秋明分享平台之

centos6.6下部署翻墙软件

包含gmail的imap

撰稿人：秋明

撰稿人邮箱：tyumen@zhoufengjie.cn

QQ群：90122290

本文撰稿日期： 2015年2月24日星期二

本站口号：开源、分享、共进

版权所有：随便使用

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 环境说明 4

3 国外服务器配置 4

3.1 安装Stunnel 4

3.2 生成Stunnel证书 4

3.3 配置Stunnel 4

3.4 安装DNS 5

3.5 安装sniproxy 6

3.6 配置sniproxy 6

3.7 启动服务 10

4 内部服务器配置 10

4.1 安装Stunnel 10

4.2 配置Stunnel 10

4.3 启动服务 11

5 代理翻墙 11

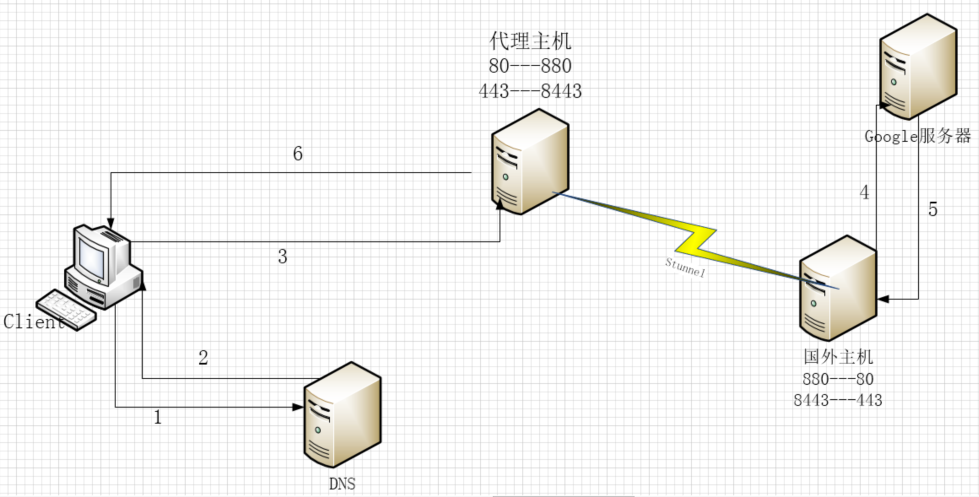
5.1 配置host文件 11

5.2 测试访问 12

# 前言

公司由于在公司每个人要访问国外的网站的时候，都需要自己翻墙到国外，为了方便大家上网方便，在公司出口部署了一个翻墙软件，大家不需要做任何操作就可以自动翻墙；

这里主要对443端口，80端口进行代理翻墙，解决Facebook，google，twitter，gmail的需求；目前我在公司做的方案为：在DNS上面做配置，将需要翻墙的域名解析到公司内部的一台代理服务器上，公司内部的代理服务器与国外主机进行建联进行服务；逻辑图如下：



这篇文章针对个人翻墙使用，因此将逻辑进行简化；DNS层面通过host实现，如果大家需要在公司内部使用，可以通过nsd的dns抢先应答或者对公司使用的LDNS进行配置特定解析（建议使用前一种+后一种，这样所有的人都可以自动访问翻墙网站了）；

前面一篇文章只写了代理http和https，这里增加了imap，pop，smtp的配置；

# 环境说明

操作系统：CentOS6.6

DNS：此文档不包含此项配置，通过固定host实现，用于个人翻墙

内网IP：192.168.231.224(配置前将此地址替换为你的内网地址)

国外IP：1.2.3.4(配置前将此地址替换为你的国外服务器地址)

# 国外服务器配置

## 安装Stunnel

# yum install -y stunnel

# wget -SO /etc/init.d/stunneld http://download.zhoufengjie.cn/ config/software/proxy/stunneld

# chmod 755 /etc/init.d/stunneld && chkconfig stunneld on

## 生成Stunnel证书

# openssl genrsa -out key.pem 2048

# openssl req -new -x509 -key key.pem -out cert.pem -days 1095

# cat key.pem cert.pem >> /etc/stunnel/stunnel.pem

# chmod 600 /etc/stunnel/stunnel.pem

## 配置Stunnel

# echo “ENABLED=1” > /etc/default/stunnel4

# vi /etc/stunnel/stunnel.conf #加入如下内容：

client = no

[http]

accept = 1.2.3.4:880

connect = 1.2.3.4:80

cert = /etc/stunnel/stunnel.pem

[https]

accept = 1.2.3.4:8443

connect = 1.2.3.4:443

cert = /etc/stunnel/stunnel.pem

[imaps]

accept = 1.2.3.4:8993

connect = 1.2.3.4:993

cert = /etc/stunnel/stunnel.pem

[pop3s]

accept = 1.2.3.4:8995

connect = 1.2.3.4:995

cert = /etc/stunnel/stunnel.pem

[smtps]

accept = 1.2.3.4:8465

connect = 1.2.3.4:465

cert = /etc/stunnel/stunnel.pem

## 安装DNS

# 说明：安装DNS的目的是为了国外的代理服务器sniproxy对要翻墙的域名进行解析；

# yum install bind bind-devel bind-chroot caching-nameserver(centos5下安装这个软件包会自动生成named.conf，centos6下没有这个软件包；关于bind的配置，请自己解决)

# 注：我使用的是公司自己开发的DNS，这里为了通用，给大家写一个使用标准bind的方法。

## 安装sniproxy

安装yum源；  
# rpm -ivh http://mirror.zhoufengjie.cn/centos/el6/x86\_64/RPMS/tyumenmirror-1.0-1.el6.noarch.rpm  
安装sniproxy；  
# yum install sniproxy –y

## 配置sniproxy

编辑配置文件：vi /usr/local/sniproxy/etc/sniproxy.conf

user daemon

pidfile /var/run/sniproxy.pid

error\_log {

syslog daemon

#filename /var/log/sniproxy.error.log

priority notice

}

listener 1.2.3.4:80 {

protocol http

table http\_hosts

access\_log {

filename /var/log/sniproxy.log

}

}

listener 1.2.3.4:443 {

protocol tls

table https\_hosts

access\_log {

filename /var/log/sniproxy.log

}

}

listener 1.2.3.4:993 {

protocol tls

table imaps\_hosts

access\_log {

filename /var/log/sniproxy.log

}

}

listener 1.2.3.4:995 {

protocol tls

table pops\_hosts

access\_log {

filename /var/log/sniproxy.log

}

}

listener 1.2.3.4:465 {

protocol tls

table smtps\_hosts

access\_log {

filename /var/log/sniproxy.log

}

}

table http\_hosts {

.\* \*:80

}

table https\_hosts {

.\* \*:443

}

table imaps\_hosts {

.\* \*:993

}

table pops\_hosts {

.\* \*:995

}

table smtps\_hosts {

.\* \*:465

}

table {

.\* 127.0.0.1

}

## 启动服务

启动stunnel：

# service stunneld start

启动dns：

# service named start

启动sniproxy：

# service sniproxyd start

# 内部服务器配置

## 安装Stunnel

# yum install -y stunnel

# wget -SO /etc/init.d/stunneld http://download.zhoufengjie.cn/config/software/proxy/stunneld

# chmod 755 /etc/init.d/stunneld && chkconfig stunneld on

## 配置Stunnel

# echo “ENABLED=1” > /etc/default/stunnel4

# vi /etc/stunnel/stunnel.conf #加入如下内容：

client = yes

pid = /etc/stunnel/stunnel.pid

[http]

accept = 80

connect = 1.2.3.4:880

[https]

accept = 443

connect = 1.2.3.4:8443

[imaps]

accept = 993

connect = 1.2.3.4:8993

[pop3s]

accept = 995

connect = 1.2.3.4:8995

[smtps]

accept = 465

connect = 1.2.3.4:8465

## 启动服务

启动stunnel：

# service stunneld start

# 代理翻墙

## 配置host文件

举例（将自己要翻墙的域名写到host文件里面即可）：

192.168.231.224 facebook.com

192.168.231.224 www.facebook.com

192.168.231.224 twitter.com

192.168.231.224 www.twitter.com

192.168.231.224 google.com

192.168.231.224 www.google.com

192.168.231.224 accounts.google.com

192.168.231.224 gmail.com

192.168.231.224 www.gmail.com

192.168.231.224 mail.google.com

192.168.231.224 smtp.gmail.com

192.168.231.224 imap.gmail.com

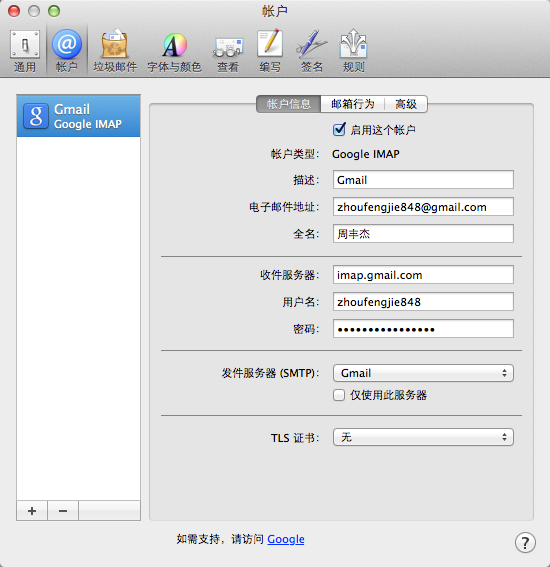
192.168.231.224 pop.gmail.com

也可以下载我的host文件,http://download.zhoufengjie.cn/config/software/proxy/hosts

## 测试访问

gmail邮箱（我开启了二次认证，因此申请了一个应用密码）：收发邮件正常





用浏览器打开要翻墙的网站，如下图所示：





