

在路由模式下配置Firepower威脅防禦介面

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[相關產品](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[配置路由介面和子介面](#)

[步驟 1. 配置邏輯介面](#)

[步驟 2. 配置物理介面](#)

[FTD路由介面作業](#)

[FTD路由介面概觀](#)

[驗證](#)

[在FTD路由介面上追蹤封包](#)

[相關資訊](#)

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：

- ASA5512-X - FTD代碼6.1.0.x
- Firepower管理中心(FMC)- 6.1.0.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。

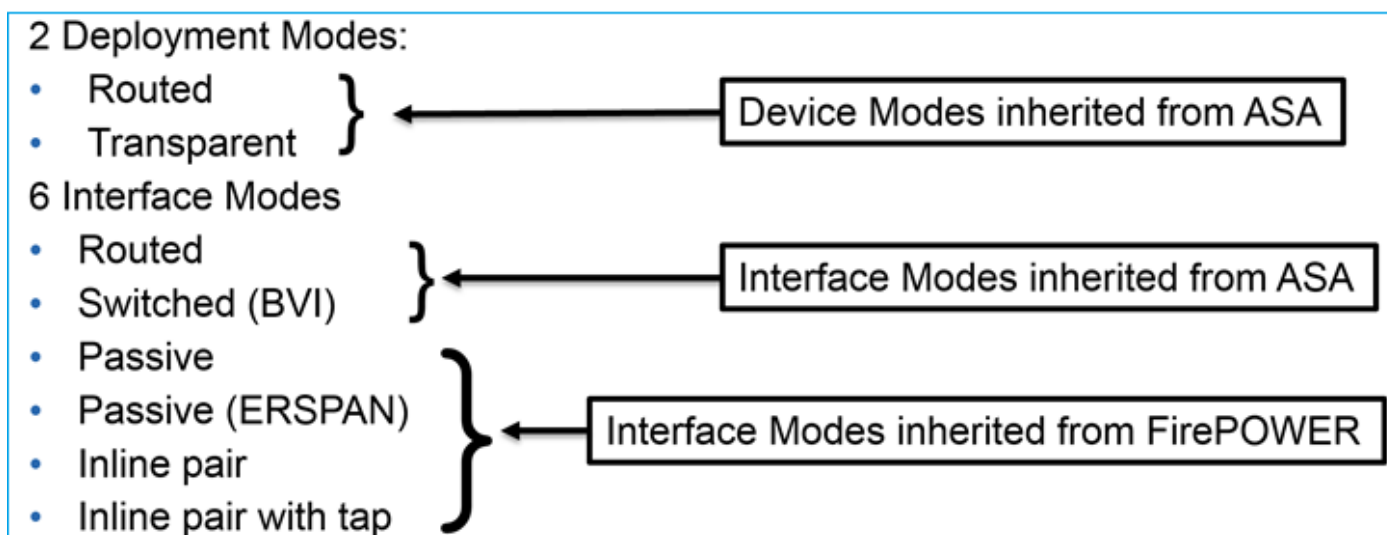
相關產品

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

Firepower威脅防禦(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。

各種FTD部署和介面模式的簡要概觀：

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

網路圖表



配置路由介面和子介面

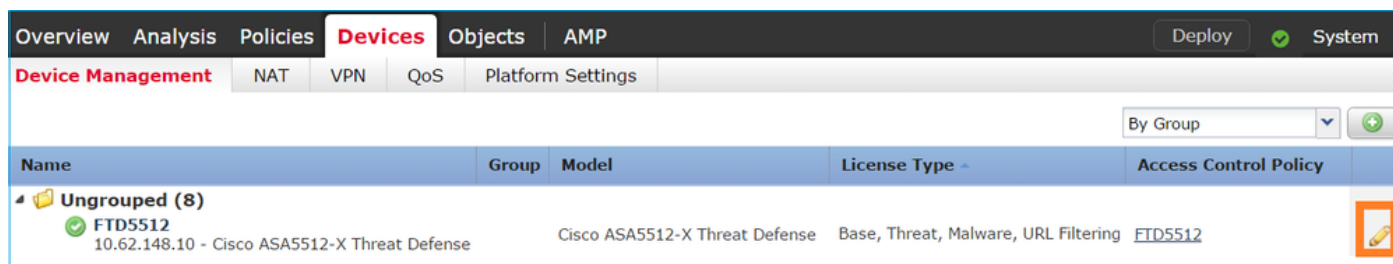
根據以下要求配置子介面G0/0.201和介面G0/1:

介面	G0/0.201	G0/1
名稱	INSIDE	OUTSIDE
安全區域	INSIDE_ZONE	OUTSIDE_ZONE
說明	內部	外部
子介面ID	201	-
VLAN ID	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
雙工/速度	自動	自動

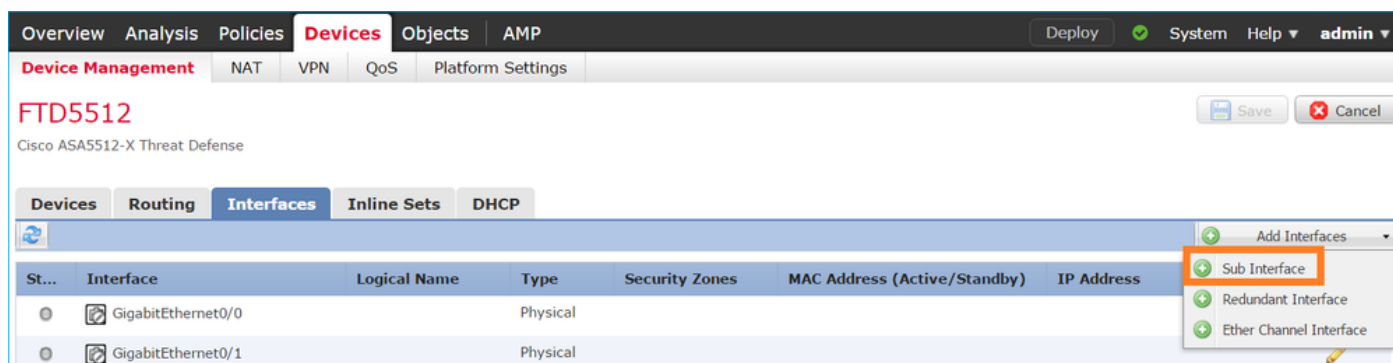
解決方案

步驟 1. 配置邏輯介面

導航到 Devices > Device Management，選擇適當的裝置，然後選擇 Edit 圖示：



選擇 Add Interfaces > Sub Interface:



根據要求配置子介面設定：

Add Sub Interface

Name: Enabled Management Only

Security Zone: ▼

Description:

General

IPv4

IPv6

Advanced

MTU: (64 - 9198)

Interface *: ▼ Enabled

Sub-Interface ID *: (1 - 4294967295)

VLAN ID: (1 - 4094)

介面IP設定：

Add Sub Interface

Name: Enabled Management Only

Security Zone: ▼

Description:

General

IPv4

IPv6

Advanced

IP Type: ▼

IP Address: eg. 1.1.1.1/255.255.255.228

在物理介面(GigabitEthernet0/0)下，指定雙工和速度設定：

General	IPv4	IPv6	Advanced	Hardware Configuration
Duplex:	<input type="text" value="auto"/> ▼			
Speed:	<input type="text" value="auto"/> ▼			

啟用物理介面 (本例中為G0/0) :

Edit Physical Interface

Mode:	<input type="text" value="None"/> ▼	
Name:	<input type="text"/>	<input checked="" type="checkbox"/> Enabled <input type="checkbox"/> Management Only
Security Zone:	<input type="text"/> ▼	
Description:	<input type="text"/>	

General	IPv4	IPv6	Advanced	Hardware Configuration
MTU:	<input type="text" value="1500"/>	(64 - 9198)		
Interface ID:	<input type="text" value="GigabitEthernet0/0"/>			

步驟 2. 配置物理介面

根據需要編輯GigabitEthernet0/1物理介面 :

Edit Physical Interface

Mode: ▼

Name: Enabled Management Only

Security Zone: ▼

Description:

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▼

IP Address: eg. 1.1.1.1/255.255.255.228

- 對於路由介面，模式為：None
- 名稱等效於ASA介面nameif
- 在FTD上，所有介面的安全層級= 0
- same-security-traffic不適用於FTD。預設會允許FTD介面之間（之間）和（內部）的流量

選擇Save和Deploy。

驗證

在FMC GUI上：

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	GigabitEthernet0/0		Physical			
	GigabitEthernet0/1	OUTSIDE	Physical	OUTSIDE_ZONE		192.168.202.1/24(Static)
	GigabitEthernet0/2		Physical			
	GigabitEthernet0/3		Physical			
	GigabitEthernet0/4		Physical			
	GigabitEthernet0/5		Physical			
	Diagnostic0/0		Physical			
	GigabitEthernet0/0.201	INSIDE	SubInterf...	INSIDE_ZONE		192.168.201.1/24(Static)

在FTD CLI上：

<#root>

>

show interface ip brief

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet0/0.201	192.168.201.1	YES	manual	up	up
GigabitEthernet0/1	192.168.202.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/3	unassigned	YES	unset	administratively down	down
GigabitEthernet0/4	unassigned	YES	unset	administratively down	down
GigabitEthernet0/5	unassigned	YES	unset	administratively down	down
Internal-Contro0/0	127.0.1.1	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
Management0/0	unassigned	YES	unset	up	up

<#root>

>

show ip

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0.201	INSIDE	192.168.201.1	255.255.255.0	manual
GigabitEthernet0/1	OUTSIDE	192.168.202.1	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0.201	INSIDE	192.168.201.1	255.255.255.0	manual
GigabitEthernet0/1	OUTSIDE	192.168.202.1	255.255.255.0	manual

FMC GUI和FTD CLI關聯：

The screenshot shows the 'Edit Sub Interface' configuration in the FMC GUI. The 'Name' field is set to 'INSIDE', the 'Security Zone' is 'INSIDE_ZONE', and the 'Description' is 'INTERNAL'. Under the 'IPv4' tab, the 'IP Type' is 'Use Static IP' and the 'IP Address' is '192.168.201.1/24'. To the right, the corresponding FTD CLI configuration is shown in a terminal window, with arrows pointing from the GUI fields to the CLI commands: 'INSIDE' in the GUI points to 'nameif INSIDE', and '192.168.201.1/24' in the GUI points to 'ip address 192.168.201.1 255.255.255.0'.

<#root>

>

show interface g0/0.201

Interface GigabitEthernet0/0.201

"

INSIDE

",

is up, line protocol is up

Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

VLAN identifier 201

Description: INTERNAL

MAC address a89d.21ce.fdea, MTU 1500

IP address 192.168.201.1, subnet mask 255.255.255.0

Traffic Statistics for "INSIDE":

1 packets input, 28 bytes

1 packets output, 28 bytes

0 packets dropped

>

show interface g0/1

Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up

Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)

Input flow control is unsupported, output flow control is off

Description: EXTERNAL

MAC address a89d.21ce.fde7, MTU 1500

IP address 192.168.202.1, subnet mask 255.255.255.0

0 packets input, 0 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 pause input, 0 resume input

0 L2 decode drops

1 packets output, 64 bytes, 0 underruns

0 pause output, 0 resume output

0 output errors, 0 collisions, 12 interface resets

0 late collisions, 0 deferred

0 input reset drops, 0 output reset drops

input queue (blocks free curr/low): hardware (511/511)

output queue (blocks free curr/low): hardware (511/511)

Traffic Statistics for "OUTSIDE":

0 packets input, 0 bytes

0 packets output, 0 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, 0 bytes/sec
 5 minute output rate 0 pkts/sec, 0 bytes/sec
 5 minute drop rate, 0 pkts/sec

>

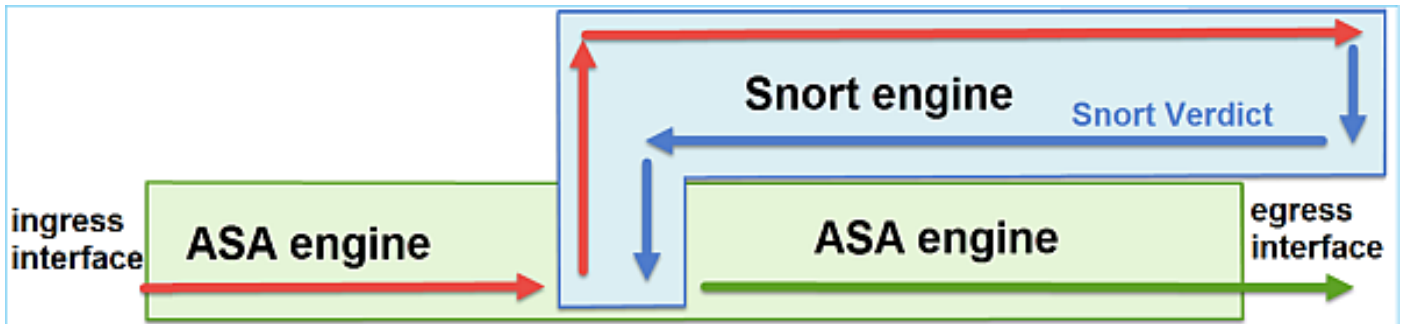
FTD路由介面作業

使用路由介面時驗證FTD封包流。

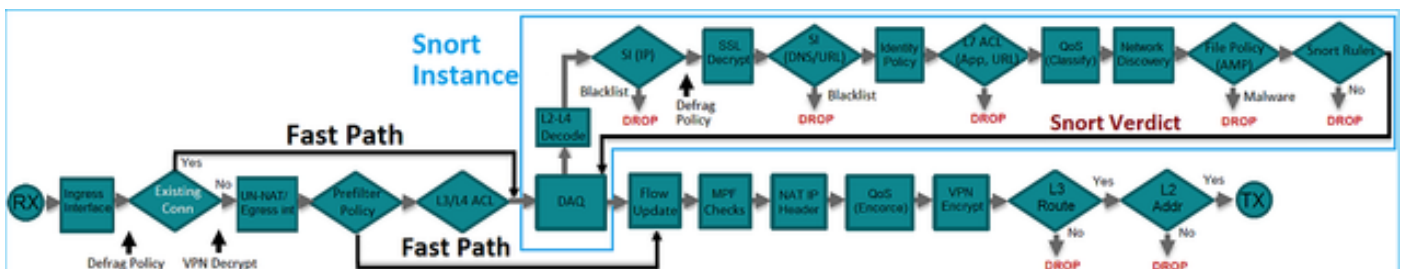
解決方案

FTD架構概觀

FTD資料平面的簡要概觀：



此圖顯示每個引擎內發生的一些檢查：



要點

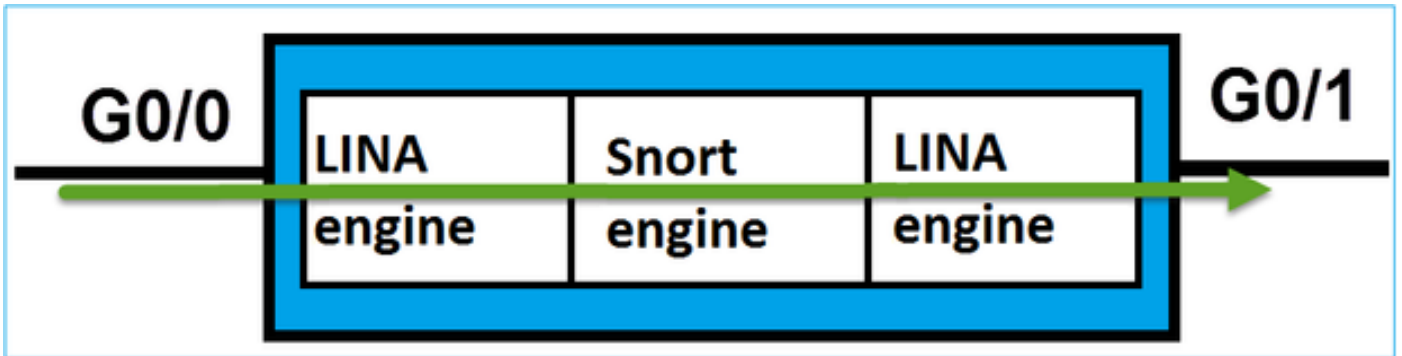
- 底部檢查對應於FTD LINA引擎資料路徑

- 藍色方框中的勾選與FTD Snort引擎例項相對應

FTD路由介面概觀

- 僅在路由部署中可用
- 傳統第3層防火牆部署
- 一個或多個物理或邏輯(VLAN)可路由介面
- 允許配置NAT或動態路由協定等功能
- 根據路由查詢轉發資料包，並根據ARP查詢解析下一跳
- 實際流量 可能遭捨棄
- 完整LINA引擎檢查會隨完整Snort引擎檢查一起應用

最後一點可以用視覺化方式呈現：



驗證

在FTD路由介面上追蹤封包

網路圖表



使用以下引數使用Packet Tracer檢視應用的策略：

輸入介面	INSIDE
通訊協定/服務	TCP埠80

來源 IP	192.168.201.100
目的地 IP	192.168.202.100

解決方案

當使用路由介面時，資料包的處理方式與傳統ASA路由介面類似。在LINA引擎資料路徑中發生路由查詢、模組化原則架構(MPF)、NAT、ARP查詢等檢查。此外，如果存取控制原則需要此功能，則封包會由Snort引擎 (其中一個Snort例項) 進行檢查，並產生判定結果傳回LINA引擎：

```
<#root>
```

```
>  
packet-tracer input INSIDE tcp 192.168.201.100 11111 192.168.202.100 80
```

```
Phase: 1
```

```
Type: ROUTE-LOOKUP
```

```
Subtype: Resolve Egress Interface
```

```
Result: ALLOW
```

```
Config:
```

```
Additional Information:
```

```
found next-hop 192.168.202.100 using egress ifc OUTSIDE
```

```
Phase: 2
```

```
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 268437505
```

```
access-list CSM_FW_ACL_ remark rule-id 268437505: ACCESS POLICY: FTD5512 - Default/1
```

```
access-list CSM_FW_ACL_ remark rule-id 268437505: L4 RULE: DEFAULT ACTION RULE
```

```
Additional Information:
```

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

Phase: 3

Type: CONN-SETTINGS

Subtype:
Result: ALLOW
Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 4

Type: NAT

Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 11336, packet dispatched to next module

Result:


input-interface: INSIDE

input-status: up
input-line-status: up

output-interface: OUTSIDE

output-status: up
output-line-status: up
Action: allow

>

 註：在第4階段，根據名為UM_STATIC_TCP_MAP的TCP對映檢查資料包。這是FTD上的預設TCP對應。

<#root>

firepower#

show run all tcp-map

```
!  
tcp-map UM_STATIC_TCP_MAP  
  no check-retransmission  
  no checksum-verification  
  exceed-mss allow  
  queue-limit 0 timeout 4  
  reserved-bits allow  
  syn-data allow  
  synack-data drop  
  invalid-ack drop  
  seq-past-window drop  
  tcp-options range 6 7 allow  
  tcp-options range 9 18 allow  
  tcp-options range 20 255 allow  
  tcp-options selective-ack allow  
  tcp-options timestamp allow
```

```
tcp-options window-scale allow
tcp-options mss allow
tcp-options md5 clear
ttl-evasion-protection
urgent-flag allow
window-variation allow-connection
!
>
```

相關資訊

- [適用於 Firepower 裝置管理員 6.1 版的 Cisco Firepower 威脅防禦設定指南](#)
- [在ASA 55xx-X裝置上安裝和升級Firepower威脅防禦](#)
- [思科安全防火牆威脅防禦](#)
- [思科技術支援與下載](#)

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）。