在內嵌配對模式下設定 FTD 介面

目錄

簡介

本檔案介紹Firepower威脅防禦(FTD)裝置上內嵌配對介面的組態、驗證和運作。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Firepower 4112 FTD（7.x版）
- Firepower管理中心(FMC)（7.x版）

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：

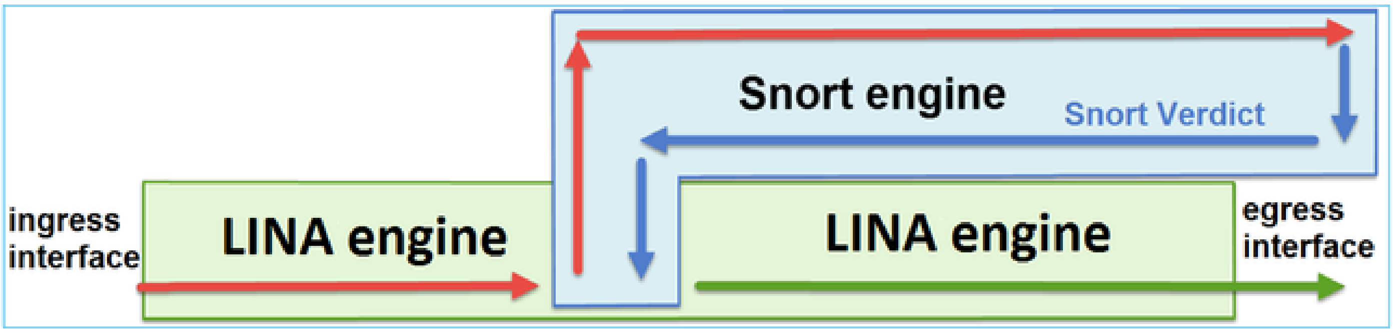
- FPR1000、FPR2100、FPR4100、FPR9300
- 安全防火牆3100和4200系列
- vFTD
- FTD 軟體 6.2.x 及更新版本

背景資訊

FTD 是一個整合的軟體映像，其中包括 2 個主引擎：

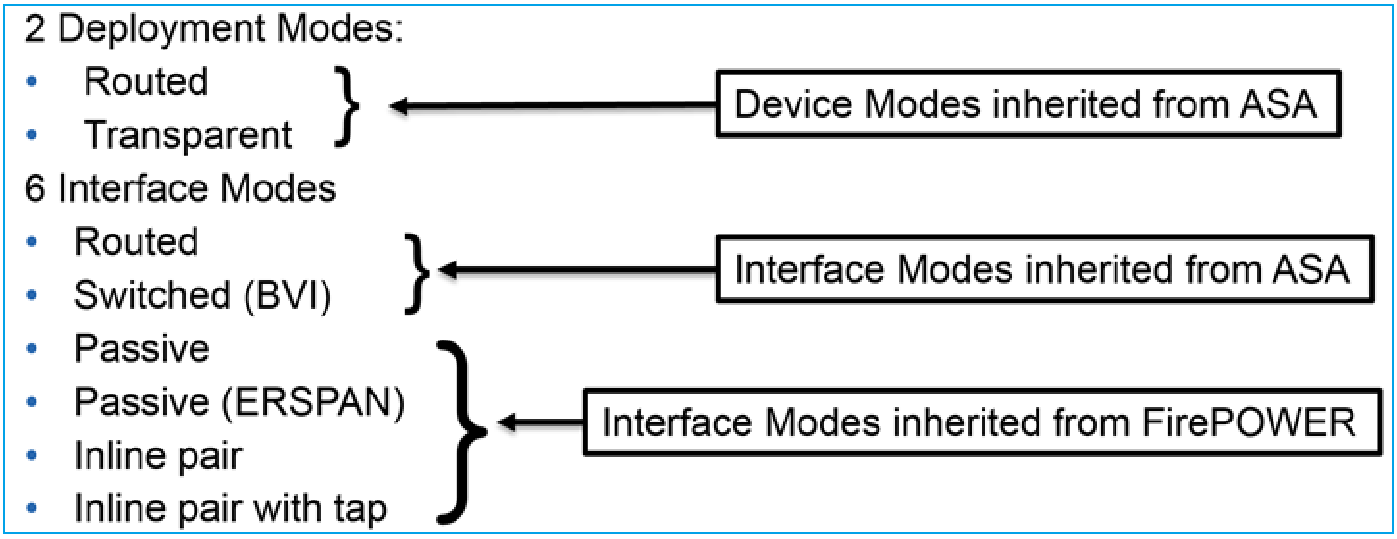
1. LINA 引擎
2. Snort 引擎

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。
- LINA 引擎根據 Snort 的判定結果捨棄或轉送封包.

FTD提供兩種部署模式和六種介面模式，如下圖所示：



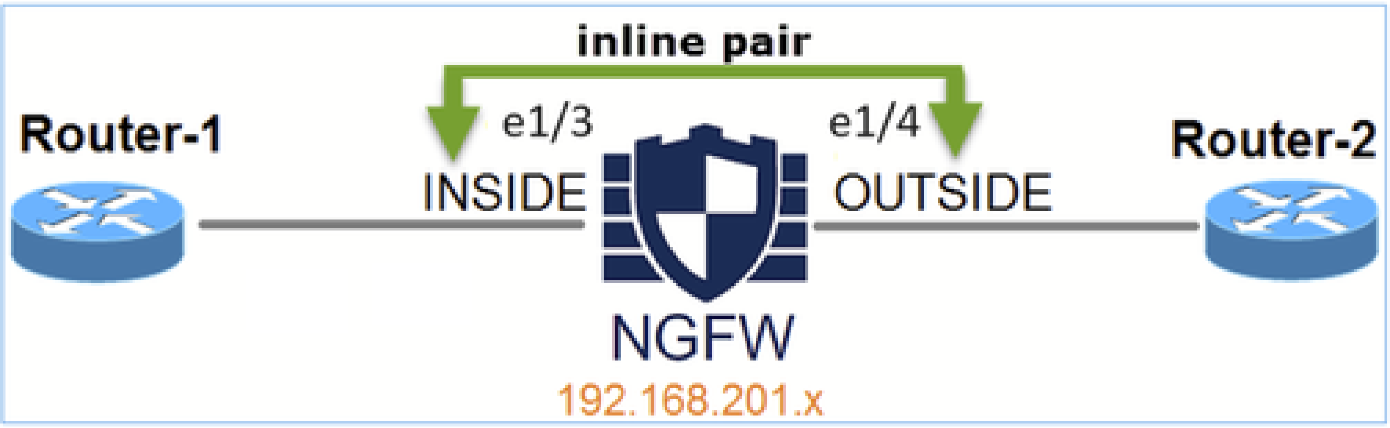
附註：您可以在單一 FTD 設備上混合使用介面模式。

以下簡要概述各種 FTD 部署和介面模式：

FTD 介面模式	FTD 部署模式	說明	流量可能遭捨棄
循路	循路	完整 LINA 引擎和 Snort 引擎檢查.	是
交換	透明	完整 LINA 引擎和 Snort 引擎檢查.	是
內嵌配對	路由或透明	部分 LINA 引擎和完整 Snort 引擎檢查.	是
使用分流器的內嵌配對	路由或透明	部分 LINA 引擎和完整 Snort 引擎檢查.	否
被動	路由或透明	部分 LINA 引擎和完整 Snort 引擎檢查.	否
被動 (ERSPAN)	循路	部分 LINA 引擎和完整 Snort 引擎檢查.	否

設定 FTD 上的內嵌配對介面

網路圖表



需求

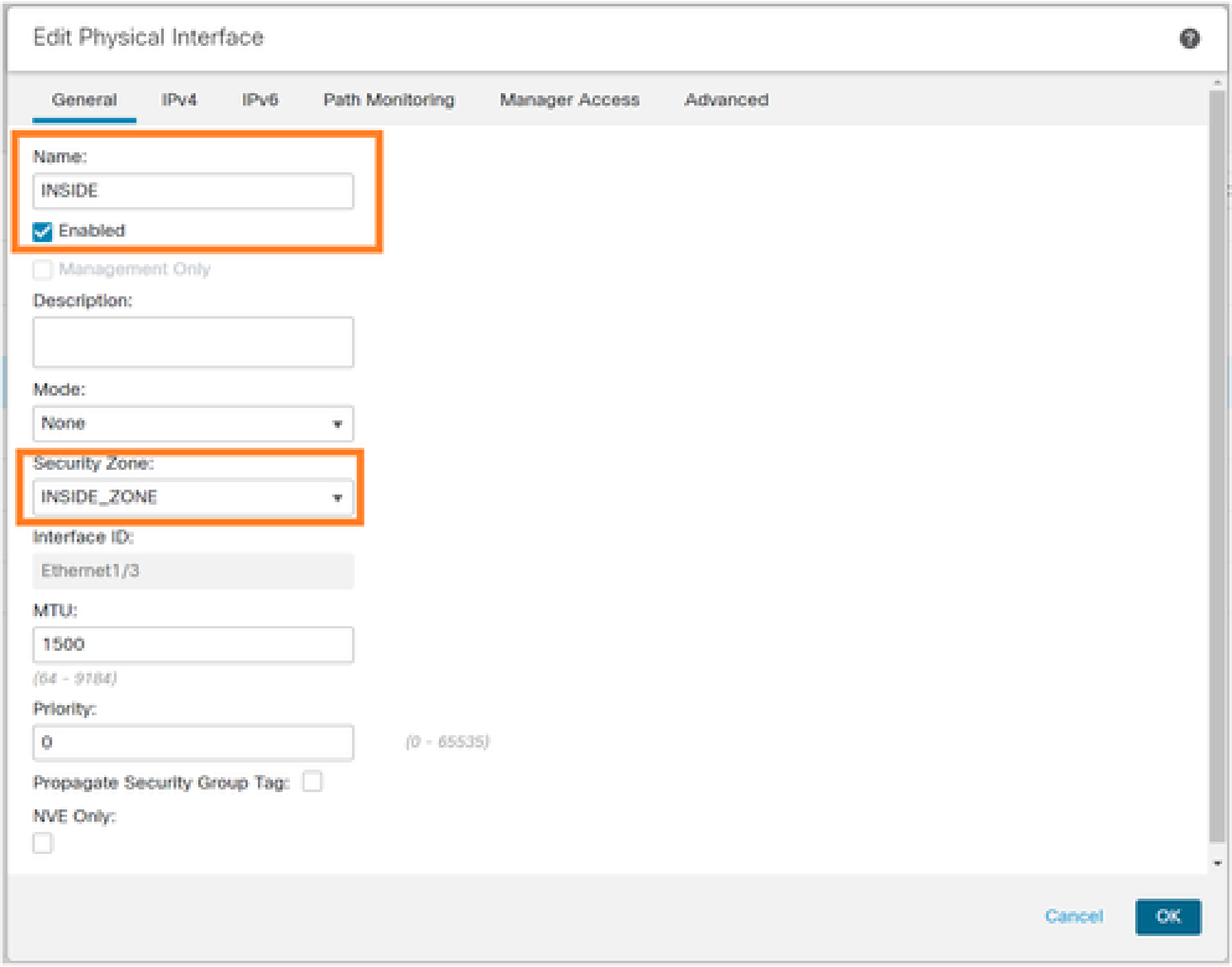
根據以下要求，在內嵌配對模式下設定實體介面e1/3和e1/4:

介面	e1/3	e1/4
名稱	INSIDE	OUTSIDE
安全區域	INSIDE_ZONE	OUTSIDE_ZONE
內嵌集名稱	Inline-Pair-1	
內嵌集 MTU	1500	
傳播連結狀態	已啟用	

解決方案

步驟1。若要設定個別介面，請導覽至Devices > Device Management，選擇適當的裝置，然後選擇Edit:

接下來，指定介面的名稱並勾選 Enabled，如下圖所示。



Edit Physical Interface

Name: INSIDE

☑ Enabled

□ Management Only

Description:

Mode: None

Security Zone: INSIDE_ZONE

Interface ID: Ethernet1/3

MTU: 1500 (64 - 9184)

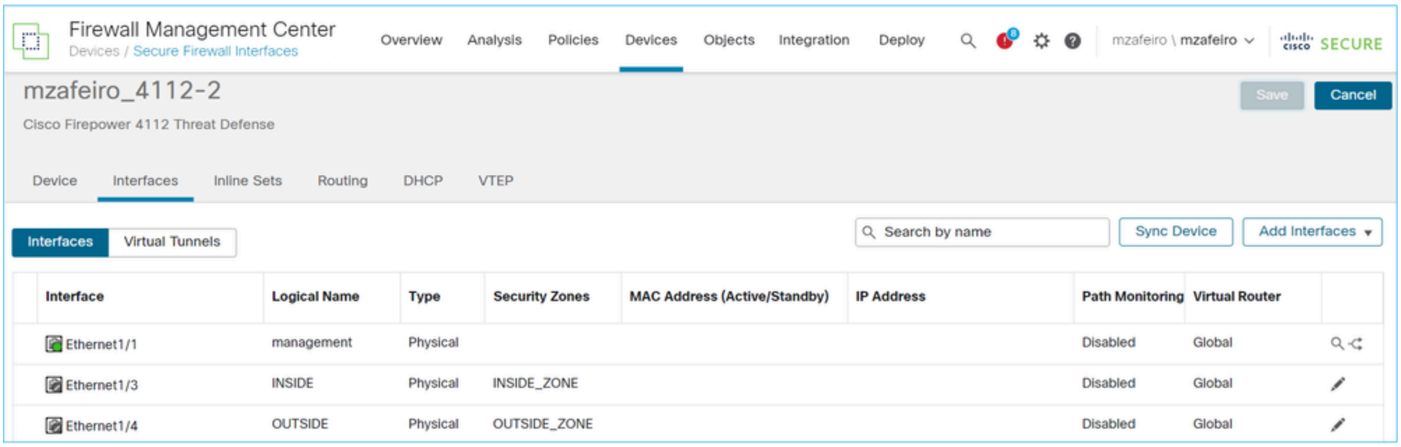
Priority: 0 (0 - 65535)

Propagate Security Group Tag: □

NVE Only: □

附註：名稱是介面的名稱。

類似地，對於介面Ethernet1/4。最後結果如下：



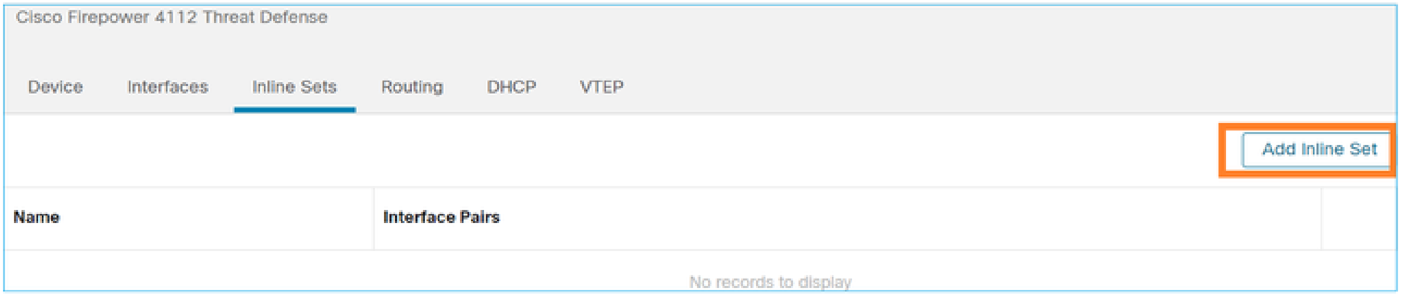
mzafeiro_4112-2

Cisco Firepower 4112 Threat Defense

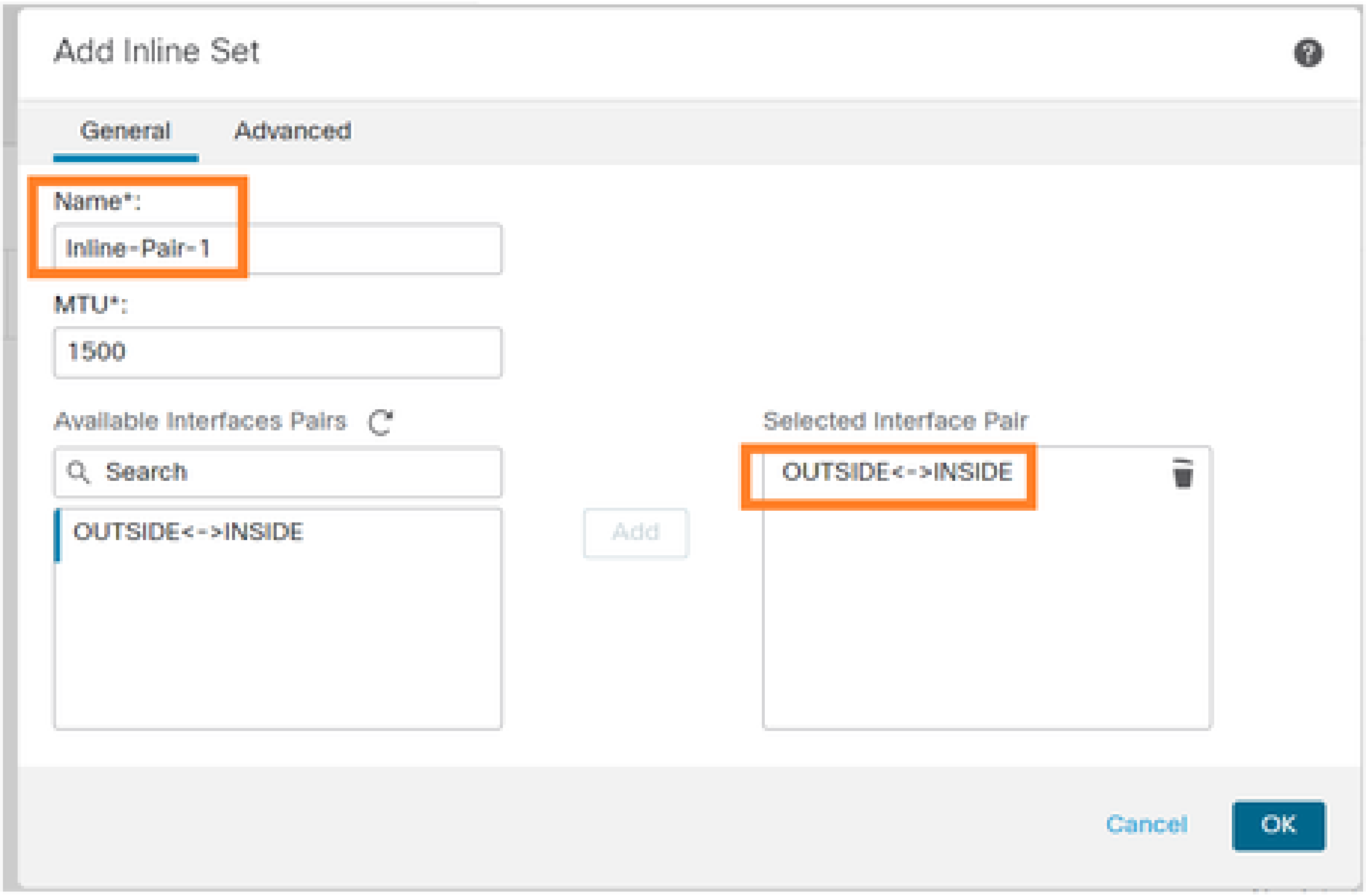
Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Ethernet1/1	management	Physical				Disabled	Global
Ethernet1/3	INSIDE	Physical	INSIDE_ZONE			Disabled	Global
Ethernet1/4	OUTSIDE	Physical	OUTSIDE_ZONE			Disabled	Global

步驟 2. 設定內嵌配對。

導覽至 Inline Sets > Add Inline Set，如下圖所示。



步驟 3. 根據要求配置「General」設定，如下圖所示。



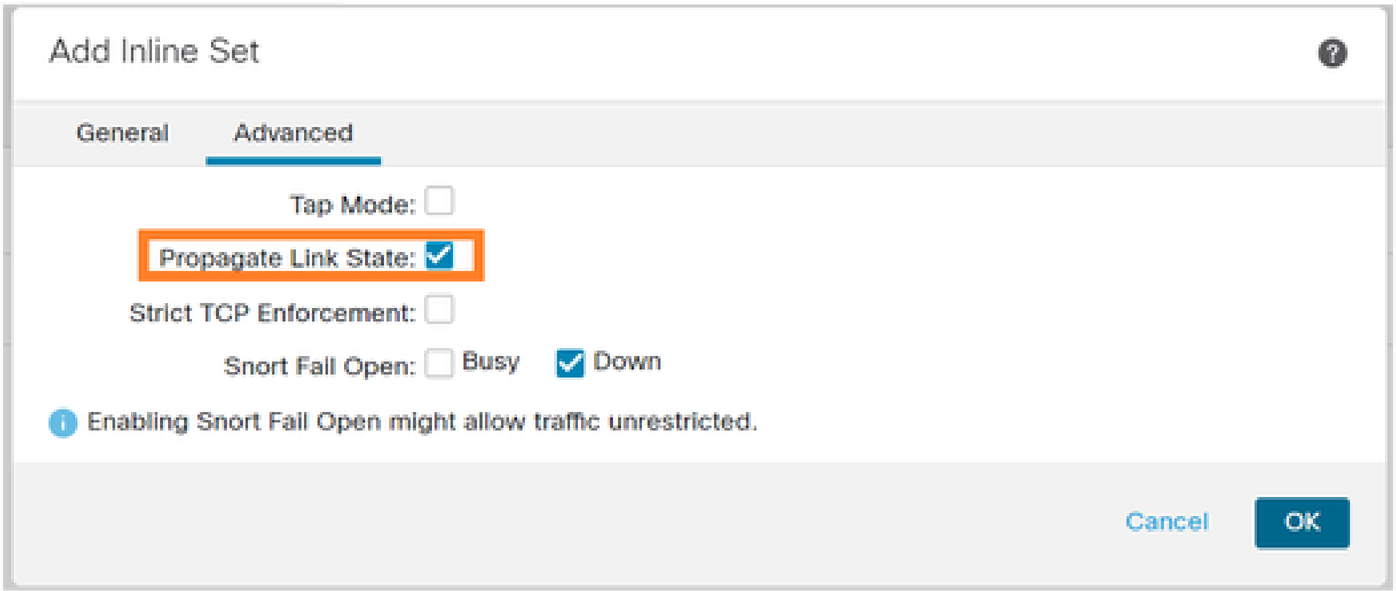
Name*: Inline-Pair-1

MTU*: 1500

OUTSIDE<->INSIDE

Selected Interface Pair: OUTSIDE<->INSIDE

步驟 4. 在「Advanced Settings」底下啟用 Propagate Link State 選項，如下圖所示。



Add Inline Set

Tap Mode: □

Propagate Link State: ☑

Strict TCP Enforcement: □

Snort Fail Open: □ Busy ☑ Down

Enabling Snort Fail Open might allow traffic unrestricted.

當內嵌集中的一個介面關閉時，連結狀態傳播會自動關閉內嵌介面配對中的第二個介面。

步驟 5. 儲存變更並進行部署。

驗證

使用本節內容，確認您的組態是否正常運作。

從 FTD CLI 驗證內嵌配對組態。

解決方案

登入 FTD CLI 並驗證內嵌配對組態：

<#root>

```
firepower#

show inline-set
```

```
Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"
      Current-Status: UP
    Interface: Ethernet1/3 "INSIDE"
      Current-Status: UP
    Bridge Group ID: 507
```

附註：網橋組ID的值不同於0。如果分流器模式為開啟狀態，則值為0。

介面和名稱資訊：

<#root>

```
firepower#

show nameif


Interface        Name             Security
Ethernet1/1      management        0
Ethernet1/3      INSIDE            0
Ethernet1/4      OUTSIDE           0
```

驗證介面狀態：

<#root>

```
firepower#

 show interface ip brief


Interface              IP-Address    OK? Method Status Protocol
Internal-Control0/0    unassigned    YES unset  up     up
Internal-Data0/0       unassigned    YES unset  up     up
Internal-Data0/1       unassigned    YES unset  up     up
Internal-Data0/2       169.254.1.1   YES unset  up     up
Internal-Data0/3       unassigned    YES unset  up     up
Internal-Data0/4       unassigned    YES unset  down   up
Ethernet1/1            203.0.113.130 YES unset  up     up

Ethernet1/3            unassigned    YES unset  up     up



Ethernet1/4            unassigned    YES unset  up     up
```

驗證實體介面資訊：

<#root>

```
firepower#
```

```
show interface e1/3


Interface Ethernet1/3 "INSIDE", is up, line protocol is up

  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
           MAC address ac4a.670e.641e, MTU 1500

IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1

           IP address unassigned
  Traffic Statistics for "INSIDE":
           170 packets input, 12241 bytes
            41 packets output, 7881 bytes
             9 packets dropped
      1 minute input rate 0 pkts/sec, 37 bytes/sec
      1 minute output rate 0 pkts/sec, 19 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec, 34 bytes/sec
      5 minute output rate 0 pkts/sec, 23 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

驗證 FTD 內嵌配對介面作業

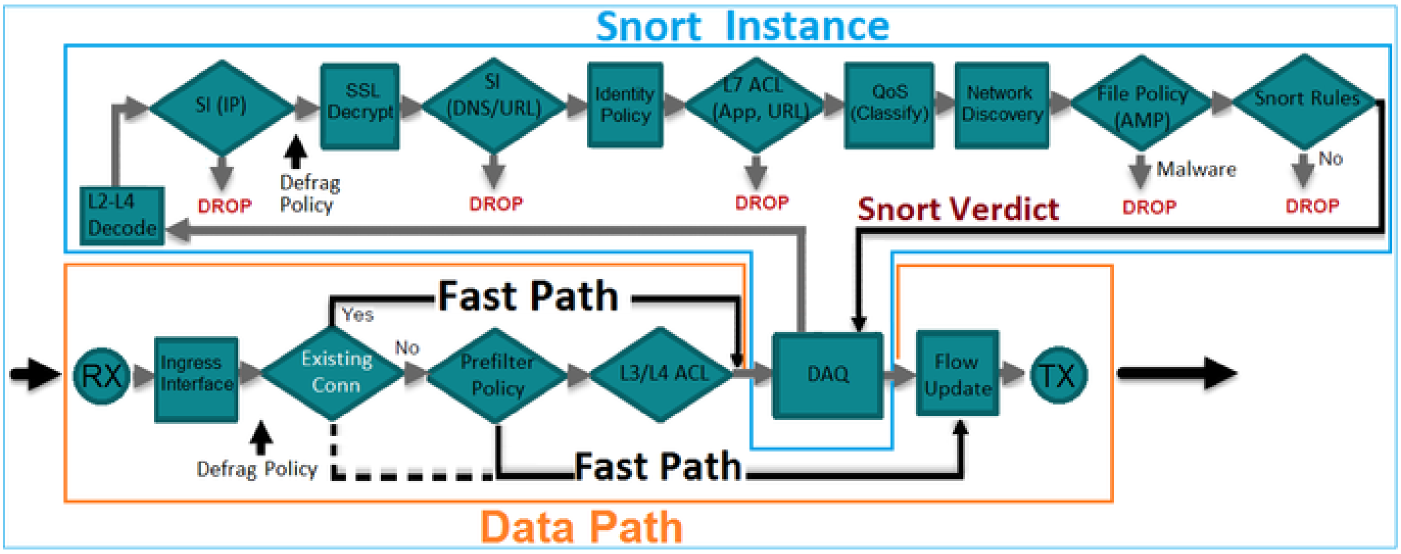
本節說明這些用於驗證內嵌配對作業的驗證檢查：

- 驗證1.使用Packet Tracer。
- 驗證2.啟用含有追蹤軌跡的擷取，並透過內嵌配對傳送TCP同步/確認(SYN/ACK)封包。
- 驗證 3. 使用防火牆引擎偵錯來監控 FTD 流量
- 驗證4.驗證連結狀態傳播功能。
- 驗證5.設定靜態網路位址轉譯(NAT)。

解決方案

架構概覽

當兩個FTD介面以內嵌配對模式運作時，系統會處理封包，如下圖所示。

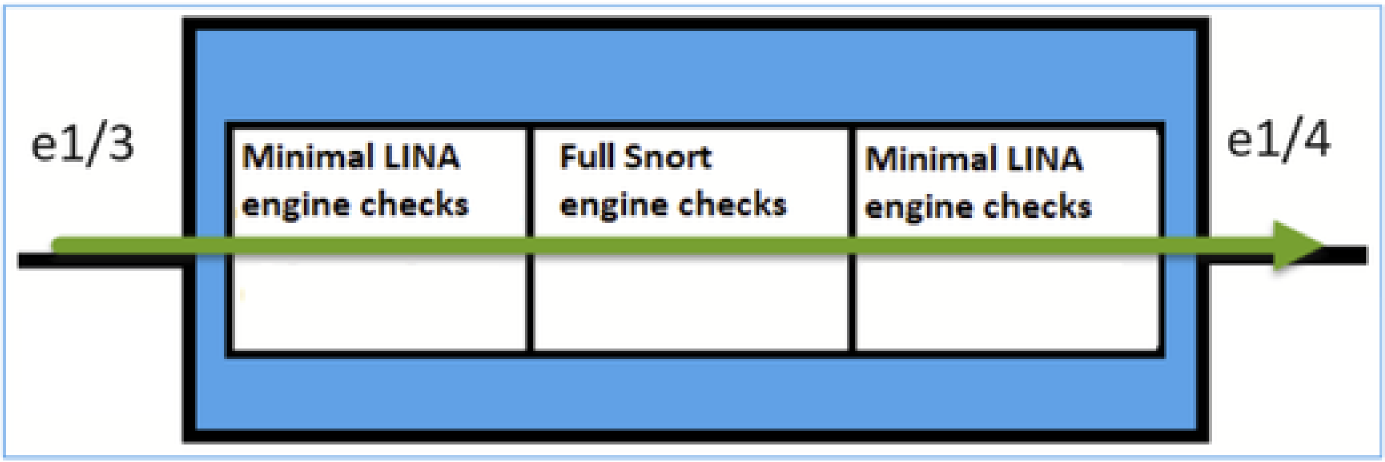


附註：只有實體介面可以是內嵌配對集的成員.

基本原理

- 設定內嵌配對2實體時，介面會在內部橋接。
- 非常類似傳統內嵌入侵防護系統(IPS)。
- 在路由或透明部署模式下可使用.
- 大多數LINA引擎功能（NAT、路由等）不可用於穿越內嵌配對的資料流。
- 傳輸流量可能遭捨棄.
- 有幾個 LINA 引擎檢查會隨完整 Snort 引擎檢查一起套用.

最後一點可以用視覺化方式呈現，如下圖所示：



驗證1.使用Packet Tracer

Packet Tracer 輸出（模擬穿越內嵌配對的封包），其中突顯出幾點重要事項：

<#root>

```
firepower#

packet-tracer input INSIDE tcp 192.168.201.50 1111 192.168.202.50 80



Phase: 1


Type: NGIPS-MODE


Subtype: ngips-mode


Result: ALLOW


Elapsed time: 11834 ns


Config:


Additional Information:


The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied



Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 11834 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.201.50 host 192.168.202.50 rule-id 268451044
access-list CSM_FW_ACL_ remark rule-id 268451044: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451044: L7 RULE: New-Rule-#1303-ALLOW
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached


Phase: 3


Type: NGIPS-EGRESS-INTERFACE-LOOKUP


Subtype: Resolve Egress Interface


Result: ALLOW
```

Elapsed time: 2440 ns

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
Elapsed time: 68320 ns
Config:
Additional Information:
New flow created with id 1801, packet dispatched to next module

Phase: 5
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 18056 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 6
Type: SNORT
Subtype: identity
Result: ALLOW
Elapsed time: 13668 ns
Config:
Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc

Phase: 7
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 67770 ns
Config:
Network 0, Inspection 0, Detection 0, Rule ID 268451044
Additional Information:
Starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt:
Matched rule ids 268451044 - Allow

Phase: 8
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 11002 ns
Config:
```

```
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:

input-interface: INSIDE(vrfid:0)


input-status: up


input-line-status: up


output-interface: OUTSIDE(vrfid:0)


output-status: up


output-line-status: up


Action: allow

Time Taken: 204924 ns
```

驗證 2. 透過內嵌配對傳送 TCP SYN/ACK 封包

您可以使用製作出 Scapy 這類公用程式的封包來產生 TCP SYN/ACK 封包。此語法會產生 3 個已啟用 SYN/ACK 旗標的封包：

<#root>

```
root@KALI:~#

scapy

INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>>

conf.iface='eth0'

>>>

packet = IP(dst="192.168.201.60")/TCP(flags="SA",dport=80)

>>>

syn_ack=[]
```

```
>>>

for i in range(0,3): # Send 3 packets

...

syn_ack.extend(packet)

...
>>>

send(syn_ack)
```

在 FTD CLI 上啟用此擷取，並傳送幾個 TCP SYN/ACK 封包：

<#root>

```
firepower#

capture CAPI interface INSIDE trace match ip host 192.168.201.60 any


firepower#

capture CAPO interface OUTSIDE match ip host 192.168.201.60 any
```

擷取顯示3個SYN/ACK封包在FTD中周遊：

<#root>

```
firepower#

show capture CAPI



3 packets captured

1: 09:20:18.206440 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
2: 09:20:18.208180 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3: 09:20:18.210026 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
firepower#

show capture CAPO



3 packets captured

1: 09:20:18.206684 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
2: 09:20:18.208210 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3: 09:20:18.210056 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
```

第一個擷取封包的追蹤軌跡顯示一些額外資訊，例如Snort引擎判定結果：

<#root>

```
firepower#

show capture CAPI packet-number 1 trace



3 packets captured

1: 09:20:18.206440 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Elapsed time: 5978 ns
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 5978 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.201.50 object-group FMC_INLINE_dst_rule_2684510
access-list CSM_FW_ACL_ remark rule-id 268451044: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451044: L7 RULE: New-Rule-#1303-ALLOW
object-group network FMC_INLINE_dst_rule_268451044
network-object 192.168.202.50 255.255.255.255
network-object 192.168.201.60 255.255.255.255
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 1952 ns
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
Elapsed time: 45872 ns
Config:
Additional Information:
New flow created with id 1953, packet dispatched to next module

Phase: 5
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
```

```
Elapsed time: 18544 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 6
Type: SNORT
Subtype: identity
Result: ALLOW
Elapsed time: 25182 ns
Config:
Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc

Phase: 7

Type: SNORT

Subtype: firewall

Result: ALLOW

Elapsed time: 50924 ns

Config:

Network 0, Inspection 0, Detection 0, Rule ID 268451044

Additional Information:

Starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 

Matched rule ids 268451044 - Allow


Phase: 8
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 17722 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:
input-interface: INSIDE(vrfid:0)
```

```
input-status: up
input-line-status: up
output-interface: OUTSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 172152 ns


1 packet shown
```

第二個擷取封包的追蹤軌跡顯示封包與現有連線相符，因此會繞過ACL檢查，但Snort引擎仍會對其進行檢查：

<#root>

```
firepower#
```

show capture CAPI packet-number 2 trace

```
3 packets captured

2: 09:20:18.208180 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 1952 ns
Config:
Additional Information:
```

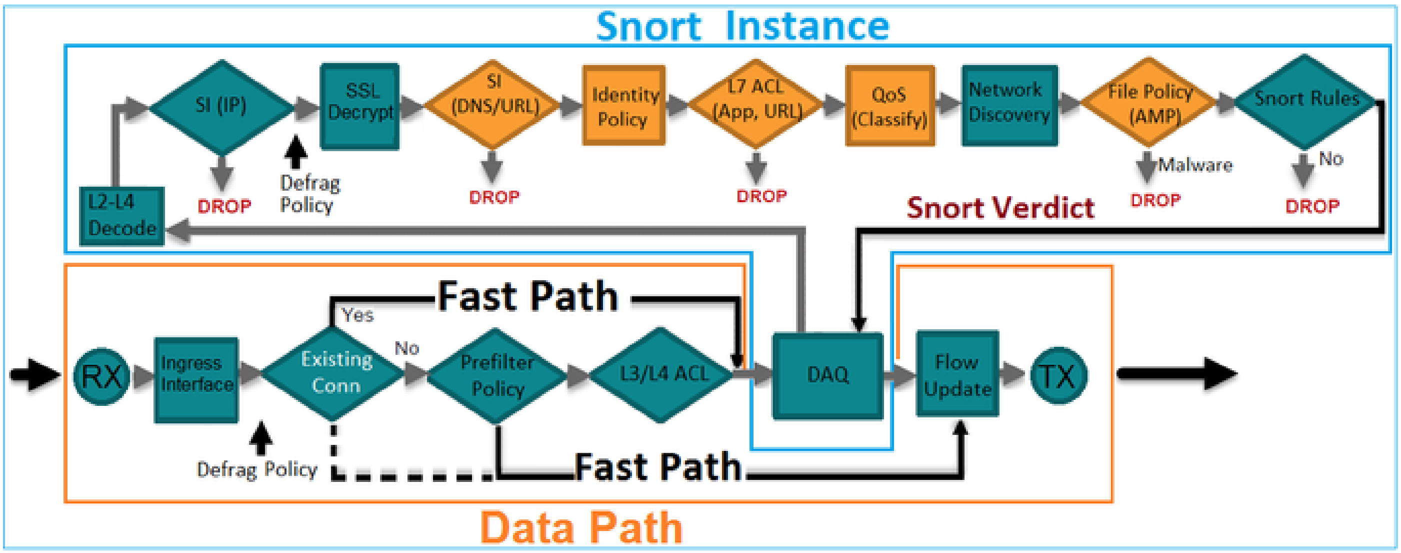
Found flow with id 1953, using existing flow

```
Phase: 2
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 7320 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 3
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 1860 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
```

```
Action: allow
Time Taken: 11132 ns


1 packet shown
```

驗證 3. 針對允許的流量進行防火牆引擎偵錯

針對FTD Snort引擎的特定元件（例如存取控制原則）執行防火牆引擎偵錯，如下圖所示：



透過內嵌配對傳送TCP SYN/ACK封包時，可以在偵錯輸出中看到：

```
<#root>

>

system support firewall-engine-debug



Please specify an IP protocol:

tcp


Please specify a client IP address:
Please specify a client port:
Please specify a server IP address:

192.168.201.60


Please specify a server port:

80


Monitoring firewall engine debug messages


192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 New session
```

```
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 using HW or preset rule order 3, id 268438528 action A
```

```
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 allow action
```

```
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 Deleting session
```

驗證 4. 驗證連結狀態傳播

在FTD上啟用緩衝區記錄功能，並關閉連線到e1/4介面的switchport。在FTD CLI上，您必須看到兩個介面都已關閉：

<#root>

```
firepower#

show interface ip brief

Interface              IP-Address     OK? Method Status     Protocol
Internal-Control0/0    unassigned     YES unset  up         up
Internal-Data0/0       unassigned     YES unset  up         up
Internal-Data0/1       unassigned     YES unset  up         up
Internal-Data0/2       169.254.1.1    YES unset  up         up
Internal-Data0/3       unassigned     YES unset  up         up
Internal-Data0/4       unassigned     YES unset  down       up
Ethernet1/1            203.0.113.130  YES unset  up         up

Ethernet1/3            unassigned     YES unset  admin down down


Ethernet1/4            unassigned     YES unset  down       down
```

FTD 記錄顯示：

<#root>

```
firepower#

show log

...

May 28 2024 07:35:10: %FTD-4-411002: Line protocol on Interface Ethernet1/4, changed state to down


May 28 2024 07:35:10: %FTD-4-411004: Interface INSIDE, changed state to administratively down
May 28 2024 07:35:10: %FTD-4-411004: Interface Ethernet1/3, changed state to administratively down


May 28 2024 07:35:10: %FTD-4-812005: Link-State-Propagation activated on inline-pair due to failure of i


May 28 2024 07:35:10: %FTD-4-411002: Line protocol on Interface Ethernet1/3, changed state to down
```

內嵌集狀態顯示 2 個介面成員的狀態：

<#root>

```
firepower#

show inline-set



Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off


Propagate-link-state option is on


  hardware-bypass mode is disabled
    Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"


    Current-Status: Down(Propagate-Link-State-Activated)


    Interface: Ethernet1/3 "INSIDE"


Current-Status: Down(Administrative-Down-By-Propagate-Link-State)


Bridge Group ID: 507
```

請注意2個介面的狀態差異：

<#root>

```
firepower#

 show interface e1/3


Interface Ethernet1/3 "INSIDE", is admin down, line protocol is down
```

```
  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        MAC address ac4a.670e.641e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1

Administrative-Down-By-Propagate-Link-State


        IP address unassigned
  Traffic Statistics for "INSIDE":
        2400 packets input, 165873 bytes
        1822 packets output, 178850 bytes
        17 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  32 bytes/sec
      5 minute output rate 0 pkts/sec,  57 bytes/sec
      5 minute drop rate, 0 pkts/sec
firepower#

show interface e1/4



Interface Ethernet1/4 "OUTSIDE", is down, line protocol is down


  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        MAC address ac4a.670e.640e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1

        Propagate-Link-State-Activated


        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        1893 packets input, 158046 bytes
        2386 packets output, 213997 bytes
        67 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  51 bytes/sec
      5 minute output rate 0 pkts/sec,  39 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

重新啟用switchport後，FTD記錄會顯示：

<#root>

```
May 28 2024 07:38:04: %FTD-4-411001: Line protocol on Interface Ethernet1/4, changed state to up


May 28 2024 07:38:04: %FTD-4-411003: Interface Ethernet1/3, changed state to administratively up


May 28 2024 07:38:04: %FTD-4-411003: Interface INSIDE, changed state to administratively up
May 28 2024 07:38:04: %FTD-4-812006: Link-State-Propagation de-activated on inline-pair due to recovery

May 28 2024 07:38:05: %FTD-4-411002: Line protocol on Interface Ethernet1/4, changed state to down
```

驗證 5. 設定靜態 NAT

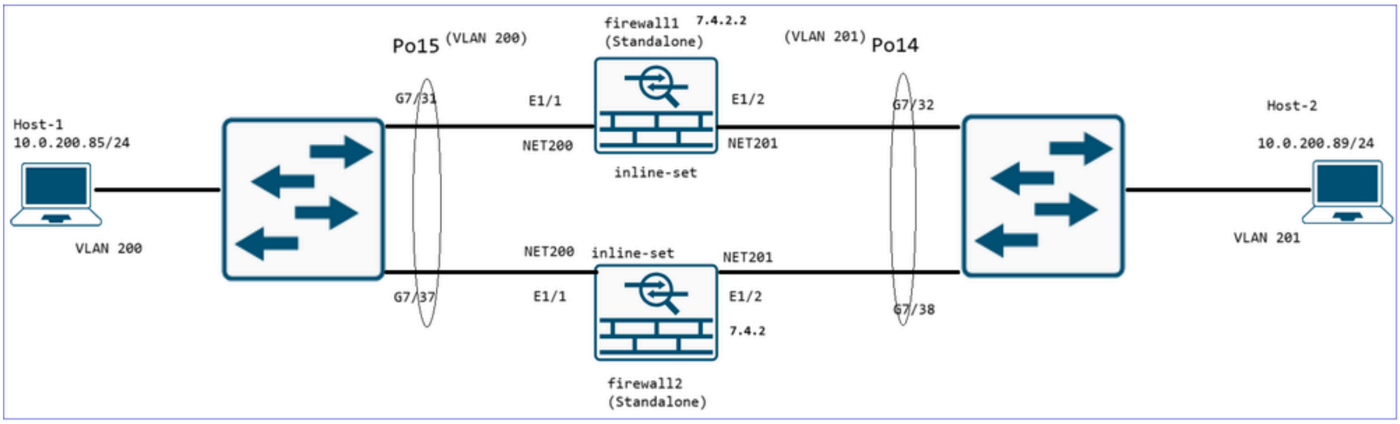
解決方案

以內嵌、內嵌分流器或被動模式執行的介面不支援NAT:

Firepower管理中心配置指南6.0.1版

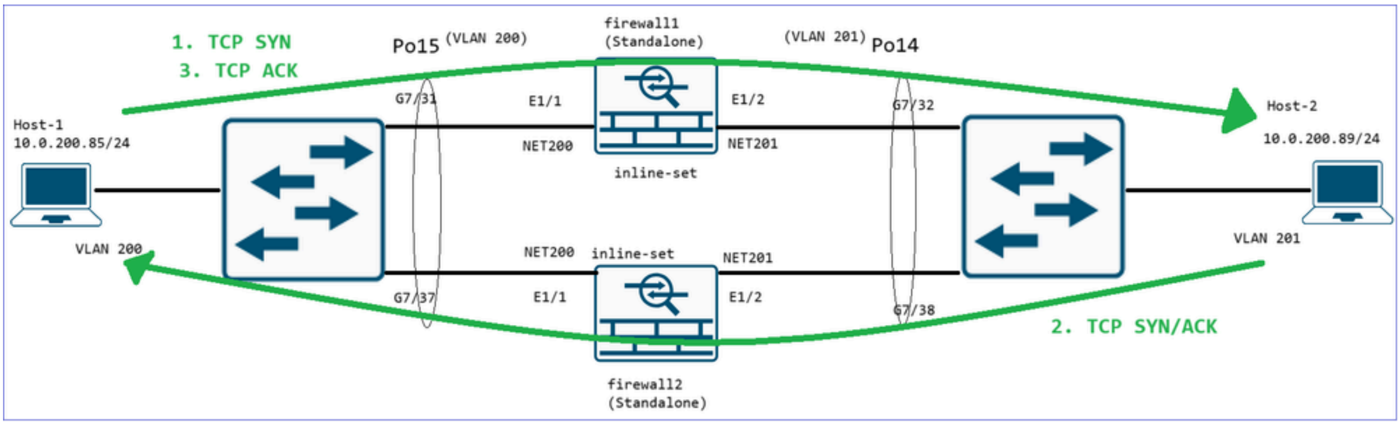
案例研究 — 通過內嵌集的非對稱流量

請考慮以下情況：



兩個防火牆在standalone模式下運行（它們甚至運行不同的軟體版本），但處理來自相同埠通道介面的流量。

在這種情況下，連線埠通道負載平衡演演算法可能會導致非對稱流量：



1. Host-1(10.0.200.85)向Host-2(10.0.200.89)傳送TCP SYN。 此封包會通過firewall1。
2. Host-2(10.0.200.89)向Host-2(10.0.200.85)傳送TCP SYN/ACK。 此封包會通過firewall2。
3. TCP三次握手完成，Host-1向Host-2傳送TCP ACK。此資料包通過firewall1。

從Host-1的角度來看，已成功建立連線：

<#root>

```
root@kali:/ #
```

`wget -O - http://10.0.200.89/10K`

```
--2025-05-06 08:20:28--  http://10.0.200.89/10K
Connecting to 10.0.200.89:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10240 (10K)
Saving to: ‘STDOUT’
-                                         100%[=========================================================
2025-05-06 08:20:28 (99.8 MB/s) - written to stdout [10240/10240]
```

firewall1上的資料包捕獲僅顯示從Host1到Host2的流量：

<#root>

```
firepower#
```

`show capture`

```
capture CAPI type raw-data trace interface NET200 [Capturing - 875 bytes]
  match ip host 10.0.200.85 host 10.0.200.89
capture CAPO type raw-data trace interface NET201 [Capturing - 875 bytes]
  match ip host 10.0.200.85 host 10.0.200.89
```

捕獲內容：

<#root>

```
firepower#
```

`show capture CAPI`

```
9 packets captured

   1: 12:21:14.161689       10.0.200.85.44806 > 10.0.200.89.80:
```

`S`

```
1877376557:1877376557(0) win 64240 <mss 1460,sackOK,timestamp 2133104674 0,nop,wscale 7>
   2: 12:21:14.162924       10.0.200.85.44806 > 10.0.200.89.80: .

ack

 3274105192 win 502 <nop,nop,timestamp 2133104676 1658009126>
   3: 12:21:14.163077       10.0.200.85.44806 > 10.0.200.89.80: P 1877376558:1877376687(129) ack 327410
   4: 12:21:14.164801       10.0.200.85.44806 > 10.0.200.89.80: . ack 3274106640 win 501 <nop,nop,times
   5: 12:21:14.164908       10.0.200.85.44806 > 10.0.200.89.80: . ack 3274108088 win 494
...
```

firewall2上的資料包捕獲僅顯示從Host2到Host1的流量：

<#root>

```
FTD1010-12#

show capture CAPI



11 packets captured

   1: 12:21:14.198949       10.0.200.89.80 > 10.0.200.85.44806:

S

 3274105191:3274105191(0)

ack

 1877376558 win 65160 <mss 1460,sackOK,timestamp 1658009126 2133104674,nop,wscale 7>
   2: 12:21:14.200001       10.0.200.89.80 > 10.0.200.85.44806: . ack 1877376687 win 509 <nop,nop,times
   3: 12:21:14.200825       10.0.200.89.80 > 10.0.200.85.44806: . 3274105192:3274106640(1448) ack 18773
   4: 12:21:14.200947       10.0.200.89.80 > 10.0.200.85.44806: . 3274106640:3274108088(1448) ack 18773
   5: 12:21:14.200963       10.0.200.89.80 > 10.0.200.85.44806: . 3274108088:3274109536(1448) ack 18773
   6: 12:21:14.200978       10.0.200.89.80 > 10.0.200.85.44806: . 3274109536:3274110984(1448) ack 18773
   7: 12:21:14.200993       10.0.200.89.80 > 10.0.200.85.44806: P 3274110984:3274112432(1448) ack
...
```

firewall1上的系統日誌顯示TCP SYN資料包建立了TCP狀態旁路連線：

<#root>

```
firepower#

show logging


...
May 06 2025 12:21:14: %FTD-6-302303:

Built TCP state-bypass connection
```

```
 106977 from NET200:10.0.200.85/44806 (10.0.200.85/44806) to NET201:10.0.200.89/80 (10.0.200.89/80)
```

在firewall2上，TCP SYN/ACK資料包還建立了TCP狀態旁路連線：

<#root>

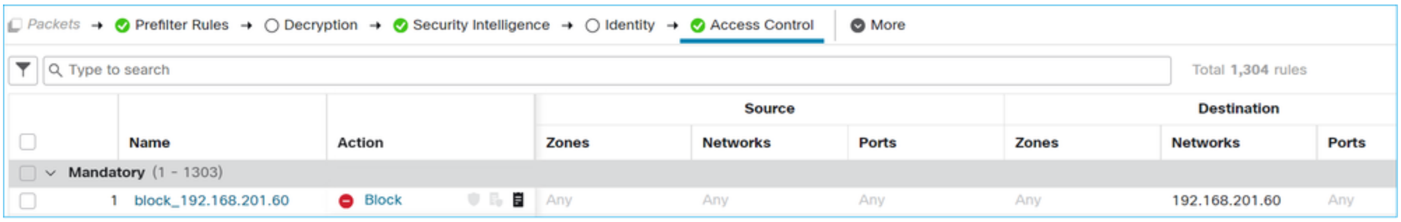
```
FTD1010-12#

show logging

...
May 06 2025 12:21:14: %FTD-6-302303:

Built TCP state-bypass


connection

 325 from NET201:10.0.200.89/80 (10.0.200.89/80) to NET200:10.0.200.85/44806 (10.0.200.85/44806)
```

主要重點

- 非對稱流量通過不同防火牆裝置的內嵌集工作，因為兩台裝置都在TCP狀態略過模式下處理TCP連線。
- 請注意，TCP狀態略過並非在防火牆上手動設定，而是內嵌集介面作業的結果。

在內嵌配對介面模式下封鎖封包

建立封鎖規則，透過FTD內嵌配對傳送流量，並觀察行為，如下圖所示。



Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control
More
Type to search
Total 1,304 rules

			Source			Destination		
□	Name	Action	Zones	Networks	Ports	Zones	Networks	Ports
□	Mandatory (1 - 1303)							
□ 1	block_192.168.201.60	Block	Any	Any	Any	Any	192.168.201.60	Any

解決方案

啟用含有追蹤軌跡的擷取，並透過 FTD 內嵌配對傳送 SYN/ACK 封包。流量遭封鎖：

<#root>

```
firepower#
```

```
show capture


capture CAPI type raw-data trace interface INSIDE

[Capturing - 270 bytes]


  match ip host 192.168.201.60 any
capture CAPO type raw-data interface OUTSIDE

[Capturing - 0 bytes]


  match ip host 192.168.201.60 any
```

在追蹤軌跡中，可以看到該封包已被FTD LINA引擎捨棄，而且沒有轉送至FTD Snort引擎。

<#root>

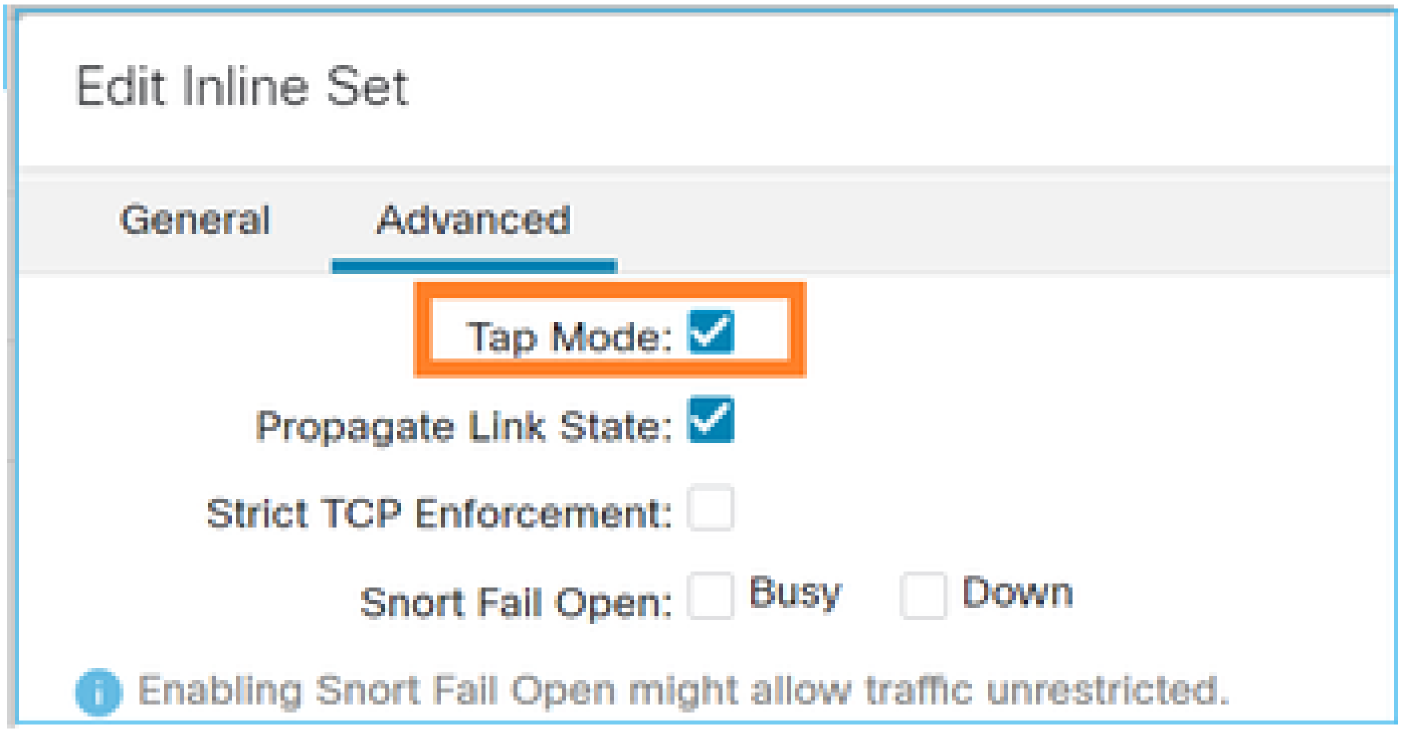
```
firepower#

show capture CAPI packet-number 1 trace



4 packets captured

   1: 09:41:54.562547       192.168.201.50.59144 > 192.168.201.60.80: S 3817586151:3817586151(0) win 64
Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Elapsed time: 10126 ns
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Elapsed time: 10126 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip any host 192.168.201.60 rule-id 268451045 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268451045: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451045: L4 RULE: block_192.168.201.60
Additional Information:

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: drop

Time Taken: 20252 ns

1 packet shown
```

設定使用分流器的內嵌配對模式

對內嵌配對啟用分流器模式。

解決方案

導覽至Devices > Device Management > Inline Sets > Edit Inline Set > Advanced，然後啟用Tap Mode，如下圖所示。



Edit Inline Set

Tap Mode: ☑

Propagate Link State: ☑

Strict TCP Enforcement: □

Snort Fail Open: □ Busy □ Down

Enabling Snort Fail Open might allow traffic unrestricted.

驗證

<#root>

```
firepower#
 show inline-set


Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Fail-open for snort down is off
  Fail-open for snort busy is off


Tap mode is on
```

```
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"
      Current-Status: UP
    Interface: Ethernet1/3 "INSIDE"
      Current-Status: UP

   Bridge Group ID: 0
```

驗證使用分流器的 FTD 內嵌配對介面作業

基本原理

- 設定使用分流器的內嵌配對時，實體介面會在內部橋接。
- 在路由或透明部署模式下可使用.
- 大多數LINA引擎功能（NAT、路由等）不可用於穿越內嵌配對的資料流。
- 無法捨棄實際流量.
- 有幾個 LINA 引擎檢查會隨完整 Snort 引擎檢查一起對實際流量的副本套用.

使用分流器模式的內嵌配對不會捨棄傳輸流量。透過封包的追蹤軌跡，可確認這點：

```
<#root>

>

show capture CAPI packet-number 2 trace


3 packets captured

   2: 13:34:30.685084       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win 8192
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: NGIPS-MODE
Subtype: ngips-mode
```

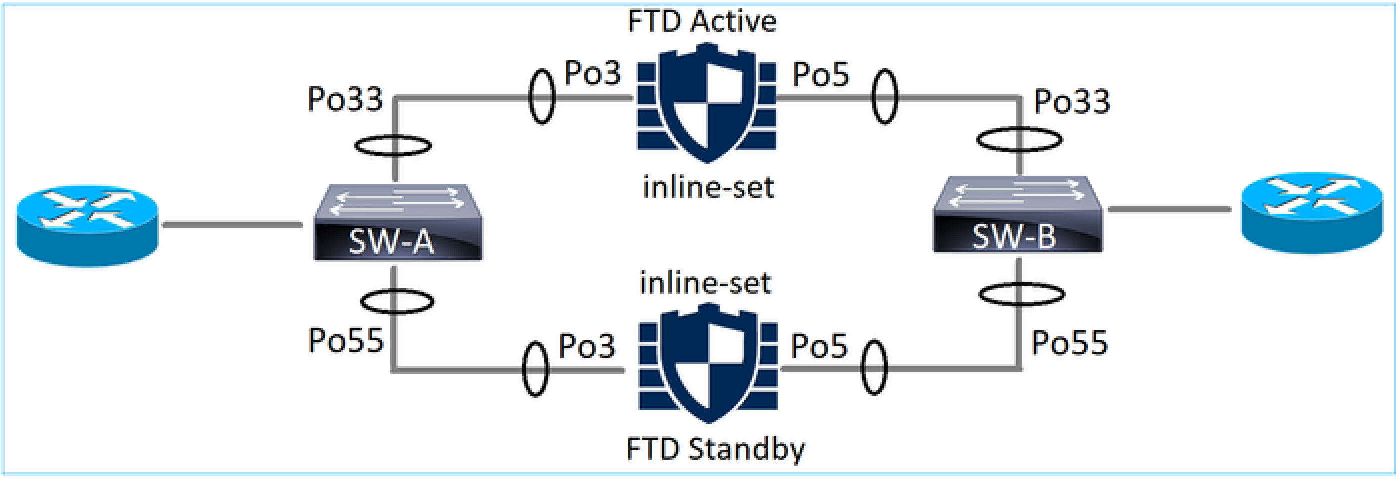
```
Result: ALLOW
Config:
Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied



Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: WOULD HAVE DROPPED

Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log fl
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Rule 1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up

Action: Access-list would have dropped, but packet forwarded due to inline-tap


1 packet shown
>
```

內嵌配對和 EtherChannel

您可以透過兩種方式透過 EtherChannel 設定內嵌配對：

1. 在 FTD 上終止的 EtherChannel.
2. Etherchannel會通過FTD（需要FXOS 2.3.1.3及更新版本）。

在 FTD 上終止的 EtherChannel



SW-A 上的 EtherChannel：

<#root>

```
SW-A#
```

```
show etherchannel summary | i Po33|Po55
```

```
33      Po33(SU)        LACP      Gi3/11(P)
35      Po55(SU)        LACP      Gi2/33(P)
```

SW-B 上的 EtherChannel：

<#root>

```
SW-B#
```

```
show etherchannel summary | i Po33|Po55
```

```
33      Po33(SU)        LACP        Gi1/0/3(P)
55      Po55(SU)        LACP        Gi1/0/4(P)
```

流量會根據得知的MAC位址，透過作用中FTD轉送：

<#root>

```
SW-B#
```

```
 show mac address-table address 0017.dfd6.ec00
```

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC
```

```
Po33
```

```
Total Mac Addresses for this criterion: 1
```

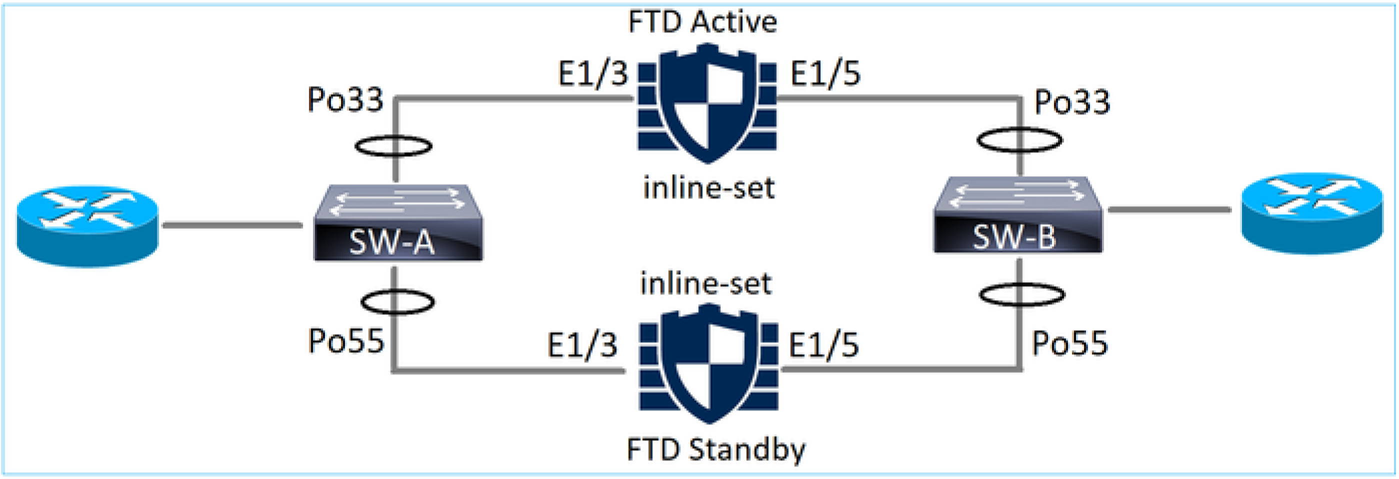
FTD 上的內嵌集：

<#root>

```
FTD#

show inline-set


Inline-set SET1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled


Interface-Pair[1]:
    Interface: Port-channel3 "INSIDE"
      Current-Status: UP
    Interface: Port-channel5 "OUTSIDE"
      Current-Status: UP

    Bridge Group ID: 775
```

附註：在發生FTD容錯移轉事件的情況下，流量中斷時間主要取決於交換器得知遠端對等點的MAC位址所花費的時間。

通過 FTD 的 EtherChannel



SW-A 上的 EtherChannel：

<#root>

```
SW-A#

show etherchannel summary | i Po33|Po55


33      Po33(SU)        LACP      Gi3/11(P)
55      Po55(SD)        LACP      Gi3/7

(I)
```

通過待命FTD的LACP封包遭封鎖：

<#root>

```
FTD#

capture ASP type asp-drop fo-standby

FTD#

show capture ASP | i 0180.c200.0002

  29: 15:28:32.658123       a0f8.4991.ba03 0180.c200.0002 0x8809 Length: 124
  70: 15:28:47.248262       f0f7.556a.11e2 0180.c200.0002 0x8809 Length: 124
```

SW-B 上的 EtherChannel：

<#root>

```
SW-B#

show etherchannel summary | i Po33|Po55


33      Po33(SU)        LACP        Gi1/0/3(P)
55      Po55(SD)        LACP        Gi1/0/4

(s)
```

流量會根據得知的MAC位址，透過作用中FTD轉送：

<#root>

```
SW-B#

 show mac address-table address 0017.dfd6.ec00

          Mac Address Table
-------------------------------------------


Vlan    Mac Address       Type        Ports
```

```
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC

Po33

Total Mac Addresses for this criterion: 1
```

FTD 上的內嵌集：

```
<#root>

FTD#

show inline-set



Inline-set SET1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled

Interface-Pair[1]:


    Interface: Ethernet1/3 "INSIDE"


      Current-Status: UP


    Interface: Ethernet1/5 "OUTSIDE"


      Current-Status: UP


    Bridge Group ID: 519
```

> ⚠ 注意：在此情況中，在發生FTD容錯移轉事件的情況下，收斂時間主要取決於EtherChannel LACP交涉，以及中斷所需的時間（可能會非常長）。如果已開啟EtherChannel模式（無LACP），則收斂時間取決於得知MAC位址的時間。

疑難排解

目前尚無適用於此組態的具體資訊。

比較：內嵌配對與使用分流器的內嵌配對

	內嵌配對	使用分流器的內嵌配對
show inline-set	> show inline-set Inline-set Inline-Pair-1 Mtu is 1500 bytes Failsafe mode is on/activated Failsecure mode is off Tap mode is off Propagate-link-state option is on hardware-bypass mode is disabled Interface-Pair[1]: Interface:Ethernet1/6 "INSIDE" Current-Status:UP Interface:Ethernet1/8 "OUTSIDE" Current-Status:UP Bridge Group ID:509 >	> show inline-set Inline-set Inline-Pair-1 Mtu is 1500 bytes Failsafe mode is on/activated Failsecure mode is off Tap mode is on Propagate-link-state option is on hardware-bypass mode is disabled Interface-Pair[1]: Interface:Ethernet1/6 "INSIDE" Current-Status:UP Interface:Ethernet1/8 "OUTSIDE" Current-Status:UP Bridge Group ID:0 >
顯示介面	> show interface e1/6 Interface Ethernet1/6 "INSIDE", is up, line protocol is up Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec MAC address 5897.bdb9.770e, MTU 1500 IPS Interface-Mode:inline, Inline-Set:Inline-Pair-1 IP address unassigned Traffic Statistics for "INSIDE": 3957 packets input, 264913 bytes 144 packets output, 58664 bytes 4 packets dropped 1 minute input rate 0 pkts/sec, 26 bytes/sec 1 minute output rate 0 pkts/sec, 7 bytes/sec 1 minute drop rate, 0 pkts/sec 5 minute input rate 0 pkts/sec, 28 bytes/sec	> show interface e1/6 Interface Ethernet1/6 "INSIDE", is up, line protocol is up Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec MAC address 5897.bdb9.770e, MTU 1500 IPS Interface-Mode:inline-tap, Inline-Set:Inline-Pair-1 IP address unassigned Traffic Statistics for "INSIDE": 24 packets input, 1378 bytes 0 packets output, 0 bytes 24 packets dropped 1 minute input rate 0 pkts/sec, 0 bytes/sec 1 minute output rate 0 pkts/sec, 0 bytes/sec 1 minute drop rate, 0 pkts/sec 5 minute input rate 0 pkts/sec, 0 bytes/sec

	5 minute output rate 0 pkts/sec, 9 bytes/sec 5 minute drop rate, 0 pkts/sec > show interface e1/8 Interface Ethernet1/8 "OUTSIDE", is up, line protocol is up Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec MAC address 5897.bdb9.774d, MTU 1500 IPS Interface-Mode:inline, Inline-Set:Inline-Pair-1 IP address unassigned Traffic Statistics for "OUTSIDE": 144 packets input, 55634 bytes 3954 packets output, 339987 bytes 0 packets dropped 1 minute input rate 0 pkts/sec, 7 bytes/sec 1 minute output rate 0 pkts/sec, 37 bytes/sec 1 minute drop rate, 0 pkts/sec 5 minute input rate 0 pkts/sec, 8 bytes/sec 5 minute output rate 0 pkts/sec, 39 bytes/sec 5 minute drop rate, 0 pkts/sec >	5 minute output rate 0 pkts/sec, 0 bytes/sec 5 minute drop rate, 0 pkts/sec > show interface e1/8 Interface Ethernet1/8 "OUTSIDE", is up, line protocol is up Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec MAC address 5897.bdb9.774d, MTU 1500 IPS Interface-Mode:inline-tap, Inline-Set:Inline-Pair-1 IP address unassigned Traffic Statistics for "OUTSIDE": 1 packets input, 441 bytes 0 packets output, 0 bytes 1 packets dropped 1 minute input rate 0 pkts/sec, 0 bytes/sec 1 minute output rate 0 pkts/sec, 0 bytes/sec 1 minute drop rate, 0 pkts/sec 5 minute input rate 0 pkts/sec, 0 bytes/sec 5 minute output rate 0 pkts/sec, 0 bytes/sec 5 minute drop rate, 0 pkts/sec >
使用封鎖規則處理封包	> show capture CAPI packet-number 1 trace 3 packets captured 1:16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80:S 0:0(0) ack 0 win 8192 Phase:1 Type:CAPTURE Subtype: Result:ALLOW Config: Additional Information: MAC Access list	> show capture CAPI packet-number 1 trace 3 packets captured 1:16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80:S 0:0(0) win 8192 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:NGIPS-MODE Subtype:ngips-mode Result:ALLOW Config: Additional Information: The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied Phase:4 Type:ACCESS-LIST Subtype:log Result:DROP Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-start access-list CSM_FW_ACL_ remark rule-id 268441600:ACCESS POLICY:FTD4100 - Mandatory/1 access-list CSM_FW_ACL_ remark rule-id 268441600:L4 RULE:Rule 1 Additional Information: Result: input-interface:INSIDE input-status:up input-line-status:up Action:drop Drop-reason:(acl-drop) Flow is denied by configured rule 1 packet shown >	Phase:2 Type:ACCESS-LIST Subtype: Result:ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase:3 Type:NGIPS-MODE Subtype:ngips-mode Result:ALLOW Config: Additional Information: The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied Phase:4 Type:ACCESS-LIST Subtype:log Result:WOULD HAVE DROPPED Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-start access-list CSM_FW_ACL_ remark rule-id 268441600:ACCESS POLICY:FTD4100 - Mandatory/1 access-list CSM_FW_ACL_ remark rule-id 268441600:L4 RULE:Rule 1 Additional Information: Result: input-interface:INSIDE input-status:up input-line-status:up Action:Access-list would have dropped,but packet forwarded due to inline-tap 1 packet shown >

摘要

- 使用內嵌配對模式時，封包主要會通過 FTD Snort 引擎.
- 在 TCP 狀態略過模式下會處理 TCP 連線.
- 從 FTD LINA 引擎的角度來看，ACL 原則已套用.
- 使用內嵌配對模式時，封包可能會被封鎖，因為系統是以內嵌方式處理封包.
- 啟用分流器模式後，實際流量在未修改的情況下通過 FTD 時，系統會於內部檢查封包的副本並將其捨棄.

相關資訊

- 思科 Firepower 新世代防火牆(NGFW)
- 技術支援與文件 - Cisco Systems