Cisco PIX Firewall と NetScreen Firewall 間の IPSec LAN-to-LAN トンネルの設定

内容

概要

このドキュメントでは、最新のソフトウェアを使って、Cisco PIX Firewall と NetScreen Firewall 間で、IPSec LAN-to-LAN トンネルを確立するために必要な手順について説明します。IPSec トンネルを介して別のファイアウォールと通信を行う各デバイスの背後には、プライベート ネットワークが存在します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- NetScreen Firewall に、信頼できるインターフェイスおよび信頼できないインターフェイスの IP アドレスが設定されていること。
- インターネットへの接続が確立されていること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- PIX Firewall ソフトウェア バージョン 6.3(1)
- NetScreen の最新のリビジョン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。

設定

このドキュメントでは、次の構成を使用します。

- PIX ファイアウォール
- NetScreen Firewall

PIX Firewall の設定

PIX ファイアウォール
PIX Version 6.3(1) interface ethernet0 10baset interface ethernet1 100full nameif ethernet0 outside security0 nameif ethernet1 inside security100

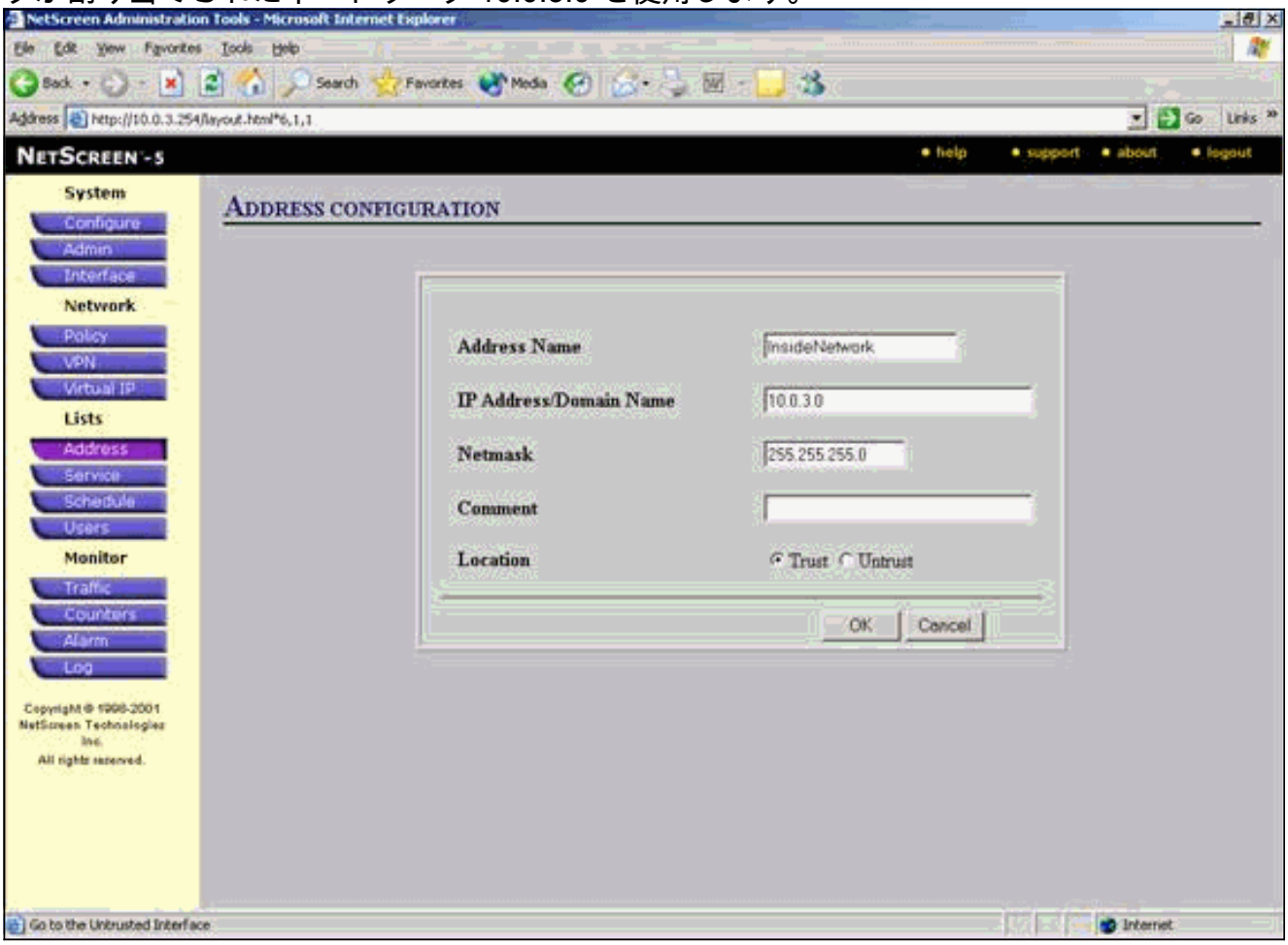
```
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554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

NetScreen Firewall の設定

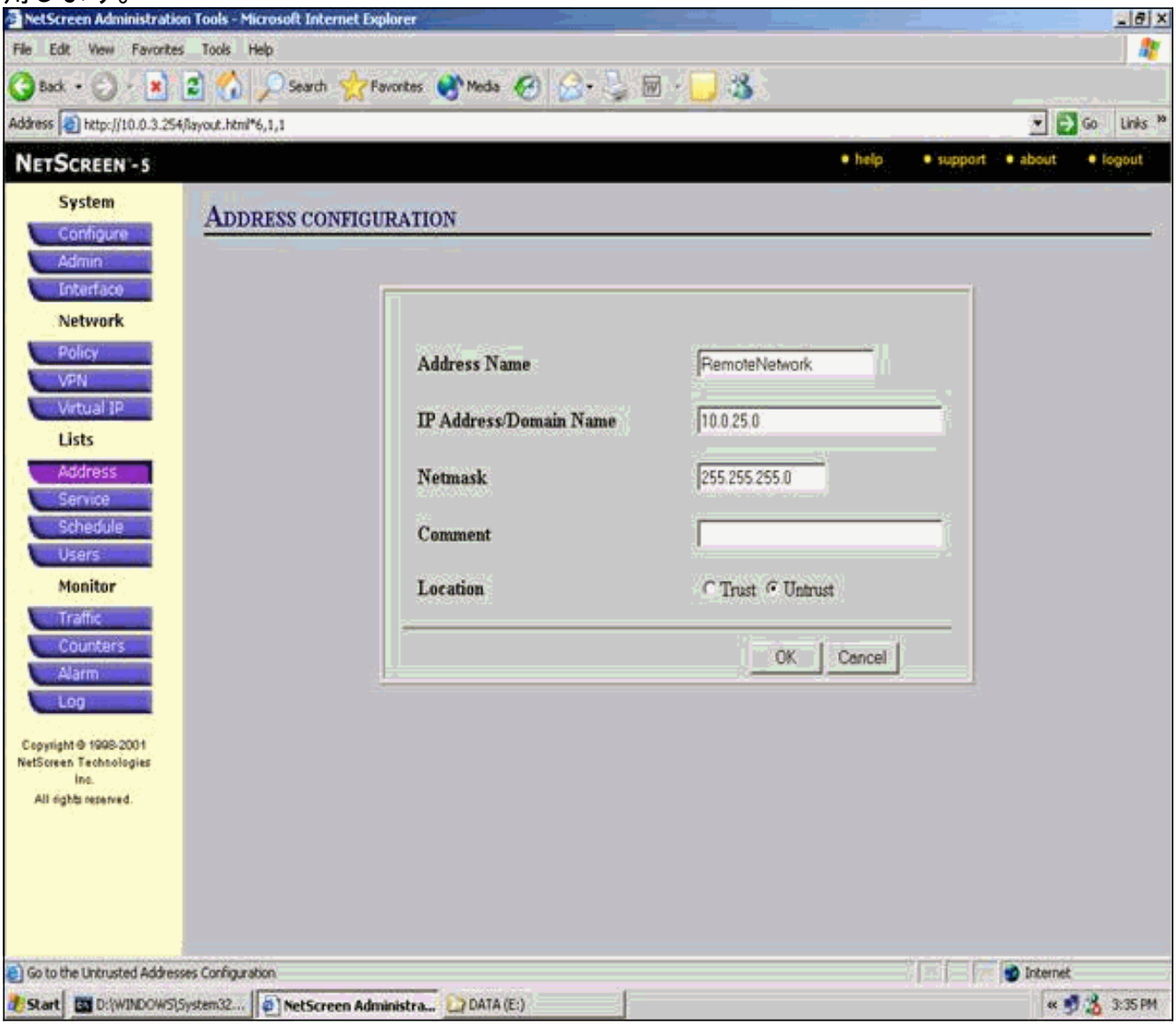
NetScreen Firewall を設定するには、次のステップを実行します。

1. **Lists > Address** の順に選択し、Trusted タブに移動し、**New Address** をクリックします。
2. トンネルで暗号化される NetScreen 内部ネットワークを追加し、**OK** をクリックします。**注：[信頼]**オプションが選択されていることを確認します。次の例では、255.255.255.0 のマスクが割り当てられたネットワーク 10.0.3.0 を使用します。

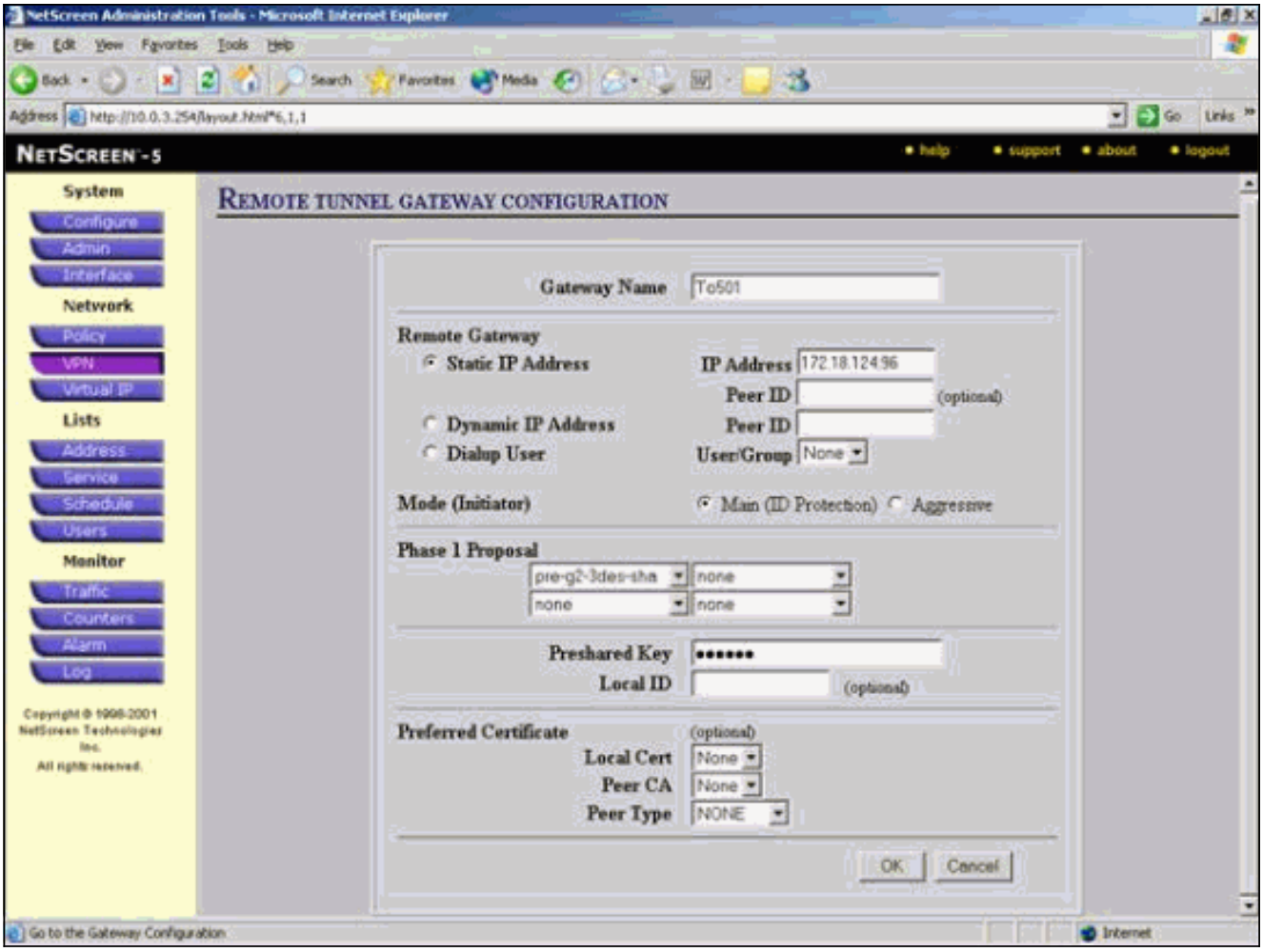


3. **Lists > Address** の順に選択し、Untrusted タブに移動し、**New Address** をクリックします。

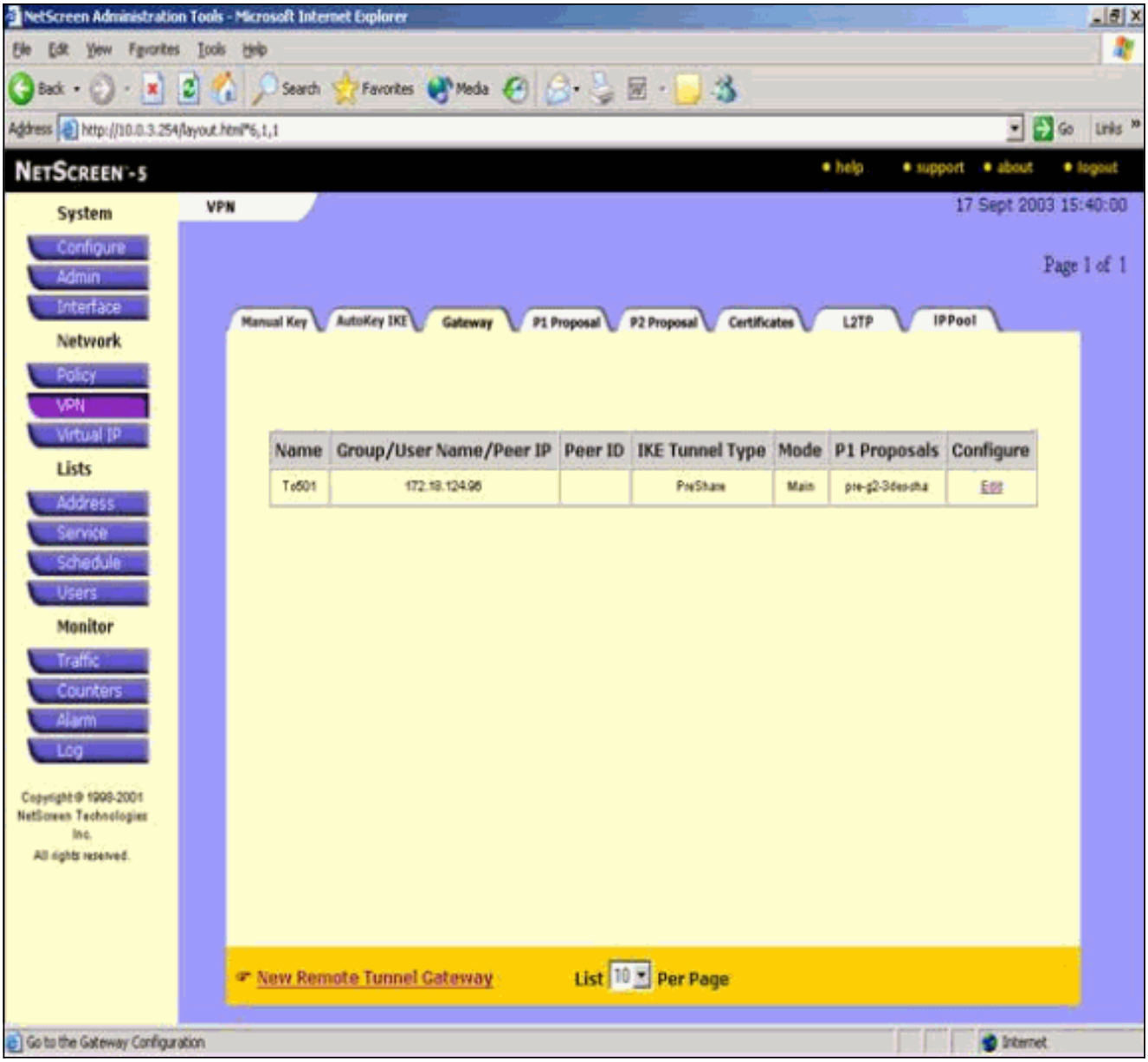
4. パケットを暗号化するときに NetScreen Firewall が使用するリモート ネットワークを追加し、**OK** をクリックします。**注：**NetScreen以外のゲートウェイにVPNを設定する場合は、アドレスグループを使用しないでください。アドレス グループを使用すると、VPN の相互運用性が損なわれます。NetScreen 以外のセキュリティ ゲートウェイは、アドレス グループが使用されていると、NetScreen によって作成されたプロキシ ID を解釈できません。この問題には、2 つの回避策があります。アドレス グループを、個別のアドレス帳エントリに分割する。アドレス帳エントリごとに、個別のポリシーを指定する。可能な場合は、非 NetScreen ゲートウェイ（ファイアウォール デバイス）でプロキシ ID を 0.0.0.0/0 に設定する。次の例では、255.255.255.0 のマスクが割り当てられたネットワーク 10.0.25.0 を使用します。



5. VPN ゲートウェイ（Phase 1 と Phase 2 の IPSec ポリシー）を設定するには、**Network > VPN** の順に選択し、Gateway タブに移動して、**New Remote Tunnel Gateway** をクリックします。
6. PIX の外部インターフェイスの IP アドレスを使ってトンネルを終端し、Phase 1 IKE オプションをバインドするように設定します。完了したら、[OK] をクリックします。この例では、次のフィールドと値を使用します。**Gateway Name（ゲートウェイ名）**：~ 501**Static IP Address（スタティック IP アドレス）**:172.18.124.96**Mode（モード）**： Main (ID Protection)（メイン（ID 保護））**Preshared Key（事前共有鍵）**： "testme"**Phase 1 proposal（Phase 1 プロポーザル）**：pre-g2-3des-sha

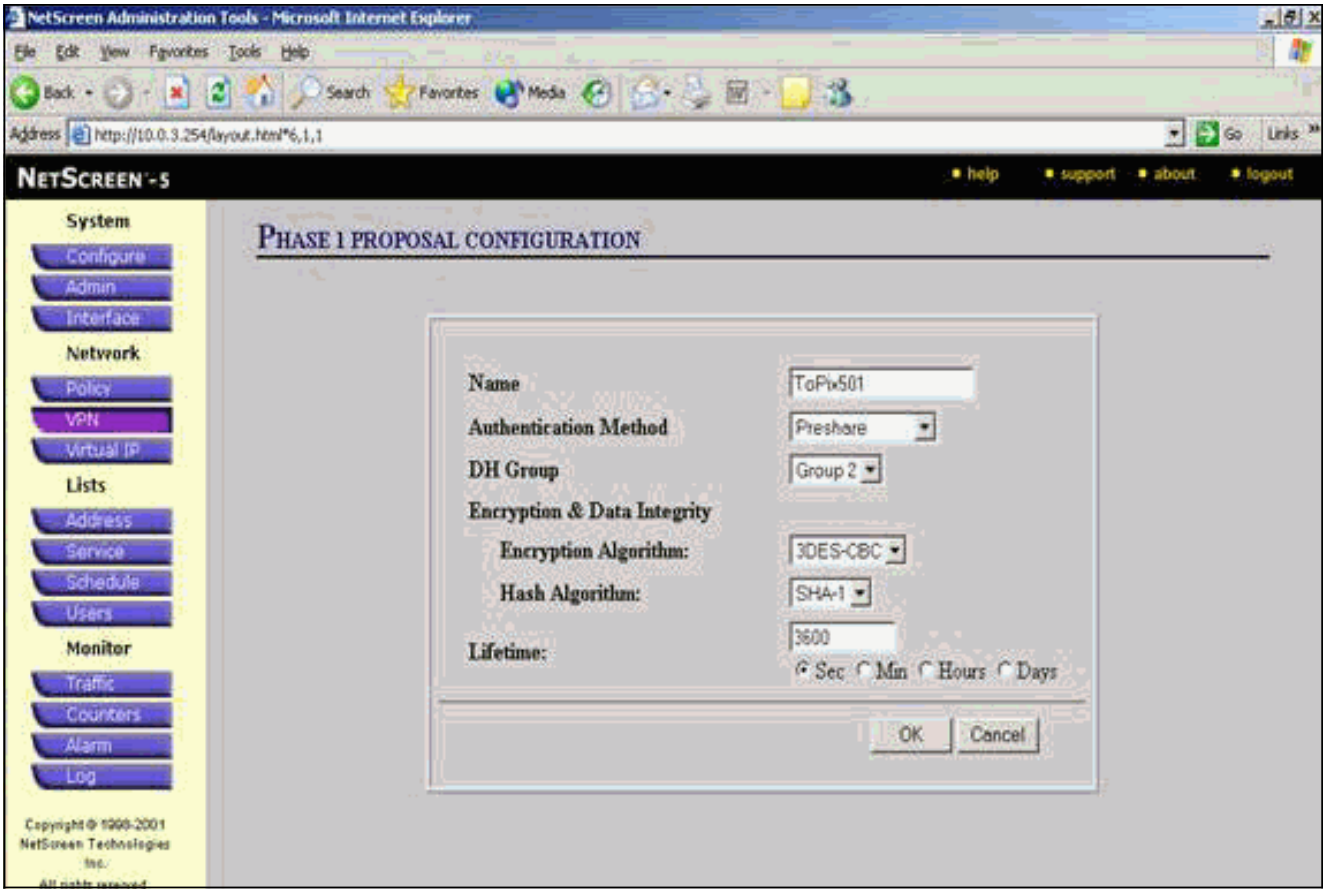


リモート ゲートウェイ トンネルを作成すると、次のような画面が表示されます。

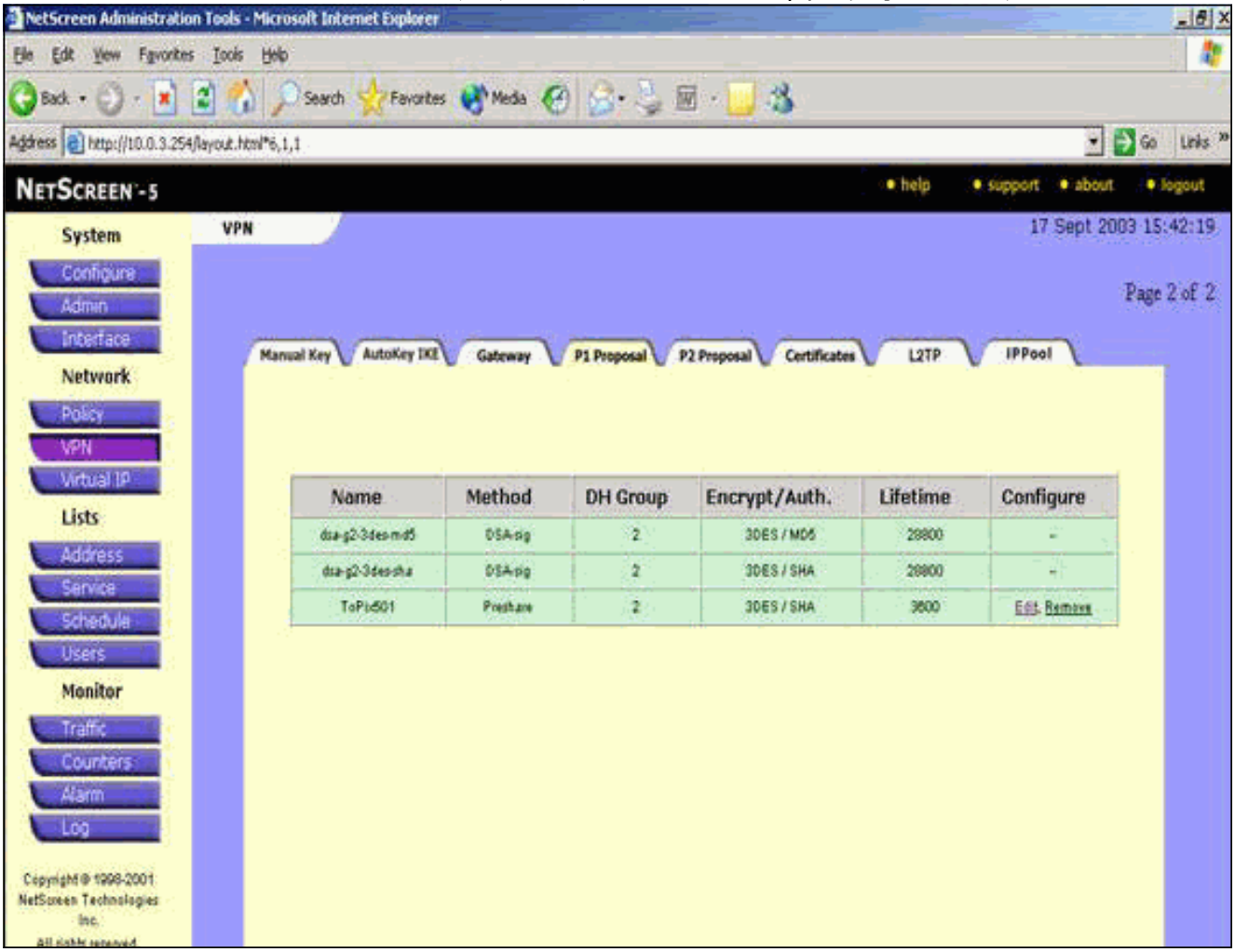


7. Proposal 1 を設定するには、P1 Proposal タブに移動し、**New Phase 1 Proposal** をクリックします。
8. Phase 1 Proposal の設定情報を入力し、**OK** をクリックします。この例では、Phase 1 交換用に次のフィールドと値を使用します。**[Name]**：ToPix501**認証**： Preshare**DH グループ**：group 2**暗号化**：3DES-CBC**Hash（ハッシュ）**：SHA-1**Lifetime（ライフタイム）**：3600秒

.

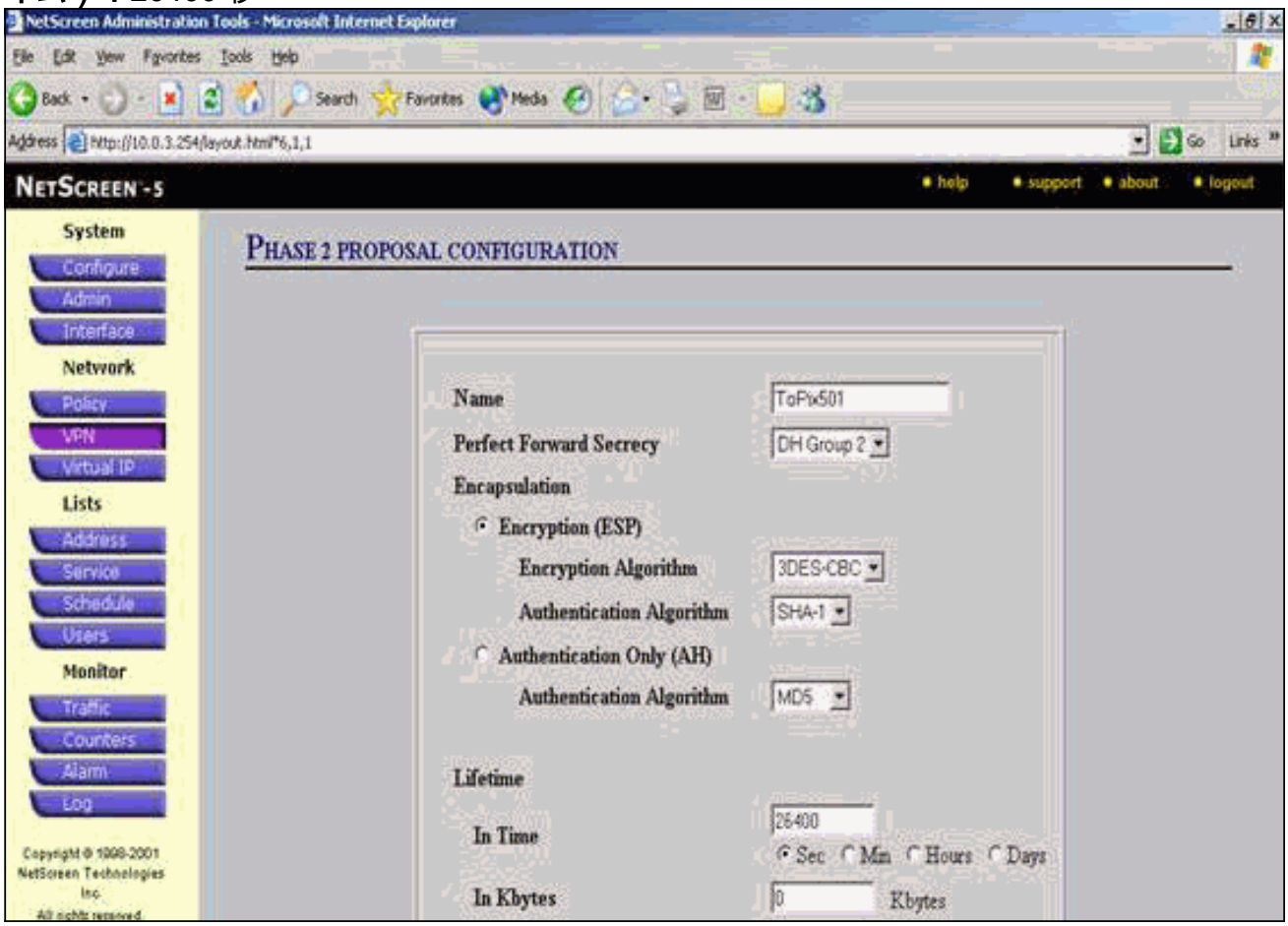


NetScreen の設定に Phase 1 を追加すると、次のような画面が表示されます。

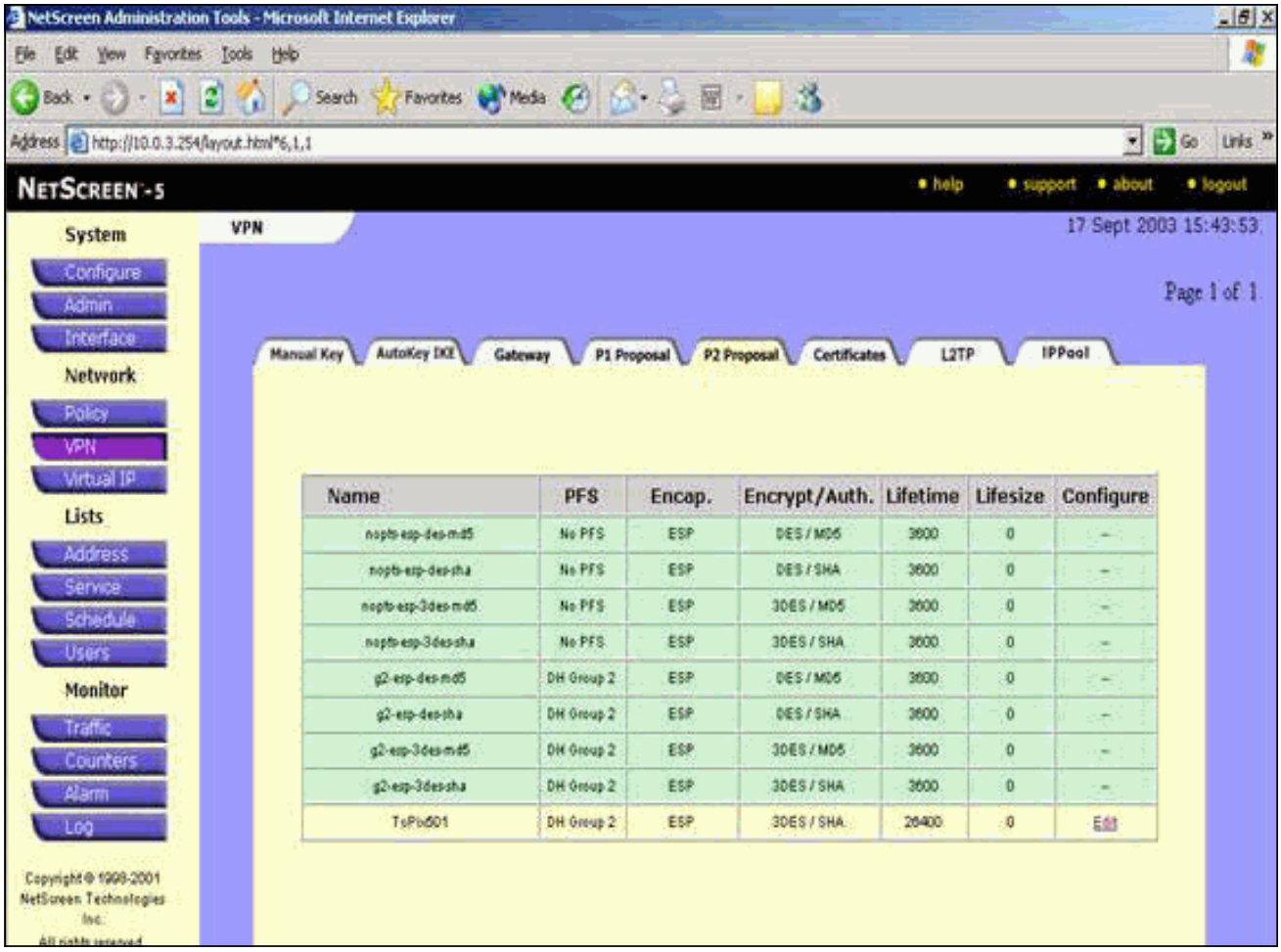


9. Proposal 2 を設定するには、P2 Proposal タブに移動し、**New Phase 2 Proposal** をクリックします。

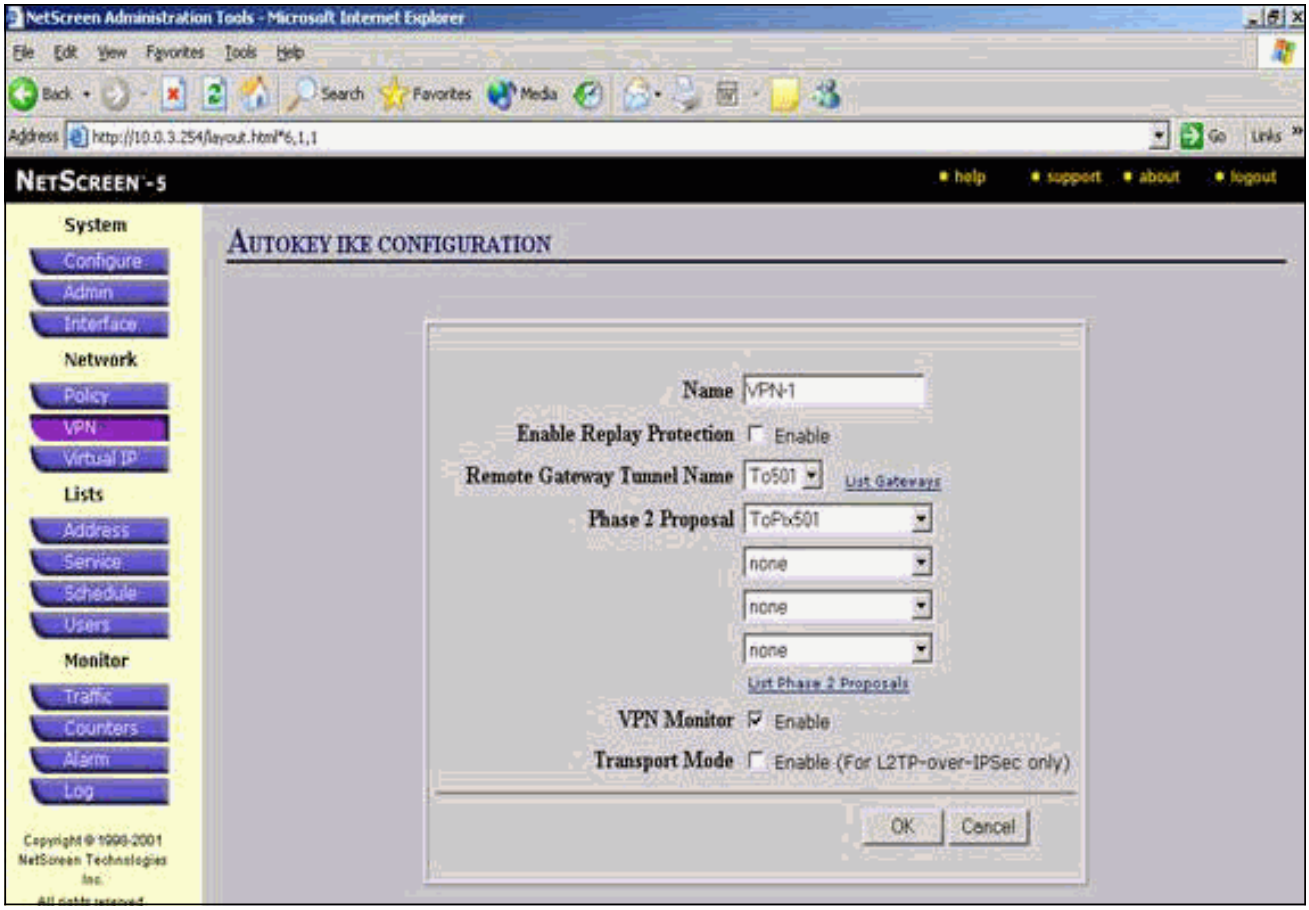
10. Phase 2 Proposal の設定情報を入力し、**OK** をクリックします。この例では、Phase 2 交換用に次のフィールドと値を使用します。**[Name]**：ToPix501**Perfect Forward Secrecy（完全転送秘密）**： DH-2（1024 ビット）**Encryption Algorithm（暗号化アルゴリズム）**：3DES-CBC**Authentication Algorithm（認証アルゴリズム）**：SHA-1**Lifetime（ライフタイム）**：26400 秒



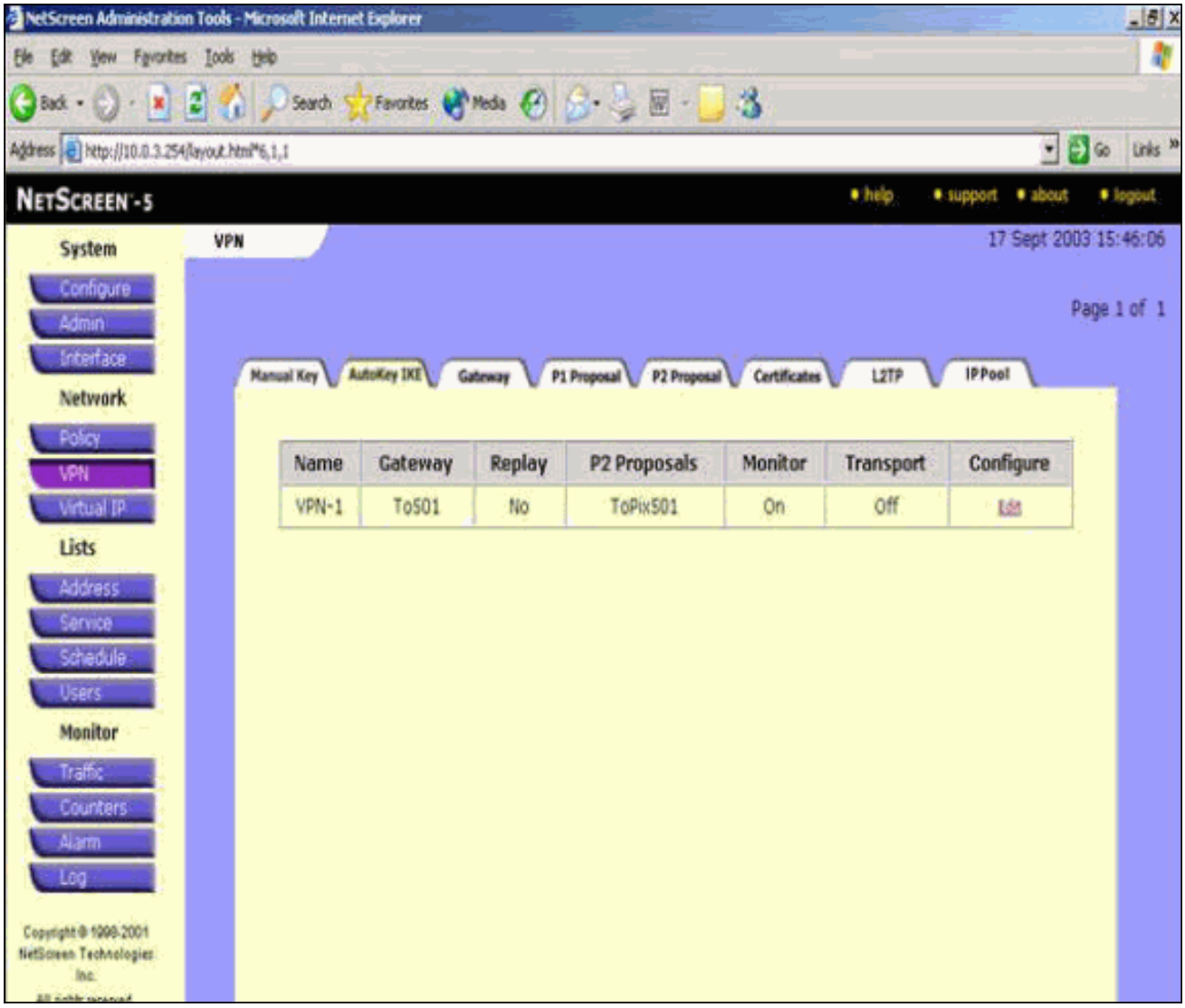
NetScreen の設定に Phase 2 を追加すると、次のような画面が表示されます。



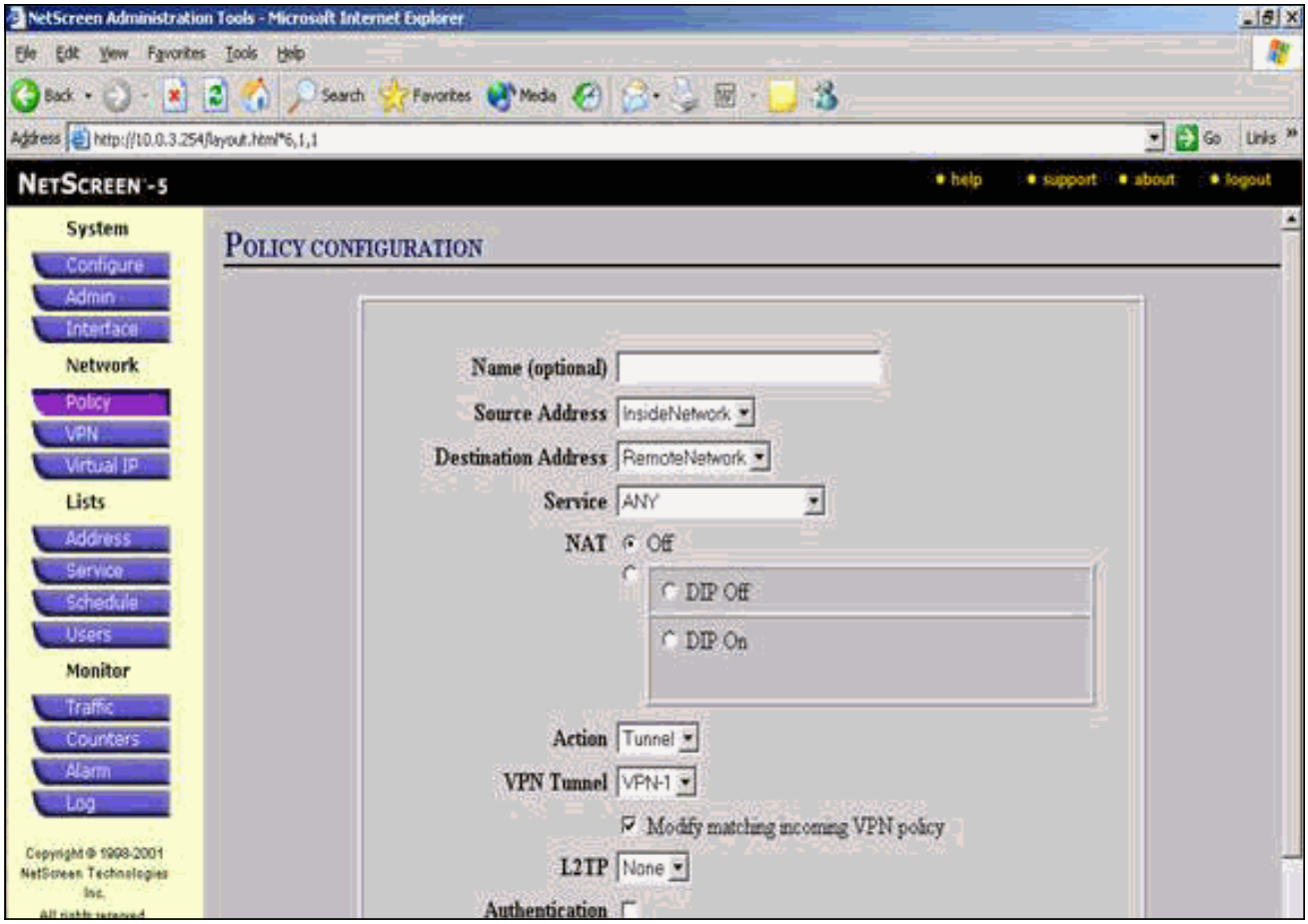
11. AutoKeys IKE の作成と設定を行うには、**AutoKey IKE** タブを選択し、**New AutoKey IKE Entry** をクリックします。
12. AutoKey IKE の設定情報を入力し、**OK** をクリックします。この例では、AutoKey IKE 用に次のフィールドと値を使用します。**[Name]**：VPN-1**Remote Gateway Tunnel Name（リモート ゲートウェイ トンネル名）**：~ 501（Gateway タブですでに作成されています。）**Phase 2 proposal（Phase 2 プロポーザル）**：ToPix501（P2 Proposal タブですでに作成されています。）**VPN Monitor（VPN モニタ）**：Enable（これにより、NetScreen デバイスで Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）トラップが設定され、VPN モニタの状態を監視できます。）



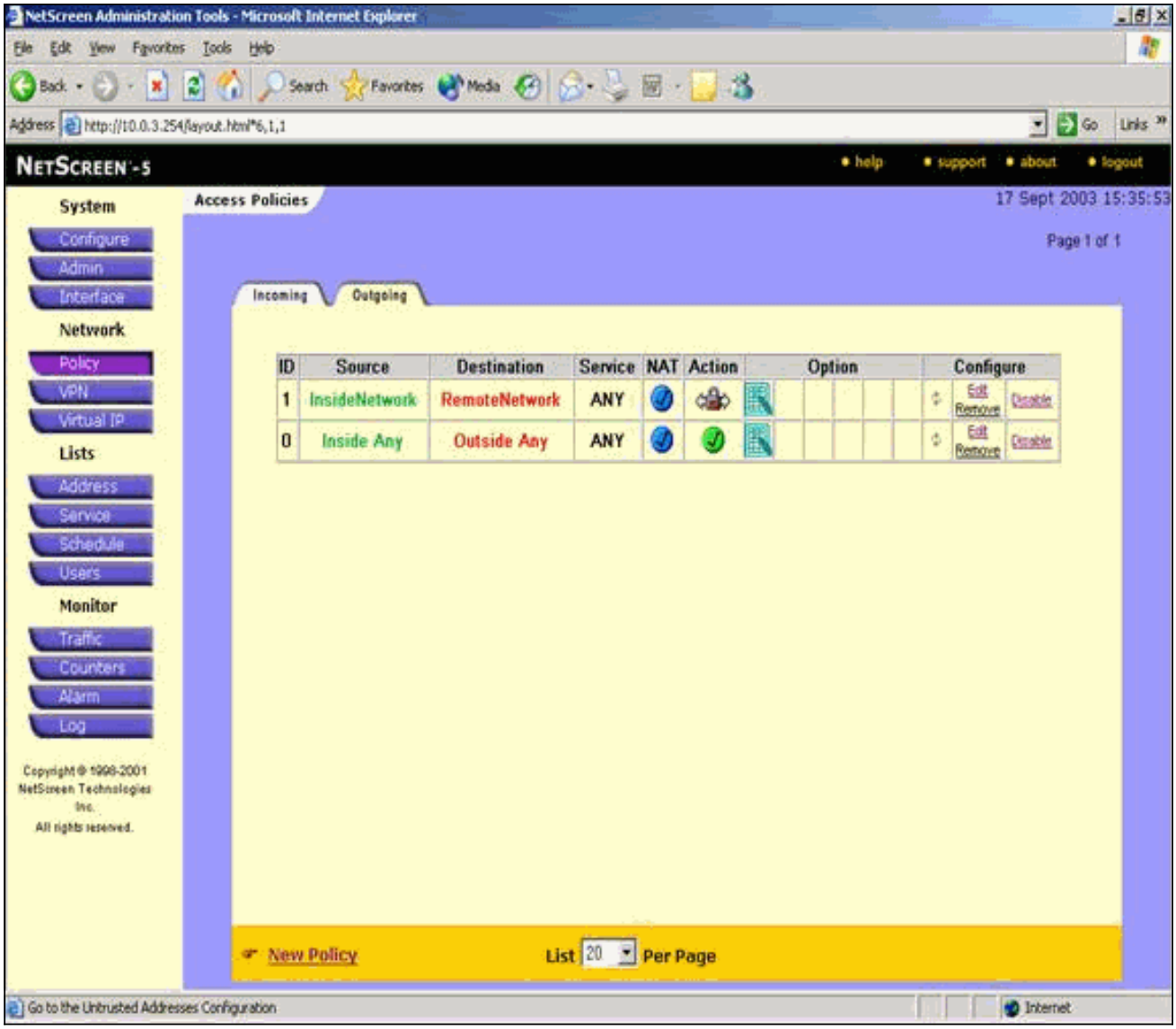
VPN-1 ルールを設定すると、次のような画面が表示されます。



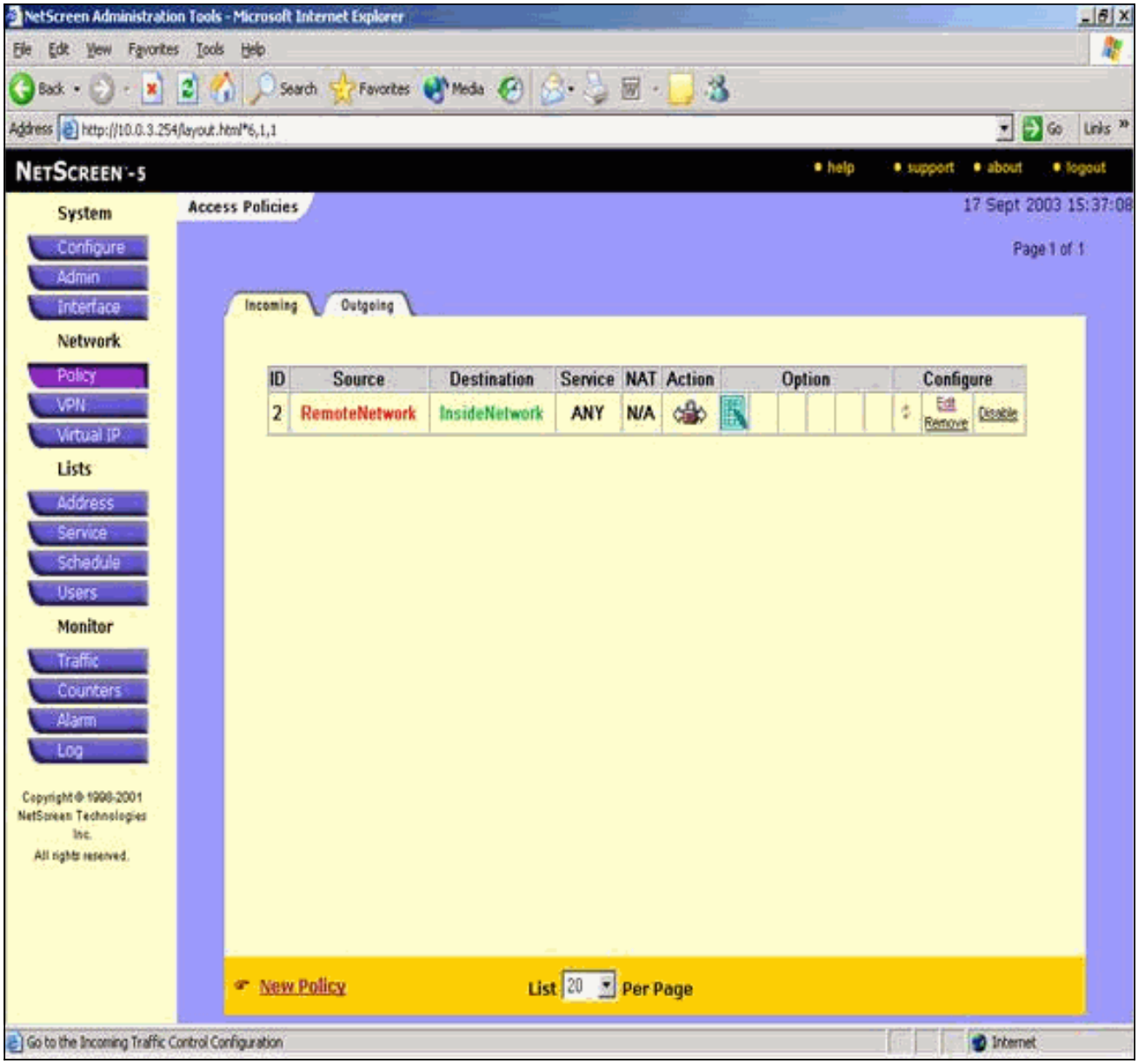
13. IPSec トラフィックの暗号化を許可するルールを設定するには、**Network > Policy** の順に選択し、Outgoing タブに移動して、**New Policy** をクリックします。
14. ポリシーの設定情報を入力し、**OK** をクリックします。この例では、ポリシー用に次のフィールドと値を使用します。Name フィールドはオプションで、この例では使用しません。**発信元アドレス：** InsideNetwork（Trusted タブですでに定義されています。）**宛先アドレス:** RemoteNetwork（Untrusted タブですでに定義されています。）**Service（サービス）：**[Any]**Action:** Tunnel（トンネル）**VPN Tunnel（VPN トンネル）：**VPN-1（AutoKey IKE タブですでに定義されています。）**Modify matching incoming VPN policy（一致する着信 VPN ポリシーの修正）：**チェックボックスをオンにします。（このオプションを有効にすると、外部ネットワークの VPN トラフィックに一致する着信ルールが自動作成されます。
）



15. ポリシーを追加したら、発信 VPN ルールが、ポリシー リストの最初にあることを確認します（着信トラフィック用に自動作成されたルールは、Incoming タブで確認できます）。ポリシーの順番を変更する場合は、次の手順に従ってください。Outgoing タブをクリックします。Move Policy Micro ウィンドウを表示するため、Configure カラムの環状の矢印をクリックします。VPN ポリシーが ポリシー ID 0 の上に来るように（VPN ポリシーがリストの一番上に来るように）、ポリシーの順番を変更します。



着信トラフィックのルールを確認するには、Incoming タブに移動します。



確認

この項では、設定が正しく動作していることを確認するために使用できる情報を説明します。

確認コマンド

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- ping - 基本ネットワークの接続を診断します。
- show crypto ipsec sa：フェーズ 2 のセキュリティ アソシエーションを表示します。
- show crypto isakmp sa：フェーズ 1 のセキュリティ アソシエーションを表示します。

確認出力

ping と show コマンドの出力例を次に示します。

この ping は、NetScreen Firewall の背後のホストから発行されました。

```
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
```

show crypto ipsec sa コマンドの出力を次に示します。

```
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:
```

show crypto isakmp sa コマンドの出力を次に示します。

```
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
```

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

注：debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- **debug crypto engine** - crypto エンジンに関する情報を表示します。
- **debug crypto ipsec** - IPsec イベントに関する情報を表示します。
- **debug crypto isakmp**：IKE イベントに関するメッセージを表示します。

debug 出力例

PIX Firewall からの **debug** の出力例を次に示します。

```
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
```

関連情報

- IPSec ネゴシエーション/IKE プロトコル
- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice (PIX を含む)
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems