Esempio di configurazione base di FWSM

Sommario

Introduzione

In questo documento viene descritto come configurare la configurazione di base del Firewall Services Module (FWSM) installato negli switch Cisco serie 6500 o nei router Cisco serie 7600. Questa configurazione include la configurazione dell'indirizzo IP, il routing predefinito, il NATing statico e dinamico, le istruzioni Access Control Lists (ACLs) per consentire il traffico desiderato o bloccare il traffico indesiderato, gli application server come Websense per l'ispezione del traffico Internet dalla rete interna e il server Web per gli utenti Internet.

Nota: in uno scenario ad alta disponibilità (HA, High Availability) di FWSM, il failover può essere sincronizzato correttamente solo quando le chiavi di licenza sono esattamente le stesse tra i moduli. Pertanto, il failover non può funzionare tra i moduli FWSM con licenze diverse.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Modulo servizi firewall con software versione 3.1 e successive
- Switch Catalyst serie 6500, con i componenti richiesti, come mostrato:Supervisor Engine con software Cisco IOS®, noto come supervisor Cisco IOS, o sistema operativo Catalyst. Vedere la tabella per le versioni software e supervisor engine supportate.Multilayer Switch Feature Card (MSFC) 2 con software Cisco IOS. Per le versioni del software Cisco IOS supportate, vedere la tabella.

[1] Il modulo FWSM non supporta il supervisor 1 o 1A.

[2]Quando si usa Catalyst OS sul supervisor, è possibile usare una qualsiasi di queste versioni software Cisco IOS supportate sull'MSFC. Quando si usa il software Cisco IOS sul supervisor, si usa la stessa versione sull'MSFC.

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.

Prodotti correlati

Questa configurazione può essere utilizzata anche per i router Cisco serie 7600, con i componenti richiesti come mostrato:

- Supervisor Engine con software Cisco IOS. Vedere la tabella per le versioni supportate di supervisor engine e software Cisco IOS.
- MSFC 2 con software Cisco IOS. Per le versioni del software Cisco IOS supportate, vedere la tabella.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Il modulo FWSM è un modulo firewall stateful, ad alte prestazioni e con risparmio di spazio che viene installato negli switch Catalyst serie 6500 e nei router Cisco serie 7600.

I firewall proteggono le reti interne dall'accesso non autorizzato da parte degli utenti di una rete esterna. Il firewall può inoltre proteggere le reti interne l'una dall'altra, ad esempio quando una rete di risorse umane è separata dalla rete di un utente. Se si dispone di risorse di rete che devono essere disponibili per un utente esterno, ad esempio un server Web o FTP, è possibile posizionare tali risorse in una rete separata dietro il firewall, denominata zona demilitarizzata

(DMZ). Il firewall consente un accesso limitato alla zona demilitarizzata, ma poiché la zona include solo i server pubblici, un attacco in tale zona colpisce solo i server e non le altre reti interne. È inoltre possibile controllare quando gli utenti interni accedono a reti esterne, ad esempio all'accesso a Internet, se si consentono solo determinati indirizzi esterni, se si richiede l'autenticazione o l'autorizzazione oppure se si è coordinati con un server filtro URL esterno.

Il modulo FWSM include molte funzionalità avanzate, ad esempio più contesti di sicurezza simili ai firewall virtualizzati, un firewall trasparente (livello 2) o instradato (livello 3), centinaia di interfacce e molte altre funzioni.

Durante la trattazione delle reti connesse a un firewall, la rete esterna si trova davanti al firewall, la rete interna è protetta e dietro il firewall e una DMZ, mentre dietro il firewall, consente un accesso limitato agli utenti esterni. Poiché FWSM consente di configurare molte interfacce con varie policy di sicurezza, che includono molte interfacce interne, molte DMZ e anche molte interfacce esterne se lo si desidera, questi termini vengono utilizzati solo in senso generale.

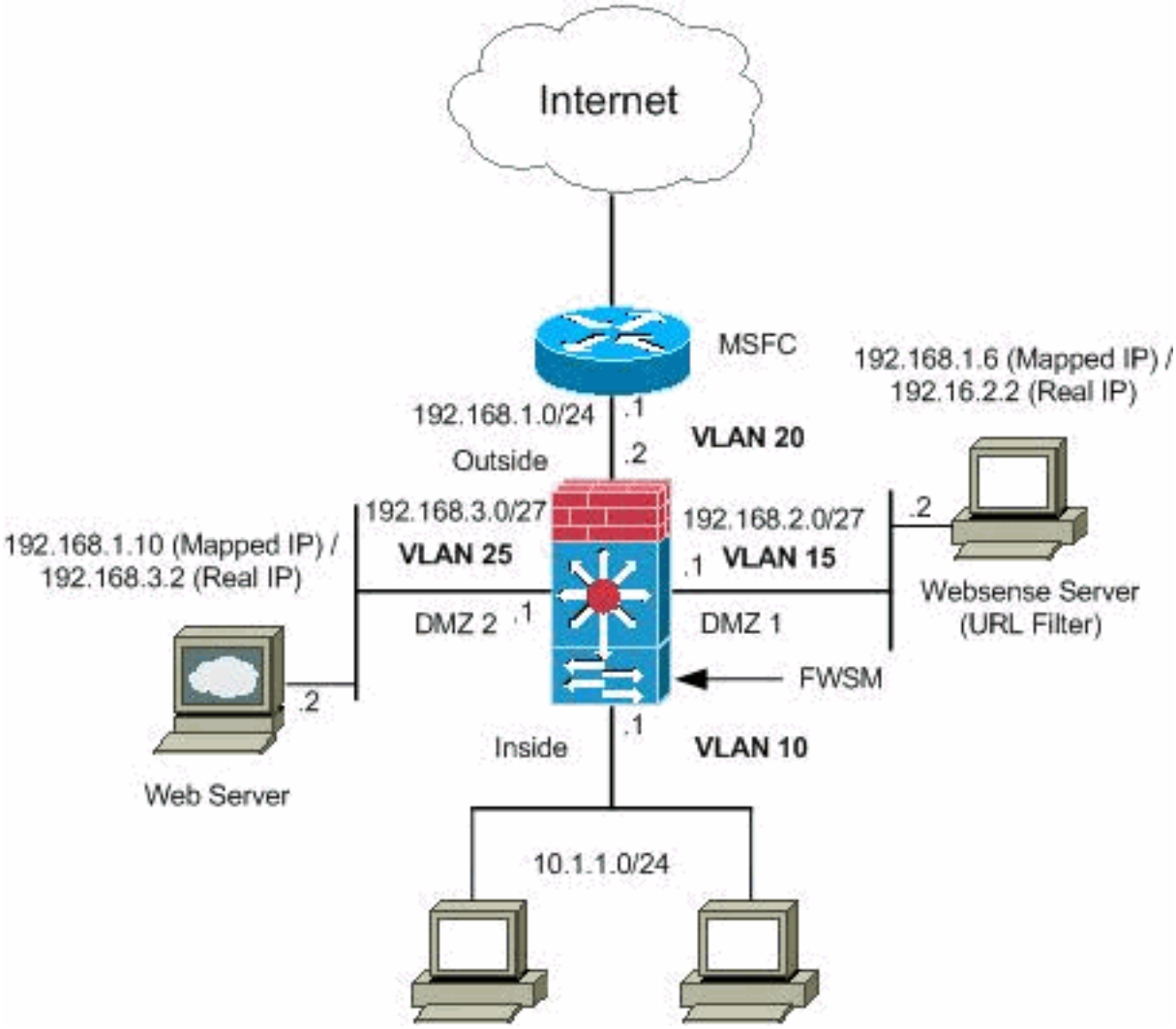
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

Configurazioni

Nel documento vengono usate queste configurazioni:

- Catalyst serie 6500 Switch Configuration
- Configurazione FWSM

Catalyst serie 6500 Switch Configuration

1. Èpossibile installare il modulo FWSM negli switch Catalyst serie 6500 o nei router Cisco serie 7600. La configurazione di entrambe le serie è identica e nel presente documento le serie vengono generalmente indicate come **switch**.**Nota:** prima di configurare il modulo FWSM, è necessario configurare lo switch in modo appropriato.
2. **Assegnare le VLAN al modulo Firewall Services**: in questa sezione viene descritto come assegnare le VLAN all'FWSM. Il modulo FWSM non comprende interfacce fisiche esterne. ma utilizza interfacce VLAN. L'assegnazione di VLAN all'FWSM è simile all'assegnazione di una VLAN a una porta dello switch; l'FWSM includa un'interfaccia interna allo switch fabric module, se presente, o al bus condiviso.**Nota:** per ulteriori informazioni su come creare le VLAN e assegnarle alle porte dello switch, consultare la sezione Configurazione delle VLAN

della guida alla configurazione del software degli switch Catalyst 6500.**Linee guida VLAN:**Èpossibile utilizzare le VLAN private con l'FWSM. assegnare la VLAN primaria all'FWSM; il modulo FWSM gestisce automaticamente il traffico della VLAN secondaria.Non è possibile usare VLAN riservate.Non è possibile usare la VLAN 1.Se si utilizza il failover FWSM nello stesso chassis dello switch, non assegnare le VLAN riservate per il failover e le comunicazioni stateful a una porta dello switch. Tuttavia, se si utilizza il failover tra gli chassis, è necessario includere le VLAN nella porta trunk tra lo chassis.Se non si aggiungono le VLAN allo switch prima di assegnarle all'FWSM, le VLAN vengono memorizzate nel database del supervisor engine e inviate all'FWSM non appena vengono aggiunte allo switch.Assegnare le VLAN all'FWSM prima di assegnarle all'MSFC.Le VLAN che non soddisfano questa condizione vengono eliminate dall'intervallo di VLAN che si tenta di assegnare all'FWSM.**Assegnare le VLAN al modulo FWSM nel software Cisco IOS:**Nel software Cisco IOS, creare fino a 16 gruppi di VLAN firewall, quindi assegnare i gruppi al modulo FWSM. Ad esempio, è possibile assegnare tutte le VLAN a un gruppo, creare un gruppo interno e un gruppo esterno oppure creare un gruppo per ciascun cliente. Ogni gruppo può contenere un numero illimitato di VLAN.non è possibile assegnare la stessa VLAN a più gruppi di firewall; è tuttavia possibile assegnare più gruppi firewall a un modulo FWSM e un singolo gruppo firewall a più moduli FWSM. Ad esempio, le VLAN che si desidera assegnare a più FWSM possono risiedere in un gruppo separato dalle VLAN che sono univoche per ciascun FWSM.Per assegnare le VLAN all'FWSM, completare i seguenti passaggi:

```
Router(config)#firewall vlan-group firewall_group vlan_range
```

L'intervallo `vlan_range` può essere rappresentato da una o più VLAN, ad esempio da 2 a 1000 e da 1025 a 4094, identificate come un singolo numero (n) come 5, 10, 15 o come un intervallo (n-x) come 5-10, 10-20.**Nota:** le porte routing e WAN usano VLAN interne, quindi è possibile che le VLAN nell'intervallo 1020-1100 siano già in uso.**Esempio:**

```
firewall vlan-group 1 10,15,20,25
```

Completare i passaggi per assegnare i gruppi firewall al modulo FWSM.

```
Router(config)#firewall module module_number vlan-group firewall_group
```

`firewall_group` è costituito da uno o più numeri di gruppo come numero singolo (n) come 5 o come intervallo come 5-10.**Esempio:**

```
firewall module 1 vlan-group 1
```

Assegnazione di VLAN all'FWSM nel software del sistema operativo Catalyst: nel software Catalyst OS, viene assegnato un elenco di VLAN all'FWSM. Se lo si desidera, è possibile assegnare la stessa VLAN a più FWSM. L'elenco può contenere un numero illimitato di VLAN.Completare la procedura per assegnare le VLAN all'FWSM.

```
Console> (enable)set vlan vlan_list firewall-vlan mod_num
```

L'elenco `vlan_list` può essere rappresentato da una o più VLAN, ad esempio da 2 a 1000 e da 1025 a 4094, identificate come un singolo numero (n) come 5, 10, 15 o come un intervallo (n-x) come 5-10, 10-20.

3. **Aggiungere interfacce virtuali commutate all'MSFC**: una VLAN definita sull'MSFC è detta interfaccia virtuale commutata. Se si assegna la VLAN utilizzata per la SVI all'FWSM, l'MSFC

eseguirà il routing tra l'FWSM e le altre VLAN di layer 3.Per motivi di sicurezza, per impostazione predefinita, tra l'MSFC e l'FWSM può esistere una sola SVI. Ad esempio, se si configura in modo errato il sistema con più SVI, è possibile che il traffico attorno all'FWSM venga inavvertitamente autorizzato se si assegnano all'MSFC le VLAN interna ed esterna.Completare la procedura per configurare la SVI

```
Router(config)#interface vlan vlan_number
Router(config-if)#ip address address mask
```

Esempio:

```
interface vlan 20
ip address 192.168.1.1 255.255.255.0
```

Catalyst serie 6500 Switch Configuration
`!--- Output Suppressed` firewall vlan-group 1 10,15,20,25 firewall module 1 vlan-group 1 interface vlan 20 ip address 192.168.1.1 255.255.255.0 `!--- Output Suppressed`

Nota: accedere all'FWSM dallo switch con il comando appropriato al sistema operativo dello switch:

- Cisco IOS Software:

```
Router#session slot
```

- Software Catalyst OS:

```
Console> (enable) session module_number
```

(Facoltativo) Condivisione di VLAN con altri moduli Servizio: se lo switch dispone di altri moduli Servizio, ad esempio Application Control Engine (ACE), è possibile che sia necessario condividere alcune VLAN con questi moduli Servizio. Per ulteriori informazioni su come ottimizzare la configurazione FWSM quando si utilizzano questi altri moduli, fare riferimento a Progettazione del modulo di servizio con ACE e FWSM.

Configurazione FWSM

1. **Configure Interfaces for FWSM** - Prima di autorizzare il traffico attraverso l'FWSM, è necessario configurare un nome di interfaccia e un indirizzo IP. È inoltre consigliabile modificare il livello di protezione predefinito, ovvero 0. Se si assegna un nome a un'interfaccia `interna` e non si imposta il livello di protezione in modo esplicito, il livello di protezione verrà impostato automaticamente su 100.**Nota:** ogni interfaccia deve avere un livello di protezione da 0 (minimo) a 100 (massimo). È ad esempio necessario assegnare la rete più sicura, ad esempio la rete host interna, al livello 100, mentre la rete esterna connessa a Internet può essere al livello 0. Altre reti, ad esempio le DMZ, possono trovarsi nel mezzo.Alla configurazione è possibile aggiungere qualsiasi ID VLAN, ma solo le VLAN,

ad esempio 10, 15, 20 e 25, assegnate al modulo FWSM dallo switch possono trasmettere il traffico. Per visualizzare tutte le VLAN assegnate all'FWSM, usare il comando **show vlan**.

```
interface vlan 20
    nameif outside
    security-level 0
    ip address 192.168.1.2 255.255.255.0
interface vlan 10
    nameif inside
    security-level 100
    ip address 10.1.1.1 255.255.255.0
interface vlan 15
    nameif dmz1
    security-level 60
    ip address 192.168.2.1 255.255.255.224
interface vlan 25
    nameif dmz2
    security-level 50
    ip address 192.168.3.1 255.255.255.224
```

Suggerimento: nel comando **name *<name>* il** *nome* **è una stringa di testo composta da un massimo di 48 caratteri e non fa distinzione tra maiuscole e minuscole.** È possibile modificare il nome se si immette nuovamente questo comando con un nuovo valore. Non immettere la forma no, in quanto tale comando determina l'eliminazione di tutti i comandi che fanno riferimento a tale nome.

2. **Configurare la route predefinita:**

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

Un percorso predefinito identifica l'indirizzo IP del gateway (192.168.1.1) a cui il modulo FWSM invia tutti i pacchetti IP per i quali non dispone di un percorso appreso o statico. Una route predefinita è semplicemente una route statica con 0.0.0.0/0 come indirizzo IP di destinazione. I percorsi che identificano una destinazione specifica hanno la precedenza sul percorso predefinito.

3. **Il NAT dinamico** converte un gruppo di indirizzi reali (10.1.1.0/24) in un pool di indirizzi mappati (192.168.1.20-192.168.1.50) che sono instradabili sulla rete di destinazione. Il pool mappato può includere un numero di indirizzi inferiore rispetto al gruppo reale. Quando un host che si desidera tradurre accede alla rete di destinazione, il modulo FWSM assegna a tale host un indirizzo IP del pool mappato. La conversione viene aggiunta solo quando l'host reale avvia la connessione. La traduzione viene eseguita solo per la durata della connessione e un determinato utente non mantiene lo stesso indirizzo IP dopo il timeout della traduzione.

```
nat (inside) 1 10.1.1.0 255.255.255.0
global (outside) 1 192.168.1.20-192.168.1.50 netmask 255.255.255.0
access-list Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any
access-group Internet in interface inside
```

Per negare il traffico proveniente dalla rete interna 10.1.1.0/24 e accedere alla rete DMZ1 (192.168.2.0) e permettere agli altri tipi di traffico diretto a Internet tramite l'applicazione dell'ACL all'interfaccia interna, è necessario creare un ACL per indirizzare il traffico in entrata verso la rete DMZ1 (192.168.2.0).

4. **Il protocollo NAT statico** crea una traduzione fissa di indirizzi reali in indirizzi mappati. Con i

protocolli NAT e PAT dinamici, ogni host utilizza un indirizzo o una porta diversa per ogni traduzione successiva. Poiché l'indirizzo mappato è lo stesso per ciascuna connessione consecutiva con NAT statico ed esiste una regola di conversione persistente, NAT statico consente agli host sulla rete di destinazione di avviare il traffico verso un host tradotto, se esiste un elenco degli accessi che lo consente.La differenza principale tra NAT dinamico e un intervallo di indirizzi per NAT statico è che NAT statico consente a un host remoto di avviare una connessione a un host tradotto, se esiste un elenco degli accessi che lo consente, a differenza di NAT dinamico. È inoltre necessario un numero uguale di indirizzi mappati come indirizzi reali con NAT statico.

```
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask 255.255.255.255
static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask 255.255.255.255
access-list outside extended permit tcp any host 192.168.1.10 eq http
access-list outside extended permit tcp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-
data
access-list outside extended permit udp host 192.168.1.30 host 192.168.1.6 eq pcanywhere-
status
access-list inbound extended permit udp any host 216.70.55.69 range 8766 30000
access-group outside in interface outside
```

Queste sono le due istruzioni NAT statiche mostrate. La prima ha lo scopo di convertire il reale IP 192.168.2.2 sull'interfaccia interna nel reale IP 192.168.1.6 sulla subnet esterna, a condizione che l'ACL autorizzi il traffico dall'origine 192.168.1.30 all'IP 192.168.1.6 mappato per accedere al server Websense nella rete DMZ1. Analogamente, la seconda istruzione NAT statica intendeva convertire il reale IP 192.168.3.2 sull'interfaccia interna nell'IP 192.168.1.10 mappato sulla subnet esterna a condizione che l'ACL autorizzi il traffico da Internet all'IP 192.168.1.10 mappato per accedere al server Web nella rete DMZ2 e che abbia il numero di porta udp nell'intervallo da 8766 a 30000.

5. Il comando **url-server** designa il server che esegue l'applicazione di filtro URL Websense. Il limite è di 16 server URL in modalità contesto singolo e di quattro server URL in modalità multipla, ma è possibile utilizzare una sola applicazione, N2H2 o Websense, alla volta. Inoltre, se si modifica la configurazione sull'accessorio di protezione, la configurazione sul server applicazioni non verrà aggiornata. Questa operazione deve essere eseguita separatamente, in conformità alle istruzioni del fornitore.Il comando **url-server** deve essere configurato prima di usare il comando **filter** per HTTPS e FTP. Se tutti i server URL vengono rimossi dall'elenco dei server, vengono rimossi anche tutti i comandi di filtro correlati al filtro URL.Dopo aver designato il server, abilitare il servizio di filtro URL con il comando **filter url**.

```
url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1
connections 5
```

Il comando **filter url** impedisce l'accesso degli utenti in uscita dagli URL del World Wide Web designati con l'applicazione di filtro Websense.

```
filter url http 10.1.1.0 255.255.255.0 0 0
```

Configurazione FWSM

```
!--- Output Suppressed interface vlan 20 nameif outside
```

```
security-level 0 ip address 192.168.1.2 255.255.255.0
interface vlan 10 nameif inside security-level 100 ip
address 10.1.1.1 255.255.255.0 interface vlan 15 nameif
dmz1 security-level 60 ip address 192.168.2.1
255.255.255.224 interface vlan 25 nameif dmz2 security-
level 50 ip address 192.168.3.1 255.255.255.224 passwd
fl0wer enable password treeh0u$e route outside 0 0
192.168.1.1 1 url-server (dmz1) vendor websense host
192.168.2.2 timeout 30 protocol TCP version 1
connections 5 url-cache dst 128 filter url http 10.1.1.0
255.255.255.0 0 0 !--- When inside users access an HTTP
server, FWSM consults with a !--- Websense server in
order to determine if the traffic is allowed. nat
(inside) 1 10.1.1.0 255.255.255.0 global (outside) 1
192.168.1.20-192.168.1.50 netmask 255.255.255.0 !---
Dynamic NAT for inside users that access the Internet
static (dmz1,outside) 192.168.1.6 192.168.2.2 netmask
255.255.255.255 !--- A host on the subnet 192.168.1.0/24
requires access to the Websense !--- server for
management that use pcAnywhere, so the Websense server
!--- uses a static translation for its private address.
static (dmz2,outside) 192.168.1.10 192.168.3.2 netmask
255.255.255.255 !--- A host on the Internet requires
access to the Webserver, so the Webserver !--- uses a
static translation for its private address. access-list
Internet extended deny ip any 192.168.2.0 255.255.255.0
access-list Internet extended permit ip any any access-
group Internet in interface inside !--- Allows all
inside hosts to access the outside for any IP traffic,
!--- but denies them access to the dmz1 access-list
outside extended permit tcp any host 192.168.1.10 eq
http !--- Allows the traffic from the internet with the
destination IP address !--- 192.168.1.10 and destination
port 80 access-list outside extended permit tcp host
192.168.1.30 host 192.168.1.6 eq pcanywhere-data access-
list outside extended permit udp host 192.168.1.30 host
192.168.1.6 eq pcanywhere-status !--- Allows the
management host 192.168.1.30 to use !--- pcAnywhere on
the Websense server access-list inbound extended permit
udp any host 216.70.55.69 range 8766 30000 !--- Allows
udp port number in the range of 8766 to 30000. access-
group outside in interface outside access-list WEBSENSE
extended permit tcp host 192.168.2.2 any eq http access-
group WEBSENSE in interface dmz1 !--- The Websense
server needs to access the Websense !--- updater server
on the outside. !--- Output Suppressed
```

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

1. Visualizzare le informazioni del modulo in base al sistema operativo in uso per verificare che lo switch riconosca l'FWSM e lo abbia portato online:Cisco IOS Software:

```
Router#show module
Mod Ports Card Type                                Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-SUP2-2GE    SAD0444099Y
```

```
  2   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD03475619
  3    2  Intrusion Detection System             WS-X6381-IDS       SAD04250KV5
  4    6  Firewall Module                         WS-SVC-FWM-1       SAD062302U4
```

Software Catalyst OS:

```
Console>show module [mod-num]
The following is sample output from the show module command:

Console> show module
Mod Slot Ports Module-Type               Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- ------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
4   4    2     Intrusion Detection Syste WS-X6381-IDS        no  ok
5   5    6     Firewall Module           WS-SVC-FWM-1        no  ok
6   6    8     1000BaseX Ethernet        WS-X6408-GBIC       no  ok
```

Nota: il comando **show module** visualizza sei porte per l'FWSM. Si tratta di porte interne raggruppate come EtherChannel.

2.

```
Router#show firewall vlan-group
Group vlans
----- ------
   1 10,15,20
   51 70-85
   52 100
```

3.

```
Router#show firewall module
Module Vlan-groups
  5    1,51
  8    1,52
```

4. Immettere il comando per il sistema operativo in uso per visualizzare la partizione di avvio corrente:Cisco IOS Software:

```
Router#show boot device [mod_num]
```

Esempio:

```
Router#show boot device
[mod:1 ]:
[mod:2 ]:
[mod:3 ]:
[mod:4 ]: cf:4
[mod:5 ]: cf:4
[mod:6 ]:
[mod:7 ]: cf:4
[mod:8 ]:
[mod:9 ]:
```

Software Catalyst OS:

```
Console> (enable) show boot device mod_num
```

Esempio:

```
Console> (enable) show boot device 6
Device BOOT variable = cf:5
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

1. **Impostazione della partizione di avvio predefinita** - Per impostazione predefinita, FWSM viene avviato dalla partizione applicativa **cf:4**. Tuttavia, è possibile scegliere di eseguire l'avvio dalla partizione dell'applicazione **cf:5** o nella partizione di manutenzione **cf:1**. Per modificare la partizione di avvio predefinita, immettere il comando per il sistema operativo:Cisco IOS Software:
   ```
   Router(config)#boot device module mod_num cf:n
   ```

   Dove n è 1 (manutenzione), 4 (applicazione) o 5 (applicazione).Software Catalyst OS:
   ```
   Console> (enable) set boot device cf:n mod_num
   ```

   Dove n è 1 (manutenzione), 4 (applicazione) o 5 (applicazione).
2. **Ripristino del modulo FWSM nel software Cisco IOS**—Per ripristinare il modulo FWSM, immettere il comando come mostrato:
   ```
   Router#hw-module module mod_num reset [cf:n] [mem-test-full]
   ```

   L'argomento **cf:n** è la partizione, 1 (manutenzione), 4 (applicazione) o 5 (applicazione). Se non si specifica la partizione, viene utilizzata quella predefinita, generalmente **cf:4**.L'opzione **mem-test-full** esegue un test completo della memoria, che richiede circa sei minuti.**Esempio:**
   ```
   Router#hw-mod module 9 reset
   Proceed with reload of module? [confirm] y
   % reset issued for module 9
   Router#
   00:26:55:%SNMP-5-MODULETRAP:Module 9 [Down] Trap
   00:26:55:SP:The PC in slot 8 is shutting down. Please wait ...
   ```
   Per il software **Catalyst OS**:
   ```
   Console> (enable) reset mod_num [cf:n]
   ```

   Dove **cf:n** è la partizione, 1 (manutenzione), 4 (applicazione) o 5 (applicazione). Se non si specifica la partizione, viene utilizzata quella predefinita, generalmente **cf:4**.

Nota: non è possibile configurare il protocollo NTP su FWSM perché le impostazioni vengono prelevate dallo switch.

Problema: Impossibile passare il traffico VLAN da FWSM al sensore IPS 4270

Impossibile passare il traffico da FWSM ai sensori IPS.

Soluzione

Per forzare il traffico attraverso l'IPS, il trucco è creare una VLAN ausiliaria in modo da suddividere efficacemente una delle VLAN correnti in due e quindi collegarle. Controllare questo esempio con le VLAN 401 e 501 per chiarire:

- Per analizzare il traffico sulla **VLAN 401** principale, creare un'altra **VLAN 501** (VLAN ausiliaria). Quindi, disabilitare l'interfaccia VLAN 401, che gli host nella versione 401 usano attualmente come gateway predefinito.
- Quindi, abilitare l'interfaccia VLAN 501 con *lo stesso* indirizzo che era stato disabilitato sull'interfaccia VLAN 401.
- Posizionare una delle interfacce IPS sulla VLAN 401 e l'altra sulla VLAN 501.

Èsufficiente spostare il gateway predefinito per la VLAN 401 sulla VLAN 501. Le modifiche devono essere effettuate anche sulle VLAN, se presenti. Si noti che le VLAN sono essenzialmente come segmenti LAN. È possibile avere un gateway predefinito su un cavo diverso da quello degli host

che lo utilizzano.

Problemi di pacchetti non ordinati in FWSM

Come risolvere il problema dei pacchetti non ordinati in FWSM?

Soluzione

Per risolvere il problema dei pacchetti non ordinati nel modulo FWSM, usare il comando system np complete-unit in modalità di configurazione globale. Questo comando è stato introdotto nella versione 3.2(5) di FWSM e assicura che i pacchetti vengano inoltrati nello stesso ordine in cui sono stati ricevuti.

Problema: Impossibile passare pacchetti con routing asimmetrico attraverso il firewall

Non è possibile passare pacchetti con routing asimmetrico attraverso il firewall.

Soluzione

Per passare i pacchetti con routing asimmetrico attraverso il firewall, usare il comando set connection advanced-options tcp-state-bypass in modalità di configurazione delle classi. Questo comando è stato introdotto nella versione 3.2(1) di FWSM.

Supporto NetFlow in FWSM

Gli FWSM supportano Netflow?

Soluzione

NetFlow non è supportato in FWSM.

Informazioni correlate

- Cisco Catalyst serie 6500 Firewall Services Module - Pagina di supporto
- Pagina di supporto per gli switch Cisco Catalyst serie 6500
- Cisco serie 7600 Router Support Page
- Spiegazione dei cookie TCP intercept e SYN FWSM
- Documentazione e supporto tecnico – Cisco Systems