# Configuración de la conmutación por fallo ISP dual para FTD gestionado por FMC

# Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Antecedentes
Descripción General de la Función Static Route Tracking
Configurar
Diagrama de la red
Configuraciones
Verificación
Información Relacionada

# Introducción

Este documento describe cómo configurar la conmutación por fallas de ISP DUAL con PBR y IP SLAs en un FTD administrado por FMC.

# Prerequisites

## Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Routing basado en políticas (PBR)
- Acuerdo de nivel de servicio de protocolo de Internet (IP SLA)
- Centro de administración Firepower (FMC)
- Firepower Threat Defense (FTD)

### **Componentes Utilizados**

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FMCv 7.3.0
- FTDv 7.3.0

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

## Descripción General de la Función Static Route Tracking

La función de seguimiento de ruta estática permite que el FTD utilice una conexión con un ISP secundario en el caso de que la línea arrendada principal deje de estar disponible. Para lograr esta redundancia, el FTD asocia una ruta estática con un destino de monitoreo que usted defina. La operación SSLA supervisa el destino con solicitudes de eco ICMP periódicas.

Si no se recibe una respuesta de eco, el objeto se considera desactivado y la ruta asociada se elimina de la tabla de routing. Una ruta de respaldo previamente configurada se utiliza en lugar de la ruta que se quita. Mientras la ruta de respaldo está en uso, la operación de monitoreo de SLA continúa con sus intentos de alcanzar el destino de monitoreo.

Una vez que el objetivo esté disponible otra vez, la primera ruta se substituye en la tabla de ruteo, y se quita la ruta de respaldo.

Ahora puede configurar múltiples saltos siguientes y acciones de reenvío de ruteo basadas en políticas al mismo tiempo. Cuando el tráfico coincide con los criterios de la ruta, el sistema intenta reenviar el tráfico a las direcciones IP en el orden especificado, hasta que tenga éxito.

La función está disponible en los dispositivos FTD que ejecutan la versión 7.1 y posteriores gestionados por un FMC versión 7.3 y posteriores.

# Configurar

Diagrama de la red

Esta imagen proporciona un ejemplo de un diagrama de red.



Imagen 1. Ejemplo de diagrama.

ISP1 = 10.115.117.1

ISP2 = 172.20.20.13

## Configuraciones

Paso 1. Configure los objetos de monitoreo de SLA.

En el FMC, navegue hastaObject > Object Management > SLA Monitor > Add SLA Monitory agregue un objeto de supervisión de SLA para las direcciones IP del ISP.

Monitor de SLA para el gateway predeterminado principal (ISP1).

Name:	_	Description:
SALI		
Frequency (seconds):		SLA Monitor ID*:
60		1
(1-604800)		
Threshold (milliseconds):		Timeout (milliseconds):
5000		5000
(0-60000)		(0-604800000)
Data Size (bytes):		ToS:
28		0
(0-16384)		
Number of Packets:		Monitor Address*:
1		10.115.117.1
Available Zones 📿	_	
Q Search		Selected Zones/Interfaces
Backbone	Add	Outside 🗑
Backup		
new		
Outside		
VLAN2816		
	_	

Imagen 2. Ventana de configuración del monitor SLA1.

## Monitor de SLA para el gateway predeterminado secundario (ISP2).

Name:		Description:
SLA2		
Frequency (seconds):		SLA Monitor ID*:
60		2
(1-604800)		
Threshold (milliseconds):		Timeout (milliseconds):
5000		5000
(0-60000)		(0-604800000)
Data Size (bytes):		ToS:
28		0
(0-16384)		
Number of Packets:		Monitor Address*:
1		172.20.20.13
Available Zones 📿		
Q Search		Selected Zones/Interfaces
Backbone	Add	Backup
васкир		
new		
Outside		
VLAN2816		

#### Paso 2. Configure las Rutas Estáticas con Route Track.

En el FMC, navegue hastaDevice > Device Management > Edit the desired FTD > Routing > Static Routesy agregue las rutas estáticas con el monitor de SLA correcto.

El monitor SLA debe ser el que monitoree el gateway predeterminado.

Ruta estática para el gateway predeterminado principal:

Edit Static Route Configuration		0
Type:  IPv4 IPv6 Interface* Interface (Interface starting with this icon Signifies it is a Available Network C	vailable for route leak)	
Q. Search       Add         10.10.10.1       10.117.0.250         10.34.24.91       172.16.0.20         172.20.20.13       192.168.1.20	any-ipv4	Ĩ
Ensure that egress virtualrouter has route to that a Gateway          I0.115.117.1       •       +         Metric:       •       +         I       •       •         (1 - 254)       •       •         Tunneled:       (Used only for default Route)         Route Tracking:       •       +	destination	

Imagen 4. Ventana de configuración de ruta estática para la interfaz externa.

Ruta estática para el gateway predeterminado secundario.

Edit Static Route Configuration	0
Type:      IPv4      IPv6	
Interface*	
backup 🔻	
(Interface starting with this icon signifies it is available for route leak)	
Available Network C + Selected Network	
Q Search Add any-ipv4	Ť
10.10.10.1	
10.117.0.250	
10.34.24.91	
172.16.0.20	
172.20.20.13	
192.168.1.20	
Ensure that egress virtualrouter has route to that destination	
Gateway	
172.20.20.13 • +	
Metric:	
254	
(1 - 254)	
Tunneled: Used only for default Route)	
Route Tracking:	
SLA2 • +	

Imagen 5. Ventana de configuración de ruta estática para la interfaz de copia de seguridad.

#### Paso 3. Configure las Rutas Base de Políticas.

Desplácese hastaDevice > Device Management > Edit the desired FTD > Routing > Policy Based Routing, agregar el PBR y elija la interfaz de ingreso.

Firewall Manageme Devices / Secure Firewall Re	nt Center Overview	Analysis Policies Devices Objects Integration	Deploy Q 🚱 🌣 🕢 admin - 🔤
FTDb-osmontoy Cisco Firepower Threat Defense for	or VMWare		You have unsaved changes Save Cancel
Device Routing Interfa	ces Inline Sets DHCP	TEP	
Manage Virtual Routers	Policy Based Routing	Add Policy Based Route	
Global 👻	Specify ingress interfaces, match	A policy based route consists of ingress interface list and a set of match criteria associated to egress interfaces	Configure Interface Priority Add
Virtual Router Properties ECMP	Ingress Interfaces	Ingress Interface*	
BFD			
OSPF		Specify forward action for chosen match criteria.	
OSPFv3			
EIGRP			
RIP			
Policy Based Routing			
<ul> <li>BOP</li> <li>IDut</li> </ul>			
IPv6		There are no forward, actions defined ust. Start hy defining the first one	
Static Route		There are no to ward-actions demined yet, stark by demand the maxime.	
Multicast Routing			
IGMP			
PIM			
Multicast Routes		Cancel Save	
Multicast Boundary Filter			

Imagen 6. Ventana de configuración PBR.

#### Configure las acciones de reenvío.

- Elija o agregue una nueva lista de control de acceso con la que desee establecer una coincidencia.
- ElijaIP Addressuna de lasSend toopciones.
- En este ejemplo, 10.115.117.234 es la dirección IP externa de FTD.

Edit Forwarding	Actions		0
Match ACL:*	all_ipv4_for_pbr v		^
Send To:*	IP Address 🗸		
IPv4 Addresses:	10.115.117.234		
IPv6 Addresses:	For example, 2001:db8::, 2002:db8::1:		
Don't Fragment:	None		
Default Interfac	e	•	
IPv4 settings	IPv6 settings		
Recursive:	For example, 192.168.0.1		- 1
Default:	For example, 192.168.0.1, 10.10.10.1		
Peer Address			
Verify Availability		+	-
		Cancel	ve

Imagen 7. Ventana de configuración de acciones de reenvío.

Desplácese hacia abajo y agregue los Verify Availability valores para ISP1.

Edit Forwardin	g Actions		Ø
Default Interface	ce		·
IPv4 settings	IPv6 settings		
Recursive:	For example, 192.168.0.1		
Default:	For example, 192.168.0.1, 10.10.10.1		
Peer Address			
Verify Availability			+
IP Address:	Sequence:	Track:	
10.115.117.1	1	1	/ 1
			Ţ
			Cancel Save

Imagen 8. Ventana de configuración de acciones de reenvío.

Repita el mismo proceso para la interfaz de copia de seguridad. Sin embargo, asegúrese de utilizar un objeto de lista de control de acceso diferente.

Edit Forwarding	Actions		0
Match ACL:*	internal_networks v +		<b>^</b>
Send To:*	IP Address 🗸		- 1
IPv4 Addresses:	172.20.20.77		- 1
IPv6 Addresses:	For example, 2001:db8::, 2002:db8::1:		- 1
Don't Fragment:	None		- 1
Default Interface			- 1
IPv4 settings	IPv6 settings		- 1
Recursive:	For example, 192.168.0.1		- 1
Default:	For example, 192.168.0.1, 10.10.10.1		
Peer Address			
Verify Availability		+	-
		Cancel	Save

Imagen 9. Ventana de configuración de acciones de reenvío

## Repita el mismo proceso paraverify Availabilityla configuración pero ahora para ISP2.

Edit Forwarding	g Actions		Ø
Default Interfac	ce		·
IPv4 settings	IPv6 settings		
Recursive:	For example, 192.168.0.1		
Default:	For example, 192.168.0.1, 10.10.10.1		
Peer Address			
Verify Availability			+
IP Address:	Sequence:	Track:	
172.20.20.13	2	2	/1
			Cancel Save

Imagen 10. Verificar configuración de disponibilidad.

#### Valide su configuración.

Firewall Managemer Devices / Secure Firewall Roo	nt Center uting	Overview	Analysis	Policies	Devices	Objects	Integration			Deploy	۹ (	<b>\$</b> \$ \$	admi	in ~   1	isco SECURE
FTDb-osmontoy Cisco Firepower Threat Defense for Device Routing Interface	VMWare es Inline Sets	DHCP	VTEP												Cancel
Manage Virtual Routers	Policy Base Specify ingress i	d Routing nterfaces, mat	tch criteria and	egress interfa	ces to route tr	raffic accordir	gly. Traffic can be rout	ted across Egress interfac	es accordingly			Configure	Interface Pr	riority	Add
Virtual Router Properties	Ingress Interfac	es			Ma	tch criteria and	forward action								
BFD	vlan2816				if tr	affic matches th	e Access List		Send through						11
OSPF					all,	.ipv4_for_pbr			10.115.117.234						
OSPFv3					If to	affic matches th	e Access List		Send through						
EIGRP					inte	ernal_network:			172.20.20.77						
RIP															
Policy Based Routing															

Imagen 11. Configuración PBR.

## Verificación

Acceda al FTD a través de Secure Shell (SSH) y utilice el comandosystem support disagnotsic-cliy ejecute estos comandos:

• show route-map: Este comando muestra la configuración de route-map.

#### <#root>

firepower#

show route-map

route-map FMC\_GENERATED\_PBR\_1679065711925

, permit, sequence 5
Match clauses:
ip address (access-lists): internal\_networks

Set clauses: ip next-hop verify-availability 10.115.117.1 1

track 1 [up]

```
ip next-hop 10.115.117.234
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
Match clauses:
ip address (access-lists): all_ipv4_for_pbr
```

Set clauses: ip next-hop verify-availability 172.20.20.13 2

track 2 [up]

ip next-hop 172.20.20.77
firepower#

• show running-config sla monitor: Este comando muestra la configuración de SLA.

#### <#root>

firepower#

show running-config sla monitor

sla monitor 1

type echo protocol ipIcmpEcho 10.115.117.1 interface outside sla monitor schedule 1 life forever start-time now

sla monitor 2

```
type echo protocol ipIcmpEcho 172.20.20.13 interface backup
sla monitor schedule 2 life forever start-time now
firepower#
```

• show sla monitor configuration: Este comando muestra los valores de configuración de SLA.

#### <#root>

firepower#

show sla monitor configuration

SA Agent, Infrastructure Engine-II Entry number:

1

```
Owner:
Tag:
Type of operation to perform: echo
```

```
Target address: 10.115.117.1
```

Interface: outside
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:

Entry number:

2

Owner: Tag: Type of operation to perform: echo

Target address: 172.20.20.13

Interface: backup 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:

• show sla monitor operational-state: Este comando muestra el estado operativo de la operación SLA.

#### <#root>

firepower#

show sla monitor operational-state

Entry number: 1

Modification time: 15:48:04.332 UTC Fri Mar 17 2023 Number of Octets Used by this Entry: 2056 Number of operations attempted: 74 Number of operations skipped: 0 Current seconds left in Life: Forever

Operational state of entry: Active

Last time this entry was reset: Never Connection loss occurred: FALSE Timeout occurred: FALSE Over thresholds occurred: FALSE Latest RTT (milliseconds): 1 Latest operation start time: 17:01:04.334 UTC Fri Mar 17 2023 Latest operation return code: OK RTT Values: RTTAvg: 1 RTTMin: 1 RTTMax: 1 NumOfRTT: 1 RTTSum: 1 RTTSum2: 1 Entry number: 2

Modification time: 15:48:04.335 UTC Fri Mar 17 2023 Number of Octets Used by this Entry: 2056 Number of operations attempted: 74 Number of operations skipped: 0 Current seconds left in Life: Forever

Operational state of entry: Active

Last time this entry was reset: Never Connection loss occurred: FALSE Timeout occurred: FALSE Over thresholds occurred: FALSE Latest RTT (milliseconds): 1 Latest operation start time: 17:01:04.337 UTC Fri Mar 17 2023 Latest operation return code: OK RTT Values: RTTAvg: 1 RTTMin: 1 RTTMax: 1 NumOfRTT: 1 RTTSum: 1 RTTSum2: 1

 show track: Este comando muestra la información sobre los objetos de los que realiza un seguimiento el proceso de seguimiento de SLA.

<#root>

firepower#

show track

Track 1

Response Time Reporter 1 reachability

Reachability is Up

```
4 changes, last change 00:53:42
Latest operation return code: OK
Latest RTT (millisecs) 1
Tracked by:
ROUTE-MAP 0
STATIC-IP-ROUTING 0
```

Track 2

Response Time Reporter 2 reachability

Reachability is Up

2 changes, last change 01:13:41 Latest operation return code: OK Latest RTT (millisecs) 1 • show running-config route: Este comando muestra la configuración de ruta actual.

#### <#root>

firepower#

show running-config route

route

outside

 $0.0.0.0 \ 0.0.0.0 \ 10.115.117.1 \ 1$ 

track 1

route

backup

0.0.0.0 0.0.0.0 172.20.20.13 254

track 2

route vlan2816 10.42.0.37 255.255.255.255 10.43.0.1 254 firepower#

• show route: Este comando muestra la tabla de ruteo para las interfaces de datos.

<#root>

firepower#

show 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, BI - BGP InterVRF
Gateway of last resort is 10.115.117.1 to network 0.0.00
```

S\* 0.0.0.0 0.0.0.0 [1/0] via 10.115.117.1, outside

S 10.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone C 10.88.243.0 255.255.255.0 is directly connected, backbone L 10.88.243.67 255.255.255.0 is directly connected, backbone C 10.115.117.0 255.255.255.0 is directly connected, outside L 10.115.117.234 255.255.255.255 is directly connected, outside C 10.42.0.0 255.255.255.0 is directly connected, vlan2816 L 10.42.0.1 255.255.255.255 is directly connected, vlan2816 S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816 C 172.20.20.0 255.255.255.0 is directly connected, backup L 172.20.20.77 255.255.255 is directly connected, backup

Cuando falla el link principal:

• show route-map: Este comando muestra la configuración de route-map cuando falla un link.

#### <#root>

firepower#

show route-map FMC\_GENERATED\_PBR\_1679065711925

route-map FMC\_GENERATED\_PBR\_1679065711925, permit, sequence 5
Match clauses:
ip address (access-lists): internal\_networks

Set clauses: ip next-hop verify-availability 10.115.117.1 1

track 1 [down]

```
ip next-hop 10.115.117.234
route-map FMC_GENERATED_PBR_1679065711925, permit, sequence 10
Match clauses:
ip address (access-lists): all_ipv4_for_pbr
```

Set clauses: ip next-hop verify-availability 172.20.20.13 2

track 2 [up]

ip next-hop 172.20.20.77
firepower#

• show route: Este comando muestra la nueva tabla de ruteo por interfaz.

<#root>

firepower#

show 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, BI - BGP InterVRF
Gateway of last resort is 10.115.117.1 to network 0.0.00
```

s\* 0.0.0.0 0.0.0.0 [1/0] via 172.20.20.13, backup

```
S 10.0.0 255.0.0.0 [1/0] via 10.88.243.1, backbone
C 10.88.243.0 255.255.255.0 is directly connected, backbone
L 10.88.243.67 255.255.255.0 is directly connected, backbone
C 10.115.117.0 255.255.255.0 is directly connected, outside
L 10.115.117.234 255.255.255.255 is directly connected, outside
C 10.42.0.0 255.255.255.0 is directly connected, vlan2816
L 10.42.0.1 255.255.255.255 is directly connected, vlan2816
S 10.42.0.37 255.255.255.255 [254/0] via 10.43.0.1, vlan2816
C 172.20.20.0 255.255.255.0 is directly connected, backup
L 172.20.20.77 255.255.255.255 is directly connected, backup
```

## Información Relacionada

- Guía de administración de Cisco Secure Firewall Management Center, 7.3
- Soporte Técnico y Documentación Cisco Systems

#### 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).