具有WLC的无线局域网上的客户端VPN配置示例

目录

简介

本文档介绍了无线环境中的虚拟私有网络 (VPN) 的概念。本文档介绍了通过无线 LAN 控制器 (WLC) 在无线客户端和 VPN 服务器之间部署 VPN 通道时所涉及的配置。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解 WLC 和如何配置 WLC 基本参数
- 了解 Wi-Fi 保护访问 (WPA) 概念
- 基本了解 VPN 及其类型
- 了解 IPSec
- 基本了解可用的加密、身份验证和散列算法

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 4.0.179.8 版本的 Cisco 2006 WLC
- Cisco 1000 系列轻量接入点 (LAP)
- 运行Cisco IOS软件版本12.4(8)的Cisco 3640
- Cisco VPN客户端软件版本4.8

注意： 本文档使用 3640 路由器作为 VPN 服务器。若要支持更高级的安全功能，您也可以使用一个专用的 VPN 服务器。

注意： 为了使路由器用作 VPN 服务器，它需要运行支持基本 IPSec 的功能集。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

VPN 是一种专用数据网络，用于通过公共电信基础架构（例如 Internet）在专用网络内安全传输数据。这种 VPN 通过使用隧道协议和安全程序保持数据的保密性。

远程访问 VPN

远程访问 VPN 配置用于允许 VPN 软件客户端（例如移动用户）安全地访问位于 VPN 服务器后的集中网络资源。在 Cisco 术语中，这些 VPN 服务器和客户端也被称为 Cisco Easy VPN 服务器和 Cisco Easy VPN 远程设备。

Cisco Easy VPN 远程设备可以是 Cisco IOS 路由器、Cisco PIX 安全设备、Cisco VPN 3002 硬件客户端和 Cisco VPN Client。它们用于在从 Cisco Easy VPN 服务器连接 VPN 通道时接收安全策略。这样可以最大限度地降低远程位置的配置要求。Cisco VPN Client 是一种软件客户端，可以安装在 PC、便携式计算机等设备上。

Cisco Easy VPN 服务器可以是 Cisco IOS 路由器、Cisco PIX 安全设备和 Cisco VPN 3000 集中器。

本文档使用在便携式计算机上运行的 Cisco VPN Client 软件作为 VPN 客户端，使用 Cisco 3640 IOS 路由器作为 VPN 服务器。本文档采用 IPSec 标准在客户端和服务器之间建立一个 VPN 通道。

IPsec

IPSec 是由 Internet 工程任务组 (IETF) 开发的开放标准框架。IPSec 旨在为通过 Internet 等未受保护的网络传输敏感信息提供安全性。

IPSec 可在 IP 数据包级别对网络数据加密，从而提供了一种功能强大、基于标准的安全解决方案。IPSec 的主要任务是实现专用信息通过不安全连接进行交换。IPSec 使用加密保护信息免受拦截或窃听。不过，为了高效地使用加密，双方应该共享用于信息加密和解密的密钥。

IPSec 分两个阶段工作以实现共享密钥的机密交换：

- 第 1 阶段 — 处理在两个 IPSec 对等体之间建立一条安全通道所需的安全参数协商。通常通过

Internet Key Exchange (IKE) 协议实施第 1 阶段。如果远程 IPSec 对等体无法执行 IKE，您可以通过预共享密钥使用手动配置完成第 1 阶段。
- 第 2 阶段 — 使用第 1 阶段中建立的安全隧道来交换实际传输用户数据所需的安全参数。在 IPsec 的两个阶段中使用的安全隧道基于每个 IPSec 端点使用的安全关联 (SA)。SA 描述了安全参数，例如两个端点都同意使用的身份验证和加密类型。

在第 2 阶段交换的安全参数用于创建 IPSec 隧道，该隧道随后又用于在 VPN 客户端和服务器之间传输数据。

有关 IPSec 及其配置的详细信息，请参阅配置 IPsec。

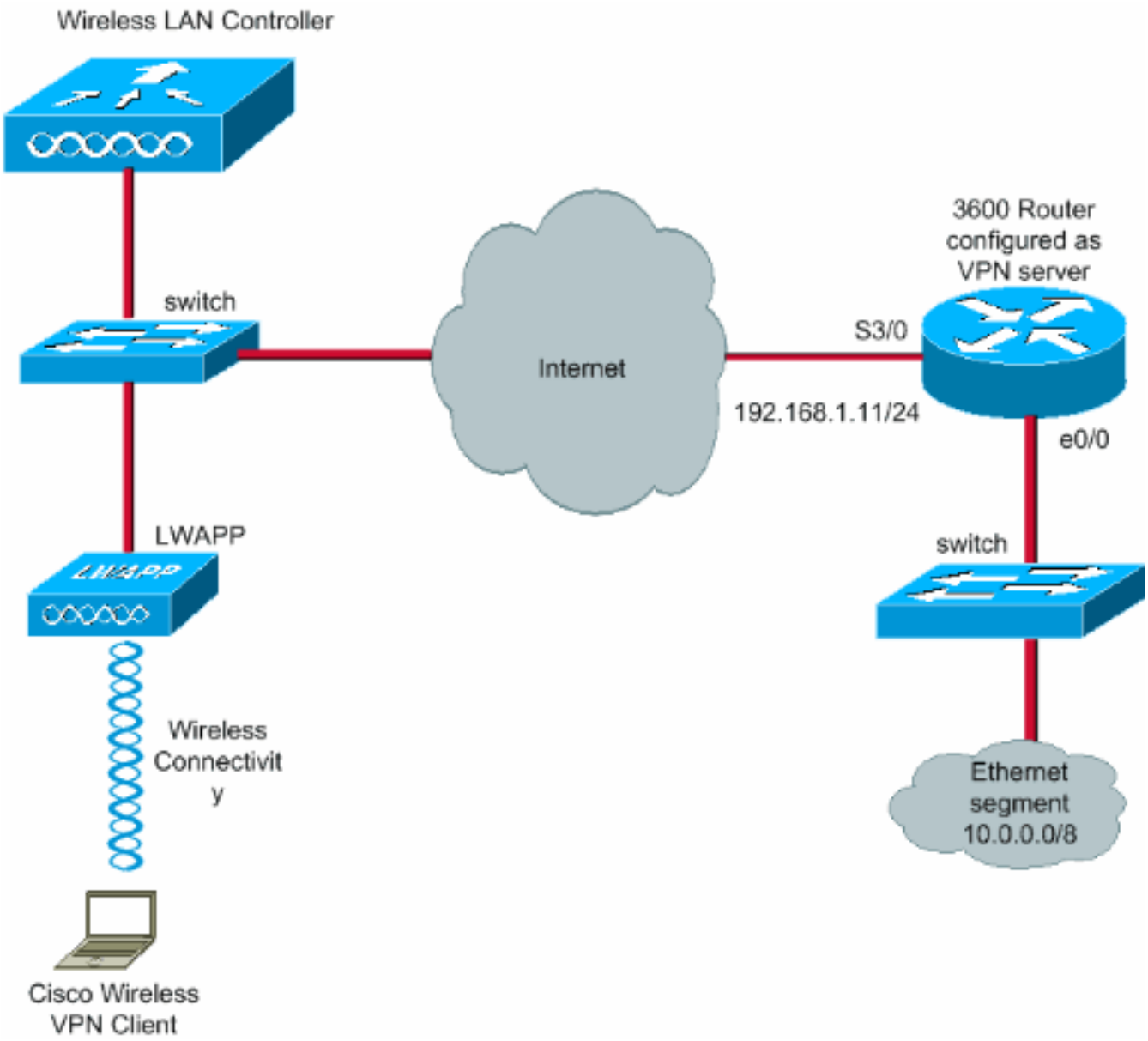
在 VPN 客户端和服务器之间建立 VPN 通道之后，*VPN 服务器上定义的安全策略将被发送到客户端*。这样可以最大限度地降低客户端一侧的配置要求。

注意： 有关本文档所用命令的详细信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下配置：

- WLC 的管理接口 IP 地址 — 172.16.1.10/16
- WLC 的 AP 管理器接口 IP 地址 — 172.16.1.11/16
- 默认网关 — 172.16.1.20/16**注意：** 在真实网络中，此默认网关应该指向最接近的路由器的传入接口，该接口将 WLC 连接到网络的其余部分和/或 Internet。
- VPN 服务器 s3/0 的 IP 地址 — 192.168.1.11/24**注意：** 此 IP 地址应该指向在 VPN 服务器端终止 VPN 通道的接口。在本示例中，s3/0 是在 VPN 服务器上终止 VPN 通道的接口。
- VPN 服务器上的 LAN 网段使用的 IP 地址范围为 10.0.0.0/8。



配置

在 WLAN 集中体系结构中，为了允许便携式计算机等无线 VPN 客户端通过 VPN 服务器建立一个 VPN 通道，客户端需要与轻量接入点 (LAP) 关联，而后者则需要在 WLC 中注册。本文档假定 LAP 已通过轻量 AP (LAP) 注册到无线 LAN 控制器 (WLC) 中介绍的本地子网广播发现过程在 WLC 中进行了注册。

下一步是对 WLC 进行 VPN 配置。

VPN 终止和 Pass-through

低于版本 4 的 Cisco 4000 系列 WLC 支持名为 IPSec VPN 终止（IPSec 支持）的功能。此功能使这些控制器能够直接在其上终止 VPN 客户端会话。总之，此功能使控制器本身能够用作 VPN 服务器。但是，这需要在控制器中安装一个独立的 VPN 终止硬件模块。

不支持此 IPSec VPN 功能的设备包括：

- Cisco 2000 系列 WLC
- 运行版本 4.0 或更高版本的任何 WLC

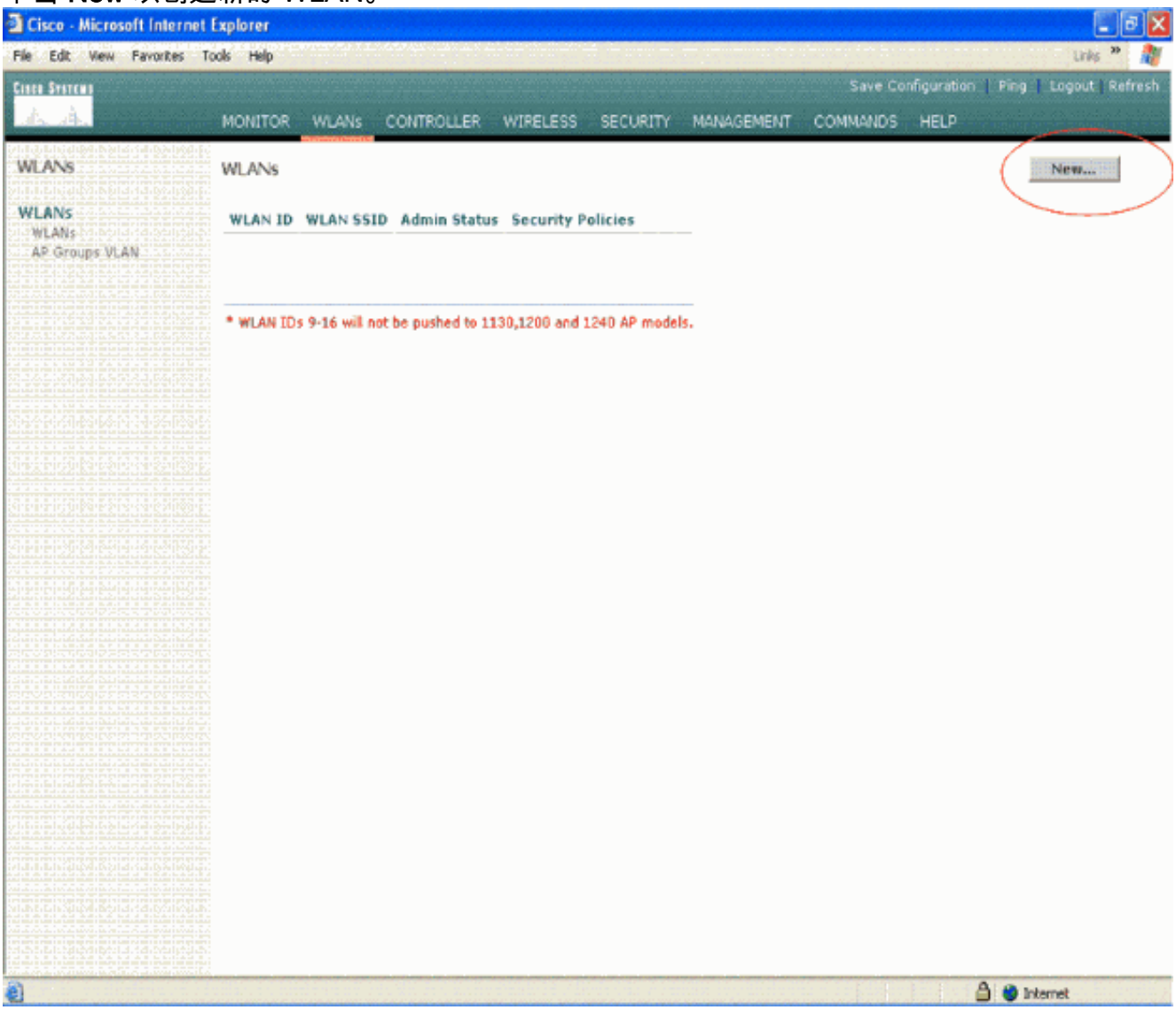
因此，高于 4.0 的版本中唯一支持的 VPN 功能为 VPN Pass-through。Cisco 2000 系列 WLC 也支持此功能。

VPN Pass-through 是一项仅允许客户端与特定的 VPN 服务器建立隧道的功能。因此，如果您需要安全地访问配置好的 VPN 服务器以及另一台 VPN 服务器或 Internet，则在控制器上已启用 VPN Pass-through 的情况下无法实现该目的。在这种情况下，您需要禁用 VPN Pass-through。不过，如果创建了合适的 ACL 并应用于相应的 WLAN，则可将 WLC 配置为直通以到达多个 VPN 网关。因此，在这种希望到达冗余的多个 VPN 网关的情况下，请禁用 VPN passthrough 并创建允许访问 VPN 网关的 ACL，然后将该 ACL 应用于 WLAN。

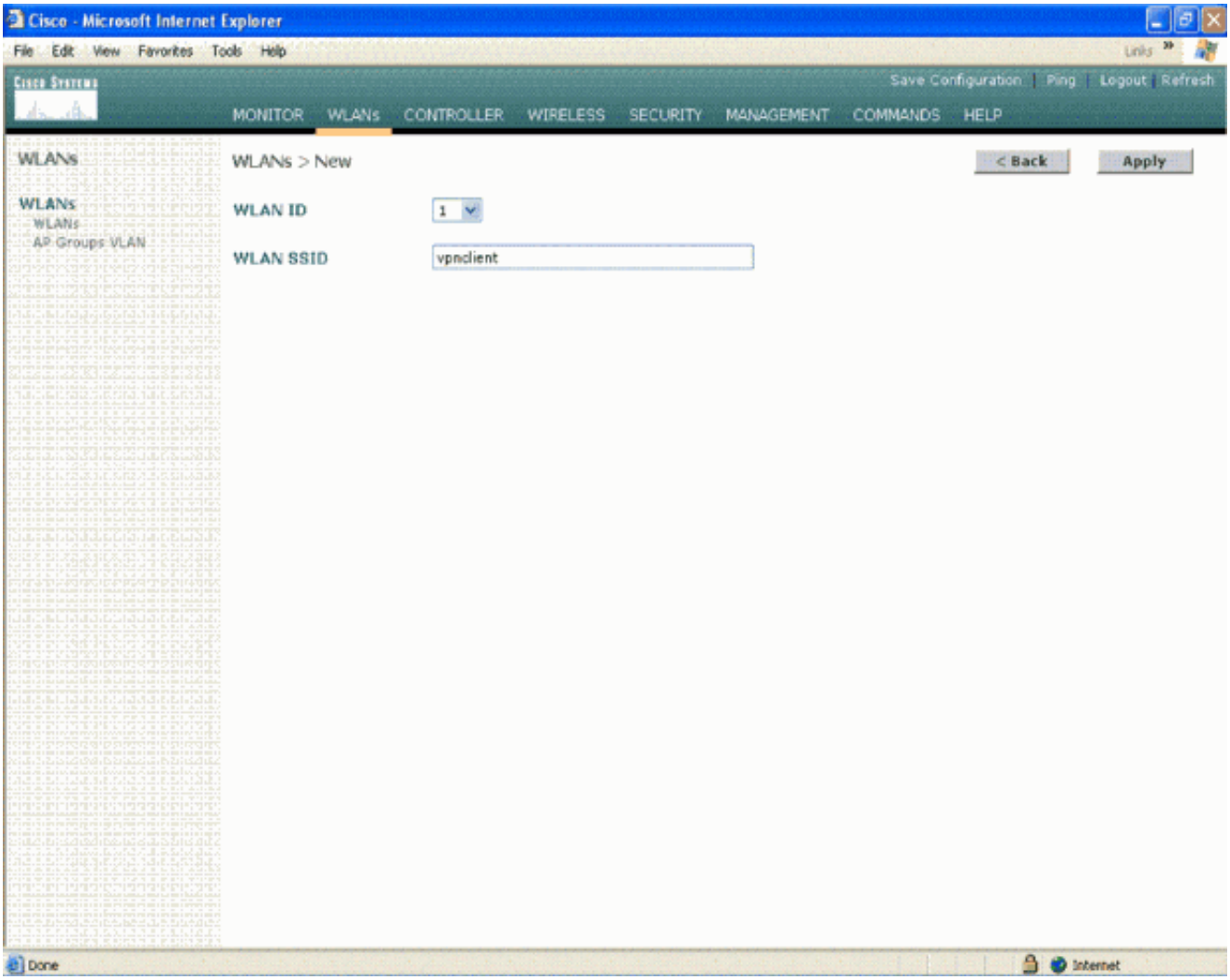
配置 WLC 的 VPN Pass-through 功能

完成以下步骤以配置 VPN Pass-through 功能。

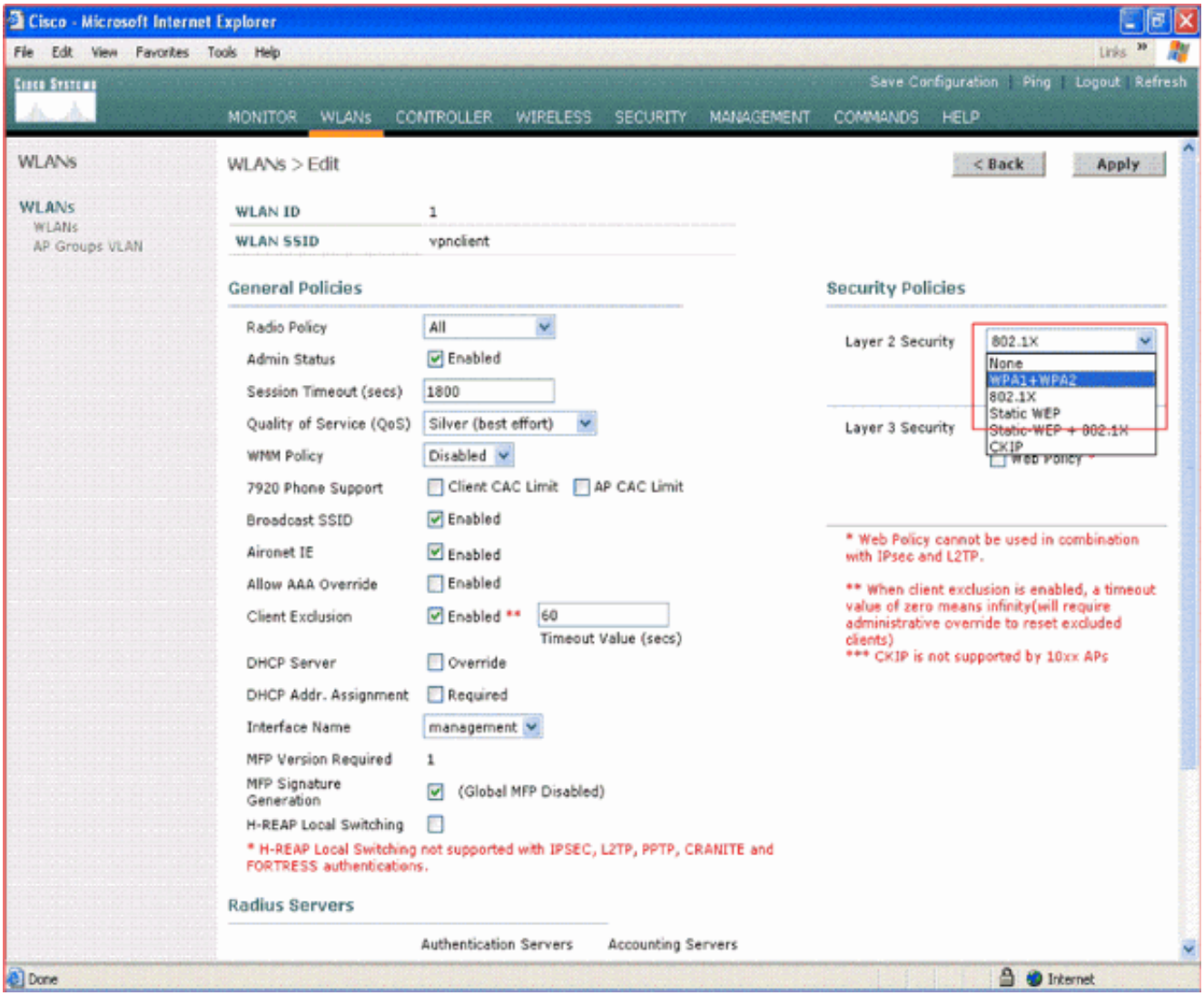
1. 从 WLC GUI 中单击 **WLAN**，转到 WLAN 页。
2. 单击 **New** 以创建新的 WLAN。



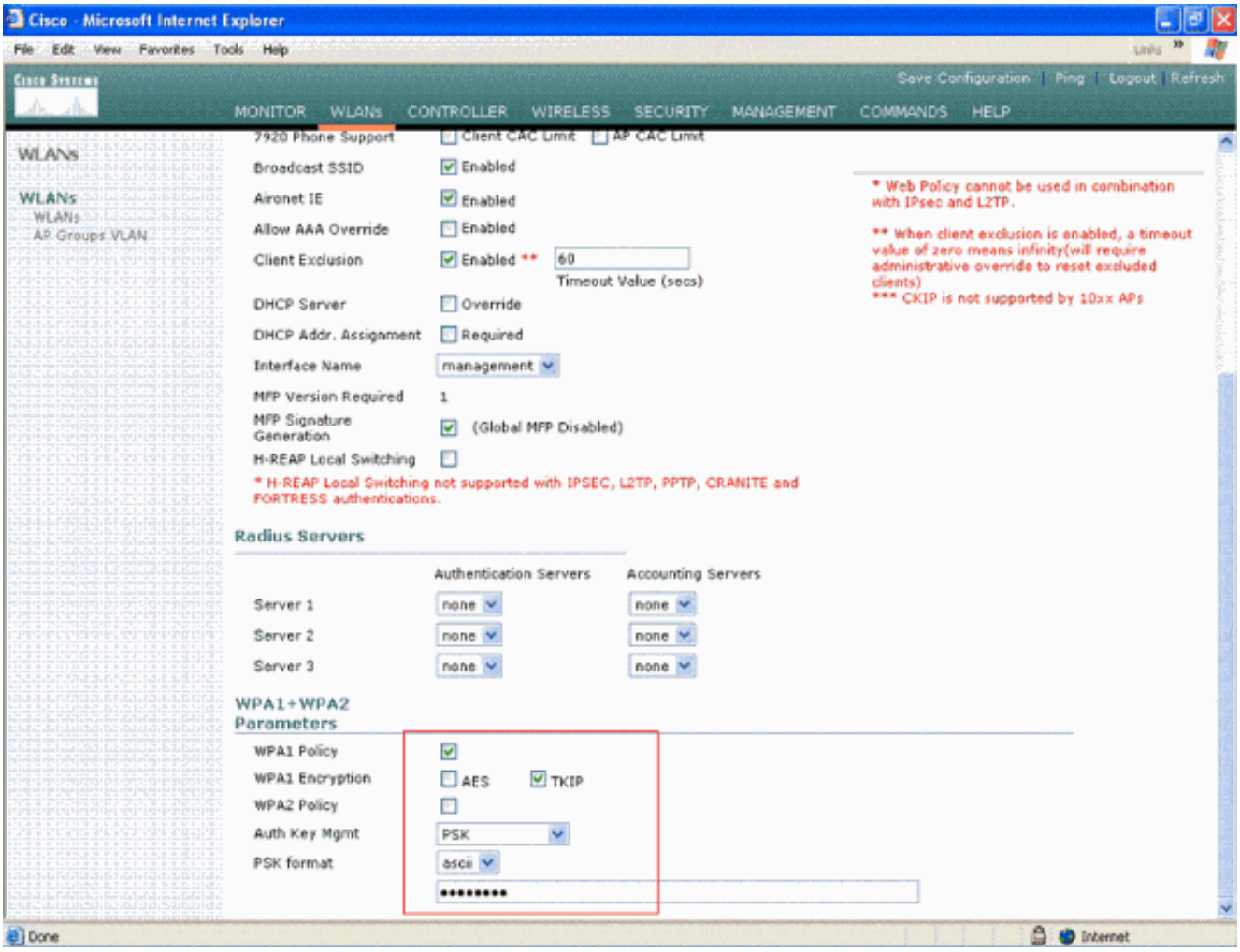
3. 在此例中 WLAN SSID 名为 **vpnclient**。单击 **Apply**。



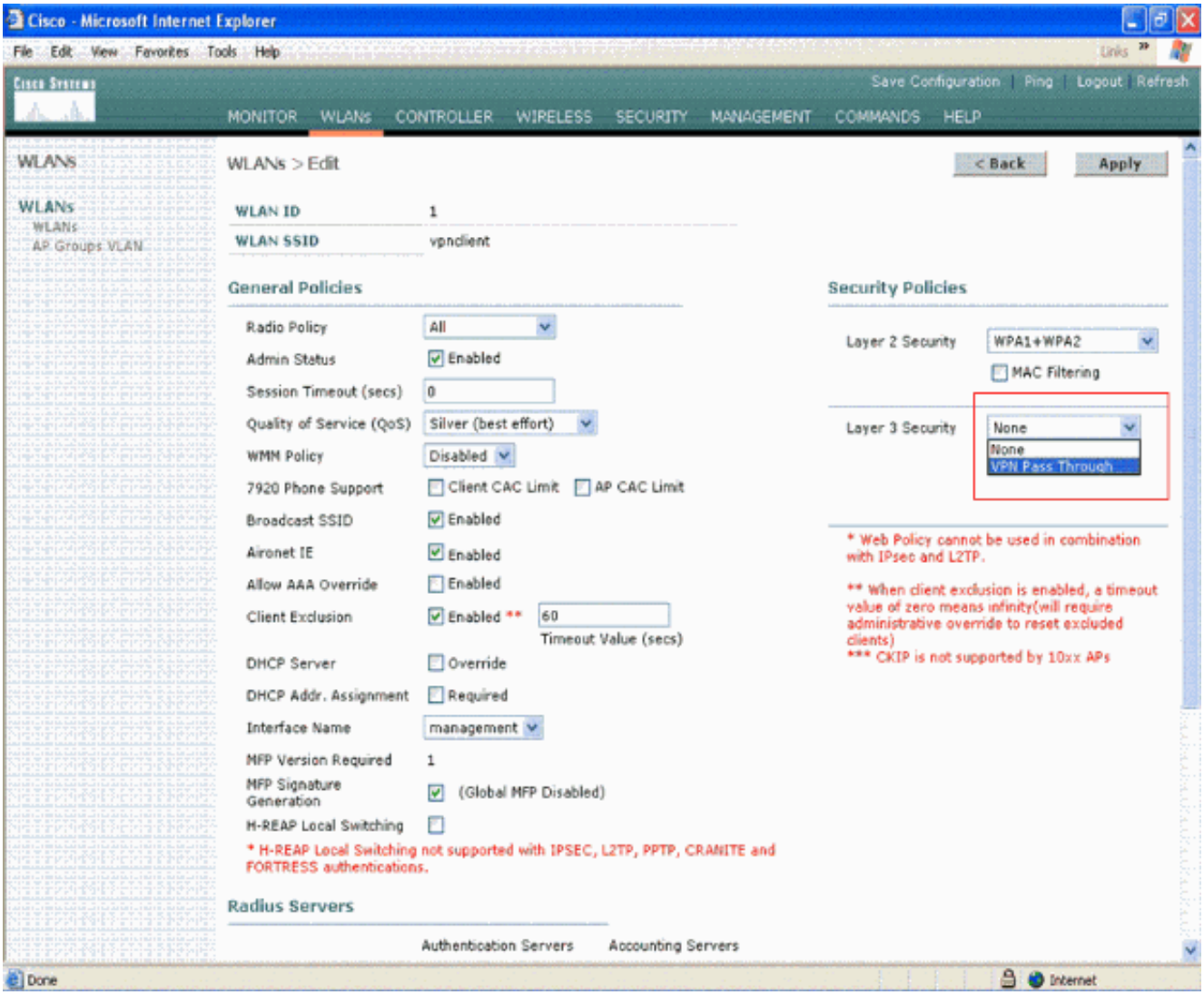
4. 使用第 2 层安全配置 SSID vpnclient。*此操作为可选操作*。此例使用 **WPA1+WPA2** 作为安全类型。



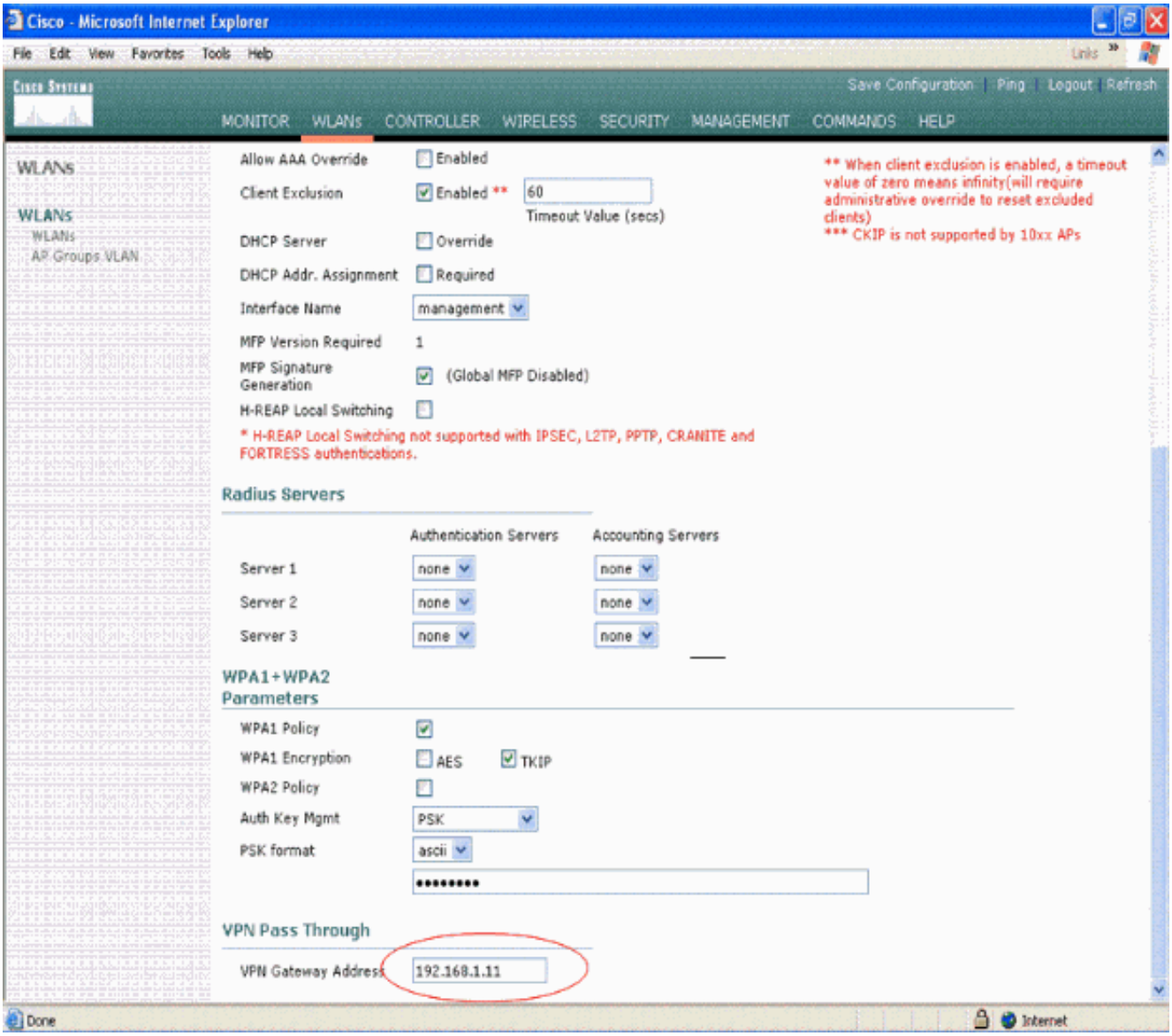
5. 配置要使用的 WPA 策略和身份验证密钥管理类型。此例使用**预共享密钥 (PSK)** 进行身份验证密钥管理。选择 PSK 之后，请选择 **ASCII** 作为 PSK 格式，并键入 PSK 值。此值应该与无线客户端 SSID 配置中的值相同，以便属于此 SSID 的客户端与此 WLAN 关联。



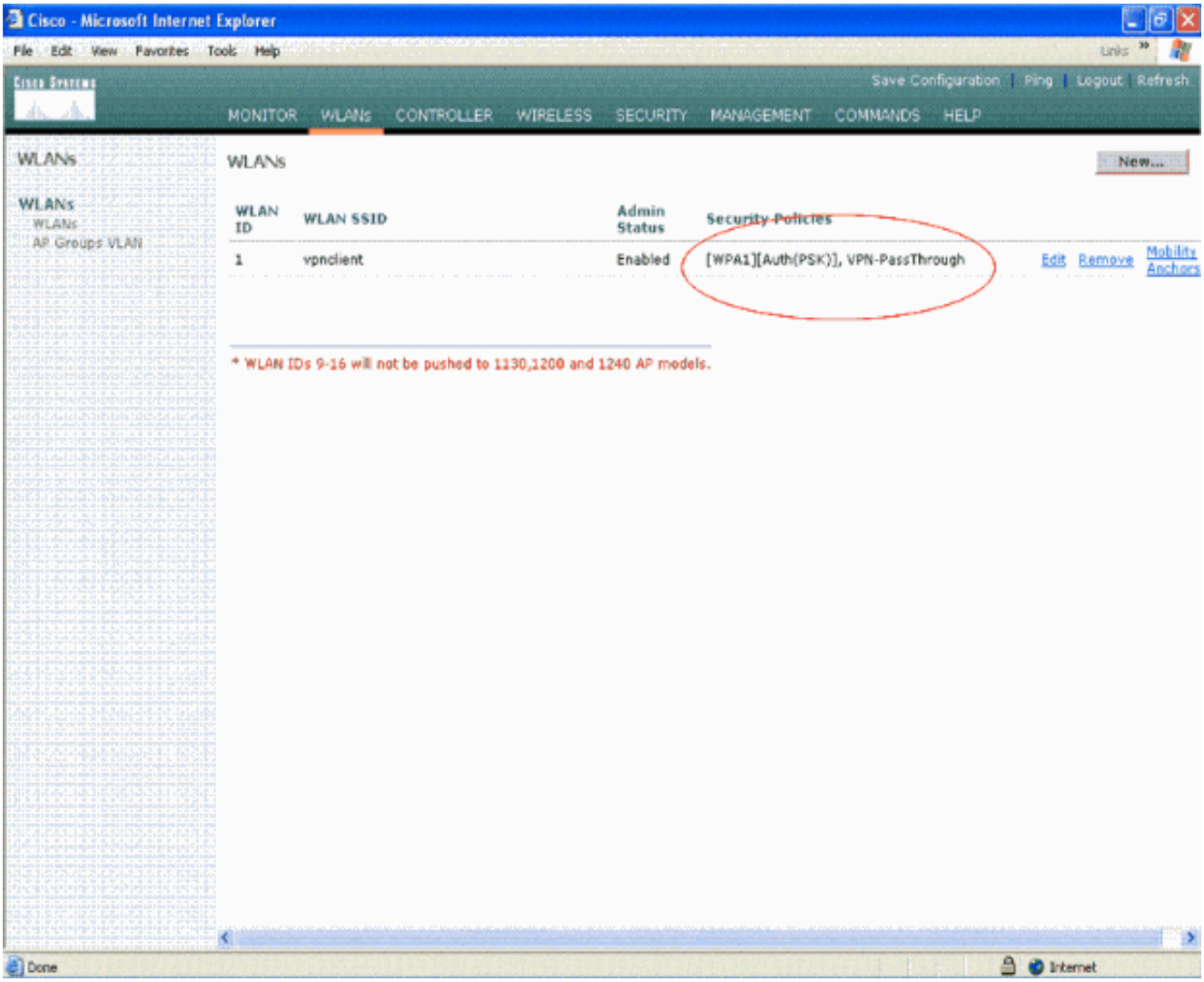
6. 选择 VPN Pass-through 作为第 3 层安全，如下面的示例所示。



7. 选择 VPN Pass-through 作为第 3 层安全之后，请添加 VPN 网关地址，如示例所示。此网关地址应为终止服务器端 VPN 通道的接口的 IP 地址。在此例中，VPN 服务器 s3/0 接口的 IP 地址 (192.168.1.11/24) 是要配置的网关地址。



8. 单击 **Apply**。名为 *vpnclient* 的 WLAN 现已完成 VPN Pass-through 配置。



VPN 服务器配置

从此配置中可看出，Cisco 3640 路由器用作 VPN 服务器。

注意： 为简单起见，此配置使用静态路由保持端点之间的 IP 可达性。您可以使用任何动态路由协议，例如路由信息协议 (RIP)、开放最短路径优先 (OSPF) 等等保持可达性。

注意： 如果客户端和服务器之间没有 IP 可达性，则无法建立隧道。

注意： 本文档假定用户了解如何在网络中启用动态路由。

Cisco 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： 此示例仅使用组身份验证方式，而不使用个人用户身份验证。

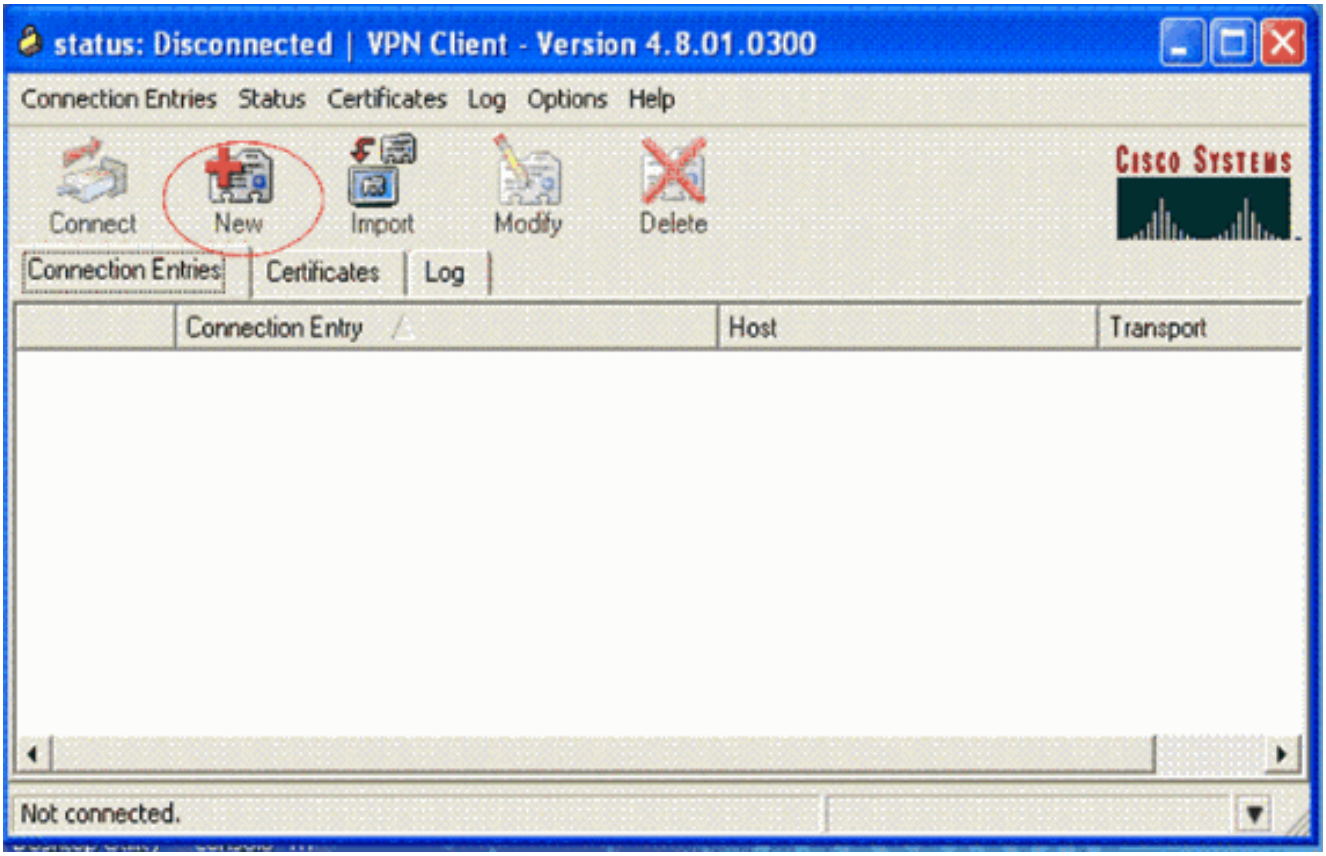
VPN 客户端配置

可以从 Cisco.com 软件中心下载 VPN 客户端软件。

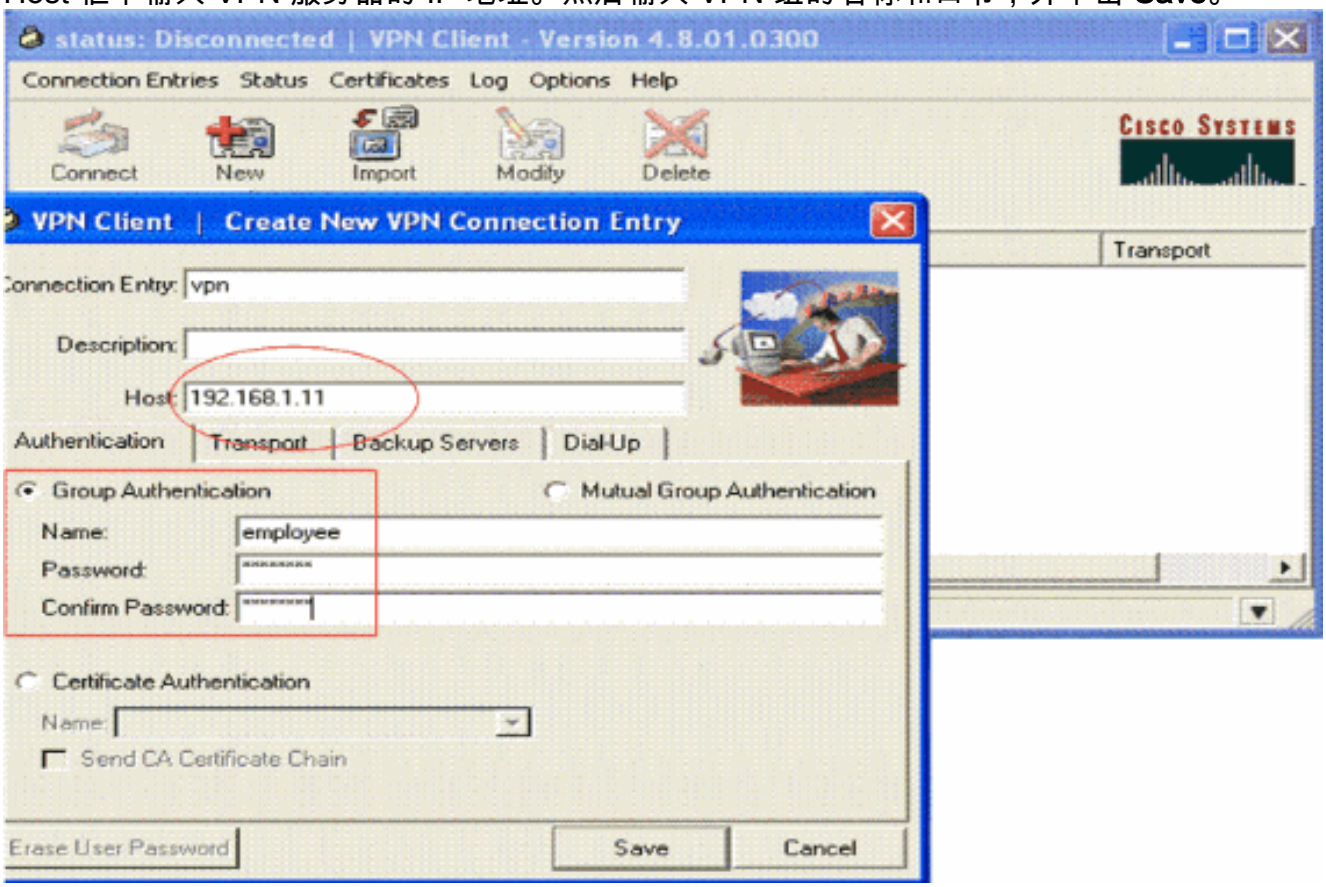
注意： 某些 Cisco 软件要求您使用 CCO 用户名和口令登录。

执行下列步骤以配置 VPN 客户端。

1. 从您的无线客户端（便携式计算机）选择 **Start > Programs > Cisco Systems VPN Client > VPN Client**，访问 VPN 客户端。这是 VPN 客户端的默认安装位置。
2. 单击 **New** 以启动 Create New VPN Connection Entry 窗口。



3. 输入 Connection Entry 的名称与说明。本示例使用 vpn。Description 字段为选填字段。在 Host 框中输入 VPN 服务器的 IP 地址。然后输入 VPN 组的名称和口令，并单击 **Save**。



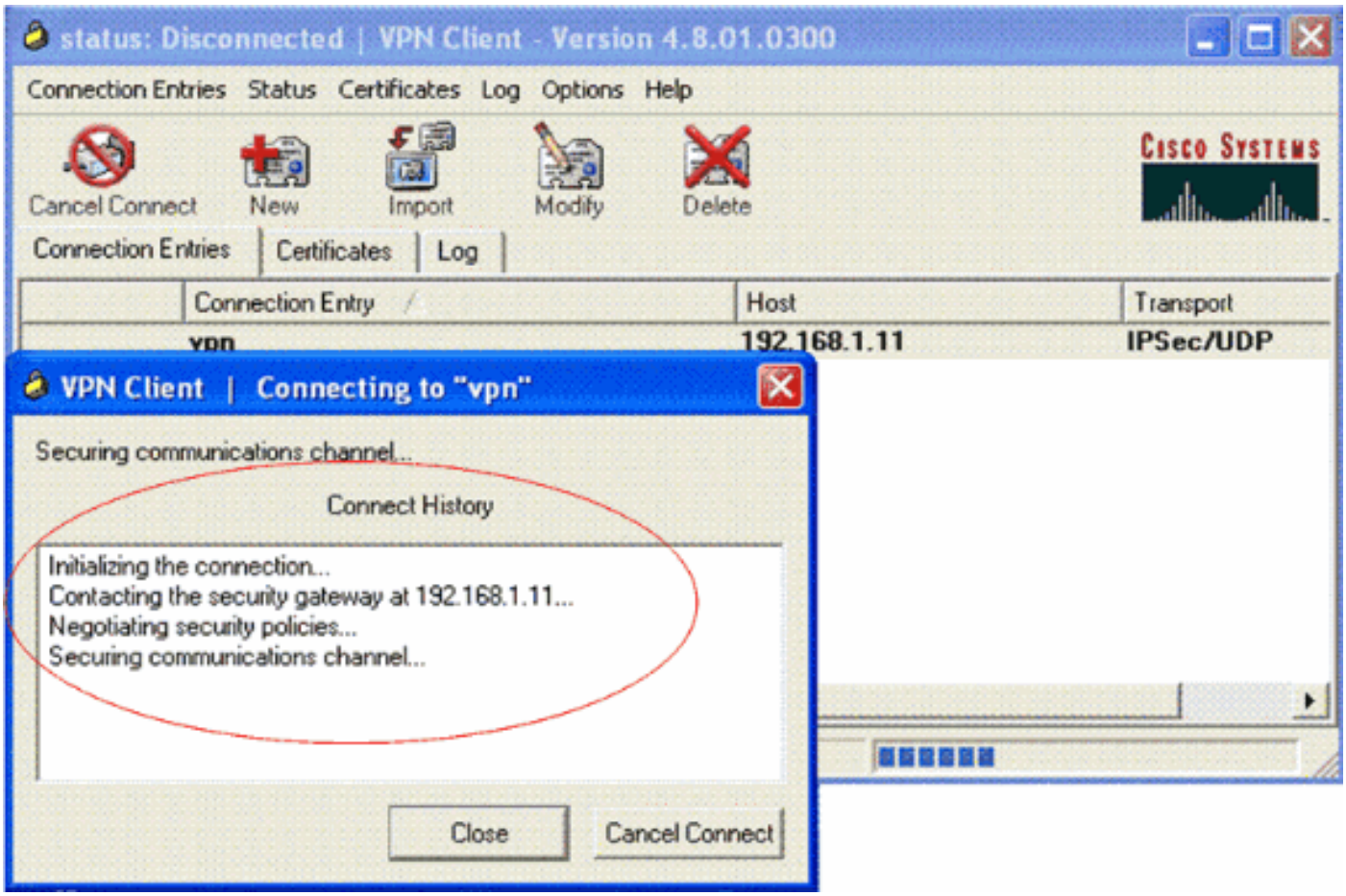
注意： 此处配置的组名和口令应该与 VPN 服务器中配置的相同。此示例使用组名 *employee* 和口令 *cisco123*。

验证

为了验证此配置，请使用在 WLC 中配置的相同安全参数配置无线客户端中的 SSID **vpnclient**，并将客户端与此 WLAN 关联。有几个文档介绍了如何使用新的配置文件配置无线客户端。

关联无线客户端之后，请转到 VPN 客户端，并单击您已配置的连接。然后从 VPN 客户端主窗口单击 **Connect**。

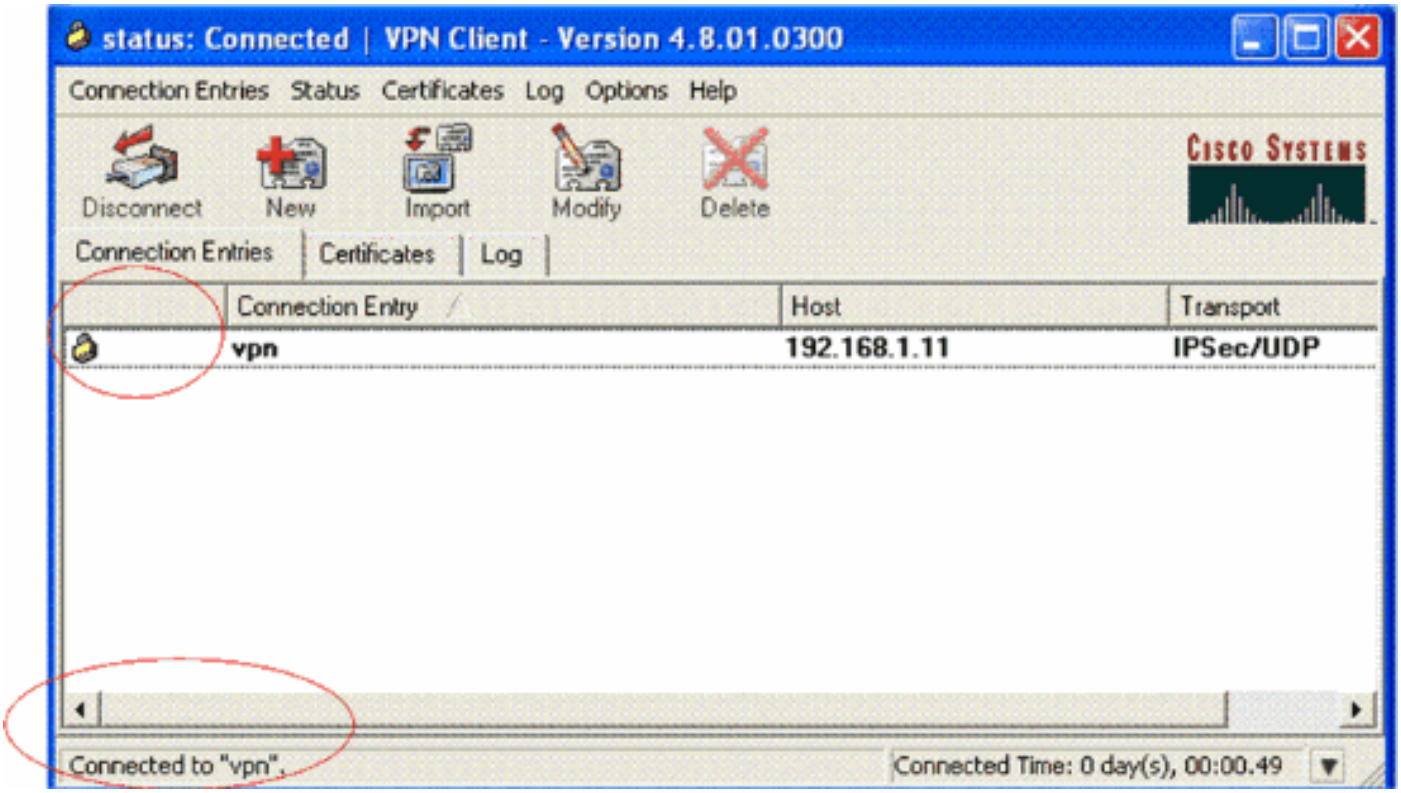
您可以看到客户端和服务器之间议定的第 1 阶段和第 2 阶段安全参数。



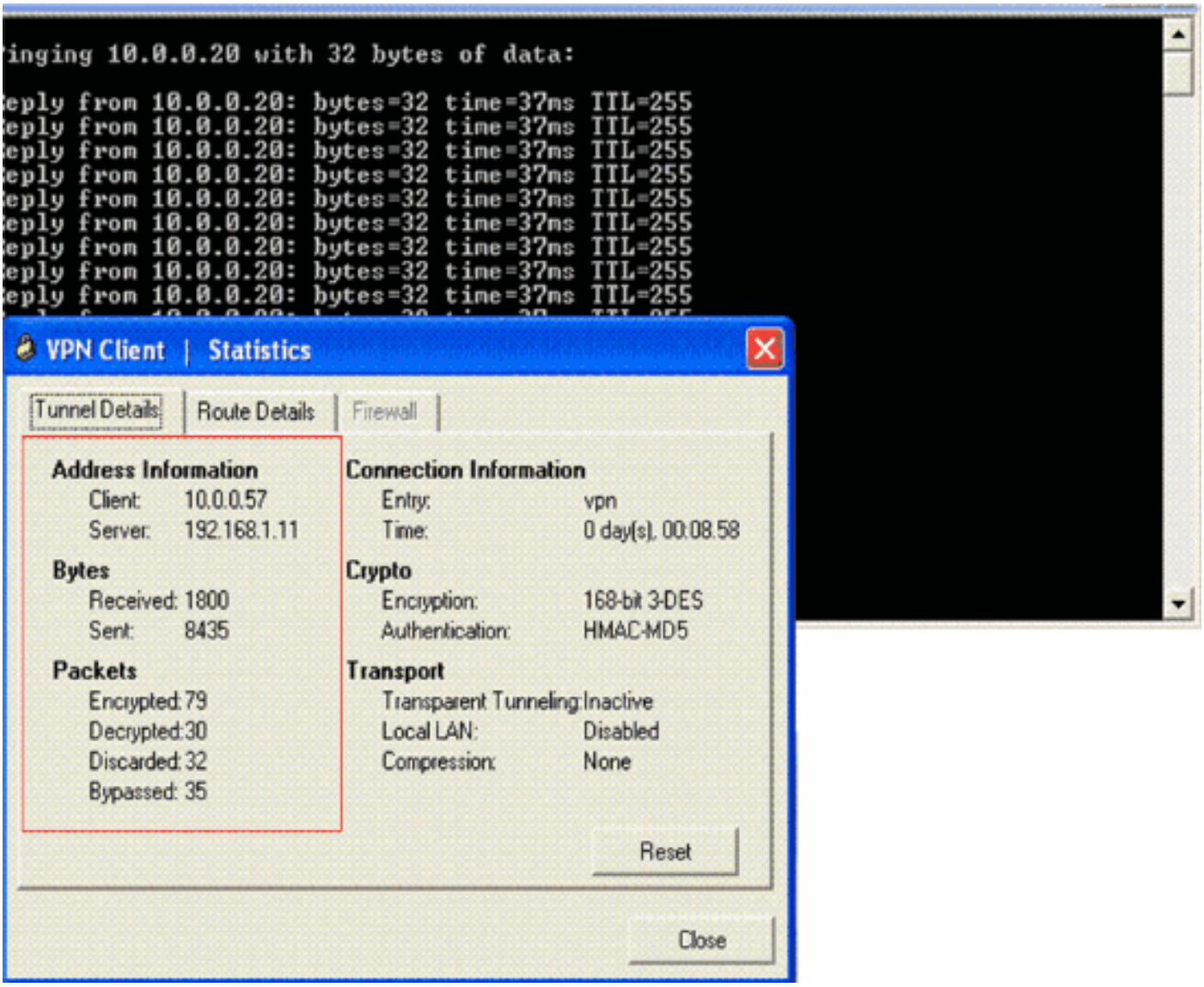
注意： 若要建立此 VPN 通道，VPN 客户端和服务器之间应具有 IP 可达性。如果 VPN 客户端无法联系安全网关（VPN 服务器），则无法建立隧道，并且客户端上会显示警告框，包含以下消息：

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

如果客户端和服务器之间已正确建立 VPN 通道，您可在已建立的 VPN 客户端旁看到一个锁图标。状态栏同时指示 **Connected to "vpn"**。下面是一个示例。



并且，请确保您能够成功将数据从 VPN 客户端传输到位于服务器端的 LAN 网段，反之亦然。从 VPN 客户端主菜单选择 **Status > Statistics**。您可在此找到通过隧道传送的加密和解密数据包的统计信息。



在此屏幕截图中，您可以看到客户端地址为 10.0.0.57。这是 VPN 服务器在第 1 阶段协商成功后从其本地配置池分配到客户端的地址。建立隧道之后，VPN 服务器会在其路由表中自动添加一个到此已分配 DHCP IP 地址的路由。

此外，当数据从客户端传输到服务器时您能够看到加密数据包的数量不断增加，而在反向的数据传输过程中解密数据包的数量会不断增加。

注意： 由于已对 WLC 进行了 VPN Pass-through 配置，WLC 仅允许客户端访问与已进行 Pass-through 配置的 VPN 网关（此处指 192.168.1.11 VPN 服务器）相连的网段。这样将过滤所有其他流量。

您可以对此进行验证，方法是将另一个 VPN 服务器配置为相同的配置，然后在 VPN 客户端上为此 VPN 服务器配置一个新连接项。现在，当您试图通过此 VPN 服务器建立隧道时将无法做到这一点。这是因为 WLC 会过滤此流量，并且仅允许在进行了 VPN Pass-through 配置的 VPN 网关地址之间建立隧道。

您也可以从 VPN 服务器的 CLI 验证配置。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

以下用在 VPN 服务器中的 **show** 命令也能帮助您验证隧道状态。

- **Show crypto session** 命令用于验证隧道状态。以下是此命令的输出示例。`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** 用于查看已配置的第 1 阶段参数。

故障排除

验证部分中介绍的 **debug** 和 **show** 命令也可用于排除故障。

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

- VPN 服务器上的 **debug crypto isakmp** 命令显示了客户端和服务器之间的整个第 1 阶段协商过程。以下是第 1 阶段成功协商的示例。----------
  ```
  *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 服务器上的 **debug crypto ipsec** 命令显示了第 1 阶段 IPsec 的成功协商和 VPN 通道的创建。示例如下：----------
  ```
  *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
```

相关信息

- IP 安全 (IPsec) 加密简介
- IPsec 协商/IKE 协议支持页
- 配置 IPSec 网络安全
- Cisco Easy VPN 问答
- Cisco 无线 LAN 控制器配置指南 4.0 版
- 无线 LAN 控制器中的 ACL 配置示例
- 无线局域网控制器(WLC)常见问题
- 无线支持页
- 技术支持和文档 - Cisco Systems