Criação de túnel redundante entre firewalls usando PDM

Contents

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

Introduction

Este documento descreve o procedimento usado para configurar túneis entre dois firewalls PIX usando o Cisco PIX Device Manager (PDM). Os PIX Firewalls são colocados em dois locais diferentes. Em caso de falha ao alcançar o caminho principal, é desejável lançar o túnel através de um link redundante. 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 existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

• Firewalls Cisco Secure PIX 515E com 6.x e PDM versão 3.0

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).

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.

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.

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.

Configuração

Este procedimento o orienta na configuração de um dos firewalls PIX para disparar o túnel quando houver tráfego interessante. Essa configuração também ajuda a estabelecer o túnel através do link de backup através do roteador 2 (R2), quando não há conectividade entre o PIX-

01 e o PIX-02 através do roteador 1 (R1). Este documento mostra a configuração do PIX-01 usando PDM. Você pode configurar PIX-02 em linhas semelhantes.

Este documento pressupõe que você já configurou o roteamento.

Para apenas um link estar ativo por vez, faça com que R2 anuncie uma métrica pior para a rede 192.168.1.0 e para a rede 172.30.0.0. Por exemplo, se você usa o RIP para o roteamento, o R2 tem essa configuração além de outros anúncios de rede:

```
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
```

Procedimento de configuração

Quando você digita https://<Inside_IP_Address_on_PIX> para iniciar o PDM e clicar na guia VPN pela primeira vez, as informações sobre o Assistente automático de VPN são exibidas.

Home Configuration	Monitoring Refresh Save Help	Cisco System
Access Rules Transla Categories	IPSec Rules Use the Rules menu, the toolbar, or the right mouse button to add, edit or del	ete rules.
 Transform Sets IKE Policies XAuth/Mode Con Pre-shared Keys Certificate Certificate Cisco VPN Clien L2TP/PPTP Cliei IP Pools VPN System Options Easy VPN Remote 	VPN Wizard PDM features a VPN Wizard to help you create site-to-site and remote access VPNs. To launch this wizard, go to the "Wizards" menu and select the menu item "VPN Wizard" (Do not show me this message again.) OK	X nnel Policy
	Apply Reset	•

1. Selecione Assistentes > Assistente de VPN.

File Rules Si	earch Options To	ols Wizards Help			
Home	Configuration	Startus Wizard VPN Wizard ah	5ave	? Help	Cisco Systems
Device	Information			Interface Status	

2. O assistente VPN é iniciado e solicita o tipo de VPN que você deseja configurar. Escolha **VPN site a site**, selecione a interface **externa** como a interface na qual a VPN será habilitada e clique em

Avançar.		
😂 VPN Wizard		×
VPN Wizard	VPN Wizard	
Brannen Brannen Brannen	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:	
and the second	Site to Site VPN Remote Access VPN	
-There	Select the interface on which the VPN will be enabled:	
	outside	
	+ Back Next + Finish Cancel H	elp

 Digite o endereço IP do peer, onde o túnel IPsec deve terminar. Neste exemplo, o túnel termina na interface externa do PIX-02. Clique em Next.

💐 YPN Wizard	2
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
Notwork	Authentication
1 the	Pre-shared Key:
HUIM	Reenter Key
	C Certificate. The peer's identity is its:
	FGDN (Fully Qualified Domain Name)
	C IP Address
	< Back Next > Finish Cancel Help

4. Insira os parâmetros da política IKE que você escolhe para usar e clique em **Avançar**.

🔮 VPN Wizard			×
VPN Wizard	IKE Policy		
Branch Branch ISP ISP Honro Konvork	Please specify the encryption algorith Diffie-Hellman group that are used by association . Since the two parties ha to each other, make sure the configu	hm, authentication algorithm, and by the PIX when negotiating an IKE security have to agree on the algorithms in order to talk uration of the other party is the same as the PI	< K.
THE REAL	Encryption:	DES	
	Authentication:	MD5	
	DH Group:	Group 1 (768-bit)	
		* Back Next > Finish Cancel H	leip

 Forneça os parâmetros de criptografia e autenticação para o conjunto de transformações e clique em Avançar.

💐 VPN Wizard	×
VPN Wizard	Transform Set
Branch Branch Fise Fise Home 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.
THE HAR	Encryption: DES
	Authentication: MD5
	Back Neid > Finish Cancel Help

6. Selecione a rede local e as redes remotas que você precisa proteger usando o IPsec para selecionar o tráfego interessante que você precisa proteger.

💐 VPN Wizard					X
VPN Wizard	IPSec Traffic Selector				The second second
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	•	reed	
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		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

Verificar

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

Para verificar isso, desligue a interface serial R1 para a qual o túnel está estabelecido entre PIX-01 e PIX-02 via R2 quando o tráfego interessante existe.

Visualize o **Status da VPN** em **Home** no PDM (realçado em vermelho) para verificar a formação do túnel.

Home C	onliguration M	onitaring Refi	resh Save	9 Help			
Device Infor	mation	Provide and the second s		Interface S	tatus		
Host Name : PIX Version: Device Type : License: Licensed I Encryption: Failover	PIX-01.cisco 6.3(3) PIX 515E Failover Only eatures DES Enabled	PDM Version Total Memory Total Flash: Inside Hosts IKE Peers	3.0(1) 64 MB 16MB 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 0 up 7 up 0 down 0 down 0 down 0	Current Köp
Max Physical Interfaces:	6	Max Interfaces:	10	Select an inter			
System Res CPU 0% 17400:91	04 04 05 05 05 05 05 05 05 05 05 05 05 05 05	nŋ 17:11 16:58:41	17:20:11	1 0.5 18:59:41 UDP: 0	10.57-11 10 TCP: 0	23 41 Total: 0	17:00:11
Memory 18MB	Memory Usage (M 48 32 10 10:55:41 10:	B) 57:11 10:58:41	17:00	10.55.41	16:57:11 15	.58:41	17:60:11

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.

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.

Consulte o <u>Cisco PIX Device Manager 3.0</u> para obter mais informações sobre a configuração do PIX Firewall usando PDM.

Troubleshoot

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

Informações Relacionadas

- <u>Configurando um túnel PIX para PIX VPN simples usando IPSec</u>
- <u>Cisco PIX Firewall Software</u>
- <u>Referências do comando Cisco Secure PIX Firewall</u>
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação Cisco Systems