Centos7 搭建 OpenVPN --多用于企业内网VPN或中国墙

如果宅|网络工程师培训 (http://www.ifzhai.com) http://www.ifzhai.com 2017-06-26 14:41 出处：PinG 作者：PinG 编辑：PinG

企业中VPN的使用非常常见，大公司多部分会买专业的VPN设备，但对于小公司来说自己搭建OpenVPN是经济实惠的。当然它的作用对于个人来说也是非常可观的，比如你买个国外的VPN然后搭建个~你懂的。

(如果本文中的图片看不清，可按住键盘Ctrl键+鼠标滚轮上键)

一、基本配置

1、时间同步

#ntpdate cn.ntp.org.cn

#hwclock -w

2、添加EPEL源

#wget http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm (http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm)

#rpm -Uvh epel-release-latest-7.noarch.rpm

二、安装篇

1、安装Openvpn

#yum install openvpn -y

2、从示例配置文件复制一份配置文件到/etc/openvpn

#cp /usr/share/doc/openvpn-（这里版本号自己打）/sample/sample-config-files/server.conf /etc/openvpn

3、修改server.conf

#cd /etc/openvpn/

#vim server.conf

去掉以下几行注释

push "redirect-gateway def1 bypass-dhcp"

push "dhcp-option DNS 208.67.222.222"

push "dhcp-option DNS 208.67.220.220"

user nobody

group nogroup

去掉下面这行的注释，并在下面添加一行

tls-auth ta.key 0 # This file is secret

key-direction 0

根据需求修改虚拟IP段，即为客户端获得IP

server 10.8.0.0 255.255.255.0（默认）

此处我改成

server 10.129.21.0 255.255.255.0

更改DNS值 此处我改为了8.8.8.8

push "dhcp-option DNS 8.8.8.8"

通过cat server.conf | grep -v ^'#' | grep -v ^';' 命令查看server.conf有效配置如下

port 1194

周点击榜

Centos7 搭建 OpenVPN -证书
使用旧PC机安装ESXI5.5 / 6.
Panabit+Panalog构建高大上
Centos 7 安装ELK 6.3.1 并汉
Centos7 安装Openmeetings3
Centos7 搭建 LogAnalyzer4.1
Centos7 搭建 OpenVPN --多
Centos7 安装 MantisBT (http
Centos 安装tomcat (http://w
Zabbix3.2 设置短信、邮件报

如果本站内容对您有所帮助

图文推荐

proto udp

dev tun

ca ca.crt

cert server.crt

key server.key # This file should be kept secret

dh dh2048.pem

server 10.129.21.0 255.255.255.0

ifconfig-pool-persist ipp.txt

push "redirect-gateway def1 bypass-dhcp"

push "dhcp-option DNS 8.8.8.8"

push "dhcp-option DNS 208.67.220.220"

keepalive 10 120

tls-auth ta.key 0 # This file is secret

key-direction 0

cipher AES-256-CBC

user nobody

group nobody

persist-key

persist-tun

status openvpn-status.log

verb 3

explicit-exit-notify 1

4、安装easy-rsa生成证书及密钥

#yum install easy-rsa

将相关文件复制到OpenVPN的配置目录

#cp -R /usr/share/easy-rsa/ /etc/openvpn

修改的是vars文件

#vim /etc/openvpn/easy-rsa/2.0/vars

随便修改以下数值export KEY_NAME处修改值建议为server 下面会调用

使变量生效：

#cd /etc/openvpn/easy-rsa/2.0/

#source vars

会提示NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/2.0/keys属于正常。

创建CA

在/etc/openvpn/easy-rsa/2.0目录中执行：

#./clean-all

#./build-ca

一路回车

./build-ca

Generating a 2048 bit RSA private key

.....+++

.....+++

writing new private key to 'ca.key'

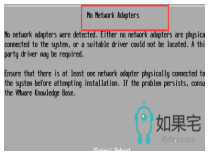
You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

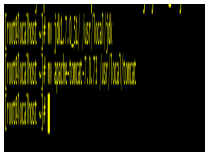
There are quite a few fields but you can leave some blank

For some fields there will be a default value,



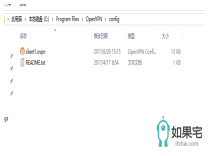
使用旧PC机安装ESXI5.5 / 6.0 网卡为Realtek r8101 (http://www.ifzhai.com/article.php?id=94)

Centos 汉化EL (http:/ article.



