Configurando o túnel de LAN para LAN de IPSec entre o Cisco PIX Firewall e um firewall de NetScreen

Índice

Introdução

Este documento descreve o procedimento necessário para criar um túnel IPSec de LAN para LAN entre um Cisco PIX Firewall e um NetScreen Firewall com o software mais recente. Há uma rede privada atrás de cada dispositivo que se comunica com o outro firewall através do túnel IPsec.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O firewall de NetScreen é configurado com os endereços IP de Um ou Mais Servidores Cisco ICM NT nas relações da confiança/untrust.
- A Conectividade é estabelecida ao Internet.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 6.3(1) do software de firewall de PIX
- A revisão a mais atrasada do NetScreen

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento utiliza as seguintes configurações:

- Firewall de PIX
- Firewall de NetScreen

Configurar o PIX Firewall

Firewall de PIX

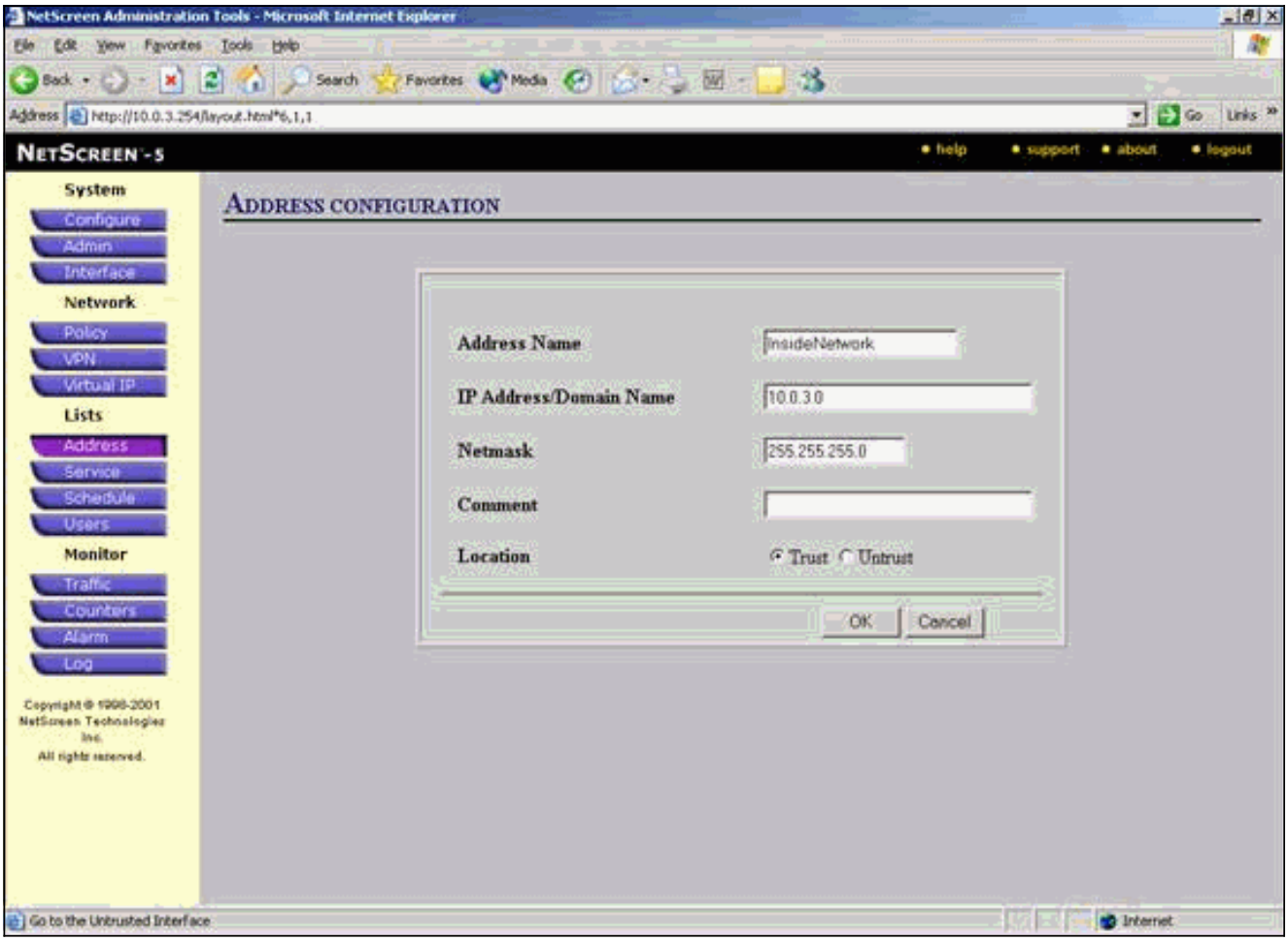
`PIX Version 6.3(1)`
`interface ethernet0 10baset`
`interface ethernet1 100full`
`nameif ethernet0 outside security0`
`nameif ethernet1 inside security100`

```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
!--- 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 10.0.3.0 255.255.255.0 pager
lines 24 logging on logging timestamp logging buffered
debugging icmp permit any inside mtu outside 1500 mtu
inside 1500 !--- IP addresses on the interfaces. ip
address outside 172.18.124.96 255.255.255.0 ip address
inside 10.0.25.254 255.255.255.0 ip audit info action
alarm ip audit attack action alarm pdm logging
informational 100 pdm history enable arp timeout 14400
global (outside) 1 interface !--- Bypass of NAT for
IPsec interesting inside network traffic. nat (inside) 0
access-list nonat nat (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 1 timeout xlate 0:05:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h225 1:00:00 timeout h323 0:05:00 mgcp 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server LOCAL protocol local http
10.0.0.0 255.0.0.0 inside no snmp-server location no
snmp-server contact snmp-server community public no
snmp-server enable traps floodguard 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-hmac crypto map mymap 10
ipsec-isakmp crypto map mymap 10 match address nonat
crypto map mymap 10 set pfs group2 crypto map mymap 10
set peer 172.18.173.85 crypto map mymap 10 set
transform-set mytrans crypto 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 255.255.255.255
isakmp identity address isakmp policy 10 authentication
pre-share isakmp policy 10 encryption 3des isakmp policy
10 hash sha isakmp policy 10 group 2 isakmp policy 10
lifetime 86400 telnet timeout 5 ssh timeout 5 console
timeout 0 dhcpd lease 3600 dhcpd ping_timeout 750
terminal width 80
```

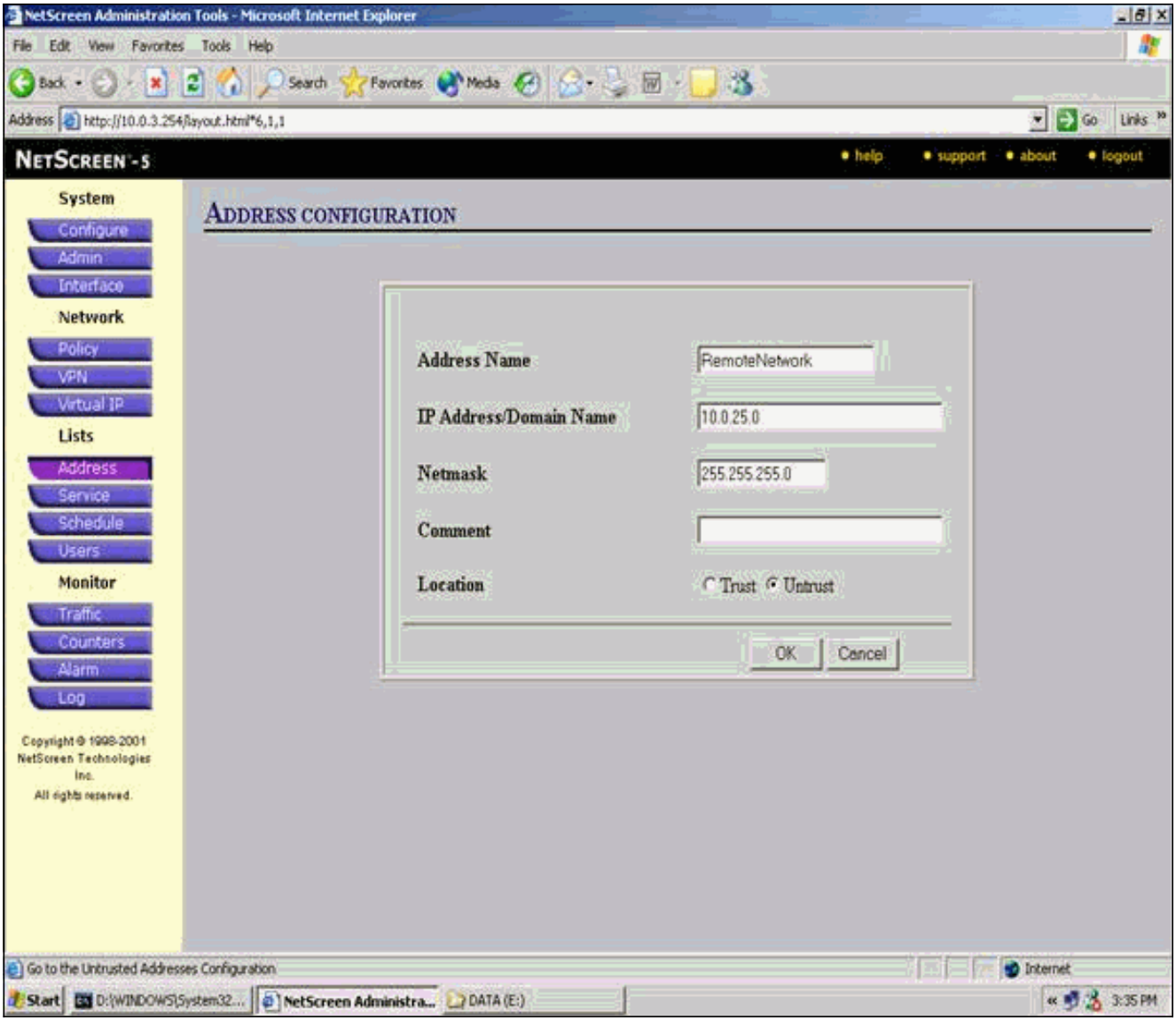
Configurar o firewall de NetScreen

Termine estas etapas a fim configurar o firewall de NetScreen.

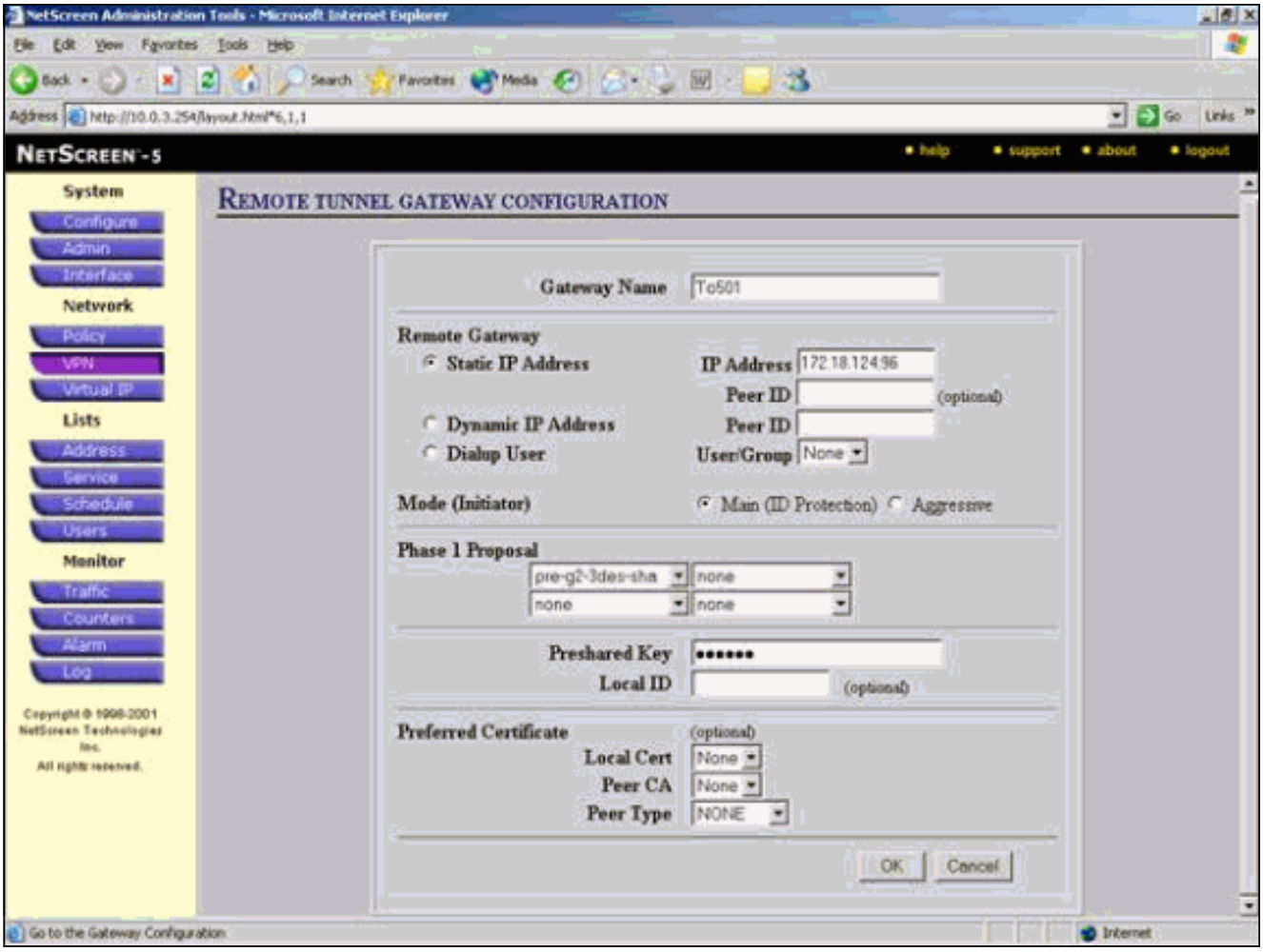
1. Selecione o **Listas > Endereço**, vá à aba confiada, e clique o **endereço novo**.
2. Adicionar a rede interna do NetScreen que é cifrada no túnel e clique a **APROVAÇÃO**.**Nota:** Assegure-se de que a opção da confiança esteja selecionada.Este exemplo usa a rede 10.0.3.0 com uma máscara de 255.255.255.0.



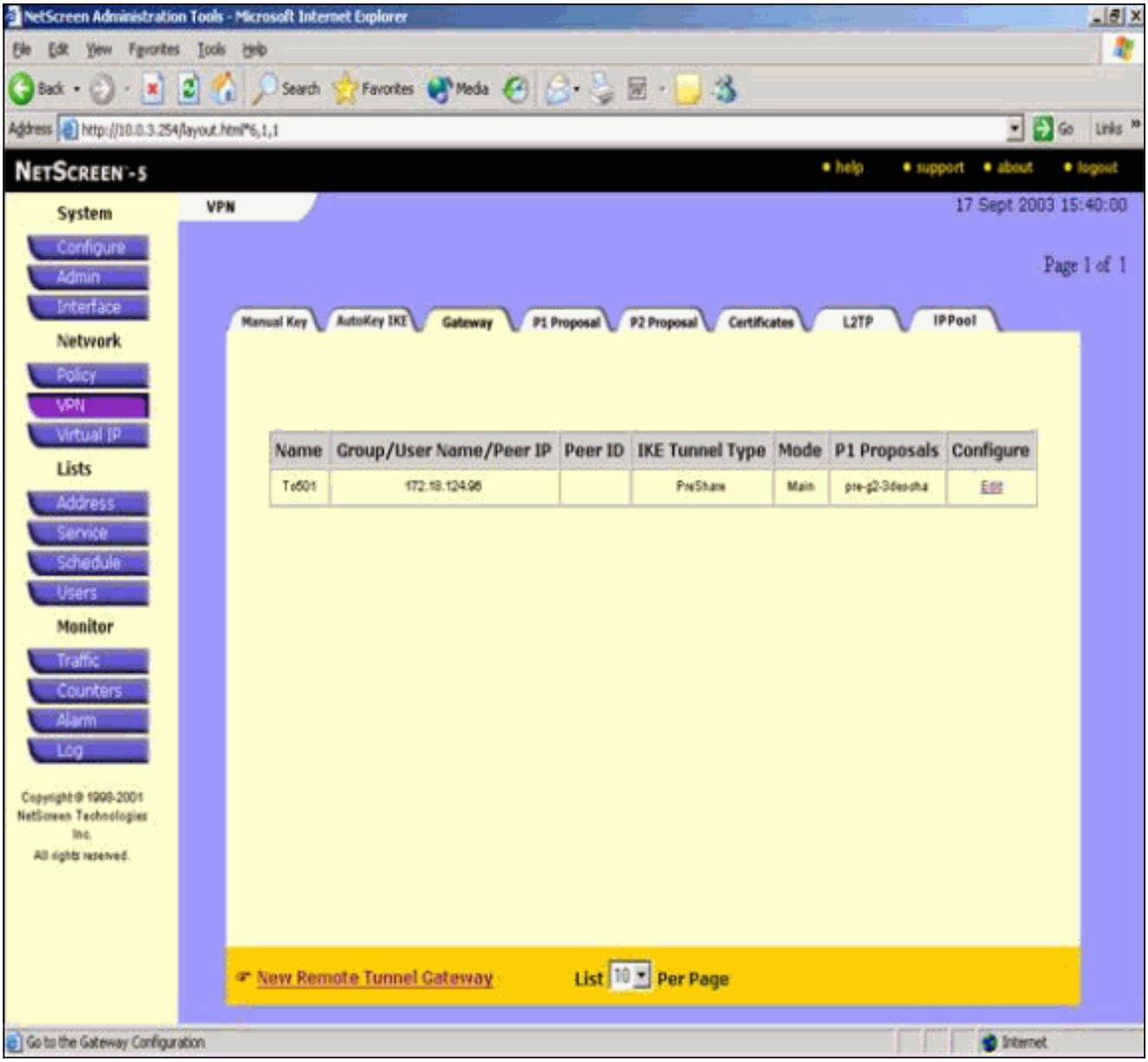
3. Selecione o **Listas > Endereço**, vá à aba não confiável, e clique o **endereço novo**.
4. Adicionar a rede remota que o firewall de NetScreen usa quando cifra pacotes e clica a **APROVAÇÃO**.**Nota:** Não use grupos de endereço quando você configura um VPN não a um gateway do NetScreen. A interoperabilidade de VPN falha se você usa grupos de endereço. Não o gateway de segurança do NetScreen não sabe interpretar o ID de proxy criado pelo NetScreen quando o grupo de endereço é usado.Há uns pares de ações alternativas para este:Separe os grupos de endereço em entradas de agenda telefônica individuais. Especifique políticas individuais na pela base da entrada de agenda telefônica.Configurar o ID de proxy para ser 0.0.0.0/0 não no gateway do NetScreen (dispositivo de firewall) se possível.Este exemplo usa a rede 10.0.25.0 com uma máscara de 255.255.255.0.



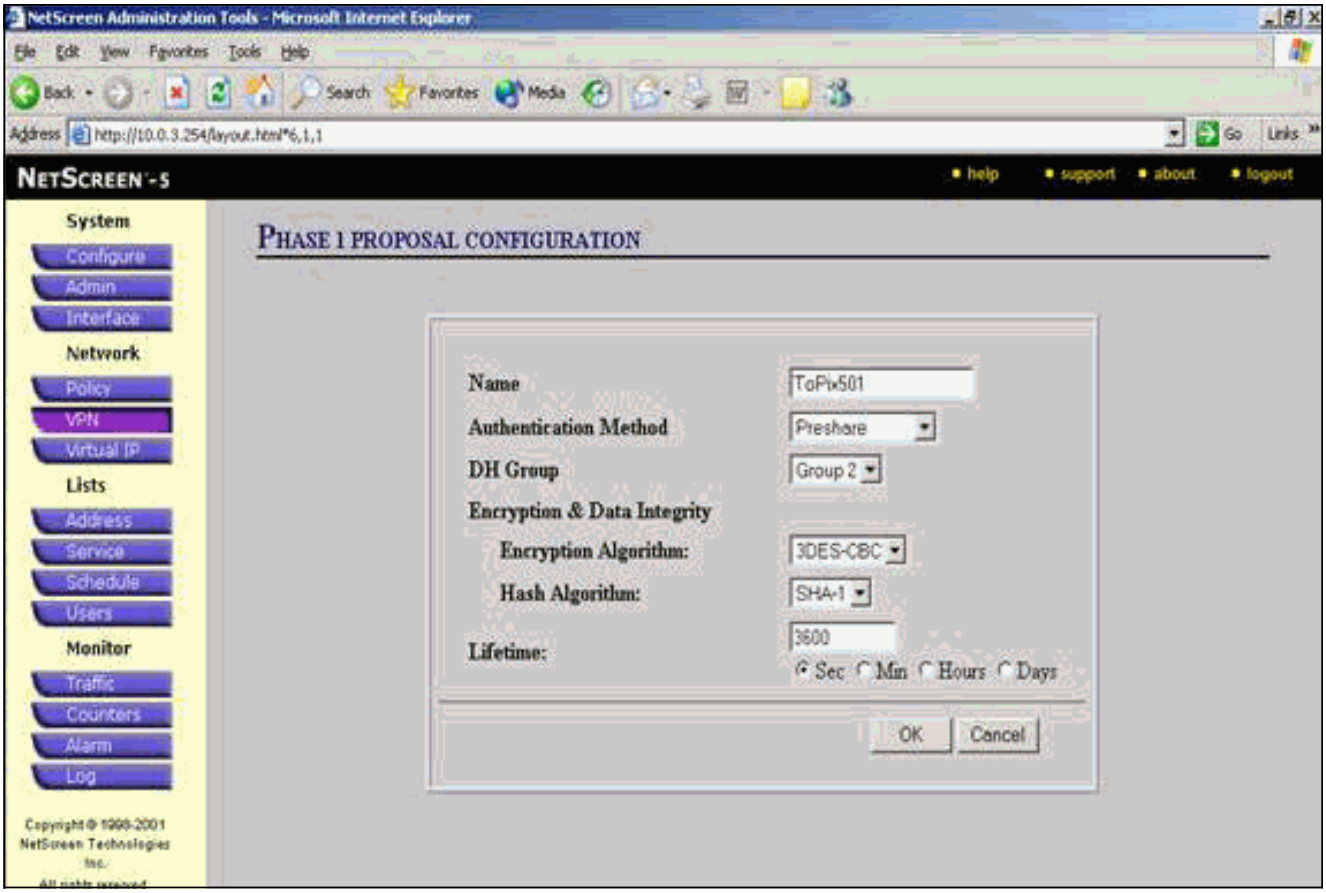
5. Selecione a **rede > o VPN**, vá à aba do gateway, e clique o **gateway remoto novo do túnel** para configurar o gateway de VPN (políticas de IPsec da fase 1 e da fase 2).
6. Use o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface externa do PIX a fim terminar o túnel, e configurar as opções IKE da fase 1 ligar. Clique a **APROVAÇÃO** quando você é terminado.Este exemplo usa estes campos e valores.**Nome do gateway:** To501**Endereço IP estático:** 172.18.124.96**Modo:** Cano principal (Proteção de ID)**Chave Preshared:** “testme”**Proposta da fase 1:** pre-g2-3des-sha



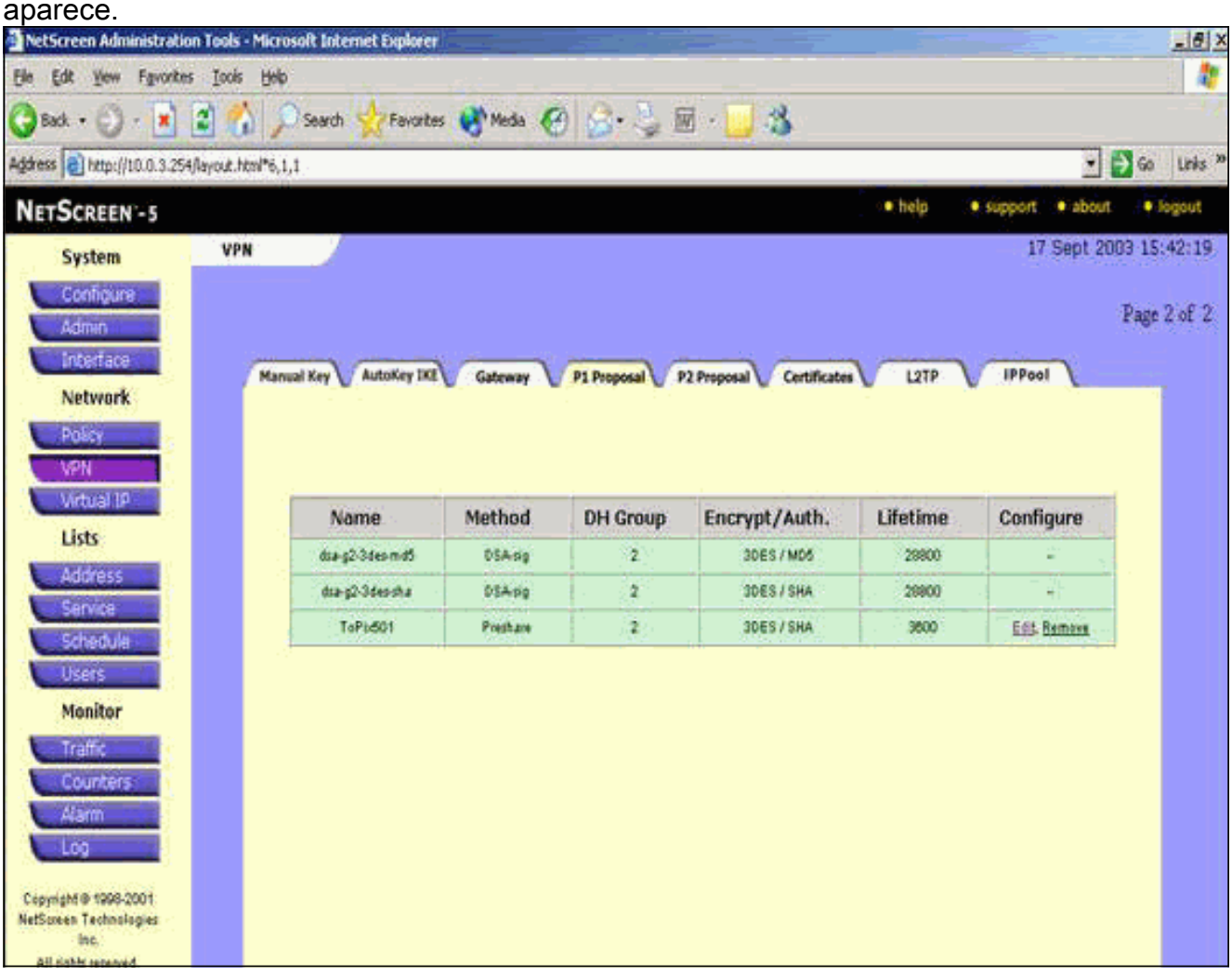
Quando o gateway remoto do túnel é criado com sucesso, uma tela similar a esta aparece.



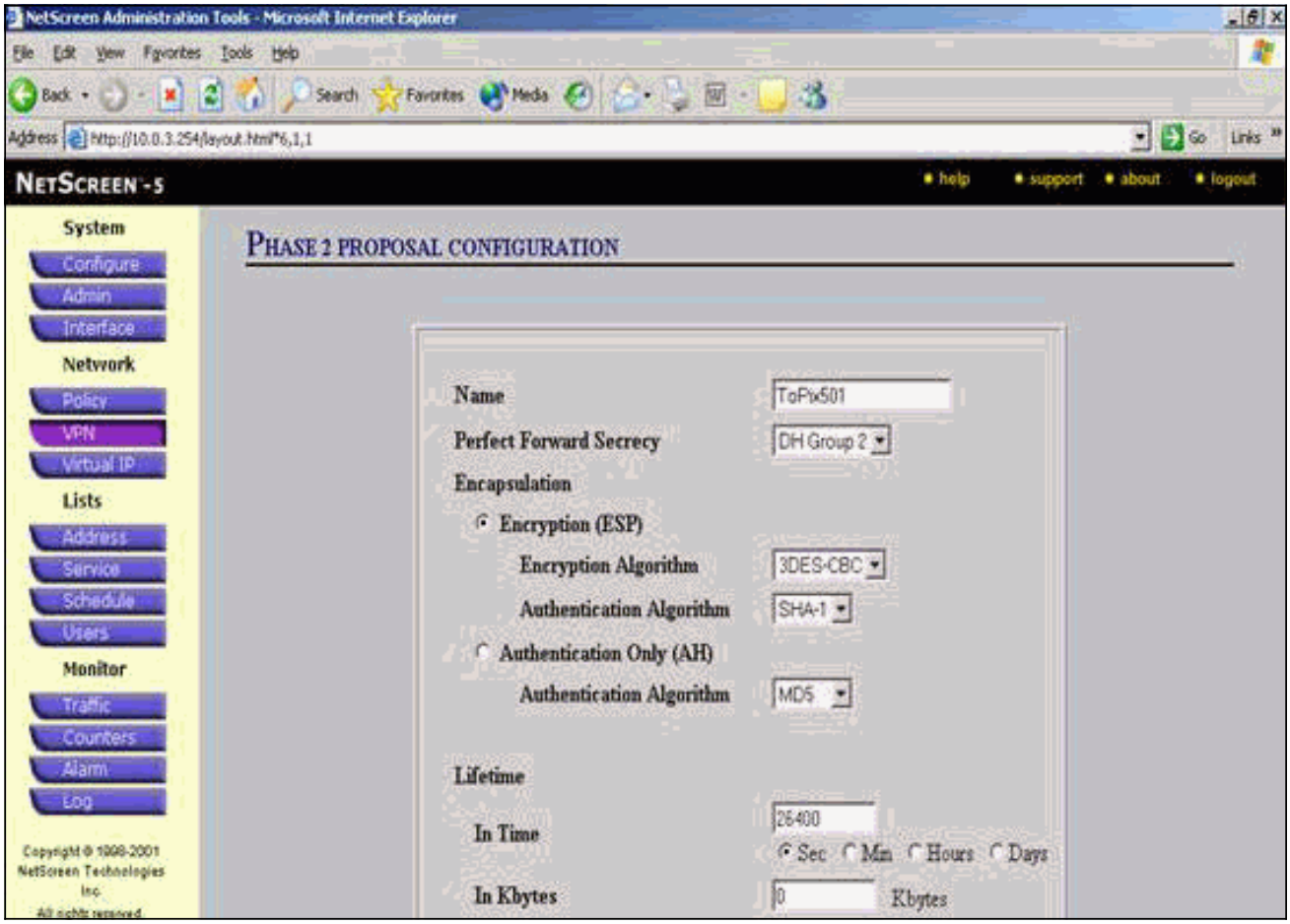
7. Vá à aba da proposta P1 e clique a **proposta nova da fase 1** para configurar a proposta 1.
8. Incorpore a informação de configuração para a proposta da fase 1 e clique a **APROVAÇÃO**.Este exemplo usa estes campos e valores para a troca da fase 1.**Nome:** ToPix501**Autenticação:** Preshare**Grupo DH:** Grupo2**Criptografia:** 3DES-CBC**Mistura:** SHA-1**Duração:** Segundo
   3600.



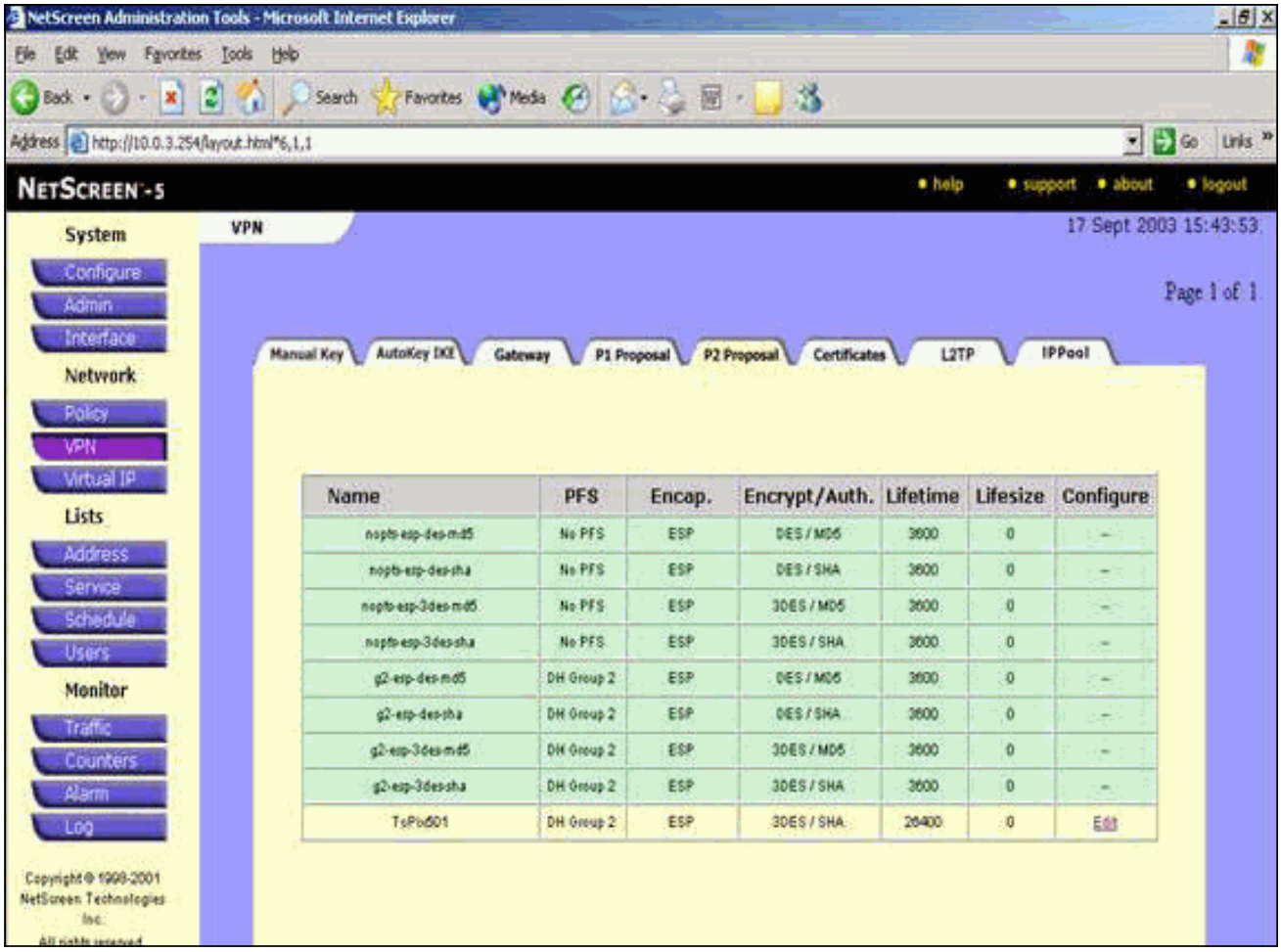
Quando a fase 1 é adicionada com sucesso à configuração NetScreen, uma tela similar a este exemplo
aparece.



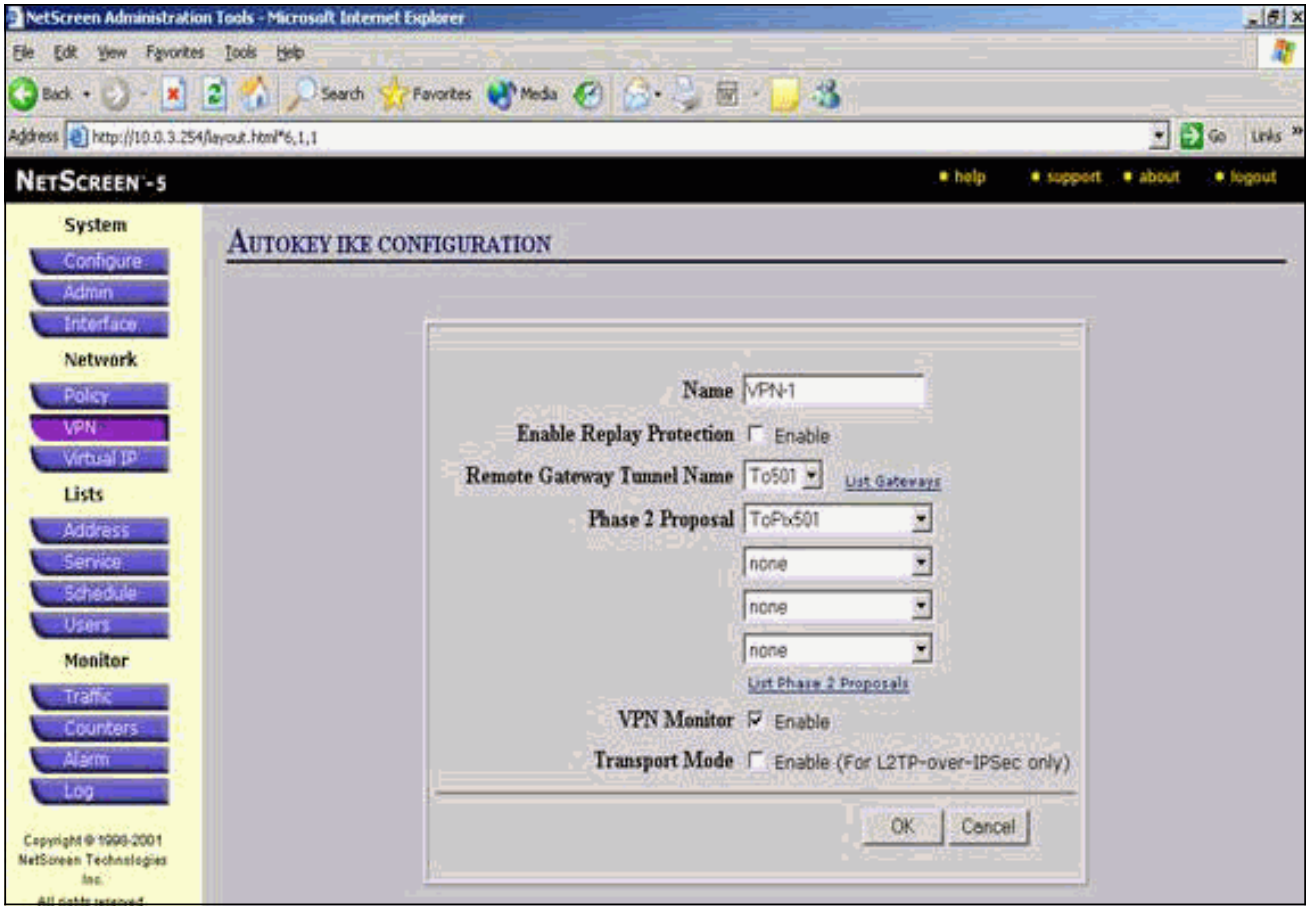
9. Vá à aba da proposta P2 e clique a **proposta nova da fase 2** para configurar a fase 2.
10. Incorpore a informação de configuração para a proposta da fase 2 e clique a **APROVAÇÃO**.Este exemplo usa estes campos e valores para a troca da fase 2.**Nome:** ToPix501**Discrição perfeita adiante:** DH-2 (1024 bit)**Algoritmo de Criptografia:** 3DES-CBC**Algoritmo de autenticação:** SHA-1**Duração:** Segundo
26400



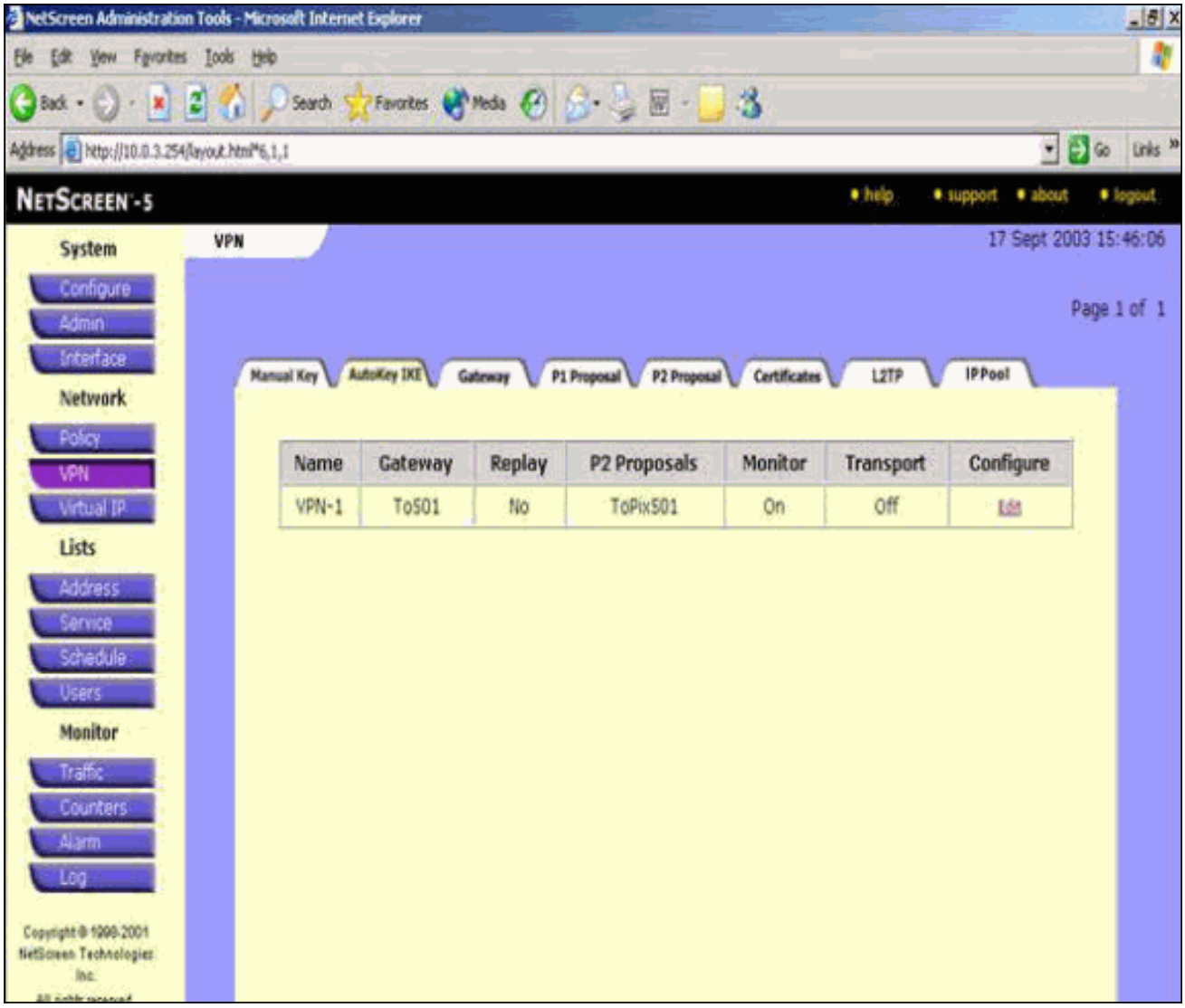
Quando a fase 2 é adicionada com sucesso à configuração NetScreen, uma tela similar a este exemplo
aparece.



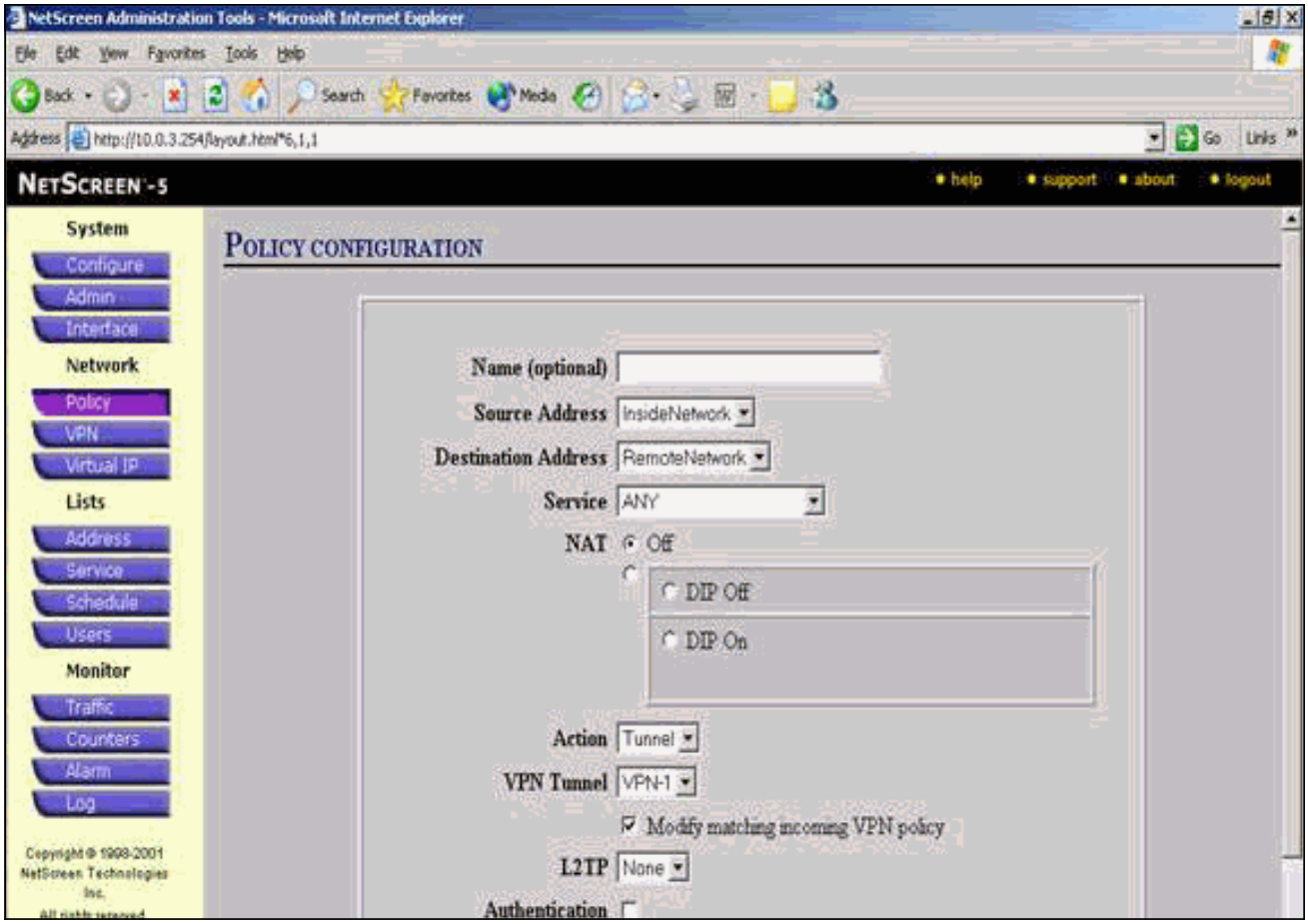
11. Selecione a aba do **AutoKey IKE**, e clique então a **entrada de IKE de Chave Automática nova** para criar e configurar os AutoKeys IKE.
12. Incorpore a informação de configuração para o AutoKey IKE, e clique então a **APROVAÇÃO**.Este exemplo usa estes campos e valores para o AutoKey IKE.**Nome:** VPN-1**Nome de túnel do gateway remoto:** To501(Isto foi criado previamente na aba do gateway.)**Proposta da fase 2:** ToPix501(Isto foi criado previamente na aba da proposta P2.)**Monitor VPN:** Enable(Isto permite o dispositivo do NetScreen de ajustar armadilhas do [SNMP] do protocolo administración de red simple a fim monitorar a condição do monitor VPN.)



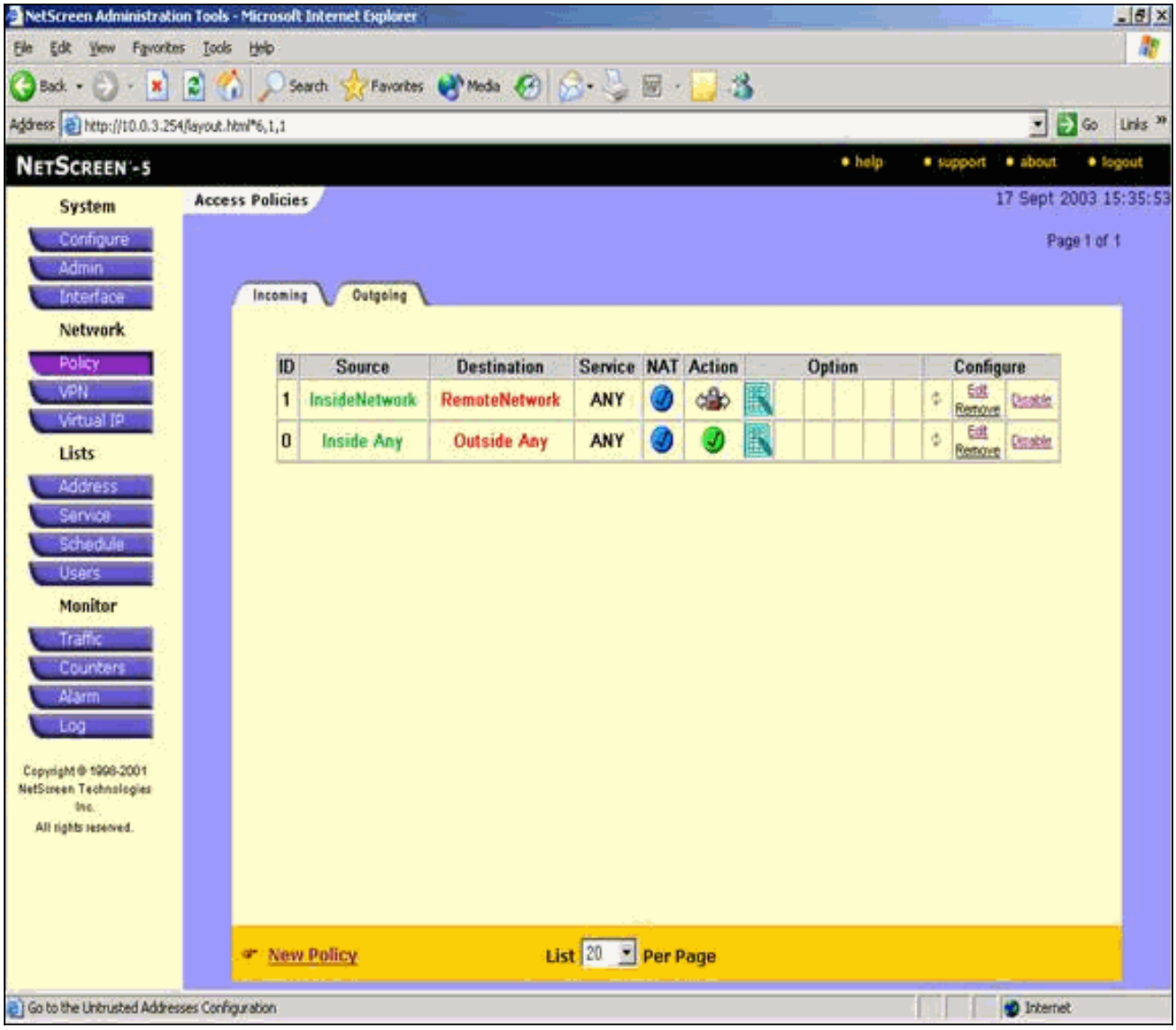
Quando a regra VPN-1 é configurada com sucesso, uma tela similar a este exemplo aparece.



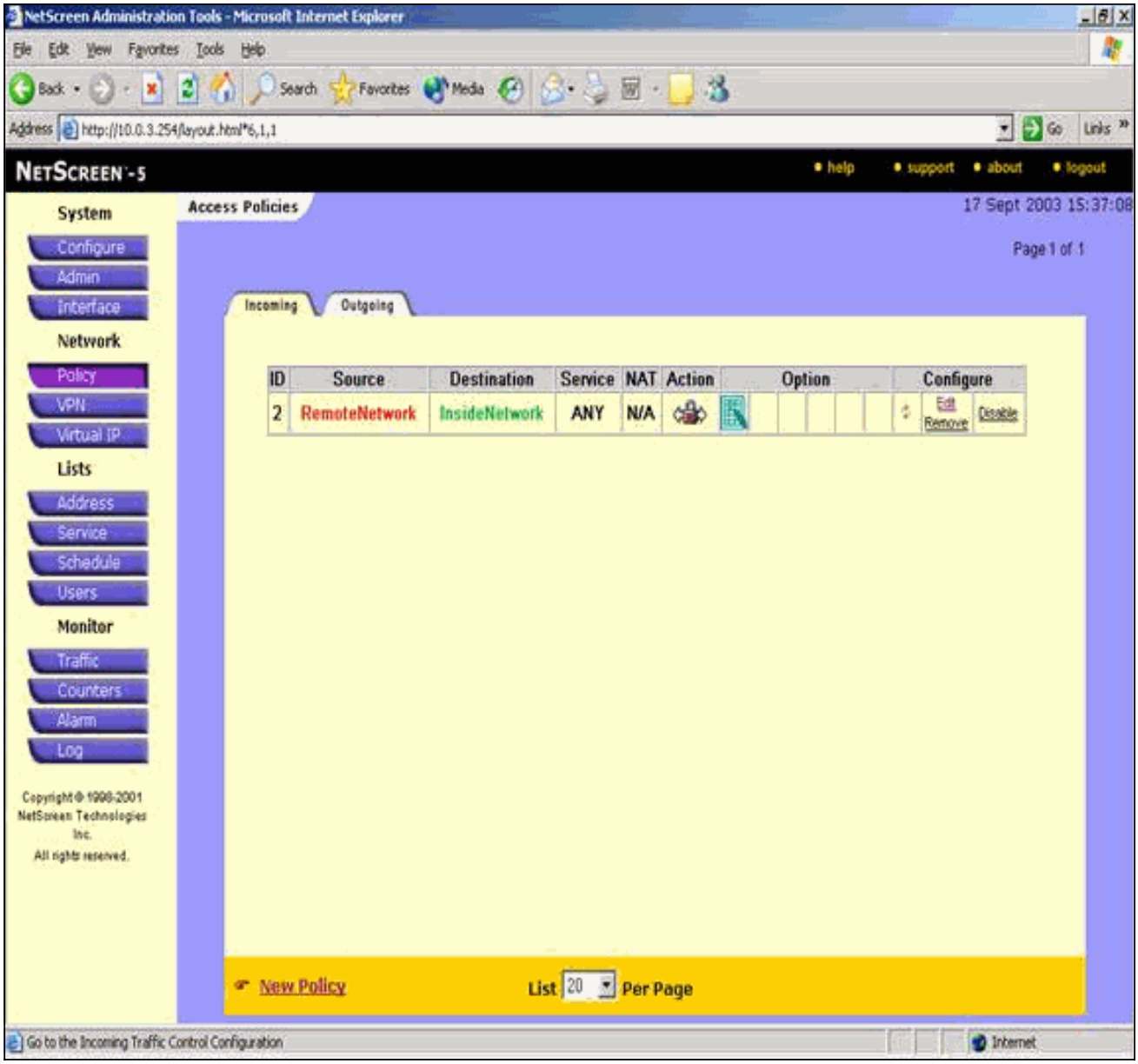
13. Selecione o **rede > política**, vá à aba que parte, e clique a **política nova** para configurar as regras que permitem a criptografia do tráfego de IPSec.
14. Incorpore a informação de configuração para a política e clique a **APROVAÇÃO**.Este exemplo usa estes campos e valores para a política. O campo de nome é opcional e não é usado neste exemplo.**Endereço de origem:** InsideNetwork(Isto foi definido previamente na aba confiada.)**Endereço de destino:** RemoteNetwork(Isto foi definido previamente sob a aba não confiável.)**Serviço:** Alguns**Ação:** Túnel**Túnel VPN:** VPN-1(Isto foi definido previamente como o túnel VPN na aba do AutoKey IKE.)**Modify que combina a política de VPN entrante:** Verificado(Esta opção cria automaticamente uma regra de entrada que combine o tráfego da rede externa
VPN.)



15. Quando a política é adicionada, assegure-se de que a regra de partida VPN seja primeira na lista de políticas. (A regra que é criada automaticamente para o tráfego de entrada está na aba entrante.)Termine estas etapas se você precisa de mudar a ordem das políticas:Clique a aba que parte.Clique as setas circular na coluna configurar a fim indicar o indicador do micro da política do movimento.Mude a ordem das políticas de modo que a política de VPN esteja acima do ID de política 0 (de modo que a política de VPN está na parte superior da
lista).



Vá à aba entrante a fim ver a regra para o tráfego de entrada.



Verificar

Esta seção fornece a informação que você pode se usar para confirmar sua configuração trabalha corretamente.

Comandos de verificação

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- **sibilo** — Diagnostica a conectividade de rede básica.
- show crypto ipsec sa – Mostra as associações de segurança da fase 2.
- show crypto isakmp sa - Mostra as associações de segurança da fase 1.

Saída da verificação

O exemplo de saída dos **comandos ping e show** é mostrado aqui.

Este sibilo é iniciado de um host atrás do firewall de NetScreen.

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

A saída do **comando show crypto ipsec sa** é mostrada aqui.

```
pixfirewall(config)#show crypto ipsec sa interface: 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:
```

A saída do **comando show crypto isakmp sa** é mostrada aqui.

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

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **motor do debug crypto** — Indica mensagens sobre as crypto-engines.
- **IPsec do debug crypto** — Indica a informação sobre eventos de IPSec.
- debug crypto isakmp - Exibe mensagens sobre eventos IKE.

Exemplo de debug

O exemplo de debug do PIX Firewall é mostrado aqui.

```
debug crypto engine
debug crypto ipsec
debug crypto isakmp

crypto_isakmp_process_block:src:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
```

```
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (basic) of 28800
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

ISAKMP (0): SA is doing pre-shared key authentication
   using id type ID_IPV4_ADDR
return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.173.85,
   dest:172.18.124.96 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

ISAKMP (0): processing NONCE payload. message ID = 0

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.173.85,
   dest:172.18.124.96 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP (0): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:172.18.173.85/500
   Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.173.85/500 Ref cnt
   incremented to:1
   Total VPN Peers:1
crypto_isakmp_process_block:src:172.18.173.85,
   dest:172.18.124.96 spt:500 dpt:500
ISAKMP (0): processing DELETE payload. message ID = 534186807,
   spi size = 4IPSEC(key_engin
e): got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas):
   delete all SAs shared with 172.18.173.85

return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:172.18.173.85,
   dest:172.18.124.96 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode: OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 4150037097

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
```

```
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of 0x0 0x0 0x67 0x20
ISAKMP:      encaps is 1
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      group is 2
ISAKMP (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= 0x24

ISAKMP (0): processing NONCE payload. message ID = 4150037097

ISAKMP (0): processing KE payload. message ID = 4150037097

ISAKMP (0): processing ID payload. message ID = 4150037097
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.0.3.0/255.255.255.0
   prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 4150037097
ISAKMP (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 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.173.85,
   dest:172.18.124.96 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 3
map_alloc_entry: allocating entry 4

ISAKMP (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= 0x25
IPSEC(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= 0x25

VPN Peer: IPSEC: Peer ip:172.18.173.85/500 Ref cnt
   incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.18.173.85/500 Ref cnt
```

```
   incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
```

Informações Relacionadas

- Negociação IPsec/Protocolos IKE
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems