Exemple de configuration d'un tunnel VPN LAN à LAN entre deux PIX à l'aide de PDM

Contenu

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

Introduction

Ce document décrit la procédure de configuration des tunnels VPN entre deux pare-feu PIX à l'aide de Cisco PIX Device Manager (PDM). PDM est un outil de configuration basé sur navigateur conçu pour vous aider à configurer, configurer et surveiller votre pare-feu PIX à l'aide d'une interface utilisateur graphique. Les pare-feux PIX sont placés à deux endroits différents.

Un tunnel est formé utilisant IPsec. 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

Il n'y a aucune exigence pour ce document.

Components Used

Les informations de ce document sont basées sur les pare-feu Cisco Secure PIX 515E avec 6.x et PDM version 3.0.

Référez-vous à <u>Configuration d'un tunnel VPN PIX à PIX simple à l'aide d'IPsec</u> pour un exemple de configuration sur la configuration d'un tunnel VPN entre deux périphériques PIX à l'aide de l'interface de ligne de commande (CLI).

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).

- 1. Un tunnel IPSec est lancé par un trafic intéressant. Le trafic est considéré comme intéressant quand il transite entre les homologues IPSec.
- 2. 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).
- 3. 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.
- 4. 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.
- 5. 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.

Procédure de configuration

Outre d'autres configurations générales sur l'interface de ligne de commande de PIX pour y

accéder via l'interface Ethernet 0, utilisez les commandes **http server enable** et **http server** <**ip_locale> <masque> <interface>** où *<ip_locale>* et *<masque>* sont l'adresse IP et le masque de la station de travail sur laquelle PDM est installé. La configuration de ce document est pour PIX-01. PIX-02 peut être configuré en utilisant les mêmes étapes avec des adresses différentes.

Procédez comme suit :

- 1. Ouvrez votre navigateur et tapez https://<Inside_IP_Address_of_PIX> pour accéder au PIX dans PDM.
- 2. Cliquez sur Configuration et accédez à l'onglet

Home Configuration	Monit	oring	@ Refresh	Save	? Help			
Access Rules Translation	in Rules		VPN	Hosts	/Networks	System Properties	- Letter	
Categories	IDS ac	Rulas						
A IPSec IPSec Rules Tunnel Policy Transform Sets	Use the	Rules menu,	the toolbar, or	the right r	nouse builton to	add, edit or delete ruk	••	Show Detail
 Policies XAuth/Mode Eonix Pre-shared Keys Eerthicate Remote Access Eisco VPN Client L2TP/PPTP Client IP Pools VPN System Options Easy VPN Remote 	#	Action	PIX Side Host/Netv	vork	Remote Side Host/Networ	k Service	Turnel Policy	
	•			Арру		Reset		•

3. Cliquez sur **Transform Sets** sous IPSec pour créer un jeu Transform.

Home Configuration	Monitoring Refresh	Save	₽ Hep			
Categories Di A IPSec - • IPSec Rules - • Turnel Policy	n Rules VPN Transform Sets Specify Transform Sets	Hα	sts/Networks Sy	stem Proportios		
Transform Sets	Name	Mode	ESP Ecouption	ESP & shortination	AH Authonia	
	ESP-DES-SHA	Tunnel	DES	SHA	None	Add
Policies Xáuth/Made Config	ESP-DES-MD5	Tunnel	DES	MD5	None	The second second
Pre-shared Keys	ESP-3DES-SHA ESP-3DES-MD5	Tunnel	3DES 3DES	SHA MD5	None	
⊕ ▼ Certificate	ESP-AES-128-SHA	Tunnel	AES-128	SHA	None	Edit
A Remote Access	ESP-AES-128-MD5	Tunnel	AES-128	MD5	None	
Cisco VPN Client	ESPAES 192-MD5	Tunnel	AES-192	MD5	None	Delete
IP Pools	ESP-AES-256-SHA	Tunnel	AES-256	SHA	None	Delete
VFN System Uptions Easy VPN Remote						
	1	Anda		eset	•	

4. Cliquez sur **Ajouter**, sélectionnez toutes les options appropriées et cliquez sur **OK** pour créer un jeu de

transformation.

Home Configuration	Monitoring Refresh	Save Het	,		CO SYST
Add Categories Categories Participation Policy Categories Participation Policy Categories Turnel Policy Categories Categories Turnel Policy Categories	Intersform Sets Transform Set Set Name MyTFSet Properties Mode ESP Encryption: ESP Authentication: AH Authentication	Hosts/Network	s System Prop	L'Authenti None None None None None None None	Add Edt Delete
	ОК	Cancel	Help	_,	

5. Cliquez sur **Clés prépartagées** sous IKE pour configurer les clés prépartagées.

Home Configuration	Monitoring Refresh	Save H	? eþ		Cisco Syst
Access Rules Translation Categories □ ▲ IPSec ↓ ◆ IPSec Rules	Pre-shared Keys Configure a pre-shared author addices a keys	Hosts/Netwo	rks) System Pro	perlies)	0)
Transform Sets KE SAuth/Mode Confin SAuth/Mode Confin Castalate Castalate	PeerIP/Name	Netmask	XAuth	Mode Config	Add Edt Delete
		Αρογ	Res	et	

6. Cliquez sur **Ajouter** pour ajouter une nouvelle clé prépartagée.

Home Configuration	Monitoring Refresh Save Help	Cisco Syst
Access Rules Translati Categories Cat	On Rules VPN Hosts/Networks System Properties Pre-shared Keys Configure a pre-shared authentication key and associate this key with an IPSec peer or security gateway address or Add Pre-shared Keys Mode Config. Peer Configure Pre-shared Keys Mode Config. Peer IP 172.30.1.1 Mode Config. Netmask: 255.255.255 Image: Configure Pre-shared Keys Configure Pre-shared Keys Mode Config. Peer IP 172.30.1.1 Netmask: 255.255.255 Image: Configure Pre-shared Keys Image: Configure Pre-shared Keys Image: Configure Pre-shared Keys Image: Pre-shared Keys I	Add Edf Ddists
1	Appl, Reset	

Cette fenêtre affiche la clé, qui est le mot de passe de l'association de tunnel. Cela doit correspondre des deux côtés du tunnel.

Cisco PIX Device Manager (3.0 - 172.16.5.101				
Home Search Options T	Monitoring Refres	h Save Hel	p		Cisco Syst
Cotegories Cotegories - IPSec - IPSec Rules - Tunnel Policy	ion Rules VPN Pre-shared Keys Configure a pre-shared authr address or host.	Hosts/Network	s System Proj this key with an IPS	perties	ay
→ IKE → Policies × XAuth/Mode Confix × Pre-shared Kays ✓ Certificate ◆ Remote Access ↓ Cisco VPN Clent ↓ 2TP/PPTP Clent ↓ 1P Pools ↓ VPN System Options ◆ Easy VPN Remote	Peer IP/Name 172.16.5.102	Netmask 255.255.255.255	XAulh disabled	Mode Config disabled	Add E dr Delete
		Арру	Ress		

7. Cliquez sur **Stratégies** sous IKE pour configurer des stratégies.

Home Configuration	Monitoring	Refre	sh Sa	ve Help			
ccess Bules Translatio	in Bules	VPN		Hosts/Networks	System Prope	ities	
Categories	Defeite						
A IPSec IPSec Rules Tunnel Policy	Configure the negotiate the	ne Internet Ser ne IKE security	curity Associa associations	ation and Key Ma and enable sec	magement Protocol po une communications	iícies. These polícies wi	1
→ IKE	Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)	Add
Consiss XAuth/Made Contx Pre-shared Keys							Edt
 B ▼ Certificate A Remote Access 							Delete
LISCO VPN Client L2TP/PPTP Client	General	Information					
	Interf	ace	KE Enabled	Identity	hostname 💌	Key Id String.	
 Easy VPN Remote 	int out:	i2 ade	faise faise	F Enabl	e NAT Traversal	NAT Keepsive	[secs]
				Set Ke	epalive & Retry value	•	
	Er	hable 0	sab/e	Keepalw	(secs)	Retry:	[secs]
				and the second		and a strange of the	Sector Sector

8. Cliquez sur **Ajouter** et renseignez les champs appropriés.

Cisco PEX Device Manager	3.0 172.16.5.10) Tools Witawis Heb	
Home Configuration	Montoring Refresh Save Help	Cisco Systems
Access Rules Transla	ion Rules VPN Hosts/Networks System Properties	San Shi ya sa
Categories ☐ ▲ IPSec IPSec Rules - ◆ Tunnel Policy	Policies Configure the Internet Security Association and Key Management Protocol policies. These policies we negotiate the IKE security associations and enable secure communications.	u
Transform Sets	I IKE Policy	Add
Auth/Mode C Fre-shared Key	Configure IKE	Edt
 ➡ ▼ Certificate ➡ Remote Access ➡ Cisco VPN Die 	Priority: 10 Authentication pre-share	Delete
L2TP/PPTP Cl IP Pools NIPN Sector Option	Encryption des D-H Group 1 -	
Easy VPN Remote	Hash md5	[secs]
	DK Cancel Help	
1	Apply Reset	
evice configuration loaded succe	essfully 🛛 🖓 🔂 🕹 00:36:40 UTC Fri.	lan 01 1993

9. Cliquez sur **OK** pour ajouter une nouvelle stratégie.

cess Rules 📄 Translati	on Rules	VPN	Sec. 18	Hosts/Networks	System Prope	enties	READERS	
Categories Categories Categories Categories Process Categories Categories Process Categories Categories Categories C	Policies Configure t negotiate t	he Internet Sec he IKE security	urity Associa associations	tion and Key Ma and enable sec	nagement Protocol p ure communications.	olicies. These policies w		
	Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)	bba [
		des	mdo		pre-share	86400	Edi	
Cisco VPN Client L2TP/PPTP Client	General Information							
IP Pools VPN System Options	Interf	ace II	KE Enabled	Identity:	hostname 💌	Key Id String	1	
 Easy VPN Remote 	ins n out	ide II2 side	false false	Enable	e NAT Traversal	NAT Keepaive	(acct)	
				T Set Ke	epalive & Retry value			
	E	nable D	natle	Kespaiw	(secs)	freby.	(secs)	

10. Sélectionnez l'interface **externe**, cliquez sur **Activer**, et dans le menu déroulant Identité, sélectionnez **adresse**.

Home Configuration	Maniford	Refrect	6	e Helo			Cisco Syste
Access Rules Translatio	n Rules	VPN		Hosts/Networks	System Prope	rties	
Categories → IPSec + ● IPSec Rules - ● Tunnel Policy	Policies Configure ti negotiate ti	ne Internet Secu ne IKE security a	nity Associations	ion and Key Ma and enable secu	nagement Protocol pr are communications.	olcies. These policies wil	
- • Transform Sets	Priority #	Enclyption	Hash	D-H Group	Authentication	Lifetime(secs)	Add
• Policies • XAuth/Mode Contig • Pre-shared Keys	10	des	md5	1	pre-share	86400	Edi
	Genera	Information					Delete
VPN System Options	Interf	aca IK de	E Enabled false	Identity:	address -	Kepid Sting:	
• Easy VEN Remote	int	f2 ide	false true	Enable	NAT Traversal	NAT Keepolive:	(eacs)
				E Set Ke	epalive & Retry value	6	
	Er	oble Dis	able	Keepaive	(scos)	Raty	lancai,
				Αρρίγ	Reset		

11. Cliquez sur **Règles IPSec** sous IPSec pour créer des règles IPsec.

Sisco PIX Device Manager 3.	0 - 172.1	6.5.101		and the second second			
File Rules Search Options To	ols Wiza Monito	rds Help) ring F	@ Ietresh Sove	? Help		Croc	O SYSTEMS
Access Rules Translation	1通 1連 n Rules	<u>()</u>	/PN Hos	ts/Networks Syst	em Properties	1	
E ▲ IPSec	IPSec	Rules		en de la companya de La companya de la comp	an a		and the second
PSec Rules Tunnel Policy Transform Sets	Use the I	Pules menu, I	he loober, or the right	mouse button to add, er	dit or delete rules.	Show [Detai
Policies XAuth/Mode Config		Action	PCK Side Host/Network	Remote Side Host/Network	Service	Tunnel Policy	
Pre-shared Keys							
4			Apoly	Res	tet		
Device configuration loaded success	stuly.		(admin)	NA (15)	😹 🔂 🖯 00	39:50 UTC Fri Jan 01 199	O

12. Renseignez les champs appropriés.

Action	State States	and the second second	Turinel Polic	y		
Select a	n action protect	-	Policy: No	ne -	· Nem.	
Firewa	TSide Host/Network			Hast/Network		
@ IPAde	hese C Name	C Gioup	IP Address	C Name	C Group	
Interface	ins de	-	Interface	Toutside		
IP addre	\$\$ 10.1.1.0		IP address:	172.16.1.0		
Misk	295.255.255.0	•	Maak	255.255.255.0		
	Browce	I.		Вгонзе		
Protoc	al and Service					
	C LOP C ICM	6 <u>6</u> 6		Pensystem	vitsfacure	
IP pro	tocol p					
Exem	al PDI side HestAnetwork fro	m address translation				
Please and	a the description below (op	tionel)				
						22.2

 Cliquez sur Nouveau dans la stratégie de tunnel. Une fenêtre Tunnel Policy s'affiche. Renseignez les champs appropriés.

Action	Section and the section of the	and the second second second	Tunnel Po	licy		
Select an acti	on: protect		Policy: N	lone	New	1
- Firewall Side	Host/Network			de Host/Network		
• IP Addr	poel Policy				vil	
Interface:	Interface:	outside	J			
IP addres	Туре:	static				
Mask:	Priority:	10				
	Transform Set:	MyTFSet		Select Multiple		
	Optional if T	vpe is dvnamic		Carlos and		
Protocc	Peer IP Address: 172.30.1.1 Advanced					1
IP Pre	Security Association Lifetime:					
IP prot	460800	0 Kilobytes				
	08	00 : 00	Hours : Minutes : S	econds		
	Enable Pe	rfect Forwarding Secr	ecy			
Exemp Please ente	Diffie-	Hellman Group	2 -			
	OK		Cancel	Help		

- 14. Cliquez sur **OK** pour afficher la règle lPsec configurée.
- 15. Cliquez sur Options des systèmes VPN et cochez la case Contourner l'accès pour tout le trafic

IPSec.



Vérification

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

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**.

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



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.

Remarque : L'interface interne du PIX ne peut pas être envoyée par ping pour la formation du tunnel, sauf si la commande <u>management-access</u> est configurée en mode de confirmation globale.

PIX-02(config)#management-access inside
PIX-02(config)#show management-access
management-access inside

Dépannage

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

Informations connexes

- Création de tunnels redondants entre pare-feu à l'aide de PDM
- <u>Références des commandes du pare-feu Cisco Secure PIX</u>
- Demandes de commentaires (RFC)
- Logiciels pare-feu Cisco PIX