Configuring an IPsec LAN−to−LAN Tunnel Between the Cisco PIX Firewall and a NetScreen Firewall

Document ID: 45423

Contents

Introduction
Prerequisites
Requirements
Components Used
Conventions
Configure
Network Diagram
Configurations
Verify
Verification Commands
Verification Output
Troubleshoot
Troubleshooting Commands
Sample Debug Output
Related Information

Introduction

This document describes the necessary procedure used to create an IPsec LAN−to−LAN tunnel between a Cisco PIX Firewall and a NetScreen Firewall with the latest software. There is a private network behind each device that communicates to the other firewall through the IPsec tunnel.

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- The NetScreen Firewall is configured with the IP addresses on the trust/untrust interfaces.
- Connectivity is established to the Internet.

Components Used

The information in this document is based on these software and hardware versions:

- PIX Firewall Software Version 6.3(1)
- NetScreen Latest Revision

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

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:

Configurations

This document uses these configurations:

- PIX Firewall
- NetScreen Firewall

Configure the PIX Firewall

PIX Firewall

```
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
```

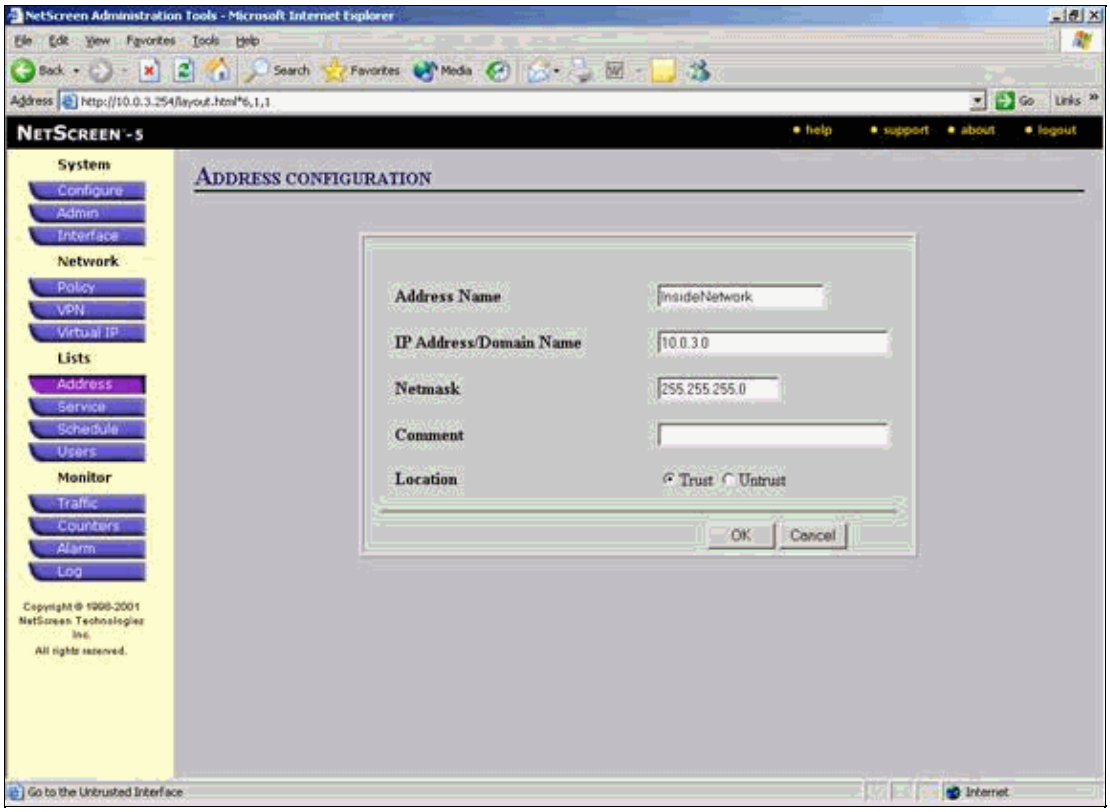
Configure the NetScreen Firewall

Complete these steps in order to configure the NetScreen Firewall.

1. Select **Lists > Address**, go to the Trusted tab, and click **New Address**.
2. Add the NetScreen internal network that is encrypted on the tunnel and click **OK**.

   Note: Ensure that the Trust option is selected.

   This example uses network 10.0.3.0 with a mask of 255.255.255.0.



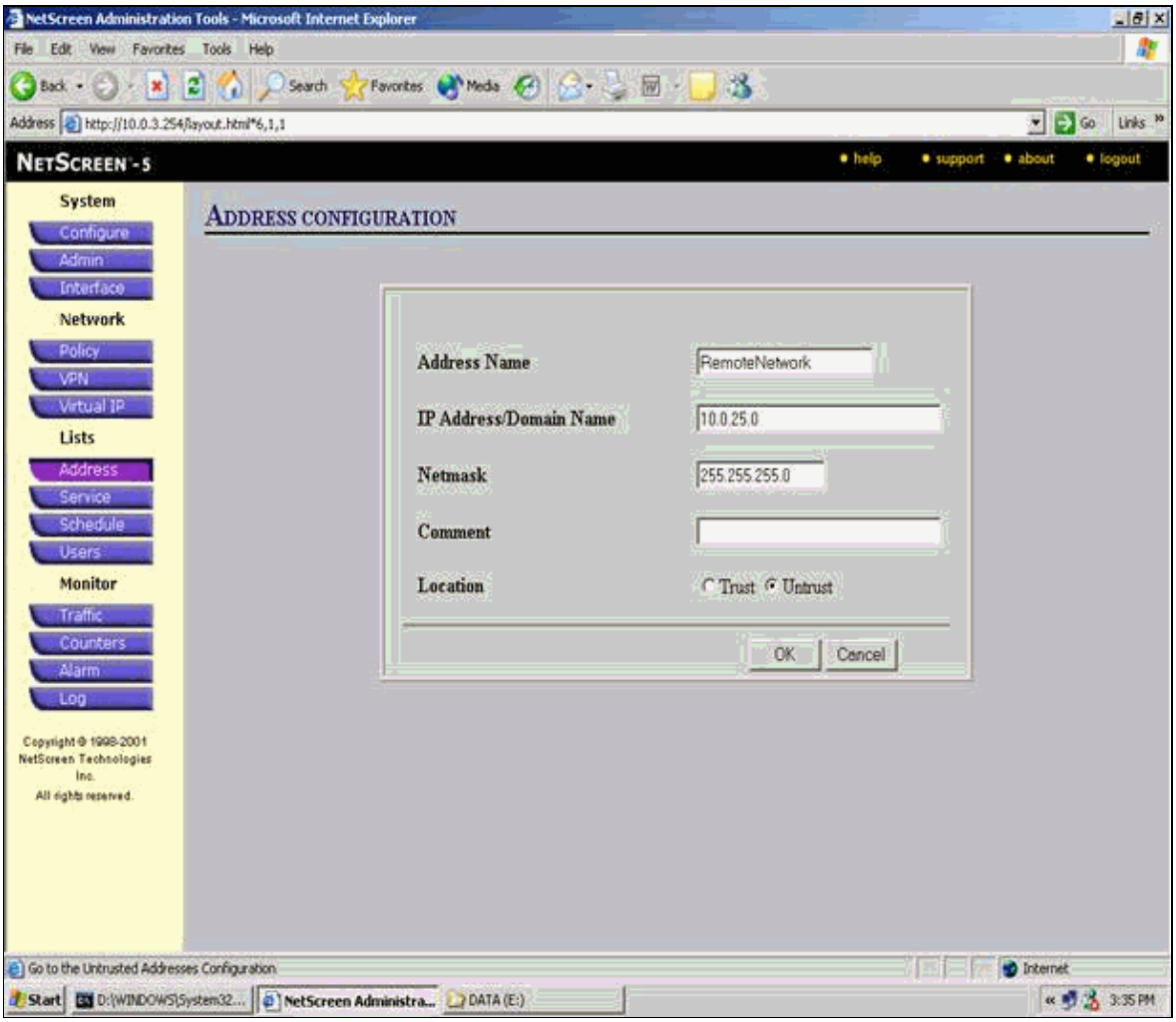
3. Select **Lists > Address**, go to the Untrusted tab, and click **New Address**.
4. Add the remote network that NetScreen Firewall uses when it encrypts packets and click **OK**.

   Note: Do not use address groups when you configure a VPN to a non NetScreen gateway. VPN interoperability fails if you use address groups. The non NetScreen security gateway does not know how to interpret the proxy ID created by NetScreen when address group is used.

   There are couple of workarounds for this:

- Separate the address groups into individual address book entries. Specify individual policies on a per address book entry basis.
- Configure proxy ID to be 0.0.0.0/0 on the non NetScreen gateway (firewall device) if possible.

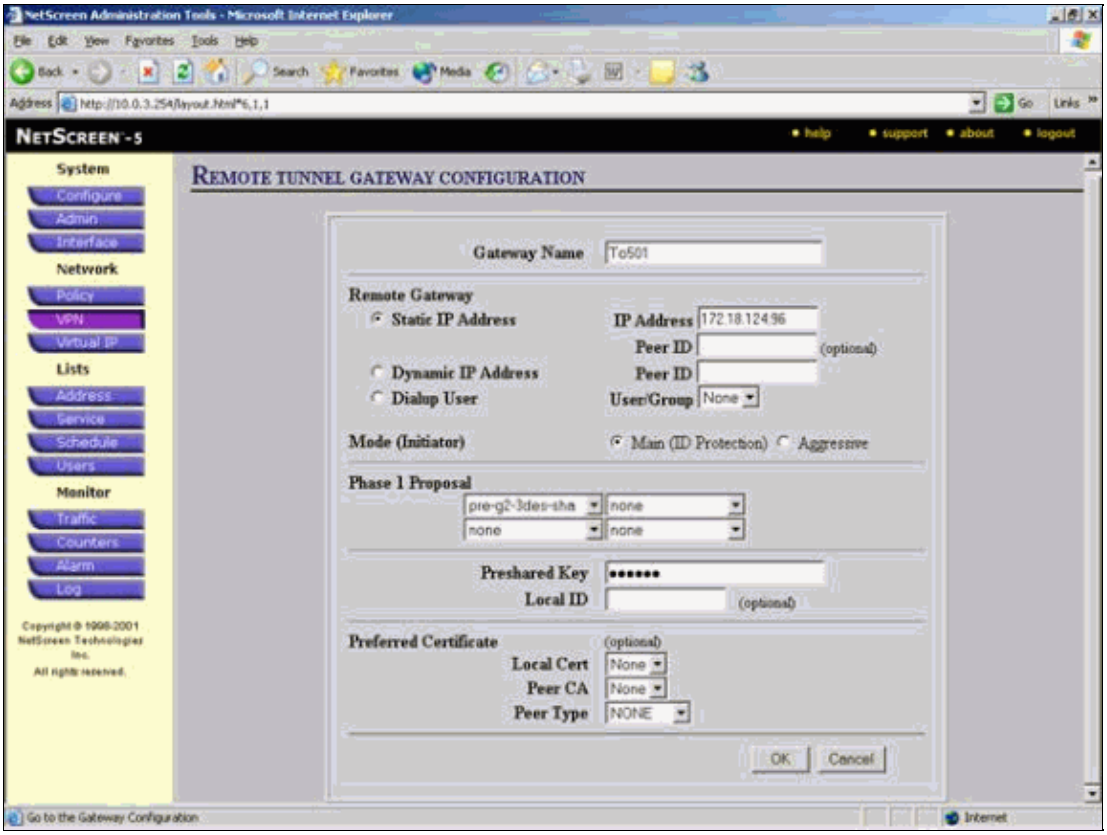
This example uses network 10.0.25.0 with a mask of 255.255.255.0.



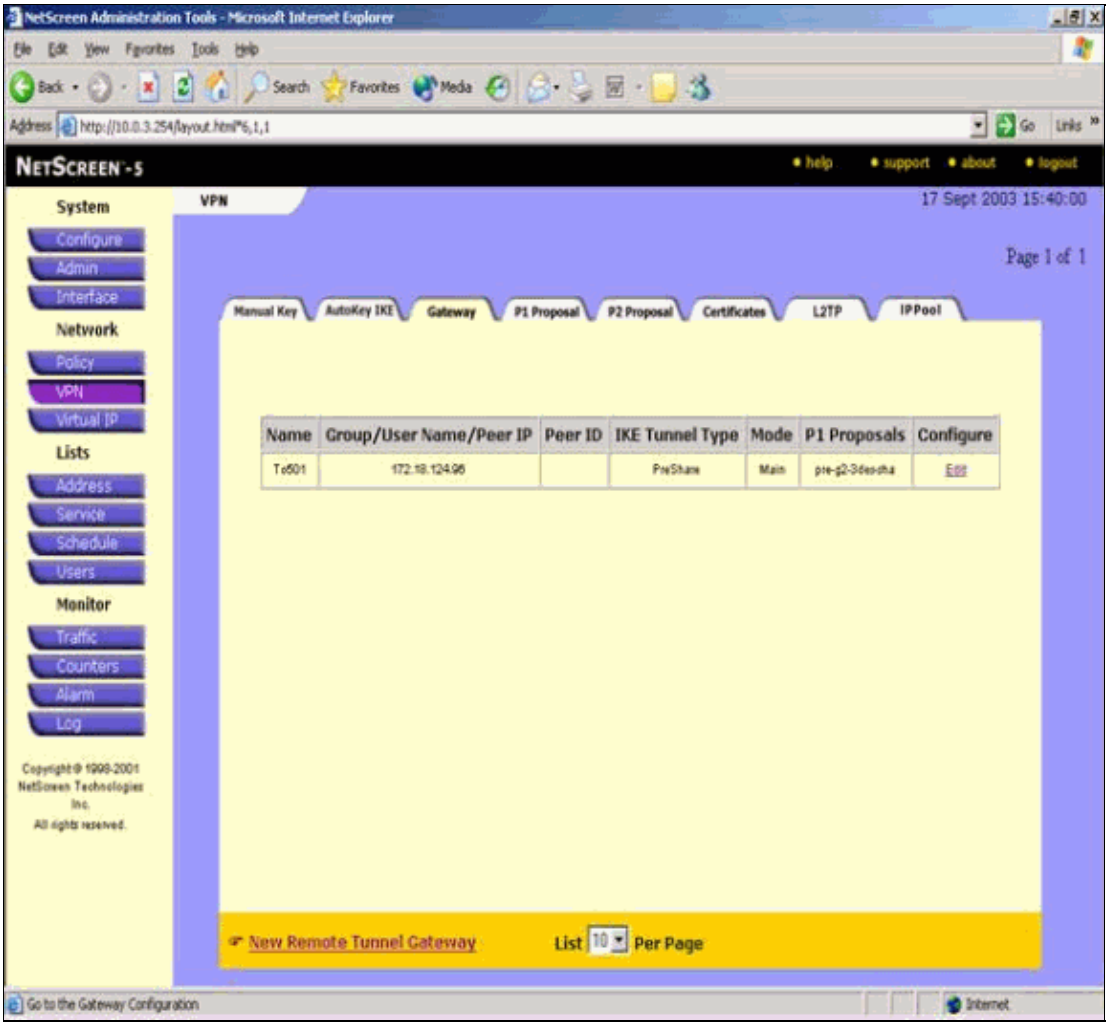
5. Select **Network > VPN**, go to the Gateway tab, and click **New Remote Tunnel Gateway** to configure the VPN gateway (Phase 1 and Phase 2 IPsec policies).
6. Use the IP address of the PIX's outside interface in order to terminate the tunnel, and configure the Phase 1 IKE options to bind. Click **OK** when you are finished.

   This example uses these fields and values.

   - **Gateway Name:** To501
   - **Static IP Address:** 172.18.124.96
   - **Mode:** Main (ID Protection)
   - **Preshared Key:** "testme"
   - **Phase 1 proposal:** pre−g2−3des−sha



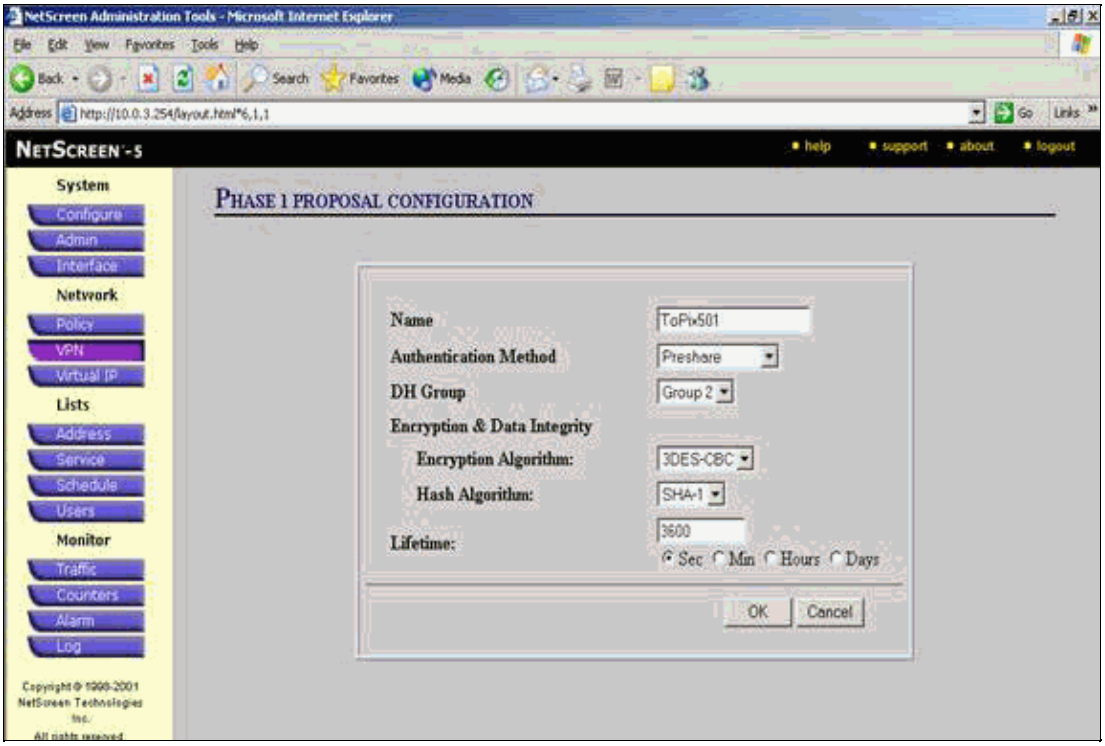
When the remote tunnel gateway is successfully created, a screen similar to this appears.



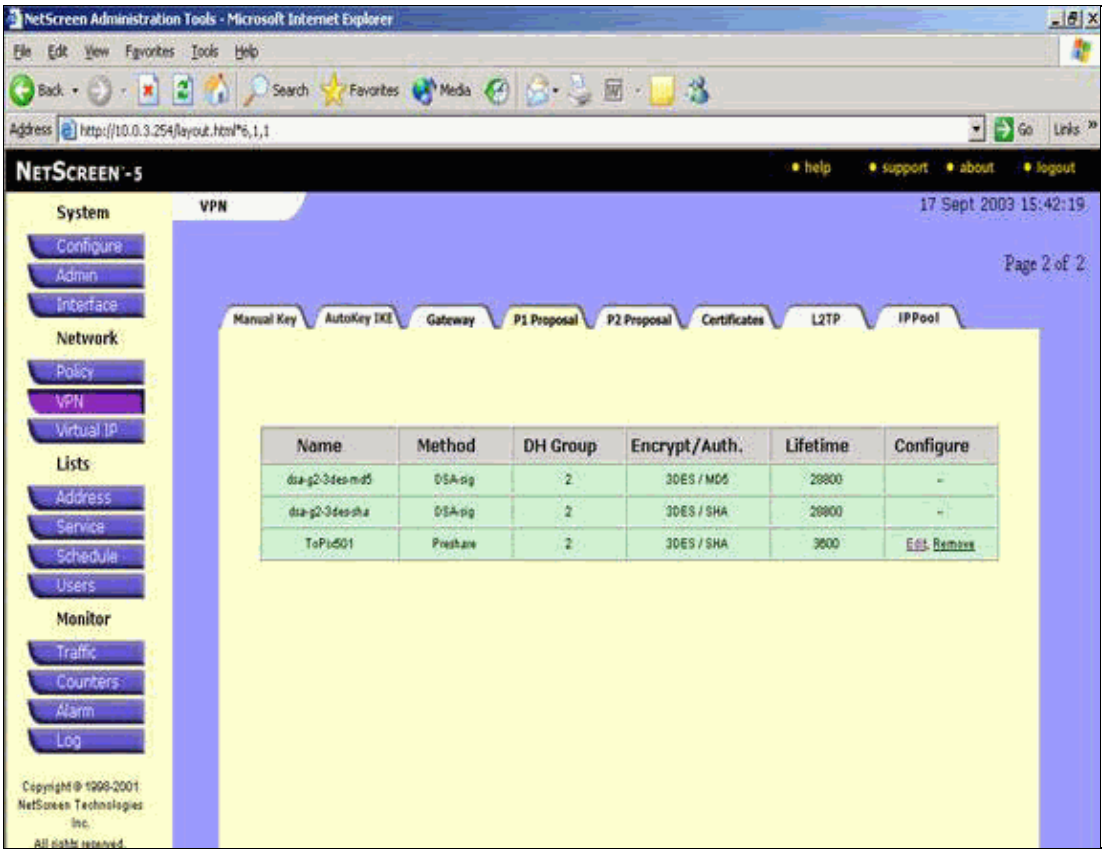
7. Go to the P1 Proposal tab and click **New Phase 1 Proposal** to configure Proposal 1.
8. Enter the configuration information for the Phase 1 Proposal and click **OK**.

This example uses these fields and values for Phase 1 exchange.

- **Name:** ToPix501
- **Authentication:** Preshare
- **DH Group:** Group 2
- **Encryption:** 3DES−CBC
- **Hash:** SHA−1
- **Lifetime:** 3600 Sec.



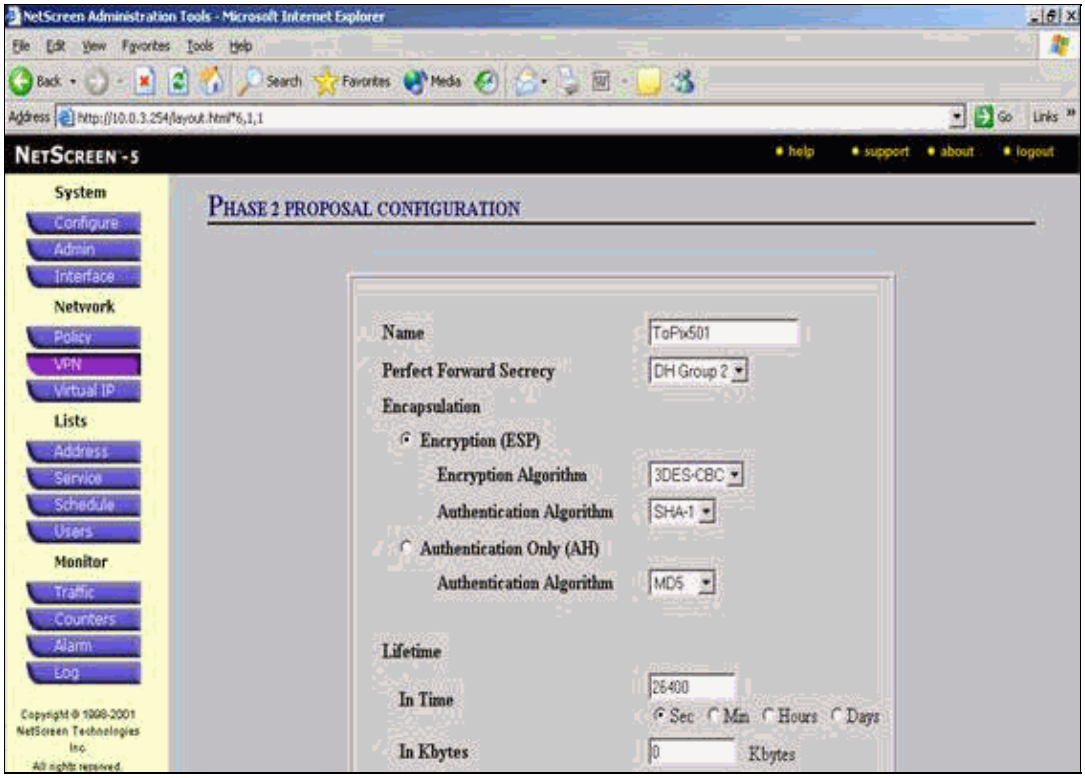
When Phase 1 is successfully added to the NetScreen configuration, a screen similar to this example appears.



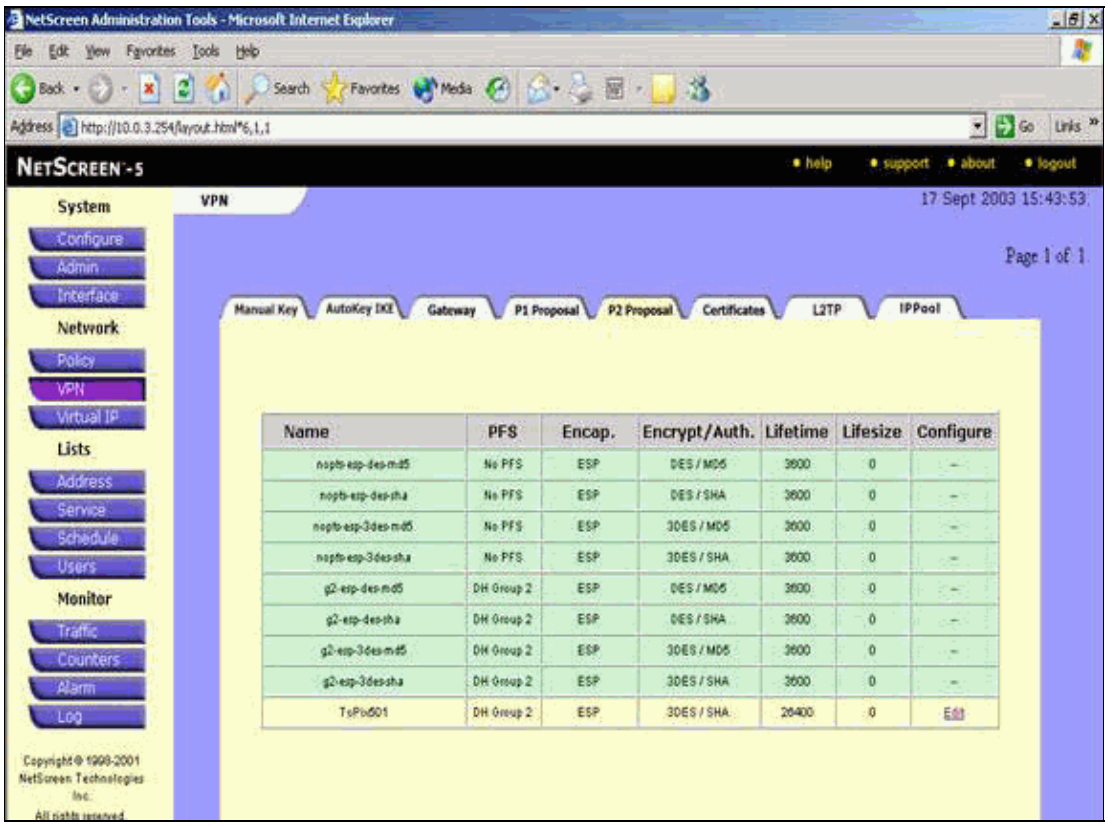
9. Go to the P2 Proposal tab and click **New Phase 2 Proposal** to configure Phase 2.
10. Enter the configuration information for the Phase 2 Proposal and click **OK**.

This example uses these fields and values for Phase 2 exchange.

- **Name:** ToPix501
- **Perfect Forward Secrecy:** DH−2 (1024 bits)
- **Encryption Algorithm:** 3DES−CBC
- **Authentication Algorithm:** SHA−1
- **Lifetime:** 26400 Sec



When Phase 2 is successfully added to the NetScreen configuration, a screen similar to this example appears.



11. Select the **AutoKey IKE** tab, and then click **New AutoKey IKE Entry** to create and configure AutoKeys IKE.
12. Enter the configuration information for AutoKey IKE, and then click **OK**.

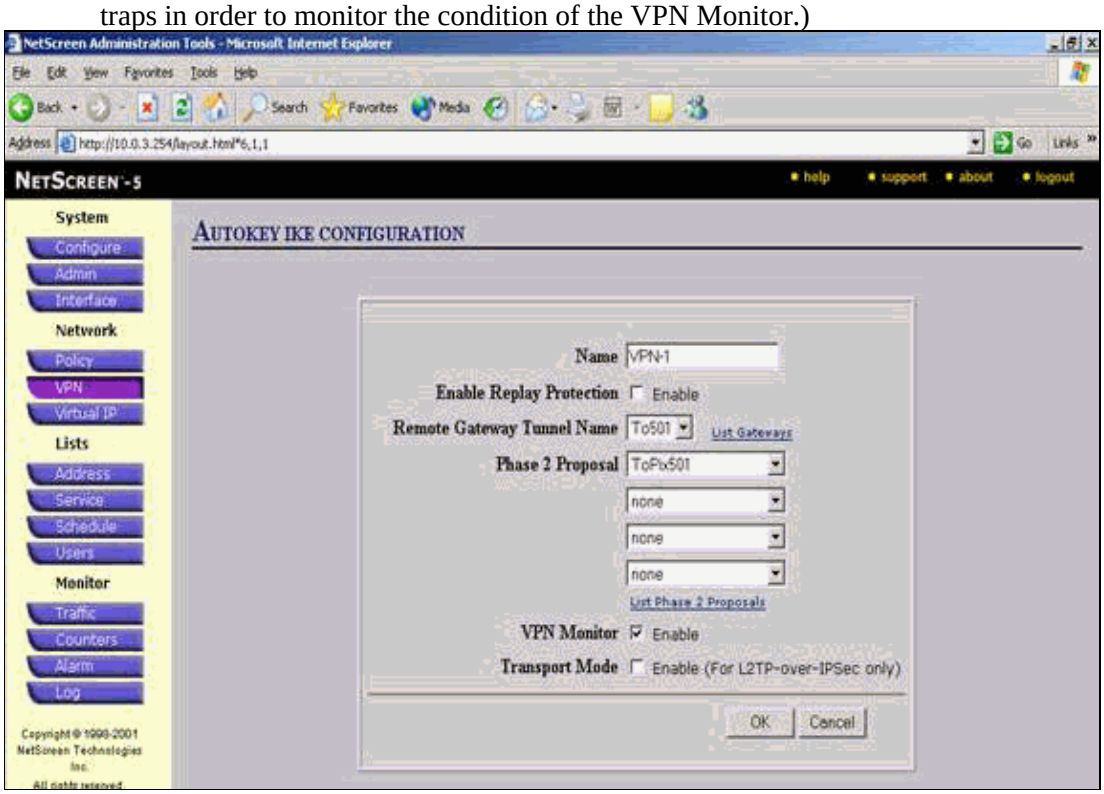
    This example uses these fields and values for AutoKey IKE.

    - **Name:** VPN−1
    - **Remote Gateway Tunnel Name:** To501

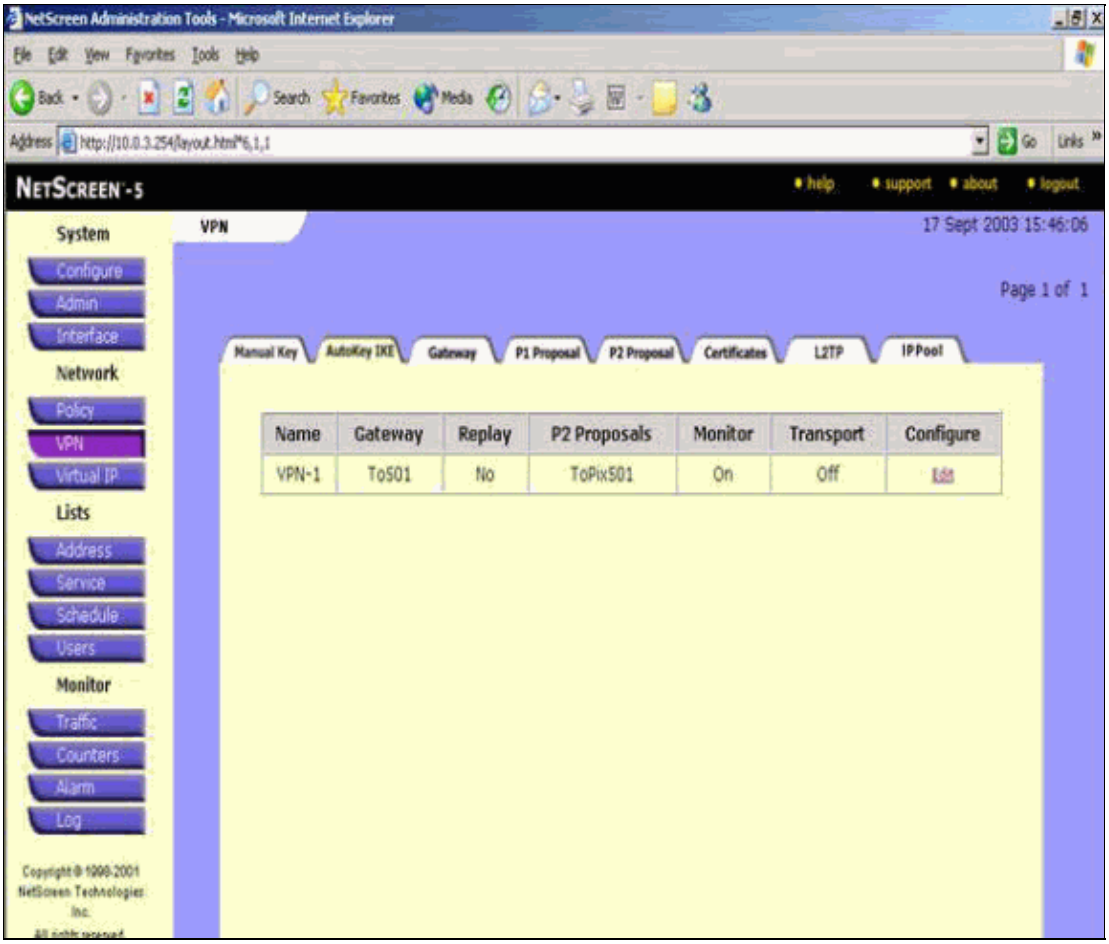
      (This was previously created on the Gateway tab.)
    - **Phase 2 Proposal:** ToPix501

      (This was previously created on the P2 Proposal tab.)
    - **VPN Monitor:** Enable

      (This enables the NetScreen device to set Simple Network Management Protocol [SNMP] traps in order to monitor the condition of the VPN Monitor.)



When the VPN−1 rule is successfully configured, a screen similar to this example appears.



13. Select **Network > Policy**, go to the Outgoing tab, and click **New Policy** to configure the rules that allow encryption of the IPsec traffic.
14. Enter the configuration information for the policy and click **OK**.

    This example uses these fields and values for the policy. The Name field is optional and is not used in this example.

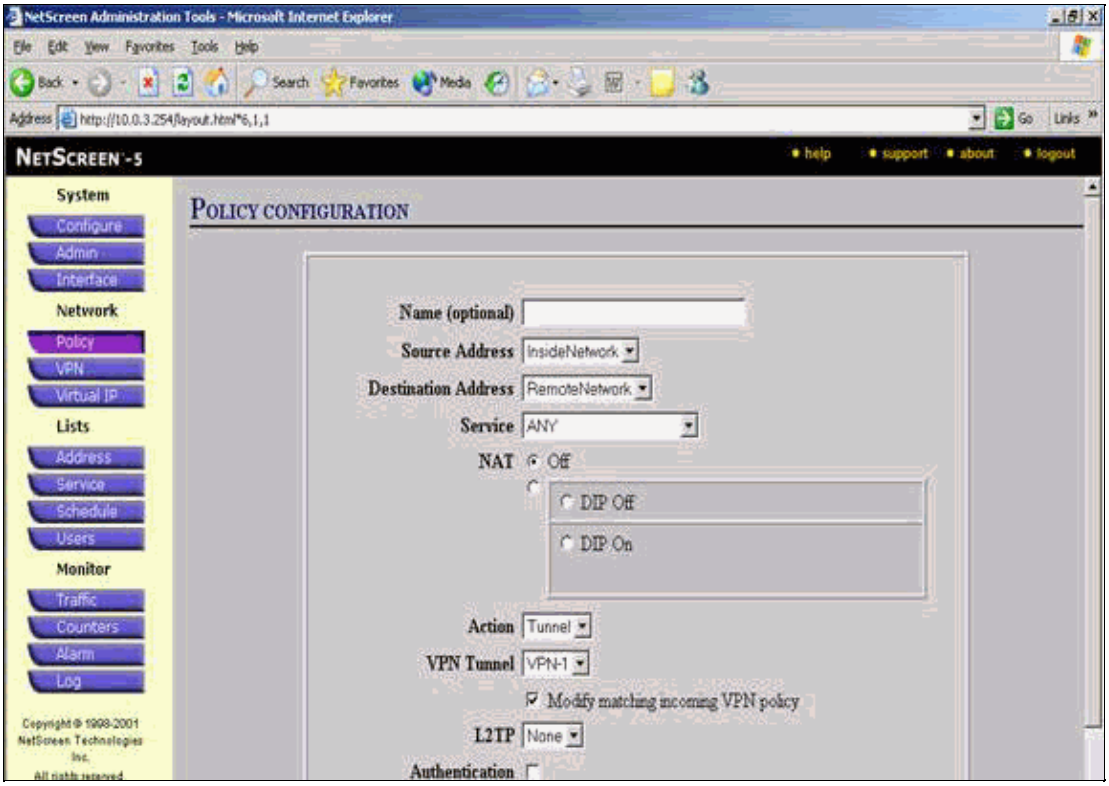
    - **Source Address:** InsideNetwork

      (This was previously defined on the Trusted tab.)
    - **Destination Address:** RemoteNetwork

      (This was previously defined under the Untrusted tab.)
    - **Service:** Any
    - **Action:** Tunnel
    - **VPN Tunnel:** VPN−1

      (This was previously defined as the VPN tunnel on the AutoKey IKE tab.)
    - **Modify matching incoming VPN policy:** Checked

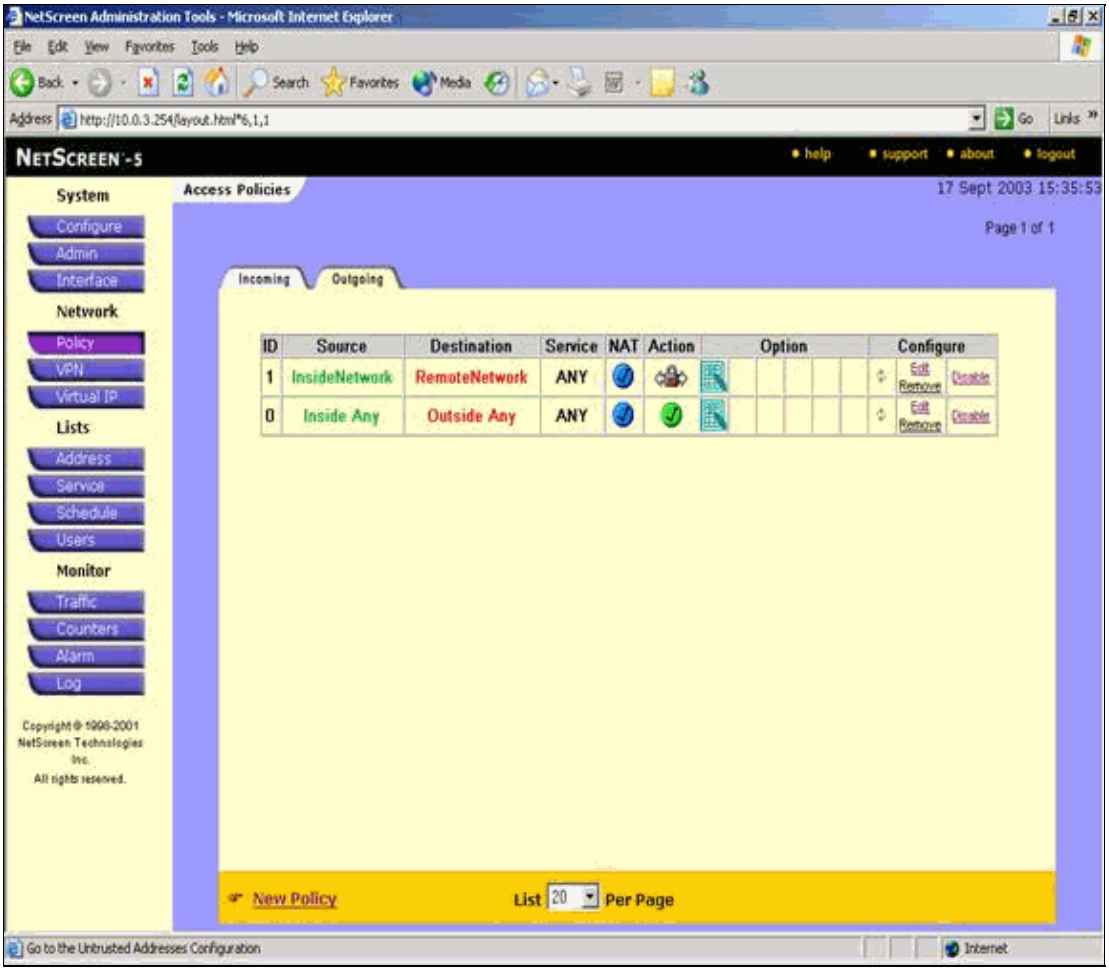
      (This option automatically creates an inbound rule that matches the outside network VPN traffic.)



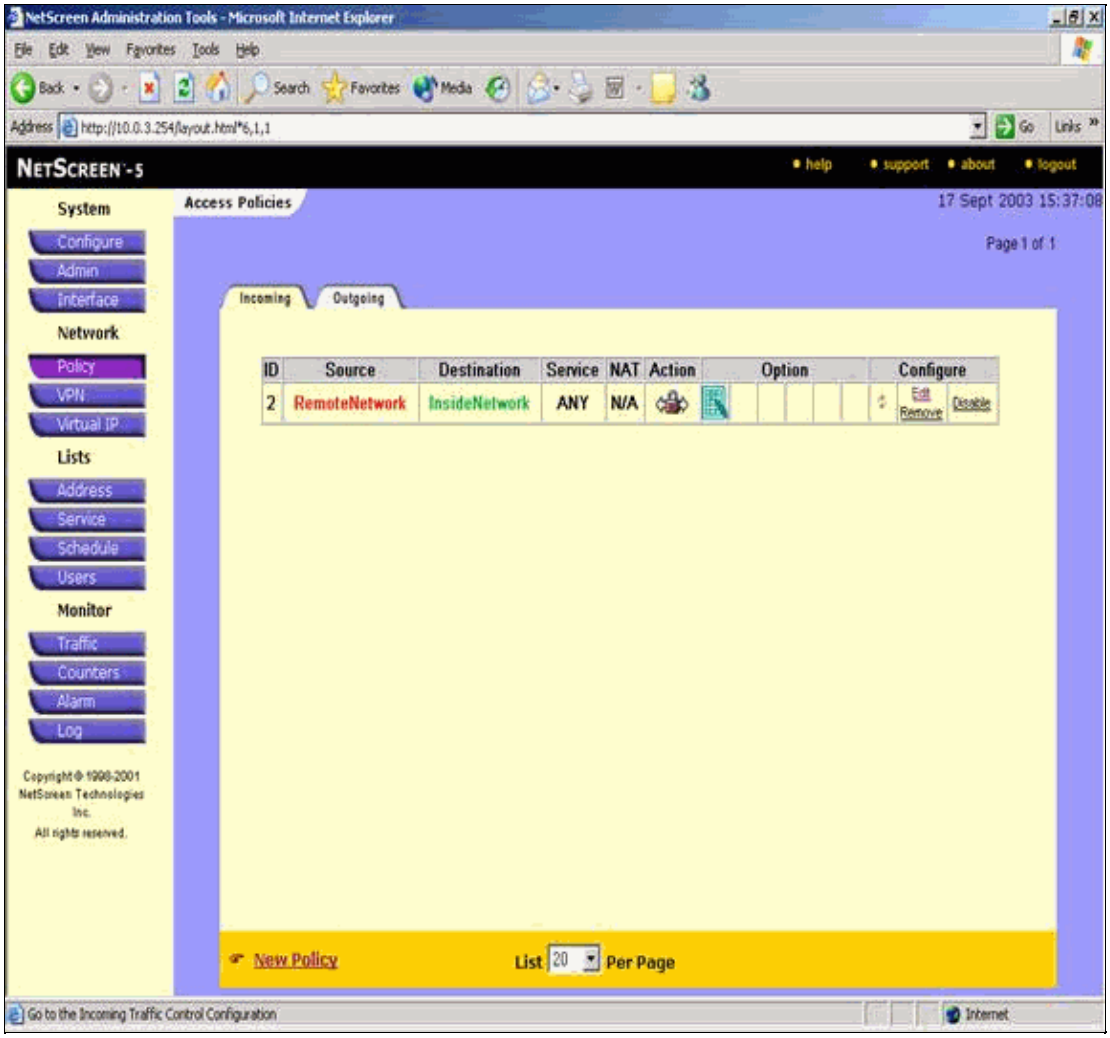
15. When the policy is added, ensure that the outbound VPN rule is first in the list of policies. (The rule that is created automatically for inbound traffic is on the Incoming tab.)

    Complete these steps if you need to change the order of the policies:

    a. Click the Outgoing tab.
    b. Click the circular arrows in the Configure column in order to display the Move Policy Micro window.
    c. Change the order of the policies so that the VPN policy is above policy ID 0 (so that the VPN policy is at the top of the list).



Go to the Incoming tab in order to view the rule for inbound traffic.



Verify

This section provides information you can use to confirm your configuration properly works.

Verification Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **ping** Diagnoses basic network connectivity.
- **show crypto ipsec sa** Shows the Phase 2 security associations.
- **show crypto isakmp sa** Shows the Phase 1 security associations.

Verification Output

Sample output from **ping** and **show** commands is shown here.

This ping is initiated from a host behind the 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
```

Output from the **show crypto ipsec sa** command is shown here.

```
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:
```

Output from the **show crypto isakmp sa** command is shown here.

```
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

This section provides information you can use to troubleshoot your configuration.

Troubleshooting Commands

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto engine** Displays messages about crypto engines.
- **debug crypto ipsec** Displays information about IPsec events.
- **debug crypto isakmp** Displays messages about IKE events.

Sample Debug Output

Sample **debug** output from the PIX Firewall is shown here.

```
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
```

Related Information

- **IPsec Negotiation/IKE Protocols**
- **Cisco PIX Firewall Software**
- **Cisco Secure PIX Firewall Command References**
- **Security Product Field Notices (including PIX)**
- **Requests for Comments (RFCs)**
- **Technical Support & Documentation − Cisco Systems**

Updated: Feb 02, 2006 Document ID: 45423