使用WLC的無線LAN的客戶端VPN配置示例

目錄

簡介

本檔案介紹無線環境中虛擬私人網路(VPN)的概念。本檔案介紹透過無線LAN控制器(WLC)在無線使用者端和VPN伺服器之間部署VPN通道時涉及的組態。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- 瞭解WLC以及如何設定WLC基本引數
- Wi-Fi保護訪問(WPA)概念知識
- VPN基本知識及其型別
- IPsec知識
- 有關可用的加密、驗證和雜湊演算法的基本知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco 2006 WLC（執行版本4.0.179.8）
- Cisco 1000系列輕量型存取點(LAP)
- 執行Cisco IOS®軟體版本12.4(8)的Cisco 3640
- Cisco VPN使用者端版本4.8

注意：本文檔使用3640路由器作為VPN伺服器。為了支援更高級的安全功能，您還可以使用專用的VPN伺服器。

注意：要使路由器充當VPN伺服器，它需要運行支援基本IPsec的功能集。

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。

背景資訊

VPN是一種專用資料網路，用於在專用網路內通過公共電信基礎設施（例如網際網路）安全地傳輸資料。此VPN通過使用隧道協定和安全過程來維護資料隱私。

遠端存取VPN

遠端訪問VPN配置用於允許VPN軟體客戶端（例如移動使用者）安全地訪問駐留在VPN伺服器之後的集中網路資源。在思科術語中，這些VPN伺服器和客戶端也稱為Cisco Easy VPN伺服器和Cisco Easy VPN Remote裝置。

Cisco Easy VPN Remote裝置可以是Cisco IOS路由器、Cisco PIX安全裝置、Cisco VPN 3002硬體客戶端和Cisco VPN客戶端。它們用於在從Cisco Easy VPN伺服器進行VPN隧道連線時接收安全策略。這樣可最大程度地降低遠端位置的配置要求。Cisco VPN Client是一種可以安裝在PC、筆記型電腦等上的軟體客戶端。

Cisco Easy VPN伺服器可以是Cisco IOS路由器、Cisco PIX安全裝置和Cisco VPN 3000集中器。

本文檔使用在筆記型電腦上運行的Cisco VPN客戶端軟體作為VPN客戶端，Cisco 3640 IOS路由器作為VPN伺服器。本文檔使用IPsec標準在客戶端和伺服器之間建立VPN隧道。

IPsec

IPsec是由Internet工程任務組(IETF)開發的開放式標準框架。IPsec為通過未受保護的網路（例如Internet）傳輸敏感資訊提供了安全性。

IPsec在IP封包層級提供網路資料加密，藉此提供基於標準的健全資安解決方案。IPsec的主要任務是允許通過不安全的連線交換專用資訊。IPsec使用加密保護資訊免遭攔截或竊聽。但是，為了有效使用加密，雙方應共用一個用於資訊加密和解密的金鑰。

IPsec分兩個階段運行，允許對共用金鑰進行機密交換：

- 階段1 — 處理兩個IPsec對等體之間建立安全通道所需的安全引數的協商。階段1通常通過網際網路金鑰交換(IKE)協定實施。如果遠端IPsec對等體無法執行IKE，則可以使用預共用金鑰的手

動配置來完成第1階段。
- 階段2 — 使用階段1中建立的安全隧道交換實際傳輸使用者資料所需的安全引數。IPsec的兩個階段中使用的安全隧道基於每個IPsec端點使用的安全關聯(SA)。SA描述安全引數，例如兩端都同意使用的身份驗證和加密型別。

在第2階段中交換的安全引數用於建立IPsec隧道，IPsec隧道又用於在VPN客戶端和伺服器之間進行資料傳輸。

有關IPsec及其配置的詳細資訊，請參閱配置IPsec。

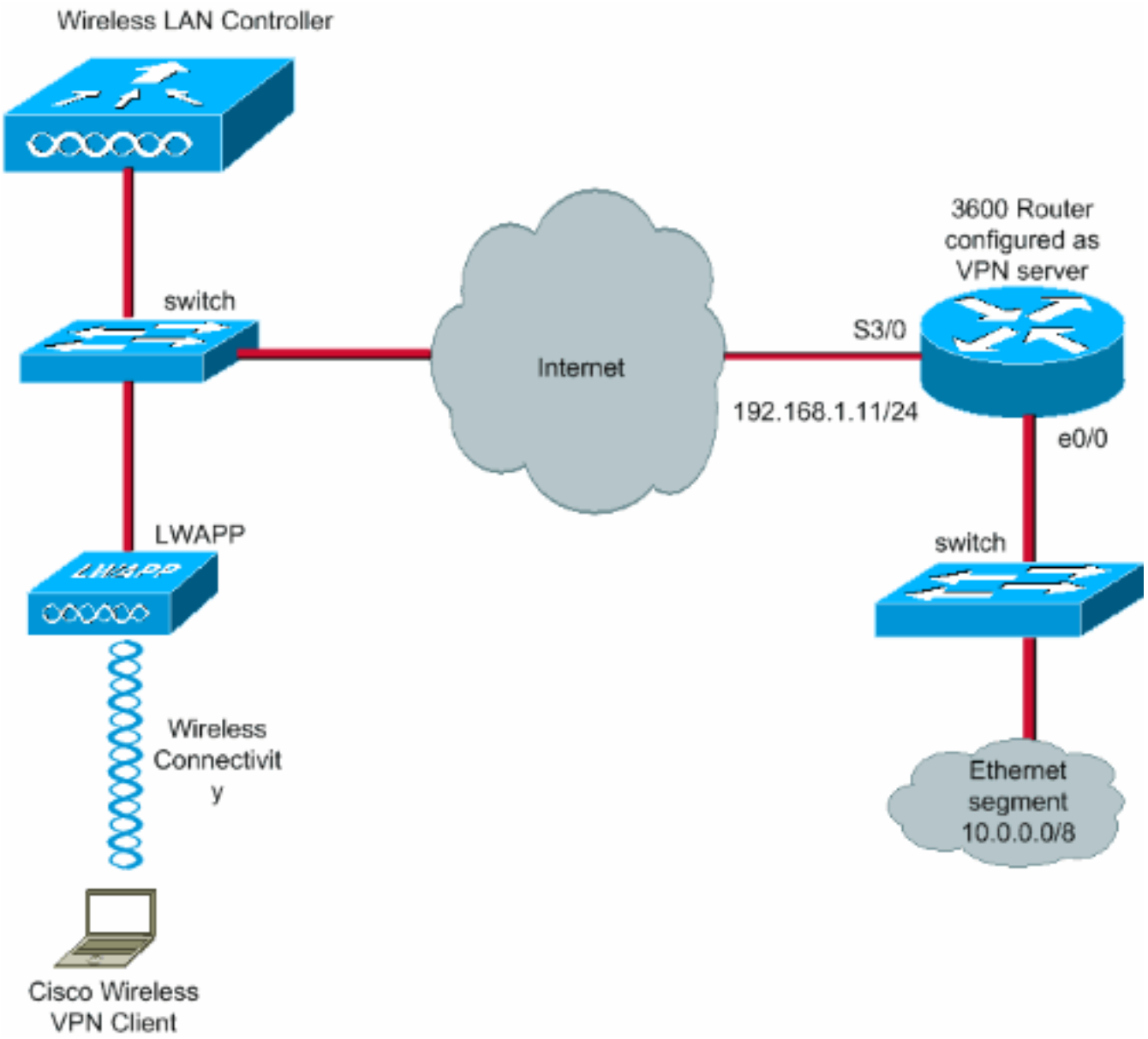
一旦在VPN客戶端和伺服器之間建立VPN隧道，*在VPN伺服器上定義的安全策略將傳送到客戶端*。這樣可最大程度地降低客戶端的配置要求。

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

本檔案會使用以下設定：

- WLC的管理介面IP地址 — 172.16.1.10/16
- AP-manager介面WLC的IP地址 — 172.16.1.11/16
- 預設網關 — 172.16.1.20/16**注意：**在即時網路中，此預設網關應指向直接路由器的傳入介面，該介面將WLC連線到網路的其餘部分和/或連線到Internet。
- VPN伺服器的IP地址s3/0 - 192.168.1.11/24**注意：**此IP地址應指向在VPN伺服器端終止VPN隧道的介面。在本示例中，s3/0是終止VPN伺服器上的VPN隧道的介面。
- VPN伺服器上的LAN網段使用10.0.0.0/8的IP地址範圍。



設定

在WLAN集中架構中，為了允許無線VPN客戶端（例如筆記型電腦）與VPN伺服器建立VPN隧道，客戶端必須與輕量型接入點(LAP)關聯，而輕量型接入點則需向WLC註冊。本檔案的LAP已透過使用輕量AP(LAP)註冊到無線LAN控制器(WLC)中說明的本地子網廣播探索程式註冊到WLC。

下一步是為VPN配置WLC。

VPN終端和傳輸

使用低於版本4的Cisco 4000系列WLC時，支援稱為IPsec VPN終止（IPsec支援）的功能。此功能可讓這些控制器直接在控制器上終止VPN客戶端會話。總而言之，此功能使控制器本身可以充當VPN伺服器。但這需要在控制器中安裝單獨的VPN終端硬體模組。

以下IPsec VPN支援不可用：

- Cisco 2000系列WLC
- 執行4.0版或更新版本的所有WLC

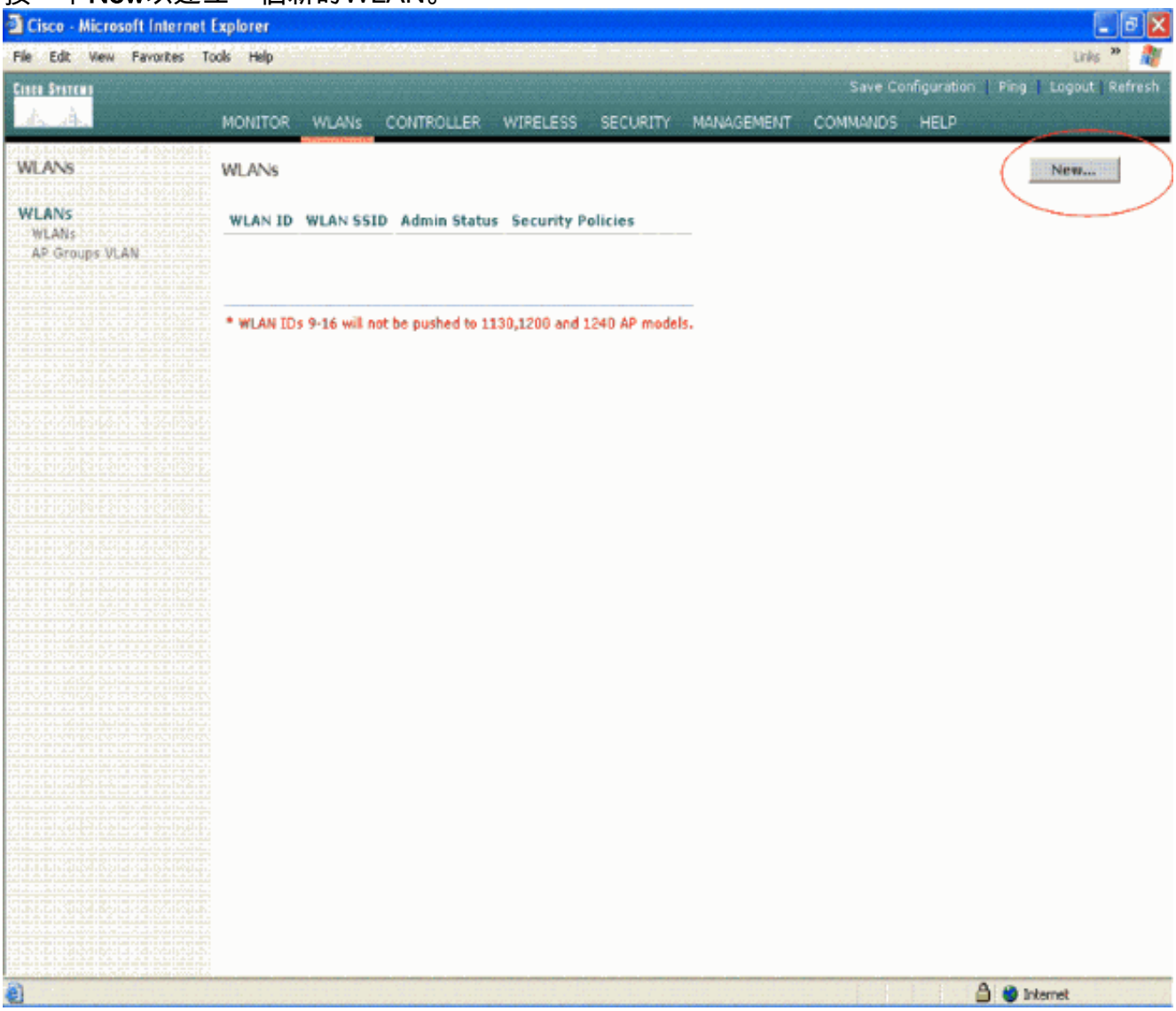
因此，4.0版本以後支援的唯一VPN功能是VPN傳輸。Cisco 2000系列WLC也支援此功能。

VPN傳遞是一種功能，允許客戶端僅與特定VPN伺服器建立隧道。因此，如果您需要安全訪問配置的VPN伺服器以及另一個VPN伺服器或網際網路，則無法在控制器上啟用VPN傳遞的情況下實現這一點。根據此類要求，您需要禁用VPN傳輸。但是，當建立適當的ACL並將其應用到對應的WLAN時，可以將WLC配置為直通以到達多個VPN網關。因此，在希望到達多個VPN網關以實現冗餘的情況下，請禁用VPN傳輸，並建立允許訪問VPN網關的ACL並將ACL應用於WLAN。

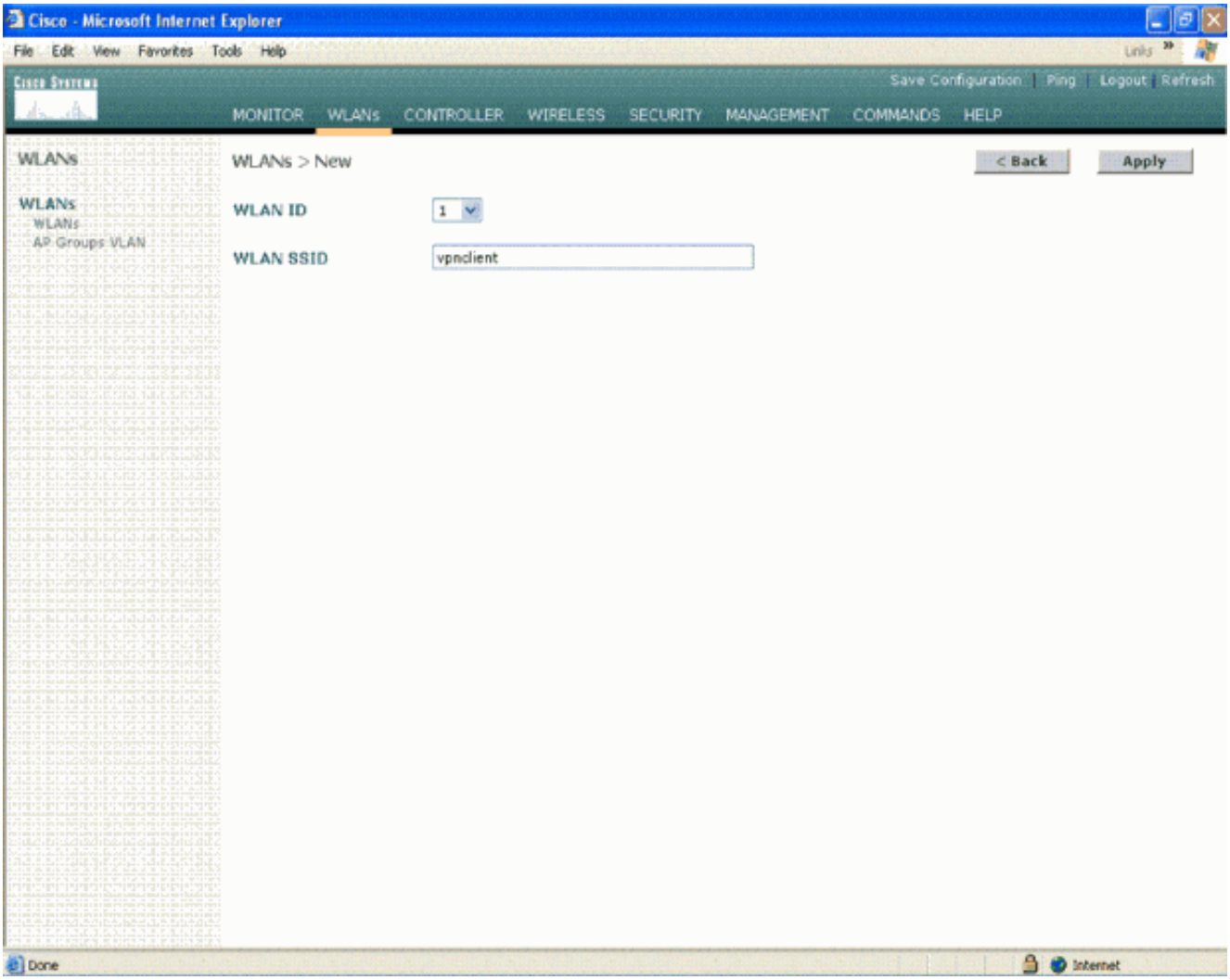
為VPN直通配置WLC

完成以下步驟以配置VPN傳輸。

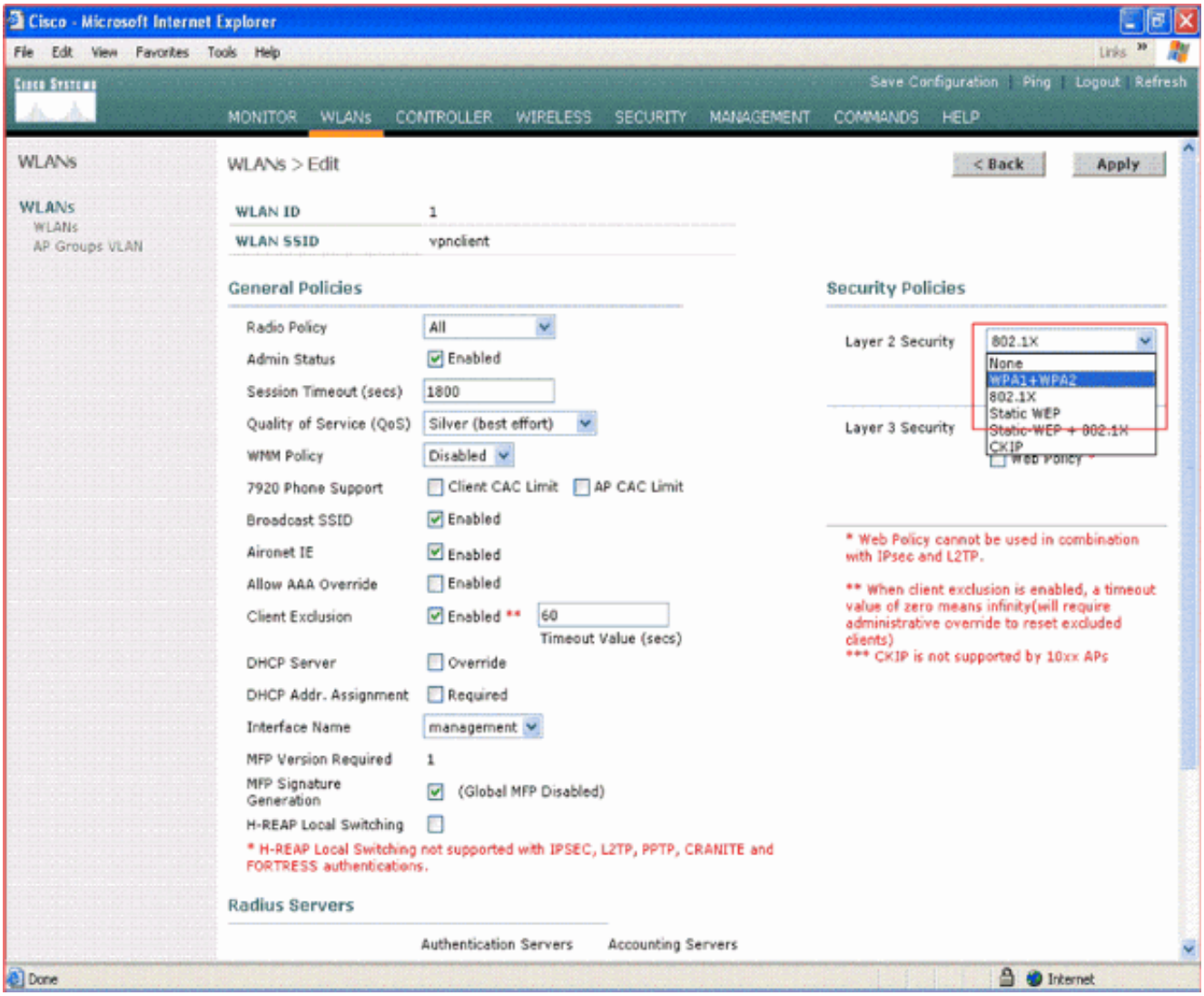
1. 在WLC GUI中，按一下**WLAN**以進入WLANs頁面。
2. 按一下**New**以建立一個新的WLAN。



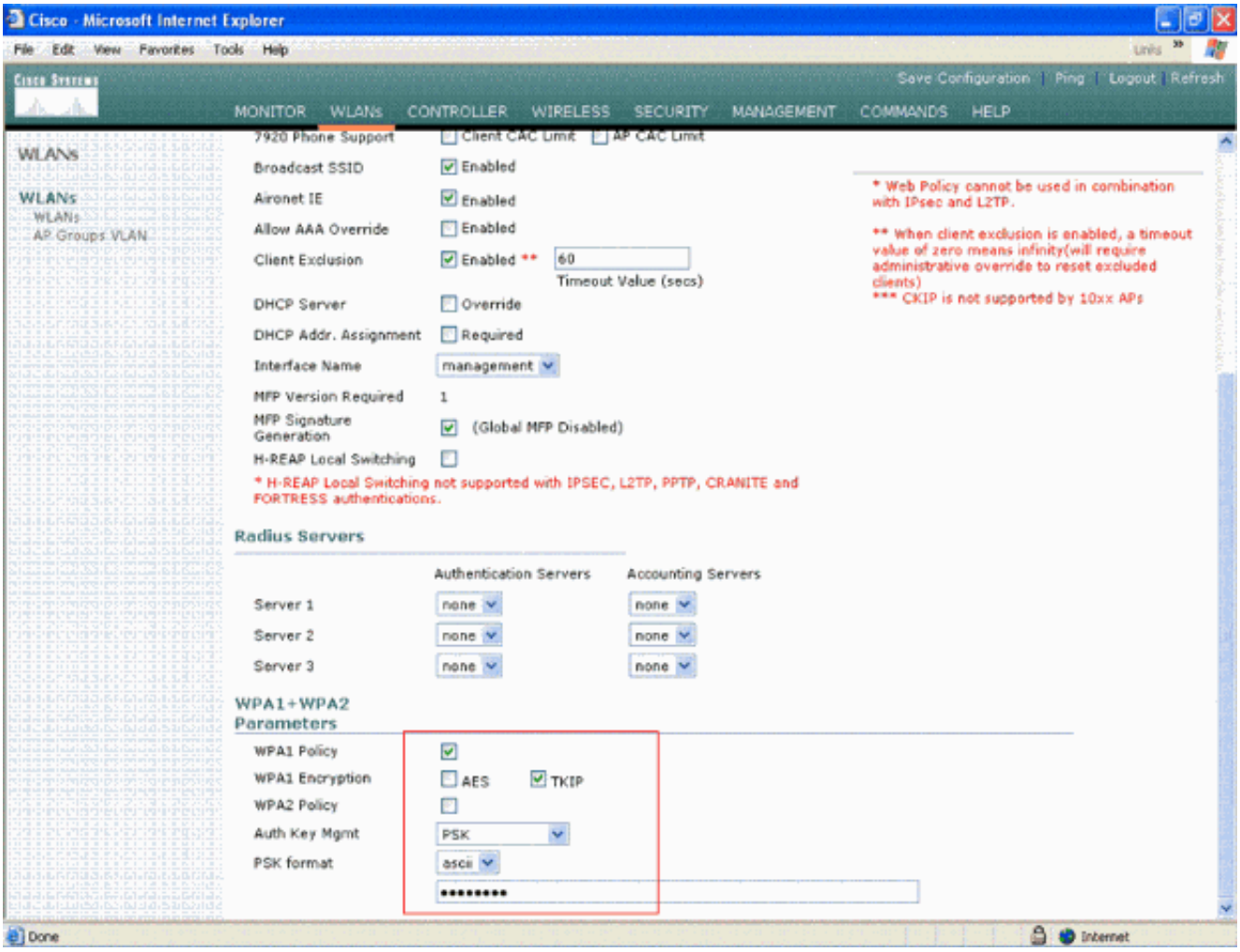
3. 在此示例中，WLAN SSID命名為 **vpnclient**。按一下「Apply」。



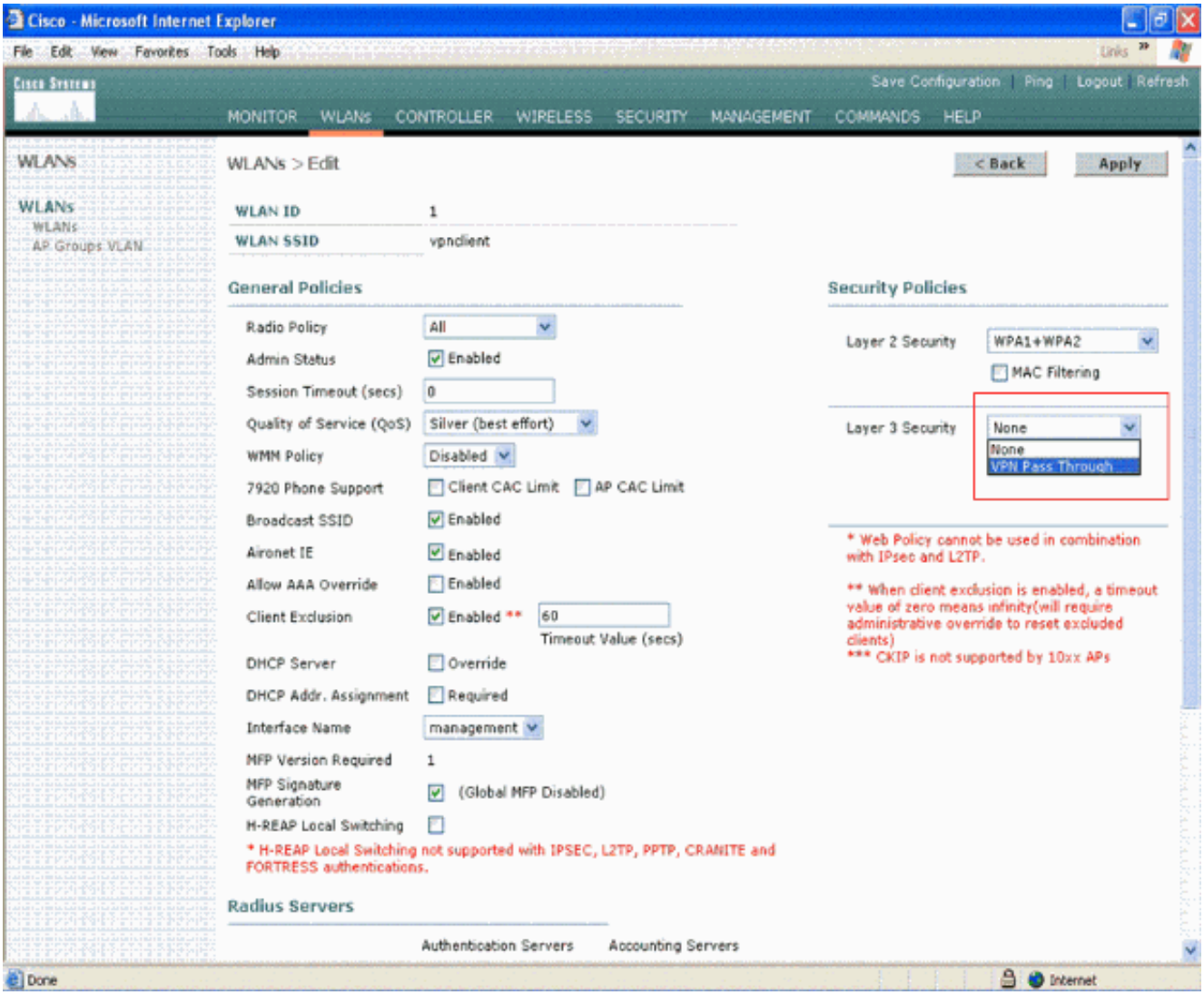
4. 使用第2層安全配置vpnclient SSID。*這是選用的*。本示例使用**WPA1+WPA2**作為安全型別。



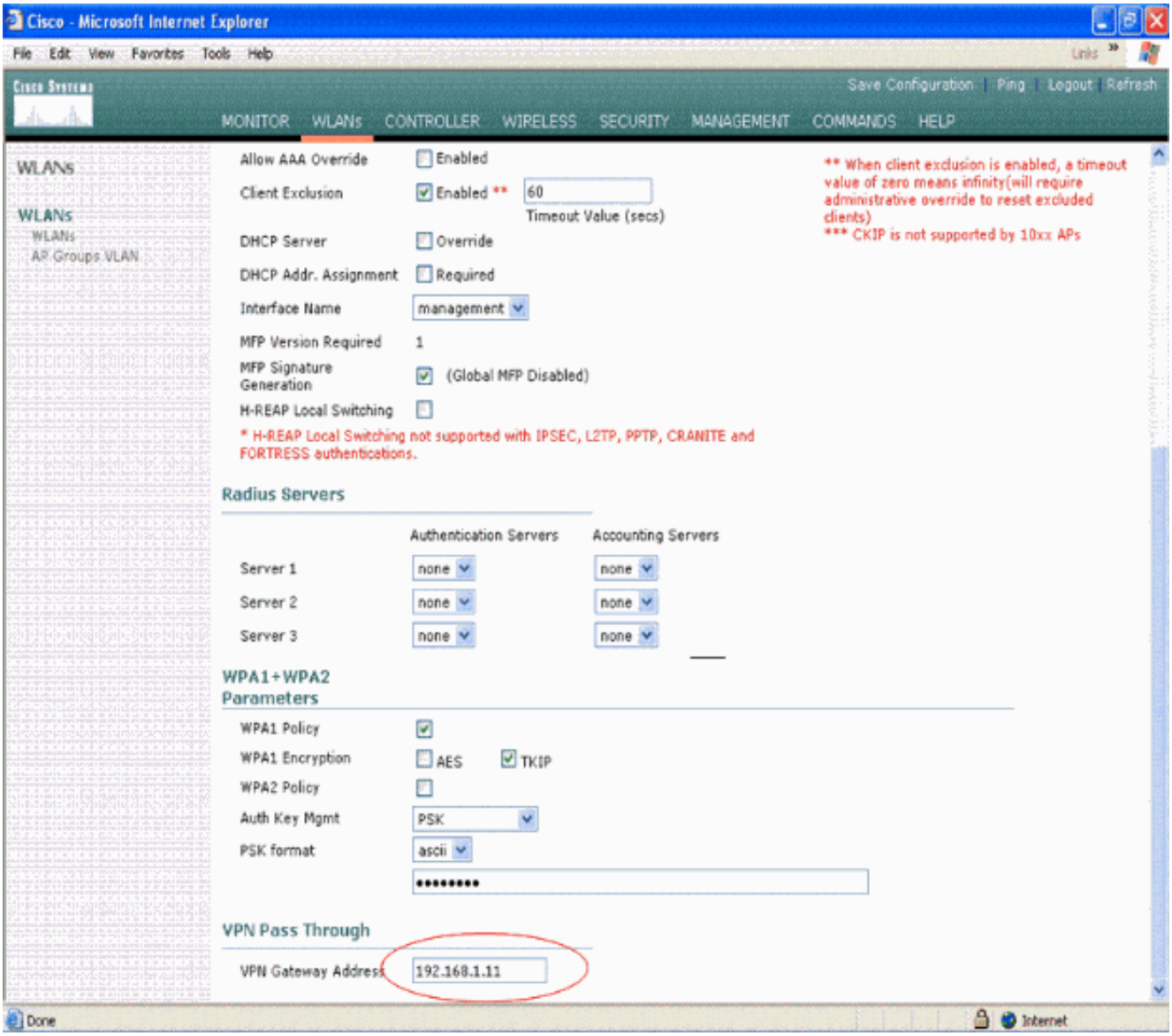
5. 配置要使用的WPA策略和身份驗證金鑰管理型別。此範例將**預先共用金鑰(PSK)用於**驗證金鑰管理。選擇PSK後，選擇**ASCII**作為PSK格式並鍵入PSK值。此值在無線客戶端的SSID配置中應該相同，以便屬於此SSID的客戶端與此WLAN關聯。



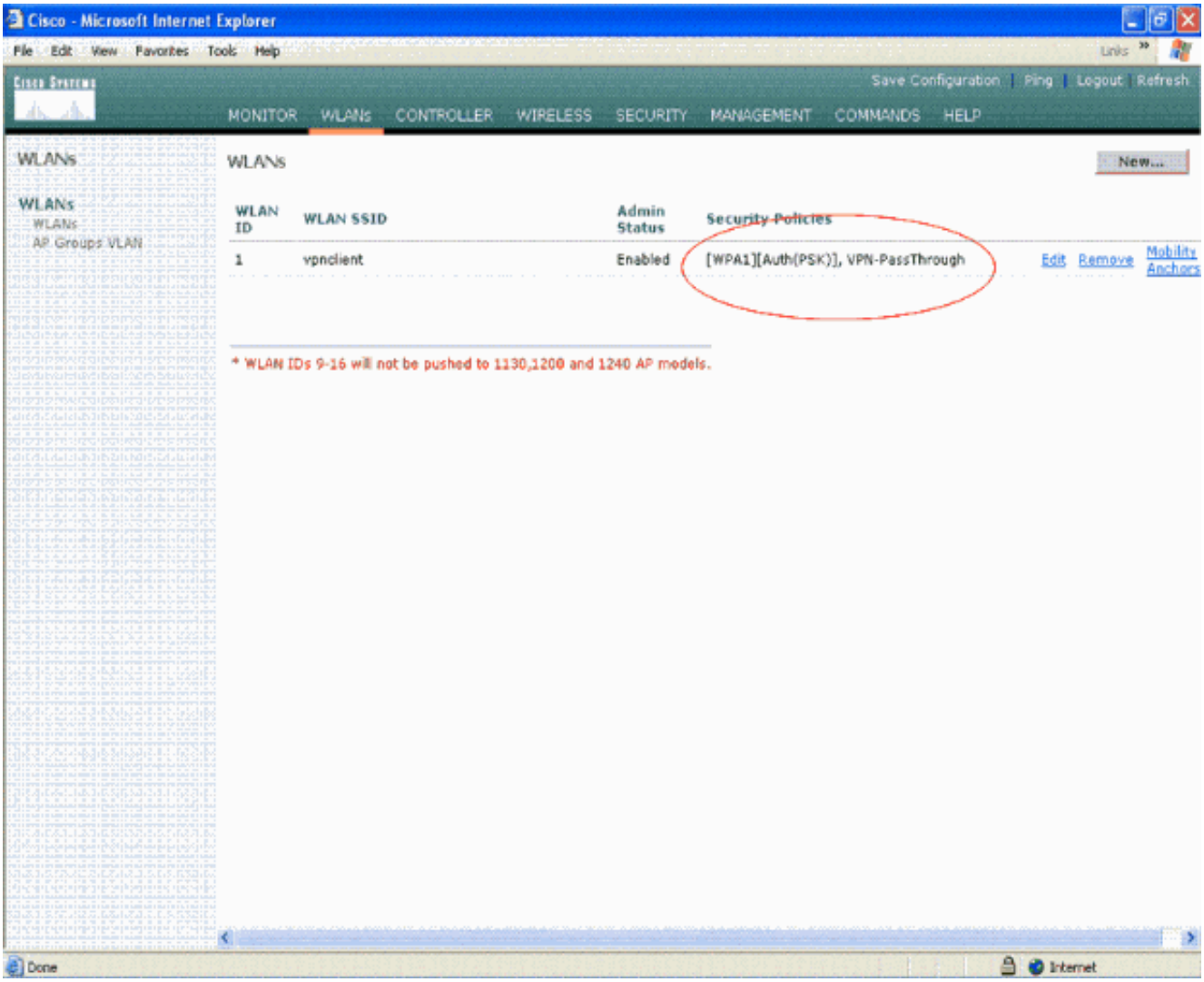
6. 選擇**VPN Pass-through**作為Layer 3 Security。以下提供範例。



7. 選擇VPN直通作為第3層安全後，新增VPN網關地址，如以下示例所示。此網關地址應為終止伺服器端VPN通道的介面的IP地址。在本示例中，VPN伺服器上的s3/0介面(192.168.1.11/24)的IP地址是要配置的網關地址。



8. 按一下「**Apply**」。現在將名為*vpnclient*的WLAN配置為VPN傳輸。



VPN伺服器配置

此配置顯示Cisco 3640路由器為VPN伺服器。

注意：為簡單起見，此配置使用靜態路由來維護端點之間的IP可達性。您可以使用任何動態路由協定(如路由資訊協定(RIP)、開放最短路徑優先(OSPF)等)來保持可達性。

注意：如果客戶端與伺服器之間沒有IP可達性，則不會建立隧道。

注意：本文檔假定使用者知道如何在網路中啟用動態路由。

思科3640路由器

```
vpnrouter#show running-config

Building configuration...

Current configuration : 1623 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname vpnrouter
```

```
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authorization network employee local
!
aaa session-id common
!
resource policy
!
memory-size iomem 10
!
!
ip cef
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
crypto isakmp policy 1
!--- Create an Internet Security Association and Key
Management !--- Protocol (ISAKMP) policy for Phase 1
negotiation. hash md5
!--- Choose the hash algorithm to be md5. authentication
pre-share
!--- The authentication method selected is pre-shared.
group 2
!--- With the group command, you can declare what size
modulus to !--- use for Diffie-Hellman calculation.
Group 1 is 768 bits long, !--- and group 2 is 1024 bits
long.


crypto isakmp client configuration group employee key
cisco123 pool mypool
!
!--- Create the Phase 2 policy for actual data
encryption. crypto ipsec transform-set myset esp-3des
esp-md5-hmac
!--- Create a dynamic map and apply the transform set
that was created. !--- Set reverse-route for the VPN
server. crypto dynamic-map mymap 10 set transform-set
myset reverse-route
!
crypto map clientmap isakmp authorization list employee
!--- Create the crypto map.
```

```
crypto map clientmap client configuration address crypto
map clientmap 10 ipsec-isakmp dynamic mymap
!
!--- Apply the employee group list that was created
earlier.



!
!
!
!
interface Ethernet0/0
 ip address 10.0.0.20 255.0.0.0
 half-duplex
!
interface Serial3/0
 ip address 192.168.1.11 255.255.255.0
 clock rate 64000
 no fair-queue
 crypto map clientmap
!--- Apply the crypto map to the interface. ! interface
Serial3/1 no ip address shutdown ! interface Serial3/2
no ip address shutdown ! interface Serial3/3 no ip
address shutdown ! interface Serial3/4 no ip address
shutdown ! interface Serial3/5 no ip address shutdown !
interface Serial3/6 no ip address shutdown ! interface
Serial3/7 no ip address shutdown ip local pool mypool
10.0.0.50 10.0.0.60
!--- Configure the Dynamic Host Configuration Protocol
!--- (DHCP) pool which assigns the tunnel !--- IP
address to the wireless client. !--- This tunnel IP
address is different from the IP address !--- assigned
locally at the wireless client (either statically or
dynamically). ip http server no ip http secure-server !
ip route 172.16.0.0 255.255.0.0 192.168.1.10 ! ! ! !
control-plane ! ! ! ! ! ! ! ! ! line con 0 line aux 0
line vty 0 4 ! ! end ip subnet-zero . . . ! end
```

注意：此示例僅使用組身份驗證。它不使用單個使用者身份驗證。

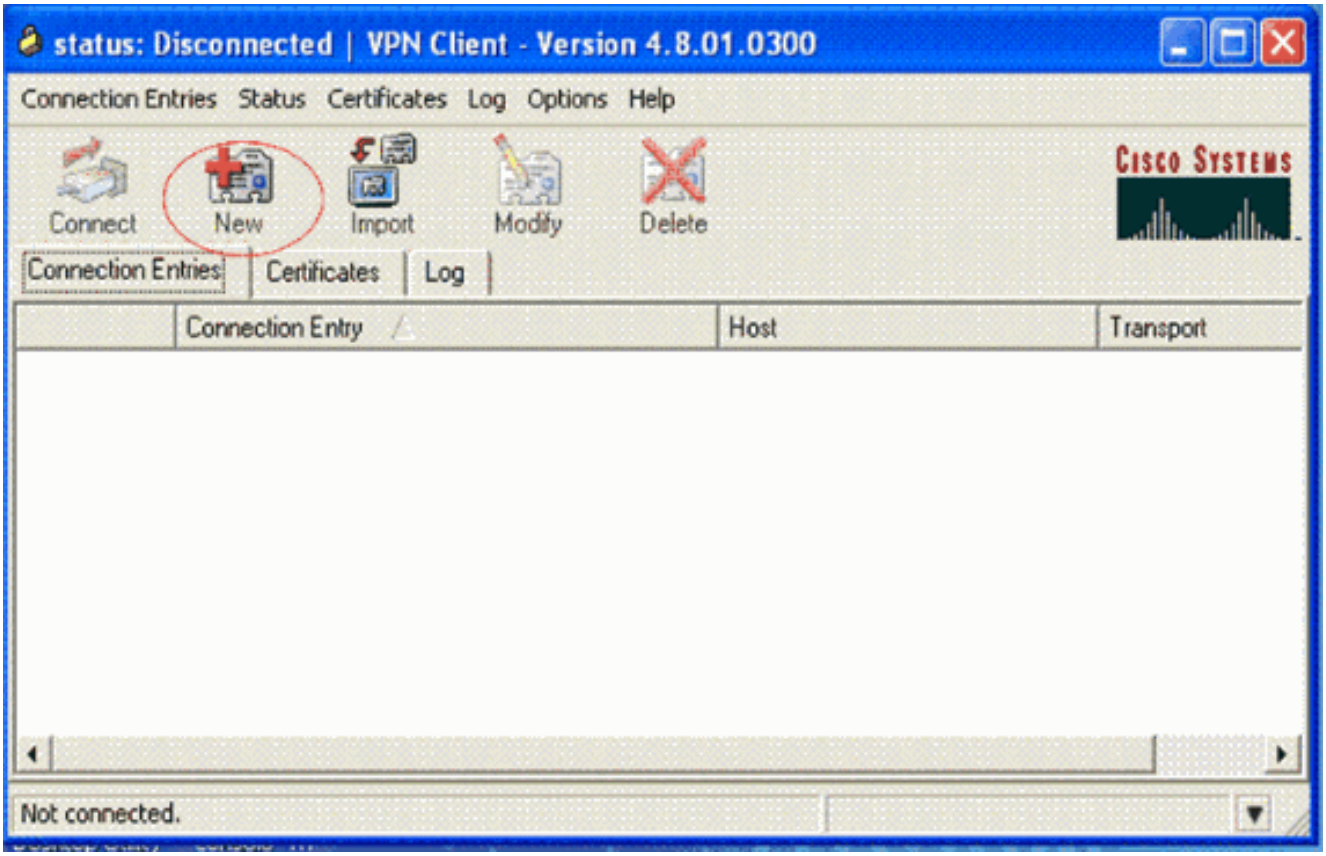
VPN客戶端配置

可從Cisco.com Software Center下載軟體VPN客戶端。

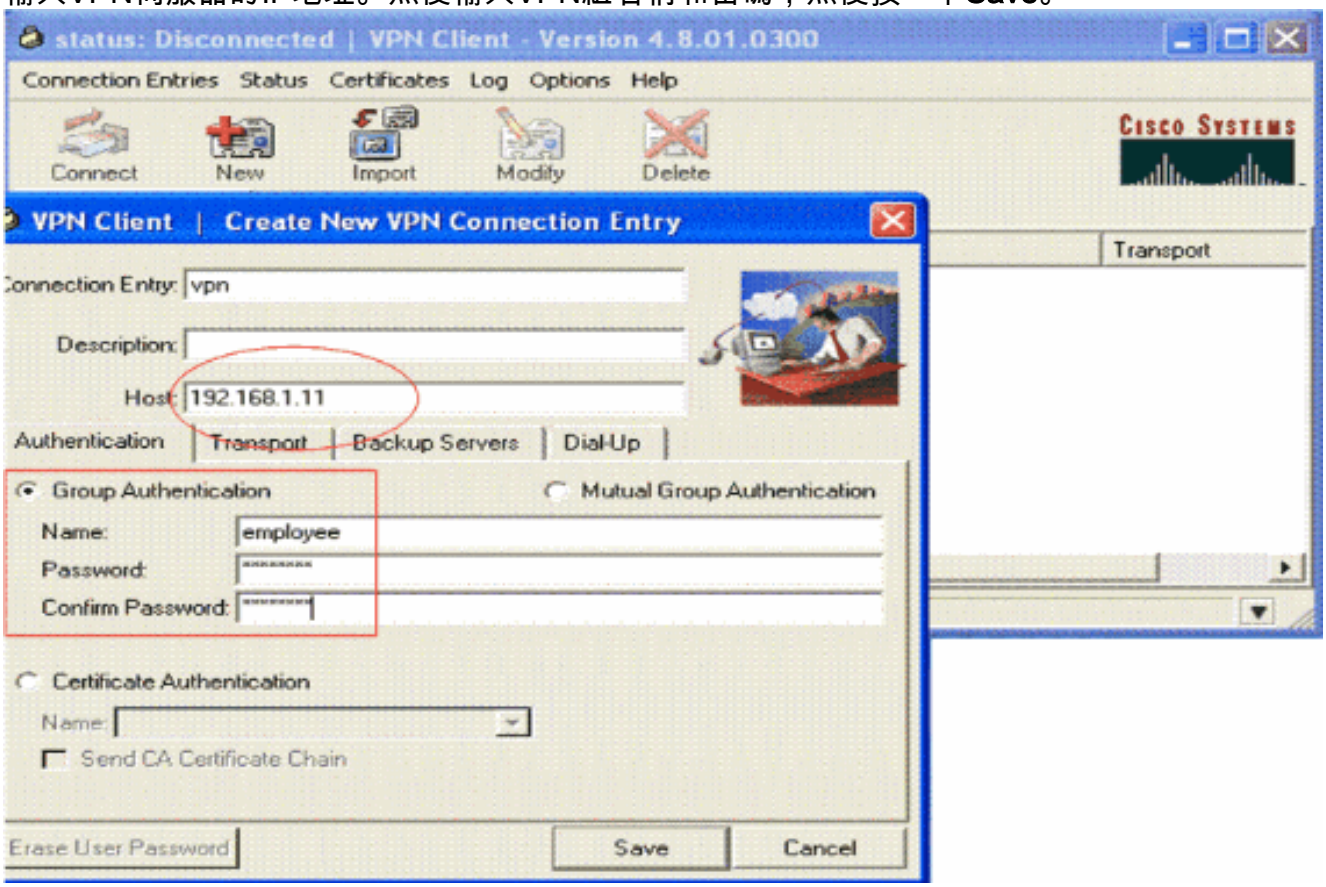
注意：某些思科軟體要求您使用CCO使用者名稱和密碼登入。

完成以下步驟以配置VPN客戶端。

1. 從無線客戶端（筆記型電腦）中選擇**開始>程式> Cisco Systems VPN客戶端> VPN客戶端**以訪問VPN客戶端。這是VPN客戶端的預設安裝位置。
2. 按一下**New**以啟動Create New VPN Connection Entry視窗。



3. 輸入連線條目的名稱和說明。本示例使用*esvpn*。Description欄位可選。在Host（主機）框中輸入VPN伺服器的IP地址。然後輸入VPN組名稱和密碼，然後按一下**Save**。



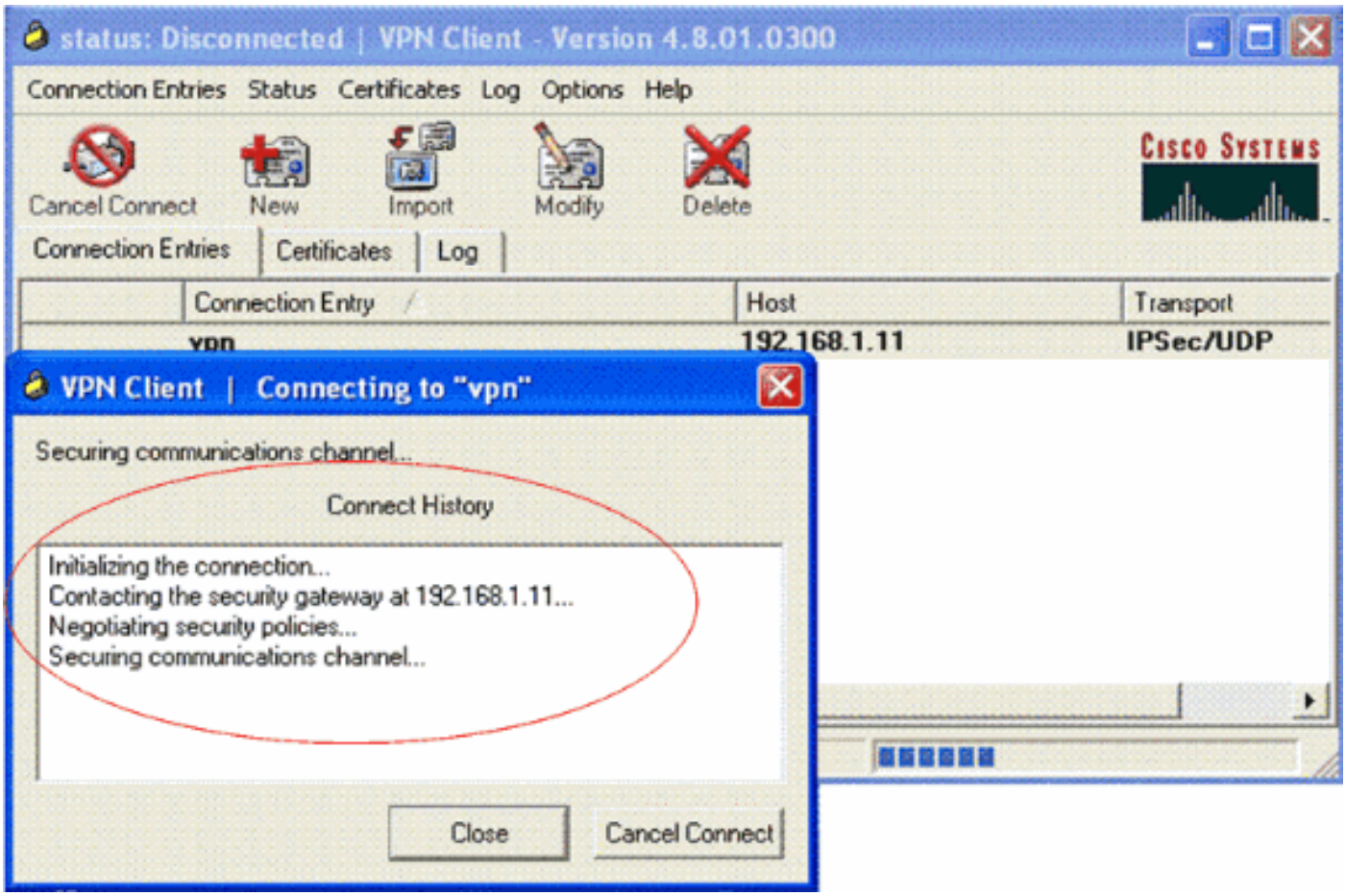
注意：此處配置的組名稱和密碼應與VPN伺服器中配置的組名稱和密碼相同。本示例使用Name *employee*和Password *cisco123*。

驗證

若要驗證此設定，請使用在WLC中設定的相同安全引數在無線使用者端中設定SSID **vpnclient**，並將使用者端與此WLAN相關聯。以下幾個文檔說明了如何使用新配置檔案配置無線客戶端。

關聯無線客戶端後，轉至VPN客戶端，然後按一下已配置的連線。然後在VPN客戶端主視窗中按一下**Connect**。

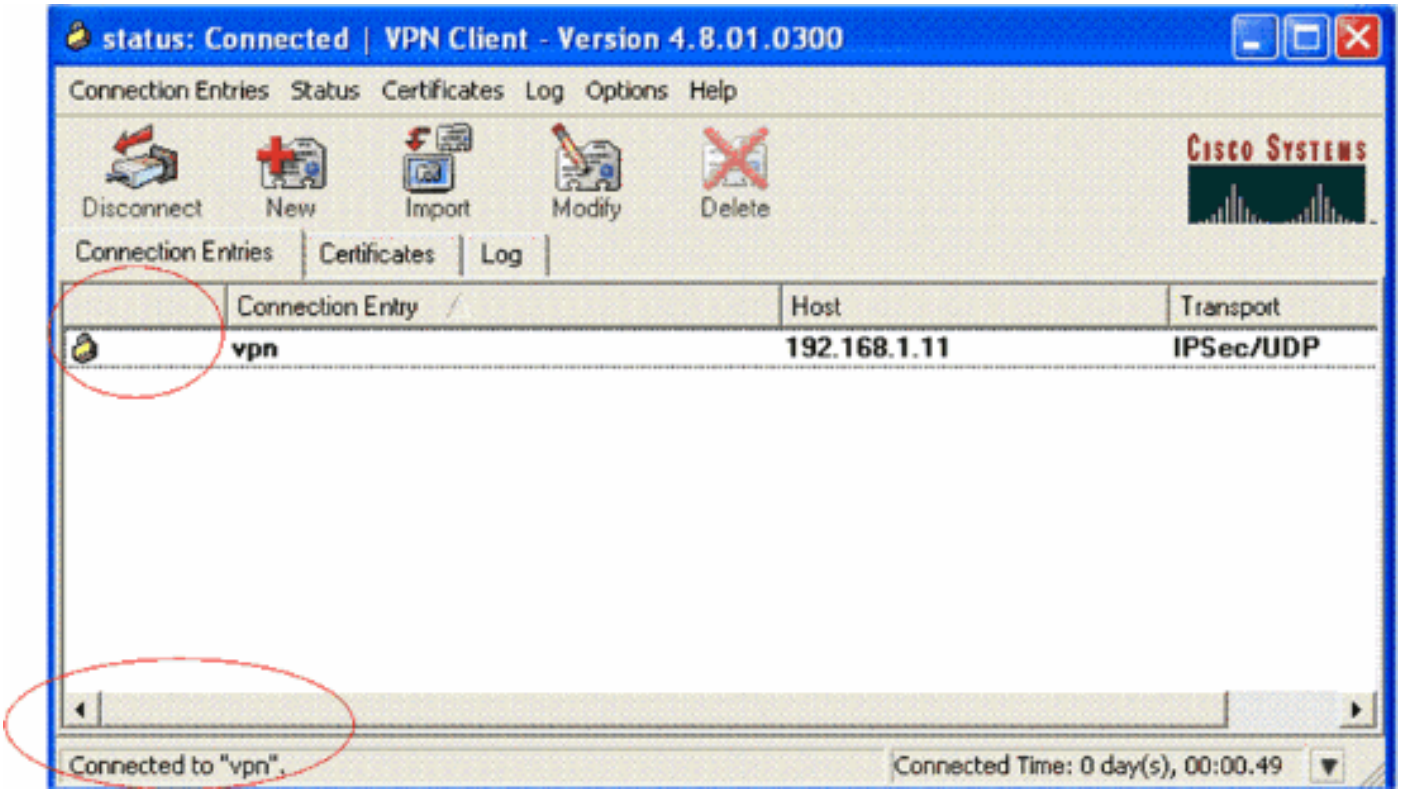
您可以看到客戶端和伺服器之間協商的第1階段和第2階段安全引數。



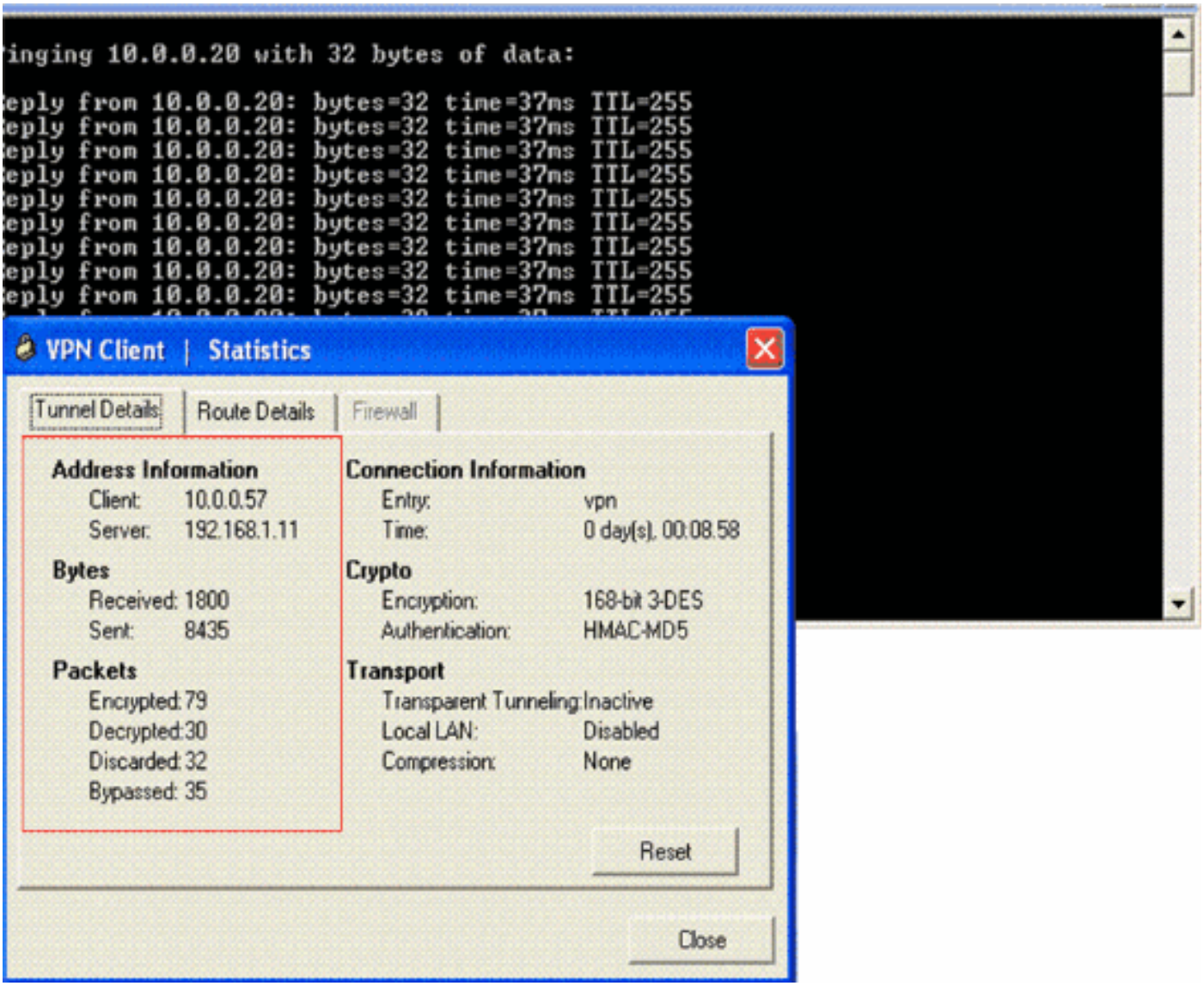
注意：為了建立此VPN隧道，VPN客戶端和伺服器之間應具有IP可達性。如果VPN客戶端無法與安全網關（VPN伺服器）聯絡，則隧道未建立，客戶端將顯示一個警報框，並顯示以下消息：

```
Reason 412: The remote peer is no longer responding
```

為了確保正確建立客戶端和伺服器之間的VPN隧道，您可以找到在已建立VPN客戶端旁建立的鎖定圖示。狀態列也顯示**Connected to "vpn"**。 以下提供範例。



此外，請確保您能夠從VPN客戶端成功將資料傳輸到伺服器端的LAN網段，反之亦然。從VPN客戶端主選單中，選擇**Status > Statistics**。您可以在此找到透過通道的加密和解密封包的統計資料。



在此螢幕截圖中，您可以看到客戶端地址為10.0.0.57。這是VPN伺服器在成功的第1階段協商後從其本地配置的池中分配給客戶端的地址。隧道建立後，VPN伺服器會自動將路由新增到其路由表中的該分配的DHCP IP地址。

您還可以看到當資料從客戶端傳輸到伺服器時，加密資料包的數量在增加，而在反向資料傳輸過程中，解密資料包的數量在增加。

注意：由於WLC配置為通過VPN，因此它僅允許客戶端訪問與配置為通過的VPN網關（這裡為192.168.1.11 VPN伺服器）連線的網段。這將過濾所有其他流量。

可以通過使用相同配置配置另一個VPN伺服器並在VPN客戶端為該VPN伺服器配置新的連線條目來驗證這一點。現在，當您嘗試與此VPN伺服器建立隧道時，不會成功。這是因為WLC會過濾此流量，並僅允許通道到達為VPN傳遞設定的VPN閘道位址。

您也可以從VPN伺服器的CLI驗證配置。

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。

在VPN伺服器中使用的這些**show**命令也可用於幫助您驗證隧道狀態。

- show crypto session命令用於驗證通道狀態。以下是此命令的示例輸出。

```
Crypto session current status

Interface: Serial3/0
Session status: UP-ACTIVE
Peer: 172.16.1.20 port 500
  IKE SA: local 192.168.1.11/500 remote 172.16.1.20/500

Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.0.0.58
        Active SAs: 2, origin: dynamic crypto map
```

- show crypto isakmp policy用於檢視已配置的階段1引數。

疑難排解

Verify一節中說明的debug和show命令也可用於故障排除。

- debug crypto isakmp
- debug crypto ipsec
- show crypto session

- VPN伺服器上的debug crypto isakmp命令顯示客戶端和伺服器之間的整個第1階段協商過程。以下是成功的第1階段協商的範例。

```
---------------------------------------------------------------------
 -------------------------------------------------------------
---------------------------------------------------------------------
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 14
   against priority 1 policy
*Aug 28 10:37:29.515: ISAKMP:      encryption DES-CBC
*Aug 28 10:37:29.515: ISAKMP:      hash MD5
*Aug 28 10:37:29.515: ISAKMP:      default group 2
*Aug 28 10:37:29.515: ISAKMP:      auth pre-share
*Aug 28 10:37:29.515: ISAKMP:      life type in seconds
*Aug 28 10:37:29.515: ISAKMP:      life duration (VPI) of  0x0 0x20 0xC4 0x9B
*Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):atts are acceptable. Next payload is 0
*Aug 28
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):SA authentication status:
authenticated
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1): Process initial contact,
  bring down existing phase 1 and 2 SA's with local 192.168.1.11
  remote 172.16.1.20 remote port 500
*Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):returning IP addr to
  the address pool: 10.0.0.57
*Aug 28 10:37:29.955: ISAKMP (0:134217743): returning address 10.0.0.57 to pool
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):received initial contact, deleting SA
*Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):peer does not do pade
  1583442981 to QM_IDLE
*Aug 28 10:37:29.963: ISAKMP:(0:15:SW:1):Sending NOTIFY
  RESPONDER_LIFETIME protocol 1
spi 1689265296, message ID = 1583442981
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1): sending packet to
  172.16.1.20 my_port 500 peer_port 500 (R) QM_IDLE
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):purging node 1583442981
*Aug 28 10:37:29.967: ISAKMP: Sending phase 1 responder lifetime 86400

*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Input = IKE_MESG_FROM_PEER, IKE_AM_EXCH
*Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Old State = IKE_R_AM2
  New State = IKE_P1_COMPLETE
```

- VPN伺服器上的**debug crypto ipsec**命令會顯示成功的VPN隧道第1階段IPsec協商和建立。以下是範例：

```
------------------------------------------------------------------------
 ------------------------------------------------------------------
------------------------------------------------------------------------
*Aug 28 10:40:04.267: IPSEC(key_engine): got a queue event with 1 kei messages
*Aug 28 10:40:04.271: IPSEC(spi_response): getting spi 2235082775 for SA
from 192.168.1.11 to 172.16.1.20 for prot 3
*Aug 28 10:40:04.279: IPSEC(key_engine): got a queue event with 2 kei messages
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0x8538A817(2235082775), conn_id= 0, keysize= 0, flags= 0x2
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0xFFC80936(4291299638), conn_id= 0, keysize= 0, flags= 0xA
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Event create routes for
  peer or rekeying for peer 172.16.1.20
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Refcount 1 Serial3/0
*Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Added
  10.0.0.58 255.255.255.255 via 172.16.1.20 in IP DEFAULT TABLE with tag 0
*Aug 28 10:40:04.283: IPSec: Flow_switching Allocated flow for sibling 8000001F
*Aug 28 10:40:04.283: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.0.0.58,
  dest_port 0

*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 192.168.1.11, sa_proto= 50,
    sa_spi= 0x8538A817(2235082775),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002
*Aug 28 10:40:04.287: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.16.1.20, sa_proto= 50,
    sa_spi= 0xFFC80936(4291299638),
    sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001
```

相關資訊

- IP安全(IPsec)加密簡介
- IPsec協商/IKE通訊協定支援頁面
- 配置IPsec網路安全
- Cisco Easy VPN問答
- 思科無線LAN控制器組態設定指南4.0版
- 無線LAN控制器上的ACL組態範例
- 無線 LAN 控制器 (WLC) 常見問題
- 無線支援頁面
- 技術支援與文件 - Cisco Systems