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.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El firewall NetScreen se configura con los IP Addresses en las interfaces de la confianza/del untrust.
- La Conectividad se establece a Internet.

Componentes Utilizados

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

- Versión 6.3(1) del Software PIX Firewall
- La última revisión del NetScreen

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando,

asegúrese de haber comprendido el impacto que puede tener cualquier comando.

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 Tool (clientes registrados solamente) 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

Configure el firewall PIX

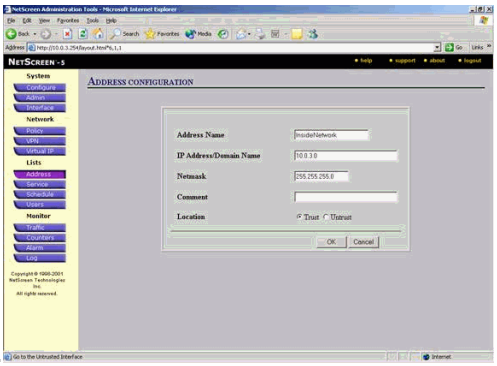
Firewall PIX
PIX Version 6.3(1)interface ethernet0 10basetinterface ethernet1 100fullnameif ethernet0 outside security0nameif ethernet1 inside security100enable password 8Ry2YjIyt7RRXU24 encryptedpasswd 2KFQnbNIdI.2KYOU encryptedhostname pixfirewalldomain-name cisco.comfixup protocol ftp 21fixup protocol 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
```

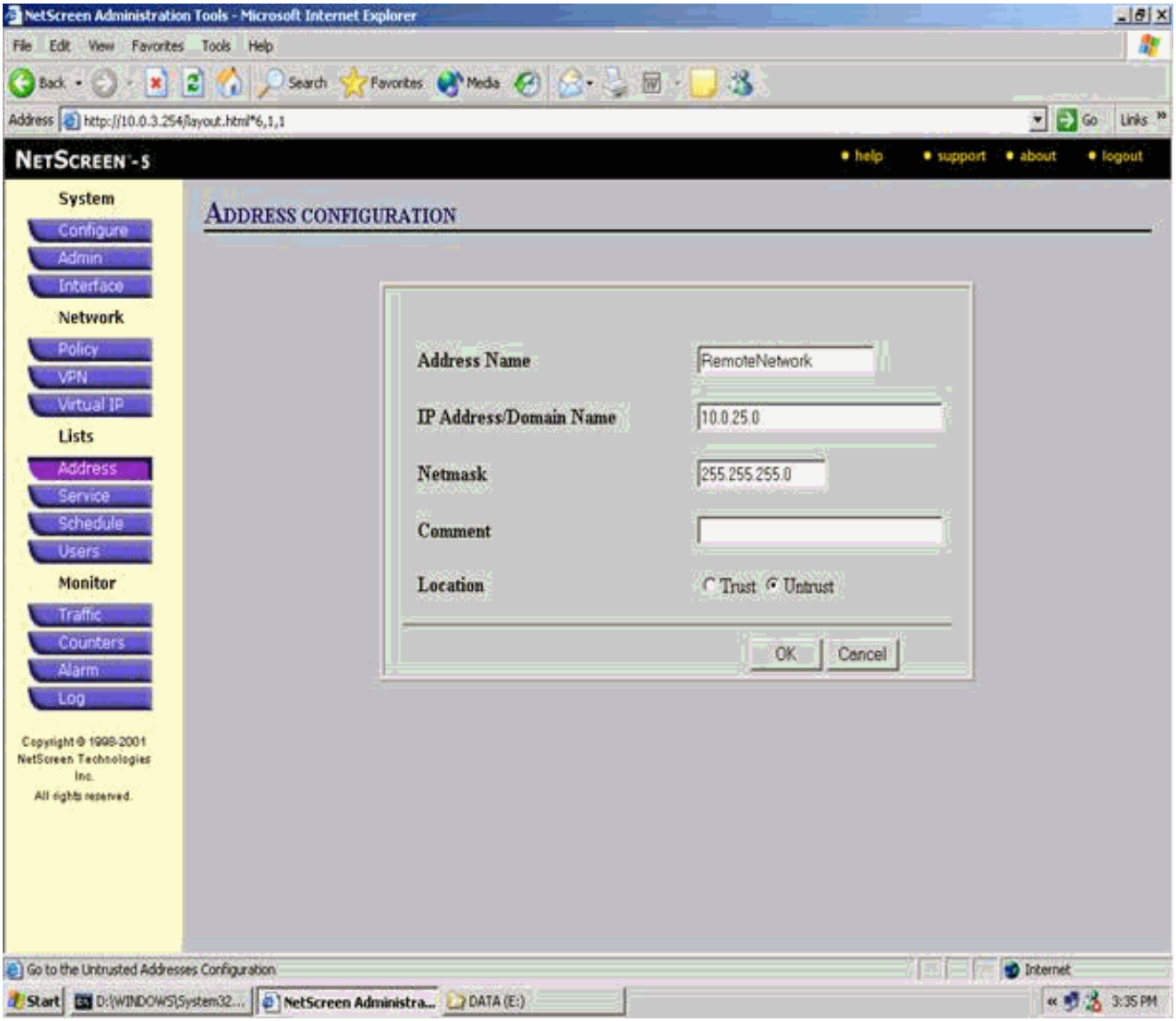
Configure el firewall NetScreen

Complete estos pasos para configurar el firewall NetScreen.

1. Seleccione el **Lists (Listas) > Address (Dirección)**, vaya a la lengueta de confianza, y haga clic el **nuevo direccionamiento**.
2. Agregue la red interna del NetScreen que se cifra en el túnel y haga clic la **AUTORIZACIÓN**.**Nota:** Asegúrese de que la opción de la confianza esté seleccionada.Este ejemplo utiliza la red 10.0.3.0 con una máscara de 255.255.255.0.



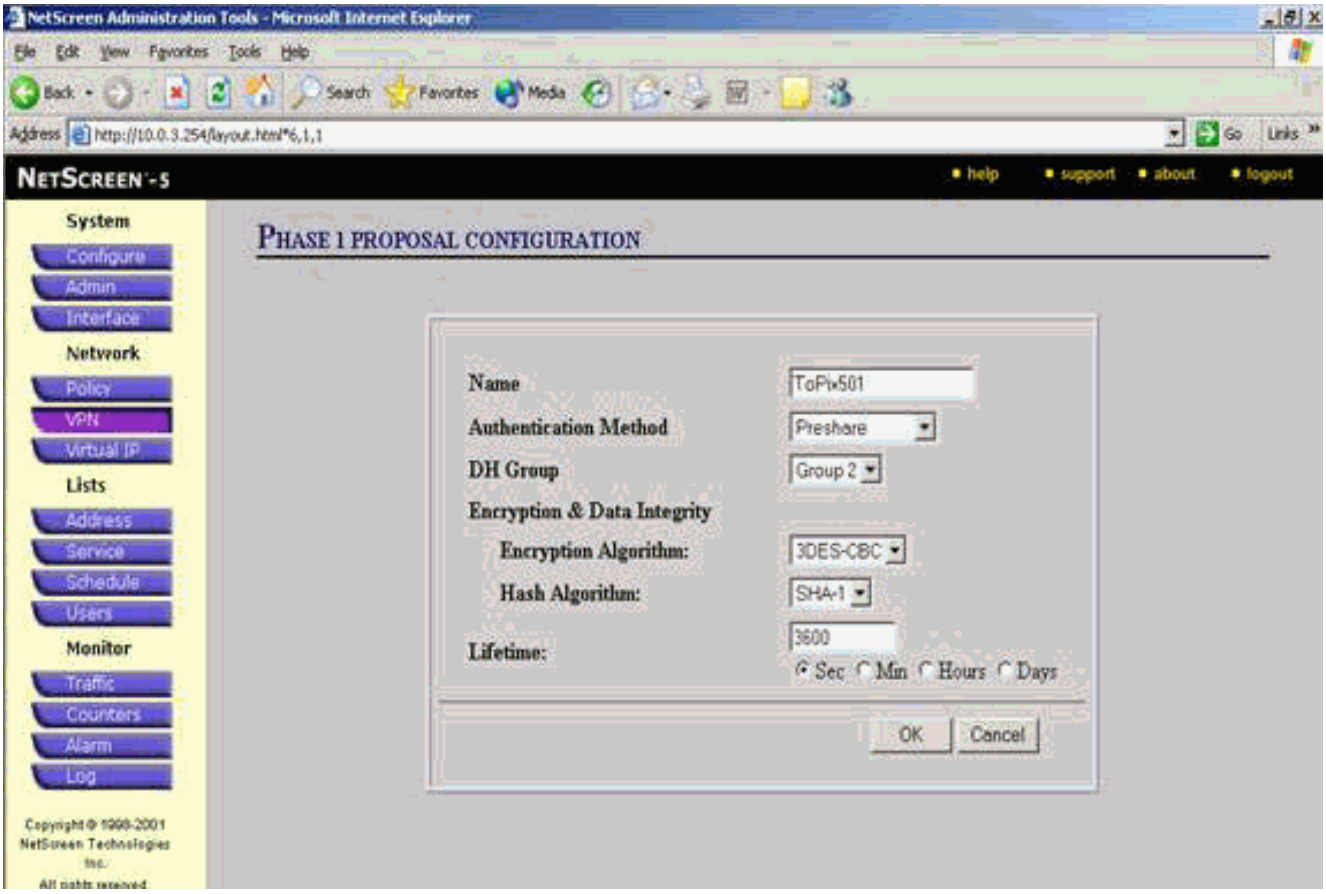
3. Seleccione el **Lists (Listas) > Address (Dirección)**, vaya a la lengueta untrusted, y haga clic el **nuevo direccionamiento**.
4. Agregue la red remota que el firewall NetScreen utiliza cuando cifra los paquetes y hace clic la **AUTORIZACIÓN.Nota:** No utilice a los grupos de dirección cuando usted configura un VPN no a un gateway del NetScreen. La interoperabilidad de VPN falla si usted utiliza a los grupos de dirección. No el gateway de seguridad del NetScreen no sabe interpretar el ID de proxy creado por el NetScreen cuando utilizan al grupo de dirección.Hay pares de las soluciones alternativas para esto:Separe a los grupos de dirección en las entradas de la libreta de direcciones individuales. Especifique las políticas individuales en a por la base de la entrada de la libreta de direcciones.Configure el ID de proxy para ser 0.0.0.0/0 en no el gateway del NetScreen (dispositivo de firewall) si es posible.Este ejemplo utiliza la red 10.0.25.0 con una máscara de 255.255.255.0.



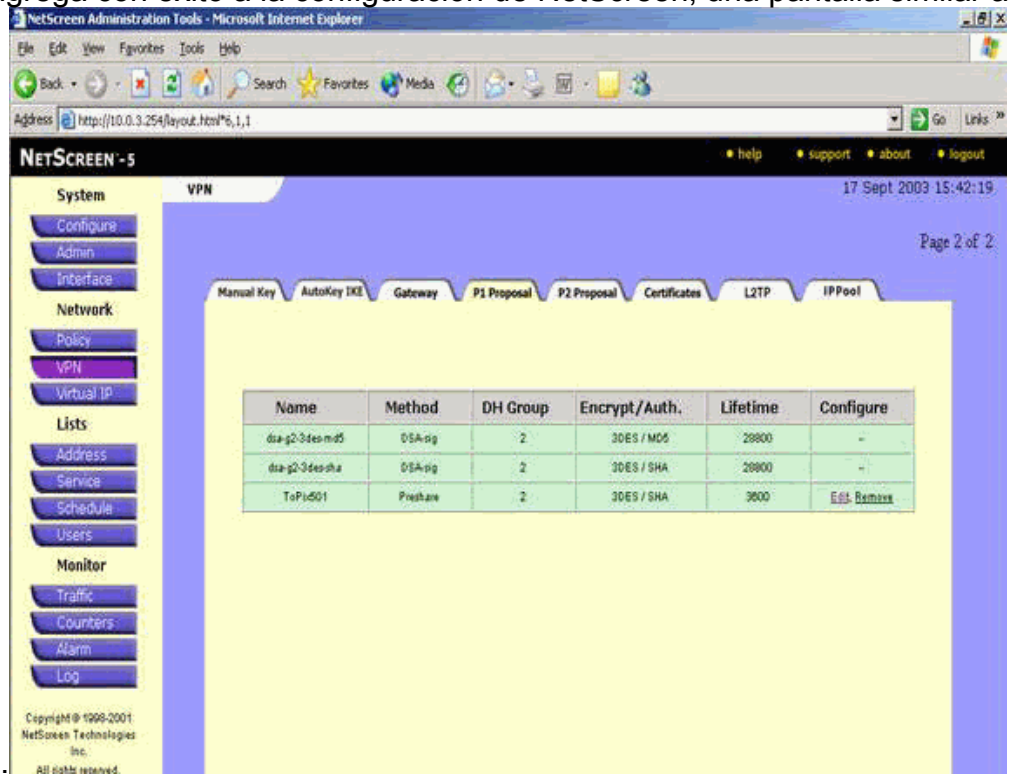
5. Seleccione el **Network (Red) > VPN**, vaya a la lengueta del gateway, y haga clic el **nuevo gateway del túnel remoto** para configurar el gateway de VPN (las directivas del IPSec de la fase 1 y de la fase 2).
6. Utilice la dirección IP de la interfaz exterior PIX para terminar el túnel, y configure las opciones IKE de la fase 1 de atar. Haga Click en OK cuando le acaban.Este ejemplo utiliza estos campos y valores.**Nombre del gateway:** To501**IP Address estático:** 172.18.124.96**Modo:** Tubería (protección de ID)**Clave del preshared:** “testme”**Oferta de la fase 1:** pre-g2-3des-sha Cuando el gateway del túnel remoto se crea con éxito, una

pantalla similar a esto aparece.

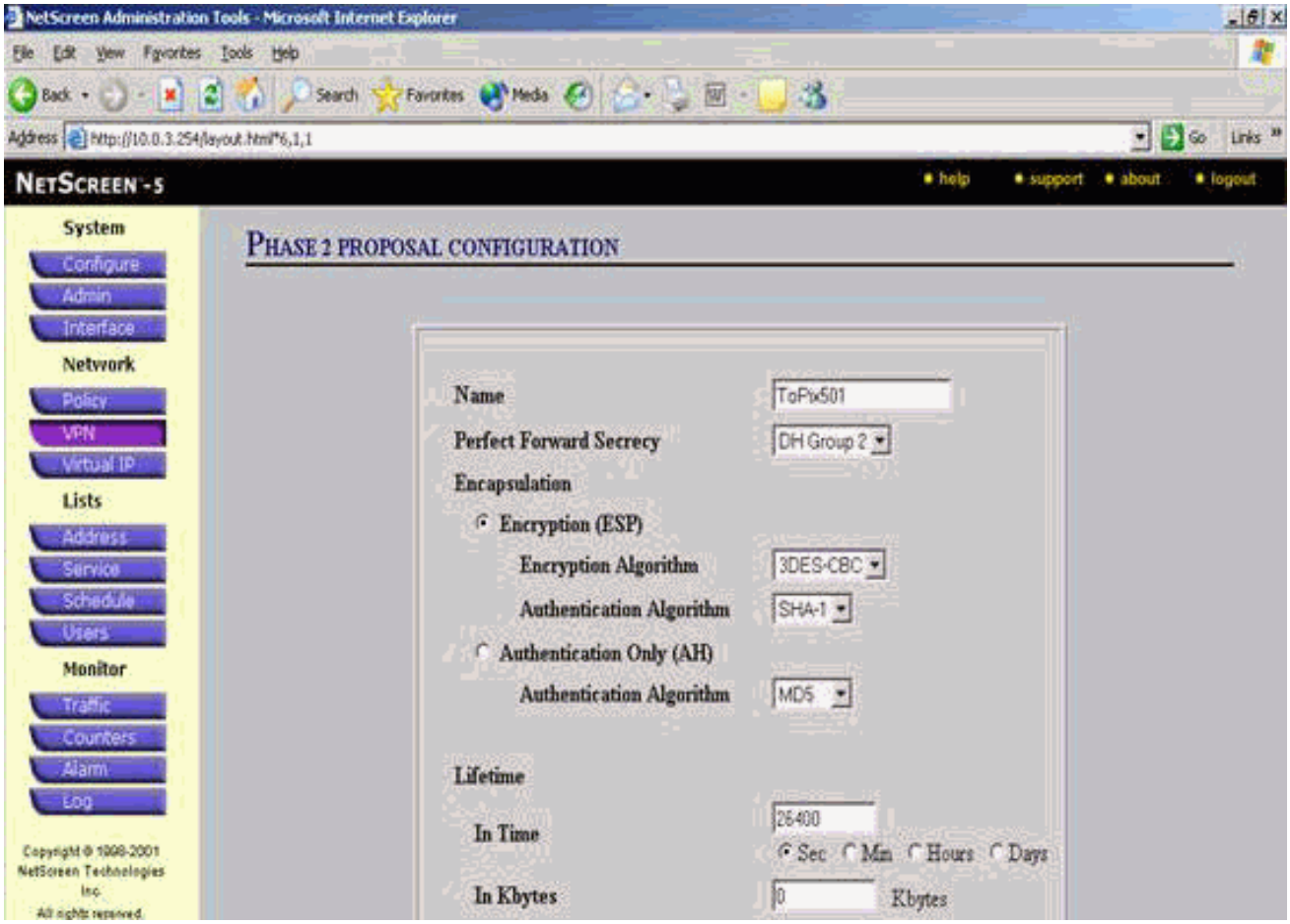
7. Vaya a la lengueta de la oferta P1 y haga clic la **nueva oferta de la fase 1** para configurar la oferta 1.
8. Ingrese la información de la configuración para la oferta de la fase 1 y haga clic la **AUTORIZACIÓN**.Este ejemplo utiliza estos campos y valores para el intercambio de la fase 1.**Nombre:** ToPix501**Autenticación:** Preshare**Grupo DH:** Group2**Cifrado:** 3DES-CBC**Hash:** SHA-1**Vida útil:** Sec
3600.



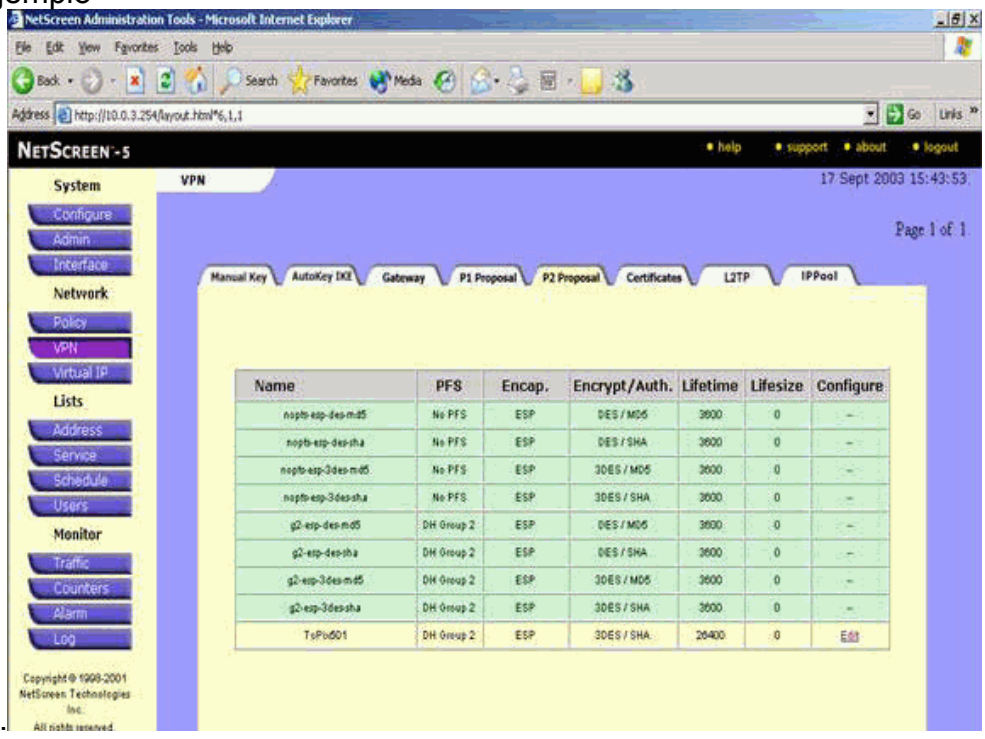
Cuando la fase 1 se agrega con éxito a la configuración de NetScreen, una pantalla similar a este ejemplo aparece.



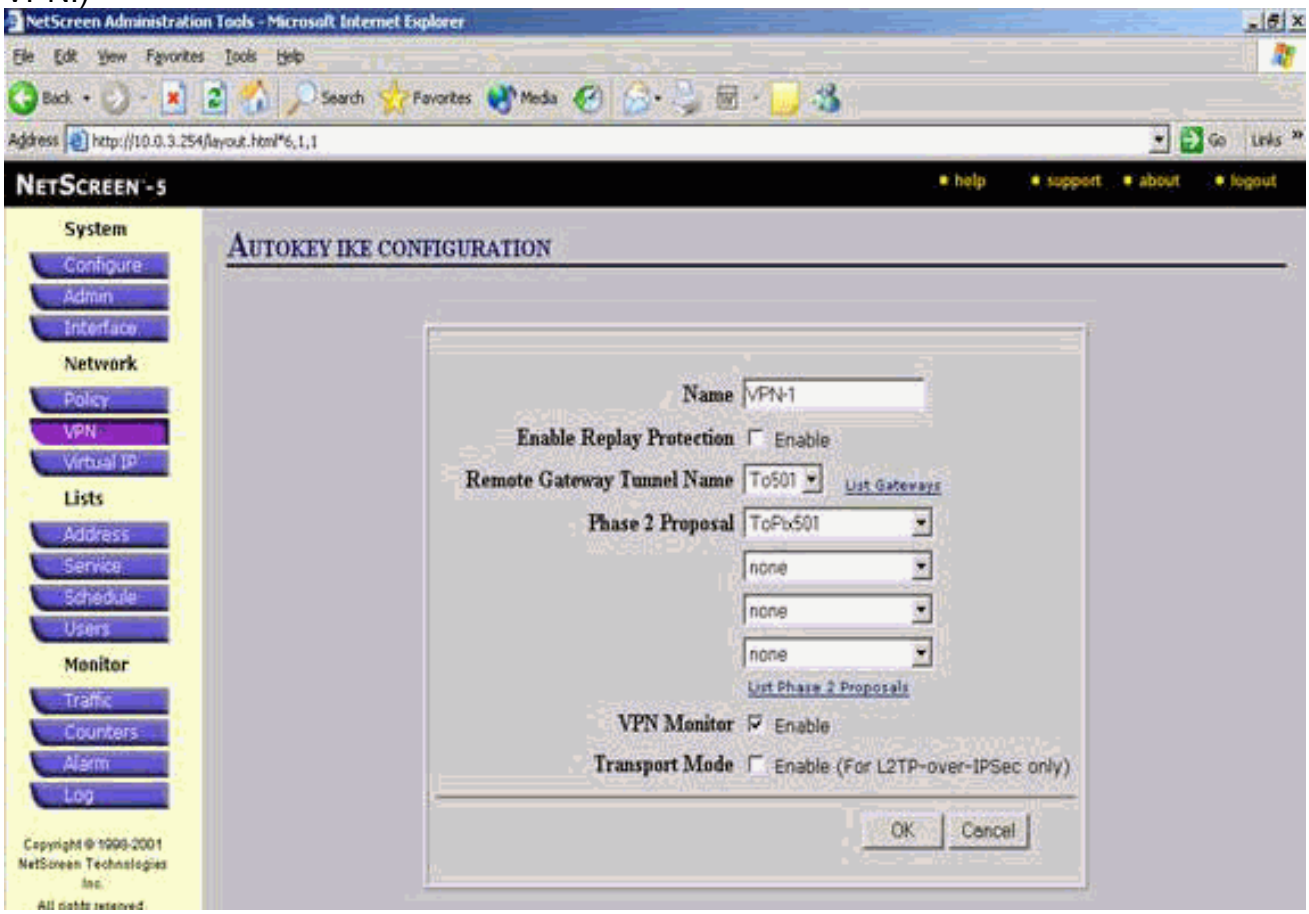
9. Vaya a la lengueta de la oferta P2 y haga clic la **nueva oferta de la fase 2** para configurar la fase 2.
10. Ingrese la información de la configuración para la oferta de la fase 2 y haga clic la **AUTORIZACIÓN**.Este ejemplo utiliza estos campos y valores para el intercambio de la fase 2.**Nombre:** ToPix501**Perfecta reserva hacia adelante:** DH-2 (1024 bits)**Algoritmo de encripción:** 3DES-CBC**Algoritmo de autenticación:** SHA-1**Vida útil:** Sec 26400



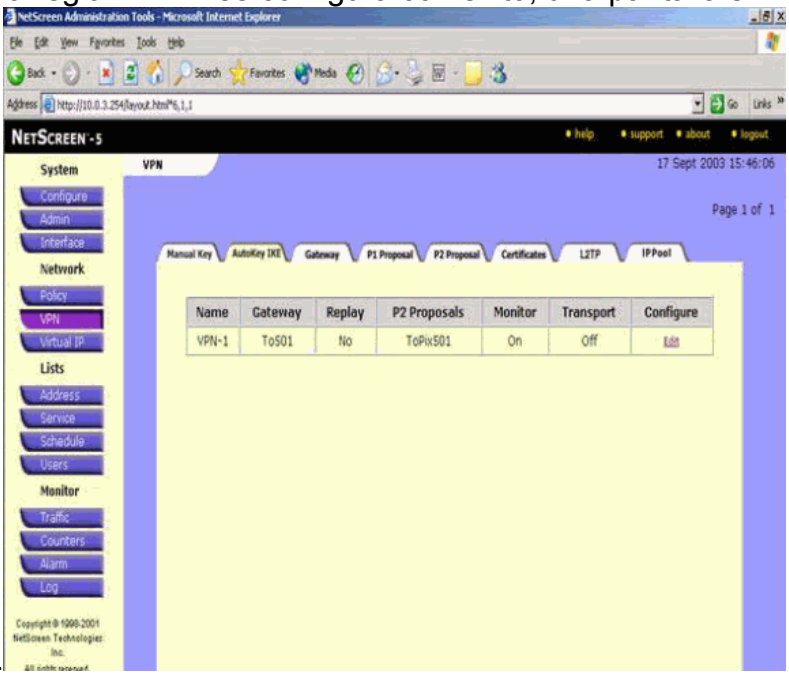
Cuando la fase 2 se agrega con éxito a la configuración de NetScreen, una pantalla similar a este ejemplo aparece.



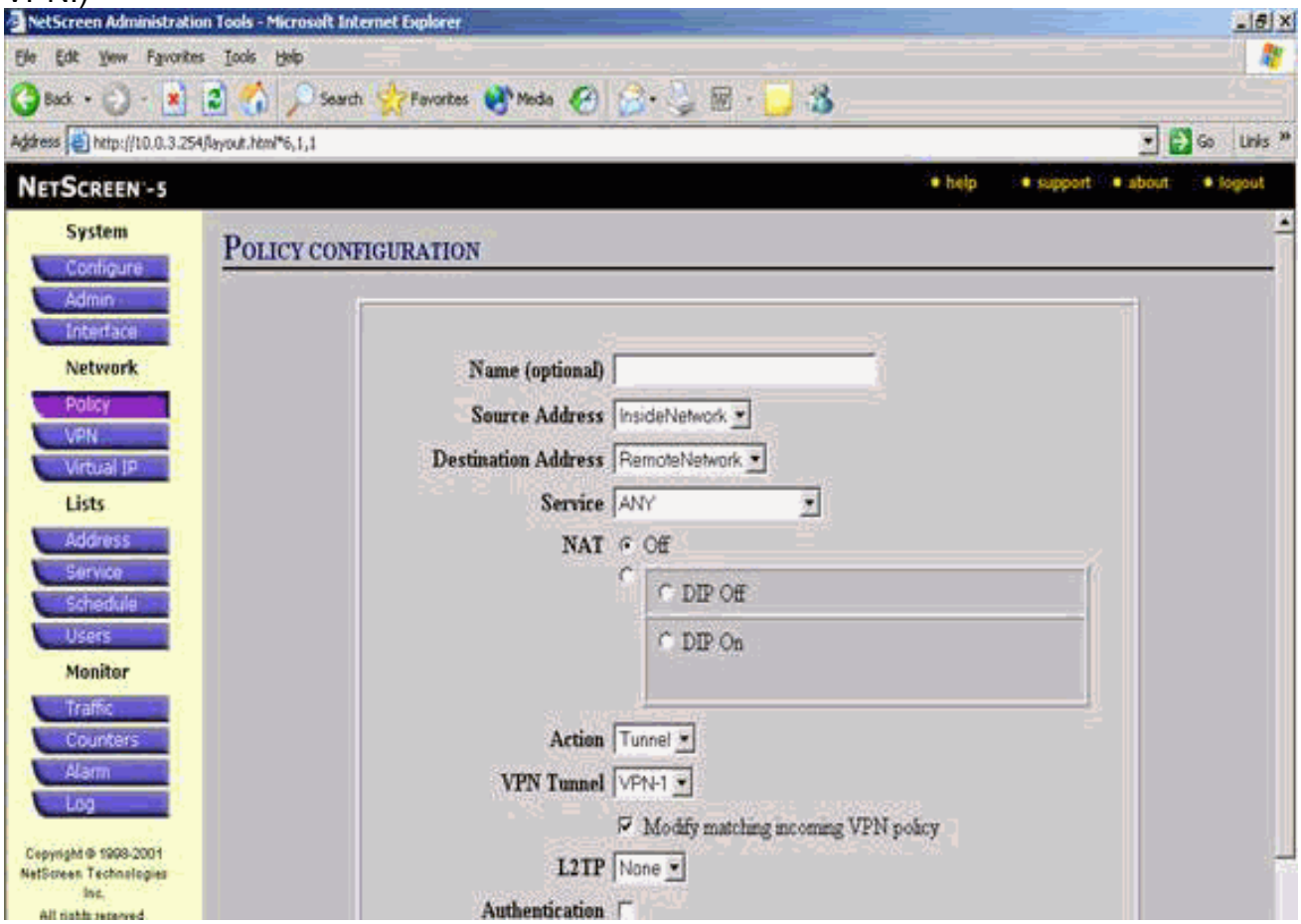
11. Seleccione la lengueta del **AutoKey IKE**, y después haga clic **nuevo entrada AutoKey IKE** para crear y para configurar AutoKeys IKE.
12. Ingrese la información de la configuración para el AutoKey IKE, y después haga clic la **AUTORIZACIÓN**.Este ejemplo utiliza estos campos y valores para el AutoKey IKE.**Nombre:** VPN-1**Nombre de túnel del gateway remoto:** To501(Esto fue creada previamente en el gateway cuadro)**Oferta de la fase 2:** ToPix501(Esto fue creada previamente en P2 la oferta cuadro)**Monitor VPN:** Habilitar(Esto habilita dispositivo NetScreen (Pantalla de red) para fijar los desvíos del protocolo administración de red simple [SNMP] para monitorear la condición del monitor
VPN.)



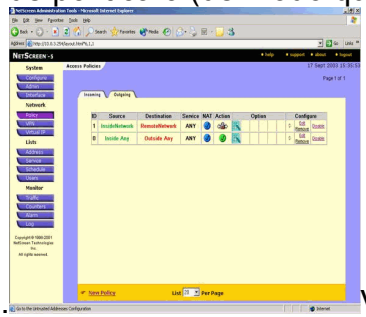
Cuando la regla VPN-1 se configura con éxito, una pantalla similar a este ejemplo aparece.



13. Seleccione el **Network (Red) > Policy (Política)**, vaya a la lengueta saliente, y haga clic la **nueva directiva** para configurar las reglas que permiten el cifrado del tráfico IPSec.
14. Ingrese la información de la configuración para la directiva y haga clic la **AUTORIZACIÓN**.Este ejemplo utiliza estos campos y valores para la directiva. El campo de nombre es opcional y no se utiliza en este ejemplo.**Dirección de la fuente:** InsideNetwork(Esto fue definida previamente en el cuadro de confianza)**Dirección destino:** RemoteNetwork(Esto fue definida previamente bajo cuadro untrusted)**Servicio:** Ningunos**Acción:** Túnel**Túnel VPN:** VPN-1(Esto fue definida previamente como el túnel VPN en el AutoKey IKE cuadro)**Modify que corresponde con la política del VPN entrante:** Marcado(Esta opción crea automáticamente una regla entrante que haga juego el tráfico de la red externa
VPN.)



15. Cuando se agrega la directiva, asegúrese de que la regla saliente VPN sea primera en la lista de directivas. (La regla que se crea automáticamente para el tráfico entrante está en el cuadro entrante)Complete estos pasos si usted necesita cambiar la orden de las directivas:Haga clic la lengueta saliente.Haga clic las flechas circulares en la columna de la configuración para visualizar la ventana del micrófono de la directiva del movimiento.Cambie la orden de las directivas de modo que la política del VPN esté sobre el ID de política 0 (de modo que la política del VPN esté en la cima de la



lista).Vaya a la lengueta entrante para ver la regla para el tráfico

entrante.

Verificación

Esta sección proporciona la información que usted puede utilizar para confirmar su configuración trabaja 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 la conectividad de red básica.
- ¿**muestre IPSec crypto sa**? Muestra a fase 2 asociaciones de seguridad.
- ¿**muestre isakmp crypto sa**? Muestra las asociaciones de seguridad de la fase 1.

Salida de la verificación

La salida de muestra de los **comandos ping y show** se muestra aquí.

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

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

```
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:
```

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

```
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
```

Troubleshooting

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

configuración.

Comandos para resolución de problemas

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

- ¿**motor del debug crypto**? Visualiza los mensajes sobre los motores de criptografía.
- ¿**IPSec del debug crypto**? Visualiza la información sobre los eventos del IPSec.
- ¿**isakmp del debug crypto**? Muestra mensajes sobre los eventos IKE.

Ejemplo de resultado del comando debug

El ejemplo de salida del debug del firewall PIX se muestra aquí.

```
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
```

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