# 在防火墙之间使用 PDM 创建冗余隧道

## 目录

<u>简先要使网规背配配验故</u>相 <u>分决求用络则景置置证障关</u> 到<u>景置置证障关</u> 主

# <u>简介</u>

本文档介绍使用 Cisco PIX Device Manager (PDM) 在两个 PIX 防火墙之间配置隧道的过程。PIX 防火墙放置在两个不同的站点。在无法到达主路径的情况下,需要通过冗余链路来开启隧道。IPsec 是在 IPsec 对等体之间提供数据机密性、数据完整性和数据原始身份验证的开放标准组合。

# <u>先决条件</u>

### <u>要求</u>

本文档没有任何特定的要求。

### <u>使用的组件</u>

本文档中的信息基于以下软件和硬件版本:

• Cisco Secure PIX 515E 防火墙 6.x 以及 PDM 版本 3.0 本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

#### <u>网络图</u>

本文档使用以下网络设置:



#### 规则

有关文档约定的更多信息,请参考 Cisco 技术提示约定。

## <u>背景信息</u>

IPsec 协商可分为五个步骤,并且包括两个 Internet 密钥交换 (IKE) 阶段。

IPsec 隧道由相关数据流启动。如果数据流在 IPsec 对等体之间传输,则它会被认为是相关数据流 。

在 IKE 第 1 阶段中,IPsec 对等体对建立的 IKE 安全关联 (SA) 策略进行协商。对等体经过身份验 证后,会使用 Internet 安全关联和密钥管理协议 (ISAKMP) 创建安全隧道。

在 IKE 第 2 阶段中,IPsec 对等体使用经身份验证的安全隧道对 IPsec SA 转换进行协商。共享策 略的协商决定建立 IPsec 隧道的方式。

根据 IPsec 转换集中配置的 IPsec 参数,将在 IPsec 对等体之间创建 IPsec 隧道并传输数据。

如果删除了 IPsec SA,或者 IPsec SA 的生存时间到期,则 IPsec 隧道将终止。

注意:如果两个IKE阶段上的SA在对等体上不匹配,则两个PIX之间的IPsec协商失败。

### 配置

下面的过程将指导您完成其中一个 PIX 防火墙的配置,以便在存在相关流量时触发隧道。此配置还 可帮助您在 PIX-01 与 PIX-02 之间没有通过路由器 1 (R1) 的连接时,建立通过备份链路的隧道,该 备份链路通过路由器 2 (R2)。本文档说明如何使用 PDM 来配置 PIX-01。您可以按照类似方法来配 置 PIX-02。

本文档假设您已配置路由。

若要一次只接通一条链路,需要让 R2 为 192.168.1.0 网络和 172.30.0.0 网络通告一个更差度量。 例如,如果您使用 RIP 进行路由,则除了其他网络通告外,R2 还具有下面的配置:

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
```

### 配置过程

在首次键入 https://<Inside\_IP\_Address\_on\_PIX> 以启动 PDM 并单击 VPN 选项卡时,会显示有关 自动 VPN 向导的信息。

Eisco PIX Device Manager 3	0 - 172.16.5.10			
Home Configuration	Montoring Retresh	ave Help		CISCO SYSTEMS
Access Rules Transla	ation Rules VPN	Hasts/Networks	System Properties	In the state of the state
Categories	IPSet Rules			用地名高加
	Use the Rules menu, the toolba	r, or the right mouse but	on to add, edit or delete	rules.
	VPN Wizard		×	ppel Poliny
<ul> <li>Policies</li> <li>XAuth/Mode Con</li> <li>Pre-shared Keys</li> <li>Certificate</li> <li>Remote Access</li> <li>Cisco VPN Clien</li> <li>L2TP/PPTP Clien</li> <li>IP Pools</li> <li>VPN System Options-</li> <li>Easy VPN Remote</li> </ul>	PDM features a VPN Wizard and remote access VPNs. To "Wizards" menu and select th To not show me this me	to help you create site-to o launch this wizard, go t ne menu Item "VPN Wiza ssage again." OK	-site o the ind ."	
SECTOR STREET	1			
		бар у	Reset	
		admin> NA (15)	😡 🔐 🔂 🔒 15:	12:07 UTC Tue Aug 23 2005

#### 1. 选择 Wizards > VPN Wizard。

file Rules Se	carch Options To	ols Wizards Help			
Home	Configuration	Startup Wizard VPN Wizard sh	5ave	<b>?</b> Help	Cisco Systems
Deváce	Information			Interface Status	

2. VPN 向导启动,并提示您选择要配置的 VPN 的类型。选择 Site-to-Site VPN,然后选择 outside 接口以作为将启用 VPN 的接口,然后单击 Next。

📦 VPN Wizard		X					
VPN Wizard	VPN Wizard						
Branch Branch Distance Hoome	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						
- T-	Select the interface on which the VPN will be enabled:						
- I - CT	outside						
	Back Next > Finish Cancel Help	<u>,                                    </u>					

3. 输入对等体 IP 地址,IPsec 隧道应在此地址终止。在本示例中,隧道在PIX-02的外部接口上 结束。单击**Next**。

📦 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					
Notwork	Authentication					
the	Pre-shared Key					
HULLING.	Reenter Key:					
- L-	Certificate. The peer's identity is its:					
	FQDN (Fully Qualified Domain Name)					
	C IP Address					
	< Back Next > Finish Cancel Help					

4. 输入您选择使用的 IKE Policy 参数,然后单击 Next。

😝 VPN Wizard	X
VPN Wizard	IKE Policy
Brenden Brenden ISP Vermoe Vermoerte Network	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 REAL	Encryption: DES
2444MM	Authentication: MD5
	DH Group: Group 1 (768-bit)
	Back Next > Finish Cancel Help

5. 为 Transform Set 提供 Encryption 和 Authentication 参数,然后单击 Next。

💐 VPN Wizard		×
VPN Wizard	Transform Set	
Breads Br	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	A REPAIR AND A REAL
	Back Next > Finish Cancel Help	

6. 为了选择需要保护的相关流量,请选择需要使用 IPsec 保护的本地网络和远程网络。

💐 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	•	reend	
HUIM	IP address:	10.1.1.0			
THE	Mask	255.255.255.0			
B		Browse			
VPN Wizard			< Back Ne	x <b>t &gt;  </b> 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



如果有流向对等体的相关流量,则将在 PIX-01 和 PIX-02 之间建立隧道。

为了验证这一点,请在存在相关流量时,关闭已在 PIX-01 和 PIX-02 之间建立通过 R2 的隧道的 R1 串行接口。

在 PDM 中查看 Home 下的 VPN Status (以红色突出显示)以验证隧道是否已形成。

Home C	onliguration M	onitaring Refr	esh Save	<b>?</b> Heb			Cisco Syst	
Device Inform	mation			Interface S	tatus			
Host Name : PIX Version: Device Type : License: Licensed f 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 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 down	Current Kbp 0 7 0 0 0 0 0	
Max Physical Interfaces: VPN Status	al 6 Max 10 Interfaces:			Select an interface to view input and output Kbps				
System Res CPU 0% 17:00:31	OUTCES Status CPU Usage (perce 04 32 18.55341 10.5	n1) 17:11 16:58:41	17:90:11	1 0.5 18:55:41 UDP: 0	10.57:11 10	53:41 Tota	17:00:11 I: 0	
Memory 1815 1290101 Memory (MB)	Memory Usage (M 48 32 10 10 10 10 10 10 10	B) 57:11 10:58:41	17/004	18:55:41	erface Traffic Usage (Kbps) 10:57:11 16 Is 0 0000000000000000000000000000000000	tos: 41	17:00:11 0	

也可以使用 PDM 中 Tools 下的 CLI 来验证隧道是否已形成。发出 show crypto isakmp sa 命令可检 查隧道是否已形成,发出 show crypto ipsec sa 命令可观察已执行了封装、加密等操作的数据包的 数量。

<u>命令输出解释程序(仅限注册用户)(OIT) 支持某些 show 命令。</u>使用 OIT 可查看对 show 命令输 出的分析。

有关使用 PDM 配置 PIX 防火墙的详细信息,请参阅 Cisco PIX Device Manager 3.0。

# <u>故障排除</u>

目前没有针对此配置的故障排除信息。

# <u>相关信息</u>

- 使用 IPsec 配置简单的 PIX 到 PIX VPN 隧道
- <u>Cisco PIX 防火墙软件</u>
- Cisco Secure PIX 防火墙命令参考
- •<u>请求注解 (RFC)</u>
- <u>技术支持和文档 Cisco Systems</u>