

目 录

DNS

关于版块

安装部署

NextCloud

关于版块

安装部署

Firewall GateWay

关于版本

安装部署

Ipsec

关于版块

安装部署

DNS

关于版块

关于DNS

公司购买了到香港的国际加速专线，即可以访问国外的网站。由于不想使用服务商提供的DNS，但用8.8.8.8的DNS即会访问aliyun等一些国内的网站也跳转到国外节点去。这时就需要自建递归DNS。

本版块维护人员

版主：子木

QQ：1242119478

交流Q群：526749756

安装部署

安装

1、安装unbound `yum install unbound -y`

2、首先生成dnsmasq-china-list加速国内域名解析，到github下载这个仓库：

`git clone https://github.com/felixonmars/dnsmasq-china-list.git`

3、进入到git clone的仓库，修改 Makefile 文件里面的第一行 `SERVER=119.29.29.29`，改为你觉得最合适的国内缓存 DNS 服务器，当然用Makefile里默认的114.114.114.114也可以

4、执行make unbound，会在此目录下生成一份accelerated-domains.china.unbound.conf文件，cp这个文件到/etc/unbound目录下

```
cp dnsmasq-china-list/accelerated-domains.china.unbound.conf
/etc/unbound/
```

5、下载named.cache到/etc/unbound目录下，下载地址如

下：<ftp://ftp.internic.net/domain/named.cache>

6、修改配置文件/etc/unbound/unbound.conf，如下：

```
num-threads: 2 # 线程数可以修改为物理核心数
interface: 0.0.0.0 # 侦听所有 IPv4 地址
interface: ::0 # 侦听所有 IPv6 地址
so-reuseport: yes # 如果开了多线程，就写 yes
msg-cache-size: 64m # 本机可以设置 4m 或者更小
rrset-cache-size: 128m # 本机可以设置 4m 或者更小
cache-max-ttl: 3600 # 建议设置一个不太大的值... 专治各种运营商 DNS 缓存不服
outgoing-num-tcp: 256 # 限制每个线程向上级查询的 TCP 并发数
incoming-num-tcp: 1024 # 限制每个线程接受查询的 TCP 并发数
# 下面这四个不需要解释了吧，不想用那个就写 no
do-ip4: yes
do-ip6: yes
do-udp: yes
do-tcp: yes
val-permissive-mode: yes # 启用此功能将禁用所有DNSSEC安全
tcp-upstream: no # 默认是 no，隧道状态比较稳的话也不需要写 yes。一些情况下强制使用 tcp 连上游的话写 yes
access-control: 0.0.0.0/0 allow # 本机用的话建议设置 127.0.0.0/8 allow，局域网用适当调整
root-hints: "/etc/unbound/named.cache" # 没有的话在
hide-identity: yes # 不返回对 id.server 和 hostname.bind 的查询。
hide-version: yes # 不返回对 version.server 和 version.bind 的查询。
harden-glue: yes # 建议打开
module-config: "ipsecmod validator iterator" # 禁用 DNSSEC 检查，如果上游不支持 DNSSEC 就关掉。注意这个选项有可能在其他 include 的文件里
unwanted-reply-threshold: 10000000 # 针对各种网络不服，数值为建议值，具体可以自己修改看看效果
prefetch: yes # 蛮好用的，开着吧
minimal-responses: yes # 省带宽，开着吧。本机用可以关掉
```

```
include: "/etc/unbound/foreigndns.conf"           #国外的域名走这个加速
forward-zone:
  name: "."
  forward-addr: 119.29.29.29
#没有指定的默认走这个
```

添加本地解析:

```
[root@dns local.d]# cp -p block-example.com.conf kubernetes.conf
[root@dns local.d]# vim kubernetes.conf

# entries in this file override toe global DNS
#
# Example blocking email going out to example.com
#
#      local-data: "example.com. 3600 IN MX 5 127.0.0.1"
#      local-data: "example.com. 3600 IN A 127.0.0.1"
#正向解析
local-data: "kubemaster01. IN A 192.168.19.44"
local-data: "kubework01. IN A 192.168.19.45"
local-data: "kubework02. IN A 192.168.19.46"
local-data: "kubework03. IN A 192.168.19.47"

#反向解析
local-data-ptr: "192.168.19.44 kubemaster01"
local-data-ptr: "192.168.19.45 kubework01"
local-data-ptr: "192.168.19.46 kubework02"
local-data-ptr: "192.168.19.47 kubework03"
```

7、为你的服务器和客户端生成一个self-signed的证书和private key，生成的文件位于/etc/unbound文件夹，执行命令：

```
unbound-control-setup
```

8、检查一下配置文件有没有报错：`unbound-checkconf`

9、没有报错的重启一下unbound服务：`systemctl restart unbound.service`

附：[国外域名列表](#)

NextCloud

关于版块

关于NextCloud

目前比较好用开源的网盘有nextcloud和seafile，nexcloud是外国人开发的，seafile即是国人开发的！各有优缺点！这里使用nextcloud的原因是nextcloud社区版几乎能免费使用所有功能，除了服务支持！这里就有企业比较常用到的ldap认证功能。nextcloud还可以安排很多第三方应用，这个你们搭建后可以一一体会！

本版块维护人员

版主：子木

QQ：1242119478

交流Q群：526749756

安装部署

基本环境:

centos 7.7

mariadb 5.5

nginx 1.61

php 7.2

redis 3.2

安装步骤:

一、安装依赖包:

```
yum install -y epel-release yum-utils unzip curl wget \
bash-completion policycoreutils-python mlocate bzip2
```

二、更新系统:

```
yum update -y
```

三、安装nginx

```
yum install -y nginx
systemctl enable nginx
systemctl start nginx

# 创建证书目录
mkdir -p /etc/nginx/cert
openssl req -new -x509 -days 365 -nodes -out /etc/nginx/cert/pan.51itop.
cn.crt -keyout /etc/nginx/cert/pan.51itop.cn.key
# 修改权限
chmod 700 /etc/nginx/cert
chmod 600 /etc/nginx/cert/*
```

四、安装php并配置php

```
yum -y install http://rpms.remirepo.net/enterprise/remi-release-7.rpm
yum-config-manager --enable remi-php72
yum -y install php php-common php-opcache php-mcrypt php-cli php-gd php-
curl php-mysql php-mbstring \
php-intl php-pecl-apcu php-mysqlnd php-pecl-redis php-imagick php-fpm p
hp-zip php-xml php-process \
php-pear php-pdo php-json php-devel php-xmlrpc php-soap php-ldap php-mem
cached
```



```

vim /etc/php-fpm.d/www.conf
# 将用户和组都改为nginx
user = nginx
group = nginx

# 注意: php-fpm所监听的端口为9000
listen = 127.0.0.1:9000

# 去掉下面几行注释
env[HOSTNAME] = $HOSTNAME
env[PATH] = /usr/local/bin:/usr/bin:/bin
env[TMP] = /tmp
env[TMPDIR] = /tmp
env[TEMP] = /tmp

vim /etc/php.ini
# 每个脚本可以消耗的时间, 单位也是秒
max_input_time = 60

#在/var/lib目录下为session路径创建一个新的文件夹, 并将用户名和组设为nginx
mkdir -p /var/lib/php/session
chown pi:pi -R /var/lib/php/session/

```

五、安装数据库并配置数据库

```

yum install -y mariadb mariadb-server
systemctl enable mariadb.service
systemctl start mariadb.service

mysql -uroot -p                                #mariadb第一次登录不需要密码就可以进入
update mysql.user set password=password("123123")where user='root'; #更新root密码
create database nextcloud;
create user 'nextcloud'@'localhost' identified by '123123';
grant all privileges on nextcloud.* to 'nextcloud'@'localhost';
flush privileges;

