Tor

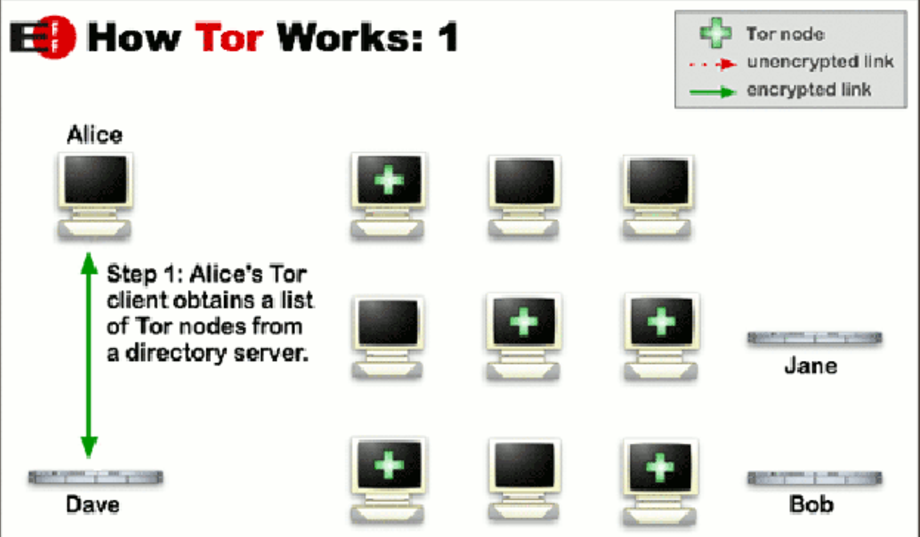
1.简介

Tor ，是英文The Onion Router 的缩写。意为“洋葱路由”。很多中国人最开始是试图寻找翻墙软件而了解到Tor 的。实际上，Tor 在设计之初并非用于翻墙，而是用来隐藏用户在网上的行踪的。使用Tor 上网，可以避免目标服务器、ISP 等获悉自己的IP 地址等信息。用户除了可以使用Tor 访问普通网站，也可以访问一些只有通Tor 才能访问的网站。“丝绸之路”就是其中最典型的一个。这些网站大多涉及毒品交易等违法行为，而警察极其难以破译Tor 的通讯来调查。

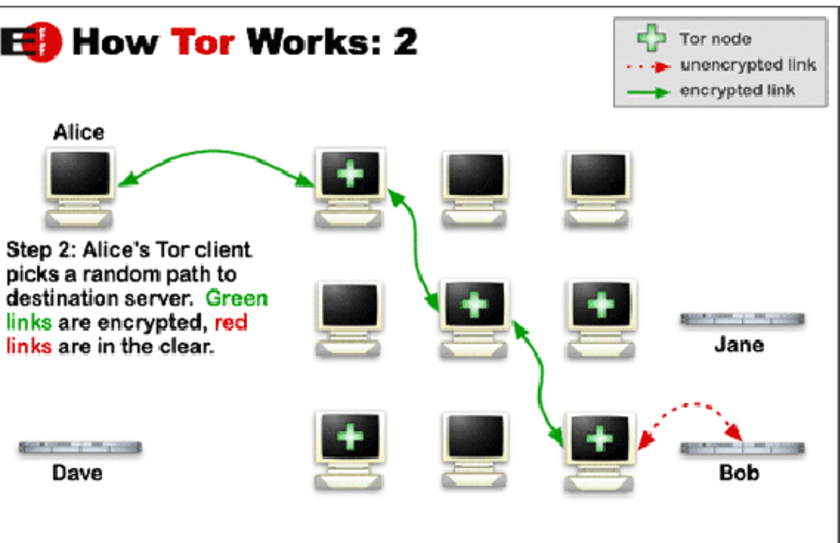
2.原理

Tor 工作的原理有些类似VPN 。传统的VPN 在传输数据的时候，需要通过一个中间服务器中转所有的数据，但与VPN 不同，Tor 需要3 个。

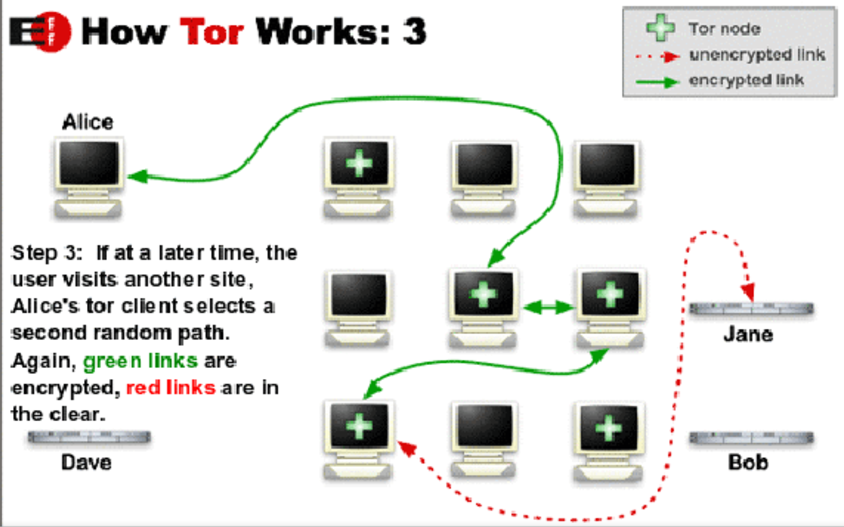
通常情况时，Tor 的工作方式如下：首先，Alice 的电脑会向一台服务器获取Tor 的节点。这些节点在图中是带有绿色加号的电脑。数据将经过这些节点



之后，Alice 会在获取到的Tor 节点当中随机选取三个。在下图中，Alice 直接连接的那台电脑（在最左侧）为入口节点，中间的为中间节点，最右侧的为出口节点。这个网站最后会通过出口节点的电脑访问，网站看到的IP 等信息都是出口节点的。出口节点会把数据通过中间节点，再通过入口节点传到Alice 的电脑。数据在经过前两个节点时都是加密的，只有出口节点才能够看到网站的内容。换句话说，出口节点的风险最大。



过一段时间，Tor 会继续随机挑选另外三个节点，使得出口节点只能看到一小片数据



这三个节点中的任意一个都无法获得用户完整的信息。入口节点无法看到网站内容，出口节点无法看到用户 IP 等信息，中间节点什么都看不到。如果网站是明文访问（使用HTTP ），那么出口节点存在着获取用户信息的风险；但是如果像是 Google 、Twitter、维基百科之类已经使用HTTPS 加密的网站，即使是出口节点也无法获知网站内容。环路上的中继仅仅知道它从哪一个中继接收数据以及向哪一个中继发送数据。没有一台单独的中继会知道数据包的完整路径。客户端与环路上的每一跳都协商一组独立的密钥，这样可以保证数据通过任何一跳时都无法跟踪。

不同于大多数商业VPN ，Tor 的所有节点都是由志愿者无私贡献的。因此，Tor 将永远免费，不过正因如此，在使用 Tor 的过程中，也要尽可能避免浪费珍贵的节点资源。