



使用obfsproxy混淆任意流量

发表于: 2015年08月22日 • 124 条评论 • 10,139 次浏览 • 翻墙

obfsproxy是由Tor Project为Tor在被审查的国家使用而开发出的流量混淆插件以规避这些国家的防火墙...不过这个插件不仅可以用在Tor网桥上,还可以用在OpenVPN,SSH等其他应用上...

配置服务端:

我们可以从python-pip安装,或者从torbrowser提取,不建议使用debian/ubuntu源安装,因为缺少scramblesuit特性..

如果是Debian/Ubuntu类系统:

先安装环境

```
apt-get install gcc python-pip python-dev
```

如果是CentOS则执行

```
yum install python-pip python-devel gcc pycrypto
```

之后安装obfsproxy

```
pip install obfsproxy
```

执行obfsproxy查看支持的混淆方式

```
xiaolan@cui:~$ obfsproxy
usage: obfsproxy [-h] [-v] [--log-file LOG_FILE]
               [--log-min-severity {error,warning,info,debug}] [--no-log]
               [--no-safe-logging] [--data-dir DATA_DIR] [--proxy PROXY]
               {managed,obfs2,dummy,obfs3,scramblesuit,b64} ...
```

运行服务端

一般使用obfs3或者scramblesuit模式

scramblesuit是obfs3的加强版,使用密码加密..使得GFW无法模拟obfs客户端来探

测被混淆的是什么..我们这里以scramblesuit作为示范..

注意: scramblesuit的密码必须为BASE32字符..

BASE32字符是:ABCDEFGHIJKLMNOPQRSTUVWXYZ3456789 且必须为32位

```
obfsproxy --data-dir ~/.obfs/ scramblesuit --dest 127.0.0.1:22
--password SBSB4444FANGBINXING4SBSBSBSBSBSB server
0.0.0.0:8080 &
```

127.0.0.1:22 是要混淆的端口 (协议)

0.0.0.0:8080 是将混淆后的端口...

那一大串长的是密码..

如果不需要后台运行则去掉最后蓝色的&

如果运行成功后应该会提示

```
2015-08-21 22:54:12,282 [WARNING] Obfsproxy (version: 0.2.13)
starting up.
2015-08-21 22:54:12,282 [ERROR]
#####
Do NOT rely on ScrambleSuit for strong security!
#####
```

至此服务端已经配置完成....

运行客户端

Windows请下载Tor Browser后, 解压打开Browser\TorBrowser\Tor
\PluggableTransports\obfsproxy.exe复制出来,用法同下..

(更新: 做了一个obfsproxy.exe的打包, 在下面...)

```
obfsproxy scramblesuit --dest 1xx.xxx.xxx.xxx:8080 --password
SBSB4444FANGBINXING4SBSBSBSBSBSB client
127.0.0.1:22222
```

1xx.xxx.xxx.xxx:8080 是你的服务器IP地址..

长串是密码,需与服务端一致

127.0.0.1:22222 是本地端口..

这时就可以用SSH翻墙而不会被特征检测了....当然也可以通过obfs混淆OpenVPN

等其他协议....

```
ssh -N -D 7070 fanqiang@127.0.0.1 -p 22222
```

附录

Windows 版本obfsproxy.exe

<https://onedrive.live.com/redir?resid=2A24B8A135949B48!111&authkey=!ANLhWx--WZ38vyg&ithint=file%2czip>

(解压密码 xiaolan.me)

EXE文件的VirusTotal扫描结果:

<https://www.virustotal.com/en/file/ef181a361dc4a882c81a370796b9331f4009d0c4cf95a3cc0d5593511c854dcb/analysis/>

SHA256:

ef181a361dc4a882c81a370796b9331f4009d0c4cf95a3cc0d5593511c854dcb

无法运行请确认是否安装python运行环境...

分享一个公共帐号..(SOCKS5代理..)

协议: *scramblesuit*

IP地址: *185.61.148.246:8080*

密码: *FUCKFANGBINXINGHEXIJINPINGSBDASB*

无限流量欢迎滥用

视频教程:

obfsproxy翻墙教程



视频中显示速度比较慢,是因为用了**Tor+VPNGate**翻回国内,实际应用中并没有那么慢,因此无需担心:)

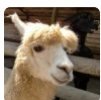
转载请注明来自Xiaolan's Blog (<https://xiaolan.me>)

124 条评论



Anonymous • 2015年08月22日 • Reply

那么用tor浏览器时用meek还是obfs3或者scramblesuit更安全？



Xiaolan • 2015年08月22日 • Reply • 博主

都一样..tor网桥会替换掉原始的入口节点,tor的入口还是安全的..



天天上 • 2015年08月24日 • Reply

meek背后是大公司，破解Tor的实力更强，还可能收集你别的资料。obfs3最好，基本是个人在搞，速度比meek快一点



Anonymous • 2015年08月26日 • Reply

开玩笑么



Anonymous • 2015年08月27日 • Reply

On August 16th, 2014 dcf said:

You're right that using meek means there are more entities who can watch the traffic patterns between you and your first hop. With ordinary bridges it is:

your ISP, all upstream routers, and the bridge itself.

With meek it is:

your ISP, all upstream routers, Amazon/Google, and the bridge itself.

Of course, none of these entities gets to see your plaintext directly—there is still a Tor encryption layer underneath meek's HTTPS tunnel. But all those entities are in a better position to do timing correlation, for example.

It's important to understand that Amazon/Google don't actually get to see what web sites you browse. What they see is a bunch of encrypted HTTPS POST requests, which they forward to a Tor bridge. Amazon/Google knows that your IP address is using Tor; what we're trying to do is prevent the censor from knowing it.



loveyb • 2015年08月24日 • Reply

经测试windows可以直接pip install obfsproxy



ben • 2015年09月01日 • Reply

确定可以PIP但还需要编译环境

error: Microsoft Visual C++ 10.0 is required (Unable to find vcvarsall.bat).



000 • 2015年08月24日 • Reply

能说的在具体些吗？看不懂啊！



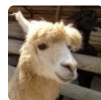
Xiaolan • 2015年08月24日 • Reply • 博主

具体是哪里呢？



000 • 2015年08月24日 • Reply

我用的是Windows系统，不知该如何操作，希望你能一步一步的教一下。



Xiaolan • 2015年08月24日 • Reply • 博主

在文章中更新了obfsproxy的windows版本..windows下客户端按照上面的就可以...



ben • 2015年09月01日 • Reply

有问题，我安装了python 3.4，并追加了PATH但，不论是使用你的zip文件解压出的obfsproxy.exe还是我自己下载torbrowser分离出obfsproxy.exe都无法执行。

The system cannot execute the specified program.

你到底是在什么环境下做的？

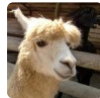
还有上面的linux的执行命令也有问题，参考openvpn的链接

<https://community.openvpn.net/openvpn/wiki/TrafficObfuscation>

在ubuntu下应该是这个样子：

```
obfsproxy --log-file=obfsproxy.log --log-min-severity=info obfs2 --dest=127.0.0.1:1194
```

```
--shared-  
secret=SBSB4444FANGBINXING4SBSBSBSBSBSB  
server 0.0.0.0:21194  
  
obfsproxy --log-file=obfsproxy.log --log-  
min-severity=info obfs2 --shared-  
secret=SBSB4444FANGBINXING4SBSBSBSBSBSB  
socks 127.0.0.1:9194
```



Xiaolan • 2015年09月01日 • Reply • 博主

我是直接从torbrowser 复制出来的...安装
py2.7试试呢?
那个命令行不对是因为wordpress自动将两
个-- 转换为- 导致无法运行



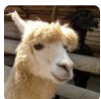
天天上 • 2015年08月24日 • Reply

站长，请问你知道csdn密码在哪里可以查看吗？



obfs • 2015年08月30日 • Reply

客户端错误。提示找不到pythondll，如何解决？



Xiaolan • 2015年09月01日 • Reply • 博主

已更新..忘记打包那几个支持库了...



Shelikhoo • 2015年09月01日 • Reply

博主现在自己架了一个服务器，大家可以用这个命令连接

```
obfsproxy scramblesuit client 127.0.0.1:2222 --dest 185.61.148.246:8080
```

```
--password FUCKFANGBINXINGHEXIJINPINGSBDASB
```

(文中的那个命令在linux下报错为

```
obfsproxy scramblesuit: error: argument mode: invalid choice: '\xe2\x80
```

```
\x93dest' (choose from 'server', 'ext_server', 'client', 'socks')
```

```
obfsproxy scramblesuit: error: argument listen_addr: Bad address
```

```
specification "--dest"
```

```
obfsproxy scramblesuit: error: one of the arguments --password
```

```
--password-file is required
```

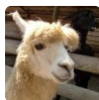
```
obfsproxy: error: unrecognized arguments: --dest 185.61.148.246:8080
```

```
)
```



Anonymous • 2015年09月02日 • Reply

直接用浏览器代理貌似不行啊，是ssh?openvpn？



Xiaolan • 2015年09月02日 • Reply • 博主

是SOCKS5代理..firefox可以直接设置...



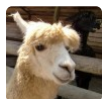
Shelikhoo • 2015年09月01日 • Reply

你的服务器可能会自动将两个 /-/- 转换为 /- 请注意这个问题，文章中的命令无法使用



Anonymous • 2015年09月01日 • Reply

BT sync的共享双方还是知道IP的啊，可以用代理（Tor等类型）下载吗？



Xiaolan • 2015年09月02日 • Reply • 博主

互相知道IP,但是可以用tor来隐匿...



Anonymous • 2015年09月02日 • Reply

有个问题就是，我用obfsproxy混淆ss流量，配置好了服务器和客户端的端口映射并启动了obfs，然而发现，服务器正常监听，客户端的ss也成功被obfs转发，但服务端和客户端两台机子却无法连接.....



Anonymous • 2015年09月02日 • Reply

经测试ssh可以使用，但出于未知原因，shadowsock混淆会出现服务器和客户端连接不上的蛋疼问题



Xiaolan • 2015年09月02日 • Reply • 博主

ss本来就是混淆过的,再次混淆反而多此一举...



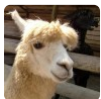
obfs • 2015年09月03日 • Reply

重起vps试试。我也混淆了ss,已成功。



123 • 2015年09月03日 • Reply

怎么安装python运行环境？第一步该如何操作，小白不懂。



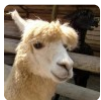
Xiaolan • 2015年09月03日 • Reply • 博主

到<https://python.org>下载符合操作系统的环境,安装即可..



Anonymous • 2015年09月06日 • Reply

用了好几天了，感觉有效果，但是好像存在内存泄漏。VPS 1G内存快要用完了。杀死obfsproxy之后正常。



Xiaolan • 2015年09月06日 • Reply • 博主

这个问题没遇到过：（



Anonymous • 2015年10月18日 • Reply

有内存泄漏,我也遇到了



Anonymous • 2015年09月07日 • Reply

客户端提示

2015-09-07 09:10:48,858 [WARNING] Obfsproxy (version: unknown) starting up.

2015-09-07 09:10:48,858 [ERROR]

#####

Do NOT rely on ScrambleSuit for strong security!

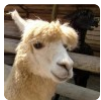
#####

Q1. 应该是已经连上你提供测试的服务器（谢谢），可是设置SwitchySharp，却打不开墙外的页面。会是什么问题？

Q2.obfsproxy 是否可以理解，单靠此就可在VPS搭建SOCKS5代理服务？

Q3.最后一个小问题。网络上大面积充斥非独享IP4的VPS，年租在3-5\$间，可否用这种VPS搭建代理服务器，SS或是obfs？

不胜感激



Xiaolan • 2015年09月07日 • Reply • 博主

A1. 有可能是DNS有问题,或者服务器线路质量不良...

A2. 不可以,只能作为服务的转发,需要搭建SOCKS5可以用dante-server等...

A3. 可以.. obfs/ss 均可...



Anonymous • 2015年09月09日 • Reply

CentOS6；安装完环境后尝试安装Ofbs，“成功”（ Successfully installed obfsproxy-0.2.13 ）但是同时提示（ Requirement already satisfied (use --upgrade to upgrade): setuptools in /usr/lib/python2.6/site-packages (from obfsproxy) ）；尝试启动Ofbs时发生错误，如下（部分），请博主予以指导；先致谢意。

Traceback (most recent call last):

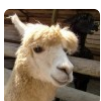
File "/usr/bin/obfsproxy", line 5, in
from pkg_resources import load_entry_point

File "/usr/lib/python2.6/site-packages/pkg_resources.py", line 2655, in
working_set.require(__requires__)

File "/usr/lib/python2.6/site-packages/pkg_resources.py", line 648, in require
needed = self.resolve(parse_requirements(requirements))

File "/usr/lib/python2.6/site-packages/pkg_resources.py", line 546, in resolve
raise DistributionNotFound(req)

pkg_resources.DistributionNotFound: argparse



Xiaolan • 2015年09月09日 • Reply • 博主

试试 pip install argparse

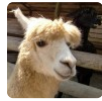
Anonymous • 2015年09月10日 • Reply

感谢博主的指导，查明是Py包的问题了，Obfs已经在服务端打



开。

想问：监听22的SSH端口后，本地Obfs客户端的该如何与SSH软件搭配使用？只看文章内容不甚明朗。



Xiaolan • 2015年09月11日 • Reply • 博主

本机PC运行

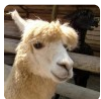
```
obfsproxy scramblesuit --dest 服务器IP:端口  
--password 密码 client 127.0.0.1:22222
```

之后用MyEnTunnel链接127.0.0.1:22222



Anonymous • 2015年09月09日 • Reply

不用ssh可以吗，能直接用squid吗？
服务器已经在国外了，直接http是不是会更快。



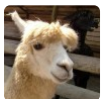
Xiaolan • 2015年09月09日 • Reply • 博主

可以...任何TCP的都可以



FUCKFANGBINXING • 2015年09月12日 • Reply

博主，用你提供的obfsproxy方案可以当Tor前置代理上网，但却无法直接给Chrome的自动代理设置上网(与Tor使用一样的前置127.0.0.1:22222, socks5), 不知道何原因？



Xiaolan • 2015年09月13日 • Reply • 博主

试试firefox呢..chrome使用系统的socks5,估计可能会有点不支持吧...



FUCKFANGBINXING • 2015年09月13日 • Reply

博主谢谢回复，我尝试过在FireFox上设置127.0.0.1:22222 socks5, 与chrome一样无法上网，倒是用作Tor的前置代理网速不错



Yuan • 2015年09月15日 • Reply

为什么用MyEnTunnel链接127.0.0.1:22222 会提示要输入密码？



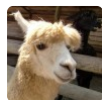
Xiaolan • 2015年09月15日 • Reply • 博主

输入SSH的密码...



yuan • 2015年09月16日 • Reply

博主，我是用你提供的公共帐号先用obfs连接，再用MyEnTunnel链接127.0.0.1:22222，根本就没有用ssh,怎么输入密码？127.0.0.1:22222不是本地监听的端口，哪有ssh帐号和密码？



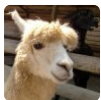
Xiaolan • 2015年09月18日 • Reply • 博主

公共帐号是SOCKS5代理，浏览器可以直接用....



ming • 2015年09月15日 • Reply

刚会用SSH翻墙，看不懂博主所写的，能否录个视频看看。



Xiaolan • 2015年09月15日 • Reply • 博主

文章已更新..包含了视频教程...

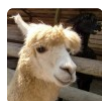


ming • 2015年09月17日 • Reply

谢谢！

我按着视频教程已经弄好了，但是没有流量啊，这是怎么回事？

还有，如果我用SSH翻墙，SSH账号里面有用户名，这又该怎么设置？



Xiaolan • 2015年09月18日 • Reply • 博主

用MyEnTunnel...

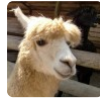
Anonymous • 2015年09月18日 • Reply

MyEnTunnel在哪里下载？我用BvSshClient-Inst



可以么？

我用BvSshClient-Inst可以翻墙，怎么和本教程的obfsproxy混淆使用，请说细一些。



Xiaolan • 2015年09月19日 • Reply • 博主

任何SSH客户端均可...就相当于你用SSH翻墙,但是服务器IP写本地的...



Anonymous • 2015年09月15日 • Reply

Shadowsocks很不稳定，不知有没有Shadowsocks的替代品啊？



Anonymous • 2015年09月15日 • Reply

可直接运行楼主微软网盘的exe文件，但连接速度非常慢，但这样的思路非常不错，谢谢你的扫盲科普，谢谢！

185.61.x.x 服务器沿途线路国外丢包非常严重，南方沿海电信mtr测试！

FUCKFANGBINXINGHEXIJINPINGSBDASB

这个密码真是好，方滨兴这个历史罪人，哪年一定要被人掘祖坟的！



Anonymous • 2015年09月16日 • Reply

好人做到底，能研究一下obfs4的该如何搭建和使用呢？
因为看到有obfs4的代理！



Anonymous • 2015年09月21日 • Reply

obfs4现在还不能单独拿出来用，只能用在tor里面。



surveillance104 • 2015年09月21日 • Reply

樓主您好

windows上版本已經運行成功，但是我這裡有一個很大的問題

在Mac版本上的TorBrowser程序打開後，並沒有發現obfsproxy.exe（廢話？然而只是看到了obfsproxy.bin

已用過open命令但是mac只是默認把bin解壓縮掉了 懇請樓主想出mac版本運行客戶端的方法

ps:

Anonymous • 2015年09月02日 • Reply

经测试ssh可以使用，但出于未知原因，shadowsock混淆会出现服务器和客户端连接不上的蛋疼问题

Xiaolan • 2015年09月02日 • Reply • 博主

ss本来就是混淆过的,再次混淆反而多此一举...

這個我有一些個人意見，因為gfw已經有深度包探測，加上ss最近開發者已經喝茶 我擔心ss的破牆能力速度已經不行。同時已有兩個博客以給出質疑：<https://typeblog.net/tech/2015/08/18/obfourscating-shadowsocks-with-obfs4.html>

這個是Github上面的提出ss端口的問題<https://github.com/shadowsocks/shadowsocks/issues/410>

這個是混合ss與ss端口的的方法：<http://www.devchen.com/blog/coding/Linux/20150825-shadowsocks-obfs/>

還有的是Ubuntu在prism-break網站上已經被懷疑裝有後門具體連結在這裏：

<https://prism-break.org/zh-CN/categories/gnu-linux/#operating-systems>

Canonical's Ubuntu本站并不推荐，因为其默认配置存在亚马逊广告和数据泄漏漏洞如果你已经用上了Ubuntu，你可以从Fix Ubuntu网站获得亡羊补牢的建议措施。

<https://www.eff.org/deeplinks/2012/10/privacy-ubuntu-1210-amazon-ads-and-data-leaks>

如樓主有時間請樓主解答一下我的問題吧，謝啦orz？



surveillance104 • 2015年09月21日 • Reply

或許可以用wine軟件來運行windows版本上的obfsproxy版本？我或許應該測試一下

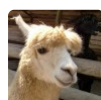


surveillance104 • 2015年09月21日 • Reply

之前已經有兩個老外已經問過我類似的問題。。。連結如下

<https://tor.stackexchange.com/questions/3793/tor-browser-bundle-on-mac-how-to-run-obfsproxy>

<https://lists.torproject.org/pipermail/tor-talk/2014-August/034347.html>



Xiaolan • 2015年09月23日 • Reply • 博主

看来已经有答案了嘛；)



Xiaolan • 2015年09月23日 • Reply • 博主

这个评论被误判为SPAM了,已人工恢复;)

问题1:mac版本下尝试在terminal输入

```
chmod +x obfsproxy.bin  
./obfsproxy.bin --help
```

看能否运行呢..

问题2:scramblesuit已经提供了一层混淆,GFW所监测到的只能是scramblesuit混淆以后的...

在Torproject.org的[研究报告](#)中也提到了通过scramblesuit的密码可以抗探测...

Luckily, we now have several pluggable transports that can defend against active probing. ScrambleSuit and its successor, obfs4, defend against probing attacks by relying on a shared secret that is distributed out of band.

问题3:不建议用原版的ubuntu,可以用Kubuntu等衍生版本...

;))



Anonymous • 2015年09月25日 • Reply

話說回來樓主的網站居然是不支持js情況下就能回覆讓我感到很欣慰。。。。

咳咳，說正經事。

感謝樓主對我的問題解答，之後我嘗試了對於obfsproxy.bin的操作，但是還是有問題

問題一：

之前樓主的操作已經試過，不過不管是python3.50還是python2.7.10均提示出一個錯誤：

Interpreter not initialized (version mismatch?)

編譯程序並沒有初始化（版本不匹配？）

是操作第二個命令“./obfsproxy.bin --help”的時候出現的

基於wine的辦法，這幾天一直拼命下載xcode所以。。。。

問題二：

樓主可能搞錯了我的意思，我說的意思是因為shadowsocks它的aes-256-cfb已經被牆可以達到深度探測包檢測的程度（當然現在也有不少人懷疑這點是否牆能達到檢測，需要用obfsproxy的scramblesuit或obfs4進行進一步的加密才能不被探測到 可能樓主的意思是shadowsocks已有加密方式並不需要二次加密，

(當然也有可能是我意思搞錯了orz)，或者是有了obfsproxy不需要shadowsocks進行加密，我不知道樓主上次說的是前者還是後者的意思。

問題三：這個方面我會去了解的ubuntu，只不過我希望樓主能夠把ubuntu以後被後門的消息說出來一下讓大家知道orz（沒有出風頭的意思

望請樓主解答;)？



surveillance104 • 2015年09月26日 • Reply

好吧我不知道Github上面的這個辦法能否行得通

<https://github.com/Homebrew/homebrew/issues/18319>

Check if you have any remains of pip/distribute /setuptools intalled in /Library/Python/2.7/site-packages or in ~/Library/Python/2.7/site-packages. Try to remove /usr/local/lib/python2.7 completely.

There brew update, brew doctor and hopefully brew install python



surveillance104 • 2015年09月26日 • Reply

仍舊提示上一個錯誤，看來這個解決辦法並不是行得通



surveillance104 • 2015年09月26日 • Reply

好吧，我才知道brew是OS X的安裝包軟件。。。網址：brew.sh

然而我已經:brew doctor brew update brew install python 然而在運行樓主提示的命令時還是會提示錯誤信息。。。。 這個辦法也不行orz



surveillance104 • 2015年09月26日 • Reply

樓主，我說明一下新的情況orz

已經安裝了brew安裝包 但之後執行 brew doctor brew update brew install python三條命令後（原來的python使用cleanmymac卸載掉的）還是會提示版本不匹配的信息

看來還得調試



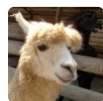
surveillance104 • 2015年09月26日 • Reply

另外一個連結https://www.nsnam.org/wiki/Python_bindings說明這是多個版本導致python混淆的錯誤，不過當我提示運行：
Check if there is a "libpythonX.Y.dylib" in /opt/local/lib by executing 'ls -l /opt/local/lib/libpython*' in a terminal.
如果想檢查libpythonX.Y.dylib文件在 /opt/local/lib的話，
請在terminal執行“ls -l /opt/local/lib/libpython”命令
然而terminal則提示“No such file or directory”
後來我在finder運行shift + ⌘+G找文件夾的時候也找不到文件夾



surveillance104 • 2015年09月26日 • Reply

樓主，我說明一下新的情況orz
已經安裝了brew安裝包 但之後執行 brew doctor brew update brew install python三條命令後
（原來的python使用cleanmymac卸載掉的）還是會提示版本不匹配的信息
看來還得調試



Xiaolan • 2015年09月26日 • Reply • 博主

问题1:
由于我的mac一直用的win7且密码忘了,暂时没有办法测试..不过在网上找到了一篇文章功参考;)
<https://deekayen.net/mac-viscosity-obfsproxy-configuration>

```
ruby -e "$(curl -fsSL \nhttps://raw.githubusercontent.com/Homebrew/install/master/install)"\nbrew install python\npip install obfsproxy
```

通过python-pip方式安装obfsproxy后使用....

问题2:
我的意思是有了obfsproxy不需要shadowsocks進行加密

orz ;)

问题3:

ubuntu已经被确认有隐私泄漏的风险了....而且各类IT新闻类网站也有报道...我就懒得提了;)

另：多谢捧场



Anonymous • 2016年01月13日 • Reply

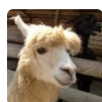
Hi, guys,

i fixed this with the following steps. enjoy it.

```
$ vim /Applications/TorBrowser.app/TorBrowser  
/Tor/PluggableTransports/obfsproxy.bin
```

change line 1:

```
- #!/usr/bin/env python  
+#!/usr/bin/env python2.6
```



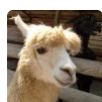
Xiaolan • 2016年02月01日 • Reply • 博主

thanks:)



surveillance104 • 2015年09月25日 • Reply

題外話：什麼時候虛擬機的話具體講解一下whonix雙虛擬機，這樣讓大家匿名的姿?勢更多一些（當我說了廢話吧



Xiaolan • 2015年09月26日 • Reply • 博主

正有计划写Whonix的扫盲；)



surveillance104 • 2015年09月26日 • Reply

有好幾位老外（和上次一樣orz 也提到了這個問題

<http://lists.reporforge.org/pipermail/tools/2011-February/003943.html>

<http://www.webr2.com/what-causes-python-interpreter-not-initialized-version-mismatch-error/>

<https://code.activestate.com/lists/python-list/434634/>

<https://lists.gnu.org/archive/html/discuss-gnuradio/2012-09>

[/msg00088.html](#) "port select python python2.7"命令無效

<http://wiki.tiker.net/PyCuda/Installation>

[/Mac#Fatal_Python_error:_Interpreter_not_initialized_.28version_mismatch](#)

在這個連結中，嘗試了：

```
% install_name_tool -change /System/Library/Frameworks
/Python.framework/Versions/2.6/Python /Library/Frameworks
/Python.framework/Versions/2.6/Python libboost_python.dylib
```

命令

然而terminal卻提示no such job.....



surveillance104 • 2015年09月26日 • Reply

樓主，我說明一下新的情況orz

已經安裝了brew安裝包 但之後執行 brew doctor brew update
brew install python三條命令後

（原來的python使用cleanmymac卸載掉的）還是會提示版本不
匹配的信息

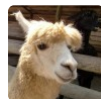


surveillance104 • 2015年09月26日 • Reply

抱歉我剛才發的信息太多了，下次如果還有問題我盡量
發郵件？，我很抱歉。。

這個問題的最新消息（第一個問題）

brew安裝的python是python3.50和python2.7.10，然而
還是不行，這時否能說明提示版本不匹配的信息並不是
正確的有效信息??



Xiaolan • 2015年09月26日 • Reply • 博主

尝试下这样安装brew呢？

```
$ ruby -e "$(curl -fsSL
```

```
https://raw.githubusercontent.com/Homebrew/install/master/install)"
```



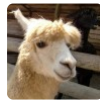
Anonymous • 2015年09月30日 • Reply

看我郵件 orz



surveillance104 • 2015年09月30日 • Reply

郵件已經發過去了，樓主大人請查收orz



Xiaolan • 2015年09月30日 • Reply • 博主

回复到gmail了..sigaint发送中文是乱码...:)



llyloo • 2015年09月23日 • Reply

你好博主，我按照你的教程在服务器上配置好了obfsproxy，协议是scramblesuit，然后测试的时候用不了，我打开了Debug日志输入，发现两边都是有收到数据的，服务器上的日志：

```
2015-09-22 13:02:46,219 [DEBUG] fact_s_0x2d379e0: New connection from [scrubbed]:45138.
```

```
2015-09-22 13:02:46,219 [DEBUG] Initialising ScrambleSuit.
```

```
2015-09-22 13:02:46,219 [INFO] Attempting to load the server's state file from `/root/.obfs/scramblesuit/server_state.cpickle'.
```

```
2015-09-22 13:02:46,221 [DEBUG] Switching to state ST_WAIT_FOR_AUTH.
```

```
2015-09-22 13:02:46,221 [DEBUG] Initialising AES-CTR instance.
```

```
2015-09-22 13:02:46,221 [DEBUG] Initialising AES-CTR instance.
```

```
2015-09-22 13:02:46,222 [INFO] Starting factory
```

```
2015-09-22 13:02:46,222 [DEBUG] fact_c_0x2d4a0e0: Client factory started connecting.
```

```
2015-09-22 13:02:46,222 [DEBUG] conn_0x2d3f5d0: connectionMade (server): Setting it as downstream on our circuit.
```

```
2015-09-22 13:02:46,222 [DEBUG] circ_0x2d4a098: Setting downstream connection (conn_0x2d3f5d0).
```

```
2015-09-22 13:02:46,223 [DEBUG] fact_c_0x2d4a0e0: Connection failed (Connection was refused by other side: 111: Connection refused.).
```

```
2015-09-22 13:02:46,223 [DEBUG] circ_0x2d4a098: Tearing down circuit.
```

```
2015-09-22 13:02:46,223 [DEBUG] conn_0x2d3f5d0: Closing connection.
```

```
2015-09-22 13:02:46,223 [INFO] Stopping factory
```

```
2015-09-22 13:02:46,223 [DEBUG] conn_0x2d3f5d0: Connection was lost (Connection was closed cleanly.).
```

客户端的日志：

```
2015-09-23 01:02:45,219 [DEBUG] fact_s_0x26a36c0: New connection from [scrubbed]:9566.
```

```
2015-09-23 01:02:45,220 [DEBUG] Initialising ScrambleSuit.
```

```
2015-09-23 01:02:45,220 [DEBUG] Switching to state ST_WAIT_FOR_AUTH.
```

2015-09-23 01:02:45,223 [DEBUG] Initialising AES-CTR instance.
2015-09-23 01:02:45,223 [DEBUG] Initialising AES-CTR instance.
2015-09-23 01:02:45,226 [DEBUG] Dumping probability distribution.
2015-09-23 01:02:45,226 [DEBUG] P(1134) = 0.011
2015-09-23 01:02:45,227 [DEBUG] P(156) = 0.045
2015-09-23 01:02:45,229 [DEBUG] P(1307) = 0.025
2015-09-23 01:02:45,230 [DEBUG] Dumping probability distribution.
2015-09-23 01:02:45,232 [DEBUG] P(0.00769573128549) = 0.197
2015-09-23 01:02:45,233 [DEBUG] P(0.00644270539992) = 0.235
2015-09-23 01:02:45,234 [DEBUG] P(0.000825783278846) = 0.117
2015-09-23 01:02:45,236 [DEBUG] P(0.00147728386844) = 0.016
2015-09-23 01:02:45,237 [DEBUG] P(4.76719791126e-05) = 0.434
2015-09-23 01:02:45,240 [INFO] Starting factory
2015-09-23 01:02:45,240 [DEBUG] fact_c_0x26b3210: Client factory started connecting.
2015-09-23 01:02:45,242 [DEBUG] conn_0x26ab690: connectionMade (client): Setting it as upstream on our circuit.
2015-09-23 01:02:45,243 [DEBUG] circ_0x26b31c0: Setting upstream connection (conn_0x26ab690).
2015-09-23 01:02:45,244 [DEBUG] conn_0x26ab690: Incomplete circuit; cached 3 bytes.
2015-09-23 01:02:45,457 [DEBUG] conn_0x26ab770: connectionMade (client): Setting it as downstream on our circuit.
2015-09-23 01:02:45,457 [DEBUG] circ_0x26b31c0: Setting downstream connection (conn_0x26ab770).
2015-09-23 01:02:45,457 [DEBUG] circ_0x26b31c0: Circuit completed.
2015-09-23 01:02:45,459 [DEBUG] Attempting to read master key and ticket from file `session_ticket.yaml'.
2015-09-23 01:02:45,459 [DEBUG] Opening `session_ticket.yaml' for reading.
2015-09-23 01:02:45,461 [INFO] Found no ticket for bridge `IPv4Address(TCP, 'x.x.x.x', xxxx)'.
2015-09-23 01:02:45,461 [DEBUG] No session ticket to redeem. Running UniformDH.
2015-09-23 01:02:45,463 [DEBUG] Creating UniformDH handshake message.
2015-09-23 01:02:45,509 [DEBUG] conn_0x26ab770: Writing 859 bytes.
2015-09-23 01:02:45,522 [DEBUG] circ_0x26b31c0: upstream: Received 3 bytes.
2015-09-23 01:02:45,522 [DEBUG] Buffered 3 bytes of outgoing data.
2015-09-23 01:02:45,671 [DEBUG] conn_0x26ab770: Connection was lost (Connection was closed cleanly.).

2015-09-23 01:02:45,673 [DEBUG] conn_0x26ab770: Closing connection.
2015-09-23 01:02:45,673 [DEBUG] circ_0x26b31c0: Tearing down circuit.
2015-09-23 01:02:45,674 [DEBUG] conn_0x26ab690: Closing connection.
2015-09-23 01:02:45,676 [INFO] Stopping factory
2015-09-23 01:02:45,677 [DEBUG] conn_0x26ab690: Connection was lost
(Connection was closed cleanly.).

求解，谢谢



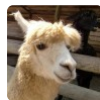
Xiaolan • 2015年09月23日 • Reply • 博主

检查下被混淆端的端口是否工作正常呢？



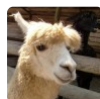
llyloo • 2015年09月25日 • Reply

博主能否把我这层删除，我问题已经解决了，但是看了一下发出来的日志里面居然有我vps的ip。。不好意思



Xiaolan • 2015年09月26日 • Reply • 博主

已经隐去IP信息...



Xiaolan • 2015年09月26日 • Reply • 博主

顺便..能否提供下解决方法呢？



llyloo • 2015年09月27日 • Reply

我按照[https://www.youtube.com](https://www.youtube.com/watch?v=sTjay0l5IWU&list=LLPTfFyadcrMR8UPzBsdbT4Q&index=1)

/watch?v=sTjay0l5IWU&

list=LLPTfFyadcrMR8UPzBsdbT4Q&index=1的
流程在vps上安装了dante，然后一开始的配置文
件是这样的：

logoutput: syslog

internal: venet0:0 port = 23468

external: venet0:0

external.rotation: same-same

method: username none

#user.privileged: proxy

user.notprivileged: nobody

client pass {

from: 0.0.0.0/0 port 1-65535 to: 0.0.0.0/0

```
}
client block {
from: 0.0.0.0/0 to: 0.0.0.0/0
}
pass {
from: 0.0.0.0/0 to: 0.0.0.0/0
protocol: tcp udp
}
block {
from: 0.0.0.0/0 to: 0.0.0.0/0
}
```

然后我测试直接用sock5协议连接是可以的，但是obfsproxy混淆之后就连不上。

后面我把配置文件改成这样：

```
logoutput: syslog
internal: 127.0.0.1 port = 23468
external: venet0:0
external.rotation: same-same
method: username none
#user.privileged: proxy
user.notprivileged: nobody
client pass {
from: 0.0.0.0/0 port 1-65535 to: 0.0.0.0/0
}
client block {
from: 0.0.0.0/0 to: 0.0.0.0/0
}
pass {
from: 0.0.0.0/0 to: 0.0.0.0/0
protocol: tcp udp
}
block {
from: 0.0.0.0/0 to: 0.0.0.0/0
}
```

惊奇地发现就可以了，问题解决。原理不明，我是Google了一下然后看了一堆文章之后乱改试出来的。

最后为了安全我改成这样子：

```
logoutput: syslog
internal: 127.0.0.1 port = 23468
external: venet0:0
external.rotation: same-same
```

```
method: username none
#user.privileged: proxy
user.notprivileged: nobody
client pass {
  from: 0.0.0.0/0 port 1-65535 to: 0.0.0.0/0
}
client block {
  from: 0.0.0.0/0 to: 0.0.0.0/0
}
pass {
  from: 127.0.0.0/0 to: 0.0.0.0/0
  protocol: tcp udp
}
block {
  from: 0.0.0.0/0 to: 0.0.0.0/0
}
貌似这样就不可以直接从外面直接使用sock5代理了，只能通过obfsproxy连接。
```



ljlou • 2015年09月27日 • Reply

我解决的方案被吞了。。。请博主恢复一下，谢谢



xclimbing • 2015年09月23日 • Reply

试了很多次，无论是混淆ssh端口（22），还是混淆ShadowSocks端口，都不能正常工作，在使用chrome连接时，vps端会不断提示错误信息：
[WARNING] Could not verify the authentication message's HMAC.

这证明obfsproxy的客户端（win端）已经跟vps(CentOS 6.7）的服务端连接上了，只不过连接不能正常工作。

如果不混淆，ssh和SS工作都是正常的。

我用google搜索这条错误信息，只是搜索到了github上scramblesuit 的相关源程序，源程序看不明白什么意思。

请问 @XiaoLan这个问题如何解决？



Xiaolan • 2015年09月23日 • Reply • 博主

确认下密码是否正确呢？



fish • 2016年04月24日 • Reply

这个问题是由于vps没有虚拟内存造成的。我买了一个vps, 没有虚拟内存，也遇到了此问题。换个有虚拟内存的 vps,此问题就消失了。



xclimbing • 2015年09月23日 • Reply

我把我操作的详细步骤列在这里，看看能不能找出问题所在。

一、首先是关于vps上相关组件的安装，我是完全按照你上面的教程操作的。我的vps的系统是centos 6.7。安装成功后，是下面的状况：

```
[root@vpn ~]# obfsproxy
usage: obfsproxy [-h] [-v] [--log-file LOG_FILE]
[--log-min-severity {error,warning,info,debug}] [--no-log]
[--no-safe-logging] [--data-dir DATA_DIR] [--proxy PROXY]
{obfs3,obfs2,dummy,managed,b64,scramblesuit} ...
obfsproxy: error: too few arguments
```

二、关于obfsproxy混淆的试验过程

为了试验混淆效果，我在vps上安装了socks5服务（这个肯定是被墙的），socks的监听端口是9080，我在IE中设置代理为这个服务，第一次是可以访问网站的，第二次时就被墙重置链接了。

然后我用obfsproxy混淆这个socks5的服务，vps端运行的命令行为：

```
obfsproxy --log-file obfsproxy_socks.log --log-min-severity debug --data-dir
/tmp/obfs/socks scramblesuit --password
FUCKGFWFUCKFANGBINXINGFBX4SBDASB --dest 127.0.0.1:9080 server
0.0.0.0:9180
```

在Windows端我运行的命令行为：

```
obfsproxy.exe --log-file obfsproxy_socks.log --log-min-severity debug
scramblesuit --password FUCKGFWFUCKFANGBINXINGFBX4SBDASB
--dest %vps_ip%:9180 client 127.0.0.1:9080
```

然后我将IE的代理服务器设置为：127.0.0.1:9080(socks代理)，再次访问网站。然后从vps端和windows端的日志文件中得到如下日志：

VPS端日志：

```
[root@vpn ~]# more obfsproxy_socks.log
2015-09-23 12:15:45,057 [WARNING] Obfsproxy (version: 0.2.13) starting
up.
2015-09-23 12:15:45,057 [DEBUG] argv: ['/usr/bin/obfsproxy', '--log-file',
'obfsproxy_socks.log', '--log-min-severity', 'debug', '--data-dir', '/tmp/obfs
/socks', 'scramblesuit',
'--password', 'FUCKGFWFUCKFANGBINXINGFBX4SBDASB', '--dest',
'127.0.0.1:9080', 'server', '0.0.0.0:9180']
2015-09-23 12:15:45,057 [DEBUG] args: Namespace(data_dir='/tmp
/obfs/socks', dest=('127.0.0.1', 9080), ext_cookie_file=None, listen_addr=
('0.0.0.0', 9180), log_file='obfsproxy_so
cks.log', log_min_severity='debug', mode='server', name='scramblesuit',
no_log=False, no_safe_logging=False, proxy=None,
uniformDHSecret='FUCKGFWFUCKFANGBINXINGFBX4SBDASB', vali
dation_function=<bound method type.validate_external_mode_cli of >)
2015-09-23 12:15:45,058 [ERROR]

#####
Do NOT rely on ScrambleSuit for strong security!
#####

2015-09-23 12:15:45,058 [DEBUG] Setting the state location to `/tmp/obfs
/socks/scramblesuit/'.
2015-09-23 12:15:45,058 [INFO] Writing server password to file `/tmp/obfs
/socks/scramblesuit/server_password'.
2015-09-23 12:15:45,076 [INFO] StaticDestinationServerFactory starting on
9180
2015-09-23 12:15:45,077 [INFO] Starting factory
2015-09-23 12:15:45,077 [DEBUG] fact_s_0x1456758: Starting up static
destination server factory.
2015-09-23 12:15:45,077 [INFO] Launched 'server' listener at
'[scrubbed]:9180' for transport 'scramblesuit'.
2015-09-23 12:18:01,016 [DEBUG] fact_s_0x1456758: New connection from
[scrubbed]:28045.
2015-09-23 12:18:01,016 [DEBUG] Initialising ScrambleSuit.
2015-09-23 12:18:01,016 [INFO] Attempting to load the server's state file
from `/tmp/obfs/socks/scramblesuit/server_state.cpickle'.
2015-09-23 12:18:01,023 [DEBUG] Switching to state
ST_WAIT_FOR_AUTH.
2015-09-23 12:18:01,024 [DEBUG] Initialising AES-CTR instance.
2015-09-23 12:18:01,024 [DEBUG] Initialising AES-CTR instance.
2015-09-23 12:18:01,024 [INFO] Starting factory
```

2015-09-23 12:18:01,024 [DEBUG] fact_c_0x1460638: Client factory started connecting.

2015-09-23 12:18:01,025 [DEBUG] conn_0x1400fd0: connectionMade (server): Setting it as downstream on our circuit.

2015-09-23 12:18:01,025 [DEBUG] circ_0x14605f0: Setting downstream connection (conn_0x1400fd0).

2015-09-23 12:18:01,035 [DEBUG] conn_0x1462350: connectionMade (server): Setting it as upstream on our circuit.

2015-09-23 12:18:01,035 [DEBUG] circ_0x14605f0: Setting upstream connection (conn_0x1462350).

2015-09-23 12:18:01,035 [DEBUG] circ_0x14605f0: Circuit completed.

2015-09-23 12:18:01,045 [DEBUG] conn_0x1400fd0: dataReceived called without a reason.

2015-09-23 12:18:01,124 [DEBUG] circ_0x14605f0: downstream: Received 442 bytes.

2015-09-23 12:18:01,124 [DEBUG] Attempting to decrypt and verify ticket.

2015-09-23 12:18:01,124 [DEBUG] Attempting to extract the remote machine's UniformDH public key out of 442 bytes of data.

2015-09-23 12:18:01,124 [DEBUG] Successfully located the mark.

2015-09-23 12:18:01,125 [DEBUG] HMAC invalid. Trying next epoch value.

2015-09-23 12:18:01,125 [DEBUG] HMAC invalid. Trying next epoch value.

2015-09-23 12:18:01,125 [DEBUG] HMAC invalid. Trying next epoch value.

2015-09-23 12:18:01,125 [WARNING] Could not verify the authentication message's HMAC.

2015-09-23 12:18:01,126 [DEBUG] Authentication unsuccessful so far. Waiting for more data.

2015-09-23 12:18:01,607 [DEBUG] fact_s_0x1456758: New connection from [scrubbed]:17772.

2015-09-23 12:18:01,607 [DEBUG] Initialising ScrambleSuit.

2015-09-23 12:18:01,607 [INFO] Attempting to load the server's state file from `/tmp/obfs/socks/scramblesuit/server_state.cpickle'.

2015-09-23 12:18:01,609 [DEBUG] Switching to state ST_WAIT_FOR_AUTH.

2015-09-23 12:18:01,609 [DEBUG] Initialising AES-CTR instance.

2015-09-23 12:18:01,609 [DEBUG] Initialising AES-CTR instance.

2015-09-23 12:18:01,609 [INFO] Starting factory

2015-09-23 12:18:01,610 [DEBUG] fact_c_0x1468e18: Client factory started connecting.

2015-09-23 12:18:01,610 [DEBUG] conn_0x1462710: connectionMade (server): Setting it as downstream on our circuit.

2015-09-23 12:18:01,610 [DEBUG] circ_0x1468dd0: Setting downstream connection (conn_0x1462710).

```
2015-09-23 12:18:01,611 [DEBUG] conn_0x1462850: connectionMade
(server): Setting it as upstream on our circuit.
2015-09-23 12:18:01,611 [DEBUG] circ_0x1468dd0: Setting upstream
connection (conn_0x1462850).
2015-09-23 12:18:01,611 [DEBUG] circ_0x1468dd0: Circuit completed.
2015-09-23 12:18:01,621 [DEBUG] conn_0x1462710: dataReceived called
without a reason.
2015-09-23 12:18:01,717 [DEBUG] circ_0x1468dd0: downstream: Received
1451 bytes.
2015-09-23 12:18:01,718 [DEBUG] Attempting to decrypt and verify ticket.
2015-09-23 12:18:01,718 [DEBUG] Attempting to extract the remote
machine's UniformDH public key out of 1451 bytes of data.
2015-09-23 12:18:01,718 [DEBUG] Successfully located the mark.
2015-09-23 12:18:01,718 [DEBUG] HMAC invalid. Trying next epoch value.
2015-09-23 12:18:01,719 [DEBUG] HMAC invalid. Trying next epoch value.
2015-09-23 12:18:01,719 [DEBUG] HMAC invalid. Trying next epoch value.
2015-09-23 12:18:01,719 [WARNING] Could not verify the authentication
message's HMAC.
2015-09-23 12:18:01,719 [DEBUG] Authentication unsuccessful so far.
Waiting for more data.
```

Windows端日志:

```
2015-09-23 16:19:59,858 [WARNING] Obfsproxy (version: unknown) starting
up.
2015-09-23 16:19:59,858 [DEBUG] argv: ['obfsproxy.exe', '--log-file',
'obfsproxy_socks.log', '--log-min-severity', 'debug', 'scramblesuit',
'--password', 'FUCKGFWFUCKFANGBINXINGFBX4SBDASB', '--dest',
'%vps_ip%:9180', 'client', '127.0.0.1:9080']
2015-09-23 16:19:59,858 [DEBUG] args: Namespace(data_dir=None,
dest=('%vps_ip%', 9180), ext_cookie_file=None, listen_addr=('127.0.0.1',
9080), log_file='obfsproxy_socks.log', log_min_severity='debug',
mode='client', name='scramblesuit', no_log=False, no_safe_logging=False,
proxy=None,
uniformDHSecret='FUCKGFWFUCKFANGBINXINGFBX4SBDASB',
validation_function=<bound method type.validate_external_mode_cli of >)
2015-09-23 16:19:59,858 [ERROR]
```

```
#####
Do NOT rely on ScrambleSuit for strong security!
#####
```

```
2015-09-23 16:19:59,858 [INFO] StaticDestinationServerFactory starting on
```

9080

2015-09-23 16:19:59,858 [INFO] Starting factory

2015-09-23 16:19:59,858 [DEBUG] fact_s_0xf9bad0: Starting up static destination server factory.

2015-09-23 16:19:59,858 [INFO] Launched 'client' listener at '[scrubbed]:9080' for transport 'scramblesuit'.

2015-09-23 16:20:45,655 [DEBUG] fact_s_0xf9bad0: New connection from [scrubbed]:2274.

2015-09-23 16:20:45,655 [DEBUG] Initialising ScrambleSuit.

2015-09-23 16:20:45,655 [DEBUG] Switching to state ST_WAIT_FOR_AUTH.

2015-09-23 16:20:45,655 [DEBUG] Initialising AES-CTR instance.

2015-09-23 16:20:45,655 [DEBUG] Initialising AES-CTR instance.

2015-09-23 16:20:45,655 [DEBUG] Dumping probability distribution.

2015-09-23 16:20:45,671 [DEBUG] P(1169) = 0.807

2015-09-23 16:20:45,671 [DEBUG] P(377) = 0.187

2015-09-23 16:20:45,671 [DEBUG] Dumping probability distribution.

2015-09-23 16:20:45,671 [DEBUG] P(0.00347823032987) = 0.129

2015-09-23 16:20:45,671 [DEBUG] P(0.00427382308033) = 0.035

2015-09-23 16:20:45,671 [DEBUG] P(0.00636557018606) = 0.039

2015-09-23 16:20:45,671 [DEBUG] P(0.00599017665133) = 0.065

2015-09-23 16:20:45,671 [DEBUG] P(0.00550654872604) = 0.717

2015-09-23 16:20:45,671 [INFO] Starting factory

2015-09-23 16:20:45,671 [DEBUG] fact_c_0xf9cf08: Client factory started connecting.

2015-09-23 16:20:45,671 [DEBUG] conn_0xf92d30: connectionMade (client): Setting it as upstream on our circuit.

2015-09-23 16:20:45,671 [DEBUG] circ_0xf9cee0: Setting upstream connection (conn_0xf92d30).

2015-09-23 16:20:45,671 [DEBUG] conn_0xf92d30: Incomplete circuit; cached 3 bytes.

2015-09-23 16:20:45,812 [DEBUG] conn_0xf929b0: connectionMade (client): Setting it as downstream on our circuit.

2015-09-23 16:20:45,812 [DEBUG] circ_0xf9cee0: Setting downstream connection (conn_0xf929b0).

2015-09-23 16:20:45,812 [DEBUG] circ_0xf9cee0: Circuit completed.

2015-09-23 16:20:45,812 [DEBUG] Attempting to read master key and ticket from file `session_ticket.yaml'.

2015-09-23 16:20:45,812 [DEBUG] Opening `session_ticket.yaml' for reading.

2015-09-23 16:20:45,812 [INFO] Found no ticket for bridge `IPv4Address(TCP, '%vps_ip%', 9180)'.

```
2015-09-23 16:20:45,812 [DEBUG] No session ticket to redeem. Running
UniformDH.
2015-09-23 16:20:45,812 [DEBUG] Creating UniformDH handshake
message.
2015-09-23 16:20:45,937 [DEBUG] conn_0xf929b0: Writing 442 bytes.
2015-09-23 16:20:45,953 [DEBUG] circ_0xf9cee0: upstream: Received 3
bytes.
2015-09-23 16:20:45,953 [DEBUG] Buffered 3 bytes of outgoing data.
2015-09-23 16:20:46,250 [DEBUG] fact_s_0xf9bad0: New connection from
[scrubbed]:2276.
2015-09-23 16:20:46,250 [DEBUG] Initialising ScrambleSuit.
2015-09-23 16:20:46,250 [DEBUG] Switching to state
ST_WAIT_FOR_AUTH.
```

在上面的日志和命令行中，%vps_ip%代理我的VPS的IP地址，为了安全，这里隐去。

请看一下问题出在哪里？谢谢。



Xiaolan • 2015年09月24日 • Reply • 博主

服务器端这样试试呢

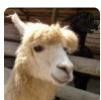
```
obfsproxy --data-dir ~/.obfs/ scramblesuit --dest 127.0.0.1:9080
--password SBSB4444FANGBINXING4SBSBSBSBSBSB server
0.0.0.0:9180
```

感觉像是--data-dir的问题导致可能的认证失败....



Nagi • 2015年09月24日 • Reply

博主知道怎么在android上的orbot设置自己搭建的obfsproxy嘛，电脑上已经用这种方法去混淆shadowsocks了，但是我在手机上用的也不少，怎么设置才能用同样的方式使用呢？



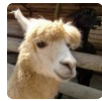
Xiaolan • 2015年09月24日 • Reply • 博主

安卓上orbot有meekbridge...手机上用meek足够了....



Nagi • 2015年09月24日 • Reply

用meek的话就不用自己搭的SS了？



Xiaolan • 2015年09月24日 • Reply • 博主
恩



horic • 2015年09月24日 • Reply

我看到有个别人维护的shadowsocks windows客户端服务器选项有个obfs选项，这个是不是就是相当于obfsproxy的客户端呢



surveillance104 • 2015年10月27日 • Reply

乃說的應該是現在流行的shadowsocks-rss版本吧。
這裡面的obfs應該是渾穀的意味，（並不是使用obfsproxy的技術），
只是借了obfs的渾穀的意思，這個shadowsocks的渾穀技術是作者本人製作的。orz



electroun • 2015年09月25日 • Reply

按照博主设置成功 但是过一段时间就会报错
重启之后再设置仍然报错
见下 请博主帮忙看一下是什么原因 怎么解决 多谢

[CRITICAL] Unhandled Error

Traceback (most recent call last):

File "/usr/local/lib/python2.7/site-packages/twisted/python/log.py", line 84, in callWithContext

return context.call({ILogContext: newCtx}, func, *args, **kw)

File "/usr/local/lib/python2.7/site-packages/twisted/python/context.py", line 118, in callWithContext

return self.currentContext().callWithContext(ctx, func, *args, **kw)

File "/usr/local/lib/python2.7/site-packages/twisted/python/context.py", line 81, in callWithContext

return func(*args,**kw)

File "/usr/local/lib/python2.7/site-packages/twisted/internet/posixbase.py", line 597, in _doReadOrWrite

why = selectable.doRead()



--- ---

File "/usr/local/lib/python2.7/site-packages/twisted/internet/tcp.py", line 1067, in doRead

protocol = self.factory.buildProtocol(self._buildAddr(addr))

File "/usr/local/lib/python2.7/site-packages/obfsproxy/network/network.py", line 380, in buildProtocol

circuit = Circuit(self.transport_class())



2016年05月01日 星期日 04:48 下午

希望保护自己的隐私，尤其不想用天朝的网。

翻墙路由器方案

目标: 让路由器透明翻墙，所有的PC/ipad不需额外设置，所有流量*强制*走翻墙通道，即使通道不通也不去碰“有毒”的墙内网。方案尽量开源安全可靠，愿意折腾。使用起来应该感觉和在海外上网一样。*不碰“有毒”的墙内网*

需要:

private server (VPS) 私用比公用更安全

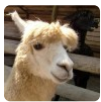
router

router firmware (OpenWRT) 好像都说这个

tunnel (VPN, SSH, SS) SS停止开发，不够保险。VPN听上去感觉比较对，其中openVPN比较主流。

obfuscate tool (obfsproxy) 据说必须混淆才能翻出去

怎么样强制走翻墙通道？是不是还需额外软件？还要哪些请补充，多谢。



Xiaolan • 2015年09月30日 • Reply • 博主

需要用obfs混淆openvpn之后在openwrt上指定路由表走openvpn...



surveillance104 • 2015年10月03日 • Reply

經過樓主?的提醒之後，Mac的步驟也有所進展，在這裏我就先發到樓主的博客上。

在選擇服務器之前一定要測速 一定要測速 一定要測速（因為很重要所以說了三遍）orz

linode:<https://www.linode.com/speedtest>

digitalocean:<http://speedtest-sfo1.digitalocean.com/>

vps服務端（最好用digitalocean（Paypal或信用卡）或者是linode（只支持信用卡），conoha支持支付寶但是速度就不如前兩者。

服務段操作：

ssh root@ip address

這時候一般會彈出這個頁面：

RSA key fingerprint is 56:80:87:7e:b8:64:2c:e0:dd:i3:83:49:37:q1:74:a9.

Are you sure you want to continue connecting (yes/no)?

你只需要輸入yes就可以了

之後他會讓你提示輸入密碼。 wetudcfd@127.0.0.1's password:

這裏不同的服務器商是有區別的。

digitalocean會往你的郵箱發送含有出示密碼的郵件 linode我沒有使用過（等

待別人或樓主補充 conoha則是設定服務器介面的時候會提示你設定。

之後輸入如下命令：（以下範例按照debain8.1系統為例）

```
apt-get update && apt-get dist-upgrade
apt-get install gcc python-pip python-dev
pip install obfsproxy
```

等這些安裝完之後，輸入以下命令：

```
obfsproxy --data-dir ~/.obfs/ scramblesuit --dest 127.0.0.1:22 --password
SHENMESHIHOUCAIKEYIYANJIUZHENG server 0.0.0.0:4980 &
```

127.0.0.1:22前半部分是你想要封裝的端口的端口名和IP地址
0.0.0.0:4980 這部分是你想要封裝完成後輸出的端口名和ip地址（0.0.0.0是任意ip地址，127.0.0.1是本機IP地址『完全屬於菜鳥知識』）
順便提一句，不管是OS X的terminal還是windows的命令提示符，隔差不多2-3小時之後連到服務器的ssh終端就會斷掉，是不是牆dpi所導致的？（看來ssh之前得先掛個lantern）

然後是因為ssh連結，你需要添加只能訪問ssh連結的用戶（這個好像樓主沒有填上去這部分）orz

```
adduser 用戶名 比如我想添加名為opengate的用戶，則輸入 adduser
opengate
```

接下來是為這個用戶添加密碼 這裏還是根據vps服務商分有兩種情況
conoha你還需要手動添加密碼 需要輸入 passwd 用戶名 命令 比如我想給剛才opengate的用戶添加密碼 則輸入：

```
passwd opegate
```

digitalocean的話，他會自動告訴你你設置什麼密碼，你的個人信息，公司名稱等 你只需要添加密碼，其他的選項一直回車就可以。

linode我並沒有使用，這個部分具體情況還不知道（需要他人詳細補充）

之後就是OS X客戶端的事情：

首先得安裝brew軟件：

重新打開一個terminal

```
$ ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
```

```
brew install python
```

```
pip install obfsproxy
```

好了這就應該可以用了 OS X的一個優點是你不需要像在windows用命令提示符去尋找obfsproxy的根目錄再輸入命令 直接terminal打開就可以了：

```
obfsproxy scramblesuit --dest IP地址:4980 --password
SBSB4444FANGBINXING4SBSBSBSBSBSB client 127.0.0.1:22222 &
```

注意剛才vps服務段的IP地址端口server 0.0.0.0:4980要與客戶端dest IP地址:4980 的端口要保持一致。

好的現在你只需要輸入：`ssh -N -D 7070 剛才添加的用戶名@127.0.0.1 -p 22222`

比如說我想要剛才的用戶opengate登陸本地ssh，那麼我該怎麼辦？你只需要
`ssh -N -D 7070 opengate@127.0.0.1 -p 22222`

注意，你需要 client 127.0.0.1:22222 & 的ip地址與端口和

opengate@127.0.0.1 -p 22222的端口和ip地址是一樣的，否則連接不上orz

下一步它會提示輸入密碼 如果是conoha，則輸入當時用 passwd 用戶名 命令
是輸入的密碼 然後輸入自己的密碼

如果是digitalocean，則是在當時新建用戶後它告訴你這個用戶輸入密碼時你
輸入的密碼即可

（注意，上面的vps與OS X客戶段的terminal在翻牆期間絕對不能關閉！！）

然後如果你使用谷歌瀏覽器 我推薦你選擇proxy switchOmega 只需要
chrome瀏覽器點右上角三個橫杆，再點擊設置，然後選擇 擴展應用 然後選擇
『取得更多擴展應用』 之後又一個搜索頁面，你只要輸入proxy，他的裡面的
選項就會有proxy switchOmega。

下載之後你需要點擊右上角的小圓圈，之後你需要點擊設置 設置 左側有一個
屬性裡面有一個代理選項 點擊它

服務器地址填寫 127.0.0.1 協議選擇socks5 端口則選擇client 127.0.0.1:22222
& 命令中一樣的端口 這裏是22222 那麼輸入22222就好了

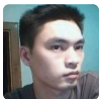
之後點擊應用改變即可

好了再點擊小圓圈 選擇『代理』（不是系統代理切記）之後你就可以翻牆了



surveillance104 • 2015年10月03日 • Reply

希望網友和樓主能夠補充我的地方 謝啦orz



jzp820927 • 2015年10月05日 • Reply

站長的scramblesuit公共帐号是不是不能用了？前几天还用的好好的，今天连不上

windows下 chrome 浏览器提示“ERR_SOCKS_CONNECTION_FAILED”

linux终端下用“`curl -x socks5://IP:22222`”命令提示“Unable to receive initial
SOCKS5 response”

把程序关了，重开还是一样？



surveillance104 • 2015年10月26日 • Reply

這個辦法可以用於mac或者是linux客戶端，windows用戶我會另外開一個帖子
進行說明

經過樓主大人的提示（當然也很感謝<https://www.digitalocean.com/community>

/tutorials/how-to-use-ssh-keys-with-digitalocean-droplets 裡面sitelifters關於操作證書的提示『他說的是Ubuntu，在detain上同樣有效』。

以前的關於obfsproxy不穩定問題是出於ssh連結本身不穩定的問題，而並不是obfsproxy渾穀所導致的。

（如果按照以前樓主大人帖子輸入ssh -N -D 7070 fanqiang@127.0.0.1 -p 22222 的話，過一段時間會自動斷線）

解決方案如下：

在操作之前，一定要進行測速：

digitalocean: speedtest-nyc2.digitalocean.com

linode:<https://www.linode.com/speedtest>

註冊vps完畢後，在Terminal輸入命令：

```
ssh root@ip address
```

可能會連接不上，這個時候需要重啓或者是重新在控制面板上設置另外一個主機重試

登陸vps後輸入以下所有命令：

```
apt-get update && apt-get upgrade -y && apt-get install gcc python-pip  
python-dev && pip install obfsproxy
```

```
adduser username
```

這個時候會提示輸入密碼 輸入密碼便是

```
obfsproxy --data-dir ~/.obfs/ scramblesuit --dest 127.0.0.1:22  
--passwordSBSB4444FANGBINXING4SBSBSBSBSBSB server  
0.0.0.0:8080 &
```

退出vps，輸入exit

在Terminal輸入這個命令（這是在客戶端完成的，不需要登陸vps）：

```
cat ~/.ssh/id_rsa.pub | ssh root@IP "cat >> ~/.ssh/authorized_keys"
```

之後輸入 ssh root@ip address 如果vps沒有提示你輸入密碼，則表示你已經成功用證書登陸vps的root用戶了。

之後進行禁止密碼登入root只進行證書登陸的選項：

在vps輸入：

```
nano /etc/ssh/sshd_config
```

打開文件後，找到此行：PermitRootLogin yes

之後把它改成這個樣子：PermitRootLogin without-password

在Terminal輸入exit，退出vps的root用戶登陸狀態

之後登陸你剛才新建立的用戶:ssh username@IP address 之後進行如下操作：

```
cd ~
```

```
mkdir .ssh
```

（如果不進行這步驟，之後驗證用戶vps證書的時候就會出現"No such file or directory"的錯誤）

之後退出vps客戶端，再進行對該用戶的證書登陸驗證操作（剛才是root用戶）

```
cat ~/.ssh/id_rsa.pub | ssh username@IP "cat >> ~/.ssh/authorized_keys"
```

vps還是會提示輸入密碼，再輸入一邊該用戶的密碼（不是root的密碼）

之後你再進行ssh username@IP address 如果不提示輸入密碼的話，那麼這個用戶的驗證證書就成功了。（這個時候你可以退出vps了，在Terminal中輸入exit即可退出vps的用戶登陸）

之後在OS X客戶端Terminal輸入以下命令：

（請注意brew安裝的客戶絕對不能是 OS X的root用戶）（linux用戶可以跳過安裝brew這個步驟）

```
$ ruby -e "$(curl -fsSL https://raw.githubusercontent.com/Homebrew/install/master/install)"
```

```
brew install python
```

```
pip install obfsproxy
```

安裝完成後，輸入如下命令（以下命令都是在OS X本機客戶端執行）

```
obfsproxy scramblesuit --dest 1xx.xxx.xxx.xxx:8080  
--passwordSBSB4444FANGBINXING4SBSBSBSBSBSB client  
127.0.0.1:22222
```

```
ssh -D 7070 proxyfight@127.0.0.1 -p 22222 -i /Users/reborn/.ssh/id_rsa
```

之後他會顯示此vps的用戶終端遠程控制見面，你可以不用管它。

之後還是和我上面說的一樣，用switchOmega 然後代理設置成 socks5 7070 即可

之後你就可以免除ssh連結的不穩定性（注意再強調一邊，ssh不穩定絕對不

是obfsproxy的原因，而是ssh連結本身的原因），來進行breakwa11了。

有什麼我說錯的地方請樓主和大家多多補充多謝了orz



surveillance104 • 2015年10月27日 • Reply

上次的教程有兩個需要修改的地方：

1. 在Terminal輸入這個命令（這是在客戶端完成的，不需要登陸vps）：
`cat ~/.ssh/id_rsa.pub | ssh root@IP "cat >> ~/.ssh/authorized_keys"`

這個命令之前需要輸入（在你本機的客戶端上）：`ssh-keygen -t rsa`

2. `cat ~/.ssh/id_rsa.pub | ssh root@IP "cat >> ~/.ssh/authorized_keys"`
這個命令如果粘貼進去是不會運行的（我犯了一個格式的錯誤）這個命令應該可以粘貼運行
`cat ~/.ssh/id_rsa.pub | ssh root@ip address "cat >> ~/.ssh/authorized_keys"`



surveillance104 • 2015年10月27日 • Reply

抱歉還有一個問題，這個命令後面需要加上"&"這個符號

`obfsproxy scramblesuit --dest 1xx.xxx.xxx.xxx:8080
--passwordSBSB4444FANGBINXING4SBSBSBSBSBSB client
127.0.0.1:22222`

修改後的：

`obfsproxy scramblesuit --dest 1xx.xxx.xxx.xxx:8080
--passwordSBSB4444FANGBINXING4SBSBSBSBSBSB client
127.0.0.1:22222 &`

要不得話，命令不會後台運行。

這樣坐在電腦面前的乃還得開一個terminal來運行"`ssh -D 7070
proxyfight@127.0.0.1 -p 22222 -i /Users/reborn/.ssh/id_rsa`"



llyloo • 2015年11月04日 • Reply

博主你好，最近我在新的服务器上配置obfsproxy的时候遇到了一个新问题，我按照之前的步骤，配置好sock5服务器，测试连接正常，但是打开了obfsproxy就连不上了，服务端一直在刷同一个错误：

Unhandled Error

Traceback (most recent call last):

File "/usr/lib/python2.6/site-packages/twisted/python/log.py", line 101, in callWithLogger

return callWithContext({"system": lp}, func, *args, **kw)

File "/usr/lib/python2.6/site-packages/twisted/python/log.py", line 84, in

```
callWithContext
return context.call({ILogContext: newCtx}, func, *args, **kw)
File "/usr/lib/python2.6/site-packages/twisted/python/context.py", line 118, in
callWithContext
return self.currentContext().callWithContext(ctx, func, *args, **kw)
File "/usr/lib/python2.6/site-packages/twisted/python/context.py", line 81, in
callWithContext
return func(*args,**kw)
--- ---
File "/usr/lib/python2.6/site-packages/twisted/internet/posixbase.py", line
597, in _doReadOrWrite
why = selectable.doRead()
File "/usr/lib/python2.6/site-packages/twisted/internet/tcp.py", line 209, in
doRead
return self._dataReceived(data)
File "/usr/lib/python2.6/site-packages/twisted/internet/tcp.py", line 215, in
_dataReceived
rval = self.protocol.dataReceived(data)
File "/usr/lib/python2.6/site-packages/obfsproxy/network/network.py", line
320, in dataReceived
self.circuit.dataReceived(self.buffer, self)
File "/usr/lib/python2.6/site-packages/obfsproxy/network/network.py", line
161, in dataReceived
self.transport.receivedDownstream(data)
File "/usr/lib/python2.6/site-packages/obfsproxy/transport/scramblesuit
/scramblesuit.py", line 531, in receivedDownstream
self.sendTicketAndSeed()
File "/usr/lib/python2.6/site-packages/obfsproxy/transport/scramblesuit
/scramblesuit.py", line 481, in sendTicketAndSeed
flags=const.FLAG_NEW_TICKET)
File "/usr/lib/python2.6/site-packages/obfsproxy/transport/scramblesuit
/scramblesuit.py", line 264, in sendRemote
self.sendHMAC) for msg in messages])
File "/usr/lib/python2.6/site-packages/obfsproxy/transport/scramblesuit
/message.py", line 129, in encryptAndHMAC
(self.totalLen - self.payloadLen) * '\0')
File "/usr/lib/python2.6/site-packages/obfsproxy/transport/scramblesuit
/mycrypto.py", line 152, in encrypt
return self.crypter.encrypt(data)
exceptions.ValueError: Input strings must be a multiple of 16 in length
望指教
```



surveillance104 • 2015年11月05日 • Reply

乃嘗試一下python3.5的安裝包試試看呢？



ljlou • 2015年11月05日 • Reply

py2跟py3不是互不兼容的么？好吧我去试试看，死马当活马医了



surveillance104 • 2015年11月06日 • Reply

我的意思是把原來的2.7刪除換成3.5 囧rz



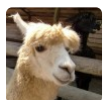
ljlou • 2015年11月06日 • Reply

只能用2.7版本的python啊



ljlou • 2015年11月05日 • Reply

我在Tor里面看到Python的版本是2.7.5



Xiaolan • 2015年11月08日 • Reply • 博主

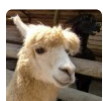
这个问题我也不太懂了,抱歉：（,看起来是程序问题..
尝试升级python到最新版本呢？



sdqf • 2016年03月07日 • Reply

想问一下，在windows里，直接使用potty或plonk这种支持混淆的软件，能不能正常连接楼主配置的服务端？

如果ubuntu作为客户端，是否使用obfuscated-openssh进行连接？在安装了obfuscated-openssh之后，ssh -h里看到多出来一个参数-z，是否就是填设置的混淆密码？



Xiaolan • 2016年03月24日 • Reply • 博主

抱歉,这几个软件都没有听说过,无法给你更多的信息了：（
如果obfuscated-openssh使用了和服务端一样的混淆手法,就可以链接....

fish • 2016年03月30日 • Reply



博主可否写篇用obfsproxy混淆openvpn流量，通过openvpn翻墙的文章？我试了一下，失败



Xiaolan • 2016年04月02日 • Reply • 博主
OK,有空



fish • 2016年04月24日 • Reply
现在都快4月底了，博主可否抽空写写呢？

Leave a Reply

Your email address will not be published.

Comment

Name

Email

Website

Post Comment