Configuración del túnel de LAN a LAN IPSec entre el Cisco Pix Firewall y un NetScreen Firewall

Contenido

Introducción

Este documento describe el procedimiento necesario usado para crear un túnel ipsec de LAN a LAN entre un Firewall Cisco PIX y un Firewall NetScreen con software más reciente. Hay una red privada detrás de cada dispositivo que se comunica con el otro firewall a través del túnel IPsec.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El firewall NetScreen se configura con las direcciones IP en las interfaces trust/untrust.
- La conectividad se establece en Internet.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Software PIX Firewall versión 6.3(1)
- Última revisión de 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.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuraciones

En este documento, se utilizan estas configuraciones:

- Firewall PIX
- Firewall NetScreen

Configuración del Firewall PIX

Firewall PIX

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

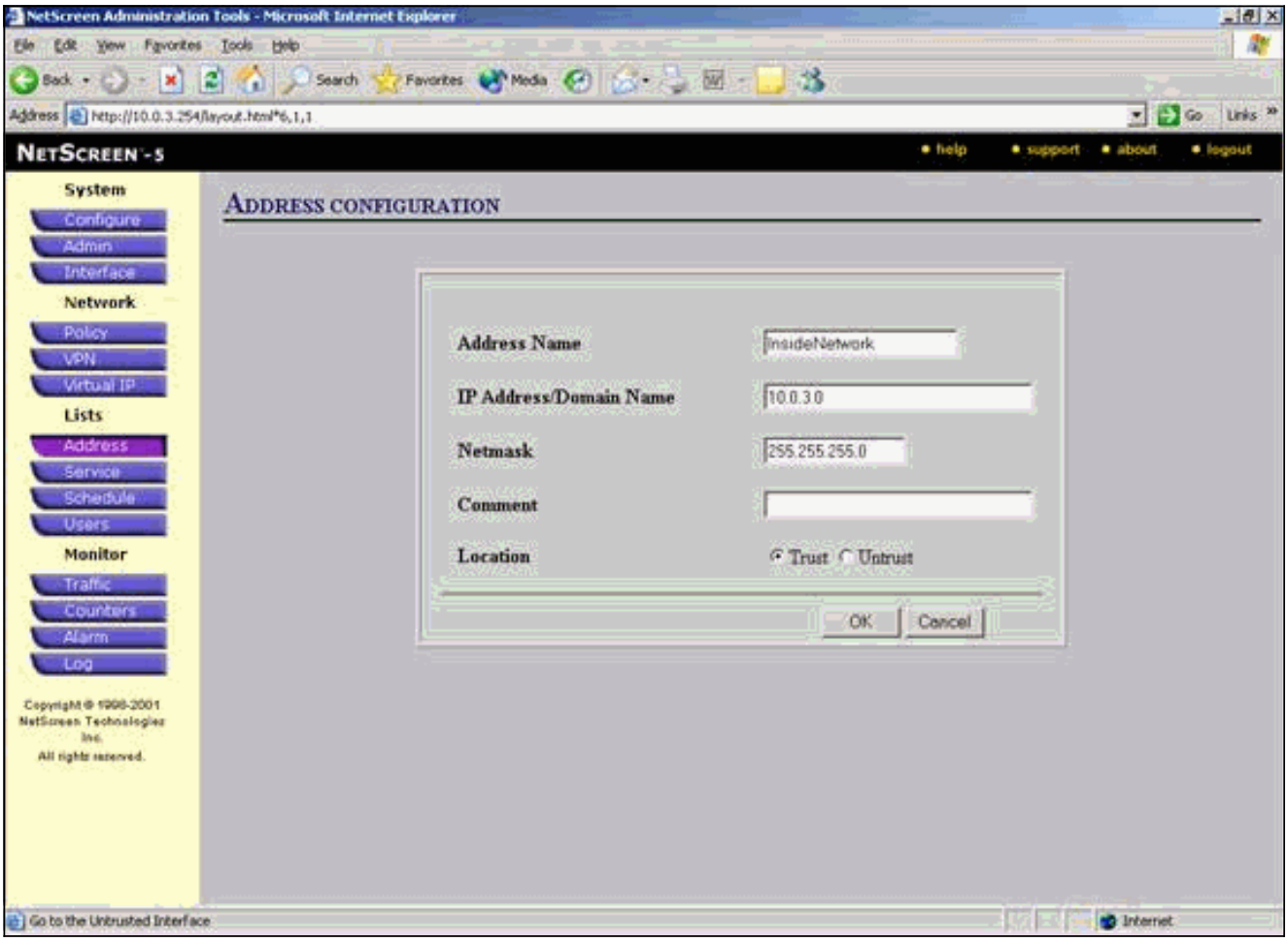
```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554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

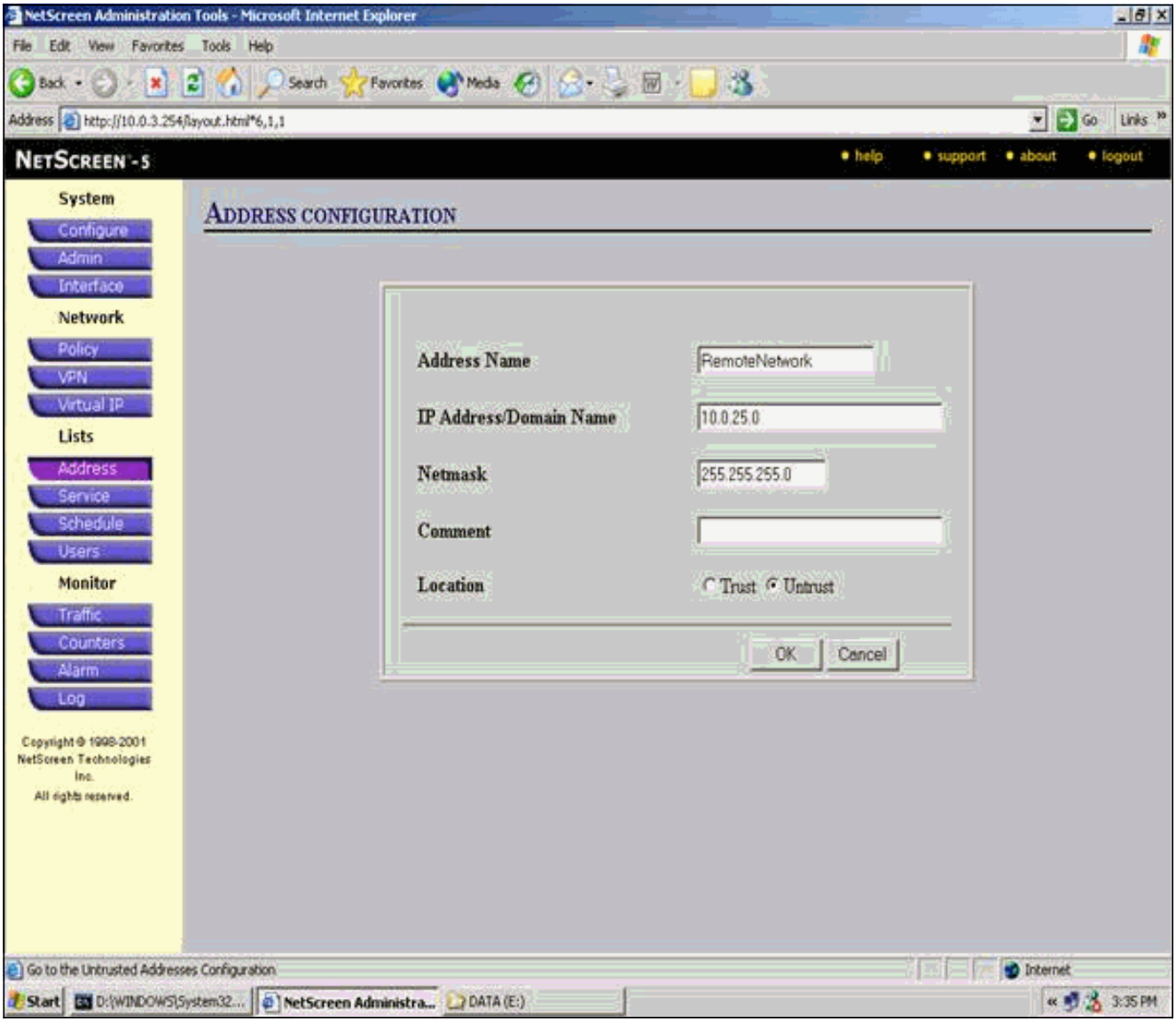
Configuración del firewall NetScreen

Complete estos pasos para configurar el firewall NetScreen.

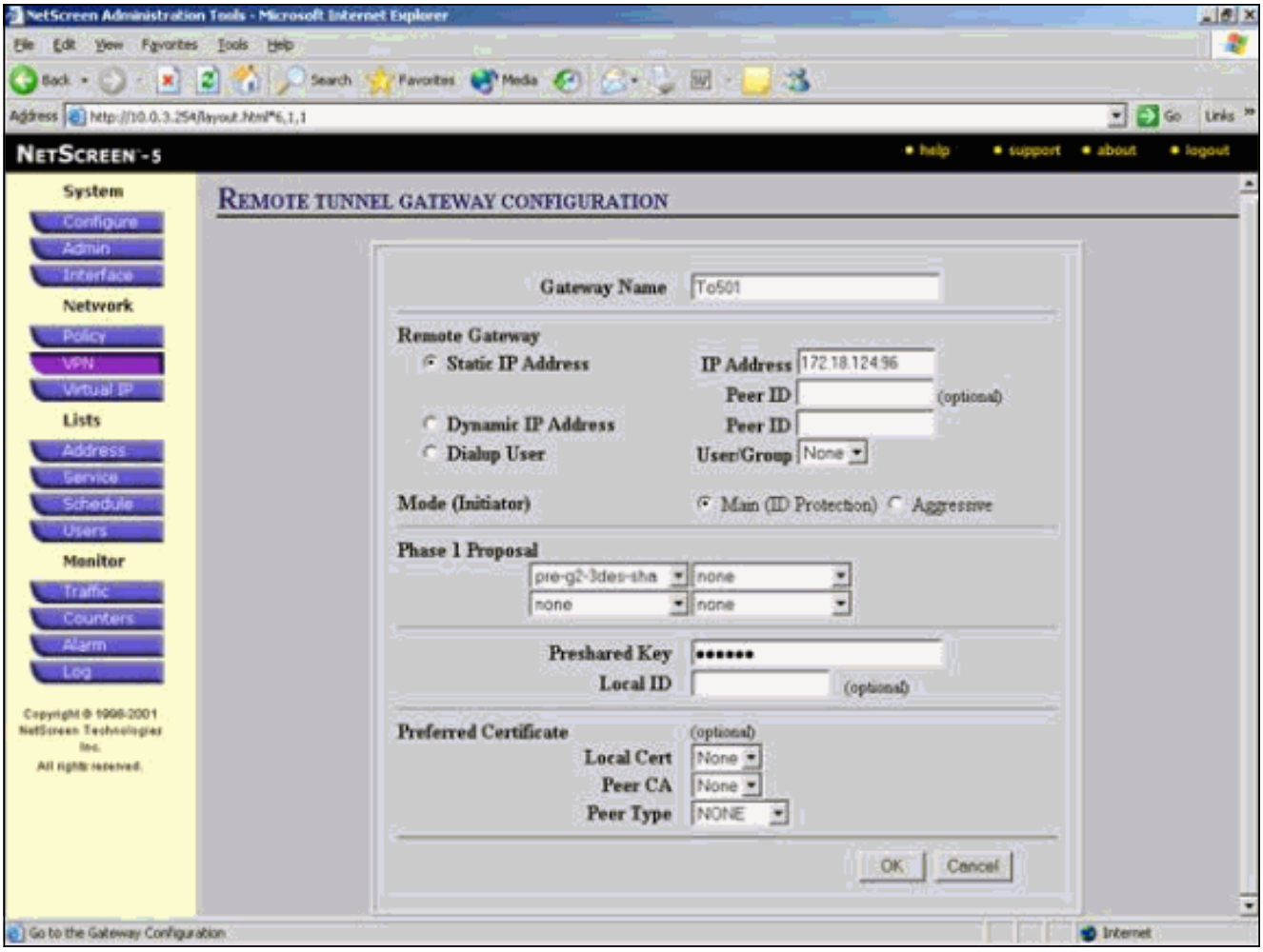
1. Seleccione **Listas > Dirección**, vaya a la ficha Confianza y haga clic en **Nueva dirección**.
2. Agregue la red interna NetScreen que está cifrada en el túnel y haga clic en **Aceptar**.**Nota:** Asegúrese de que la opción Confianza esté seleccionada.Este ejemplo utiliza la red 10.0.3.0 con una máscara de 255.255.255.0.



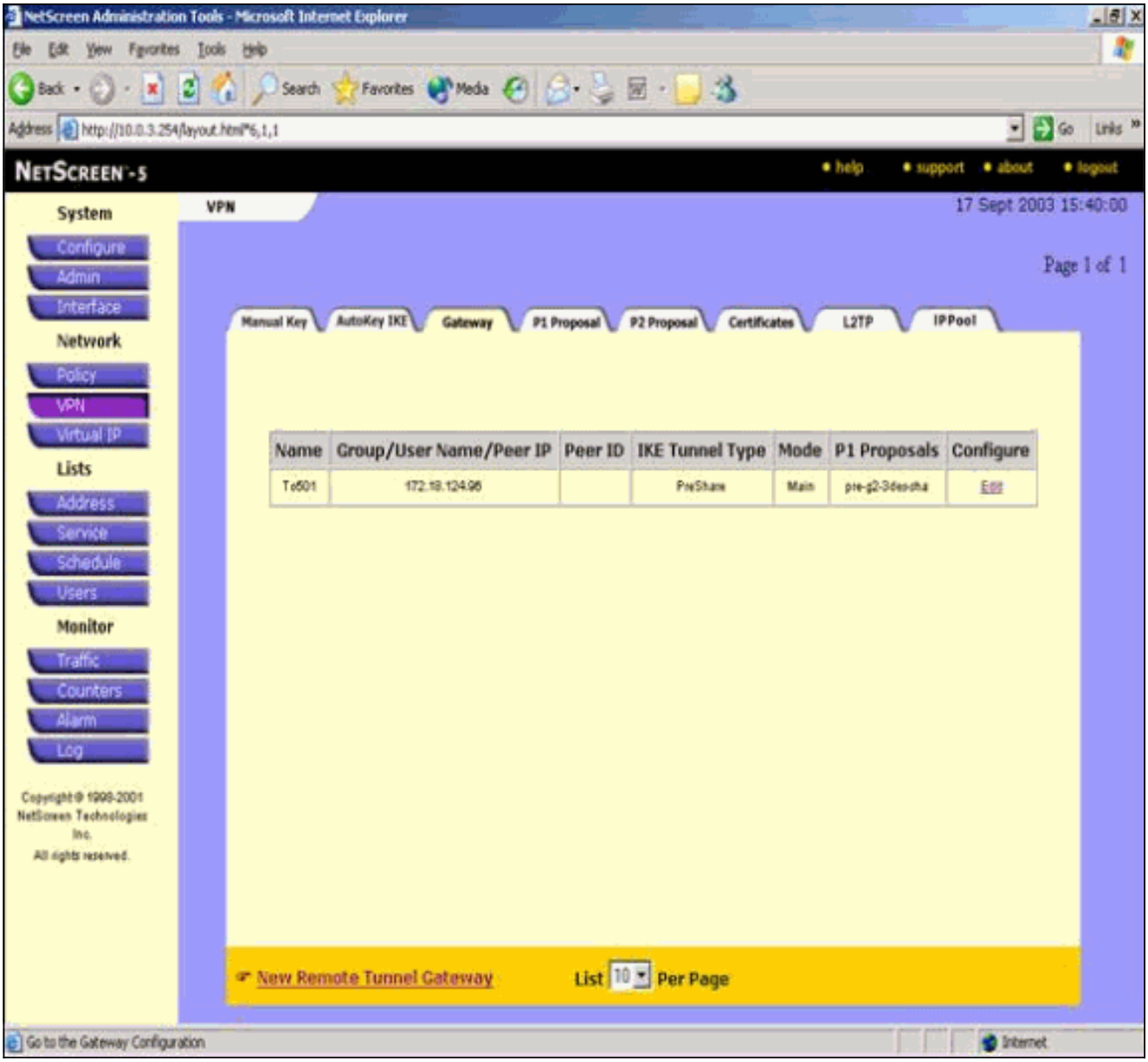
3. Seleccione **Listas > Dirección**, vaya a la ficha No fiable y haga clic en **Nueva dirección**.
4. Agregue la red remota que NetScreen Firewall utiliza cuando cifra los paquetes y haga clic en **Aceptar**.**Nota:** No utilice grupos de direcciones cuando configure una VPN en un gateway que no sea NetScreen. La interoperabilidad de VPN falla si utiliza grupos de direcciones. El gateway de seguridad que no es de NetScreen no sabe cómo interpretar el ID de proxy creado por NetScreen cuando se utiliza el grupo de direcciones.Hay un par de soluciones para esto:Separe los grupos de direcciones en entradas individuales de la libreta de direcciones. Especifique políticas individuales por entrada de la libreta de direcciones.Configure el ID de proxy para que sea 0.0.0.0/0 en el gateway que no sea NetScreen (dispositivo de firewall) si es posible.Este ejemplo utiliza la red 10.0.25.0 con una máscara de
255.255.255.0.



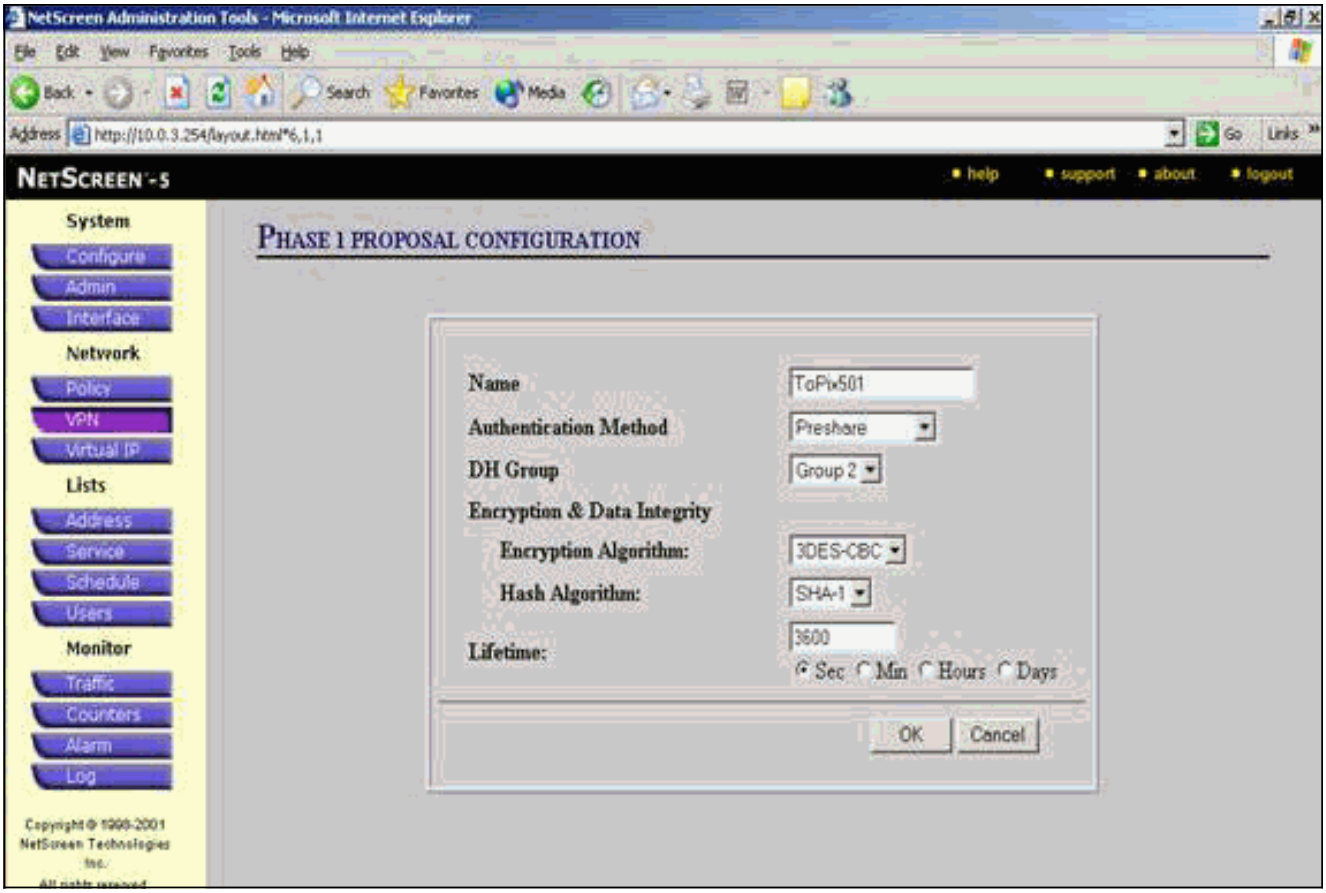
5. Seleccione **Network > VPN**, vaya a la ficha Gateway y haga clic en **New Remote Tunnel Gateway** para configurar el gateway VPN (políticas IPsec Fase 1 y Fase 2).
6. Utilice la dirección IP de la interfaz exterior del PIX para terminar el túnel y configure las opciones IKE de Fase 1 para enlazar. Haga clic en **Aceptar** cuando haya terminado.Este ejemplo utiliza estos campos y valores.**Nombre de la puerta de enlace:** To501**Dirección IP estática:** 172.18.124.96**Modo:** Principal (protección de ID)**Clave precompartida:** "testme"**Propuesta de la fase 1:** pre-g2-3des-
sha



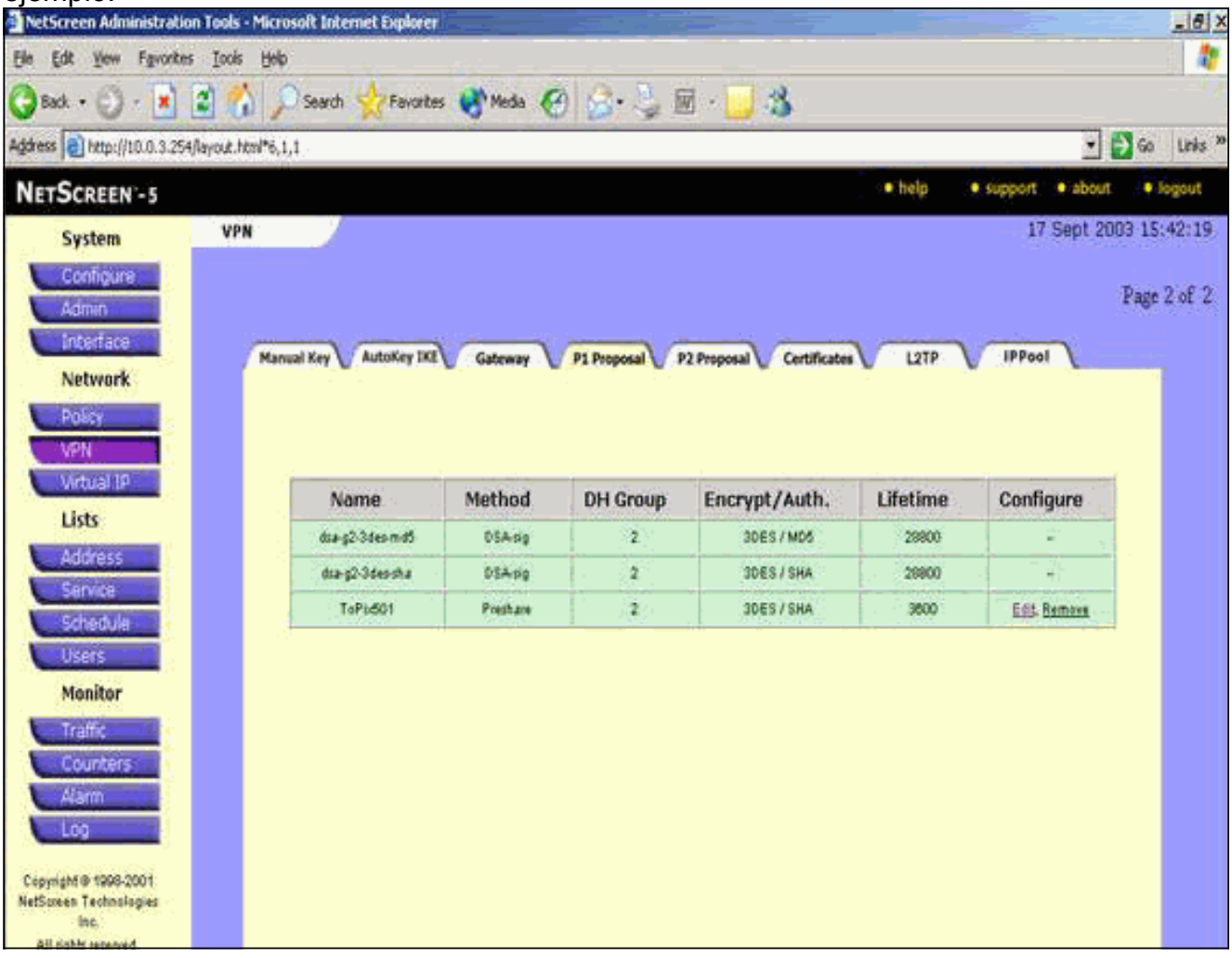
Cuando se crea correctamente el gateway de túnel remoto, aparece una pantalla similar a esta.



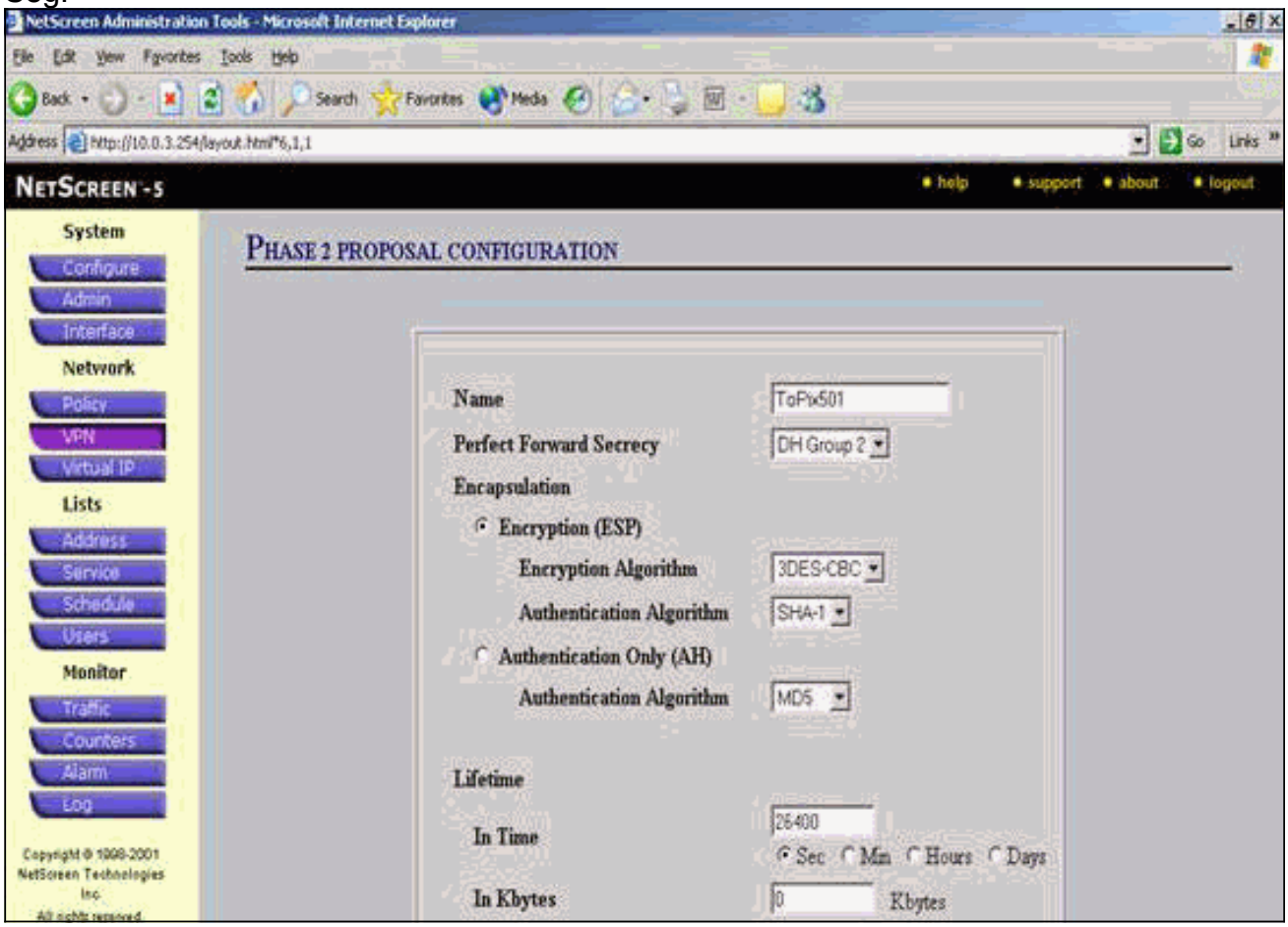
7. Vaya a la pestaña P1 Propuesta y haga clic en **Nueva propuesta de fase 1** para configurar la Propuesta 1.
8. Ingrese la información de configuración para la propuesta de la Fase 1 y haga clic en **Aceptar**.Este ejemplo utiliza estos campos y valores para el intercambio de Fase 1.**Nombre:** ToPix501**Autenticación:** Preshare**Grupo DH:** Grupo 2**Cifrado:** 3DES-CBC**Hash:** SHA-1**Vida útil:** 3600
seg.



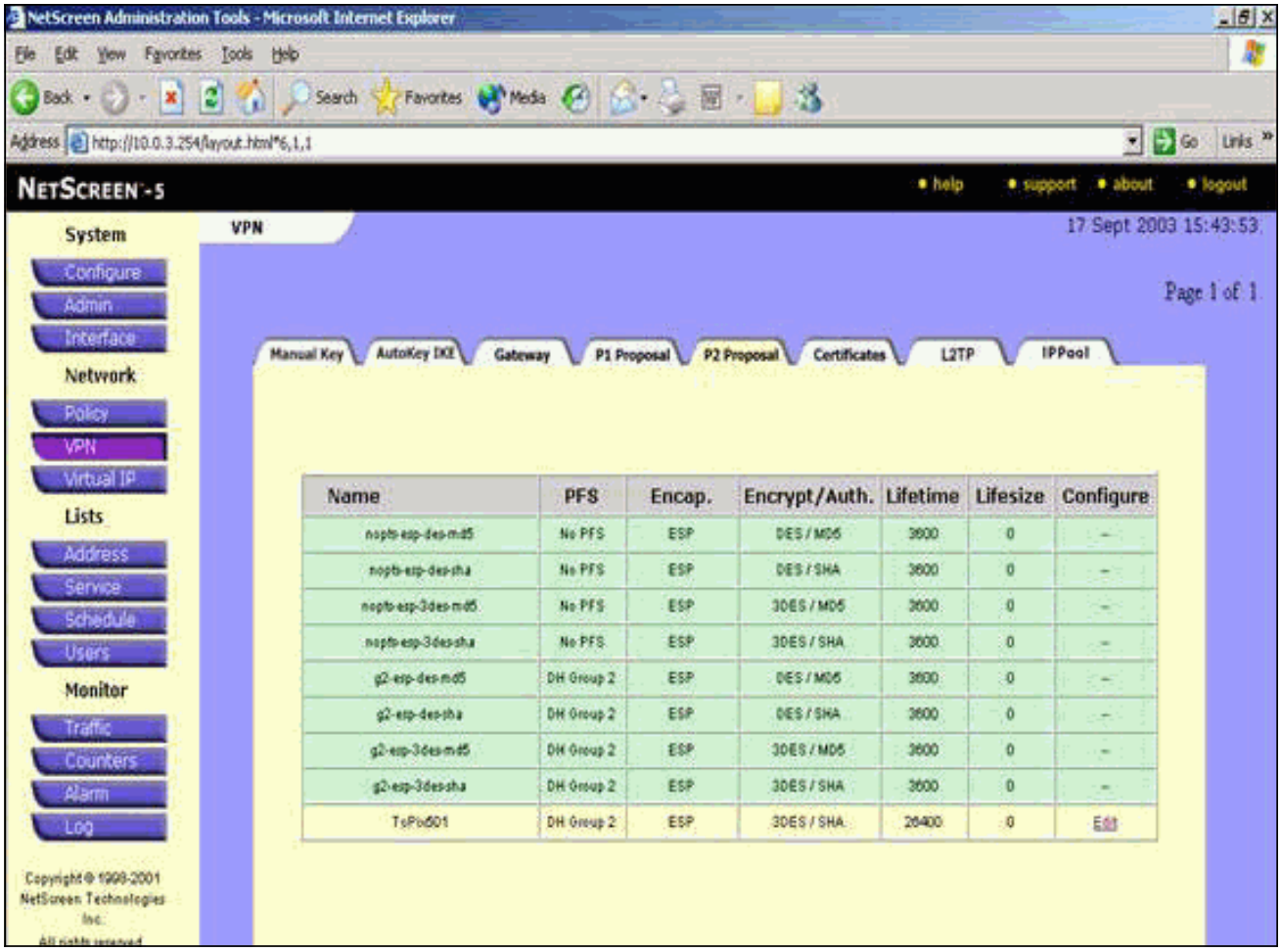
Cuando la Fase 1 se agrega correctamente a la configuración de NetScreen, aparece una pantalla similar a este
ejemplo.



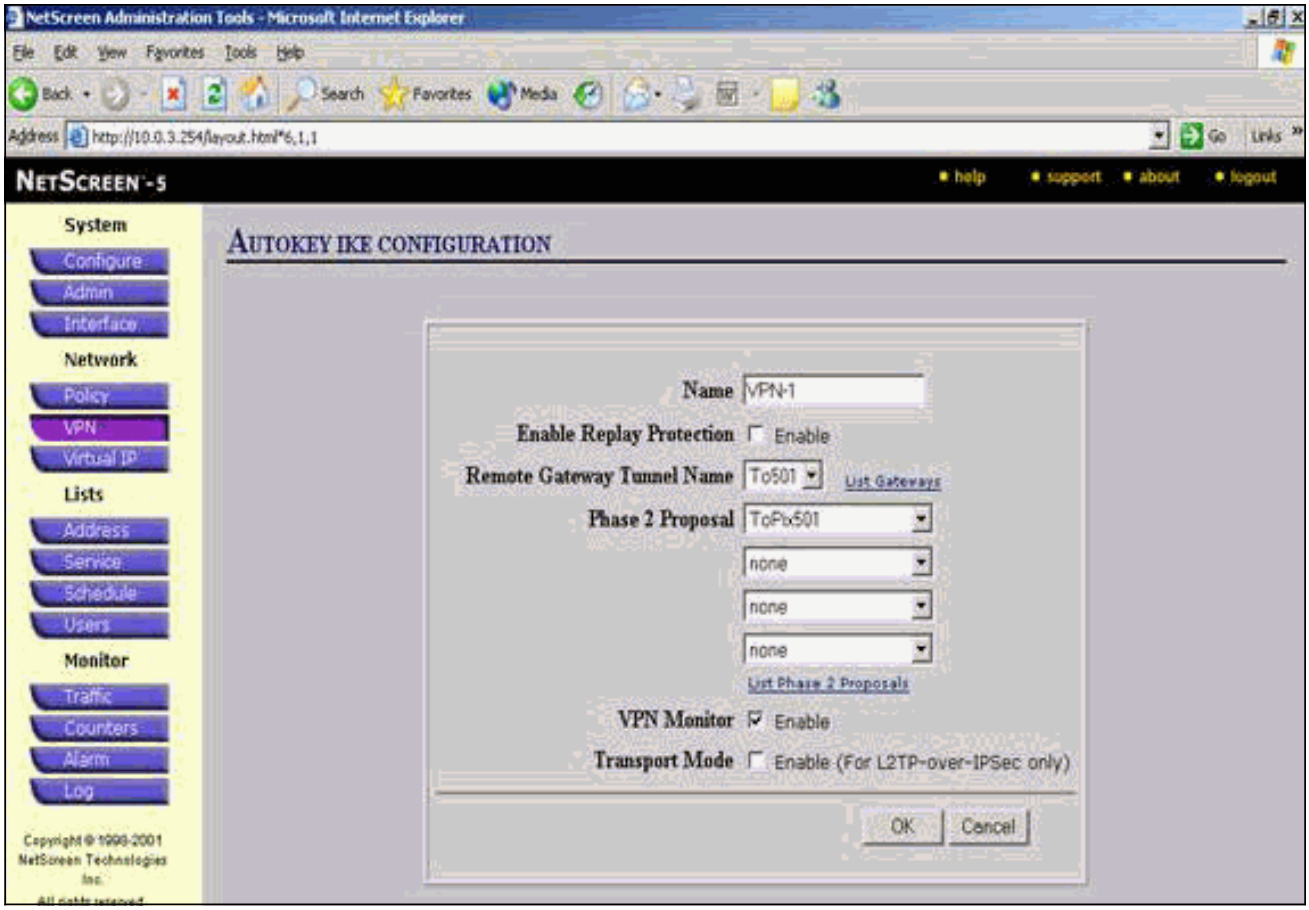
9. Vaya a la pestaña P2 Propuesta y haga clic en **Nueva propuesta de fase 2** para configurar la fase 2.
10. Ingrese la información de configuración para la Propuesta de Fase 2 y haga clic en **Aceptar**.Este ejemplo utiliza estos campos y valores para el intercambio de Fase 2.**Nombre:** ToPix501**Confidencialidad directa perfecta:** DH-2 (1024 bits)**Algoritmo de encripción:** 3DES-CBC**Algoritmo de autenticación:** SHA-1**Vida útil:** 26400
Seg.



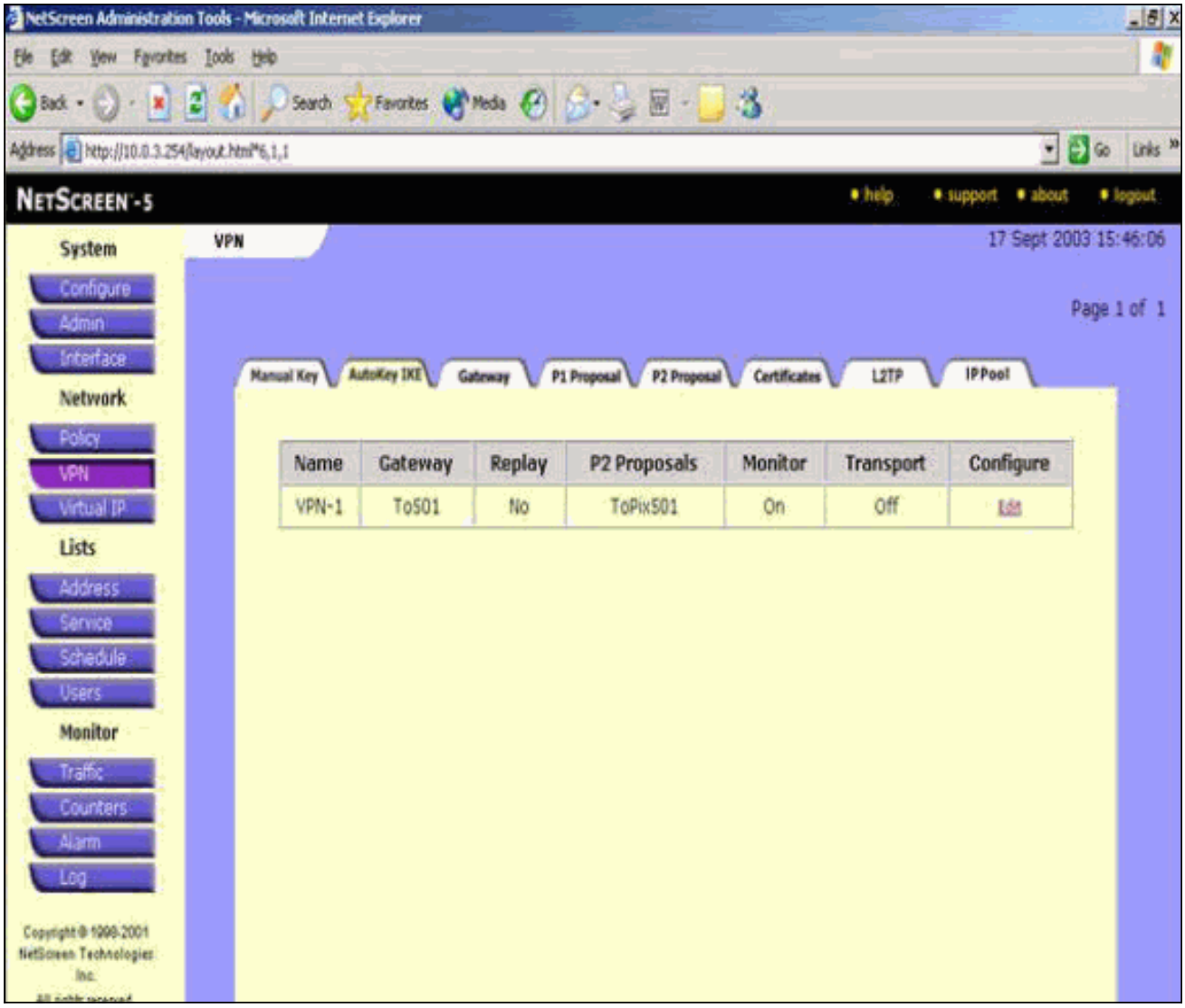
Cuando la Fase 2 se agrega correctamente a la configuración de NetScreen, aparece una pantalla similar a este
ejemplo.



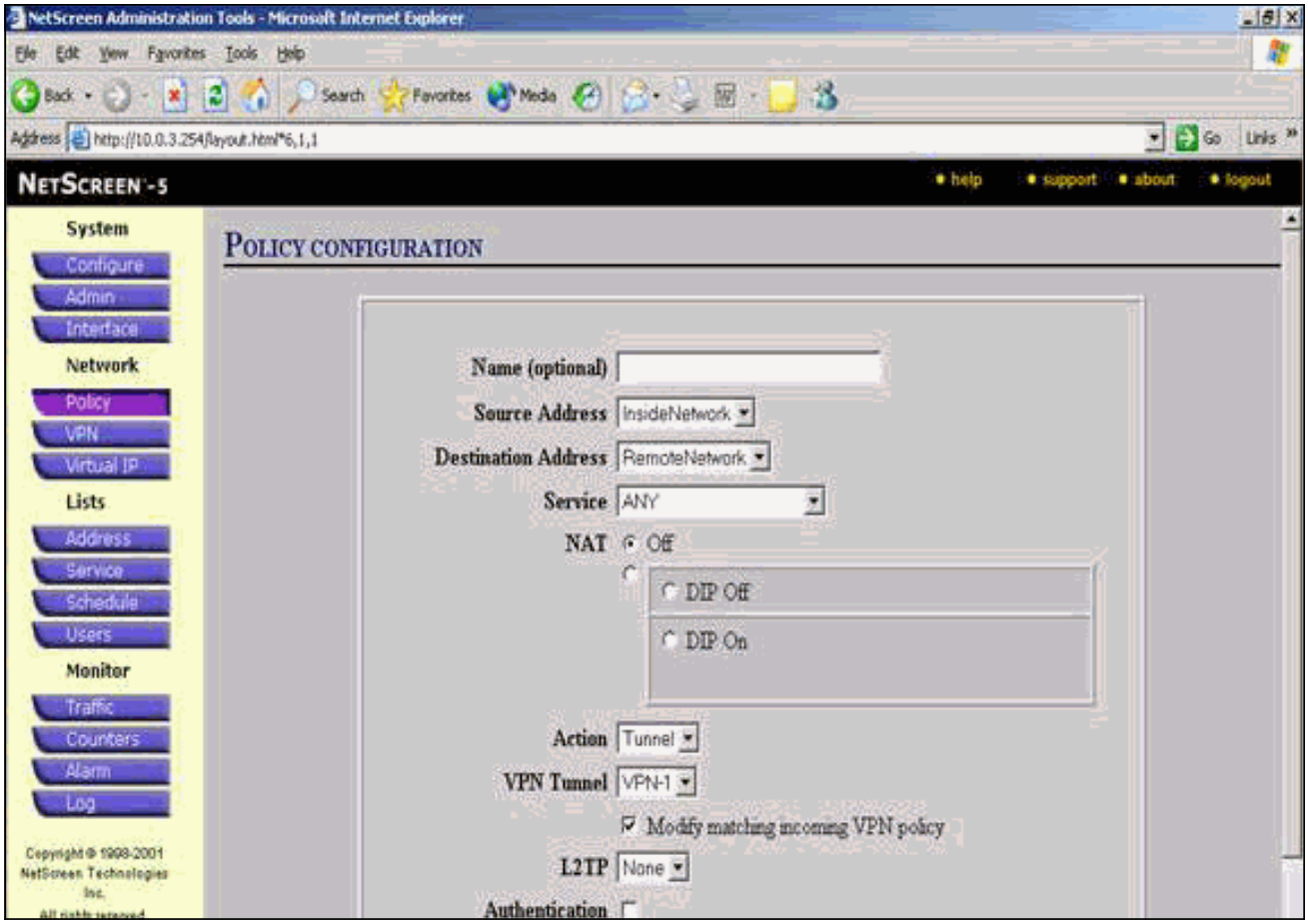
11. Seleccione la ficha **AutoKey IKE** y, a continuación, haga clic en **Nueva entrada IKE de AutoKey** para crear y configurar AutoKeys IKE.
12. Ingrese la información de configuración para AutoKey IKE y luego haga clic en **Aceptar**.Este ejemplo utiliza estos campos y valores para AutoKey IKE.**Nombre:** VPN-1**Nombre del túnel de la puerta de enlace remota:** To501(Anteriormente se creó en la ficha Puerta de enlace.)**Fase 2 Propuesta:** ToPix501(Anteriormente se creó en la pestaña Propuesta P2.)**Monitor VPN:** Habilitar(Esto habilita el dispositivo NetScreen para establecer trampas SNMP para monitorear la condición del monitor
VPN).



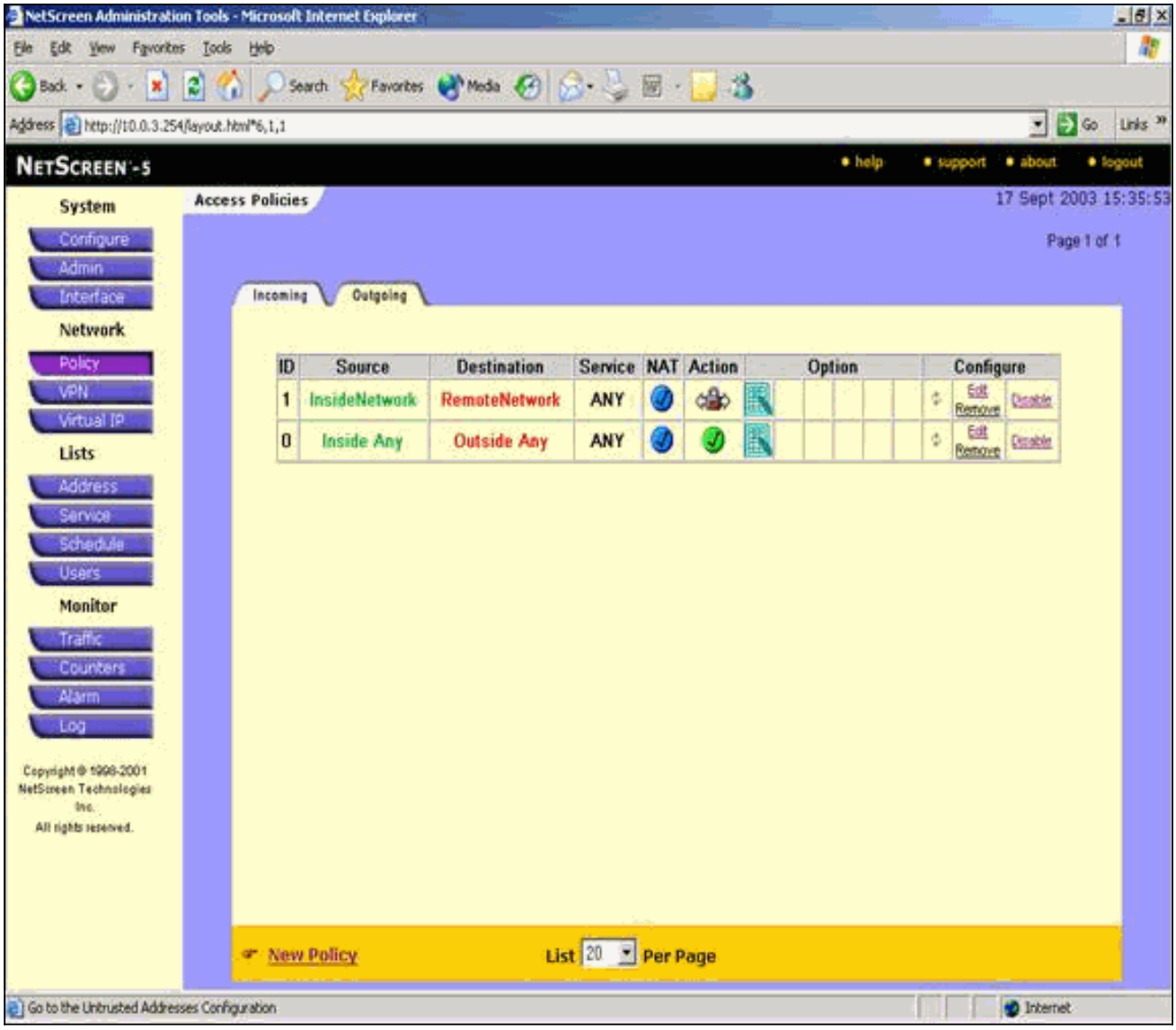
Cuando la regla VPN-1 se configura correctamente, aparece una pantalla similar a este ejemplo.



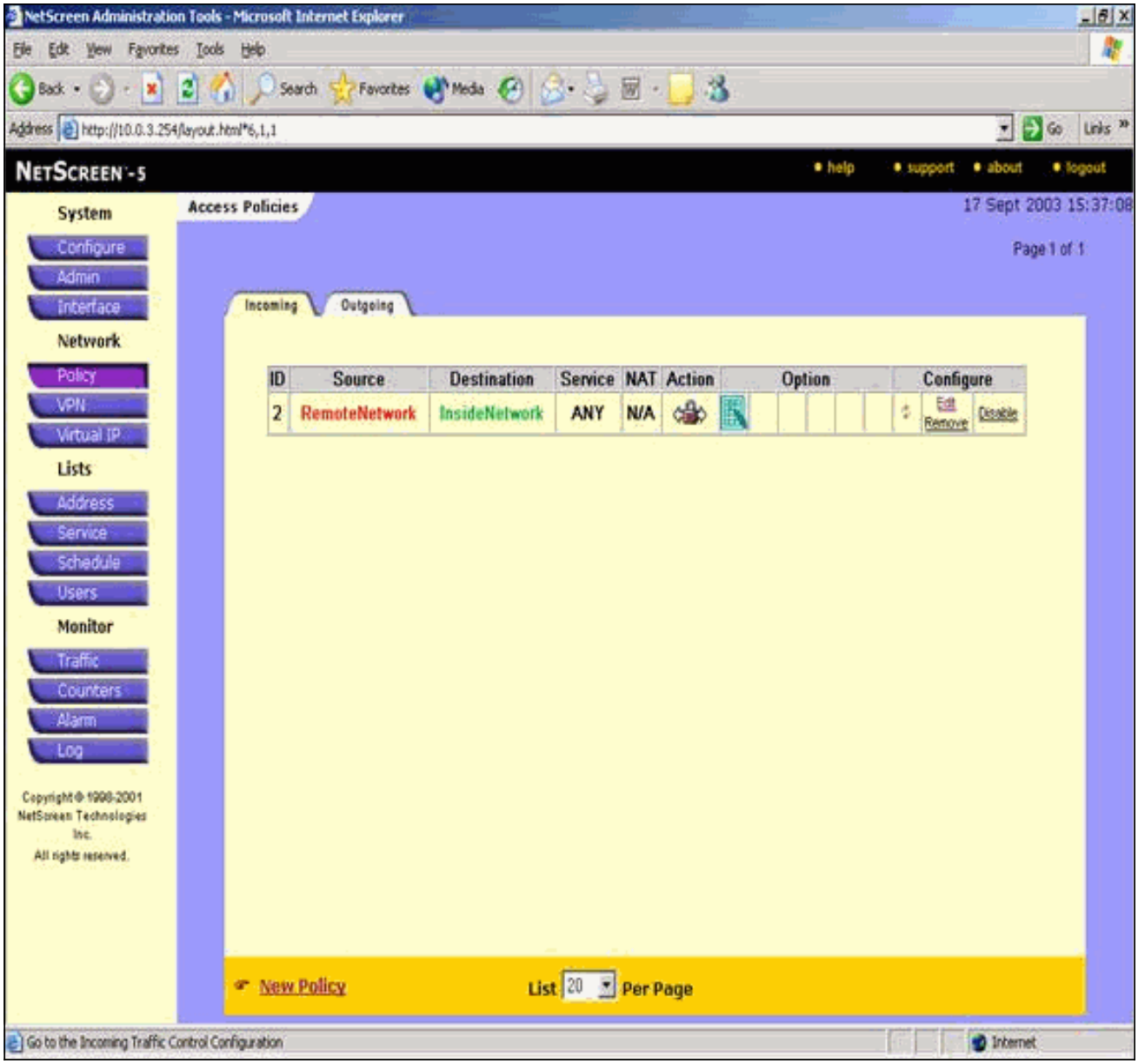
13. Seleccione **Network > Policy**, vaya a la ficha Outgoing y haga clic en **New Policy** para configurar las reglas que permiten el cifrado del tráfico IPsec.
14. Ingrese la información de configuración para la política y haga clic en **Aceptar**.Este ejemplo utiliza estos campos y valores para la política. El campo Nombre es opcional y no se utiliza en este ejemplo.**Dirección de la fuente:** Red interna(Anteriormente se había definido en la ficha Trusted (Confianza)).**dirección de destino:** RemoteNetwork(Anteriormente se definió en la ficha No fiable.)**Servicio:** cualquiera**Acción:** Túnel**Túnel VPN:** VPN-1(Anteriormente se definía como el túnel VPN en la ficha IKE de la clave automática.)**Modificar la política de VPN entrante que coincida:** Activado(Esta opción crea automáticamente una regla de entrada que coincide con el tráfico VPN de la red externa.)



15. Cuando se agrega la política, asegúrese de que la regla de VPN saliente esté primero en la lista de políticas. (La regla que se crea automáticamente para el tráfico entrante se encuentra en la ficha Entrantes.)Complete estos pasos si necesita cambiar el orden de las políticas:Haga clic en la ficha Saliente.Haga clic en las flechas circulares de la columna Configure para mostrar la ventana Move Policy Micro.Cambie el orden de las políticas para que la política VPN esté por encima del ID de política 0 (de modo que la política VPN esté en la parte superior de la
lista).



Vaya a la ficha Entrantes para ver la regla para el tráfico entrante.



Verificación

Esta sección proporciona información que puede utilizar para confirmar que su configuración funciona correctamente.

Comandos de verificación

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **ping**: diagnostica conectividad de red básica.
- **show crypto ipsec sa**: muestra las asociaciones de seguridad de la Fase 2.
- **show crypto isakmp sa — Muestra las asociaciones de seguridad de la fase 1.**

Salida de verificación

Aquí se muestra el ejemplo de salida de los comandos **ping** y **show**.

Este ping se inicia desde un host detrás del firewall 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
```

El resultado del comando **show crypto ipsec sa** se muestra aquí.

```
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:
```

La salida del comando **show crypto isakmp sa** se muestra aquí.

```
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

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos **debug**.

- **debug crypto engine**: muestra mensajes sobre motores criptográficos.
- **debug crypto ipsec—Muestra información acerca de eventos de IPSec.**
- **debug crypto isakmp — Muestra mensajes acerca de eventos IKE.**

Ejemplo de resultado del comando debug

Aquí se muestra el ejemplo de **salida de debug** del Firewall PIX.

```
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
```

Información Relacionada

- Negociación IPSec/Protocolos IKE
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems