Création de tunnels redondants entre pare-feu à l'aide de PDM

Contenu

Introduction Conditions préalables Conditions requises Components Used Diagramme du réseau Conventions Informations générales Configuration Procédure de configuration Vérification Dépannage Informations connexes

Introduction

Ce document décrit la procédure que vous utilisez pour configurer des tunnels entre deux pare-feu PIX à l'aide de Cisco PIX Device Manager (PDM). Les pare-feux PIX sont placés à deux endroits différents. En cas d'échec d'accès au chemin principal, il est souhaitable de démarrer le tunnel via une liaison redondante. IPSec est une combinaison de normes ouvertes qui fournissent la confidentialité des données, l'intégrité des données et l'authentification de l'origine des données entre des homologues 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 :

• Pare-feu Cisco Secure PIX 515E avec 6.x et PDM version 3.0

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

Ce document utilise la configuration réseau suivante :



Conventions

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

Informations générales

La négociation IPSec peut être décomposée en cinq étapes et inclut deux phases d'échange de clés Internet (IKE).

Un tunnel IPSec est lancé par un trafic intéressant. Le trafic est considéré comme intéressant quand il transite entre les homologues IPSec.

Dans la phase 1 d'IKE, les homologues IPSec négocient la stratégie d'association de sécurité IKE. Une fois que les homologues sont authentifiés, un tunnel sécurisé est créé en utilisant Internet Security Association and Key Management Protocol (ISAKMP).

Dans la phase 2 d'IKE, les homologues IPSec utilisent le tunnel authentifié et sécurisé pour négocier des transformations d'association de sécurité IPSec. La négociation de la stratégie partagée détermine comment le tunnel IPSec est établi.

Le tunnel IPSec est créé et les données sont transférées entre les homologues IPSec en fonction des paramètres IPSec configurés dans les jeux de transformations IPSec.

Le tunnel IPSec se termine quand les associations de sécurité IPSec sont supprimées ou quand leur durée de vie expire.

Remarque : la négociation IPsec entre les deux PIXes échoue si les SA des deux phases IKE ne correspondent pas sur les homologues.

Configuration

Cette procédure vous guide tout au long de la configuration d'un des pare-feu PIX pour déclencher le tunnel lorsqu'il existe un trafic intéressant. Cette configuration vous aide également à établir le

tunnel via la liaison de sauvegarde via le routeur 2 (R2), lorsqu'il n'y a aucune connectivité entre le PIX-01 et le PIX-02 via le routeur 1 (R1). Ce document montre la configuration de PIX-01 à l'aide de PDM. Vous pouvez configurer PIX-02 sur des lignes similaires.

Ce document suppose que vous avez déjà configuré le routage.

Pour qu'une seule liaison soit active à la fois, faites en sorte que R2 annonce une métrique pire pour le réseau 192.168.1.0 ainsi que pour le réseau 172.30.0.0. Par exemple, si vous utilisez RIP pour le routage, R2 a cette configuration en dehors des autres annonces réseau :

```
R2(config)#router rip
R2(config-router)#offset-list 1 out 2 s1
R2(config-router)#offset-list 2 out 2 e0
R2(config-router)#exit
R2(config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

Procédure de configuration

Lorsque vous tapez https://<Inside_IP_Address_on_PIX> afin de lancer PDM et que vous cliquez pour la première fois sur l'onglet VPN, les informations relatives à l'assistant VPN automatique s'affichent.

Eisco PIX Device Manager 3	.0 - 172.16.5.10			<u></u>
Home Configuration	Mankaing Retresh	Save Help		CISCO SYSTEMS
■■■×××	「連連陣」。			and the second
Access Rules Transia	ation Rules VPN	Hosts/Networks	System Properties	的自己的法律
Categories	IPSec Rules	自由社会認知		
IPSec IPSec Rules	Use the Rules menu, the toolba	r, or the right mouse but	on to add, edit or delet	e rules.
	VPN Wizard		×	nnel Policy
 Policies XAuth/Mode Con Pre-shared Keys Certificate Remote Access Cisco VPN Clien L2TP/PPTP Cliei IP Pools VPN System Option:- Easy VPN Remote 	PDM features a VPN Wizard and remote access VPNs. T "Wizards" menu and select t Do not show me this me	to help you create site-to o launch this wizard, go t he menu item "VPN Wiza ssage again." OK	-site ind"	
		Apply F	Reset	
		<admin> NA (15)</admin>	😡 🏭 🔂 15	:12:07 UTC Tue Aug 23 2005

1. Sélectionnez Wizards > VPN

file Rules Search Option	s Tools Wizards Help			Providence and the second second
Home Configuration	Startup Wizard VPN Wizard th	Save He	Hp	Cisco Systems

 L'assistant VPN démarre et vous invite à indiquer le type de VPN que vous voulez configurer. Choisissez VPN site à site, sélectionnez l'interface externe comme interface sur laquelle le VPN sera activé, puis cliquez sur Suivant.

📦 VPN Wizard		X
VPN Wizard	VPN Wizard	
Branch Branch Distance Hoome	Welcome to the VPN Wizard. This wizard will help you create site-to-site VPNs which can be used to securely connect this PIX to another VPN device, or remote access VPNs which can be used to securely connect mobile users and telecommuters to this PIX.	
Corporate Network	Select the type of VPN:	
THE IN	(Site to Site VPN)	
	C Remote Access VPN	
- T- T- T-	Select the interface on which the VPN will be enabled:	
- I - L	outside	
	- Back Next > Finish Cancel Help	1

3. Entrez l'adresse IP de l'homologue, où le tunnel IPsec doit se terminer. Dans cet exemple, le tunnel se termine sur l'interface externe de PIX-02. Cliquez sur **Next** (Suivant).

📦 YPN Wizard		×
VPN Wizard	Remote Site Peer	
	Please specify the remote peer VPN device to which this PIX will connect over the VPN. The PIX and the remote peer device will authenticate each other before negotiating any IPSec tunnel to pass traffic. The authentication is done by configuring a shared password between the two peers, or certificates issued by a	
(Corporate)	Peer IP Address: 172.30.1.1	
Notwork	Authentication	
the state	Pre-shared Key	
HUIT	Reenter Key:	
THE	C Certificate. The peer's identity is its:	
	FQDN (Fully Qualified Domain Name)	
	C IP Address	The second second
	< Back Next > Finish Cancel Help	I

4. Entrez les paramètres de stratégie IKE que vous choisissez d'utiliser et cliquez sur **Suivant**.

😂 VPN Wizard		
VPN Wizard	IKE Policy	
Branch Branch Deserver ISP Homo Network	Please specify the encryption algorith Diffie-Hellman group that are used by association . Since the two parties ha to each other, make sure the configu	rm, authentication algorithm, and y the PIX when negotiating an IKE security ave to agree on the algorithms in order to talk ration of the other party is the same as the PIX.
THE ALLE	Encryption:	DES
24441	Authentication:	MD5
	DH Group:	Group 1 (768-bit)
		< Back Next > Finish Cancel Help

5. Fournissez les paramètres de chiffrement et d'authentification pour le jeu de transformation, puis cliquez sur **Suivant**.

💐 VPN Wizard	<u>×</u>
VPN Wizard	Transform Set
Branch Branch Fried Fried Fried Honro Network	Please specify the encryption and authentication algorithms used by the IPSec VPN tunnel. Since the two parties must use the same algorithms to talk to each other, make sure the configuration of the other party is the same as this PIX. This assumes the usage of ESP. If you want to use AH, you can change it later using the VPN tab from the main PDM window.
	Encryption: DES
	Authentication: MD5
	*Back Next > Finish Cancel Help

6. Sélectionnez le réseau local et les réseaux distants que vous devez protéger à l'aide d'IPsec afin de sélectionner le trafic intéressant que vous devez protéger.

💐 VPN Wizard					X
VPN Wizard	IPSec Traffic Selector				The second second
Branch Br	IPSec Traffic Sele IPSec tunnel. Pac (which you specif (which you will sp On Local Site	ctor selects the tra kets that flow betw y below) and the th ecify on the next so (protected by this F	ffic flows that are een the selected e selected hosts creen) will be pro	e going to I d hosts/net s/networks htected by t	be protected by the tworks inside the PIX at the remote site the IPSec tunnel.
Corporate	HostiNetwor	k			Selected
	(IP Address	C Name	C Group		10.1.1.0/24
1 Alle	Interface:	inside	•	reed	
HUIM	IP address:	10.1.1.0			
THE	Mask	255.255.255.0			
B		Browse			
VPN Wizard			< Back Ne	x t > Farin	sh Cancel Help
VPN Wizard	IPSec Traffic Selector	(Continue)	SECTOR SECTOR		
Branch Branch Branch Branch	Use this panel to IPSec Traffic Sele	specify the hosts/r ctor to select traffic	networks at the re flows to be prot	emote site ected by th	that are used in e IPSec tunnel.
Home		he			
(Corporate)	Host/Network				
Notwo	(IP Address	C Name	C Group		Selected:
the state	Interface:	outside	•		172.30.0.0/16
LULING	IP address:	172.30.0.0		>>	
T	Mask:	255.255.0.0	•		
-6-	第12 年至	Browse			
			< Back Ne	d> Finis	sh Cancel Help

Vérification

S'il y a du trafic intéressant à l'homologue, le tunnel est établi entre pix-01 et PIX-02.

Afin de vérifier cela, arrêtez l'interface série de R1 pour laquelle le tunnel est établi entre PIX-01 et PIX-02 via R2 lorsque le trafic intéressant existe.

Affichez l'**état du VPN** sous **Accueil** dans le PDM (mis en évidence en rouge) afin de vérifier la formation du tunnel.

G Home C	onliguration M	lonitoring Refi	resh Save	? Heb				
Device Inform	nation			Interface S	tatus			
Host Name : PIX Version: Device Type : License: Licensed F Encryption: Fallover Max Physical	PIX-01.cisco 6.3(3) PIX 515E Failover Only eatures DES Enabled	PDM Version Total Memory Total Flash: Inside Hosts IKE Peers Max	3.0(1) 64 MB 16MB Unlimited Unlimited	Interface Intr2 inside outside intr5 intr5 intr4 intr3	IP Address/Mask 0.0.0.0/0 172.16.5.99/24 150.1.1.66/24 0.0.0.0/0 0.0.0/0 0.0.0/0	Link down up up down down down	Current Kbp 0 7 0 0 0 0	
Interfaces: VPN Status	•	Interfaces:	10	Select an interface to view input and output Kbps Traffic Status				
System Res CPU 0% 17:00:31 Memory 18MB	CPU Usage (perce 04 04 16:55:41 15:4 Memory Usage (M 84 48 32 10	nn) 57:11 18:58:41 18)	17:00:11	1 0.5 18:55:41 UDP: 0 - 'outside' Inte	10.57-11 10 TCP: 0 enface Traffic Usage (Kbps)	53:41 Total	17:00:11 : 0	
17:00:31 Memory (MB) Used: 18.16	16:55:41 10: 5 Free: 45	835 Total 8	17:00: 4	15:55:41	18:67:11 16 Is 0 <mark>0</mark> 00	itput Kbps	0	

Vous pouvez également vérifier la formation des tunnels à l'aide de l'interface de ligne de commande sous Outils dans le PDM. Exécutez la commande show crypto isakmp sa pour vérifier la formation des tunnels et exécutez la commande show crypto ipsec sa pour observer le nombre de paquets encapsulés, chiffrés, etc.

L'<u>Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines</u> <u>commandes show.</u> Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

Référez-vous à <u>Cisco PIX Device Manager 3.0</u> pour plus d'informations sur la configuration du pare-feu PIX à l'aide de PDM.

Dépannage

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

Informations connexes

- Configuration d'un tunnel VPN PIX-to-PIX simple à l'aide d'IPsec
- Logiciels pare-feu Cisco PIX
- <u>Références des commandes du pare-feu Cisco Secure PIX</u>
- Demandes de commentaires (RFC)
- Support et documentation techniques Cisco Systems