# AWS动手实验VPN搭建

实验目的

通过在Linux上搭建基于PPTP协议的VPN, 实现用户远程连接服务器, 并通过配置nat转发访问internet.

学前建议

了解Amazon Web Services

了解VPC

了解EC2

有Linux基础

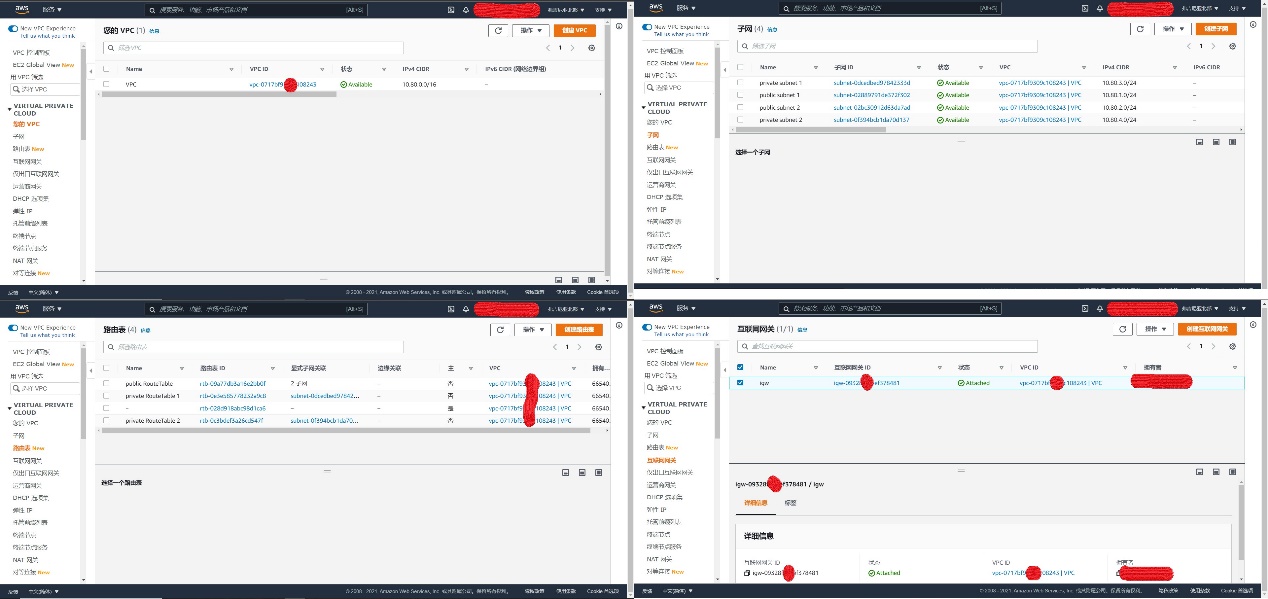
了解PPTP VPN

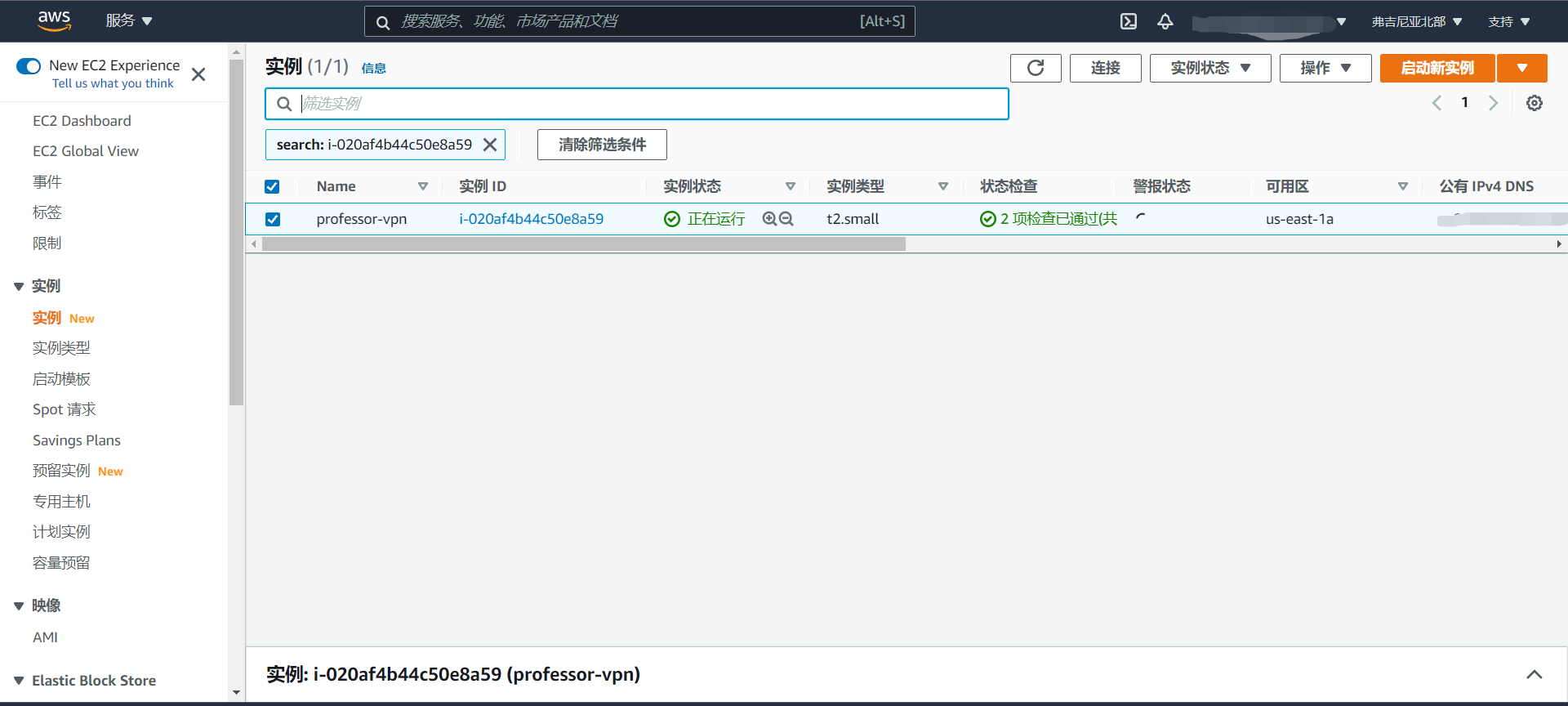
实验原理

通过搭建VPN服务器让用户远程接入, 并访问Internet.

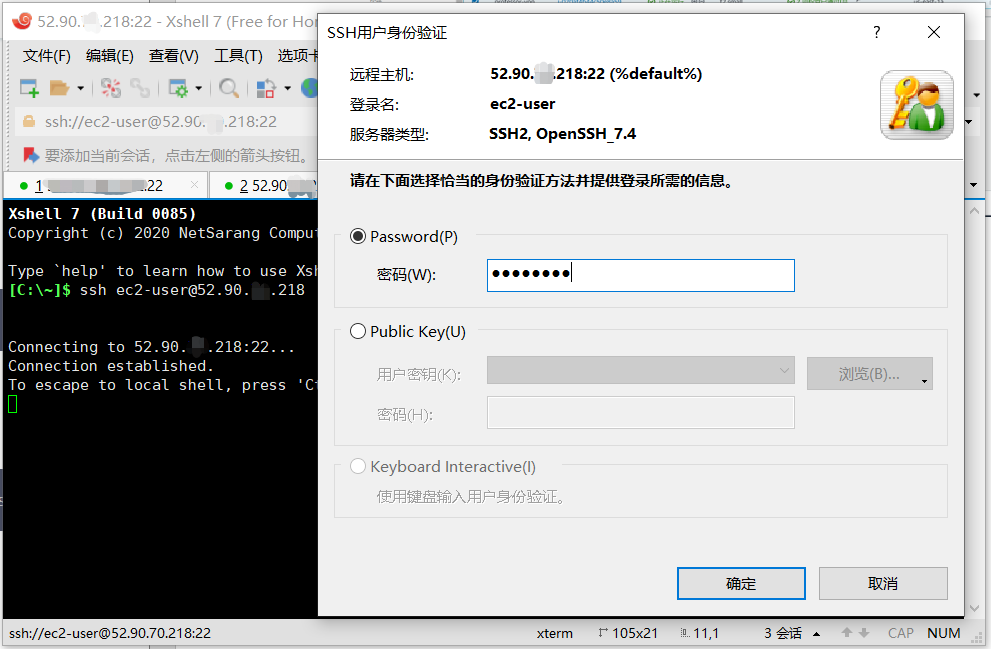
实验步骤

1. 事先创建好基础环境，和一台EC2实例.





1. 配置VPN服务器
2. 使用ssh工具进行连接VPN服务器.



1. 安装所需的软件包:

yum update -y

sudo amazon-linux-extras install epel

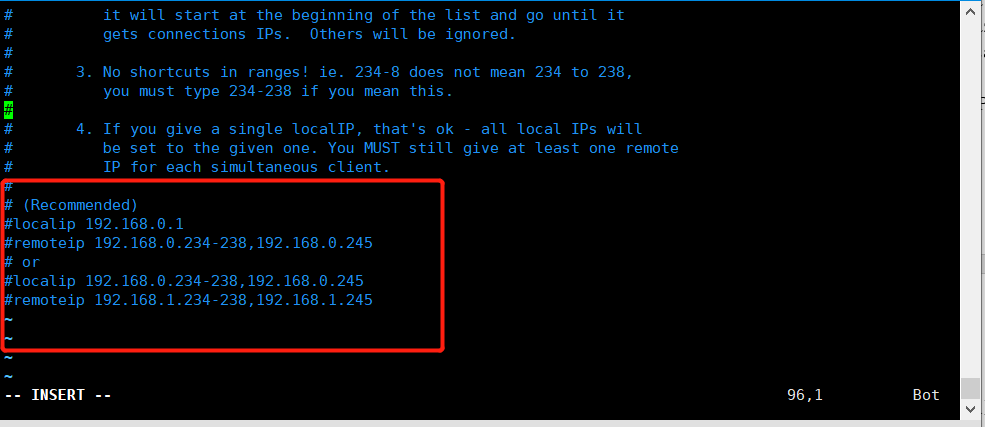
yum install ppp pptpd net-tools iptables-services -y

1. 配置PPTP配置文件

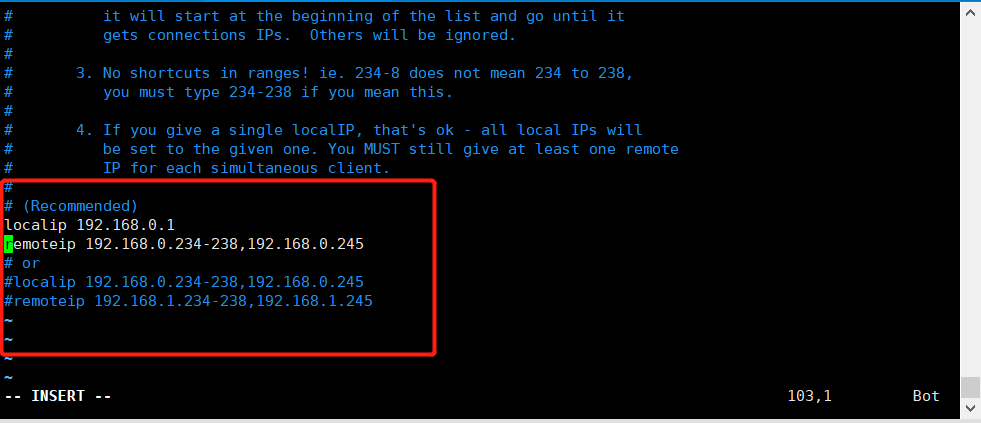
编辑配置文件

vim /etc/pptpd.conf

在文件末尾找到如下几行:



将任意一组localip和remoteip前面的#号去掉,或按自己需要添加:



保存退出文件.

说明:

localip表示服务器VPN虚拟接口将分配的IP地址, 可以使用与VPN服务器内网地址相同网段的IP, 也可以设置为另一网段的IP;

remoteip表示VPN客户端连接成功后将分配的IP地址段, 同样可以使用与VPN服务内网地址相同网段的IP地址段, 也可以使用不同地址段, 只要与localip互不冲突即可

1. 配置PPP配置文件

***PPP有两个文件需要配置, 一个是options.pptpd选项文件, 另一个是chap-secrets账号文件.***

编辑选项文件:

vim /etc/ppp/options.pptpd

确认以下行已启用, 且已使用指定值:

**name pptpd**

**refuse-pap**

**refuse-chap**

**refuse-mschap**

**require-mschap-v2**

**require-mppe-128**

**ms-dns 8.8.8.8**

**ms-dns 8.8.4.4**

**proxyarp**

**lock**

**nobsdcomp**

**novj**

**novjccomp**

**nologfd**

**注: 如果要启用日志记录,则把”nologfd”注释掉,并在它的下面加一行日志路径(自定)**

说明:

在以上配置中, 其中name后面的pptpd是服务名称, 可按自己需要修改. refuse表示拒绝的加密码方式, 而require表示启用的回密方式,

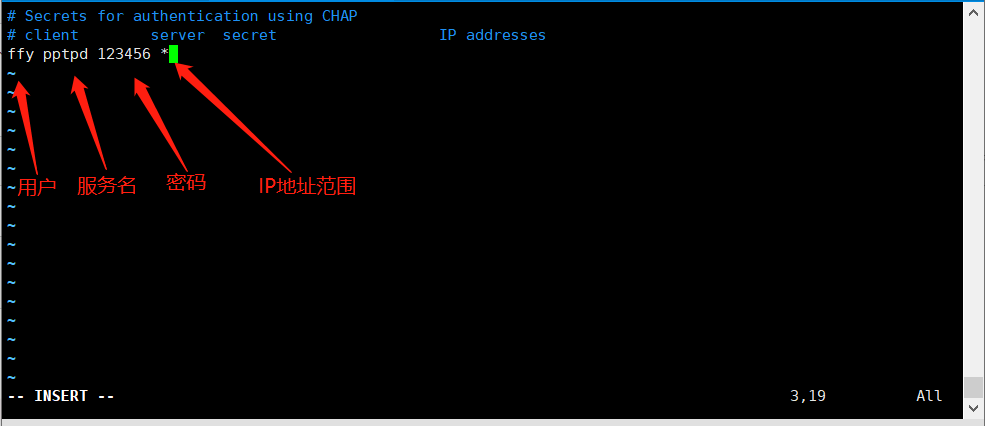
这里使用了mschap-v2、mppe-128两种加密方式. ms-dns是配置VPN的DNS服务器, 这里使用了两个Google的DNS服务器地址.

编辑VPN账号文件:

vim /etc/ppp/chap-secrets

***#这个文件以明文的方式保存了使用VPN用户的用户名、服务名、密码、IP地址范围, 每一行表示一个用户.***

例:



说明:

前面 /etc/ppp/options.pptpd 中name 项设置的什么, 这里的服务名就写什么.

IP addresses设置的” \* ”号, 意思为随机分配 remoteip 范围内的地址.

1. 开启路由转发功能

编辑以下文件

vim /etc/sysctl.conf

添加以下行(如果原先有, 则修改为):

net.ipv4.ip\_forward = 1

执行以下命令, 使配置生效:

sysctl -p

如果执行上面命令出现类型如下错误:

error: "net.bridge.bridge-nf-call-ip6tables" is an unknown key error: "net.bridge.bridge-nf-call-iptables" is an unknown key error: "net.bridge.bridge-nf-call-arptables" is an unknown key

请执行以下命令修复:

rm -f /sbin/modprobe ln -s /bin/true /sbin/modproberm -f /sbin/sysctl ln -s /bin/true /sbin/sysctl

1. 配置iptables防火墙

iptables -A FORWARD -p tcp --syn -s 192.168.0.0/24 -j TCPMSS --set-mss 1356

iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -o eth0 -j SNAT –-to-source 10.80.1.202

192.168.0.0/24 – 请修改为自己前面/etc/pptpd.conf配置中使用的IP

10.80.1.202 – 是服务器的私有地址, 请修改为自己服务器的私有地址

说明:

第一条规则是配置filter表FORWARD链过滤转发的源数据包的地址为192.168.0.0/24,协议为tcp, 修改其TCP最大报文段长度为1356

第二条规则是配置nat表POSTROUTING链过滤要路由出去的数据包, 映射其地址段192.168.0.0/24为10.80.1.202, 从eth0出.

保存规则:

service iptables save

应用规则:  
service iptables restart

iptables添加开机自启动项:

chkconfig iptables on

1. 启动

启动服务:

service pptpd start

pptpd开机自启动:

chkconfig pptpd on

在使用过程中, 如果修改了配置(添加用户无需重启), 请执行以下命令重启服务:

service pptpd restart