Configurando o PIX para Cisco Secure VPN Client Wild-card, pré-compartilhado, sem configuração de modo

Contents

Introduction

Esta configuração demonstra como conectar um VPN Client a um PIX Firewall com o uso de curingas e os comandos **sysopt connection permit-ipsec** e **sysopt ipsec pl-compatible**. Este documento também aborda o comando **nat 0 access-list**.

Observação: a tecnologia de criptografia está sujeita a controles de exportação. É sua responsabilidade conhecer a lei relacionada à exportação de tecnologia de criptografia. Se você tiver alguma dúvida relacionada ao controle de exportação, envie um e-mail para export@cisco.com.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware.

- Cisco Secure PIX Software versão 5.0.3 com Cisco Secure VPN Client 1.0 (mostrado como 2.0.7 no menu Ajuda > Sobre) ou Cisco Secure PIX Software versão 6.2.1 com Cisco Secure VPN Client 1.1 (mostrado como 2.1.12 no menu Ajuda > Sobre).
- As máquinas da Internet acessam o host da Web no interior com o endereço IP 192.68.0.50.
- O VPN Client acessa todas as máquinas internas com o uso de todas as portas (10.1.1.0 /24 e 10.2.2.0 /24).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você trabalhar em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informações de Apoio

No PIX, os comandos access-list e nat 0 trabalham juntos. O comando **nat 0 access-list** deve ser usado em vez do comando **sysopt ipsec pl-compatible**. Se você usa o comando **nat 0** com o comando **access-list** correspondente, você precisa saber o endereço IP do cliente que faz a conexão VPN para criar a lista de controle de acesso (ACL) correspondente para ignorar o NAT.

Observação: o comando **sysopt ipsec pl-compatible** é dimensionado melhor do que o **nat 0** com o **access-list** command ir correspondente para ignorar a Network Address Translation (NAT). O motivo é que você não precisa saber o endereço IP dos clientes que fazem a conexão. Os comandos intercambiáveis estão em negrito na configuração neste documento.

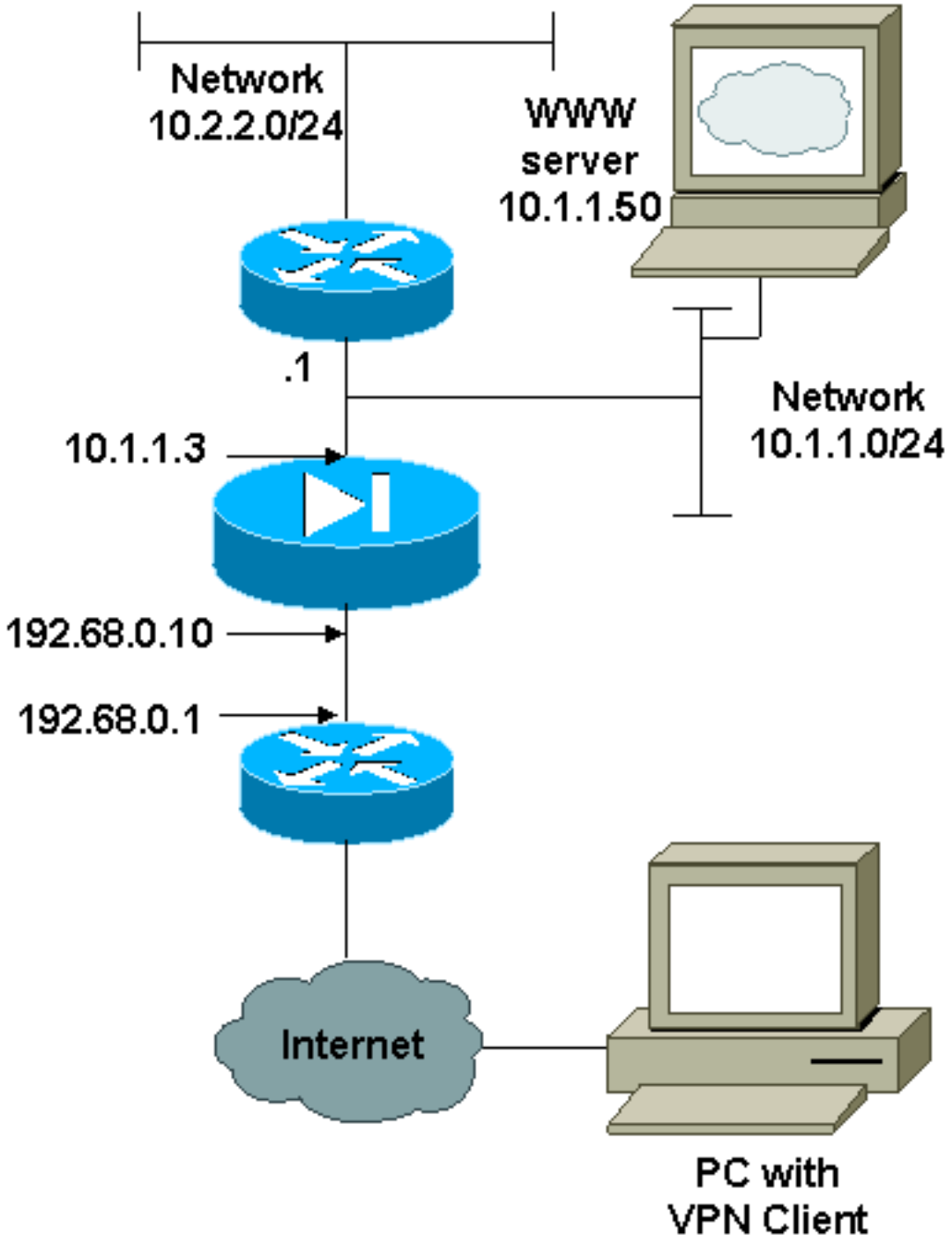
Um usuário com um VPN Client se conecta e recebe um endereço IP de seu provedor de serviços de Internet (ISP). O usuário tem acesso a tudo no interior do firewall. Isso inclui redes. Além disso, os usuários que não executam o cliente podem se conectar ao Servidor Web com o uso do endereço fornecido pela atribuição estática. Os usuários internos podem se conectar à Internet. Não é necessário que seu tráfego passe pelo túnel IPSec.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.



Configurações

Este documento utiliza as configurações mostradas aqui.

- PIX
- Cliente de VPN

Configuração de PIX

```
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]
```

Configuração de cliente de VPN

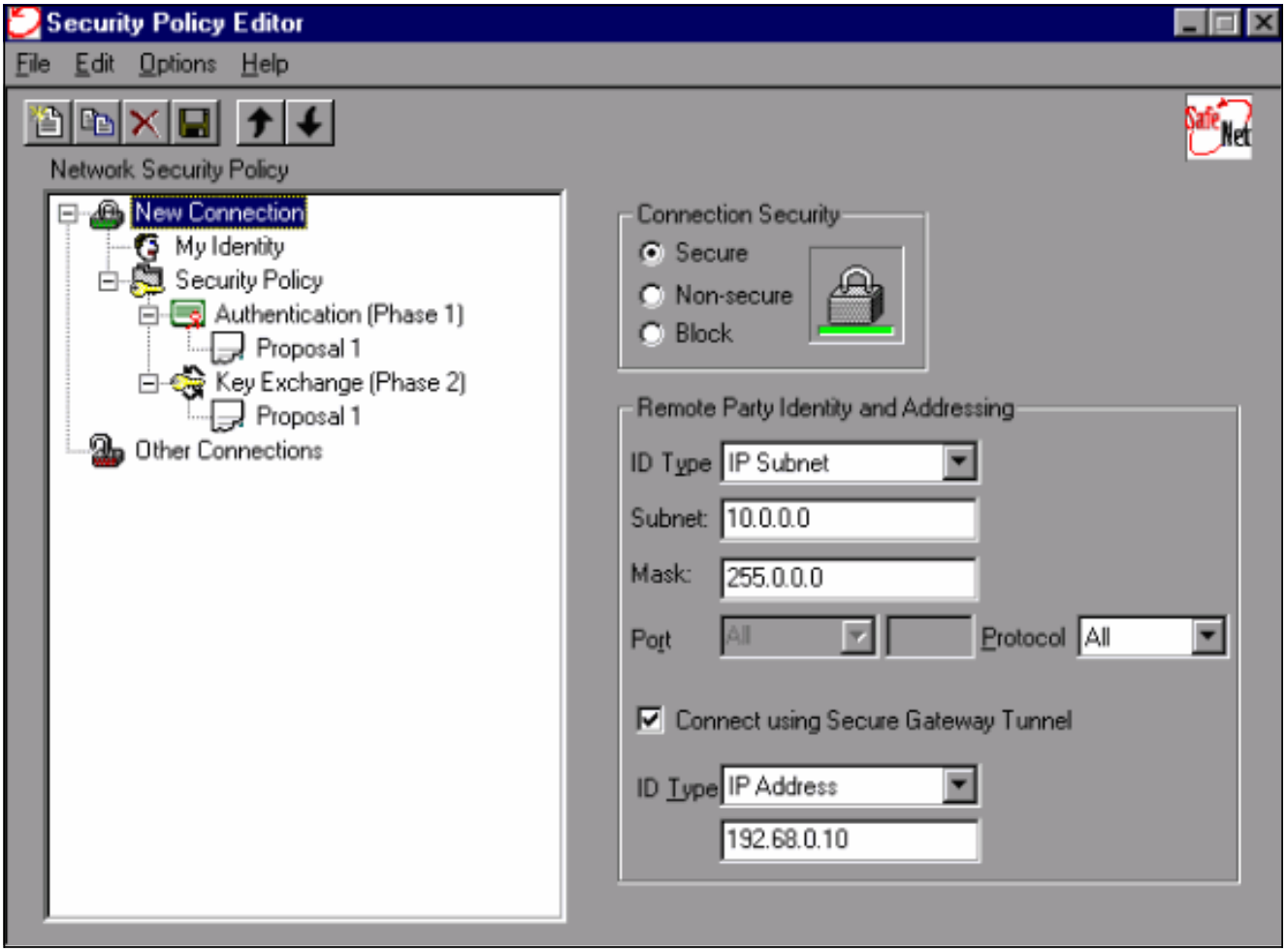
```
Network Security policy:
 1- TACconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP subnet
          10.0.0.0
           255.0.0.0
          Port all Protocol all

     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
```

Configurar a política para a conexão IPSec do cliente VPN

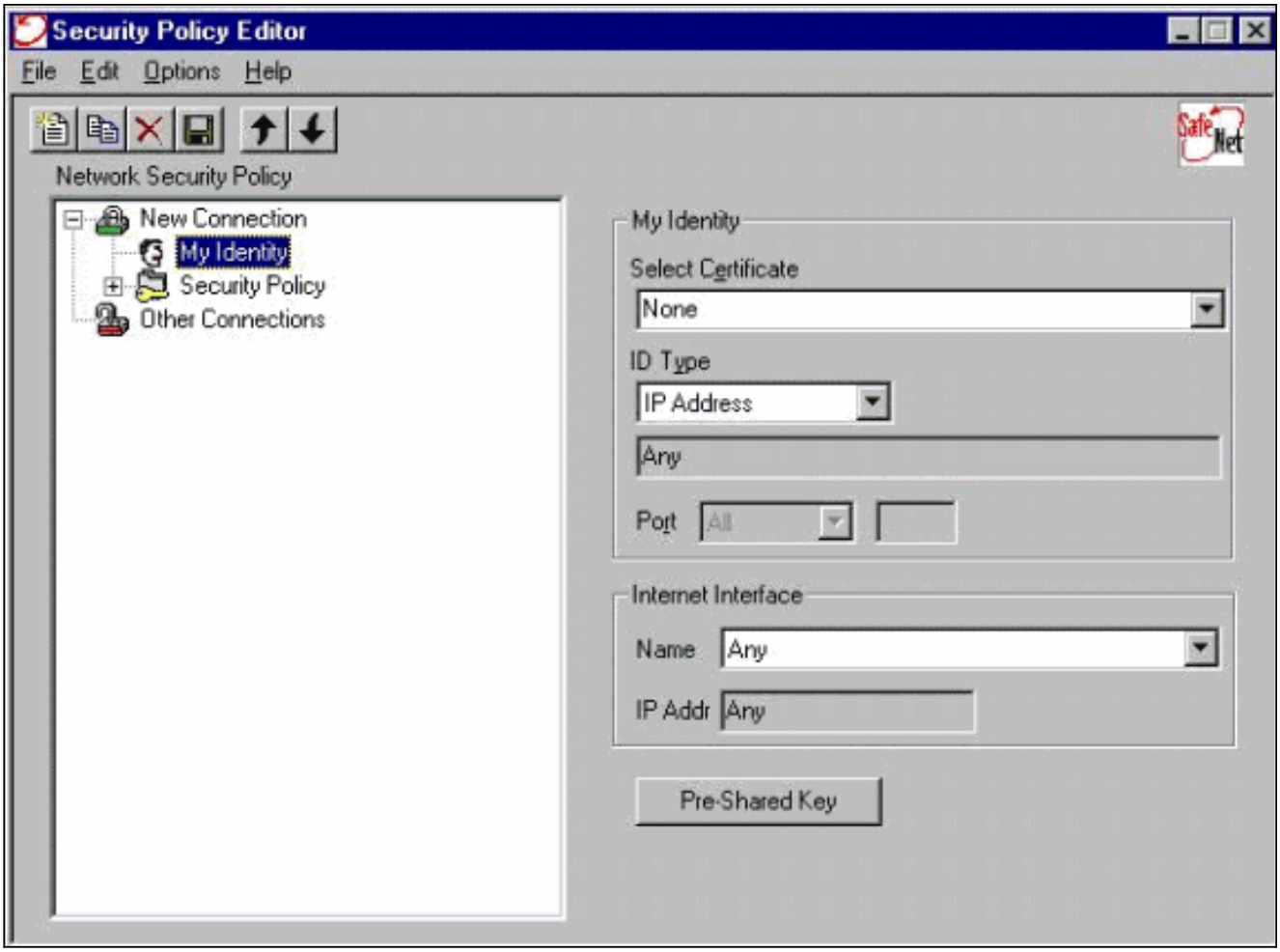
Siga estas etapas para configurar a política para a conexão IPSec do VPN Client.

1. Na guia Remote Party Identity and Addressing, defina a rede privada que você deseja

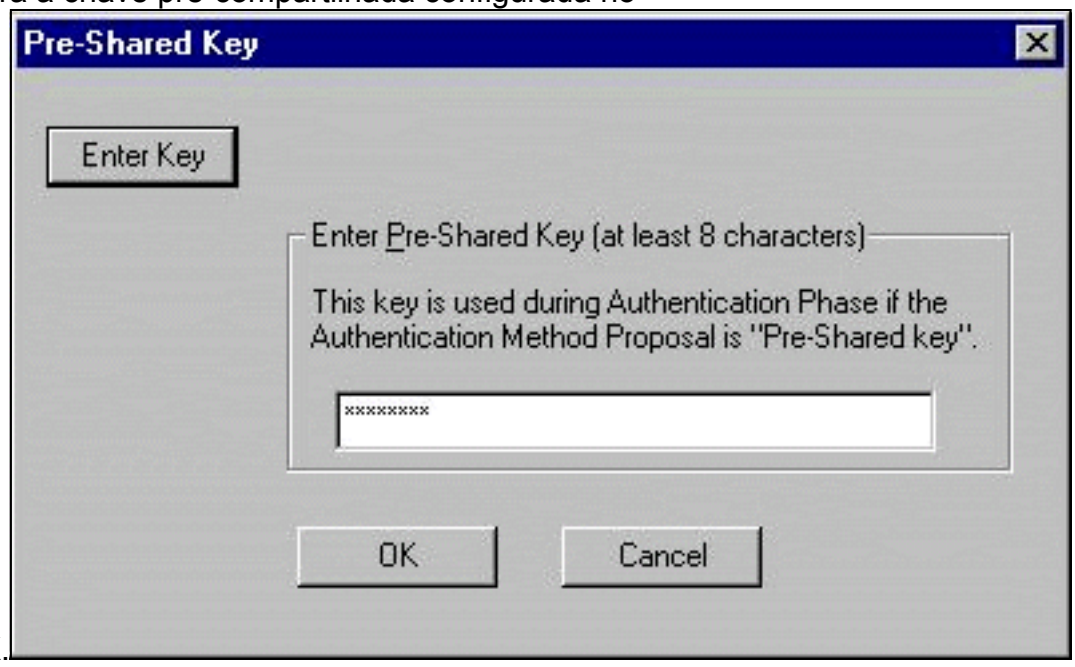
acessar com o uso do VPN Client. Em seguida, selecione **Connect using Secure Gateway Tunnel** e defina o endereço IP externo do PIX.



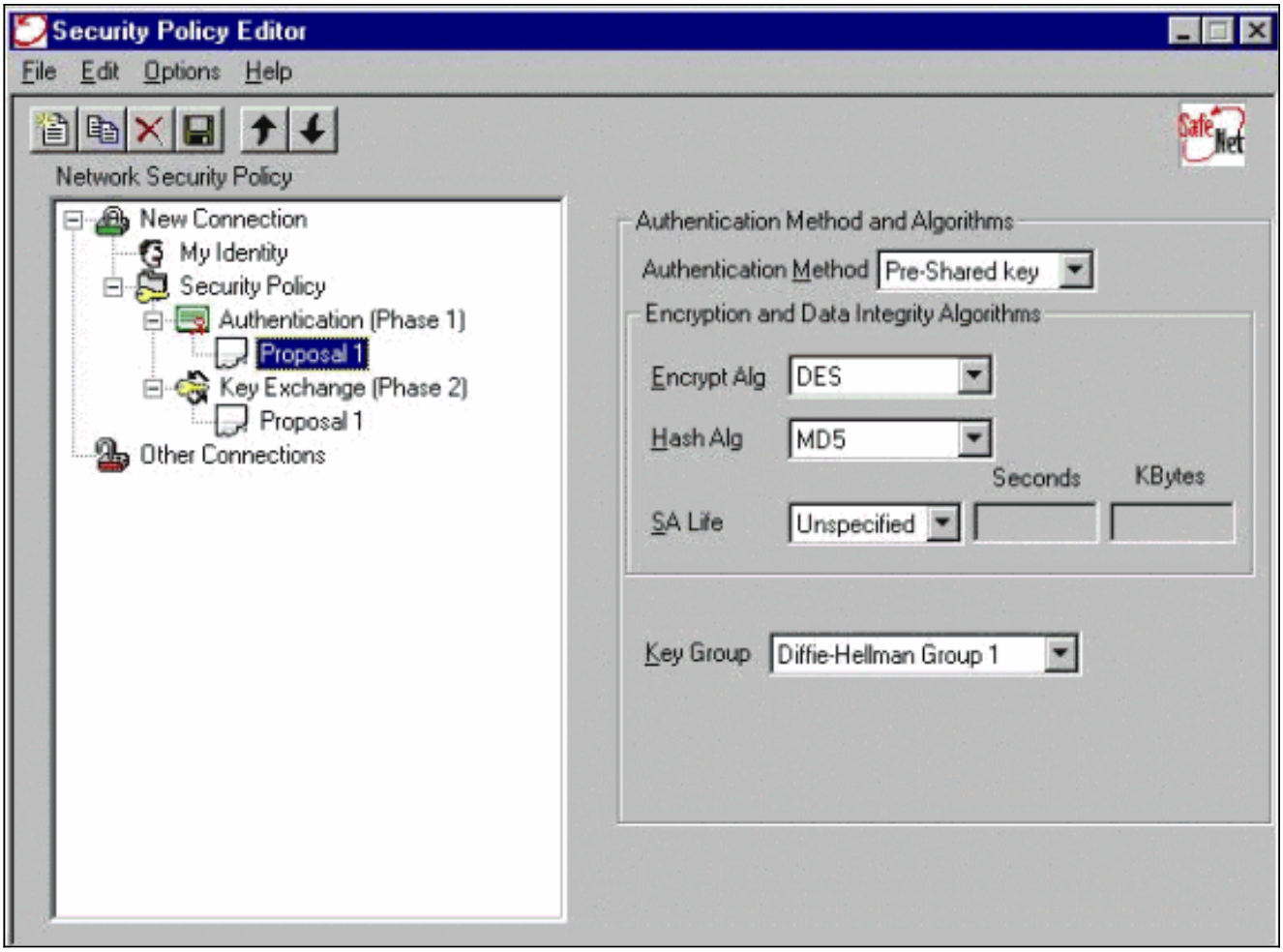
2. Selecione **Minha identidade** e deixe a configuração para o padrão. Em seguida, clique no botão **Pre-Shared Key (Chave pré-compartilhada)**.



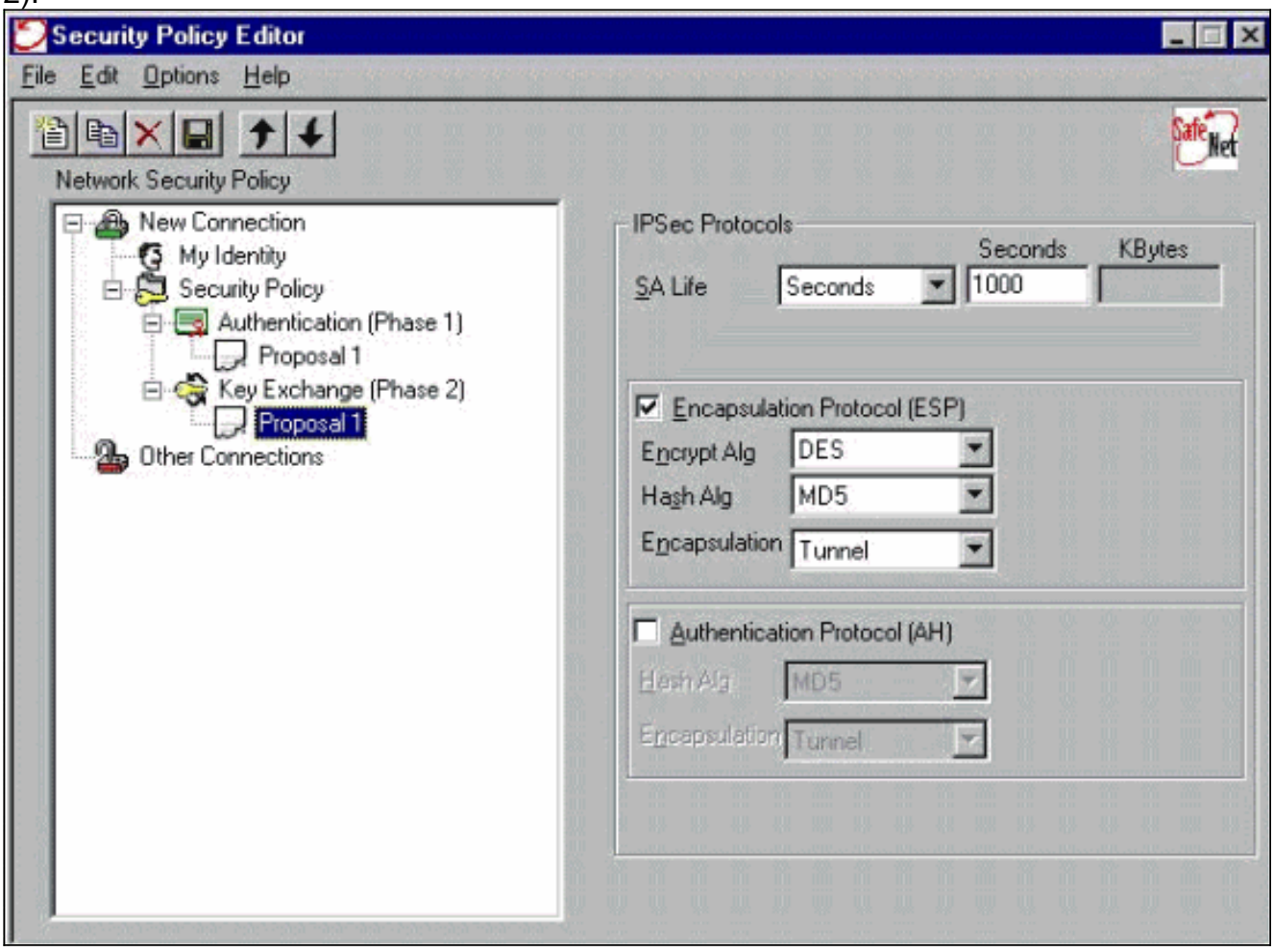
3. Insira a chave pré-compartilhada configurada no PIX.



4. Configure a proposta de autenticação (política da Fase 1).



5. Configure a proposta de IPSec (política da Fase 2).



Nota: não se esqueça de salvar a diretiva quando terminar. Abra uma janela do DOS e faça ping em um host conhecido na rede interna do PIX para iniciar o túnel a partir do cliente. Você recebe uma mensagem de Internet Control Message Protocol (ICMP) inalcançável do primeiro ping enquanto ele tenta negociar o túnel.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos debug

Observação: antes de emitir comandos **debug**, consulte Informações Importantes sobre Comandos Debug.

Para ver as depurações no lado do cliente, ative o Cisco Secure Log Viewer:

- **debug crypto ipsec sa** - Exibe as negociações de IPSec da fase 2.
- **debug crypto isakmp sa** - Exibe as negociações ISAKMP da fase 1.
- **debug crypto engine** - Exibe as sessões criptografadas.

Informações Relacionadas

- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Suporte ao produto do software Cisco PIX Firewall
- Solicitações de Comentários (RFCs)
- Páginas de Suporte do Produto IPSec (Protocolo de Segurança IP)
- Configuração da segurança de rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Uma introdução à criptografia do protocolo de segurança IP (IPSEC)
- Conectividade através do PIX Firewall
- Configurando IPSec
- Suporte Técnico e Documentação - Cisco Systems