手把手教你搭建自己的 VPS 服务器

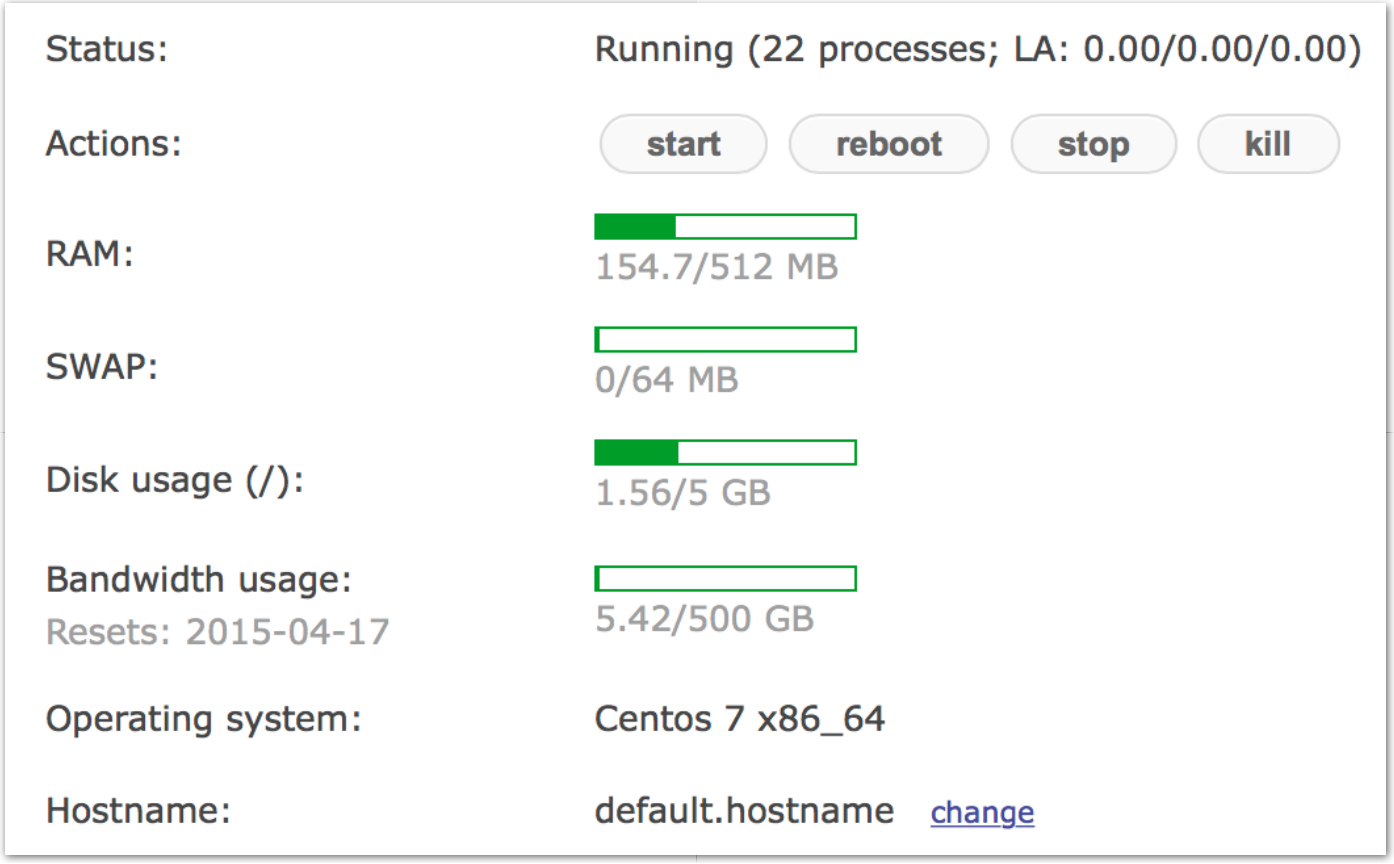
作者： zhgqThomas | 2016-01-27 08:02 评论: 19 收藏: 19

总有一些时候，你想要一台自己的 VPS 。本文分享了作者在实践过程中的一些经验，可以给那些自己搭建 VPS 的朋友一点帮助。

前期准备

需要购买一台拥有 root 权限的 VPS ，我选择的是 **搬瓦工** ,当时购买的是 512 M 内存 5 G SSD，500 G 流量/月， 9.99 刀每年，但是好像现在这种低价套餐已经结束了。有意的朋友可以看一下其他的套餐或者别的公司的 VPS。有的朋友说 **DigitalOcean** 的速度非常快，看YouTube直接 1440p，但是我还没测试过，目前搬瓦工的速度能满足我的需求，而且 DO 的价格比较昂贵。

下图是搭了 SS 和 IPsec VPN 服务的使用情况，仅供参考：



使用情况

服务器购买后，安装 CentOS7，因为以下教程都是基于 CentOS7 的，安装新的 OS 后，搬瓦工会告诉你 SSH 的端口和 root 的密码，这些是自己无法自定义的，要记住了如果实在忘了也可以重置 root 密码，或者直接使用搬瓦工提供的在线SSH登录来操作也可，就是反应比较慢，所以我们以后还是常用 ssh 登录来配置 VPS，Mac 下直接使用终端就好，win 下自行寻找一个 ssh 工具就好。

登录 ssh 的命令:

```
$ ssh -p vps 端口号 root@vpsIP 地址
```

登录上以后就相当于在本地操作一样了，你可以使用各种 Linux 命令来操作了。

配置防火墙

如果 SSH 无法登录，那说明防火墙关闭了 SSH 端口，需要通过在线 SSH 登录进去关闭防火墙重新配置。

清除防火墙配置

```
$ iptables -F
```

清除 iptabels 所有表项，同时 nat 设置也没了，但是我们后续的脚本里会配置的，不用担心。如果 SSH 登录正常就不用管防火墙。

安装 **firewalld**

```
$ yum install firewalld firewall-config
$ systemctl start firewalld
```

P.S. 我在安装完 firewalld 之后然后启动服务的时候一直显示失败，然后重启了一遍服务器就可以正常的启动 firewalld 服务了，有类似情况的朋友可以重启一下服务器。

修改 SSH 端口

```
$ vi /usr/lib/firewalld/services/ssh.xml
```

会出现以下的内容：

```
<?xml version="1.0" encoding="utf-8"?><service>
   <short>SSH</short>
   <description>Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides secure encrypted communications. If you plan on accessing your machine remotely via SH over a firewalled interface, enable this option. You need the openssh-server package installed for this option to be useful.</description>
   <port protocol="tcp" port="22"/>
</service>
```

将 port=”22”，修改成搬瓦工提供给你的端口号，然后重载 firewalld 就 OK。

vi 的命令: 按 “ i ” 是编辑模式，编辑后按 “ esc ” 退出编辑模式，然后按 Shift 输入 “ : ” 和 “ wq ” 保存退出 vi。

```
$ firewall-cmd --permanent --add-service=ssh
$ firewall-cmd --reload
```

OK，现在准备工作都已就绪，安装了源，安装配置了防火墙，下一步开始搭建服务了。

搭建 Shadowsocks 服务

这个服务是最简单也是最常用的。

安装组件

```
$ yum install m2crypto python-setuptools
$ easy_install pip
$ pip install shadowsocks
```

安装时部分组件需要输入 Y 确认。小内存 VPS 可以分别安装组件。

安装完成后配置服务器参数

```
$ vi  /etc/shadowsocks.json
```

写入如下配置：

```
{
    "server":"0.0.0.0",
    "server_port":8388,
    "local_address": "127.0.0.1",
```

```
    "local_port":1080,
    "password":"mypassword",
    "timeout":300,
    "method":"aes-256-cfb",
    "fast_open": false,
    "workers": 1
}
```

将上面的 mypassword 替换成你的密码， server_port 也是可以修改的，例如 443 是 Shadowsocks 客户端默认的端口号。

如果需要修改端口，需要在防火墙里打开响应的端口，用 firewalld 操作就比较简单了：

```
$ vi /usr/lib/firewalld/services/ss.xml
```

下面代码粘贴到里面：

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>SS</short>
  <description>Shadowsocks port
  </description>
  <port protocol="tcp" port="自定义ss端口号"/>
</service>
```

保存退出，然后重启 firewalld 服务：

```
$ firewall-cmd --permanent --add-service=ss
$ firewall-cmd --reload
```

运行命令，启动 Shadowsocks 服务

运行下面的命令：

```
$ ssserver -c /etc/shadowsocks.json
```

至此 shadowsocks 搭建完成，shadowsocks 已经可以使用，如果你没有过高的要求，下面的步骤可以省略，下面是后台运行 Shadowsocks 的步骤。

安装 supervisor 实现后台运行

运行以下命令下载 supervisor：

```
$ yum install python-setuptools
$ easy_install supervisor
```

然后创建配置文件：

```
$ echo_supervisord_conf > /etc/supervisord.conf
```

修改配置文件：

```
$ vi /etc/supervisord.conf
```

在文件末尾添加：

```
[program:ssserver]command = ssserver -c /etc/shadowsocks.json
autostart=true
autorestart=true
startsecs=3
```

设置 supervisord 开机启动，编辑启动文件：

```
$ vi /etc/rc.local
```

在末尾另起一行添加：

```
$ supervisord
```

保存退出（和上文类似）。另 centOS7 还需要为 `rc.local` 添加执行权限：

```
$ chmod +x /etc/rc.local
```

至此运用 supervisord 控制 Shadowsocks 开机自启和后台运行设置完成。重启服务器即可。

搭建 Strongswan 实现在 iOS 上连接 VPN

如果你只是需要在 Android, PC 上使用 VPN，那可以直接忽略此章内容， Shadowsocks 已经可以非常完美的帮助以上设备实现翻墙。 但是由于 iOS 上无法使用 Shadowsocks 所以需要使用 Strongswon 建立 IPsecVPN。

下载并编译 Strongswan

首先我们来编译 Strongswan， 因为直接用 yum install 的不能用，原因不明，所以直接下载源码和依赖包进行编译。

下载 Strongswan 的源码：

```
$ wget http://download.strongswan.org/strongswan.tar.gz && tar zxvf strongswan*
$ cd strongswan*
```

下载编译源码所需要的依赖包(小内存请分批下载)：

```
$ yum install -y make gcc gmp-devel openssl openssl-devel
```

因搬瓦工是 OpenVZ 的所以用下面的命令来进行配置：

```
$ ./configure --sysconfdir=/etc --disable-sql --disable-mysql --disable-ldap --enable-dhcp --enable-eap-identity --enable-eap-mschapv2 --enable-md4 --enable-xauth-eap --enable-eap-peap --enable-eap-md5 --enable-openssl --enable-shared --enable-unity --enable-eap-tls   --enable-eap-ttls --enable-eap-tnc --enable-eap-dynamic --enable-addrblock --enable-radattr --enable-nat-transport --enable-kernel-netlink --enable-kernel-libipsec
```

非 OpenVZ 的请用下面的命令来进行配置：

```
./configure --sysconfdir=/etc --disable-sql --disable-mysql --disable-ldap --enable-dhcp --enable-eap-identity --enable-eap-mschapv2 --enable-md4 --enable-xauth-eap --enable-eap-peap --enable-eap-md5 --enable-openssl --enable-shared --enable-unity --enable-eap-tls   --enable-eap-ttls --enable-eap-tnc --enable-eap-dynamic --enable-addrblock --enable-radattr --enable-nat-transport --enable-kernel-netlink
```

开始编译源代码：

```
$ make && sudo make install
```

没有错误出现后，可进行下一步。

生成证书

建立个临时目录来生成证书：

```
$ mkdir ~/ipsec_cert && cd ~/ipsec_cert
```

生成服务器证书

用的是 **iOS8 不越狱翻墙方案** 中创建的脚本。SERVER 换成自己的域名或IP 都行。

```
$ wget https://gist.githubusercontent.com/songchenwen/14c1c663ea65d5d4a28b/raw/cef8d8bafe6168388b105f780c442412e6f8ede7/server_key.sh
$ sh server_key.sh SERVER
```

生成客户端证书

同样是他的脚本，这个脚本还会生成一个 .p12 证书，这个证书需要导入到 iOS 里，USER 换成你自己的用户名 EMAIL 换成你自己的 email。

```
$ wget https://gist.githubusercontent.com/songchenwen/14c1c663ea65d5d4a28b/raw/54843ae2e5e6d1159134cd9a90a08c31ff5a253d/client_key.sh
$ sh client_key.sh USER EMAIL
```

复制证书到 /etc/ipsec.d/

Strongswan 需要的是 `cacerts/strongswanCert.pem` 、 `certs/vpnHostCert.pem` 、 `private/vpnHostKey.pem` 这三个文件。

```
$ sudo cp cacerts/strongswanCert.pem /etc/ipsec.d/cacerts/strongswanCert.pem
```

```
$ sudo cp certs/vpnHostCert.pem /etc/ipsec.d/certs/vpnHostCert.pem
$ sudo cp private/vpnHostKey.pem /etc/ipsec.d/private/vpnHostKey.pem
```

同步客户端证书到本地

客户端需要的是 .p12 证书和 `cacerts/strongswanCert.pem` 将这两个证书同步到本地，然后通过邮件发送到 iOS 设备中并安装

```
$ scp -P ssh端口 root@服务器ip:~/ipsec_cert/****.p12 ~/
$ scp -P ssh端口 root@服务器ip:~/ipsec_cert/cacerts strongswanCert.pem ~/
```

配置 Strongswan

编辑 `/etc/ipsec.conf` ：

```
$ vi /etc/ipsec.conf
```

将下面的代码覆盖原有内容：

```
config setup
    ### strictcrlpolicy=yes
    ### uniqueids = replace
    ### charondebug="cfg 2, dmn 2, ike 2, net 0" ### 要看Log时，取消注释本行

conn %default
    keyexchange=ikev1
    dpdaction=hold
    dpddelay=600s
    dpdtimeout=5s
    lifetime=24h
    ikelifetime=240h
    rekey=no
    left=emptyzone.github.io ### 这里换成你登录 VPN 用的域名或 IP，与生成证书时相同
    leftsubnet=0.0.0.0/0
    leftcert=vpnHostCert.pem
    leftsendcert=always
    right=%any
    rightdns=8.8.8.8
    rightsourceip=10.0.0.0/8

conn CiscoIPSec
    rightauth=pubkey
    rightauth2=xauth
    auto=add
```

编辑 `/etc/ipsec.secrets` ， 创建用户名及密码：

```
vi /etc/ipsec.secrets
```

将以下内容添加进去：

```
### 验证用户所需的信息
### 用户名 : EAP "密码"
: RSA vpnHostKey.pem
你的用户名 : EAP "你的密码"
```

使用 firewalld 配置防火墙

用 firewalld 开放 4500、500 端口和 esp 协议。

```
$ vi /usr/lib/firewalld/services/ipsec.xml
```

内容如下：

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>IPsec</short>
  <description>Internet Protocol Security (IPsec) incorporates security for network transmissions directly into the Internet Protocol (IP). IPsec provides methods for both encrypting data and authentication for the host or network it sends to. If you plan to use a vpnc server or FreeS/WAN, do not disable this option.</description>
  <port protocol="ah" port=""/>
  <port protocol="esp" port=""/>
  <port protocol="udp" port="500"/>
  <port protocol="udp" port="4500"/>
</service>
```

然后输入以下命令后，至此整个搭建过程就结束了。

```
$ firewall-cmd --permanent --add-service=ipsec
$ firewall-cmd --permanent --add-masquerade
$ firewall-cmd --reload
```

把下载的两个证书用 email 发送到你的 iOS 上，安装后建立个 VPN 连接，选 IPsec，使用证书，选择你的用户名的证书即可，登录下试试吧。

最新评论

发表评论

来自北京的 Chrome 59.0|Mac 10.12 用户 2017-08-04 09:54 赞 回复

解答的很详细，我刚刚接触，没有代码基础，有问题请教楼主，可以有偿咨询，非常期盼得到楼主的回复，q916007459

六朝如梦 [Chrome 55.0|Windows 10] 2017-01-19 21:26 3 赞 回复

支持下

来自北京的 Chrome Mobile 33.0|Android 4.4 用户 2016-10-07 01:37

改ssh的端口直接去/etc/ssh/sshd_config改就好了呀，没见过你这样改端口的。。。还有，使用firewalld打开一个端口只需要用firewalld-cmd --add-port=6666/tcp(udp) --permanent就行啊。你这开端口的姿势也是够奇葩-_-||

来自湖南的 Mobile Safari 6.0|iOS 9.3 用户 2016-09-07 18:50 赞 回复

可以帮我搭建下vps吗？可以付工资的加我QQ2991363991

[1] 来自北京的 Chrome 40.0|Windows XP 用户 发表于 2016-02-19 10:51 的评论： 赞 回复

这题目有点让人误解吧，个人觉得应该是搭建自己的VPN才对，在vps上搭建vpn，而非是搭建vps

linux [Chrome 47.0|Mac 10.11] 2016-02-20 18:53 3 赞 回复

题目是特意的，你懂得。

[1] 来自广东广州的 Chrome 47.0|Windows 7 用户 发表于 2016-01-30 10:24 的评论： 赞 回复

很不错，值得收藏！有些是有格式错误的，自己测试吧，小问题

[2] linux [Chrome 47.0|Mac 10.11] 发表于 2016-01-30 12:18 的评论： 赞 回复

可以告诉我们哪里有错误， 完善这篇~

[3] 来自广东的 Firefox 43.0|Windows 7 用户 发表于 2016-01-30 23:33 的评论： 3 赞 回复

额，教程只是有点小问题而已。
先说明，本人用的是搬瓦工的CentOS 7 minimal。
firewalld这一段，安装的时候确实提示没有相应包，用yum search all firewall找到对应的软件包就好了；
安装supervisor这段，python-setuptools这个没有，不过不影响；
supervisord.conf的[program:ssserver]要换行，不然程序会运行失败；
IOS这块，问题很严重，因为我没有iPhone，版主赶紧寄手机过来测试

linux [Chrome 47.0|Mac 10.11] 2016-01-31 20:41 赞 回复

iPhone 我都没有。。。

[1] 来自广东广州的 Chrome 31.0|Windows 7 用户 发表于 2016-01-27 17:12 的评论： 赞 回复

[root@localhost /]# yum install firewalld firewall-config
Loaded plugins: fastestmirror
Setting up Install Process
Loading mirror speeds from cached hostfile
* base: centos.mia.host-engine.com
* extras: reflector.westga.edu
* updates: mirror.us.leaseweb.net
No package firewalld available.
No package firewall-config available.
Error: Nothing to do

到这里就不知道怎么搞了

来自广东广州的 Chrome 47.0|Windows 7 用户 2016-01-30 10:22 赞 回复

yum search all firewall

[1] 来自湖北鄂州的 Chrome Mobile 47.0|Android 5.1 用户 发表于 2016-01-27 10:51 的评论： 1 赞 回复

那么问题来了：哪家不用信用卡

ryt [Chrome 47.0|GNU/Linux] 2016-01-28 05:59 2 赞 回复

DO可以使用Paypal.

[1] 来自湖北鄂州的 Chrome Mobile 47.0|Android 5.1 用户 发表于 2016-01-27 10:51 的评论： 1 赞 回复

那么问题来了：哪家不用信用卡

yiqihaha [Chrome 47.0|Windows 10] 2016-01-27 21:32 1 赞 回复

这个 搬瓦工 就可以用支付宝支付

来自湖南长沙的 Chrome 47.0|Windows 10 用户 2016-01-27 20:58 1 赞 回复

班瓦工ss早就可以一键部署的,只要自己改个帐户密码就够了, 看了这文章也是够折腾的,不知道猴年马月的文章被你扒拉出来了吧

[1] 来自广东广州的 Chrome 31.0|Windows 7 用户 发表于 2016-01-27 17:12 的评论： 赞 回复

[root@localhost /]# yum install firewalld firewall-config
Loaded plugins: fastestmirror
Setting up Install Process
Loading mirror speeds from cached hostfile
* base: centos.mia.host-engine.com
* extras: reflector.westga.edu
* updates: mirror.us.leaseweb.net
No package firewalld available.
No package firewall-config available.
Error: Nothing to do

到这里就不知道怎么搞了

来自北京的 Firefox 43.0|Windows 7 用户 2016-01-27 17:28 赞 回复

提示是没有这个包，请问你的系统是centos7吗?

[1] 来自湖北鄂州的 Chrome Mobile 47.0|Android 5.1 用户 发表于 2016-01-27 10:51 的评论： 1 赞 回复

那么问题来了：哪家不用信用卡

来自北京的 Chrome 45.0|Windows 10 用户 2016-01-27 13:52 2 赞 回复

host1plus的支持支付宝，找找有很多支持支付宝的。

来自河南洛阳的 Chrome 45.0|Windows 10 用户 2016-01-27 13:47 2 赞 回复

很详细，不错，已经ctrl+D了。后面的VPN教程可以用于Win连接吗？我自己搭建的pptp VPN连接速度不如SS啊感觉。

转自：http://letchinese.com/2015/04/12/build-your-own-vps/ 作者： zhgqThomas

上一篇：如何通过阅读源代码了解 vmstat 中的指标
下一篇：grep 命令系列：grep 中的正则表达式

相关阅读

VPS VPN

Opera 浏览器内置的 VPN 只是个代理而已，而 2016-04-23
四种立即改善在线安全的方法 2017-02-23
什么是 Linux VPS 托管? 2017-04-11
2019 年最好的 7 款虚拟私人网络服务 2019-04-07
使用 sshuttle 构建一个穷人的虚拟专网 2019-10-18