

# ةي امحل ا نارءج ني ب رركم ق فن عاشنإ PDM م اءءء س اب

## المءءوءاء

- [المءءمة](#)
- [المءءلباء الأساءة](#)
- [المءءلباء](#)
- [المءوءاء المسءءءمة](#)
- [الرسم الأءءلبي للشبكة](#)
- [الاصءلاءاء](#)
- [مءلواء أساسة](#)
- [الأءوءن](#)
- [إءراء الأءوءن](#)
- [الأءءق من الصءءة](#)
- [اسءءشف الأءءاء وإصلاءها](#)
- [مءلواء ذاء صلة](#)

## المءءمة

يصف هذا المسءء الإءراء الذي اسءءءمه لأءوءن الأنفاق بين ءءرءي ءماة PIX باسءءءام مءر أءءة PIX (PDM) من Cisco. يتم وءع ءءران ءءماة من طراز PIX في موءعن مءءلبن. وفي ءالة الفشل في الوءول إلى المسار الأساسى، من المسءءسن بءء اشءل النفق من ءلال إرباء مءرر. IPsec هو مءوءة من المعاببر المءوءوءة الءى ءوفر سربة الببانا وءلماة الببانا ومصاءقة أصل الببانا بين نطائر IPsec.

## المءءلباء الأساسة

### المءءلباء

لا ءوء مءءلباء ءاصة لهذا المسءء.

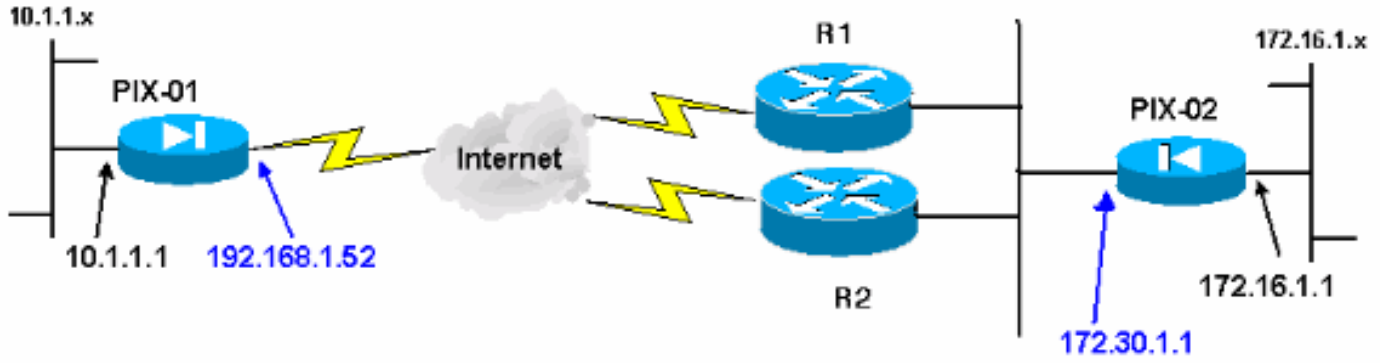
### المءوءاء المسءءءمة

ءسءء المءلواء الوارءة في هذا المسءء إلى إصداراء البرامء والمءوءاء الماءة الآلءة:

- ءءران ءءماة Cisco Secure PIX 515e مع الإصدار x.6 و PDM الإصدار 3.0
- تم إنشاء المءلواء الوارءة في هذا المسءء من الأءءة الموءوءة في ببئة معملبة ءاصة. بءأء ءمبب الأءءة المسءءءمة في هذا المسءء بءوءن ممسوء (افءراضى). إذا ءانء شبءءك مباءرة، فءأكد من فهمك للأءبب المءءمل لأى أمر.

## الرسم الأءءلبي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



## الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

## معلومات أساسية

يمكن تقسيم مفاوضات IPsec إلى خمس خطوات، وتتضمن مرحلتين من عملية تبادل مفتاح الإنترنت (IKE).

يتم بدء نفق IPsec بواسطة حركة مرور مثيرة للاهتمام. تعتبر حركة المرور مثيرة للاهتمام عندما تنتقل بين نظائر IPsec.

في المرحلة الأولى من IKE، يتفاوض نظراء IPsec على سياسة اقتران أمان (SA) (IKE) التي تم إنشاؤها. بمجرد مصادقة النظراء، يتم إنشاء نفق آمن باستخدام بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP).

في المرحلة 2 من IKE، يستخدم نظراء IPsec النفق الآمن والمصدع للتفاوض على تحويلات IPsec SA. يحدد التفاوض على السياسة المشتركة كيفية إنشاء نفق IPsec.

يتم إنشاء نفق IPsec ويتم نقل البيانات بين نظائر IPsec استناداً إلى معلمات IPsec التي تم تكوينها في مجموعات تحويل IPsec.

ينتهي نفق IPsec عند حذف وحدات IPsec SAs أو عند انتهاء صلاحية مدة حياتها.

ملاحظة: يفشل مفاوضة IPsec بين PIXs إذا لم تتطابق عمليات SAs على كل من مرحلتي IKE مع عمليات النظير.

## التكوين

يرشدك هذا الإجراء خلال تكوين أحد جدران حماية PIX لتشغيل النفق عند وجود حركة مرور مثيرة للاهتمام. كما يساعدك هذا التكوين في إنشاء النفق من خلال إرتباط النسخ الاحتياطي عبر الموجه 2 (R2)، في حالة عدم وجود اتصال بين PIX-01 و PIX-02 عبر الموجه 1 (R1). يوضح هذا المستند تكوين PIX-01 باستخدام PDM. يمكنك تكوين PIX-02 على خطوط مماثلة.

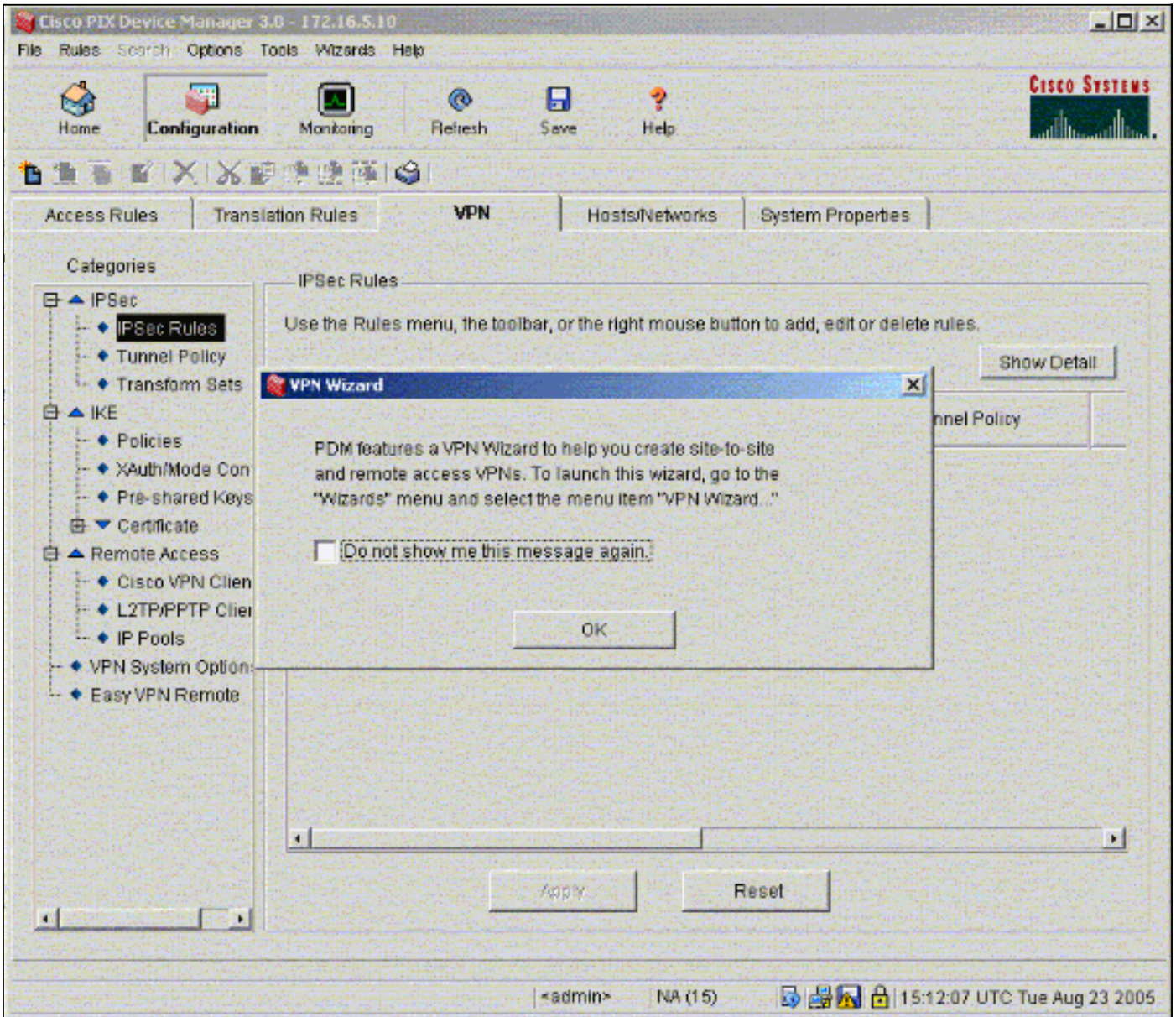
يفترض هذا المستند أنك قمت بتكوين التوجيه بالفعل.

من أجل إرتباط واحد فقط يمكن تشغيله في المرة الواحدة، أجعل إعلان R2 مقياساً أسوأ لشبكة 192.168.1.0 بالإضافة إلى شبكة 172.30.0. على سبيل المثال، إذا كنت تستخدم RIP للتوجيه، فإن R2 له هذا التكوين بخلاف إعلانات الشبكة الأخرى:

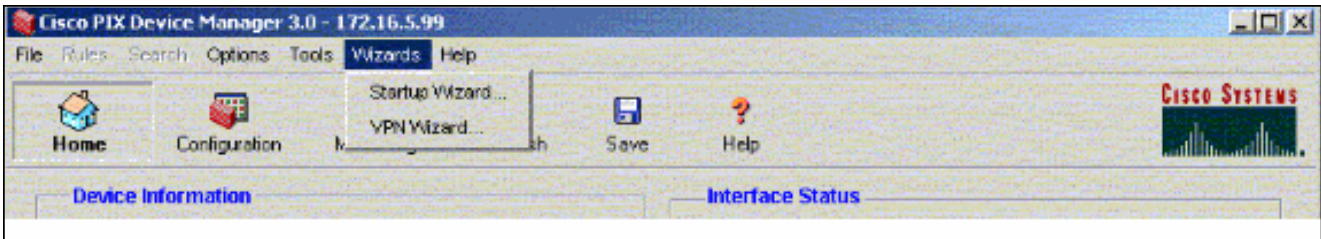
```
R2 (config)#router rip
R2 (config-router)#offset-list 1 out 2 s1
R2 (config-router)#offset-list 2 out 2 e0
R2 (config-router)#exit
R2 (config)#access-list 1 permit 172.30.0.0 0.0.255.255
R2 (config)#access-list 2 permit 192.168.1.0 0.0.0.255
```

## إجراء التكوين

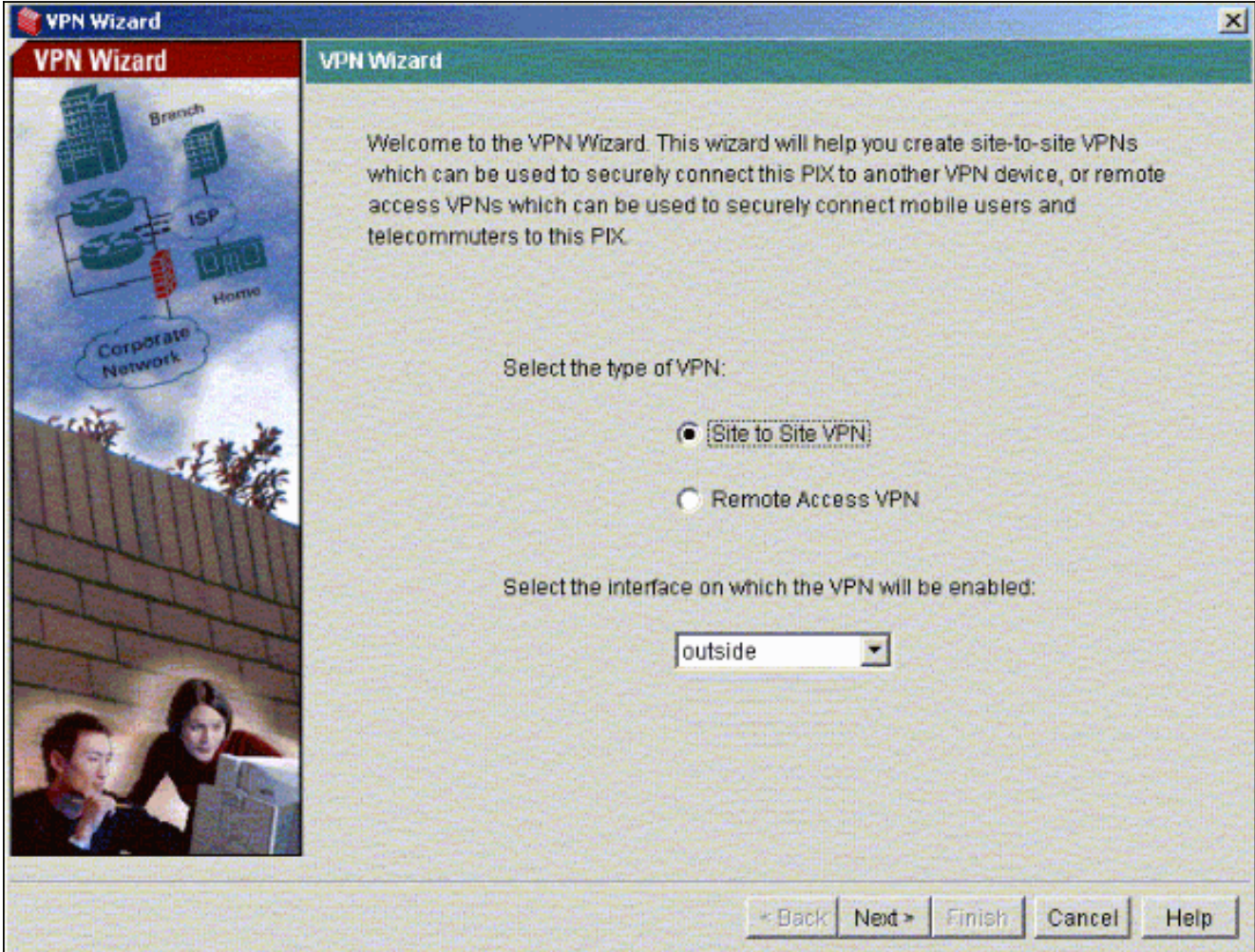
عندما تكتب [https://<Inside\\_IP\\_ADDRESS\\_on\\_PIX](https://<Inside_IP_ADDRESS_on_PIX) والنقر فوق علامة التبويب VPN لأول مرة، قم بعرض معلومات حول معالج VPN التلقائي.



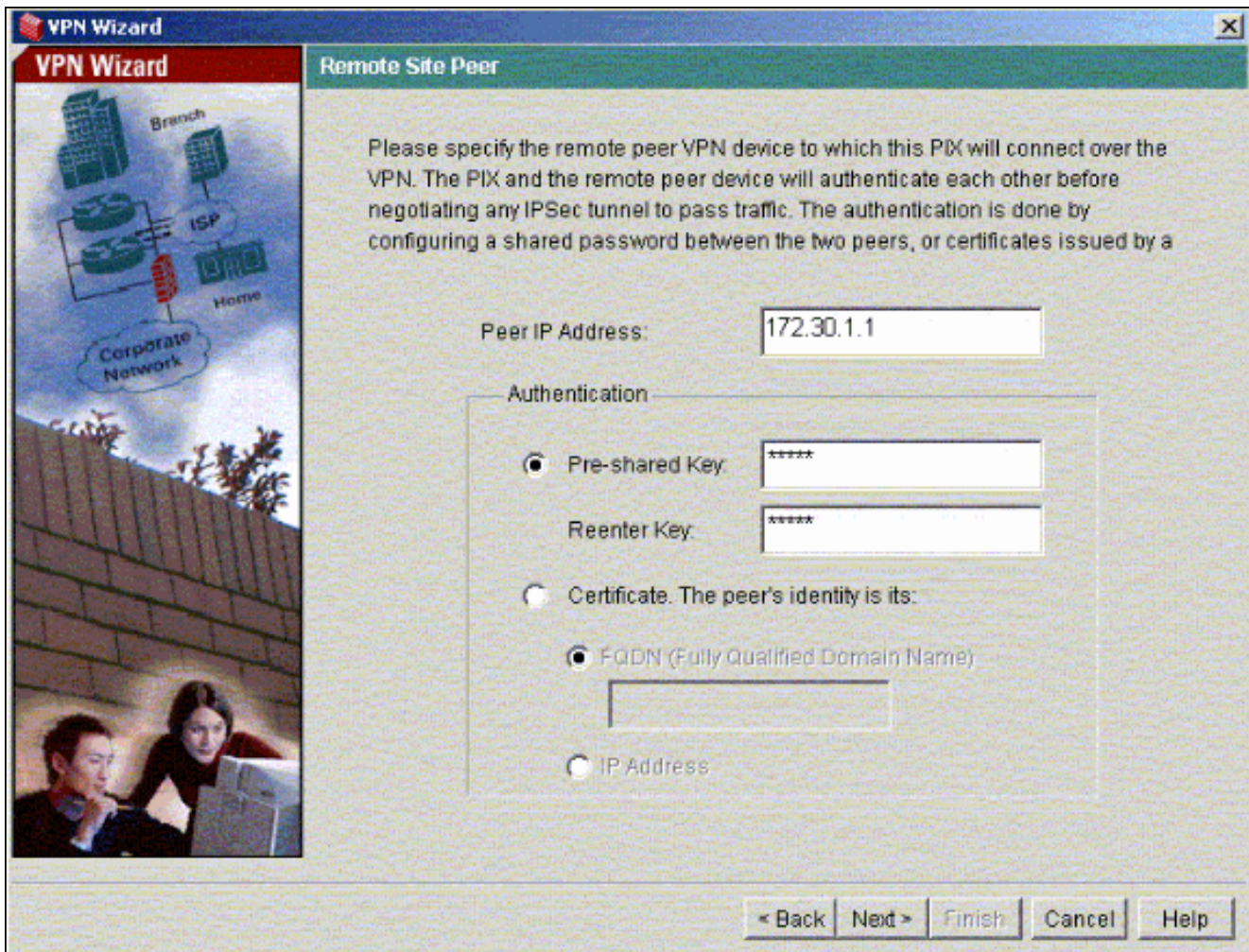
1. حدد المعالجات < معالج  
.VPN



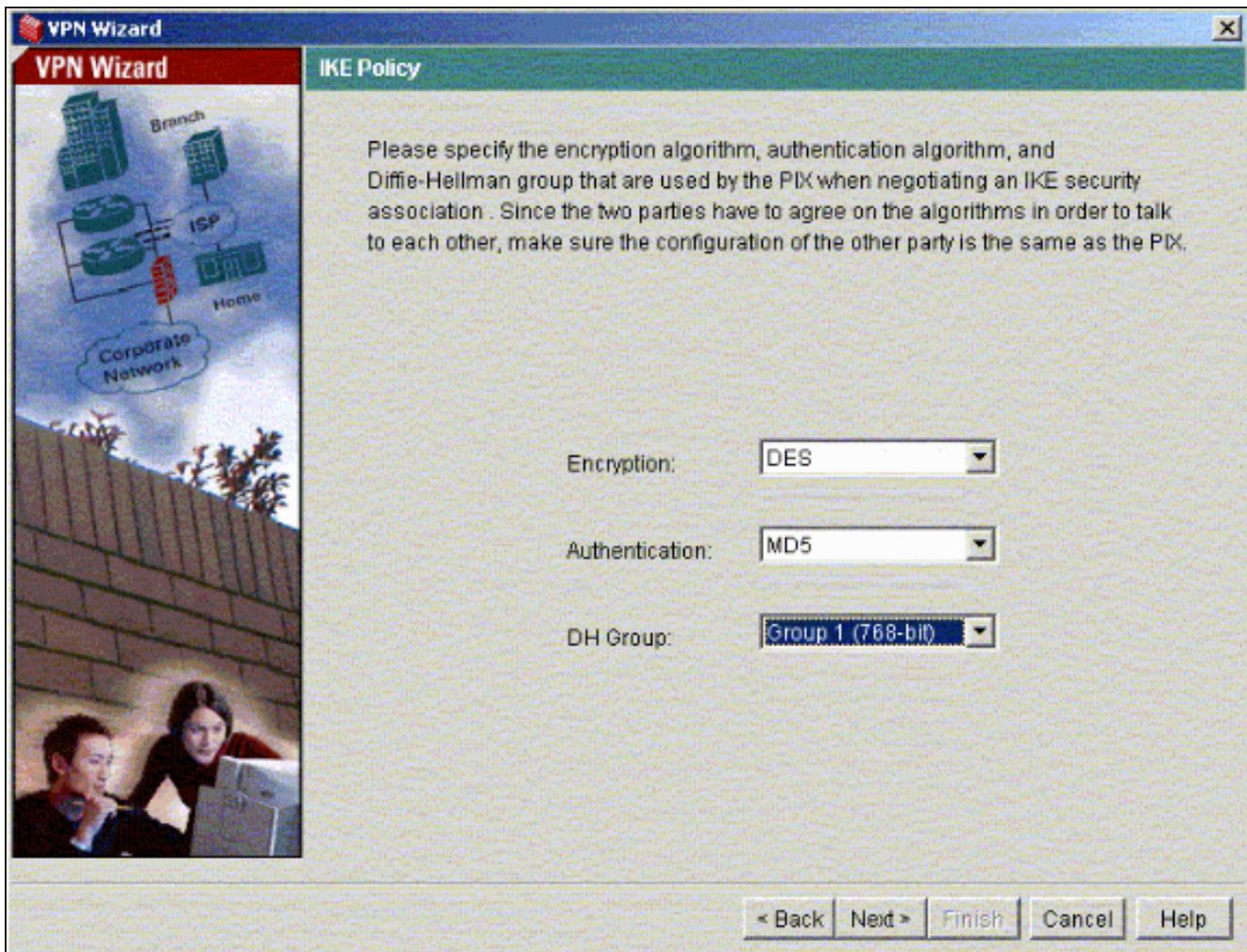
2. يبدأ معالج VPN وبطالبك بنوع شبكة VPN التي تريد تكوينها. اخترت موقع إلى موقع VPN، القارن خارجي بما أن القارن أي ال VPN يكون مكنت، وطقطقة بعد ذلك.



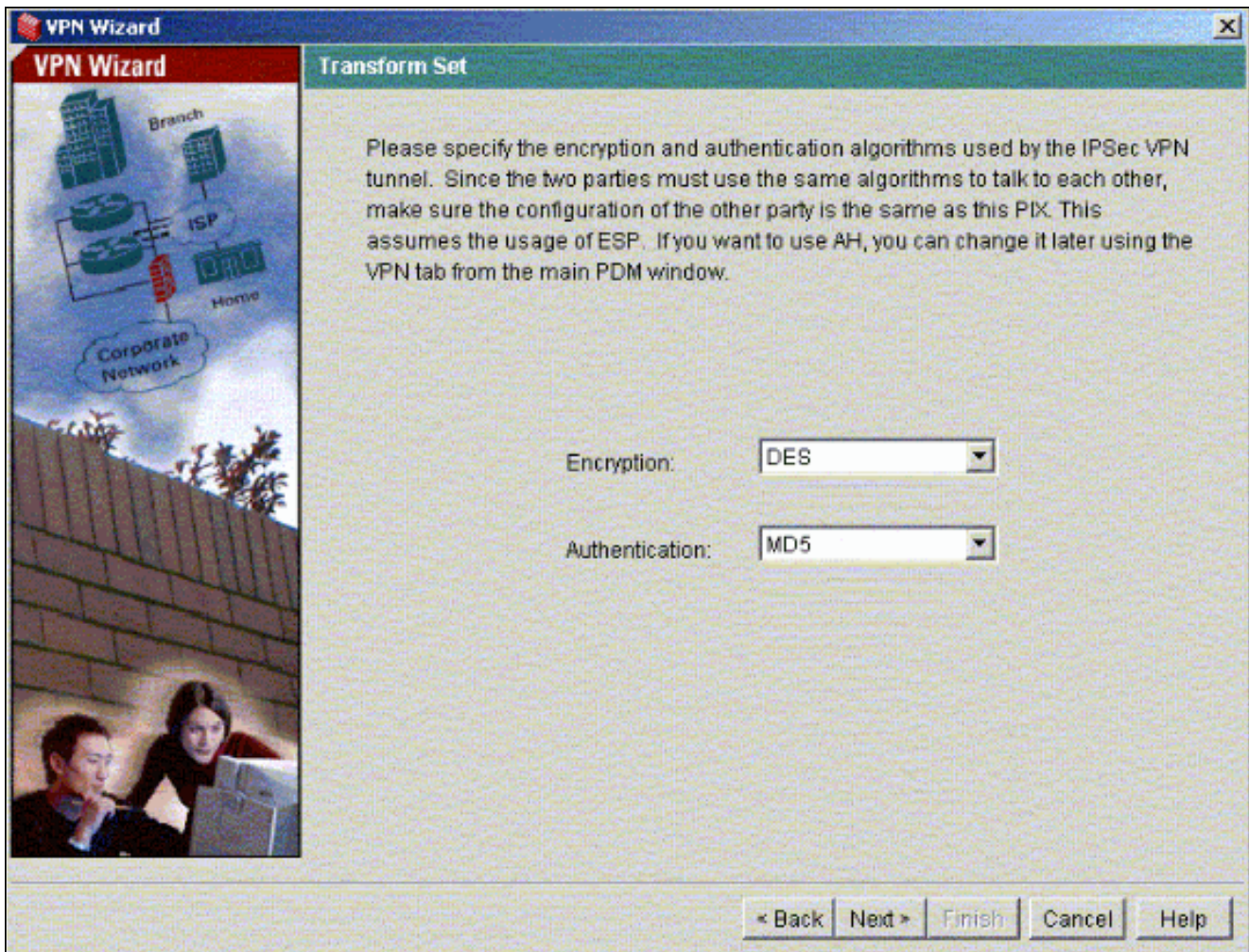
3. أدخل عنوان IP للنظير، حيث يجب أن ينتهي نفق IPsec. في هذا المثال، ينتهي النفق على الواجهة الخارجية ل PIX-02. انقر فوق Next (التالي).



4. أدخل معلومات نهج IKE التي تختار إستخدامها وانقر فوق التالي.




5. قم بتوفير معلمات التشفير والمصادقة لمجموعة التحويل وانقر فوق التالي.



6. حدد الشبكة المحلية والشبكات البعيدة التي تحتاج إلى حمايتها باستخدام IPsec لتحديد حركة المرور المثيرة للاهتمام التي تحتاج إلى حمايتها.

**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:

10.1.1.0/24

**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:

172.30.0.0/16



## التحقق من الصحة

إذا كان هناك حركة مرور مثيرة للانتباه إلى النظير، يتم إنشاء النفق بين PIX-01 و PIX-02.

للتحقق من ذلك، قم بإيقاف تشغيل الواجهة التسلسلية R1 التي تم إنشاء النفق من أجلها بين PIX-01 و PIX-02 عبر R2 عند وجود حركة مرور مثيرة للاهتمام.

اعرض حالة شبكة VPN ضمن الصفحة الرئيسية في PDM (مميزة بالأحمر) للتحقق من تكوين النفق.

The screenshot displays the Cisco PIX Device Manager 3.0 interface. The 'VPN Status' section is highlighted with a red box, showing 1 IKE Tunnel and 1 IPSec Tunnel. The 'System Resources Status' section shows CPU usage at 0% and memory usage at 18MB. The 'Interface Status' table shows the 'inside' interface is up with 7 Kbps current traffic, while other interfaces are down. The 'Traffic Status' section includes graphs for Connections Per Second Usage and 'outside' Interface Traffic Usage (Kbps).

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

يمكنك أيضا التحقق من تكوين الأنفاق باستخدام CLI تحت أدوات في PDM. قم بإصدار الأمر `show crypto isakmp sa` للتحقق من تكوين الأنفاق وأصدر الأمر `show crypto ipSec` لمراقبة عدد الحزم التي تم تكوينها، وتشغيلها، وما إلى ذلك.

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر `show`.

راجع مدير أجهزة PIX 3.0 من Cisco للحصول على مزيد من المعلومات حول تكوين جدار حماية PIX باستخدام PDM.

## استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

### معلومات ذات صلة

- [تكوين نفق VPN بسيط من PIX إلى PIX باستخدام IPsec](#)
- [برنامج جدار حماية Cisco PIX](#)
- [مراجع أوامر جدار حماية PIX الآمن من Cisco](#)
- [طلبات التعليقات \(RFCs\)](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد عوچرلاب يصوت وتامچرتل هذه ةقدنع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) يلصلأل يزي لچنإل دن تسمل