Настройка и подключение маршрутизатора Cisco IOS к другому маршрутизатору Cisco IOS, сконфигурированному как CA-сервер

Содержание

Введение

В этом документе освещен порядок настройки маршрутизатора Cisco IOS® в качестве сервера центра сертификации (CA). Дополнительно иллюстрируется зачисление другого маршрутизатора Cisco IOS для получения корневого и идентифицирующего сертификата для аутентификации IPsec с сервера CA.

Предварительные условия

Требования

Для этого документа нет особых требований.

Используемые компоненты

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

- Два маршрутизатора Cisco серии 2600, работающие под управлением выпуска ПО Cisco IOS 12.3(4)T3.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе в действующей сети необходимо

понимать последствия выполнения любой команды.

Схема сети

В настоящем документе используется следующая схема сети:

Условные обозначения

Подробные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Формирование и экспорт пары ключей RSA для сервера сертификатов

Первый шаг — формирование пары ключей RSA, используемой сервером центра сертификации Cisco IOS. На маршрутизаторе (R1) сформируйте ключи RSA, как показано в следующих выходных данных:

```
R1(config)#crypto key generate rsa general-keys label cisco1 exportable
The name for the keys will be: cisco1
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]

R1(config)#
*Jan 22 09:51:46.116: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Примечание. Необходимо использовать ту же пару ключей (*key-label*), которую планируется использовать для сервера сертификатов (посредством команды **crypto pki server** *cs-label*, описанной далее).

Экспорт сформированной пары ключей

Экспортируйте ключи в энергонезависимую оперативную память (NVRAM) или перешлите их по протоколу TFTP (в зависимости от конфигурации). В данном примере используется NVRAM. С учетом специфики конкретной реализации, предпочтительным может быть хранение сведений о сертификатах на отдельном TFTP-сервере.

```
R1(config)#crypto key export rsa cisco1 pem url nvram: 3des cisco123

% Key name: cisco1
   Usage: General Purpose Key
Exporting public key...
Destination filename [cisco1.pub]?
Writing file to nvram:cisco1.pub
Exporting private key...
Destination filename [cisco1.prv]?
Writing file to nvram:cisco1.prv
R1(config)#
```

В случае использования TFTP-сервера можно повторно импортировать сформированную пару ключей, как иллюстрируется следующей командой:

```
crypto key import rsa key-label pem [usage-keys] {terminal | url url} [exportable]
passphrase
```

Примечание. Если вы не хотите, чтобы ключ экспортировался с сервера сертификатов, то после экспорта импортируйте его обратно на сервер сертификатов в виде неэкспортируемой пары ключей. В этом случае извлечь ключ повторно будет невозможно.

Просмотр сформированной пары ключей

Для проверки сформированной пары ключей выполните команду **show crypto key mypubkey rsa**.

Интерпретатор выходных данных (OIT), доступный только зарегистрированным пользователям, поддерживает некоторые команды **show**. Посредством OIT можно анализировать выходные данные команд **show**.

```
R1#show crypto key mypubkey rsa
% Key pair was generated at: 09:51:45 UTC Jan 22 2004
Key name: cisco1
 Usage: General Purpose Key
 Key is exportable.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00CC2DC8 ED26163A
  B3642376 FAA91C2F 93A3825B 3ABE6A55 C9DD3E83 F7B2BD56 126E0F11 50552843
  7F7CA4DA 3EC3E2CE 0F42BD6F 4C585385 3C43FF1E 04330AE3 37020301 0001
% Key pair was generated at: 09:51:54 UTC Jan 22 2004
Key name: cisco1.server
 Usage: Encryption Key
 Key is exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00EC5578 025D3066
  72149A35 32224BC4 3E41DD68 38B08D39 93A1AA43 B353F112 1E56DA42 49741698
  EBD02905 FE4EC392 7174EEBF D82B4475 2A2D7DEC 83E277F8 AEC590BE 124E00E1
  C1607433 5C7BC549 D532D18C DD0B7AE3 AECDDE9C 07AD84DD 89020301 0001
```

Включение HTTP-сервера на маршрутизаторе

Сервер центра сертификации в Cisco IOS поддерживает только зачисление по простому протоколу зачисления сертификата (SCEP). Для того, чтобы этот механизм работал, на маршрутизаторе должен действовать встроенный http-сервер Cisco IOS. Для включения сервера используйте команду **ip http server**:

```
R1(config)#ip http server
```

Включение и настройка сервера CA на маршрутизаторе

Выполните следующие действия:

Крайне важно помнить о том, что на сервере сертификатов должно использоваться то же имя, что и для сформированной вручную пары ключей.

Метка соответствует метке сформированной пары ключей:

```
R1(config)#crypto pki server cisco1
```

После включения сервера сертификатов можно указать значения функций сервера сертификатов через командную строку или использовать предварительно настроенные значения по умолчанию.

Команда **database url** указывает местоположение сохраняемых записей базы данных сервера CA. Если эта команда не определена, то все записи базы данных записываются на флэш-носитель.

```
R1(cs-server)#database url nvram:
```

Примечание. В случае использования TFTP-сервера URL-адрес должен иметь вид: **tftp://<ip-адрес>/каталог**.

Настройте уровень базы данных.

```
R1(cs-server)#database level minimum
```

Эта команда определяет типы данных, сохраняемых в базе данных зачисления сертификатов:

Minimum (Минимум). Сохраняется только достаточно сведений для продолжения выпуска новых сертификатов без конфликта. Это значение по умолчанию.

Names (Имена). В дополнение к информации, предусмотренной минимальным уровнем, сохраняются серийные номера и предметные наименования каждого сертификата.

Complete (Полностью). В дополнение к информации, предусмотренной минимальным уровнем и уровнем имен, в базу данных записывается каждый выпущенный сертификат.

Примечание. Ключевое слово **complete** создает большой объем данных. Выполняя эту команду, нужно также командой **database url** указать внешний TFTP-сервер, на котором будут храниться данные.

Настройте имя поставщика CA в виде соответствующей строки отличительного имени. В этом примере используются: CN (общее имя) cisco1.cisco.com, L (локализация) RTP и C (страна) США:

```
R1(cs-server)#issuer-name CN=cisco1.cisco.com L=RTP C=US
```

Определите период действия сертификата CA или обычного сертификата в днях.

Допустимые значения — *от 1 дня до 1825 дней*. Период действия сертификата CA по умолчанию — три года, период действия обычного сертификата по умолчанию — один год. Максимальный период действия обычного сертификата — *на один месяц короче* периода действия сертификата CA. Например:

```
R1(cs-server)#lifetime ca-certificate 365
R1(cs-server)#lifetime certificate 200
```

Определите период действия в часах для списка отзыва сертификатов (CRL), используемого сервером сертификатов. Максимальное значение периода действия — **336 часов** (две недели). Значение по умолчанию — **168 часов** (одна неделя).

```
R1(cs-server)#lifetime crl 24
```

Определите пункт распространения списка отзыва сертификатов (CDP), используемый в сертификатах, выдаваемых сервером сертификации.

URL-адресом должен быть URL-адрес HTTP. Например, у нашего сервера имеется IP-адрес 172.18.108.26:

```
R1(cs-server)#cdp-url http://172.18.108.26/cisco1cdp.cisco1.crl
```

Включите сервер CA, выполнив команду **no shutdown**:

```
R1(cs-server)#no shutdown
```

Примечание. Выполнять эту команду следует только после того, как сервер сертификатов будет полностью настроен.

Настройка второго маршрутизатора IOS (R2) и его зачисление на сервер сертификатов

Придерживайтесь следующего порядка действий.

На маршрутизаторе R2 настройте имя хоста и имя домена. Сгенерируйте ключи RSA keys.

Используя команду **hostname**, настройте имя хоста маршрутизатора как «R2»:

```
Router(config)#hostname R2
R2(config)#
```

Обратите внимание, что имя хоста маршрутизатора изменяется сразу после ввода команды **hostname**.

При помощи команды **ip domain-name** настройте имя домена на маршрутизаторе:

```
R2(config)#ip domain-name cisco.com
```

Для создания пары ключей R2 используйте команду **crypto key generate rsa**:

```
R2(config)#crypto key generate rsa
The name for the keys will be: R2.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
```

При помощи следующих команд в режиме глобальной конфигурации можно объявить центр сертификации, который должен использоваться маршрутизатором (в этом примере — Cisco IOS CA) и определить характеристики для доверенной точки центра сертификации:

```
crypto ca trustpoint cisco
 enrollment retry count 5
 enrollment retry period 3
 enrollment url http://14.38.99.99:80
 revocation-check none
```

Примечание. Команда **crypto ca trustpoint** унифицирует существующие команды **crypto ca identity** и **crypto ca trusted-root**, реализуя их функциональность в виде единой команды.

Для получения корневого сертификата с сервера CA используйте команду **crypto ca authenticate cisco** (наименование доверенной точки — cisco):

```
R2(config)#crypto ca authenticate cisco
```

Для зачисления и формирования сертификата используйте команду **crypto ca enroll cisco** (cisco — наименование доверенной точки):

```
R2(config)#crypto ca enroll cisco
```

После успешного зачисления на сервер центра сертификации Cisco IOS следует просмотреть выпущенные сертификаты командой **show crypto ca certificates**. Ниже приведены выходные данные команды. Команда отображает подробные сведения о сертификатах, которые соответствуют параметрам, настроенным на сервере центра сертификации Cisco IOS:

```
R2#show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 02
  Certificate Usage: General Purpose
  Issuer:
    cn=cisco1.cisco.com
    l=RTP
    c=US
  Subject:
    Name: R2.cisco.com
```

```
    hostname=R2.cisco.com
  CRL Distribution Point:
 http://172.18.108.26/cisco1cdp.cisco1.crl
Validity Date:
    start date: 15:41:11 UTC Jan 21 2004
    end   date: 15:41:11 UTC Aug 8 2004
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: cisco

CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: Signature
  Issuer:
    cn=cisco1.cisco.com
    l=RTP
    c=US
  Subject:
    cn=cisco1.cisco.com
    l=RTP
    c=US
  Validity Date:
    start date: 15:39:00 UTC Jan 21 2004
    end   date: 15:39:00 UTC Jan 20 2005
  Associated Trustpoints: cisco
```

Для сохранения ключа в постоянной флеш-памяти введите команду:

```
hostname(config)#write memory
```

Для сохранения конфигурации выполните следующую команду:

```
hostname#copy run start
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Интерпретатор выходных данных (OIT), доступный только зарегистрированным пользователям, поддерживает некоторые команды **show**. Посредством OIT можно анализировать выходные данные команд **show**.

show crypto ca certificates — показывает сертификаты.

show crypto key mypubkey rsa — показывает пару ключей.

```
hostname#copy run start
```

crypto pki server ese-ios-ca info crl — показывает список отзыва сертификатов (CRL).

```
hostname#copy run start
```

crypto pki server ese-ios-ca info requests — показывает ожидающие запросы зачисления.

```
hostname#copy run start
```

show crypto pki server — показывает текущее состояние сервера инфраструктуры открытых ключей (PKI).

```
hostname#copy run start
```

crypto pki server *cs-label* **grant { all |** *код-транзакции* **}** — разрешает все или только указанные запросы SCEP.

crypto pki server *cs-label* **reject { all |** *код-транзакции* **}** — отклоняет все или только указанные запросы SCEP.

crypto pki server cs-label password generate [*число-минут* **]** — формирует разовый пароль (OTP) для запроса SCEP (число-минут — продолжительность действия пароля в минутах). Допустимые значения — от 1 до 1440 минут. Значение по умолчанию равно 60 минутам.

Примечание. Одновременно может действовать только один пароль OTP. При формировании второго пароля OTP предыдущий пароль становится недействительным.

crypto pki server *cs-label* **revoke** *серийный-номер-сертификата* — отзывает сертификат по его серийному номеру.

crypto pki server *cs-label* **request** *pkcs10* **{url** *url* **|** *terminal***} [pem]** — вручную добавляет запрос зачисления сертификата base64 или PEM PKCS10 в базу данных запросов.

crypto pki server *cs-label* **info crl** — показывает сведения о состоянии текущего списка CRL.

crypto pki server *cs-label* **info request** — показывает все ожидающие запросы на зачисление сертификата.

Дополнительные сведения о проверке см. в разделе Проверка сформированной пары ключей настоящего документа.

Поиск и устранение неполадок

Сведения об устранении неполадок см. в разделе Устранение неполадок IP-безопасности — общие сведения и использование команд debug.

Примечание. Часто проблемы удается решить путем удаления и повторного определения

сервера центра сертификации.

Дополнительные сведения

- Согласование IPsec и протоколы IKE
- Cisco Systems — техническая поддержка и документация