Konfigurieren von PIX für Cisco Secure VPN Client Wild Card, Pre-Shared, No Mode-Config

Inhalt

Einführung

Diese Konfiguration veranschaulicht, wie ein VPN-Client mithilfe von Platzhaltern und der **sysopt-Verbindung permit-ipsec** und **sysopt ipsec pl-kompatiblen** Befehlen mit einer PIX-Firewall verbunden wird. In diesem Dokument wird auch der Befehl **nat 0 access-list** behandelt.

Hinweis: Verschlüsselungstechnologie unterliegt Exportkontrollen. Es liegt in Ihrer Verantwortung, das Gesetz über den Export von Verschlüsselungstechnologien zu kennen. Wenn Sie Fragen zur Exportkontrolle haben, senden Sie eine E-Mail an export@cisco.com.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf diesen Software- und Hardwareversionen.

- Cisco Secure PIX Software Version 5.0.3 mit Cisco Secure VPN Client 1.0 (im Menü Hilfe unter "Über" als 2.0.7 dargestellt) oder Cisco Secure PIX Software Version 6.2.1 mit Cisco

Secure VPN Client 1.1 (im Menü Hilfe > Info als 2.1.12 angezeigt).
- Internetgeräte greifen mit der IP-Adresse 192.68.0.50 auf den Web-Host innen zu.
- Der VPN-Client greift auf alle internen Systeme zu, wobei alle Ports verwendet werden (10.1.1.0/24 und 10.2.2.0/24).

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Hintergrundinformationen

Auf dem PIX arbeiten die Befehle **access-list** und **nat 0** zusammen. Der Befehl **nat 0 access-list** soll anstelle des **Befehls sysopt ipsec pl-kompatible** Befehle verwendet werden. Wenn Sie den Befehl **nat 0** mit dem entsprechenden Befehl **access-list** verwenden, müssen Sie die IP-Adresse des Clients, der die VPN-Verbindung herstellt, kennen, um die entsprechende Zugriffskontrollliste (ACL) zur Umgehung der NAT zu erstellen.

Hinweis: Der **sysopt ipsec pl-kompatible** Befehl lässt sich besser skalieren als der **nat 0-**Befehl mit der entsprechenden Befehlsreihenfolge **der Zugriffsliste**, um die Network Address Translation (NAT) zu umgehen. Der Grund hierfür ist, dass Sie die IP-Adresse der Clients, die die Verbindung herstellen, nicht kennen müssen. Die austauschbaren Befehle sind in der Konfiguration in diesem Dokument fett formatiert.

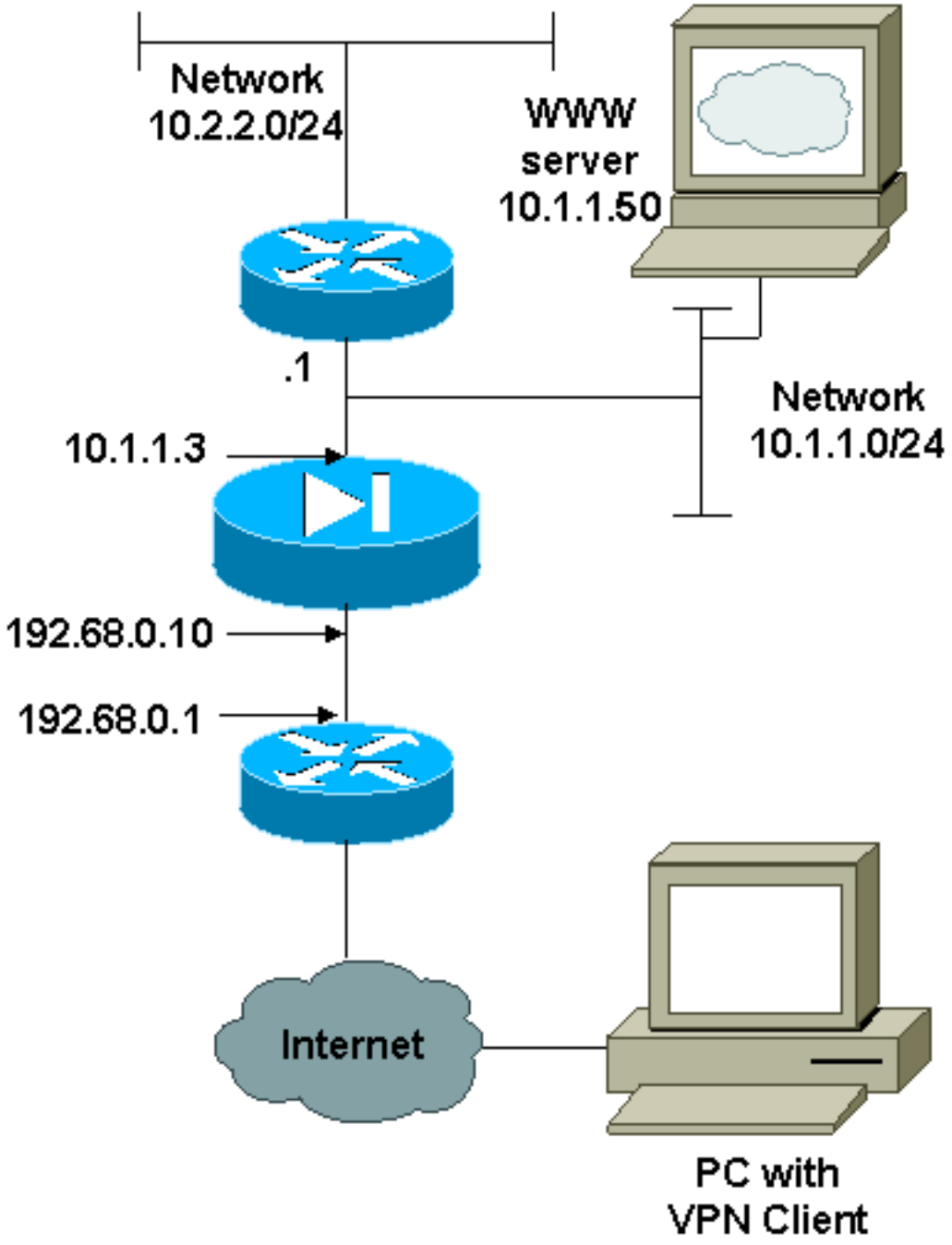
Ein Benutzer mit einem VPN-Client stellt eine Verbindung her und erhält eine IP-Adresse von seinem Internetdienstanbieter (Internet Service Provider, ISP). Der Benutzer hat Zugriff auf alles innerhalb der Firewall. Dazu gehören auch Netzwerke. Außerdem können Benutzer, die den Client nicht ausführen, mithilfe der von der statischen Zuweisung angegebenen Adresse eine Verbindung zum Webserver herstellen. Benutzer im Inneren können eine Verbindung zum Internet herstellen. Der Datenverkehr muss nicht über den IPSec-Tunnel geleitet werden.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden die hier gezeigten Konfigurationen verwendet.

- PIX
- VPN-Client

PIX-Konfiguration

```
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]
```

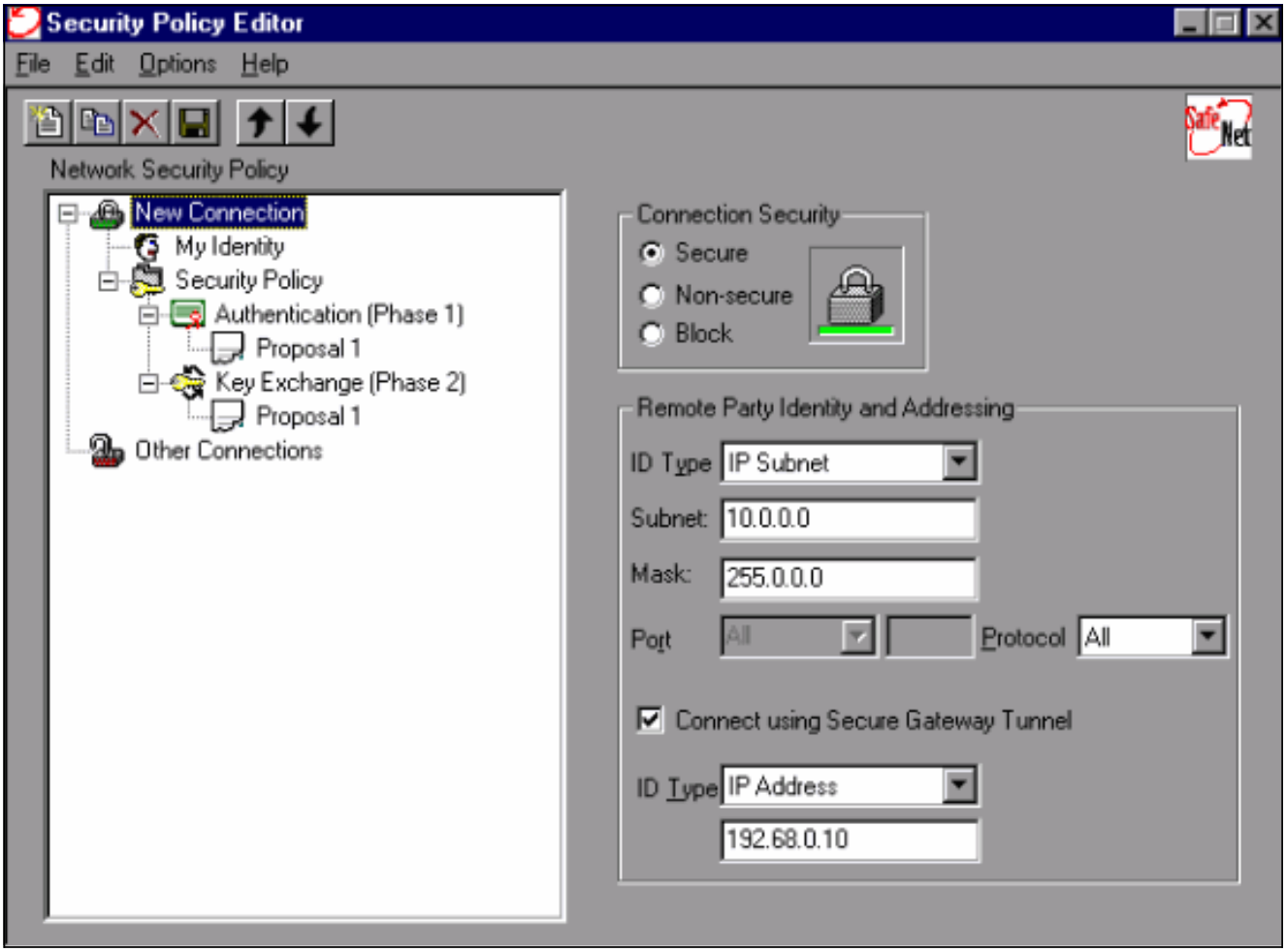
VPN-Client-Konfiguration

```
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
```

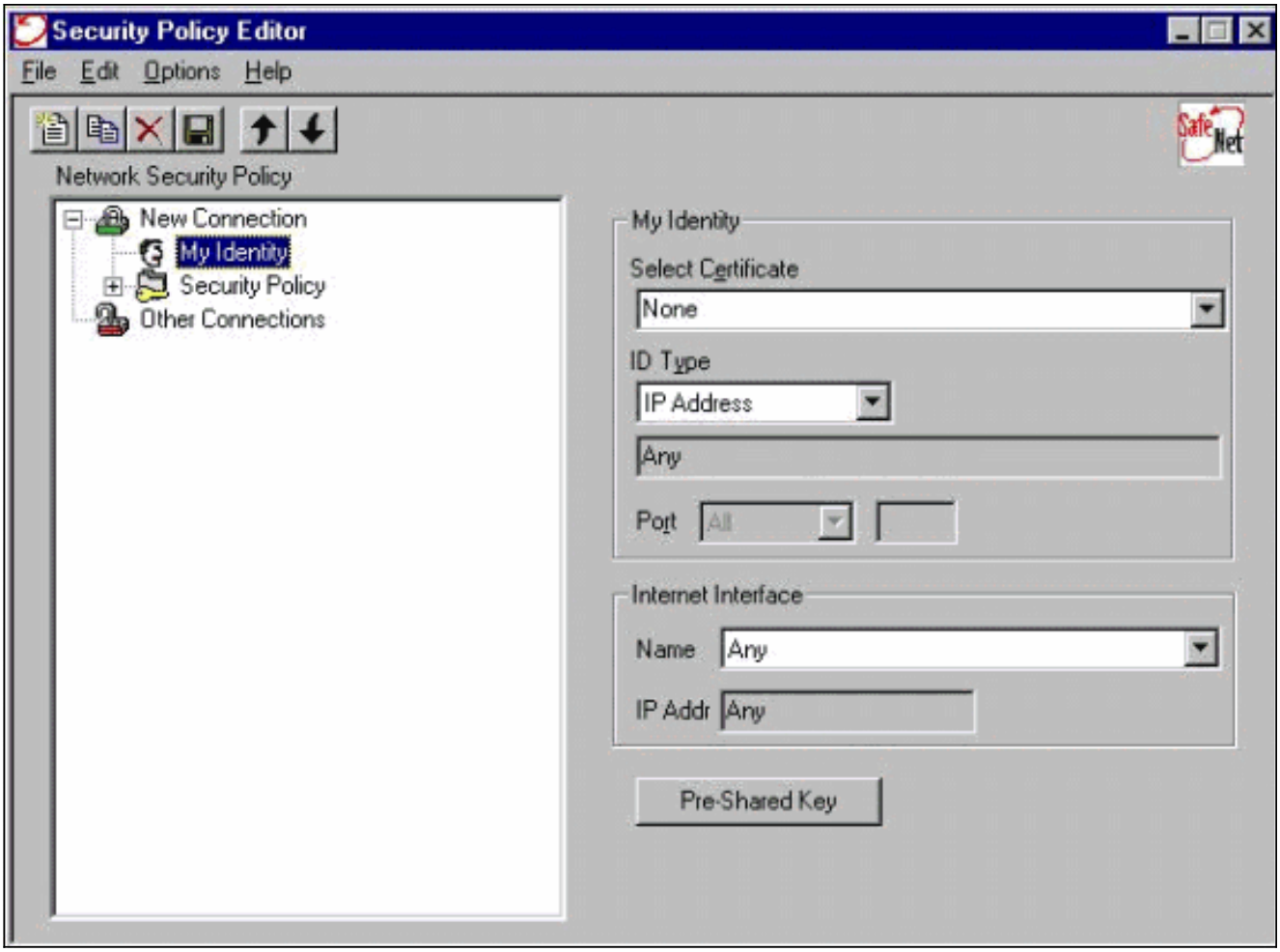
Konfigurieren der Richtlinie für die VPN Client IPSec-Verbindung

Führen Sie diese Schritte aus, um die Richtlinie für die VPN Client IPSec-Verbindung zu konfigurieren.

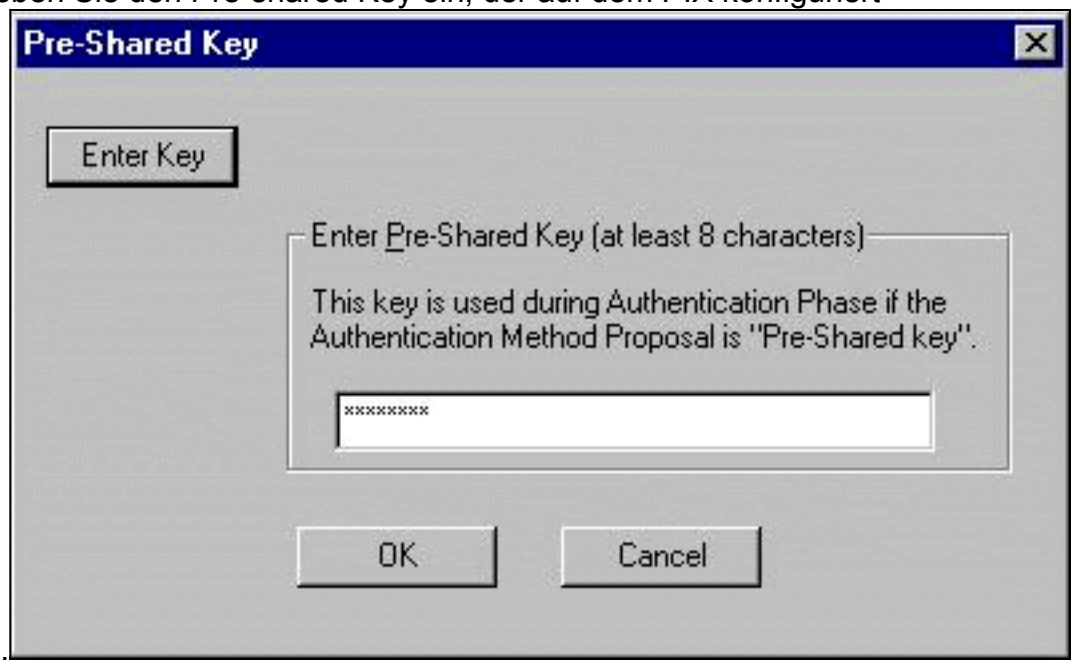
1. Legen Sie auf der Registerkarte "Remote Party Identity and Addressing" (Identität und Adressierung von Remote-Teilnehmern) das private Netzwerk fest, das Sie mithilfe des VPN-Clients erreichen möchten. Wählen Sie als Nächstes **Connect Using Secure Gateway Tunnel (Verbinden mit sicherem Gateway-Tunnel)** aus, und legen Sie die externe IP-Adresse des PIX
fest.



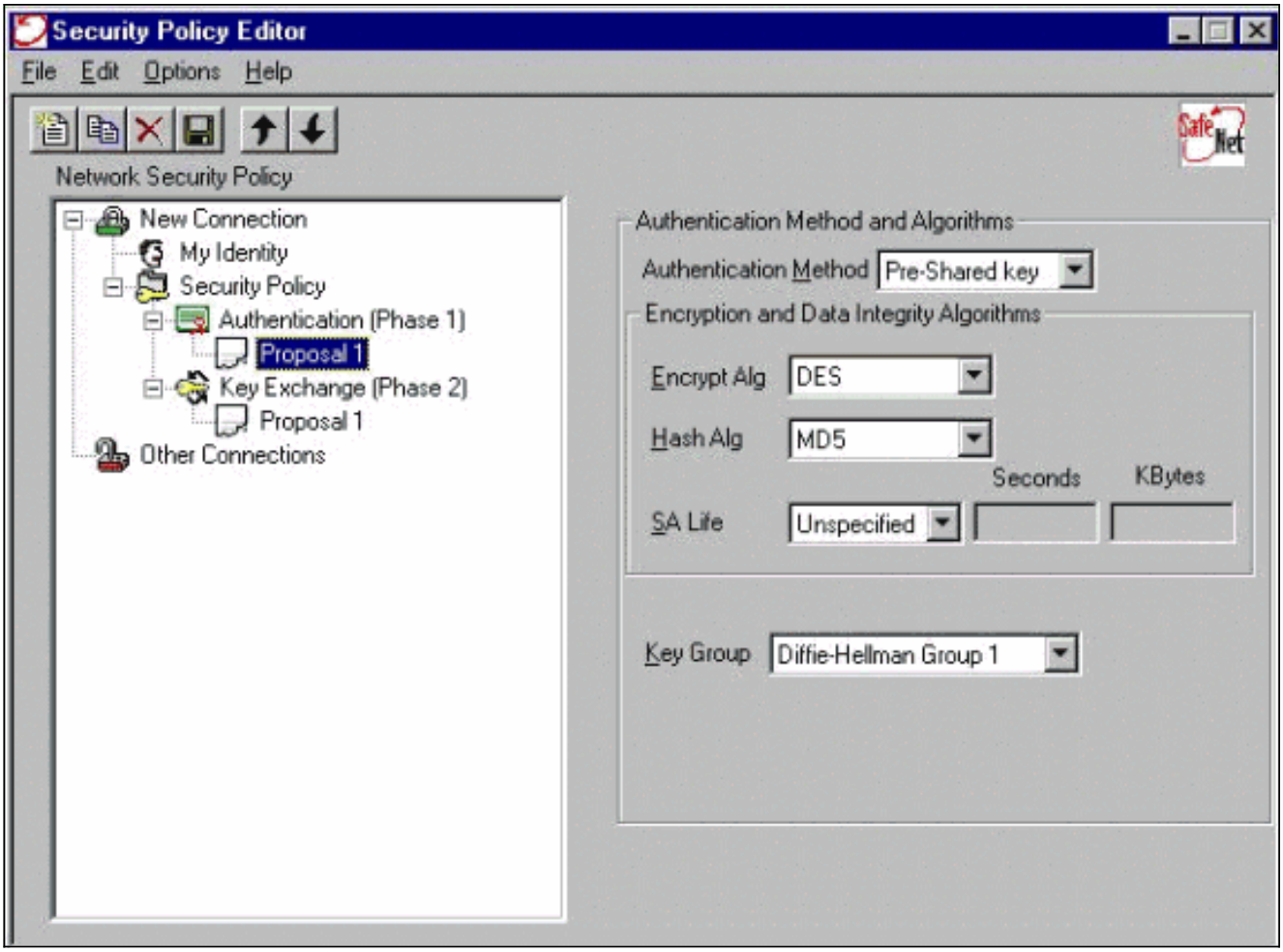
2. Wählen Sie **Meine Identität**, und belassen Sie die Standardeinstellung. Klicken Sie anschließend auf die Schaltfläche **Vorinstallierter Schlüssel**.



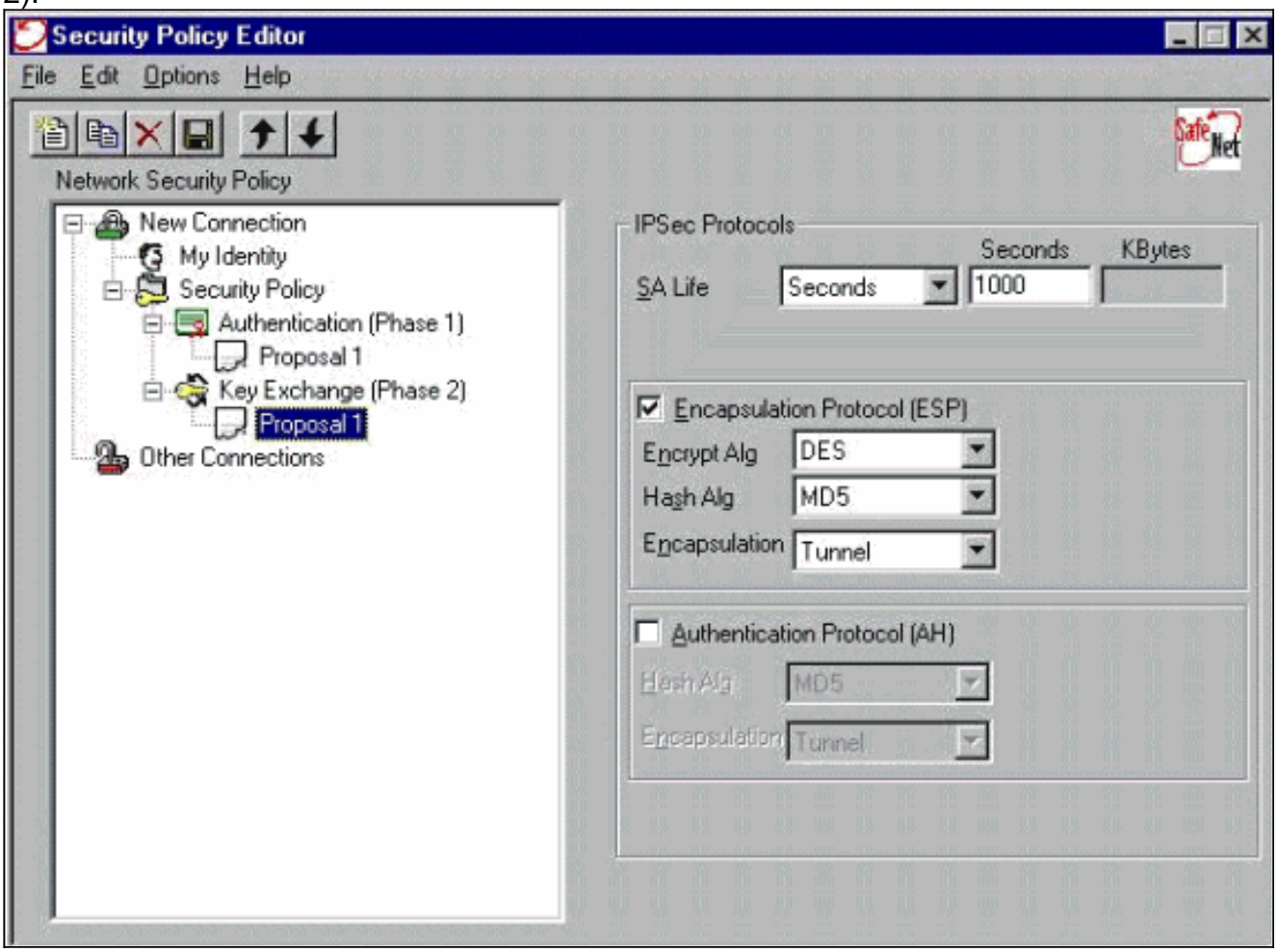
3. Geben Sie den Pre-shared Key ein, der auf dem PIX konfiguriert ist.



4. Konfigurieren Sie den Authentifizierungsvorschlag (Richtlinie für Phase 1).



5. Konfigurieren Sie den IPSec-Vorschlag (Richtlinie für Phase 2).



Hinweis: Vergessen Sie nicht, die Richtlinie zu speichern, wenn Sie fertig sind. Öffnen Sie ein DOS-Fenster, und pingen Sie einen bekannten Host im internen Netzwerk des PIX, um den Tunnel vom Client aus zu initiieren. Beim Versuch, den Tunnel zu verhandeln, erhalten Sie vom ersten Ping eine nicht erreichbare Meldung über das Internet Control Message Protocol (ICMP).

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Debug-Befehle

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie die Informationen Wichtige Informationen über Debug-Befehle.

Um die clientseitigen Debuggen anzuzeigen, aktivieren Sie den Cisco Secure Log Viewer:

- **debug crypto ipsec sa** - Zeigt die IPSec-Verhandlungen für Phase 2 an.
- **debug crypto isakmp sa** - Zeigt die ISAKMP-Verhandlungen für Phase 1 an.
- **debug crypto engine** - Zeigt die verschlüsselten Sitzungen an.

Zugehörige Informationen

- Cisco Secure PIX Firewall - Befehlsreferenzen
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Produkt-Support für die Cisco PIX Firewall
- Anforderungen für Kommentare (RFCs)
- Support-Seiten für IP Security-Produkte (IPSec)
- Konfigurieren der IPSec-Netzwerksicherheit
- Konfigurieren des Internet Key Exchange Security Protocol
- Eine Einführung in die IP Security (IPSec)-Verschlüsselung
- Konnektivität über die PIX-Firewall
- Konfigurieren von IPSec
- Technischer Support und Dokumentation - Cisco Systems