配置Cisco Pix防火牆和NetScreen防火牆之間的IPSec LAN到LAN隧道

目錄

簡介

本文檔介紹使用最新軟體在Cisco PIX防火牆和NetScreen防火牆之間建立IPsec LAN到LAN隧道的必要過程。每個裝置後都有一個專用網路，通過IPsec隧道與其他防火牆通訊。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- NetScreen防火牆使用信任/不信任介面上的IP地址進行配置。
- 已建立與Internet的連線。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX防火牆軟體版本6.3(1)
- NetScreen最新修訂版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

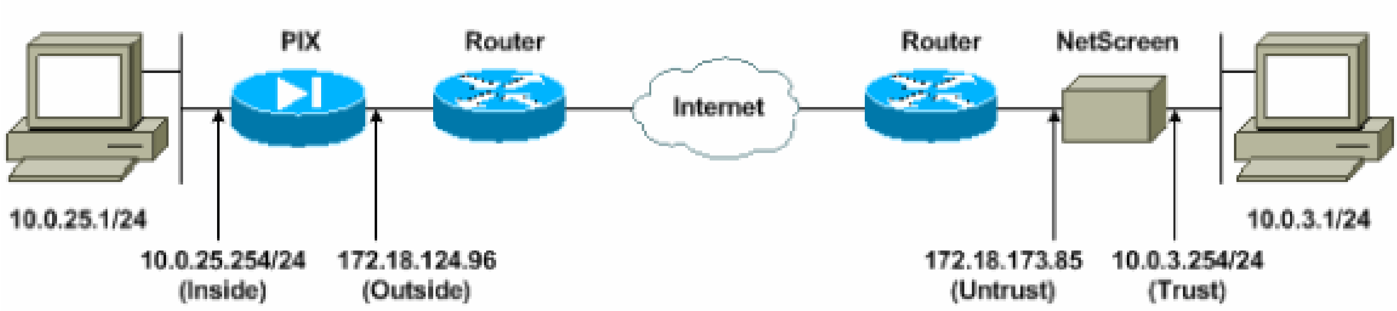
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用以下設定：

- PIX防火牆
- NetScreen防火牆

配置PIX防火牆

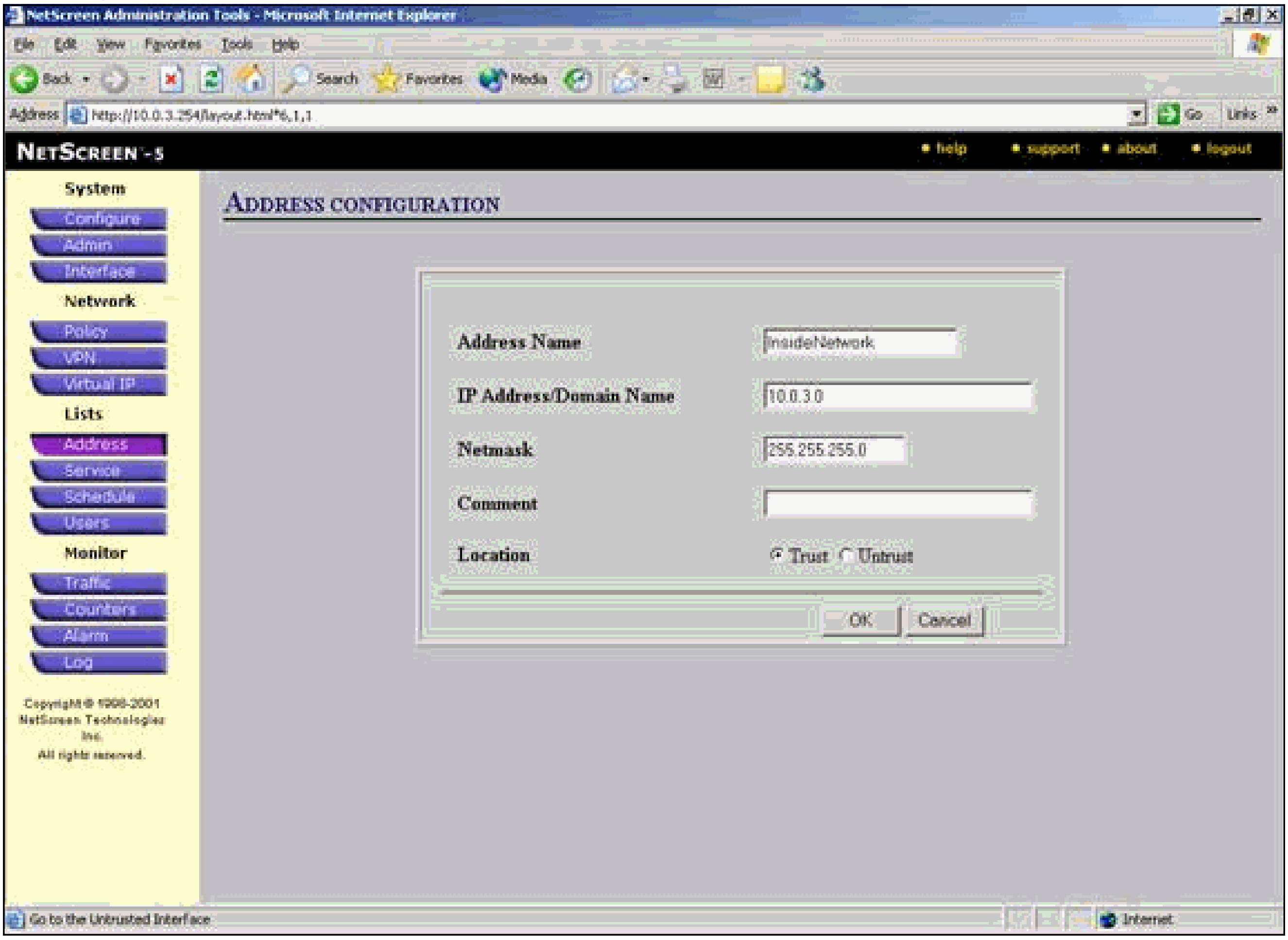
PIX防火牆

```
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
```

配置NetScreen防火牆

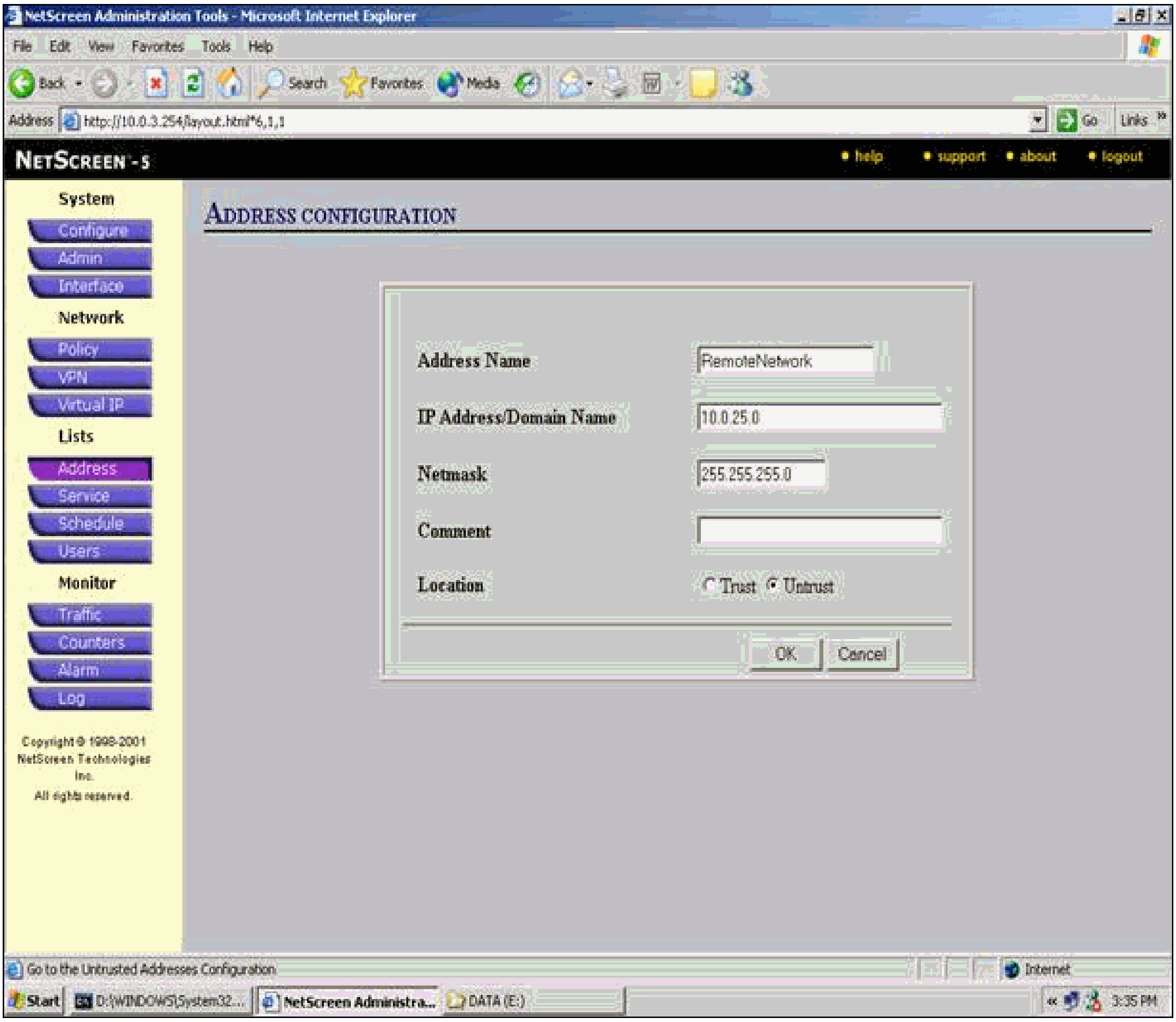
完成以下步驟以配置NetScreen防火牆。

1. 選擇**Lists > Address**，轉到Trusted頁籤，然後按一下**New Address**。
2. 新增在隧道上加密的NetScreen內部網路，然後按一下**OK**。**注意：**確保選擇了「信任」選項。此範例使用遮罩為255.255.255.0的網路10.0.3.0。


NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.3.254/layout.html*6,1,1
Go Links
NETSCREEN-5
help support about logout
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.
ADDRESS CONFIGURATION
Go to the Untrusted Interface
Internet

Address Name: InsideNetwork
IP Address/Domain Name: 10.0.3.0
Netmask: 255.255.255.0
Comment:
Location: ● Trust ○ Untrust
OK Cancel

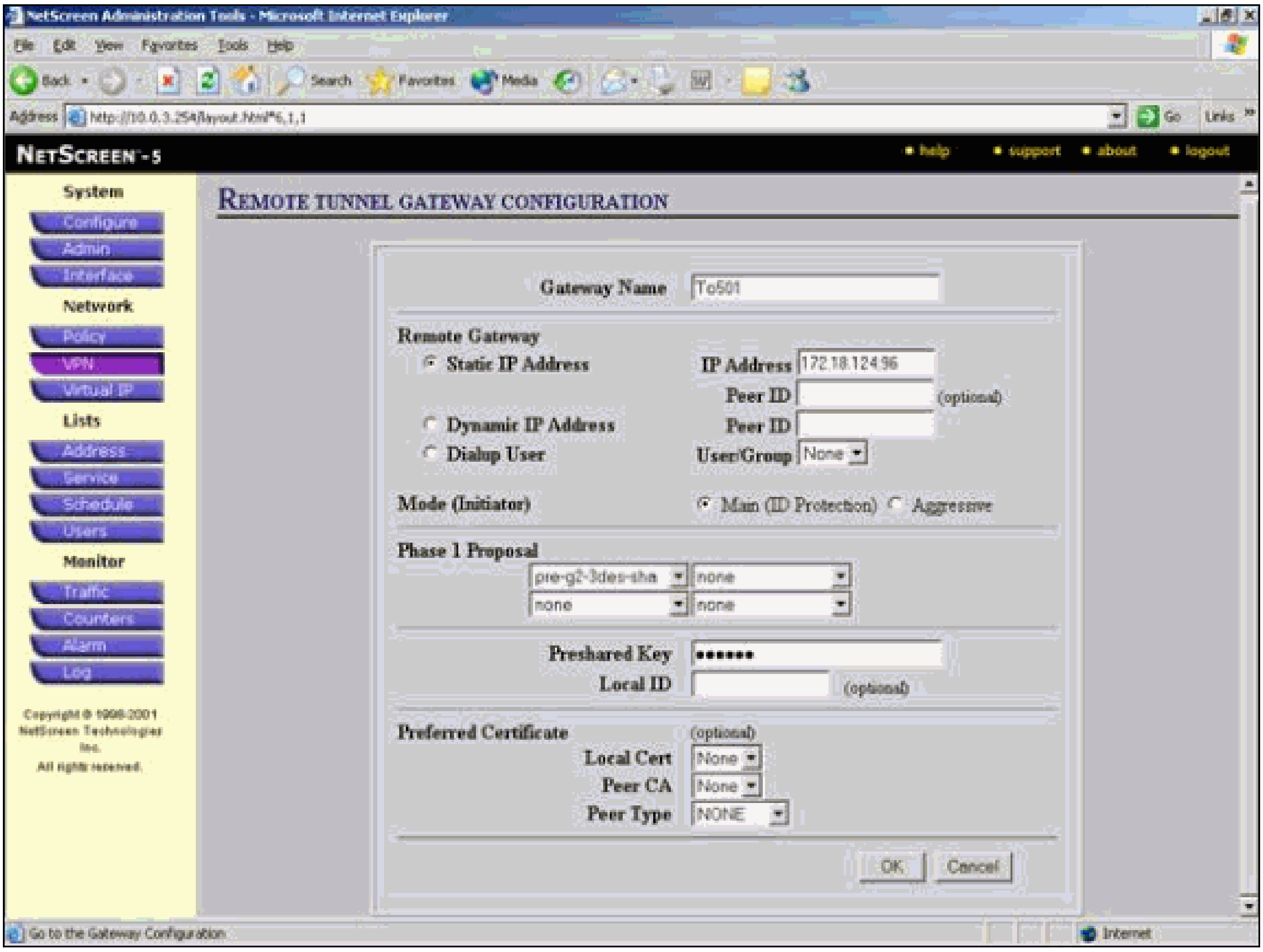
3. 選擇**Lists > Address**，轉到Untrusted頁籤，然後按一下**New Address**。
4. 新增NetScreen防火牆在加密資料包時使用的遠端網路，然後按一下**OK**。**注意：**將VPN配置為非NetScreen網關時，請勿使用地址組。如果您使用地址組，則VPN互操作性將失敗。使用地址組時，非NetScreen安全網關不知道如何解釋NetScreen建立的代理ID。對此有幾種變通辦法：將地址組劃分為各個通訊簿條目。基於每個通訊簿條目指定單個策略。如果可能，在非NetScreen網關（防火牆裝置）上將代理ID配置為0.0.0.0/0。此範例使用網路10.0.25.0（遮罩為255.255.255.0）。


NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.3.254/layout.html*6,1,1
Go Links
NETSCREEN-5
help support about logout
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.
Go to the Untrusted Addresses Configuration
Internet
Start
D:\WINDOWS\System32...
NetScreen Administra...
DATA (E:)
3:35 PM
OK
Cancel

ADDRESS CONFIGURATION

Address Name	RemoteNetwork
IP Address/Domain Name	10.0.25.0
Netmask	255.255.255.0
Comment	
Location	○ Trust ● Untrust

5. 選擇**Network > VPN**，轉到Gateway頁籤，然後按一下**New Remote Tunnel Gateway**以配置VPN網關（第1階段和第2階段IPsec策略）。
6. 使用PIX外部介面的IP地址終止隧道，並配置要繫結的第1階段IKE選項。完成後按一下**OK**。此示例使用這些欄位和值。**網關名稱**：To501**靜態IP地址**：172.18.124.96**模式**：主要（ID保護）**預共用金鑰**："測試"**第1階段建議**：pre-g2-3des-sha


NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.3.254/layout.html*6,1,1
Go Links
NetScreen-5
help support about logout
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright © 1998-2001 NetScreen Technologies Inc.
All rights reserved.
Go to the Gateway Configuration
Internet

REMOTE TUNNEL GATEWAY CONFIGURATION

Gateway Name: To501

Remote Gateway

● Static IP Address — IP Address: 172.18.124.96

Peer ID: (optional)

○ Dynamic IP Address — Peer ID:

○ Dialup User — User/Group: None

Mode (Initiator): ● Main (ID Protection) ○ Aggressive

Phase 1 Proposal: pre-g2-3des-sha, none, none, none

Preshared Key: •••••••

Local ID: (optional)

Preferred Certificate (optional)

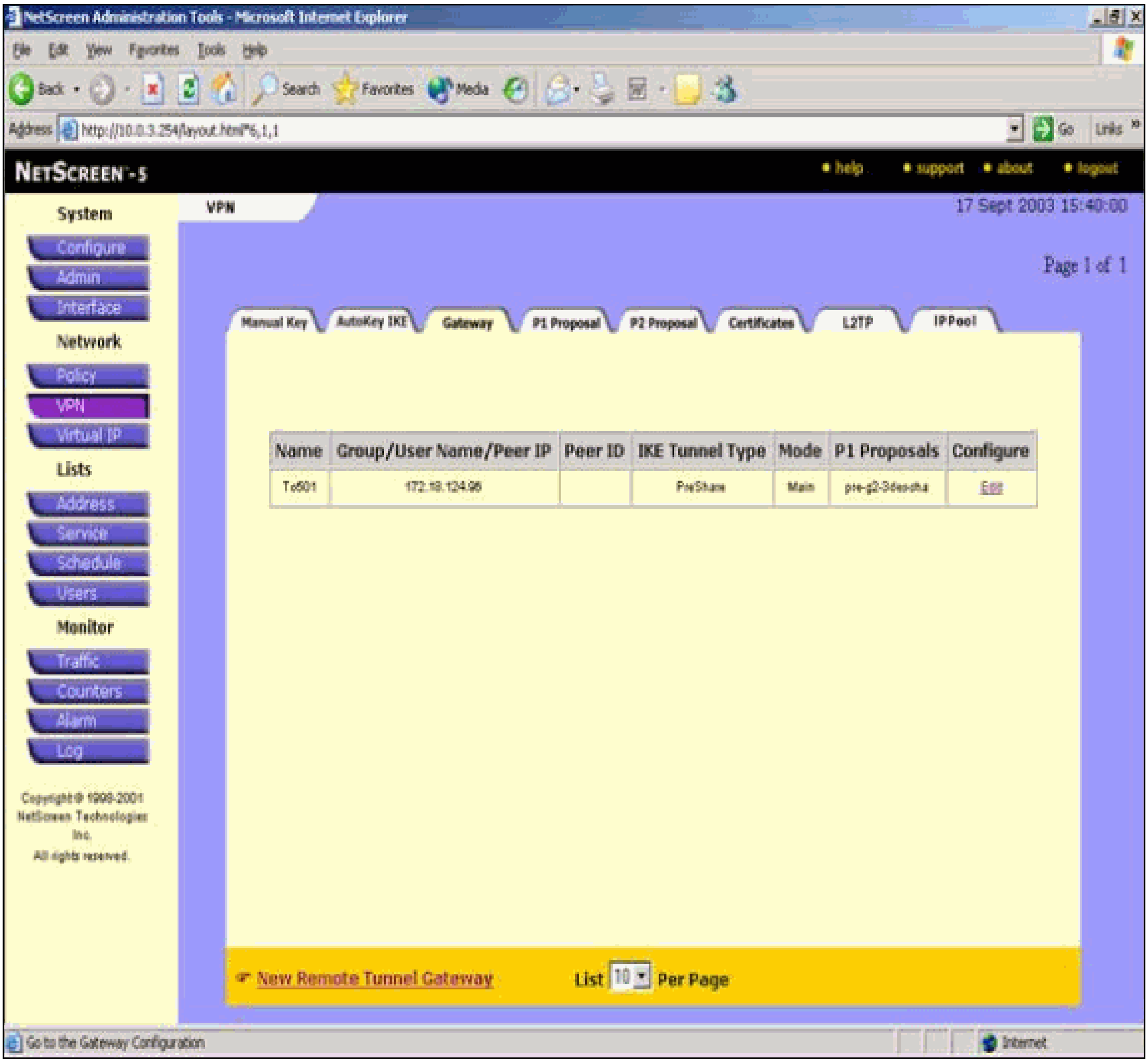
Local Cert: None

Peer CA: None

Peer Type: NONE

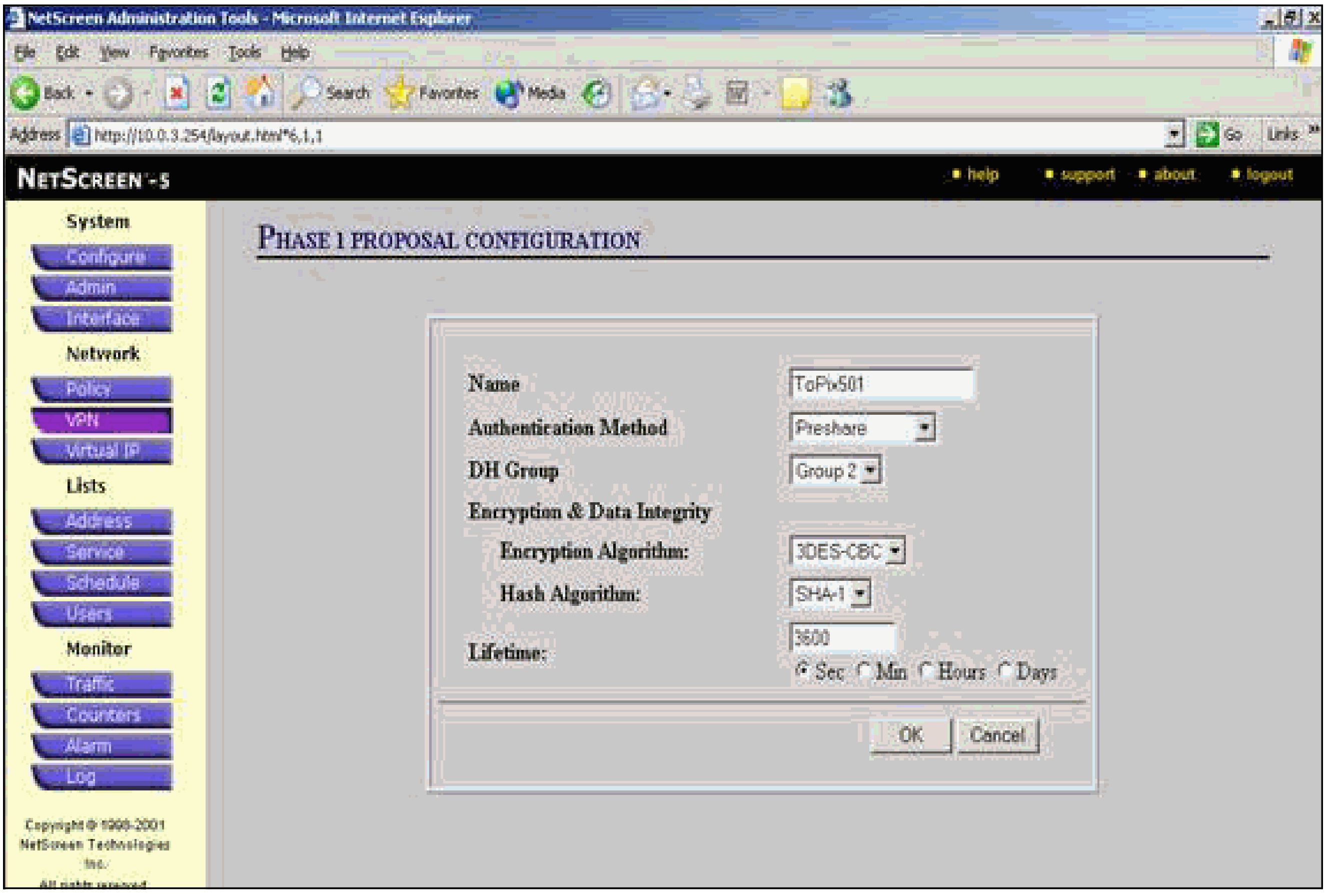
OK Cancel

成功建立遠端隧道網關後，將出現一個類似此的螢幕。


NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.3.254/layout.html*6,1,1
Go Links
NETSCREEN-5
help support about logout
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright© 1998-2001 NetScreen Technologies Inc. All rights reserved.
VPN
17 Sept 2003 15:40:00
Page 1 of 1
Manual Key
AutoKey IKE
Gateway
P1 Proposal
P2 Proposal
Certificates
L2TP
IPPool
New Remote Tunnel Gateway
List 10 Per Page
Go to the Gateway Configuration
Internet

