

# Храним учетные записи VPN в связке RADIUS/MySQL

**Виталий Банковский**

В современном мире, полном опасностей в виде хакерских атак, значимость и популярность виртуальных частных сетей (Virtual Private Networks, VPN) постоянно растет. Сегодня рассмотрим один из аспектов интеграции устройств доступа к VPN в корпоративную сеть.

## Структура и используемые компоненты

В качестве сервера VPN я использовал одно из наиболее популярных решений от компании Cisco, Inc. – Cisco VPN 506E. Учитывая традиции и стандарты, которых придерживается эта компания, другие продукты (Cisco VPN concentrator 3000, Cisco ASA) настраиваются аналогичным образом.

В качестве сервера авторизации для Cisco VPN Server я использовал RADIUS с поддержкой хранения учетных записей в сервере данных MySQL.

Предположим, что сервер MySQL у нас будет находиться по адресу 10.10.10.10, сервер RADIUS – 10.10.10.11, а адрес 10.10.10.12 присвоен серверу VPN.

## Настройка базы данных

Приступим к созданию базы данных для хранения учетных записей. Запись для каждого пользователя состоит из имени пользователя и зашифрованного пароля.

Создаем базу данных:

```
mysql> create database vpn;
mysql> grant all on vpn.* to vpn@'10.10.10.11'
identified by 'PASSW905';
mysql> flush privileges;
```

где «PASSW905» – пароль доступа к базе данных. Этот же пароль прописывается в настройках сервера RADIUS для обеспечения доступа последнего к таблицам с учетными записями.

Создаем таблицу для хранения учетных записей пользователей:

```
create table users (
  username varchar(32),
  password varchar(64),
  contact varchar(80),
  role varchar(80),
  unique key username (username)
);
```

Кроме имени пользователя и пароля, я храню контактную информацию и роль пользователя.

И вносим несколько учетных записей:

```
mysql> insert into users(username,password)
values('user1', encrypt('pass1'));
mysql> insert into users(username,password)
values('user2', encrypt('pass2'));
```

где «pass1» и «pass2» – пароли учетных записей пользователей.

## Выбор сервера RADIUS

Итак, в предыдущем разделе мы создали хранилище, где находятся учетные записи наших пользователей. Теперь можно приступить к установке сервера RADIUS, который бы подключался к нашему серверу SQL за данными.

Немного о службе. RADIUS (Remote Authentication in Dial-In User Service) – протокол AAA (authentication, authorization and accounting) – изначально был разработан для совместной работы серверов доступа (NAS, Network Access Server) и систем авторизации и биллинга.

- **Authentication** – процесс, позволяющий идентифицировать (узнать) субъект по его данным, например, по имени пользователя и паролю.
- **Authorization** – процесс, определяющий полномочия идентифицированного субъекта на доступ к определенным объектам или сервисам.
- **Accounting** – процесс, позволяющий вести учет доступа к услугам.

Наиболее популярными на данный момент серверами RADIUS являются:

- FreeRADIUS;
- OpenRADIUS;
- GNU RADIUS;
- ClearBox Enterprise RADIUS Server.

В мире существует много других серверов RADIUS. С наиболее полным списком можно ознакомиться по адресу – [http://en.wikipedia.org/wiki/List\\_of\\_RADIUS\\_Servers](http://en.wikipedia.org/wiki/List_of_RADIUS_Servers).

Я выбрал GNU RADIUS как простой и легко устанавливаемый сервер. Домашняя страничка проекта находится по адресу – <http://www.gnu.org/software/radius/radius.html>.

## Установка и настройка сервера RADIUS

В своей работе я использую CentOS 4.x семейства RedHat, поэтому все настройки и пути размещения будут описаны для этого семейства дистрибутивов. Я использовал установку сервера RADIUS из исходных кодов, так как такой способ позволяет оперативно устанавливать последние версии в случае обнаружения проблем с безопасностью в пакете без ожидания обновлений от поставщика дистрибутива.

Получаем исходные коды сервера, распаковываем и устанавливаем:

```
tar -xvzf radius-1.5.tar.gz
cd radius-1.5
./configure --with-mysql
make
make install
```

Конфигурационные файлы будут установлены в каталог `/usr/local/etc/raddb/`.

Настройки по умолчанию не требуют больших изменений, за исключением настройки доступа к серверу MySQL и авторизации сервера VPN к службе RADIUS. Ниже приведены основные параметры, которые должны быть изменены.

Файл `/usr/local/etc/raddb/sqlserver`:

```
# Тип сервера
interface mysql

# Параметры сервера MySQL
server 10.10.10.10
port 3306
login vpn
password PASSW905

# Включить авторизацию MySQL
doauth yes

# Имя базы данных, где находится таблица «users»
auth_db vpn

# Запрос SQL, который используется для проверки
# аккредитации пользователя:
auth_query SELECT password FROM users WHERE username='%u'
```

Далее настраиваем подключение сервера VPN к серверу RADIUS. Для этого открываем файл `/usr/local/etc/raddb/clients` и вписываем следующую строку (или несколько в случае нескольких устройств):

```
#Client Name      Key
#-----
10.10.10.12      our_password_key
```

где:

- 10.10.10.12 – адрес IP нашего VPN-сервера;
- our\_password\_key – пароль.

Далее необходимо создать файл начального запуска службы RADIUS при старте сервера и включить его в процесс загрузки. Для этого создаем файл `/etc/init.d/raddb` со следующим содержанием:

```
#!/bin/sh
# chkconfig: 2345 55 25
# description: radius server

PREFIX=/usr/local
OPTS=

test -x /usr/local/sbin/radiusd || exit 0

case "$1" in
  start)
    echo -n "Starting: radius"
    /usr/local/sbin/radiusd
    echo "."
    ;;
  stop)
    echo -n "Stopping service: radius"
    killall radiusd
    echo "."
    ;;
  restart)
    $0 stop
    sleep 2
    $0 start
    ;;
  *)
    echo "Usage: /etc/init.d/radius {start|stop|restart}" >&2
    exit 1
    ;;
esac

exit 0
```

Включаем запуск сервера RADIUS в процесс загрузки сервера:

```
chkconfig raddb on
```


## Настройка сервера VPN

В этом разделе я расскажу, как настроить устройство доступа к VPN Cisco PIX-506E для работы с сервером RADIUS. Для других концентраторов этого семейства настройка производится аналогично:

```
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadline 10
aaa-server RADIUS (inside) host 10.10.10.11
our_password_key timeout 5
```

Последняя строка содержит адрес сервера VPN и пароль-ключ для доступа, который был прописан в `/usr/local/etc/raddb/clients`.

## Заключение

В этой статье я рассмотрел базовую конфигурацию для хранения учетных записей в сервере данных MySQL для последующей интеграции сервера доступа CISCO. Так как большинство производителей сетевого оборудования поддерживают использование авторизации через службу RADIUS, то эта статья может послужить началом для построения централизованной системы по работе с учетными записями пользователей. 

1. <http://cisco.com/en/US/products/hw/vpndevc/index.html>.
2. <http://www.gnu.org/software/radius/radius.html>.
3. [http://en.wikipedia.org/wiki/List\\_of\\_RADIUS\\_Servers](http://en.wikipedia.org/wiki/List_of_RADIUS_Servers).
4. <http://en.wikipedia.org/wiki/RADIUS>.