Renégociation des configurations LAN à LAN entre les concentrateurs Cisco VPN, Cisco IOS et les périphériques PIX

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Diagramme du réseau
Conventions
Scénarios de test
Résultats de test
Informations connexes

Introduction

Ce document signale les résultats de test de laboratoire de la renégociation de tunnel entre réseaux locaux de sécurité IP (IPSec) entre différents Produits de Cisco VPN dans divers scénarios, tels que la réinitialisation de périphérique VPN, le rekey, et l'arrêt manuel des associations de sécurité d'IPSec (SAS).

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 :

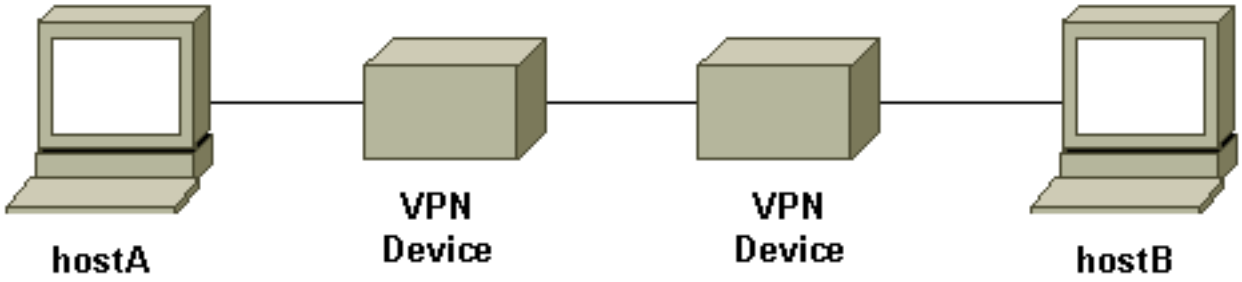
- Version de logiciel 12.1(5)T8 de Cisco IOS®
- Version du logiciel PIX de Cisco 6.0(1)
- Version 3.0(3)A de logiciel du concentrateur de Cisco VPN 3000
- Version 5.2(21) de logiciel du concentrateur de Cisco VPN 5000

Le trafic IP utilisé dans ce test est les paquets bidirectionnels de Protocole ICMP (Internet Control Message Protocol) entre le hostA et le hostB.

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.

Diagramme du réseau

C'est un diagramme de concept du banc d'essai.



Les périphériques VPN représentent un routeur Cisco IOS, un pare-feu Cisco Secure PIX, un concentrateur de Cisco VPN 3000 ou un concentrateur de Cisco VPN 5000.

Conventions

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

Scénarios de test

Trois scénarios communs ont été testés. Ce qui suit est une brève définition des scénarios de test :

- **Arrêt manuel d'IPSec SAS** — L'utilisateur ouvre une session aux périphériques VPN et efface manuellement l'IPSec SAS utilisant l'interface de ligne de commande (CLI) ou l'interface utilisateur graphique (GUI).
- **Rekey** — Rekey normal de la phase I et de la phase II d'IPSec quand la vie définie expire. Dans ce test, les deux périphériques de terminaison VPN ont la même vie de la phase I et de la phase II configurée.
- **Réinitialisation de périphérique VPN** — L'un ou l'autre d'extrémité des points d'arrêt de tunnel VPN a été redémarrée pour simuler la panne de service.

Remarque: Pour des tunnels entre réseaux locaux où le concentrateur VPN 5000 est utilisé, le concentrateur est configuré utilisant le responder PRINCIPAL de mode et de tunnel.

Résultats de test

Installation	Manuellement arrêt d'IPSec SAS	Rekey	Réinitialisation de périphérique VPN
IOS à	• Le tunnel a rétabli après la	• Le trafic	• La keepalive

PIX	phase I ou SA de la phase II est autorisée de chaque côté • Travaux du trafic de test	de test fonctionne toujours après rekey de la phase I ou de la phase II	d'IKE étant activé sur les deux périphériques, tunnel rétablis • Travaux du trafic[1] de test après le tunnel récupéré
IOS au VPN 3000	• Le tunnel a rétabli après la phase I ou SA de la phase II est autorisée de chaque côté • Travaux du trafic de test	• Le trafic de test fonctionne toujours après rekey de la phase I ou de la phase II	• La keepalive d'IKE étant activé sur les deux périphériques, tunnel rétablis • Travaux du trafic[1] de test après le tunnel récupéré
IOS au VPN 5000	• Sur l'IOS : Le trafic de test fonctionne toujours après SA de la phase II est effacéLe tunnel VPN va en bas de quand SA de la phase I est autoriséeLe trafic de test cesse de fonctionner • Sur le VPN 5000 : Le tunnel ne récupère pas	• Le trafic de test fonctionne toujours après rekey de la phase II • Le rekey de la phase	• Le tunnel ne récupère pas après réinitialisation l'un ou l'autre de périphérique VPN (avec le trafic bidirectionnel de test) • Le trafic de test cesse de fonctionner • Nécessité

	après avoir manuellement autorisé SADoit autoriser SA de la phase I et de la phase II sur l'IOS pour rétablir le tunnel	l a réduit le tunnel • Le trafic de test cesse de fonctionner • Nécessité manuellement SAS claire pour rapporter le tunnel	manuellement claire SA sur le périphérique qui n'a pas été redémarré pour rapporter le tunnel
PIX au VPN 3000	• Le tunnel a rétabli après la phase I ou SA de la phase II est autorisée de chaque côté • Travaux du trafic de test	• Le trafic de test fonctionne toujours après rekey de la phase I ou de la phase II	• Travaux du trafic[1 de] test après le tunnel récupéré • Avec Dead Peer Detection (DPD) [2] (activé par défaut), tunnel rétabli
PIX au VPN 5000	• Sur PIX : Le trafic de test fonctionne toujours après SA de la phase II est effacéLe tunnel VPN est allé en bas de	• Le trafic de test fonctionne toujours	• Le tunnel ne récupère pas après réinitialisation l'un ou l'autre de périphérique VPN

	quand SA de la phase I est autoriséeLe trafic de test cesse de fonctionner • Sur le VPN 5000 : Le tunnel ne récupère pas après que manuellement espaces libres SADoit autoriser SA de la phase I et de la phase II sur PIX pour rétablir le tunnel	après rekey de la phase II • Le rekey de la phase I a réduit le tunnel • Le trafic de test cesse de fonctionner • Nécessité manuellement SAS claire pour rapporter le tunnel	(avec le trafic bidirectionnel de test) • Le trafic de test cesse de fonctionner • Nécessité manuellement claire SA sur le périphérique qui n'a pas été redémarré pour rapporter le tunnel
VPN 3000 au VPN 5000	• Sur le VPN 3000 : Le tunnel est récupéré après manuellement clair la sessionDu trafic toujours travaux • Sur le VPN 5000 : Le tunnel ne récupère pas après manuellement clair le tunnelLe trafic de test cesse de	• Le trafic de test fonctionne toujours après que rekey de la phase I ou de la phase	• Le tunnel ne récupère pas après réinitialisation de l'un ou l'autre de périphérique VPN (avec le trafic bidirectionnel de test) • Le trafic de test cesse de

	fonctionnerDoit autoriser SA sur le VPN 3000 pour rétablir le tunnel	II	fonctionner • Nécessité manuellement claire SA sur le périphérique qui n'a pas été redémarré pour rapporter le tunnel

[1] comme décrit ci-dessus, le trafic de test utilisé est les paquets bidirectionnels d'ICMP entre le hostA et le hostB. Dans le test de réinitialisation de périphérique VPN, le trafic unidirectionnel est également testé pour simuler le scénario de le pire des cas (où le trafic est seulement de l'hôte derrière le périphérique VPN qui n'est pas redémarré au périphérique VPN qui est redémarré). De même que peut vu de la table, avec la keepalive d'IKE ou avec le protocole DPD, le tunnel VPN peut être récupéré du scénario de le pire des cas.

[2] DPD font partie du protocole d'Unity. Actuellement cette caractéristique est seulement disponible sur le concentrateur de Cisco VPN 3000 avec la version de logiciel 3.0 et au-dessus et sur du Pare-feu PIX avec la version de logiciel 6.0(1) et en haut.

Informations connexes

- Page d'assistance des concentrateurs VPN Cisco 3000
- Page d'assistance du concentrateur VPN Cisco 5000
- Page de support PIX
- Page d'assistance IPsec
- Support et documentation techniques - Cisco Systems