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 4150 FTD（6.1.0.x 和 6.3.x 版）
- Firepower 管理中心 (FMC)（6.1.0.x 和 6.3.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：

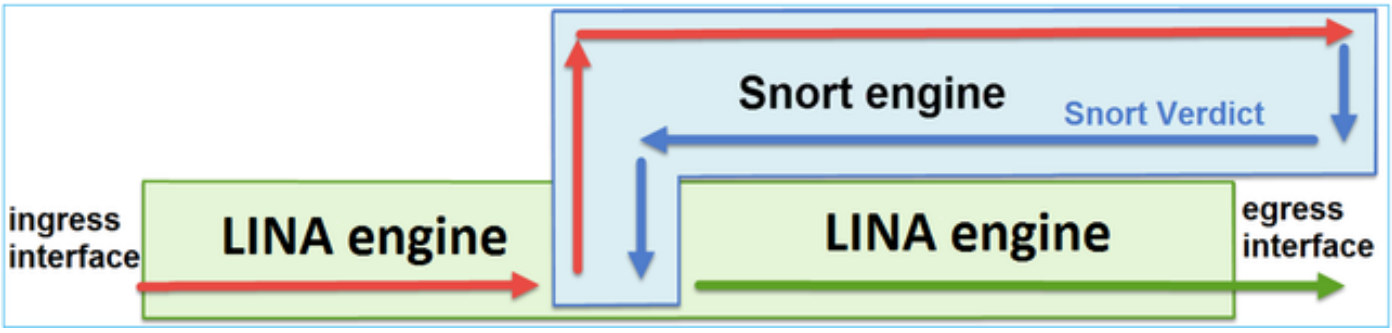
- ASA5506-X、ASA5506W-X、ASA5506H-X、ASA5508-X、ASA5516-X
- ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X
- FPR2100、FPR4100、FPR9300
- VMware (ESXi)、Amazon Web Services (AWS)、核心式虛擬機器 (KVM)
- FTD 軟體 6.2.x 及更新版本

背景資訊

FTD 是一個整合的軟體映像，其中包括 2 個主引擎：

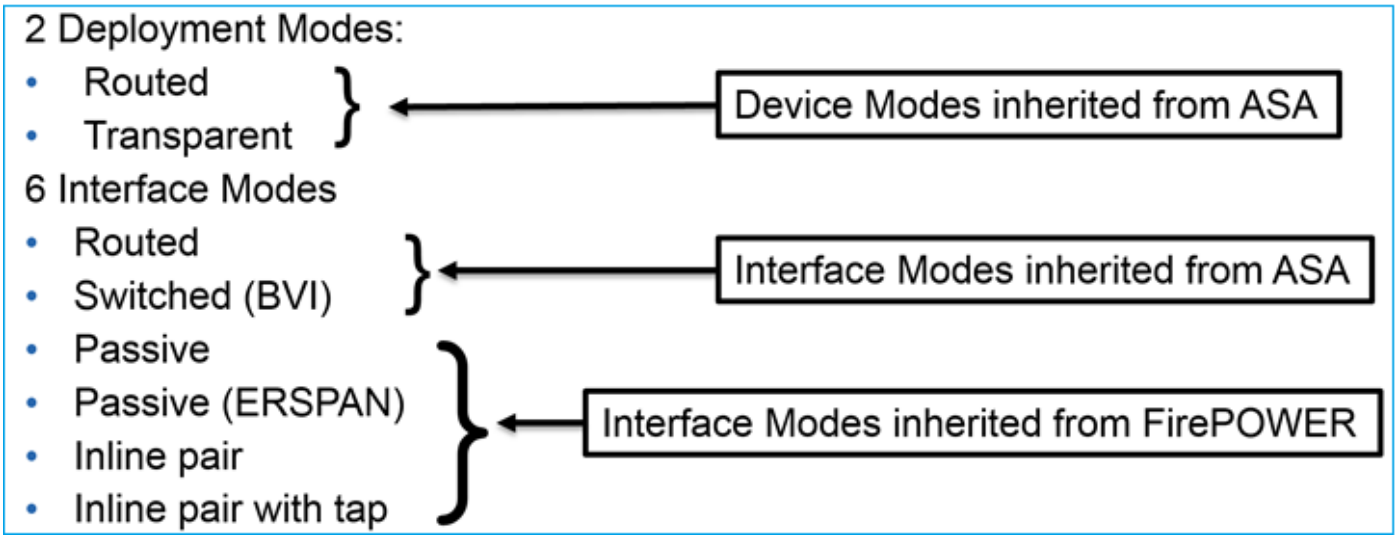
- LINA 引擎
- Snort 引擎

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
- 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：



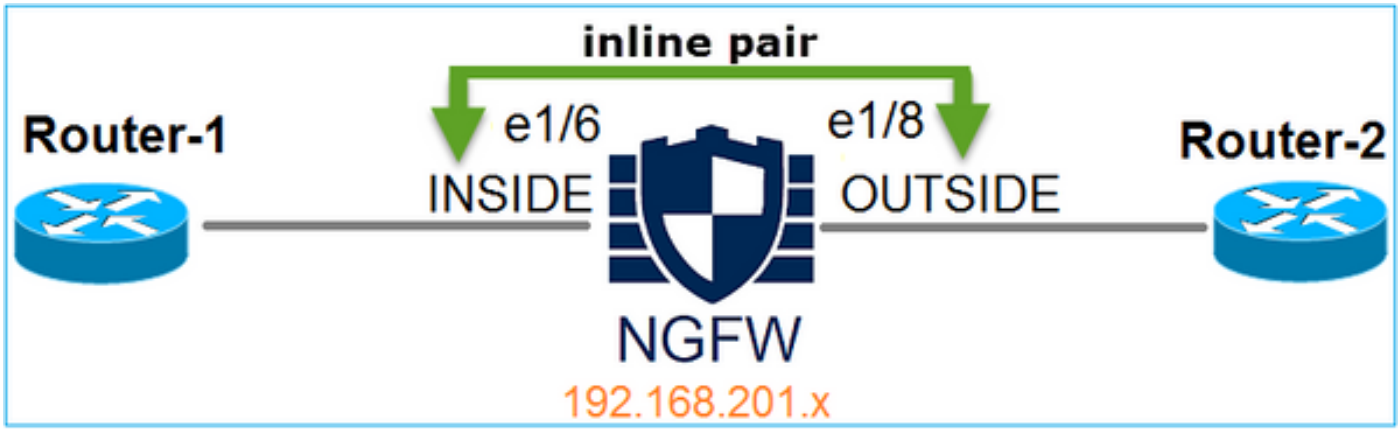
附註：您可以在單一FTD裝置上混合使用介面模式。

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



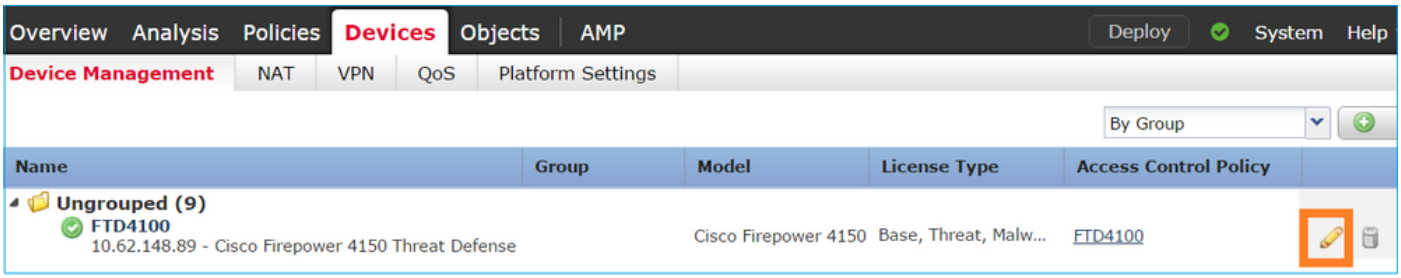
需求

根據以下要求，在內嵌配對模式下設定實體介面 e1/6 和 e1/8：

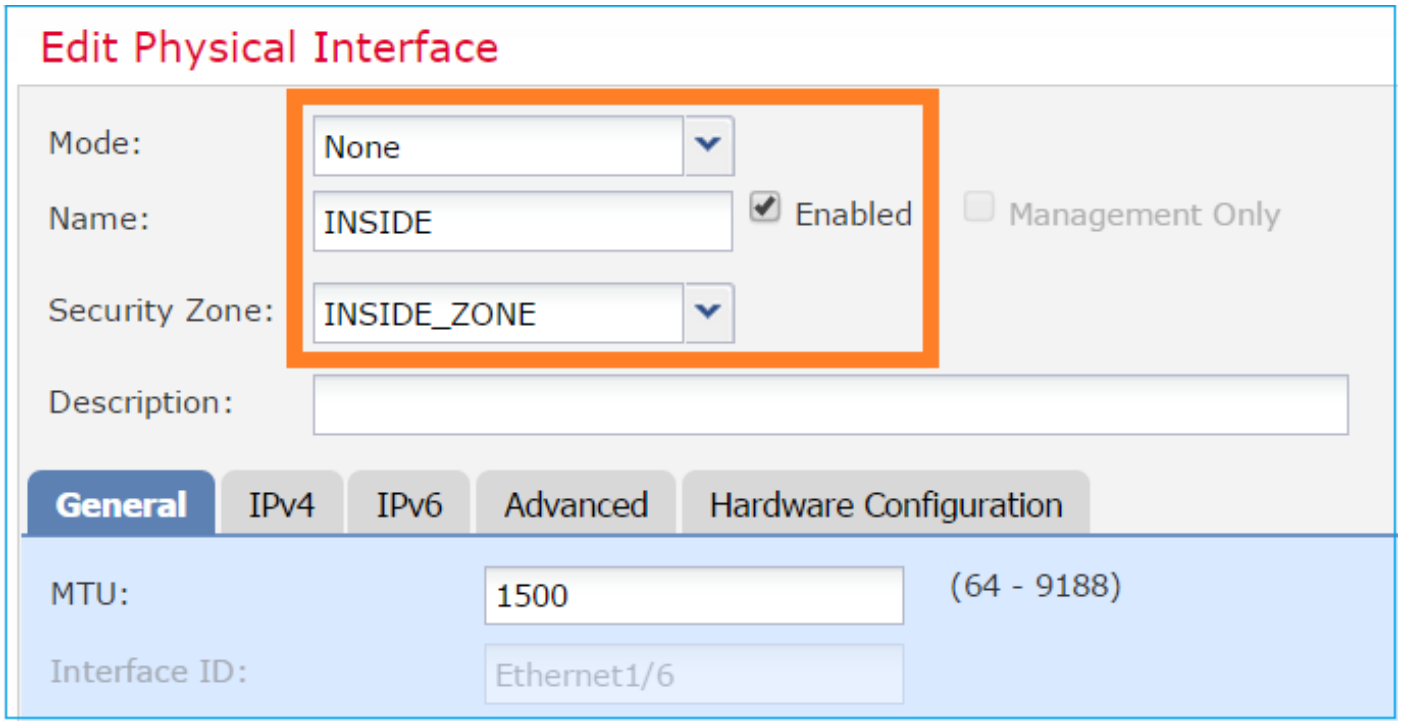
介面	e1/6	e1/8
名稱	INSIDE	OUTSIDE
安全區域	INSIDE_ZONE	OUTSIDE_ZONE
內嵌集名稱	Inline-Pair-1	
內嵌集 MTU	1500	
防故障	已啟用	
傳播連結狀態	已啟用	

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，如下圖所示。

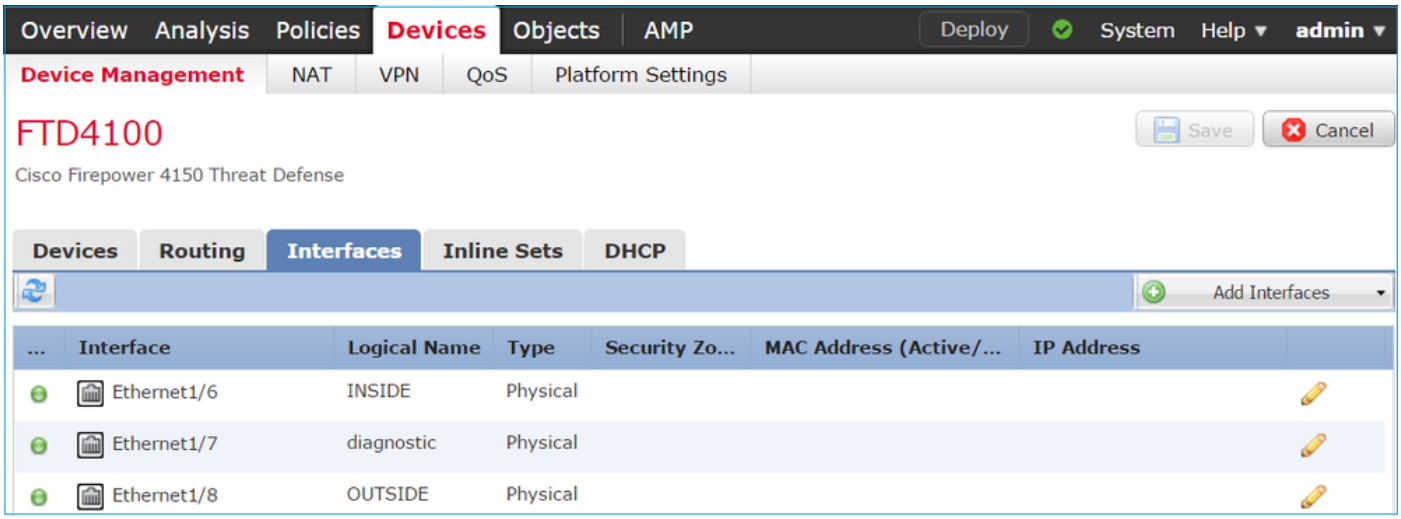


接下來，指定介面的名稱並勾選 Enabled，如下圖所示。



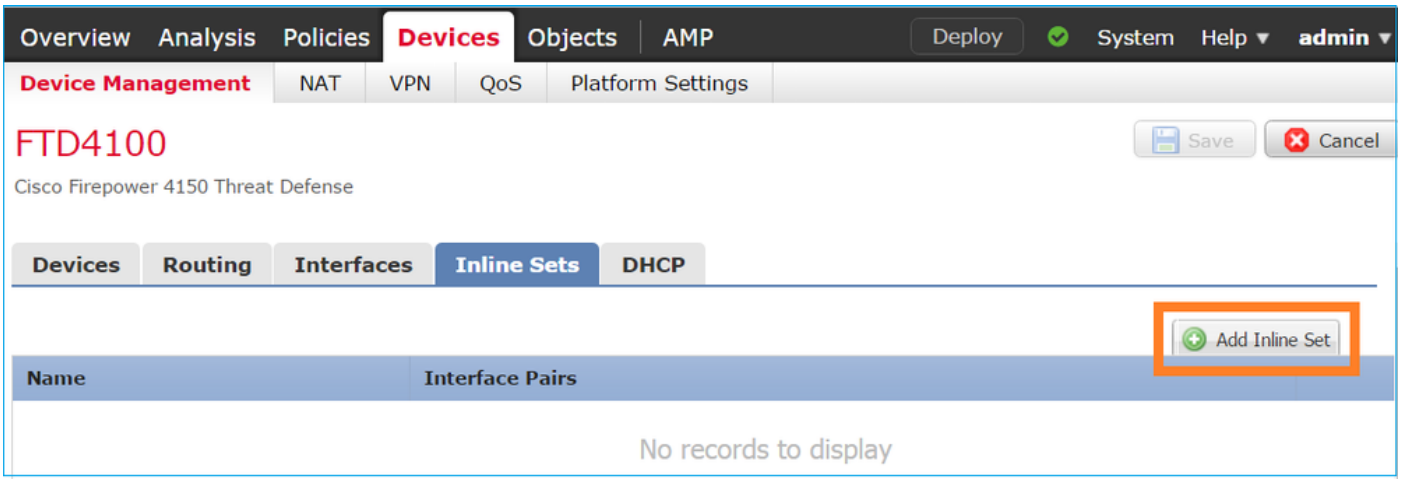
註：名稱是介面的nameif。

類似介面 Ethernet1/8。最終結果如下圖所示。

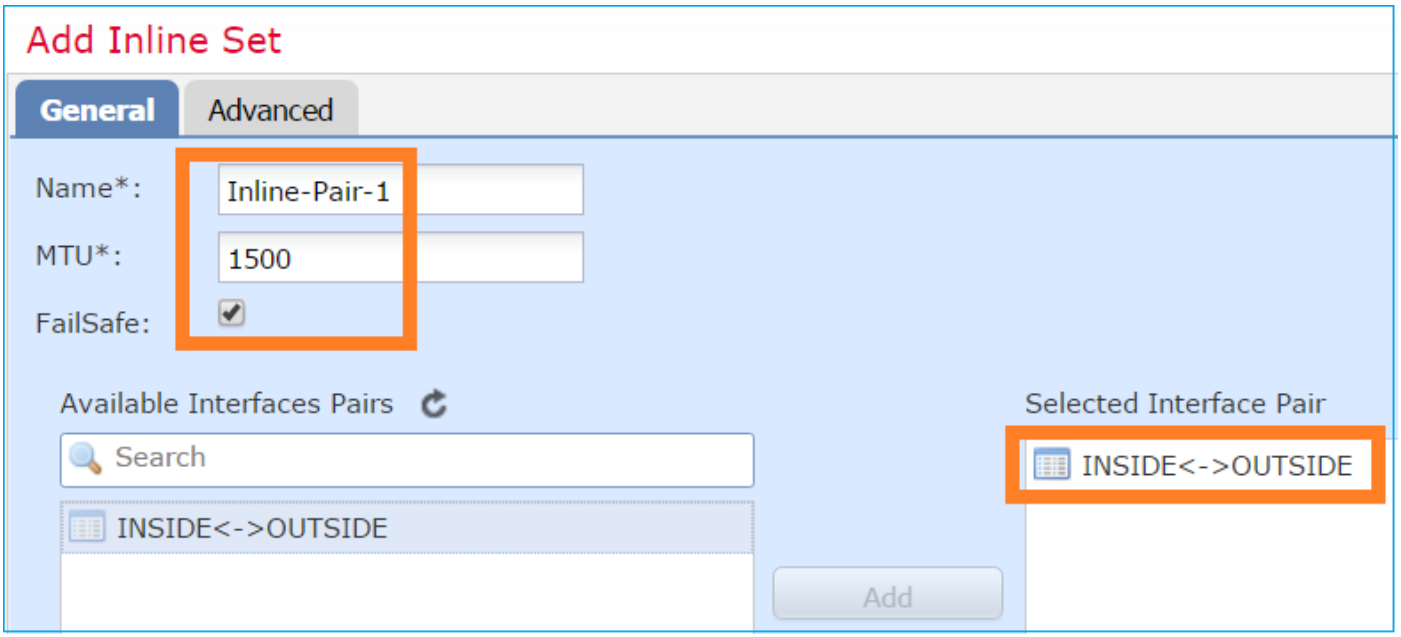


步驟 2.設定內嵌配對。

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

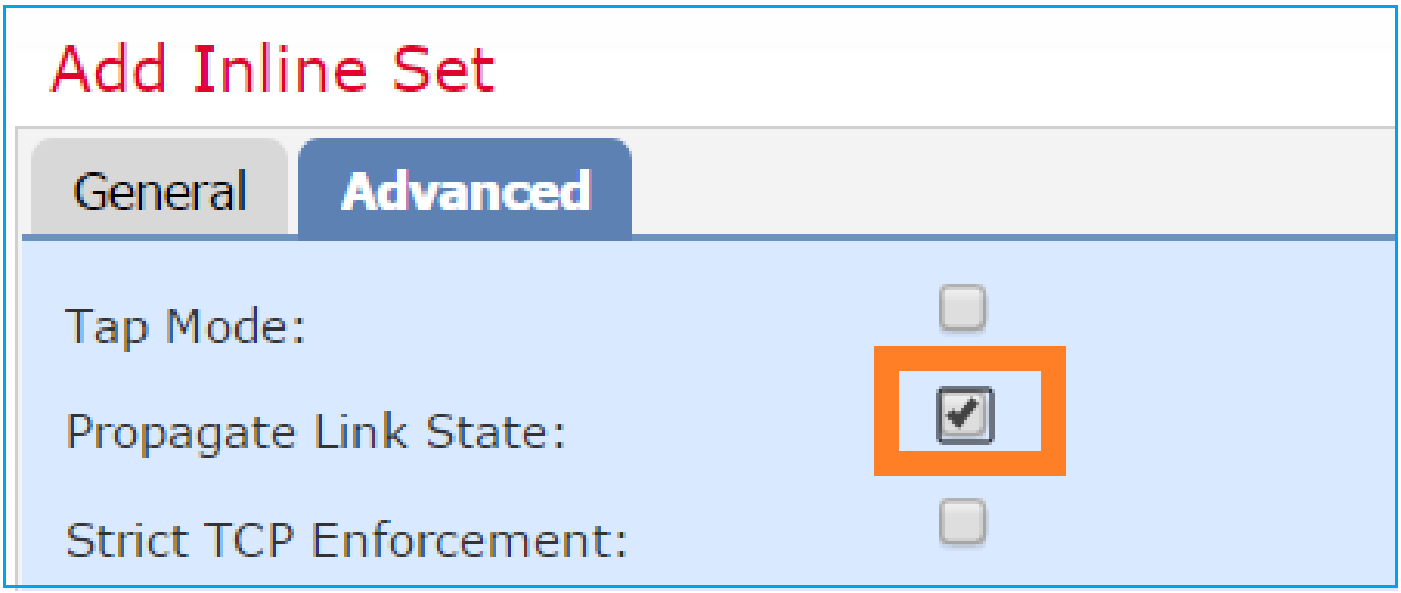


步驟 3.根據要求配置「General」設定，如下圖所示。



注意：防故障功能允許流量未經檢查就通過內嵌配對，以防介面緩衝區滿載（通常發生在裝置超載或Snort引擎超載時）。介面緩衝區大小以動態方式分配。

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



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：

```
> 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
>
```

註：網橋組ID是一個不同於0的值。如果分流器模式為開啟狀態則為 0

介面和名稱資訊：

```
<#root>

>

show nameif

Interface                  Name                       Security
Ethernet1/6                INSIDE                       0

Ethernet1/7                diagnostic                   0
Ethernet1/8                OUTSIDE                      0

>
```

驗證介面狀態：

```
<#root>

> show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
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

Ethernet1/6                unassigned      YES unset  up                    up
Ethernet1/7                unassigned      YES unset  up                    up
Ethernet1/8                unassigned      YES unset  up                    up
```

驗證實體介面資訊：

```
<#root>

>

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":
        468 packets input, 47627 bytes
        12 packets output, 4750 bytes
        1 packets dropped
      1 minute input rate 0 pkts/sec,  200 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,  96 bytes/sec
      5 minute output rate 0 pkts/sec,  8 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":
        12 packets input, 4486 bytes
        470 packets output, 54089 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  7 bytes/sec
      1 minute output rate 0 pkts/sec,  212 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  7 bytes/sec
      5 minute output rate 0 pkts/sec,  106 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：

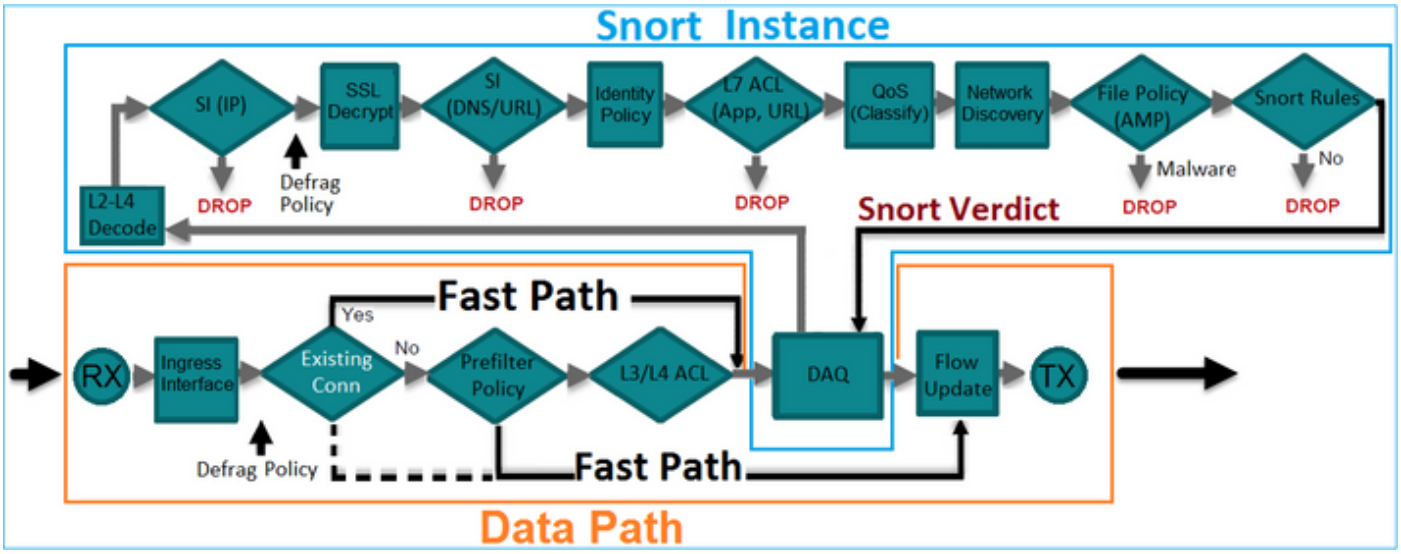
- 驗證 1.使用 Packet Tracer
- 驗證 2.啟用含有追蹤軌跡的擷取，並透過內嵌配對傳送TCP同步/確認(SYN/ACK)封包

- 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，封包的處理方式如下圖所示。

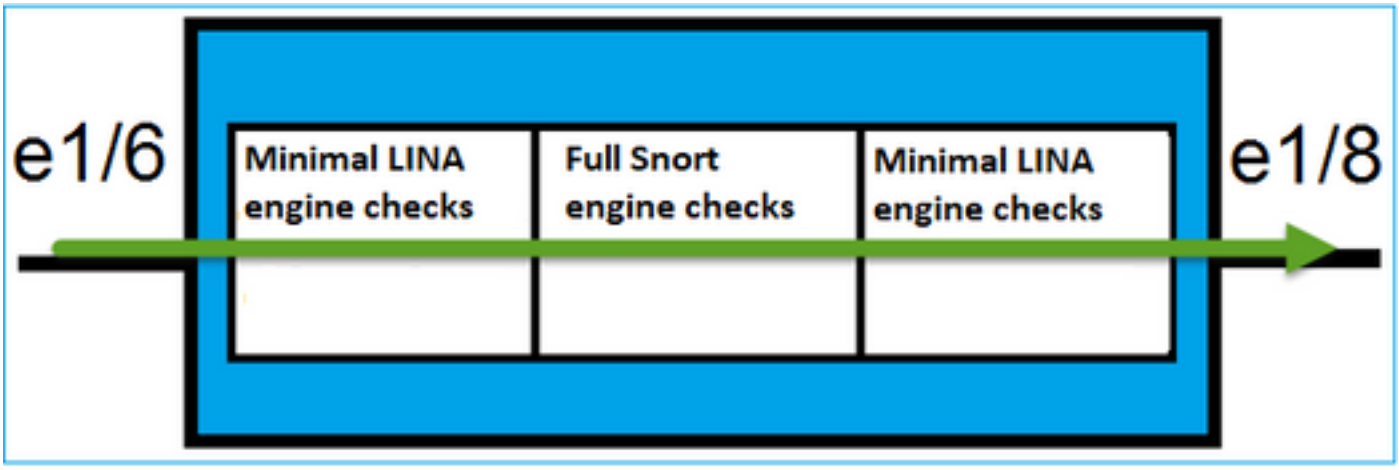


注意：只有實體介面可以是內嵌配對集的成員

基本原理

- 設定一個內嵌配對時，2 個實體介面會在內部橋接
- 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>

>

packet-tracer input INSIDE tcp 192.168.201.50 1111 192.168.202.50 80

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2

Type: NGIPS-MODE

Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:

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

Phase: 3

Type: ACCESS-LIST

Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet is sent to snort for additional processing where a verdict is reached

Phase: 4

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: 5

Type: FLOW-CREATION

Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 106, packet dispatched to next module

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

>

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>

>

capture CAPI interface INSIDE trace match ip host 192.168.201.60 any


>

capture CAPO interface OUTSIDE match ip host 192.168.201.60 any


>
```

透過 FTD 傳送封包後，可以看到已建立的連線：

```
<#root>

>

show conn detail


1 in use, 34 most used
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,


 b - TCP state-bypass or nailed,


       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media,

N - inspected by Snort

, n - GUP
       O - responder data, P - inside back connection,
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow


TCP Inline-Pair-1:OUTSIDE(OUTSIDE): 192.168.201.60/80 Inline-Pair-1:INSIDE(INSIDE): 192.168.201.50/20,



flags b N

, idle 13s, uptime 13s, timeout 1h0m, bytes 0

>
```

注意:b標誌 — 傳統ASA將丟棄未經請求的SYN/ACK資料包，除非啟用了TCP狀態旁路。在內嵌配對模式下，FTD介面會處理處於TCP狀態略過模式的TCP連線，而且不會捨棄不屬於已存在連線的TCP封包。

附註：N旗標 — FTD Snort引擎會檢查封包。

擷取可證明此情況，因為您可以看到有 3 個封包在 FTD 中周遊：

```
<#root>

>

show capture CAPI



3 packets captured



   1: 15:27:54.327146       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
   2: 15:27:54.330000       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
   3: 15:27:54.332517       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
3 packets shown
>
```

3 個封包退出 FTD 裝置：

```
<#root>

>

show capture CAPO



3 packets captured



   1: 15:27:54.327299       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack
```

```
 0 win 8192
   2: 15:27:54.330030       192.168.201.50.20 > 192.168.201.60.80:
S
 0:0(0)
ack
 0 win 8192
   3: 15:27:54.332548       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>
>
show capture CAPI packet-number 1 trace

3 packets captured
   1: 15:27:54.327146       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

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: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE

Additional Information:
This packet is sent to snort for additional processing where a verdict is reached

Phase: 5
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: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 282, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT

Subtype:
Result: ALLOW
Config:
Additional Information:

Application: 'SNORT Inspect'

Phase: 8
Type: SNORT

Subtype:

Result: ALLOW

Config:

Additional Information:
Snort Verdict: (pass-packet) allow this packet

```
Phase: 9
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

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


1 packet shown
>
```

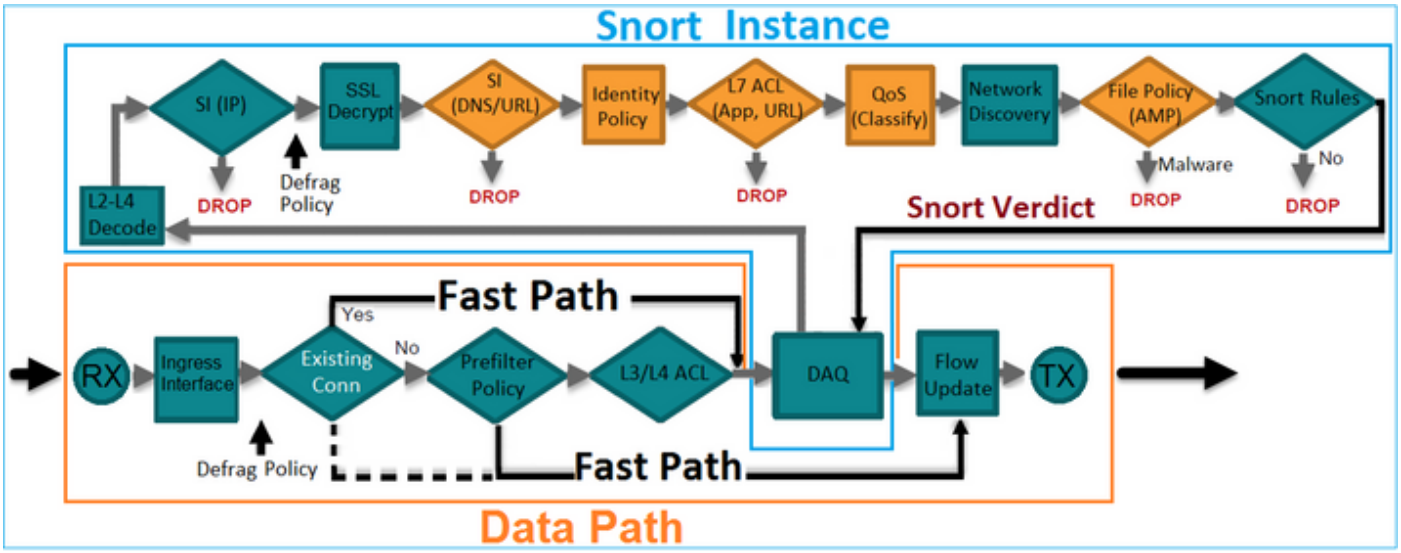
第二個擷取封包的追蹤軌跡顯示封包與當前連線相符，因此會繞過ACL檢查，但Snort引擎仍會對其進行檢查：

```
<#root>

>

show capture CAPI packet-number 2 trace


3 packets captured

   2: 15:27:54.330000       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

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
```

```
Phase: 3
Type: FLOW-LOOKUP
Subtype:ing
Result: ALLOW
Config:
Additional Information:
Found flow with id 282, using current flow


Phase: 4
Type: EXTERNAL-INSPECT

Subtype:
Result: ALLOW
Config:

Additional Information:
Application: 'SNORT Inspect'


Phase: 5
Type: SNORT

Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet


Phase: 6
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

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


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e1/6介面的switchport。在 FTD CLI 上，您必須看到兩個介面都已關閉：

```
<#root>

>

show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
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

Ethernet1/6                unassigned      YES unset  down                  down

Ethernet1/7                unassigned      YES unset  up                    up

Ethernet1/8                unassigned      YES unset  administratively down up

>
```

FTD 記錄顯示：

```
<#root>

>

show log

Jan 03 2017 15:53:19: %ASA-4-411002:

Line protocol on Interface Ethernet1/6, changed state to down

Jan 03 2017 15:53:19: %ASA-4-411004:

Interface OUTSIDE, changed state to administratively down

Jan 03 2017 15:53:19: %ASA-4-411004:

Interface Ethernet1/8, changed state to administratively down

Jan 03 2017 15:53:19: %ASA-4-812005:

Link-State-Propagation activated on inline-pair due to failure of interface Ethernet1/6(INSIDE) bringing

>
```

內嵌集狀態顯示 2 個介面成員的狀態：

```
<#root>

>

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: Down(Propagate-Link-State-Activated)


    Interface: Ethernet1/8 "OUTSIDE"


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

    Bridge Group ID: 509
>
```

請注意 2 個介面的狀態差異：

```
<#root>

>

show interface e1/6



Interface Ethernet1/6 "INSIDE", is down, line protocol is down


  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
```

```
  Propagate-Link-State-Activated


        IP address unassigned
  Traffic Statistics for "INSIDE":
        3393 packets input, 234923 bytes
        120 packets output, 49174 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,  6 bytes/sec
      5 minute output rate 0 pkts/sec,  3 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

若為 Ethernet1/8 介面：

```
<#root>

>

show interface e1/8


Interface Ethernet1/8 "OUTSIDE", is administratively down, 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


Down-By-Propagate-Link-State


        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        120 packets input, 46664 bytes
        3391 packets output, 298455 bytes
        0 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,  3 bytes/sec
      5 minute output rate 0 pkts/sec,  8 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

重新啟用 switchport 後，FTD 記錄會顯示：

```
<#root>

>
```

```
show log

...
Jan 03 2017 15:59:35: %ASA-4-411001:
Line protocol on Interface Ethernet1/6, changed state to up

Jan 03 2017 15:59:35: %ASA-4-411003:
Interface Ethernet1/8, changed state to administratively up

Jan 03 2017 15:59:35: %ASA-4-411003:
Interface OUTSIDE, changed state to administratively up

Jan 03 2017 15:59:35: %ASA-4-812006:
Link-State-Propagation de-activated on inline-pair due to recovery of interface Ethernet1/6(INSIDE) brir

>
```

驗證 5.配置靜態NAT

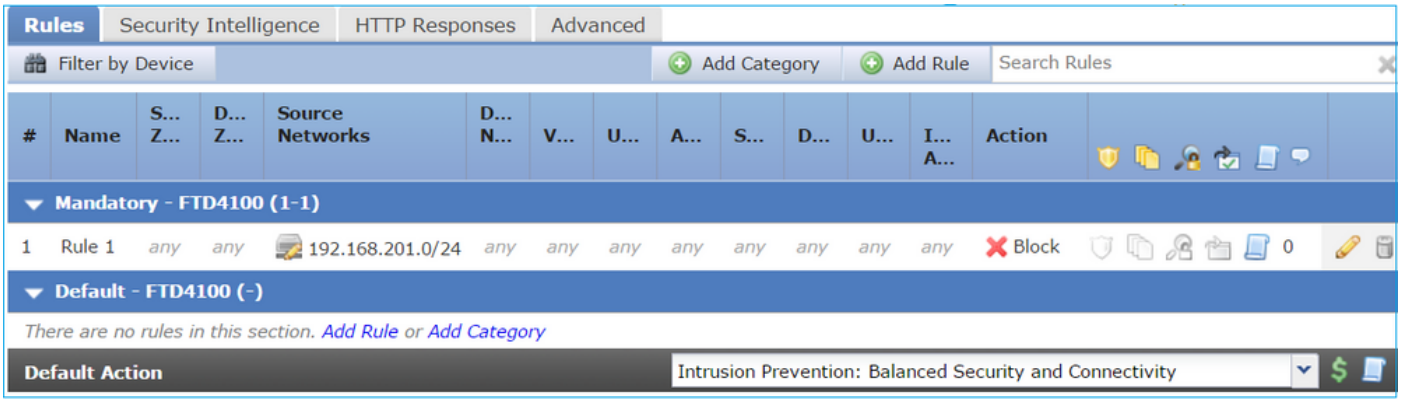
解決方案

以內嵌、內嵌分流器或被動模式執行的介面不支援 NAT：

https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Network_Address_Translation__NAT__for_Threat_Defense.html

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，並觀察映像中顯示的行為。



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>

>

show capture

capture CAPI type raw-data trace interface INSIDE

[Capturing - 210 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

透過追蹤軌跡，封包顯示：

<#root>

>

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

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 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: drop

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

```
1 packet shown
```

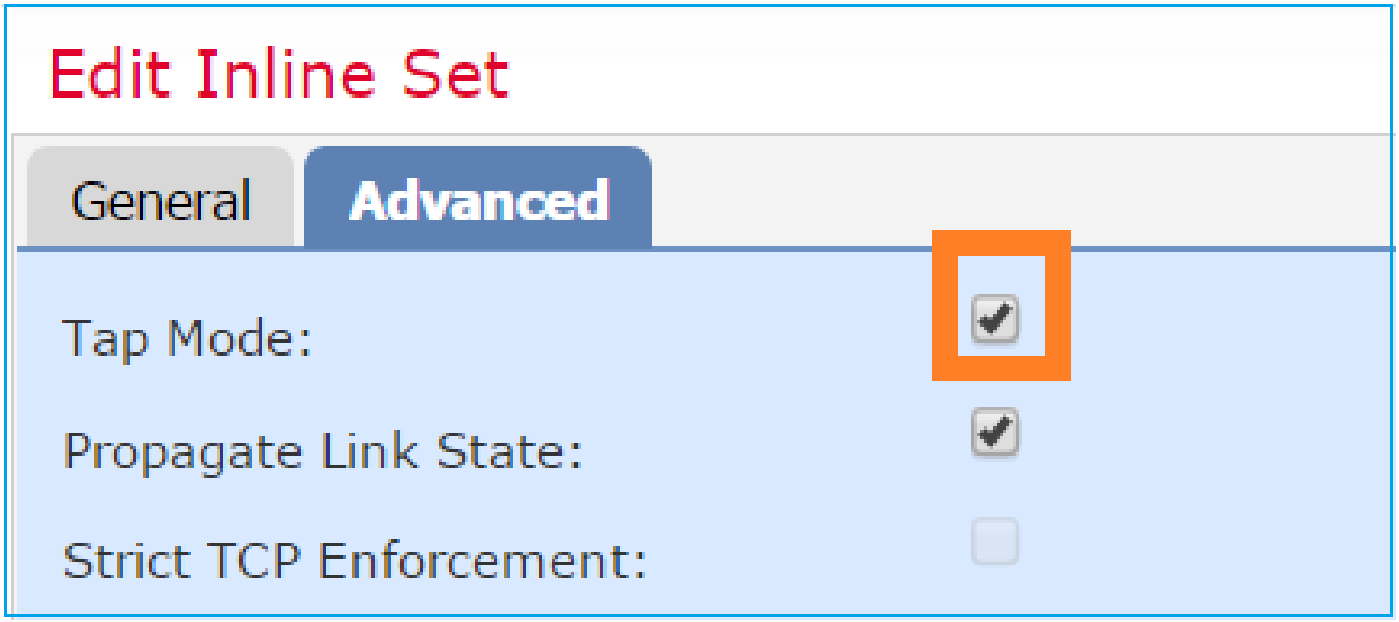
在此追蹤軌跡中，可以看到該封包已被 FTD LINA 引擎捨棄，而且沒有轉送至 FTD Snort 引擎。

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。



驗證

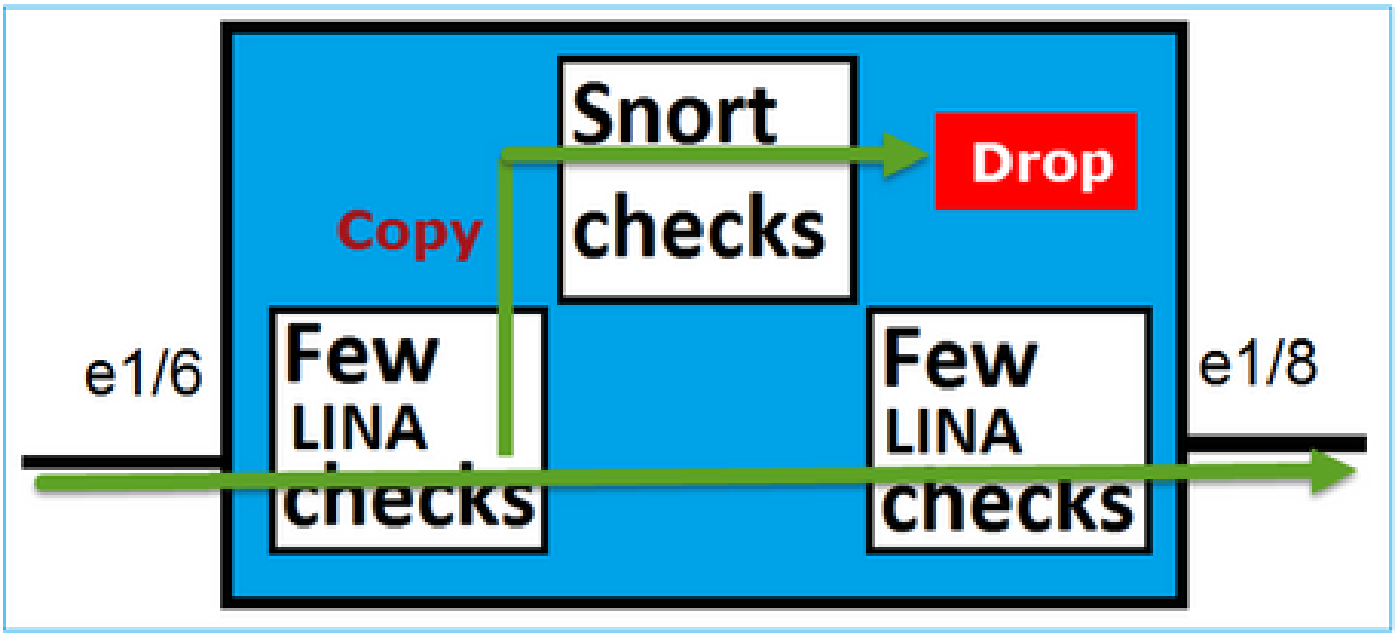
```
<#root>

>

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
>
```

驗證使用分流器的 FTD 內嵌配對介面作業

基本原理

- 使用分流器 2 設定內嵌配對時，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

最後一點如下圖所示：



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
```

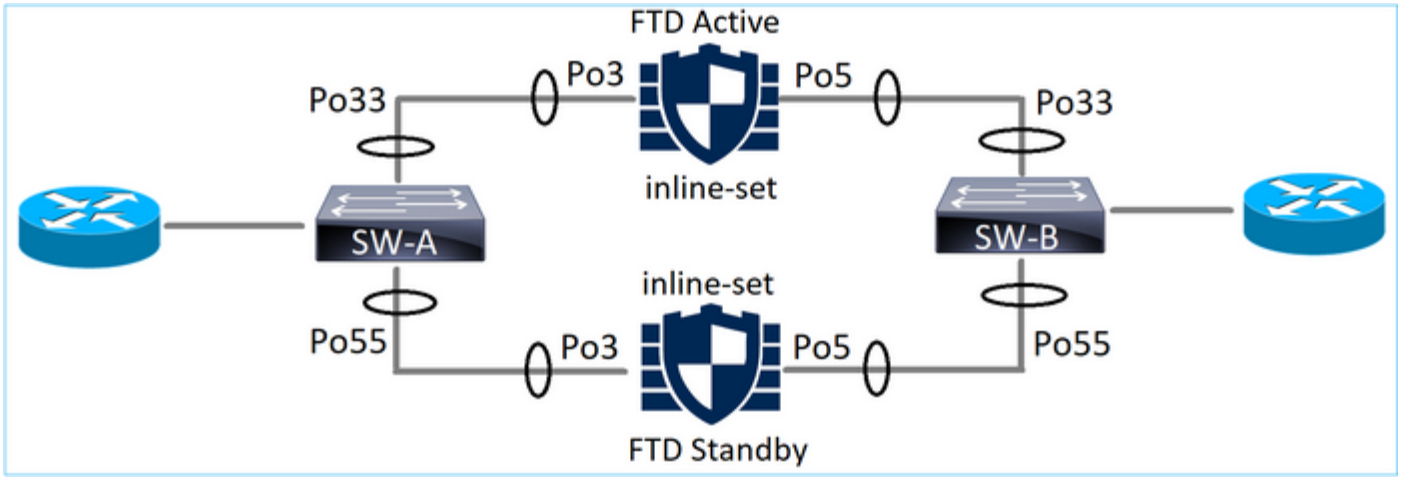
```
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list


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     Po35(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>

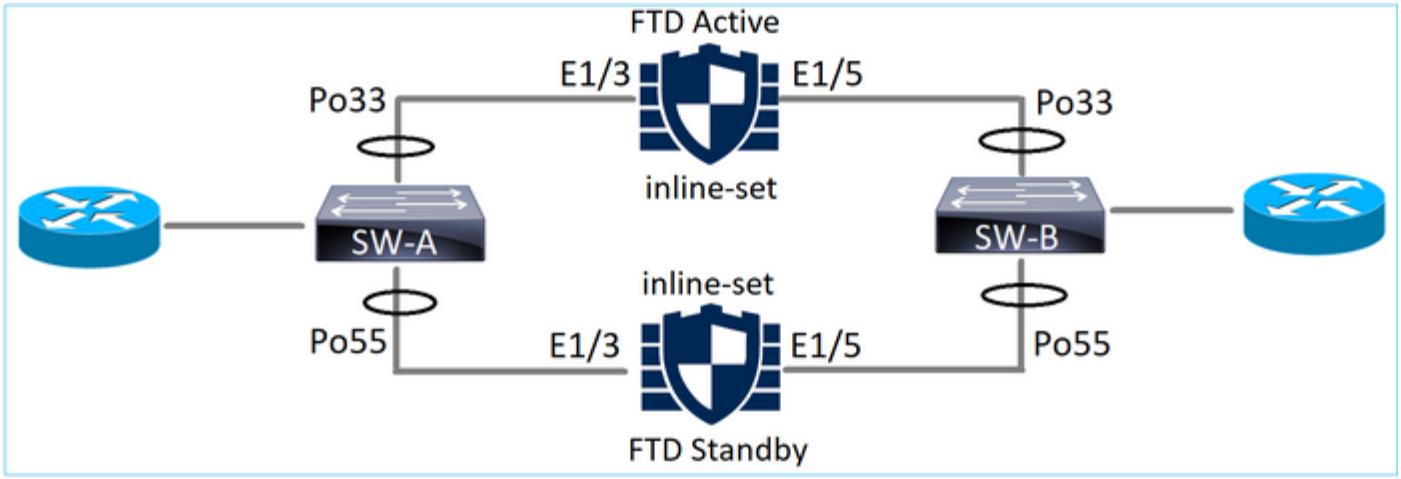
```
FTD#
```

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
```

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，若需花很長時間，中斷時間可能會非常長。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]:
	  介面：Ethernet1/6 "INSIDE"
	  Current-Status:UP
	  介面：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]:
		  介面：Ethernet1/6 "INSIDE"
		  Current-Status:UP
		  介面：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 階段：1 型別：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 階段：1 型別：CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list 階段：2

	階段：2 型別：ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list 階段：3 型別：NGIPS-MODE Subtype: ngips-mode Result: ALLOW Config: Additional Information: The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied 階段：4 型別：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	型別：ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list 階段：3 型別：NGIPS-MODE Subtype: ngips-mode Result: ALLOW Config: Additional Information: The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied 階段：4 型別：ACCESS-LIST Subtype: log 結果：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 操作：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

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）。