

无需Java使用I2P——I2Pd简单扫盲

发表于: 2016年02月12日 • 43 条评论 • 2,954 次浏览 • 翻墙

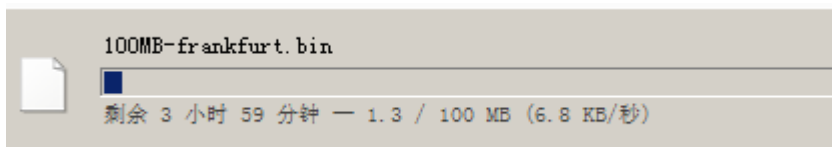
最近收到朋友的来信让我写一篇关于i2p的文章,顺便博客也好久没更新都快长草了..那就写一篇关于i2pd的简介+扫盲文章吧...

什么是I2P?

I2P是Tor的变种,比Tor网络更加安全、更据隐蔽性,如果你不知道Tor又是什么,请戳洋葱路由Tor。TOR和I2P共同点都是通过若干个节点将你的数据进行层层转包、加密,防止你的真实IP暴露。(摘自谷歌)

I2P与Tor有什么区别?

1. 安全性:Tor使用单一的链路进行传输你的数据;而I2P则使用多条链路分别传输你的数据并且每条链路传输的数据量可以不一样。
2. 难以封杀:I2P使用 Kad 算法来获取网络节点的信息,即不需要目录服务器且Kad算法拿到的节点信息只是整个 I2P 网络的一小部分并且每一台运行 I2P 的主机都可以成为中继。
3. 速度很慢:这是I2P最大的缺点了,速度很慢...根据笔者的测试,下载速度能上20k左右就谢天谢地了,平时只有10k左右...(如图)



这么慢能干什么用呢?应急翻墙,在所有梯子都失效的情况下,可以使用I2P应急翻墙下载新的梯子../**难以封杀**/

什么是I2Pd,与传统的I2P有何不同?

I2Pd与I2P最大的不同是I2Pd是一个采用C++编写的I2P网络的客户端,而传统的I2P使用的是Java语言..也就是说你再也不用安装臃肿的JRE了... /**Java退散 **/

哪里能下载到?

前面废话说了那么多,那么来进入正题吧..

I2Pd的官方网站为: <http://i2pd.website/releases/> 这里可以下载已经编译好的I2Pd.. 点击进入最新的版本的目录.

Index of /releases/2.4.0

- [Parent Directory](#)
- [i2pd_2.4.0-1jessie1_amd64.deb](#)
- [i2pd_2.4.0-1jessie1_i386.deb](#)
- [i2pd_2.4.0-1precise1_i386.deb](#)
- [i2pd_2.4.0-1trusty1_amd64.deb](#)
- [i2pd_2.4.0-1trusty1_i386.deb](#)
- [i2pd_2.4.0-1wheezy1_amd64.deb](#)
- [i2pd_2.4.0-1wheezy1_i386.deb](#)
- [i2pd_2.4.0_osx.tar.gz](#)
- [i2pd_2.4.0_win32_mingw.zip](#)
- [i2pd_2.4.0_win32_mingw_aesni.zip](#)
- [i2pd_2.4.0_win64_mingw.zip](#)
- [i2pd_2.4.0_win64_mingw_aesni.zip](#)

如果你是32位系统,则下载 **win32_mingw.zip** 如果是64位系统,则下载 **win64_mingw.zip**..

*/** 居然没有HTTPS, 真是奇怪呢... **/*

安装与配置?

下载解压后,在任何位置建立一个目录,将**i2pd.exe**放到新建立好的目录中...之后在同目录下建立一个文件名为**tunnel.cfg**的文件 */** 抱歉之前手滑,多打了个n **/*

内容如下:

```
[FanQiangProxy-XiaoLan-01]
type=client
host=127.0.0.1
port=8964
destination=nqiki6zqs7j6vzmwmpdcf3cyleqtzabvlzpu6bzdc27ncvjih4eq.b32.i2p
inbound.length=0
outbound.length=0
inbound.quantity=3
outbound.quantity=3
```

这里的**nqiki6zqs7j6vzmwmpdcf3cyleqtzabvlzpu6bzdc27ncvjih4eq.b32.i2p**是我搭建的出口代理,如果你找到了更好的出口代理,也可以换成其他的...

为了方便使用,我们可以来建立一个启动器, **start.bat**, 内容如下

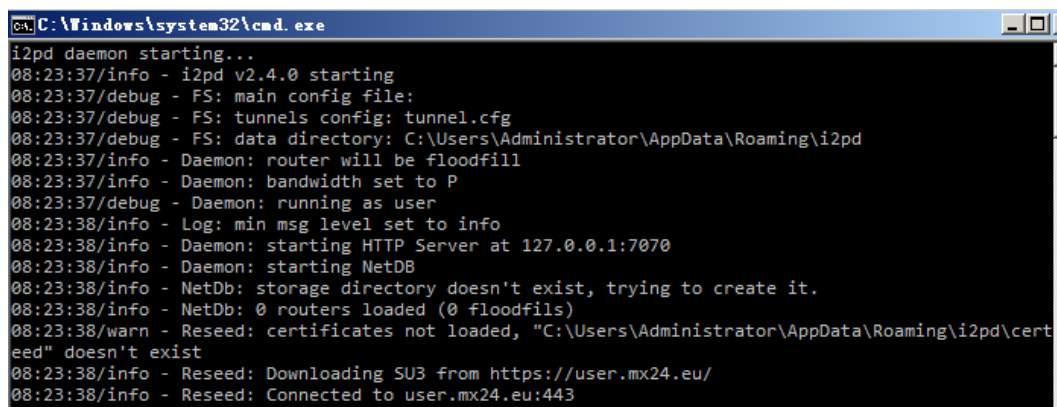
```
@echo off
echo i2pd daemon starting...
i2pd --socksproxy.enabled=0 --httpproxy.enabled=0 --floodfill
```

```
--bandwidth=P --tunconf=tunnel.cfg --ipv6
```

这些都完成之后,该目录下应该有3个文件:

- i2pd.exe - I2Pd主程序
- start.bat - 启动器
- tunnel.cfg - 配置文件

双击start.bat运行I2Pd后应该会弹出如下窗口,并且会卡在Reseed环节..别见怪,这很正常,因为补种的URL已经被墙



```
C:\Windows\system32\cmd.exe
i2pd daemon starting...
08:23:37/info - i2pd v2.4.0 starting
08:23:37/debug - FS: main config file:
08:23:37/debug - FS: tunnels config: tunnel.cfg
08:23:37/debug - FS: data directory: C:\Users\Administrator\AppData\Roaming\i2pd
08:23:37/info - Daemon: router will be floodfill
08:23:37/info - Daemon: bandwidth set to P
08:23:37/debug - Daemon: running as user
08:23:38/info - Log: min msg level set to info
08:23:38/info - Daemon: starting HTTP Server at 127.0.0.1:7070
08:23:38/info - Daemon: starting NetDB
08:23:38/info - NetDb: storage directory doesn't exist, trying to create it.
08:23:38/info - NetDb: 0 routers loaded (0 floodfills)
08:23:38/warn - Reseed: certificates not loaded, "C:\Users\Administrator\AppData\Roaming\i2pd\cert
eed" doesn't exist
08:23:38/info - Reseed: Downloading SU3 from https://user.mx24.eu/
08:23:38/info - Reseed: Connected to user.mx24.eu:443
```

之后我们将这个程序关掉退出I2P, 打开%APPDATA%\i2pd\netDb目录(将黑体字直接贴到地址栏中回车)

然后下载补种包,补种包可以有两种方式下载

1. <https://github.com/XL2014/I2PdSeed>

将补种包解压到%APPDATA%\i2pd\netDb目录

2. 使用脚本下载

```
strFileURL = "https://raw.githubusercontent.com/XL2014/I2PdSeed/master/netDb.zip"
strHDLocation = "file.zip"
Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP")
objXMLHTTP.open "GET", strFileURL, false
objXMLHTTP.send()
If objXMLHTTP.Status = 200 Then
Set objADOStream = CreateObject("ADODB.Stream")
objADOStream.Open
objADOStream.Type = 1
objADOStream.Write objXMLHTTP.ResponseBody
objADOStream.Position = 0' Set the stream position to the start
Set objFSO = CreateObject("Scripting.FileSystemObject")
If objFSO.FileExists(strHDLocation) Then objFSO.DeleteFile
```

```
strHDLocation
Set objFSO = Nothing
objADOSTream.SaveToFile strHDLocation
objADOSTream.Close
Set objADOSTream = Nothing
End if
Set objXMLHTTP = Nothing
ZipFile="file.zip"
Set objShell = CreateObject( "WScript.Shell" )
appDataLocation=objShell.ExpandEnvironmentStrings("%APPDATA%")
ExtractTo= appDataLocation & "i2pd\"
Set fso = CreateObject("Scripting.FileSystemObject")
sourceFile = fso.GetAbsolutePathName(ZipFile)
destFolder = fso.GetAbsolutePathName(ExtractTo)
Set objShell = CreateObject("Shell.Application")
Set FilesInZip=objShell.NameSpace(sourceFile).Items()
objShell.NameSpace(destFolder).copyHere FilesInZip, 16
Set fso = Nothing
Set objShell = Nothing
Set FilesInZip = Nothing
MsgBox("补种完毕")
```

将以上内容保存为reseed.vbs然后双击运行,即可自动补种....(感谢不愿透露姓名的唐马儒的建议...)

之后运行运行start.bat

等待大约2分钟,将浏览器的SOCKS5代理设置为 127.0.0.1:8964 就可以使用I2Pd翻墙了.. :)

提示: 最好长期运行以便自动获取最新的种子避免封杀....

参考资料: [“如何翻墙”系列: 简单扫盲 I2P 的使用](#)

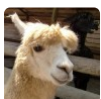
转载请注明来自Xiaolan's Blog (<https://xiaolan.me>)

43 条评论



posclegom • 2016年02月12日 • Reply

xiaolan兄, 愚弟是posclegom, 兄的ptbooks.1984.city网站down掉了。



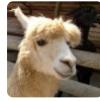
Xiaolan • 2016年02月12日 • Reply • 博主

服务器重装系统了...内容都要重新同步..1小时后就应该可以恢复了....



posclegom • 2016年02月12日 • Reply

谢谢xiaolan兄！另外翻墙软件目录和编程兄博客离线版打包还望xiaolan兄加入。



Xiaolan • 2016年02月13日 • Reply • 博主

搞定..



posclegom • 2016年02月13日 • Reply

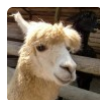
xiaolan兄神速！愚弟佩服的五体投地！



posclegom • 2016年02月14日 • Reply

xiaolan兄，愚弟近日在折腾编程兄的免翻墙镜像一事，有几件事要请教兄：

- 1.愚弟是否需要先要架设好诸如一台搬瓦工主机来host编程兄的免翻墙镜像，然后再为这台主机加上cloudflare保护？还是cloudflare本身就出售虚拟主机供愚弟host编程兄的免翻墙镜像？
- 2.comodo的安全证书是否包含在cloudflare的套餐里面？还是兄需要另行为自己的域名购买安全证书？
- 3.愚弟看了一下兄的comodo安全证书，subjectAltNames里包含了包括xiaolan.me和1984.city在内的各种各样的域名，请问在comodo网站上面愚弟应该选择哪一种套餐才能获得如此灵活的证书？还是cloudflare提供这种灵活的证书？如果日后愚弟要在subjectAltNames里加入新的域名，手续繁不繁琐？



Xiaolan • 2016年02月14日 • Reply • 博主

1. 需要一个VPS服务器
2. ssl证书由cloudflare免费提供...
3. 免费套餐就可以用SSL证书..在cloudflare加入新域名,证书也会自动随之更新..

posclegom • 2016年02月17日 • Reply



多谢xiaolan兄指导！



音业 • 2016年02月13日 • Reply

哎呀，多谢普及i2pd！最近编程随想君好久没发文章呀.....

顺带广告以下我的新文《抛砖引玉——對趙家人一詞的進一步演繹》

网址：<https://classcalliberal.blogspot.com/2016/02/Zhao-family.html>



Anonymous • 2016年02月13日 • Reply

最好就是Linux运行虚拟机+Tails进行整机隔离，Tails本身就是Tor的操作系统，也就不必在虚拟机内操心了，如果再在运行虚拟机的操作系统加多一层加密软件（比如自由门）那网站封锁Tor也无济于事，请问站长要怎么设置Linux呢？



beijing2008 • 2016年02月14日 • Reply

这样做怎么可以，这样设置出口明明是Tor，自由门帮助Tor联网，就像VPN帮助Tor联网



Anonymous • 2016年03月23日 • Reply

Tails内无法运行自由门，别的代理可能可以吧！

无需Java使用I2P——I2Pd简单扫盲 – 细节的力量 • 2016年02月14日 • Reply

[...] 原文：<https://xiaolan.me/howtousei2pd.html> [...]



PW • 2016年02月14日 • Reply

从推特上看到，过来看看，
以前试用过，速度慢，还要安装JRE，又删了，
这下终于不用再安装JRE。



caofengzi • 2016年02月15日 • Reply

藍總為什麼俺啟動玩i2pd以後把補種包解壓到c/%APPDATA%/i2pd/netDb目錄以後在啟動程序會報錯呢？

Xiaolan • 2016年02月22日 • Reply • 博主



有什么错误提示呢？



Shark • 2016年02月20日 • Reply

我在1984.city上回了一条帖子，关于hs是否有必要用ssl，一直没看见有人回，在这儿在“回复”一下，SSL对于Tor来说，用处不大，以下是tor blog关于facebook的hs开ssl的看法：

Part four: what do we think about an https cert for a .onion address?

Facebook didn't just set up a hidden service. They also got an https certificate for their hidden service, and it's signed by Digicert so your browser will accept it. This choice has produced some feisty discussions in the CA/Browser community, which decides what kinds of names can get official certificates. That discussion is still ongoing, but here are my early thoughts on it.

In favor: we, the Internet security community, have taught people that https is necessary and http is scary. So it makes sense that users want to see the string "https" in front of them.

Against: Tor's .onion handshake basically gives you all of that for free, so by encouraging people to pay Digicert we're reinforcing the CA business model when maybe we should be continuing to demonstrate an alternative.

In favor: Actually https does give you a little bit more, in the case where the service (Facebook's webserver farm) isn't in the same location as the Tor program. Remember that there's no requirement for the webserver and the Tor process to be on the same machine, and in a complicated set-up like Facebook's they probably shouldn't be. One could argue that this last mile is inside their corporate network, so who cares if it's unencrypted, but I think the simple phrase "ssl added and removed here" will kill that argument.

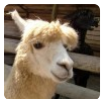
Against: if one site gets a cert, it will further reinforce to users that it's "needed", and then the users will start asking other sites why they don't have one. I worry about starting a trend where you need to pay Digicert money to have a hidden service or your users think it's sketchy — especially since hidden services that value their anonymity could have a hard time getting a certificate.

One alternative would be to teach Tor Browser that https .onion addresses don't deserve a scary pop-up warning. A more thorough approach in that direction is to have a way for a hidden service to generate its own signed https cert using its onion private key, and teach Tor Browser how to verify them — basically a decentralized CA for .onion addresses, since they are

self-authenticating anyway. Then you don't have to go through the nonsense of pretending to see if they could read email at the domain, and generally furthering the current CA model.

We could also imagine a pet name model where the user can tell her Tor Browser that this .onion address "is" Facebook. Or the more direct approach would be to ship a bookmark list of "known" hidden services in Tor Browser — like being our own CA, using the old-fashioned /etc/hosts model. That approach would raise the political question though of which sites we should endorse in this way.

So I haven't made up my mind yet about which direction I think this discussion should go. I'm sympathetic to "we've taught the users to check for https, so let's not confuse them", but I also worry about the slippery slope where getting a cert becomes a required step to having a reputable service. Let us know if you have other compelling arguments for or against.



Xiaolan • 2016年02月22日 • Reply • 博主

多谢提供资料...不得不使用HTTPS的原因在1984city上回复你了：)



Shark • 2016年02月20日 • Reply

SSL/TLS isn't necessary

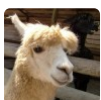
You don't really need SSL/TLS in an onion address (ie. https) since it's a complete encrypted tunnel + PFS (perfect forward secrecy), but it does not hurt having extra layers in that onion!

Although it is true that extra layers are good beware that usually redirecting to SSL/TLS will mean that the certificate will not validate (because the hostname will be *.onion, instead of the certificate that you have for your public service). If you can get a .onion certificate, that works



jkle • 2016年02月23日 • Reply

需要便携版本!等于就是将配置文件放在主目录下,不要留在电脑的用户目录!



Xiaolan • 2016年02月27日 • Reply • 博主

这个需要等待官方来更新了...据说下个版本有自定义路径的功能



Anonymous • 2016年02月27日 • Reply

草泥馬，I2P是個設計比較失敗的產品，已經有了汽車的時代，現在換上小驢車，哪個願意去坐？想一想是不是這道理？

至於安全，談不上有多安全，我看，不上網最安全。



Anonymous • 2016年02月28日 • Reply

1 <https://bitcointalk.org/index.php?topic=841375.0;wap2> 这篇文章说用tor使用比特币不安全，文章大概不是很懂，如果使用多重代理，在tor再加入一个固定ip代理构成三重代理可以保证安全吗？如果不行，怎么解决

2<http://btckan.com/news/topic/13880> 这篇文章里说“确保不要通过Tor来使用blockchain.info clearnet url，这样做的话，你会打开另一个可能的漏洞（恶意Tor出口节点）”那我像1里那样使用三重代理就能保证安全了吗



Xiaolan • 2016年03月02日 • Reply • 博主

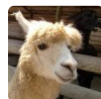
1. 只要不联系到自己的真实身份就是安全的,比如不要把用tor的比特币提现之类的....
2. 恶意tor出口节点对于https是无效的,因此无所谓.....



Anonymous • 2016年03月03日 • Reply

1比特币肯定要提现啊，钱就是要花的啊。如果按照你的那篇洗钱文章去多个兑换中心流转再在tor后面加一重代理是不是就安全了？

2如果只是http呢，在tor后面加一重代理可以保证身份安全了吗



Xiaolan • 2016年03月24日 • Reply • 博主

那篇文章是简单的从经侦的角度去看,没从网侦的方面去观察..

tor已经足够安全了,没必要在后面再加一重代理..

倒是可以把代理加在前面....



zxzz • 2016年03月08日 • Reply

能不能介绍下 Linux 纯终端下面的配置方法，就是没有图像界面的 ubuntu 系统？



Xiaolan • 2016年03月24日 • Reply • 博主

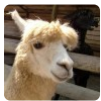
纯终端下没有浏览器呀...配置了也没作用呢...



CyberThink • 2016年03月16日 • Reply

嘿嘿，使用了我自己发明/*当然也不一定*/的注释方法。

关于比特币的话，我有想过一个方案，用Alipay在localbitcoins上面付款，然后deposit到bitcoin fog/*手续费只有1% ~ 3%*/然后再withdraw到另一个比特币账户上，最后在namecheap或者namesilo上购买域名，应该不会产生您之前所说的十几刀的手续费吧，而且TheCthulhu.com的Thomas White告诉我说namecheap几乎是匿名的因为不会double check信息，且支持比特币。如果有空的话你或许（用邮箱）可以告诉我一下你的域名大致是怎么买的吗？Google上搜不到enom bitcoin相关的信息：（公钥在我博客上。



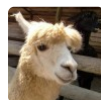
Xiaolan • 2016年03月24日 • Reply • 博主

确实是模仿了你的注释方法：）
域名的购买地址发到你的邮箱了....



CyberThink • 2016年03月24日 • Reply

看到你的邮件了，原来是这样啊，之前的确没想到：）
哦对，Twitter上的那个类似私聊的功能怎么样（消息内容应该不会被公开吧）？（我最近计算机被Seize了。。所以加解密邮件有点麻烦）或许可试试用twitter进行IM？



Xiaolan • 2016年03月26日 • Reply • 博主

可以.不过不是端对端加密....



gongminyu • 2016年03月31日 • Reply

很专业



Anonymous • 2016年04月07日 • Reply

如文设置后运行start，弹出cmd界面，显示：i2pd daemon starting和一个i2pd的窗口

然后就长期卡在这里不动了。

win7 64, i2pd_2.5.1_win64_mingw.zip

麻烦 你看下怎么回事？

谢谢



Xiaolan • 2016年04月18日 • Reply • 博主

能否发个截图呢？

无需Java使用I2P——I2Pd简单扫盲 – 中国数字时代 • 2016年04月07日 • Reply

[...] 最近收到朋友的来信让我写一篇关于i2p的文章,顺便博客也好久没更新都快长草了..那就写一篇关于i2pd的简介+扫盲文章吧...来源: <https://xiaolan.me/howtousei2pd.html> 什么是I2P? I2P是Tor的变种,比Tor网络更加安全、更据隐蔽性,如果你不知道Tor又是什么,请戳洋葱路由Tor。TOR和I2P共同点都是通过若干个节点将你的数据进行层层转包、加密,防止你的真实IP暴露。(摘自谷歌) I2P与Tor有什么区别? [...]



Anonymous • 2016年04月07日 • Reply

我xp,你的方案在i2pd_2.6.0_win32_mingw上出现错误:

Microsoft Visual C++ Runtime Library

Runtime Error!

Program: ...\My Documents\代理\I2Pd\i2pd_2.6.0_win32_mingw\i2pd.exe

This application has requested the Runtime to terminate it in an unusual way.
Please contact the application's support team for more information.

确定



Anonymous • 2016年04月07日 • Reply

PCX45.0.1访问你的网站显示: 安全连接失败



Anonymous • 2016年04月08日 • Reply

连接被重置

fireflyoo • 2016年04月13日 • Reply



不行啊..XP上运行崩溃..根本不能用..

Microsoft Visual C++ Runtime Library

Runtime Error!

Program: D:\Toolkit\i2pd\i2pd.exe

This application has requested the Runtime to terminate it in an unusual way.
Please contact the application's support team for more information.



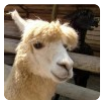
Xiaolan • 2016年04月18日 • Reply • 博主

需要安装VC++运行库...



caofengzi • 2016年04月17日 • Reply

藍總好，那個i2p啟動以後窗口一直在滾動是否已經運行成功？是否在補種？



Xiaolan • 2016年04月18日 • Reply • 博主

试试i2p网络能不能访问就可以了...

Leave a Reply

Your email address will not be published.

Comment

Name

Email

Website

Post Comment