黑客派

CentOS6.5 OpenVPN

作者：xfell

原文链接：https://hacpai.com/article/1549034418080

来源网站：黑客派

<h4 id="VPN概述">VPN 概述</h4>

<blockquote>
VPN(全称 Virtual Private Network)虚拟专用网络，是依靠 ISP 和其他的 NSP，在公共网络中立专用的数据通信网络的技术，可以为企业之间或者个人与企业之间提供安全的数据传输隧道服务。在VPN 中任意两点之间的连接并没有传统专网所需的端到端的物理链路，而是利用公共网络资源动态成的，可以理解为通过私有的隧道技术在公共数据网络上模拟出来的和专网有同样功能的点到点的专技术。
</blockquote>
<h4 id="企业需求">企业需求</h4>
<blockquote>
企业内部员工出差、休假或特殊情况下在远离办公室的时候，又有需求访问公司的内部网络获相关资源，就可以通过 VPN 拨号到公司内部。此时远程拨号的员工和办公室内的员工以及其他拨号员工之间都相当于在一个局域网内。例如：访问内部的域控制器，文件服务器，OA 系统，ERP，HTT 服务，内网飞秋聊天工具等局域网服务应用。运维人员需要个人电脑远程拨号到企业网站的 IDC 机，远程维护 IDC 内网服务器
</blockquote>
<pre><code class="highlight-chroma">#添加epel源：
rpm -ivh http://mirrors.yun-idc.com/epel/epel-release-latest-6.noarch.rpm

#安装openvpn和easy-rsa（创建证书）：
yum install openvpn easy-rsa -y

#拷贝easy-rsa文件夹到openvpn里 并只保留3.0.3 其余删除
cp -a /usr/share/easy-rsa/ /etc/openvpn/

#修改默认vars 文件
cd /etc/openvpn/easy-rsa/3.0.3
find / -type f -name “vars.example” | xargs -i cp {} . not found render function for node [typ=NodeHTMLEntity, Tokens=&]not found render function for node [type=NodeHTMLEntity, Tkens=&]not found render function for node [type=NodeHTMLEntity, Tokens=&]not ound render function for node [type=NodeHTMLEntity, Tokens=&] mv vars.example vars
#修改以下内容：
set_var EASYRSA_REQ_COUNTRY “CN”
set_var EASYRSA_REQ_PROVINCE “Beijing”
set_var EASYRSA_REQ_CITY “Beijing”
set_var EASYRSA_REQ_ORG “XfellCert”
set_var EASYRSA_REQ_EMAIL “xfell96@163.com”
set_var EASYRSA_REQ_OU “My OpenVPN”</code></pre>

生成证书

#创建一个新的 PKI 和 CA

cd /etc/openvpn/easy-rsa/3.0.3

./easyrsa init-pki　　#创建空的pki

./easyrsa build-ca nopass　#创建新的CA，不使用密码 然后 回车

#创建服务端证书

./easyrsa gen-req server nopass # 回车

#签约服务端证书

./easyrsa sign server server

创建 Diffie-Hellman

./easyrsa gen-dh

创建客户端证书

mkdir /etc/openvpn/client/

cp -a /usr/share/easy-rsa/ /etc/openvpn/client/

rm -rf 3 3.0

cd 3.0.3/

find / -type f -name "vars.example" | xargs -i cp {} . not found render function for node [typ
=NodeHTMLEntity, Tokens=&]not found render function for node [type=NodeHTMLEntity, T
kens=&]not found render function for node [type=NodeHTMLEntity, Tokens=&]not
ound render function for node [type=NodeHTMLEntity, Tokens=&] mv vars.example vars

./easyrsa init-pki

./easyrsa gen-req xfell nopass　　# 客户证书名 xfell 不需要密码 回车

进openvpn_server 签约客户端证书

cd /etc/openvpn/easy-rsa/3.0.3/

./easyrsa import-req /etc/openvpn/client/easy-rsa/3.0.3/pki/reqs/xfell.req xfell

./easyrsa sign client xfell # 输入yes

#整理证书:

mkdir /etc/openvpn/certs

cd /etc/openvpn/certs/

cp /etc/openvpn/easy-rsa/3.0.3/pki/dh.pem .

cp /etc/openvpn/easy-rsa/3.0.3/pki/ca.crt .

cp /etc/openvpn/easy-rsa/3.0.3/pki/issued/server.crt .

cp /etc/openvpn/easy-rsa/3.0.3/pki/private/server.key .

#没问题的话 应该是以下文件：

ca.crt dh.pem server.crt server.key

#客户端所需文件：

mkdir /etc/openvpn/client/xfell

cp /etc/openvpn/easy-rsa/3.0.3/pki/ca.crt /etc/openvpn/client/xfell

cp /etc/openvpn/easy-rsa/3.0.3/pki/issued/xfell.crt /etc/openvpn/client/xfell

cp /etc/openvpn/client/easy-rsa/3.0.3/pki/private/xfell.key /etc/openvpn/client/xfell

#没问题的话 应该是以下文件：

ca.crt xfell.crt xfell.key

#编辑服务端配置文件：

cp /usr/share/doc/openvpn-2.4.5/sample/sample-config-files/server.conf /etc/openvpn/server conf

local 192.168.1.113 #本机ip 服务器处于NAT后面 写公网ip

port 52000 #监听端口 建议修改为其他端口 避免端口被封

; proto tcp

proto udp #采用udp协议 传输速度快

dev tun # 网卡名称

ca /etc/openvpn/certs/ca.crt # 4个证书位置

cert /etc/openvpn/certs/server.crt

key /etc/openvpn/certs/server.key

dh /etc/openvpn/certs/dh.pem

ifconfig-pool-persist /etc/openvpn/ipp.txt #使用过vpn的ip日志列表

server 17.166.221.0 255.255.255.0 # VPN 连接后DHCP分配的 地址

push “route 192.168.1.0 255.255.255.0” # 让上面分配的17网段ip 可以和这个 互通

push “redirect-gateway def1 bypass-dhcp” # 想客户端 推送路由信息 所有流量都走推送的路由

push “dhcp-option DNS 223.5.5.5” # DNS解析

push “dhcp-option DNS 223.6.6.6”

client-to-client # 客户端之间互通

keepalive 20 120 # ping机制 20秒检测一次 120秒无响应 即断开连接

comp-lzo # 启用lzo压缩

duplicate-cn

user openvpn # 指定运行OpenVPN运行用户

group openvpn

persist-key # 持久化选项可以尽量避免访问那些在重启之后由于用户权限降低而无法访问的某些资源

persist-tun

status openvpn-status.log

log-append openvpn.log

verb 1 #日志级别 一般选择5 -6

mute 20 # 相同日志 只用前20条显示

</code></pre>

<pre><code class="highlight-chroma">#配置iptables 转发:
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state –state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state –state NEW -m tcp -p tcp –dport 22 -j ACCEPT
-A INPUT -m state –state NEW -m tcp -p tcp –dport 80 -j ACCEPT
-A INPUT -m state –state NEW -m tcp -p tcp –dport 3306 -j ACCEPT
-A INPUT -m state –state NEW -m udp -p udp –dport 52000 -j ACCEPT # OpenVPN的UDP端口
-A INPUT -j REJECT –reject-with icmp-host-prohibited
#-A FORWARD -j REJECT –reject-with icmp-host-prohibited # 连接正常 ping不通 就是这条规导致的 网上大部分文档 都有 要结合自己服务器注意一下
COMMIT
Completed on Tue Apr 24 15:53:06 2018
Generated by iptables-save v1.4.7 on Tue Apr 24 15:53:06 2018
*nat
:PREROUTING ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
[5:417] -A POSTROUTING -s 17.166.221.0/24 -o eth0 -j MASQUERADE # 绑定连接成功的ip 通VPN服务器的eth0网卡 上网
COMMIT

命令行操作也可以：iptables -t nat -I POSTROUTING -s 17.166.221.0/255.255.255.0 -o eth0 -j ASQUERADE # masquerade的意思是 动态获取公网ip

#吊销证书:

./vars 初始化

./easyrsa revoke EntityName # EntityName 是 Client-Name 证书名字

#执行之后会得到一个 .pem 结尾的文件 （里面写了被注释的证书列表）

#编辑server.conf 添加 /etc/openvpn/ *.pem 重启服务端即可

</code></pre>

<h4 id="Windows客户端配置-下载-http---build-openvpn-net-downloads-releases-">Windows客户端配置 下载：http://build.openvpn.net/downloads/releases/</h4>

<pre><code class="highlight-chroma">#将服务器中的 /etc/openvpn/client/xfell文件夹下的3文件和手动生成的 ta.key 文件 全部拷贝下来 放到 C:\Program Files\OpenVPN\config
#生成命令：
openvpn –genkey –secret /etc/openvpn/ta.key 缺少ta.key 启动时会报 Options error: –tls-auth fils with ‘ta.key’ : No such file or directory错误
</code></pre>
<script async src="https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></script>
<!-- 黑客派PC帖子内嵌-展示 -->
<ins class="adsbygoogle" style="display:block" data-ad-client="ca-pub-5357405790190342" data-ad-slot="8316640078" data-ad-format="auto" data-full-width-responsive="true"></ins>
<script>
    (adsbygoogle = window.adsbygoogle || []).push({});
</script>

<pre><code class="highlight-chroma">#然后把 /usr/share/doc/openvpn-2.4.5/sample/sample-config-files/client.conf 也拷到C:\Program Files\OpenVPN\config 文件夹下 并重命名client.ovp

#client.ovpn 配置文件如下（官方注释内容以及删除）
client # 指定此配置文件是客户端
;dev tap # 桥接模式 此配置中是注释的
dev tun # 路由模式
;dev-node MyTap # windows系统中 配置多个隧道 需要
;proto tcp # 指定服务器采用TCP还是UDP协议
proto udp
remote x.x.x.x 52000 # VPN服务器的公网ip 以及连接端口
;remote my-server-2 1194 # 如果有多个服务器做负载均衡 需要填写多个
;remote-random # 如果有多个服务器 改指令 会随机连接
resolv-retry infinite # 客户端与服务器断开连接 会自动重新连接
nobind # 用来绑定端口号 一般没用
;user nobody # 降低vpn权限 一般不用
;group nobody
persist-key # 持久化选项 避免在重启时 由于权限问题 无法访问资源
;persist-tun # 此选项要注释 会导致客户端连接之后 频繁掉线
;http-proxy-retry # retry on connection failures # 通过HTTP代理方式来连接VPN服务器
;http-proxy [proxy server] [proxy port #]
;mute-replay-warnings # 忽视重复数据包的警告信息
ca ca.crt # 以下3个选项是指定 证书文件的位置
cert xfell.crt
key xfell.key
remote-cert-tls server
tls-auth ta.key 1 # 使用 tls-auth 密钥
cipher AES-256-CBC # 认证默认密码
comp-lzo yes # 使用lzo压缩

verb 3 # 日志级别
;mute 20 # 只显示不同信息前20条

保存 打开客户端 连接即可

</code></pre>

<img src="https://static.hacpai.com/images/img-loading.svg" alt="clipboard11png" data
src="https://fly.qxfell.com//file/2019/02/8eb17056fa7c40848418668ba3dc7d06_clipboard11.
ng">
<h4 id="遇到的一些坑">遇到的一些坑</h4>
<pre><code class="highlight-chroma">1，OpenVPN客户端连接正常 无法ping通主机 注释下
这条 iptables规则 因为防火墙中没有FORWARD链中没有规则，所以数据包都被drop掉
#-A FORWARD -j REJECT –reject-with icmp-host-prohibited

2，启动openvpn 报错 Options error: –tls-auth fails with ‘ta.key’ : No such file or directory
openvpn –genkey –secret /etc/openvpn/ta.key

3，客户端正常 访问也正常 但是频繁有规律的掉线 在2分钟左右 （参考连接https://www.ifshow.co
/openvpn-server-and-client-configuration-file-description/）将Client端中的 ;persist-tun选项
释掉

4，无法解析内网自建DNS域名（参考连接https://www.petenetlive.com/KB/Article/0001402）
修改系统的TCP/IP 协议的 接口跃点数 为10
</code></pre>

<script async src="https://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js"></scr
pt>

<!-- 黑客派PC帖子内嵌-展示 -->

<ins class="adsbygoogle" style="display:block" data-ad-client="ca-pub-5357405790190342"
data-ad-slot="8316640078" data-ad-format="auto" data-full-width-responsive="true"></in
>
<script>
    (adsbygoogle = window.adsbygoogle || []).push({});
</script>
<h4 id="Mac-Install">Mac Install</h4>
下载链接：<a href="https://link.hacpai.com/forward?goto=https%3A%2F%2Ftunnelblick.
et%2Fdownloads.html" target="_blank" rel="nofollow ugc">https://tunnelblick.net/download
.html （需翻墙）
 Tunnelblick_3.7.5a_build_5011.dmg 打开双击安装运行
 然后 将
的 client.ovpn 文件拖到菜单栏 接着连接即可