O ASA tiver o uso da alta utilização da CPU devido a um laço do tráfego quando disconexão dos clientes VPN

Índice

Introdução

Este documento descreve um problema comum que ocorra quando a disconexão dos clientes VPN de uma ferramenta de segurança adaptável de Cisco (ASA) essa é executado como um final do cabeçalho do acesso remoto VPN. Este documento igualmente descreve a situação onde um laço do tráfego ocorre quando disconexão dos usuários VPN de um Firewall ASA. Este documento não cobre como configurar ou estabelecer o Acesso remoto ao VPN, simplesmente a situação específica que elevara de determinadas configurações de roteamento comuns.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do acesso remoto VPN no ASA
- Conceitos de distribuição da camada básica 3

Componentes Utilizados

A informação neste documento é baseada em um modelo 5520 ASA que execute a versão de código ASA 9.1(1).

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.

Produtos Relacionados

Este documento pode ser usado com estes versão de hardware e software:

- Algum modelo ASA
- Alguma versão de código ASA

Informações de Apoio

Quando um usuário conecta ao ASA como um concentrador do acesso remoto VPN, o ASA instala uma rota host-baseada na tabela de roteamento ASA que distribui o tráfego a esse cliente VPN fora da interface externa (para o Internet). Quando as disconexões desse usuário, a rota são removidas da tabela, e os pacotes na rede interna (destinada àquela o usuário desligado VPN) pôde ser dado laços entre o ASA e um dispositivo de roteamento interno.

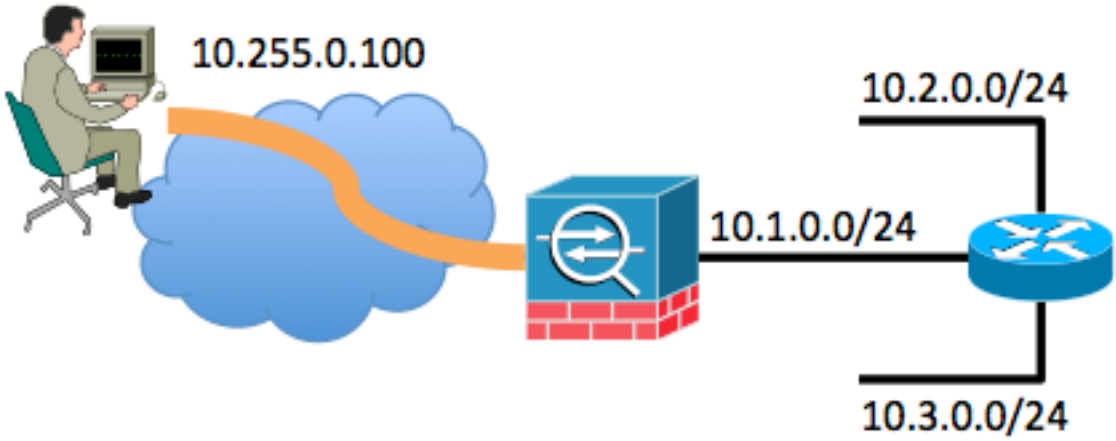
Um outro problema é que os pacotes de transmissão dirigidos (da rede) (gerados pela remoção dos clientes VPN) puderam ser enviados pelo ASA como um frame de unicast para a rede interna. Isto pôde enviá-lo de volta ao ASA, que faz com que o pacote esteja dado laços até que o Time to Live (TTL) expire.

Este documento explica estas edições e mostra que técnicas de configuração podem ser usadas a fim impedir o problema.

Problema: Pacotes destinados para um laço desligado do cliente VPN dentro da rede interna

Quando as disconexões de um usuário do acesso remoto VPN de um Firewall ASA, os pacotes ainda atuais na rede interna (destinada para aqueles usuários desligado) e o endereço do IP atribuído VPN puderam se tornar dados laços dentro da rede interna. Estes loop de pacote puderam fazer com que o USO de CPU no ASA aumente até as paradas de laço ou devido ao valor IP TTL no cabeçalho do pacote IP que decresce a 0, ou o usuário reconecta e o endereço IP de Um ou Mais Servidores Cisco ICM NT é atribuído novamente a um cliente VPN.

A fim compreender melhor esta encenação, considere esta topologia:



Neste exemplo, o cliente de acesso remoto foi atribuído o endereço IP de Um ou Mais Servidores Cisco ICM NT de 10.255.0.100. O ASA neste exemplo é conectado ao mesmo segmento da rede interna junto com um roteador. O roteador tem duas camadas adicionais 3 segmentos de rede conectados a ela. A interface relevante (roteamento) e as configurações de VPN do ASA e do roteador são mostradas nos exemplos.

Os destaques da configuração ASA são mostrados neste exemplo:

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.100 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.1.0.1 255.255.255.0
!
same-security-traffic permit intra-interface
!
ip local pool VPNpool 10.255.0.1-10.255.0.255
!
route outside 0.0.0.0 0.0.0.0 198.51.100.1
route inside 10.0.0.0 255.0.0.0 10.1.0.2
```

Os destaques da configuração de roteador são mostrados neste exemplo:

```
interface FastEthernet0
description connected to the inside interface of the ASA G0/1
ip address 10.1.0.2 255.255.255.0
!
interface FastEthernet1
 description connected to network segment
 ip address 10.2.0.1 255.255.255.0
!
interface FastEthernet2
 description connected to other network segment
 ip address 10.3.0.1 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.0.1
```

A tabela de roteamento do roteador conectado ao interior do ASA tem simplesmente uma rota padrão apontada à interface interna ASA de 10.1.0.1.

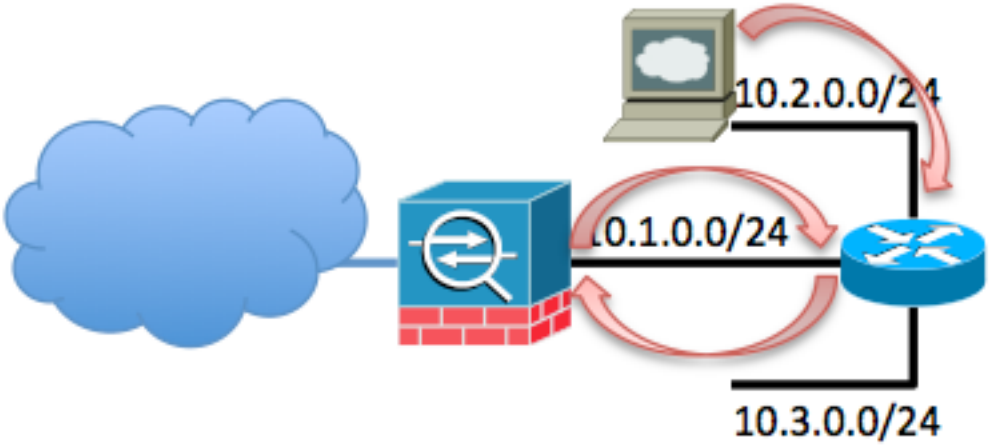
Quando o usuário for conectado através do VPN ao ASA, a tabela de roteamento ASA mostra como segue:

```
ASA# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 198.51.100.1 to network 0.0.0.0
S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

O problema ocorrer quando as disconexões do usuário do acesso remoto VPN do VPN. Neste momento, a rota host-baseada é removida da tabela de roteamento ASA. Se um host dentro da rede tenta enviar o tráfego ao cliente VPN, esse tráfego está distribuído à interface interna ASA pelo roteador. Esta série de etapas ocorre:

1. O pacote destinado a 10.255.0.100 chega na interface interna do ASA.
2. As verificações do padrão ACL são executadas.
3. A tabela de roteamento ASA é verificada a fim determinar a interface de saída para este tráfego.
4. O destino do pacote combina a rota 10.0.0.0/8 larga esses pontos para trás fora da interface interna para o roteador.
5. O ASA verifica se o tráfego do hair pinning é permitido - procura pela intra-**relação da licença da mesmo-Segurança** e encontra que está permitido.
6. Uma conexão é construída a e da interface interna e o pacote é enviado para trás ao roteador como um salto seguinte.
7. O roteador recebe um pacote destinado a 10.255.0.100 na relação que enfrenta o ASA. O roteador verifica sua tabela de roteamento para ver se há um salto seguinte apropriado. O roteador encontra que o salto seguinte seria a interface interna ASA, e o pacote é enviado ao ASA.
8. retornar à etapa 1.

Um exemplo é mostrado aqui:



Este laço ocorre até o TTL de decréscimos deste pacote a 0. Note que o Firewall ASA não decresce o valor TTL à revelia quando processar um pacote. O roteador decresce o TTL enquanto distribui o pacote. Isto impede a ocorrência deste laço indefinidamente, mas este laço aumenta a carga de tráfego no ASA e faz com que o USO de CPU crave.

Problema: Os pacotes de transmissão dirigidos (da rede) gerados por clientes VPN são dados laços em uma rede interna

Esta edição é similar ao primeiro problema. Se um cliente VPN gerencie um pacote da transmissão direcionada a sua sub-rede do IP atribuído (10.255.0.255 no exemplo anterior), a seguir esse pacote pôde ser enviado como um frame de unicast pelo ASA ao roteador interno. O roteador interno pôde então enviá-lo de volta ao ASA, que faz com que o pacote dê laços até que o TTL expire.

Esta série de eventos ocorre:

1. A máquina de cliente VPN gerencie um pacote destinado ao endereço 10.255.0.255 do broadcast de rede, e o pacote chega no ASA.
2. O ASA trata-a este pacote como um frame de unicast (devido à tabela de roteamento) e para a frente ao roteador interno.

3. O roteador interno, que igualmente trata o pacote como um frame de unicast, decresce o TTL do pacote e para a frente do ele de volta ao ASA.

4. As repetições do processo até o TTL do pacote são reduzidas a 0.

Soluções ao problema

Há diversas soluções potencial a esta edição. Segundo a topologia de rede e a situação específica, uma solução pôde ser mais fácil de executar do que outra.

Rota estática da solução 1 para a relação do null0 (versão ASA 9.2.1 e mais atrasados)

Quando você envia o tráfego a uma relação do **null0**, causa os pacotes destinados à rede

especificada a ser deixada cair. Esta característica é útil quando você configura o buraco negro remotamente provocado (RTBH) para o Border Gateway Protocol (BGP). Nesta situação, se você configura uma rota ao null0 para a sub-rede do cliente de acesso remoto, força o ASA para deixar cair o tráfego destinado aos anfitriões nessa sub-rede se uma rota mais específica (fornecida pelo Reverse Route Injection) não está atual.

```
route Null0 10.255.0.0 255.255.255.0
```

Solução 2 - Use um IP pool diferente para clientes VPN

Esta solução é atribuir aos usuários remotos VPN um endereço IP de Um ou Mais Servidores Cisco ICM NT que não sobreponha com nenhuma sub-rede da rede interna. Isto impediria o ASA dos pacotes da transmissão destinados a essa sub-rede VPN de volta ao roteador interno se o usuário VPN não foi conectado.

Solução 3 - Faça a tabela de roteamento ASA mais específica para rotas internas

Esta solução é assegurar-se de que a tabela de roteamento do ASA não tenha nenhuma rotas muito larga que sobrepõem com o IP pool VPN. Para este exemplo de rede específico, remova a rota 10.0.0.0/8 do ASA e configurar umas rotas estáticas mais específicas para as sub-redes que residem fora da interface interna. O dependente em cima do número de sub-redes e da topologia de rede, isto pôde ser um grande número rotas estáticas e não pôde ser possível.

Solução 4 - Adicionar uma rota mais específica para a sub-rede VPN para trás fora da interface externa

Esta solução é mais complicada que a outro que é descrita neste documento. Cisco recomenda que você tenta usar primeiramente as outras soluções devido à situação que é descrita na nota mais tarde nesta seção. Esta solução é impedir o ASA dos pacotes IP da transmissão originado da sub-rede IP VPN de volta ao roteador interno; você pode fazer este se você adiciona uma rota mais específica para a sub-rede VPN fora da interface externa. Desde que esta sub-rede IP é reservada para usuários exteriores VPN, os pacotes com um endereço IP de origem desta sub-rede IP VPN devem nunca chegar de entrada na interface interna ASA. A maneira a mais fácil de conseguir isto é adicionar uma rota para o IP pool do acesso remoto VPN fora da interface externa com um endereço IP de Um ou Mais Servidores Cisco ICM NT do salto seguinte do roteador ISP ascendente.

Neste exemplo da topologia de rede, essa rota olharia como esta:

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

Além do que esta rota, adicionar o **IP verificam o caminho reverso dentro do** comando a fim fazer com que o ASA deixe cair todos os pacotes recebeu de entrada na interface interna originado da sub-rede IP VPN devido a mais rota preferida que existe na interface externa:

```
ip verify reverse-path inside
```

Depois que estes comandos implemeted, a tabela de roteamento ASA olha similar a esta quando o usuário é conectado:

```
ASA# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S 10.255.0.100 255.255.255.255 [1/0] via 198.51.100.1, outside
S 10.0.0.0 255.0.0.0 [1/0] via 10.1.0.2, inside
S 10.255.0.0 255.255.255.0 [1/0] via 198.51.100.1, outside
C 198.51.100.0 255.255.255.0 is directly connected, outside
C 10.1.0.0 255.255.255.0 is directly connected, inside
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Quando o cliente VPN é conectado, a rota host-baseada a esse endereço IP de Um ou Mais Servidores Cisco ICM NT VPN esta presente na tabela e está preferida. Quando as disconexões do cliente VPN, traficam originado desse endereço IP cliente que chega na interface interna é verificado contra a tabela de roteamento e deixados cair devido ao **IP verificam o caminho reverso dentro do** comando.

Se o cliente VPN gerencie um broadcast de rede dirigido à sub-rede IP VPN, a seguir esse pacote está enviado ao roteador interno e enviado pelo roteador de volta ao ASA, onde é deixado cair devido ao **IP verifique o caminho reverso dentro do** comando.

> Nota: Depois que esta solução está executada, se o **comando intra-interface da licença da mesmo-Segurança** esta presente na configuração e as políticas de acesso a permitem, trafique originado de um usuário VPN destinado a um endereço IP de Um ou Mais Servidores Cisco ICM NT no IP pool VPN para um usuário que não seja conectado possa ser distribuído para trás fora da interface externa na minuta. Esta é uma situação rara e pode ser abrandada com o uso dos VPN-filtros dentro da política de VPN. Esta situação ocorre somente se o **comando intra-interface da licença da mesmo-Segurança** esta presente na configuração do ASA.
>
> Igualmente, se os host internos gerenciem o tráfego destinados a um endereço IP de Um ou Mais Servidores Cisco ICM NT no pool VPN e esse endereço IP de Um ou Mais Servidores Cisco ICM NT não está atribuído a um usuário remoto VPN, esse tráfego pôde saída a parte externa do ASA na minuta.