使用AES的Cisco VPN 3000集中器和路由器之間的LAN到LAN IPsec隧道配置示例

目錄

簡介

本文說明如何使用高級加密標準(AES)作為加密演算法，在Cisco VPN 3000集中器和思科路由器之間配置IPsec隧道。

AES是由美國國家標準與技術研究所(NIST)建立的新聯邦資訊處理標準(FIPS)出版物，用於加密方法。此標準指定一個AES對稱加密演算法，該演算法取代資料加密標準(DES)作為IPsec和Internet金鑰交換(IKE)的隱私轉換。AES有三種不同的金鑰長度，一個128位金鑰（預設），一個192位金鑰和一個256位金鑰。Cisco IOS®中的AES功能新增了對IPsec對具有密碼塊連結(CBC)模式的新加密標準AES的支援。

有關AES的詳細資訊，請參閱NIST電腦保安資源中心站點 。

有關VPN 3000集中器和PIX防火牆之間的LAN到LAN隧道配置的詳細資訊，請參閱Cisco VPN 3000集中器和PIX防火牆之間的LAN到LAN IPsec隧道配置示例。

有關PIX軟體版本7.1的詳細資訊，請參閱PIX 7.x和VPN 3000集中器之間的IPsec隧道配置示例。

必要條件

需求

本文檔需要對IPsec協定有基本的瞭解。請參閱IPSec加密簡介以瞭解有關IPsec的詳細資訊。

嘗試此組態之前，請確保符合以下要求：

- **路由器**要求 — AES功能是在Cisco IOS軟體版本12.2(13)T中匯入。為了啟用AES，您的路由器必須支援IPsec並使用「k9」長金鑰運行IOS映像（「k9」子系統）。**註：**Cisco 2600XM、2691、3725和3745 AES加速VPN模組也提供AES硬體支援。此功能沒有配置影響，如果兩個模組都可用，將自動選擇硬體模組。
- **VPN集中器要**求 — AES功能的軟體支援是在3.6版中引入的。硬體支援通過新的增強型可擴展加密處理器(SEP-E)提供。 此功能不涉及配置。**注意：**在Cisco VPN 3000 Concentrator 3.6.3版中，由於Cisco錯誤ID CSCdy88797(僅限註冊客戶)，通道不會與AES協商。 3.6.4版中已解決此問題。**注意：**Cisco VPN 3000 Concentrator使用SEP或SEP-E模組，而不是同時使用兩者。請勿將兩者安裝在同一裝置上。如果在已經包含SEP模組的VPN集中器上安裝SEP-E模組，則VPN集中器會禁用SEP模組並僅使用SEP-E模組。

採用元件

本檔案中的資訊是根據軟體和硬體版本：

- 採用Cisco IOS軟體版本12.3(5)的Cisco 3600系列路由器
- 軟體版本4.0.3的Cisco VPN 3060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

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。

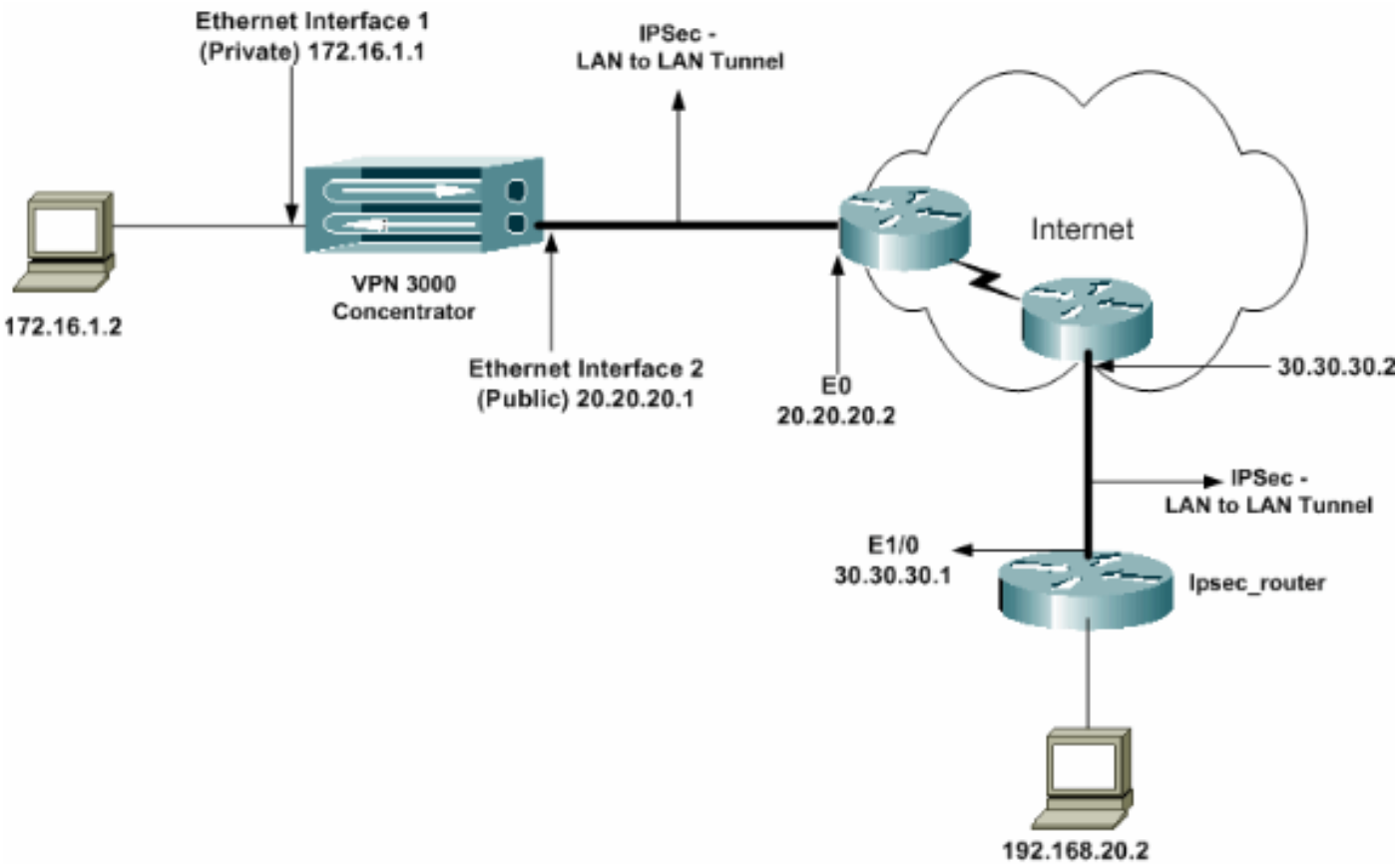
設定

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：

- IPsec路由器
- VPN集中器

ipsec_router組態

```
version 12.3
service timestamps debug uptime
service timestamps log datetime msec
no service password-encryption
!
hostname ipsec_router
!
memory-size iomem 10
no aaa new-model
ip subnet-zero
!
!--- Configuration for IKE policies. crypto isakmp
policy 1
!--- Enables the IKE policy configuration (config-
isakmp) command mode, !--- where you can specify the
parameters to be used during !--- an IKE negotiation.
encryption aes 256
!--- Specifies the encryption algorithm as AES with a
256 !--- bit key within an IKE policy. authentication
pre-share
group 2
crypto isakmp key cisco123 address 20.20.20.1
!--- Specifies the preshared key "cisco123" which !---
```

```
should be identical at both peers. !
!--- Configuration for IPsec policies. crypto ipsec
security-association lifetime seconds 28800
!--- Specifies the lifetime of the IPsec security
association (SA). ! crypto ipsec transform-set vpn esp-
aes 256 esp-md5-hmac
!--- Enables the crypto transform configuration mode,
where you can !--- specify the transform sets to be used
during an IPsec negotiation. ! crypto map vpn 10 ipsec-
isakmp
!--- Indicates that IKE is used to establish the IPsec
SA for protecting !--- the traffic specified by this
crypto map entry. set peer 20.20.20.1
!--- Sets the IP address of the remote end (VPN
Concentrator). set transform-set vpn
!--- Configures IPsec to use the transform-set "vpn"
defined earlier. ! !--- Specifies the traffic to be
encrypted. match address 110
!
interface Ethernet1/0
ip address 30.30.30.1 255.255.255.0
ip nat outside
half-duplex
crypto map vpn
!--- Configures the interface to use the crypto map
"vpn" for IPsec. !
interface FastEthernet2/0
ip address 192.168.20.1 255.255.255.0
ip nat inside
duplex auto
speed auto
!
ip nat pool mypool 30.30.30.3 30.30.30.3 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 30.30.30.2
!
access-list 110 permit ip 192.168.20.0 0.0.0.255
172.16.0.0 0.0.255.255
!--- This crypto ACL-permit identifies the matching
traffic !--- flows to be protected via encryption. !---
Specifies the traffic not to be encrypted. access-list
120 deny ip 192.168.20.0 0.0.0.255 172.16.0.0
0.0.255.255
!--- This crypto ACL-deny identifies the matching
traffic flows not to be encrypted. !
access-list 120 permit ip 192.168.20.0 0.0.0.255 any
!--- The access control list (ACL) used in the NAT
configuration exempts !--- the LAN-to-LAN traffic from
the NAT process, !--- but allows all traffic going to
the Internet to be translated. !
route-map nonat permit 10
!--- The traffic flows not encrypted from the !--- peer
network are allowed. match ip address 120
!
line con 0
line aux 0
line vty 0 4
login
!
```

```
end
```

注意：雖然ACL語法未更改，但加密ACL的含義略有不同。在加密ACL中，**permit**指定應加密匹配的資料包，而**deny**指定不需要加密匹配的資料包。

配置VPN集中器

VPN集中器出廠設定中未預先設定IP地址。必須使用控制檯埠來配置初始配置，這些配置是基於選單的命令列介面(CLI)。 有關如何通過控制檯進行配置的資訊，請參閱通過控制檯配置VPN集中器。

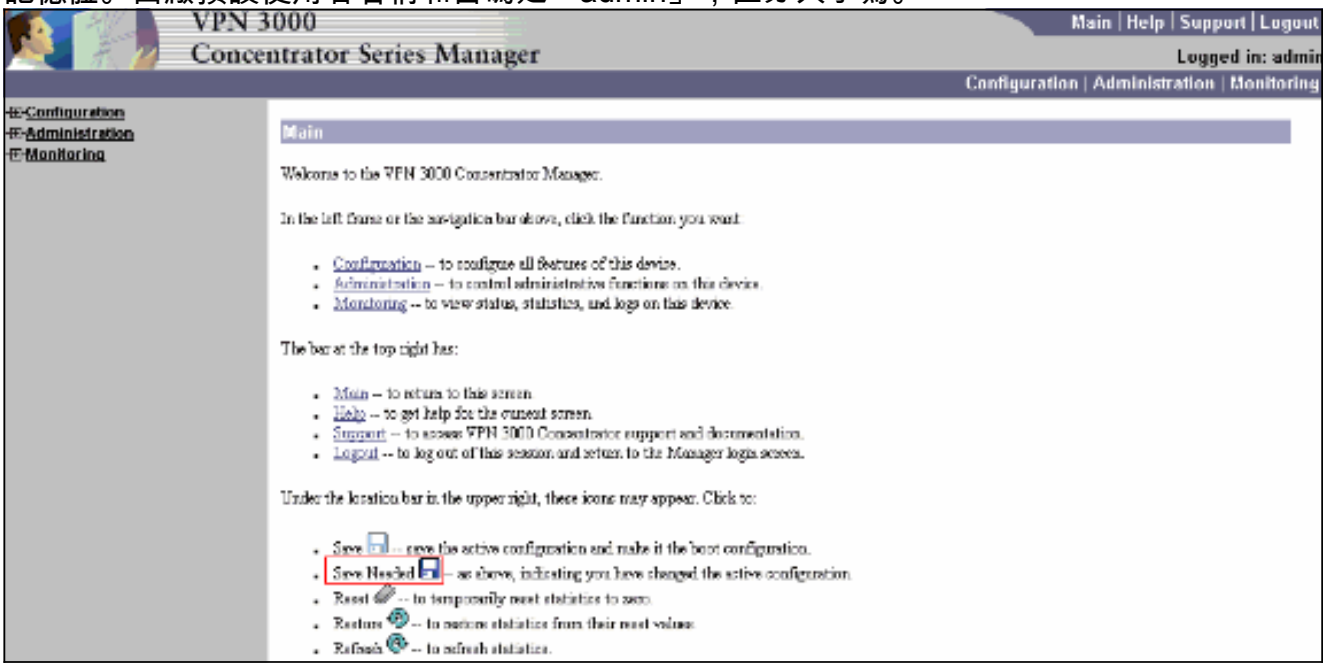
在Ethernet 1（專用）介面上配置IP地址後，可以使用CLI或通過瀏覽器介面配置其餘地址。瀏覽器介面同時支援HTTP和HTTP over Secure Socket Layer(SSL)。

這些引數是通過控制檯配置的：

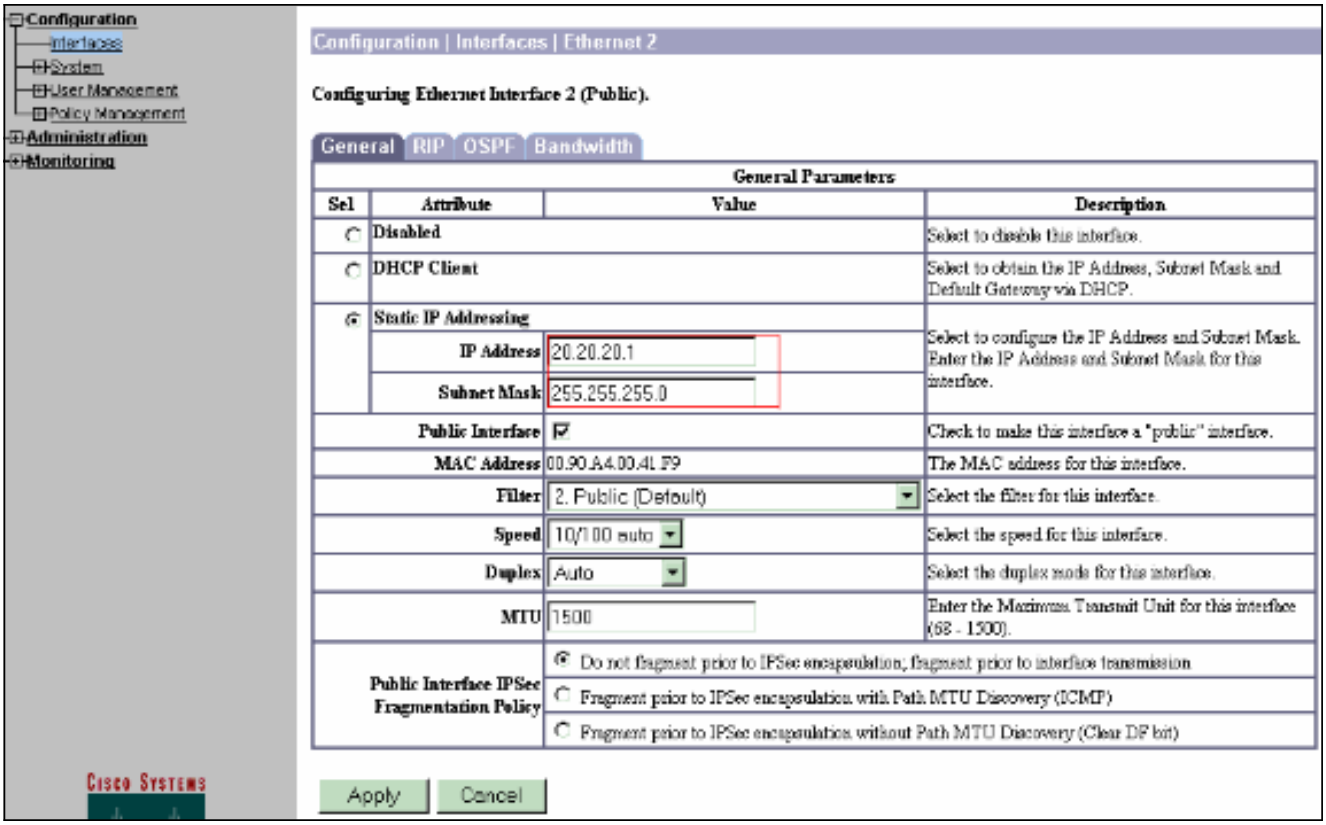
- **時間/日期** — 正確的時間和日期非常重要。它們有助於確保日誌記錄和會計分錄準確無誤，並且系統可以建立有效的安全證書。
- **Ethernet 1(private)interface** - IP地址和掩碼(來自我們的網路拓撲172.16.1.1/24)。

此時，可從內部網路通過HTML瀏覽器訪問VPN集中器。有關在CLI模式下配置VPN集中器的資訊，請參閱使用CLI快速配置。

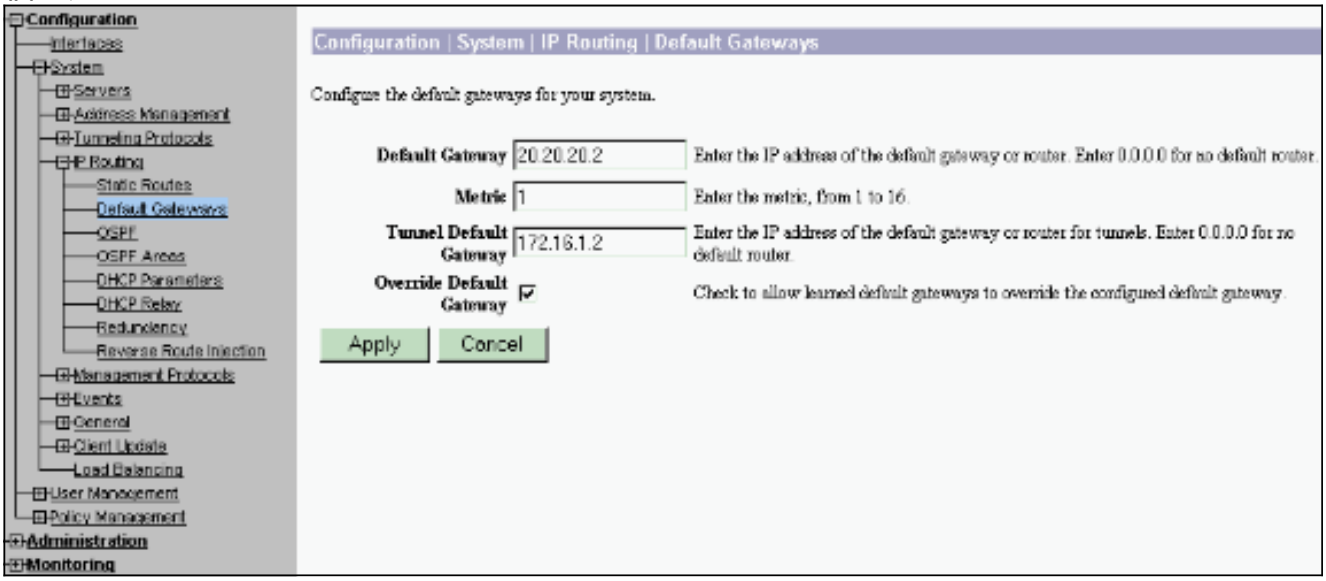
1. 從Web瀏覽器鍵入專用介面的IP地址以啟用GUI介面。按一下**save needed**圖示將更改儲存到記憶體。出廠預設使用者名稱和密碼是「admin」，區分大小寫。



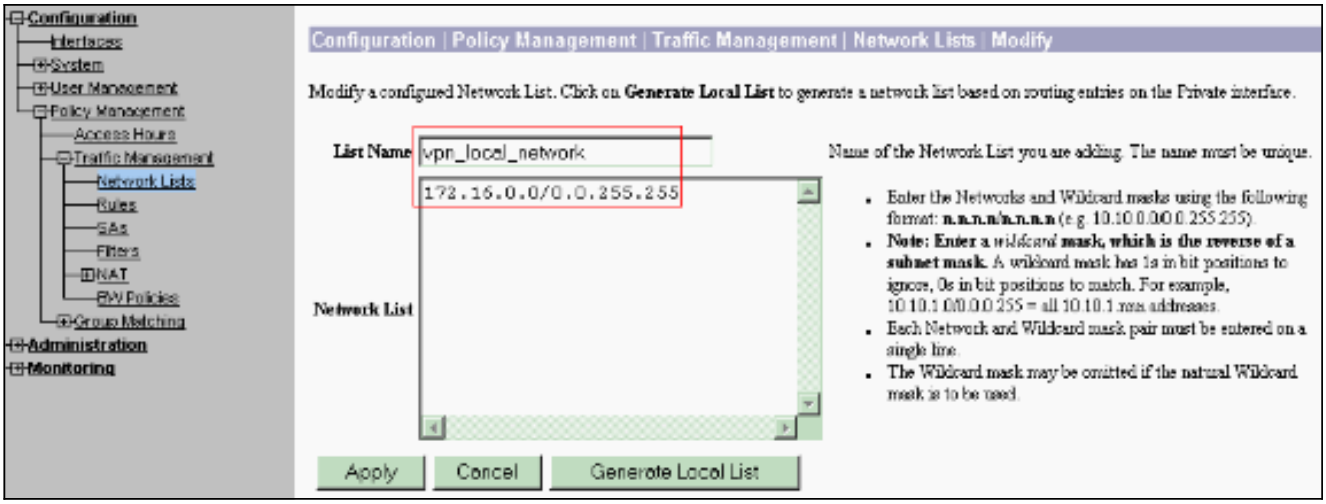
2. 啟動GUI後，選擇**Configuration > Interfaces > Ethernet 2(Public)**以設定Ethernet 2介面。



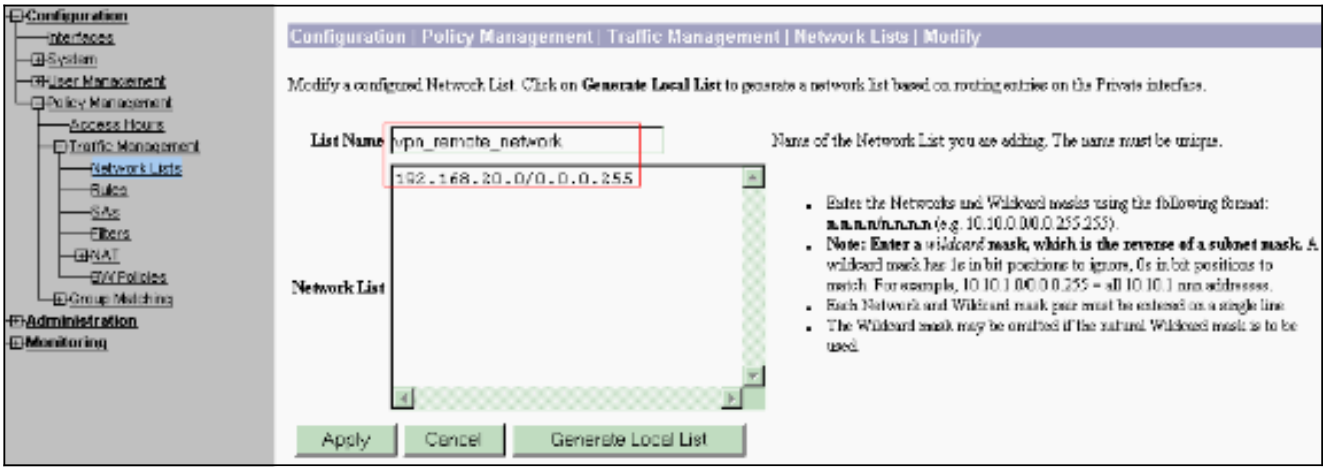
3. 選擇**Configuration > System > IP Routing > Default Gateways**，為IPsec配置預設(Internet)網關和隧道預設（內部）網關，以到達專用網路中的其他子網。在此場景中，內部網路中只有一個可用的子網。



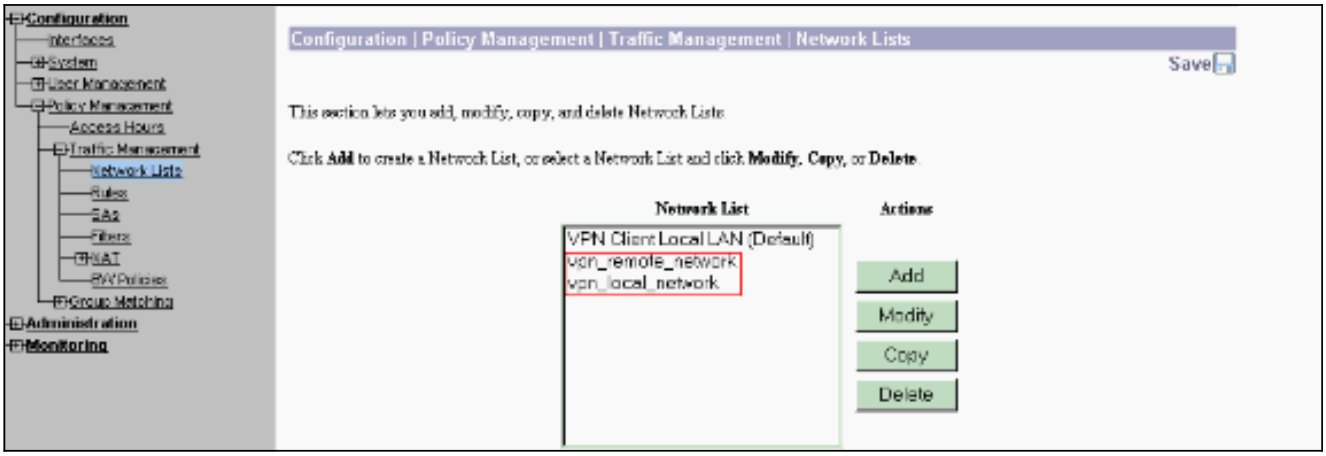
4. 選擇Configuration > **Policy Management > Traffic Management > Network Lists > Add**以建立定義要加密的流量的網路清單。清單中提到的網路可以到達遠端網路。以下清單顯示的網路是本地網路。按一下**Generate Local List**時，還可以通過RIP自動生成本地網路清單。



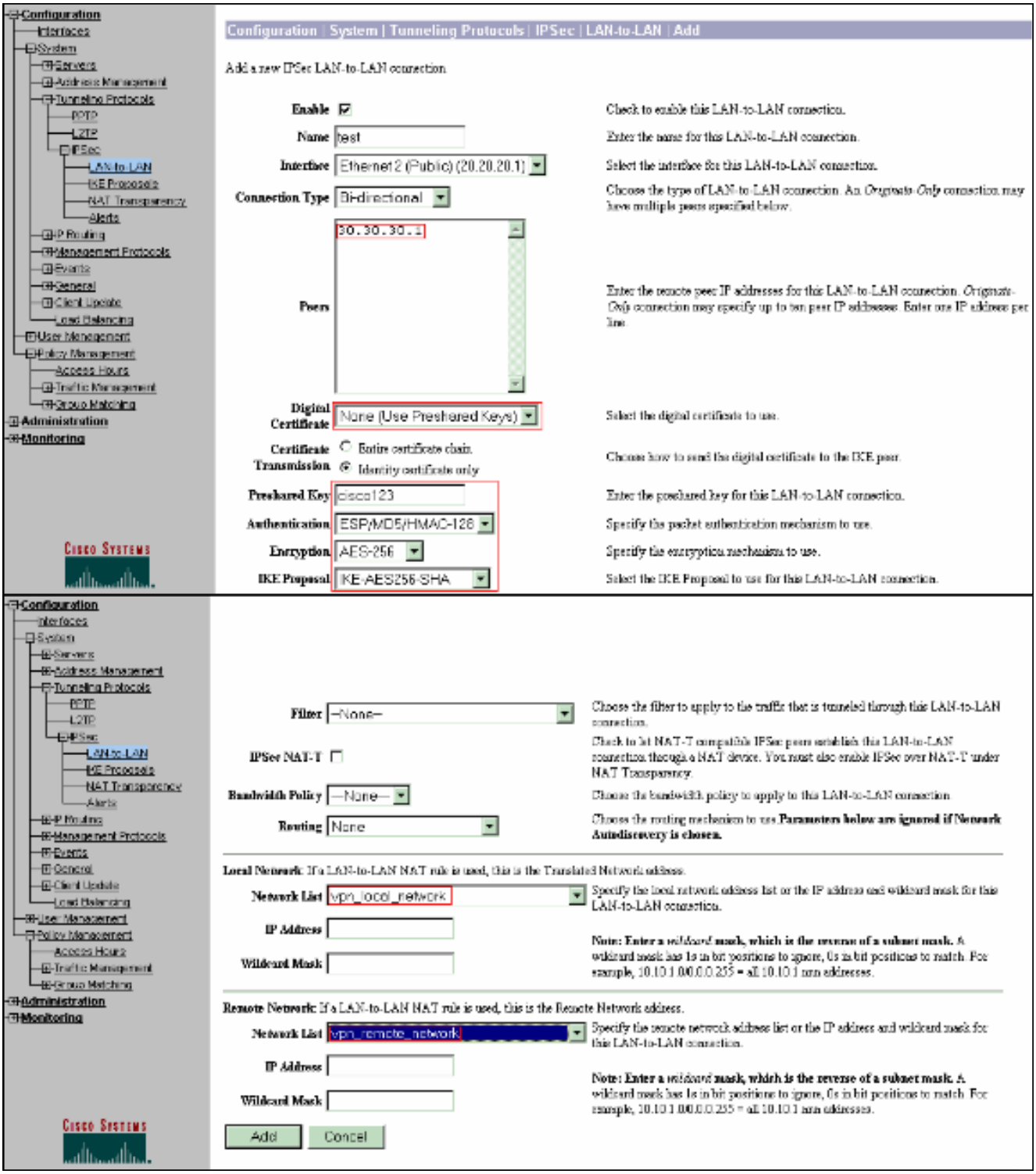
5. 此清單中的網路是遠端網路，需要手動配置。為此，請為每個可到達子網輸入網路/萬用字元。



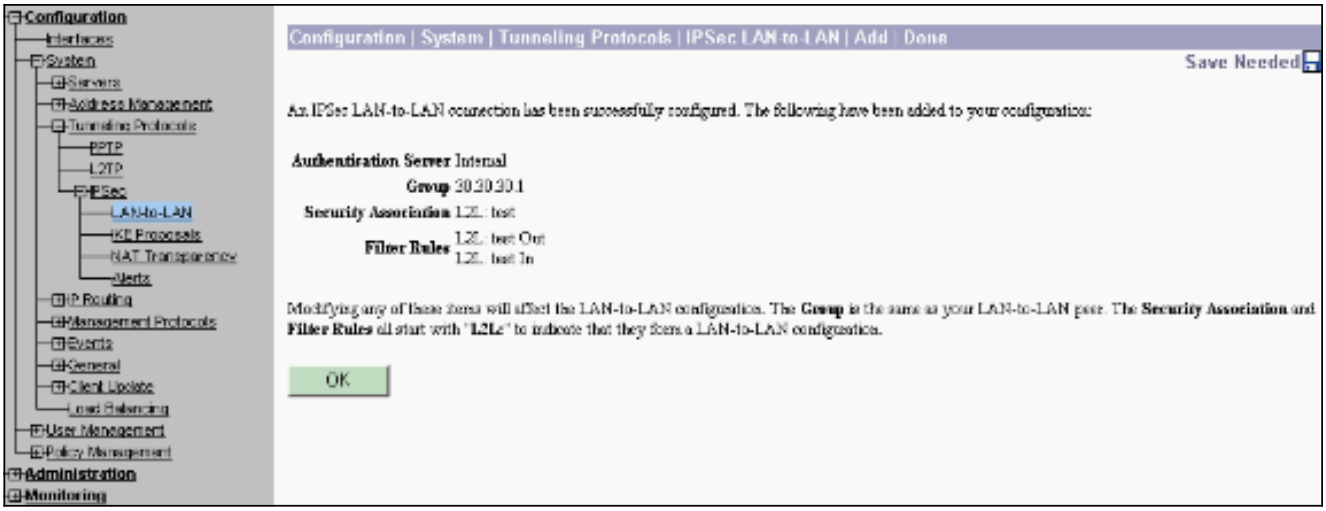
完成後，以下是兩個網路清單：



6. 選擇Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN > Add，然後定義LAN到LAN隧道。此視窗有三個部分。頂部用於網路資訊，底部兩部分用於本地和遠端網路清單。在Network Information（網路資訊）部分，選擇AES加密、身份驗證型別、IKE建議，然後鍵入預共用金鑰。在底部部分中，分別指向您已建立的本地和遠端網路清單。

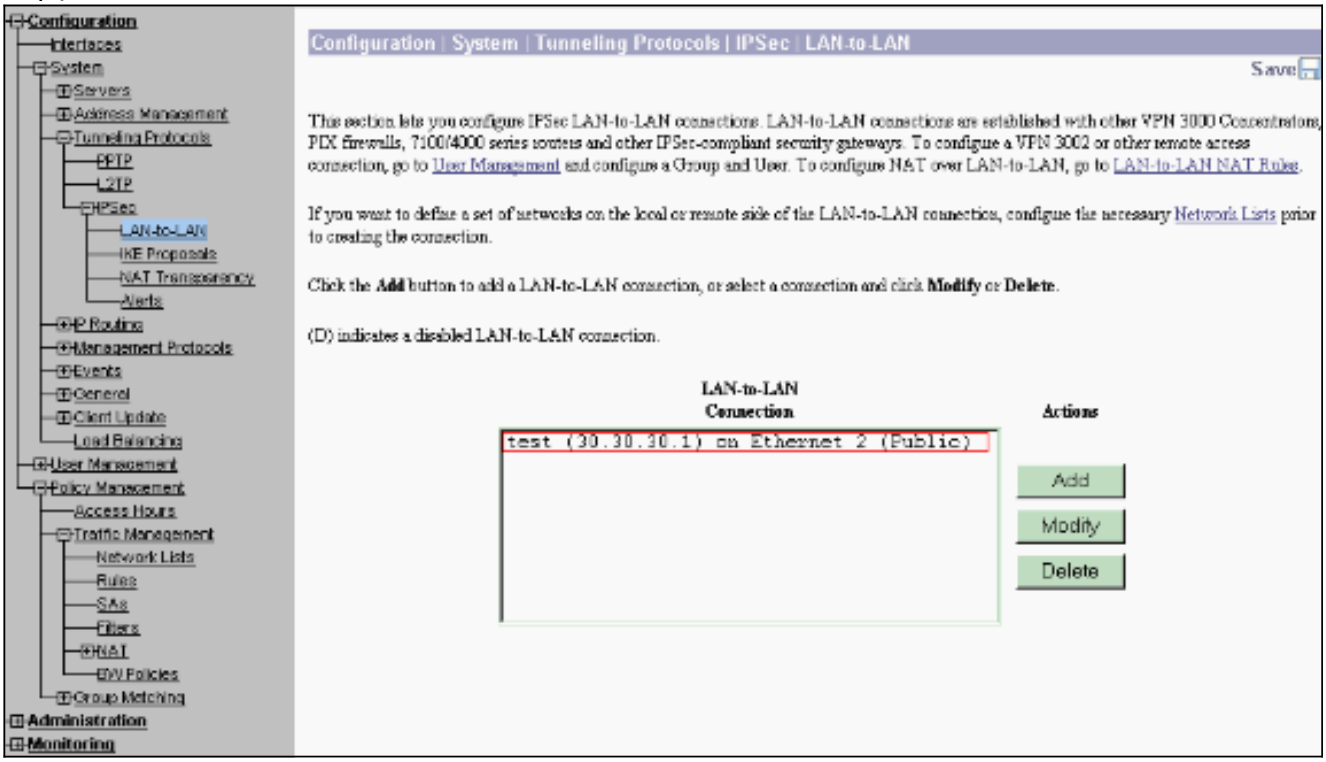


7. 按一下**Add**後，如果連線正確，系統將顯示一個IPSec LAN-to-LAN-Add-Done視窗。此視窗顯示隧道配置資訊的概要。它還自動配置組名、SA名和過濾器名。可以編輯此表中的任何引數。

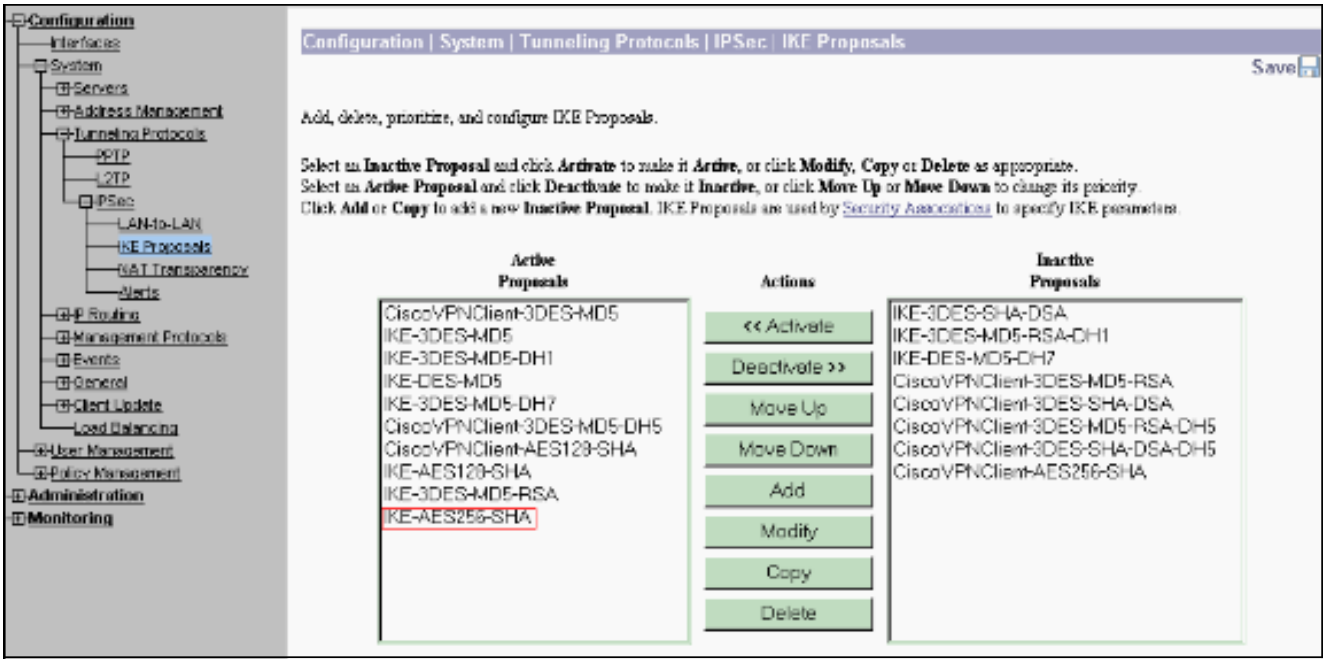


此時已設定IPsec LAN到LAN隧道，您可以開始工作。如果由於某種原因，通道無法正常工作，您可以檢查是否配置錯誤。

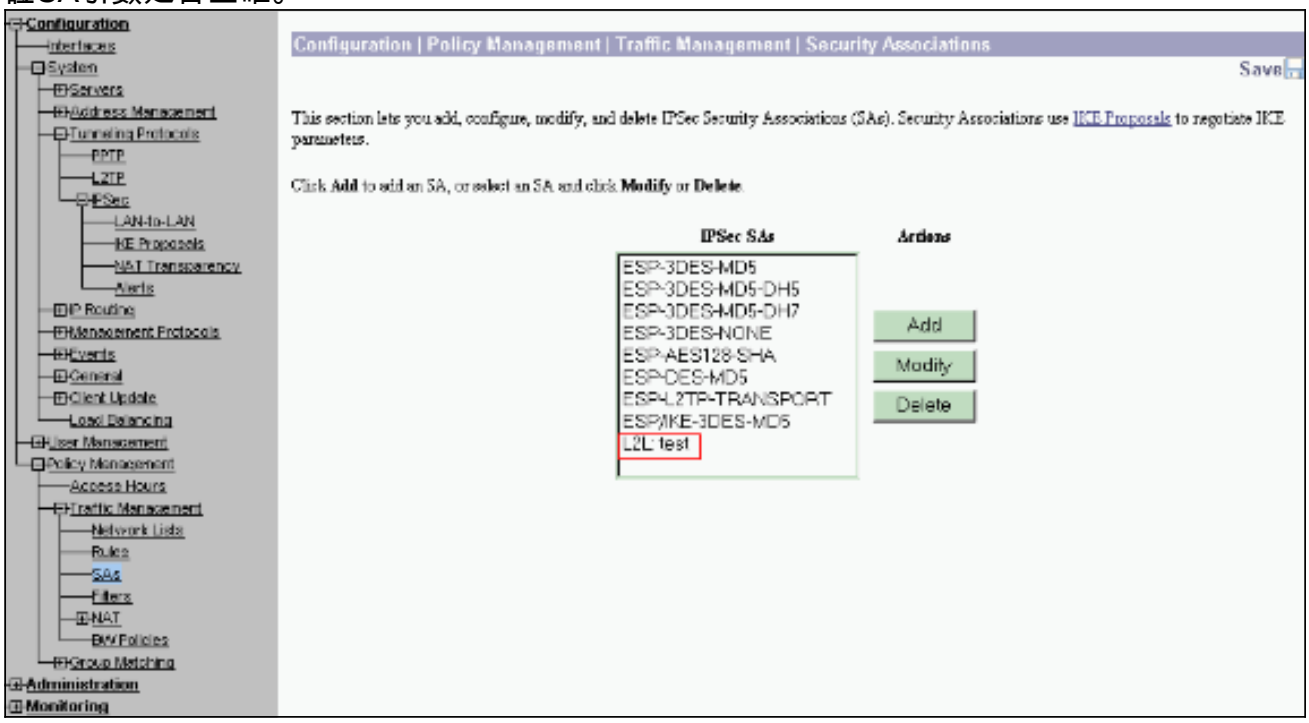
8. 選擇**Configuration > System > Tunneling Protocols > IPSec LAN-to-LAN**時，您可以檢視或修改先前建立的LAN到LAN IPsec引數。此圖顯示「測試」為通道名稱，依照案例，遠端的公共介面為30.30.30.1。



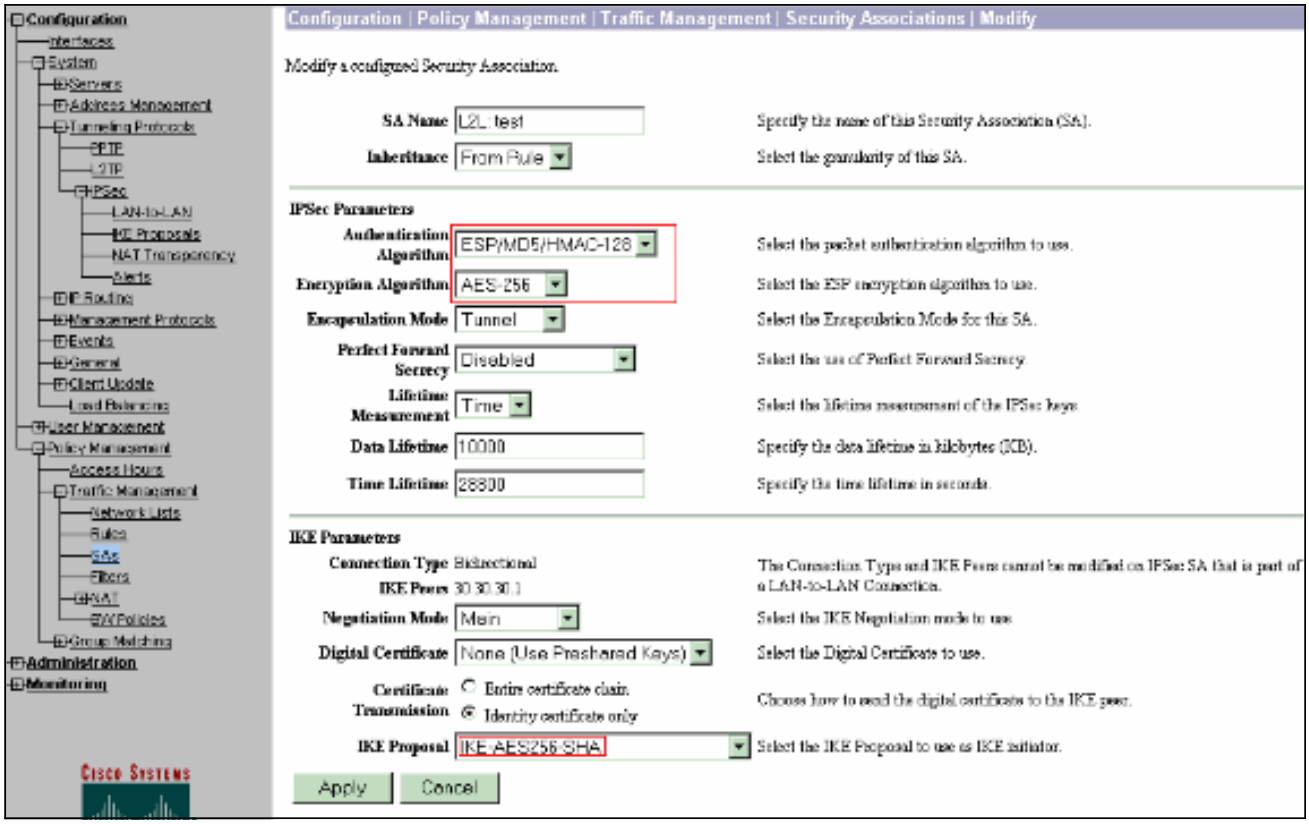
9. 有時，如果您的IKE建議在「非活動建議」清單中，則通道可能無法啟動。選擇Configuration > System > Tunneling Protocols > IPSec > IKE Proposals以配置活動的IKE提議。如果您的IKE建議位於「非活動建議」清單中，則可以在選擇IKE建議並按一下**啟用**按鈕時啟用它。在此圖中，選定的建議「IKE-AES256-SHA」位於活動建議清單中。



10. 選擇**Configuration > Policy Management > Traffic Management > Security Associations**以驗證SA引數是否正確。



11. 按一下SA名稱(在本例中為**L2L:test**)，然後按一下**Modify以驗證SA。**如果任何引數與遠端對等配置不匹配，可以在此處對其進行更改。



驗證

檢驗路由器配置

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。

- **show crypto isakmp sa** — 顯示對等體上的所有當前IKE SA。狀態QM_IDLE表示SA保持其對等體的身份驗證，可用於後續的快速模式交換。它處於靜止狀態。

```
ipsec_router#show crypto isakmp sa

 dst             src             state     conn-id    slot

 20.20.20.1      30.30.30.1      QM_IDLE          1       0
```

- **show crypto ipsec sa** — 顯示當前SA使用的設定。檢查對等IP地址、可在本地和遠端端訪問的網路，以及使用的轉換集。有兩個ESP SA，每個方向一個。由於使用了AH轉換集，因此它是空的。

```
ipsec_router#show crypto ipsec sa

interface: Ethernet1/0

        Crypto map tag: vpn, local addr. 30.30.30.1

        protected vrf:

         local ident (addr/mask/prot/port): (192.168.20.0/255.255.255.0/0/0)

        remote ident (addr/mask/prot/port): (172.16.0.0/255.255.0.0/0/0)

        current_peer: 20.20.20.1:500
```

```
 PERMIT, flags={origin_is_acl,}
 #pkts encaps: 145, #pkts encrypt: 145, #pkts digest 145
 #pkts decaps: 51, #pkts decrypt: 51, #pkts verify 51
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 0, #pkts compr. failed: 0
 #pkts not decompressed: 0, #pkts decompress failed: 0
 #send errors 6, #recv errors 0
 local crypto endpt.: 30.30.30.1, remote crypto endpt.: 20.20.20.1
 path mtu 1500, media mtu 1500
 current outbound spi: 54FA9805
inbound esp sas:
spi: 0x4091292(67703442)
 transform: esp-256-aes esp-md5-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 2000, flow_id: 1, crypto map: vpn
 sa timing: remaining key lifetime (k/sec): (4471883/28110)
 IV size: 16 bytes
 replay detection support: Y
inbound ah sas:
inbound pcp sas:
 outbound esp sas:
spi: 0x54FA9805(1425709061)
 transform: esp-256-aes esp-md5-hmac ,
 in use settings ={Tunnel, }
 slot: 0, conn id: 2001, flow_id: 2, crypto map: vpn
 sa timing: remaining key lifetime (k/sec): (4471883/28110)
 IV size: 16 bytes
 replay detection support: Y
outbound ah sas:
outbound pcp sas:
```

- **show crypto engine connections active** — 顯示所有加密引擎的當前活動加密會話連線。每個連線ID都是唯一的。加密和解密的資料包數量顯示在最後兩列中。

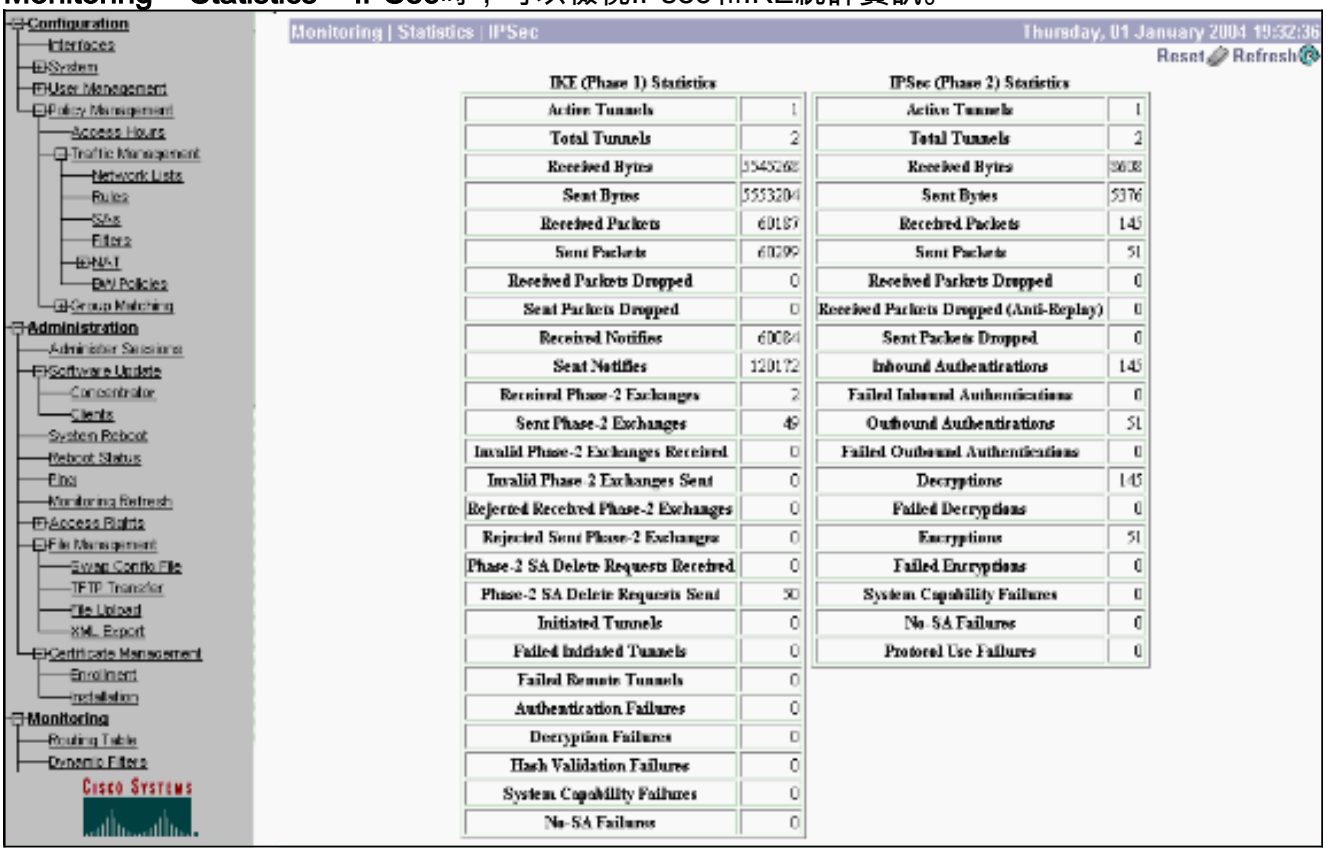
```
ipsec_router#show crypto engine connections active
   ID     Interface     IP-Address   State   Algorithm          Encrypt Decrypt
```

1	Ethernet1/0	30.30.30.1	set	HMAC_SHA+AES_256_C	0	0
2000	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	0	19
2001	Ethernet1/0	30.30.30.1	set	HMAC_MD5+AES_256_C	19	0

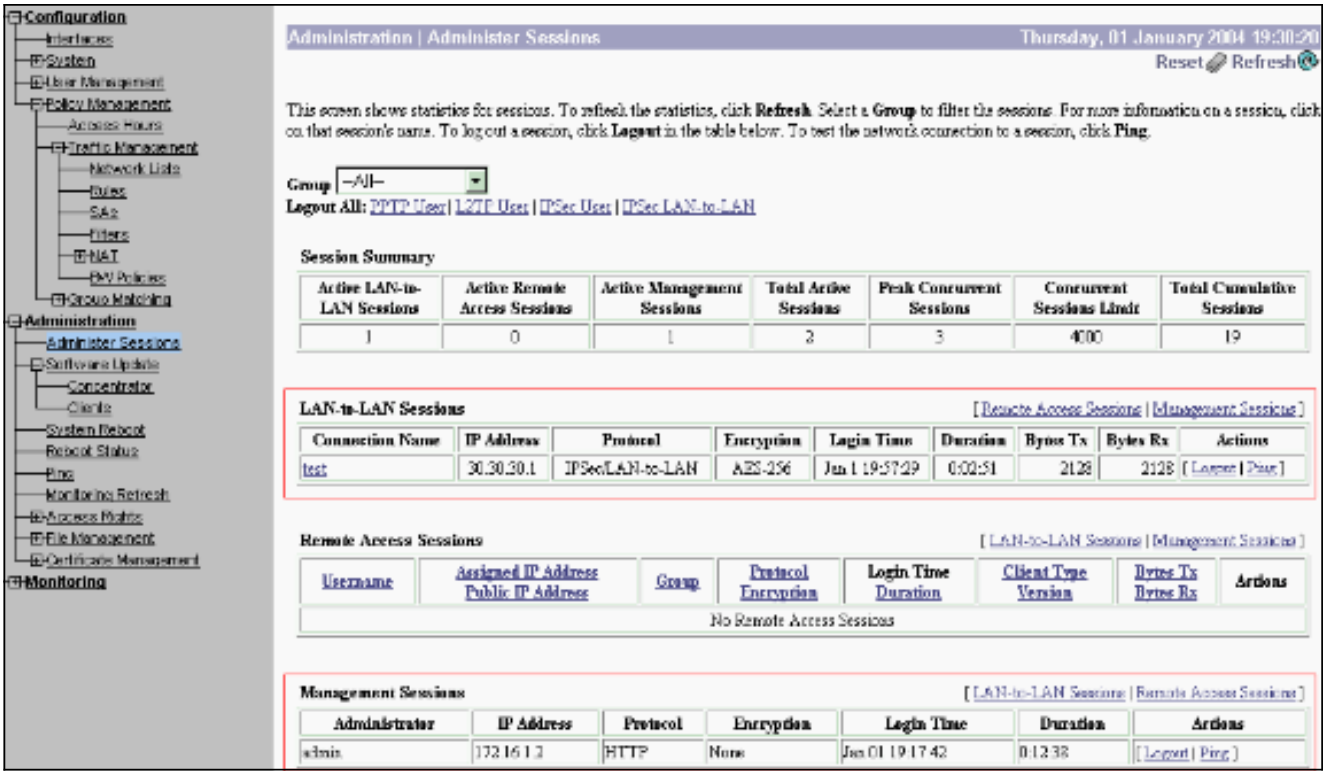
驗證VPN集中器配置

完成以下步驟以驗證VPN集中器配置。

1. 與路由器上的show crypto ipsec sa和**show crypto isakmp sa**命令類似，在VPN集中器上選擇**Monitoring > Statistics > IPSec**時，可以檢視IPsec和IKE統計資訊。



2. 與路由器上的**show crypto engine connections active**命令類似，可以使用VPN集中器上的Administration-Sessions視窗檢視所有活動IPsec LAN到LAN連線或通道的引數和統計資訊。



疑難排解

本節提供的資訊可用於對組態進行疑難排解。

路由器故障排除

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。

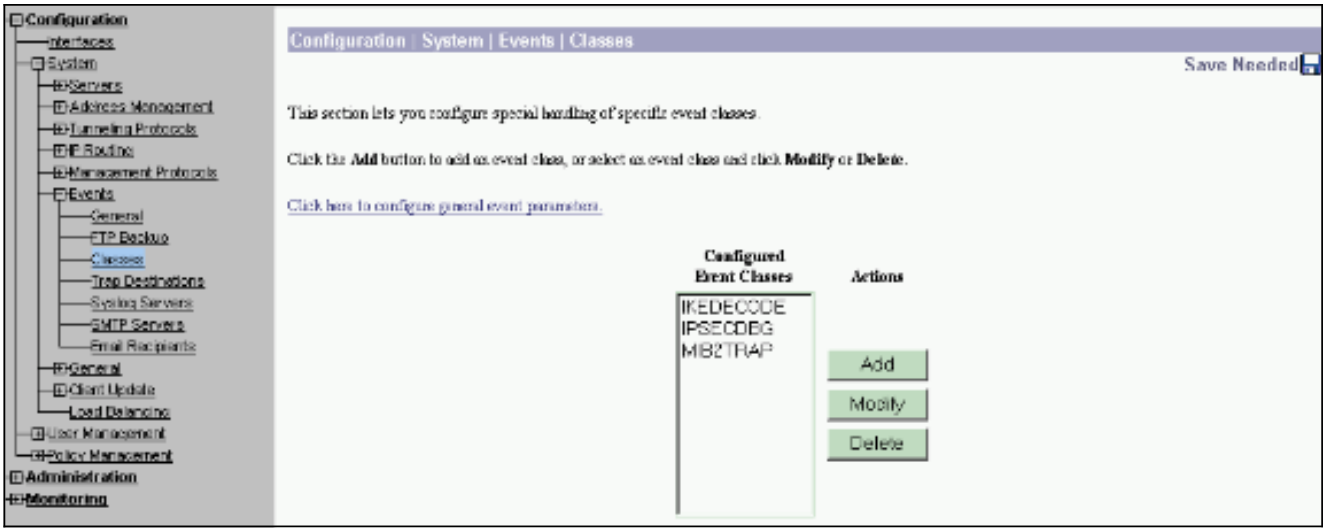
- **debug crypto engine** — 顯示加密的流量。加密引擎是執行加密和解密的實際機制。加密引擎可以是軟體或硬體加速器。
- **debug crypto isakmp** — 顯示IKE第1階段的網際網路安全關聯和金鑰管理協定(ISAKMP)協商。
- **debug crypto ipsec** — 顯示IKE第2階段的IPsec協商。

如需更多詳細資訊和範例輸出，請參閱IPSec疑難排解 — 瞭解和使用debug命令。

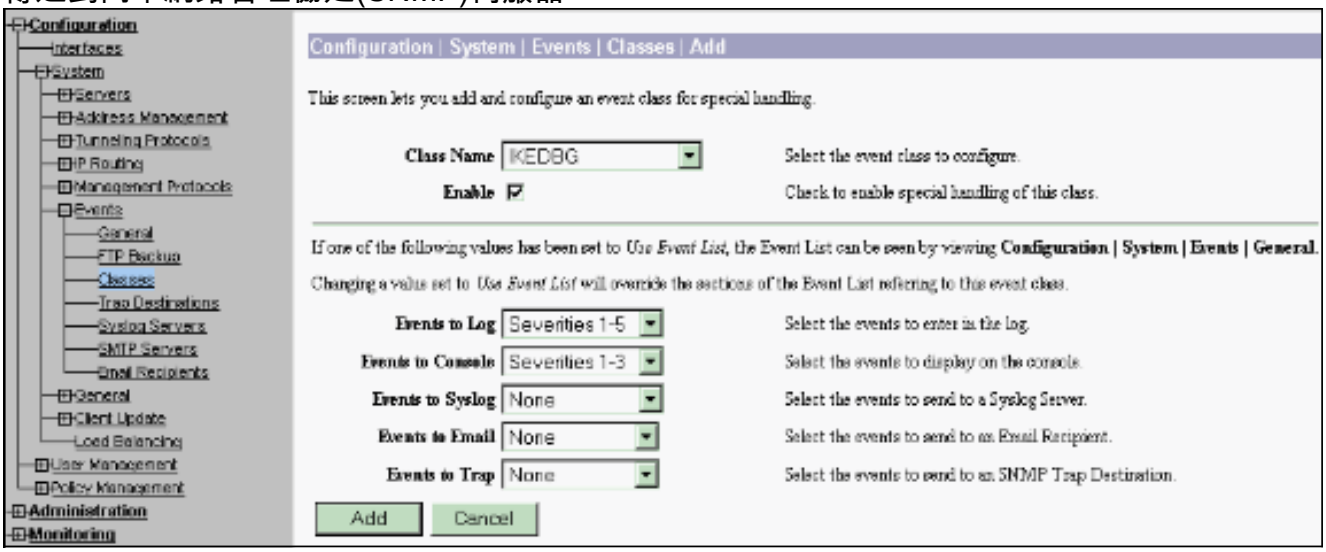
排除VPN集中器故障

與Cisco路由器上的**debug**命令類似，您可以配置事件類以檢視所有警報。

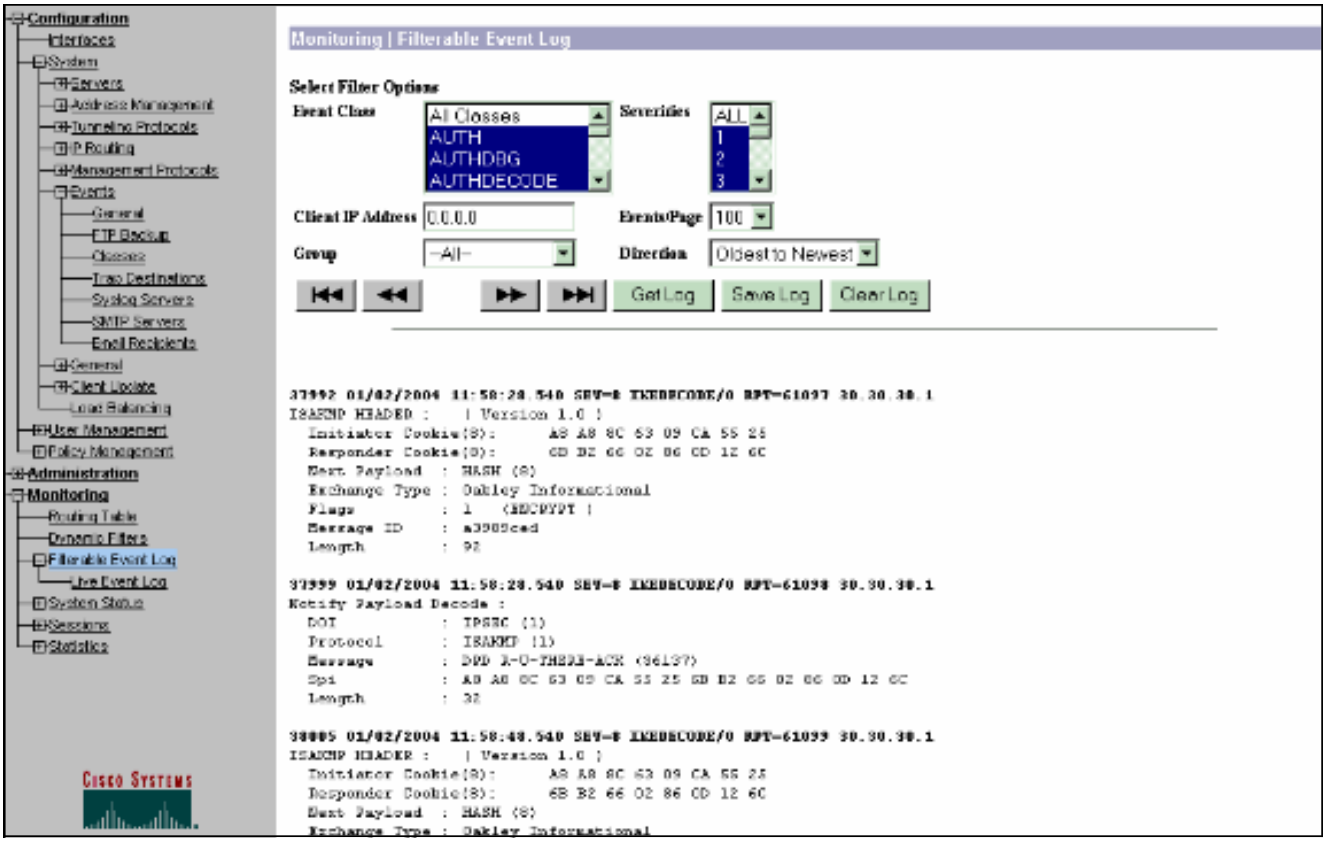
1. 選擇Configuration > **System** > **Events** > **Classes** > **Add**以開啟事件類的日誌記錄。以下類可用於IPsec:IKEIKEDBGIKEDECODEIPSECIPSECDBGIPSECDECODE



2. 新增時，您還可以根據警報傳送的嚴重性級別選擇每個類的嚴重性級別。可通過以下方法之一處理警報：按日誌顯示在控制檯上傳送到UNIX系統日誌伺服器作為電子郵件傳送以陷阱形式傳送到簡單網路管理協定(SNMP)伺服器



3. 選擇**Monitoring > Filterable Event Log**以監視已啟用的警報。



相關資訊

- 進階加密標準(AES)
- DES/3DES/AES VPN加密模組
- IPSec示例配置
- Cisco VPN 3000系列使用者端支援頁面
- IPSec協商/IKE通訊協定支援頁面