Configurare route statiche con Centro gestione firewall

Sommario	
Introduzione	
Prerequisiti	
Requisiti	
<u>Componenti usati</u>	
Premesse	
<u>Configurazione</u>	
Configurazioni	
<u>Verifica</u>	

Introduzione

In questo documento viene descritto il processo di distribuzione delle route statiche in Secure Firewall Threat Defense tramite Centro gestione firewall.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Centro gestione firewall
- Secure Firewall Threat Defense (FTD)
- · Concetti fondamentali dei percorsi di rete.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software e hardware:

- Firewall Management Center per VMWare v7.3
- Cisco Secure Firewall Threat Defense per VMWare v7.3

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

Questa procedura è supportata sugli accessori:

- Centro gestione firewall locale
- Centro gestione firewall per VMWare
- CdFMC
- Appliance Cisco Secure Firewall serie 1000
- Appliance Cisco Secure Firewall serie 2100
- Appliance Cisco Secure Firewall serie 3100
- Appliance Cisco Secure Firewall serie 4100
- Appliance Cisco Secure Firewall serie 4200
- Appliance Cisco Secure Firewall 9300
- Cisco Secure Firewall Threat Defense per VMWare

Configurazione

Configurazioni

Passaggio 1. Nell'interfaccia utente di FMC, selezionare Devices > Device Management (Dispositivi > Gestione dispositivi).

Passaggio 2. Identificare l'FTD da configurare e fare clic sull'icona a forma di matita per modificare la configurazione corrente dell'FTD.

Firewall Management Center Overview Analysis	Policies Devices Objec	ts Integra	tion		Deploy Q 🗳 🕻	> 🛛 admin • 🔤	diade SECURE
View By: Group •						Deploym	ent History
All (1) • Error (0) • Warning (0) • Offline (0) • Normal (1)	 Deployment Pending (0) 	Upgrade (0)	 Snort 3 (1) 		٩	Search Device	Add 👻
Collaose All							
Name Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (1)							
0 172.16.0.41 Snort 3 172.16.0.41 - Routed	FTDv for VMware	7.3.0	N/A	Essentials, IPS (2 more)	recreates_policy	49	1

Passaggio 2. Fare clic sulla scheda Instradamento.

Firewall Management Center Devices / Secure Firewall Interfaces	Overview Analysis	Policies	Devices Objects	Integration		Deploy Q 🗳	🖗 🕸 admin 🕶	enco SECURE
172.16.0.41 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Set	ts DHCP VTEP							o Cancel
						Q. Search by name	Sync Device Ad	d Interfaces 🔻
Interface	Logical Name	Туре	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router	
Diagnostic0/0	diagnostic	Physical				Disabled	Global	1
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	8 interfaces 15 5 Page 1	Ja	f1 > >⊨ C

Passaggio 3. Nel menu a sinistra selezionare Static Route

Firewall Management Devices / Secure Firewall Routing	Center Overview	Analysis Policies Devic	es Objects Integration			Deploy C	२ 💣 🌣	admin dealer secure
172.16.0.41 Cisco Firepower Threat Defense for VI	Mware							Save Cancel
Device Routing Interfaces	Inline Sets DHCP V	/TEP						
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								
FIGRP								
RIP								
Policy Based Routing								
✓ BGP								
IPv4								
IPv6								
Static Route								
IGMP								
PIM								
Multicast Routes								
Multicast Boundary Filter								
General Settings								
ROD					No data to disp	Nay IC I Page 1		of 1 > > C

Passaggio 4. fare clic sull'opzione (+) Aggiungi route.

Firewall Management Devices / Secure Firewall Routing	Center Overview	Analysis Policies Devic	es Objects Integration			Deploy C	रे 🗳 🌣 🔞 ad	min • dude SECURE
172.16.0.41 Cisco Firepower Threat Defense for V Device Routing Interfaces	Mware Inline Sets DHCP V	/TEP						Save Cancel
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								
OSPFV3 FIGDD								
RIP								
Policy Based Routing								
∼ BGP								
IPv4								
IPv6								
Static Route								
 Multicast Routing IGMP 								
PIM								
Multicast Routes								
Multicast Boundary Filter								
General Settings					No data to dire	aw K C Page 1		at s s c
RGP					NO GALA LO GISE	ual IV / LaAg		

Passaggio 5. Nella sezione Configurazione route statica immettere le informazioni richieste nei campi Tipo, Interfaccia, Rete disponibile, Gateway e Metrica (nonché Tunneled e Route Tracing se necessario).

Tipo: fare clic su IPv4o IPv6 a seconda del tipo di route statica che si sta aggiungendo.

Interfaccia: scegliere l'interfaccia a cui applicare la route statica.

Rete disponibile: nell'elenco Rete disponibile scegliere la rete di destinazione. Per definire una route predefinita, creare un oggetto con l'indirizzo 0.0.0.0/0 e selezionarlo qui.

Gateway: nel campo Gateway o Gateway IPv6, immettere o scegliere il router gateway che rappresenta l'hop successivo per la route. È possibile specificare un indirizzo IP o un oggetto Networks/Hosts.

Metrica: nel campo Metrica, immettere il numero di hop per la rete di destinazione. I valori validi sono compresi tra 1 e 255; il valore predefinito è 1.

Tunneled: (facoltativo) per un percorso predefinito, fare clic sulla casella di controllo Tunneled per definire un percorso predefinito separato per il traffico VPN

Tracciamento route: (solo route statica IPv4) Per monitorare la disponibilità della route, immettere o scegliere il nome di un oggetto di monitoraggio SLA (Service Level Agreement) che definisce il criterio di monitoraggio nel campo Tracciamento route.

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	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



Suggerimento: i campi Rete disponibile, Gateway e Traffico di routing richiedono l'uso di oggetti di rete. Se gli oggetti non sono stati ancora creati, fare clic sul segno (+) a destra di ciascun campo per creare un nuovo oggetto di rete.

Passaggio 6. Scegliere OK.

Passaggio 7. Salvare la configurazione e convalidare la nuova route statica visualizzata come previsto.

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								
 Multicast Routing 								
PIM								
Multicast Routes								
Multicast Boundary Filter								
General Settings					Displaying 1-1 of 1 n	ows IC < Page 1	of 1 >	н с
BGP								

Passaggio 7. Passare a Distribuisci e selezionare l'FTD selezionato nel passaggio 2, quindi fare clic sull'icona blu di distribuzione per distribuire la nuova configurazione.

Firewall Management Devices / Secure Firewall Routi	Center Overview	Analysis Policies Device	es Objects Integration				🚱 🌣 🔞 admin 🕶 🖓 🖓 SECURE
172.16.0.41 Cisco Firepower Threat Defense for V Device Routing Interfaces	Mware Inline Sets DHCP V	TEP			_	Q.	Advanced Deploy Deploy see
Manage Virtual Routers							
Global v	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						i selected V i pending	127 + 17
EIGRP							
RIP Policy Based Pouting							
~ BGP							
IPv4							
IPv6							
Static Route							
 Multicast Routing IGMP 							
PIM							
Multicast Routes							
Multicast Boundary Filter							
General Settings						Displaying 1-1 of 1 must 1/ / Dage 1	
BGP						Displaying Friderions (C Page 1	JIT 7 7 C

Passaggio 8. Verificare che la distribuzione sia visualizzata come completata.

Firewall Management Devices / Secure Firewall Routi	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 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	12 +9
EIGRP							
RIP							
Policy Based Routing							
IPv4							
IPv6							
Static Route							
V Multicast Routing							
IGMP							
PIM Multicast Routes							
Multicast Boundary Filter							
General Settings						Displaying 1-1 of 1 rows 14 4 Page	of 1 >> C
000							

Verifica

1. Eseguire il log con SSH, Telnet o console sull'FTD precedentemente implementato.

2. Eseguire il comando show route e show running-config route

3. Verificare che la tabella di routing FTD disponga ora della route statica distribuita con il flag S e che sia visualizzata anche nella configurazione in esecuzione.

```
> 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
10.203.18.0 255.255.255.0 [1/0] via 10.203.18.100, outside
172.16.0.60 255.255.255.255 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
>
```

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).