

# Configurazione del failover per i tunnel IPsec da sito a sito con collegamenti ISP di backup su FTD Gestiti da FMC

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurare l'FTD](#)

[Passaggio 1. Definizione delle interfacce ISP primaria e secondaria](#)

[Passaggio 2. Definire la topologia VPN per l'interfaccia ISP primaria](#)

[Passaggio 3. Definizione della topologia VPN per l'interfaccia ISP secondaria](#)

[Passaggio 4. Configurare il monitor SLA](#)

[Passaggio 5. Configurare le route statiche con il monitor SLA](#)

[Passaggio 6. Configurare l'esenzione NAT](#)

[Passaggio 7. Configurare i criteri di controllo di accesso per il traffico interessato](#)

[Configurazione dell'ASA](#)

[Verifica](#)

[FTD](#)

[Percorso](#)

[Brano](#)

[NAT](#)

[Esegui failover](#)

[Percorso](#)

[Brano](#)

[NAT](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritto come configurare il failover basato su mappa crittografica per il collegamento ISP con la funzione di tracciamento dello SLA IP sull'FTD gestito da FMC.

Contributo di Amanda Nava, Cisco TAC Engineer.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di una rete VPN (Virtual Private Network)

- Esperienza con FTD
- Esperienza con FMC
- Esperienza con la riga di comando di Adaptive Security Appliance (ASA)

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- FMC versione 6.6.0
- FTD versione 6.6.0
- ASA versione 9.14.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse

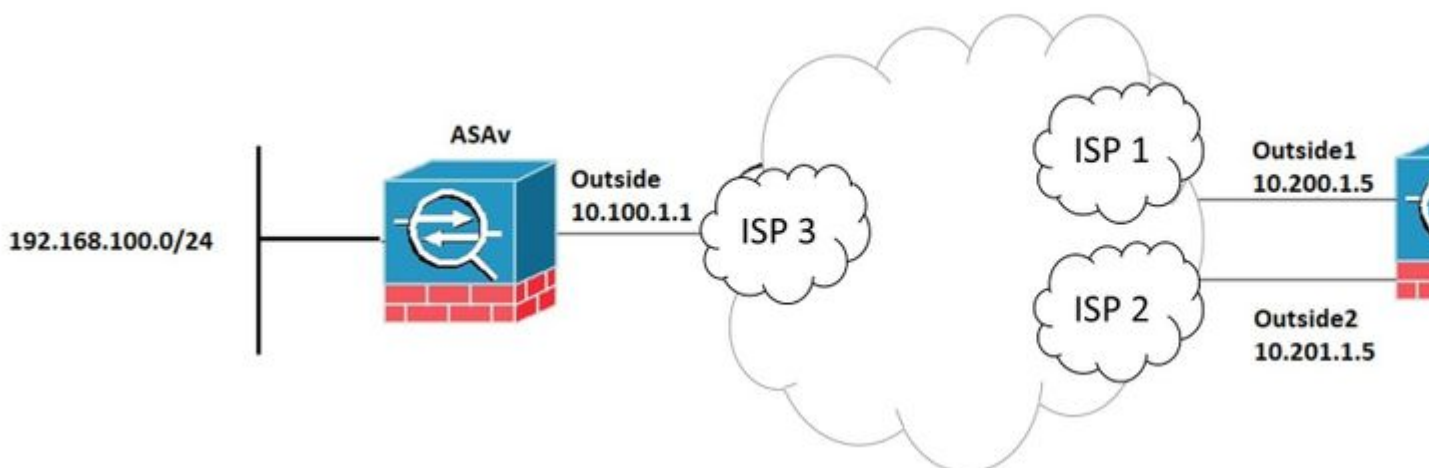
In questo documento viene descritto come configurare il failover basato su mappa crittografica per il collegamento del provider di servizi Internet (ISP) di backup con la funzionalità di monitoraggio IP SLA (Internet Protocol Service Level Agreement) su Firepower Threat Defense (FTD) gestito da Firepower Management Center (FMC). Spiega anche come configurare l'esenzione NAT (Network Address Translation) per il traffico VPN quando sono presenti due ISP e richiede un failover perfetto.

In questo scenario, la VPN viene stabilita dal FTD verso l'ASA come peer VPN con una sola interfaccia ISP. L'FTD utilizza un collegamento ISP in quel momento per stabilire la VPN. Quando il collegamento dell'ISP principale diventa inattivo, l'FTD subentra al collegamento dell'ISP secondario tramite il monitor SLA e la VPN viene stabilita.

## Configurazione

### Esempio di rete

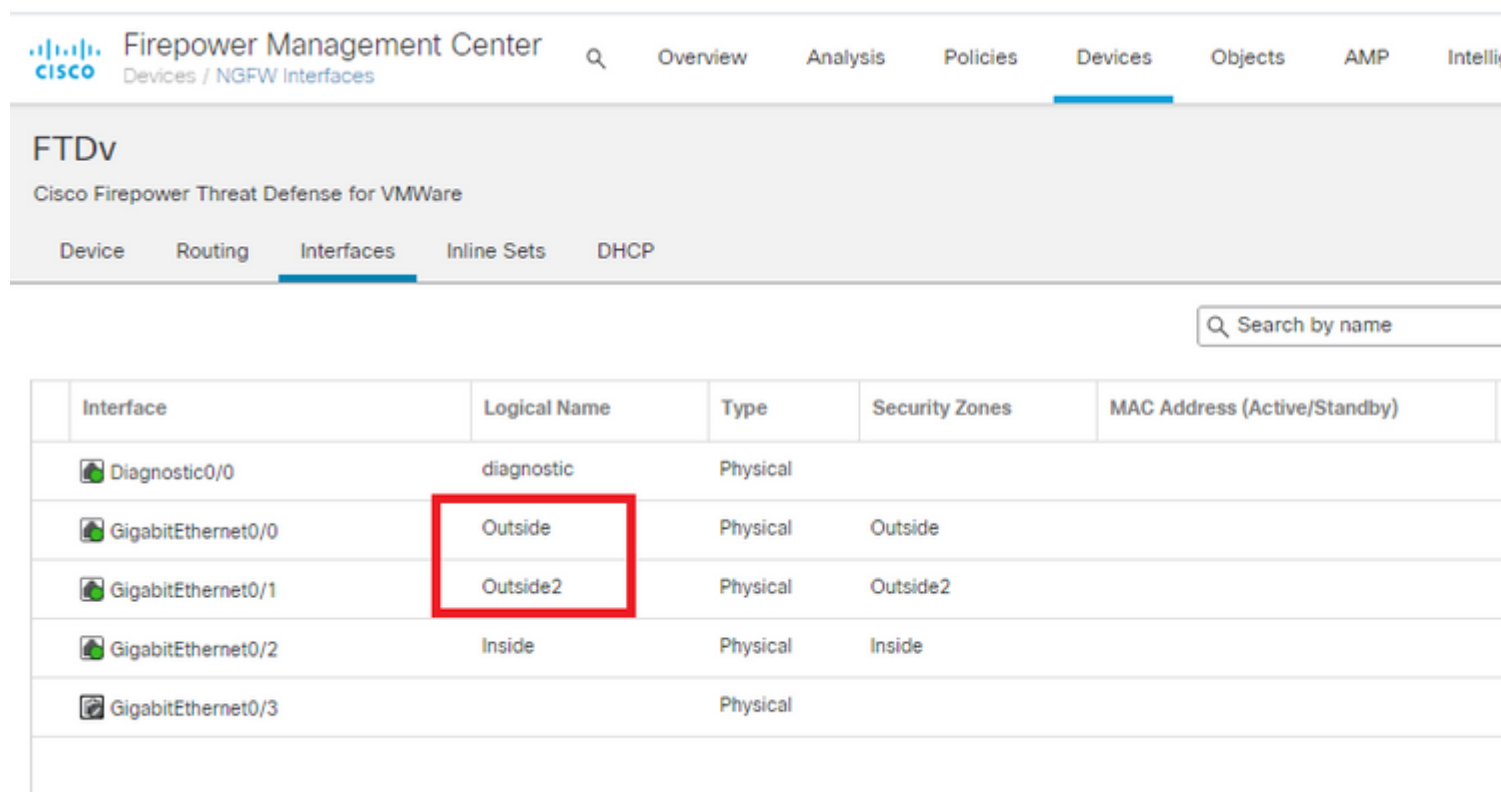
Questa è la topologia usata nell'esempio in questo documento:



## Configurare l'FTD

## Passaggio 1. Definizione delle interfacce ISP primaria e secondaria

1. Passare a **Dispositivi** > **Gestione dispositivi** > **Interfacce** come mostrato nell'immagine.



The screenshot shows the Cisco Firepower Management Center interface for FTDv. The 'Interfaces' tab is selected. A search bar is present with the text 'Search by name'. Below the search bar is a table with the following columns: Interface, Logical Name, Type, Security Zones, and MAC Address (Active/Standby). The table contains the following rows:

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		

## Passaggio 2. Definire la topologia VPN per l'interfaccia ISP primaria

1. Passare a **Dispositivi** > **VPN** > **Sito - Sito**. In **Aggiungi VPN**, fare clic su **Firepower Threat Defense Device**, creare la VPN e selezionare l'interfaccia esterna.

**Nota:** questo documento non descrive come configurare una VPN da sito a sito da zero. Per ulteriori riferimenti alla configurazione della VPN da sito a sito su FTD, visitare il sito <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.

### Passaggio 3. Definizione della topologia VPN per l'interfaccia ISP secondaria

1. Passare a **Dispositivi > VPN > Sito - Sito**. In **Add VPN**, fare clic su **Firepower Threat Defense Device**, creare la VPN e selezionare l'interfaccia Outside2.

---

**Nota:** la configurazione VPN che utilizza l'interfaccia Outside2 deve essere esattamente uguale alla topologia della VPN esterna, ad eccezione dell'interfaccia VPN.

---

### 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.

Le topologie VPN devono essere configurate come mostrato nell'immagine.

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

#### Passaggio 4. Configurare il monitor SLA

1. Passare a **Oggetti > Monitoraggio contratto di servizio > Aggiungi monitoraggio contratto di servizio**. In **Aggiungi VPN**, fare clic su **Firepower Threat Defense Device** e configurare il monitor SLA come mostrato nell'immagine.

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. Per il campo **SLA Monitor ID\*** utilizzare l'indirizzo IP esterno dell'hop successivo.

**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


### Passaggio 5. Configurare le route statiche con il monitor SLA

1. Passare a **Dispositivi > Ciclo > Instradamento statico**. Selezionare **Aggiungi instradamento** e configurare il instradamento predefinito per l'interfaccia esterna (principale) con le informazioni di monitoraggio del contratto di servizio (create al passaggio 4) nel campo **Instradamento**.

**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

any-ipv4 

Gateway\*  
10.200.1.1 +

Metric:  
1  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
ISP\_Outside1 +


2. Configurare il percorso predefinito per l'interfaccia esterna 2 (secondaria). Il valore della metrica deve essere maggiore della route primaria predefinita. In questa sezione non è necessario un campo **Tracciamento percorso**.




### 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

Add

any-ipv4

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

Gateway\*  
10.201.1.1 +

Metric:  
2  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
+

Cancel OK

Le route devono essere configurate come mostrato nell'immagine.



## 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				

### Passaggio 6. Configurare l'esenzione NAT

1. Passare a **Dispositivi** > **NAT** > **Criterio NAT** e selezionare il Criterio che ha come destinazione il dispositivo FTD. **Selezionare Add Rule** (Aggiungi regola) e configurare un'esenzione NAT per interfaccia ISP (Esterna e Esterna2). Le regole NAT devono essere le stesse ad eccezione dell'interfaccia di destinazione.

Firepower Management Center  
Devices / NGFW NAT Policy Editor

Overview Analysis Policies **Devices** Objects AMP Intelligence

NAT\_FTDv  
Enter Description

Rules

[Filter by Device](#)

#	Direction	Type	Source Interface	Destination Interface	Original Packet			Translated	
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated 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									

**Nota:** per questo scenario, entrambe le regole NAT richiedono l'abilitazione **della ricerca di route**. In caso contrario, il traffico supererebbe la prima regola e non si manterrebbe sulle route di failover. Se la ricerca route non è abilitata, il traffico verrà sempre inviato con l'utilizzo della (prima regola NAT) interfaccia esterna. Se la funzione **Ricerca route** è abilitata, il traffico si mantiene sempre nella tabella di routing controllata tramite il monitor SLA.

## Passaggio 7. Configurare i criteri di controllo di accesso per il traffico interessato

1. Passare a **Criteri > Controllo di accesso > Selezionare il criterio di controllo di accesso**. Per aggiungere una regola, fare clic su **Aggiungi regola**, come mostrato nell'immagine.

Configurare una regola da All'interno a All'esterno delle zone (Esterno 1 ed Esterno 2) che consenta il traffico interessato dalla porta 10.10.10.0/24 a 192.168.100.24.

Configurare un'altra regola dalle aree esterne (Esterne 1 e Esterne 2) a All'interno che consente il traffico interessante da 192.168.100.24 a 10.10.10.0/24.

Firepower Management Center Policies / Access Control / Firewall Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence

## 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	192.168.100.0	Any	Any	Any	Any	Any	Any	Any
2	VPN_1_in	Outside2 Outside	Inside	192.168.100.0	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

## Configurazione dell'ASA

**Nota:** per questo scenario specifico, sulla mappa crittografica IKEv2 è configurato un peer di backup. Per questa funzione, l'ASA deve essere nella versione 9.14.1 o successive. Se sull'appliance ASA è in esecuzione una versione precedente, usare il protocollo IKEv1 per risolvere il problema. Per ulteriori informazioni, fare riferimento all'ID bug Cisco [CSCud2276](#).

1. Abilitare IKEv2 sull'interfaccia esterna dell'appliance ASA:

```
Crypto ikev2 enable Outside
```

2. Creare il criterio IKEv2 che definisce gli stessi parametri configurati nell'FTD:

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

3. Creare un criterio di gruppo per consentire il protocollo ikev2:

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

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

4. Creare un gruppo di tunnel per ciascun indirizzo IP FTD esterno (Esterno1 e Esterno2). Fare riferimento ai criteri di gruppo e specificare la chiave già condivisa:

```
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. Creare un elenco degli accessi che definisca il traffico da crittografare: (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. Creare una proposta ipsec ikev2 per fare riferimento agli algoritmi specificati nell'FTD:

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

7. Creare una voce della mappa crittografica che colleghi la configurazione e aggiungere gli indirizzi IP FTD Esterno1 e Esterno2:

```
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. Creare un'istruzione di esenzione NAT che impedisca al traffico VPN di essere NATTED dal firewall:

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

## Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

## FTD

Nella riga di comando, utilizzare il comando **show crypto ikev2 sa** per verificare lo stato della VPN.

---

**Nota:** la VPN viene stabilita con l'indirizzo IP di Outside1 (10.200.1.5) come locale.

---

```
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
```

## Percorso

Il percorso predefinito mostra l'indirizzo IP dell'hop successivo di 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
```

## Brano

Come si vede nell'output show track 1, "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

È necessario confermare che il traffico interessante raggiunge la regola di esenzione NAT con l'interfaccia Outside1.

Utilizzare il comando "packet-tracer input Inside icmp 10.10.10.1 8 0 192.168.100.10 detail" per verificare la regola NAT applicata per il traffico interessante.

```
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
```

## Esegui failover

Nell'esempio, il failover viene eseguito da un arresto dell'hop successivo esterno1 utilizzato nella configurazione del monitoraggio dello SLA IP.

```
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:
```

## Percorso

Il percorso predefinito ora utilizza l'indirizzo IP dell'hop successivo di Outside2 e Reachability è 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
```

## Branco

Come mostrato nell'output del **show track 1**, a questo punto "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

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).