秋明分享平台之

ipsec+pptp搭建企业级翻墙vpn

撰稿人：秋明

撰稿人邮箱：tyumen@zhoufengjie.cn

本文撰稿日期： 2015年6月16日星期二

本站口号：开源、分享、共进

注解：任何想通过本平台分享文档的，可以随时联系，文档里面注明出稿人和邮箱，方便文档使用者同撰稿的兄弟技术咨询沟通和交流；

目录

1 前言 3

2 安装 4

2.1 准备工作 4

2.1.1 软件下载解压 4

2.1.2 生成配置 4

3 简介 5

4 IPsec隧道建立 5

4.1 国内服务器A部署 5

4.1.1 安装yum仓库 5

4.1.2 下载安装ipsec-tools 5

4.1.3 配置ipsec 6

4.1.3.1 配置ipsec密钥 6

4.1.3.2 配置ipsec配置文件 6

4.1.3.3 配置ipsec连接 7

4.1.3.4 调整内核参数配置 8

4.1.3.5 调整安全策略 8

4.1.3.6 调整iptables配置 8

4.1.3.7 启动ipsc 8

4.2 国外服务器B部署 9

4.2.1 安装yum仓库 9

4.2.2 下载安装ipsec-tools 9

4.2.3 配置ipsec 9

4.2.3.1 配置ipsec密钥 9

4.2.3.2 配置ipsec配置文件 10

4.2.3.3 配置ipsec连接 11

4.2.3.4 调整内核参数配置 11

4.2.3.5 调整安全策略 12

4.2.3.6 调整iptables配置 12

4.2.3.7 启动ipsc 12

4.3 ipsec验证 12

5 GRE隧道建立 13

5.1 国内服务器 13

5.1.1 配置gre 13

5.2 国外服务器 13

5.2.1 配置gre 13

5.2.2 配置iptables 13

5.3 测试gre 13

6 国内服务器vpn配置 14

6.1 配置路由 14

6.1.1 静态路由配置 14

6.1.2 策略路由配置 15

6.2 搭建pptp vpn 15

6.2.1 pptp安装 15

6.2.2 pptp配置 15

6.2.3 pptp测试 16

# 简介

网上实在是没有好的ipsec搭建材料，没办法自己写一份吧；本项目的部署场景和部署需求为：国内用户，vpn到国内的服务器上面，国内的服务器跟国外的服务器建立隧道，所有的内容通过vpn隧道传输到国外取资源；

服务器假设：

国内服务器A ip为：114.112.96.37

国外服务器B ip为：69.28.56.10

国内服务器A gre ip为：172.16.1.1

国外服务器B gre ip为：172.16.1.2

# IPsec隧道建立

这里使用ipsec-tools进行隧道建立；建立好隧道之后，进行验证，便于第三步的gre隧道建立；

* 1. 国内服务器A部署

国内服务器作为国内的用户接入的一个接口；

* + 1. 安装yum仓库

yum install wget vim -y

wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-6.repo

yum makecache

* + 1. 下载安装ipsec-tools

cd /usr/local/src

wget ftp://ftp.pbone.net/mirror/ftp.pramberger.at/systems/linux/contrib/rhel5/x86\_64/ipsec-tools-libs-0.8.0-1.el5.pp.x86\_64.rpm

wget ftp://ftp.pbone.net/mirror/ftp5.gwdg.de/pub/opensuse/repositories/home:/aevseev/CentOS\_CentOS-6/x86\_64/ipsec-tools-0.8.0-25.3.x86\_64.rpm

yum install openssl098e-0.9.8e-18.el6\_5.2.x86\_64 -y

yum install compat-openldap-2.3.43-2.el6.x86\_64 -y

rpm -ivh ipsec-tools-libs-0.8.0-1.el5.pp.x86\_64.rpm

rpm -ivh ipsec-tools-0.8.0-25.3.x86\_64.rpm

echo “ipsec by fengjie.zhou” > /etc/racoon/motd

* + 1. 配置ipsec

ipsec的目录为：/etc/racoon，配置部署分为vpn密钥配置、ipsec配置文件配置（racoon.conf）、系统内核参数调整、隧道key配置（setkey.conf）等；这里配置部署按照如下的方法来进行即可；

* + - 1. 配置ipsec密钥

echo "123456 0x123456" > /etc/racoon/psk.txt

chmod 700 /etc/racoon/psk.txt

说明：这里配置的123456为密钥串，0x123456为密钥串调用，会在setkey.conf中使用；

* + - 1. 配置ipsec配置文件

编辑ipsec的配置文件：vim /etc/racoon/racoon.conf，输入如下内容：

path include "/etc/racoon";

#include "remote.conf";

path pre\_shared\_key "/etc/racoon/psk.txt";

path certificate "/etc/racoon/cert";

#log debug;

listen

{

isakmp 69.28.56.10 [500];

isakmp\_natt 69.28.56.10 [4500];

}

remote anonymous

{

exchange\_mode main, aggressive, base;

mode\_cfg on;

proposal\_check obey; # obey, strict, or claim

nat\_traversal on;

generate\_policy unique;

ike\_frag on;

passive on;

dpd\_delay 30;

proposal {

lifetime time 28800 sec;

encryption\_algorithm 3des;

hash\_algorithm md5;

authentication\_method xauth\_psk\_server;

dh\_group 2;

}

}

sainfo anonymous

{

encryption\_algorithm 3des, aes, blowfish;

authentication\_algorithm hmac\_sha1, hmac\_md5;

compression\_algorithm deflate;

}

mode\_cfg

{

auth\_source system;

dns4 8.8.8.8, 114.114.114.114;

banner "/etc/racoon/motd";

save\_passwd on;

network4 114.112.96.37;

netmask4 255.255.255.0;

pool\_size 100;

pfs\_group 2;

}

* + - 1. 配置ipsec连接

编辑setkey.conf配置文件，vim /etc/racoon/setkey.conf，输入如下内容：

#flush SAD entries

flush;

#flush SPD entries

spdflush;

#add SA entries

#add SP entries

spdadd 69.28.56.0/24[any] 114.112.96.0/24[any] any -P in ipsec esp/tunnel/69.28.56.10-114.112.96.37/require;

spdadd 114.112.96.0/24[any] 69.28.56.0/24[any] any -P out ipsec esp/tunnel/114.112.96.37-69.28.56.10/require;

# Using ESP tunnel:

add 69.28.56.10 114.112.96.37 esp 0x123456 -m tunnel

-E 3des-cbc 0x5152535455565758595a5b5c5d5e5f606162636465666768

-A hmac-sha1 0x5152535455565758595a5b5c5d5e5f6061626364;

add 114.112.96.37 69.28.56.10 esp 0x123456 -m tunnel

-E 3des-cbc 0x0102030405060708090a0b0c0d0e0f101112131415161718

-A hmac-sha1 0x0102030405060708090a0b0c0d0e0f1011121314;

* + - 1. 调整内核参数配置

sed -i 's/^\(net.ipv4.ip\_forward =\).\*/\1 1/' /etc/sysctl.conf

sed -i 's/^\(net.ipv4.conf.default.rp\_filter =\).\*/\1 0/' /etc/sysctl.conf

sysctl -a | egrep "ipv4.\*(accept|send)\_redirects" | awk -F "=" '{print $1"= 0"}' >> /etc/sysctl.conf

sysctl -p

* + - 1. 调整安全策略

setenforce 0

sed -i 's/^SELINUX=.\*/SELINUX=disabled/g' /etc/selinux/config

最好重启设备： reboot

* + - 1. 调整iptables配置

如果设备起了iptables，需要增加如下操作：

iptables -I INPUT -p udp --dport 500 -j ACCEPT

iptables -I INPUT -p udp --dport 4500 -j ACCEPT

* + - 1. 启动ipsc

setkey -f /etc/racoon/setkey.conf

racoon -f /etc/racoon/racoon.conf -l /var/log/racoon.log -d

* 1. 国外服务器B部署

国外服务器作为所有数据包出去的一个窗口；

* + 1. 安装yum仓库

yum install wget vim -y

wget -O /etc/yum.repos.d/CentOS-Base.repo http://mirrors.aliyun.com/repo/Centos-6.repo

yum makecache

* + 1. 下载安装ipsec-tools

cd /usr/local/src

wget ftp://ftp.pbone.net/mirror/ftp.pramberger.at/systems/linux/contrib/rhel5/x86\_64/ipsec-tools-libs-0.8.0-1.el5.pp.x86\_64.rpm

wget ftp://ftp.pbone.net/mirror/ftp5.gwdg.de/pub/opensuse/repositories/home:/aevseev/CentOS\_CentOS-6/x86\_64/ipsec-tools-0.8.0-25.3.x86\_64.rpm

yum install openssl098e-0.9.8e-18.el6\_5.2.x86\_64 -y

yum install compat-openldap-2.3.43-2.el6.x86\_64 -y

rpm -ivh ipsec-tools-libs-0.8.0-1.el5.pp.x86\_64.rpm

rpm -ivh ipsec-tools-0.8.0-25.3.x86\_64.rpm

echo “ipsec by fengjie.zhou” > /etc/racoon/motd

* + 1. 配置ipsec

ipsec的目录为：/etc/racoon，配置部署分为vpn密钥配置、ipsec配置文件配置（racoon.conf）、系统内核参数调整、隧道key配置（setkey.conf）等；这里配置部署按照如下的方法来进行即可；

* + - 1. 配置ipsec密钥

echo "123456 0x123456" > /etc/racoon/psk.txt

chmod 700 /etc/racoon/psk.txt

说明：这里配置的123456为密钥串，0x123456为密钥串调用，会在setkey.conf中使用；

* + - 1. 配置ipsec配置文件

编辑ipsec的配置文件：vim /etc/racoon/racoon.conf，输入如下内容：

path include "/etc/racoon";

#include "remote.conf";

path pre\_shared\_key "/etc/racoon/psk.txt";

path certificate "/etc/racoon/cert";

#log debug;

listen

{

isakmp 114.112.96.37 [500];

isakmp\_natt 114.112.96.37 [4500];

}

remote anonymous

{

exchange\_mode main, aggressive, base;

mode\_cfg on;

proposal\_check obey; # obey, strict, or claim

nat\_traversal on;

generate\_policy unique;

ike\_frag on;

passive on;

dpd\_delay 30;

proposal {

lifetime time 28800 sec;

encryption\_algorithm 3des;

hash\_algorithm md5;

authentication\_method xauth\_psk\_server;

dh\_group 2;

}

}

sainfo anonymous

{

encryption\_algorithm 3des, aes, blowfish;

authentication\_algorithm hmac\_sha1, hmac\_md5;

compression\_algorithm deflate;

}

mode\_cfg

{

auth\_source system;

dns4 8.8.8.8, 114.114.114.114;

banner "/etc/racoon/motd";

save\_passwd on;

network4 69.28.56.10;

netmask4 255.255.255.0;

pool\_size 100;

pfs\_group 2;

}

* + - 1. 配置ipsec连接

编辑setkey.conf配置文件，vim /etc/racoon/setkey.conf，输入如下内容：

#flush SAD entries

flush;

#flush SPD entries

spdflush;

#add SA entries

#add SP entries

spdadd 114.112.96.0/24[any] 69.28.56.0/24[any] any -P in ipsec esp/tunnel/114.112.96.37-69.28.56.10/require;

spdadd 69.28.56.0/24[any] 114.112.96.0/24[any] any -P out ipsec esp/tunnel/69.28.56.10-114.112.96.37/require;

# Using ESP tunnel:

add 69.28.56.10 114.112.96.37 esp 0x123456 -m tunnel

-E 3des-cbc 0x5152535455565758595a5b5c5d5e5f606162636465666768

-A hmac-sha1 0x5152535455565758595a5b5c5d5e5f6061626364;

add 114.112.96.37 69.28.56.10 esp 0x123456 -m tunnel

-E 3des-cbc 0x0102030405060708090a0b0c0d0e0f101112131415161718

-A hmac-sha1 0x0102030405060708090a0b0c0d0e0f1011121314;

* + - 1. 调整内核参数配置

sed -i 's/^\(net.ipv4.ip\_forward =\).\*/\1 1/' /etc/sysctl.conf

sed -i 's/^\(net.ipv4.conf.default.rp\_filter =\).\*/\1 0/' /etc/sysctl.conf

sysctl -a | egrep "ipv4.\*(accept|send)\_redirects" | awk -F "=" '{print $1"= 0"}' >> /etc/sysctl.conf

sysctl -p

* + - 1. 调整安全策略

setenforce 0

sed -i 's/^SELINUX=.\*/SELINUX=disabled/g' /etc/selinux/config

最好重启设备： reboot

* + - 1. 调整iptables配置

如果设备起了iptables，需要增加如下操作：

iptables -I INPUT -p udp --dport 500 -j ACCEPT

iptables -I INPUT -p udp --dport 4500 -j ACCEPT

iptables -t nat -A POSTROUTING -s 114.112.96.0/24 -o eth2 -j MASQUERADE

iptables -A FORWARD -s 114.112.96.0/24 -j ACCEPT

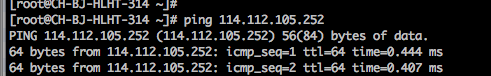
* + - 1. 启动ipsc

setkey -f /etc/racoon/setkey.conf

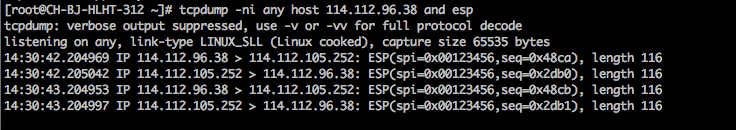
racoon -f /etc/racoon/racoon.conf -l /var/log/racoon.log -d

* 1. ipsec验证

在国内服务器发起ping到国外的服务器，在国外的服务器上面抓包：



国外服务器上面抓到的报文为esp封装的；



# GRE隧道建立

在ipsec隧道的基础之上建立gre隧道，gre over ipsec;

* 1. 国内服务器
     1. 配置gre

modprobe ip\_gre

ip tunnel add tunnel0 mode gre remote 69.28.56.10 local 114.112.96.37 ttl 255

ip link set tunnel0 up mtu 1400

ip addr add 172.16.1.1/30 dev tunnel0

ip addr add 172.16.1.1/30 peer 172.16.1.2/30 dev tunnel0

* 1. 国外服务器
     1. 配置gre

modprobe ip\_gre

ip tunnel add tunnel0 mode gre remote 114.112.96.37 local 69.28.56.10 ttl 255

ip link set tunnel0 up mtu 1400

ip addr add 172.16.1.2/30 dev tunnel0

ip addr add 172.16.1.2/30 peer 172.16.1.1/30 dev tunnel0

* + 1. 配置iptables

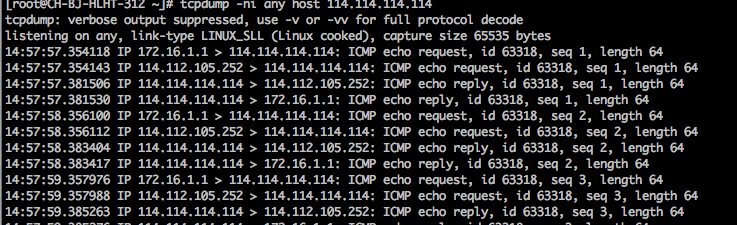
iptables -t nat -A POSTROUTING -s 172.16.1.0/24 -j SNAT --to 69.28.56.10

* 1. 测试gre

在国内服务器上面指路由

route add -host 114.114.114.114 dev tunnel0

在国内服务器上面ping 114.114.114.114，然后在国外服务器上面抓包：



# 国内服务器vpn配置

目前需要实现的是，国内网民vpn到国内的服务器上面，国内的服务器所有的报文都从gre隧道走向到国外，然后nat之后进行服务；

这样需要做的操作是：默认路由需要走隧道，网民的方向仍然从公网回去；所以要保证隧道的路由走公网，网民走公网，其它的走默认路由；

* 1. 配置路由

这里分两个路由，第一：管理地址和隧道对端要走静态路由走公网；第二：网民请求要配置策略路由，从哪入从哪出；

* + 1. 静态路由配置

隧道对端的ip地址要走公网网关

route add -host 69.28.56.10 gw 114.112.96.1

管理地址走公网网关

route add -host 111.198.33.132 gw 114.112.96.1

route add -host 111.198.33.131 gw 114.112.96.1

route add -host 118.144.77.226 gw 114.112.96.1

然后把配置写入配置文件：vi /etc/sysconfig/static-routes写入如下内容：

any host 69.28.56.10 gw 114.112.96.1

any host 111.198.33.132 gw 114.112.96.1

any host 111.198.33.131 gw 114.112.96.1

any host 118.144.77.226 gw 114.112.96.1

然后配置所有路由走隧道：

route add default dev tunnel0

* + 1. 策略路由配置

编辑配置文件：vi /etc/iproute2/rt\_tables,写入如下内容：

10 NetEth0

然后执行如下命令：

ip route flush table NetEth0

ip rule add from 114.112.96.37/24 dev eth0 table NetEth0

ip route add default via 114.112.96.1 dev eth0 src 114.112.96.37 table NetEth0

然后将如上命令写入：vi /etc/rc.d/init.d/network的最有一条exit之前；



* 1. 搭建pptp vpn
     1. pptp安装

cd /usr/local/src

wget http://lamp.teddysun.com/files/pptpd-1.3.4-2.el6.x86\_64.rpm

yum -y install net-tools make libpcap iptables gcc-c++ logrotate tar cpio perl pam tcp\_wrappers dkms ppp

rpm -ivh pptpd-1.3.4-2.el6.x86\_64.rpm

* + 1. pptp配置

rm -f /dev/ppp

mknod /dev/ppp c 108 0

echo 1 > /proc/sys/net/ipv4/ip\_forward

echo "mknod /dev/ppp c 108 0" >> /etc/rc.local

echo "pptpvpn pptpd pptppasswd \*" >> /etc/ppp/chap-secrets

echo "echo 1 > /proc/sys/net/ipv4/ip\_forward" >> /etc/rc.local

echo "localip 192.168.8.1" >> /etc/pptpd.conf

echo "remoteip 192.168.8.2-254" >> /etc/pptpd.conf

echo "ms-dns 8.8.8.8" >> /etc/ppp/options.pptpd

echo "ms-dns 8.8.4.4" >> /etc/ppp/options.pptpd

chkconfig --add pptpd

chkconfig pptpd on

service pptpd start

iptables -t nat -A POSTROUTING -s 192.168.8.0/24 -j SNAT --to-source 172.16.1.1

iptables -A FORWARD -p tcp --syn -s 192.168.8.0/24 -j TCPMSS --set-mss 1356

* + 1. pptp测试

用户名：pptpvpn，密码：pptppasswd