

Exemple de configuration d'une connexion client VPN ASA via un tunnel L2L

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Ajouter une entrée dynamique](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer le dispositif de sécurité adaptatif Cisco (ASA) afin d'autoriser une connexion client VPN à distance à partir d'une adresse homologue Lan-to-Lan (L2L).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ASA
- [VPN d'accès à distance](#)
- [VPN LAN à LAN](#)

Components Used

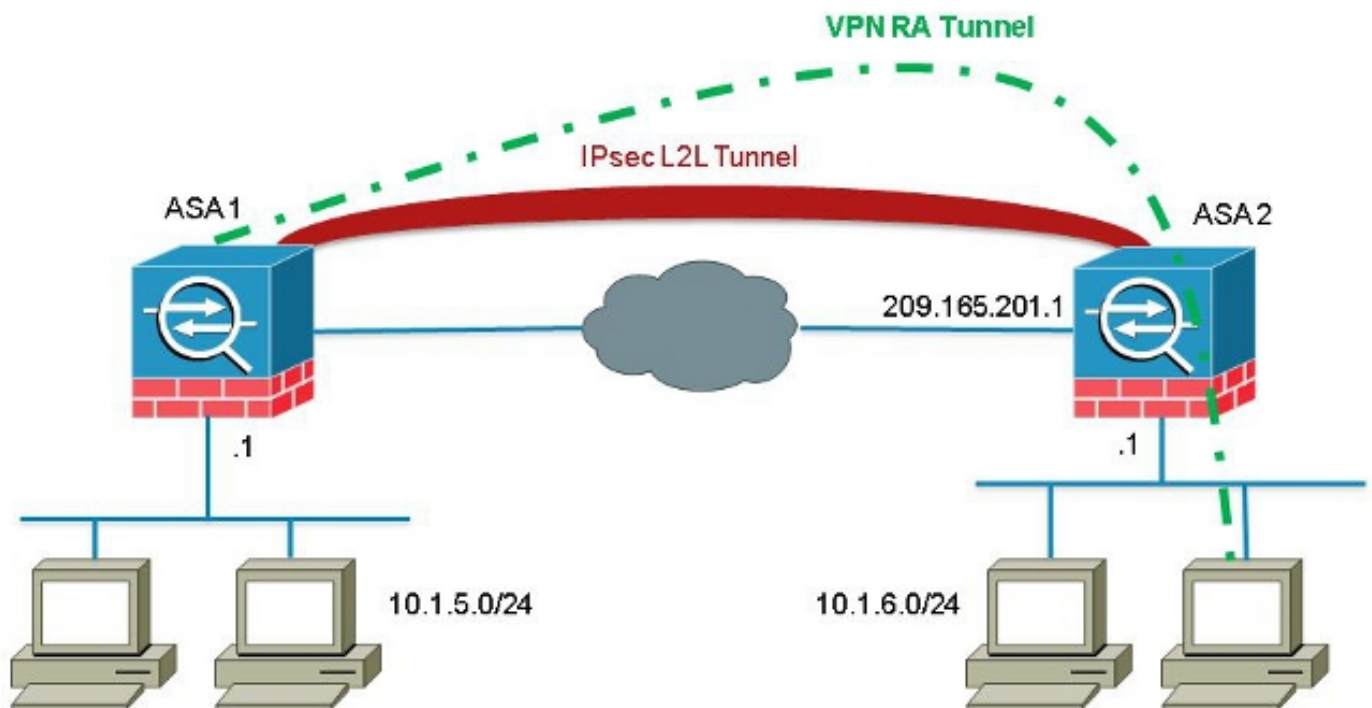
Les informations de ce document sont basées sur l'ASA de la gamme Cisco 5520 qui exécute le logiciel version 8.4(7).

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.

Informations générales

Bien qu'il ne soit pas courant de rencontrer un scénario dans lequel un client VPN tente d'établir une connexion via un tunnel L2L, les administrateurs peuvent vouloir attribuer des privilèges ou des restrictions d'accès spécifiques à certains utilisateurs distants et leur demander d'utiliser le client logiciel lorsque l'accès à ces ressources est requis.

Note: Ce scénario a fonctionné dans le passé, mais après une mise à niveau de la tête de réseau ASA vers la version 8.4(6) ou ultérieure, le client VPN n'est plus en mesure d'établir la connexion.



L'ID de bogue Cisco [CSCuc75090](#) a introduit un changement de comportement. Auparavant, avec le protocole PIX (Private Internet Exchange), lorsque le proxy IPsec (Internet Protocol Security) ne correspondait pas à une liste de contrôle d'accès crypto-map (ACL), il continuait à vérifier les entrées plus bas dans la liste. Cela inclut des correspondances avec une crypto-carte dynamique sans homologue spécifié.

Ceci a été considéré comme une vulnérabilité, car les administrateurs distants pouvaient accéder aux ressources que l'administrateur de tête de réseau n'avait pas l'intention de configurer lors de la configuration de L2L statique.

Un correctif a été créé qui a ajouté une vérification afin d'empêcher les correspondances avec une entrée de crypto-carte sans homologue lorsqu'il a déjà vérifié une entrée de carte qui correspondait à l'homologue. Toutefois, cela a affecté le scénario abordé dans ce document. Plus précisément, un client VPN distant qui tente de se connecter à partir d'une adresse homologue L2L ne peut pas se connecter à la tête de réseau.

Configuration

Utilisez cette section afin de configurer l'ASA afin d'autoriser une connexion client VPN à distance à partir d'une adresse homologue L2L.

Ajouter une entrée dynamique

Afin d'autoriser les connexions VPN distantes à partir d'adresses homologues L2L, vous devez ajouter une nouvelle entrée dynamique qui contient la même adresse IP homologue.

Note: Vous devez également laisser une autre entrée dynamique sans homologue pour que n'importe quel client d'Internet puisse également se connecter.

Voici un exemple de la configuration de travail de crypto-carte dynamique précédente :

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

Voici la configuration de crypto-carte dynamique avec la nouvelle entrée dynamique configurée :

```
crypto dynamic-map ra-dyn-map 10 set ikev1 transform-set ESP-AES-128-SHA
crypto dynamic-map ra-dyn-map 10 set peer 209.165.201.1
crypto dynamic-map ra-dyn-map 20 set ikev1 transform-set ESP-AES-128-SHA

crypto map outside_map 1 match address outside_cryptomap_1
crypto map outside_map 1 set peer 209.165.201.1
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA
crypto map outside_map 65535 ipsec-isakmp dynamic ra-dyn-map
```

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.