

PIX يتحتف ني ب LAN إلى LAN نم VPN ق فن PDM ني وكت لاثم مادختساب

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الرسم التخطيطي للشبكة](#)
- [الاصطلاحات](#)
- [معلومات أساسية](#)
- [إجراء التكوين](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يصف هذا المستند إجراء تكوين أنفاق VPN بين جدرتي حماية PIX باستخدام مدير جهاز PDM (PIX) من Cisco. PDM هي أداة تكوين قائمة على المستعرض تم تصميمها لتساعدك في إعداد جدار حماية PIX لديك وتكوينه ومراقبته باستخدام واجهة المستخدم الرسومية (GUI). يتم وضع جدران الحماية من طراز PIX في موقعين مختلفين.

يتم تكوين نفق باستخدام IPsec. IPsec هو مجموعة من المعايير المفتوحة التي توفر سرية البيانات وسلامة البيانات ومصادقة أصل البيانات بين نظائر IPsec.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات لهذا المستند.

المكونات المستخدمة

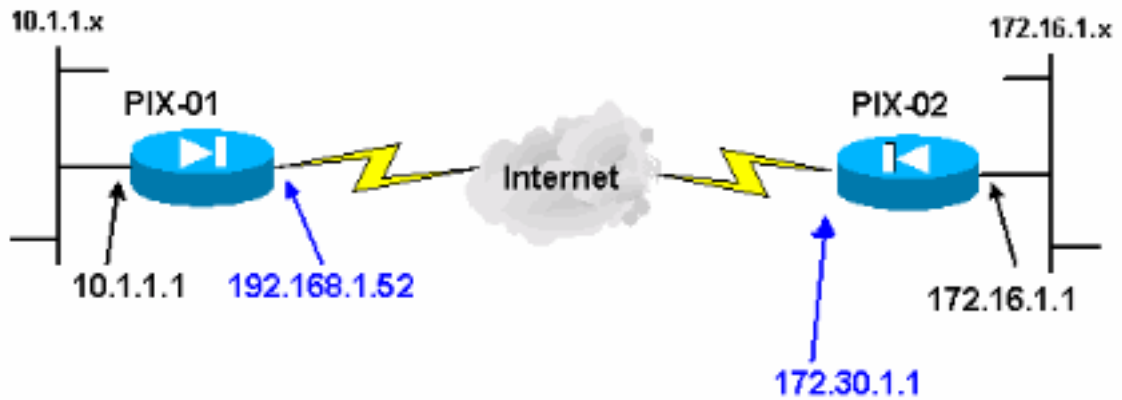
تستند المعلومات الواردة في هذا المستند إلى جدران الحماية Cisco Secure PIX 515e مع الإصدار x.6 و PDM الإصدار 3.0.

ارجع إلى [تكوين نفق VPN بسيط من PIX إلى PIX باستخدام IPsec](#) للحصول على مثال تكوين نفق VPN بين جهازي PIX باستخدام واجهة سطر الأوامر (CLI).

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



الاصطلاحات

راجع اصطلاحات تلميح 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).

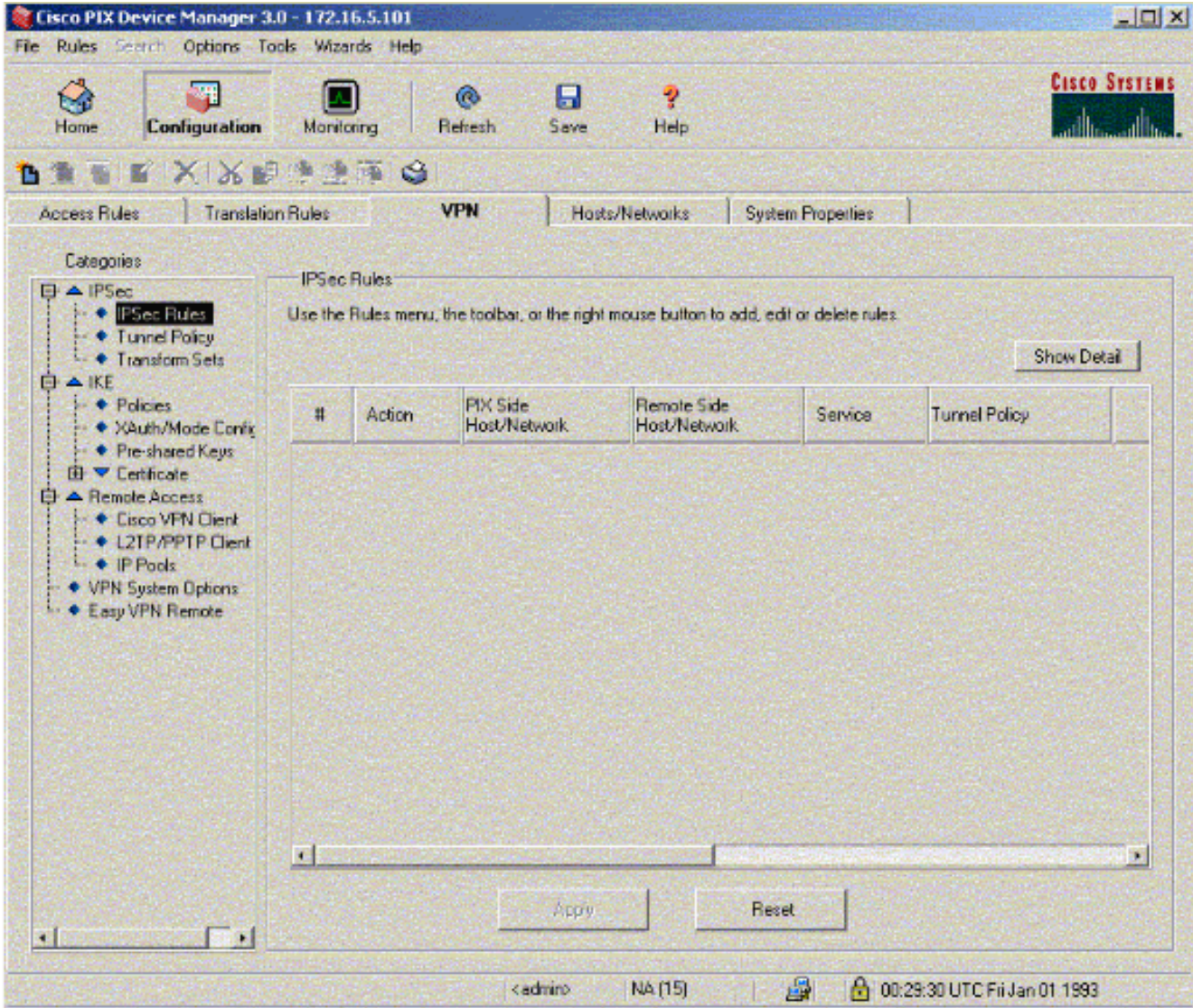
1. يتم بدء نفق IPsec بواسطة حركة مرور مثيرة للاهتمام. تعتبر حركة المرور مثيرة للاهتمام عندما تنتقل بين نظائر IPsec.
2. في المرحلة الأولى من IKE، يتفاوض نظراء IPsec على سياسة اقتران أمان (SA) (IKE) التي تم إنشاؤها. بمجرد مصادقة النظراء، يتم إنشاء نفق آمن باستخدام بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (ISAKMP).
3. 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.
4. يتم إنشاء نفق IPsec ويتم نقل البيانات بين نظائر IPsec استناداً إلى معلمات IPsec التي تم تكوينها في مجموعات تحويل IPsec.
5. 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 النظرير.

إجراء التكوين

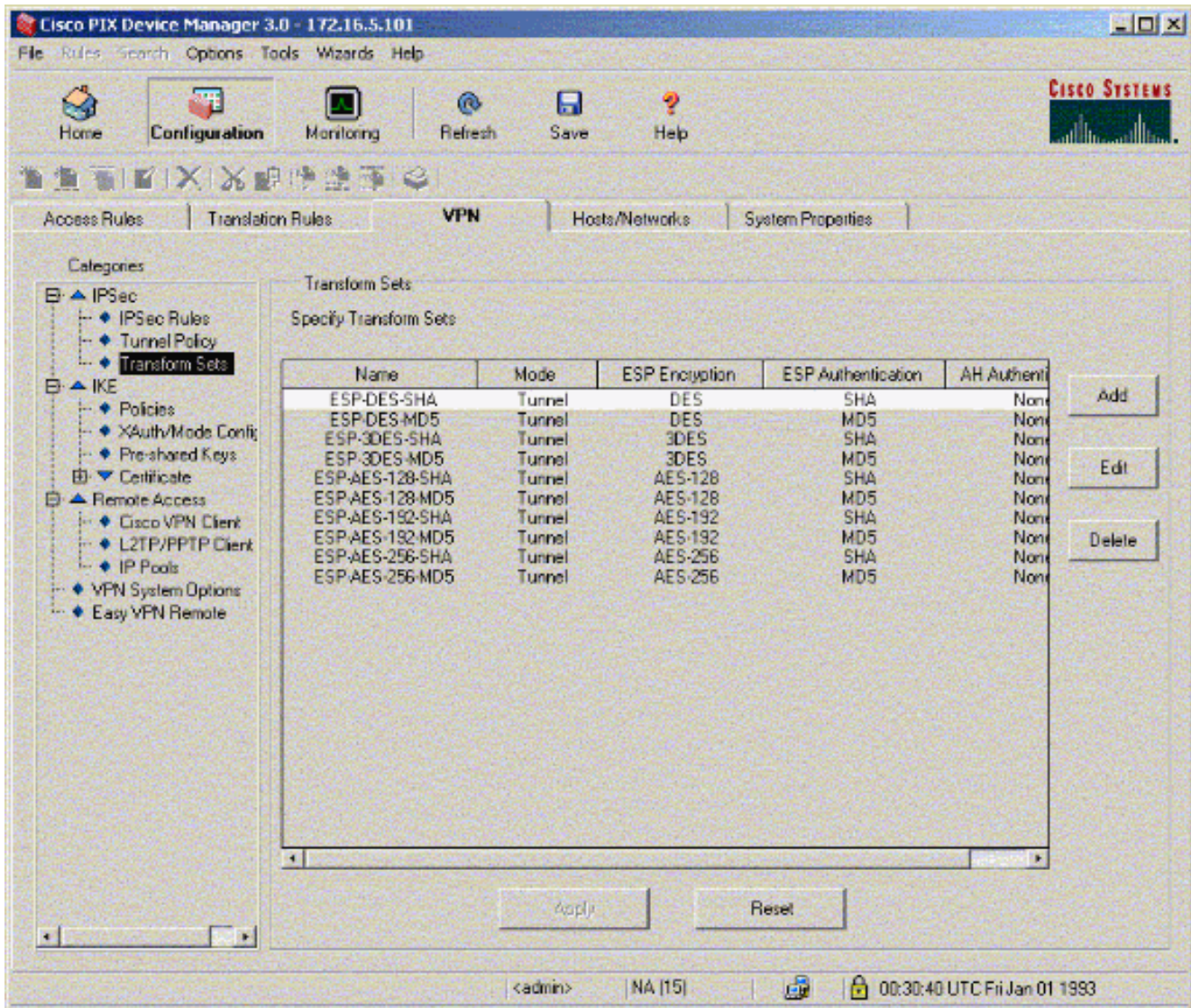
بخلاف التكوين العام الآخر على CLI من PIX للوصول إليه من خلال واجهة إيثرنت 0، أستخدم الأوامر `http server enable` و `interface <local_ip> <mask>` حيث يكون `<local_ip>` و `<mask>` عنوان IP وقناع محطة العمل التي يتم تثبيت PDM عليها. التكوين الموجود في هذا المستند ل PIX-01. يمكن تكوين PIX-02 باستخدام الخطوات نفسها ذات العناوين المختلفة.

أكمل الخطوات التالية:

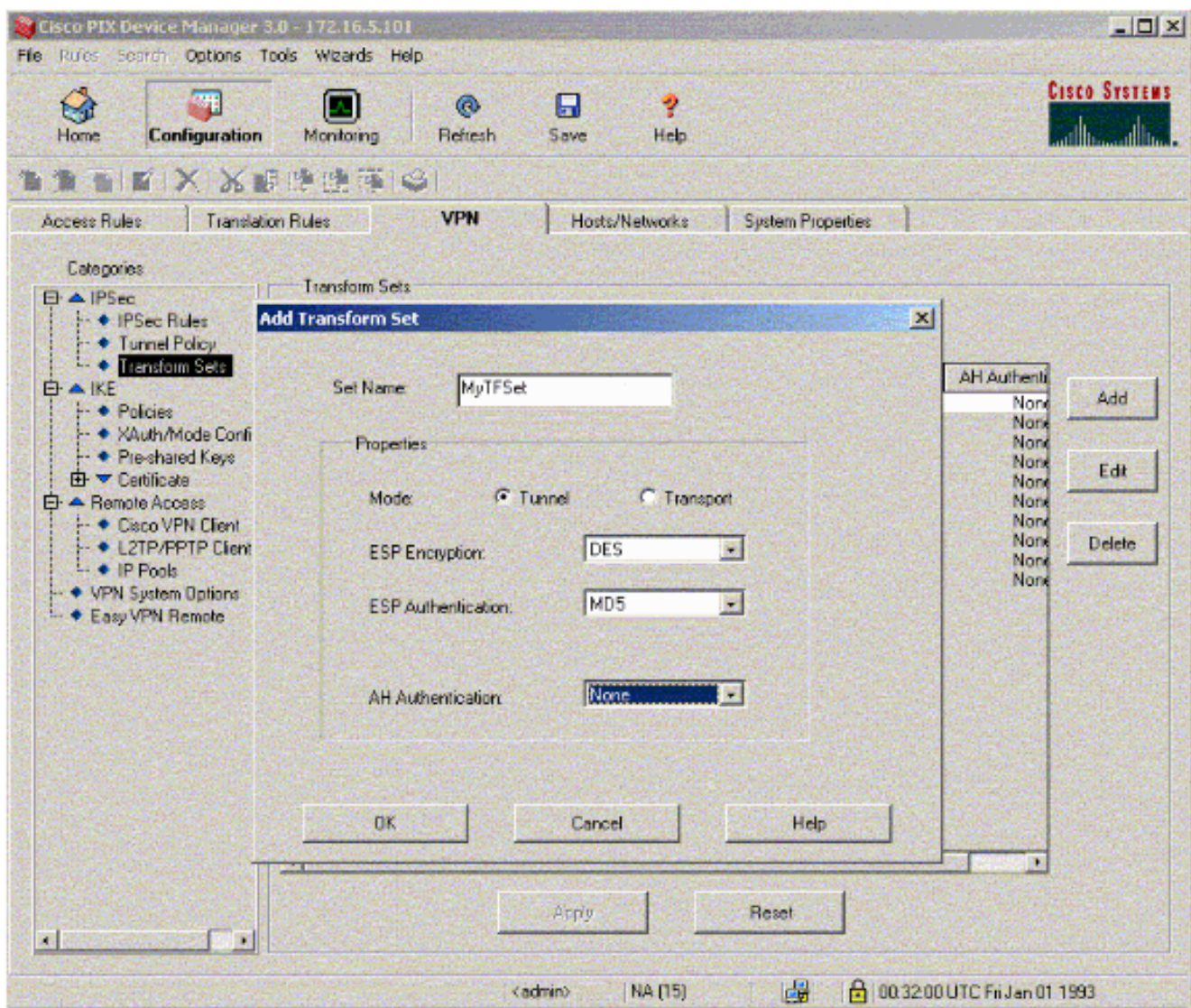
1. افتح المستعرض واكتب https://<inside_ip_address_of_pix> للوصول إلى PIX في PDM.
2. انقر فوق التكوين وانتقل إلى علامة التبويب .VPN



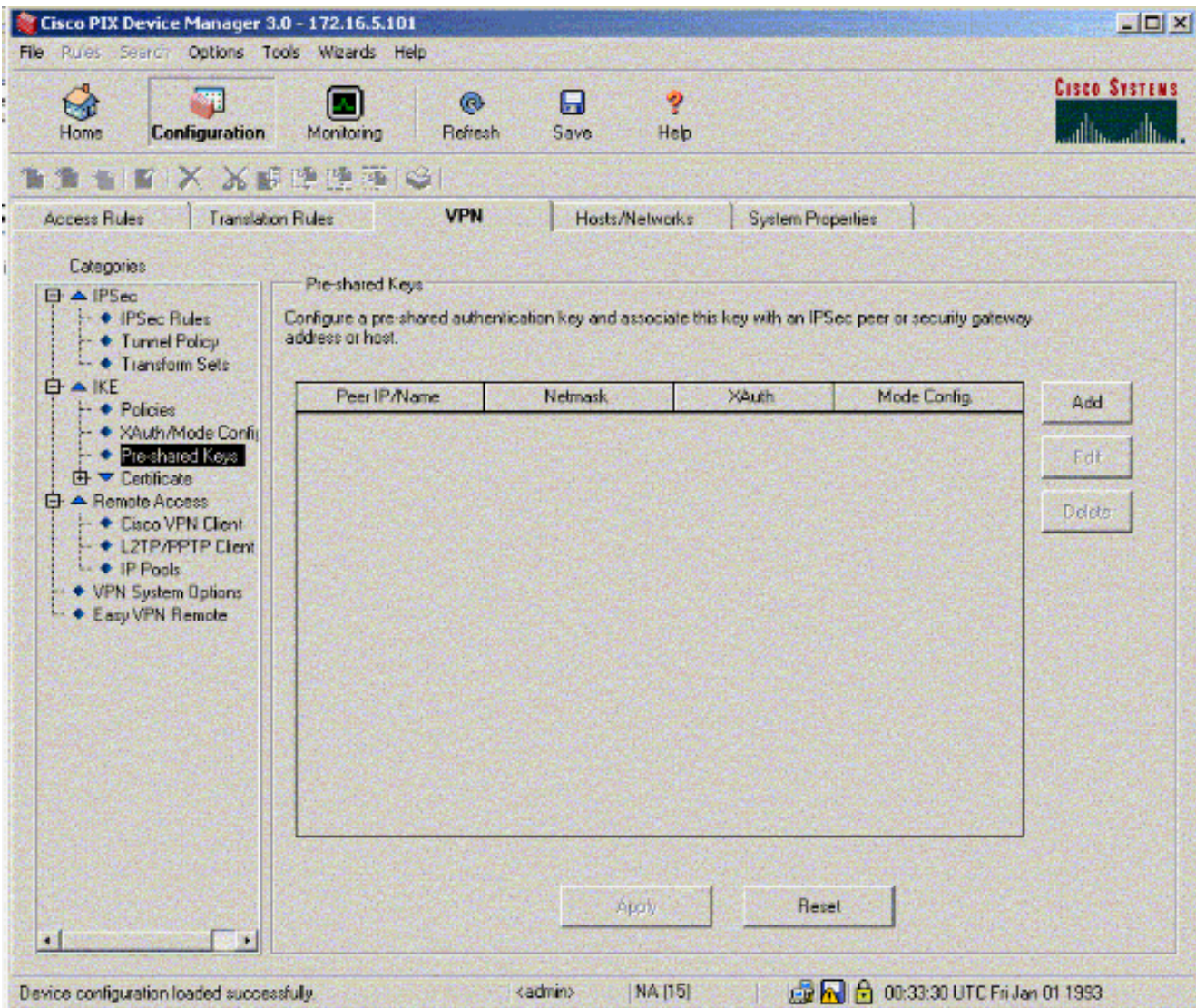
3. انقر فوق مجموعات التحويل ضمن IPSec لإنشاء مجموعة تحويل.



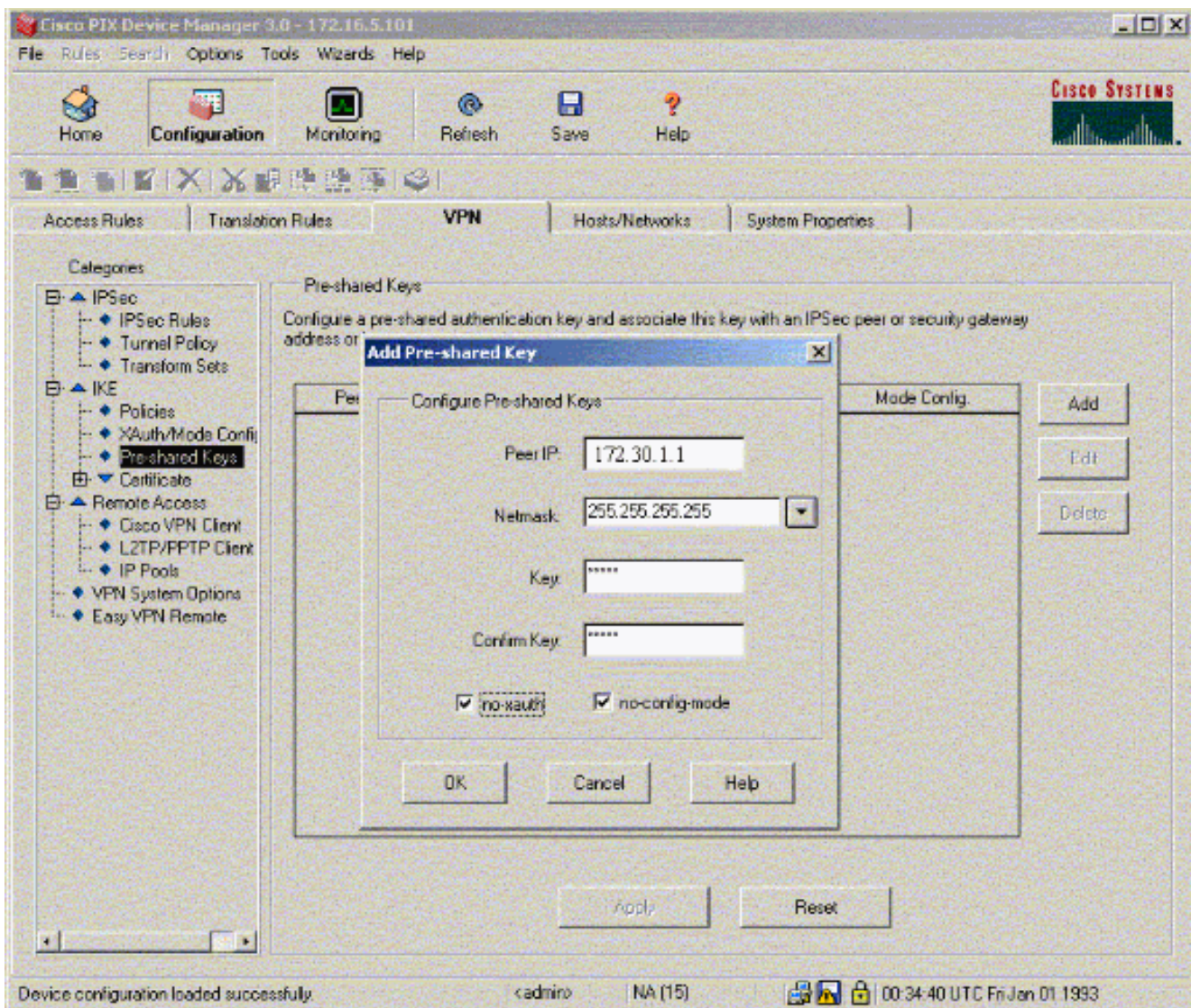
4. انقر إضافة، حدد كل الخيارات المناسبة، وانقر موافق لإنشاء مجموعة تحويل جديدة.



5. انقر فوق مفاتيح مشتركة مسبقا ضمن IKE لتكون المفاتيح المشتركة مسبقاً.



6. انقر فوق إضافة لإضافة مفتاح جديد مشترك مسبقاً.



بيدي هذا نافذة المفتاح، أي يكون الكلمة لاقتران نفق. يجب أن يتطابق هذا على جانبي النفق.

Cisco PIX Device Manager 3.0 - 172.16.5.101

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Refresh Save Help

Access Rules Translation Rules **VPN** Hosts/Networks System Properties

Categories

- IPSec
 - IPSec Rules
 - Tunnel Policy
 - Transform Sets
- IKE
 - Policies
 - XAuth/Mode Config
 - Pre-shared Keys**
 - Certificate
- Remote Access
 - Cisco VPN Client
 - L2TP/PPTP Client
 - IP Pools
 - VPN System Options
 - Easy VPN Remote

Pre-shared Keys

Configure a pre-shared authentication key and associate this key with an IPSec peer or security gateway address or host.

Peer IP/Name	Netmask	XAuth	Mode Config
172.16.5.102	255.255.255.255	disabled	disabled

Buttons: Add, Edit, Delete, Apply, Reset

Device configuration loaded successfully. <admin> NA (15) 00:35:10 UTC Fri Jan 01 1993

7. انقر فوق السياسات ضمن IKE لتكوين السياسات.

Cisco PIX Device Manager 3.0 - 172.16.5.101

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Refresh Save Help

Access Rules Translation Rules **VPN** Hosts/Networks System Properties

Categories

- IPSec
 - IPSec Rules
 - Tunnel Policy
 - Transform Sets
- IKE
 - Policies**
 - XAuth/Mode Config
 - Pre-shared Keys
 - Certificate
- Remote Access
 - Cisco VPN Client
 - L2TP/PPTP Client
 - IP Pools
 - VPN System Options
 - Easy VPN Remote

Policies

Configure the Internet Security Association and Key Management Protocol policies. These policies will negotiate the IKE security associations and enable secure communications.

Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime[secs]

Add Edit Delete

General Information

Interface	IKE Enabled
inside	false
in112	false
outside	false

Enable Disable

Identity: Key Id String:

Enable NAT Traversal NAT Keepalive: [secs]

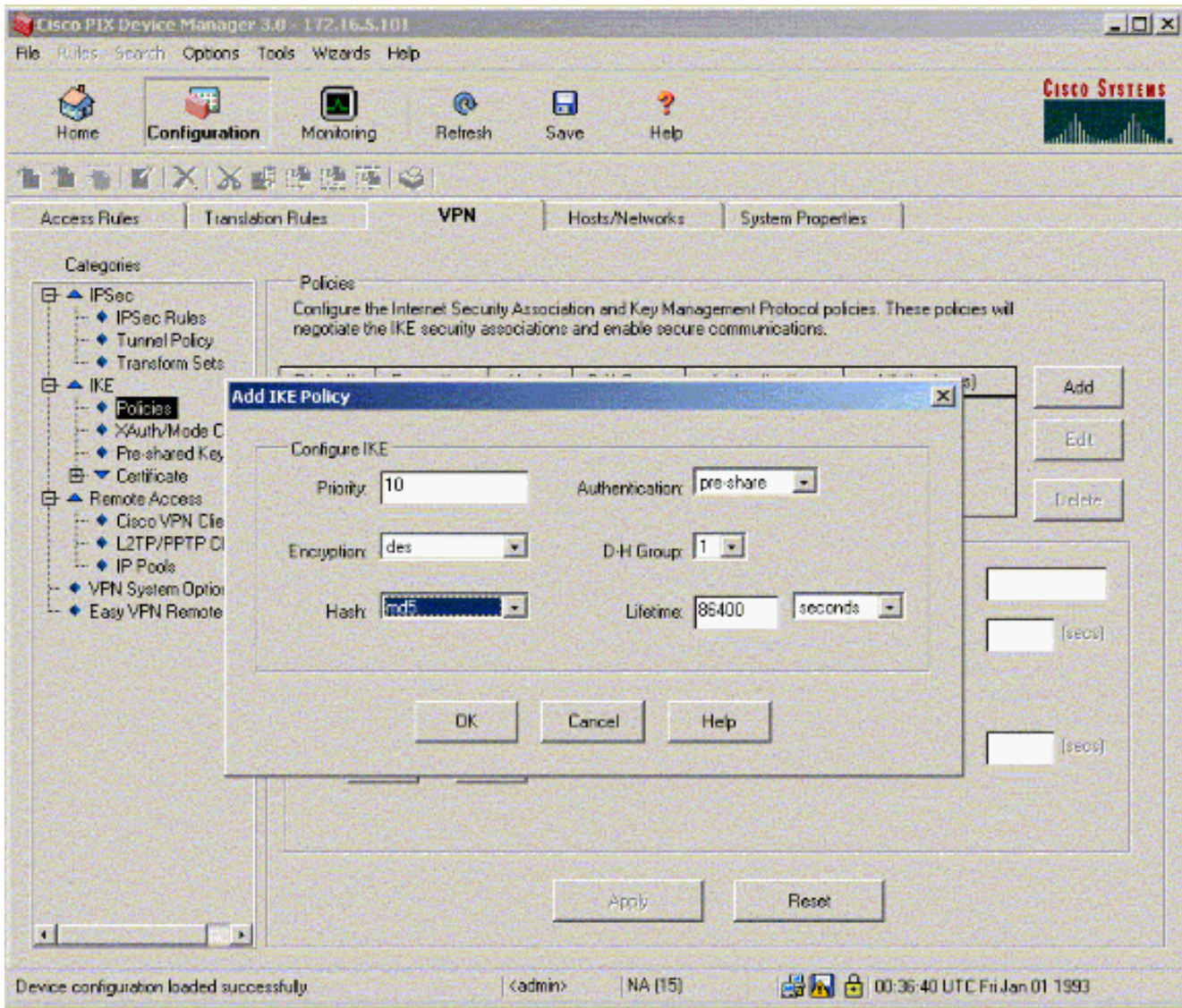
Set Keepalive & Retry values

Keepalive: [secs] Retry: [secs]

Apply Reset

Device configuration loaded successfully. <admin> | NA (15) | 00:35:50 UTC Fri Jan 01 1993

8. انقر فوق إضافة وتعينة الحقول المناسبة.



9. انقر فوق موافق لإضافة نهج جديد.

Cisco PIX Device Manager 3.0 - 172.16.5.101

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Refresh Save Help

Access Rules Translation Rules **VPN** Hosts/Networks System Properties

Categories

- IPSec
 - IPSec Rules
 - Tunnel Policy
 - Transform Sets
- IKE
 - Policies**
 - Auth/Mode Config
 - Pre-shared Keys
 - Certificate
- Remote Access
 - Cisco VPN Client
 - L2TP/PPTP Client
 - IP Pools
 - VPN System Options
 - Easy VPN Remote

Policies

Configure the Internet Security Association and Key Management Protocol policies. These policies will negotiate the IKE security associations and enable secure communications.

Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)
10	des	md5	1	pre-share	86400

Buttons: Add, Edit, Delete

General Information

Interface	IKE Enabled
inside	false
int2	false
outside	false

Buttons: Enable, Disable

Identity: hostname Key Id String:

Enable NAT Traversal NAT Keepalive: (secs)

Set Keepalive & Retry values

Keepalive: (secs) Retry: (secs)

Buttons: Apply, Reset

Device configuration loaded successfully. | admin | NA (15) | 00:37:00 UTC Fri Jan 01 1993

10. حدد الواجهة الخارجية، انقر فوق تمكين، ثم حدد العنوان من القائمة المنسدلة للهوية.

Cisco PIX Device Manager 3.0 - 172.16.5.101

File Rules Search Options Tools Wizards Help

Home Configuration Monitoring Refresh Save Help

Access Rules Translation Rules **VPN** Hosts/Networks System Properties

Categories

- IPSec
 - IPSec Rules
 - Tunnel Policy
 - Transform Sets
- IKE
 - Policies**
 - XAuth/Mode Config
 - Pre-shared Keys
- Certificate
- Remote Access
 - Cisco VPN Client
 - L2TP/PPTP Client
 - IP Pools
- VPN System Options
- Easy VPN Remote

Policies

Configure the Internet Security Association and Key Management Protocol policies. These policies will negotiate the IKE security associations and enable secure communications.

Priority #	Encryption	Hash	D-H Group	Authentication	Lifetime(secs)
10	des	md5	1	pre-share	86400

Buttons: Add, Edit, Delete

General Information

Interface	IKE Enabled
inside	false
intf2	false
outside	true

Buttons: Enable, Disable

Identity: KeyID String:

Enable NAT Traversal NAT Keepalive: (secs)

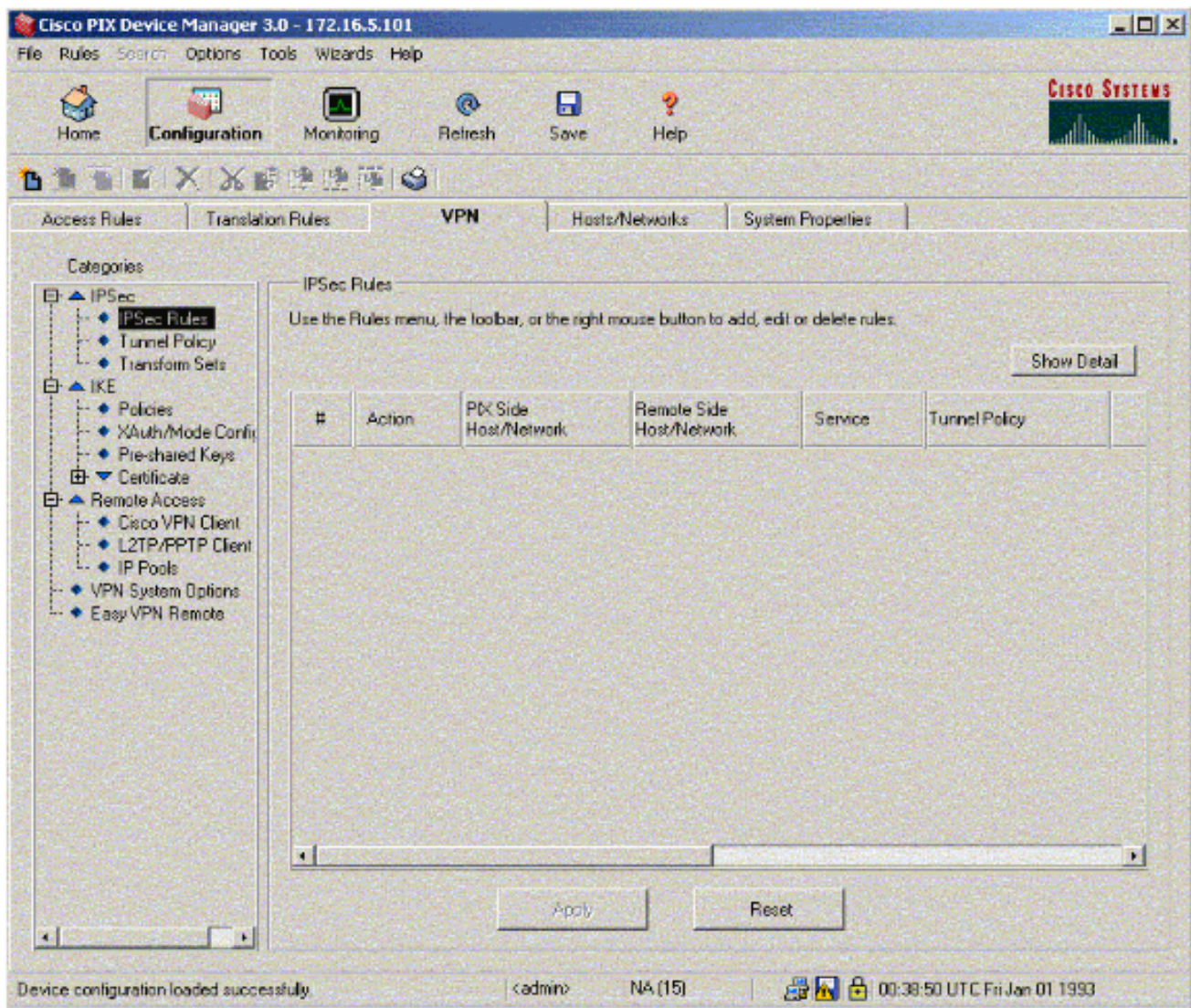
Set Keepalive & Retry values

Keepalive: (secs) Retry: (secs)

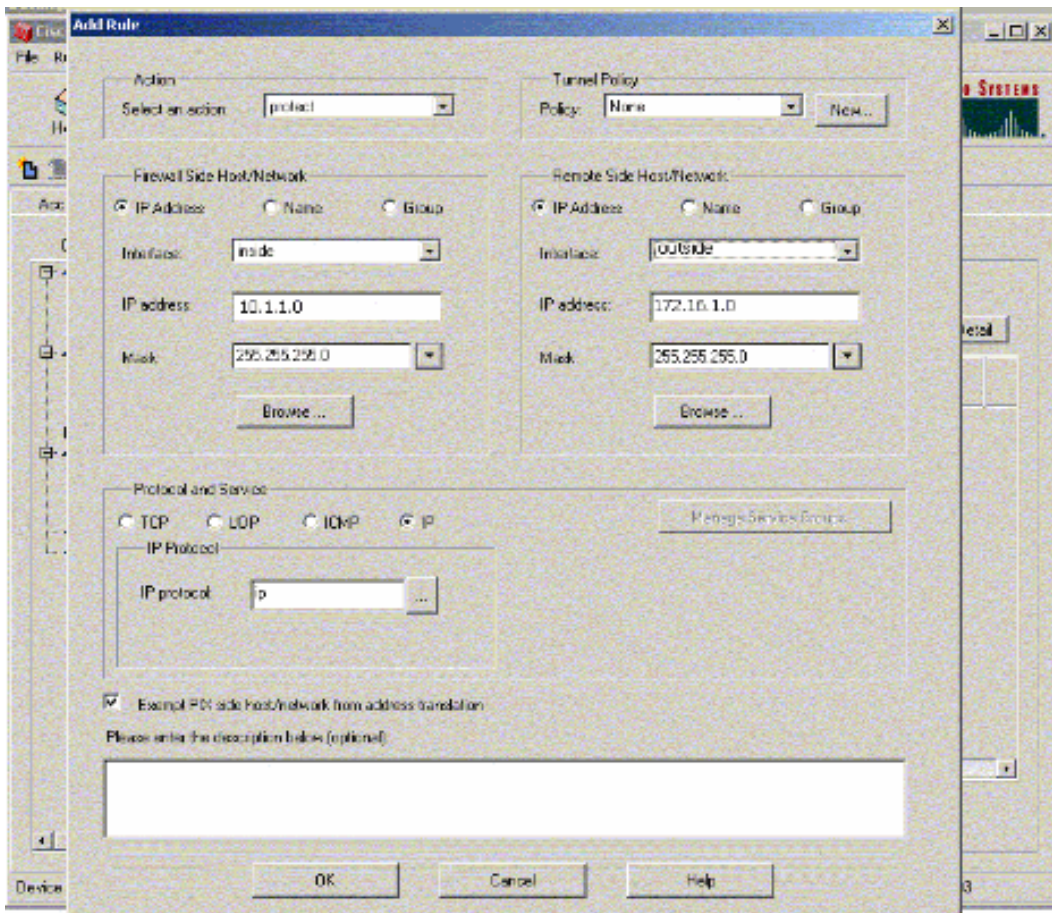
Buttons: Apply, Reset

Device configuration loaded successfully. <admin> NA (15) 00:38:00 UTC Fri Jan 01 1993

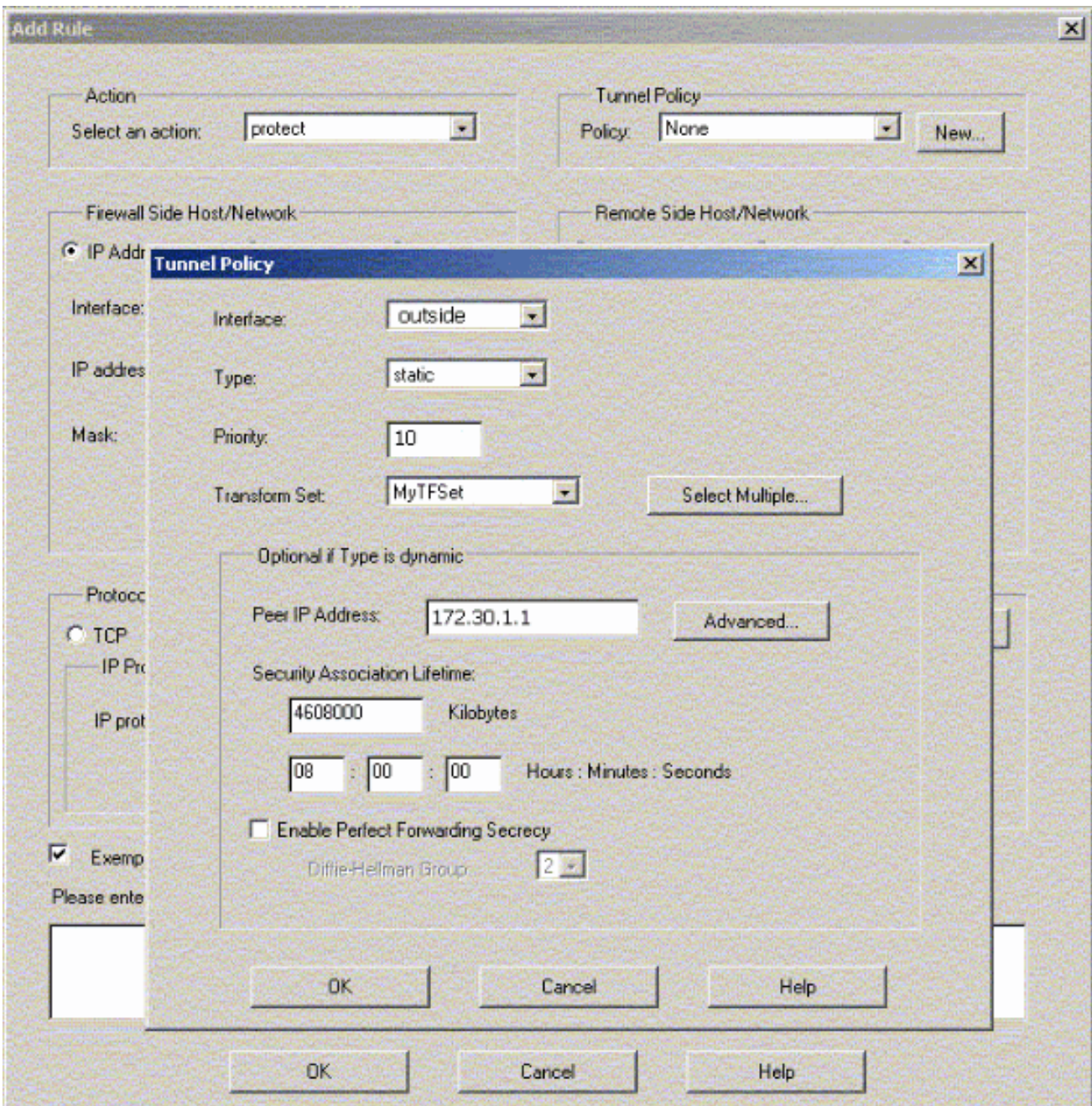
11. انقر فوق قواعد IPSec ضمن إنشاء قواعد IPSec.



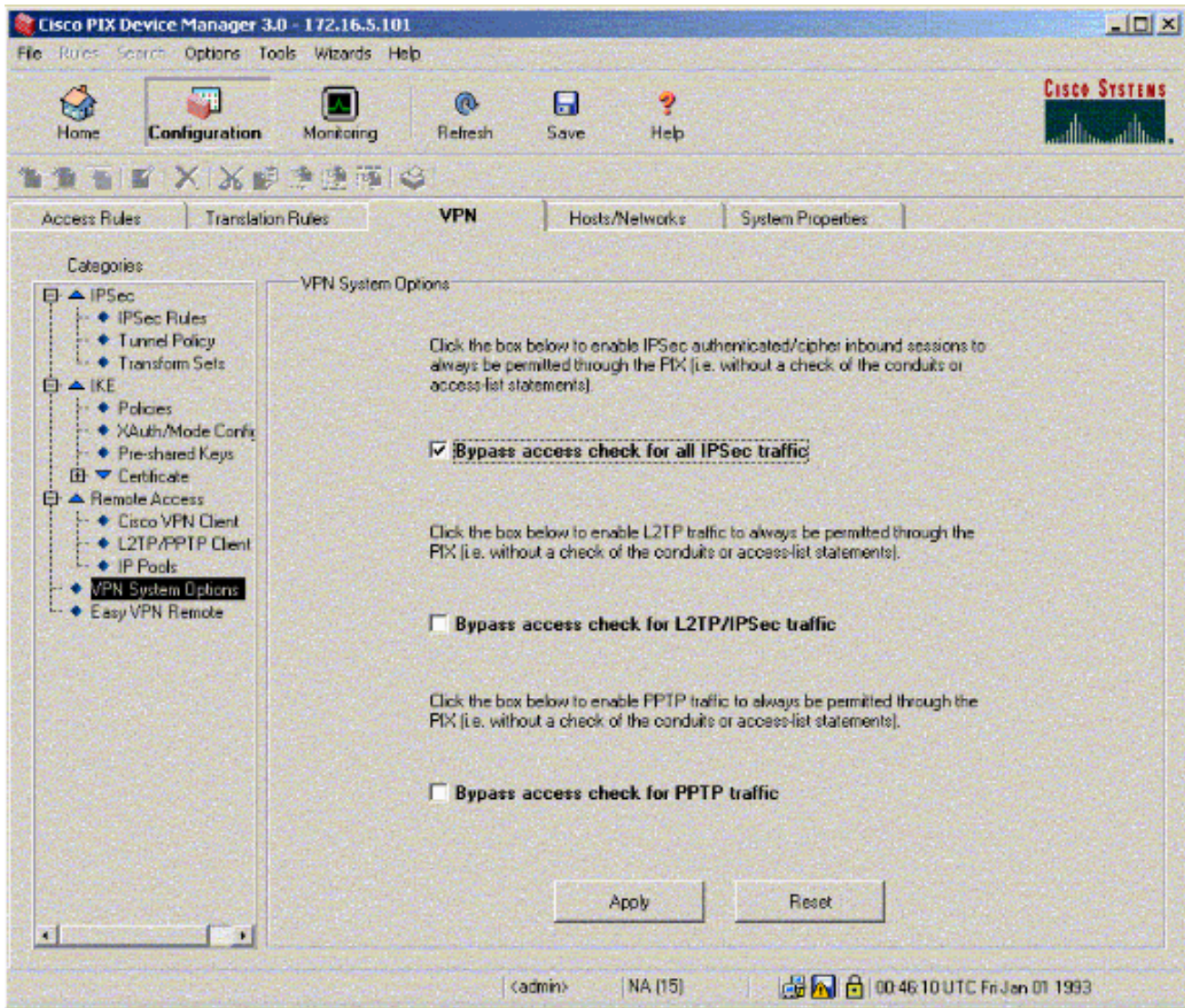
12. املأ الحقول المناسبة.



13. انقر فوق جديد في نهج النفق. تظهر نافذة نهج نفق. املأ الحقول المناسبة.



14. انقر فوق موافق لعرض قاعدة IPsec التي تم تكوينها.
15. انقر فوق خيارات أنظمة VPN وحدد التحقق من الوصول الالتفافي لجميع حركة مرور IPsec.

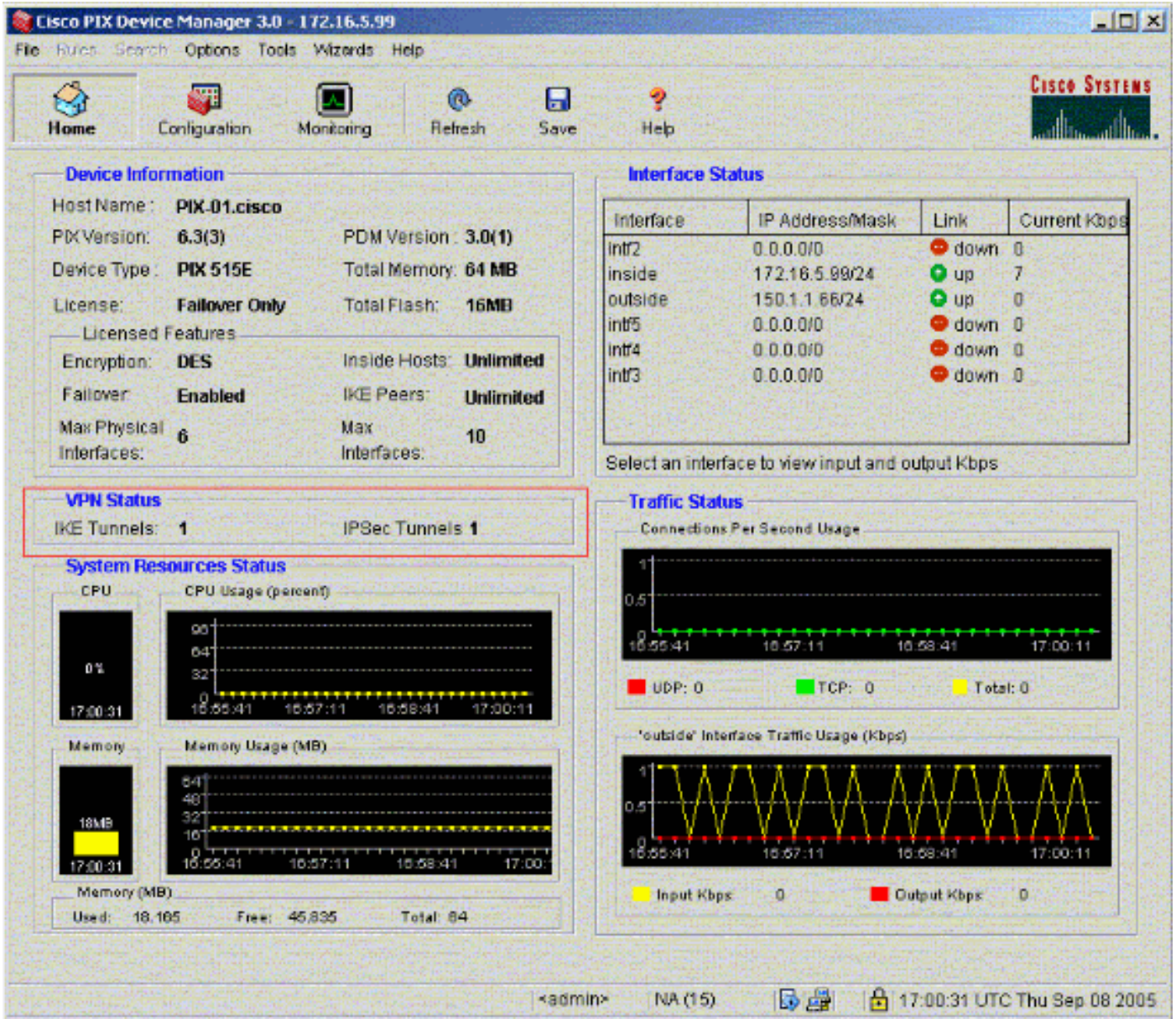


التحقق من الصحة

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

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

اعرض حالة الشبكة الخاصة الظاهرية (VPN) ضمن الصفحة الرئيسية في PDM (مبرزة بالأحمر) للتحقق من تكوين النفق.



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.

ملاحظة: لا يمكن إدخال الواجهة الداخلية ل PIX لتكوين النفق ما لم يتم تكوين الأمر `management-access` في وضع التأكيد العام.

```
PIX-02 (config) #management-access inside
PIX-02 (config) #show management-access
management-access inside
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- [إنشاء نفق متكرر بين جدران الحماية باستخدام PDM](#)
- [مراجع أوامر جدار حماية PIX الآمن من Cisco](#)

- [طلبات التعليقات \(RFCs\)](#)
- [برنامج جدار حماية Cisco PIX](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س مل ا ذه Cisco ت مچرت
م ل اع ل اء ن ا ع مچ ي ف ن م دخت س مل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س مل ا