FWSM: Pesquise defeitos o tráfego falhas devido para lesar xlates

Índice

Introdução

Devido ao projeto do processamento de pacotes do Firewall Services Module (FWSM), os xlates compilados por pacotes incorretamente roteados podem causar falhas de tráfego em conexões através do firewall. A fim selecionar uma interface de saída para um pacote de entrada, as primeiras verificações FWSM para ver se o IP de destino do pacote de entrada combina qualquer IP/Network global existente em uma tradução NAT (xlate) para essa relação em sua tabela do xlate. Se um fósforo é encontrado, a interface de saída está escolhida simplesmente baseada na interface local na entrada do xlate e o Firewall não consulta a tabela de roteamento para fazer a decisão da interface de saída.

O comportamento padrão do FWSM é construir uma entrada do xlate para o IP da fonte de todo o pacote permitido que for recebido em uma de suas relações. Se um pacote está distribuído através da rede incorretamente (para algum número de razões) e chega de entrada na interface errada do FWSM, um xlate está construído para refletir este. Quando isto ocorre, as entradas na tabela do xlate podem cancelar entradas na tabela de roteamento e causar falhas do tráfego para os destinos afetados.

Este documento descreve os sintomas e os disparadores para esta edição, como diagnosticá-la, e fornece soluções impedindo que ocorra.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento dos FWSM.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

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

Sintomas

Topologia lógica

Configuração relevante

```
interface Vlan1
 nameif outside
 security-level 0
 ip address 192.168.100.50 255.255.255.0
!
interface Vlan10
 nameif inside
 security-level 100
 ip address 10.10.1.50 255.255.255.0
!
interface Vlan20
 nameif dmz
 security-level 50
 ip address 10.20.1.50 255.255.255.0
!
same-security-traffic permit intra-interface
access-list outside_in extended permit tcp any host 10.30.1.1 eq www
access-list inside_in extended permit ip any any
access-group inside_in in interface inside
access-group outside_in in interface outside
route outside 0.0.0.0 0.0.0.0 192.168.100.254
route dmz 10.30.1.0 255.255.255.0 10.20.1.254
```

Comportamentos observados

As conexões do PC cliente em 172.16.1.10 ao servidor de Web em 10.30.1.1 falham.

Uma captura de pacote de informação na **interface externa** mostra um TCP SYN do PC cliente que chega na relação do FWSM.

```
FWSM# show capture outside
3 packets seen, 3 packets captured
   1: 13:58:09.280752960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
```

```
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   2: 13:58:12.280755950 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
   3: 13:58:18.280761960 802.1Q vlan#1 P0 172.16.1.10.57389 > 10.30.1.1.80: S
      918518428:918518428(0) win 8192 <mss 1380,nop,nop,sackOK>
3 packets shown
```

Uma captura de pacote de informação na relação do **dmz** não mostra esse pacote que sae do Firewall.

```
FWSM# show capture dmz
0 packet seen, 0 packet captured
0 packet shown
```

Nenhuma entrada é construída na tabela de conexão do FWSM e os Syslog não mostram relativo à informação ao cliente ou aos endereços IP do servidor.

Disparadores

A nível fundamental, esta edição é causada por uma entrada na tabela do xlate do FWSM que foi construída incorretamente por um pacote roteado. Devido à maneira que o processamento do pacote do FWSM é projetado, o Firewall verifica a tabela do xlate antes que verifique a tabela de roteamento para determinar a interface de saída. Em consequência, se um pacote combina um xlate existente a interface de saída será selecionada com base nessa entrada, mesmo se a entrada opõe ao o que é alistado na tabela de roteamento. Ou seja a tabela do xlate toma a precedência sobre a tabela de roteamento.

A fim diagnosticar esta edição, verifique a saída do **comando debug do xlate da mostra**:

```
FWSM# show xlate debug
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
3 in use, 3 most used
NAT from inside:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:00 timeout 3:00:00 connections
0
NAT from inside:10.30.1.1 to inside:10.30.1.1 flags Ii idle 0:00:07 timeout 3:00:00 connections
0

NAT from dmz:10.30.1.1 to outside:10.30.1.1 flags Ii idle 0:00:10 timeout 3:00:00 connections 0
```

Nota: A palavra-chave debugar no xlate da mostra é crucial. Sem ela, as entradas do xlate não incluirão os nomes da relação que a entrada está associada com.

A tabela do xlate mostra que há 3 xlates construídos para o servidor de Web. O primeiro xlate é construído entre a **interface interna** e a **interface externa**. O segundo xlate é construído como um xlate hairpinned ou u-girado na **interface interna**. O terceiro xlate é construído entre o **dmz** e a **interface externa**. A bandeira I indica que este é um xlate da identidade e o IP não está sendo traduzido realmente.

A primeira relação alistada na entrada é “a relação real” ou “local” onde o IP é suposto para existir realmente. A segunda relação alistada é a relação traçada” ou “global” “onde o IP está sendo traduzido. Nenhuns destes xlates mostrados estão corretos. Isto é porque o servidor de Web (10.30.1.1) existe realmente atrás da relação do **dmz**. O terceiro xlate está correto para este projeto de rede.

A falha de conexão ocorre devido ao primeiro xlate alistado na tabela. Quando o pacote SYN de TCP do cliente chega na interface externa destinada a 10.30.1.1, o FWSM verifica a tabela do xlate e combina a primeira entrada. Esta entrada indica que o pacote saída na **interface interna**,

que está incorreta, e o pacote blackholed.

Àrevelia, o FWSM construirá automaticamente um xlate da identidade para todo o tráfego que não combinar uma regra explicitamente configurada NAT. Devido a isto, mesmo se um pacote chega erroneamente em uma interface incorreta, um xlate será construído. Especificamente para este caso, os pacotes com origem de 10.30.1.1 chegaram de entrada na **interface interna** em vez da chegada na relação do **dmz** como é esperado.

O primeiro xlate (**interior > fora**) foi construído quando o servidor de Web tentou sibilar um endereço IP de Um ou Mais Servidores Cisco ICM NT inexistente (10.199.199.1). A requisição de eco deixada o servidor de Web destinado a seu gateway padrão (roteador DMZ). O roteador DMZ enviou o pacote para o roteador interno, por sua rota estática:

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

Porque a rede 10.199.199.0/24 não existe realmente em qualquer lugar, o roteador interno segue simplesmente sua rota padrão e envia o pacote à **interface interna do** FWSM:

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

Igualmente, o FWSM igualmente não tem uma rota para a rede de destino. Consequentemente, seleciona a interface externa como a interface de saída e constrói um xlate da identidade do interior de **> parte externa**:

```
S    0.0.0.0 0.0.0.0 [1/0] via 192.168.100.254, outside
```

O segundo xlate (**interior > para dentro**) foi construído quando o servidor de Web tentou alcançar o servidor DNS quando a relação de 10.40.1.254 do roteador interno era temporariamente abaixo de devido a um flap do link. O pedido DNS deixado o servidor de Web destinado a seu gateway padrão (roteador DMZ). O roteador DMZ enviou o pacote para o roteador interno, por sua rota estática:

```
S       10.0.0.0/8 [1/0] via 10.50.1.254
```

Contudo, a relação do roteador interno conectada à rede 10.40.1.0/24 era temporariamente para baixo e sua diretamente rota conectada para esta rede faltava. Consequentemente, a única rota de harmonização na tabela de roteamento era a rota padrão para trás para o FWSM:

```
S*   0.0.0.0/0 [1/0] via 10.20.1.50
```

O pacote foi distribuído à **interface interna do** FWSM. A tabela de roteamento do FWSM indicou que a rede de destino de 10.40.1.0/24 existiu atrás da mesma **interface interna**:

```
S    10.40.1.0 255.255.255.0 [1/0] via 10.10.1.254, inside
```

Porque o **comando intra-interface da licença do same-security-traffic** é permitido, o FWSM permitirá que o xlate u-girado seja construído.

Para resumir, o primeiro xlate foi provocado por:

- Uma rota 10.0.0.0/8 larga configurada no roteador DMZ
- **Uma licença IP algum algum ACL** configurado na interface interna do FWSM

O segundo xlate foi provocado por:

- Uma interface de não-sincronização no roteador interno
- **intra-relação da licença do same-security-traffic** configurada no FWSM

Soluções

Há muitas soluções possíveis diferentes a este problema. Principalmente, suprimir do xlate da tabela deve permitir que o tráfego comece trabalhar outra vez até que o xlate esteja reconstruído. Isto pode ser feito com o **comando clear xlate**. Por exemplo:

```
FWSM# clear xlate interface inside local 10.30.1.1 global 10.30.1.1
```

Nota: Todas as conexões que usarem os xlates suprimidos serão rasgadas igualmente para baixo.

Uma vez que isso está completo, o foco deve estar em impedir que os xlates retornem. Frequentemente épocas, a maioria de maneira preferida fazer isto é fixar a configuração de roteamento no ambiente para impedir que o tráfego chegue na relação errada FWSM. O FWSM igualmente oferece um punhado das opções de configuração endereçar estas edições.

Configurações de roteamento incorretas da resolução

Esta solução toma o planeamento cuidadoso e uma compreensão profunda do ambiente de rede. No primeiro exemplo acima, a rota 10.0.0.0/8 no roteador DMZ está tecnicamente incorreta desde que a rede inteira de /8 não existe além de sua relação de 10.50.1.253. Em lugar de, algumas opções que existem são:

- Elimine 10.50.1.0/24 a rede todos junto e distribua simplesmente todo o tráfego com o FWSM. Isto igualmente fornece a melhores segmentação e Segurança entre o interior e as redes do DMZ.
- Configurar uma rota estática no DMZ para somente 10.40.1.0/24 e remova a rota 10.0.0.0/8.
- Use um protocolo de roteamento dinâmico entre o Roteadores interno e DMZ para anunciar corretamente somente as redes que existem realmente.

Há frequentemente muitas possibilidades para ajustar a configuração de roteamento, mas o objetivo do fim é assegurar-se de que o tráfego de um host dado possa chegar somente em uma única relação FWSM.

Intra-relação da licença do same-security-traffic do desabilitação

O comando intra-interface da licença do same-security-traffic permite o FWSM à inversão de marcha ou ao tráfego do gancho de cabelo em uma relação. Isto significa que um pacote pode entrar no Firewall na mesma relação que sae sobre. Esta funcionalidade é desabilitada à revelia e tem muito pouco uso na maioria de projetos FWSM. Porque o FWSM usa interfaces de VLAN, trafique que as estadas dentro do mesmo VLAN devem nunca ser processadas pelo FWSM.

No segundo exemplo acima, o **comando intra-interface da licença do same-security-traffic** permitiu um pacote a incorpora e deixa a **interface interna**. **A intra-relação de** desabilitação da **licença do same-security-traffic** impediu este comportamento e deixou cair o pacote antes que um xlate esteve construído nunca:

```
FWSM(config)# no same-security-traffic permit intra-interface
```

Deixe cair os pacotes que chegam em uma interface incorreta (ACL ou o uRPF)

Em ambos os exemplos acima, os xlates foram construídos quando um pacote do servidor de Web chegou incorretamente na **interface interna**. A fim impedir junto todo o problema, o FWSM pode ser configurado para deixar cair os pacotes que chegam na interface errada.

O FWSM exige que todo o tráfego esteja permitido por um ACL antes que possa passar.

Consequentemente, esta funcionalidade pode ser conseguida somente permitindo o tráfego das redes da fonte apropriadas em cada relação. Nos exemplos acima, a **interface interna** permite todo o tráfego IP:

```
access-list inside_in extended permit ip any any
```

Em lugar de, isto deve ser mudado para permitir somente o tráfego das 10.10.1.0/24 e 10.40.1.0/24 sub-redes:

```
access-list inside_in extended permit ip 10.10.1.0 255.255.255.0 any

access-list inside_in extended permit ip 10.40.1.0 255.255.255.0 any
```

Em alguns ambientes, esta não é uma opção fatível devido ao tamanho e/ou à escala das redes diferentes que passam com o FWSM. Contudo, esta funcionalidade pode ser conseguida mais simplesmente usando uma característica chamada Unicast Reverse Path Forwarding (uRPF).

Quando a característica do uRPF é permitida, o FWSM comparará o endereço IP de origem do primeiro pacote de cada conexão contra sua tabela de roteamento. Se a rota que está encontrada não combina acima com a relação que o pacote chegou sobre, esse pacote será deixado cair devido a uma falha de RPF.

No exemplo acima, o FWSM tem uma rota estática que use a relação do **dmz** para alcançar a rede 10.30.1.0/24. Consequentemente, se o uRPF é permitido na **interface interna**, os pacotes com origem do servidor de Web (10.30.1.1) que chega incorretamente na **interface interna** serão deixados cair.

A fim permitir o uRPF, aplique o **IP verificam o** comando do **caminho reverso a** cada relação na pergunta. Por exemplo:

```
FWSM(config)# ip verify reverse-path interface inside
```

Permita o xlate-desvio

Em ambos os exemplos acima, os xlates são criados com as bandeiras Ii. Estas bandeiras indicam que o xlate é uma tradução da identidade (i) que origine em uma relação da segurança elevada (i). À revelia, o FWSM construirá estes xlates para todo o tráfego que não combinar uma regra explícita NAT/PAT. A fim desabilitar este comportamento, o comando do xlate-**desvio** pode ser permitido em FWSM 3.2(1) e mais atrasado:

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

Esta característica impedirá o FWSM dos xlates da identidade da construção no primeiro lugar. Assim, o tráfego nos exemplos acima não seria reorientado a uma interface incorreta devido a uma entrada de tabela do xlate. Contudo, o tráfego ainda passará com o FWSM untranslated.

Resumo

A fim determinar a interface de saída para um pacote, o FWSM consultará sempre sua tabela do xlate antes de olhar sua tabela de roteamento. Se esse pacote combina um xlate existente, a interface de saída está selecionada com base na relação associada do xlate. Isto acontece apesar de todas as contradições que possam ser encontradas na tabela de roteamento. Desta maneira, a tabela do xlate toma a precedência sobre a tabela de roteamento.

Porque o FWSM construirá sempre uma entrada do xlate para todas as novas conexões à revelia, este pode causar falhas do tráfego nos casos onde incorretamente os pacotes roteado fazem com

que o FWSM construa um xlate. Como esboçado acima, há muitos cenários possíveis onde este pode ocorrer mas todos se relacionam de volta a um pacote que está sendo recebido em uma interface incorreta. Este documento cobriu estes possíveis problemas:

- Uma configuração larga do roteamento envia pacotes em uma direção incorreta
- O FWSM é configurado para permitir o tráfego das redes da fonte incorretas
- O FWSM é configurado ao tráfego hairpin/u-turn

A fim restaurar rapidamente a Conectividade para as conexões que falham devido a um xlate errado, suprima da entrada com o **comando clear xlate**. Este documento igualmente cobriu as soluções múltiplas para impedir que estes xlates retornem no futuro, incluindo:

- Configurações de roteamento incorretas da resolução usando rotas mais específicas
- Intra-relação da licença do same-security-traffic do desabilitação
- Pacotes da gota que chegam em uma interface incorreta usando ACL ou uRPF
- Permita o xlate-desvio

Informações Relacionadas

- Referência de comandos: o IP verifica o caminho reverso
- Referência de comandos: xlate-desvio
- Suporte Técnico e Documentação - Cisco Systems