Exemple de configuration du trafic VPN SSL sans client ASA sur un tunnel LAN à LAN IPsec

Contenu

Introduction

Ce document décrit comment se connecter à un portail SSLVPN sans client Cisco ASA (Adaptive Security Appliance) et accéder à un serveur situé dans un emplacement distant connecté via un tunnel LAN à LAN IPsec.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN SSL sans client.
- Configuration VPN LAN à LAN

Components Used

Les informations de ce document sont basées sur la gamme ASA 5500-X qui exécute la version 9.2(1), mais elles s'appliquent à toutes les versions ASA.

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. Assurez-vous de

bien comprendre l'impact potentiel de toute commande avant d'apporter des modifications à un réseau actif.

Informations générales

Lorsque le trafic d'une session VPN sans client traverse un tunnel LAN à LAN, notez qu'il existe deux connexions :

- Du client à l'ASA
- De l'ASA à l'hôte de destination.

Pour la connexion de l'hôte ASA à destination, l'adresse IP de l'interface ASA « la plus proche » de l'hôte de destination est utilisée. Par conséquent, le trafic intéressant de LAN à LAN doit inclure une identité de proxy de cette adresse d'interface au réseau distant.

> **Note**: Si Smart-Tunnel est utilisé pour un signet, l'adresse IP de l'interface ASA la plus proche de la destination est toujours utilisée.

Configuration

Dans ce schéma, il existe un tunnel LAN à LAN entre deux ASA qui permet au trafic de passer de 192.168.10.x à 192.168.20.x.

La liste d'accès qui détermine le trafic intéressant pour ce tunnel :

ASA1

```
access-list l2l-list extended permit ip 192.168.10.0 255.255.255.0 192.168.20.0
255.255.255.0
```

ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 192.168.10.0
255.255.255.0
```

Si l'utilisateur SSLVPN sans client tente de communiquer avec un hôte sur le réseau 192.168.20.x, ASA1 utilise l'adresse 209.165.200.225 comme source pour ce trafic. Comme la liste de contrôle d'accès LAN à LAN ne contient pas 209.168.200.225 en tant qu'identité proxy, le trafic n'est pas envoyé via le tunnel LAN à LAN.

Afin d'envoyer le trafic sur le tunnel LAN à LAN, une nouvelle entrée de contrôle d'accès (ACE) doit être ajoutée à la liste de contrôle d'accès de trafic intéressante.

ASA1

```
access-list l2l-list extended permit ip host 209.165.200.225 192.168.20.0
255.255.255.0
```

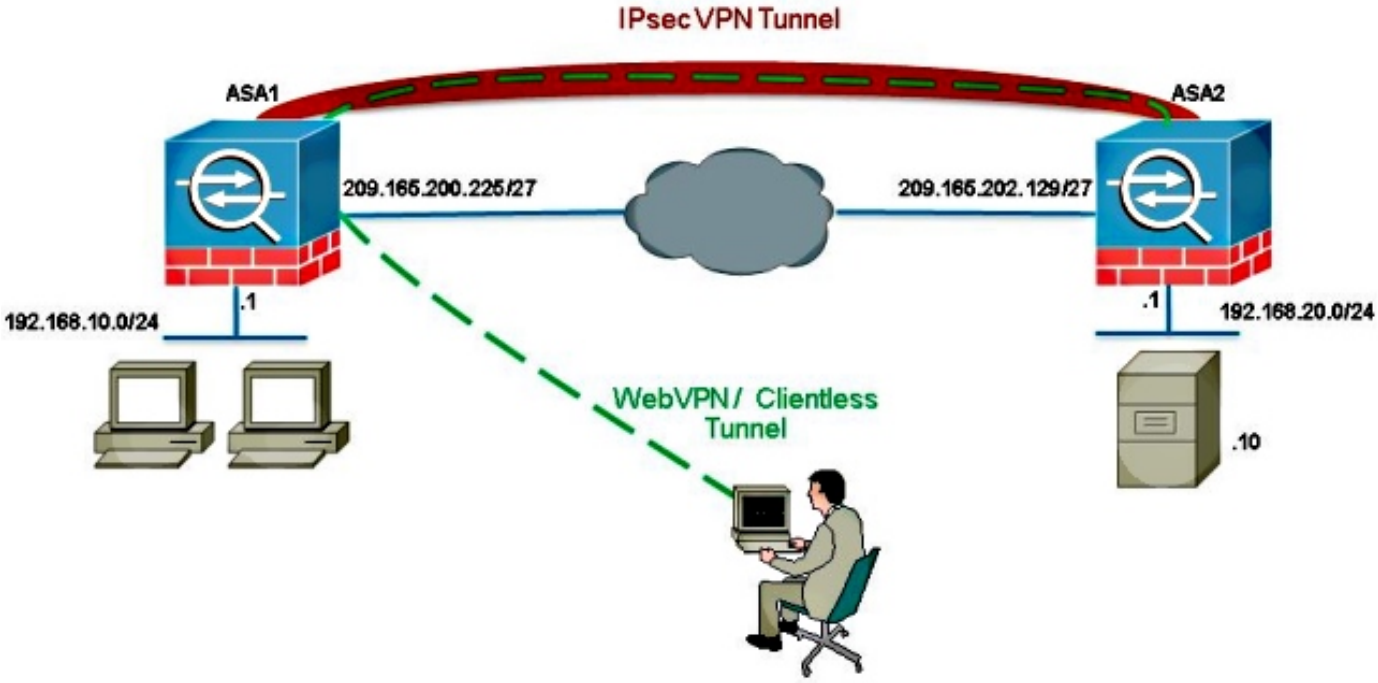
ASA2

```
access-list l2l-list extended permit ip 192.168.20.0 255.255.255.0 host
209.165.200.225
```

Ce même principe s'applique aux configurations où le trafic SSLVPN sans client doit **activer** la même interface qu'elle est entrée, même s'il n'est pas censé passer par un tunnel LAN à LAN.

> **Note**: Utilisez l'Outil de recherche de commande (clients inscrits seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau



En règle générale, ASA2 effectue la traduction d'adresses de port (PAT) pour 192.168.20.0/24 afin de fournir un accès à Internet. Dans ce cas, le trafic de 192.168.20.0/24 sur ASA 2 doit être exclu du processus PAT lorsqu'il va à 209.165.200.225. Sinon, la réponse ne passerait pas par le tunnel LAN à LAN. Exemple :

ASA2

```
nat (inside,outside) source static obj-192.168.20.0 obj-
192.168.20.0 destination
static obj-209.165.200.225 obj-209.165.200.225
!
object network obj-192.168.20.0
nat (inside,outside) dynamic interface
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

- **show crypto ipsec sa**-Vérifiez avec cette commande qu'une association de sécurité (SA) entre l'adresse IP du proxy ASA1 et le réseau distant a été créée. Vérifiez si les compteurs chiffrés et déchiffrés augmentent lorsque l'utilisateur SLVPN sans client accède à ce serveur.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Si l'association de sécurité n'est pas créée, vous pouvez utiliser le débogage IPsec à la cause de l'échec :

- **debug crypto ipsec <level>**

  Note: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.