Exemplo da configuração básica FWSM

Índice

Introdução

Este documento descreve como configurar a configuração básica do módulo de serviços de firewall (FWSM) instalou nos Cisco 6500 Series Switch ou nos Cisco 7600 Series Router. Isto inclui a configuração do endereço IP de Um ou Mais Servidores Cisco ICM NT, do roteamento padrão, das indicações estáticas e dinâmicas do NATing, do Access Control Lists (ACLs) a fim permitir o tráfego desejado ou obstruir o tráfego não desejado, dos serveres de aplicativo como Websense para a inspeção do tráfego do Internet da rede interna, e do web server para os usuários do Internet.

Nota: Em uma Alta disponibilidade da encenação FWSM (HA), o Failover pode somente com sucesso sincronização quando as chaves de licença são exatamente as mesmas entre os módulos. Consequentemente, o Failover não pode trabalhar entre os FWSM com licenças diferentes.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Módulo de serviços de firewall que executa a versão de software 3.1 e mais atrasado
- Catalyst 6500 Series Switch, com os componentes requeridos como mostrado:Supervisor Engine com software do ® do Cisco IOS, que é sabido como o Cisco IOS do supervisor, ou Catalyst Operating System (OS). Veja a tabela para o motor e os software release do supervisor suportado.Multilayer Switch Feature Card (MSFC) 2 com Cisco IOS Software. Veja a tabela para Cisco IOS Software Release apoiados.

1 O FWSM não apoia o Supervisor 1 ou o 1A.

2When que você usa o OS do catalizador no supervisor, você pode usar qualquens um Cisco IOS Software Release apoiados no MSFC. Quando você usa o Cisco IOS Software no supervisor, você usa a mesma liberação no MSFC.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Produtos Relacionados

Esta configuração pode igualmente ser usada para os Cisco 7600 Series Router, com os componentes requeridos como mostrado:

- Supervisor Engine com Cisco IOS Software. Veja a tabela para o motor e os Cisco IOS Software Release do supervisor suportado.
- MSFC2 com Cisco IOS Software. Veja a tabela para Cisco IOS Software Release apoiados.

Convenções

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

Informações de Apoio

O FWSM é um de capacidade elevada, espaço-economia, o módulo do firewall stateful que instala nos Catalyst 6500 Series Switch e nos Cisco 7600 Series Router.

Os Firewall protegem redes internas do acesso não autorizado por usuários em uma rede externa. O Firewall pode igualmente proteger redes internas de se, por exemplo, quando você mantém uma rede dos recursos humanos para separar de uma rede de usuário. Se você tem os recursos de rede que precisam de estar disponíveis a um usuário externo, tal como uma Web ou um servidor FTP, você pode colocar estes recursos em uma rede separada atrás do Firewall,

chamado uma zona desmilitarizada (DMZ). O Firewall permite acesso limitado ao DMZ, mas porque o DMZ inclui somente os server públicos, um ataque lá afeta somente os server e não afeta as outras redes internas. Você pode igualmente controlar quando redes externas internas do acesso de usuários, por exemplo, o acesso ao Internet, se você permite somente determinados endereços para fora, exige a autenticação ou a autorização, ou coordena-os com um server externo da Filtragem URL.

O FWSM inclui muitos recursos avançados, tais como os contextos de segurança múltiplos que são similares aos Firewall virtualizados, (camada 2) Firewall transparente ou (camada 3) operação roteado do Firewall, centenas de relações, e muito mais características.

Durante o exame das redes conectadas a um Firewall, a rede externa é na frente do Firewall, a rede interna é protegida e atrás do Firewall, e um DMZ, quando atrás do Firewall, permitir acesso limitado aos usuários externos. Porque o FWSM o deixa configurar muitas relações com políticas de segurança variadas, que inclui muitas interfaces internas, muitos DMZ, e mesmo muitas interfaces externas se desejado, estes termos são usados em um sentido geral somente.

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:

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

Configurações

Este documento utiliza as seguintes configurações:

- Configuração do Catalyst 6500 Series Switch
- Configuração FWSM

Configuração do Catalyst 6500 Series Switch

1. Você pode instalar o FWSM nos Catalyst 6500 Series Switch ou nos Cisco 7600 Series Router. A configuração da série é idêntica e as séries são referidas genericamente neste documento como o **interruptor**.**Nota:** Você precisa de configurar apropriadamente o interruptor antes que você configure o FWSM.
2. **Atribua VLAN ao módulo de serviços de firewall** — Esta seção descreve como atribuir VLAN ao FWSM. O FWSM não inclui nenhuma interfaces física externo. Em lugar de, usa interfaces de VLAN. Atribuir VLAN ao FWSM é similar a como você atribui um VLAN a uma

porta de switch; o FWSM inclui uma interface interna ao módulo switch fabric, se presente, ou o barramento compartilhado.**Nota:** Refira a seção configurando VLAN do manual de configuração do software dos Catalyst 6500 Switch para obter mais informações sobre de como criar VLAN e atribui-los às portas de switch.**Diretrizes VLAN:**Você pode usar VLAN privados com o FWSM. Atribua o VLAN principal ao FWSM; o FWSM segura automaticamente o tráfego do VLAN secundário.Você não pode usar VLAN reservados.Você não pode usar o VLAN1.Se você usa o Failover FWSM dentro do mesmo chassi do switch, não atribua o VLAN que você reservou para comunicações do Failover e do stateful a uma porta de switch. Mas, se você usa o Failover entre o chassi, você deve incluir os VLAN na porta de tronco entre o chassi.Se você não adiciona os VLAN ao interruptor antes que você os atribua ao FWSM, os VLAN estão armazenados no base de dados do Supervisor Engine e enviados ao FWSM assim que forem adicionados ao interruptor.Atribua VLAN ao FWSM antes que você os atribua ao MSFC.Os VLAN que não satisfazem esta circunstância são rejeitados da escala dos VLAN que você tenta atribuir no FWSM.**Atribua VLAN ao FWSM no Cisco IOS Software:**No Cisco IOS Software, crie até 16 grupos vlan do Firewall, e atribua então os grupos ao FWSM. Por exemplo, você pode atribuir todos os VLAN a um grupo, ou você pode criar um grupo interno e um grupo exterior, ou você pode criar um grupo para cada cliente. Cada grupo pode conter VLAN ilimitados.Você não pode atribuir o mesmo VLAN aos grupos múltiplos do Firewall; contudo, você pode atribuir grupos múltiplos do Firewall a um FWSM e você pode atribuir um único grupo do Firewall aos FWSM múltiplos. Os VLAN que você quer atribuir aos FWSM múltiplos, por exemplo, podem residir em um grupo separado dos VLAN que são originais a cada FWSM.Termine as etapas a fim atribuir VLAN ao FWSM:`Router(config)#` **`firewall vlan-group firewall_group vlan_range`** `0 vlan_range` pode ser uns ou vários VLAN, por exemplo, 2 a 1000 e desde 1025 a 4094, identificado como qualquer um um único número (n) como 5, 10, 15 ou uma escala (n-x) como 5-10, 10-20.**Nota:** As portas roteada e as portas de WAN consomem VLAN internos, assim que é possível que os VLAN na escala 1020-1100 podem já estar no uso.**Exemplo:**
`firewall vlan-group 1 10,15,20,25` Termine as etapas a fim atribuir os grupos do Firewall ao FWSM.`Router(config)#` **`firewall module module_number vlan-group firewall_group`** `0 firewall_group` é uns ou vários números do grupo como um único número (n) como 5 ou uma escala como 5-10.**Exemplo:**
`firewall module 1 vlan-group 1` **Atribua VLAN ao FWSM no Catalyst Operating System Software** — no Catalyst OS Software, você atribui uma lista de VLAN ao FWSM. Você pode atribuir o mesmo VLAN aos FWSM múltiplos se desejado. A lista pode conter VLAN ilimitados.Termine as etapas a fim atribuir VLAN ao FWSM.`Console> (enable)` **`set vlan vlan_list firewall-vlan mod_num`** `0 vlan_list` pode ser uns ou vários VLAN, por exemplo, 2 a 1000 e desde 1025 a 4094, identificado como qualquer um um único número (n) como 5, 10, 15 ou uma escala (n-x) como 5-10, 10-20.

3. **Adicionar interfaces virtuais comutadas ao MSFC** — Um VLAN definido no MSFC é chamado um Switched Virtual Interface. Se você atribui o VLAN usado para o SVI ao FWSM, a seguir as rotas MSFC entre o FWSM e outro mergulham 3 VLAN.Por razões de segurança, à revelia, somente um SVI pode existir entre o MSFC e o FWSM. Por exemplo, se você desconfigura o sistema com SVI múltiplos, você pode acidentalmente permitir que o tráfego passe em torno do FWSM se você atribui ambos os VLAN internos e exteriores ao MSFC.Termine as etapas a fim 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 Catalyst 6500 Series Switch
!--- 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: Sessão dentro ao FWSM do interruptor com o comando apropriado para seu sistema operacional do interruptor:

- Cisco IOS Software:`Router#session slot <number> processor 1`
- Catalyst OS Software:`Console> (enable) session module_number`

(Opcional) compartilhando de VLAN com os módulos de outro serviço — se o interruptor tem os módulos de outro serviço, por exemplo, o motor do controle de aplicativo (ACE), é possível que você tem que compartilhar de alguns VLAN com estes módulos de serviço. Refira o projeto do módulo de serviço com ACE e FWSM para obter mais informações sobre de como aperfeiçoar a configuração FWSM quando você trabalha com tais outros módulos.

Configuração FWSM

1. **Configurar relações para o FWSM** — Antes que você possa permitir o tráfego com o FWSM, você precisa de configurar um nome da relação e um endereço IP de Um ou Mais Servidores Cisco ICM NT. Você deve igualmente mudar o nível de segurança do padrão, que é 0. Se você nomeia uma relação `para dentro`, e você não ajusta o nível de segurança explicitamente, a seguir o FWSM ajusta o nível de segurança a 100.**Nota:** Cada relação deve ter um nível de segurança de 0 (mais baixo) a 100 (o mais altamente). Por exemplo, você deve atribuir sua rede mais segura, tal como a rede do host interno, ao nível 100, quando a rede externa conectada ao Internet puder ser o nível 0. Outras redes, tais como DMZ, podem ser in-between.Você pode adicionar todo o ID de VLAN à configuração, mas somente os VLAN, por exemplo, 10, 15, 20 e 25, que são atribuídos ao FWSM pelo interruptor podem passar o tráfego. Use o **comando show vlan** a fim ver todos os VLAN atribuídos 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 do *<name> do* **nameif**, o *nome* é uma sequência de caracteres de texto até 48 caráteres e não é diferenciando maiúsculas e minúsculas. Você pode mudar o nome se você reenter este comando com um valor novo. Não incorpore nenhum formulário, porque esse comando causa os comandos all que referem esse nome a ser suprimido.
2. **Configurar a rota padrão:**
   `route outside 0.0.0.0 0.0.0.0 192.168.1.1` Uma rota padrão identifica o endereço IP de Gateway (192.168.1.1) a que o FWSM envia todos os pacotes IP para que não tem um instruído ou uma rota estática. Uma rota padrão é simplesmente uma rota estática com o 0.0.0.0/0 como o endereço IP de destino. As rotas que identificam um destino específico tomam a precedência sobre a rota padrão.
3. **O NAT dinâmico** traduz um grupo dos endereços reais (10.1.1.0/24) a um pool dos endereços traçados (192.168.1.20-192.168.1.50) que são roteável na rede de destino. O pool traçado pode incluir menos endereços do que o grupo real. Quando um host que você quer traduzir alcança a rede de destino, o FWSM atribui-lhe um endereço IP de Um ou Mais Servidores Cisco ICM NT do pool traçado. A tradução é adicionada somente quando o host

real inicia a conexão. A tradução é no lugar somente para a duração da conexão, e um usuário dado não mantém o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT após os tempos da tradução para fora.
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 de criar um ACL a fim negar o tráfego da rede interna 10.1.1.0/24 para entrar na rede DMZ1 (192.168.2.0) e para permitir para dentro os outros tipos do tráfego ao Internet com o pedido do *Internet* ACL à interface interna como o sentido para o tráfego de entrada.

4. O NAT estático cria uma tradução fixa de endereço real ao endereço traçado. Com NAT dinâmico e PANCADINHA, cada host usa um endereço ou uma porta diferente para cada tradução subsequente. Porque o endereço traçado é o mesmo para cada conexão consecutiva com o NAT estático, e uma regra de tradução persistente existe, o NAT estático permite que os anfitriões na rede de destino iniciem o tráfego a um host traduzido, se há uma lista de acessos que o permita.O principal diferença entre o NAT dinâmico e um intervalo de endereço para o NAT estático é que o NAT estático permite que um host remoto inicie uma conexão a um host traduzido, se há uma lista de acessos que o permita, quando o NAT dinâmico não fizer. Você igualmente precisa um número igual de endereços traçados 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 indicações do NAT estático mostradas. Primeiro está significado traduzir o IP real 192.168.2.2 na interface interna ao IP traçado 192.168.1.6 na sub-rede exterior contanto que o ACL permite que o tráfego da fonte 192.168.1.30 ao IP traçado 192.168.1.6 a fim alcançar o servidor websense na rede DMZ1. Similarmente, a segunda indicação do NAT estático significou traduzir o IP real 192.168.3.2 na interface interna ao IP traçado 192.168.1.10 na sub-rede exterior contanto que o ACL permite que o tráfego do Internet ao IP traçado 192.168.1.10 a fim alcançar o web server na rede DMZ2 e ter o número de porta UDP na escala de 8766 a 30000.
5. O comando do URL-**server** designa o server que executa o aplicativo da Filtragem URL de Websense. O limite é 16 server URL no único modo do contexto e quatro server URL no multi-modo, mas você pode usar somente um aplicativo, N2H2 ou Websense, em um momento. Adicionalmente, se você muda sua configuração na ferramenta de segurança, isto não atualiza a configuração no server de aplicativo. Isto deve ser feito separadamente, do acordo às instruções do vendedor.O comando do URL-**server** deve ser configurado antes que você emita o comando do **filtro** para o HTTPS e o FTP. Se todos os server URL são removidos da lista de servidor, a seguir todos os comandos do filtro relativos à Filtragem URL estão removidos igualmente.Uma vez que você designa o server, permita o serviço da Filtragem URL com o **comando url do filtro**.
url-server (dmz1) vendor websense host 192.168.2.2 timeout 30 protocol TCP version 1 connections 5 **O comando url do filtro** permite a prevenção do acesso dos usuários externos do world wide web URL que você designa com Websense que filtra o aplicativo.
filter url http 10.1.1.0 255.255.255.0 0 0

Configuração 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 (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use o OIT a fim ver uma análise do emissor de comando de execução.

1. Veja a informação de módulo do acordo a seu sistema operacional a fim verificar que o interruptor reconhece o FWSM e o trouxe em linha: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

Catalyst OS Software:`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: O comando show module** mostra seis portas para o FWSM. Estas são as portas internas que são agrupadas junto 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. Incorpore o comando para seu sistema operacional a fim ver a separação de bota 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 ]:`Catalyst OS Software:`Console> (enable) **show boot device mod_num**` **Exemplo:**`Console> (enable) **show boot device 6** Device BOOT variable = cf:5`

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

1. **Ajustando a separação de bota do padrão** — À revelia, as botas FWSM do partição de aplicativo **cf:4**. Mas, você pode escolher carreg do partição de aplicativo **cf:5** ou na separação da manutenção **cf:1**. A fim mudar a separação de bota do padrão, incorpore o comando para seu sistema operacional:Cisco IOS Software:`Router(config)#boot device module mod_num cf:n` Onde n é 1 (manutenção), 4 (aplicativo), ou 5 (aplicativo).Catalyst OS Software:`Console> (enable) **set boot device cf:n mod_num**` Onde n é 1 (manutenção), 4 (aplicativo), ou 5 (aplicativo).
2. **Restaurando o FWSM no Cisco IOS Software** — A fim restaurar o FWSM, incorpore o comando como mostrado:`Router#**hw-module module mod_num reset [cf:n] [mem-test-full]`** **Os cf:** o argumento **n** é a separação, 1 (manutenção), 4 (aplicativo), ou 5 (aplicativo). Se você não especifica a separação, a divisória padrão está usada, que é tipicamente **cf:4**.A opção MEM-teste-**FULL** executa um teste da memória cheia, que tome 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 **Catalyst OS Software**:`Console> (enable) **reset mod_num [cf:n]**` Onde **cf: n** é a separação, 1 (manutenção), 4 (aplicativo), ou 5 (aplicativo). Se você não especifica a separação, a divisória padrão está usada, que é tipicamente **cf:4**.

Nota: O NTP não pode ser configurado no FWSM, porque toma seus ajustes do interruptor.

Problema: Incapaz de passar o tráfego de VLAN do FWSM ao sensor 4270 IPS

Você é incapaz de passar o tráfego do FWSM aos sensores IPS.

Solução

A fim forçar o tráfego com o IPS, o truque é criar um VLAN auxiliar a fim quebrar eficazmente um

de seus VLAN atuais em dois e construi-los uma ponte sobre então junto. Verifique este exemplo com o VLAN 401 e 501 a fim esclarecer:

- Se você quer fazer a varredura do tráfego em **VLAN** principal **401**, crie um outro **VLAN** vlan **501** (VLAN auxillary). Desabilite então a interface de VLAN 401, que os anfitriões em 401 usam atualmente como seu gateway padrão.
- Permita em seguida a relação VLAN 501 com o *mesmo* endereço esse você desabilitou previamente na relação VLAN 401.
- Coloque uma das relações IPS em VLAN 401 e a outro em VLAN 501.

Tudo que você tem que fazer é mover o gateway padrão para VLAN 401 em VLAN 501. Você precisa de fazer as mudanças similares para VLAN se presente. Note que os VLAN são essencialmente como segmentos de LAN. Você pode ter um gateway padrão em uma parte diferente de fio do que os anfitriões que a usam.

Os pacotes estragados emitem no FWSM

Como posso eu resolver os pacotes estragados emito no FWSM?

Solução

Emita o comando da conclusão-unidade NP do sysopt no modo de configuração global a fim resolver a edição do pacote estragado no FWSM. Este comando foi introduzido na versão de FWSM 3.2(5) e assegura-se de que os pacotes estivessem enviados para fora na mesma ordem que foram recebidos.

Problema: Incapaz de passar assimetricamente pacotes roteado com o Firewall

Você é incapaz de passar assimetricamente pacotes roteado com o Firewall.

Solução

Emita o comando do TCP-estado-desvio das avançado-opções da conexão do grupo no modo de configuração de classe a fim passar assimetricamente pacotes roteado com o Firewall. Este comando foi introduzido na versão de FWSM 3.2(1).

Apoio do Netflow no FWSM

O FWSM apoia o Netflow?

Solução

O Netflow não é apoiado no FWSM.

Informações Relacionadas

- Página de suporte do Módulo de serviços de firewall Cisco Catalyst série 6500
- Página de suporte dos Cisco Catalyst 6500 Series Switch
- Página de suporte do Cisco 7600 Series Router

- Cookie FWSM TCP Intercept e SYN explicados
- Suporte Técnico e Documentação - Cisco Systems