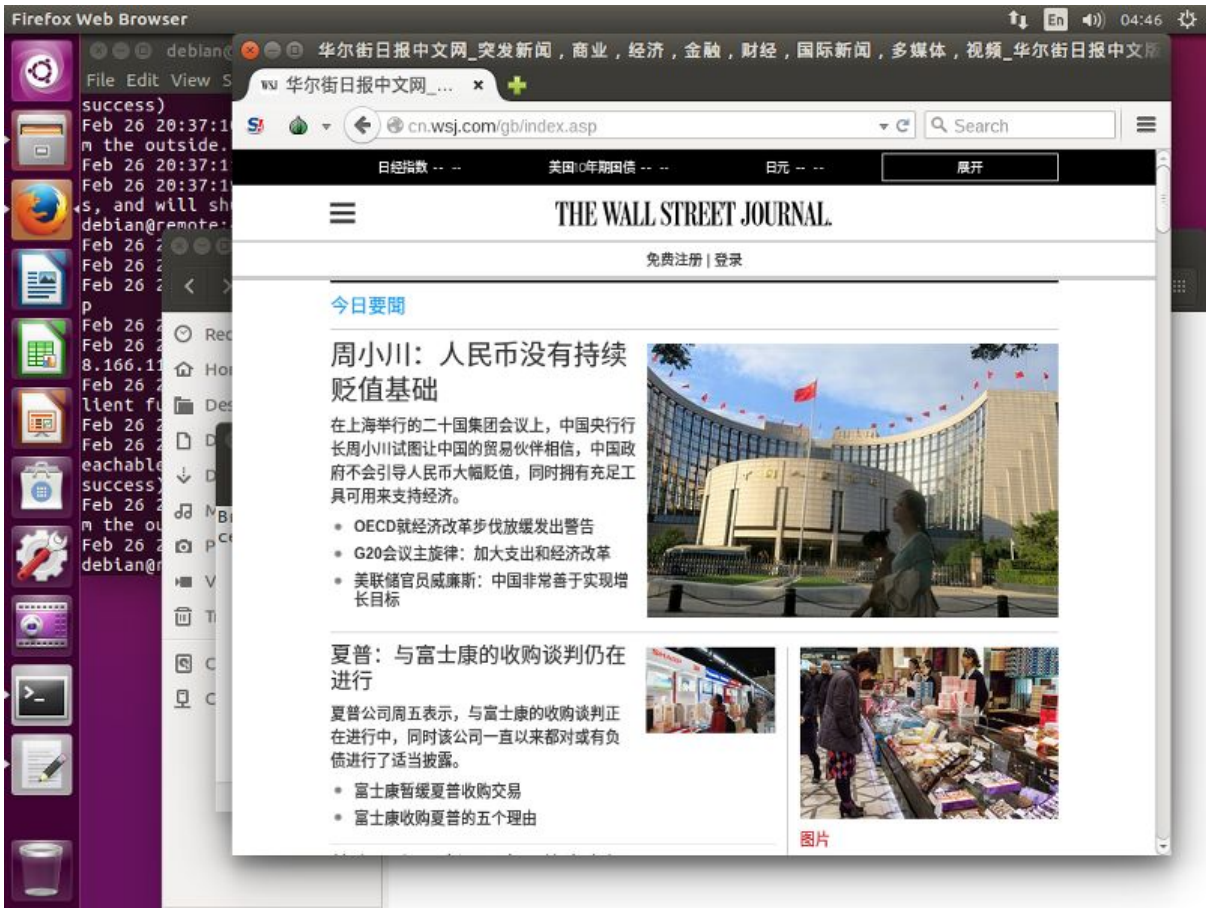
架设Tor Obfs4 网桥绕过中国审查

Tor Obfs4 Bridge for GFW



GFW能轻易的探测和封锁Tor的网桥，而Obfs4 致力于解决这一难题。Obfs4不会对GFW的主动探测回应，另外，如果你不公开你的私人网桥，GFW不能轻易得到你网桥的信息。

The Great Firewall (GFW) of China can easily detect and block Tor bridges.[1] Obfs4 aims to solve this problem. It will not respond to active probing by the GFW. Also, if you keep your

bridge IP address and port number private, the GFW cannot get these details from public sources.

