Ejemplo de Configuración de Túnel VPN de LAN a LAN entre Dos PIX que Utilizan PDM

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Diagrama de la red Convenciones Antecedentes Procedimiento de Configuración Verificación Troubleshoot Información Relacionada

Introducción

Este documento describe el procedimiento para configurar túneles VPN entre dos firewalls PIX utilizando Cisco PIX Device Manager (PDM). PDM es una herramienta de configuración basada en navegador diseñada para ayudarle a configurar, configurar y monitorear su PIX Firewall con una GUI. Los firewalls PIX se colocan en dos sitios diferentes.

Un túnel se forma usando IPSec. IPSec es una combinación de estándares abiertos que proporcionan confidencialidad de datos, integridad de datos y autenticación de origen de datos entre peers IPSec.

Prerequisites

Requirements

No hay requisitos para este documento.

Componentes Utilizados

La información de este documento se basa en los firewalls Cisco Secure PIX 515E con 6.x y PDM versión 3.0.

Consulte <u>Configuración de un Túnel VPN PIX a PIX Simple Usando IPSec</u> para ver un ejemplo de configuración en la configuración de un túnel VPN entre dos dispositivos PIX usando la Interfaz de Línea de Comandos (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.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

La negociación IPSec se puede dividir en cinco pasos e incluye dos fases de intercambio de claves de Internet (IKE).

- 1. Un túnel IPSec es iniciado por un tráfico interesado. Se considera que el tráfico es interesante cuando se transmite entre los pares IPSec.
- En la Fase 1 IKE, las entidades pares IPSec negocian la política establecida de la Asociación de seguridad (SA) IKE. Una vez que se autentican los pares, se crea un túnel seguro por medio de la Asociación de Seguridad en Internet y del Protocolo de administración de clave (ISAKMP).
- 3. En la fase 2 de IKE, los pares IPSec usan el túnel autenticado y seguro para negociar las transformaciones de IPSec SA. La negociación de la política compartida determina el modo en que se establece el túnel IPSec.
- 4. Se crea el túnel IPSec y los datos se transfieren entre los pares IPSec según los parámetros IPSec configurados en los conjuntos de transformaciones de IPSec.
- 5. El túnel IPSec termina cuando los IPSec SAs son borrados o cuando caduca su vigencia. **Nota:** La negociación IPSec entre los dos PIX falla si las SA en ambas fases IKE no coinciden en los pares.

Procedimiento de Configuración

Aparte de otra configuración general en la CLI de PIX para acceder a ella a través de la interfaz Ethernet 0, utilice los comandos **http server enable** y **http server <local_ip> <mask> <interface>** donde *<local_ip>* y **<mask>** es la dirección IP y la máscara de la estación de trabajo en la que está instalado PDM. La configuración en este documento es para PIX-01. PIX-02 se puede configurar usando los mismos pasos con diferentes direcciones.

Complete estos pasos:

- 1. Abra su navegador y escriba https://<Inside_IP_Address_of_PIX> para acceder al PIX en PDM.
- 2. Haga clic en Configuration y vaya a la ficha

	Monito	anng	heresh	Save	нер			
ccess Rules Translation	Rules		VPN	Hosts	Networks	System Properties	le servere de la compañía de la comp	
Categories	IPSec Use the	Rules Rules menu,	the toolbar, o	t the right r	iouse builton to	add, edit or delete rules	Show D	etai
 Policies XAuth/Mode Contig Pre-shared Keys Certificate A Remote Access Cisco VPN Client L2TP/PPTP Client IP Pools VPN Sustem Options 	-	Action	PIX Side Host/Netv	vork	Remote Side Host/Netwo	ik Service	Turnel Policy	

3. Haga clic en **Transformar conjuntos** en IPSec para crear un conjunto de transformación.

Home Configuration	Marritoring Refrest	h Save	? Help sts/Networks ∫ Sy	stem Properties		SCO SYST
Categories	Transform Sets Specify Transform Sets					
Transform Sets	Name	Mode	ESP Ecouption	ESP Authoritication	AH Authorit	
B A IKE	ESP-DES-SHA	Tunnel	DES	SHA	None	Add
 Policies XAuth/Mode Confir 	ESP-DES-MD5	Tunnel	DES	MD5	None	-
- • Pre-shared Keys	ESP-3DES-MD5	Tunnel	3DES	MD5	None	Edi
B ▼ Certificate	ESP-AES-128-SHA	Tunnel	AES-128	SHA	None	Eur
I Cisco VPN Client	ESP-AES-192-SHA	Tunnel	AES-120	SHA	None	
L2TP/PPTP Client	ESP AES 192 MD5	Tunnel	AES-192	MD5	None	Delete
- • IP Pools	ESPAES-256-MD5	Tunnel	AES-256	MD5	None	12.7
Easy VPN Remote						
S. S. Carlos de	I Design of the second	and the second	Street States			
		Appl)	F	leset		

4. Haga clic en **Agregar**, seleccione todas las opciones apropiadas y haga clic en **Aceptar** para crear un nuevo conjunto de transformación.

Home Configuration	Montoring Refresh	Save Hel;	,		
Cocess Rules Translation Bi Categories	des VPN Inansform Sets Fansform Set Set Name MyTFSet Properties Mode © Tun ESP Encryption: ESP Authentication: AH Authentication	Hosts/Network	s System Prop	ettes	LAuthenti None None None None None None None None
	OK	Cancel Arpy	Help Reset		-

5. Haga clic en **Pre-Shared Keys** en IKE para configurar claves previamente compartidas.

Home Configuration	Monitoring Refresh	Save He	? ep		Cisco Syst
Access Rules Translato Categories D ▲ IPSec I → IPSec Rules	Pre-shared Keys Configure a pre-shared authen address or host.	Hosts/Netwo	rks) System Pro	perifies	3
Transform Sets IKE Auth/Mode Config XAuth/Mode Config Cathloade Cathloade Cathloade Cathloade Cathloade Cathloade Cathloade Cathloade VPN Clent Cathloade VPN System Options Easy VPN Remote	PeerIP/Name	Netmask	XAuth	Mode Contig	Add Edt Delete
		Apply	Rex	et	J

6. Haga clic en **Agregar** para agregar una nueva clave previamente compartida.

Home Configuration	Monitoring Refresh Save Help	
Categories	VPN Hosts/Networks System Properties Pre-shared Keys Configure a pre-shared authentication key and associate this key with an IPSec peer or security gateward address or Add Pre-shared Keys Mode Conlig. Peer Configure Pre-shared Keys Mode Conlig. Peer IP: 172.30.1.1 Mode Conlig. Netmask: 255.255.255 Image: Configure Pre-shared Keys Configure Pre-shared Keys Mode Conlig. Peer IP: 172.30.1.1 Netmask: 255.255.255 Key Image: Configure Pre-shared Keys	y Add Edf Ddets
1	Apply Reset	

Esta ventana muestra la clave, que es la contraseña para la asociación de túnel. Esto tiene que coincidir en ambos lados del túnel.

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 Keys ✓ Certificate ◆ Remote Access ↓ Cisco VPN Client ↓ 2TP/PPTP Client ↓ 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. Haga clic en **Políticas** en IKE para configurar las políticas.

開きを入るる							
ccess Rules 📄 Translati	on Rules	VP	• - E	Hosts/Networks	system Prope	rbes)	202.000
Categories	Deficies			影響的意			
A IPSec IPSec Rules Funnel Policy	Configure the	ne Internet Se ne IKE security	curity Associa y associations	ation and Key Ma s and enable sec	magement Protocol po ure communications.	licies. These policies wil	
A IKE	Priority #	Encyption	Hash	D-H Group	Authentication	Lifetime(secs)	Add
Contract Contract							Edit
 B ▼ Certificate A Remote Access 							Deleta
Cisco VPN Client L2TP/PPTP Client	General	Information				Contraction of	
	Interfe	ace	IKE Enabled	Identity	hostname 🔹	Key Id String:	and a second
Easy VPN Remote	ins int outs	de 12 ade	false false false	Enabl	e NAT Traversal	NAT Keepsive	(secs)
				Set Ke	eepalive & Retry value	•	
	Er	able) sable	Keepalw	(secs)	Bietry:	[secs]

8. Haga clic en **Agregar** y rellene los campos correspondientes.

Cisco PIX Device Manager 3	.0 172 (6.5.10)	<u>_o×</u>
Hie Poles Search Opcons II	Monitoring Refresh Save Help	Cisco Systems
Access Rules Translation	on Bules VPN Hosts/Networks System Properties	
Categories	Policies Configure the Internet Security Association and Key Management Protocol policies. These policies will negotiate the IKE security associations and enable secure communications.	
Add	IKE Policy	Add
- XAuth/Mode C Pre-shared Key	Configure IKE	Edt
B ▼ Certificate A Remote Access	Priority: 10 Authentication pre-share -	Delete
Cisco VPN Cie L2TP/PPTP Ci	Encryption des D-H Group 1 .	
 VPN System Option Easy VPN Remote 	Hash: Hash: Lifetime: 86400 seconds -	[secs]
	DK Cancel Help	[secs]
	Apply Reset	
Device configuration loaded succes	ssfuly (admin) NA (15) 🔡 🚮 🔒 00:36:40 UTC Fri Jan	01 1993

9. Haga clic en **Aceptar** para agregar una nueva política.

cess Bules] Translati	n Bules	VPN		Hosts/Networks	Sustem Prope	aties	ACC ACCESS
Categories A IPSec • IPSec Rules • Tunnel Policy	Policies Configure t negotiate t	he Internet Sec ne IKE security	urity Associations	tion and Key Ma and enable sec	nagement Protocol pure communications.	olicies. These policies wi	1
Transform Sets	Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)	
	10	des	md5		pre-share	86400	Edi
	General Information						
• IP Pools • VPN System Options	Interf	ace II	KE Enabled	Identity:	hostname 💌	Key Id String	
 Easy VPN Remote 	n	ide il2 side	false false	Enable	NAT Traversal	NAT Keepaive	(acct)
				T Set Ke	epalive & Retry value		
	E	vable 0	natle	Kespalive	(secs)	Fielty:	[secs]

10. Seleccione la interfaz **externa**, haga clic en **Enable** y, en el menú desplegable Identity, seleccione **address**.

Home Configuration	Monitoring	@	10. C				
		Refres	h Sav	? re Help			Cisco System
T T X X P	修建国			(1999) (1999)	a valerie		
Access Rules Translation Categories P A IPSec - • IPSec Rules - • Tunnel Policy	Policies Configure ti negoliate ti	ne Internet Security a	uity Associat associations	Hosts/Networks ion and Kay Ma and enable sect	agement Protocol po are communications.	rties licies These policies wil	
 Transform Sets KF 	Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)	444
	10	des	mc5		pre-share	85400	Edit
- Cisco VPN Client L2TP/PPTP Client	General	Information					
	Interf	ace IK	E Enabled	Identity:	address -	Keyld String:	
- • Easy VPN Remote	int out:	ide f2 iide	false false true	Enable	NAT Traversal	NAT Keepstve:	(esca)
				☐ Set Ke	epalive & Retry value	•	
	Er	oble Dia	able	Keepaive	[sccs]	Rety	(secs)
				Арріу	Reset		

11. Haga clic en **Reglas IPSec** en IPSec para crear reglas 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. Rellene los campos correspondientes.

Select en soin protect Frevel Side Host/Network Frevel Side	Ad	ion			Turnel Policy		A CONTRACTOR OF THE	
Frevel Side Host/Network Remote Side Host/Network © IP Address Name Sidup Interfaces made IP Address Name Sidup Interfaces made IP Address OUIS/DE IP IP address 10.1.1.0 IP address 172.16.1.0 IP Mask 255.255.255.0 IP IP Browse Browse Browse Browse Pectocial and Sarvice IP address IP address IP address Pectocial and Sarvice IP protocial Penege Sarvice Score IP protocial p IP address IP protocial <th>Selec</th> <th>t en action</th> <th>n protect</th> <th>E</th> <th>Policy: Nor</th> <th>8</th> <th>• Nem</th> <th></th>	Selec	t en action	n protect	E	Policy: Nor	8	• Nem	
© IP Address Name Group Imatase nade	Fit	wall Side I	Host/Network		Remote Side	Hast/Network		
Interface: made IP address: 10.1.1.0 Mask: 255.255.250.0 Browse: 172.10.1.0 Browse: 172.10.1.0 Protocol and Sarvee: Browse: Protocol and Sarvee: Browse: Protocol and Sarvee: Protocol Protocol Protocol IP protocol p	G IP.	Addresse	C Nano	Gioup	IP Address	C Name	Gioup	
IP address 10.1.1.0 IP address: 172.16.1.0 Mask 295.255.290.0 • Mask 255.255.0 • Browne Browne Browne Browne Browne Browne Protocol and Service C TOP LOP OkeP Protocol Protocol IP Protocol p Browne Browne Browne IP protocol p Browne Browne IP protocol p Browne Browne Browne IP protocol p Browne Browne Browne IP protocol p Browne Browne Browne IP protocol p	Inter	arse:	inade	-	Intratacia	lioutside		
Mask 225.255.295.0 Browne Browne Protocol and Stavies Protocol and Stavies Protocol p Protocol p Protocol p Protocol	IP ec	dress	10.1.1.0	1	IP address:	172.16.1.0	10	
Browne Browne Protocial and Starvice Procession TOP LOP O MP IP Protocol P	Mush		295.255.251.0		Minde	255.255.255.0		le:
Protocol and Sarves			Browse	1		Вгонзе		
 Example POL side Post/Indexork from address translation Please antist the discoption balance (optione); 		P C Protocol protocol		р (° р 		Penegsber	etes forenza.	
	₩ Ex	angt POCs attes the d	ade Prest-Andwork for Vezenation bakes (op	m address translation				
N S	Contraction of the local division of the loc	1996.05	and the second second second	and the state of the			0.000	

 Haga clic en Nuevo en la Política de Túnel. Aparece una ventana Tunnel Policy . Rellene los campos correspondientes.

Action			Tunnel Policy				
Select an acti	on: protect		Policy: None	New			
Firewall Side	e Host/Network	1000	Remote Side Host/Ne	twork			
• IP Addr Tu	nnel Policy	CE STATE		×			
Interface:	Interface:	outside	J				
IP addres	Туре:	static	J				
Mask:	Priority:	10					
	Transform Set:	MyTFSet	- Select Mul	iple			
	Optional if Ty	ype is dynamic					
Protocc	Peer IP Addr	ess: 172.30.1.	1 Advanc	ed			
IP Prc	Security Association Lifetime:						
IP prot	ot 4608000 Kilobytes						
	08 :	00 : 00	Hours : Minutes : Seconds				
	Enable Pe	afect Forwarding Secr	ecy				
Exemp Please ente	Diffie	Hellman Group	2.				
	04		Cancel	Help			

- 14. Haga clic en Aceptar para ver la regla IPsec configurada.
- 15. Haga clic en Opciones de sistemas VPN y marque Omitir verificación de acceso para todo el tráfico

IPSec.



Verificación

Si hay tráfico interesante al par, el túnel se establece entre PIX-01 y PIX-02.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Vea el estado de VPN en Inicio en el PDM (resaltado en rojo) para verificar la formación del túnel.

lome C	onliguration M	onitoring Refi	resh Save	? Heb		addina at
Device Infor	mation	and Alexandra Starting Internet College Starting	Constant and the	Interface S	tatus	
Host Name : PD(Version: Device Type : License: Licensed I Encryption: Failover Max Physical	PIX-01.cisco 6.3(3) PIX 515E Failover Only eatures DES Enabled 6	PDM Version : Total Memory: Total Flash: Inside Hosts: IKE Peers: Max	3.0(1) 64 MB 16MB Unlimited Unlimited	Interface Intf2 Inside outside Intf5 Intf4 Intf3	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 0.0.0/0	Link Current Kap down 0 up 7 up 0 down 0 down 0 down 0
Interfaces:		Interfaces: Select an interface to view input and output Kbps				utput Kbps
0% CPU 0% 17:00:31 Memory 18MB	CPU Usage (perce 04 32 15:55:41 18:5 Memory Usage (M 64 48 16 16 16 16 16 16 16 16 16 16	nī) 57:11 16:58:41 8) 57:11 10:58:41	17:00:11	0.5 18:55:41 UDP: 0 'outside' Inte 0.5 18:55:41	10.57-11 10 TCP: 0 enface Traffic Usage (Kbps) 10:57:11 10	58:41 17:00:11 Total: 0
Memory (MB) Used: 18.16))5. Free: 45/	835 Total: 8	4	Input Kbp	s 0 <mark>=</mark> Ou	tput Kbps D

También puede verificar la formación de túneles mediante CLI en Herramientas en el PDM. Ejecute el comando **show crypto isakmp sa** para verificar la formación de túneles y ejecute el comando **show crypto ipsec sa** para observar el número de paquetes encapsulados, cifrados, etc.

Nota: La interfaz interna del PIX no se puede hacer ping para la formación del túnel a menos que el comando <u>management-access</u> se configure en el modo de confirmación global.

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

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- <u>Creación de túneles redundantes entre firewalls mediante PDM</u>
- Referencias de Comandos de Cisco Secure PIX Firewall

- <u>Solicitudes de Comentarios (RFC)</u>
 <u>Cisco PIX Firewall Software</u>