# Redundante Tunnelerstellung zwischen Firewalls mithilfe von PDM

## Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Netzwerkdiagramm Konventionen Hintergrundinformationen Konfiguration Konfigurationsverfahren Überprüfen Fehlerbehebung Zugehörige Informationen

# **Einführung**

In diesem Dokument wird das Verfahren beschrieben, mit dem Sie Tunnel zwischen zwei PIX-Firewalls mithilfe des Cisco PIX Device Manager (PDM) konfigurieren. PIX-Firewalls werden an zwei verschiedenen Standorten platziert. Falls der primäre Pfad nicht erreicht wird, sollte der Tunnel über eine redundante Verbindung angestoßen werden. IPsec ist eine Kombination offener Standards, die Datensicherheit, Datenintegrität und Datenursprungsauthentifizierung zwischen IPsec-Peers bieten.

## **Voraussetzungen**

#### **Anforderungen**

Für dieses Dokument bestehen keine speziellen Anforderungen.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

• Cisco Secure PIX 515E-Firewalls mit 6.x und PDM Version 3.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

#### **Netzwerkdiagramm**

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

## **Hintergrundinformationen**

Die IPsec-Aushandlung kann in fünf Schritte unterteilt werden und umfasst zwei IKE-Phasen (Internet Key Exchange).

Ein IPsec-Tunnel wird durch interessanten Datenverkehr initiiert. Datenverkehr gilt als interessant, wenn er zwischen den IPsec-Peers übertragen wird.

In IKE Phase 1 handeln die IPsec-Peers die etablierte IKE Security Association (SA)-Richtlinie aus. Nach der Authentifizierung der Peers wird ein sicherer Tunnel mithilfe von Internet Security Association und Key Management Protocol (ISAKMP) erstellt.

In IKE Phase 2 verwenden die IPsec-Peers den authentifizierten und sicheren Tunnel, um IPsec-SA-Transformationen auszuhandeln. Die Aushandlung der freigegebenen Richtlinie bestimmt, wie der IPsec-Tunnel eingerichtet wird.

Der IPsec-Tunnel wird erstellt, und Daten werden zwischen den IPsec-Peers übertragen, basierend auf den in den IPsec-Transformationssätzen konfigurierten IPsec-Parametern.

Der IPsec-Tunnel endet, wenn die IPsec-SAs gelöscht werden oder ihre Lebensdauer abläuft.

**Hinweis:** Die IPsec-Aushandlung zwischen den beiden PIXs schlägt fehl, wenn die SAs in beiden IKE-Phasen auf den Peers nicht übereinstimmen.

## **Konfiguration**

Dieses Verfahren führt Sie durch die Konfiguration einer der PIX-Firewalls, um den Tunnel

auszulösen, wenn interessanter Datenverkehr vorhanden ist. Mit dieser Konfiguration können Sie auch den Tunnel über die Backup-Verbindung über Router 2 (R2) erstellen, wenn zwischen PIX-01 und PIX-02 keine Verbindung über Router 1 (R1) besteht. Dieses Dokument zeigt die Konfiguration von PIX-01 mithilfe von PDM. Sie können PIX-02 auf ähnlichen Leitungen konfigurieren.

In diesem Dokument wird davon ausgegangen, dass Sie das Routing bereits konfiguriert haben.

Damit immer nur eine Verbindung aktiv ist, sollte R2 eine schlechtere Kennzahl für das Netzwerk 192.168.1.0 sowie für das Netzwerk 172.30.0.0 angeben. Wenn Sie beispielsweise RIP für das Routing verwenden, verfügt R2 über diese Konfiguration, die von anderen Netzwerkwerbespots abweicht:

```
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
```

#### Konfigurationsverfahren

Wenn Sie https://<Inside\_IP\_Address\_on\_PIX> eingeben, um PDM zu starten, und zum ersten Mal auf die Registerkarte VPN klicken, werden Informationen zum automatischen VPN-Assistenten angezeigt.



1. Wählen Sie Assistenten > VPN-Assistent

le Rules Search Options 1	ools Wizards Help		
Home Configuration	Stortup Wizard VPN Wizard Nsh	Save Help	Cisco System

 Der VPN-Assistent wird gestartet, und Sie werden aufgefordert, den zu konfigurierenden VPN-Typ einzugeben. W\u00e4hlen Sie Site-to-Site VPN aus, w\u00e4hlen Sie die externe Schnittstelle als Schnittstelle aus, auf der das VPN aktiviert wird, und klicken Sie auf Weiter.

📦 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. Geben Sie die Peer-IP-Adresse ein, an der der IPsec-Tunnel enden soll. In diesem Beispiel endet der Tunnel an der externen Schnittstelle von PIX-02. Klicken Sie auf Weiter.

📦 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				
1 Aren	Pre-shared Key:				
FATTINE	Reenter Key:				
The	C Certificate. The peer's identity is its:				
	FODN (Fully Qualified Domain Name)				
	C IP Address				
	< Back Next > Finish Cancel Help				

4. Geben Sie die IKE-Richtlinienparameter ein, die Sie verwenden möchten, und klicken Sie auf **Weiter**.

🔮 VPN Wizard	× · · · · · · · · · · · · · · · · · · ·					
VPN Wizard	IKE Policy					
Brench Brench 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 ALL	Encryption: DES					
	Authentication: MD5					
	DH Group: Group 1 (768-bit)					
	Sack Next > Finish Cancel Help					

5. Geben Sie die Verschlüsselungs- und Authentifizierungsparameter für den Konfigurationssatz an, und klicken Sie auf **Weiter**.

💐 VPN Wizard	×					
VPN Wizard	Transform Set					
Branch Branch Fried Frie	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					
	Seck Next > Finish Cancel Help					

6. Wählen Sie das lokale Netzwerk und die Remote-Netzwerke aus, die Sie mithilfe von IPsec schützen müssen, um den interessanten Datenverkehr auszuwählen, den Sie schützen müssen.

💐 VPN Wizard					X
VPN Wizard	IPSec Traffic Selector				
Branch Br	IPSec Traffic Sele IPSec tunnel. Pac (which you specif (which you will sp On Local Site	ector 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 t d hosts/net s/networks ntected 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	xt> Farin	sh Cancel Help
VPN Wizard	IPSec Traffic Selector	(Continue)	THE NEW YORK	and the second	
Branch Branch	Use this panel to IPSec Traffic Sele	specify the hosts/r ctor to select traffic	etworks at the re flows to be prot	emote site ected by th	that are used in e IPSec tunnel.
Home		te			
(Corporate)	Host/Network				
Notwo	( IP Address	C Name	C Group		Selected:
the state	Interface:	outside	•		172.30.0.0016
LULING	IP address:	172.30.0.0		>>	
The	Mask:	255.255.0.0			
-6-		Browse			
			< Back Ne	d> Finis	sh Cancel Help

# <u>Überprüfen</u>

Wenn ein interessanter Datenverkehr zum Peer besteht, wird der Tunnel zwischen PIX-01 und PIX-02 erstellt.

Um dies zu überprüfen, fahren Sie die serielle Schnittstelle R1, für die der Tunnel zwischen PIX-01 und PIX-02 über R2 eingerichtet wird, herunter, wenn der interessante Datenverkehr vorhanden ist.

Zeigen Sie den VPN-Status unter Home im PDM (rot markiert) an, um die Bildung des Tunnels zu überprüfen.

Gene C	onliguration M	onitoring Ref	resh Save	<b>?</b> Heb					
Device Inform	nation			Interface S	tatus				
Host Name :	PIX-01.cisco			Interface	IP Address/Mask	Link	Current Kbp		
PIX Version:	6.3(3)	PDM Version :	3.0(1)	intr2	0.0.0/0	odown	0		
Device Type :	PIX 515E	Total Memory.	64 MB	inside	172.16.5.99/24	🛛 up	7		
License:	Failover Only	Total Flash:	16MB	outside	150.1.1 66/24	🕒 up	0		
Licensed F	eatures			intro	0.0.0/0	e down	0		
Encryption:	DES	Inside Hosts:	Unlimited	intr4	0.0.0/0	e down	0		
Failover	Enabled	IKE Peers	Unlimited	INU 3	0.0.0/0	- down	U		
Max Physical		Max	40	1 22 15 15					
Interfaces:	nterfaces: 10				Select an interface to view input and output Kbps				
VPN Status				Traffic Stat	us	19 States			
IKE Tunnels:	1	IPSec Tunnels	1	Connection	s Per Second Usage	aler hards	anti-fi di secili		
CPU 0% 17:00:31	CPU Usage (percei 00 04 32 15:55:41 10:5	nŋ 17:11 16:59:41	17:00:11	0.5 18:55:41 UDP: 0	10.57-11 10	28:41 Tota	17:00:11 1: 0		
Memory	Memory Usage (M	B)		outside' Inte	erface Traffic Usage (Kbps)		Part of the		
18MB 17:00:31	84 46 32 16 16 55:41 10:	57:11 10:58:41	17:00	18,95,41	10:57:11 10	69:41	17:00:11		
Memory (MB)			A CONTRACTOR OF THE OWNER OF THE	Input Kbp	is 0 <mark>0</mark> 00	itput Kbps	0		
Used: 18.16	5 Free: 45/	835 Total: 8	4	States and states		And an Address	sound in the second difference of		

Sie können auch die Bildung von Tunneln mithilfe der CLI im PDM unter Tools überprüfen. Geben Sie den Befehl **show crypto isakmp sa** ein, um die Bildung von Tunneln zu überprüfen und den Befehl **show crypto ipsec als** Befehl auszugeben, um die Anzahl der eingekapselten, verschlüsselten Pakete usw. zu beobachten.

Das <u>Output Interpreter Tool</u> (nur <u>registrierte</u> Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**. Weitere Informationen zur Konfiguration der PIX-Firewall mithilfe von PDM finden Sie im <u>Cisco</u> <u>PIX Device Manager 3.0</u>.

# **Fehlerbehebung**

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

# Zugehörige Informationen

- Konfigurieren eines einfachen PIX-zu-PIX-VPN-Tunnels mithilfe von IPsec
- <u>Cisco PIX Firewall-Software</u>
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- Anforderungen für Kommentare (RFCs)
- <u>Technischer Support und Dokumentation Cisco Systems</u>