服务器配置

Server

你需要一个运行debian8 的虚拟私人服务器来搭建网桥。
#当然独立主机更好，其他系统以此类推
#官方文档
#ssh 进入主机，然后编辑apt软件源

```
sudo vi /etc/apt/sources.list
```

然后加入如下内容

```
deb http://deb.torproject.org/torproject.org jessie main
```

```
deb-src http://deb.torproject.org/torproject.org jessie main
```

```
deb http://deb.torproject.org/torproject.org obfs4proxy main
```

加入gpg密钥

```
gpg --keyserver keys.gnupg.net --recv 886DDD89
```

```
gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | sudo apt-key add -
```

更新apt的缓存，然后安装如下软件包。如果报错依赖的话，应该是元没有配置好，参考官方文档

```
sudo apt-get update
```

```
sudo apt-get install tor deb.torproject.org-keyring
```

```
sudo apt-get install obfs4proxy
```

我们先选择一个端口号，最好不用9001（用来接受tor链接）。比如说，我们可以用9388端口。你搭建的时候最好选个不一样的。

另外我们需要设定obfs4 的端口，我们这次设为8168.

如果你开启了iptables，使用以下命令来开放端口

```
sudo iptables -A INPUT -p tcp --dport 9388 -j ACCEPT
```

```
sudo iptables -A INPUT -p tcp --dport 8168 -j ACCEPT
```

sudo dpkg-reconfigure iptables-persistent

然后编辑下obfs的配置文件

```
sudo vi /etc/tor/torrc
```

这是一个配置文件的样本：

```
BridgeRelay 1

ORPort tor的端口

ExtORPort auto

SocksPort 0

ExitPolicy reject *:*

RunAsDaemon 1

ServerTransportPlugin obfs4 exec /usr/bin/obfs4proxy
```

```
ServerTransportListenAddr obfs4 0.0.0.0:8168 #obfs端口
```

#如果是aws，0.0.0.0要改为内网地址才行

```
PublishServerDescriptor 0
```

(最后一行设为0的话就是你私人的网桥啦)

保存后重启一下tor

```
sudo service tor restart
```

查看日志

```
sudo tail -F /var/log/tor/log
```

当日志显示ORPort可以从互联网访问的时候就可以用了

了

那么，网桥的地址是什么呢？使用

```
sudo cat /var/lib/tor/pt_state/obfs4_bridgeline.txt
```

来看

一般来说，是这样的：

```
Bridge obfs4 <IP ADDRESS>:<PORT> <FINGERPRINT>
cert=6LMNcXh6MIfApbZiMksnS4Kj+2sffZ5pybSqtcOO5YoHgfrMpkBJqvLxh
uR2Ppau0L2seg iat-mode=0
```

把它复制下来放在一个文件里

删掉“Bridge”

把 <IP ADDRESS> 换为你VPS的IP

把 <PORT> 换成你设定obfs的端口

用以下命令得到服务器身份指纹:

```
sudo cat /var/log/tor/log | grep fingerprint
```

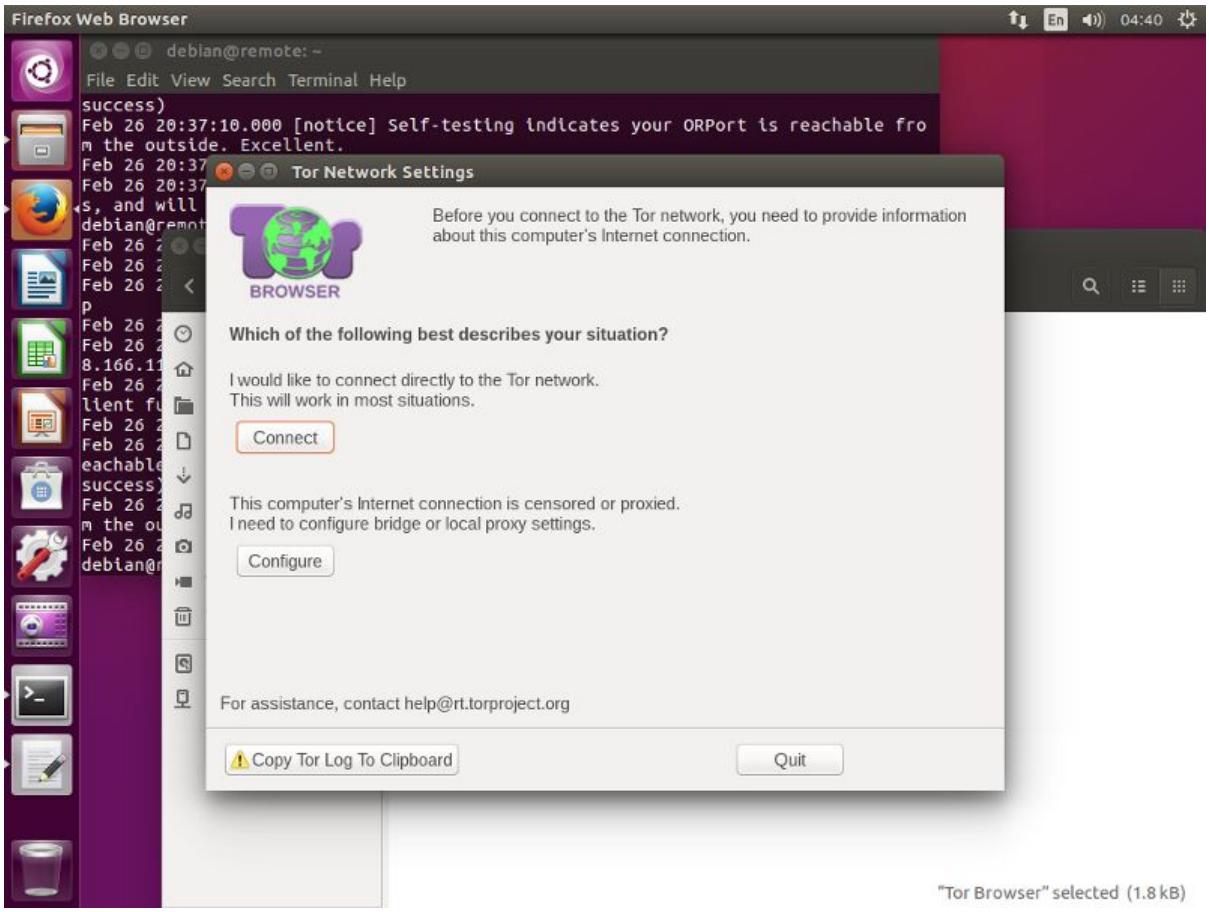
把<FINGERPRINT>替换为刚才搜索的Your Tor server's identity key

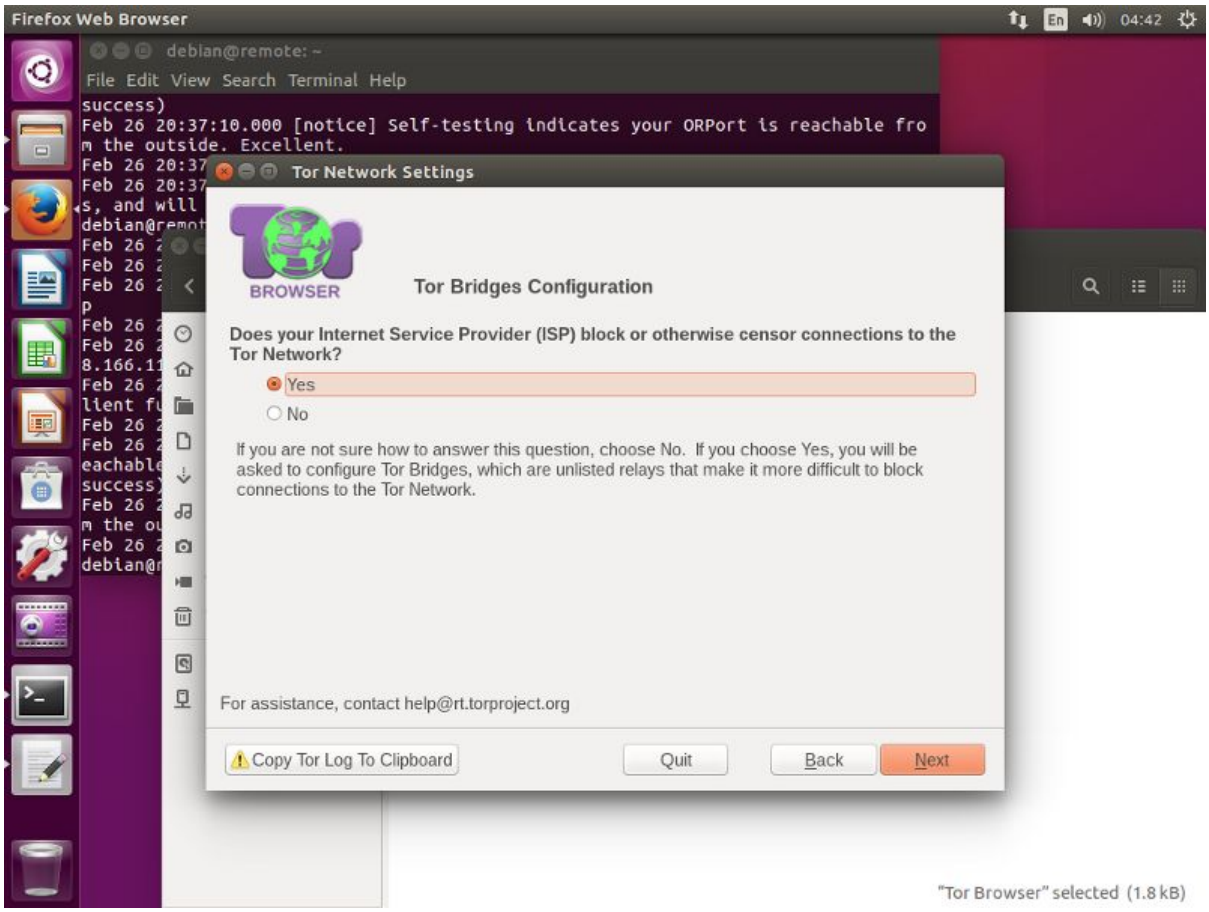
现在服务器端的设置完事了。

客户端

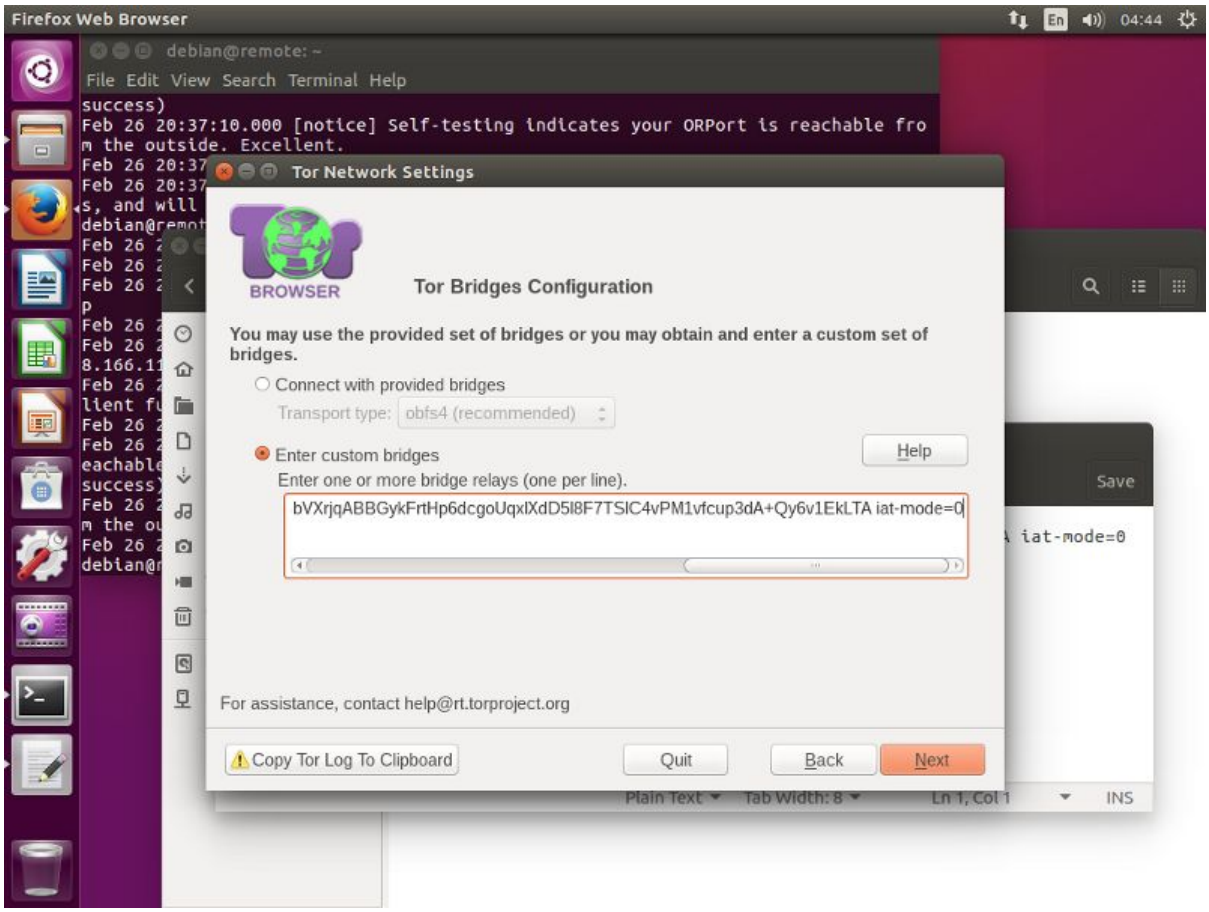
打开tor，点击configure，然后加入自定义的网桥，吧刚才的文字复制进去，

例如：obfs4 22.9.29.31:1234 JKBD$JBDKJHGIHDIHIED97bBLL cert=iwlskeigiwhaesgaergarghraiuiewy58y5j452w43gq65gbgtfajs iat-mode=0


Firefox Web Browser
En
04:40
debian@remote: ~
File Edit View Search Terminal Help
success)
Feb 26 20:37:10.000 [notice] Self-testing indicates your ORPort is reachable fro
m the outside. Excellent.
Tor Network Settings
BROWSER
Before you connect to the Tor network, you need to provide information about this computer's Internet connection.
Which of the following best describes your situation?
I would like to connect directly to the Tor network.
This will work in most situations.
Connect
This computer's Internet connection is censored or proxied.
I need to configure bridge or local proxy settings.
Configure
For assistance, contact help@rt.torproject.org
Copy Tor Log To Clipboard
Quit
"Tor Browser" selected (1.8 kB)

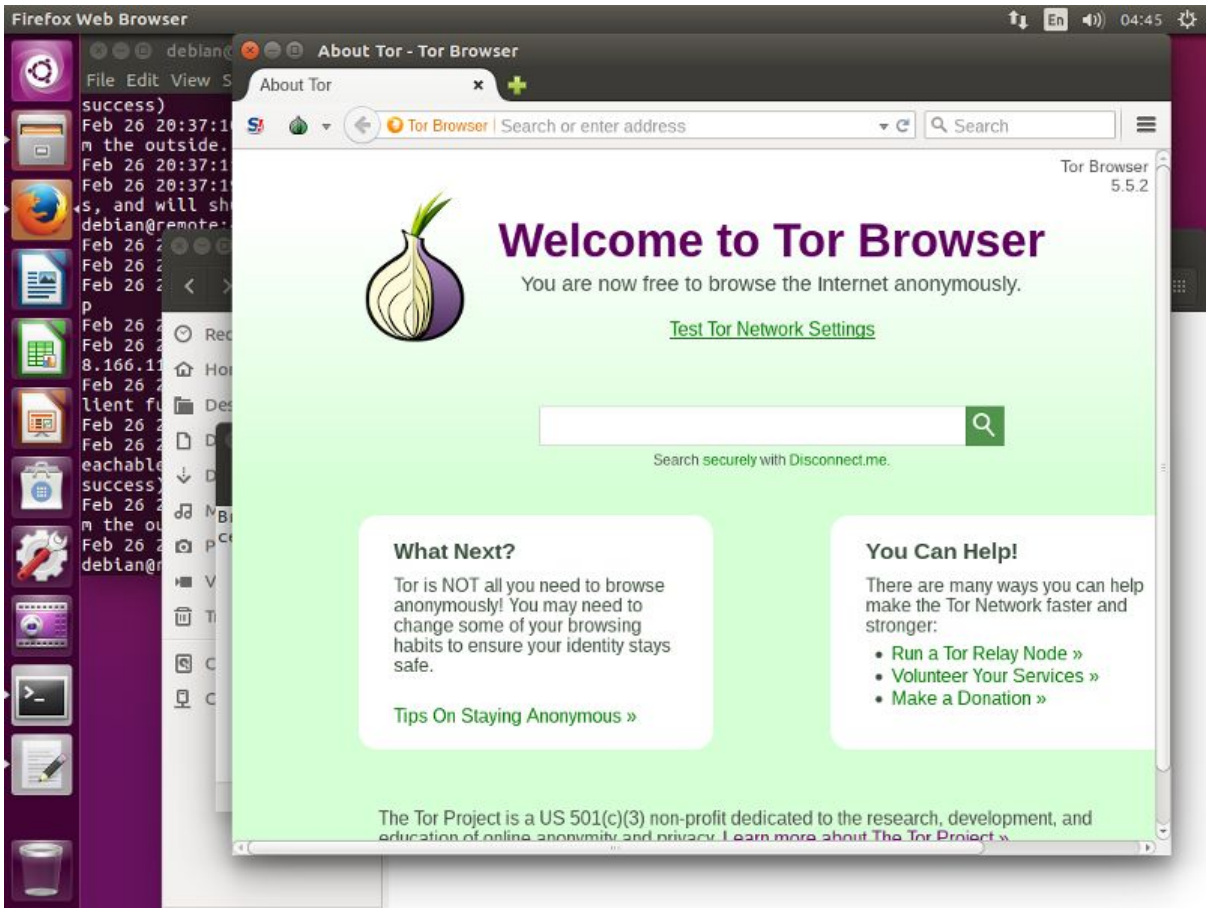


Select the radio button for Enter custom bridges. In the box below, paste in your edited bridge line, with the placeholders now replaced by real values. Click Next.

