FlexVPN с примером настройки шифрования следующего поколения

Содержание

[Введение](#)
[Шифрование следующего поколения](#)
[Комплект Suite-B-GCM-128](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Центр сертификации](#)
[Настройка](#)
[Топология сети](#)
[Шаги, Требуемые, чтобы Позволить маршрутизатору использовать Алгоритм цифровой подписи Эллиптической кривой](#)
[!--- конфигурацию](#)
[Проверьте соединение](#)
[Устранение неполадок](#)
[Заключение](#)

Введение

Этот документ описывает, как настроить FlexVPN между двумя маршрутизаторами, которые поддерживают набор Шифрования следующего поколения (NGE) Cisco алгоритмов.

Шифрование следующего поколения

Криптография NGE Cisco защищает информацию, которая перемещается по сетям, которые используют четыре конфигурируемых, известных криптографических алгоритма, и общественного достояния:

- Шифрование на основе Расширенного стандарта шифрования (AES), который использует 128-разрядные или 256-разрядные ключи
- Цифровые подписи с Алгоритмом цифровой подписи эллиптической кривой (ECDSA), которые используют кривые с 256-разрядными и 384-разрядными главными модулями
- Обмен ключами, который использует метод Диффи-Хеллмана эллиптической кривой (ECDH)
- Хеширование (цифровых отпечатков) на основе Защищенного алгоритма хэширования 2 (SHA 2)

National Security Agency (NSA) сообщает, что эти четыре алгоритма в комбинации

предоставляют обеспечение достоверных сведений для секретных данных. Комплект NSA B криптография для IPsec был публикован как стандарт в RFC 6379 и получил принятие в отрасли.

Комплект Suite-B-GCM-128

Согласно RFC 6379, эти алгоритмы требуются для комплекта Suite-B-GCM-128.

Этот комплект предоставляет защиту целостности Безопасного закрытия полезной нагрузки (ESP) и конфиденциальность с 128-разрядным AES-GCM (см. RFC4106). Когда ESP защита целостности и шифрование оба необходимы, этот комплект должен использоваться.

ESP
AES шифрования с 128-разрядными ключами и Значением проверки целостности (ICV) с 16 октетами в Режиме Галуа/Счетчика (GCM) (RFC4106)
NULL целостности

IKEv2
AES шифрования с 128-разрядными ключами в режиме Cipher Block Chaining (CBC) (RFC3602)
Псевдослучайная функция HMAC SHA 256 (RFC4868)
Целостность HMAC-SHA-256-128 (RFC4868)
Группа Диффи-Хеллмана 256-разрядная случайная группа ECP (RFC5903)

Дополнительные сведения о Комплекте B и NGE могут быть найдены в Шифровании Следующего поколения.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- FlexVPN
- Вторая версия протокола Internet Key Exchange (IKEv2)
- IPSec

Используемые компоненты

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

- Аппаратные средства: Поколение 2 Маршрутизаторов ISR (ISR) (G2), которые выполняют лицензию безопасности.
- Программное обеспечение: Выпуск 15.2.3T2 Программного обеспечения Cisco IOS. Любой выпуск Cisco IOS Software Release M или 15.1.2T или позже может использоваться, так как это - когда был представлен GCM.

Для получения дополнительной информации обратитесь к Навигатору Функции.

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.

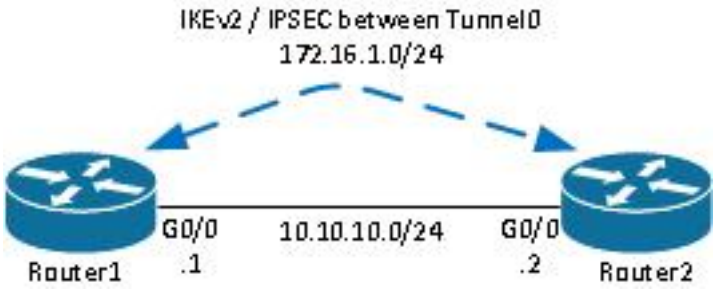
Центр сертификации

В настоящее время программное обеспечение Cisco IOS не поддерживает локальный сервер Центра сертификации (CA), который выполняет ECDH, который требуется для Комплекта B. Третья сторона CA сервер должна быть внедрена. Данный пример использует Microsoft CA на основе Комплекта B PKI

Настройка

Топология сети

Это руководство основывается на этой проиллюстрированной топологии. IP-адреса должны быть исправлены для удовлетворения требованиям.



Примечания:

Настройка состоит из двух маршрутизаторов, непосредственно связанных, который мог бы быть разделен многими переходами. Если так, гарантируйте, что существует маршрут для получения до IP - адреса адресуемого точки. Эта конфигурация только детализирует используемое шифрование. Маршрутизация IKEv2 или протокол маршрутизации должны быть внедрены по IPSEC VPN.

Шаги, Требуемые, чтобы Позволить маршрутизатору использовать Алгоритм цифровой подписи Эллиптической кривой

1. Создайте доменное имя и имя хоста, которые являются предварительными условиями для создания пары ключей EC.
```
ip domain-name cisco.com
hostname Router1
```

```
crypto key generate ec keysize 256 label Router1.cisco.com
```

Примечание: Пока вы не выполните версию с исправлением для идентификатора ошибки Cisco CSCue59994, маршрутизатор не позволит вам регистрировать сертификат с размером ключа меньше чем 768.

2. Создайте локальную точку доверия для получения сертификата от CA.

```
crypto pki trustpoint ecdh
 enrollment terminal
 revocation-check none
 eckeypair Router1.cisco.com
```

Примечание: Так как CA был офлайновым, проверки аннулирования были отключены. Проверки аннулирования должны быть включены для максимальной безопасности в производственной среде.

3. Аутентифицируйте точку доверия (это получает копию сертификата CA, который содержит открытый ключ).

```
crypto pki authenticate ecdh
```

4. Введите ядро 64 закодированных сертификата CA в приглашении. Введите **выход** и затем введите **да** для принятия.

5. Зарегистрируйте маршрутизатор в PKI на CA.

```
crypto pki enrol ecdh
```

6. Отображенные выходные данные используются, чтобы отправить запрос сертификата CA. Для Microsoft CA, соединиться с веб-интерфейсом CA и выбрать **Submit запрос сертификата**.

7. Импортируйте сертификат, полученный от CA в маршрутизатор. Введите **выход**, как только импортирован сертификат.

```
crypto pki import ecdh certificate
```

!--- конфигурацию

Конфигурация, предоставленная здесь, для Router1. Router2 требует зеркала конфигурации, где только IP-адреса на туннельном интерфейсе уникальны.

1. Создайте карту сертификата для соответствия с сертификатом однорангового устройства.

```
crypto pki certificate map certmap 10
 subject-name co cisco.com
```

2. Настройте предложение IKEv2 по Комплекту B.

```
crypto ikev2 proposal default
 encryption aes-cbc-128
 integrity sha256
 group 19
```

Примечание: IKEv2 Умные Настройки по умолчанию внедряет много предварительно сконфигурированных алгоритмов в рамках предложения IKEv2 по умолчанию. Так как aes-cbc-128 и sha256 требуются для комплекта Suite-B-GCM-128, необходимо удалить

aes-cbc-256, sha384, и sha512 в рамках этих алгоритмов. Причина для этого состоит в том, что IKEv2 выбирает самый сильный алгоритм, когда предоставлено выбор. Для максимальной безопасности используйте aes-cbc-256 и sha512. Однако это не требуется для Suite-B-GCM-128. Для просмотра настроенного предложения IKEv2 введите **показ крипто-ikev2** команда **предложения**.

3. Настройте профиль IKEv2, чтобы совпасть с картой сертификата и использовать ECDSA с точкой доверия, определенной ранее.
```
crypto ikev2 profile default
 match certificate certmap
 identity local dn
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
 pki trustpoint ecdh
```

4. Настройте IPSec, преобразовывают для использования GCM.
```
crypto ipsec transform-set ESP_GCM esp-gcm
 mode transport
```

5. Настройте Профиль IPSEC с параметрами, настроенными ранее.
```
crypto ipsec profile default
 set transform-set ESP_GCM
 set pfs group19
 set ikev2-profile default
```

6. Настройте туннельный интерфейс.
```
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel source Gigabit0/0 tunnel destination 10.10.10.2
 tunnel protection ipsec profile default
```

Проверьте соединение

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

1. Проверьте, что успешно генерировались ключи ECDSA.
```
Router1#show crypto key mypubkey ec
% Key pair was generated at: 04:05:07 JST Jul 6 2012
Key name: Router1.cisco.com
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 Key is not exportable.
 Key Data&colon;
 30593013 06072A86 48CE3D02 0106082A 8648CE3D 03010703 4200048F 2B0B5B5E
(...omitted...)
```

2. Проверьте, что сертификат был успешно импортирован и что используется ECDH.
```
Router1#show crypto pki certificates verbose ecdh
Certificate
 Status: Available
 Version: 3
 Certificate Serial Number (hex): 6156E3D5000000000009
(...omitted...)
```

3. Проверьте, что IKEv2 SA были успешно созданы и используют Комплект B алгоритмы.

```
Router1#show crypto ikev2 sa
 IPv4 Crypto IKEv2 SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.10.10.1/500        10.10.10.2/500        none/none            READY
      Encr: AES-CBC, keysize: 128, Hash: SHA256, DH Grp:19, Auth sign: ECDSA, Auth verify:
ECDSA
      Life/Active Time: 86400/20 sec
```

4. Проверьте, что IKEv2 SA были успешно созданы и используют Комплект B алгоритмы.

```
Router1#show crypto ipsec sa

interface: Tunnel0
   Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

(...omitted...)

    local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2
    plaintext mtu 1466, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0xAC5845E1(2891466209)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xAEF7FD9C(2935487900)
       transform: esp-gcm ,
       in use settings ={Transport, }
       conn id: 6, flow_id: SW:6, sibling_flags 80000000, crypto map: Tunnel0-head-0
       sa timing: remaining key lifetime (k/sec): (4341883/3471)
       IV size: 8 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)
```

Примечание: В этих выходных данных, в отличие от этого в Версии 1 обмена ключами между сетями (IKEv1), групповое значение Diffie-Hellman (DH) абсолютной секретности переадресации (PFS) показывает как **безопасная пересылка (PFS) (Y/N): N, группа DH: ни один** во время первого согласования туннеля, но после того, как повторно введение происходит, правильные значения показывают. Это не дефект даже при том, что поведение описано в идентификаторе ошибки Cisco CSCug67056. Различие между IKEv1 и IKEv2 - то, что в последнем Дочерние Сопоставления безопасности (SA) созданы как часть самого обмена AUTH. DH Group, настроенная под криптокартой, используется только во время повторно введения. Следовательно, вы видите **безопасную пересылку (PFS) (Y/N): N, группа DH: ни один** до первого не повторно вводит. Но 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.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Заключение

Эффективные и сильные криптографические алгоритмы, определенные в NGE, предоставляют долгосрочное обеспечение, что данные конфиденциально и целостность предоставлены и поддержаны в низкой стоимости для обработки. NGE может легко быть внедрен с FlexVPN, который предоставляет Комплект B стандартная криптография.

Дополнительная информация о реализации Cisco Комплекта B может быть найдена в Шифровании Следующего поколения.