Exemplo de configuração básica de FWSM

Contents

Introduction

Este documento descreve como configurar a configuração básica do Firewall Services Module (FWSM) instalado nos Cisco 6500 Series Switches ou nos Cisco 7600 Series Routers. Isso inclui a configuração do endereço IP, roteamento padrão, NATing estático e dinâmico, ACLs (Access Control Lists, listas de controle de acesso) para permitir o tráfego desejado ou bloquear o tráfego indesejado, servidores de aplicativos como Websense para a inspeção do tráfego de Internet da rede interna e o Servidor Web para os usuários de Internet.

Observação: em um cenário de alta disponibilidade (HA) do FWSM, o failover só pode ser sincronizado com êxito quando as chaves de licença são exatamente as mesmas entre os módulos. Portanto, o failover não pode funcionar entre os FWSMs com licenças diferentes.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firewall Services Module que executa o software versão 3.1 e posterior
- Switches da série Catalyst 6500, com os componentes necessários conforme mostrado:Mecanismo supervisor com o software Cisco IOS®, conhecido como supervisor Cisco IOS ou sistema operacional Catalyst (OS). Consulte a Tabela para obter as versões de software e do mecanismo de supervisor compatíveis.Multilayer Switch Feature Card (MSFC) 2 com software Cisco IOS. Consulte a Tabela para obter as versões suportadas do software Cisco IOS.

[1] O FWSM não suporta o supervisor 1 ou 1A.

[2] Quando você usa o Catalyst OS no supervisor, você pode usar qualquer uma dessas versões suportadas do Cisco IOS Software no MSFC. Ao usar o software Cisco IOS no supervisor, você usa a mesma versão no MSFC.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produtos Relacionados

Essa configuração também pode ser usada para os roteadores da série Cisco 7600, com os componentes necessários conforme mostrado:

- Mecanismo de supervisor com software Cisco IOS. Consulte a Tabela para obter as versões suportadas do Supervisor Engine e do Cisco IOS Software.
- MSFC 2 com software Cisco IOS. Consulte a Tabela para obter as versões suportadas do software Cisco IOS.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O FWSM é um módulo de firewall de alto desempenho, com economia de espaço e stateful que é instalado nos switches da série Catalyst 6500 e nos roteadores da série Cisco 7600.

Os firewalls protegem as redes internas contra o acesso não autorizado de usuários em uma rede externa. O firewall também pode proteger redes internas umas das outras, por exemplo, quando você mantém uma rede de recursos humanos separada de uma rede de usuários. Se você tiver recursos de rede que precisam estar disponíveis para um usuário externo, como um servidor Web ou FTP, você poderá colocar esses recursos em uma rede separada atrás do firewall, chamada de zona desmilitarizada (DMZ). O firewall permite acesso limitado à DMZ, mas como a DMZ inclui

apenas os servidores públicos, um ataque afeta apenas os servidores e não afeta as outras redes internas. Você também pode controlar quando usuários internos acessam redes externas, por exemplo, acesso à Internet, se você permitir apenas determinados endereços fora, exigir autenticação ou autorização ou coordenar com um servidor externo de filtragem de URL.

O FWSM inclui muitos recursos avançados, como vários contextos de segurança semelhantes a firewalls virtualizados, firewall transparente (Camada 2) ou operação de firewall roteado (Camada 3), centenas de interfaces e muitos outros recursos.

Durante a discussão sobre redes conectadas a um firewall, a rede externa está em frente ao firewall, a rede interna está protegida e atrás do firewall e uma DMZ, enquanto atrás do firewall, permite acesso limitado a usuários externos. Como o FWSM permite que você configure muitas interfaces com políticas de segurança variadas, o que inclui muitas interfaces internas, muitos DMZs e até mesmo muitas interfaces externas, se desejado, esses termos são usados em sentido geral apenas.

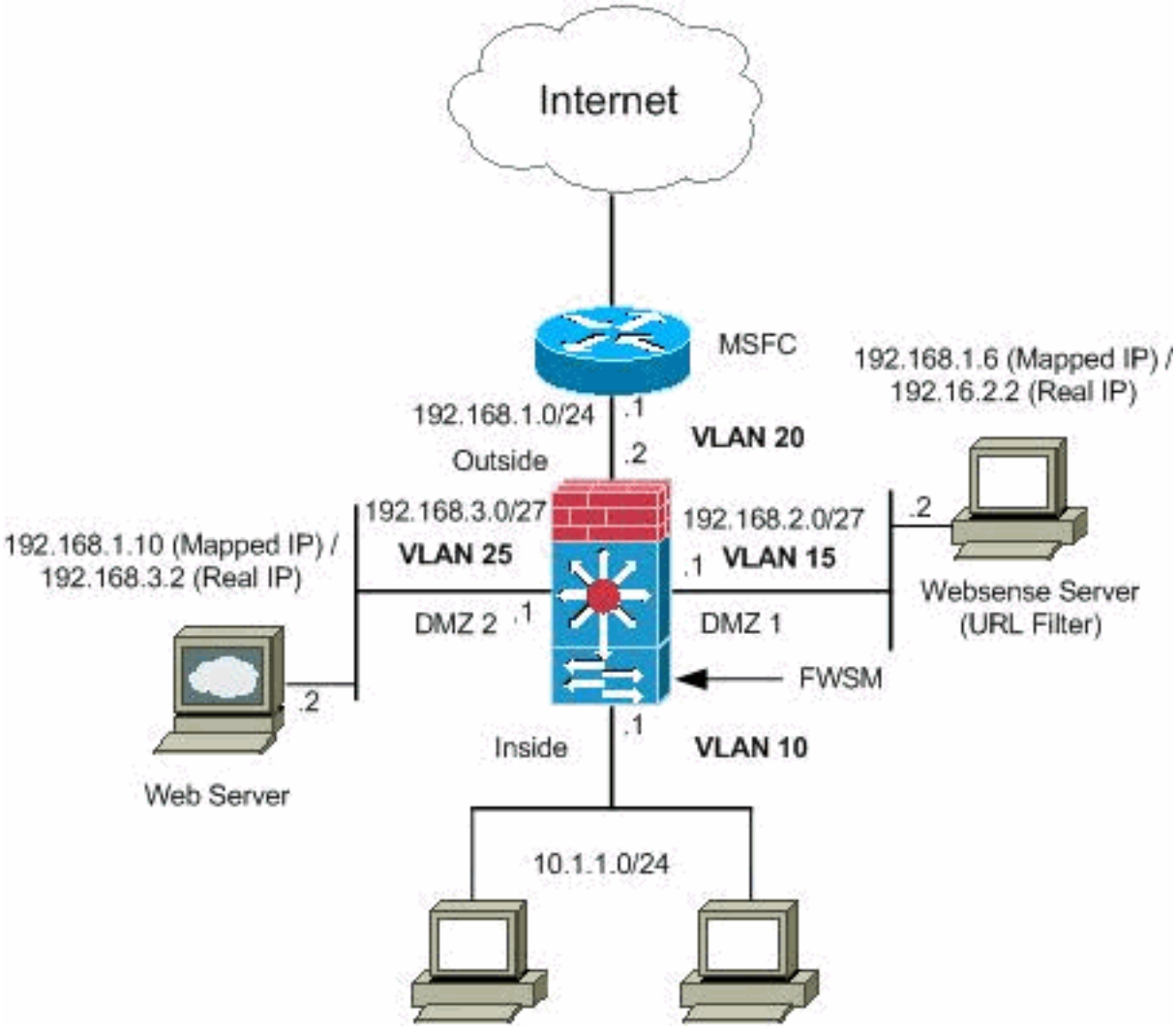
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Observação: os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. Eles são endereços RFC 1918, que foram usados em um ambiente de laboratório.

Configurações

Este documento utiliza as seguintes configurações:

- Configuração do Switch Catalyst 6500 Series
- Configuração do FWSM

Configuração do Switch Catalyst 6500 Series

1. Você pode instalar o FWSM nos Catalyst 6500 Series Switches ou nos Cisco 7600 Series Routers. A configuração de ambas as séries é idêntica e a série é chamada genericamente neste documento como o **switch**.**Observação:** você precisa configurar o switch adequadamente antes de configurar o FWSM.
2. **Atribuir VLANs ao módulo de serviços de firewall** — Esta seção descreve como atribuir VLANs ao FWSM. O FWSM não inclui nenhuma interface física externa. Em vez disso, ele usa interfaces VLAN. A atribuição de VLANs ao FWSM é semelhante à forma como você atribui uma VLAN a uma porta do switch; o FWSM inclui uma interface interna para o Switch Fabric Module, se presente, ou o barramento compartilhado.**Observação:** consulte a seção

Configurando VLANs do Guia de Configuração de Software dos Catalyst 6500 Switches para obter mais informações sobre como criar VLANs e atribuí-las às portas do switch.**Diretrizes de VLAN:**Você pode usar VLANs privadas com o FWSM. Atribuir a VLAN principal ao FWSM; o FWSM trata automaticamente o tráfego de VLAN secundário.Você não pode usar VLANs reservadas.Você não pode usar a VLAN 1.Se você usar o failover de FWSM dentro do mesmo chassi do switch, não atribua as VLANs que você reservou para comunicação com failover e stateful a uma porta do switch. Mas, se você usar o failover entre os chassis, deverá incluir as VLANs na porta de tronco entre os chassis.Se você não adicionar as VLANs ao switch antes de atribuí-las ao FWSM, as VLANs serão armazenadas no banco de dados do mecanismo supervisor e enviadas ao FWSM assim que forem adicionadas ao switch.Atribua VLANs ao FWSM antes de atribuí-las ao MSFC.As VLANs que não atendem a essa condição são descartadas do intervalo de VLANs que você tenta atribuir no FWSM.**Atribuir VLANs ao FWSM no Cisco IOS Software:**No software Cisco IOS, crie até 16 grupos de VLAN de firewall e atribua os grupos ao FWSM. Por exemplo, você pode atribuir todas as VLANs a um grupo, criar um grupo interno e um grupo externo ou criar um grupo para cada cliente. Cada grupo pode conter VLANs ilimitadas.Você não pode atribuir a mesma VLAN a vários grupos de firewall; no entanto, você pode atribuir vários grupos de firewall a um FWSM e pode atribuir um único grupo de firewall a vários FWSMs. As VLANs que você deseja atribuir a vários FWSMs, por exemplo, podem residir em um grupo separado das VLANs que são exclusivas de cada FWSM.Conclua as etapas para atribuir VLANs ao FWSM:

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

O `vlan_range` pode ser uma ou mais VLANs, por exemplo, de 2 a 1000 e de 1025 a 4094, identificadas como um único número (n) como 5, 10, 15 ou um intervalo (n-x) como 5-10, 10-20.**Observação:** as portas roteadas e as portas WAN consomem VLANs internas, portanto, é possível que as VLANs no intervalo 1020-1100 já estejam em uso.**Exemplo:**

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

Conclua as etapas para atribuir os grupos de firewall ao FWSM.

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

O `firewall_group` é um ou mais números de grupo como um único número (n) como 5 ou um intervalo como 5-10.**Exemplo:**

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

Atribuir VLANs ao FWSM no Catalyst Operating System Software —No Catalyst OS Software, você atribui uma lista de VLANs ao FWSM. Você pode atribuir a mesma VLAN a vários FWSMs, se desejado. A lista pode conter VLANs ilimitadas.Conclua as etapas para atribuir VLANs ao FWSM.

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

A `vlan_list` pode ser uma ou mais VLANs, por exemplo, de 2 a 1000 e de 1025 a 4094, identificadas como um único número (n) como 5, 10, 15 ou um intervalo (n-x) como 5-10, 10-20.

3. **Adicionar interfaces virtuais comutadas ao MSFC** — Uma VLAN definida no MSFC é chamada de interface virtual comutada. Se você atribuir a VLAN usada para SVI ao FWSM,

as rotas MSFC entre o FWSM e outras VLANs de Camada 3.Por motivos de segurança, por padrão, somente uma SVI pode existir entre a MSFC e o FWSM. Por exemplo, se você configurar o sistema de forma incorreta com vários SVIs, poderá acidentalmente permitir que o tráfego passe pelo FWSM se atribuir as VLANs internas e externas ao MSFC.Conclua as etapas para configurar o SVI

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

Exemplo:

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

Configuração do Switch Catalyst 6500 Series

`!--- 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`

Observação: entre no FWSM a partir do switch com o comando apropriado para o seu sistema operacional de switch:

- Cisco IOS Software:

```
Router#session slot
```

- Software Catalyst OS:

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

(Opcional) Compartilhando VLANs com outros módulos de serviço—Se o switch tiver outros módulos de serviço, por exemplo, Mecanismo de controle de aplicativos (ACE), é possível que você tenha que compartilhar algumas VLANs com esses módulos de serviço. Consulte Service Module Design with ACE and FWSM para obter mais informações sobre como otimizar a configuração do FWSM quando você trabalha com esses outros módulos.

Configuração do FWSM

1. **Configurar interfaces para FWSM** — Antes de permitir tráfego através do FWSM, é necessário configurar um nome de interface e um endereço IP. Você também deve alterar o nível de segurança do padrão, que é 0. Se você nomear uma interface `interna` e não definir o nível de segurança explicitamente, o FWSM definirá o nível de segurança como 100.**Observação:** cada interface deve ter um nível de segurança de 0 (mais baixo) a 100 (mais alto). Por exemplo, você deve atribuir sua rede mais segura, como a rede do host interno, ao nível 100, enquanto a rede externa conectada à Internet pode ser do nível 0. Outras redes, como DMZs, podem estar no meio.Você pode adicionar qualquer ID de VLAN à configuração, mas somente as VLANs, por exemplo, 10, 15, 20 e 25, que são atribuídas

ao FWSM pelo switch podem transmitir tráfego. Use o comando **show vlan** para ver todas as VLANs atribuídas ao FWSM.

```
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
```

Dica: no comando **nameif** *<name>* , o *nome* é uma string de texto com até 48 caracteres e não diferencia maiúsculas de minúsculas. Você pode alterar o nome se digitar novamente este comando com um novo valor. Não digite o formulário no, pois esse comando faz com que todos os comandos que se referem a esse nome sejam excluídos.

2. **Configure a rota padrão:**

```
route outside 0.0.0.0 0.0.0.0 192.168.1.1
```

Uma rota padrão identifica o endereço IP do gateway (192.168.1.1) para o qual o FWSM envia todos os pacotes IP para os quais não tem uma rota aprendida ou estática. Uma rota padrão é simplesmente uma rota estática com 0.0.0.0/0 como o endereço IP destino. As rotas que identificam um destino específico têm precedência sobre a rota padrão.

3. O **NAT dinâmico** converte um grupo de endereços reais (10.1.1.0/24) em um pool de endereços mapeados (192.168.1.20-192.168.1.50) que são roteáveis na rede de destino. O pool mapeado pode incluir menos endereços do que o grupo real. Quando um host que você deseja converter acessa a rede de destino, o FWSM atribui a ele um endereço IP do pool mapeado. A tradução é adicionada somente quando o host real inicia a conexão. A conversão está em vigor somente durante a conexão, e um determinado usuário não mantém o mesmo endereço IP após o tempo limite de tradução.

```
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
```

Você precisa criar uma ACL para negar o tráfego da rede interna 10.1.1.0/24 para entrar na rede DMZ1 (192.168.2.0) e permitir que os outros tipos de tráfego para a Internet através da aplicação da *Internet* ACL à interface interna como direção interna para o tráfego de entrada.

4. **O NAT estático** cria uma tradução fixa de endereços reais para endereços mapeados.Com o NAT dinâmico e o PAT, cada host usa um endereço ou porta diferente para cada tradução subsequente. Como o endereço mapeado é o mesmo para cada conexão consecutiva com NAT estático e existe uma regra de conversão persistente, o NAT estático permite que os hosts na rede de destino iniciem o tráfego para um host traduzido, se houver uma lista de

acesso que permita isso.A principal diferença entre o NAT dinâmico e um intervalo de endereços para o NAT estático é que o NAT estático permite que um host remoto inicie uma conexão com um host traduzido, se houver uma lista de acesso que permita, enquanto o NAT dinâmico não. Você também precisa de um número igual de endereços mapeados como endereços reais com NAT estático.

```
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
```

Estas são as duas instruções de NAT estático exibidas. O primeiro serve para converter o IP real 192.168.2.2 na interface interna para o IP 192.168.1.6 mapeado na sub-rede externa, desde que a ACL permita o tráfego da origem 192.168.1.30 para o IP 192.168.1 mapeado.6 para acessar o servidor Websense na rede DMZ1. Da mesma forma, a segunda instrução de NAT estático pretendia converter o IP real 192.168.3.2 na interface interna para o IP 192.168.1.10 mapeado na sub-rede externa, desde que a ACL permita o tráfego da Internet para o IP 192.168.1.10 mapeado para acessar o servidor Web na rede DMZ2 e tenha o número da porta udp no intervalo de 8766 a 30000.

5. O comando **url-server** designa o servidor que executa o aplicativo de filtragem de URL do Websense. O limite é de 16 servidores de URL em modo de contexto único e quatro servidores de URL em multimodo, mas você pode usar apenas um aplicativo, N2H2 ou Websense, por vez. Além disso, se você alterar sua configuração no Security Appliance, isso não atualizará a configuração no servidor de aplicativos. Isso deve ser feito separadamente, de acordo com as instruções do fornecedor.O comando **url-server** deve ser configurado antes de você emitir o comando **filter** para HTTPS e FTP. Se todos os servidores de URL forem removidos da lista de servidores, todos os comandos de filtro relacionados à filtragem de URL também serão removidos.Depois de designar o servidor, ative o serviço de filtragem de URL com o comando **filter url**.

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

O comando **filter url** permite a prevenção do acesso de usuários de saída de URLS da World Wide Web que você designar com o aplicativo de filtragem Websense.

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

Configuração do 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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para visualizar uma análise da saída do comando **show**.

1. Visualize as informações do módulo de acordo com o seu sistema operacional para verificar se o switch reconhece o FWSM e o colocou on-line: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
```

Observação: o comando **show module** mostra seis portas para o FWSM. Essas são portas internas agrupadas como um 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. Insira o comando para o seu sistema operacional para visualizar a partição de inicialização atual:Cisco IOS Software:

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

Exemplo:

```
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
```

Exemplo:

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

Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

1. **Definindo a partição de inicialização padrão** — Por padrão, o FWSM é inicializado a partir da partição do aplicativo **cf:4**. Mas você pode optar por inicializar a partir da partição do aplicativo **cf:5** ou na partição de manutenção **cf:1**. Para alterar a partição de inicialização padrão, digite o comando para o seu sistema operacional:Cisco IOS Software:

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

Em que n é 1 (manutenção), 4 (pedido) ou 5 (pedido).Software Catalyst OS:

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

Em que n é 1 (manutenção), 4 (pedido) ou 5 (pedido).

2. **Redefinindo o FWSM no Cisco IOS Software** —Para redefinir o FWSM, insira o comando como mostrado:

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

O argumento **cf:n** é a partição, 1 (manutenção), 4 (aplicação) ou 5 (aplicação). Se você não especificar a partição, a partição padrão será usada, que normalmente é **cf:4**.A opção **mem-test-full** executa um teste de memória completa, que leva aproximadamente seis minutos.**Exemplo:**

```
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 ...
```

Para o software **Catalyst OS**:

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

Se **cf:n** for a partição, 1 (manutenção), 4 (aplicação) ou 5 (aplicação). Se você não especificar a partição, a partição padrão será usada, que normalmente é **cf:4**.

Observação: o NTP não pode ser configurado no FWSM, pois ele tira suas configurações do Switch.

Problema: Não é possível passar o tráfego da VLAN do FWSM para o sensor IPS 4270

Você não pode passar o tráfego do FWSM para os sensores IPS.

Solução

Para forçar o tráfego através do IPS, o truque é criar uma VLAN auxiliar para efetivamente quebrar uma das VLANs atuais em duas e depois conectá-las. Verifique este exemplo com a VLAN 401 e 501 para esclarecer:

- Se quiser verificar o tráfego na **VLAN 401** principal, crie outra **VLAN 501** de vlan (VLAN auxiliar). Em seguida, desative a interface VLAN 401, que os hosts em 401 usam atualmente como seu gateway padrão.
- Em seguida, ative a interface da VLAN 501 com o *mesmo* endereço que você desativou anteriormente na interface da VLAN 401.
- Coloque uma das interfaces IPS na VLAN 401 e a outra na VLAN 501.

Tudo o que você precisa fazer é mover o gateway padrão para a VLAN 401 para a VLAN 501. Você precisa fazer as alterações semelhantes para VLANs, se presentes. Observe que as VLANs são essencialmente como segmentos de LAN. Você pode ter um gateway padrão em um pedaço de fio diferente dos hosts que o usam.

Emissão de pacotes fora de ordem no FWSM

Como posso resolver o problema dos pacotes desordenados no FWSM?

Solução

Emita o comando sysopt np Completion unit no modo de configuração global para resolver o problema de pacote fora de ordem no FWSM. Esse comando foi introduzido no FWSM Versão 3.2(5) e garante que os pacotes sejam encaminhados pela mesma ordem em que foram recebidos.

Problema: Não é possível passar pacotes roteados assimetricamente pelo firewall

Você não pode passar pacotes roteados assimetricamente pelo firewall.

Solução

Execute o comando set connection advanced-options tcp-state-bypass no modo de configuração de classe para passar pacotes roteados assimetricamente pelo firewall. Esse comando foi introduzido na versão 3.2(1) do FWSM.

Suporte a Netflow no FWSM

O FWSM é compatível com o Netflow?

Solução

O Netflow não é suportado no FWSM.

Informações Relacionadas

- Página de suporte do módulo de serviços de firewall Cisco Catalyst 6500 Series
- Página de suporte dos switches Cisco Catalyst 6500 Series
- Página de suporte do Cisco 7600 Series Router
- Interceptação TCP FWSM e cookies SYN explicados
- Suporte Técnico e Documentação - Cisco Systems