# Implantação do FireSIGHT Management Center no VMware ESXi

# Contents

Introduction Prerequisites Componentes Utilizados Configuração Implantar um modelo OVF Ligar e concluir a inicialização Definir as configurações de rede Executar configuração inicial Informações Relacionadas

# Introduction

Este documento descreve a configuração inicial de um FireSIGHT Management Center (também conhecido como Defense Center) executado no VMware ESXi. Um FireSIGHT Management Center permite que você gerencie um ou mais dispositivos FirePOWER, dispositivos virtuais do Next Generation Intrusion Prevention System (NGIPS) e Adaptive Security Appliance (ASA) com FirePOWER Services.

**Note**: Este documento é um suplemento do Guia de instalação do sistema FireSIGHT e do Guia do usuário. Para uma pergunta específica sobre configuração e solução de problemas do ESXi, consulte a base de conhecimento e a documentação do VMware.

# Prerequisites

## **Componentes Utilizados**

As informações neste documento são baseadas nas seguintes plataformas:

- Cisco FireSIGHT Management Center
- Dispositivo virtual do Cisco FireSIGHT Management Center
- VMware ESXI 5.0

Neste documento, um "dispositivo" refere-se a estas plataformas:

- Dispositivos Sourcefire FirePOWER 7000 Series e 8000 Series
- Dispositivos virtuais Sourcefire NGIPS para VMware ESXi
- Cisco ASA 5500-X Series com serviço FirePOWER

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# Configuração

## Implantar um modelo OVF

- 1. Baixe o Cisco FireSIGHT Management Center Virtual Appliance do site Cisco Support & Downloads.
- 2. Extraia o conteúdo do arquivo tar.gz para um diretório local.
- 3. Conecte-se ao servidor ESXi com um cliente VMware

	🕗 VN	Iware vSphere Client	×
	vmware <sup>•</sup> VMware vSphere <sup>••</sup> Client		
	To directly manage a sin To manage multiple host vCenter Server. IP address / Name: User name: Password:	gle host, enter the IP address or host nam s, enter the IP address or name of a	e.
<b>vSphere</b> . 4. Depois de	e fazer login no vSphere C	Use Windows session credentials Login Close Client, escolha File > Deploy OVF	Help
Touch	File Edit View Invent New Deploy OVF Temp Export Report Browse VA Market Print Maps Exit	tory Administration Plug-ins Help htory Reg Inventory late b localhost. VMware ES cplace b	

5. Clique em Procurar e localize os arquivos que você extraiu na etapa 2. Escolha o arquivo

OVF Sourcefire\_Defense\_Center\_Virtual64\_VMware-ESXi-X.X.X-xxx.ovf e clique em **Avançar.** 

Ø	Deploy OVF Template	-		23
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 >		Cance	

6. Na tela **OVF Template Details**, clique em **Next** para aceitar as configurações padrão.

Ø	Deploy	y OVF Template		
OVF Template Details Verify OVF template details.				
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. Forneça um nome para o Centro de Gerenciamento e clique em

#### Avancar.

1

Help

	Deploy OVF Template
Name and Location Specify a name and loca	ition for the deployed template
Source	Name:
<u>OVF Template Details</u>	VirtualDC64
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.

< Back Next >

8. Escolha um **Armazenamento de Dados** no qual deseja criar a máquina virtual e clique em **Avançar**.

	Depl	oy OVF Template			>
Datastore Where do you want t	o store the virtual machine	files?			
Source	Select a datastore in	which to store the VM files:			
OVF Template Details	Name	Capacity Provisioned	Free Type	Thin Provisioning	Acce
Datastore	[datastore2]	1.29 TB 866.14 GB	469.36 GB VMFS	Supported	Sing
Disk Format Network Mapping Ready to Complete	[datastore1]	459.75 GB 563.00 MB	459.20 GB VMFS	Supported	Singl
Help	<		< Back	Next > C	ancel

 Clique no botão de opção Thick provisioned format para o formato do disco e clique em Next. O formato de provisionamento grosso aloca o espaço em disco necessário no momento da criação de um disco virtual, enquanto o formato de provisionamento thin usa espaço sob demanda.

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 (* Thick provisioned format All storage is allocated immediately. Estimated disk usage: 250.0 GB
Help	< Back Next > Cancel

10. Na seção **Mapeamento de rede**, associe a interface de gerenciamento do FireSIGHT Management Center a uma rede VMware e clique em **Avançar**.

	Dep	loy	OVF	Temp	late
--	-----	-----	-----	------	------

#### Network Mapping

Ø

What networks should the deployed template use?

atastore	Source Networks	Destination Networks	
<u>sk Format</u> etwork Mapping	Management	VM Network	•
eady to Complete		VM Network	
		VM Network 2	
	Description:		
	The Management network		
	1		

11. Clique em **Finish** para concluir a implantação do modelo OVF.



## Ligar e concluir a inicialização

 Navegue até a máquina virtual recém-criada. Clique com o botão direito do mouse no nome do servidor e escolha Power > Power On para inicializar o servidor pela primeira vez.



2. Navegue até a guia **Console** para monitorar o console do servidor. O menu de inicialização LILO é



Quando a verificação de dados do BIOS for bem-sucedida, o processo de inicialização será iniciado. A primeira inicialização pode levar mais tempo para ser concluída, pois o banco de dados de configuração é inicializado pela primeira vez.

```
Firstboot detected, executing scripts
Executing S03install-math-pari.sh
                                                                       E
                                                                          OK
                                                                              ]
                                                                              ]
                                                                       E
                                                                          OK
Executing S04async_syslog_dc.sh
                                                                       E
                                                                              ]
Executing S04fix-httpd.sh
                                                                          OK
                                                                       Ľ
                                                                              ]
Executing S05set-MgMnt-port
                                                                          OK
                                                                              ]
                                                                       E
                                                                          OK
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
```

Depois de concluído, você poderá ver uma mensagem para Nenhum dispositivo desse tipo.

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

3. Pressione Enter para obter um prompt de

login.

```
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: _
```

**Note**: Uma mensagem "WRITE SAME failed. Zerando manualmente." pode aparecer após o sistema ser inicializado pela primeira vez. Isso não indica um defeito, indica corretamente que o driver de armazenamento VMware não suporta o comando WRITE SAME. O sistema exibe essa mensagem e continua com um comando fallback para executar a mesma operação.

### Definir as configurações de rede

- No prompt de login Sourcefire3D, use estas credenciais para fazer login: Para a versão 5.xNome de usuário: adminSenha: SourcefirePara a versão 6.x e posteriorNome de usuário: adminSenha: Admin123Tip: Você poderá alterar a senha padrão no processo de configuração inicial na GUI.
- 2. A configuração inicial da rede é feita com um script. Você precisa executar o script como um usuário raiz. Para alternar para o usuário raiz, digite o comando sudo su junto com a senha Sourcefire ou Admin123 (para 6.x). Tenha cuidado ao fazer login na linha de comando do Management Center como um usuário raiz.

```
admin@Sourcefire3D:~$ sudo su -
Password:
```

3. Para iniciar a configuração de rede, insira o script **configure-network** como root. root@Sourcefire3D:~# configure-network

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

Você será solicitado a fornecer um endereço IP de gerenciamento, uma máscara de rede e um gateway padrão. Depois de confirmar as configurações, o serviço de rede será reiniciado. Como resultado, a interface de gerenciamento fica inativa e

```
volta.
 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:~# _
```

## Executar configuração inicial

- Depois que as configurações de rede estiverem configuradas, abra um navegador da Web e navegue até o IP configurado via HTTPS (<u>https://192.0.2.2</u> neste exemplo). Autentique o certificado SSL padrão, se solicitado. Use estas credenciais para fazer login:Para a versão 5.x Nome de usuário: adminSenha: SourcefirePara a versão 6.x e posteriorNome de usuário: adminSenha: Admin123
- 2. Na tela a seguir, todas as secões de configuração da GUI são opcionais, exceto a alteração de senha e a aceitação dos termos de serviço. Se as informações forem conhecidas, é recomendável usar o assistente de configuração para simplificar a configuração inicial do Management Center. Depois de configurado, clique em Apply para aplicar a configuração ao Management Center e aos dispositivos registrados. Uma breve visão geral das opções de configuração é a seguinte: Alterar Senha: Permite alterar a senha da conta admin padrão. É necessário alterar a senha. Configurações de rede: Permite modificar as configurações de rede IPv4 e IPv6 previamente configuradas para a interface de gerenciamento do dispositivo ou da máquina virtual Configurações de horário: é recomendável sincronizar o Management Center com uma fonte NTP confiável. Os sensores IPS podem ser configurados por meio de política de sistema para sincronizar seu tempo com o Management Center. Opcionalmente, o fuso horário e o fuso horário de exibição podem ser definidos manualmente. Importações de atualização de regra recorrente: Habilite atualizações de regra de Snort recorrentes e, opcionalmente, instale agora durante a configuração inicial Atualizações recorrentes da localização geográfica: ativar atualizações recorrentes da regra de localização geográfica e, opcionalmente, instalar agora durante a configuração inicial Backups automáticos: agende backups automáticos de configuração. Configurações da licença: Adicione a licença do recurso. Device Registration: permite que você adicione, licencie e aplique as políticas iniciais de controle de acesso aos dispositivos pré-registrados. O nome do host/endereço IP

e a chave de registro devem corresponder ao endereço IP e à chave de registro configurados no módulo IPS do FirePOWER. **Contrato de licença de usuário final:** é necessária a aceitação do

## EULA.

Change Password	
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.
New Password	
Confirm	
Network Settings	
Use these fields to specify network-related information	ation 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	

# Informações Relacionadas

- Guia de início rápido virtual do Firepower Management Center para VMware, versão 6.0
- Suporte Técnico e Documentação Cisco Systems