配置PIX到Cisco安全VPN客戶端萬用字元，預共用，無模式配置

目錄

簡介

此配置演示如何使用萬用字元和**sysopt connection permit-ipsec**和**sysopt ipsec pl-compatible**命令將VPN客戶端連線到PIX防火牆。本文檔還介紹了**nat 0 access-list**命令。

註：加密技術受出口管制約束。您有責任瞭解與加密技術出口相關的法律。如果您有任何有關出口管制的問題，請傳送電子郵件至export@cisco.com。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件中的資訊是以下列軟體和硬體版本為依據.

- Cisco Secure PIX軟體版本5.0.3與Cisco Secure VPN Client 1.0（在「幫助」>「關於」選單中顯示2.0.7）或與Cisco Secure VPN Client 1.1一起使用的Cisco Secure PIX軟體版本6.2.1（在「幫助」>「關於」選單中顯示2.1.12）。

- Internet電腦訪問IP地址為192.68.0.50的內部網路主機。
- VPN客戶端使用所有埠（10.1.1.0 /24和10.2.2.0 /24）訪問內部的所有電腦。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果在實際網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

在PIX上，**access-list**和**nat 0**命令協同工作。**nat 0 access-list**命令旨在替代與**sysopt ipsec pl-compatible**命令。如果將**nat 0**命令與匹配的**access-list**命令一起使用，您必須知道建立VPN連線的客戶端的IP地址，以便建立匹配的訪問控制清單(ACL)以繞過NAT。

注意：sysopt ipsec pl-compatible 命令比**nat 0命令使用匹配的access-list命令擴展得更好，以便繞過網路地址轉換(NAT)。** 這是因為您不需要知道建立連線的客戶端的IP地址。可互換命令在本文檔的配置中以粗體顯示。

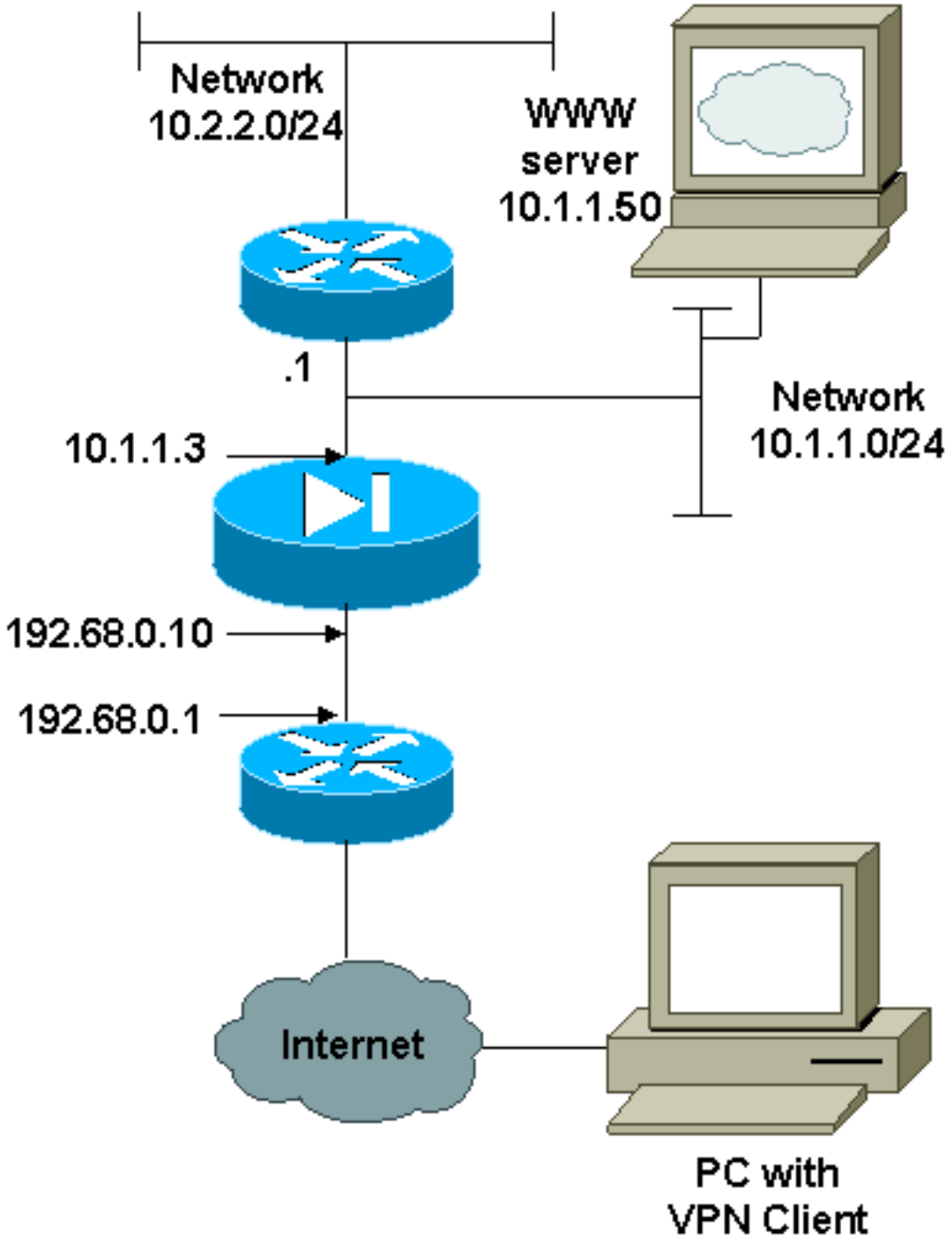
使用VPN客戶端的使用者連線並接收來自其網際網路服務提供商(ISP)的IP地址。 使用者可以訪問防火牆內部的所有內容。這包括網路。此外，不運行客戶端的使用者可以使用靜態分配提供的地址連線到Web伺服器。內部使用者可以連線到Internet。他們的流量無需通過IPSec隧道。

設定

本節提供用於設定本文件中所述功能的資訊。

網路圖表

本檔案會使用下圖中所示的網路設定。



組態

本文檔使用此處顯示的配置。

- PIX
- VPN使用者端

PIX配置

```
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客戶端配置

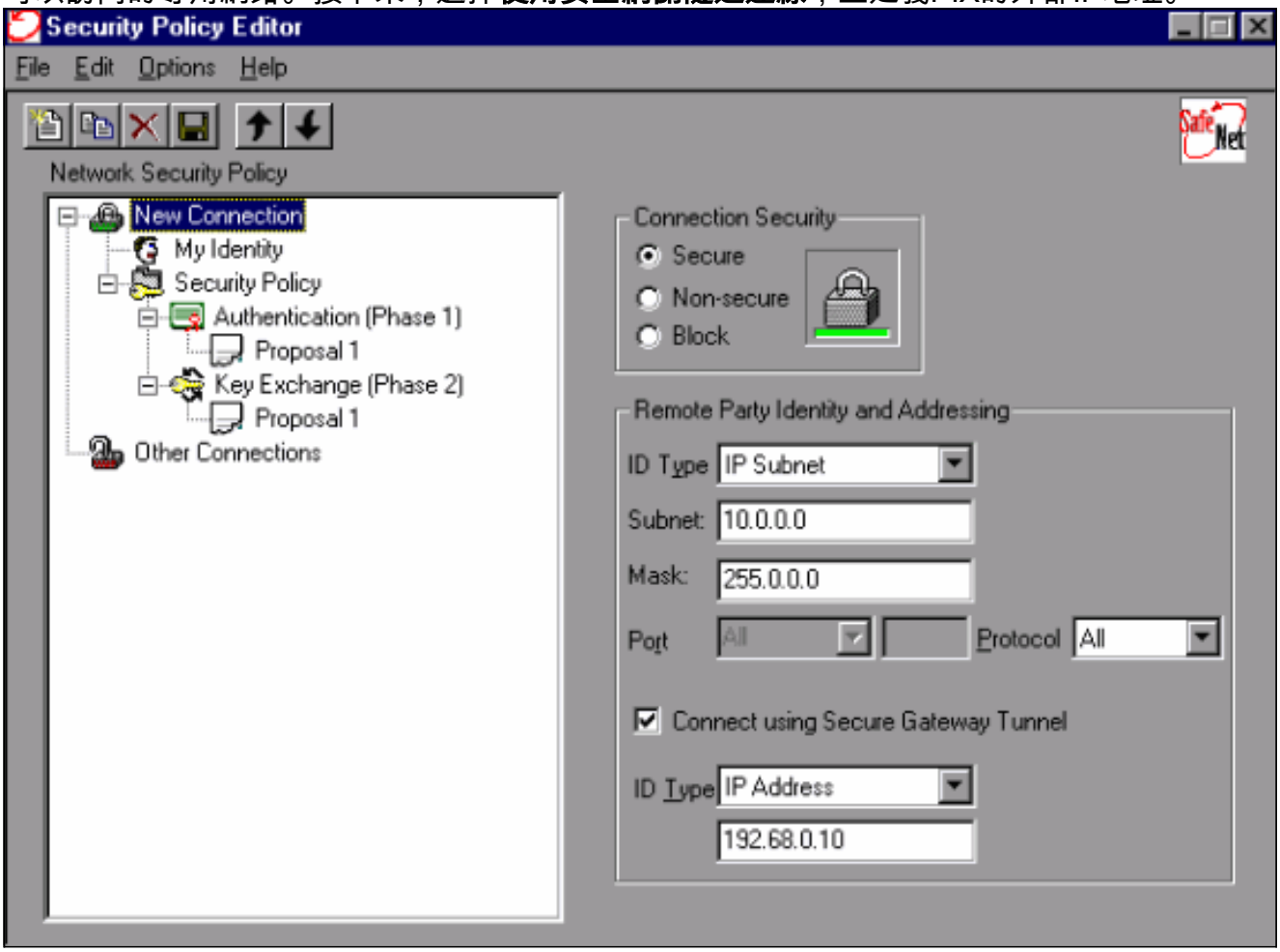
```
Network Security policy:
 1- TACconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP subnet
          10.0.0.0
           255.0.0.0
          Port all Protocol all

     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
```

配置VPN客戶端IPSec連線的策略

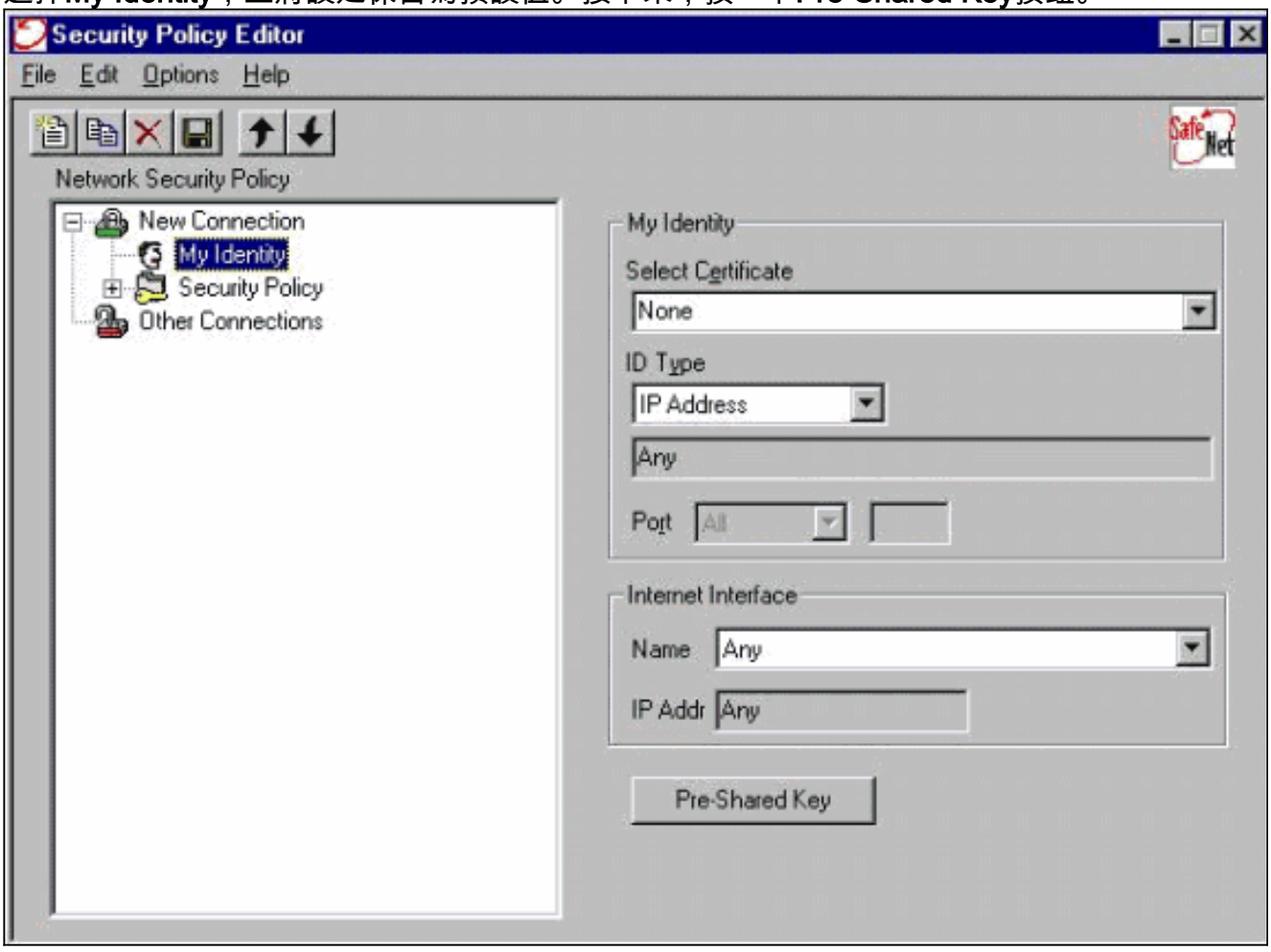
按照以下步驟配置VPN客戶端IPSec連線的策略。

1. 在Remote Party Identity and Addressing（遠端方身份和定址）頁籤上，定義使用VPN客戶端

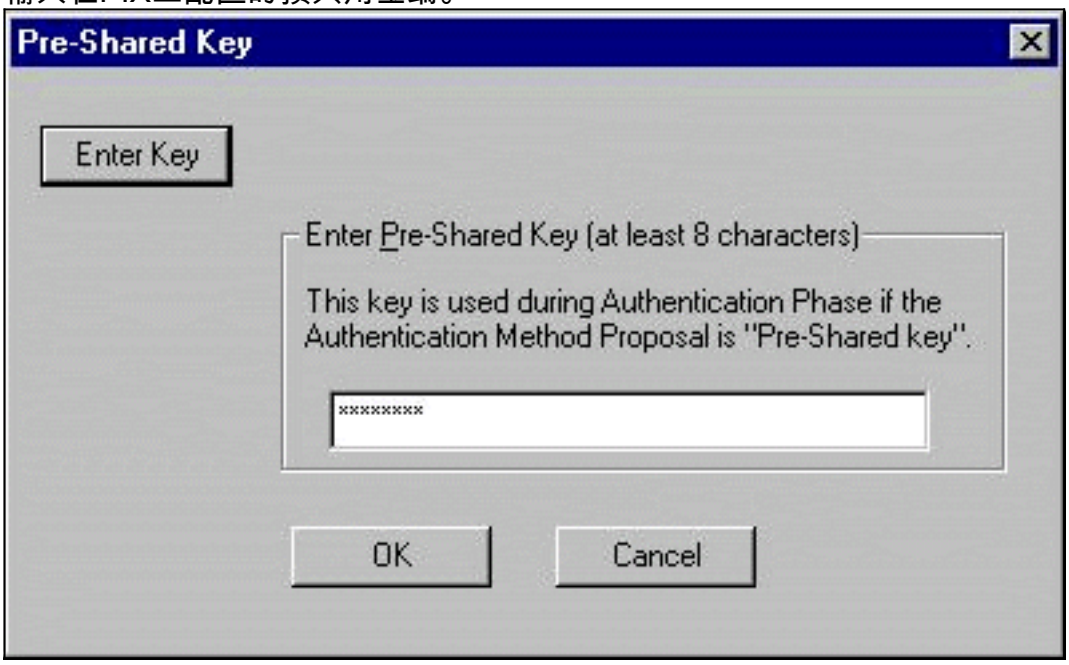
可以訪問的專用網路。接下來，選擇**使用安全網關隧道連線**，並定義PIX的外部IP地址。



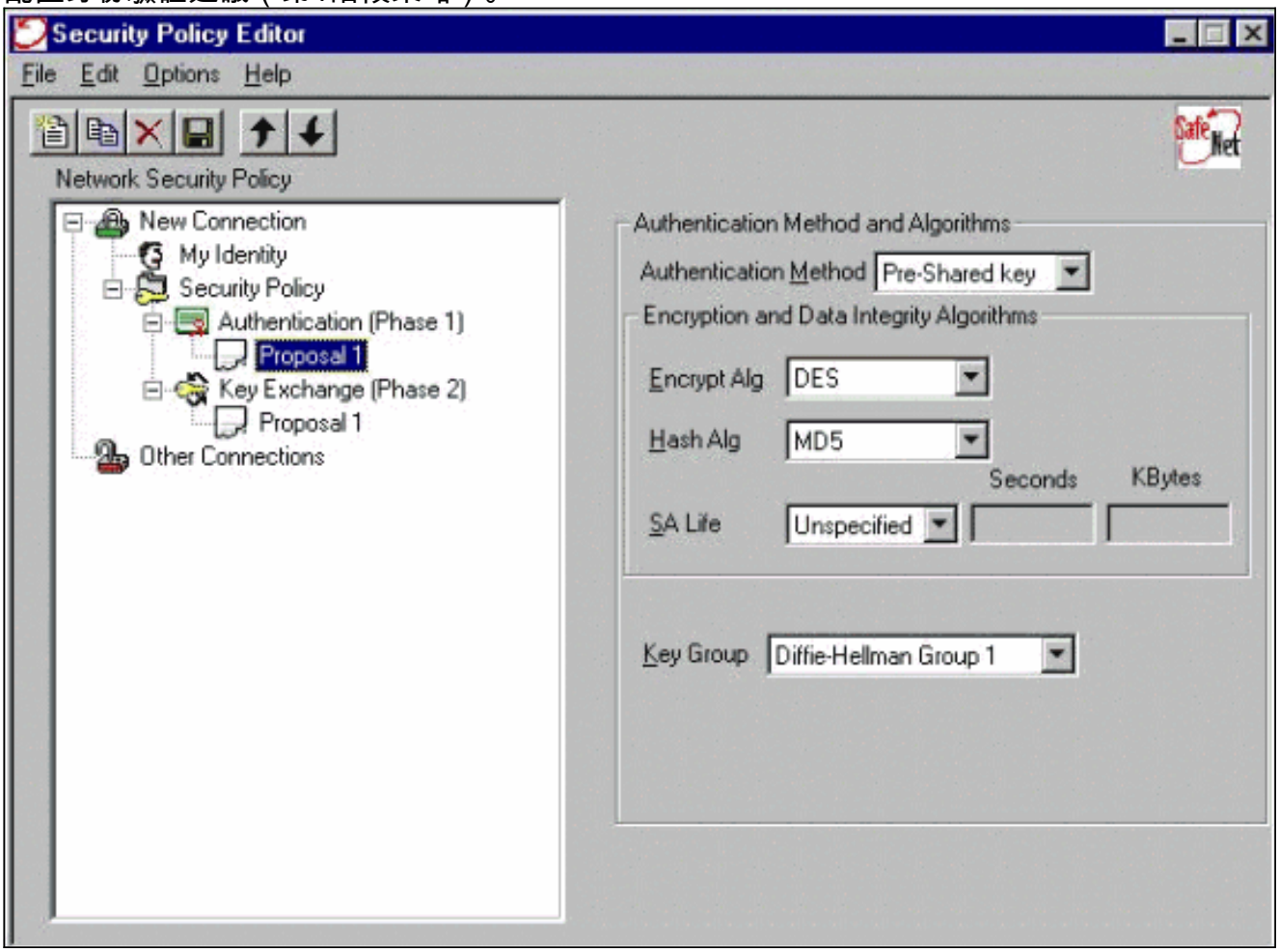
2. 選擇**My Identity**，並將設定保留為預設值。接下來，按一下**Pre-Shared Key**按鈕。



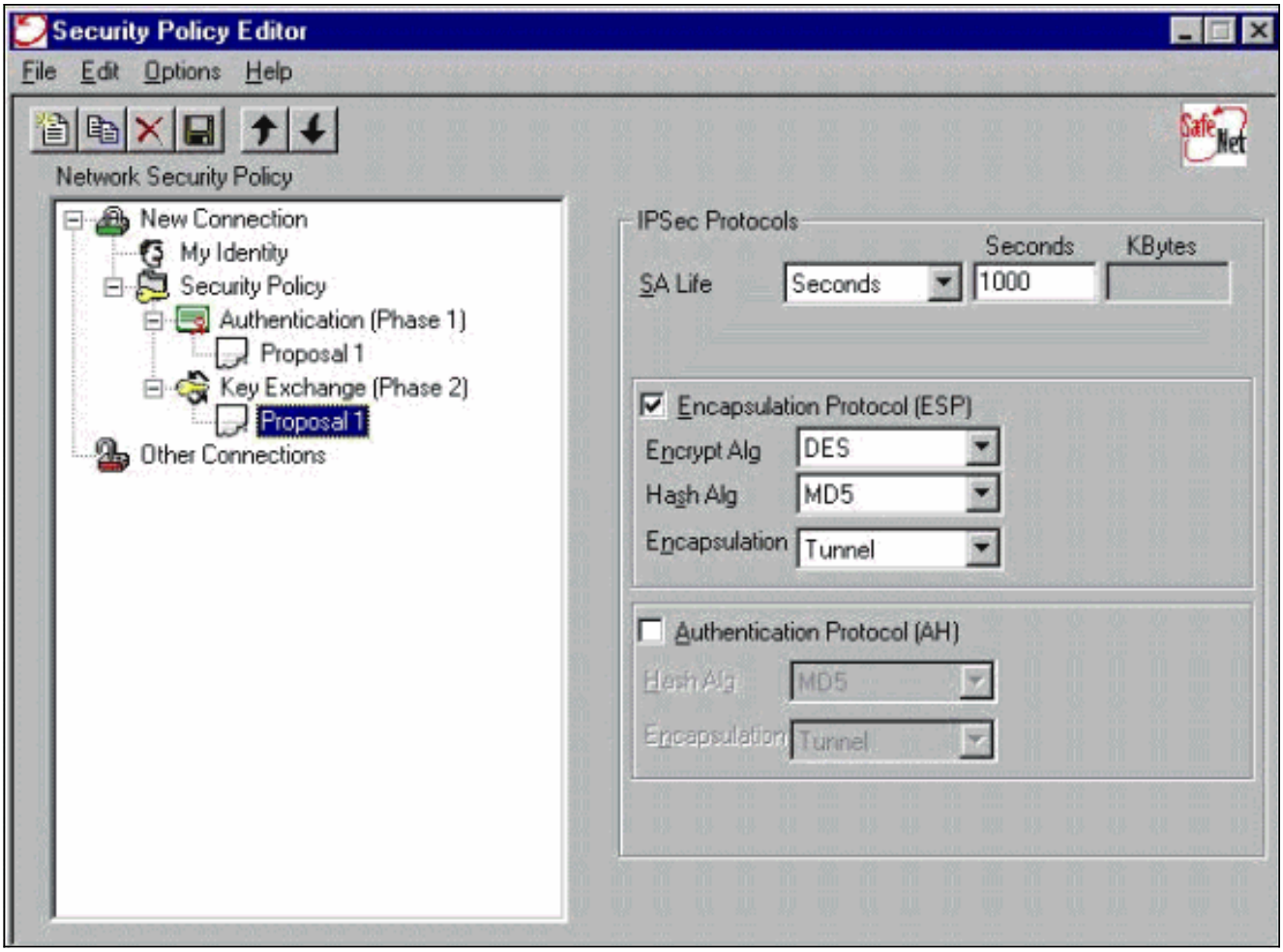
3. 輸入在PIX上配置的預共用金鑰。



4. 配置身份驗證建議（第1階段策略）。



5. 配置IPSec建議（第2階段策略）。



註：完成時不要忘記儲存策略。開啟DOS視窗並ping PIX內部網路上的已知主機，以便從客戶端啟動隧道。您會在第一次ping嘗試交涉通道時收到網際網路控制訊息通訊協定(ICMP)無法連線訊息。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

debug指令

注意：發出**debug指令之前，請參閱**有關Debug指令的重要資訊**。**

要檢視客戶端調試，請啟用思科安全日誌檢視器：

- **debug crypto ipsec sa** — 顯示第2階段的IPSec協商。
- **debug crypto isakmp sa** — 顯示第1階段的ISAKMP協商。
- **debug crypto engine** — 顯示加密會話。

相關資訊

- Cisco Secure PIX防火牆命令參考

- 安全產品現場通知（包括PIX）
- Cisco PIX防火牆軟體產品支援
- 要求建議 (RFC)
- IP安全(IPSec)產品支援頁面
- 配置IPSec網路安全
- 配置Internet金鑰交換安全協定
- IP安全(IPSec)加密簡介
- 通過PIX防火牆的連線
- 配置IPSec
- 技術支援與文件 - Cisco Systems