Configuration d'une connexion entre un pare-feu PIX et un Cisco Secure VPN Client avec des caractères génériques, des clés pré-partagées et sans le mode config

Contenu

Introduction

Cette configuration montre comment connecter un client VPN à un pare-feu PIX avec l'utilisation de caractères génériques et les commandes **sysopt connection permit-ipsec** et **sysopt ipsec pl-compatible**. Ce document couvre également la commande **nat 0 access-list**.

Remarque : La technologie de chiffrement est soumise à des contrôles d'exportation. Il est de votre responsabilité de connaître la loi relative à l'exportation de la technologie de chiffrement. Si vous avez des questions concernant le contrôle des exportations, envoyez un courriel à export@cisco.com.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations dans ce document sont basées sur les versions de logiciel et matériel suivantes :

- Logiciel Cisco Secure PIX version 5.0.3 avec Cisco Secure VPN Client 1.0 (voir 2.0.7 dans le menu Help > About) ou Logiciel Cisco Secure PIX version 6.2.1 avec Cisco Secure VPN Client 1.1 (voir 2.1.12 dans le menu Help > About).
- Les machines Internet accèdent à l'hôte Web à l'intérieur avec l'adresse IP 192.68.0.50.
- Le client VPN accède à toutes les machines internes à l'aide de tous les ports (10.1.1.0 /24 et 10.2.2.0 /24).

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Informations générales

Sur PIX, les commandes **access-list** et **nat 0** fonctionnent ensemble. La commande **nat 0 access-list** doit être utilisée au lieu de la commande **sysopt ipsec pl-compatible**. Si vous utilisez la commande **nat 0** avec la commande correspondante **access-list**, vous devez connaître l'adresse IP du client qui établit la connexion VPN afin de créer la liste de contrôle d'accès correspondante (ACL) pour contourner la NAT.

Remarque : La commande **sysopt ipsec pl-compatible** évolue mieux que la commande **nat 0** avec la commande correspondante **access-list** afin de contourner la traduction d'adresses réseau (NAT). La raison est que vous n'avez pas besoin de connaître l'adresse IP des clients qui établissent la connexion. Les commandes interchangeables sont en gras dans la configuration de ce document.

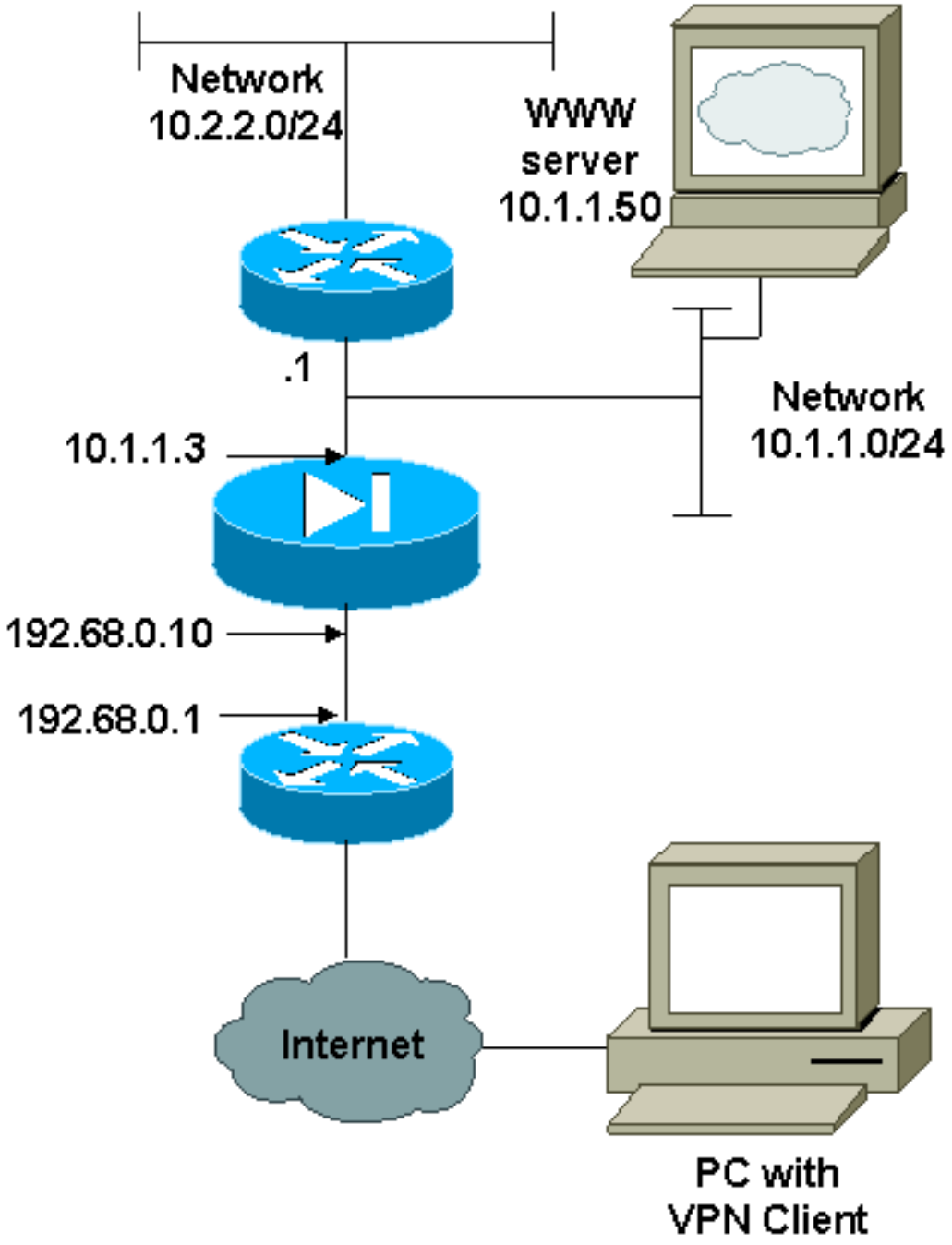
Un utilisateur disposant d'un client VPN se connecte et reçoit une adresse IP de son fournisseur d'accès Internet (FAI). L'utilisateur a accès à tout ce qui se trouve à l'intérieur du pare-feu. Cela inclut les réseaux. En outre, les utilisateurs qui n'exécutent pas le client peuvent se connecter au serveur Web à l'aide de l'adresse fournie par l'affectation statique. Les utilisateurs internes peuvent se connecter à Internet. Il n'est pas nécessaire que leur trafic passe par le tunnel IPSec.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.



Configurations

Ce document utilise les configurations indiquées ici.

- PIX
- Client VPN

Configuration 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]
```

Configuration du client VPN

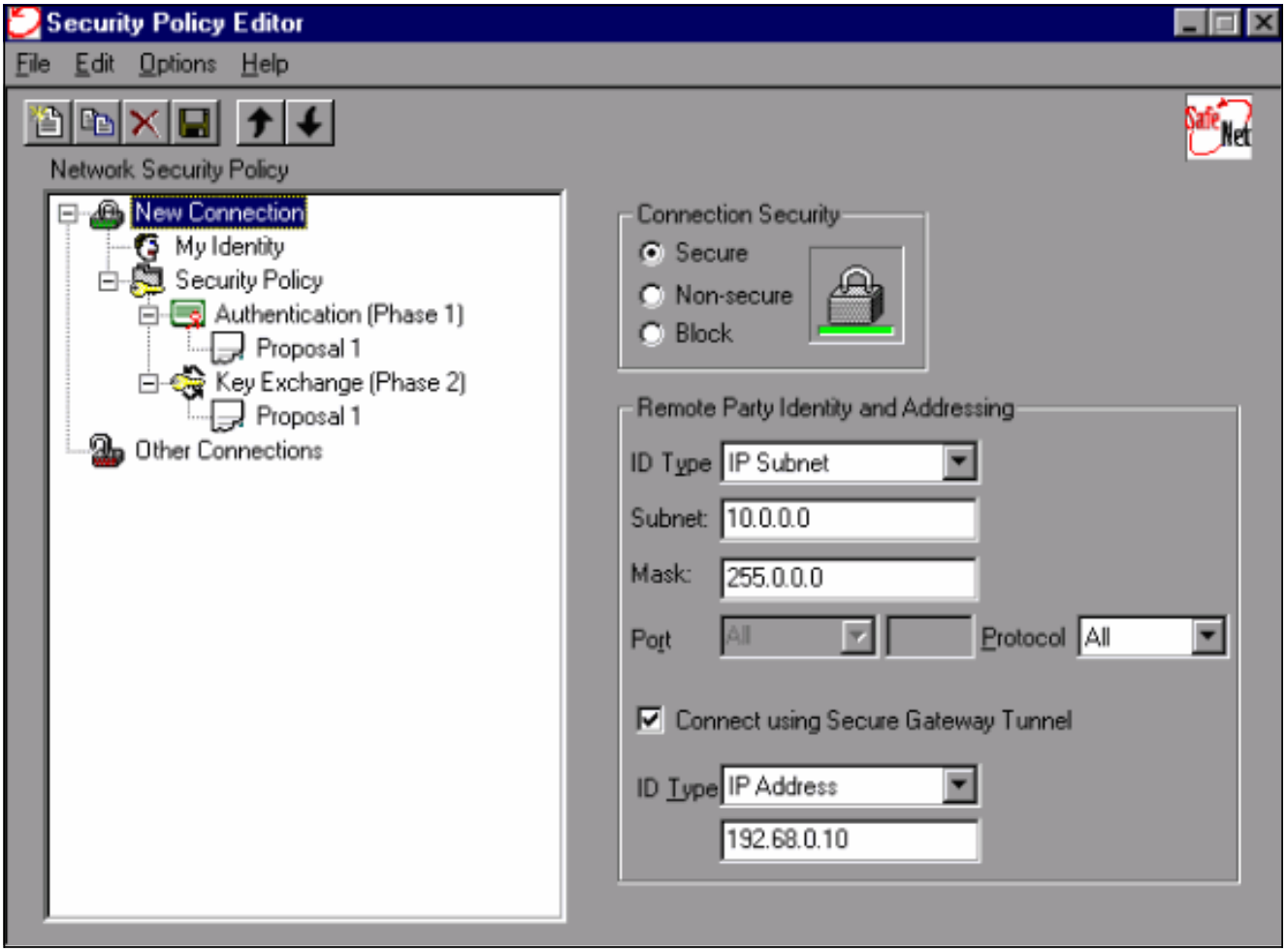
```
Network Security policy:
 1- TACconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP subnet
          10.0.0.0
           255.0.0.0
          Port all Protocol all

     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
```

Configurer la stratégie pour la connexion IPSec du client VPN

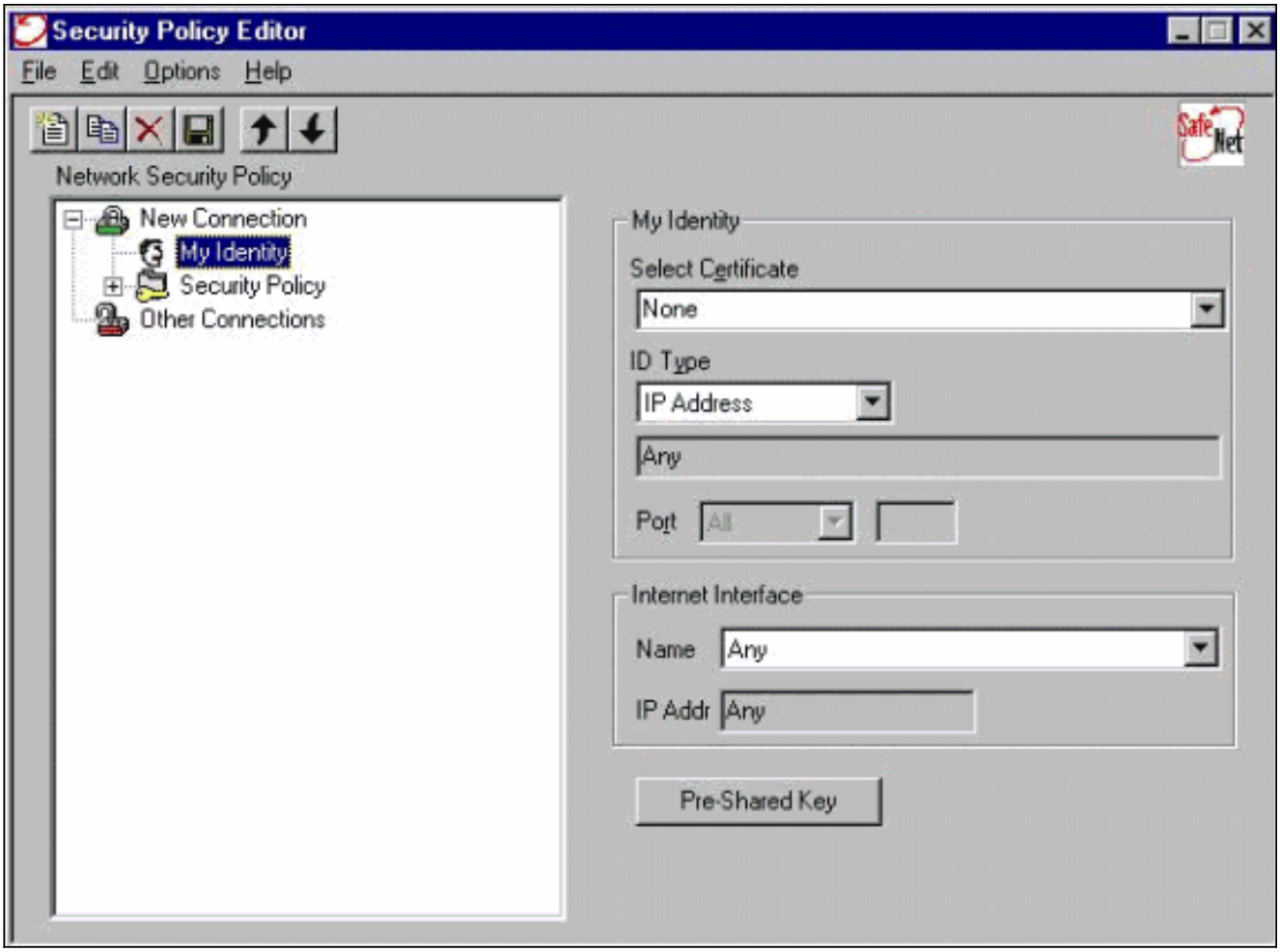
Procédez comme suit pour configurer la stratégie pour la connexion IPSec du client VPN.

1. Dans l'onglet Remote Party Identity and Addressing, définissez le réseau privé que vous

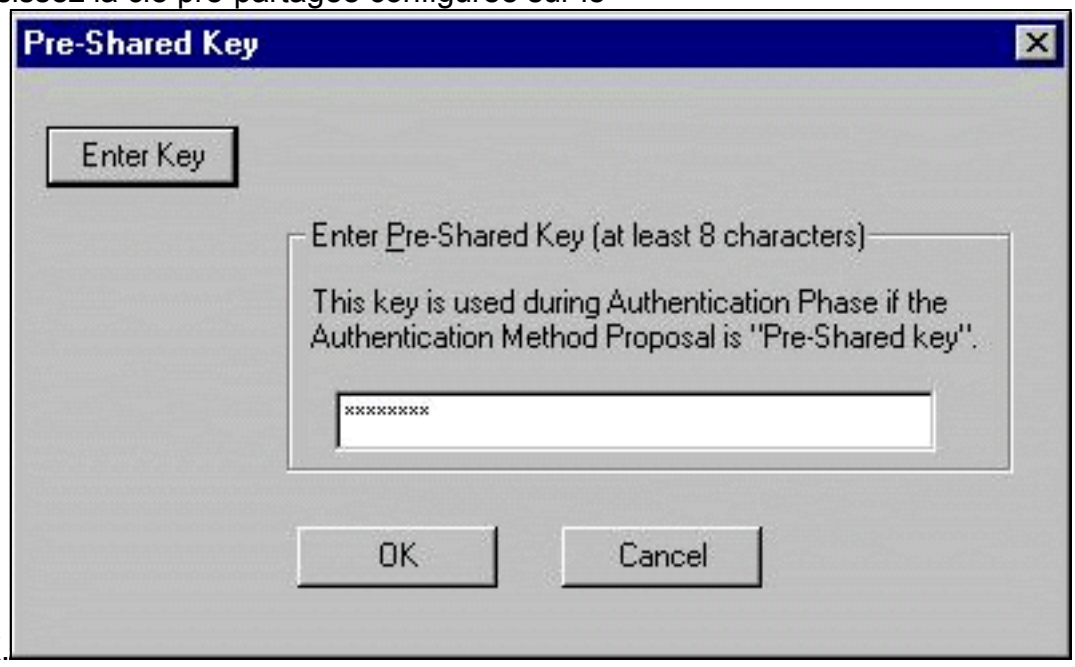
souhaitez atteindre à l'aide du client VPN. Ensuite, sélectionnez **Connect using Secure Gateway Tunnel** et définissez l'adresse IP externe du PIX.



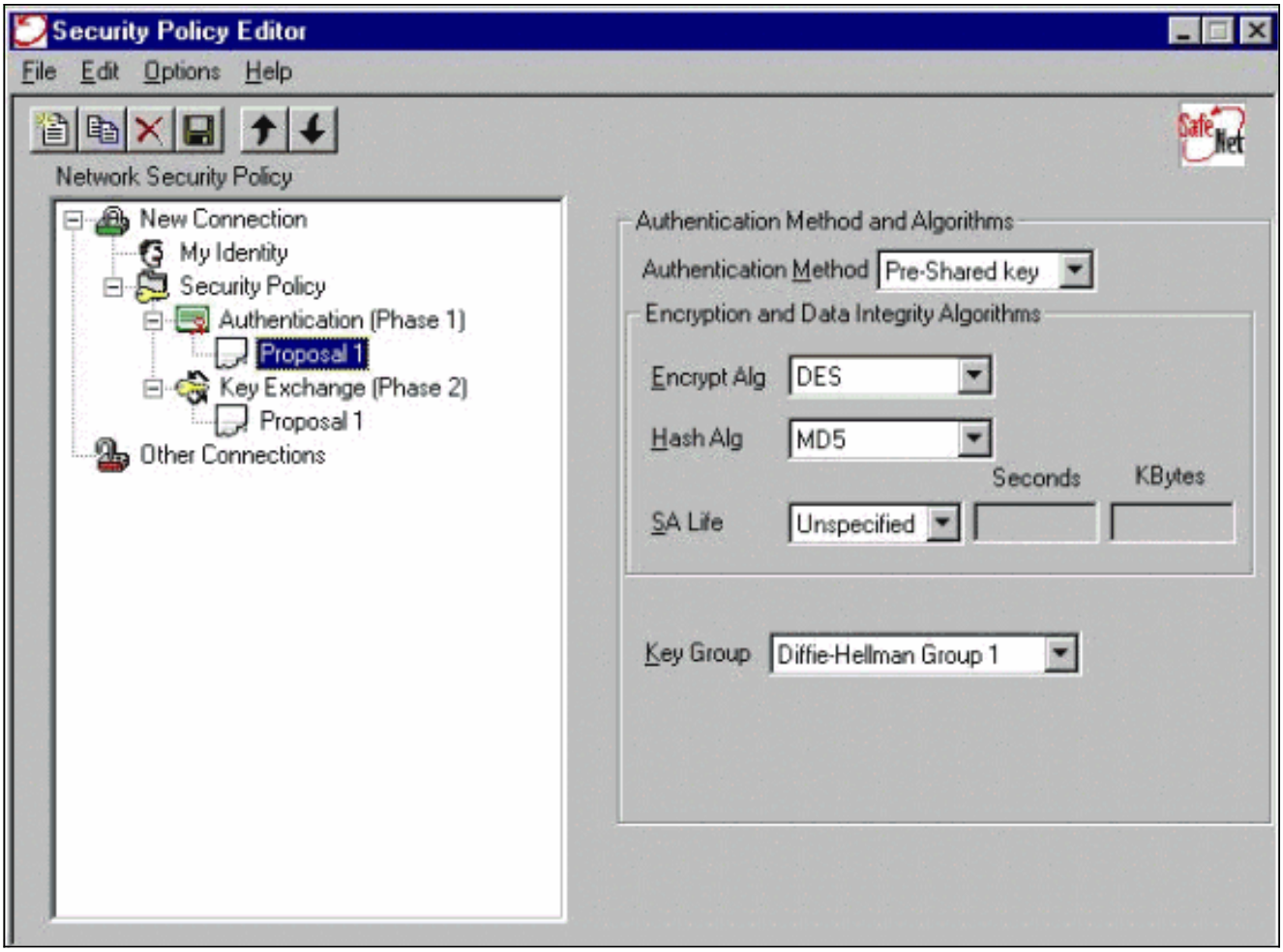
2. Sélectionnez **Mon identité** et conservez le paramètre par défaut. Cliquez ensuite sur le bouton **Clé prépartagée**.



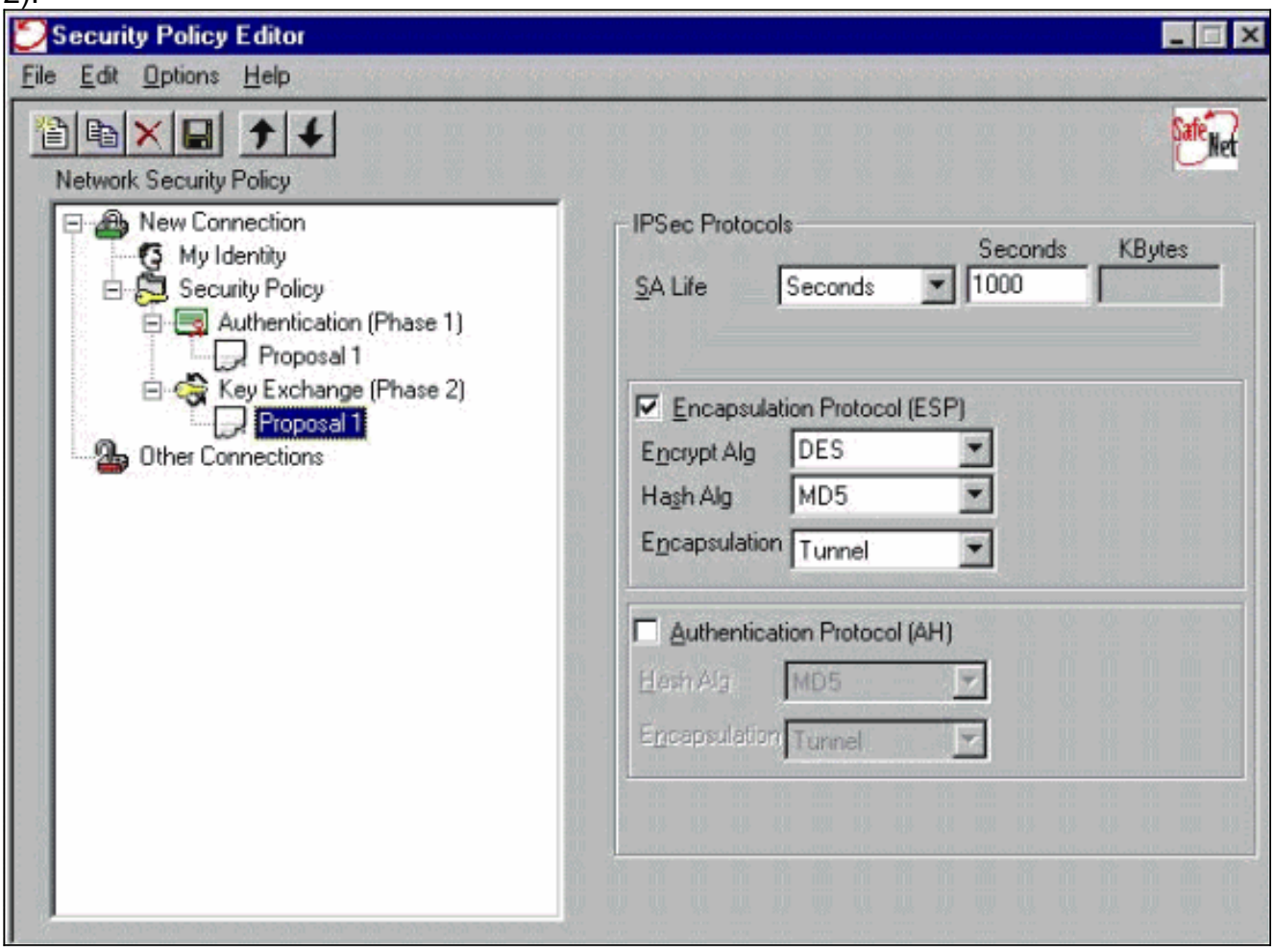
3. Saisissez la clé pré-partagée configurée sur le PIX.



4. Configurez la proposition d'authentification (stratégie de phase 1).



5. Configurez la proposition IPSec (stratégie de phase 2).



Remarque : N'oubliez pas d'enregistrer la stratégie lorsque vous avez terminé. Ouvrez une fenêtre DOS et envoyez une requête ping à un hôte connu sur le réseau interne du PIX afin d'initier le tunnel à partir du client. Vous recevez un message ICMP (Internet Control Message Protocol) inaccessible depuis la première requête ping lorsqu'elle tente de négocier le tunnel.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Commandes de débogage

Remarque : Avant d'émettre des commandes **debug**, reportez-vous à Informations importantes sur les commandes de débogage.

Pour afficher les débogages côté client, activez Cisco Secure Log Viewer :

- **debug crypto ipsec sa** - Affiche les négociations IPSec de la phase 2.
- **debug crypto isakmp sa** - Affiche les négociations ISAKMP de la phase 1.
- **debug crypto engine** - Affiche les sessions chiffrées.

Informations connexes

- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Assistance produit du logiciel Cisco PIX Firewall
- Demandes de commentaires (RFC)
- Pages d'assistance produit IPSec (IP Security)
- Configuration de la sécurité des réseaux IPSec
- Configuration du protocole IKE (Internet Key Exchange)
- Présentation du chiffrement IPSec (IP Security)
- Connectivité via le pare-feu PIX
- Configuration d'IPSec
- Support et documentation techniques - Cisco Systems