Вопросы и ответы по VPN-клиенту Cisco

Вопросы

Введение

В этом документе содержатся ответы на часто задаваемые вопросы о VPN-клиенте Cisco.

Note: Соглашения по именованию для различных VPN-клиентов:

- Cisco Secure VPN Client только версий от 1.0 до 1.1a
- Cisco VPN 3000 Client только версий 2.x
- Cisco VPN Client только версий 3.x и выше

Более подробную информацию о применяемых в документе обозначениях см. в документе Cisco Technical Tips Conventions (Условные обозначения, используемые в технической документации Cisco).

Загрузка программного обеспечения VPN-клиента

Q. Где можно загрузить программное обеспечение VPN-клиента?

A. Для доступа к программному обеспечению VPN-клиента **необходимо** зарегистрироваться в системе, обладая действующим контрактом на обслуживание. Программное обеспечение VPN-клиента можно загрузить из Центра программного обеспечения (registered customers only) . **Без действующего контракта, связанного с соответствующим профилем Cisco.com, нельзя зарегистрироваться в системе и загрузить программное обеспечение VPN-клиента.**

Выполните следующие действия, чтобы получить действующий контракт на обслуживание.

- При наличии прямого соглашения о покупке свяжитесь с соответствующей группой Cisco по связям с клиентами.
- Обратитесь к партнеру Cisco или продавцу продуктов Cisco, чтобы приобрести соглашение об обслуживании.
- Используйте диспетчер профилей (registered customers only) , чтобы обновить свой профиль Cisco.com и запросить связь с

соглашением об обслуживании.

Q. Область загрузки VPN-клиента пуста. Почему?

A. Перед переходом к области VPN-клиента Центра программного обеспечения (registered customers only) необходимо в средней части страницы выбрать область загрузки для нужной операционной системы.

Q. Как отключить динамический брандмауэр во время установки VPN-клиента?

A. Для ознакомления с темами "Использование MSI для установки VPN-клиента Windows без брандмауэра с отслеживанием состояния соединений" и "Использование InstallShield для установки VPN-клиента Windows без брандмауэра с отслеживанием состояния соединений" см. раздел Изменения документации документа Заметки о выпуске Cisco VPN Client 4.7.

Операционная система

Q. Предоставляет ли Cisco VPN-клиент для Windows Vista?

A. На момент написания документа (июнь 2007 г.) VPN-клиент версии 5 доступен для 32-разрядной версии Windows Vista. 64-разрядная версия Windows Vista в настоящее время не поддерживается. Данный клиент и заметки о выпуске можно получить из Центра программного обеспечения (registered customers only) .

Note: Без действующего контракта, связанного с соответствующим профилем Cisco.com, нельзя зарегистрироваться в системе и загрузить программное обеспечение VPN-клиента. Дополнительные сведения см. в разделе Загрузка программного обеспечения VPN-клиента.

Tip: В настоящее время VPN-клиент Cisco AnyConnect доступен для операционных систем Windows, включая 32- и 64-разрядные версии Vista. Клиент AnyConnect поддерживает SSL и DTLS. В настоящее время он не поддерживает IPSec. Кроме того, клиент AnyConnect можно использовать только с устройством адаптивной защиты Cisco, на котором выполняется программное обеспечение версии 8.0(2) или выше. Данный клиент также можно использовать в режиме веб-запуска с устройствами IOS версии 12.4(15)T. VPN 3000 не поддерживается.

VPN-клиент Cisco AnyConnect и ASA 8.0 можно получить из Центра программного обеспечения (registered customers only) . См. в документе Заметки о выпуске VPN-клиента Cisco AnyConnect дополнительную информацию о клиенте AnyConnect. Дополнительные сведения об ASA 8.0 см. в документе Заметки о выпуске устройства адаптивной защиты Cisco ASA серии 5500.

Note: Без действующего контракта, связанного с соответствующим профилем Cisco.com, нельзя зарегистрироваться в системе и загрузить программное обеспечение VPN-клиента AnyConnect или ASA. Дополнительные сведения см. в разделе Загрузка программного обеспечения VPN-клиента.

Q. Как установить PPTP-соединение на компьютере под управлением ОС Microsoft Windows?

A. Это зависит от версии используемой операционной системы Microsoft Windows. За конкретной информацией следует обратиться в корпорацию Майкрософт. Ниже приводятся инструкции по установке соединения для некоторых распространенных версий Windows.

A. Windows 95

1. Установите Msdun13.exe.
2. Выберите **Программы > Стандартные > Удаленный доступ > Сеть**.
3. Создайте новое подключение под названием "PPTP".
4. В качестве устройства для подключения выберите **адаптер VPN**.
5. Введите IP-адрес общедоступного интерфейса коммутатора и нажмите кнопку **Готово**.
6. Вернитесь к только что созданному подключению, щелкните правой кнопкой мыши и выберите пункт **Свойства**.
7. В разделе "Разрешенные сетевые протоколы" снимите флажок **NetBEUI**.
8. Настройте параметры в окне **Дополнительные параметры**:
    1. Оставьте настройки по умолчанию, чтобы разрешить коммутатору и клиенту автоматически согласовывать способ проверки подлинности.
    2. Установите флажок **Требовать шифрованный пароль**, чтобы принудительно использовать проверку подлинности протокола CHAP.
    3. Установите флажки **Требовать шифрованный пароль** и **Требовать шифрования данных**, чтобы принудительно использовать проверку подлинности MS-CHAP.

A. Windows 98

1. Выполните следующие действия для установки компонента PPTP.
    1. Выберите **Пуск > Параметры > Панель управления > Установить новое оборудование**. Нажмите кнопку **Далее**.
    2. Щелкните **Выбрать из списка** и выберите **Сетевой адаптер**. Нажмите кнопку **Далее**.
    3. В панели слева выберите **Microsoft**, а справа - **Адаптер Microsoft VPN**.
2. Чтобы настроить компонент PPTP, выполните следующие действия.
    1. Выберите **Пуск > Программы > Стандартные > Связь > Удаленный доступ к сети**.
    2. Щелкните **Создать новое подключение** и в списке **Выбор устройства** выберите **Адаптер Microsoft VPN**. IP-адрес VPN-сервера = конечная точка туннеля 3000.
3. Выполните следующие действия по изменению ПК, чтобы также разрешить использование протокола проверки пароля (PAP).
   Note: Проверка подлинности по умолчанию Windows 98 заключается в шифровании пароля (протокол CHAP или MS-CHAP).

    1. Выберите **Свойства> Типы серверов**.
    2. Снимите флажок **Требовать шифрованный пароль**. В этой области можно настроить шифрование данных (с помощью шифрования MPPE или без него).

A. Windows 2000

1. Выберите **Пуск > Программы > Стандартные > Связь >Сеть и удаленные соединения**.
2. Щелкните **Создать новое подключение** и нажмите кнопку **Далее**.
3. Установите флажок **Подключаться к частной сети через Интернет, устанавливая соединение заранее** (не устанавливается при наличии ЛВС). Щелкните **Далее**.
4. Введите имя узла или IP-адрес конечной точки туннеля (3000).
5. Если требуется изменить тип пароля, выберите **Свойства > Защита подключения > Дополнительно**. По умолчанию используется MS-CHAP и MS-CHAP версии 2 (а не CHAP или PAP). В этой области можно настроить шифрование данных (с помощью MPPE или без).

A. Windows NT

См. документ Установка, настройка и использование PPTP клиентами и серверами Microsoft .

Q. В каких версиях операционной системы поддерживается VPN-клиент Cisco?

A. Для данного VPN-клиента постоянно увеличивается число поддерживаемых операционных систем. Требования к системе см. в заметках о выпуске последней версии клиента или в документе Оборудование Cisco и VPN-клиенты, поддерживающие IPsec/PPTP/L2TP.

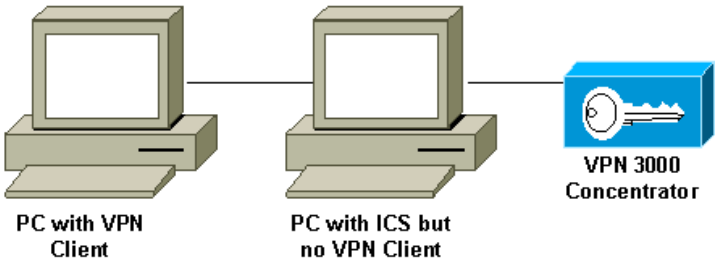
Q. Требуется ли быть администратором на компьютере Windows NT/2000, чтобы загрузить VPN-клиент?

A. Да, для установки VPN-клиента в Windows NT и Windows 2000 нужны права администратора, так как с их использованием выполняется привязка к существующим сетевым драйверам или установка новых сетевых драйверов. VPN-клиент представляет собой программное обеспечение для работы с сетью. Для его установки требуются права администратора.

Q. Может ли VPN-клиент Cisco работать с компонентом Microsoft общего Интернет-подключения (ICS), установленным на том же компьютере?

A. Нет, клиент Cisco VPN 3000 Client не совместим с компонентом Microsoft ICS на одном компьютере. Перед установкой данного VPN-клиента компонент ICS требуется удалить. Дополнительные сведения см. в документе Отключение ICS при подготовке к установке или обновлению Cisco VPN Client 3.5.x в Microsoft Windows XP.

Хотя данный VPN-клиент и ICS не могут совместно работать на одном ПК, следующая комбинация поможет решить эту проблему.



Q. Создается впечатление, что VPN-клиент подключается только к определенным адресам. Используется Windows XP. Какие действия следует предпринять?

A. Убедитесь, что встроенный брандмауэр Windows XP отключен.

Q. Совместим ли VPN-клиент Cisco с динамическим брандмауэром ОС Windows XP?

A. Данная проблема была решена. Дополнительные сведения см. в описании ошибки Cisco с идентификатором CSCdx15865 (registered customers only) в средстве обнаружения ошибок.

Q. Отключается ли многопользовательский интерфейс при установке VPN-клиента в Windows XP или Windows 2000?

A. При установке отключается экран приветствия и быстрое переключение пользователей. Дополнительные сведения см. в описании ошибки Cisco с идентификатором CSCdu24073 (registered customers only) в средстве обнаружения ошибок.

Q. Как заставить VPN-клиент для Linux переходить в фоновый режим после выполнения? При вызове подключения, например, vpnclient connect foo, вход выполняется, но оболочка возвращается.

A. После регистрации введите следующие комбинации.

- **^Z**
- **bg**

Q. После установки VPN-клиента Cisco в Windows XP Home Edition пропала панель задач. Как вернуть отображение панели?

A. Выберите **Панель управления> Сетевые подключения > Удалить сетевой мост**, чтобы отрегулировать данную настройку.

Q. При попытке установки VPN-клиента для Linux в RedHat 8.0 выдается сообщение об ошибке, в котором говорится, что не удается загрузить модуль, так как он скомпилирован с помощью GCC 2, а ядро скомпилировано с помощью GCC 3.2. Какие действия следует предпринять?

A. Причина в том, что в новом выпуске RedHat используется новая версия компилятора GCC (3.2+), что вызывает сбой текущего VPN-клиента Cisco. Эта проблема исправлена в VPN-клиенте Cisco версии 3.6.2a. См. дополнительные сведения в описании ошибки Cisco с идентификатором CSCdy49082 (registered customers only) в средстве обнаружения ошибок или загрузите данное программное обеспечение из Центра программного обеспечения VPN (registered customers only) .

Q. Почему после установки VPN-клиента версии 3.1 в Windows XP отключается функция быстрого переключения пользователей?

A. Функция быстрого переключения пользователей автоматически отключается в Windows XP, когда в реестре указывается файл GINA.dll. VPN-клиент устанавливает CSgina.dll для реализации возможности "Start Before Login" (Запуск до входа в систему). Если требуется быстрое переключение пользователей, отключите функцию "Start Before Login". Зарегистрированные пользователи могут получить дополнительные сведения в описании ошибки Cisco с идентификатором CSCdu24073 (registered customers only) в средстве обнаружения ошибок.

Сообщения об ошибках

Q. При установке VPN-клиента версии 4.x появляется следующее сообщение об ошибке: "Предупреждение 201. Требуемая подсистема VPN недоступна. Подключение к удаленному VPN-серверу невозможно."

A. Эта проблема может возникать из-за брандмауэра, установленного на компьютере VPN-клиента. Чтобы избежать появления этого сообщения об ошибке, убедитесь, что во время установки брандмауэр или антивирусная программа не установлены или не выполняются на ПК.

Q. После обновления до Mac OS X 10.3 (Panther) VPN-клиент версии 4.x выдает следующее сообщение об ошибке: "Безопасное VPN-подключение разорвано клиентом локально по следующей причине: Не удается связаться с шлюзом безопасности".

A. Необходимо добавить UseLegacyIKEPort=0 к профилю (PCF-файл), найденному в каталоге /etc/CiscoSystemsVPNClient/Profiles/, чтобы VPN-клиент версии 4.x мог работать в Mac OS X 10.3 ("Партнер").

Q. Что означает появление сообщения "Сообщение об ошибке: не удается найти файл удаления программы..." при попытке установки VPN-клиента? А также, что необходимо сделать, чтобы успешно завершить удаление программного обеспечения?

A. Проверьте сетевую панель управления, чтобы убедиться, что компонент DNE (Deterministic NDIS Extender) не установлен. Также откройте **Microsoft > Текущая версия > Удалить**, чтобы убедиться в наличии файла удаления программы. Удалите файл **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{5624C000-B109-11D4-9DB4-00E0290FCAC5}** и повторите операцию отмены установки программы.

Q. Не удается установить VPN-клиент в Windows 2000 Professional. Выдается следующее сообщение об ошибке: "Не удалось установить файл поддержки установки" Глобальный сбой. Какие действия следует предпринять?

A. Удалите раздел **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall**. Затем перезагрузите компьютер и заново установите VPN-клиент.

Note: Чтобы найти правильный раздел реестра для VPN-клиента Cisco в ветке HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\<раздел, который требуется определить>, перейдите к ветке HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\ и выберите **VPN Client**. В правом окне должно отображаться Uninstall Path (в столбце "Имя"). В соответствующем столбце "Значение" отображается значение параметра "VPN Client". Взяв данный параметр в качестве ссылки, необходимо перейти к ветке HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\. Затем выберите определенный параметр и удалите его.

Дополнительные сведения см. в статье Initialization Error Troubleshooting (Устранение ошибок инициализации) и сообщении об ошибке Cisco с идентификатором CSCdv15391 (registered customers only) в средстве обнаружения ошибок.

Q. При попытке установки VPN-клиента для Linux в RedHat 8.0 выдается сообщение об ошибке, в котором

говорится, что не удается загрузить модуль, так как он скомпилирован с помощью GCC 2, а ядро скомпилировано с помощью GCC 3.2. Какие действия следует предпринять?

A. Причина в том, что в новом выпуске RedHat используется новая версия компилятора GCC (3.2+), что вызывает сбой текущего VPN-клиента Cisco. Эта проблема исправлена в VPN-клиенте Cisco версии 3.6.2a. Дополнительные сведения см. в описании ошибки Cisco с идентификатором CSCdy49082 (registered customers only) в средстве обнаружения ошибок или загрузите это программное обеспечение из Центра программного обеспечения VPN (registered customers only) .

Q. При попытке Linux Client 3.5 установить IPSec-подключение к PIX или к концентратору VPN 3000 выдается сообщение об ошибке "равноправный узел не отвечает". Какие действия следует предпринять?

A. Симптомом этой проблемы является то, что клиент для Linux пытается подключиться, но не получает ответа от устройства шлюза.

В Linux OS есть встроенный брандмауэр (ipchains), который блокирует UDP-порт 500, UDP-порт 1000 и пакеты ESP (Encapsulating Security Payload). Поскольку брандмауэр по умолчанию включен, то для решения проблемы придется либо отключить его, либо открыть порты для передачи данных по протоколу IPSec как для входящих, так и для исходящих подключений.

Q. Выдается сообщение об ошибке расширения ядра при попытке запуска клиента Cisco VPN 5000 5.2.2 в Mac OS X 10.3. Какие действия следует предпринять?

A. Как указывается в заметках о выпуске продукта, клиент Cisco VPN 5000 поддерживается в ОС версий не выше 10.1.x, т.е. он не поддерживается в версии 10.3. Данный VPN-клиент можно заставить работать, если сбросить разрешения на два установленных файла после выполнения сценария установки. Ниже рассмотрен пример.

Note: Эта конфигурация *не* поддерживается продуктами Cisco.

```
sudo chown -R root:wheel /System/Library/Extensions/VPN5000.kext
sudo chmod -R go-w /System/Library/Extensions/VPN5000.kext
```

Q. Не удается установить новую версию VPN-клиента. Во время установки выдается сообщение об ошибке "Ошибка выполнения DNEinst при установке DNE, код возврата -2146500093" или "Ошибка InstallDNE: ошибка выполнения DNEinst при установке DNE, код возврата -2147024891". Это происходит при установке компонента Deterministic Network Enhancer.

