在ASA 5585-X硬體模組上安裝SFR模組

目錄

簡介

ASA FirePOWER模組（也稱為ASA SFR）提供下一代防火牆服務，包括下一代IPS(NGIPS)、應用可視性與可控性(AVC)、URL過濾和高級惡意軟體防護(AMP)。 您可以在單情景或多情景模式下以及在路由或透明模式下使用該模組。本文檔介紹ASA 5585-X硬體模組上FirePOWER(SFR)模組的必備條件和安裝過程。它還提供了向FireSIGHT管理中心註冊SFR模組的步驟。

> **附註**：FirePOWER(SFR)服務駐留在ASA 5585-X中的硬體模組上，而ASA 5512-X至5555-X系列裝置上的FirePOWER服務安裝在軟體模組上，導致安裝過程不同。

必要條件

需求

本文檔中的說明要求訪問特權EXEC模式。若要存取許可權EXEC模式，請輸入enable指令。如果未設定密碼，只需按Enter鍵。

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

要在ASA上安裝FirePOWER服務，需要以下元件：

- ASA軟體9.2.2版或更高版本
- ASA 5585-X平台
- FirePOWER模組的管理介面可訪問的TFTP伺服器
- FireSIGHT管理中心（版本5.3.1或更高版本）

附註：本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

組態

開始之前

假設ASA SSM始終佔用ASA 5585-X機箱的兩個插槽之一，如果您有一個除FirePOWER(SFR)服務SSP之外的硬體模組，例如SSP-CX（情景感知）或AIP-SSM（高級檢測和預防安全），則必須解除安裝另一個模組以為SSP-SFR留出空間。刪除硬體模組之前，請運行以下命令來關閉模組：

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

佈線和管理

- 您無法通過ASA 5585-X上的ASA控制檯訪問SFR模組的串列埠。
- 調配SFR模組後，您可以使用「session 1」命令將會話連線到刀片。
- 為了在ASA 5585-X上完全重新映像SFR模組，您必須使用管理乙太網介面和串列管理埠上的控制檯會話（位於SFR模組上，與ASA的管理介面和控制檯分離）。

提示：要查詢ASA上模組的狀態，請運行「show module 1 details」命令，該命令將檢索SFR模組的管理IP和關聯的防禦中心。

在ASA上安裝FirePOWER(SFR)模組

1.將ASA FirePOWER SFR模組初始載入程式映像從Cisco.com下載到TFTP伺服器，該伺服器可通過ASA FirePOWER管理介面訪問。映像名稱類似「asasfr-boot-5.3.1-152.img」

2.將ASA FirePOWER系統軟體從Cisco.com下載到可從ASA FirePOWER管理介面訪問的HTTP、HTTPS或FTP伺服器。

3.重新啟動SFR模組

選項1:如果您沒有SFR模組的密碼，則可以從ASA發出以下命令以重新啟動該模組。

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

選項2:如果您有SFR模組的密碼，可以直接從命令列重新啟動感測器。

```
Sourcefire3D login: admin
Password:

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

>system reboot
```

4.使用ESCAPE或終端會話軟體的break序列中斷SFR模組的引導過程，將模組放入ROMMON中。

```
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.使用IP地址配置SFR模組管理介面，並指示TFTP伺服器的位置以及載入程式映像的TFTP路徑。輸入以下命令設定介面的IP地址並檢索TFTP映像：

- set
- ADDRESS = Your_IP_Address
- GATEWAY = Your_Gateway
- SERVER = Your_TFTP_Server
- IMAGE = Your_TFTP_Filepath
-
- tftp

!使用的IP地址資訊示例。更新您的環境。

```
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.登入到初始啟動映像。以admin身份登入，密碼為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.使用初始啟動映像在模組的管理介面上配置IP地址。輸入setup命令進入嚮導。系統將提示您輸入以下資訊：

- **主機名**:最多65個字母數字字元，無空格。允許使用連字元。
- **網路地址**:您可以設定靜態IPv4或IPv6地址，或者使用DHCP（用於IPv4）或IPv6無狀態自動配置。
- **DNS資訊**:您必須至少識別一個DNS伺服器，並且還可以設定域名和搜尋域。
- **NTP資訊**:您可以啟用NTP並配置NTP伺服器來設定系統時間。

!使用的示例資訊。更新您的環境。

```
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.使用**system install**命令，使用啟動映像提取並安裝系統軟體映像。如果您不想響應確認消息，請包括**noconfirm**選項。將*url*關鍵字替換為.pkg檔案的位置。

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

例如，

```
> 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 ...
```

附註：安裝在20到30分鐘內完成時，系統將提示您按Enter鍵重新啟動。為應用程式元件安裝和ASA FirePOWER服務啟動留出10分鐘或更長時間。show module 1 details輸出應將所有進程顯示為Up。

安裝期間的模組狀態

```
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
```

成功安裝後的模組狀態

```
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
```

組態

配置FirePOWER軟體

1.您可以通過以下其中一個外部埠連線到ASA 5585-X FirePOWER模組：

- ASA FirePOWER控制檯埠
- 使用SSH的ASA FirePOWER管理1/0介面

附註：使用session sfr命令無法通過ASA背板訪問ASA FirePOWER硬體模組CLI。

2.通過控制檯訪問FirePOWER模組後，使用使用者名稱**admin**和密碼**Sourcefire**登入。

```
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.

>
```

配置FireSIGHT管理中心

為了管理ASA FirePOWER模組和安全策略，您必須向FireSIGHT管理中心註冊該模組。不能使用

FireSIGHT管理中心執行以下操作：

- 無法配置ASA FirePOWER介面。
- 無法關閉、重新啟動或以其他方式管理ASA FirePOWER進程。
- 無法從ASA FirePOWER裝置建立備份或將備份還原到ASA FirePOWER裝置。
- 無法使用VLAN標籤條件寫入訪問控制規則以匹配流量。

將流量重定向至SFR模組

通過建立標識特定流量的服務策略，可將流量重定向到ASA FirePOWER模組。若要將流量重新導向到FirePOWER模組，請執行以下步驟：

第1步：選擇流量

首先，使用access-list命令選擇流量。在以下示例中，我們正在重定向來自所有介面的所有流量。您也可以針對特定流量執行此操作。

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

第2步：匹配流量

以下示例展示如何建立類對映並匹配訪問清單上的流量：

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

步驟3:指定操作

您可以在被動（「僅監控」）或內聯部署中配置裝置。您無法在ASA上同時配置僅監控模式和正常內聯模式。只允許一種安全策略。

內嵌模式

在內聯部署中，丟棄不需要的流量並執行策略應用的任何其他操作後，流量將返回到ASA以進行進一步處理和最終傳輸。以下示例展示如何建立策略對映並在內聯模式下配置FirePOWER模組：

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

被動模式

在被動部署中，

- 流量的副本傳送到裝置，但不返回到ASA。
- 被動模式允許您檢視裝置對流量會執行的操作，並讓您評估流量的內容，而不會影響網路。

如果要將FirePOWER模組配置為被動模式，請使用monitor-only關鍵字，如下所示。如果不包含關鍵字，則流量以內嵌模式傳送。

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

第4步：指定位置

最後一步是應用該策略。可以全域性應用策略，也可以在介面上應用策略。可以通過將服務策略應用到介面來覆蓋該介面上的全域性策略。

global關鍵字將策略對映應用於所有介面，interface將策略應用於一個介面。只允許一個全域性策略。在以下示例中，策略全域性應用：

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

> **注意**：策略對映global_policy是預設策略。如果您使用此策略，並想要出於故障排除目的在裝置上刪除此策略，請確保您瞭解其含義。

相關檔案

- 向FireSIGHT管理中心註冊裝置
- 在VMware ESXi上部署FireSIGHT管理中心
- 5500-X IPS模組上的IPS管理配置方案