Konfigurieren statischer Routen mit Firewall Management Center (FMC)

Inhalt

Einleitung	
/oraussetzungen	
Anforderungen	
Verwendete Komponenten	
Hintergrundinformationen	
<u>Konfigurieren</u>	
Konfigurationen	
Überprüfung	

Einleitung

Dieses Dokument beschreibt den Prozess, wie statische Routen in Secure Firewall Threat Defense über das Firewall Management Center bereitgestellt werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, in den folgenden Bereichen über Kenntnisse zu verfügen:

- Firewall Management Center (FMC)
- Sicherer Firewall-Schutz vor Bedrohungen (FTD)
- Netzwerkrouten bilden die Grundlage.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Dieses Verfahren wird auf folgenden Appliances unterstützt:

- Firewall Management Center am Standort
- Firewall Management Center für VMware
- CdFMC
- Cisco Secure Firewall Appliances der Serie 1000
- Cisco Secure Firewall Appliances der Serie 2100
- Cisco Secure Firewall Appliances der Serie 3100
- Cisco Secure Firewall Appliances der Serie 4100
- Cisco Secure Firewall Appliances der Serie 4200
- Cisco Secure Firewall der Serie 9300
- Cisco Secure Firewall Threat Defense für VMware

Konfigurieren

Konfigurationen

Schritt 1: Navigieren Sie in der FMC-GUI zu Geräte > Geräteverwaltung.

Schritt 2: Identifizieren Sie das FTD, das konfiguriert werden soll, und klicken Sie auf das Bleistiftsymbol, um die aktuelle Konfiguration des FTD zu bearbeiten.

Firewall Management Center Overview Analysis	Policies Devices Obje	cts Integra	tion		Deploy Q 🚱 H	🜣 🛛 admin • 📩	SECURE
View By: Group •						Deployme	ent History
All (1) • Error (0) • Warning (0) • Offline (0) • Normal (1)	 Deployment Pending (0) 	Upgrade (0)	 Snort 3 (1) 		C	2, Search Device	Add 💌
Collagse All							
Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	
Ungrouped (1)							
	FTDv for VMware	7.3.0	N/A	Essentials, IPS (2 more)	recreates_policy	49	1

Schritt 2: Klicken Sie auf die Registerkarte Routing.

Firewall Management Center Devices / Secure Firewall Interfaces	Overview Analysis	Policies	Devices Objects	Integration		Deploy Q 🌖	🕈 😨 admin 🕶 🗄	ice SECURE
172.16.0.41 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Set	ts DHCP VTEP							Cancel
					Q. Set	arch by name	Sync Device Add In	nterfaces +
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 inter	faces IK IK Page 1	of 1	i > >l C

Schritt 3: Wählen Sie im Menü links die Option Static Route (Statische Route).

Firewall Management Devices / Secure Firewall Root	t Center Overview	Analysis Policies Devic	ces Objects Integration			Deploy	् 🗳 🔅 🕲 adm	nin • secure
172.16.0.41 Cisco Firepower Threat Defense for	VMware							Save Cancel
Device Routing Interface	s Inline Sets DHCP	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								
OSPFv3								
EIGRP								
KiP Doliny Reced Douting								
✓ BGP								
IPv4								
IPv6								
Static Route								
✓ Multicast Routing								
IGMP								
PIM								
Multicast Routes								
Multicast Boundary Filter								
General Settings					No dete to disc	in la c Dans 1		
RGP					ivo data to disp	nay is is Page		Juit 2 21 G

Schritt 4: Klicken Sie auf die Option (+) Route hinzufügen.

Firewall Management Devices / Secure Firewall Routi	Center Overview	Analysis Policies Devic	es Objects Integration			Deploy C	🕻 🗳 🍄 adr	min • dada SECURE
172.16.0.41 Cisco Firepower Threat Defense for V Device Routing Interfaces	Mware Inline Sets DHCP V	ТЕР						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								
FIGRP								
RIP								
Policy Based Routing								
✓ BGP								
IPv4								
IPv6								
Static Route								
IGMP								
PIM								
Multicast Routes								
Multicast Boundary Filter								
General Settings								
BGP					No data to disp	lay IC < Page 1		or 1 > > C

Schritt 5: Geben Sie im Abschnitt "Static Route Configuration" (Statische Routenkonfiguration) die erforderlichen Informationen in die Felder "Type" (Schnittstelle), "Available Network" (Verfügbares Netzwerk), "Gateway" (Gateway) und "Metric" (sowie bei Bedarf "Tunneled" und "Route Tracking" (Routenverfolgung) ein.

Typ: Klicken Sie je nach Art der statischen Route, die Sie hinzufügen, auf IPv4 oder IPv6. Schnittstelle: Wählen Sie die Schnittstelle aus, auf die diese statische Route angewendet wird. Available Network (Verfügbares Netzwerk): Wählen Sie in der Liste Available Network (Verfügbares Netzwerk) das Zielnetzwerk aus. Um eine Standardroute zu definieren, erstellen Sie ein Objekt mit der Adresse 0.0.0.0/0 und wählen es hier aus.

Gateway: Geben Sie im Feld Gateway or IPv6 Gateway (Gateway oder IPv6-Gateway) den Gateway-Router ein, der den nächsten Hop für diese Route darstellt, oder wählen Sie diesen aus. Sie können eine IP-Adresse oder ein Netzwerk-/Hosts-Objekt angeben.

Metrisch: Geben Sie im Feld "Metrisch" die Anzahl der Hops zum Zielnetzwerk ein. Gültige Werte liegen zwischen 1 und 255; der Standardwert ist 1.

Getunnelt: (Optional) Klicken Sie bei einer Standardroute auf das Kontrollkästchen Getunnelt, um eine separate Standardroute für VPN-Datenverkehr zu definieren.

Routenverfolgung: (Nur statische IPv4-Route) Geben Sie zum Überwachen der

Routenverfügbarkeit den Namen eines SLA-Objekts (Service Level Agreement), das die

Überwachungsrichtlinie definiert, in das Feld "Routenverfolgung" ein, oder wählen Sie diesen aus.

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



Tipp: Die Felder Available Network , Gateway und Route traffic erfordern die Verwendung von Netzwerkobjekten. Falls die Objekte noch nicht erstellt wurden, klicken Sie bitte auf das (+) Zeichen rechts von jedem Feld, um ein neues Netzwerkobjekt zu erstellen.

Schritt 6: Klicken Sie auf OK

Schritt 7. Speichern Sie die Konfiguration, und validieren Sie die neue statische Route, die wie erwartet angezeigt wird.

Firewall Management Devices / Secure Firewall Routin	Center Overview	Analysis Policies Devic	es Objects Integration			Deploy	익 🗳 🌣 🚳 admin 🔹 🗧	ste SECURE
172.16.0.41						Ye	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							
OSPFv3								
EIGRP								
RIP								
Policy Based Routing								
∼ BGP								
IPv4								
IPv6								
Static Route								
 Multicast Kouting 								
DIM								
Multicast Routes								
Multicast Boundary Filter								
General Settings					Displaying 1-1 of 1 n	ows IC IC Page	of 1 >	жe
BGP								· · ·

Schritt 7: Navigieren Sie zu Deploy (Bereitstellen), und aktivieren Sie das in Schritt 2 ausgewählte FTD, und klicken Sie dann auf das blaue Symbol "Deployment" (Bereitstellung), um die neue Konfiguration bereitzustellen.

Firewall Management Devices / Secure Firewall Routing	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 rcel
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
OSPE	► IPv6 Routes						
OSPFv3						1 selected of 1 pending	₽ 0
EIGRP							
RIP							
Policy Based Routing							
V BGP							
IPv6							
Static Route							
✓ Multicast Routing							
IGMP							
PIM							
Multicast Routes Multicast Roundary Eilter							
matocolic countrality r mon							
General Settings						Displaying 1-1 of 1 rows I < < Page 1	of 1 > > C
BGP							

Schritt 8: Überprüfen, ob die Bereitstellung als abgeschlossen angezeigt wird

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							

Überprüfung

1. Melden Sie sich mithilfe von SSH, Telnet oder der Konsole bei der zuvor bereitgestellten FTD an.

2. Führen Sie den Befehl show route und show running-config route aus

3. Überprüfen Sie, ob die FTD-Routing-Tabelle nun die bereitgestellte statische Route mit dem S-Flag enthält und in der aktuellen Konfiguration angezeigt wird.

```
> show route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, 0 - 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 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
172.16.0.0 255.255.255.255 is directly connected, outside
L 172.16.0.60 255.255.255 is directly connected, outside
```

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.