Installare un modulo SFR su un modulo hardware ASA 5585-X

Sommario

Introduzione

Il modulo ASA FirePOWER, noto anche come ASA SFR, fornisce servizi firewall di nuova generazione, tra cui NGIPS (Next-Generation IPS), AVC (Application Visibility and Control), filtro URL e AMP (Advanced Malware Protection). È possibile utilizzare il modulo in modalità contesto singolo o multiplo e in modalità instradato o trasparente. Questo documento descrive i prerequisiti e i processi di installazione di un modulo FirePOWER (SFR) su un modulo hardware ASA 5585-X. Fornisce inoltre le procedure per registrare un modulo SFR con FireSIGHT Management Center.

> Nota: i servizi FirePOWER (SFR) risiedono su un modulo hardware nell'appliance ASA 5585-X, mentre i servizi FirePOWER sugli accessori ASA serie 5512-X fino a 5555-X sono installati su un modulo software, con conseguenti differenze nei processi di installazione.

Prerequisiti

Requisiti

Le istruzioni riportate in questo documento richiedono l'accesso alla modalità di esecuzione privilegiata. Per accedere alla modalità di esecuzione privilegiata, immettere il comando enable.

Se non è stata impostata una password, premere Invio.

```
<#root>

ciscoasa>

enable


Password:
ciscoasa#
```

Per installare i servizi FirePOWER su un'appliance ASA, sono necessari i seguenti componenti:

- Software ASA versione 9.2.2 o successive
- Piattaforma ASA 5585-X
- Server TFTP raggiungibile tramite l'interfaccia di gestione del modulo FirePOWER
- FireSIGHT Management Center con versione 5.3.1 o successiva

---

Nota: le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Operazioni preliminari

Poiché un SSM ASA occupa sempre uno dei due slot nello chassis ASA 5585-X, se si dispone di un modulo hardware diverso dal provider di servizi SSP FirePOWER (SFR), ad esempio SSP-CX (Context Aware) o AIP-SSM (Advanced Inspection and Prevention Security), è necessario disinstallare l'altro modulo per liberare spazio per SSP-SFR. Prima di rimuovere un modulo hardware, eseguire il comando seguente per arrestare un modulo:

```
<#root>

ciscoasa#

hw-module module 1 shutdown
```

Cablaggio e gestione

- Non è possibile accedere alla porta seriale del modulo SFR tramite la console dell'ASA sull'appliance ASA 5585-X.
- Una volta effettuato il provisioning del modulo SFR, è possibile eseguire la sessione nel

blade utilizzando il comando "session 1".
- Per ricreare completamente l'immagine del modulo SFR su un'ASA 5585-X, è necessario usare l'interfaccia Ethernet di gestione e una sessione console sulla porta di gestione seriale, che si trova sul modulo SFR e è separata dall'interfaccia e dalla console di gestione dell'ASA.

Suggerimento: per trovare lo stato di un modulo sull'ASA, eseguire il comando "show module 1 details" (mostra dettagli modulo 1) per recuperare l'IP di gestione del modulo SFR e il Defense Center associato.

Installare il modulo FirePOWER (SFR) sull'appliance ASA

1. Scaricare l'immagine iniziale del bootstrap del modulo ASA FirePOWER SFR da Cisco.com su un server TFTP accessibile dall'interfaccia di gestione ASA FirePOWER. Il nome dell'immagine è "asfr-boot-5.3.1-152.img"

2. Scaricare il software di sistema ASA FirePOWER da Cisco.com su un server HTTP, HTTPS o FTP accessibile dall'interfaccia di gestione ASA FirePOWER.

3. Riavviare il modulo SFR

Opzione 1: se non si dispone della password per il modulo SFR, è possibile usare il seguente comando dall'appliance ASA per riavviare il modulo.

```
<#root>

ciscoasa#

hw-module module 1 reload


Reload module 1? [confirm]
Reload issued for module 1
```

Opzione 2: Se si dispone della password per il modulo SFR, è possibile riavviare il sensore direttamente dalla riga di comando.

```
<#root>

Sourcefire3D login:

admin


Password:
```

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

>
```

system reboot

4. Interrompere il processo di avvio del modulo SFR utilizzando ESCAPE o la sequenza di interruzione del software della sessione terminale per inserire il modulo in ROMMON.

```
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. Configurare l'interfaccia di gestione del modulo SFR con un indirizzo IP e indicare la posizione del server TFTP e il percorso TFTP dell'immagine bootstrap. Immettere i seguenti comandi per impostare un indirizzo IP sull'interfaccia e recuperare l'immagine TFTP:

- `impostare`
- ADDRESS = Indirizzo_IP_personale
- GATEWAY = Gateway_in_uso
- SERVER = Server_TFTP
- IMAGE = Percorso_file_TFTP
- `sincronizzazione`
- `tftp`

! Esempio di informazioni sull'indirizzo IP utilizzate. Aggiornamento per l'ambiente.

<#root>

```
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. Accedere all'immagine d'avvio iniziale. Eseguire il login come admin e con la password Admin123

```
<#root>

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. Usare l'immagine di avvio iniziale per configurare un indirizzo IP sull'interfaccia di gestione del modulo. Immettere il comando setup per accedere alla procedura guidata. Vengono richieste le seguenti informazioni:

- Nome host: fino a 65 caratteri alfanumerici, senza spazi. I trattini sono consentiti.
- Indirizzo di rete: è possibile impostare indirizzi IPv4 o IPv6 statici oppure utilizzare la configurazione automatica DHCP (per IPv4) o IPv6 senza stato.
- Informazioni DNS: è necessario identificare almeno un server DNS ed è inoltre possibile impostare il nome di dominio e il dominio di ricerca.
- Informazioni NTP: è possibile abilitare NTP e configurare i server NTP per impostare l'ora di sistema.

! Informazioni di esempio utilizzate. Aggiornamento per l'ambiente.

```
<#root>

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. Usare l'immagine d'avvio per estrarre e installare l'immagine del software di sistema usando il comando system install. Includere l'opzione noconfirm se non si desidera rispondere ai messaggi di conferma. Sostituire la parola chiave url con il percorso del file .pkg.

<#root>

```
asasfr-boot>
```

system install [noconfirm]

url

Ad esempio,

<#root>

```
>
```

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 ...
```

> Nota: al termine dell'installazione, tra 20 e 30 minuti, verrà richiesto di premere Invio per riavviare. Attendere 10 o più minuti per l'installazione dei componenti dell'applicazione e l'avvio dei servizi ASA FirePOWER. L'output show module 1 details dovrebbe mostrare tutti i processi come Up (Attivo).

Stato del modulo durante l'installazione

<#root>

```
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:
```

Unresponsiv

e

Stato del modulo dopo l'installazione

<#root>

```
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
```

Configurazione

Configurazione del software FirePOWER

1. È possibile connettersi all'appliance ASA 5585-X FirePOWER tramite una delle seguenti porte esterne:

- Porta della console ASA FirePOWER
- Interfaccia ASA FirePOWER Management 1/0 con SSH

Nota: non è possibile accedere all'interfaccia CLI del modulo hardware FirePOWER ASA sul backplane ASA con il comando session sfr.

2. Dopo aver effettuato l'accesso al modulo FirePOWER dalla console, eseguire il login con il nome utente admin e la password Sourcefire.

<#root>

```
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.

>
```

Configurazione di FireSIGHT Management Center

Per gestire un modulo ASA FirePOWER e la policy di sicurezza, è necessario registrarlo su un centro di gestione FireSIGHT. Con un centro di gestione FireSIGHT non è possibile effettuare le seguenti operazioni:

- Impossibile configurare le interfacce ASA FirePOWER.
- Impossibile arrestare, riavviare o gestire in altro modo i processi ASA FirePOWER.
- Impossibile creare backup o ripristinarli su dispositivi ASA FirePOWER.
- Impossibile scrivere le regole di controllo di accesso per far corrispondere il traffico utilizzando le condizioni dei tag VLAN.

Reindirizza il traffico al modulo SFR

Il traffico viene reindirizzato al modulo ASA FirePOWER creando una policy del servizio che identifica il traffico specifico. Per reindirizzare il traffico a un modulo FirePOWER, attenersi alla seguente procedura:

Passaggio 1: Selezionare il traffico

Innanzitutto, selezionare il traffico con il comando access-list. Nell'esempio che segue viene reindirizzato tutto il traffico proveniente da tutte le interfacce. Potresti farlo anche per un traffico specifico.

```
<#root>

ciscoasa(config)#

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

Fase 2: abbinare il traffico

Nell'esempio seguente viene illustrato come creare una mappa delle classi e far corrispondere il traffico in un elenco degli accessi:

```
<#root>

ciscoasa(config)#

class-map sfr
```

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

Passaggio 3: Specificare l'azione

È possibile configurare il dispositivo in una distribuzione passiva ("solo monitor") o in linea. Non è possibile configurare contemporaneamente la modalità solo monitor e la modalità in linea normale sull'appliance ASA. È consentito un solo tipo di criterio di protezione.

Modalità in linea

In un'implementazione in linea, dopo aver eliminato il traffico indesiderato e aver intrapreso qualsiasi altra azione applicata dalla policy, il traffico viene restituito all'ASA per un'ulteriore elaborazione e trasmissione. L'esempio seguente mostra come creare una mappa dei criteri e configurare il modulo FirePOWER in modalità inline:

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

ciscoasa(config-pmap)#
class sfr

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

Modalità passiva

In un'installazione passiva,

- Una copia del traffico viene inviata al dispositivo, ma non viene restituita all'appliance ASA.
- La modalità passiva consente di visualizzare le operazioni che il dispositivo avrebbe eseguito sul traffico e di valutare il contenuto del traffico, senza alcun impatto sulla rete.

Se si desidera configurare il modulo FirePOWER in modalità passiva, utilizzare la parola chiave monitor-only come indicato di seguito. Se non si include la parola chiave, il traffico viene inviato in modalità inline.

```
<#root>
ciscoasa(config-pmap-c)#
```

```
sfr fail-open


monitor-only
```

Passaggio 4: Specificare la posizione

L'ultimo passaggio consiste nell'applicare la politica. È possibile applicare un criterio a livello globale o su un'interfaccia. È possibile sostituire il criterio globale in un'interfaccia applicando un criterio del servizio a tale interfaccia.

La parola chiave global applica la mappa dei criteri a tutte le interfacce e interface applica il criterio a un'interfaccia. È consentito un solo criterio globale. Nell'esempio seguente il criterio viene applicato globalmente:

```
<#root>

ciscoasa(config)#

service-policy global_policy global
```

> Attenzione: la mappa dei criteri global_policy è un criterio predefinito. Se si utilizza questo criterio e si desidera rimuoverlo dal dispositivo a scopo di risoluzione dei problemi, è necessario comprenderne le implicazioni.

Documenti correlati

- Registrazione di un dispositivo con un centro di gestione FireSIGHT
- Installazione di FireSIGHT Management Center su VMware ESXi
- Scenari di configurazione della gestione IPS su un modulo IPS 5500-X

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).