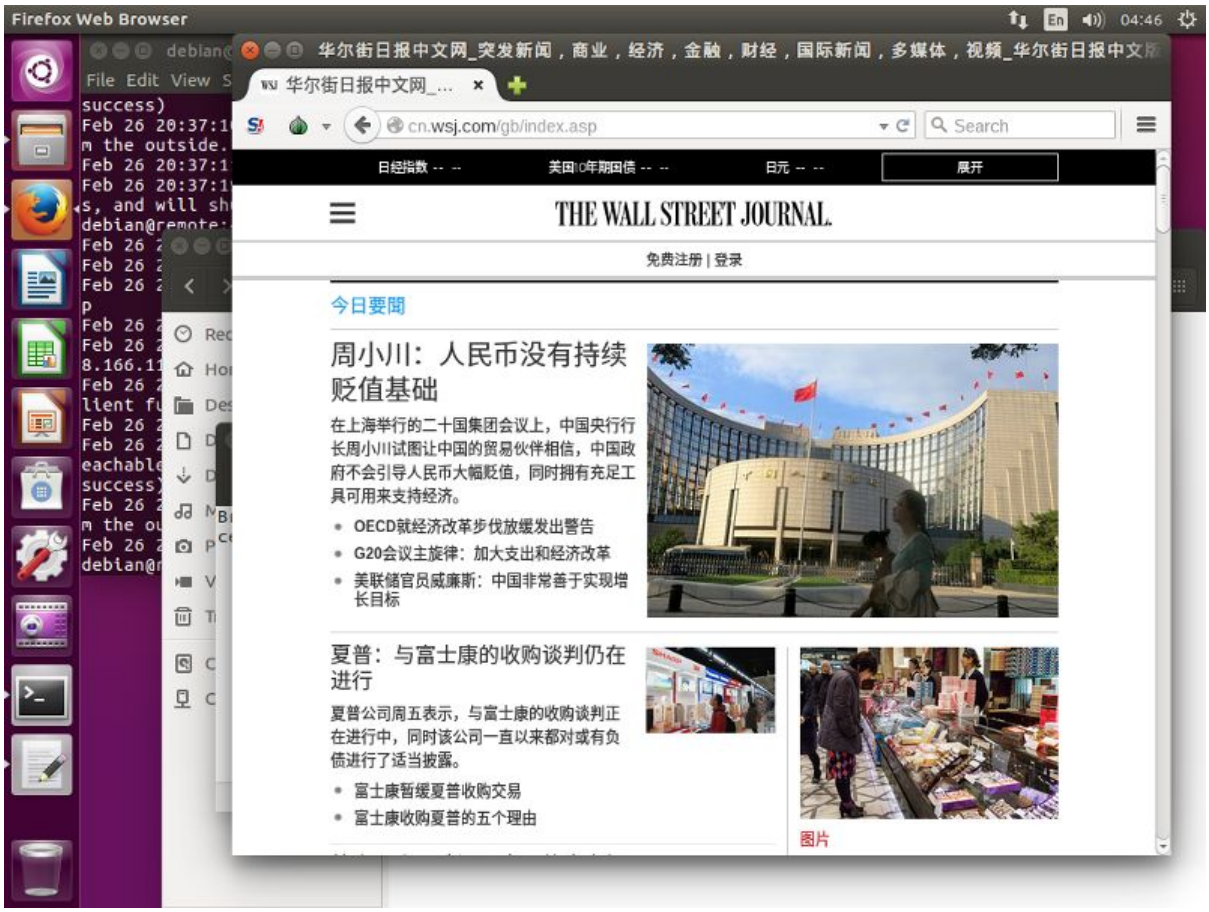


For local proxy, select No, and click Connect.

You will see the Tor Browser welcome page.



Enter the URL of a site you wish to visit. You can now visit that site via obfs4 and Tor.



引用

Reference

[1] Philipp Winter and Stefan Lindskog. “How the Great Firewall of China is Blocking Tor.” http://www.cs.kau.se/philwint/pdf/foci2012.pdf