Instale e configurar um Módulo de serviços de FirePOWER em uma plataforma ASA

Índice

Introdução

Este documento descreve como instalar e configurar um módulo de Cisco FirePOWER (SFR) que seja executado em uma ferramenta de segurança adaptável de Cisco (ASA) e como registrar o módulo SFR com o centro de gerenciamento de Cisco FireSIGHT.

Pré-requisitos

Requisitos

Cisco recomenda que sua reunião do sistema estas exigências antes que você tente os procedimentos que estão descritos neste documento:

- Assegure-se de que você tenha pelo menos 3GB do espaço livre na movimentação instantânea (disco 0), além do que o tamanho do software da bota.
- Assegure-se de que você tenha o acesso ao modo de exec privilegiado. A fim alcançar o modo de exec privilegiado, inscreva o **comando enable no** CLI. Se uma senha não foi ajustada, a seguir pressione **entram**:

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

Componentes Utilizados

A fim instalar os serviços de FirePOWER em Cisco ASA, estes componentes são exigidos:

- Versão de software 9.2.2 de Cisco ASA ou mais atrasado
- Plataformas ASA Cisco 5512-X com 5555-X
- Versão de software 5.3.1 de FirePOWER ou mais atrasado

> **Note**: Se você quer instalar serviços de FirePOWER (SFR) em um módulo de hardware ASA 5585-X, leia a instalação de serviços de FirePOWER (SFR) no módulo de hardware ASA 5585-X.

Estes componentes são exigidos no centro de gerenciamento de Cisco FireSIGHT:

- Versão de software 5.3.1 de FirePOWER ou mais atrasado
- Centro de gerenciamento FS2000, FS4000 ou dispositivo virtual de FireSIGHT

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

O módulo de Cisco ASA FirePOWER, igualmente conhecido como o ASA SFR, proporciona serviços de firewall da próxima geração, como:

- Sistema da prevenção de intrusão da próxima geração (NGIPS)
- Visibilidade do aplicativo e controle (AVC)
- Filtragem URL
- Proteção avançada do malware (AMP)

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

Antes de Começar

Considere esta informação importante antes que você tente os procedimentos que estão descritos neste documento:

- Se você tem uma política de serviço ativo que reoriente o tráfego a um módulo ciente do Intrusion Prevention System (IPS) /Context (CX) (esse você substituiu com o ASA SFR), você deve removê-lo antes que você configure a política de serviços ASA SFR.

- Você deve fechar todos os módulos de outro software que forem executado atualmente. Um dispositivo pode executar um único módulo de software em um momento. Você deve fazer este do ASA CLI. Por exemplo, estes comandos fecham e desinstalam o módulo de software IPS, e recarregam então o ASA:

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

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

Os comandos que são usados a fim remover o módulo CX são os mesmos, a não ser que a palavra-chave do **cxsc** seja usada em vez dos **IP**:

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

- Quando você nova imagem um módulo, usar a mesma **parada programada** e **desinstalar os** comandos que estão usados a fim remover uma imagem velha SFR. Aqui está um exemplo:

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

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

Tip: A fim determinar o estado de um módulo no ASA, inscreva o **comando show module**.

Instalação

Esta seção descreve como instalar o módulo SFR no ASA e como estabelecer a imagem de boot ASA SFR.

Instale o módulo SFR no ASA

Termine estas etapas a fim instalar o módulo SFR no ASA:

1. Transfira o software do sistema ASA SFR do cisco.com a um HTTP, a um HTTPS, ou a um servidor FTP que seja acessível da interface de gerenciamento ASA SFR.
2. Transfira a imagem de boot ao dispositivo. Você pode usar o Cisco Adaptive Security Device Manager (ASDM) ou o ASA CLI a fim transferir a imagem de boot ao dispositivo. **Note**: Não transfira o software do sistema; é transferido mais tarde à movimentação de circuito integrado (SSD).Termine estas etapas a fim transferir a imagem de boot através do ASDM: Transfira a imagem de boot a sua estação de trabalho, ou coloque-a em um server FTP, TFTP, HTTP, HTTPS, de bloqueio de mensagem de servidor (SMB), ou de Secure Copy (SCP).Escolha **ferramentas > gerenciamento de arquivos no** ASDM.Escolha o comando apropriado de transferência de arquivo, *entre o PC local e o flash* ou *entre o servidor remoto e o flash*.Transfira o software da bota à movimentação instantânea (disco 0) no ASA.Termine estas etapas a fim transferir a imagem de boot através do ASA CLI:Transfira a imagem de boot em um FTP, em um TFTP, em um HTTP, ou em um servidor HTTPS.Inscreva o **comando copy no** CLI a fim transferir a imagem de boot à movimentação instantânea. Está aqui um exemplo que use o protocolo HTTP (substitua o **<HTTP_Server>** com seu endereço IP do servidor ou nome de host):
   ```
   ciscoasa# copy http://<HTTP_SERVER>/asasfr-5500x-boot-5.3.1-152.img disk0:/asasfr-5500x-boot-5.3.1-152.img
   ```
3. Incorpore este comando a fim configurar o lugar da imagem de boot ASA SFR na movimentação do flash 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. Incorpore este comando a fim carregar a imagem de boot ASA SFR:

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

Durante este tempo, se você permite **debugar a inicialização de módulo no** ASA, estes debuga são imprimidos:

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

5. Espere aproximadamente 5 a 15 minutos pelo módulo ASA SFR para carreg acima, e para abrir então uma sessão de console à imagem de boot operacional ASA SFR.

Estabelecer a imagem de boot ASA SFR

Termine estas etapas a fim estabelecer o a imagem de boot recentemente instalada ASA SFR:

1. A imprensa **entra** depois que você abre uma sessão a fim alcançar a alerta de login. **Note**: O nome de usuário padrão é **admin**, e a senha padrão é **Admin123**.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 de módulo ASA SFR não terminou, o comando session falha e uma mensagem parece indicar que o sistema é incapaz de conectar sobre TTYS1. Se isto ocorre, espere a inicialização de módulo para terminar outra vez e tentar.

2. Inscreva o **comando setup** a fim 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 é alertado então para esta informação:**Nome de host** - O nome de host pode ser até 65 caráteres alfanuméricos, sem espaços. O uso dos hífens é permitido.**Endereço de rede** - O endereço de rede pode ser endereços estáticos do IPv4 ou do IPv6. Você pode igualmente usar o DHCP para o IPv4, ou a configuração automática apátrida do IPv6.**Informação de DNS** - Você deve identificar pelo menos um server do Domain Name System (DNS), e você pode igualmente ajustar o Domain Name e procurar o domínio.**Informação de NTP** - Você pode permitir o Network Time Protocol (NTP) e configurar os servidores de NTP a fim ajustar o tempo de sistema.

3. Inscreva o **comando install do sistema** a fim instalar a imagem de software de sistema:

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

Inclua a opção do **noconfirm** se você não quer responder aos mensagens de confirmação. Substitua a palavra-chave **URL** com o lugar do arquivo **.package**. Aqui está um exemplo:

```
asasfr-boot >system install http://<HTTP_SERVER>/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.
```

Note: Quando a instalação estiver completa, as repartições do sistema. Permita que dez ou mais minutos para a instalação do componente do aplicativo e para que os serviços ASA SFR comecem. A saída do comando do **sfr do módulo show** deve indicar que todos os processos estão **acima**.

Configurar

Esta seção descreve como configurar o software de FirePOWER e o centro de gerenciamento de FireSIGHT, e como reorientar o tráfego ao módulo SFR.

Configurar o software de FirePOWER

Termine estas etapas a fim configurar o software de FirePOWER:

1. Abra uma sessão ao módulo ASA SFR.
   Note: Uma alerta de login diferente aparece agora porque o início de uma sessão ocorre em um módulo completo-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. Entre com o admin de nome de usuário e a senha **Admin123**.
3. Termine a configuração de sistema como alertada, que ocorre nesta ordem: Leia e aceite o contrato de licença do utilizador final (EULA).Mude a senha de admin.Configurar o endereço de gerenciamento e ajustes DNS, como alertados. **Note**: Você pode configurar endereços de

gerenciamento do IPv4 e do IPv6.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:
```

4. Espera para que o sistema reconfigure-se.

Configurar o centro de gerenciamento de FireSIGHT

A fim controlar um módulo e a política de segurança ASA SFR, você deve registrar-la com um centro de gerenciamento de FireSIGHT. Você não pode executar estas ações com um centro de gerenciamento de FireSIGHT:

- Configurar as interfaces de módulo ASA SFR
- Feche, reinicie, ou controle de outra maneira os processos do módulo ASA SFR
- Crie backup, ou restaure backup, aos dispositivos de módulo ASA SFR
- Escreva regras do controle de acesso a fim combinar o tráfego com o uso de condições da etiqueta VLAN

Reoriente o tráfego ao módulo SFR

A fim reorientar o tráfego ao módulo ASA SFR, você deve criar uma política de serviços que identifique o tráfego específico. Termine estas etapas a fim reorientar o tráfego a um módulo ASA SFR:

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

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

2. Crie um mapa de classe a fim combinar o tráfego em uma lista de acessos:

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

3. Especifique o modo do desenvolvimento. Você pode configurar seu dispositivo em um modo (normal) passivo (monitor-somente) ou inline do desenvolvimento.
   Note: Você não pode configurar um modo passivo e o modo inline ao mesmo tempo no ASA. Somente um tipo de política de segurança é permitido.Em um desenvolvimento inline, depois que o tráfego indesejado está deixado cair e todas as outras ações que estiverem aplicadas pela política estão executados, o tráfego é retornado ao ASA para o processamento adicional e a transmissão final. Este exemplo mostra como criar um mapa de política e configurar o módulo ASA SFR no modo inline:

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

   Em um desenvolvimento passivo, uma cópia do tráfego é enviada ao módulo de serviço

SFR, mas não é retornada ao ASA. O modo passivo permite que você ver as ações que o módulo SFR terminaria com respeito ao tráfego. Igualmente permite que você avalie o índice do tráfego, sem um impacto à rede.

Se você quer configurar o módulo SFR no modo passivo, use a palavra-chave do **monitor-somente** (segundo as indicações do exemplo seguinte). Se você não inclui a palavra-chave, o tráfego está enviado no modo inline.

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

aviso: O modo de **monitor-somente** não permite que o módulo de serviço SFR negue ou obstrua o tráfego malicioso.**Caution**: Pôde ser possível configurar um ASA no modo de *monitor-somente* com o uso do comando de **monitor-somente tráfego-dianteiro do sfr do relação-**nível; contudo, esta configuração é puramente para a funcionalidade da demonstração e não deve ser usada em uma produção ASA. Nenhuma edições que são encontradas nesta característica da demonstração não são apoiadas pelo centro de assistência técnica da Cisco (TAC). Se você deseja distribuir o serviço ASA SFR no modo passivo, configurar-lo com o uso de um *mapa de política*.

4. Especifique um lugar e aplique a política. Você pode aplicar uma política globalmente ou em uma relação. A fim cancelar a política global em uma relação, você pode aplicar uma política de serviços a essa relação.

   A palavra-chave **global** aplica o mapa de política a todas as relações, e a palavra-chave da **relação** aplica a política a uma relação. Somente uma política global é permitida. Neste exemplo, a política é aplicada globalmente:

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

   Caution: **O global_policy do** mapa de política é uma política padrão. Se você usa esta política e a quer a remover em seu dispositivo para propósitos de Troubleshooting, assegure-se de que você compreenda sua implicação.

Verificar

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

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Registrar um dispositivo com um centro de gerenciamento de FireSIGHT
- Desenvolvimento do centro de gerenciamento de FireSIGHT em VMware ESXi
- Cenários de configuração do Gerenciamento de IPS em um módulo ips 5500-X
- Suporte Técnico e Documentação - Cisco Systems