Настройка автоматического приглашения VPN клиента Cisco VPN в среде беспроводной локальной сети

Содержание

Введение

Этот документ описывает, как настроить Cisco VPN Client для автоматического инициирования соединений IPSEC VPN с Cisco VPN 3000 Concentrator в Проводном (WLAN) среда / Беспроводная локальная сеть (WLAN) среда.

В среде WLAN беспроводной клиент сначала привязывает себя к точке беспроводного доступа (AP). На основе Диапазона IP-адресов это получает от беспроводного соединения, Клиент VPN установил на радио, автоматически запускает запрос VPN-подключения к соответствующему Концентратору VPN на месте. Соединение IPSEC VPN тогда используется для обеспечения радио 802.11x трафик. Без успешного установления VPN-подключения Cisco у беспроводных клиентов нет доступа к сетевым ресурсам.

Этот пример конфигурации показывает конфигурацию Клиента VPN для активации опции автоинициации.

Предварительные условия

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Требования

Прежде чем вы будете делать попытку этой конфигурации, будете гарантировать, что вы знакомы с этими понятиями:

- Поймите, как установить и настроить Cisco VPN Client и Cisco VPN 3000 Concentrator для установления VPN-туннеля IPSec
- Поймите конфигурации, отнесенные к беспроводным локальным сетям

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco VPN Client версии 4.x
- Версия 3.6 Cisco VPN 3000 Concentrator
- Точка доступа Cisco Aironet серии 340
- Адаптер беспроводной сети Cisco Aironet серии 350 (версия 5.0.1)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Примечание: В данном примере Cisco Network Registrar используется в качестве сервера протокола динамической конфигурации узла (DHCP) для обеспечения IP-адресов и беспроводным клиентам и Клиентам VPN.

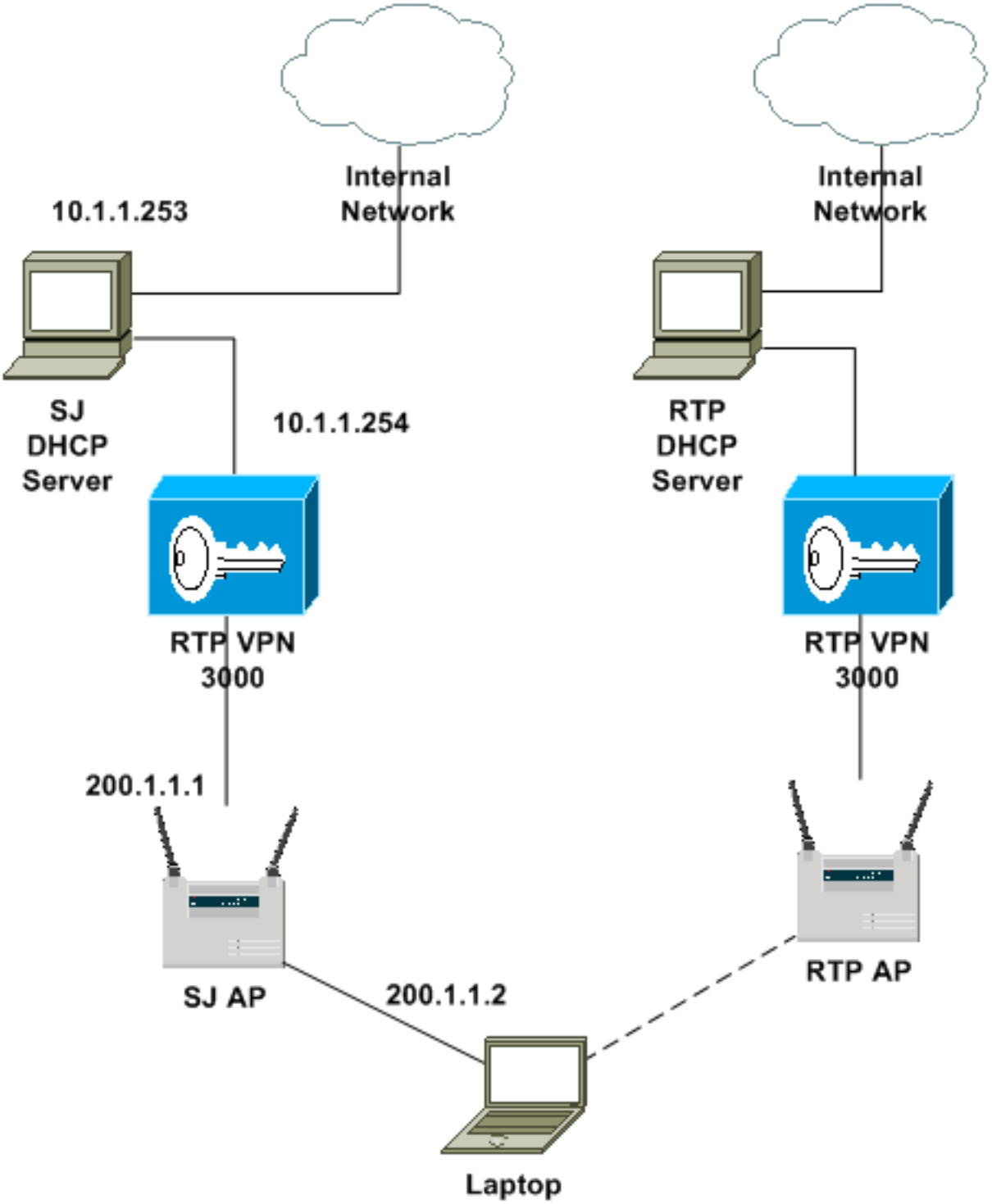
Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:



Примечание: В этой настройке сервер DHCP SJ используется для обеспечения IP-адресов и беспроводным соединениям и VPN-подключениям. Это имеет два определенные Диапазона IP-адресов:

- Для беспроводных соединений пользователи беспроводной связи получают IP-адрес в диапазоне от 200.1.1.50 до 200.1.1.250.
- Для VPN-подключений клиенты VPN получают IP-адрес в диапазоне от 50.1.1.1 до 50.1.1.254.

Конфигурации

В данном примере, на основе которого помещают пользователя, перемещается в, беспроводной клиент автоматически запускает или одно из этих двух VPN-подключений (а

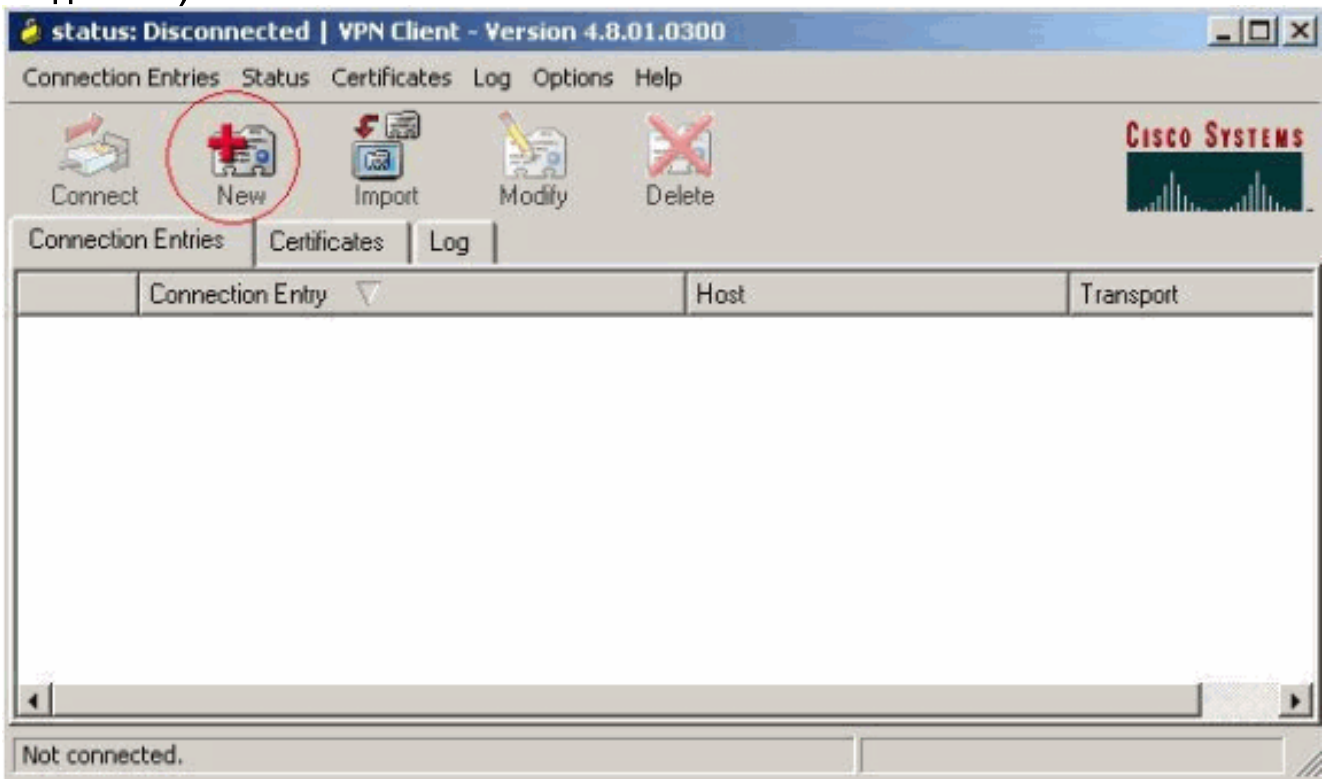
именно, SJWireless или RTPWireless), которые предустановлены в программе VPN dialer. Более в частности, если пользователь беспроводной связи получает IP-адрес в диапазоне 200.1.1.0/24 от связи с беспроводным устройством до AP SJ, это запускает соединение SJWireless от программы VPN dialer. Если это получает IP-адрес в диапазоне 150.1.1.0/24 от связи с беспроводным устройством до AP RTP, это запускает соединение RTPWireless от программы VPN dialer.

В этом разделе VPN-подключения сначала настроены под программой VPN dialer, тогда файл vpnclient.ini отредактирован для добавления конфигурации автоматического инициирования. Как только эти шаги закончены на одном Клиенте VPN, генерируемые профили VPN (файлы .pcf) и настроенный vpnclient.ini могут быть упакованы, наряду с образом Клиента VPN, для распределения конечным пользователям. Запуск VPN-подключения очевиден для конечных пользователей после установки Клиента VPN.

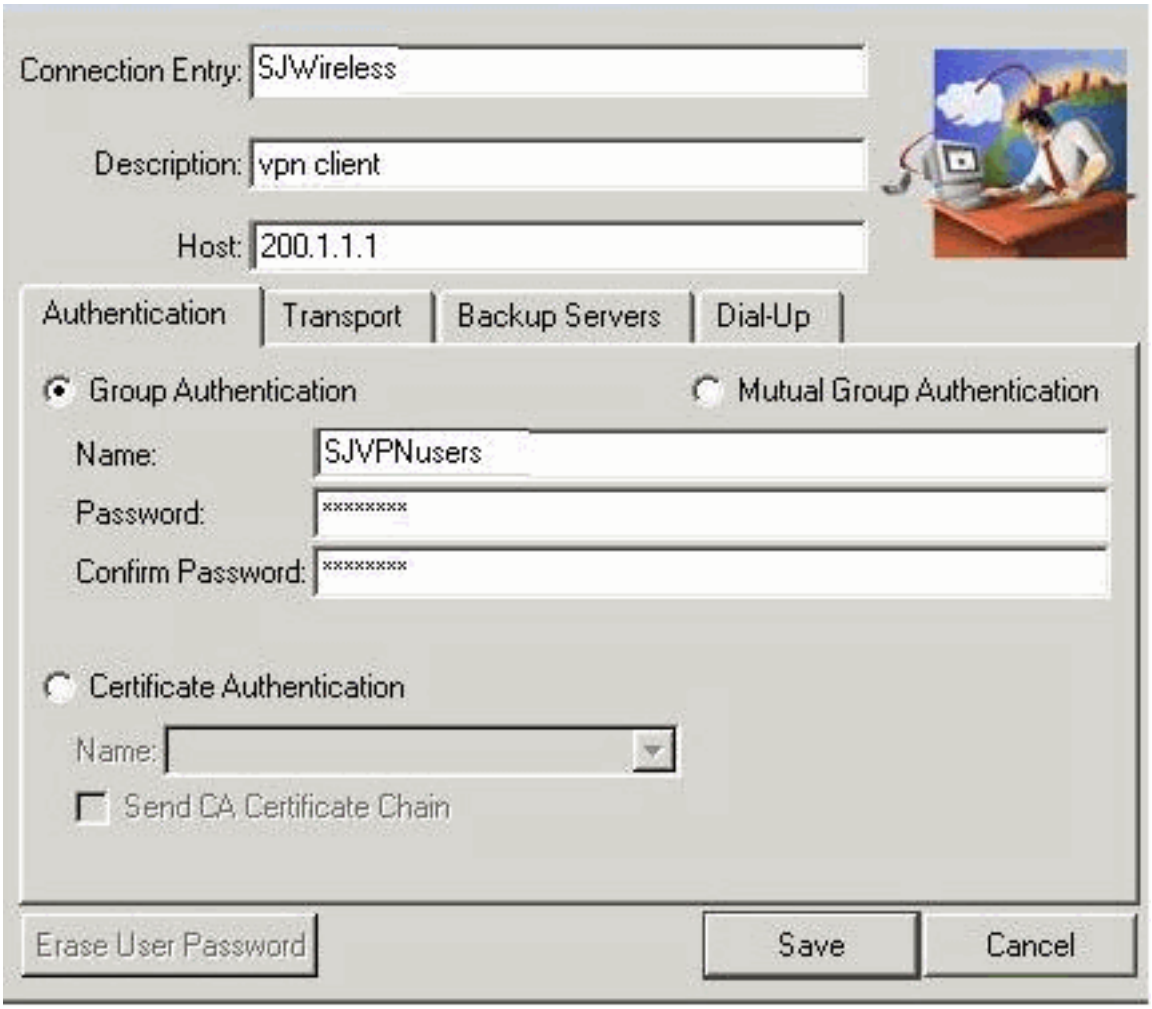
Конфигурация номеронабирателя VPN

Завершите эти действия настройки:

1. Выберите Пуск > Программы > Cisco Systems VPN Client > VPN Client. **Нажмите New, чтобы открыть окно "Create New VPN Connection Entry" (Создание новой записи VPN-соединения).**



2. Введите имя записи и описание подключения. Введите внешний IP - адрес Концентратора VPN в коробке Хоста. **Затем введите имя группы VPN и нажмите кнопку Save (Сохранить).**



3. Повторите шаги 1 и 2 для создания другого VPN-подключения с **RTPWireless** названия от программы VPN dialer Cisco.Когда второй процесс конфигурирования завершен, два профиля VPN-подключения под названием SJWireless.pcf и RTPWireless.pcf генерируются на клиентском компьютере.
4. Выполните эти шаги для редактирования файла vpnclient.ini по умолчанию, найденного на клиентском компьютере для активации опции автоинициации:Активируйте опцию автоинициации с **ключевым словом AutoInitiationEnable** под [основным] разделом.Определите **AutoInitiationList**. Каждый элемент в списке соответствует разделу, где привязано название VPN-подключения и беспроводного Диапазона IP-адресов.В данном примере беспроводное подключение VPN SJ соответствует 200.1.1.0/24, и соединение RTPWireless соответствует 150.1.1.0/24.Когда шаги a и b завершены, vpnclient.ini файла похож на это:

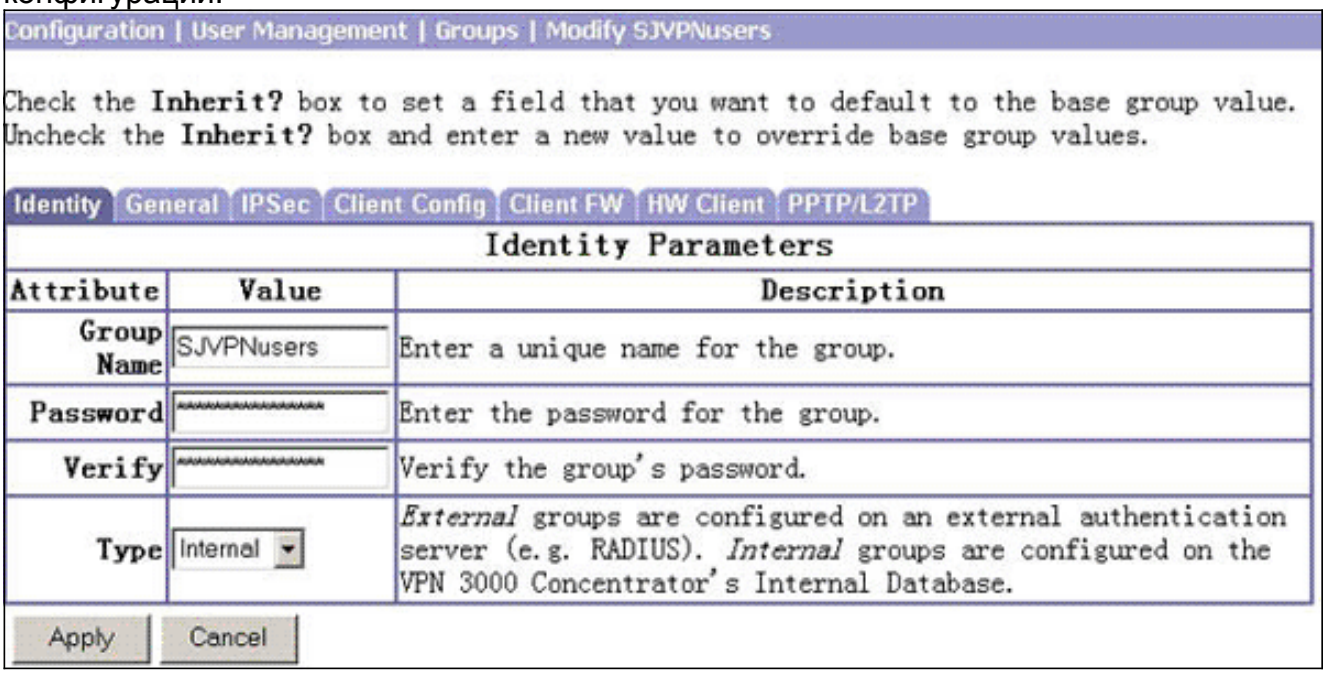
```
[LOG.CVPND]
LogLevel=1
[LOG.CERT]
LogLevel=3
[LOG.PPP]
LogLevel=2
[LOG.CM]
LogLevel=1
[LOG.IPSEC]
LogLevel=3
[main]
AutoInitiationEnable=1 AutoInitiationRetryInterval=3 AutoInitiationList=SJVPN,RTPVPN
EnableLog=1 [SJVPN] Network=200.1.1.0 Mask=255.255.255.0 ConnectionEntry=SJWireless
[RTPVPN] Network=150.1.1.0 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. После того, как шаги 1 - 3 завершены на одном Клиенте VPN, vpnclient.ini и VPN-подключение представляют (.pcf), может быть собран и распределен конечным пользователям в пакете установки. См. Руководство администратора Клиента VPN, Выпуск 3.6 для получения информации о том, как предварительно сконфигурировать Клиенты VPN для удаленных пользователей.

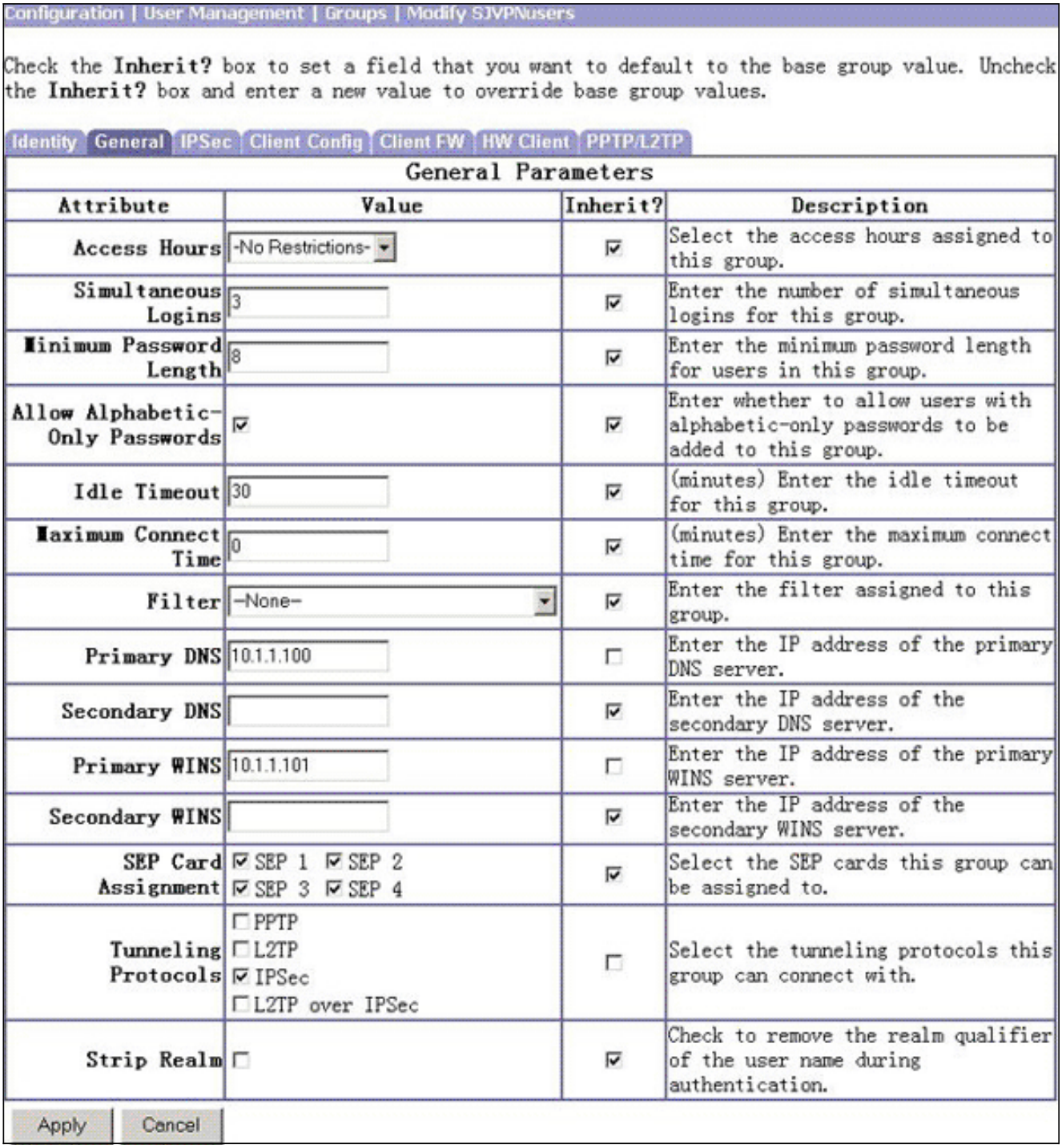
Конфигурация концентратора Cisco VPN 3000

Завершите эти действия настройки:

1. На VPN 3000 Concentrator группы VPN должны быть настроены для установления IP - безопасного соединения с Клиентом VPN. В примере пользователи беспроводной связи могут соединиться с другими Концентраторами VPN на основе узла, в котором они перемещаются. Здесь, только важные задачи конфигурации на Концентраторе VPN SJ выделены. Группа VPN вызвала **SJVPNusers**, который совпадает с Именем группы VPN на клиенте, создан.
2. **Choose Configuration> User Management> Groups** и выбирает **SJVPNusers** из Текущего перечня групп. Выберите **Modify Group** от Параметра действий, если группа уже создана, или **Add Group** и затем **Modify Group**, если должна быть создана группа.
3. Нажмите вкладку Identity.Окно параметров идентичности появляется. Проверьте, что информация, отображенная в этом окне, корректна для вашей конфигурации.



4. Нажмите Вкладку Общие и затем установите флажок **IPSec** для атрибута Протоколов туннелирования.



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.

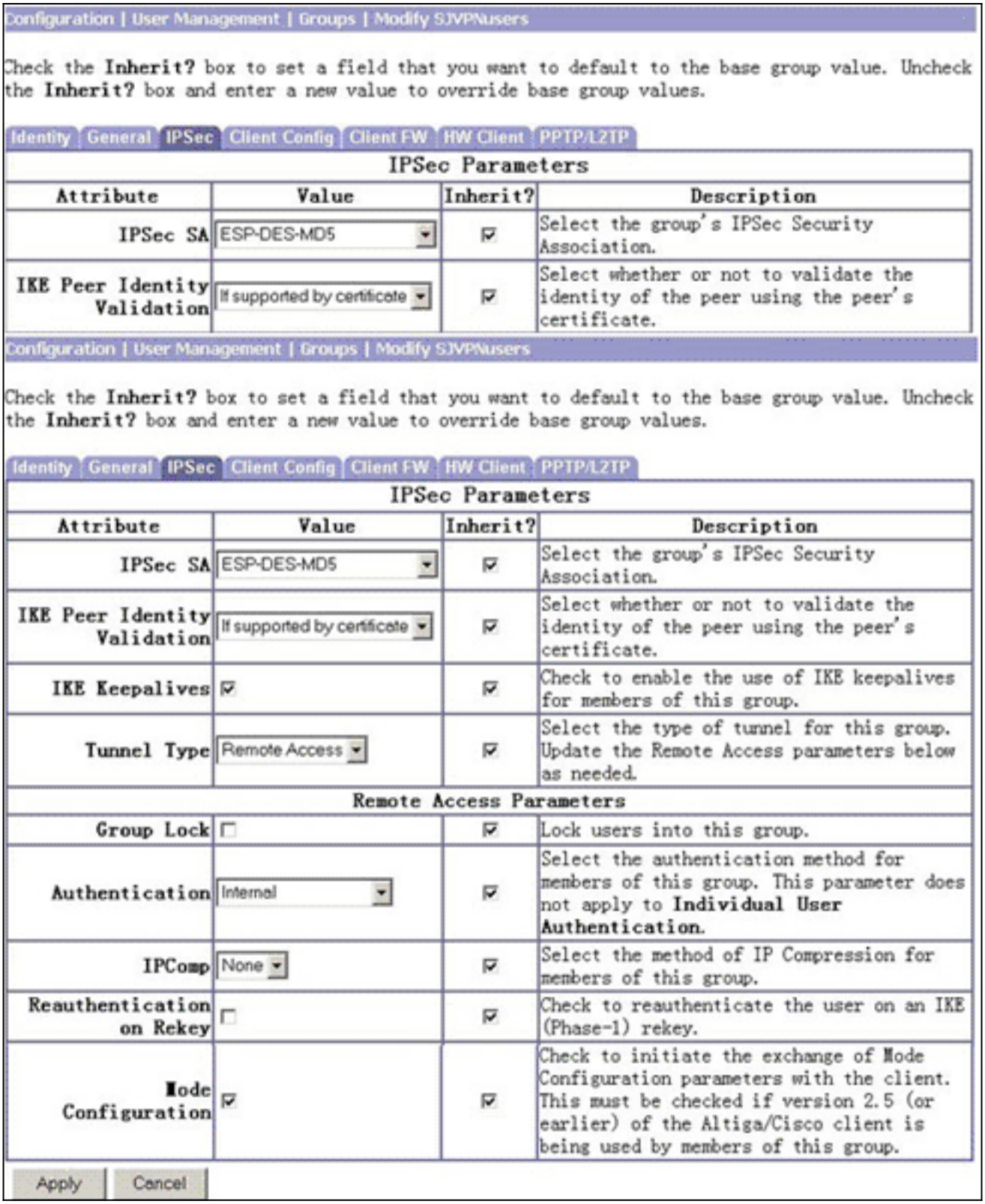
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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. Нажмите вкладку IPSec, затем задайте Сопоставление безопасности IPSec (SA) и атрибут Метода аутентификации с раскрывающимися меню и предоставленными флажками.В этом случае пользователи VPN определены локально на VPN 3000 Concentrator, таким образом, метод аутентификации является Внутренним.


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.

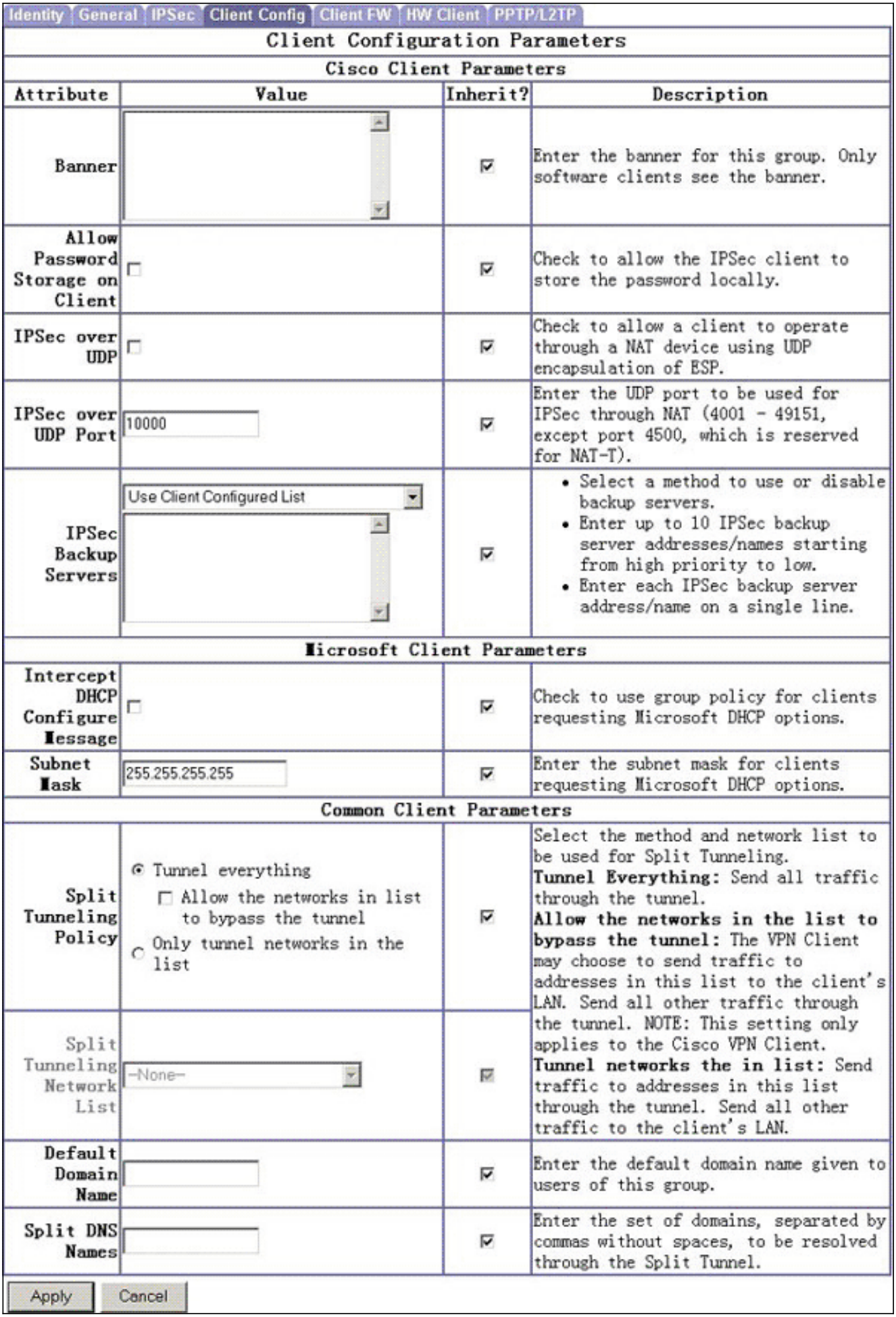
Identity | General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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. Нажмите Client Config tab, затем задайте параметры конфигурации режима на Окне Parameters Конфигурации клиента. **Щелкните "Применить".**В этом случае весь трафик от Клиента VPN зашифрован и передан Туннелю IPSec. Это задано под Общими параметрами
клиентов.



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

Client Configuration Parameters

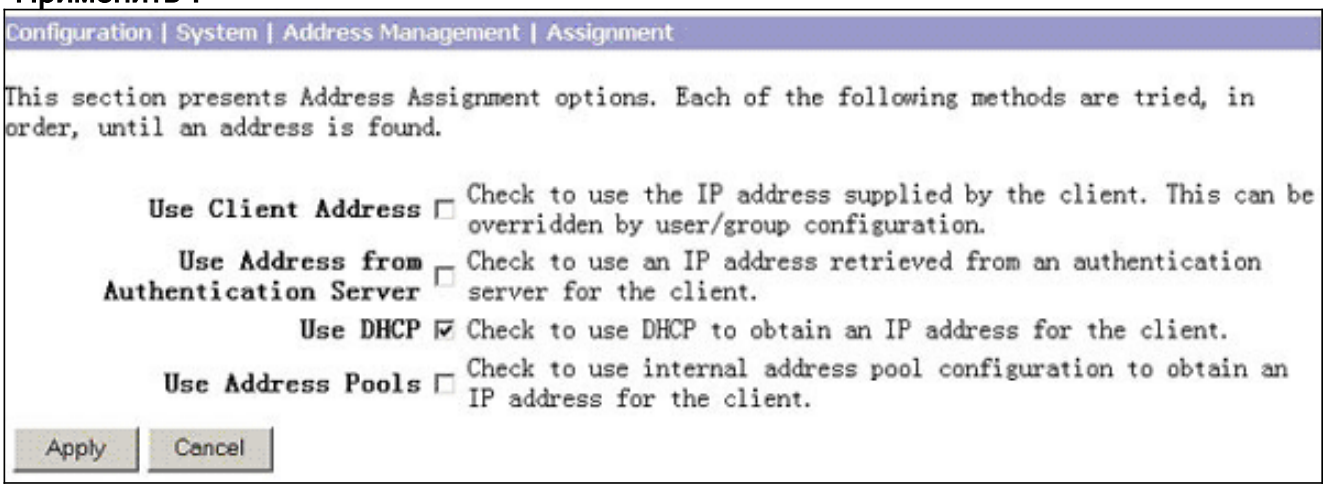
Cisco Client Parameters

Attribute	Value	Inherit?	Description
Banner		☑	Enter the banner for this group. Only software clients see the banner.
Allow Password Storage on Client	☐	☑	Check to allow the IPSec client to store the password locally.
IPSec over UDP	☐	☑	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPSec over UDP Port	10000	☑	Enter the UDP port to be used for IPSec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPSec Backup Servers	Use Client Configured List	☑	• Select a method to use or disable backup servers. • Enter up to 10 IPSec backup server addresses/names starting from high priority to low. • Enter each IPSec backup server address/name on a single line.
Microsoft Client Parameters			
Intercept DHCP Configure Message	☐	☑	Check to use group policy for clients requesting Microsoft DHCP options.
Subnet Mask	255.255.255.255	☑	Enter the subnet mask for clients requesting Microsoft DHCP options.
Common Client Parameters			
Split Tunneling Policy	◉ Tunnel everything ☐ Allow the networks in list to bypass the tunnel ○ Only tunnel networks in the list	☑	Select the method and network list to be used for Split Tunneling. **Tunnel Everything:** Send all traffic through the tunnel. **Allow the networks in the list to bypass the tunnel:** The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco VPN Client. **Tunnel networks the in list:** Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.
Split Tunneling Network List	-None-	☑	
Default Domain Name		☑	Enter the default domain name given to users of this group.
Split DNS Names		☑	Enter the set of domains, separated by commas without spaces, to be resolved through the Split Tunnel.

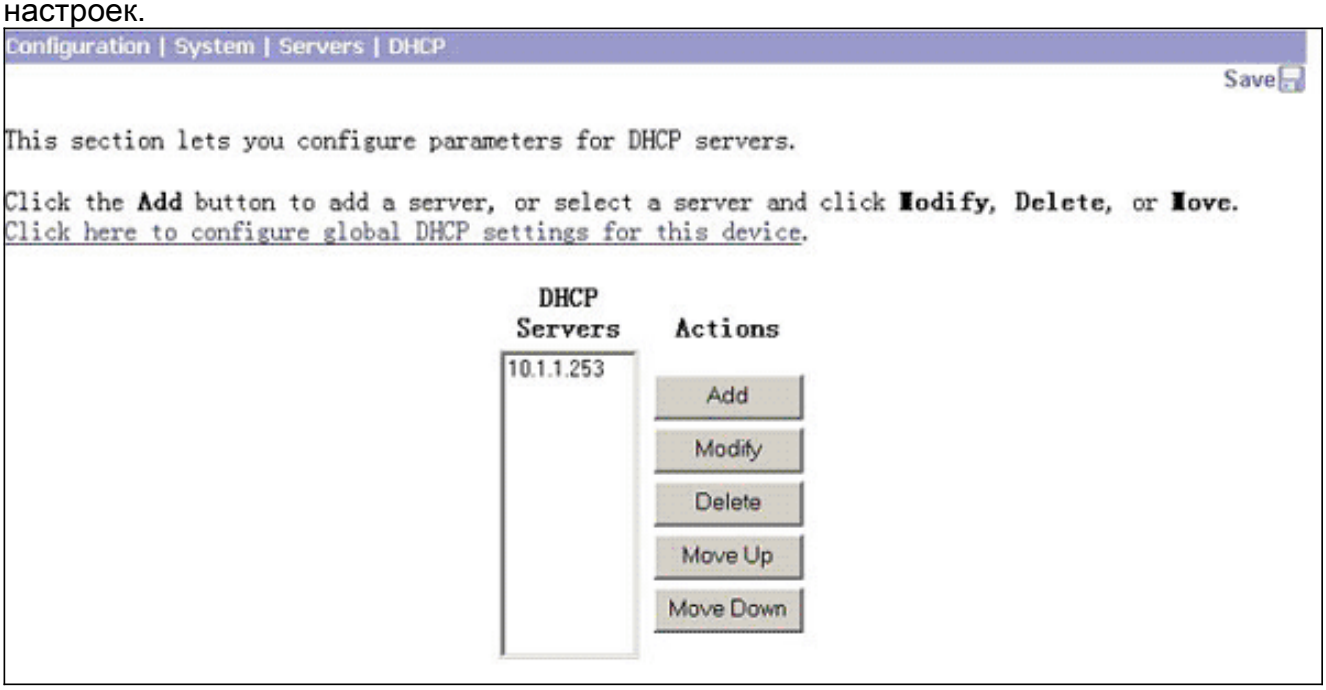
Apply | Cancel

7. Выберите **Configuration> System> Address Management> Assignment**. От окна свойств Address Assignment задайте метод присвоения IP-адреса с предоставленными

флажками.В этом случае Клиент VPN получает IP-адрес от сервера DHCP во время Ike согласование, таким образом, проверен параметр DHCP Использования. **Щелкните "Применить".**



8. Используйте окно конфигурации сервера DHCP, чтобы установить параметры сервера DHCP и нажать **Save** для сохранения
настроек.



Как упомянуто, один сервер DHCP позади VPN 3000 Concentrator используется и для беспроводных соединений и для VPN-подключений. Для беспроводных соединений концентратор служит агентом ретрансляции DHCP для передачи сообщения DHCP между беспроводным AP и сервером DHCP.

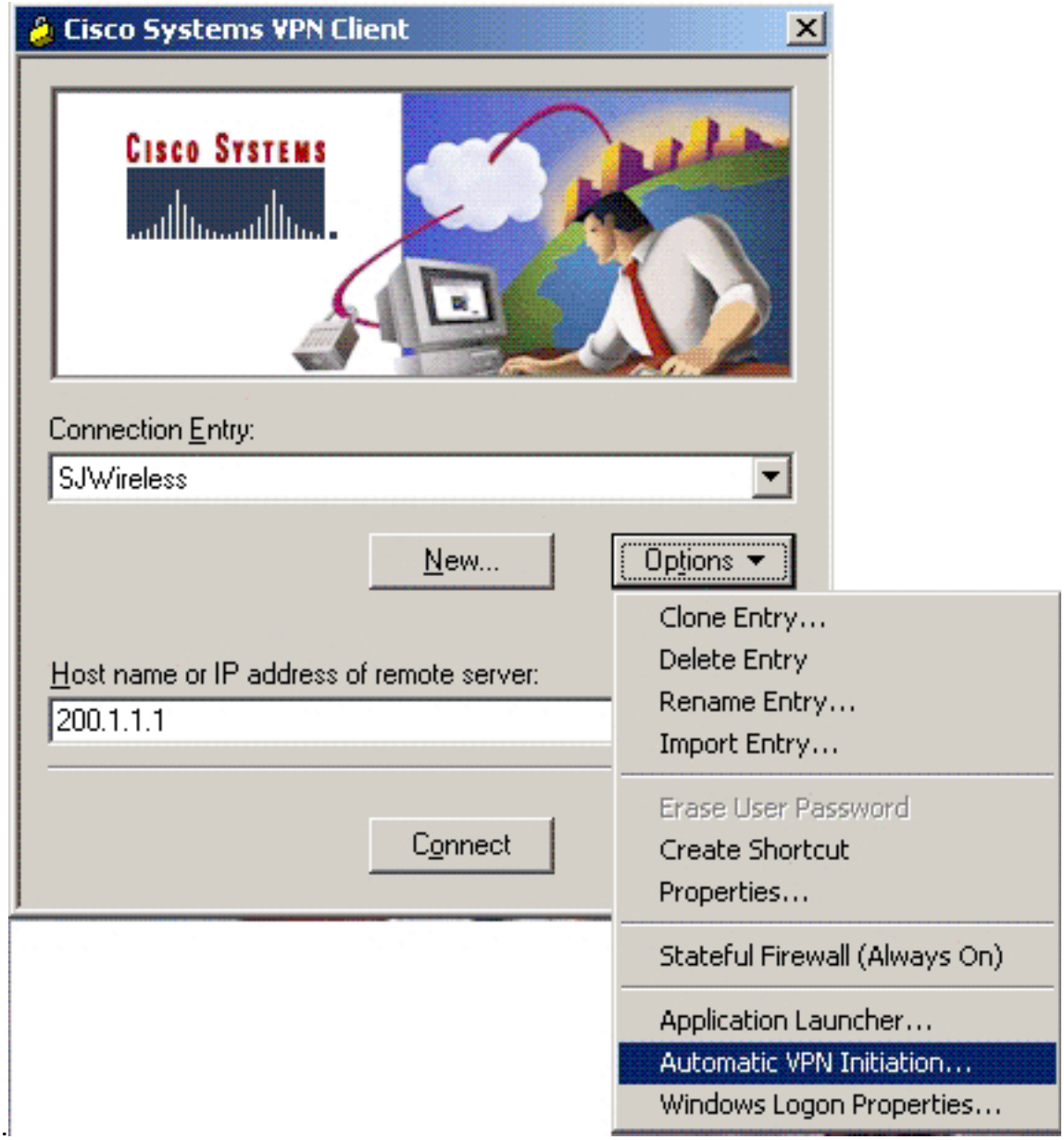
Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

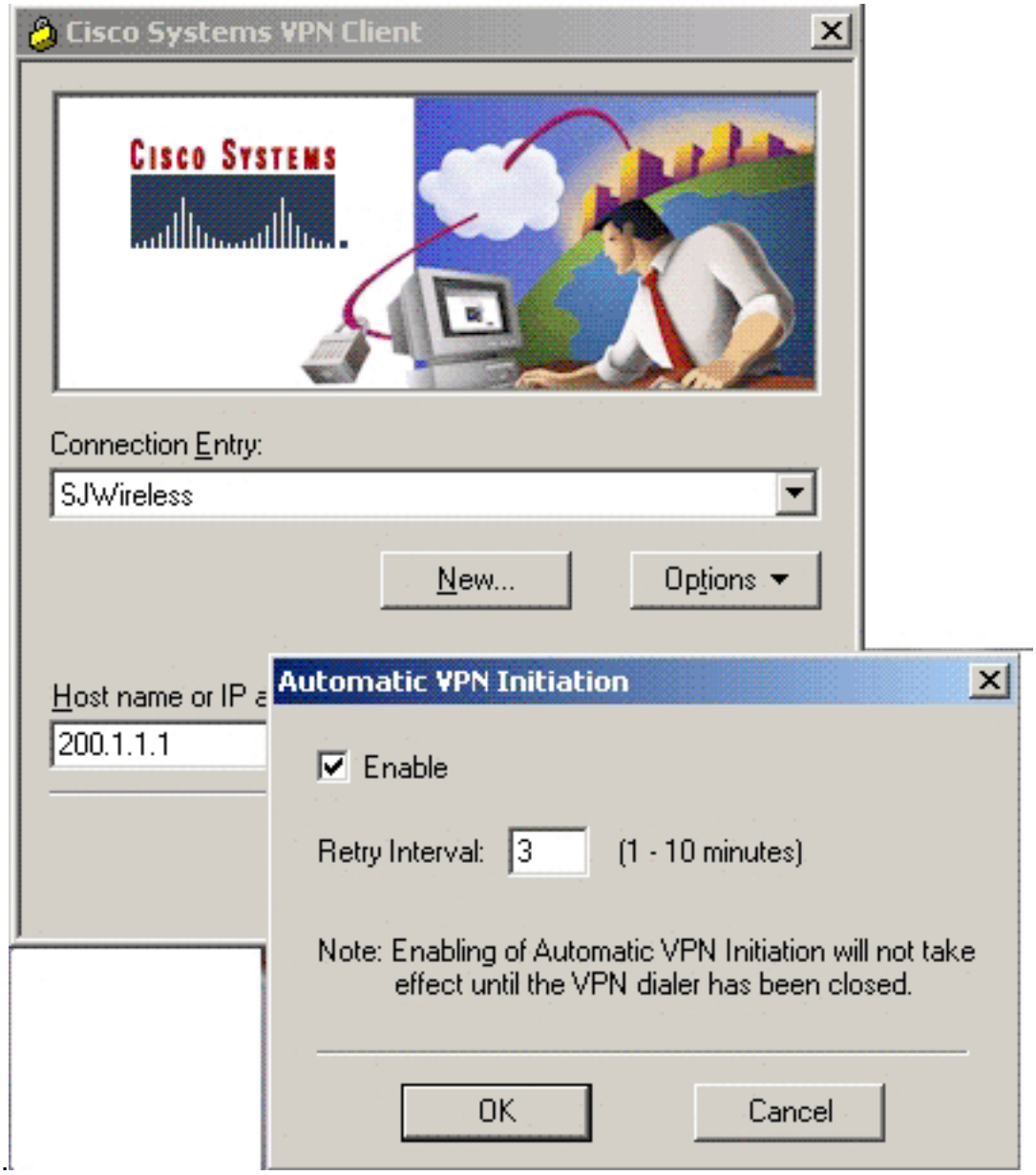
Подтвердите конфигурацию автоматической инициации с устройства набора VPN

Выполните эти шаги для проверки конфигурации автоматического инициирования от программы VPN dialer:

1. Из окна Cisco VPN Dialer на рабочей станции Клиента VPN нажмите **Options** и выберите **Automatic VPN Initiation**.



2. На окне Automatic VPN Initiation проверьте, что проверен флажок Enable. Если это не, проверьте его. Нажмите **OK** для закрытия

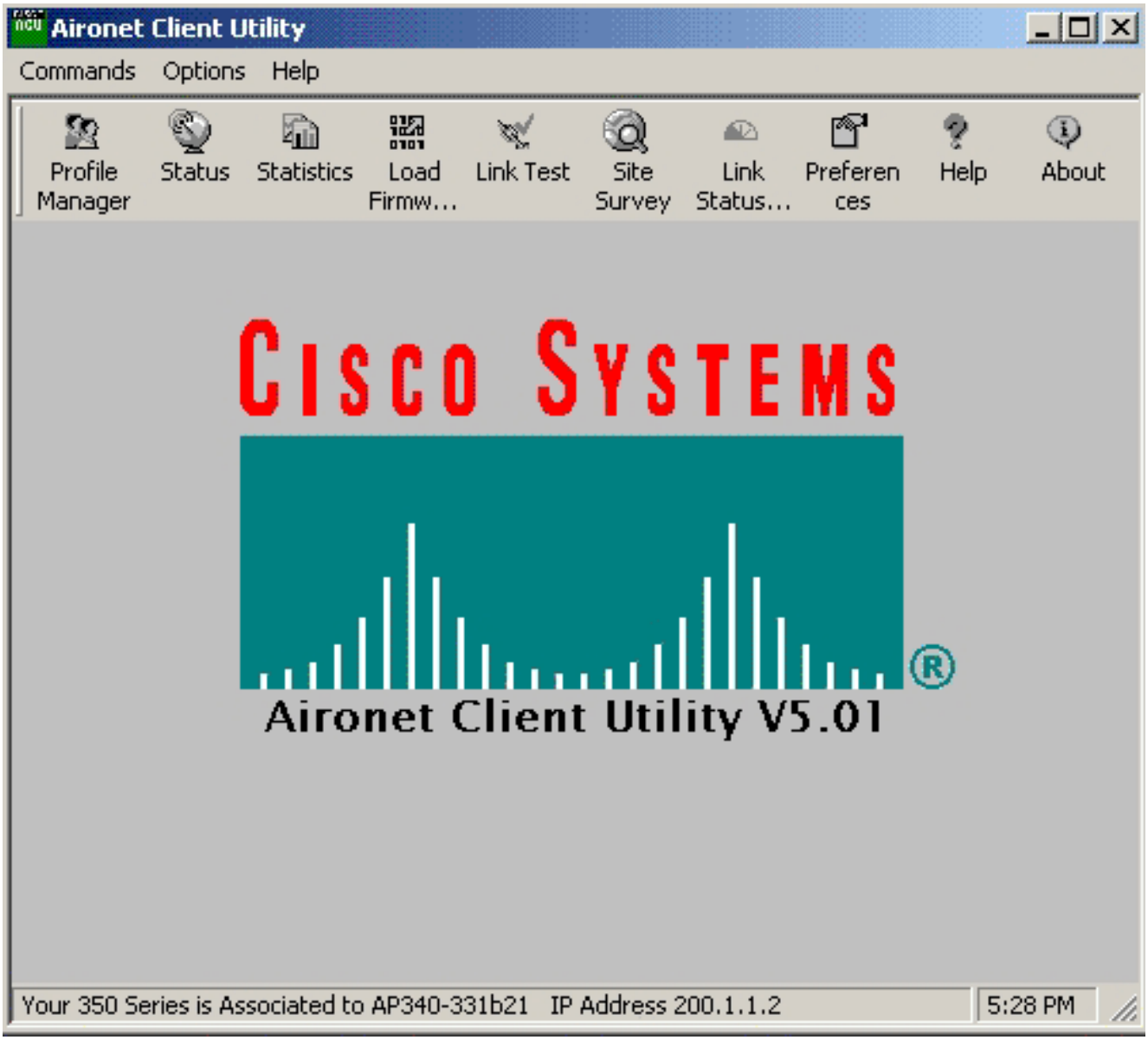


окна.

Проверка функции автоматической инициации в среде беспроводной локальной сети

Выполните эти шаги для проверки функции автоинициации в среде WLAN:

1. Вставьте адаптер беспроводной сети в ПК и ждите ассоциации к беспроводному AP.Для проверки связи с беспроводным устройством запустите программное обеспечение Aironet Client Utility и проверьте нижнюю часть окна Aironet Client. Беспроводной клиент, показанный на рисунке, в состоянии связаться к беспроводному AP, IP-адрес которого
200.1.1.2.



2. Как только связь с беспроводным устройством завершена, Клиент VPN автоматически запускает соединение на основе IP-адреса, полученного от беспроводного соединения. В этом случае беспроводной клиент получает 200.1.1.52 от беспроводного AP, и Клиент VPN запускает Соединение SJWireless на основе конфигурации в vpnclient.ini.Как только VPN-подключение установлено, клиент в состоянии обратиться к сетевым ресурсам при защите IPSEC VPN безопасные сервисы, как

показано.

Проверка журнала событий клиента VPN

Этот раздел показывает, как проверить журнал событий Клиента VPN для проверки той автоинициации доходы должным образом.

Откройте средство просмотра журнала Cisco VPN Client, и вы видите информацию, подобную этому во время автоинициации. Как вы можете видеть Клиент VPN получает 200.1.1.52 IP-адреса от связи с беспроводным устройством, которая попадает в 200.1.1.0/24 список сети, определенный в vpnclient.ini. Клиент VPN тогда запускает соединение SJWireless соответственно. Во время Ike согласование Cisco VPN Client получает IP-адрес 50.1.1.8. Это использует этот IP-адрес в качестве source IP для доступа к внутренней сети позади 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
```

Проверка других состояний автоматической инициации

См. Использование Автоматической информации о носе Инициирования VPN о других состояниях автоинициации.

Дополнительные сведения

- Справочный том концентратора серии VPN 3000 I: !--- конфигурацию
- Страница поддержки концентратора Cisco VPN серии 3000
- Страница поддержки Cisco VPN 3000 Series Client
- Страница поддержки IPSec
- Cisco Systems – техническая поддержка и документация