

在FMC管理的FTD上，使用備份ISP鏈路配置IPSec站點到站點隧道的故障轉移

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[設定FTD](#)

[步驟 1.定義主要和輔助ISP介面](#)

[步驟 2.定義主ISP介面的VPN拓撲](#)

[步驟 3.定義輔助ISP介面的VPN拓撲](#)

[步驟 4.配置SLA監控器](#)

[步驟 5.使用SLA監控器配置靜態路由](#)

[步驟 6.配置NAT免除](#)

[步驟 7.為關注流量配置訪問控制策略](#)

[配置ASA](#)

[驗證](#)

[FTD](#)

[路由](#)

[跟蹤](#)

[NAT](#)

[執行故障轉移](#)

[路由](#)

[跟蹤](#)

[NAT](#)

[疑難排解](#)

簡介

本檔案介紹如何在FMC管理的FTD上使用IP SLA追蹤功能為ISP連結設定基於密碼編譯對應之容錯移轉。

作者：思科TAC工程師Amanda Nava。

必要條件

需求

思科建議您瞭解以下主題：

- 對虛擬私人網路(VPN)的基本瞭解
- 使用FTD的經驗
- 使用FMC的經驗
- 使用自適應安全裝置(ASA)命令列體驗

採用元件

本檔案中的資訊是根據以下軟體版本：

- FMC版本6.6.0
- FTD版本6.6.0
- ASA版本9.14.1

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。

背景資訊

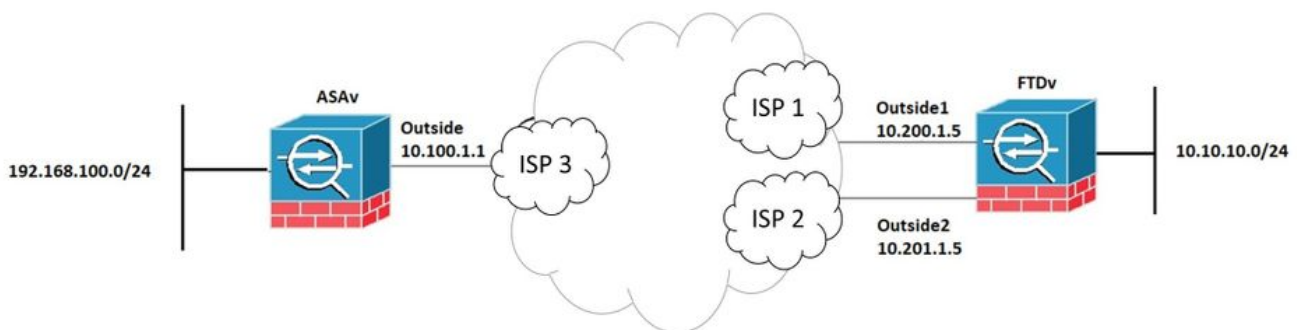
本檔案介紹如何在Firepower管理中心(FMC)管理的Firepower威脅防禦(FTD)上，使用網際網路通訊協定服務等級協定(IP SLA)追蹤功能，為備份網際網路服務供應商(ISP)連結設定基於加密對映的容錯移轉。它還解釋了當存在兩個ISP並且需要無縫故障切換時，如何為VPN流量配置網路地址轉換(NAT)免除。

在此案例中，VPN是從FTD建立到ASA，作為只有一個ISP介面的VPN對等體。FTD當時使用一個ISP鏈路來建立VPN。當主ISP鏈路斷開時，FTD通過SLA監控器接管輔助ISP鏈路，並建立VPN。

設定

網路圖表

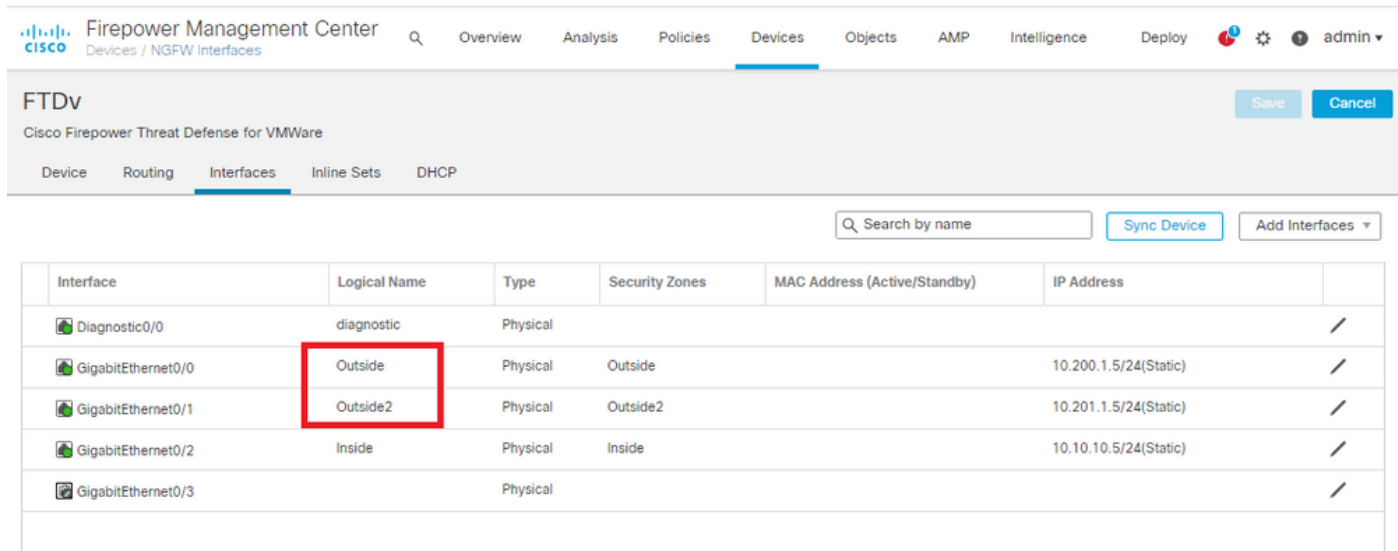
以下是本文檔中示例使用的拓撲：



設定FTD

步驟 1. 定義主要和輔助ISP介面

1.導覽至Devices > Device Management > Interfaces , 如下圖所示。




The screenshot shows the Cisco Firepower Management Center interface for an FTDv device. The 'Interfaces' tab is selected, and a table lists several interfaces. The 'Logical Name' column for 'GigabitEthernet0/1' is highlighted with a red box, showing 'Outside2'.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
Diagnostic0/0	diagnostic	Physical			
GigabitEthernet0/0	Outside	Physical	Outside		10.200.1.5/24(Static)
GigabitEthernet0/1	Outside2	Physical	Outside2		10.201.1.5/24(Static)
GigabitEthernet0/2	Inside	Physical	Inside		10.10.10.5/24(Static)
GigabitEthernet0/3		Physical			

步驟 2.定義主ISP介面的VPN拓撲

1.導航到Devices > VPN > Site To Site。 在Add VPN下 , 按一下Firepower Threat Defense Device , 建立VPN並選擇外部介面。

 注意：本文檔不介紹如何從頭開始配置S2S VPN。有關FTD上S2S VPN配置的更多詳情，請訪問<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html>

Edit VPN Topology

Topology Name:*

Network Topology:
 Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A: +

Device Name	VPN Interface	Protected Networks	
ASAv	10.100.1.1	10.10.20.0_24	

Node B: +

Device Name	VPN Interface	Protected Networks	
FTDv	Outside/10.200.1.5	10.10.10.0_24	

Ensure the protected networks are allowed by access control policy of each device.

步驟 3. 定義輔助ISP介面的VPN拓撲

1. 導航到 Devices > VPN > Site To Site。在 Add VPN 下，按一下 Firepower Threat Defense Device，建立 VPN 並選擇 Outside2 介面。

注意：使用 Outside2 介面的 VPN 配置必須與 Outside VPN 拓撲完全相同，但 VPN 介面除外。

Edit VPN Topology

Topology Name:*

Network Topology:
 Point to Point Hub and Spoke Full Mesh

IKE Version:* IKEv1 IKEv2

Endpoints IKE IPsec Advanced

Node A: +

Device Name	VPN Interface	Protected Networks	
ASAv	10.100.1.1	10.10.20.0_24	

Node B: +

Device Name	VPN Interface	Protected Networks	
FTDv	Outside2/10.201.1.5	10.10.10.0_24	

Ensure the protected networks are allowed by access control policy of each device.

必須如圖所示配置VPN拓撲。

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence Deploy admin

Devices / VPN / Site To Site

Add VPN

Node A	Node B	
-- VPN_Outside1		
extranet : ASAv / 10.100.1.1	FTDv / Outside / 10.200.1.5	
-- VPN_Outside2		
extranet : ASAv / 10.100.1.1	FTDv / Outside2 / 10.201.1.5	

步驟 4. 配置SLA監控器

1. 導航到對象 > SLA監控器 > 新增SLA監控器。在Add VPN下，按一下Firepower Threat Defense Device，然後配置SLA監控器，如下圖所示。

Firepower Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** AMP Intelligence Deploy admin

Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
RADIUS Server Group
Route Map
Security Group Tag
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone
URL
Variable Set
VLAN Tag
VPN

SLA Monitor

[Add SLA Monitor](#) Filter

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

Name	Value
ISP_Outside1	Security Zone: Outside Monitor ID: 10 Monitor Address: 10.200.1.1

2.對於SLA Monitor ID*欄位，使用Outside next-hop IP address。

Edit SLA Monitor Object



Name:

Description:

Frequency (seconds):

(1-604800)

SLA Monitor ID*:

Threshold

(milliseconds):

(0-60000)

Timeout

(milliseconds):

(0-604800000)

Data Size (bytes):

(0-16384)

ToS:

Number of Packets:

Monitor Address*:

Available Zones

Inside

Outside

Outside2

Selected Zones/Interfaces

Add

Outside

Cancel

Save

步驟 5. 使用SLA監控器配置靜態路由

1. 定位至 Devices > Routing > Static Route。選擇 Add Route，並使用 Route tracking 欄位中的 SLA Monitor 資訊（步驟 4 中建立的）配置外部（主）介面的默認路由。

Edit Static Route Configuration

Type: IPv4 IPv6

Interface*
Outside1
(Interface starting with this icon signifies it is available for route leak)

Available Network +

Search

- 10.10.10.0
- 192.168.100.1
- 192.168.200.0
- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local

Add

Selected Network

any-ipv4

Gateway*
10.200.1.1 +

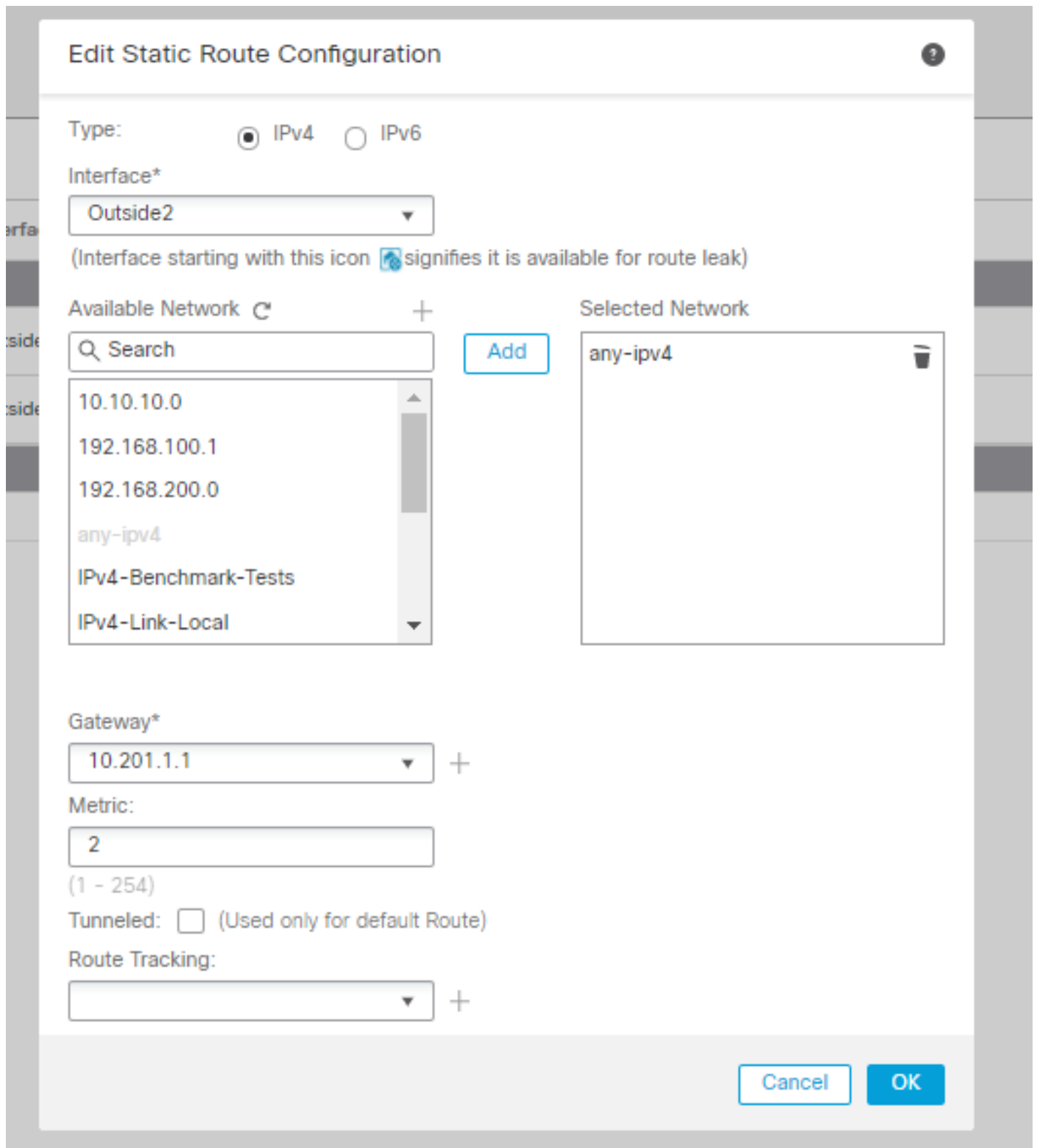
Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
ISP_Outside1 +

Cancel OK

2. 配置 Outside2（輔助）介面的預設路由。Metric 值必須高於主預設路由。本節中不需要任何路由跟蹤欄位。



必須如圖所示配置路由。

Firepower Management Center
Devices / NGFW Routing

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy admin

FTDv
Cisco Firepower Threat Defense for VMWare

Device **Routing** Interfaces Inline Sets DHCP

OSPF
OSPFv3
RIP
BGP
IPv4
IPv6
Static Route
Multicast Routing
IGMP
PIM
Multicast Routes
Multicast Boundary Filter

+ Add Route

Network	Interface	Gateway	Tunneled	Metric	Tracked	
IPv4 Routes						
any-ipv4	Outside2	10.201.1.1	false	2		
any-ipv4	Outside	10.200.1.1	false	1	ISP_Outside1	
IPv6 Routes						

步驟 6. 配置NAT免除

1. 導覽至 Devices > NAT > NAT Policy，然後選擇針對FTD裝置的策略。選擇Add Rule並配置每個ISP介面（Outside和Outside2）的NAT例外。NAT規則必須相同，但目標介面除外。

Firepower Management Center
Devices / NGFW NAT Policy Editor


Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy admin

NAT_FTDv
Enter Description

Rules Policy Assignments (1)

Filter by Device + Add Rule

#	Direction	Type	Source Interface	Destination Interface	Original Packet			Translated Packet			Options	
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services		
NAT Rules Before												
1		Static	Inside	Outside	10.10.10.0	192.168.100.1		10.10.10.0	192.168.100.1		route-lookup no-proxy-arp	
2		Static	Inside	Outside2	10.10.10.0	192.168.100.1		10.10.10.0	192.168.100.1		route-lookup no-proxy-arp	
Auto NAT Rules												
NAT Rules After												

 注意：對於此情況，兩個NAT規則都需要啟用路由查詢。否則，流量將到達第一個規則，並且不會保留到故障轉移路由。如果未啟用路由查詢，則始終使用（第一個NAT規則）Outside介面傳送流量。啟用Route-lookup後，流量始終保持到通過SLA監控器控制的路由表。

步驟 7. 為關注流量配置訪問控制策略

1. 定位至 Policies > Access Control > Select the Access Control Policy。要新增規則，請點選Add Rule，如下圖所示。

配置一條從Inside到Outside區域（Outside1和Outside2）的規則，允許從10.10.10.0/24到

192.168.100/24的相關流量。

配置從Outside zones (Outside1和Outside 2) 到Inside的另一個規則，允許從192.168.100/24到10.10.10.0/24的有趣流量。

The screenshot shows the Cisco Firepower Management Center interface for configuring rules in the ACP-FTDv policy. The 'Rules' tab is active, and a search filter is applied. Two rules are listed and highlighted with a red border:

ID	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action	Icons
1	VPN_1_out	Inside	Outside Outside2	10.10.10.0	192.168.100.	Any	Any	Any	Any	Any	Any	Any	Any	Allow	[Icons]
2	VPN_1_in	Outside2 Outside	Inside	192.168.100.	10.10.10.0	Any	Any	Any	Any	Any	Any	Any	Any	Allow	[Icons]

配置ASA

注意：對於此特定情況，在IKEv2加密對映上配置備份對等體，此功能要求ASA在9.14.1或更高版本上。如果您的ASA運行的是較舊版本，請使用IKEv1作為解決方法。如需更多參考，請參閱Cisco錯誤ID [CSCud22276](#)。

1. 在ASA的外部介面上啟用IKEv2:

```
Crypto ikev2 enable Outside
```

2. 建立定義在FTD上配置的相同引數的IKEv2策略：

```
crypto ikev2 policy 1  
encryption aes-256  
integrity sha256  
group 14  
prf sha256  
lifetime seconds 86400
```

3. 建立允許ikev2協定的組策略：

```
group-policy IKEV2 internal
```

```
group-policy IKEV2 attributes
vpn-tunnel-protocol ikev2
```

4. 為每個外部FTD IP位址 (Outside1和Outside2) 建立通道群組。引用組策略並指定預共用金鑰：

```
tunnel-group 10.200.1.5 type ipsec-l2l
tunnel-group 10.200.1.5 general-attributes
  default-group-policy IKEV2
tunnel-group 10.200.1.5 ipsec-attributes
  ikev2 remote-authentication pre-shared-key Cisco123
  ikev2 local-authentication pre-shared-key Cisco123

tunnel-group 10.201.1.5 type ipsec-l2l
tunnel-group 10.201.1.5 general-attributes
  default-group-policy IKEV2
tunnel-group 10.201.1.5 ipsec-attributes
  ikev2 remote-authentication pre-shared-key Cisco123
  ikev2 local-authentication pre-shared-key Cisco123
```

5. 建立定義要加密的流量的訪問清單：(FTD子網10.10.10.0/24)(ASA子網192.168.100.0/24):

```
Object network FTD-Subnet
  Subnet 10.10.10.0 255.255.255.0
Object network ASA-Subnet
  Subnet 192.168.100.0 255.255.255.0
access-list VPN_1 extended permit ip 192.168.100.0 255.255.255.0 10.10.10.0 255.255.255.0
```

6. 建立ikev2 ipsec-proposal以引用FTD上指定的演算法：

```
crypto ipsec ikev2 ipsec-proposal CSM_IP_1
  protocol esp encryption aes-256
  protocol esp integrity sha-256
```

7. 建立將配置關聯在一起的加密對映條目，並新增Outside1和Outside2 FTD IP地址：

```
crypto map CSM_Outside_map 1 match address VPN_1
crypto map CSM_Outside_map 1 set peer 10.200.1.5 10.201.1.5
crypto map CSM_Outside_map 1 set ikev2 ipsec-proposal CSM_IP_1
crypto map CSM_Outside_map 1 set reverse-route
crypto map CSM_Outside_map interface Outside
```

8. 建立阻止防火牆NAT的NAT免除語句：

```
Nat (inside,Outside) 1 source static ASA-Subnet ASA-Subnet destination static FTD-Subnet FTD-Subnet
```

驗證

使用本節內容，確認您的組態是否正常運作。

FTD

在命令列中，使用show crypto ikev2 sa命令驗證VPN狀態。

 注意：VPN是使用Outside1的IP地址(10.200.1.5)作為本地地址建立的。

```
firepower# sh crypto ikev2 sa
```

```
IKEv2 SAs:
```

```
Session-id:24, Status:UP-ACTIVE, IKE count:1, CHILD count:1
```

```
Tunnel-id Local Remote
373101057 10.200.1.5/500 10.100.1.1/500
    Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:14, Auth sign: PSK, Auth verify: PSK
    Life/Active Time: 86400/37 sec
Child sa: local selector 10.10.10.0/0 - 10.10.10.255/65535
          remote selector 192.168.100.0/0 - 192.168.100.255/65535
          ESP spi in/out: 0x829ed58d/0x2051ccc9
```

路由

預設路由顯示Outside1的下一跳IP地址。

```
firepower# sh route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.200.1.1 to network 0.0.0.0
```

```
S*    0.0.0.0 0.0.0.0 [1/0] via 10.200.1.1, Outside1
C    10.10.10.0 255.255.255.0 is directly connected, Inside
L    10.10.10.5 255.255.255.255 is directly connected, Inside
C    10.200.1.0 255.255.255.0 is directly connected, Outside1
L    10.200.1.5 255.255.255.255 is directly connected, Outside1
C    10.201.1.0 255.255.255.0 is directly connected, Outside2
L    10.201.1.5 255.255.255.255 is directly connected, Outside2
```

跟蹤

如show track 1輸出所示，「Reachability is Up」。

```
firepower# sh track 1
Track 1
  Response Time Reporter 10 reachability
  Reachability is Up          <-----
  36 changes, last change 00:00:04
  Latest operation return code: OK
  Latest RTT (milliseconds) 1
  Tracked by:
    STATIC-IP-ROUTING 0
```

NAT

需要確認相關流量通過Outside1介面到達NAT免除規則。

使用Packet Tracer input Inside icmp 10.10.1 8 0 192.168.100.10 detail命令檢驗應用於相關流量的NAT規則。

```
firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det
```

```
-----OMITTED OUTPUT -----
```

```
Phase: 4
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
Additional Information:
NAT divert to egress interface Outside1(vrfid:0)
Untranslate 192.168.100.1/0 to 192.168.100.1/0
```

```
-----OMITTED OUTPUT -----
```

```
Phase: 7
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
```

Additional Information:

Static translate 10.10.10.1/0 to 10.10.10.1/0

Forward Flow based lookup yields rule:

```
in id=0x2b3e09576290, priority=6, domain=nat, deny=false
  hits=19, user_data=0x2b3e0c341370, cs_id=0x0, flags=0x0, protocol=0
  src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0)
```

Phase: 8

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

```
in id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
  hits=3596, user_data=0x0, cs_id=0x0, reverse, use_real_addr, 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=any, output_ifc=any
```

-----OMITTED OUTPUT -----

Phase: 12

Type: VPN

Subtype: encrypt

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

```
out id=0x2b3e0c8d0250, priority=70, domain=encrypt, deny=false
  hits=5, user_data=0x16794, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0
  src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=any(vrfid:65535), output_ifc=Outside1
```

Phase: 13

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
nat (Inside,Outside1) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
```

Additional Information:

Forward Flow based lookup yields rule:

```
out id=0x2b3e095d49a0, priority=6, domain=nat-reverse, deny=false
  hits=1, user_data=0x2b3e0c3544f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=Inside(vrfid:0), output_ifc=Outside1(vrfid:0)
```

Phase: 14

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

```
in id=0x2b3e0c8ad890, priority=70, domain=ipsec-tunnel-flow, deny=false
  hits=5, user_data=0x192ec, cs_id=0x2b3e0b633c60, reverse, flags=0x0, protocol=0
  src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=Outside1(vrfid:0), output_ifc=any
```

```
Phase: 15
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
  hits=3598, user_data=0x0, cs_id=0x0, reverse, use_real_addr, 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=any, output_ifc=any
```

-----OMITTED OUTPUT -----

```
Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: Outside1(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

執行故障轉移

在本示例中，故障切換是通過在IP SLA監控器配置中使用的Outside1的Next hop上關閉來執行的。

```
firepower# sh sla monitor configuration 10
IP SLA Monitor, Infrastructure Engine-II.
Entry number: 10
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.200.1.1
Interface: Outside1
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 60
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:
```

路由

預設路由現在使用Outside2的下一跳IP地址，可達性為Down。

```
firepower# sh route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.201.1.1 to network 0.0.0.0
```

```
S*      0.0.0.0 0.0.0.0 [2/0] via 10.201.1.1, Outside2
C       10.10.10.0 255.255.255.0 is directly connected, Inside
L       10.10.10.5 255.255.255.255 is directly connected, Inside
C       10.200.1.0 255.255.255.0 is directly connected, Outside1
L       10.200.1.5 255.255.255.255 is directly connected, Outside1
C       10.201.1.0 255.255.255.0 is directly connected, Outside2
L       10.201.1.5 255.255.255.255 is directly connected, Outside2
```

跟蹤

如show track 1輸出所示，此時顯示「Reachability is Down」。

```
firepower# sh track 1
Track 1
Response Time Reporter 10 reachability
Reachability is Down <----
37 changes, last change 00:17:02
Latest operation return code: Timeout
Tracked by:
STATIC-IP-ROUTING 0
```

NAT

```
firepower# packet-tracer input inside icmp 10.10.10.1 8 0 192.168.100.1 det
-----OMITTED OUTPUT -----
```

```
Phase: 4
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
Additional Information:
Static translate 10.10.10.1/0 to 10.10.10.1/0
Forward Flow based lookup yields rule:
```

```
in id=0x2b3e0c67d470, priority=6, domain=nat, deny=false
  hits=44, user_data=0x2b3e0c3170e0, cs_id=0x0, flags=0x0, protocol=0
  src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0)
```

-----OMITTED OUTPUT -----

Phase: 9

Type: VPN

Subtype: encrypt

Result: ALLOW

Config:

Additional Information:

Forward Flow based lookup yields rule:

```
out id=0x2b3e0c67bdb0, priority=70, domain=encrypt, deny=false
  hits=1, user_data=0x1d4cfb24, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0
  src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=any(vrfid:65535), output_ifc=Outside2
```

Phase: 10

Type: NAT

Subtype: rpf-check

Result: ALLOW

Config:

```
nat (Inside,Outside2) source static 10.10.10.0 10.10.10.0 destination static 192.168.100.1 192.168.100.1
```

Additional Information:

Forward Flow based lookup yields rule:

```
out id=0x2b3e0c6d5bb0, priority=6, domain=nat-reverse, deny=false
  hits=1, user_data=0x2b3e0b81bc00, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
  src ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=Inside(vrfid:0), output_ifc=Outside2(vrfid:0)
```

Phase: 11

Type: VPN

Subtype: ipsec-tunnel-flow

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

```
in id=0x2b3e0c8a14f0, priority=70, domain=ipsec-tunnel-flow, deny=false
  hits=1, user_data=0x1d4d073c, cs_id=0x2b3e0c273db0, reverse, flags=0x0, protocol=0
  src ip/id=192.168.100.0, mask=255.255.255.0, port=0, tag=any
  dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
  input_ifc=Outside2(vrfid:0), output_ifc=any
```

Phase: 12

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Reverse Flow based lookup yields rule:

```
in id=0x2b3e0a482330, priority=0, domain=nat-per-session, deny=true
  hits=3669, user_data=0x0, cs_id=0x0, reverse, use_real_addr, 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=any, output_ifc=any
```

-----OMITTED OUTPUT -----

Result:
input-interface: Inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: Outside2(vrfid:0)
output-status: up
output-line-status: up
Action: allow

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）。