

# Configuratie van failover voor IPsec site-to-site tunnels met back-up van ISP-links op FTD beheerd door FMC

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Het FTD configureren](#)

[Stap 1. De primaire en secundaire ISP-interfaces definiëren](#)

[Stap 2. De VPN-topologie voor de primaire ISP-interface definiëren](#)

[Stap 3. De VPN-topologie voor de secundaire ISP-interface definiëren](#)

[Stap 4. De SLA-monitor configureren](#)

[Stap 5. De statische routes configureren met de SLA-monitor](#)

[Stap 6. De NAT-vrijstelling configureren](#)

[Stap 7. Het toegangscontrolebeleid voor interessant verkeer configureren](#)

[ASA configureren](#)

[Verifiëren](#)

[FTD](#)

[Route](#)

[Spoor](#)

[NAT](#)

[failover uitvoeren](#)

[Route](#)

[Spoor](#)

[NAT](#)

[Problemen oplossen](#)

## Inleiding

In dit document wordt beschreven hoe u op crypto map gebaseerde failover voor ISP-koppeling kunt configureren met de functie IP SLA-track op de FTD die wordt beheerd door FMC.

Bijgedragen door Amanda Nava, Cisco TAC Engineer.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van een Virtual Private Network (VPN)

- Ervaring met FTD
- Ervaring met het VCC
- Ervaring met opdrachtregel voor adaptieve security applicatie (ASA)

## Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- FMC versie 6.6.0
- FTD versie 6.6.0
- ASA versie 9.14.1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

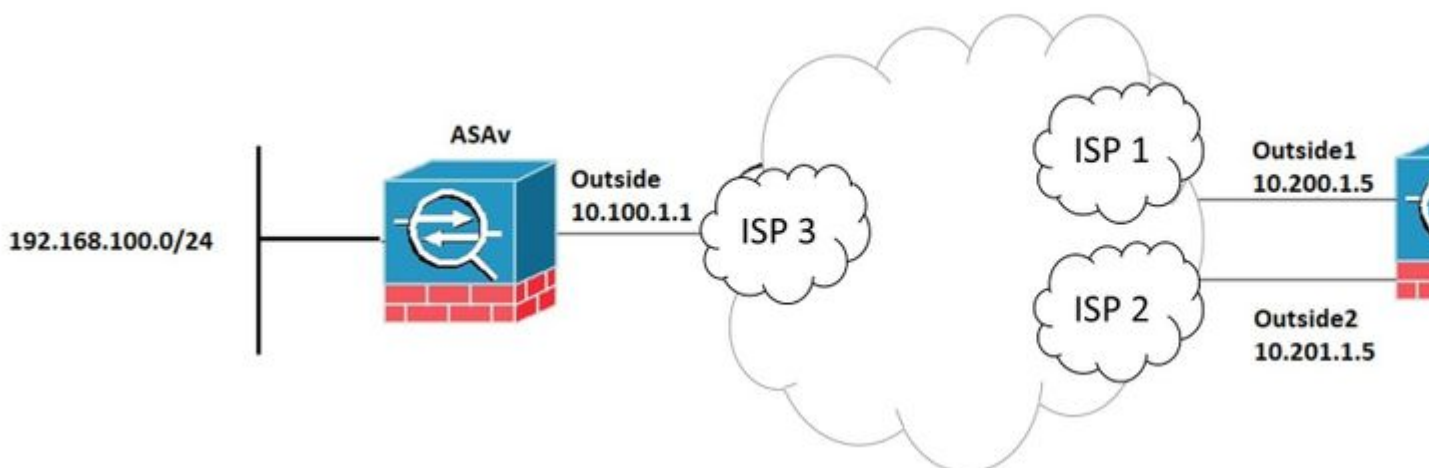
In dit document wordt beschreven hoe u op crypto map gebaseerde failover kunt configureren voor een koppeling van een back-up naar een Internet Service Provider (ISP) en de trackfunctie van de Internet Protocol Service Level Agreement (IP SLA) op de Firepower Threat Defence (FTD) die wordt beheerd door Firepower Management Center (FMC). Het legt ook uit hoe u de NAT-vrijstelling (Network Address Translation) kunt configureren voor VPN-verkeer wanneer er twee ISP's zijn en wanneer er een naadloze failover vereist is.

In dit scenario is de VPN vanuit de FTD naar de ASA opgezet als de VPN-peer met slechts één ISP-interface. De FTD gebruikt op dat moment één ISP-link om de VPN tot stand te brengen. Wanneer de primaire ISP-link naar beneden gaat, neemt de FTD de secundaire ISP-link over via de SLA Monitor en wordt de VPN tot stand gebracht.

## Configureren

### Netwerkdigram

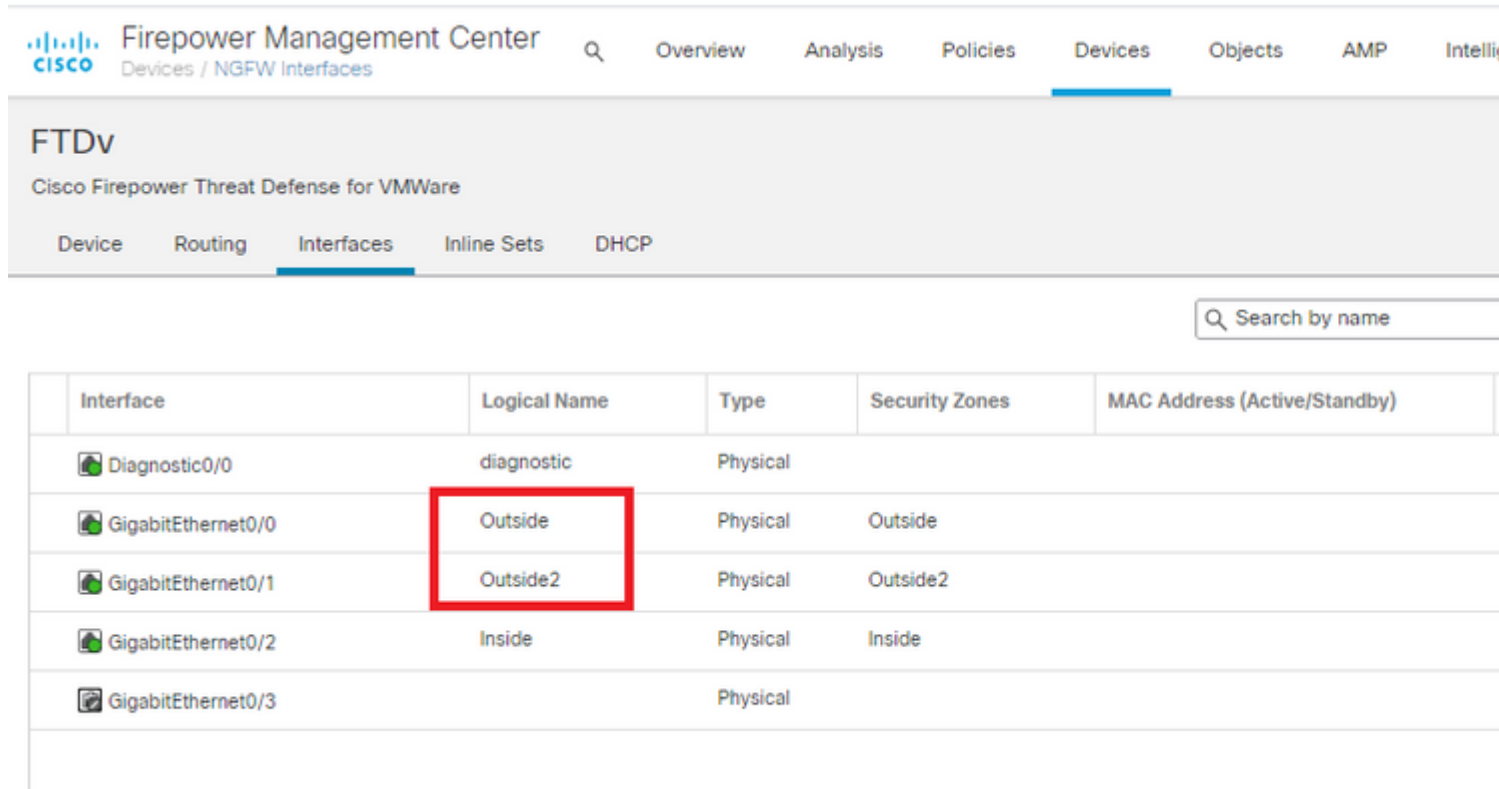
Dit is de topologie die bij het voorbeeld door dit document wordt gebruikt:



### Het FTD configureren

## Stap 1. De primaire en secundaire ISP-interfaces definiëren

1. Navigeer naar **Apparaten > Apparaatbeheer > Interfaces** zoals in de afbeelding.



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 shows 'Outside' and 'Outside2' highlighted with a red box.

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

## Stap 2. De VPN-topologie voor de primaire ISP-interface definiëren

1. Navigeer naar **Apparaten > VPN > Site to Site**. Klik onder **Add VPN** op **Firepower Threat Defence Device**, maak de VPN en selecteer de buiteninterface.

**Opmerking:** dit document beschrijft niet hoe u een S2S VPN vanuit het niets kunt configureren. Ga voor meer informatie over de S2S VPN-configuratie op FTD naar <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:

IKE Version:\*  IKEv1  IKEv2

Endpoints

---

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.

### Stap 3. De VPN-topologie voor de secundaire ISP-interface definiëren

1. Navigeer naar **Apparaten > VPN > Site to Site**. Klik onder **Add VPN** op **Firepower Threat Defense Device**, maak de VPN en selecteer de interface Outside2.

---

**Opmerking:** de VPN-configuratie die de Outside2-interface gebruikt, moet exact hetzelfde zijn als de Outside VPN-topologie, behalve de VPN-interface.

---

### Edit VPN Topology

Topology Name:\*

Network Topology:

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.

VPN-topologieën moeten worden geconfigureerd zoals in de afbeelding.

Firepower Management Center Overview Analysis Policies **Devices** Objects AMP Intelli

Devices / VPN / Site To Site

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

#### Stap 4. De SLA-monitor configureren

1. Ga naar **Objecten > SLA-monitor > SLA-monitor toevoegen**. Klik onder **Add VPN** op **Firepower Threat Defence Device** en configureer de SLA-monitor zoals in de afbeelding.

Firepower Management Center  
Objects / Object Management

Overview Analysis Policies Devices **Objects** AMP Intell

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

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. 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: 10.20

Add SLA Monitor

2. Gebruik voor het veld **SLA Monitor ID\*** het IP-adres van de volgende hop buiten.

**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

Selected Zones/Interfaces

Inside  Outside

Outside


Outside2


## Stap 5. De statische routes configureren met de SLA-monitor

1. Navigeer naar **Apparaten > Routing > Statische Route**. Selecteer **Route toevoegen** en configureer de standaardroute voor de (primaire) buiteninterface met de informatie over SLA-monitor (gemaakt in stap 4) in het veld **Routertracering**.

### Edit Static Route Configuration

Type:  IPv4  IPv6

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

Available Network  +

Selected Network

Q Search

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

Gateway\*  
10.200.1.1 +

Metric:  
1  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
ISP\_Outside1 +


2. Configureer de standaardroute voor de (secundaire) interface Outside2. De metrieke waarde moet hoger zijn dan de primaire standaardroute. In deze sectie is geen veld **voor** routertracing nodig.




### Edit Static Route Configuration

Type:  IPv4  IPv6

Interface\*  
Outside2

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


Available Network  +

Selected Network

Search

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


Add

any-ipv4 

Gateway\*  
10.201.1.1 +

Metric:  
2  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
+ 

Cancel OK

De routers moeten worden geconfigureerd zoals in het beeld.



## 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

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

### Stap 6. De NAT-vrijstelling configureren

1. Navigeer naar **Apparaten > NAT > NAT-beleid** en selecteer het Beleid dat zich op het FTD-apparaat richt. **Selecteer Add Rule** en vorm een NAT vrijstelling per ISP interface (Buiten en Outside2). NAT-regels moeten hetzelfde zijn, behalve voor de doelinterface.



## NAT\_FTDv

Enter Description

Rules

[Filter by Device](#)

#	Direction	Type	Source Interface	Destination Interface	Original Packet			Translated		
					Original Sources	Original Destinations	Original Services	Sources	Destinations	
NAT Rules Before										
1	↔	Static	Inside	Outside	10.10.10.0	192.168.100.1		10.10.10.0	192.168.100.1	
2	↔	Static	Inside	Outside2	10.10.10.0	192.168.100.1		10.10.10.0	192.168.100.1	
Auto NAT Rules										
NAT Rules After										

**Opmerking:** voor dit scenario is voor beide NAT-regels **de optie Route-lookup** ingeschakeld. Anders zou het verkeer de eerste regel raken en niet aan de failover routes houden. Als route lookup niet is ingeschakeld, wordt het verkeer altijd verzonden met behulp van de (eerste NAT-regel) Buiten interface. Als **Route-lookup** is ingeschakeld, behoudt verkeer zich altijd aan de Routing-tabel die via de SLA-monitor wordt beheerd.

### Stap 7. Het toegangscontrolebeleid voor interessant verkeer configureren

1. Navigeer naar **Beleid > Toegangsbeheer > Selecteer het Toegangsbeheerbeleid**. Klik op **Regel toevoegen** om een regel toe te voegen, zoals in de afbeelding hier.

Configureer één regel van Inside naar Outside zones (Outside1 en Outside2) die het geïnteresseerde verkeer van 10.10.10.0/24 naar 192.168.100/24 mogelijk maakt.

Configureer een andere regel van Outside zones (Outside1 en Outside 2) naar Inside, die het interessante verkeer van 192.168.100/24 naar 10.10.10.0/24 mogelijk maakt.



## ACP-FTDv

Enter Description

Rules Security Intelligence HTTP Responses Logging Advanced

Prefilter Policy: Default Prefilter

Filter by Device

Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicati...	Source Ports	Dest Ports	URLs	Source SGT
Mandatory - ACP-FTDv (1-2)												
1	VPN_1_out	Inside	Outside Outside2	10.10.10.0	192.168.100.	Any	Any	Any	Any	Any	Any	Any
2	VPN_1_in	Outside2 Outside	Inside	192.168.100.	10.10.10.0	Any	Any	Any	Any	Any	Any	Any

Default - ACP-FTDv (-)

There are no rules in this section. [Add Rule](#) or [Add Category](#)

Default Action

## ASA configureren

**Opmerking:** voor dit specifieke scenario is een back-uppeer geconfigureerd op de IKEv2 crypto-kaart, deze optie vereist dat de ASA op 9.14.1 of latere versies is ingesteld. Als uw ASA een oudere versie gebruikt, gebruikt u IKEv1 als tijdelijke oplossing. Ga voor meer informatie naar Cisco bug-id [CSCud22276](#).

1. IKEv2 inschakelen op de buiteninterface van de ASA:

```
Crypto ikev2 enable Outside
```

2. Maak het IKEv2-beleid dat dezelfde parameters definieert die op de FTD zijn geconfigureerd:

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

3. Maak een groepsbeleid om het ikev2 protocol toe te staan:

```
group-policy IKEV2 internal  
group-policy IKEV2 attributes
```

```
vpn-tunnel-protocol ikev2
```

4. Maak een tunnelgroep voor elk buitenste FTD IP-adres (Outside1 en Outside2). Verwijzing naar het groepsbeleid en specificeer de pre-gedeelde sleutel:

```
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. Maak een toegangslijst waarin het te versleutelen verkeer wordt gedefinieerd: (FTD-Subnet 10.10.10.0/24) (ASA-Subnet 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. Maak een ikev2 ipsec-voorstel om de algoritmen te verwijzen die op de FTD gespecificeerd zijn:

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

7. Maak een crypto map-ingang die de configuratie verbindt en voeg de Outside1 en Outside2 FTD IP-adressen toe:

```
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. Maak een NAT-vrijstellingsverklaring die voorkomt dat het VPN-verkeer door de firewall wordt genaturaliseerd:

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

## Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

### FTD

Gebruik in de opdrachtregel de opdracht **show crypto ikev2 sa** om de VPN-status te verifiëren.

---

**Opmerking:** VPN is ingesteld met het IP-adres van Outside1 (10.200.1.5) als lokaal.

---

```
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
```

### Route

De standaardroute toont het volgende-hop IP adres van Outside1.

```
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
```

## Spoor

Zoals te zien in de show track 1 uitvoer, "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

Het is nodig om het interessante verkeer te bevestigen raakt de NAT-vrijstellingsregel met de interface Outside1.

Gebruik de opdracht "Packet-tracer input Inside ICMP 10.10.1 8 0 192.168.100.10 detail" om de NAT-regel voor het interessante verkeer te controleren.

```
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

## failover uitvoeren

Dit voorbeeld, wordt de failover uitgevoerd door een sluiting op de Next hop van Outside1 die op de IP SLA monitorconfiguratie wordt gebruikt.

```
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:
```

## Route

De standaardroute gebruikt nu het volgende-hop IP adres van Outside2 en Reachability is 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
```

## Spoor

Zoals te zien in de **show track 1** output, "Reachability is Down" op dit punt.

```
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

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.