ASA 5585-X 하드웨어 모듈에 SFR 모듈 설치

목차

소개

ASA SFR이라고도 하는 ASA FirePOWER 모듈은 NGIPS(Next-Generation IPS), AVC(Application Visibility and Control), URL 필터링, AMP(Advance Malware Protection)를 비롯한 차세대 방화벽 서비스를 제공합니다. 단일 또는 다중 컨텍스트 모드 및 라우팅 또는 투명 모드에서 모듈을 사용할 수 있습니다. 이 문서에서는 ASA 5585-X 하드웨어 모듈에서 FirePOWER(SFR) 모듈의 사전 요구 사항 및 설치 프로세스에 대해 설명합니다. 또한 FireSIGHT Management Center에 SFR 모듈을 등록하는 단계를 제공합니다.

> **참고:** SFR(FirePOWER) 서비스는 ASA 5585-X의 하드웨어 모듈에 있는 반면, ASA 5512-X~555-X Series 어플라이언스의 FirePOWER 서비스는 소프트웨어 모듈에 설치되므로 설치 프로세스가 달라집니다.

사전 요구 사항

요구 사항

이 문서의 지침에 따라 특별 권한 EXEC 모드에 액세스해야 합니다. 특별 권한 EXEC 모드에 액세

스하려면 enable 명령을 입력합니다. 비밀번호가 설정되지 않은 경우 Enter 키를 누르십시오.

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

ASA에 FirePOWER Services를 설치하려면 다음 구성 요소가 필요합니다.

- ASA 소프트웨어 버전 9.2.2 이상
- ASA 5585-X 플랫폼
- FirePOWER 모듈의 관리 인터페이스에서 연결할 수 있는 TFTP 서버
- FireSIGHT Management Center 버전 5.3.1 이상

참고: 이 문서의 정보는 특정 랩 환경의 디바이스에서 생성됩니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

시작하기 전에

ASA SSM은 항상 ASA 5585-X 섀시에 있는 두 슬롯 중 하나를 차지합니다. SSP-CX(Context Aware) 또는 AIP-SSM(Advanced Inspection and Prevention Security)과 같은 FirePOWER(SFR) 서비스 SSP 이외의 하드웨어 모듈이 있는 경우 SSP-SSP의 공간을 확보하려면 다른 모듈을 제거해야 합니다. 하드웨어 모듈을 제거하기 전에 다음 명령을 실행하여 모듈을 종료합니다.

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

케이블 및 관리

- ASA 5585-X의 ASA 콘솔을 통해 SFR 모듈의 시리얼 포트에 액세스할 수 없습니다.
- SFR 모듈이 프로비저닝되면 "session 1" 명령을 사용하여 블레이드에 세션을 시작할 수 있습니다.
- ASA 5585-X에서 SFR 모듈을 완전히 재이미지화하려면 SFR 모듈에 있고 ASA의 관리 인터페이스 및 콘솔과는 별도로 직렬 관리 포트에서 관리 이더넷 인터페이스 및 콘솔 세션을 사용해야 합니다.

팁: ASA에서 모듈의 상태를 찾으려면 SFR 모듈의 관리 IP 및 관련 Defense Center를 검색하는 "show module 1 details" 명령을 실행합니다.

ASA에 FirePOWER(SFR) 모듈 설치

1. Cisco.com에서 ASA FirePOWER 관리 인터페이스에서 액세스할 수 있는 TFTP 서버로 ASA FirePOWER SFR 모듈 초기 부트스트랩 이미지를 다운로드합니다. 이미지 이름은 "asasfr-boot-5.3.1-152.img"와 같습니다.

2. Cisco.com에서 ASA FirePOWER 관리 인터페이스에서 액세스할 수 있는 HTTP, HTTPS 또는 FTP 서버로 ASA FirePOWER 시스템 소프트웨어를 다운로드합니다.

3. SFR 모듈을 다시 시작합니다.

옵션 1: SFR 모듈에 대한 비밀번호가 없는 경우 ASA에서 다음 명령을 실행하여 모듈을 다시 시작할 수 있습니다.

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

옵션 2: SFR 모듈에 대한 비밀번호가 있는 경우 명령행에서 센서를 직접 재부팅할 수 있습니다.

```
Sourcefire3D login: admin
Password:

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

>system reboot
```

4. 모듈을 ROMMON에 배치하기 위해 ESCAPE 또는 터미널 세션 소프트웨어의 브레이크 시퀀스를 사용하여 SFR 모듈의 부팅 프로세스를 중단합니다.

```
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. IP 주소를 사용하여 SFR 모듈 관리 인터페이스를 구성하고 부트스트랩 이미지의 TFTP 서버 및 TFTP 경로 위치를 지정합니다. 인터페이스에서 IP 주소를 설정하고 TFTP 이미지를 검색하려면 다음 명령을 입력합니다.

-

- ADDRESS = Your_IP_Address
- GATEWAY = Your_Gateway
- 서버 = Your_TFTP_Server
- 이미지 = Your_TFTP_Filepath
-
- `tftp`

! 사용된 IP 주소 정보의 예. 환경을 업데이트합니다.

```
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. 초기 부팅 이미지에 로그인합니다. admin으로 로그인하고 비밀번호 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. 초기 부팅 이미지를 사용하여 모듈의 관리 인터페이스에서 IP 주소를 구성합니다. setup 명령을 입력하여 마법사를 시작합니다. 다음 정보를 입력하라는 메시지가 표시됩니다.

- **호스트 이름**: 최대 65자의 영숫자, 공백 없음 하이픈이 허용됩니다.

- **네트워크 주소**: 고정 IPv4 또는 IPv6 주소를 설정하거나 DHCP(IPv4) 또는 IPv6 무상태 자동 컨피그레이션을 사용할 수 있습니다.
- **DNS 정보**: 하나 이상의 DNS 서버를 식별해야 하며 도메인 이름과 검색 도메인을 설정할 수도 있습니다.
- **NTP 정보**: 시스템 시간을 설정하기 위해 NTP를 활성화하고 NTP 서버를 구성할 수 있습니다.

! 사용된 정보의 예 환경을 업데이트합니다.

```
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. boot 이미지를 사용하여 **system install** 명령을 사용하여 시스템 소프트웨어 이미지를 가져오고 설치합니다. 확인 메시지에 응답하지 않으려면 noconfirm 옵션을 포함합니다. url 키워드를 .pkg 파일의 위치로 바꿉니다.

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

예를 들어

```
> 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 ...
```

> **참고:** 설치가 20~30분 후에 완료되면 Enter 키를 눌러 재부팅하라는 메시지가 표시됩니다. 애플리케이션 구성 요소를 설치하고 ASA FirePOWER 서비스를 시작할 때까지 10분 이상 기다립니다. show module 1 details 출력에는 모든 프로세스가 Up으로 표시됩니다.

설치 중 모듈 상태

```
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
```

설치 성공 후 모듈 상태

```
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
```

구성

FirePOWER 소프트웨어 구성

1.다음 외부 포트 중 하나를 통해 ASA 5585-X FirePOWER 모듈에 연결할 수 있습니다.

- ASA FirePOWER 콘솔 포트
- SSH를 사용하는 ASA FirePOWER Management 1/0 인터페이스

  참고: session sfr 명령을 사용하여 ASA 백플레인을 통해 ASA FirePOWER 하드웨어 모듈 CLI에 액세스할 수 없습니다.

2. 콘솔을 통해 FirePOWER 모듈에 액세스한 후 사용자 이름 admin 및 비밀번호 Sourcefire로 **로그인합니다**.

```
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.

>
```

FireSIGHT Management Center 구성

ASA FirePOWER 모듈 및 보안 정책을 관리하려면 FireSIGHT Management Center에 등록해야 **합니다**. FireSIGHT Management Center에서는 다음을 수행할 수 없습니다.

- ASA FirePOWER 인터페이스를 구성할 수 없습니다.
- ASA FirePOWER 프로세스를 종료, 재시작 또는 관리할 수 없습니다.
- 백업을 만들거나 ASA FirePOWER 디바이스에서 백업을 복원할 수 없습니다.
- VLAN 태그 조건을 사용하여 트래픽과 일치시키기 위해 액세스 제어 규칙을 작성할 수 없습니다.

SFR 모듈에 트래픽 리디렉션

특정 트래픽을 식별하는 서비스 정책을 생성하여 ASA FirePOWER 모듈로 트래픽을 리디렉션합니다. 트래픽을 FirePOWER 모듈로 리디렉션하려면 다음 단계를 수행하십시오.

1단계: 트래픽 선택

먼저 access-list 명령을 사용하여 트래픽을 선택합니다. 다음 예에서는 모든 인터페이스의 모든 트래픽을 리디렉션합니다. 특정 트래픽에도 적용할 수 있습니다.

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

2단계: 트래픽 일치

다음 예는 클래스 맵을 만들고 액세스 목록의 트래픽을 매칭하는 방법을 보여줍니다.

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

3단계: 작업 지정

패시브("모니터 전용") 또는 인라인 구축에서 디바이스를 구성할 수 있습니다. ASA에서 모니터 전용 모드와 일반 인라인 모드를 동시에 구성할 수는 없습니다. 하나의 보안 정책 유형만 허용됩니다.

인라인 모드

인라인 구축에서 원하지 않는 트래픽을 삭제하고 정책에 의해 적용된 다른 작업을 수행한 후 추가 처리 및 최종 전송을 위해 트래픽이 ASA로 반환됩니다. 다음 예에서는 정책 맵을 만들고 인라인 모드에서 FirePOWER 모듈을 구성하는 방법을 보여줍니다.

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

수동 모드

수동 구축에서는

- 트래픽의 복사본이 디바이스로 전송되지만 ASA로 반환되지는 않습니다.
- 패시브 모드에서는 디바이스에 트래픽이 어떤 작업을 수행했는지 볼 수 있으며, 네트워크에 영향을 주지 않고 트래픽의 내용을 평가할 수 있습니다.

패시브 모드에서 FirePOWER 모듈을 구성하려면 아래와 같이 monitor-only 키워드를 사용합니다. 키워드를 포함하지 않으면 트래픽이 인라인 모드로 전송됩니다.

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

4단계: 위치 지정

마지막 단계는 정책을 적용하는 것입니다. 전역 또는 인터페이스에서 정책을 적용할 수 있습니다. 해당 인터페이스에 서비스 정책을 적용하여 인터페이스에서 전역 정책을 재정의할 수 있습니다.

global 키워드는 모든 인터페이스에 정책 맵을 적용하고 인터페이스는 하나의 인터페이스에 정책을 적용합니다. 하나의 전역 정책만 허용됩니다. 다음 예에서는 정책이 전역적으로 적용됩니다.

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

> **주의:** 정책 맵 global_policy는 기본 정책입니다. 이 정책을 사용하고 문제 해결을 위해 디바이스에서 이 정책을 제거하려면 해당 정책의 의미를 이해해야 합니다.

관련 문서

- FireSIGHT Management Center에 디바이스 등록
- VMware ESXi에 FireSIGHT Management Center 구축
- 5500-X IPS 모듈의 IPS 관리 컨피그레이션 시나리오