Configuring Automatic VPN Initiation on a Cisco VPN Client in a Wired/Wireless LAN Environment

Document ID: 26582

Contents

Introduction

This document describes how to configure the Cisco VPN Client to automatically initiate IPSec VPN connections to Cisco VPN 3000 Concentrators in a Wired/Wireless LAN (WLAN) environment.

In the WLAN environment, the wireless client first associates itself to a wireless Access Point (AP). Based on the IP address range it receives from the wireless connection, the VPN Client installed on the wireless automatically launches a VPN connection request to the corresponding VPN Concentrator on site. The IPSec VPN connection is then used in order to secure the wireless 802.11x traffic. Without the successful establishment of the Cisco VPN connection, the wireless clients have no access to the network resources.

This sample configuration shows the configuration of the VPN Client in order to enable the autoinitiation feature.

Prerequisites

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Requirements

Before you attempt this configuration, ensure that you are familiar with these concepts:

- Understand how to set up and configure the Cisco VPN Client and Cisco VPN 3000 Concentrator in order to establish an IPSec VPN tunnel
- Understand configurations related to wireless LANs

Components Used

The information in this document is based on these software and hardware versions:

- Cisco VPN Client version 4.x
- Cisco VPN 3000 Concentrator version 3.6
- Cisco Aironet 340 series Access Point
- Cisco Aironet 350 series wireless LAN adapter (version 5.0.1)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Note: In this example, Cisco Network Registrar is used as a Dynamic Host Configuration Protocol (DHCP) server in order to provide IP addresses to both wireless clients and VPN Clients.

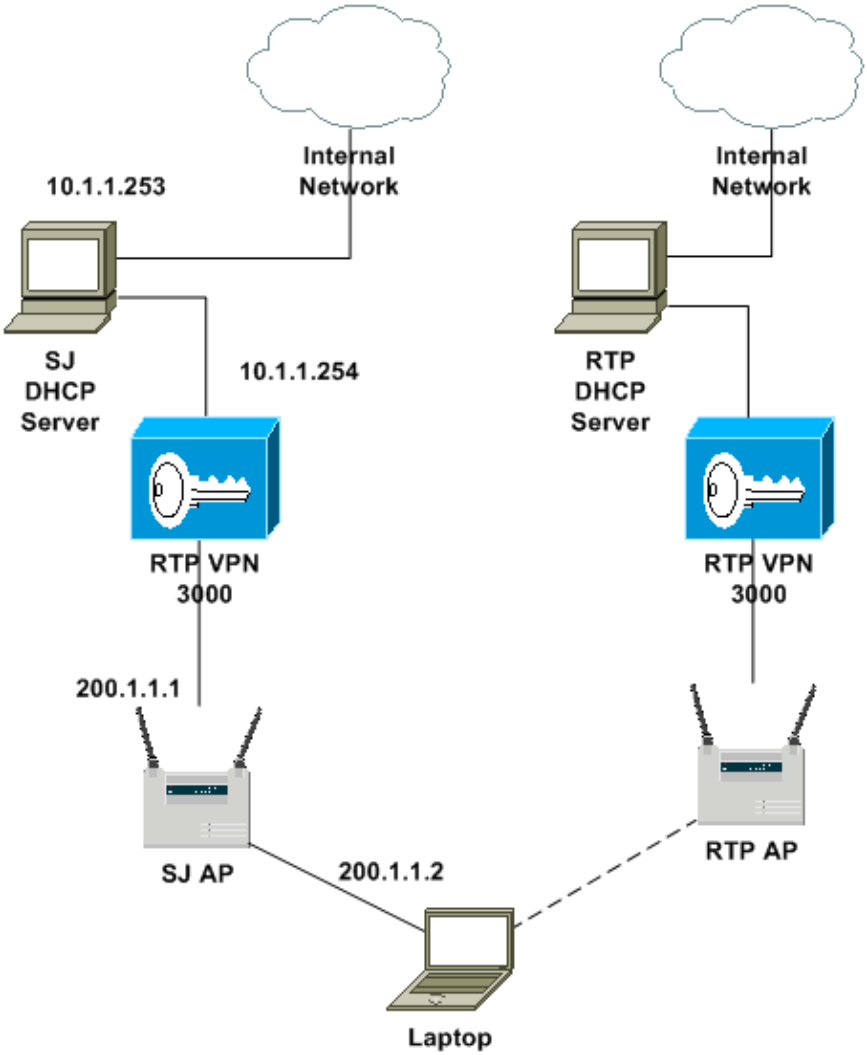
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: In this setup, the SJ DHCP server is used in order to provide IP addresses to both wireless connections and VPN connections. It has two IP address ranges defined:

- For wireless connections, the wireless users receive an IP address in the range from 200.1.1.50 to 200.1.1.250.
- For VPN connections, the VPN clients receive an IP address in the range from 50.1.1.1 to 50.1.1.254.

Configurations

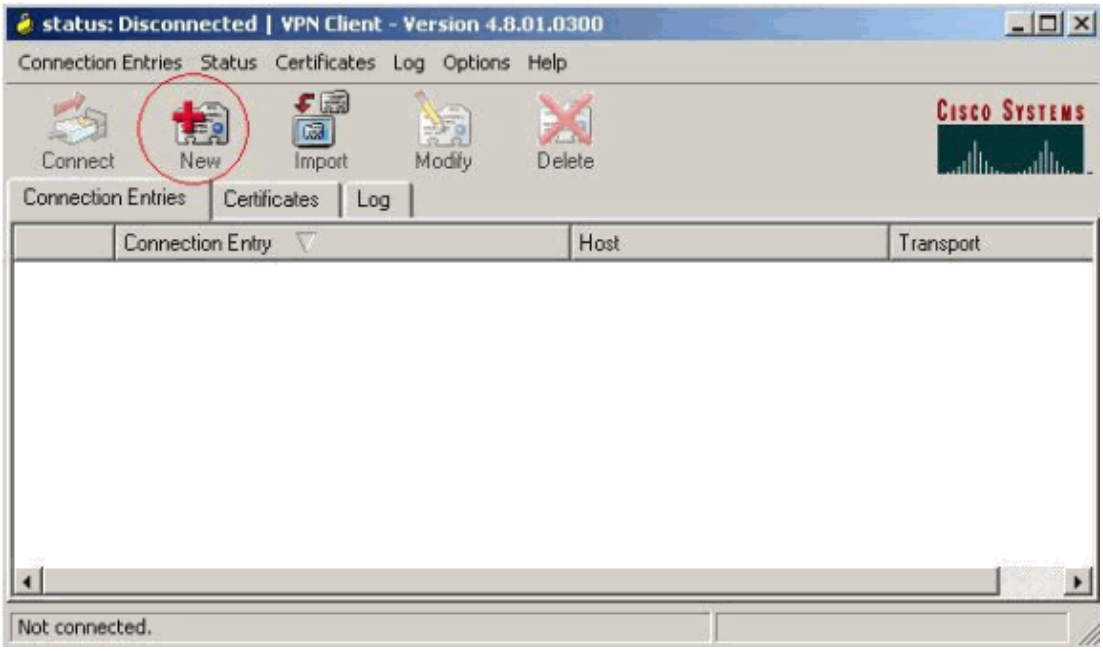
In this example, based on which site the user roams into, the wireless client automatically launches either one of the two VPN connections (namely SJWireless or RTPWireless) that are pre−defined in the VPN dialer. More specifically, if the wireless user gets an IP address in the range of 200.1.1.0/24 from the wireless association to the SJ AP, it launches the SJWireless connection from the VPN dialer. If it gets an IP address in the range of 150.1.1.0/24 from the wireless association to the RTP AP, it launches the RTPWireless connection from the VPN dialer.

In this section, the VPN connections are first configured under the VPN dialer, then the vpnclient.ini file is edited to add the autoinitiation configuration. Once these steps are finished on one VPN Client, the generated VPN profiles (.pcf files) and configured vpnclient.ini can be packaged, along with the VPN Client image, in order to distribute to the end users. The VPN connection launch is transparent to end users after VPN Client installation.

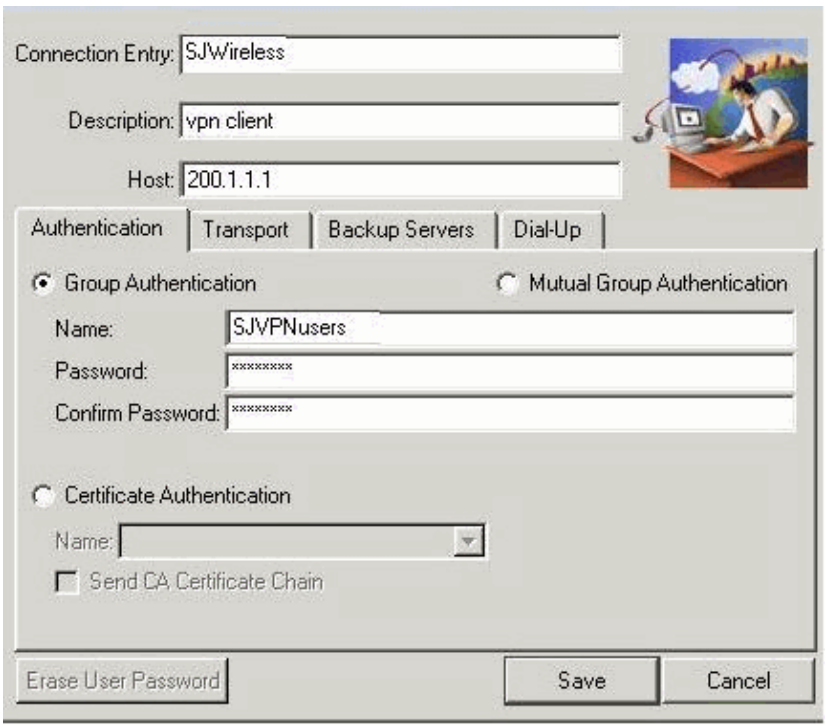
VPN Dialer Configuration

Complete these configuration steps:

1. Choose Start > Programs > Cisco Systems VPN Client > VPN Client. .Click **New** in order to launch the Create New VPN Connection Entry window.



2. Enter the name of the Connection Entry along with a description. Enter the outside IP address of the VPN Concentrator in the Host box. Then enter the VPN Group name and password, and click **Save**.



3. Repeat steps 1 and 2 in order to create another VPN connection with the name **RTPWireless** from the Cisco VPN dialer.

   When the second configuration process is complete, two VPN connection profiles named SJWireless.pcf and RTPWireless.pcf are generated on the client PC.

4. Complete these steps in order to edit the default vpnclient.ini file found on the client PC in order to enable the autoinitiation feature:

    a. Enable the autoinitiation feature with the **AutoInitiationEnable** keyword under the [main] section.
    b. Define the **AutoInitiationList**. Each item in the list corresponds to a section, where the name of the VPN connection and wireless IP address range are associated.

    In this example, SJWireless VPN connection corresponds to 200.1.1.0/24 and RTPWireless connection corresponds to 150.1.1.0/24.

    When steps a and b are complete, the file vpnclient.ini looks like this:

```
[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. After steps 1 − 3 are complete on one VPN Client, the vpnclient.ini and the VPN connection profiles (.pcf) can be collected and distributed to the end users in the installation package. Refer to VPN Client Administrator Guide, Release 3.6 for information on how to preconfigure the VPN Clients for remote users.

Cisco VPN 3000 Concentrator Configuration

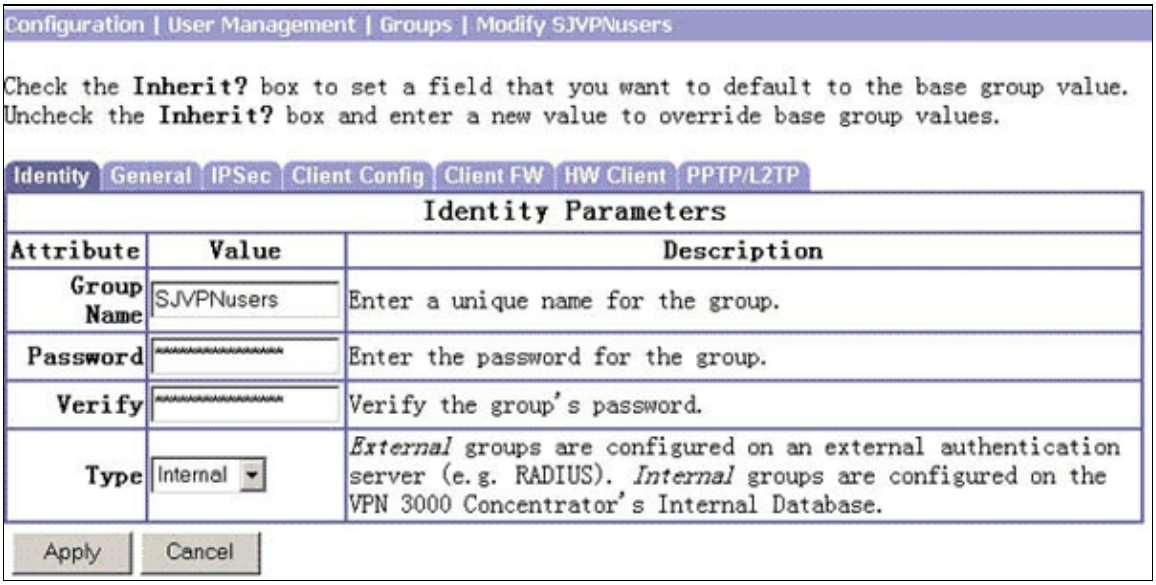
Complete these configuration steps:

1. On VPN 3000 Concentrators, the VPN groups need to be configured to establish an IPSec connection with the VPN Client. In the example, the wireless users can connect to different VPN Concentrators

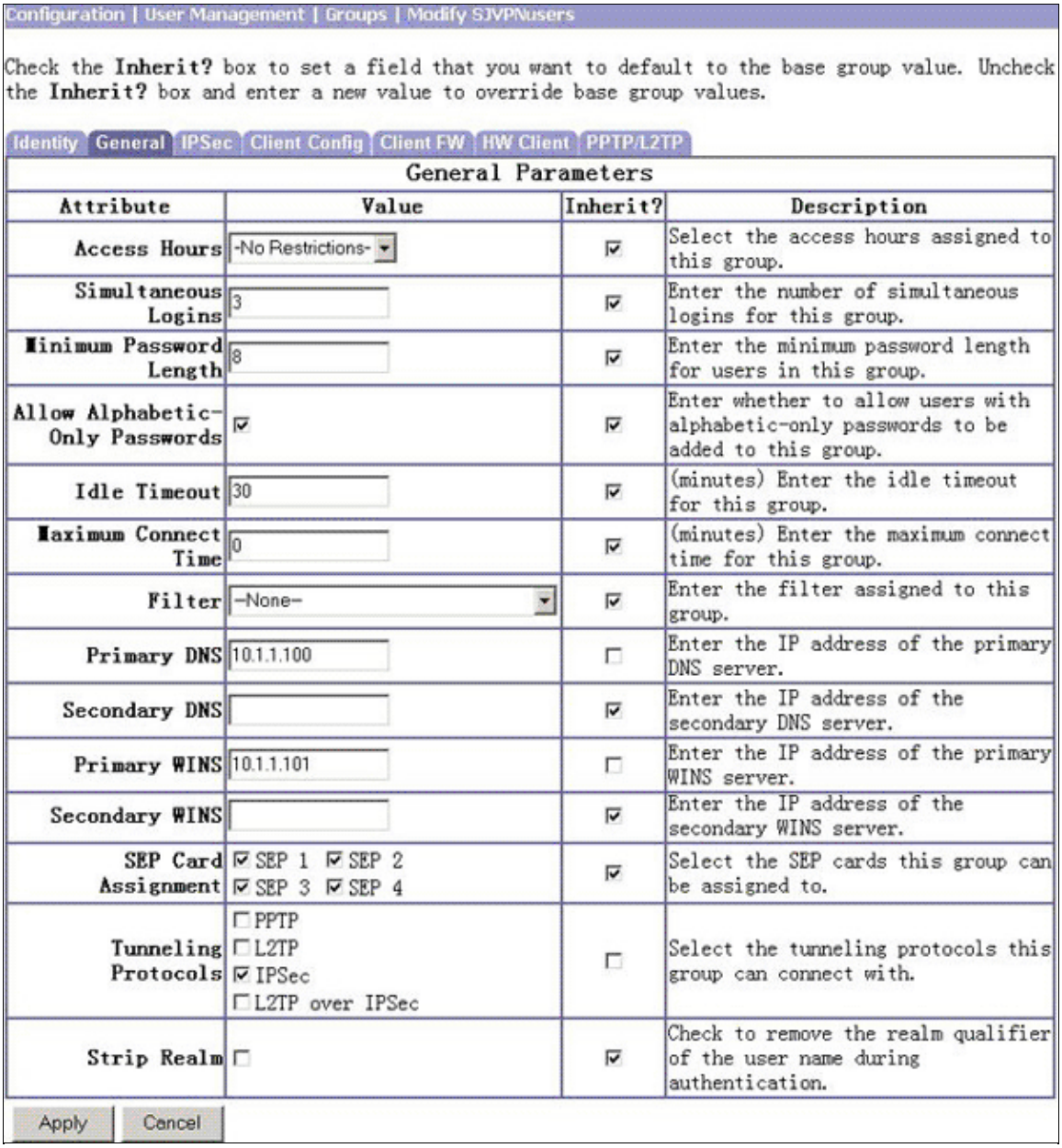
based on the site in which they roam. Here, only the important configuration tasks on the SJ VPN Concentrator are highlighted. A VPN group called **SJVPNusers**, which matches the VPN group name on the client, is created.

2. Choose **Configuration > User Management > Groups** and choose **SJVPNusers** from the Current Group listing. Select **Modify Group** from the Actions option if the group is already created, or **Add Group** and then **Modify Group** if the group must be created.
3. Click the Identity tab.

   The Identity Parameters window appears. Verify that the information displayed in this window is correct for your configuration.

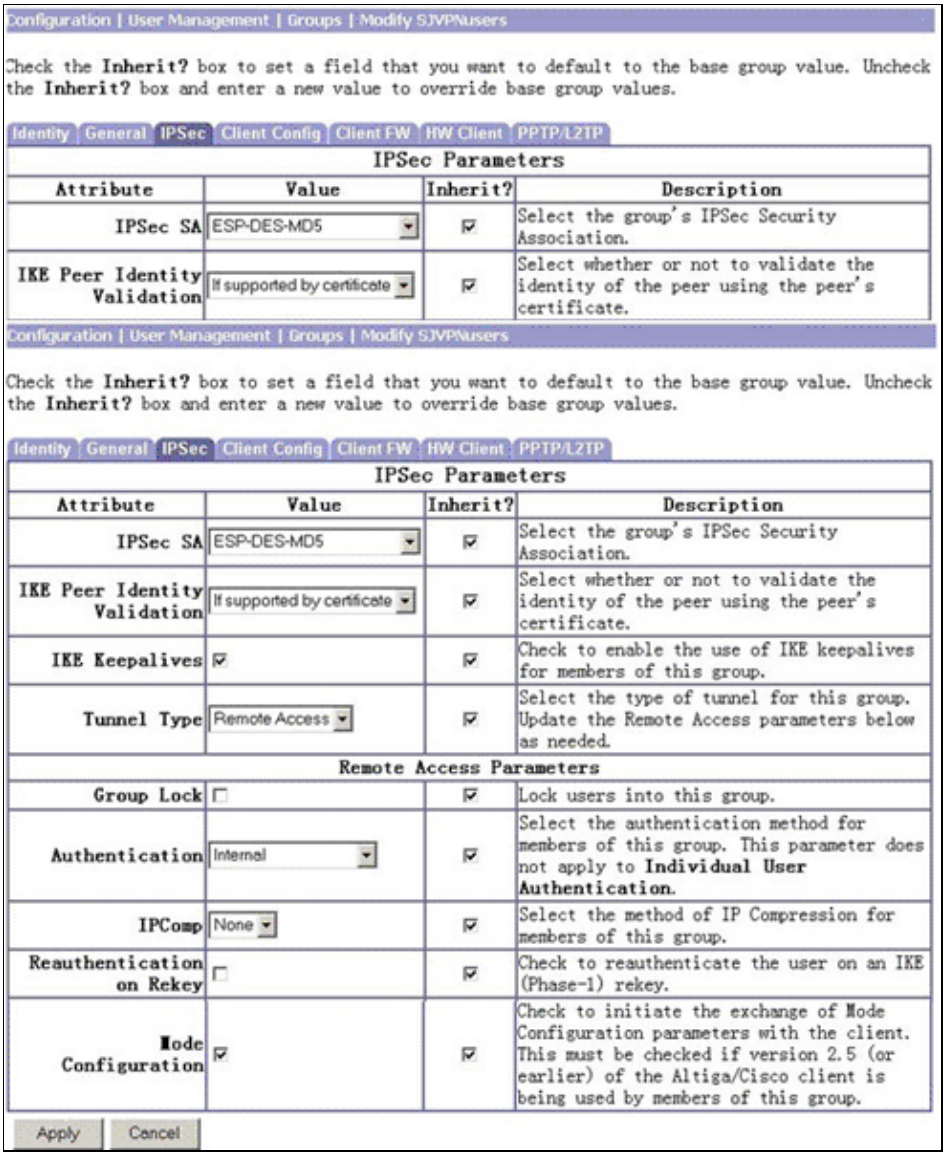


4. Click the General tab and then check the **IPSec** box for the Tunneling Protocols attribute.



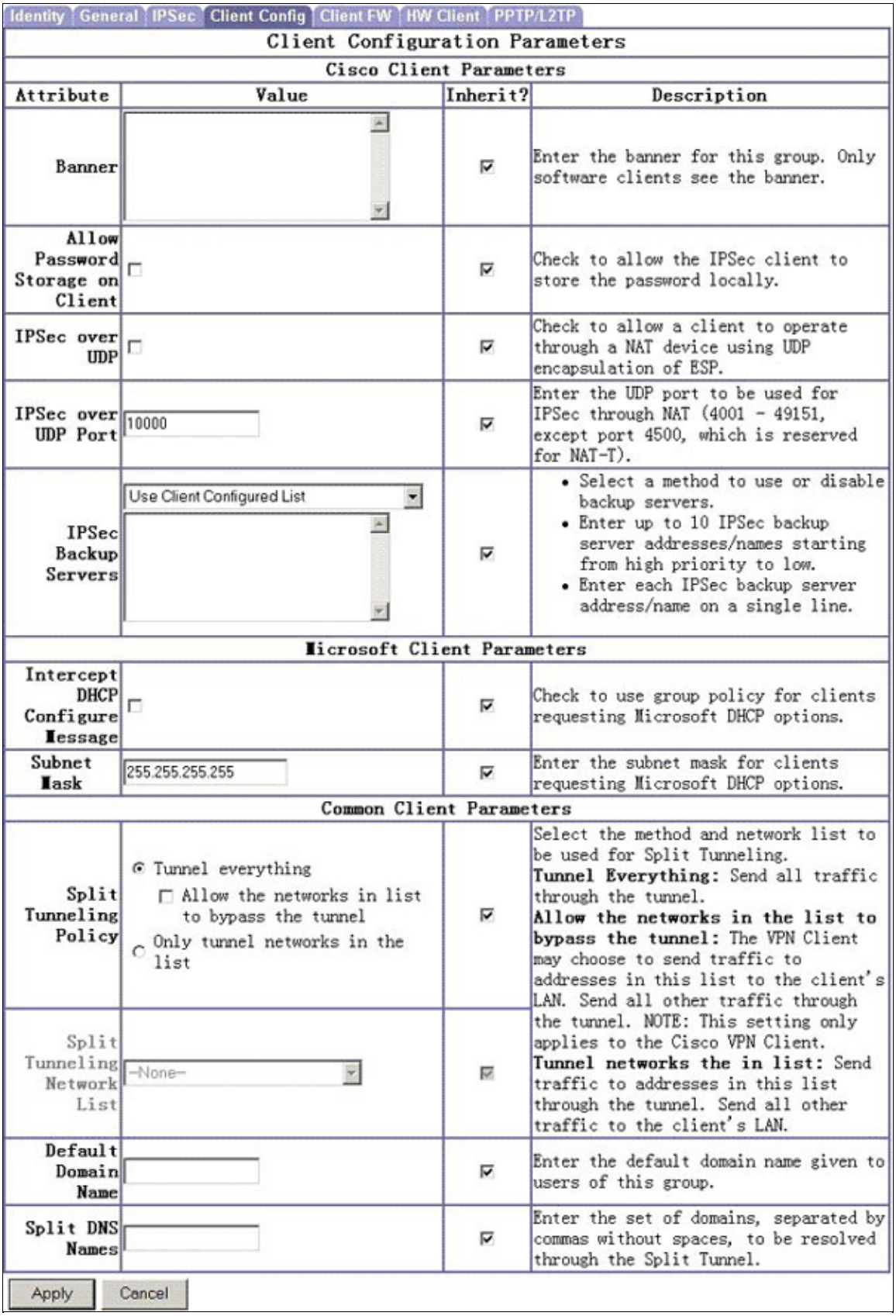
5. Click the IPSec tab, then specify the IPSec security association (SA) and the Authentication method attribute with the drop−down menus and check boxes provided.

   In this case, the VPN users are defined locally on the VPN 3000 Concentrator, so the authentication method is Internal.



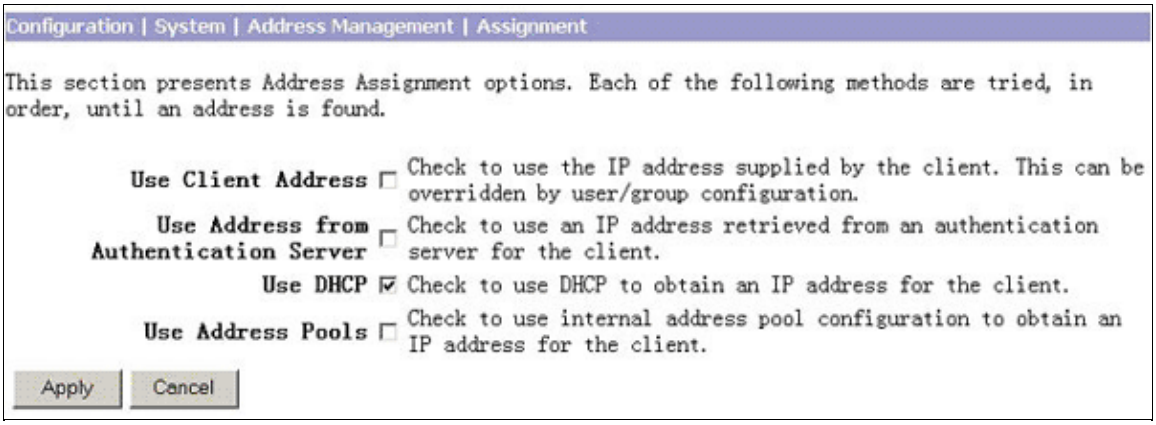
6. Click the Client Config tab, then specify the mode configuration parameters on the Client Configuration Parameters window. Click **Apply**.

   In this case, all the traffic from the VPN Client is encrypted and sent to the IPSec tunnel. This is specified under the Common Client Parameters.

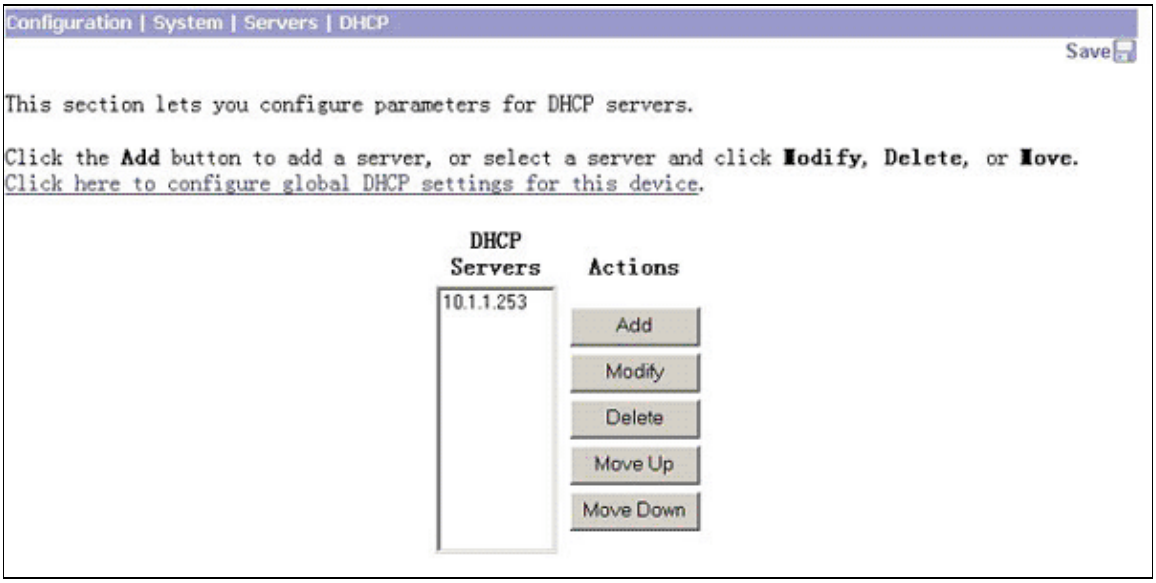


7. Choose **Configuration > System > Address Management > Assignment**. From the Address Assignment options window, specify the IP address assignment method with the checkboxes provided.

   In this case, the VPN Client gets an IP address from a DHCP server during IKE negotiation, so the Use DHCP option is checked. Click **Apply**.



8. Use the DHCP server configuration window in order to set up the DHCP server parameters, and click **Save** in order to save the settings.



As mentioned, one DHCP server behind the VPN 3000 Concentrator is used for both wireless connections and VPN connections. For wireless connections, the concentrator serves as a DHCP relay agent to relay the DHCP message between the wireless AP and DHCP server.

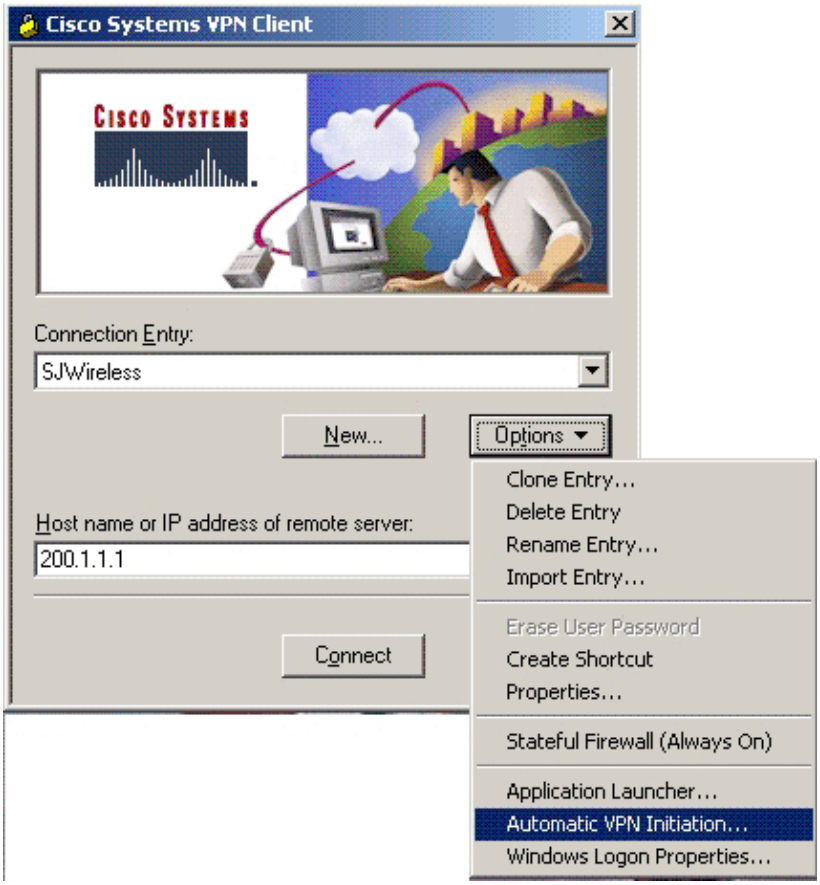
Verify

Use this section to confirm that your configuration works properly.

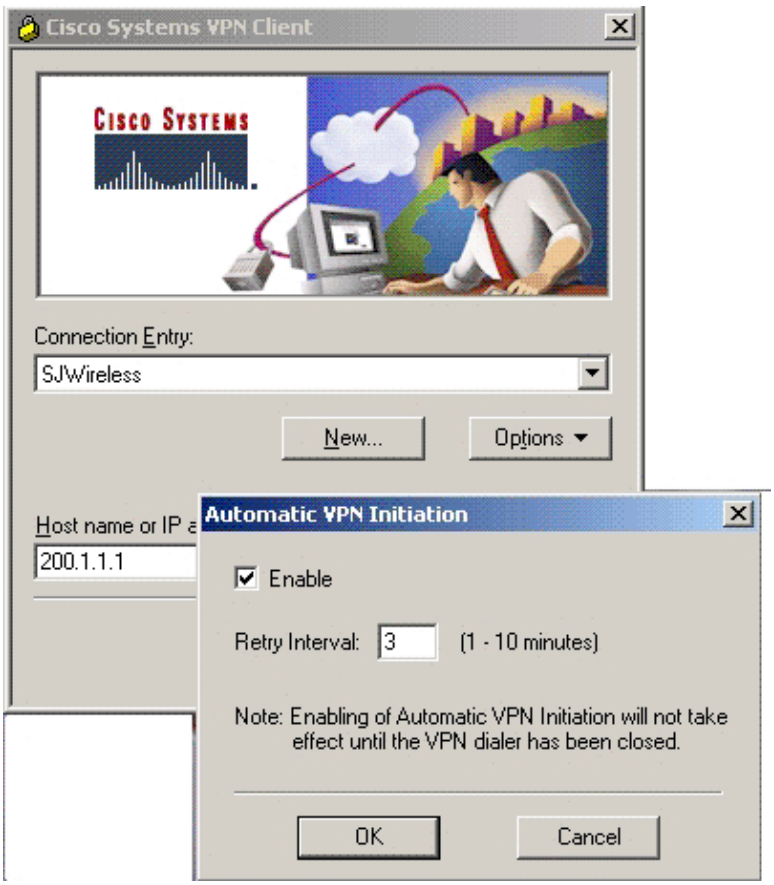
Verify the Auto−Initiation Configuration from the VPN Dialer

Complete these steps in order to verify the autoinitiation configuration from the VPN dialer:

1. From the Cisco VPN Dialer window on the VPN Client workstation, click **Options** and select **Automatic VPN Initiation**.



2. On the Automatic VPN Initiation window, verify that the Enable check box is checked. If it is not, check it. Click **OK** in order to close the window.

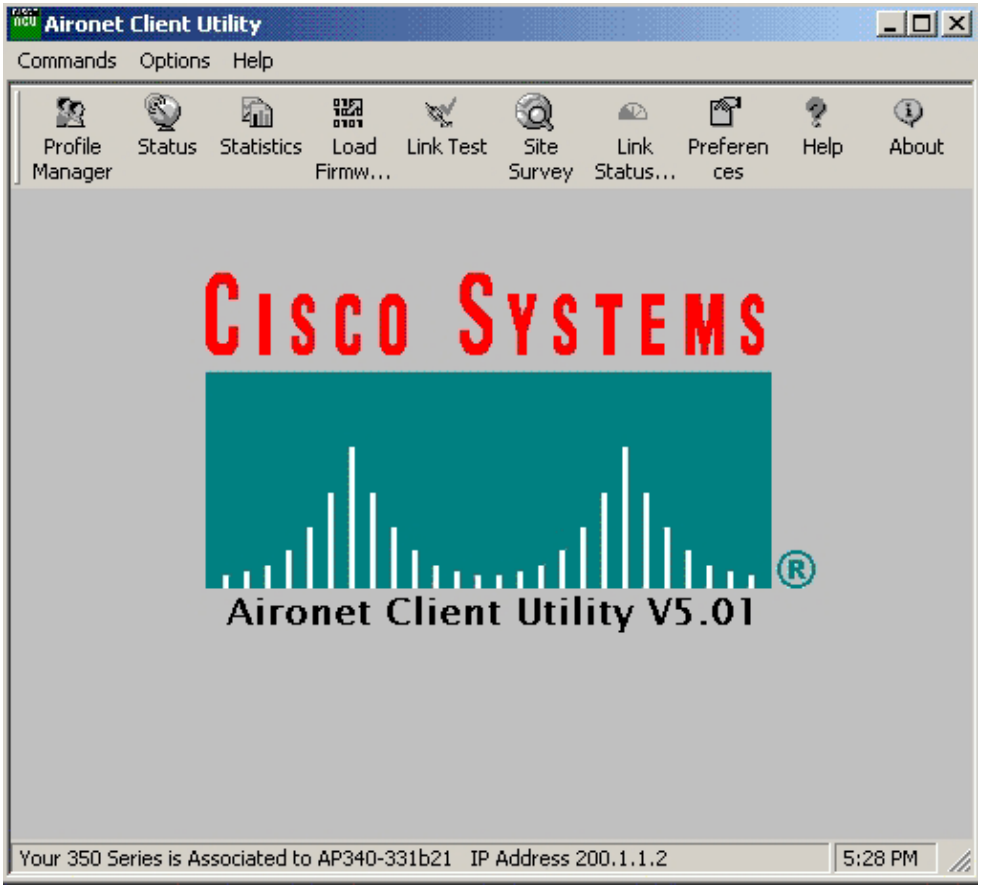


Verify the Auto−Initiation Feature in the WLAN Environment

Complete these steps in order to verify the autoinitiation feature in the WLAN environment:

1. Insert the wireless LAN adapter into the PC, and wait for the association to the wireless AP.

   In order to verify the wireless association, start the Aironet Client Utility software and check the bottom of the Aironet Client window. The wireless client shown in the figure is able to associate to the wireless AP whose IP address is 200.1.1.2.



2. Once the wireless association is complete, the VPN Client automatically launches a connection based on the IP address received from the wireless connection. In this case, the wireless client receives 200.1.1.52 from the wireless AP, and the VPN Client launches the SJWireless Connection based on the configuration in vpnclient.ini.

   Once the VPN connection is established, the client is able to access the network resources under the protection of the IPSec VPN secure services, as shown.

Check the VPN Client Event Log

This section shows how to check the VPN Client event log in order to verify that autoinitiation proceeds properly.

Open the Cisco VPN Client log viewer and you see information similar to this during the autoinitiation. As you can see, the VPN Client receives the 200.1.1.52 IP address from the wireless association, which falls into the 200.1.1.0/24 network list defined in vpnclient.ini. The VPN Client then starts the SJWireless connection accordingly. During the IKE negotiation, the Cisco VPN Client receives an IP address of 50.1.1.8. It uses this IP address as the source IP to access the internal network behind the 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
```

Verify a Different Auto−Initiation State

Refer to Using Automatic VPN Initiation fore information about other states of autoinitiation.

Related Information

- **VPN 3000 Series Concentrator Reference Volume I: Configuration**
- **Cisco VPN 3000 Series Concentrator Support Page**
- **Cisco VPN 3000 Series Client Support Page**
- **IPSec Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 09, 2007 Document ID: 26582