Configurazione di PIX su Cisco Secure VPN Client Wild-card, pre-condiviso, senza configurazione di modalità

Sommario

Introduzione

In questa configurazione viene illustrato come connettere un client VPN a un firewall PIX con l'utilizzo di caratteri jolly e dei comandi **allow-ipsec** e **sysopt ipsec compatibili con pl**. Nel documento viene descritto anche il comando **access-list nat 0**.

Nota: la tecnologia di crittografia è soggetta ai controlli sulle esportazioni. È tua responsabilità conoscere la legge relativa all'esportazione della tecnologia di crittografia. In caso di domande relative al controllo delle esportazioni, invia un'e-mail a export@cisco.com.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware.

- Cisco Secure PIX Software release 5.0.3 con Cisco Secure VPN Client 1.0 (mostrato come 2.0.7 nel menu? > Informazioni su) o Cisco Secure PIX Software release 6.2.1 con Cisco Secure VPN Client 1.1 (mostrato come 2.1.12 nel menu? > Informazioni su).
- I computer Internet accedono all'host Web all'interno con l'indirizzo IP 192.68.0.50.
- Il client VPN accede a tutti i computer all'interno utilizzando tutte le porte (10.1.1.0 /24 e 10.2.2.0 /24).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Sul PIX, i comandi **access-list** e **nat 0** funzionano insieme. il comando **nat 0 access-list** è stato ideato per essere usato al posto del comando **syspot ipsec compatibile con pl**. Se si usa il comando **nat 0** con il corrispondente comando **access-list**, è necessario conoscere l'indirizzo IP del client che crea la connessione VPN per creare l'elenco di controllo di accesso (ACL) corrispondente e ignorare il NAT.

Nota: il comando **sysopt ipsec pl-compatible** offre una scalabilità migliore rispetto al comando **nat 0** con il comando **access-list** corrispondente ir per ignorare Network Address Translation (NAT). Il motivo è che non è necessario conoscere l'indirizzo IP dei client che effettuano la connessione. I comandi intercambiabili sono visualizzati in grassetto nella configurazione riportata in questo documento.

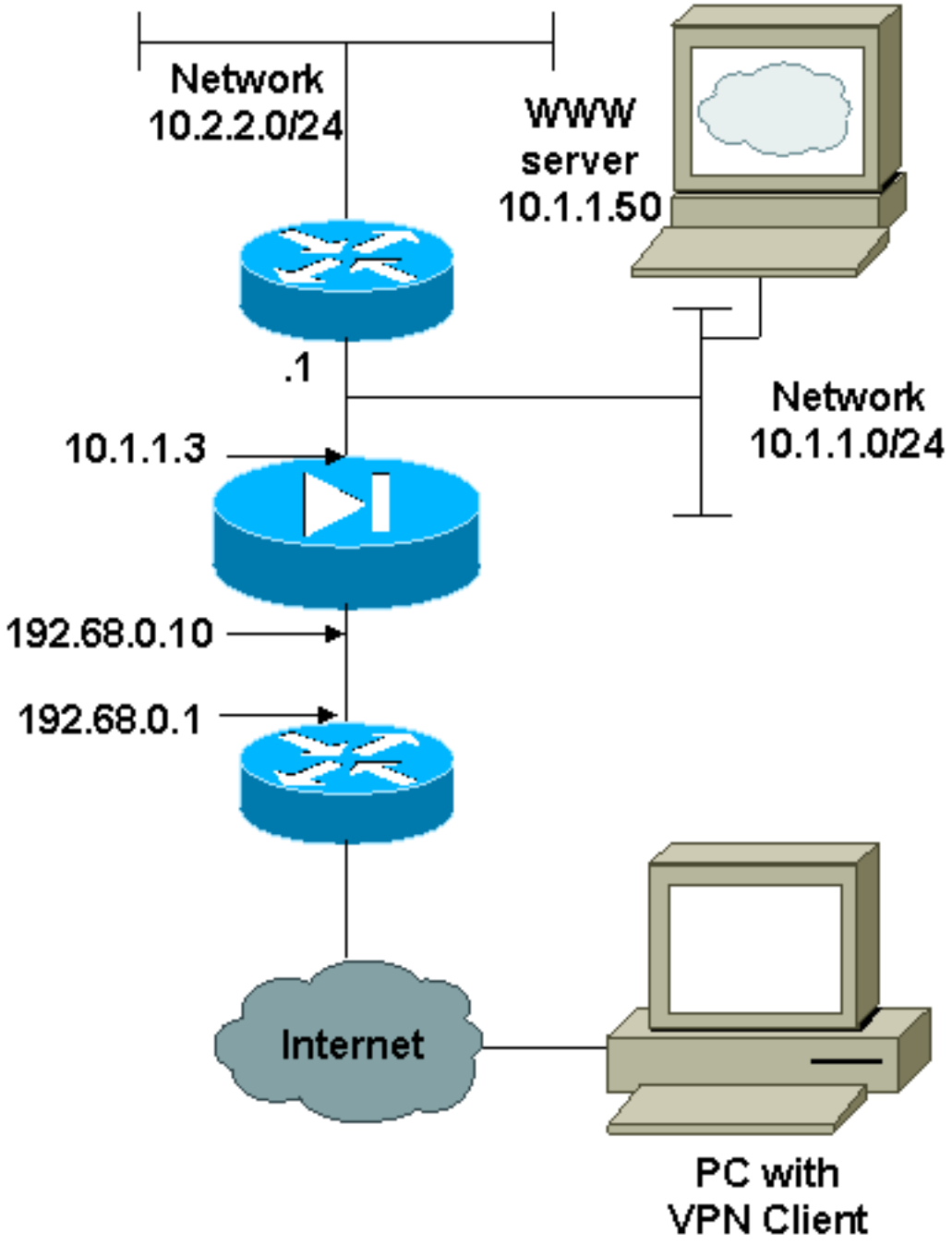
Un utente con un client VPN si connette e riceve un indirizzo IP dal proprio provider di servizi Internet (ISP). L'utente ha accesso a tutto ciò che si trova all'interno del firewall. incluse le reti. Gli utenti che non eseguono il client possono inoltre connettersi al server Web utilizzando l'indirizzo fornito dall'assegnazione statica. Gli utenti all'interno possono connettersi a Internet. non è necessario che il traffico passi attraverso il tunnel IPSec.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Esempio di rete

Nel documento viene usata l'impostazione di rete mostrata nel diagramma.



Configurazioni

Nel documento vengono usate le configurazioni mostrate di seguito.

- PIX
- Client VPN

Configurazione 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]
```

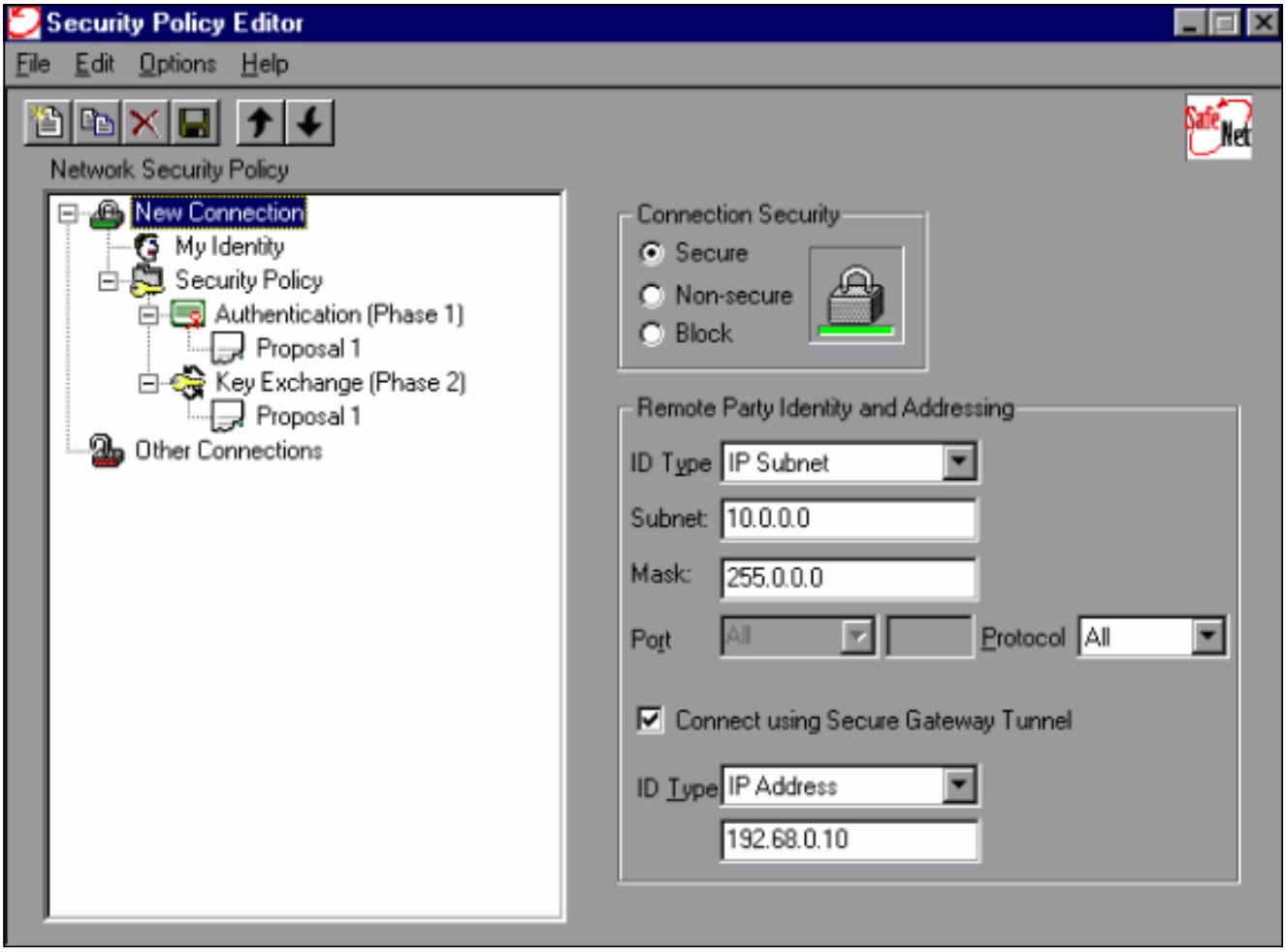
Configurazione client VPN

```
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
```

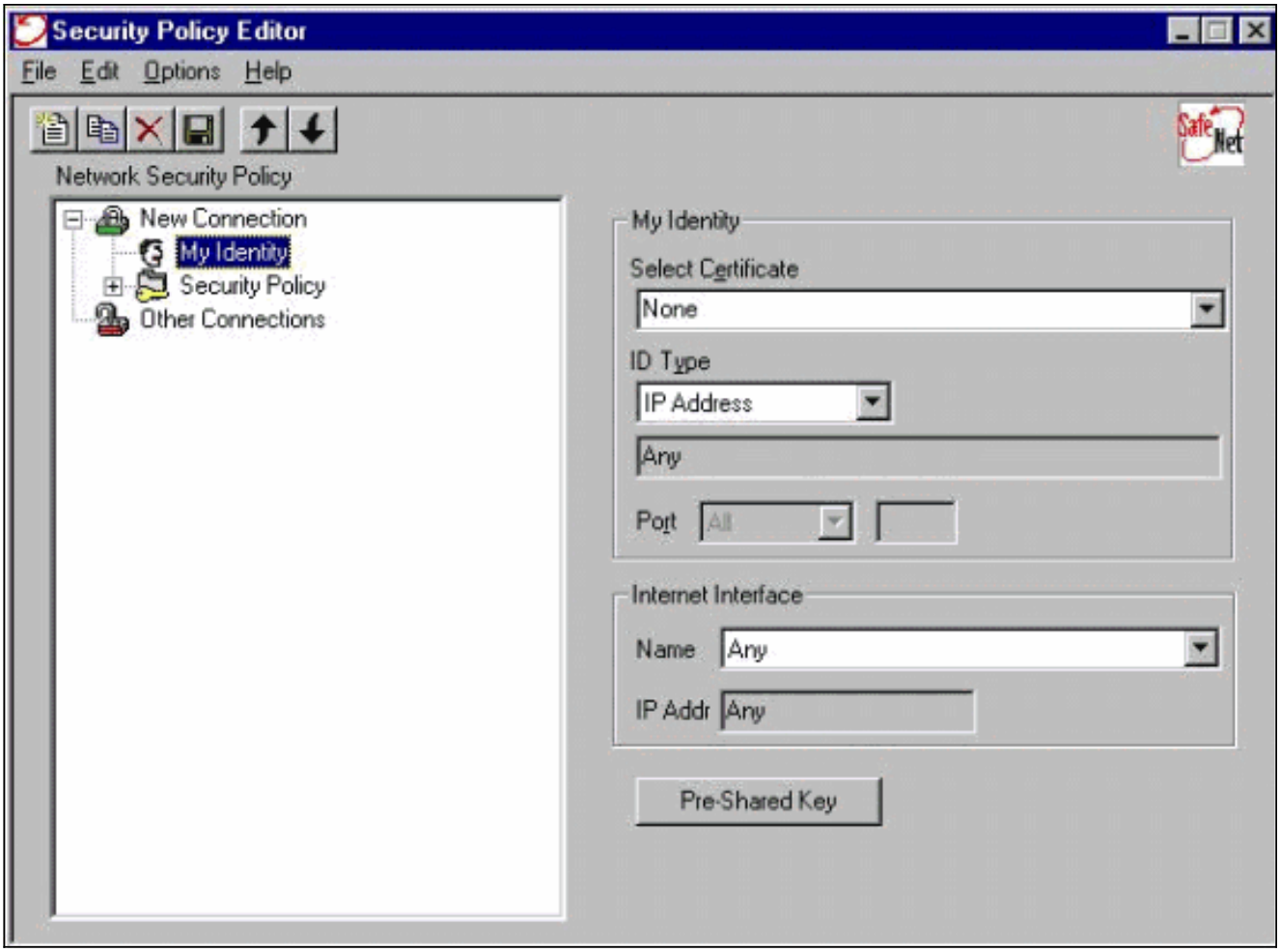
Configurare il criterio per la connessione IPSec del client VPN

Per configurare il criterio per la connessione IPSec del client VPN, eseguire la procedura seguente.

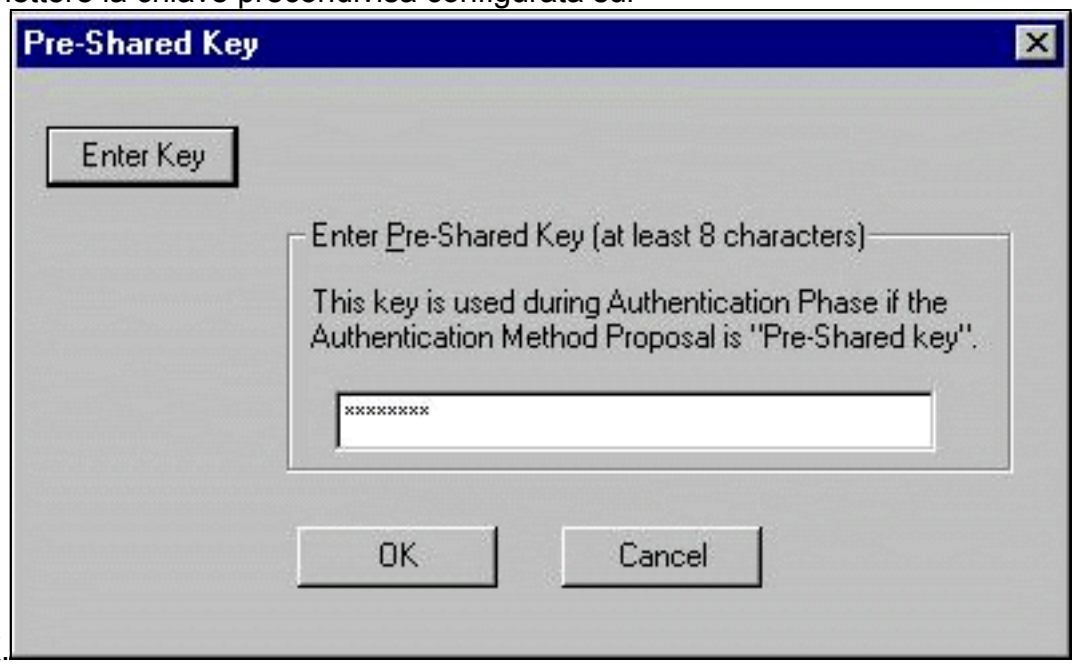
1. Nella scheda Identità e indirizzamento parte remota definire la rete privata che si desidera sia in grado di raggiungere con l'utilizzo del client VPN. Quindi, selezionare **Connect using Secure Gateway Tunnel** (Connetti tramite tunnel gateway sicuro) e definire l'indirizzo IP esterno del
PIX.



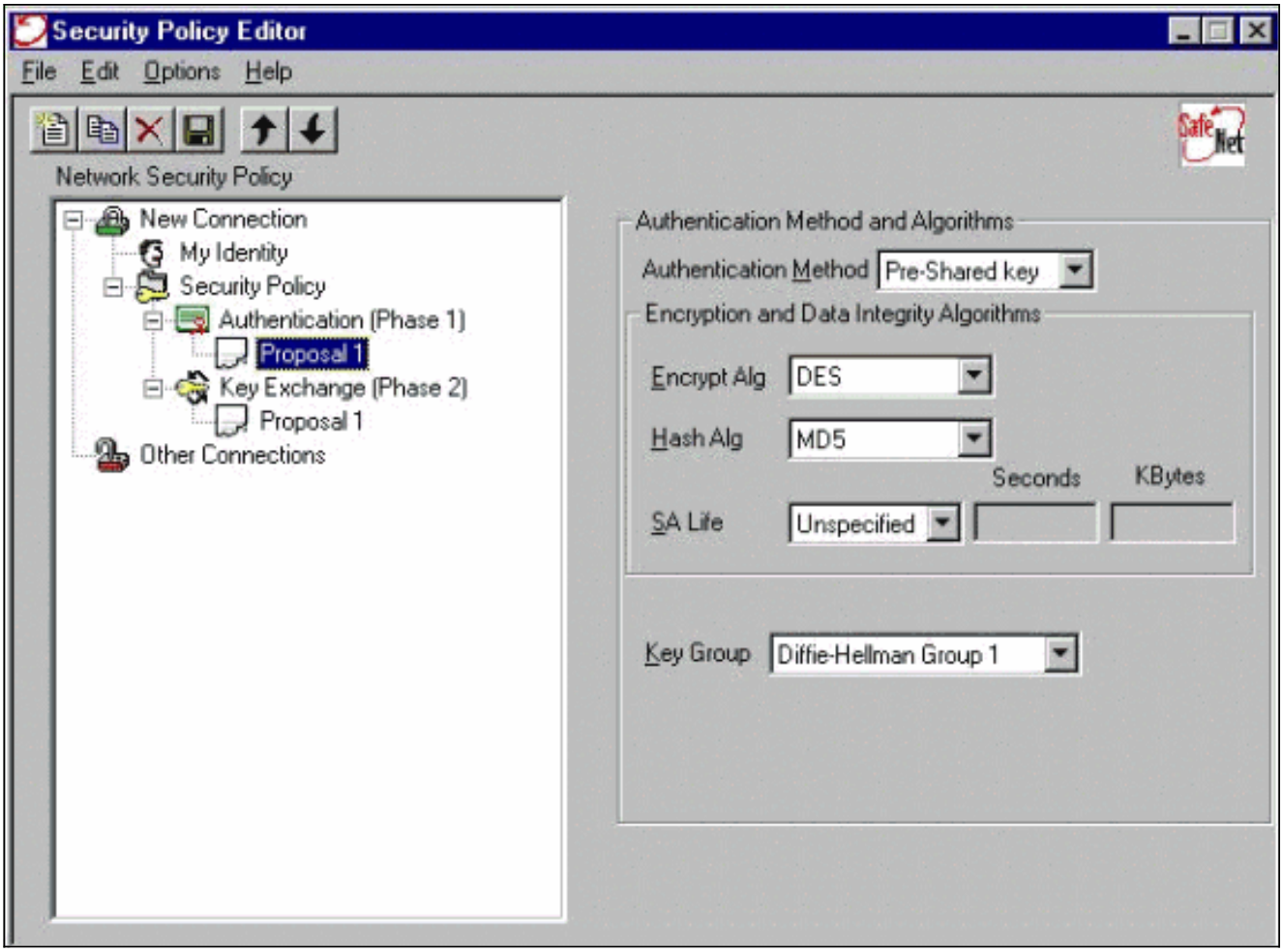
2. Selezionare **Identità personale** e lasciare l'impostazione predefinita. Fare quindi clic sul pulsante **Chiave già condivisa**.



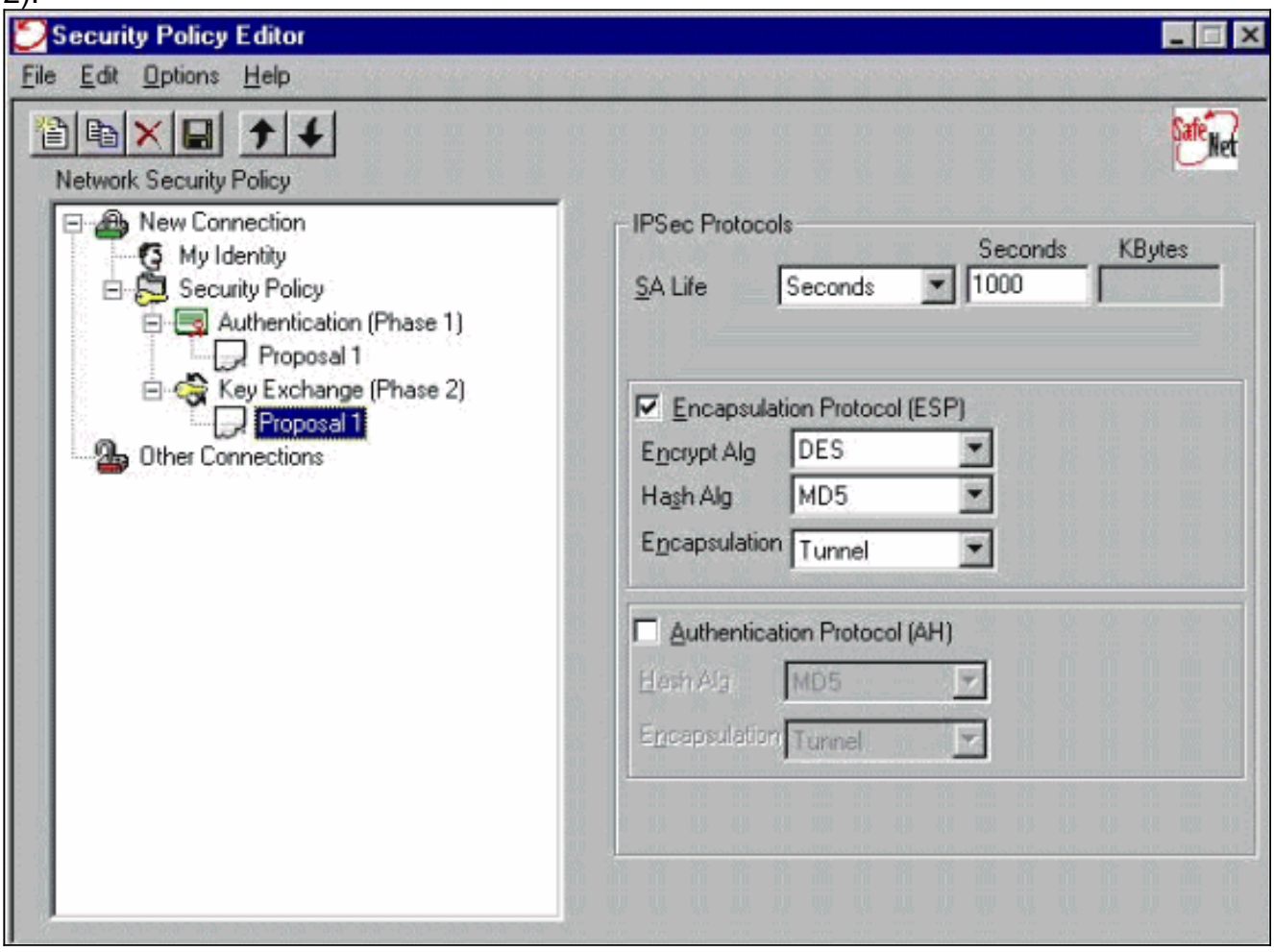
3. Immettere la chiave precondivisa configurata sul PIX.



4. Configurare la proposta di autenticazione (criterio Fase 1).



5. Configurare la proposta IPSec (criterio Fase 2).



Nota: non dimenticare di salvare il criterio al termine dell'operazione. Aprire una finestra DOS ed eseguire il ping di un host noto sulla rete interna del PIX per avviare il tunnel dal client. Durante il tentativo di negoziazione del tunnel, il primo ping restituisce un messaggio ICMP (Internet Control Message Protocol) non raggiungibile.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi debug

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

Per visualizzare i debug sul lato client, abilitare Cisco Secure Log Viewer:

- **debug crypto ipsec sa**: visualizza le negoziazioni IPSec della fase 2.
- **debug crypto isakmp sa**: visualizza le negoziazioni ISAKMP della fase 1.
- **debug crypto engine**: visualizza le sessioni crittografate.

Informazioni correlate

- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- Supporto dei prodotti software Cisco PIX Firewall
- RFC (Requests for Comments)
- Pagine di supporto dei prodotti IP Security (IPSec)
- Configurazione di IPSec Network Security
- Configurazione del protocollo di protezione di Internet Key Exchange
- Introduzione alla crittografia IP Security (IPSec)
- Connettività tramite il firewall PIX
- Configurazione di IPSec
- Documentazione e supporto tecnico – Cisco Systems