A. Установите последнее обновление DNE с веб-узла Deterministic Networks .

Совместимость со сторонними продуктами

Q. Совместим ли клиент Nortel с концентраторами Cisco VPN 3000?

A. Нет. Клиент Nortel не может подключаться к концентратору Cisco VPN 3000.

Q. Можно ли устанавливать VPN-клиенты других производителей, например, VPN-клиент Nortel Contivity, одновременно с VPN-клиентом Cisco?

A. Нет. Известно много проблем, возникающих при установке на одном ПК нескольких VPN-клиентов.

Q. Поддерживаются ли VPN-клиенты Cisco VPN-концентраторами сторонних производителей?

A. VPN-клиенты Cisco не поддерживаются VPN-концентраторами сторонних производителей.

Проверка подлинности

Q. Как VPN-клиенты версий 1.1 и 3.x внутренне хранят цифровые сертификаты (X.509v3)?

A. У VPN-клиента версии 1.1 имеется собственное хранилище сертификатов. Клиент VPN Client 3.x может хранить сертификаты либо в хранилище Microsoft с помощью интерфейса CAPI, либо в собственном хранилище Cisco (безопасность данных RSA)

Q. Можно ли использовать одинаковые имя группы и имя пользователя в VPN-концентраторе?

A. Нет, имя группы и имя пользователя не могут быть одинаковыми. Это известная проблема, обнаруженная в программном обеспечении версий 2.5.2 и 3.0 и перенесенная в версию 3.1.2. Дополнительные сведения см. в описании ошибки Cisco с идентификатором CSCdw29034 (registered customers only) в средстве обнаружения ошибок.

Q. Поддерживает ли VPN-клиент Cisco для PIX полнофункциональные платы, такие как Defender?

A. Нет, платы данного типа не поддерживаются.

Версия программного обеспечения VPN-клиента

Q. Почему отсутствует функция "Set MTU Utility" (Утилита настройки MTU), доступная в VPN-клиенте версии 2.5.2 и более ранних?

A. В VPN-клиенте выполняется настройка максимального размера передаваемого блока данных (MTU). Функция Set MTU Utility больше не требуется при установке и была удалена из меню "Пуск". Воспользуйтесь обозревателем Internet Explorer, чтобы получить доступ к функции Set MTU Utility. Также можно выбрать **Пуск > Выполнить**, нажать кнопку **Обзор** и перейти в каталог Cisco Systems VPN Client.

Q. Какие персональные брандмауэры поддерживаются VPN-клиентом Cisco?

A. См. раздел "Требования к системе" в заметках о выпуске используемого VPN-клиента, чтобы узнать о проблемах взаимодействия или поддержке персональных брандмауэров. Начиная с версии 3.1, в концентратор VPN 3000 добавлена новая функция, которая обнаруживает, какие удаленные пользователи персонального брандмауэра установлены, и препятствует подключению этих пользователей при отсутствии соответствующего программного обеспечения. Чтобы настроить эту функцию, выберите **Configuration > User Management > Groups > Client FW** (Конфигурация > Управление пользователями > Группы > Брандмауэр клиента), а затем перейдите на вкладку требуемой группы.

Q. Возникают ли проблемы подключения при использовании клиента VPN Client 3.x с AOL 7.0?

A. VPN-клиент не работает с AOL 7.0 без использования раздельного туннелирования. Дополнительные сведения см. в описании ошибки Cisco с идентификатором CSCdx04842 (registered customers only) в средстве обнаружения ошибок.

Настройка программного обеспечения VPN-клиента

Q. Почему VPN-клиент отключается через 30 минут? Как увеличить этот промежуток времени?

A. Система разрывает пользовательское соединение, если оно не используется в течение 30 минут. По умолчанию тайм-аут простоя равен 30 минутам, его минимально допустимое значение равно 1 минуте, а максимальное значение равно 2 147 483 647 минутам (более 4 000 лет).

