Configuración de la iniciación automática de VPN en Cisco VPN Client dentro de un entorno de LAN inalámbrico.

Contenido

Introducción

Este documento describe cómo configurar al Cliente Cisco VPN para iniciar automáticamente las conexiones del IPSec VPN a los concentradores del Cisco VPN 3000 en entorno atados con alambre/del Wireless LAN (red inalámbrica (WLAN)).

En el entorno WLAN, el cliente de red inalámbrica primero se asocia a un unto de acceso de red inalámbrica (AP). De acuerdo con el alcance del IP Address que recibe de la conexión de red inalámbrica, el cliente VPN instalado en la Tecnología inalámbrica pone en marcha automáticamente una petición de conexión VPN al concentrador VPN correspondiente en el sitio. La conexión del IPSec VPN entonces se utiliza para asegurar el tráfico de la Tecnología inalámbrica 802.11x. Sin el establecimiento exitoso de la conexión del Cisco VPN, los clientes de red inalámbrica no tienen ningún acceso a los recursos de red.

Esta configuración de muestra muestra la configuración del cliente VPN para habilitar la característica del autoinitiation.

prerrequisitos

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Requisitos

Antes de que usted intente esta configuración, asegúrese de que usted sea familiar con estos conceptos:

- Entienda cómo configurar y configurar el Cliente Cisco VPN y el Cisco VPN 3000 Concentrator para establecer un túnel del IPSec VPN
- Entienda las configuraciones relacionadas con la Tecnología inalámbrica LAN

Componentes Utilizados

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

- Cliente VPN de Cisco versión 4.x
- Versión 3.6 del Cisco VPN 3000 Concentrator
- Punto de acceso del Cisco Aironet de la serie 340
- Adaptador de red inalámbrica LAN del Cisco Aironet de la serie 350 (versión 5.0.1)

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.

Nota: En este ejemplo, utilizan al Cisco Network Registrar como un servidor del Protocolo de configuración dinámica de host (DHCP) para proporcionar los IP Addresses a los clientes de red inalámbrica y a los clientes VPN.

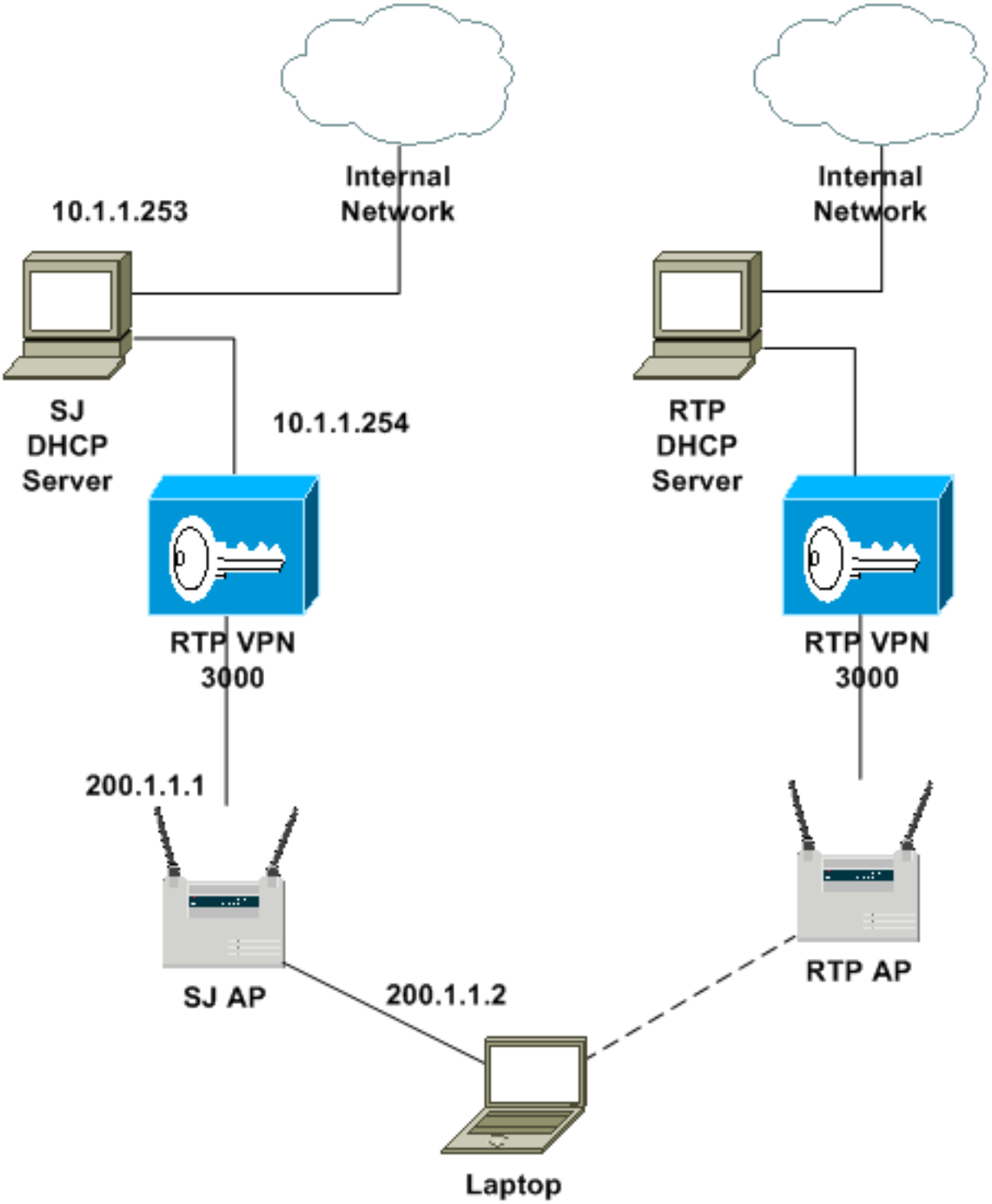
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: En esta configuración, utilizan al servidor DHCP SJ para proporcionar los IP Addresses a las conexiones de red inalámbrica y a las conexiones VPN. Hace dos alcances del IP Address definir:

- Para las conexiones de red inalámbrica, los usuarios de red inalámbrica reciben una dirección IP en el rango de 200.1.1.50 a 200.1.1.250.
- Para las conexiones VPN, los clientes VPN reciben una dirección IP en el rango de 50.1.1.1 a 50.1.1.254.

Configuraciones

En este ejemplo, sobre la base en cuyo de sitio el usuario vaga por, el cliente de red inalámbrica inicia automáticamente cualquiera una de las dos conexiones VPN (a saber SJWireless o

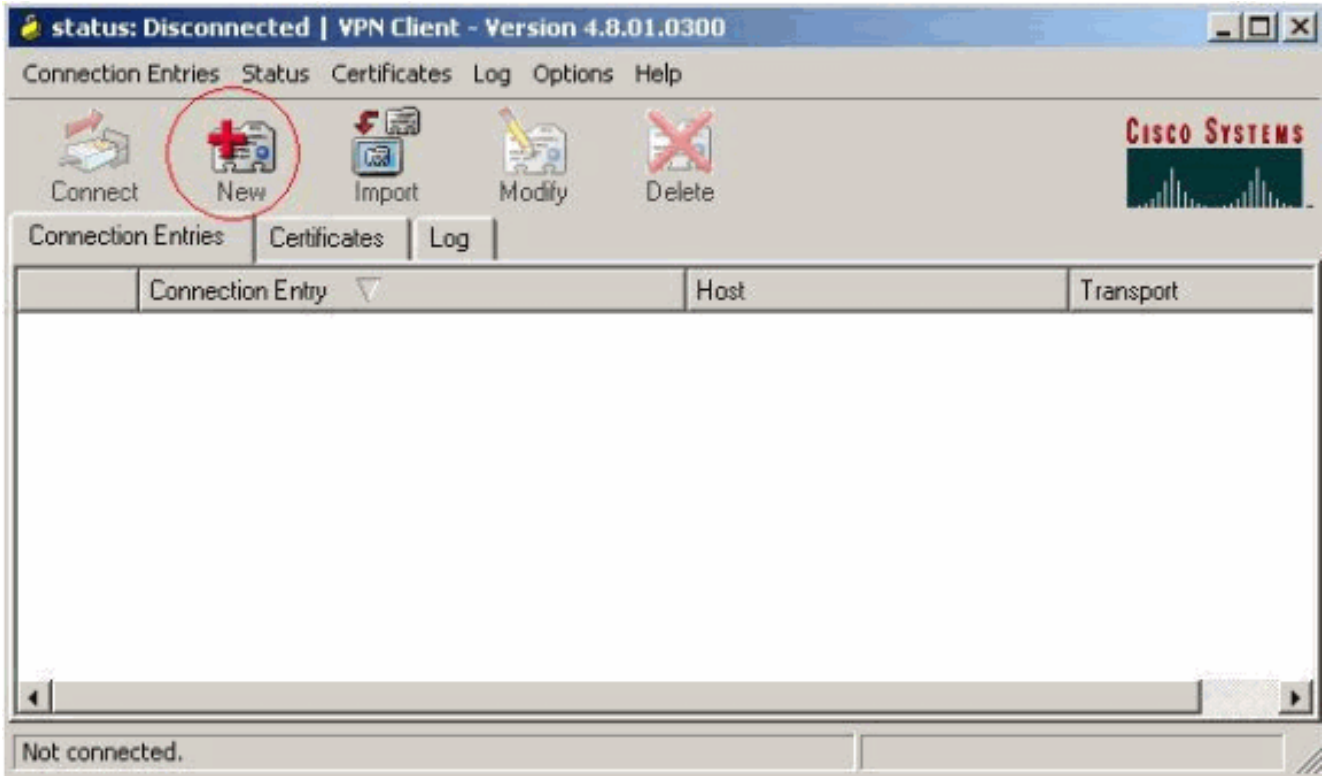
RTPWireless) que se predefinen en el dialer VPN. Más concretamente, si el usuario de red inalámbrica consigue una dirección IP en el rango de 200.1.1.0/24 de la asociación de red inalámbrica al SJ AP, pone en marcha la conexión SJWireless del dialer VPN. Si consigue una dirección IP en el rango de 150.1.1.0/24 de la asociación de red inalámbrica al RTP AP, pone en marcha la conexión RTPWireless del dialer VPN.

En esta sección, las conexiones VPN primero se configuran bajo el dialer VPN, después el archivo del vpnclient.ini se edita para agregar la configuración de la iniciación automática. Una vez que estos pasos se acaban en un cliente VPN, los perfiles generados VPN (archivos del .pcf) y el vpnclient.ini configurado se pueden empaquetar, junto con la imagen del cliente VPN, para distribuir a los usuarios finales. El lanzamiento de la conexión VPN es transparente a los usuarios finales después de la instalación del cliente VPN.

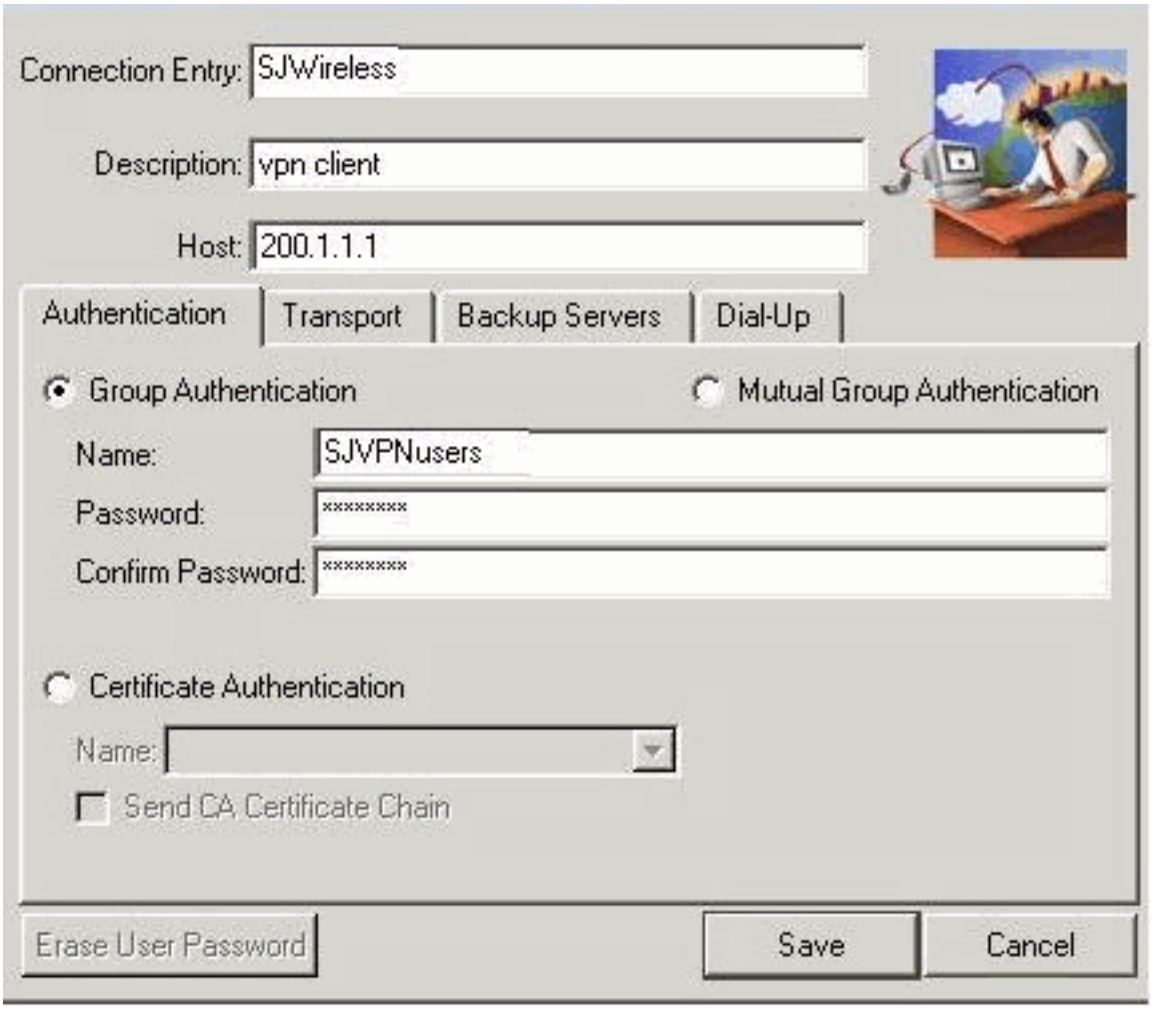
Configuración del dialer VPN

Complete estos pasos para la configuración:

1. Elija el Start (Inicio) > Programs (Programas) > Cisco Systems VPN Client (VPN Client de Cisco Systems) > al cliente VPN. Haga clic **nuevo** para iniciar la nueva ventana de entrada de la conexión VPN del
   crear.



2. Ingrese el nombre del Entrada de conexión junto con una descripción. Ingrese el IP Address externo del concentrador VPN en el rectángulo del host. Entonces ingrese el nombre del grupo VPN y la contraseña, y haga clic la
   salvaguardia.



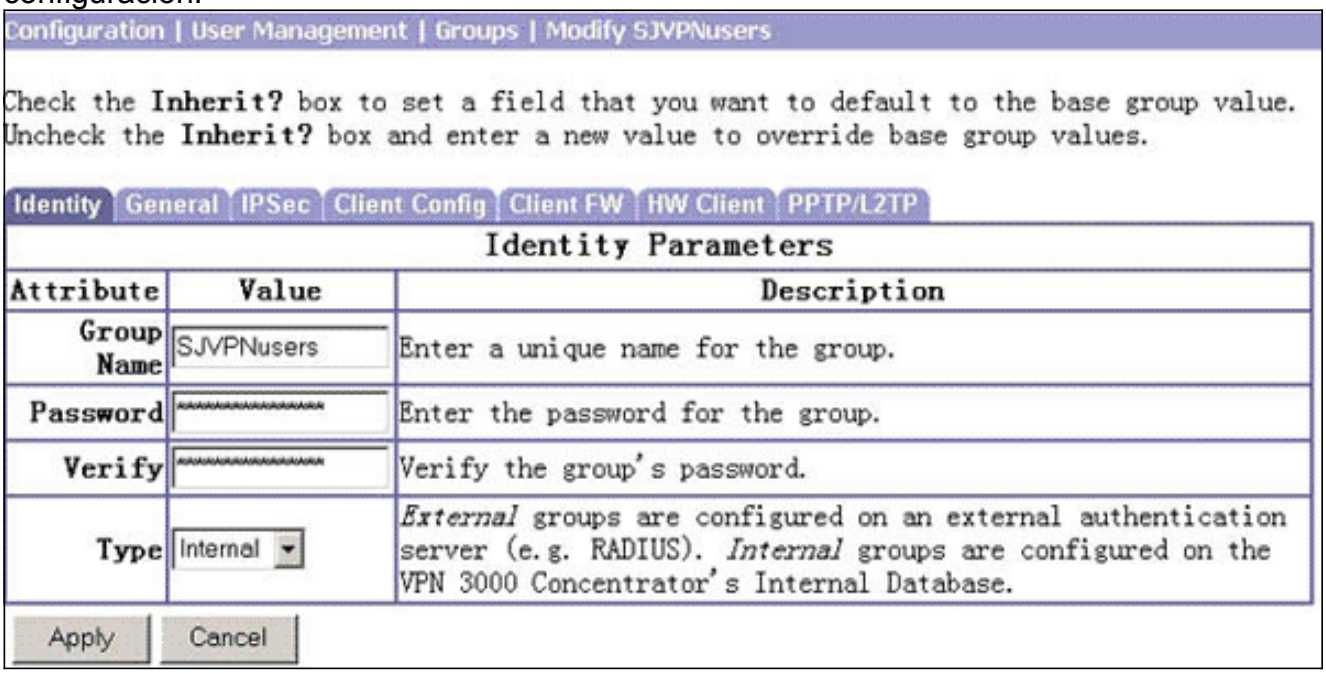
3. Relance los pasos 1 y 2 para crear otra conexión VPN con el nombre **RTPWireless del** marcador del Cisco VPN.Cuando el segundo proceso de configuración es completo, dos perfiles de la conexión VPN nombraron SJWireless.pcf y RTPWireless.pcf se generan en PC del cliente.
4. Complete estos pasos para editar el archivo predeterminado del vpnclient.ini encontrado en PC del cliente para habilitar la característica del autoinitiation:Habilite la característica del autoinitiation con **palabra clave para activar el inicio automático** bajo sección del [main].Defina el **AutoInitiationList**. Cada elemento en la lista corresponde a una sección, donde está asociado el nombre del alcance del IP Address de la conexión VPN y de la Tecnología inalámbrica.En este ejemplo, la conexión SJWireless VPN corresponde a 200.1.1.0/24 y la conexión RTPWireless corresponde a 150.1.1.0/24.Cuando camina a y b son completos, el vpnclient.ini del archivo parece esto:`[LOG.CVPND]`
`LogLevel=1`
`[LOG.CERT]`
`LogLevel=3`
`[LOG.PPP]`
`LogLevel=2`
`[LOG.CM]`
`LogLevel=1`
`[LOG.IPSEC]`
`LogLevel=3`
`[main]`
`AutoInitiationEnable=1 AutoInitiationRetryInterval=3 AutoInitiationList=SJVPN,RTPVPN`
`EnableLog=1` **`[SJVPN] Network=200.1.1.0 Mask=255.255.255.0 ConnectionEntry=SJWireless`**
`[RTPVPN] Network=150.1.1.0 Mask=255.255.255.0 ConnectionEntry=RTPWireless` `RunAtLogon=0`
`EnableLog=1 XAuthHandler=ipsxauth.exe IsNoTrayIcon=0 StatefulFirewall=0 [LOG.DIALER]`
`LogLevel=2 [LOG.IKE] LogLevel=3 [LOG.XAUTH] LogLevel=3 [LOG.CLI] LogLevel=1 [LOG.FIREWALL]`
`LogLevel=1`

5. Después de que los pasos 1 - 3 sean completos en un cliente VPN, el vpnclient.ini y los perfiles de la conexión VPN (.pcf) se pueden recoger y distribuir a los usuarios finales en el paquete de la instalación. Refiera al guía del administrador VPNCLIENT, libere 3.6 para la información sobre cómo preconfigurar a los clientes VPN para los usuarios remotos.

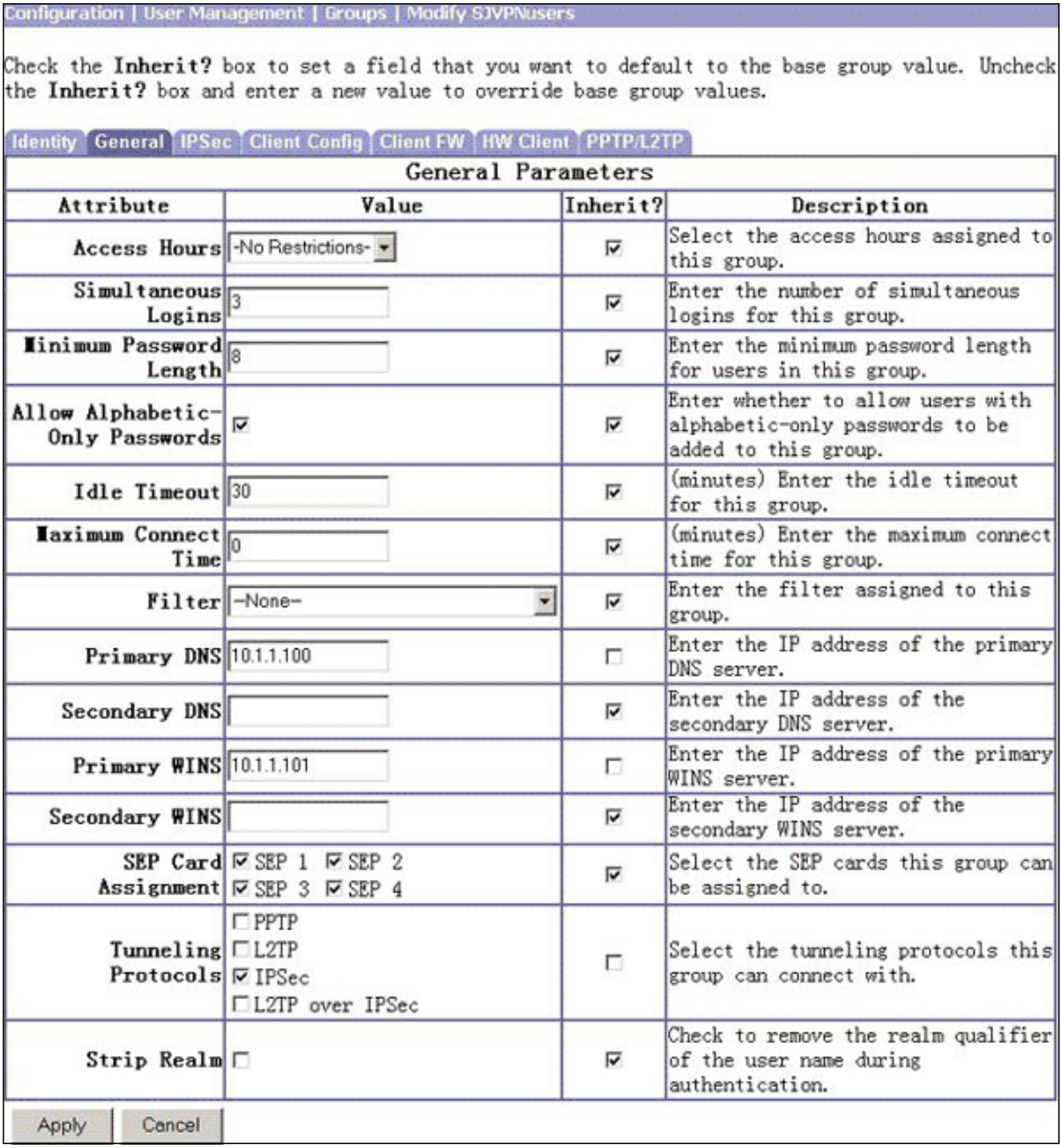
Configuración del concentrador VPN 3000 de Cisco

Complete estos pasos para la configuración:

1. En los concentradores VPN 3000, los grupos VPN necesitan ser configurados para establecer conexión IPSec con el cliente VPN. En el ejemplo, los usuarios de red inalámbrica pueden conectar con diversos concentradores VPN basados en el sitio en el cual vagan por. Aquí, solamente las tareas de configuración importantes en el concentrador VPN SJ se resaltan. Se crea un grupo VPN llamó a **SJVPNusers**, que hace juego el nombre del grupo VPN en el cliente.
2. Elija el **Configuration (Configuración)>User Management (Administración del usuario) >Groups (Grupos)** y elija el **SJVPNusers de la** lista del grupo actual. Selecto **modifique al grupo de la** opción Actions (Acciones) si crean al grupo ya, o **agregue al grupo** y después **modifique al grupo** si el grupo debe ser creado.
3. Haga clic la lengueta de la identidad.Ventana Identity Parameters (Parámetros de identidad) aparece. Verifique que la información visualizada en esta ventana esté correcta para su configuración.



4. Haga clic la ficha general y después marque el cuadro del **IPSec** para el atributo de los protocolos de
túneles.



Configuration | User Management | Groups | Modify SJVPNusers

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

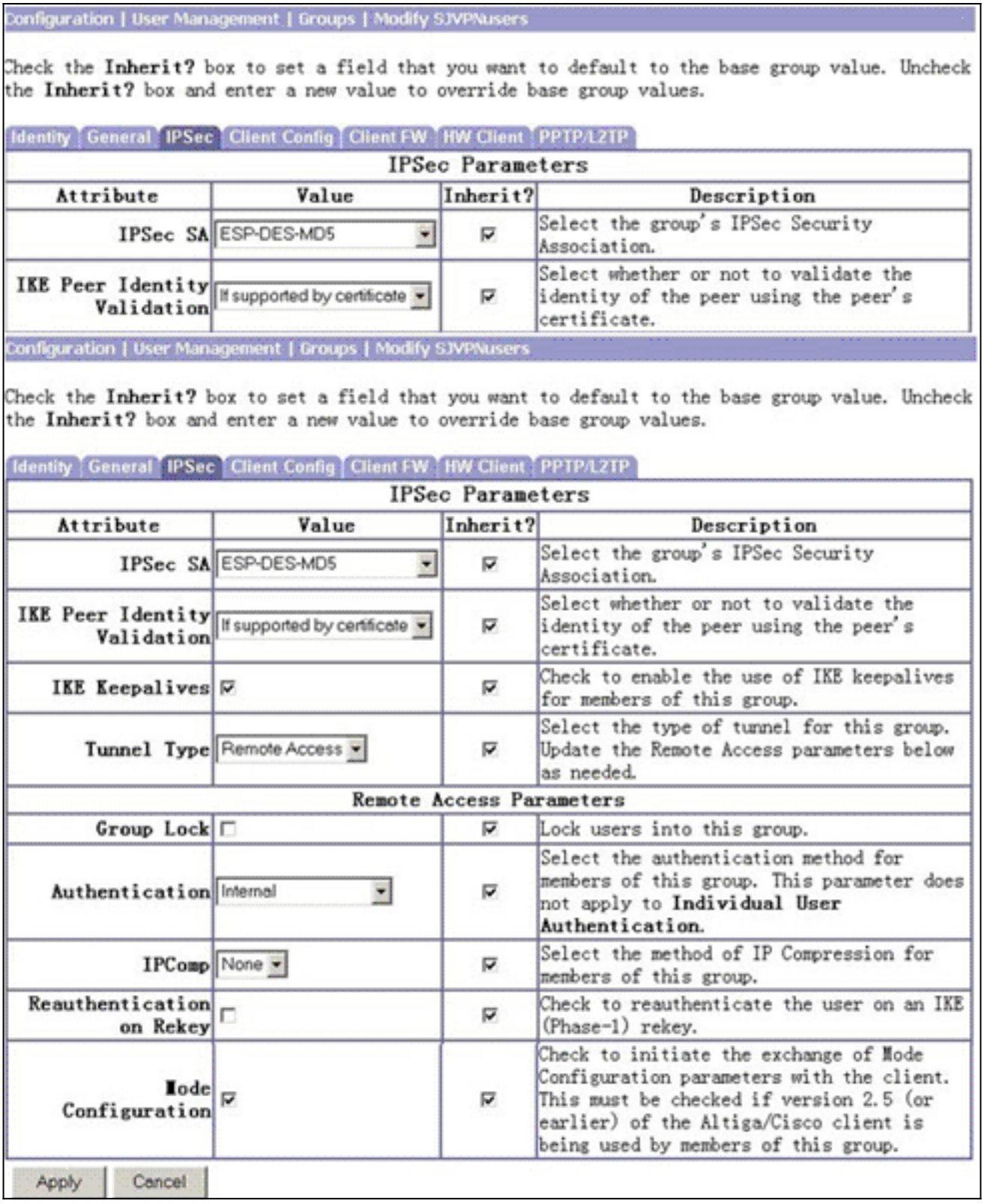
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	☑	Select the access hours assigned to this group.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	☑	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this group.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	-None-	☑	Enter the filter assigned to this group.
Primary DNS	10.1.1.100	☐	Enter the IP address of the primary DNS server.
Secondary DNS		☑	Enter the IP address of the secondary DNS server.
Primary WINS	10.1.1.101	☐	Enter the IP address of the primary WINS server.
Secondary WINS		☑	Enter the IP address of the secondary WINS server.
SEP Card Assignment	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	☑	Select the SEP cards this group can be assigned to.
Tunneling Protocols	☐ PPTP ☐ L2TP ☑ IPSec ☐ L2TP over IPSec	☐	Select the tunneling protocols this group can connect with.
Strip Realm	☐	☑	Check to remove the realm qualifier of the user name during authentication.

Apply | Cancel

5. Haga clic la lengueta del IPSec, después especifique la asociación de seguridad IPSec (SA) y el atributo del método de autentificación con los menús desplegables y las casillas de verificación proporcionados.En este caso, definen a los usuarios de VPN localmente en el concentrador VPN 3000, así que el método de autentificación es interno.



Configuration | User Management | Groups | Modify SJVPNusers

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

Attribute	Value	Inherit?	Description
IPSec SA	ESP-DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.

Configuration | User Management | Groups | Modify SJVPNusers

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

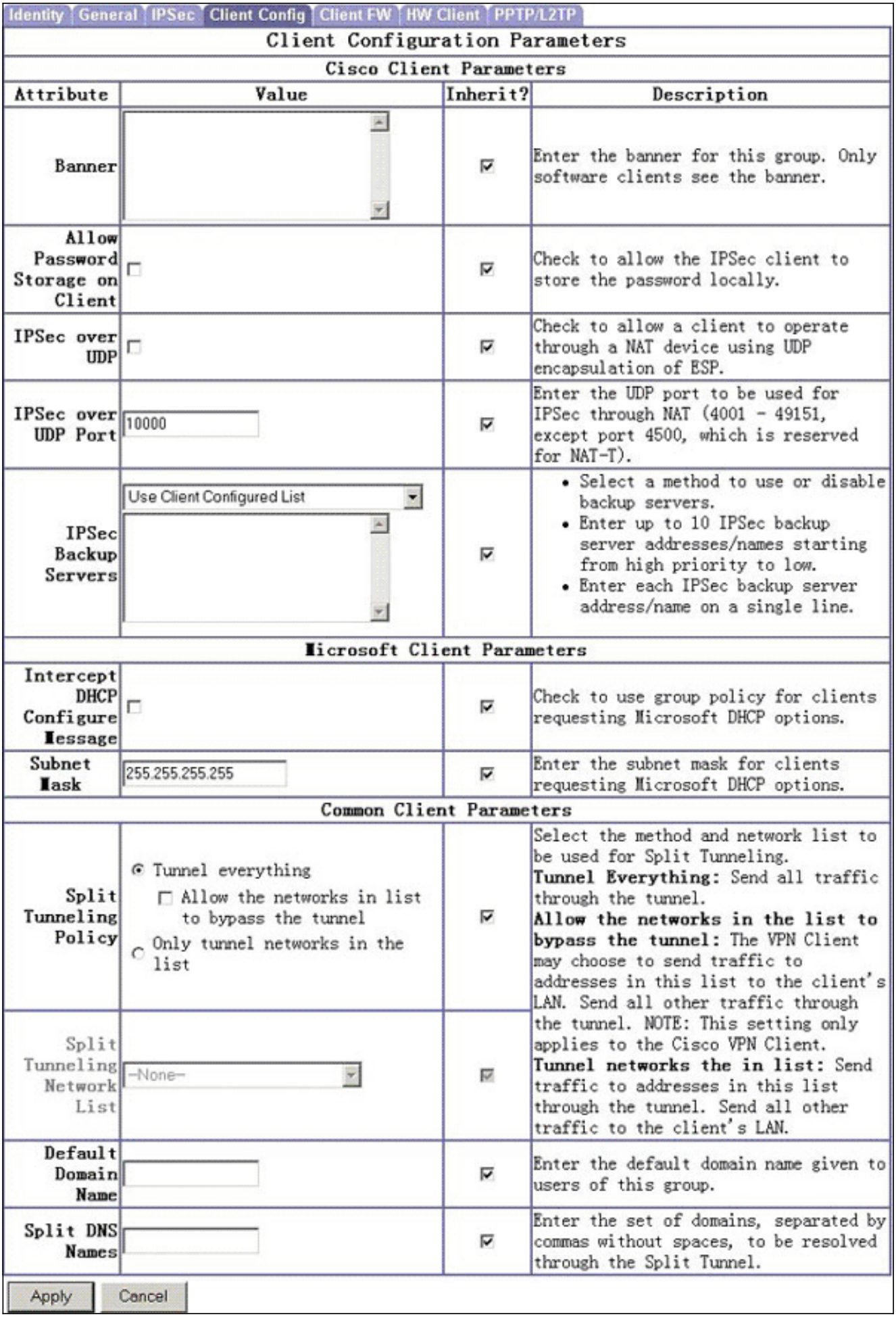
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

IPSec Parameters

Attribute	Value	Inherit?	Description
IPSec SA	ESP-DES-MD5	☑	Select the group's IPSec Security Association.
IKE Peer Identity Validation	If supported by certificate	☑	Select whether or not to validate the identity of the peer using the peer's certificate.
IKE Keepalives	☑	☑	Check to enable the use of IKE keepalives for members of this group.
Tunnel Type	Remote Access	☑	Select the type of tunnel for this group. Update the Remote Access parameters below as needed.
Remote Access Parameters			
Group Lock	☐	☑	Lock users into this group.
Authentication	Internal	☑	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.
IPComp	None	☑	Select the method of IP Compression for members of this group.
Reauthentication on Rekey	☐	☑	Check to reauthenticate the user on an IKE (Phase-1) rekey.
Mode Configuration	☑	☑	Check to initiate the exchange of Mode Configuration parameters with the client. This must be checked if version 2.5 (or earlier) of the Altiga/Cisco client is being used by members of this group.

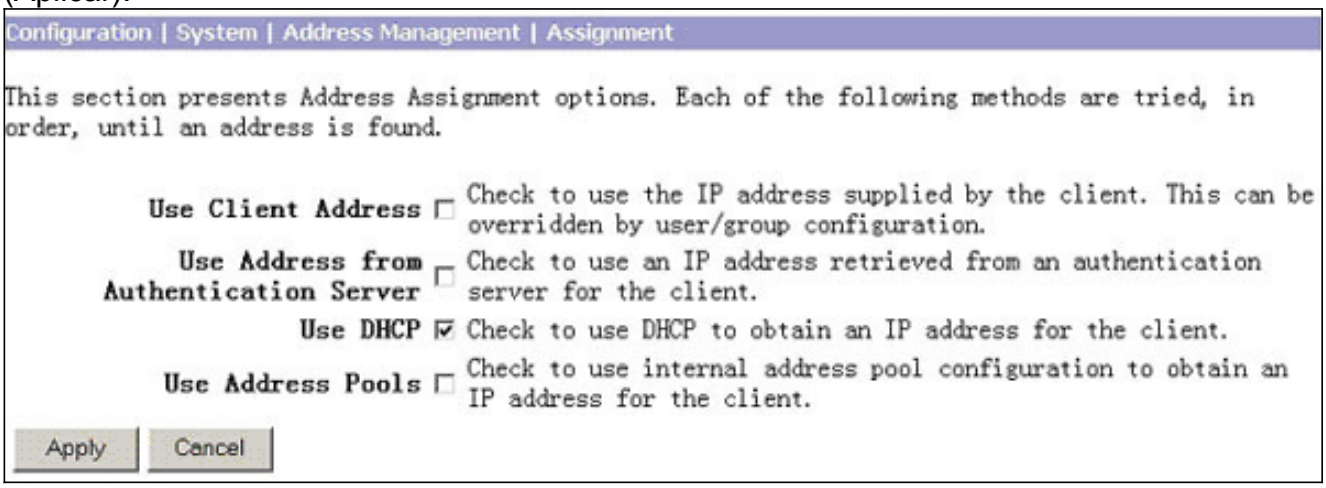
Apply | Cancel

6. Haga clic la ficha de configuración del cliente, después especifique los parámetros de la configuración de modo en la ventana de parámetros de la configuración del cliente. Haga clic en Apply (Aplicar).En este caso, todo el tráfico del cliente VPN se cifra y se envía al túnel IPsec. Esto se especifica bajo Parámetros del cliente
común.

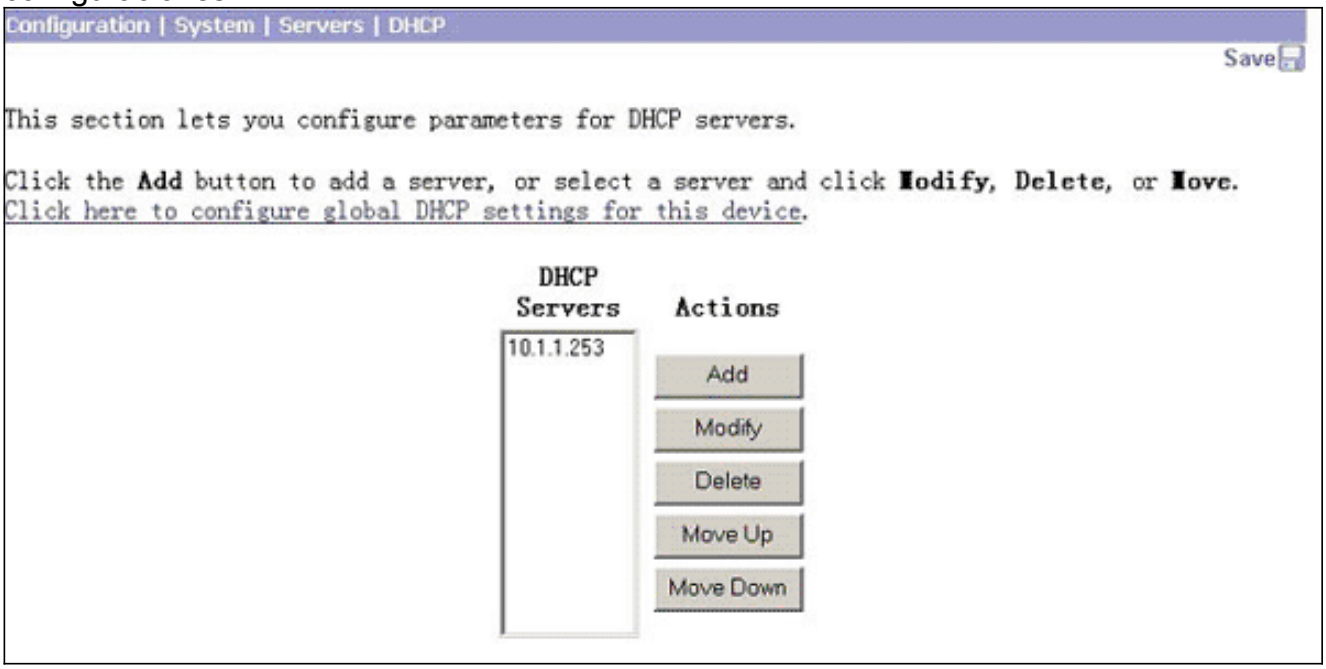


7. Elija el **Configuration (Configuración) > System (Sistema) > Address Management (Administración de direcciones) > Assigment (Asignación)**. De la ventana de opciones de la

asignación de dirección, especifique el método de asignación de la dirección IP con el checkboxes proporcionado.En este caso, el cliente VPN consigue una dirección IP de un servidor DHCP durante la negociación IKE, así que se marca la opción DHCP del uso. Haga clic en Apply
(Aplicar).



8. Utilice la ventana de la configuración del servidor DHCP para configurar los parámetros del servidor DHCP, y haga clic la **salvaguardia** para salvar las configuraciones.



Según lo mencionado, utilizan a un servidor DHCP detrás del concentrador VPN 3000 para las conexiones de red inalámbrica y las conexiones VPN. Para las conexiones de red inalámbrica, el concentrador sirve como agente de relé DHCP retransmitir el mensaje DHCP entre la Tecnología inalámbrica AP y el servidor DHCP.

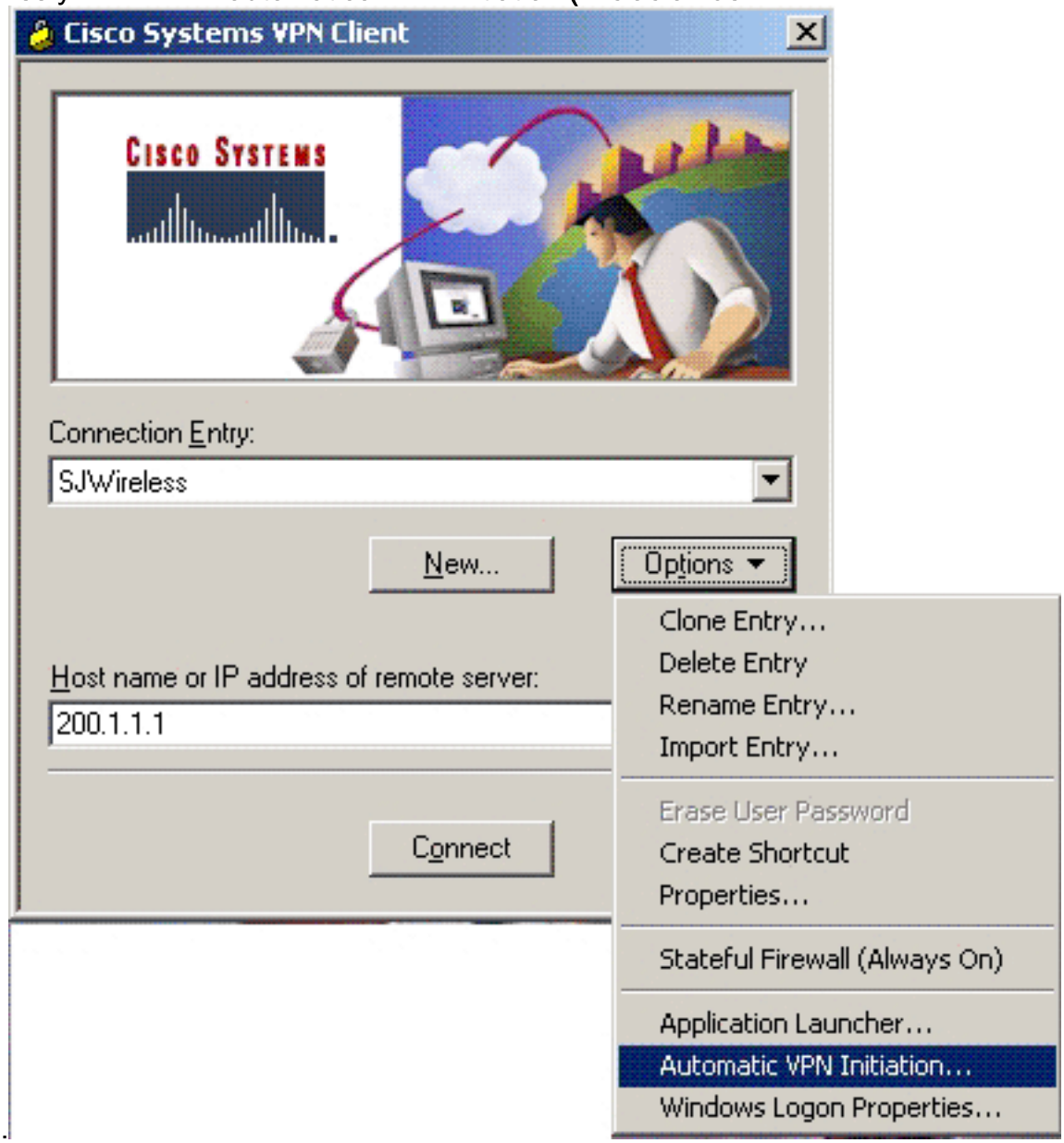
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

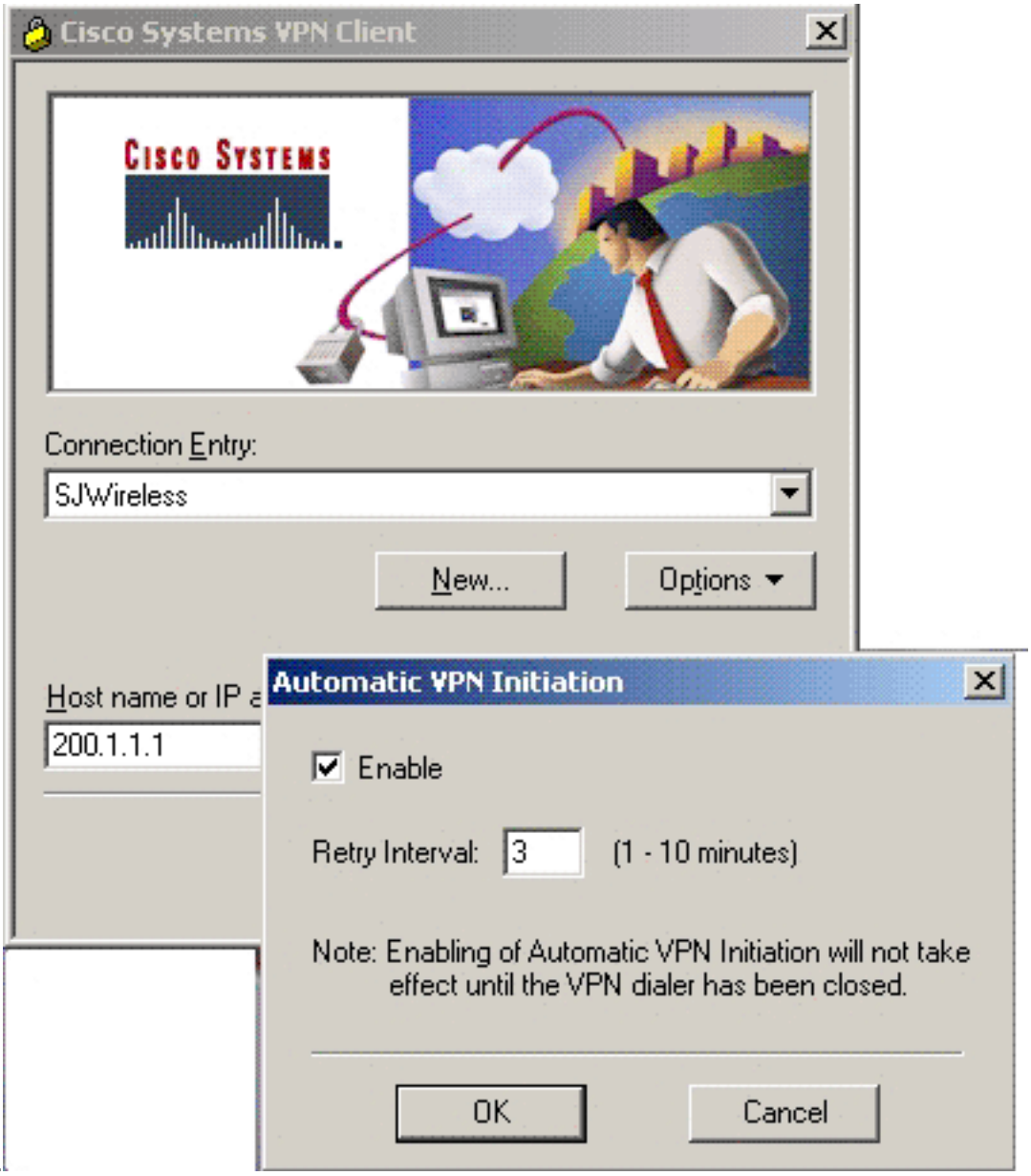
Verificar la configuración de iniciación automática desde el marcador VPN

Complete estos pasos para verificar la configuración de la iniciación automática del dialer VPN:

1. De la ventana dialer del Cisco VPN en el puesto de trabajo del cliente VPN, haga clic las **opciones** y seleccione **automático VPN Initiation (Iniciación de VPN)**.



2. En VPN Initiation (Iniciación de VPN) la ventana automática, verifique que la casilla de verificación del permiso esté marcada. Si no es, marquela. Haga Click en OK para cerrar la

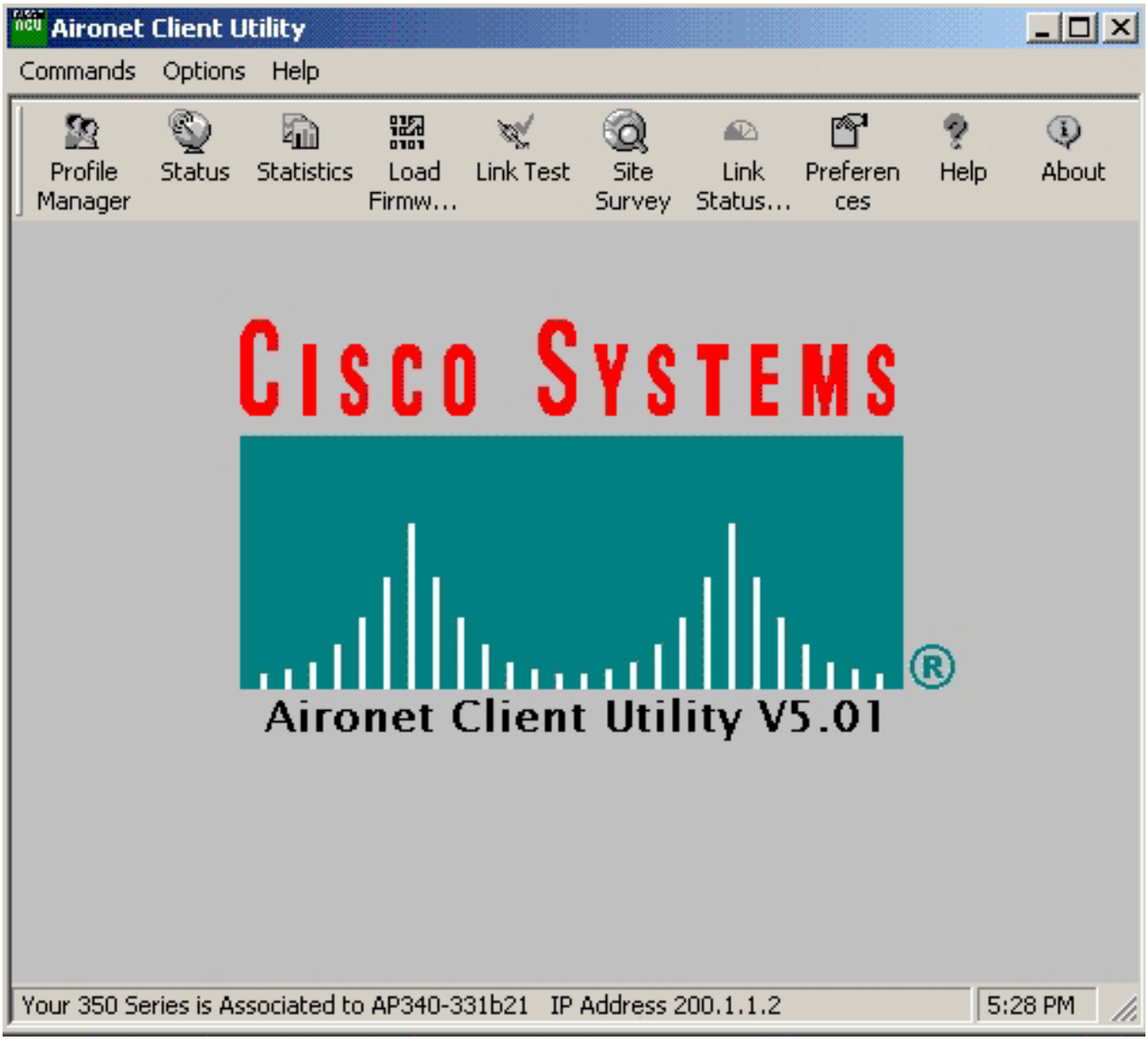


ventana.

Verifique la función Iniciación automática en el entorno WLAN

Complete estos pasos para verificar la característica del autoinitiation en el entorno WLAN:

1. Inserte el adaptador de red inalámbrica LAN en el PC, y espere la asociación a la Tecnología inalámbrica AP.Para verificar la asociación de red inalámbrica, comience el software del Aironet Client Utility y marque la parte inferior de la ventana del cliente Aironet. El cliente de red inalámbrica mostrado en la figura puede asociarse a la Tecnología inalámbrica AP cuya dirección IP es 200.1.1.2.



2. Una vez que la asociación de red inalámbrica es completa, el cliente VPN pone en marcha automáticamente una conexión basada en la dirección IP recibida de la conexión de red inalámbrica. En este caso, el cliente de red inalámbrica recibe 200.1.1.52 de la Tecnología inalámbrica AP, y el cliente VPN pone en marcha la conexión SJWireless basada en la configuración en el vpnclient.ini.Una vez que se establece la conexión VPN, el cliente puede acceder a los recursos de red bajo la protección de los servicios seguros del IPSec VPN,

como se muestra.

Verificación del registro de eventos del cliente VPN

Esta sección muestra cómo marcar la orden del login del evento del cliente VPN para verificar que procede el autoinitiation correctamente.

Abra el Visualizador del registro del Cliente Cisco VPN y usted ve la información similar a esto durante el autoinitiation. Como usted puede ver, el cliente VPN recibe a la dirección IP 200.1.1.52 de la asociación de red inalámbrica, que cae en la lista de red 200.1.1.0/24 definida en el vpnclient.ini. El cliente VPN entonces enciende la conexión SJWireless por consiguiente. Durante la negociación IKE, el Cliente Cisco VPN recibe una dirección IP de 50.1.1.8. Utiliza esta dirección IP como el IP de la fuente para acceder la red interna detrás del Cisco VPN 3000 Concentrator.

```
222 17:26:05.019 11/19/02 Sev=Info/6 CM/0x63100036 autoinitiation condition detected: Local IP
200.1.1.52 Network 200.1.1.0 Mask 255.255.255.0 Connection Entry "SJWireless" 223 17:26:06.071
11/19/02 Sev=Info/6 DIALER/0x63300002 Initiating connection. 224 17:26:06.081 11/19/02
Sev=Info/4 CM/0x63100002 Begin connection process 225 17:26:06.091 11/19/02 Sev=Info/4
CM/0x63100004 Establish secure connection using Ethernet 226 17:26:06.091 11/19/02 Sev=Info/4
CM/0x63100026 Attempt connection with server "200.1.1.1" 227 17:26:06.091 11/19/02 Sev=Info/6
IKE/0x6300003B Attempting to establish a connection with 200.1.1.1. 228 17:26:06.131 11/19/02
Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK AG (SA, KE, NON, ID, VID, VID, VID) to
200.1.1.1 229 17:26:06.131 11/19/02 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 230
17:26:06.281 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 231
17:26:06.281 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK AG (SA, KE, NON, ID,
HASH, VID, VID, VID, VID, VID) from 200.1.1.1 232 17:26:06.281 11/19/02 Sev=Info/5
IKE/0x63000059 Vendor ID payload = 12F5F28C457168A9702D9FE274CC0100 233 17:26:06.281 11/19/02
Sev=Info/5 IKE/0x63000001 Peer is a Cisco-Unity compliant peer 234 17:26:06.281 11/19/02
Sev=Info/5 IKE/0x63000059 Vendor ID payload = 09002689DFD6B712 235 17:26:06.281 11/19/02
Sev=Info/5 IKE/0x63000001 Peer supports XAUTH 236 17:26:06.281 11/19/02 Sev=Info/5
IKE/0x63000059 Vendor ID payload = AFCAD71368A1F1C96B8696FC77570100 237 17:26:06.281 11/19/02
Sev=Info/5 IKE/0x63000001 Peer supports DPD 238 17:26:06.281 11/19/02 Sev=Info/5 IKE/0x63000059
Vendor ID payload = 4048B7D56EBCE88525E7DE7F00D6C2D3C0000000 239 17:26:06.281 11/19/02
Sev=Info/5 IKE/0x63000059 Vendor ID payload = 1F07F70EAA6514D3B0FA96542A500306 240 17:26:06.301
11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK AG *(HASH,
NOTIFY:STATUS_INITIAL_CONTACT) to 200.1.1.1 241 17:26:06.311 11/19/02 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 200.1.1.1 242 17:26:06.311 11/19/02 Sev=Warning/2 IKE/0xA3000062
Attempted incoming connection from 200.1.1.1. Inbound connections are not allowed. 243
```

17:26:06.311 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 244 17:26:06.311 11/19/02 Sev=Warning/2 IKE/0xA3000062 Attempted incoming connection from 200.1.1.1. Inbound connections are not allowed. 245 17:26:06.321 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 246 17:26:06.321 11/19/02 Sev=Warning/2 IKE/0xA3000062 Attempted incoming connection from 200.1.1.1. Inbound connections are not allowed. 247 17:26:06.321 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 248 17:26:06.321 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 200.1.1.1 249 17:26:06.321 11/19/02 Sev=Info/4 CM/0x63100015 Launch xAuth application 250 17:26:10.397 11/19/02 Sev=Info/4 CM/0x63100017 xAuth application returned 251 17:26:10.397 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 200.1.1.1 252 17:26:10.697 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 253 17:26:10.697 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 200.1.1.1 254 17:26:10.697 11/19/02 Sev=Info/4 CM/0x6310000E Established Phase 1 SA. 1 Phase 1 SA in the system 255 17:26:10.707 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 200.1.1.1 256 17:26:11.779 11/19/02 Sev=Info/5 IKE/0x6300005D Client sending a firewall request to concentrator 257 17:26:11.779 11/19/02 Sev=Info/5 IKE/0x6300005C Firewall Policy: Product=Cisco Integrated Client, Capability= (Centralized Protection Policy). 258 17:26:11.779 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK TRANS *(HASH, ATTR) to 200.1.1.1 259 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 260 17:26:11.809 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK TRANS *(HASH, ATTR) from 200.1.1.1 **261 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_ADDRESS: , value = 50.1.1.8 262 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_DNS(1): , value = 10.1.1.100 263 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x63000010 MODE_CFG_REPLY: Attribute = INTERNAL_IPV4_NBNS(1) (a.k.a. WINS) : , value = 10.1.1.101** 264 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_SAVEPWD: , value = 0x00000000 265 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300000D MODE_CFG_REPLY: Attribute = MODECFG_UNITY_PFS: , value = 0x00000000 266 17:26:11.809 11/19/02 Sev=Info/5 IKE/0x6300000E MODE_CFG_REPLY: Attribute = APPLICATION_VERSION, value = Cisco Systems, Inc./ VPN 3000 Concentrator Version 3.6.Rel built by vmurphy on Aug 06 2002 10:41:35 267 17:26:11.819 11/19/02 Sev=Info/4 CM/0x63100019 Mode Config data received 268 17:26:11.839 11/19/02 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP address 200.1.1.1, GW IP = 200.1.1.1 269 17:26:11.839 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 200.1.1.1 270 17:26:11.849 11/19/02 Sev=Info/5 IKE/0x63000055 Received a key request from Driver for IP address 10.10.10.255, GW IP = 200.1.1.1 271 17:26:11.849 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH, SA, NON, ID, ID) to 200.1.1.1 272 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 273 17:26:11.859 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK INFO *(HASH, NOTIFY:STATUS_RESP_LIFETIME) from 200.1.1.1 274 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 86400 seconds 275 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000046 This SA has already been alive for 5 seconds, setting expiry to 86395 seconds from now 276 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 277 17:26:11.859 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 200.1.1.1 278 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800 seconds 279 17:26:11.859 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to 200.1.1.1 280 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000058 Loading IPSec SA (Message ID = 0xF9D733A7 OUTBOUND SPI = 0x1AD0BBA1 INBOUND SPI = 0xA99C00B3) 281 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000025 Loaded OUTBOUND ESP SPI: 0x1AD0BBA1 282 17:26:11.859 11/19/02 Sev=Info/5 IKE/0x63000026 Loaded INBOUND ESP SPI: 0xA99C00B3 283 17:26:11.859 11/19/02 Sev=Info/4 CM/0x6310001A One secure connection established 284 17:26:11.879 11/19/02 Sev=Info/6 DIALER/0x63300003 Connection established. 285 17:26:11.889 11/19/02 Sev=Info/6 DIALER/0x63300008 MAPI32 Information - Outlook not default mail client 286 17:26:11.929 11/19/02 Sev=Info/5 IKE/0x6300002F Received ISAKMP packet: peer = 200.1.1.1 287 17:26:11.929 11/19/02 Sev=Info/4 IKE/0x63000014 RECEIVING <<< ISAKMP OAK QM *(HASH, SA, NON, ID, ID, NOTIFY:STATUS_RESP_LIFETIME) from 200.1.1.1 288 17:26:11.929 11/19/02 Sev=Info/5 IKE/0x63000044 RESPONDER-LIFETIME notify has value of 28800 seconds 289 17:26:11.929 11/19/02 Sev=Info/4 IKE/0x63000013 SENDING >>> ISAKMP OAK QM *(HASH) to 200.1.1.1 290 17:26:11.939 11/19/02 Sev=Info/5 IKE/0x63000058 Loading IPSec SA (Message ID = 0x0660AF57 OUTBOUND SPI = 0x5E6E8676 INBOUND SPI = 0xF5EAA827) 291 17:26:11.939 11/19/02 Sev=Info/5 IKE/0x63000025 Loaded OUTBOUND ESP SPI: 0x5E6E8676 292 17:26:11.939 11/19/02 Sev=Info/5 IKE/0x63000026 Loaded INBOUND ESP SPI: 0xF5EAA827 293 17:26:11.939 11/19/02 Sev=Info/4 CM/0x63100022 Additional Phase 2 SA established. 294 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700014 Deleted all keys 295 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new key structure 296 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with SPI=0xa1bbd01a into key list 297 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new

```
key structure 298 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with
SPI=0xb3009ca9 into key list 299 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new
key structure 300 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with
SPI=0x76866e5e into key list 301 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x63700010 Created a new
key structure 302 17:26:12.891 11/19/02 Sev=Info/4 IPSEC/0x6370000F Added key with
SPI=0x27a8eaf5 into key list 303 17:26:21.904 11/19/02 Sev=Info/6 IKE/0x6300003D Sending DPD
request to 200.1.1.1, seq# = 2877451244 304 17:26:21.904 11/19/02 Sev=Info/4 IKE/0x63000013
SENDING >>> ISAKMP OAK INFO *(HASH, NOTIFY:DPD_REQUEST) to 200.1.1.1
```

Verifique un estado de inicialización automática diferente

Refiérase usando VPN Initiation (Iniciación de VPN) la información delantera automática sobre otros estados del autoinitiation.

Información Relacionada

- Volumen de referencia I del concentrador VPN de la serie 3000: Configuración
- Página de soporte del concentrador de la serie Cisco VPN 3000
- Página de soporte al cliente Serie Cisco VPN 3000
- Página de soporte de IPSec
- Soporte Técnico y Documentación - Cisco Systems