將Cisco VPN 3000集中器配置到Cisco路由器

目錄

簡介

此組態範例顯示如何在執行Cisco IOS®軟體的路由器後方的私人網路連線到Cisco VPN 3000集中器後方的私人網路。網路上的裝置通過其私有地址相互認識。

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：

- 採用Cisco IOS軟體版本12.3.(1)a的Cisco 2611路由器**注意：**確保Cisco 2600系列路由器安裝了支援VPN功能的加密IPsec VPN IOS映像。
- 採用4.0.1 B的Cisco VPN 3000集中器

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。

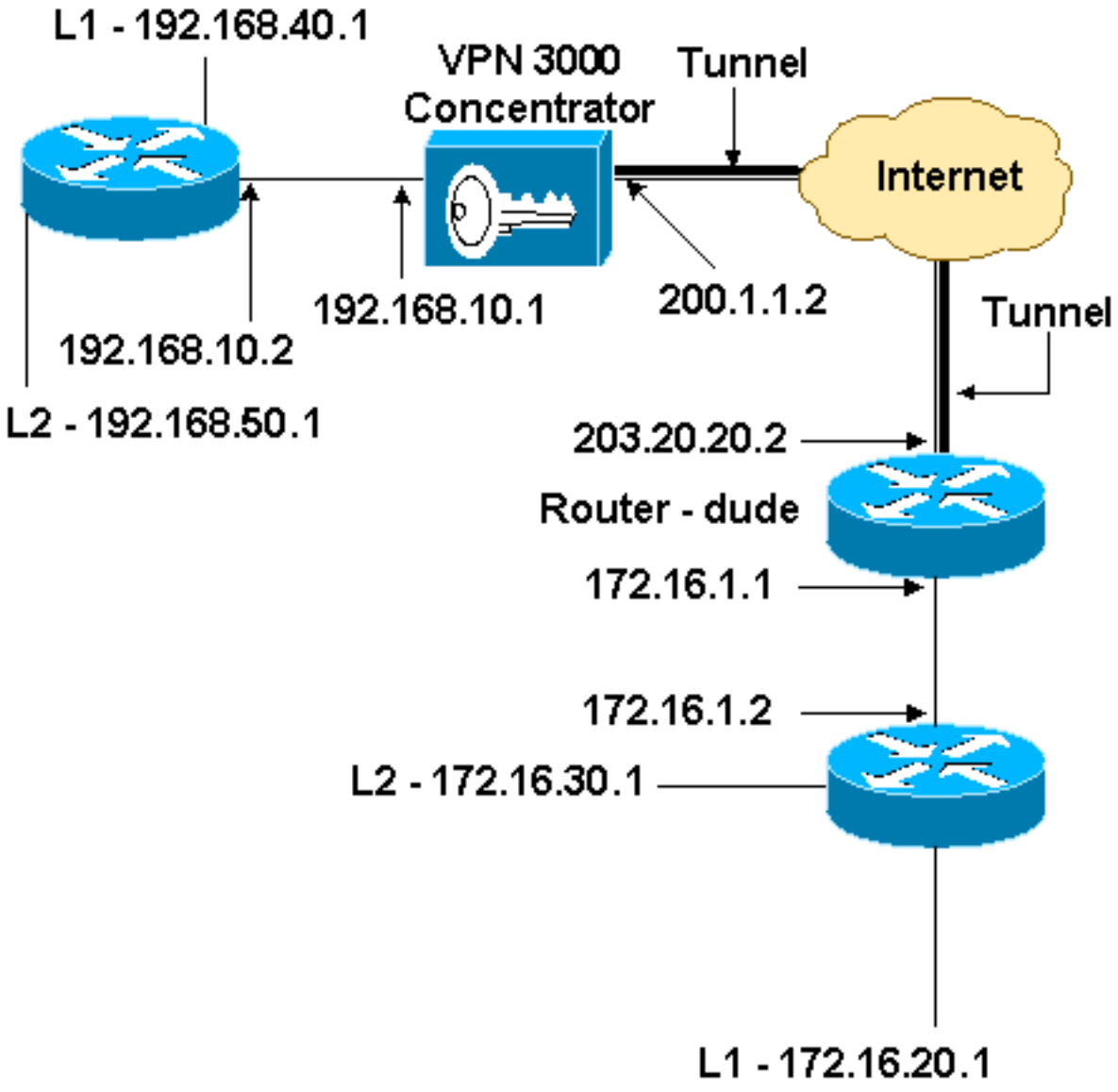
設定

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

本檔案會使用此網路設定。



組態

本檔案會使用此組態。

路由器配置

```
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname dude
!
memory-size iomem 15
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
!!--- IKE policies. crypto isakmp policy 1
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 200.1.1.2
!!--- IPsec policies. crypto ipsec transform-set to_vpn
esp-3des esp-md5-hmac
!
crypto map to_vpn 10 ipsec-isakmp
 set peer 200.1.1.2
 set transform-set to_vpn
!--- Traffic to encrypt. match address 101
!
interface Ethernet0/0
 ip address 203.20.20.2 255.255.255.0
 ip nat outside
 half-duplex
 crypto map to_vpn
!
interface Ethernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip nat inside
 half-duplex
!
ip nat pool mypool 203.20.20.3 203.20.20.3 netmask
255.255.255.0
ip nat inside source route-map nonat pool mypool
overload
ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 203.20.20.1
ip route 172.16.20.0 255.255.255.0 172.16.1.2
ip route 172.16.30.0 255.255.255.0 172.16.1.2
!!--- Traffic to encrypt. access-list 101 permit ip
172.16.1.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
```

```
192.168.40.0 0.0.0.255
access-list 101 permit ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
!--- Traffic to except from the NAT process. access-list
110 deny   ip 172.16.1.0 0.0.0.255 192.168.10.0
0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.1.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.20.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.10.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.40.0 0.0.0.255
access-list 110 deny   ip 172.16.30.0 0.0.0.255
192.168.50.0 0.0.0.255
access-list 110 permit ip 172.16.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
line aux 0
line vty 0 4
!
end
```

VPN集中器配置

在本實驗設定中，首先通過控制檯埠訪問VPN集中器，然後新增最小配置，以便通過圖形使用者介面(GUI)完成進一步的配置。

選擇**Administration > System Reboot > Schedule reboot > Reboot with Factory/Default Configuration**以確保VPN集中器中沒有現有配置。

VPN集中器顯示在Quick Configuration中，這些專案會在重新啟動後配置：

- 時間/日期
- **Configuration > Interfaces**中的介面/遮罩(public=200.1.1.2/24, private=192.168.10.1/24)
- **Configuration > System > IP routing > Default_Gateway**中的預設閘道(200.1.1.1)

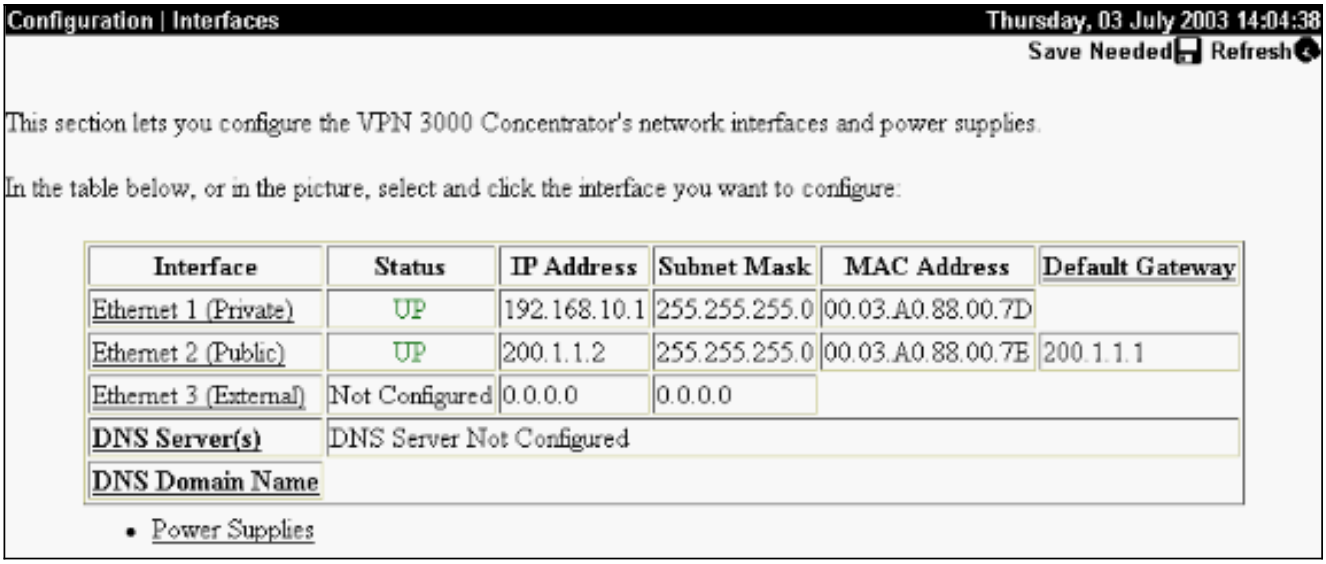
此時，可從內部網路通過HTML訪問VPN集中器。

注意：由於VPN集中器是從外部管理的，因此您還必須選擇：

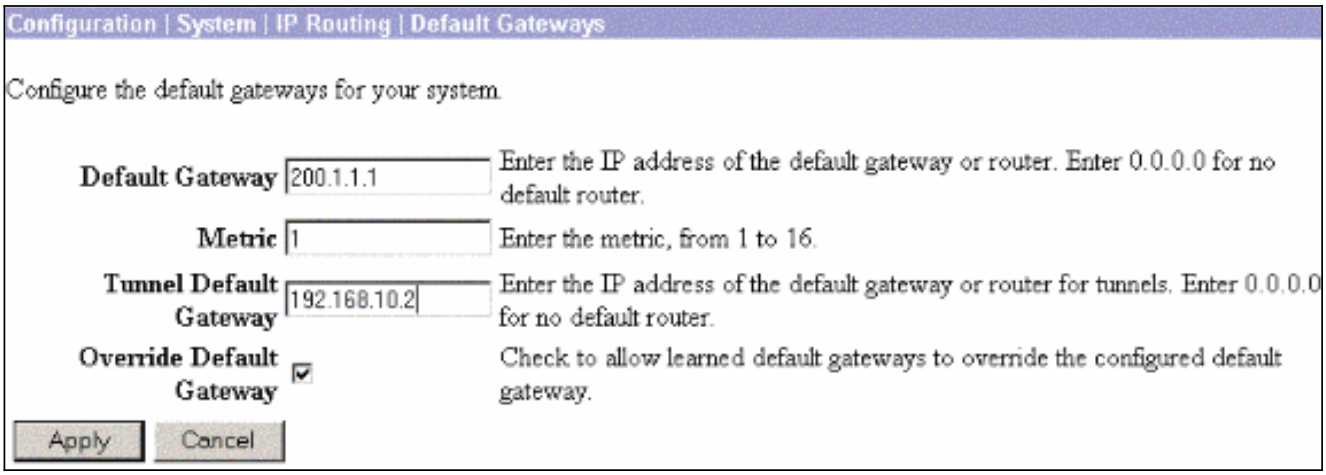
- **Configuration > Interfaces > 2-public > Select IP Filter > 1. Private（預設）**。
- **Administration > Access Rights > Access Control List > Add Manager Workstation**以新增*external*管理器的IP地址。

除非您從外部管理VPN集中器，否則無需執行此*操作*。

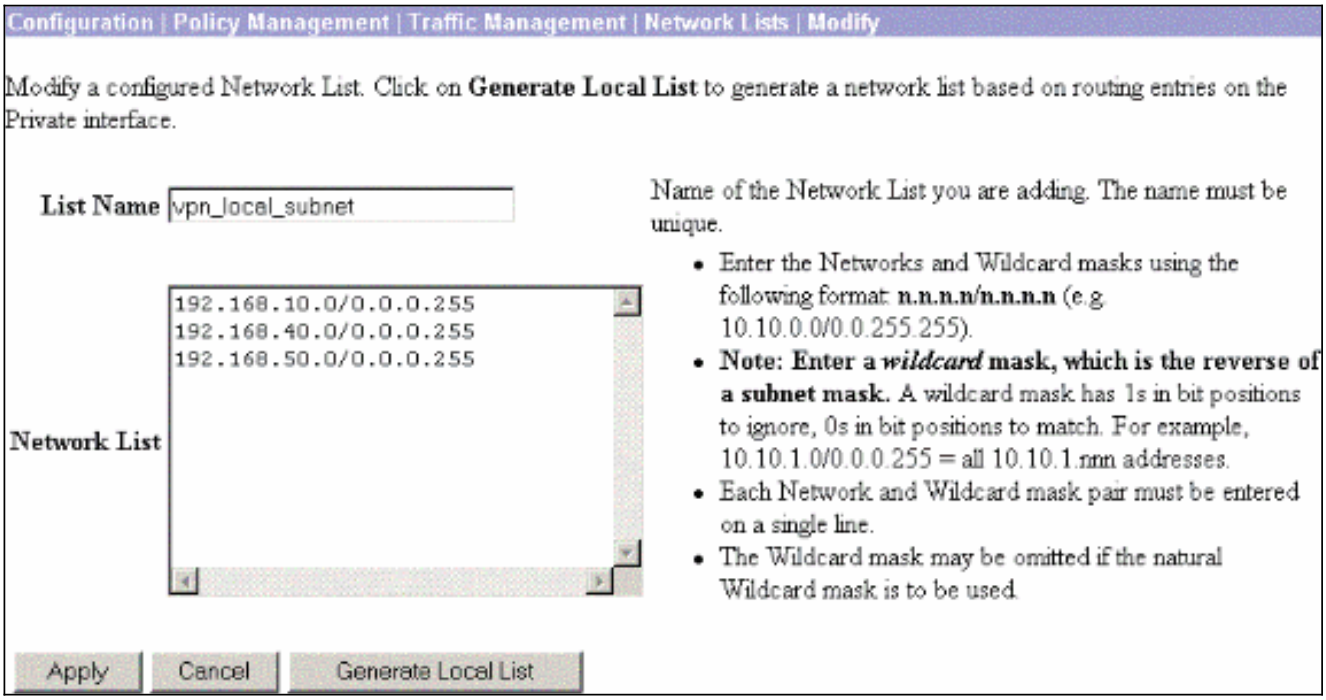
1. 啟動GUI後，選擇**Configuration > Interfaces**以重新檢查介面。



2. 選擇Configuration > System > IP Routing > Default Gateways，配置Default (Internet)Gateway和Tunnel Default (inside)**Gateway**，以使IPsec到達專用網路中的其他子網。

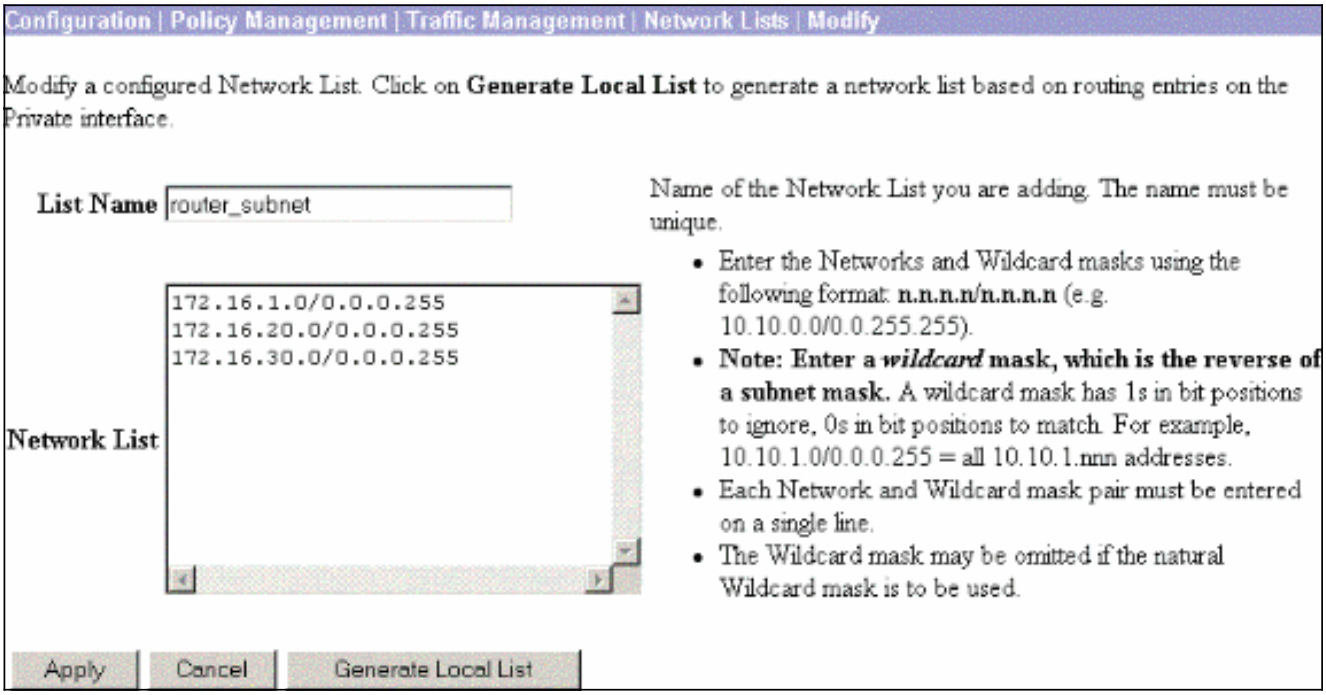


3. 選擇**Configuration > Policy Management > Network Lists**以建立定義要加密的流量的網路清單。以下是本地網路：

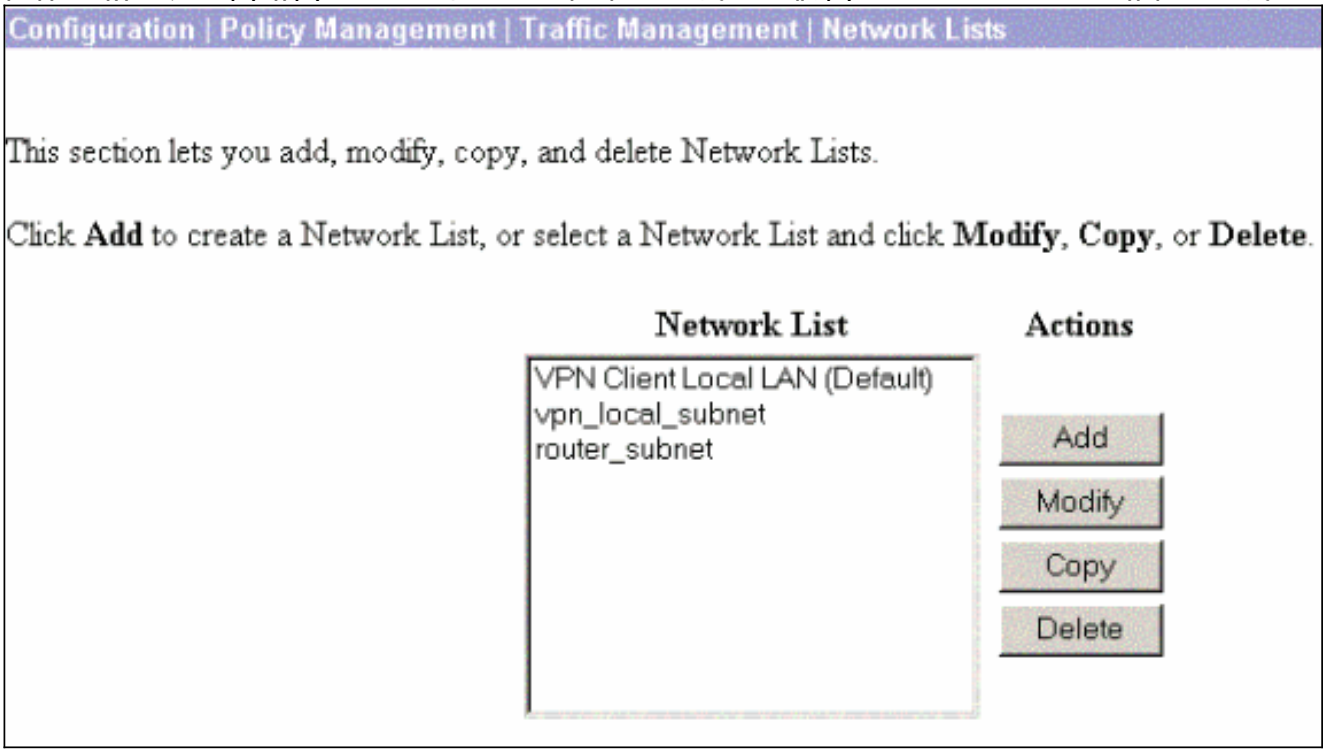


這些是遠端網路

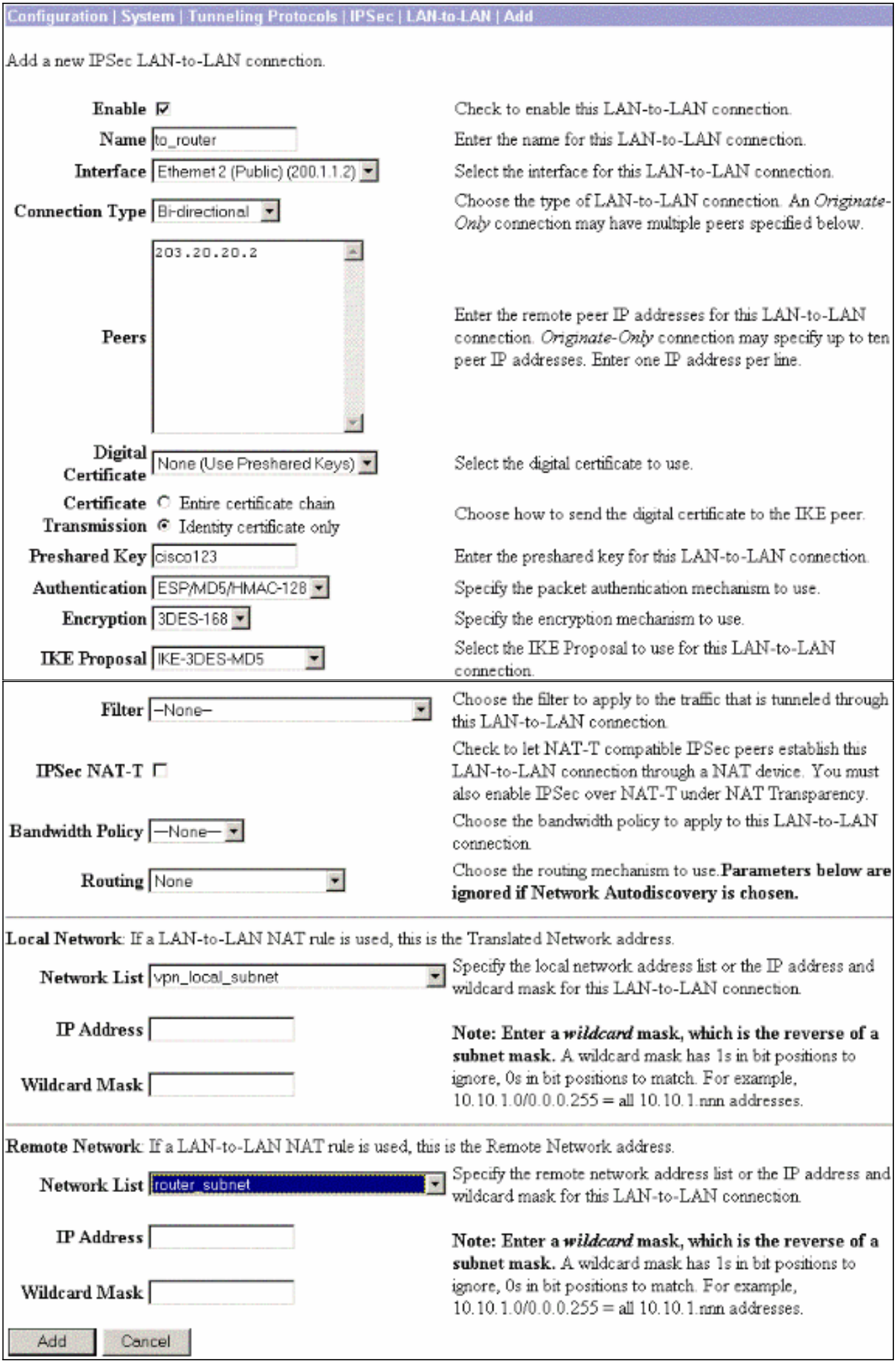
：



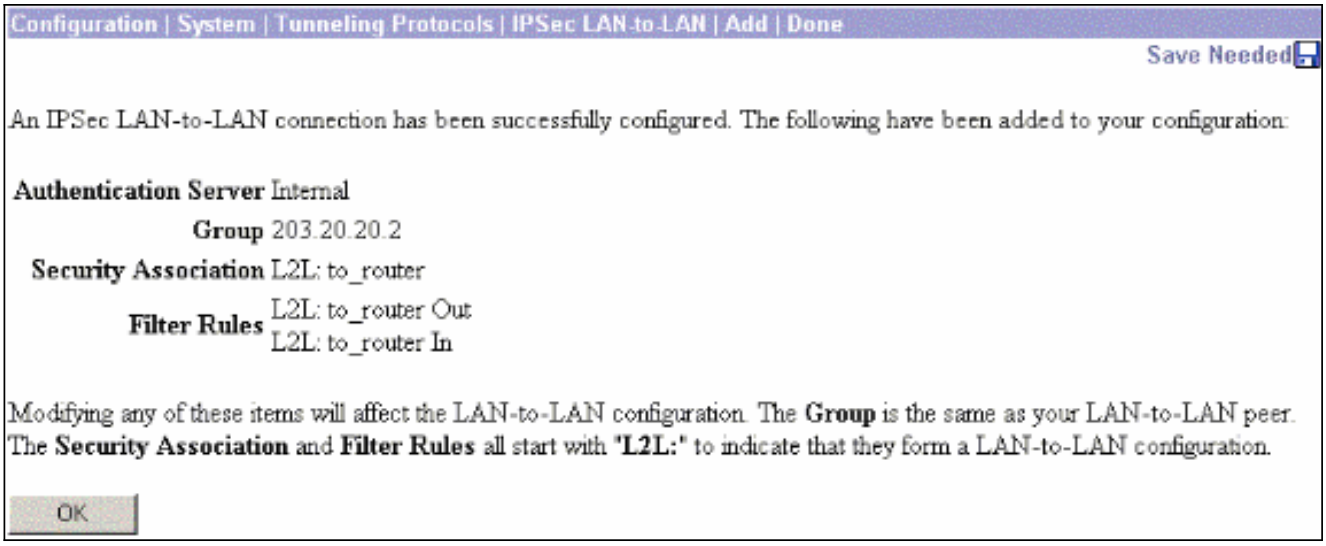
4. 完成後，以下是兩個網路清單：**注意：**如果IPsec隧道沒有啟動，請檢查兩端的相關流量是否匹配。相關流量由路由器和PIX框上的訪問清單定義。它們由VPN集中器中的網路清單定義。



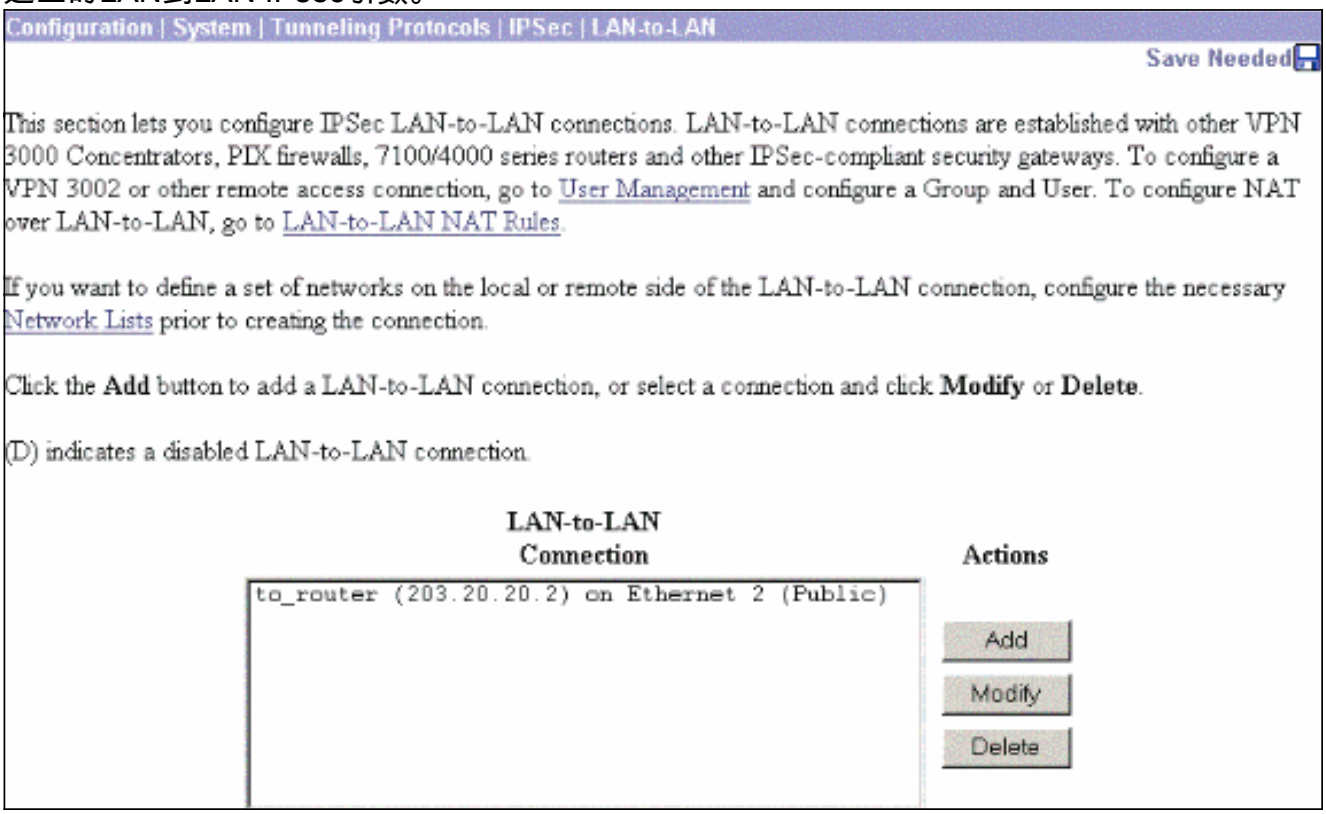
5. 選擇**Configuration > System> Tunneling Protocols > IPSec LAN-to-LAN**並定義LAN-to-LAN隧道。



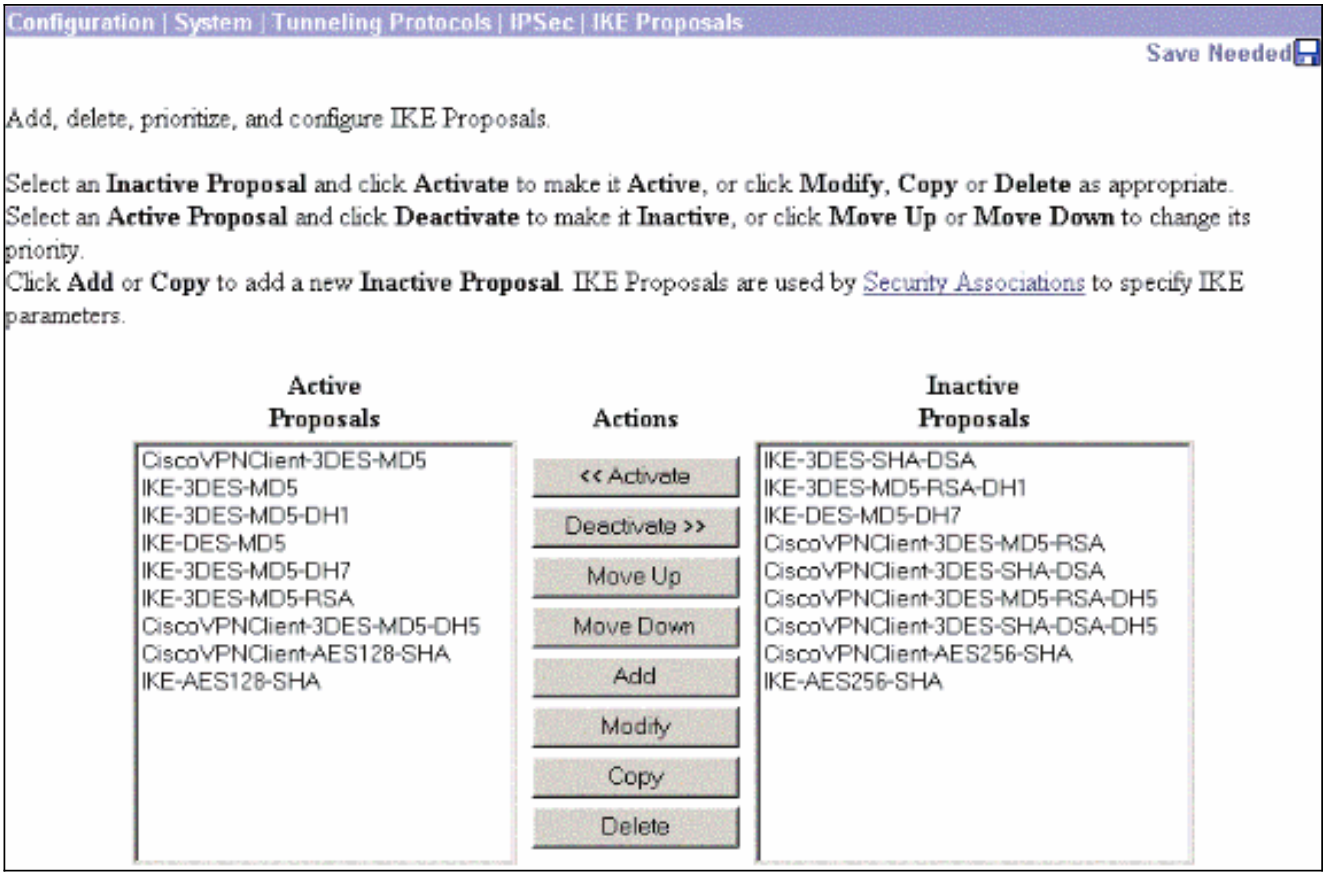
6. 按一下Apply後，此視窗會顯示其他組態，作為LAN到LAN通道組態的結果自動建立。



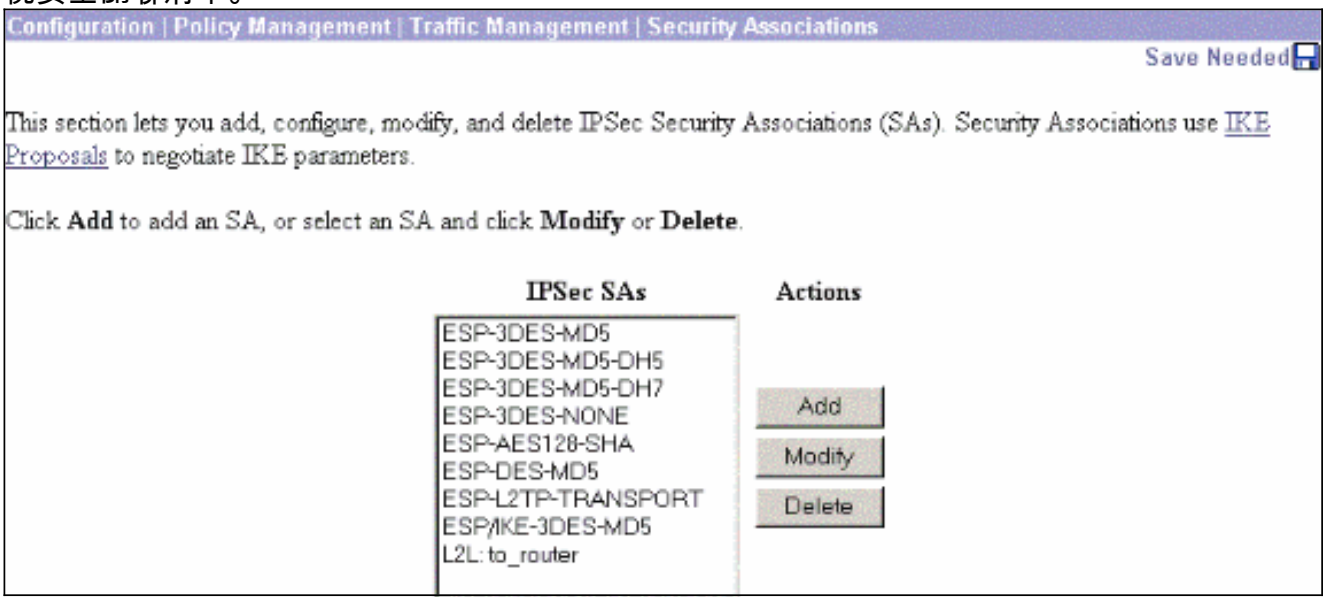
可以在**Configuration > System > Tunneling** Protocols > **IPSec LAN-to-LAN**中檢視或修改先前建立的LAN到LAN IPsec引數。



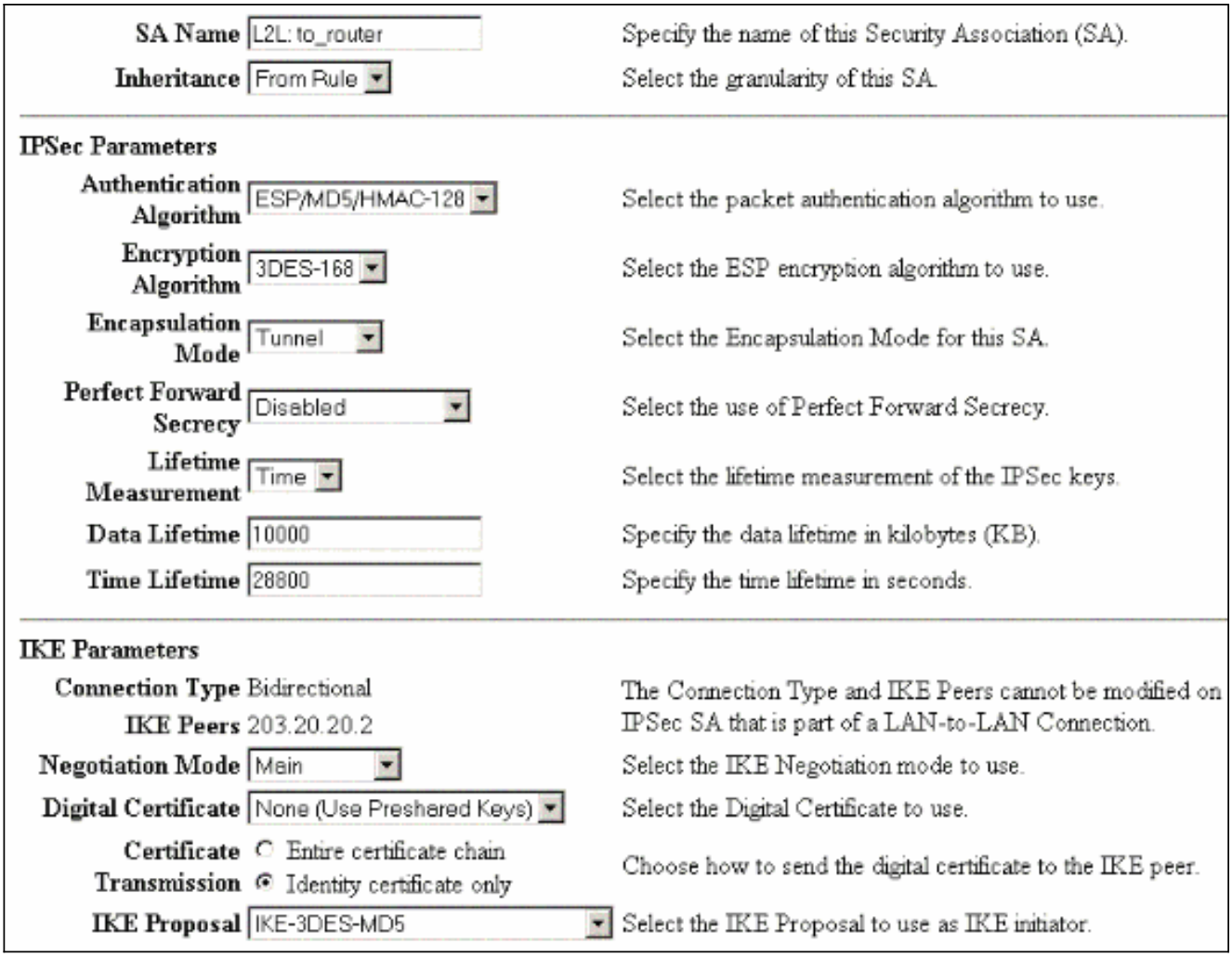
7. 選擇Configuration > **System > Tunneling Protocols > IPSec > IKE Proposals**以確認活動的IKE建議。



8. 選擇Configuration > Policy Management> Traffic Management > Security Associations以檢視安全關聯清單。



9. 按一下安全關聯名稱，然後按一下**修改**以驗證安全關聯。



驗證

本節列出此設定中使用的**show**命令。

在路由器上

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 ipsec sa** — 顯示當前安全關聯使用的設定。
- **show crypto isakmp sa** — 顯示對等體上的所有當前Internet金鑰交換安全關聯。
- **show crypto engine connection active** — 顯示所有加密引擎的當前活動加密會話連線。

您可以使用IOS命令查詢工具(僅供已註冊客戶使用)檢視有關特定命令的更多資訊。

在VPN集中器上

選擇Configuration > **System** > **Events** > **Classes** > **Modify**以開啟日誌記錄。以下選項可用：

- IKE
- IKEDBG
- IKEDECODE

- IPSEC
- IPSECDBG
- IPSECDECODE

記錄嚴重性= 1-13

控制檯嚴重性= 1-3

選擇**Monitoring > Event Log**以檢索事件日誌。

疑難排解

在路由器上

嘗試任何debug指令之前，請先參閱有關Debug指令的重要資訊。

- **debug crypto engine** — 顯示加密的流量。
- **debug crypto ipsec** — 顯示第2階段的IPsec協商。
- **debug crypto isakmp** — 顯示第1階段的ISAKMP協商。

問題 — 無法啟動隧道

錯誤消息

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

解決方案

完成此操作可配置所需的同時登入數，或將此SA的同步登入數設定為5:

轉至**Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneouts Logins**，將登入數更改為5。

PFS

在IPsec協商中，完全向前保密(PFS)可確保每個新的加密金鑰與之前的任何金鑰無關。啟用或停用兩個通道對等點上的PFS。否則，路由器中未建立LAN到LAN(L2L)IPsec通道。

若要指定在為此加密對映條目請求新的安全關聯時IPsec應請求PFS，或指定IPsec在收到新安全關聯請求時需要PFS，請在加密對映配置模式下使用**set pfs**命令。要指定IPsec不應請求PFS，請使用此命令的**no**形式。

```
set pfs [group1 | group2]
no set pfs
```

對於**set pfs**命令：

- *group1* — 指定在執行新的Diffie-Hellman交換時IPsec應使用768位Diffie-Hellman主模陣列。

• *group2* — 指定在執行新的Diffie-Hellman交換時IPsec應使用1024位Diffie-Hellman主模陣列。預設情況下，不請求PFS。如果使用此命令未指定組，則*group1*用作預設值。

範例：

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

有關**set pfs**命令的詳細資訊，請參閱Cisco IOS安全命令參考。

相關資訊

- **最常見的L2L和遠端訪問IPSec VPN故障排除解決方案**
- **Cisco VPN 3000系列集中器**
- **Cisco VPN 3002硬體使用者端**
- **IPSec 協商/IKE 通訊協定**
- **技術支援與文件 - Cisco Systems**