配置IPsec隧道 — Cisco VPN 5000集中器到Checkpoint 4.1防火牆

目錄

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。它將Cisco VPN 5000集中器(192.168.1.x)內的專用網路加入Checkpoint 4.1防火牆(10.32.50.x)內的專用網路。 在您開始此配置之前，假定從VPN集中器內部和檢查點內部到Internet（在本文檔中由172.18.124.x網路表示）的流量會流動。

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：

- Cisco VPN 5000 Concentrator
- Cisco VPN 5000 Concentrator軟體版本5.2.19.0001

- 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

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

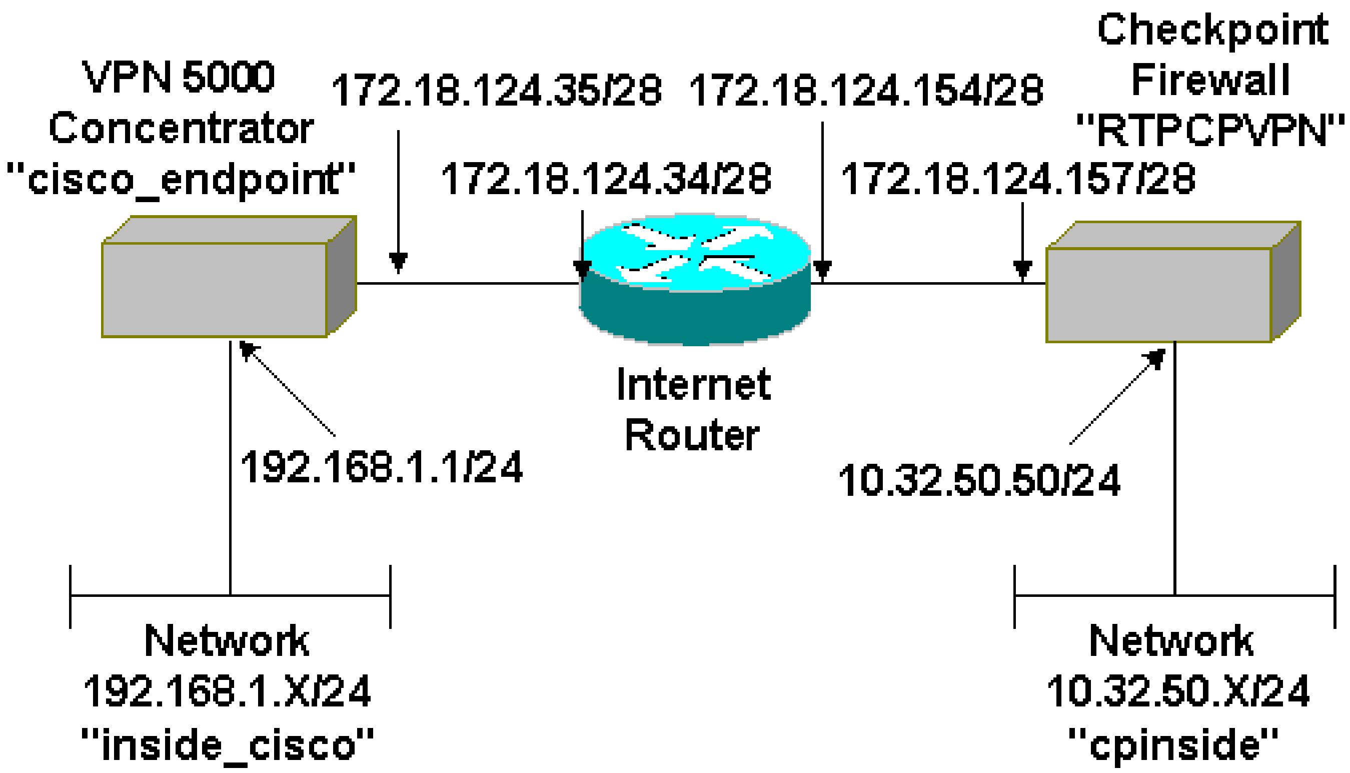
設定

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

本檔案會使用此組態。

Cisco VPN 5000 Concentrator

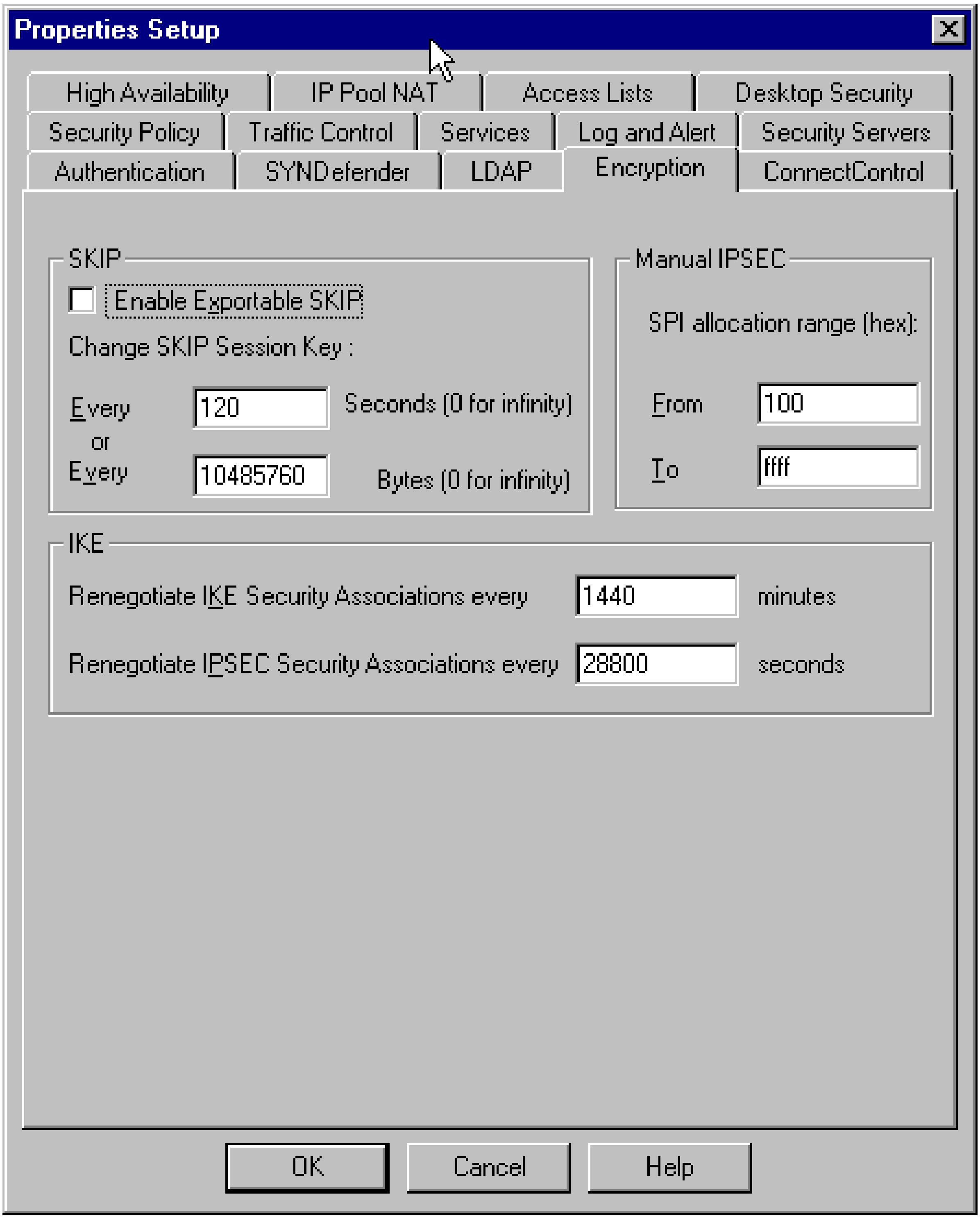
```
[ IP Ethernet 0:0 ]
Mode                         = Routed
SubnetMask                   = 255.255.255.0
IPAddress                    = 192.168.1.1
```

```
[ General ]
EthernetAddress          = 00:00:a5:e9:c8:00
DeviceType               = VPN 5002/8 Concentrator
ConfiguredOn             = Timeserver not configured
ConfiguredFrom           = Command Line, from Console
DeviceName               = "cisco_endpoint"
IPSecGateway             = 172.18.124.34

[ IKE Policy ]
Protection               = SHA_DES_G2

[ Tunnel Partner VPN 1 ]
KeyLifeSecs              = 28800
LocalAccess              = "192.168.1.0/24"
Peer                     = "10.32.50.0/24"
BindTo                   = "ethernet 1:0"
SharedKey                = "ciscorules"
KeyManage                = Auto
Transform                = esp(sha,des)
Partner                  = 172.18.124.157
Mode                     = Main

[ IP VPN 1 ]
Numbered                 = Off
Mode                     = Routed

[ IP Ethernet 1:0 ]
IPAddress                = 172.18.124.35
SubnetMask               = 255.255.255.240
Mode                     = Routed

[ IP Static ]
10.32.50.0 255.255.255.0 VPN 1 1

Configuration size is 1131 out of 65500 bytes.
```

Checkpoint 4.1防火牆

完成以下步驟以配置Checkpoint 4.1防火牆。

1. 選擇**Properties > Encryption**以設定檢查點IPsec生存時間，以與**KeyLifeSecs = 28800** VPN Concentrator命令一致。**注意：**將Checkpoint Internet Key Exchange(IKE)生存時間保留為預



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

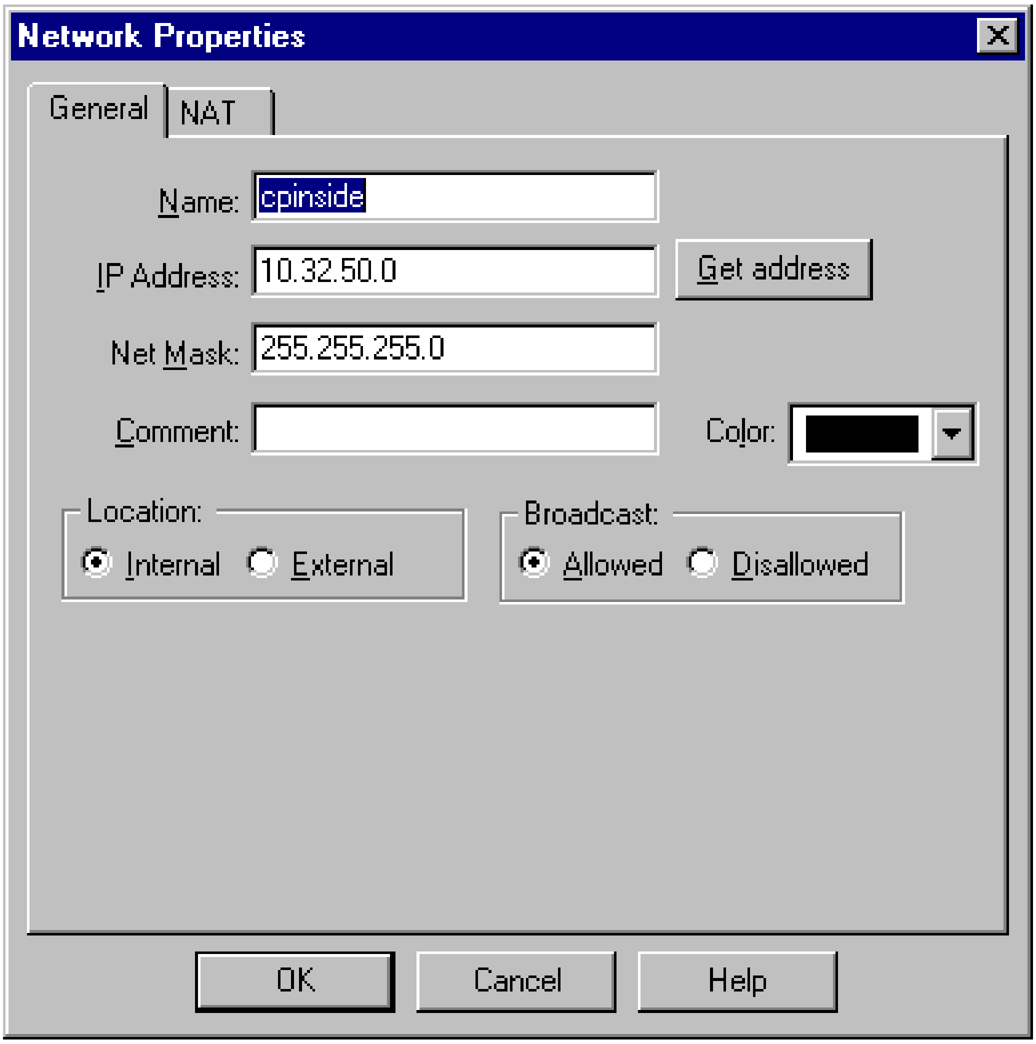
IKE

Renegotiate IKE Security Associations every 1440 minutes

Renegotiate IPSEC Security Associations every 28800 seconds

設值。

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。這應符合**Peer = "10.32.50.0/24" VPN集中器命令**。



Name: cpinside

IP Address: 10.32.50.0

Net Mask: 255.255.255.0

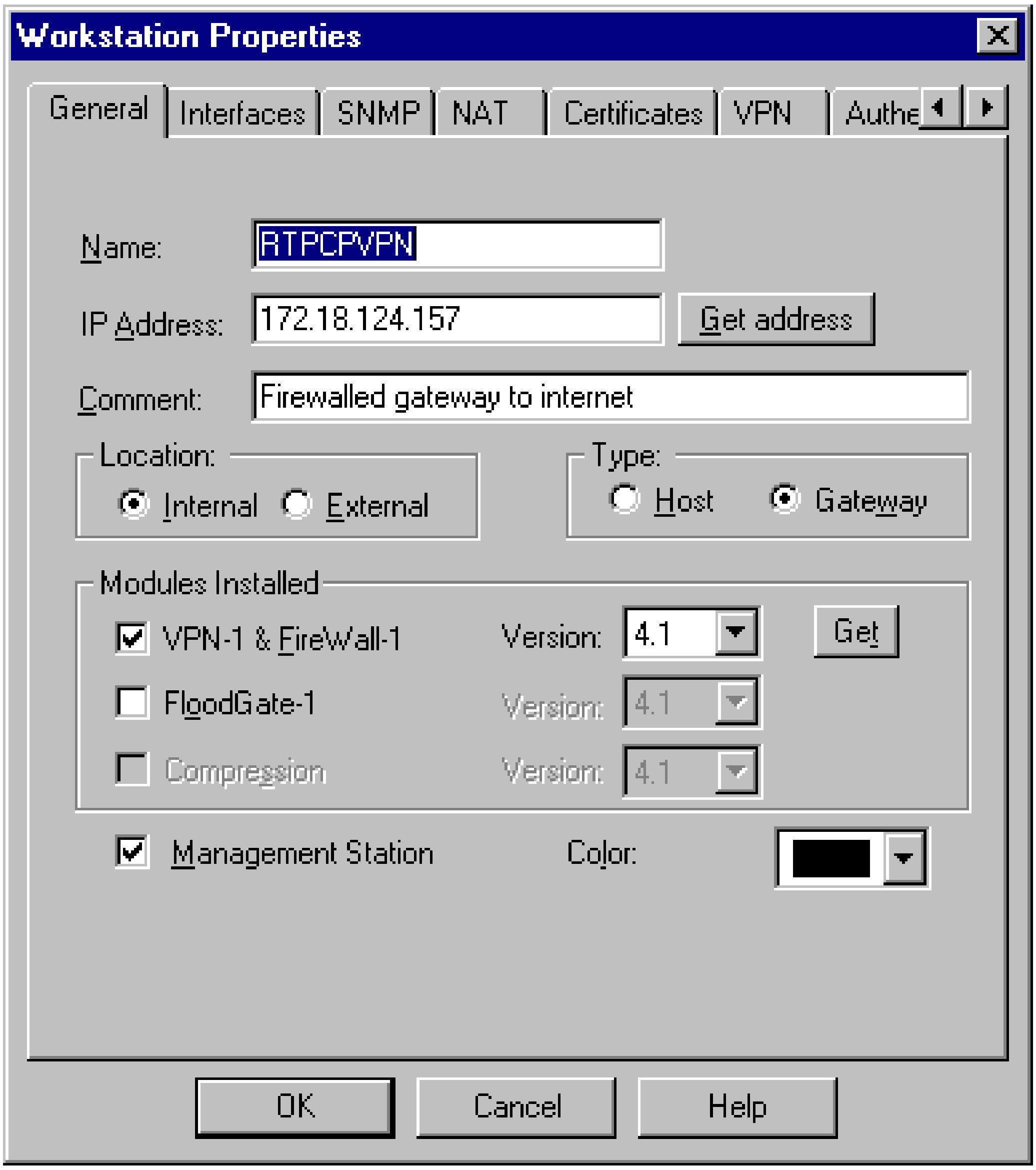
Comment:

Color:

Location: ● Internal ○ External

Broadcast: ● Allowed ○ Disallowed

3. 選擇**Manage > Network objects > Edit**以編輯VPN集中器在**Partner = <ip>命令中指向的網關（「RTPCPVPN」檢查點）端點的**對象。在Location下選擇**Internal**。選擇**Gateway**作為型別。檢查**Modules Installed**下的**VPN-1 & FireWall-1**和**Management Station**。



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

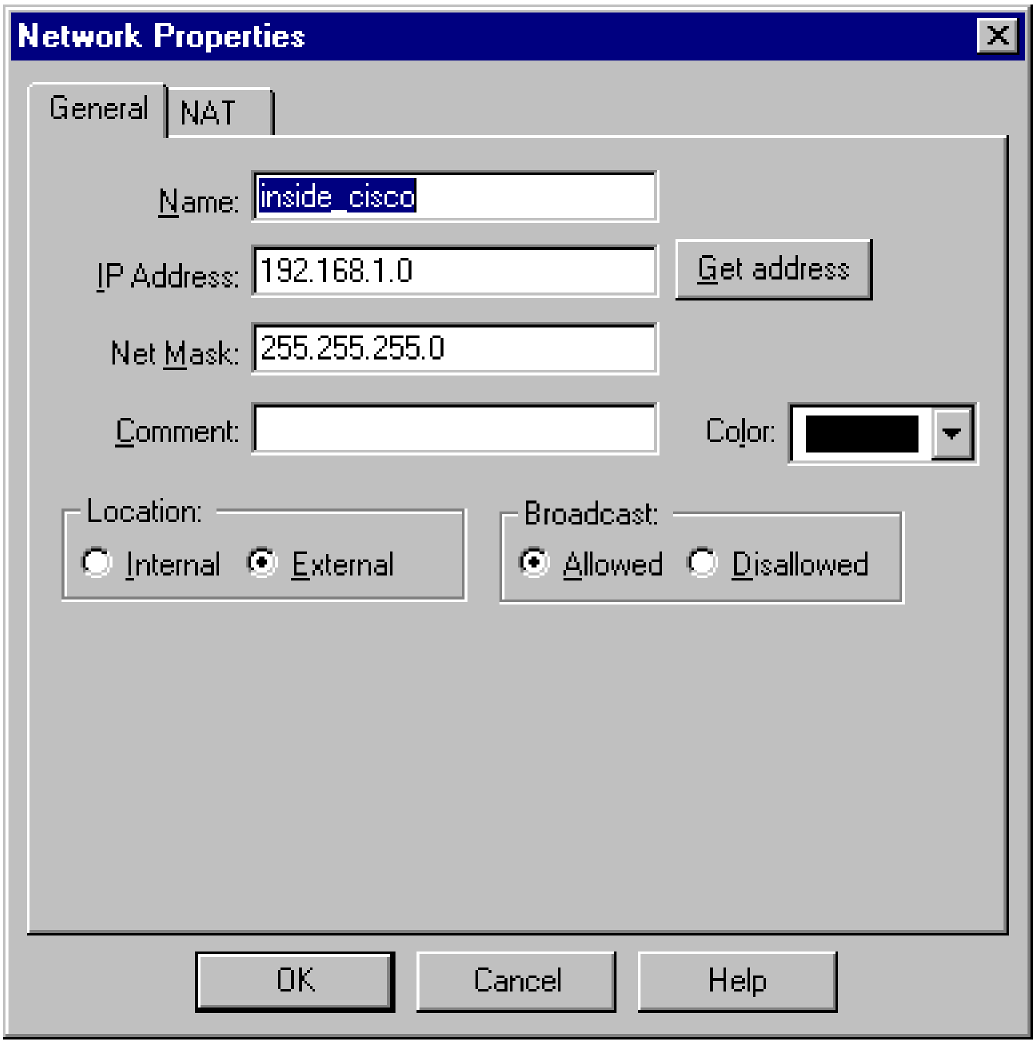
☐ FloodGate-1 Version: 4.1

☐ Compression Version: 4.1

☑ Management Station Color: ■

4. 選擇**Manage > Network objects > New（或Edit）> Network**，為VPN集中器後的外部("inside_cisco")網路配置對象。這應符合**LocalAccess = <192.168.1.0/24>** VPN

Concentrator命令。



Name: inside_cisco

IP Address: 192.168.1.0

Net Mask: 255.255.255.0

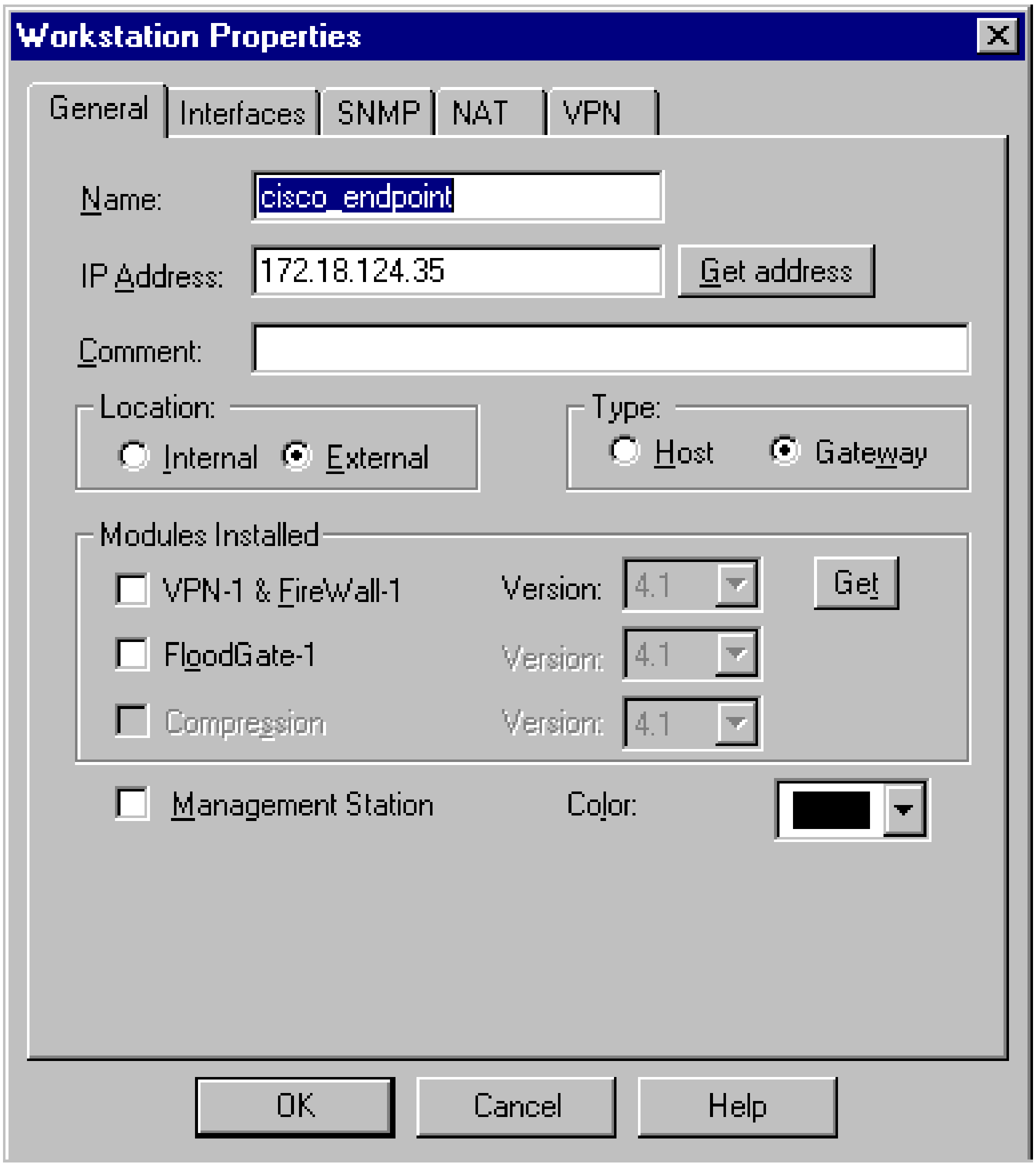
Comment:

Color: ■

Location: ○ Internal ● External

Broadcast: ● Allowed ○ Disallowed

5. 選擇**Manage > Network objects > New > Workstation**，為外部(「cisco_endpoint」)VPN集中器網關新增對象。這是連線到檢查點的VPN集中器的「outside」介面(在本文檔中，172.18.124.35是**IPAddress = <ip>命令中的IP地**址)。在Location下選擇**External**。選擇**Gateway**作為型別。**註：**請勿檢查VPN-1/FireWall-1。



Name: cisco_endpoint

IP Address: 172.18.124.35

Comment:

Location: ○ Internal ● External

Type: ○ Host ● Gateway

Modules Installed

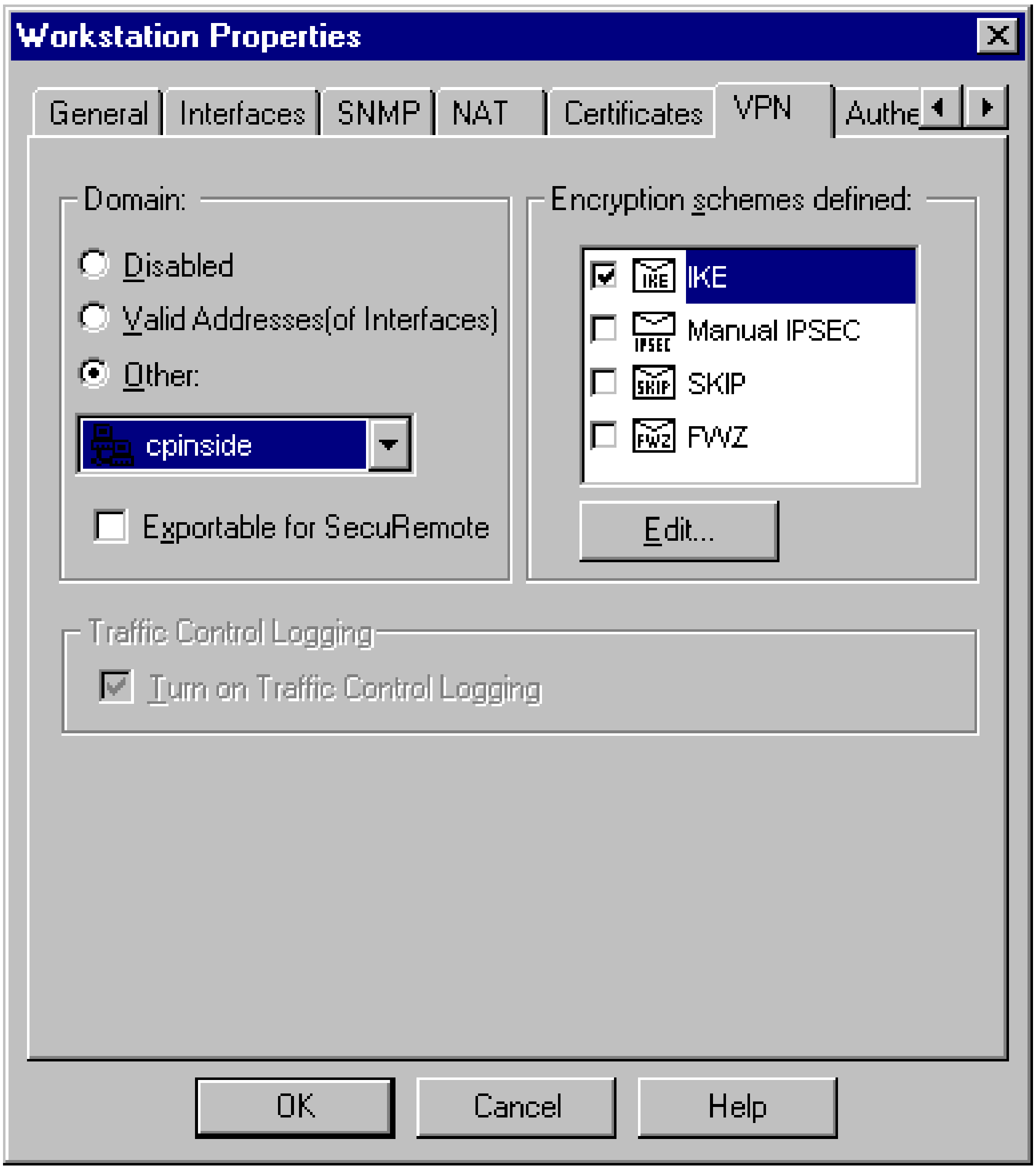
□ VPN-1 & FireWall-1 Version: 4.1

□ 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

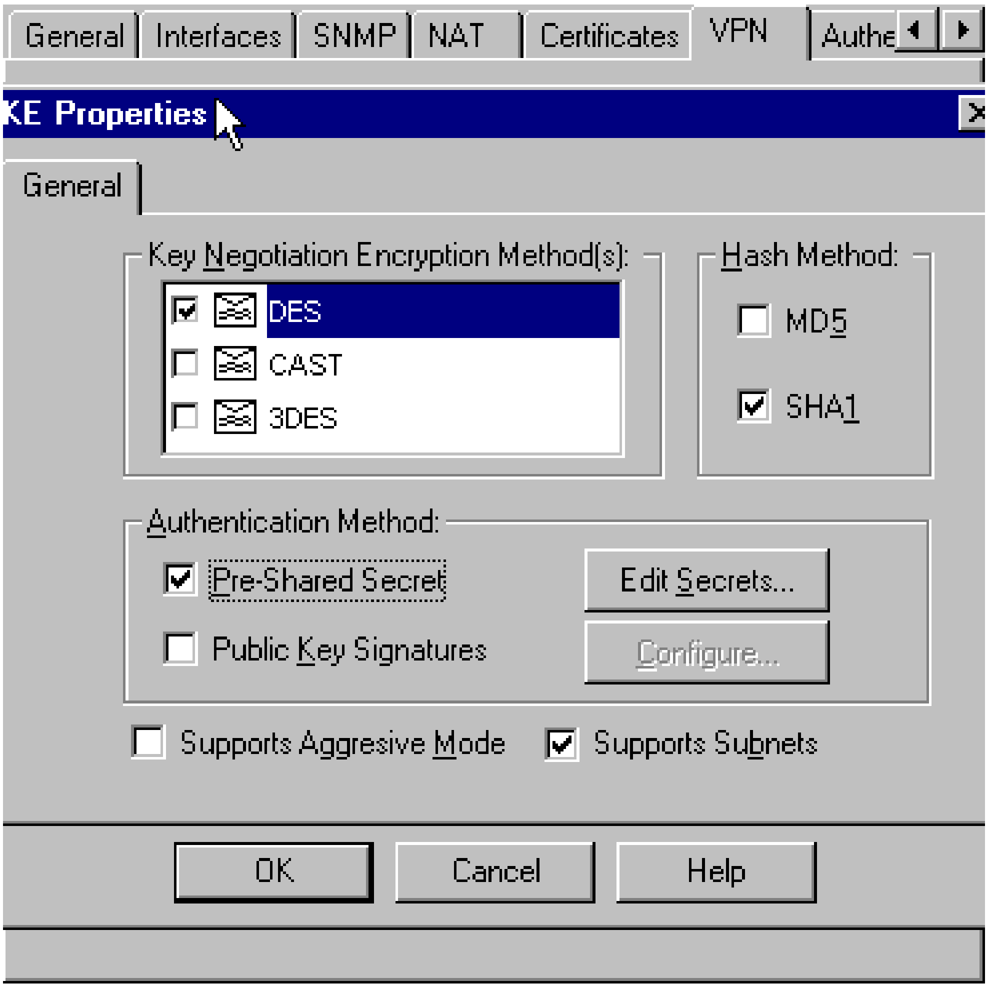
□ SKIP

□ FWZ

Traffic Control Logging

☑ Turn on Traffic Control Logging

7. 將IKE屬性更改為**DES**加密和**SHA1**雜湊，以與**SHA_DES_G2** VPN集中器命令一致。**註：**「G2」是指Diffie-Hellman組1或2。在測試中，發現檢查點接受「G2」或「G1」。更改以下設定：取消選擇**Aggressive Mode**。選中**Supports Subnets**。在Authentication Method下檢查



Key Negotiation Encryption Method(s):

☑ DES

□ CAST

□ 3DES

Hash Method:

□ MD5

☑ SHA1

Authentication Method:

☑ Pre-Shared Secret

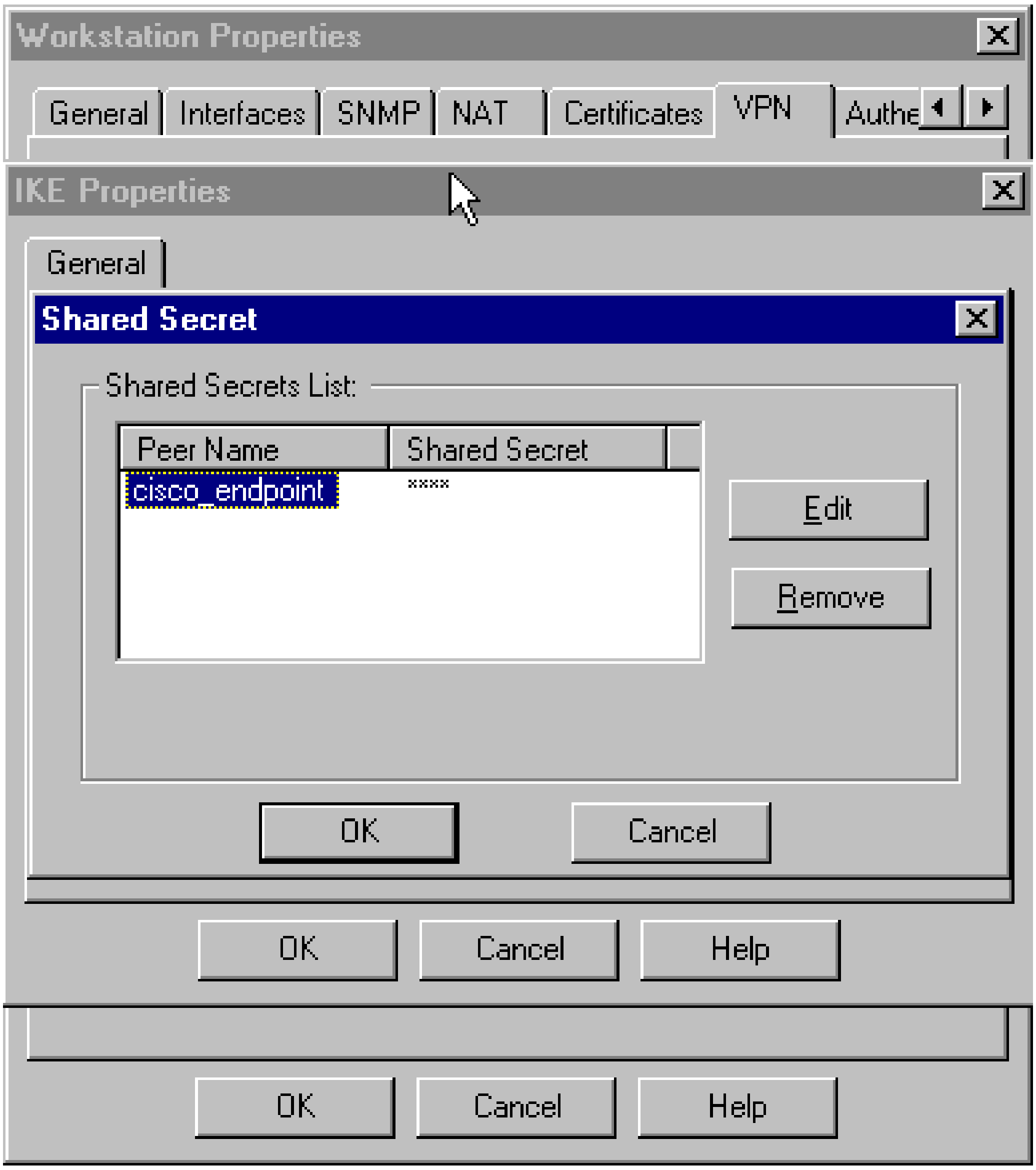
□ Public Key Signatures

□ Supports Aggresive Mode

☑ Supports Subnets

Pre-Shared Secret。

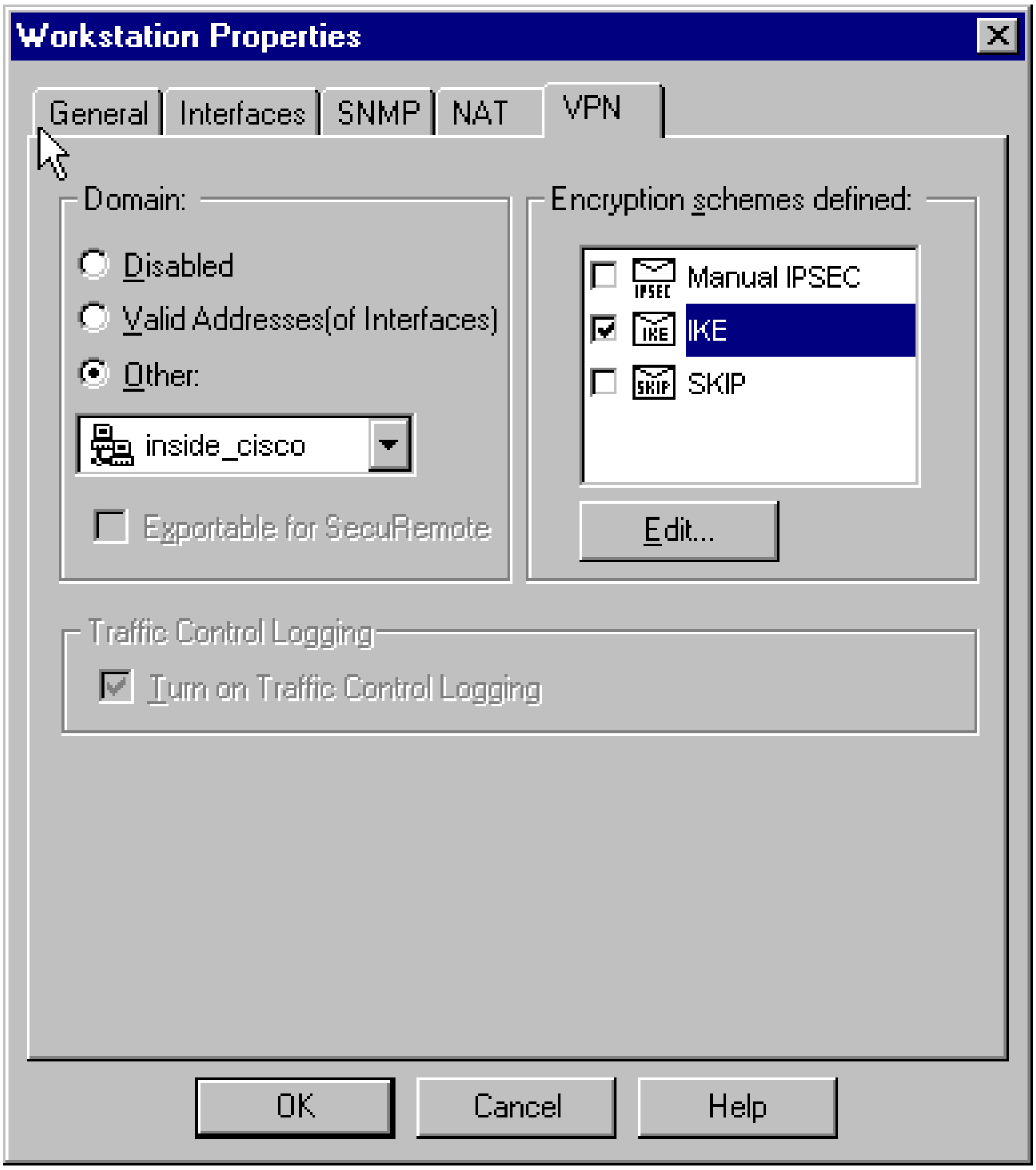
8. 按一下**Edit Secrets**以設定預共用金鑰，以便與**SharedKey = <key>** VPN Concentrator命令一



Peer Name	Shared Secret
cisco_endpoint	****

致。

9. 選擇**Manage > Network objects > Edit**以編輯「cisco_endpoint」VPN頁籤。在Domain下，選擇**Other**，然後選擇VPN集中器網路（稱為"inside_cisco"）的內部。 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

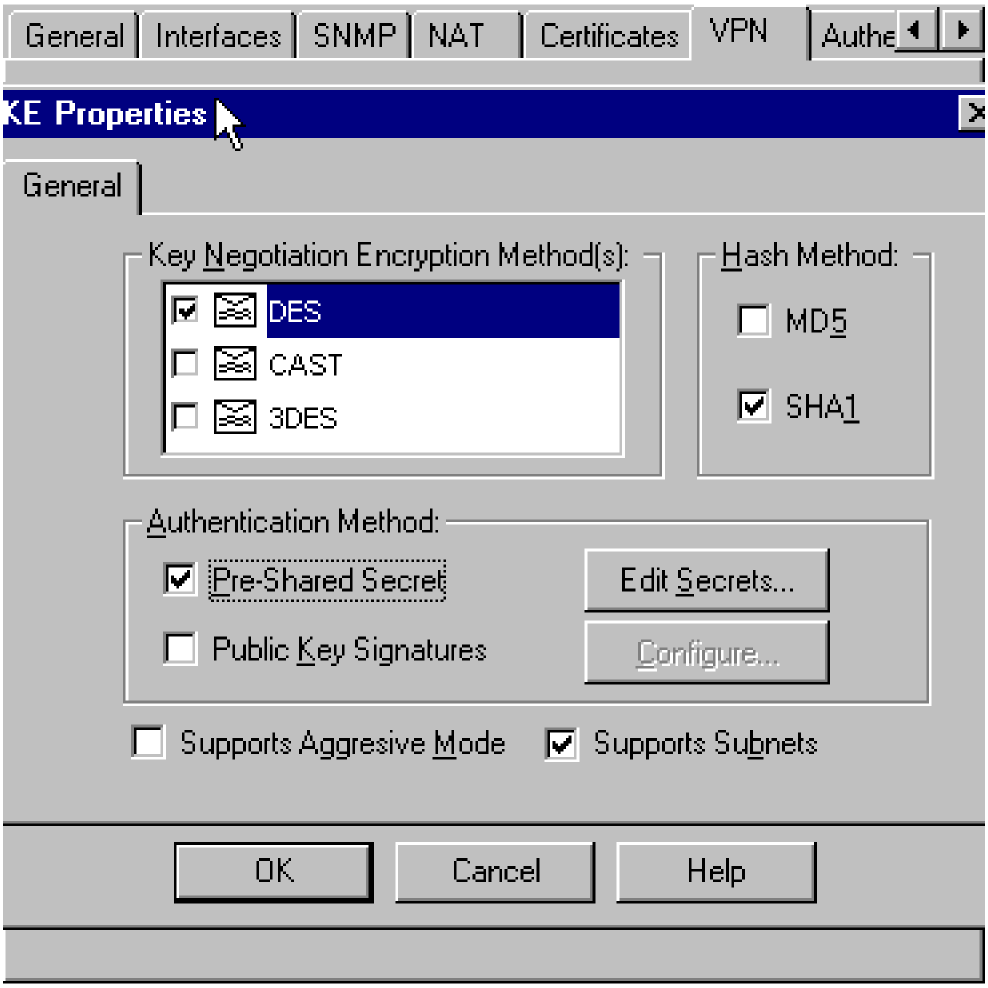
☑ IKE

□ SKIP

Traffic Control Logging

☑ Turn on Traffic Control Logging

10. 將IKE屬性更改為**DES**加密和**SHA1**雜湊，以與**SHA_DES_G2** VPN集中器命令一致。**注意：**「G2」是指Diffie-Hellman組1或2。在測試中，發現檢查點接受「G2」或「G1」。更改以下設定：取消選擇**Aggressive Mode**。選中**Supports Subnets**。在Authentication Method下檢查



Key Negotiation Encryption Method(s):
☑ DES
□ CAST
□ 3DES

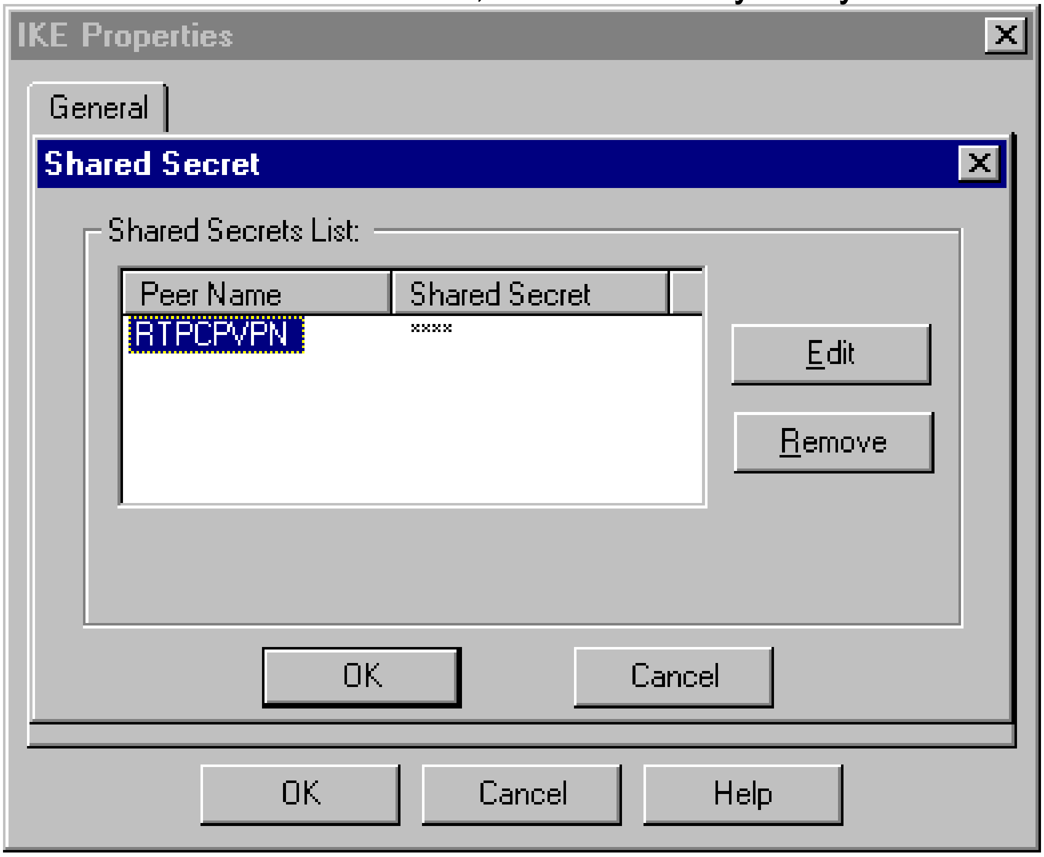
Hash Method:
□ MD5
☑ SHA1

Authentication Method:
☑ Pre-Shared Secret
□ Public Key Signatures

□ Supports Aggresive Mode ☑ Supports Subnets

Pre-Shared Secret。

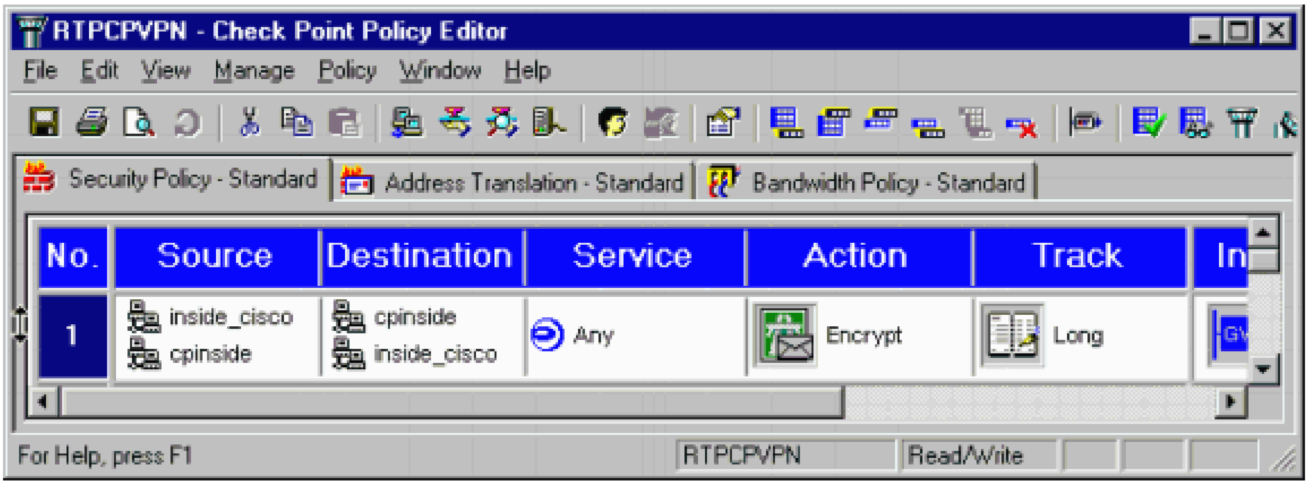
11. 按一下**Edit Secrets**以設定預共用金鑰，以便與**SharedKey = <key>** VPN Concentrator命令一致。



Shared Secrets List:

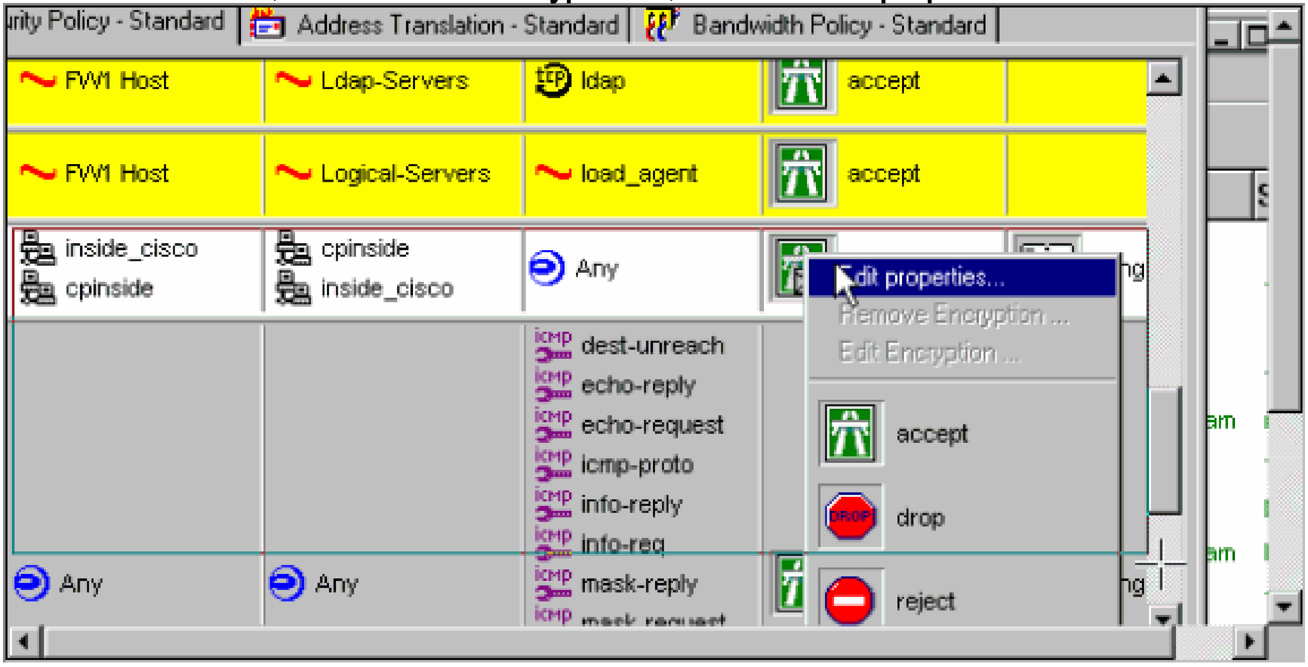
Peer Name	Shared Secret
RTPCPVPN	****

12. 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

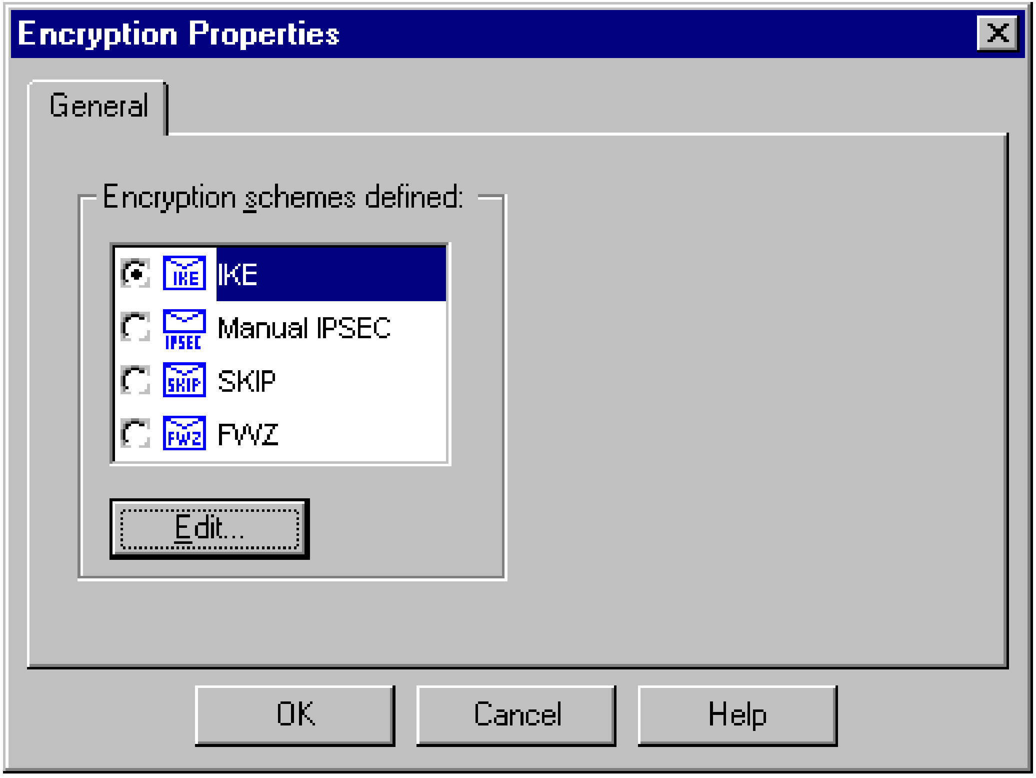
No.	Source	Destination	Service	Action	Track	In
1	inside_cisco cpinside	cpinside inside_cisco	Any	Encrypt	Long	GW

13. 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。



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

14. 選擇**IKE**，然後按一下**Edit**。

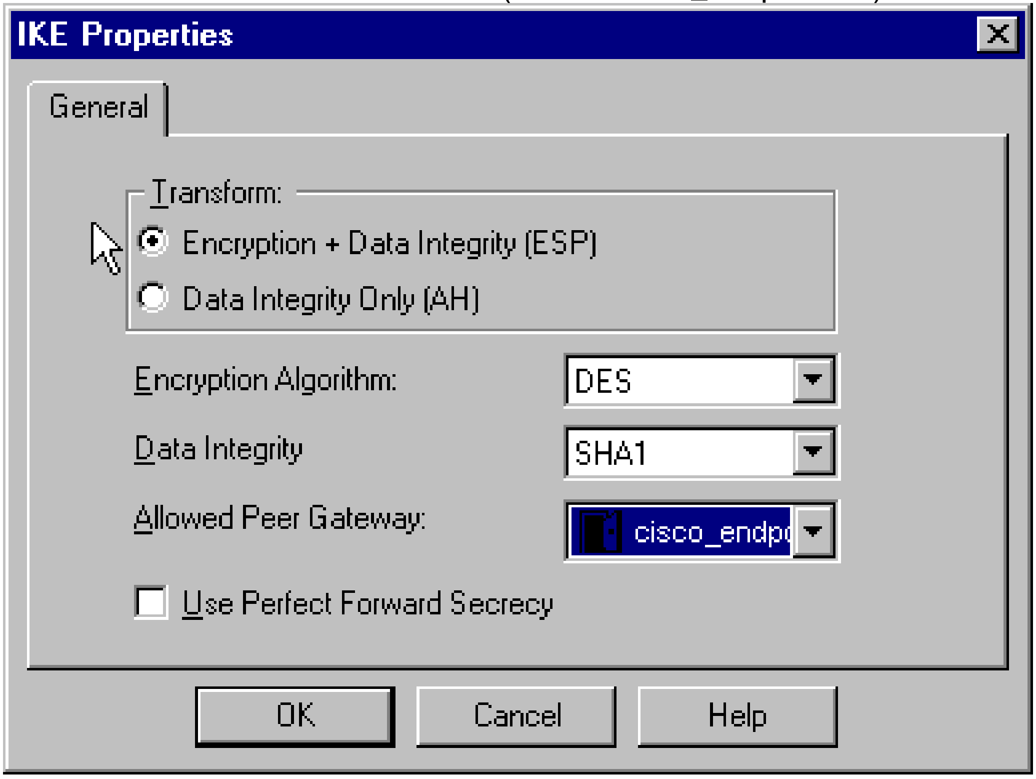


Encryption schemes defined:

● IKE
○ Manual IPSEC
○ SKIP
○ FWZ

15. 在「IKE屬性」視窗中，更改這些屬性以與**Transform = esp(sha，des)**VPN Concentrator命

令一致。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VPN集中器網關（稱為「cisco_endpoint」）。 按一下


IKE Properties

General

Transform:

● Encryption + Data Integrity (ESP)

○ Data Integrity Only (AH)

Encryption Algorithm: DES

Data Integrity: SHA1

Allowed Peer Gateway: cisco_endpc

□ Use Perfect Forward Secrecy

「OK」（確定）。

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

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

VPN 5000 Concentrator故障排除命令

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。

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

- **vpn trace dump all** — 顯示有關所有匹配的VPN連線的資訊，包括有關時間、VPN編號、對等體的實際IP地址、已運行哪些指令碼的資訊，以及在發生錯誤的情況下顯示發生錯誤的軟體代碼的常式和行號。
- **show system log buffer** — 顯示內部日誌緩衝區的內容。
- **show vpn statistics** — 顯示使用者、合作夥伴的此資訊以及兩者的總數。(對於模組化型號，顯示器包括每個模組插槽的部分。請參閱調試輸出示例部分。)(Current Active) — 當前活動連線。`Negot` — 當前協商連線。`High Water` — 自上次重新啟動以來最大併發活動連線數。`Running Total` — 自上次重新啟動後成功的連線總數。`Tunnel OK` — 沒有錯誤的隧道數。`Tunnel Starts` — 隧道啟動次數。`Tunnel Error` — 出錯的隧道數。
- **show vpn statistics verbose** — 顯示ISAKMP協商統計資訊以及更多活動連線統計資訊。

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VPN集中器未配置為匹配，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，則它們可能會總結為10.0.0.0 /23。

檢查點4.1防火牆調試

這是Microsoft Windows NT安裝。由於在策略編輯器視窗中將跟蹤設定為Long(如步驟12中所示)，因此被拒絕的流量應在日誌檢視器中顯示為紅色。可通過以下方式獲取更詳細的調試：

```
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
```

發出以下命令以清除檢查點上的安全關聯(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？）提示。

調試輸出示例

```
cisco_endpoint#vpn trac dump all
         4 seconds -- stepmngr trace enabled --
   new script: lan-lan primary initiator for <no id> (start)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing l2lp_init, (0 @ 0)
         38 seconds doing l2lp_do_negotiation, (0 @ 0)
   new script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_init, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_2, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         38 seconds doing isa_i_main_process_pkt_4, (0 @ 0)
manage @ 38 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing isa_i_main_process_pkt_6, (0 @ 0)
         39 seconds doing isa_i_main_last_op, (0 @ 0)
   end script: ISAKMP secondary Main for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_phase_1_done, (0 @ 0)
         39 seconds doing l2lp_start_phase_2, (0 @ 0)
   new script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_init, (0 @ 0)
         39 seconds doing iph2_build_pkt_1, (0 @ 0)
         39 seconds doing iph2_send_pkt_1, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing iph2_pkt_2_wait, (0 @ 0)
         39 seconds doing ihp2_process_pkt_2, (0 @ 0)
         39 seconds doing iph2_build_pkt_3, (0 @ 0)
         39 seconds doing iph2_config_SAs, (0 @ 0)
         39 seconds doing iph2_send_pkt_3, (0 @ 0)
         39 seconds doing iph2_last_op, (0 @ 0)
   end script: phase 2 initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
   next script: lan-lan primary initiator for lan-lan-VPN0:1:[172.18.124.157], (0 @ 0)
         39 seconds doing l2lp_open_tunnel, (0 @ 0)
         39 seconds doing l2lp_start_i_maint, (0 @ 0)
   new script: initiator maintenance for lan-lan-VPN0:1:[172.18.124.157] (start)
         39 seconds doing imnt_init, (0 @ 0)
manage @ 39 seconds :: lan-lan-VPN0:1:[172.18.124.157] (done)


cisco_endpoint#show vpn stat

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          --------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          --------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

cisco_endpoint#show vpn stat verb

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          --------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  1        0        1        1        1        0        0
Total     1        0        1        1        1        0        0

Stats             VPN0:1
Wrapped               13
Unwrapped              9
BadEncap               0
BadAuth                0
BadEncrypt             0
rx IP                  9
rx IPX                 0
rx Other               0
tx IP                 13
tx IPX                 0
tx Other               0
IKE rekey              0

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        4
Fastswitch packets in   0
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      1
Inserted cookie(R)      0
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        0
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0

IOP slot 1:

          Current  In       High     Running  Tunnel   Tunnel   Tunnel
          Active   Negot    Water    Total    Starts   OK       Error
          --------------------------------------------------------------
Users     0        0        0        0        0        0        0
Partners  0        0        0        0        0        0        0
Total     0        0        0        0        0        0        0

Stats
Wrapped
Unwrapped
BadEncap
BadAuth
BadEncrypt
rx IP
rx IPX
rx Other
tx IP
tx IPX
tx Other
IKE rekey

Input VPN pkts dropped due to no SA: 0

Input VPN pkts dropped due to no free queue entries: 0

ISAKMP Negotiation stats
Admin packets in        0
Fastswitch packets in   3
```

```
No cookie found         0
Can't insert cookie     0
Inserted cookie(L)      0
Inserted cookie(R)      1
Cookie not inserted(L)  0
Cookie not inserted(R)  0
Cookie conn changed     0
Cookie already inserted  0
Deleted cookie(L)       0
Deleted cookie(R)       0
Cookie not deleted(L)   0
Cookie not deleted(R)   0
Forwarded to RP         0
Forwarded to IOP        3
Bad UDP checksum        0
Not fastswitched        0
Bad Initiator cookie    0
Bad Responder cookie    0
Has Responder cookie    0
No Responder cookie     0
No SA                   0
Bad find conn           0
Admin queue full        0
Priority queue full     0
Bad IKE packet          0
No memory               0
Bad Admin Put           0
IKE pkt dropped         0
No UDP PBuf             0
No Manager              0
Mgr w/ no cookie        0
Cookie Scavenge Add     1
Cookie Scavenge Rem     0
Cookie Scavenged        0
Cookie has mgr err      0
New conn limited        0
```

相關資訊

- Cisco VPN 5000系列集中器銷售終止公告
- IPSec 協商/IKE 通訊協定
- 技術支援與文件 - Cisco Systems