```

六、下载并解压安装包到指定目录

```

wget https://download.nextcloud.com/server/releases/nextcloud-17.0.1.zip
unzip nextcloud-17.0.1.zip
cp -R nextcloud/ /var/www/                    #因为用的是apache的, 拷贝默认网页目录
mkdir /var/www/nextcloud/data
chown -R nginx:nginx /var/www/nextcloud/

```

七、创建nextcloud的nginx配置文件

```
[root@test12 config]# cat /etc/nginx/conf.d/nextcloud.conf
upstream php-handler {
    server 127.0.0.1:9000;
    #server unix:/var/run/php/php7.2-fpm.sock;
}

server {
    listen 80;
    listen [::]:80;
    server_name pan.51itop.cn;
    # enforce https
    return 301 https://$server_name:443$request_uri;
}

server {
    listen 443 ssl http2;
    listen [::]:443 ssl http2;
    server_name pan.51itop.cn;

    # Use Mozilla's guidelines for SSL/TLS settings
    # https://mozilla.github.io/server-side-tls/ssl-config-generator/
    # NOTE: some settings below might be redundant
    ssl_certificate /etc/nginx/cert/pan.51itop.cn.crt;
    ssl_certificate_key /etc/nginx/cert/pan.51itop.cn.key;

    # Add headers to serve security related headers
    # Before enabling Strict-Transport-Security headers please read into
    this
    # topic first.
    add_header Strict-Transport-Security "max-age=15552000; includeSubDo
mains; preload;" always;
    #
    # WARNING: Only add the preload option once you read about
    # the consequences in https://hstspreload.org/. This option
    # will add the domain to a hardcoded list that is shipped
    # in all major browsers and getting removed from this list
    # could take several months.
    add_header Referrer-Policy "no-referrer" always;
    add_header X-Content-Type-Options "nosniff" always;
    add_header X-Download-Options "noopen" always;
    add_header X-Frame-Options "SAMEORIGIN" always;
    add_header X-Permitted-Cross-Domain-Policies "none" always;
    add_header X-Robots-Tag "none" always;
    add_header X-XSS-Protection "1; mode=block" always;

    # Remove X-Powered-By, which is an information leak
```

```

fastcgi_hide_header X-Powered-By;

# Path to the root of your installation
root /var/www/nextcloud/;

location = /robots.txt {
    allow all;
    log_not_found off;
    access_log off;
}

# The following 2 rules are only needed for the user_webfinger app.
# Uncomment it if you're planning to use this app.
#rewrite ^/.well-known/host-meta /public.php?service=host-meta last;
#rewrite ^/.well-known/host-meta.json /public.php?service=host-meta-
json last;

# The following rule is only needed for the Social app.
# Uncomment it if you're planning to use this app.
#rewrite ^/.well-known/webfinger /public.php?service=webfinger last;

location = /.well-known/carddav {
    return 301 $scheme://$host:$server_port/remote.php/dav;
}
location = /.well-known/caldav {
    return 301 $scheme://$host:$server_port/remote.php/dav;
}

# set max upload size
client_max_body_size 512M;
fastcgi_buffers 64 4K;

# Enable gzip but do not remove ETag headers
gzip on;
gzip_vary on;
gzip_comp_level 4;
gzip_min_length 256;
gzip_proxied expired no-cache no-store private no_last_modified no_e
tag auth;
gzip_types application/atom+xml application/javascript application/j
son application/ld+json application/manifest+json application/rss+xml ap
plication/vnd.geo+json application/vnd.ms-fontobject application/x-font-
ttf application/x-web-app-manifest+json application/xhtml+xml applicatio
n/xml font/opentype image/bmp image/svg+xml image/x-icon text/cache-mani
fest text/css text/plain text/vcard text/vnd.rim.location.xloc text/vtt
text/x-component text/x-cross-domain-policy;

# Uncomment if your server is build with the ngx_pagespeed module

```

```

# This module is currently not supported.
#pagespeed off;

location / {
    rewrite ^ /index.php$request_uri;
}

location ~ ^\/(?:build|tests|config|lib|3rdparty|templates|data)\/ {
    deny all;
}
location ~ ^\/(?:\.|autotest|occ|issue|indie|db_|console) {
    deny all;
}

location ~ ^\/(?:index|remote|public|cron|core\/ajax\/update|status|ocs\/v[12]|updater\/.+|oc[ms]-provider\/.+)\.php(?:$|\/) {
    fastcgi_split_path_info ^(.+?\.php)(\/.*|)$;
    include fastcgi_params;
    fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name
;
    fastcgi_param PATH_INFO $fastcgi_path_info;
    fastcgi_param HTTPS on;
    # Avoid sending the security headers twice
    fastcgi_param modHeadersAvailable true;
    # Enable pretty urls
    fastcgi_param front_controller_active true;
    fastcgi_pass php-handler;
    fastcgi_intercept_errors on;
    fastcgi_request_buffering off;
}

location ~ ^\/(?:updater|oc[ms]-provider)(?:$|\/) {
    try_files $uri/ =404;
    index index.php;
}

# Adding the cache control header for js, css and map files
# Make sure it is BELOW the PHP block
location ~ \.(?:css|js|woff2?|svg|gif|map)$ {
    try_files $uri /index.php$request_uri;
    add_header Cache-Control "public, max-age=15778463";
    # Add headers to serve security related headers (It is intended
to
    # have those duplicated to the ones above)
    # Before enabling Strict-Transport-Security headers please read
into
    # this topic first.
    #add_header Strict-Transport-Security "max-age=15768000; include

```

```

SubDomains; preload;" always;
#
# WARNING: Only add the preload option once you read about
# the consequences in https://hstspreload.org/. This option
# will add the domain to a hardcoded list that is shipped
# in all major browsers and getting removed from this list
# could take several months.
add_header Referrer-Policy "no-referrer" always;
add_header X-Content-Type-Options "nosniff" always;
add_header X-Download-Options "noopen" always;
add_header X-Frame-Options "SAMEORIGIN" always;
add_header X-Permitted-Cross-Domain-Policies "none" always;
add_header X-Robots-Tag "none" always;
add_header X-XSS-Protection "1; mode=block" always;

# Optional: Don't log access to assets
access_log off;
}

location ~ \.(?:png|html|ttf|ico|jpg|jpeg|bcmap)$ {
    try_files $uri /index.php$request_uri;
    # Optional: Don't log access to other assets
    access_log off;
}
}

```

```

[root@test12 ~]# nginx -t
[root@test12 ~]# nginx -s reload

```

八、web登录一下，我设置的域名为<https://pan.51itop.cn>，填写前面步骤五创建的数据库名、用户及密码！完成安装！

九、根据下图提示，优化一下：

```

[root@test12 config]#yum install -y redis
[root@test12 config]#systemctl enable redis.service
[root@test12 config]#systemctl start redis.service
[root@test12 config]# vim config.php
'memcache.distributed' => '\OC\Memcache\Redis',
'memcache.locking' => '\OC\Memcache\Redis',
'memcache.local' => '\OC\Memcache\APCu',
'redis' => array(
    'host' => 'localhost',
    'port' => 6379,
),

[root@test12 config]# vim /etc/php.ini

```

```
memory_limit = 4096M
```

```
[root@test12 config]# vim /etc/php.d/10-opcache.ini
opcache.enable=1
opcache.interned_strings_buffer=8
opcache.max_accelerated_files=10000
opcache.memory_consumption=128
opcache.save_comments=1
opcache.revalidate_freq=1
```

#提示：所使用的数据库为MySQL但没有对4字节字符的支持。为正确处理文件名或评论中使用的4字节字符（比如emoji表情），建议开启MySQL的4字节字符支持。详细信息请阅读相关文档页面
#请参考以下链接(https://docs.nextcloud.com/server/17/admin_manual/configuration_database/mysql_4byte_support.html "参考页面")
#注意，参考链接上涉及的occ的要写occ文件夹的绝对路径

```
[root@test12 config]# systemctl restart php-fpm
```

十、安装smbclient扩展模块

```
yum -y install libsmbclient libsmbclient-devel php-smbclient
pecl install smbclient
```

十一、安装collabora online

```
#安装docker
yum install -y yum-utils
yum-config-manager \
    --add-repo \
    https://download.docker.com/linux/centos/docker-ce.repo
yum makecache fast
yum -y install docker-ce
systemctl start docker
#拉取镜像
docker pull collabora/code
#运行镜像
#注意：domain为你的nextcloud服务器地址，此处为授权的意思，并注意域名部分中的“.”要加转义字符“\”，多个域名之间用“|”隔开
docker run -t -d -p 9980:9980 -e 'domain=owncloud\|.domain\|.com\' --restart always --cap-add MKNOD collabora/code
```

十二、nginx反向代理collabora online

```
server {
    listen      443 ssl;
    server_name office.example.com;
```

```

ssl_certificate /path/to/certificate;
ssl_certificate_key /path/to/key;

# static files
location ^~ /loleaflet {
    proxy_pass https://localhost:9980;
    proxy_set_header Host $http_host;
}

# WOPI discovery URL
location ^~ /hosting/discovery {
    proxy_pass https://localhost:9980;
    proxy_set_header Host $http_host;
}

# main websocket
location ~ ^/lool/(.*)/ws$ {
    proxy_pass https://localhost:9980;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "Upgrade";
    proxy_set_header Host $http_host;
    proxy_read_timeout 36000s;
}

# download, presentation and image upload
location ~ ^/lool {
    proxy_pass https://localhost:9980;
    proxy_set_header Host $http_host;
}

# Admin Console websocket
location ^~ /lool/adminws {
    proxy_pass https://localhost:9980;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection "Upgrade";
    proxy_set_header Host $http_host;
    proxy_read_timeout 36000s;
}
}

```

十三、在nextcloud应用中下载并启用collabora online



十四、在nextcloud应用中启用并配置Idap认证，默认已经下载。

Firewall GateWay

关于版本

关于**firewall gateway**

由于公司需要更改一下外网出口拓扑，原来是一个网康的NI3200-60即当上网行为管理又当网关的。但后面增加了一条出口带宽，需要把网康更改为双桥模式，更好的对流量进行监控，这时就缺少了网关设备了！购买一台适合几百人办公的防火墙设备当网关又要增加额外的费用，刚好公司就很多空闲的服务器，就想到了安装一台centos的系统，用**firewall**做**nat**转发。

注：一般路由器的**nat**转发能力真的不行，防火墙的**nat**性能还可以，但是好点的防火墙价格也挺高的。

本版块维护人员

版主：子木

QQ：1242119478

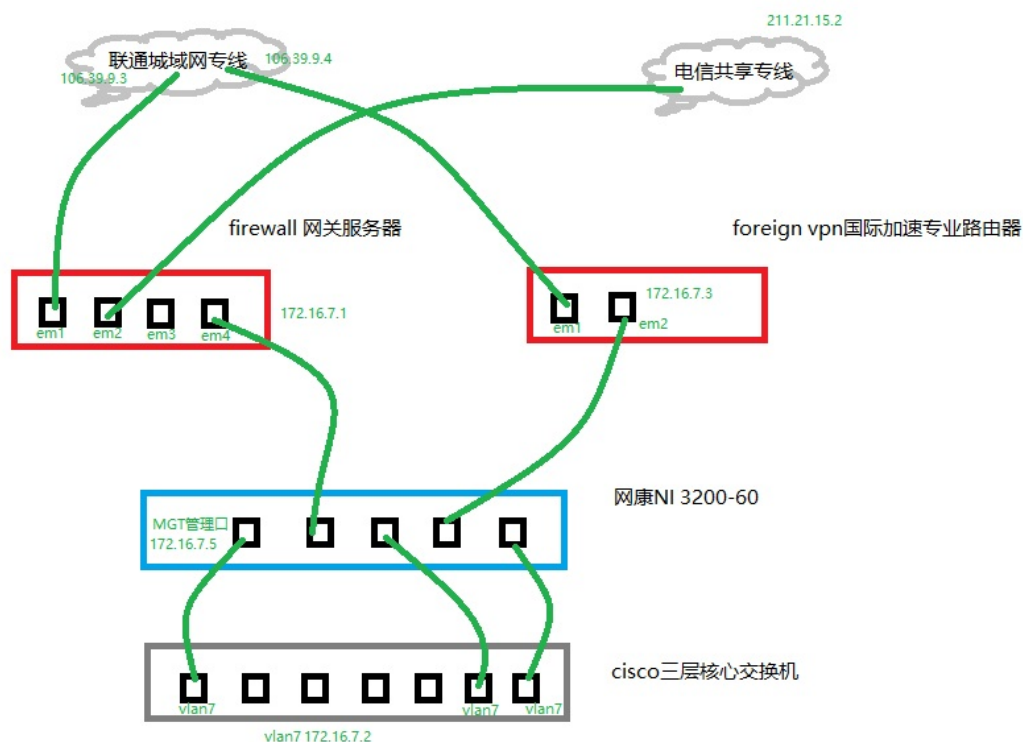
交流Q群：526749756

安装部署

基本环境:

centos 7.7

网络拓扑图:



三层交换机上的配置:

由于拓扑图可以，我会把指定的一些内网网段分流到开通国际加速专线的路由器上，使这部份内网网段可以访问国外网站，这里需要在三层交换机上做，配置如下：

```
#默认的路由是指向linux服务器网关的
HX-3560X(config)#ip route 0.0.0.0 0.0.0.0 172.16.7.1

#在三层交换机上做策略路由，指定内网网段走foreign vpn国际加速专线路由器
HX-3560X(config)#sdm prefer routing #cisco交换机升级到ip servers许可后还需要执行这个命令保存重启才可以
HX-3560X#copy running-config startup-config
HX-3560X#reload

#创建acl规则，把这三个网段的内网网段访问其它的网段的拦截在三层交换机内交换，即内网网段互访时不能路由器上
HX-3560X(config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
HX-3560X(config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 172.16.
```

```

0.0 0.0.255.255
#指定内网网段
HX-3560X(config)#access-list 101 permit ip 192.168.2.0 0.0.0.255 any
HX-3560X(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 any
HX-3560X(config)#access-list 101 permit ip 192.168.4.0 0.0.0.255 any

#起个名字，这里的10是策略路由序号
rote-map foreign permit 10

#匹配一个访问列表，这里的101是访问列表号
match ip address 101

#设置一个策略，定义下一跳172.16.7.3，该地址foreign vpn国际加速专线路由器
set ip next-hop 172.16.7.3
exit
int vlan 2
接口调用
ip policy route-map foreign
exit
int vlan 3
接口调用
ip policy route-map foreign
exit
int vlan 4
接口调用
ip policy route-map foreign

```

网康上的配置：

给MGT管理口配置：还是设置为172.16.7.5 255.255.255.248

配置默认路由让网康设备能上外网：下一跳地址为网关，接口为管理口 设置dns

配置双桥网口

三层交换机上就设置为access模式，vlan7

勾选双入双出。

双桥地址为虚拟地址，可以随便设置：172.16.0.11/12 255.255.255.0 网关172.16.0.1

网关服务器的配置：

1、设置ip修改网卡防火墙zone

```

#按照下面来设置ip，个人习惯在/etc/sysconfig/network-scripts/ifcfg-em4这样的脚本下设置
em1: 106.39.95.3 mask 255.255.255.248 gw 106.39.95.1 main表生成一条默认路由
em2: 211.21.15.2 mask 255.255.255.248 网关不设
em4: 172.16.7.1 mask 255.255.255.248 网关不设

```

```
firewall-cmd --permanent --zone=external --change-interface=em1
firewall-cmd --permanent --zone=external --change-interface=em2
firewall-cmd --permanent --zone=trusted --change-interface=em4
```

2、开启路由转发功能

```
echo "1" >/proc/sys/net/ipv4/ip_forward
```

3、配置内网静态路由

```
ip route add 192.168.0.0/16 via 172.16.7.2 dev em4
#添加到永久路由:
vim /etc/sysconfig/network-scripts/route-em4
192.168.0.0/16 via 172.16.7.2 dev em4
```

4、添加路由表

```
#因为一台服务器上默认网关只能设置一个，多条线路的其它网关设置到路由表上
echo "11 telecom" >>/etc/iproute2/rt_tables
ip route add default via 211.21.15.2 dev em2 table telecom
```

5、配置策略路由，分流一部分内网流量到电信出口线路上

```
/sbin/ip rule add from 192.168.5.0/24 table telecom pref 99
/sbin/ip rule add from 192.168.6.0/24 table telecom pref 100
/sbin/ip rule add from 192.168.7.0/24 table telecom pref 101
/sbin/ip rule add from 192.168.8.0/24 table telecom pref 102
/sbin/ip rule add from 192.168.9.0/24 table telecom pref 103

#策略路由重启失效，需要添加到上面命令到rc.local开机自动执行，centos7的rc.local需要添加执行权限
chmod +x /etc/rc.d/rc.local
```

6、防火墙配置

```
systemctl enable firewalld
systemctl start firewalld
```

7、删除外网ssh连接服务

```
firewall-cmd --permanent --zone=external --remove-service=ssh
```

8、开启nat转发

#external默认已开启masquerade伪装了，只需要再添加NAT规则就可以了

```

firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em1 -j MASQUERADE -s 192.168.10.0/24
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em1 -j MASQUERADE -s 192.168.11.0/24
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em1 -j MASQUERADE -s 192.168.12.0/24
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em1 -j MASQUERADE -s 192.168.13.0/24
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em1 -j MASQUERADE -s 192.168.14.0/24
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em1 -j MASQUERADE -s 192.168.15.0/24
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em2 -j MASQUERADE -s 192.168.5.0/24
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em2 -j MASQUERADE -s 192.168.6.0/24
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em2 -j MASQUERADE -s 192.168.7.0/24
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em2 -j MASQUERADE -s 192.168.8.0/24
firewall-cmd --permanent --direct --passthrough ipv4 -t nat -I POSTROUTI
NG -o em2 -j MASQUERADE -s 192.168.9.0/24

```

9、重启防火墙

```
firewall-cmd --reload
```

10、有需要开启端口转发，可以配置

```

firewall-cmd --permanent --zone=external --add-port=8070/tcp
firewall-cmd --permanent --zone=external --add-port=8071/tcp
firewall-cmd --permanent --zone=external --add-port=8072/tcp
firewall-cmd --permanent --zone=external --add-forward-port=port=8070:pr
oto=tcp:toaddr=192.168.10.10:toport=8070
firewall-cmd --permanent --zone=external --add-forward-port=port=8071:pr
oto=tcp:toaddr=192.168.10.10:toport=8071
firewall-cmd --permanent --zone=external --add-forward-port=port=8072:pr
oto=tcp:toaddr=192.168.10.10:toport=8072

```

注意：搭建linux服务器网关时，有一个很奇怪的现象就是在网关后的内网通过pptp拨号拨其它外网服务器搭建的pptp服务器时，是拨不通的，这个是因为PPTP使用TCP端口1723传输控制命令，并使用GRE传输数据。由于GRE没有端口，因此服务器必须使用CallID来跟踪端点并实现NAT。

需要加载这两个模块：

```

# lsmod | grep pptp
# modprobe ip_nat_pptp

```

```
# modprobe ip_conntrack_pptp
```

当然，如果你这个网关服务器还搭建为pptp服务器的，你还需要设置，可以参照下面iptables时的做法：

链接：<https://stackoverflow.com/questions/31731067/linux-pptp-server-relay>

现在，您可以创建iptables规则来接受传入和转发请求：

```
# iptables -A INPUT -d $VPS1_IP_ADDR -p tcp --dport 1723 -j ACCEPT
# iptables -A INPUT -d $VPS1_IP_ADDR -p gre -j ACCEPT
# iptables -A FORWARD -d $VPS2_IP_ADDR -p tcp --dport 1723 -j ACCEPT
# iptables -A FORWARD -d $VPS2_IP_ADDR -p gre -j ACCEPT
```

最后设置DNAT规则：

```
# iptables -A PREROUTING -d $VPS1_IP_ADDR -p tcp --dport 1723 -j DNAT --
to-destination $VPS2_IP_ADDR
# iptables -A POSTROUTING -d $VPS2_IP_ADDR -p tcp --dport 1723 -j MASQUE
RADE
```

Ipsec

关于版块

关于Ipsec

IPSEC有两种封装模式：传输模式和隧道模式，常用的是隧道模式。隧道模式生成新的IP包头作为封装后加密后报文的IP头部，这样完全地对原始IP数据报进行认证和加密，可以隐藏用户私有的IP地址。IPSEC隧道搭建常用于总部与分支机构的连接或各IDC机房的相互通信。

本版块维护人员

版主：子木

QQ：1242119478

交流Q群：526749756

安装部署

以Cisco路由器端配置IPSEC隧道为例

前置条件

固定外网IP: 1.202.249.162

路由内网IP: 10.88.0.1

第一阶段配置

```
crypto isakmp enable #启用ike协商

crypto isakmp policy 1 #创建IEK协商，数字小则优

authentication pre-share #规定使用预共享密钥PSK来认证对等体是否合法

hash sha/md5 #配置在建立连接时协商IKE使用的散列算法，两种均可，但选择其中一种，对端也要一致

encryption DES/3DES/AES #配置在建立连接时协商IKE使用的加密算法，要和对端一致

group 2 #选择group 2

lifetime 86400 #管理连接的生存周期

crypto isakmp key zxkm4ykdVH4jyXiy address 210.212.167.9 #配置对等体认证PSK

crypto isakmp key zxkm4ykdVH4jyXiy address 210.212.167.10 #要配置多点ipsec，在这里继续加
```

第二阶段配置

```
crypto ipsec transform-set ubox-set esp-aes esp-md5-hmac #配置ipsec参数，协商通过ipsec隧道的数据的安全参数，注意安全协议和验证方式要和对端一致

mode tunnel #模式选择

#配置ACL（访问控制列表），定义需要保护的数据流
access-list 100 permit ip 10.88.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 101 permit ip 10.88.0.0 0.0.255.255 172.16.0.0 0.0.255.255

#配置IPsec策略
crypto map ubox-map 1 ipsec-isakmp
```

```
set peer 210.212.167.9
set transform-set ubox-set
set pfs group2
match address 100

#多点IPsec可继续加
crypto map ubox-map 1 ipsec-isakmp
set peer 210.212.167.10
set transform-set ubox-set
set pfs group2
match address 101

#外网接口应用ipsec策略
interface GigabitEthernet0/0
crypto map ubox-map
```

配置路由

```
ip route 0.0.0.0 0.0.0.0 1.202.249.161
ip route 10.88.0.0 255.255.0.0 10.88.0.2
```

配置ACL，隧道流量不经过NAT

```
ip nat inside source list 110 interface GigabitEthernet0/0 overload
access-list 110 deny ip 10.88.0.0 0.0.255.255 192.168.0.0 0.0.255.255
access-list 110 permit ip 10.88.0.0 0.0.255.255 any
```