Contenu

Introduction

Ce document fournit des informations sur la façon dont configurer un périphérique de passerelle VPN pour agir toujours en tant que responder dans une négociation d'IKE. Le périphérique répondra à toutes les cryptos négociations initiées par ses pairs.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur de Cisco avec la version de logiciel 12.4(24)T et ultérieures de Cisco IOS®
- Appliance de sécurité adaptable Cisco (ASA) avec la version 7.0 et ultérieures

Produits connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

- Pare-feu de Cisco PIX avec la version de logiciel 7.0 et plus tard

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

N'importe quelle crypto négociation a deux interlocuteurs pour lire les rôles de demandeur et de responder. Le demandeur envoie les cryptos propositions au responder qui contient différents paramètres au sujet du cryptage, des algorithmes d'authentification, réintroduisant des options et les valeurs de vie et ainsi de suite. Le responder choisit la bonne proposition et une crypto session établit. Le rôle joué par un fin-périphérique peut être visualisé par cette sortie de commande :

```
Router#show crypto isakmp sa1   IKE Peer: XX.XX.XX.XX    Type    : L2L             Role    :
initiator    Rekey   : no              State   : MM_ACTIVEASA(config)#show crypto isakmp sa
detailIKE Peer    Type  Dir   Rky    State      Encrypt    Hash  Auth       Lifetime1
209.165.200.225 User  Resp  No   AM_Active    3des      SHA   preshrd     86400
```

Avantages de la caractéristique réservée au responder de mode d'IKE

Puisque l'apparition des caractéristiques du réseau privé virtuel (VPN) qui permettent des négociations bidirectionnelles simultanées d'IKE (avec ou sans le trafic intéressant), les questions avec la manipulation et la reprise des données de l'IKE en double SAS se sont produites. L'IKE comme protocole n'a aucune capacité de comparer des négociations d'IKE pour déterminer s'il y a déjà une négociation de exister ou de dans-processus entre deux pairs ayant lieu. Ces négociations en double peuvent être coûteuses en termes de ressources et confondre aux administrateurs de routeur. Quand un périphérique est configuré comme périphérique réservé au responder, il n'initiera pas des modes principaux, agressifs, ou rapides d'IKE (pour l'IKE et l'établissement d'IPSec SA), ni il réintroduira l'IKE et l'IPSec SAS. Par conséquent, la probabilité du doublon SAS est réduite.

L'autre avantage de cette caractéristique est de permettre le support commandé pour les connexions de négociation dans une direction seulement dans un scénario d'Équilibrage de charge. On ne le recommande pas que les serveurs ou les Concentrateurs initient des connexions VPN vers les clients ou les rais parce que ces périphériques sont tous qui sont accédés à par une adresse IP de simple-revêtement comme annoncé par l'intermédiaire de l'équilibreur de charge. Si les Concentrateurs étaient d'initier la connexion, ils feraient ainsi utilisant une adresse IP individuelle, de ce fait évitant les avantages de l'équilibreur de charge. Le même est vrai de réintroduire les demandes qui sont originaires des Concentrateurs ou des serveurs derrière l'équilibreur de charge.

Un routeur à configurer comme périphérique réservé au responder dans une crypto négociation

Le Logiciel Cisco IOS version 12.4(24)T introduit la fonctionnalité du routeur pour répondre toujours aux négociations d'IKE initiées par ses pairs. La limite principale est que cette caractéristique est configurable seulement sous un profil IPSec et est appropriée seulement à un scénario d'interface virtuelle. Aucun soutien des scénarios de charge statique ou de crypto-carte dynamique.

Afin de configurer votre routeur comme réservé au responder, exécutez ces étapes :

```
enable configure terminal crypto ipsec profile <name>   responder-only
```

Une ASA à configurer comme périphérique réservé au responder dans une crypto négociation

En général les connexions entre réseaux locaux d'IPSec, l'ASA peuvent fonctionner comme demandeur ou responder. Dans des connexions de client-à-RÉSEAU LOCAL d'IPSec, l'ASA fonctionne seulement comme responder. Une ASA peut être configurée en tant que périphérique réservé répondre dans des connexions VPN d'entre réseaux locaux. Cependant, la restriction est que le périphérique à l'autre bout du tunnel VPN doit être l'un de ces derniers :

- Appliance de gamme de Cisco ASA 5500
- Concentrateur de gamme de Cisco VPN 3000
- Pare-feu de gamme 500 de Cisco PIX qui exécute le logiciel 7.0 et plus tard

Afin de configurer votre ASA en tant que périphérique réservé au responder, émettez cette commande :

connexion-type réglé du mymap 10 de crypto map de hostname(config)# réservé à la réponse

Remarque: On lui suggère de configurer un périphérique de passerelle VPN comme réservé au responder où les plusieurs homologues VPN se terminent.

Informations connexes

- Configuration d'un tunnel LAN à LAN entre deux routeurs, l'un des deux initiant IKE en mode agressif
- Exemples et TechNotes de configuration de Cisco ASA
- Support et documentation techniques - Cisco Systems