Configuration de l'interconnexion du trafic entre deux tunnels de site à site

Table des matières

Introduction

Ce document décrit comment transférer le trafic VPN entre deux tunnels VPN sur une interface unique.

Conditions préalables

Exigences

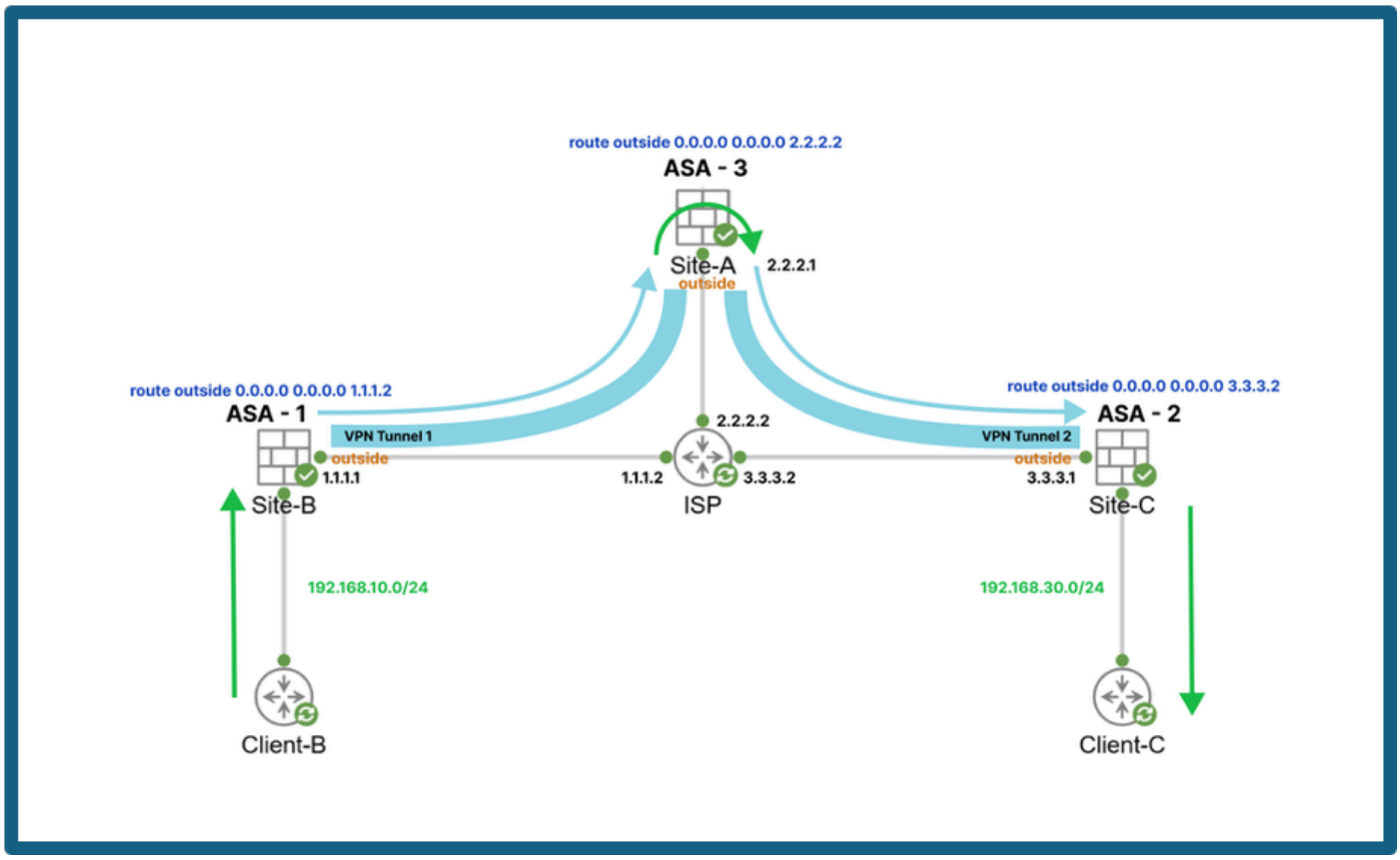
Cisco recommande de connaître les sujets suivants :
· Compréhension de base du VPN site à site basé sur des politiques
· Expérience avec la ligne de commande ASA

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :
· Adaptive Security Appliance (ASA) version 9.20
· IKEv1

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Topologie



Topologie

Informations générales

Cette configuration montre comment rediriger le trafic d'un tunnel de site à site vers un autre sur le même périphérique. Pour illustrer cette configuration, nous avons utilisé trois ASA représentant les sites A, B et C.

Configuration

Cette section décrit la configuration requise pour autoriser le trafic entre ASA-1 (Site B) et ASA-2 (Site C) via ASA-3 (Site A).

Deux tunnels VPN sont configurés :

- Tunnel VPN 1 : Tunnel VPN entre Site-B et Site-A
- Tunnel VPN 2 : Tunnel VPN entre Site-C et Site-A

Pour obtenir des instructions détaillées sur la création d'un tunnel VPN basé sur des stratégies sur ASA, reportez-vous à la section Configuration ASA de la documentation Cisco : Configuration d'un tunnel IPSec IKEv1 site à site entre ASA et le routeur Cisco IOS XE

Configuration ASA (Site B)

Nous devons autoriser le trafic du réseau de Site-B vers le réseau de Site-C dans la liste d'accès de chiffrement du tunnel VPN 1 sur l'interface externe d'ASA 1.
Dans ce scénario, il est compris entre 192.168.10.0/24 et 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
```

Exception Nat :

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

Crypto-carte pour le tunnel 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
```

Configuration du cryptage ASA (Site C)

Autorisez le trafic du réseau de Site-C vers le réseau de Site-B dans la liste d'accès de chiffrement du tunnel VPN 2 sur l'interface externe d'ASA 2.
Dans ce scénario, il est compris entre 192.168.30.0/24 et 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
```

Exception Nat :

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

Crypto-carte pour le tunnel 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
```

Configuration du cryptage ASA (Site A)

Autorisez le trafic du réseau du Site-C vers le réseau du Site-B dans la crypto access-list du tunnel VPN 1 et le trafic du réseau du Site-B vers le réseau du Site-C dans la crypto access-list du tunnel VPN 2 sur l'interface externe de l'ASA au Site-A qui est dans le sens inverse de ce que nous avons configuré sur les _ ASA.

Dans ce scénario, il est compris entre 192.168.30.0/24 et 192.168.10.0/24 pour le tunnel VPN 1 et entre 192.168.10.0/24 et 192.168.30.0/24 pour le tunnel 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
```

Configuration de crypto-carte pour les tunnels VPN 1 et 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
```

En plus de cela, comme nous devons router le trafic de l'extérieur vers l'extérieur qui est la même interface avec le même niveau de sécurité, nous devons configurer la commande :

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

Flux de trafic du site B au site C

Considérons que le trafic est initié de Site-B vers Site-c, c'est-à-dire de 192.168.10.0/24 à 192.168.30.0/24.

Site-B (source)

1. Le trafic initié à partir de 192.168.10.0/24 network (Site-B) et destiné à 192.168.30.0/24 network (Site-C) est routé vers l'interface externe d'ASA-1 en fonction de la table de routage configurée.

2. Une fois que le trafic atteint ASA-1, il correspond à la crypto access-list 110 configurée sur ASA-1. Cela déclenche le chiffrement du trafic à l'aide du tunnel VPN 1, qui envoie les données vers Site-A en toute sécurité.

Site-A (Intermédiaire)

1. Le trafic chiffré de 192.168.10.0/24 to 192.168.30.0/24 arrives à l'interface externe de l'ASA sur Site-A.
2. Au niveau du Site-A, le trafic est décrypté par le tunnel VPN 1 pour restaurer la charge utile d'origine.
3. Le trafic décrypté est ensuite re-crypté à l'aide du tunnel VPN 2 au niveau de l'interface externe de l'ASA au niveau du Site-A.

Site-C (destination)

1. Le trafic chiffré de 192.168.10.0/24 to 192.168.30.0/24 reaches est l'interface externe de l'ASA-2 sur Site-C.
2. ASA-2 décrypte le trafic à l'aide du tunnel VPN 2 et transfère les paquets vers le côté LAN de Site-C, en les délivrant à la destination prévue dans le réseau 192.168.30.0/24 network.

Flux de trafic inverse du site C vers le site B

Le flux de trafic inverse, en provenance du Site-C (192.168.30.0/24) and) et à destination du Site-B (192.168.10.0/24), entraîne le même processus, mais dans le sens inverse :
1. Au niveau du site C, le trafic est chiffré par le tunnel VPN 2 avant d'être envoyé au site A.
2. Au niveau du site A, le trafic est déchiffré par le tunnel VPN 2, puis re-chiffré à l'aide du tunnel VPN 1 avant d'être transféré au site B.
3. Sur le site B, le trafic est décrypté par le tunnel VPN 1 et livré à l'adresse 192.168.10.0/24 network.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.