# 洋葱头

## （Tor）

洋葱头既Tor（The Onion Router）是第二代洋葱路由（onion routing）的一种实现，用户通过Tor可以在[因特网](http://baike.baidu.com/item/%E5%9B%A0%E7%89%B9%E7%BD%91" \t "http://baike.baidu.com/item/%E6%B4%8B%E8%91%B1%E5%A4%B4/_blank)上进行匿名交流。

Tor（The Onion Router[1]  ）是第二代洋葱路由（onion routing）的一种实现，用户通过Tor可以在因特网上进行匿名交流。最初该项目由美国海军研究实验室（US Naval Research Laboratory）赞助。2004年的后期，Tor成为电子前哨基金会（Electronic Frontier Foundation，EFF）的一个项目。2005年后期，EFF不再赞助Tor项目，但他们继续维持Tor的官方网站。

Tor专门防范流量过滤、嗅探分析，让用户免受其害。Tor在由“onion routers”（洋葱）组成的表层网（overlay network）上进行通信，可以实现匿名对外连接、匿名隐藏服务。

Tor浏览器包

Tor浏览器包是一个免费的计算机应用程序，可以下载和使用，以避免互联网过滤。它可用来屏蔽一个互联网用户的IP地址，允许匿名浏览。Tor浏览器包是提供包括汉语在内的多国语言界面。

Tor用户在本机运行一个洋葱代理服务器（onion proxy），这个代理周期性地与其他Tor交流，从而在Tor网络中构成虚电路（virtual circuit）。Tor是在5层协议栈中的应用层进行加密（也就是按照'onion'的模式）。而它之所以被称为onion，是因为它的结构就跟洋葱相同，你只能看出它的外表，而想要看到核心，就必须把它层层的剥开。即每个路由器间的传输都经过对等密钥（symmetric key）来加密，形成有层次的结构。它中间所经过的各节点，都好像洋葱的一层皮，把客户端包在里面，算是保护信息来源的一种方式，这样在洋葱路由器之间可以保持通讯安全。同时对于客户端，洋葱代理服务器又作为SOCKS接口。一些应用程序就可以将Tor作为代理服务器，网络通讯就可以通过Tor的虚拟环路来进行。

进入Tor网络后，加密信息在路由器间层层传递，最后到达“出口节点”（exit node），明文数据从这个节点直接发往原来的目的地。对于目的地主机而言，是从“出口节点”发来信息。要注意的是明文信息即使在Tor网络中是加密的，离开Tor后仍然是明文的。维基解密创始人便声称其公开的某些文件是截获于Tor的出口节点。

由于在TCP数据流的级别通讯，Tor显得卓然独立于其他匿名网络。通过使用Tor，一般的应用程序都可以实现匿名，比如IRC、即时通讯，以及浏览网页。浏览网页时，Tor常常与Privoxy或Polipo等联合使用，Privoxy、Polipo是开源代理服务器，可以在应用层增加保护隐私。

由于Tor可以匿名进行[TCP](http://baike.baidu.com/item/TCP" \t "http://baike.baidu.com/item/%E6%B4%8B%E8%91%B1%E5%A4%B4/_blank)传输，这就导致了被滥用的可能。路由器存放有一个“出口政策”（*exit policy*），内有各种地址、端口的组合规定，通过这个来区别哪些传输可以通过这个节点而离开Tor网络，这样就可能防范许多滥用的可能。潜在的滥用包括：

P2P：抛开合法性不谈，如果通过Tor网络来进行大量数据的传输，这就有些不礼貌了，毕竟洋葱[路由器](http://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8" \t "http://baike.baidu.com/item/%E6%B4%8B%E8%91%B1%E5%A4%B4/_blank)是由志愿者，花费自己的带宽创建起来的。

E-mail：匿名的[SMTP](http://baike.baidu.com/item/SMTP" \t "http://baike.baidu.com/item/%E6%B4%8B%E8%91%B1%E5%A4%B4/_blank)很容易导致[垃圾邮件](http://baike.baidu.com/item/%E5%9E%83%E5%9C%BE%E9%82%AE%E4%BB%B6" \t "http://baike.baidu.com/item/%E6%B4%8B%E8%91%B1%E5%A4%B4/_blank)的产生，一般Tor节点的“出口政策”，都拒绝对外连接到端口25（smtp的端口）。

蓄意破坏：由于不会被识破，用户有时会利用Tor来对协作网站进行破坏，这导致许多的网站，决定部分限制对Tor的通讯。

T

Tor不仅可以提供客户端的匿名访问，Tor还可以提供服务器的匿名。通过使用Tor网络，用户可以维护位置不可知的服务器。当然如果要访问这个隐蔽的服务，客户端也得安装Tor。

通过Tor指定的顶级域名（Top Level Domain，TLD）.onion，可以访问其隐藏的服务。Tor网络可以识别自己的TLD，并自动路由到隐藏的服务。然后，隐藏的服务将请求交由标准的服务器软件进行处理，这个服务器软件应该预先进行配置，从而只侦听非公开的接口。如果这个服务还可以通过公共的因特网来访问，那也会受到相关连的攻击，这样就没有真正的隐藏起来。

Tor隐藏服务有个另外的好处，由于不需要公开的IP地址，服务就可以躲在防火墙和NAT背后。

Tor在中国大陆被许多人用于突破防火长城，这主要是因为中国大陆屏蔽了大量的海外网站和服务器。Tor会自动检测节点是否可达目标地址。如果返回错误无法到达，它会自动更换节点。相应地，这种技术也可以用在中国境外模拟中国境内的节点，以访问一些境外无法访问的内容。

而防火长城对于Tor一直没有很好的解决方法。现行比较有效的方法是对未使用[SSL](http://baike.baidu.com/item/SSL" \t "http://baike.baidu.com/item/%E6%B4%8B%E8%91%B1%E5%A4%B4/_blank)([HTTPS](http://baike.baidu.com/item/HTTPS" \t "http://baike.baidu.com/item/%E6%B4%8B%E8%91%B1%E5%A4%B4/_blank))加密的连接进行特征检测并重置连接，或对已知节点和[网桥](http://baike.baidu.com/item/%E7%BD%91%E6%A1%A5" \t "http://baike.baidu.com/item/%E6%B4%8B%E8%91%B1%E5%A4%B4/_blank)进行IP地址屏蔽，也有在中国境内创建Tor的虚假节点以对通过其传输的数据进行最大限度的审查。

作为反制，有部分大陆网民自发在中国境内建起网桥，帮助中国境内未能连接上Tor网络的用户连接。

2009年9月以后的一段时间内，使用的Tor的0.2.1.19版本，并不使用网桥的情况之下无法创建Tor的连接。然而使用的Tor的稳定版0.2.1.20，仍能够创建Tor的连接，突破网络封锁且不需要勾选“我的 ISP 阻挡了对 Tor 网络的连接”的选项，即使用网桥。从理论上来说，在使用网桥的情况下，Tor的总能创建连接，而不被封锁，因为网桥是可以动态更新的。

2010年6月3日前后的一段时间内，使用Tor的0.2.1.26版本，在使用Bridges的情况之下，创建Tor的连接也相当的困难，显示的信息是“创建Tor回路failed”，这说明防火长城成功侦测并截断了Tor的连接。但Tor的连接一旦创建后切断并不容易，所以Tor一旦成功创建连接后就无法被防火长城干扰。同年8月前后至今，Tor又可以连接上。据全球互联网自由联盟上的用户说，只要加一次网桥，接下来就可以轻松连上Tor网络。

但在2011年1月之后，据大陆的网民反映Tor即使更换了网桥也无法正常连接上，但事实上这是网桥已经被屏蔽的结果。对于长期频繁使用和连接Tor的用户来说，由于Tor会缓存节点路由信息，所以只要这些节点或网桥没被封锁，他们照样能正常使用Tor。

自2011年10月后，当中国的一个Tor客户端与美国的网桥中继创建连接，一个中国的数据探针会在15分钟周期内尝试与Tor进行SSL协商和重协商，但目的不是创建TCP连接。12月后这种行为停止 。