# Implementatie van FireSIGHT Management Center op VMware ESXi

## Inhoud

Inleiding Voorwaarden Gebruikte componenten Configuratie Een OVF-sjabloon implementeren Inschakelen en initialiseren Netwerkinstellingen configureren Eerste installatie uitvoeren Gerelateerde informatie

## Inleiding

In dit document wordt de eerste installatie beschreven van een FireSIGHT Management Center (ook bekend als Defense Center) dat op VMware ESXi draait. Met een FireSIGHT Management Center kunt u één of meer FirePOWER-applicaties, next-generation inbraakpreventiesysteem (NGIPS) virtuele applicaties en adaptieve security applicatie (ASA) met FirePOWER Services beheren.

Opmerking: Dit document is een aanvulling op de FireSIGHT System Installatie Guide en de Gebruikersgids. Raadpleeg voor een ESXi-specifieke configuratie en probleemoplossing de VMware-kennisbasis en -documentatie.

## Voorwaarden

### Gebruikte componenten

De informatie op dit document is gebaseerd op de volgende platforms:

- Cisco FireSIGHT Management Center
- Cisco FireSIGHT Management Center virtuele applicatie
- VMware ESXI 5.0

In dit document verwijst een 'apparaat' naar deze platforms:

- Sourcefire FirePOWER 7000 Series-applicaties en 8000 Series applicaties
- Sourcefire NGIPS virtuele applicaties voor VMware ESXi
- Cisco ASA met FirePOWER Services

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

## Configuratie

### Een OVF-sjabloon implementeren

- 1. Download de Cisco FireSIGHT Management Center virtuele applicatie van de Cisco Support <u>& Downloads</u>-website.
- 2. Trek de inhoud van het tar.gz-bestand naar een lokale map.
- 3. Sluit aan op uw ESXi-server met een VMware vSphere-

2 VM	ware vSphere Client 🛛 💌
vmware <sup>.</sup> VMware vSphere <sup></sup> Client	
To directly manage a singl To manage multiple hosts, vCenter Server.	e host, enter the IP address or host name. , enter the IP address or name of a
IP address / Name:	<b>_</b>
User name:	
Password:	
	Use Windows session credentials
	Login Close Help

client.

4. Selecteer Bestand > OVF-sjabloon implementeren als u hebt aangemeld bij de vSphere-

Ć	2								
	File	Edit	View	Inventory	Adminis	tration	Plug	-ins	Helj
		New	1		•	ntory	Þ 🗊	Inve	entory
		Depl	loy OVI	Template.					
		Expo	ort		+				
		Repo	ort		•	localh	ost. VI	1wai	re ES
		Brov	vse VA	Marketplac	e	Getti	ng Start	ed	Sum
		Print	t Maps		Þ				
client.		Exit							

5. Klik op **Bladeren** en lokeer de bestanden die u in stap 2 hebt geëxtraheerd. Kies het OVFbestand Sourcefire\_Defense\_Center\_Virtual64\_VMware-ESXi-X.X.x-xxx.ovf en klik op **Volgende.** 

0	Deploy OVF Template
Source Select the source location.	
Source OVF 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. Klik in het scherm **OVF Sjabloongegevens** op **Volgende** om de standaardinstellingen te aanvaarden.

Ø	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	> Cancel

7. Typ een naam voor het beheercentrum en klik op

#### Volgende

t elgenae.		
Ø	Deploy OVF Template	

#### Name and Location

Specify a name and location for the deployed template

Source	Name:
OVF Template Details	VirtualDC64
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. Kies een **Datastore** waarop u de virtuele machine wilt maken en klik op **Volgende**.

Ø	Deploy	y OVF Template		- • •
Datastore Where do you want to sto	re the virtual machine fil	es?		
Source	Select a datastore in w	hich to store the VM files:		
OVF Template Details Name and Location	Name	Capacity Provisioned	Free Type	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			< Back	Next > Cancel

9. Klik op de radioknop **voor dikke** bestandsindeling voor de **schijf** en klik op **Volgende**. Het dikke leveringsformaat wijst de benodigde schijfruimte toe op het moment dat een virtuele schijf wordt gemaakt, terwijl het dunne provisioningformaat op verzoek ruimte gebruikt.

Ø	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: C 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 C Thick provisioned format All storage is allocated immediately. Estimated disk usage: 250.0 GB
Help	<back next=""> Cancel</back>

10. Koppel in het gedeelte **Network mapping** de beheerinterface van het FireSIGHT Management Center aan een VMware-netwerk en klik op **Volgende**.

)er	olo	v O۱	/F 1	Tem	pla	ate
~~	5.0					acc.

I

#### Network Mapping

Ø

What networks should the deployed template use?

	Jource Networks	Destination Networks	
isk Format	Management	VM Network	
eady to Complete		VM Network	
,,		VM Network 2	
	Description:		
	The Management network		
	The Hanagement network		
	1		

11. Klik op **Voltooien** om de OVF-modelplaatsing te voltooien.



### Inschakelen en initialiseren

 Navigeren naar de nieuwe virtuele machine. Klik met de rechtermuisknop op de servernaam en kies Aan/uit > Aan/uit om de server voor het eerst op te starten.



2. Navigeer naar het tabblad **console** om de serverconsole te bewaken. Het LILO Boot Menu verschijnt.

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

Nadat de door het systeem ingestelde gegevens zijn gecontroleerd, wordt het initialisatieproces gestart. De eerste start kan extra tijd in beslag nemen om te voltooien aangezien de configuratiedatabase voor het eerst wordt geformatteerd.

```
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
                                                                              1
Executing S06addusers
                                                                       E
                                                                          OK
                                                                              ]
Executing S07uuid-init
                                                                       E
                                                                          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
```

Zodra dit is voltooid, ziet u mogelijk een bericht voor Geen dergelijk

apparaat.

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

3. Druk op ENTER om een aanmelding te

verkrijgen.

```
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: _
```

Opmerking: Een bericht "SCHRIJF DEZELFDE. handmatig op nul stellen." Mogelijk verschijnt nadat het systeem voor het eerst is opgestart. Dit wijst niet op een defect, het geeft juist aan dat de VMware-opslagstuurprogramma de opdracht SCHRIFTELIJK SAME niet ondersteunt. Het systeem geeft dit bericht weer en gaat met een back-upopdracht verder om dezelfde bewerking uit te voeren.

### Netwerkinstellingen configureren

- Gebruik de inlognaam Sourcefire3D om in te loggen op deze aanmeldingsgegevens: Voor versie 5.xUsername: besturenWachtwoord: SourcefireVoor versie 6.x en laterUsername: besturenWachtwoord: Admin123Tip: U kunt het standaardwachtwoord tijdens de eerste installatie in de GUI wijzigen.
- 2. De eerste configuratie van het netwerk gebeurt met een script. U moet het script als wortel gebruiker uitvoeren. Om op de root gebruiker te kunnen overschakelen, voert u de sudo su opdracht in samen met het wachtwoord Sourcefire of Admin123 (voor 6.x). Wees voorzichtig met inloggen in de opdrachtregel van het beheercentrum als basisgebruiker. admin@sourcefire3D:~\$ sudo su - Password:
- 3. Om met de netwerkconfiguratie te beginnen, voer het **configuratie-netwerk** script als root in. **root@Sourcefire3D:~# configure-network**

Do you wish to configure IPv4? (y or n) y

U zal worden gevraagd een IP-adres, netmasker en standaardgateway te verstrekken. Zodra u de instellingen hebt bevestigd, start de netwerkservice opnieuw. Als resultaat hiervan gaat de managementinterface omlaag en komt dan

```
teruq.
 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:~# _
```

### Eerste installatie uitvoeren

- Nadat de netwerkinstellingen zijn ingesteld, opent u een webbrowser en bladert u naar de geconfigureerde IP via HTTPS (<u>https://192.0.2.2</u> in dit voorbeeld). Verifieer het standaard SSL-certificaat indien dit wordt gevraagd. Gebruik deze aanmeldingsgegevens om in te loggen:Voor versie 5.x Username: **besturen**Wachtwoord: **Sourcefire**Voor versie 6.x en laterUsername: **besturen**Wachtwoord: **Admin123**
- 2. Op het volgende scherm zijn alle GUI-configuratiesecties optioneel, behalve de wachtwoordwijziging en de acceptatie van de servicebepalingen. Als de informatie bekend is, wordt het aanbevolen de installatiewizard te gebruiken om de eerste configuratie van het Management Center te vereenvoudigen. Klik na configuratie op Toepassen om de configuratie toe te passen op het Management Center en de geregistreerde apparaten. Een kort overzicht van de configuratieopties is als volgt: Wachtwoord wijzigen Hiermee kunt u het wachtwoord wijzigen voor de standaard-beheeraccount. Het wachtwoord moet worden gewijzigd. Netwerkinstellingen: Hiermee kunt u de eerder ingestelde IPv4- en IPv6netwerkinstellingen aanpassen voor de beheerinterface van het apparaat of de virtuele machine. Tijdinstellingen: Aanbevolen wordt om het Management Center te synchroniseren met een betrouwbare NTP-bron. De IPS sensoren kunnen via systeembeleid worden geconfigureerd om hun tijd met het Management Center te synchroniseren. Optioneel kan de tijd- en weergavetijdzone handmatig worden ingesteld. Recurring Rule Update: Kunt u terugkerende updates voor de kortregel inschakelen en desgewenst tijdens de eerste installatie nu installeren. Herstel van geolocatie-updates: Schakel terugkerende geolocatiereedschappen in en installeer nu optioneel tijdens de eerste instelling. Automatische back-ups: Schema's voor automatische configuratie. Instellingen licentie: Voeg de functiekaart toe. Apparaatregistratie: Hier kunt u beleid voor toegangscontrole toevoegen, licentiëren en toepassen op gepreregistreerde apparaten. De hostname/IP-adres en de

registratiesleutel moeten overeenkomen met het IP-adres en de registratiesleutel die in de FirePOWER IPS-module zijn ingesteld. **Gebruiksrechtovereenkomst:** Aanvaarding van de EULA is

#### vereist.

Change Password			
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			
Confirm			
Network Settings			
Use these fields to specify network-related informa	tion 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			

## Gerelateerde informatie

- Firepower Management Center Virtual Quick Start Guide voor VMware, versie 6.0
- Technische ondersteuning en documentatie Cisco Systems