O tráfego UDP com o ASA falha depois que o link do ISP principal volta Online em uma instalação dupla ISP

Índice

Introdução

Se uma ferramenta de segurança adaptável (ASA) tem duas interfaces de saída pela sub-rede de destino e a rota preferida a um destino é removida da tabela de roteamento por algum tempo, as conexões do User Datagram Protocol (UDP) podem falhar quando a rota preferida obtém adicionar novamente à tabela de roteamento. As conexões de TCP puderam igualmente ser afetadas pelo problema, mas desde que o TCP detecta a perda de pacotes, estas conexões são rasgadas para baixo automaticamente pelos valores-limite, e reconstruído usando mais rotas ótima após as rotas mude.

Este problema pode igualmente ser considerado se um protocolo de roteamento é usado e uma alteração de topologia provoca uma mudança na tabela de roteamento no ASA.

Antes de Começar

Requisitos

A fim encontrar este problema, a tabela de roteamento do ASA deve mudar. Isto é comum com links duplos ISP em uma forma redundante ou quando o ASA aprender rotas através de um IGP (OSPF, EIGRP, RASGO).

Esta edição ocorre quando o link do ISP principal volta em linha ou o IGP dito vê uma reconvergência devido a qual menos rota preferida que era usada pelo ASA está substituída com a baixo-métrica-rota preferida. Você veria então conexões duradouros, tais como registros do SORVO UDP, GRE, etc., falhando uma vez que o preliminar ou a rota preferida são reinstalados na tabela de roteamento do ASA.

Componentes Utilizados

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

- Alguma ferramenta de segurança adaptável do 5500 Series de Cisco ASA
- Versões ASA 8.2(5), 8.3(2)12, 8.4(1)1, 8.5(1) e mais atrasado

Convenções

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

Problema

Se uma entrada de tabela de roteamento está removida da tabela de roteamento do ASA e não há nenhuma rota fora de uma relação para alcançar um destino, as conexões construídas com o Firewall com esse destino estrangeiro estarão suprimidas pelo ASA. Isto ocorre de modo que as conexões possam ser construídas outra vez usando uma relação diferente com as entradas de roteamento para o presente do destino.

Contudo, se umas rotas mais específicas são adicionadas de volta à tabela, as conexões não serão atualizadas para usar as rotas novas, mais específicas, e continuarão a usar a relação menos-ótima.

Por exemplo, considere que o Firewall tem duas relações que enfrentam o Internet - “parte externa” e “backup” - e estas 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 a parte externa e as Interfaces de backup estão “acima de”, a seguir as conexões construíram de partida com o Firewall usarão a interface externa, porque tem a métrica preferida de 1. Se a interface externa é fechada (ou a função de monitoramento SLA que está seguindo a rota encontra uma perda de conectividade ao IP seguido), as conexões que usam a interface externa seriam rasgadas para baixo e reconstruídas usando a Interface de backup, porque a Interface de backup é a única relação com uma rota ao destino.

O problema ocorre quando a interface externa está trazida o apoio ou a rota seguida se transforma a rota favorecida outra vez. A tabela de roteamento é atualizada para preferir a rota original, mas as conexões existentes continuam a existir no ASA e a atravessar a Interface de backup e não são suprimidas e são recreadas na interface externa com a métrica mais-preferida. Isto é porque a rota padrão alternativa ainda existe na tabela de roteamento relação-específica do ASA. A conexão continua a usar a relação com menos rota preferida até que a conexão esteja suprimida; no caso do UDP, isto pôde ser indefinido.

Esta situação pode causar problemas com conexões duradouros, tais como registros externos do SORVO ou outras conexões de UDP.

Solução

A fim endereçar este problema específico, uns novos recursos foram adicionados ao ASA que fará com que as conexões estejam rasgadas para baixo e reconstruídas em uma relação nova se

mais rota preferida ao destino é adicionada à tabela de roteamento. A fim ativar a característica (é desabilitada à revelia), ajuste um intervalo diferente de zero ao comando do **intervalo flutuar-CONN**. Este intervalo (especificado no HH: MILÍMETRO: O SS) especifica o tempo onde o ASA espera antes que rasgue para baixo a conexão mais rota preferida está adicionada uma vez de volta à tabela de roteamento:

Este é um exemplo CLI de permitir a característica. Com este CLI, se um pacote é recebido em uma conexão existente para que há agora um diferente, mais rota preferida ao destino, a conexão será rasgada para baixo 1 minuto mais tarde (e reconstruído usando o novo, mais rota preferida):

```
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#
```

Esta característica é adicionada à plataforma ASA nas versões 8.2(5), 8.3(2)12, 8.4(1)1, e 8.5(1), incluindo umas versões mais atrasadas do software ASA.

Se você executa uma versão do código ASA que não executa esta característica, uma ação alternativa à edição seria nivelar manualmente as conexões de UDP que continuam a tomar menos rota preferida apesar de uma rota melhor que está sendo feita disponível através de um **host local claro** *<IP>* ou claro-**CONN** *<IP>*.

As lista de referência de comandos estes novos recursos sob a seção do intervalo.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems