Instalar e configurar um módulo FirePOWER Services em uma plataforma ASA

Contents

Introduction

Este documento descreve como instalar e configurar um módulo Cisco FirePOWER (SFR) executado em um Cisco Adaptive Security Appliance (ASA) e como registrar o módulo SFR no Cisco FireSIGHT Management Center.

Prerequisites

Requirements

A Cisco recomenda que seu sistema atenda a esses requisitos antes de tentar os procedimentos descritos neste documento:

- Verifique se você tem pelo menos 3 GB de espaço livre na unidade flash (disk0), além do tamanho do software de inicialização.
- Certifique-se de ter acesso ao modo EXEC privilegiado. Para acessar o modo EXEC privilegiado, insira o comando **enable** no CLI. Se não tiver sido definida uma senha, prima **Enter**:

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

Componentes Utilizados

Para instalar o FirePOWER Services em um Cisco ASA, esses componentes são necessários:

- Software Cisco ASA versão 9.2.2 ou posterior
- Plataformas Cisco ASA 5512-X a 5555-X
- Software FirePOWER versão 5.3.1 ou posterior

Note: Se quiser instalar o FirePOWER (SFR) Services em um módulo de hardware ASA 5585-X, consulte Instalar um módulo SFR em um módulo de hardware ASA 5585-X.

Esses componentes são necessários no Cisco FireSIGHT Management Center:

- Software FirePOWER versão 5.3.1 ou posterior
- FireSIGHT Management Center FS2000, FS4000 ou dispositivo virtual

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O módulo Cisco ASA FirePOWER, também conhecido como ASA SFR, fornece serviços de firewall de próxima geração, como:

- Sistema de prevenção de intrusão de próxima geração (NGIPS)
- Visibilidade e controle de aplicativo (AVC)
- Filtrar URLs
- Advanced malware protection (AMP)

Note: Você pode usar o módulo ASA SFR no modo de contexto único ou múltiplo e no modo roteado ou transparente.

Antes de Começar

Considere estas informações importantes antes de tentar os procedimentos descritos neste documento:

- Se você tiver uma política de serviço ativa que redireciona o tráfego para um módulo IPS (Intrusion Prevention System, Sistema de Prevenção de Invasão)/CX (Context Aware, Reconhecimento de Contexto) (substituído pelo ASA SFR), deverá removê-lo antes de configurar a política de serviço ASA SFR.
- Você deve desligar todos os outros módulos de software executados no momento. Um dispositivo pode executar um único módulo de software por vez. Você deve fazer isso no ASA CLI. Por exemplo, esses comandos desligam e desinstalam o módulo de software IPS e depois recarregam o ASA:

```
ciscoasa# sw-module module ips shutdown
ciscoasa# sw-module module ips uninstall
ciscoasa# reload
```

- Os comandos usados para remover o módulo CX são os mesmos, exceto o **cxsc** palavra-chave é usada em vez de **ips**:

```
ciscoasa# sw-module module cxsc shutdown
ciscoasa# sw-module module cxsc uninstall
ciscoasa# reload
```

- Ao recriar um módulo, use o mesmo **shutdown** e **uninstall** comandos usados para remover uma imagem antiga do SFR. Aqui está um exemplo:

```
ciscoasa# sw-module module sfr uninstall
```

- Se o módulo ASA SFR for usado no modo de contexto múltiplo, execute os procedimentos descritos neste documento no espaço de execução do sistema.

Tip: Para determinar o status de um módulo no ASA, insira o comando **show module** comando.

Instalação

Esta seção descreve como instalar o módulo SFR no ASA e como configurar a imagem de inicialização do ASA SFR.

Instale o módulo SFR no ASA

Conclua estes passos para instalar o módulo SFR no ASA:

1. Faça o download do software do sistema ASA SFR de Cisco.com para um servidor HTTP, HTTPS ou FTP que esteja acessível na interface de gerenciamento do ASA SFR.
2. Baixe a imagem de inicialização no dispositivo. Você pode usar o Cisco Adaptive Security Device Manager (ASDM) ou o ASA CLI para fazer o download da imagem de inicialização para o dispositivo. **Note**: Não transfira o software do sistema; é baixado posteriormente na unidade de estado sólido (SSD).Conclua estes passos para fazer o download da imagem de inicialização por meio do ASDM: Baixe a imagem de inicialização em sua estação de trabalho ou coloque-a em um servidor FTP, TFTP, HTTP, HTTPS, Server Message Block (SMB) ou Secure Copy (SCP).Escolher**Tools > File Management** no ASDM.Escolha o comando apropriado File Transfer (Transferência de arquivos), *Entre PC local e Flash* ou *Entre servidor remoto e Flash*.Transfira o software de inicialização para a unidade flash (disk0) no ASA.Conclua estes passos para fazer o download da imagem de inicialização através da CLI do ASA:Faça download da imagem de inicialização em um servidor FTP, TFTP, HTTP ou HTTPS.Digite o **copy** na CLI para baixar a imagem de inicialização na unidade flash. Aqui está um exemplo que usa o protocolo HTTP (substitua o com o endereço IP do servidor ou o nome do host). Para o servidor FTP, a URL é semelhante a esta:**ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img .**
```
ciscoasa# copy http:///asasfr-5500x-boot-5.3.1-152.img disk0:/asasfr-5500x-boot-5.3.1-152.img
```
3. Insira este comando para configurar o local da imagem de inicialização do ASA SFR na unidade flash do ASA:

```
ciscoasa# sw-module module sfr recover configure image disk0:/file_path
```

   Aqui está um exemplo:
```
ciscoasa# sw-module module sfr recover configure image disk0:
 /asasfr-5500x-boot-5.3.1-152.img
```
4. Insira este comando para carregar a imagem de inicialização do ASA SFR:

```
ciscoasa# sw-module module sfr recover boot
```

Durante esse período, se você habilitar **debug module-boot** no ASA, essas depurações são impressas:

```
Mod-sfr 788> *** EVENT: Creating the Disk Image...
Mod-sfr 789> *** TIME: 05:50:26 UTC Jul 1 2014
Mod-sfr 790> ***
Mod-sfr 791> ***
Mod-sfr 792> *** EVENT: The module is being recovered.
Mod-sfr 793> *** TIME: 05:50:26 UTC Jul 1 2014
Mod-sfr 794> ***
...
Mod-sfr 795> ***
Mod-sfr 796> *** EVENT: Disk Image created successfully.
Mod-sfr 797> *** TIME: 05:53:06 UTC Jul 1 2014
Mod-sfr 798> ***
Mod-sfr 799> ***
Mod-sfr 800> *** EVENT: Start Parameters: Image: /mnt/disk0/vm/vm_3.img,
ISO: -cdrom /mnt/disk0
Mod-sfr 801> /asasfr-5500x-boot-5.3.1-152.img, Num CPUs: 6, RAM: 7659MB,
Mgmt MAC: A4:4C:11:29:
Mod-sfr 802> CC:FB, CP MAC: 00:00:00:04:00:01, HDD: -drive file=/dev/md0,
cache=none,if=virtio,
Mod-sfr 803> Dev
Mod-sfr 804> ***
Mod-sfr 805> *** EVENT: Start Parameters Continued: RegEx Shared Mem:
32MB, Cmd Op: r, Shared M
Mod-sfr 806> em Key: 8061, Shared Mem Size: 64, Log Pipe: /dev/ttyS0_vm3,
Sock: /dev/ttyS1_vm3,
Mod-sfr 807>  Mem-Path: -mem-path /hugepages
Mod-sfr 808> *** TIME: 05:53:06 UTC Jul 1 2014
Mod-sfr 809> ***
Mod-sfr 810> IVSHMEM: optarg is key=8061,64,unix:/tmp/nahanni, name is,
key is 8061, size is 6
...
Mod-sfr 239> Starting Advanced Configuration and Power Interface daemon:
acpid.
Mod-sfr 240> acpid: starting up with proc fs
Mod-sfr 241> acpid: opendir(/etc/acpi/events): No such file or directory
Mod-sfr 242> starting Busybox inetd: inetd... done.
Mod-sfr 243> Starting ntpd: done
Mod-sfr 244> Starting syslogd/klogd: done
Mod-sfr 245>
Cisco ASA SFR Boot Image 5.3.1
```

5. Aguarde aproximadamente de 5 a 15 minutos para que o módulo ASA SFR seja inicializado e abra uma sessão de console para a imagem de inicialização do ASA SFR.

Configurar a imagem de inicialização do ASA SFR

Conclua estes passos para configurar a imagem de inicialização do ASA SFR recém-instalada:

1. Pressione **Enter** depois de abrir uma sessão para acessar o prompt de login. **Note**: O nome de usuário padrão é **admin**. A senha difere com base na versão do software:**Adm!n123** para 7.0.1 (novo dispositivo apenas de fábrica), **Admin123** para 6.0 e posterior, **Sourcefire** para pré-6.0.Aqui está um exemplo:

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.
```

```
Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

Tip: Se a inicialização do módulo ASA SFR não tiver sido concluída, o comando session falhará e uma mensagem será exibida para indicar que o sistema não consegue se conectar via TTYS1. Se isso ocorrer, aguarde a inicialização do módulo ser concluída e tente novamente.

2. Digite o **setup** para configurar o sistema de modo que você possa instalar o pacote de software do sistema:

```
asasfr-boot> setup
Welcome to SFR Setup
[hit Ctrl-C to abort]
Default values are inside []
```

Você será solicitado a fornecer essas informações:**Host name** - O nome do host pode ter até 65 caracteres alfanuméricos, sem espaços. É permitida a utilização de hífens.**Network address** - O endereço de rede pode ser endereços IPv4 ou IPv6 estáticos. Você também pode usar DHCP para configuração automática de IPv4 ou IPv6 stateless.**DNS information** - Você deve identificar pelo menos um servidor DNS (Domain Name System) e também pode definir o nome de domínio e o domínio de pesquisa.**NTP information** - Você pode ativar o Network Time Protocol (NTP) e configurar os servidores NTP para definir a hora do sistema.

3. Digite o **system install** para instalar a imagem do software do sistema:

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

Incluir o **noconfirm** se não desejar responder a mensagens de confirmação. Substitua o **url** palavra-chave com a localização do **.pkg** arquivo. Novamente, você pode usar um servidor FTP, HTTP ou HTTPS. Aqui está um exemplo:

```
asasfr-boot >system install http:///asasfr-sys-5.3.1-152.pkg
Verifying
Downloading
Extracting

Package Detail
Description: Cisco ASA-FirePOWER 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
Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
(press Enter)

Broadcast message from root (ttyS1) (Mon Jun 23 09:28:38 2014):
The system is going down for reboot NOW!
Console session with module sfr terminated.
```

Para o servidor FTP, a URL é semelhante a esta:**ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg**.

Observação O SFR está em um "**Recover**" durante o processo de instalação. Pode levar

cerca de uma hora para concluir a instalação do módulo SFR. Quando a instalação estiver concluída, o sistema será reinicializado. Aguarde dez ou mais minutos para a instalação do componente do aplicativo e para que os serviços ASA SFR sejam iniciados. A saída do comando **show module sfr** indica que todos os processos são **Up**.

Configurar

Esta seção descreve como configurar o software FirePOWER e o FireSIGHT Management Center e como redirecionar o tráfego para o módulo SFR.

Configure o software FirePOWER

Conclua estes passos para configurar o software FirePOWER:

1. Abra uma sessão no módulo ASA SFR.
   Note: Um prompt de login diferente agora é exibido porque o login ocorre em um módulo totalmente funcional.Aqui está um exemplo:

   ```
   ciscoasa# session sfr
   Opening command session with module sfr.
   Connected to module sfr. Escape character sequence is 'CTRL-^X'.
   Sourcefire ASA5555 v5.3.1 (build 152)
   Sourcefire3D login:
   ```
2. Faça login com o nome de usuário **admin** e a senha difere com base na versão do software:**Adm!n123** para 7.0.1 (novo dispositivo apenas de fábrica), **Admin123** para 6.0 e posterior,**Sourcefire** para pré-6.0.
3. Conclua a configuração do sistema conforme solicitado, que ocorre nesta ordem: Leia e aceite o Contrato de Licença de Usuário Final (EULA).Altere a senha do administrador.Configure o endereço de gerenciamento e as configurações de DNS, conforme solicitado. **Note**: Você pode configurar os endereços de gerenciamento IPv4 e IPv6.Aqui está um exemplo:

   ```
   System initialization in progress. Please stand by. You must change the password
    for 'admin' to continue. Enter new password: <new password>
   Confirm new password: <repeat password>
   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]:
   Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
   Enter an IPv4 address for the management interface [192.168.45.45]:198.51.100.3
   Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0
   Enter the IPv4 default gateway for the management interface []: 198.51.100.1
   Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
   Enter a comma-separated list of DNS servers or 'none' []:
   198.51.100.15, 198.51.100.14 Enter a comma-separated list of search domains or 'none'
   [example.net]: example.com If your networking information has changed, you will need to
   reconnect. For HTTP Proxy configuration, run 'configure network http-proxy'
   ```
4. Aguarde até que o sistema se reconfigure.

Configure o FireSIGHT Management Center

Para gerenciar um módulo ASA SFR e uma política de segurança, você deve registrá-lo em um FireSIGHT Management Center. Consulte Registrar um dispositivo com um FireSIGHT Management Center para obter mais informações. Não é possível executar essas ações com um FireSIGHT Management Center:

- Configurar as interfaces do módulo ASA SFR
- Desligar, reiniciar ou gerenciar de outra forma os processos do módulo ASA SFR
- Criar backups ou restaurar backups para os dispositivos do módulo ASA SFR
- Gravar regras de controle de acesso para corresponder o tráfego com o uso de condições de marca de VLAN

Redirecionar tráfego para o módulo SFR

Para redirecionar o tráfego para o módulo ASA SFR, você deve criar uma política de serviço que identifique o tráfego específico. Conclua estes passos para redirecionar o tráfego para um módulo ASA SFR:

1. Selecione o tráfego que deve ser identificado com o comando **access-list** comando. Neste exemplo, todo o tráfego de todas as interfaces é redirecionado. Você também pode fazer isso para tráfego específico.

   ```
   ciscoasa(config)# access-list sfr_redirect extended permit ip any any
   ```
2. Crie um mapa de classe para corresponder o tráfego em uma lista de acesso:

   ```
   ciscoasa(config)# class-map sfr
   ciscoasa(config-cmap)# match access-list sfr_redirect
   ```
3. Especifique o modo de implantação. Você pode configurar seu dispositivo em um modo de implantação passivo (somente monitor) ou em linha (normal).
   Note: Não é possível configurar um modo passivo e um modo em linha ao mesmo tempo no ASA. Somente um tipo de política de segurança é permitido.Em uma implantação em linha, o módulo SFR inspeciona o tráfego com base na política de controle de acesso e fornece o veredito ao ASA para tomar a ação apropriada (Permitir, Negar e assim por diante) no fluxo de tráfego. Este exemplo mostra como criar um mapa de políticas e configurar o módulo ASA SFR no modo em linha. Verifique se o **global_policy** está configurado com outra configuração de módulo**(show run policy-map global_policy, show run service-policy)**, primeiro redefina/remova a política_global para a configuração de outro módulo e, em seguida, reconfigure a **global_policy**.

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

   Em uma implantação passiva, uma cópia do tráfego é enviada ao módulo de serviço SFR, mas não é devolvida ao ASA. O modo passivo permite exibir as ações que o módulo SFR teria concluído em relação ao tráfego. Ele também permite avaliar o conteúdo do tráfego, sem causar impacto na rede.

   Se desejar configurar o módulo SFR no modo passivo, use o comando **monitor-only** palavra-chave (como mostrado no próximo exemplo). Se você não incluir a palavra-chave, o tráfego

será enviado no modo em linha.

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

aviso: O **monitor-only** o modo não permite que o módulo de serviço SFR negue ou bloqueie o tráfego mal-intencionado.**Caution**: Pode ser possível configurar um ASA no modo *somente monitor* com o uso do nível de interface **traffic-forward sfr monitor-only** comando; no entanto, essa configuração é meramente para funcionalidade de demonstração e não deve ser usada em um ASA de produção. Quaisquer problemas encontrados neste recurso de demonstração não são suportados pelo Cisco Technical Assistance Center (TAC). Se desejar implantar o serviço ASA SFR no modo passivo, configure-o com o uso de um *mapa de políticas*.

4. Especifique um local e aplique a política. Você pode aplicar uma política globalmente ou em uma interface. Para substituir a política global em uma interface, você pode aplicar uma política de serviço a essa interface.

   O **global** a palavra-chave aplica o mapa de política a todas as interfaces e **interface** a palavra-chave aplica a política a uma interface. Apenas uma política global é permitida. Neste exemplo, a política é aplicada globalmente:

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

   Caution: O mapa de políticas **global_policy** é uma política padrão. Se você usar essa política e quiser removê-la no dispositivo para solucionar problemas, certifique-se de que entendeu sua implicação.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

- Você pode executar este comando (**debug module-boot**) para ativar a depuração no início da instalação da imagem de inicialização do SFR.
- Se o ASA ficou preso no modo de recuperação e o console não foi ativado, tente este comando (**sw-module module sfr recover stop**).
- Se o módulo SFR não puder sair do estado de recuperação, você poderá tentar recarregar o ASA **(reload quick)**. (Se o tráfego passa, ele pode causar distúrbios na rede). Se Ainda houver um SFR preso no estado de recuperação, você poderá desligar o ASA e **unplug the SSD** e inicie o ASA. Verifique o status do módulo e ele deve estar no estado INIT. Novamente, desligue o ASA, **insert the SSD** e inicie o ASA. você pode iniciar a reimagem do módulo ASA SFR.

Informações Relacionadas

- Cisco Secure IPS - Recursos do Cisco NGIPS
- Registre um dispositivo com um FireSIGHT Management Center
- Guia de início rápido do módulo Cisco ASA FirePOWER
- Implantação do FireSIGHT Management Center no VMware ESXi

- Suporte Técnico e Documentação - Cisco Systems