O tráfego UDP através do ASA falha depois que o link principal do ISP volta on-line em uma configuração de ISP duplo

Contents

Introduction

Se um ASA (Adaptive Security Appliance) tiver duas interfaces de saída por sub-rede de destino e a rota preferencial para um destino for removida da tabela de roteamento por algum tempo, as conexões UDP (User Datagram Protocol) poderão falhar quando a rota preferencial for adicionada novamente à tabela de roteamento. As conexões TCP também podem ser afetadas pelo problema, mas como o TCP detecta a perda de pacotes, essas conexões são automaticamente interrompidas pelos endpoints e recriadas usando-se as rotas mais ótimas após a alteração das rotas.

Esse problema também pode ser visto se um protocolo de roteamento for usado e uma alteração de topologia disparar uma alteração na tabela de roteamento no ASA.

Antes de Começar

Requirements

Para encontrar esse problema, a tabela de roteamento do ASA deve ser alterada. Isso é comum em links ISP duplos de forma redundante ou quando o ASA está aprendendo rotas através de um IGP (OSPF, EIGRP, RIP).

Esse problema ocorre quando o link principal do ISP volta on-line ou o IGP em questão vê uma reconvergência devido à qual uma rota menos preferencial que estava sendo usada pelo ASA é substituída pela rota mais baixa preferida. Em seguida, você veria conexões de longa duração, como registros SIP UDP, GRE, etc., falhando quando a rota primária ou preferencial fosse reinstalada na tabela de roteamento do ASA.

Componentes Utilizados

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

- Qualquer dispositivo de segurança adaptável Cisco ASA 5500 Series
- ASA versões 8.2(5), 8.3(2)12, 8.4(1)1, 8.5(1) e posterior

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Problema

Se uma entrada da tabela de roteamento for removida da tabela de roteamento do ASA e não houver rotas de uma interface para alcançar um destino, as conexões criadas pelo firewall com esse destino externo serão excluídas pelo ASA. Isso ocorre para que as conexões possam ser criadas novamente usando uma interface diferente com entradas de roteamento para o destino presente.

No entanto, se rotas mais específicas forem adicionadas de volta à tabela, as conexões não serão atualizadas para usar as novas rotas mais específicas e continuarão a usar a interface menos otimizada.

Por exemplo, considere que o firewall tem duas interfaces que enfrentam a Internet - "externa" e "backup" - e essas duas rotas existem na configuração do ASA:

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

Se as interfaces externa e de backup estiverem "ativadas", então as conexões criadas através do firewall usarão a interface externa, pois ela tem a métrica preferencial de 1. Se a interface externa for desligada (ou a função de monitoramento SLA que está rastreando a rota encontrar uma perda de conectividade com o IP rastreado), as conexões usando a interface externa serão desligadas e recriadas usando-se a interface de backup, já que a interface de backup é a única interface com uma rota para o destino.

O problema ocorre quando a interface externa é ativada novamente ou a rota rastreada se torna a rota favorita novamente. A tabela de roteamento é atualizada para preferir a rota original, mas as conexões existentes continuam existindo no ASA e atravessam a interface de backup e NÃO são excluídas e recriadas na interface externa com a métrica mais preferencial. Isso ocorre porque a rota padrão de backup ainda existe na tabela de roteamento específico da interface do ASA. A conexão continua a usar a interface com a rota menos preferencial até que a conexão seja excluída; no caso do UDP, isso pode ser indefinido.

Essa situação pode causar problemas com conexões de longa duração, como registros SIP externos ou outras conexões UDP.

Solução

Para resolver esse problema específico, um novo recurso foi adicionado ao ASA que fará com

que as conexões sejam interrompidas e recriadas em uma nova interface se uma rota mais preferencial para o destino for adicionada à tabela de roteamento. Para ativar o recurso (ele é desabilitado por padrão), defina um tempo limite diferente de zero para o comando **timeout floating-conn**. Esse tempo limite (especificado no formato HH:MM:SS) especifica o tempo que o ASA espera antes de romper a conexão quando uma rota mais preferencial é adicionada à tabela de roteamento:

Este é um exemplo CLI de como ativar o recurso. Com essa CLI, se um pacote for recebido em uma conexão existente para a qual agora há uma rota diferente e mais preferencial para o destino, a conexão será interrompida 1 minuto depois (e reconstruída usando a nova rota mais preferencial):

```
ASA# config terminal
ASA(config)# timeout floating-conn 0:01:00
ASA(config)# end
ASA# show run timeout
timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:01:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout xlate 0:01:00
timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00
ASA#
```

Esse recurso é adicionado à plataforma ASA nas versões 8.2(5), 8.3(2)12, 8.4(1)1 e 8.5(1), incluindo versões posteriores do software ASA.

Se você executar uma versão do código ASA que não implemente esse recurso, uma solução alternativa para o problema seria limpar manualmente as conexões UDP que continuam tomando a rota menos preferencial apesar de uma rota melhor estar disponível por meio de um **clear local-host** *<IP>* ou **clear-conn** *<IP>* .

O comando reference lista esse novo recurso na seção timeout.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems