Bereitstellung von FireSIGHT Management Center auf VMware ESXi

Inhalt

Einführung Voraussetzungen Verwendete Komponenten Konfiguration Bereitstellen einer OVF-Vorlage Einschalten und vollständige Initialisierung Konfigurieren der Netzwerkeinstellungen Ersteinrichtung durchführen Zugehörige Informationen

Einführung

Dieses Dokument beschreibt die erste Einrichtung eines FireSIGHT Management Center (auch Defense Center genannt), das auf VMware ESXi ausgeführt wird. Mit einem FireSIGHT Management Center können Sie eine oder mehrere FirePOWER-Appliances, Next Generation Intrusion Prevention System (NGIPS) Virtual Appliances und Adaptive Security Appliance (ASA) mit FirePOWER-Services verwalten.

Hinweis: Dieses Dokument ist eine Ergänzung der FireSIGHT-Systeminstallationsanleitung und -anleitung. Eine ESXi-spezifische Frage zur Konfiguration und Fehlerbehebung finden Sie in der VMware Knowledge Base und in der Dokumentation.

Voraussetzungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Plattformen:

- Cisco FireSIGHT Management Center
- Virtuelle Cisco FireSIGHT Management Center-Appliance
- VMware ESXI 5.0

In diesem Dokument bezieht sich ein "Gerät" auf die folgenden Plattformen:

- Sourcefire FirePOWER Appliances der Serie 7000 und Appliances der Serie 8000
- Virtuelle Sourcefire NGIPS Appliances für VMware ESXi
- Cisco Serie ASA 5500-X mit FirePOWER-Service

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfiguration

Bereitstellen einer OVF-Vorlage

- 1. Laden Sie die **Cisco FireSIGHT Management Center Virtual Appliance** von der <u>Cisco</u> <u>Support & Downloads-</u>Website herunter.
- 2. Extrahieren Sie den Inhalt der Datei tar.gz in ein lokales Verzeichnis.
- 3. Stellen Sie über einen VMware vSphere-Client eine Verbindung zum ESXi-Server

🖉 VMv	ware vSphere Client	— ×
vmware ™ware vSphere Client		
To directly manage a singl To manage multiple hosts, vCenter Server.	e host, enter the IP address or ho enter the IP address or name of a	st name.
IP address / Name:		•
User name:		
Password:		
	Use Windows session creder	ntials Help

her.

4. Wenn Sie sich beim vSphere-Client angemeldet haben, wählen Sie **Datei > OVF-Vorlage**

Ć	2					
	File	Edit View Inventory	Adminis	tration	Plug-	ins Helj
		New	•	ntory	Þ 🗊	Inventory
		Deploy OVF Template				
		Export	Export +			
		Report •		localho	ost. VM	ware ES
		Browse VA Marketplace	Browse VA Marketplace		g Starte	d Sum
		Print Maps	Þ			
bereitstellen.		Exit				

5. Klicken Sie auf **Durchsuchen** und suchen Sie die Dateien, die Sie in Schritt 2 extrahiert haben. Wählen Sie die OVF-Datei Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf aus, und klicken Sie auf Weiter

V V CI		
0		Deploy OVF Template
5	Select the source location.	
	Source DVF Template Details Name and Location Datastore Disk Format Ready to Complete	Deploy from a file or URL C:\Temp\Sourcefire_Defense_Center_Virtual64_VMware-5.3 Browse Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.
	Help	< Back Next > Cancel

6. Klicken Sie im Bildschirm **OVF Template Details (OVF-Vorlagendetails**) auf **Next (Weiter)**, um die Standardeinstellungen zu übernehmen.

)	Deploy	y OVF Template		
OVF Template Details Verify OVF template details	5.			
Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	Product: Version: Vendor: Publisher: Download size: Size on disk: Description:	VirtualDC64 No certificate present 523.4 MB 1.4 GB (thin provisioned) 250.0 GB (thick provisioned) Sourcefire Defense Center Virtual64 Sourcefire Inc. 9770 Patuxent Woods Drive Columbia, MD 21046		
Help			< Back Next 3	> Cancel

7. Geben Sie einen Namen für das Management Center ein, und klicken Sie auf **Weiter**.

	Deploy OVF Template
Name and Location Specify a name and loc	ation for the deployed template
Source	Name:
Name and Location Datastore Disk Format Network Mapping Ready to Complete	The name can contain up to 80 characters and it must be unique within the inventory folder.

8. Wählen Sie einen **Datenspeicher aus**, auf dem Sie das virtuelle System erstellen möchten, und klicken Sie auf

Weiter.

Ø		Deplo	y OVF Temp	olate				
1	Datastore Where do you want to stor	e the virtual machine f	iles?					
	Source	Select a datastore in	which to store th	e VM files:				
	OVF Template Details Name and Location	Name	Capacity	Provisioned	Free	Туре	Thin Provisioning	Access
	Datastore	[datastore2]	1.29 TB	866.14 GB	469.36 GB	VMFS	Supported	Single
	Disk Format Network Mapping Ready to Complete	[datastore1]	459.75 GB	563.00 MB	459.20 GB	VMFS	Supported	Single >
	Help				< B	ack	Next > Ca	incel

9. Klicken Sie auf das Optionsfeld Thick provisioned format f
ür das Datenträgerformat und klicken Sie auf Weiter. Beim Thick Provisioning-Format wird der erforderliche Speicherplatz zum Zeitpunkt der Erstellung einer virtuellen Festplatte zugewiesen, w
ährend im Thin Provisioning-Format bedarfsgesteuert Speicherplatz belegt wird.

0	Deploy OVF Template
Disk Format In which format do you	want to store the virtual disks?
Source OVF Template Details Name and Location Datastore Disk Format Network Mapping Ready to Complete	Information about the selected datastore: Name: datastore2 Capacity: 1.3 TB Free space: 469.4 GB Select a format in which to store the virtual machines virtual disks: Thin provisioned format The storage is allocated on demand as data is written to the virtual disks. This is supported only on VMFS3 and newer datastores. Other types of datastores might create thick disks. Estimated disk usage: 1.4 GB Thick provisioned format All storage is allocated immediately. Estimated disk usage: 250.0 GB
Help	< Back Next > Cancel

10. Ordnen Sie im Abschnitt **Netzwerkzuordnung** die Verwaltungsschnittstelle des FireSIGHT Management Center einem VMware-Netzwerk zu, und klicken Sie auf **Weiter**.

0		Deploy OVF Templa	te	
I	Network Mapping What networks should the	deployed template use?		
	Source OVF Template Details Name and Location	Map the networks used in this OVF ter	nplate to networks in your inventory	
	Datastore	Source Networks	Destination Networks	
	<u>Disk Format</u>	Management	VM Network	•
	Ready to Complete		VM Network VM Network 2	
		Description:		
		The Management network		^ _
		,		

1						_
Help			< Back	Next >	Cancel	
						1
	6 - 1 1 1					

11. Klicken Sie auf **Fertig stellen**, um die OVF-Vorlagenbereitstellung abzuschließen.



Einschalten und vollständige Initialisierung

 Navigieren Sie zum neu erstellten virtuellen System. Klicken Sie mit der rechten Maustaste auf den Servernamen, und wählen Sie Power > Power On (Ein) aus, um den Server zum ersten Mal zu starten.



2. Navigieren Sie zum Register Konsole, um die Serverkonsole zu überwachen. Das LILO-Startmenü wird

angezeigt.		
VirtualDC64		
Getting Started Summary Res	ource Allocation Performance Events Console Permissions	
	LILO 22.8 Boot Menu	
	3D-5.3.0	
	Hit any key to cancel timeout $00:00$ Use $\uparrow\uparrow\downarrow\rightarrow$ arrow keys to make selection Enter choice & options, hit CR to boot	
boot: Loading 3D-5.3.0		

Sobald die BIOS-Datenüberprüfung erfolgreich war, wird der Initialisierungsprozess gestartet. Der erste Start kann zusätzliche Zeit in Anspruch nehmen, da die Konfigurationsdatenbank zum ersten Mal initialisiert wird.

```
Firstboot detected, executing scripts
Executing S03install-math-pari.sh
                                                                       E
                                                                          OK
                                                                               ]
                                                                               ]
                                                                       E
                                                                          OK
Executing S04async_syslog_dc.sh
                                                                       E
                                                                               ]
Executing S04fix-httpd.sh
                                                                          OK
                                                                       l
                                                                               ]
Executing S05set-MgMnt-port
                                                                          OK
                                                                               ]
                                                                       E
                                                                          OK
Executing S06addusers
                                                                       E
                                                                          OK
                                                                               ]
Executing S07uuid-init
                                                                       ſ
                                                                          OK
                                                                               ]
Executing S09configure_mysql
************ Attention ********
   Initializing the configuration database.
                                              Depending on available
   system resources (CPU, memory, and disk), this may take 30 minutes
   or more to complete.
************ Attention ********
Executing S10database
```

Wenn Sie den Vorgang abgeschlossen haben, sehen Sie möglicherweise die Meldung Kein solches

Gerät.

```
Copyright (c) 1999-2010 Intel Corporation.
Silicom Bypass-SD Control driver v5.0.39.5
No such device
```

3. Drücken Sie die Eingabetaste, um eine Anmeldeaufforderung

abzurufen.

```
Copyright (c) 1999-2010 Intel Corporation.
Silicom Bypass-SD Control driver v5.0.39.5
No such device
Sourcefire Virtual Defense Center 64bit v5.3.0 (build 571)
Sourcefire3D login: _
```

Hinweis: Die Meldung "SCHREIBEN SIE DAS GLEICHE MAL. Manuelles Zeroing." kann angezeigt werden, nachdem das System zum ersten Mal gestartet wurde. Dies weist nicht auf einen Defekt hin, sondern weist richtig darauf hin, dass der VMware-Storage-Treiber den Befehl WRITE SAME nicht unterstützt. Das System zeigt diese Meldung an und fährt mit einem Fallback-Befehl fort, um denselben Vorgang auszuführen.

Konfigurieren der Netzwerkeinstellungen

- Melden Sie sich bei der Sourcefire3D-Anmeldeaufforderung mit diesen Anmeldeinformationen an: Für Version 5.xBenutzername: AdministratorKennwort: SourcefireFür Version 6.x und höherBenutzername: AdministratorKennwort: Administrator123Tipp: Sie können das Standardkennwort bei der Ersteinrichtung in der GUI ändern.
- 2. Die Erstkonfiguration des Netzwerks erfolgt mithilfe eines Skripts. Sie müssen das Skript als root-Benutzer ausführen. Um zum root-Benutzer zu wechseln, geben Sie den Befehl sudo su zusammen mit dem Kennwort Sourcefire oder Admin123 (für 6.x) ein. Seien Sie vorsichtig, wenn Sie bei der Management Center-Befehlszeile als Stammbenutzer angemeldet sind. admin@Sourcefire3D:~\$ sudo su Password:
- 3. Um mit der Netzwerkkonfiguration zu beginnen, geben Sie das Skript **configure-network** als root ein.

```
root@Sourcefire3D:~# configure-network
Do you wish to configure IPv4? (y or n) y
```

Sie werden aufgefordert, eine Management-IP-Adresse, eine Netzmaske und ein Standard-Gateway anzugeben. Sobald Sie die Einstellungen bestätigen, wird der Netzwerkdienst neu gestartet. Als Ergebnis wird die Management-Schnittstelle deaktiviert und kehrt dann wieder zurück.

```
Do you wish to configure IPv4? (y or n) y
Management IP address? [192.168.45.45] 192.0.2.2
Management netmask? [255.255.255.0]
Management default gateway? 192.0.2.1
Management IP address?
                              192.0.2.2
Management netmask?
                               255.255.255.0
Management default gateway?
                              192.0.2.1
Are these settings correct? (y or n) y
Do you wish to configure IPv6? (y or n) n
e1000: eth0: e1000_watchdog_task: NIC Link is Up 1000 Mbps Full Duplex, Flow Con
trol: None
ADDRCONF(NETDEV_UP): eth0: link is not ready
ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
Updated network configuration.
Updated comms. channel configuration.
Please go to https://192.0.2.2/ or https://[]/ to finish installation.
root@Sourcefire3D:~# _
```

Ersteinrichtung durchführen

- Öffnen Sie nach der Konfiguration der Netzwerkeinstellungen einen Webbrowser, und navigieren Sie über HTTPS zur konfigurierten IP (<u>https://192.0.2.2</u> in diesem Beispiel). Wenn Sie dazu aufgefordert werden, authentifizieren Sie das SSL-Standardzertifikat. Verwenden Sie diese Anmeldeinformationen, um sich anzumelden:Für Version 5.x Benutzername: AdministratorKennwort: SourcefireFür Version 6.x und höherBenutzername: AdministratorKennwort: Administrator123
- 2. Auf dem folgenden Bildschirm sind alle Konfigurationsabschnitte der grafischen Benutzeroberfläche (GUI) mit Ausnahme der Kennwortänderung und der Annahme der Nutzungsbedingungen optional. Wenn die Informationen bekannt sind, wird empfohlen, den Setup-Assistenten zu verwenden, um die Erstkonfiguration des Management Center zu vereinfachen. Klicken Sie nach der Konfiguration auf Apply, um die Konfiguration auf das Management Center und registrierte Geräte anzuwenden. Eine kurze Übersicht über die Konfigurationsoptionen ist wie folgt: Kennwort ändern: Ermöglicht Ihnen, das Kennwort für das Standard-Administratorkonto zu ändern. Das Kennwort muss geändert werden. Netzwerkeinstellungen: Ermöglicht das Andern der zuvor konfigurierten IPv4- und IPv6-Netzwerkeinstellungen für die Verwaltungsschnittstelle der Appliance oder des virtuellen Systems Zeiteinstellungen: Es wird empfohlen, das Management Center mit einer zuverlässigen NTP-Quelle zu synchronisieren. Die IPS-Sensoren können mithilfe von Systemrichtlinien konfiguriert werden, um ihre Zeit mit dem Management Center zu synchronisieren. Optional können die Zeitzone für die Zeit und die Anzeige auch manuell festgelegt werden Regelaktualisierungsimporte: Aktivieren Sie wiederkehrende Snort-Regelaktualisierungen und können Sie diese optional während der Ersteinrichtung jetzt

installieren. Wiederholte Standortaktualisierungen: Aktivieren Sie regelmäßige Aktualisierungen von Geolokationsregeln, und installieren Sie diese optional während der Ersteinrichtung. Automatische Backups: Planen Sie automatische Konfigurations-Backups. Lizenzeinstellungen: Fügen Sie die Funktionslizenz hinzu. Geräteregistrierung: Ermöglicht das Hinzufügen, die Lizenzierung und die Anwendung von Richtlinien zur anfänglichen Zugriffskontrolle auf vorab registrierte Geräte. Der Hostname/die IP-Adresse und der Registrierungsschlüssel müssen mit der IP-Adresse und dem Registrierungsschlüssel übereinstimmen, die auf dem FirePOWER IPS-Modul konfiguriert wurden. Endbenutzer-Lizenzvertrag: Die Annahme des Endbenutzer-Lizenzvertrags ist erforderlich.

Use these fields to change the password for the admin account. Sourcefire recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary. New Password	Change Password	
New Password Confirm Confirm Network Settings Vise these fields to specify network-related information for the management interface on the appliance. Protocol IPv4 Management IP Netmask IPv4 Default Network Gateway Hostname Domain Primary DNS Server Secondary DNS Server Tertiary DNS Server	Use these fields to change the password for the ad characters of mixed case and includes at least one	min account. Sourcefire recommends that you use a password that has at least eight alphanumeric numeric character. Avoid using words that appear in a dictionary.
Network Settings Use these fields to specify network-related information for the management interface on the appliance. Protocol IPv4 IPv6 Both IPv4 Management IP Netmask IPv4 Default Network Gateway Hostname Domain Primary DNS Server Secondary DNS Server Tertiary DNS Server	New Password Confirm	
Use these fields to specify network-related information for the management interface on the appliance. Protocol IPv4 <	Network Settings	
Protocol IPv4 IPv4 Management IP Netmask IPv4 Default Network Gateway Hostname Domain Primary DNS Server Secondary DNS Server Intervance	Use these fields to specify network-related informa	tion for the management interface on the appliance.
IPv4 Default Network Gateway Hostname Domain Primary DNS Server Secondary DNS Server Tertiary DNS Server	Protocol IPv4 Management IP	● IPv4 ○ IPv6 ○ Both
Hostname Image: Comparing the second and the second	IPv4 Default Network Gateway	
Primary DNS Server Ended	Hostname Domain	
Secondary DNS Server Tertiary DNS Server	Primary DNS Server	
Tertiary DNS Server	Secondary DNS Server	
	Tertiary DNS Server	

Zugehörige Informationen

- FirePOWER Management Center Virtual Quick Start Guide for VMware, Version 6.0
- <u>Technischer Support und Dokumentation Cisco Systems</u>