Recrie uma defesa contra ameaças de firewall seguro para as séries 1000, 2100 e 3100

Contents

Introdução

Este documento descreve um exemplo de um procedimento de recriação para o Secure Firewall Threat Defense (anteriormente Firepower Threat Defense).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Não há requisitos específicos para este guia

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Firewall Threat Defense 2110 (FTD) Versão 7.2.4

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

Informações de Apoio

Os requisitos específicos deste documento incluem:

- Um cabo de console conectado ao FTD
- Um servidor TFTP com o pacote de instalação (**.SPA**) já carregado

Este procedimento de recriação é compatível com dispositivos:

- Cisco Secure Firewall Threat Defense 1000 Series
- Cisco Secure Firewall Threat Defense 2100 Series

- Cisco Secure Firewall Threat Defense série 3100

Antes de Começar

1. Um procedimento de recriação apaga todas as configurações anteriores. Para restaurar qualquer configuração, gere um backup antes de iniciar este procedimento.
2. Este procedimento aplica-se somente a Firewalls que executam o software FTD.
3. Verifique se o modelo é compatível com este procedimento.

Configurar

Etapa 1. Formatar o equipamento:

I. Conecte-se à porta de console do seu equipamento e crie uma conexão de console.

II. Faça login na CLI do chassi FXOS.

III. Digite **connect local-mgmt** para ir para o console de gerenciamento.

III. Use o comando **format everything** para excluir todas as configurações e imagens de inicialização no dispositivo.

III. Digite **yes** para confirmar o procedimento

```
firepower-2110# connect local-mgmt admin
firepower-2110(local-mgmt)# format everything
All configuration and bootable images will be lost.
Do you still want to format? (yes/no):yes
```

Etapa 2. Interrompa o processo de inicialização pressionando a tecla ESC para entrar no modo ROMMON:

```
********************************************************************************
Cisco System ROMMON, Version 1.0.12, RELEASE SOFTWARE
Copyright (c) 1994-2019  by Cisco Systems, Inc.
Compiled Mon 06/17/2019 16:23:23.36 by builder
********************************************************************************

Current image running: Boot ROM0
Last reset cause: ResetRequest (0x00001000)
DIMM_1/1 : Present
DIMM_2/1 : Absent

Platform FPR-2110 with 16384 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 18:59:f5:d9:6a:00

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.


rommon 1 >
```

Etapa 3. Preencha os parâmetros de rede e armazenamento remoto com suas configurações para preparar o download TFTP:

I. Os parâmetros a preencher são:

A. ADDRESS=*ip_address*

B. NETMASK=*netmask*

C. GATEWAY=*gateway_ip*

D. SERVER=*remote_storage_server*

E. IMAGE=*path_to_the_file*

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.


rommon 1 > ADDRESS=10.122.187.166
rommon 2 > NETMASK=255.255.255.224
rommon 3 > GATEWAY=10.122.187.161
rommon 4 > SERVER=10.207.204.10
rommon 5 > IMAGE=cisco-ftd-fp2k.7.2.4-165.SPA
rommon 6 >
```

Cuidado: o modo ROMMON suporta apenas o protocolo TFTP, o FTP, SCP e SFTP e o USB não são suportados no processo de inicialização inicial.

Etapa 4. Digite set para confirmar as configurações fornecidas:

```
rommon 6 > set
     ADDRESS=10.122.187.166
     NETMASK=255.255.255.224
     GATEWAY=10.122.187.161
     SERVER=10.207.204.10
     IMAGE=cisco-ftd-fp2k.7.2.4-165.SPA
     CONFIG=
     PS1="rommon ! > "
```

Observação: verifique se as informações fornecidas estão corretas e, se você notar um erro, ajuste o parâmetro e o tipo **definido** novamente.

Etapa 5. Digite **sync** para aplicar as configurações de rede e armazenamento remoto:

```
rommon 7 > sync
rommon 8 >
```

Etapa 6. Inicie o processo de inicialização com o comando tftp -b:

```
rommon 8 > tftp -b
Enable boot bundle: tftp_reqsize = 268435456

            ADDRESS: 10.122.187.166
            NETMASK: 255.255.255.224
            GATEWAY: 10.122.187.161
             SERVER: 10.207.204.10
              IMAGE: cisco-ftd-fp2k.7.2.4-165.SPA
           MACADDR: 18:59:f5:d9:6a:00
         VERBOSITY: Progress
             RETRY: 40
        PKTTIMEOUT: 7200
           BLKSIZE: 1460
          CHECKSUM: Yes
              PORT: GbE/1
           PHYMODE: Auto Detect

link up
Receiving cisco-ftd-fp2k.7.2.4-165.SPA from 10.207.204.10!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Observação: se o download da imagem de inicialização for bem-sucedido, você verá vários pontos de exclamação (**!**) confirmando o download. Caso contrário, verifique se suas configurações são apropriadas ou valide se o dispositivo pode acessar o servidor de armazenamento remoto.

Passo 7. Quando o sistema for ativado, faça login no dispositivo usando as credenciais padrão (admin/Admin123) e altere a senha do equipamento:

```
firepower-2110 login: admin
Password:
Successful login attempts for user 'admin' : 1
Enter new password:
Confirm new password:
Your password was updated successfully.
```

Observação: esse erro pode ser exibido enquanto a configuração inicial estiver ocorrendo. No entanto, ele será apagado após a instalação do software de defesa contra ameaças, conforme descrito nas etapas posteriores.

```
Jun 14 21:37:17 firepower-2110 FPRM: <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>
nfra-version-missing][org-root/fw-infra-pack-default] Bundle version in firmwar
 re-install
```

Etapa 8. Configure o IP da interface de gerenciamento:

I. Vá para o escopo da malha com o comando **scope fabric-interconnect a**

II. Defina a configuração do IP de gerenciamento com o comando **set out-of-band static ip** *ip* netmask *netmask* gw *gateway*

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # set out-of-band static ip 10.122.187.168 netmask 25
10.122.187.161
Warning: When committed, this change may disconnect the current CLI session.
Use commit-buffer command to commit the changes.
firepower-2110 /fabric-interconnect* # commit-buffer
```

Etapa 9. Faça o download do pacote de instalação do Threat Defense:

I. Mude para o escopo de firmware com o comando **scope firmware**

II. Faça o download do pacote de instalação:

R. Se estiver usando um USB, você pode usar o comando **download image** usbA:package_name

B. Se você estiver usando um servidor de armazenamento remoto compatível, poderá usar o comando **download image** tftp/ftp/scp/sftp://path_to_your_package

```
firepower-2110# scope firmware
firepower-2110 /firmware # download image tftp://10.207.204.10/cisco-ftd-fp2k.7.2.4-165.SP
firepower-2110 /firmware #
```

Observação: ao usar servidores de armazenamento remotos, é necessário usar caminhos absolutos na sintaxe do comando, conforme exibido no exemplo.

Etapa 10. Valide o progresso do download com o comando **show download-task**:

```
firepower-2110 /firmware # show download-task

Download task:
    File Name Protocol Server          Port       Userid          State
    --------- -------- --------------- ---------- --------------- -----
    cisco-ftd-fp2k.7.2.4-165.SPA
              Tftp     10.207.204.10            0                 Downloaded
```

Observação: depois que o estado de download mudar para *Download*, você poderá prosseguir para a próxima etapa.

Etapa 11. Verifique se o pacote já está na lista de firmware com o comando show package:

```
firepower-2110 /firmware # show package
Name                                                 Package-Vers
---------------------------------------------------- ------------
cisco-ftd-fp2k.7.2.4-165.SPA                         7.2.4-165
```

Observação: copie a *versão do pacote* como ela será usada na instalação do software Threat Defense.

Etapa 12. Instale o software Threat Defense para finalizar a recriação:

I. Vá para o escopo de instalação com o comando **scope autoinstall**.

II. Continue com a instalação do software de defesa contra ameaças com o comando **install security-pack version** *version* **force**

III. Dois prompts de confirmação serão exibidos no console. Confirme ambos digitando **yes**.

```
firepower-2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 7.2.4 force

Invalid software pack
Please contact technical support for help                                    5

The system is currently installed with security software package not set, which has:
   - The platform version: not set
If you proceed with the upgrade 7.2.4-165, it will do the following:
   - upgrade to the new platform version 2.12.0.499
   - install with CSP ftd version 7.2.4.165
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
(1) Review current critical/major faults
(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggered the install of software package version 7.2.4-165
Install started. This will take several minutes.
For monitoring the upgrade progress, please enter 'show' or 'show detail' command.
```

Cuidado: o processo de recriação demora até 45 minutos; lembre-se de que o firewall será reinicializado durante a instalação.

Validação

Valide o processo de atualização com o comando **show detail**:

```
firepower-2110 /firmware/auto-install # show detail

Firmware Auto-Install:
    Package-Vers: 7.2.4-165
    Oper State: Scheduled
    Installation Time: 2023-06-14T22:07:28.777
    Upgrade State: Validating Images
    Upgrade Status: validating the software package
    Validation Software Pack Status:
    Firmware Upgrade Status: Ok
    Firmware Upgrade Message:
    Current Task: Validating the application pack(FSM-STAGE:sam:dme:FirmwareSyst
emDeploy:ValidateApplicationPack)
firepower-2110 /firmware/auto-install #
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.