openvpn配置实现服务器代理上网

原创 调试大师 于 2024-01-27 10:55:38 发布 阅读量8.3k 收藏 45 点赞数 58 版权
分类专栏： 计算机网络 vpn 文章标签： 服务器 运维

摘要 本文详细介绍了OpenVPN的原理、应用场景，以及在CentOS系统中搭建OpenVPN服务器，涉及环境准备、证书生成、iptables配置、服务端和客户端的详细步骤，旨在帮助读者实现安全的远程连接和企业内部网络扩展。

摘要由CSDN通过智能技术生成

1.概述

OpenVPN是一个开源的虚拟专用网络（VPN）软件，可以用于在不安全的网络（如互联网）上为用户提供安全的网络连接。它使用加密的数据通道来确保数据的安全性，并可以通过多种方式来构建虚拟网络，包括使用TCP或UDP协议，使用安全套接字层（SSL）或传输层安全（TLS）加密数据通道，或者使用混合模式，即同时使用多种方式。

OpenVPN可以在多种平台上运行，包括Windows、MacOS、Linux、Android和iOS等。它可以与多种路由器和网络设备集成，并提供了丰富的配置选项，使用者可以根据自己的需要来自定义设置。

支持多种加密算法：OpenVPN支持使用多种加密算法来保护数据的安全性，包括AES、Blowfish、CAST-128、DES、3DES、RC5和IDEA等。

支持多种协议：OpenVPN可以使用TCP或UDP协议来建立虚拟网络，并且支持使用SSL或TLS来加密数据通道。

2.应用场景

2.1总部与分支机构之间联通，打通分支与总部的连接

2.2 通过 VPN 远程连接到公司的服务器，企业员工远程办公，访问公司内网的ERP、OA等系统。

3. 环境搭建

本篇文章以centos为例演示如何搭建并使用openvpn。

3.1环境准备

3.1.1安装 easy-rsa、iptables-service

```
yum -y install easy-rsa iptables-service
```

3.1.2 配置系统转发，并使配置立即生效

```
echo net.ipv4.ip_forward=1 >> /etc/sysctl.conf
sysctl -p
```

3.1.2 关闭firewall

```
systemctl stop firewalld

systemctl disable firewalld
```

3.1.3启动iptables

```
systemctl enable iptables

systemctl start iptables
```

3.1.4 配置iptables转发流量,代理主要以iptables转发实现

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE
```

3.1.5 允许tcp/udp 1194通过防火墙

```
iptables -I INPUT -p tcp –dport 1194 -j ACCEPT

iptables -I INPUT -p udp –dport 1194 -j ACCEPT
```

3.1.6 保存规则并重启

```
service iptables save

systemctl restart iptables
```

3.2 服务端环境搭建

3.2.1 安装openvpn

```
yum -y install openvpn
```

3.2.2 生成服务器端证书

查看easy-rs安装路径

```
rpm -ql easy-rsa
```

复制easy-rsa到/etc/openvpn目录

```
cp -r /usr/share/easy-rsa/ /etc/openvpn/easy-rsa
```

复制easy-rsa配置文件到/etc/openvpn/easy-rsa/3.0.8目录,并重命名为vars

```
cp -r /usr/share/doc/easy-rsa/vars.example /etc/openvpn/easy-rsa/3.0.8/vars
```

查看/etc/openvpn目录结构

```
tree /etc/openvpn
```

修改证书配置文件vars,其他的默认即可,主要是修改个人信息,也可以不改

```
vim /etc/openvpn/easy-rsa/3.0.8/vars
```

修改内容如下

```
set_var EASYRSA_REQ_COUNTRY "CN"

set_var EASYRSA_REQ_PROVINCE "SD"
```

```
set_var EASYRSA_REQ_CITY "JN"
set_var EASYRSA_REQ_ORG "SY"
set_var EASYRSA_REQ_EMAIL "sywl@sywl123.com"
set_var EASYRSA_REQ_OU "tpc"
```

初始化

```
cd /etc/openvpn/easy-rsa/3.0.8
./easyrsa init-pki
```

为方便安装测试，这里使用onpass参数选择不要密码创建根证书

```
./easyrsa build-ca nopass
```

创建server端证书、私钥文件

```
./easyrsa gen-req server nopass
```

给server端证书签名,提示confirm request details:时,输入yes

```
./easyrsa sign server server
```

创建dh文件（秘钥交换算法）

```
./easyrsa gen-dh
```

创建tls认证秘钥

```
openvpn –genkey –secret ta.key
```

查看当前生成的文件目录结构

```
tree pki
```

拷贝证书文件到openvpn目录下

```
mkdir /etc/openvpn/certs
cp ./pki/ca.crt /etc/openvpn/certs/
cp ./pki/dh.pem /etc/openvpn/certs/
cp ./pki/issued/server.crt /etc/openvpn/certs
cp ./pki/private/server.key /etc/openvpn/certs
cp ta.key /etc/openvpn/certs
```

3.2.3 创建server配置文件

复制配置模板文件server.conf到/etc/openvpn/

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

修改server.conf配置文件

```
cd /etc/openvpn
```

```
vim server.conf
```

内容如下：

```
#监听本机ip地址
local 0.0.0.0(这里填本机地址)
#监控本机端口号
port 1194
#指定采用的传输协议，可以选择tcp或udp
proto tcp
#指定创建的通信隧道类型，可选tun或tap,window服务器必须是tap
dev tun
#指CA证书的文件路径
ca /etc/openvpn/certs/ca.crt
#指定服务器端的证书文件路径
cert /etc/openvpn/certs/server.crt
#指定服务器端的私钥文件路径
key /etc/openvpn/certs/server.key
dh /etc/openvpn/certs/dh.pem
#指定虚拟局域网占用的IP地址段和子网掩码，不能和服务器eth0同网段
server 10.8.0.0 255.255.255.0
#服务器自动给客户端分配IP后，客户端下次连接时，仍然采用上次的IP地址(第一次 分配的IP保存在ipp.txt中，下一次分配其中保存的IP)。
ifconfig-pool-persist ipp.txt
#自动推送客户端上的网关及DHCP,此项开启了流量转发,有这项才能使用服务器代理上 网
push "redirect-gateway def1 bypass-dhcp"
#OpenVPN的DHCP功能为客户端提供指定的 DNS、WINS 等
push "dhcp-option DNS 114.114.114.114"
#允许客户端与客户端相连接，默认情况下客户端只能与服务器相连接
client-to-client
#允许同一个客户端证书多次登录,看需配置
#duplicate-cn
#每10秒ping一次，连接超时时间设为120秒
keepalive 10 120
#开启TLS-auth，使用ta.key防御攻击。服务器端的第二个参数值为0，客户端的为1。
tls-auth /etc/openvpn/certs/ta.key 0
#加密认证算法,2.4之前是AES-256-CBC
cipher AES-256-GCM
#使用lzo压缩的通讯,服务端和客户端都必须配置
comp-lzo
#最大连接用户
max-clients 100
#定义运行的用户和组,openvpn用户是安装的时候系统自动创建的
user openvpn
group openvpn
#重启时仍保留一些状态
```

```
persist-key

persist-tun

#输出短日志,每分钟刷新一次,以显示当前的客户端

status /var/log/openvpn-status.log

#日志保存路径

log /etc/openvpn/log/openvpn.log

log-append /etc/openvpn/log/openvpn.log

#指定日志文件的记录详细级别，可选0-9，等级越高日志内容越详细

verb 3

#相同信息的数量，如果连续出现 20 条相同的信息，将不记录到日志中

mute 20

#下面这项只能udp连接开启

#explicit-exit-notify 1

#设置tls最低版本为1.3,连接的客户端如果是2.4以下则配置为1.0

tls-version-min 1.3
```

3.2.4 创建启动的服务脚本

创建unit文件

```
vim /lib/systemd/system/openvpn@.service
```

内容如下:

```
[Unit]

Description=OpenVPN Robust And Highly Flexible Tunneling Application On %I

After=network.target

[Service]

Type=notify

PrivateTmp=true

ExecStart=/usr/sbin/openvpn —cd /etc/openvpn/ —config %i.conf

[Install]

WantedBy=multi-user.target
```

设置openvpn开机启动

```
systemctl enable openvpn@server
```

启动openvpn

```
systemctl start openvpn@server
```

查看端口和进程是否启动成功,

```
netstat -lntp|grep openvpn
```

```
ps -aux|grep openvpn
```

3.3 客户端配置

3.3.1 下载windows客户端

https://openvpn.net/index.php/download/community-downloads.html

3.3.2 服务端生成并配置客户端证书信息

进入证书管理目录

```
cd /etc/openvpn/easy-rsa/3.0.8
```

生成客户端证书

```
./easyrsa gen-req client1 nopass
```

注册客户端1的证书,输入yes

```
./easyrsa sign client client1
```

将证书拷贝到一个目录存着

```
cp ./pki/issued/client1.crt /etc/openvpn/client
cp ./pki/private/client1.key /etc/openvpn/client
```

3.3.3 本地电脑客户端配置

将client1.crt client1.key ta.key ca.crt四个文件下载到本地客户端目录的config目录下。

配置客户端配置文件,复制客户端sample-config目录下的client.ovpn文件到config目录下修改内容如下:

```
#客户端
client
#隧道类型,与服务器一致
dev tun
#tcp还是udp,与服务器一致
proto tcp
#服务器ip和端口
remote xxx.xxx.xxx.xxx 1194
#自动重连
resolv-retry infinite
#不绑定本地特定的端口
nobind
#服务器重启后保持一些状态
persist-key
persist-tun
#客户端证书目录
ca ca.crt
cert client.crt
key client.key
#远程证书验证
remote-cert-tls server
#tls握手秘钥,与服务器保持一致,服务器0,客户端1
tls-auth ta.key 1
#加密方式
```

```
cipher AES-256-GCM

开启数据压缩

comp-lzo

#日志级别

verb 3

#同信息的数量，如果连续出现 20 条相同的信息，将不记录到日志中

mute 20

#tls最低版本,与服务器保持一致

tls-version-min 1.3

#不保存密码

auth-nocache

#使客户端中所有流量经过VPN,所有网络连接都使用vpn

redirect-gateway def1
```

打开客户端,右键选项修改配置文件目录,双击连接服务器

文章知识点与官方知识档案匹配，可进一步学习相关知识

云原生入门技能树 > 首页 > 概览　20393 人正在系统学习中

搭建OpenVpn实现服务器代理上网　weixin_44105868的博客　2653
8. 装配完成后root目录下生成了对应的xxx.ovpn文件（xxx就是第6步的client名字）10. 腾讯云服务器管理页面添加防火墙规则，UDP-1194-允许。6. 运行后我们可以在右下角任务栏…

史上最详细保姆级教程部署OpenVPN　XLB　9767
提供给公司与子公司或者公司个人与公司之间建立安全的数据传输

代理(Proxy)和虚拟专用网络(VPN)有区别,现在才明白。　10-13
代理可以用于浏览器或单个应用程序,通常只改变特定应用程序的IP地址。代理通常可以来提供网络加速服务或者访问被公司或学校防火墙阻止的网站等。 例子:通俗来讲代理用来加…

代理服务器、虚拟专用网络、网关_虚拟专网和虚拟网关的区别　9-30
反向代理:代理服务器接受所有访问(Nginx负载均衡等) VPN:虚拟专用网络 概念 VPN在公用网络上建立专用网络,进行加密通讯。 特点 类似一种代理服务器 过程 客户机的VPN客户端…

openVPN客户端开机自动连接（系统启动文件夹法）　FJSAY　537
本文章为个人学习记录/笔记，如有错误请指出，如有雷同纯属巧合！4.把这个快捷方式复制到系统开机启动文件夹。1.首先在桌面找到openVPN的图标。2.右键，属性，然后在目标…

用树莓派搭建（虚拟专用网络）服务器　silent_F的博客　1万+
笔者这里是使用树莓派搭建VPN服务器,树莓派是用的ubuntu系统,所以该方法使用于所有的ubuntu系统的服务器.　想要用服务器搭建VPN服务器,你首先得上手一个树莓派,可以参…

计算机网络体系结构-虚拟专用网_vpls和vpws的区别　10-15
计算机网络体系结构-虚拟专用网 VPN的用途 代理服务器Proxy Server,其功能就是代理网络用户去取得网络信息。形象的说:它是网络信息的中转站。 与代理服务器不同。VPN是解决…

浅谈VPC,VPS,VPN,frp,代理服务器,云服务器_vps和vpc　10-11
VPC 私有网络是针对公有云的基础网络来定义的,简单来说,就是在公有云上开辟一处只属于自己的网络。 那么什么又是公有云? 公有云是面向大众提供计算资源的服务 2.VPS: VPS(…

vpn和代理有啥区别　smallfatman的博客　3698
VPN和代理都是网络上常见的工具，用于隐藏用户的真实IP地址和提供更安全的网络连接。虽然它们有一些相似之处，但也存在一些重要的区别。

VPN（虚拟专用网络）和代理（Proxy）　最新发布　u012698191的博客　1113
VPN（虚拟专用网络）和代理（Proxy）都是用于隐藏用户的真实IP地址、保护隐私并绕过网络限制的工具，但它们的工作原理和应用场景有所不同。

从OSI七层模型和代理、虚拟专用网络_代理是哪个网络层的东西　10-9
应用层: FTP服务代理器:主要用于访问FTP服务器,一般有上传、下载以及缓存的功能,端口号一般为21、2121等。 HTTP服务代理器:主要用于访问网页,一般有内容过滤和缓存功能,端…

代理ip与vps的区别是什么_代理ip与vps有什么区别,哪个更好用?-CSDN...　10-15
代理IP与VPS(Virtual Private Server,虚拟专用服务器)在网络技术和应用领域中扮演着不同的角色,它们在功能、独立性、控制权以及应用场景等方面存在显著的差异。以下是对代理IP…

Windows 下的 OpenVPN 安装　热门推荐　pcplayer的博客　2万+
Windows 底下的 OpenVPN 安装配置。

傻瓜式一键命令自动搭建OpenVPN反向代理，学习交流　坚持，努力，奋斗不止　2235
这里用的是centos 7.6。

网络知识_vps反向代理虚拟主机　10-12
反向代理 反向代理:比方,租房子。房东小红想把房子租出去,但