Exemplo transparente da configuração de firewall do módulo firewall service

Índice

Introdução

Tradicionalmente, um firewall é um salto na rota e funciona como um gateway padrão para os hosts que se conectam a uma de suas sub-redes selecionadas. Um Firewall transparente, por outro lado, é um Firewall da camada 2 que os atos como um *Bump In The Wire* ou um *firewall furtivo* e não sejam considerados como um salto do roteador aos dispositivos conectados. O módulo firewall service (FWSM) conecta a mesma rede em suas interfaces internas e externas. Porque o Firewall não é um salto roteado, você pode facilmente introduzir um Firewall transparente em uma rede existente. Especificar um novo endereço IP é desnecessário.

A manutenção é facilitada porque não há nenhum teste padrão complicado do roteamento a pesquisar defeitos e nenhuma configuração de NAT.

Mesmo que o modo transparente atue como uma ponte, mergulhe 3 que o tráfego (tal como o tráfego IP) não pode passar com o FWSM a menos que você o permitir explicitamente com uma lista de acesso extendida. O único tráfego permitido com o Firewall transparente sem uma lista de acessos é tráfego ARP. O tráfego ARP pode ser controlado pela inspeção ARP.

No modo roteado, alguns tipos de tráfego não podem passar com o FWSM mesmo se você o permite em uma lista de acessos. Alternativamente, o Firewall transparente pode permitir todo o tráfego completamente com uma lista de acesso extendida (para o tráfego IP) ou uma lista de acessos de Ethertype (para o tráfego não-IP).

Por exemplo, você pode estabelecer adjacências do protocolo de roteamento com um Firewall transparente. Você pode permitir o tráfego VPN (IPsec), OSPF, de RASGO, EIGRP, ou BGP baseado completamente em uma lista de acesso extendida. Igualmente, os protocolos tais como o HSRP ou o VRRP podem passar com o FWSM.

O tráfego não-IP (por exemplo, APPLETALK, IPX, BPDU, e MPLS) pode ser configurado para ir completamente com uma lista de acessos de Ethertype.

Para as características que não são apoiadas diretamente no Firewall transparente, você pode permitir que o tráfego passe completamente de modo que o Roteadores do fluxo acima e fluxo abaixo possa apoiar a funcionalidade. Por exemplo, com uma lista de acesso extendida, você pode permitir o tráfego DHCP (em vez dos recursos de Frame Relay DHCP unsupported) ou o tráfego multicast, tal como isso criado pelo IP/TV.

Quando o FWSM é executado no modo transparente, a interface externa de um pacote está determinada por uma consulta do MAC address em vez de uma consulta da rota. As declarações de rota podem ainda ser configuradas, mas aplicam-se somente ao tráfego FWSM-originado. Por exemplo, se seu servidor de SYSLOG é ficado situado em uma rede remota, você deve usar uma rota estática, assim que o FWSM pode alcançar essa sub-rede.

Uma exceção a esta regra é quando você usa inspeçãos da Voz e o valor-limite é pelo menos um salto longe do FWSM. Por exemplo, se você usa o Firewall transparente entre um CCM e um gateway de H.323, e há um roteador entre o Firewall transparente e o gateway de H.323, a seguir você precisa de adicionar uma rota estática no FWSM para o gateway de H.323 para a conclusão da chamada bem sucedida.

Nota: O modo transparente FWSM não passa os pacotes de CDP ou o nenhuns pacotes que não têm Ethertype superior ou igual a um 0x600 válidos. Por exemplo, você não pode passar pacotes IS-IS. Uma exceção é feita para os BPDU, que são apoiados.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada no FWSM com versão 3.x.

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.

Convenções

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

Firewall transparente

Grupos de bridge

Se você não quer as despesas gerais dos contextos de segurança, ou queira maximizar seu uso dos contextos de segurança, você pode configurar até oito pares de relações, chamados grupos de bridge. Cada grupo de bridge conecta a uma rede separada. O tráfego do grupo de bridge é isolado de outros grupos de bridge. O tráfego não é distribuído a um outro grupo de bridge dentro do FWSM, e o tráfego deve retirar o FWSM antes que esteja distribuído por um roteador externo de volta a um outro grupo de bridge no FWSM. Embora as funções de Bridging sejam separadas para cada grupo de bridge, muitas outras funções são compartilhadas entre todos os grupos de bridge. Por exemplo, todos os grupos de bridge compartilham de um server ou de uma configuração do servidor AAA do log de sistema. Para a separação completa da política de segurança, use contextos de segurança com um grupo de bridge em cada contexto.

Porque o Firewall não é um salto roteado, você pode facilmente introduzir um Firewall transparente em uma rede existente. Especificar um novo endereço IP é desnecessário. A manutenção é facilitada porque não há nenhum teste padrão complicado do roteamento a pesquisar defeitos e nenhuma configuração de NAT.

Nota: Cada grupo de bridge exige um endereço IP de gerenciamento. O FWSM usa este endereço IP de Um ou Mais Servidores Cisco ICM NT como o endereço de origem para os pacotes que originam do grupo de bridge. O endereço IP de gerenciamento deve estar na mesma sub-rede como a rede conectada.

Diretrizes

Siga estas diretrizes quando você planeia seu firewall network transparente:

- Um endereço IP de gerenciamento é exigido para cada grupo de bridge.Ao contrário do modo roteado, que exige um endereço IP de Um ou Mais Servidores Cisco ICM NT para cada relação, um Firewall transparente tem um endereço IP de Um ou Mais Servidores Cisco ICM NT atribuído ao grupo de bridge inteiro. O FWSM usa este endereço IP de Um ou Mais Servidores Cisco ICM NT como o endereço de origem para os pacotes que originam no FWSM, tal como mensagens de sistema ou comunicações AAA.O endereço IP de gerenciamento deve estar na mesma sub-rede como a rede conectada. Você não pode ajustar a sub-rede a uma sub-rede do host (255.255.255.255). O FWSM não apoia o tráfego em redes secundárias; somente o tráfego na mesma rede que o endereço IP de gerenciamento é apoiado. Refira a atribuição de um endereço IP de Um ou Mais Servidores Cisco ICM NT a um grupo de bridge para obter mais informações sobre das sub-redes do IP

de gerenciamento.
- Cada grupo de bridge usa uma interface interna e uma interface externa somente.
- Cada um diretamente rede conectada deve estar na mesma sub-rede.
- Não especifique o endereço IP de gerenciamento do grupo de bridge como o gateway padrão para dispositivos conectados. Os dispositivos precisam de especificar o roteador no outro lado do FWSM como o gateway padrão.
- A rota padrão para o Firewall transparente, que é exigido para fornecer um caminho de retorno para o tráfego de gerenciamento, é aplicada somente ao tráfego de gerenciamento de uma rede do grupo de bridge. Isto é porque a rota padrão especifica uma relação no grupo de bridge assim como no endereço IP de roteador na rede do grupo de bridge, e você pode somente definir uma rota padrão. Se você tem o tráfego de gerenciamento de mais de uma rede do grupo de bridge, você precisa de especificar uma rota estática que identifique a rede de que você espera o tráfego de gerenciamento.
- Para o modo de contexto múltiplo, cada contexto deve usar relações diferentes. Você não pode compartilhar de uma relação através dos contextos.
- Para o modo de contexto múltiplo, cada contexto usa tipicamente sub-redes diferentes. Você pode usar sub-redes de sobreposição, mas sua topologia de rede exige o roteador e a configuração de NAT torná-la possível de um ponto de vista do roteamento.Você deve usar uma lista de acesso extendida para permitir o tráfego da camada 3, tal como o tráfego IP, com o FWSM. Você pode igualmente opcionalmente usar uma lista de acessos de Ethertype para permitir completamente o tráfego não-IP.

Endereços permitidos MAC

Estes endereços MAC de destino são permitidos com o Firewall transparente. Todo o MAC address não nesta lista é deixado cair.

- RETIFIQUE o endereço MAC de destino da transmissão igual ao FFFF.FFFF.FFFF
- Endereços MAC de transmissão múltipla do IPv4 de 0100.5E00.0000 a 0100.5EFE.FFFF
- Endereços do Multicast IPv6 MAC de 3333.0000.0000 a 3333.FFFF.FFFF
- Endereço de multicast BPDU igual a 0100.0CCC.CCCD
- Endereços MAC de transmissão múltipla do APPLETALK de 0900.0700.0000 a 0900.07FF.FFFF

Recursos não suportados

Estas características não são apoiadas no modo transparente:

- NAT /PATO NAT é executado no roteador fluxo acima.**Nota:** O NAT/PAT é apoiado no Firewall transparente para a versão de FWSM 3.2 e umas liberações mais atrasadas.
- Protocolos de roteamento dinâmico (tais como o RASGO, EIGRP, OSPF)Você pode adicionar rotas estáticas para o tráfego que origina no FWSM. Você pode igualmente permitir protocolos de roteamento dinâmico com o FWSM com uma lista de acesso extendida.
- IPv6 para o endereço IP de Um ou Mais Servidores Cisco ICM NT do grupo de bridge.Contudo, você pode passar o IPv6 Ethertype usando uma lista de acessos de Ethertype.
- Transmissão de DHCPO Firewall transparente pode atuar como um servidor DHCP, mas não apoia os comandos da transmissão de DHCP. A transmissão de DHCP não é exigida porque

você pode permitir que o tráfego DHCP passe completamente com uma lista de acesso extendida.
- Quality of Service (QoS)
- Transmissão múltiplaVocê pode permitir o tráfego multicast com o FWSM se você o permite em uma lista de acesso extendida. Refira a passagem através da seção do tráfego para mais informação.
- Terminação VPN para o tráfego diretoO Firewall transparente apoia túneis do VPN de Site-para-Site para conexões de gerenciamento somente. Não termina conexões de VPN para o tráfego com o FWSM. Você pode passar o tráfego VPN com o FWSM com uma lista de acesso extendida, mas não termina conexões do NON-Gerenciamento.
- LoopGuard no interruptorNão permita LoopGuard globalmente no interruptor se o FWSM reage do modo transparente. LoopGuard é aplicado automaticamente ao EtherChannel interno entre o interruptor e o FWSM, assim que após um Failover e um failback, LoopGuard faz com que a unidade secundária seja desligada porque o EtherChannel entra no estado errdisable.

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

O diagrama da rede mostra a um firewall network transparente típico onde os dispositivos exteriores estão na mesma sub-rede como os dispositivos internos. O roteador interno e os anfitriões parecem ser conectados diretamente ao roteador exterior.

Configurações

Você pode ajustar cada contexto para ser executado no modo de firewall roteado (o padrão) ou no modo de firewall transparente.

Quando você muda modos, o FWSM cancela a configuração porque muitos comandos não são apoiados para ambos os modos. Se você já tem uma configuração povoada, seja certo suportar sua configuração antes que você mude o modo. Você pode usar este backup para a referência ao criar sua configuração nova.

Se você transfere uma configuração de texto ao FWSM que muda o modo com o comando transparent do Firewall, seja certo pôr o comando na parte superior da configuração. O FWSM muda o modo assim que ler o comando e continuar então a ler a configuração que você transferiu. Se o comando está mais atrasado na configuração, o FWSM cancela todas as linhas precedentes na configuração.

A fim ajustar o modo a transparente, incorpore este comando a cada contexto:

```
hostname(config)#firewall transparent
```

A fim ajustar o modo a roteado, incorpore este comando a cada contexto:

```
hostname(config)#no firewall transparent
```

Os dados movem-se através do Firewall transparente em encenações diferentes

Acessos de usuário internos o servidor de e-mail exterior

O usuário nos acessos que de rede interna o servidor de e-mail colocou no Internet (fora). O FWSM recebe o pacote e adiciona o endereço MAC de origem à tabela de endereços MAC, se for necessário. Porque é uma sessão nova, verifica que o pacote está permitido de acordo com os termos da política de segurança (Listas de acesso, filtros, ou AAA).

Nota: Para o modo de contexto múltiplo, o FWSM classifica primeiramente o pacote de acordo com uma relação original.

O FWSM grava que uma sessão está estabelecida. Se o endereço MAC de destino está em sua tabela, o FWSM para a frente o pacote fora da interface externa. O endereço MAC de destino é aquele do roteador fluxo acima, 192.168.1.2. Se o endereço MAC de destino não está na tabela FWSM, o FWSM tenta descobrir o MAC address quando envia uma requisição ARP e um sibilo. O primeiro pacote é deixado cair.

O servidor de e-mail responde ao pedido. Porque a sessão é estabelecida já, o pacote contorneia muitas consultas associadas com uma nova conexão. O FWSM encaminha o pacote ao usuário interno.

Um usuário interno visita um servidor de e-mail com NAT

Se você permite o NAT no roteador de Internet, o fluxo do pacote através do roteador de Internet está mudado levemente.

O usuário nos acessos que de rede interna o servidor de e-mail colocou no Internet (fora). O FWSM recebe o pacote e adiciona o endereço MAC de origem à tabela de endereços MAC, se for necessário. Porque é uma sessão nova, verifica que o pacote está permitido de acordo com os termos da política de segurança (Listas de acesso, filtros, ou AAA).

Nota: Para o modo de contexto múltiplo, o FWSM classifica primeiramente o pacote de acordo com uma relação original.

O roteador de Internet traduz o endereço real do host A (192.168.1.5) ao endereço traçado do roteador de Internet (172.16.1.1). Porque o endereço traçado não está na mesma rede que a interface externa, certifique-se de que o roteador fluxo acima tem uma rota estática à rede traçada esses pontos ao FWSM.

O FWSM grava que uma sessão está estabelecida e para a frente o pacote da interface externa. Se o endereço MAC de destino está em sua tabela, o FWSM para a frente o pacote fora da interface externa. O endereço MAC de destino é aquele do roteador fluxo acima, 172.16.1.1. Se o endereço MAC de destino não está na tabela FWSM, o FWSM tenta descobrir o MAC address quando envia uma requisição ARP e um sibilo. O primeiro pacote é deixado cair.

O servidor de e-mail responde ao pedido. Porque a sessão é estabelecida já, o pacote contorneia

muitas consultas associadas com uma nova conexão. O FWSM executa o NAT quando traduz o endereço traçado ao endereço real, 192.168.1.5.

Um usuário interno visita um servidor de Web interno

Se o host A tenta alcançar o servidor de Web interno (10.1.1.1), hospede A (192.168.1.5) envia o pacote de requisição ao roteador de Internet (desde que é um gateway padrão) com o FWSM do interior à parte externa. O pacote é reorientado então ao servidor de Web (10.1.1.1) através do FWSM (fora ao interior) e do roteador interno.

Nota: O pacote de requisição retorna ao servidor de Web somente se o FWSM tem uma lista de acessos para permitir o tráfego da parte externa ao interior.

A fim resolver esta edição, mude o gateway padrão para o host A (10.1.1.1) para ser o roteador interno (192.168.1.3) em vez do roteador de Internet (192.168.1.2). Isto evita todo o tráfego desnecessário enviado ao gateway exterior e reorienta ocorrências no roteador exterior (roteador de Internet). Igualmente resolve na maneira reversa, isto é, quando o servidor de Web ou algum hospedam o presente (de 10.1.1.0/24) no interior das tentativas do roteador interno para alcançar o host A (192.168.1.5).

Um usuário externo visita um servidor de Web na rede interna

Estas etapas descrevem como os dados se movem com o FWSM:

1. Um usuário na rede externa pede um página da web do servidor de Web interno. O FWSM recebe o pacote e adiciona o endereço MAC de origem à tabela de endereços MAC, se for necessário. Porque é uma sessão nova, verifica que o pacote está permitido de acordo com os termos da política de segurança (Listas de acesso, filtros, ou AAA).**Nota:** Para o modo de contexto múltiplo, o FWSM classifica primeiramente o pacote de acordo com uma relação original.
2. O FWSM grava que uma sessão está estabelecida somente se o usuário externo tem o acesso válido ao servidor de Web interno. A lista de acessos deve ser configurada para permitir que o usuário externo obtenha o acesso para o servidor de Web.
3. Se o endereço MAC de destino está em sua tabela, o FWSM para a frente o pacote fora da interface interna. O endereço MAC de destino é aquele do roteador downstream, 192.168.1.3.
4. Se o endereço MAC de destino não está na tabela FWSM, o FWSM tenta descobrir o MAC address quando envia uma requisição ARP e um sibilo. O primeiro pacote é deixado cair.
5. O servidor de Web responde ao pedido. Porque a sessão é estabelecida já, o pacote contorneia muitas consultas associadas com uma nova conexão. O FWSM para a frente o pacote ao usuário externo.

Um usuário externo tenta alcançar um host interno

Um usuário na rede externa tenta alcançar um host interno. O FWSM recebe o pacote e adiciona o endereço MAC de origem à tabela de endereços MAC, se for necessário. Porque é uma sessão nova, verifica se o pacote está permitido de acordo com os termos da política de segurança (Listas de acesso, filtros, ou AAA).

Nota: Para o modo de contexto múltiplo, o FWSM classifica primeiramente o pacote de acordo

com uma relação original.

O pacote é negado, e o FWSM deixa cair o pacote porque o usuário externo não tem o acesso ao host interno. Se o usuário externo tenta atacar a rede interna, o FWSM emprega muitas Tecnologias para determinar se um pacote é válido para já uma sessão estabelecida.

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 a OIT para exibir uma análise da saída do comando show.

```
cisco(config)#show firewall Firewall mode: Transparent
```

Troubleshooting

Passe com o tráfego

No Firewall transparente, para passar o tráfego multicast da elevação a baixo e a baixo às listas de acesso altas são exigidos. Em Firewall normais da elevação ao ponto baixo não é exigido.

Nota: O endereço de multicast (224.0.0.9) pode nunca ser endereço de origem para o tráfego de retorno, assim que ele não será reservado voltar dentro, é por isso nós precisamos ACL de dentro a para fora e para fora a dentro.

Por exemplo, a fim passar com o tráfego do rasgo, a lista de acessos transparente do Firewall seria similar a este exemplo:

RIP

ACL exterior (de para fora a dentro):

```
access-list outside permit udp host (outside source router) host 224.0.0.9 eq 520
access-group outside in interface outside
```

ACL interno (do interior à parte externa):

```
access-list inside permit udp host (inside source router) host 224.0.0.9 eq 520
access-group inside in interface inside
```

EIGRP a ser executado:

```
access-list inside permit eigrp host (inside source) host 224.0.0.10
 access-group inside in interface inside
access-list outside permit eigrp host (outside source) host 224.0.0.10
access-group outside in interface outside
```

Para OSPF:

```
access-list inside permit ospf host ( inside source ) host 224.0.0.5
( this access-list is for hello packets )
access-list inside permit ospf host ( inside source ) host 224.0.0.6
( dr send update on this port )
access-list inside permit ospf host ( inside source ) host ( outside source )
access-group inside in interface inside
```

```
 access-list outside permit ospf host ( outside source ) host 224.0.0.5
access-list outside permit ospf host ( outside source ) host 224.0.0.6
access-list outside permit ospf host ( outside sourec ) host ( inside source )
access-group outside in interafce outside
```

MSFC VLAN contra FWSM VLAN

No modo transparente, não é necessário ter os mesmos VLAN na relação MSFC e no FWSM, desde que é um tipo de construção de uma ponte sobre.

Informações Relacionadas

- Cisco PIX Firewall Software
- Solicitações de Comentários (RFCs)
- Avisos de campo de produto de segurança (incluindo PIX)
- Referências do comando Cisco Secure PIX Firewall
- PIX/ASA: Exemplo transparente da configuração de firewall
- Suporte Técnico e Documentação - Cisco Systems