

openvpn2.0.9 实现 radius 认证

- **核心提示:** 经过实践, 实现了 openvpn2.0.9 版本使用 radius 认证的配置功能。以下简要说明, 与大家分享。 我的环境是 server 端是 linux9.0, Client 端是 winxp。 基本的配置就不复述了, 使用证书认证的文章很多, 其中网友 elm 就有不少好的配置手册。 网络上关于 username/password 认证的文章.....

- 经过实践, 实现了 openvpn2.0.9 版本使用 radius 认证的配置功能。以下简要说明, 与大家分享。

我的环境是 server 端是 linux9.0, Client 端是 winxp。

基本的配置就不复述了, 使用证书认证的文章很多, 其中网友 elm 就有不少好的配置手册。

网络上关于 username/password 认证的文章也不少, 但不是需要用到 mysql 数据库就是要用到 freeradius 认证库, 我就想简单快速的实现把用户名密码提交到第三方 radius 服务器认证就可以了。第三方 radius 服务器很多比如 windows ActiveDirectory 或 WinRadius 2.01, 我这里用 WinRadius2.01 作为 radius 服务器。

1.radiusplugin_v2.0.tar.gz: 可以编译得到 radiusplugin.so

到 <http://www.nongnu.org/radiusplugin/> 下载

2.libgcrypt 支持库: 可以编译得到/usr/lib/libgcrypt.so.11

到 <ftp://ftp.gnupg.org/gcrypt/libgcrypt/libgcrypt-1.2.4.tar.gz> 下载

3.libgpg-error 支持库: 可以编译得到/usr/local/lib/libgpg-error.so.0

到 <ftp://ftp.gnupg.org/gcrypt/libgpg-error/libgpg-error-1.5.tar.gz> 下载

简单的编译以上 3 个支持库, configure; make; make install。

我们要用到 radiusplugin.so, 其他是 radiusplugin.so 的支持库。

好了如果能够得到 radiusplugin.so, 已经成功了 80%, 其他的就是配置了。

把 radiusplugin.so 拷贝到/etc/openvpn 下, 并配置其配置文件 radiusplugin.conf 内容如下:

```
# The NAS identifier which is sent to the RADIUS server
NAS-Identifier=OpenVpn
# The service type which is sent to the RADIUS server
Service-Type=5
# The framed protocol which is sent to the RADIUS server
Framed-Protocol=1
# The NAS port type which is sent to the RADIUS server
NAS-Port-Type=5
# 这是运行 openvpn 服务器的 ip, 作为 radius 客户端
NAS-IP-Address=192.168.2.8
#这里指明 openvpn 的配置位置
OpenVPNConfig=/etc/openvpn/cert_conf/server.conf
```

```
# 这里定义 radius server 参数可以超过 1 个作为备份
server
```

```
{
```

```
    # The UDP port for radius accounting.
```

```
    acctport=1813
```

```
    # The UDP port for radius authentication.
```

```
authport=1812
# 这是我 radius 服务器的 ip, 也就是运行 winradius, 并添加了用户。
name=192.168.2.2
# How many times should the plugin send the if there is no response?
retry=1
# How long should the plugin wait for a response?
wait=1
# The shared secret.共享密钥, 在 winradius 里配置, 设置-系统-NAS 密钥
sharedsecret=winradius
}
```

以下配置 openvpn 服务器, server.conf

这个配置跟证书配置只需新增以下 3 行不同。

```
plugin /etc/openvpn/radiusplugin.so /etc/openvpn/radius.conf
```

```
client-cert-not-required
```

```
username-as-common-name
```

客户端配置: 在 winxp 下

去掉客户端证书, 并添加提示用户密码的参数就可以了。

```
ca ca.crt
```

```
#cert client.crt
```

```
#key client.key
```

```
auth-user-pass
```

启动服务器

```
openvpn --config server.conf
```

如果出错查看日志文件如 openvpn.log 一般可以解决.

启动客户端, 提示

```
Sat Aug 25 17:52:38 2007 OpenVPN 2.0.9 Win32-MinGW [SSL] [LZO] built>
```