Serviços de firewall Module(FWSM) FAQ

Índice

Introdução

Este documento contém as perguntas mais frequentes (FAQ) sobre o módulo de serviços do Firewall Services Module (FWSM) da Catalyst 6500 Series.

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

Recursos suportados

Q. Que é a versão mínima do código que eu preciso de executar o apoio meus FWSM, módulo intrusion detection system 2 (IDSM2), e módulo de serviço VPN (VPNSM)?

A. A versão de código apropriada depende do tipo de módulo do supervisor em seus 6500 ou 7600 chassis, assim como do tipo de software que você executa ([Hybrid] de Cactos ou [Native] do Cisco IOS). Veja esta tabela para versões de código específicas para seu módulo e Multilayer Switch Feature Card (MSFC).

	Sup1 (com MSFC)		Sup2 (com MSFC)		Sup720	
Módulo	Cisco IOS	CatOS	Cisco IOS	CatOS	Cisco IOS	CatOS
FWSM	12.1(13)E	7.5(1)	12.1(13)E	7.5(1)	12.2(14)SX1	8.2(1)
IDSM2	não suportado	7.6(1)	12.1(19)E	7.6(1)	12.2(14)SX1	8.2(1)
VPNSM	não suport	não suport	12.2(14)SY	não suport	12.2(17a)SX10	Não apoi

	ado	ado		ado		ado *

* Há uns planos para introduzir o apoio.

Nota: Refira a comparação do Cisco catalyst e dos sistemas operacionais do Cisco IOS para o Cisco Catalyst 6500 Series Switch para obter informações sobre das diferenças entre Cactos (híbrido) e Cisco IOS (nativo).

Q. Posso eu executar o FWSM, o módulo intrusion detection system 2 (IDSM2), e o módulo de serviço VPN (VPNSM) no mesmo chassi?

A. Sim, você pode executar estes módulos no mesmo chassi se o interruptor executa o software do Cisco IOS integrado com uma versão mínima do Cisco IOS Software Release 12.2(14)SY (Sup2) ou do 12.2(17a)SX10 (Sup720). Atualmente, não há nenhuma versão cactos que pode apoiar estes módulos de serviço nos mesmos 6500 ou 7600 chassis.

Q. Que são minhas configuração e opções de gerenciamento para o FWSM?

A. A configuração e as opções de gerenciamento incluem estes.

Opção	Versão	Descrição
Centro de gerenciamento para Firewall	Versões 1.1.1 e later*	Esta é uma interface baseada NA Web para configurar e controlar firewalls múltiplos. **Nota:** O apoio para grupos de serviço dentro do agrupamento do objeto é limitado. Os grupos de serviço são analisados gramaticalmente com sucesso, mas aplainam imediatamente. Isto afeta comandos com ICMP-**tipo**, **protocolo**, e palavras-chaves do **serviço**. Esta limitação aplica-se às versões 1.3 e anterior.
Monitorando o centro para a Segurança	Versões 1.2 e later*	Esta é uma interface baseada NA Web para monitorar dispositivos de segurança de Cisco. O software centraliza o gerenciamento syslog dos dispositivos de segurança múltiplos de Cisco com relatório flexível e opções da alerta.
Monitorando o centro para o desempenho	Versões 2.0 e later*	Este é uma interface baseada NA Web para monitorar e pesquisar defeitos a saúde e desempenho dos serviços que contribuem à segurança de rede. O Simple Network Management Protocol (SNMP) é o protocolo subjacente usado.
PDM	Versão	Esta é uma interface baseada NA Web para configurar, controlar, e monitorar um

	2.1	único Firewall. O gerenciador de dispositivo pix (PDM) deve ser instalado localmente no PIX Firewall.
Telnet	N/A	O telnet fornece o acesso remoto do comando line interface(cli) a um Firewall. **Nota:** A fim permitir o acesso do telnet à mais baixa interface de segurança (conhecida geralmente como a interface externa), você precisa de configurar o IPsec para o Gerenciamento.
Secure Shell (SSH)	N/A	O SSH fornece o acesso seguro do telecontrole CLI a um Firewall.
SNMP:	N/A	O SNMP fornece um método de monitorar o FWSM. **Nota:** O SNMP é de leitura apenas no FWSM.
Syslog	N/A	O Syslog fornece um método de monitorar o FWSM.

* Este software é parte de Este software fornece uma aproximação integrada a controlar dispositivos de segurança de Cisco através de uma relação com base em navegador para redes de empreendimento.

Q. Que é um SVI? Posso eu configurar SVI múltiplos?

A. O SVI representa o Switched Virtual Interface. Representa uma relação lógica da camada 3 em um interruptor. Para versões cactos mais cedo de 7.6(1) e os Cisco IOS Software Release mais cedo do que 12.2(14)SY, somente um SVI são permitidos como parte do Firewall VLAN. Ou seja somente uma relação da camada 3 pode ser configurada entre o FWSM e o Multilayer Switch Feature Card (MSFC). Uma tentativa de configurar SVI múltiplos produz um Mensagem de Erro do comando line interface(cli).

Para versões cactos 7.6(1) e mais atrasado e Cisco IOS Software Release 12.2(14)SY e Mais Recente, o FWSM suporta múltiplo SVI. À revelia, somente um SVI é apoiado. Use um destes comandos permitir o apoio para SVI múltiplos em seu interruptor.

- Para Cactos, as múltiplo-VLAN-relações do type set firewall permitem.Para o Cisco IOS, datilografe múltiplo-VLAN-relações do Firewall.

Se você configura seu interruptor para o FWSM VLAN e recebe um Mensagem de Erro que indique que você tem mais de um SVI, olhar em seu interruptor e/ou configuração de MSFC para se assegurar de que somente uma relação da camada 3 (ou a interface de VLAN) existam como parte do Firewall VLAN.

Nota: Use somente um SVI. Isto permite que você evite uma configuração complicada que envolva o roteamento de política.

Q. O FWSM apoia o SNMPv3?

A. Não.

Q. Quantos VLAN o FWSM apoia?

A. A versão de FWSM 1.1 apoia 100 2.1 VLAN e de versão de FWSM apoia 250 VLAN.

Q. O FWSM apoia o comando access-list compiled?

A. Desde que o FWSM compila automaticamente Listas de acesso no hardware após os segundos 10 da inatividade no CLI, não há nenhuma necessidade para Listas de acesso do turbocompressor. O 2.1 da versão de FWSM oferece a funcionalidade adicional de poder nomear quando as Listas de acesso são compiladas.

Q. Faz o apoio FWSM o comando? da referência-largura de banda do auto-custo do Open Shortest Path First (OSPF) IO

A. Não. O FWSM não está ciente das portas física conectadas a ele. Os custos de OSPF devem ser configurados manualmente para cada relação com o comando ospf cost.

Q. Posso eu executar o protocolo do Open Shortest Path First (OSPF) em uma topologia onde duas relações diferentes do FWSM conectem à mesma rede?

A. Sim. Esta funcionalidade é apoiada nas versões 2.1 e mais recente.

Q. Que protocolos de roteamento são apoiados pelo FWSM?

A. O Open Shortest Path First (OSPF) e o Routing Information Protocol (RIP) são os protocolos de roteamento apoiados. Para obter mais informações sobre do FWSM, refira a documentação disponível na página do Módulo de serviços de firewall Cisco Catalyst série 6500.

Q. O Multicast ([IGMP] v2 do protocolo de gestão do grupo do Internet e roteamento de transmissão múltipla stub) é apoiado no FWSM?

A. Sim. Esta funcionalidade é apoiada no 2.1 das versões de FWSM e mais tarde. Se você executa a versão 1.1, você pode usar o Generic Routing Encapsulation (GRE) que escava um túnel como uma ação alternativa.

Q. O FWSM apoia a Filtragem URL?

A. Sim. Websense é apoiado nas versões 1.1 e mais recente, com suporte adicional para o N2H2 adicionado na versão 2.1.

Q. Por que os pacotes fragmentados são deixados cair pelo FWSM?

A. À revelia, os pacotes fragmentados não podem atravessar o FWSM. Você pode usar o comando fragment configurar esta característica. Este comportamento difere daquele do PIX Firewall. Os protocolos comuns que usam pacotes fragmentados são Open Shortest Path First (OSPF) e Network File System (NFS).

Q. Posso eu terminar conexões de VPN em meu FWSM?

A. A funcionalidade de VPN não é apoiada no FWSM. A Terminação de conexões VPN é a responsabilidade do interruptor e/ou do módulo de serviços VPN. A licença 3DES é fornecida para propósitos do gerenciamento somente, como a conexão a uma relação da baixo-Segurança através do telnet, do Shell Seguro (ssh), e de HTTP seguro (HTTPS).

Q. O Authentication, Authorization, and Accounting (AAA) para o RAIO ou o TACACS+ é apoiado no FWSM?

A. O AAA é apoiado para o gerenciamento FWSM e o tráfego que passam com o FWSM. Refira a documentação de módulo dos serviços de firewall para detalhes adicionais.

O FWSM oferece a funcionalidade similar àquela do PIX Firewall, com as exceções de Listas de acesso carregável e de VPN. Com isto em mente, você pode usar estes documentos do PIX Firewall como guias para a configuração FWSM.

- Como executar a autenticação e ativação no Cisco Secure PIX Firewall (5.2 a 6.2)
- Realizando autenticação, autorização e relatório de usuários por meio do PIX versões 5.2 e posteriores

Q. Como eu executo uma recuperação de senha para o FWSM?

A. Refira estes documentos para obter informações sobre da recuperação de senha.

- Para a versão 1.1(1), refira a nota da configuração FWSM 1.1(1) em mudar e em recuperar senhas.
- Para versões 1.1(2) e 1.1(3), refira a nota da configuração FWSM 1.1(2) em mudar e em recuperar senhas.

Q. O FWSM apoia o Jumbo Frames?

A. Sim, o FWSM pode apoiar o Jumbo Frames.

Q. Como o FWSM responde quando recebe um pacote com seu endereço de origem como um endereço do laço de retorno?

A. Trata o pacote como inválido e deixa cair o pacote. À revelia, o FWSM deixa cair os pacotes com um endereço de origem inválido tal como um endereço do laço de retorno, um endereço de broadcast e um endereço de host do destino. Um mensagem de registro segundo as indicações deste exemplo é gerado.

```
%FWSM-2-106016: Deny IP spoof from (IP_address) to
 IP_address on interface interface_name.
```

Q. O PVLAN é apoiado no FWSM?

A. O apoio do PVLAN começa na versão de software 3.1. Se você executa uma versão de software mais cedo de 3.1, a única alternativa possível é conectar a porta misturada do PVLAN usando o cabo crossover a uma porta de acesso regular, e faz então o VLAN dessa porta de acesso firewalled.

Q. O número de linha da lista de acessos é apoiado no FWSM?

A. Esta característica é apoiada somente na versão de software 3.1 e mais atrasado.

Q. Pode você limitar o número de conexões que um usuário pode ter no FWSM?

A. Sim, você pode limitar as conexões com a ajuda da estrutura de política modular. Termine estas etapas a fim limitar o número de conexões:

1. Crie um mapa da classe a fim combinar o tráfego.
2. Coloque o mapa da classe a um mapa de política e use a conexão que limita no mapa de política.
3. Aplique o mapa de política usando a política de serviços.

Refira configurar limites e intervalos da conexão para mais informação e etapas detalhadas.

Q. Há alguma limitação na aplicação do Multicast no FWSM?

A. Sim. O FWSM não apoia a sub-rede 232.x.x.x como um nome do grupo, porque tem sido reservado já para o módulo de Serviços de segurança (SS).

Q. A transmissão direcionada é permitida com o FWSM?

A. Não. Ao contrário de um roteador, o FWSM não permite a transmissão direcionada através de suas relações. Uma ação alternativa mais similar é usar os recursos de Frame Relay DHCP incorporados para enviar transmissões de uma relação a outra.

Q. Pode o motor da inspeção HTTP detectar o tráfego NON-HTTP ou o tráfego não padronizado em uma sessão de HTTP?

A. Sim. O Firewall do aplicativo com inspeção avançada HTTP pode detectar e para controlar estes trafique. Refira a vista geral do motor da inspeção de aplicativo para mais informação.

Q. São as características da normalização no ASA e no FWSM compatíveis?

A. No FWSM, a normalização TCP aplica-se somente para traficar que bate o complexo TCP. O tráfego normal do plano dos dados (caminho rápido) não é afetado. Isto difere do ASA que todo o tráfego ASA está sujeitado ao normalizador.

No FWSM, se o normalizador é desabilitado as quedas do módulo de volta ao comportamento 2.3. Mas, se você desabilita o TCP-**normalizador do ponto de controle**, isto impede verificações restritas TCP, tais como a detecção de segmentos do out-of-sequence e de opções de TCP da monitoração, nos pacotes de TCP recebidos no plano do controle para a inspeção da camada 7 no FWSM, e não é executado. Assim, é aconselhável não o desabilitar. O FWSM não reserva ajustar em parâmetros do TCP-mapa do padrão.

Q. Nós precisamos de permitir/normalizador do desabilitação TCP?

A. Devido à incapacidade passar a alguma conexão a informação específica dos NP para controlar o plano, o normalizador TCP possivelmente não funciona corretamente todo o tempo no

FWSM. Adicionalmente, os TCP-mapas originais associados com as conexões não podem ser identificados. Assim, o FWSM confia no TCP-mapa do padrão que possivelmente não trabalham corretamente para todas as conexões. Devido a estas limitações, há uma necessidade de permitir/normalizador do desabilitação TCP no plano do controle para o tráfego que atravessa o Firewall. O FWSM não reserva ajustar em parâmetros do TCP-mapa do padrão.

Q. Que é o número máximo de entradas do mfib que um FWSM pode apoiar?

A. O número máximo de entradas é 5000 entradas.

Q. Como posso eu capturar pacotes no FWSM?

A. Os pacotes podem ser capturados no FWSM. O uso do CLI como a captura de pacote de informação não é apoiado no ASDM e o **comando capture** não é apoiado no ASDM. Refira comandos ignorada e da vista-Somente para mais informação. Refira a captura de pacotes para obter mais informações sobre da configuração do pacote que captura no FWSM. Refira ASA/PIX/FWSM: Pacote que captura usando o CLI e o exemplo da configuração ASDM para obter mais informações sobre de um exemplo de configuração da captura de pacote de informação.

Q. Que versão do ASDM O FWSM apoia?

A. Refira compatibilidade da liberação FWSM e ASDM para obter mais informações sobre compatibilidade da liberação FWSM e ASDM.

Licenciar

Q. Eu tenho uma licença para um FWSM que seja executado no modo de contexto múltiplo. Posso eu obter uma licença para um FWSM de reposição no caso de uma falha do hardware?

A. Você pode obter uma licença para o FWSM de reposição. Contudo, você precisa de colocar uma ordem para a licença de reposição FWSM enquanto você uma licença regular. No caso de uma falha do hardware, de um Suporte técnico de Cisco do contato verificar a falha e obter uma licença para o FWSM de reposição. Refira o Module Software Release do Firewall de Cisco 2.2(1) para a informação licenciando.

Q. O FWSM apoia relações compartilhadas múltiplo?

A. O FWSM não apoia relações compartilhadas múltiplo, mas pelo contrário você pode ter um VLAN através dos contextos múltiplos. Refira a partilha de recursos e de relações entre contextos para mais informação.

Edições VLAN

Q. Como eu coloco VLAN adicionais atrás do FWSM?

A. Use o **comando nameif** se você quer adicionar 200 vlan à configuração. O nível de segurança

deve estar entre 0 e 100. A sintaxe de comando complete é **level> do <security do name> do <interface do nameif vlan200**.

Q. Quantos VLAN posso eu colocar atrás do FWSM usando o único contexto, modo roteado?

A. Você pode colocar 1000 VLAN atrás do FWSM usando o único contexto, modo roteado.

Edições do sibilo

Q. Por que sou eu incapaz de sibilar diretamente meu FWSM em uma interface conectada?

A. À revelia, cada relação nega o Internet Control Message Protocol (ICMP). Use o **comando icmp** permitir este tráfego à relação. Este comportamento difere daquele do PIX.

Nota: Quando o ICMP à relação é negado pelo **comando icmp**, você ainda vê o MAC address correto na tabela do Address Resolution Protocol (ARP). Se você não vê o MAC address, veja a pergunta seguinte.

Q. Eu sou incapaz de sibilar diretamente meu FWSM em uma interface conectada, e eu não ver uma entrada do Address Resolution Protocol (ARP) para a relação. Eu estou executando o software de Cactos (ou híbrido) em meu interruptor. O que devo fazer?

A. Configurar as relações dentro da configuração FWSM (com o comando nameif) ou no [with the interface vlan command] do Multilayer Switch Feature Card (MSFC) antes que estejam configurados no interruptor (no módulo do supervisor em Cactos) pode fazer as relações aparecer como se não estão respondendo de todo, sem a resposta da entrada de ARP ou do Internet Control Message Protocol (ICMP).

Se você configurou uma relação no FWSM ou no MSFC que pertence ao Firewall VLAN antes que você configurou o interruptor, remover o FWSM ou a entrada de MSFC, recarregue o módulo, a seguir adicionar novamente a entrada.

Q. Por que sou eu incapaz de sibilar ou passar algum tráfego com o FWSM?

A. O Network Address Translation (NAT) deve ser configurado usando o 0 nat, nat/global, ou o comando static para que o tráfego passe com o FWSM de uma interface de segurança mais elevada (a interface interna) a uma interface de segurança mais baixa (interface externa).

Você deve igualmente usar o comando access-list executar as Listas de acesso que permitem o tráfego correr através do FWSM. À revelia, as Listas de acesso negam todo o tráfego em todas as relações (**deny ip any any**). Este comportamento difere da configuração padrão do PIX, que permite que o tráfego de mais altamente abaixe a Segurança e nega o tráfego de mais baixo à segurança mais elevada. Configurar uma lista de acessos com a **licença IP alguma** e aplique-a às relações da segurança elevada para conseguir o FWSM comportar-se como o PIX.

Q. Eu posso sibilar a relação FWSM que é conectada diretamente a minha rede,

mas eu sou incapaz de sibilar outras relações. É este normal?

A. Sim. Este é um mecanismo de segurança incorporado que igualmente exista no PIX Firewall.

Edições do Failover

Q. Posso eu configurar um Failover entre dois FWSM que executam versões de código diferentes?

A. Não O Failover exige que ambos os FWSM executam a mesma versão de código. Um mecanismo dentro da característica do Failover verifica a versão do par e impede o Failover se as versões de código são diferentes. Por este motivo, você deve promover ambos os FWSM ao mesmo tempo.

Q. Posso eu configurar um Failover entre dois FWSM em chassis diferentes?

A. Sim. Mas os FWSM devem ser conectados pela camada 2 em todas as relações. Ou seja todas as relações devem poder trocar um com o otro o [Address Resolution Protocol (ARP), and so forth] dos pacotes de transmissão da camada 2. Os pacotes do protocolo de failover não podem ser distribuídos na camada 3.

Q. Eu estabeleci um Failover entre dois FWSM, mas não são em sincronismo. Qual poderia ser o problema?

A. Assegure-se de que sua configuração cumpra estes requisitos de failover bem-sucedido.

- Ambos os FWSM devem executar a mesma versão de código.
- Ambos os FWSM devem ter o mesmo número de VLAN.
- Uma conexão da camada 2 deve existir entre todos os VLAN nos FWSM. Se os FWSM existem no chassi diferente com um tronco configurado entre ele, verifique que todos os VLAN existem e estão permitidos no tronco.

Q. Posso eu configurar o Failover para três ou mais unidades de FWSM, que são espalhadas sobre o chassi do switch diferente?

A. **Não** A instalação do Failover é apoiada somente para um par de FWSM, por exemplo, 2 unidades. Estas duas unidades podem estar em um mesmo interruptor ou em dois switch separados. Se você instala o FWSM secundário no mesmo interruptor que o FWSM preliminar, você protege contra a falha do módulo-nível. A fim proteger contra a falha do módulo-nível e assim como a falha do interruptor-nível, você pode instalar o FWSM secundário em um switch separado. O FWSM não coordena o Failover diretamente com o interruptor, mas trabalha harmoniosamente com a operação do Failover do interruptor. Refira a colocação intra e dos Inter-chassis do módulo para mais informação.

Diversos

Q. O FWSM tem uma etiqueta que indique, “não remove o cartão quando a luz de

status for verde ou o corrompimento de disco pode ocorrer.” O que isso significa?

A. O módulo do Firewall deve ser removido somente depois que você desabilita a potência usando um destes métodos. (Não há nenhuma preferência para um método particular.)

- Use o comando line interface(cli) do interruptor e emita um destes comandos.Cactos - **ajuste a *modificação da* potência do módulo para baixo**Cisco IOS ® Software - ***nenhuma* potência permite o *slot de módulo***
- Pressione o botão da **parada programada na** lâmina.
- Põe fisicamente para baixo o chassi.

Você pode remover o módulo de forma segura quando a luz de status não é verde.

Q. Eu usei o comando show module, e meu FWSM tem um estado de `defeituoso/de outro`. O que devo fazer?

A. Refira esta lista de verificação para pesquisar defeitos um FWSM com um estado de `defeituoso/de outro`.

- Assegure-se de que você execute uma versão suportada do código em seu interruptor.
- Assegure-se de que o FWSM possa coexistir com as outras lâminas posicionadas no mesmo chassi. Refira os Release Note do Catalyst 6500 e/ou o Software Advisor (clientes registrados somente) para mais informação.
- Se você executa Cactos/código híbrido em seu interruptor, restaure a configuração para o entalhe ocupado pelo módulo FWSM. Use estes comandos a fim fazer isto.Datilografe ***modificação* ajustada da potência do módulo para baixo** para pôr para baixo o FWSM.Datilografe a **modificação clara da configuração** para cancelar a configuração do interruptor associado com esse entalhe e para pôr acima o módulo.

Refira esta documentação para mais informação.

- Hardware Failure Checklist for Catalyst 4000, 5000, and 6000 Series Switches Running CatOS
- Pesquisar defeitos o hardware e os problemas comuns nos Catalyst 6000 Series Switch que executam o Cisco IOS integrado (modo nativo)

Se você continua a experimentar problemas, contacte o Suporte técnico de Cisco para um Troubleshooting mais adicional.

Q. Onde posso eu encontrar a documentação FWSM?

A. Os Release Note para o FWSM podem ser encontrados sob os Release Note do Catalyst 6500 Series. Para mais informação, refira a documentação disponível na página do Módulo de serviços de firewall Cisco Catalyst série 6500.

Q. Onde posso eu encontrar a informação nos Mensagens de Erro que eu ver em meu FWSM?

A. O decodificador do mensagem de erro (clientes registrados somente) fornece detalhes em muitos Mensagens de Erro FWSM. A documentação do produto em mensagens de sistema igualmente contém a informação util. Se você exige a assistência adicional, contacte o Suporte

técnico de Cisco.

Q. Onde posso eu encontrar a informação em erros existentes para meu FWSM?

A. Os detalhes em erros existentes podem ser encontrados no Bug Toolkit (clientes registrados somente).

Q. Que são as diferenças entre o PIX Firewall e o módulo de serviços de firewall?

A. O PIX e o FWSM são baseados no código similar. Contudo, há duas diferenças fundamentais. O PIX (apoio das ofertas) fornece a funcionalidade VPN e IDS. O FWSM não fornece a funcionalidade VPN e IDS porque estas características são oferecidas em outras placas de linha. Refira a folha de dados do Módulo de serviços do sistema de detecção de intrusões do Catalyst 6500 Series (IDSM-2) para obter mais informações sobre do Módulo de serviços do sistema de detecção de intrusões do Catalyst 6500 Series (IDSM-2). Refira a folha de dados do produto do Módulo de serviços do IPSec VPN do Catalyst 6500 para obter mais informações sobre do Módulo de serviços do IPSec VPN do Catalyst 6500.

Refira esta documentação para diferenças pequenas entre o PIX e o FWSM:

- Documentação técnica PIX
- Release Note PIX
- Referências de comando PIX
- Documentação técnica FWSM
- Release Note FWSM
- Referências de comandos FWSM

Q. Eu não poderia emitir comandos do grupo de acesso múltiplo no FWSM pela relação. O FWSM parece tomar somente um grupo de acesso pela relação. Por quê?

A. Quando você emitir estes comandos no FWSM, simplesmente o último **comando access-group** aparece:

```
access-group allow_icmp in interface outside
access-group allow_caltech in interface outside
```

Isto é porque o FWSM permite somente uma lista de acesso pela relação pelo sentido.

Q. Que informação é armazenada nas entradas do xlate no FWSM?

A. As entradas do xlate armazenam esta informação:

1. **Interface de origem** — Esta é a relação que o pacote está recebido, por exemplo, `fora`.
2. **Endereço IP de origem** — Este é o endereço IP de origem do pacote.
3. **Endereço IP de Um ou Mais Servidores Cisco ICM NT traduzido** — No caso de nenhumas declarações NAT, o endereço IP de Um ou Mais Servidores Cisco ICM NT traduzido e o endereço IP de origem são o mesmo.
4. **Interface de destino** — A relação que as folhas do pacote basearam na pesquisa na tabela de roteamento do endereço IP de destino do pacote.

Q. Que os valores e as estatísticas no **perfmon da mostra no** FWSM implicam?

A. Use o **comando show perfmon** a fim capturar a informação sobre o desempenho do FWSM.

```
FWSM#show perfmon FWSM#show console-output Context: my_context PERFMON STATS: Current Average
Xlates 0/s 0/s Connections 0/s 0/s TCP Conns 0/s 0/s UDP Conns 0/s 0/s URL Access 0/s 0/s URL
Server Req 0/s 0/s WebSns Req 0/s 0/s TCP Fixup 0/s 0/s TCP Intercept 0/s 0/s HTTP Fixup 0/s 0/s
FTP Fixup 0/s 0/s AAA Authen 0/s 0/s AAA Author 0/s 0/s AAA Account 0/s 0/s
```

`A corrente da` coluna mostra as estatísticas no intervalo atual, onde enquanto a última `média da` coluna mostra a média cumulativa desde que as estatísticas da última vez estiveram canceladas. Mostra-se como `/s` porque é a taxa, um pouco do que um valor absoluto.

As estatísticas mostradas na saída do comando são atualizadas em um intervalo de 120 segundos à revelia. O intervalo pode ser mudado com o comando do **intervalo do perfmon**.

```
FWSM#perfmon interval 20
```

Significa que a taxa das estatísticas relatadas na coluna `atual` está calculada cada 20 segundos. Além, sempre que você inscreve o **comando show perfmon**, as taxas são calculadas com as estatísticas nesse ponto do tempo.

O FWSM não inclui uma porta de console serial, mas algumas mensagens são indicadas somente em uma porta de Console, que inclua a saída do **perfmon da mostra** e dos comandos do **perfmon**. Use o comando do saída-**console da mostra** a fim ver o buffer de console, que inclui a saída do **comando show perfmon**.

Q. Haverá uma batida do desempenho no FWSM com **nenhum** comando? do **servicemodule da sessão de monitor**

`A.` A sessão span é exigida no FWSM devido a uma limitação do hardware de um ASIC para a replicação do tráfego. O FWSM precisa um ASIC para a replicação do pacote e a sessão span passa os pacotes para comutar para essa utilização da sessão span. O tráfego afetado por este comando é EtherChannel, Multicast e GRE distribuídos. Recomenda-se ter a sessão span configurada e não a remover.

Se por qualquer motivo você precisa do remover, certifique-se de que você não replicated o tráfego da natureza, por exemplo, o EtherChannel distribuído, que pode ser afetado pelo Field Notice: FN - 61935 - incompatibilidade do módulo de serviço do Catalyst 6500 Series e do 7600 Series com recirculação distribuída do EtherChannel e do pacote.

Q. Pode você aumentar a memória a fim armazenar mais Access Control Lists (ACLs)?

A. A memória atribuída para ACL no FWSM é limitada. Refira especificações - Ordene limites para obter mais informações sobre do alocamento de recursos FWSM.

Quando a memória atribuída para ACL em um contexto é excedida, você pode receber qualquens um Mensagens de Erro:

- `ERRO: Incapaz de adicionar, limite da configuração da lista de acesso alcançado`
- `ERRO: Incapaz de adicionar regras da política`
- `Incapaz de adicionar um furo à regra da política`

Algumas Listas de acesso usam mais memória do que outro. Depende do tipo de lista de acessos, e o limite que real o sistema pode apoiar é menos do que o máximo. O mapeamento

entre as regras e a alocação de memória não é um mapeamento um a um. Depende realmente da regra e como obtém programado no hardware.

Você tem duas opções para a otimização da utilização de memória ACE:

- Resuma e simplifique suas entradas ACE — isto pode ser feito se você termina estas práticas recomendadas:Use endereços contíguos dos anfitriões sempre que possível. Agregue indicações do host nos ACE/grupos de objetos em redes.Use `alguns` em vez das redes, e das redes em vez dos anfitriões quando possível.Tente simplificar grupos de objetos. Isto pode potencialmente salvar centenas de ACE quando os ACL são expandidos. Um exemplo é agrupar junto indicações da porta individual em uma escala.
- Re-separação a memória atribuída para o ACE em cada separação. Isto exige a repartição do módulo FWSM.O FWSM divide basicamente a memória atribuída para o ACE em 12 separações, e atribui a memória correspondente para cada um. Isto é feito automaticamente. Da versão 2.3(2) e mais recente, você pode usar o gerenciador de recurso para readjudicar a memória, que depende do número de contextos que você tem.Emita o **comando count do contexto da mostra** a fim verificar quantos contextos você tem. Você pode então verificar este com a configuração. Encontre então o número de separações que usam o comando da ACL-**separação do recurso da mostra**. Se você tem mais separações do que seu contexto definido, a seguir você pode combinar o número de separações ao número de contexto com o comando das número--*separações da ACL*-**separação do recurso**.Você precisa de salvar a configuração e de recarregar o FWSM após este. O comando precedente dá-lhe mais memória para o ACE, se este é bastante ou depende não outra vez do ACE que você adiciona ao contexto.**Cuidado:** Um inconveniente do remapping precedente é que se você quer adicionar um outro contexto, a seguir você tem que readjudicar o mapeamento de memória outra vez. Isto causa menos memória disponível a cada contexto e pode quebrar definições atuais ACE. A memória no FWSM atribuído a é uma quantidade finita e cinzela-a para fora em conformidade em uma maneira predeterminada ou com o alocamento de recursos manual como mencionado previamente.

Da versão 4.0 avante, o FWSM introduziu uma característica chamada a “otimização ACL” que utiliza eficientemente os recursos de memória para entradas ACL do múltiplo de armazenagem. Isto trata um algoritmo incorporado que agregue automaticamente as entradas ACL na medida do possível sem faltar a eficácia de toda a uma entrada ACL. Este algoritmo junta-se junto às sub-redes contíguas referidas em entradas ACL diferentes em uma única indicação, e detecta-se sobreposições nos intervalos de porta. Esta característica é permitida usando um comando e, depois que a otimização é executada, os olhares completos da configuração ACL diferentemente da configuração ACL (original) precedente. Esta configuração ACL em ordem poderia ser retida após a verificação e a otimização poderia ser desabilitada para salvar o sobrecarregamento computacional CPU. Para obter mais informações sobre desta característica, refira a seção da otimização do grupo da lista de acessos que descreve a funcionalidade da otimização ACL junto com seus detalhes de configuração.

A versão 4.0 igualmente introduziu uma outra característica chamada de “capacidade da lista de acessos Increasaed”. Com esta característica, os usuários têm agora a capacidade armazenar 130,000 entradas ACL no modo do único-contexto e nas 150,000 entradas no modo do multicontext. Para obter mais informações sobre desta característica, refira “a seção da capacidade aumentada da lista de acessos” no boletim da versão 4.0 do software do módulo dos serviços de firewall de Cisco.

Q. Por que faz o comando capture quando aplicado às paradas FWSM e não

captura o tráfego assim que um outro comando capture for aplicado na relação?

A. Quando você configurar a captação “z” na mesma relação onde a captação “x” dos supercedes da captação “z” da captação “x” é já aplicado, a seguir. A captação ativa é última anexada à interface particular.

A única exceção é quando a lista de acesso na captação “x” sobrepõe com a lista de acesso da captação “z”. Se aquele é o caso, a seguir ambas as captações continuam a capturar o tráfego onde as listas de acesso sobrepõem.

Q. Como posso eu resolver o erro do `frame timeout do registador NP-PCcmplx no` FWSM?

A. Recarregue o módulo FWSM a fim resolver este erro.

Q. Como posso eu configurar o FWSM para usar o TCP Intercept para defender contra determinados tipos de inundações de SYN?

A. Você pode configurar o FWSM para usar o TCP Intercept para defender contra determinados tipos de inundações de SYN. Refira os Cookie FWSM TCP Intercept e SYN explicados para mais informação.

Q. Haveria algum problema de desempenho para processar pacotes do IPv6?

A. Sim. Você pode ver problemas de desempenho ao enviar o tráfego do IPv6, como o pacote precisa de ser processado pelo CPU. Devido às diferenças em segurar o tráfego do IPv4 e o tráfego do IPv6 pelo CPU, o processamento do pacote do IPv6 causará determinados problemas de desempenho com o FWSM.

Q. Como posso eu impedir que o FWSM responda a um server distante com seu próprio MAC address?

A. Você precisa de desabilitar a característica do proxy ARP na interface especificada com este comando:

```
"sysopt noproxyarp <interface>"
```

Para obter mais informações sobre da característica do proxy ARP, refira o guia de referência de comando FWSM.

Q. Como posso eu impedir os atendimentos com o FWSM de ser deixado cair?

A. A fim resolver este problema, inspeção do desabilitação para H323 e H225:

```
policy-map global_policy
class inspection_default
no inspect h323 h225
no inspect h323 ras
```

Q. Como posso eu resolver edições da tradução NAT no FWSM?

A. A fim resolver este problema, use o comando do xlate-**desvio**. À revelia, o FWSM cria sessões

NAT para todas as conexões mesmo se você não usa o NAT. Você pode desabilitar sessões NAT para o tráfego untranslated, que é chamado desvio do xlate, a fim evitar o limite máximo da sessão NAT. O comando do xlate-**desvio** pode ser configurado como mostrado:

```
hostname(config)#xlate-bypass
```

Refira configurar o desvio do xlate para obter mais informações sobre de como à configuração do xlate-desvio.

Informações Relacionadas

- Exemplo da configuração básica FWSM
- Documentação de módulo dos serviços de firewall
- Página de suporte do produto do módulo de serviços de firewall
- Suporte Técnico e Documentação - Cisco Systems