Настройка PIX для Cisco Secure VPN Client Wild-card, Pre-shared, No Mode-Config

Содержание

Введение

Эта конфигурация демонстрирует, как подключить Клиент VPN с межсетевым экраном PIX с использованием подстановочных знаков и **sysopt connection permit-ipsec** и **команд sysopt ipsec pl-compatible**. Этот документ также покрывает **команду nat 0 access-list**.

Примечание: Технология шифрования подлежит экспортному контролю. Это - ваша обязанность знать законы, отнесенные к экспорту технологии шифрования. При возникновении любых вопросов отнесенные к экспортному контролю, пошлите Электронное письмо export@cisco.com.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования.

- Выпуск ПО Cisco Secure PIX 5.0.3 с Cisco Secure VPN Client 1.0 (показанный как 2.0.7 в меню Help> About) или Выпуск ПО Cisco Secure PIX 6.2.1 с Cisco Secure VPN Client 1.1 (показанный как 2.1.12 в меню Help> About).
- Интернет-машины обращаются к веб-хосту на внутренней части с IP-адресом 192.68.0.50.
- Клиент VPN обращается ко всем машинам на внутренней части с использованием всех портов (10.1.1.0 / 24 и 10.2.2.0 / 24).

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. Перед выполнением любых команд в активной сети необходимо осознавать потенциальные последствия их применения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Общие сведения

В PIX команды access-list и nat 0 работают совместно. Команда nat 0 access-list предназначена, чтобы использоваться вместо **команды sysopt ipsec pl-compatible**. При использовании **команды nat 0** с соответствующей **командой access-list** необходимо знать IP-адрес клиента, который делает VPN-подключение для создания соответствующего списка контроля доступа (ACL) для обхода NAT.

Примечание: Sysopt ipsec pl-compatible command scales лучше, чем **команда nat 0** с соответствующей **командой access-list** ir заказ обойти Технологию NAT. Причина состоит в том, потому что вы не должны знать IP-адрес клиентов, которые делают соединение. Взаимозаменяемые команды являются полужирными в конфигурации в этом документе.

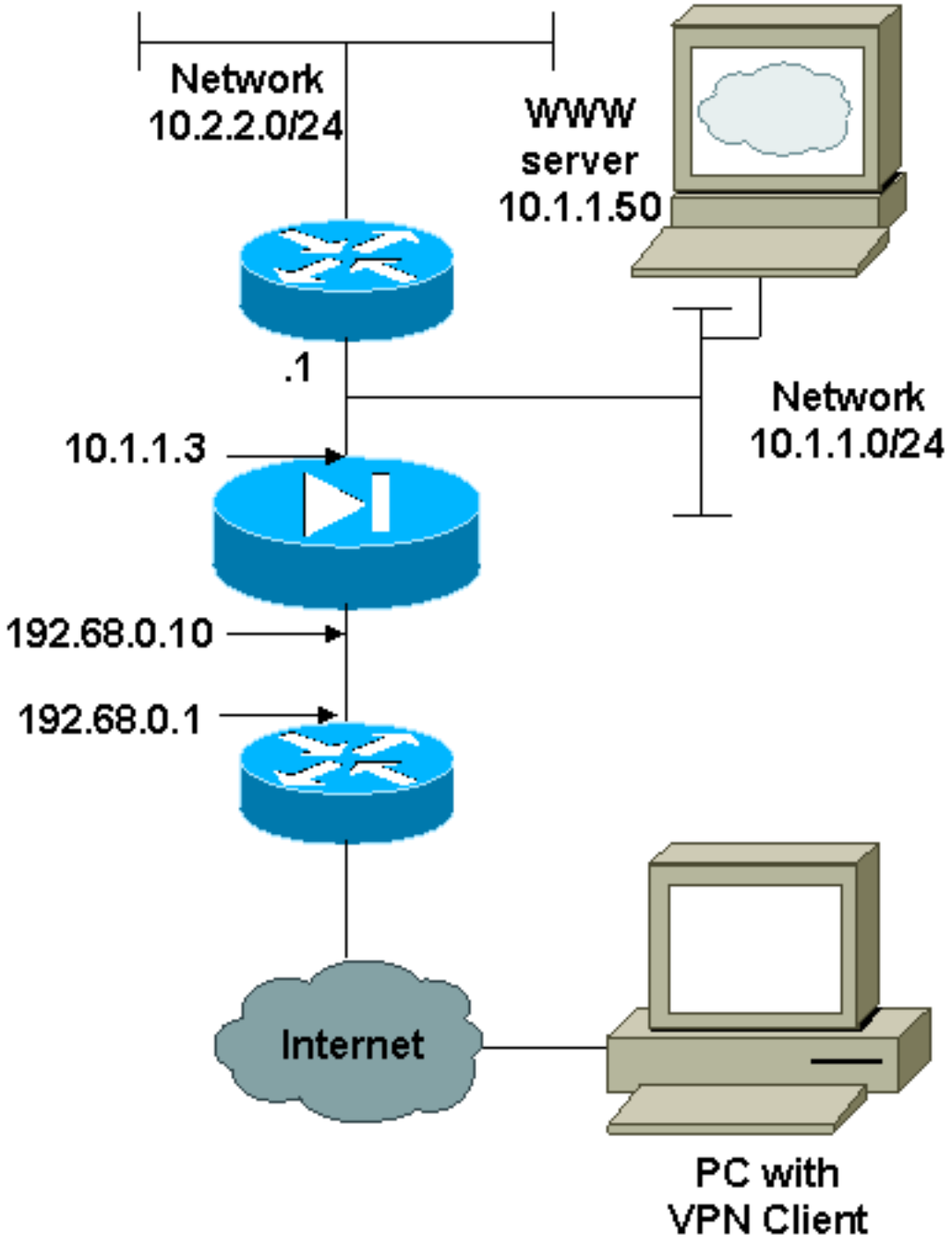
Пользователь с Клиентом VPN подключает и получает IP-адрес от их интернет-провайдера (ISP). У пользователя есть доступ ко всему на внутренней части межсетевого экрана. Это включает сети. Кроме того, пользователи, которые не выполняют клиента, могут соединиться с Web-сервером с использованием адреса, предоставленного статическим назначением. Пользователи на внутренней части могут соединиться с Интернетом. Необязательно для их трафика для прохождения через Туннеля IPSec.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Схема сети

В этом документе используются настройки сети, показанные на данной диаграмме.



Конфигурации

В данном документе используется следующая конфигурация.

- PIX
- VPN-клиент

Конфигурация 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]
```

Конфигурация клиента VPN

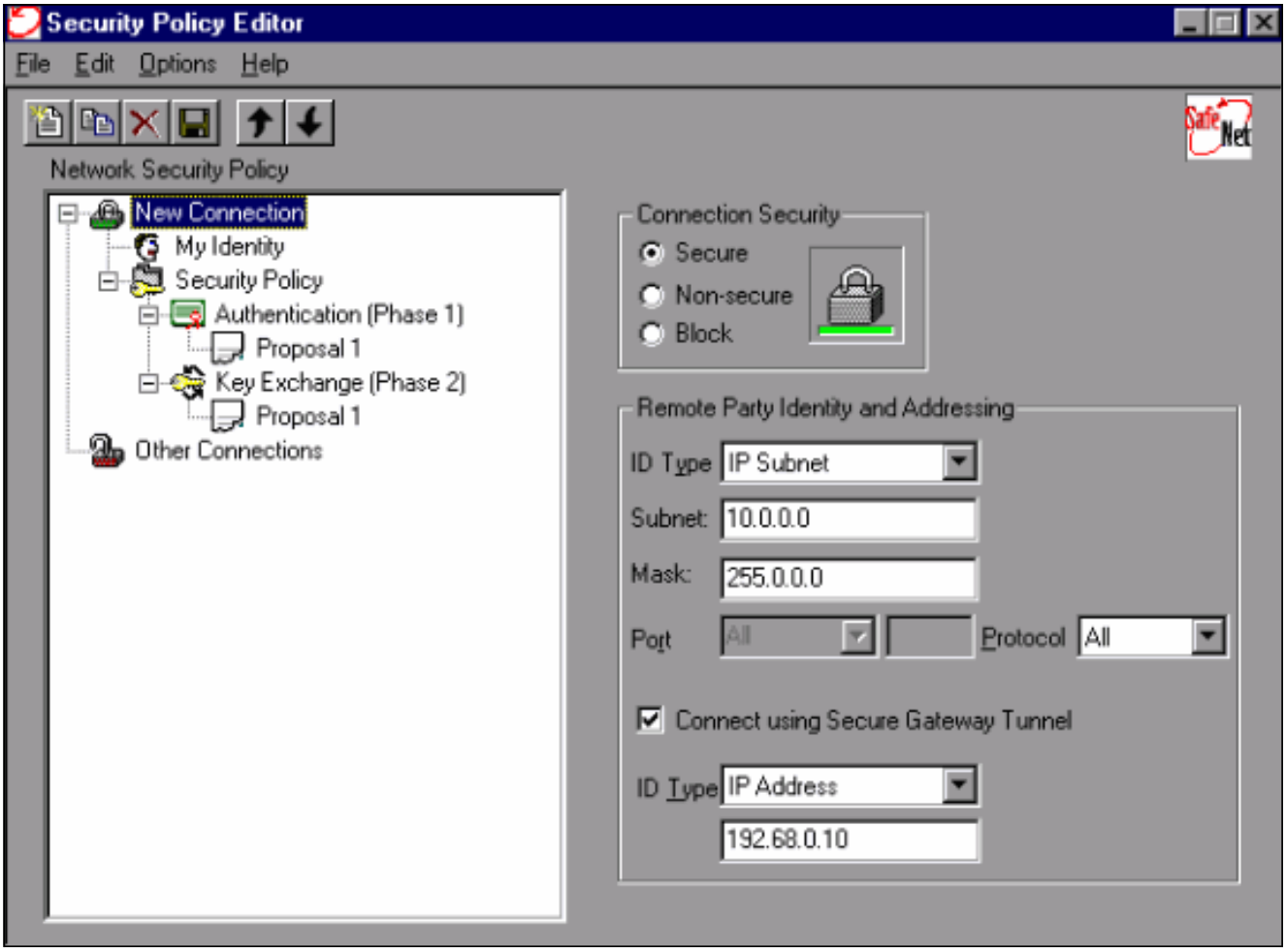
```
Network Security policy:
 1- TACconn
     My Identity
          Connection security: Secure
          Remote Party Identity and addressing
          ID Type: IP subnet
          10.0.0.0
           255.0.0.0
          Port all Protocol all

     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
```

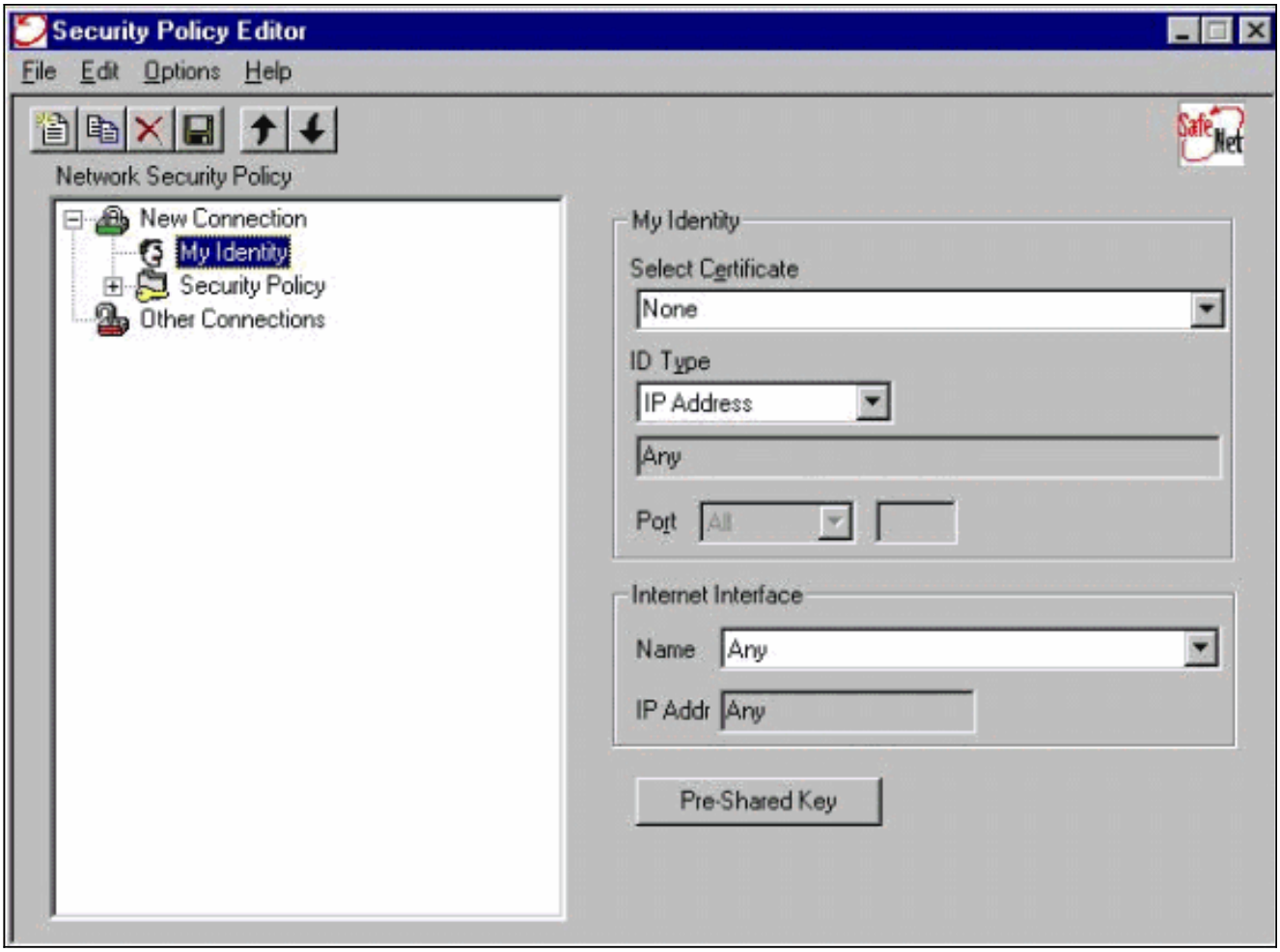
Настройте политику для IP - безопасного соединения клиента VPN

Выполните эти действия для настройки политики для IP - безопасного соединения Клиента VPN.

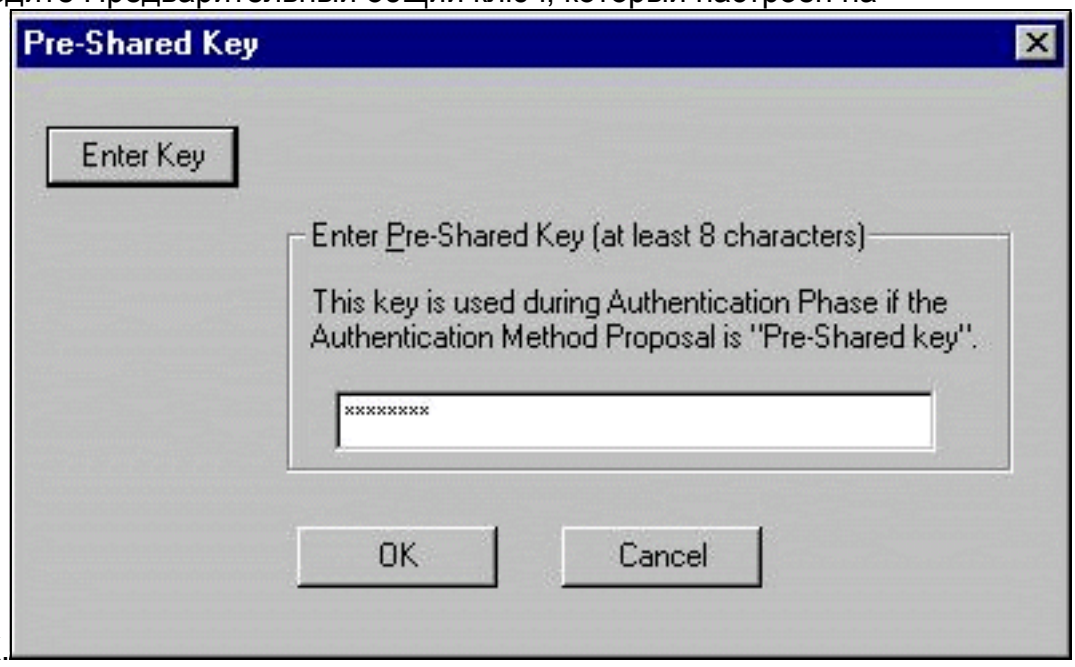
1. На вкладке Remote Party Identity и Addressing определите частную сеть, которой вы хотите быть в состоянии достигнуть с использованием Клиента VPN. Затем, выберите **Connect с помощью Туннеля Защищенного шлюза** и определите внешний IP - адрес PIX.



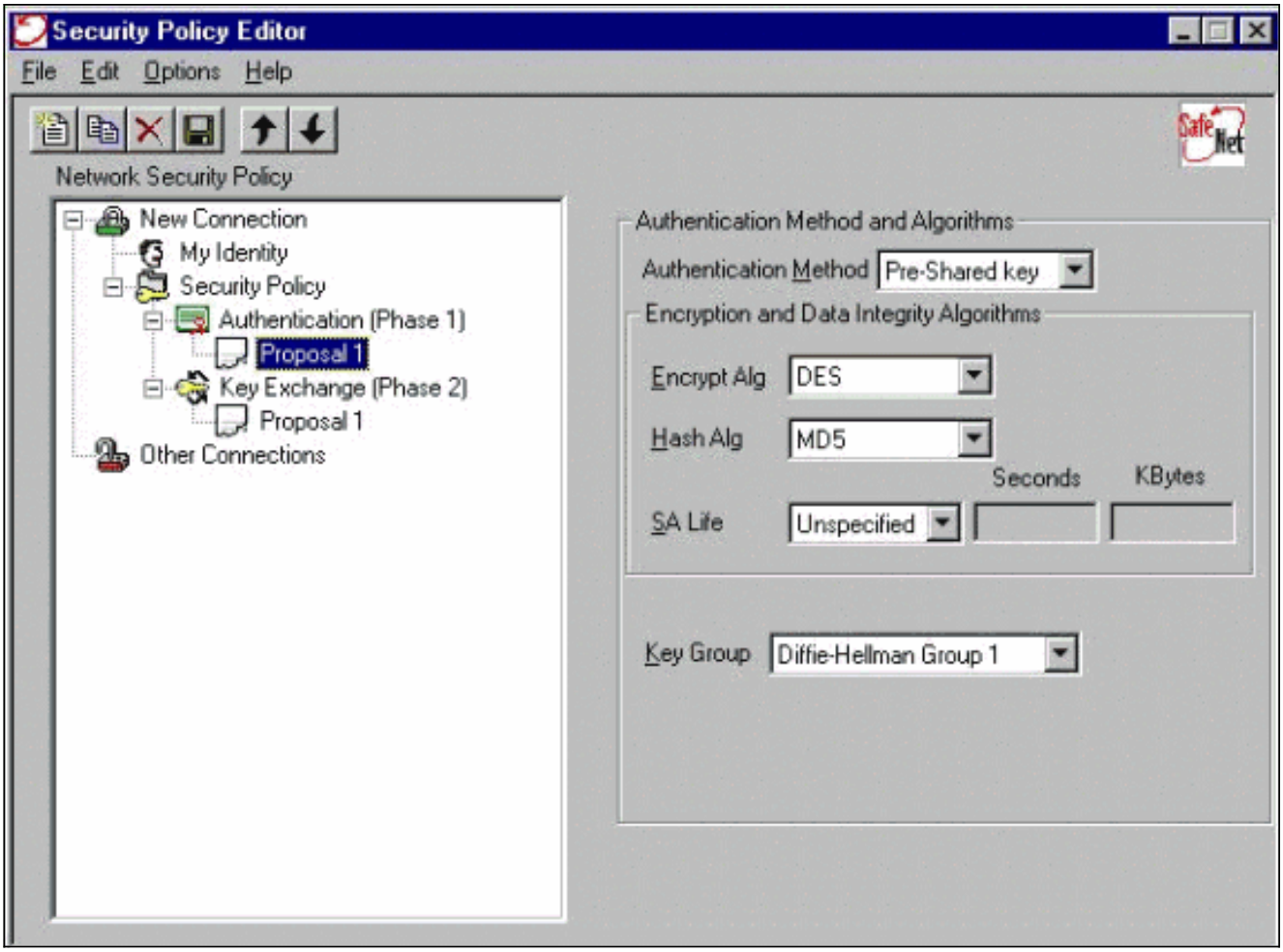
2. Выберите **My Identity** и оставьте установку по умолчанию. Затем, нажмите кнопку **Pre-Shared Key**.



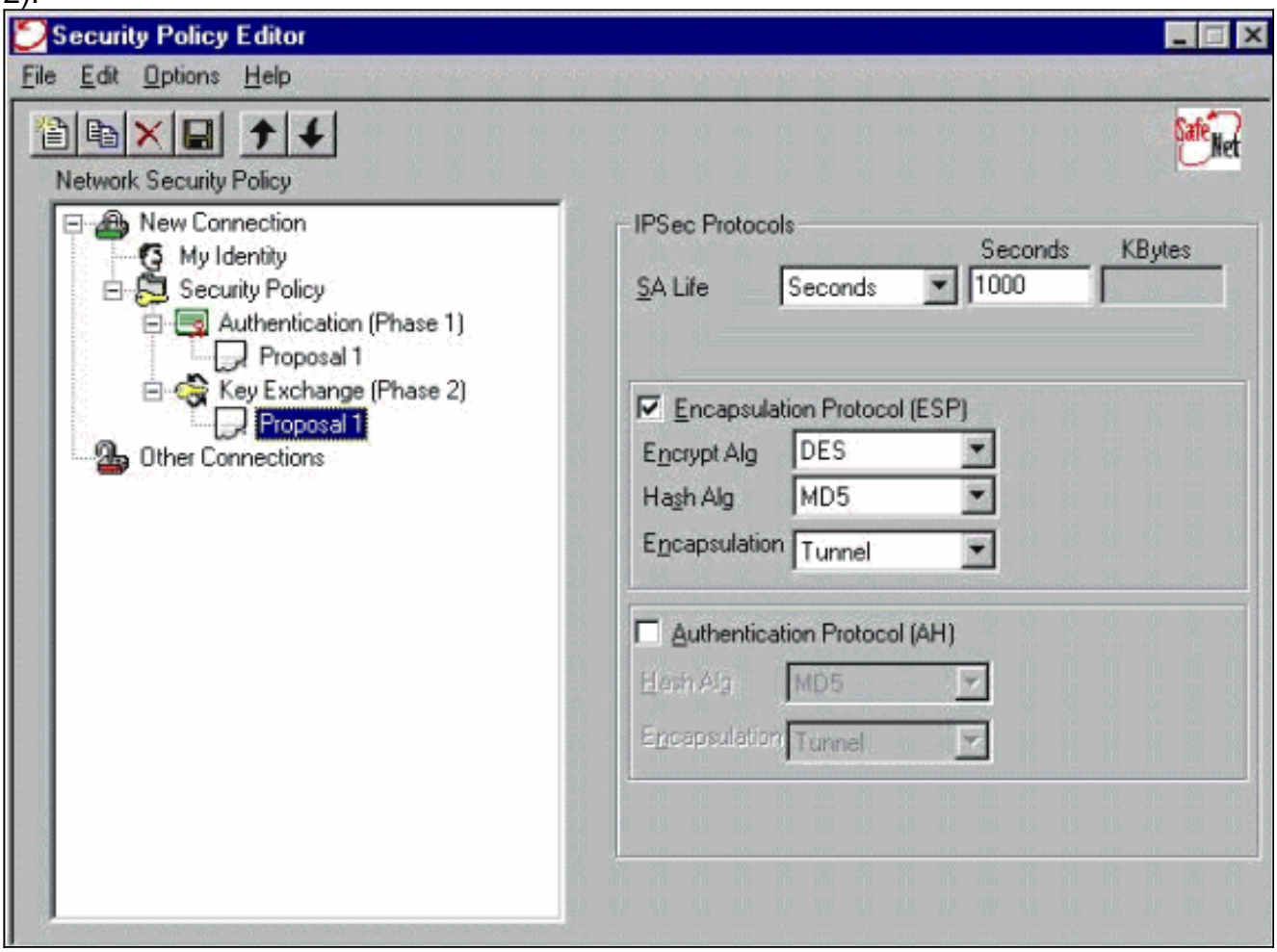
3. Введите Предварительный общий ключ, который настроен на PIX.



4. Настройте Предложение аутентификации (Политика фазы 1).



5. Настройте предложение IPSec (Политика фазы 2).



Примечание: Не забывайте сохранять политику, когда вы будете закончены. Откройте Окно DOS и пропингуйте известный хост на внутренней сети PIX для инициирования туннеля от клиента. Вы получаете недостижимое сообщение Протокола ICMP от первого эхо-запроса, поскольку он пытается выполнить согласование о туннеле.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

команды "debug"

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

Для наблюдения Отладок на стороне клиента включите Служебной программе просмотра журнала Cisco Secure:

- **debug crypto ipsec sa– показывает процесс согласования по протоколу IPSec на этапе 2.**
- **debug crypto isakmp sa** - Отображает Isakmp - согласование фазы 1.
- **debug crypto engine– служит для просмотра шифруемых сеансов.**

Дополнительные сведения

- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Поддержка продуктов программного обеспечения Cisco PIX Firewall
- Запросы комментариев (RFC)
- Страницы поддержки продуктов с IP Security (IPSec)
- Настройка параметров сетевой безопасности IPSec Network Security
- Настройка протокола защищенного обмена ключами IKE
- Введение в шифрование IPSec
- Возможность соединения через PIX Firewall
- Выбор конфигурации IPSec
- Cisco Systems – техническая поддержка и документация