نفق VPN من LAN إلى LAN بين فتحتي PIX باستخدام مثال تكوين PDM

المحتويات

المقدمة

يصف هذا المستند إجراء تكوين أنفاق VPN بين جدرتي حماية PIX باستخدام مدير جهاز PIX (PDM) 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.

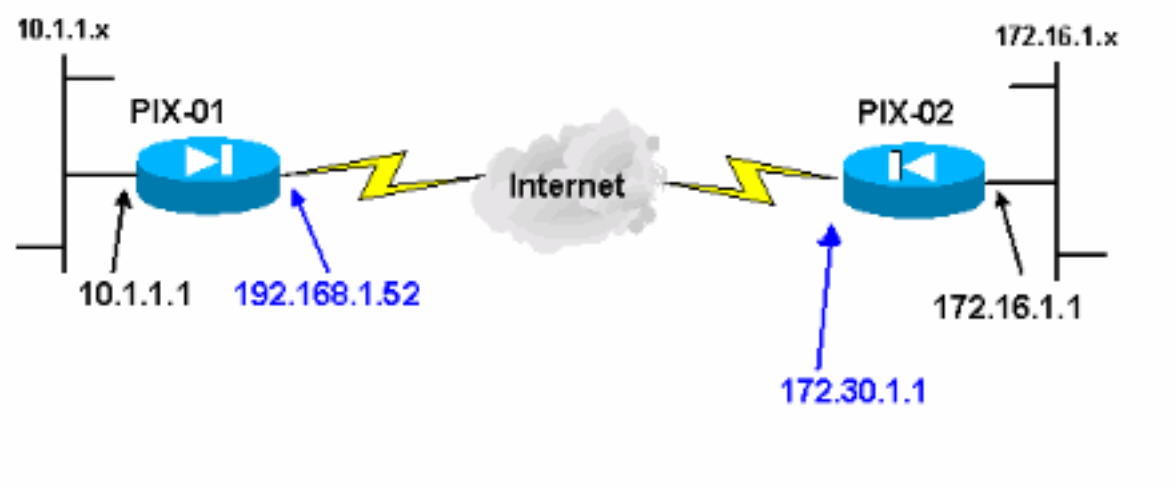
ارجع إلى تكوين نفق VPN بسيط من PIX إلى PIX باستخدام IPsec للحصول على مثال تكوين على تكوين نفق VPN بين جهازي PIX باستخدام واجهة سطر الأوامر (CLI).

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

أمر.

الرسم التخطيطي 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).

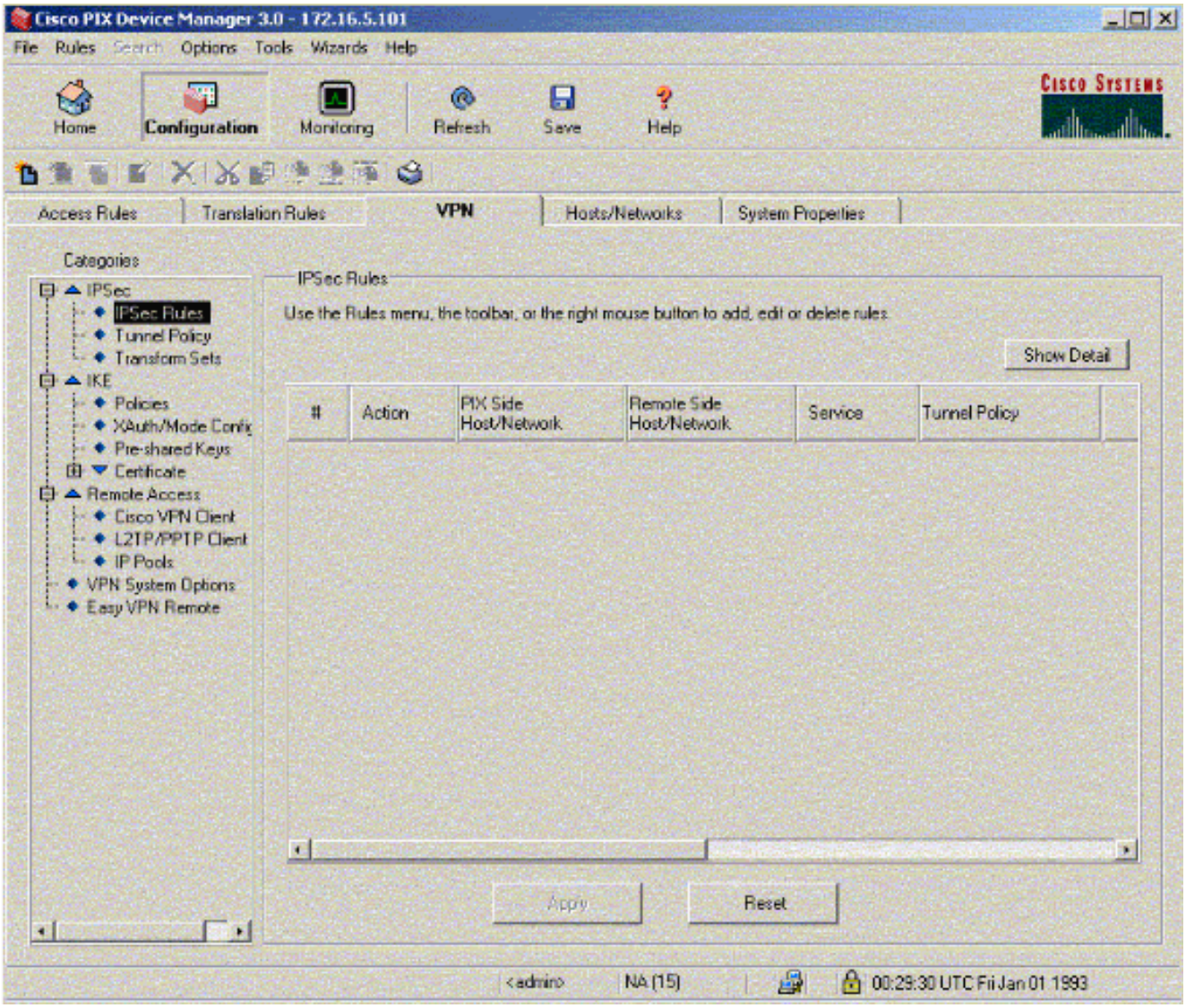
1. يتم بدء نفق IPsec بواسطة حركة مرور مثيرة للاهتمام. تعتبر حركة المرور مثيرة للاهتمام عندما تنتقل بين نظائر IPsec.
2. في المرحلة الأولى من IKE، يتفاوض نظراء IPsec على سياسة اقتران أمان IKE (SA) التي تم إنشاؤها. بمجرد مصادقة النظراء، يتم إنشاء نفق آمن باستخدام بروتوكول إدارة المفاتيح وارتباط أمان الإنترنت (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 استنادا 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 النظير.

إجراء التكوين

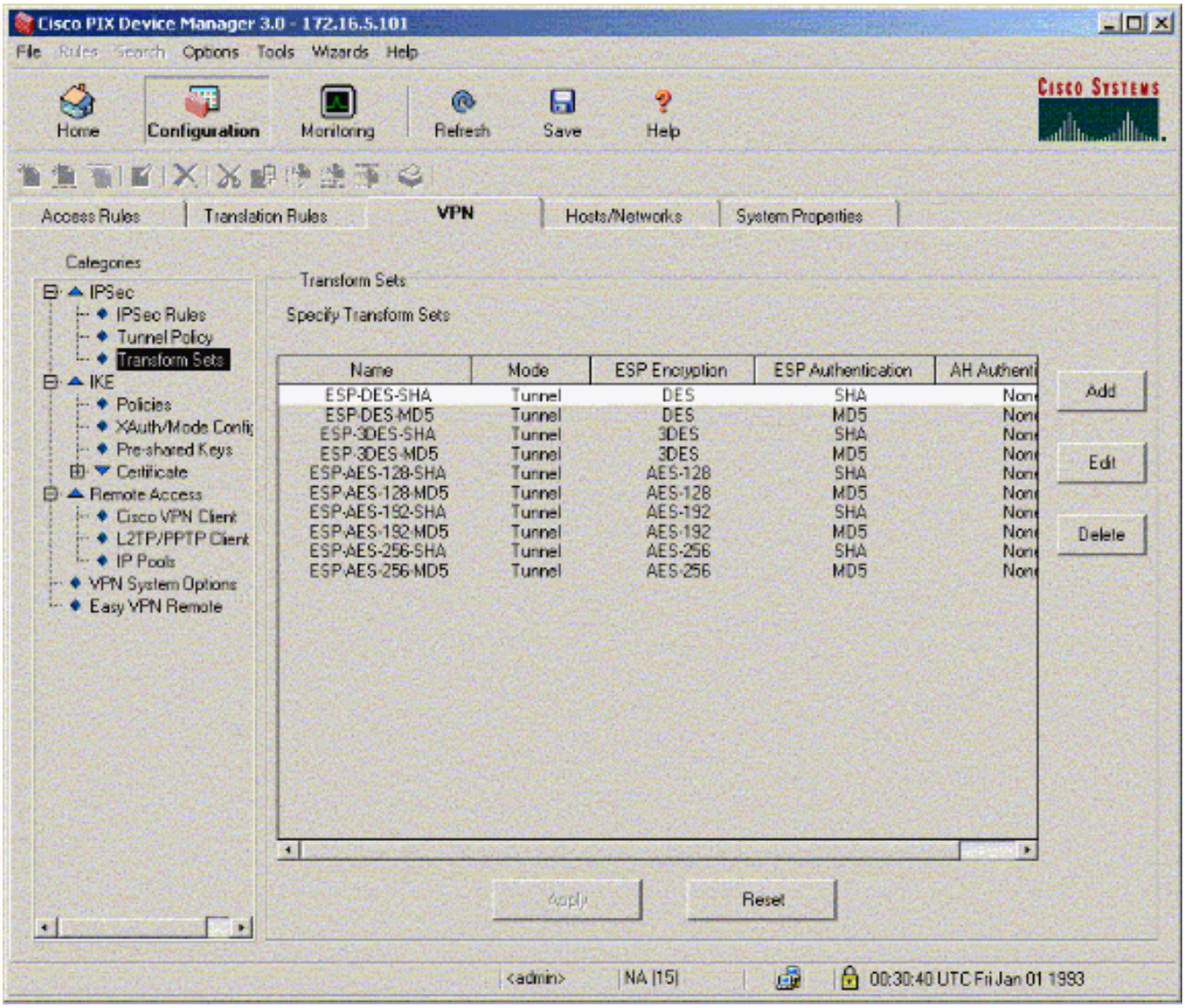
بخلاف التكوين العام الآخر على CLI من PIX للوصول إليه من خلال واجهة إيثرنت 0، أستخدم الأوامر **http server enable** و**http server <local_ip> <mask> <interface>حيث يكون *<local_ip>*** وقناع <mask> عنوان IP محطة العمل التي يتم تثبيت PDM عليها. التكوين الموجود في هذا المستند ل PIX-01. يمكن تكوين PIX-02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

أكمل الخطوات التالية:

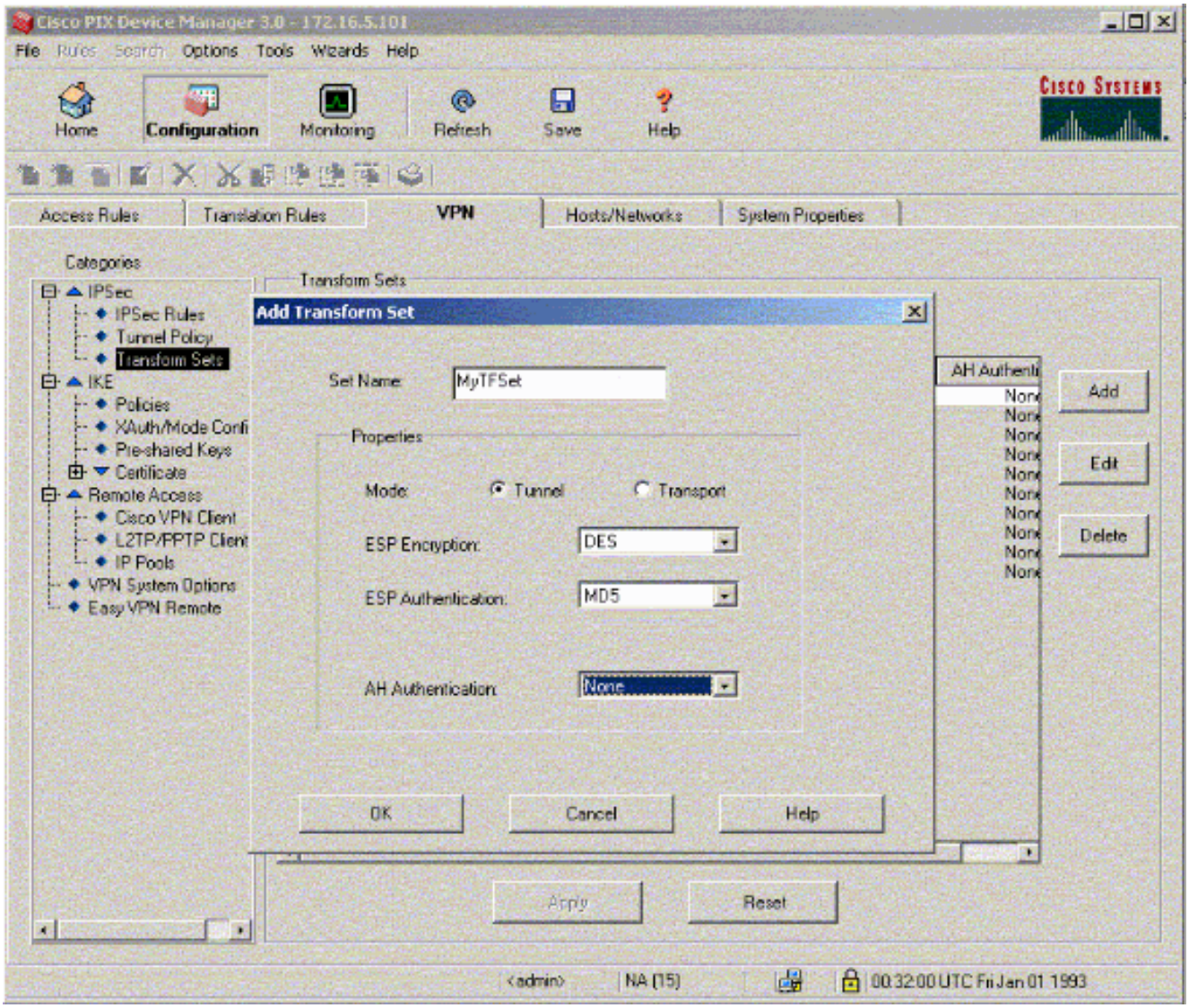
1. افتح المستعرض واكتب **https://<inside_ip_address_of_pix>**للوصول إلى PIX في PDM.
2. انقر فوق **التكوين** وانتقل إلى علامة التبويب VPN.



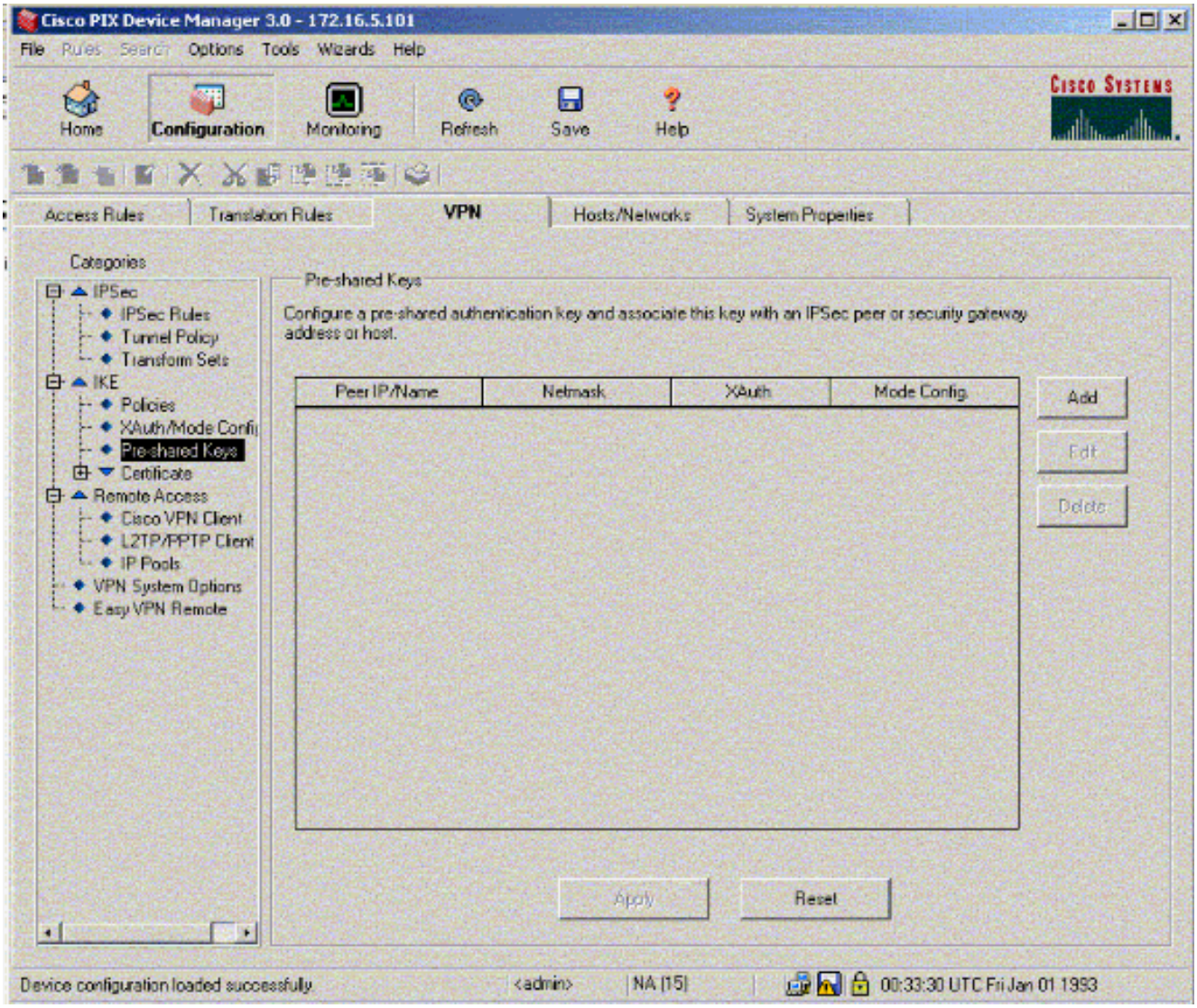
3. انقر فوق **مجموعات التحويل** ضمن IPSec لإنشاء مجموعة تحويل.



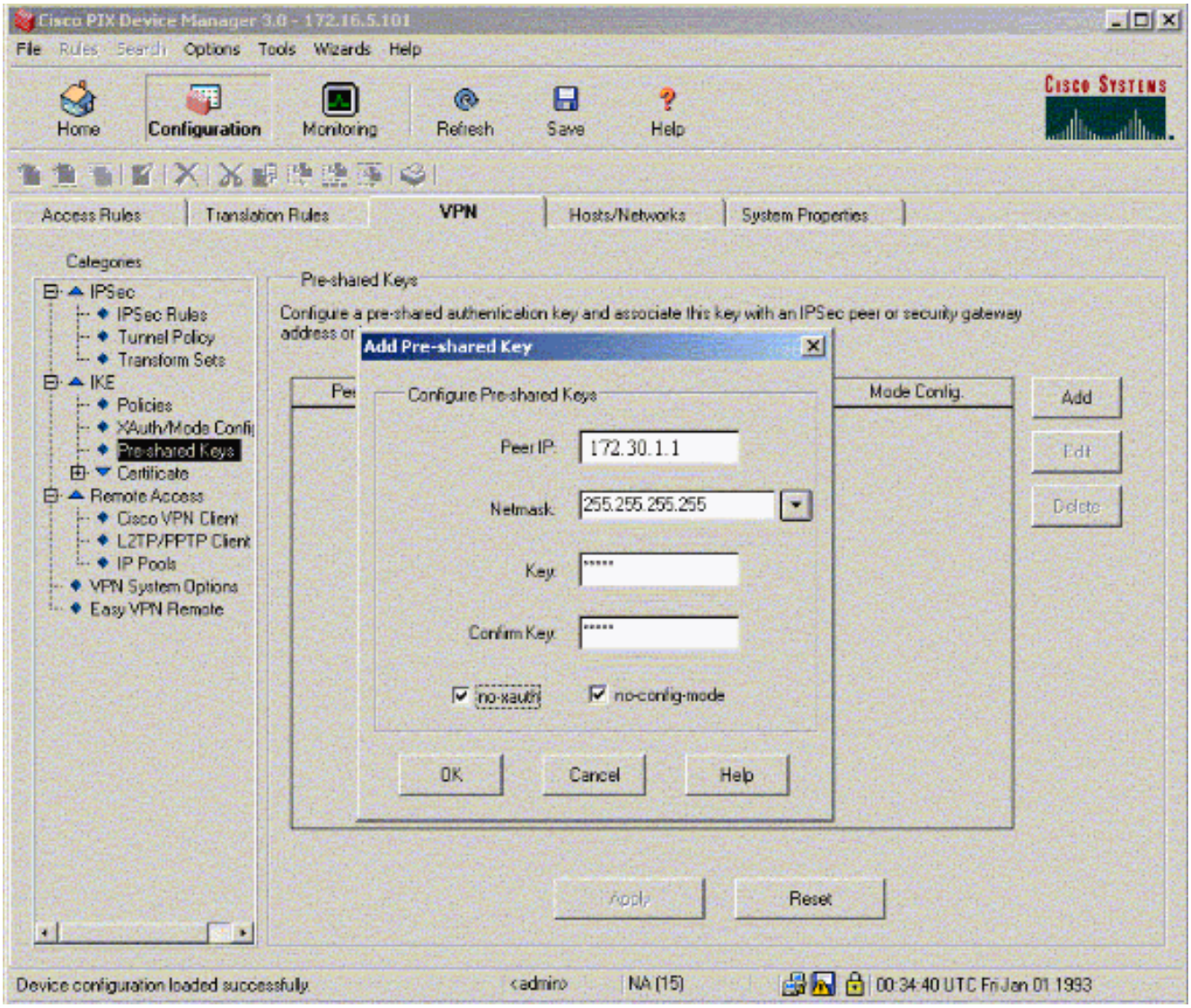
4. انقر **إضافة**، حدد كل الخيارات المناسبة، وانقر **موافق** لإنشاء مجموعة تحويل جديدة.



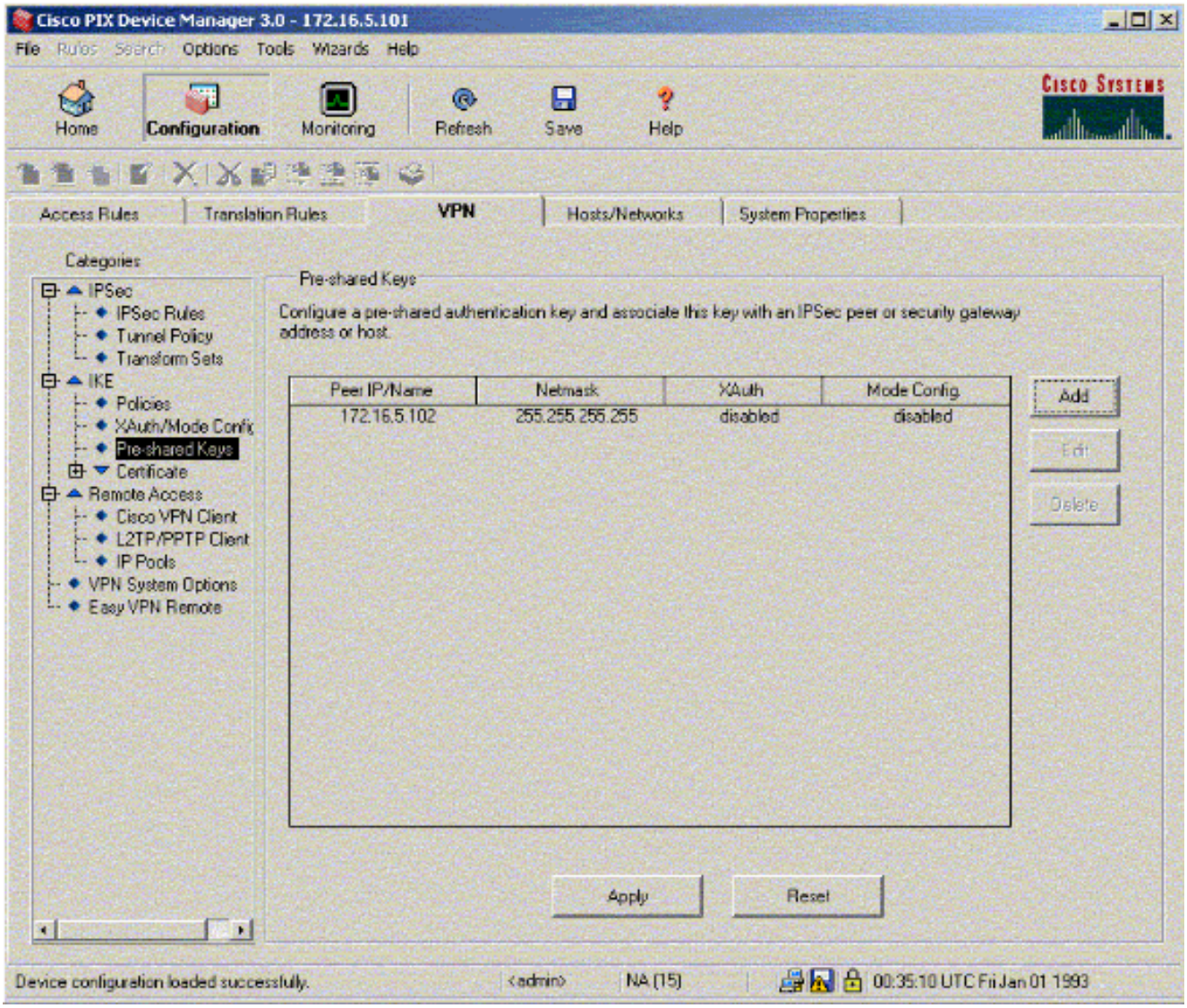
5. انقر فوق **مفاتيح مشتركة مسبقا** ضمن IKE لتكوين المفاتيح المشتركة مسبقا.



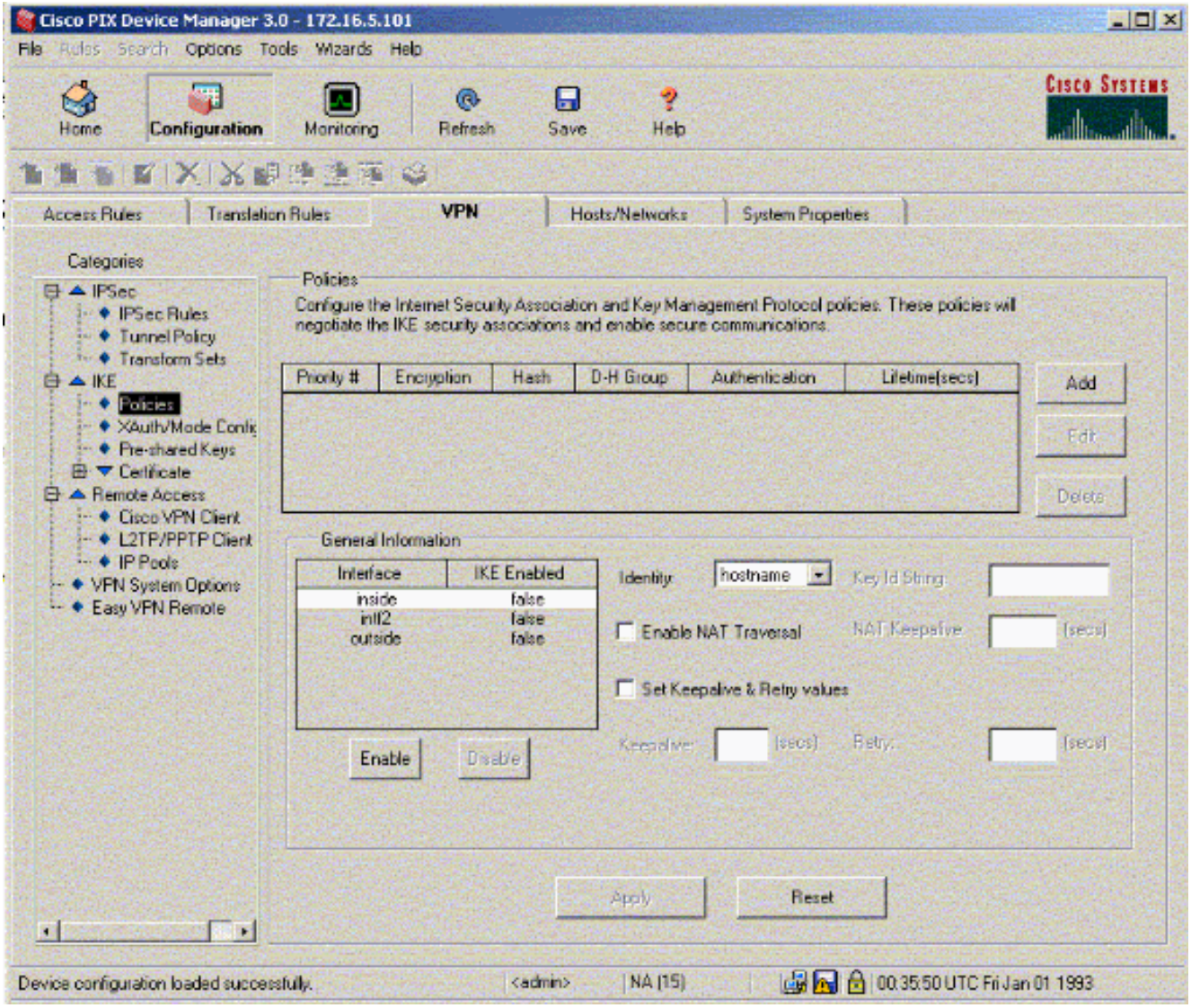
6. انقر فوق **إضافة** لإضافة مفتاح جديد مشترك مسبقا.



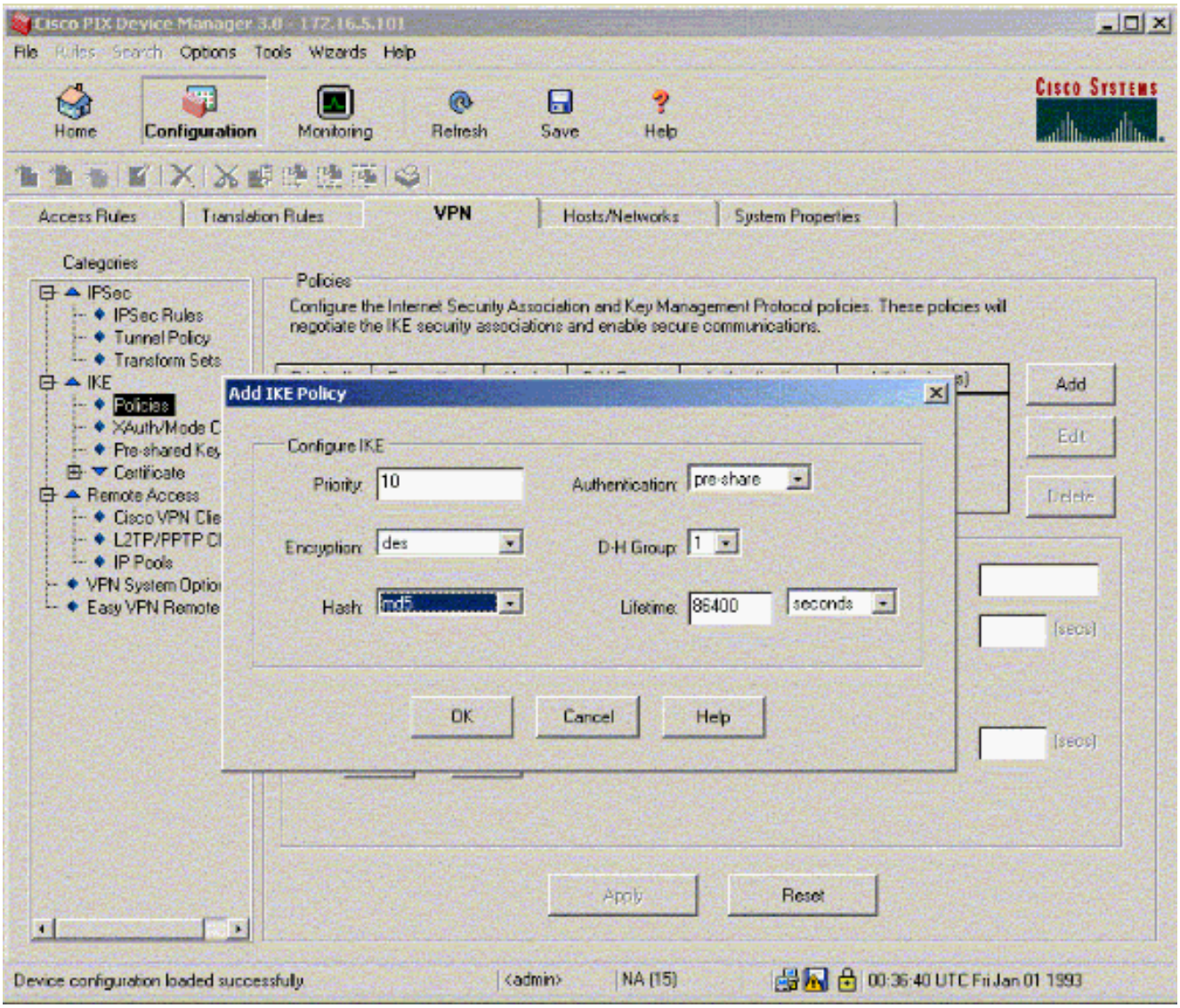
يبدي هذا نافذة المفتاح، أي يكون الكلمة لاقتران نفق. يجب أن يتطابق هذا على جانبي النفق.



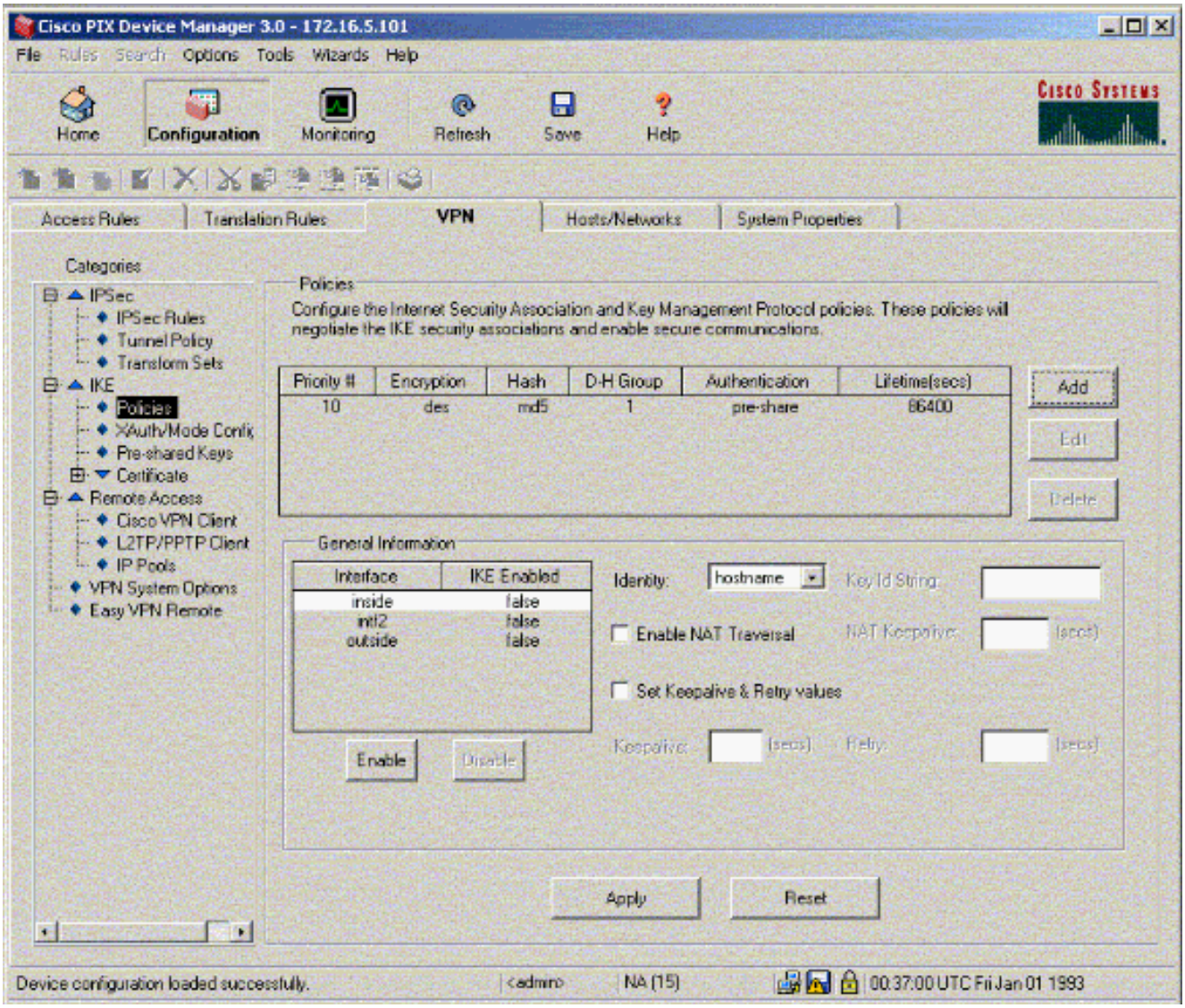
7. انقر فوق **السياسات** ضمن IKE لتكوين السياسات.



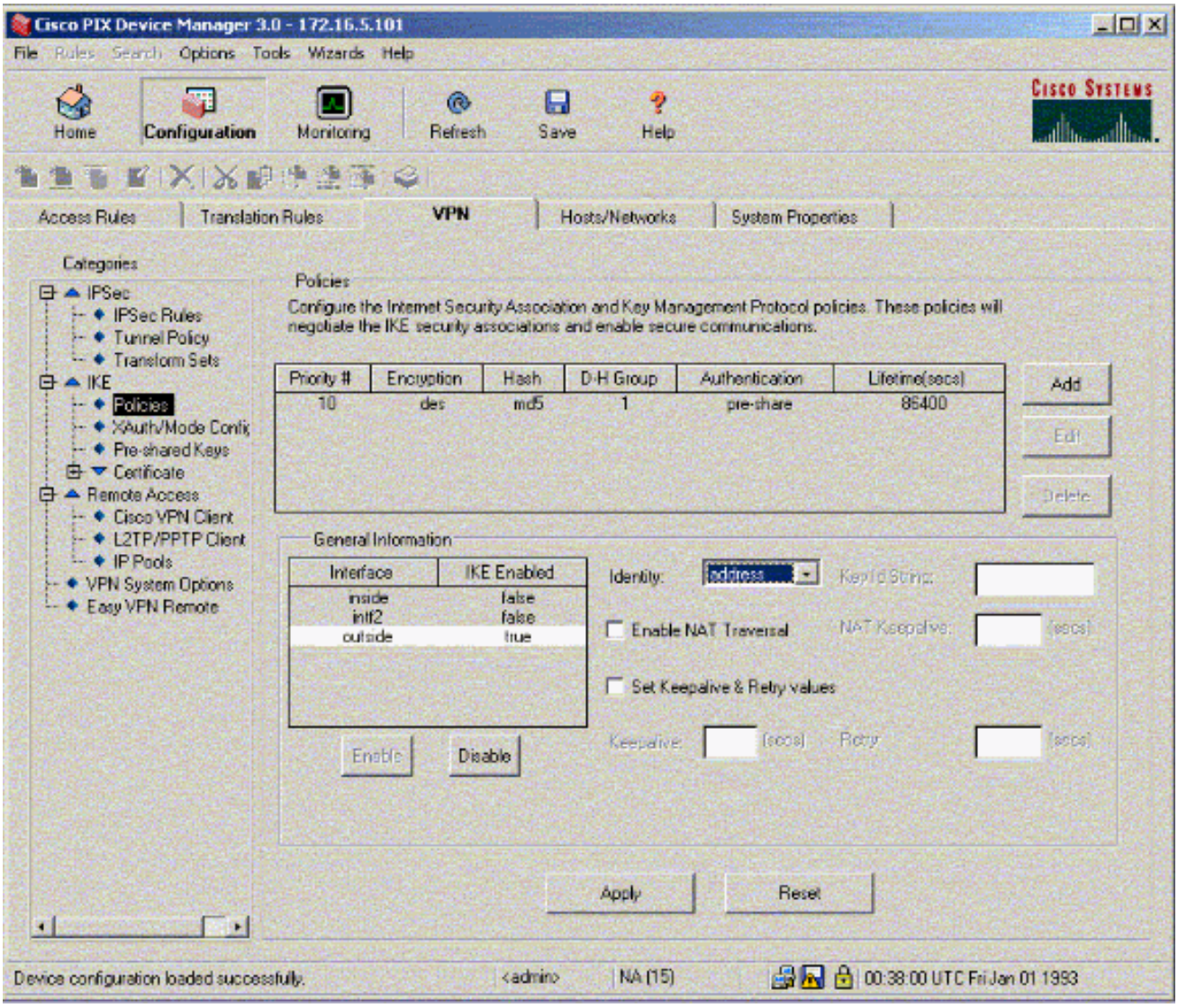
8. انقر فوق **إضافة** وتعبئة الحقول المناسبة.



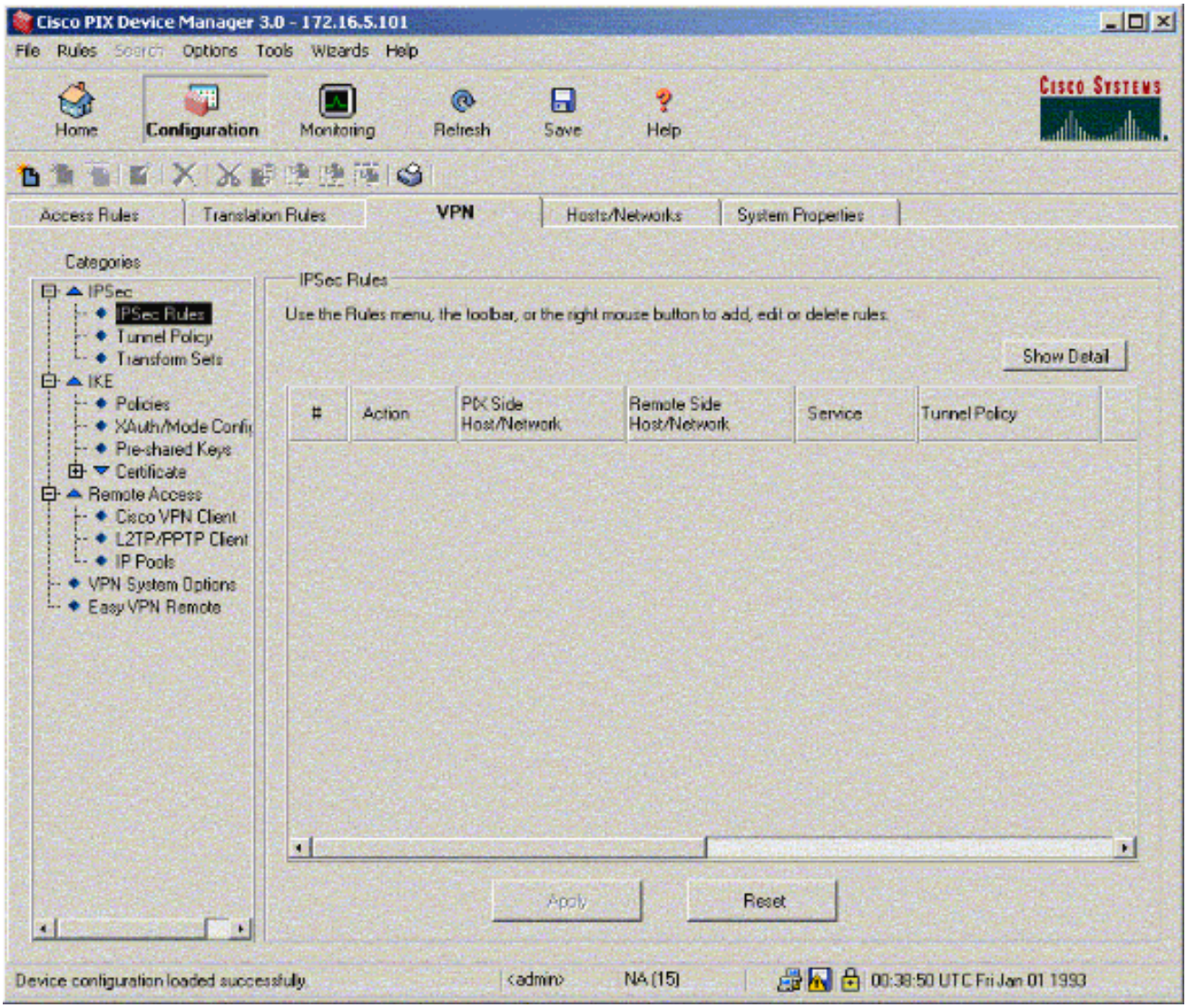
9. انقر فوق **موافق** لإضافة نهج جديد.



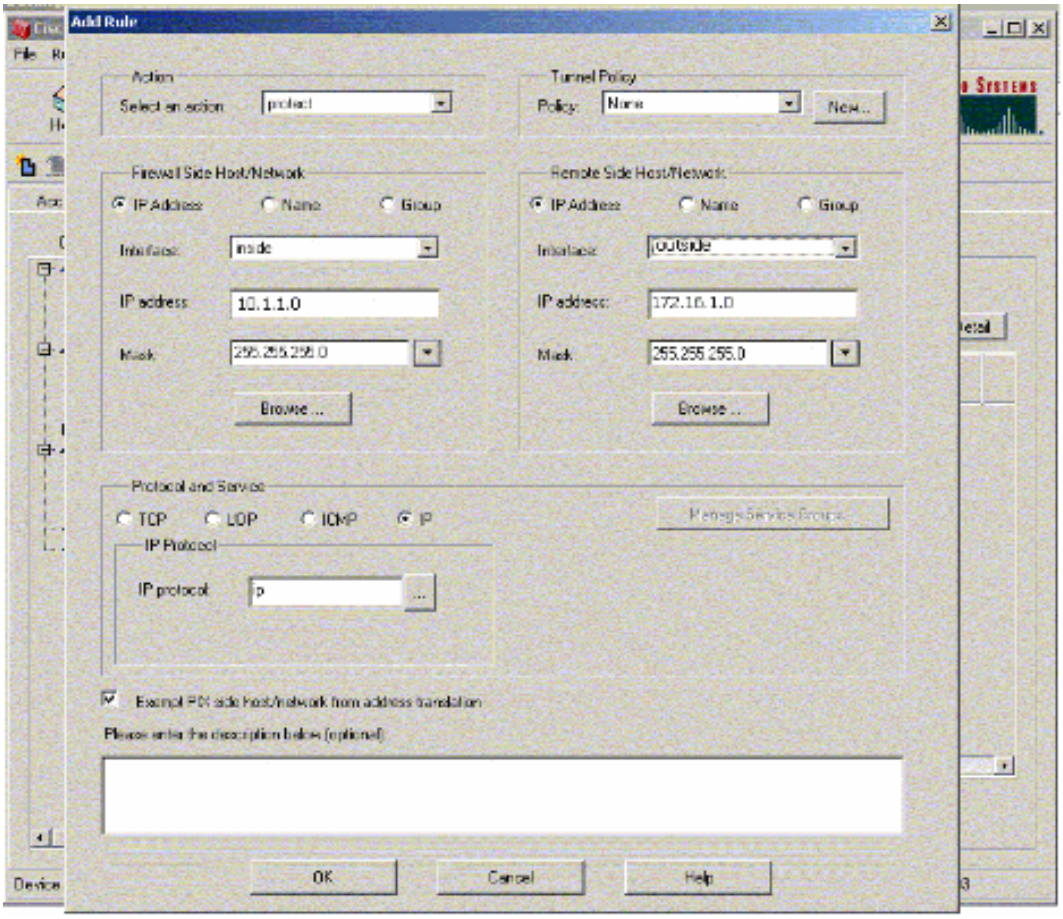
10. حدد الواجهة **الخارجية**، انقر فوق **تمكين**، ثم حدد **العنوان** من القائمة المنسدلة للهوية.



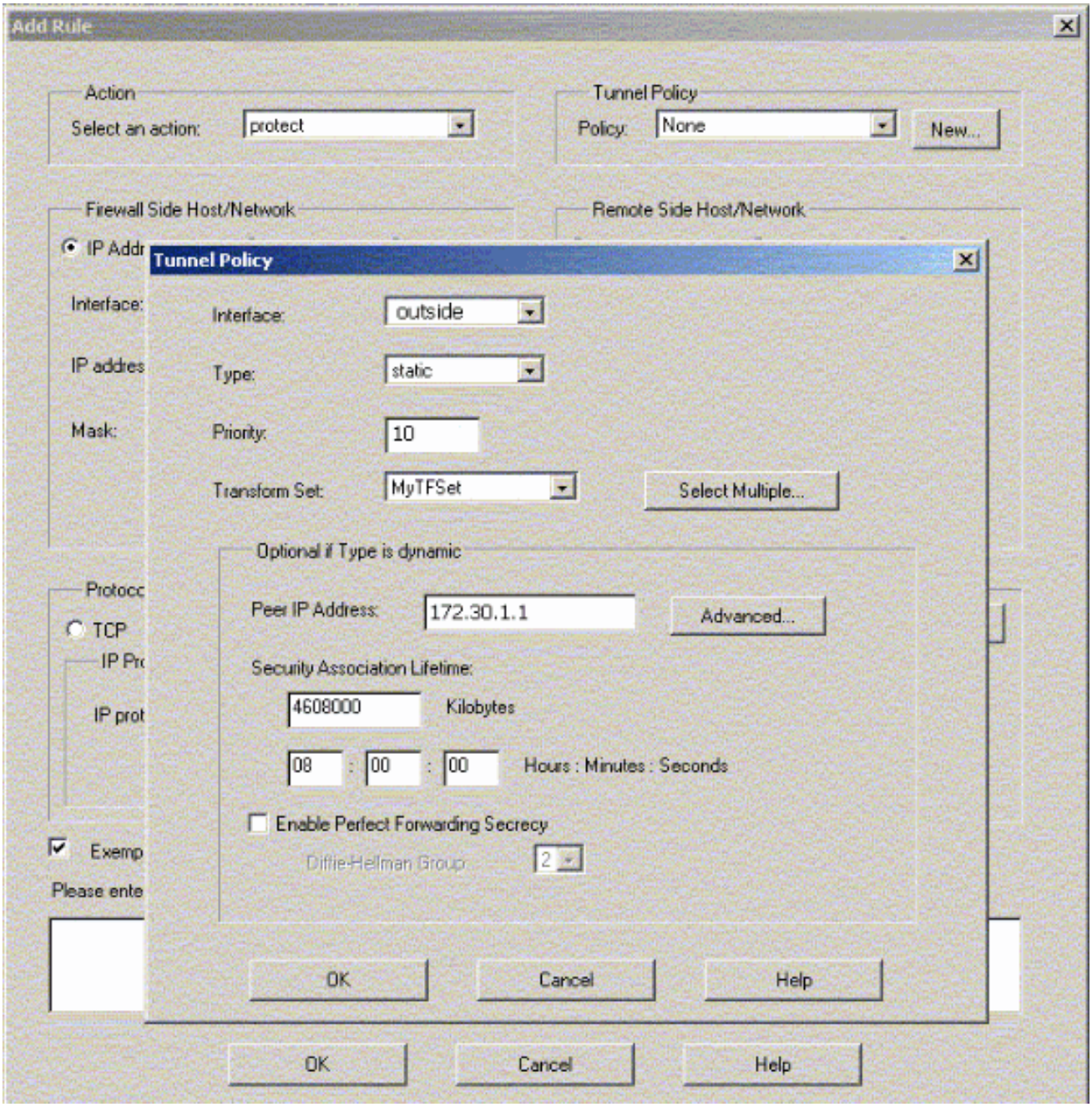
11. انقر فوق **قواعد IPSec** ضمن IPSec لإنشاء قواعد IPsec.



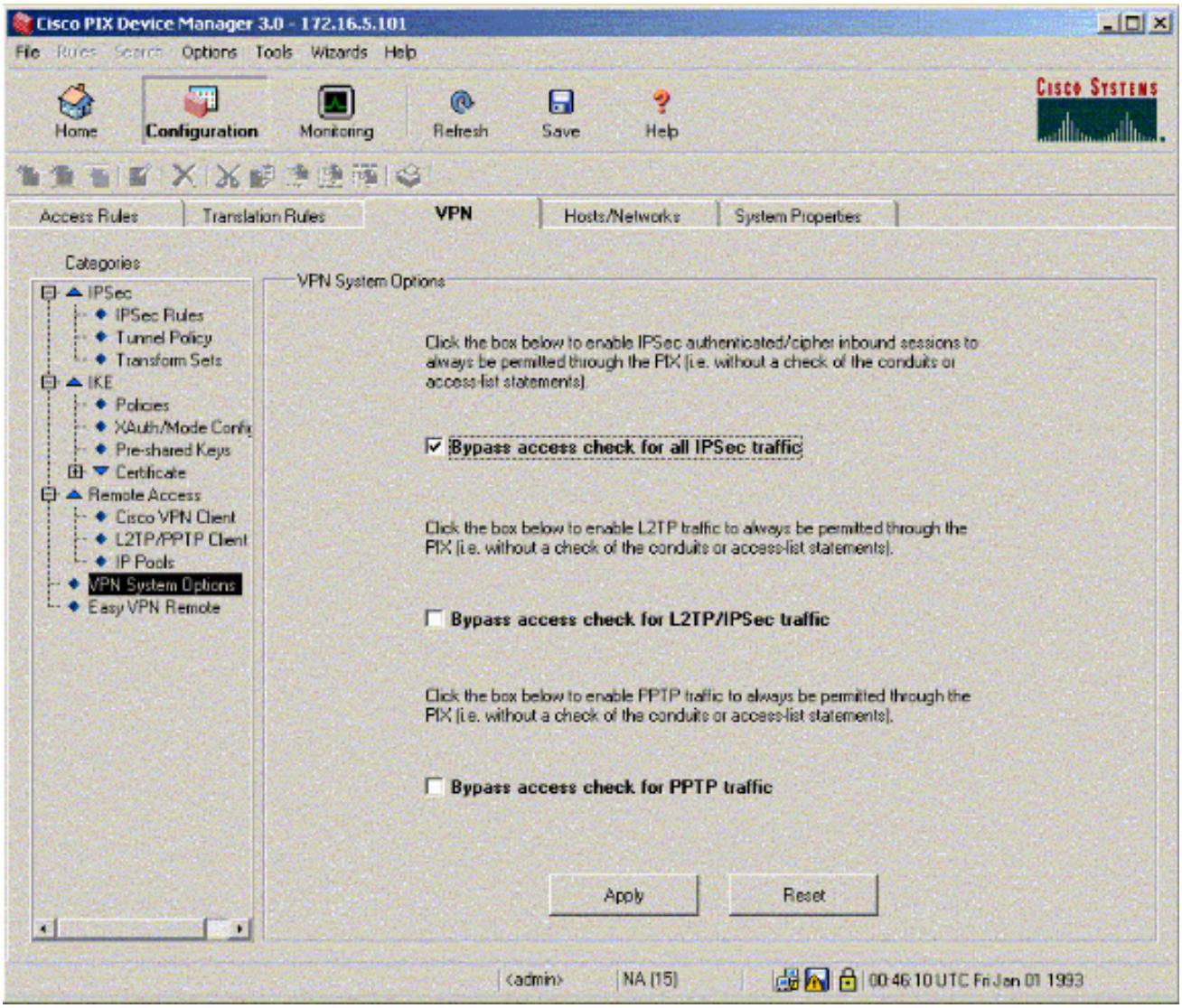
12. املأ الحقول المناسبة.



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**.

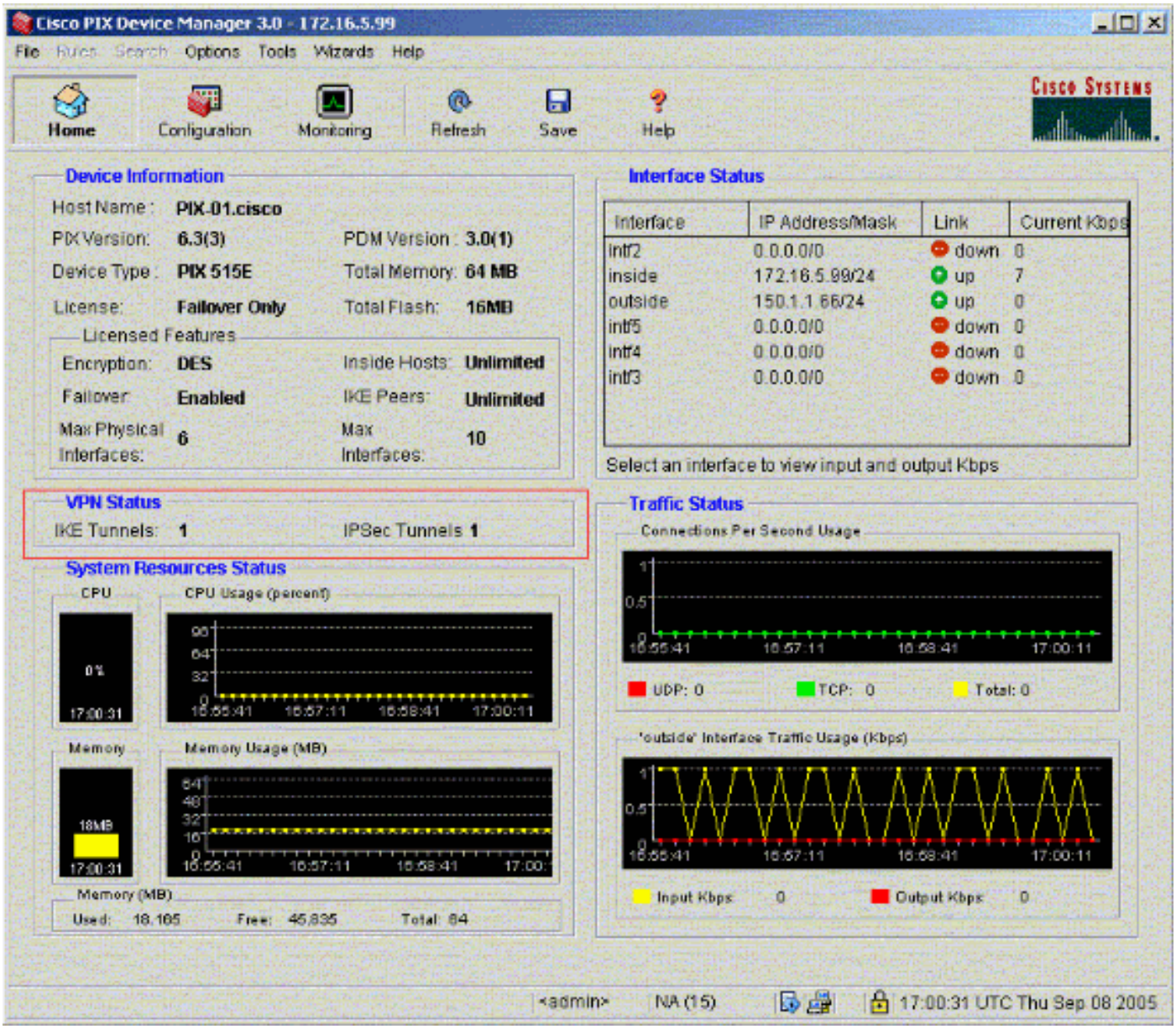


التحقق من الصحة

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

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج 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، وتشفيرها، 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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).