Пример конфигурации VPN клиента по беспроводной LAN с WLC

Содержание

Введение

Этот документ представляет понятие Виртуальной частной сети (VPN) в Беспроводной среде. Документ объясняет конфигурации, вовлеченные в развертывания VPN-туннеля между беспроводным клиентом и сервером VPN через Контроллер беспроводной локальной сети (WLC).

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Знание WLC и как настроить основные параметры WLC
- Знание понятий Защищенного доступа по протоколу Wi-Fi (WAP)
- Базовые знания о VPN и ее типах
- Знание IPsec

- Базовые знания о доступном шифровании, аутентификации и алгоритмах хеширования

Используемые компоненты

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

- 2006 WLC Cisco, который выполняет версию 4.0.179.8
- Точка доступа облегченных серий Cisco 1000 (LAP)
- Cisco 3640, который выполняет Выпуск 12.4 (8) программного обеспечения Cisco IOS
- Cisco VPN Client версии 4.8

Примечание: Этот документ использует 3640 маршрутизаторов в качестве сервера VPN. Для поддержки большего количества расширенных функций безопасности можно также использовать специализированный сервер VPN.

Примечание: Для маршрутизатора для действия как сервер VPN это должно выполнить набор функций, который поддерживает основной IPsec.

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

VPN является Сетью передачи данных общего пользования, которая используется для безопасной передачи данных в частной сети через общую телекоммуникационную инфраструктуру, такую как Интернет. Эта VPN поддерживает конфиденциальность данных с помощью протокола туннелирования и процедур обеспечения безопасности.

VPN для удаленного доступа

Конфигурация VPN для удаленного доступа используется, чтобы позволить клиентам программного обеспечения VPN, таким как мобильные пользователи надежно обращаться к ресурсам централизованной сети, которые находятся позади сервера VPN. В Терминологии Cisco эти серверы VPN и клиентов также называют сервером Cisco Easy VPN и устройством Cisco Easy VPN remote.

Устройство Cisco Easy VPN remote может быть маршрутизаторами Cisco IOS, Cisco PIX Security Appliance, аппаратными клиентами Cisco VPN 3002 и Cisco VPN Client. Они используются для получения политики безопасности после туннельного соединения VPN от Сервера Cisco Easy VPN. Это минимизирует конфигурационные требования в удаленном местоположении. Cisco VPN Client является клиентским программным обеспечением, которое может быть установлено на PC, портативных ПК, и т.д.

Сервер Cisco Easy VPN может быть маршрутизаторами Cisco IOS, Cisco PIX Security Appliance и Cisco VPN 3000 Concentrator.

Этот документ использует Клиентское программное обеспечение Cisco VPN, которое работает на портативном ПК как на Маршрутизаторе IOS Клиента VPN и Cisco 3640 как сервер VPN. Документ использует стандарт IPsec для установления VPN-туннеля между клиентом и сервером.

IPSec

IPsec является платформой открытых стандартов, разработанных инженерной группой по развитию Интернета (IETF). IPsec предоставляет безопасность для передачи уязвимых данных по незащищенным сетям, таким как Интернет.

IPsec предоставляет шифрование сетевых данных на пакетном уровне IP, который предлагает надежное решение по безопасности, которое является на основе стандартов. Основная задача IPsec должна позволить обмен частной информацией по опасному соединению. IPsec использует шифрование для защиты информации от перехвата или подслушивания. Однако для использования шифрования эффективно обе стороны должны совместно использовать тайну, которая используется и для шифрования и для расшифровки информации.

IPsec работает в двух фазах для разрешения конфиденциального обмена общим секретным ключом:

- Фаза 1 — Обрабатывает согласование параметров безопасности, требуемых установить безопасный канал между двумя узлами IPsec. Фаза 1 обычно внедряется через Протокол IKE. Если удаленный узел IPsec не может выполнить IKE, можно использовать настройку вручную с предварительными общими ключами для завершения Фазы 1.
- Фаза 2 — Использует безопасный туннель, установленный в фазе 1 для обмена параметрами безопасности, требуемыми фактически передать пользовательские данные. Безопасные туннели, используемые в обеих фазах IPsec, основываются на сопоставлениях безопасности (SA), используемые в каждой оконечная точке IPsec. SA описывают параметры безопасности, такие как тип аутентификации и шифрования, которое точки обоих концов соглашаются использовать.

Параметры безопасности, которыми обмениваются в фазе 2, используются для создания Туннеля IPSec, который в свою очередь используется для передачи данных между Клиентом VPN и сервером.

См. IPsec Настройки для получения дополнительной информации о IPsec и его конфигурации.

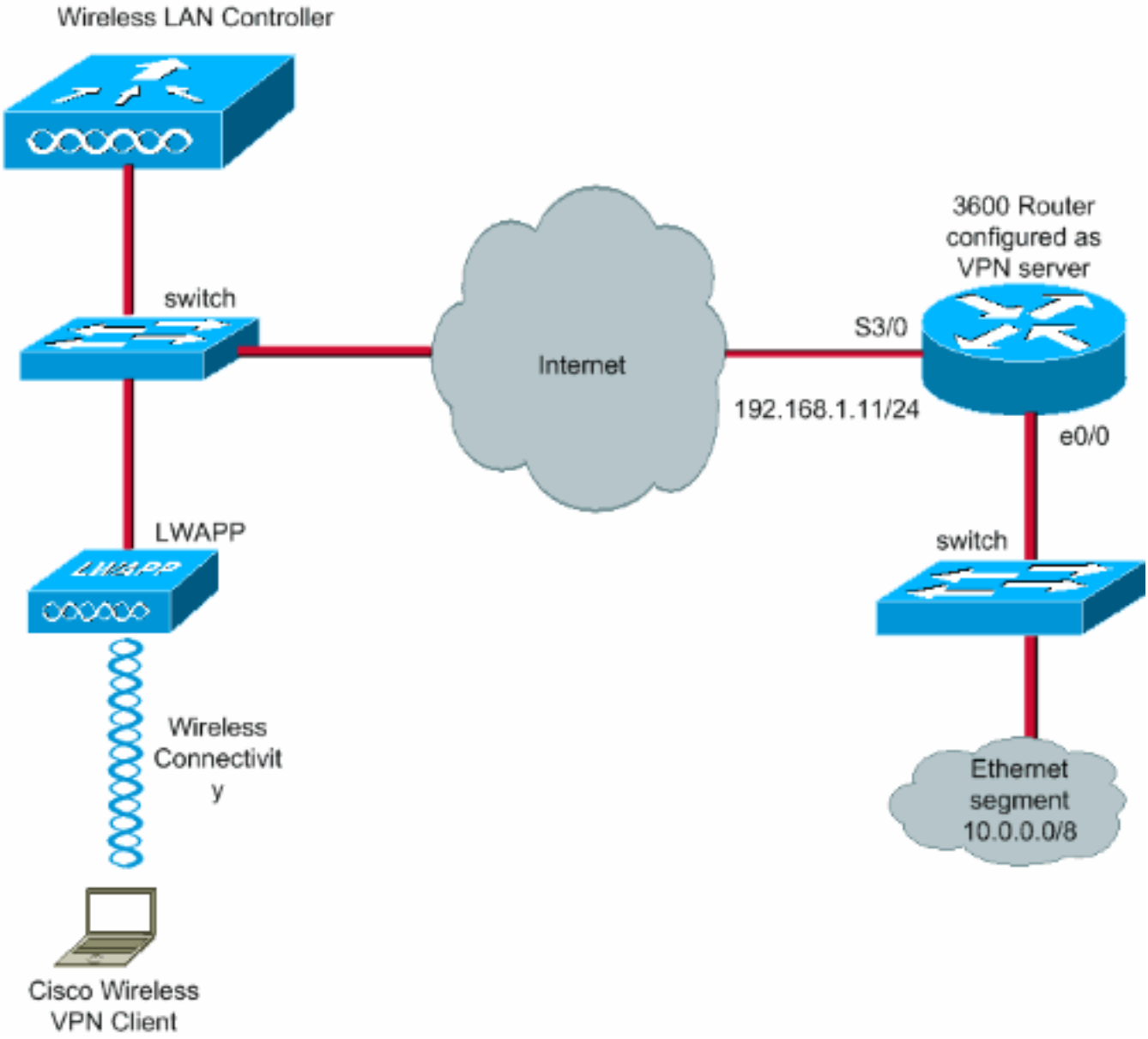
Как только VPN-туннель установлен между Клиентом VPN и сервером, *политика безопасности, определенная в сервере VPN, передается клиенту*. Это минимизирует конфигурационные требования в клиентской стороне.

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

Схема сети

Эти конфигурации используются в данном документе:

- IP-адрес интерфейса управления WLC — 172.16.1.10/16
- IP-адрес интерфейса менеджера точки доступа WLC — 172.16.1.11/16
- Шлюз по умолчанию — 172.16.1.20/16**Примечание:** В действующей сети этот шлюз по умолчанию должен указать к входящему интерфейсу непосредственного маршрутизатора, который подключает WLC с остатком сети и/или с Интернетом.
- IP-адрес сервера VPN s3/0 — 192.168.1.11/24**Примечание:** Этот IP-адрес должен указать к интерфейсу, который завершает VPN-туннель в стороне сервера VPN. В данном примере s3/0 является интерфейсом, который завершает VPN-туннель в сервере VPN.
- Сегмент LAN в сервере VPN использует Диапазон IP-адресов 10.0.0.0/8.



Настройка

В централизованной архитектуре WLAN, чтобы позволить беспроводному Клиенту VPN, такому как портативный ПК устанавливать VPN-туннель с сервером VPN, необходимо, чтобы клиент был привязан к Облегченной точке доступа (LAP), которая в свою очередь должна быть зарегистрирована в WLC. Этот документ имеет LAP, как уже зарегистрировано

в WLC с помощью широковещательного процесса обнаружения локальной подсети, объясненного в регистрации облегченных точек доступа Контроллеру беспроводной локальной сети (WLC).

Следующий шаг должен настроить WLC для VPN.

Завершение VPN и passthrough

С WLC Серии Cisco 4000 ранее, чем версия 4, звонила функция, завершение IPSec VPN (Поддержка IPSec) поддерживается. Эта функция позволяет этим контроллерам завершить сеансы Клиента VPN непосредственно на контроллере. Таким образом, эта функция позволяет самому контроллеру действовать как сервер VPN. Но это требует, чтобы отдельный модуль оборудования завершения VPN был установлен в контроллере.

Эта поддержка IPSec VPN не доступна в:

- Cisco WLC серии 2000
- Любые WLC, которые выполняют версию 4.0 или позже

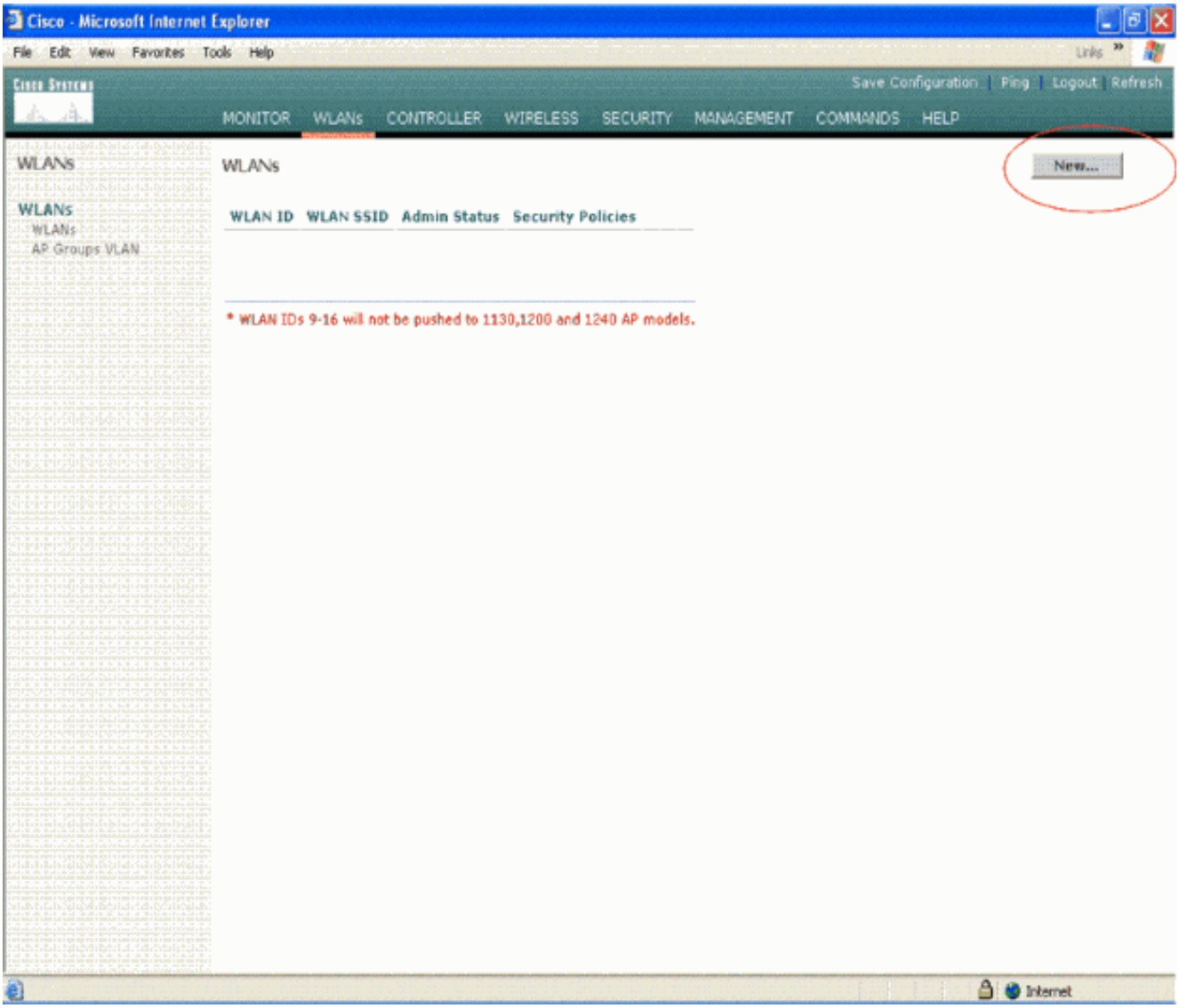
Поэтому единственной функцией VPN, поддерживавшей в версиях позже, чем 4.0, является Passthrough VPN. Эта функция также поддерживается в Cisco WLC серии 2000.

Passthrough VPN является функцией, которая позволяет клиенту устанавливать туннель только с определенным сервером VPN. Так, если необходимо надежно обратиться к настроенному серверу VPN, а также другому серверу VPN или Интернету, это не возможно с Passthrough VPN, включенным на контроллере. В соответствии с такими требованиями, необходимо отключить Passthrough VPN. Когда соответствующий ACL создан и применен к соответствующий WLAN, Однако WLC может быть настроен для действия как passthrough для достижения множественных Шлюзов VPN. Так, согласно таким сценариям, где вы хотите достигнуть множественных Шлюзов VPN для резервирования, отключите passthrough VPN и создайте ACL, который предоставляет доступ к Шлюзам VPN, и примените ACL к WLAN.

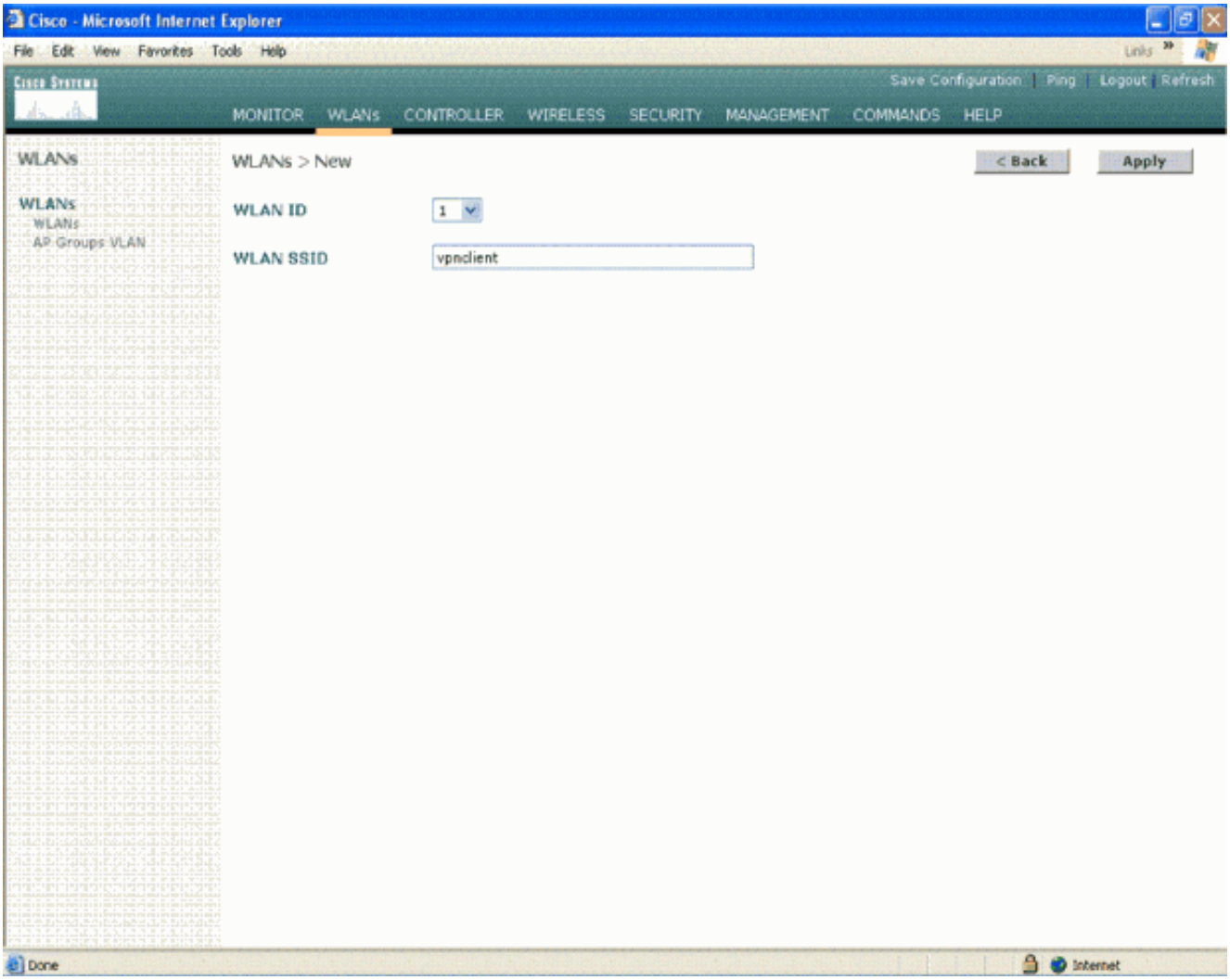
Настройте WLC для passthrough VPN

Выполните эти шаги для настройки Passthrough VPN.

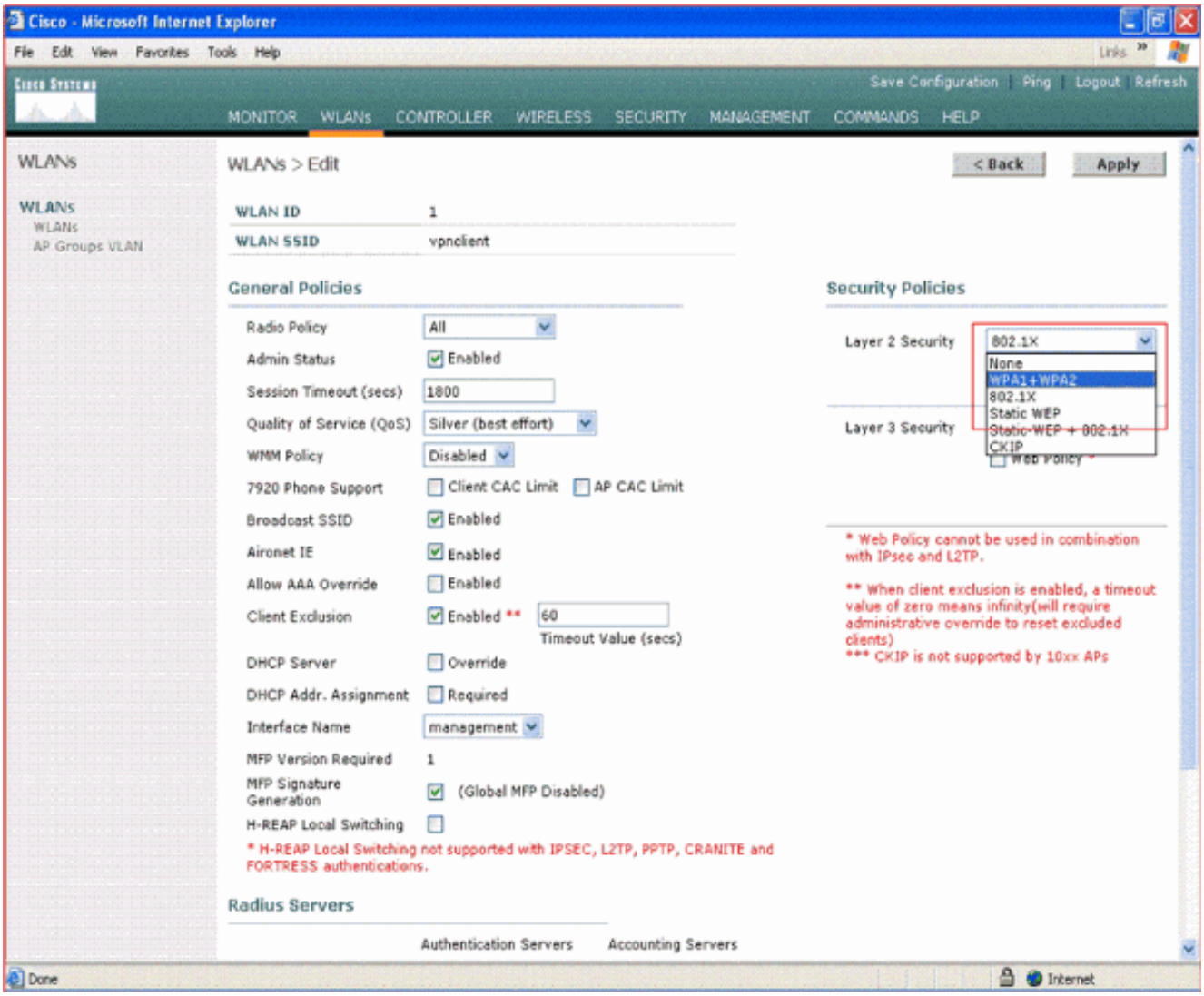
1. От GUI WLC нажмите **WLAN**, чтобы перейти к странице WLANs.
2. Нажмите **New** для создания нового WLAN.



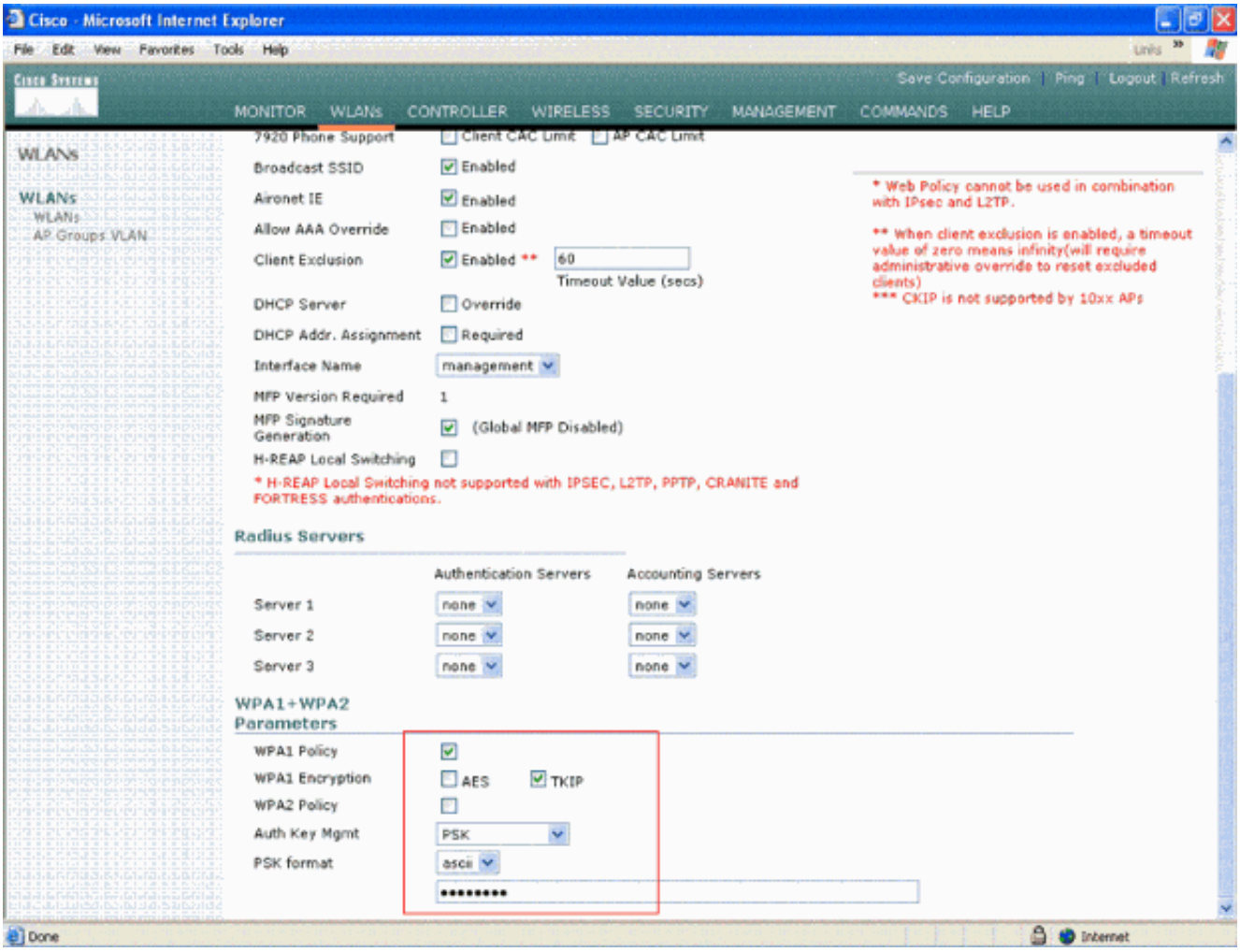
3. SSID WLAN называют как **vpnclient** в данном примере. **Щелкните "Применить".**



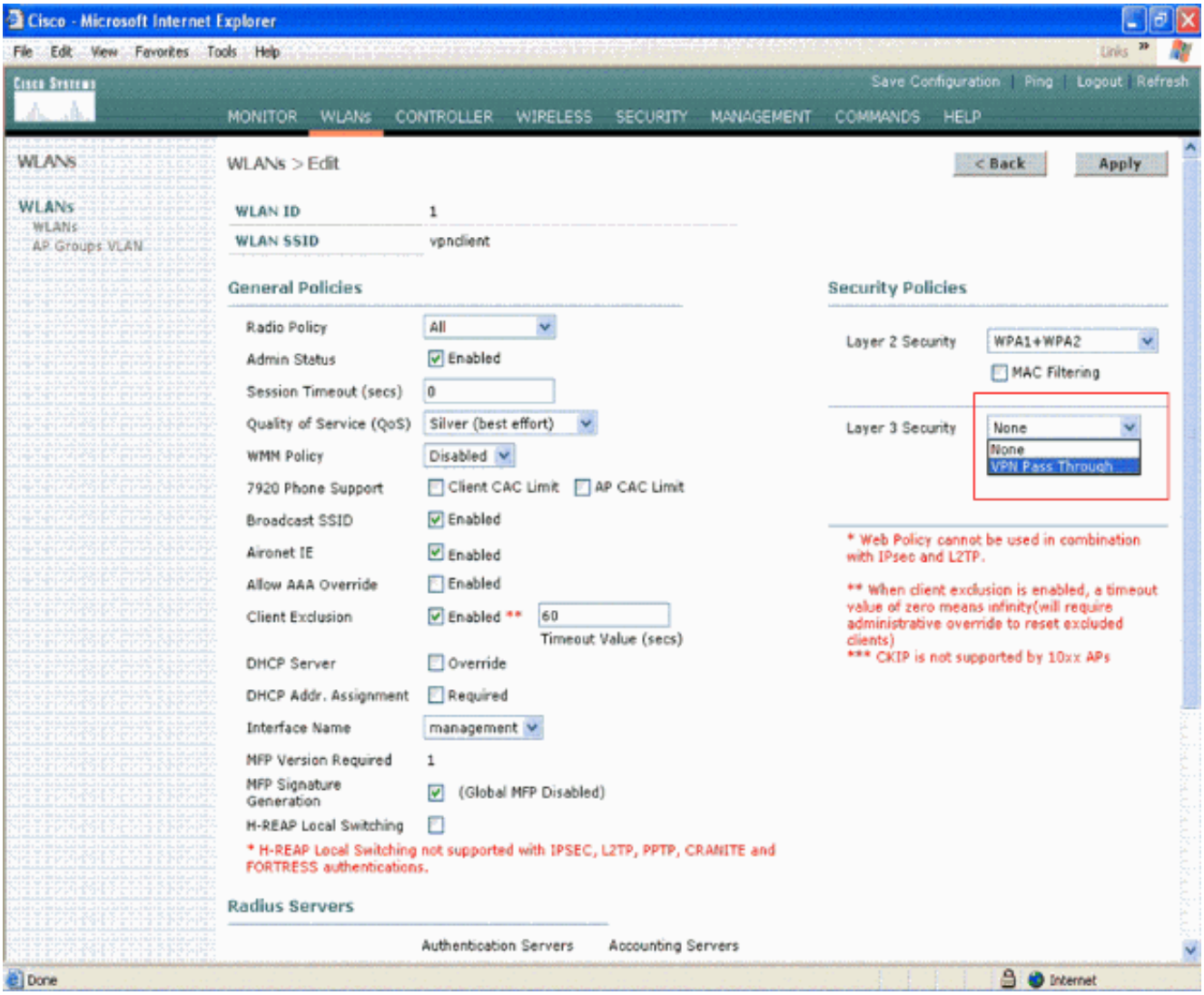
4. Настройте vpnclient SSID с безопасностью уровня 2. *!--- Следующее необязательно.*Данный пример использует **WPA1+WPA2** в качестве типа безопасности.



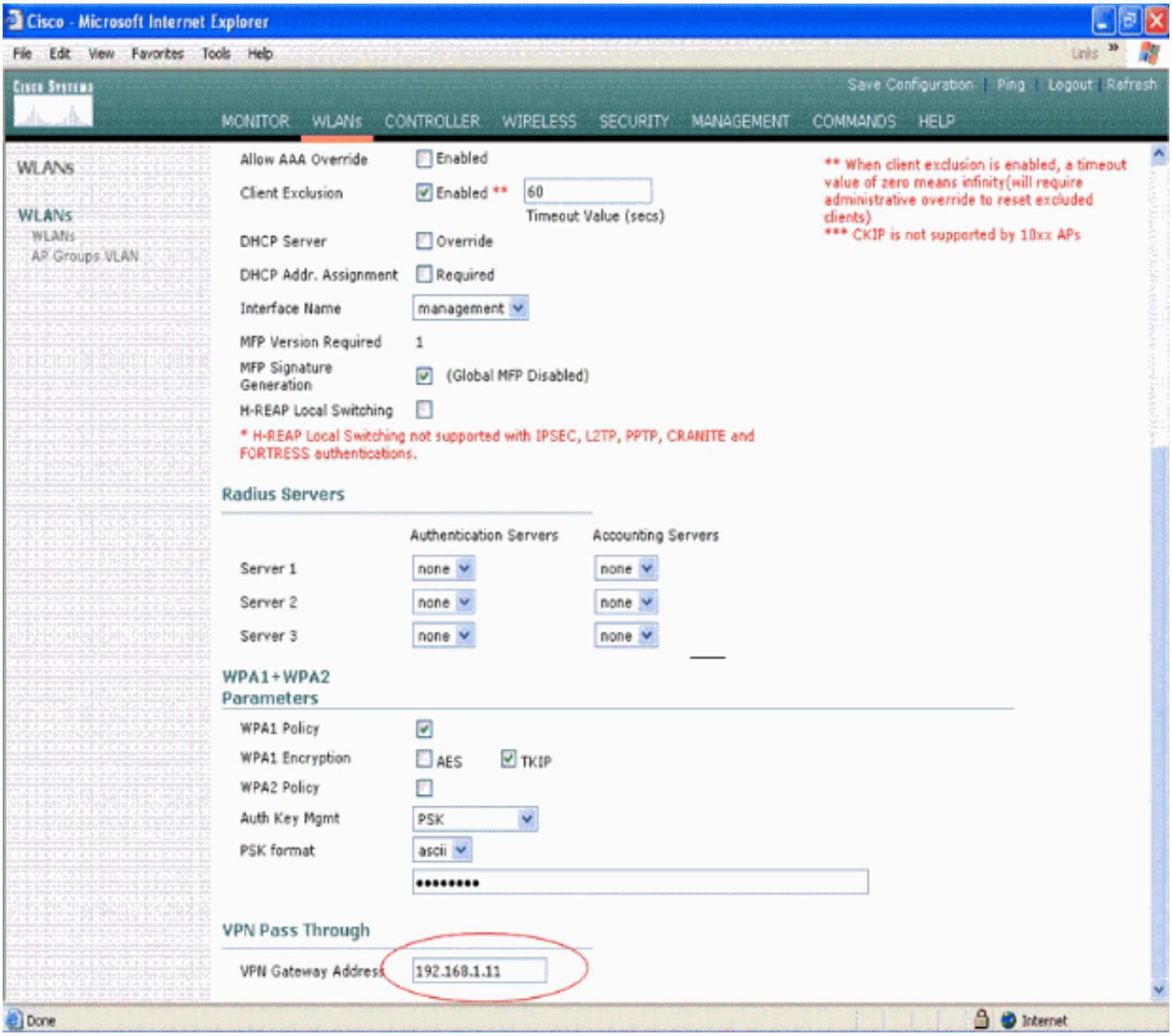
5. Настройте политику WPA и тип управления Ключа проверки подлинности, который будет использоваться.Данный пример использует **Предварительный общий ключ (PSK)** для управления ключа проверки подлинности. Как только PSK выбран, выберите **ASCII** как формат PSK и введите значение PSK. Это значение должно быть тем же в конфигурации SSID беспроводного клиента для клиентов, которые принадлежат этому SSID для соединения с этим
WLAN.



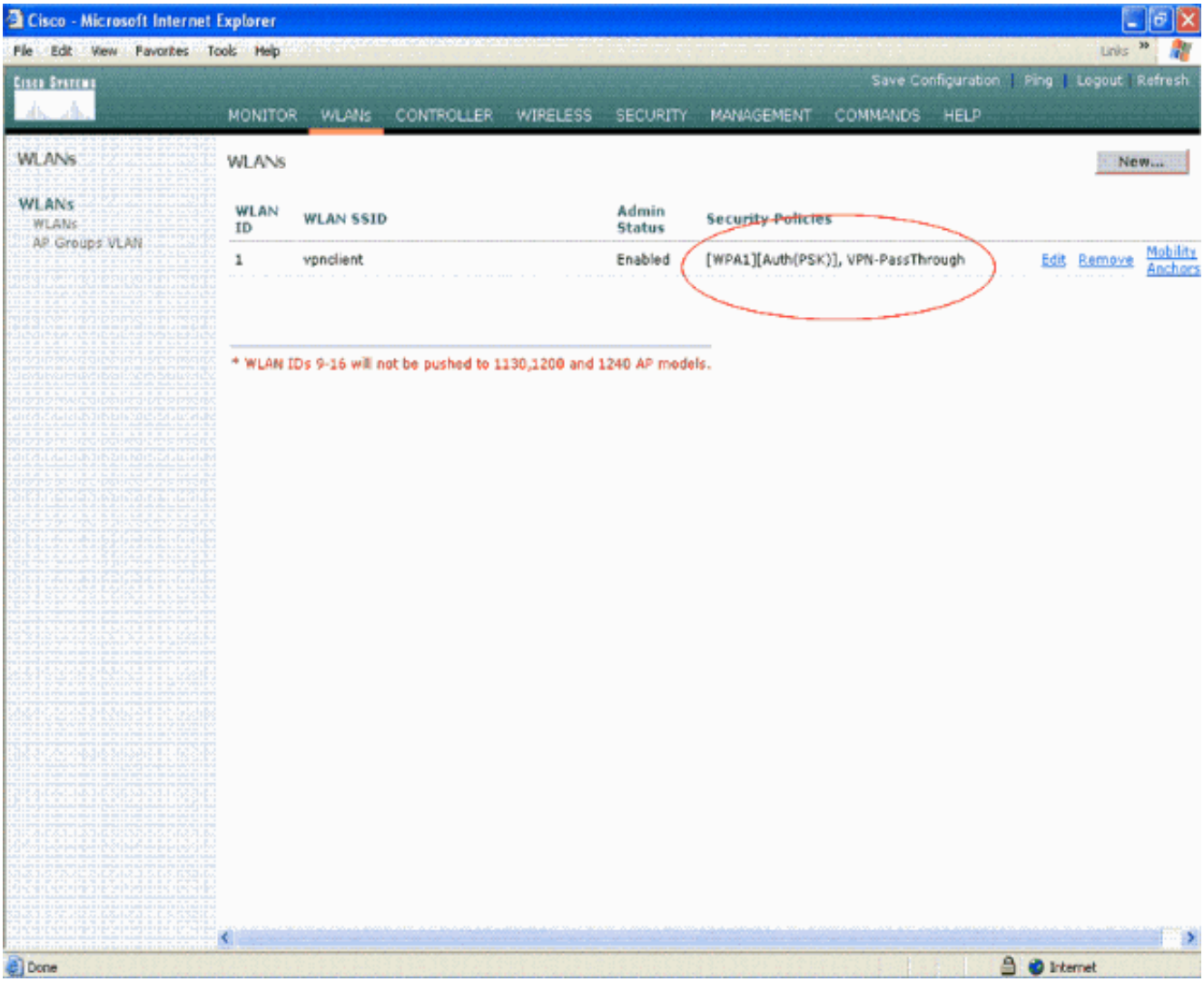
6. Выберите **VPN Pass-through** как безопасность уровня 3. Ниже представлен пример.



7. Как только Passthrough VPN выбран как безопасность уровня 3, добавьте Адрес Шлюза VPN как показано в примере.Этим адресом шлюза должен быть IP-адрес интерфейса, который завершает VPN-туннель в стороне сервера. В данном примере IP-адрес интерфейса s3/0 (192.168.1.11/24) в сервере VPN является адресом шлюза, который будет
настроен.



8. **Щелкните "Применить".** WLAN, названный *vpnclient*, теперь настроен для Passthrough VPN.



Конфигурация сервера VPN

Эта конфигурация показывает Маршрутизатор Cisco 3640 как сервер VPN.

Примечание: Для простоты эта конфигурация использует статичную маршрутизацию для поддержания возможностей IP - доступов между оконечная точками. Можно использовать любой протокол динамической маршрутизации, такой как Протокол RIP, Протокол OSPF, и т.д для поддержания достижимости.

Примечание: Если нет никаких возможностей IP - доступов между клиентом и сервером, туннель не установлен.

Примечание: Этот документ предполагает, что пользователь знает, как включить динамическую маршрутизацию в сети.

Маршрутизатор Cisco 3640
vpnrouter#**show running-config** Building configuration... Current configuration : 1623 bytes ! version 12.4 service timestamps debug datetime msec service timestamps log datetime msec no service password-encryption ! hostname vpnrouter ! boot-start-marker boot-end-marker ! ! **aaa new-model** ! ! **aaa authorization network *employee* local** ! aaa session-id common ! resource policy ! memory-size iomem 10 ! ! ip cef no ip domain lookup ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! ! **crypto**

```
isakmp policy 1 !--- Create an Internet Security
Association and Key Management !--- Protocol (ISAKMP)
policy for Phase 1 negotiation. hash md5 !--- Choose the
hash algorithm to be md5. authentication pre-share !---
The authentication method selected is pre-shared. group
2 !--- With the group command, you can declare what size
modulus to !--- use for Diffie-Hellman calculation.
Group 1 is 768 bits long, !--- and group 2 is 1024 bits
long. crypto isakmp client configuration group employee
key cisco123 pool mypool ! !--- Create the Phase 2
policy for actual data encryption. crypto ipsec
transform-set myset esp-3des esp-md5-hmac !--- Create a
dynamic map and apply the transform set that was
created. !--- Set reverse-route for the VPN server.
crypto dynamic-map mymap 10 set transform-set myset
reverse-route ! crypto map clientmap isakmp
authorization list employee !--- Create the crypto map.
crypto map clientmap client configuration address crypto
map clientmap 10 ipsec-isakmp dynamic mymap ! !--- Apply
the employee group list that was created earlier. ! ! !
! interface Ethernet0/0 ip address 10.0.0.20 255.0.0.0
half-duplex ! interface Serial3/0 ip address
192.168.1.11 255.255.255.0 clock rate 64000 no fair-
queue crypto map clientmap !--- Apply the crypto map to
the interface. ! interface Serial3/1 no ip address
shutdown ! interface Serial3/2 no ip address shutdown !
interface Serial3/3 no ip address shutdown ! interface
Serial3/4 no ip address shutdown ! interface Serial3/5
no ip address shutdown ! interface Serial3/6 no ip
address shutdown ! interface Serial3/7 no ip address
shutdown ip local pool mypool 10.0.0.50 10.0.0.60 !---
Configure the Dynamic Host Configuration Protocol !---
(DHCP) pool which assigns the tunnel !--- IP address to
the wireless client. !--- This tunnel IP address is
different from the IP address !--- assigned locally at
the wireless client (either statically or dynamically).
ip http server no ip http secure-server ! ip route
172.16.0.0 255.255.0.0 192.168.1.10 ! ! ! ! control-
plane ! ! ! ! ! ! ! ! ! line con 0 line aux 0 line vty
0 4 ! ! end ip subnet-zero . . . ! end
```

Примечание: Данный пример использует только групповую аутентификацию. Это не использует проверку подлинности отдельного пользователя.

Конфигурация клиента VPN

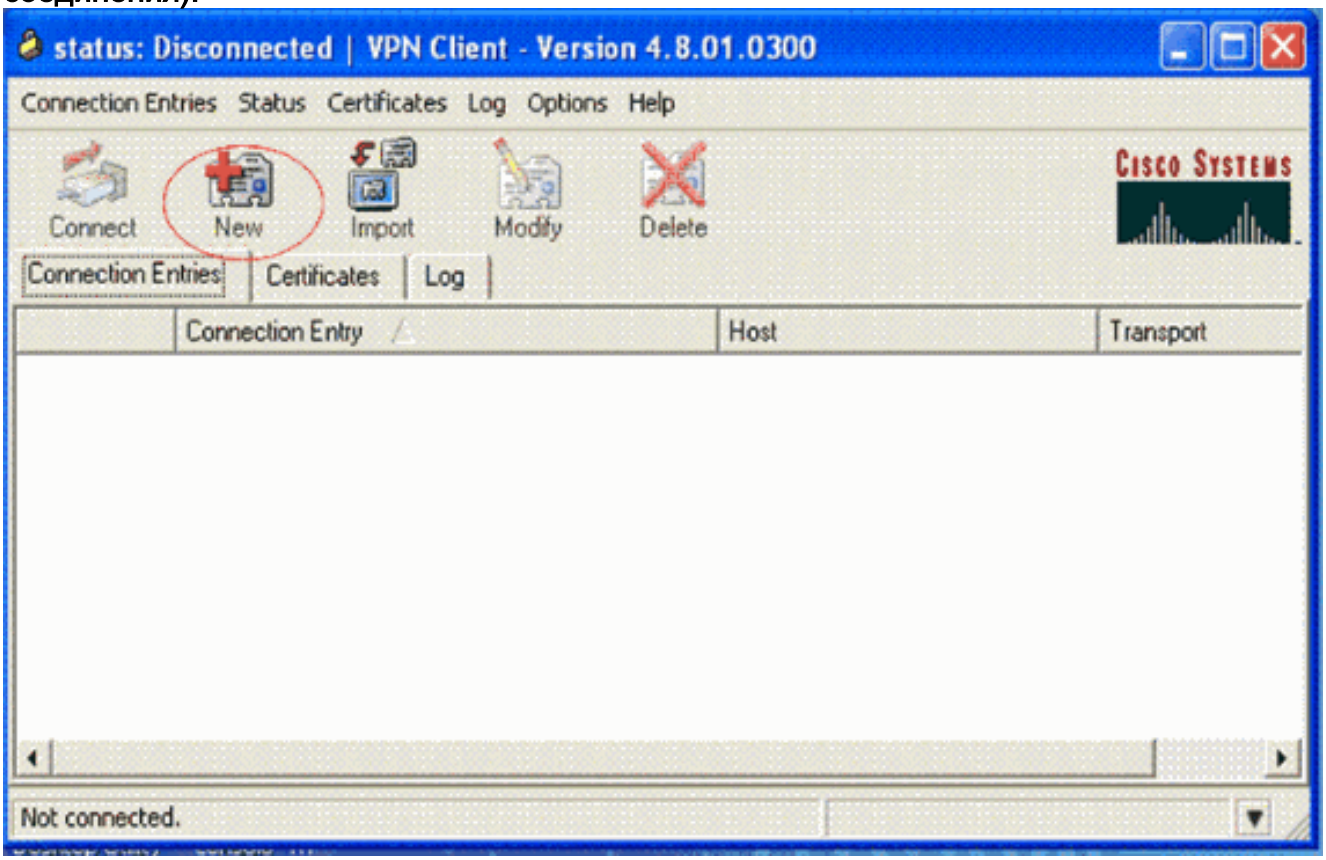
Программное обеспечение VPN Client может быть загружено от Центра Программного обеспечения cisco.com.

Примечание: Некоторое Программное обеспечение Cisco требует, чтобы вы вошли с именем пользователя и паролем CCO.

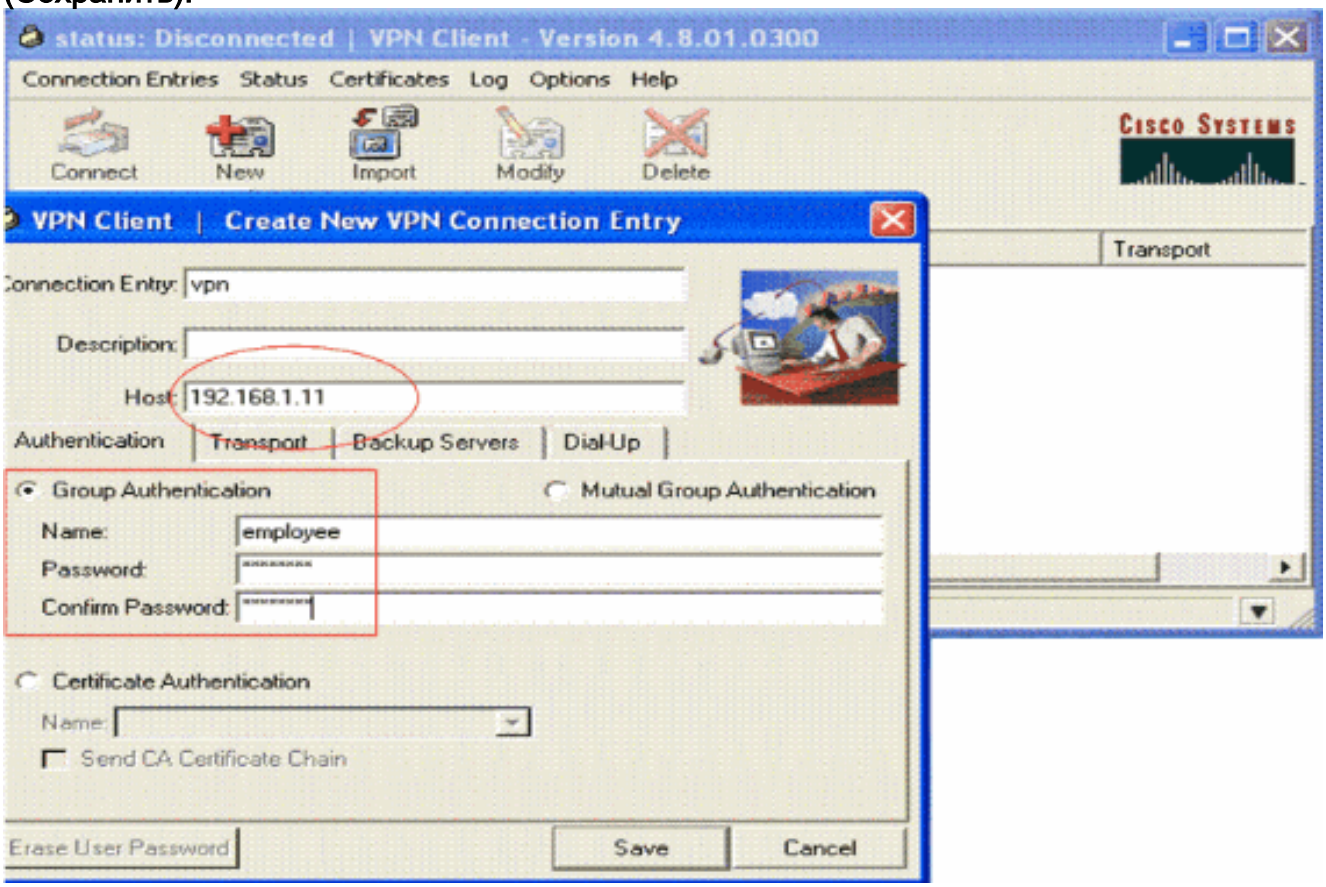
Выполните эти шаги, чтобы настроить VPN-клиент.

1. Сформируйте своего беспроводного клиента (портативный ПК), выберите **Start> Programs> Cisco Systems VPN Client> VPN Client** для доступа к Клиенту VPN. Это - расположение по умолчанию, где установлен Клиент VPN.
2. **Нажмите New, чтобы открыть окно "Create New VPN Connection Entry" (Создание новой**

записи VPN-
соединения).



3. Введите имя записи и описание подключения. Данный пример *usesvpn*.Поле описания является дополнительным. Введите IP-адрес сервера VPN в коробке Хоста. **Затем введите имя группы VPN и нажмите кнопку Save (Сохранить).**



Примечание: Имя группы и Пароль, настроенный здесь, должны совпасть с тем,

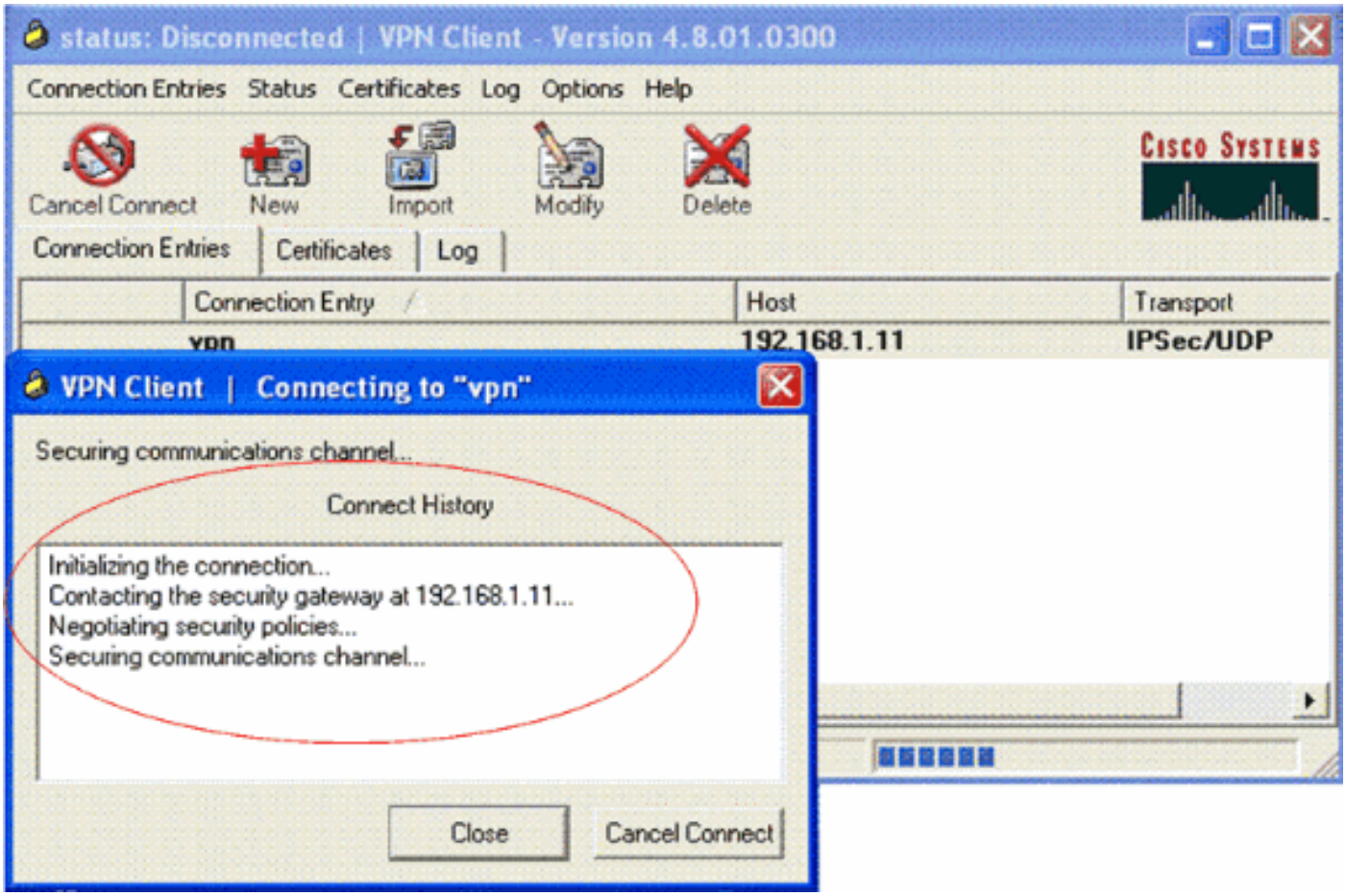
настроенным в сервере VPN. Данный пример использует *сотрудника* Названия и *Пароль cisco123.*

Проверка

Для проверки этой конфигурации настройте SSID **vpnclient** в беспроводном клиенте с теми же параметрами безопасности, настроенными в WLC, и привяжите клиента к этому WLAN. Существует несколько документов, которые объясняют, как настроить беспроводного клиента с новым профилем.

Как только беспроводной клиент привязан, перейдите к Клиенту VPN и щелкните по соединению, которое вы настроили. Затем нажмите **Connect** от главного окна VPN Client.

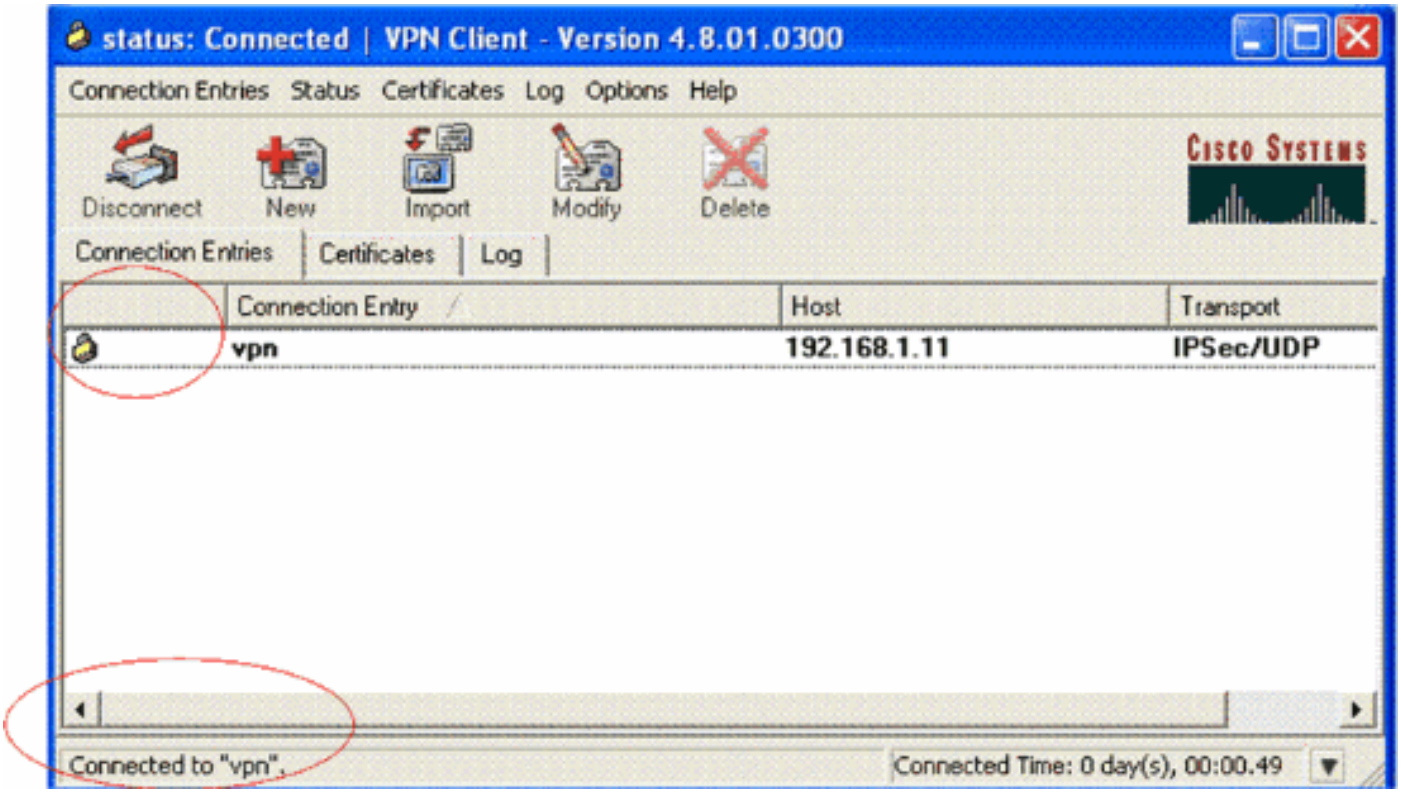
Вы видите параметры безопасности Фазы 1 и Фазы 2, о которых выполняют согласование между клиентом и сервером.



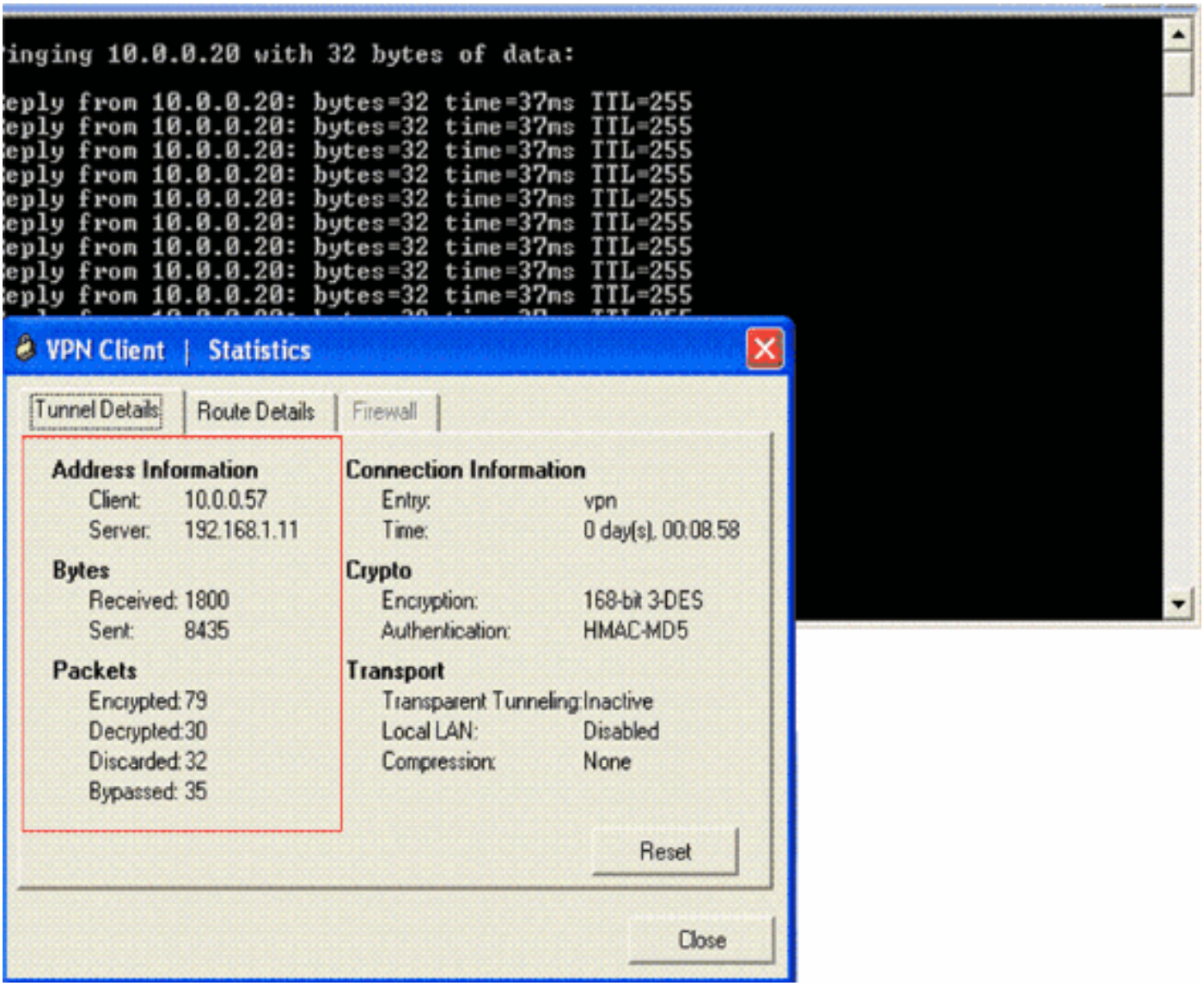
Примечание: Для установления этого VPN-туннеля у Клиента VPN и сервера должны быть возможности IP - доступы между ними. Если Клиент VPN не в состоянии связаться со шлюзом безопасности (сервер VPN), то туннель не установлен, и окно с предупреждением отображено в клиентской стороне с этим сообщением:

```
Reason 412: The remote peer is no longer responding
```

Чтобы гарантировать, что VPN-туннель должным образом установлен между клиентом и сервером, можно найти значок блокировки, который создан рядом с установленным Клиентом VPN. Строка состояния также указывает **Связанный к "vpn"**. Например.



Кроме того, гарантируйте, что вы в состоянии успешно передать данные к сегменту LAN в стороне сервера от Клиента VPN и наоборот. Из главного меню Клиента VPN выберите **Status> Statistics**. Там можно найти статистику зашифрованных и расшифрованных пакетов, которые передают через туннель.



В этом снимке экрана вы видите адрес клиента как 10.0.0.57. Это - адрес, что сервер VPN назначает на клиента от локально настроенный пул после успешного согласования Фазы 1. Как только туннель установлен, сервер VPN автоматически добавляет маршрут к этому назначенному IP-адресу DHCP в его таблице маршрутизации.

В то время как данные переданы от клиента серверу и количеству расшифрованных пакетов, увеличивающихся во время обратной передачи данных, можно также видеть количество увеличения зашифрованных пакетов.

Примечание: Так как WLC настроен для Passthrough VPN, он позволяет клиенту обращаться только к сегменту, связанному со Шлюзом VPN (здесь, это - 192.168.1.11 сервера VPN), настроенный для Passthrough. Это фильтрует весь другой трафик.

Можно проверить это путем настройки другого сервера VPN с одинаковой конфигурацией и настроить запись нового соединения для этого сервера VPN в Клиенте VPN. Теперь, когда вы пытаетесь установить туннель с этим сервером VPN, это не успешно. Это вызвано тем, что WLC фильтрует этот трафик и позволяет туннель только адресу Шлюза VPN, настроенному для Passthrough VPN.

Можно также проверить конфигурацию от CLI сервера VPN.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает

определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Эти **команды показа**, используемые в сервере VPN, могли бы также быть полезными, чтобы помочь вам проверять статус туннеля.

- **Команда show crypto session** используется для проверки статуса туннеля. Вот пример выходных данных этой команды.`Crypto session current status`

  ```
  Interface: Serial3/0
  Session status: UP-ACTIVE Peer: 172.16.1.20 port 500 IKE SA: local 192.168.1.11/500 remote
  172.16.1.20/500 Active IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.0.0.58 Active SAs: 2,
  origin: dynamic crypto map
  ```
- **Show crypto isakmp policy** используется для просмотра настроенных параметров Фазы 1.

Устранение неполадок

Команды debug и show, объясненные в Сверять разделе, могут также использоваться для устранения проблем.

- **debug crypto isakmp**
- **debug crypto ipsec**
- **show crypto session**

- **Команда debug crypto isakmp** в сервере VPN отображает весь процесс согласования Фазы 1 между клиентом и сервером. Вот пример успешного согласования Фазы 1.-------
  ```
  ------------------------------------------------------------
   ------------------------------------------------------------
  ------------------------------------------------------------
  *Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):Checking ISAKMP transform 14 against priority 1
  policy *Aug 28 10:37:29.515: ISAKMP: encryption DES-CBC *Aug 28 10:37:29.515: ISAKMP: hash
  MD5 *Aug 28 10:37:29.515: ISAKMP: default group 2 *Aug 28 10:37:29.515: ISAKMP: auth pre-
  share *Aug 28 10:37:29.515: ISAKMP: life type in seconds *Aug 28 10:37:29.515: ISAKMP: life
  duration (VPI) of 0x0 0x20 0xC4 0x9B *Aug 28 10:37:29.515: ISAKMP:(0:0:N/A:0):atts are
  acceptable. Next payload is 0 *Aug 28 *Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):SA
  authentication status: authenticated *Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1): Process
  initial contact, bring down existing phase 1 and 2 SA's with local 192.168.1.11 remote
  172.16.1.20 remote port 500 *Aug 28 10:37:29.955: ISAKMP:(0:15:SW:1):returning IP addr to
  the address pool: 10.0.0.57 *Aug 28 10:37:29.955: ISAKMP (0:134217743): returning address
  10.0.0.57 to pool *Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):received initial contact,
  deleting SA *Aug 28 10:37:29.959: ISAKMP:(0:14:SW:1):peer does not do pade 1583442981 to
  QM_IDLE *Aug 28 10:37:29.963: ISAKMP:(0:15:SW:1):Sending NOTIFY RESPONDER_LIFETIME protocol
  1 spi 1689265296, message ID = 1583442981 *Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1): sending
  packet to 172.16.1.20 my_port 500 peer_port 500 (R) QM_IDLE *Aug 28 10:37:29.967:
  ISAKMP:(0:15:SW:1):purging node 1583442981 *Aug 28 10:37:29.967: ISAKMP: Sending phase 1
  responder lifetime 86400 *Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Input =
  IKE_MESG_FROM_PEER, IKE_AM_EXCH *Aug 28 10:37:29.967: ISAKMP:(0:15:SW:1):Old State =
  IKE_R_AM2 New State = IKE_P1_COMPLETE
  ```
- **Команда debug crypto ipsec** в сервере VPN отображает успешное согласование IPsec Фазы 1 и создание VPN-туннеля. Например:----------
  ```
  ------------------------
   ------------------------------------------------------------------
  ------------------------------------------------------------------------
  ```

```
*Aug 28 10:40:04.267: IPSEC(key_engine): got a queue event with 1 kei messages
*Aug 28 10:40:04.271: IPSEC(spi_response): getting spi 2235082775 for SA
from 192.168.1.11 to 172.16.1.20 for prot 3
*Aug 28 10:40:04.279: IPSEC(key_engine): got a queue event with 2 kei messages
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) INBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0x8538A817(2235082775), conn_id= 0, keysize= 0, flags= 0x2
*Aug 28 10:40:04.279: IPSEC(initialize_sas): ,
  (key eng. msg.) OUTBOUND local= 192.168.1.11, remote= 172.16.1.20,
    local_proxy= 0.0.0.0/0.0.0.0/0/0 (type=4),
    remote_proxy= 10.0.0.58/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac  (Tunnel),
    lifedur= 2147483s and 0kb,
    spi= 0xFFC80936(4291299638), conn_id= 0, keysize= 0, flags= 0xA
```

***Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Event create routes for peer or rekeying for peer 172.16.1.20** *Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Refcount 1 Serial3/0 ***Aug 28 10:40:04.283: IPSEC(rte_mgr): VPN Route Added 10.0.0.58 255.255.255.255 via 172.16.1.20 in IP DEFAULT TABLE with tag 0** *Aug 28 10:40:04.283: IPSec: Flow_switching Allocated flow for sibling 8000001F *Aug 28 10:40:04.283: IPSEC(policy_db_add_ident): src 0.0.0.0, dest 10.0.0.58, dest_port 0 *Aug 28 10:40:04.287: IPSEC(create_sa): sa created, (sa) sa_dest= 192.168.1.11, sa_proto= 50, sa_spi= 0x8538A817(2235082775), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2002 ***Aug 28 10:40:04.287: IPSEC(create_sa): sa created, (sa) sa_dest= 172.16.1.20, sa_proto= 50, sa_spi= 0xFFC80936(4291299638), sa_trans= esp-3des esp-md5-hmac , sa_conn_id= 2001**

Дополнительные сведения

- Введение в шифрование IPSec
- Страница поддержки IPsec Negotiation/IKE
- Настройка параметров сетевой безопасности IPSec Network Security
- Вопросы и ответы Cisco Easy VPN
- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 4.0
- Пример конфигурации ACL на контроллере беспроводных LAN
- Часто задаваемые вопросы по контроллеру беспроводной LAN (WLC)
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация