配置IPSec隧道 — Cisco Secure PIX防火牆到Checkpoint 4.1防火牆

目錄

簡介

此示例配置演示如何使用預共用金鑰形成IPSec隧道以加入兩個專用網路。在我們的示例中，加入的網路是Cisco安全Pix防火牆(PIX)內部的192.168.1.X專用網路和Checkpoint內部的10.32.50.X專用網路。假設從PIX內部和Checkpoint 4.1防火牆內部到Internet（此處由172.18.124.X網路表示）的流量會在開始此配置之前流動。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- PIX軟體版本5.3.1
- Checkpoint 4.1防火牆

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。

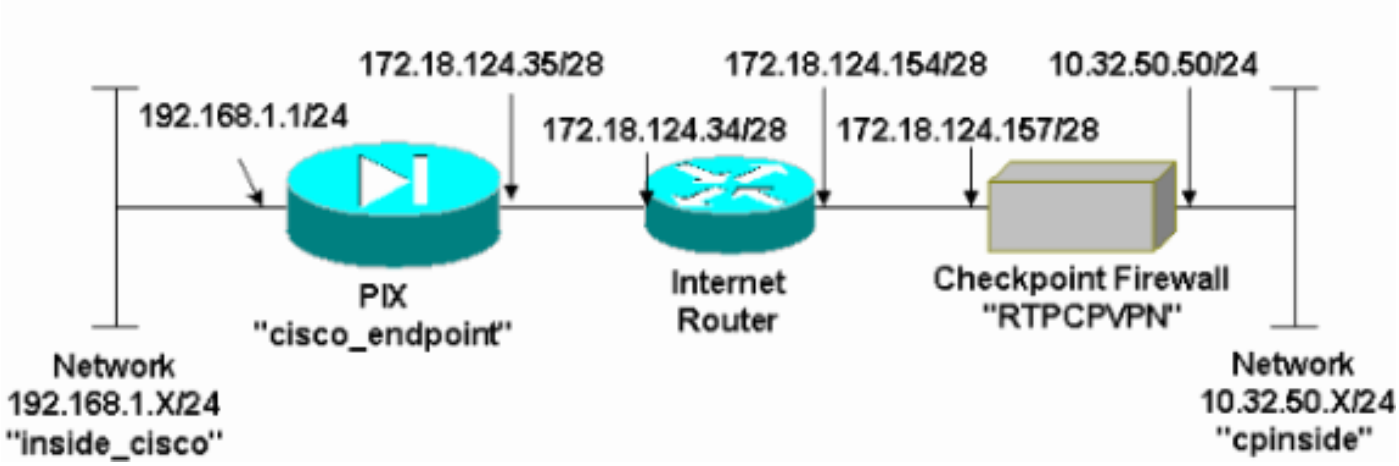
設定

本節提供用於設定本文件中所述功能的資訊。

注意：要查詢有關本文檔中使用的命令的其他資訊，請使用命令查詢工具(僅限註冊客戶)。

網路圖表

本檔案會使用下圖所示的網路設定：



組態

本文檔使用本節中顯示的配置。

PIX配置

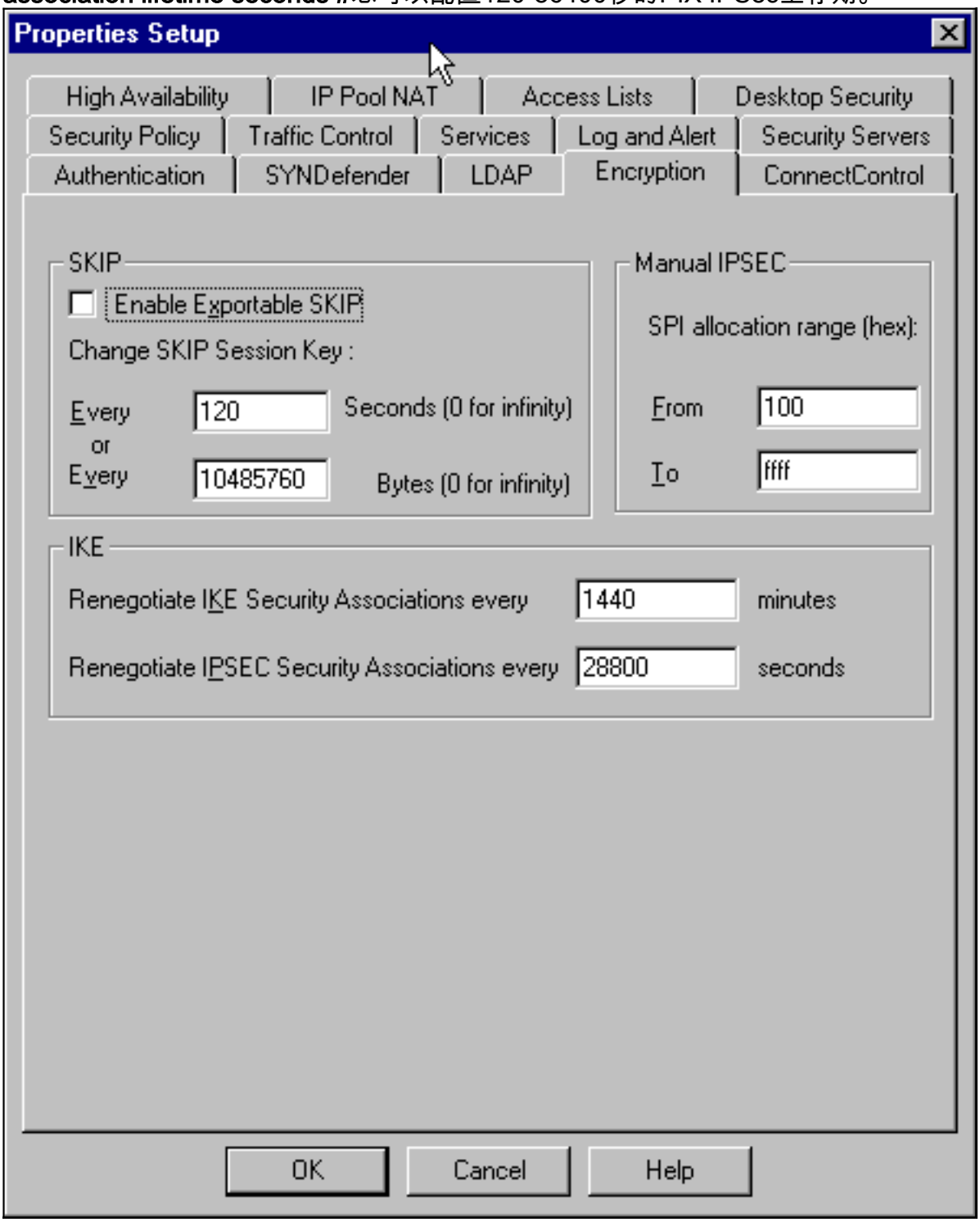
```
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname cisco_endpoint
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list 115 permit ip 192.168.1.0 255.255.255.0
10.32.50.0 255.255.255.0
access-list 115 deny ip 192.168.1.0 255.255.255.0 any
```

```
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
logging monitor debugging
no logging buffered
logging trap debugging
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.35 255.255.255.240
ip address inside 192.168.1.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 172.18.124.36
nat (inside) 0 access-list 115
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.18.124.34 1
timeout xlate 3:00:00g SA 0x80bd6a10, conn_id = 0
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h323
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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- IPSec configuration sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-sha-hmac
crypto map rtpmap 10 ipsec-isakmp
crypto map rtpmap 10 match address 115
crypto map rtpmap 10 set peer 172.18.124.157
crypto map rtpmap 10 set transform-set myset
crypto map rtpmap 10 set security-association lifetime
seconds
3600 kilobytes 4608000
crypto map rtpmap interface outside
!--- IKE configuration isakmp enable outside
isakmp key ******** address 172.18.124.157 netmask
255.255.255.240
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash sha
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
telnet timeout 5
ssh timeout 5
terminal width 80
```

```
Cryptochecksum:dc43c44e4513d3633a3fc7b1c3802c79
: end
[OK]
```

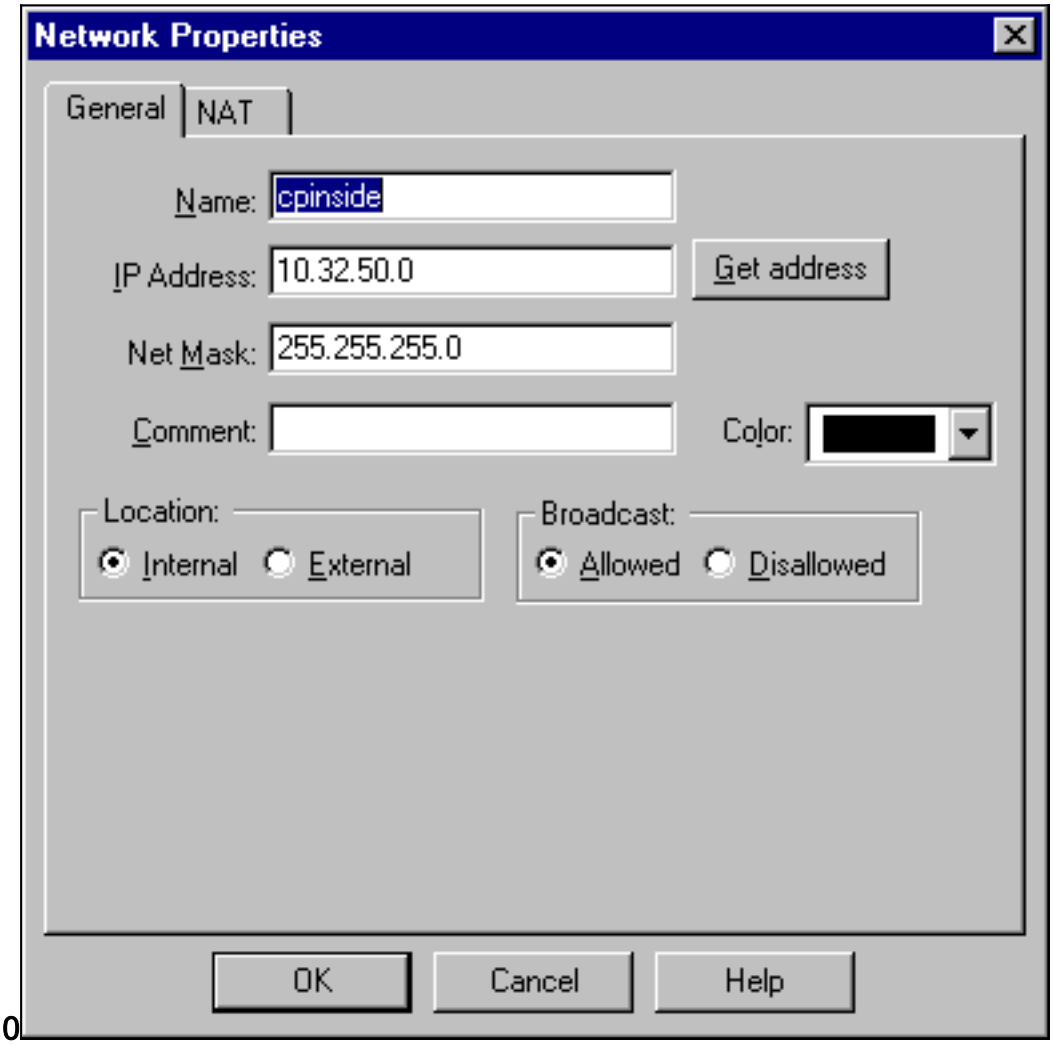
檢查點防火牆

1. 由於IKE和IPSec的預設生存時間因供應商而異，請選擇**Properties > Encryption**以設定檢查點生存時間以與PIX預設值一致。PIX預設IKE生存時間為86400秒（=1440分鐘），可通過以下命令進行修改：**isakmp policy # lifetime 86400**PIX IKE生存期可以在60到100秒86400配置。PIX預設IPSec生存時間為28800秒，可通過以下命令進行修改：**crypto ipsec security-association lifetime seconds #**您可以配置120-86400秒的PIX IPSec生存期。

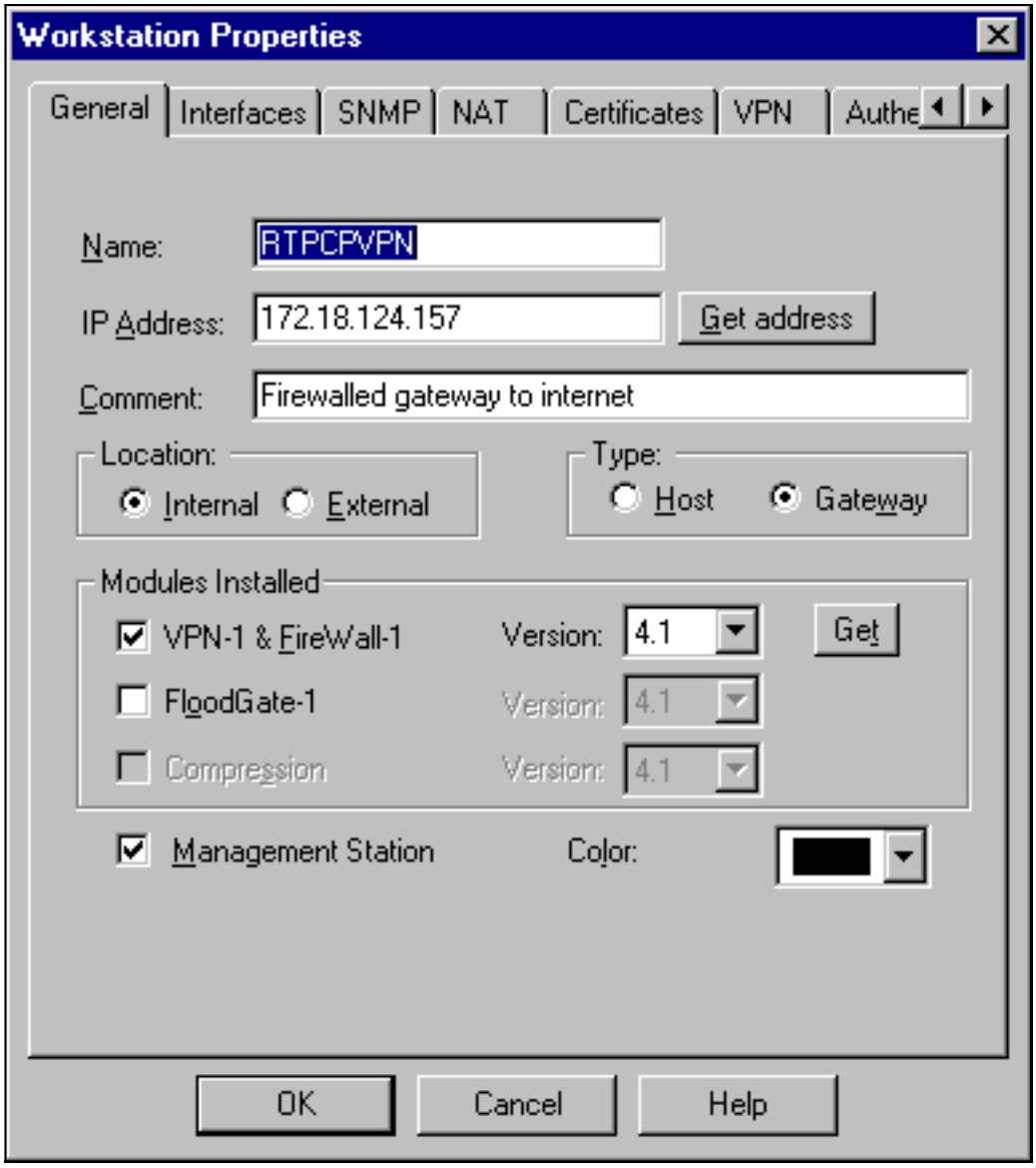


2. 選擇**Manage > Network objects > New（或Edit） > Network**，為檢查點後面的內部("cpinside")網路配置對象。這必須與此PIX命令中的目標（秒）網路一致：**access-list 115**

permit ip 192.168.1.0 255.255.255.0 10.32.50.0 255.255.255.0

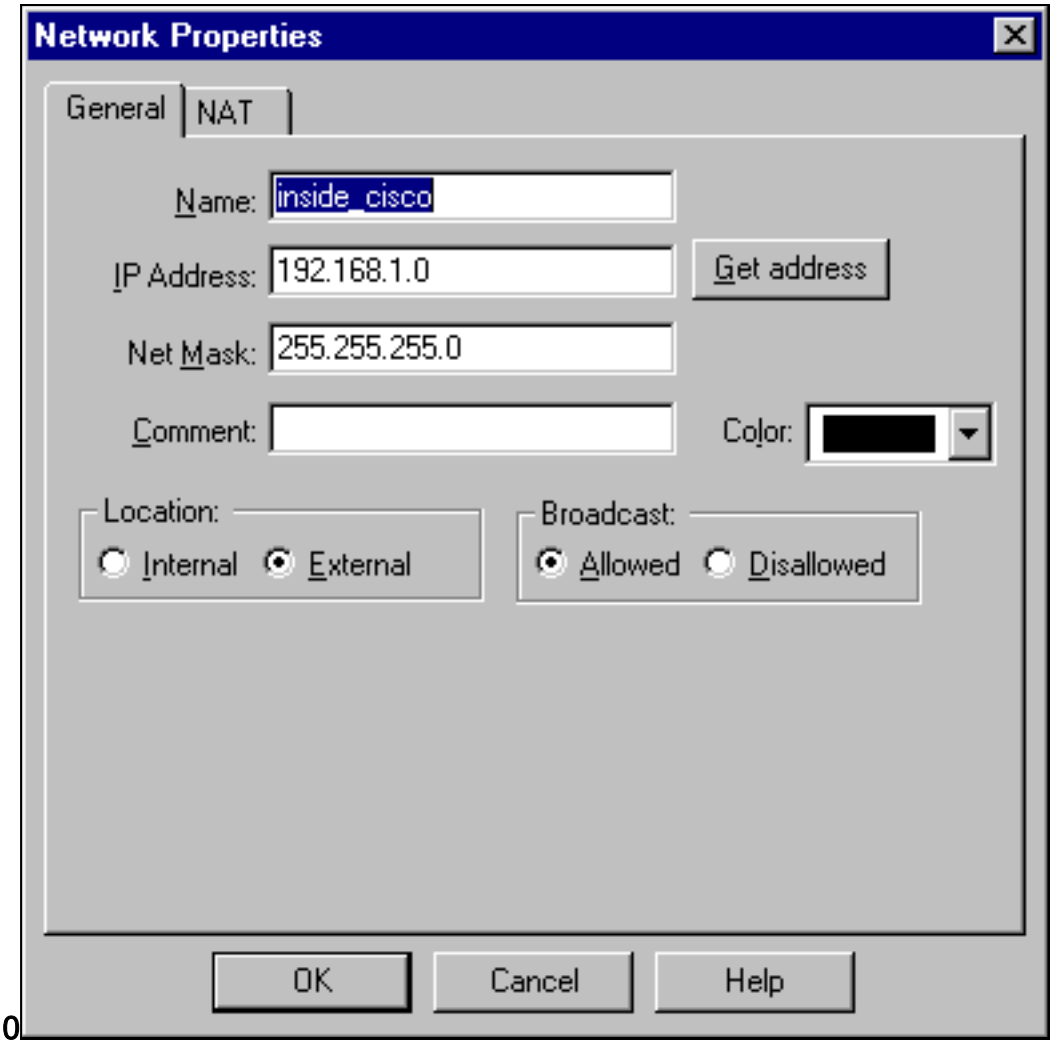


3. 選擇**Manage > Network objects > Edit**以編輯PIX在此命令中指向的網關（「RTPCPVPN」檢查點）端點的對象：**crypto map name # set peer ip_address**在Location下，選擇**Internal**。對於Type，選擇**Gateway**。在Modules Installed下，選中**VPN-1 & FireWall-1**覈取方塊，同時選中**Management Station**覈取方塊



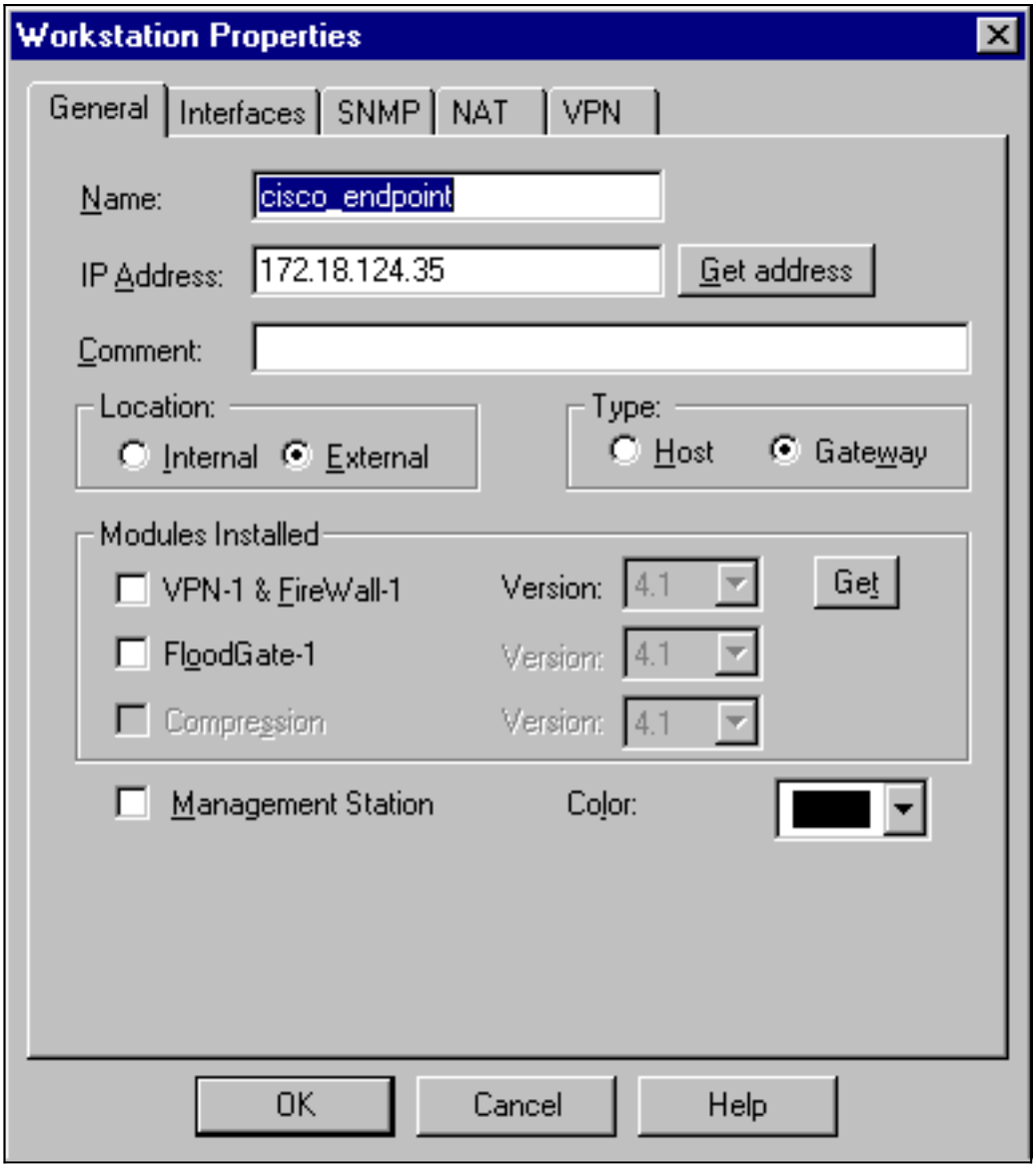
:

4. 選擇**Manage > Network objects > New > Network**，為PIX後面的外部("inside_cisco")網路配置對象。這必須與此PIX命令中的源（第一個）網路一致：**access-list 115 permit ip 192.168.1.0 255.255.255.0 10.32.50.0**

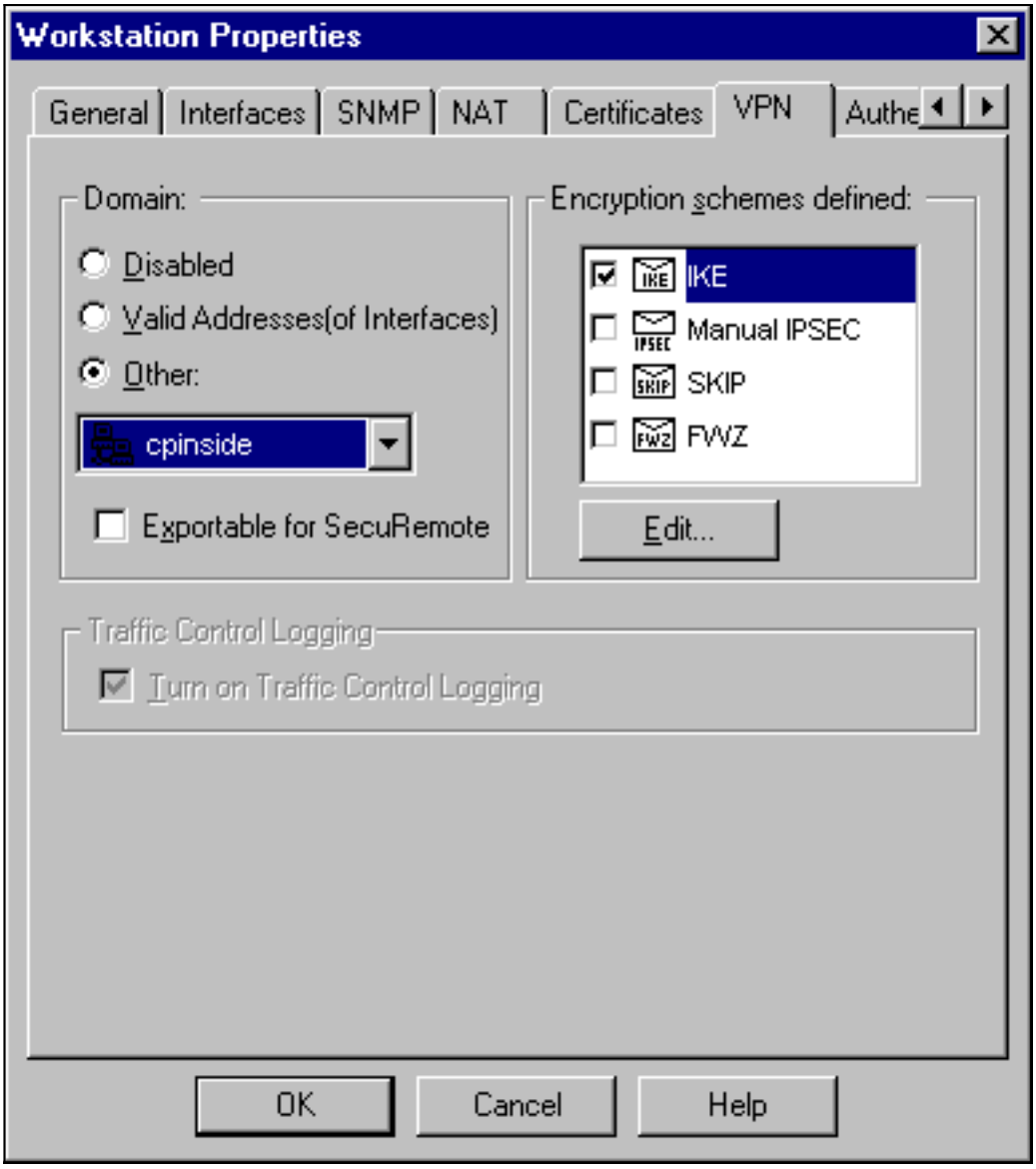


255.255.255.0

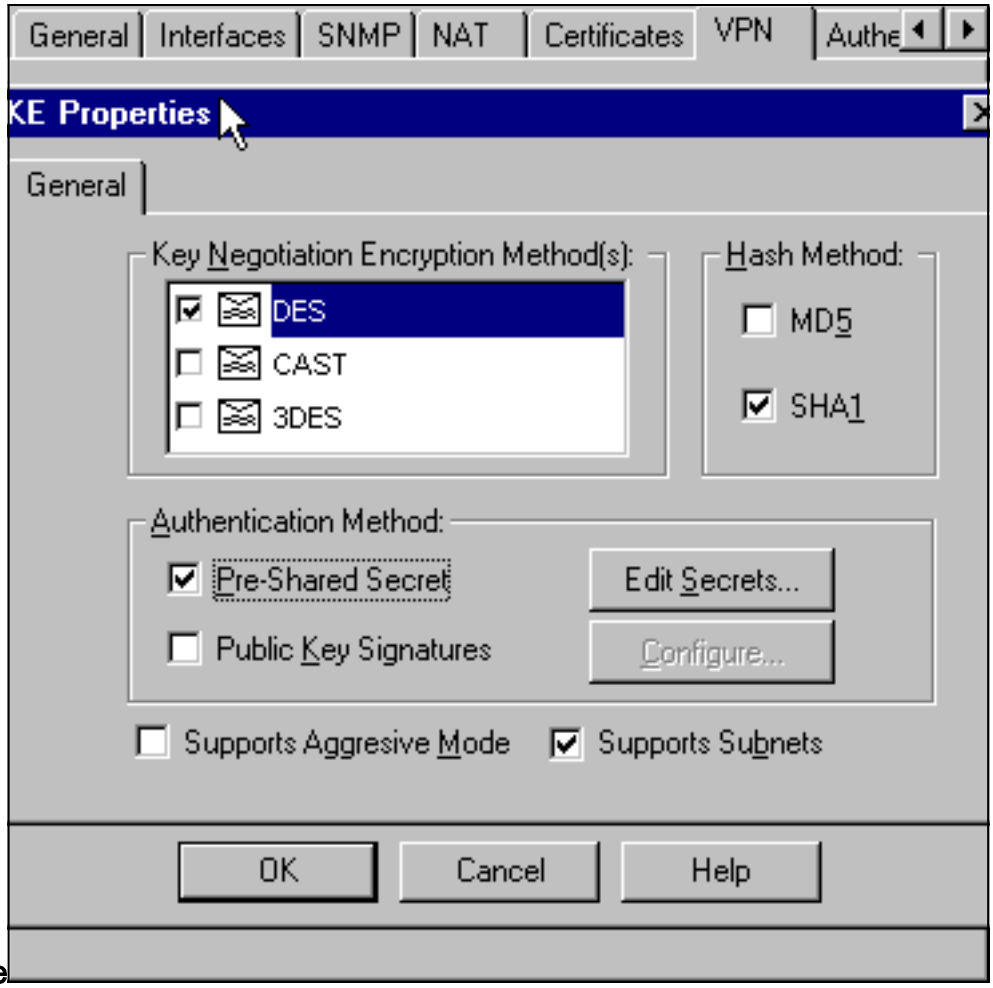
5. 選擇**Manage > Network objects > New > Workstation**，為外部(「cisco_endpoint」)PIX網關新增對象。這是應用此命令的PIX介面：**crypto map *name* interface outside**在「位置」下，選擇**「外部」**。對於Type，選擇**Gateway**。**注意：**不要選中VPN-1/FireWall-1覈取方塊。



6. 選擇**Manage > Network objects > Edit**以編輯檢查點網關端點（稱為「RTPCPVPN」）VPN頁籤。在域下，選擇**其他**，然後從下拉選單中選擇檢查點網路（稱為「cpinside」）內部。在Encryption schemes defined下，選擇**IKE**，然後按一下**Edit**。

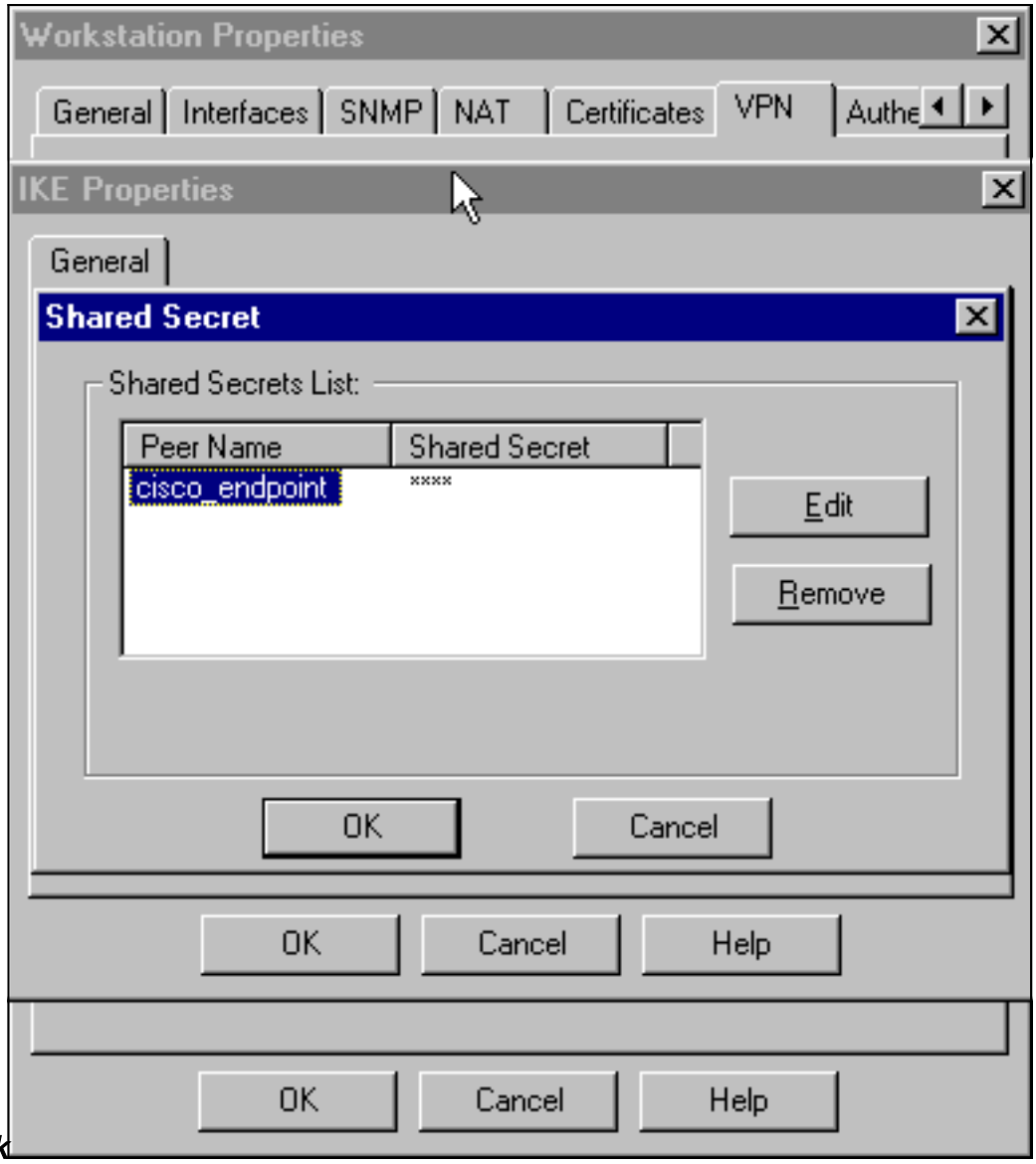


7. 更改DES加密的IKE屬性以同意以下命令：**isakmp policy # encryption des**
8. 將IKE屬性更改為SHA1雜湊，以同意以下命令：**isakmp policy # hash sha**更改以下設定：取消選擇**Aggressive Mode**。選中**Supports Subnets**覈取方塊。在Authentication Method下，選中**Pre-Shared Secret複選**框。此指令與此指令一致：**isakmp policy # authentication pre-**



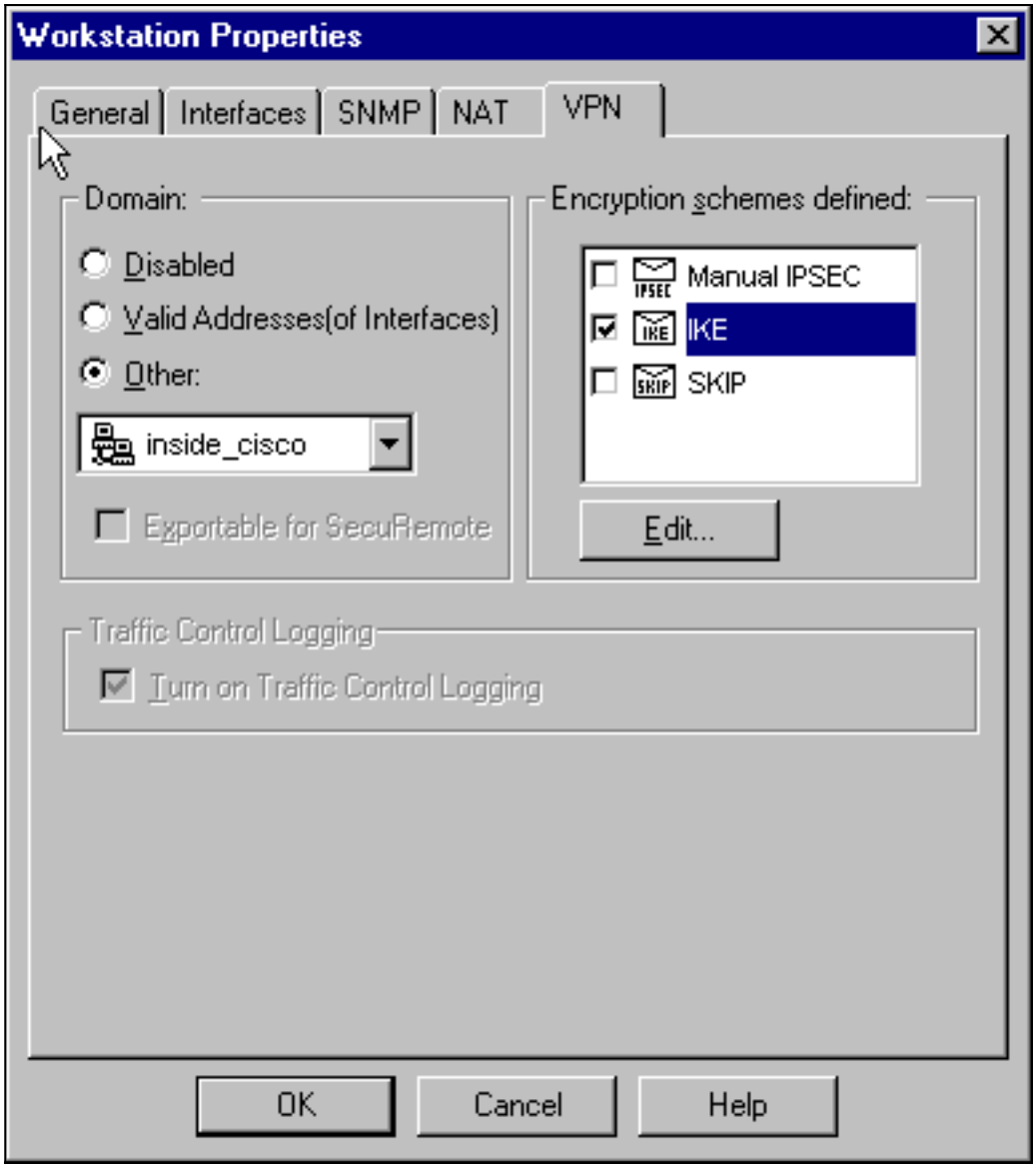
share

9. 按一下**Edit Secrets**設定預共用金鑰以與PIX命令一致：**isakmp key *key address* netmask**

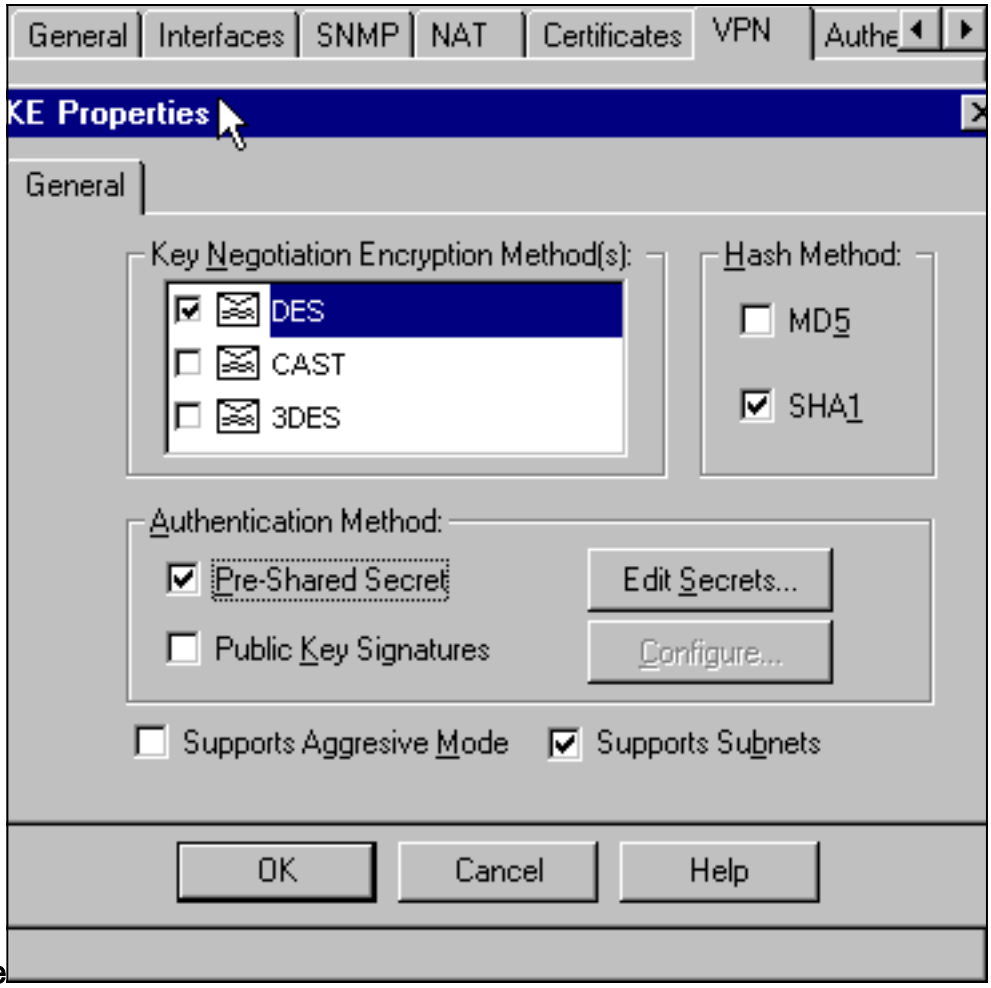


netmask

10. 選擇**Manage > Network Objects > Edit**以編輯「cisco_endpoint」VPN頁籤。在Domain下，選擇**Other**，然後選擇PIX網路內部（稱為"inside_cisco"）。 在Encryption schemes defined下，選擇**IKE**，然後按一下**Edit**。

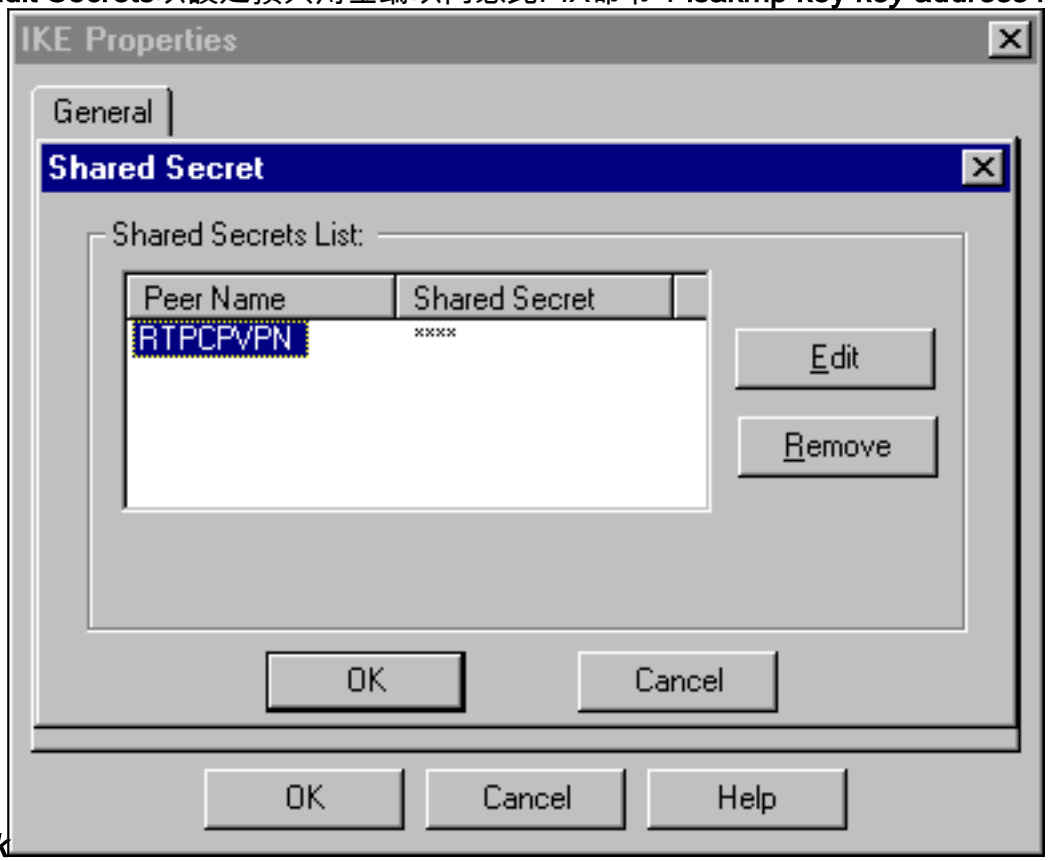


11. 更改IKE屬性DES加密以同意以下命令：**isakmp policy # encryption des**
12. 將IKE屬性更改為SHA1雜湊，以同意以下命令：**crypto isakmp policy # hash sha**更改以下設定：取消選擇**Aggressive Mode**。選中**Supports Subnets**覈取方塊。在Authentication Method下，選中**Pre-Shared Secret**覈取方塊。此運算子合以下命令：**isakmp policy # authentication pre-**



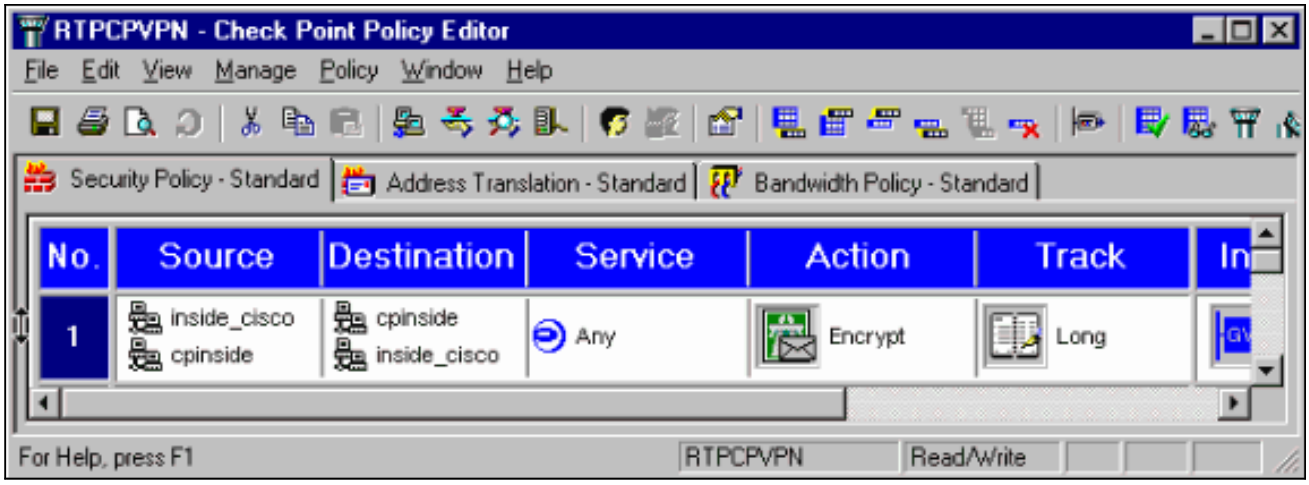
share

13. 按一下**Edit Secrets**以設定預共用金鑰以同意此PIX命令：**isakmp key *key address* netmask**

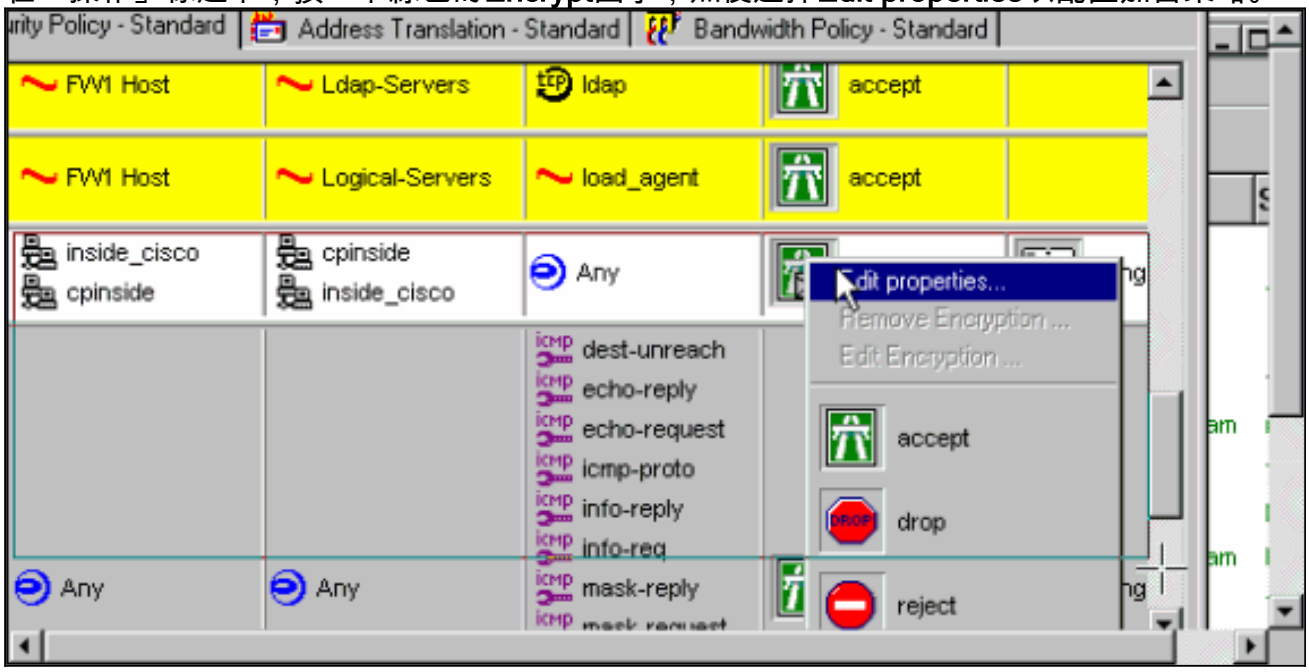


netmask

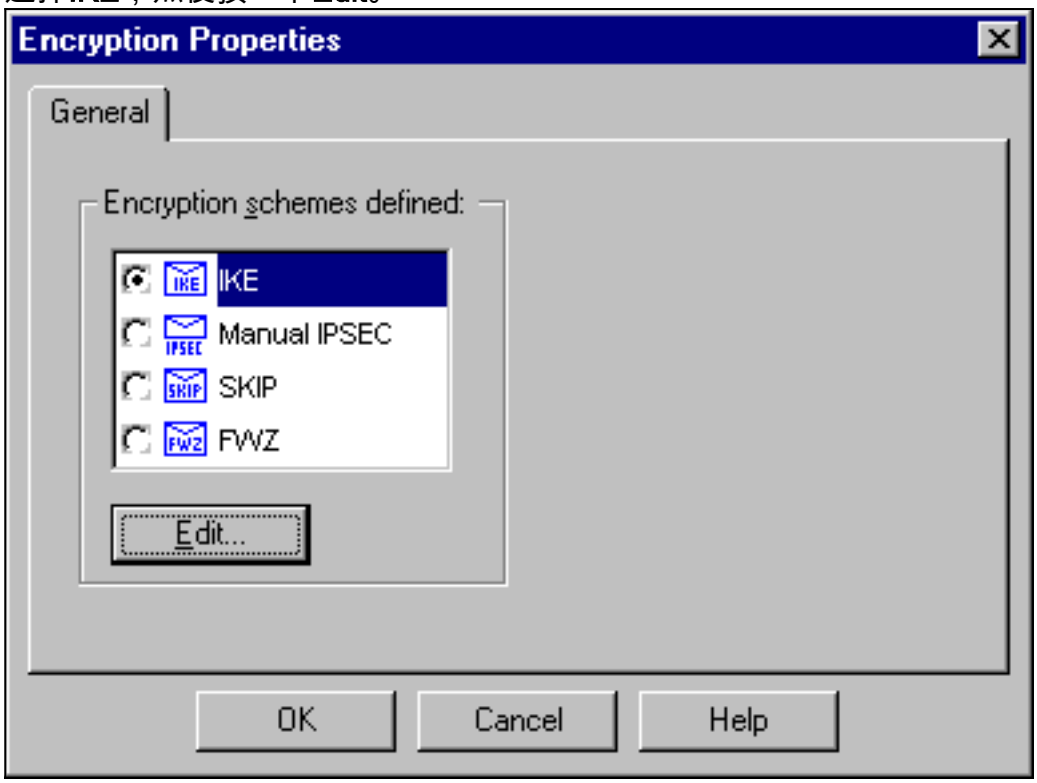
14. 在「策略編輯器」視窗中，插入一條規則，其中源和目標都為「inside_cisco」和「cpinside」（雙向）。 Set **Service=Any、Action=Encrypt**和**Track=Long**。



15. 在「操作」標題下，按一下綠色的**Encrypt**圖示，然後選擇**Edit properties**以配置加密策略。

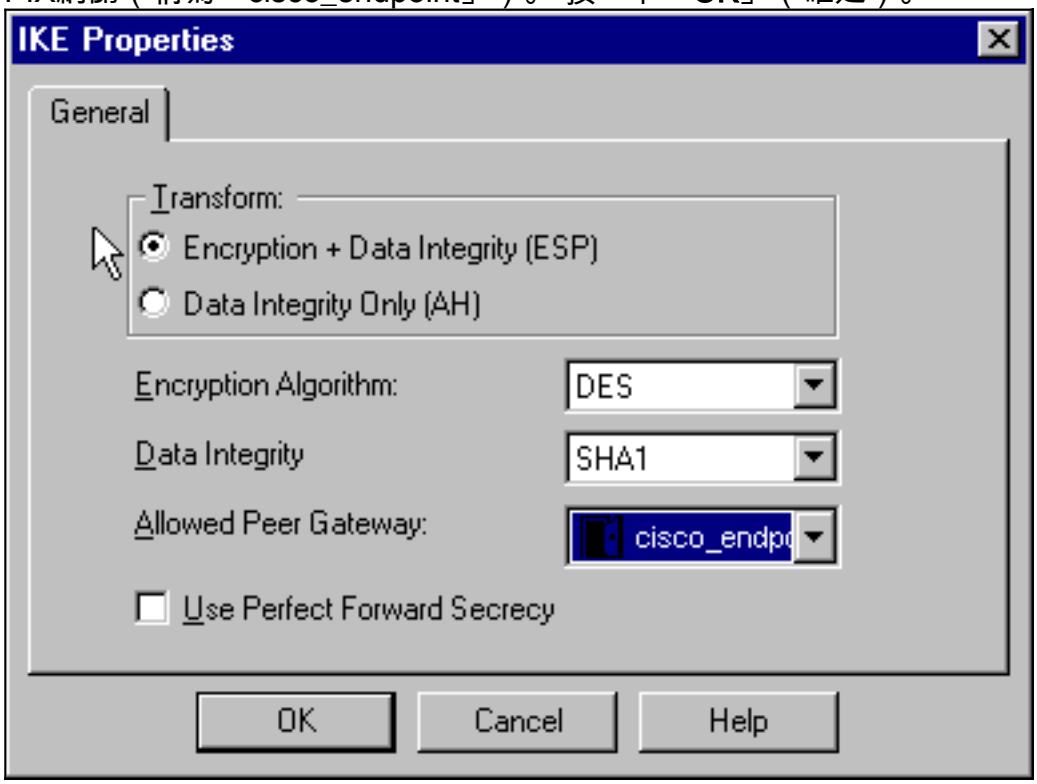


16. 選擇**IKE**，然後按一下**Edit**。



17. 在「IKE屬性」螢幕上，更改這些屬性，以便與以下命令中的PIX IPSec轉換一致：**crypto**

ipsec transform-set myset esp-des esp-sha-hmac在「轉換」下，選擇**加密+資料完整性(ESP)**。 加密演算法必須是**DES**，資料完整性必須是**SHA1**，而允許的對等網關必須是外部PIX網關（稱為「cisco_endpoint」）。 按一下「**OK**」（確定）。



18. 配置檢查點後，在Checkpoint選單中選擇**Policy > Install**以使更改生效。

debug、show和clear命令

本節提供的資訊可用於確認您的組態是否正常運作。

輸出直譯器工具(僅供註冊客戶使用)支援某些**show**命令，此工具可讓您檢視show命令輸出的分析。

發出debug指令之前，請先參閱**有關Debug指令的重要資訊**。

Cisco PIX 防火牆

- **debug crypto engine** — 顯示有關執行加密和解密的加密引擎的調試消息。
- **debug crypto isakmp** — 顯示有關IKE事件的消息。
- **debug crypto ipsec** — 顯示IPSec事件。
- **show crypto isakmp sa** — 檢視對等體上的所有當前IKE安全關聯(SA)。
- **show crypto ipsec sa** — 檢視當前安全關聯使用的設定。
- **clear crypto isakmp sa** — （從配置模式）清除所有活動的IKE連線。
- **clear crypto ipsec sa** — （從配置模式）刪除所有IPSec安全關聯。

檢查點：

由於在步驟14中所示的「策略編輯器」視窗中將「跟蹤」設定為「長」，因此「日誌檢視器」中以紅色顯示被拒絕的流量。可通過輸入以下命令獲取更詳細的調試：

```
C:\WINNT\FW1\4.1\fwstop
```

```
C:\WINNT\FW1\4.1\fw d -d
```

在另一視窗中：

```
C:\WINNT\FW1\4.1\fwstart
```

注意：這是一個Microsoft Windows NT安裝。

您可以使用以下命令清除檢查點上的SA:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

並在Are you sure中回答yes?提示。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

網路摘要

當在檢查點上的加密域中配置多個相鄰的內部網路時，裝置可以針對感興趣的流量自動彙總這些網路。如果PIX上的加密ACL未配置為匹配，則通道可能會失敗。例如，如果將10.0.0.0 /24和10.0.1.0 /24的內部網路配置為包括在隧道中，則可以將它們總結為10.0.0.0 /23。

PIX的調試輸出示例

```
cisco_endpoint# show debug
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto engine
debug fover status
        tx      Off
        rx      Off
        open    Off
        cable   Off
        txdmp   Off
        rxdmp   Off
        ifc     Off
        rxip    Off
        txip    Off
        get     Off
        put     Off
        verify  Off
        switch  Off
        fail    Off
        fmsg    Off
cisco_endpoint# term mon
cisco_endpoint#
```

```
ISAKMP (0): beginning Quick Mode exchange,
M-ID of 2112882468:7df00724IPSEC(key_engine):
 got a queue event...
IPSEC(spi_response): getting spi 0x9d71f29c(2641490588) for SA
        from  172.18.124.157 to   172.18.124.35 for prot 3
70
crypto_isakmp_process_block: src 172.18.124.157, dest 172.18.124.35
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 2112882468

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      encaps is 1
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (basic) of 28800
ISAKMP:      SA life type in kilobytes
ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
ISAKMP:      authenticator is HMAC-SHA
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request):
proposal part #1,
  (key eng. msg.) dest= 172.18.124.157, src= 172.18.124.35,
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 2112882468

ISAKMP (0): processing ID payload. message ID = 2112882468
ISAKMP (0): processing ID payload. message ID = 2112882468map_alloc_entry:
allocating entry 3
map_alloc_entry: allocating entry 4

ISAKMP (0): Creating IPSec SAs
        inbound SA from  172.18.124.157 to   172.18.124.35 (proxy
      10.32.50.0 to 192.168.1.0)
        has spi 2641490588 and conn_id 3 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytes
        outbound SA from   172.18.124.35 to  172.18.124.157 (proxy
     192.168.1.0 to 10.32.50.0)
        has spi 3955804195 and conn_id 4 and flags 4
        lifetime of 28800 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157,
    dest_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x9d71f29c(2641490588), conn_id= 3, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157,
    src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0xebc8c823(3955804195), conn_id= 4, keysize= 0, flags= 0x4
```

```
return status is IKMP_NO_ERROR2303: sa_request, (key eng. msg.)
src= 172.18.124.35, dest= 172.18.124.157,
src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy=
10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP,
transform= esp-des esp-sha-hmac , lifedur= 28800s and 4608000kb,
spi= 0x0(0), conn_id= 0, keysize= 0,
flags= 0x4004

602301: sa created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi=
0x9d71f29c(2641490588),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 3

602301: sa created, (sa) sa_dest= 172.18.124.157, sa_prot= 50, sa_spi=
0xebc8c823(3955804195),
sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4

cisco_endpoint# sho cry ips sa

interface: outside
    Crypto map tag: rtpmap, local addr. 172.18.124.35

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0 #send errors 0, #recv errors 0

     local crypto endpt.: 172.18.124.35,
     remote crypto endpt.: 172.18.124.157
     path mtu 1500, ipsec overhead 0, media mtu 1500
     current outbound spi: 0

     inbound esp sas:

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:

     outbound ah sas:

     outbound pcp sas:

   local  ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

   local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: ebc8c823

     inbound esp sas:
```

```
      spi: 0x9d71f29c(2641490588)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 3, crypto map: rtpmap
        sa timing: remaining key lifetime (k/sec): (4607999/28777)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xebc8c823(3955804195)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 4, crypto map: rtpmap
        sa timing: remaining key lifetime (k/sec): (4607999/28777)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

cisco_endpoint# sho cry is sa
        dst             src         state     pending    created
  172.18.124.157   172.18.124.35    QM_IDLE         0           2
```

相關資訊

- PIX支援頁
- PIX命令參考
- 要求建議 (RFC)
- 配置IPSec網路安全
- 配置Internet金鑰交換安全協定
- PIX 5.2:配置IPSec
- PIX 5.3:配置IPSec
- IPSec支援頁面
- 技術支援 - Cisco Systems