# Configuración de rutas estáticas con Firewall Management Center (FMC)

# Contenido

troducción	
erequisites	
Requirements	
Componentes Utilizados	
ntecedentes	
onfigurar	
Configuraciones	
erificación	

# Introducción

Este documento describe el proceso de implementación de rutas estáticas en Secure Firewall Threat Defense mediante Firewall Management Center.

# Prerequisites

#### Requirements

Cisco recomienda tener conocimiento de estos temas:

- Centro de gestión de firewall (FMC)
- Firewall seguro Threat Defence (FTD)
- Fundamentos de rutas de red.

#### **Componentes Utilizados**

La información de este documento se basa en estas versiones de software y hardware:

- Firewall Management Center para VMWare v7.3
- Cisco Secure Firewall Threat Defence para VMWare v7.3

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 procedimiento es compatible con los dispositivos:

- Firewall Management Center in situ
- Centro de gestión de firewall para VMWare
- cdFMC
- Dispositivos Cisco Secure Firewall serie 1000
- Dispositivos Cisco Secure Firewall serie 2100
- Dispositivos Cisco Secure Firewall serie 3100
- Dispositivos Cisco Secure Firewall serie 4100
- Dispositivos Cisco Secure Firewall serie 4200
- Dispositivo Cisco Secure Firewall 9300
- Cisco Secure Firewall Threat Defence para VMWare

# Configurar

Configuraciones

Paso 1. En la GUI de FMC , vaya a Devices > Device Management .

Paso 2. Identifique el FTD que se va a configurar y haga clic en el icono del lápiz para editar la configuración actual del FTD.

Firewall Management Center Overview Analysis	Policies Devices Obje	ects Integra	ition		Deploy 🔍 💞 🐇	🗘 🔕 admin 🔹 🤤	6.4b. SECURE
View By: Group •						Deploym	ent History
All (1) • Error (0) • Warning (0) • Offline (0) • Normal (1)	<ul> <li>Deployment Pending (0)</li> </ul>	Upgrade (0)	<ul> <li>Snort 3 (1)</li> </ul>		a	& Search Device	Add 💌
Collagse All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (1)							
172.16.0.41 Snort 3     172.16.0.41 - Routed	FTDv for VMware	7.3.0	N/A	Essentials, IPS (2 more)	recreates_policy	\$P	1

Paso 2. Haga clic en la ficha Routing.

Firewall Management Center Devices / Secure Firewall Interfaces	Overview Analysis	Policies	Devices Objects	Integration		Deploy Q 🎸	🕨 🔅 🚳 admin 🔹 🦿	Inde SECURE
172.16.0.41 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Set	s DHCP VTEP							Cancel
					[	Q. Search by name	Sync Device Add	Interfaces +
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Diagnostic0/0	diagnostic	Physical				Disabled	Global	/
GigabitEthernet0/0	inside	Physical	inside		2.2.2.1/24(Static)	Disabled	Global	/
GigabitEthernet0/1	outside	Physical	outside		172.16.0.60/24(Static)	Disabled	Global	/
GigabitEthernet0/2		Physical				Disabled		/
GigabitEthernet0/3		Physical				Disabled		/
GigabitEthernet0/4		Physical				Disabled		/
GigabitEthernet0/5		Physical				Disabled		/
GigabitEthernet0/6		Physical				Disabled		/
					Displaying 1-8 of I	8 interfaces IC < Page 1	of	1 > >⊨ C

Paso 3. En el menú de la izquierda seleccione Static Route

Firewall Management Devices / Secure Firewall Routing	Center Overview	Analysis Policies Devi	ces Objects Integration			Deploy C	२ 🗳 🛊 (	admin • secure
172.16.0.41 Cisco Firepower Threat Defense for V	Mware							Save Cancel
Device Routing Interfaces	Inline Sets DHCP V	VTEP						
Manage Virtual Routers								+ Add Route
Global 👻	Network +	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
Virtual Router Properties	▼ IPv4 Routes							
ECMP								
BFD	▼ IPv6 Routes							
OSPF-0								
EIGRP								
RIP								
Policy Based Routing								
∼ BGP								
IPv4								
IPv6								
V Multicast Routing								
IGMP								
PIM								
Multicast Routes								
Multicast Boundary Filter								
General Settings								
ROP					No data to disp	stay IC I Page 1		of 1 > > C

Paso 4. haga clic en la opción (+) Agregar ruta.

Firewall Management Devices / Secure Firewall Rout	t Center Overview	Analysis Policies Devic	es Objects Integration			Deploy C	🕻 🥝 🔅 🕲 admin 🕶 讨 🖏 St	ECURE
172.16.0.41 Cisco Firepower Threat Defense for	/Mware	тғр					Save	Cancel
terite neurong interiore								_
Manage Virtual Routers							+ Add Rou	ute
Global 👻	Network *	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
Virtual Router Properties	▼ IPv4 Routes							
ECMP								
BFD	▼ IPv6 Routes							
OSPF								
OSPFv3								
EIGRP								
KIP Dalicu Parad Dautina								
Policy based Routing								
iPv4								
IPv6								
Static Route								
✓ Multicast Routing								
IGMP								
PIM								
Multicast Routes								
Multicast Boundary Filter								
General Settings								
BGP					No data to disg	lay IC < Page 1	of 1 > >I <	e -

Paso 5. En la sección Configuración de ruta estática, introduzca la información necesaria en los campos Tipo, Interfaz, Red disponible, Puerta de enlace y Métrica (así como Tunelizado y Seguimiento de ruta si es necesario).

Tipo: Haga clic en IPv4o IPv6 en función del tipo de ruta estática que esté agregando. Interfaz: Elija la interfaz a la que se aplica esta ruta estática.

Red disponible: en la lista Red disponible, elija la red de destino. Para definir una ruta por defecto, cree un objeto con la dirección 0.0.0/0 y selecciónelo aquí.

Gateway: En el campo Gateway o IPv6 Gateway, ingrese o elija el router de gateway que es el siguiente salto para esta ruta. Puede proporcionar una dirección IP o un objeto Networks/Hosts. Métrica: En el campo Métrica, introduzca el número de saltos a la red de destino. Los valores válidos oscilan entre 1 y 255; el valor predeterminado es 1.

Tunelizada: (Opcional) Para una ruta predeterminada, haga clic en la casilla de verificación Tunelizada para definir una ruta predeterminada independiente para el tráfico VPN

Seguimiento de rutas: (solo ruta estática IPv4) Para supervisar la disponibilidad de rutas,

introduzca o seleccione el nombre de un objeto Monitor de SLA (acuerdo de nivel de servicio) que defina la política de supervisión en el campo Seguimiento de rutas.

Firewall Management Devices / Secure Firewall Routi	t Center Overview	Analysis Policies	Devices Objects Integration	Deploy Q 🚱 🌣 🔕 admin v 👘 secure
172.16.0.41 Cisco Firepower Threat Defense for V Device Routing Interfaces	/Mware s Inline Sets DHCP	VTEP	Add Static Route Configuration	Save Carcel
Device Routing Interfaces Manage Virtual Routers Global Virtual Router Properties ECMP BFD OSPF OSPF OSPF EGRP RIP Policy Based Routing VBP IPv4 IPv6 Static Route VMulticast Routing IGMP PM Multicast Routes Multicast Routes Multicast Routes Multicast Routes	Network 4 Vetwork 4 Vetwork 5 Vetwork 7 Vetwork 7	Interface	Type:       ● IPv4       ● IPv6         Interface*       outside       •         (Interface starting with this icon @signifies it is available for route leak)       Available Network C*       +         Available Network C*       +       Selected Network         10.203.18.100       •       +         10.203.18.101       •       +         10.203.18.104       •       •         128.231.210.0-26       •       •         128.231.210.0-26       •       •         128.231.210.0-26       •       •         128.231.210.0-26       •       •         128.231.210.0-26       •       •         128.231.210.0-26       •       •         128.231.210.0-26       •       •         128.231.210.0-26       •       •         128.231.210.0-26       •       •         10.203.18.100       •       +         Metric:       •       •         1       •       •         1       •       •         1       •       •         1       •       •         1       •       •         1       •       • <t< td=""><td>+ Add Route</td></t<>	+ Add Route
General Settings BGP			Cancel OK	ata to display IC I > > C



Sugerencia: Los campos de red disponible, gateway y tráfico de ruta requieren el uso de objetos de red. Si los objetos aún no se han creado, haga clic en el signo (+) situado a la derecha de cada campo para crear un nuevo objeto de red.

Paso 6. Haga clic en Aceptar

Paso 7. Guarde la configuración y valide la nueva ruta estática que se muestra como se esperaba.

Firewall Management Devices / Secure Firewall Routin	Center Overview	Analysis Policies Devic	es Objects Integration			Deploy	୦. 🗳 🌣 🙆 admin •   -;	see SECURE
172.16.0.41						Y	ou have unsaved changes Save	Cancel
Cisco Firepower Threat Defense for VI	Mware							
Device Routing Interfaces	Inline Sets DHCP V	TEP						
Manage Virtual Routers							+ /	dd Route
Global 🔻	Network *	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked	
Virtual Router Properties	▼ IPv4 Routes							
ECMP	10.203.18.0	outside	Global	10.203.18.100	false	1		11
BFD	► IPv6 Routes							
OSPF COSPF.								
FIGRP								
RIP								
Policy Based Routing								
∼ BGP								
IPv4								
IPv6								
Static Route								
<ul> <li>Multicast Routing</li> </ul>								
PIM								
Multicast Routes								
Multicast Boundary Filter								
General Settings					Displaying 1-1 of 1 n	ows IC < Page 1	of 1 >	н с
BGP								

Paso 7. Navegue hasta Desplegar y marque el FTD seleccionado en el Paso 2 y, a continuación, haga clic en el icono de despliegue azul para desplegar la nueva configuración.

Firewall Management Devices / Secure Firewall Routing	Center Overview	Analysis Policies Devic	ces Objects Integration				🚱 🌣 🕲 admin 🔹 讨 🐯 SECURE
172.16.0.41 Cisco Firepower Threat Defense for V	Mware					Q 172.16.0.41	Advanced Deploy Deploy neel
Device Routing Interfaces	Inline Sets DHCP V	TEP					1
Manage Virtual Routers							
Global 🔻	Network *	Interface	Leaked from Virtual Router	Gateway	Tunnel		
Virtual Router Properties	▼ IPv4 Routes						
ECMP	10.203.18.0	outside	Global	10.203.18.100	false		1
OSPF	► IPv6 Routes						
OSPFv3						1 selected   O 1 pending	20
EIGRP							
RIP							
Policy Based Routing							
IPv4							
IPv6							
Static Route							
V Multicast Routing							
IGMP							
Multicast Routes							
Multicast Boundary Filter							
General Settings						Displaying 1-1 of 1 rows I < Page 1	of 1 > > C
BGP							

Paso 8. Validar que la implementación se muestre como completada.

Firewall Management Devices / Secure Firewall Rout	Center Overview	Analysis Policies Devic	es Objects Integration			Deploy Q	😵 🌣 🞯 admin 🕶 🖓 🖏 SECURE
172.16.0.41 Cisco Firepower Threat Defense for V Device Routing Interfaces	'Mware s Inline Sets DHCP V	TEP				Q. 172.16.0.41	Advanced Deploy Deploy All cel Completed
Manage Virtual Routers							
Global 👻	Network +	Interface	Leaked from Virtual Router	Gateway	Tunnel		
Virtual Router Properties	▼ IPv4 Routes						
ECMP	10.203.18.0	outside	Global	10.203.18.100	false		
OSPF	▼ IPv6 Routes						
OSPFv3						O 1 succeeded	2 +9
EIGRP							
RIP Dalieu Rased Dauties							
~ BGP							
IPv4							
IPv6							
Static Route							
V Multicast Routing							
PIM							
Multicast Routes							
Multicast Boundary Filter							
General Settings						Displaying 1-1 of 1 rows	of 1 >>> C
RGP							

# Verificación

1. Registre mediante SSH, Telnet o la consola el FTD previamente implementado.

2. Ejecute el comando show route y show running-config route

3. Valide que la tabla de routing de FTD tenga ahora la ruta estática desplegada con el indicador S y que también se muestre en la configuración en ejecución.

```
> show route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, 0 - 0SPF, IA - 0SPF inter area
N1 - 0SPF NSSA external type 1, N2 - 0SPF NSSA external type 2
E1 - 0SPF external type 1, E2 - 0SPF 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 - 0DR, P - periodic downloaded static route, + - replicated route
SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is not set
C 2.2.2.0 255.255.255.0 is directly connected, inside
1.0.203.18.0 255.255.255.0 [1/0] via 10.203.18.100, outside
1.72.16.0.0 255.255.255.255 is directly connected, outside
L 172.16.0.60 255.255.255.255 is directly connected, outside
```

```
> show running-config route
route outside 10.203.18.0 255.255.255.0 10.203.18.100 1
>
```

#### 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).