

PDM を使用した 2 台の PIX 間の LAN-to-LAN VPN トンネルの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ネットワーク図](#)

[表記法](#)

[背景説明](#)

[構成手順](#)

[確認](#)

[トラブルシュート](#)

[関連情報](#)

概要

このドキュメントでは、Cisco PIX Device Manager (PDM) を使用して 2 つの PIX Firewall 間に VPN のトンネルを設定する手順について説明します。PDM は、GUI を使用して PIX Firewall をセットアップ、設定、モニタするために設計されているブラウザ ベースの設定ツールです。PIX Firewall は 2 つの別のサイトに配置されます。

トンネルはIPsecを使用して形成されます。IPSec とは、IPSec ピア間でデータの機密性、データの完全性、およびデータの発信元の認証を提供するオープン スタンドアードの組み合わせです。

前提条件

要件

このドキュメントの要件はありません。

使用するコンポーネント

このドキュメントの情報は、6.xおよびPDMバージョン3.0のCisco Secure PIX 515E Firewallに基づいています。

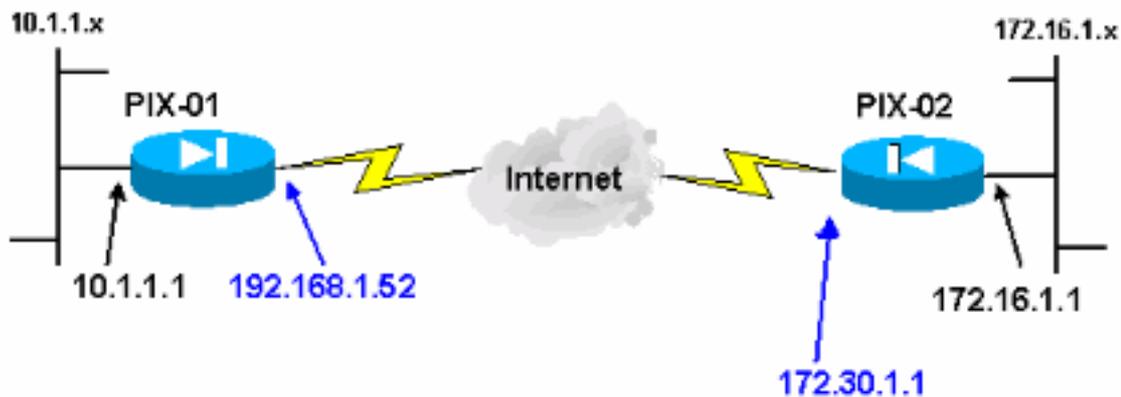
コマンドラインインターフェイス(CLI)を使用した2つのPIXデバイス間のVPNトンネルの設定例については、『[IPSecを使用した単純なPIX-to-PIX VPNトンネルの設定](#)』を参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



表記法

ドキュメント表記の詳細については、『[シスコ テクニカル ティップスの表記法](#)』を参照してください。

背景説明

IPsecネゴシエーションは5つのステップに分けられ、2つのInternet Key Exchange (IKE ; インターネット鍵交換) フェーズが含まれます。

1. 対象トラフィックによって IPsec トンネルが開始されます。IPsec ピアの間を転送されるトラフィックは、対象トラフィックとみなされます。
2. IKE フェーズ 1 では、IPsec ピア同士が、IKE セキュリティ アソシエーション (SA) ポリシーについてネゴシエートします。ピアが認証されると、Internet Security Association and Key Management Protocol (ISAKMP) を使用して安全なトンネルが作成されます。
3. IKE フェーズ 2 では、IPsec ピア同士が認証済みの安全なトンネルを使用して、IPsec SA トランスフォームをネゴシエートします。共有ポリシーのネゴシエーションによって、IPsec トンネルの確立方法が決まります。
4. IPsec トンネルが作成され、IPsec トランスフォーム セットに設定された IPsec パラメータに基づいて、IPsec 間でデータが伝送されます。
5. IPsec SA が削除されるか、そのライフタイムの有効期限が切れると、IPsec トンネルは終了します。注：ピアで両方のIKEフェーズのSAが一致しない場合、2つのPIX間のIPSecネゴシエーションは失敗します。

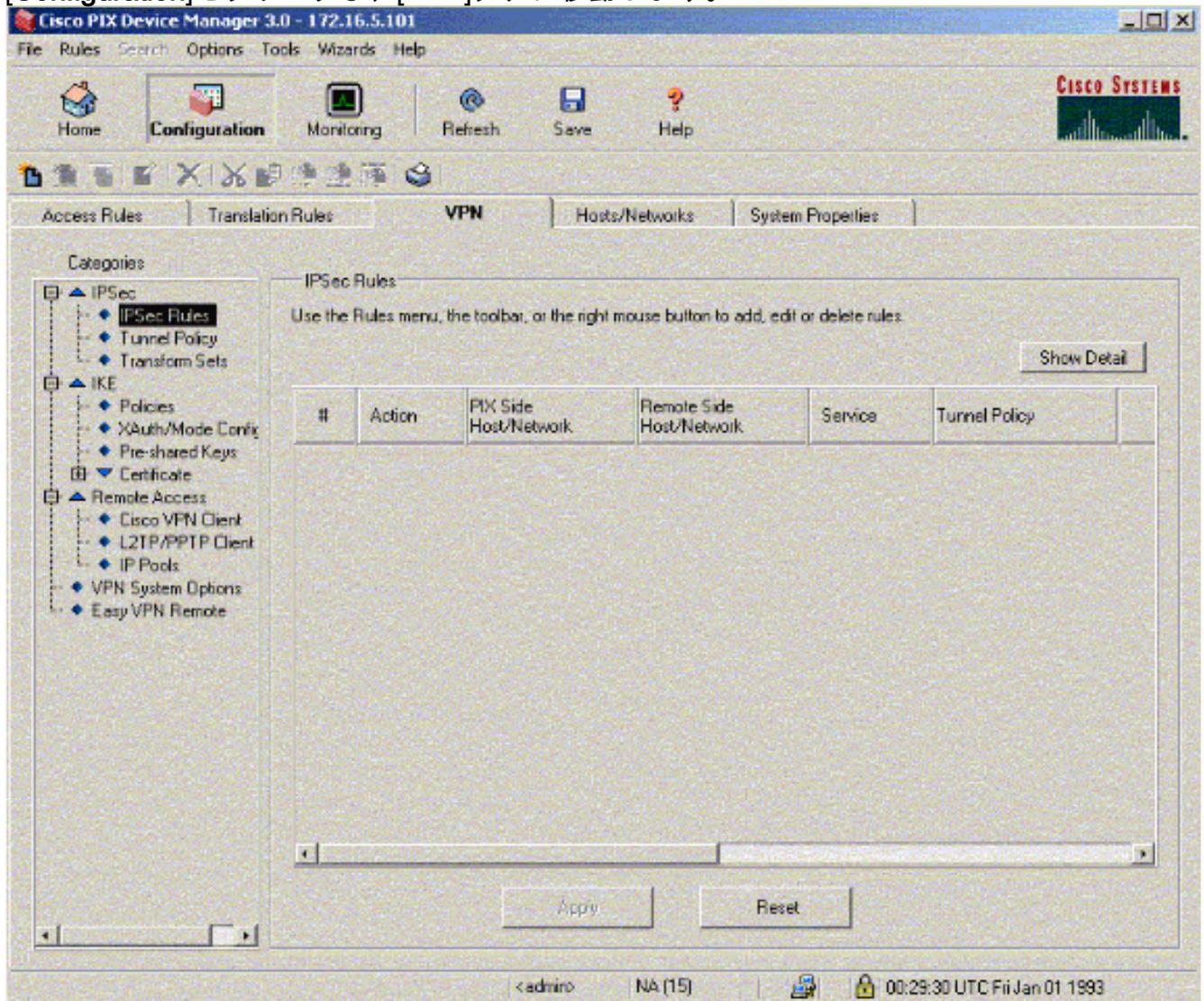
構成手順

PIXのCLIでの他の一般的な設定とは別に、`http server enable`コマンドと`http server <local_ip>`

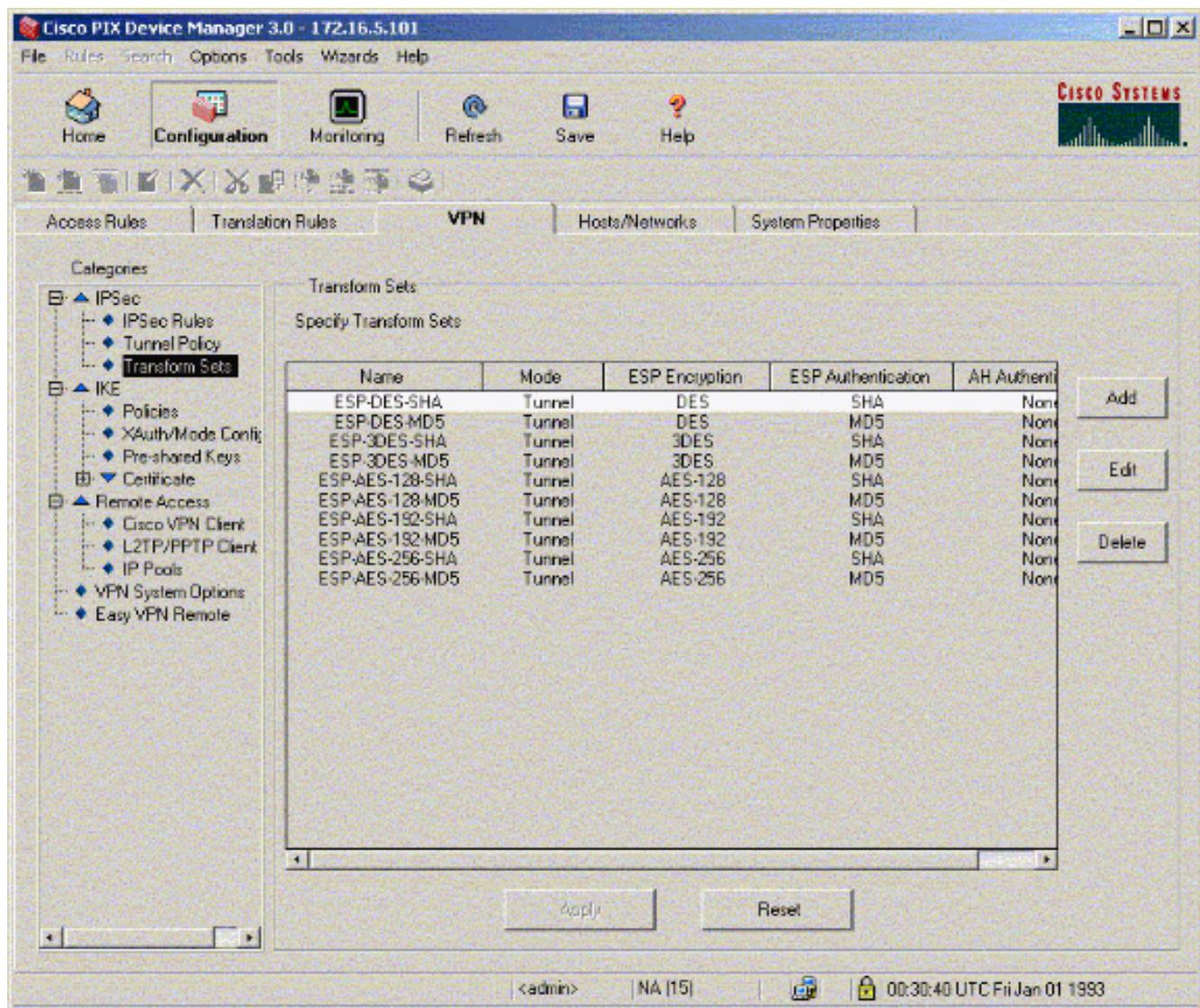
<mask> <interface>コマンドを使用します。ここで、<local_ip>と<mask>は、PDMがインストールされているワークステーションのIPアドレスとマスクです。このドキュメントの設定はPIX-01用です。PIX-02は、異なるアドレスを持つ同じ手順で設定できます。

次のステップを実行します。

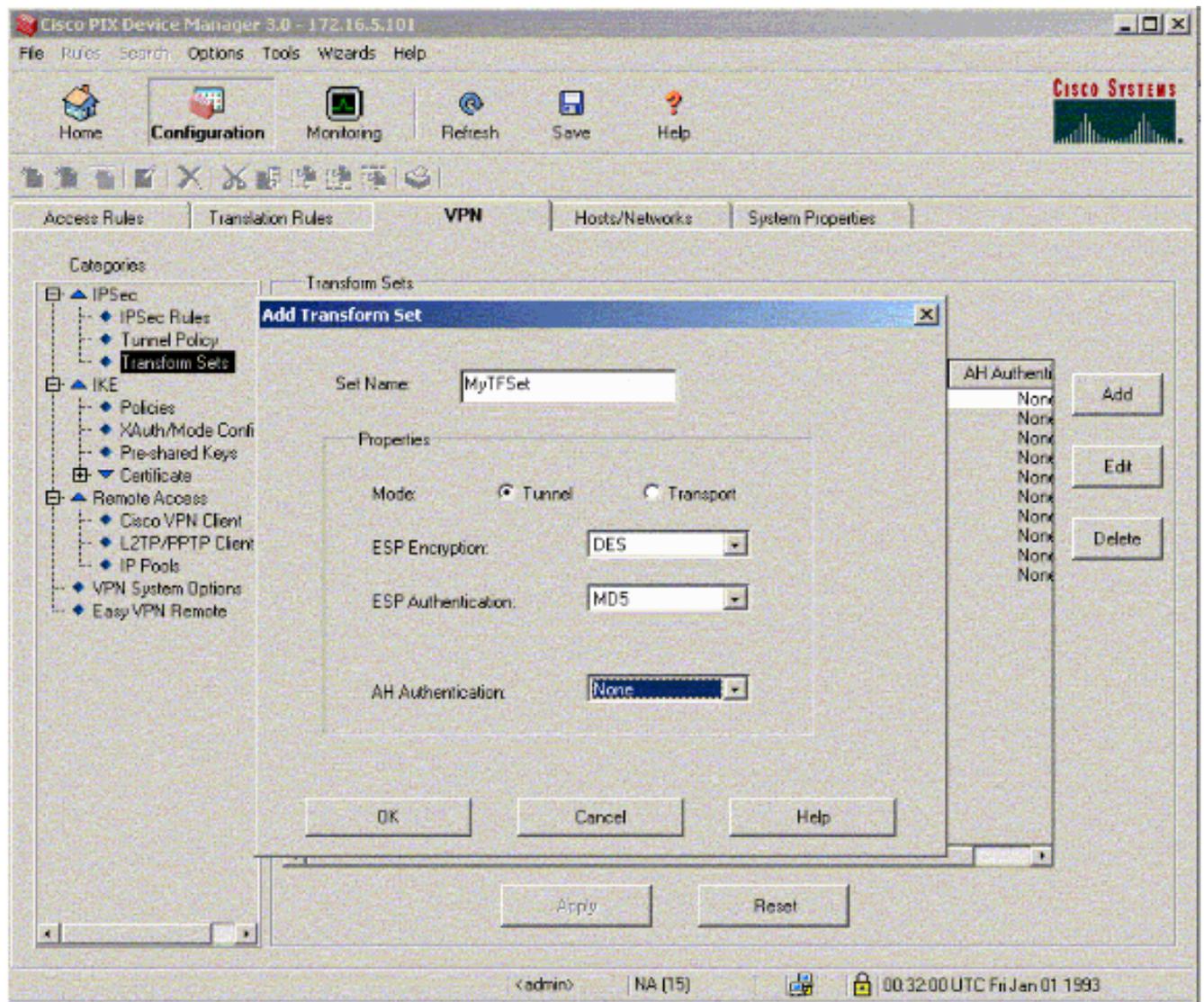
1. ブラウザを開き、https://<Inside_IP_Address_of_PIX>と入力してPDM内のPIXにアクセスします。
2. [Configuration]をクリックし、[VPN]タブに移動します。



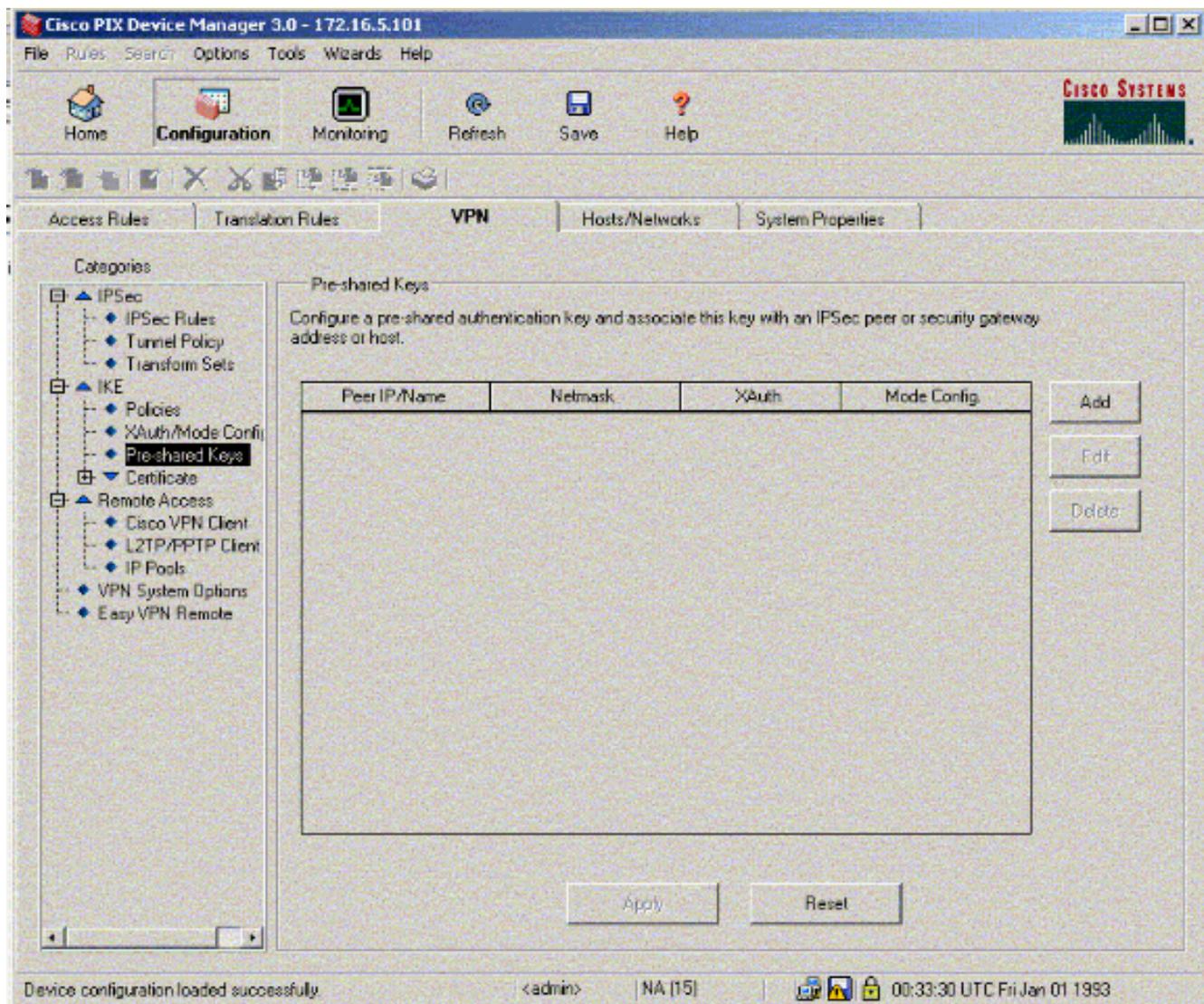
3. IPSecの下のTransform Setsをクリックして、トランスフォームセットを作成します。



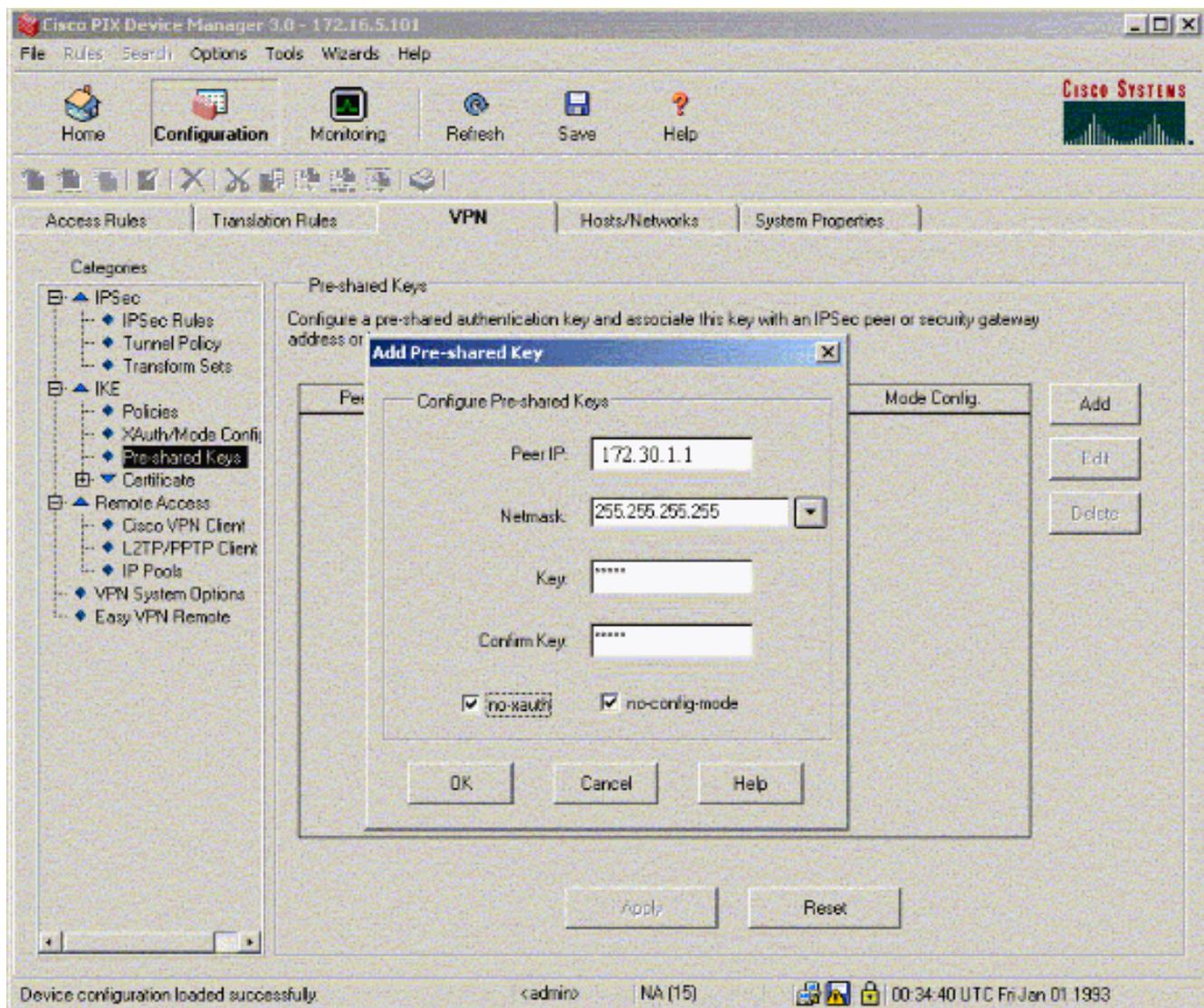
4. [Add]をクリックし、適切なオプションをすべて選択し、[OK]をクリックして、新しいトランスフォームセットを作成します。



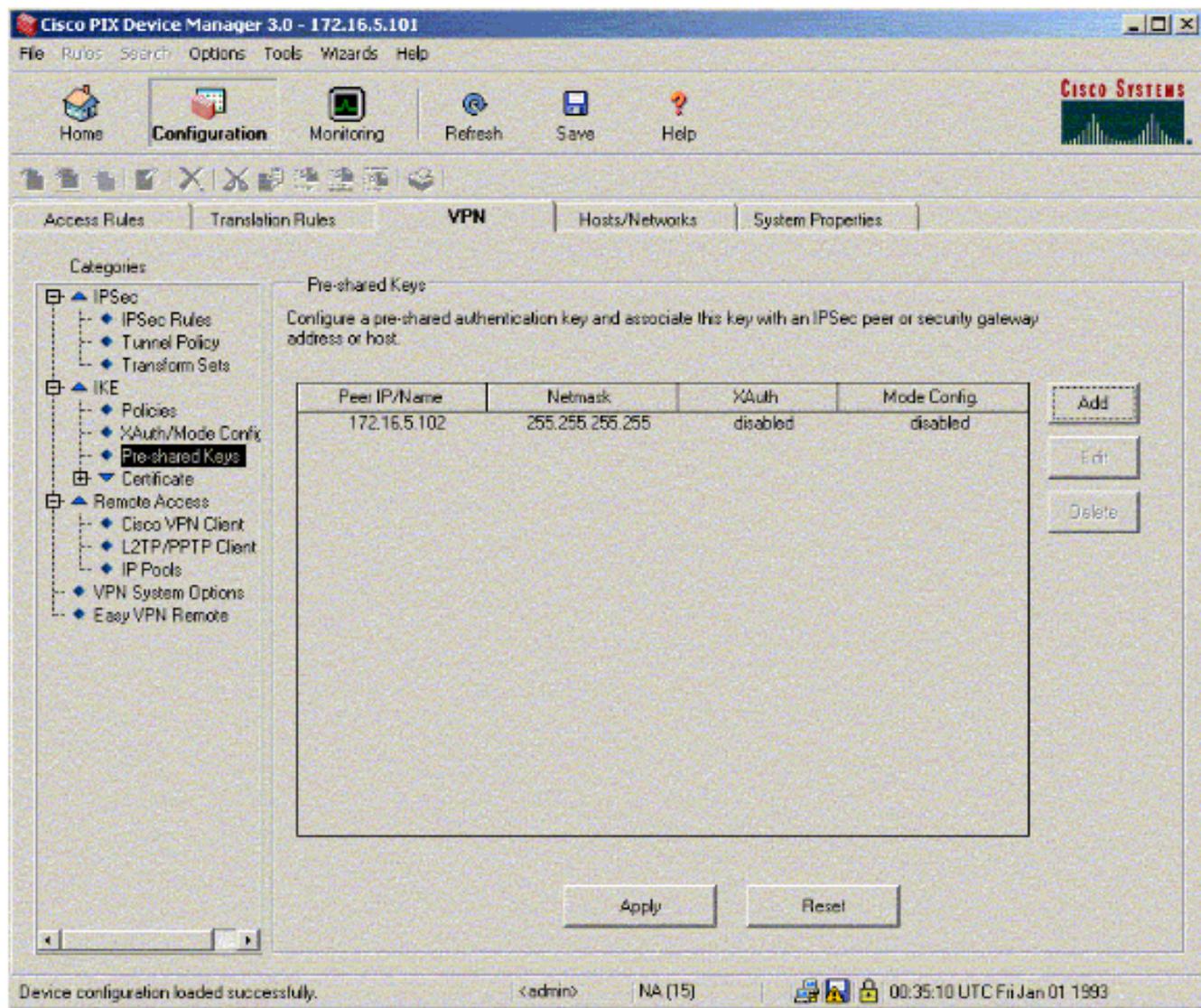
5. IKEの下の[Pre-Shared Keys]をクリックして、事前共有キーを設定します。



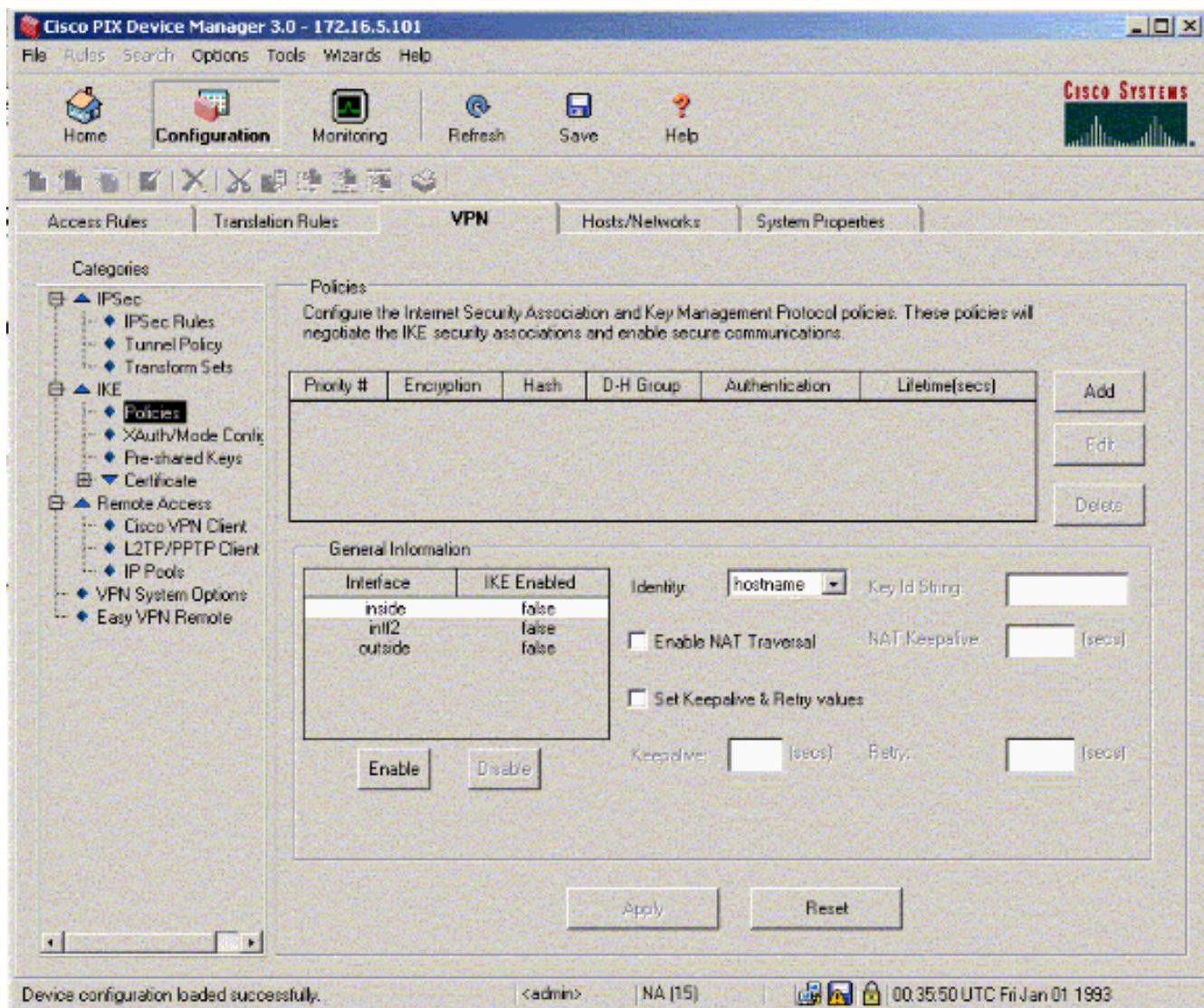
6. [Add]をクリックして、新しい事前共有キーを追加します。



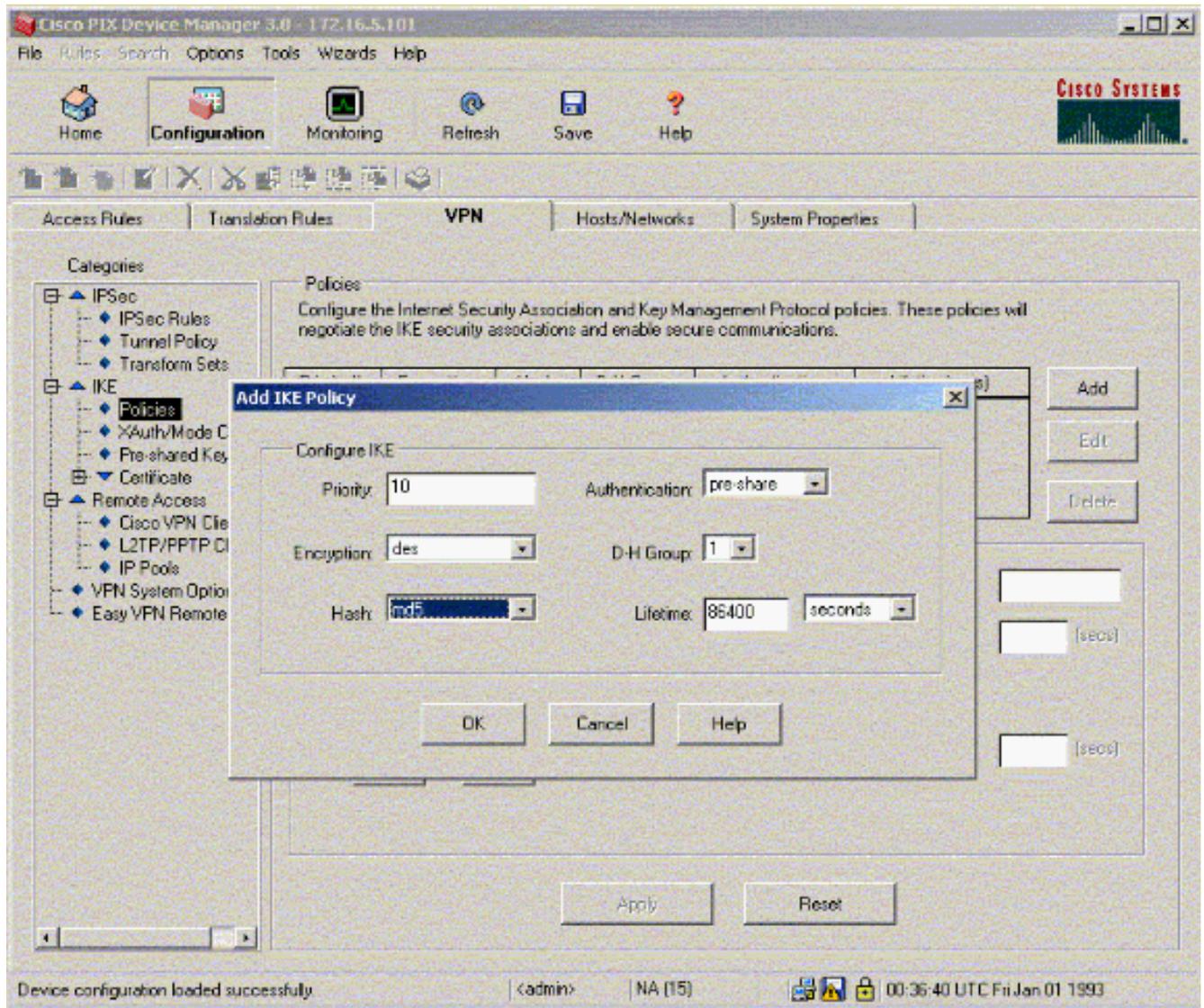
このウィンドウには、トンネルアソシエーションのパスワードであるキーが表示されます。これは、トンネルの両側で一致する必要があります。



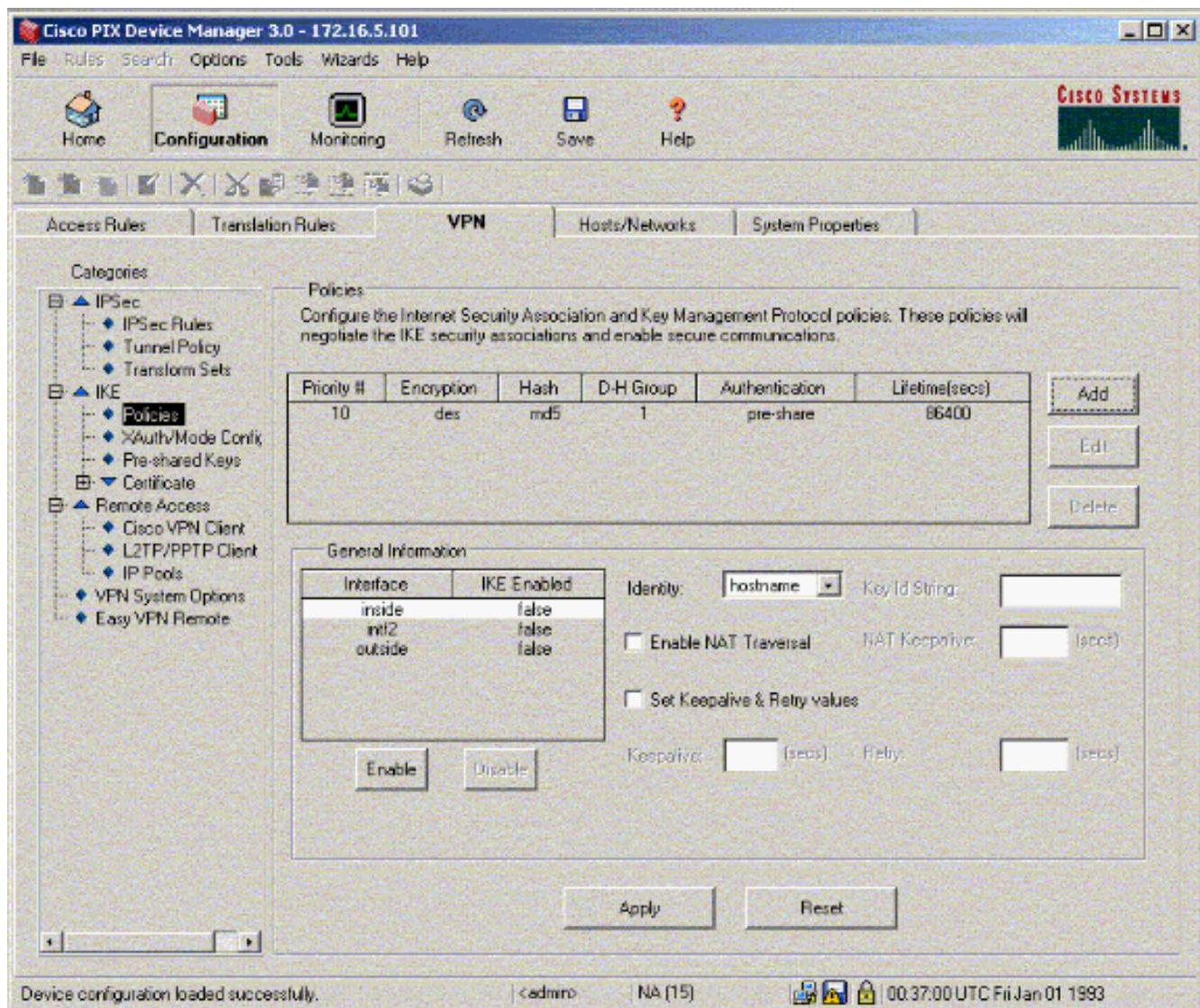
7. IKEの下の[Policies] をクリックして、ポリシーを設定します。



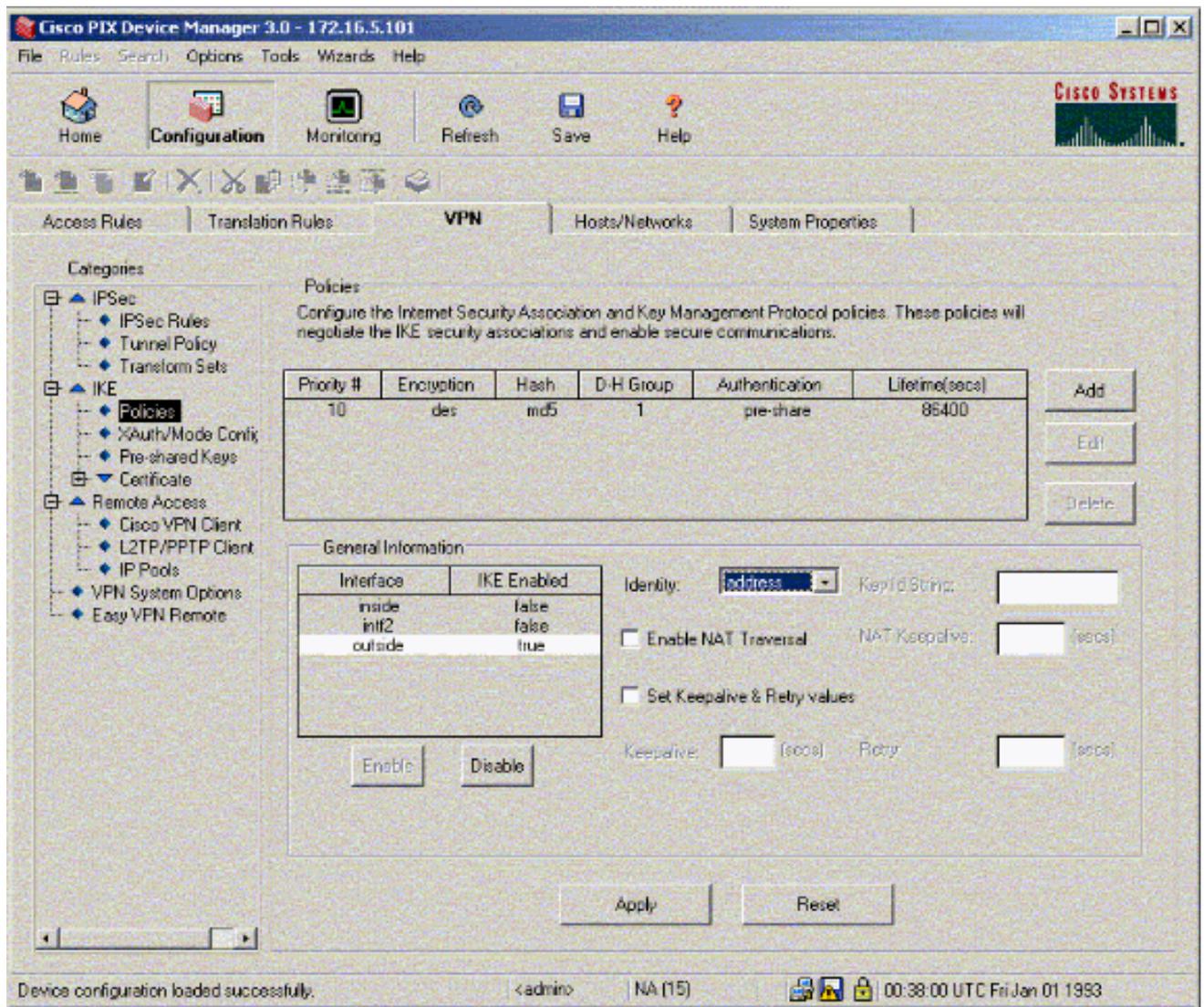
8. [Add]をクリックし、該当するフィールドに入力します。



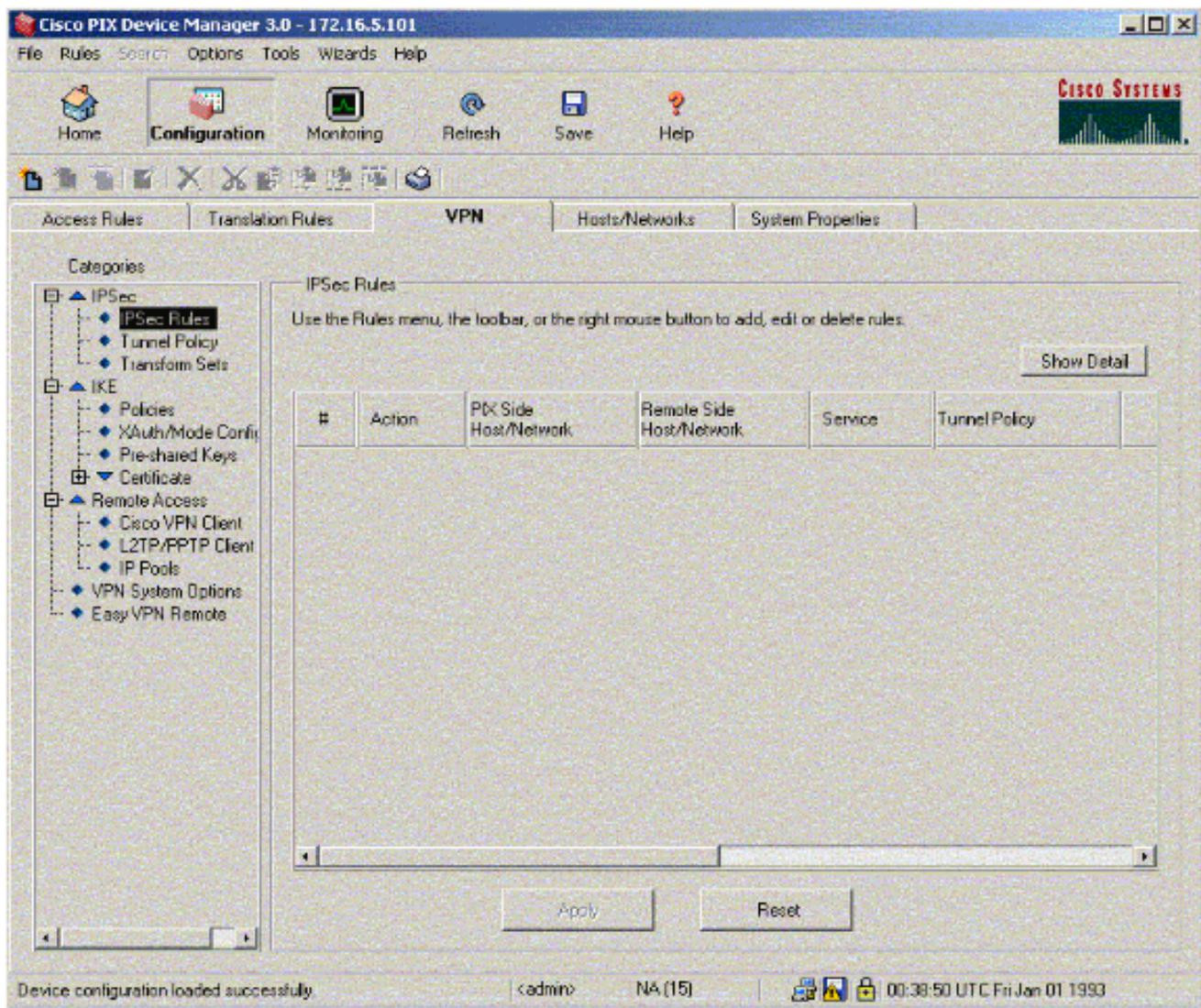
9. [OK]をクリックして、新しいポリシーを追加します。



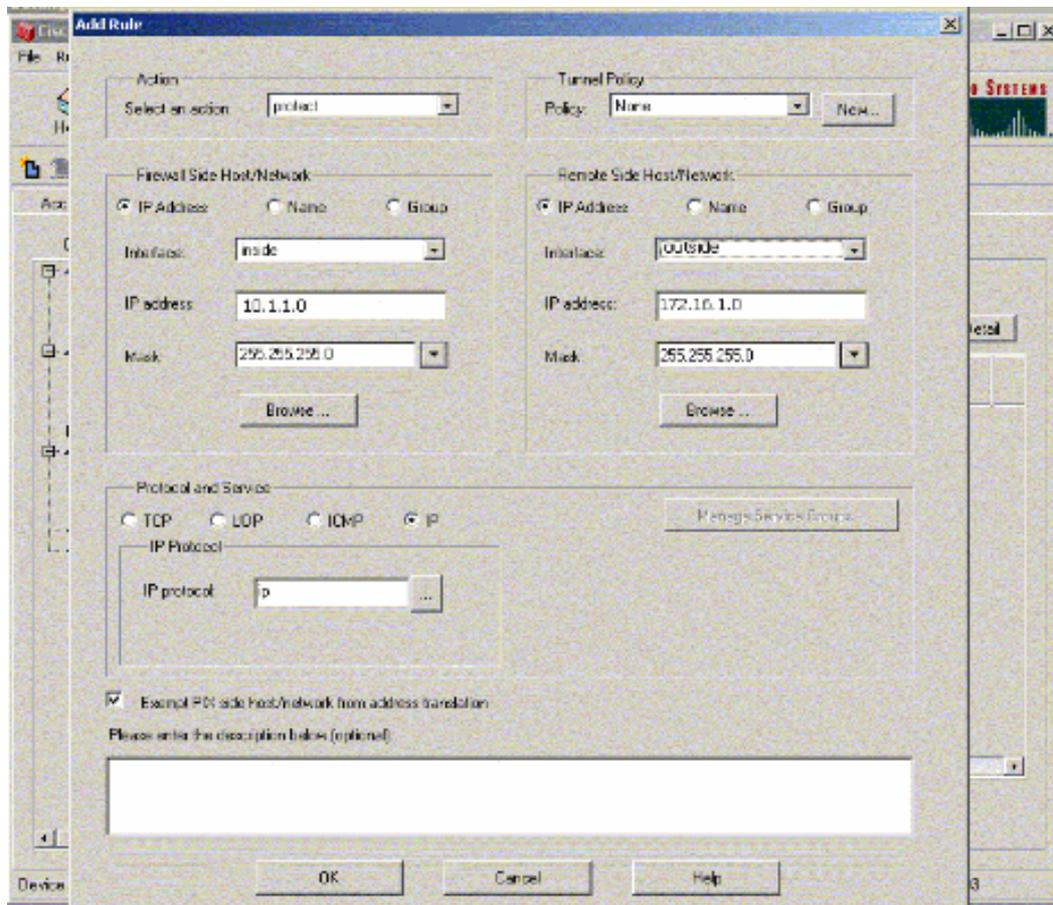
10. 外部インターフェイスを選択し、[有効]をクリックし、[ID]プルダウンメニューから[アドレス]を選択します。



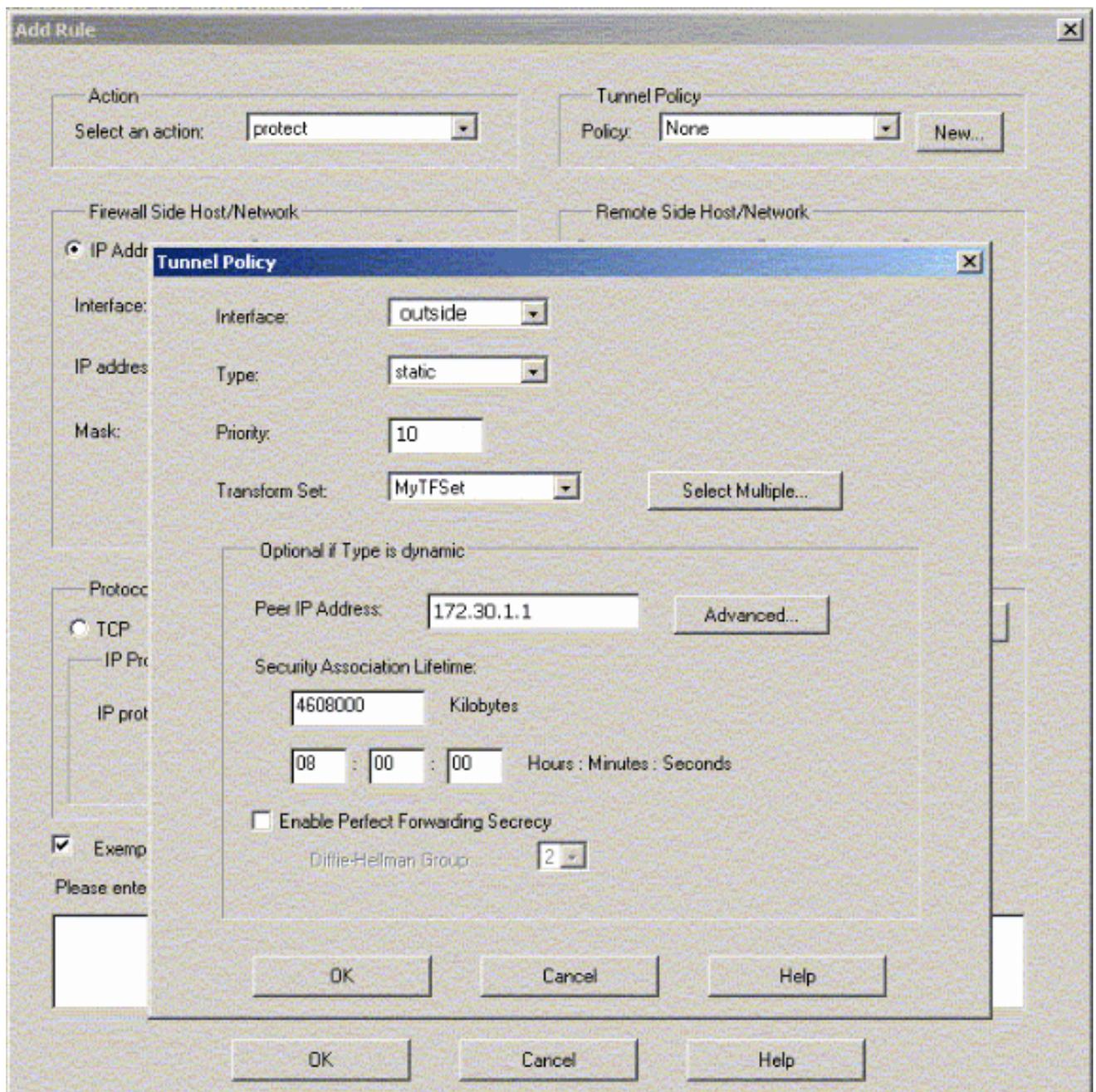
11. IPSecの下の[IPSec Rules]をクリックして、IPSecルールを作成します。



12. 該当するフィールドに入力します。

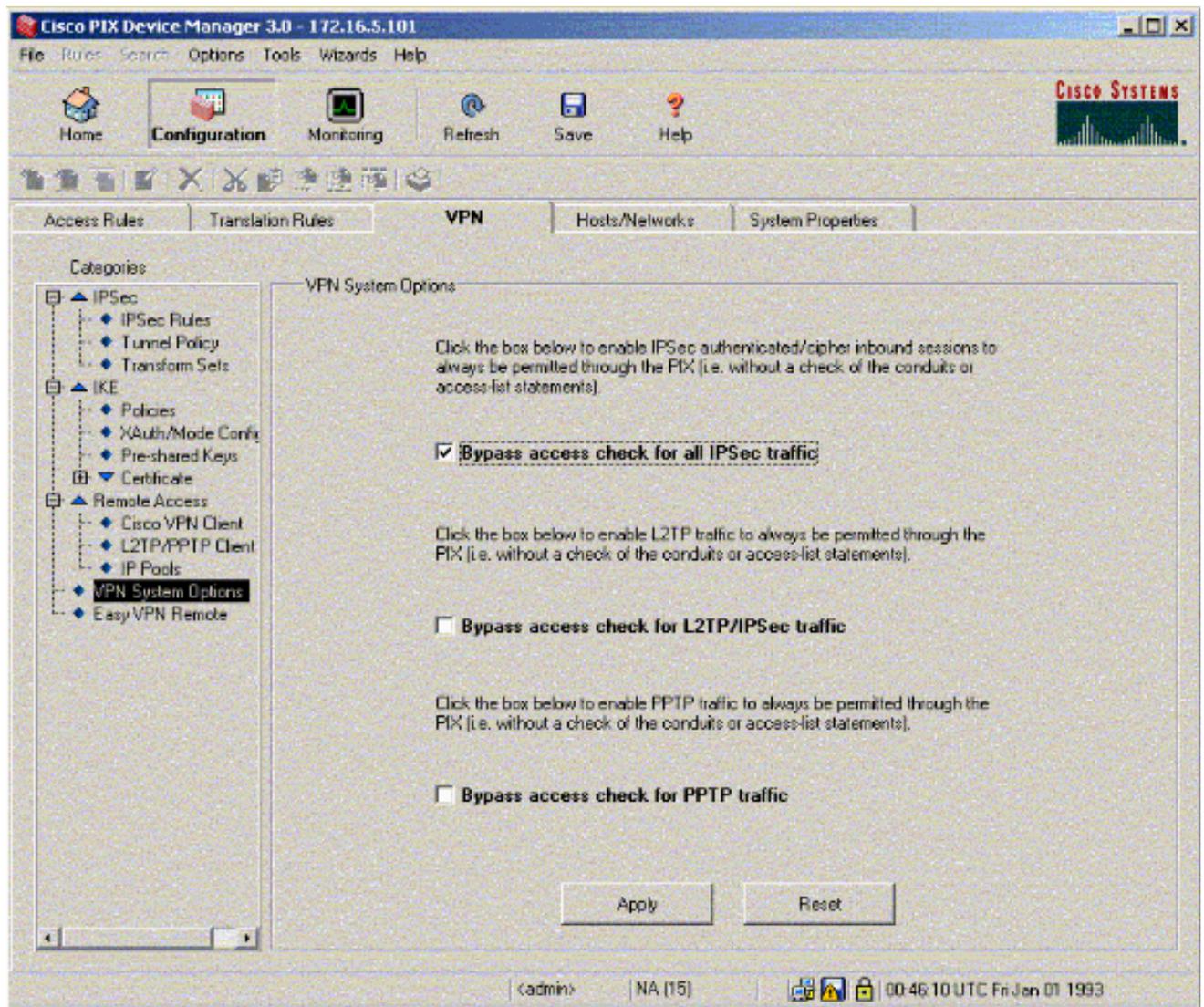


13. [Tunnel Policy]で[New]をクリックします。[Tunnel Policy]ウィンドウが表示されます。該当するフィールドに入力します。



14. [OK]をクリックして、設定されたIPsecルールを表示します。

15. [VPN Systems Options]をクリックし、[Bypass access check for all IPSec traffic]をオンにします。



確認

ピアへの対象トラフィックがある場合、トンネルはPIX-01とPIX-02の間に確立されます。

[アウトプット インタープリタ ツール \(登録ユーザ専用\) \(OIT\)](#) は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

トンネルの形成を確認するには、PDMの[Home]の下の[VPN Status]を (赤色で強調表示) します。

The screenshot displays the Cisco PIX Device Manager 3.0 interface. The top menu includes File, Run, Search, Options, Tools, Wizards, and Help. The main area is divided into several sections:

- Device Information:** Host Name: PIX-01.cisco, PIX Version: 6.3(3), PDM Version: 3.0(1), Device Type: PIX 515E, Total Memory: 64 MB, License: Fallback Only, Total Flash: 16MB. Licensed Features include Encryption: DES, Inside Hosts: Unlimited, Fallback: Enabled, IKE Peers: Unlimited, Max Physical Interfaces: 6, and Max Interfaces: 10.
- Interface Status:** A table showing interface status:

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
- VPN Status:** IKE Tunnels: 1, IPsec Tunnels: 1.
- System Resources Status:** CPU Usage (percent) is 0%. Memory Usage (MB) is 18MB. A graph shows CPU usage over time, and another graph shows memory usage over time.
- Traffic Status:** Connections Per Second Usage graph shows 0 connections. 'outside' Interface Traffic Usage (Kbps) graph shows 0 input and output Kbps.

The bottom status bar shows: <admin> NA (15) 17:00:31 UTC Thu Sep 08 2005.

PDMの[Tools]の下にあるCLIを使用して、トンネルの形成を確認することもできます。show crypto isakmp saコマンドを発行してトンネルの形成を確認し、show crypto ipsec saコマンドを発行してカプセル化、暗号化などのパケットの数を調べます。

注：グローバル設定モードでmanagement-accessコマンドが設定されていない限り、PIXの内部インターフェイスに対してトンネル形成のpingを実行できません。

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

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [PDMを使用したファイアウォール間の冗長トンネルの作成](#)
- [Cisco Secure PIX ファイアウォール コマンド リファレンス](#)

- [Requests for Comments \(RFCs\)](#)
- [Cisco PIX Firewall ソフトウェア](#)