

Création de tunnels redondants entre pare-feu à l'aide de PDM

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Diagramme du réseau](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Procédure de configuration](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit la procédure que vous utilisez pour configurer des tunnels entre deux pare-feu PIX à l'aide de Cisco PIX Device Manager (PDM). Les pare-feux PIX sont placés à deux endroits différents. En cas d'échec d'accès au chemin principal, il est souhaitable de démarrer le tunnel via une liaison redondante. IPSec est une combinaison de normes ouvertes qui fournissent la confidentialité des données, l'intégrité des données et l'authentification de l'origine des données entre des homologues IPSec.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Components Used](#)

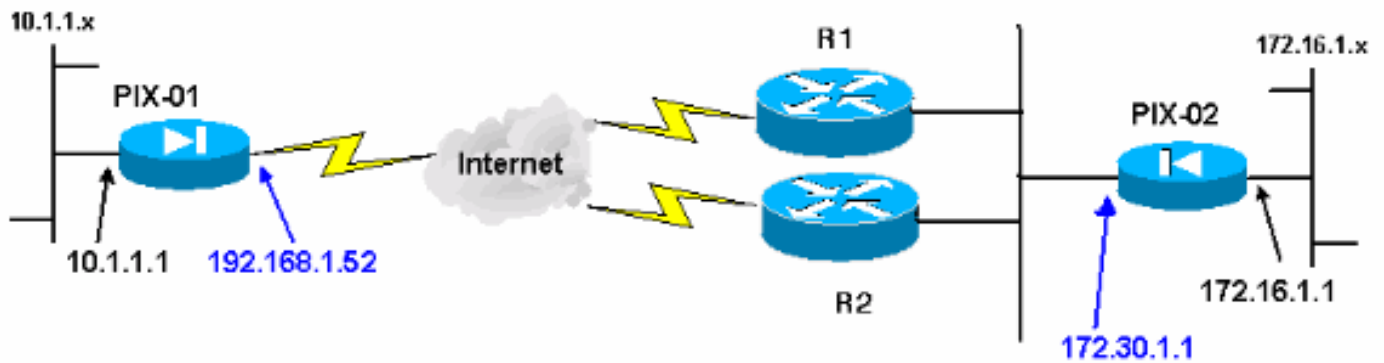
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Pare-feu Cisco Secure PIX 515E avec 6.x et PDM version 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.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

La négociation IPsec peut être décomposée en cinq étapes et inclut deux phases d'échange de clés Internet (IKE).

Un tunnel IPsec est lancé par un trafic intéressant. Le trafic est considéré comme intéressant quand il transite entre les homologues IPsec.

Dans la phase 1 d'IKE, les homologues IPsec négocient la stratégie d'association de sécurité IKE. Une fois que les homologues sont authentifiés, un tunnel sécurisé est créé en utilisant Internet Security Association and Key Management Protocol (ISAKMP).

Dans la phase 2 d'IKE, les homologues IPsec utilisent le tunnel authentifié et sécurisé pour négocier des transformations d'association de sécurité IPsec. La négociation de la stratégie partagée détermine comment le tunnel IPsec est établi.

Le tunnel IPsec est créé et les données sont transférées entre les homologues IPsec en fonction des paramètres IPsec configurés dans les jeux de transformations IPsec.

Le tunnel IPsec se termine quand les associations de sécurité IPsec sont supprimées ou quand leur durée de vie expire.

Remarque : la négociation IPsec entre les deux PIXes échoue si les SA des deux phases IKE ne correspondent pas sur les homologues.

Configuration

Cette procédure vous guide tout au long de la configuration d'un des pare-feu PIX pour déclencher le tunnel lorsqu'il existe un trafic intéressant. Cette configuration vous aide également à établir le

tunnel via la liaison de sauvegarde via le routeur 2 (R2), lorsqu'il n'y a aucune connectivité entre le PIX-01 et le PIX-02 via le routeur 1 (R1). Ce document montre la configuration de PIX-01 à l'aide de PDM. Vous pouvez configurer PIX-02 sur des lignes similaires.

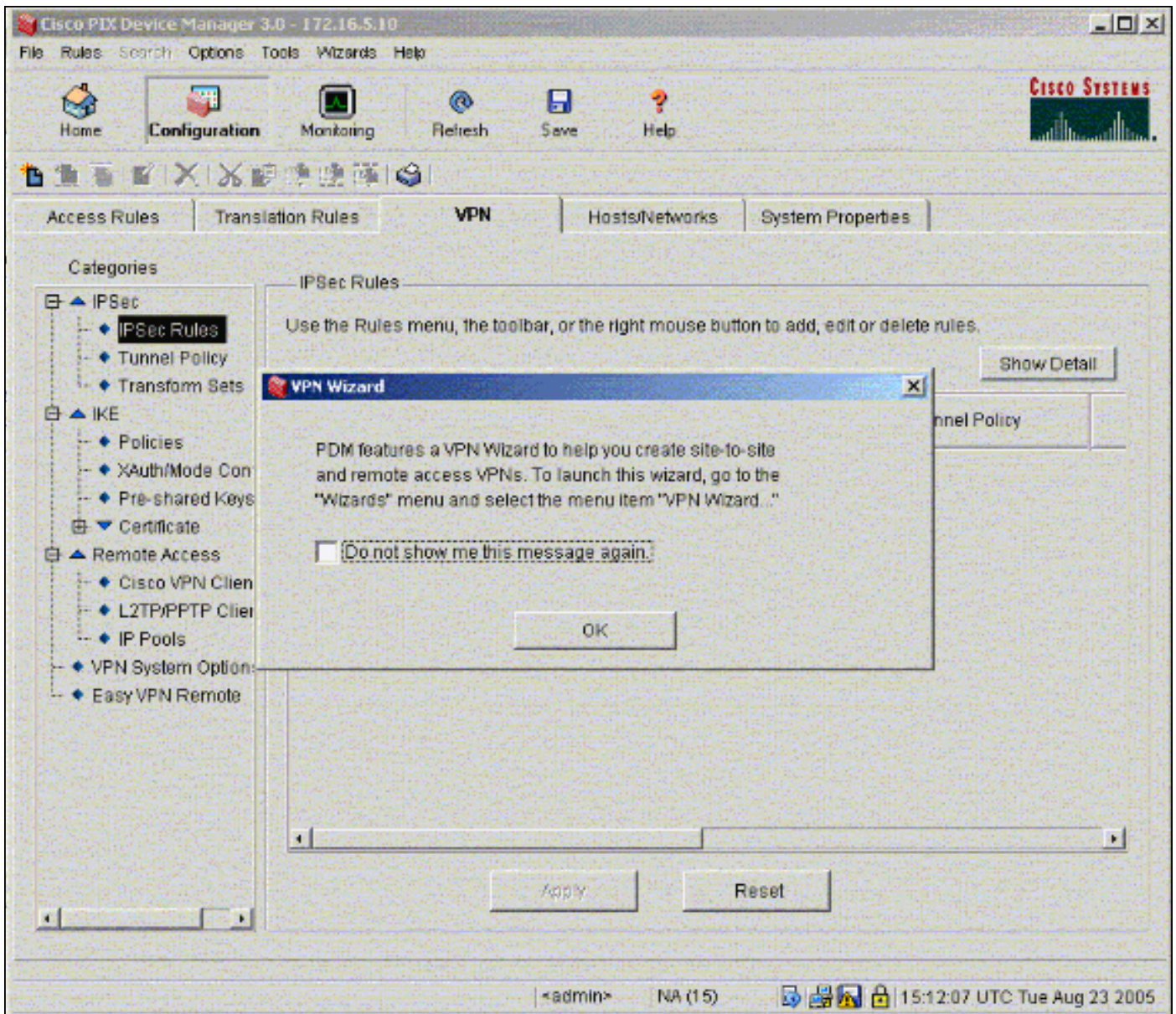
Ce document suppose que vous avez déjà configuré le routage.

Pour qu'une seule liaison soit active à la fois, faites en sorte que R2 annonce une métrique pire pour le réseau 192.168.1.0 ainsi que pour le réseau 172.30.0.0. Par exemple, si vous utilisez RIP pour le routage, R2 a cette configuration en dehors des autres annonces réseau :

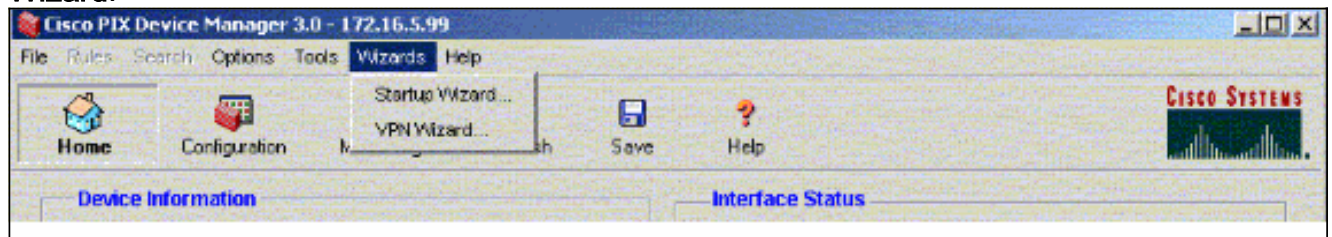
```
R2(config)#router rip
R2(config-router)#offset-list 1 out 2 s1
R2(config-router)#offset-list 2 out 2 e0
R2(config-router)#exit
R2(config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2(config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

[Procédure de configuration](#)

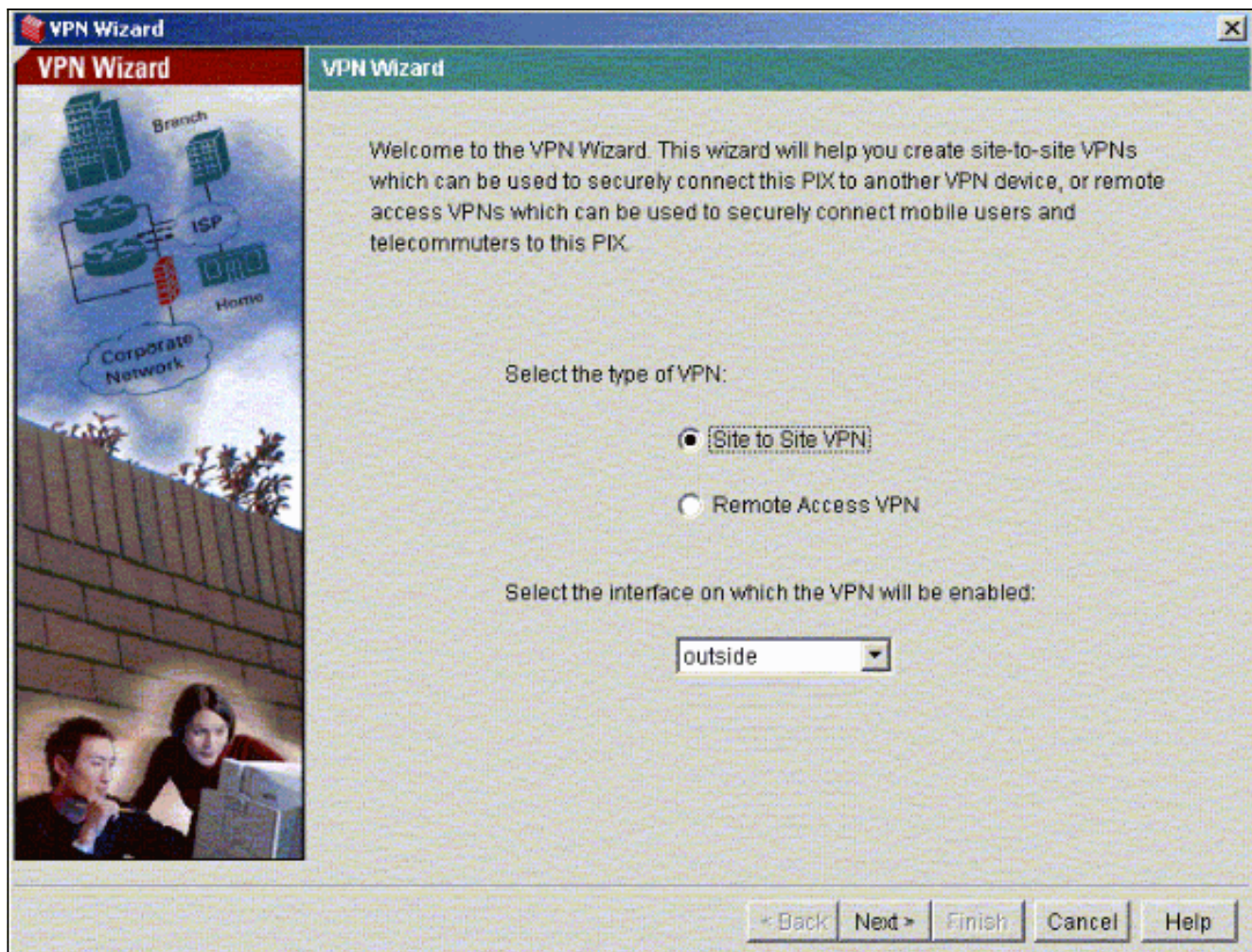
Lorsque vous tapez https://<Inside_IP_Address_on_PIX> afin de lancer PDM et que vous cliquez pour la première fois sur l'onglet VPN, les informations relatives à l'assistant VPN automatique s'affichent.



1. Sélectionnez Wizards > VPN Wizard.



2. L'assistant VPN démarre et vous invite à indiquer le type de VPN que vous voulez configurer. Choisissez **VPN site à site**, sélectionnez l'interface **externe** comme interface sur laquelle le VPN sera activé, puis cliquez sur **Suivant**.



3. Entrez l'adresse IP de l'homologue, où le tunnel IPsec doit se terminer. Dans cet exemple, le tunnel se termine sur l'interface externe de PIX-02. Cliquez sur **Next** (Suivant).

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

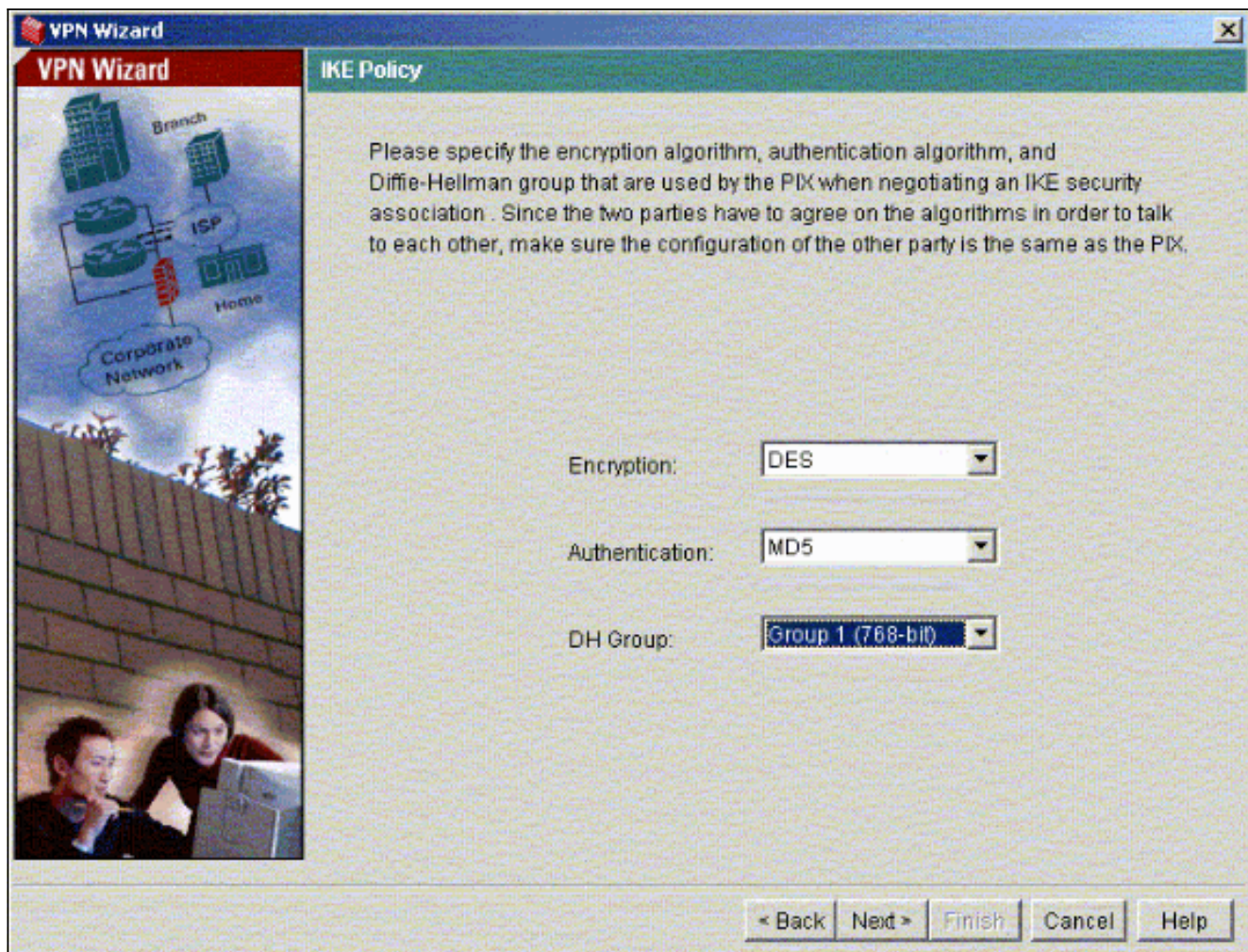
Pre-shared Key
Reenter Key:

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

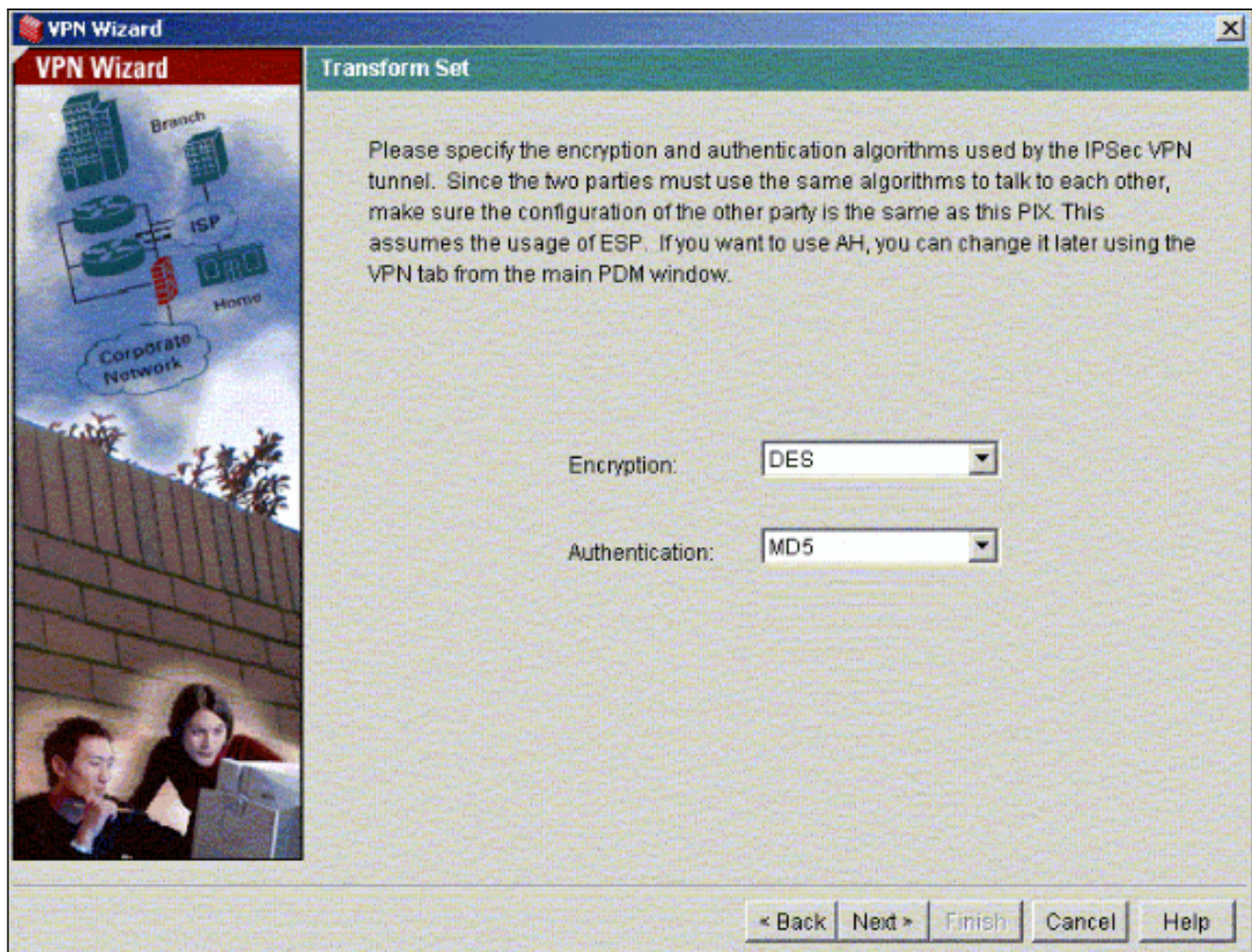
< Back Next > Finish Cancel Help

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 'Home' site, which is in turn connected to an 'ISP' and a 'Branch' site. On the right side, the main window is titled 'Remote Site Peer'. It 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 associated text input fields. At the bottom right, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

4. Entrez les paramètres de stratégie IKE que vous choisissez d'utiliser et cliquez sur Suivant.




5. Fournissez les paramètres de chiffrement et d'authentification pour le jeu de transformation, puis cliquez sur **Suivant**.



6. Sélectionnez le réseau local et les réseaux distants que vous devez protéger à l'aide d'IPsec afin de sélectionner le trafic intéressant que vous devez protéger.

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:

>>

<<

Vérification

S'il y a du trafic intéressant à l'homologue, le tunnel est établi entre pix-01 et PIX-02.

Afin de vérifier cela, arrêtez l'interface série de R1 pour laquelle le tunnel est établi entre PIX-01 et PIX-02 via R2 lorsque le trafic intéressant existe.

Affichez l'état du VPN sous Accueil dans le PDM (mis en évidence en rouge) afin de vérifier la formation du tunnel.

The screenshot displays the Cisco PIX Device Manager 3.0 interface for device 172.16.5.99. The 'VPN Status' section is highlighted with a red box, showing 1 IKE Tunnel and 1 IPsec Tunnel. The 'Interface Status' table is as follows:

Interface	IP Address/Mask	Link	Current Kbps
intf2	0.0.0.0/0	down	0
inside	172.16.5.99/24	up	7
outside	150.1.1.66/24	up	0
intf5	0.0.0.0/0	down	0
intf4	0.0.0.0/0	down	0
intf3	0.0.0.0/0	down	0

The 'System Resources Status' section shows CPU usage at 0% and memory usage at 18MB. The 'Traffic Status' section includes graphs for Connections Per Second Usage and 'outside' Interface Traffic Usage (Kbps).

Vous pouvez également vérifier la formation des tunnels à l'aide de l'interface de ligne de commande sous Outils dans le PDM. Exécutez la commande `show crypto isakmp sa` pour vérifier la formation des tunnels et exécutez la commande `show crypto ipsec sa` pour observer le nombre de paquets encapsulés, chiffrés, etc.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\)](#) prend en charge certaines commandes `show`. Utilisez l'OIT pour afficher une analyse de la sortie de la commande `show`.

Référez-vous à [Cisco PIX Device Manager 3.0](#) pour plus d'informations sur la configuration du pare-feu PIX à l'aide de PDM.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Configuration d'un tunnel VPN PIX-to-PIX simple à l'aide d'IPsec](#)
- [Logiciels pare-feu Cisco PIX](#)
- [Références des commandes du pare-feu Cisco Secure PIX](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)