

Организуем Cisco IPSec VPN с авторизацией по сертификатам на ключах eToken

**Роман Совалов
Константин Троицкий
Кирилл Случанко**

Вы всё ещё аутентифицируете удалённые подключения по логину и паролю? Тогда мы расскажем вам, как аутентифицировать их по сертификатам.

Возникла необходимость организовать доступ в локальную сеть мобильных пользователей. Аутентификация по логину/паролю уже не является самой безопасной (например, легко подсмотреть), поэтому будем производить аутентификацию по сертификатам. Реализуемая схема представлена на **рис. 1**.

Как видно из рисунка, будет использоваться контроллер домена, работающий под управлением Windows Server 2003 Ent. На контроллере домена поднят центр сертификации Enterprise Root CA. В качестве шлюза между локальной сетью и Интернетом использу-

ется Cisco Router 2611 XM с IOS C2600-ADVIPSERVICESK9-M (Cisco Router может быть другой, главное, чтобы на нём был образ с ADVIPSERVICESK). На компьютере/ноутбуке мобильного сотрудника установлен Cisco VPN Client. Для хранения ключевого материала будем использовать ключи eToken компании Aladdin.

Начнём с сервера сертификации. Установку Active Directory и Certification Authority (центра сертификации) я рассматривать не буду. Так как авторизация на шлюзе будет проходить по сертификатам, то маршрутизатор Cisco должен иметь возможность проверять

сертификаты пользователей. Это сделать можно двумя путями: вручную импортировать сертификаты на маршрутизатор или настроить маршрутизатор на работу с Microsoft CA. Естественно, второй вариант наиболее интересен. Для его реализации нам потребуется произвести некоторые действия на нашем AD. Далее все описываемые действия, выполняемые на сервере, будут производиться под учётной записью администратора домена.

Создаём учётную запись пользователя SCEP, которого помещаем в группу IIS_WPS.

Скачиваем небольшое дополне-

ние для центра сертификации (mscep add-on): <http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=9f306763-d036-41d8-8860-1636411b2d01>.

Запускаем установку скачанного дополнения (sersetup.exe).

На вопрос: «Are you sure you want to install Simple Certificate Enrollment Protocol (SCEP) Add-On for Certificate Services?» – отвечаем «Yes».

Соглашаемся с лицензионным соглашением.

Затем в окне «Welcome to the SCEP Add-On for Certificate Services Setup Wizard» нажимаем «Next».

В окне «Application Identity Options» выбираем пункт «Use a service account» и нажимаем «Next».

В окне «Service Account Information» вводим учетные данные аккаунта SCEP, созданного ранее, и нажимаем «Next».

В окне «Challenge Phrase Options» убеждаемся, что установлена галочка «Require SCEP Challenge Phrase to Enroll», и нажимаем «Next».

В следующем окне – «SCEP RA Certificate Enrollment» заполняем все поля и нажимаем кнопку «Next».

В окне «Completing the SCEP Add-On for Certificate Services Setup Wizard» проверяем наши настройки и нажимаем «Finish».

Теперь для проверки на сервере сертификатов заходим на страничку <http://localhost/certsrv/mscep/mscep.dll>, должна отобразиться страничка, показанная на рис. 2. Если страничка отобразилась, то значит, SCEP Add-On установлен. Если возникли какие-то проблемы, то попробуйте переустановить SCEP Add-On.

Теперь открываем консоль управления Certification Authority, правой кнопкой нажимаем на «Certificate Templates» и из контекстного меню выбираем пункт «Manage».

В открывшемся окне из списка шаблонов сертификатов выбираем шаблон IPSec (Offline Request), открываем его свойства.

В свойствах шаблона сертификата переходим на вкладку «Security». На этой вкладке добавляем пользователя SCEP и выдаём ему права Read и Enroll. После чего нажимаем «ОК».

Переходим в консоль управления Certification Authority, правой кнопкой

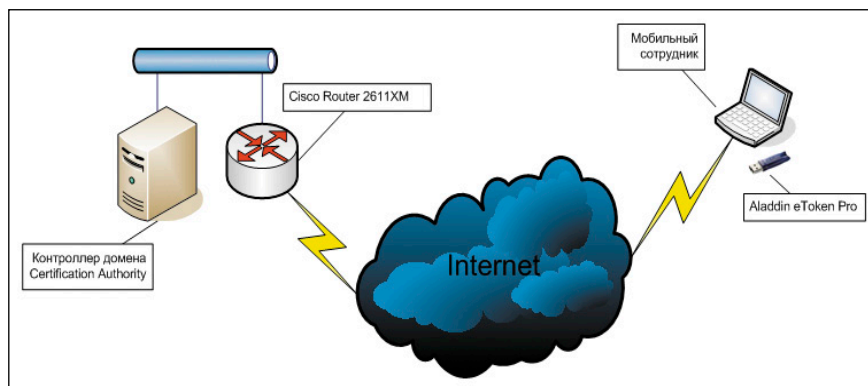


Рисунок 1. Общая схема описываемого решения

нажимаем на «Certificate Templates» и из контекстного меню выбираем пункт «New → Certificate Template to Issue». В появившемся окне «Enable Certificate Templates» из списка шаблонов сертификатов выбираем шаблон IPSec (Offline Request) и нажимаем «ОК».

В консоли управления Certification Authority выбираем пункт «Certificate Templates» и смотрим список выдаваемых шаблонов, убеждаемся, что шаблон IPSec (Offline Request) присутствует в этом списке.

Теперь необходимо настроить центр сертификации на выдачу сертификатов на ключи eToken.

С сайта www.aladdin.ru скачиваем драйвер PKI, устанавливаем его на наш сервер. Этот же драйвер необходимо установить на рабочую станцию клиента (например, на домашний компьютер или ноутбук). Этот драйвер необходим для работы с ключами eToken компании Aladdin.

Опять переходим в консоль управления Certification Authority, правой кнопкой нажимаем на «Certificate Templates» и из контекстного меню выбираем пункт «Manage».

В открывшемся окне из списка шаблонов сертификатов выбираем нужный нам шаблон – «Smartcard Logon». Наводим на него курсор, нажимаем правую кнопку мыши и из контекстного меню выбираем пункт «Duplicate Template».

В открывшемся окне «Properties of New Template» на вкладке «General» вводим имя нового сертификата в поле «Template display name: eToken Smartcard Logon». Напротив пункта «Publish certificate in Active Directory» устанавливаем переключатель во включённое состояние.

Переходим на вкладку «Request Handling». Убеждаемся, что в поле «Purpose» установлено значение: Signature and Encryption (подпись и шифрование). Также убеждаемся, что

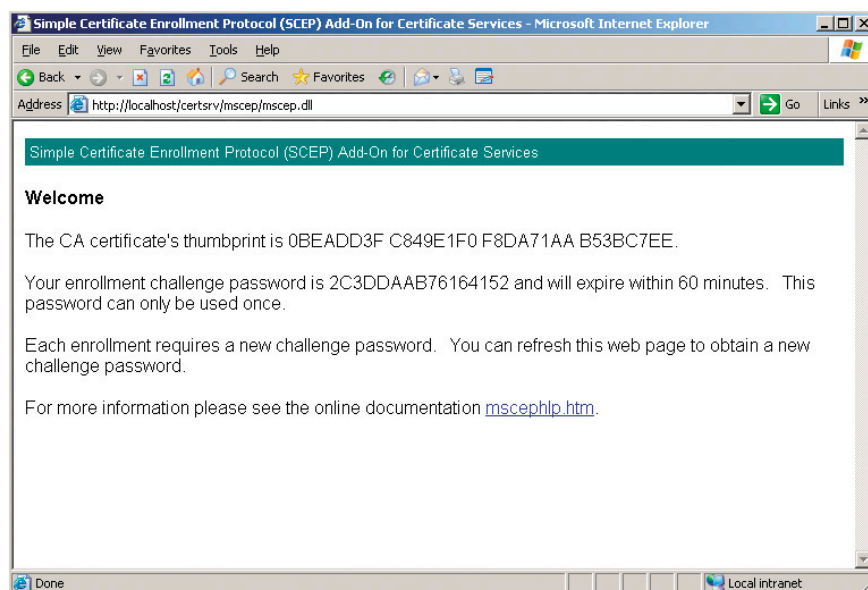


Рисунок 2. Скриншот веб-интерфейса модуля SCEP

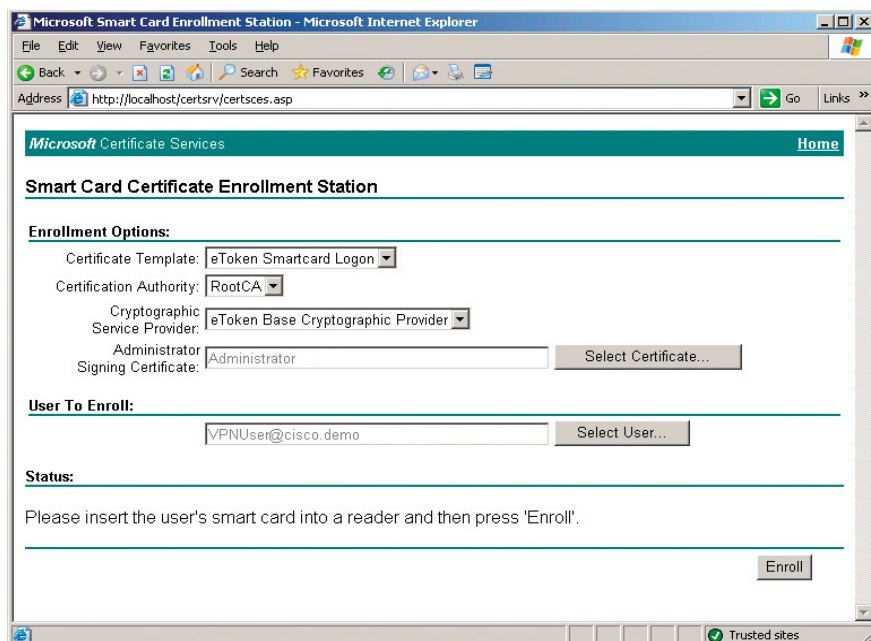


Рисунок 3. Скриншот веб-интерфейса центра сертификации

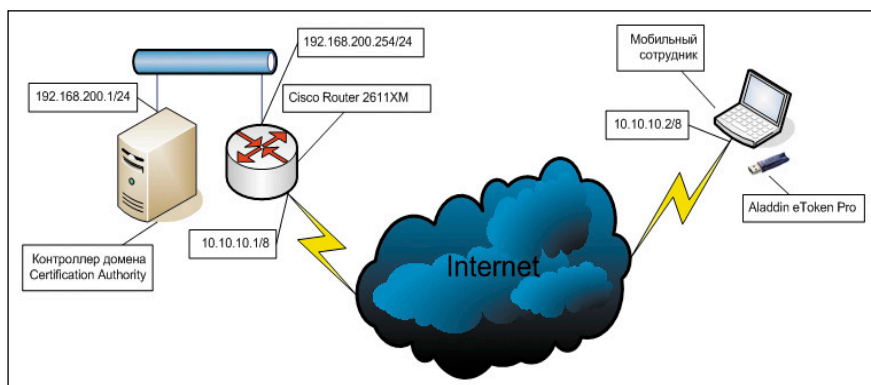


Рисунок 4. Уточнённая схема решения

выбран параметр «Enroll subject without requiring any user input». Затем нажимаем на кнопку «CSPs...». В окне «CSP Selection» выбираем пункт «Requests must use one of the following CSPs:» и затем из списка доступных CSP выбираем «eToken Base Cryptographic Provider». Нажимаем «OK».

Переходим на вкладку «Issuance Requirements». Устанавливаем переключатель «This number of authorized signatures» во включенное состояние. Убеждаемся, что в поле «Policy type required in signature:» установлено значение «Application policy», а в поле «Application policy:» установлено значение «Certificate Request Agent». После этого нажимаем кнопку «OK».

Переходим в консоль управления Certification Authority, наводим курсор на «Certificate Templates», нажимаем правой кнопкой мыши и из контекстного меню выбираем пункт «New → Certificate Template to Issue». В появившемся окне «Enable Certificate Templates» из списка шаблонов сертификатов выбираем шаблон «eToken Smartcard Logon» и нажимаем «OK».

В консоли управления Certification Authority выбираем пункт «Certificate Templates» и смотрим список выдаваемых шаблонов, убеждаемся, что шаблон eToken Smartcard Logon присутствует в этом списке.

Далее, давайте создадим учетную запись пользователя, который будет подключаться удалённо, и выпишем ему сертификат, который будет храниться на ключе eToken.

В оснастке Active Directory Users and Computers создаём учётную запись пользователя VPNUser.

Открываем Internet Explorer и вводим адрес: `http://имя_сервера_с_установленным_центром_сертификации/certsrv` (в нашем случае мы будем выполнять последующие действия на сервере, следовательно, адрес будет иметь вид: `http://localhost/certsrv`), попадаем на страничку Microsoft Certificate Services. Из раздела «Select a task» (внизу страницы) выбираем ссылку «Request a certificate». На следующей странице нажимаем на ссылку «Advanced certificate request». Затем переходим по ссылке «Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station». Откроется страничка Smart Card Certificate Enrollment. На этой странице в разделе «User To Enroll» указываем нашего пользователя – VPNUser. У вас должно получиться примерно следующее, показанное на **рис. 3**.

Подключаем eToken к компьютеру, на котором выписываем сертификат (в нашем случае это сервер), и нажимаем Enroll, при записи на ключ появится окно с просьбой ввести пин-код.

По умолчанию пин 1234567890, или введите тот пин, который вы указали при форматировании ключа. После выдачи сертификата и записи его на ключ получим сообщение об успешном завершении операции.

На этом настройка центра сертификации закончена. Теперь приступим к настройке нашего Cisco Router.

Перед настройкой немножко уточним схему (см. **рис. 4**). Предполагаю, что с настройкой интерфейсов на маршрутизаторе вы справитесь.

Нам необходимо поменять имя маршрутизатора на отличное от Router.

```
Router>enable
Router#conf t
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router (config) #hostname R1
R1 (config) #
```

Для работы с сертификатами на маршрутизаторе надо указать домен:

```
R1 (config) #ip domain-name cisco.demo
```


Укажем DNS:

```
R1(config)#ip name-server 192.168.200.1
```

Теперь настроим маршрутизатор, чтобы он общался с Microsoft Certification Authority:

```
R1(config)#crypto ca trustpoint RootCA
R1(ca-trustpoint)#enrollment url _J
http://192.168.200.1/certsrv/mscep/mscep.dll
R1(ca-trustpoint)#enrollment mode ra
R1(ca-trustpoint)#ip-address none
R1(ca-trustpoint)#serial-number none
R1(ca-trustpoint)#revocation-check crl
R1(ca-trustpoint)#crl query ldap://192.168.200.1
R1(ca-trustpoint)#auto-enroll
R1(ca-trustpoint)#usage ike
```

Теперь необходимо получить с центра сертификации корневой сертификат:

```
R1(config)#crypto ca authenticate RootCA
```

```
Certificate has the following attributes:
Fingerprint MD5: 0BEADD3F C849E1F0 F8DA71AA B53BC7EE
Fingerprint SHA1: 1FBC346D 247259D3 C6927C35 F72EACFA 5EC2899C
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
```

Теперь запросим сертификат для маршрутизатора. Для этого на сервере заходим через Internet Explorer на страничку <http://localhost/certsrv/mscep/mscep.dll>. На этой страничке в строке, начинающейся на «Your enrollment challenge password is...», смотрим пароль, который необходимо будет ввести на маршрутизаторе при запросе сертификата. На данный момент у меня этот пароль выглядит так: 41B20A111D8F37E2. Он действителен в течение 60 минут с момента генерации, то есть фактически с момента открытия вами странички. Теперь в консоли вводим:

```
R1(config)#crypto ca enroll RootCA
```

```
%
% Start certificate enrollment ...
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your
certificate. For security reasons your password will not be saved in
the configuration.
Please make a note of it.
Password:
```

Вводим пароль, который мы получили ранее.

```
Re-enter password:
```

Повторяем ввод. Обращаю внимание, что вводимые символы не отображаются.

```
% The subject name in the certificate will include: R1.cisco.demo
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The 'show crypto ca certificate RootCA verbose' command will
show the fingerprint.

R1(config)#
Jun 17 16:05:42.014: CRYPTO PKI: Certificate Request
Fingerprint MD5: 23CF4C96 D0C7505F 5DBFD079 A6DABE71
Jun 17 16:05:42.014: CRYPTO PKI: Certificate Request
Fingerprint SHA1: FD8351FF 8E419652 804ADC1F 367D2FE3 35970ED6
Jun 17 16:05:45.295: %PKI-6-CERTRET: Certificate received from
Certificate Authority
```

Вы должны получить сообщение «Certificate received

from Certificate Authority». Это означает, что ваш запрос успешно обработан центром сертификации и вам выдан сертификат.

Теперь осталось настроить IPSec VPN, чтобы маршрутизатор выступал в роли VPN-сервера:

```
R1(config)#aaa new-model
R1(config)#aaa authentication login UserAuthn local
R1(config)#aaa authorization network GroupAuthn local
R1(config)#aaa session-id common
```

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)#group 2
```

```
R1(config)#crypto isakmp client configuration group _J
VPNclients
```

```
R1(config)#crypto isakmp client configuration address-pool _J
local VPNpool
```

```
R1(config)#crypto ipsec transform-set myset esp-des _J
esp-sha-hmac
```

```
R1(config)#crypto dynamic-map dynmap 10
R1(config-crypto-map)#set transform-set myset
```

```
R1(config)#crypto map vpn client configuration address _J
respond
```

```
R1(config)#crypto map vpn 10 ipsec-isakmp dynamic dynmap
```

```
R1(config)#ip local pool VPNpool 192.168.222.100 _J
192.168.222.200
```

Далее на внешнем интерфейсе (в нашем примере это интерфейс с адресом 10.10.10.1) вводим:

```
R1(config-if)#crypto map vpn
```

Прописываем статический маршрут:

```
R1(config)#ip route 0.0.0.0 0.0.0.0 f0/0
```

где f0/0 – это внешний интерфейс с адресом 10.10.10.1.

На этом настройка маршрутизатора закончена. Осталось настроить рабочую станцию клиента.

Устанавливаем на клиентском компьютере Cisco VPN Client.

Проверяем, установлен ли на компьютере пользователь драйвер PKI для работы с ключами eToken, если не установлен, то необходимо установить.

Подключаем ключ с сертификатом, который выдали ранее, к компьютеру пользователя.

Запускаем Cisco VPN Client. Нажимаем кнопку «New» для создания нового VPN-соединения. Указываем имя соединения и IP-адрес, в нашем случае 10.10.10.1. Далее на вкладке «Authentication» выбираем пункт «Certificate Authentication» и нажимаем «Save». После чего закрываем Cisco VPN Client.

Снова запускаем VPN Client, выбираем только что созданное подключение и нажимаем «Modify». На вкладке «Authentication», в разделе «Certificate Authentication», выбираем сертификат, который мы выдали ранее (ключ должен быть подключен). После чего опять нажимаем «Save» и пробуем подключиться.

Этот вариант самый простой, возможно, и не для всех подходящий, но для организации простого VPN-соединения с авторизацией по сертификатам, без применения к клиентам различных политик, вполне подойдет. 