Configurar Hairpinning de Tráfego Entre Dois Túneis Site a Site

Contents

Introdução

Este documento descreve como encaminhar o tráfego VPN entre dois túneis VPN em uma única interface.

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:
· Compreensão básica da VPN de site para site com base em políticas
· Experiência com a linha de comando ASA

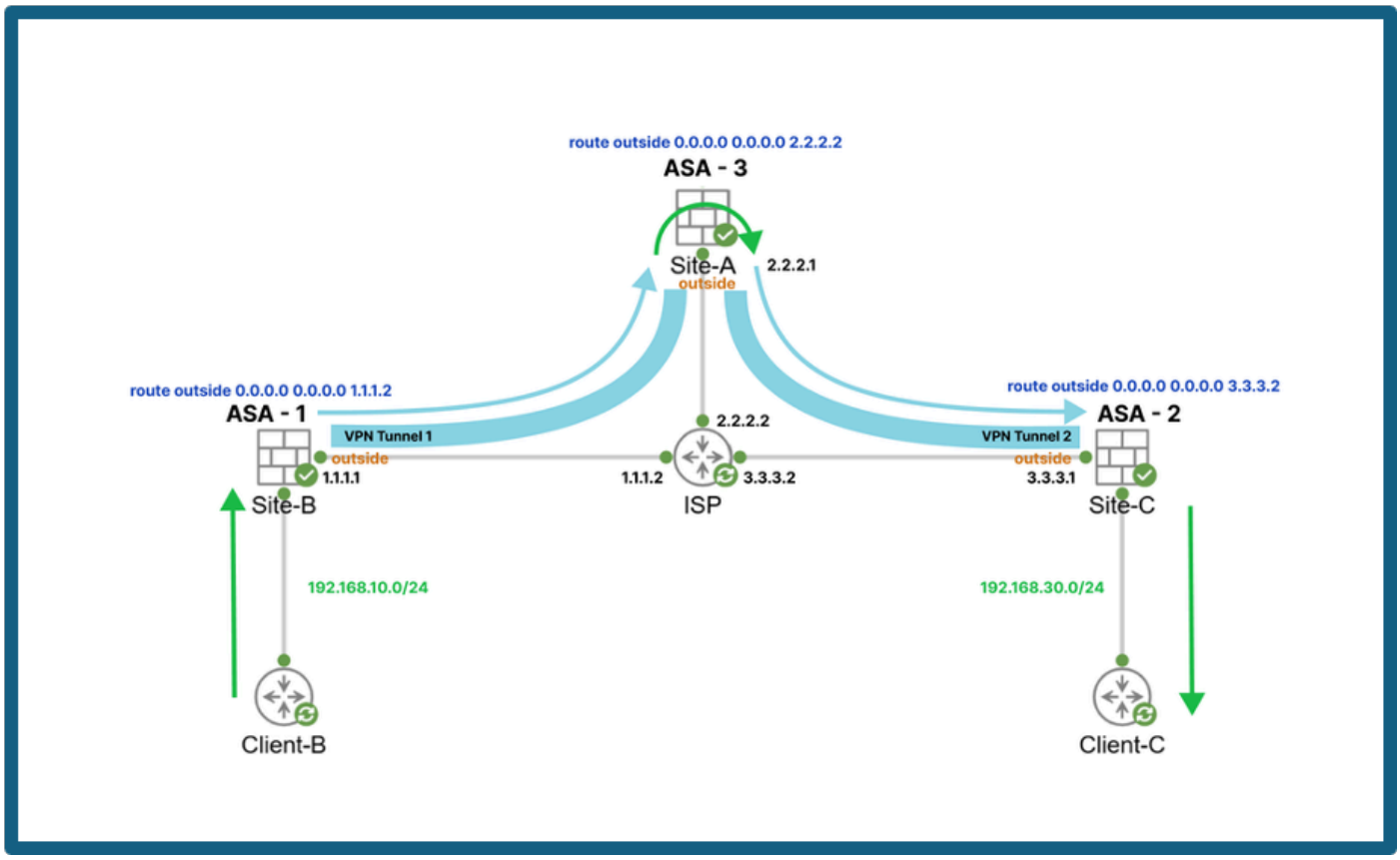
Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:
· Adaptive Security Appliance (ASA) versão 9.20
IKEv1

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Topologia



Topologia

Informações de Apoio

Essa configuração demonstra como redirecionar o tráfego de um túnel site a site para outro no mesmo dispositivo. Para ilustrar essa configuração, usamos três ASAs que representam o Local A, o Local B e o Local C.

Configuração

Esta seção descreve a configuração necessária para permitir o tráfego do ASA-1 (Local B) para o ASA-2 (Local C) através do ASA-3 (Local A).

Temos dois túneis VPN configurados:

- Túnel VPN 1: Túnel VPN entre os Sites B e A
- Túnel VPN 2: Túnel VPN entre os Sites-C e A

Para obter orientação detalhada sobre como criar um túnel VPN baseado em política no ASA, consulte a seção Configuração do ASA na documentação da Cisco: Configurar um túnel IPSec de site a site IKEv1 entre o ASA e o roteador Cisco IOS XE

Configuração do ASA (local B)

Precisamos permitir o tráfego da rede Site-B para a rede Site-C na lista de acesso criptografada do Túnel 1 da VPN na interface externa do ASA 1.
Neste cenário, é de 192.168.10.0/24 a 192.168.30.0/24

Crypto Access-list:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Exceção Nat:

```
nat (inside,outside) source static192.168.10.0_24192.168.10.0_24 destination static192.168.30.0_24192.1
```

Mapa de criptografia para o túnel VPN 1:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 2.2.2.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA (Site C) Configuração de criptografia

Permita o tráfego da rede Site-C para a rede Site-B na lista de acesso criptografada do Túnel VPN 2 na interface externa do ASA 2.
Neste cenário, é de 192.168.30.0/24 a 192.168.10.0/24

Crypto Access-list:

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
```

Exceção Nat:

```
nat (inside,outside) source static 192.168.30.0_24 192.168.30.0_24 destination static 192.168.10.0_24 1
```

Mapa de criptografia para o túnel VPN 2:

```
crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 2.2.2.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA (Site A) Configuração de criptografia

Permita o tráfego da rede do Site-C para a rede do Site-B na lista de acesso criptografada do Túnel VPN 1 e o tráfego da rede do Site-B para a rede do Site-C na lista de acesso criptografada do Túnel VPN 2 na interface externa do ASA no Site-A que está na direção inversa ao que configuramos em _ ASAs.

Neste cenário, é de 192.168.30.0/24 a 192.168.10.0/24 para o túnel VPN 1 e de 192.168.10.0/24 a 192.168.30.0/24 para o túnel VPN 2

Crypto Access-list:

```
object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
access-list 120 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Configuração do mapa de criptografia para os Túneis VPN 1 e 2:

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 1.1.1.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 3.3.3.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

Além disso, como precisamos rotear o tráfego de fora para fora, que é a mesma interface com o mesmo nível de segurança, precisamos configurar o comando:

```
same-security-traffic permit intra-interface
```

Fluxo de tráfego do local B para o local C

Considere que o tráfego seja iniciado do Site-B para o Site-c, que é de 192.168.10.0/24 a 192.168.30.0/24.

Local-B (Origem)

1. O tráfego iniciado em 192.168.10.0/24 network (Site-B) e destinado a 192.168.30.0/24 network (Site-C) é roteado para a interface externa do ASA-1 com base na tabela de roteamento configurada.

2. Quando o tráfego chega ao ASA-1, ele corresponde à lista de acesso de criptografia 110 configurada no ASA-1. Isso aciona a criptografia do tráfego usando o Túnel VPN 1, que envia

com segurança os dados para o Site-A.

Local A (intermediário)

1. O tráfego criptografado de 192.168.10.0/24 to 192.168.30.0/24 arrives na interface externa do ASA no Local-A.
2. No Site-A, o tráfego é descriptografado pelo Túnel VPN 1 para restaurar o payload original.
3. O tráfego descriptografado é, então, criptografado novamente usando o túnel VPN 2 na interface externa do ASA no local A.

Site-C (Destino)

1. O tráfego criptografado de 192.168.10.0/24 to 192.168.30.0/24 reaches na interface externa do ASA-2 no local C.
2. O ASA-2 descriptografa o tráfego usando o Túnel VPN 2 e encaminha os pacotes para o lado LAN do Site-C, entregando-os ao destino pretendido dentro do 192.168.30.0/24 network.

Fluxo de tráfego reverso do local C para o local B

O fluxo de tráfego reverso, originário do Site-C (192.168.30.0/24) and) destinado ao Site-B (192.168.10.0/24), resulta no mesmo processo, mas na direção inversa:
1. No Site-C, o tráfego é criptografado pelo Túnel VPN 2 antes de ser enviado para o Site-A.
2. No Site-A, o tráfego é descriptografado pelo Túnel VPN 2 e, em seguida, recriptografado usando o Túnel VPN 1 antes de ser encaminhado ao Site-B.
3. No Local-B, o tráfego é descriptografado pelo Túnel VPN 1 e entregue ao 192.168.10.0/24 network.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.