

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:

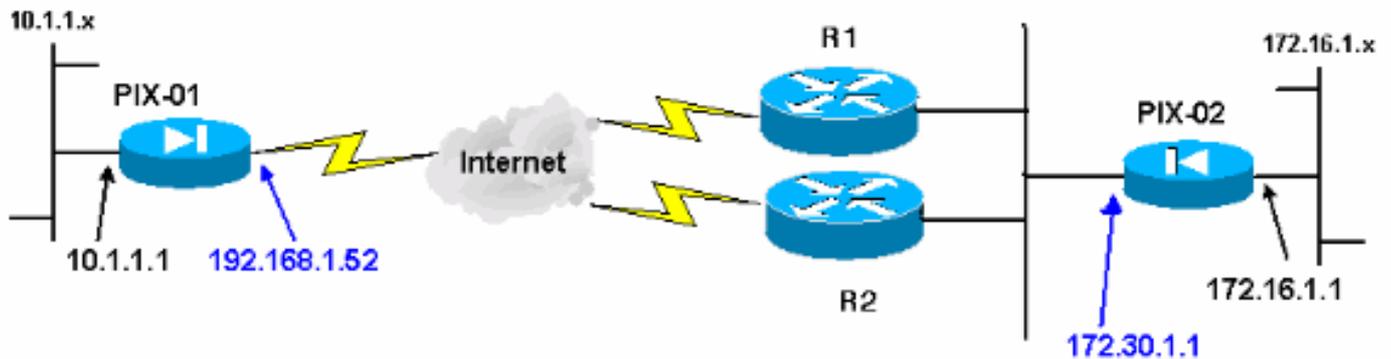
- Cisco Secure PIX 515E-Firewalls mit 6.x und PDM Version 3.0

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 [Cisco Technical Tips Conventions](#) (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.

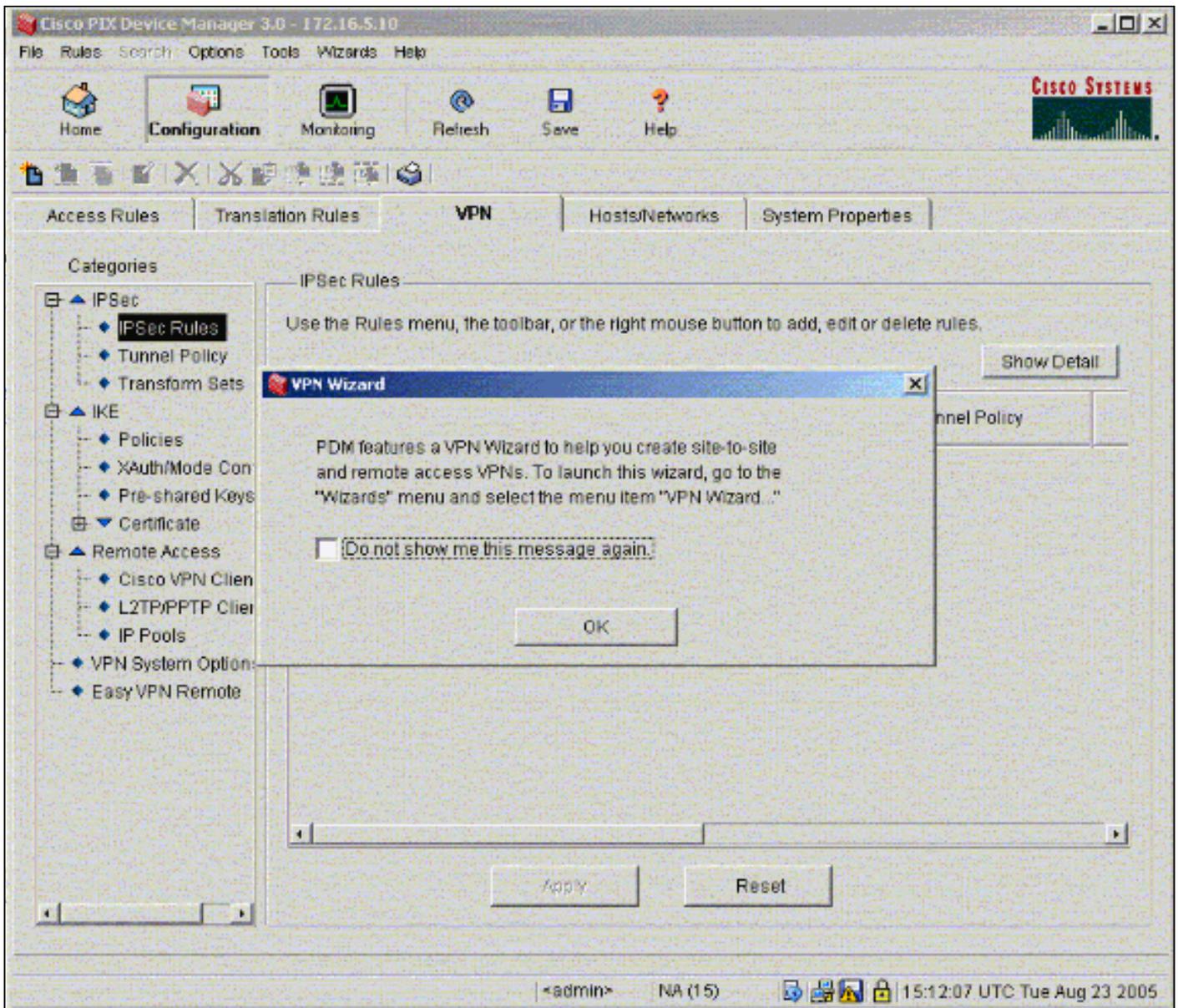
In diesem Dokument wird davon ausgegangen, dass Sie das Routing bereits konfiguriert haben.

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:

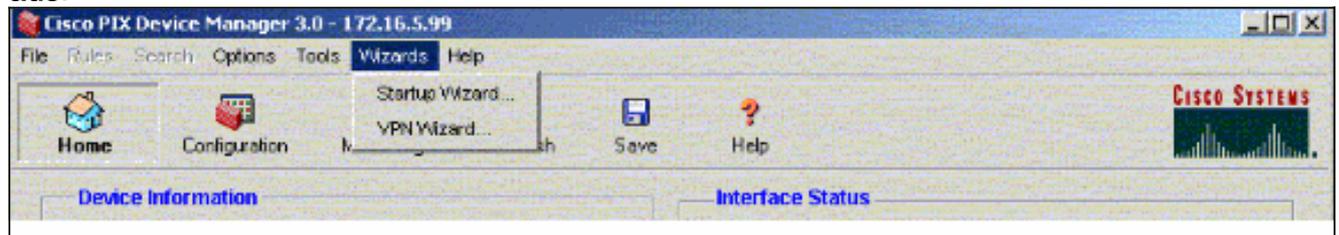
```
R2(config)#router rip
R2(config-router)#offset-list 1 out 2 s1
R2(config-router)#offset-list 2 out 2 e0
R2(config-router)#exit
R2(config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

[Konfigurationsverfahren](#)

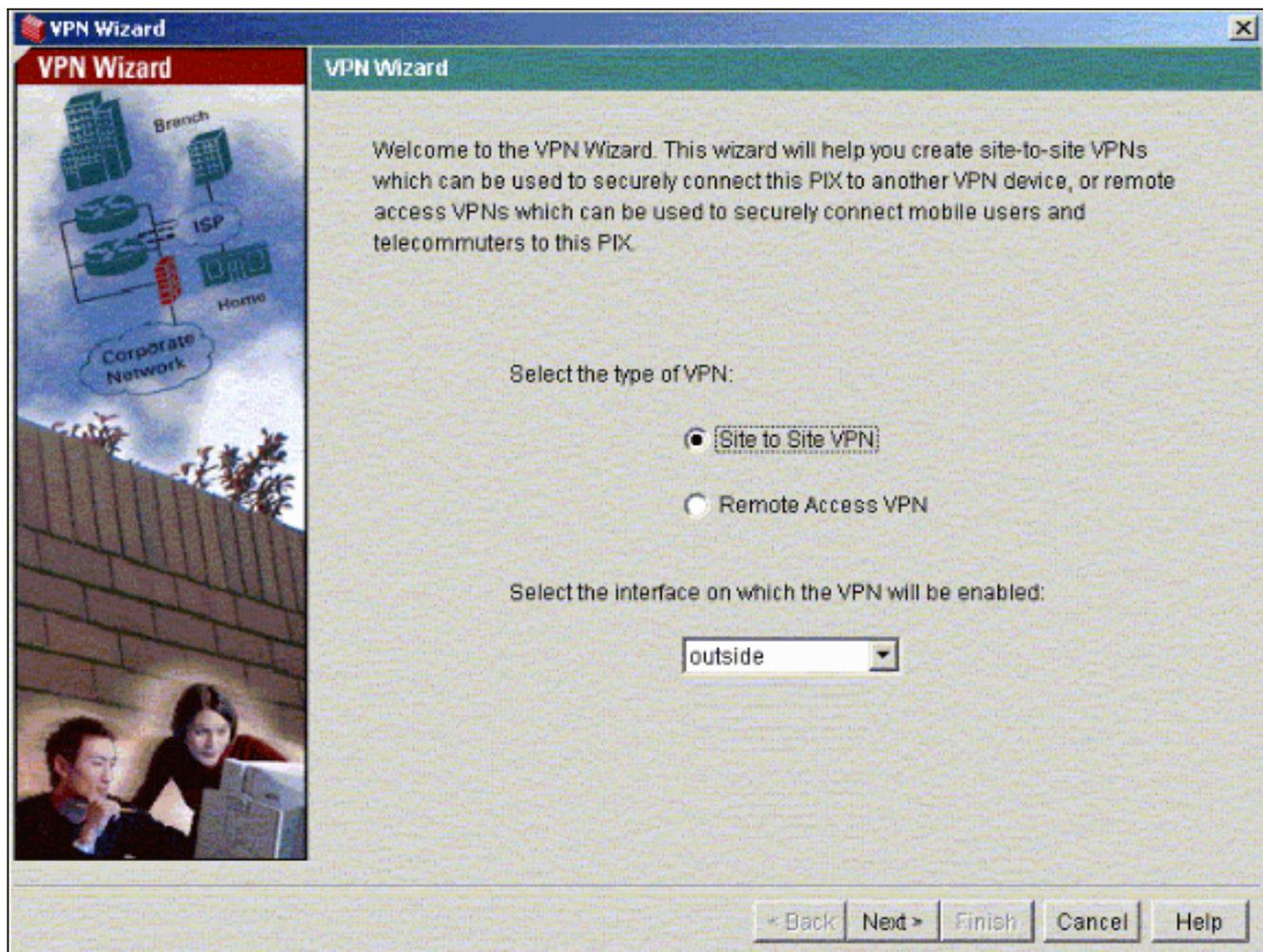
Wenn Sie https://<Inside_IP_Address_on_PIX> eingeben, um PDM zu starten, und zum ersten Mal auf die Registerkarte VPN klicken, werden Informationen zum automatischen VPN-Assistenten angezeigt.



1. Wählen Sie Assistenten > VPN-Assistent aus.



2. Der VPN-Assistent wird gestartet, und Sie werden aufgefordert, den zu konfigurierenden VPN-Typ einzugeben. Wählen Sie **Site-to-Site VPN** aus, wählen Sie die **externe** Schnittstelle als Schnittstelle aus, auf der das VPN aktiviert wird, und klicken Sie auf **Weiter**.



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**.

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

Peer IP Address:

Authentication

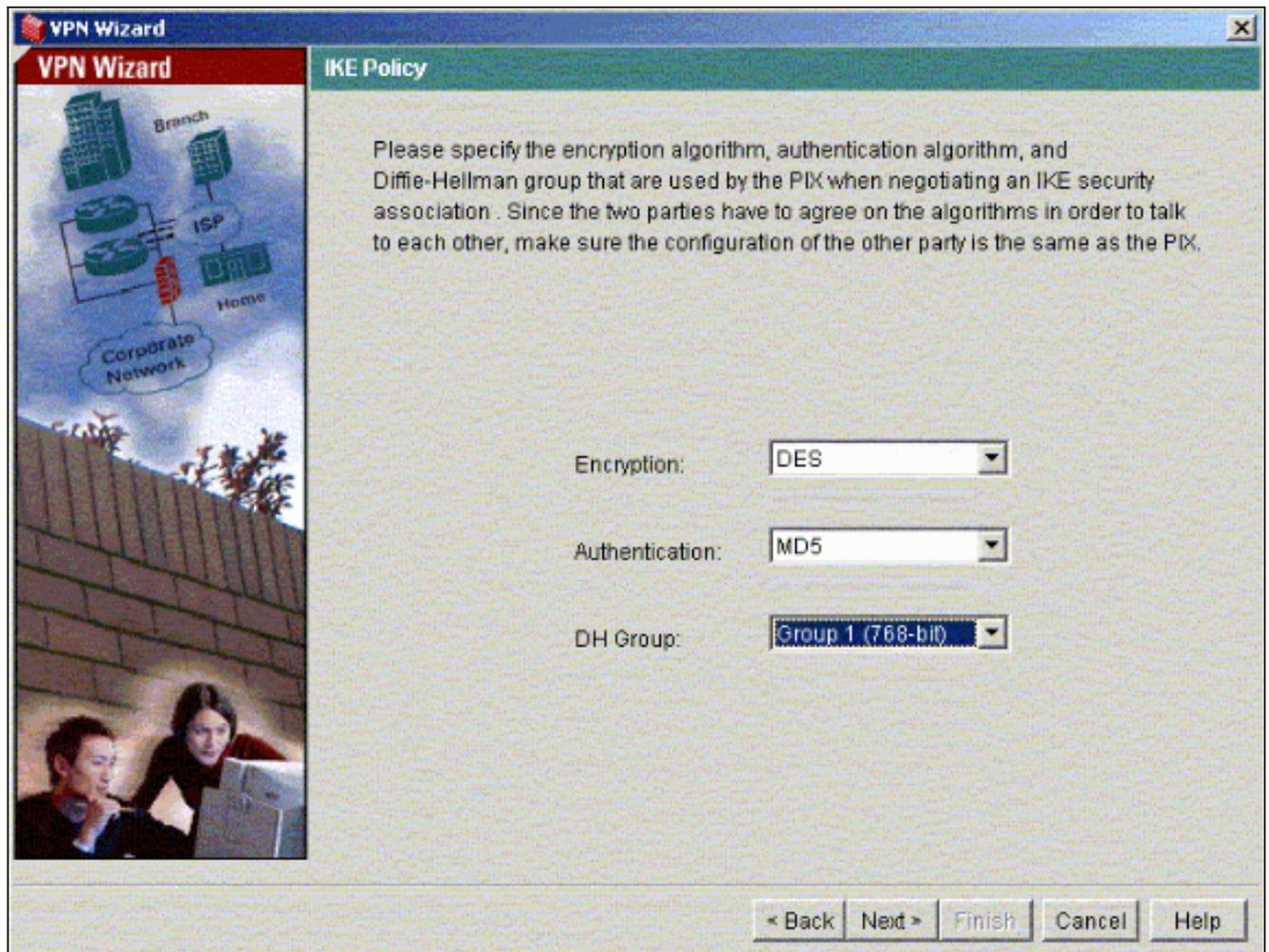
Pre-shared Key
Reenter Key:

Certificate. The peer's identity is its:
 FQDN (Fully Qualified Domain Name)
 IP Address

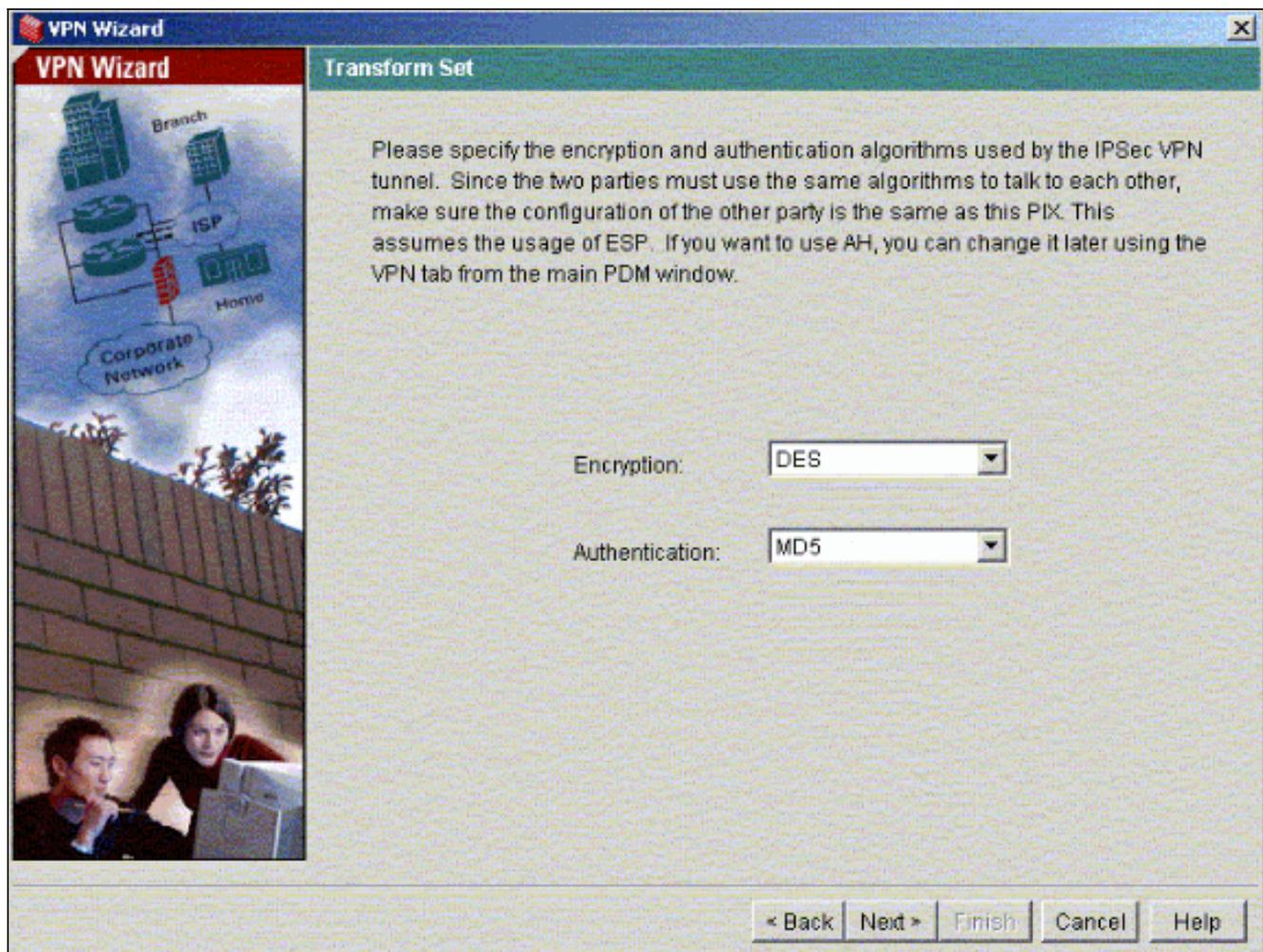
< Back Next > Finish Cancel Help

The image shows a screenshot of the 'VPN Wizard' software interface. On the left side, there is a vertical panel with a red header 'VPN Wizard' and a network diagram. The diagram shows a 'Corporate Network' at the bottom, connected to a 'Branch' and 'Home' office, both of which are connected to an 'ISP'. The main area of the window is titled 'Remote Site Peer' and contains a text box for 'Peer IP Address' with the value '172.30.1.1'. Below this is an 'Authentication' section with four radio button options: 'Pre-shared Key' (selected), 'Certificate. The peer's identity is its:', 'FQDN (Fully Qualified Domain Name)' (selected), and 'IP Address'. The 'Pre-shared Key' and 'FQDN' options have corresponding text input fields. At the bottom right, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

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



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



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



IPSec Traffic Selector selects the traffic flows that are going to be protected by the IPSec tunnel. Packets that flow between the selected hosts/networks inside the PIX (which you specify below) and the the selected hosts/networks at the remote site (which you will specify on the next screen) will be protected by the IPSec tunnel.

On Local Site (protected by this PIX)

Host/Network

IP Address
 Name
 Group

Interface:

IP address:

Mask:

Selected:

>>

<<

VPN Wizard X

VPN Wizard IPSec Traffic Selector (Continue)



Use this panel to specify the hosts/networks at the remote site that are used in IPSec Traffic Selector to select traffic flows to be protected by the IPSec tunnel.

On Remote Site

Host/Network

IP Address
 Name
 Group

Interface:

IP address:

Mask:

Selected:

>>

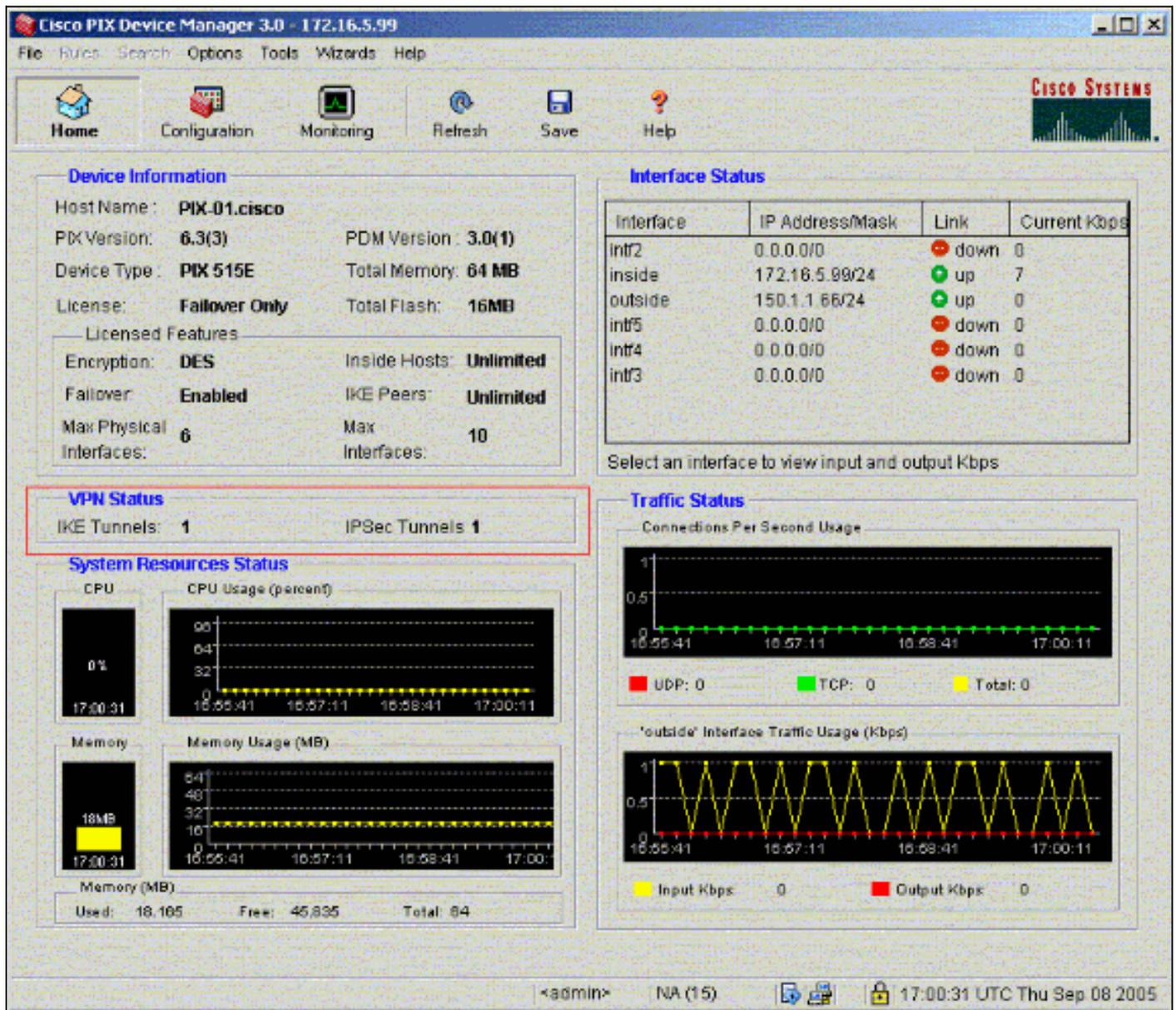
<<

Überprüfen

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.



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 [Output Interpreter Tool](#) (nur [registrierte](#) 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 [Cisco PIX Device Manager 3.0](#).

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](#)
- [Cisco PIX Firewall-Software](#)
- [Cisco Secure PIX Firewall - Befehlsreferenzen](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)