配置IPsec隧道 — 思科路由器到檢查點防火牆4.1

目錄

簡介
必要條件
需求
採用元件
慣例
設定
網路圖表
組態
驗證
疑難排解
疑難排解指令
網路摘要
檢查點
調試輸出示例
相關資訊

簡介

本文檔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：Cisco路由器內部的192.168.1.x專用網路和Checkpoint防火牆內部的10.32.50.x專用網路。

必要條件

需求

此示例配置假定在開始配置之前，從路由器內部和檢查點內部到Internet（此處由172.18.124.x網路表示）的流量會流動。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科3600路由器
- Cisco IOS®軟體(C3640-JO3S56I-M)，版本12.1(5)T，版本軟體(fc1)
- 檢查點防火牆4.1

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

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

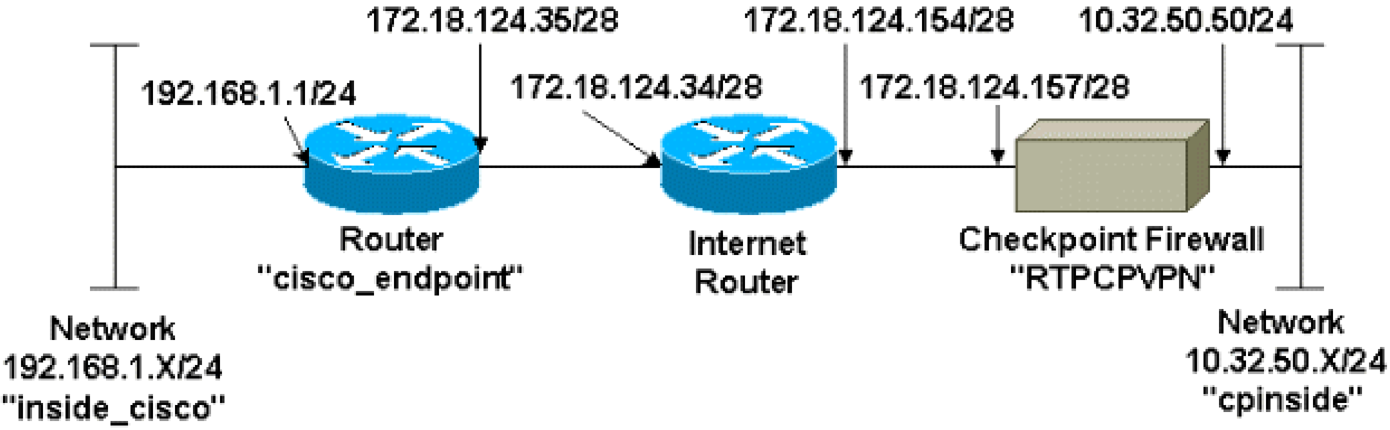
設定

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(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用以下網路設定：



組態

本檔案會使用這些設定。

- 路由器配置
- 檢查點防火牆配置

路由器配置

Cisco 3600路由器配置

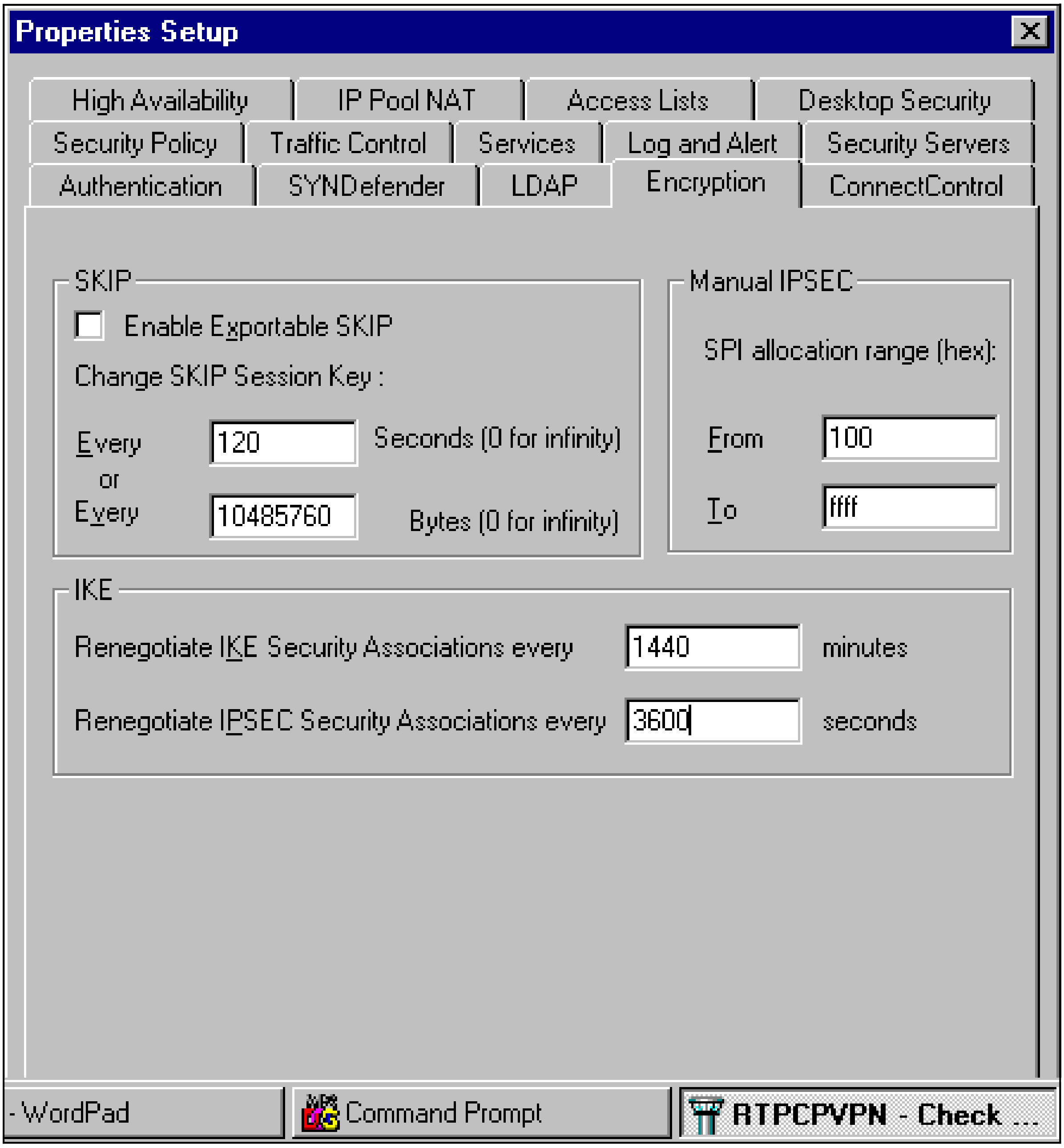
```
Current configuration : 1608 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
```

```
!
ip audit notify log
ip audit po max-events 100
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1
authentication pre-share
crypto isakmp key ciscorules address 172.18.124.157
!
!--- IPsec configuration crypto ipsec transform-set
rtpset esp-des esp-sha-hmac
!
crypto map rtp 1 ipsec-isakmp
set peer 172.18.124.157
set transform-set rtpset
match address 115
!
call rsvp-sync
cns event-service server
!
controller T1 1/0
!
controller T1 1/1
!
interface Ethernet0/0
ip address 172.18.124.35 255.255.255.240
ip nat outside
no ip mroute-cache
half-duplex
crypto map rtp
!
interface Ethernet0/1
ip address 192.168.1.1 255.255.255.0
ip nat inside
half-duplex
!
interface FastEthernet1/0
no ip address
shutdown
duplex auto
speed auto
!
ip kerberos source-interface any
ip nat pool INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 172.18.124.34
no ip http server
!
access-list 101 deny ip 192.168.1.0 0.0.0.255 10.32.50.0
0.0.0.255
access-list 101 permit ip 192.168.1.0 0.0.0.255 any
access-list 115 permit ip 192.168.1.0 0.0.0.255
10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any
route-map nonat permit 10
match ip address 101
!
dial-peer cor custom
!
line con 0
transport input none
line aux 0
line vty 0 4
login
!
end
```

檢查點防火牆配置

完成以下步驟以配置檢查點防火牆。

1. 由於IKE和IPsec的預設生存時間在供應商之間不同，因此選擇**Properties > Encryption**將檢查點生存時間設定為與Cisco預設值一致。Cisco預設IKE生存時間為86400秒（= 1440分鐘），可通過以下命令進行修改：**crypto isakmp policy #生存期編號**可配置的Cisco IKE生命週期為60-86400秒。Cisco預設IPsec生存時間為3600秒，可以通過**crypto ipsec security-association lifetime seconds #**命令對其進行修改。可配置的Cisco IPsec生命週期為120-86400秒。



SKIP

☐ Enable Exportable SKIP

Change SKIP Session Key :

Every 120 Seconds (0 for infinity)

or

Every 10485760 Bytes (0 for infinity)

Manual IPSEC

SPI allocation range (hex):

From 100

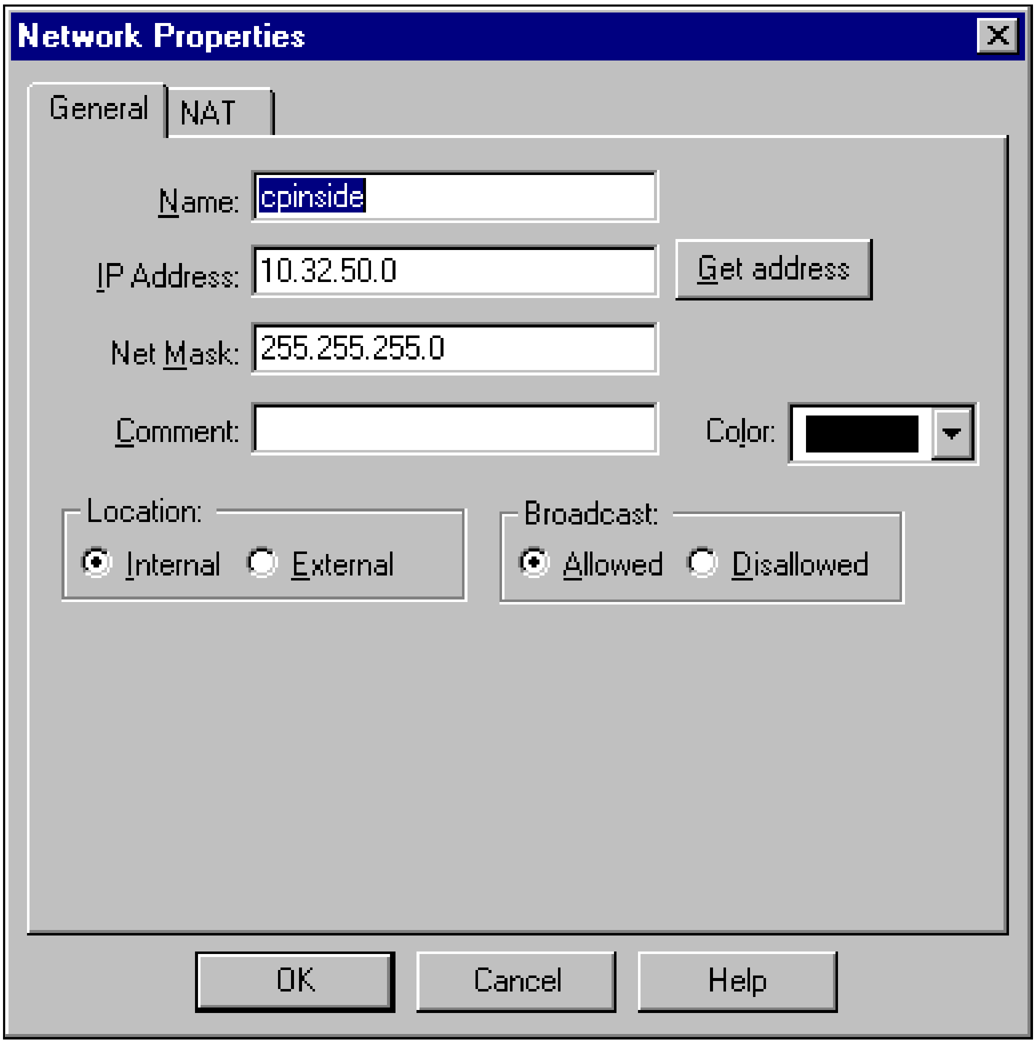
To ffff

IKE

Renegotiate IKE Security Associations every 1440 minutes

Renegotiate IPSEC Security Associations every 3600 seconds

2. 選擇**Manage > Network objects > New（或Edit）> Network**，為檢查點後面的內部網路（稱為「cpinside」）配置對象。這應與Cisco **access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255**命令中的目的地（第二個）網路相符。在Location下選擇**Internal**。



Name: cpinside

IP Address: 10.32.50.0

Net Mask: 255.255.255.0

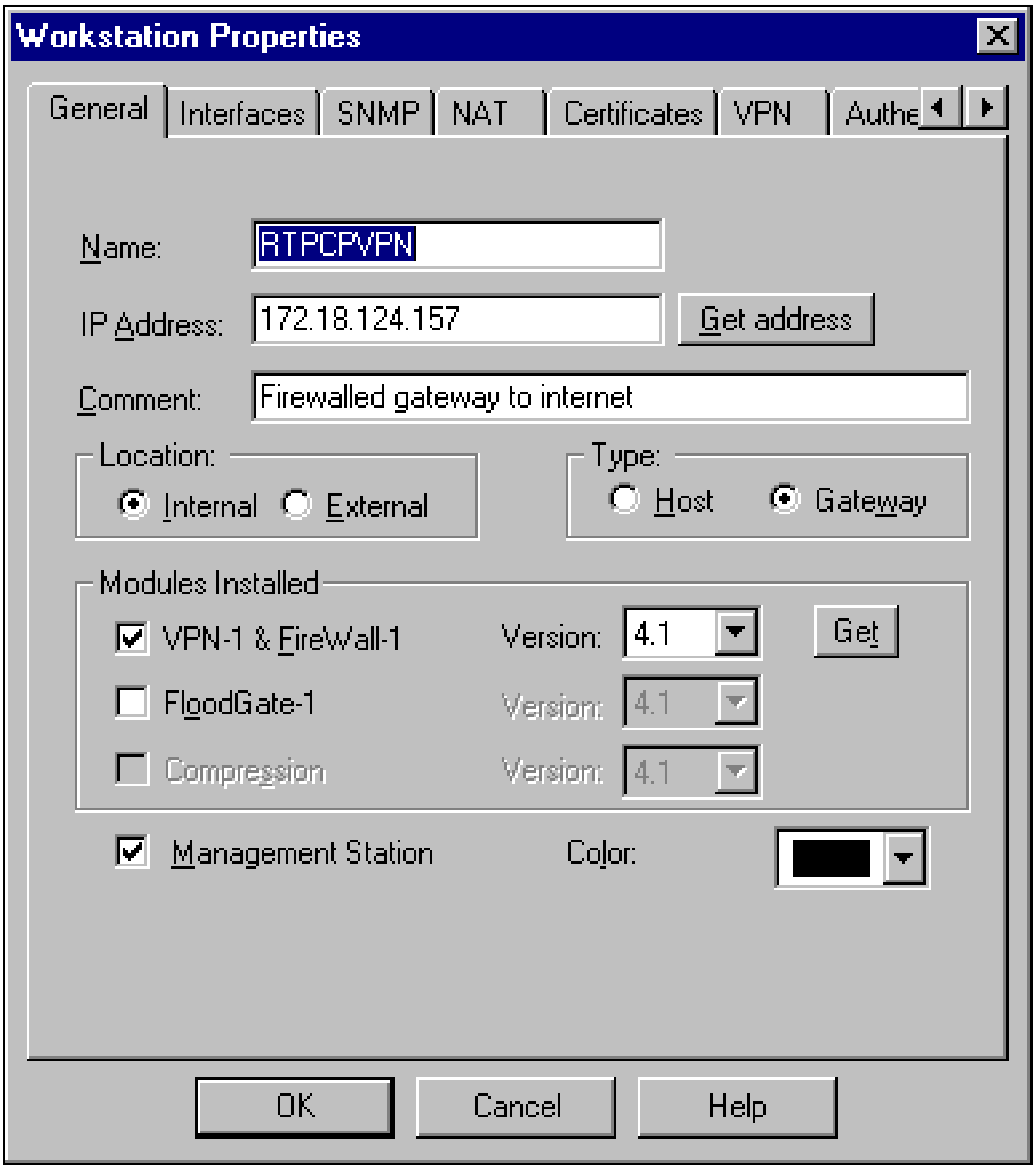
Comment:

Color: ■

Location: ● Internal ○ External

Broadcast: ● Allowed ○ Disallowed

3. 選擇**Manage > Network objects > Edit**，編輯思科路由器在**set peer 172.18.124.157**命令中指向的RTPCPVPN檢查點（網關）端點的對象。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



Name: RTPCPVPN

IP Address: 172.18.124.157

Comment: Firewalled gateway to internet

Location: ● Internal ○ External

Type: ○ Host ● Gateway

Modules Installed

☑ VPN-1 & FireWall-1 Version: 4.1

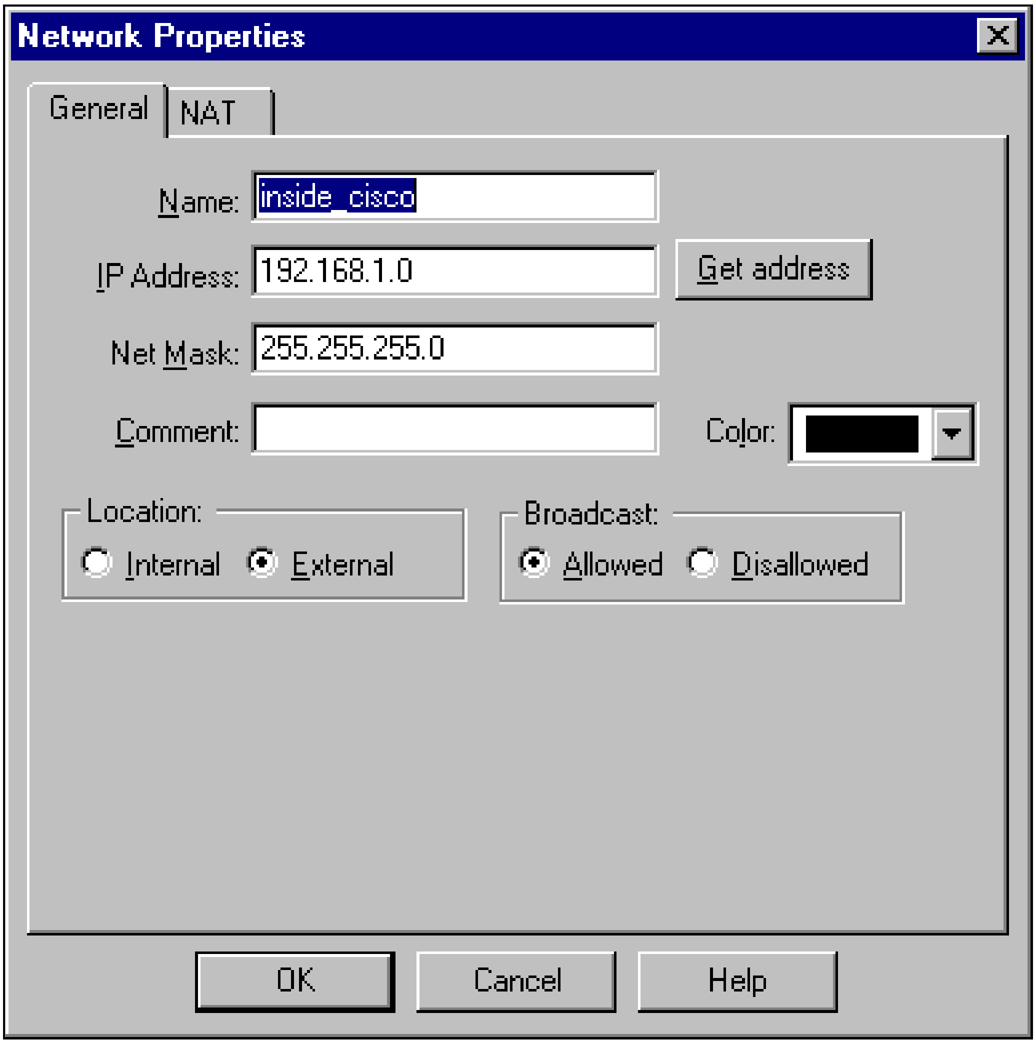
□ FloodGate-1 Version: 4.1

□ Compression Version: 4.1

☑ Management Station Color: ■

:

4. 選擇**Manage > Network objects > New > Network**，為Cisco路由器後面的外部網路（稱為「inside_cisco」）配置對象。這應與Cisco **access-list 115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255**命令中的來源（第一個）網路相符。在Location下選擇**External**。



Name: inside_cisco

IP Address: 192.168.1.0

Net Mask: 255.255.255.0

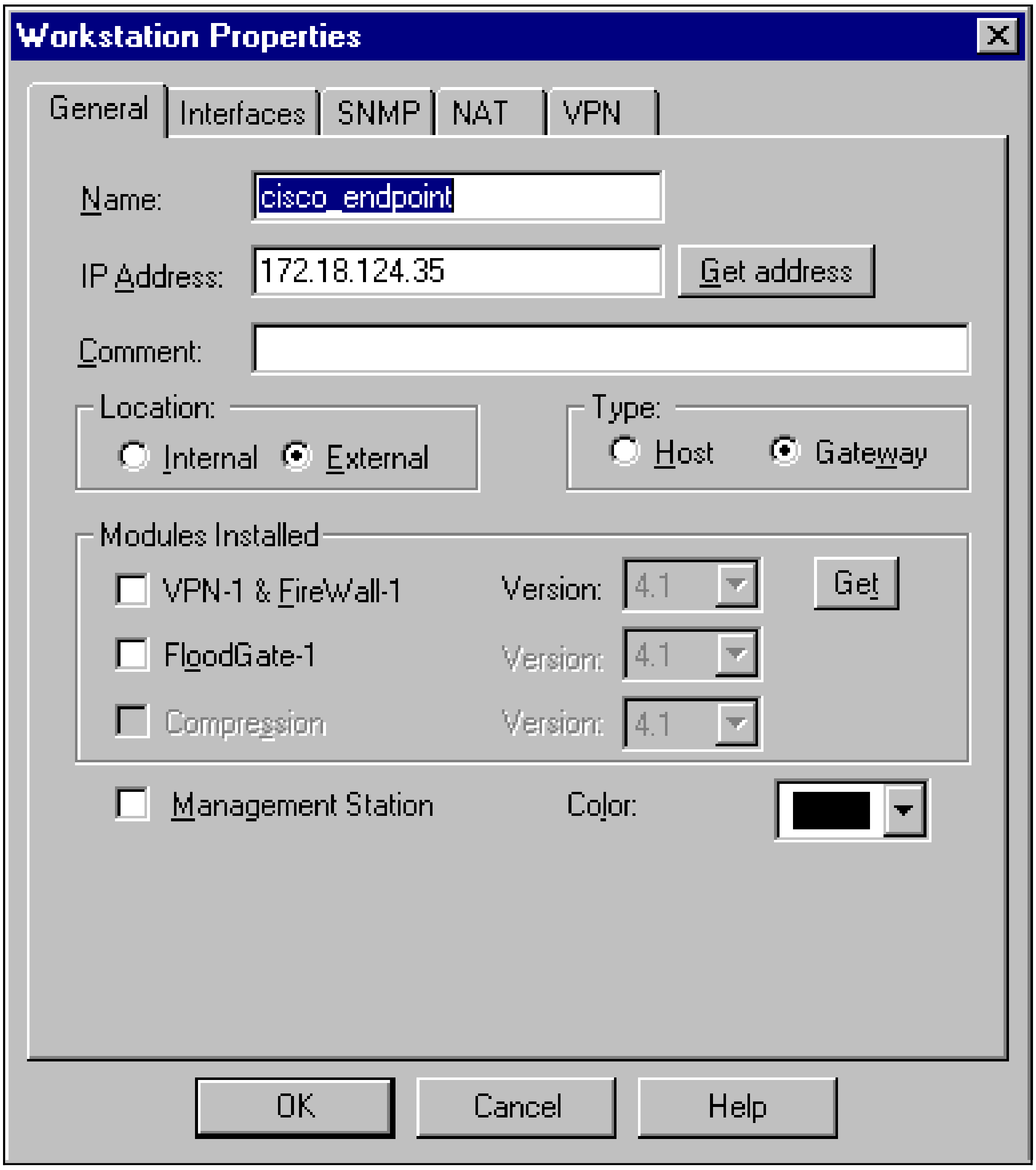
Comment:

Color: ■

Location: ○ Internal ● External

Broadcast: ● Allowed ○ Disallowed

5. 選擇**Manage > Network objects > New > Workstation**，為外部Cisco路由器網關（稱為「cisco_endpoint」）新增對象。 這是應用**crypto map *name*** 命令的Cisco介面。在Location下選擇**External**。對於Type，選擇**Gateway**。**注意**：不要選中VPN-1/FireWall-1覈取方塊。



Workstation Properties

Name: cisco_endpoint

IP Address: 172.18.124.35

Comment:

Location: ○ Internal ● External

Type: ○ Host ● Gateway

Modules Installed

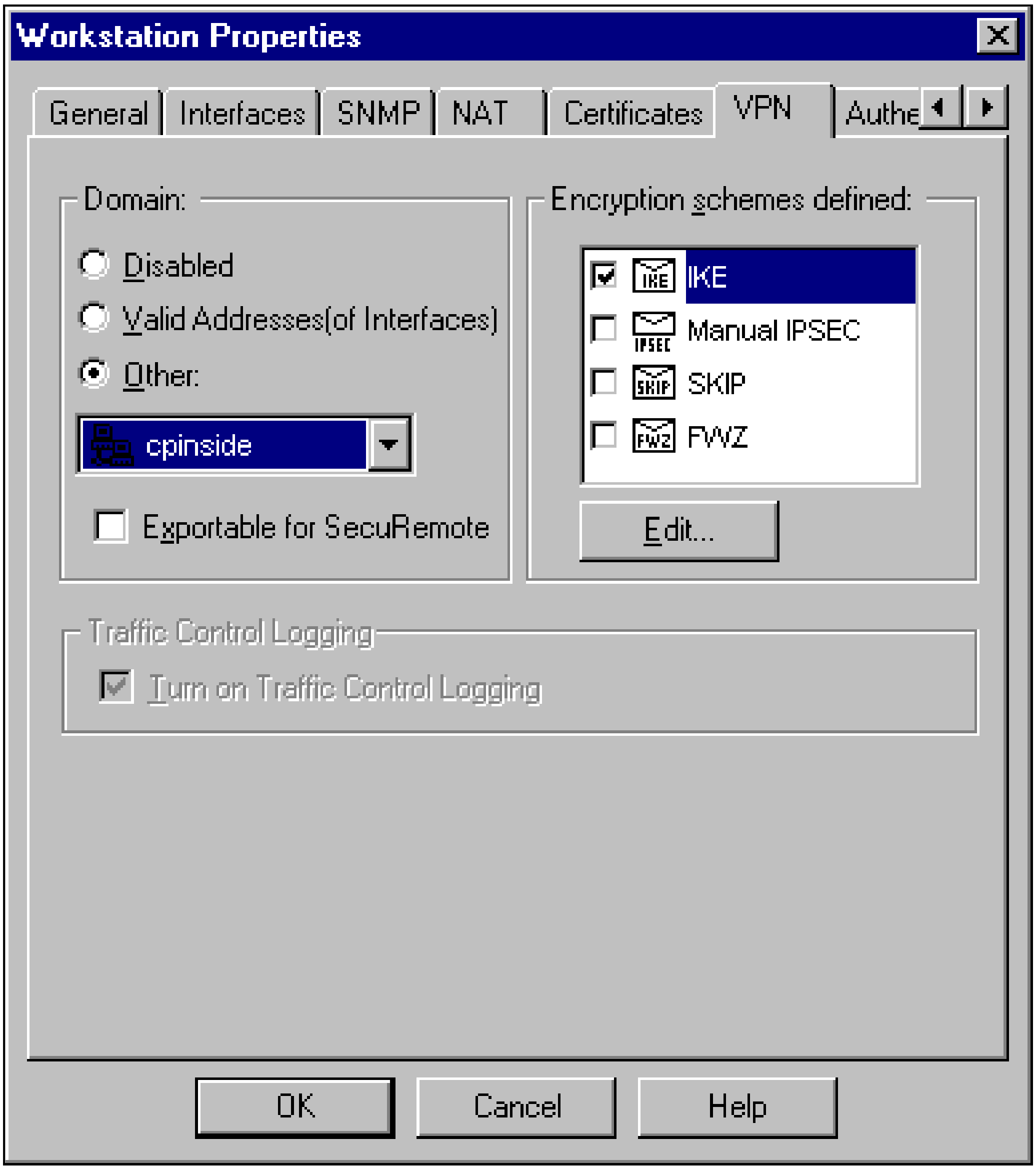
□ VPN-1 & FireWall-1 Version: 4.1

□ FloodGate-1 Version: 4.1

□ Compression Version: 4.1

□ Management Station Color: ■

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**。



Domain:

○ Disabled

○ Valid Addresses(of Interfaces)

● Other:

cpinside

□ Exportable for SecuRemote

Encryption schemes defined:

☑ IKE

□ Manual IPSEC

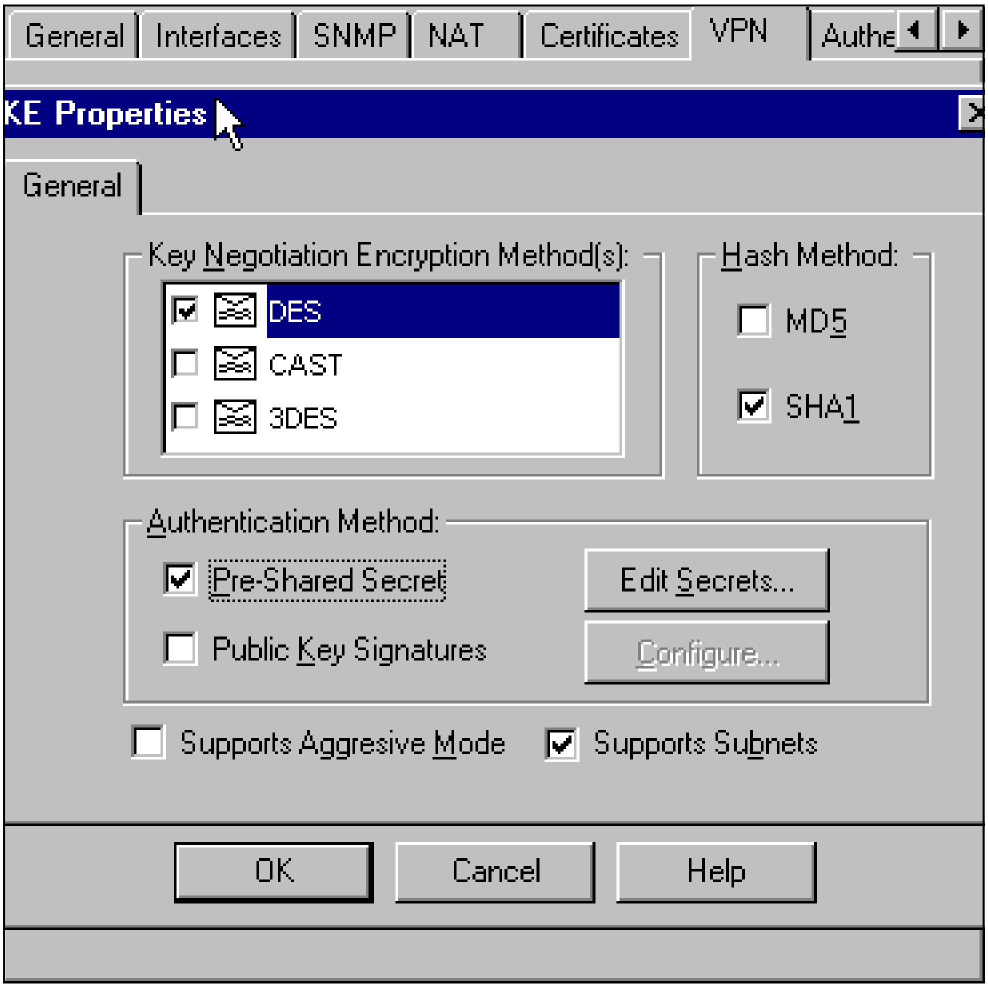
□ SKIP

□ FWZ

Traffic Control Logging

☑ Turn on Traffic Control Logging

7. 更改DES加密的IKE屬性以同意以下命令：**crypto isakmp policy #加密des注意：**DES加密是預設加密，因此在Cisco配置中不可見。
8. 將IKE屬性更改為SHA1雜湊，以同意以下命令：**crypto isakmp policy #hash sha注意：**SHA雜湊演算法是預設演算法，因此在Cisco配置中不可見。更改以下設定：取消選擇**Aggressive Mode**。選中**Supports Subnets**。在Authentication Method下檢查**Pre-Shared Secret**。這符合以下命令：**crypto isakmp policy #身份驗證預共用**



KE Properties

General

Key Negotiation Encryption Method(s):

☑ DES
☐ CAST
☐ 3DES

Hash Method:

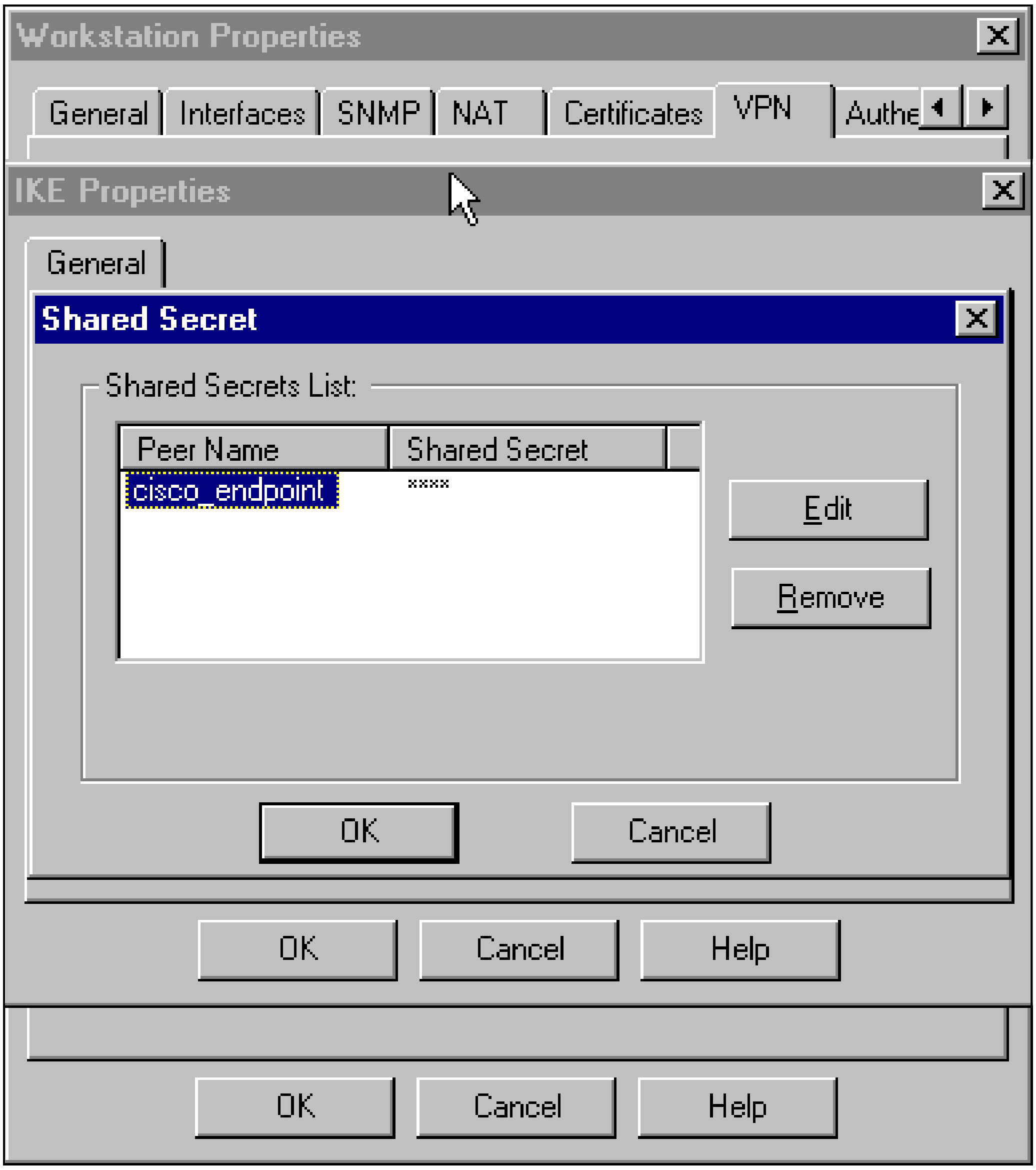
☐ MD5
☑ SHA1

Authentication Method:

☑ Pre-Shared Secret
☐ Public Key Signatures

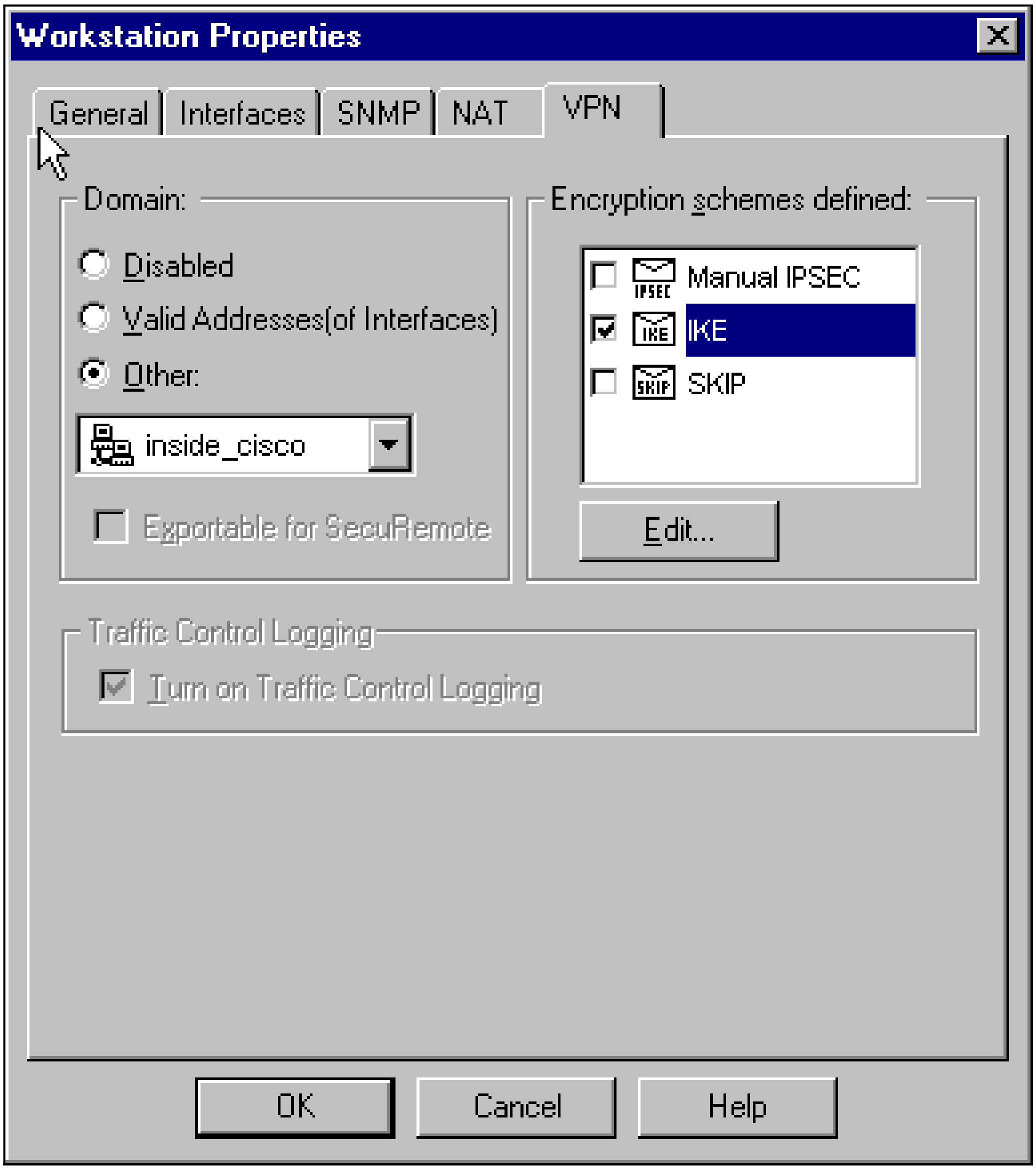
☐ Supports Aggresive Mode ☑ Supports Subnets

9. 按一下**Edit Secrets**以設定預共用金鑰，以與Cisco **crypto isakmp key** ***key*** **address** 命令一致



:

10. 選擇**Manage > Network objects > Edit**以編輯「cisco_endpoint」VPN頁籤。在域下，選擇**Other**，然後選擇思科網路內部（稱為「inside_cisco」）。 在Encryption schemes defined下，選擇**IKE**，然後按一下**Edit**。



Domain:

○ Disabled

○ Valid Addresses(of Interfaces)

● Other:

inside_cisco

□ Exportable for SecuRemote

Encryption schemes defined:

□ Manual IPSEC

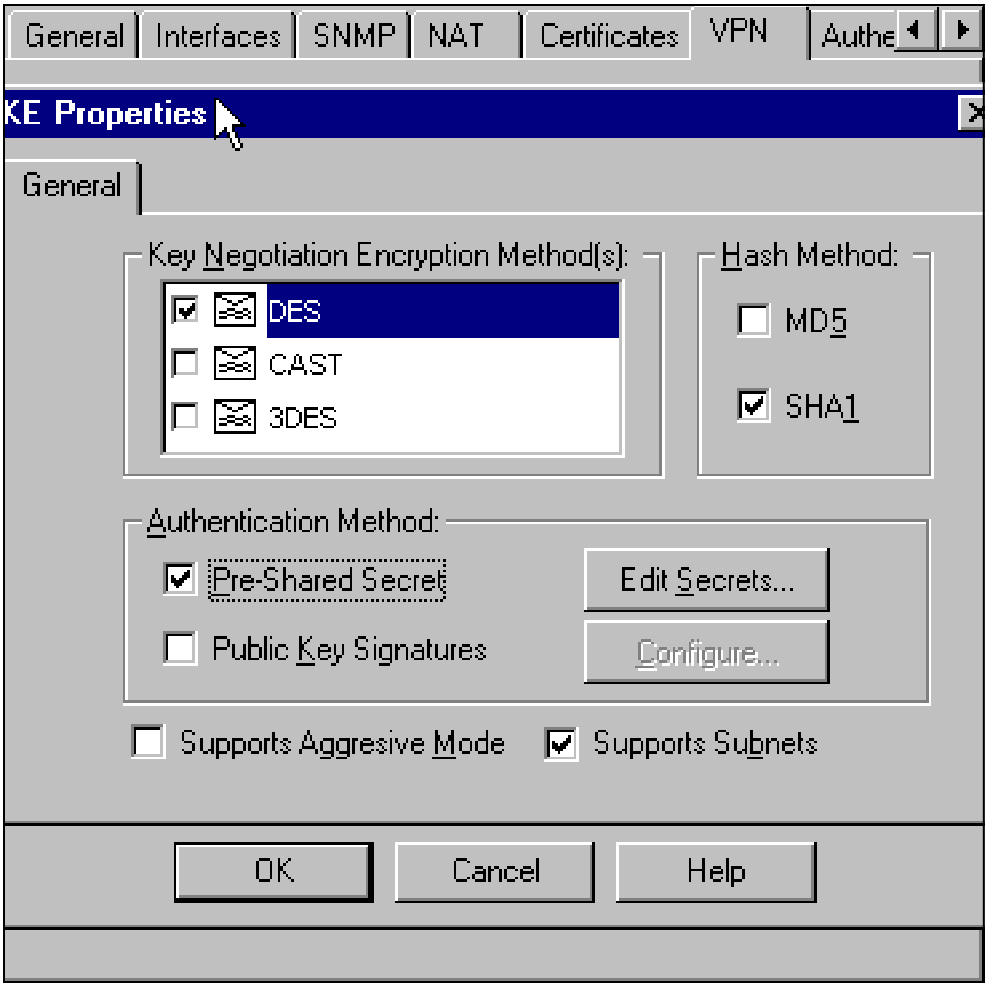
☑ IKE

□ SKIP

Traffic Control Logging

☑ Turn on Traffic Control Logging

11. 更改IKE屬性DES加密以同意以下命令：**crypto isakmp policy #加密des注意：**DES加密是預設加密，因此在Cisco配置中不可見。
12. 將IKE屬性更改為SHA1雜湊，以同意以下命令：**crypto isakmp policy #hash sha注意：**SHA雜湊演算法是預設演算法，因此在Cisco配置中不可見。更改以下設定：取消選擇**Aggressive Mode**。選中**Supports Subnets**。在Authentication Method下檢查**Pre-Shared Secret**。這符合以下命令：**crypto isakmp policy #身份驗證預共用**



Key Negotiation Encryption Method(s):

☑ DES
□ CAST
□ 3DES

Hash Method:

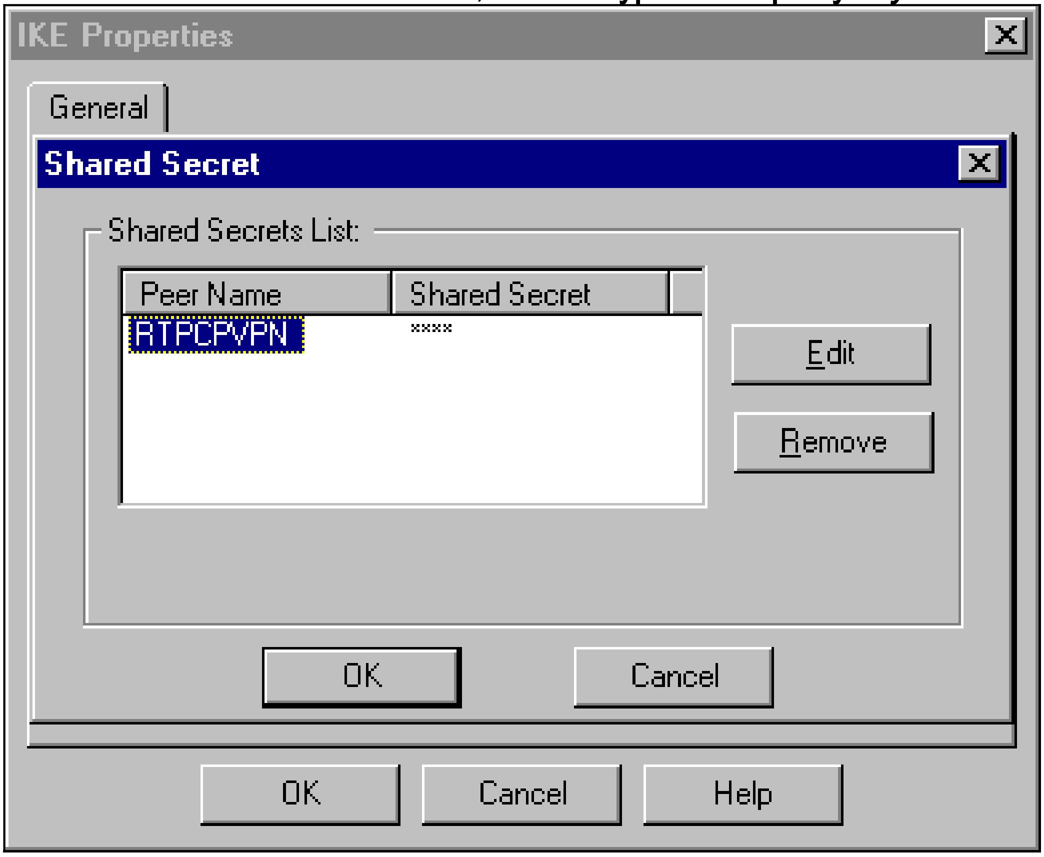
□ MD5
☑ SHA1

Authentication Method:

☑ Pre-Shared Secret
□ Public Key Signatures

□ Supports Aggresive Mode ☑ Supports Subnets

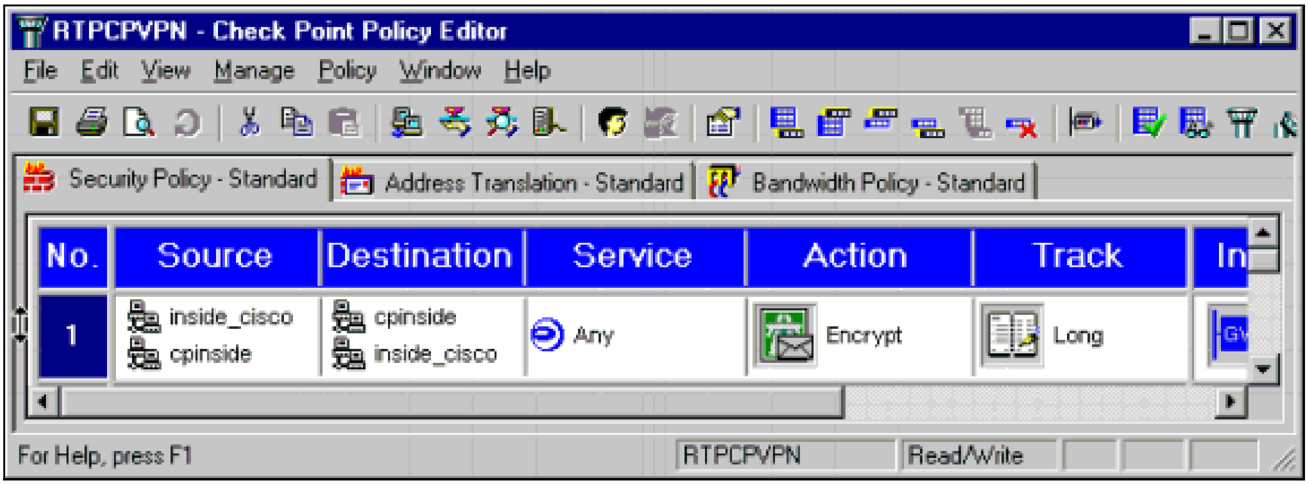
13. 按一下**Edit Secrets**以設定預共用金鑰，以便與**crypto isakmp key *key* address** Cisco命令一致。



Shared Secrets List:

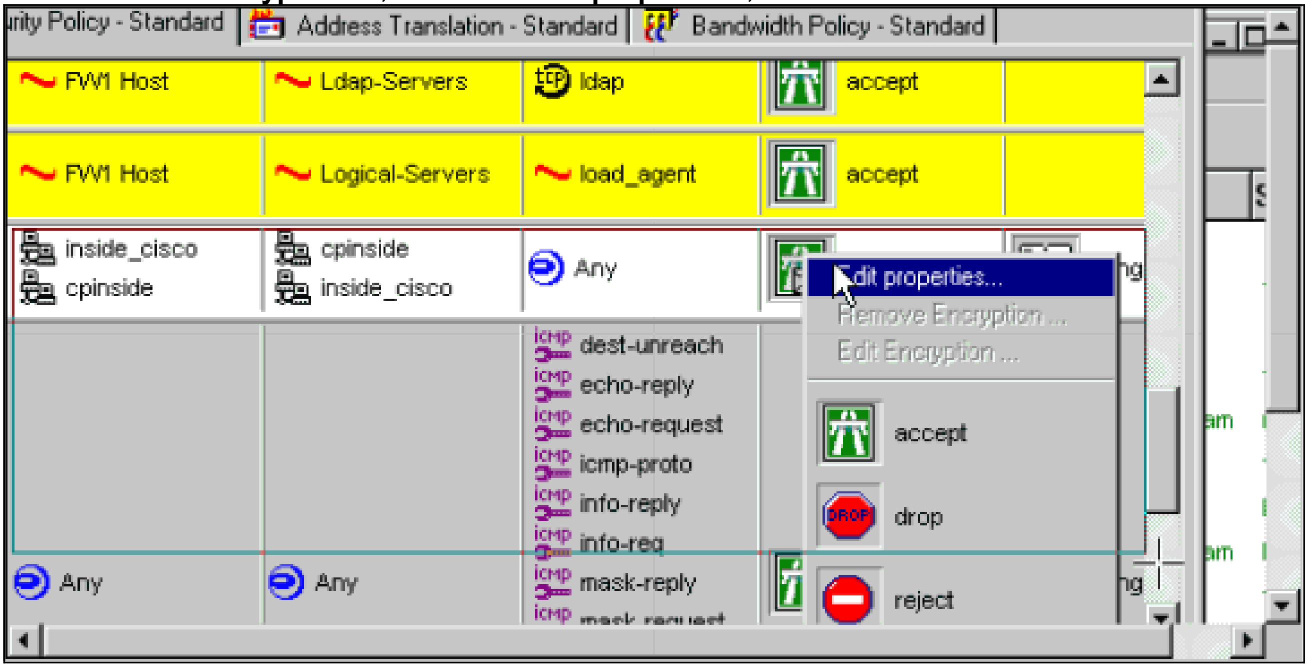
Peer Name	Shared Secret
RTPCPVPN	****

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**。


RTPCPVPN - Check Point Policy Editor
File Edit View Manage Policy Window Help
Security Policy - Standard
Address Translation - Standard
Bandwidth Policy - Standard
For Help, press F1
RTPCPVPN
Read/Write

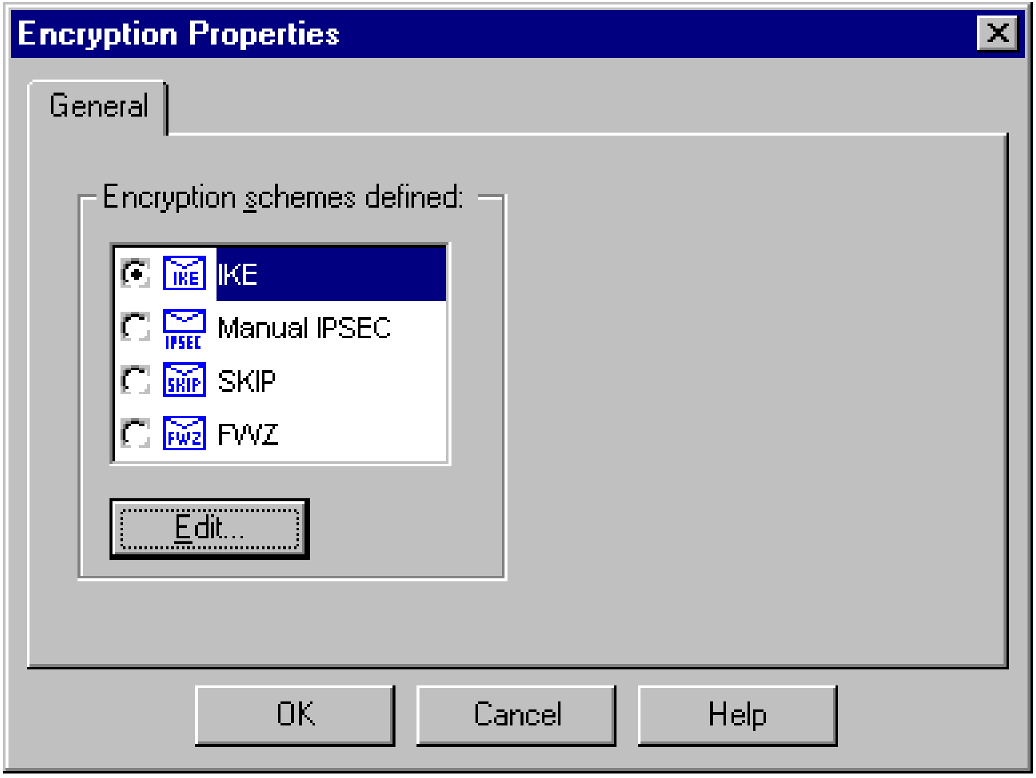
No.	Source	Destination	Service	Action	Track	In
1	inside_cisco cpinside	cpinside inside_cisco	Any	Encrypt	Long	GV

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



FW1 Host	Ldap-Servers	ldap	accept
FW1 Host	Logical-Servers	load_agent	accept
inside_cisco cpinside	cpinside inside_cisco	Any	
		dest-unreach echo-reply echo-request icmp-proto info-reply info-req mask-reply mask-request	
Any	Any		

16. 選擇**IKE**，然後按一下**Edit**。

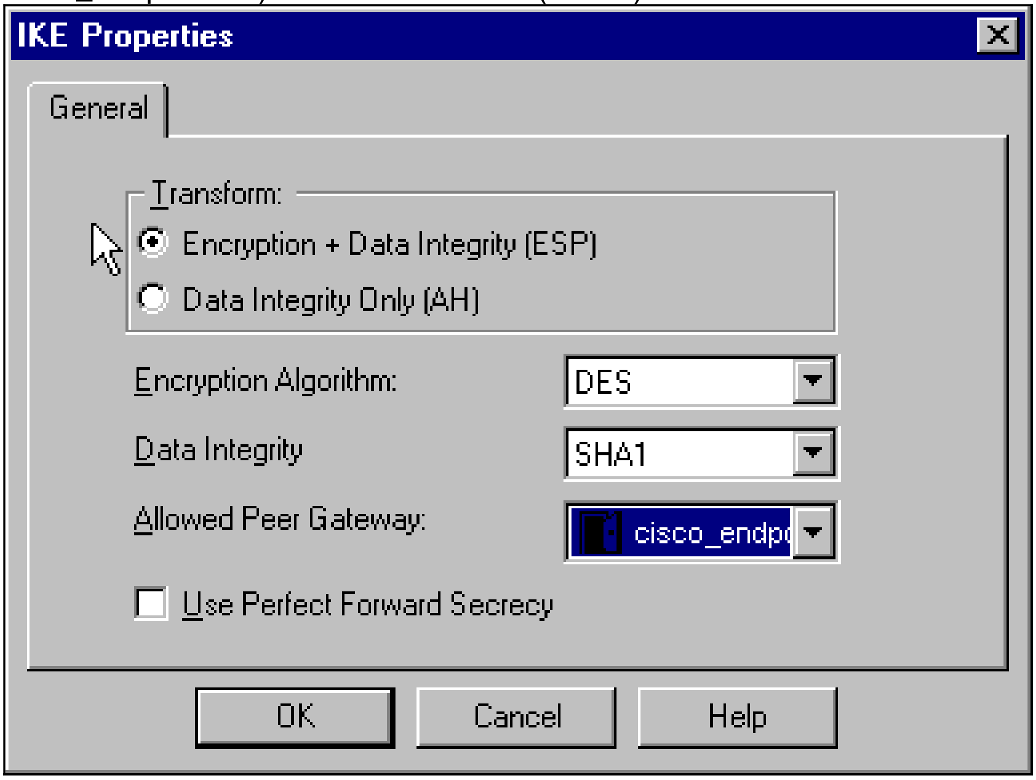


Encryption schemes defined:

● IKE
○ Manual IPSEC
○ SKIP
○ FWZ

17. 在「IKE屬性」視窗中，更改這些屬性，以與**crypto ipsec transform-set rtpset esp-des esp-**

sha-hmac 命令中的Cisco IPsec轉換一致：在「轉換」下，選擇**加密+資料完整性(ESP)**。 加密演算法應為**DES**，資料完整性應為**SHA1**，而允許的對等網關應為外部路由器網關（稱為「cisco_endpoint」）。 按一下「**OK**」（確定）。



Transform:
● Encryption + Data Integrity (ESP)
○ Data Integrity Only (AH)

Encryption Algorithm: DES

Data Integrity SHA1

Allowed Peer Gateway: cisco_endp

□ Use Perfect Forward Secrecy

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

驗證

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。

- **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SA使用的設定。

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。
- **clear crypto isakmp** — 清除所有活動的IKE連線。
- **clear crypto sa** — 清除所有IPsec SA。

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，裝置可能會根據感興趣的流量自動彙總這些網路。如果路由器未配置為匹配，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，則它們可能會總結為10.0.0.0 /23。

檢查點

由於在Policy Editor（策略編輯器）視窗中將Tracking（跟蹤）設定為Long（長），因此被拒絕的流量應在日誌檢視器中顯示為紅色。可以使用以下命令獲取更多詳細調試：

```
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。

發出以下命令以清除檢查點上的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
```

在「Are you sure？（是否確定？）」處回答**yes**提示。

調試輸出示例

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp
Crypto ISAKMP debugging is on
cisco_endpoint#debug crypto isakmp
Crypto IPSEC debugging is on
cisco_endpoint#debug crypto engine
Crypto Engine debugging is on
cisco_endpoint#
20:54:06: IPSEC(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= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1)
20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_NO_STATE
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: ISAKMP (0:1): Checking ISAKMP transform 1 against priority 1 policy
20:54:06: ISAKMP:      encryption DES-CBC
```

```
20:54:06: ISAKMP:      hash SHA
20:54:06: ISAKMP:      default group 1
20:54:06: ISAKMP:      auth pre-share
20:54:06: ISAKMP (0:1): atts are acceptable. Next payload is 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication
   using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_SA_SETUP
20:54:06: ISAKMP (0:1): processing KE payload. message ID = 0
20:54:06: CryptoEngine0: generate alg parameter
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 0
20:54:06: ISAKMP (0:1): found peer pre-shared key matching 172.18.124.157
20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1
20:54:06: ISAKMP (0:1): SKEYID state generated
20:54:06: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
20:54:06: ISAKMP (1): Total payload length: 12
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) MM_KEY_EXCH
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 0
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157
20:54:06: ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: clear dh number for conn id 1
20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I) QM_IDLE
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing SA payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): Checking IPSec proposal 1
20:54:06: ISAKMP: transform 1, ESP_DES
20:54:06: ISAKMP:   attributes in transform:
20:54:06: ISAKMP:      encaps is 1
20:54:06: ISAKMP:      SA life type in seconds
20:54:06: ISAKMP:      SA life duration (basic) of 3600
20:54:06: ISAKMP:      SA life type in kilobytes
20:54:06: ISAKMP:      SA life duration (VPI) of  0x0 0x46 0x50 0x0
20:54:06: ISAKMP:      authenticator is HMAC-SHA
20:54:06: validate proposal 0
20:54:06: ISAKMP (0:1): atts are acceptable.
20:54:06: 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
20:54:06: validate proposal request 0
20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: ISAKMP (0:1): processing ID payload. message ID = 1855173267
20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0
20:54:06: ipsec allocate flow 0
```

```
20:54:06: ISAKMP (0:1): Creating IPSec SAs
20:54:06:         inbound SA from 172.18.124.157 to 172.18.124.35
        (proxy 10.32.50.0 to 192.168.1.0)
20:54:06:         has spi 0xA29984CA and conn_id 2000 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06:         outbound SA from 172.18.124.35   to 172.18.124.157
   (proxy 192.168.1.0 to 10.32.50.0)
20:54:06:         has spi 404516441 and conn_id 2001 and flags 4
20:54:06:         lifetime of 3600 seconds
20:54:06:         lifetime of 4608000 kilobytes
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE
20:54:06: ISAKMP (0:1): deleting node 1855173267 error FALSE reason ""
20:54:06: IPSEC(key_engine): got a queue event...
20:54:06: 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= 3600s and 4608000kb,
    spi= 0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4
20:54:06: 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= 3600s and 4608000kb,
    spi= 0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.35, sa_prot= 50,
    sa_spi= 0xA29984CA(2727969994),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2000
20:54:06: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.18.124.157, sa_prot= 50,
    sa_spi= 0x181C6E59(404516441),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 2001
cisco_endpoint#sho cry ips sa

interface: Ethernet0/0
    Crypto map tag: rtp, 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): (10.32.50.0/255.255.255.0/0/0)
   current_peer: 172.18.124.157
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14
    #pkts decaps: 14, #pkts decrypt: 14, #pkts verify 14
    #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, media mtu 1500
     current outbound spi: 181C6E59

     inbound esp sas:
      spi: 0xA29984CA(2727969994)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2000, flow_id: 1, crypto map: rtp
 --More--                 sa timing: remaining key lifetime (k/sec):
    (4607998/3447)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x181C6E59(404516441)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 2001, flow_id: 2, crypto map: rtp
        sa timing: remaining key lifetime (k/sec): (4607997/3447)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:


cisco_endpoint#show crypto isakmp sa
    dst           src          state        conn-id   slot
172.18.124.157 172.18.124.35  QM_IDLE           1       0

cisco_endpoint#exit
```

相關資訊

- IPSec 協商/IKE 通訊協定
- 配置IPsec網路安全
- 配置Internet金鑰交換安全協定
- 技術支援與文件 - Cisco Systems