Instale um módulo SFR em um módulo de hardware ASA 5585-X

Contents

Introduction

O módulo ASA FirePOWER, também conhecido como ASA SFR, fornece serviços de firewall de próxima geração, incluindo IPS de próxima geração (NGIPS), Application Visibility and Control (AVC), filtragem de URL e Advanced Malware Protection (AMP). Você pode usar o módulo no modo de contexto único ou múltiplo e no modo roteado ou transparente. Este documento descreve os pré-requisitos e os processos de instalação de um módulo FirePOWER (SFR) no módulo de hardware ASA 5585-X. Ele também fornece as etapas para registrar um módulo SFR no FireSIGHT Management Center.

> **Note**: Os FirePOWER Services (SFR) residem em um módulo de hardware no ASA 5585-X, enquanto os FirePOWER Services nos dispositivos ASA 5512-X a 5555-X Series são instalados em um módulo de software, resultando em diferenças nos processos de instalação.

Prerequisites

Requirements

As instruções neste documento exigem acesso ao modo EXEC privilegiado. Para acessar o modo EXEC privilegiado, insira o comando enable. Se não tiver sido definida uma senha, basta pressionar Enter.

```
ciscoasa> enable
Password:
ciscoasa#
```

Para instalar o FirePOWER Services em um ASA, os seguintes componentes são necessários:

- Software ASA versão 9.2.2 ou posterior
- Plataforma ASA 5585-X
- Um servidor TFTP alcançável pela interface de gerenciamento do módulo FirePOWER
- FireSIGHT Management Center com versão 5.3.1 ou posterior

> **Note**: As informações neste documento são criadas a partir dos dispositivos em um ambiente de laboratório específico. 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

Antes de Começar

Dado que um ASA SSM sempre ocupa um dos dois slots no chassi do ASA 5585-X, se você tiver um módulo de hardware diferente do FirePOWER (SFR) Services SSP, como o SSP-CX (Context Aware) ou AIP-SSM (Advanced Inspection and Prevention Security), o outro módulo deve ser desinstalado para criar espaço para o SSP-SFR. Antes de remover um módulo de hardware, execute o seguinte comando para desligar um módulo:

```
ciscoasa# hw-module module 1 shutdown
```

Cabeamento e gerenciamento

- Você não pode acessar a porta serial do módulo SFR pelo console do ASA no ASA 5585-X.
- Depois que o módulo SFR for provisionado, você poderá realizar uma sessão no blade usando o comando "session 1".
- Para recriar completamente o módulo SFR em um ASA 5585-X, você deve usar a interface Ethernet de gerenciamento e uma sessão de console na porta de gerenciamento serial, que estão no módulo SFR e separados da interface de gerenciamento e do console do ASA.

> **Tip**: Para localizar o status de um módulo no ASA, execute o comando "show module 1 details" que recupera o IP de gerenciamento do módulo SFR e o Centro de Defesa associado.

Instalar o módulo FirePOWER (SFR) no ASA

1. Faça o download da imagem inicial de bootstrap do módulo ASA FirePOWER SFR do Cisco.com para um servidor TFTP acessível a partir da interface de gerenciamento do ASA FirePOWER. O nome da imagem se parece com "asasfr-boot-5.3.1-152.img"

2. Baixe o software do sistema ASA FirePOWER do Cisco.com para um servidor HTTP, HTTPS ou FTP acessível da interface de gerenciamento do ASA FirePOWER.

3. Reinicie o módulo SFR

Opção 1: Se você não tiver a senha para o módulo SFR, poderá emitir o seguinte comando do ASA para reiniciar o módulo.

```
ciscoasa# hw-module module 1 reload
Reload module 1? [confirm]
Reload issued for module 1
```

Opção 2: Se você tiver a senha para o módulo SFR, poderá reinicializar o sensor diretamente da linha de comando.

```
Sourcefire3D login: admin
Password:

Sourcefire Linux OS v5.3.1 (build 43)
Sourcefire ASA5585-SSP-10 v5.3.1 (build 152)

>system reboot
```

4. Interrompa o processo de inicialização do módulo SFR usando ESCAPE ou a sequência de interrupção do software da sessão de terminal para colocar o módulo no ROMMON.

```
The system is restarting...
CISCO SYSTEMS
Embedded BIOS Version 2.0(14)1 15:16:31 01/25/14



Cisco Systems ROMMON Version (2.0(14)1) #0: Sat Jan 25 16:44:38 CST 2014

Platform ASA 5585-X FirePOWER SSP-10, 8GE

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in 8 seconds.

Boot interrupted.

Management0/0
Link is UP
MAC Address: xxxx.xxxx.xxxx

Use ? for help.
```

```
rommon #0>
```

5. Configure a interface de gerenciamento do módulo SFR com um endereço IP e indique a localização do servidor TFTP e do caminho TFTP para a imagem de bootstrap. Insira os seguintes comandos para definir um endereço IP na interface e recuperar a imagem TFTP:

- `configurado`
- ADDRESS = Your_IP_Address
- GATEWAY = Your_Gateway
- SERVER = Your_TFTP_Server
- IMAGE = Your_TFTP_FilePath
- `sync`
- `tftp`

! Exemplo de informações de endereço IP usadas. Atualize para o seu ambiente.

```
rommon #1> ADDRESS=198.51.100.3
rommon #2> GATEWAY=198.51.100.1
rommon #3> SERVER=198.51.100.100
rommon #4> IMAGE=/tftpboot/asasfr-boot-5.3.1-152.img
rommon #5> sync

Updating NVRAM Parameters...

rommon #6> tftp
ROMMON Variable Settings:
ADDRESS=198.51.100.3
SERVER=198.51.100.100
GATEWAY=198.51.100.1
PORT=Management0/0
VLAN=untagged
IMAGE=/tftpboot/asasfr-boot-5.3.1-152.img
CONFIG=
LINKTIMEOUT=20
PKTTIMEOUT=4
RETRY=20

tftp /tftpboot/asasfr-boot-5.3.1-152.img@198.51.100.100 via 198.51.100.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
<truncated output>

Received 41235627 bytes

Launching TFTP Image...

Execute image at 0x14000
```

6. Faça login na imagem de inicialização inicial. Faça login como admin e com a senha Admin123

```
Cisco ASA SFR Boot Image 5.3.1

asasfr login: admin
Password:
```

```
Cisco ASA SFR Boot 5.3.1 (152)
Type ? for list of commands
```

7. Use a imagem de inicialização inicial para configurar um endereço IP na interface de gerenciamento do módulo. Digite o comando setup para entrar no assistente. Você será solicitado a fornecer as seguintes informações:

- **Hostname:** Até 65 caracteres alfanuméricos, sem espaços. Hífens são permitidos.
- **Endereço de rede**: Você pode definir endereços IPv4 ou IPv6 estáticos ou usar a configuração automática de DHCP (para IPv4) ou IPv6 stateless.
- **Informações de DNS**: Você deve identificar pelo menos um servidor DNS e também pode definir o nome de domínio e o domínio de pesquisa.
- **Informações de NTP**: Você pode habilitar o NTP e configurar os servidores NTP para definir a hora do sistema.

! Informações de exemplo usadas. Atualize para o seu ambiente.

```
asasfr-boot>setup

Welcome to SFR Setup
[hit Ctrl-C to abort]
Default values are inside []

Enter a hostname [asasfr]: sfr-module-5585
Do you want to configure IPv4 address on management interface?(y/n) [Y]: Y
Do you want to enable DHCP for IPv4 address on management interface?(y/n) [N]: N
Enter an IPv4 address [192.168.8.8]: 198.51.100.3
Enter the netmask [255.255.255.0]: 255.255.255.0
Enter the gateway [192.168.8.1]: 198.51.100.1
Do you want to configure static IPv6 address on management interface?(y/n) [N]: N
Stateless autoconfiguration will be enabled for IPv6 addresses.
Enter the primary DNS server IP address: 198.51.100.15
Do you want to configure Secondary DNS Server? (y/n) [n]: N
Do you want to configure Local Domain Name? (y/n) [n]: N
Do you want to configure Search domains? (y/n) [n]: N
Do you want to enable the NTP service? [Y]: N

Please review the final configuration:
Hostname: sfr-module-5585
Management Interface Configuration

IPv4 Configuration: static
IP Address: 198.51.100.3
Netmask: 255.255.255.0
Gateway: 198.51.100.1

IPv6 Configuration: Stateless autoconfiguration

DNS Configuration:
DNS Server: 198.51.100.15

Apply the changes?(y,n) [Y]: Y
Configuration saved successfully!
Applying...
Restarting network services...
Restarting NTP service...
Done.
```

8. Use a imagem de inicialização para puxar e instalar a imagem do software do sistema usando o comando **system install**. Inclua opção **não confirmar** se você não quiser responder a mensagens de confirmação. Substitua a palavra-chave *url* pelo local do arquivo .pkg.

```
asasfr-boot> system install [noconfirm] url
```

Por exemplo,

```
> system install http://Server_IP_Address/asasfr-sys-5.3.1-152.pkg

Verifying
Downloading
Extracting

Package Detail
Description: Cisco ASA-SFR 5.3.1-152 System Install
Requires reboot: Yes

Do you want to continue with upgrade? [y]: Y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image ...
```

> **Note**: Quando a instalação estiver concluída em 20 a 30 minutos, você será solicitado a pressionar a tecla Enter para reinicializar. Aguarde 10 minutos ou mais para a instalação do componente do aplicativo e para que os serviços ASA FirePOWER sejam iniciados. A saída de detalhes do show module 1 deve mostrar todos os processos como Up.

Status do módulo durante a instalação

```
ciscoasa# show module 1 details

Getting details from the Service Module, please wait...
Unable to read details from module 1

Card Type: ASA 5585-X FirePOWER SSP-10, 8GE
Model: ASA5585-SSP-SFR10
Hardware version: 1.0
Serial Number: JAD18400028
Firmware version: 2.0(14)1
Software version: 5.3.1-152
MAC Address Range: 58f3.9ca0.1190 to 58f3.9ca0.119b
App. name: ASA FirePOWER
App. Status: Not Applicable
App. Status Desc: Not Applicable
App. version: 5.3.1-152
Data Plane Status: Not Applicable
Console session: Not ready
Status: Unresponsive
```

Status do módulo após a instalação bem-sucedida

```
ciscoasa# show module 1 details
```

```
Getting details from the Service Module, please wait...

Card Type: ASA 5585-X FirePOWER SSP-10, 8GE
Model: ASA5585-SSP-SFR10
Hardware version: 1.0
Serial Number: JAD18400028
Firmware version: 2.0(14)1
Software version: 5.3.1-152
MAC Address Range: 58f3.9ca0.1190 to 58f3.9ca0.119b
App. name: ASA FirePOWER
App. Status: Up
App. Status Desc: Normal Operation
App. version: 5.3.1-152
Data Plane Status: Up
Console session: Ready
Status: Up
DC addr: No DC Configured
Mgmt IP addr: 192.168.45.45
Mgmt Network mask: 255.255.255.0
Mgmt Gateway: 0.0.0.0
Mgmt web ports: 443
Mgmt TLS enabled: true
```

Configuração

Configurar o software FirePOWER

1. Você pode se conectar ao módulo ASA 5585-X FirePOWER através de uma das seguintes portas externas:

- Porta de console ASA FirePOWER
- Interface ASA FirePOWER Management 1/0 usando SSH

  Note: Você não pode acessar o módulo de hardware do ASA FirePOWER CLI no painel traseiro do ASA usando o comando session sfr.

2. Depois de acessar o módulo FirePOWER pelo console, faça login com o nome de usuário **admin** e a senha **Sourcefire**.

```
Sourcefire3D login: admin
Password:

Last login: Fri Jan 30 14:00:51 UTC 2015 on ttyS0

Copyright 2001-2013, Sourcefire, Inc. All rights reserved. Sourcefire is a registered
trademark of Sourcefire, Inc. All other trademarks are property of their respective
owners.

Sourcefire Linux OS v5.3.1 (build 43)
Sourcefire ASA5585-SSP-10 v5.3.1 (build 152)

Last login: Wed Feb 18 14:22:19 on ttyS0
```

```
System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: dhcp
If your networking information has changed, you will need to reconnect.
[1640209.830367] ADDRCONF(NETDEV_UP): eth0: link is not ready
[1640212.873978] e1000e: eth0 NIC Link is Up 1000 Mbps Full Duplex, Flow Control: None
[1640212.966250] ADDRCONF(NETDEV_CHANGE): eth0: link becomes ready
For HTTP Proxy configuration, run 'configure network http-proxy'

This sensor must be managed by a Defense Center.  A unique alphanumeric registration
key is always required.  In most cases, to register a sensor to a Defense Center,
you must provide the hostname or the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Defense Center are separated by a NAT device, you
must enter a unique NAT ID, along with the unique registration key. 'configure
manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.

>
```

Configurar o FireSIGHT Management Center

Para gerenciar um módulo ASA FirePOWER e uma política de segurança, você **deve** registrá-lo com um FireSIGHT Management Center. Não é possível fazer o seguinte com um FireSIGHT Management Center:

- Não é possível configurar as interfaces do ASA FirePOWER.
- Não é possível desligar, reiniciar ou gerenciar de outra forma os processos do ASA FirePOWER.
- Não é possível criar backups ou restaurar backups em dispositivos ASA FirePOWER.
- Não é possível gravar regras de controle de acesso para corresponder ao tráfego usando condições de marca de VLAN.

Redirecionar tráfego para o módulo SFR

Você redireciona o tráfego para o módulo ASA FirePOWER criando uma política de serviço que identifica o tráfego específico. Para redirecionar o tráfego para um módulo FirePOWER, siga as etapas abaixo:

Passo 1: Selecionar tráfego

Primeiro, selecione o tráfego usando o comando access-list. No exemplo a seguir, estamos redirecionando todo o tráfego de todas as interfaces. Você pode fazer isso para tráfego específico também.

```
ciscoasa(config)# access-list sfr_redirect extended permit ip any any
```

Passo 2: Corresponder tráfego

O exemplo a seguir mostra como criar um mapa de classe e corresponder ao tráfego em uma lista de acesso:

```
ciscoasa(config)# class-map sfr
ciscoasa(config-cmap)# match access-list sfr_redirect
```

Passo 3: Especificar ação

Você pode configurar seu dispositivo em uma implantação passiva ("somente monitor") ou em linha. Você não pode configurar o modo somente monitor e o modo em linha normal ao mesmo tempo no ASA. Somente um tipo de política de segurança é permitido.

Modo em linha

Em uma implantação em linha, depois de descartar tráfego indesejado e tomar outras ações aplicadas pela política, o tráfego é devolvido ao ASA para processamento adicional e transmissão final. O exemplo a seguir mostra como criar um mapa de políticas e configurar o módulo FirePOWER no modo em linha:

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class sfr
ciscoasa(config-pmap-c)# sfr fail-open
```

Modo passivo

Em uma implantação passiva,

- Uma cópia do tráfego é enviada ao dispositivo, mas não é devolvida ao ASA.
- O modo passivo permite que você veja o que o dispositivo teria feito com o tráfego e permite que você avalie o conteúdo do tráfego, sem afetar a rede.

Se quiser configurar o módulo FirePOWER no modo passivo, use a palavra-chave monitor-only como abaixo. Se você não incluir a palavra-chave, o tráfego será enviado no modo em linha.

```
ciscoasa(config-pmap-c)# sfr fail-open monitor-only
```

Passo 4: Especificar local

A última etapa é aplicar a política. Você pode aplicar uma política globalmente ou em uma interface. Você pode substituir a política global em uma interface aplicando uma política de serviço a essa interface.

A palavra-chave global aplica o mapa de políticas a todas as interfaces e a interface aplica a política a uma interface. Apenas uma política global é permitida. No exemplo a seguir, a política é aplicada globalmente:

```
ciscoasa(config)# service-policy global_policy global
```

Caution: O mapa de política global_policy é uma política padrão. Se você usar essa política e quiser remover essa política em seu dispositivo para fins de solução de problemas, certifique-se de entender sua implicação.

Documento relacionado

- Registre um dispositivo com um FireSIGHT Management Center
- Implantação do FireSIGHT Management Center no VMware ESXi
- Cenários de configuração de gerenciamento de IPS em um módulo IPS 5500-X