

ASA 플랫폼에 FirePOWER Services 모듈 설치 및 설정

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[시작하기 전에](#)

[Install](#)

[ASA에 SFR 모듈 설치](#)

[ASA SFR 부팅 이미지 설정](#)

[구성](#)

[firepower 소프트웨어 구성](#)

[FireSIGHT Management Center 구성](#)

[SFR 모듈로 트래픽 리디렉션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 Cisco ASA에 Cisco SFR(Firepower) 모듈을 설치 및 구성하고 Cisco FireSIGHT에 SFR 모듈을 등록하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 설명된 절차를 시도하기 전에 시스템이 다음 요구 사항을 충족하는 것이 좋습니다.

- 부트 소프트웨어의 크기 외에 플래시 드라이브(disk0)에 3GB 이상의 사용 가능한 공간이 있는지 확인합니다.
- 특별 권한 EXEC 모드에 액세스할 수 있는지 확인합니다. 특별 권한 EXEC 모드에 액세스하려면 `enable` 명령을 사용하여 CLI에 액세스합니다. 비밀번호가 설정되지 않은 경우 `Enter`:

```
<#root>
```

```
ciscoasa>
```


```
enable
```

Password:
ciscoasa#

사용되는 구성 요소

Cisco ASA에 Firepower 서비스를 설치하려면 다음 구성 요소가 필요합니다.

- Cisco ASA 소프트웨어 버전 9.2.2 이상
- Cisco ASA 플랫폼 5512-X~5555-X
- Firepower 소프트웨어 버전 5.3.1 이상

 참고: ASA 5585-X 하드웨어 모듈에 SFR(Firepower) 서비스를 설치하려면 ASA 5585-X 하드웨어 모듈에 [SFR 모듈 설치를 참조하십시오.](#)

Cisco FireSIGHT Management Center에는 다음 구성 요소가 필요합니다.


- Firepower 소프트웨어 버전 5.3.1 이상
- FireSIGHT Management Center FS2000, FS4000 또는 가상 어플라이언스

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

ASA SFR이라고도 하는 Cisco ASA Firepower 모듈은 다음과 같은 차세대 방화벽 서비스를 제공합니다.

- NGIPS(차세대 침입 방지 시스템)
- AVC(Application Visibility and Control)
- 필터 URL
- AMP(Advanced Malware Protection)

 참고: 단일 또는 다중 컨텍스트 모드, 라우팅 또는 투명 모드에서 ASA SFR 모듈을 사용할 수 있습니다.

시작하기 전에

이 문서에 설명된 절차를 시도하기 전에 이 중요한 정보를 고려하십시오.

- 트래픽을 ASA SFR로 교체한 IPS(Intrusion Prevention System)/CX(Context Aware) 모듈로 리디렉션하는 활성 서비스 정책이 있는 경우, ASA SFR 서비스 정책을 구성하기 전에 이를 제거해야 합니다.
- 현재 실행 중인 다른 소프트웨어 모듈을 종료해야 합니다. 디바이스는 한 번에 하나의 소프트웨어 모듈을 실행할 수 있습니다. ASA CLI에서 이 작업을 수행해야 합니다. 예를

들어 다음 명령은 IPS 소프트웨어 모듈을 종료하고 제거한 다음 ASA를 다시 로드합니다.

```
<#root>
ciscoasa#
sw-module module ips shutdown

ciscoasa#
sw-module module ips uninstall

ciscoasa#
reload
```

- CX 모듈을 제거하기 위해 사용되는 명령은 동일합니다. 단, `cxsc` 키워드가 대신 사용됩니다. `ips`:

```
<#root>
ciscoasa#
sw-module module cxsc shutdown

ciscoasa#
sw-module module cxsc uninstall

ciscoasa#
reload
```

- 모듈을 리이미징할 때 같은 방법을 사용합니다 `shutdown` 및 `uninstall` 이전 SFR 이미지를 제거하는 데 사용되는 명령입니다. 예를 들면 다음과 같습니다.

```
<#root>
ciscoasa#
sw-module module sfr uninstall
```

- ASA SFR 모듈이 다중 컨텍스트 모드에서 사용되는 경우, 시스템 실행 영역에서 이 문서에 설명된 절차를 수행합니다.



팁: ASA에서 모듈의 상태를 확인하려면 `show module` 명령을 실행합니다.

Install

이 섹션에서는 ASA에 SFR 모듈을 설치하는 방법 및 ASA SFR 부트 이미지를 설정하는 방법에 대

해 설명합니다.

ASA에 SFR 모듈 설치

ASA에 SFR 모듈을 설치하려면 다음 단계를 완료하십시오.

1. Cisco.com에서 ASA SFR 관리 인터페이스에서 액세스할 수 있는 HTTP, HTTPS 또는 FTP 서버로 ASA SFR 시스템 소프트웨어를 다운로드합니다.
2. 부팅 이미지를 디바이스에 다운로드합니다. 부팅 이미지를 디바이스로 다운로드하려면 Cisco ASDM(Adaptive Security Device Manager) 또는 ASA CLI를 사용할 수 있습니다.



참고: 시스템 소프트웨어를 전송하지 마십시오. 나중에 SSD(Solid State Drive)로 다운로드됩니다.

ASDM을 통해 부트 이미지를 다운로드하려면 다음 단계를 완료하십시오.

- a. 부트 이미지를 워크스테이션에 다운로드하거나 FTP, TFTP, HTTP, HTTPS, SMB(Server Message Block) 또는 SCP(Secure Copy) 서버에 배치합니다.
- b. 선택 **Tools > File Management** ASDM에서 수행합니다.
- c. 로컬 PC와 플래시 사이 또는 원격 서버와 플래시 사이에서 적절한 파일 전송 명령을 선택합니다.
- d. 부트 소프트웨어를 ASA의 플래시 드라이브(disk0)로 전송합니다.

ASA CLI를 통해 부트 이미지를 다운로드하려면 다음 단계를 완료하십시오.

- a. FTP, TFTP, HTTP 또는 HTTPS 서버에서 부트 이미지를 다운로드합니다.
- b. 다음을 입력합니다. `copy` 명령을 실행하여 부트 이미지를 플래시 드라이브에 다운로드합니다.

다음은 HTTP 프로토콜을 사용하는 예입니다.

서버 IP 주소 또는 호스트 이름). FTP 서버의 URL은 다음과 같습니다

`.ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img .`

```
<#root>
```

```
ciscoasa#
```

```
copy http://
```

```
 /asasfr-5500x-boot-5.3.1-152.img
```

```
 disk0:/asasfr-5500x-boot-5.3.1-152.img
```

3. ASA 플래시 드라이브에서 ASA SFR 부트 이미지 위치를 구성하려면 다음 명령을 입력합니다

.

```
<#root>
```

```
ciscoasa#
```

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

예를 들면 다음과 같습니다.

```
<#root>
ciscoasa#
sw-module module sfr recover configure image disk0:
/asasfr-5500x-boot-5.3.1-152.img
```

4. ASA SFR 부트 이미지를 로드하려면 다음 명령을 입력합니다.

```
<#root>
ciscoasa#
sw-module module sfr recover boot
```

이 시간 동안 `debug module-boot asa`에서 이러한 디버깅은 다음과 같이 인쇄됩니다.

```
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. ASA SFR 모듈이 부팅될 때까지 약 5~15분 정도 기다린 다음 작동 중인 ASA SFR 부팅 이미지에 대한 콘솔 세션을 엽니다.

ASA SFR 부팅 이미지 설정

새로 설치된 ASA SFR 부팅 이미지를 설정하려면 다음 단계를 완료하십시오.

1. 누르기 **Enter** 로그인 프롬프트에 도달하기 위해 세션을 연 후



참고: 기본 사용자 이름은 **admin**. 비밀번호는 소프트웨어 릴리스에 따라 다릅니다. **.Adm!n123 7.0.1**의 경우(공장에서 새 장치만 제공), **Admin123 6.0** 이상에서는 **Sourcefire 6.0** 이전.

예를 들면 다음과 같습니다.

```
<#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
```



팁: ASA SFR 모듈 부팅이 완료되지 않은 경우 **session** 명령이 실패하고 시스템이 **TTYS1**을 통해 연결할 수 없음을 나타내는 메시지가 나타납니다. 이 경우 모듈 부팅이 완료될 때까지 기다린 후 다시 시도하십시오.

2. 다음을 입력합니다. **setup** 명령을 입력하여 시스템 소프트웨어 패키지를 설치할 수 있도록 시스템을 구성합니다.

```
<#root>
```

```
asasfr-boot>
```

```
setup
```

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

그러면 다음 정보를 입력하라는 프롬프트가 표시됩니다.

- **Host name** - 호스트 이름은 공백 없이 최대 65자의 영숫자로 구성할 수 있습니다. 하이픈을 사용할 수 있습니다.
- **Network address** - 네트워크 주소는 고정 IPv4 또는 IPv6 주소일 수 있습니다. IPv4 또는 IPv6 상태 비저장 자동 컨피그레이션에 DHCP를 사용할 수도 있습니다.
- **DNS information** - 하나 이상의 DNS(Domain Name System) 서버를 식별해야 하며, 도메인 이름을 설정하고 도메인을 검색할 수도 있습니다.
- **NTP information** - NTP(Network Time Protocol)를 활성화하고 NTP 서버를 구성하여 시스템 시간을 설정할 수 있습니다.

3. 다음을 입력합니다. `system install` 명령을 사용하여 시스템 소프트웨어 이미지를 설치합니다.

```
<#root>
```

```
asasfr-boot >
```

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

포함: `noconfirm` 확인 메시지에 응답하지 않으려면 선택합니다. 교체 `url` 키워드(위치: `.pkg` 파일을 클릭합니다. FTP, HTTP 또는 HTTPS 서버를 사용할 수도 있습니다. 예를 들면 다음과 같습니다.

```
<#root>
```

```
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.
```

FTP 서버의 URL은 다음과 같습니다. `ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg`.

 SFR은 "Recover" 설치 프로세스 중 상태를 표시합니다. SFR 모듈 설치를 완료하는 데 최대 1시간 정도 걸릴 수 있습니다. 설치가 완료되면 시스템이 재부팅됩니다. 애플리케이션 구성 요소 설치 및 ASA SFR 서비스가 시작될 때까지 10분 이상 기다립니다. 의 출력 `show module sfr` 이 명령은 모든 프로세스가 Up.


구성

이 섹션에서는 Firepower 소프트웨어 및 FireSIGHT Management Center를 구성하는 방법과 트래픽을 SFR 모듈로 리디렉션하는 방법에 대해 설명합니다.

firepower 소프트웨어 구성

firepower 소프트웨어를 구성하려면 다음 단계를 완료하십시오.

1. ASA SFR 모듈에 대한 세션을 엽니다.

 참고: 완전히 작동하는 모듈에서 로그인 수행되므로 이제 다른 로그인 프롬프트가 나타납니다.


예를 들면 다음과 같습니다.

```
<#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:

2. 사용자 이름으로 로그인합니다 admin 비밀번호는 소프트웨어 릴리스에 따라 다릅니다. Adm!n123 7.0.1의 경우(공장에서 새 장치만 제공), Admin123 6.0 이상에서는 Sourcefire 6.0 이전.
3. 프롬프트에 따라 시스템 컨피그레이션을 완료합니다. 이 순서는 다음과 같습니다.
 - a. EULA(End User License Agreement)를 읽고 동의합니다.
 - b. 관리자 비밀번호를 변경합니다.
 - c. 프롬프트에 따라 관리 주소 및 DNS 설정을 구성합니다.

 참고: IPv4 및 IPv6 관리 주소를 모두 구성할 수 있습니다.

예를 들면 다음과 같습니다.

```
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. 시스템이 스스로 재구성할 때까지 기다립니다.

FireSIGHT Management Center 구성

ASA SFR 모듈 및 보안 정책을 관리하려면 FireSIGHT Management Center에 등록해야 합니다. 자세한 내용은 [FireSIGHT Management Center에 디바이스](#) 등록을 참조하십시오. FireSIGHT Management Center에서는 다음 작업을 수행할 수 없습니다.

- ASA SFR 모듈 인터페이스 구성
- ASA SFR 모듈 프로세스를 종료 또는 재시작하거나 다른 방법으로 관리
- ASA SFR 모듈 디바이스에서 백업을 생성하거나 백업을 복원합니다.
- 트래픽을 VLAN 태그 조건 사용과 일치시키기 위한 쓰기 액세스 제어 규칙

SFR 모듈로 트래픽 리디렉션

ASA SFR 모듈로 트래픽을 리디렉션하려면 특정 트래픽을 식별하는 서비스 정책을 생성해야 합니다. 트래픽을 ASA SFR 모듈로 리디렉션하려면 다음 단계를 완료하십시오.

1. 식별해야 하는 트래픽을 선택합니다. `access-list` 명령을 실행합니다. 이 예에서는 모든 인터페이스의 모든 트래픽이 리디렉션됩니다. 특정 트래픽에 대해서도 이 작업을 수행할 수 있습니다.

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

2. 액세스 목록의 트래픽과 일치시키기 위해 클래스 맵을 만듭니다.

```
<#root>
ciscoasa(config)#
class-map sfr

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

3. 구축 모드를 지정합니다. 패시브(모니터 전용) 또는 인라인(일반) 구축 모드에서 디바이스를 구성할 수 있습니다.

 참고: ASA에서 패시브 모드와 인라인 모드를 동시에 구성할 수는 없습니다. 한 가지 유형의 보안 정책만 허용됩니다.

- 인라인 구축에서 SFR 모듈은 액세스 제어 정책을 기반으로 트래픽을 검사하고 ASA에 트래픽 흐름에 대해 적절한 작업(허용, 거부 등)을 수행할 수 있는 판정을 제공합니다. 이 예에서는 정책 맵을 만들고 인라인 모드에서 ASA SFR 모듈을 구성하는 방법을 보여줍니다.
- 현재 `global_policy` 다른 모듈 컨피그레이션으로 구성됨(`show run policy-map global_policy`, `show run service-policy`) 그런 다음 먼저 다른 모듈 컨피그레이션에 대한 `global_policy`를 재설정/제거한 다음 `global_policy`.

```
<#root>
ciscoasa(config)#
policy-map global_policy

ciscoasa(config-pmap)#
class sfr


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


```
sfr fail-open
```

- 패시브 구축에서는 트래픽의 복사본이 SFR 서비스 모듈로 전송되지만 ASA로 반환되지는 않습니다. 패시브 모드에서는 트래픽과 관련하여 SFR 모듈이 완료했을 작업을 볼 수 있습니다. 또한 네트워크에 영향을 미치지 않고 트래픽의 내용을 평가할 수 있습니다.

SFR 모듈을 패시브 모드로 구성하려면 `monitor-only` 키워드(다음 예제에 나와 있는 것처럼) 키워드를 포함하지 않으면 트래픽이 인라인 모드로 전송됩니다.

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


 경고: `monitor-only` 모드에서는 SFR 서비스 모듈이 악성 트래픽을 거부하거나 차단할 수 없습니다.

 주의: 인터페이스 레벨을 사용하여 모니터 전용 모드로 ASA를 구성할 수 있습니다 `traffic-forward sfr monitor-only` 그러나 이 컨피그레이션은 데모 기능용으로만 사용되며 프로덕션 ASA에서 사용해서는 안 됩니다. 이 데모 기능에 있는 모든 문제는 Cisco TAC(Technical Assistance Center)에서 지원되지 않습니다. 패시브 모드에서 ASA SFR 서비스를 구축하려는 경우 정책 맵을 사용하여 구성합니다.

4. 위치를 지정하고 정책을 적용합니다. 정책을 전역적으로 또는 인터페이스에 적용할 수 있습니다. 인터페이스에서 전역 정책을 재정의하려면 해당 인터페이스에 서비스 정책을 적용할 수 있습니다.

이 `global` 키워드는 모든 인터페이스에 정책 맵을 적용하고 `interface` 키워드는 하나의 인터페이스에 정책을 적용합니다. 하나의 전역 정책만 허용됩니다. 이 예에서는 정책이 전역적으로 적용됩니다.

```
<#root>
ciscoasa(config)#
service-policy global_policy global
```

 주의: 정책 맵 `global_policy` 는 기본 정책입니다. 이 정책을 사용하고 문제를 해결하기 위해 장치에서 제거하려는 경우 그 의미를 이해해야 합니다.

다음을 확인합니다.

현재 이 설정에 사용 가능한 확인 절차는 없습니다.

문제 해결

- 이 명령(`debug module-boot`)를 클릭하여 SFR 부팅 이미지 설치 시작 시 디버그를 활성화합니다.
- ASA가 복구 모드에서 중단되었고 콘솔이 시작되지 않은 경우 이 명령(`sw-module module sfr recover stop`).
- SFR 모듈이 복구 상태에서 벗어날 수 없는 경우 ASA를 다시 로드할 수 있습니다 (`reload quick`). (트래픽이 통과하면 네트워크 교란이 발생할 수 있습니다.) Still SFR이 복구 상태로 유지되면 ASA를 종료하고 `unplug the SSD` ASA를 시작합니다. 모듈의 상태를 확인하고 INIT 상태여야 합니다. ASA를 종료하고 `insert the SSD` 카드를 사용하여 ASA를 시작합니다. ASA SFR 모듈의 이미지로 다시 설치할 수 있습니다.

관련 정보

- [Cisco Secure IPS - Cisco NGIPS의 기능](#)
- [FireSIGHT Management Center에 디바이스 등록](#)
- [Cisco ASA Firepower 모듈 빠른 시작 설명서](#)
- [VMware ESXi에 FireSIGHT Management Center 구축](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.