Configurazione del tunnel IPSec LAN-LAN tra Cisco Pix Firewall e un firewall NetScreen

Sommario

Introduzione

In questo documento viene descritta la procedura necessaria per creare un tunnel LAN-LAN IPsec tra un firewall Cisco PIX e un firewall NetScreen con il software più recente. Dietro ogni dispositivo è presente una rete privata che comunica con l'altro firewall tramite il tunnel IPsec.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Il firewall NetScreen è configurato con gli indirizzi IP nelle interfacce trust/untrust.
- Viene stabilita la connessione a Internet.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Software PIX Firewall versione 6.3(1)
- Ultima revisione NetScreen

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:

Configurazioni

Nel documento vengono usate queste configurazioni:

- PIX Firewall
- Firewall NetScreen

Configurazione del firewall PIX

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`

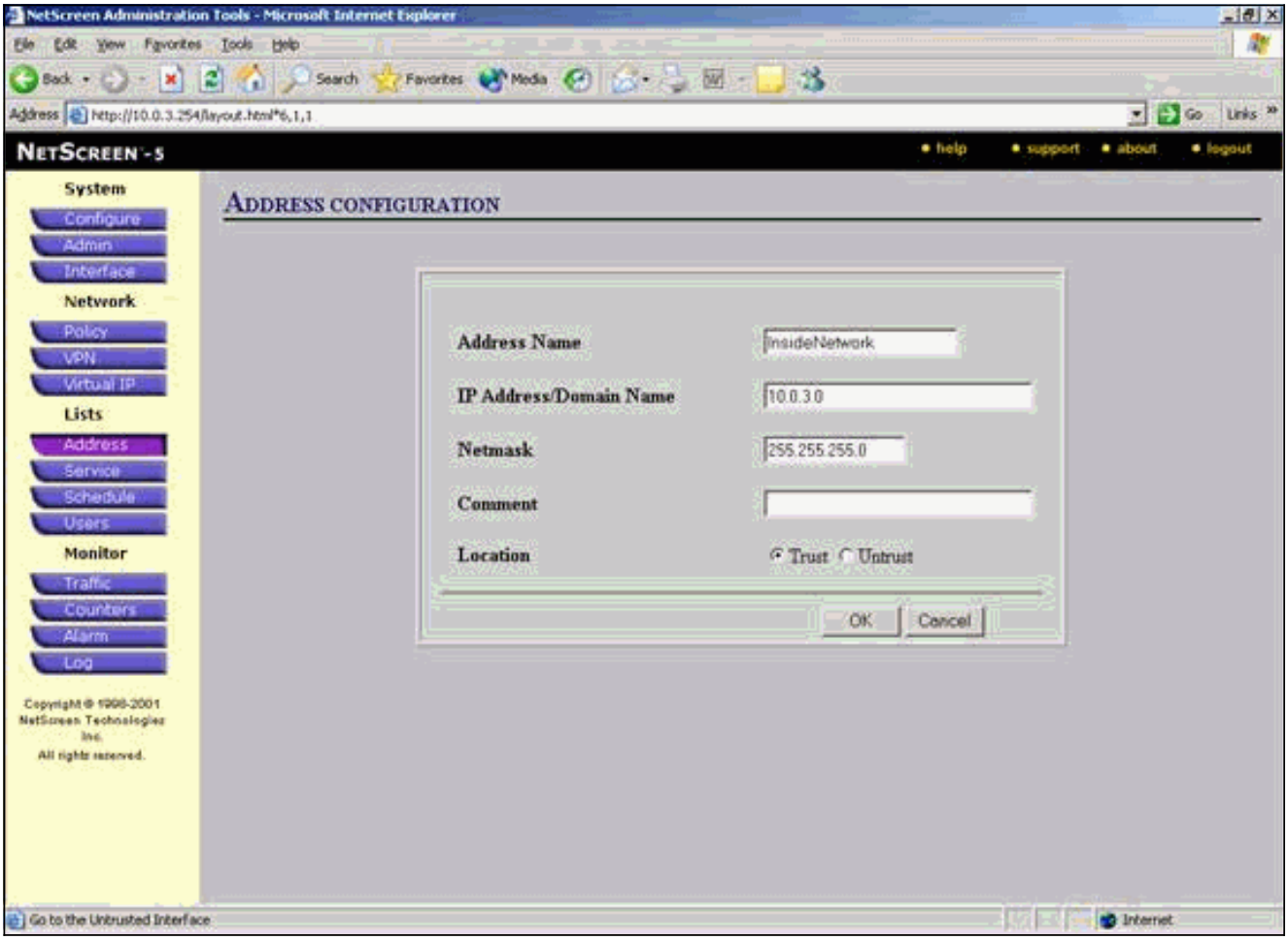
```
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip 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
```

Configurazione del firewall NetScreen

Completare questa procedura per configurare il firewall NetScreen.

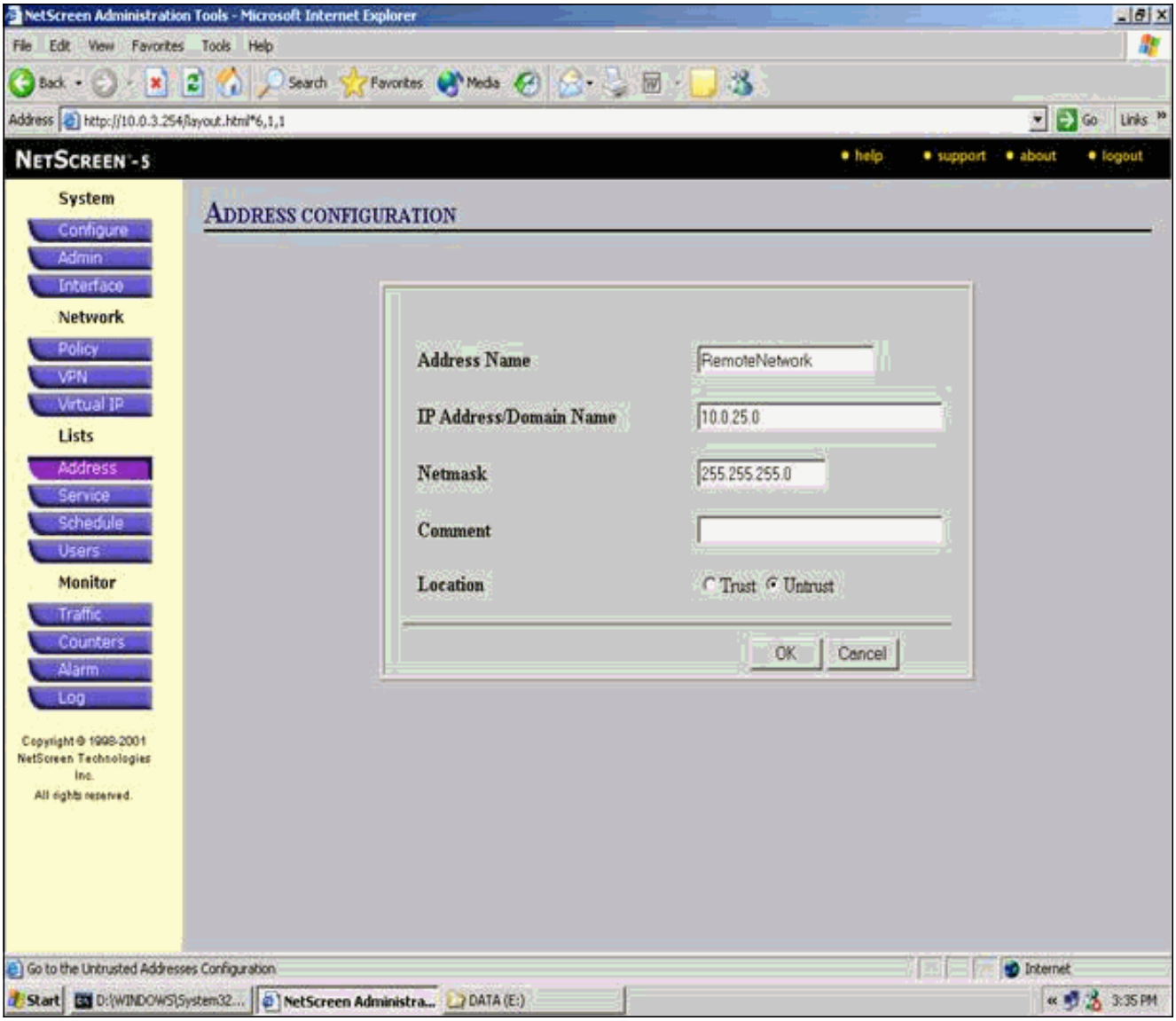
1. Selezionare **Elenchi > Indirizzo**, andare alla scheda Attendibile e fare clic su **Nuovo indirizzo**.
2. Aggiungere la rete interna NetScreen crittografata sul tunnel e fare clic su **OK**.**Nota:** assicurarsi che l'opzione Trust sia selezionata.Nell'esempio, viene usata la rete 10.0.3.0 con una maschera di 255.255.255.0.



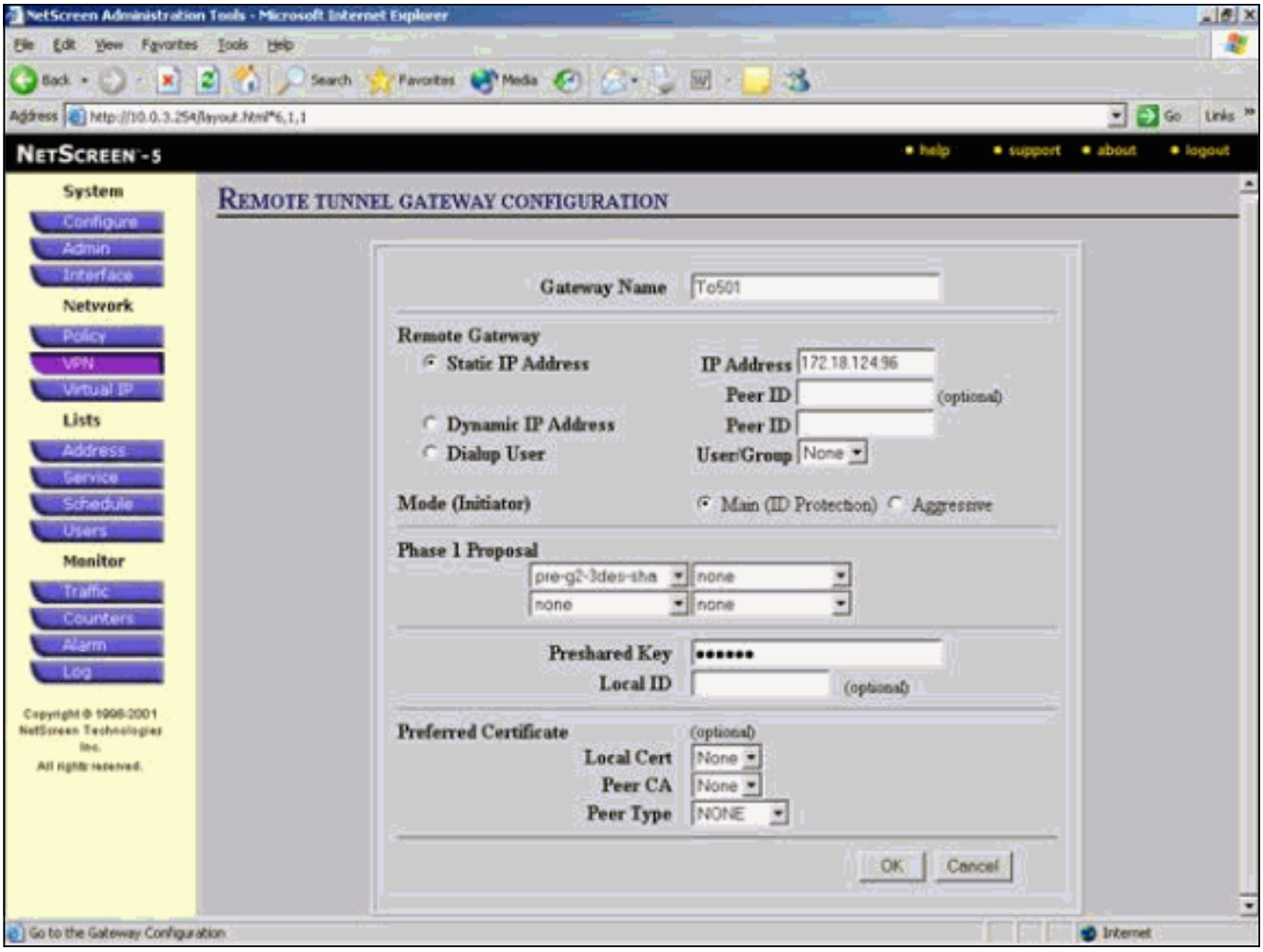
3. Selezionare **Elenchi > Indirizzo**, andare alla scheda Non attendibile e fare clic su **Nuovo**

indirizzo.

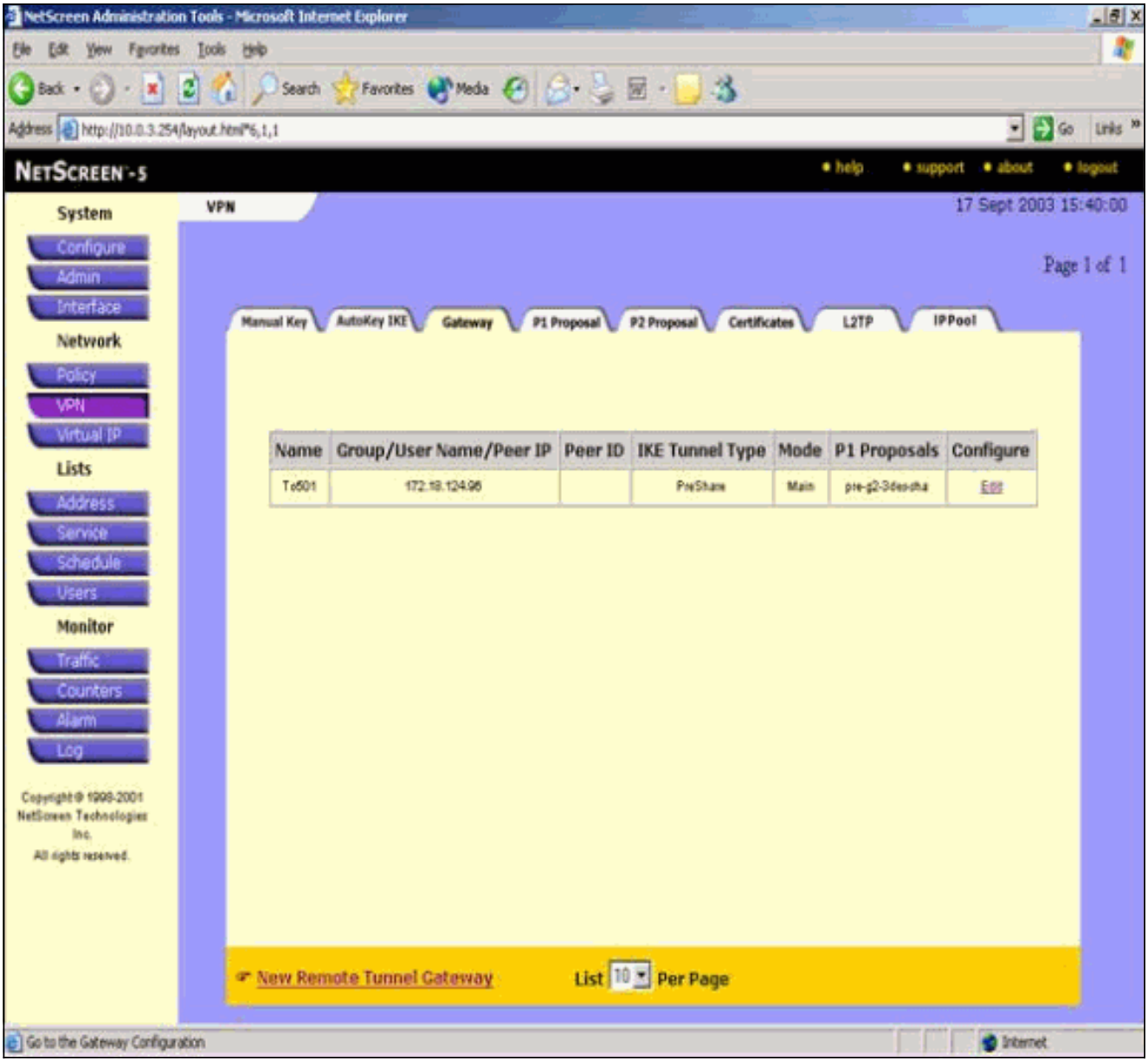
4. Aggiungere la rete remota utilizzata da NetScreen Firewall per crittografare i pacchetti e fare clic su **OK**.**Nota:** non utilizzare i gruppi di indirizzi quando si configura una VPN per un gateway non NetScreen. L'interoperabilità VPN non riesce se si utilizzano gruppi di indirizzi. Il gateway di protezione non NetScreen non è in grado di interpretare l'ID proxy creato da NetScreen quando viene utilizzato il gruppo di indirizzi.Per risolvere questo problema, sono disponibili due soluzioni:Separare i gruppi di indirizzi in singole voci della rubrica. Specificare i singoli criteri in base alla voce della rubrica.Se possibile, configurare l'ID proxy su 0.0.0.0/0 sul gateway non NetScreen (dispositivo firewall).Nell'esempio, viene usata la rete 10.0.25.0 con una maschera di
255.255.255.0.



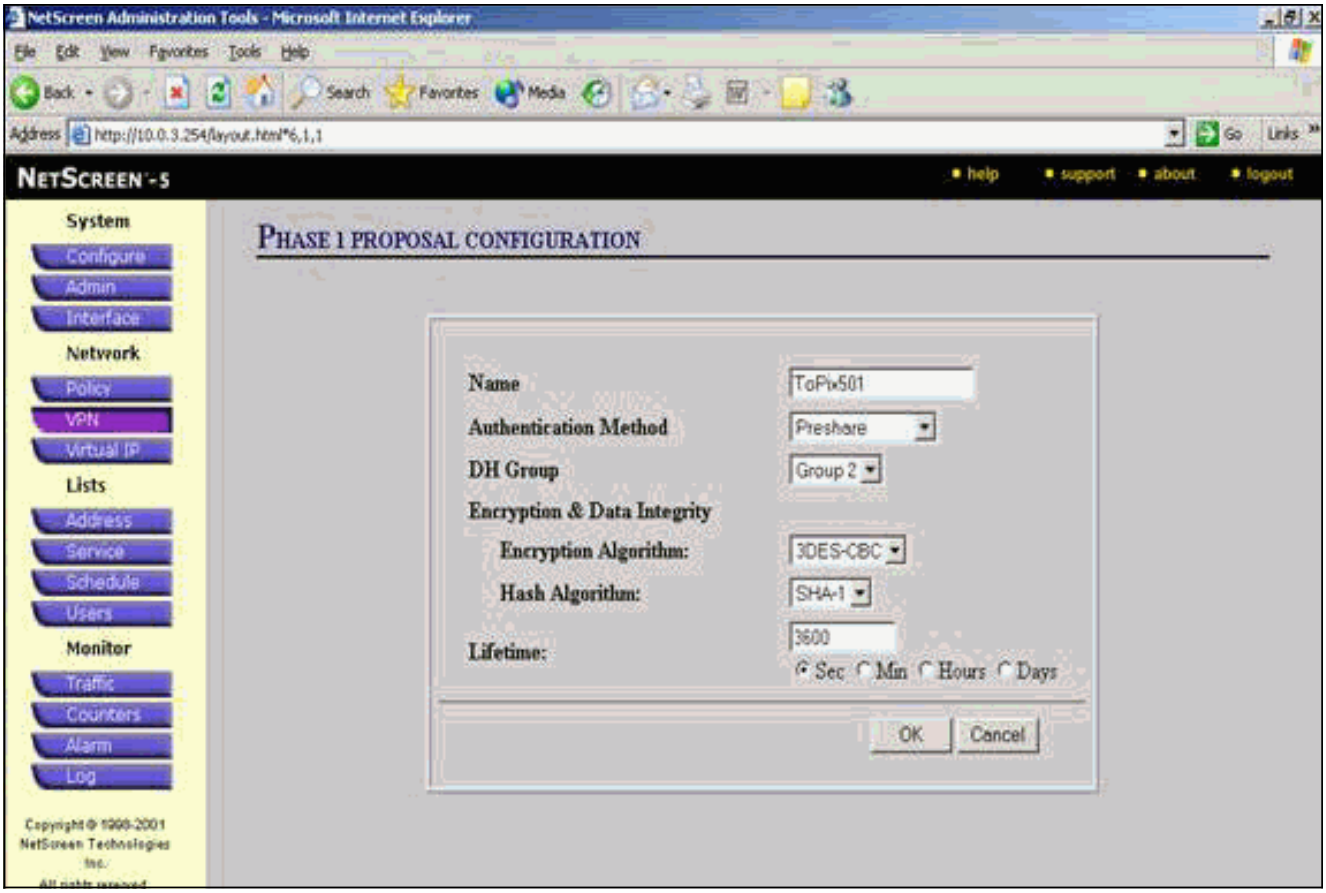
5. Selezionare **Rete > VPN**, andare alla scheda Gateway e fare clic su **Nuovo gateway tunnel remoto** per configurare il gateway VPN (criteri IPsec fase 1 e fase 2).
6. Usare l'indirizzo IP dell'interfaccia esterna del PIX per terminare il tunnel e configurare le opzioni IKE della fase 1 da associare. Al termine, fare clic su **OK**.In questo esempio vengono utilizzati i campi e i valori seguenti.**Nome gateway:** A501**Indirizzo IP statico:** 172.18.124.96**Modalità:** Principale (protezione ID)**Chiave già condivisa:** "testme"**Proposta fase 1:** pre-g2-3des-
sha



