上海富虎系统网络有限公司

专业

值得信赖

OPENVPN
安装配置和生产实践

提纲

一、OPENVPN介绍
二、安装配置
三、CA证书安装
四、服务器端配置
五、客户端安装
六、启动和停止
七、WIN客户端安装
八、经验交流

一、OPEN VPN介绍

1.1、基本情况

- VPN--虚拟专用通道，提供给企业之间或者个人与公司之间安全数据传输的隧道
- OPENVPN是一个基于 OpenSSL 库的应用层 VPN 实现,大量使用了OpenSSL加密库中的SSLv3/TLSv1协议函数库
- 能在Solaris、Linux、OpenBSD、FreeBSD、NetBSD、Mac OS X与Microsoft Windows以及Android和iOS上运行
- 不是一个基于Web的VPN软件，也不与IPsec及其他VPN软件包兼容

1.2、优点

- 简单易用
- 良好的性能
- 友好的用户GUI

1.3、身份验证方式

- 用户名/密码组合——可以省略客户端证书，但是仍有一份服务器证书需要被用作加密
- 预享密钥——最为简单，但同时它只能用于建立点对点的VPN；
- CA证书——基于PKI的第三方证书提供了最完善的功能，但是需要额外的精力去维护一个PKI证书体系。

1.4、网络特性(1)

- 通信都基于一个单一的IP端口；
- 默认且推荐使用UDP协议通讯，同时TCP也被支持。
- 有高延迟或者丢包较多的情况下，请选择TCP协议作为底层协议
- OpenVPN连接能通过大多数的代理服务器，并且能够在NAT的环境中很好地工作。
- 服务端具有向客户端“推送”某些网络配置信息的功能，这些信息包括：IP地址、路由设置等。

1.4、网络特性(2)

- 提供两种虚拟网络接口：TUN和TAP驱动，建立三层IP隧道，或者虚拟二层以太网，后者可以传送任何类型的二层以太网络数据
- 传送的数据可通过LZO算法压缩
- 每个进程可以同时管理数个并发的隧道
- 能通过大多数的代理服务器，并且能够在NAT的环境中很好地工作
- 服务端具有向客户端“推送”某些网络配置信息的功能，这些信息包括：IP地址、路由设置等。

1.5、安全特性

- 在用户空间运行，无须对内核及网络协议栈作修改；
- 初始完毕后以chroot方式运行，放弃root权限；
- 使用mlockall以防止敏感数据交换到磁盘；
- OpenVPN通过PKCS#11支持硬件加密标识，如智能卡；
- 使用OpenSSL库加密数据与控制信息，能够使用任何OpenSSL支持的算法。
- 提供了可选的数据包HMAC功能以提高连接的安全性。
- OpenSSL的硬件加速也能提高它的性能。

1.6、工作原理(1)

- OPENVPN的技术核心：虚拟网卡、SSL协议实现
- 虚拟网卡是使用网络底层编程技术实现的一个驱动软件，安装后在主机上多出现一个网卡，可以像其它网卡一样进行配置
- 服务程序可以在应用层打开虚拟网卡
- 虚拟网卡底层驱动在很多的操作系统下都有相应的实现，所以它能够跨平台实现

1.6、工作原理(2)

- 访问一个远程的虚拟地址(属于虚拟网卡配用的地址系列，区别于真实地址)，则操作系统会通过路由机制将数据包(TUN模式)或数据帧(TAP模式)发送到虚拟网卡上
- 服务程序接收该数据并进行相应的处理后，通过SOCKET从外网上发送出去，
- 远程服务程序通过SOCKET从外网上接收数据，并进行相应的处理后，发送给虚拟网卡
- 应用软件可以接收到，完成了一个单向传输的过程

- 二、安装配置

2.1、服务器端编译安装

- 从openvpn.net下载最新版本的tar.gz包
- 使用命令 tar –zxvf 解开tar.gz包
- ./configure –prefix=/opt/openvpn-2.3.a
- make
- make install

2.2、客户端安装

- REDHAT/CENTOS：yum install openvpn
- DEBIAN/UNBONTU：apt-get install openvpn

- 三、CA证书安装

3.1、准备阶段

- Init-config—复制自动运行脚本
- ./vars—运行脚本
- ./Clean-all—复制index.txt和serial文件

3.2、制作根证书

./build-ca

- 根据步骤输入国家、省、地区、公司名称、e-mail、common Name
- 生成ca.key和ca.crt文件

3.3、制作服务器证书

./build-key-server server-name

- 根据步骤输入国家、省、地区、公司名称、e-mail、common Name
- 生成server-name.key、server-name.crt、server-name.csr文件和pem文件

3.4、制作客户端证书

./build-key client

- 根据步骤输入国家、省、地区、公司名称、e-mail、common Name
- 生成client.key、client.crt、client.csr文件和相关的pem文件

3.5、制作DH证书

./build-dh

- 生成dh.pem文件

3.6、所有证书文件

- ca.crt
- ca.key
- dh.pem
- server.crt
- server.key
- client.crt
- client.key

- 四、服务器端配置

4.1、配置清单(1)

```
persist-key          ##默认值，避免重启后信息丢失
persist-tun          ##默认值，避免重启后信息丢失
comp-lzo             ##LZO压缩
client-to-client     ##允许客户端之间互相通讯
tls-server       ##安全加固
```

4.1、配置清单(2)

```
local        xxx.xxx.xxx.xxx##绑定本地IP地址
port         xxxx            ##端口号
proto        udp             ##协议
dev          tun0            ##设备名称:tun或TAP
ca           ca.crt          ##CA证书
cert         server.crt      ##服务器证书
key          server.key      ##服务器密钥
dh           dh.pem          ##DH证书
```

4.1、配置清单(3)

server 192.168.11.0 255.255.255.0 ##虚拟网卡网段

push “route 192.168.10.0 255.255.255.0“ ##推送静态路由

route 192.168.11.0 255.255.255.252 ##路由虚拟网卡

keepalive 10 60 ##会话保持时间

tls-auth ta.key 0 ##安全加固,防攻击

注意:openvpn –genkey –secret ta.key

cipher DES-EDE3-CBC ##安全加固，大键值

4.1、配置清单(4)

```
max-clients     5           ##最大客户端数量
user            nobody      ##安全加固
group           nobody      ##安全加固
verb            4           #日志级别
mute            20          #默认值，消息重复次数
chroot          /opt/openvpn/etc  ##安全加固
tls-cipher      AES256-SHA ##安全加固
mode            server      ##安全加固
```

4.1、配置清单(5)

ifconfig-pool-persist ipp.txt ip地址池

client-config-dir ccd ##CLIENT获得固定的IP地址

注意:在ccd目录下配置和证书一致的文件名，内容如下:

ifconfig-push 192.168.11.5 192.168.11.6

#status openvpn-status.log ##OPENVPN状态信息

#log openvpn.log ##OPENVPN日志

4.1、配置清单(6)

crl-verify　　crl.pem

注意:

./vars

./revoke-full client生成crl.pem文件

- 五、客户端配置

5.1、配置清单(1)

```
Client                          ##申明是客户端
dev tun0                        ##设备名称，同服务器端
proto udp                       ##协议
remote xxx.xxx.xxx.xxx  xxx     ##服务器端的IP地址和端口
resolv-retry infinite           ##默认值
                        ##用于主机名域名解析
Nobind                  ##客户端不绑定端口号
persist-key             ##避免重启后信息丢失
persist-tun             ##避免重启后信息丢失
```

5.1、配置清单(2)

```
mute-replay-warnings    ##避免重复数据包的报警
ca ca.crt               ##CA证书
cert client.crt         ##客户端证书
key client.key          ##客户端密钥
```

5.1、配置清单(3)

```
ns-cert-type server                 ##强化认证
tls-auth ta.key 1                   ##与服务器端相配
cipher DES-EDE3-CBC                 ##与服务器端相配
comp-lzo                            ##与服务器端相配
verb 4                              ##与服务器端相配
mute 20                             ##与服务器端相配
```

5.1、配置清单(4)

```
remote-cert-tls server                  #强化认证
tls-remote server                       ##强化认证
tls-client                          ##与服务器端相配
tls-cipher AES256-SHA                   ##与服务器端相配
#status     openvpn-status.log  ##与服务器端相配
#log-append  openvpn.log  ##与服务器端相配
```

六、启动和停止

- （1）启动：

  /etc/init.d/openvpn start

- （2）停止：

- /etc/init.d/openvpn stop

七、WIN客户端安装

- （1）从OPENVPN.NET上下载openvpn.exe(windows版)
- （2）安装openvpn.exe
- （3）安装完毕后右击openvpn GUI图标并选择属性，勾选以管理员身份运行；
- （4）将client.key、client.crt、client.crt文件存放在安装目录的config目录下；
- （5）配置文件openvpn.ovpn的内容见WORD文档；

八、经验交流

- 比堡垒机和跳板机更加安全可靠
- 比专线便宜
- 对技术人员行为约束和规范
- 大网环境统一管理
- 提升运维效率和质量