Installazione e configurazione di un modulo servizi FirePOWER su una piattaforma ASA

Sommario

Introduzione

In questo documento viene descritto come installare e configurare un modulo Cisco FirePOWER (SFR) in esecuzione su un'appliance Cisco Adaptive Security (ASA) e come registrare il modulo SFR con Cisco FireSIGHT Management Center.

Prerequisiti

Requisiti

Cisco consiglia al sistema di soddisfare i seguenti requisiti prima di provare le procedure descritte in questo documento:

- Accertarsi di disporre di almeno 3 GB di spazio libero sull'unità flash (disco0), oltre alle dimensioni del software di avvio.
- Accertarsi di disporre dell'accesso in modalità di esecuzione privilegiata. Per accedere alla modalità di esecuzione privilegiata, immettere il **enable** nella CLI. Se non è stata impostata una password, premere **Enter**:

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

Componenti usati

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

- Software Cisco ASA versione 9.2.2 o successive
- Piattaforme Cisco ASA da 5512-X a 5555-X
- Software FirePOWER versione 5.3.1 o successive

Nota: Per installare i servizi FirePOWER (SFR) su un modulo hardware ASA 5585-X, consultare il documento sull'installazione di un modulo SFR su un modulo hardware ASA 5585-X.

Questi componenti sono richiesti sul Cisco FireSIGHT Management Center:

- Software FirePOWER versione 5.3.1 o successive
- Appliance virtuale o FireSIGHT Management Center FS2000, FS4000

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.

Premesse

Il modulo Cisco ASA FirePOWER, noto anche come ASA SFR, fornisce servizi firewall di nuova generazione, quali:

- Next-Generation Intrusion Prevention System (NGIPS)
- Visibilità e controllo delle applicazioni (AVC)
- Filtra URL
- Advanced Malware Protection (AMP)

Nota: È possibile utilizzare il modulo ASA SFR in modalità contesto singolo o multiplo e in modalità instradato o trasparente.

Operazioni preliminari

Prendere in considerazione queste informazioni importanti prima di provare le procedure descritte in questo documento:

- Se sono presenti criteri del servizio attivi che reindirizzano il traffico a un modulo IPS (Intrusion Prevention System)/CX (Context Aware) sostituito con ASA SFR, è necessario rimuoverli prima di configurare i criteri del servizio ASA SFR.
- Ènecessario chiudere tutti gli altri moduli software attualmente in esecuzione. Un dispositivo può eseguire un singolo modulo software alla volta. Questa operazione deve essere eseguita dalla CLI dell'ASA. Ad esempio, questi comandi arrestano e disinstallano il modulo software IPS, quindi ricaricano l'appliance ASA:

```
ciscoasa# sw-module module ips shutdown
```

```
ciscoasa# sw-module module ips uninstall
ciscoasa# reload
```

- I comandi utilizzati per rimuovere il modulo CX sono gli stessi, ad eccezione **cxsc** viene utilizzata una parola chiave anziché **ips**:

```
ciscoasa# sw-module module cxsc shutdown
ciscoasa# sw-module module cxsc uninstall
ciscoasa# reload
```

- Quando si ricrea un'immagine di un modulo, utilizzare lo stesso **shutdown** e **uninstall** comandi utilizzati per rimuovere un'immagine SFR precedente. Di seguito è riportato un esempio:

```
ciscoasa# sw-module module sfr uninstall
```

- Se il modulo ASA SFR viene utilizzato in modalità contesto multiplo, eseguire le procedure descritte in questo documento all'interno dello spazio di esecuzione del sistema.

Suggerimento: Per determinare lo stato di un modulo sull'appliance ASA, immettere il comando **show module**

Install

Questa sezione descrive come installare il modulo SFR sull'appliance ASA e come configurare l'immagine di avvio di ASA SFR.

Installare il modulo SFR sull'appliance ASA

Per installare il modulo SFR sull'appliance ASA, completare i seguenti passaggi:

1. Scaricare il software di sistema ASA SFR da Cisco.com su un server HTTP, HTTPS o FTP accessibile dall'interfaccia di gestione ASA SFR.
2. Scaricare l'immagine di avvio nel dispositivo. Per scaricare l'immagine di avvio sul dispositivo, è possibile usare Cisco Adaptive Security Device Manager (ASDM) o la CLI dell'ASA. **Nota:** Non trasferire il software di sistema; viene scaricato successivamente sull'unità a stato solido (SSD).Per scaricare l'immagine di avvio tramite ASDM, completare la procedura seguente: Scaricare l'immagine di avvio nella workstation o inserirla in un server FTP, TFTP, HTTP, HTTPS, Server Message Block (SMB) o Secure Copy (SCP).Scegli**Tools > File Management** in ASDM.Scegliere il comando di trasferimento file appropriato, *tra computer locale e flash* o *tra server remoto e flash*.Trasferire il software di avvio sull'unità flash (disco0) dell'appliance ASA.Per scaricare l'immagine di avvio dalla CLI dell'ASA, completare la procedura seguente:Scaricare l'immagine di avvio su un server FTP, TFTP, HTTP o HTTPS.Immettere il **copy** nella CLI per scaricare l'immagine di avvio sull'unità flash. Di seguito è riportato un esempio che utilizza il protocollo HTTP (sostituire il con l'indirizzo IP o il nome host del server). Per il server FTP, l'URL ha il seguente aspetto:**ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img** .
```
ciscoasa# copy http:///asasfr-5500x-boot-5.3.1-152.img disk0:/asasfr-5500x-boot-5.3.1-152.img
```
3. Immettere questo comando per configurare la posizione dell'immagine di avvio ASA SFR nell'unità flash ASA:

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

Di seguito è riportato un esempio:

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

4. Per caricare l'immagine di avvio dell'ASA SFR, immettere questo comando:

```
ciscoasa# sw-module module sfr recover boot
```

Durante questo periodo, se si attiva **debug module-boot** sull'appliance ASA, vengono stampati i seguenti debug:

```
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. Attendere circa 5-15 minuti l'avvio del modulo ASA SFR e aprire una sessione console per l'immagine di avvio operativa di ASA SFR.

Configurazione dell'immagine di avvio di ASA SFR

Completare questa procedura per configurare l'immagine di avvio di ASA SFR appena installata:

1. Premere **Enter** dopo aver aperto una sessione per accedere al prompt di accesso. **Nota:** Il

nome utente predefinito è **admin**. La password varia a seconda della versione del software:**Adm!n123** per 7.0.1 (solo dispositivi nuovi in fabbrica), **Admin123** 6.0 e versioni successive, **Sourcefire** per le versioni precedenti alla 6.0.Di seguito è riportato un esempio:

```
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
```

Suggerimento: Se l'avvio del modulo ASA SFR non è stato completato, il comando session ha esito negativo e viene visualizzato un messaggio che indica che il sistema non è in grado di connettersi tramite TTYS1. In questo caso, attendere il completamento dell'avvio del modulo e riprovare.

2. Immettere il **setup** per configurare il sistema in modo da poter installare il pacchetto software del sistema:

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

Vengono quindi richieste le seguenti informazioni:**Host name** - Il nome host può contenere fino a 65 caratteri alfanumerici, senza spazi. È consentito l'uso di trattini.**Network address** - L'indirizzo di rete può essere un indirizzo IPv4 statico o un indirizzo IPv6. È inoltre possibile utilizzare DHCP per la configurazione automatica IPv4 o IPv6 senza stato.**DNS information** - È necessario identificare almeno un server DNS (Domain Name System) ed è inoltre possibile impostare il nome di dominio e il dominio di ricerca.**NTP information** - È possibile abilitare il protocollo NTP (Network Time Protocol) e configurare i server NTP per impostare l'ora del sistema.

3. Immettere il **system install** per installare l'immagine software del sistema:

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

Includi **noconfirm** se non si desidera rispondere ai messaggi di conferma. Sostituire il **url** parola chiave con il percorso della **.pkg** file. Anche in questo caso è possibile utilizzare un server FTP, HTTP o HTTPS. Di seguito è riportato un esempio:

```
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.
```

Per il server FTP, l'URL ha il seguente aspetto:**ftp://username:password@server-ip/asasfr-sys-5.3.1-152.pkg**.

Nota La SFR si trova in un "**Recover**" durante il processo di installazione. L'installazione del modulo SFR può richiedere all'incirca un'ora. Al termine dell'installazione, il sistema si riavvia. Attendere dieci o più minuti per l'installazione del componente applicativo e l'avvio dei servizi ASA SFR. L'output del **show module sfr** indica che tutti i processi sono **Up**.

Configurazione

Questa sezione descrive come configurare il software FirePOWER e il centro di gestione FireSIGHT e come reindirizzare il traffico al modulo SFR.

Configurazione del software FirePOWER

Completare questi passaggi per configurare il software FirePOWER:

1. Aprire una sessione sul modulo ASA SFR.
   Nota: Viene visualizzato un prompt di accesso diverso perché l'accesso viene eseguito su un modulo completamente funzionante.Di seguito è riportato un esempio:

   ```
   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. Accedere con il nome utente **admin** e la password varia a seconda della versione del software:**Adm!n123** per 7.0.1 (solo dispositivi nuovi in fabbrica), **Admin123** 6.0 e versioni successive,**Sourcefire** per le versioni precedenti alla 6.0.
3. Completare la configurazione del sistema come richiesto, nell'ordine seguente: Leggere e accettare il Contratto di Licenza con l'utente finale (EULA).Modificare la password amministratore.Configurare l'indirizzo di gestione e le impostazioni DNS, come richiesto.
   Nota: È possibile configurare indirizzi di gestione IPv4 e IPv6.Di seguito è riportato un esempio:

   ```
   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. Attendere che il sistema si riconfiguri.

Configurazione di FireSIGHT Management Center

Per gestire un modulo ASA SFR e la policy di sicurezza, è necessario registrarlo su un centro di gestione FireSIGHT. Per ulteriori informazioni, fare riferimento a Registrazione di un dispositivo con un centro di gestione FireSIGHT. Non è possibile eseguire queste operazioni con un centro di gestione FireSIGHT:

- Configurare le interfacce del modulo ASA SFR
- Arrestare, riavviare o gestire in altro modo i processi del modulo ASA SFR
- Creazione o ripristino di backup dai dispositivi del modulo ASA SFR
- Scrittura delle regole di controllo di accesso per far corrispondere il traffico con l'uso delle condizioni dei tag VLAN

Reindirizza il traffico al modulo SFR

Per reindirizzare il traffico al modulo ASA SFR, è necessario creare una policy del servizio che identifichi il traffico specifico. Per reindirizzare il traffico su un modulo ASA SFR, completare la procedura seguente:

1. Selezionare il traffico che deve essere identificato con **access-list** Nell'esempio, tutto il traffico proveniente da tutte le interfacce viene reindirizzato. Questa operazione può essere effettuata anche per un traffico specifico.

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

2. Creare una mappa delle classi per far corrispondere il traffico in un elenco degli accessi:

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

3. Specificare la modalità di distribuzione. È possibile configurare il dispositivo in modalità passiva (solo monitor) o inline (normale).
Nota: Non è possibile configurare contemporaneamente la modalità passiva e la modalità inline sull'appliance ASA. È consentito un solo tipo di criterio di protezione.In una implementazione in linea, il modulo SFR controlla il traffico in base ai criteri di controllo dell'accesso e fornisce all'ASA il verdetto di intraprendere l'azione appropriata (consenti, nega e così via) sul flusso del traffico. Nell'esempio viene mostrato come creare una mappa dei criteri e configurare il modulo ASA SFR in modalità inline. Verificare che il **global_policy** è configurato con un'altra configurazione di modulo**(show run policy-map global_policy, show run service-policy)**, quindi reimpostare/rimuovere prima global_policy per un'altra configurazione di modulo e riconfigurare **global_policy**.

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

In un'implementazione passiva, una copia del traffico viene inviata al modulo del servizio SFR, ma non viene restituita all'appliance ASA. La modalità passiva consente di visualizzare

le azioni che il modulo SFR avrebbe completato relativamente al traffico. Consente inoltre di valutare il contenuto del traffico, senza alcun impatto sulla rete.

Se si desidera configurare il modulo SFR in modalità passiva, utilizzare il **monitor-only** (come illustrato nell'esempio seguente). Se la parola chiave non viene inclusa, il traffico viene inviato in modalità inline.

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

Avviso: OSPF (Open Shortest Path First) **monitor-only** Questa modalità non consente al modulo del servizio SFR di negare o bloccare il traffico dannoso.**Attenzione:** È possibile configurare un'ASA in modalità *solo monitor* usando il comando interface-level **traffic-forward sfr monitor-only** comando; tuttavia, questa configurazione è solo a scopo dimostrativo e non deve essere utilizzata su un'appliance ASA di produzione. I problemi rilevati in questa funzionalità dimostrativa non sono supportati dal Cisco Technical Assistance Center (TAC). Se si desidera distribuire il servizio ASA SFR in modalità passiva, configurarlo con l'uso di una *mappa* dei *criteri*.

4. Specificare un percorso e applicare il criterio. È possibile applicare un criterio a livello globale o su un'interfaccia. Per eseguire l'override del criterio globale in un'interfaccia, è possibile applicare un criterio servizio a tale interfaccia.

   OSPF (Open Shortest Path First) **global** la parola chiave applica la mappa dei criteri a tutte le interfacce e **interface** la parola chiave applica il criterio a un'interfaccia. È consentito un solo criterio globale. In questo esempio, il criterio viene applicato globalmente:

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

   Attenzione: Mappa dei criteri **global_policy** è un criterio predefinito. Se si utilizza questo criterio e si desidera rimuoverlo dal dispositivo per la risoluzione dei problemi, verificare di averne compreso le implicazioni.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

- Èpossibile eseguire questo comando (**debug module-boot**) per attivare il debug all'inizio dell'installazione dell'immagine di avvio SFR.
- Se l'appliance ASA è bloccata in modalità di ripristino e la console non si accende, provare a eseguire questo comando (**sw-module module sfr recover stop**).
- Se il modulo SFR non è riuscito a uscire dallo stato di ripristino, è possibile provare a ricaricare l'appliance ASA **(reload quick)**. (se il traffico attraversa la rete, può causare disturbi alla rete). Se Still SFR è bloccato nello stato di ripristino, è possibile arrestare l'ASA e **unplug the SSD** e avviare l'appliance ASA. Verificare lo stato del modulo e che sia INIT. Anche in questo caso, chiudere l'appliance ASA, **insert the SSD** e avviare l'ASA. È possibile avviare la re-immagine del modulo ASA SFR.

Informazioni correlate

- Cisco Secure IPS - Funzionalità Cisco NGIPS
- Registrazione di un dispositivo con un centro di gestione FireSIGHT
- Guida introduttiva al modulo Cisco ASA FirePOWER
- Installazione di FireSIGHT Management Center su VMware ESXi
- Documentazione e supporto tecnico – Cisco Systems