Часто задаванмые вопросы по концентратору Cisco VPN 3000

Содержание

Введение

Данный документ содержит ответы на часто задаваемые вопросы о концентраторе Cisco VPN 3000.

[Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.](#)

Общие сведения

Вопрос. . Что делает сообщение об ошибках " " среднее значение?

О. Если существует "no traffic" (нет трафика), передаваемый между Концентратором VPN и Клиентом VPN сроком на время, пакет Dead Peer Detection (DPD) передан от Концентратора VPN до Клиента VPN, чтобы гарантировать, что его узел все еще там. Если существует проблема подключения между двумя узлами сети, когда клиент VPN не отвечает на запросы концентратора VPN, то концентратор VPN продолжает отправлять DPD-пакеты через определенный период времени. Если в течение определенного времени ответ на эти пакеты не будет получен, то туннель будет закрыт с генерацией сообщения об ошибке. [Дополнительные сведения см. в документе CSCdz45586(только для зарегистрированных пользователей).](#)

Сообщение об ошибке должно выглядеть приблизительно так:

```
SEV=4 AUTH/28 RPT=381 XXX.XXX.XXX.XX User [SomeUser] disconnected:
Duration: HH:MM:SS Bytes xmt: 19560 Bytes rcv: 17704 Reason:
Lost Service YYYY/MM/DD HH:MM:SS XXX.XXX.XXX.XXX
syslog notice
45549 MM/DD/YYYY HH:MM:SS SEV=4 IKE/123 RPT=XXX.XXX.XXX.XXX
Group [SomeDefault] User [SomeUser]
IKE lost contact with remote peer, deleting connection (keepalive type: DPD)
```

Причина: Удаленный узел IKE не отвечал на запросы о своём состоянии в течение определенного периода времени, поэтому соединение с узлом IKE было прервано. Сообщение содержит сведения об использованном механизме поддержания в активном

состоянии. Эта проблема повторяется только если общий интерфейс отключается во время сеанса активного туннеля. Пользователь должен отслеживать свое сетевое подключение, так как эти события генерируются для выявления основной причины потенциальных проблем с сетевым подключением.

Отключите поддержание в активном состоянии IKE, перейдя к %System Root%\Program Files\Cisco Systems\VPN Client\Profiles на клиентском персональном компьютере, испытывающем проблему в работе, и отредактируйте файл PCF (где применимо) для подключения.

Измените 'ForceKeepAlives=0' (по умолчанию) на 'ForceKeepAlives=1'.

Если проблема не устранена, то откройте Service Request (Запрос на обслуживание) с помощью Центра технической поддержки компании Cisco и предоставьте журналы событий клиента и концентратора VPN для возникших проблем.

Вопрос. . Что делает сообщение об ошибках "q_send" сбои, обнаруженные для среднего значения очереди EMQ1?

O. Когда существует слишком много событий отладки / информация в буфере, это сообщение об ошибках происходит. Кроме возможной потери нескольких сообщений о событиях это не оказывает другого негативного влияния. Попытайтесь уменьшить число событий до минимально возможного для предотвращения появления этого сообщения об ошибке.

Вопрос. . Моя удаленная группа все еще показывает в конфигурации концентраторов VPN. Как удалить эту группу из конфигурации?

O. Скопируйте конфигурацию в текстовый редактор (такой как Блокнот) и вручную отредактируйте или удалите информацию о группе, на которую влияют, обозначенную **[ipaddrgrouppool #.0]**. Сохраните конфигурацию и загрузите ее в концентратор VPN. Пример выходных данных команды приводится ниже.

```
!--- Change to 14.1 or any other number that is not in use !--- any number other than 0).
[ipaddrgrouppool 14.0] rowstatus=1 rangename= startaddr=172.18.124.1 endaddr=172.18.124.2
```

Вопрос. . Действительно ли возможно иметь несколько основныхи серверов SDI?

O. VPN 3000 Concentrator только в состоянии загрузить один файл секретного узла за один раз. В SDI предварительной версии 5.0, можно добавлять несколько SDI-серверов, но все они должны совместно использовать один и тот же секретный файл (основной и резервные серверы). В SDI версии 5.0 можно использовать только один основной SDI-сервер (резервные серверы содержатся в списке узлового секретного файла) и серверы репликации.

Вопрос. . Я добираюсь, " SSL 28 " сообщение об ошибках Отправителя. Какие действия следует предпринять?

O. Сообщение показывает, что срок действия вашего Secure Socket Layer (SSL) истекает в течение 28 дней. Этот сертификат используется для веб-управления через соединение по

HTTPS-протоколу. Настройки по умолчанию этого сертификата можно оставить без изменений или задать другие параметры перед созданием нового сертификата. Выберите **Configuration> System> Management Protocols> SSL**, чтобы сделать это. Выберите **Administration> Certificate Management** и нажмите **Generate** для возобновления сертификата.

Чтобы отключить HTTP или HTTPS в общем интерфейсе для повышения уровня безопасности концентратора VPN и предотвращения несанкционированного доступа, выберите Configuration > Policy Management > Traffic Management > Filters (Конфигурация > Управление политикой > Управление трафиком > Фильтры). Если требуется получить доступ к VPN-концентратору через Интернет с помощью HTTP или HTTPS, можно настроить доступ, основанный на адресе источника, в меню Administration > Access Rights > Access Control List. Дополнительная информация доступна в меню справки, расположенном в верхнем правом углу окна.

Вопрос. . Как я могу просмотреть сведения о пользователе в базе данных внутреннего пользователя? Эти сведения не видны при просмотре файла конфигурации.

O. Выберите **Administration> Access Rights> Access Settings**, выберите **Config File Encryption=None** и сохраните config для просмотра пользователей и паролей. Необходимо иметь возможность поиска определенного пользователя.

Вопрос. . Сколько пользователей может хранение во внутренней базе данных?

O. Количество пользователей является зависимым от версии и указанным в разделе **Configuration> User Management** Руководства пользователя для вашего выпуска VPN 3000 Concentrator. В VPN 3000 с номером выпуска 2.2 - 2.5.2 общее число пользователей или групп не превышает 100 (сумма пользователей и групп не должна превышать 100). В VPN 3000 версии 3.0 и более поздних для концентраторов 3005 и 3015 число пользователей или групп остается равным 100. Для концентраторов VPN 3030 и 3020 это число равно 500, для концентраторов VPN 3060 и 3080 — 1000. Кроме того, использование внешнего сервера аутентификации повышает возможности масштабирования и управления.

Вопрос. . В чем разница между шлюзом туннеля по умолчанию и шлюзом по умолчанию?

O. Концентратор VPN 3000 использует туннельный шлюз по умолчанию для маршрутизации туннелированных пользователей внутри частной сети (обычно внутренний маршрутизатор). Концентратор VPN использует шлюз по умолчанию для маршрутизации пакетов в Интернет (обычно внешний маршрутизатор).

Вопрос. . Если разместить концентратор VPN 3000 за межсетевым экраном или маршрутизатором, на которых запущены списки управления доступом, то через какие порты и протоколы следует разрешить передачу?

O. Эта диаграмма перечисляет порты и протоколы.

Сервис	Номер протокола	Исходный порт	Номер порта

PPTP управляемое соединение	6 (TCP)	1023	1723
Инкапсуляция туннеля PPTP	47 – GRE	Н/Д	Н/Д
Менеджмент ISAKMP/КЛЮЧА IPSEC	17 (UDP)	500	500
Инкапсуляция туннеля IPSec	50 (ESP)	Н/Д	Н/Д
Прозрачность NAT для IPSec	17 (UDP)	10000 (по умолчанию)	10000 (по умолчанию)

Примечание: Порт прозрачности Технологии NAT конфигурируем к любому значению в этом 4001 - 49151 диапазоне. В версиях 3.5 или позже, можно настроить IPsec через TCP, перейдя **к Configuration> System> Tunneling Protocols> IPsec> IPSec по TCP**. Можно ввести до 10 TCP-портов через запятую (1 - 65535). Если этот параметр настроен, убедитесь, что эти порты разрешены списками управления доступом в межсетевом экране или маршрутизаторе.

Вопрос. . Как вернуть заводские настройки концентратора VPN?

О. Из экрана File Management удалите файл "config" и перезагрузите концентратор. Если случайно этот файл удаляется, то сохраняется его резервная копия, "config.bak".

Вопрос. . Я могу использовать TACACS + для Административной проверки подлинности? О чем следует помнить во время ее выполнения?

О. Да, начиная с выпуска 3.0 концентратора VPN 3000, для административной аутентификации вы можете использовать TACACS+. После настройки TACACS+ убедитесь в работоспособности аутентификации перед выходом из системы. Неправильная настройка TACACS+ может заблокировать выход из системы. Это требует использования консольного порта для отключения TACACS+ и устранения проблемы.

Вопрос. . Что делать, если административный пароль утрачен?

О. В версиях 2.5.1 и позже, подключите ПК с консольным портом Концентратора VPN с помощью сквозного кабеля последовательного порта RS-232 с набором ПК для:

- 9600 бит в секунду
- 8 информационных битов
- без контроля четности
- 1 стоповый бит
- аппаратное управлением потоком разрешено
- Эмуляция терминала VT100

Перезагрузите концентратор виртуальной частной сети (VPN). После завершения диагностической проверки, в консоли отобразится линия из трех точек (...). **Нажмите клавиши CTRL-C не позднее трех секунд с момента появления этих точек.** После этого появится меню, позволяющее сбрасывать системные пароли до значений, принятых по

умолчанию.

Вопрос. . Какова цель имени группы и пароля группы?

О. Имя группы и пароль группы используются для создания хэша, который затем используется для создания ассоциации безопасности.

Вопрос. . Прокси - протокол преобразования адресов Концентратора VPN от имени туннелированных пользователей?

О. Да.

Вопрос. . Где поместить концентратор VPN 3000 по отношению к межсетевому экрану сети?

О. Концентратор VPN 3000 может быть размещен перед межсетевым экраном, позади него или параллельно ему, либо в демилитаризованной зоне (DMZ) межсетевого экрана. Не рекомендуется использовать общий и частный интерфейсы в той же самой виртуальной частной сети (VLAN).

Вопрос. . Там какой-либо путь состоит в том, чтобы отключить прокси - протокол преобразования адресов на Cisco VPN 3000 Concentrator?

О. Протокол разрешения proxy - адресации (ARP) не может быть отключен на Cisco VPN 3000 Concentrator.

Вопрос. . Где можно найти информацию об ошибках для концентратора VPN 3000?

О. Пользователи могут использовать Bug Toolkit (только зарегистрированные клиенты) для обнаружения подробных сведений о дефектах.

Вопрос. . Где можно найти примеры конфигурации для концентратора VPN 3000?

О. В дополнение к документации VPN 3000 Concentrator больше примеров конфигурации может быть найдено на Странице технической поддержки концентратора Cisco VPN серии 3000.

Вопрос. . Как расширить запись событий в журнал, чтобы улучшить отладку определенных событий?

О. Можно перейти по пути Configuration > System > Events > Classes и настроить определенные события (например, IPSec или PPTP) для оптимизации отладки. Режим отладки должен быть разрешен только на время поиска и устранения неисправностей, так как это может привести к падению производительности. Для отладки IPsec включите IKE, IKEDBG, IPSEC, IPSECDBG, AUTH и AUTHDBG. При использовании сертификатов добавьте в список класс CERT.

Вопрос. . Как можно отслеживать трафик к концентратору VPN 3000?

О. Интерфейс HTML, который идет с VPN 3000 Concentrator, позволяет вам иметь основной мониторинг функциональных возможностей, если вы смотрите под **Monitoring> Sessions**. Концентратор VPN 3000 может также контролироваться с помощью любого SNMP-менеджера. Кроме того, можно купить программу управления безопасностью и виртуальной частной сетью (Cisco VPN / Security Management Solution (VMS)). Cisco VMS предоставляет ключевую функциональность для оказания помощи при развертывании концентратора VPN 3000 и требует глубокого контроля удаленного доступа и VPN, основанных на протоколах IPsec, L2TP и PPTP. Дополнительные сведения о VMS см. в документе под названием Программа управления безопасностью виртуальной частной сети.

Вопрос. . Концентратор серии Cisco VPN 3000 имеет интегрированный межсетевой экран? Если это так, какие функции поддерживаются?

О. В то время как серия интегрировала порт не сохраняющий состояние / фильтрация возможностей и NAT, Cisco предлагает, чтобы вы использовали устройство как межсетевой экран Cisco Secure PIX для корпоративного межсетевого экрана.

Вопрос. . Какие параметры маршрутизации и протоколы VPN поддерживаются Концентратором серии Cisco VPN 3000?

О. Серия поддерживает эти параметры маршрутизации:

- Протокол маршрутной информации (RIP)
- RIP2
- Open Shortest Path First (OSPF)
- статические маршруты
- VRRP-протокол

Поддерживаемыми протоколами VPN являются следующие протоколы — PPTP, L2TP, L2TP / IPsec и IPsec с или без устройства трансляции сетевых адресов между VPN 3000 и конечным клиентом. IPsec-протокол использующий трансляцию сетевых адресов известен в качестве прозрачной трансляции сетевых адресов.

Вопрос. . Какие механизмы/системы аутентификации поддерживает Концентратор VPN Cisco серии 3000?

О. Домен NT, RADIUS или RADIUS прокси, RSA Security SecurID (SDI), Цифровые сертификаты и внутренняя аутентификация поддерживаются.

Вопрос. . Я могу сделать статическую трансляцию сетевых адресов (NAT) для пользователей, выходящих через VPN 3000 Concentrator?

О. Для выходящих пользователей вы можете выполнить только трансляцию адреса порта (PAT). Выполнить статическую трансляцию сетевых адресов на концентраторе VPN 3000 невозможно.

Вопрос. . Как можно назначить статический IP-адрес конкретному пользователю PPTP или IPSec через VPN 3000 Concentrator?

О. Этот список объясняет, как назначить статические IP - адреса:

- **Пользователи PPTP**В разделе Управления IP-адресами, в дополнение к выбору вашего пула или опций Протокола DHCP (динамического конфигурирования узла), проверяют опцию **Use Client Address**. Затем определите пользователя и IP-адрес в концентраторе VPN 3000. При подключении пользователь всегда будет получать IP-адрес указанный в концентраторе VPN.
- **Пользователи IPSec**В разделе Управления IP-адресами, в дополнение к выбору к вашему пулу или параметрам DHCP, проверяют опцию **Use Address from Authentication Server**. Затем определите пользователя и IP-адрес в концентраторе VPN 3000. При подключении пользователь всегда будет получать IP-адрес указанный в концентраторе VPN. Все остальные пользователи, которые принадлежат к той же самой группе или к другим группам будут получать IP-адрес из глобального пула или от DHCP-сервера.С помощью программного обеспечения концентратора Cisco VPN 3000 версии 3.0 и выше можно настроить адресный пул по группам. С помощью этой функции также можно назначить статический IP-адрес определенному пользователю. Если пул настраивается для группы, то пользователь со статическим IP-адресом получает назначенный ему IP-адрес, а другие члены той же самой группы получают IP-адреса от пула группы. Эта последовательность назначения IP-адреса применяется только тогда, когда концентратор VPN используется в качестве сервера аутентификации.

Примечание: При использовании внешний сервер проверки подлинности, то необходимо использовать внешний сервер для присвоения адресов правильно.

Вопрос. . Какова совместимость с продуктами PPTP Майкрософт и концентратором VPN 3000?

О. Эта информация основывается на Выпуске ПО Концентратора серии VPN 3000 3.5 и позже; Концентраторы серии VPN 3000, Модели 3005, 3015, 3020, 3030, 3060, 3080; а также ОС Microsoft Windows 95 и более поздние.

- **Windows 95 Dial-Up Networking (DUN) 1.2**DUN 1.2 не поддерживает протокол шифрования Microsoft Point-to-Point Encryption (MPPE). Для соединения с использованием MPPE установите DUN 1.3 для Windows 95. Обновление Microsoft DUN 1.3 можно загрузить с веб-узла Microsoft.
- **Windows NT4.0**Windows NT полностью поддерживается для соединений Протокола PPTP с Концентратором VPN. Требуется пакет обновления 3 (SP3) или более новый. Если Вы запустили пакет обновления SP3, Вам следует установить исправления, связанные с управлением производительностью и безопасностью протокола PPTP. Дополнительные сведения о производительности PPTP и безопасном обновлении для WinNT 4.0 см. на веб-узле Microsoft.Обратите внимание на то, что 128-битный пятый пакет обновления некорректно обрабатывает MPPE-ключи, а PPTP может не передать данные. Если это происходит, то в журнале регистрации событий появится следующее сообщение:`103 12/09/1999 09:08:01.550 SEV=6 PPP/4 RPT=3 80.50.0.4 User [ testuser ] disconnected. Experiencing excessive packet decrypt failure.`Для решения этой проблемы загрузите обновление для того, Как получить последнего Windows NT Service Pack 6a и Пакет обновления Windows NT 4.0 6a Доступный. Дополнительные сведения см. в статье Майкрософт под названием MPPE Keys Not Handled Correctly for a 128-Bit MS-

CHAP Request .

Вопрос. . Какое максимальное число фильтров допускается на концентраторе VPN 3000?

O. Максимальное число фильтров, что можно прибавить VPN 30xx модуль (даже 3030 или 3060) исправлено в 100. Пользователи могут найти дополнительные сведения об этой проблеме путем просматривания идентификатор ошибки Cisco CSCdw86558 (только зарегистрированные клиенты).

Вопрос. . Каково максимальное число маршрутов в линейке 30xx концентраторов VPN?

O. Максимальное число маршрутов:

- Ранее концентратор VPN 3005 мог работать не более чем с 200 маршрутами. Теперь их число увеличено до 350. Пользователи могут получить дополнительную информацию, ознакомившись со сведениями об ошибке CSCeb35779 (только для зарегистрированных пользователей) .
- Концентратор VPN 3030 был проверен на 10000 маршрутов.
- Предельное значение таблицы маршрутизации в концентраторах VPN 3030, 3060 и 3080 пропорционально доступным ресурсам или памяти в каждом устройстве.
- Концентратор VPN 3015 не имеет предварительно задаваемых ограничений на число маршрутов. Это выполняется для протокола маршрутной информации (RIP) и протокола первоочередного открытия кратчайших маршрутов (OSPF).
- Концентратор VPN 3020 из-за ограничений Microsoft Windows XP не способен обрабатывать большое число бесклассовых статических маршрутов(CSR). Концентратор VPN 3000 ограничивает число бесклассовых статических маршрутов, которые содержатся в информационном сообщении DHCP, при соответствующей настройке. Концентратор VPN 3000 в зависимости от класса ограничивает число маршрутов до 28-42.

Вопрос. . Как делают меня абсолютно ясный интерфейсная статистика по VPN 3000 Concentrator?

O. Выберите **Monitoring> Statistics> MIB-II> Ethernet** и перезагрузите статистику для очистки статистики для текущего сеанса. Помните, что это не приводит к полному удалению статистики. Для реального сброса статистики необходимо выполнить перезагрузку (в противоположность сбросу параметров для целей слежения).

Вопрос. . Какие порты я должен позволить на Концентраторе VPN для связи Протокола NTP?

O. Позвольте порт 123 UDP и TCP.

Вопрос. . Каковы функции UDP-портов 625xx?

O. Порты используются для связи Клиента VPN между фактическим контейнером /

Deterministic NDIS Extender (DNE) и TCP / стек IP ПК, и для внутреннего использования развития только. Например, порт 62515 используется клиентом VPN для отправки данных в журнал клиента VPN. Другие функции показаны далее.

- 62514 - Cisco Systems, Inc. Служба VPN для драйвера IPSec Cisco Systems
- 62515 - передача с драйвера IPSec Cisco Systems на VPN-службу Cisco Systems
- 62516 – Служба VPN Cisco Systems, Inc. XAUTH
- 62517 – аутентификация XAUTH для доступа к службам VPN корпорации Cisco Systems
- 62518 – Cisco Systems, Inc. Службы VPN для CLI
- 62519 - от CLI к службе VPN Cisco Systems, Inc
- 62520 - Cisco Systems, Inc. Службы VPN для UI
- 62521 – UI к службе VPN Cisco Systems, Inc
- 62522 – сообщения журнала
- 62523 – диспетчер подключений к службе VPN Cisco Systems, Inc
- 62524 – PPPTool к службе VPN Cisco Systems, Inc

Вопрос. . Я могу удалить WebVPN, пускающий в ход панель?

O. Вы не можете удалить плавающую строку инструментов, ни избежать загружать плавающую панель инструментов при установлении сеанса WebVPN. Причиной этого является то, что при закрытии этого окна сеанс будет сразу же завершен, а при повторной попытке регистрации в системе это окно будет снова загружено. Такая организация сеансов WebVPN была спроектирована изначально. Можно закрыть главное окно, но закрыть плавающее окно нельзя.

Программное обеспечение

Вопрос. . WebVPN поддерживает Веб - доступ Outlook (OWA) 2003?

O. Поддержка OWA 2003 года WebVPN на VPN 3000 Concentrator теперь доступна с (только зарегистрированными клиентами) загрузок версии 4.1.7.

Вопрос. . Где я могу получить обзор новейшего программного обеспечения для концентратора VPN 3000?

O. Вся поставка Cisco VPN 3000 Concentrator с актуальнейшим кодом, но пользователи может проверить загрузки (только зарегистрированные клиенты), чтобы видеть, доступно ли более актуальное программное обеспечение.

Самая последняя документация по концентратору VPN 3000 может быть найдена в разделе Cisco VPN 3000 Series Concentrator (Концентратор Cisco VPN 3000).

Вопрос. . Мне нужен сервер TFTP для обновления VPN 3000 Concentrator? Существуют ли альтернативные способы обновления?

O. В дополнение к использованию TFTP можно обновить Концентратор VPN путем загрузки последних версий программного обеспечения на жесткий диск. Затем от браузера в системе, где программное обеспечение расположено, перейдите **к Administration> Software Update** и найдите загруженное программное обеспечение на своем жестком диске (точно

так же, как открытие файла). **Когда найдете эту программу, перейдите на вкладку Upload (Выгрузка).**

Вопрос. . Что обозначает "k9" в последних условных именах (например, "vpn3000-3.0.4.Rel-k9.bin")?

О. Обозначение "k9" для имени образа заменило изначально используемое обозначение 3DES (например, vpn3000-2.5.2.F-3des.bin). Таким образом, "k9" указывает, что это образ 3DES.

Вопрос. . Необходимо ли использовать сжатие данных в группе IPSec для всех пользователей?

О. Сжатие данных увеличивает требования к памяти и загрузку ЦПУ для каждого пользовательского сеанса и следовательно уменьшает суммарную пропускную способность Концентратора VPN. По этой причине компания Cisco рекомендует разрешать использование сжатия данных только если каждый член группы является удаленным пользователем, который подключается через модем. Если какой-либо член группы подключается с помощью широкополосного соединения, то не следует использовать сжатие данных для этой группы. Вместо этого, разделите эту группу на две подгруппы — пользователи модемного соединения и пользователи широкополосного соединения. Включение компрессии данных только для группы пользователей модема.

Другие дополнительные возможности

Вопрос. . Распределение нагрузки работает с прямыми соединениями локальных сетей?

О. Распределение нагрузки является эффективным только на удаленных сеансах, инициируемых с Cisco VPN software client (Выпуск 3.0 и позже). Все остальные клиенты (PPTP, L2TP) и соединения LAN-to-LAN могут подключаться к концентратору VPN, на котором разрешена балансировка нагрузки, но участвовать в ее управлении они не могут.

Вопрос. . Как я дешифрую пароли от файла config?

О. Перейдите **к Configuration> System> Протоколы управления> XML** и затем к **администрированию |, управление файлами выбирает формат XML**. Используйте то же название, или другой, и откройте файл для просмотра паролей.

Вопрос. . Можно ли использовать вместе протокол резервного виртуального маршрутизатора (VRRP) и балансировку нагрузки?

О. Выравнивание нагрузки нельзя использовать вместе с VRRP. В конфигурации VRRP, устройство резервного копирования данных остается неработоспособным даже при выходе из строя активного концентратора VPN. В конфигурации выравнивания нагрузки нет бездействующих устройств.

Вопрос. . Весь трафик VPN клиента удаленного доступа должен пройти

зашифрованный туннель к Концентратору VPN в предприятии или поставщике услуг? Например, можно ли планировать веб-доступ к другим узлам без шифрования, непосредственно через ISP Интернет-соединение?

O. Да. Это понятие известно как "разделение туннелей". Разделение туннелей предоставляет безопасный доступ к ресурсам предприятия через зашифрованный туннель, в то время, как доступ к Интернет осуществляется напрямую через ресурсы ISP (доступ к сети предприятия не может быть получен через Интернет). Концентратор Cisco VPN 3000 для клиента VPN Cisco и аппаратного клиента VPN 3002 может поддерживать раздельное туннелирование. Для обеспечения дополнительной безопасности эта функция контролируется администратором концентратора VPN, а не пользователем.

Вопрос. . Безопасно ли использование раздельного туннелирования?

O. Разделенное туннелирование позволяет вам иметь удобство просмотра Интернета, в то время как связано через VPN-туннель. Однако, это может представлять определенную опасность, если пользователь VPN, подключенный к сети предприятия, станет объектом сетевой атаки. В этом случае пользователям рекомендуется использовать персональный межсетевой экран. В примечаниях к выпуску любой версии клиента VPN обсуждаются вопросы, связанные с возможностью взаимодействия с персональными брандмауэрами.

Вопрос. . Как делает распределение нагрузки, работают на Cisco VPN 3000 Concentrator?

O. Загрузка вычислена как процент, полученный из активных соединений, разделенных на максимальные числа настроенных подключений. Ведущий концентратор всегда пытается брать на себя наименьшую нагрузку, так как он работает с дополнительной нагрузкой обслуживания всех административных сеансов LAN-LAN, рассчитывая нагрузку всех остальных членов кластера, и отвечает за все перенаправления клиента.

Для вновь настраиваемых рабочих кластеров ведущий концентратор нагружен примерно на 1 % перед установкой любого соединения. Таким образом, ведущий концентратор перенаправляет соединения к резервному концентратору до тех пор, пока процент нагрузки на резервном концентраторе выше, чем на ведущем. Например, имеются два концентратора VPN 3030 в "неактивном" состоянии, а ведущий концентратор загружен на 1 %. Вторичный концентратор имеет 30 соединений (нагрузка 2 %) перед принятием соединений ведущим концентратором.

Чтобы проверить, что ведущее устройство принимает соединения, перейдите **к Configuration> System> General> Sessions** и понизьте максимальное число соединений с искусственно малое число для быстрого увеличения загрузки, размещенной в резервный Концентратор VPN.

Вопрос. . Сколько устройств головной станции VPN может Контролировать дорожку?

O. Монитор VPN может отслеживать 20 головных устройств. В топологии типа "звезда", соединения от удаленных узлов отслеживаются в головном узле сети. Необходимость контроля всех удаленных узлов и пользователей отсутствует, так как эти данные могут прослеживаться центральным маршрутизатором. Эти головные устройства могут

поддерживать до 20000 удаленных пользователей или до 2500 удаленных узлов. Устройство VPN с двойным подключением, которое соединяется за пределами узла, считается за два устройства, а их число не может превышать 20 устройств, которые могут контролироваться.

Дополнительные сведения

- Страница технической поддержки для концентратора Cisco VPN 3000
- Страница поддержки Cisco VPN 3000 Client
- Cisco Systems – техническая поддержка и документация