Настройка и устранение неполадок шифрования данных на уровне сети Cisco: Общие сведения – Часть 1

Содержание

Введение

В этом документе обсуждается настройка и устранение неисправностей шифрования на уровне сети Cisco с ассоциациями безопасности IPsec и ISA и протоколом управления ключами (ISAKMP), а также объясняются основы шифрования сетевого уровня и базовая конфигурацию с IPSec и ISAKMP.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Выпуск 11.2 Программного обеспечения Cisco IOS и позже

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 Технические рекомендации Cisco. Условные обозначения.

Общие сведения и настройки шифрования данных на сетевом уровне

Функция шифрования Сетевого уровня была представлена в Выпуске 11.2 программного обеспечения Cisco IOS. Это предоставляет механизм для безопасной передачи данных и состоит из двух компонентов:

- **Проверка подлинности маршрутизатора:** До мимолетного зашифрованного потока данных два маршрутизатора выполняют одноразовое, двухсторонняя проверка подлинности с помощью открытых ключей Стандарта цифровой подписи (DDS) для подписания случайных проблем.
- **Шифрование сетевого уровня:** Для шифрования полезной нагрузки IP маршрутизаторы используют Обмен ключами Диффи-Хеллмана для безопасной генерации DES (40-или 56-разрядный ключ сеанса), Тройной DES - (168-разрядный) 3DES, или более свежий Расширенный стандарт шифрования - AES (128-разрядный (по умолчанию) или 192-разрядный, или 256-разрядный ключ), представленный в 12.2 (13) T. Новые ключи сеанса генерируются на настраиваемой основе. Политика шифрования установлена криптокартами, которые используют расширенные списки доступа IP для определения, какая сеть, подсеть, хост или пары протокола должны быть зашифрованы между маршрутизаторами.

Основы криптографии

Поле криптографии касается поддерживающей частной связи. Защита чувствительных средств связи была акцентом на криптографии всюду по большой части его истории. Шифрование является преобразованием данных в некоторую нечитабельную форму. Его цель состоит в том, чтобы гарантировать конфиденциальность путем сохранения информации скрытой от любого, для кого это не предназначено, даже если они видят

зашифрованные данные. Расшифровка является реверсом шифрования: это - преобразование зашифрованных данных назад в понятную форму.

Шифрование и расшифровка требуют использования некоторой секретной информации, обычно называемой "ключом". В зависимости от используемого механизма шифрования тот же ключ мог бы использоваться и для шифрования и для расшифровки; в то время как для других механизмов, ключи, используемые для шифрования и расшифровки, могли бы быть другими.

В то время как цифровая метка времени связывает документ своему созданию в определенное время, цифровая подпись связывает документ обладателю определенного ключа. Эти криптографические механизмы могут использоваться для управления доступом к дисководу совместно используемого диска, установке высокого уровня безопасности, или к телевизионному каналу Pay Per View.

В то время как современное шифрование становится все более и более разнообразным, криптография существенно основана на проблемах, которые трудно решить. Проблема может быть трудной, потому что ее решение требует знания ключа, такого как дешифрование зашифрованного сообщения или подписание некоторого цифрового документа. Проблема может также быть трудной, потому что внутренне трудно завершить, такие как обнаружение сообщения, которое производит данное значение хеш-функции.

Поскольку поле криптографии совершенствовалось, линии раздела для того, что и что не является криптографией, стали размытыми. Криптографии сегодня можно было бы подвести итог как исследование способов и приложений, которые зависят от существования математических проблем, которые трудно решить. Криптоаналитик пытается поставить под угрозу криптографические механизмы, и криптология является дисциплиной криптографии и объединенного криптоанализа.

Определения

В данном разделе содержатся термины, относящиеся к данному документу.

- **Authentication:** Возможность убедиться в том, что полученные данные действительно отправлены заявленным отправителем.
- **Конфиденциальность:** Передача данных таким образом, что уполномоченные получатели знают, что отправляется, а неуполномоченные лица не могут определить, что отправлено.
- **Стандарт шифрования данных (DES):** DES использует метод симметричного ключа, который также известен как метод секретного ключа. Это значит, что если блок данных зашифрован с помощью ключа, то зашифрованный блок должен быть расшифрован тем же ключом, следовательно, шифрование и дешифрование должны выполняться с помощью одного и того же ключа. Несмотря на то, что данный способ шифрования широко известен и опубликован, наиболее известным способом взламывания является применение грубой силы. Необходимо протестировать ключи по отношению к зашифрованным блокам, чтобы проверить, могут ли они правильно расшифровывать их. По мере того, как процессоры становятся более мощными, существование стандарта шифрования DES приближается к концу. Например, координированные усилия с использованием дополнительной вычислительной мощности тысяч компьютеров, подключенных к Интернету, способны найти 56-битный ключ к

зашифрованному с помощью DES сообщению в течение 21 дня.DES проверяется каждые пять лет Агентством национальной безопасности (АНБ) США на соответствие целям правительства США. Срок действия текущего утверждения оканчивается в 1998 году; Агентство национальной безопасности заявило, что не планирует повторную сертификацию DES. Помимо DES существуют другие алгоритмы шифрования, которые также не имеют других известных недостатков, кроме подверженности атакам с применением грубой силы. Дополнительные сведения см. в DES FIPS 46-2 Национального института стандартов и технологий (NIST) .

- **Расшифровка:** Обратное применение алгоритма шифрования к зашифрованным данным, заключающееся в восстановлении данных в их исходном незашифрованном состоянии.
- **DSS и алгоритм цифровой подписи (DSA):** DSA опубликован Национальным институтом стандартов и технологий США в "Стандартной цифровой подписи" (DSS), в рамках государственного проекта США Capstone. DSS выбран Национальным институтом стандартов и технологий США(NIST), в сотрудничестве с Управлением национальной безопасности (NSA) в качестве стандарта цифровой аутентификации правительства США. Стандарт выпушен 19 мая 1994 г.
- **Шифрование:** Применение особого алгоритма к данным для изменения внешнего вида данных, что делает их непонятными для лиц, не уполномоченных просматривать данные сведения.
- **Целостность:** Обеспечение передачи данных из источника в место назначения без незамеченных изменений.
- **Невозможность отрицать факт отправки:** Способность получателя доказать, что отправитель данных действительно отправил их, даже если впоследствии отправитель будет отрицать факт отправки данных.
- **Криптография с открытым ключом:** Традиционная криптография основывается на знании и использовании отправителем и получателем одного и того же секретного ключа. Отправитель использует секретный ключ для шифрования сообщения, а получатель использует тот же секретный ключ для расшифровки сообщения. Этот способ известен как "секретный ключ" или "симметричная криптография.". Основная проблема заключается в согласованном использовании получателем и отправителем секретного ключа, недоступного другим лицам. Если получатель и отправитель находятся в разных местоположениях, они должны прибегать к услугам курьера, использовать телефонную систему или другой способ передачи данных, чтобы предотвратить разглашение информации о секретном ключе. Любой, кто прослушивает или перехватывает ключи во время передачи, может позднее прочитать, изменить и подделать все зашифрованные или аутентифицированные сообщения с помощью данного ключа. Создание, передача и хранение ключей называется "управление ключом"; все криптографические системы должны решать вопросы, связанные с управлением ключами. Поскольку все ключи в криптографической системе секретного ключа должны оставаться секретными, в криптографии секретного ключа часто имеются трудности в обеспечении безопасного управления ключом, особенно в открытой системе с большим количеством пользователей.Понятие о криптографии с использованием общего ключа было введено в 1976 году Витфилдом Диффи (Whitfield Diffie) и Мартином Хелманом (Martin Hellman), чтобы решить проблемы управления ключами. Данная концепция предусматривает, что каждое лицо получает два ключа: один, называемый открытым ключом, и другой, известный как частный ключ. Открытый ключ каждого лица подлежит публикации, в то время как частный ключ держится в

секрете. Необходимость для получателя и отправителя обмениваться секретной информацией устранена; при передаче всех данных задействованы только открытые ключи, причем частные ключи не подлежат передаче или совместному использованию. Более нет необходимости доверять какому-либо каналу связи, рискуя стать жертвой подслушивания или предательства. Единственное требование состоит в том, чтобы открытые ключи были связаны с пользователями надежным (аутентифицированным) способом (например в доверенном каталоге). Каждый может отправить конфиденциальное сообщение с помощью общедоступных сведений, но сообщение может быть расшифровано только с помощью частного ключа, которым обладает только уполномоченный получатель. Кроме того, криптографию с использованием общего ключа можно применять не только в целях конфиденциальности (шифрования), но также для аутентификации (цифровые подписи).

- **Цифровая подпись с открытым ключом:** Чтобы подписать сообщение, необходимо произвести вычисление с использованием как частного ключа, так и самого сообщения. Выходные данные называются цифровой подписью и прикрепляются к сообщению, которое затем отправляется. Второе лицо проверяет подпись, выполняя вычисление, включающее сообщение, означенную подпись и открытый ключ первого лица. Если результат соотносится с математической точки зрения, подпись признается подлинной. В противном случае, или подпись была сфальсифицирована, или сообщение было изменено.
- **Шифрование с помощью общего ключа:** Если одно лицо желает отправить секретное сообщение другому, отправитель ищет открытый ключ получателя в каталоге, использует его для шифрования сообщения, которое затем отправляет. Получатель затем использует частный ключ для расшифровки и чтения сообщения. Сообщение не может быть расшифровано путем прослушивания. Любой может отправить зашифрованное сообщение получателю, но только получатель сможет прочитать данное сообщение. Единственное требование состоит в том, что открытый ключ не должен содержать подсказок, позволяющих определить частный ключ.
- **Анализ трафика:** Анализ потоков сетевого трафика для получения информации, полезной для нарушителя. Например, частота передачи, идентификаторы взаимодействующих сторон, размеры пакетов, идентификаторы используемых потоков и т.д.

Предварительные сведения

В этом разделе рассматриваются некоторые основные Концепции шифрования Сетевого уровня. Это содержит аспекты шифрования, которые необходимо высматривать. Первоначально, эти проблемы могут не быть целесообразными вам, но это - хорошая идея перечитать их теперь и знать о них, потому что они будут иметь больше смысла после работы с шифрованием в течение нескольких месяцев.

- Следует отметить, что шифрование происходит только на выходных данных интерфейса, и расшифровка происходит только после ввода к интерфейсу. Это различие важно при планировании политики. Политика шифрования и расшифровка симметричны. Это означает, что определение того дает вам другой автоматически. С криптокартами и их связанными расширенными списками доступа, только явно определена политика шифрования.Политика расшифровки использует идентичную информацию, но когда соответствующие пакеты, это инвертирует адреса источника и

назначения и порты. Таким образом, данные защищены в обоих направлениях дуплексного соединения. Оператор *адреса X соответствия* в команде **криптокарты** используется для описания пакетов, оставляя интерфейс. Другими словами, это описывает шифрование пакетов. Однако с пакетами нужно также совпасть для расшифровки, поскольку они вводят интерфейс. Это сделано автоматически путем пересечения списка доступа с адресами источника и назначения и инвертированными портами. Это предоставляет симметрию для соединения. Список доступа, на который указывает **криптокарта**, должен описать трафик в одном (исходящем) направлении только. Пакеты IP, не совпадающие со списком доступа, который вы определяете, будут переданы, но не зашифрованы. "Запрещение" в списке доступа указывает, что с теми хостами нельзя совпасть, что означает, что они не будут зашифрованы. "Запрещение", в этом контексте, не означает, что отброшен пакет.

- Будьте очень осторожны в использовании слова "любой" в расширенных списках доступа. Использование "любых" причин ваш трафик, который будет отброшен, пока это не возглавляется к соответствию с "дешифровавшим" интерфейсом. Кроме того, с IPSec в программном обеспечении Cisco IOS версии 11.3(3)T, "любому" не разрешают.
- Использованию "любого" ключевого слова обескураживают в определении адресов источника или назначения. Определение "любого" может вызвать проблемы с протоколами маршрутизации, Протоколом NTP, эхом, ответом эха и многоадресным трафиком, поскольку принимающий маршрутизатор тихо сбрасывает от этого трафика. Если "кто-либо" должен использоваться, этим нужно предшествовать "опровергают" заявления для трафика, который не должен быть зашифрован, такие как "ntp".
- Чтобы сэкономить время, удостоверьтесь, что можно **пропинговать** равный маршрутизатор, с которым вы пытаетесь иметь связь шифрования. Кроме того, имейте конечные устройства (которые зависят от получения их зашифрованного трафика), пропинговывают друг друга перед расходами слишком большого количества времени, устраняя неправильную проблему. Другими словами, удостоверьтесь, что маршрутизация работает прежде, чем попытаться сделать **крипто-**. Удаленный узел может не иметь маршрута для исходящего интерфейса, в этом случае вы не в состоянии иметь сеанс с шифрованием с тем узлом (можно быть в состоянии использовать **ip, ненумерованный** на том последовательном интерфейсе).
- Много каналов типа точка-точка глобальной сети (WAN) используют адреса немаршрутизируемого IP - протоколы, и Шифрование программного обеспечения Cisco IOS версии 11.2 полагается на Протокол ICMP (подразумевать, что это использует IP-адрес выходного последовательного интерфейса для ICMP). Это может вынудить вас использовать **ip, ненумерованный** на Интерфейсе WAN. Всегда делайте **эхо-запрос** и **команду traceroute**, чтобы удостовериться, что маршрутизация существует для двух пирингов (шифрование/дешифрование) маршрутизаторы.
- Только двум маршрутизаторам позволяют совместно использовать ключ сеанса Диффи-Хеллмана. Т.е. один маршрутизатор не может обмениваться зашифрованными пакетами к двум узлам с помощью того же ключа сеанса; каждая пара маршрутизаторов должна иметь ключ сеанса, который является результатом Обмена Диффи-Хеллмана между ними.
- Ядро шифрования или в Cisco IOS, Cisco IOS VIP2, или в аппаратных средствах Адаптер сервисов шифрования (ESA) на VIP2. Без VIP2 ядро шифрования Cisco IOS управляет политикой шифрования на всех портах. На платформах с помощью VIP2 существуют множественные ядра шифрования: один в Cisco IOS, и один на каждом VIP2. Ядро шифрования на VIP2 управляет шифрованием на портах, которые находятся

на плате.
- Удостоверьтесь, что трафик собирается поступить в интерфейс, подготовленный зашифровать его. Если трафик может так или иначе поступить в интерфейс кроме того с примененной **криптокартой**, это тихо отброшено.
- Это помогает иметь консоль (или альтернатива) доступ к обоим маршрутизаторам при выполнении обмена ключами; возможно заставить пассивную сторону "зависать" при ожидании ключа.
- **cfb-64** более эффективен для обработки, чем **cfb-8** с точки зрения Загрузки ЦПУ.
- Маршрутизатор должен выполнять алгоритм, что вы хотите использовать с отзывом шифра (CFB) режим, который вы хотите использовать; настройки по умолчанию для каждого образа являются именем образа (такой как "56") с **cfb-64**.
- Рассмотрите изменение ключевого таймаута. 30-минутный по умолчанию очень короток. Попытайтесь увеличить его до одного дня (1440 минут).
- IP - трафик отброшен во время ключевого пересмотра каждый раз, когда ключ истекает.
- Выберите только трафик, который вы действительно хотите зашифровать (это сохраняет циклы ЦПУ).
- С технологией DDR сделайте ICMP содержательным, или это никогда не будет набирать.
- Если вы хотите зашифровать трафик кроме IP, используйте туннель. С туннелями примените криптокарты и к медосмотру и к туннельным интерфейсам. Посмотрите Выборку 5: Шифрование Трафика IPX в Туннеле IP для получения дополнительной информации.
- Два маршрутизатора одноранговое шифрования не должны напрямую подключаться.
- Маршрутизатор младшей модели может дать вам сообщение "захвата ЦПУ". Это может быть проигнорировано, потому что это говорит вам, что шифрование использует много ресурсов ЦПУ.
- Не размещайте маршрутизаторы шифрования избыточно так, чтобы вы дешифровали и повторно шифровали трафик и ненужный ЦП. Просто зашифруйте в этих двух оконечных точках. Посмотрите Выборку 3: Шифрование К и Через маршрутизатор для получения дополнительной информации.
- В настоящее время шифрование широковещания и пакетов групповой адресации не поддерживается. Если "безопасные" обновления маршрута важны для организации сети, протокол со встроенной аутентификацией должен использоваться, такие как Протокол EIGRP, Протокол OSPF или Версия 2 (RIPv2) Протокола RIP (Routing Information Protocol) для обеспечения целостности обновления.

Предупреждения

Примечание: Предупреждения, упомянутые ниже, были все решены.

- Маршрутизатор Cisco 7200 с помощью ESA для шифрования не может дешифровать пакет под одним ключом сеанса и затем повторно шифровать его под другим ключом сеанса. См. идентификатор ошибки Cisco CSCdj82613 (только зарегистрированные клиенты).
- Когда два маршрутизатора связаны зашифрованной выделенной линией и линией резервного ISDN, если выделенная линия понижается, соединение ISDN подходит прекрасное. Однако, когда выделенная линия возвращается снова, маршрутизатор, который разместил сбои вызова ISDN. См. идентификатор ошибки Cisco CSCdj00310

(только зарегистрированные клиенты).
- Для маршрутизаторов Cisco серии 7500 с несколько VIP, если **криптокарте** применяются к даже один интерфейс какого-либо VIP, одного или более катастрофических отказов VIP. См. идентификатор ошибки Cisco CSCdi88459 (только зарегистрированные клиенты).
- Для маршрутизаторов Cisco серии 7500 с VIP2 и ESA, **показ крипто-**команда **карты** не делает отображаемых выходных данных, пока пользователь не в консольном порту. См. идентификатор ошибки Cisco CSCdj89070 (только зарегистрированные клиенты).

Настройка шифрования сетевого уровня Cisco IOS

В данном документе рабочие примеры конфигураций Cisco IOS получены непосредственно с маршрутизатора, установленного в лаборатории. Единственное изменение, которое было произведено, – удаление конфигураций не используемых интерфейсов. Материал в данном разделе извлечен из доступных источников в Интернете или из раздела Дополнительные сведения в конце данного документа.

Все примеры конфигурации в этом документе от программного обеспечения Cisco IOS версии 11.3. Было несколько отличий от команд программного обеспечения Cisco IOS версии 11.2, таких как добавление следующих слов:

- dss в некоторых ключевых командах настройки.
- Cisco в некоторых **командах показа** и командах **криптокарты** для различения шифрование по собственному алгоритму Cisco (как найдено в программном обеспечении Cisco IOS версии 11.2 и позже) и IPSec, который находится в программном обеспечении Cisco IOS версии 11.3(2)T.

Примечание: IP-адреса, используемые в этих примерах конфигурации, были выбраны случайным образом в лабораторной работе Cisco и предназначены для непатентованного средства.

Шаг 1: Вручную генерируйте пары ключей DSS

Пара ключей DSS (открытый и закрытый ключ) должна вручную генерироваться на каждом маршрутизаторе, участвующем в сеансе с шифрованием. Другими словами, каждый маршрутизатор должен иметь свои собственные ключи DSS для участия. Устройство шифрования может иметь только один ключ DSS, который однозначно определяет его. Ключевое слово "dss" было добавлено в программном обеспечении Cisco IOS версии 11.3 для различения DSS от ключей RSA. Можно задать любое название для собственных ключей DSS маршрутизатора (невзирая на то, что, рекомендуется использовать имя хоста маршрутизатора). На менее мощном CPU (такие как серия Cisco 2500), генерация пары ключей занимает приблизительно 5 секунд или меньше.

Маршрутизатор генерирует пару ключей:

- Открытый ключ (который позже передан маршрутизаторам, участвующим в сеансах с шифрованием).
- Секретный ключ (который не замечают, ни обмениваются с кем-либо еще; фактически, это сохранено в отдельном разделе NVRAM, который не может быть просмотрен).

Как только пара ключей DSS маршрутизатора генерировалась, она уникально привязана к

ядру шифрования в том маршрутизаторе. Генерацию пары ключей показывают в примере вывода команды ниже.

```
dial-5(config)#crypto key generate dss dial5 Generating DSS keys .... [OK] dial-5#show crypto key mypubkey dss crypto public-key dial5 05679919 160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145 quit dial-5#show crypto engine configuration slot: 0 engine name: dial5 engine type: software serial number: 05679919 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 43 input queue bot: 43 input queue count: 0 dial-5#
```

Поскольку можно генерировать только одну пару ключей, которая определяет маршрутизатор, вы можете перезаписать свой исходный ключ и должны повторно передать ваш открытый ключ с каждым маршрутизатором в связи шифрования. Это показывают в примере вывода команды ниже:

```
StHelen(config)#crypto key generate dss barney % Generating new DSS keys will require re-exchanging public keys with peers who already have the public key named barney! Generate new DSS keys? [yes/no]: yes Generating DSS keys .... [OK] StHelen(config)# Mar 16 12:13:12.851: Crypto engine 0: create key pairs.
```

Шаг 2: Вручную измените открытые ключи DSS с одноранговыми узлами (нестандартное подключение)

Генерация собственной пары ключей DSS маршрутизатора является первым шагом в установлении установления сеанса с шифрованием. Следующий шаг должен обмениваться открытыми ключами с любым маршрутизатором. Можно ввести эти открытые ключи вручную первым вводом **команды show crypto mypubkey** для отображения открытого ключа DSS маршрутизатора. Вы тогда обмениваетесь этими открытыми ключами (по электронной почте, например) и, с **командой crypto key pubkey-chain dss**, вырезаете и вставить открытый ключ вашего равного маршрутизатора в маршрутизатор.

Можно также использовать **обмен криптографического ключа dss**, команда для имения маршрутизаторов обмениваются открытыми ключами автоматически. При использовании автоматического метода удостоверьтесь, что нет никаких **инструкций криптокарты** на интерфейсах, используемых для обмена ключами. **Ключ debug crypto** полезен здесь.

Примечание: Это - хорошая идея **пропинговать** ваш узел прежде, чем попытаться обмениваться ключами.

```
Loser#ping 19.19.19.20 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds: !!!!! Loser(config)#crypto key exchange dss passive Enter escape character to abort if connection does not complete. Wait for connection from peer[confirm] Waiting .... StHelen(config)#crypto key exchange dss 19.19.19.19 barney Public key for barney: Serial Number 05694352 Fingerprint 309E D1DE B6DA 5145 D034 Wait for peer to send a key[confirm] Public key for barney: Serial Number 05694352 Fingerprint 309E D1DE B6DA 5145 D034 Add this public key to the configuration? [yes/no]:yes Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes. Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes. Mar 16 12:16:45.099: CRYPTO-KE: Received 4 bytes. Mar 16 12:16:45.099: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:45.103: CRYPTO-KE: Received 6 bytes. Mar 16 12:16:45.103: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:45.107: CRYPTO-KE: Received 50 bytes. Mar 16 12:16:45.111: CRYPTO-KE: Received 14 bytes. Send peer a key in return[confirm] Which one? fred? [yes]: Public key for fred: Serial Number 02802219 Fingerprint 2963 05F9 ED55 576D CF9D Waiting .... Public key for fred: Serial Number 02802219 Fingerprint 2963 05F9 ED55 576D CF9D Add this public key to the configuration? [yes/no]: Loser(config)# Mar 16 12:16:55.339: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes. Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes. Loser(config)# Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes. Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes. Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.091: CRYPTO-
```

```
KE: Received 52 bytes. Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes. Add this public key to the configuration? [yes/no]: yes StHelen(config)#^Z StHelen#
```

Теперь, когда общими ключами DSS обменялись, удостоверьтесь, что оба маршрутизатора имеют открытые ключи друг друга и что они совпадают, как показано в выходных данных команды ниже.

```
Loser#show crypto key mypubkey dss crypto public-key fred 02802219 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E quit Loser#show crypto key pubkey-chain dss crypto public-key barney 05694352 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341 quit -------- StHelen#show crypto key mypubkey dss crypto public-key barney 05694352 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341 quit StHelen#show crypto key pubkey-chain dss crypto public-key fred 02802219 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E quit
```

Пример 1: Конфигурация Cisco IOS для выделенного соединения

После того, как ключи DSS генерировались на каждом маршрутизаторе, и открытыми ключами DSS обменялись, команда **криптокарты** может быть применена к интерфейсу. Сеанс шифрования начинается путем генерирования трафика, который совпадает со списком доступа, используемым криптокартами.

```
Loser#write terminal Building configuration... Current configuration: ! ! Last configuration change at 13:01:18 UTC Mon Mar 16 1998 ! NVRAM config last updated at 13:03:02 UTC Mon Mar 16 1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption ! hostname Loser ! enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0 ! ip subnet-zero no ip domain-lookup crypto map oldstyle 10 set peer barney match address 133 ! crypto key pubkey-chain dss named-key barney serial-number 05694352 key-string B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341 quit ! interface Ethernet0 ip address 40.40.40.41 255.255.255.0 no ip mroute-cache ! interface Serial0 ip address 18.18.18.18 255.255.255.0 encapsulation ppp no ip mroute-cache shutdown ! interface Serial1 ip address 19.19.19.19 255.255.255.0 encapsulation ppp no ip mroute-cache clockrate 2400 no cdp enable crypto map oldstyle ! ip default-gateway 10.11.19.254 ip classless ip route 0.0.0.0 0.0.0.0 19.19.19.20 access-list 133 permit ip 40.40.40.0 0.0.0.255 30.30.30.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 no exec transport input all line vty 0 4 password ww login ! end Loser# ------------------------- StHelen#write terminal Building configuration... Current configuration: ! ! Last configuration change at 13:03:05 UTC Mon Mar 16 1998 ! NVRAM config last updated at 13:03:07 UTC Mon Mar 16 1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption ! hostname StHelen ! boot system flash c2500-is56-l enable password ww ! partition flash 2 8 8 ! no ip domain-lookup crypto map oldstyle 10 set peer fred match address 144 ! crypto key pubkey-chain dss named-key fred serial-number 02802219 key-string 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E quit ! ! interface Ethernet0 ip address 30.30.30.31 255.255.255.0 ! interface Ethernet1 no ip address shutdown ! interface Serial0 no ip address encapsulation x25 no ip mroute-cache shutdown ! interface Serial1 ip address 19.19.19.20 255.255.255.0 encapsulation ppp no ip mroute-cache load-interval 30 compress stac no cdp enable crypto map oldstyle ! ip default-gateway 10.11.19.254 ip classless ip route 0.0.0.0 0.0.0.0 19.19.19.19 access-list 144 permit ip 30.30.30.0 0.0.0.255 40.40.40.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 transport input all line vty 0 4 password ww login ! end StHelen#
```

Пример 2: Конфигурация Cisco IOS для многоточечной сети Frame Relay

Следующий пример вывода команды был взят от Маршрутизатора концентратора.

```
Loser#write terminal Building configuration... Current configuration: ! ! Last configuration change at 10:45:20 UTC Wed Mar 11 1998 ! NVRAM config last updated at 18:28:27 UTC Tue Mar 10 1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption ! hostname Loser ! enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0 ! ip subnet-zero no ip domain-
```

```
lookup ! crypto map oldstuff 10 set peer barney match address 133 crypto map oldstuff 20 set
peer wilma match address 144 ! crypto key pubkey-chain dss named-key barney serial-number
05694352 key-string 1D460DC3 BDC73312 93B7E220 1861D55C E00DA5D8 DB2B04CD FABD297C 899D40E7
D284F07D 6EEC83B8 E3676EC2 D813F7C8 F532DC7F 0A9913E7 8A6CB7E9 BE18790D quit named-key wilma
serial-number 01496536 key-string C26CB3DD 2A56DD50 CC2116C9 2697CE93 6DBFD824 1889F791 9BF36E70
7B29279C E343C56F 32266443 989B4528 1CF32C2D 9E3F2447 A5DBE054 879487F6 26A55939 quit ! crypto
cisco pregen-dh-pairs 5 ! crypto cisco key-timeout 1440 ! interface Ethernet0 ip address
190.190.190.190 255.255.255.0 no ip mroute-cache ! interface Serial1 ip address 19.19.19.19
255.255.255.0 encapsulation frame-relay no ip mroute-cache clockrate 500000 crypto map oldstuff
! ! ip default-gateway 10.11.19.254 ip classless ip route 200.200.200.0 255.255.255.0
19.19.19.20 ip route 210.210.210.0 255.255.255.0 19.19.19.21 access-list 133 permit ip
190.190.190.0 0.0.0.255 200.200.200.0 0.0.0.255 access-list 144 permit ip 190.190.190.0
0.0.0.255 210.210.210.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 no exec transport
input all line vty 0 4 password ww login ! end Loser#
```

Следующий пример вывода команды был взят от Удаленного Узла A.

```
WAN-2511a#write terminal Building configuration... Current configuration: ! version 11.3 no
service password-encryption ! hostname WAN-2511a ! enable password ww ! no ip domain-lookup !
crypto map mymap 10 set peer fred match address 133 ! crypto key pubkey-chain dss named-key fred
serial-number 02802219 key-string 56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592
021B295D D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436 quit !
interface Ethernet0 ip address 210.210.210.210 255.255.255.0 shutdown ! interface Serial0 ip
address 19.19.19.21 255.255.255.0 encapsulation frame-relay no fair-queue crypto map mymap ! ip
default-gateway 10.11.19.254 ip classless ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 133 permit ip 210.210.210.0 0.0.0.255 190.190.190.0 0.0.0.255 ! line con 0 exec-
timeout 0 0 line 1 no exec transport input all line 2 16 no exec line aux 0 line vty 0 4
password ww login ! end WAN-2511a#
```

Следующий пример вывода команды был взят от Удаленного Узла B.

```
StHelen#write terminal Building configuration... Current configuration: ! ! Last configuration
change at 19:00:34 UTC Tue Mar 10 1998 ! NVRAM config last updated at 18:48:39 UTC Tue Mar 10
1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption !
hostname StHelen ! boot system flash c2500-is56-l enable password ww ! partition flash 2 8 8 !
no ip domain-lookup ! crypto map wabba 10 set peer fred match address 144 ! crypto key pubkey-
chain dss named-key fred serial-number 02802219 key-string 56841777 4F27A574 5005E0F0 CF3C33F5
C6AAD000 5518A8FF 7422C592 021B295D D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D
0256EFF5 0EE89436 quit ! interface Ethernet0 ip address 200.200.200.200 255.255.255.0 !
interface Serial1 ip address 19.19.19.20 255.255.255.0 encapsulation frame-relay no ip mroute-
cache crypto map wabba ! ip default-gateway 10.11.19.254 ip classless ip route 190.190.190.0
255.255.255.0 19.19.19.19 access-list 144 permit ip 200.200.200.0 0.0.0.255 190.190.190.0
0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 transport input all line vty 0 4 password ww
login ! end StHelen#
```

Следующий пример вывода команды был взят от Коммутатора Frame Relay.

```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname wan-4700a
!
enable password ww
!
no ip domain-lookup
frame-relay switching
!
interface Serial0
 no ip address
 encapsulation frame-relay
 clockrate 500000
```

```
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 100
!
interface Serial1
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 100 interface Serial0 200
 frame-relay route 300 interface Serial2 200
!
interface Serial2
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 300
!
```

Пример 3: Входное и сквозное шифрование маршрутизатора

Равные маршрутизаторы не должны быть одним переходом далеко. Можно создать сеанс с равноправным участием с удаленным маршрутизатором. В следующем примере цель состоит в том, чтобы зашифровать весь сетевой трафик между 180.180.180.0/24 и 40.40.40.0/24 и между 180.180.180.0/24 и 30.30.30.0/24. Нет никакого беспокойства с зашифрованным трафиком между 40.40.40.0/24 и 30.30.30.0/24.

wan-4500b маршрутизатора имеет установление сеанса с шифрованием с Проигравшим и также с StHelen. Путем шифрования трафика от бледного-4500b's Сегмента Ethernet до Сегмента Ethernet StHelen ' s вы избегаете ненужного шага расшифровки в Проигравшего. Проигравший просто передает зашифрованный поток данных на последовательный интерфейс StHelen ' s, где это дешифровано. Это уменьшает задержку трафика для пакетов IP и циклов ЦПУ на маршрутизаторе Loser. Что еще более важно, это значительно увеличивает безопасность системы, так как eavesdropper в Проигравшем не может считать трафик. Если бы Проигравший дешифровал трафик, то был бы шанс, что могли быть отклонены дешифрованные данные.

```
[wan-4500b]<Ser0>--   ---<Ser0> [Loser] <Ser1>--   ----<Ser1>[StHelen]
             |                              |                            |
             |                              |                            |
           -----                         -------                      -------
          180.180.180/24                 40.40.40/24                 30.30.30/24 wan-4500b#write
terminal Building configuration... Current configuration: ! version 11.3 no service password-
encryption ! hostname wan-4500b ! enable password 7 111E0E ! username cse password 0 ww no ip
domain-lookup ! crypto map toworld 10 set peer loser match address 133 crypto map toworld 20 set
peer sthelen match address 144 ! crypto key pubkey-chain dss named-key loser serial-number
02802219 key-string F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24 quit named-key sthelen
serial-number 05694352 key-string 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB
D3964C10 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618 quit !
interface Ethernet0 ip address 180.180.180.180 255.255.255.0 ! interface Serial0 ip address
18.18.18.19 255.255.255.0 encapsulation ppp crypto map toworld ! router rip network 18.0.0.0
network 180.180.0.0 ! ip classless ip route 0.0.0.0 0.0.0.0 30.30.30.31 ip route 171.68.118.0
255.255.255.0 10.11.19.254 access-list 133 permit ip 180.180.180.0 0.0.0.255 40.40.40.0
0.0.0.255 access-list 144 permit ip 180.180.180.0 0.0.0.255 30.30.30.0 0.0.0.255 ! line con 0
exec-timeout 0 0 line aux 0 password 7 044C1C line vty 0 4 login local ! end wan-4500b# --------
------------ Loser#write terminal Building configuration... Current configuration: ! ! Last
configuration change at 11:01:54 UTC Wed Mar 18 1998 ! NVRAM config last updated at 11:09:59 UTC
Wed Mar 18 1998 ! version 11.3 service timestamps debug datetime msec no service password-
encryption ! hostname Loser ! enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0 ! ip subnet-zero no
ip domain-lookup ip host StHelen.cisco.com 19.19.19.20 ip domain-name cisco.com ! crypto map
```

towan 10 set peer wan match address 133 ! crypto key pubkey-chain dss named-key wan serial-number 07365004 key-string A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit ! interface Ethernet0 ip address 40.40.40.40 255.255.255.0 no ip mroute-cache ! interface Serial0 ip address 18.18.18.18 255.255.255.0 encapsulation ppp no ip mroute-cache clockrate 64000 crypto map towan ! interface Serial1 ip address 19.19.19.19 255.255.255.0 encapsulation ppp no ip mroute-cache priority-group 1 clockrate 64000 ! ! router rip network 19.0.0.0 network 18.0.0.0 network 40.0.0.0 ! ip default-gateway 10.11.19.254 ip classless access-list 133 permit ip 40.40.40.0 0.0.0.255 180.180.180.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 no exec transport input all line vty 0 4 password ww login ! end Loser# ------------------------ StHelen#**write terminal** Building configuration... Current configuration: ! ! Last configuration change at 11:13:18 UTC Wed Mar 18 1998 ! NVRAM config last updated at 11:21:30 UTC Wed Mar 18 1998 ! version 11.3 service timestamps debug datetime msec no service password-encryption ! hostname StHelen ! boot system flash c2500-is56-l enable password ww ! partition flash 2 8 8 ! no ip domain-lookup ! crypto map towan 10 set peer wan match address 144 ! crypto key pubkey-chain dss named-key wan serial-number 07365004 key-string A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit ! interface Ethernet0 no ip address ! interface Ethernet1 ip address 30.30.30.30 255.255.255.0 ! interface Serial1 ip address 19.19.19.20 255.255.255.0 encapsulation ppp no ip mroute-cache load-interval 30 crypto map towan ! router rip network 30.0.0.0 network 19.0.0.0 ! ip default-gateway 10.11.19.254 ip classless access-list 144 permit ip 30.30.30.0 0.0.0.255 180.180.180.0 0.0.0.255 ! line con 0 exec-timeout 0 0 line aux 0 transport input all line vty 0 4 password ww login ! end StHelen# ------------------------- wan-4500b#**show crypto cisco algorithms** des cfb-64 40-bit-des cfb-64 wan-4500b#**show crypto cisco key-timeout** Session keys will be re-negotiated every 30 minutes wan-4500b#**show crypto cisco pregen-dh-pairs** Number of pregenerated DH pairs: 0 wan-4500b#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 1 Serial0 18.18.18.19 set DES_56_CFB64 1683 1682 5 Serial0 18.18.18.19 set DES_56_CFB64 1693 1693 wan-4500b#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count Serial0 18.18.18.19 52 wan-4500b#**show crypto engine configuration** slot: 0 engine name: wan engine type: software serial number: 07365004 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 303 input queue bot: 303 input queue count: 0 wan-4500b#**show crypto key mypubkey dss** crypto public-key wan 07365004 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit wan-4500b#**show crypto key pubkey-chain dss** crypto public-key loser 02802219 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24 quit crypto public-key sthelen 05694352 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618 quit wan-4500b#**show crypto map interface serial 1** No crypto maps found. wan-4500b#**show crypto map** Crypto Map "toworld" 10 cisco Connection Id = 1 (1 established, 0 failed) Peer = loser PE = 180.180.180.0 UPE = 40.40.40.0 Extended IP access list 133 access-list 133 permit ip source: addr = 180.180.180.0/0.0.0.255 dest: addr = 40.40.40.0/0.0.0.255 Crypto Map "toworld" 20 cisco Connection Id = 5 (1 established, 0 failed) Peer = sthelen PE = 180.180.180.0 UPE = 30.30.30.0 Extended IP access list 144 access-list 144 permit ip source: addr = 180.180.180.0/0.0.0.255 dest: addr = 30.30.30.0/0.0.0.255 wan-4500b# ------------------------- Loser#**show crypto cisco algorithms** des cfb-64 des cfb-8 40-bit-des cfb-64 40-bit-des cfb-8 Loser#**show crypto cisco key-timeout** Session keys will be re-negotiated every 30 minutes Loser#**show crypto cisco pregen-dh-pairs** Number of pregenerated DH pairs: 10 Loser#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 61 Serial0 18.18.18.18 set DES_56_CFB64 1683 1682 Loser#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count Serial0 18.18.18.18 1 Serial1 19.19.19.19 90 Loser#**show crypto engine configuration** slot: 0 engine name: loser engine type: software serial number: 02802219 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 235 input queue bot: 235 input queue count: 0 Loser#**show crypto key mypubkey dss** crypto public-key loser 02802219 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24 quit Loser#**show crypto key pubkey-chain dss** crypto public-key wan 07365004 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit Loser#**show crypto map interface serial 1** No crypto maps found. Loser#**show crypto map** Crypto Map "towan" 10 cisco Connection Id = 61 (0 established, 0 failed) Peer = wan PE = 40.40.40.0 UPE = 180.180.180.0 Extended IP access list 133 access-list 133 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 180.180.180.0/0.0.0.255 Loser# ------------------------ ----------------- StHelen#**show crypto cisco algorithms** des cfb-64 StHelen#**show crypto cisco key-timeout** Session keys will be re-negotiated every 30 minutes StHelen#**show crypto cisco pregen-dh-**

pairs Number of pregenerated DH pairs: 10 StHelen#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 58 Serial1 19.19.19.20 set DES_56_CFB64 1694 1693 StHelen#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count Ethernet0 0.0.0.0 1 Serial1 19.19.19.20 80 StHelen#**show crypto engine configuration** slot: 0 engine name: sthelen engine type: software serial number: 05694352 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 220 input queue bot: 220 input queue count: 0 StHelen#**show crypto key mypubkey dss** crypto public-key sthelen 05694352 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618 quit StHelen#**show crypto key pubkey-chain dss** crypto public-key wan 07365004 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B quit StHelen#**show crypto map interface serial 1** Crypto Map "towan" 10 cisco Connection Id = 58 (1 established, 0 failed) Peer = wan PE = 30.30.30.0 UPE = 180.180.180.0 Extended IP access list 144 access-list 144 permit ip source: addr = 30.30.30.0/0.0.0.255 dest: addr = 180.180.180.0/0.0.0.255 StHelen#**show crypto map** Crypto Map "towan" 10 cisco Connection Id = 58 (1 established, 0 failed) Peer = wan PE = 30.30.30.0 UPE = 180.180.180.0 Extended IP access list 144 access-list 144 permit ip source: addr = 30.30.30.0/0.0.0.255 dest: addr = 180.180.180.0/0.0.0.255 StHelen#

Выборка 4: Криптография с DDR

Поскольку Cisco IOS полагается на ICMP для установления сеансов с шифрованием, трафик ICMP должен быть классифицирован как "содержательный" в списке номеронабирателя при выполнении шифрования по соединению DDR.

Примечание: Сжатие действительно работает в программном обеспечении Cisco IOS версии 11.3, но это не очень userful для зашифрованных данных. Поскольку зашифрованные данные довольно случайно выглядят, сжатие только замедляет вещи. Но можно оставить функцию на для незашифрованного трафика.

В некоторых ситуациях вы захотите резервирование коммутируемыми каналами к тому жю маршрутизатор. Например, когда пользователи хотят защитить против сбоя отдельного соединения в их глобальных сетях (WAN), это - usefuel. Если два интерфейса переходят к тому же узлу, та же криптокарта может использоваться на обоих интерфейсах. Резервный интерфейс должен использоваться для этой функции для функционирования должным образом. Если резервный дизайн имеет набор маршрутизатора в другую коробку, другие криптокарты должны быть созданы и одноранговый набор соответственно. Снова, **команда резервного интерфейса** должна использоваться.

dial-5#**write terminal** Building configuration... Current configuration: ! version 11.3 no service password-encryption service udp-small-servers service tcp-small-servers ! hostname dial-5 ! boot system c1600-sy56-l 171.68.118.83 enable secret 5 1oNe1wDbhBdcN6x9Y5gfuMjqh10 ! username dial-6 password 0 cisco isdn switch-type basic-ni1 ! crypto map dial6 10 set peer dial6 match address 133 ! crypto key pubkey-chain dss named-key dial6 serial-number 05679987 key-string 753F71AB E5305AD4 3FCDFB6D 47AA2BB5 656BFCAA 53DBE37F 07465189 06E91A82 2BC91236 13DC4AA8 7EC5B48C D276E5FE 0D093014 6D3061C5 03158820 B609CA7C quit ! interface Ethernet0 ip address 20.20.20.20 255.255.255.0 ! interface BRI0 ip address 10.10.10.11 255.255.255.0 encapsulation ppp no ip mroute-cache load-interval 30 dialer idle-timeout 9000 dialer map ip 10.10.10.10 name dial-6 4724118 dialer hold-queue 40 dialer-group 1 isdn spid1 919472417100 4724171 isdn spid2 919472417201 4724172 compress stac ppp authentication chap ppp multilink crypto map dial6 ! ip classless ip route 40.40.40.0 255.255.255.0 10.10.10.10 access-list 133 permit ip 20.20.20.0 0.0.0.255 40.40.40.0 0.0.0.255 dialer-list 1 protocol ip permit ! line con 0 exec-timeout 0 0 line vty 0 4 password ww login ! end dial-5# ---------- dial-6#**write terminal** Building configuration... Current configuration: ! version 11.3 no service password-encryption service udp-small-servers service tcp-small-servers ! hostname dial-6 ! boot system c1600-sy56-l 171.68.118.83 enable secret 5 1VdPYuA/BIVeEm9UAFEm.PPJFc. ! username dial-5 password 0 cisco no ip domain-lookup isdn switch-type basic-ni1 ! crypto map dial5 10 set peer dial5 match address 144 ! crypto key pubkey-chain dss named-key dial5 serial-number 05679919 key-string 160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145 quit ! ! interface Ethernet0 ip address

```
40.40.40.40 255.255.255.0 ! interface BRI0 ip address 10.10.10.10 255.255.255.0 encapsulation
ppp no ip mroute-cache dialer idle-timeout 9000 dialer map ip 10.10.10.11 name dial-5 4724171
dialer hold-queue 40 dialer load-threshold 5 outbound dialer-group 1 isdn spid1 919472411800
4724118 isdn spid2 919472411901 4724119 compress stac ppp authentication chap ppp multilink
crypto map dial5 ! ip classless ip route 20.20.20.0 255.255.255.0 10.10.10.11 access-list 144
permit ip 40.40.40.0 0.0.0.255 20.20.20.0 0.0.0.255 dialer-list 1 protocol ip permit ! line con
0 exec-timeout 0 0 line vty 0 4 password ww login ! end dial-6#
```

Выборка 5: Шифрование IPX-трафика в IP-туннеле

В данном примере зашифрован трафик IPX в туннеле IP.

Примечание: Только трафик в этом туннеле (IPX) зашифрован. Весь другой IP - трафик оставлен в покое.

```
WAN-2511a#write terminal Building configuration... Current configuration: ! version 11.2 no
service password-encryption no service udp-small-servers no service tcp-small-servers ! hostname
WAN-2511a ! enable password ww ! no ip domain-lookup ipx routing 0000.0c34.aa6a ! crypto public-
key wan2516 01698232 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962 quit ! crypto map
wan2516 10 set peer wan2516 match address 133 ! ! interface Loopback1 ip address 50.50.50.50
255.255.255.0 ! interface Tunnel1 no ip address ipx network 100 tunnel source 50.50.50.50 tunnel
destination 60.60.60.60 crypto map wan2516 ! interface Ethernet0 ip address 40.40.40.40
255.255.255.0 ipx network 600 ! interface Serial0 ip address 20.20.20.21 255.255.255.0
encapsulation ppp no ip mroute-cache crypto map wan2516 ! interface Serial1 no ip address
shutdown ! ip default-gateway 10.11.19.254 ip classless ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit ip host 50.50.50.50 host 60.60.60.60 ! line con 0 exec-timeout 0 0
password ww login line 1 16 line aux 0 password ww login line vty 0 4 password ww login ! end
WAN-2511a# ---------- WAN-2516a#write terminal Building configuration... Current
configuration: ! version 11.2 no service pad no service password-encryption service udp-small-
servers service tcp-small-servers ! hostname WAN-2516a ! enable password ww ! no ip domain-
lookup ipx routing 0000.0c3b.cc1e ! crypto public-key wan2511 01496536 C8EA7C21 DF3E48F5
C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D 5646DC78 DDC77EFC 823F302A F112AF97
668E39A1 E2FCDC05 545E0529 9B3C9553 quit ! crypto map wan2511 10 set peer wan2511 match address
144 ! ! hub ether 0 1 link-test auto-polarity ! ! <other hub interfaces snipped> ! hub ether 0
14 link-test auto-polarity ! interface Loopback1 ip address 60.60.60.60 255.255.255.0 !
interface Tunnel1 no ip address ipx network 100 tunnel source 60.60.60.60 tunnel destination
50.50.50.50 crypto map wan2511 ! interface Ethernet0 ip address 30.30.30.30 255.255.255.0 ipx
network 400 ! interface Serial0 ip address 20.20.20.20 255.255.255.0 encapsulation ppp clockrate
2000000 crypto map wan2511 ! interface Serial1 no ip address shutdown ! interface BRI0 no ip
address shutdown ! ip default-gateway 20.20.20.21 ip classless ip route 0.0.0.0 0.0.0.0
20.20.20.21 access-list 144 permit ip host 60.60.60.60 host 50.50.50.50 access-list 188 permit
gre any any ! line con 0 exec-timeout 0 0 password ww login line aux 0 password ww login modem
InOut transport input all flowcontrol hardware line vty 0 4 password ww login ! end WAN-2516a# -
---------- WAN-2511a#show ipx route Codes: C - Connected primary network, c -
Connected secondary network S - Static, F - Floating static, L - Local (internal), W - IPXWAN R
- RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate s - seconds, u - uses 3 Total IPX
routes. Up to 1 parallel paths and 16 hops allowed. No default route known. C 100 (TUNNEL), Tu1
C 600 (NOVELL-ETHER), Et0 R 400 [151/01] via 100.0000.0c3b.cc1e, 24s, Tu1 WAN-2511a#show crypto
engine connections active ID Interface IP-Address State Algorithm Encrypt Decrypt 1 Serial0
20.20.20.21 set DES_56_CFB64 207 207 WAN-2511a#ping 400.0000.0c3b.cc1e Translating
"400.0000.0c3b.cc1e" Type escape sequence to abort. Sending 5, 100-byte IPX cisco Echoes to
400.0000.0c3b.cc1e, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip
min/avg/max = 32/35/48 ms WAN-2511a#show crypto engine connections active ID Interface IP-
Address State Algorithm Encrypt Decrypt 1 Serial0 20.20.20.21 set DES_56_CFB64 212 212 WAN-
2511a#ping 30.30.30.30 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to
30.30.30.30, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip
min/avg/max = 4/5/8 ms WAN-2511a#show crypto engine connections active ID Interface IP-Address
State Algorithm Encrypt Decrypt 1 Serial0 20.20.20.21 set DES_56_CFB64 212 212 WAN-2511a#
```

Выборка 6: Шифрование туннелей L2F

В данном примере, только шифруя трафик L2F для пользователей, набирающих в, предпринят. Здесь, "user@cisco.com" вызывает Сервер доступа к локальной сети (NAS) названный "DEMO2" в их городе и туннелирован к CD домашнего шлюза. Весь трафик DEMO2 (наряду с тем из других абонентов L2F) зашифрован. Поскольку L2F использует порт 1701 UDP, это - то, как список доступа создан, определив, какой трафик зашифрован.

Примечание: Если связь шифрования уже не установлена, подразумевая, что абонент является первым человеком, который призовет и создаст туннель L2F, абонент может быть отброшен из-за задержки устанавливания связи шифрования. Это может не произойти на маршрутизаторах с достаточным количеством Питания ЦПУ. Кроме того, можно хотеть увеличить **keytimeout** так, чтобы настройка шифрования и разрушение только произошли в течение непиковый часов.

Следующий пример вывода команды был взят от удаленного NAS.

```
DEMO2#write terminal Building configuration... Current configuration: ! version 11.2 no service
password-encryption no service udp-small-servers no service tcp-small-servers ! hostname DEMO2 !
enable password ww ! username NAS1 password 0 SECRET username HomeGateway password 0 SECRET no
ip domain-lookup vpdn enable vpdn outgoing cisco.com NAS1 ip 20.20.20.20 ! crypto public-key
wan2516 01698232 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962 quit ! crypto map vpdn
10 set peer wan2516 match address 133 ! crypto key-timeout 1440 ! interface Ethernet0 ip address
40.40.40.40 255.255.255.0 ! interface Serial0 ip address 20.20.20.21 255.255.255.0 encapsulation
ppp no ip mroute-cache crypto map vpdn ! interface Serial1 no ip address shutdown ! interface
Group-Async1 no ip address encapsulation ppp async mode dedicated no peer default ip address no
cdp enable ppp authentication chap pap group-range 1 16 ! ip default-gateway 10.11.19.254 ip
classless ip route 0.0.0.0 0.0.0.0 20.20.20.20 access-list 133 permit udp host 20.20.20.21 eq
1701 host 20.20.20.20 eq 1701 ! ! line con 0 exec-timeout 0 0 password ww login line 1 16 modem
InOut transport input all speed 115200 flowcontrol hardware line aux 0 login local modem InOut
transport input all flowcontrol hardware line vty 0 4 password ww login ! end DEMO2#
```

Следующий пример вывода команды был взят от Домашнего шлюза.

```
CD#write terminal Building configuration... Current configuration: ! version 11.2 no service pad
no service password-encryption service udp-small-servers service tcp-small-servers ! hostname CD
! enable password ww ! username NAS1 password 0 SECRET username HomeGateway password 0 SECRET
username user@cisco.com password 0 cisco no ip domain-lookup vpdn enable vpdn incoming NAS1
HomeGateway virtual-template 1 ! crypto public-key wan2511 01496536 C8EA7C21 DF3E48F5 C6C069DB
3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1
E2FCDC05 545E0529 9B3C9553 quit ! crypto key-timeout 1440 ! crypto map vpdn 10 set peer wan2511
match address 144 ! ! hub ether 0 1 link-test auto-polarity ! interface Loopback0 ip address
70.70.70.1 255.255.255.0 ! interface Ethernet0 ip address 30.30.30.30 255.255.255.0 ! interface
Virtual-Template1 ip unnumbered Loopback0 no ip mroute-cache peer default ip address pool
default ppp authentication chap ! interface Serial0 ip address 20.20.20.20 255.255.255.0
encapsulation ppp clockrate 2000000 crypto map vpdn ! interface Serial1 no ip address shutdown !
interface BRI0 no ip address shutdown ! ip local pool default 70.70.70.2 70.70.70.77 ip default-
gateway 20.20.20.21 ip classless ip route 0.0.0.0 0.0.0.0 20.20.20.21 access-list 144 permit udp
host 20.20.20.20 eq 1701 host 20.20.20.21 eq 1701 ! line con 0 exec-timeout 0 0 password ww
login line aux 0 password ww login modem InOut transport input all flowcontrol hardware line vty
0 4 password ww login ! end
```

Устранение неисправностей

Обычно лучше начать каждый сеанс устранения проблем путем собирания информации с помощью следующих **команд показа**. Символ "звездочка" (*) указывает на особенно полезную команду. Дополнительные сведения см. в разделе Устранение проблем IP-безопасности — общие сведения и использование команд отладки.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику

выходных данных команды show.

Примечание: Прежде чем применять команды отладки, ознакомьтесь с разделом "Важные сведения о командах отладки".

Команды	
покажите крипто-cisco algorithm	покажите крипто-ключевой таймаут Cisco
покажите крипто-Pregen-dh-pairs Cisco	show crypto engine connections active
show crypto engine connections dropped-packet	show crypto engine configuration
show crypto key mypubkey dss	* pubkey-цепочка show crypto key dss
interface serial 1 карты покажите крипто-	* карта покажите крипто-
debug crypto engine	debug crypto sess
отладьте ключ крика	clear crypto connection
crypto zeroize	никакой крипто-общий ключ

- **покажите крипто-cisco algorithm**- Необходимо включить все алгоритмы Стандарта шифрования данных (DES), которые используются для передачи с любым другим одноранговым маршрутизатором шифрования. Если вы не включите алгоритм DES, то вы не будете в состоянии использовать тот алгоритм, даже при попытке назначить алгоритм на **криптокарту** в более позднее время.Если ваш маршрутизатор пытается установить сеанс с зашифрованным обменом данными с равным маршрутизатором, и этим двум маршрутизаторам не включили тот же алгоритм DES в обоих концах, сбоях шифрованного сеанса. Если по крайней мере один общий алгоритм DES включен в обоих концах, шифрованный сеанс может продолжиться.**Примечание:** Дополнительный Cisco слова обнаруживается в программном обеспечении Cisco IOS версии 11.3 и необходим для различения IPSec и шифрование по собственному алгоритму Cisco, найденное в программном обеспечении Cisco IOS версии 11.2.`Loser#`**`show crypto cisco algorithms`** `des cfb-64 des cfb-8 40-bit-des cfb-64 40-bit-des cfb-8`
- **покажите крипто-ключевой таймаут Cisco** - После того, как сеанс с зашифрованным обменом данными установлен, это допустимо в течение определенного промежутка времени. После этого промежутка времени, времен сеанса. О новом сеансе нужно выполнить согласование, и новый DES (сеанс), ключ должен генерироваться для зашифрованного подключения для продолжения. Используйте эту команду для изменения времени, когда сеанс с зашифрованным обменом данными длится, прежде чем это истечет (испытывает таймаут).`Loser#`**`show crypto cisco key-timeout`** `Session keys will be re-negotiated every 30 minutes` Используйте эти команды для определения промежутка времени, прежде чем будут пересмотрены ключи DES.`StHelen#`**`show crypto conn`** `Connection Table PE UPE Conn_id New_id Algorithm Time 0.0.0.1 0.0.0.1 4 0 DES_56_CFB64 Mar 01 1993 03:16:09 flags:TIME_KEYS StHelen#`**`show crypto key`** `Session keys will be re-negotiated every 30 minutes StHelen#`**`show clock`** `*03:21:23.031 UTC Mon Mar 1 1993`
- **покажите крипто-Pregen-dh-pairs Cisco** - Каждый шифрованный сеанс использует уникальную пару номеров DH. Каждый раз, когда новый сеанс установлен, новые пары номеров DH должны генерироваться. Когда сеанс завершает, от этих номеров

сбрасывают. Генерация новых пар номеров DH с высокой загрузкой ЦПУ действие, которое может сделать настройку сеанса медленной, специально для маршрутизаторов младшей модели.Для ускорения настройки сеанса можно принять решение иметь определенное количество пар номеров DH, предварительно генерируемых и проводимых в резерве. Затем когда сеанс с зашифрованным обменом данными устанавливается, пара номеров DH предоставлена от того резерва. После того, как пара номеров DH используется, резерв автоматически пополнен новой парой номеров DH, так, чтобы всегда была готовая к употреблению пара номеров DH.Обычно не необходимо иметь несколько или две предварительно генерируемые пары номеров DH, пока ваш маршрутизатор не устанавливает множественные шифрованные сеансы так часто, что предварительно генерируемый резерв одной или двух пар номеров DH истощен слишком быстро.Loser#**show crypto cisco pregen-dh-pairs** Number of pregenerated DH pairs: 10

- активные соединения Cisco покажите крипто-Ниже приведен пример выходных данных команды.Loser#**show crypto engine connections active** ID Interface IP-Address State Algorithm Encrypt Decrypt 16 Serial1 19.19.19.19 set DES_56_CFB64 376 884
- покажите крипто-dropped-packet engine connection CiscoНиже приведен пример выходных данных команды.Loser#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count Serial1 19.19.19.19 39
- конфигурация show crypto engine (был show crypto engine brief в программном обеспечении Cisco IOS версии 11.2.)Ниже приведен пример выходных данных команды.Loser#**show crypto engine configuration** slot: 0 engine name: fred engine type: software serial number: 02802219 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 465 input queue bot: 465 input queue count: 0
- show crypto key mypubkey dssНиже приведен пример выходных данных команды.Loser#**show crypto key mypubkey dss** crypto public-key fred 02802219 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E quit
- pubkey-цепочка show crypto key dssНиже приведен пример выходных данных команды.Loser#**show crypto key pubkey-chain dss** crypto public-key barney 05694352 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341 quit
- interface serial 1 карты покажите крипто-Ниже приведен пример выходных данных команды.Loser#**show crypto map interface serial 1** Crypto Map "oldstyle" 10 cisco Connection Id = 16 (8 established, 0 failed) Peer = barney PE = 40.40.40.0 UPE = 30.30.30.0 Extended IP access list 133 access-list 133 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 30.30.30.0/0.0.0.255 Обратите внимание на несоизмеримость времени при использовании команды ping.wan-5200b#**ping 30.30.30.30** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms wan-5200b# ---------- wan-5200b#**ping 30.30.30.31** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 30.30.30.31, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms ---------- wan-5200b#**ping 19.19.19.20** Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds: !!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms ----------
- interface serial 1 карты покажите крипто-Ниже приведен пример выходных данных команды.Loser#**show crypto map** Crypto Map "oldstyle" 10 cisco Connection Id = 16 (8 established, 0 failed) Peer = barney PE = 40.40.40.0 UPE = 30.30.30.0 Extended IP access list 133 access-list 133 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 30.30.30.0/0.0.0.255
- debug crypto engineНиже приведен пример выходных данных команды.Loser#**debug crypto engine** Mar 17 11:49:07.902: Crypto engine 0: generate alg param Mar 17 11:49:07.906: CRYPTO_ENGINE: Dh phase 1 status: 0 Mar 17 11:49:07.910: Crypto engine 0: sign message using crypto engine Mar 17 11:49:09.894: CRYPTO_ENGINE: packets dropped: State = 0 Mar 17

11:49:11.758: Crypto engine 0: generate alg param Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0 Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25 Mar 17 11:49:13.346: Crypto engine 0: verify signature Mar 17 11:49:14.054: CRYPTO_ENGINE: packets dropped: State = 0 Mar 17 11:49:14.402: Crypto engine 0: sign message using crypto engine Mar 17 11:49:14.934: Crypto engine 0: create session for conn id 25 Mar 17 11:49:14.942: CRYPTO ENGINE 0: clear dh number for conn id 25 Mar 17 11:49:24.946: Crypto engine 0: generate alg param

- **debug crypto sessmgmt**Ниже приведен пример выходных данных команды.StHelen#**debug crypto sessmgmt** Mar 17 11:49:08.918: IP: s=40.40.40.40 (Serial1), d=30.30.30.30, len 328, Found an ICMP connection message. Mar 17 11:49:08.922: CRYPTO: Dequeued a message: CIM Mar 17 11:49:08.926: CRYPTO-SDU: Key Timeout, Re-exchange Crypto Keys Mar 17 11:49:09.978: CRYPTO: Verify done. Status=OK Mar 17 11:49:09.994: CRYPTO: DH gen phase 1 status for conn_id 22 slot 0:OK Mar 17 11:49:11.594: CRYPTO: DH gen phase 2 status for conn_id 22 slot 0:OK Mar 17 11:49:11.598: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK Mar 17 11:49:12.134: CRYPTO: Sign done. Status=OK Mar 17 11:49:12.142: CRYPTO: ICMP message sent: s=19.19.19.20, d=19.19.19.19 Mar 17 11:49:12.146: CRYPTO-SDU: act_on_nnc_req: NNC Echo Reply sent Mar 17 11:49:12.154: CRYPTO: Create encryption key for conn_id 22 slot 0:OK Mar 17 11:49:15.366: CRYPTO: Dequeued a message: CCM Mar 17 11:49:15.370: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK Mar 17 11:49:16.430: CRYPTO: Verify done. Status=OK Mar 17 11:49:16.434: CRYPTO: Replacing -23 in crypto maps with 22 (slot 0) Mar 17 11:49:26.438: CRYPTO: Need to pregenerate 1 pairs for slot 0. Mar 17 11:49:26.438: CRYPTO: Pregenerating DH for conn_id 32 slot 0 Mar 17 11:49:28.050: CRYPTO: DH phase 1 status for conn_id 32 slot 0:OK ~~ <---------- This is good ----------> ~~ Если набор неверного одноранговой узла на Криптокарте, вы получаете это сообщение об ошибках.Mar 2 12:19:12.639: CRYPTO-SDU:Far end authentication error:

  Connection message verify failedЕсли алгоритмы шифрования не совпадают, вы получаете это сообщение об ошибках.Mar 2 12:26:51.091: CRYPTO-SDU: Connection failed due to incompatible policyЕсли ключ DSS отсутствует или недопустимый, вы получаете это сообщение об ошибках.Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error:

  Connection message verify failed
- **debug crypto key**Ниже приведен пример выходных данных команды.StHelen#**debug crypto key** Mar 16 12:16:45.795: CRYPTO-KE: Sent 4 bytes. Mar 16 12:16:45.795: CRYPTO-KE: Sent 2 bytes. Mar 16 12:16:45.799: CRYPTO-KE: Sent 6 bytes. Mar 16 12:16:45.799: CRYPTO-KE: Sent 2 bytes. Mar 16 12:16:45.803: CRYPTO-KE: Sent 64 bytes. Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes. Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes. Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes. Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes. Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
- **clear crypto connection**Ниже приведен пример выходных данных команды.wan-2511#**show crypto engine connections act** ID Interface IP-Address State Algorithm Encrypt Decrypt 9 Serial0 20.20.20.21 set DES_56_CFB64 29 28 wan-2511#**clear crypto connection 9** wan-2511# *Mar 5 04:58:20.690: CRYPTO: Replacing 9 in crypto maps with 0 (slot 0) *Mar 5 04:58:20.694: Crypto engine 0: delete connection 9 *Mar 5 04:58:20.694: CRYPTO: Crypto Engine clear conn_id 9 slot 0: OK wan-2511# wan-2511#**show crypto engine connections act** ID Interface IP-Address State Algorithm Encrypt Decrypt wan-2511#
- **crypto zeroize**Ниже приведен пример выходных данных команды.wan-2511#**show crypto mypubkey** crypto public-key wan2511 01496536 11F43C02 70C0ADB7 5DD50600 A0219E04 C867A5AF C40A4FE5 CE99CCAB A8ECA840 EB95FBEE D727ED5B F0A6F042 BDB5529B DBB0698D DB0B2756 F6CABE8F 05E4B27F quit wan-2511#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. wan-2511(config)#crypto zeroize Warning! Zeroize will remove your DSS signature keys. Do you want to continue? [yes/no]: **yes** % Keys to be removed are named wan2511. Do you really want to remove these keys? [yes/no]: **yes** % Zeroize done. wan-2511(config)#**^Z** wan-2511# wan-2511#show crypto mypubkey wan-2511#
- **никакой крипто-общий ключ**Ниже приведен пример выходных данных команды.wan-2511#**show crypto pubkey** crypto public-key wan2516 01698232 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962 quit wan-2511#**configure terminal** Enter configuration commands, one per line. End with CNTL/Z. wan-2511(config)#**crypto public-key ?** WORD Peer name wan-2511(config)# wan-2511(config)#**no crypto public-key wan2516 01698232** wan-2511(config)#**^Z**

```
wan-2511# wan-2511#show crypto pubkey wan-2511#
```

Устранение проблем Cisco 7200 с ESA

Cisco также предоставляет возможность аппаратной поддержки, чтобы сделать шифрование на маршрутизаторах Cisco серии 7200, которое называют ESA. ESA находится в форме адаптера порта для карты VIP2-40 или автономного адаптера порта для Cisco 7200. Это расположение позволяет использованию или аппаратного адаптера или ядра программного обеспечения VIP2 шифровать и дешифровать данные, которые входят или уезжают через интерфейсы на карте VIP2 Cisco 7500. Cisco 7200 позволяет аппаратной поддержке шифровать трафик для любых интерфейсов на шасси Cisco 7200. Использование поддержки шифрования сохраняет драгоценные циклы ЦПУ, которые могут использоваться для других целей, таких как маршрутизация или любая из других функций Cisco IOS.

На Cisco 7200 автономный адаптер порта настроен точно то же как ядро шифрования программного обеспечения Cisco IOS, но имеет несколько дополнительных команд, которые только используются для аппаратных средств и для решения, какой механизм (программное обеспечение или аппаратные средства) сделает шифрование.

Во-первых, подготовьте маршрутизатор к аппаратному шифрованию:

```
wan-7206a(config)#
%OIR-6-REMCARD: Card removed from slot 3, interfaces disabled
*Mar  2 08:17:16.739: ...switching to SW crypto engine

wan-7206a#show crypto card 3 Crypto card in slot: 3 Tampered: No Xtracted: Yes Password set: Yes
DSS Key set: Yes FW version 0x5049702 wan-7206a# wan-7206a(config)# wan-7206a(config)#crypto
zeroize 3 Warning! Zeroize will remove your DSS signature keys. Do you want to continue?
[yes/no]: yes % Keys to be removed are named hard. Do you really want to remove these keys?
[yes/no]: yes [OK]
```

Включите или отключите аппаратное шифрование как показано ниже:

```
wan-7206a(config)#crypto esa shutdown 3 ...switching to SW crypto engine wan-
7206a(config)#crypto esa enable 3 There are no keys on the ESA in slot 3- ESA not enabled.
```

Затем, генерируйте ключи для ESA перед включением его.

```
wan-7206a(config)#crypto gen-signature-keys hard % Initialize the crypto card password. You will
need this password in order to generate new signature keys or clear the crypto card extraction
latch. Password: Re-enter password: Generating DSS keys .... [OK] wan-7206a(config)# wan-
7206a#show crypto mypubkey crypto public-key hard 00000052 EE691A1F BD013874 5BA26DC4 91F17595
C8C06F4E F7F736F1 AD0CACEC 74AB8905 DF426171 29257F8E B26D49B3 A8E11FB0 A3501B13 D3F19623
DCCE7322 3D97B804 quit wan-7206a# wan-7206a(config)#crypto esa enable 3 ...switching to HW
crypto engine wan-7206a#show crypto engine brie crypto engine name: hard crypto engine type: ESA
serial number: 00000052 crypto engine state: installed crypto firmware version: 5049702 crypto
engine in slot: 3 wan-7206a#
```

Устранение проблем VIP2 С ПОДДЕРЖКОЙ ESA

Адаптер аппаратного порта ESA на карте VIP2 используется, чтобы зашифровать и дешифровать данные, которые входят или уезжают через интерфейсы на карте VIP2. Как с Cisco 7200, с помощью поддержки шифрования сохраняет драгоценные циклы ЦПУ. В этом случае **команда crypto esa enable** не существует, потому что адаптер порта ESA делает шифрование для портов на карте VIP2, если включен ESA. Если бы адаптер порта ESA был просто установлен впервые или демонтирован тогда повторно установленный, **крипто-ясный фиксатор** должен быть применен к тому слоту.

Router#show crypto card 11 Crypto card in slot: 11 Tampered: No Xtracted: Yes Password set: Yes DSS Key set: Yes FW version 0x5049702 Router#

Поскольку криптографический модуль ESA был извлечен, вы получите следующее сообщение об ошибке, пока вы не сделаете **команду crypto clear-latch** на том слоте, как показано ниже.

```
----
*Jan 24 02:57:09.583: CRYPTO: Sign done. Status= Extraction latch set. Request not allowed.
-----
Router(config)#crypto clear-latch ? <0-15> Chassis slot number Router(config)#crypto clear-latch
11 % Enter the crypto card password. Password: Router(config)#^Z
```

Если вы забываете ранее назначенный пароль, используйте **команду crypto zeroize** вместо **команды crypto clear-latch** для сброса ESA. После запуска **команды crypto zeroize** необходимо восстановить и ключи DSS повторного обмена. При регенерации ключей DSS вам предлагают создать новый пароль. Ниже приводится пример.

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show crypto card 11 Crypto card in slot: 11 Tampered: No Xtracted: No Password set: Yes
DSS Key set: Yes FW version 0x5049702 Router# ------------------------------------------------
- Router#show crypto engine brief crypto engine name: TERT crypto engine type: software serial
number: 0459FC8C crypto engine state: dss key generated crypto lib version: 5.0.0 crypto engine
in slot: 6 crypto engine name: WAAA crypto engine type: ESA serial number: 00000078 crypto
engine state: dss key generated crypto firmware version: 5049702 crypto engine in slot: 11
Router# ----------- Router(config)#crypto zeroize Warning! Zeroize will remove your DSS
signature keys. Do you want to continue? [yes/no]: yes % Keys to be removed are named TERT. Do
you really want to remove these keys? [yes/no]: yes % Zeroize done. Router(config)#crypto
zeroize 11 Warning! Zeroize will remove your DSS signature keys. Do you want to continue?
[yes/no]: yes % Keys to be removed are named WAAA. Do you really want to remove these keys?
[yes/no]: yes [OK] Router(config)#^Z Router#show crypto engine brief crypto engine name: unknown
crypto engine type: software serial number: 0459FC8C crypto engine state: installed crypto lib
version: 5.0.0 crypto engine in slot: 6 crypto engine name: unknown crypto engine type: ESA
serial number: 00000078 crypto engine state: installed crypto firmware version: 5049702 crypto
engine in slot: 11 Router# -------------- Router(config)#crypto gen-signature-keys VIPESA 11 %
Initialize the crypto card password. You will need this password in order to generate new
signature keys or clear the crypto card extraction latch. Password: Re-enter password:
Generating DSS keys .... [OK] Router(config)# *Jan 24 01:39:52.923: Crypto engine 11: create key
pairs. ^Z Router# ------ Router#show crypto engine brief crypto engine name: unknown crypto
engine type: software serial number: 0459FC8C crypto engine state: installed crypto lib version:
5.0.0 crypto engine in slot: 6 crypto engine name: VIPESA crypto engine type: ESA serial number:
00000078 crypto engine state: dss key generated crypto firmware version: 5049702 crypto engine
in slot: 11 Router# ---------- Router#show crypto engine connections active 11 ID Interface IP-
Address State Algorithm Encrypt Decrypt 2 Serial11/0/0 20.20.20.21 set DES_56_CFB64 9996 9996
Router# Router#clear crypto connection 2 11 Router# *Jan 24 01:41:04.611: CRYPTO: Replacing 2 in
crypto maps with 0 (slot 11) *Jan 24 01:41:04.611: Crypto engine 11: delete connection 2 *Jan 24
01:41:04.611: CRYPTO: Crypto Engine clear conn_id 2 slot 11: OK Router#show crypto engine
connections active 11 No connections. Router# *Jan 24 01:41:29.355: CRYPTO ENGINE:Number of
connection entries received from VIP 0 ------------ Router#show crypto mypub % Key for slot 11:
crypto public-key VIPESA 00000078 CF33BA60 56FCEE01 2D4E32A2 5D7ADE70 6AF361EE 2964F3ED A7CE08BD
A87BF7FE 90A39F1C DF96143A 9B7B9C78 5F59445C 27860F1E 4CD92B6C FBC4CBCC 32D64508 quit
Router#show crypto pub crypto public-key wan2516 01698232 C5DE8C46 8A69932C 70C92A2C 729449B3
FD10AC4D 1773A997 7F6BA37D 61997AC3 DBEDBEA7 51BF3ADD 2BB35CB5 B9126B4D 13ACF93E 0DF0CD22
CFAAC1A8 9CE82985 quit Router# ---------- interface Serial11/0/0 ip address 20.20.20.21
255.255.255.0 encapsulation ppp ip route-cache distributed no fair-queue no cdp enable crypto
map test ! ---------- Router#show crypto eng conn act 11 ID Interface IP-Address State Algorithm
Encrypt Decrypt 3 Serial11/0/0 20.20.20.21 set DES_56_CFB64 761 760 Router# *Jan 24
01:50:43.555: CRYPTO ENGINE:Number of connection entries received from VIP 1 Router#
```

Дополнительные сведения

- Настройка и устранение неполадок шифрования данных на уровне сети Cisco: IPSec и ISAKMP - Часть 2
- DES FIPS 46-2 в Национальном институте стандартов и технологий (NIST)
- DES FIPS 186 в Национальном институте стандартов и технологий (NIST)
- Лаборатории RSA. Часто задаваемые вопросы о современной криптографии
- Стандарты безопасности IETF
- Настройка протокола защищенного обмена ключами IKE
- Настройка параметров сетевой безопасности IPSec Network Security
- Страница поддержки IPSec
- Техническая поддержка - Cisco Systems