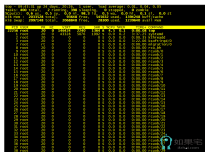
Centos 安装tomcat (http://www.ifzhai.com/article.php?id=84)

Ubuntu 务器 (http:/ article.



Centos7 搭建 OpenVPN - 证书及用户密码双重认证 - (http://www.ifzhai.com/article.php?id=80)

Windov (http:/ article.



centos 6.x 7.x 安装zabbix agent (http://www.ifzhai.com/article.php?id=46)

centos 安装图 (http:/ article.

If you enter '.', the field will be left blank.

Country Name (2 letter code) [CN]:

State or Province Name (full name) [BJ]:

Locality Name (eg, city) [BeiJing]:

Organization Name (eg, company) [PinG]:

Organizational Unit Name (eg, section) [haha]:

Common Name (eg, your name or your server's hostname) [PinG CA]:

Name [server]:

Email Address [ping@ping.com]:

生成服务端证书、密钥

#./build-key-server server

一直回车，先不要设置密码，最后有两个y需要按一下

./build-key-server server

Generating a 2048 bit RSA private key

.....+++

.+++

writing new private key to 'server.key'

You are about to be asked to enter information that will be incorporated

into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

Country Name (2 letter code) [CN]:

State or Province Name (full name) [BJ]:

Locality Name (eg, city) [BeiJing]:

Organization Name (eg, company) [PinG]:

Organizational Unit Name (eg, section) [haha]:

Common Name (eg, your name or your server's hostname) [server]:

Name [server]:

Email Address [ping@ping.com]:

Please enter the following 'extra' attributes

to be sent with your certificate request

A challenge password []:

An optional company name []:

Using configuration from /etc/openvpn/easy-rsa/2.0/openssl-1.0.0.cnf

Check that the request matches the signature

Signature ok

The Subject's Distinguished Name is as follows

countryName :PRINTABLE:'CN'

stateOrProvinceName :PRINTABLE:'BJ'

localityName :PRINTABLE:'BeiJing'

organizationName :PRINTABLE:'PinG'

organizationalUnitName:PRINTABLE:'haha'

commonName :PRINTABLE:'server'

name :PRINTABLE:'server'

emailAddress :IA5STRING:'ping@ping.com'

Certificate is to be certified until Jun 24 07:06:49 2027 GMT (3650 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

生成Diffie-Hellman key：

#./build-dh

等待几分钟；

生成HMAC签名加强TLS认证：

#openvpn --genkey --secret keys/ta.key

生成客户端证书、密钥

#./build-key client1

一直回车无需密码，有两个Y需要按。

拷贝证书到/etc/openvpn下

#cd keys/

cp ca.crt ca.key server.crt server.key ta.key dh2048.pem /etc/openvpn/

打开IP转发

#vim /etc/sysctl.conf

添加

net.ipv4.ip_forward=1

生效

#sysctl -p

防火墙配置

#service firewalld start

#firewall-cmd --add-service openvpn

#firewall-cmd --permanent --add-service openvpn

#firewall-cmd --add-masquerade

#firewall-cmd --permanent --add-masquerade

启动VPN服务

#systemctl start openvpn@server

#systemctl enable openvpn@server

生成OpenVPN客户端使用的ovpn

#cp /usr/share/doc/openvpn-2.4.1（此处目录换成你的版本号）/sample/sample-config-files/client.conf /etc/openvpn/easy-rsa/2.0/keys/

编辑client.conf

#cd /etc/openvpn/easy-rsa/2.0/keys

#vim client.conf

找到remote一段：

remote server_IP_or_domain 1194

修改ip为服务器ip

去掉如下两行的注释

user nobody

group nogroup

更改ca, cert 和 key的值，修改为[inline]：inline代表本文件。

ca [inline]

cert [inline]

key [inline]

找到tls-auth一段，去掉注释并在其下添加一行

tls-auth [inline] 1

key-direction 1

生成ovpn文件：

#cat client.conf <(echo -e '<ca>') ca.crt <(echo -e '</ca>\n<cert>') client1.crt <(echo -e '</cert>\n<key>') client1.key <(echo -e '</key>\n<tls-auth>') ta.key <(echo -e '</tls-auth>') > client1.ovpn

然后把client1.ovpn传给客户端放入config目录下即可

三、客户端安装

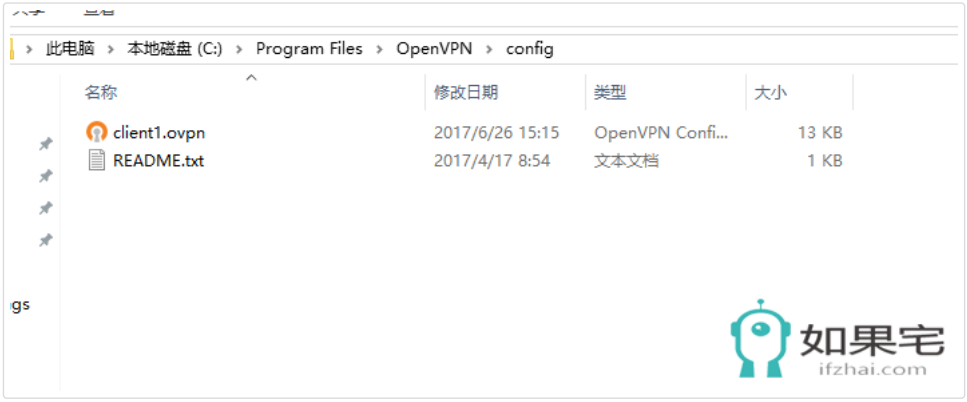
软件包在我的云盘里（http://pan.baidu.com/s/1jIFqDTk）

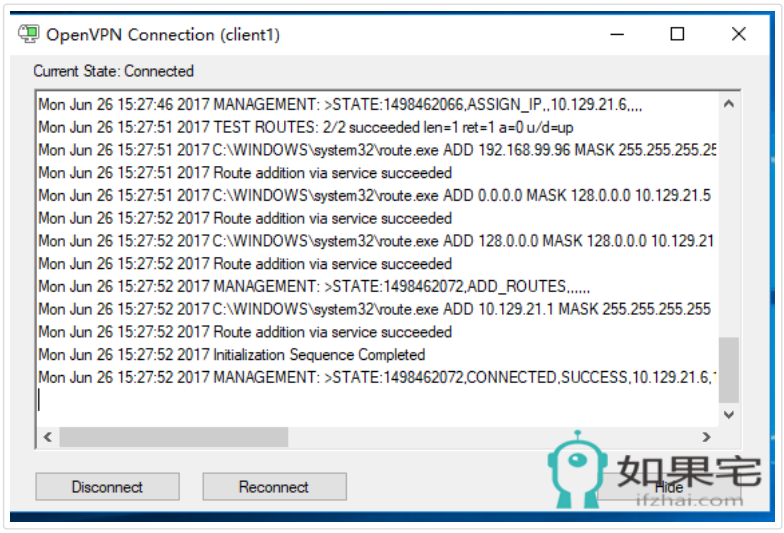
安装包为openvpn-2.2.2-install.exe

默认安装后找到

C:\Program Files\OpenVPN\config目录

将client1.ovpn放入该目录后即可连接。





（转载请注明出处：如果宅www.ifzhai.com）

上一篇: Centos7 安装Openmeetings3.2.1 -开源视频会议系统 (http://www.ifzhai.com/article.php?id=6)

Centos7 搭建 LogAnalyzer4.1.5 - 开源日志服务器 (http://www.ifzhai.com/article.php?id=9) :下一篇

更多 服务器开源 (http://www.ifzhai.com/category.php?cid=3) 相关资讯：

使用旧PC机安装ESXI5.5 / 6.0 网卡为Realtek r810

Centos 7 安装ELK 6.3.1 并汉化ELK (http://www.if

Centos 安装tomcat (http://www.ifzhai.com/articl

Ubuntu 16.04 搭建SVN服务器 (http://www.ifzhai.

Centos7 搭建 OpenVPN -证书及用户密码双重认证