FWSM 基本組態範例

目錄

簡介

本檔案介紹如何設定安裝在Cisco 6500系列交換器或Cisco 7600系列路由器上的防火牆服務模組(FWSM)的基本組態。這包括配置IP地址、預設路由、靜態和動態NATing、訪問控制清單(ACL)語句以允許所需的流量或阻止不需要的流量、用於檢查來自內部網路的網際網路流量的應用伺服器（如Websense）以及用於Internet使用者的Web伺服器。

注意：在FWSM高可用性(HA)方案中，僅當模組之間的許可證金鑰完全相同時，故障切換才能成功同步。因此，故障轉移無法在具有不同許可證的FWSM之間工作。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行軟體版本3.1和更新版本的防火牆服務模組
- Catalyst 6500系列交換器，以及所需的元件，如下所示：搭載Cisco IOS®軟體(稱為Supervisor Cisco IOS或Catalyst作業系統(OS)的Supervisor engine。 有關支援的supervisor engine和軟體版本，請參閱表。採用Cisco IOS軟體的多層交換器功能卡(MSFC)2。有關支援的Cisco IOS軟體版本，請參閱表。

[1] FWSM不支援Supervisor 1或1A。

[2]在Supervisor上使用Catalyst OS時，您可以在MSFC上使用這些受支援的Cisco IOS軟體版本中的任意一個。在Supervisor上使用Cisco IOS軟體時，在MSFC上使用相同的版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置還可用於Cisco 7600系列路由器，其所需元件如下所示：

- 搭載Cisco IOS軟體的Supervisor engine。有關支援的Supervisor引擎和Cisco IOS軟體版本，請參閱表。
- 採用Cisco IOS軟體的MSFC 2。有關支援的Cisco IOS軟體版本，請參閱表。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

FWSM是安裝在Catalyst 6500系列交換機和Cisco 7600系列路由器上的高效能、節省空間的有狀態防火牆模組。

防火牆保護內部網路免受外部網路上的使用者未經授權的訪問。防火牆還可以保護內部網路彼此隔絕，例如，當您將人力資源網路與使用者網路分開時。如果您有需要可供外部使用者使用的網路資源（例如Web或FTP伺服器），則可以將這些資源放在防火牆後面的單獨網路上，稱為隔離區(DMZ)。 防火牆允許對DMZ的有限訪問，但由於DMZ僅包含公共伺服器，因此該處的攻擊僅影響伺服器，而不影響其他內部網路。您還可以控制內部使用者何時訪問外部網路，例如，訪問Internet（僅允許某些地址外寄）、要求身份驗證或授權，或與外部URL過濾伺服器協調。

FWSM包括許多高級功能，例如類似於虛擬化防火牆的多個安全情景、透明（第2層）防火牆或路由（第3層）防火牆操作、數百個介面以及許多其他功能。

在討論連線到防火牆的網路時，外部網路位於防火牆之前，內部網路受到保護並位於防火牆之後，而DMZ位於防火牆之後，允許外部使用者的有限訪問。由於FWSM允許您使用不同的安全策略配置許多介面（包括許多內部介面、許多DMZ甚至許多外部介面，如果需要），因此這些術語僅在一般意義上使用。

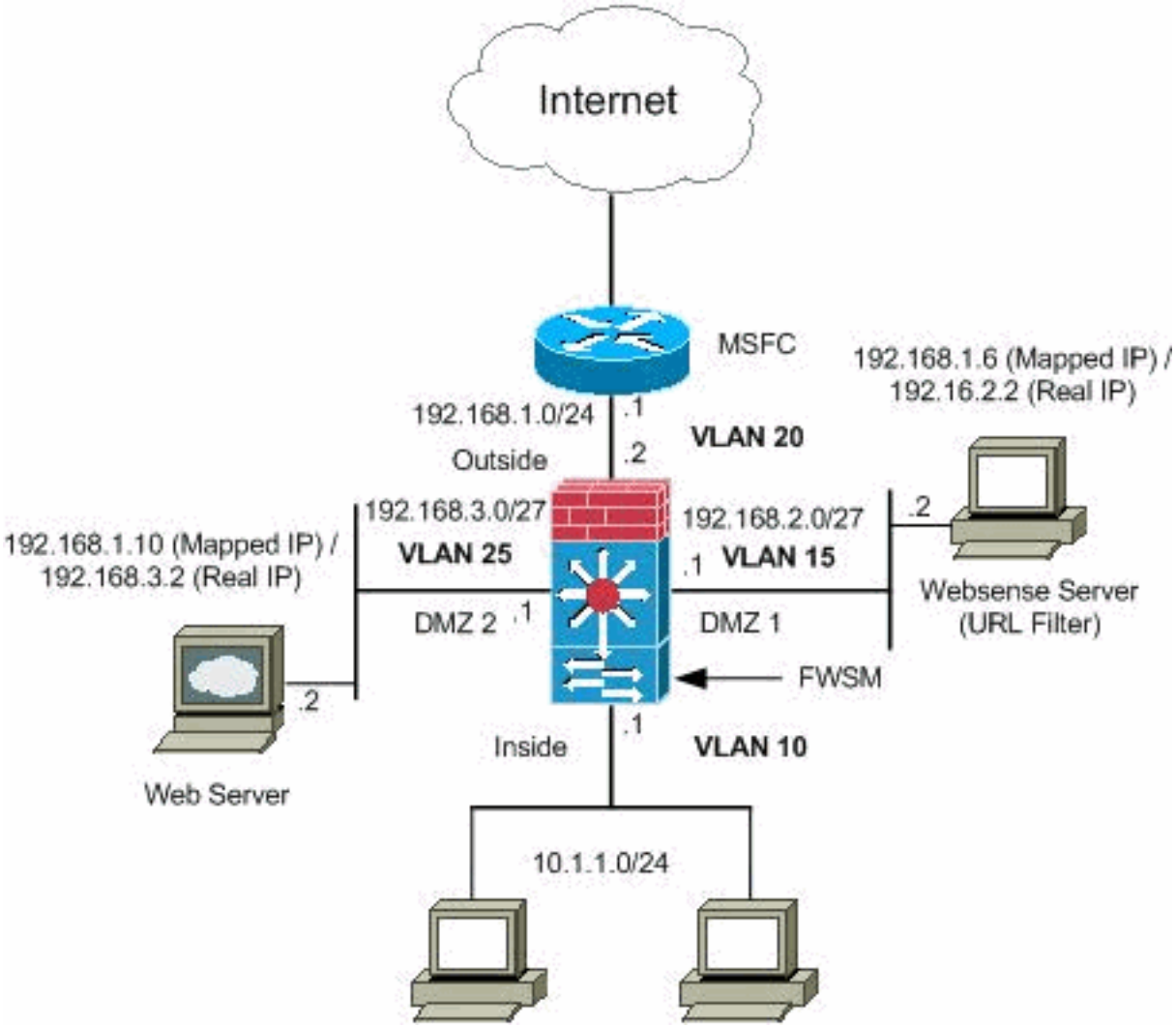
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用 Command Lookup Tool(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意：此配置中使用的IP編址方案在Internet上不能合法路由。它們是RFC 1918地址，已在實驗室環境中使用。

組態

本檔案會使用以下設定：

- Catalyst 6500系列交換器組態
- FWSM配置

Catalyst 6500系列交換器組態

1. 您可以在Catalyst 6500系列交換機或Cisco 7600系列路由器中安裝FWSM。這兩個系列的配置是相同的，在本文檔中，該系列一般稱為**switch**。**注意：**在配置FWSM之前，需要正確配置交換機。
2. **將VLAN分配到防火牆服務模**塊 — 本節介紹如何將VLAN分配到FWSM。FWSM不包括任何外部物理介面。相反，它使用VLAN介面。為FWSM分配VLAN類似於為交換機埠分配VLAN;fwsm包括到交換機交換矩陣模組（如果有）或共用匯流排的內部介面。**註：有關**如何建立VLAN並將其分配給交換機埠的詳細資訊，請參閱Catalyst 6500交換機軟體配置指南**的**配置VLAN**部分。VLAN指南：**您可以將專用VLAN與FWSM一起使用。將主VLAN分配給FWSM;fwsm會自動處理輔助VLAN流量。不能使用保留VLAN。不能使用VLAN 1。如果在同一交換機機箱內使用FWSM故障切換，請勿將您為故障切換和有狀態通訊保留的VLAN分配給交換機埠。但是，如果在機箱之間使用故障切換，則必須在機箱之間的中繼埠包括VLAN。如果在將VLAN分配給FWSM之前沒有將VLAN新增到交換機，則這些VLAN會儲存在Supervisor Engine資料庫中，一旦新增到交換機，就會傳送到FWSM。將VLAN分配到MSFC之前，請將其分配到FWSM。不滿足此條件的VLAN會從您嘗試在FWSM上分配的VLAN範圍中丟棄。**在Cisco IOS軟體中為FWSM分配VLAN:**在Cisco IOS軟體中，建立最多16個防火牆VLAN組，然後將組分配給FWSM。例如，您可以將所有VLAN分配給一個組，或者建立一個內部組和一個外部組，或者為每個客戶建立一個組。每個組可以包含無限制的VLAN。不能將同一個VLAN分配給多個防火牆組；但是，您可以將多個防火牆組分配給一個FWSM，也可以將一個防火牆組分配給多個FWSM。例如，要分配給多個FWSM的VLAN可以位於與每個FWSM唯一的VLAN不同的單獨組中。完成以下步驟，以便將VLAN分配到FWSM:
```
Router(config)#firewall vlan-group firewall_group vlan_range
```
`vlan_range`可以是一個或多個VLAN，例如2到1000和從1025到4094，標識為單個數字(n)（如5、10、15）或範圍(n-x)（如5-10、10-20）。**注意：**路由埠和WAN埠會消耗內部VLAN，因此1020-1100範圍內的VLAN可能已在使用中。**範例：**
```
firewall vlan-group 1 10,15,20,25
```
完成這些步驟，將防火牆組分配給FWSM。
```
Router(config)#firewall module module_number vlan-group firewall_group
```
`firewall_group`是一個或多個組號，可以是單個數字(n)（如5）或範圍（如5-10）。**範例：**
```
firewall module 1 vlan-group 1
```
在Catalyst作業系統軟體中為FWSM分配VLAN — 在Catalyst OS軟體中，為FWSM分配VLAN清單。如果需要，您可以將同一VLAN分配給多個FWSM。該清單可以包含無限制的VLAN。完成這些步驟，以便為FWSM分配VLAN。
```
Console> (enable)set vlan vlan_list firewall-vlan mod_num
```
`vlan_list`可以是一個或多個VLAN，例如2到1000和從1025到4094，標識為單個數字(n)（例如5、10、15）或範圍(n-x)（例如5-10、10-20）。
3. **將交換虛擬介面新增到MSFC** — 在MSFC上定義的VLAN稱為交換虛擬介面。如果將用於SVI的VLAN分配給FWSM，則MSFC會在FWSM和其他第3層VLAN之間進行路由。出於安全原因，預設情況下，MSFC和FWSM之間只能存在一個SVI。例如，如果使用多個SVI對系統配置錯誤，如果將內部和外部VLAN分配給MSFC，則可能會意外允許流量通過FWSM。完成這些步驟以配置SVI
```
Router(config)#interface vlan vlan_number
Router(config-if)#ip address address mask
```

範例：

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

Catalyst 6500系列交換器組態
!--- 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*

注意：使用適用於您的交換機作業系統的命令從交換機登入到FWSM:

- Cisco IOS軟體：
  `Router#session slot`

- Catalyst OS軟體：
  `Console> (enable) session module_number`

（可選）與其他服務模組共用VLAN — 如果交換機具有其他服務模組，例如應用控制引擎(ACE)，則可能必須與這些服務模組共用某些VLAN。請參閱使用ACE和FWSM的服務模組設計，瞭解更多有關使用此類其他模組時如何最佳化FWSM配置的詳細資訊。

FWSM配置

1. **為FWSM配置介面** — 在允許流量通過FWSM之前，需要配置介面名稱和IP地址。您還應更改預設安全級別，預設值為0。如果您在內部命名了一個介面，但未明確設定安全級別，則FWSM會將安全級別設定為100。**注意：**每個介面的安全級別必須介於0（最低）到100（最高）之間。 例如，您應將最安全的網路（例如內部主機網路）分配到100級，而連線到Internet的外部網路可以是0級。其他網路（例如DMZ）可以在兩者之間。可以向配置中新增任何VLAN ID，但只有VLAN（例如10、15、20和25）可以傳遞流量，這些流量是由交換機分配給FWSM的。使用**show VLAN**命令以檢視指派給FWSM的所有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
```

提示：在**nameif *<name>* 命令中，*name*是一個最多包含48個字元的文本字串，不區分大小寫**。如果用新值重新輸入此命令，則可以更改名稱。請勿輸入no形式，因為該命令會導致引用該名稱的所有命令被刪除。

2. **配置預設路由：**

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

預設路由標識FWSM向其傳送其沒有已獲取或靜態路由的所有IP資料包的網關IP地址(192.168.1.1)。預設路由只是以0.0.0.0/0作為目標IP地址的靜態路由。標識特定目標的路由優先於預設路由。

3. **動態NAT將一組實際地址(10.1.1.0/24)轉換為可在目標網路上路由的對映地址池(192.168.1.20-192.168.1.50)。**對映池可以包含比實際組更少的地址。當要轉換的主機訪問目標網路時，FWSM會從對映池為其分配IP地址。僅當實際主機發起連線時，才會新增轉換。轉換僅在連線期間進行，並且給定使用者不會在轉換超時後保留相同的IP地址。

```
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
```

您需要建立一個ACL，以拒絕來自內部網路10.1.1.0/24的流量進入DMZ1網路(192.168.2.0)，並允許其他型別的流量通過ACL *Internet*應用（內部）介面進入Internet，作為傳入流量的傳入方向。

4. **靜態NAT**建立實際地址到對映地址的固定轉換。使用動態NAT和PAT，每台主機在每次後續轉換時使用不同的地址或埠。由於對映地址對於具有靜態NAT的每個連續連線都是相同的，並且存在永續性轉換規則，因此，如果存在允許轉換的接入清單，靜態NAT允許目標網路上的主機向轉換的主機發起流量。動態NAT和靜態NAT地址範圍的主要區別在於，如果存在允許連線的訪問清單，則靜態NAT允許遠端主機發起到已轉換主機的連線，而動態NAT則不允許。使用靜態NAT時，還需要相同數量的對映地址作為實際地址。

```
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
```

以下是所示的兩個靜態NAT語句。第一個目標是將內部介面上的實際IP 192.168.2.2轉換為外部子網上的對映IP 192.168.1.6，前提是ACL允許從源192.168.1.30到對映IP 192.168.1.6的流量訪問DMZ1網路中的Websense伺服器。同樣，第二個靜態NAT語句旨在將內部介面上的實際IP 192.168.3.2轉換為外部子網上的對映IP 192.168.1.10，前提是ACL允許從Internet到對映IP 192.168.1.10的流量訪問DMZ2網路中的Web伺服器，並且udp埠號在8766到30000的範圍內。

5. **url-server**命令指定運行Websense URL過濾應用程式的伺服器。限制是單情景模式下的16個URL伺服器和多模式下的4個URL伺服器，但是一次只能使用一個應用程式，即N2H2或Websense。此外，如果更改安全裝置上的配置，則不會更新應用伺服器上的配置。此操作必

須根據供應商說明單獨完成。對HTTPS和FTP發出**filter**命令之前，必須配置**url-server**命令。如果從伺服器清單中刪除所有URL伺服器，則也會刪除與URL過濾相關的所有過濾命令。指定伺服器後，使用**filter url**命令啟用URL過濾服務。

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

filter url命令允許阻止從您使用Websense過濾應用程式指定的全球資訊網URL訪問出站使用者。

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

FWSM配置

```
!--- 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
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**指令輸出的分析。

1. 根據您的作業系統檢視模組資訊，以驗證交換機是否確認FWSM並已使其聯機：Cisco IOS軟體：

```
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
```

Catalyst OS軟體：

```
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
```

註：show module命令顯示FWSM的六個埠。這些是作為EtherChannel組合在一起的內部埠。

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. 輸入作業系統的命令以檢視當前引導分割槽：Cisco IOS軟體：

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

範例：

```
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 ]:
```

Catalyst OS軟體：

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

範例：

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

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

1. **設定預設引導分割槽** — 預設情況下，FWSM從**cf**:4應**用程式分割槽**引導。但是，您可以選擇從**cf:5應用程式**分割槽引導或引導到**cf:1維護**分割槽。要更改預設引導分割槽，請輸入作業系統的命令：Cisco IOS軟體：

   ```
   Router(config)#boot device module mod_num cf:n
   ```

   其中n為1（維護）、4（應用程式）或5（應用程式）。Catalyst OS軟體：

   ```
   Console> (enable) set boot device cf:n mod_num
   ```

   其中n為1（維護）、4（應用程式）或5（應用程式）。
2. **重置Cisco IOS軟體中的FWSM** — 要重置FWSM，請輸入以下命令：

   ```
   Router#hw-module module mod_num reset [cf:n] [mem-test-full]
   ```

   cf:n引數是分割槽，可以是1（維護）、4（應用程式）或5（應用程式）。 如果不指定分割槽，則使用預設分割槽，通常為**cf:4**。**mem-test-full**選項運行完全記憶體測試，大約需要6分鐘。

   範例：

   ```
   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 ...
   ```

   對於**Catalyst OS軟體**：

   ```
   Console> (enable) reset mod_num [cf:n]
   ```

   其中**cf:n**是分割槽，可以是1（維護）、4（應用程式）或5（應用程式）。 如果不指定分割槽，則使用預設分割槽，通常為**cf:4**。

注意：無法在FWSM上配置NTP，因為它從交換機獲取其設定。

問題：無法將VLAN通訊量從FWSM傳遞到IPS感測器4270

無法將通訊量從FWSM傳遞到IPS感測器。

解決方案

為了強制流量通過IPS，關鍵是要建立輔助VLAN，以便有效地將一個當前VLAN分為兩個，然後將它們橋接在一起。使用VLAN 401和501檢查此範例以說明：

- 如果要掃描主**VLAN** 401上的**流量**，請建立另一個**VLAN 501**（輔助VLAN）。 然後禁用VLAN介面401,401中的主機當前將其用作預設網關。
- 接下來，使用您之前在VLAN 401介面上禁用的*地址*啟用VLAN 501介面。
- 將其中一個IPS介面放在VLAN 401中，將另一個放在VLAN 501中。

您只需將VLAN 401的預設網關移動到VLAN 501上。如果存在，您需要對VLAN進行類似的更改。請注意，VLAN本質上與LAN網段類似。預設網關可以位於與使用它的主機不同的線路上。

FWSM中的無序資料包問題

如何解決FWSM中的無序資料包問題？

解決方案

在全域性配置模式下發出sysopt np completion-unit命令，以解決FWSM中的無序資料包問題。此命令是在FWSM版本3.2(5)中匯入，並確保按照接收資料包的相同順序轉發資料包。

問題：無法通過防火牆傳遞非對稱路由的資料包

您無法通過防火牆傳遞非對稱路由的資料包。

解決方案

在類配置模式下發出set connection advanced-options tcp-state-bypass 命令，以便通過防火牆傳遞非對稱路由資料包。此命令是在FWSM版本3.2(1)中匯入。

FWSM中的Netflow支援

FWSM是否支援Netflow?

解決方案

FWSM不支援Netflow。

相關資訊

- Cisco Catalyst 6500系列防火牆服務模組支援頁面
- Cisco Catalyst 6500系列交換器支援頁面
- Cisco 7600系列路由器支援頁面
- 解釋了FWSM TCP攔截和SYN cookie
- 技術支援與文件 - Cisco Systems