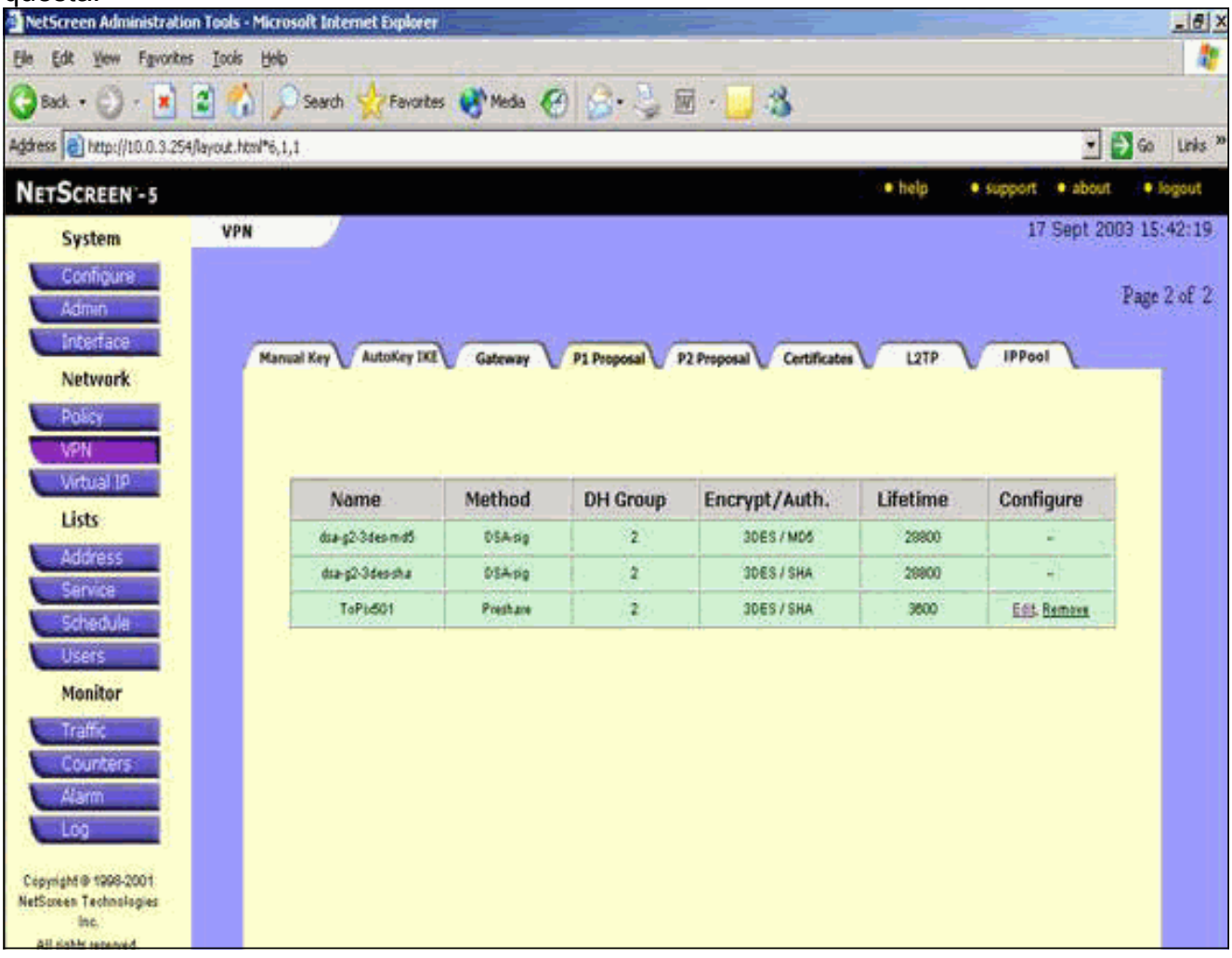
Una volta creato il gateway del tunnel remoto, viene visualizzata una schermata simile a questa.



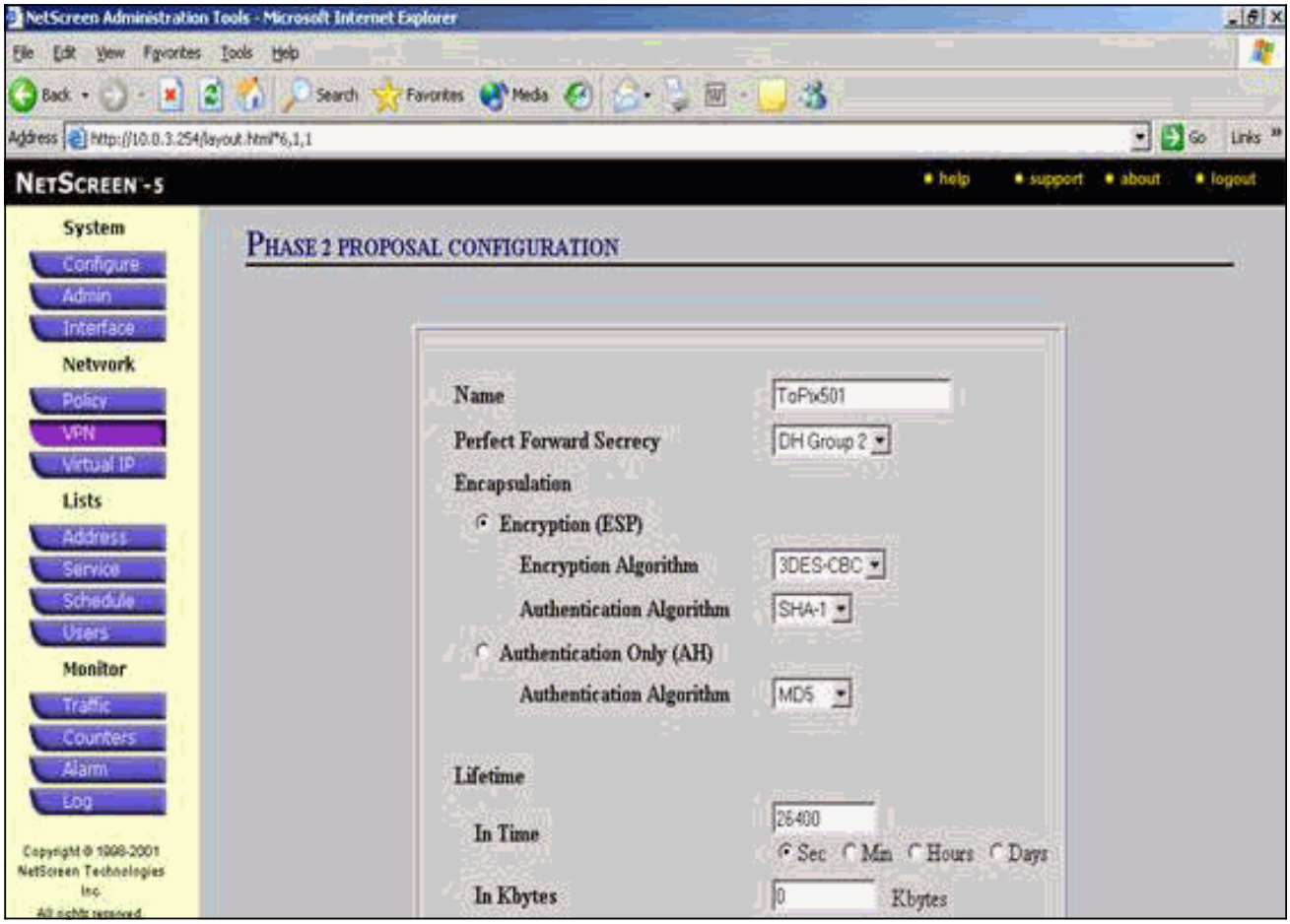
7. Andare alla scheda Proposta P1 e fare clic su **Nuova proposta fase 1** per configurare la proposta 1.
8. Immettere le informazioni di configurazione per la proposta di fase 1 e fare clic su **OK**.In questo esempio vengono utilizzati questi campi e valori per lo scambio Fase 1.**Nome:** ToPix501**Autenticazione:** Precondivisione**Gruppo DH:** Gruppo 2**Crittografia:** 3DES-CBC**Hash:** SHA-1**Durata:** 3600
sec.



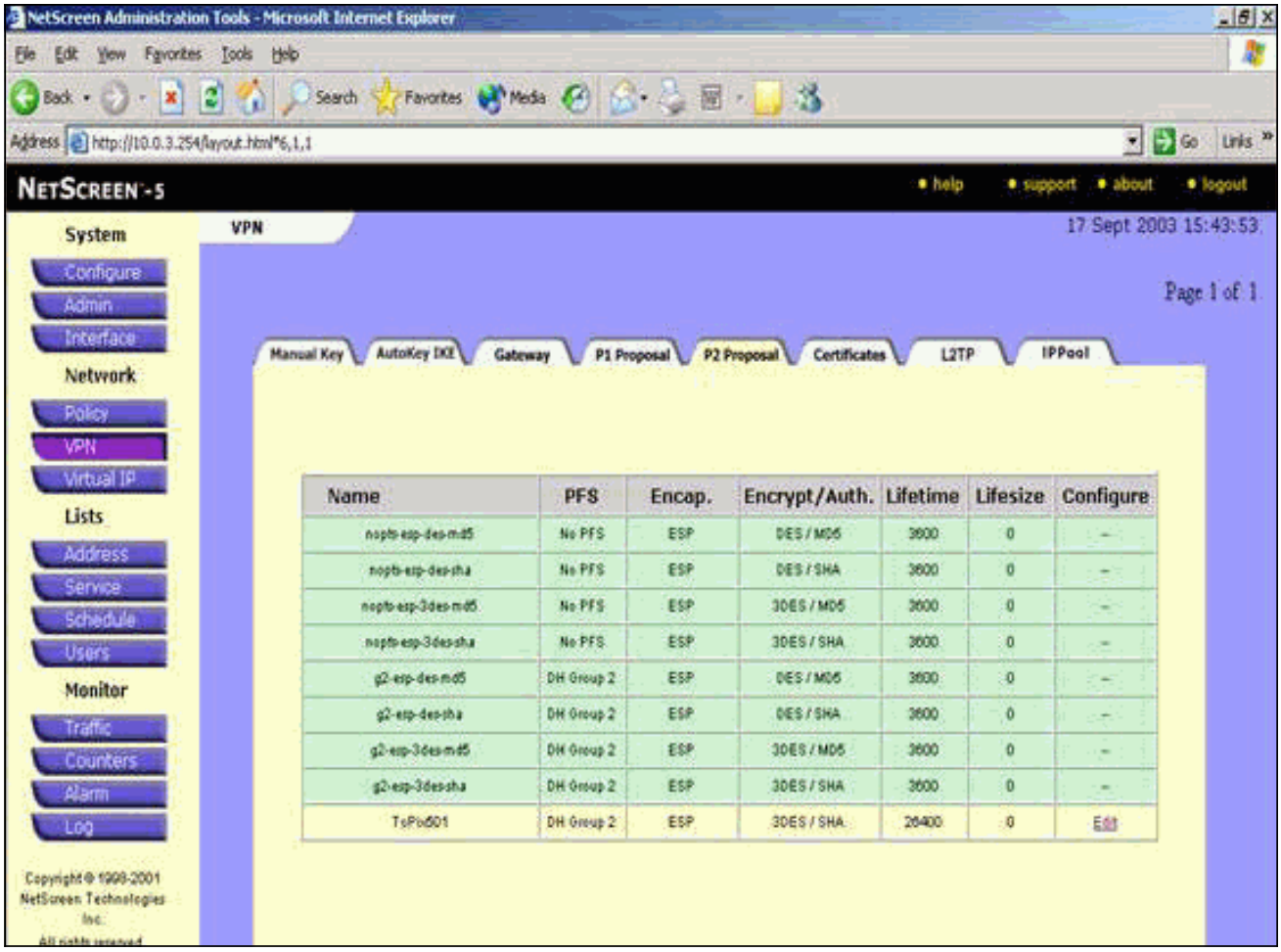
Quando la fase 1 è stata aggiunta correttamente alla configurazione NetScreen, viene visualizzata una schermata simile a questa.



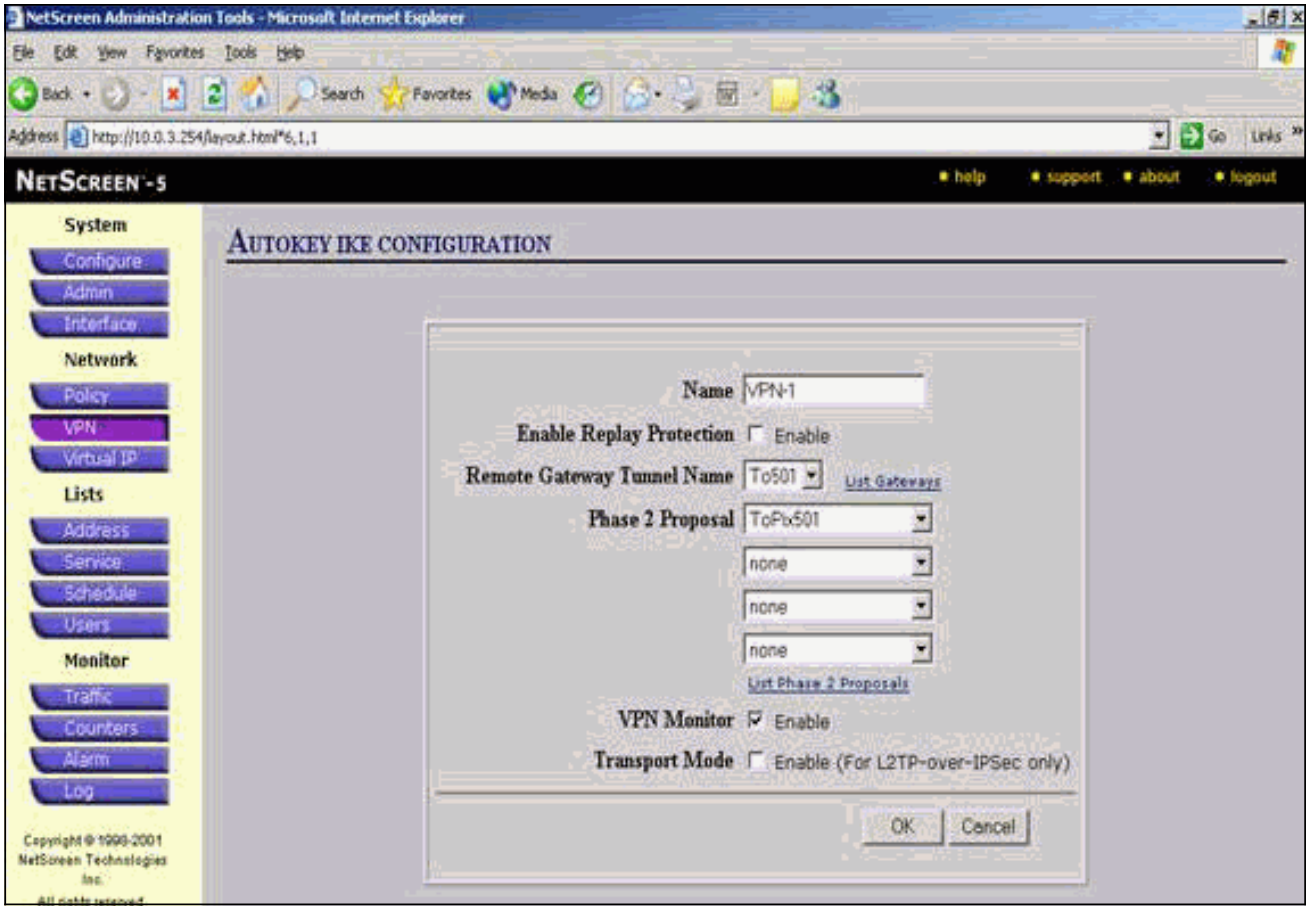
9. Andare alla scheda Proposta P2 e fare clic su **Nuova proposta fase 2** per configurare la fase 2.
10. Immettere le informazioni di configurazione per la proposta per la fase 2 e fare clic su **OK**.In questo esempio vengono utilizzati questi campi e valori per lo scambio Fase 2.**Nome:** ToPix501**Perfect Forward Secrecy:** DH-2 (1024 bit)**Algoritmo di crittografia:** 3DES-CBC**Algoritmo di autenticazione:** SHA-1**Durata:** 26400
sec



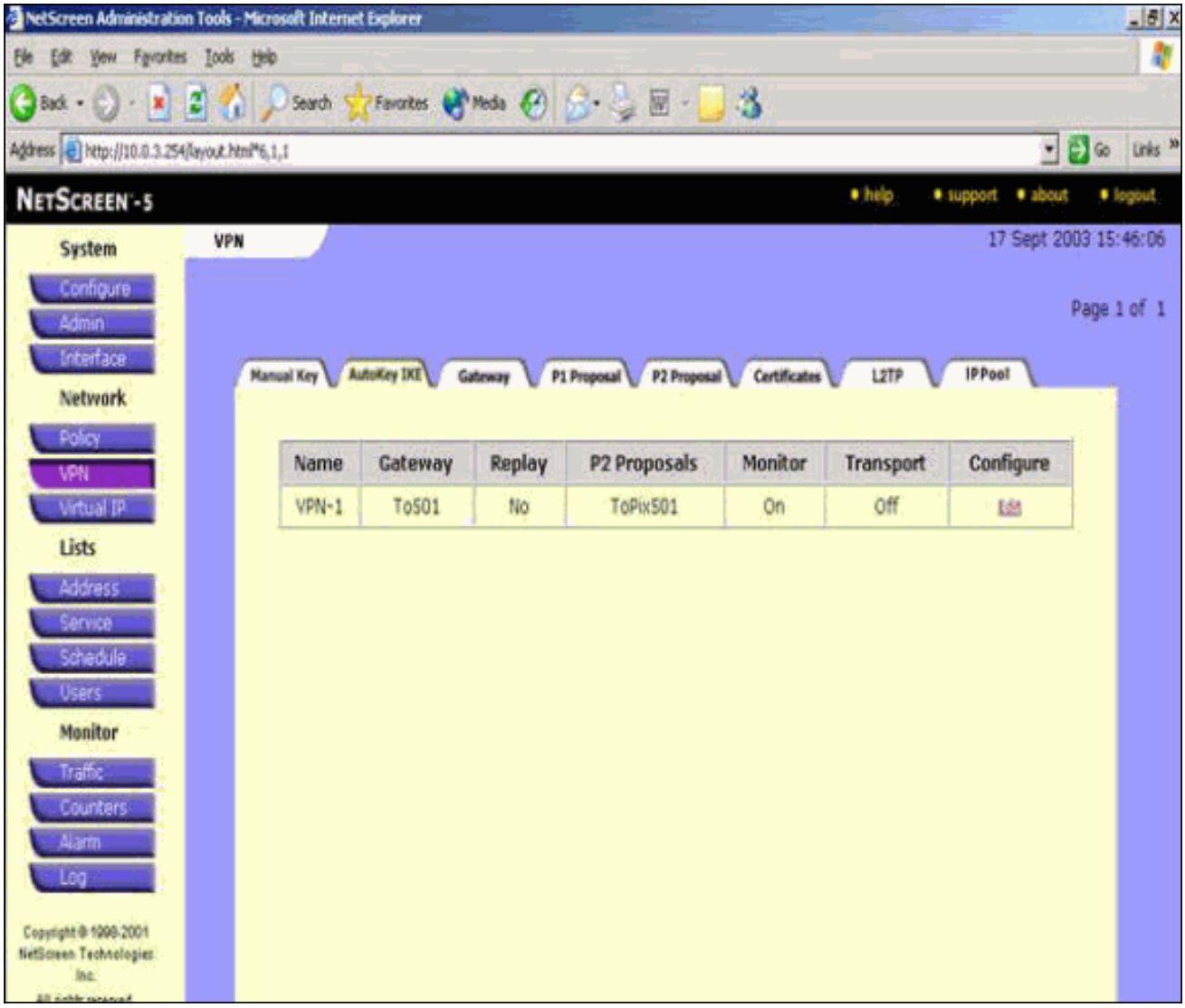
Quando la fase 2 è stata aggiunta correttamente alla configurazione NetScreen, viene visualizzata una schermata simile a
questa.



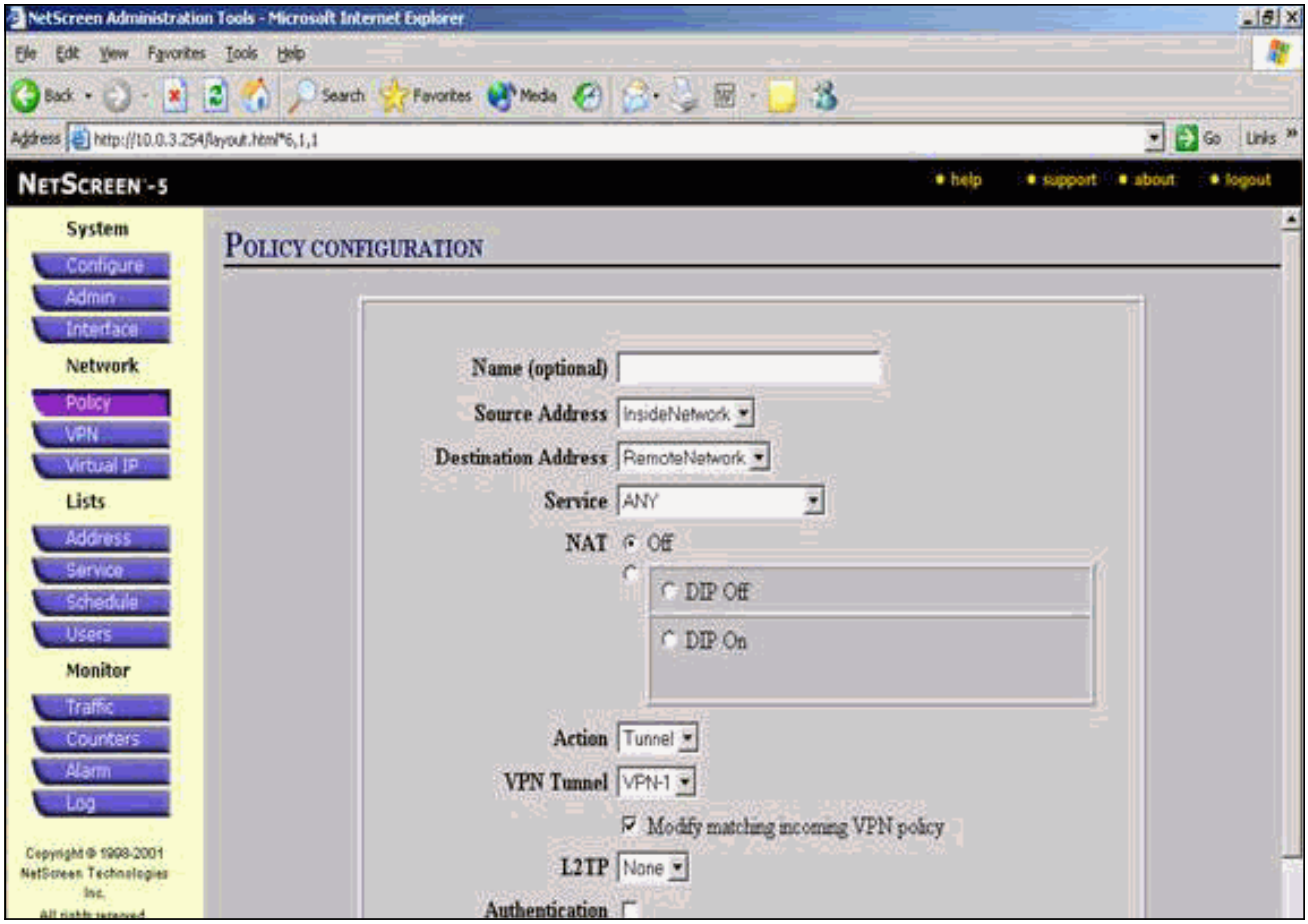
11. Selezionare la scheda **AutoKey IKE**, quindi fare clic su **Nuova voce IKE AutoKey** per creare e configurare AutoKey IKE.
12. Immettere le informazioni di configurazione per AutoKey IKE e quindi fare clic su **OK**.In questo esempio vengono utilizzati questi campi e valori per AutoKey IKE.**Nome:** VPN-1**Nome tunnel gateway remoto:** A501Questa opzione è stata creata in precedenza nella scheda Gateway.**Proposta fase 2:** ToPix501Questa opzione è stata creata in precedenza nella scheda Proposta P2.**Monitor VPN:** AttivaIn questo modo il dispositivo NetScreen può impostare le trap SNMP (Simple Network Management Protocol) per monitorare le condizioni del monitor
VPN.



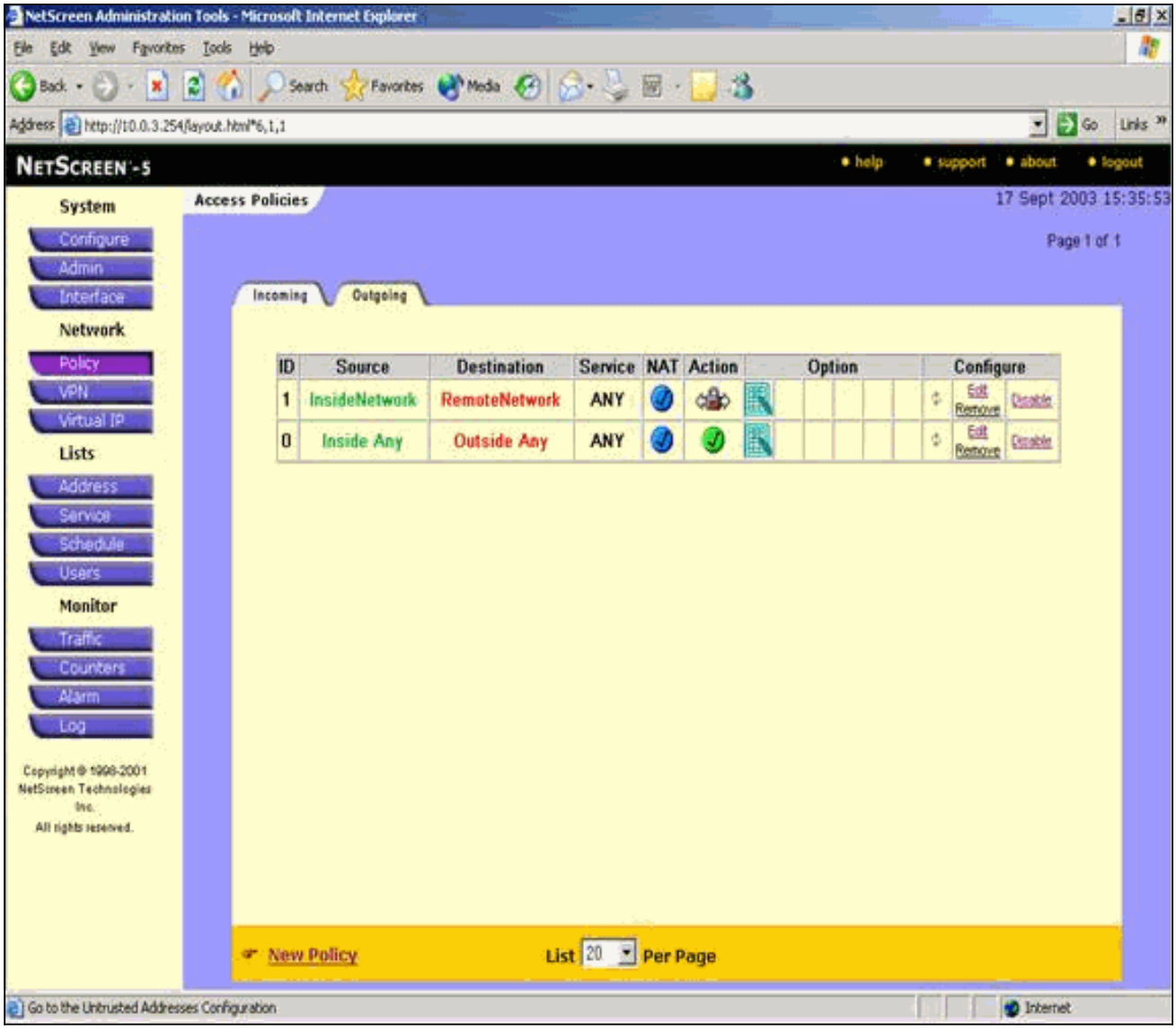
Una volta configurata correttamente la regola VPN-1, viene visualizzata una schermata simile a quella
dell'esempio.



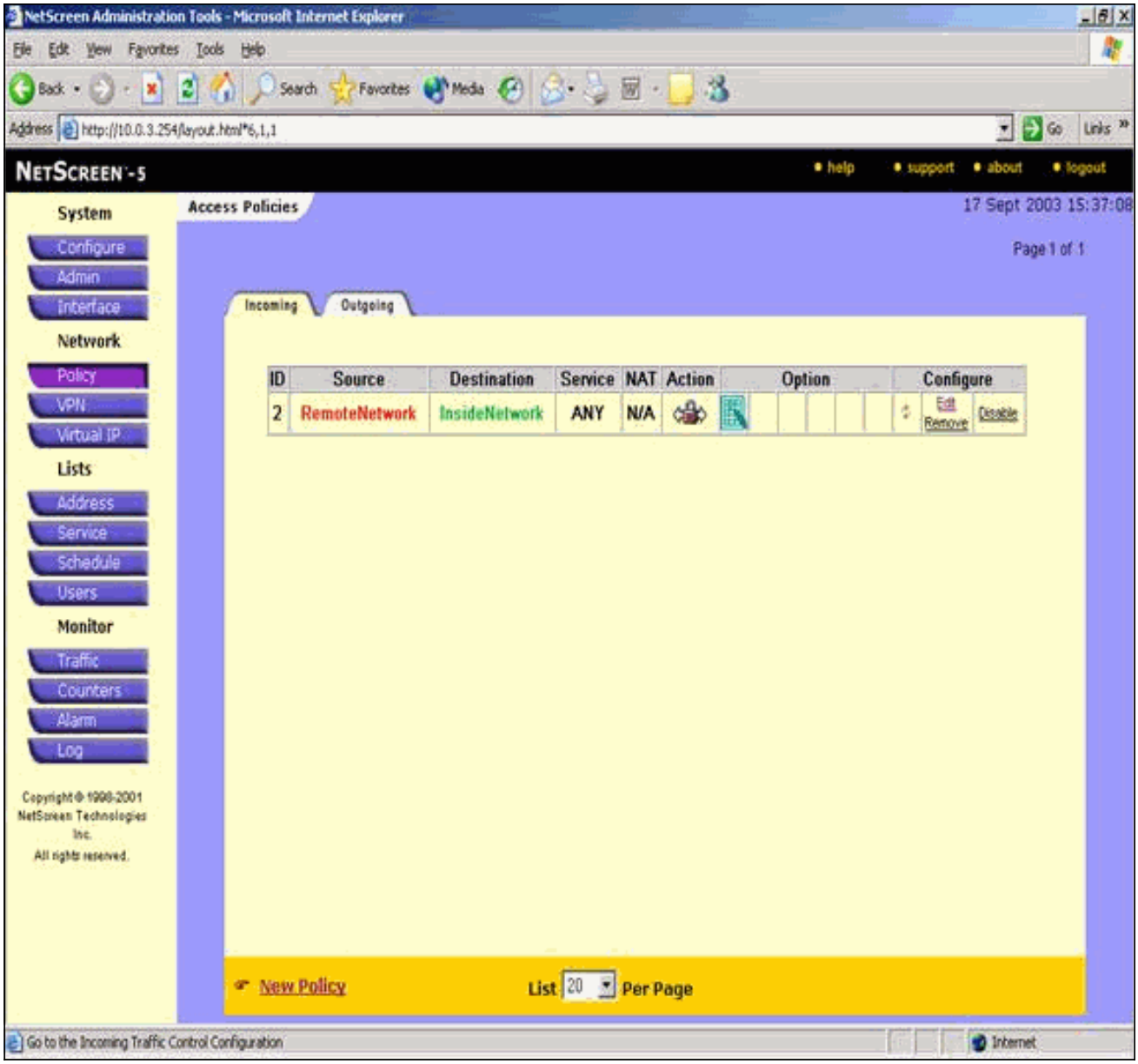
13. Selezionare **Rete > Criterio**, andare alla scheda In uscita e fare clic su **Nuovo criterio** per configurare le regole che consentono la crittografia del traffico IPSec.
14. Immettere le informazioni di configurazione per il criterio e fare clic su **OK**.In questo esempio vengono utilizzati questi campi e valori per il criterio. Il campo Name (Nome) è facoltativo e non viene utilizzato in questo esempio.**Source address:** All'interno della reteQuesta impostazione è stata definita in precedenza nella scheda Attendibile.**Indirizzo di destinazione:** ReteRemotaQuesta impostazione è stata definita in precedenza nella scheda Non attendibile.**Servizio:** Qualsiasi**Azione:** Tunnel**Tunnel VPN:** VPN-1(precedentemente definito come tunnel VPN nella scheda AutoKey IKE).**Modifica criterio VPN in ingresso corrispondente:** ControllatoQuesta opzione crea automaticamente una regola in entrata che corrisponde al traffico VPN della rete
esterna.



15. Quando il criterio viene aggiunto, verificare che la regola VPN in uscita sia la prima nell'elenco dei criteri. La regola creata automaticamente per il traffico in entrata si trova nella scheda In entrata.Completare questi passaggi se è necessario modificare l'ordine dei criteri:Fare clic sulla scheda In uscita.Fare clic sulle frecce circolari nella colonna Configura per visualizzare la finestra Sposta macro criteri.Modificare l'ordine dei criteri in modo che il criterio VPN sia superiore all'ID criterio 0 (in modo che il criterio VPN sia in cima all'elenco).



Andare alla scheda In entrata per visualizzare la regola per il traffico in entrata.



Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

Comandi di verifica

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

- **ping** - Esegue la diagnosi della connettività di rete di base.
- **show crypto ipsec sa**: visualizza le associazioni di sicurezza della fase 2.
- **show crypto isakmp sa**: visualizza le associazioni di sicurezza della fase 1.

Output verifica

Di seguito è riportato un esempio di output dei comandi **ping** e **show**.

Il ping viene avviato da un host dietro il 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
```

Di seguito è riportato l'output del comando **show crypto ipsec sa**.

```
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:
```

Di seguito è riportato l'output del comando **show crypto isakmp sa**.

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug**.

- **debug crypto engine**: visualizza i messaggi relativi ai motori di crittografia.
- **debug crypto ipsec**: visualizza le informazioni sugli eventi IPsec.
- **debug crypto isakmp**: visualizza i messaggi sugli eventi IKE.

Output di esempio del comando debug

Di seguito è riportato un esempio di output del comando **debug** per il 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
```

Informazioni correlate

- Negoziazione IPSec/protocolli IKE
- Software Cisco PIX Firewall
- Riferimenti per i comandi di Cisco Secure PIX Firewall
- Avvisi sui prodotti per la sicurezza (inclusi PIX)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems