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

Contents

Introduction

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.

Prerequisites

Requirements

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

- O NetScreen Firewall está configurado com os endereços IP nas interfaces de confiança/não confiança.
- A conectividade é estabelecida na Internet.

Componentes Utilizados

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

- Software PIX Firewall versão 6.3(1)
- Revisão mais recente da NetScreen

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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 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`

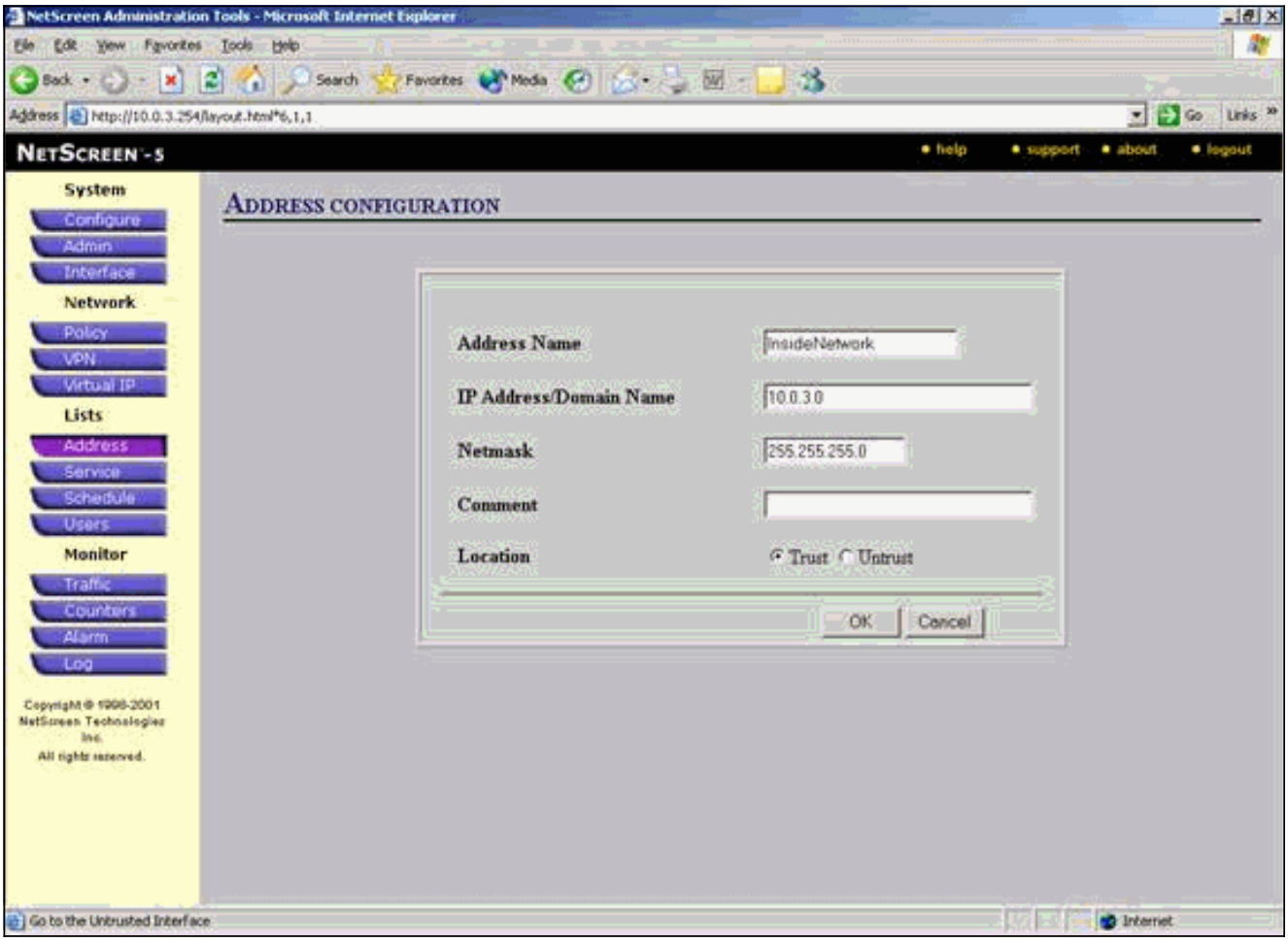
```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
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
```

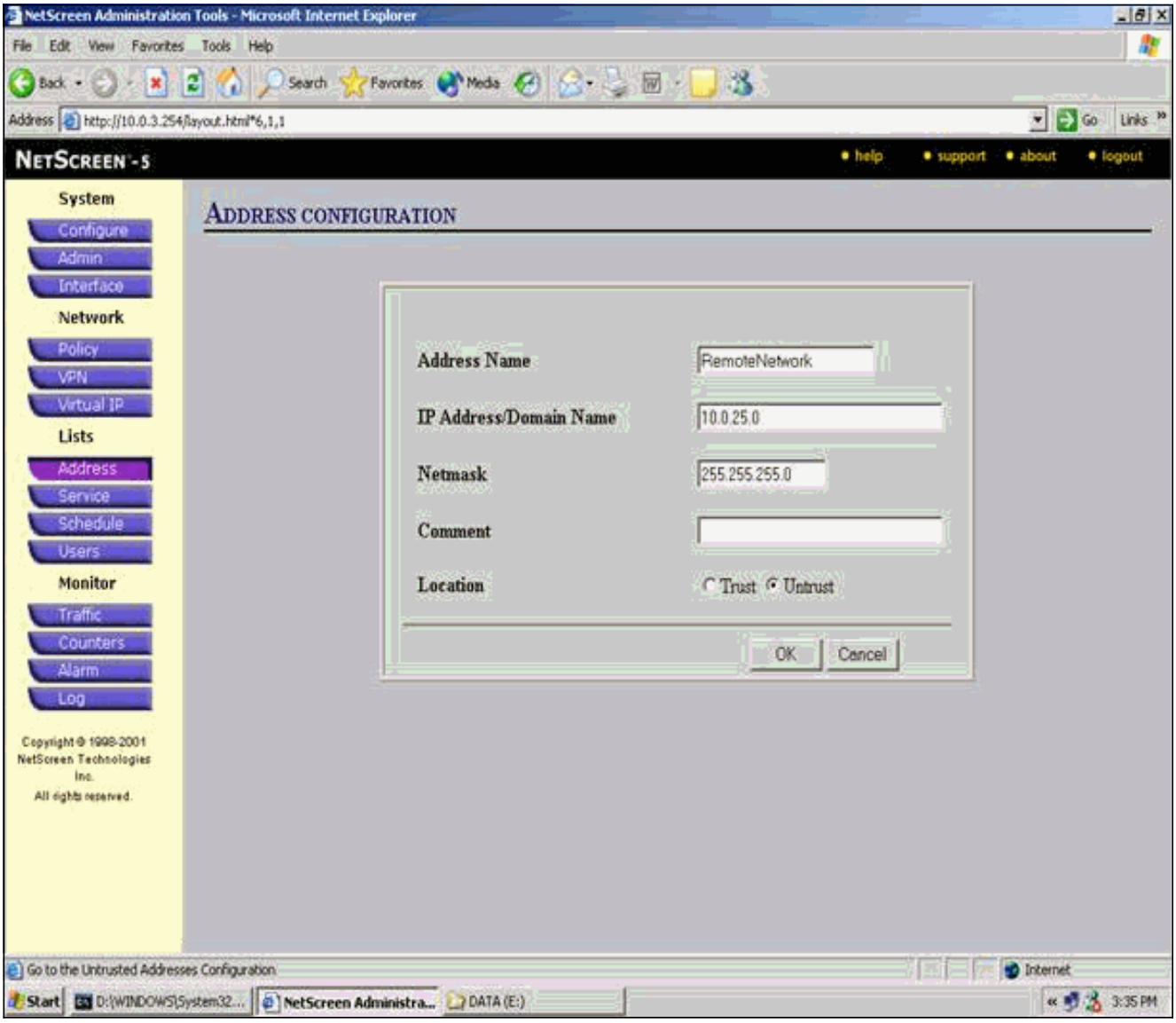
Configurar o firewall NetScreen

Conclua estes passos para configurar o NetScreen Firewall.

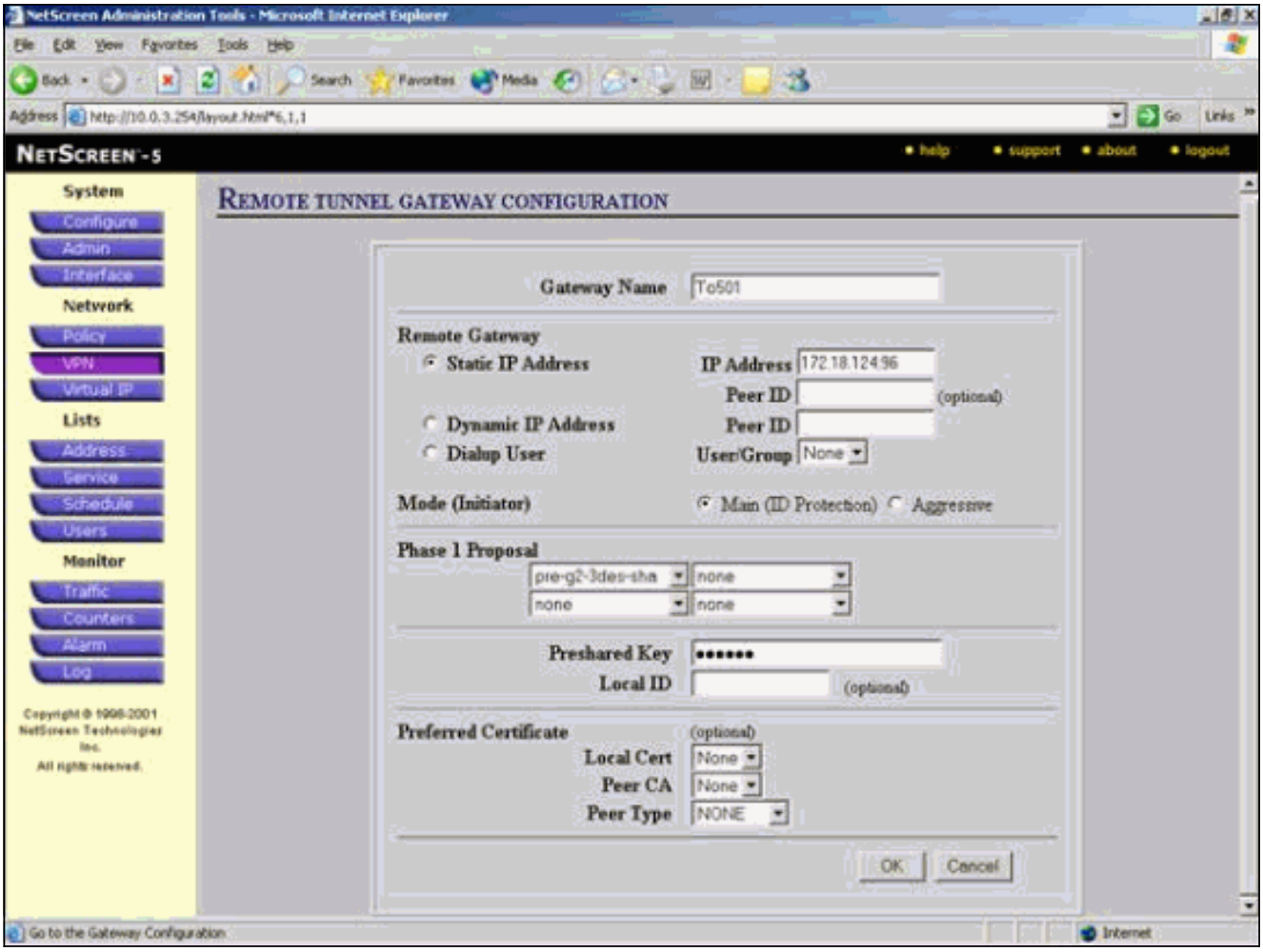
1. Selecione **Listas > Endereço**, vá para a guia Confiável e clique em **Novo endereço**.
2. Adicione a rede interna NetScreen criptografada no túnel e clique em **OK**.**Observação:** verifique se a opção Confiar está selecionada.Este exemplo usa a rede 10.0.3.0 com uma máscara
255.255.255.0.



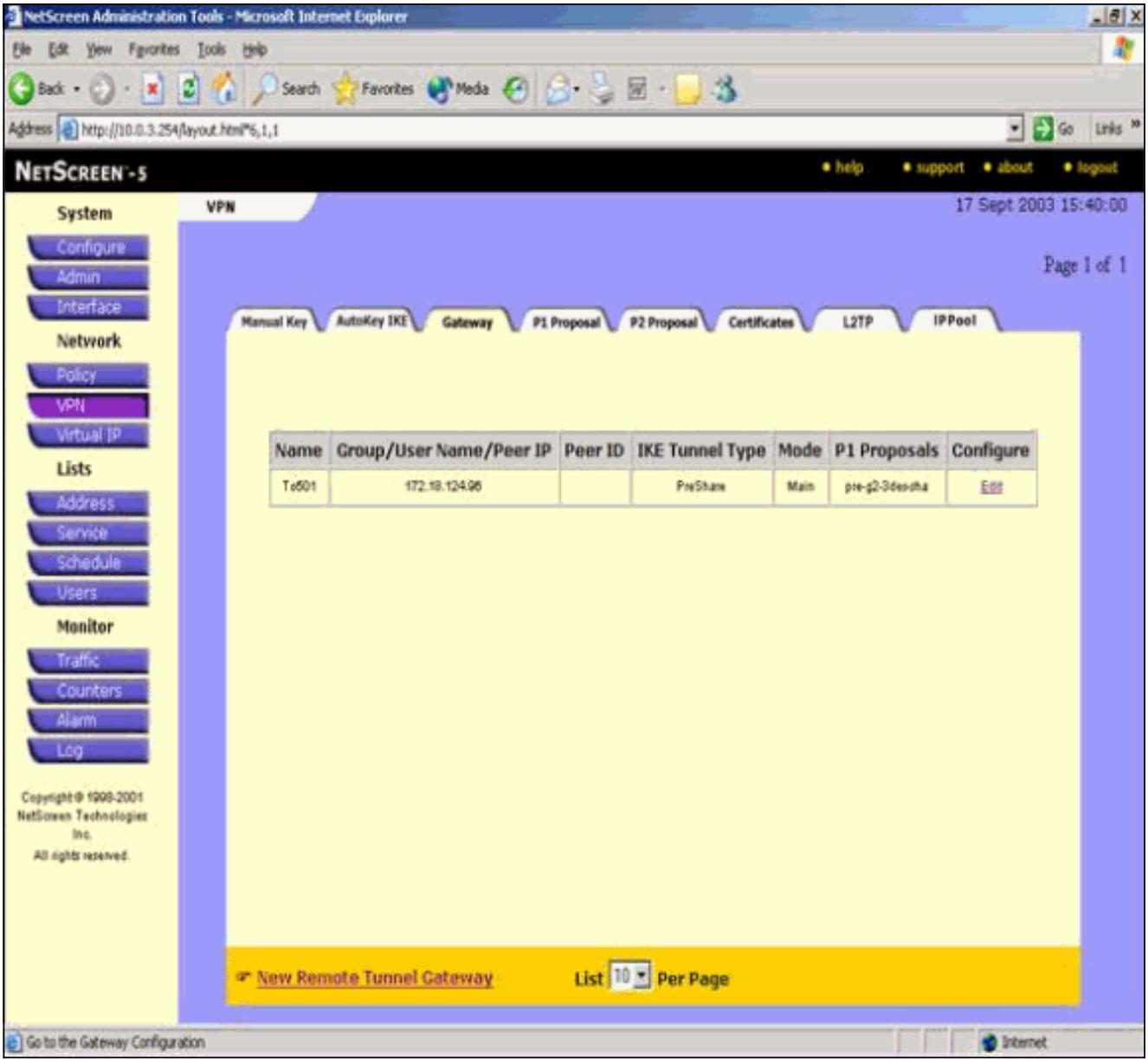
3. Selecione **Listas > Endereço**, vá para a guia Não confiável e clique em **Novo endereço**.
4. Adicione a rede remota que o NetScreen Firewall usa quando criptografa pacotes e clique em **OK**.**Observação:** não use grupos de endereços ao configurar uma VPN para um gateway que não seja NetScreen. A interoperabilidade de VPN falha se você usa grupos de endereços. O gateway de segurança que não é NetScreen não sabe como interpretar a ID de proxy criada pelo NetScreen quando o grupo de endereços é usado.Há algumas soluções alternativas para isso:Separe os grupos de endereços em entradas individuais do catálogo de endereços. Especifique políticas individuais em uma base de entrada por catálogo de endereços.Configure o ID do proxy para 0.0.0.0/0 no gateway que não é NetScreen (dispositivo de firewall), se possível.Este exemplo usa a rede 10.0.25.0 com uma máscara
255.255.255.0.



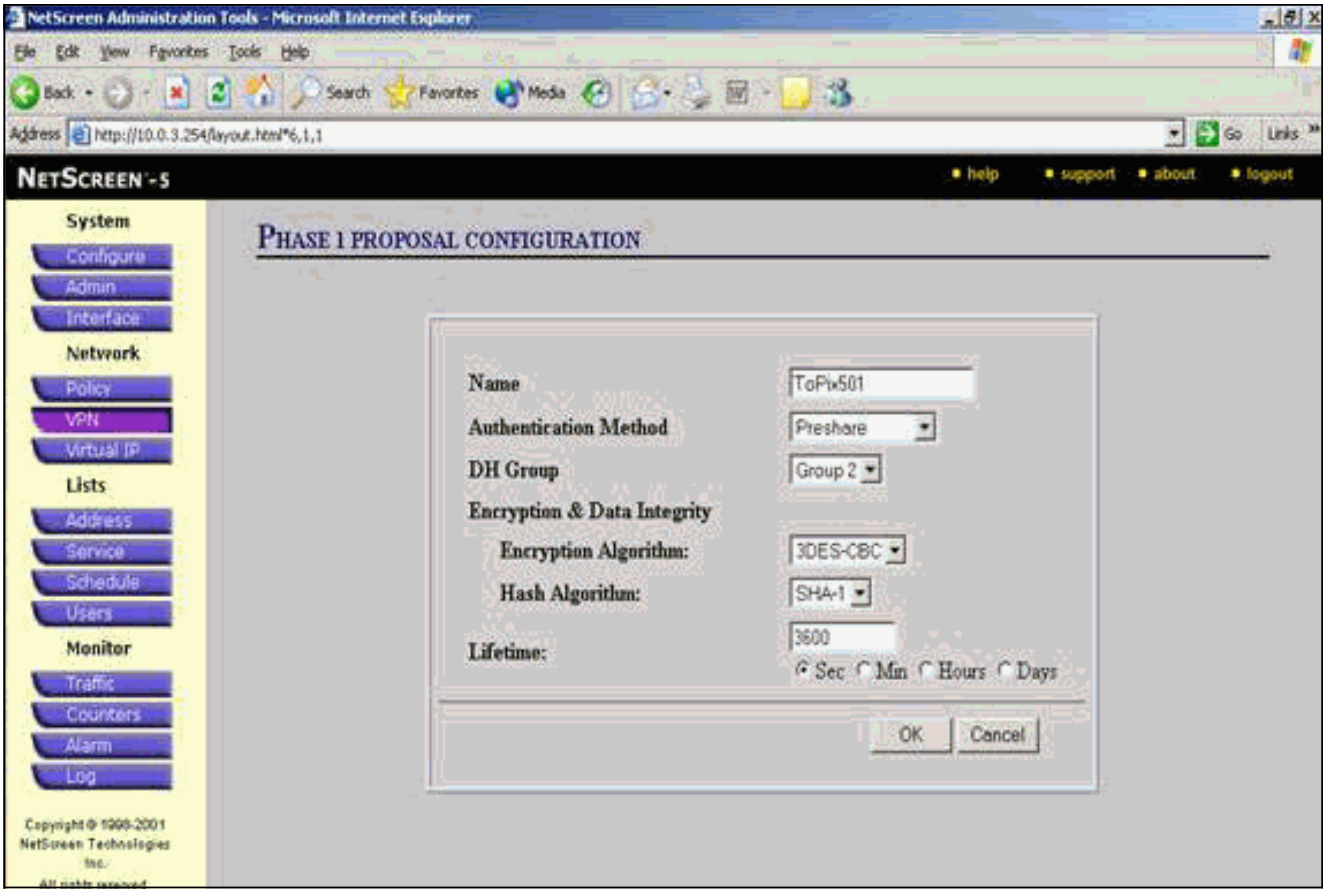
5. Selecione **Rede > VPN**, vá até a guia Gateway e clique em **Novo gateway de túnel remoto** para configurar o gateway VPN (políticas IPsec da Fase 1 e Fase 2).
6. Use o endereço IP da interface externa do PIX para terminar o túnel e configure as opções IKE da Fase 1 para vincular. Clique em **OK** quando terminar.Este exemplo usa esses campos e valores.**Nome do gateway:** To501**Endereço IP estático:** 172.18.124.96**Modo:** Principal (Proteção de ID)**Chave pré-compartilhada:** "testme"**Fase 1 proposta:** pre-g2-3des-sha



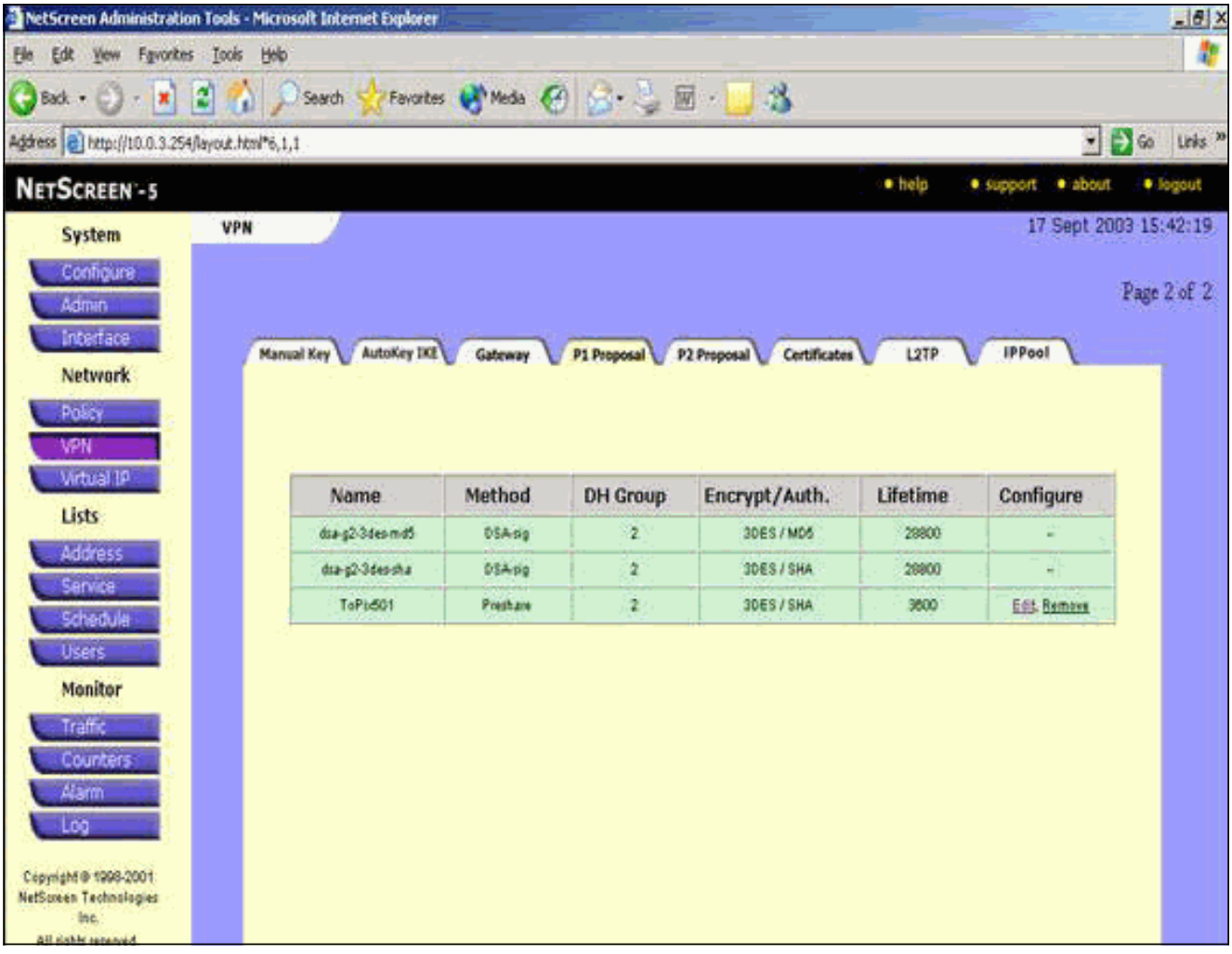
Quando o gateway de túnel remoto é criado com êxito, uma tela semelhante a esta é exibida.



7. Acesse a guia P1 Proposal (Proposta P1) e clique em **New Phase 1 Proposal (Nova fase 1)** para configurar a Proposta 1.
8. Insira as informações de configuração para a Fase 1 da Proposta e clique em **OK**.Este exemplo usa esses campos e valores para a troca da Fase 1.**Nome:** ToPix501**Autenticação:** Preshare**Grupo DH:** Grupo 2**Criptografia:** 3DES-CBC**Hash:** SHA-1**Duração:** 3600 S.

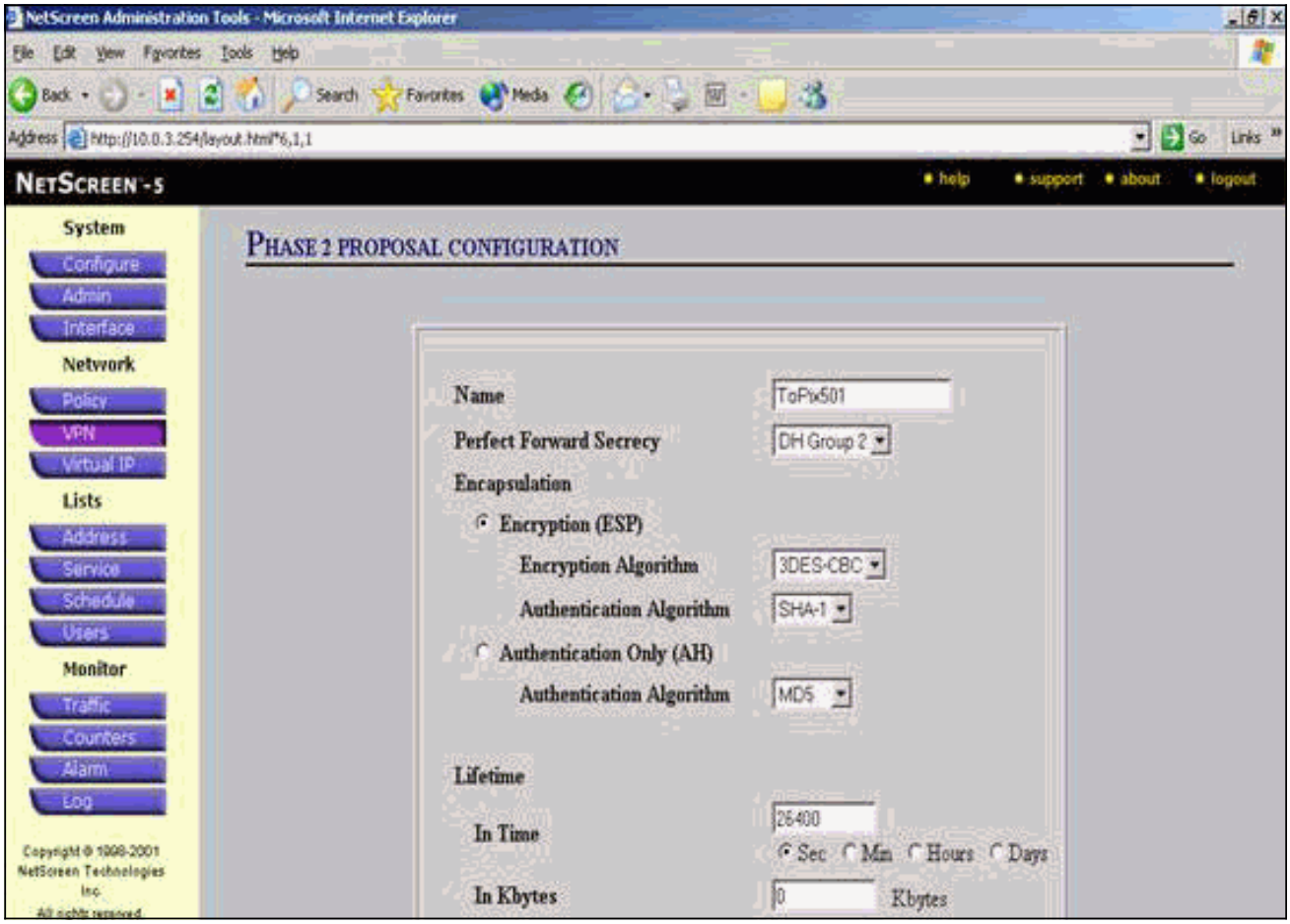


Quando a Fase 1 é adicionada com êxito à configuração da NetScreen, uma tela semelhante a este exemplo é
exibida.

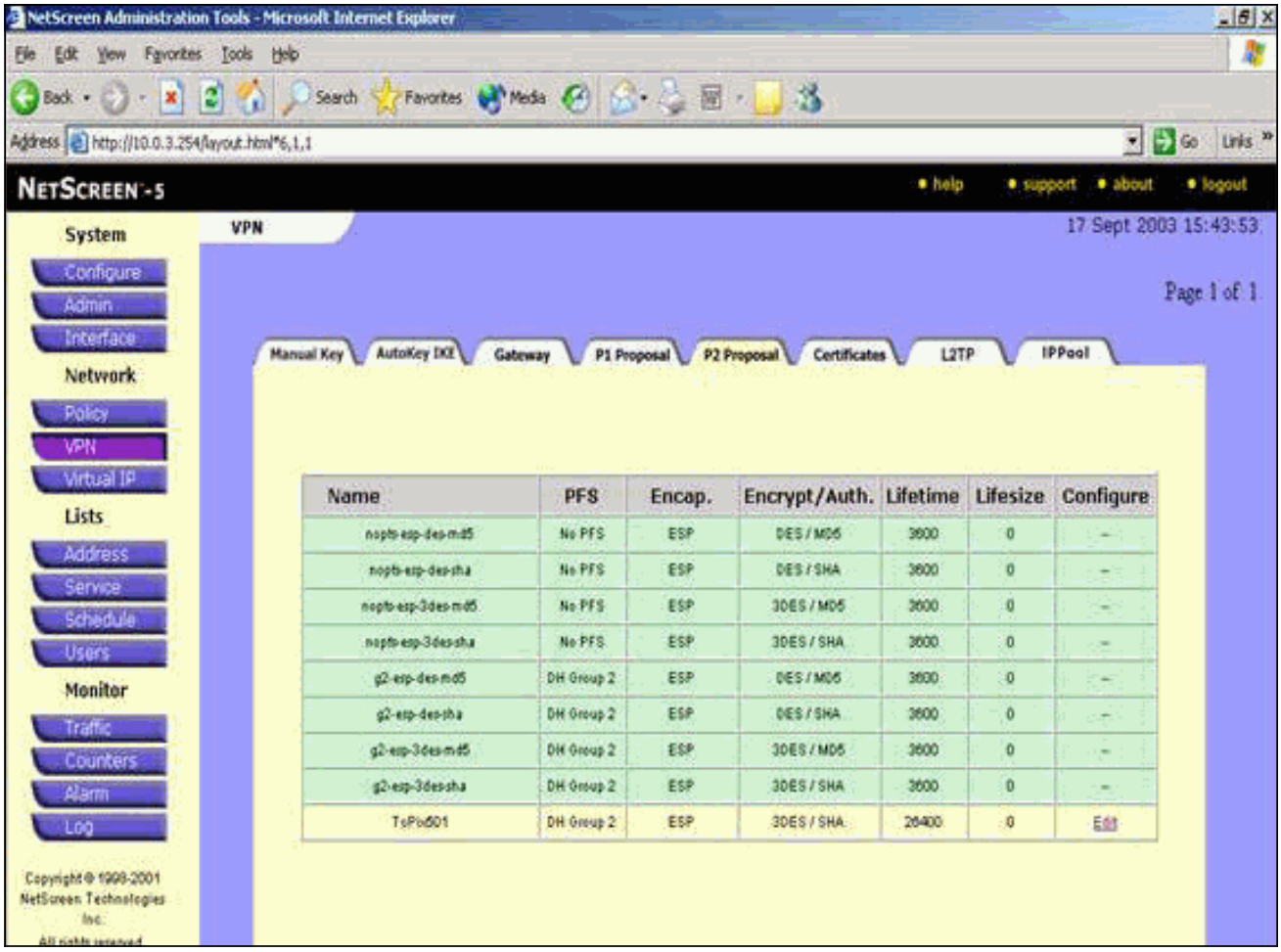


9. Acesse a guia P2 Proposal (Proposta P2) e clique em **New Phase 2 Proposal** para configurar a Fase 2.
10. Insira as informações de configuração da Proposta da Fase 2 e clique em **OK**.Este exemplo usa esses campos e valores para a troca da Fase 2.**Nome:** ToPix501**Segredo de encaminhamento perfeito:** DH-2 (1024 bits)**Algoritmo de Criptografia:** 3DES-CBC**Algoritmo de autenticação:** SHA-1**Duração:** 26400

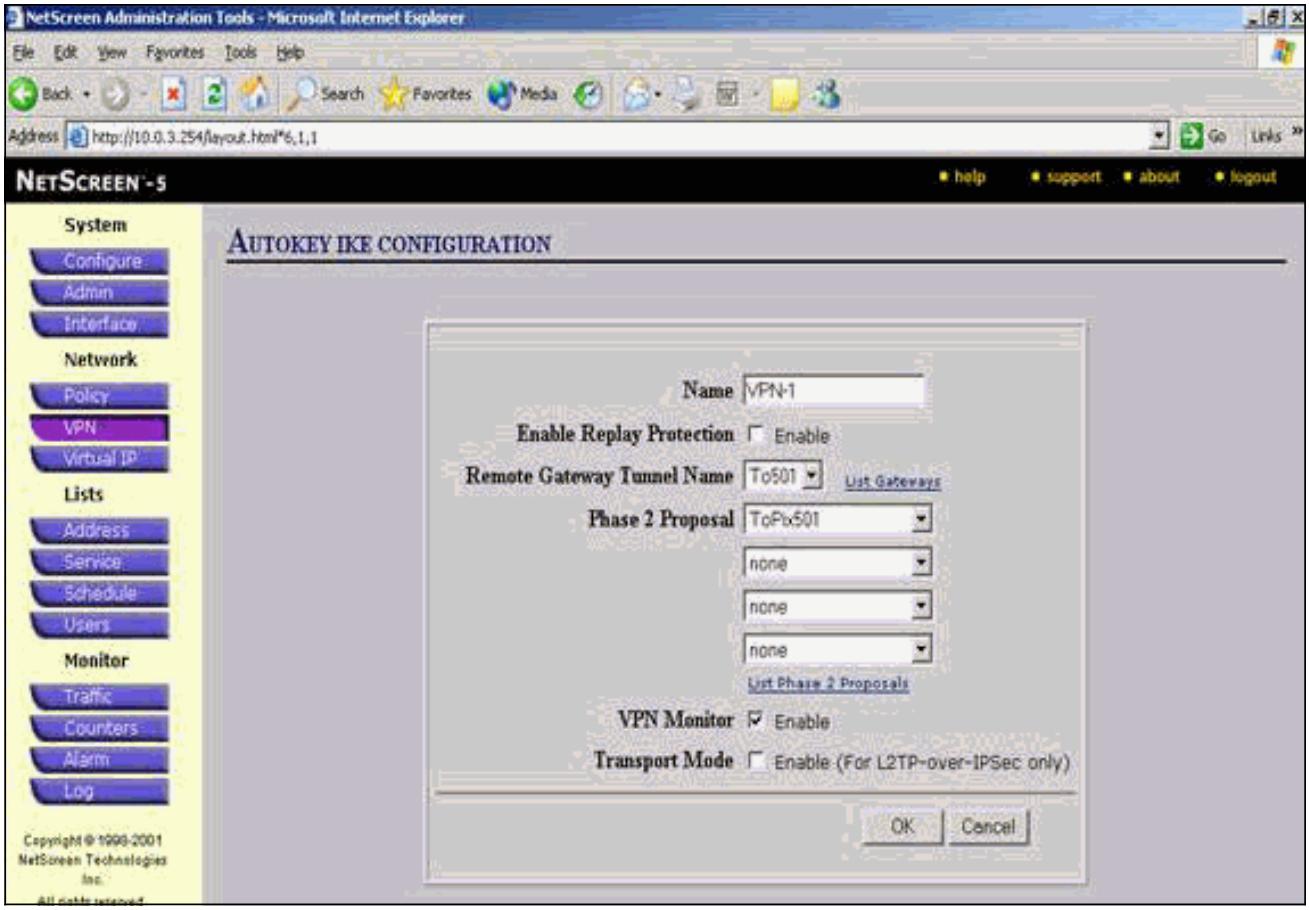
S



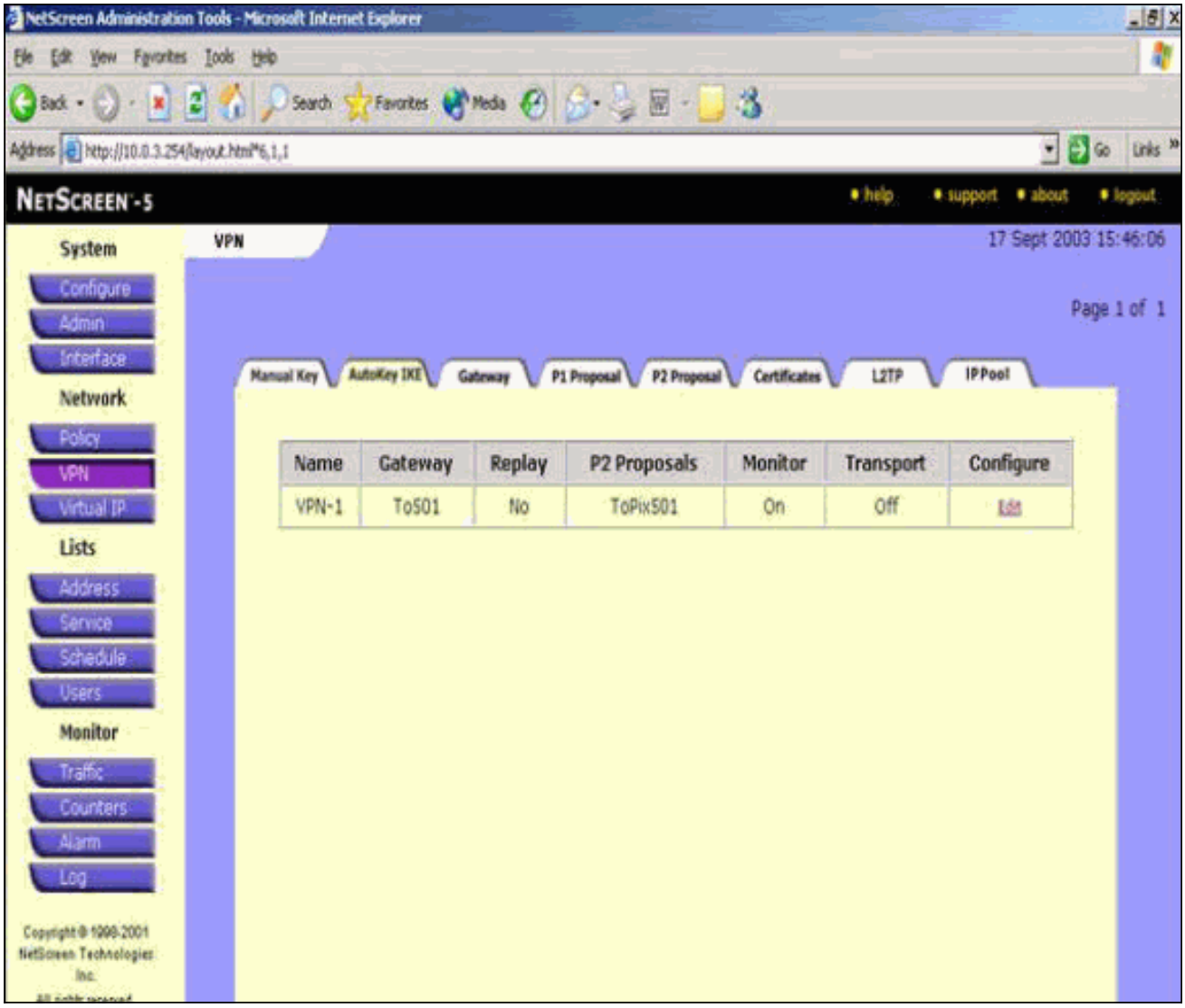
Quando a Fase 2 é adicionada com êxito à configuração da NetScreen, uma tela semelhante a este exemplo é
exibida.



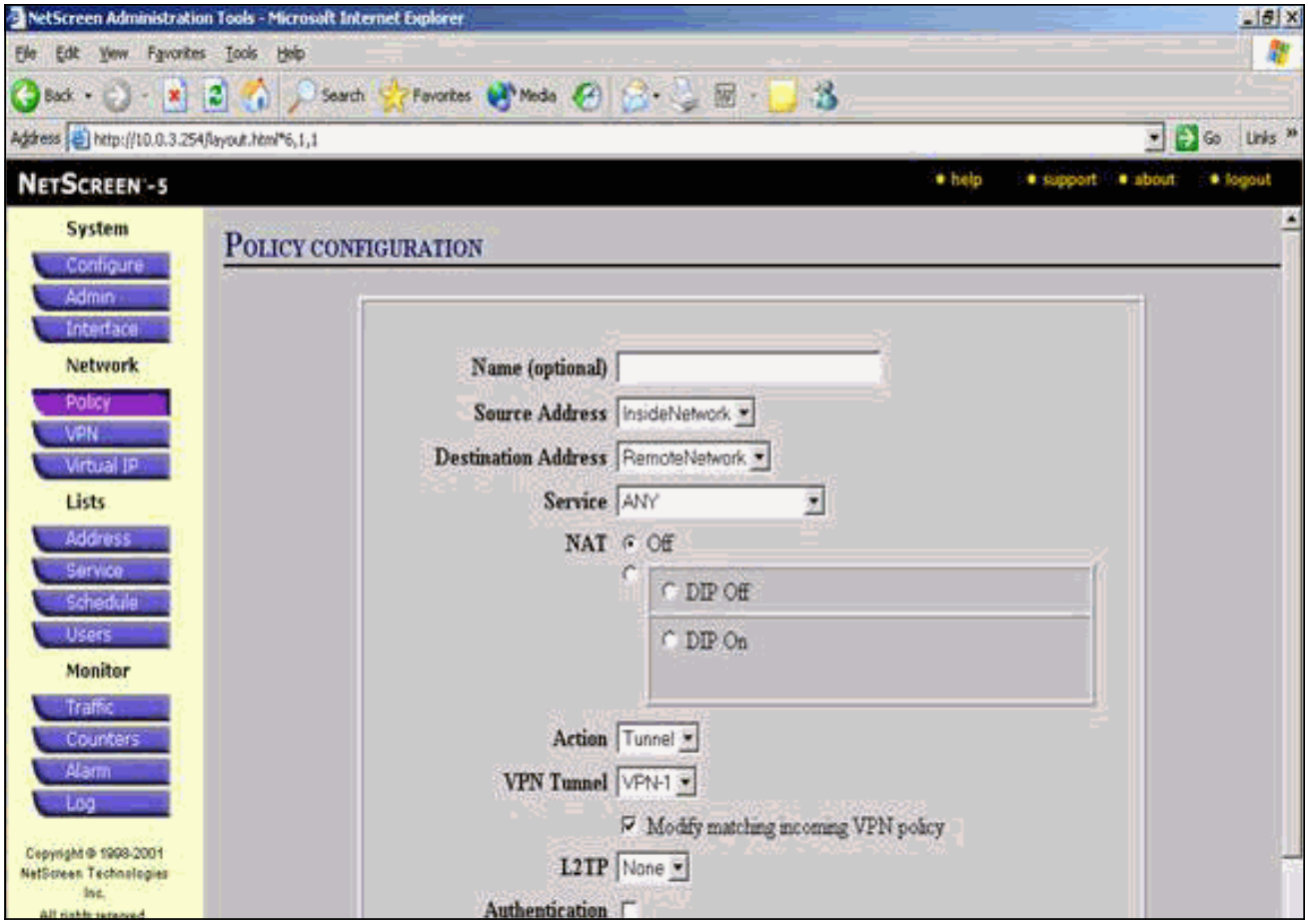
11. Selecione a guia **AutoKey IKE** e clique em **New AutoKey IKE Entry** para criar e configurar AutoKeys IKE.
12. Insira as informações de configuração para o IKE de AutoKey e clique em **OK**.Este exemplo usa estes campos e valores para a IKE de AutoKey.**Nome:** VPN-1**Nome do túnel de gateway remoto:** To501(Isso foi criado anteriormente na guia Gateway.)**Fase 2 Proposta:** ToPix501(Isso foi criado anteriormente na guia Proposta P2.)**Monitor VPN:** Enable(Isso permite que o dispositivo NetScreen defina interceptações SNMP (Simple Network Management Protocol) para monitorar a condição do VPN Monitor.)



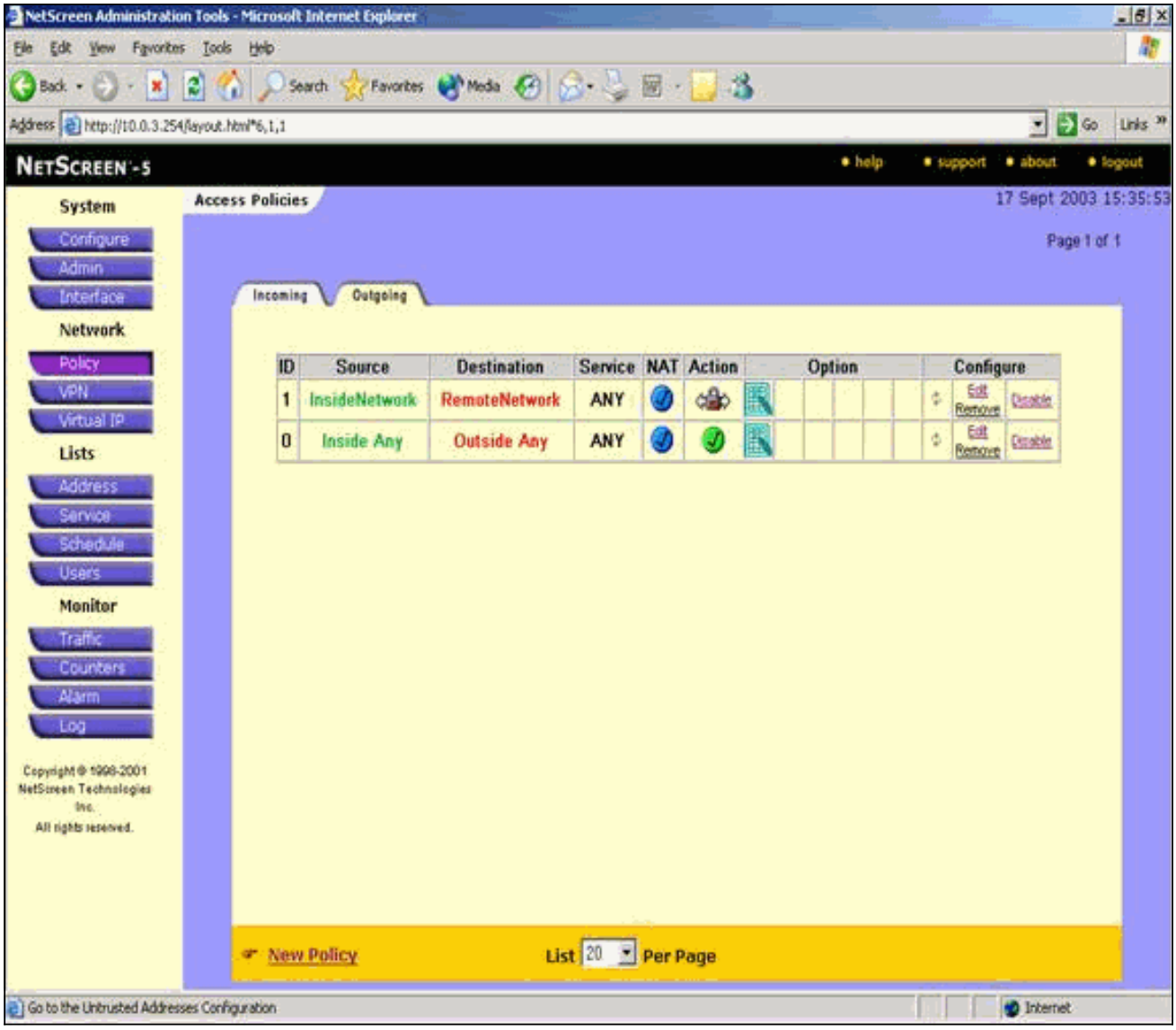
Quando a regra VPN-1 é configurada com êxito, uma tela semelhante a este exemplo é exibida.



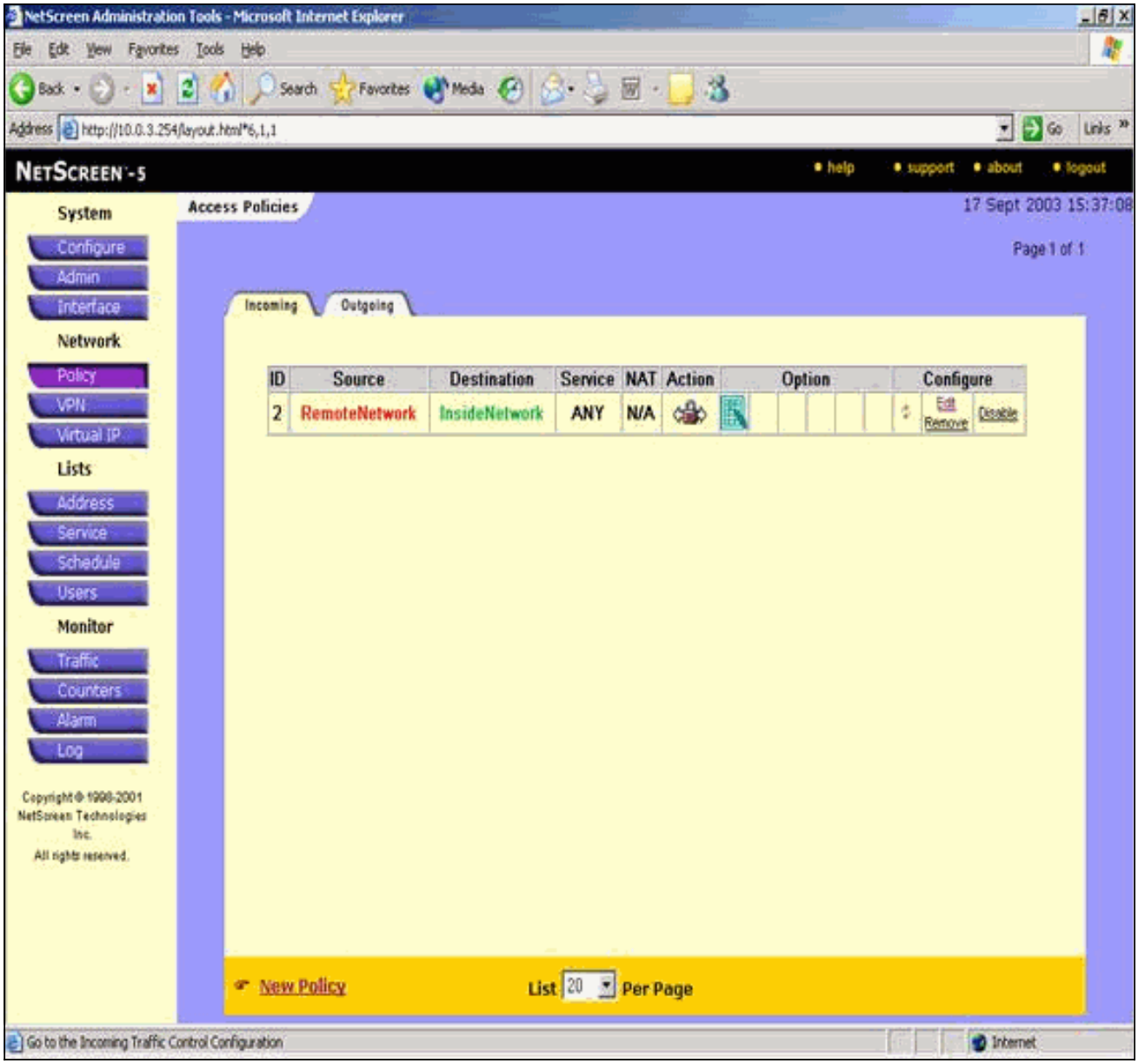
13. Selecione **Rede > Política**, vá para a guia Saída e clique em **Nova Política** para configurar as regras que permitem criptografia do tráfego IPsec.
14. Insira as informações de configuração da diretiva e clique em **OK**.Este exemplo usa esses campos e valores para a política. O campo Nome é opcional e não é usado neste exemplo.**Endereço de origem:** RedeInterna(Isso foi definido anteriormente na guia Confiável.)**endereço de destino:** Rede remota(Isso foi definido anteriormente na guia Não confiável.)**Serviço:** qualquer um**Ação:** Túnel**Túnel VPN:** VPN-1(Isso foi definido anteriormente como o túnel VPN na guia AutoKey IKE.)**Modificar política de VPN de entrada correspondente:** Verificado(Essa opção cria automaticamente uma regra de entrada que corresponde ao tráfego de VPN da rede externa.)



15. Quando a política for adicionada, certifique-se de que a regra de VPN de saída esteja primeiro na lista de políticas. (A regra criada automaticamente para o tráfego de entrada está na guia Entrada.)Siga estes passos se precisar alterar a ordem das políticas:Clique na guia Saída.Clique nas setas circulares na coluna Configure para exibir a janela Move Policy Micro.Altere a ordem das políticas para que a política de VPN esteja acima da ID de política 0 (para que a política de VPN esteja no topo da lista).



Vá até a guia Entrada para exibir a regra de tráfego de entrada.



Verificar

Esta seção fornece informações que você pode usar para confirmar se a configuração funciona corretamente.

Comandos de verificação

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

- **ping** — Diagnostica a conectividade básica da rede.
- **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 de verificação

A saída de exemplo dos comandos **ping** e **show** é mostrada aqui.

Esse ping é iniciado de um host por trás do NetScreen Firewall.

```
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
```

Troubleshoot

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.

- **debug crypto engine** — Exibe mensagens sobre mecanismos de criptografia.
- **debug crypto ipsec** — Exibe informações sobre eventos IPsec.
- **debug crypto isakmp — Exibe mensagens sobre eventos de IKE.**

Exemplo de saída de depuração

A saída de **depuração de** exemplo do PIX Firewall é mostrada 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