Esempio di tunnel VPN da LAN a LAN tra due PIX con configurazione PDM

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Esempio di rete Convenzioni Premesse Procedura di configurazione Verifica Risoluzione dei problemi Informazioni correlate

Introduzione

Questo documento descrive la procedura per configurare i tunnel VPN tra due firewall PIX con Cisco PIX Device Manager (PDM). PDM è uno strumento di configurazione basato su browser progettato per semplificare la configurazione, la configurazione e il monitoraggio del firewall PIX tramite un'interfaccia utente grafica. I firewall PIX si trovano in due siti diversi.

Tunnel formato tramite IPsec. IPsec è una combinazione di standard aperti che forniscono riservatezza, integrità e autenticazione dell'origine dei dati tra peer IPsec.

Prerequisiti

Requisiti

Nessun requisito previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sui firewall Cisco Secure PIX 515E con 6.x e PDM versione 3.0.

Per un esempio sulla configurazione di un tunnel VPN tra due dispositivi PIX tramite l'interfaccia della riga di comando (CLI), fare riferimento a <u>Configurazione di un tunnel VPN da PIX a PIX</u> <u>semplice con IPsec</u>.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni</u> <u>dei documenti.</u>

Premesse

La negoziazione IPSec può essere suddivisa in cinque fasi e include due fasi IKE (Internet Key Exchange).

- 1. Un tunnel IPsec viene avviato da traffico interessante. Il traffico è considerato interessante quando avviene tra peer IPsec.
- 2. Nella fase 1 di IKE, i peer IPsec negoziano il criterio SA (Security Association) IKE stabilito. Dopo l'autenticazione dei peer, viene creato un tunnel protetto utilizzando Internet Security Association and Key Management Protocol (ISAKMP).
- 3. In IKE fase 2, i peer IPsec utilizzano il tunnel autenticato e sicuro per negoziare le trasformazioni di associazione di sicurezza IPsec. La negoziazione del criterio condiviso determina la modalità di definizione del tunnel IPSec.
- 4. Il tunnel IPSec viene creato e i dati vengono trasferiti tra i peer IPSec in base ai parametri IPSec configurati nei set di trasformazioni IPSec.
- 5. Il tunnel IPsec termina quando le associazioni di protezione IPsec vengono eliminate o quando scade la loro durata. **Nota:** la negoziazione IPSec tra i due PIX non ha esito positivo se le associazioni di protezione su entrambe le fasi IKE non corrispondono sui peer.

Procedura di configurazione

A parte altre configurazioni generali nella CLI di PIX per accedere tramite l'interfaccia Ethernet 0, usare i comandi **http server enable** e **http server <ip_locale> <mask> <interface>** dove *<ip_locale>* e *<mask>* è l'indirizzo IP e la maschera della workstation su cui è installato PDM. La configurazione di questo documento è per PIX-01. PIX-02 può essere configurato usando gli stessi passaggi con indirizzi diversi.

Attenersi alla seguente procedura:

- 1. Aprire il browser e digitare https://<lnside_IP_Address_of_PIX> per accedere al PIX in PDM.
- 2. Fare clic su Configuration (Configurazione) e andare alla scheda



3. Fare clic su **Set di trasformazioni** in IPSec per creare un set di trasformazioni.

Home Configuration	Morritoring Refrest	Save	? Help			SEO SYSTE
Access Rules Translation Categories D: ▲ IPSec H ● IPSec Rules	n Rules VPN Transform Sets Specify Transform Sets	Ho	sts/Networks Sy	stem Properties		
Transform Sets	Name	Mode	ESP Ecouption	ESP Authoritination	AH Authonia	
	ESP-DES-SHA	Tunnel	DES	SHA	None	Add
 Policies Xáuth/Made Confi 	ESP DES MD5	Tunnel	DES	MD5	Non	1000 C
- 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	Non	
Cisco VPN Client	ESP AES 192 MD5	Tunnel	AES-192	MD5	None	Delete
• IP Pools	ESP-AES-256-SHA	Tunnel	AES-256	SHA	None	
 The system options Easy VPN Remote 						
	1	- Andi		eset		

4. Fare clic su **Aggiungi**, selezionare tutte le opzioni appropriate e fare clic su **OK** per creare un nuovo set di

trasformazione.

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. Fare clic su **Chiavi già condivise** in IKE per configurare le chiavi già condivise.

Home Configuration	Monitoring Refresh	Save H	? eþ		Cisco Syst
Access Rules Translation Categories □ ▲ IPSec ↓ ◆ IPSec Rules	Pre-shared Keys Configure a pre-shared author address 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. Fare clic su **Add** (Aggiungi) per aggiungere una nuova chiave già condivisa.

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	

In questa finestra viene visualizzata la chiave, ovvero la password per l'associazione del tunnel. Deve essere uguale su entrambi i lati del tunnel.

Cisco PIX Device Manager :	3.0 - 172.16.5.101				
Home Search options T	Monitoring Refres	sh Save He	P		Cisco Srsti
Access Rules Translati Categories Categor	on Rules VPN Pre-shared Keys Configure a pre-shared auth address or host.	Hosts/Network	s System Prop e this key with an IPS	verties) ec peer or security galew	ay
	Peer IP/Name 172.16.5.102	Netmask 255.255.255.255	XAuh dipabled	Mode Config disabled	Add Ectr Delete
		Δρρίγ	Rese	·	

7. Fare clic su **Criteri** in IKE per configurare i criteri.

	1 (1 1 1 1	14					
ccess Rules 🔰 Translatio	n Rules	VPN		Hosts/Networks	System Prope	ntes)	
Categories	Defeire						
A IPSec IPSec Rules Tunnel Policy Tunnel Policy	Configure the negotiate the	ne Internet Sec ne IKE security	unly Associa associations	ation and Key Ma and enable secu	nagement Protocol po ure communications.	olicies. These policies wil	1
	Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)	Add
Xouth/Mode Conlig Xouth/Mode Conlig Pre-shared Keys Certificate A Remote Access							Edt
							Deleta
Cisco VPN Client L2TP/PPTP Client	General	Information				Contraction of the	
	Interf	ace II	KE Enabled	Identity	hostname 🔸	Key Id String:	
Easy VPN Remote	int out:	ide 12 side	false false false	Enabk	e NAT Traversal	NAT Keepsive	(secs)
				Set Ke	epalive & Reity value		
	Er	nable D	sable	Keepalw	(secs)	Fietry:	[secs]
		<u>1. 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 - 200 -</u>	630 N	A CONTRACTOR	NE CARE AND A		

8. Fare clic su **Add** (Aggiungi) e compilare i campi appropriati.

Cisco PIX Device Manager	3.0 172.16.5.101	<u>×</u>
Home Configuration	Monitoring Refresh Save Help	Cisco Systems
Access Rules Translat	ion Rules 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 Kes	Configure IKE	Edt
⊕ ▼ Certificate ⊕ ▲ Remote Access	Priority: 10 Authentication: pre-share	Lelete
- • L2TP/PPTP CI	Encryption des DH Group 1	
VPN System Option Easy VPN Remote	Hash Hash Lifetime 86400 seconds	(secs)
	DK Cancel Hep	[secc]
	Apply Reset	
Device configuration loaded succe	essfully 🛛 🕹 🖓 🔂 🕹 00:36:40 UTC Fri Jan	01 1993

9. Fare clic su **OK** per aggiungere un nuovo criterio.

ccess Rules Translati	on Rules	VPN		Hosts/Networks	System Prope	nties	NGA UNSA
Categories A IPSec • IPSec Rules • Tunnel Policy	Policies Configure t negotiate t	he Internet Sec he IKE security	urity Associa associations	tion and Key Ma and enable sec	nagement Protocol p are communications.	olicies. These policies wi	1
Transform Sets	Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)	
	10	des	chm		pre-share	86400	Edi
	Genera	Information				3.2.2.64 7.4	
 VPN System Options 	Inter	ace I	KE Enabled	Identity:	hostname 💌	Key Id String	
 Easy VPN Remote 	in: n out	ide II2 side	false false	Enable	NAT Traversal	NAT Keepaive	(acct)
				T Set Ke	epalive & Retry value		
	E	nable 0	natle	Kespalive	([sens])	Fieldy.	(secs)

10. Selezionare l'interfaccia **esterna**, fare clic su **Attiva**, quindi dal menu a discesa Identità selezionare **indirizzo**.

Hotes Search Options To Home Configuration	Monitoring	Refres	h San) ? re Help			Cisco Syste
	1	i (\$1		- 14 M (2)			
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	nty Associations	tion and Key Ma and enable sec	nagement Protocol p ure communications.	olicies. These policies wil	
i ··· ● Transform Sets ∃ ▲ IKE	Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)	Add
• Folicies • XAuth/Mode Config • Pre-shared Keys	10	des	md5		pre-share	85400	Edi
 E T Certificate A Remote Access 							Delete
- Cisco VPN Client U2TP/PPTP Client	Genera	Unformation			Sec. Sec.	- Links and a	Contraction of the
- • IP Pools	Interf	ace IK	E Enabled	Identity:	address -	Keyld Sting	- ter fan i fer
Easy VPN Remote	ins	ide f2	faise faise		Section of the	- 10 C	
	out	ide	true	Enable	NAT Traversal	NAT Ksepstve:	(eecs)
				E Set Ke	epalive & Reby value	•	
	Er	oble Die	able	Keepaiw	[sccs]	Rety	(socal
		S.Sec.s					
	le Case					State St	14 A. P
				Apply	Beset		

11. Fare clic su **Regole IPSec** in IPSec per creare le regole IPSec.

Sisco PIX Device Manager 3.0) - 172.1	6.5.101	Chel - Coldina	North Contraction of the	Renderatio		
File Rules Search Options Too Home Configuration	Monito	rds Help) ring R	@ etresh Save	? Hep		Cise	O SYSTEMS
Access Rules Translation Categories Categ	IPSes Use the l	Rules Rules menu, If Action	PN Hast re toolbar, or the right PC: Side Host/Network	s/Networks Syst mouse button to add, er Remote Side Host/Network	em Properties dit or delete rules Service	Show E	etal
• L2TP/PPTP Client • IP Pools • VPN System Options • Easy VPN Remote	-		Apoly	Res	ret		
Device configuration loaded success	iuly.		(admin)	NA (15)	😹 🔂 🔂 00:	38:50 UTC Fri Jan 01 199	0

12. Compilare i campi appropriati.

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 and Sarvee: Protocol Protocol P Protocol P Protocol P Protocol P Protocol P P Exampl FN add Foot/Indexet from address translation Peace and a to decorption below (optione)	G IP.	Addresse	C Nano	C Group	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 Proto	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	anpl PC: s	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	

13. Fare clic su **Nuovo** in Criteri tunnel. Viene visualizzata la finestra Criteri tunnel. Compilare i campi appropriati.

Select an acti	on: protect	•	Tunnel Polic Policy	y	• New
Jelect an del			- Cologe - Cologe		
Firewall Side	e Host/Network		Remote Side	Host/Network	
• IP Addr Tu	nnel Policy				×
Interface:	Interface:	outside	J		
IP addres	Туре:	static			
Mask:	Priority:	10			
	Transform Set:	MyTFSet	- s	elect Multiple	
	Online of X T			Constant of	
-Protocc	Uptional II I	ype is dynamic			
C TCP	Peer IP Addr	ess: [172.30.1.	1	Advanced	
IP Pro	Security Ass	ociation Lifetime:			
IP prot	460800	0 Kilobytes			
	08	00 : 00	Hours : Minutes : Sec	onds	
	Enable P	erfect Forwarding Secr	ecy		
Exemp	Diffie	Helman Group	2.		
riease ente					
			Cancel	Help	1
	the second s			The second second second second	CONTRACTOR OF A DESCRIPTION OF A DESCRIP

- 14. Fare clic su **OK** per visualizzare la regola IPSec configurata.
- 15. Fare clic su VPN Systems Options (Opzioni di sistema VPN) e selezionare Bypass access check (Ignora controllo accesso) per tutto il traffico IPSec.



Verifica

Se è presente traffico interessante verso il peer, il tunnel viene stabilito tra PIX-01 e PIX-02.

Lo <u>strumento Output Interpreter</u> (solo utenti <u>registrati</u>) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Visualizzare lo stato VPN in Home (Pagina iniziale) nel PDM (evidenziato in rosso) per verificare la formazione del tunnel.



Èinoltre possibile verificare la formazione dei tunnel utilizzando CLI in Strumenti in PDM. Utilizzare il comando **show crypto isakmp sa** per controllare la formazione dei tunnel e il comando **show crypto ipsec sa** per osservare il numero di pacchetti incapsulati, crittografati e così via.

Nota: non è possibile eseguire il ping dell'interfaccia interna del PIX per la formazione del tunnel a meno che il comando <u>management-access</u> non sia configurato in modalità di conferma globale.

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

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

<u>Creazione di tunnel ridondanti tra firewall tramite PDM</u>

- <u>Riferimenti per i comandi di Cisco Secure PIX Firewall</u>
 <u>RFC (Requests for Comments)</u>
- Software Cisco PIX Firewall