

在 ASA 平台上安裝和設定 FirePOWER 服務模組

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[開始之前](#)

[安裝](#)

[在ASA上安裝SFR模組](#)

[設定ASA SFR引導映像](#)

[設定](#)

[配置FirePOWER軟體](#)

[配置FireSIGHT管理中心](#)

[將流量重定向至SFR模組](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何在Cisco ASA上安裝並配置Cisco FirePOWER(SFR)模組，以及如何使用Cisco FireSIGHT註冊SFR模組。

必要條件

需求

思科建議您在嘗試執行本檔案所述的程式之前，先滿足以下要求：

- 除了啟動軟體的大小之外，請確保快閃記憶體驅動器(disk0)上至少有3GB的可用空間。
- 確保您有權訪問特權執行模式。要訪問特權EXEC模式，請在CLI中 `enable` 輸入該命令。如果未設定密碼，請按 `Enter`下：

```
<#root>
```

```
ciscoasa>
```

enable

Password:
ciscoasa#

採用元件

要在Cisco ASA上安裝FirePOWER服務，需要以下元件：

- Cisco ASA軟體版本9.2.2或更高版本
- Cisco ASA平台5512-X至5555-X
- FirePOWER軟體5.3.1版或更高版本



註：如果要在ASA 5585-X硬體模組上安裝FirePOWER(SFR)服務，請參閱[在ASA 5585-X硬體模組上安裝SFR模組](#)。

Cisco FireSIGHT管理中心需要以下元件：

- FirePOWER軟體5.3.1版或更高版本
- FireSIGHT管理中心FS2000、FS4000或虛擬裝置

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。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco ASA FirePOWER模組（也稱為ASA SFR）提供下一代防火牆服務，例如：

- 新世代入侵防禦系統(NGIPS)
- 應用可視性與可控性(AVC)
- 篩選URL
- 進階惡意軟體防護 (AMP)



注意：您可以在單情景或多情景模式以及路由或透明模式下使用ASA SFR模組。

開始之前

在嘗試本文檔中所述的步驟之前，請考慮以下重要資訊：

- 如果具有將流量重定向到入侵防禦系統(IPS)/情景感知(CX)模組 (已替換為ASA SFR) 的活動服務策略，則必須在配置ASA SFR服務策略之前將其刪除。
- 您必須關閉當前運行的所有其他軟體模組。裝置一次可以運行單個軟體模組。您必須從ASA CLI執行此操作。例如，這些命令關閉並解除安裝IPS軟體模組，然後重新載入ASA:

```
<#root>

ciscoasa#

sw-module module ips shutdown

ciscoasa#

sw-module module ips uninstall

ciscoasa#

reload
```

- 用於刪除CX模組的命令是相同的，不同之處在於使用關 **cxsc** 鍵字而不是以下命 **ips** 令：

```
<#root>
```

```
ciscoasa#
```

```
sw-module module cxsc shutdown
```

```
ciscoasa#
```

```
sw-module module cxsc uninstall
```

```
ciscoasa#
```

```
reload
```

- 重新映像模組時，請使 shutdown 用 uninstall 與刪除舊SFR映像相同的和命令。以下是範例：

```
<#root>
```

```
ciscoasa#
```

```
sw-module module sfr uninstall
```

- 如果ASA SFR模組用於多情景模式，請在系統執行空間中執行本文檔中介紹的步驟。



提示：要確定ASA上模組的狀態，請輸入命令 `show module` 。

安裝

本節介紹如何在ASA上安裝SFR模組以及如何設定ASA SFR引導映像。

在ASA上安裝SFR模組

完成以下步驟，以便在ASA上安裝SFR模組：

- 從Cisco.com將ASA SFR系統軟體下載到HTTP、HTTPS或FTP伺服器，該伺服器可通過ASA SFR管理介面訪問。
- 將啟動映像下載到裝置。您可以使用Cisco Adaptive Security Device Manager(ASDM)或ASA CLI將引導映像下載到裝置。



註：請勿傳輸系統軟體；稍後會將其下載到固態硬碟(SSD)。

完成以下步驟，以便通過ASDM下載啟動映像：

- a. 將啟動映像下載到您的工作站，或將其置於FTP、TFTP、HTTP、HTTPS、伺服器訊息塊(SMB)或安全複製(SCP)伺服器上。
- b. **Tools > File Management** ASDM的喬辛。
 - 選擇適當的File Transfer命令，*Between Local PC and Flash*或*Between Remote Server and Flash*。
 - 將引導軟體傳輸到ASA上的快閃記憶體驅動器(disk0)。

完成以下步驟，以便通過ASA CLI下載啟動映像：

- a. 在FTP、TFTP、HTTP或HTTPS伺服器上下載開機映像。
- b. 在CLI中 `copy` 輸入指令，將開機映像下載到快閃磁碟機。

以下是使用HTTP協定的示例(用您的服 `<HTTP_Server>` 務器IP地址或主機名替換)。對於FTP伺服器，URL如下所示：
`ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img .`

```
<#root>
```

```
ciscoasa#
```

```
copy http://<HTTP_SERVER>/asasfr-5500x-boot-5.3.1-152.img
disk0:/asasfr-5500x-boot-5.3.1-152.img
```

- 輸入以下命令可配置ASA SFR引導映像`在ASA快閃記憶體驅動器中的位置`：

```
<#root>
```

```
ciscoasa#
```

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

以下是範例：

```
<#root>
```

```
ciscoasa#
```

```
sw-module module sfr recover configure image disk0:
/asasfr-5500x-boot-5.3.1-152.img
```

- 輸入以下命令以載入ASA SFR啟動映像：

```
<#root>
```

ciscoasa#

sw-module module sfr recover boot

在此期間，如果在ASA上啟 debug module-boot 用，將會列印以下調試：

```
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
```

- 等待大約5到15分鐘以啟動ASA SFR模組，然後開啟可操作的ASA SFR啟動映像的控制檯會話。

設定ASA SFR引導映像

完成以下步驟，設定新安裝的ASA SFR引導映像：

- 開啟 **Enter** 會話後按進入登入提示。



註：預設使用者名稱是 **admin**Cisco IOS ID。密碼因軟體版本而異：**Adm!n123** 7.0.1版（僅限出廠新裝置）、**Admin123** 6.0版及更高版 **Sourcefire** 本6.0版之前的版本。

以下是範例：

```
<#root>

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
```



提示：如果ASA SFR模組引導尚未完成，則session命令將失敗，並顯示一條消息，指示系統無法通過TTYs1進行連線。如果發生這種情況，請等待模組引導完成，然後重試。

- 輸入命 **setup** 令以配置系統，以便安裝系統軟體包：

```
<#root>

asasfr-boot>
```


setup

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

然後系統會提示您輸入以下資訊：

- **Host name** — 主機名最多可以包含65個字母數字字元，不含空格。允許使用連字元。
- **Network address** — 網路地址可以是靜態IPv4或IPv6地址。您還可以將DHCP用於IPv4，或IPv6無狀態自動配置。
- **DNS information** — 您必須至少識別一個域名系統(DNS)伺服器，而且您還可以設定域名和搜尋域。
- **NTP information** — 可以啟用網路時間協定(NTP)並配置NTP伺服器以設定系統時間。

- 輸入命 `system install` 令以安裝系統軟體映像：

```
<#root>
```

```
asasfr-boot >
```

```
system install [noconfirm] url
```

如果您不 `noconfirm` 想響應確認消息，請包括此選項。將關鍵 `url` 字替換為檔案的位 `.pkg` 置。同樣地，您可以使用FTP、HTTP或HTTPS伺服器。以下是範例：

```
<#root>
```

```
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.
```

對於FTP伺服器，URL如下所示：`ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg`。

 **注意：**在安裝過程中RecoverSFR處於「安全」狀態。完成SFR模組的安裝最多可能需要一個小時左右。安裝完成後，系統重新啟動。為應用程式元件安裝和ASA SFR服務啟動留出10分鐘或更長時間。該命令的輸出表 `show module sfr` 示所有進程都已 Up完成。

設定

本節介紹如何配置FirePOWER軟體和FireSIGHT管理中心，以及如何將流量重定向到SFR模組。

配置FirePOWER軟體

完成以下步驟以配置FirePOWER軟體：

- 開啟ASA SFR模組的會話。



注意：現在顯示另一個登入提示，因為登入發生在功能完整的模組上。

以下是範例：

```
admin
```

```
<#root>
```

```
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:
```

- 使用使用者名稱和密碼登入，密碼因軟體版本而異：Adm!n123 對於7.0.1版(僅限出廠新設 Admin123 備)，對於6.0版及更高版Sourcefire 本 (對於6.0版之前)。
- 根據提示完成系統配置，按照以下順序執行：
 - a. 閱讀並接受終端使用者許可協定(EULA)。
 - b. 更改管理員密碼。
 - c. 根據提示配置管理地址和DNS設定。



注意：您可以同時配置IPv4和IPv6管理地址。

以下是範例：

```
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'
```

- 等待系統重新配置自身。

配置FireSIGHT管理中心

為了管理ASA SFR模組和安全策略，您必須向FireSIGHT管理中心註冊。有關詳細資訊，請參閱[向FireSIGHT管理中心註冊裝置](#)。您不能使用FireSIGHT管理中心執行這些操作：

- 配置ASA SFR模組介面
- 關閉、重新啟動或以其他方式管理ASA SFR模組進程
- 從ASA SFR模組裝置建立備份或將備份還原到
- 編寫訪問控制規則，使流量與使用VLAN標籤條件相匹配

將流量重定向至SFR模組

為了將流量重定向到ASA SFR模組，您必須建立標識特定流量的服務策略。完成以下步驟，將流量重新導向到ASA SFR模組：

- 選擇必須用命令標識的流 `access-list` 量。在此範例中，來自所有介面的所有流量都會重新導向。您也可以針對特定流量執行此操作。

```
<#root>
```

```
ciscoasa(config)#
```

```
access-list sfr_redirect extended permit ip any any
```

- 建立類別對映以匹配存取清單上的流量：

```
<#root>
```

```
ciscoasa(config)#
```

```
class-map sfr
```

```
ciscoasa(config-cmap)#
```

```
match access-list sfr_redirect
```

- 指定部署模式。您可以在被動（僅監控）或內聯（正常）部署模式下配置裝置。



註：您不能在ASA上同時配置被動模式和內聯模式。只允許一種安全策略。

- 在內聯部署中，SFR模組根據訪問控制策略檢查流量，並向ASA提供判定以對流量流採取相應操作（允許、拒絕等）。此示例說明如何建立策略對映並在內聯模式下配置ASA SFR模組。
- 請驗證當前配置 `global_policy` 的是其他模組配置(`show run policy-map global_policy, show run service-policy`)，然後先重置/刪除其他模組配置的`global_policy`，然後重新配 `global_policy`置。

```
<#root>
```

```
ciscoasa(config)#
```

```
policy-map global_policy
```

```
ciscoasa(config-pmap)#
```

```
class sfr
```

```
ciscoasa(config-pmap-c)#
```

```
sfr fail-open
```

- 在被动部署中，流量的副本被传送到SFR服务模组，但不会返回到ASA。被动模式允许您检视SFR模组针对流量应完成的操作。它还允许您评估流量的内容，而不会影响网络。

如果要將SFR模组配置為被动模式，請使用 **monitor-only** 關鍵字（如下一個示例所示）。如果不包含關鍵字，則流量以內嵌模式傳送。

```
<#root>
```

```
ciscoasa(config-pmap-c)#
```

```
sfr fail-open monitor-only
```



警告：此模 **monitor-only** 式不允許SFR服務模組拒絕或阻止惡意流量。



注意：可以使用interface-level命令在`monitor-only`模式下配置ASA；但是，此配置僅用於演示功 `traffic-forward sfr monitor-only` 能，不得在生產ASA上使用。思科技術協助中心(TAC)不支援此演示功能中發現的任何問題。如果您希望在被動模式下部署ASA SFR服務，請使用`policy-map`對其進行配置。

- 指定位置並應用策略。可以全域性應用策略，也可以在介面上應用策略。要覆蓋介面上的全域性策略，可以將服務策略應用於該介面。

關鍵 `global` 字將策略對映應用於所有介面，關鍵字 `interface` 將策略應用於一個介面。只允許一個全域性策略。在此示例中，策略被全域性應用：

```
<#root>
```

```
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希望在裝置上刪除它以進行故障排除，請確保您理解其含義。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

- 您可以運行此命令(`debug module-boot`)在SFR引導映像安裝開始時啟用調試。
- 如果ASA停滯在「恢復」模式，並且控制檯沒有啟動，則嘗試此命令(`sw-module module sfr recover stop`)。
- 如果SFR模組無法退出恢復狀態，則可以嘗試重新載入ASA (`reload quick`)。(如果流量通過，則可能導致網路干擾)。如果Still SFR停滯在恢復狀態，您可以關閉ASA和 **unplug the SSD** 卡並啟動ASA。檢查模組的狀態，它必須是INIT狀態。再次關閉ASA、卡 **insert the SSD** 並啟動ASA。您可以開始重新映像ASA SFR模組。

相關資訊

- [Cisco安全IPS - Cisco NGIPS功能](#)

- [向FireSIGHT管理中心註冊裝置](#)

-

[Cisco ASA FirePOWER模組快速入門手冊](#)

- [在VMware ESXi上部署FireSIGHT管理中心](#)

- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。