配置 PIX 到 Cisco Secure VPN 客户端的连接，使用通配符、预置共享、无模式设置

目录

简介

此配置展示如何通过使用通配符以及 **sysopt connection permit-ipsec 和 sysopt ipsec pl-compatible 命令将 VPN 客户端连接至 PIX 防火墙。**本文档还包括 **nat 0 access-list 命令。**

注：加密技术受出口控制。您有责任了解与加密技术出口有关的法律。如果对出口管制有任何疑问，请发送电子邮件到 export@cisco.com。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- 含 Cisco 安全 VPN 客户端 1.0 的 Cisco 安全 PIX 软件版本 5.0.3（在 Help > About 菜单中显示为 2.0.7）或含 Cisco 安全 VPN 客户端 1.1 的 Cisco 安全 PIX 软件版本 6.2.1（在 Help > About 菜单中显示为 2.1.12）。

- Internet 设备在内部访问 Web 主机，IP 地址为 192.68.0.50。
- VPN 客户端使用所有端口在内部访问所有设备（10.1.1.0 /24 和 10.2.2.0 /24）。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您在使用任何命令前已经了解其潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

背景信息

在 PIX 上，**access-list 和 nat 0 命令协同工作。nat 0 access-list 命令旨在代替使用 sysopt ipsec pl-compatible 命令。**如果结合使用 **nat 0 命令和 matching access-list 命令，则必须知道建立 VPN 连接的客户端的 IP 地址，以便创建匹配的访问控制表 (ACL)，绕过 NAT。**

注意： **sysopt ipsec pl-compatible** 命令的扩展性优于**nat 0** 命令和matching **access-list** 命令ir，以绕过网络地址转换(NAT)。 原因是您不需要知道建立连接的客户端 IP 地址。本文档中的可互换命令在配置中以粗体显示。

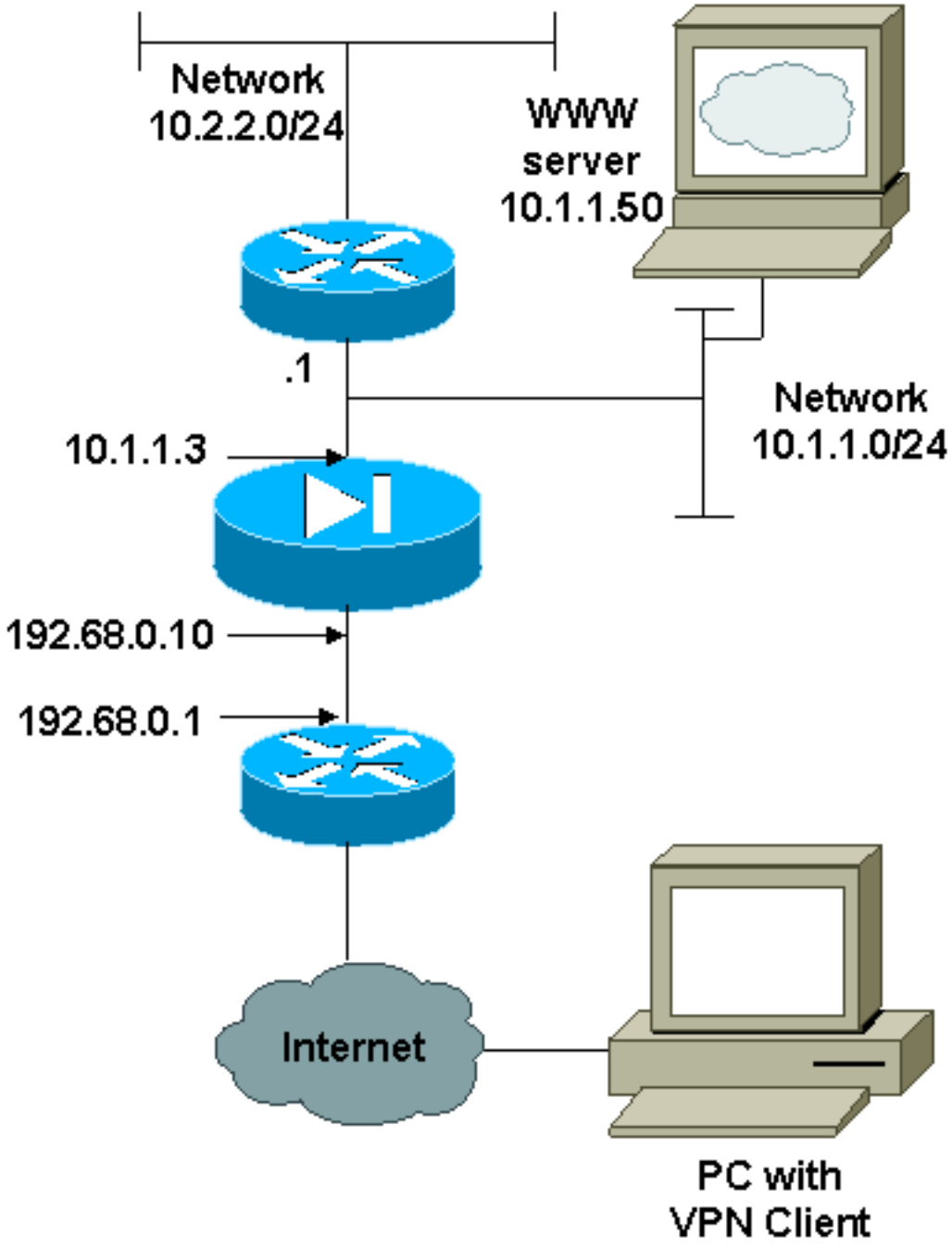
具有 VPN 客户端的用户连接并且接收来自 Internet 服务提供商 (ISP) 的 IP 地址。 用户具有访问防火墙内部所有内容的权限。包括访问网络。此外，不运行客户端的用户可以使用静态分配提供的地址连接至 Web 服务器。内部用户可以连接至 Internet。无需使其流量通过 IPSec 隧道。

配置

本部分提供有关如何配置本文档所述功能的信息。

网络图

本文档使用此图所示的网络设置。



配置

本文档使用此处所示的配置。

- PIX
- VPN 客户

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 客户端配置

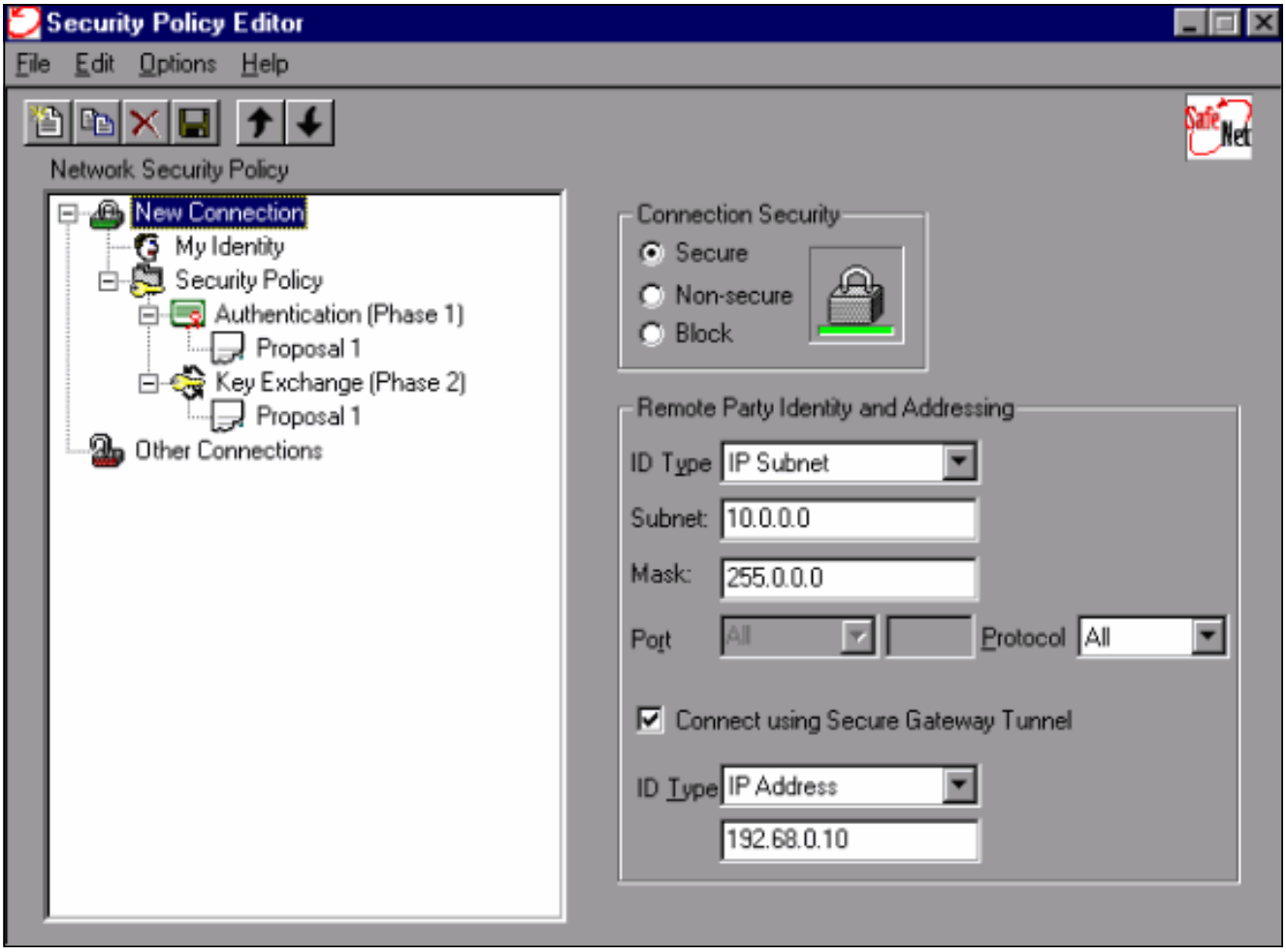
```
Network Security policy:
 1- TACconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP subnet
          10.0.0.0
           255.0.0.0
          Port all Protocol all

     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 客户端 IPSec 的连接策略

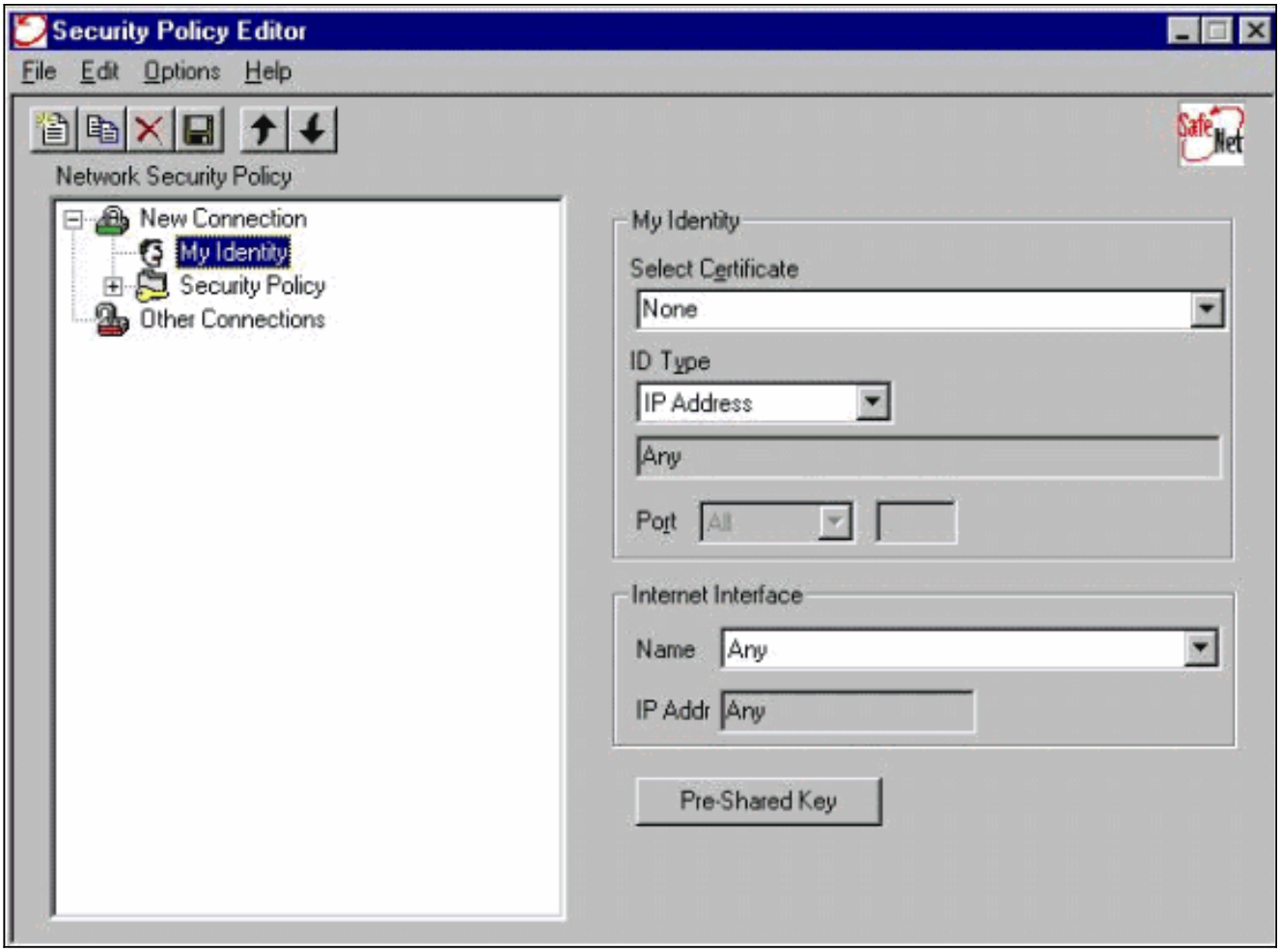
按照以下步骤配置 VPN 客户端 IPSec 的连接策略。

1. 在 Remote Party Identity 和 Addressing 选项卡上，限定您想要使用 VPN 客户端能够到达的

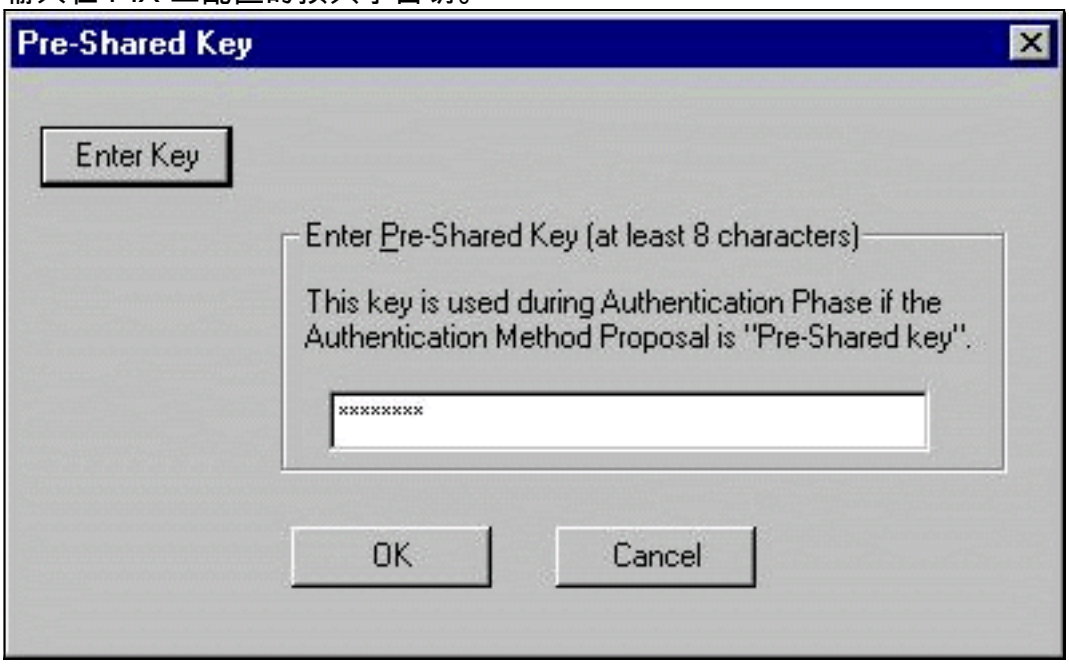
专用网络。然后，选择 **Connect using Secure Gateway Tunnel 并且限定 PIX 的外部 IP 地址**。



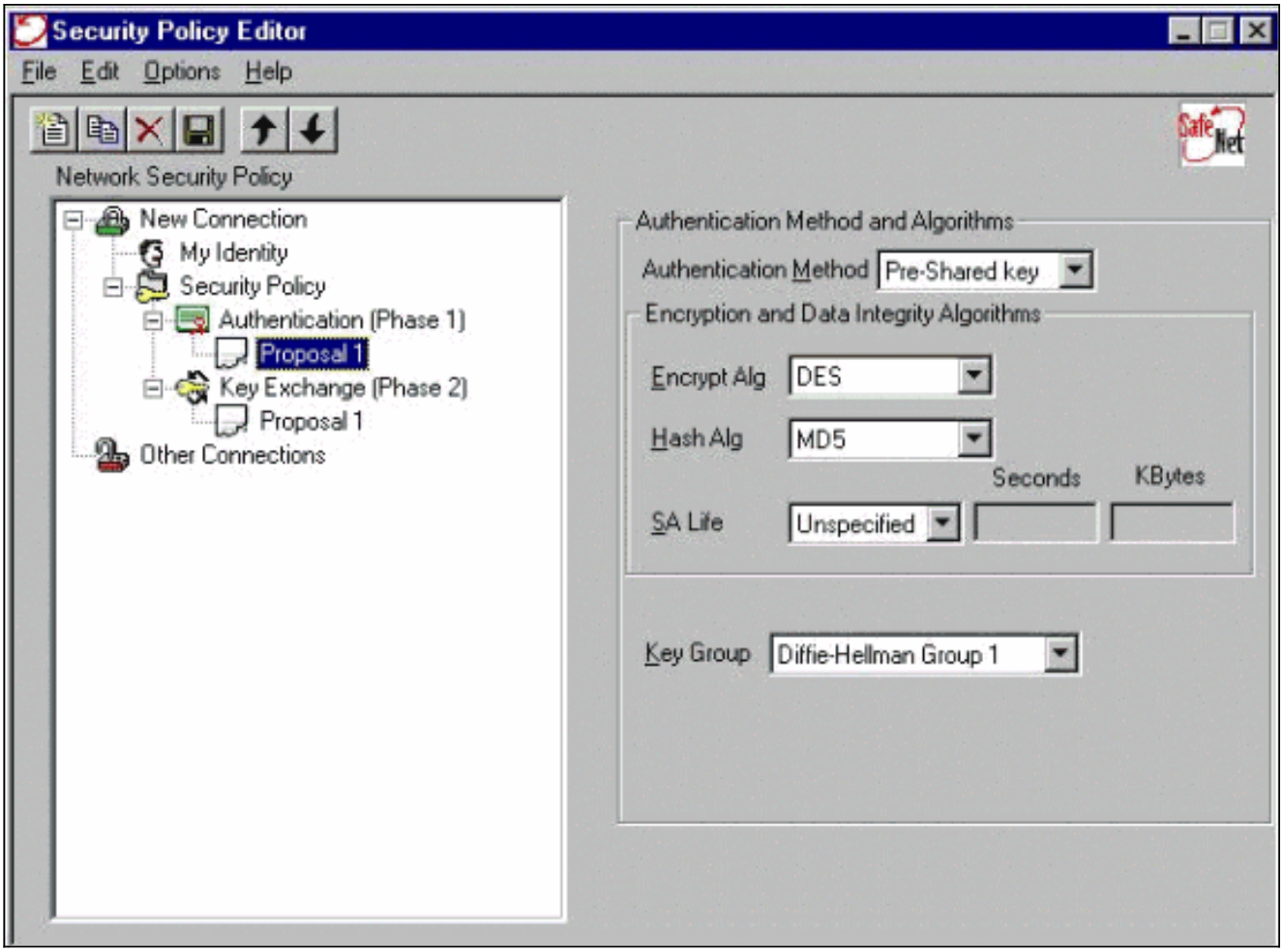
2. 选择 **My Identity 并保留默认设置。**然后，单击 **Pre-Shared Key 按钮。**



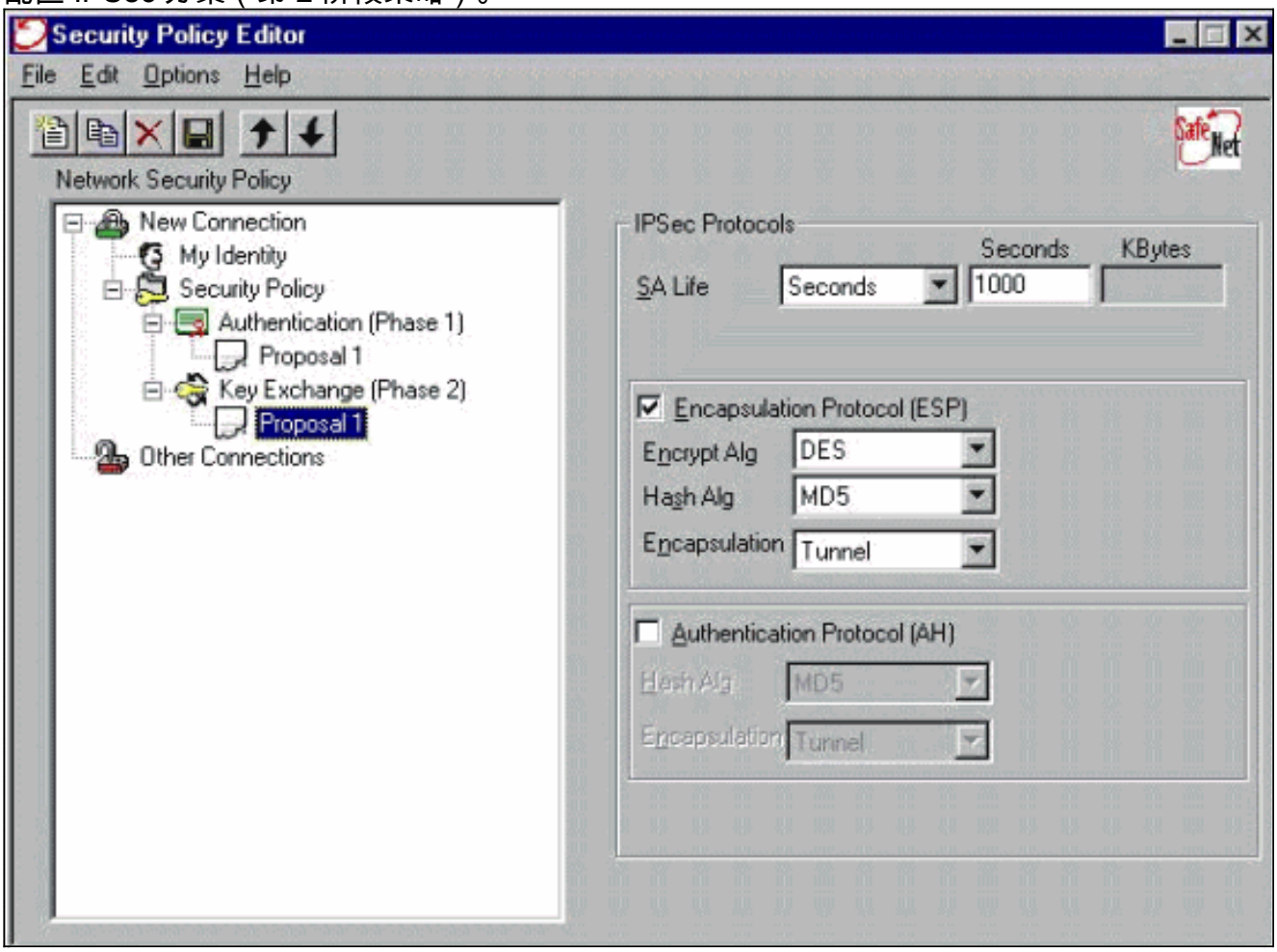
3. 输入在 PIX 上配置的预共享密钥。



4. 配置验证方案（第 1 阶段策略)。



5. 配置 IPSec 方案（第 2 阶段策略）。



注意：完成后，不要忘记保存策略。打开 DOS 窗口并且在 PIX 的网络内部 ping 已知主机，以便从

客户端启动隧道。在 Ping 设法协商隧道时，您会从第一个 ping 中获得 Internet 控制消息协议 (ICMP) 无法到达的消息。

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

调试命令

注意：在发出debug命**令**之前，请参阅有关debug命令的重要信息。

要查看客户端调试，请启用Cisco安全日志查看器：

- **debug crypto ipsec sa** — 显示第2阶段的IPSec协商。
- **debug crypto isakmp sa** — 显示第1阶段的ISAKMP协商。
- **debug crypto engine** — 显示加密会话。

相关信息

- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- Cisco PIX防火墙软件产品支持
- 请求注解 (RFC)
- IP 安全 (IPSec) 产品支持页面
- 配置 IPSec 网络安全
- 配置 Internet 密钥交换安全协议
- IP 安全 (IPsec) 加密简介
- 通过 PIX 防火墙的连接
- 配置 IPSec
- 技术支持和文档 - Cisco Systems