Выберите **Configuration > User Management > Groups > Groups** (Конфигурация > Управление пользователями > Группы), а затем — имя соответствующей группы, чтобы изменить значение тайм-аута простоя. Выберите команду **Изменить группу**, перейдите на вкладку "HW Client" (Аппаратный клиент) и укажите требуемое значение в поле "User Idle Timeout" (Пользовательский тайм-аут простоя). Введите **0**, чтобы отключить завершение по тайм-ауту и разрешить неограниченный период простоя.

Q. Можно ли развернуть VPN-клиент Cisco со всеми предварительно настроенными параметрами?

A. Да. Администраторы могу создавать загрузочные дискеты VPN-клиента Cisco, на которых заранее настроены все параметры конфигурации клиента, что позволяет выполнять полную установку без вмешательства конечных пользователей. Информация о создании предварительно настроенной конфигурации содержится в документации по VPN-клиенту Cisco.

Q. Вероятно, VPN-клиент конфликтует с сетевой интерфейсной платой. Как устранить эту неполадку?

A. Убедитесь, что для используемой сетевой интерфейсной платы установлены драйвера последней версии. Это универсальная рекомендация. Если возможно, выполните тесты, чтобы выяснить, характерна ли данная проблема для используемой операционной системы, оборудования ПК или для других сетевых интерфейсных плат.

Q. Как автоматизировать подключение VPN-клиента из программы удаленного доступа к сети?

A. Выберите **Параметры> Свойства > Подключения** и в VPN-клиенте раскройте запись телефонной книги "Удаленный доступ к сети", чтобы полностью автоматизировать установку VPN-подключения.

Q. Как настроить концентратор Cisco VPN 3000 на уведомление удаленных пользователей об обновлении VPN-клиента?

A. См. Уведомление удаленных пользователей об обновлении клиента. Убедитесь, что сведения о версии введены как "(Rel)", см. шаг 6 данного процесса.

Q. Что может вызвать задержку открытия VPN-клиента, особенно когда установлен флажок "Start Before Logon" (Запуск перед входом)?

A. VPN-клиент функционирует в "аварийном" режиме. Этим обусловлена задержка. Отмените установку VPN-клиента и удалите проблемные приложения, чтобы разрешить запуск клиента без перехода в "аварийный" режим. После этого переустановите VPN-клиент.

Дополнительные сведения см. в описании ошибок Cisco с идентификаторами CSCdt88922 (registered customers only) и CSCdt55739 (registered customers only) в средстве обнаружения ошибок.

Q. Требуется понять разницу между ipsecdialer.exe и vpngui.exe. Почему программа vpngui.exe установлена в папке STARTUP операционной системы Windows XP, но все равно приходится вручную запускать ipsecdialer, чтобы получить доступ к ресурсам компании? Кроме того, (помимо размера) эти программы, похоже, инициируют одно и то же действие — VPN-вход в сеть компании.

A. Программа ipsecdialer.exe была первоначальным механизмом запуска VPN-клиентов 3.x. После изменения графического

интерфейса пользователя в версиях 4.x был создан новый исполняемый файл vpngui.exe. Файл ipsecdialer.exe сохранил имя только для обратной совместимости и просто запускает файл vpngui.exe. Это причина видимой разницы в размерах файлов.

Поэтому при понижении версии VPN-клиента от 4.x к 3.x для запуска программы нужен файл ipsecdialer.exe.

Q. Можно ли без последствий удалить значок запуска VPN-клиента в папке автозагрузки? Зачем он нужен?

A. VPN-клиент в папке автозагрузки поддерживает функцию "Start Before Logon" (Запуск перед входом). Если эта функция не используется, то значок можно удалить из папки автозапуска.

Q. Почему добавляется запись "user_logon", но не к ярлыку программы ipsecdialer.exe? Каково назначение "user_logon"?

A. "user_logon" требуется для функции "Start Before Logon", но при обычном запуске VPN-клиента пользователем она не нужна.

Проблемы NAT/PAT

Q. При подключении через устройство преобразования адресов портов (PAT) возникают проблемы только с одним клиентом VPN (версии 3.3 и более ранних). Что можно сделать, чтобы снизить остроту этой проблемы?

A. В некоторых реализациях преобразования сетевых адресов (NAT)или PAT содержалась ошибка, из-за которой порты с номерами менее 1024 не преобразовывались. В VPN-клиентах версии 3.1 даже при включенной прозрачности NAT в сеансе ISAKMP (Internet Security Association and Key Management Protocol) используется UDP 512. Пакеты первого VPN-клиента проходят через устройство PAT, а на выходе сохраняется исходный порт 512. При подключении второго VPN-клиента порт 512 уже используется. Попытка завершается неуспешно.

Существует три возможных способа решения проблемы.

- Исправьте устройство PAT.
- Обновите версию VPN-клиента до 3.4 и используйте TCP-инкапсуляцию.
- Установите клиент VPN 3002, который заменяет все VPN-клиенты.

Q. Можно ли два расположенных рядом портативных компьютера соединить с помощью VPN-клиента?

A. Два расположенных рядом клиента можно подключить к одному головному узлу, так как оба клиента не находятся за устройством, выполняющим преобразование адресов портов (PAT), таким как маршрутизатор или брандмауэр для малого или домашнего офиса. Многие PAT-устройства могут сопоставлять ОДНО VPN-подключение расположенному за ними клиенту, но не двум. Чтобы разрешить соединение двух VPN-клиентов, расположенных рядом за PAT-устройством, включите на головном узле такой тип инкапсуляции, как NAT-T, IPSec через UDP или IPSec через TCP. Обычно NAT-T или другую инкапсуляцию следует включать, если между клиентом и головным узлом находится ЛЮБОЕ NAT-устройство.

Прочее

Q. Переносной компьютер используется для подключения к сети в офисе. При попытке его использования дома возникают проблемы с подключением к концентратору VPN 3000 из дома. В чем проблема?

A. В переносном компьютере могут сохраняться сведения маршрутизации от соединения по ЛВС. Информацию о решении этой проблемы см. в документе VPN-клиенты с проблемами маршрутизации Microsoft.

Q. Как узнать, подключен ли VPN-клиент к VPN-концентратору?

A. Проверьте значение параметра реестра HKLM\Software\Cisco Systems\VPN Client\TunnelEstablished. Если туннель активен, значение параметра равно 1. Если туннеля нет, значение параметра равно 0.

Q. Не удается создать подключение NetMeeting от ПК, отделенного VPN-концентратором, к VPN-клиенту, хотя при подключении данного ПК к VPN-клиенту, отделенному VPN-концентратором, проблем не возникает. Как устранить эту проблему?

A. Выполните соответствующие действия, перечисленные здесь, чтобы управлять настройками соединения.

- На основном диске ПК выберите **Program Files > Cisco Systems > VPN Client > Profiles**. Щелкните правой кнопкой мыши используемый профиль и выберите пункт **Открыть с помощью** из подменю, чтобы открыть профиль в программе, такой как Блокнот. (При выборе программы для использования следует снять флажок **Использовать ее для всех файлов такого типа**). Найдите параметр профиля для ForcekeepAlives и измените его значение с 0 на **1**, а затем сохраните данный профиль. или
- В VPN-клиенте выберите **Options > Properties > General** (Параметры > Свойства > Общие) и введите значение параметра "Peer response timeout" (Тайм-аут ответа равноправного узла), как показано в следующем примере окна. Можно указать значение таймаута в пределах от 30 до 480 секунд. или
- В VPN-концентраторе выберите **Configuration > User Management > Groups *modify group*** (Конфигурация > Управление пользователями > Группы > Изменить группу). На вкладке "IPSec" выберите вариант для IKE Keepalives, как показано в этом примере окна.

Интервал DPD (обнаружение недоступных равноправных узлов) изменяется в зависимости от настройки чувствительности. Если ответ не получен, устройство переключается в более агрессивный режим и отправляет пакеты каждые пять секунд, пока не будет достигнуто пороговое значение для ответа равноправного узла. В этот момент соединение отключается. Сообщения/запросы keepalive можно отключить, однако если соединение не было отброшено на самом деле, необходимо дождаться завершения по тайм-ауту. Корпорация Cisco рекомендует задать первоначальное значение чувствительности очень низким.

Дополнительные сведения

- **Страница поддержки VPN-клиента Cisco 3000**
- **Страница поддержки VPN-клиентов Cisco**

- **Устранение распространенных неполадок L2L и удаленного доступа к VPN с поддержкой IPsec**
- **Cisco Systems — техническая поддержка и документация**

Дата генерации PDF файла: Jan 05, 2010

---

http://www.cisco.com/support/RU/customer/content/10/105423/vpnclientfaq.shtml

---