的規則始終適用於內部會話 **(inner headers).**通道流量係指以下通訊協定：

- GRE
- IP-in-IP
- IPv6-in-IP
- Teredo 連接埠 3544

2. 它提供早期存取控制(EAC)，允許流量完全繞過Snort引擎，如圖所示。



預過濾器規則在FTD上部署為L3/L4存取控制元件(ACE)，並在已設定的L3/L4 ACE之前，如下圖所示：

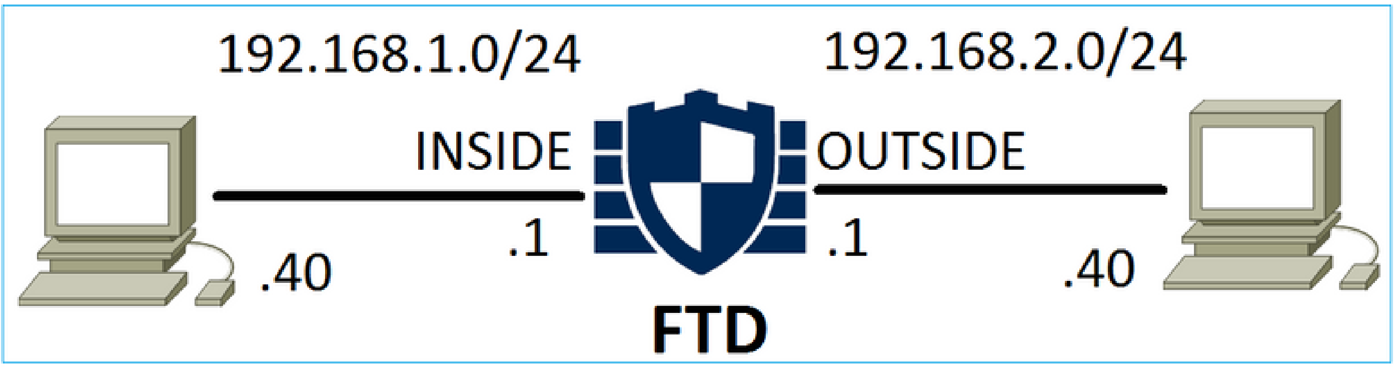


```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log 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
```

附註：預先篩選原則與 ACP 原則 = 第一個相符項目受到套用。

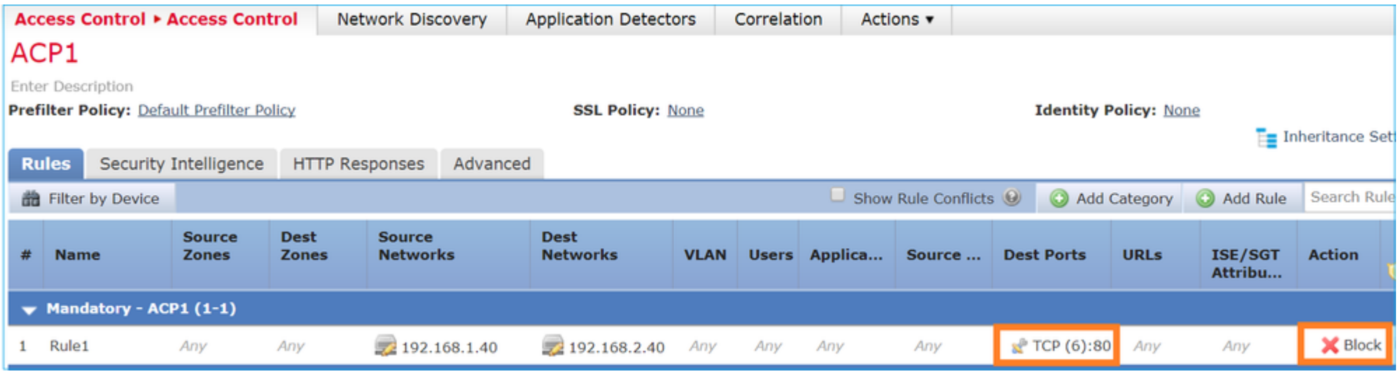
ACP Block 動作

請考慮以下圖中所示的拓撲：



情況 1. Early LINA 捨棄

ACP 包含 Block 規則，該規則會使用 L4 條件（目的地連接埠 TCP 80），如下圖所示：



Access Control ▸ Access Control | Network Discovery | Application Detectors | Correlation | Actions ▾

ACP1

Enter Description

Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

Inheritance Sett

Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device   Show Rule Conflicts   Add Category   Add Rule   Search Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN	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	TCP (6):80	Any	Any	Block

Snort 中部署的原則：

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

LINA 中部署的原則。請注意，規則推送為 **deny** action:

```
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
```

驗證行為：

主機A(192.168.1.40)嘗試開啟與主機B(192.168.2.40)的HTTP作業階段時，FTD LINA引擎捨棄TCP同步(SYN)封包，但確實到達Snort引擎或目的地：

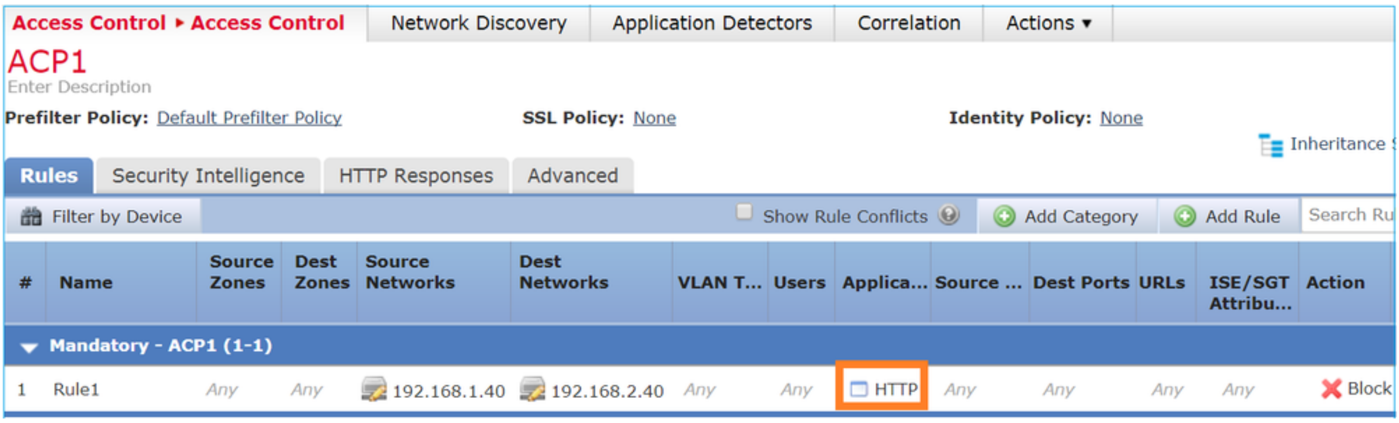
```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -
430 bytes]
  match ip host 192.168.1.40 any
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -
0 bytes]
  match ip host 192.168.1.40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

情況 2. 因 Snort 判定結果捨棄

ACP 包含 Block 規則，該規則會使用 L7 條件（應用 HTTP），如下圖所示：



ACP1

Enter Description

Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

#	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 中部署的原則：

```
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 中部署的原則。

> **附註**：規則推送為 **permit** 操作，因為LINA無法確定作業階段使用HTTP。在FTD上，應用檢測機制位於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
```

對於使用 **Application** 實際情況，實際封包的追蹤軌跡顯示，由於Snort引擎判定結果，LINA捨棄了作業階段。

> **附註**：若要使 Snort 引擎能判斷應用程式，則其必須檢查數個封包（通常 3 至 10 個，視應用程式解碼器而定）。 因此，系統會允許數個封包通過 FTD，並連線至目的地。所允許的資料包仍要接受基於以下內容的入侵策略檢查： **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** 選項。

驗證行為：

當主機 A (192.168.1.40) 嘗試與主機 B (192.168.2.40) 建立 HTTP 作業階段時，LINA 輸入擷取會顯示：

```
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>
 ...
```

輸出擷取：

```
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>
```

追蹤軌跡顯示，由於尚未達成應用偵測判定結果，Snort允許第一個封包(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 封包亦同：

```
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
```

完成第三個封包的檢查後，Snort會傳回DROP判定結果：

```
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
```

您也可以執行 **system support trace** 在FTD清除模式下。此工具提供 2 種功能：

- 顯示將每個封包傳送到資料收集庫(DAQ)時以及在LINA中看到的Snort判定結果。DAQ 為位於 FTD LINA 引擎和 Snort 引擎之間的元件
- 允許運行 **system support firewall-engine-debug** 同時瞭解Snort引擎內部所發生的變化

以下為輸出內容：

```
> 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
```

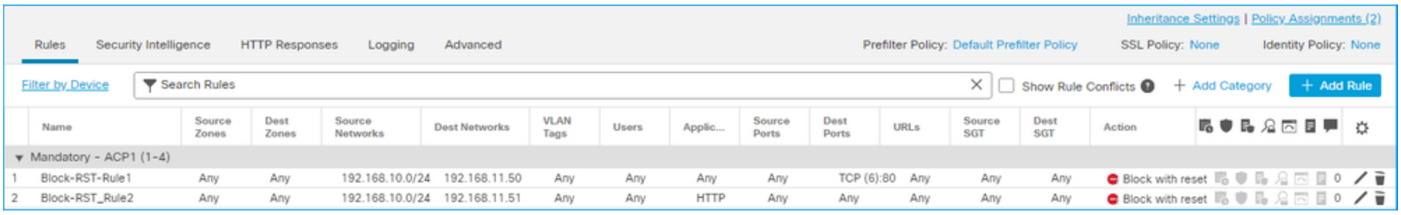
```
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0)
-> 0, vlan 0, sgt 65535, user 9999997, url http://192.168.2.40/128k.html
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 match rule order 2, 'Rule1', action Block
192.168.1.40-32791 > 192.168.2.40-80 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 Block 動作根據 LINA 中的 permit 或 deny 規則受到部署（視規則條件而定）
- 如果條件為 L3/L4，則 LINA 會封鎖封包。若是TCP，第一個封包(TCP SYN)遭封鎖
- 如果條件為 L7，則封包會轉送至 Snort 引擎做進一步檢查。在 TCP 情況下，系統會允許數個封包通過 FTD，直到 Snort 連線至判定結果。所允許的資料包仍要接受基於以下內容的入侵策略檢查： **Access Policy > Advanced > 'Intrusion Policy used before Access Control rule is determined'** 選項。

ACP Block with reset 動作

FMC UI 中設定的 Block with rest 規則：



	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	0
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	0

具有重設的封鎖規則部署在FTD LINA引擎上，作為 **permit** 和Snort引擎 **reset** rule:

```
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
```

當封包與Block with reset rule相符時，FTD會傳送 **TCP Reset** 資料包或 **ICMP Type 3 Code 13** 無法到達目的地（管理性過濾）訊息：

```
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.
```

以下為 FTD 輸入介面取得的擷取內容：

```
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) win 29200 <mss 1460,sackOK,timestamp 3740873275 0,nop,wscale 7>
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 win 0 2 packets shown
```

System support trace 輸出（在此案例中）顯示封包由於Snort判定結果而遭捨棄：

```
> 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

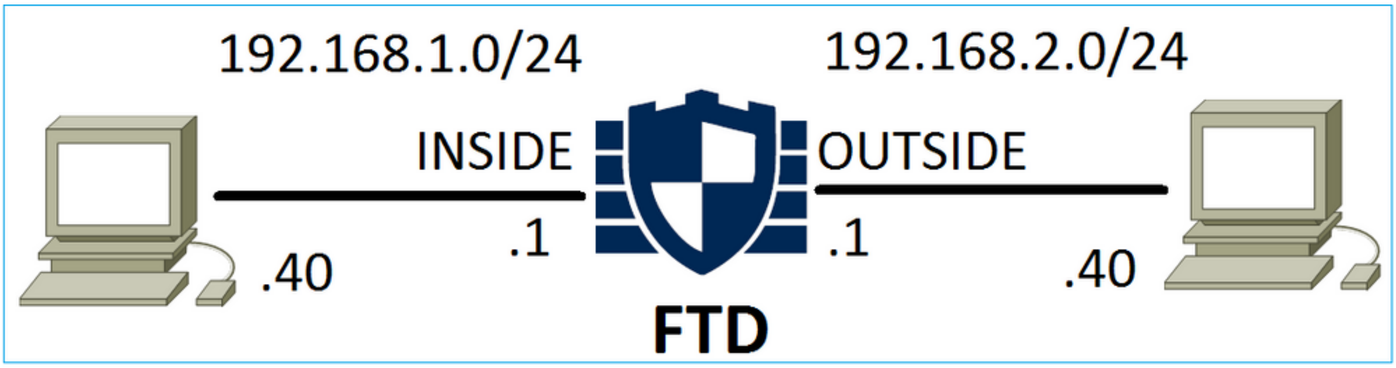
與 **Block** 操作，但立即終止連線。

ACP Allow 動作

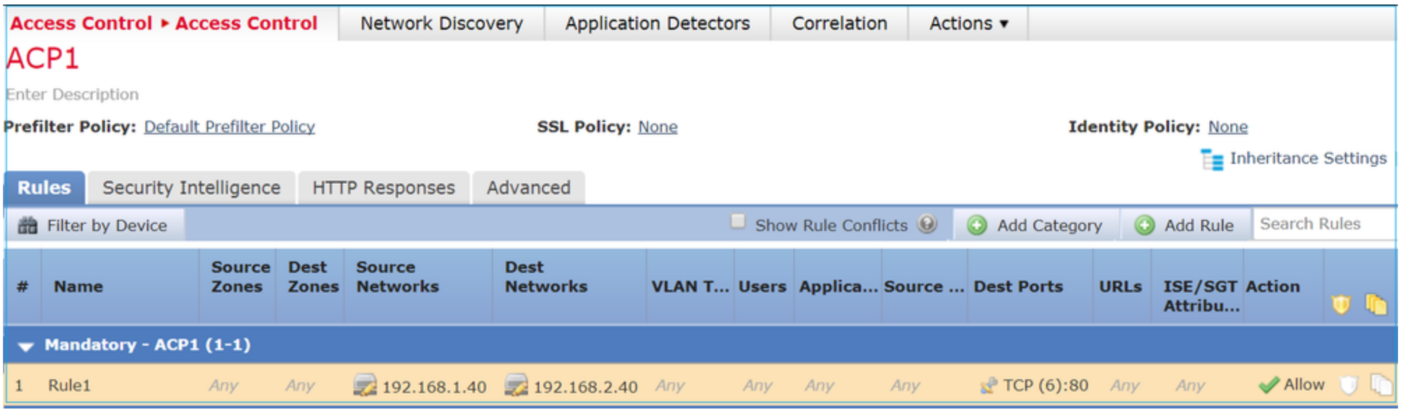
情況 1. ACP Allow 動作（L3/L4 條件）

正常來說，您會設定 Allow 規則以指定其他檢查，例如入侵原則和/或檔案原則。第一個場景演示應用L3/L4條件時Allow規則的操作。

考量下圖所示的拓撲：



此原則會受到套用，如下圖所示：



ACP1

Enter Description

Prefilter Policy: Default Prefilter Policy **SSL Policy:** None **Identity Policy:** None

#	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	TCP (6):80	Any	Any	✓ Allow

Snort 中的部署原則。請注意，規則部署為 **allow** action:

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

LINA 中的原則。

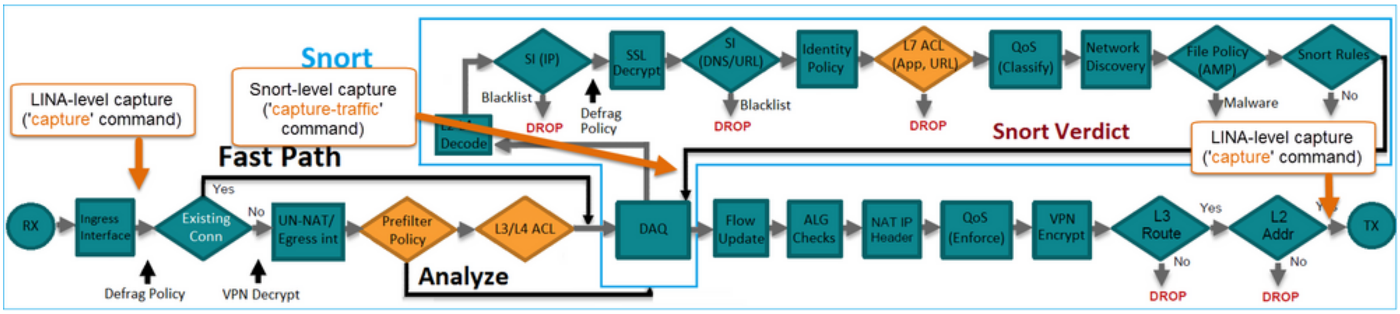
> **附註**：規則部署為 **permit** 操作，實質上表示重新導向至Snort以進行進一步檢查。

```
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
```

若要瞭解FTD如何處理與Allow規則相符的流，可以使用以下幾種方式：

- 驗證 Snort 統計
- 使用 system support trace CLISH 工具
- 使用 LINA 中的「含有追蹤軌跡的擷取」選項，且可選用 Snort 引擎中的擷取流量

LINA 擷取與 Snort 擷取流量：



驗證行為：

清除Snort統計資訊，啟用 **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
```

傳遞資料包計數器增加：

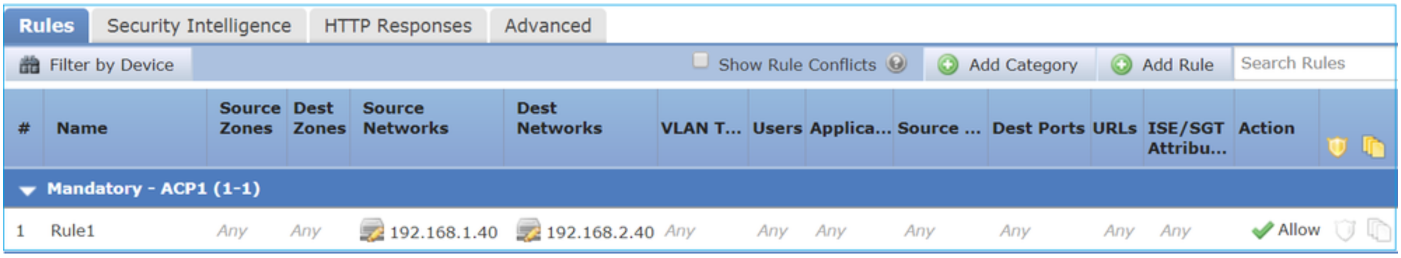
```
> show snort statistics

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
...
```

通過的封包 = 經 Snort 引擎完成檢查

情況 2. ACP Allow 動作（L3-7 條件）

當 Allow 規則透過以下方式部署後，會出現類似行為。

只有L3/L4條件，如下圖所示：

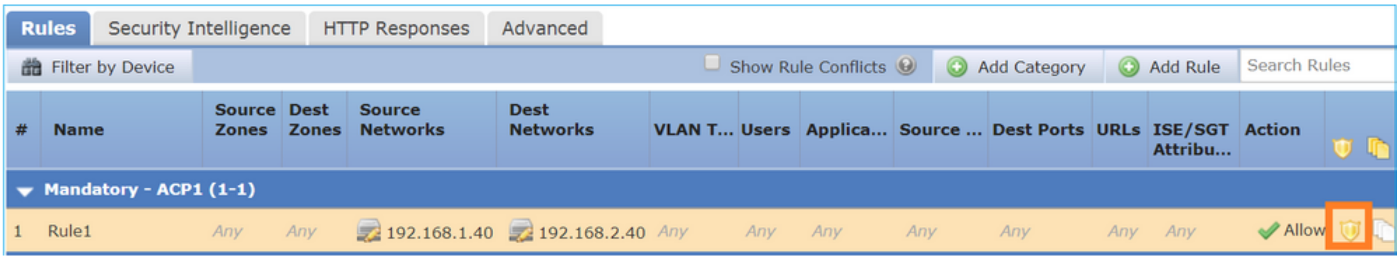


Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device　□ Show Rule Conflicts　Add Category　Add Rule　Search Rules

#	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條件（例如Intrusion Policy、File Policy、Application等）如下圖所示：



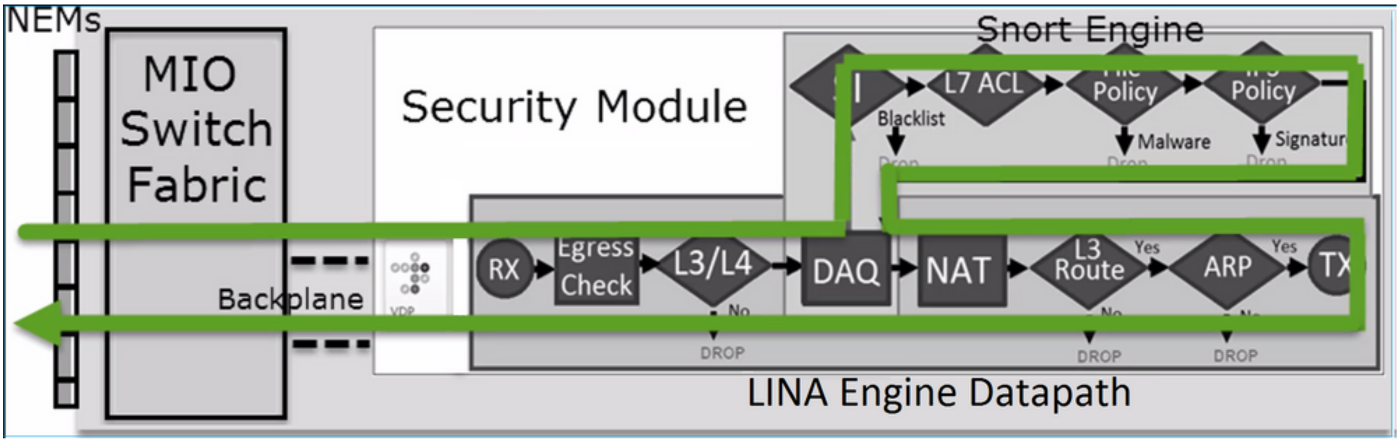
Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device　□ Show Rule Conflicts　Add Category　Add Rule　Search Rules

#	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

總結一下，當 Allow 規則符合（如下圖所示）時，以下為部署於 FP4100/9300 之 FTD 處理流量的方式：



附註：Management Input Output (MIO) 為 Firepower 機箱的監控引擎。

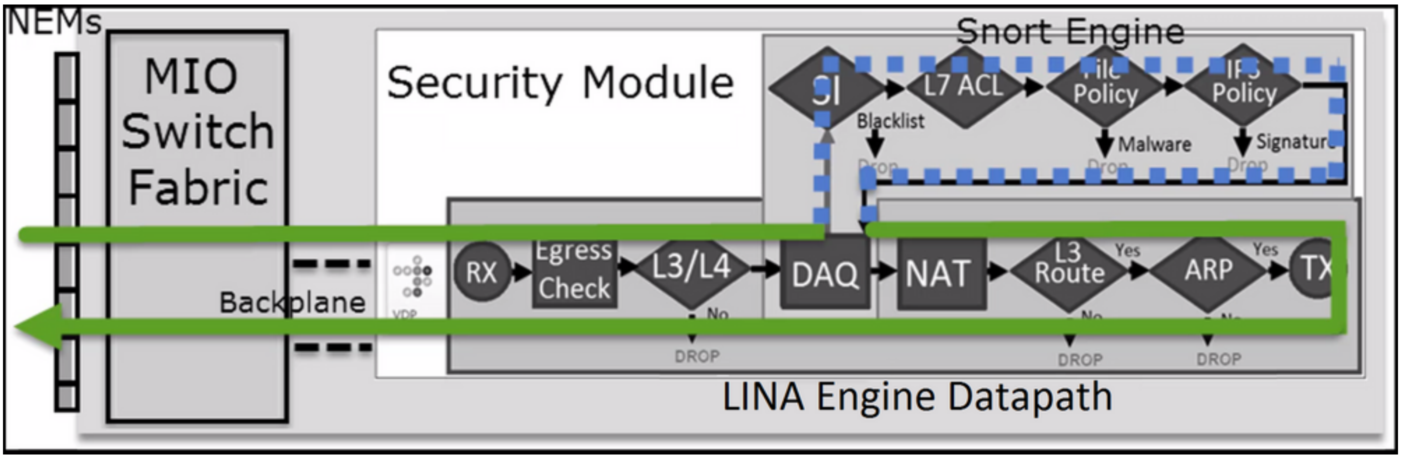
案例 3. 使用 Allow 的 Snort 快速轉送判定結果

在某些特定情況下，FTD Snort引擎會提供PERMITLIST判定結果（快速轉送），而其餘的流量則解

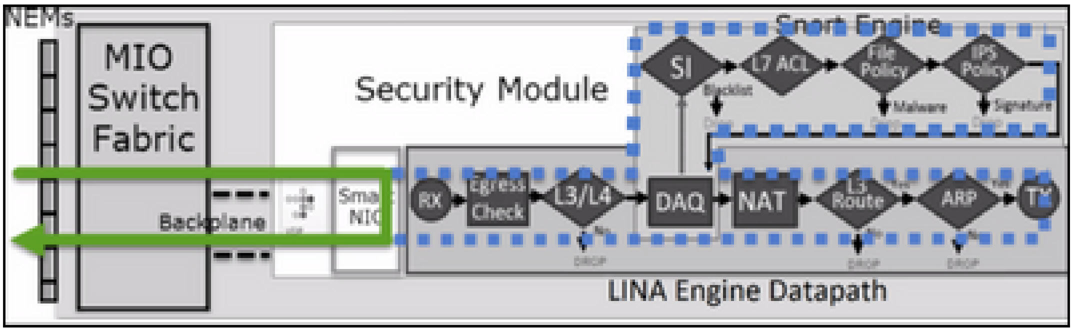
除安裝到LINA引擎（在某些情況下，接著解除安裝到HW加速器 — SmartNIC）。 它們是：

1. 未設定 SSL 原則的 SSL 流量
2. 智慧型應用程式略過 (IAB)

以下是封包路徑的視覺化表示：



在某些情況下：



主要重點

- 允許規則部署為 **allow** 在Snort和 **permit** 在LINA中
- 在大多數情況下，一個會話的所有資料包都會轉發到Snort引擎以進行其他檢查

使用案例

當您需要透過 Snort 引擎進行以下 L7 檢查時，會設定 Allow 規則：

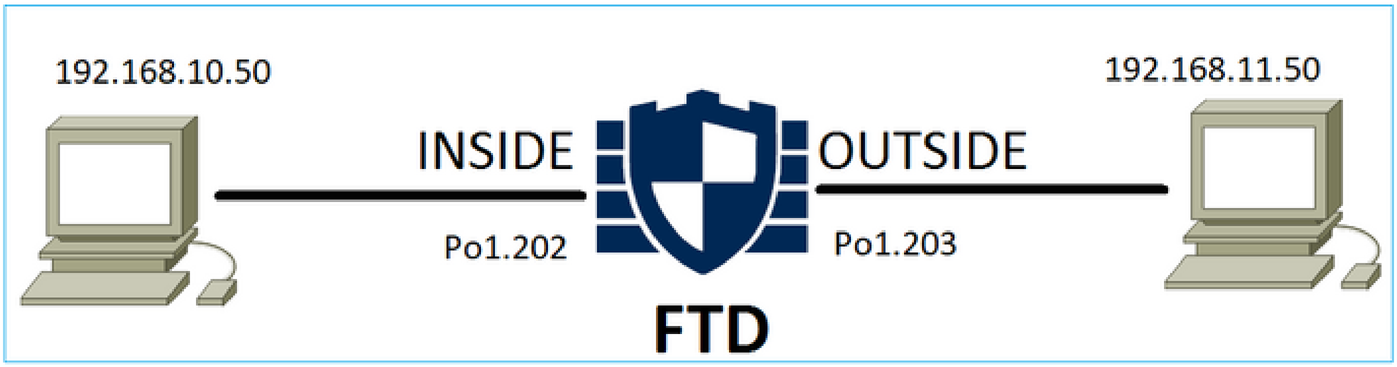
- 入侵原則
- 檔案原則

ACP Trust 動作

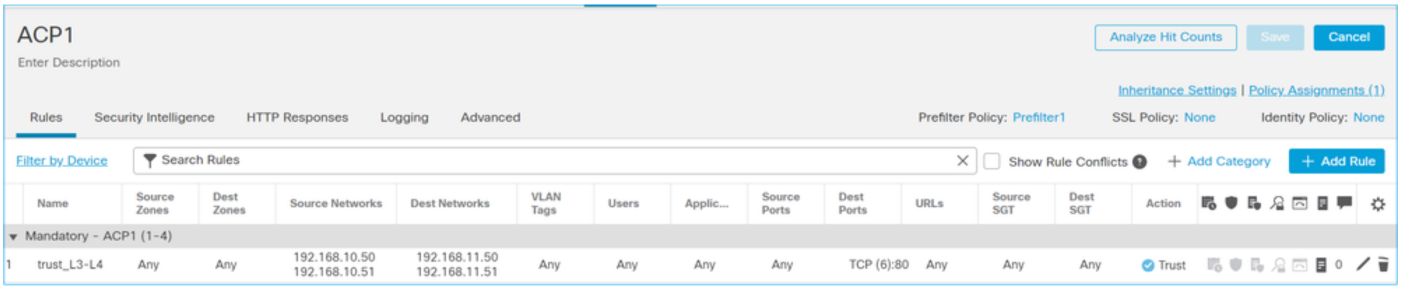
情況 1. ACP Trust 動作

如果您不想在Snort級別應用高級L7檢測（例如，入侵策略、檔案策略、網路發現），但您仍想使用安全情報(SI)、身份策略、QoS等功能，則建議在規則中使用Trust操作。

拓撲：



已設定的原則：



Prefilter Policy: Prefilter1 SSL Policy: None Identity Policy: None

	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	0

部署於 FTD Snort 引擎的 Trust 規則：

```
# 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)
```

附註：數字 6 為通訊協定 (TCP)。

FTD LINA 中的規則：

```
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
```

驗證：

啟用 **system support trace** 並起始從主機A(192.168.10.50)到主機B(192.168.11.50)的HTTP作業階段。以下有 3 個轉送至 Snort 引擎的封包。Snort引擎向LINA傳送PERMITLIST判定結果，該判定結果實質上會將流量的其餘部分解除安裝到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
```

當連線終止時，Snort 引擎會從 LINA 引擎取得中繼資料資訊，並刪除作業階段：

```
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 capture顯示到達Snort引擎的3個封包：

```
> 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 擷取會顯示通過其中的流量：

```
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>

…
```

LINA 的封包追蹤軌跡為檢視 Snort 判定結果的其他方式。取得 PASS 判定結果的第一個封包：

```
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介面上TCP SYN/ACK封包的追蹤軌跡：

```
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會收到允許清單判定結果：

```
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
```

此為 Snort 判定結果的完整輸出內容 (第 3 個封包)

```
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個封包不會轉送到Snort引擎，因為LINA引擎已快取判定結果：

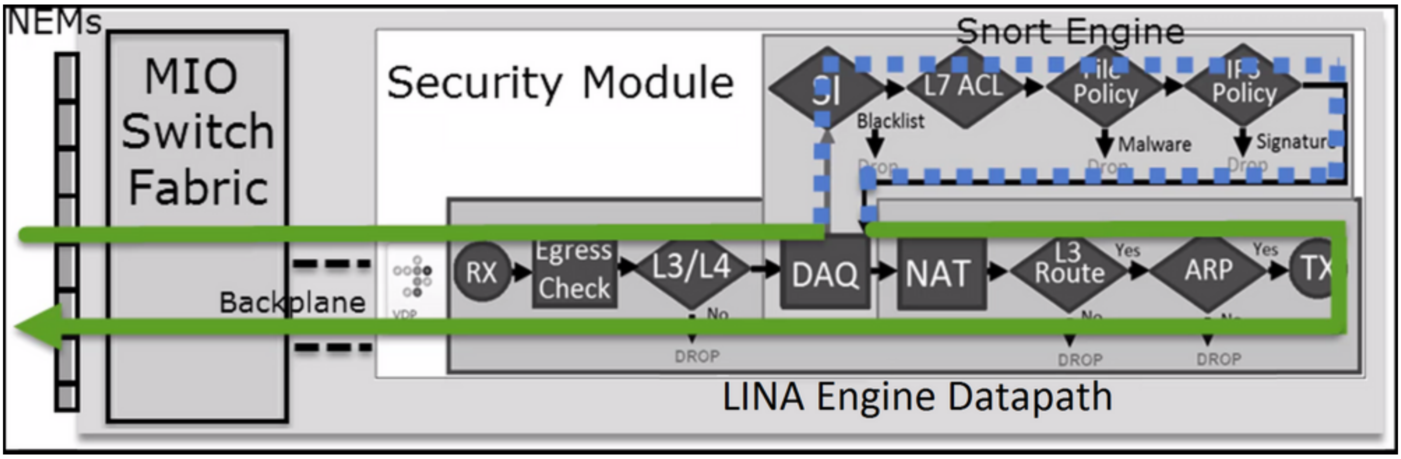
```
firepower# show capture CAPI packet-number 4 trace

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 統計已證實這點：

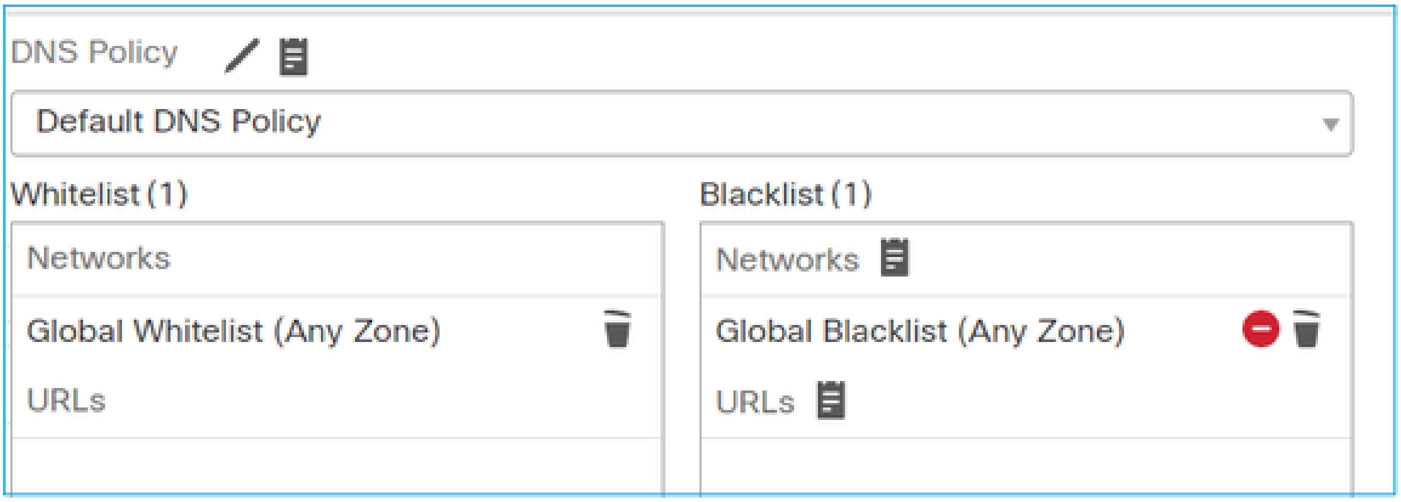
```
firepower# show snort statistics

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
```

使用 Trust 規則的封包流量。數個封包會受到 Snort 檢查，而其餘封包會受到 LINA 檢查：



案例2. ACP信任操作（無SI、QoS和身份策略）

如果您希望FTD對所有流應用安全情報(SI)檢查，則已在ACP級別啟用SI，您可以指定SI來源（TALOS、源、清單等）。 另一方面，如果您想要停用該功能，則您必須針對 ACP 全域停用網路的 SI、URL 的 SI 及 DNS 的 SI。網路和 URL 的 SI 會遭到停用，如下圖所示：



DNS Policy

Default DNS Policy

Whitelist (1)

Networks

Global Whitelist (Any Zone)

URLs

Blacklist (1)

Networks

Global Blacklist (Any Zone)

URLs

在此情況下，Trust 規則會部署於 LINA 做為信任項目：

```
> 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
```

> **附註**：自6.2.2起，FTD支援TID。TID 的運作方式與 SI 類似，但如果 SI 停用，並不會「強制」封包重新導向至 Snort 引擎作 TID 檢查。

驗證行為

初始化從主機 A (192.168.1.40) 至主機 B (192.168.2.40) 的 HTTP 作業階段。 由於這是FP4100並

支援硬體中的流量分流，因此會發生以下情況：

- 數個封包會透過 FTD LINA 引擎轉送，而其餘的流量會卸載至 SmartNIC (硬體加速器)
- 沒有資料包轉發到Snort引擎

FTD LINA連線表顯示旗標'**o**」這表示流已解除安裝到HW。另請注意，沒有「**N**'標誌。此情況實際上表示「沒有任何 Snort 重新導向」：

```
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
```

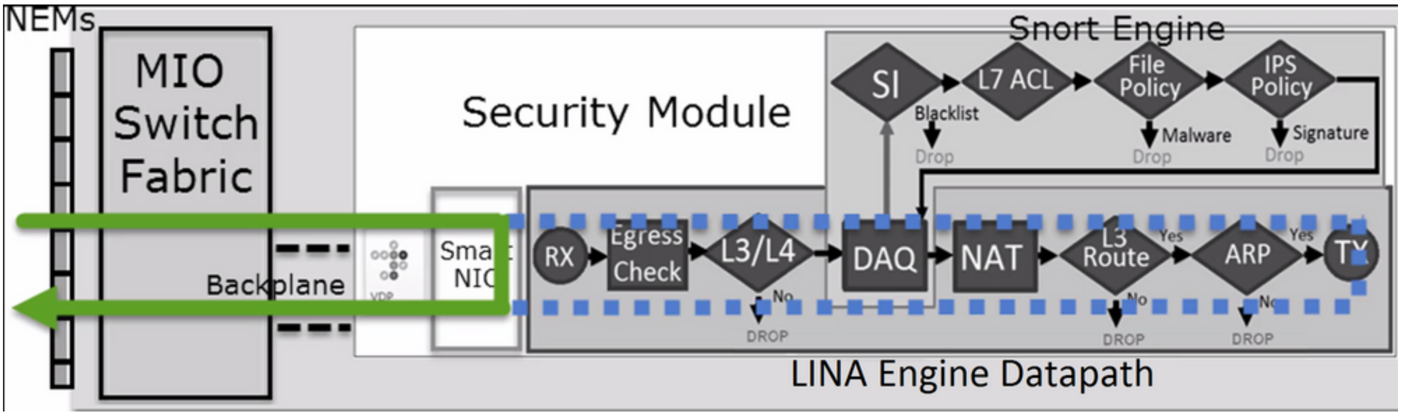
在作業階段開始和結束時，Snort 統計僅會顯示記錄事件：

```
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:
  Start-of-Flow events                                      1
  End-of-Flow events                                        1
```

FTD LINA 記錄會顯示每個作業階段有 2 個流量（每個導向一個）卸載至硬體：

```
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
```

將信任規則部署為 **trust** lina中的動作。數個封包會受到 LINA 檢查，而其餘封包會卸載至 SmartNIC (FP4100/FP9300)：

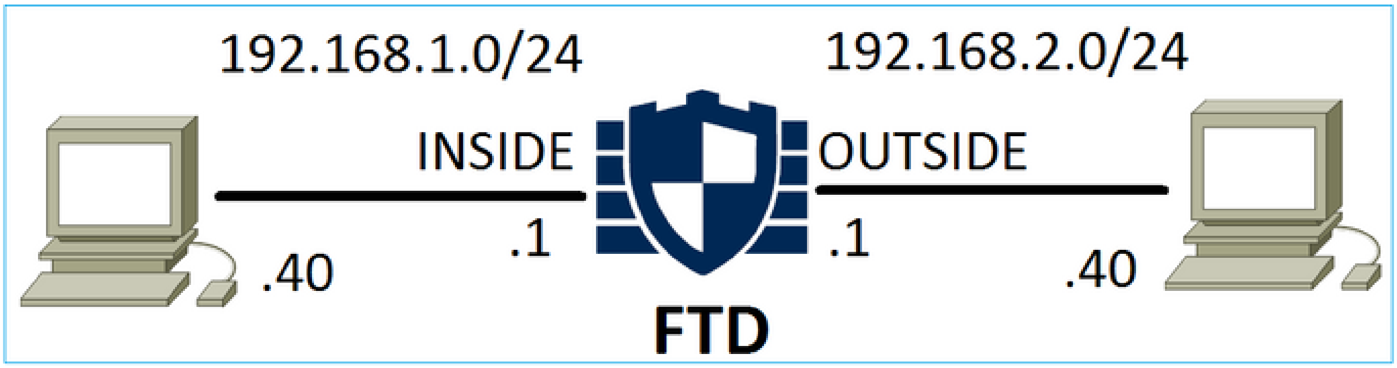


使用案例

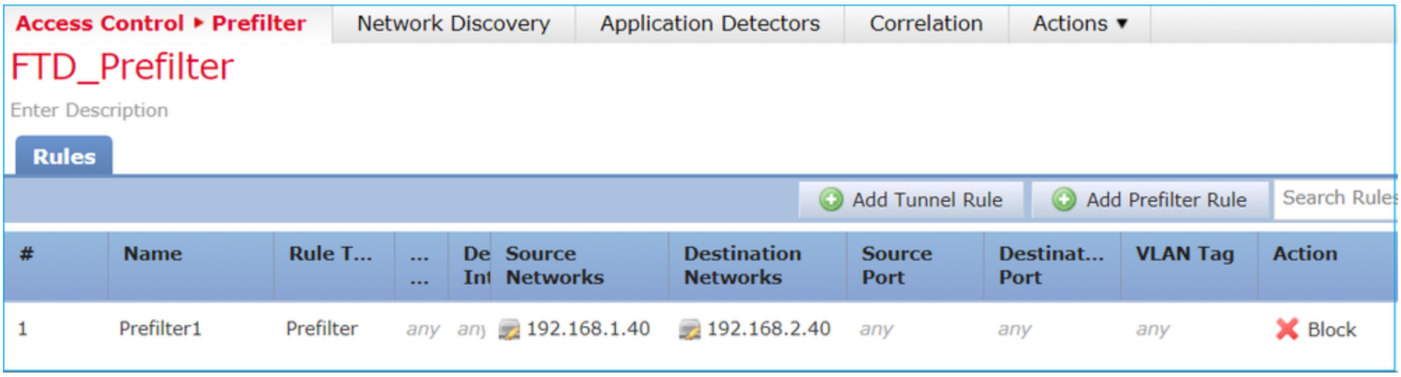
- 必須使用 **Trust** 當您僅希望由Snort引擎檢查幾個封包（例如應用程式偵測、SI檢查）並將流程的其餘部分解除安裝到LINA引擎時執行的動作
- 如果您在FP4100/9300上使用FTD，並希望流量完全繞過Snort檢查，則請考慮使用預過濾器規則 **Fastpath** action（請參閱本文檔中的相關部分）

預先篩選原則 Block 動作

考量下圖所示的拓撲：



另考量下圖所示的拓撲：



FTD_Prefilter

Enter Description

#	Name	Rule T...	... ...	De Int	Source Networks	Destination Networks	Source Port	Destinat... Port	VLAN Tag	Action
1	Prefilter1	Prefilter	any	an)	192.168.1.40	192.168.2.40	any	any	any	✗ Block

這是FTD Snort引擎（ngfw.rules檔案）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
```

在 LINA 中：

```
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
```

當您追蹤虛擬封包時，其會顯示該封包遭到 LINA 捨棄，且從未轉送至 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 統計會顯示：

```
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 捨棄會顯示：

```
firepower# show asp drop
```

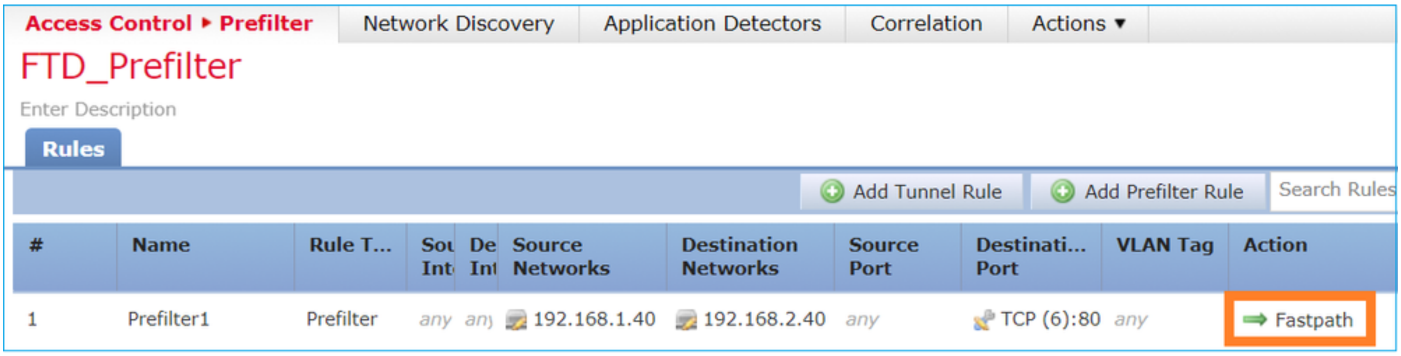
```
Frame drop:
  Flow is denied by configured rule (acl-drop)                1
```

使用案例

當您想要根據L3/L4條件封鎖流量，而不需要對流量進行任何Snort檢查時，可以使用Prefilter Block規則。

預先篩選原則 Fastpath 動作

考量下圖所示的預先篩選原則規則：



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

以下是FTD Snort引擎中部署的原則：

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

在 FTD LINA 中：

```
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
```

驗證行為

當主機 A (192.168.1.40) 嘗試開啟至主機 B (192.168.2.40) 的 HTTP 作業階段時，數個封包會通過 LINA，而其餘的封包會卸載至 SmartNIC。在這種情況下 **system support trace** 與 **firewall-engine-debug** enabled顯示：

```
> 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 記錄會顯示卸載流量：

```
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擷取show 8封包通過：

```
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 流量卸載統計會顯示卸載至硬體的 22 個封包：

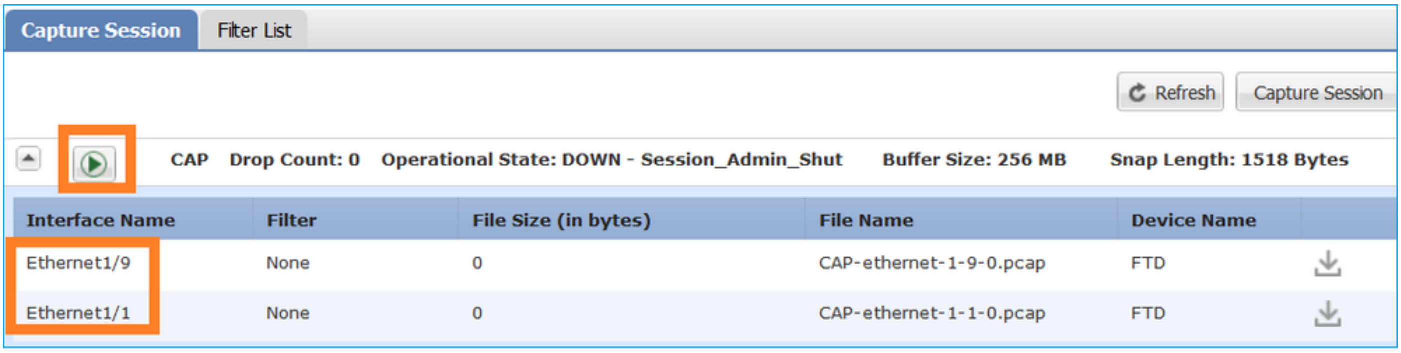
```
firepower# show flow-offload statistics
 Packet stats of port : 0
        Tx Packet count                 :                 22
        Rx Packet count                 :                 22
        Dropped Packet count            :                  0
        VNIC transmitted packet         :                 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
```

您還可以使用 **show flow-offload flow** 命令檢視與解除安裝流相關的其他資訊。以下是範例：

```
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, bytes 2326800
TCP intfc 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
```

- 百分比基於「show conn'輸出。例如，如果總共5個連線埠通過FTD LINA引擎，且其中的1個連線埠解除安裝，則20%報告為解除安裝
- 解除安裝作業階段的最大限制取決於軟體版本(例如ASA 9.8.3和FTD 6.2.3支援400萬雙向（或800萬單向）解除安裝流量)
- 如果解除安裝流的數量達到限制（例如400萬個雙向流），則不會解除安裝任何新連線，直到從解除安裝表中刪除當前連線

若要檢視通過 FTD 之 FP4100/9300 的所有封包（已卸載 + LINA），則需要在機箱層級啟用擷取，如下圖所示：



CAP Drop Count: 0 Operational State: DOWN - Session_Admin_Shut Buffer Size: 256 MB Snap Length: 1518 Bytes

Interface Name	Filter	File Size (in bytes)	File Name	Device Name
Ethernet1/9	None	0	CAP-ethernet-1-9-0.pcap	FTD
Ethernet1/1	None	0	CAP-ethernet-1-1-0.pcap	FTD

機箱背板擷取會顯示兩個方向。由於 FXOS 擷取架構（每個方向 2 個擷取點）緣故，因此每個封包會顯示**兩次**，如下圖所示：

資料包統計資訊：

- 通過 FTD 的封包總數：30
- 通過 FTD LINA 的封包數：8
- 卸載至 SmartNIC 硬體加速器的封包數：22

在平台不同於FP4100/FP9300的情況下，所有資料包都由LINA引擎處理，因為不支援流量分流(請

注意，沒有**o**標誌):

```
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 系統日誌僅會顯示連線設定和連線終止事件：

```
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** 當您要完全繞過Snort檢測時執行操作。您通常會想要針對信任的大流量（例如，備份、資料庫傳輸等）執行此操作
- 在FP4100/9300裝置上 **Fastpath** 操作會觸發流量解除安裝，只有少數封包會通過FTD LINA引擎。其餘的封包會受到 SmartNIC 處理，如此會減少延遲

預先篩選原則 Fastpath 動作（內嵌集合）

在對通過內嵌集（NGIPS介面）的流量應用預過濾器策略Fastpath操作時，必須考慮以下幾點：

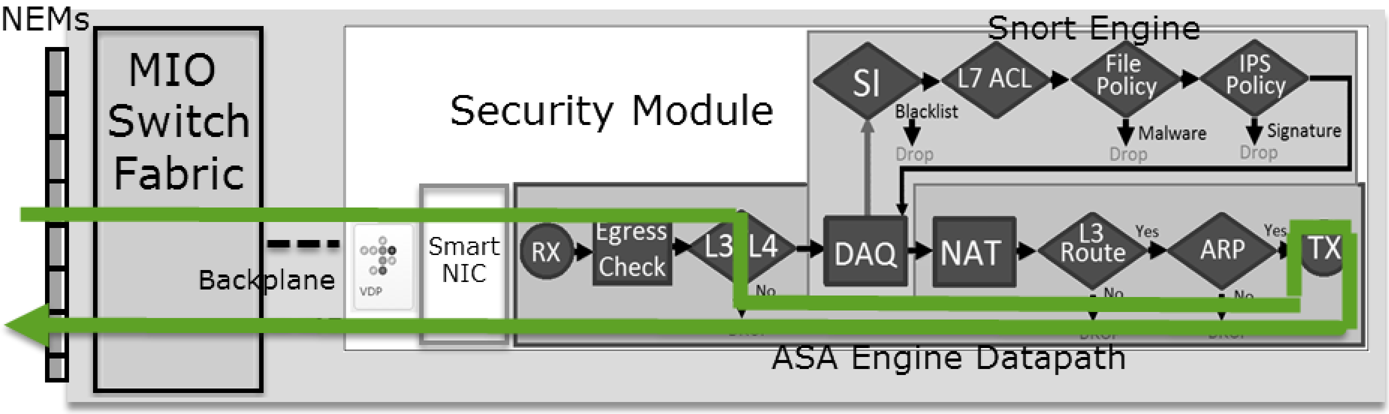
- 此規則應用於LINA引擎，作為 **trust** 動作
- 流量不會受到 Snort 引擎檢查
- 由於 NGIPS 介面不接受流量卸載，因此流量卸載（硬體加速）不會發生

以下是在內嵌集上套用Prefilter Fastpath動作的情況下封包追蹤的範例：

```
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
```

以下是封包路徑的視覺化表示：



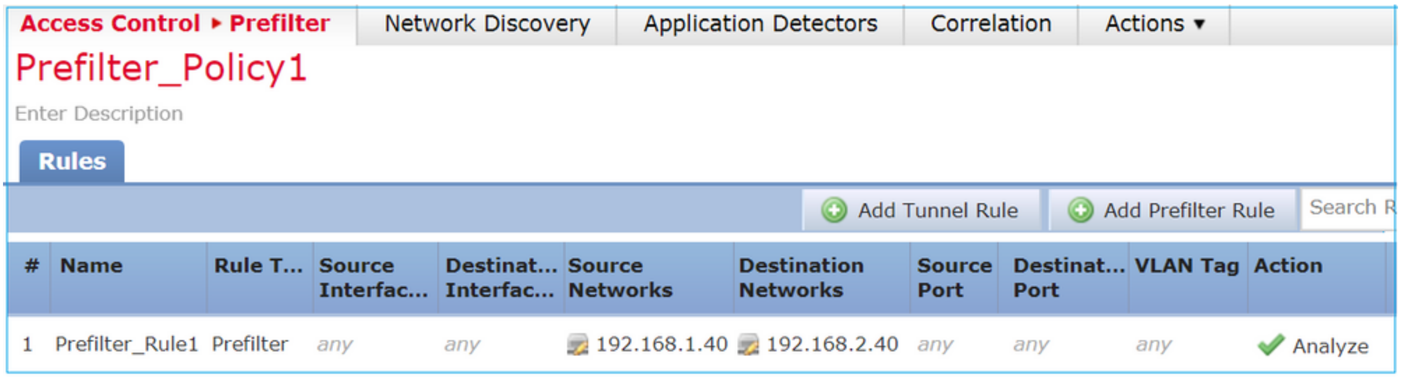
預先篩選原則 Fastpath 動作（使用 Tap 的內嵌集合）

與內嵌集合情況相同

預先篩選原則 Analyze 動作

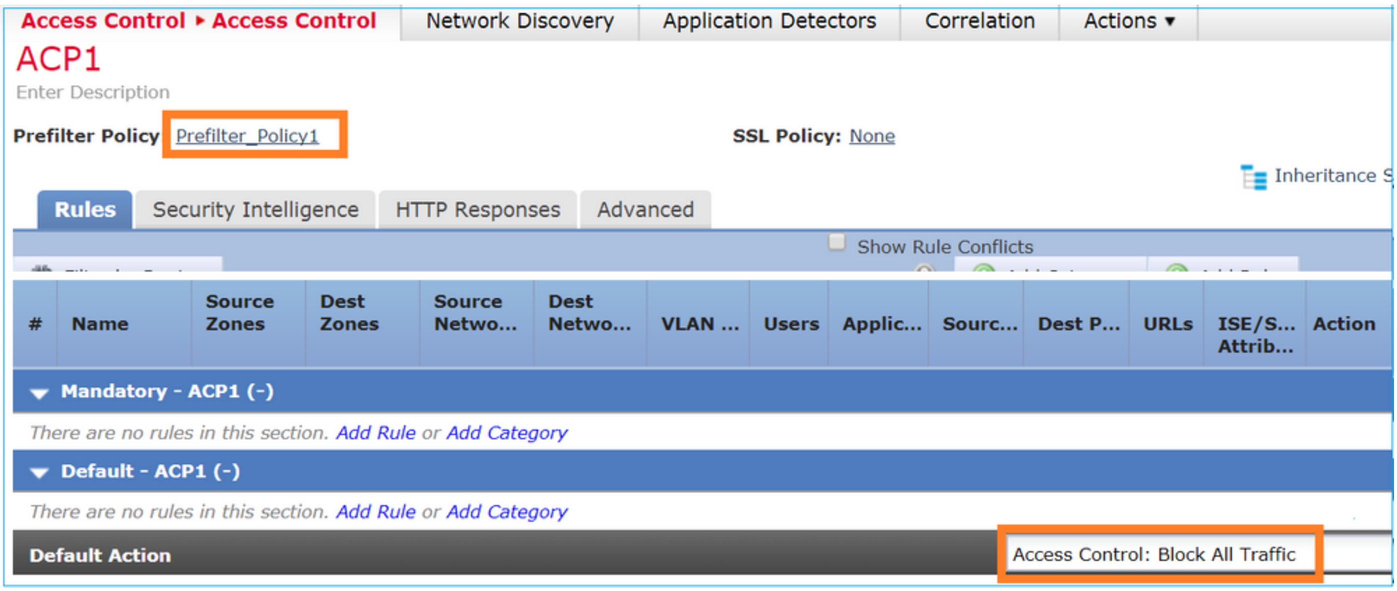
情況 1. 使用 ACP Block 規則的預先篩選 Analyze

考量包含 Analyze 規則的預先篩選原則，如下圖所示：



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

ACP僅包含設定為的預設規則 **Block All Traffic** 如下圖所示：



Prefilter Policy Prefilter_Policy1

SSL Policy: None

#	Name	Source Zones	Dest Zones	Source Netwo...	Dest Netwo...	VLAN ...	Users	Applic...	Sourc...	Dest P...	URLs	ISE/S... Attrib...	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

這是FTD Snort引擎（ngfw.rules檔案）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 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.
```

此為 FTD LINA 引擎中部署的原則：

```
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
```

驗證行為

Packet Tracer顯示LINA允許該封包，並將其轉送到Snort引擎(由於 **permit** action)和Snort Engine返回 **Block** 判定結果，因為來自AC的預設操作已匹配。

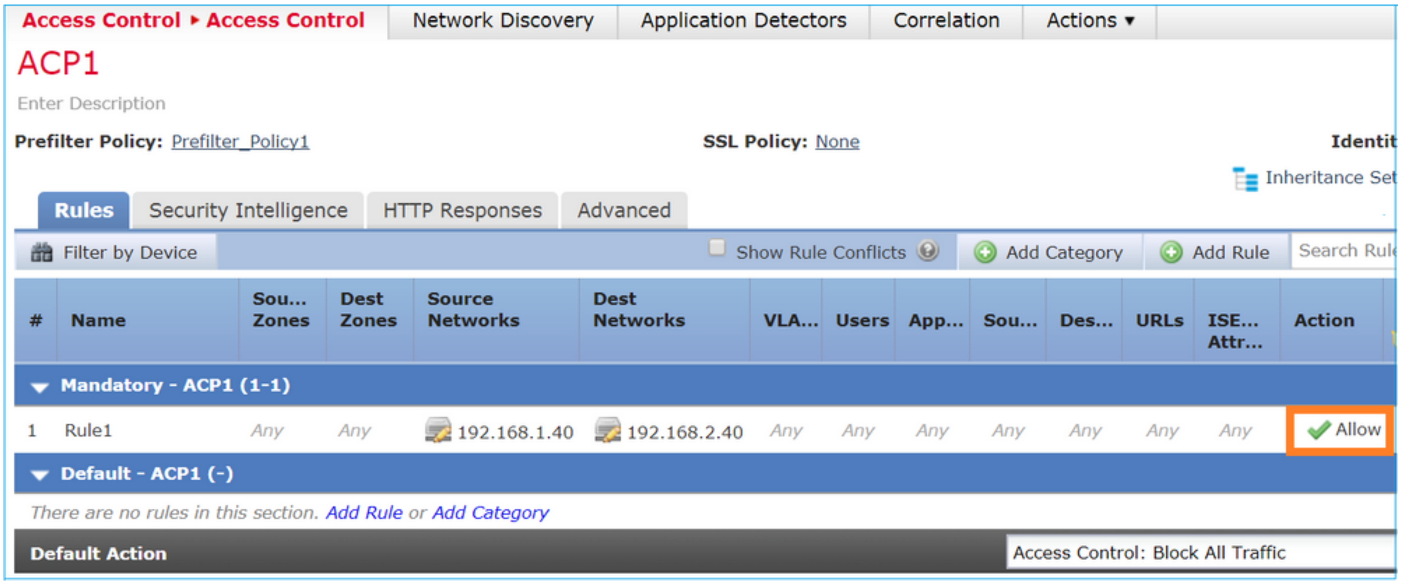
> **附註**：Snort 不會根據通道規則評估流量

當您追蹤封包時，封包會顯示相同結果：

```
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
```

情況 2. 使用 ACP Allow 規則的預先篩選 Analyze

如果目標允許封包通過 FTD，則需要在 ACP 中新增規則。動作可以是允許或信任，這取決於目標(例如，如果要應用L7檢測，必須使用 **Allow** action)，如下圖所示：



ACP1

Enter Description

Prefilter Policy: Prefilter_Policy1 SSL Policy: None Identit

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	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
▼ Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													

Default Action: Access Control: Block All Traffic

此為 FTD Snort 引擎中部署的原則：

```
# 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：

```
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
```

驗證行為

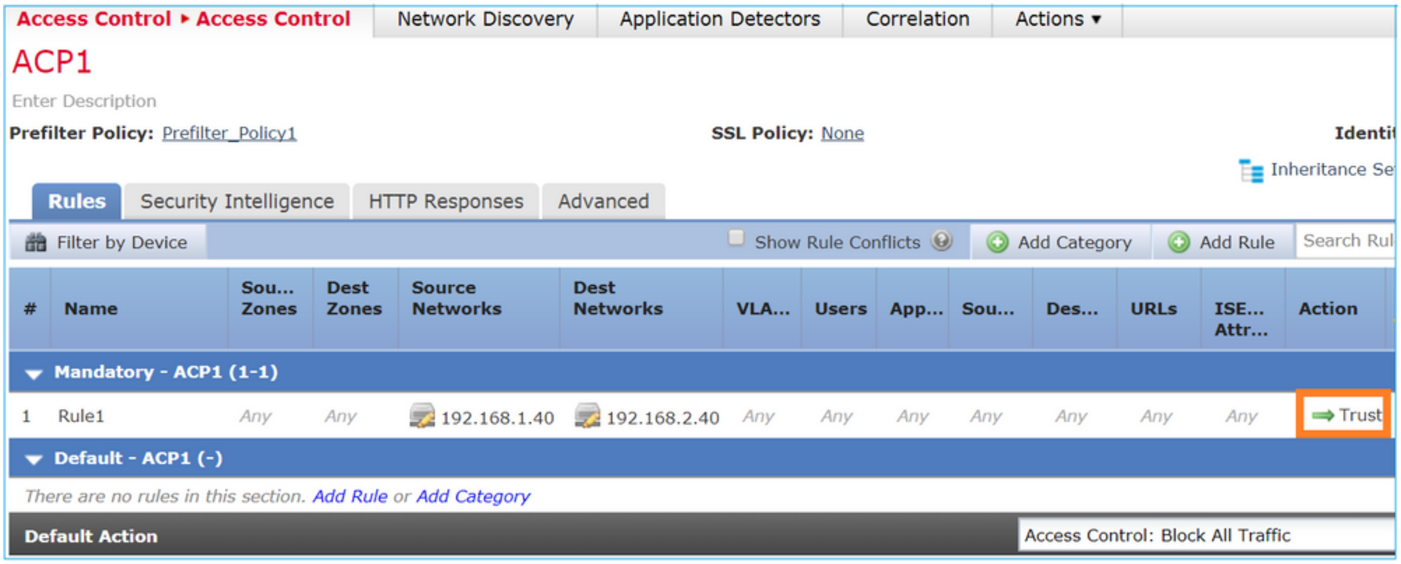
Packet Tracer顯示資料包匹配規則 **268435460** 在LINA和 **268435461** 在Snort引擎中：

```
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
```

案例 3. 使用 ACP Trust 規則的預先篩選 Analyze

如果 ACP 包含 Trust 規則，則您會取得下圖所示的結果：



Access Control ▸ Access Control | Network Discovery | Application Detectors | Correlation | Actions ▾

ACP1

Enter Description

Prefilter Policy: Prefilter_Policy1 SSL Policy: None Identi

Inheritance Se

Rules | Security Intelligence | HTTP Responses | Advanced

Filter by Device □ Show Rule Conflicts Add Category Add Rule Search Rul

#	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLA...	Users	App...	Sou...	Des...	URLs	ISE... Attr...	Action
▾ Mandatory - ACP1 (1-1)													
1	Rule1	Any	Any	192.168.1.40	192.168.2.40	Any	Any	Any	Any	Any	Any	Any	⇒ Trust
▾ Default - ACP1 (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action													Access Control: Block All Traffic

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  (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
```

請記住，由於預設情況下啟用了SI，因此信任規則部署為 **permit** 在LINA上執行的動作，因此至少有少數封包重新導向到Snort引擎進行檢查。

驗證行為

Packet Tracer顯示Snort引擎允許列出封包，並從根本上將其餘流量解除安裝到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
```

案例 4. 使用 ACP Trust 規則的預先篩選 Analyze

在此案例中，SI 以手動方式停用。

規則會部署於 Snort，如下所示：

```
# 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，該規則會部署為 Trust。根據Analyze Prefilter規則部署的允許規則（請參閱ACE命中計數）匹配的資料包，Snort引擎會檢查該資料包：

```
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
```

驗證行為

```
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
```

主要重點

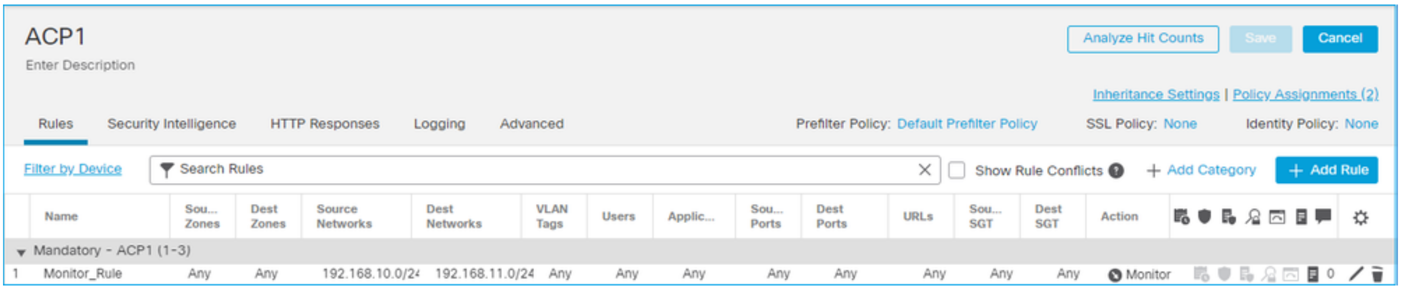
- 其 **Analyze** 操作在LINA引擎中部署為允許規則。這會對要轉送到Snort引擎進行檢查的封包產生影響
- 其 **Analyze** 操作不會在Snort引擎中部署任何規則，因此您需要確保在ACP中配置與Snort匹配的規則<
- 這取決於Snort引擎中部署的ACP規則(**block** 與 **allow** 與 **fastpath**)Snort不允許、也不允許全部或少數資料包

使用案例

- 使用案例 **Analyze** 操作是當您在預過濾器策略中有廣泛的Fastpath規則，並且希望為特定流放置一些例外以便由Snort對其進行檢查時

ACP Monitor 動作

FMC UI 中設定的 Monitor 規則：



	Name	Sou... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applic...	Sou... Ports	Dest Ports	URLs	Sou... SGT	Dest SGT	Action	
▾ Mandatory - ACP1 (1-3)															
1	Monitor_Rule	Any	Any	192.168.10.0/24	192.168.11.0/24	Any	Any	Any	Any	Any	Any	Any	Any	Monitor	0

監控規則部署在FTD LINA引擎上作為 **permit** 動作並向Snort引擎發出 **audit** 動作.

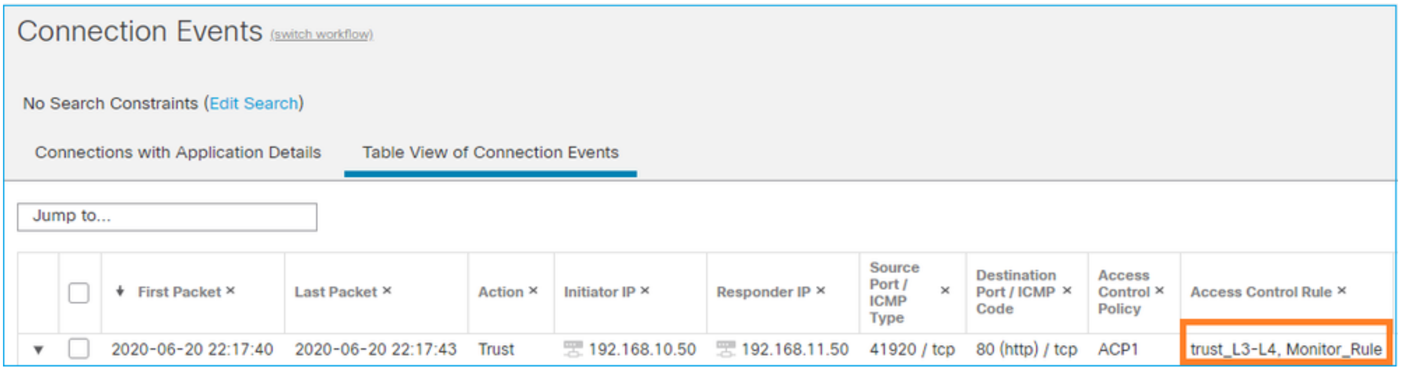
```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 10 advanced permit ip 192.168.10.0 255.255.255.0 192.168.11.0
255.255.255.0 rule-id 268438863 (hitcnt=0) 0x61bbaf0c
```

Snort 規則：

```
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
```

主要重點

- Monitor Rule不丟棄或允許流量，但生成連線事件。封包會根據後續規則受到檢查，且會受到允許或遭到捨棄
- FMC連線事件顯示資料包匹配了2個規則：


Connection Events
(switch workflow)
No Search Constraints (Edit Search)
Connections with Application Details
Table View of Connection Events
Jump to...

	☐	↓ First Packet ×	Last Packet ×	Action ×	Initiator IP ×	Responder IP ×	Source Port / ICMP Type ×	Destination Port / ICMP Code ×	Access Control Policy ×	Access Control Rule ×
▾	☐	2020-06-20 22:17:40	2020-06-20 22:17:43	Trust	192.168.10.50	192.168.11.50	41920 / tcp	80 (http) / tcp	ACP1	trust_L3-L4, Monitor_Rule

System support trace 輸出顯示資料包同時匹配兩個規則：

```
> system support trace

Enable firewall-engine-debug too? [n]: y
```

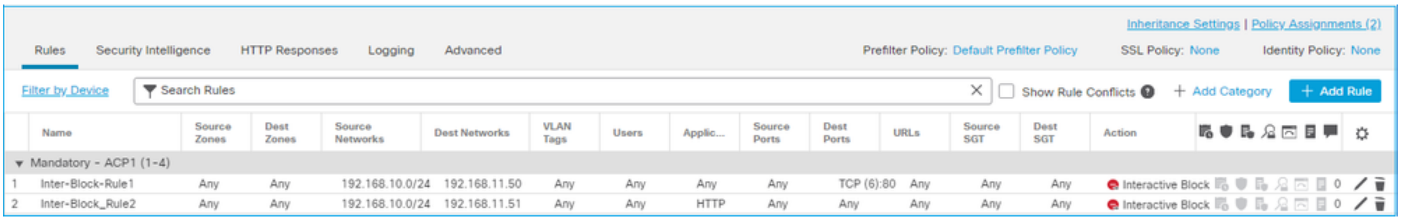
```
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.10.50
Please specify a client port:
Please specify a server IP address: 192.168.11.50
Please specify a server port:
Monitoring packet tracer and firewall debug messages


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 IPProto 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

用於監控網路活動與產生連線事件

ACP Interactive Block 動作

FMC UI 中設定的 Interactive Block 規則：



Prefilter Policy: Default Prefilter Policy   SSL Policy: None   Identity Policy: None

☐ Show Rule Conflicts

	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	Any	TCP (6):80	Any	Any	Any	Interactive Block	0	
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	0	

互動封鎖規則部署在FTD LINA引擎上作為 **permit** 作為旁路規則對Snort引擎執行操作：

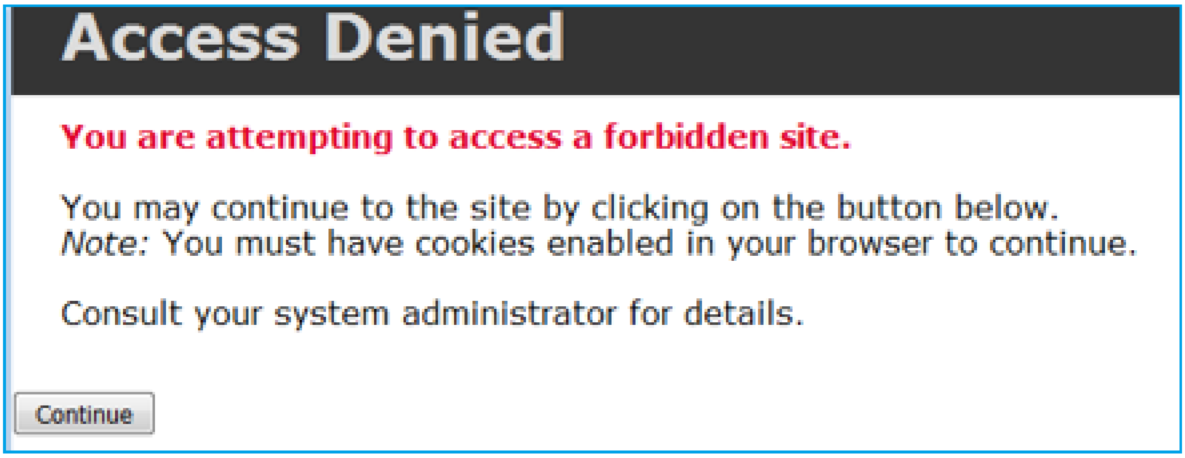
```
firepower# show access-list
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced permit tcp 192.168.10.0 255.255.255.0 host
192.168.11.50 eq www rule-id 268438864 (hitcnt=3) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark 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
```

Interactive Block 規則會提示使用者目的地遭到禁止



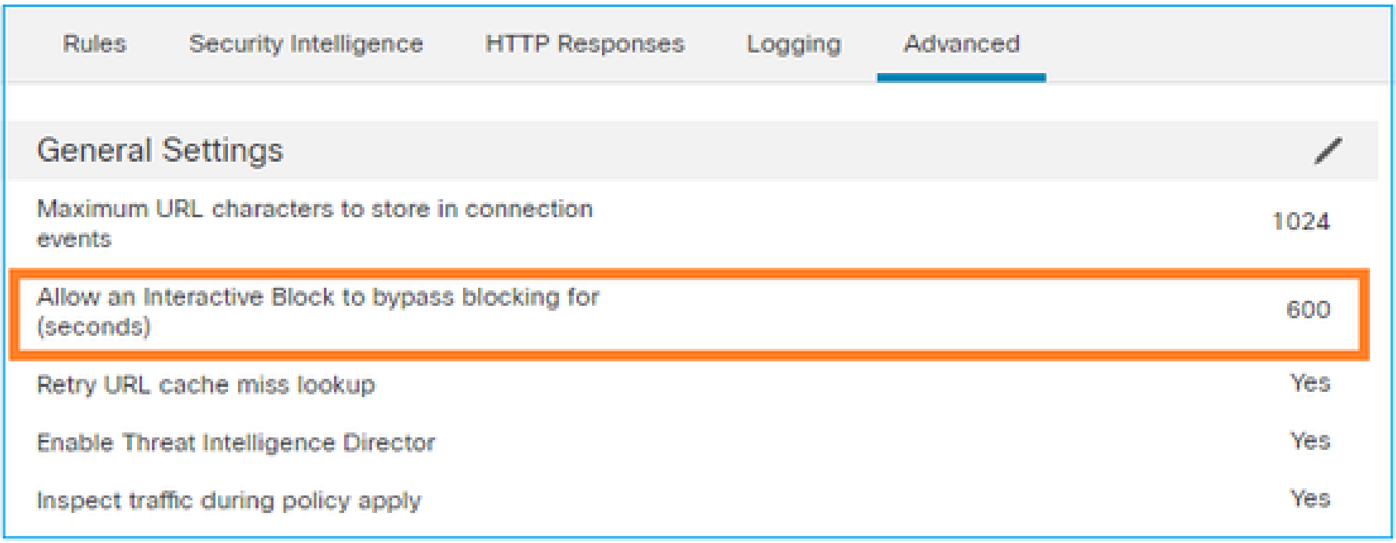
Access Denied

You are attempting to access a forbidden site.

You may continue to the site by clicking on the button below.
Note: You must have cookies enabled in your browser to continue.

Consult your system administrator for details.

依預設，防火牆會允許略過封鎖 600 秒：



General Settings

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

在 **system support trace** 輸出您可以看到防火牆最初阻止流量並顯示阻止頁面：

```
> 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
```

一旦使用者選擇 **Continue** （或刷新瀏覽器頁面）debug顯示資料包被同一規則允許，該規則模擬並 **Allow** action:

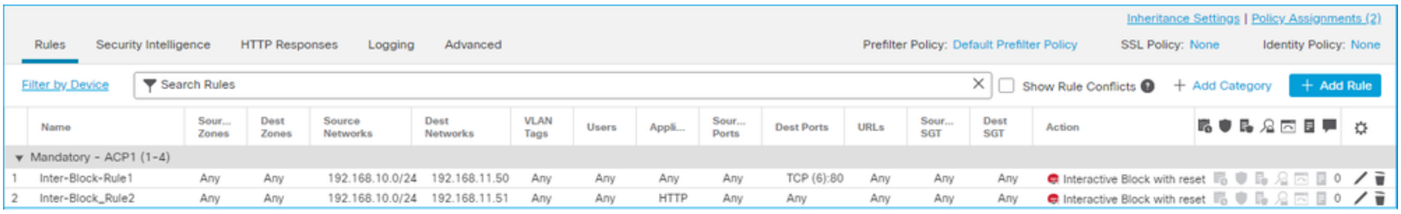
```
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1357413630, ack
2607625293
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application
unknown (0)
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 Starting AC with minimum 2, 'Inter-Block-
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 使用者顯示警告頁面，並提供其選項以繼續操作。

ACP Interactive Block with reset 動作

FMC UI 中設定的 Interactive Block with reset 規則：



Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: None

☐ Show Rule Conflicts

	Name	Sour... Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Appli...	Sour... Ports	Dest Ports	URLs	Sour... 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	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

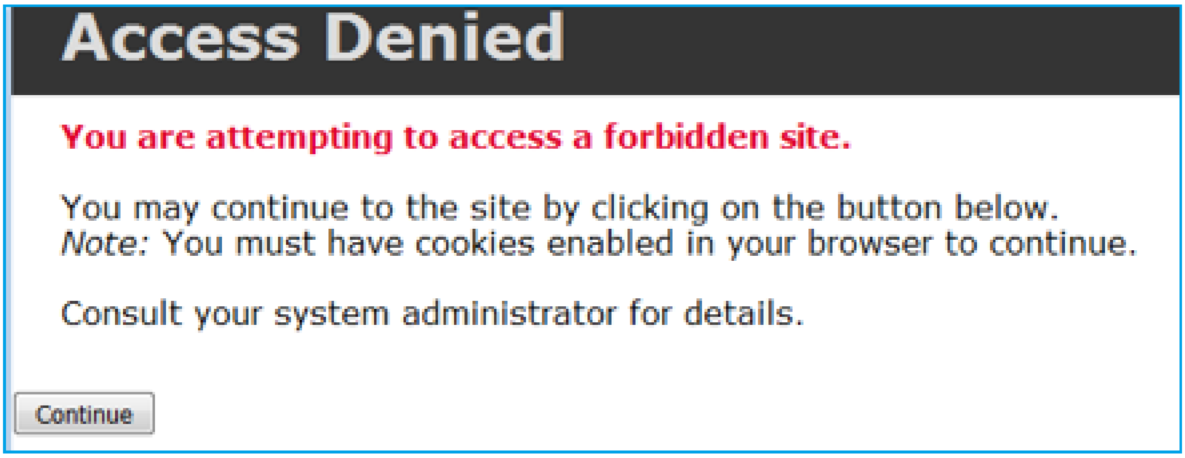
具有重設規則的互動封鎖部署在FTD LINA引擎上作為 **permit** 作為重置規則對Snort引擎執行操作：

```
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=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
```

與「阻止並重置」類似，使用者可以選擇 **Continue** 選項：



Access Denied

You are attempting to access a forbidden site.

You may continue to the site by clicking on the button below.
Note: You must have cookies enabled in your browser to continue.

Consult your system administrator for details.

在 Snort 偵錯中，顯示於 Interactive Reset 中的動作：

```
> 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
```

此時，將向終端使用者顯示阻止頁面。如果使用者選擇 **Continue**（或刷新網頁）與這次允許流量通過的規則相匹配：

```
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
```

Interactive Block with reset 規則會傳送 TCP RST 至非網路的流量：

```
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次要連線和 針孔

在較舊版本（例如6.2.2、6.2.3等）中，如果您使用 **Trust** 動作.在最新版本中，此行為會改變，並且 Snort引擎會開啟針孔，即使 **Trust** 動作.

FTD 規則指南

- 針對大流量使用預先篩選原則 Fastpath 規則，以減少通過方塊的延遲
- 針對必須根據 L3/L4 條件封鎖的流量使用預先篩選 Block 規則
- 如果您想要略過多數 Snort 檢查，但仍想要充分利用身分識別原則、QoS、SI、應用程式偵測、URL 篩選等功能，請使用 ACP Trust 規則
- 透過使用以下指南，設置對於存取控制原則頂端之防火牆效能影響不大的規則：

1. Block 規則（第 1 層至第 4 層）- 預先篩選 Block
2. Allow 規則（第 1 層至第 4 層）- 預先篩選 Fastpath
3. ACP Block 規則（第 1 層至第 4 層）
4. Trust 規則（第 1 層至第 4 層）
5. Block 規則（第 5 層至第 7 層 - 應用程式偵測、URL 篩選）
6. Allow 規則（第 1 層至第 7 層 - 應用程式偵測、URL 篩選、入侵原則/檔案原則）
7. Block 規則（預設規則）

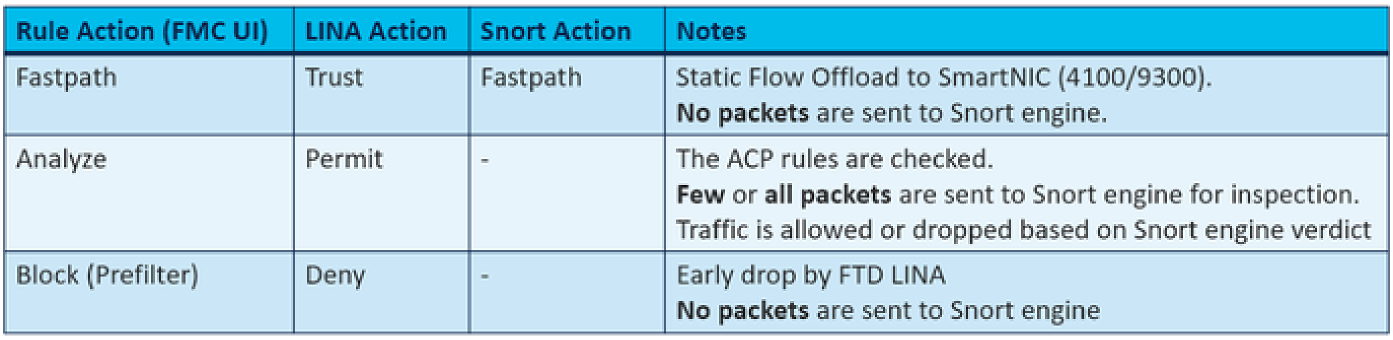
- 避免過度記錄（在開始或結束時記錄，並避免同時記錄）

- 注意規則擴充，檢查 LINA 中的規則數量

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

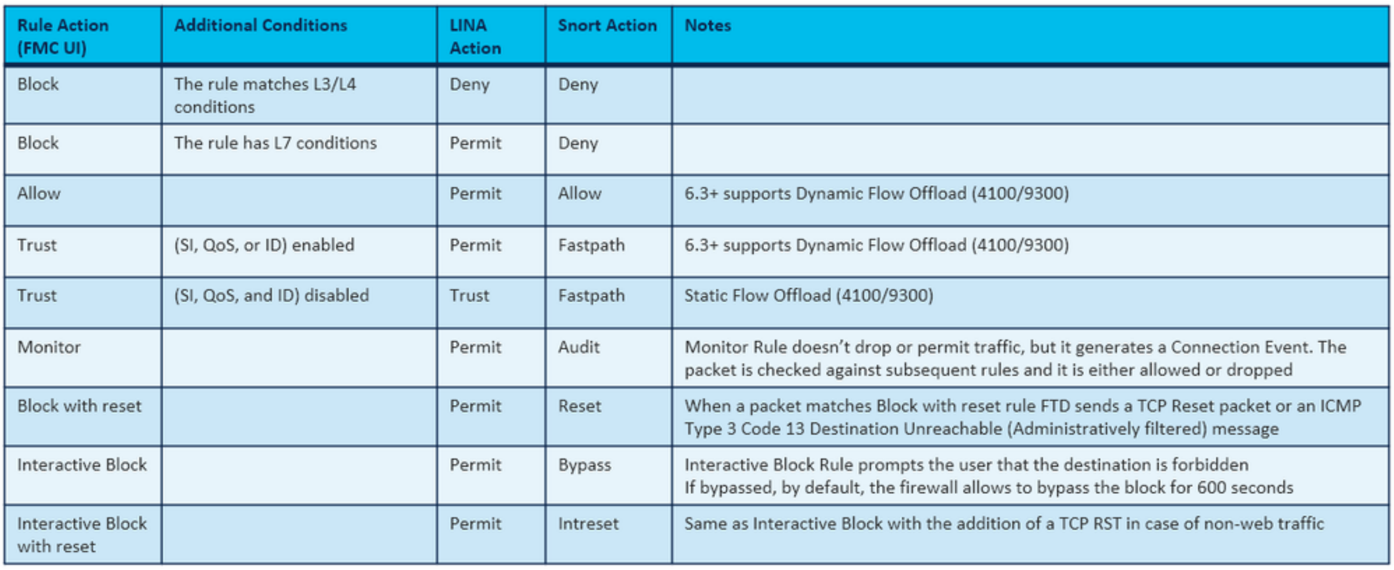
摘要

預先篩選動作



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 動作



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

附註：從6.3 FTD軟體代碼開始，動態流量分流可以分流符合其他標準的連線（例如需要Snort檢查的受信任封包）。如需詳細資料，請查看 Firepower 管理中心組態設定指南的「卸載大型連線（流量）」章節。

相關資訊

- FTD 存取控制規則
- FTD 預先篩選和預先篩選原則

- 分析 Firepower 防火牆擷取，以有效針對網路問題進行疑難排解
- 搭配使用 Firepower Threat Defense (FTD) 擷取和 Packet-Tracer
- 透過 FMC 設定 FTD 中的記錄
- 技術支援與文件 - Cisco Systems
- 卸載大型連線

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。