

Настройка и регистрация концентратора Cisco VPN 3000, подключенного к маршрутизатору Cisco IOS как сервер CA

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Схема сети](#)

[Условные обозначения](#)

[Формирование и экспорт пары ключей RSA для сервера сертификатов](#)

[Экспорт сформированной пары ключей](#)

[Просмотр сформированной пары ключей](#)

[Включение HTTP-сервера на маршрутизаторе](#)

[Включение и настройка сервера CA на маршрутизаторе](#)

[Настройте и зарегистрируйте Cisco VPN 3000 Concentrator](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

Введение

В этом документе освещен порядок настройки маршрутизатора Cisco IOS® в качестве сервера центра сертификации (CA). Кроме того, это иллюстрирует, как зарегистрировать Cisco VPN 3000 Concentrator к маршрутизатору Cisco IOS для получения root и сертификата ID для Аутентификации IPSec.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Маршрутизатор серии Cisco 2600, который выполняет программное обеспечение Cisco

IOS версии 12.3 (4) T3

- Версия 4.1.2 концентратора Cisco VPN 3030

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

[Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.](#)

Формирование и экспорт пары ключей RSA для сервера сертификатов

Первый шаг должен генерировать Открытые и секретные ключи криптосистемы RSA, которые Cisco IOS CA использует сервер. На маршрутизаторе (R1) генерируйте ключи RSA, как замечено здесь:

```
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

Ключи тогда должны быть экспортированы в Энергонезависимую память (NVRAM) или TFTP (на основе вашей конфигурации). В данном примере используется NVRAM. На основе вашей реализации вы могли бы потенциально хотеть использовать отдельный сервер TFTP, чтобы хранить вашу информацию сертификата.

```
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)#
```

При использовании сервера TFTP можно повторно импортировать генерируемую пару ключей, как замечено сюда:

```
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. Поэтому ключ не может быть снят снова.

[Просмотр сформированной пары ключей](#)

Можно проверить генерируемую пару ключей путем призыва команды `show crypto key mypubkey rsa`:

Некоторые команды `show` поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды `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 AECDDDE9C 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 его используйте команду `ip http server`:

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

Включение и настройка сервера CA на маршрутизаторе

Придерживайтесь следующего порядка действий.

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. Если это выполнено, также необходимо задать внешний сервер TFTP, в котором можно хранить данные через команду `database url`.
4. Настройте имя поставщика CA в виде соответствующей строки отличительного имени. В данном примере, CN (Общее имя) `cisco1.cisco.com`, L (Местность) `RTP` и (страна) `US` используется:

```
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.* Срок действия сертификата CA по умолчанию составляет **3 года**, и срок действия сертификата по умолчанию составляет **1 год**. Максимальный срок существования сертификата составляет *1 месяц меньше*, чем срок 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 пожизненное значение составляет **336 часов** (2 недели). Значение по умолчанию составляет **168 часов** (1 неделя).

```
R1(cs-server)#lifetime crl 24
```
7. Определите Точку распространения Certificate-Revocation-List (CDP), который будет использоваться в сертификатах, которые выполнены сервером сертификатов. URL-адресом должен быть URL-адрес HTTP. Например, IP-адрес нашего сервера `172.18.108.26`.

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

8. Включите сервер CA путем запуска команды `no shutdown.R1 (cs-server)#no shutdown`
Примечание: Выполните эту команду только после завершения настройки сервера сертификатов.

[Настройте и зарегистрируйте Cisco VPN 3000 Concentrator](#)

Придерживайтесь следующего порядка действий.

1. Выбор **Administration > Certificate Management** и выбирает **Click here** для установки сертификата CA для получения корневого сертификата из Cisco IOS CA Сервер.

The screenshot shows the 'Administration | Certificate Management' page. The header includes the date and time 'Sunday, 25 January 2004 08:47:49' and a 'Refresh' button. The main content area contains the following text: 'This section lets you view and manage certificates on the VPN 3000 Concentrator. Installation of a CA certificate is required before identity and SSL certificates can be installed.' Below this is a list of three links: 'Click here to install a CA certificate' (highlighted with a red box), 'Click here to enroll with a Certificate Authority', and 'Click here to install a certificate'. There are two sections for certificate lists: 'Certificate Authorities' (current: 0, maximum: 20) and 'Identity Certificates' (current: 0, maximum: 20). Both sections have a table with columns for Subject, Issuer, Expiration, and Actions, and both show 'No Certificate Authorities' and 'No Identity Certificates' respectively.

2. Выберите **SCEP** как метод

The screenshot shows the 'Administration | Certificate Management | Install | CA Certificate' page. The main content area contains the text: 'Choose the method of installation:'. Below this is a list of three links: 'SCEP (Simple Certificate Enrollment Protocol)' (highlighted with a red box), 'Cut & Paste Text', and 'Upload File from Workstation'. At the bottom of the page, there is a link: '<< Go back to and choose a different type of certificate'.

установки.

3. Введите URL Cisco IOS CA Сервер, дескриптор CA, и нажмите **Retrieve**. **Примечание:** Корректный URL в данном примере является `http://14.38.99.99/cgi-bin/pkiclient.exe` (необходимо включать полный путь/`cgi-bin/pkiclient.exe`).


Administration | Certificate Management | Install | CA Certificate | SCEP

Enter the information needed to retrieve the CA certificate via SCEP. Please wait for the operation to complete.

URL

CA Descriptor Required for some PKI configurations.

Выберите **Administration > Certificate Management**, чтобы проверить, что был установлен корневой сертификат. Этот рисунок иллюстрирует подробные данные корневого сертификата.

Administration | Certificate Management Sunday, 25 January 2004 08:52:23
Refresh 

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)


Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
cisco1.cisco.com	cisco1.cisco.com	01/20/2005	Yes	View Configure Delete SCEP

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

4. Выберите **Click here** для регистрации с Центром сертификации для получения сертификата ID из Cisco IOS CA Сервер.

Administration | Certificate Management Sunday, 25 January 2004 08:52:23
Refresh 

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
cisco1.cisco.com	cisco1.cisco.com	01/20/2005	Yes	View Configure Delete SCEP

Identity Certificates (current: 0, maximum: 20)

Subject	Issuer	Expiration	Actions
No Identity Certificates			

5. Выберите **Enroll via SCEP** в `cisco1.cisco.com` (`cisco1.cisco.com` является CN Cisco IOS CA Сервер).

Administration | Certificate Management | Enroll | Identity Certificate

Select the enrollment method for the identity certificate. To install a certificate with SCEP, the issuing CA's certificate must also be installed with SCEP. [Click here to install a new CA using SCEP before enrolling.](#)

- [Enroll via PKCS10 Request \(Manual\)](#)
- [Enroll via SCEP at cisco1.cisco.com](#)

[<< Go back to Certificate Management](#)

6. Завершите регистрационную форму путем ввода всей информации, которая будет включена в запросе сертификата. После завершения формы нажмите **Enroll** для начала запроса регистрации к серверу CA.

Administration Certificate Management Enroll | Identity Certificate | SSCP

Enter the information to be included in the certificate request. Please wait for the operation to finish.

Common Name (CN)	<input type="text" value="rtp-vpn3000"/>	Enter the common name for the VPN 3000 Concentrator to be used in this PKI.
Organizational Unit (OU)	<input type="text" value="TAC"/>	Enter the department.
Organization (O)	<input type="text" value="Cisco"/>	Enter the Organization or company.
Locality (L)	<input type="text" value="RTP"/>	Enter the city or town.
State/Province (SP)	<input type="text" value="NC"/>	Enter the State or Province.
Country (C)	<input type="text" value="US"/>	Enter the two-letter country abbreviation (e.g. United States = US).
Subject AlternativeName (FQDN)	<input type="text"/>	Enter the Fully Qualified Domain Name for the VPN 3000 Concentrator to be used in this PKI.
Subject AlternativeName (E-Mail Address)	<input type="text"/>	Enter the E-Mail Address for the VPN 3000 Concentrator to be used in this PKI.
Challenge Password	<input type="text"/>	Enter and verify the challenge password for this certificate request.
Verify Challenge Password	<input type="text"/>	
Key Size	<input type="text" value="RSA 512 bits"/>	Select the key size for the generated RSA key pair.

После нажатия Enroll показы VPN 3000 Concentrator "Запрос сертификата генерировался".

Administration Certificate Management Enrollment | Request Generated

A certificate request has been generated.

SCEP Status: Installed

- [Go to Certificate Management](#)
- [Go to Certificate Enrollment](#)
- [Go to Certificate Installation](#)

Прим

вчание: Cisco IOS CA Сервер может быть настроена для автоматического предоставления сертификатов с Cisco IOS CA **автоматическое предоставление** подкоманды Server. Эта команда используется для данного примера. Для наблюдения подробных данных сертификата ID выберите **Administration> Certificate Management**. Отображенный сертификат подобен этому.

Administration | Certificate Management Sunday, 25 January 2004

This section lets you view and manage certificates on the VPN 3000 Concentrator.

- [Click here to enroll with a Certificate Authority](#)
- [Click here to install a certificate](#)

Certificate Authorities [[View All CRL Caches](#) | [Clear All CRL Caches](#)] (current: 1, maximum: 20)

Subject	Issuer	Expiration	SCEP Issuer	Actions
cisco1.cisco.com	cisco1.cisco.com	01/20/2005	Yes	View Configure Delete SCEP

Identity Certificates (current: 1, maximum: 20)

Subject	Issuer	Expiration	Actions
rtsp-vpn3000 at Cisco	cisco1.cisco.com	08/12/2004	View Renew Delete

Проверка

Посмотрите [Сверение Генерируемого](#) раздела [Пары ключей](#) для данных проверки.

Устранение неполадок

Для сведений об устранении проблем обратитесь или к [Проблемам с подключением](#) [Устранения проблем на VPN 3000 Concentrator](#) или к [Устранению проблем системы безопасности IP - Понимание и Использование команд отладки](#).

Дополнительные сведения

- [Страница поддержки концентратора Cisco VPN серии 3000](#)
- [Страница поддержки Cisco VPN 3000 Series Client](#)
- [Страница поддержки IPSec](#)
- [Техническая поддержка - Cisco Systems](#)