Wild-card, Pre-shared, No Mode-Config を使用した Cisco Secure VPN クライアントPIX 設定

内容

概要

この設定では、ワイルドカードと**sysopt connection permit-ipsec**および**sysopt ipsec pl-compatible**コマンドを使用して、VPN ClientをPIXファイアウォールに接続する方法を示します。このドキュメントでは、**nat 0 access-list**コマンドについても説明します。

注：暗号化テクノロジーは、輸出規制の対象となります。暗号化技術の輸出に関する法律を知ることは、お客様の責任です。輸出規制に関する質問がございましたら、電子メールで export@cisco.comまでお問い合わせください。

前提条件

要件

このドキュメントに特有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、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure PIXソフトウェアリリース5.0.3(Cisco Secure VPN Client 1.0(Help > Aboutメニューで2.0.7と表示)またはCisco Secure VPN Client 1.1を使用したCisco Secure PIXソフトウ

エアリリース6.2.1(Help > Aboutメニューで2.1.12と表示)。
- インターネットマシンは、内部のWebホストにIPアドレス192.68.0.50でアクセスします。
- VPN Clientは、すべてのポート(10.1.1.0 /24および10.2.2.0 /24)を使用して、内部のすべてのマシンにアクセスします。

このマニュアルの情報は、特定のラボ環境に置かれた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でも、使用する前に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。

表記法

ドキュメント表記の詳細は、「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

PIX では、**access-list** および **nat 0** コマンドが連携して機能します。**nat 0 access-listコマンドは**、**sysopt ipsec pl-compatibleコマンドの代わりに使用することを意図して**います。**nat 0**コマンドをmatching **access-list**コマンドとともに使用する場合は、VPN接続を行うクライアントのIPアドレスを知っている必要があります。これにより、NATをバイパスする一致するアクセスコントロールリスト(ACL)が作成されます。

注： sysopt ipsec pl-compatibleコマンドは、ネットワークアドレス変換(NAT)をバイパスするために、一致する**access-listコマンド**を使用して**nat 0コマンドよりも**拡張が適切です。 これは、接続を行うクライアントのIPアドレスを知る必要がないためです。このドキュメントの設定では、交換可能なコマンドは太字で示されています。

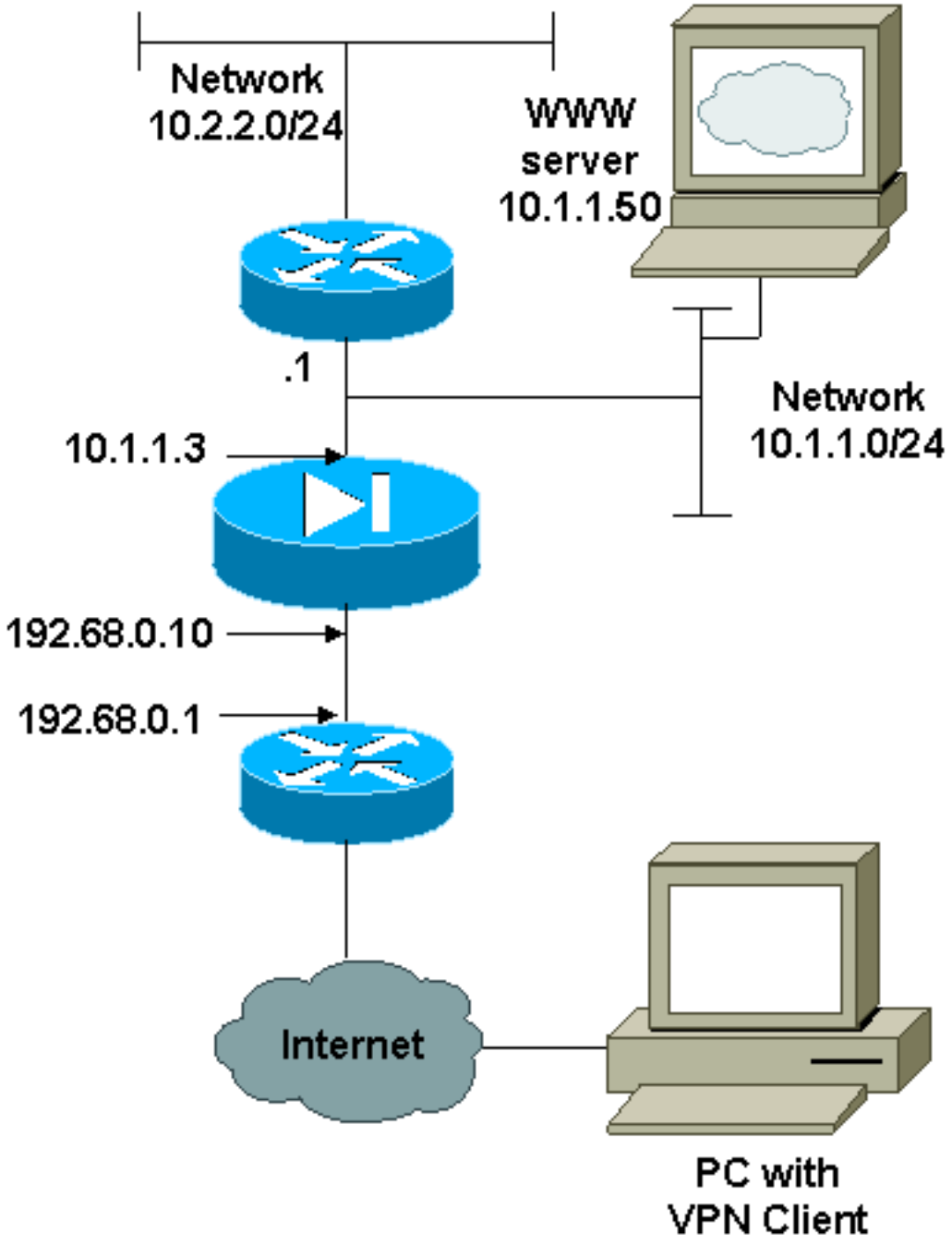
VPN Clientを持つユーザは、インターネットサービスプロバイダー(ISP)に接続し、IPアドレスを受信します。 ユーザは、ファイアウォールの内側にあるすべてのデバイスにアクセスできます。これにはネットワークが含まれます。また、クライアントを実行しないユーザは、静的割り当てによって提供されるアドレスを使用してWebサーバに接続できます。内部のユーザはインターネットに接続できます。トラフィックがIPSecトンネルを通過する必要はありません。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

ネットワーク図

このドキュメントでは、次の図で示されるネットワーク設定を使用しています。



設定

このドキュメントでは、次に示す設定を使用しています。

- PIX
- VPN クライアント

PIX の設定

```
PIX Version 6.2.1
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
```

```
fixup protocol smtp 25
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol sqlnet 1521
names
!--- The ACL to bypass the NAT. You have to know the !--
- IP address of the Client. In this case, it is !---
subnet 65.10.10.0/24. access-list 103 permit ip 10.0.0.0
255.0.0.0 65.10.10.0 255.255.255.0
pager lines 24
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
no logging trap
logging facility 20
logging queue 512
interface ethernet0 10baset
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 192.68.0.10 255.255.255.0
ip address inside 10.1.1.3 255.255.255.0
no failover
failover timeout 0:00:00
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 192.68.0.11-192.168.0.15 netmask
255.255.255.0
!--- Binding ACL 103 to the NAT statement in order to !-
-- avoid NAT on the IPSec packet. nat (inside) 0 access-
list 103
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 192.68.0.50 10.1.1.50 netmask
255.255.255.255 0 0
conduit permit icmp any any
no rip outside passive
no rip outside default
no rip inside passive
no rip inside default
route outside 0.0.0.0 0.0.0.0 192.68.0.1 1
route inside 10.2.2.0 255.255.255.0 10.1.1.1 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00
udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
!--- The sysopt ipsec pl-compatible command !--- avoids
conduit on the IPSec encrypted traffic. !--- This
command needs to be used if you do not use !--- the nat
0 access-list command.

sysopt ipsec pl-compatible
sysopt connection permit-ipsec
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set myset
crypto map dyn-map 20 ipsec-isakmp dynamic cisco
```

```
crypto map dyn-map interface outside
isakmp enable outside
isakmp key cisco123 address 0.0.0.0 netmask 0.0.0.0
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
terminal width 80
Cryptochecksum:c687aa0afb1dd03abce04c31566b5c52
: end
[OK]
```

VPN Client の設定

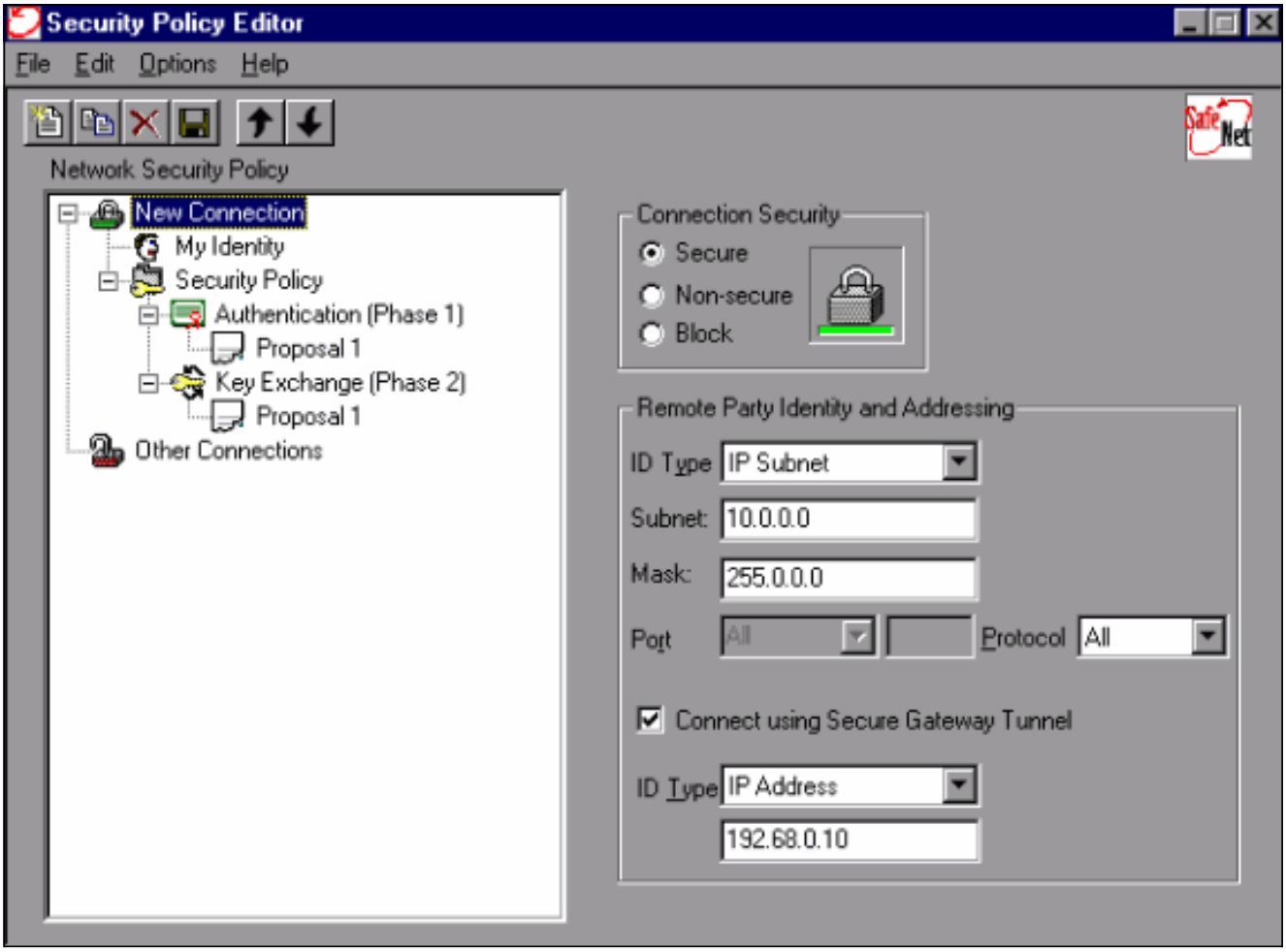
```
Network Security policy:
 1- TACconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP subnet
          10.0.0.0
           255.0.0.0
          Port all Protocol all

     Connect using secure tunnel
          ID Type: IP address
          192.68.0.10

     Authentication (Phase 1)
     Proposal 1
         Authentication method: pre-shared key
         Encryp Alg: DES
         Hash Alg: MD5
         SA life: Unspecified
         Key Group: DH 1


     Key exchange (Phase 2)
     Proposal 1
         Encapsulation ESP
         Encrypt Alg: DES
         Hash Alg: MD5
         Encap: tunnel
         SA life: Unspecified
         no AH


 2- Other Connections
        Connection security: Non-secure
        Local Network Interface
          Name: Any
          IP Addr: Any
          Port: All
```

VPN Client IPSec接続用ポリシーの設定

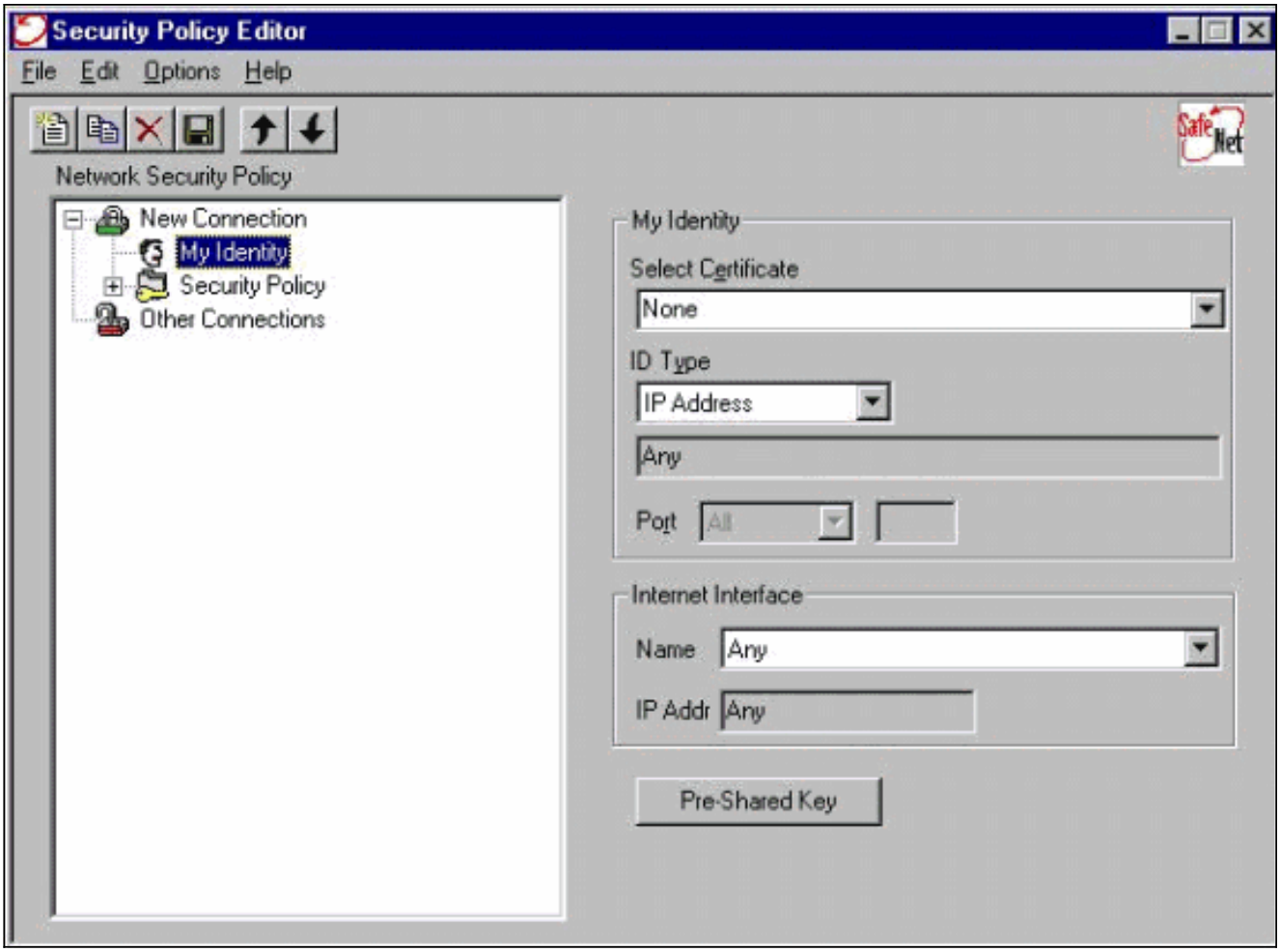
VPN Client IPSec接続用のポリシーを設定するには、次の手順を実行します。

1. [Remote Party Identity and Addressing]タブで、VPN Clientを使用して到達できるプライベ

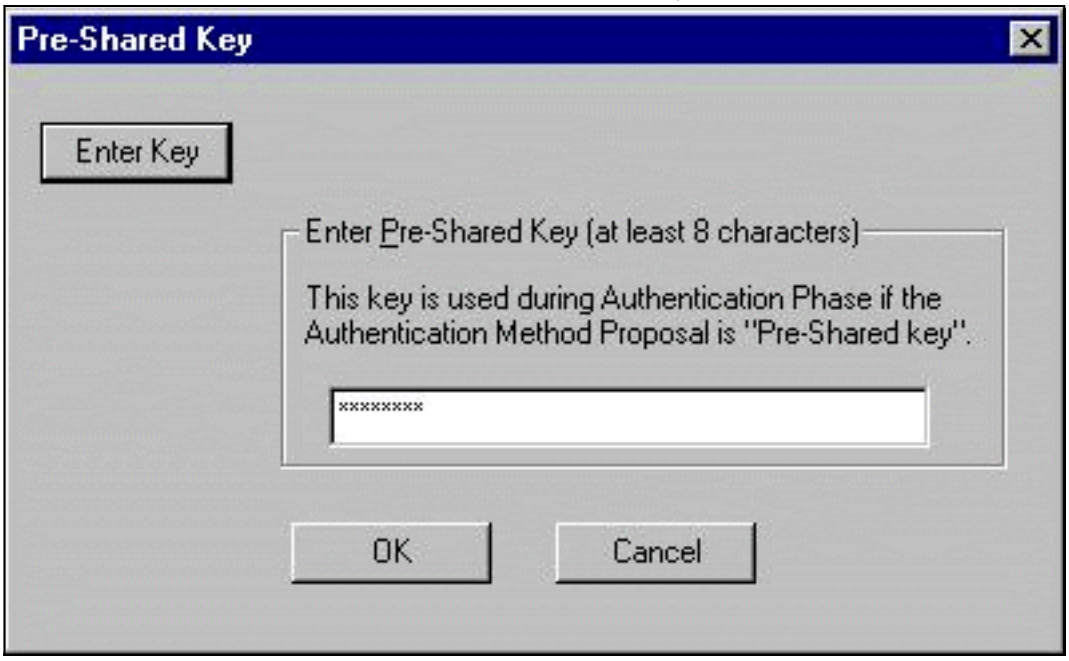
ートネットワークを定義します。次に、[Connect using **Secure Gateway Tunnel]を選択**し、PIXの外部IPアドレスを定義します。



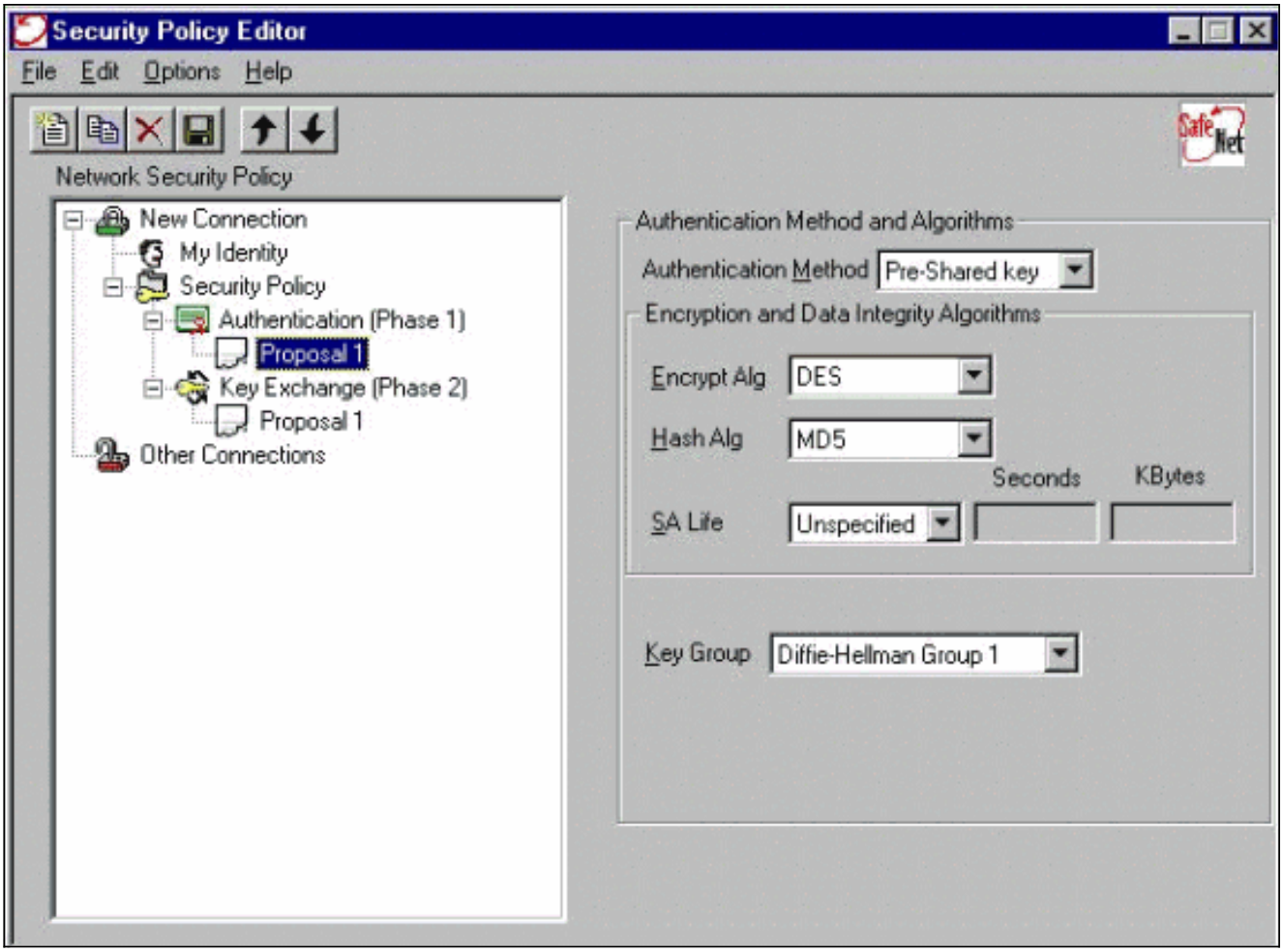
2. [マイ**アイデンティティ**]を選択し、設定をデフォルトのままにします。次に、[事前共有キー]**ボタンをクリック**します。



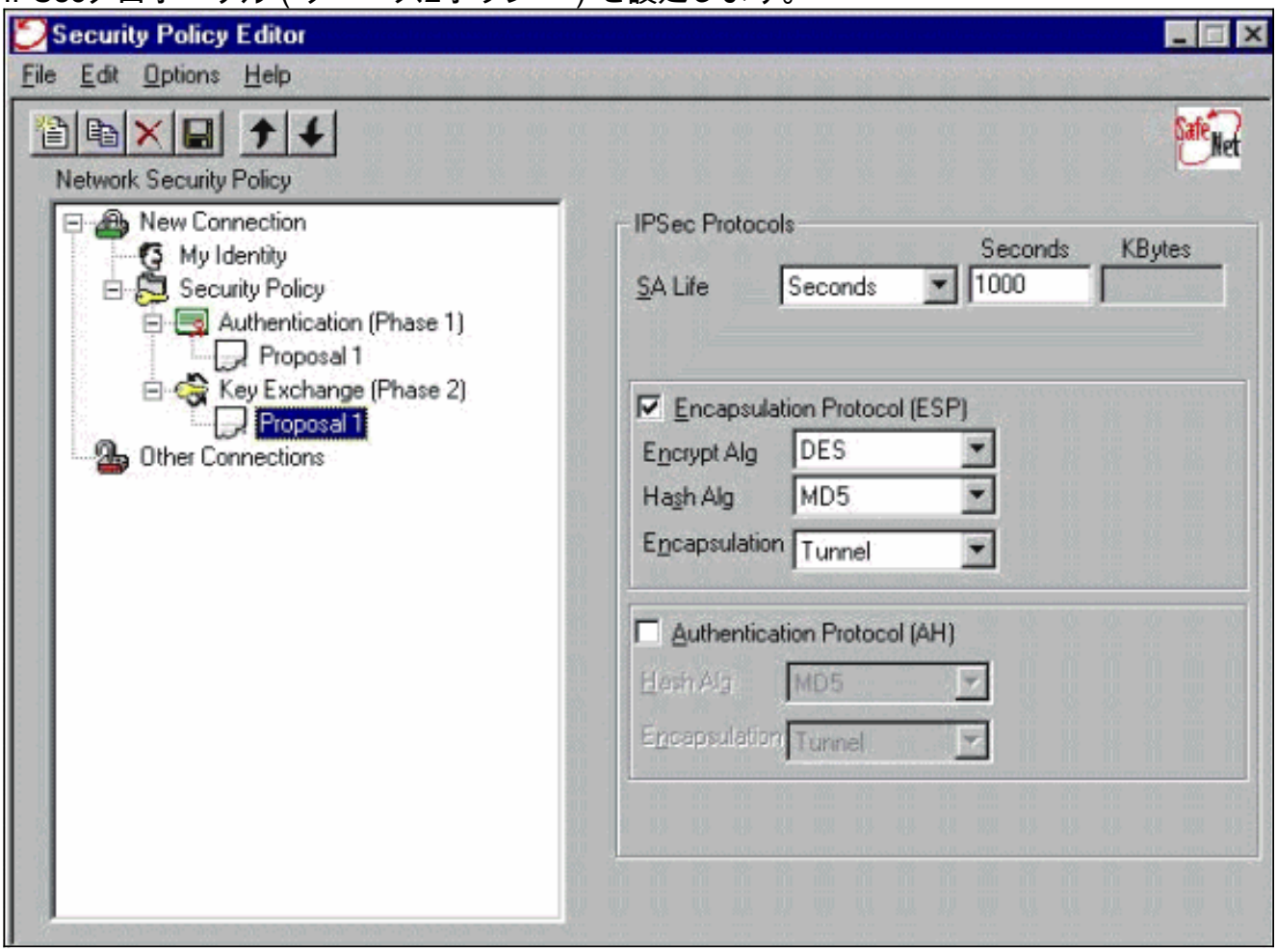
3. PIXで設定されている事前共有キーを入力します。



4. 認証提案を設定します（フェーズ1ポリシー）。



5. IPSecプロポーザル（フェーズ2ポリシー）を設定します。



注：完了したら、必ずポリシーを保存してください。DOSウィンドウを開き、PIXの内部ネット

ワーク上の既知のホストにpingを実行して、クライアントからトンネルを開始します。トンネルのネゴシエートを試みる最初のpingから、インターネット制御メッセージプロトコル(ICMP)到達不能メッセージを受信します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

デバッグ コマンド

注：debugコマンドを発行する前に、『debugコマンドの重要な情報』を参照してください。

クライアント側のデバッグを表示するには、Cisco Secure Log Viewerを有効にします。

- **debug crypto ipsec sa**：フェーズ2のIPSecネゴシエーションを表示します。
- **debug crypto isakmp sa**：フェーズ1のISAKMPネゴシエーションを表示します。
- **debug crypto engine**：暗号化されたセッションを表示します。

関連情報

- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- Cisco PIX Firewall Software に関する製品サポート
- Requests for Comments (RFCs)
- IP セキュリティ（IPSec）製品に関するサポートページ
- IPSec ネットワーク セキュリティの設定
- Internet Key Exchange セキュリティ プロトコルの設定
- IP セキュリティ（IPSec）暗号化の概要
- PIX ファイアウォールを介した接続
- IPSec の設定
- テクニカル サポートとドキュメント – Cisco Systems