Creazione di tunnel ridondanti tra firewall tramite PDM

Sommario

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

Introduzione

Questo documento descrive la procedura da utilizzare per configurare i tunnel tra due firewall PIX con Cisco PIX Device Manager (PDM). I firewall PIX si trovano in due siti diversi. In caso di mancato raggiungimento del percorso principale, è consigliabile avviare il tunnel tramite un collegamento ridondante. IPsec è una combinazione di standard aperti che forniscono riservatezza, integrità e autenticazione dell'origine dei dati tra peer IPsec.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

• Cisco Secure PIX 515E Firewall con 6.x e PDM versione 3.0

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).

Un tunnel IPsec viene avviato da traffico interessante. Il traffico è considerato interessante quando avviene tra peer IPsec.

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).

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.

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.

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.

Configurazione

Questa procedura guida l'utente nella configurazione di uno dei firewall PIX per attivare il tunnel quando esiste traffico interessante. Questa configurazione consente anche di stabilire il tunnel

attraverso il collegamento di backup attraverso il router 2 (R2), quando non vi è connettività tra PIX-01 e PIX-02 attraverso il router 1 (R1). Questo documento mostra la configurazione di PIX-01 con PDM. È possibile configurare PIX-02 su linee simili.

in questo documento si presume che il routing sia già stato configurato.

Affinché sia attivo un solo collegamento alla volta, rendere R2 pubblicizza una metrica peggiore per la rete 192.168.1.0 e per la rete 172.30.0.0. Ad esempio, se si utilizza RIP per il routing, R2 ha questa configurazione a parte altri annunci di rete:

```
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
```

Procedura di configurazione

Quando si digita https://<Inside_IP_Address_on_PIX> per avviare PDM e si fa clic per la prima volta sulla scheda VPN, vengono visualizzate informazioni sulla Creazione guidata VPN automatica.

Cisco PIX Device Manager 3 File Rules Scarch Options 1	.0 - 172.16.5.10 ools Wizards Halp			-DX
Home Configuration	Monitoring Refiresh	Save Help		Cisco Systems
Access Rules Transl	ation Rules VPN	Hosts/Networks	System Properties	
Categories	IPSec Rules Use the Rules menu, the toolb VPN Wizard PDM features a VPN Wizard and remote access VPNs. "Wizards" menu and select	ar, or the right mouse but I to help you create site to To launch this wizard, go t the menu item "VPN Wiza essage again." OK	ton to add, edit or delete Solution to add, edit or delete Solut	rules. Show Detail
	1		CC / Standard and Ale Standard Standards	•
		Арру	Reset	
		<admin> NA (15)</admin>	🕞 🏭 🔂 15:1	2:07 UTC Tue Aug 23 2005

1. Selezionare Procedure guidate > Creazione guidata

File Rules Search Options Tools Wizard	s Help		
Home Configuration	up Wizard Mizard th Save	? Help	Cisco Systems
Device Information		Interface Status	

 Verrà avviata la Creazione guidata VPN e verrà richiesto il tipo di VPN che si desidera configurare. Scegliere VPN da sito a sito, selezionare l'interfaccia esterna come interfaccia su cui verrà abilitata la VPN e fare clic su Avanti.

📦 VPN Wizard	×				
VPN Wizard	VPN Wizard				
Branch Distance ISP Honro	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				
	Select the interface on which the VPN will be enabled:				
1 III	outside 💌				
	*Back Next > Finish Cancel Help				

3. Immettere l'indirizzo IP del peer in cui deve terminare il tunnel IPsec. In questo esempio, il tunnel termina sull'interfaccia esterna del PIX-02. Fare clic su **Avanti**.

📦 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					
Natwork	Authentication					
1 Alexandre	Pre-shared Key *****					
	Reenter Key:					
- There we have	Certificate. The peer's identity is its:					
- I - I	FODN (Fully Qualified Domain Name)					
	IP Address					
	< Back Next > Finish Cancel Help					

4. Immettere i parametri dei criteri IKE che si sceglie di utilizzare e fare clic su Avanti.

😝 VPN Wizard		×
VPN Wizard	IKE Policy	
Branch Branch I I I I I I I I I I I I I I I I I I I	Please specify the encryption algorithm, authentication algorithm, and Diffie-Hellman group that are used by the PIX when negotiating an IKE security association . Since the two parties have to agree on the algorithms in order to talk to each other, make sure the configuration of the other party is the same as the PIX.	
THE ALLE	Encryption: DES	
THUM I	Authentication: MD5	
TTT	DH Group: Group 1 (768-bit)	
		A CALL OF A CALL
	Back Next > Finish Cancel Help	L

5. Specificare i parametri di crittografia e autenticazione per il set di trasformazioni e fare clic su Avanti.

😫 VPN Wizard	×
VPN Wizard	Transform Set
Branch Branch III IIII IIIII Horne Corporate 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 * Emish Cancel Help

6. Selezionare la rete locale e le reti remote da proteggere utilizzando IPSec per selezionare il traffico interessante da proteggere.

💐 VPN Wizard					X
VPN Wizard	IPSec Traffic Selector				The second second
Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch Branch 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	•	reend	
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	On Remote Sit	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-		Browse			
			< Back Ne	d> Finis	sh Cancel Help

Verifica

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

Per verificare questa condizione, chiudere l'interfaccia seriale R1 per la quale viene stabilito il tunnel tra PIX-01 e PIX-02 tramite R2 quando esiste il traffico interessato.

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

G Iome C	onliguration M	onitoring Ref	resh Save	? Help			
Device Inform	nation	and Aller and Aller and An ann an Anglia an Aller		Interface S	tatus		
Host Name : PIX Version: Device Type : License: Encryption: Failover 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 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 0.0.0.0/0	Link down up up down down down	Current Kap 0 7 0 0 0 0
Interfaces: VPN Status		Interfaces:		Select an interface to view input and output Kbps Traffic Status			
System Res CPU 0% 17:00:01 Memory 18MB	CPU Usage (perce 04 04 32 18:55:41 15:5 Memory Usage (M 64 40 32 10	n1) 57:11 18:58:41 B)	17:00:11	1 0.5 18:55:41 UDP: 0 	10.57-11 10 TCP: 0 erface Traffic Usage (Kbps)	53.41 Tota	17:00:11 1: 0
17:00:01 Memory (MB) Used: 18:16	18:55:41 10: 5 Free: 45.	97:11 10:58:41 835 Total: 8	4	15,55,41	18597:11 18 ns 0 <mark>0</mark> 00	itput Kbps	17:00:11

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.

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**.

Fare riferimento a <u>Cisco PIX Device Manager 3.0</u> per ulteriori informazioni sulla configurazione del firewall PIX con PDM.

Risoluzione dei problemi

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

Informazioni correlate

- Configurazione di un tunnel VPN da PIX a PIX semplice con IPsec
- Software Cisco PIX Firewall
- <u>Riferimenti per i comandi di Cisco Secure PIX Firewall</u>
- <u>RFC (Requests for Comments)</u>
- Documentazione e supporto tecnico Cisco Systems