Настройка туннеля локальных сетей IPSec между брандмауэром Cisco Pix и брандмауэром NetScreen

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Настройка
Схема сети
Конфигурации
Проверка
Команды проверки
Выходные данные проверки
Устранение неполадок
Команды для устранения неполадок
Пример результата отладки
Дополнительные сведения

Введение

Этот документ описывает необходимый порядок действий для создания IPSec-туннеля между локальными сетями сетевого экрана Cisco PIX и межсетевого экрана NetScreen с последними версиями программного обеспечения. За каждым устройством существует частная сеть, соединяемая с другим межсетевым экраном через туннель IPSec.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Межсетевой экран NetScreen настроен с IP-адресами на трастовых/нетрастовых интерфейсах.
- Подключение установлено к Интернету.

Используемые компоненты

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

- Версия 6.3 (1) программного обеспечения межсетевого экрана PIX
- NetScreen последний пересмотр

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

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

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурации

Эти конфигурации используются в данном документе:

- Сетевой экран PIX
- Межсетевой экран NetScreen

Настройте межсетевой экран PIX

Сетевой экран PIX
`PIX Version 6.3(1)interface ethernet0 10basetinterface`

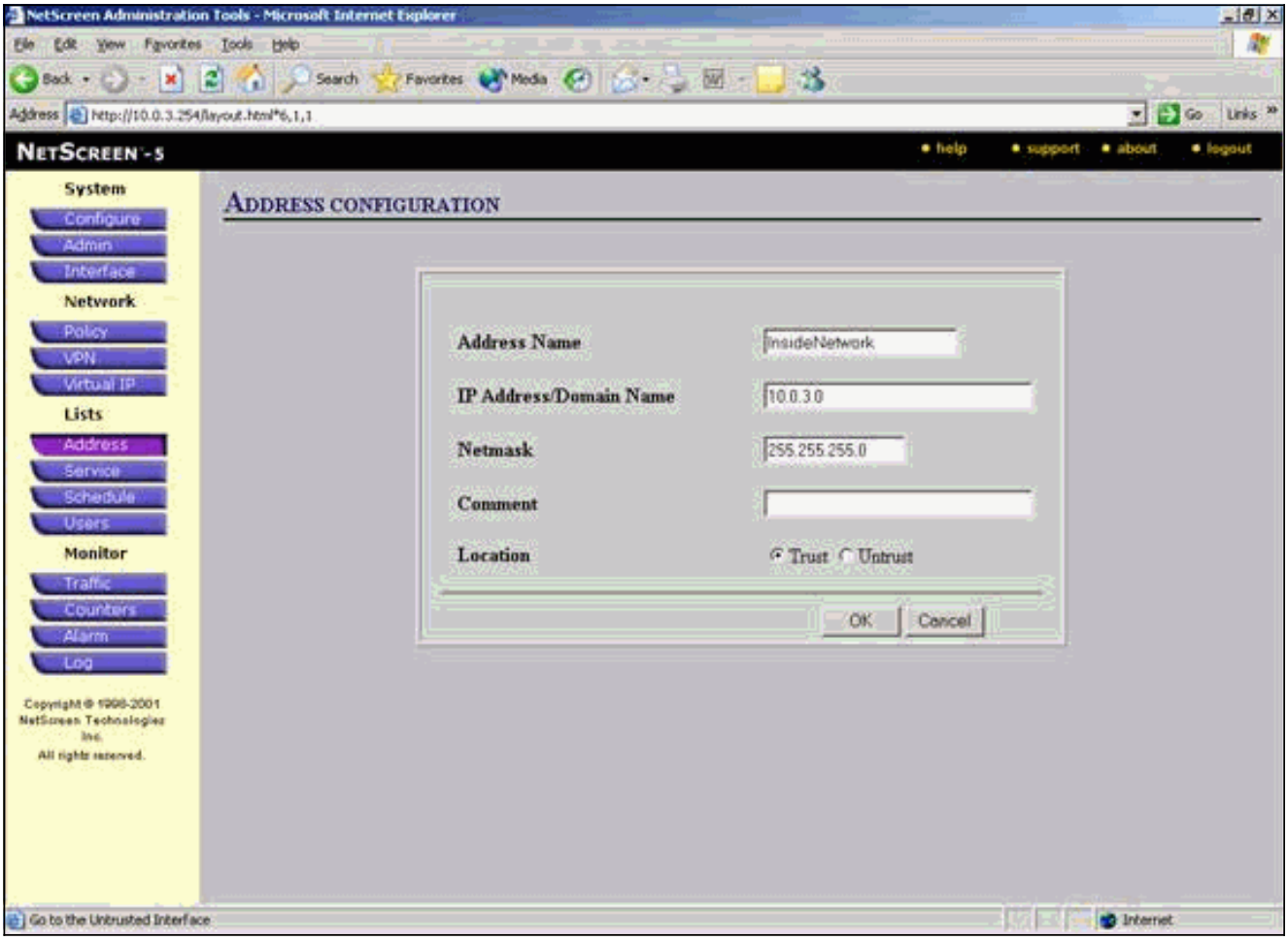
```
ethernet1 100fullnameif ethernet0 outside
security0nameif ethernet1 inside security100enable
password 8Ry2YjIyt7RRXU24 encryptedpasswd
2KFQnbNIdI.2KYOU encryptedhostname pixfirewalldomain-
name cisco.comfixup protocol ftp 21fixup protocol h323
h225 1720fixup protocol h323 ras 1718-1719fixup protocol
http 80fixup protocol ils 389fixup protocol rsh 514fixup
protocol rtsp 554fixup protocol sip 5060fixup protocol
sip udp 5060fixup protocol skinny 2000fixup protocol
smtp 25fixup protocol sqlnet 1521names!--- Access
control list (ACL) for interesting traffic to be
encrypted and !--- to bypass the Network Address
Translation (NAT) process.access-list nonat permit ip
10.0.25.0 255.255.255.0 10.0.3.0 255.255.255.0pager
lines 24logging onlogging timestamplogging buffered
debuggingicmp permit any insidemtu outside 1500mtu
inside 1500!--- IP addresses on the interfaces.ip
address outside 172.18.124.96 255.255.255.0ip address
inside 10.0.25.254 255.255.255.0ip audit info action
alarmip audit attack action alarmpdm logging
informational 100pdm history enablearp timeout
14400global (outside) 1 interface!--- Bypass of NAT for
IPsec interesting inside network traffic.nat (inside) 0
access-list nonatnat (inside) 1 0.0.0.0 0.0.0.0 0 0!---
Default gateway to the Internet.route outside 0.0.0.0
0.0.0.0 172.18.124.1 1timeout xlate 0:05:00timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225
1:00:00timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00
sip_media 0:02:00timeout uauth 0:05:00 absoluteaaa-
server TACACS+ protocol tacacs+aaa-server RADIUS
protocol radiusaaa-server LOCAL protocol localhttp
10.0.0.0 255.0.0.0 insideno snmp-server locationno snmp-
server contactsnmp-server community publicno snmp-server
enable trapsfloodguard enable!--- This command avoids
applied ACLs or conduits on encrypted packets.sysopt
connection permit-ipsec!--- Configuration of IPsec Phase
2.crypto ipsec transform-set mytrans esp-3des esp-sha-
hmaccrypto map mymap 10 ipsec-isakmpcrypto map mymap 10
match address nonatcrypto map mymap 10 set pfs
group2crypto map mymap 10 set peer 172.18.173.85crypto
map mymap 10 set transform-set mytranscrypto map mymap
interface outside!--- Configuration of IPsec Phase
1.isakmp enable outside!--- Internet Key Exchange (IKE)
pre-shared key !--- that the peers use to
authenticate.isakmp key testme address 172.18.173.85
netmask 255.255.255.255isakmp identity addressisakmp
policy 10 authentication pre-shareisakmp policy 10
encryption 3desisakmp policy 10 hash shaisakmp policy 10
group 2isakmp policy 10 lifetime 86400telnet timeout
5ssh timeout 5console timeout 0dhcpd lease 3600dhcpd
ping_timeout 750terminal width 80
```

Настройте межсетевой экран NetScreen

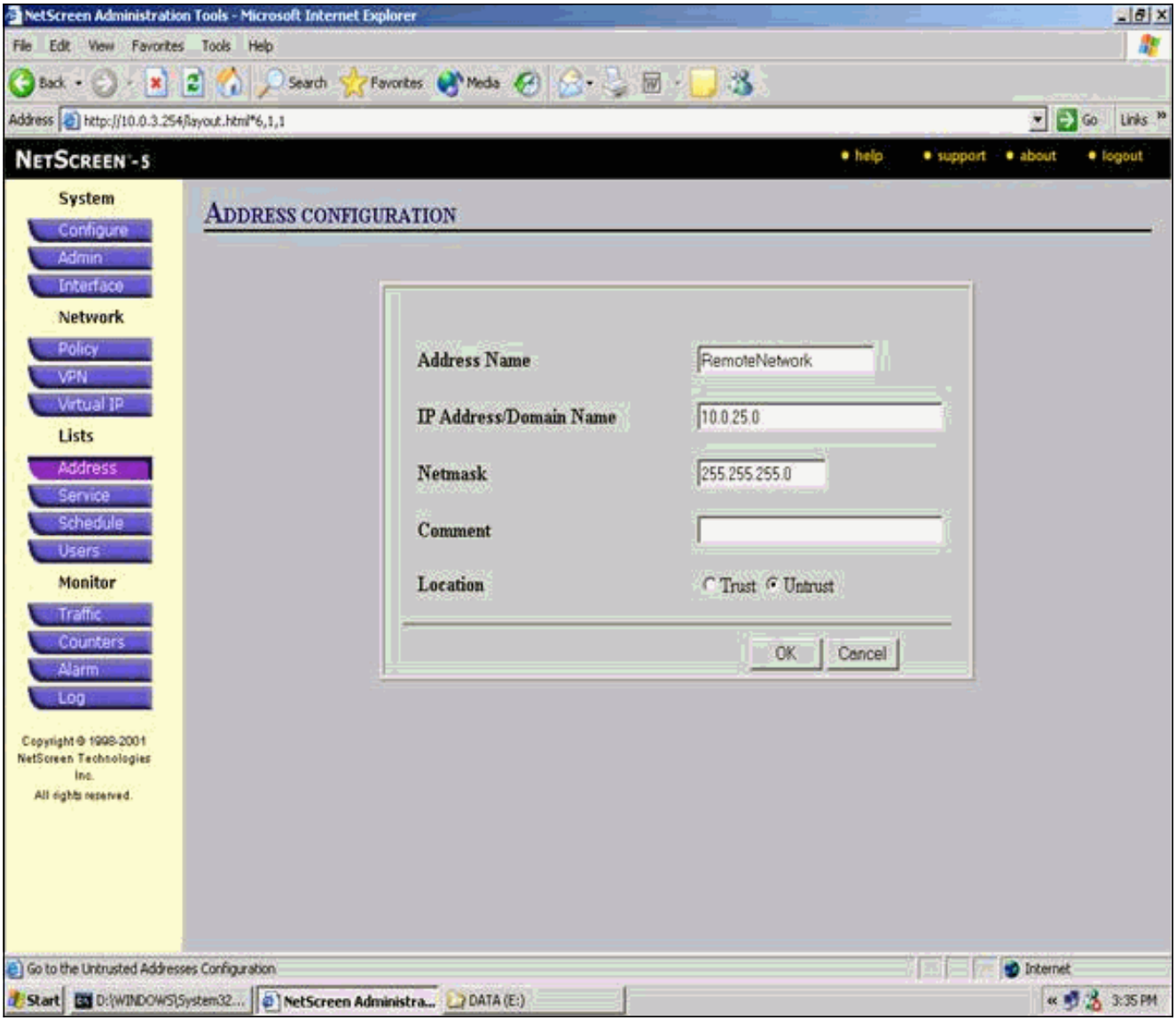
Выполните эти шаги для настройки межсетевого экрана NetScreen.

1. **Списки выборки> Адрес**, перейдите к вкладке Trusted и нажмите **New Address**.
2. Добавьте внутреннюю сеть NetScreen, которая зашифрована на туннеле, и нажмите **OK**.**Примечание:** Гарантируйте, что выбрана опция Trust.Данный пример использует сеть 10.0.3.0 с маской

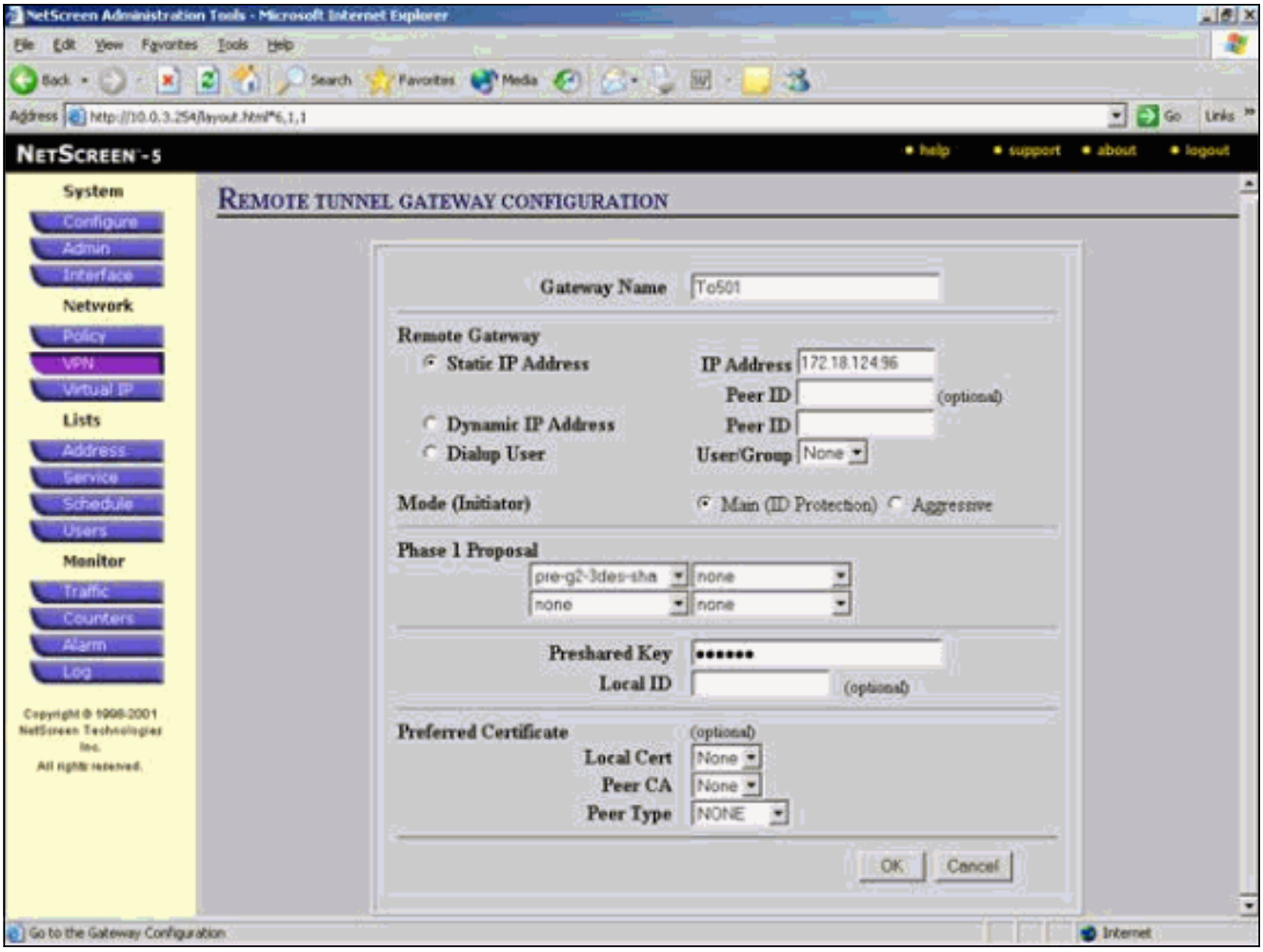
255.255.255.0.



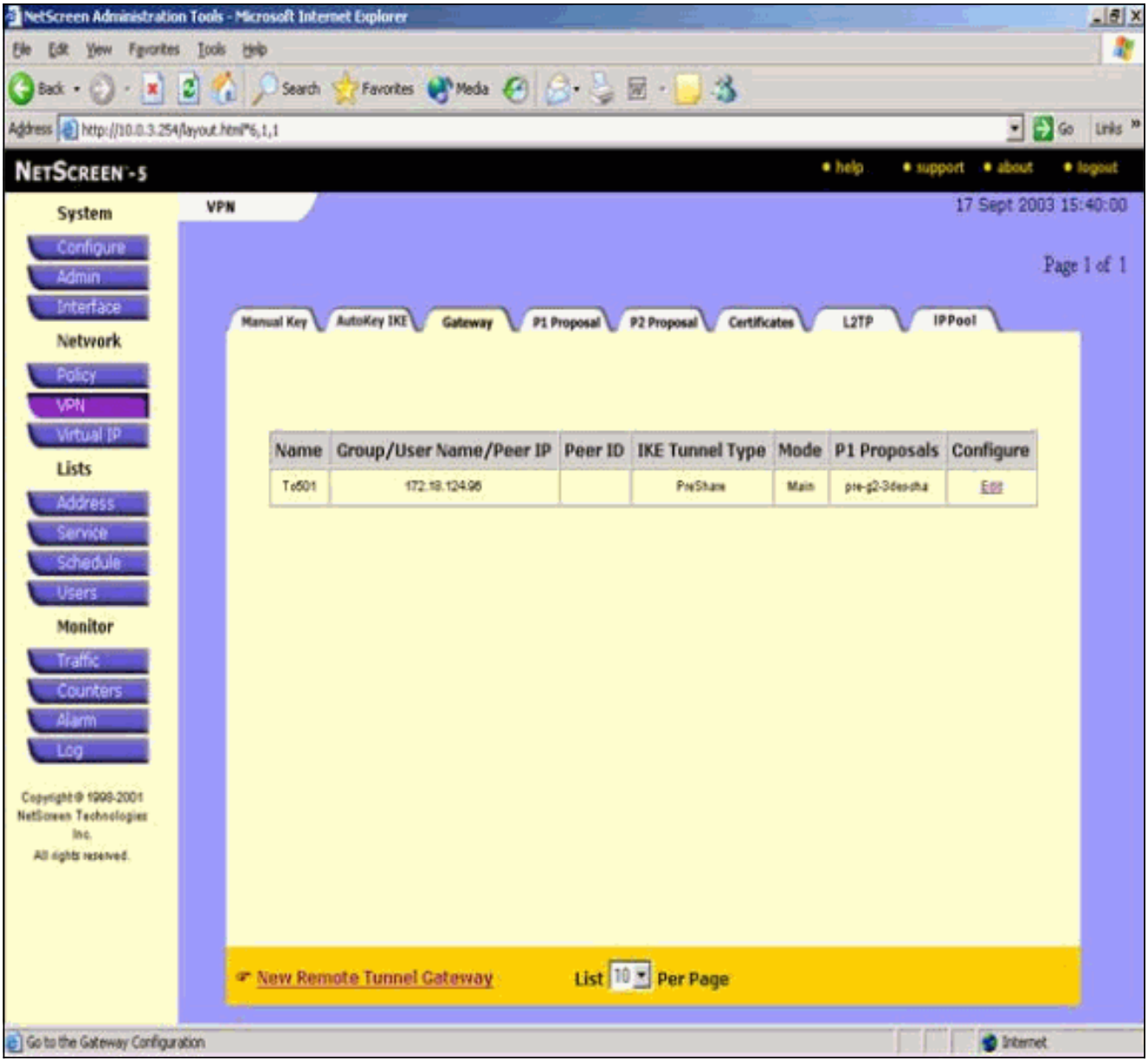
3. **Списки выборки> Адрес**, перейдите к вкладке Untrusted и нажмите **New Address**.
4. Добавьте удаленную сеть, которую использует межсетевой экран NetScreen, когда это шифрует пакеты, и нажмите **OK**.**Примечание:** Не используйте группы адресов при настройке VPN к шлюзу NetScreen non. Совместимость VPN отказывает при использовании групп адресов. Шлюз безопасности NetScreen non не знает, как интерпретировать Proxy Id, созданный NetScreen, когда используется группа адресов.Существует несколько обходных путей для этого:Разделите группы адресов на отдельные записи адресной книги. Задайте индивидуальную политику на на основание записи адресной книги.Настройте Proxy Id, чтобы быть 0.0.0.0/0 на шлюзе NetScreen non (устройство с функциями межсетевого экрана), если это возможно.Данный пример использует сеть 10.0.25.0 с маской 255.255.255.0.



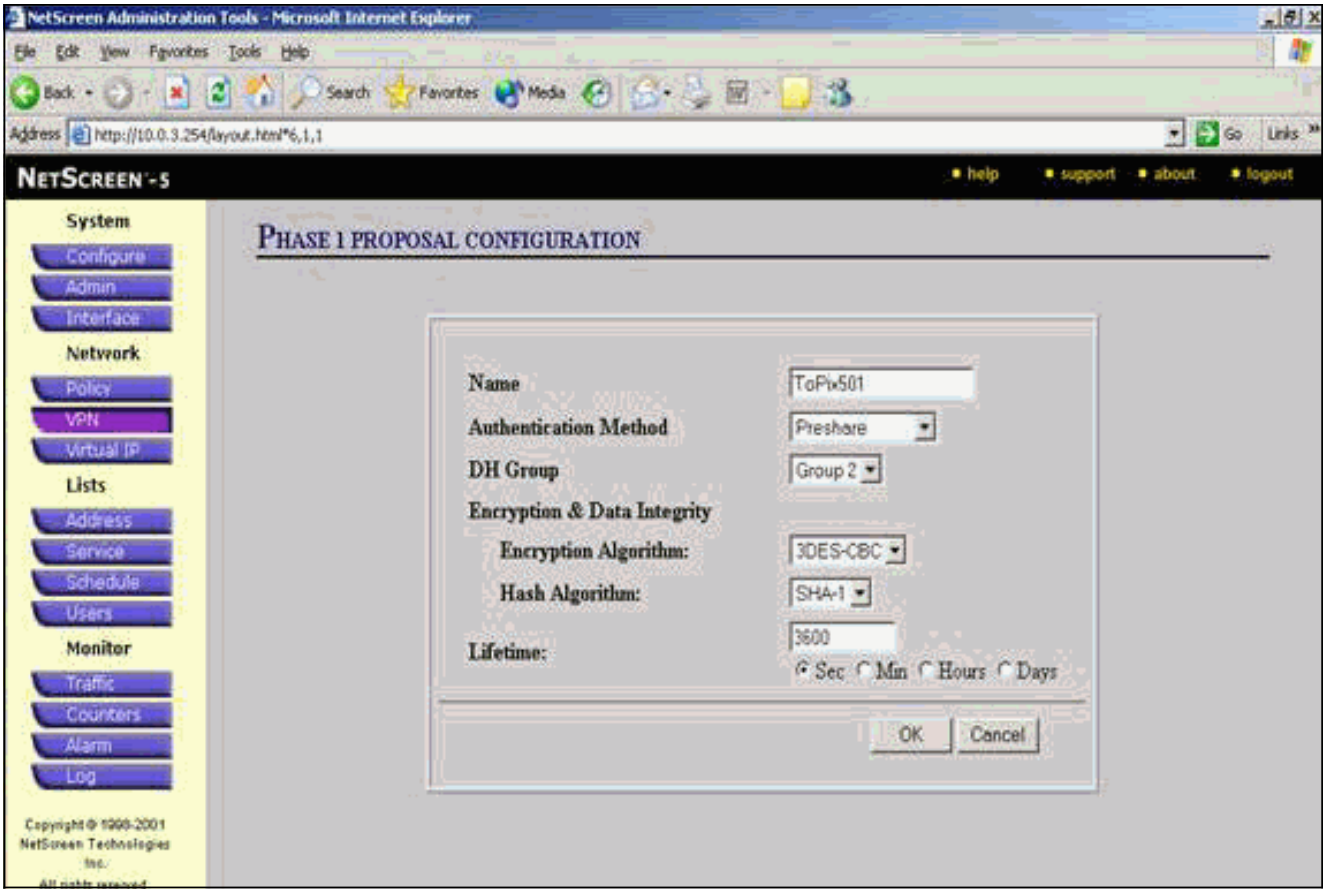
5. Выберите **Network> VPN**, перейдите к вкладке Gateway и нажмите **New Remote Tunnel Gateway** для настройки Шлюза VPN (Фаза 1 и политика IPsec Фазы 2).
6. Используйте IP-адрес внешнего интерфейса PIX, чтобы завершить туннель и настроить параметры IKE Фазы 1 для привязки. **Закончив все действия, нажмите кнопку OK.**Данный пример использует эти поля и значения.**Название шлюза:** To501**Статический IP-адрес:** 172.18.124.96**Режим:** Основной (идентификационная защита)**Pre-shared-key *:** "testme"**Предложение по фазе 1:** pre-g2-3des-sha



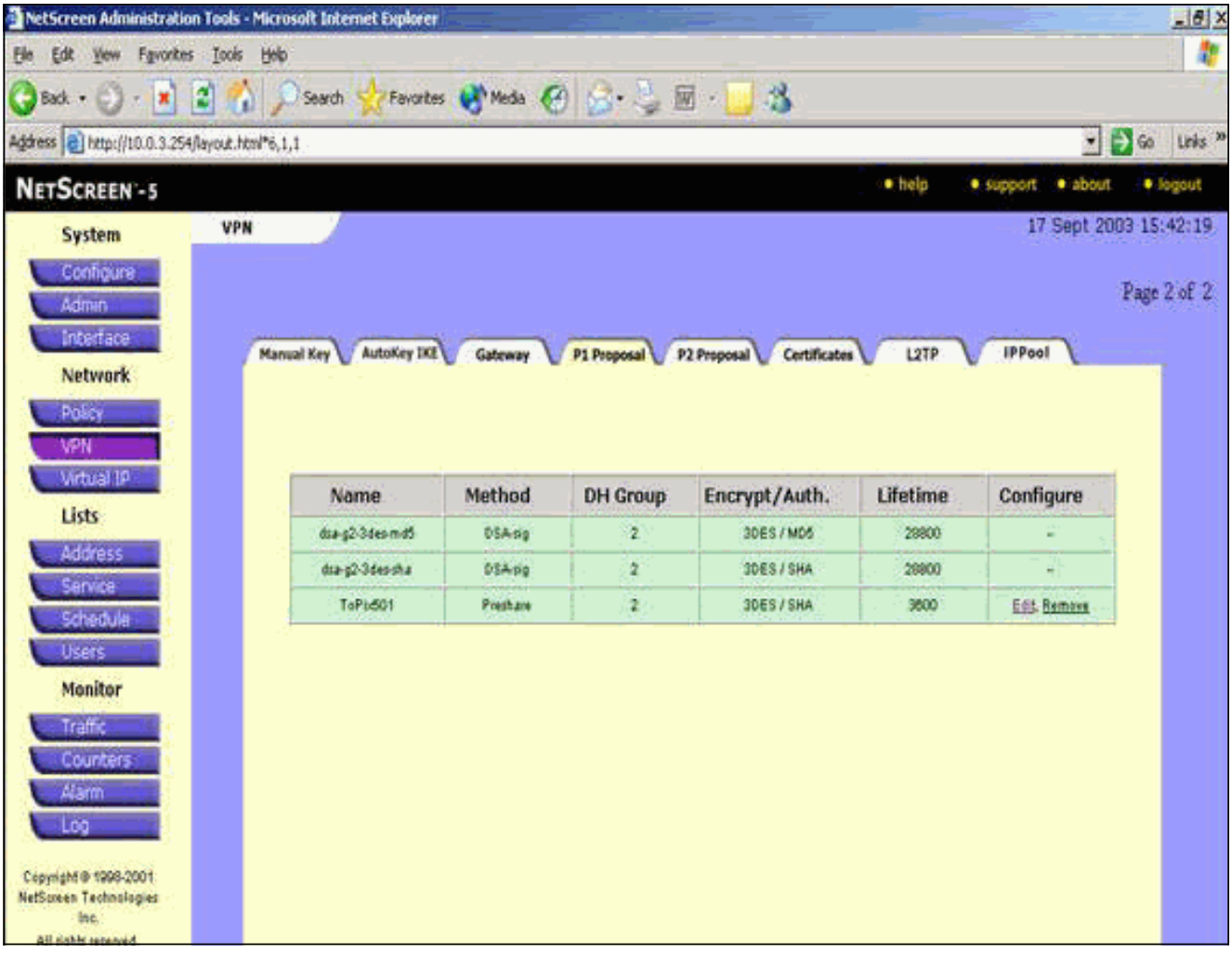
Когда удаленный туннельный шлюз успешно создан, экран, подобный этому, появляется.



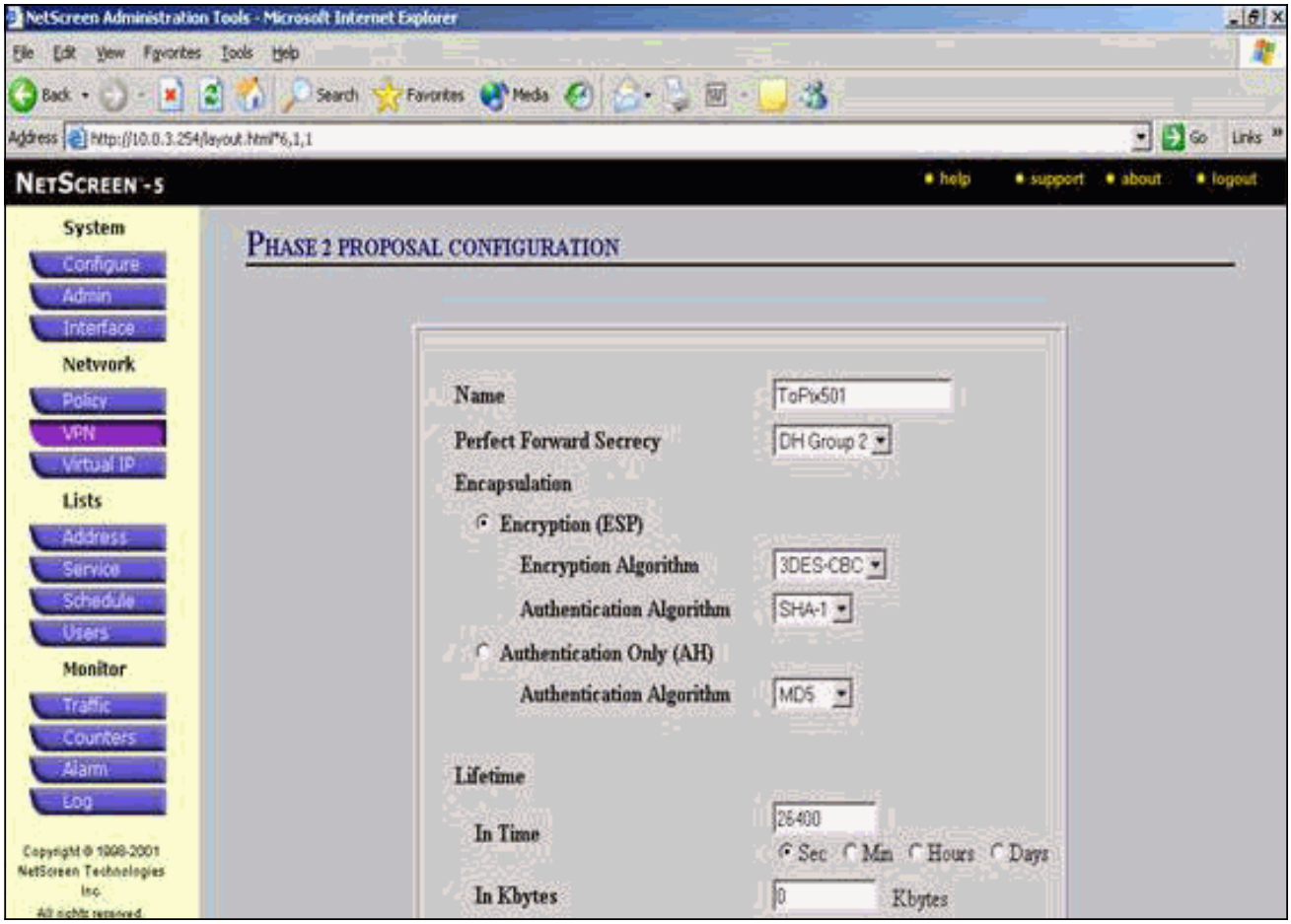
7. Перейдите к вкладке P1 Proposal и нажмите **New Phase 1 Proposal** для настройки Предложения 1.
8. Введите сведения о конфигурации для Предложения по Фазе 1 и нажмите **OK**.Данный пример использует эти поля и оценивает для обмена Фазы 1.**Name:** ToPix501**Authentication pre-shareDH Group:** Group 2**Шифрование:** CBC 3DES**Хэш:** SHA-1**Срок действия:** 3600
сек.



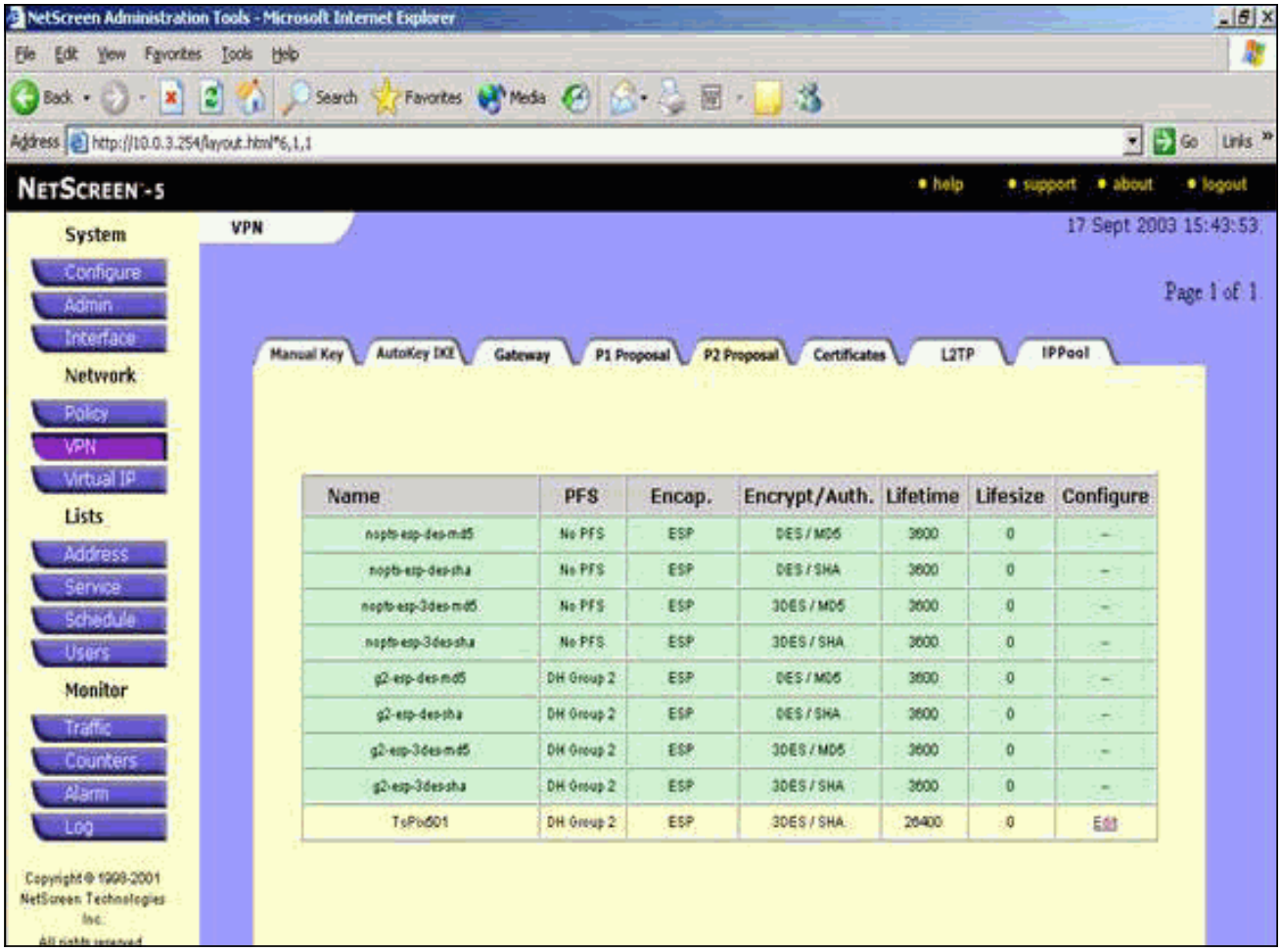
Когда Фаза 1 успешно добавлена к конфигурации NetScreen, экран, подобный данному примеру,
появляется.



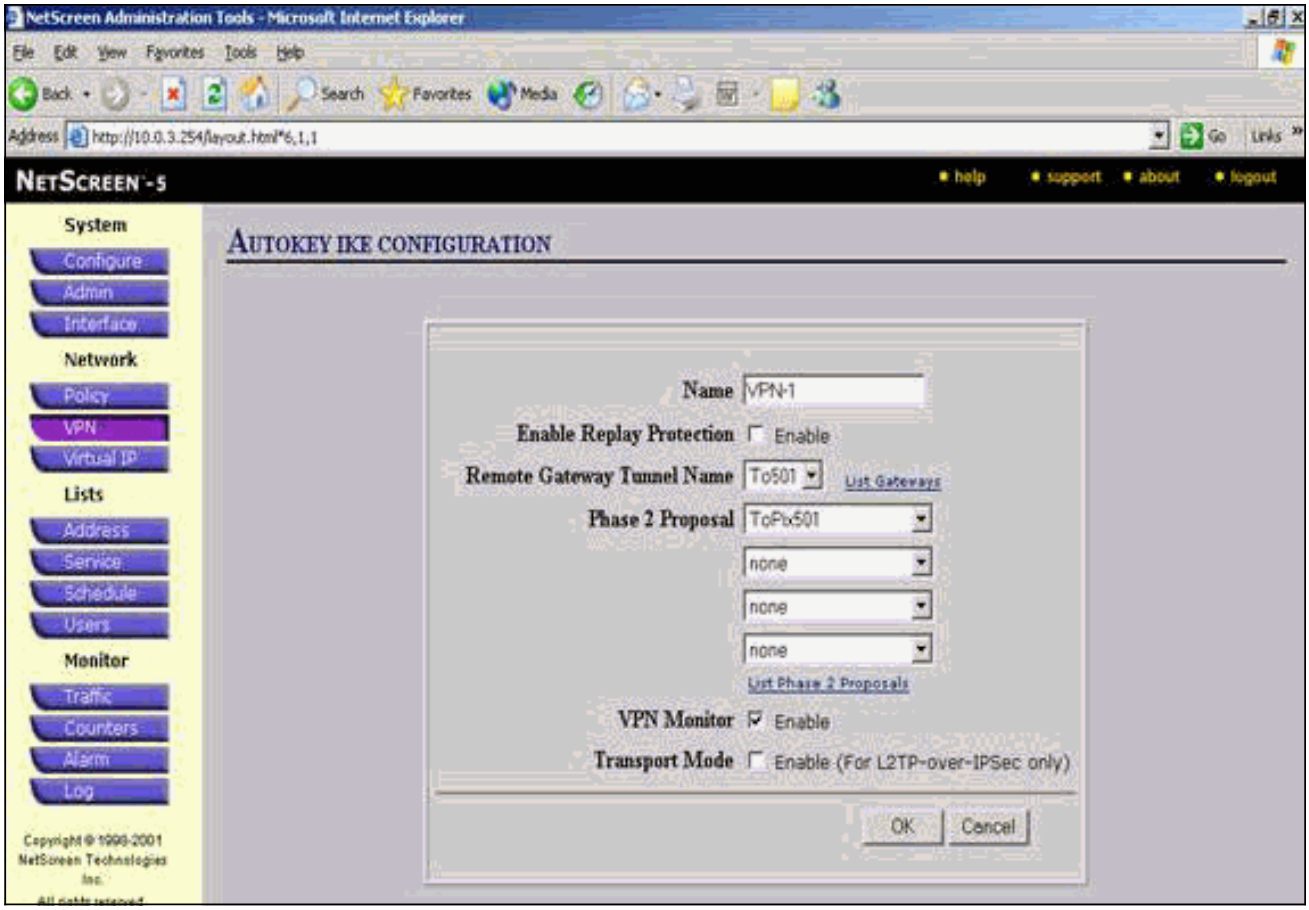
9. Перейдите к вкладке P2 Proposal и нажмите **New Phase 2 Proposal** для настройки Фазы 2.
10. Введите сведения о конфигурации для Предложения по Фазе 2 и нажмите **OK**.Данный пример использует эти поля и оценивает для обмена Фазы 2.**Name:** ToPix501**Непосредственный контроль секретности (Perfect Forward Secrecy):** DH-2 (1024 бита)**Алгоритм шифрования:** CBC 3DES**Алгоритм аутентификации:** SHA-1**Срок действия:** 26400
сек.



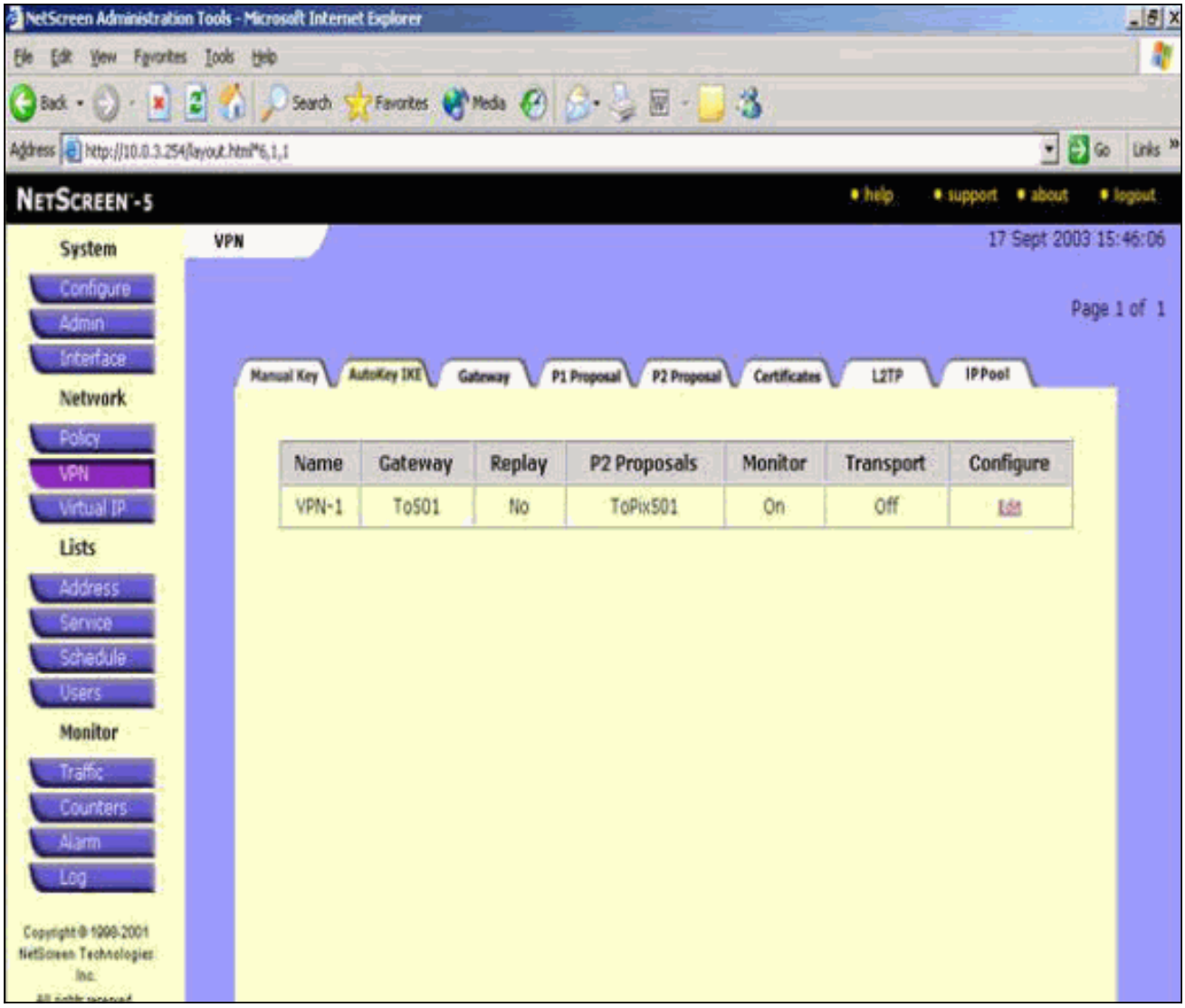
Когда Фаза 2 успешно добавлена к конфигурации NetScreen, экран, подобный данному примеру,
появляется.



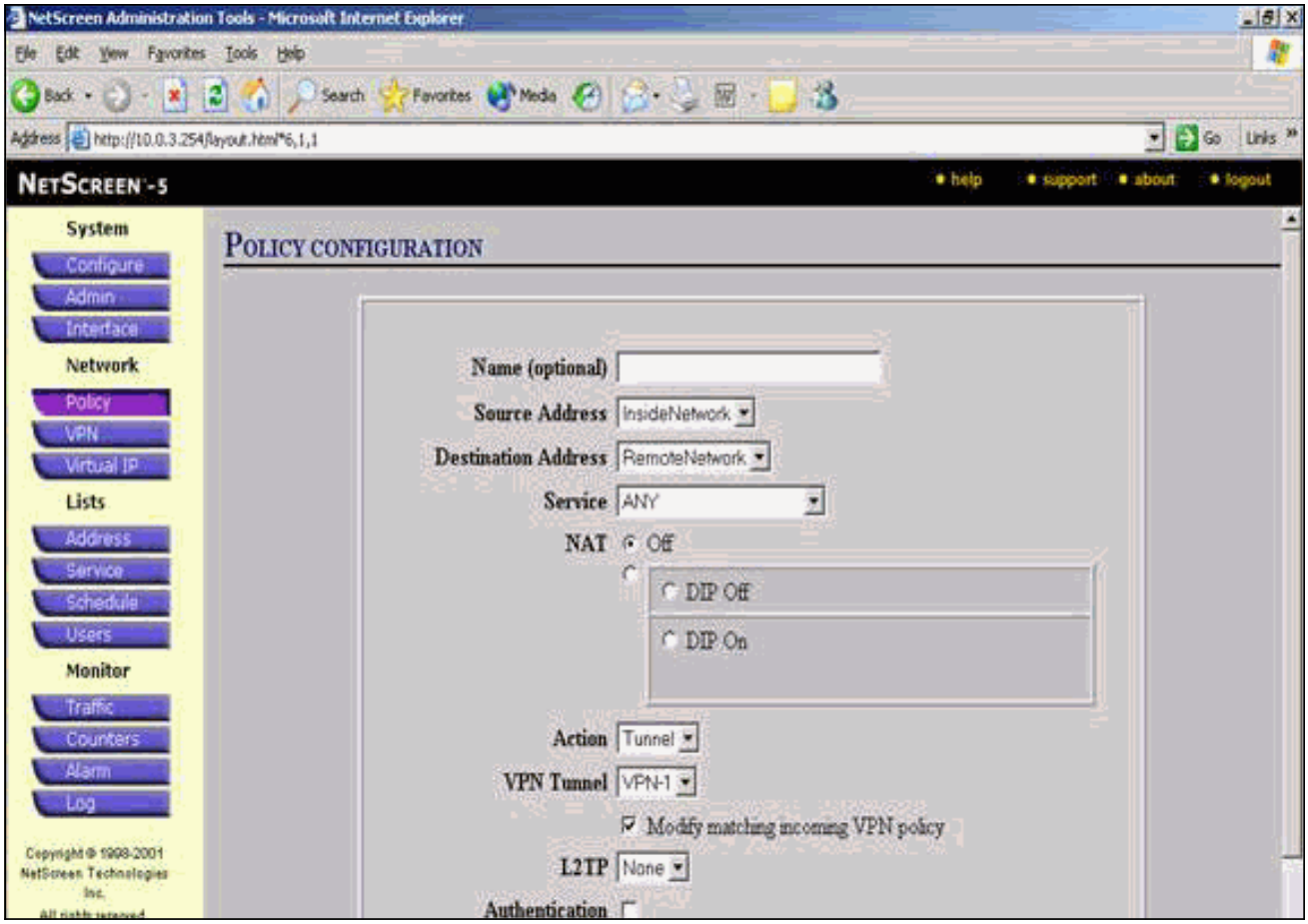
11. Выберите вкладку **AutoKey IKE**, и затем нажмите **New AutoKey IKE Entry**, чтобы создать и настроить AutoKeys IKE.
12. Введите сведения о конфигурации для IKE AutoKey, и затем нажмите **OK**.Данный пример использует эти поля и оценивает для IKE AutoKey.**Name:** VPN-1**Имя туннеля удаленного шлюза:** To501(Это было создано на предыдущем этапе на вкладке Gateway.)**Предложение по фазе 2:** ToPix501(Это было создано на предыдущем этапе на вкладке P2 Proposal.)**Монитор VPN:** включить(Это позволяет устройству NetScreen поставить капканы Простоя протокол управления сетью [SNMP] для мониторинга условия Монитора
VPN.)



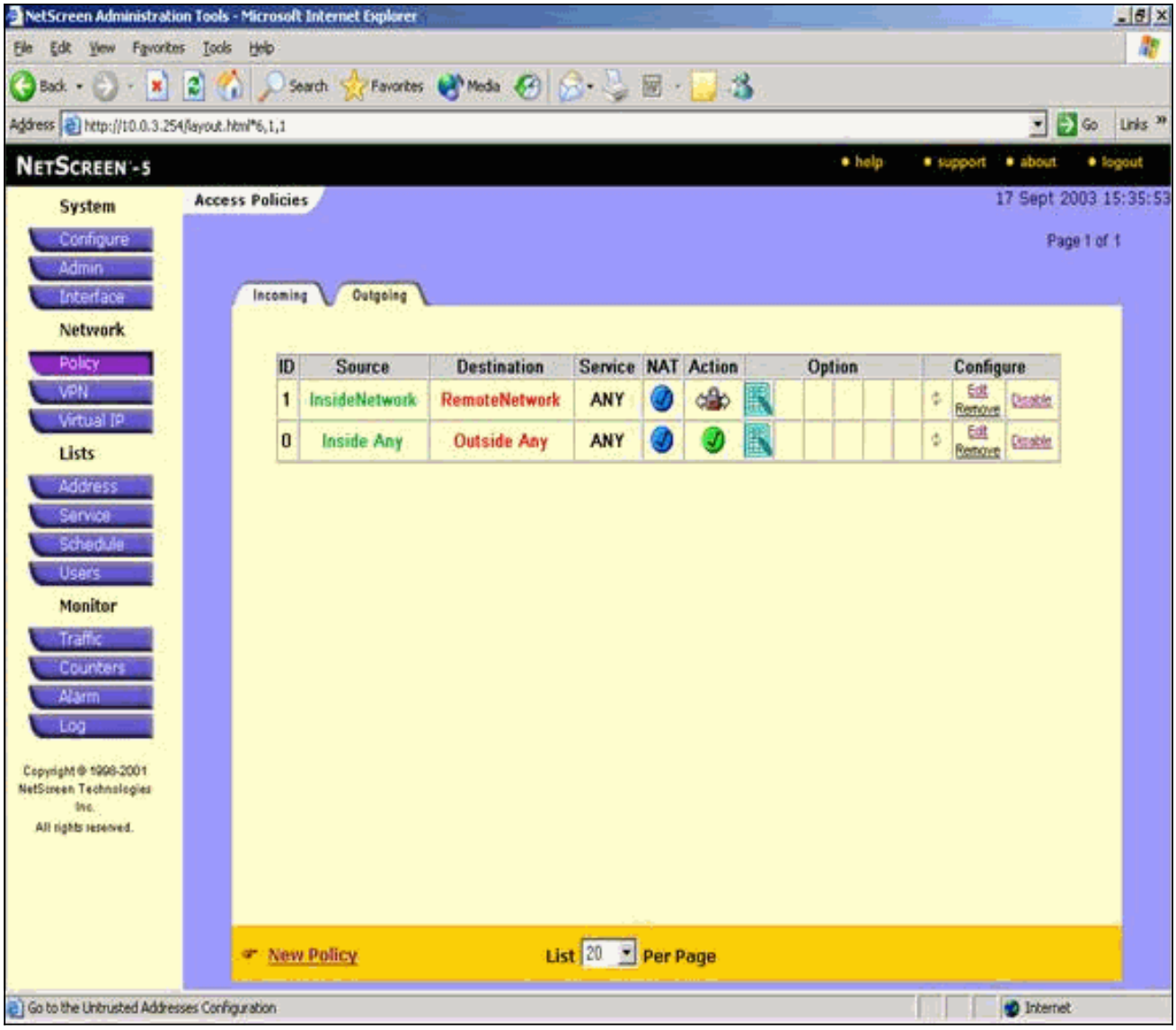
Когда правило VPN-1 успешно настроено, экран, подобный данному примеру, появляется.



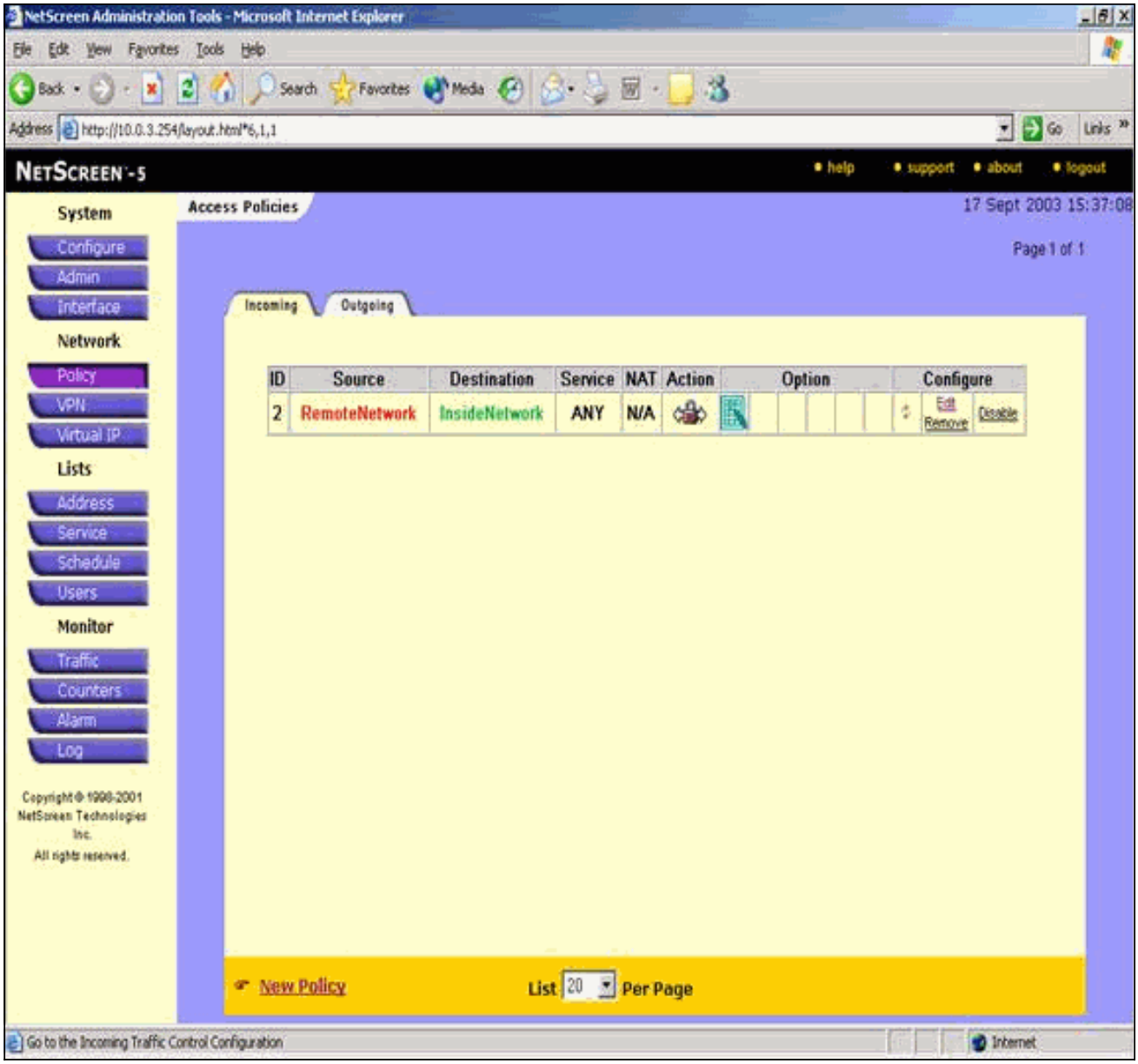
13. Выберите **Network> Policy**, перейдите к вкладке Outgoing и нажмите **New Policy** для настройки правил, которые позволяют шифрование Трафика IPSec.
14. Введите сведения о конфигурации для политики и нажмите **OK**.Данный пример использует эти поля и оценивает для политики. Поле имени является дополнительным и не используется в данном примере.**Исходный адрес:** Внутренняя сеть(Это было ранее определено на вкладке Trusted.)**Адрес получателя:** RemoteNetwork(Это было ранее определено под вкладкой Untrusted.)**Сервис:** любой**Действие:** Туннель**VPN-туннель:** VPN-1(Это было ранее определено как VPN-туннель на вкладке AutoKey IKE.)**Модифицируйте соответствие входящая политика VPN:** Проверенный(Эта опция автоматически создает входящее правило, которое совпадает с трафиком VPN внешней
сети.)



15. Когда политика добавлена, гарантируйте, что исходящее правило VPN является первым в списке политики. (Правило, которое создано автоматически для входящего трафика, находится на вкладке Incoming.)Выполните эти шаги, если необходимо изменить заказ политики:Нажмите вкладку Outgoing.Нажмите кольцевые стрелки в столбце Configure для отображения окна Move Policy Micro.Измените заказ политики так, чтобы политика VPN была выше идентификатора политики 0 (так, чтобы политика VPN была наверху
списка).



Перейдите к вкладке Incoming для просмотра правила для входящего трафика.



Проверка

Этот раздел предоставляет сведения, можно использовать, чтобы подтвердить, что должным образом работает конфигурация.

Команды проверки

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **эхо-запрос**? Базовое сетевое подключение диагнозов.
- **команда show crypto ipsec sa – отображает связи безопасности, соответствующие второму этапу.**
- **команда show crypto isakmp sa вЂ отображает сопоставления безопасности, соответствующие первому этапу.**

Выходные данные проверки

Пример выходных данных от **эхо-запроса** и **команд показа** показывают здесь.

Этот эхо-запрос инициируется от хоста позади межсетевого экрана NetScreen.

```
C:\>ping 10.0.25.1 -tRequest timed out.Request timed out.Reply from 10.0.25.1: bytes=32
time<105ms TTL=128Reply from 10.0.25.1: bytes=32 time<114ms TTL=128Reply from 10.0.25.1:
bytes=32 time<106ms TTL=128Reply from 10.0.25.1: bytes=32 time<121ms TTL=128Reply from
10.0.25.1: bytes=32 time<110ms TTL=128Reply from 10.0.25.1: bytes=32 time<116ms TTL=128Reply
from 10.0.25.1: bytes=32 time<109ms TTL=128Reply from 10.0.25.1: bytes=32 time<110ms
TTL=128Reply from 10.0.25.1: bytes=32 time<118ms TTL=128
```

Выходные данные от **команды show crypto ipsec sa** показывают здесь.

```
pixfirewall(config)#show crypto ipsec sainterface: outside Crypto map tag: mymap, local addr.
172.18.124.96 local ident (addr/mask/prot/port): (10.0.25.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.0.3.0/255.255.255.0/0/0) current_peer: 172.18.173.85:500 PERMIT,
flags={origin_is_acl,} #pkts encaps: 11, #pkts encrypt: 11, #pkts digest 11 #pkts decaps: 11,
#pkts decrypt: 13, #pkts verify 13 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0, #send errors 0, #recv errors
1 local crypto endpt.: 172.18.124.96, remote crypto endpt.: 172.18.173.85 path mtu 1500, ipsec
overhead 56, media mtu 1500 current outbound spi: f0f376eb inbound esp sas: spi:
0x1225ce5c(304467548) transform: esp-3des esp-sha-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 3, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4607974/24637) IV
size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas:
spi: 0xf0f376eb(4042487531) transform: esp-3des esp-sha-hmac , in use settings ={Tunnel, } slot:
0, conn id: 4, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4607999/24628) IV
size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:
```

Выходные данные от **команды show crypto isakmp sa** показывают здесь.

```
pixfirewall(config)#show crypto isakmp saTotal : 1Embryonic : 0 dst src state pending created
172.18.124.96 172.18.173.85 QM_IDLE 0 1
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

- **debug crypto engine?** Отображает сообщения о ядрах шифрования.
- **debug crypto ipsec – Отображает сведения о событиях IPSec.**
- **debug crypto isakmp – отображает сообщения о событиях IKE.**

Пример результата отладки

Пример отладочных выходных данных от Межсетевого экрана PIX показывают здесь.

```
debug crypto enginedebug crypto ipsecdebug crypto
isakmpcrypto_isakmp_process_block:src:172.18.173.85,   dest:172.18.124.96 spt:500 dpt:500OAK_MM
exchangeISAKMP (0): processing SA payload. message ID = 0ISAKMP (0): Checking ISAKMP transform 1
against priority 10 policyISAKMP:      encryption 3DES-CBCISAKMP:      hash SHAISAKMP:
default group 2ISAKMP:      auth pre-shareISAKMP:      life type in secondsISAKMP:      life
duration (basic) of 28800ISAKMP (0): atts are acceptable. Next payload is 0ISAKMP (0):
processing vendor id payloadISAKMP (0): processing vendor id payload ISAKMP (0): SA is doing
pre-shared key authentication    using id type ID_IPV4_ADDRreturn status is
```

```
IKMP_NO_ERRORcrypto_isakmp_process_block:src:172.18.173.85,    dest:172.18.124.96 spt:500
dpt:500OAK_MM exchangeISAKMP (0): processing KE payload. message ID = 0ISAKMP (0): processing
NONCE payload. message ID = 0return status is
IKMP_NO_ERRORcrypto_isakmp_process_block:src:172.18.173.85,    dest:172.18.124.96 spt:500
dpt:500OAK_MM exchangeISAKMP (0): processing ID payload. message ID = 0ISAKMP (0): processing
HASH payload. message ID = 0ISAKMP (0): SA has been authenticatedISAKMP (0): ID payload
next-payload : 8        type         : 1        protocol     : 17        port         : 500
length       : 8ISAKMP (0): Total payload length: 12return status is IKMP_NO_ERRORISAKMP (0):
sending INITIAL_CONTACT notifyISAKMP (0): sending NOTIFY message 24578 protocol 1VPN Peer:
ISAKMP: Added new peer: ip:172.18.173.85/500    Total VPN Peers:1VPN Peer: ISAKMP: Peer
ip:172.18.173.85/500 Ref cnt    incremented to:1    Total VPN
Peers:1crypto_isakmp_process_block:src:172.18.173.85,    dest:172.18.124.96 spt:500
dpt:500ISAKMP (0): processing DELETE payload. message ID = 534186807,    spi size =
4IPSEC(key_engine): got a queue event...IPSEC(key_engine_delete_sas): rec'd delete notify from
ISAKMPIPSEC(key_engine_delete_sas):    delete all SAs shared with 172.18.173.85return status is
IKMP_NO_ERR_NO_TRANScrypto_isakmp_process_block:src:172.18.173.85,    dest:172.18.124.96 spt:500
dpt:500OAK_QM exchangeoakley_process_quick_mode: OAK_QM_IDLEISAKMP (0): processing SA payload.
message ID = 4150037097ISAKMP : Checking IPSec proposal 1ISAKMP: transform 1, ESP_3DESISAKMP:
attributes in transform:ISAKMP:      SA life type in secondsISAKMP:      SA life duration (VPI)
of 0x0 0x0 0x67 0x20ISAKMP:      encaps is 1ISAKMP:      authenticator is HMAC-SHAISAKMP:
group is 2ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part #1,
(key eng. msg.) dest= 172.18.124.96, src= 172.18.173.85,    dest_proxy=
10.0.25.0/255.255.255.0/0/0 (type=4),    src_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-sha-hmac ,    lifedur= 0s and 0kb,    spi= 0x0(0),
conn_id= 0, keysize= 0, flags= 0x24ISAKMP (0): processing NONCE payload. message ID =
4150037097ISAKMP (0): processing KE payload. message ID = 4150037097ISAKMP (0): processing ID
payload. message ID = 4150037097ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.0.3.0/255.255.255.0
prot 0 port 0ISAKMP (0): processing ID payload. message ID = 4150037097ISAKMP (0):
ID_IPV4_ADDR_SUBNET dst 10.0.25.0/255.255.255.0    prot 0 port 0IPSEC(key_engine): got a queue
event...IPSEC(spi_response): getting spi 0x1225ce5c(304467548) for SA        from
172.18.173.85 to   172.18.124.96 for prot 3return status is
IKMP_NO_ERRORcrypto_isakmp_process_block:src:172.18.173.85,    dest:172.18.124.96 spt:500
dpt:500OAK_QM exchangeoakley_process_quick_mode:OAK_QM_AUTH_AWAITmap_alloc_entry: allocating
entry 3map_alloc_entry: allocating entry 4ISAKMP (0): Creating IPSec SAs        inbound SA from
172.18.173.85 to 172.18.124.96          (proxy 10.0.3.0 to 10.0.25.0)        has spi 304467548
and conn_id 3 and flags 25        lifetime of 26400 seconds        outbound SA from
172.18.124.96 to 172.18.173.85          (proxy 10.0.25.0 to 10.0.3.0)        has spi 4042487531
and conn_id 4 and flags 25        lifetime of 26400 secondsIPSEC(key_engine): got a queue
event...IPSEC(initialize_sas): ,  (key eng. msg.) dest= 172.18.124.96, src= 172.18.173.85,
dest_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4),    src_proxy= 10.0.3.0/255.255.255.0/0/0
(type=4),    protocol= ESP, transform= esp-3des esp-sha-hmac ,    lifedur= 26400s and 0kb,
spi= 0x1225ce5c(304467548), conn_id= 3,        keysize= 0, flags= 0x25IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.96, dest= 172.18.173.85,    src_proxy=
10.0.25.0/255.255.255.0/0/0 (type=4),    dest_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-3des esp-sha-hmac ,    lifedur= 26400s and 0kb,    spi=
0xf0f376eb(4042487531), conn_id= 4, keysize= 0, flags= 0x25VPN Peer: IPSEC: Peer
ip:172.18.173.85/500 Ref cnt    incremented to:2 Total VPN Peers:1VPN Peer: IPSEC: Peer
ip:172.18.173.85/500 Ref cnt    incremented to:3 Total VPN Peers:1return status is IKMP_NO_ERROR
```

Дополнительные сведения

- Согласование IPsec/Протоколы IKE
- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация