Het configureren van IPSec LAN-to-LAN tunnel tussen de Cisco Pix-firewall en een NetScreen-firewall

Inhoud

Inleiding

Dit document beschrijft de gewenste procedure die wordt gebruikt om een IPsec LAN-to-LAN tunnel te maken tussen een Cisco PIX-firewall en een NetScreen-firewall met de nieuwste software. Er is een privé netwerk achter elk apparaat dat aan de andere firewall door de IPsec-tunnel communiceert.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- De NetScreen Firewall wordt met de IP-adressen ingesteld op de trust/ontrust-interfaces.
- Connectiviteit is gevestigd op het internet.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- PIX-firewall, versie 6.3(1)
- Laatste herziening NetScreen

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

Configuraties

Dit document gebruikt deze configuraties:

- PIX-firewall
- NetScreen-firewall

De PIX-firewall configureren

PIX-firewall

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

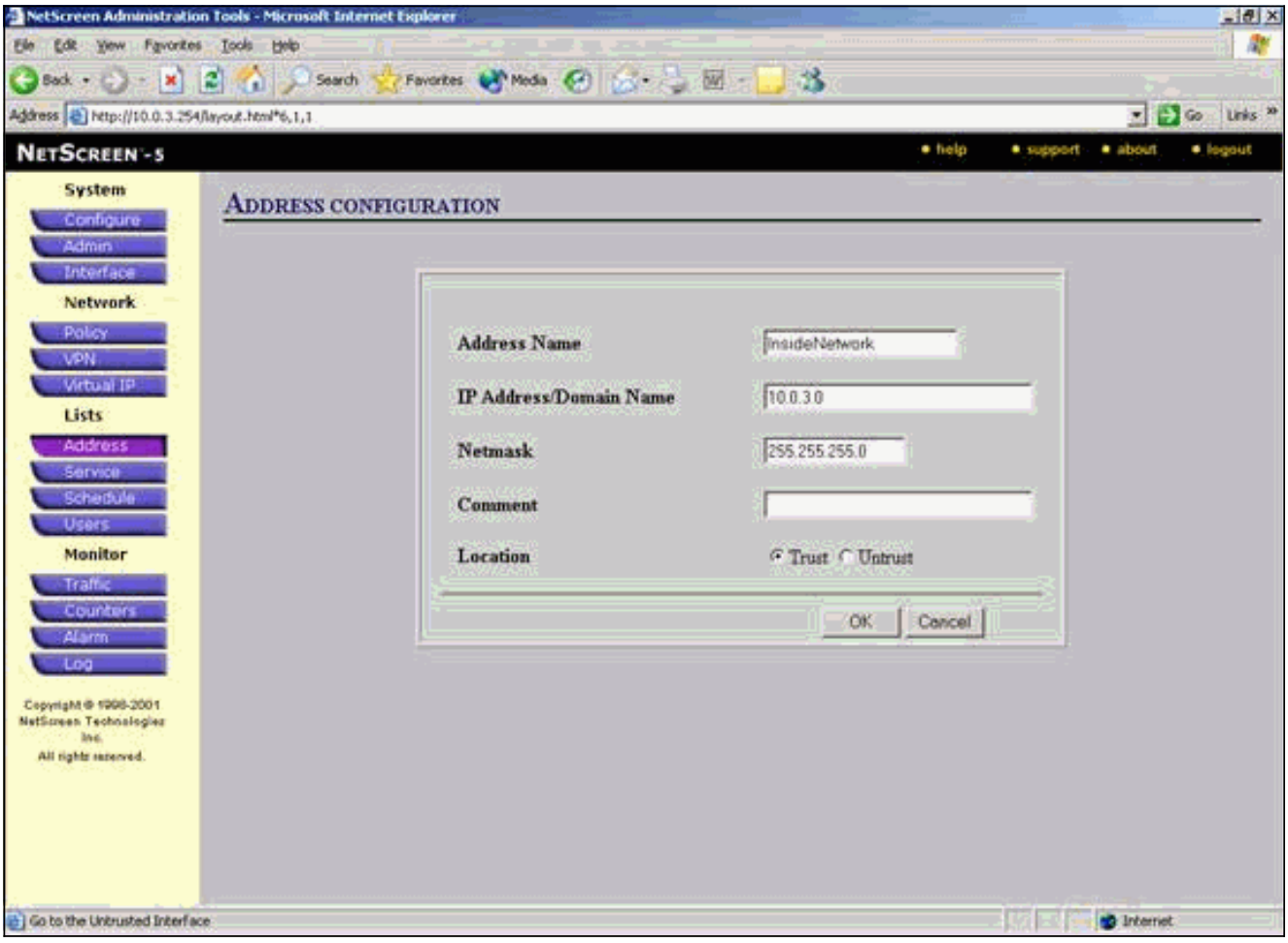
```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554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

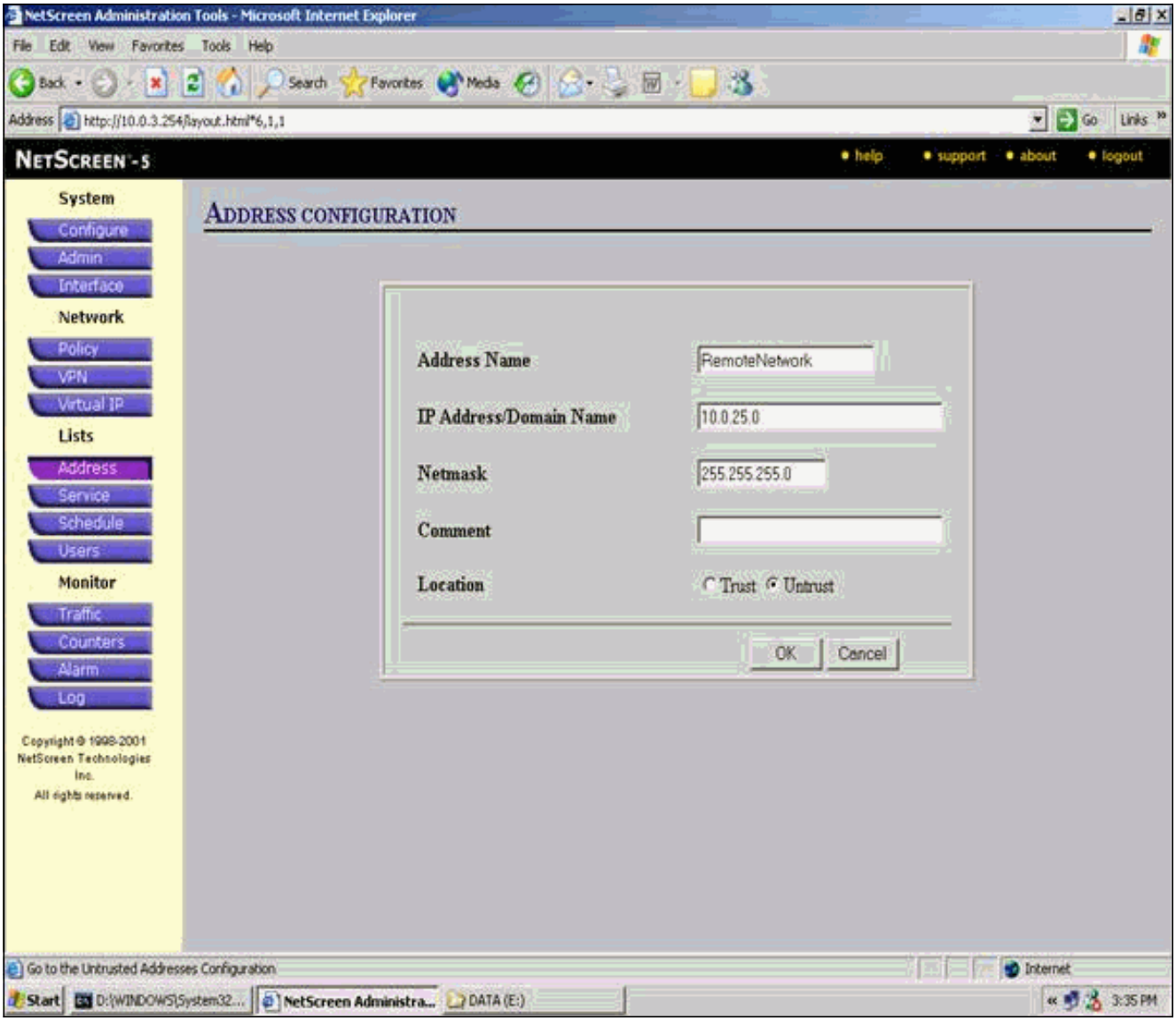
De NetScreen Firewall configureren

Voltooi deze stappen om de NetScreen Firewall te configureren.

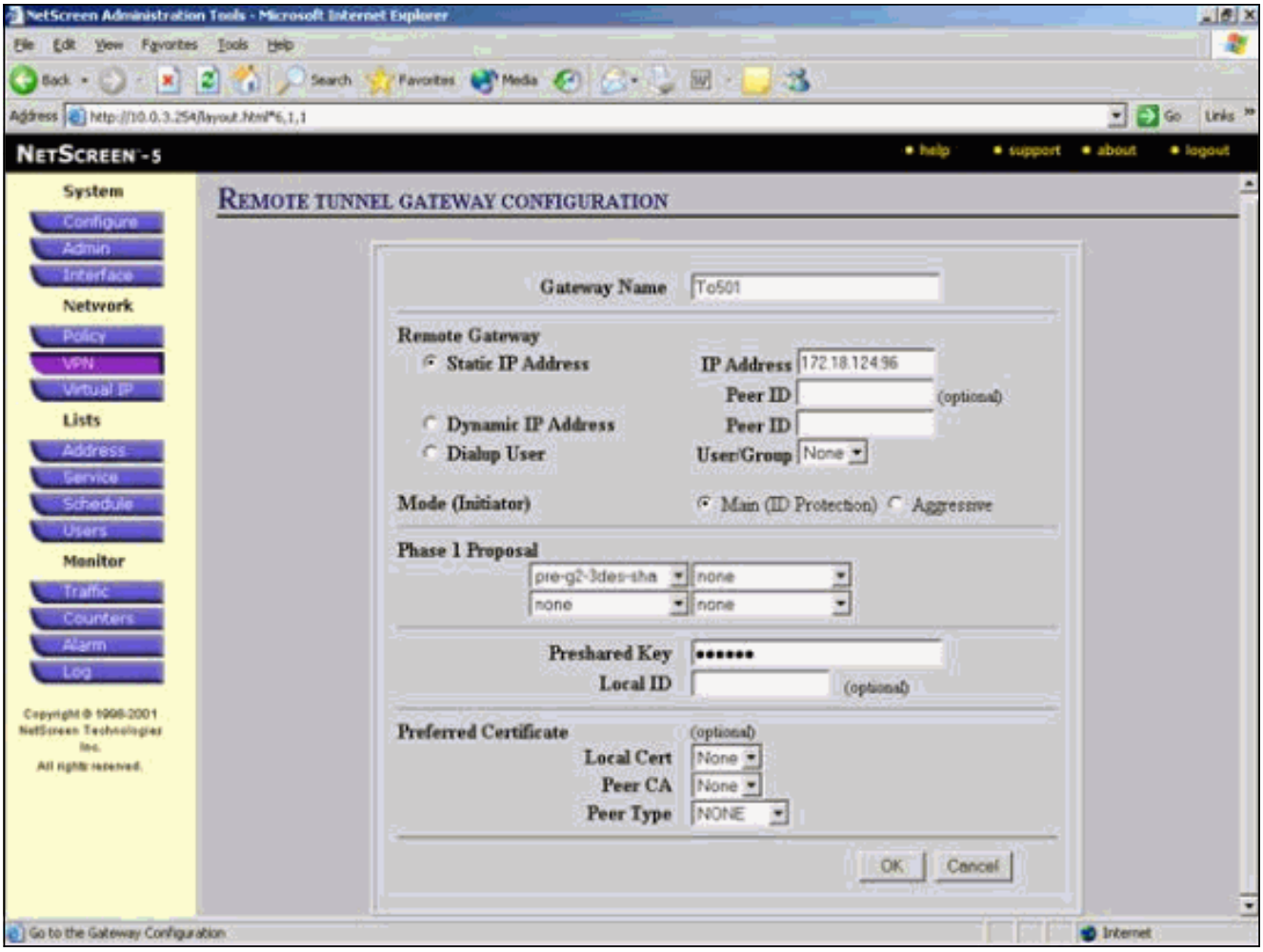
1. Selecteer **Lijsten > Adres**, ga naar het tabblad Vertrouwd en klik op **Nieuw Adres**.
2. Voeg het interne netwerk NetScreen toe dat versleuteld is in de tunnel en klik op **OK**.**Opmerking:** Zorg ervoor dat de optie Vertrouwen is geselecteerd.Dit voorbeeld gebruikt netwerk 10.0.3.0 met een masker van 255.255.255.0.



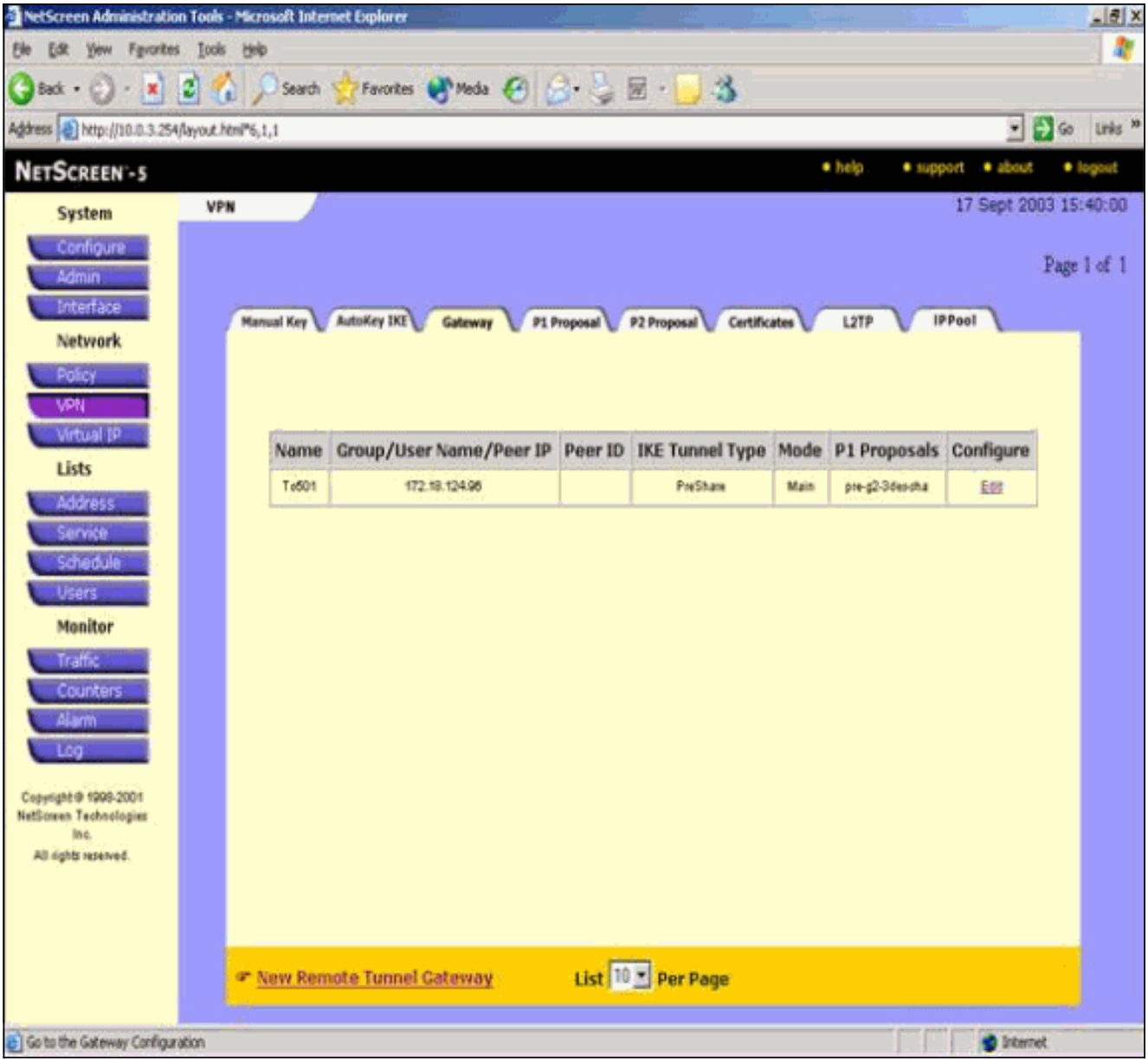
3. Selecteer **Lijsten > Adres**, ga naar het tabblad Onvertrouwde en klik op **Nieuw Adres**.
4. Voeg het externe netwerk toe dat NetScreen Firewall gebruikt wanneer het pakketjes versleutelt en klik op **OK**.**Opmerking:** Gebruik geen adresgroepen wanneer u een VPN vormt naar een niet NetScreen poort. VPN-interoperabiliteit mislukt als u adresgroepen gebruikt. De niet NetScreen security gateway weet niet hoe de proxy-ID moet worden geïnterpreteerd die door NetScreen is gecreëerd wanneer de adresgroep wordt gebruikt.Hier zijn een paar redenen voor:De adresgroepen in individuele adresboekingangen scheiden. Specificeer individueel beleid op basis van een adresboekregistratie.Configureer proxy-ID om 0.0.0.0/0 op de niet NetScreen-gateway (firewallapparaat) indien mogelijk te zijn.Dit voorbeeld gebruikt netwerk 10.0.25.0 met een masker van 255.255.255.0.



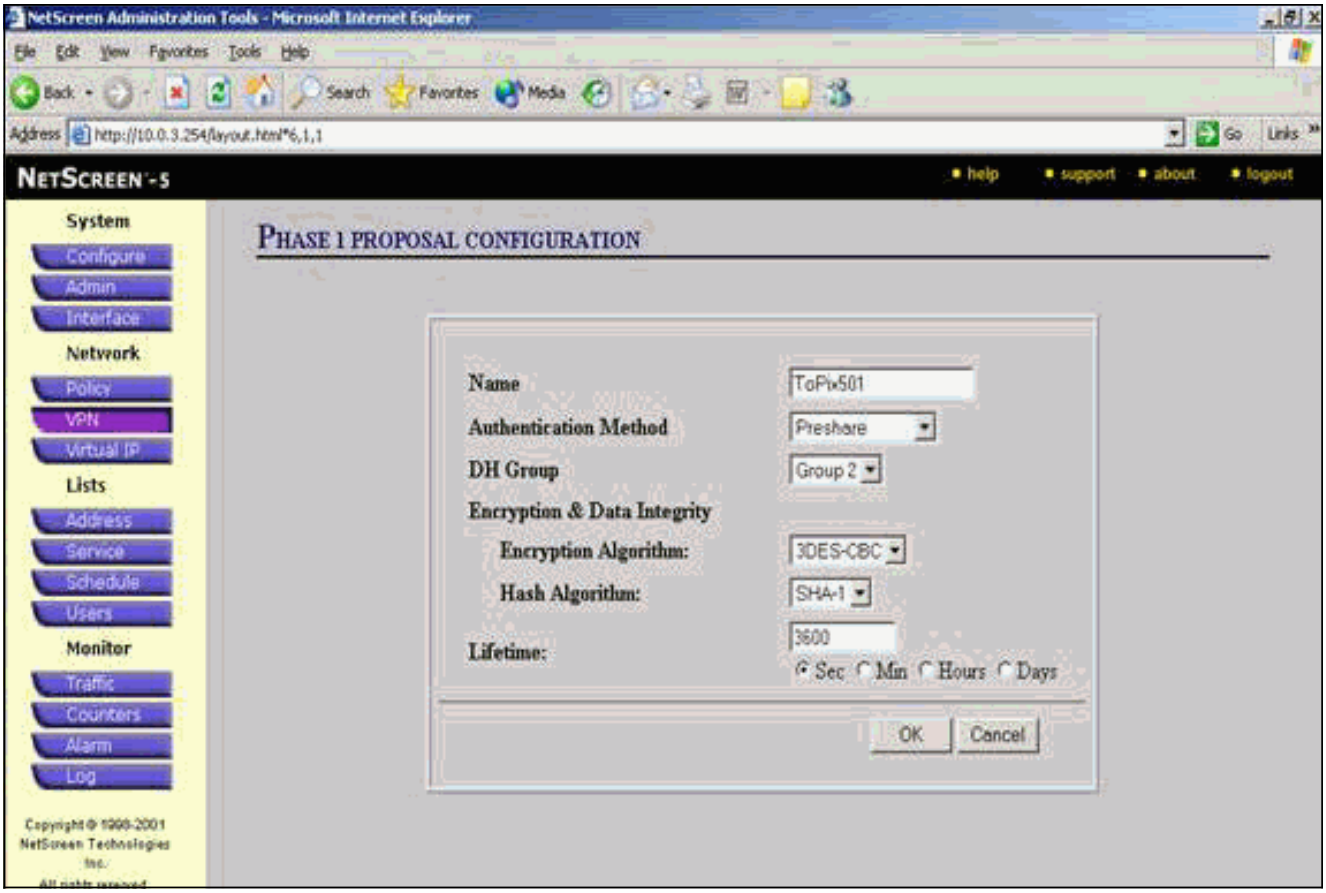
5. Selecteer **Netwerk > VPN**, ga naar het tabblad Gateway en klik op **New Remote Tunnel Gateway** om de VPN-gateway te configureren (fase 1 en fase 2 IPsec-beleid).
6. Gebruik het IP-adres van de externe interface van PIX om de tunnel te sluiten en stel de opties Fase 1 IKE in om te binden. Klik op **OK** wanneer u klaar bent.Dit voorbeeld gebruikt deze velden en waarden.**Naam gateway:** To501**Statisch IP-adres:** 172.18.124.96**Modus:** Hoofdvenster (ID-bescherming)**Voorgedeelde sleutel:** "testme"**Voorstel fase 1:** pre-g2-3des-sha



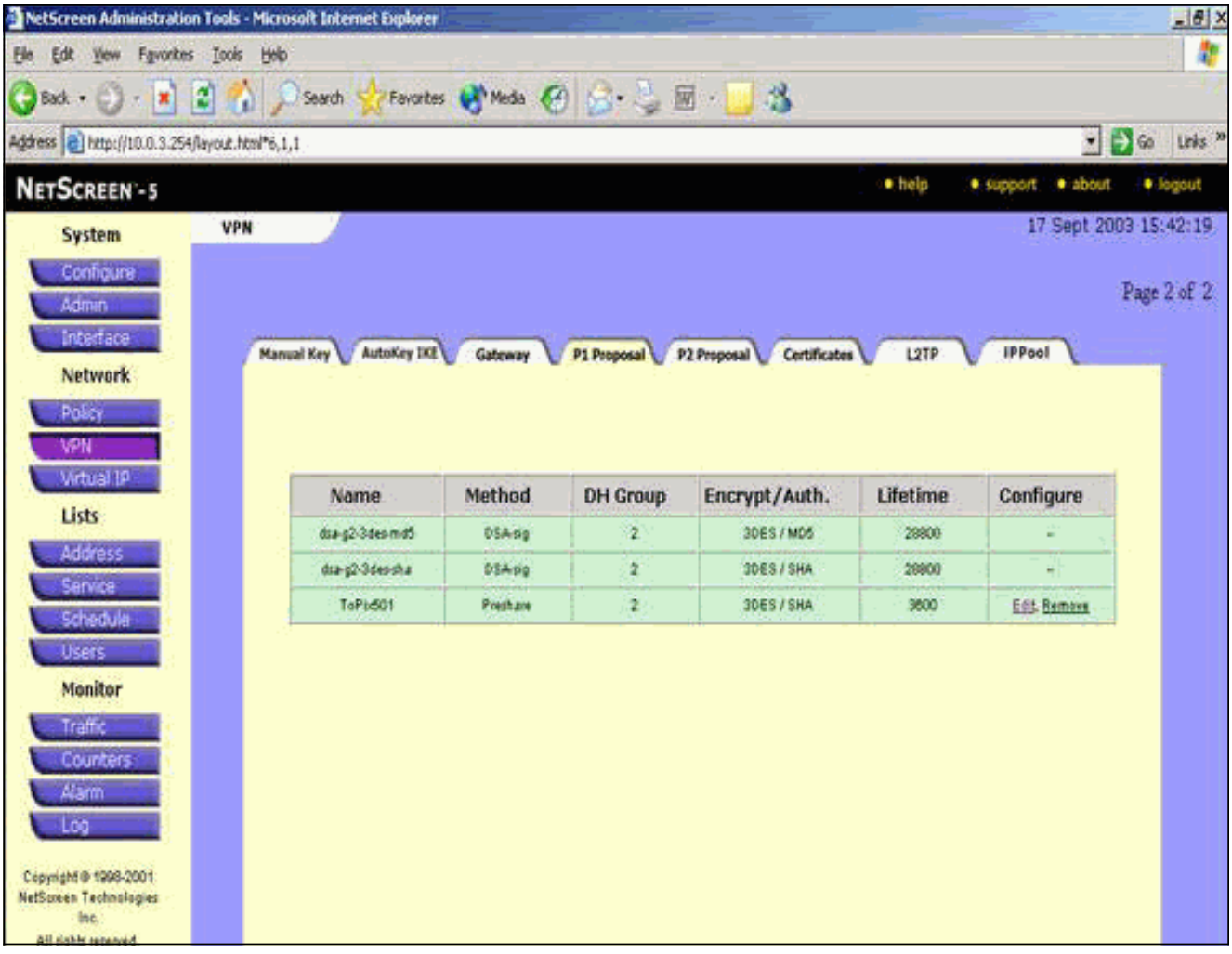
Wanneer de externe tunnelgateway met succes wordt gecreëerd, verschijnt er een vergelijkbaar
scherm.



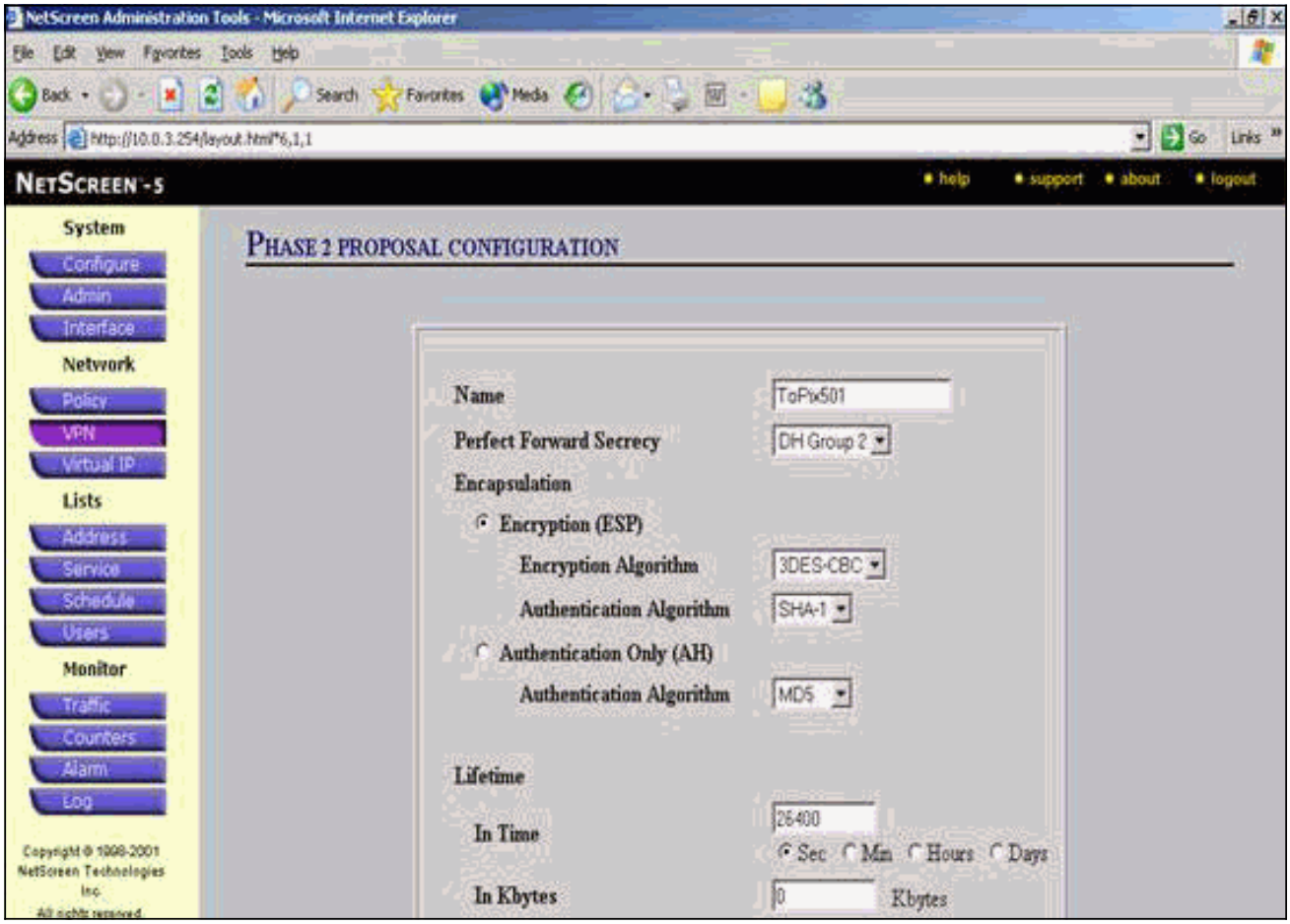
7. Ga naar het tabblad P1 Voorstel en klik op **Nieuw Fase 1 Voorstel** om Voorstel 1 te configureren.
8. Voer de configuratieinformatie in voor het fase 1-voorstel en klik op **OK**.Dit voorbeeld gebruikt deze velden en waarden voor Fase 1 uitwisseling.**Name:** ToPIX501**Verificatie:** preken**DH-groep:** Groep 2**Encryptie:** 3DES-CBC**Hash:** SHA-1**Levensduur:** 3600 sec.



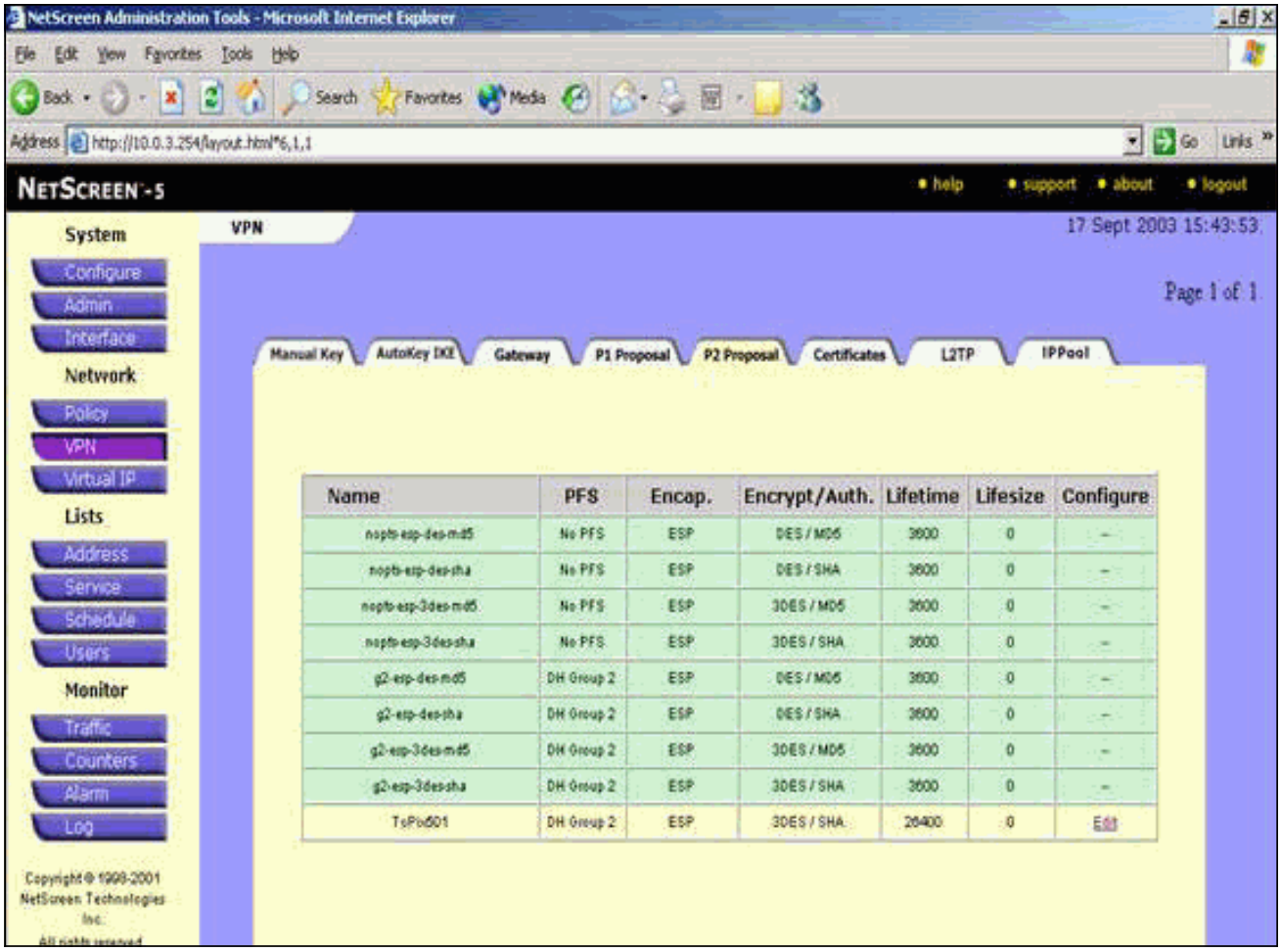
Wanneer fase 1 met succes is toegevoegd aan de NetScreen-configuratie, verschijnt er een scherm dat vergelijkbaar is met dit voorbeeld.



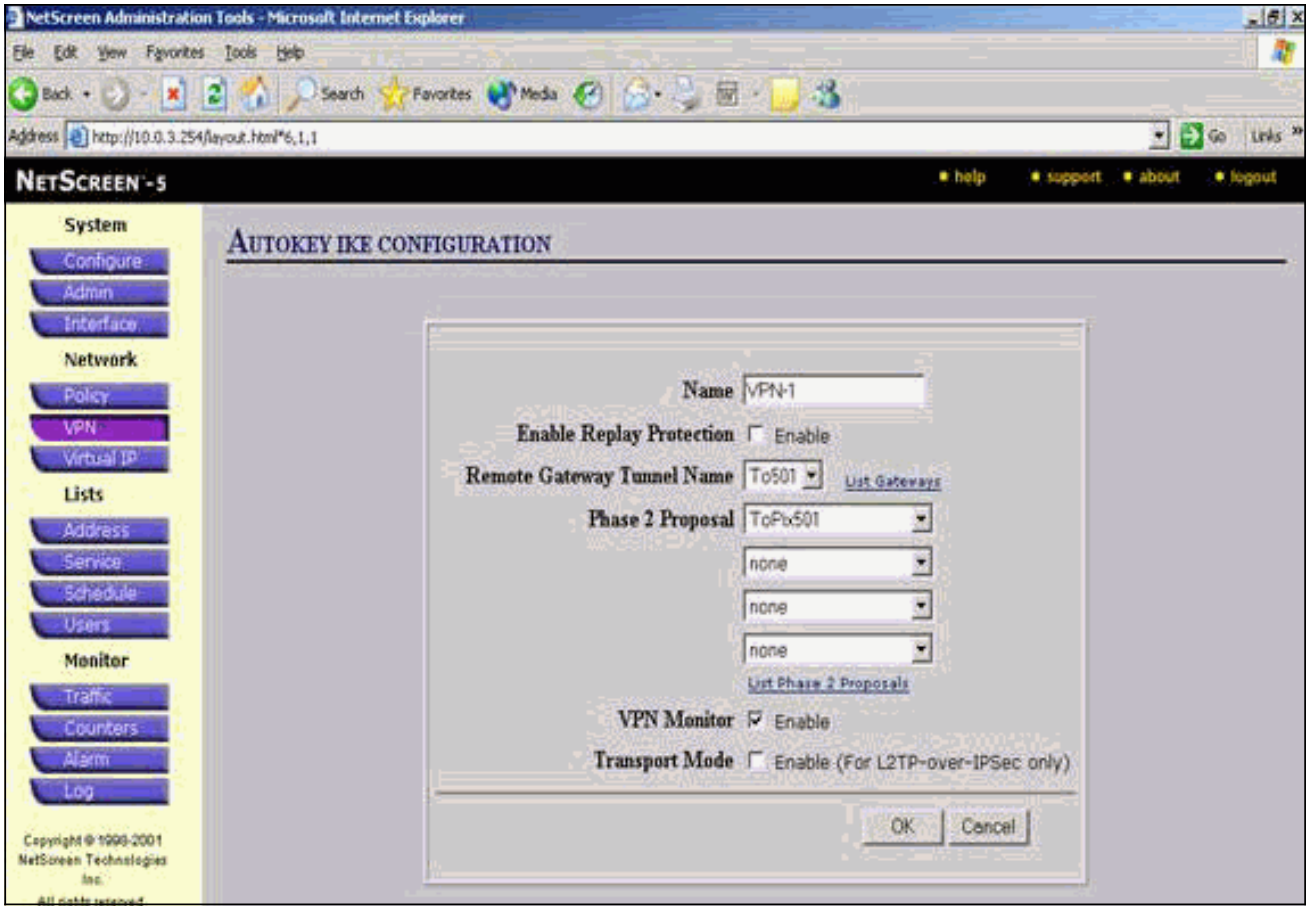
9. Ga naar het tabblad P2 Voorstel en klik op **Nieuw Fase 2 Voorstel** om fase 2 te configureren.
10. Voer de configuratieinformatie in voor fase 2 en klik op **OK**.Dit voorbeeld gebruikt deze velden en waarden voor Fase 2 uitwisseling.**Name:** ToPIX501**Perfect voorwaartse geheimhouding:** DH-2 (1024 bits)**Encryptiealgoritme:** 3DES-CBC**Verificatiealgoritme:** SHA-1**Levensduur:** 2640
sec



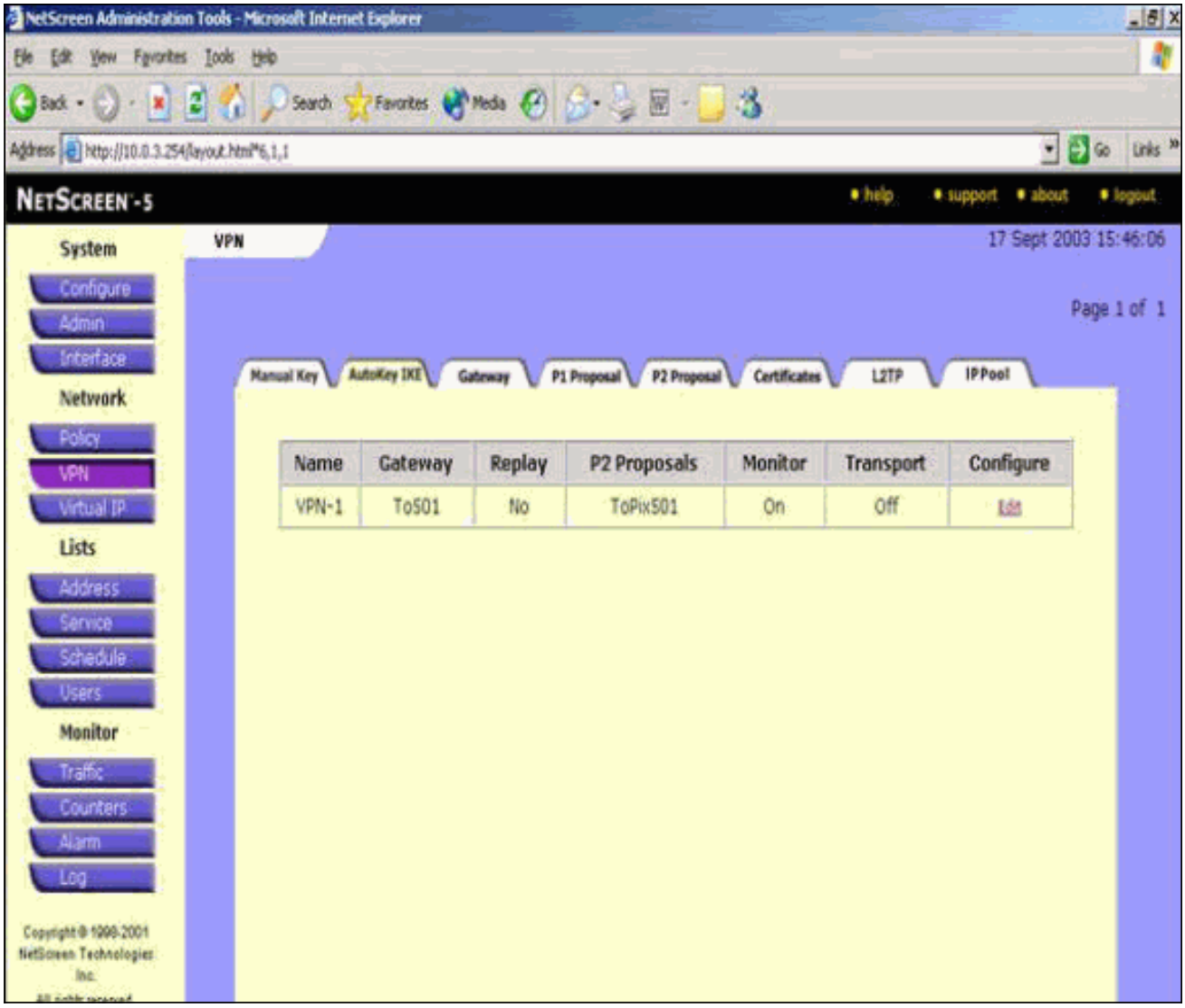
Wanneer fase 2 met succes is toegevoegd aan de NetScreen-configuratie, verschijnt er een scherm dat vergelijkbaar is met dit
voorbeeld.



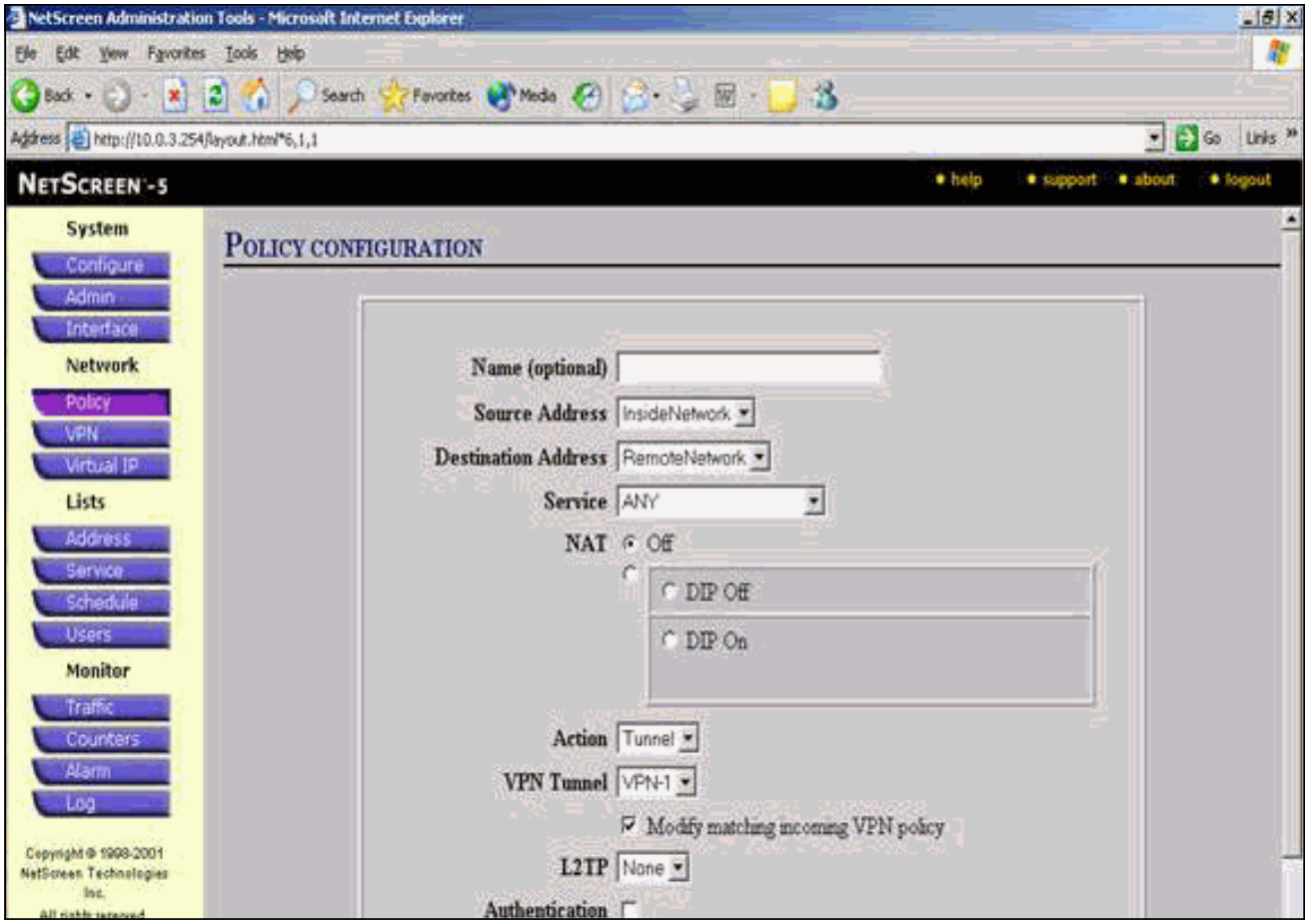
11. Selecteer het tabblad **AutoKey IKE** en klik vervolgens op **Nieuwe AutoKey IKE-ingang** om AutoKeys IKE te maken en te configureren.
12. Voer de configuratieinformatie in voor AutoKey IKE in en klik vervolgens op **OK**.Dit voorbeeld gebruikt deze velden en waarden voor AutoKey IKE.**Name:** VPN-1**Remote Gateway-tunnelnaam:** To501(Dit werd eerder gemaakt op het tabblad Gateway.)**Fase 2 Voorstel:** ToPIX501(Dit is eerder gemaakt op het tabblad P2 Voorstel.)**VPN-monitor:** inschakelen(Dit stelt het NetScreen-apparaat in om Simple Network Management Protocol [SNMP]-traps in te stellen om de toestand van de VPN-monitor te bewaken.)



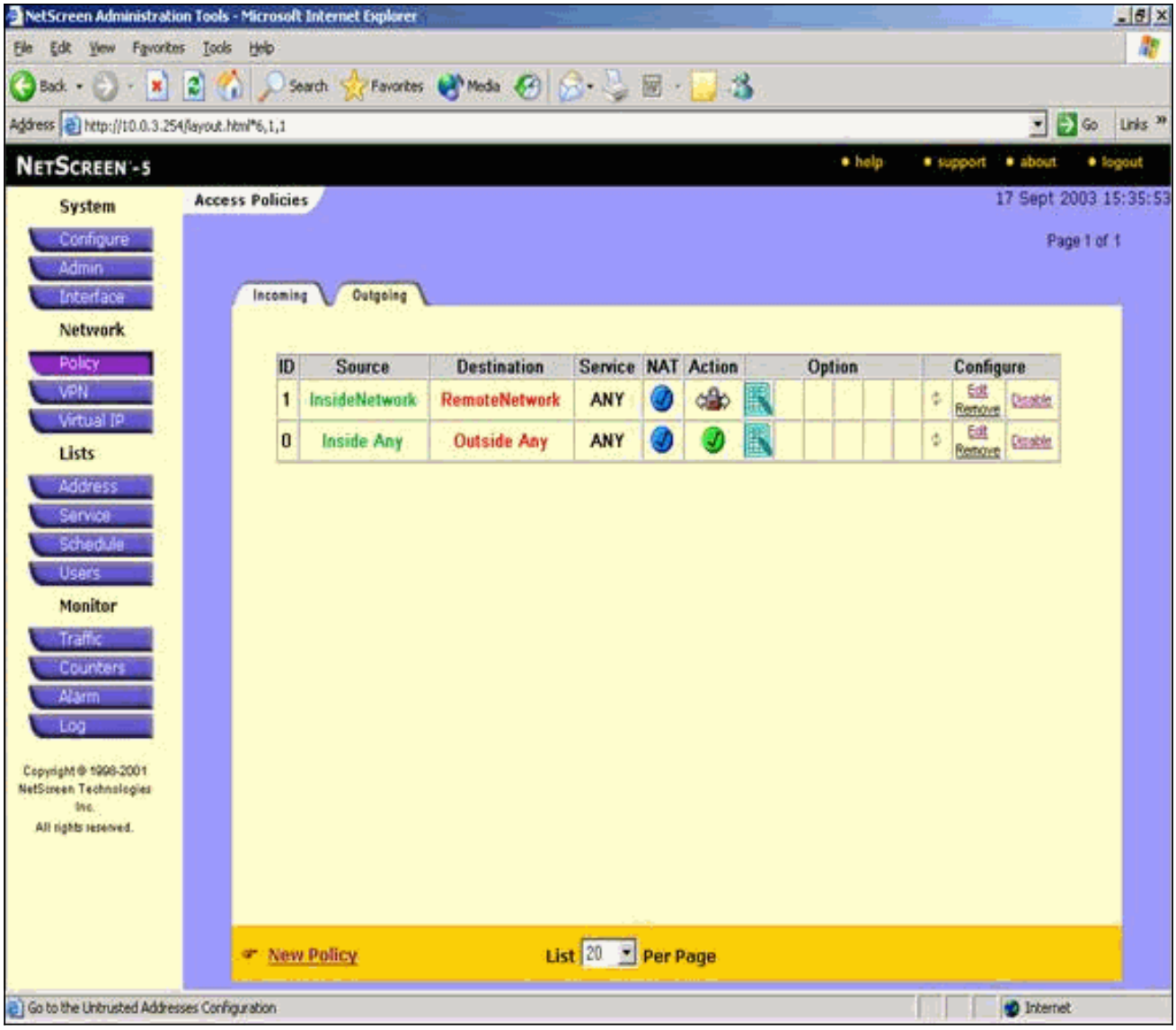
Wanneer de VPN-1 regel met succes is geconfigureerd, verschijnt er een scherm dat vergelijkbaar is met dit
voorbeeld.



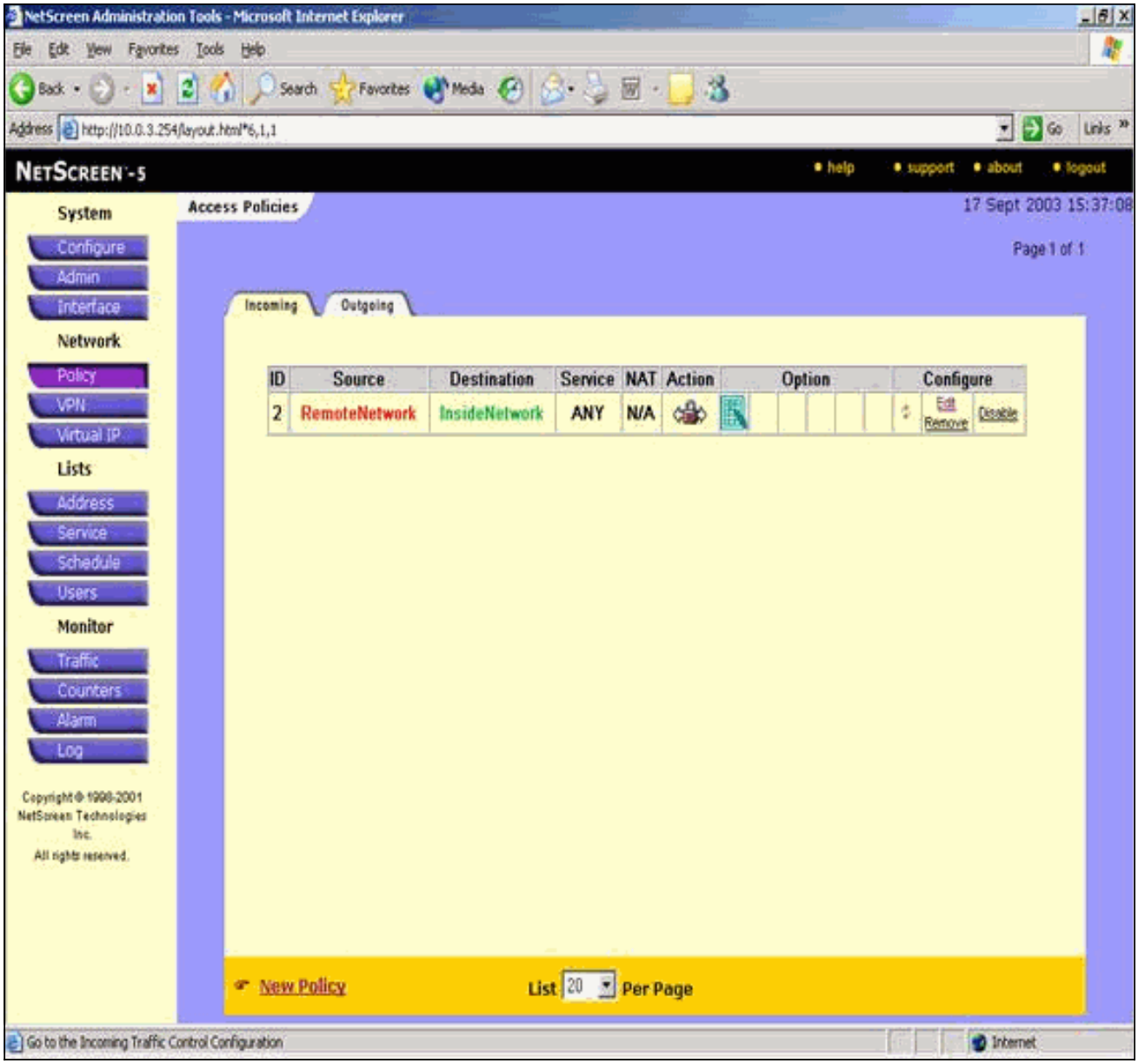
13. Selecteer **Netwerk > Beleid**, ga naar het tabblad Uitgaande en klik op **Nieuw Beleid** om de regels te configureren die encryptie van het IPsec-verkeer toestaan.
14. Voer de configuratieinformatie voor het beleid in en klik op **OK**.Dit voorbeeld gebruikt deze velden en waarden voor het beleid. Het veld Naam is optioneel en wordt in dit voorbeeld niet gebruikt.**Bronadres:** Binnennetwerk(Dit is eerder gedefinieerd op het tabblad Trusted.)**Bestemmingsadres:** Remote-Network(Dit werd eerder gedefinieerd onder het tabblad Onvertrouwd)**Service:** Alle**Actie:** Tunnel**VPN-tunnels:** VPN-1(Dit was eerder gedefinieerd als de VPN-tunnel op het tabblad AutoKey IKE.)**Een inkomend VPN-beleid wijzigen:** gecontroleerd(Deze optie maakt automatisch een inkomende regel die het verkeer van het buitennetwerk van VPN
aanpast.)



15. Wanneer het beleid wordt toegevoegd, zorg er dan voor dat de uitgaande VPN-regel eerst in de lijst met beleidsmaatregelen voorkomt. (De regel die automatisch voor inkomend verkeer wordt gemaakt, staat op het tabblad Inkomend.)Volg deze stappen als u de volgorde van het beleid wilt wijzigen:Klik op het tabblad Uitvoer.Klik de cirkelpijlen in de kolom Configure aan om het venster van de Micro van het Bewegingsbeleid te tonen.Wijzig de volgorde van het beleid zodat het VPN-beleid boven beleid-ID 0 staat (zodat het VPN-beleid bovenaan de lijst
staat).



Ga naar het tabblad Inkomend om de regel voor inkomende verkeer te bekijken.



Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat de configuratie correct werkt.

Verificatieopdrachten

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **ping**-diagnosticeert basisnetwerkconnectiviteit.
- **toon crypto ipsec sa**-shows the Phase 2 security associaties.
- **toon crypto isakmp sa** - toont de fase 1 veiligheidsassociaties.

Verificatieoutput

Hier wordt een voorbeelduitvoer van **ping-** en **show**-opdrachten weergegeven.

Dit ping wordt gestart vanuit een host achter de 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
```

Uitvoer van de **show crypto ipsec als** opdracht wordt hier getoond.

```
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:
```

Uitvoer van de **show crypto isakmp als** opdracht wordt hier getoond.

```
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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

- **debug van crypto motor**-displays over cryptomotoren.
- **debug van crypto ipsec** - informatie over IPsec gebeurtenissen.
- **debug van crypto isakmp**-displays over IKE gebeurtenissen.

Voorbeeld van output van foutopsporing

U vindt hier voorbeelden van debug-uitvoer van de PIX-firewall.

```
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
```

Gerelateerde informatie

- IPsec-onderhandeling/IKE-protocollen
- Cisco PIX-firewallsoftware
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems