# Configurando o início automático de VPN em um cliente VPN Cisco em um ambiente de LAN sem fio

## Índice



## Introdução

Este documento descreve como configurar o Cisco VPN Client para iniciar automaticamente conexões do IPSec VPN aos concentradores do Cisco VPN 3000 no ambiente prendidos/Wireless LAN (WLAN).

No ambiente de WLAN, o cliente Wireless associa-se primeiramente a um ponto de acesso Wireless (AP). Baseado no intervalo de endereço IP que recebe da conexão Wireless, o cliente VPN instalado no Sem fio lança automaticamente um pedido de conexão de VPN ao concentrador VPN correspondente no local. A conexão do IPSec VPN é usada então a fim fixar o tráfego do Sem fio 802.11x. Sem o estabelecimento bem-sucedido da conexão de VPN de Cisco, os clientes Wireless não têm nenhum acesso aos recursos de rede.

Esta configuração de exemplo mostra a configuração do cliente VPN a fim permitir a característica da inicialização automática.

## Pré-requisitos

### Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

## Requisitos

Antes que você tente esta configuração, assegure-se de que você esteja familiar com estes conceitos:

- Compreenda como estabelecer e configurar o Cisco VPN Client e o Cisco VPN 3000 Concentrator a fim estabelecer um túnel do IPSec VPN
- Compreenda as configurações relativas ao Sem fio LAN

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão Cliente VPN Cisco 4.x
- Versão 3.6 do Cisco VPN 3000 Concentrator
- Access point do Cisco Aironet série 340
- Adaptador de Wireless LAN do Cisco Aironet série 350 (versão 5.0.1)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

**Nota:** Neste exemplo, o Cisco Network Registrar é usado como um server do protocolo de configuração dinâmica host (DHCP) a fim fornecer endereços IP de Um ou Mais Servidores Cisco ICM NT aos clientes Wireless e aos clientes VPN.

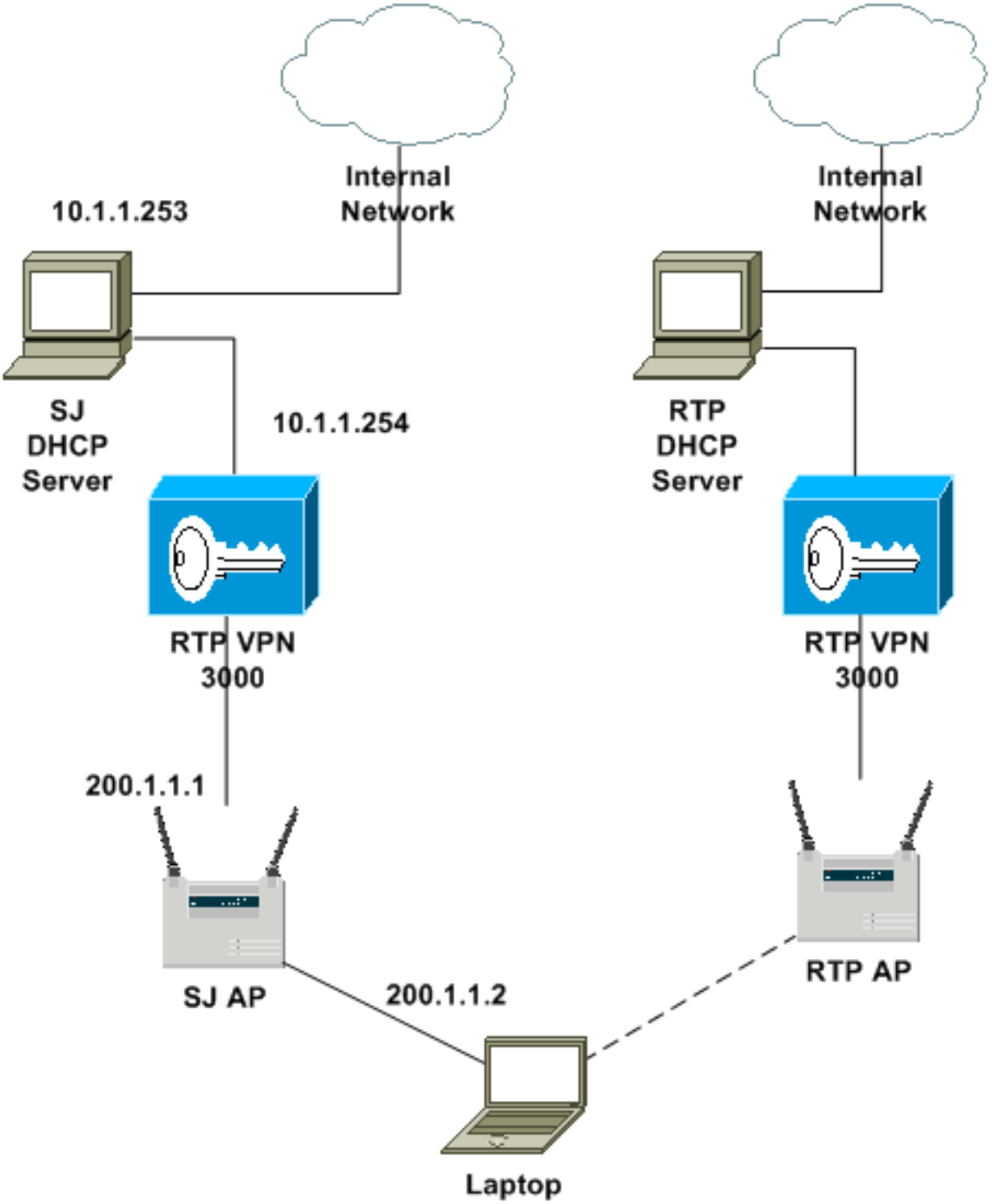
# Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Use a Command Lookup Tool ( somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:




**Nota:** Nesta instalação, o servidor DHCP SJ é usado a fim fornecer endereços IP de Um ou Mais Servidores Cisco ICM NT às conexões Wireless e às conexões de VPN. Tem dois intervalos de endereço IP definidos:

- Para conexões Wireless, os usuários Wireless recebem um endereço IP de Um ou Mais Servidores Cisco ICM NT na escala de 200.1.1.50 a 200.1.1.250.
- Para conexões de VPN, os clientes VPN recebem um endereço IP de Um ou Mais Servidores Cisco ICM NT na escala de 50.1.1.1 a 50.1.1.254.

## Configurações

Neste exemplo, com base no que no local o usuário vagueia, o cliente Wireless lança automaticamente qualquer um uma das duas conexões de VPN (a saber SJWireless ou

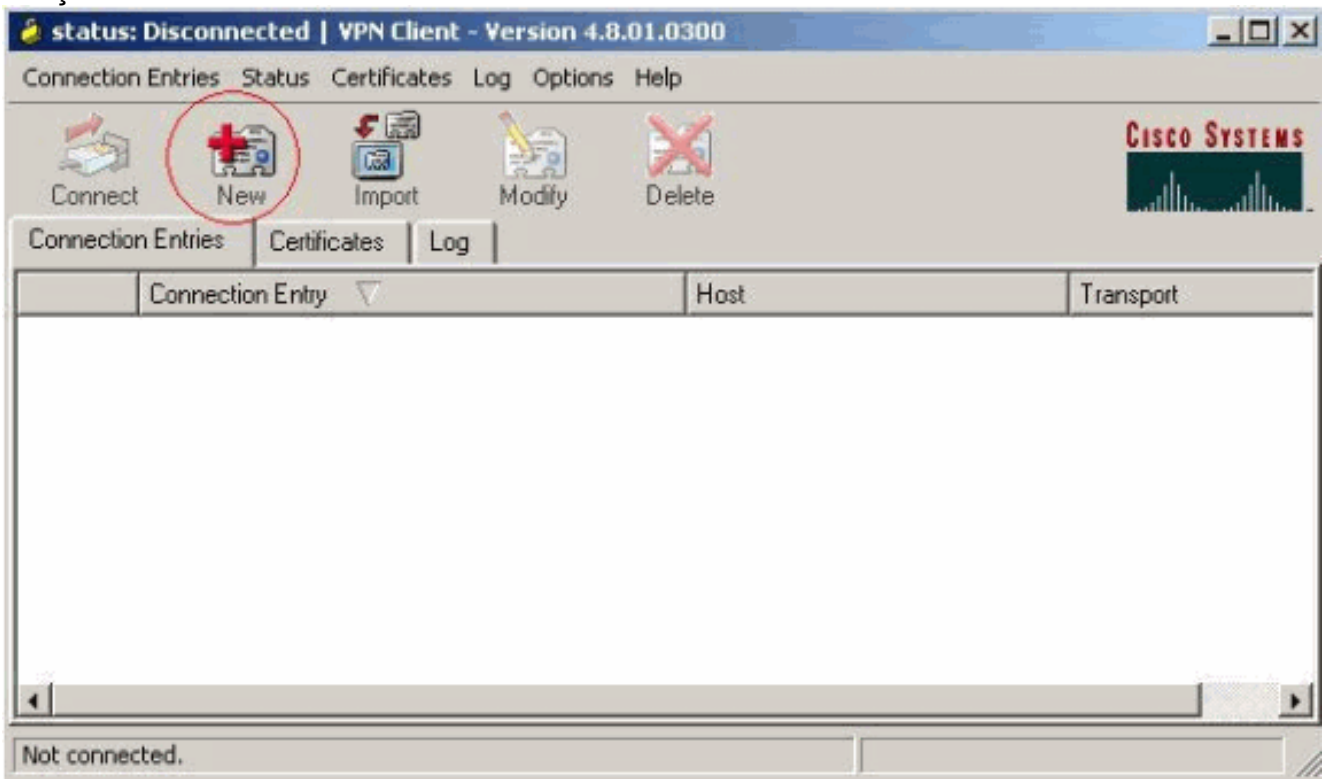
RTPWireless) que são predefinidas no discador de VPN. Mais especificamente, se o usuário Wireless obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT na escala de 200.1.1.0/24 do wireless association ao SJ AP, lança a conexão de SJWireless do discador de VPN. Se obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT na escala de 150.1.1.0/24 do wireless association ao RTP AP, lança a conexão RTP Wireless do discador de VPN.

Nesta seção, as conexões de VPN são configuradas primeiramente sob o discador de VPN, a seguir o arquivo vpnclient.ini é editado para adicionar a configuração de autoiniciação. Uma vez que estas etapas são terminadas em um cliente VPN, os perfis gerados VPN (arquivos do .pcf) e vpnclient.ini configurado podem ser empacotados, junto com a imagem do cliente VPN, a fim distribuir aos utilizadores finais. O lançamento da conexão de VPN é transparente aos utilizadores finais após a instalação do cliente VPN.

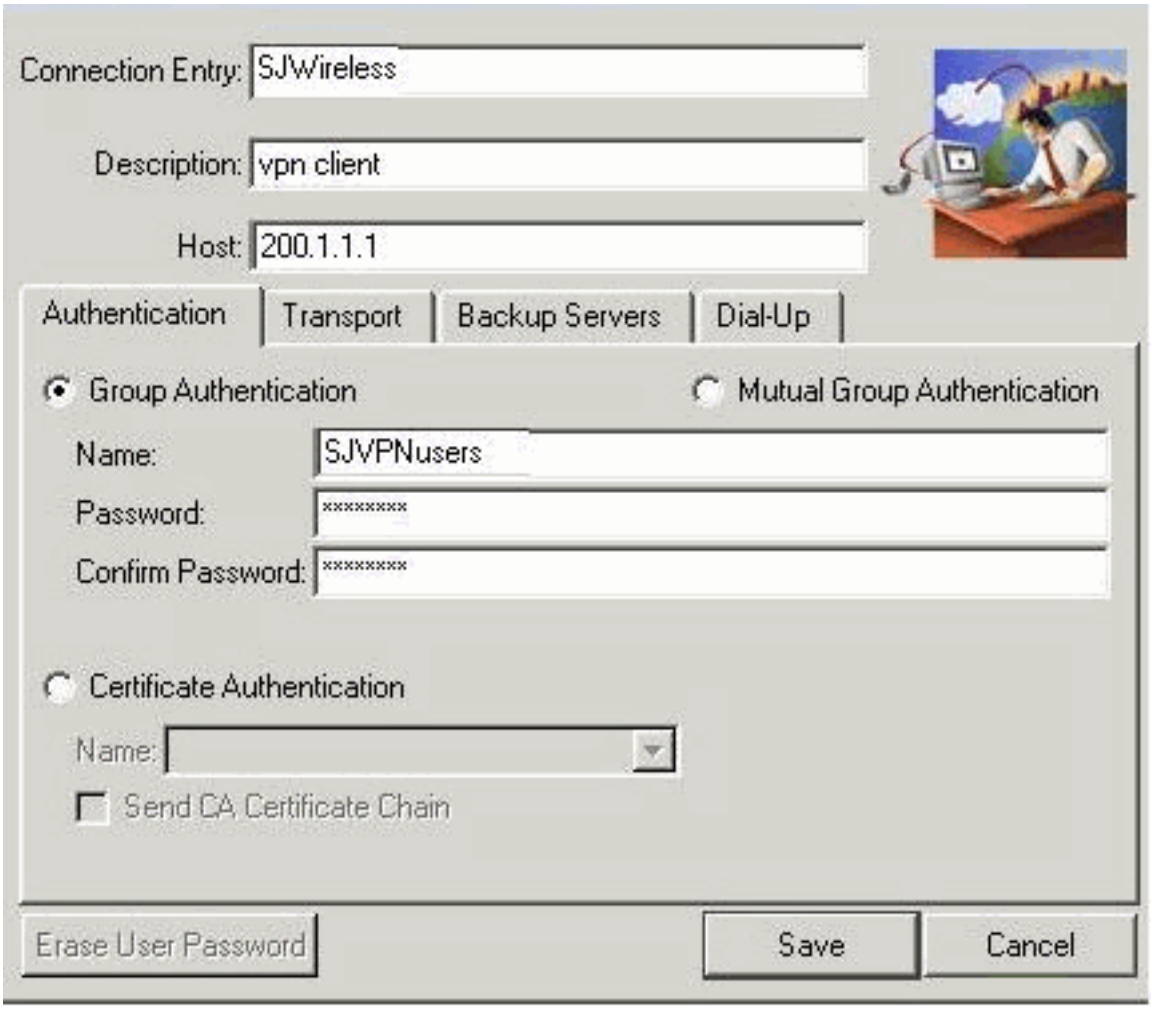
## Configuração de Discador VPN

Termine estas etapas de configuração:

1. Escolha o Iniciar > Programas > Cliente de VPN de Sistemas Cisco > o cliente VPN. Clique **novo** a fim lançar a janela de entrada nova da conexão de VPN da criação.




2. Dê entrada com o nome da entrada de conexão junto com uma descrição. Incorpore o endereço IP externo do concentrador VPN à caixa do host. Incorpore então o nome do grupo VPN e a senha, e clique a **salvaguarda**.



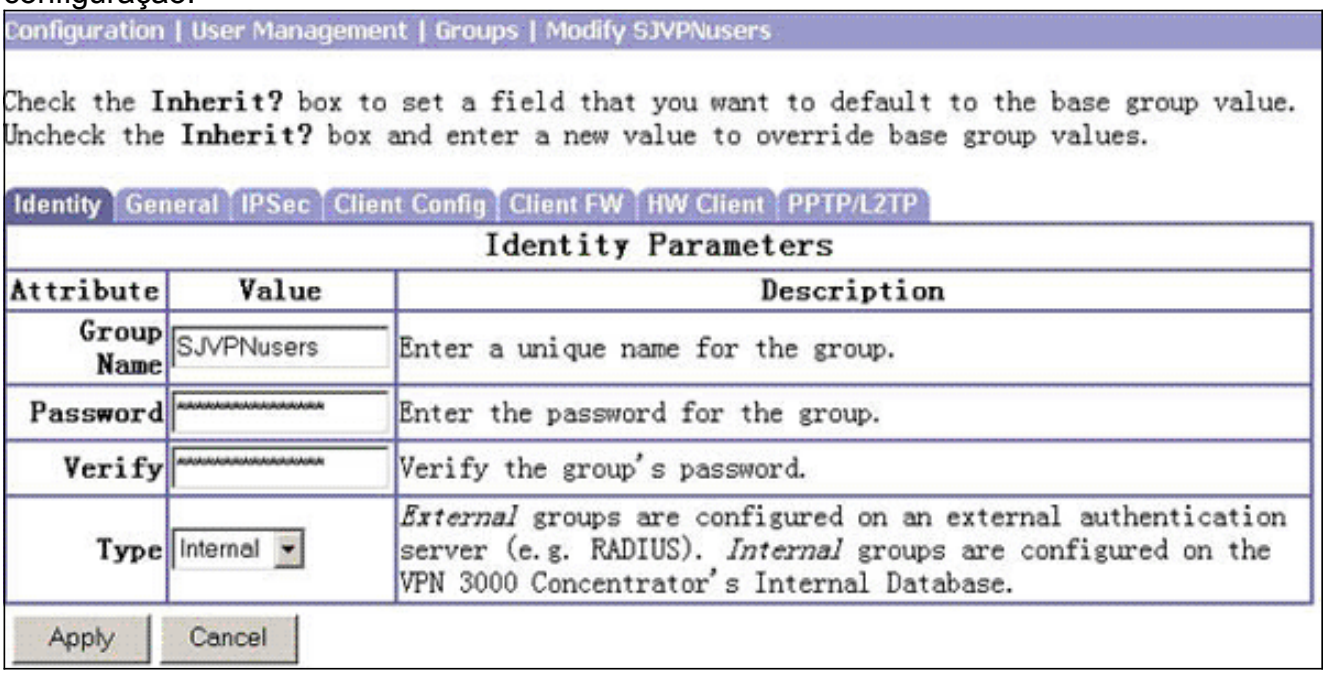

3. Repita etapas 1 e 2 a fim criar uma outra conexão de VPN com o nome **RTPWireless do** discador de VPN de Cisco.Quando o segundo processo de configuração está completo, dois perfis da conexão de VPN nomearam SJWireless.pcf e RTPWireless.pcf estão gerados no PC cliente.
4. Termine estas etapas a fim editar o arquivo do padrão vpnclient.ini encontrado no PC cliente a fim permitir a característica da inicialização automática:Permita a característica da inicialização automática com as **palavras-chave "AutoInitiationEnable" Habilitação de Iniciação Automática** sob a seção do [main].Defina o **AutoInitiationList**. Cada artigo na lista corresponde a uma seção, onde o nome do intervalo de endereço IP da conexão de VPN e do Sem fio seja associado.Neste exemplo, a conexão de VPN Sem fio de SJ corresponde a 200.1.1.0/24 e a conexão RTP Wireless corresponde a 150.1.1.0/24.Quando pisam a e b estão completos, o arquivo vpnclient.ini olha como este:`[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. Depois que etapas 1 - 3 estão completas em um cliente VPN, o vpnclient.ini e os perfis da conexão de VPN (.pcf) podem ser recolhidos e distribuído aos utilizadores finais no pacote da instalação. Refira o guia do administrador VPNCLIENT, libere 3.6 para obter informações sobre de como preconfigure os clientes VPN para usuários remotos.

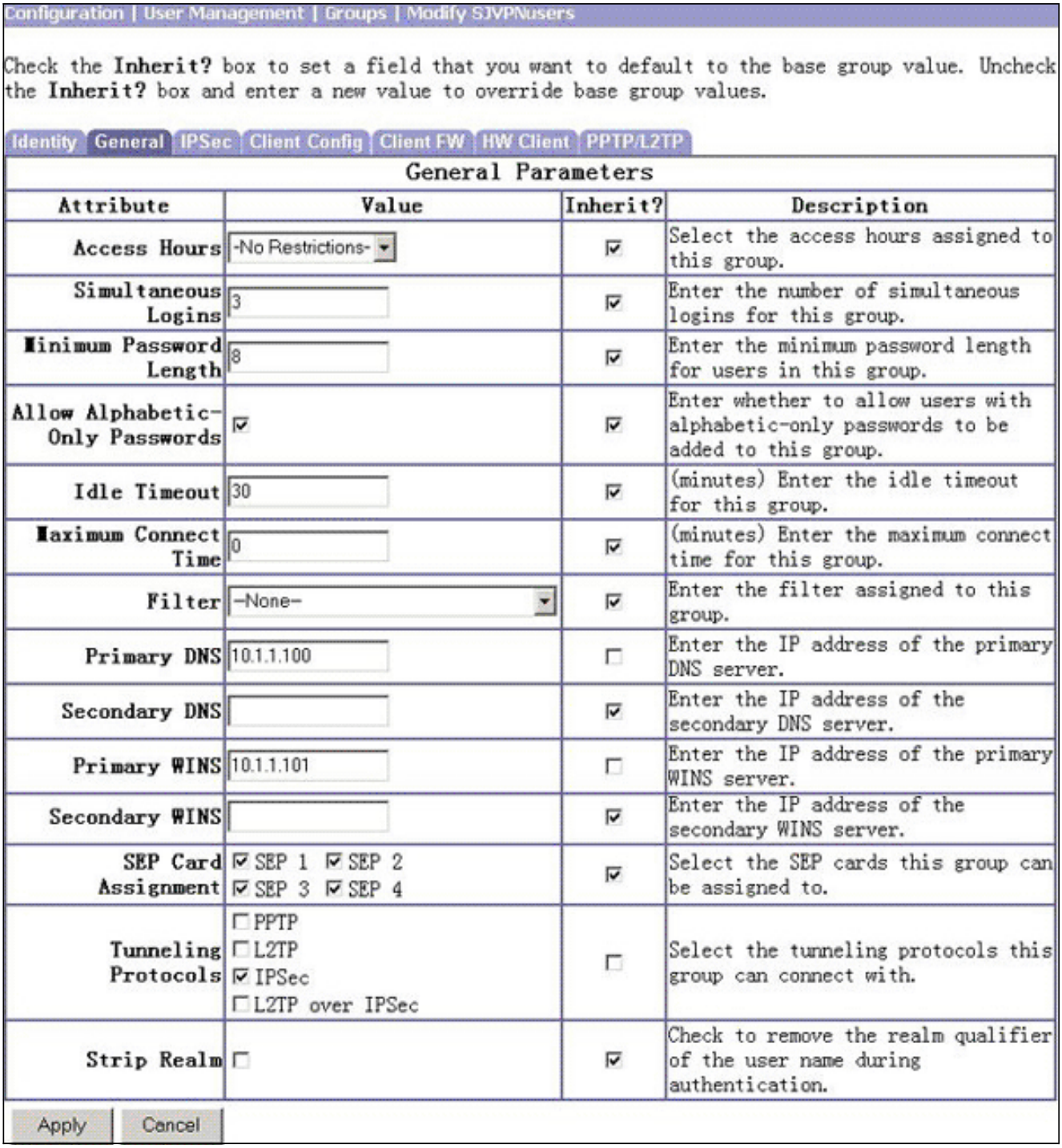
### Configuração do Cisco VPN 3000 Concentrator

Termine estas etapas de configuração:

1. Em VPN 3000 concentratores, os grupos de VPN precisam de ser configurados para estabelecer uma conexão IPSec com o cliente VPN. No exemplo, os usuários Wireless podem conectar aos concentradores VPN diferentes baseados no local em que vagueiam. Aqui, somente as tarefas de configuração importantes no concentrador VPN SJ são destacadas. Um grupo de VPN chamou **SJVPNusers**, que combinam o nome do grupo VPN no cliente, é criado.
2. Escolha o **configuration > user management > os grupos** e escolha **SJVPNusers da** lista de grupo atual. Seleto **altere o grupo da** opção de ações se o grupo é criado já, ou **adicionar o grupo** e **altere** então o **grupo** se o grupo deve ser criado.
3. Clique a aba da identidade.A janela Parâmetros de identidade aparece. Verifique que a informação indicada neste indicador está correta para sua configuração.




4. Clique o tab geral e verifique então a caixa do **IPsec** para ver se há o atributo dos protocolos de tunelamento.



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.

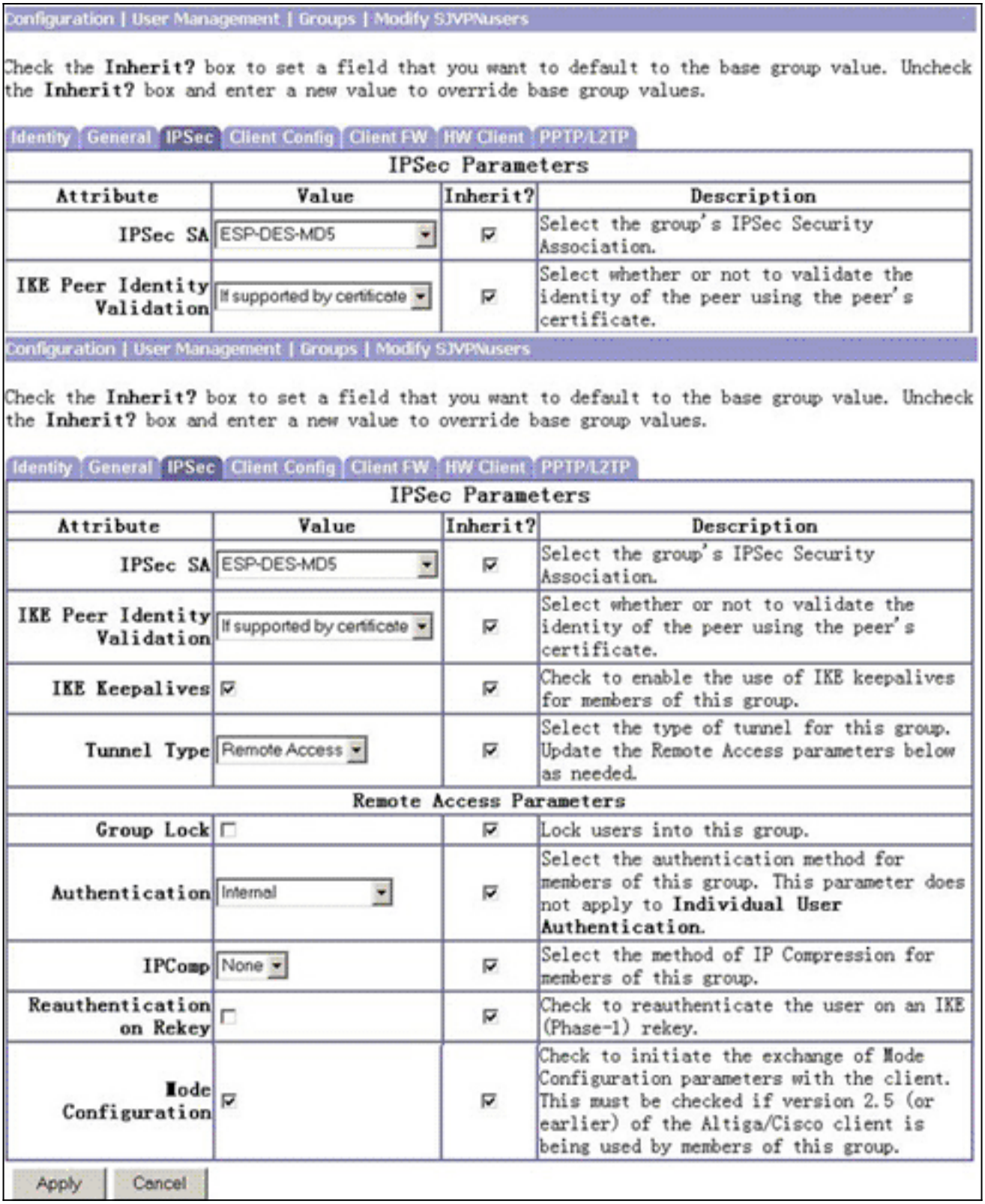
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

**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. Clique a aba do IPsec, a seguir especifique a associação de segurança IPSec (SA) e o atributo do método de autenticação com os menus suspensos e as caixas de seleção fornecidos.Neste caso, os usuários VPN são definidos localmente no VPN 3000 concentrator, assim que o método de autenticação é 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.

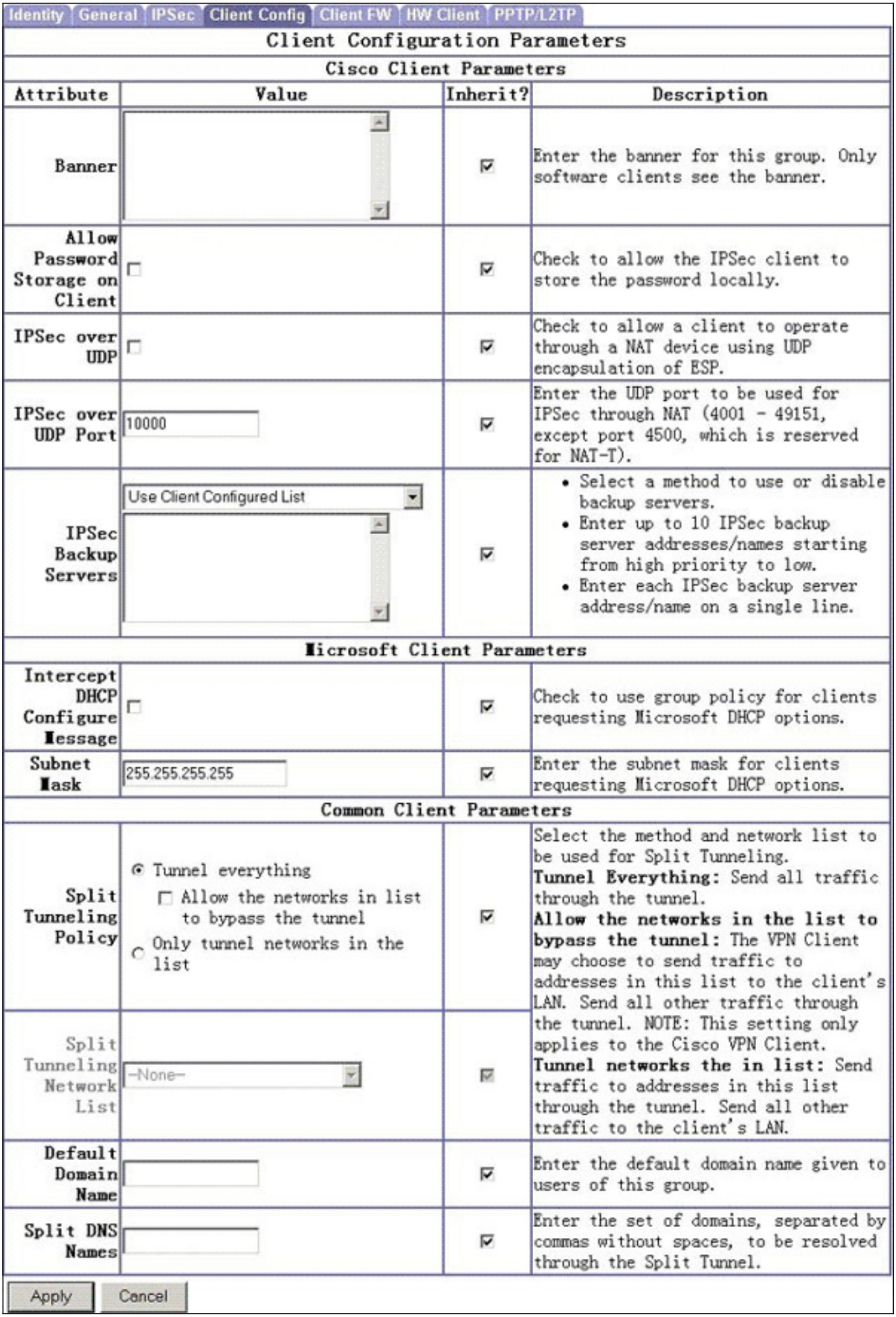
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

**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. |

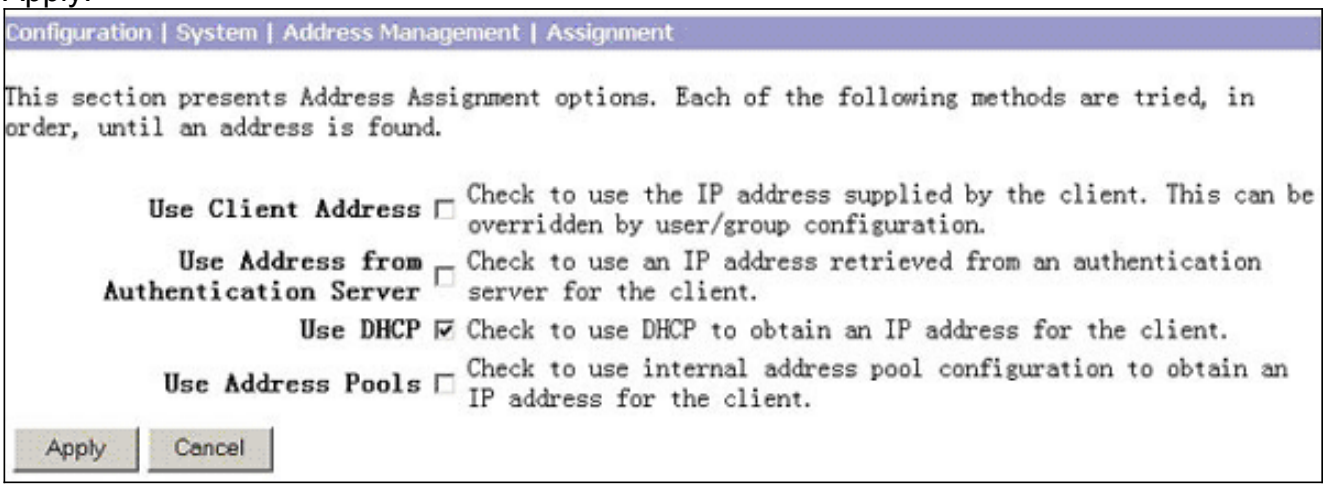
Apply | Cancel

6. Clique o guia de configuração do cliente, a seguir especifique os parâmetros da configuração de modo na janela Parâmetros da configuração de cliente. Clique em Apply.Neste caso, todo o tráfego do cliente VPN é cifrado e enviado ao túnel de IPsec. Isto é especificado sob os parâmetros de cliente
comum.

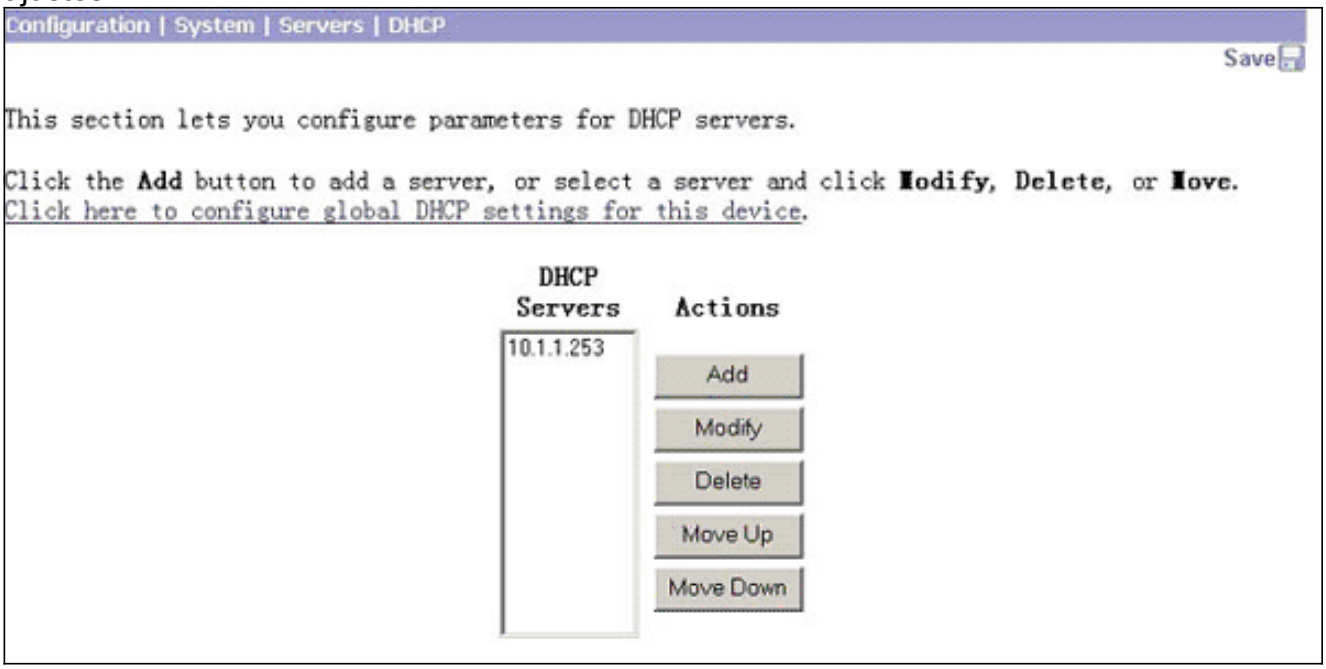



7. Escolha o **configuração > sistema > gerenciamento de endereço > atribuição**. Da janela de opções da atribuição de endereço, especifique o método de atribuição do endereço IP de

Um ou Mais Servidores Cisco ICM NT com as caixas de seleção fornecidas.Neste caso, o cliente VPN obtém um endereço IP de Um ou Mais Servidores Cisco ICM NT de um servidor DHCP durante a negociação de IKE, assim que a opção de DHCP do uso é verificada.
Clique em
Apply.




8. Use o indicador da configuração do servidor de DHCP a fim estabelecer os parâmetros do servidor DHCP, e clique a **salvaguarda** a fim salvar os
ajustes.




Como mencionado, um servidor DHCP atrás do VPN 3000 concentrator é usado para conexões Wireless e conexões de VPN. Para conexões Wireless, o concentrador serve como um agente de transmissão de DHCP para retransmitir o mensagem DHCP entre o Sem fio AP e o servidor DHCP.

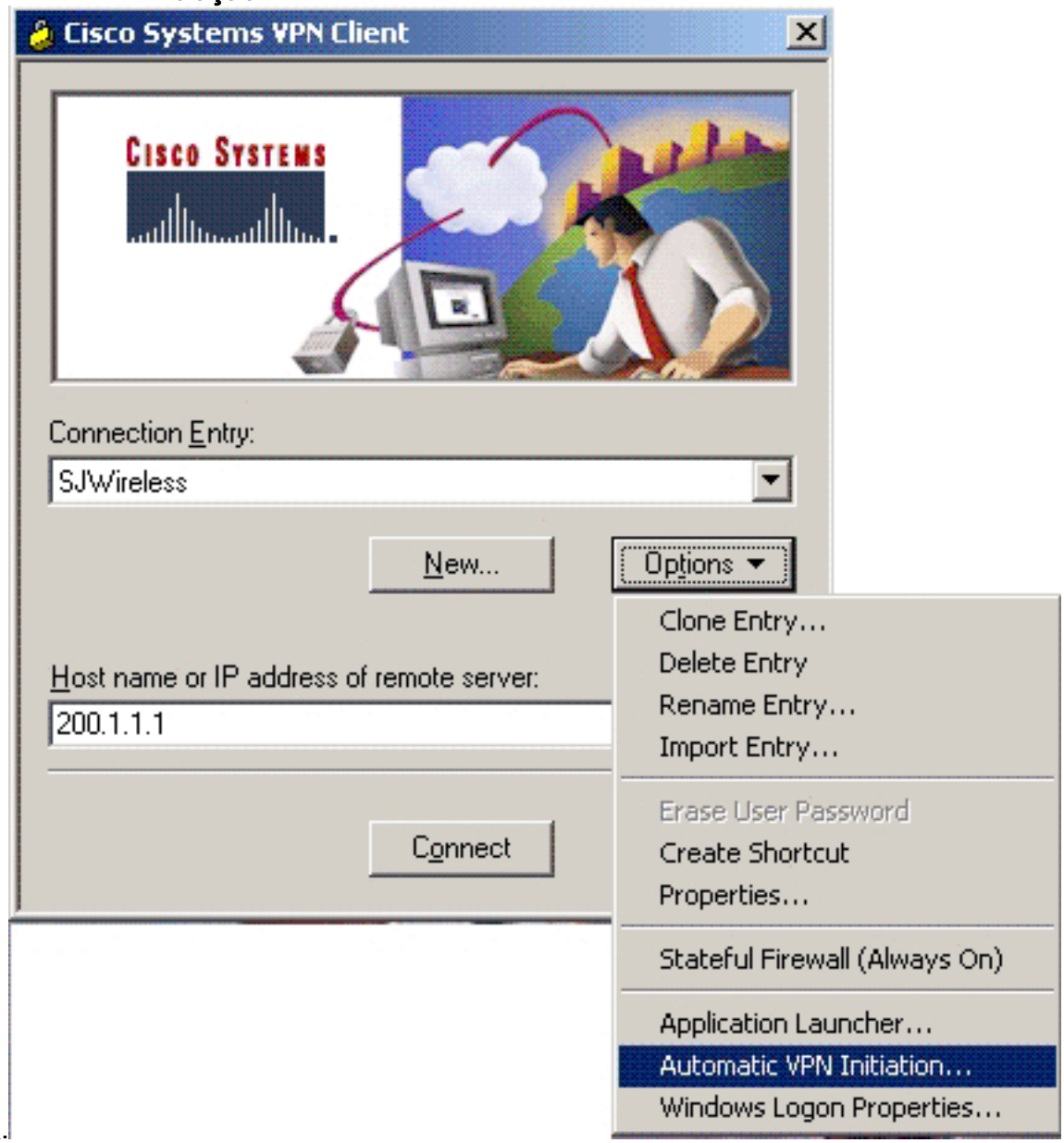
# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

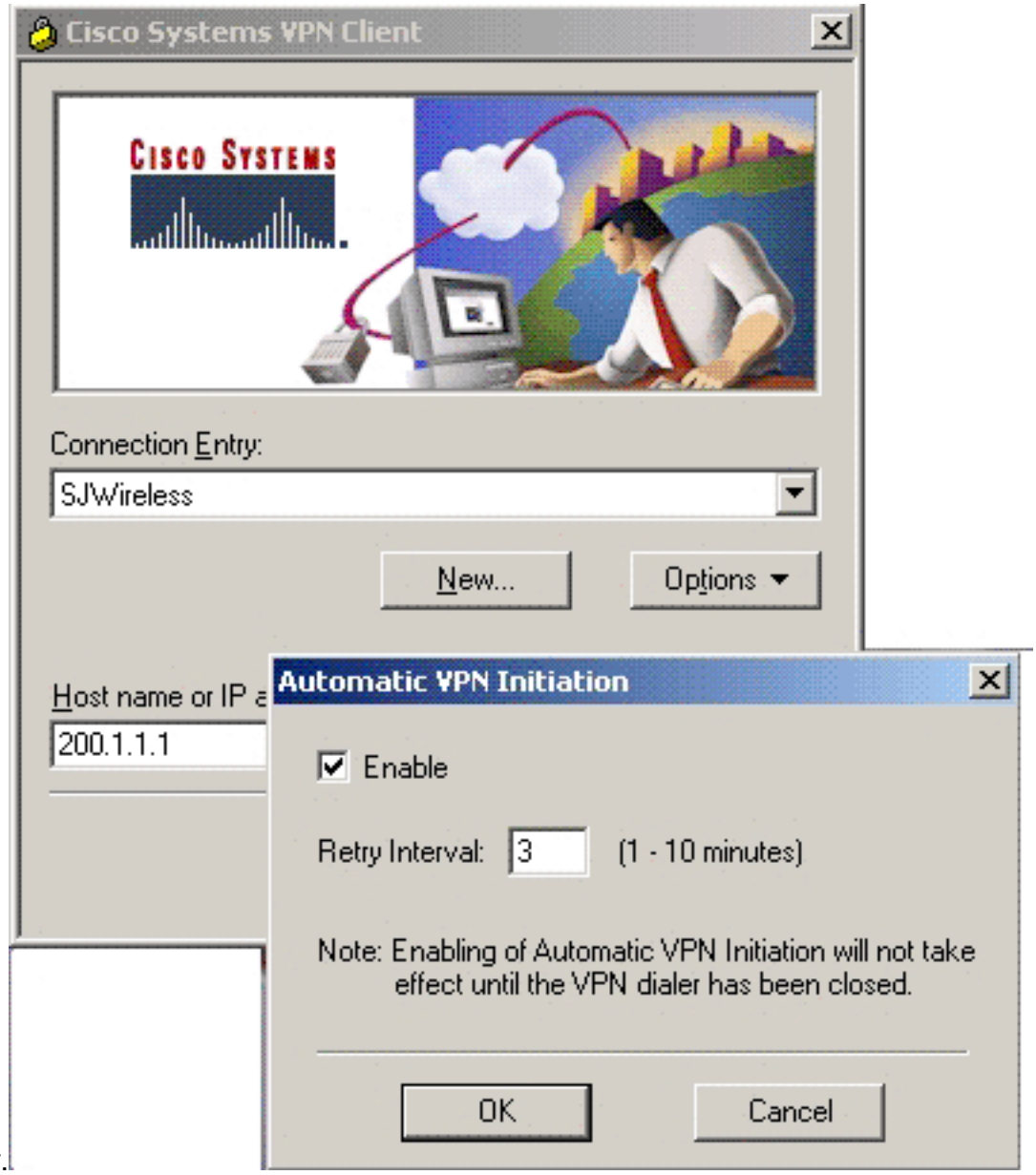
## Verifique a configuração de iniciação automática do discador VPN

Termine estas etapas a fim verificar a configuração de autoiniciação do discador de VPN:

1. Do indicador do discador de VPN de Cisco na estação de trabalho do cliente VPN, clique **opções** e selecione a **iniciação VPN automática**.




2. No indicador automático da iniciação VPN, verifique que a caixa de verificação da possibilidade está verificada. Se não é, verifique-a. Clique a **APROVAÇÃO** a fim fechar o

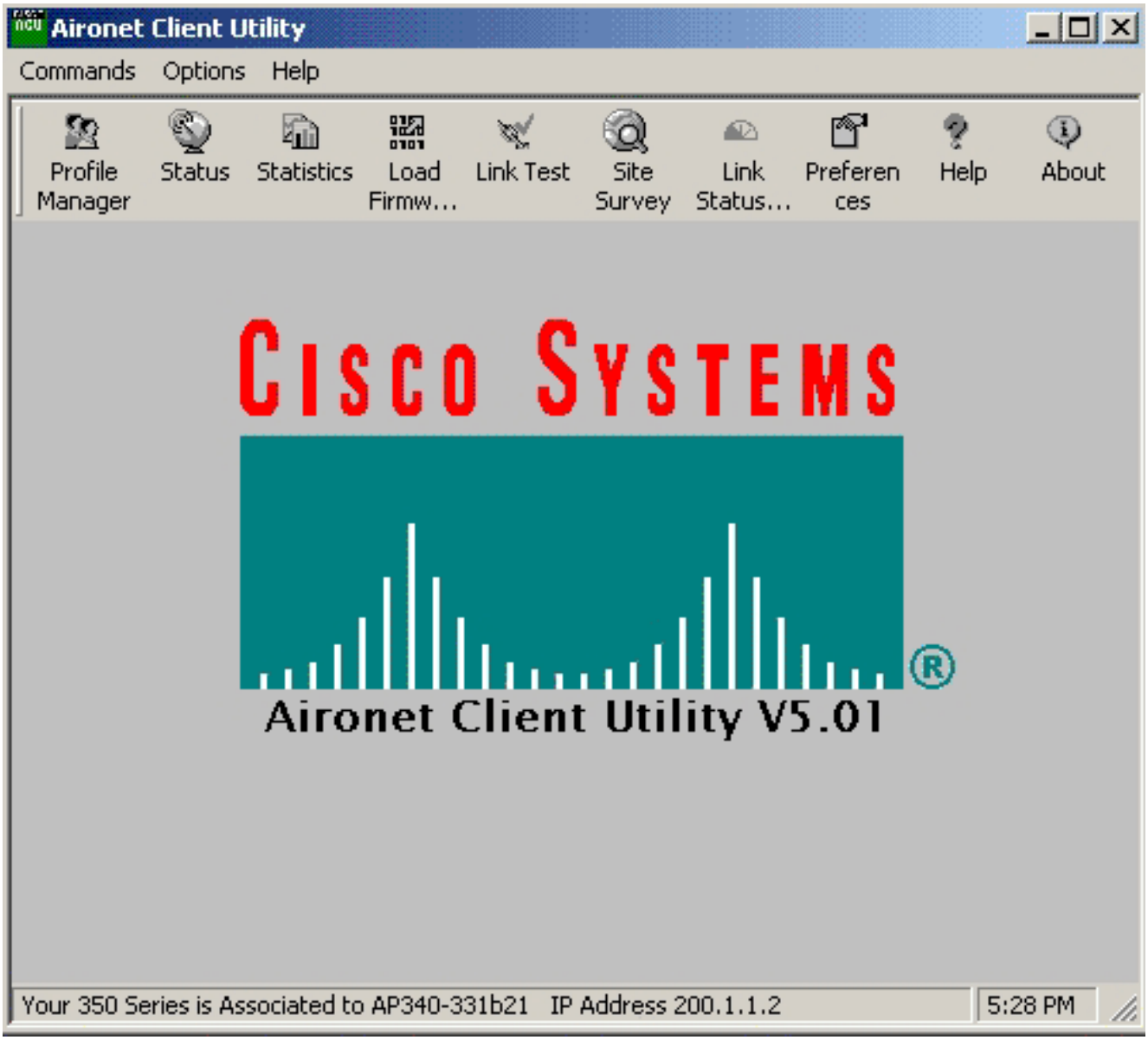



indicador.

## Verifique o recurso Iniciação automática no ambiente WLAN

Termine estas etapas a fim verificar a característica da inicialização automática no ambiente de WLAN:

1. Introduza o adaptador de Wireless LAN no PC, e espere a associação ao Sem fio AP.A fim verificar o wireless association, comece o software do Aironet Client Utility e verifique a parte inferior do indicador do cliente Aironet. O cliente Wireless mostrado na figura pode associar ao Sem fio AP cujo o endereço IP de Um ou Mais Servidores Cisco ICM NT é 200.1.1.2.




2. Uma vez que o wireless association está completo, o cliente VPN lança automaticamente uma conexão baseada no endereço IP de Um ou Mais Servidores Cisco ICM NT recebido da conexão Wireless. Neste caso, o cliente Wireless recebe 200.1.1.52 do Sem fio AP, e o cliente VPN lança a conexão de SJWireless baseada na configuração em vpnclient.ini.Uma vez que a conexão de VPN é estabelecida, o cliente pode alcançar os recursos de rede sob a proteção do IPSec VPN fixa serviços, como

mostrado.

## Verifique o log de eventos do cliente de VPN

Esta seção mostra como verificar a ordem do início de uma sessão do evento do cliente VPN para verificar que a inicialização automática continua corretamente.

Abra o visor do log do Cisco VPN Client e você vê a informação similar a esta durante a inicialização automática. Como você pode ver, o cliente VPN recebe o endereço IP 200.1.1.52 do wireless association, que cai no liste de redes 200.1.1.0/24 definido em vpnclient.ini. O cliente VPN liga então a conexão de SJWireless em conformidade. Durante a negociação de IKE, o Cisco VPN Client recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT de 50.1.1.8. Usa este endereço IP de Um ou Mais Servidores Cisco ICM NT como o IP da fonte para alcançar a rede interna atrás do 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 um estado de auto-iniciação diferente

Refira a utilização da informação dianteira da iniciação VPN automática sobre outros estados de inicialização automática.

## Informações Relacionadas

- Volume de referência do VPN 3000 series concentrator mim: Configuração
- Página de suporte do Cisco VPN 3000 Series Concentrator
- Página de suporte ao cliente do Cisco VPN 3000 Series
- Página de suporte do IPSec
- Suporte Técnico e Documentação - Cisco Systems