Name	Group/User Name/Peer IP	Peer ID	IKE Tunnel Type	Mode	P1 Proposals	Configure
To501	172.18.124.96		PreShare	Main	pre-g2-3des-sha	Edit

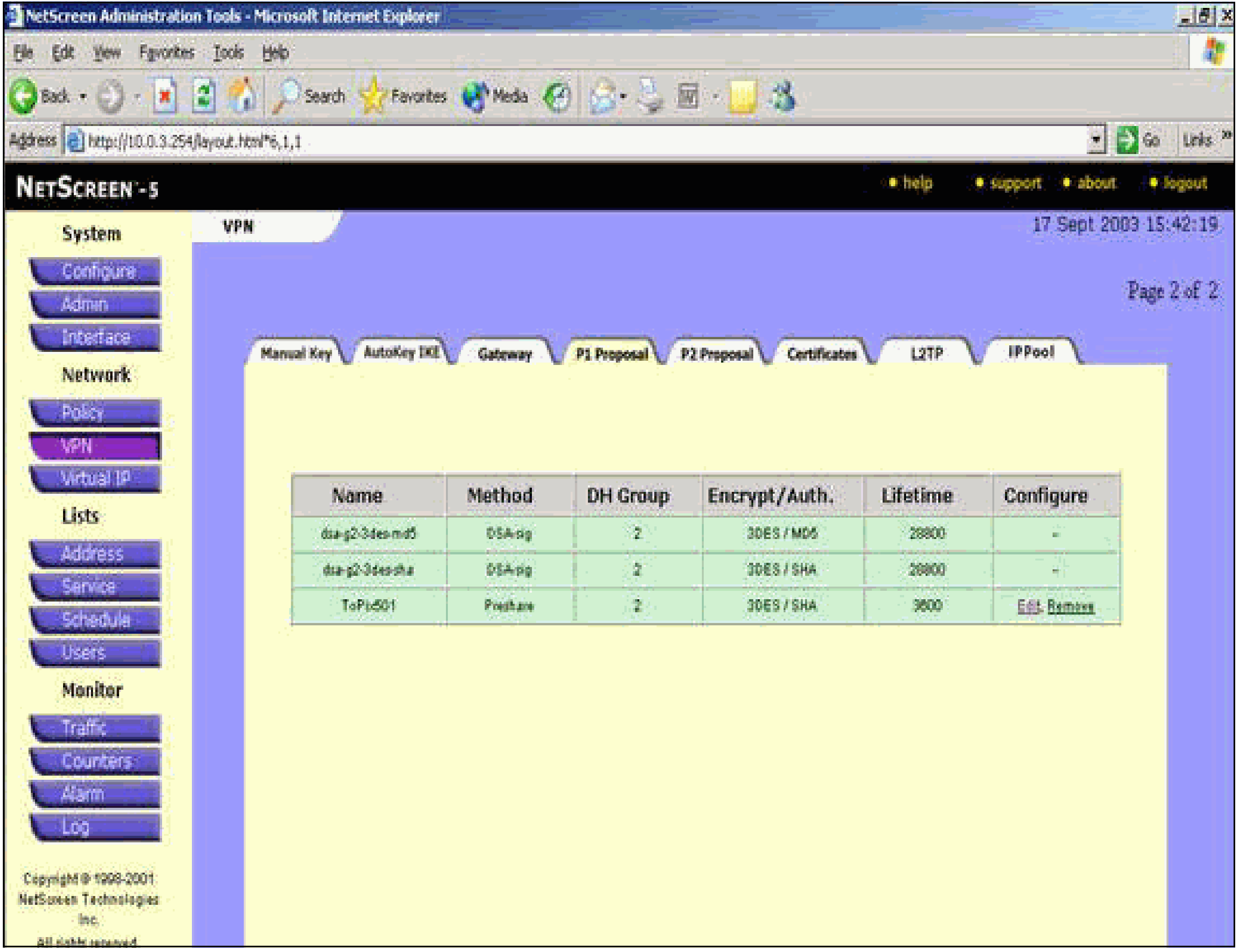
7. 轉到P1建議頁籤，然後按一下**New Phase 1 Proposal**以配置建議1。
8. 輸入第1階段建議的配置資訊，然後按一下**OK**。此示例將這些欄位和值用於階段1交換。**名稱**:ToPix501**驗證:**普雷沙雷**DH組**：組2**加密**：3DES-CBC**雜湊**：SHA-1**生存期**：3600秒


NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://10.0.3.254/layout.html*6,1,1
NETSCREEN-5
help support about logout
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright © 1998-2001 NetScreen Technologies Inc.
All rights reserved.
OK
Cancel

PHASE 1 PROPOSAL CONFIGURATION

Name	ToPix501
Authentication Method	Preshare
DH Group	Group 2
Encryption & Data Integrity	
Encryption Algorithm:	3DES-CBC
Hash Algorithm:	SHA-1
Lifetime:	3600 ● Sec ○ Min ○ Hours ○ Days

第1階段成功新增到NetScreen配置後，會出現一個類似於此示例的螢幕。

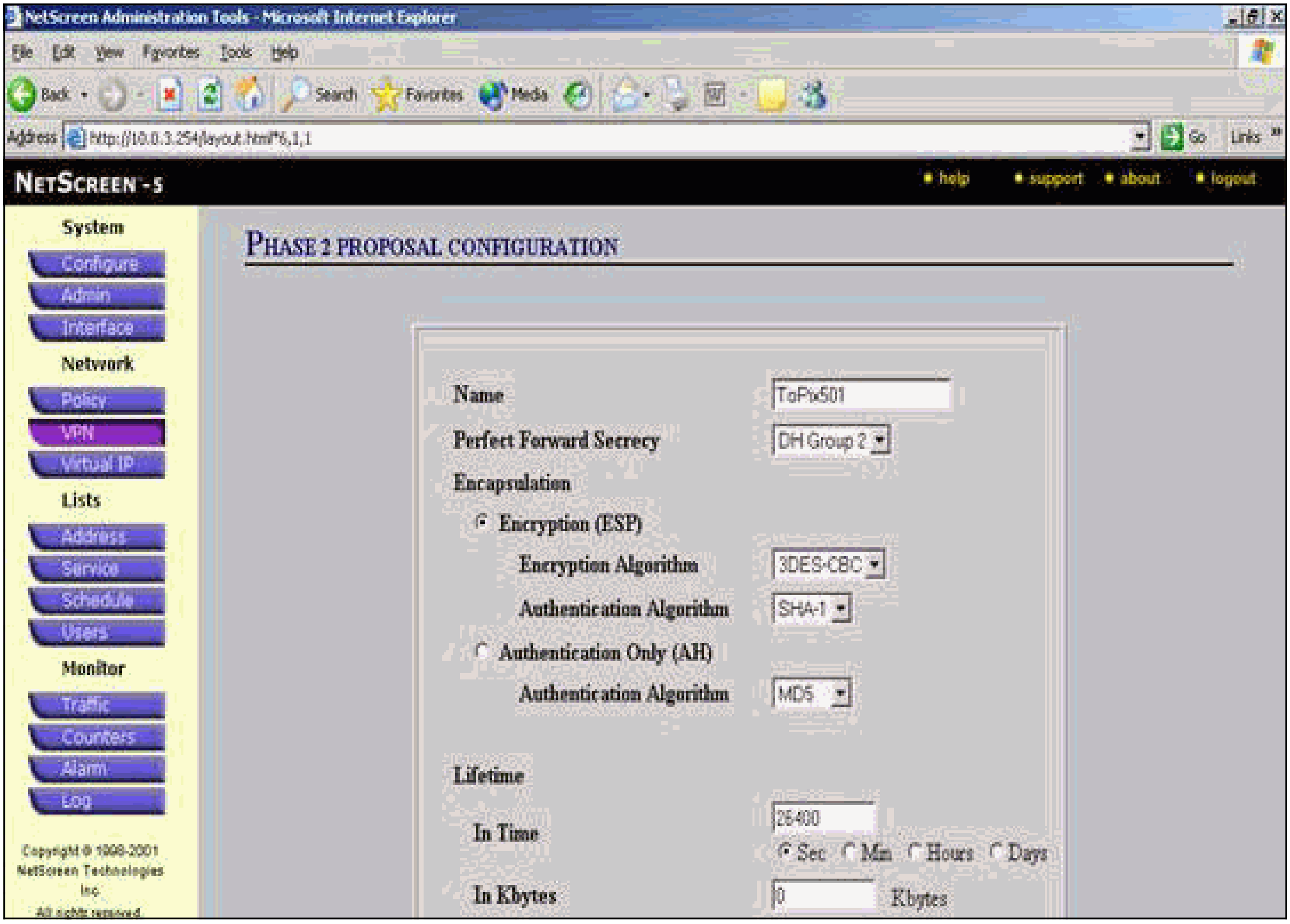


Name	Method	DH Group	Encrypt/Auth.	Lifetime	Configure
dsa-g2-3des-md5	DSA-sig	2	3DES / MD5	28800	-
dsa-g2-3des-sha	DSA-sig	2	3DES / SHA	28800	-
ToPix501	Preshare	2	3DES / SHA	3600	Edit, Remove

9. 轉到P2計畫書頁籤，然後按一下**New Phase 2 Proposal**以配置第2階段。

10. 輸入第2階段建議的配置資訊，然後按一下**OK**。此示例將這些欄位和值用於第2階段交換。**名**

稱:ToPix501**完全向前保密**：DH-2（1024位）**加密演算法**：3DES-CBC**驗證演算法**：SHA-1**生存期**：26400秒

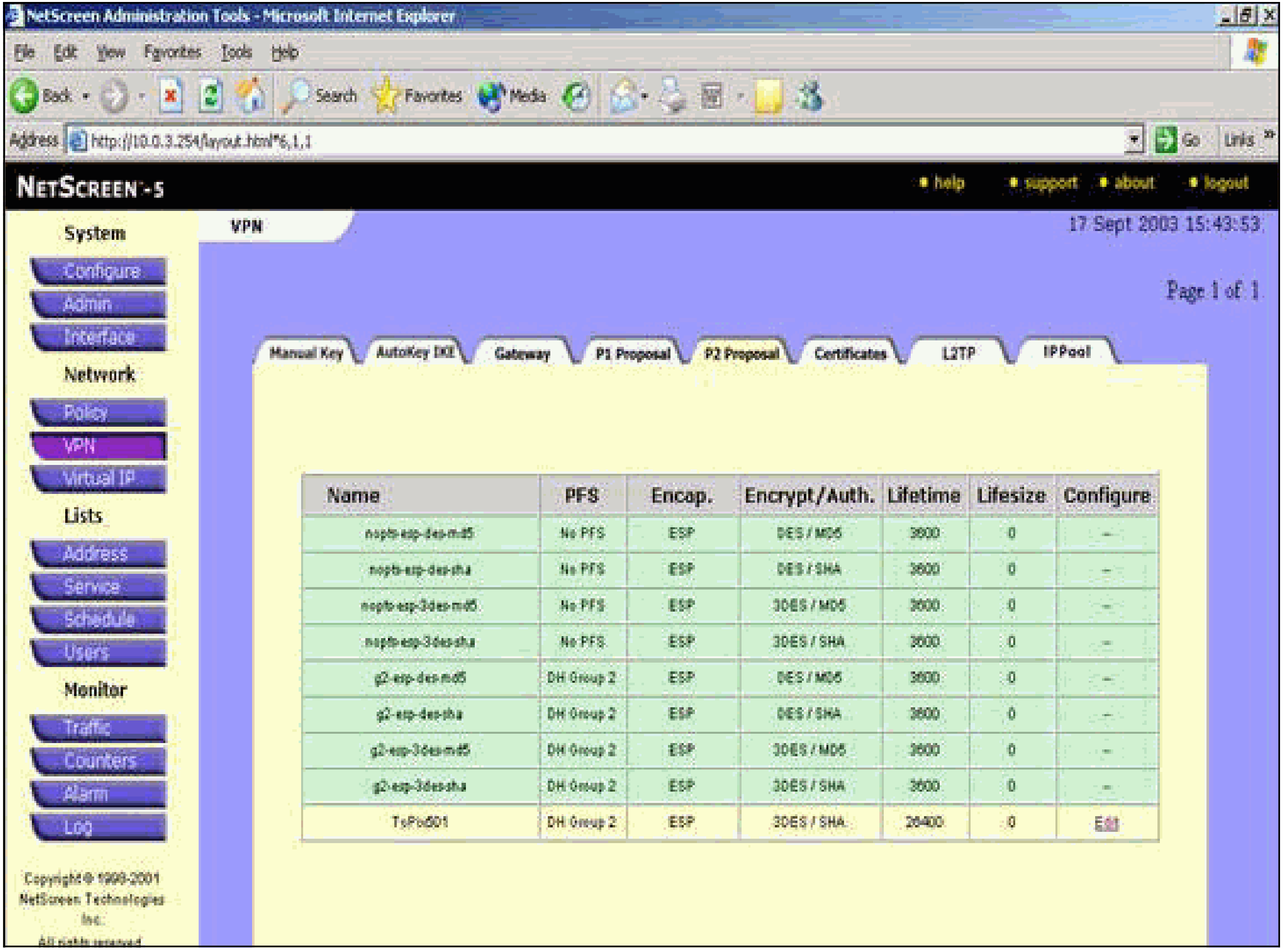


PHASE 2 PROPOSAL CONFIGURATION

Name	ToPix501
Perfect Forward Secrecy	DH Group 2
Encapsulation	
● Encryption (ESP)	
Encryption Algorithm	3DES-CBC
Authentication Algorithm	SHA-1
○ Authentication Only (AH)	
Authentication Algorithm	MD5
Lifetime	
In Time	26400 ● Sec ○ Min ○ Hours ○ Days
In Kbytes	0 Kbytes

NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.3.254/layout.html*6,1,1
Go Links
NETSCREEN-5
help support about logout
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright © 1998-2001 NetScreen Technologies Inc.
All rights reserved

第2階段成功新增到NetScreen配置後，會出現一個類似於此示例的螢幕。



VPN

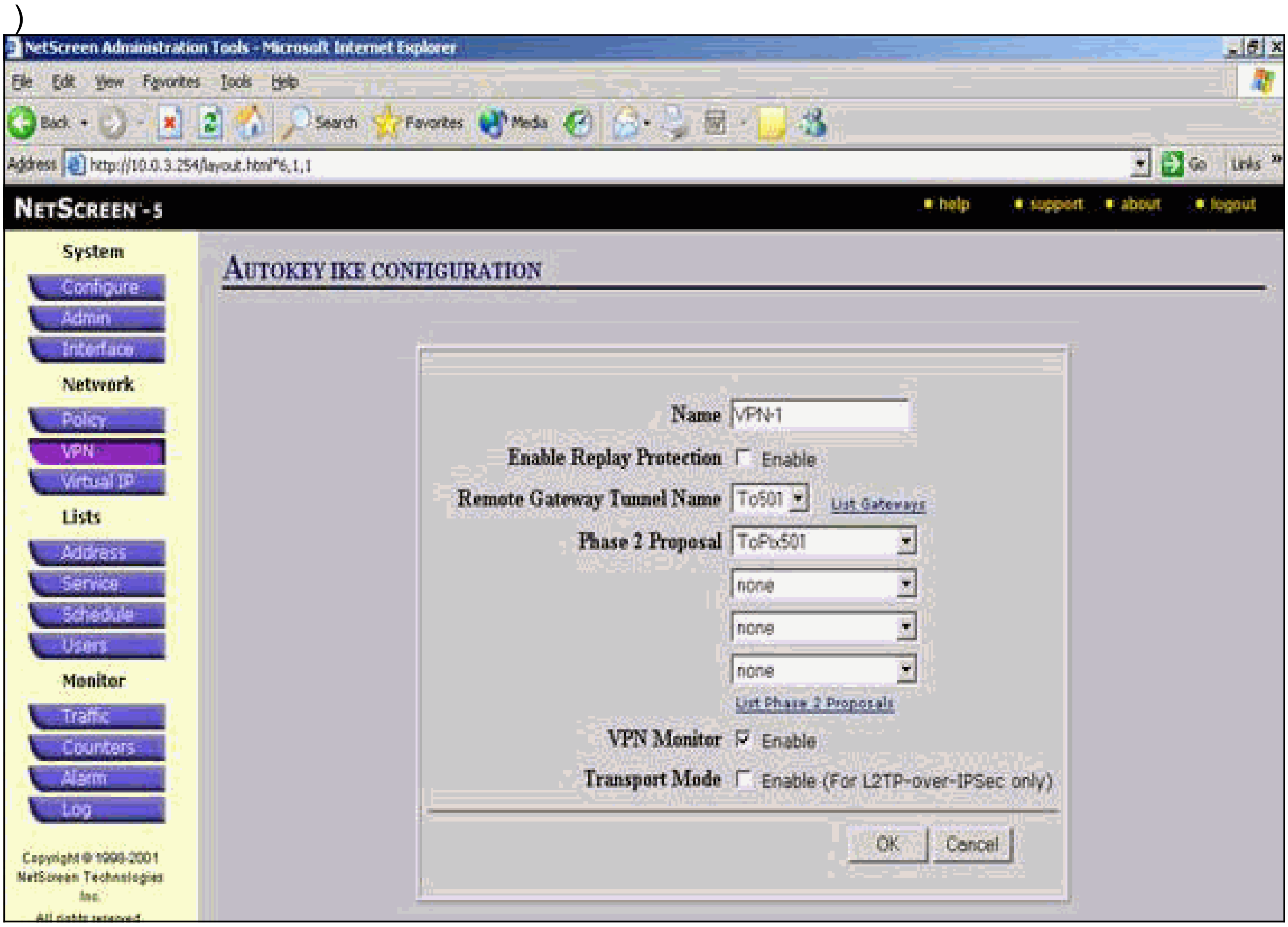
17 Sept 2003 15:43:53

Page 1 of 1

Name	PFS	Encap.	Encrypt/Auth.	Lifetime	Lifesize	Configure
nopfs-esp-des-md5	No PFS	ESP	DES / MD5	3600	0	-
nopfs-esp-des-sha	No PFS	ESP	DES / SHA	3600	0	-
nopfs-esp-3des-md5	No PFS	ESP	3DES / MD5	3600	0	-
nopfs-esp-3des-sha	No PFS	ESP	3DES / SHA	3600	0	-
g2-esp-des-md5	DH Group 2	ESP	DES / MD5	3600	0	-
g2-esp-des-sha	DH Group 2	ESP	DES / SHA	3600	0	-
g2-esp-3des-md5	DH Group 2	ESP	3DES / MD5	3600	0	-
g2-esp-3des-sha	DH Group 2	ESP	3DES / SHA	3600	0	-
ToPix501	DH Group 2	ESP	3DES / SHA	26400	0	Edit

NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.3.254/layout.html*6,1,1
Go Links
NETSCREEN-5
help support about logout
Manual Key
AutoKey IKE
Gateway
P1 Proposal
P2 Proposal
Certificates
L2TP
IPPool
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright © 1998-2001 NetScreen Technologies Inc.
All rights reserved

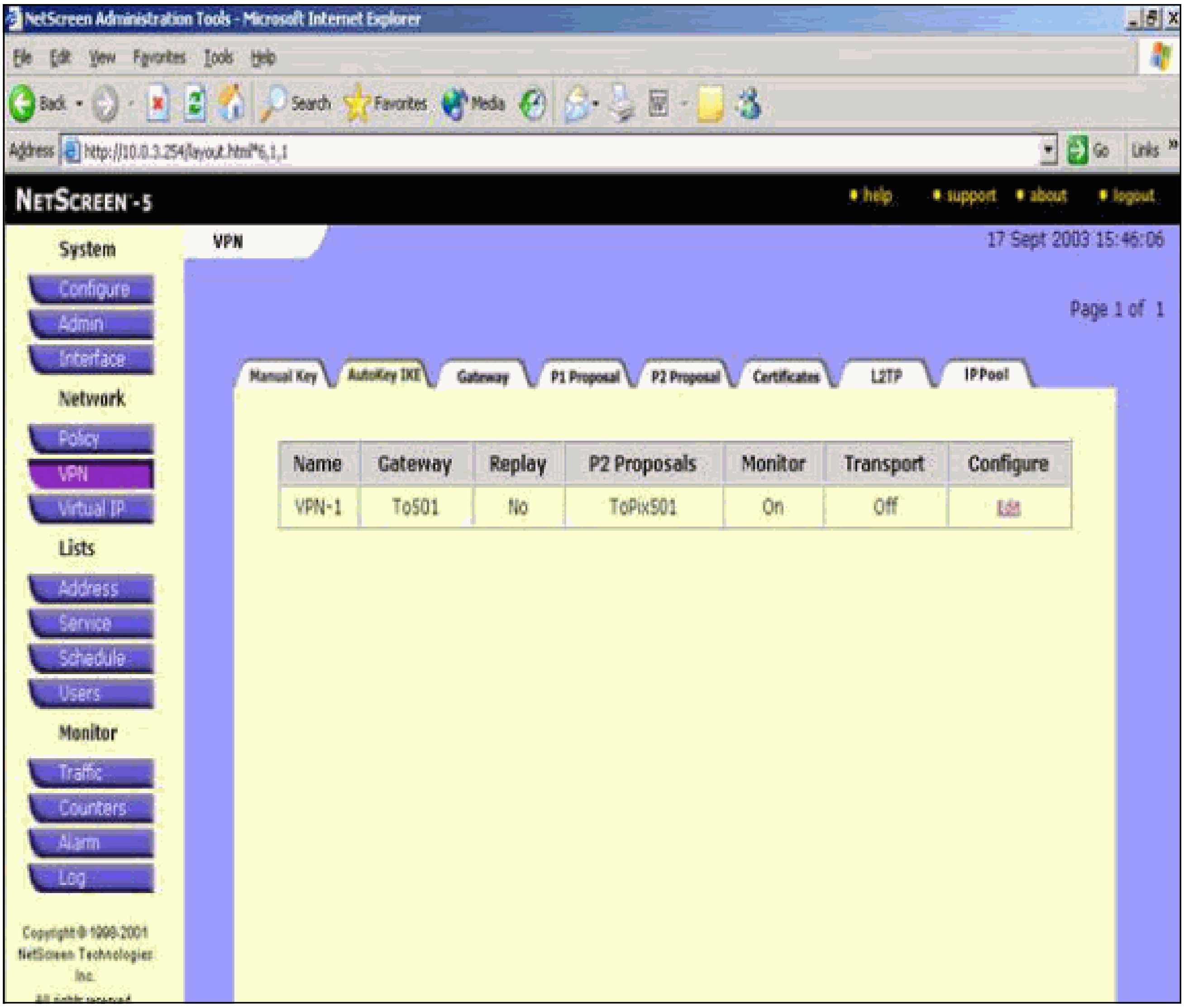
11. 選擇**AutoKey IKE**頁籤，然後按一下**New AutoKey IKE Entry**以建立和配置AutoKeys IKE。
12. 輸入AutoKey IKE的配置資訊，然後按一下**OK**。此示例對AutoKey IKE使用這些欄位和值。
名稱:VPN-1**遠端網關隧道名稱：**To501（這之前在「網關」頁籤上建立。）**第2階段建議**
：ToPix501（這之前在P2 Proposal頁籤上建立。）**VPN監控器：**啟用（這使NetScreen裝置能夠設定簡單網路管理協定[SNMP]陷阱，以便監控VPN監控器的狀況。
）


NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.3.254/layout.html*6,1,1
Go Links
NETSCREEN-5
help support about logout
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved
List Gateways
List Phase 2 Proposals
OK
Cancel

AUTOKEY IKE CONFIGURATION

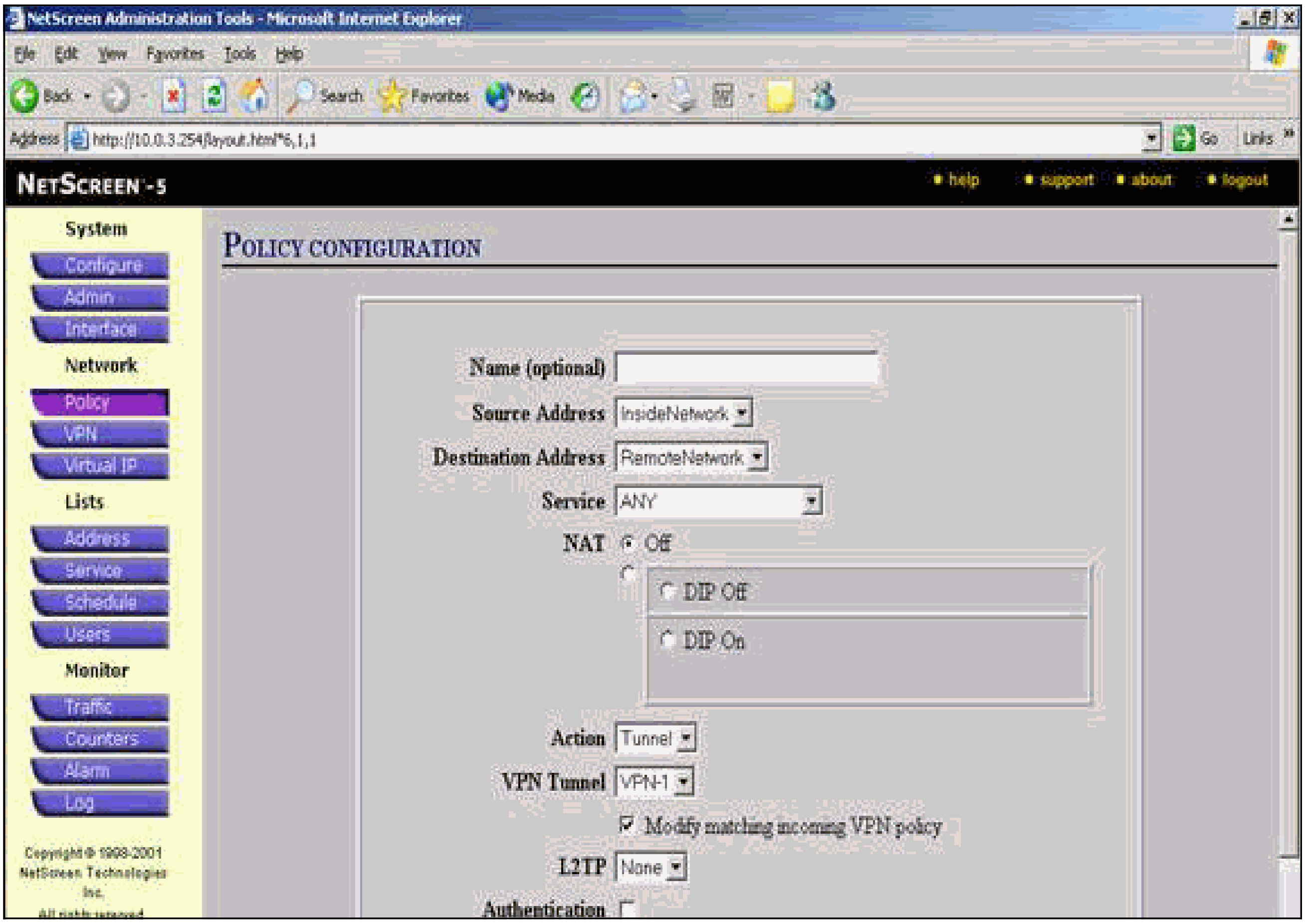
Name VPN-1
Enable Replay Protection □ Enable
Remote Gateway Tunnel Name To501
Phase 2 Proposal ToPix501
none
none
none
VPN Monitor ☑ Enable
Transport Mode □ Enable (For L2TP-over-IPSec only)

成功配置VPN-1規則後，會出現一個類似於此示例的螢幕。



Name	Gateway	Replay	P2 Proposals	Monitor	Transport	Configure
VPN-1	To501	No	ToPix501	On	Off	Edit

13. 選擇**Network > Policy**，轉到Outgoing頁籤，然後按一下**New Policy**以配置允許加密IPsec流量的規則。
14. 輸入策略的配置資訊，然後按一下**OK**。此示例對策略使用這些欄位和值。Name欄位是可選的，在此示例中未使用。**來源位址:**InsideNetwork(這之前在「受信任」(Trusted)頁籤上定義。)**目的地位址:**遠端網路(這之前在「不受信任」(Untrusted)頁籤下定義。)**服務：**任何**Action:**通道**VPN隧道：**VPN-1（先前在AutoKey IKE頁籤上將其定義為VPN隧道。）**修改匹配的傳入VPN策略：**已檢查（此選項自動建立與外部網路VPN流量匹配的入站規則。）


NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.3.254/layout.html*6,1,1
Go Links
NETSCREEN-5
help support about logout
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright © 1998-2001 NetScreen Technologies Inc.
All rights reserved

POLICY CONFIGURATION

Name (optional)

Source Address InsideNetwork

Destination Address RemoteNetwork

Service ANY

NAT ● Off
○
○ DIP Off
○ DIP On

Action Tunnel

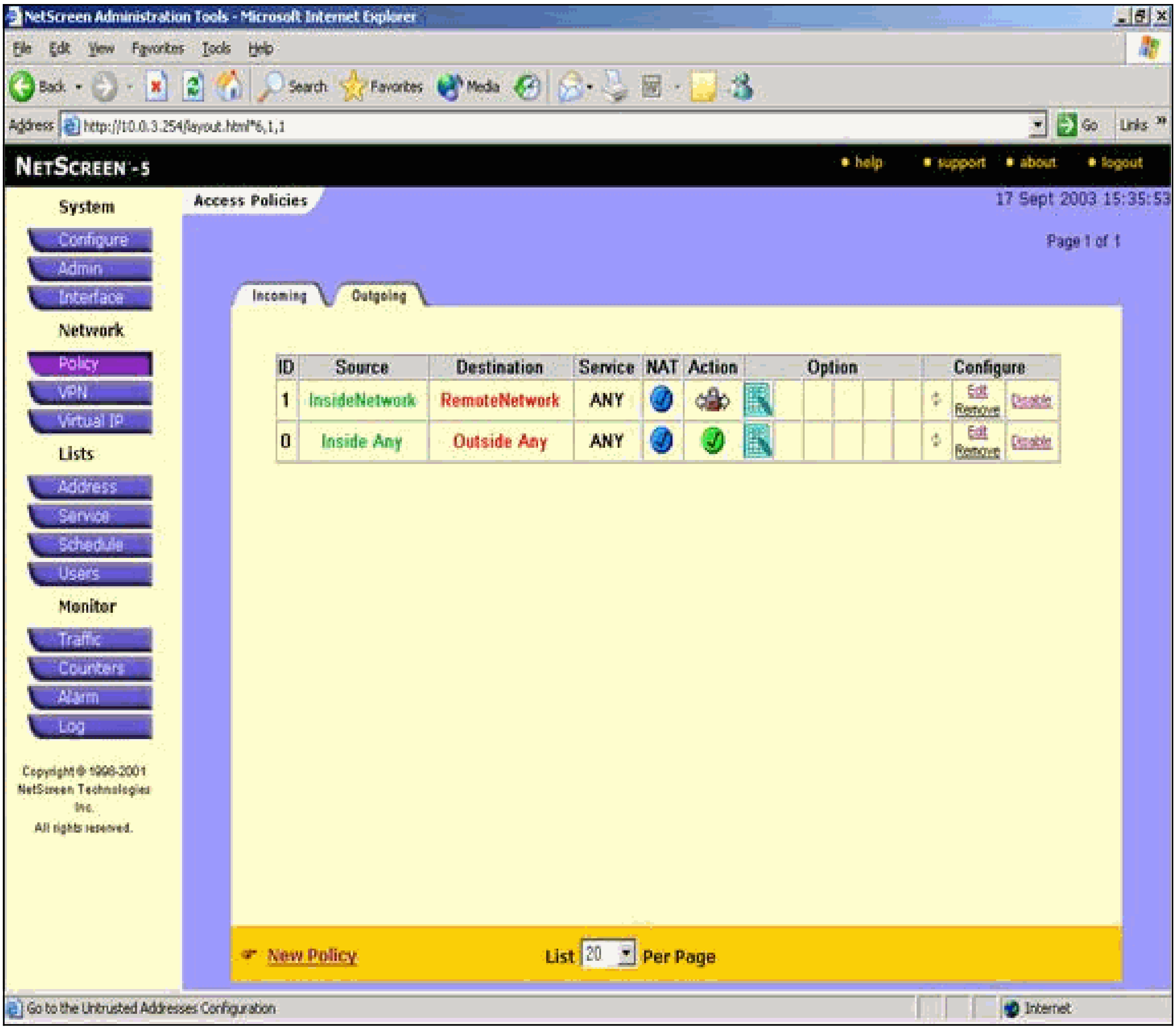
VPN Tunnel VPN-1

☑ Modify matching incoming VPN policy

L2TP None

Authentication □

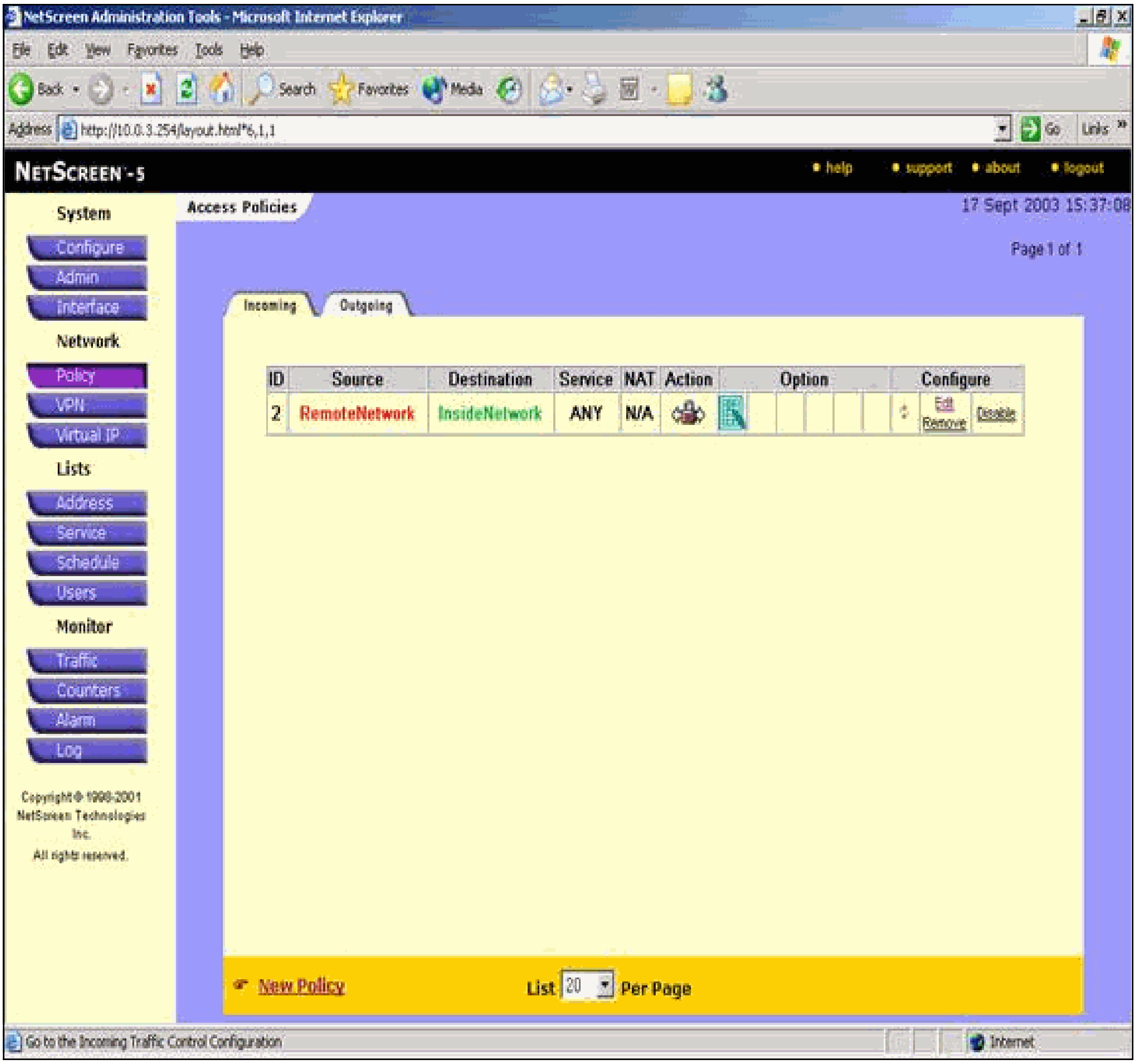
15. 新增策略時，請確保出站VPN規則在策略清單中排在第一位。（為入站流量自動建立的規則位於「入站」頁籤上。）如果需要更改策略的順序，請完成以下步驟：按一下Outgoing（傳出）頁籤。按一下Configure列中的循環箭頭以顯示Move Policy Micro視窗。更改策略的順序，使VPN策略高於策略ID 0（使VPN策略位於清單頂部）。


NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.3.254/layout.html*6,1,1 Go Links
NETSCREEN-5
help support about logout
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright © 1998-2001 NetScreen Technologies Inc. All rights reserved.
Access Policies
Page 1 of 1
Incoming
Outgoing
New Policy
List 20 Per Page
Go to the Untrusted Addresses Configuration
Internet

17 Sept 2003 15:35:53

ID	Source	Destination	Service	NAT	Action	Option	Configure	
1	InsideNetwork	RemoteNetwork	ANY				Edit Remove	Disable
0	Inside Any	Outside Any	ANY		✓		Edit Remove	Disable

轉到Incoming頁籤以檢視入站流量的規則。


NetScreen Administration Tools - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://10.0.3.254/layout.html*6,1,1
Go Links
NETSCREEN-5
help support about logout
System
Configure
Admin
Interface
Network
Policy
VPN
Virtual IP
Lists
Address
Service
Schedule
Users
Monitor
Traffic
Counters
Alarm
Log
Copyright© 1998-2001 NetScreen Technologies Inc. All rights reserved.
Access Policies
17 Sept 2003 15:37:08
Page 1 of 1
Incoming
Outgoing
New Policy
List 20 Per Page
Go to the Incoming Traffic Control Configuration
Internet

ID	Source	Destination	Service	NAT	Action	Option	Configure	
2	RemoteNetwork	InsideNetwork	ANY	N/A			Edit Remove	Disable

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

驗證命令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

- ping — 診斷基本網路連線。
- show crypto ipsec sa — 顯示第2階段安全關聯。
- show crypto isakmp sa — 顯示第1階段安全關聯。

驗證輸出

ping和show命令的輸出示例如下所示。

此ping操作是從NetScreen防火牆後的主機發起的。

```
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命令的輸出如下所示。

```
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命令的輸出如下所示。

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **debug crypto engine** — 顯示有關加密引擎的消息。
- **debug crypto ipsec** — 顯示有關IPsec事件的資訊。
- **debug crypto isakmp** — 顯示有關IKE事件的消息。

調試輸出示例

此處顯示了PIX防火牆的**debug**輸出示例。

```
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
```

相關資訊

- IPSec 協商/IKE 通訊協定
- Cisco PIX防火牆軟體
- Cisco Secure PIX防火牆命令參考
- 安全產品現場通知（包括PIX）
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems