O ASA tem alto uso da CPU devido a um loop de tráfego quando os clientes VPN se desconectam

Contents

Introduction

Este documento descreve um problema comum que ocorre quando os clientes VPN se desconectam de um Cisco Adaptive Security Appliance (ASA) executado como headend de VPN de acesso remoto. Este documento também descreve a situação em que um loop de tráfego ocorre quando os usuários de VPN se desconectam de um firewall ASA. Este documento não aborda como configurar ou configurar o acesso remoto à VPN, somente a situação específica que surge de certas configurações de roteamento comuns.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de VPN de acesso remoto no ASA
- Conceitos básicos de roteamento de Camada 3

Componentes Utilizados

As informações neste documento são baseadas em um ASA Model 5520 que executa o ASA code versão 9.1(1).

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Produtos Relacionados

Este documento pode ser usado com estas versões de hardware e software:

- Qualquer modelo ASA
- Qualquer versão de código ASA

Informações de Apoio

Quando um usuário se conecta ao ASA como um concentrador VPN de acesso remoto, o ASA instala uma rota baseada em host na tabela de roteamento do ASA que roteia o tráfego para esse cliente VPN para fora da interface externa (em direção à Internet). Quando esse usuário se desconecta, a rota é removida da tabela e os pacotes na rede interna (destinados a esse usuário desconectado da VPN) podem estar em loop entre o ASA e um dispositivo de roteamento interno.

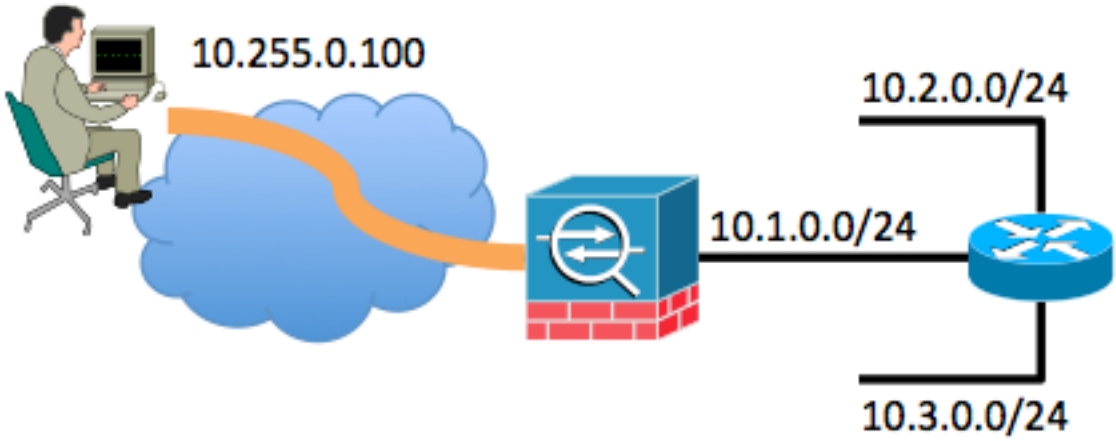
Outro problema é que os pacotes de broadcast direcionados (rede) (gerados pela remoção dos clientes VPN) podem ser encaminhados pelo ASA como um quadro unicast para a rede interna. Isso pode encaminhá-lo de volta ao ASA, que faz com que o pacote seja bloqueado até que o Time to Live (TTL) expire.

Este documento explica esses problemas e mostra quais técnicas de configuração podem ser usadas para evitar o problema.

Problema: Pacotes destinados a um loop de cliente VPN desconectado dentro da rede interna

Quando um usuário de VPN de acesso remoto se desconecta de um firewall ASA, os pacotes ainda estão presentes na rede interna (destinados aos usuários desconectados) e o endereço IP VPN atribuído pode ficar em loop na rede interna. Esses loops de pacote podem fazer com que o uso da CPU no ASA aumente até que o loop pare devido ao valor TTL do IP no cabeçalho do pacote IP decrementando para 0, ou o usuário se reconecta e o endereço IP é atribuído novamente a um cliente VPN.

Para entender melhor esse cenário, considere esta topologia:



Neste exemplo, o cliente de acesso remoto recebeu o endereço IP 10.255.0.100. O ASA neste exemplo está conectado ao mesmo segmento de rede interno junto com um roteador. O roteador tem dois segmentos de rede adicionais de Camada 3 conectados a ele. As configurações relevantes de interface (roteamento) e VPN do ASA e do roteador são mostradas nos exemplos.

Os destaques da configuração do 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 do 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 simplesmente tem uma rota padrão apontada para a interface interna do ASA de 10.1.0.1.

Enquanto o usuário está conectado via VPN ao ASA, a tabela de roteamento do ASA mostra o

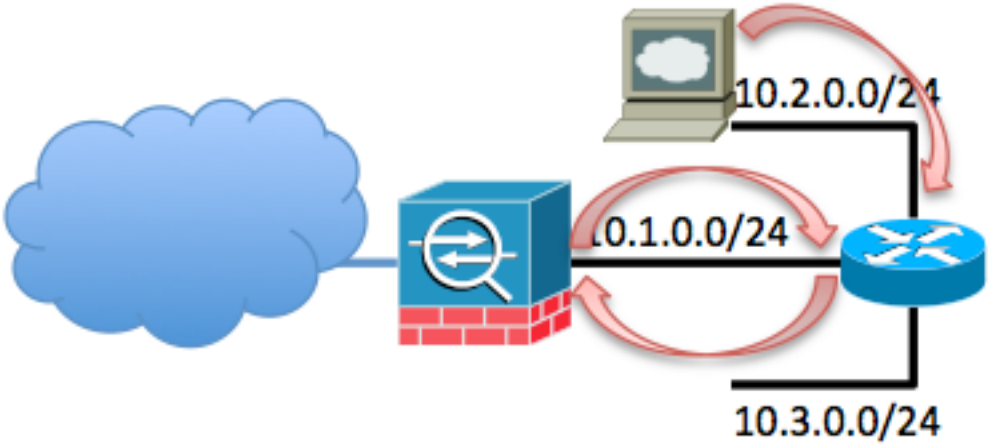
seguinte:

```
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 ocorre quando o usuário VPN de acesso remoto se desconecta da VPN. Neste ponto, a rota baseada em host é removida da tabela de roteamento ASA. Se um host dentro da rede tenta enviar tráfego para o cliente VPN, esse tráfego é roteado para a interface interna do 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 da ACL padrão são realizadas.
3. A tabela de roteamento ASA é verificada para determinar a interface de saída para esse tráfego.
4. O destino do pacote corresponde à rota 10.0.0.0/8 ampla que aponta de volta para fora da interface interna em direção ao roteador.
5. O ASA verifica se o tráfego de pinning é permitido - ele procura por **intrainterface de permissão de segurança igual** e descobre que é permitido.
6. Uma conexão é construída para e da interface interna e o pacote é enviado de volta ao roteador como um próximo salto.
7. O roteador recebe um pacote destinado a 10.255.0.100 na interface que enfrenta o ASA. O roteador verifica sua tabela de roteamento em busca de um próximo salto adequado. O roteador descobre que o próximo salto seria a interface interna do ASA e o pacote é enviado para o ASA.
8. retornar à etapa 1.

Um exemplo é mostrado abaixo:



Esse loop ocorre até que o TTL desse pacote diminua para 0. Observe que o ASA Firewall **não** decrementa o valor TTL por padrão quando processa um pacote. O roteador diminui o TTL à medida que roteia o pacote. Isso evita a ocorrência desse loop indefinidamente, mas esse loop aumenta a carga de tráfego no ASA e faz com que o uso da CPU aumente.

Problema: Pacotes de broadcast direcionados (rede) gerados por clientes VPN são em loop em uma rede interna

Esse problema é semelhante ao primeiro. Se um cliente VPN gera um pacote de broadcast direcionado para sua sub-rede IP atribuída (10.255.0.255 no exemplo anterior), esse pacote pode ser encaminhado como um quadro unicast pelo ASA para o roteador interno. O roteador interno pode, então, encaminhá-lo de volta ao ASA, que faz com que o pacote entre em loop até que o TTL expire.

Esta série de eventos ocorre:

1. A máquina do cliente VPN gera um pacote destinado ao endereço de broadcast da rede 10.255.0.255, e o pacote chega ao ASA.
2. O ASA trata esse pacote como um quadro unicast (devido à tabela de roteamento) e o encaminha para o roteador interno.

3. O roteador interno, que também trata o pacote como um quadro unicast, diminui o TTL do pacote e o encaminha de volta ao ASA.

4. O processo se repete até que o TTL do pacote seja reduzido para 0.

Soluções para o problema

Há várias soluções em potencial para esse problema. Dependendo da topologia da rede e da situação específica, uma solução pode ser mais fácil de implementar do que outra.

Solução 1- Rota estática para a interface Null0 (ASA versão 9.2.1 e posterior)

Quando você envia tráfego para uma interface **Null0**, isso faz com que os pacotes destinados à rede especificada sejam descartados. Esse recurso é útil quando você configura Remote

Triggered Black Hole (RTBH) para Border Gateway Protocol (BGP). Nessa situação, se você configurar uma rota para Null0 para a sub-rede do cliente de acesso remoto, ela forçará o ASA a descartar o tráfego destinado aos hosts nessa sub-rede se uma rota mais específica (fornecida pela Injeção de rota inversa) não estiver presente.

```
route Null0 10.255.0.0 255.255.255.0
```

Solução 2 - Usar um pool IP diferente para clientes VPN

Essa solução é atribuir aos usuários remotos de VPN um endereço IP que não se sobreponha a nenhuma sub-rede interna da rede. Isso impediria que o ASA encaminhasse pacotes destinados àquela sub-rede VPN de volta ao roteador interno se o usuário VPN não estivesse conectado.

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

Essa solução é garantir que a tabela de roteamento do ASA não tenha nenhuma rota muito ampla que se sobreponha ao pool de IP da VPN. Para este exemplo de rede específico, remova a rota 10.0.0.0/8 do ASA e configure rotas estáticas mais específicas para as sub-redes que residem fora da interface interna. Dependendo do número de sub-redes e da topologia de rede, isso pode ser um grande número de rotas estáticas e pode não ser possível.

Solução 4 - Adicione uma rota mais específica para a sub-rede VPN de volta à interface externa

Essa solução é mais complicada do que as outras descritas neste documento. A Cisco recomenda que você tente usar as outras soluções primeiro devido à situação descrita na Nota mais adiante nesta seção. Essa solução é impedir que o ASA encaminhe pacotes IP originados da sub-rede IP da VPN de volta ao roteador interno; você pode fazer isso se adicionar uma rota mais específica para a sub-rede VPN fora da interface externa. Como essa sub-rede IP é reservada para usuários de VPN externos, os pacotes com um endereço IP de origem dessa sub-rede IP de VPN nunca devem chegar na entrada na interface interna do ASA. A maneira mais fácil de conseguir isso é adicionar uma rota para o pool IP da VPN de acesso remoto fora da interface externa com um endereço IP do próximo salto do roteador ISP upstream.

Neste exemplo de topologia de rede, essa rota seria assim:

```
route outside 10.255.0.0 255.255.255.0 198.51.100.1
```

Além dessa rota, adicione o **comando ip verify reverse-path inside** para que o ASA descarte todos os pacotes recebidos na interface interna originados da sub-rede IP VPN devido à rota mais preferencial existente na interface externa:

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

Depois que esses comandos são implementados, a tabela de roteamento ASA é semelhante a esta quando o usuário está 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 está conectado, a rota baseada em host para esse endereço IP de VPN está presente na tabela e é preferida. Quando o cliente VPN se desconecta, o tráfego originado desse endereço IP do cliente que chega na interface interna é verificado em relação à tabela de roteamento e descartado devido ao comando **ip verify reverse-path inside**.

Se o cliente VPN gera um broadcast de rede direcionado para a sub-rede IP da VPN, esse pacote é encaminhado para o roteador interno e encaminhado pelo roteador de volta para o ASA, onde é descartado devido ao comando **ip verify reverse-path inside**.

> **Note**: Depois que essa solução for implementada, se o comando **same-security permit intrainterface** estiver presente na configuração e as políticas de acesso permitirem, o tráfego originado de um usuário VPN destinado a um endereço IP no pool IP da VPN para um usuário que não está conectado pode ser roteado de volta para fora da interface externa em texto claro. Essa é uma situação rara e pode ser atenuada com o uso de filtros de VPN na política de VPN. Essa situação ocorre somente se o comando **same-security permit intrainterface** estiver presente na configuração do ASA.
>
> Da mesma forma, se os hosts internos gerarem tráfego destinado a um endereço IP no pool de VPNs e esse endereço IP não for atribuído a um usuário remoto de VPN, esse tráfego poderá sair do lado de fora do ASA em texto claro.