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

Contenido

Introducción

Esta configuración demuestra cómo conectar a un cliente VPN con un firewall PIX con el uso de los comodines y de 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 encripción está sujeta a los controles de exportación. Es su responsabilidad conocer la ley relacionada con la exportación de tecnología de encripción. Si usted tiene cualesquiera preguntas relacionadas con el control de la exportación, envíe un email a export@cisco.com.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Software Release 5.0.3 del Secure PIX de Cisco con el Cliente Cisco Secure VPN 1.0 (mostrado como 2.0.7 en el menú del Help (Ayuda) > About (Acerca de)) o el Software Release 6.2.1 del Secure PIX de Cisco con el Cliente Cisco Secure VPN 1.1 (mostrado como 2.1.12 en el menú del Help (Ayuda) > About (Acerca de)).
- Las máquinas de Internet acceden el host web en el interior con la dirección IP 192.68.0.50.
- Los accesos de cliente VPN 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. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Antecedentes

En el PIX, los comandos access-list y nat 0 funcionan de manera conjunta. Piensan al **comando nat 0 access-list** de ser utilizado en vez del **comando sysopt ipsec pl-compatible**. Si usted utiliza el **comando nat 0** con el comando matching access-list, usted tiene que conocer la dirección IP del cliente que hace la conexión VPN para crear el Access Control List que corresponde con (ACL) para desviar el NAT.

Nota: El sysopt ipsec pl-compatible command scales mejor que el **comando nat 0** con la orden ir del comando matching access-list de desviar el Network Address Translation (NAT). La razón es porque usted no necesita conocer la dirección IP de los clientes que hacen la conexión. Los comandos interchangeable son intrépidos en la configuración en este documento.

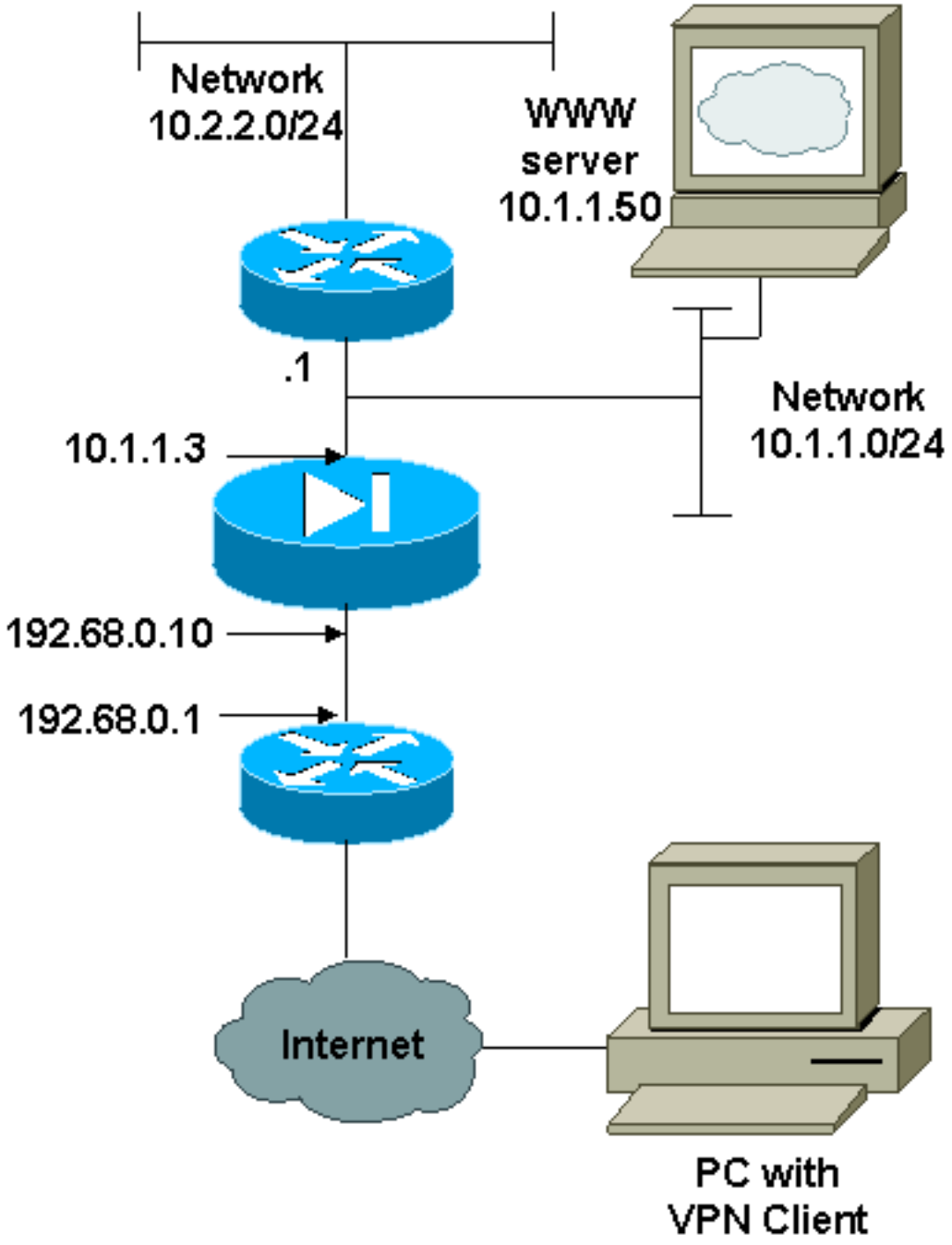
Un usuario con un cliente VPN conecta y recibe una dirección IP de su Proveedor de servicios de Internet (ISP). El usuario tiene acceso todo en el interior del Firewall. Esto incluye las redes. También, los usuarios que no funcionan con al cliente pueden conectar con el servidor Web con el uso del direccionamiento proporcionado por la asignación estática. Los usuarios en el interior pueden conectar con Internet. No es necesario que su tráfico pase a través del 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

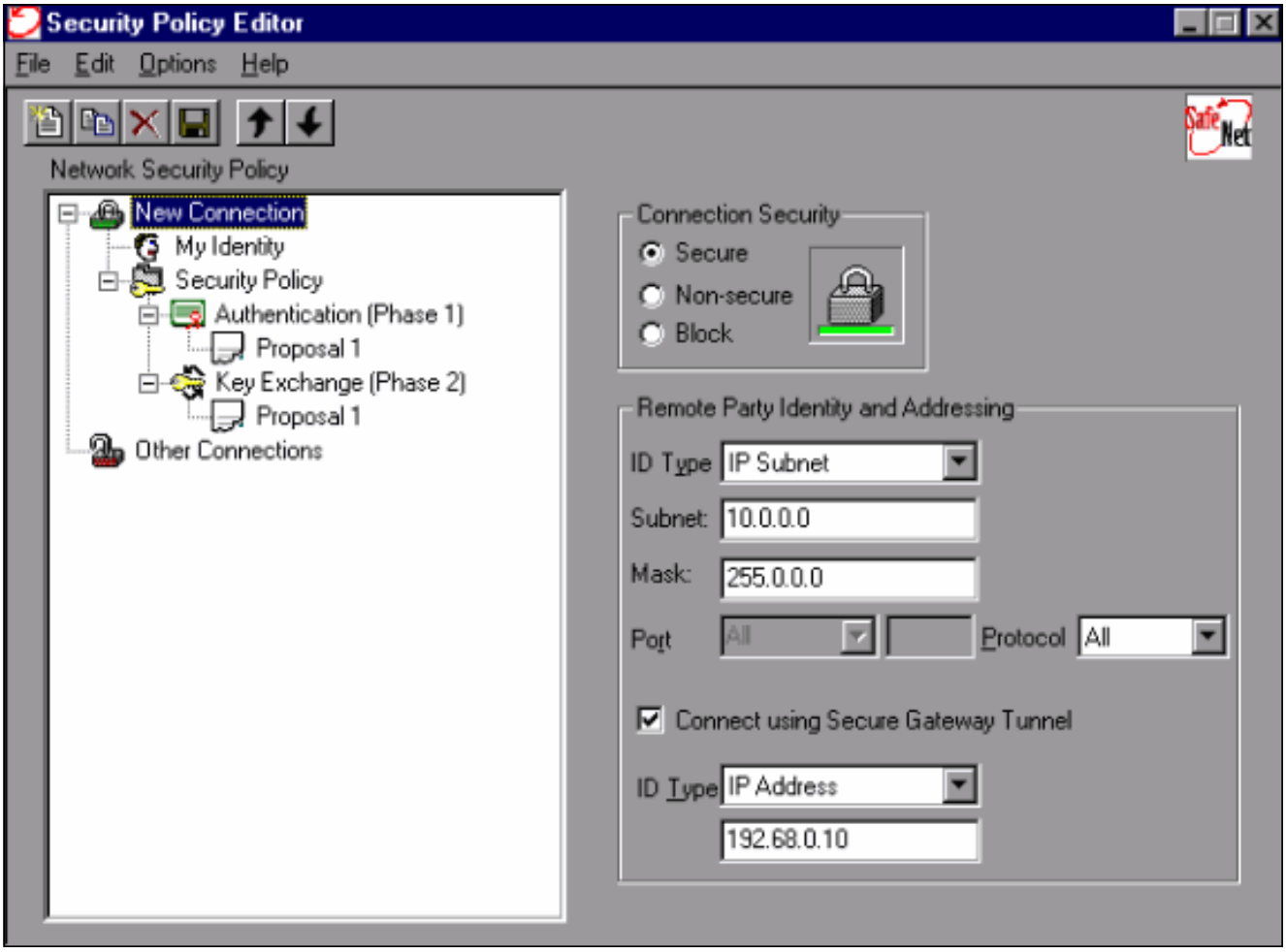
```
Network Security policy:
 1- TACconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP subnet
          10.0.0.0
           255.0.0.0
          Port all Protocol all

     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
```

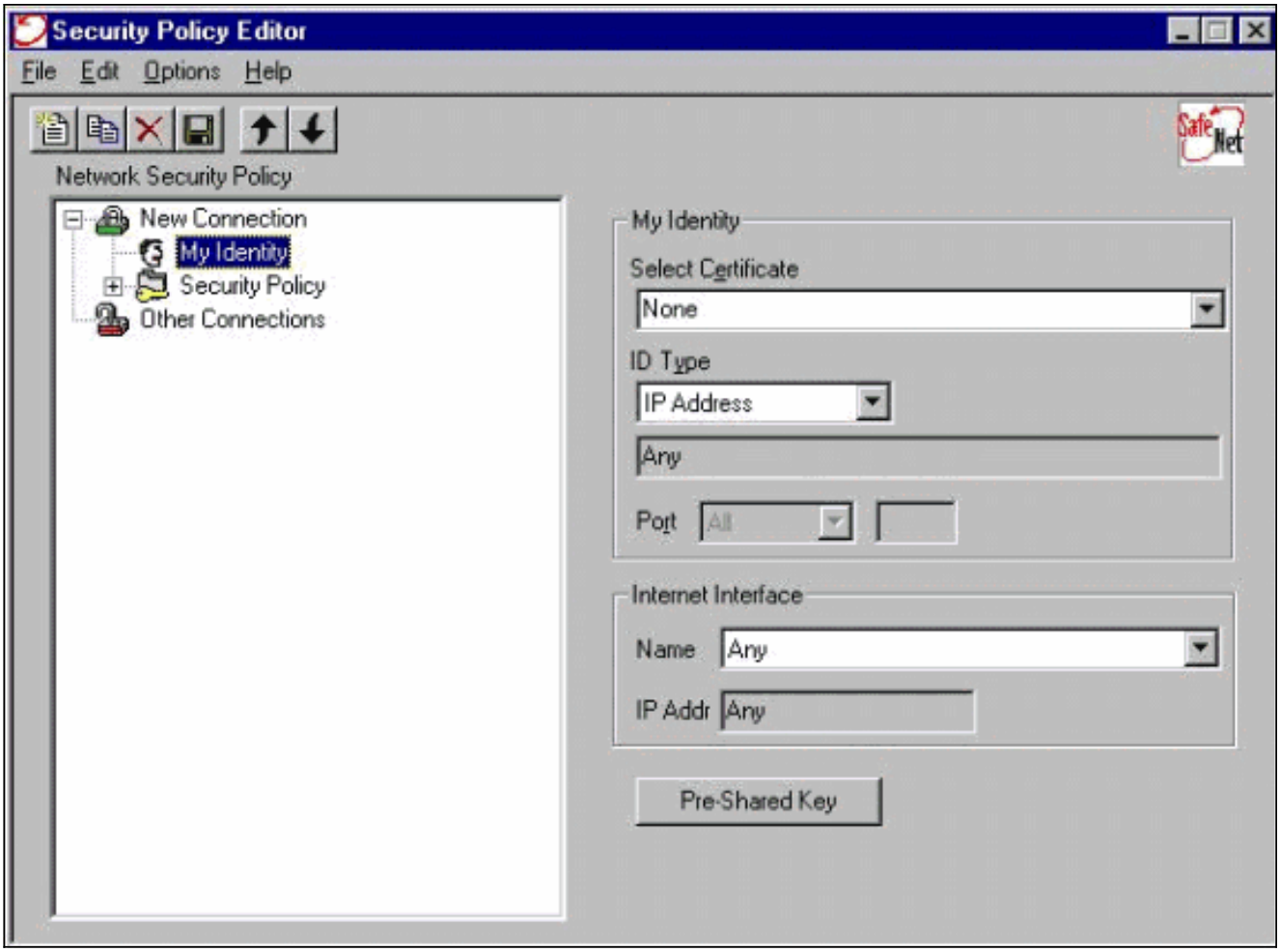
Configure la directiva para el cliente VPN conexión IPSec

Siga los siguientes pasos para configurar la directiva para el cliente VPN conexión IPSec.

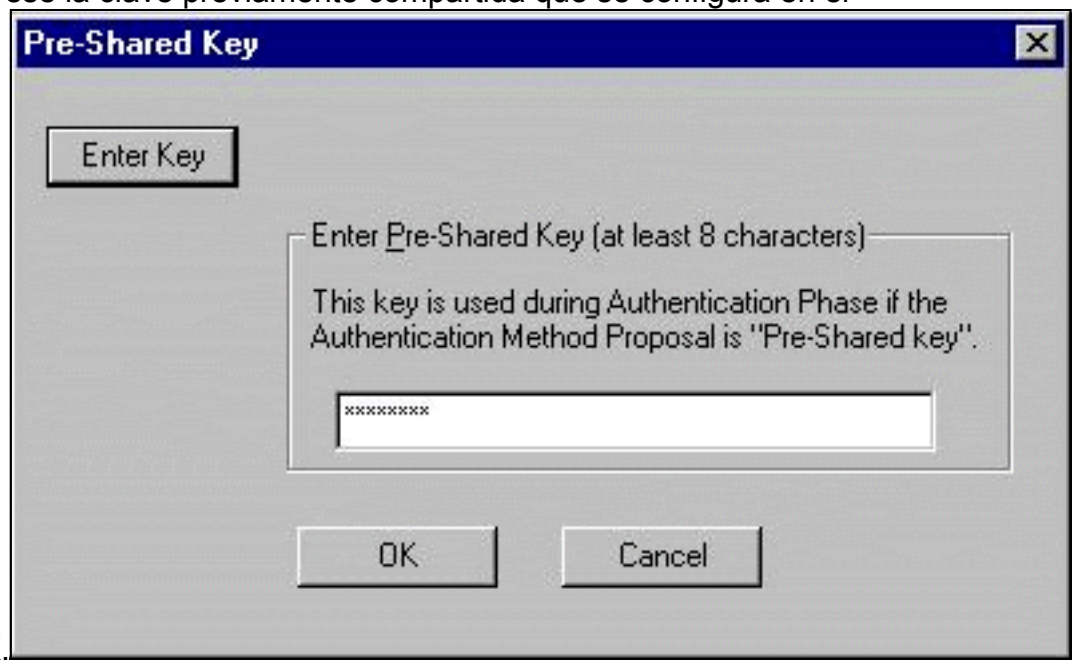
1. En la lengueta de la identidad de parte remota y de la dirección, defina la red privada que usted quiere poder alcanzar con el uso del cliente VPN. Después, selecto **conecte con el túnel de gateway seguro** y defina el IP Address externo del PIX.



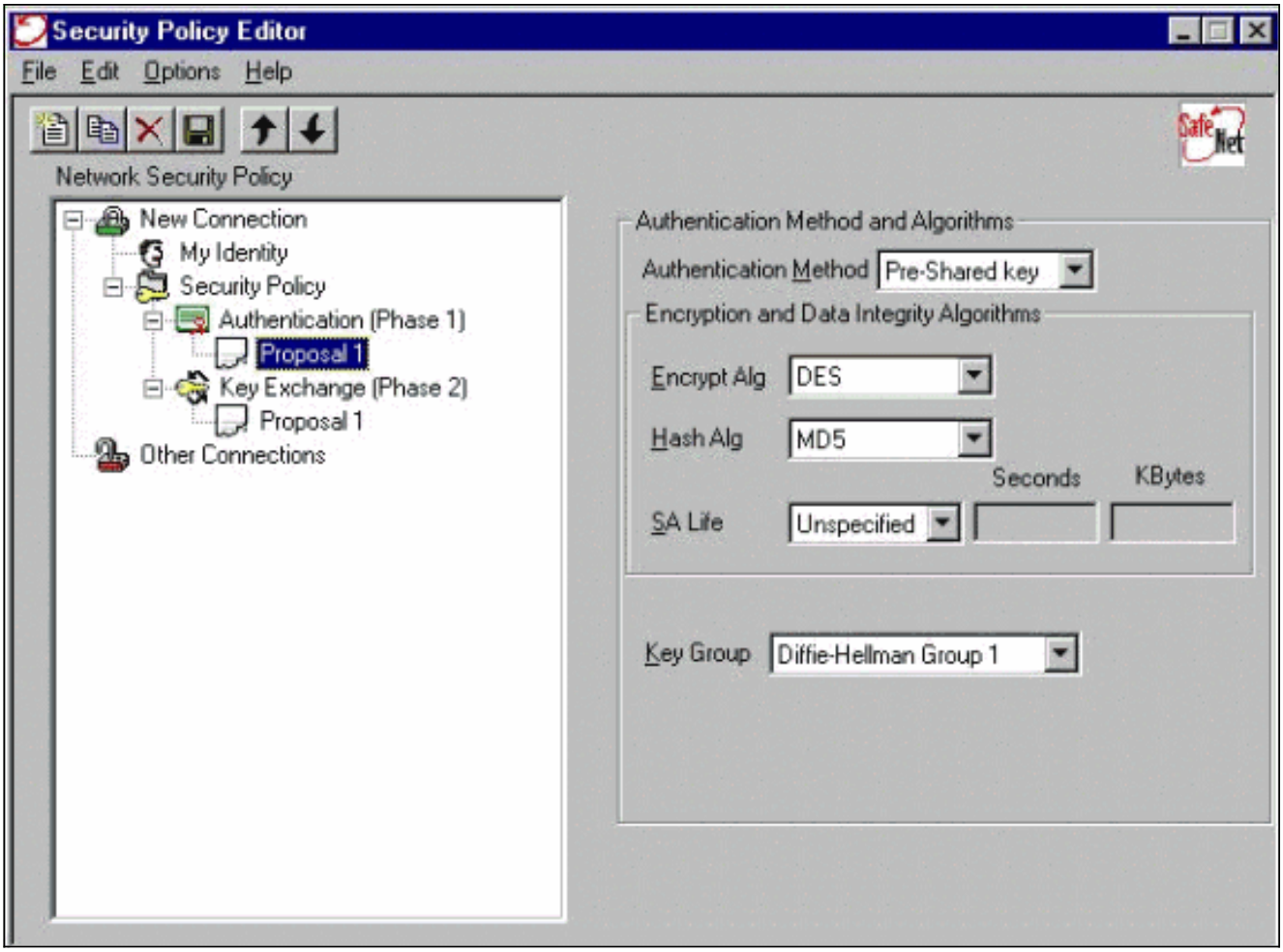
2. Seleccione **mi identidad** y deje la configuración al valor por defecto. Después, haga clic el botón de la **clave previamente compartida**.



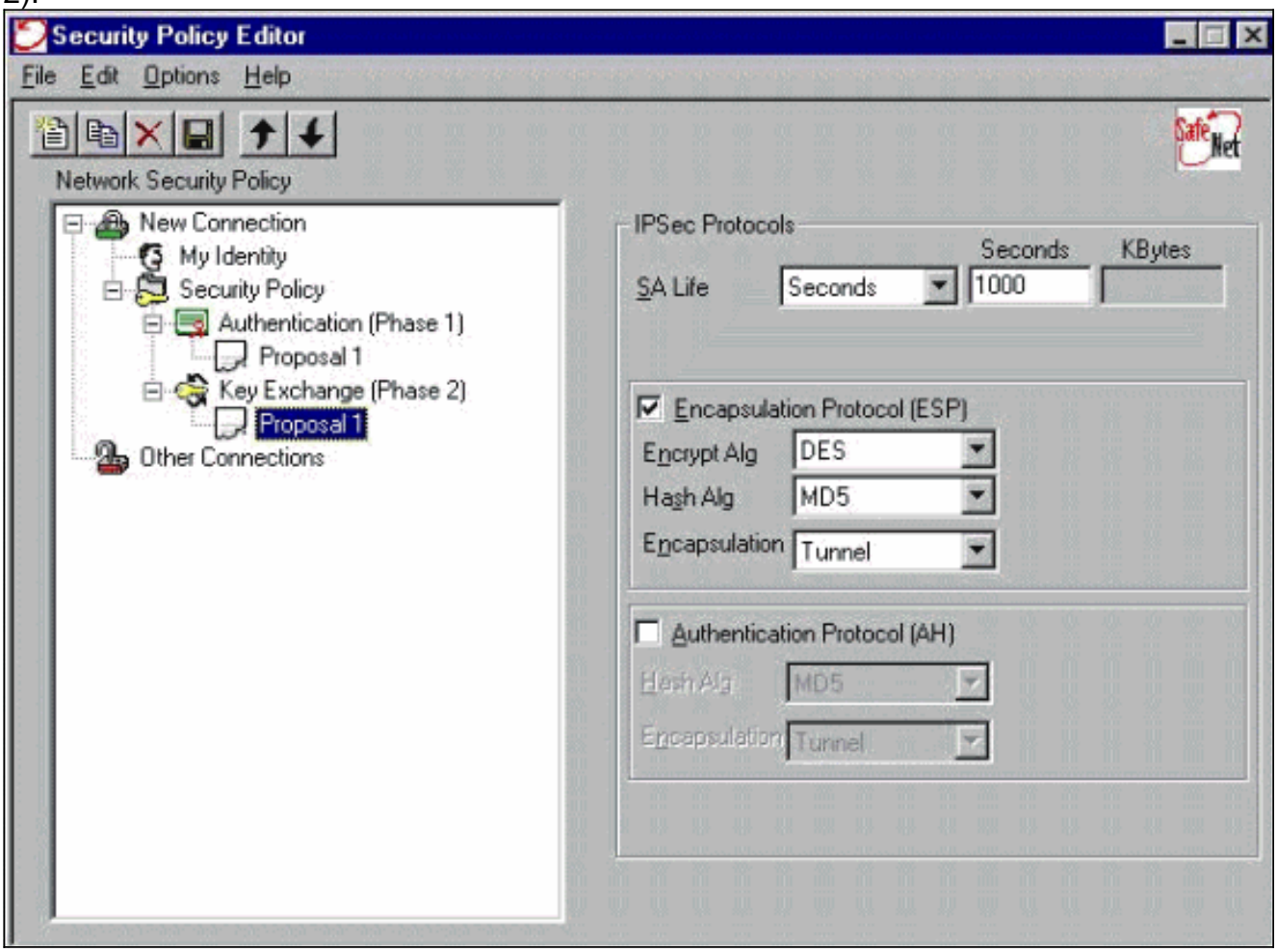
3. Ingrese la clave previamente compartida que se configura en el PIX.



4. Configure la propuesta de Autenticación (directiva de la fase 1).



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



Nota: No olvide salvar la directiva cuando le acaban. Abra una ventana de DOS y haga ping un host sabido en la red interna del PIX para iniciar el túnel del cliente. Usted recibe un mensaje inalcanzable del Protocolo de mensaje de control de Internet (ICMP) del primer ping mientras que intenta negociar el túnel.

Verificación

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

Troubleshooting

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

comandos debug

Nota: Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.

Para ver los client-side debug, habilite visualizador de registro seguro de Cisco:

- **debug crypto ipsec sa** - Visualiza los IPSec Negotiations de la fase 2.
- **debug crypto isakmp sa** - Visualiza negociaciones ISAKMP de la fase 1.
- **motor del debug crypto** - Visualiza a las sesiones encriptadas.

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