Configuración de PIX para comodín, previamente compartido, no configuración de modo del cliente VPN de Cisco Secure.

Contenido

Introducción

Esta configuración demuestra cómo conectar un VPN Client a un firewall PIX con el uso de comodines y los comandos **sysopt connection permit-ipsec** y **sysopt ipsec pl-compatible**. Este documento también cubre el comando **nat 0 access-list**.

Nota: La tecnología de cifrado está sujeta a controles de exportación. Es su responsabilidad conocer la ley relacionada con la exportación de tecnología de cifrado. Si tiene alguna pregunta relacionada con el control de exportaciones, envíe un correo electrónico a export@cisco.com.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Cisco Secure PIX Software versión 5.0.3 con Cisco Secure VPN Client 1.0 (mostrado como 2.0.7 en el menú Ayuda > Acerca de) o Cisco Secure PIX Software versión 6.2.1 con Cisco Secure VPN Client 1.1 (mostrado como 2.1.12 en el menú Ayuda > Acerca de).
- Las máquinas de Internet acceden al host web en el interior con la dirección IP 192.68.0.50.
- El VPN Client accede a todas las máquinas en el interior con el uso de todos los puertos (10.1.1.0 /24 y 10.2.2.0 /24).

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

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

Antecedentes

En el PIX, los comandos access-list y nat 0 funcionan de manera conjunta. El comando **nat 0 access-list** está destinado a ser utilizado en lugar del **comando sysopt ipsec pl-compatible**. Si utiliza el comando **nat 0** con el **comando access-list** coincidente, debe conocer la dirección IP del cliente que realiza la conexión VPN para crear la lista de control de acceso (ACL) coincidente para saltear la NAT.

Nota: El comando **sysopt ipsec pl-compatible** escala mejor que el comando **nat 0** con el comando **access-list** coincidente para omitir la traducción de direcciones de red (NAT). La razón es que no necesita conocer la dirección IP de los clientes que realizan la conexión. Los comandos intercambiables están en negrita en la configuración de este documento.

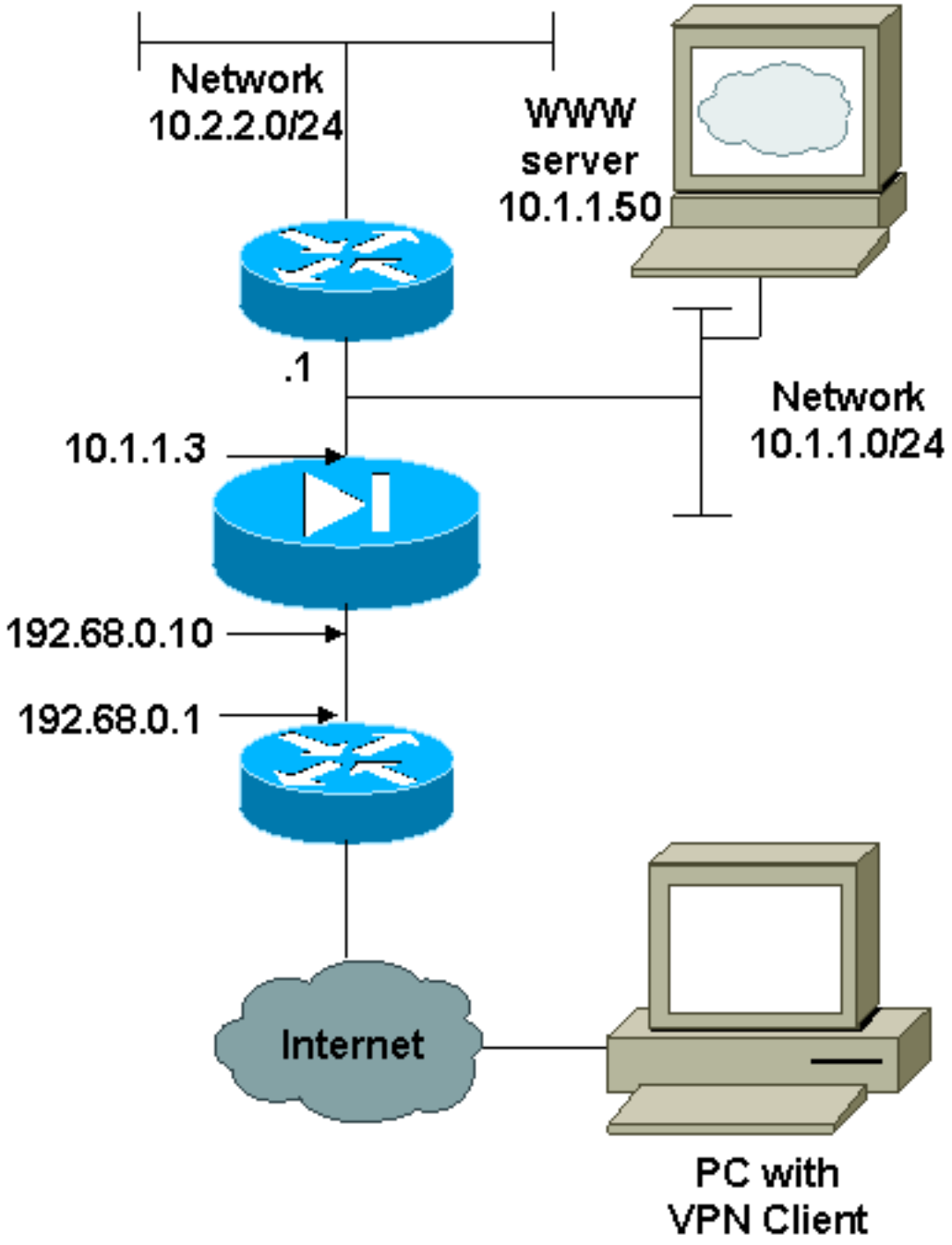
Un usuario con un cliente VPN se conecta y recibe una dirección IP de su proveedor de servicios de Internet (ISP). El usuario tiene acceso a todo lo que se encuentra dentro del firewall. Esto incluye las redes. Además, los usuarios que no ejecutan el cliente pueden conectarse al servidor web con el uso de la dirección proporcionada por la asignación estática. Los usuarios internos pueden conectarse a Internet. No es necesario que su tráfico pase por el túnel IPSec.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.



Configuraciones

Este documento usa las configuraciones detalladas aquí.

- PIX
- Cliente VPN

Configuración 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]
```

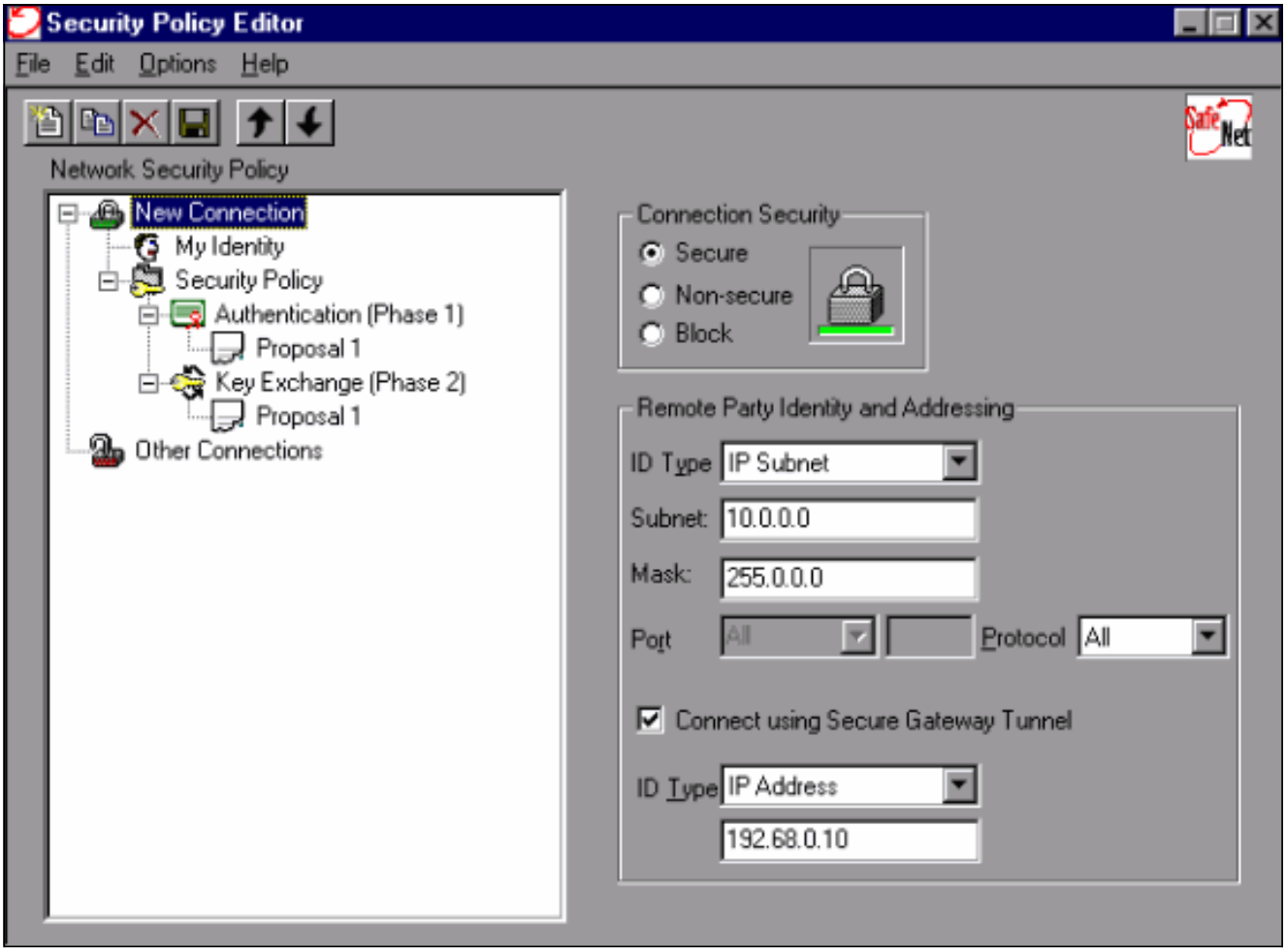
Configuración de cliente VPN

```
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
```

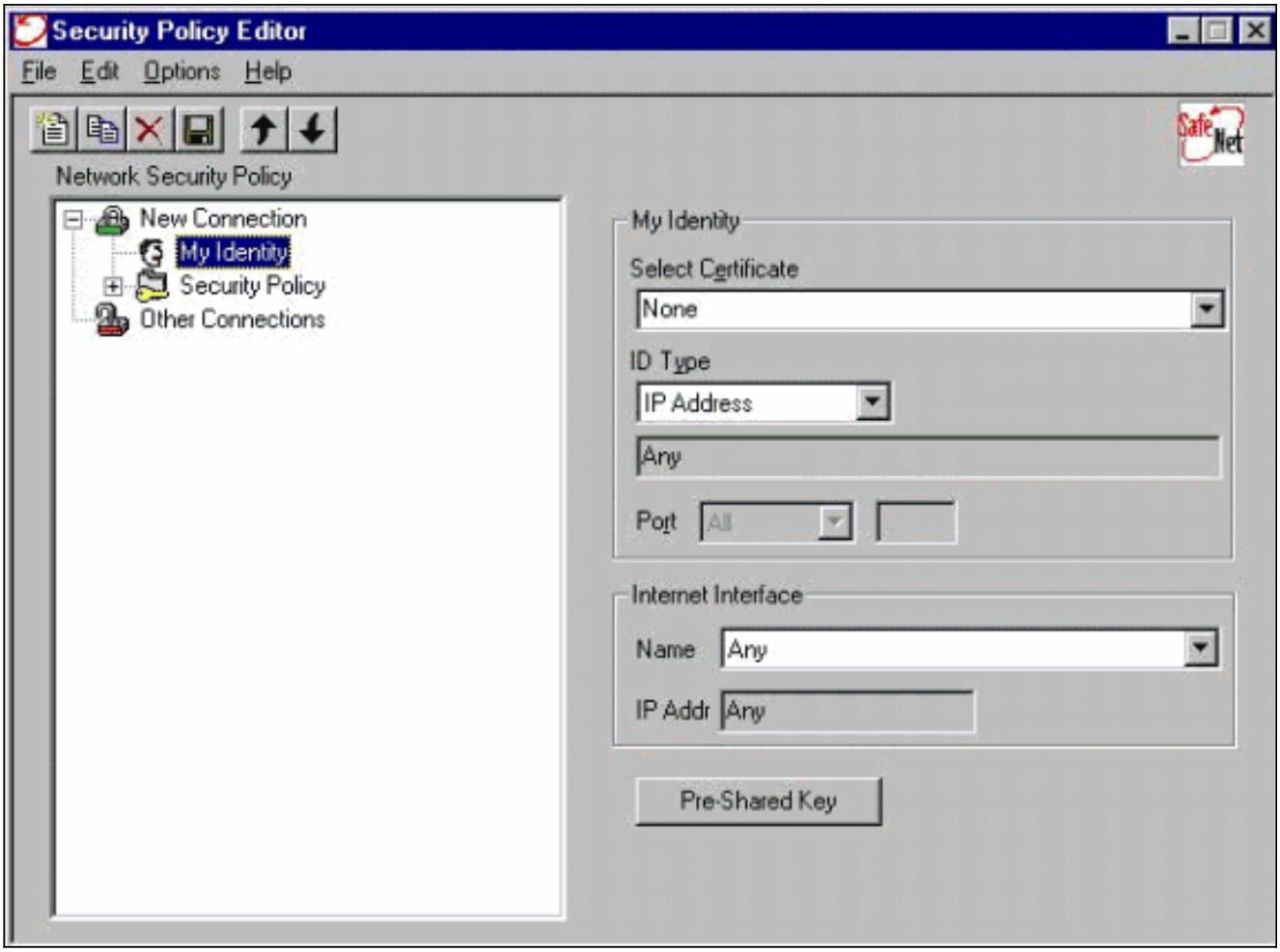
Configuración de la Política para la Conexión IPSec del Cliente VPN

Siga estos pasos para configurar la política para la conexión IPSec del cliente VPN.

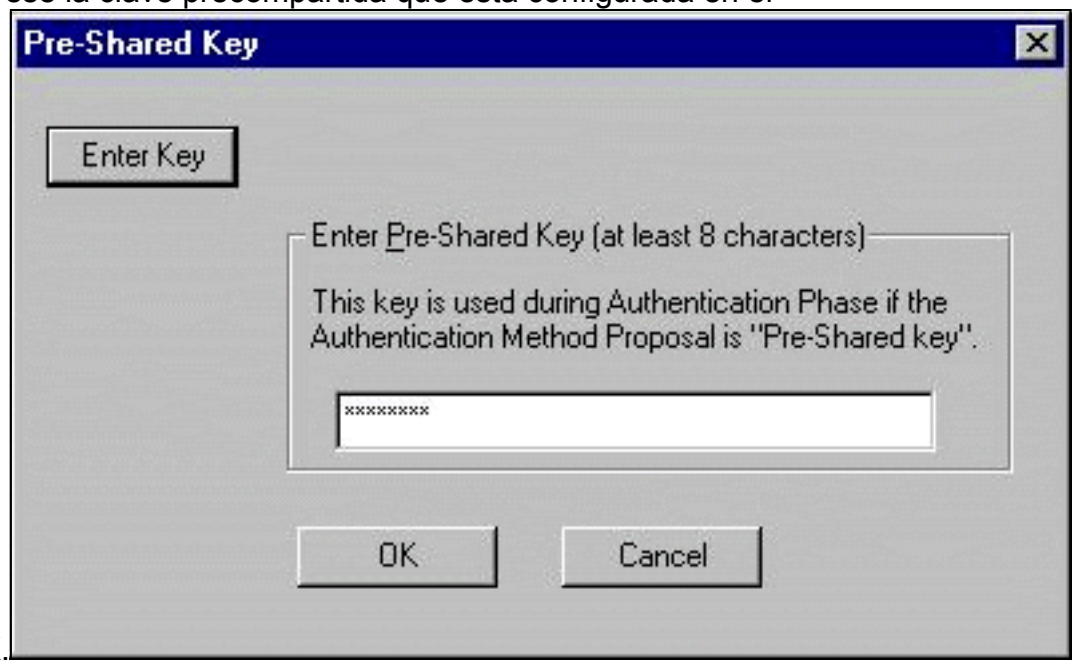
1. En la ficha Remote Party Identity and Addressing (Identidad de persona remota y dirección), defina la red privada a la que desea poder acceder con el uso del VPN Client. A continuación, seleccione **Connect using Secure Gateway Tunnel** y defina la dirección IP externa del
PIX.



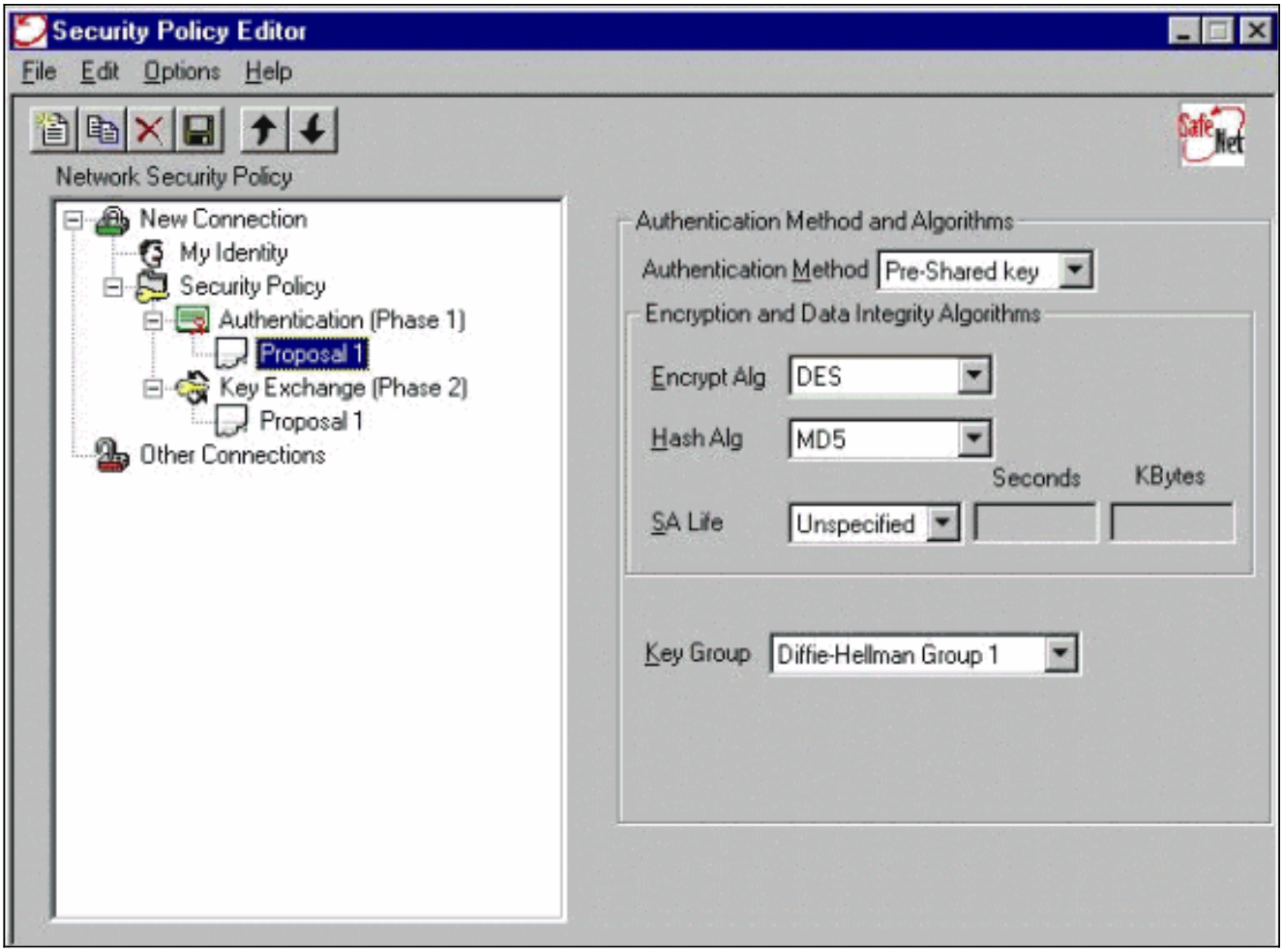
2. Seleccione **Mi identidad** y deje el valor predeterminado. A continuación, haga clic en el botón **Pre-Shared Key (Clave precompartida)**.



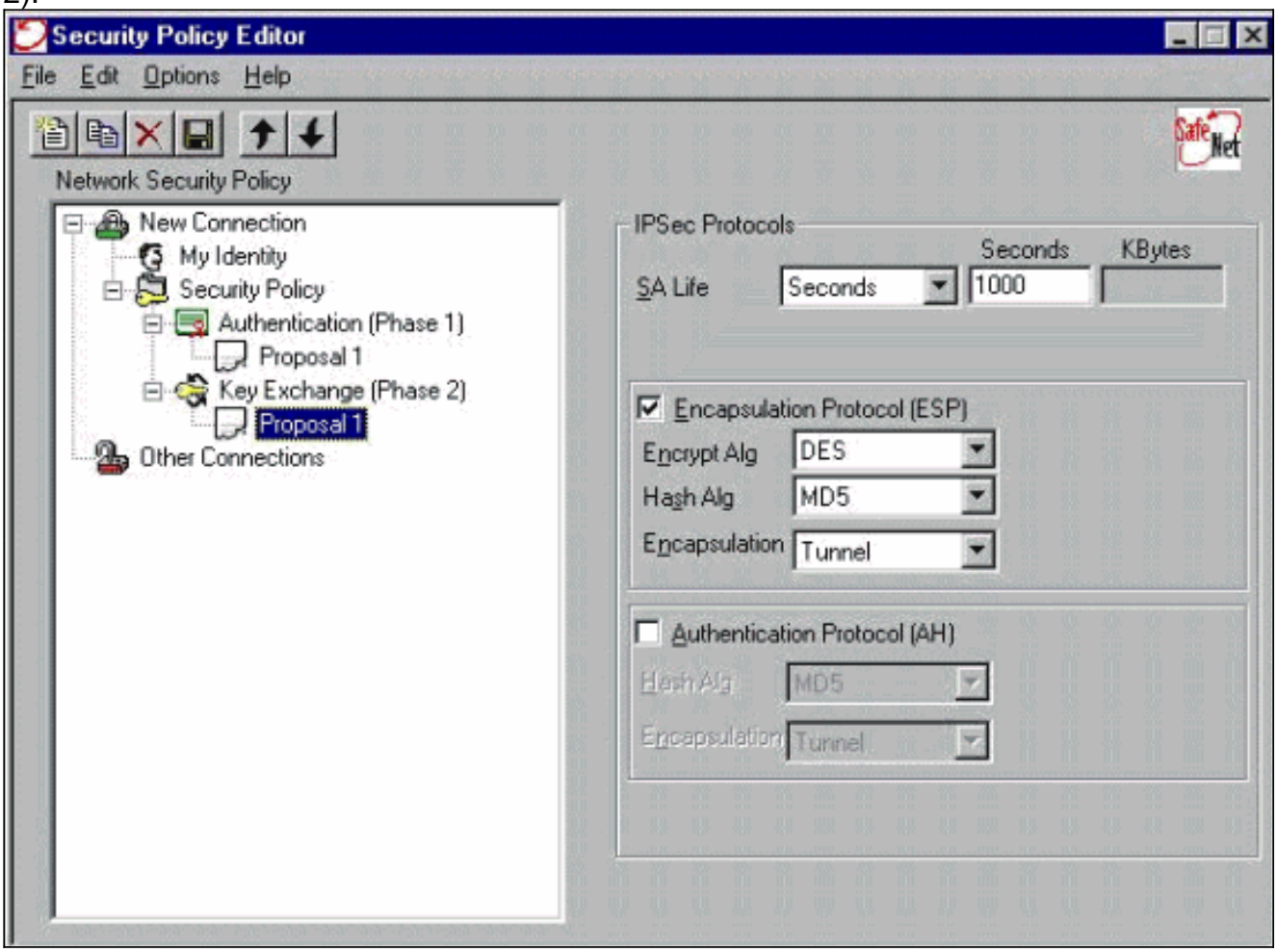
3. Ingrese la clave precompartida que está configurada en el PIX.



4. Configure la propuesta de autenticación (política de fase 1).



5. Configure la propuesta IPSec (política de fase 2).



Nota: No olvide guardar la política cuando haya terminado. Abra una ventana DOS y haga ping a un host conocido en la red interna del PIX para iniciar el túnel desde el cliente. Recibe un mensaje de protocolo de mensajes de control de Internet (ICMP) inalcanzable del primer ping cuando intenta negociar el túnel.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos de Debug

Nota: Antes de ejecutar **comandos debug**, consulte Información Importante sobre Comandos Debug.

Para ver las depuraciones del lado del cliente, habilite Cisco Secure Log Viewer:

- **debug crypto ipsec sa** - Muestra las negociaciones IPSec de la fase 2.
- **debug crypto isakmp sa** - Muestra las negociaciones ISAKMP de la fase 1.
- **debug crypto engine** - Muestra las sesiones cifradas.

Información Relacionada

- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Soporte de Productos del Software Cisco PIX Firewall
- Solicitudes de Comentarios (RFC)
- Páginas de soporte de productos de seguridad IP (IPSec)
- Configuración de seguridad de red IPSec
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Una Introducción al Cifrado de Seguridad IP (IPSec)
- Conectividad a través del Firewall PIX
- Configuración del IPSec
- Soporte Técnico y Documentación - Cisco Systems