PIX configureren voor Cisco beveiligde VPN-client, joch-kaart, voorgedeeld, geen modus-configuratie

Inhoud

Inleiding

Deze configuratie laat zien hoe u een VPN-client kunt aansluiten op een PIX-firewall met behulp van wildcards en de opdrachten **voor** de **systeemverbinding** en **ipsec compatibel met ipsec**. Dit document bevat ook de opdracht **nat 0 toegangslijsten**.

Opmerking: Encryptietechnologie is onderworpen aan exportcontroles. Het is uw verantwoordelijkheid om te weten welke wetgeving betrekking heeft op de export van encryptietechnologie. Als u vragen hebt over exportcontrole, stuurt u een e-mail naar export@cisco.com.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies.

- Cisco Secure PIX-softwarerelease 5.0.3 met Cisco Secure VPN-client 1.0 (weergegeven als 2.0.7 in het menu Help > About) of Cisco Secure PIX-softwarerelease 6.2.1 met Cisco Secure VPN-client 1.1 (weergegeven als 2.1.12 in het menu Help > About).
- Internetmachines hebben toegang tot de webhost binnen met het IP-adres 192.68.0.50.
- De VPN client heeft toegang tot alle machines aan de binnenkant met het gebruik van alle poorten (10.1.1.0/24 en 10.2.2.0/24).

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de mogelijke impact van een opdracht begrijpt voordat u het gebruikt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

In de PIX werken de **toegangslijst** en de **nat 0** opdrachten samen. De opdracht **nat 0access-list** is bedoeld om te worden gebruikt in plaats van de **met ipsec compatibele** opdracht. Als u de **opdracht NAT 0** gebruikt met de opdracht **toegangslijst**, moet u het IP-adres van de client kennen die de VPN-verbinding maakt om de bijbehorende toegangscontrolelijst (ACL) te maken om de NAT te omzeilen.

Opmerking: de met **ipsec compatibel-pl-**opdracht kan beter worden geschaald dan de **nat 0**-opdracht met de opdracht **toegangslijst** om netwerkadresomzetting (NAT) te omzeilen. De reden is omdat u het IP-adres van de klanten die de verbinding maken niet hoeft te kennen. De opdrachten die voor elkaar kunnen worden verwisseld, zijn dikker dan normaal tijdens de configuratie in dit document.

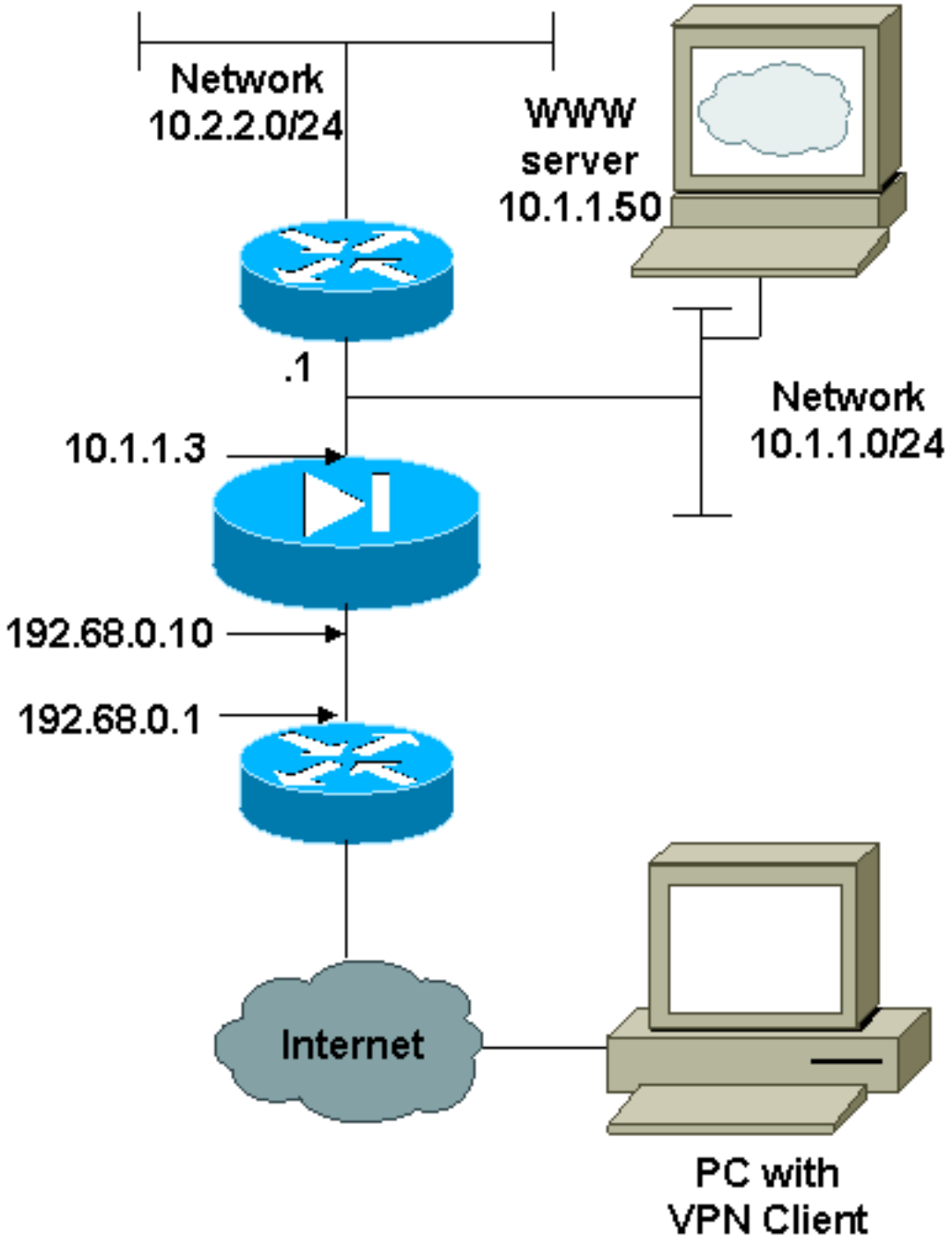
Een gebruiker met een VPN-client sluit een IP-adres aan en ontvangt dit van hun Internet Service provider. De gebruiker heeft toegang tot alles binnen de firewall. Dit omvat netwerken. Ook kunnen gebruikers die de client niet uitvoeren, verbinding maken met de webserver met het gebruik van het adres dat bij de statische toewijzing wordt opgegeven. De gebruikers aan de binnenkant kunnen met internet verbinden. Het is niet nodig dat hun verkeer door de IPSec-tunnel gaat.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven.



Configuraties

Dit document gebruikt de configuraties die hier worden weergegeven.

- PIX
- VPN-client

PIX-configuratie
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-clientconfiguratie

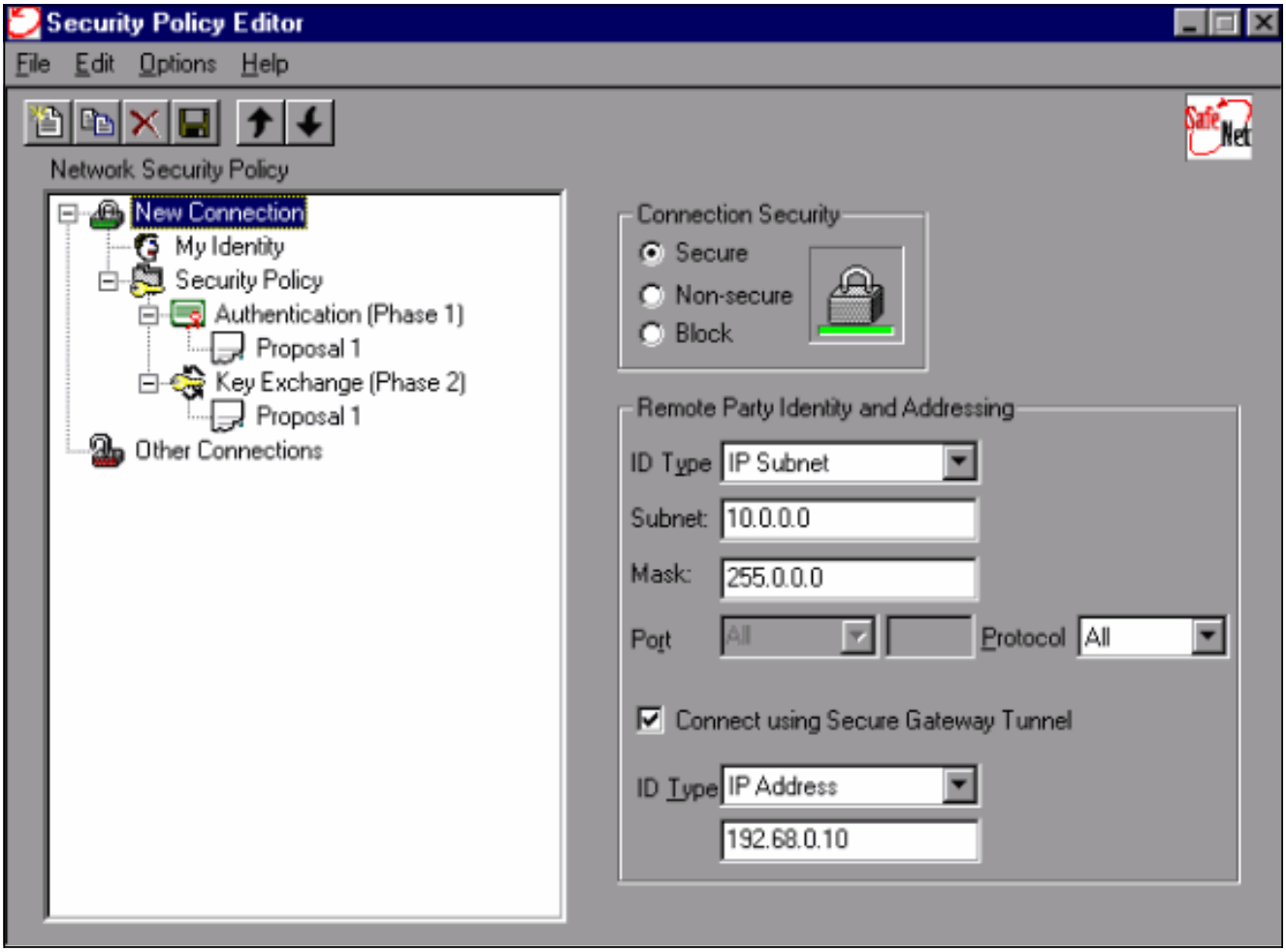
```
Network Security policy:
 1- TACconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP subnet
          10.0.0.0
           255.0.0.0
          Port all Protocol all

     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
```

Het beleid voor de VPN-clientverbinding configureren

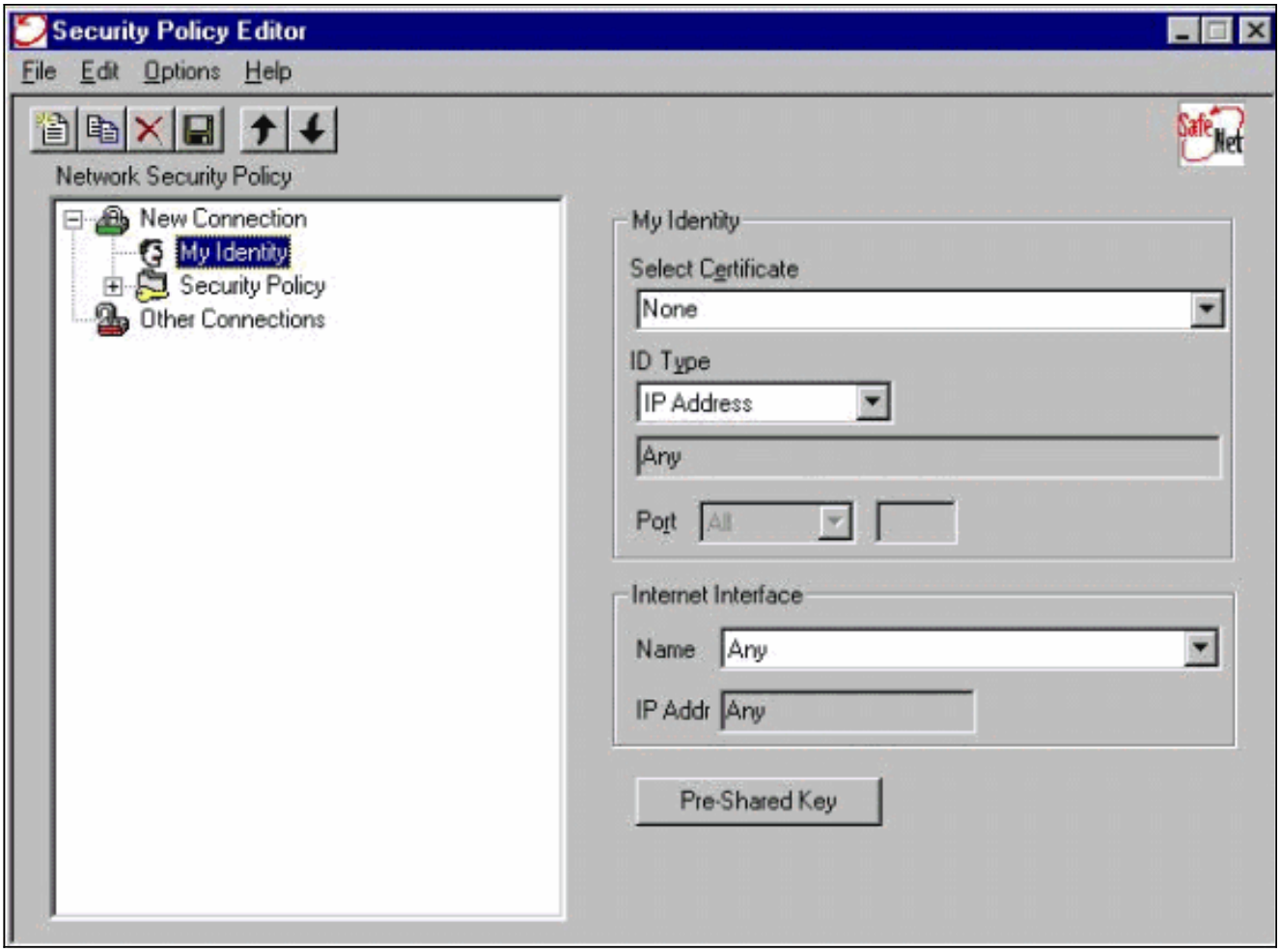
Volg deze stappen om het beleid voor de VPN client-IPSec-verbinding te configureren.

1. Specificeer op het tabblad Identity en Adressatie het privé-netwerk dat u met het gebruik van

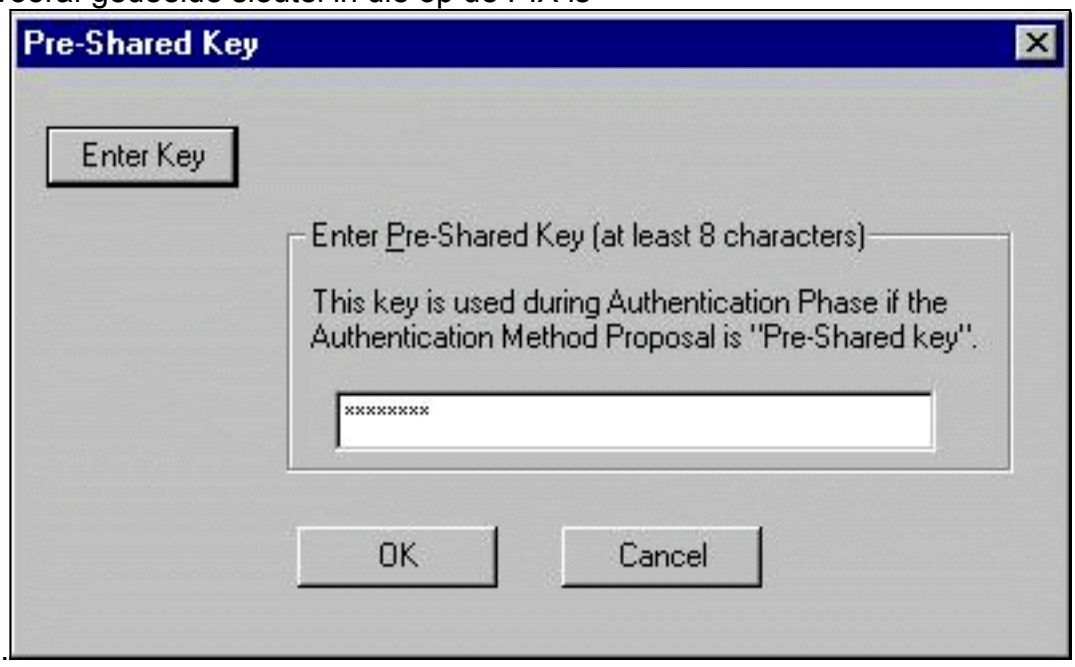
de VPN-client wilt kunnen bereiken. Selecteer vervolgens **Connect met Secure Gateway Tunnel** en definieer het externe IP-adres van de PIX.



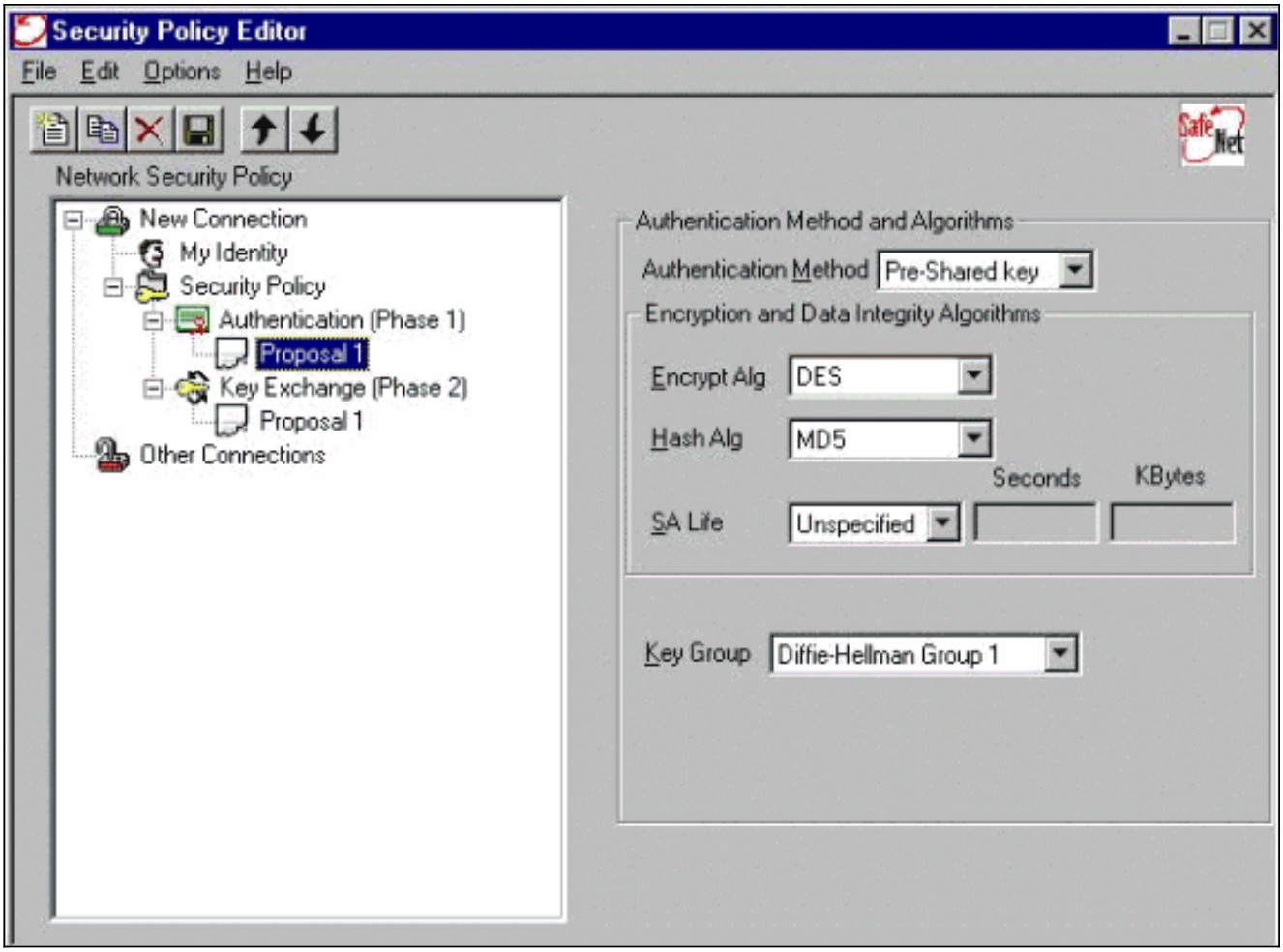
2. Selecteer **Mijn identiteit** en laat de instelling in de standaardinstelling achter. Klik vervolgens op de knop **Vooraf gedeelde sleutel**.



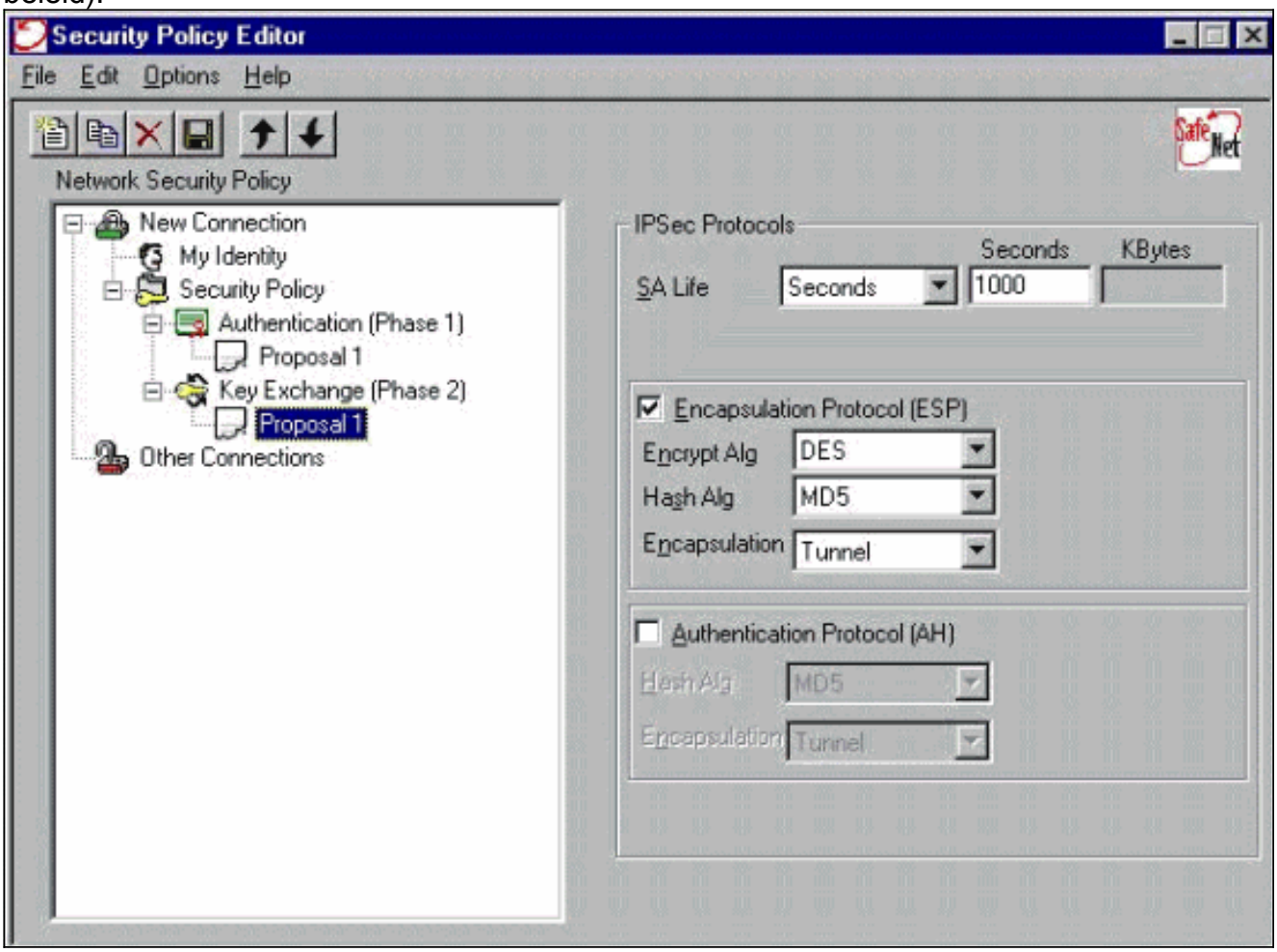
3. Voer de vooraf gedeelde sleutel in die op de PIX is ingesteld.



4. Configureer het verificatievoorstel (fase 1-beleid).



5. Configureer het IPSec-voorstel (fase 2-beleid).



Opmerking: vergeet niet het beleid op te slaan als u klaar bent. Open een DOS-venster en ping van een bekende host in het interne netwerk van de PIX om de tunnel te openen vanaf de client. U ontvangt een onbereikbaar bericht van Internet Control Message Protocol (ICMP) van het eerste pingelt wanneer het probeert de tunnel te onderhandelen.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten debug

Opmerking: Voordat u **debug-**opdrachten afgeeft, raadpleegt u Belangrijke informatie over debug-opdrachten.

Schakel het Cisco Secure Log Viewer in om de uiteinden van de clientzijde te zien:

- **debug crypto ipsec sa** - Hiermee geeft u de IPSec-onderhandelingen van fase 2 weer.
- **debug crypto isakmp sa** - Hiermee geeft u de ISAKMP-onderhandelingen van fase 1 weer.
- **debug-encryptie-motor** - Hiermee worden de versleutelde sessies weergegeven.

Gerelateerde informatie

- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Productondersteuning voor Cisco PIX-firewall
- Verzoeken om opmerkingen (RFC's)
- Productondersteuningspagina's voor IP Security (IPSec)
- IPsec-netwerkbeveiliging configureren
- Het configureren van Internet Key Exchange-beveiligingsprotocol
- Een Inleiding aan IP Security (IPSec) encryptie
- Connectiviteit met de PIX-firewall
- IPsec configureren
- Technische ondersteuning en documentatie – Cisco Systems