Connexion client VPN ASA par un exemple de configuration de tunnel L2L

Contenu

Introduction

Ce document décrit comment configurer l'appliance de sécurité adaptable Cisco (ASA) afin de permettre une connexion client VPN distante d'une adresse de pair du Réseau local-à-réseau local (L2L).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ASA
- Accès à distance VPN
- Entre réseaux locaux VPN

Composants utilisés

Les informations dans ce document sont basées sur la gamme Cisco 5520 ASA qui exécutent la version de logiciel 8.4(7).

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Bien qu'il ne soit pas commun pour rencontrer un scénario où les tentatives d'un client vpn d'établir une connexion par un tunnel L2L, des administrateurs pourraient vouloir assigner des privilèges spécifiques ou accéder à des restrictions à certains utilisateurs distants et les instruire utiliser le client logiciel quand l'accès à ces ressources est exigé.

> Remarque: Ce scénario fonctionné dans le passé, mais après qu'une mise à jour du headend ASA à la version 8.4(6) ou ultérieures, le client VPN soit ne puisse plus établir la connexion.

L'ID de bogue Cisco CSCuc75090 a introduit une modification de comportement. Précédemment, avec le Private Internet Exchange (PIX), quand le proxy d'IPSec (IPSec) n'a pas apparié une liste de contrôle d'accès de crypto map (ACL), il a continué à vérifier des entrées plus loin en bas de la liste. Ceci a inclus des correspondances avec une crypto-carte dynamique sans le pair spécifié.

Ceci a été considéré une vulnérabilité, car les administrateurs distants pourraient accéder aux ressources que l'administrateur de headend n'a pas destinées quand le L2L statique a été configuré.

On a créé une difficulté qui a ajouté un contrôle afin d'empêcher des correspondances avec une entrée de crypto map sans pair quand elle a déjà vérifié une entrée de mappage qui a apparié le pair. Cependant, ceci a affecté le scénario qui est discuté dans ce document. Spécifiquement, un client vpn distant qui tente de se connecter d'une adresse de pair L2L ne peut pas se connecter au headend.

Configurez

Employez cette section afin de configurer l'ASA afin de permettre une connexion client VPN distante d'une adresse de pair L2L.

Ajoutez une nouvelle entrée dynamique

Afin de permettre les connexions VPN distantes des adresses de pair L2L, vous devez ajouter une nouvelle entrée dynamique qui contient la même adresse IP de pair.

> Remarque: Vous devez également laisser une autre entrée dynamique sans pair de sorte que n'importe quel client de l'Internet puisse se connecter aussi bien.

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

```
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
```

Vérifiez

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

Dépannez

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