Túnel VPN de LAN para LAN entre dois PIXs usando o exemplo de configuração de PDM

Contents

Introduction Prerequisites Requirements Componentes Utilizados Diagrama de Rede Conventions Informações de Apoio Procedimento de configuração Verificar Troubleshoot Informações Relacionadas

Introduction

Este documento descreve o procedimento para configurar túneis VPN entre dois PIX Firewalls usando o Cisco PIX Device Manager (PDM). O PDM é uma ferramenta de configuração baseada em navegador projetada para ajudá-lo a configurar, configurar e monitorar seu PIX Firewall com uma GUI. Os PIX Firewalls são colocados em dois locais diferentes.

Um túnel é formado usando IPsec. O IPsec é uma combinação de padrões abertos que fornece confidencialidade de dados, integridade de dados e autenticação de origem de dados entre pares IPsec.

Prerequisites

Requirements

Não há requisitos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nos Cisco Secure PIX 515E Firewalls com 6.x e PDM versão 3.0.

Consulte <u>Configurando um Túnel VPN PIX para PIX Simples Usando IPsec</u> para obter um exemplo de configuração na configuração de um túnel VPN entre dois dispositivos PIX usando a CLI (Command Line Interface, Interface de Linha de Comando).

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 Rede

Este documento utiliza a seguinte configuração de rede:



Conventions

Consulte as <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

Informações de Apoio

A negociação de IPsec pode ser dividida em cinco etapas e inclui duas fases de Internet Key Exchange (IKE).

- 1. Um túnel de IPSec é iniciado por um tráfego interessante. O tráfego é considerado interessante quando ele é transmitido entre os peers IPSec.
- Na Fase 1 IKE, os correspondentes IPSec negociam a política de Associação de segurança (SA) IKE estabelecida. Quando os peers são autenticados, um túnel seguro é criado com o uso do Internet Security Association and Key Management Protocol (ISAKMP).
- Em IKE Phase 2, os correspondentes de IPSec utilizam o túnel autenticado e seguro para negociar transformações de IPSec AS. A negociação da política compartilhada determina como o túnel de IPSec é estabelecido.
- 4. O túnel de IPSec é criado e os dados são transferidos entre peers de IPSec com base nos parâmetros de IPSec configurados em grupos de transformação do IPSec.
- 5. O túnel de IPSec finaliza quando os IPSec SAs são excluídos ou quando sua vida útil expira. **Observação:** a negociação de IPsec entre os dois PIXes falhará se os SAs em ambas as fases de IKE não coincidirem com os correspondentes.

Procedimento de configuração

Além de outras configurações gerais na CLI do PIX para acessá-lo através da interface Ethernet

0, use os comandos **http server enable** e **http server <local_ip> <mask> <interface>** onde *<local_ip>* e *<mask>* são o endereço IP e a máscara da estação de trabalho na qual o PDM está instalado. A configuração neste documento é para PIX-01. O PIX-02 pode ser configurado usando as mesmas etapas com endereços diferentes.

Conclua estes passos:

- 1. Abra o navegador e digite https://<Inside_IP_Address_of_PIX> para acessar o PIX no PDM.
- 2. Clique em Configuração e vá para a guia



3. Clique em **Transform Sets** em IPSec para criar um conjunto de transformações.

Home Configuration	Monitoring Refrect	Save	? Help	vstem Properties	CI 	SEO SYST
Categories	Transform Sets Specify Transform Sets					
Transform Sets	Name	Mode	ESP Execution	ESP Authentication	AH Authenti	
	ESP-DES-SHA	Tunnel	DES	SHA	None	Add
- • XAuth/Mode Confir	ESP DES MD5	Tunnel	DES	MD5	Non	1000
Pre-shared Keys	ESP-3DES-MD5	Tunnel	3DES	MD5	None	5.0
E Certificate	ESP-AES-128-SHA	Tunnel	AES-128	SHA	None	Edi
A Remote Access	ESP-AES-128-MD5 ESP-AES-192-SHA	Tunnel	AES-128 AES-192	MD5 SHA	Non	
UISCO VPN Lient	ESP AES 192 MD5	Tunnel	AES-192	MD5	None	Delete
- • IP Pools	ESP-AES-256-SHA	Tunnel	AES-256	SHA	None	
• • Easy VPN Remote						
	<u>ا</u>	Appl	F	leset		

4. Clique em **Adicionar**, selecione todas as opções apropriadas e clique em **OK** para criar um novo conjunto de transformações.

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. Clique em **Pre-Shared Keys** em IKE para configurar chaves précompartilhadas.

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. Clique em **Adicionar** para adicionar uma nova chave précompartilhada.

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 janela mostra a chave, que é a senha para a associação do túnel. Isso tem que coincidir em ambos os lados do 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 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. Clique em **Policies** em IKE para configurar políticas.

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
Poictes Xauth/Mode Contig Pre-shared Keys Pre-shared Keys Pre-shared Keys A renote Access							Edt
							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. Clique em **Adicionar** e preencha os campos apropriados.

Cisco PIX Device Manager :	3.0 - 172.16.5.101	-o×
Home Configuration	Monitoring Refresh Save Help	CISCO SYSTEMS
Access Rules Translati	on 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
-	Configure IKE	Edt
B ▼ Certificate A Remote Access	Priority: 10 Authentication pre-share •	Delete
Cisco VPN Cile L2TP/PPTP Ci LP Pode	Encryption des D-H Group: 1 .	
VPN System Option Easy VPN Remote	Hashr Hashr Lifetime: 86400 seconds -	[secs]
	DK Cancel Help	[secs]
	Apoly Reset	
Device configuration loaded succe	ssfuly (admin) NA (15) 🔡 🚮 🔒 00:36:40 UTC Fri Jan	01 1993

9. Clique em **OK** para adicionar uma nova política.

cess Rules 📄 Translati	on Rules	VPN	Sec. 18	Hosts/Networks	System Prope	enties	READERS
Categories A IPSec IPSec Rules Tunnel Policy	Policies Configure to negotiate ti	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 [
Poicies XAuth/Mode Conti, Auth/Mode Conti, Pre-shared Keys Certificate Certificate Certificate Cisco VPN Client Cisco VPN Client		des	mdo		pre-share	86400	Edi
	Genera	Information			24 2428 25 22		
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. Selecione a interface **externa**, clique em **Enable** e, no menu suspenso Identity, selecione **address**.

Hotes Search Options To Home Configuration	Monitoring	Refres	h San) ? re Help			Cisco Syste
	1	i (\$1		- 14 M (1)			
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	Contractor (
- • IP Pools	Interf	ace IK	E Enabled	Identity:	address -	Keyld Sting	- ter fan er er
Easy VPN Remote	ins	ide f2	faise faise		Section of the	- 10 C	
	out	ide	true	Enable	NAT Traversal	NAT Ksepstve:	(6905)
				E Set Ke	epalive & Reby value	•	
	Er	oble Dia	able	Keepaiw	[sccs]	Rety	(socal
		S.Sela					
	le Case					State St	14 A. P
				Apply	Beset		

11. Clique em **IPSec Rules** em IPSec para criar regras IPsec.

Sisco PIX Device Manager 3.	0 - 172.1	6.5.101	Rive cident	and the second second			
File Rules Search Options To	Monito	rds Help) ring f	@ 🔒 Retresh Save	? Hep		Cese	CO SYSTEMS
Access Rules Translation Categories Cate	IPSec Use the I	Rules Rules menu, Action	VPN Has the toober, or the righ PDK Side Host/Network	ts/Networks Syst t mouse button to add, e Remote Side Host/Network	em Properties dit or delete rules Service	Show Turnel Policy	Detal
Easy VPN Remote	-1		Aprily	Re	set		
Device configuration loaded success	fully		kadmin>	NA (15)	😹 🔂 🔂 00	38:50 UTC Fri Jan 01 19	93

12. Preencha os campos apropriados.

	Action			Turnel Policy		1.	
	Select an actio	n protect		Policy: Nor	8	. Neн	
	Firewall Side	Host/Network		Remote Side	Hast/Network		
	@ IP Address	C Nano	C Group	IPAddress	C Name	C Gio.p	
	Inbularse.	inside	-	Interface	Joutside		
	IP address	10.1.1.0	2.3	IP address:	172.16.1.0		
	Misk	295.255.291.0		Mack	255.255.255.0	•	eal
		Browse			Browse		
	C TCP C	цор стом	e ee		Pensysion	iestern.	
	IP protocol	P					
	Exampl PN	side hest/hetwork fro	m address translation				
	riede antei frei	search de calinadore (la ba				States (18)	
							223
_							2.50 6 60

 Clique em New na Tunnel Policy (Política de túnel). Uma janela Política de túnel é exibida. Preencha os campos apropriados.

Action	Contraction of the local distance		Tunnel Poli	cy	
Select an acti	on: protect		Policy. No	one	New
	Contraction of the				
- Firewall Side	Host/Network		Remote Sic	le Host/Network	18-28-28-28-38-
(• IP Addr Tu	nnel Policy				×
Interface:	Interface:	outside	J		
IP addres	Tupe	static	-		
	, ype	Sector and			
Mask:	Priority:	10			
	Transform Set:	MyTFSet	•	Select Multiple	
				and the second second	
Durtras	Uptional # 1	ype is dynamic			
O TOP	Peer IP Addr	ess. 172.30.1.1		Advanced	
IP Pro	Security Asso	ciation Lifetime:			F
IP prot	460800	0 Kilobytes			
		[00 [00			
	Ins.		Hours : Minutes : Se	conds	
	Enable Pe	erfect Forwarding Secr	всу		
 Exemp 	Diffie	Helman Group	2 -		
Hease ente					
1					Parente (
	UK		Lancel	Help	

- 14. Clique em **OK** para ver a regra IPsec configurada.
- 15. Clique em Opções de sistemas VPN e marque Ignorar verificação de acesso para todo o tráfego

IPSec.



Verificar

Se houver tráfego interessante para o peer, o túnel é estabelecido entre PIX-01 e PIX-02.

A <u>Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados</u> <u>comandos show.</u> Use a OIT para exibir uma análise da saída do comando show.

Visualize o Status da VPN em Início no PDM (destacado em vermelho) para verificar a formação do túnel.



Você também pode verificar a formação de túneis usando CLI em Ferramentas no PDM. Emita o comando **show crypto isakmp sa** para verificar a formação de túneis e emita o comando **show crypto ipsec sa** para observar o número de pacotes encapsulados, criptografados e assim por diante.

Observação: a interface interna do PIX não pode receber ping para a formação do túnel, a menos que o comando management-access esteja configurado no modo de confirmação global.

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

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Criação de túnel redundante entre firewalls usando PDM
- <u>Referências do comando Cisco Secure PIX Firewall</u>
- Solicitações de Comentários (RFCs)
- <u>Cisco PIX Firewall Software</u>