Вопросы и ответы по протоколу PPTP

Содержание

Введение

Данный документ рассматривает часто задаваемые вопросы по протоколу туннелирования "точка-точка" (PPTP).

Дополнительные сведения об условных обозначениях данного документа см. в разделе Условные обозначения, использованные в практических рекомендациях компании Cisco.

Аппаратные средства

Вопрос. . Как я могу определить, какие платформы поддерживают PPTP?

О. Можно определить, какое программное обеспечение Cisco IOS освобождает PPTP поддержки при помощи Характерного средства навигатора (только зарегистрированные клиенты). Это средство позволяет сравнивать версии программного обеспечения Cisco IOS, устанавливать соответствия между функциями Cisco IOS и CatOS и версиями программ, выбирать нужные версии программного обеспечения для поддержки оборудования.

Вопрос. . Когда протокол PPTP был впервые представлен в межсетевом экране Cisco Secure PIX?

О. PPTP был сначала представлен в версии 5.1 межсетевого экрана Cisco Secure PIX. См. документ PIX 6.x: PPTP с Примером настройки аутентификации RADIUS для получения дополнительной информации.

Примечание: Версии PIX 7.x и выше не поддерживают функцию оконечных устройств для соединений по протоколу PPTP.

Вопрос. . Есть ли подробные данные о Средствах шифрования Microsoft точка-точка (MPPE), о которых я должен знать?

О. MPPE требует Протокола квитирования с аутентификацией Microsoft (MS-CHAP). Он работает только с системой RADIUS или с локальной аутентификацией, а сервер RADIUS должен поддерживать значения атрибутов для ключей MPPE.

В следующем списке показаны некоторые платформы и их совместимость с технологией MPPE.

- Cisco Secure ACS для UNIX (CSUNIX) — Нет
- Access Registrar — Нет
- Funk RADIUS — Да
- Cisco Secure ACS для Windows — Да
- Сервер Microsoft Windows 2000 Internet Authentication Server — Да

Вопрос. . Какая версия программного обеспечения Cisco IOS изначально поддерживала PPTP?

O. PPTP первоначально поддерживался в программном обеспечении Cisco IOS версии 12.0(5)XE5 на маршрутизаторах Cisco 7100/7200. Затем, начиная с ПО Cisco IOS версии 12.1(5)T, эта поддержка была реализована во всех платформах Cisco IOS.

Вопрос. . Каковы некоторые известные проблемы совместимости с Microsoft PPTP products и VPN 3000 Concentrator?

O. Эта информация основывается на выпусках ПО Концентратора серии VPN 3000 3.5 и позже; Концентраторы серии VPN 3000, Модели 3005, 3015, 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 PPTP на концентраторе VPN. Требуется пакет обновления 3 (SP3) или более новый. Если запущен пакет обновления SP3, необходимо установить исправления, связанные с управлением производительностью и безопасностью протокола PPTP. Дополнительные сведения о производительности PPTP и обновлении безопасности для WinNT 4.0 см. на веб-узле Microsoft. Единственно возможный выход — переустановка NT 4.0 Server Option Pack без дополнительной установки пакета обновления.**Примечание:** Пакет услуг на 128-бит 5 не обрабатывает MPPE ключи правильно, и 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.
```
Дополнительные сведения см. в статье Майкрософт под названием MPPE Keys Not Handled Correctly for a 128-Bit MS-CHAP Request .

Вопрос. . Маршрутизаторы Cisco IOS или Межсетевые экраны PIX поддерживают PPTP, проходят или PPTP по функции Преобразования адресов портов (PAT)?

O. Cisco IOS Software Release 12.1T и более поздний PPTP поддержки проходят или PPTP по функции PAT. Дополнительную информацию см. в разделе "NAT — поддержка PPTP в

конфигурации с перегрузкой (с использованием PAT)" документацииКраткое описание ПО Cisco IOS версии 12.1T для первичного развертывания. Чтобы настроить передачу протокола PPTP через PAT или прохождение PPTP через маршрутизатор Cisco IOS, обратитесь к разделу IP-туннелирование — конфигурирование PPTP через PAT для сервера Microsoft PPTP.

PIX версии 6.3 и более поздние поддерживают проход PPTP или использование PPTP по PAT с помощью функции привязки PPTP. Эта функция позволяет PPTP-трафику проходить PIX, если выполнена настройка для работы с PAT. PIX выполняет постоянную проверку пакетов PPTP в процессе. Для того чтобы зафиксировать PPTP на PIX, обратитесь к разделу Настройка PPTP в документе Проверка настройки приложений (фиксация).
Команда fixup protocol pptp 1723 настраивает адресную привязку PPTP.

Устранение неполадок

Вопрос. . Какие порты нужно открыть в межсетевом экране для создания PPTP туннеля?

О. Откройте эти порты.

- TCP/1723
- IP Protocol/47 GREДополнительную информацию см. в документе Разрешение соединений PPTP через PIX.

Вопрос. . Каковы известные дефекты PPTP программного обеспечения Cisco IOS?

О. Эти дефекты были определены:

- CSCdt46181 (только зарегистрированные клиенты) - См. Уязвимость PPTP Cisco IOS для получения дополнительной информации.
- CSCdz47290 (только зарегистрированные клиенты) - Быстрый PPTP / коммутация в контексте процесса, сломанная, когда технология CEF включена глобально.
- CSCdx86482 (только зарегистрированные клиенты) - Туннелирование PPTP сломалось.
- CSCdt11570 (только зарегистрированные клиенты) - 128-разрядные Средства шифрования Microsoft точка-точка (MPPE) не работают на аппаратный Модуль предоставления комплексных услуг (ISM).
- CSCdt66607 (только зарегистрированные клиенты) - PPTP 128-разрядный MPPE не работает с Cisco Secure ACS для Windows.
- CSCdu19654 (только зарегистрированные клиенты) - Сбои PPTP.
- CSCdv50861 (только зарегистрированные клиенты) - MPPE не выполняет согласование с Windows 2000.

Зарегистрированные заказчики могут просмотреть подробные информации об ошибке при помощи Инструментария ошибки Cisco (только зарегистрированные клиенты) для получения дополнительной информации.

Вопрос. . Каковы ограничения PPTP?

O. PPTP имеет некоторые ограничения.

- PPTP поддерживает только Cisco Express Forwarding (CEF) и коммутацию процессов. Быстрая коммутация не поддерживается.
- ПО Cisco IOS поддерживает только добровольное туннелирование в виде сетевого сервера PPTP (PNS).
- Для поддержки MPPE необходимы криптографические образы. Для шифрования MPPE требуется аутентификация MS-CHAP, а MPPE не поддерживается с TACACS+.

Вопрос. . На какие существенные события отладки следует обращать внимание в процессе устранения неполадок PPTP для маршрутизатора?

O. Ищите эти отладки.

- **debug aaa authentication**
- **debug aaa authorization**
- **debug radius**
- **debug ppp negotiation –**
- **debug ppp authenticaion –**
- **debug vpdn events**
- **debug vpdn errors**
- **debug vpdn l2x-packet**
- **debug ppp mppe events**
- **debug ppp chap**

Контролируйте наступление этих важных событий.

```
SCCRQ = Start-Control-Connection-Request -
   message code bytes 9 and 10 = 0001
SCCRP = Start-Control-Connection-Reply
OCRQ = Outgoing-Call-Request -
   message code bytes 9 and 10 = 0007
OCRP = Outgoing-Call-Reply
```

Вопрос. . Что означает получение сообщения "Error 734" и последующее отключение?

O. Эта ошибка показывает, что маршрутизатор и компьютер не могут согласовать аутентификацию. **Например, если заданы протоколы аутентификации ПК для Shiva PAP (SPAP) и MS-CHAP версии 2 (если маршрутизатор не способен поддерживать эту версию), и задан маршрутизатор для CHAP, то в этом случае при отправке на моршрутизатор команды debug ppp negotiation, выдается следующая информация.**

```
04:30:55: Vi1 LCP: Failed to negotiate with peer
```

Другим примером является ситуация, когда на маршрутизатор отправлена команда vpdn group 1 ppp encrypt mppe 40 required, а для ПК задан "запрет любого шифрования". Этот ПК не может установить соединение и выдает сообщение "Error 734," а при отправке на маршрутизатор команды debug ppp negotiation, выдается следующая информация.

```
04:51:55: Vi1 LCP: I PROTREJ
      [Open] id 3 len 16 protocol CCP (0x80FD0157000A120601000020)
```

Вопрос. . Что означает ошибка 742?

О. Эта ошибка означает, что удаленный компьютер не поддерживает тип обязательного шифрования данных. **Например, если для ПК задан режим "только зашифрованный трафик", а с маршрутизатора убрана команда pptp encrypt mppe auto, то в этом случае ПК и маршрутизатор не смогут согласовать шифрование. В результате выполнения команды debug ppp negotiation отображаются следующие выходные данные.**

```
04:41:09: Vi1 LCP: O PROTREJ
      [Open] id 5 len 16 protocol CCP (0x80FD0102000A1206010000B0)
```

Другой пример включает проблему с маршрутизатором MPPE RADIUS. **Если для маршрутизатора установлено ppp encrypt mppe auto required, а ПК для "шифрования, разрешенного с аутентификацией на сервер RADIUS, не возвращает ключ MPPE", то на ПК выдается следующее сообщение об ошибке "Error 742: The remote computer does not support the required data encryption type (Ошибка 742: удаленный компьютер не поддерживает требуемый тип шифрования данных)".** Отладчик маршрутизатора отображает Call-Clear-Request (bytes 9 and 10 = 0x000C = 12 = Call-Clear-Request per RFC) как показано здесь.

```
00:45:58: Tnl 17 PPTP: CC I 001000011A2B3C4D000C000000000000
00:45:58: Vi1 Tnl/Cl 17/17 PPTP: CC I ClearRQ
```

Вопрос. . Я думаю, что у меня есть проблема разделенного туннелирования. Что делать, когда появляется PPTP туннель, метрика PPTP маршрутизатора выше, чем предыдущие настройки по умолчанию, и связь теряется?

О. Выполните пакетный файл (batch.bat) для изменения Организации маршрутизации Microsoft для решения этой проблемы. Удалите и повторно установите заданный по умолчанию маршрутизатор (необходимо знать IP-адрес, которому назначен клиент PPTP, например 192.168.1.1).

В рассматриваемом примере сетевой адрес в маршрутизаторе равен 10.13.1.x.

```
route delete 0.0.0.0
route add 0.0.0.0 mask 0.0.0.0 161.44.17.1 metric 1
route add 10.13.1.0 mask 255.255.255.0 192.168.1.1 metric 1
```

Вопрос. . Когда я устраняю неполадки PPTP, каковы некоторые проблемы для рассмотрения?

О. Ниже перечислены некоторые проблемы, связанные с использованием Microsoft, которые необходимо учитывать при устранении неполадок PPTP. Подробнее см. Базу знаний Майкрософт и приведенные ниже ссылки.

- Как поддержать RAS - подключения активными после того, чтобы выходить из системыСоединения службы удаленного доступа Windows (RAS) автоматически разрываются при отключении клиента RAS. **Можно оставаться подключенным, включив в клиенте RAS ключ реестра KeepRasConnections.**
- Пользователь не предупрежден при входе с кэшированными учетными даннымиЕсли при регистрации в домене с рабочей станции под управлением Windows или с рядового сервера не может быть найден контроллер домена, не выдается никакого сообщения об ошибке, информирующего об этой проблеме. Вместо этого происходит регистрация на локальном компьютере с использованием кэшированных учетных данных.
- Как записать файл LMHOSTS для проверки данных домена и других проблем разрешения именЕсли в сети TCP/IP возникают проблемы с разрешением имен, возможно, необходимо использовать файлы Lmhosts для разрешения имен NetBIOS.

Следуйте специальной процедуре для создания файла Lmhosts, который используется в разрешении имен и проверке данных домена.

Дополнительные сведения

- Страница поддержки PPTP
- Страница поддержки PIX
- Страница поддержки концентраторов семейства VPN 3000
- RFC 2637: Протокол PPTP
- Cisco Systems – техническая поддержка и документация