Настройка и регистрация маршрутизатора Cisco IOS, подключенного к другому маршрутизатору Cisco IOS, настроенному как сервер CA

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 отсутствуют особые требования.

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 этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Схема сети

В настоящем документе используется следующая схема сети:

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации 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 то же название для пары ключей *(ключевая метка)*, которую вы планируете использовать для сервера сертификатов (через команду *cs-label* **crypto pki server**, покрытую позже).

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 был экспортным от вашего сервера сертификатов, импортируете его назад к серверу сертификатов после того, как это было экспортировано как неэкспортная пара 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.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные 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 CA 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:

1. 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.
2. **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:** При использовании сервера TFTP URL должен быть **tftp://<ip_address> / каталог**.

3. 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: Завершенное** ключевое слово производит большое количество информации. **Выполняя эту команду, нужно также командой database url указать внешний TFTP-сервер, на котором будут храниться данные.**
4. 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`
5. 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.* Пример:`R1(cs-server)#lifetime ca-certificate 365 R1(cs-server)#lifetime certificate 200`
6. 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`
7. 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`
8. **Включите сервер CA, выполнив команду no shutdown:**`R1(cs-server)#no shutdown` **Примечание:** Выполните эту команду только после завершенной настройки сервера сертификатов.

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

Придерживайтесь следующего порядка действий.

1. 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]
```

2. 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** объединяет существующую **команду crypto ca identity** и **команду crypto ca trusted-root**, таким образом предоставляя объединенную функциональность под одиночной командой.
3. **Для получения корневого сертификата с сервера CA используйте команду crypto ca authenticate cisco (наименование доверенной точки — cisco):**`R2(config)#`**`crypto ca authenticate cisco`**
4. **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`**
5. Для сохранения ключа в постоянной флеш-памяти введите команду:`hostname(config)#`**`write memory`**
6. Для сохранения конфигурации выполните следующую команду:`hostname#`**`copy run start`**

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- **show crypto ca certificates— показывает сертификаты.**
- **show crypto key mypubkey rsa— показывает пару ключей.**`!% Key pair was generated at: 09:28:16 EST Jan 30 2004`
  `!Key name: ese-ios-ca`
  `! Usage: General Purpose Key`
  `! Key is exportable.`
  `! Key Data:`
  `!  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AF2198`
  `!  C56F1A8F 5AC501FF ADFB1489 1F503F91 CA3C3FA3 9FB2C150 FFCBF815 2AA73060`
  `!  E79AF510 E292C171 C6804B45 0CAAD4AF 5834AB85 B204208B 3960D20D 9B51AF7B`
  `!  ACF12D3D F5BC6EAE 77186AE9 1471F5A4 443CE5B5 1336EC33 5FEB3398 002C15EE`

```
!  9F8FD331 83490D8A 983FBBE1 9E72A130 121A3B97 A3ACD147 C37DA3D6 77020301 0001
!% Key pair was generated at: 09:28:17 EST Jan 30 2004
!Key name: ese-ios-ca.server
! Usage: Encryption Key
! Key is exportable.
! Key Data:
!  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 0096456A 01AEC6A5
!  0049CCA7 B41B675E 5317328D DF879CAE DB96A739 26F2A03E 09638A7A 99DFF8E9
!  18F7635D 6FB6EE27 EF93B3DE 336C148A 6A7A91CB 6A5F7E1B E0084174 2C22B3E2
!  3ABF260F 5C4498ED 20E76948 9BC2A360 1C799F8C 1B518DD8 D9020301 0001
```

- **crypto pki server ese-ios-ca info crl— показывает список отзыва сертификатов (CRL).**
```
Certificate Revocation List:
  !    Issuer: cn=ese-ios-ca,ou=ESE,o=Cisco Systems Inc,l=Raleigh,st=NC
  !    This Update: 09:58:27 EST Jan 30 2004
  !    Next Update: 09:58:27 EST Jan 31 2004
  !    Number of CRL entries: 0
  !    CRL size: 300 bytes
```

- **crypto pki server ese-ios-ca info requests— показывает ожидающие запросы зачисления.**
```
Enrollment Request Database:
  ! ReqID  State      Fingerprint                      SubjectName
  ! --------------------------------------------------------------
```

- **show crypto pki server— показывает текущее состояние сервера инфраструктуры открытых ключей (PKI).**
```
! Certificate Server status: enabled, configured
  !    Granting mode is: manual
  !    Last certificate issued serial number: 0x1
  !    CA certificate expiration timer: 10:58:20 EDT Jun 21 2005
  !    CRL NextUpdate timer: 09:58:26 EST Jan 31 2004
  !    Current storage dir: nvram:
  !    Database Level: Names - subject name data written as .cnm
```

- *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:** Только один OTP допустим за один раз. 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.

Устранение неполадок

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

Примечание: Когда вы удаляете и переопределяете сервер CA, во многих ситуациях можно решить проблемы.

Дополнительные сведения

- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация