Содержание

Введение

Этот документ описывает, как установить туннель второй версии протокола Internet Key Exchange (IKEv2) от узла к узлу между устройством адаптивной защиты Cisco (ASA) и маршрутизатором, который выполняет программное обеспечение Cisco IOSÂ®.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Вторая версия протокола Internet Key Exchange (IKEv2)
- Сертификаты и инфраструктура открытых ключей (PKI)
- Network Time Protocol (NTP)

Используемые компоненты

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

- Многофункциональное устройство защиты Cisco ASA серии 5510, которое работает под управлением ПО версии 9.1 (3)
- Маршрутизатор интегрированных служб Cisco 2900 (ISR), который выполняет версию программного обеспечения Cisco IOS 15.3 (3) M1

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.

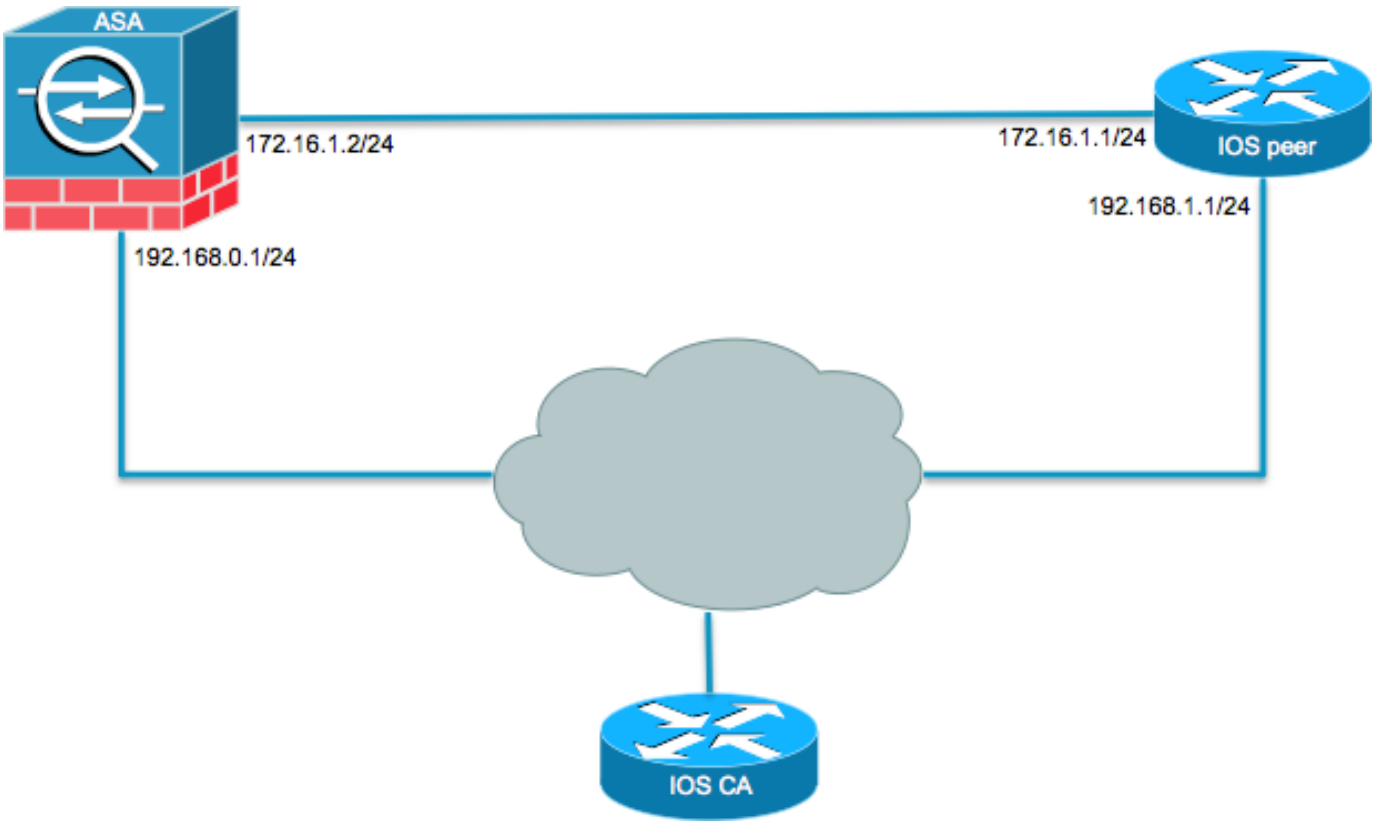
Родственные продукты

Этот документ может также использоваться с этими версиями программного и аппаратного обеспечения:

- Cisco ASA, который работает под управлением ПО версии 8.4 (1) или позже
- Поколение 2 ISR Cisco (G2), который выполняет версию программного обеспечения Cisco IOS 15.2 (4) M или позже
- Сервисные маршрутизаторы агрегации Cisco ASR серии 1000, которые выполняют версию 15.2 (4) S программного обеспечения Cisco IOS XE или позже
- Связанные маршрутизаторы Сетки Cisco, которые работают под управлением ПО версии 15.2 (4) M или позже

Настройка

Схема сети



Общие сведения

Конфигурация туннеля IKEv2 между ASA и маршрутизатором с использованием предварительных общих ключей является прямой. Однако при использовании проверки подлинности сертификата существуют определенные предупреждения иметь в виду.

NTP

Проверка подлинности сертификата требует, чтобы часы на всех участвующих устройствах синхронизировались с общим источником. В то время как часы могут быть установлены вручную на каждом устройстве, это не является очень точным и может быть громоздким. Наилегчайший метод для синхронизации часов на всех устройствах должен использовать NTP. NTP синхронизирует хронометраж среди ряда распределенных временных серверов и клиентов. Эта синхронизация позволяет событиям быть коррелированными, когда системные журналы созданы и когда другие специфичные для времени события имеют место. Для получения дополнительной информации о том, как настроить NTP, обратитесь к Протоколу сетевого времени: Рекомендации и Описание технологических решений.

> **Совет:** Когда сервер Центра сертификации (CA) программного обеспечения Cisco IOS используется, это - общая практика для настройки того же устройства как NTP master. В данном примере сервер CA также служит сервером NTP.

ОСНОВАННЫЙ НА HTTP URL поиск сертификата

Поиск сертификата на основе HTTP URL избегает фрагментации, которая заканчивается, когда переданы большие сертификаты. Эта опция активирована на Cisco IOS Doftware Device по умолчанию, таким образом, тип 12 req свидетельства используется программным обеспечением Cisco IOS.

Если версии программного обеспечения, которые не имеют исправления для идентификатора ошибки Cisco CSCul48246, используются на ASA, то об ОСНОВАННОМ НА HTTP URL поиске не выполняют согласование относительно ASA, и программное обеспечение Cisco IOS вызывает попытку авторизации отказать.

На ASA, если отладки протокола IKEv2 включены, появляются эти сообщения:

Во избежание этой проблемы не используйте **крипто-ikev2** команду **свидетельства http url** для отключения этой опции на маршрутизаторе, когда это взаимодействует с ASA.

Проверка идентификатора равноправного узла

Во время IKE AUTH организует согласования Протокола ISAKMP, узлы должны определить себя друг другу. Однако существует различие в способе, которым маршрутизаторы и ASA выбирают свою локальную идентичность.

ID ISAKMP выбор на маршрутизаторах

Когда туннели IKEv2 используются на маршрутизаторах, локальная идентичность, используемая на согласовании, определена **идентификационной локальной командой** под

профилем IKEv2:

По умолчанию маршрутизатор использует адрес в качестве локальной идентичности.

ID ISAKMP проверка на маршрутизаторах

Ожидаемый идентификатор равноправного узла также настроен вручную в том же профиле с **match identity удаленная** команда:

ID ISAKMP выбор на ASA

На ASA ISAKMP - идентичность выбран глобально с **командой crypto isakmp identity**:

По умолчанию командный режим установлен в автоматический, что означает, что ASA определяет согласование ISAKMP типом соединения:

- IP-адрес для предварительного общего ключа.
- Составное имя свидетельства для проверки подлинности сертификата.

Примечание: Идентификатор ошибки Cisco CSCul48099 является запросом на расширение для способности настроить на основе на туннельную группу, а не в глобальной конфигурации.

ID ISAKMP проверка на ASA

Удаленная проверка ID сделана автоматически (определенный типом соединения) и не может быть изменена. Проверка может быть включена или отключена на основе на туннельную группу с **peer-id-validate** командой:

Проблемы совместимости

Различие в выборе/проверке ID вызывает две отдельных проблемы совместимости:

1. Когда аутентификация свидетельства используется на ASA, ASA пытается проверить идентификатор равноправного узла от альтернативного имени субъекта (SAN) на полученном сертификате. Если проверка идентификатора равноправного узла включена и если отладки платформы IKEv2 включены на ASA, эти отладки появляются: Для этой проблемы или IP-адрес сертификата должен быть включен в сертификат узла, или проверка идентификатора равноправного узла должна быть отключена на ASA.
2. Точно так же по умолчанию ASA выбирает локальный ID автоматически так, когда аутентификация свидетельства используется, это передает Составное имя (DN) как идентичность. Если маршрутизатор настроен для получения адреса как удаленного ID, сбоев проверки идентификатора равноправного узла на маршрутизаторе. Если отладки IKEv2 включены на маршрутизаторе, эти отладки появляются:
Для этой проблемы, или настроить маршрутизатор, чтобы проверить полное доменное имя (FQDN) или настроить ASA для использования адреса в качестве ID ISAKMP.**Примечание:** На маршрутизаторе карта сертификата, которая присоединена к профилю IKEv2, должна быть настроена для распознавания DN. См. Сертификат

к разделу Сопоставления Профиля ISAKMP *Обмена ключами между сетями для Руководства по конфигурации IPSec VPN,* Документа Cisco *Выпуска 3S Cisco IOS XE*

Размер подлинного информационного наполнения

Если сертификаты (а не предварительные общие ключи) используются для аутентификации, подлинные информационные наполнения значительно больше. Это обычно приводит к фрагментации, которая может тогда заставить аутентификацию отказывать, если фрагмент теряется или заглядывается путь. Если туннель не подходит из-за размера подлинного информационного наполнения, обычные причины:

1. Применение политик плана контроля на маршрутизаторе, который мог бы заблокировать пакеты.
2. Неправильное согласование максимального модуля перехода (MTU), которое может быть исправлено с **крипто-ikev2** командой *размера* **mtu фрагментации**.

Выделение ресурсов в режиме мультиконтекста на ASA

С версии ASA 9.0 ASA поддерживает VPN в режиме мультиконтекста. Однако, когда вы настраиваете VPN в режиме мультиконтекста, убедиться выделить соответствующие ресурсы в системе, которая будет использовать VPN.

Для получения дополнительной информации обратитесь к информации О разделе Управления ресурсами руководства по настройке интерфейса командной строки для Cisco ASA, 9.0.

Проверка списка отозванных сертификатов

Список отозванных сертификатов (CRL) является списком отозванного certi? киты, которые были выполнены и впоследствии отозваны данным CA. Certi? киты могли бы быть отозваны по ряду причин, такие как:

- Сбой или компромисс устройства, которое использует данный сертификат.
- Компромисс пары ключей используется certi? cate.
- Ошибки в выполненном certi? cate, такой как неправильная идентичность или потребность принять изменение имени.

Механизм используется для certi? аннулирование cate зависит от CA. Отозванный certi? киты представлены в CRL их серийными номерами. Если сетевое устройство пытается проверить законность certi? cate, это загружает и просматривает текущий CRL для серийного номера представленного сертификата. Поэтому, если проверка CRL включена на любом узле, надлежащий URL CRL должен быть настроен также, таким образом, может быть проверена законность сертификатов ID.

Для получения дополнительной информации о CRL обратитесь к, Что Является разделом CRL Руководства по конфигурации Инфраструктуры открытых ключей, Выпуска 3S Cisco IOS XE.

Проверка цепочки сертификатов

Если ASA настроен с сертификатом, который имеет Промежуточный CAs, и это однорангово, мог бы или не мог бы иметь того же Промежуточного звена CA, то ASA должен быть явно настроен для передачи завершенной цепочки сертификатов к маршрутизатору. Маршрутизатор делает это по умолчанию. Чтобы сделать это при определении точки доверия под криптокартой, добавляет цепочечное ключевое слово как показано здесь:

Если это не будет сделано, то о туннеле только выполнят согласование, пока ASA является респондентом. Если это будет инициатор, то туннель откажет и PKI, и отладки IKEv2 на маршрутизаторе покажут это:

Типовая конфигурация ASA

Конфигурация примера отладки маршрутизатора

Типовой IOS CA конфигурация

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

> **Примечание:** Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Эти команды работают и на ASA и на маршрутизаторы:

- **show crypto ikev2 sa** - Отображает состояние Сопоставления безопасности (SA) фазы 1.
- **show crypto ipsec sa-** Отображает состояние SA фазы 2.

> **Примечание:** В этих выходных данных, в отличие от этого в IKEv1, групповое значение Diffie-Hellman (DH) Совершенной передающей тайны (PFS) отображается как 'безопасная пересылка (PFS) (Y/N): N, группа DH: ни один' во время первого согласования туннеля; после того, как повторно введение происходит, правильные значения появляются. Это не дефект даже при том, что поведение описано в идентификаторе ошибки Cisco CSCug67056.
>
> Различие между IKEv1 и IKEv2 - то, что в IKEv2 Дочерние SA созданы как часть самого обмена AUTH. DH Group, настроенная под криптокартой, используется только во время повторно введения. Таким образом вы видите 'безопасную пересылку (PFS) (Y/N): N, группа DH: ни один' до первого не повторно вводит. С IKEv1 вы видите другое поведение, потому что создание Child SA происходит во время Быстрого режима, и сообщение CREATE_CHILD_SA имеет условие для переноса информационного наполнения Обмена ключами, которое задает параметры DH для получения нового общего секретного ключа.

Проверка фазы 1

Эта процедура проверяет действия фазы 1:

1. Введите команду **show crypto ikev2 sa** в маршрутизатор:

2. Введите **показ крипто-ikev2 sacommand** в ASA:

Проверка фазы 2

Эта процедура описывает, как проверить, выполнили ли об индексе параметров безопасности (SPI) согласование правильно на двух узлах:

1. Введите **show crypto ipsec sa | я spi** команда на маршрутизаторе:
2. Введите **show crypto ipsec sa | я spicommand** на ASA:

Эта процедура описывает, как подтвердить ли трафики через туннель:

1. Введите **show crypto ipsec sa | я** команда **pkts** на маршрутизаторе:
2. Введите **show crypto ipsec sa | я pktscommand** на ASA:

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

> **Примечание:** Обратитесь к документу Важная информация о командах отладки, прежде чем использовать команды debug.

Отладки на ASA

> **Внимание:** На ASA можно установить различные уровни отладки; по умолчанию уровень 1 используется. При изменении уровня отладки многословие отладок могло бы увеличиться. Сделайте это с осторожностью, особенно в производственных средах!

Отладки ASA для согласования туннеля:

- **debug crypto ikev2 протокол**
- **debug crypto ikev2 платформа**

Отладка ASA для проверки подлинности сертификата:

- **debug crypto ca**

Отладки на маршрутизаторе

Отладки маршрутизатора для согласования туннеля:

- **debug crypto ikev2**
- **debug crypto ikev2 ошибка**

- debug crypto ikev2 внутренний

Отладки маршрутизатора для проверки подлинности сертификата:

- отладьте проверку pki крика
- отладьте транзакцию pki крика
- отладьте сообщения pki крика