

Configuración de Failover para Túneles IPSec de Sitio a Sitio con Links ISP de Respaldo en FTD Administrado por FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuración del FTD](#)

[Paso 1. Definir las interfaces ISP principal y secundaria](#)

[Paso 2. Defina la topología VPN para la interfaz ISP principal](#)

[Paso 3. Defina la topología VPN para la interfaz ISP secundaria](#)

[Paso 4. Configuración del monitor de SLA](#)

[Paso 5. Configure las rutas estáticas con el Monitor de SLA](#)

[Paso 6. Configuración de la exención de NAT](#)

[Paso 7. Configuración de la política de control de acceso para el tráfico interesante](#)

[Configuración del ASA](#)

[Verificación](#)

[FTD](#)

[Ruta](#)

[Seguimiento](#)

[NAT](#)

[Realizar conmutación por fallo](#)

[Ruta](#)

[Seguimiento](#)

[NAT](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar la conmutación por fallas basada en mapas criptográficos para el link ISP con la función de seguimiento de SLA IP en el FTD administrado por FMC.

Colaboración de Amanda Nava, ingeniera del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Comprensión básica de una red privada virtual (VPN)

- Experiencia con FTD
- Experiencia con FMC
- Experiencia con la línea de comandos del dispositivo de seguridad adaptable (ASA)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- FMC versión 6.6.0
- FTD versión 6.6.0
- ASA versión 9.14.1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

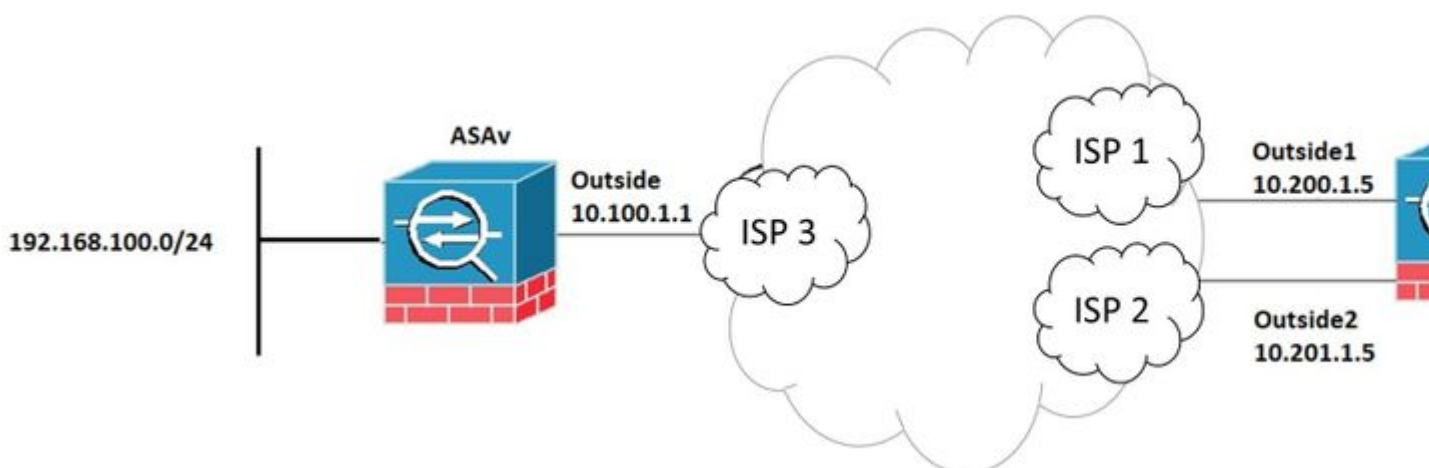
Este documento describe cómo configurar la conmutación por error basada en mapas criptográficos para el enlace de reserva del Proveedor de servicios de Internet (ISP) con la función de seguimiento del Acuerdo de nivel de servicio de protocolo de Internet (IP SLA) en Firepower Threat Defence (FTD) gestionado por Firepower Management Center (FMC). También explica cómo configurar la exención de la traducción de direcciones de red (NAT) para el tráfico VPN cuando hay dos ISP y requiere una conmutación por fallo perfecta.

En este escenario, la VPN se establece desde el FTD hacia el ASA como el peer VPN con una sola interfaz ISP. El FTD utiliza un enlace ISP en ese momento para establecer la VPN. Cuando el link ISP primario deja de funcionar, el FTD toma el control con el link ISP secundario a través del Monitor SLA y se establece la VPN.

Configurar

Diagrama de la red

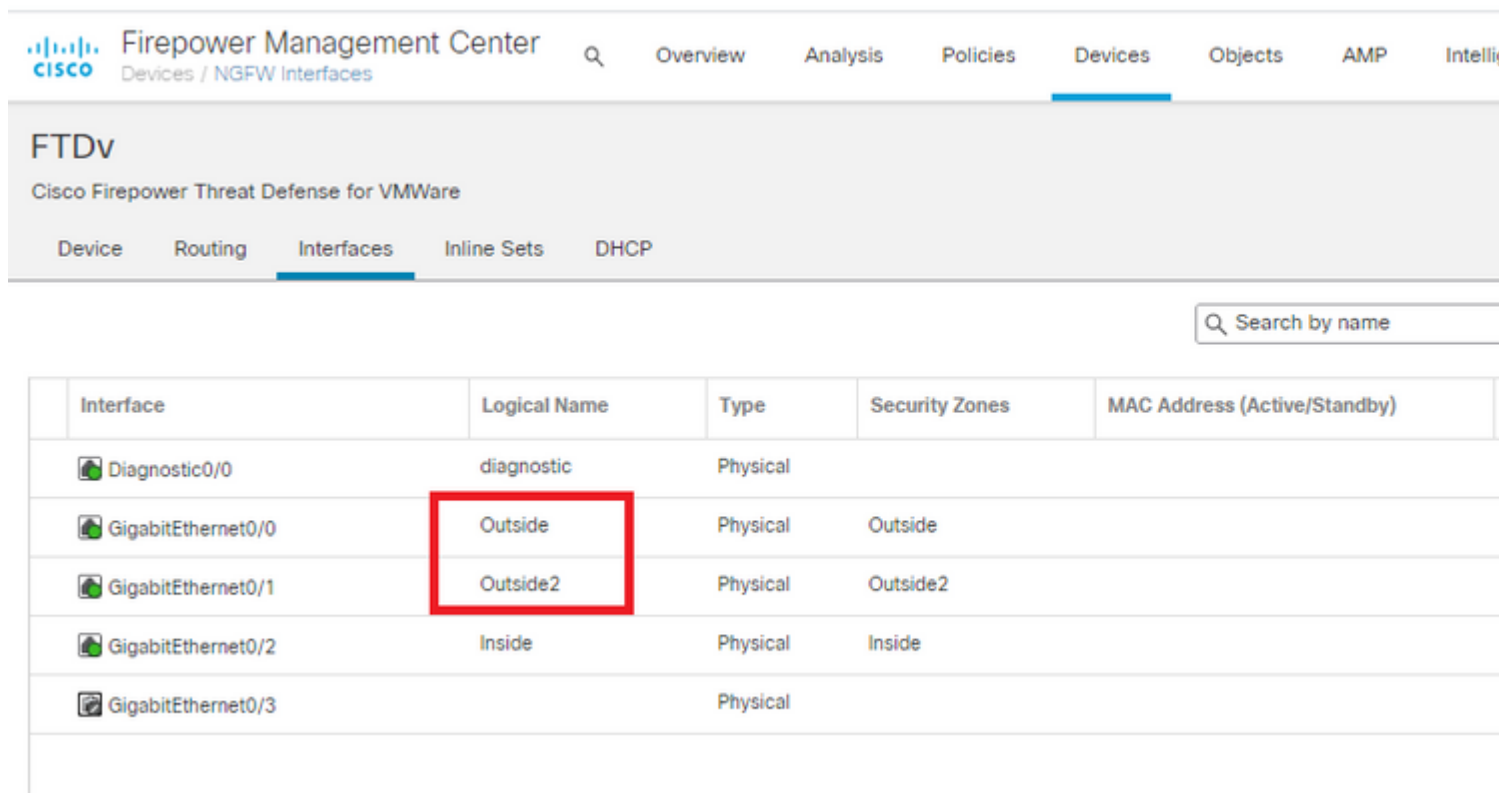
Esta es la topología utilizada para el ejemplo a lo largo de este documento:



Configuración del FTD

Paso 1. Definir las interfaces ISP principal y secundaria

1. Navegue hasta **Devices > Device Management > Interfaces** como se muestra en la imagen.



Firepower Management Center
Devices / NGFW Interfaces

Overview Analysis Policies Devices Objects AMP Intelli

FTDv
Cisco Firepower Threat Defense for VMWare

Device Routing Interfaces Inline Sets DHCP

Search by name

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		

Paso 2. Defina la topología VPN para la interfaz ISP principal

1. Vaya a **Dispositivos > VPN > Sitio a sitio**. En **Add VPN**, haga clic en **Firepower Threat Defence Device**, cree la VPN y seleccione la interfaz externa.

Nota: Este documento no describe cómo configurar una VPN S2S desde cero. Para obtener más información sobre la configuración de VPN S2S en FTD, visite <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:*
VPN_Outside1

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.

Paso 3. Defina la topología VPN para la interfaz ISP secundaria

1. Vaya a **Dispositivos > VPN > Sitio a sitio**. En **Add VPN**, haga clic en **Firepower Threat Defence Device**, cree la VPN y seleccione la interfaz Outside2.

Nota: La configuración VPN que utiliza la interfaz Outside2 debe ser exactamente la misma que la topología de VPN externa, excepto para la interfaz VPN.

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.

Las topologías VPN deben configurarse tal como se muestra en la imagen.

Firepower Management Center
 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

Paso 4. Configuración del monitor de SLA

1. Vaya a **Objetos > Monitor SLA > Agregar Monitor SLA**. En **Add VPN**, haga clic en **Firepower Threat Defence Device** y configure el monitor de SLA como se muestra en la imagen.

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
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. Para el campo **SLA Monitor ID***, utilice la dirección IP de siguiente salto externa.

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

Paso 5. Configure las rutas estáticas con el Monitor de SLA

1. Vaya a **Dispositivos > Enrutamiento > Ruta estática**. Seleccione **Add Route** y configure la ruta predeterminada para la interfaz externa (principal) con la información de monitoreo de SLA (Creado en el paso 4) en el campo **Route tracking**.

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. Configure la ruta por defecto para la interfaz Outside2 (secundaria). El valor de la métrica debe ser superior a la ruta predeterminada principal. En esta sección no se necesita ningún campo de **seguimiento de rutas**.

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

Las rutas deben configurarse tal como se muestra en la imagen.



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				

Paso 6. Configuración de la exención de NAT

1. Navegue hasta **Devices > NAT > NAT Policy** y seleccione la política que se dirige al dispositivo FTD. **Seleccione Add Rule** y configure una exención de NAT por interfaz ISP (Outside and Outside2). Las reglas NAT deben ser las mismas, excepto para la interfaz de destino.



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: Para este escenario, ambas reglas NAT requieren que se habilite **Route-lookup**. De lo contrario, el tráfico llegaría a la primera regla y no se mantendría en las rutas de conmutación por fallas. Si la búsqueda de rutas no está habilitada, el tráfico siempre se enviaría con el uso de la interfaz externa (primera regla NAT). Con **Route-lookup** habilitado, el tráfico siempre se mantiene en la tabla de ruteo que se controla a través del Monitor de SLA.

Paso 7. Configuración de la política de control de acceso para el tráfico interesante

1. Vaya a **Políticas > Control de acceso > Seleccione la Política de control de acceso**. Para agregar una regla, haga clic en **Add Rule**, como se muestra en la imagen.

Configure una regla desde las zonas internas a las externas (Outside1 y Outside2) que permita el tráfico interesado desde 10.10.10.0/24 a 192.168.100.24.

Configure otra regla de las zonas externas (Outside1 y Outside 2) a las internas que permita el tráfico interesante de 192.168.100.24 a 10.10.10.24.



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

Configuración del ASA

Nota: Para este escenario específico, se configura un par de respaldo en el mapa criptográfico IKEv2, esta función requiere que el ASA esté en la versión 9.14.1 o posterior. Si su ASA está ejecutando una versión anterior, utilice IKEv1 como solución alternativa. Para obtener más información, consulte la identificación de error de Cisco [CSCud22276](#).

1. Habilite IKEv2 en la interfaz externa del ASA:

```
Crypto ikev2 enable Outside
```

2. Cree la política IKEv2 que define los mismos parámetros configurados en el FTD:

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

3. Cree una política de grupo para permitir el protocolo ikev2:

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

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

4. Cree un grupo de túneles para cada dirección IP de FTD exterior (Outside1 y Outside2). Haga referencia a la política de grupo y especifique la clave previamente compartida:

```
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. Cree una lista de acceso que defina el tráfico que se va a cifrar: (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. Cree una propuesta ikev2 ipsec para hacer referencia a los algoritmos especificados en el FTD:

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

7. Cree una entrada de mapa criptográfico que una la configuración y agregue las direcciones IP de FTD Outside1 y Outside2:

```
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. Cree una declaración de exención de NAT que evite que el firewall NATTED el tráfico VPN:

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

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

FTD

En la línea de comandos, utilice el comando **show crypto ikev2 sa** para verificar el estado de VPN.

Nota: VPN se establece con la dirección IP de Outside1 (10.200.1.5) como local.

```
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
```

Ruta

La ruta predeterminada muestra la dirección IP del siguiente salto de 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
```

Seguimiento

Como se puede ver en el resultado de 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

Es necesario confirmar que el tráfico interesante llega a la regla de exención de NAT con la interfaz Outside1.

Utilice el comando "packet-tracer input Inside icmp 10.10.10.1 8 0 192.168.100.10 detail" para verificar la regla NAT aplicada para el tráfico interesante.

```
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
```

Realizar conmutación por fallo

Para este ejemplo, la conmutación por fallas se realiza mediante un apagado en el siguiente salto de Outside1 utilizado en la configuración del monitor de IP SLA.

```
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:
```

Ruta

La ruta predeterminada ahora utiliza la dirección IP de siguiente salto de Outside2 y el alcance es inactivo.

```
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
```

Seguimiento

Como se ve en el resultado de **show track 1**, "Reachability is Down" en este punto.

```
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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).