Configuration du tunnel IPSec LAN à LAN entre le pare-feu Cisco Pix et un pare-feu NetScreen

Contenu

Introduction

Ce document décrit la procédure pour créer un tunnel IPsec réseau à réseau entre un pare-feu Cisco PIX et un pare-feu NetScreen au moyen du logiciel le plus récent. Un réseau privé derrière chaque périphérique communique à l'autre pare-feu par l'intermédiaire du tunnel IPsec.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Le pare-feu NetScreen est configuré avec les adresses IP sur les interfaces trust/untrust.
- La connectivité est établie à Internet.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel pare-feu PIX version 6.3(1)
- Dernière révision 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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations suivantes :

- Pare-feu PIX
- Pare-feu NetScreen

Configurer le pare-feu PIX

Pare-feu 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`

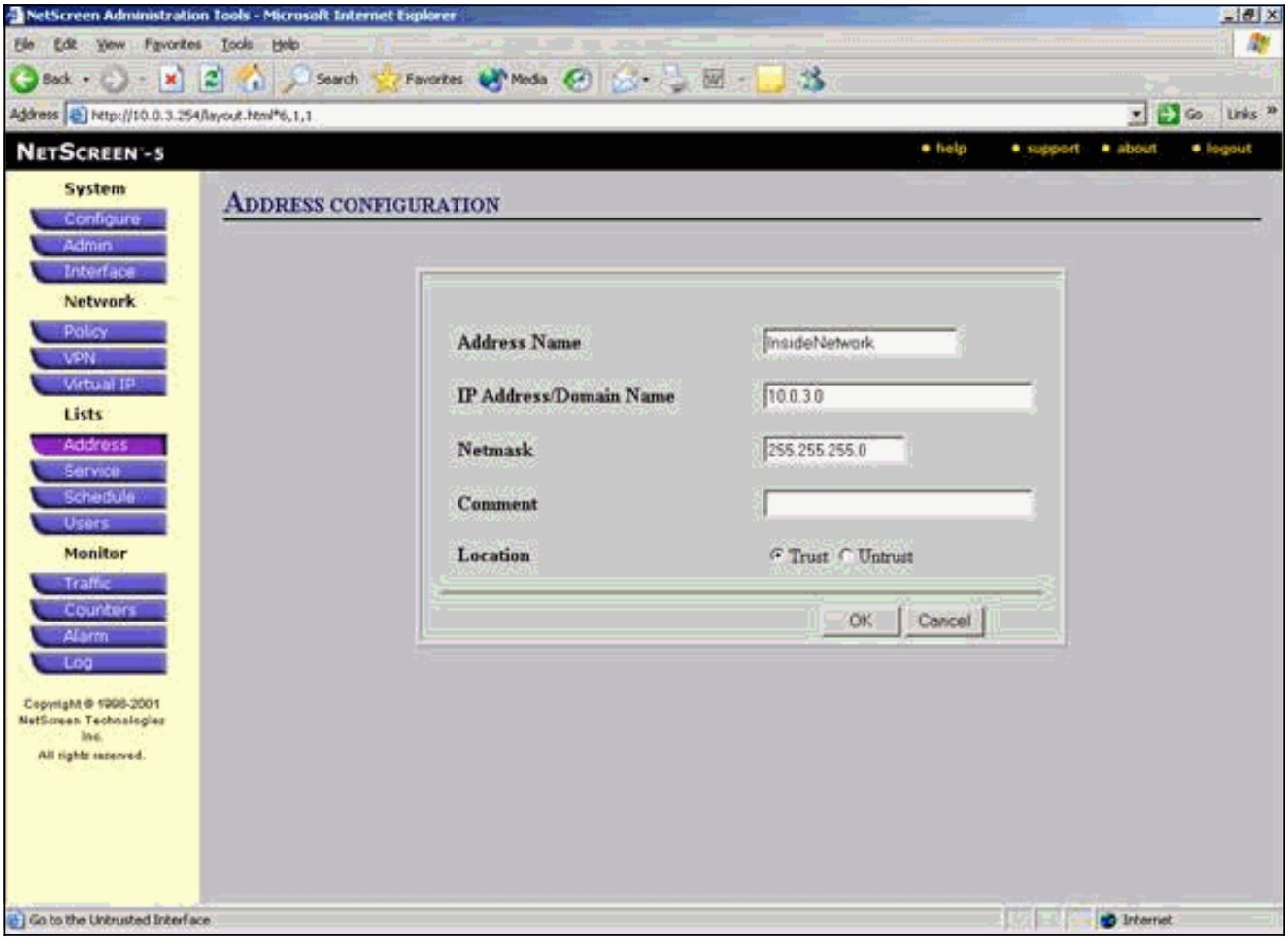
```
hostname pixfirewall
domain-name cisco.com
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
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
```

Configurer le pare-feu NetScreen

Complétez ces étapes afin de configurer le pare-feu NetScreen.

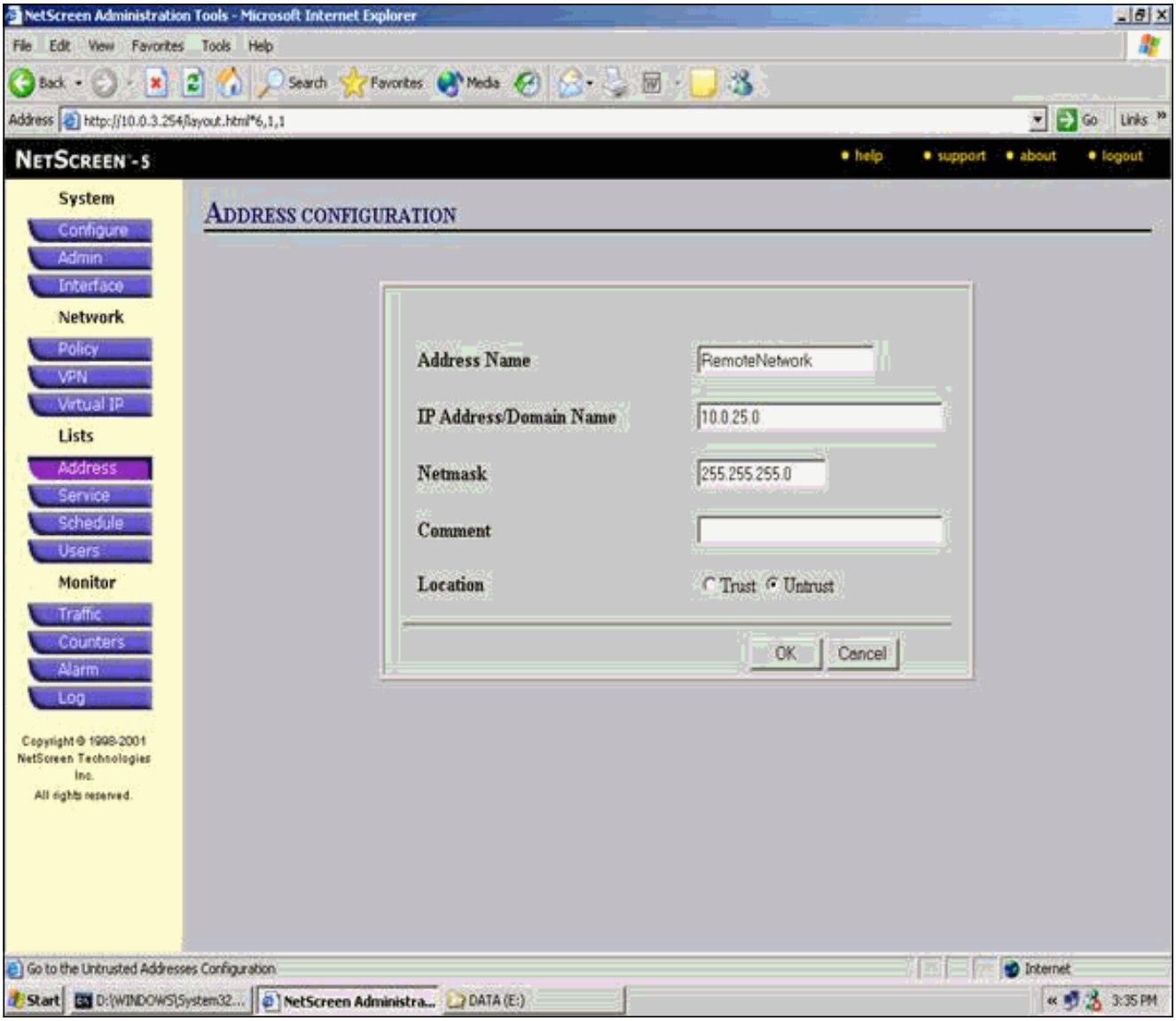
1. Sélectionnez **Lists > Address**, accédez à l'onglet Trusted, puis cliquez sur **New Address**.
2. Ajoutez le réseau interne NetScreen chiffré sur le tunnel et cliquez sur **OK**.**Remarque :** assurez-vous que l'option Approbation est sélectionnée.Cet exemple utilise le réseau 10.0.3.0 avec le masque 255.255.255.0.



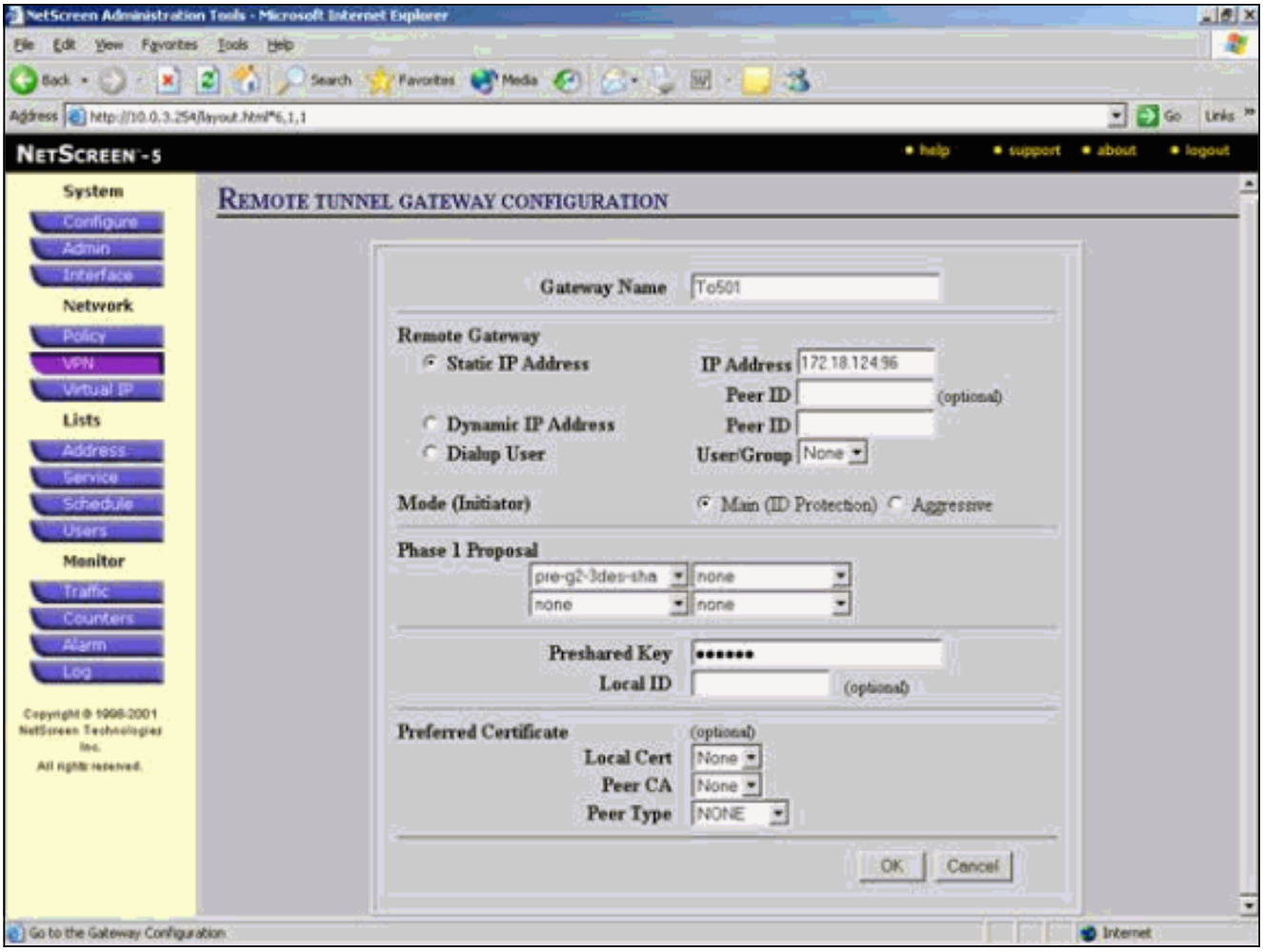
3. Sélectionnez **Listes > Adresse**, accédez à l'onglet Non approuvé, puis cliquez sur **Nouvelle**

adresse.

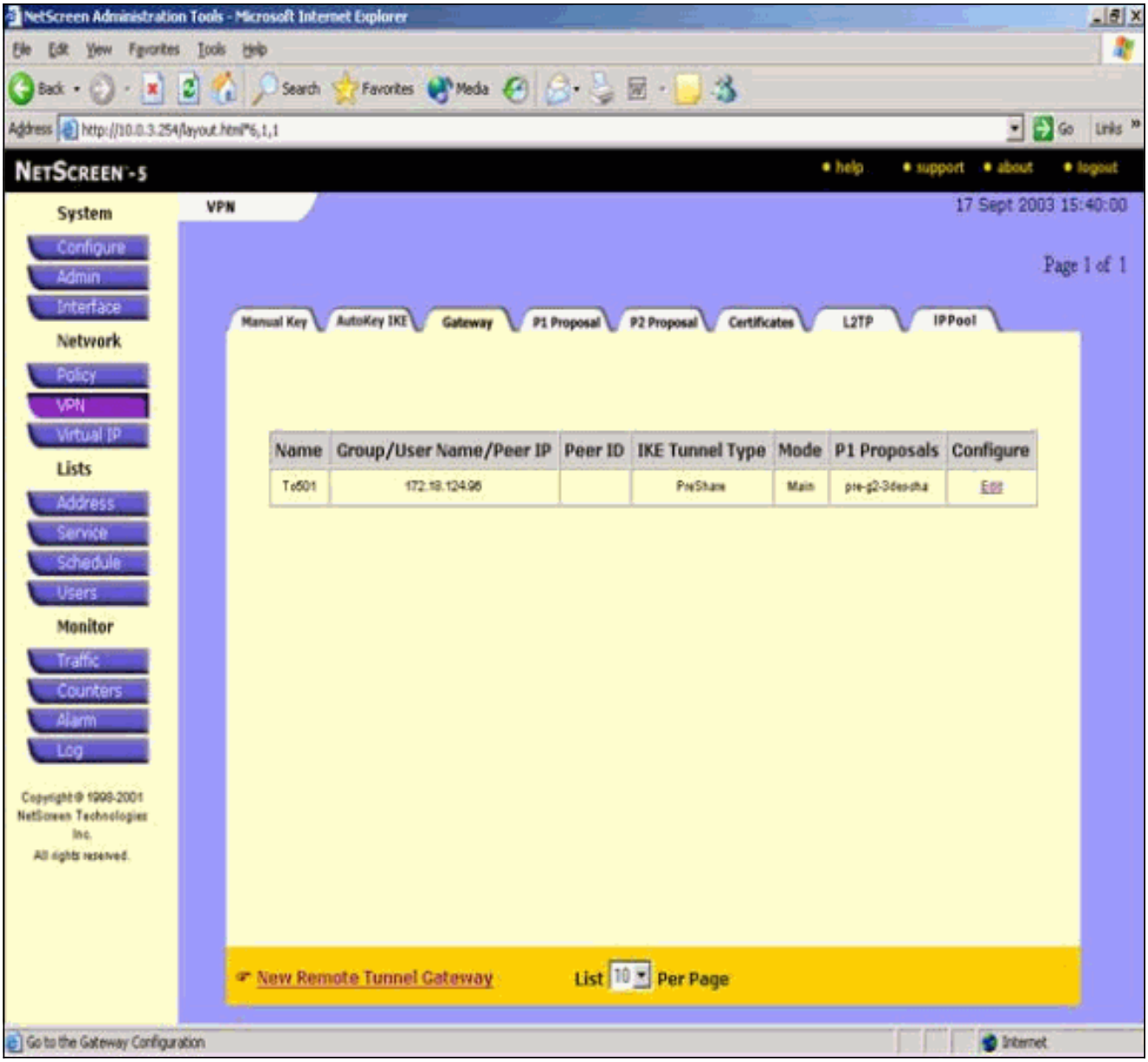
4. Ajoutez le réseau distant utilisé par NetScreen Firewall lors du chiffrement des paquets et cliquez sur **OK**.**Remarque :** N'utilisez pas de groupes d'adresses lorsque vous configurez un VPN sur une passerelle non NetScreen. L'interopérabilité VPN échoue si vous utilisez des groupes d'adresses. La passerelle de sécurité non NetScreen ne sait pas comment interpréter l'ID de proxy créé par NetScreen lorsque le groupe d'adresses est utilisé.Il y a quelques solutions pour cela :Séparez les groupes d'adresses en entrées de carnet d'adresses individuelles. Spécifiez des stratégies individuelles par entrée de carnet d'adresses.Configurez l'ID de proxy sur 0.0.0.0/0 sur la passerelle non NetScreen (périphérique pare-feu) si possible.Cet exemple utilise le réseau 10.0.25.0 avec le masque 255.255.255.0.



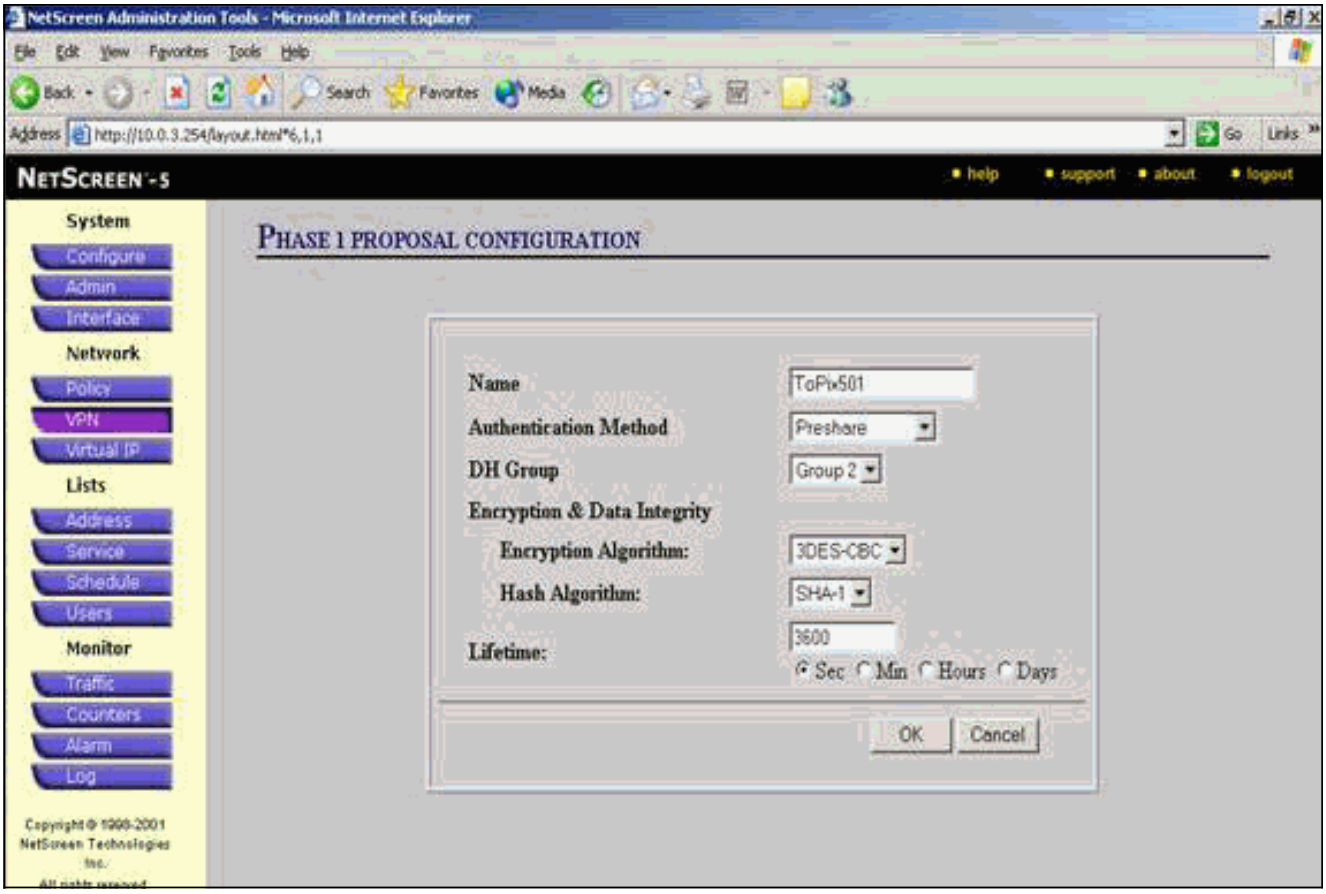
5. Sélectionnez **Réseau > VPN**, accédez à l'onglet Passerelle, puis cliquez sur **Nouvelle passerelle de tunnel distant** pour configurer la passerelle VPN (stratégies IPsec des phases 1 et 2).
6. Utilisez l'adresse IP de l'interface externe du PIX afin de terminer le tunnel, et configurez les options IKE de phase 1 pour la liaison. Cliquez sur **OK quand vous avez terminé.**Cet exemple utilise ces champs et ces valeurs.**Nom de la passerelle :** À501**Adresse IP statique:** 172.18.124.96**Mode :** Principal (Protection des ID)**Clé prépartagée :** « testme »**Proposition de la phase 1 :** pré-g2-3des-
sha



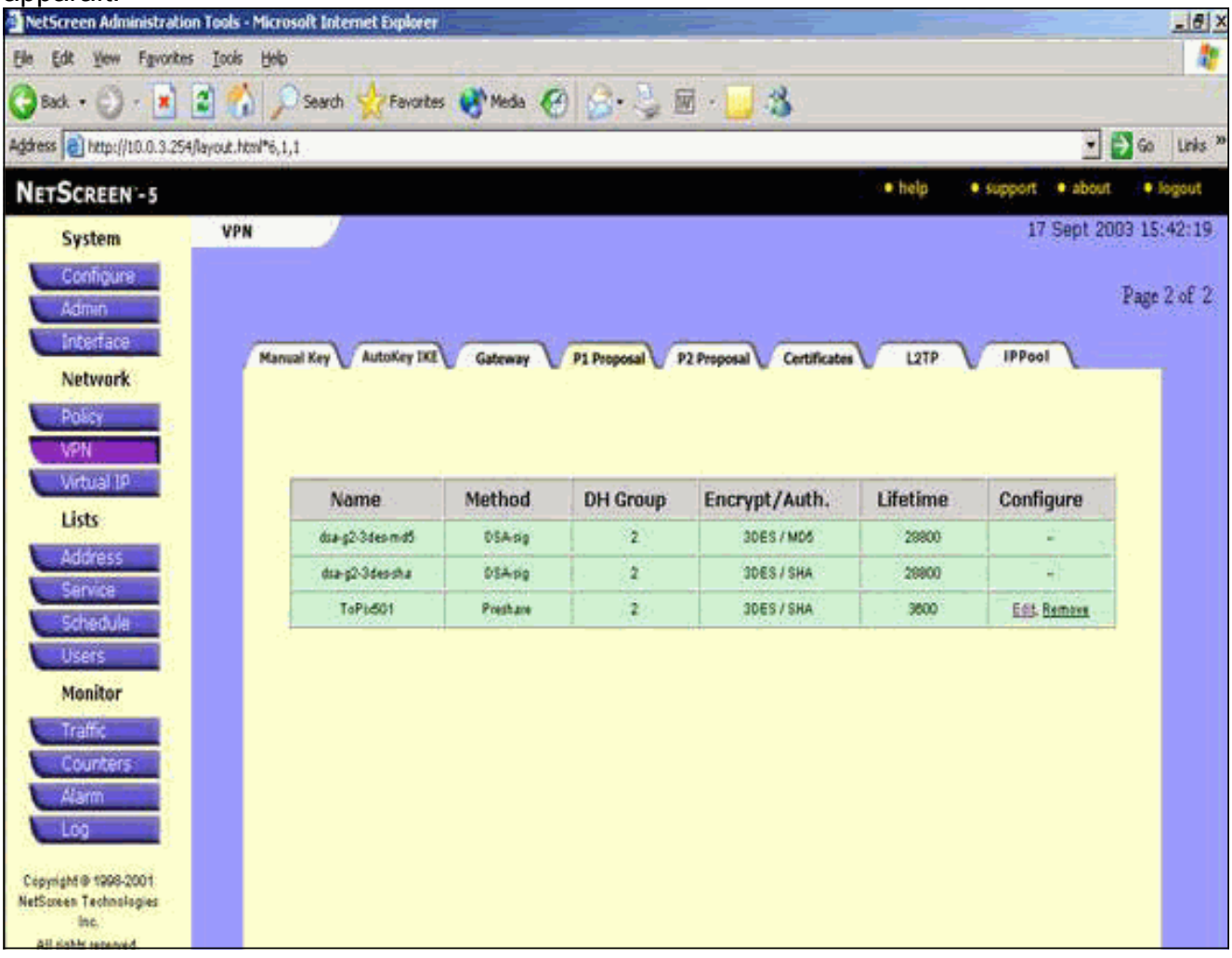
Lorsque la passerelle de tunnel distante est créée, un écran similaire à celui-ci s'affiche.



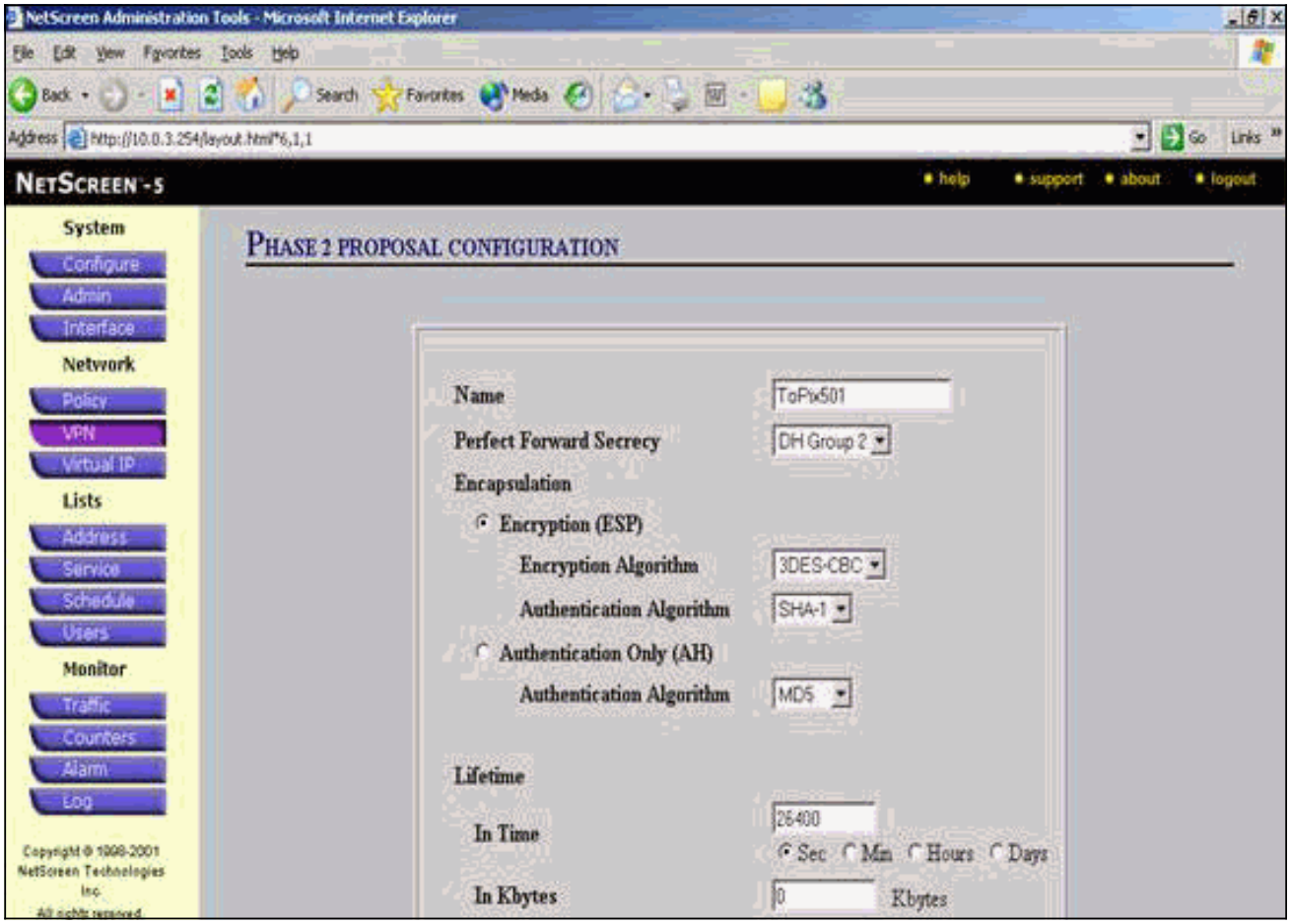
7. Accédez à l'onglet Proposition P1 et cliquez sur **Nouvelle proposition de phase 1** pour configurer la proposition 1.
8. Entrez les informations de configuration de la proposition de phase 1 et cliquez sur **OK**.Cet exemple utilise ces champs et ces valeurs pour l'échange de phase 1.**Name :** ToPix501**Authentification:** Éclairage**Groupe DH :** Groupe 2**Chiffrement :** 3DES-CBC**Hachage :** SHA-1**Durée de vie :** 3600
   Sec.



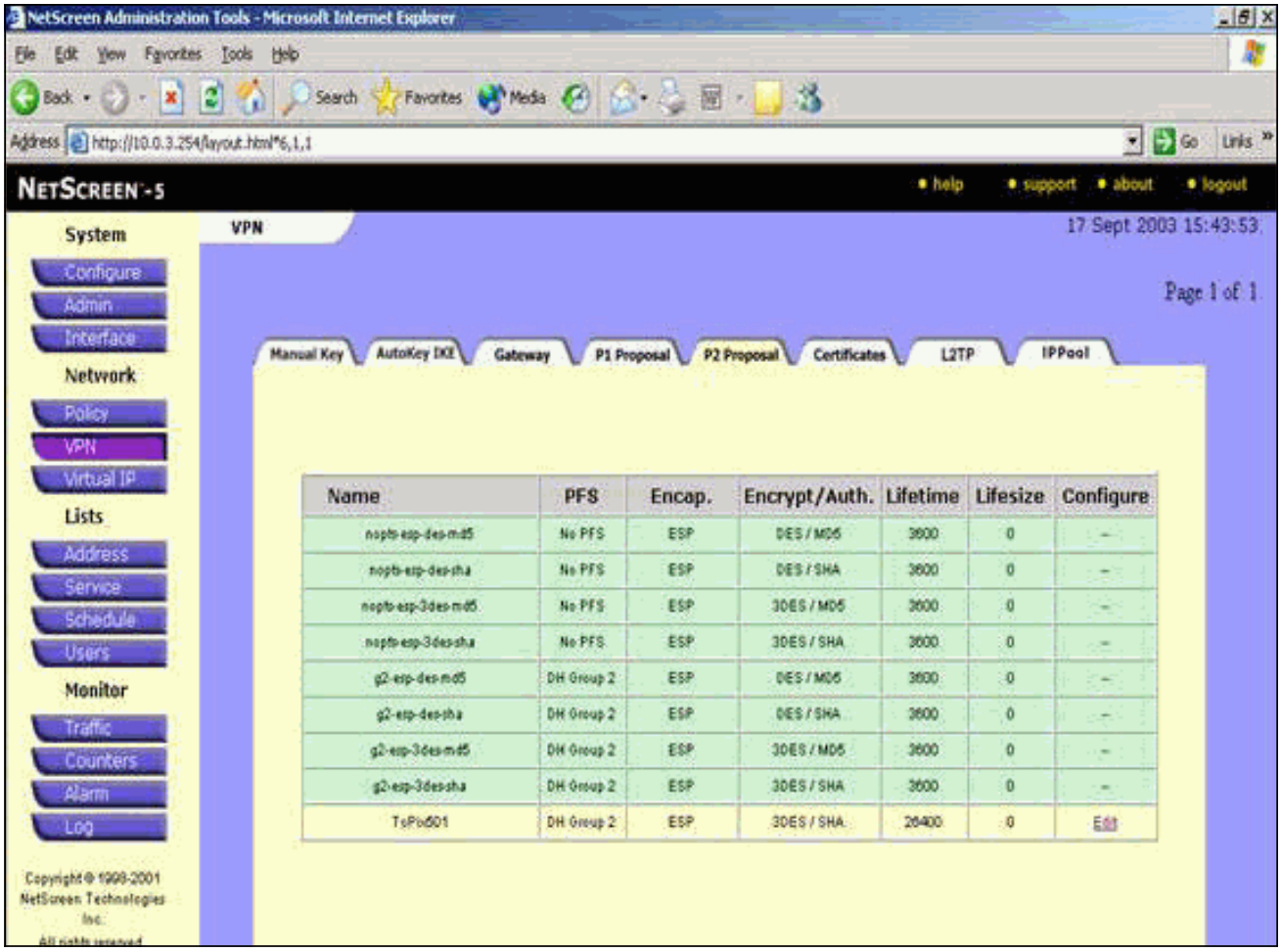
Lorsque la phase 1 est correctement ajoutée à la configuration NetScreen, un écran similaire à cet exemple
apparaît.



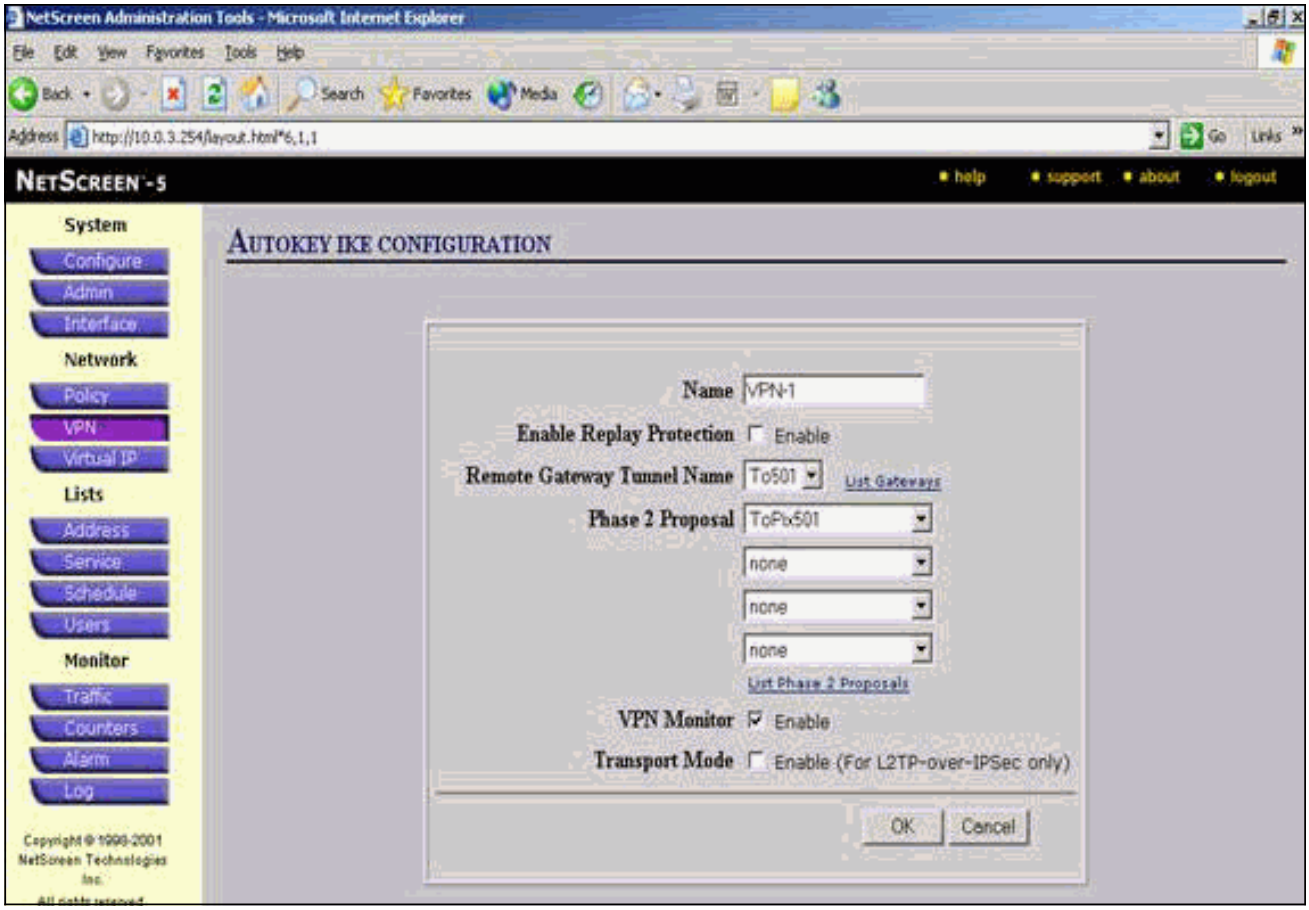
9. Accédez à l'onglet Proposition P2 et cliquez sur **Nouvelle proposition de phase 2** pour configurer la phase 2.
10. Entrez les informations de configuration de la proposition de phase 2 et cliquez sur **OK**.Cet exemple utilise ces champs et ces valeurs pour l'échange de phase 2.**Name :** ToPix501**Secret de transmission parfait :** DH-2 (1 024 bits)**Algorithme de chiffrement :** 3DES-CBC**Algorithme d'authentification :** SHA-1**Durée de vie :** 26400
Sec



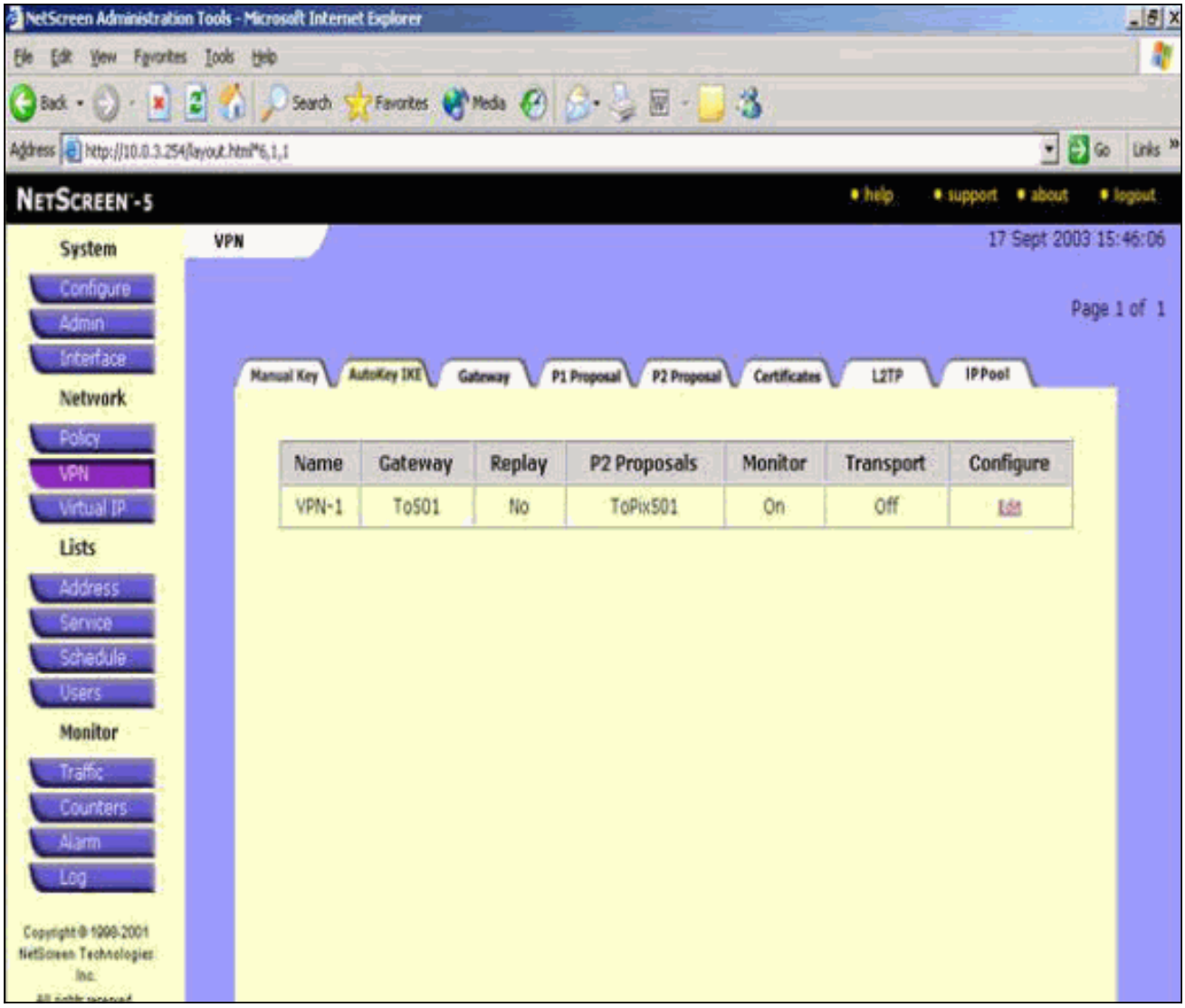
Lorsque la phase 2 est correctement ajoutée à la configuration NetScreen, un écran similaire à cet exemple
apparaît.



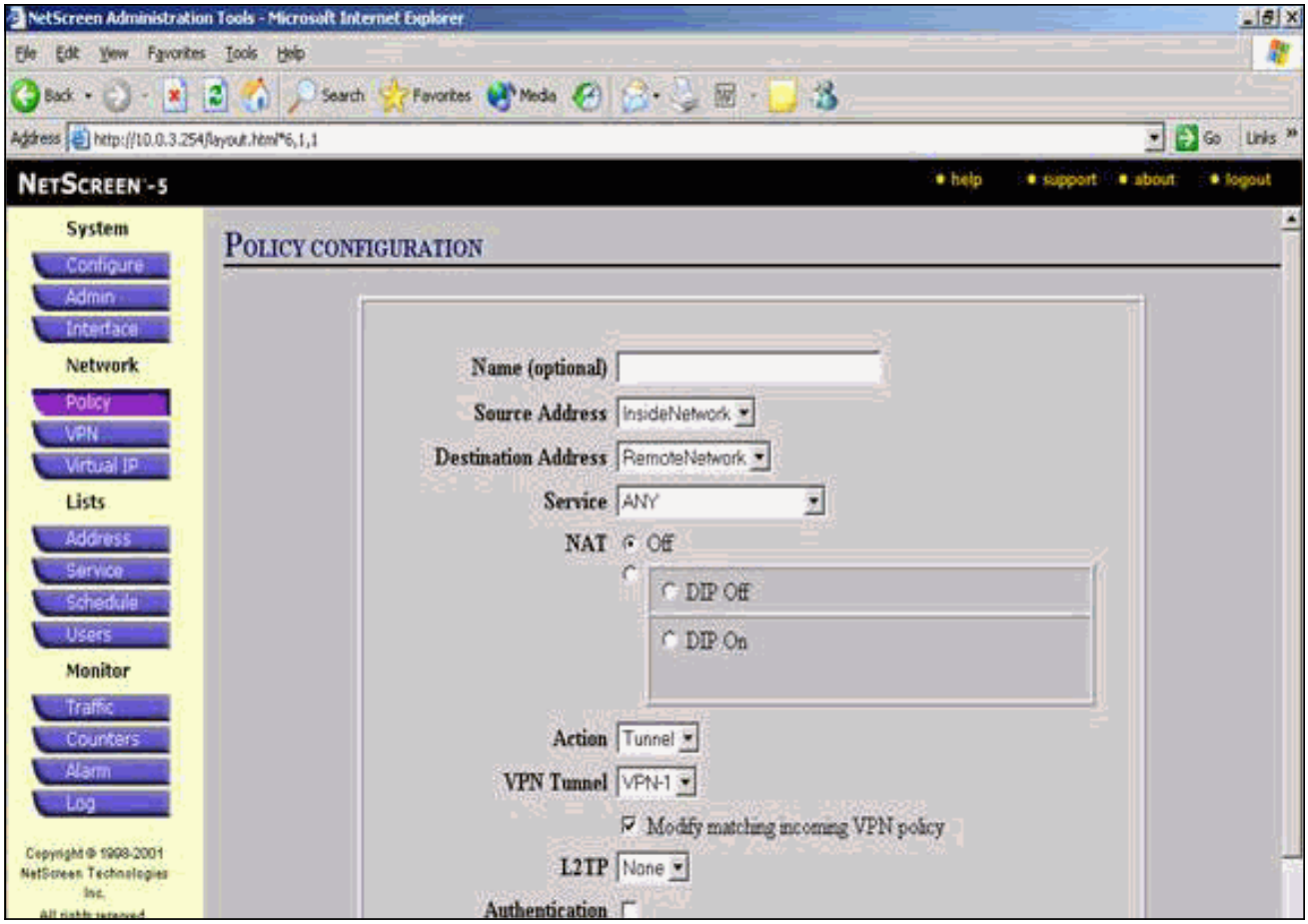
11. Sélectionnez l'onglet **AutoKey IKE**, puis cliquez sur **Nouvelle entrée IKE AutoKey** pour créer et configurer AutoKeys IKE.
12. Entrez les informations de configuration pour AutoKey IKE, puis cliquez sur **OK**.Cet exemple utilise ces champs et ces valeurs pour AutoKey IKE.**Name :** VPN-1**Nom du tunnel de la passerelle distante :** À501(Ceci a déjà été créé dans l'onglet Passerelle.)**Proposition de la phase 2 :** ToPix501(Ceci a déjà été créé dans l'onglet Proposition P2.)**Moniteur VPN :** Activer(Cela permet au périphérique NetScreen de définir des interruptions SNMP (Simple Network Management Protocol) afin de surveiller l'état du moniteur VPN.)



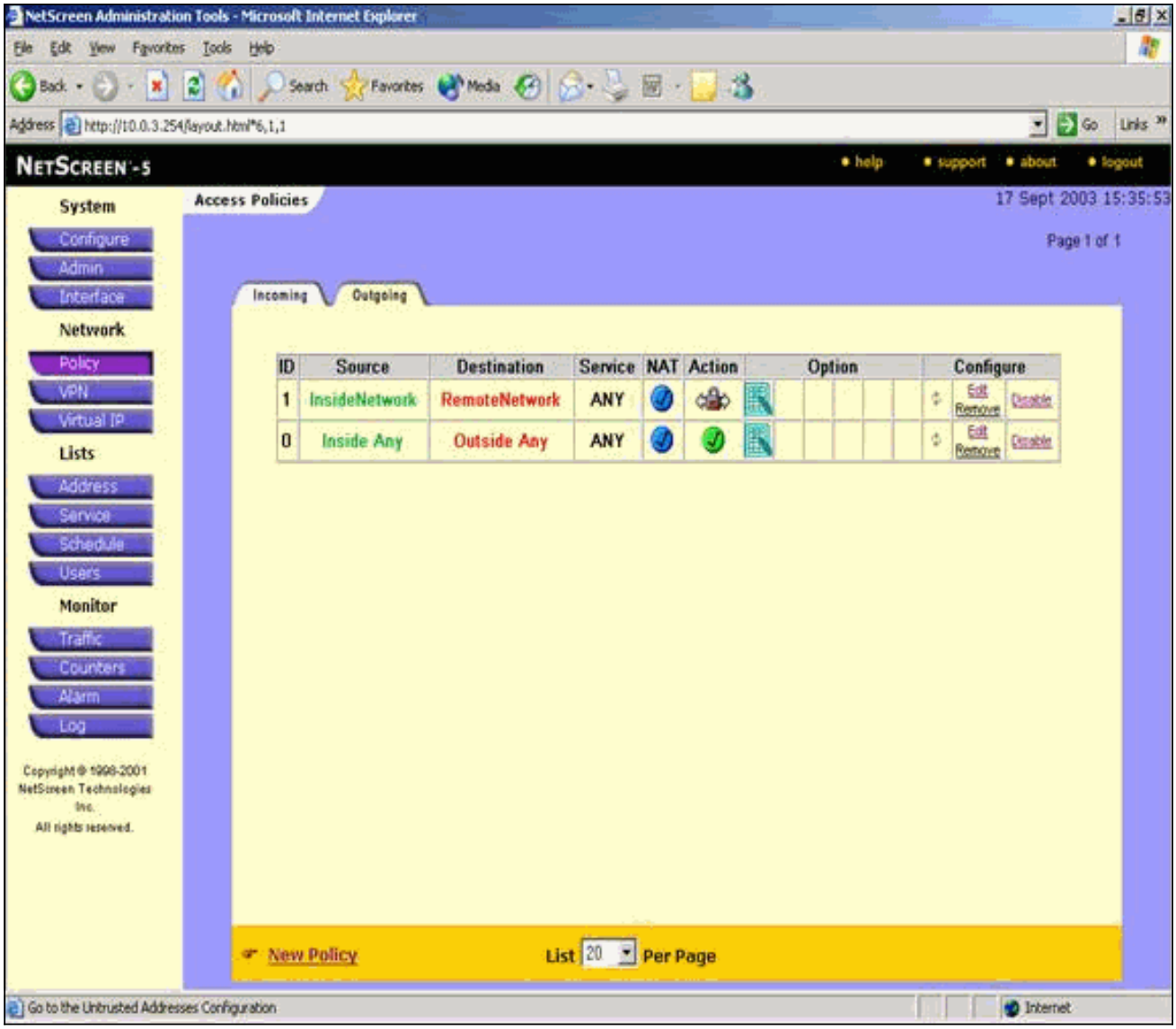
Lorsque la règle VPN-1 est correctement configurée, un écran similaire à cet exemple apparaît.



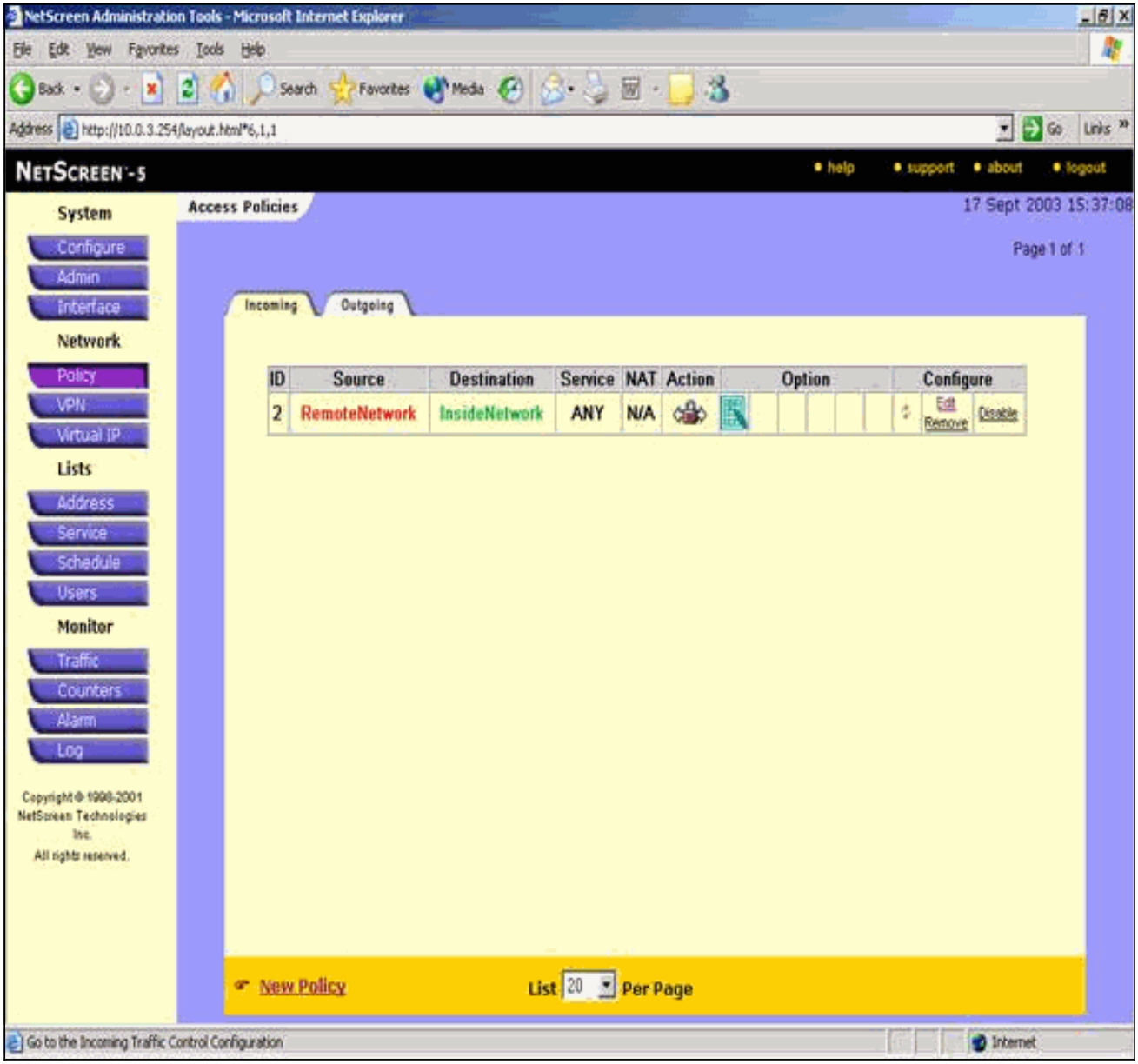
13. Sélectionnez **Network > Policy**, accédez à l'onglet Outgoing, puis cliquez sur **New Policy** pour configurer les règles permettant le chiffrement du trafic IPsec.
14. Entrez les informations de configuration de la stratégie et cliquez sur **OK**.Cet exemple utilise ces champs et ces valeurs pour la stratégie. Le champ Nom est facultatif et n'est pas utilisé dans cet exemple.**Adresse source:** Réseau interne(Ceci a été précédemment défini dans l'onglet Approuvé.)**Adresse de destination:** Réseau distant(Ceci a été précédemment défini sous l'onglet Non approuvé.)**Service :** tous les modèles**Action :** Tunnel**Tunnel VPN :** VPN-1(Il s'agissait précédemment du tunnel VPN de l'onglet AutoKey IKE.)**Modifier la stratégie VPN entrante correspondante :** Coché(Cette option crée automatiquement une règle entrante qui correspond au trafic VPN du réseau externe.)



15. Lorsque la stratégie est ajoutée, assurez-vous que la règle VPN sortante figure en premier dans la liste des stratégies. (La règle créée automatiquement pour le trafic entrant se trouve dans l'onglet Entrant.)Complétez ces étapes si vous devez modifier l'ordre des stratégies :Cliquez sur l'onglet Sortant.Cliquez sur les flèches circulaires dans la colonne Configurer afin d'afficher la fenêtre Déplacer le micro de stratégie.Modifiez l'ordre des stratégies de sorte que la stratégie VPN soit supérieure à l'ID de stratégie 0 (de sorte que la stratégie VPN se trouve en haut de la
liste).



Accédez à l'onglet Entrant afin d'afficher la règle pour le trafic entrant.



Vérification

Cette section fournit des informations que vous pouvez utiliser pour confirmer que votre configuration fonctionne correctement.

Commandes de vérification

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **ping** : diagnostic de la connectivité réseau de base.
- **show crypto ipsec sa - Montre les associations de sécurisation de phase 2.**
- **show crypto isakmp sa - Montre les associations de sécurisation de phase 1.**

Sortie de vérification

Un exemple de sortie des commandes **ping** et **show** est présenté ici.

Cette requête ping est lancée à partir d'un hôte derrière le pare-feu 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
```

La sortie de la commande **show crypto ipsec sa** est affichée ici.

```
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 sortie de la commande **show crypto isakmp sa** est affichée ici.

```
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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug crypto engine** : affiche les messages relatifs aux moteurs de chiffrement.
- **debug crypto ipsec** - Affiche des informations sur les événements IPsec.
- **debug crypto isakmp—Affichage de messages d'événements IKE.**

Exemple de sortie de débogage

Un exemple de sortie **debug** du pare-feu PIX est affiché ici.

```
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
```

Informations connexes

- Négociation IPSec/Protocoles IKE
- Logiciels pare-feu Cisco PIX
- Références des commandes du pare-feu Cisco Secure PIX
- Notices de champs relatives aux produits de sécurité (y compris PIX)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems