openvpn常见问题汇总及其解决办法

Openvpn 常见问题及其解决办法

（2007-01-23 姜道友）

前言：

目前网络或论坛内已经有很多关于openvpn配置或疑难问题的技术文章了，但有一些问题在论坛里讨论得太多，有些贴子根本就是错误的，容易误人子弟。在此我结合官方网站上的FAQ及我自身的技术经验，总结一下，供大家参考，希望对大家有所裨益，并多谢支持。

1、 openvpn资料站点

官方网站：http://www.openvpn.net

论坛：http://bbs.chinaunix.net/forumdisplay.php?fid=50

教程：http://blog.chinaunix.net/u/9284/article_28653.html 内有服务器和客户端配置

2、 如何保存openvpn用户拨入的日志？

可在server.conf中增加如下项即可

status /etc/openvpn/server.log 30

log-append /var/log/openvpn.log

3、 Openvpn采用UDP方式有什么好处？

Openvpn一般使用udp 1194端口（如果你没有修改的话），稳定性比pptp好（实践上的，不是理论上的）。因为NAT不影响UDP，所以openvpn用户不用担心网关设备（如路由器）是否支持NAT-T

4、 客户端拨入成功后如何获取固定IP地址？

在server.conf中增加一行：client-config-dir /etc/openvpn/ccd 然后在ccd目录下分别建立以command name命名的文件，内容为：如：ifconfig-push 192.168.1.5 192.168.1.6

5、 Openvpn服务器是否可以通过图形界面操作？

可以。如可以在ipcop（一种优化的linux防火墙系统）系统中，下载ZERINA-0.9.1b-Installer.tar.gz安装即可通过web方式进行管理：生成用户证书，查看连接信息……等等

6、 如何查看及吊销证书信息？

如果common name为test，则查看test证书为：openssl x509 -in test.pem -noout -subject

查看证书命令为：revoke-crt test

然后make-crl 在server的配置文件中申明crl文件

7、 如何让用户拨入后通过openvpn server连接Internet？

可在server.conf中增加push "redirect-gateway local"，然后在服务器端配置NAT（可以用iptables也可以用RRAS做NAT）

8、 OpenVPN手册中说可以把用户名和密码保存到文件中，我按照手册写的配置文件，启动却发现错误？

为了安全，OpenVPN默认不支持把用户名和密码保存到文件中，如果要支持，在编译时使用：

rpmbuild -tb [openvpn.x.tar.gz] --define 'with_password_save 1'
或使用：./configure --enable-password-save
Windows版本: http://www.cublog.cn/u/2389/showart.php?id=67269

9、 我已经执行了./vars了，为什么还是提示我没有定义KEY_DIR?

注意：vars里面是定义环境变量，每次你重新登录，或者对vars内容进行了修改都要重新读入环境变量，你可以使用： . vars (是：点 空格 vars)或 source vars 来完成。

10、 我在使用easy-rsa脚本生成build-key的时候出现：failed to update database TXT_DB error number 2等，如何解决?

在生成证书时，CommonName不能重复，CN类似一个人的ID

11、 我在运行easy-rsa/build-dh时，屏幕输出的字符很少，请问正常吗?

在第一次运行buidl-dh时会慢且输出很多字符，再次运行时很少为正常

12、 我OpenVPN配置完整后，用户也可以连接Server，且获得了VPN内网地址，但是我ping不通VPN Server的Tap或Tun的地址?

这个问题一般有很多情况，最常见的就是你的机器有多个IP地址且你的OpenVPN使用的是UDP协议，如： eth0(192.168.0.1) eth0:0 (192.168.0.2) 默认网关: 192.168.0.254 ， 解决办法，使用TCP连接，或者在配置文件里面指明 local 192.168.0.1 或 local 192.168.0.2。

13、 我的OpenVPN连接上了，也可以ping同VPN Server的VPN内网地址，为什么我访问不了远程内网的机器呢?

这个问题已经超出了VPN的范围了，只要你能ping同Server的VPN内网地址，说明VPN工作正常了，剩下是网络配置的问题了。VPN Server的forward要打开，并查看远程机器路由表项里面有去往VPN 内网网段的路由项（也可以在VPN Server上启用iptables的MASQUERADE，这个简单）

14、 所有用户都使用相同的用户名/密码 (证书)，但是用户总是频繁掉线?

配置文件里面增加duplicate-cn即可

15、 如何配置使用用户名和密码验证?

可参考此位openvpn专家的文章：
http://blog.chinaunix.net/u/2389/showart.php?id=15825

16、 客户端有时无法获取IP地址，任务图标为黄色?

如果不是网络或服务器问题，可能与客户端电脑有关，可试着重新启动一下DHCP client 服务或重新启动一下电脑（注：有时防病毒软件会造成openvpn不能成功拨入）

17、 64位操作系统是否支持?

目前虽然官方站点提供了64位的TAP驱动程序，但支持性不好，不稳定，建议不要使用64位机器。

18、 其它问题?

直接留言或发邮件给我jdaoyou@sohu.com

发表于： 2007-02-25 ，修改于： 2007-02-25 14:30，已浏览2723次，有评论3条 推荐 投诉

网友评论

内容： 您好!我想請問一下您知道如何把VPN的加密方式改成AES嗎?

它的配置檔裡面有一個指定的選項 不過這樣就算成功了嗎?

fema 评论于：2007-04-23 01:22:58 （122.127.64.★）

内容： 你好 。

请问

动态IP 能做openvpn 服务器不 ？

我在AS4 上 安装 openvpn 已经 成功

可是

我是用 ADSL +Squid 上网的

动态的IP 很是麻烦 能不能有什么方法 让client 知道我 server的 ip ？

easyadmi 评论于：2007-07-09 08:56:13 （219.132.205.★）

内容： 你好，我现在想在openVPN的每个节点上都用读卡器和智能卡来读存密钥和证书，应该怎么实现，请你指导一下！！

本站网友评论于：2008-05-07 20:54:49 （121.229.180.★）

发表评论

用户名： 密码： 免费注册

验证码： X559 匿名

提交