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

Contenu

Introduction

Ce document présente les résultats des tests de laboratoire de la renégociation de tunnel LAN à LAN IPSec (IP Security) entre différents produits VPN Cisco dans différents scénarios, tels que le redémarrage du périphérique VPN, la retouche et la fin manuelle des associations de sécurité IPSec.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

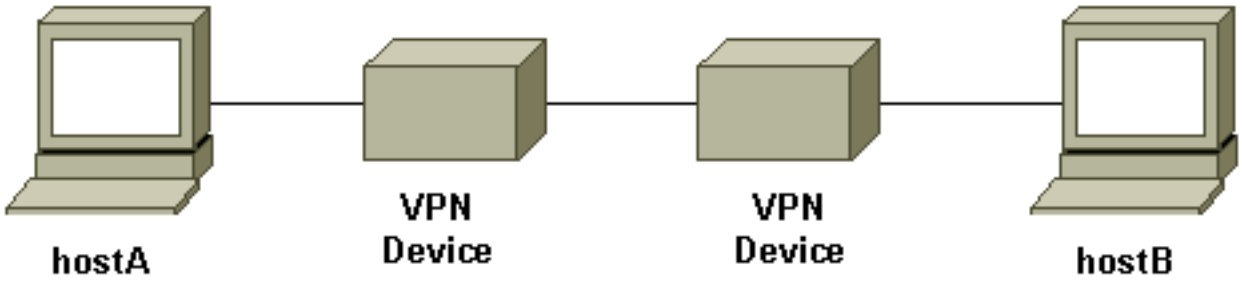
- Logiciel Cisco IOS® Version 12.1(5)T8
- Logiciel Cisco PIX Version 6.0(1)
- Logiciel Cisco VPN 3000 Concentrator version 3.0(3)A
- Logiciel Cisco VPN 5000 Concentrator version 5.2(21)

Le trafic IP utilisé dans ce test est des paquets ICMP (Internet Control Message Protocol) bidirectionnels entre les hôtes A et B.

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.

Diagramme du réseau

Voici un schéma de concept du banc d'essai.



Les périphériques VPN représentent un routeur Cisco IOS, un pare-feu Cisco Secure PIX Firewall, un concentrateur Cisco VPN 3000 ou un concentrateur 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. Voici une brève définition des scénarios de test :

- **Fermeture manuelle des SA IPSec** : l'utilisateur se connecte aux périphériques VPN et efface manuellement les SA IPSec à l'aide de l'interface de ligne de commande (CLI) ou de l'interface utilisateur graphique (GUI).
- **Rekey** - Rekey de phase I et II normal IPSec lorsque la durée de vie définie expire. Dans ce test, les deux périphériques de terminaison VPN ont la même durée de vie de phase I et de phase II configurée.
- **Redémarrage du périphérique VPN** - Chaque extrémité des points de terminaison du tunnel VPN a été redémarrée pour simuler une panne de service.

Remarque : Pour les tunnels LAN à LAN où le concentrateur VPN 5000 est utilisé, le concentrateur est configuré à l'aide du mode MAIN et du répondeur de tunnel.

Résultats des tests

Configuration	Terminaison manuelle des SA IPSec	Retouche	Redémarrage du périphérique VPN
IOS vers PIX	• Le tunnel rétabli après la phase I ou la phase II SA est effacé	• Le trafic de	• Avec IKE keepalive activé sur les deux

	de chaque côté • Tester le trafic	test fonctionne toujours après la phase I ou la phase II	périphériques, le tunnel est rétabli • Le trafic de test [1] fonctionne après récupération du tunnel
IOS vers VPN 3000	• Le tunnel rétabli après la phase I ou la phase II SA est effacé de chaque côté • Tester le trafic	• Le trafic de test fonctionne toujours après la phase I ou la phase II	• Avec IKE keepalive activé sur les deux périphériques, le tunnel est rétabli • Le trafic de test [1] fonctionne après récupération du tunnel
IOS vers VPN 5000	• Sur IOS : Le trafic de test fonctionne toujours après l'effacement de la SA de phase IILe tunnel VPN tombe en panne lorsque la SA	• Le trafic de test fonctionne touj	• Le tunnel ne parvient pas à se rétablir après le redémarrage de l'un ou l'autre des périphériques VPN (avec

	de phase I est effacéeLe trafic de test cesse de fonctionner • Sur VPN 5000 : Le tunnel ne parvient pas à se restaurer après avoir effacé manuellement l'SADoit effacer les SA de phase I et de phase II sur IOS pour rétablir le tunnel	ours après la retouche de phase II • La clé de phase I est tombée du tunnel • Le trafic de test cesse de fonctionner • Doit effacer manuellement les SA pour	un trafic de test bidirectionnel) • Le trafic de test cesse de fonctionner • Doit effacer manuellement la SA sur le périphérique qui n'a pas été redémarré pour ramener le tunnel

		rétablir le tunnel	
PIX vers VPN 3000	• Le tunnel rétabli après la phase I ou la phase II SA est effacé de chaque côté • Tester le trafic	• Le trafic de test fonctionne toujours après la phase I ou la phase II	• Le trafic de test [1] fonctionne après récupération du tunnel • Avec la détection DPD (Dead Peer Detection)[2] (activée par défaut), le tunnel est rétabli
PIX vers VPN 5000	• Sur PIX : Le trafic de test fonctionne toujours après l'effacement de la SA de phase IILe tunnel VPN est tombé en panne lorsque la SA de phase I a été suppriméeLe trafic de test cesse de fonctionner • Sur VPN 5000 : Le tunnel ne parvient pas à se restaurer après le nettoyage	• Le trafic de test fonctionne toujours après la retouche de phase II	• Le tunnel ne parvient pas à se rétablir après le redémarrage de l'un ou l'autre des périphériques VPN (avec un trafic de test bidirectionnel) • Le trafic de test cesse de fonctionner • Doit effacer manuellement la SA sur le périphérique qui n'a pas

	manuel de SADoit effacer les SA de phase I et de phase II sur PIX pour rétablir le tunnel	• La clé de phase I est tombée du tunnel • Le trafic de test ces se de fonctionner • Doit effacer manuellement les SA pour rétablir le tunnel	été redémarré pour ramener le tunnel
VPN 3000 à VPN 5000	• Sur VPN 3000 : Le tunnel est récupéré après effacement manuel de la sessionLe trafic	• Le trafic de test fon	• Le tunnel ne parvient pas à se rétablir après le redémarrage de l'un ou

	fonctionne toujours • Sur VPN 5000 : Le tunnel ne parvient pas à se rétablir après avoir effacé manuellement le tunnelLe trafic de test cesse de fonctionnerDoit effacer SA sur VPN 3000 pour rétablir le tunnel	ctionne toujours après la phase I ou la phase II	l'autre des périphériques VPN (avec un trafic de test bidirectionnel) • Le trafic de test cesse de fonctionner • Doit effacer manuellement la SA sur le périphérique qui n'a pas été redémarré pour ramener le tunnel

[1] Comme décrit ci-dessus, le trafic de test utilisé est des paquets ICMP bidirectionnels entre l'hôte A et l'hôte B. Dans le test de redémarrage du périphérique VPN, le trafic unidirectionnel est également testé pour simuler le pire scénario (où le trafic provient uniquement de l'hôte derrière le périphérique VPN qui n'est pas redémarré sur le périphérique VPN qui est redémarré). Comme le montre la table, avec IKE keepalive ou avec le protocole DPD, le tunnel VPN peut être récupéré du pire scénario.

[2] DPD fait partie du protocole Unity. Actuellement, cette fonctionnalité n'est disponible que sur le concentrateur Cisco VPN 3000 avec les versions 3.0 et ultérieures du logiciel et sur le pare-feu PIX avec les versions 6.0(1) et ultérieures du logiciel.

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