Ejemplo de Configuración del Cliente VPN sobre LAN Inalámbrica con WLC

Contenido

Introducción

Este documento introduce el concepto de Red privada virtual (VPN) en un entorno de red inalámbrica. El documento explica las configuraciones implicadas en el despliegue de un túnel VPN entre un cliente de red inalámbrica y un servidor VPN a través de un regulador LAN de la Tecnología inalámbrica (WLC).

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de WLCs y cómo configurar los parámetros básicos WLC
- Conocimiento de los conceptos del Acceso protegido de Wi-Fi (WPA)
- Conocimiento básico del VPN y de sus tipos
- Conocimiento de IPsec
- Conocimiento básico del cifrado, de la autenticación y de los algoritmos de troceo disponibles

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2006 WLC que funciona con la versión 4.0.179.8
- Punto de acceso ligero de las Cisco 1000 Series (REVESTIMIENTO)
- Cisco 3640 que funciona con la versión del Cisco IOS ® Software 12.4(8)
- Cliente VPN de Cisco versión 4.8

Nota: Este documento utiliza a un 3640 Router como servidor VPN. Para utilizar más funciones de seguridad avanzada, usted puede también utilizar a un servidor VPN dedicado.

Nota: Para que un router actúe como servidor VPN, necesita funcionar con una característica fijada que utilice IPsec básico.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Un VPN es una red de datos privada que se utiliza para transmitir con seguridad los datos dentro de una red privada a través de la infraestructura de telecomunicación pública tal como Internet. Este VPN mantiene la privacidad de los datos con el uso de un Tunneling Protocol y de los procedimientos de seguridad.

VPN de acceso remoto

Una configuración del VPN de acceso remoto se utiliza para permitir que los clientes del software VPN tales como usuarios ambulantes tengan acceso con seguridad a los recursos de red centralizada que residen detrás de un servidor VPN. En terminologías de Cisco, llaman estos servidores VPN y clientes también el servidor del Cisco Easy VPN y el dispositivo remoto del Cisco Easy VPN.

Un dispositivo remoto del Cisco Easy VPN puede ser Routers del Cisco IOS, dispositivos de seguridad de Cisco PIX, Clientes de hardware Cisco VPN 3002 y el Cliente Cisco VPN. Los utilizan para recibir las políticas de seguridad sobre una conexión del túnel VPN de un servidor del Cisco Easy VPN. Esto minimiza los requisitos de configuración en el lugar remoto. El Cliente Cisco VPN es un cliente del software que puede ser instalado en las PC, las computadoras portátiles, y así sucesivamente.

Un servidor del Cisco Easy VPN puede ser Routers del Cisco IOS, dispositivos de seguridad de Cisco PIX, y concentradores de Cisco VPN 3000.

Este documento utiliza el software de VPN Client de Cisco que se ejecuta en una computadora portátil como router VPN IOS del cliente y de Cisco 3640 como el servidor VPN. El documento utiliza el estándar de IPsec para establecer un túnel VPN entre un cliente y un servidor.

IPsec

IPsec es un marco de los estándares abiertos desarrollados por el Internet Engineering Task Force (IETF). IPsec proporciona a la Seguridad para la transmisión de la información vulnerable sobre las redes no protegidas tales como Internet.

IPsec proporciona al cifrado de datos de red en el nivel del paquete IP, que ofrece solución acerca de la seguridad robusta estándar-se basa que. La tarea principal de IPsec es permitir el intercambio de la información privada sobre una conexión insegura. IPsec utiliza el cifrado para proteger la información contra la interceptación o escuchar detras de las puertas. Sin embargo, para utilizar el cifrado eficientemente, ambas partes deben compartir un secreto que se utilice para el cifrado y el desciframiento de la información.

IPsec actúa en dos fases para permitir el intercambio confidencial de un secreto compartido:

- Fase 1 — Maneja la negociación de los parámetros de Seguridad requeridos establecer un canal seguro entre dos peeres IPSec. La fase 1 se ejecuta generalmente con el protocolo del Internet Key Exchange (IKE). Si el peer IPSec remoto no puede realizar a IKE, usted puede utilizar la configuración manual con las claves previamente compartidas para completar la fase 1.
- Fase 2 — Utiliza el túnel seguro establecido en la fase 1 para intercambiar los parámetros de Seguridad requeridos para transmitir realmente los datos del usuario. Los túneles seguros usados en ambas fases de IPsec se basan en las asociaciones de seguridad (SAs) usadas en cada punto final de IPsec. El SAs describen los parámetros de Seguridad, tales como el tipo de autenticación y el cifrado que las puntas de los ambos extremos acuerdan utilizar.

Los parámetros de Seguridad intercambiados en la fase 2 se utilizan para crear un túnel de IPsec que a su vez se utilice para la Transferencia de datos entre el cliente VPN y el servidor.

Refiera a configurar IPsec para más información sobre IPsec y su configuración.

Una vez que un túnel VPN se establece entre el cliente VPN y el servidor, las *políticas de seguridad definidas en el servidor VPN se envían al cliente*. Esto minimiza los requisitos de configuración en el lado del cliente.

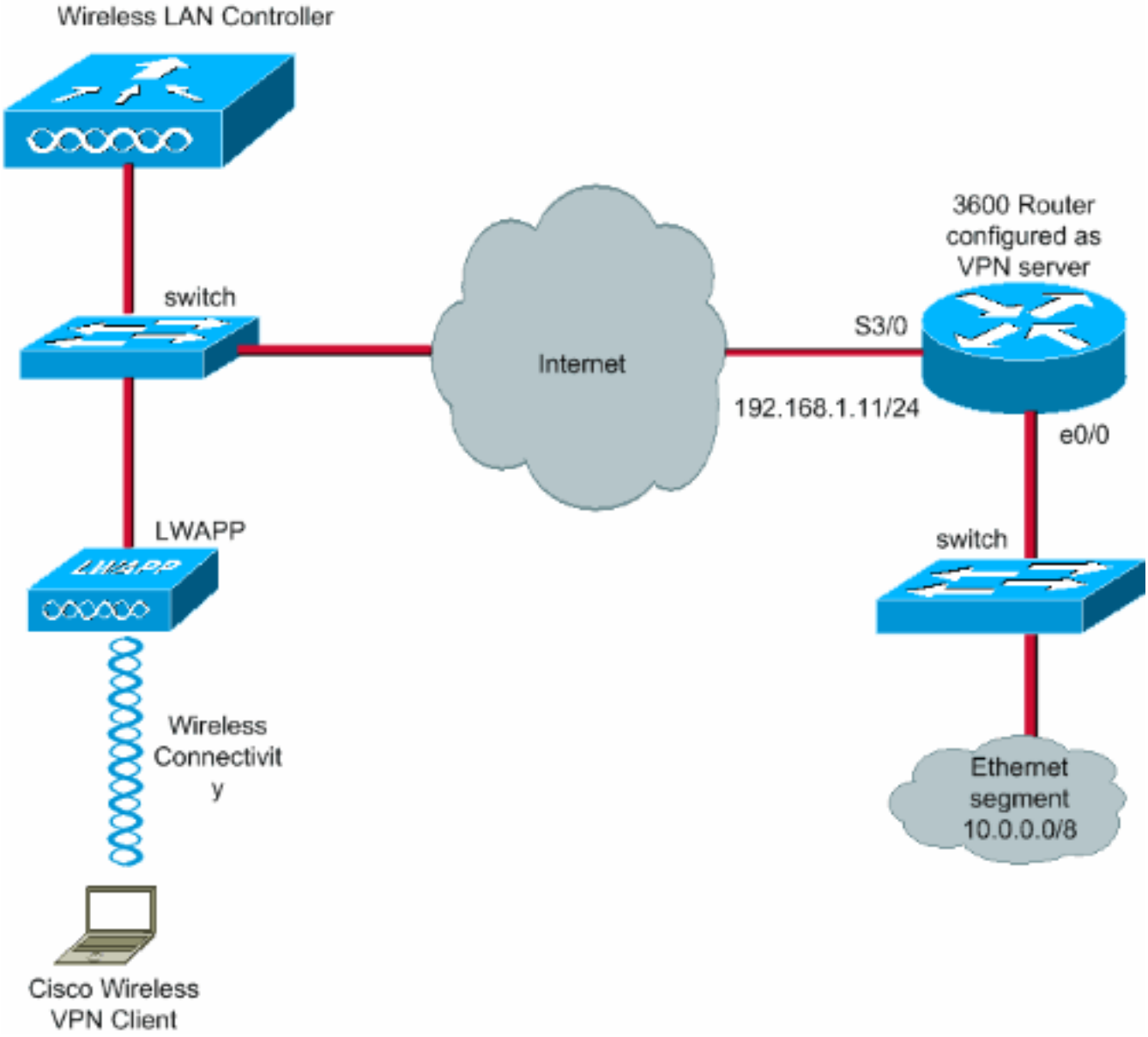
Nota: Use la herramienta Command Lookup Tool (clientes registrados solamente) para encontrar más información sobre los comandos usados en este documento.

Diagrama de la red

Este documento utiliza estas configuraciones:

- Dirección IP de la interfaz de administración del WLC — 172.16.1.10/16
- dirección IP del interfaz del AP-encargado del WLC — 172.16.1.11/16
- Gateway de valor por defecto — 172.16.1.20/16**Nota:** En una red en funcionamiento, este gateway de valor por defecto debe señalar a la interfaz entrante del router inmediato que conecta el WLC con el resto de la red y/o con Internet.

- Dirección IP del servidor VPN s3/0 — 192.168.1.11/24**Nota:** Esta dirección IP debe señalar al interfaz que termina el túnel VPN en el lado del servidor VPN. En este ejemplo, s3/0 es el interfaz que termina el túnel VPN en el servidor VPN.
- El segmento LAN en el servidor VPN utiliza el rango de dirección IP de 10.0.0.0/8.



Configurar

En una red inalámbrica (WLAN) arquitectura centralizada, para permitir que un cliente de la Tecnología inalámbrica VPN tal como una computadora portátil establezca un túnel VPN con un servidor VPN, es necesario que el cliente consigue asociado con un Punto de acceso ligero (REVESTIMIENTO) que a su vez las necesidades de ser registrado con un WLC. Este documento tiene el REVESTIMIENTO según lo registrado ya con el WLC usando el proceso de descubrimiento de la difusión de la subred local explicado en el registro ligero AP (REVESTIMIENTO) a un regulador LAN de la Tecnología inalámbrica (WLC).

El siguiente paso es configurar el WLC para el VPN.

Terminación VPN y paso

Con las Cisco 4000 Series WLCs anterior que la versión 4, una característica llamada terminación

VPN de IPsec (soporte para IPSec) se utiliza. Esta característica permite a estos reguladores terminar a las sesiones de cliente VPN directamente en el regulador. En resumen, esta característica permite al regulador sí mismo actuar como servidor VPN. Pero esto requiere un módulo de hardware separado de la terminación VPN ser instalada en el regulador.

Esta ayuda de IPsec VPN no está disponible en:

- Cisco 2000 Series WLC
- Cualquier WLCs que funciona con la versión 4.0 o posterior

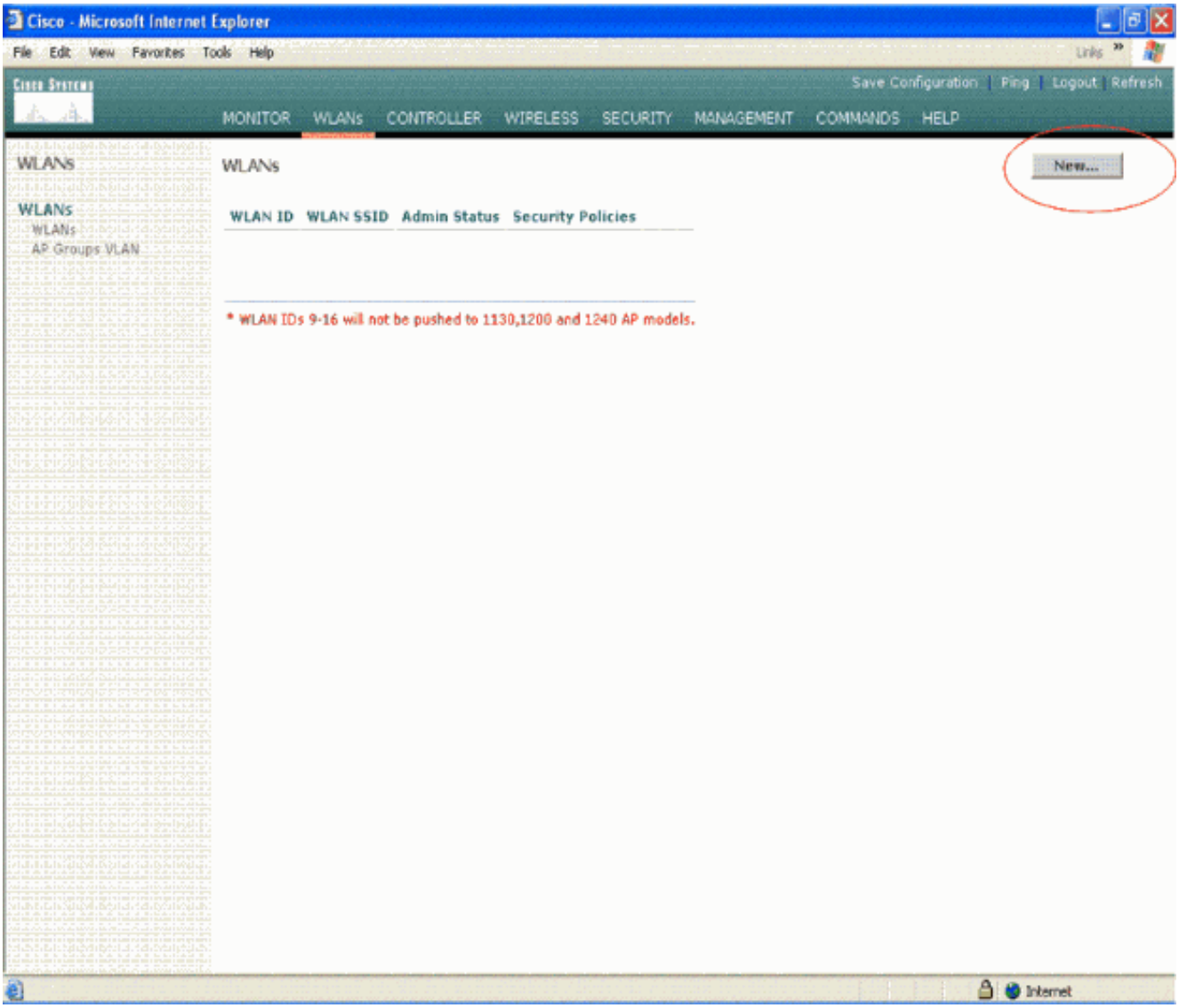
Por lo tanto, la única característica VPN utilizada en las versiones de 4.0 es más adelante paso VPN. Esta característica también se utiliza en las Cisco 2000 Series WLC.

El paso VPN es una característica que permite que un cliente establezca un túnel solamente con un servidor VPN específico. Así pues, si usted necesita tener acceso con seguridad al servidor VPN configurado así como otro servidor VPN o Internet, esto no es posible con el paso VPN activado en el regulador. Bajo tales requisitos, usted necesita inhabilitar el paso VPN. Sin embargo, el WLC se puede configurar para actuar como paso para alcanzar los gatewayes de VPN múltiples cuando un ACL apropiado se crea y se aplica a la red inalámbrica (WLAN) correspondiente. Así pues, bajo tales decorados donde usted quiere alcanzar los gatewayes de VPN múltiples para la Redundancia, inhabilita el paso VPN y crea un ACL que permita el acceso a los gatewayes de VPN y aplica el ACL a la red inalámbrica (WLAN).

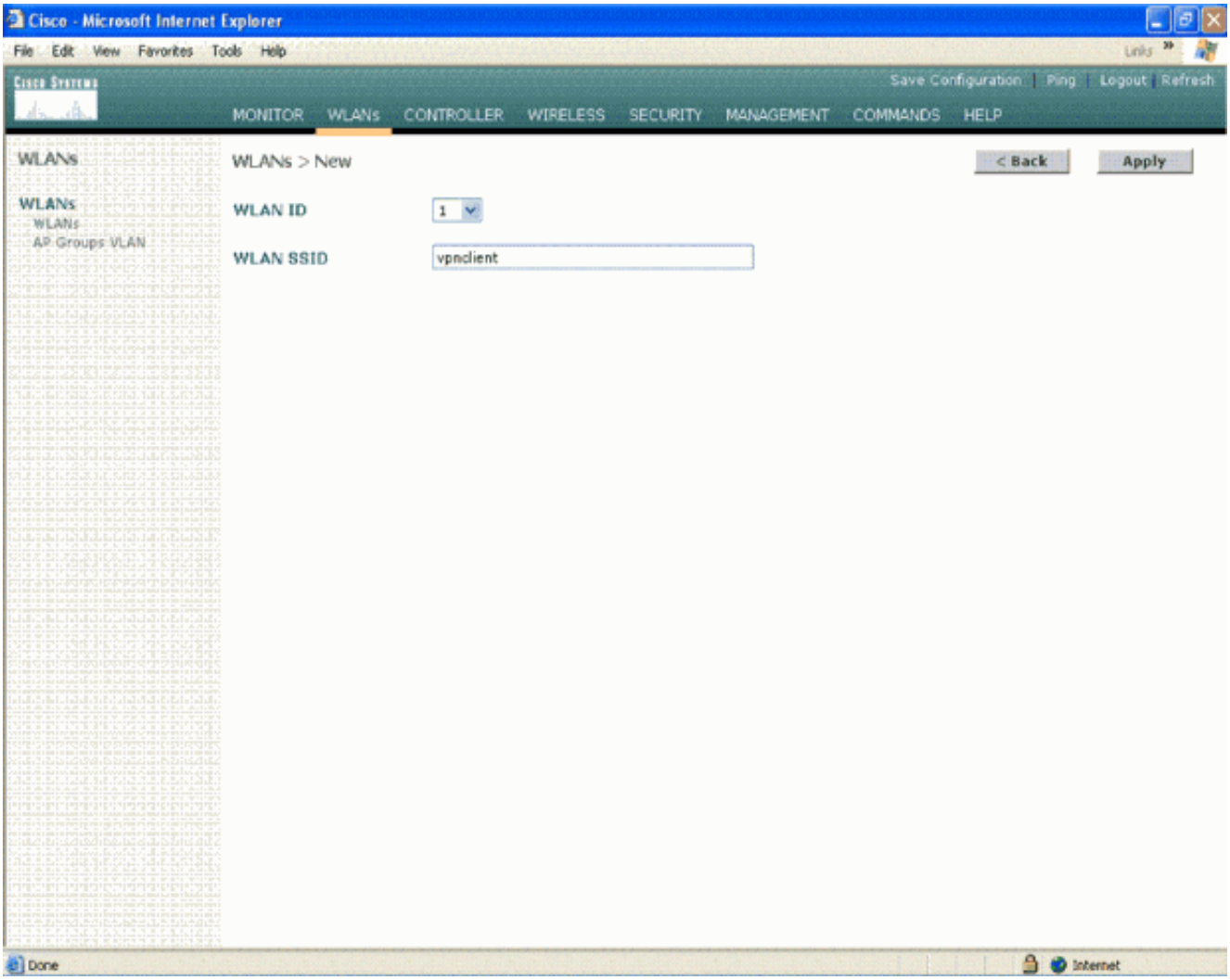
Configure el WLC para el paso VPN

Complete estos pasos para configurar el paso VPN.

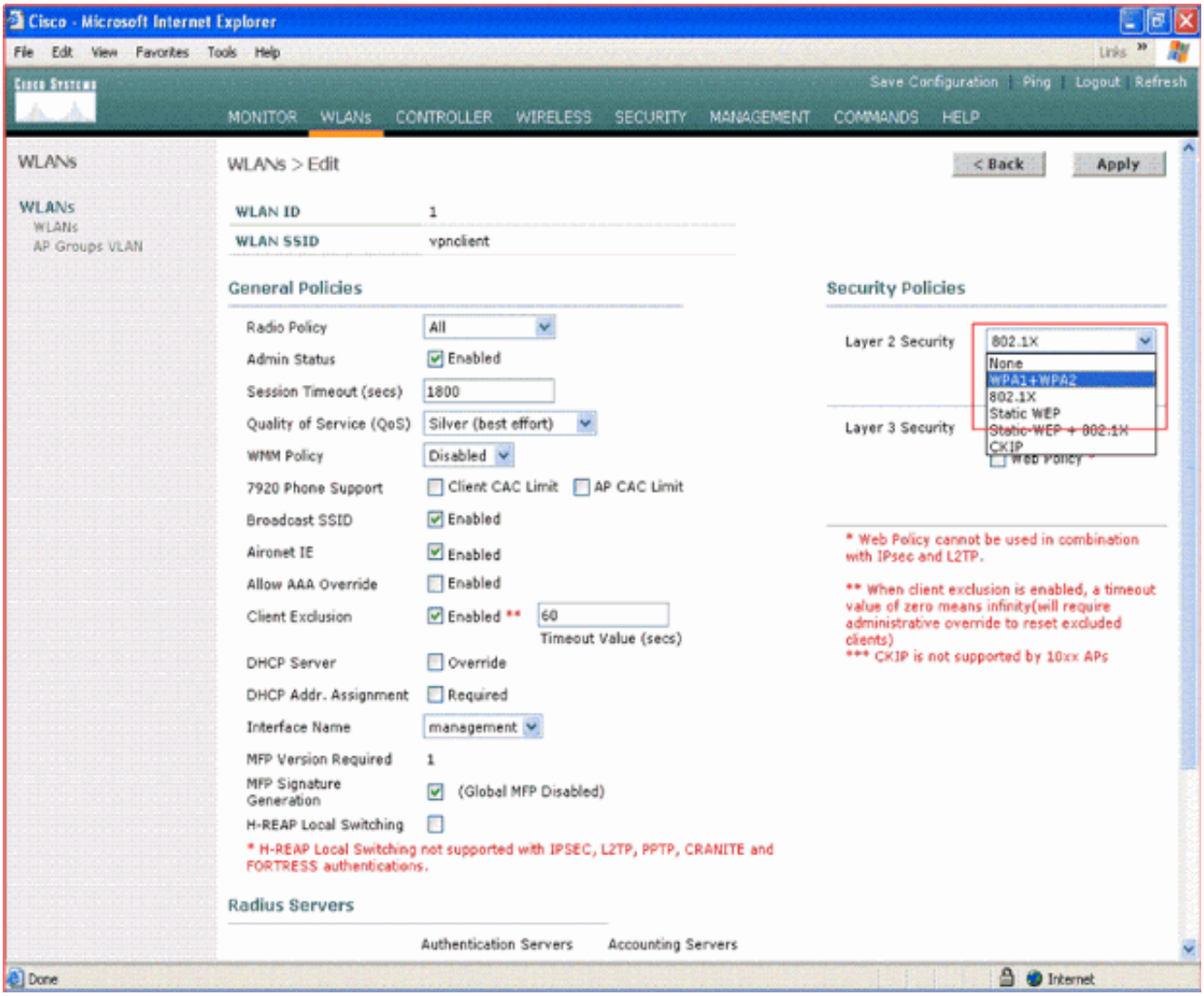
1. Del GUI WLC, haga clic la **red inalámbrica (WLAN)** para ir a la página de las redes inalámbricas (WLAN).
2. Haga clic **nuevo** para crear una nueva red inalámbrica (WLAN).



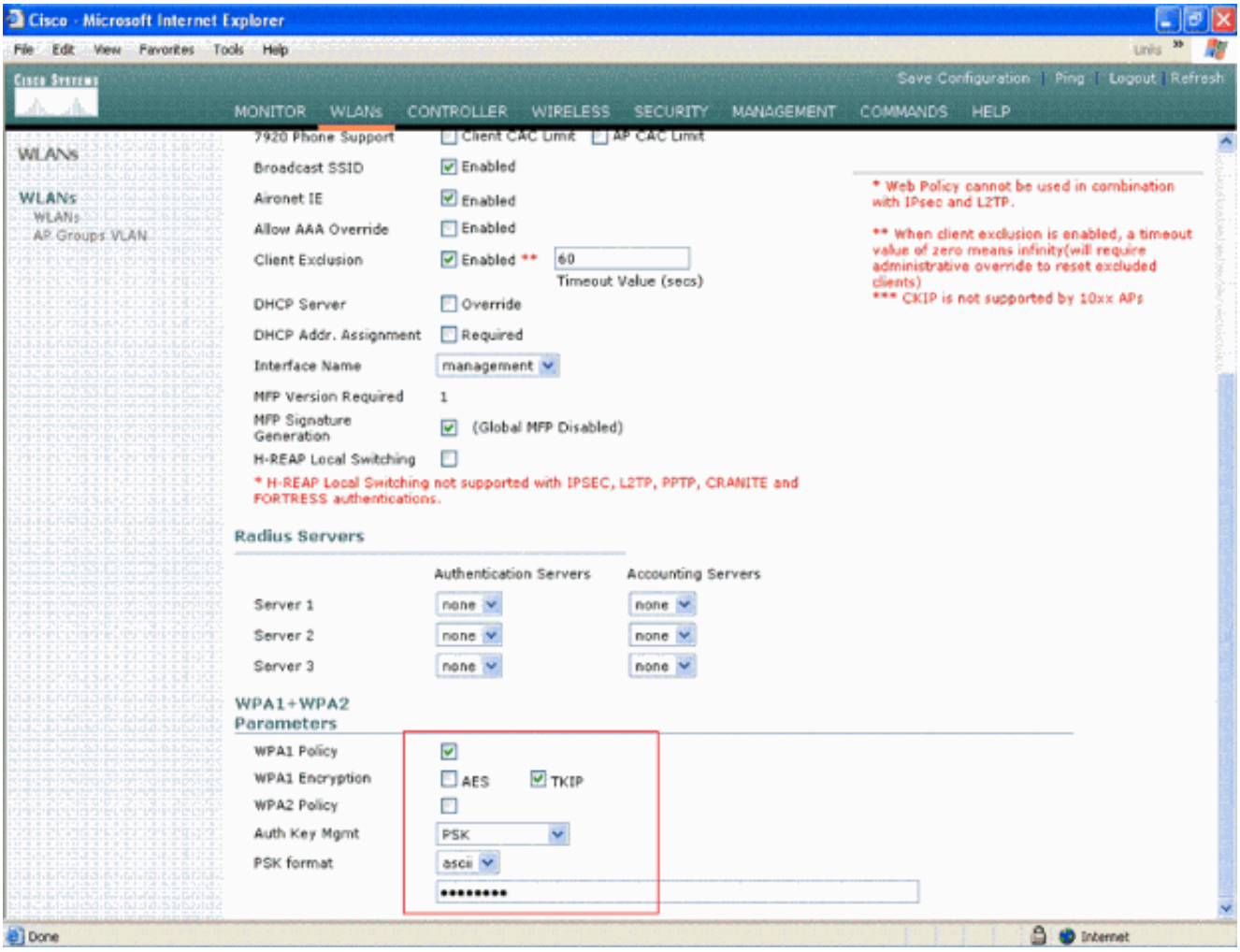
3. La red inalámbrica (WLAN) SSID se nombra como **vpnclient** en este ejemplo. Haga clic en Apply
(Aplicar).



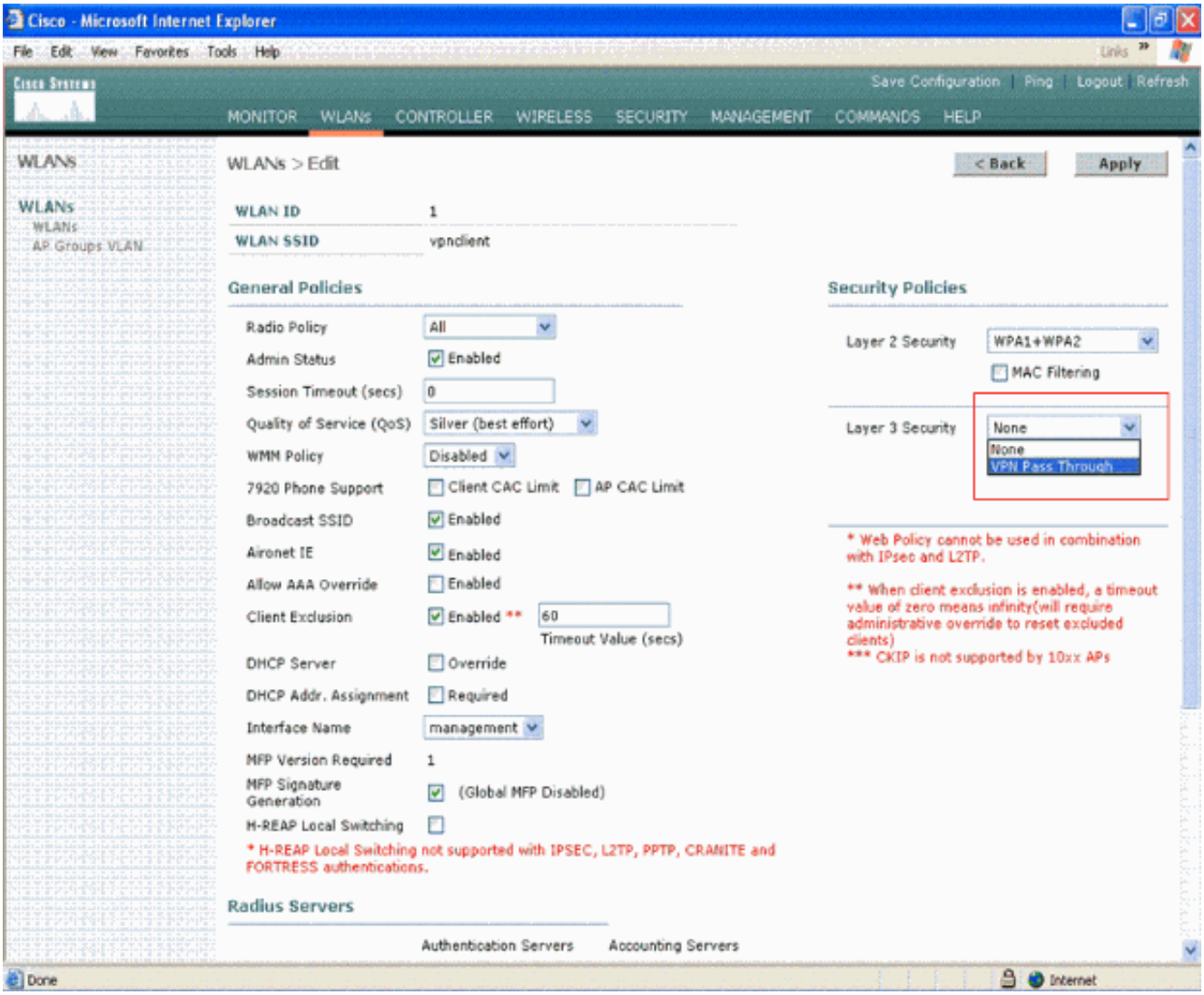
4. Configure el SSID vpnclient con la Seguridad de la capa 2. *Esto es opcional*.Este ejemplo utiliza **WPA1+WPA2** como el tipo de la Seguridad.



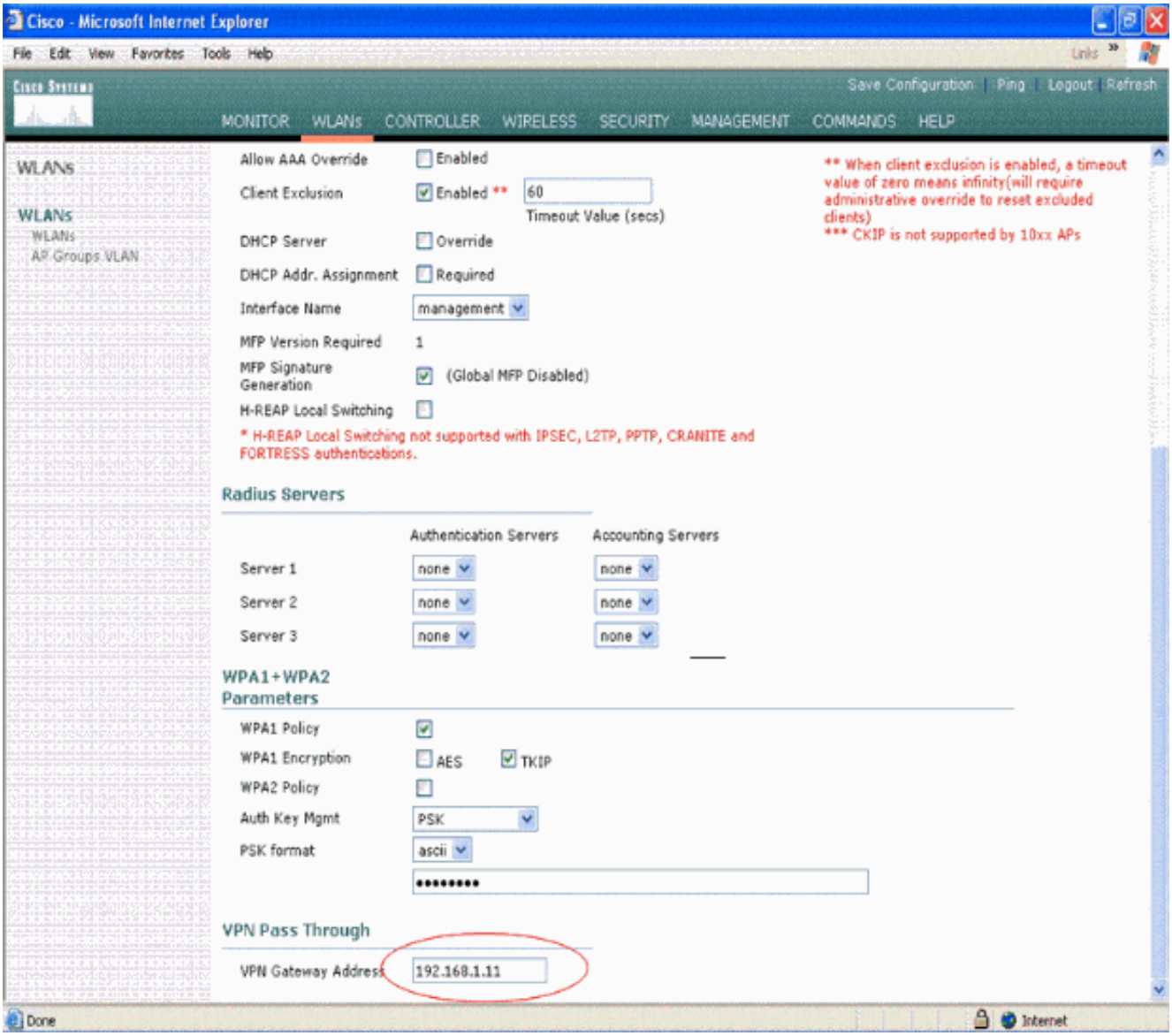
5. Configure la directiva WPA y el tipo de la administración de claves de la autenticación que se utilizarán.Este ejemplo utiliza la **clave previamente compartida (PSK)** para la administración de claves de la autenticación. Una vez que se selecciona PSK, seleccione el **ASCII** mientras que el formato PSK y pulse el valor PSK. Este valor debe ser lo mismo en la configuración SSID del cliente de red inalámbrica para que los clientes que pertenecen a este SSID para asociarse a esta red inalámbrica
(WLAN).



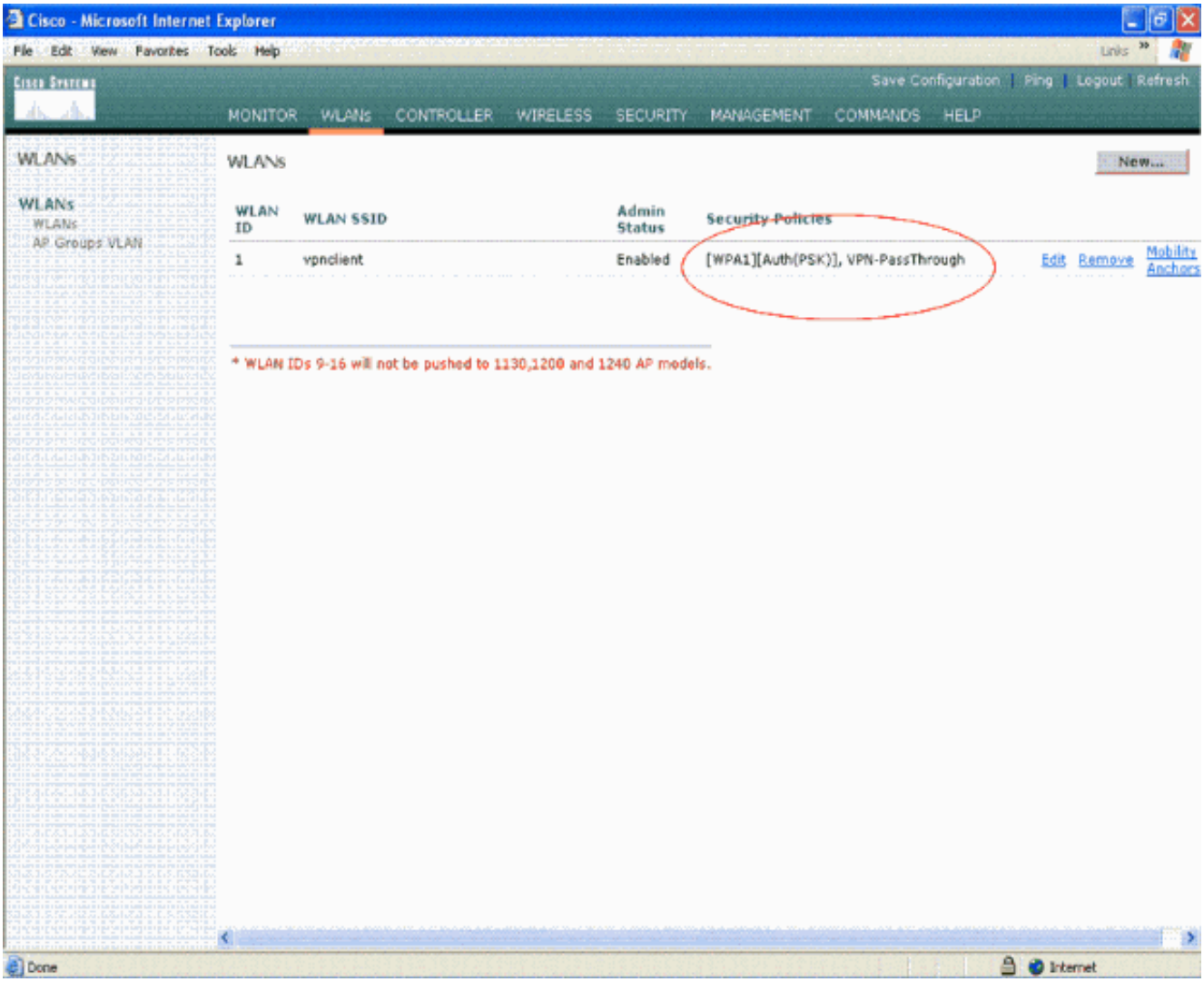
6. Seleccione el **paso VPN** como la Seguridad de la capa 3. Aquí está el ejemplo.



7. Una vez que el paso VPN se selecciona como la Seguridad de la capa 3, agregue el direccionamiento del gateway de VPN como este ejemplo muestra.Esta dirección del gateway debe ser la dirección IP del interfaz que termina el túnel VPN en el lado del servidor. En este ejemplo, la dirección IP del interfaz s3/0 (192.168.1.11/24) en el servidor VPN es la dirección del gateway que se configurará.



8. Haga clic en Apply (Aplicar). La red inalámbrica (WLAN) llamada *vpnclient* ahora se configura para el paso
VPN.



Configuración de servidor VPN

Esta configuración muestra al Cisco 3640 Router como el servidor VPN.

Nota: Para la simplicidad, esta configuración utiliza la encaminamiento estática para mantener el reachability IP entre las puntas del extremo. Usted puede utilizar cualquier protocolo de la encaminamiento dinámica tal como Routing Information Protocol (RIP), Open Shortest Path First (OSPF), y así sucesivamente para mantener el reachability.

Nota: El túnel no se establece si no hay reachability IP entre el cliente y el servidor.

Nota: Este documento asume que el usuario es consciente de cómo activar la encaminamiento dinámica en la red.

Cisco 3640 Router
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
```

Nota: Este ejemplo utiliza solamente la autenticación del grupo. No utiliza la autenticación de usuario individual.

Configuración de cliente VPN

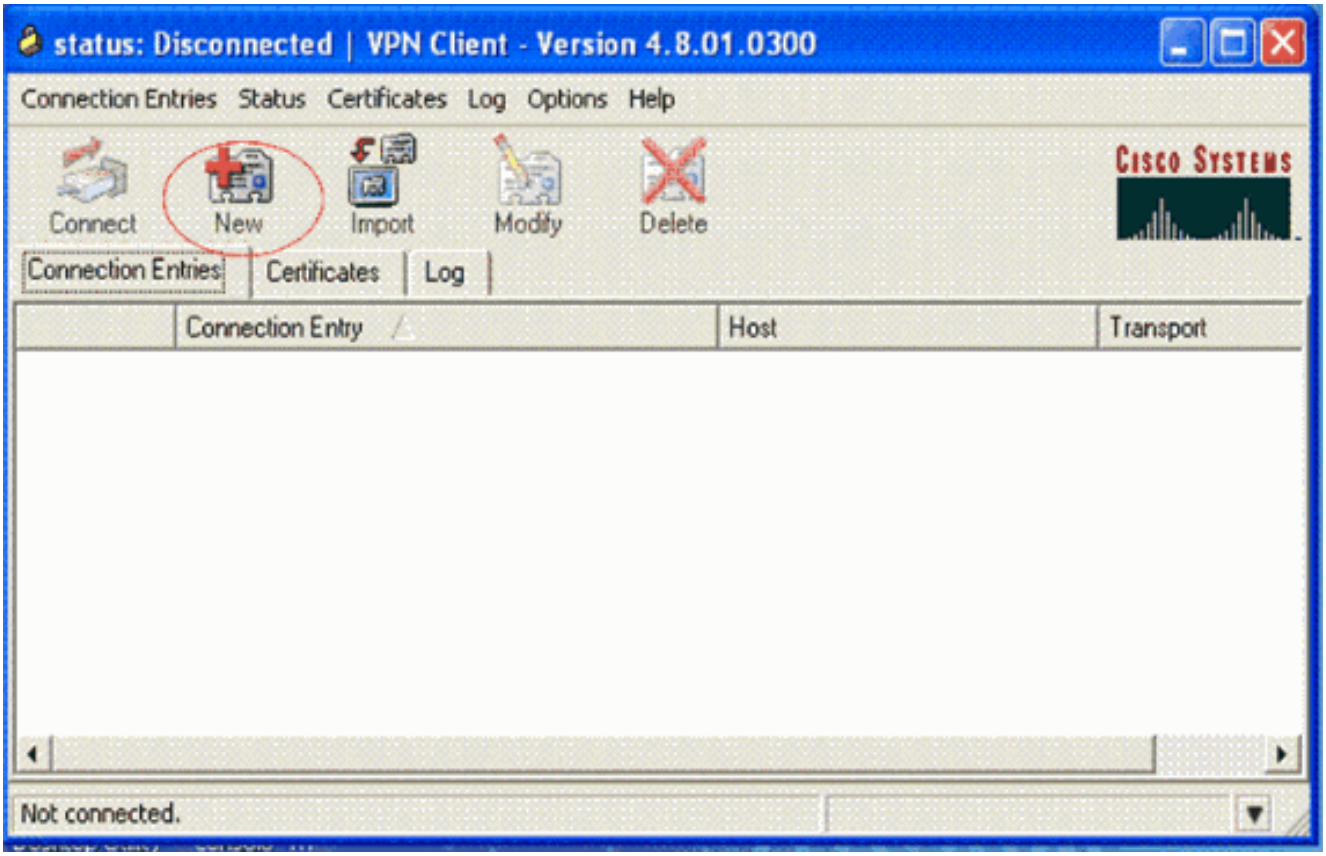
Un cliente del software VPN puede ser descargado del centro de software de Cisco.com.

Nota: Un cierto software de Cisco le requiere abrirse una sesión con un nombre de usuario y contraseña CCO.

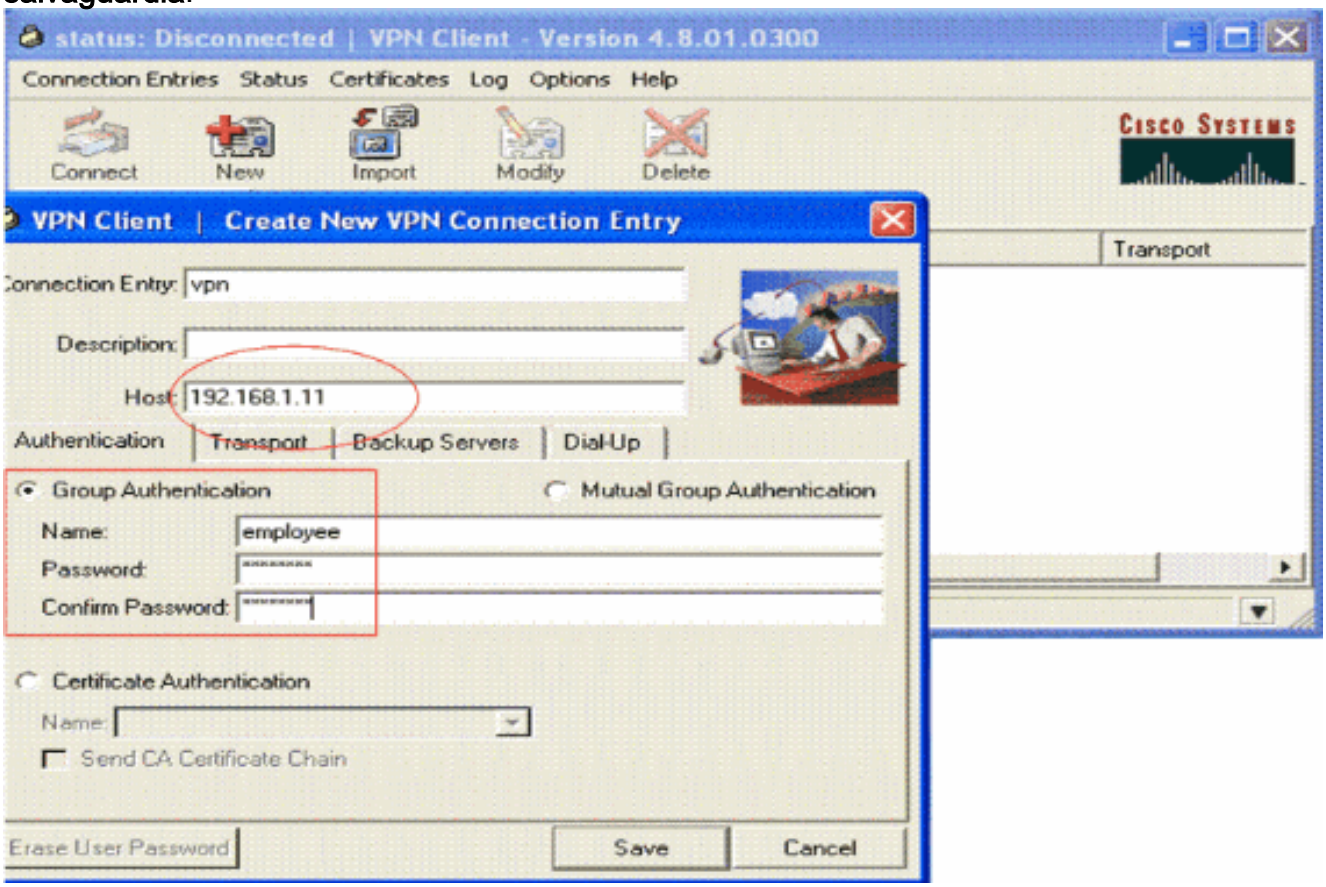
Complete estos pasos para configurar al cliente VPN.

1. Forme a su cliente de red inalámbrica (computadora portátil), elija el **Start (Inicio) > Programs (Programas) > Cisco Systems VPN Client (VPN Client de Cisco Systems) > al cliente VPN** para tener acceso al cliente VPN. Ésta es la ubicación predeterminada en donde el cliente VPN está instalado.
2. Haga clic **nuevo** para lanzar la nueva ventana de la entrada de la conexión VPN del

crear.



3. Ingrese el nombre del Entrada de conexión junto con una descripción. Este usesvpn del ejemplo.El campo Description (Descripción) es opcional. Ingrese el IP address del servidor VPN en el rectángulo del host. Después ingrese el nombre del grupo VPN y la contraseña y haga clic la
salvaguardia.



Nota: El nombre del grupo y la contraseña configurados aquí deben ser lo mismo que el que

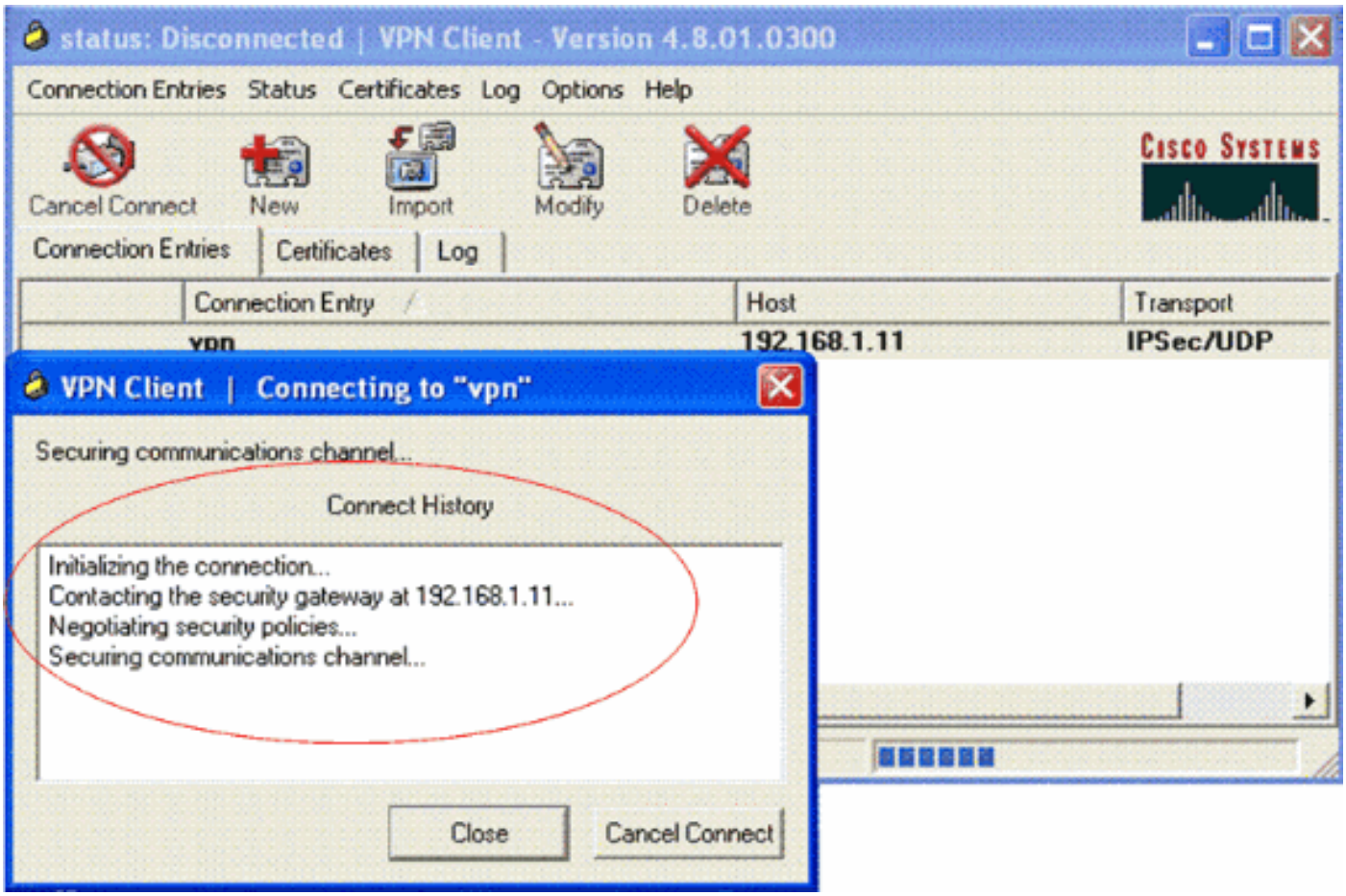
está configurado en el servidor VPN. Este ejemplo utiliza el *empleado* y la contraseña *cisco123 del* nombre.

Verificación

Para verificar esta configuración, configure el SSID **vpnclient** en el cliente de red inalámbrica con los mismos parámetros de Seguridad configurados en el WLC y asocie al cliente a esta red inalámbrica (WLAN). Hay varios documentos que explican cómo configurar a un cliente de red inalámbrica con un nuevo perfil.

Una vez que el cliente de red inalámbrica es asociado, vaya al cliente VPN y haga clic en la conexión que usted ha configurado. Entonces haga clic **conectan de la** ventana principal del cliente VPN.

Usted puede ver los parámetros de la Seguridad de la fase 1 y de la fase 2 negociados entre el cliente y el servidor.



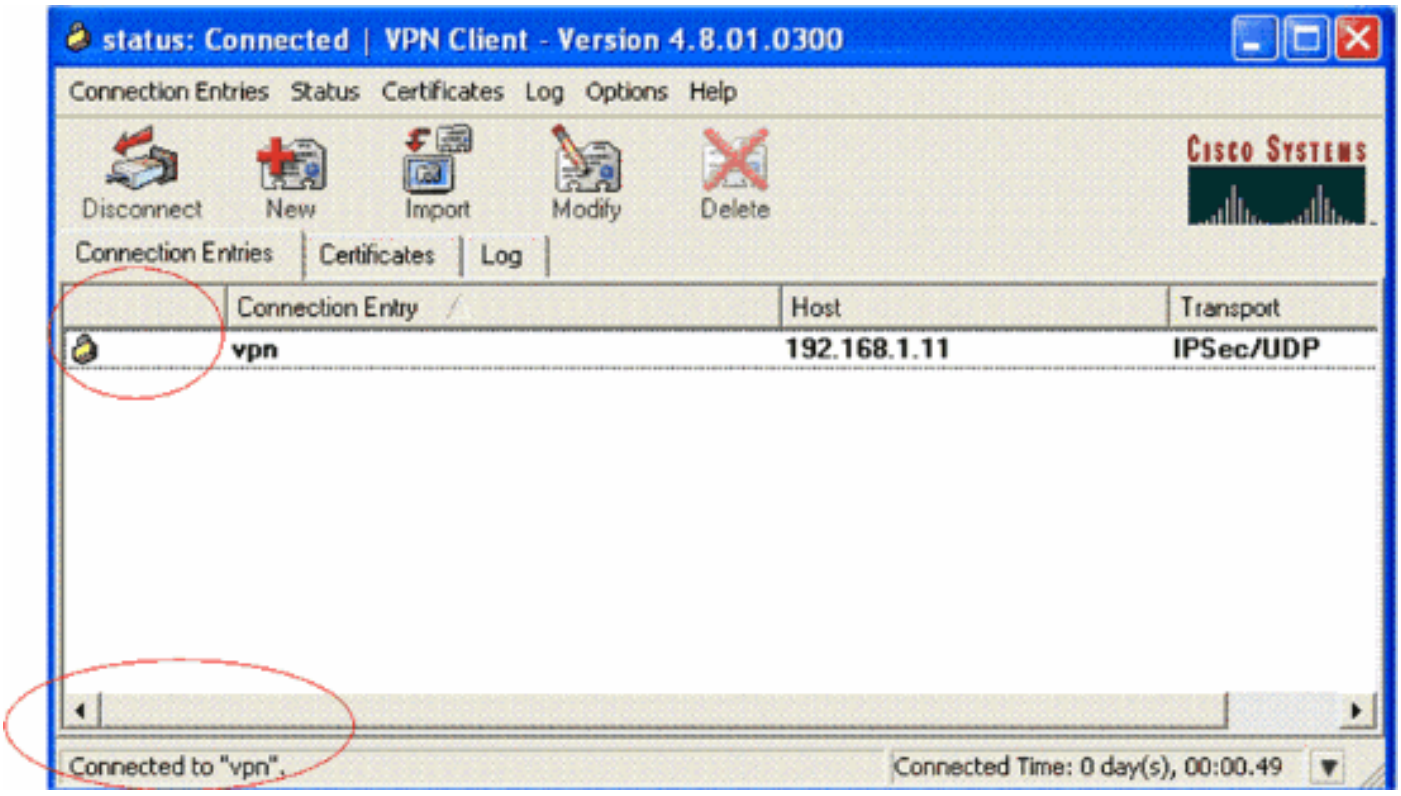
Nota: Para establecer este túnel VPN, el cliente VPN y el servidor deben tener reachability IP entre ellos. Si el cliente VPN no puede entrar en contacto con el gateway de seguridad (servidor VPN), después el túnel no se establece y un cuadro alerta se visualiza en el lado del cliente con este mensaje:

```
vpnrouter#show running-config

Building configuration...

Current configuration : 1623 bytes
```

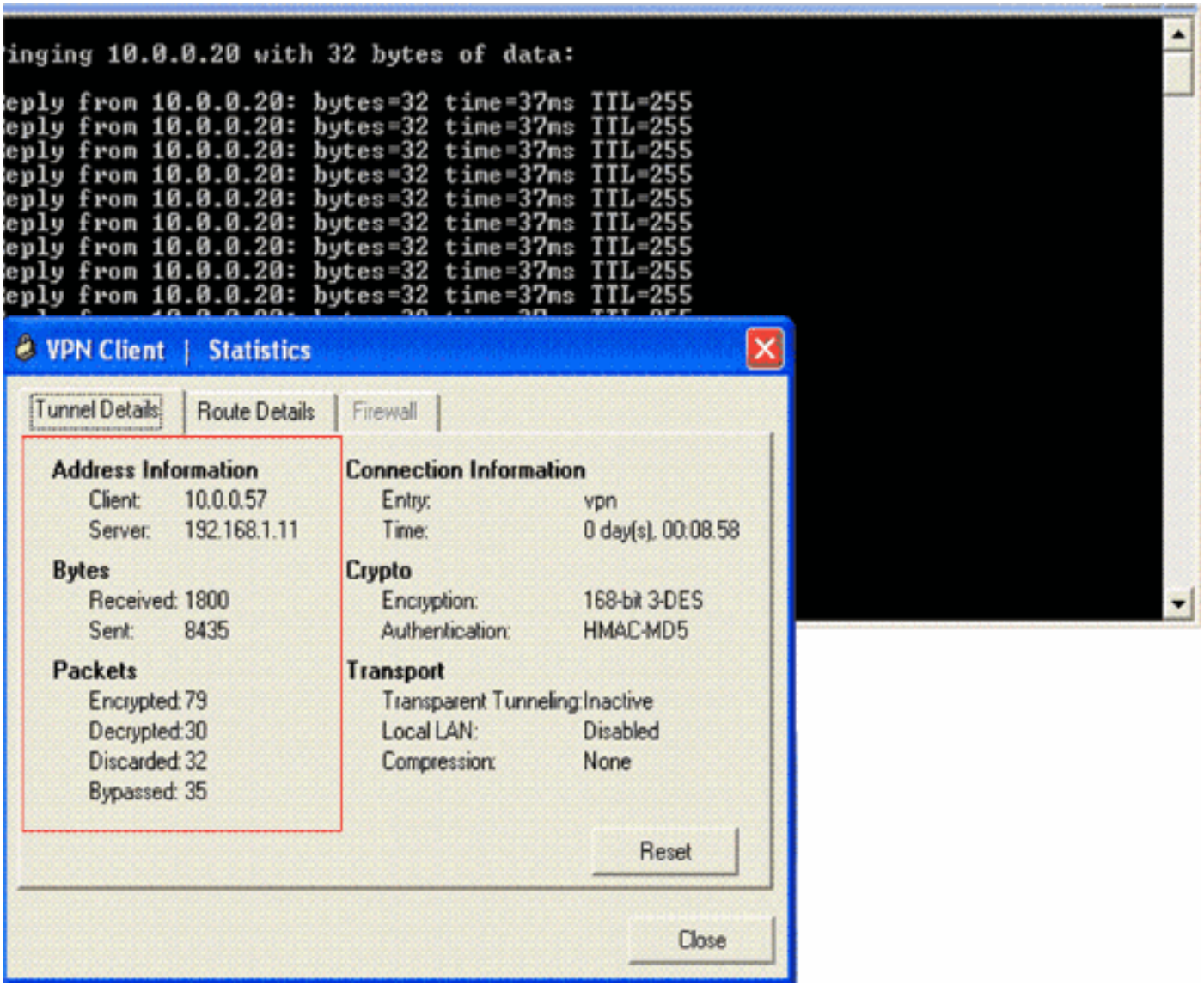
```
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname vpnrouter
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authorization network employee local
!
aaa session-id common
!
resource policy
!
memory-size 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
```

Para asegurarse de que un túnel VPN esté establecido correctamente entre el cliente y servidor, usted puede encontrar un icono del bloqueo que se cree al lado del cliente establecido VPN. La barra de estado también indica **conectado con el "vpn"**. Aquí está un ejemplo.



También, asegúrese de que usted pueda transmitir con éxito los datos al segmento LAN en el lado del servidor del cliente VPN y viceversa. Del menú principal del cliente VPN, elija el **estatus > las estadísticas**. Allí usted puede encontrar las estadísticas de los paquetes encriptados y desencriptados que se pasan a través del túnel.



En este tiro de pantalla, usted puede ver a la dirección cliente como 10.0.0.57. Éste es el direccionamiento que el servidor VPN asigna al cliente de su localmente agrupación configurada después de la negociación acertada de la fase 1. Una vez que se establece el túnel, el servidor VPN agrega automáticamente una ruta a esta dirección IP asignada del DHCP en su tabla de la ruta.

Usted puede también ver el número de paquetes encriptados que aumentan mientras que los datos se transfieren del cliente al servidor y del número de paquetes desencriptados que aumentan durante una Transferencia de datos reversa.

Nota: Puesto que el WLC se configura para el paso VPN, permite que el cliente tenga acceso solamente al segmento conectado con el gateway de VPN (aquí, es servidor VPN de 192.168.1.11) configurado para el paso. Esto filtra el resto del tráfico.

Usted puede verificar esto configurando a otro servidor VPN con la misma configuración y configurar una entrada de la nueva conexión para este servidor VPN en el cliente VPN. Ahora, cuando usted intenta establecer un túnel con este servidor VPN, no es acertado. Esto es porque el WLC filtra este tráfico y permite un túnel solamente al direccionamiento del gateway de VPN configurado para el paso VPN.

Usted puede también verificar la configuración del CLI del servidor VPN.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice el OIT para ver un análisis de la **salida del comando show**.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Estos **comandos show** usados en el servidor VPN pudieron también ser útiles para ayudarle a verificar el estado del túnel.

- Se utiliza el comando de **sesión de criptografía de la demostración** de verificar el estado del túnel. Aquí está una salida de ejemplo de este comando.

```
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
```

- **La directiva crypto del isakmp de la demostración** se utiliza para ver los parámetros configurados de la fase 1.

Troubleshooting

Los comandos debug and show explicados en la sección del verificar pueden también ser utilizados para resolver problemas.

- debug crypto isakmp
- **ipsec crypto de la depuración**
- **show crypto session**

- **El comando debug crypto isakmp** en el servidor VPN visualiza el proceso de negociación entero de la fase 1 entre el cliente y el servidor. Aquí está un ejemplo de una negociación acertada de la fase 1.

```
------------------------------------------------------------------
 ----------------------------------------------------------
----------------------------------------------------------------
*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
```

- El comando debug crypto ipsec en el servidor VPN visualiza el IPSec Negotiation de la fase 1 y la creación acertados del túnel VPN. Aquí tiene un ejemplo:

```
---------------------------------------------------------------------
 ---------------------------------------------------------------------
---------------------------------------------------------------------
*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
```

Información Relacionada

- Una Introducción al encripción de seguridad IP (IPSec)
- Página de Soporte del Protocolo IKE/la Negociación de IPSec
- Configurar el IPSec Network Security
- Q&A del Cisco Easy VPN
- Guía de configuración del Controlador de LAN de la Red Inalámbrica Cisco, versión 4.0
- ACL en el ejemplo inalámbrico de la configuración del regulador LAN
- FAQ inalámbrico del regulador LAN (WLC)
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems