CIPHERSPACE/DARKNETS: ANONYMIZING NETWORKS

Adrian Crenshaw

About Adrian

- I run Irongeek.com
- I have an interest in InfoSec education
- I don't know everything - I'm just a geek with time on my hands
- (ir)Regular on the ISDPodcast http://www.isd-podcast.com/

A little background…

Darknets

- There are many definitions, but mine is "anonymizing private networks "
- Use of encryption and proxies (some times other peers) to obfuscate who is communicating to whom
- Sometimes referred to as Cipherspace (love that term)

Isn't the Internet anonymous enough? Not really

- IPs can be associated with ISPs
- Bills have to be paid
- Websites log IPs as a matter of course
- ISPs can look at their logs for who was leased an IP
- Lots of plain text protocols allow for easy sniffing

http://www.irongeek.com/i.php?page=security/ipinfo

http://www.irongeek.com/i.php?page=security/AQuickIntrotoSniffers

http://www.irongeek.com/i.php?page=videos/footprinting-scoping-and-recon-with-dns-google-hacking-and-metadata

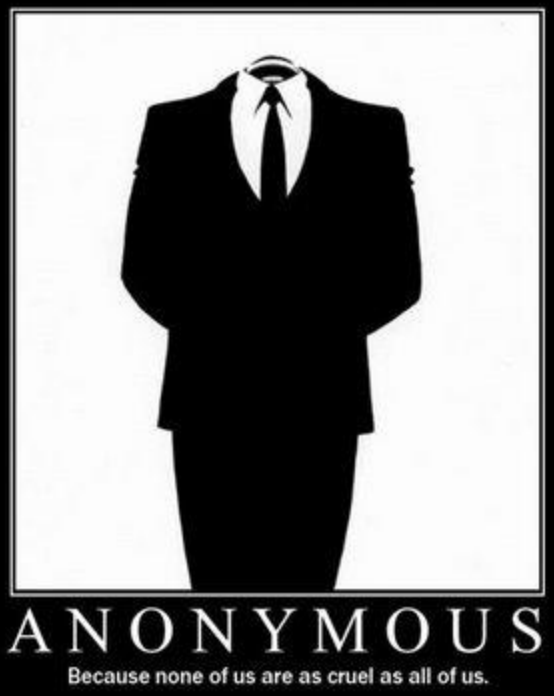
Who cares?

- Privacy enthusiasts and those worried about censorship
- Firms worried about policy compliance and leaked data
- Law enforcement

Average Citizen
Why do you care?

Do you want to stay anonymous?

- P2P
- Censorship
- Privacy



http://Irongeek.com

Corporations
Why do you care?

Is someone sneaking out private data?

- Trade secrets
- Personally identifiable information

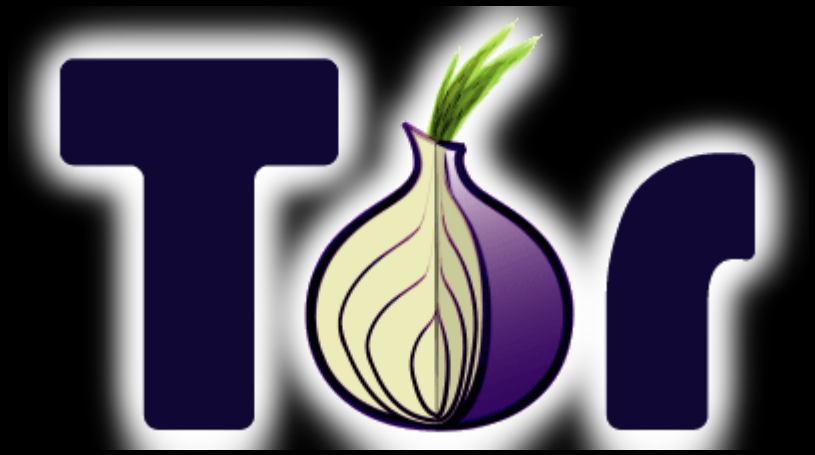
Law Enforcement
Why do you care?

Contraband and bad people?

- Criminals
- Terrorists
- Pedos

Some key terms

- Proxy
  Something that does something for something else
- Encryption
  Obfuscating a message with an algorithm and one or more keys
- Signing
  Using public key cryptography, a message can be verified based on a signature that in all likelihood had to be made by a signer that had the secret key
- Small world model
  Ever heard of six degrees of Kevin Bacon?



The Onion Router

http://Irongeek.com

Overview

- **Who?**
  First the US Naval Research Laboratory, then the EFF and now the Tor Project (501c3 non-profit).
  http://www.torproject.org/
- **Why?**
  "Tor is free software and an open network that helps you defend against a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security known as traffic analysis." ~ As defined by their site
- **What?**
  Access normal Internet sites anonymously, and Tor hidden services.
- **How?**
  Locally run SOCKS proxy that connects to the Tor network.

Layout to connect to Internet

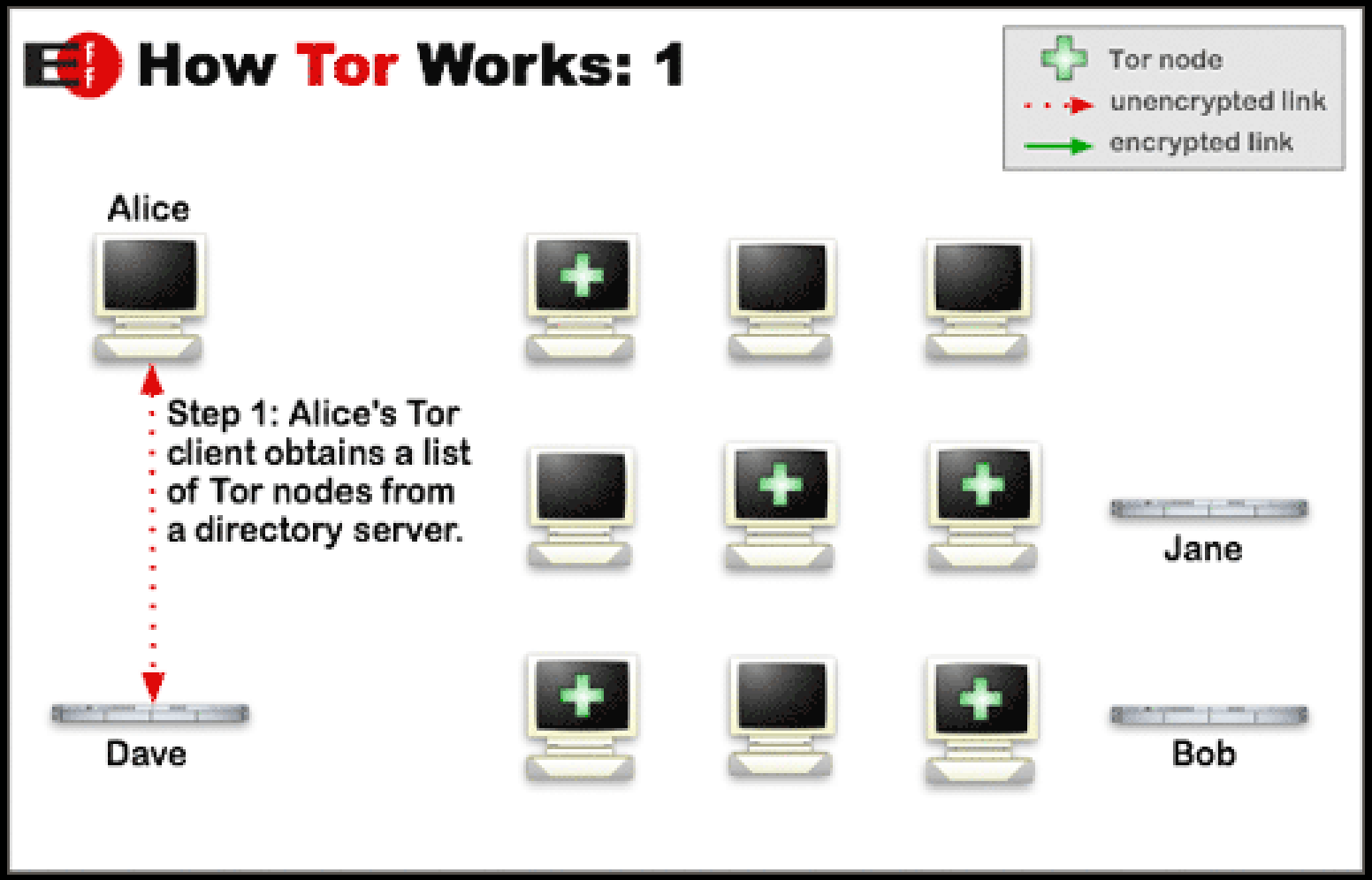


Image from http://www.torproject.org/overview.html.en

Layout to connect to Internet

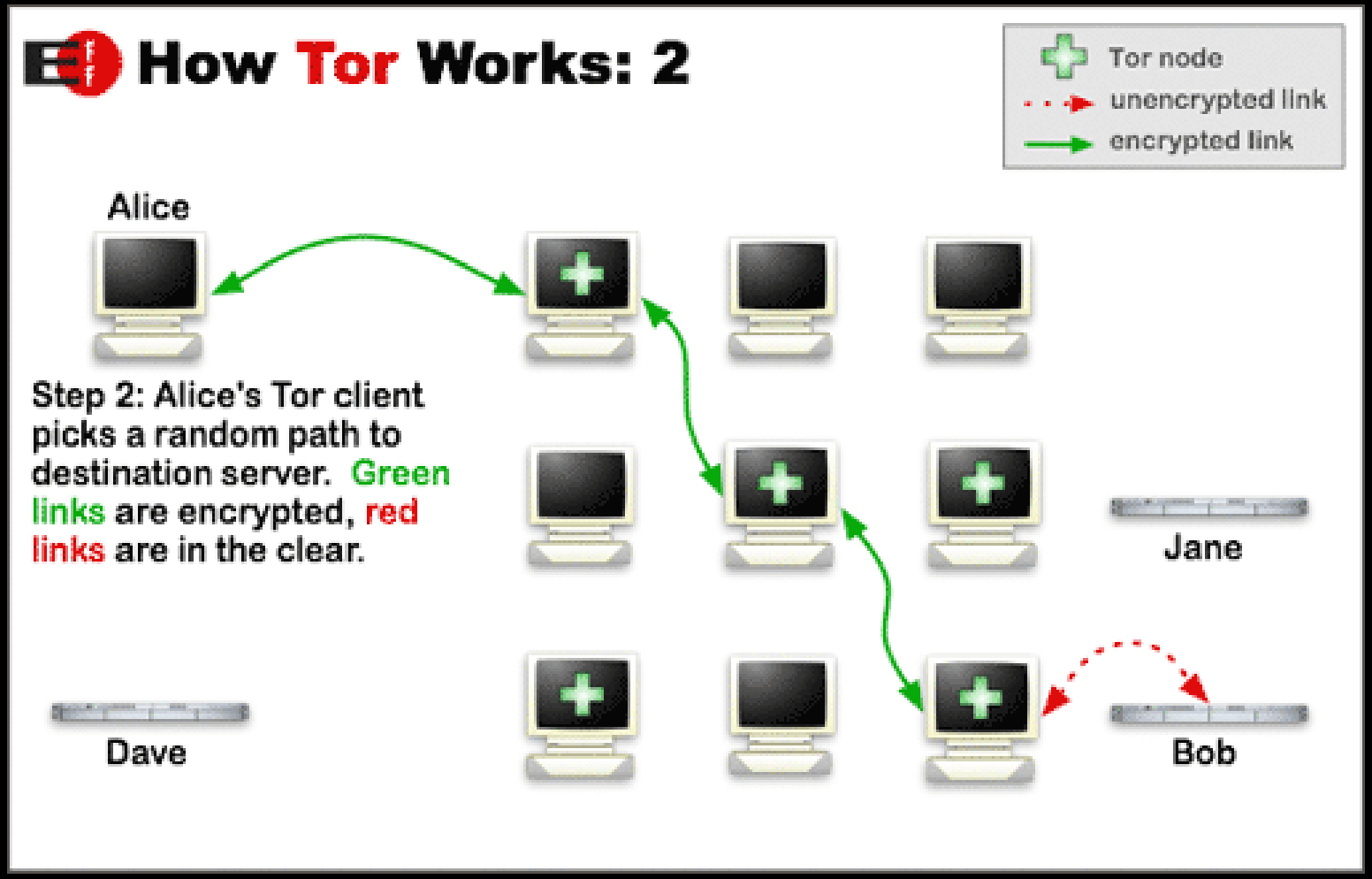


Image from http://www.torproject.org/overview.html.en

Layout to connect to Internet

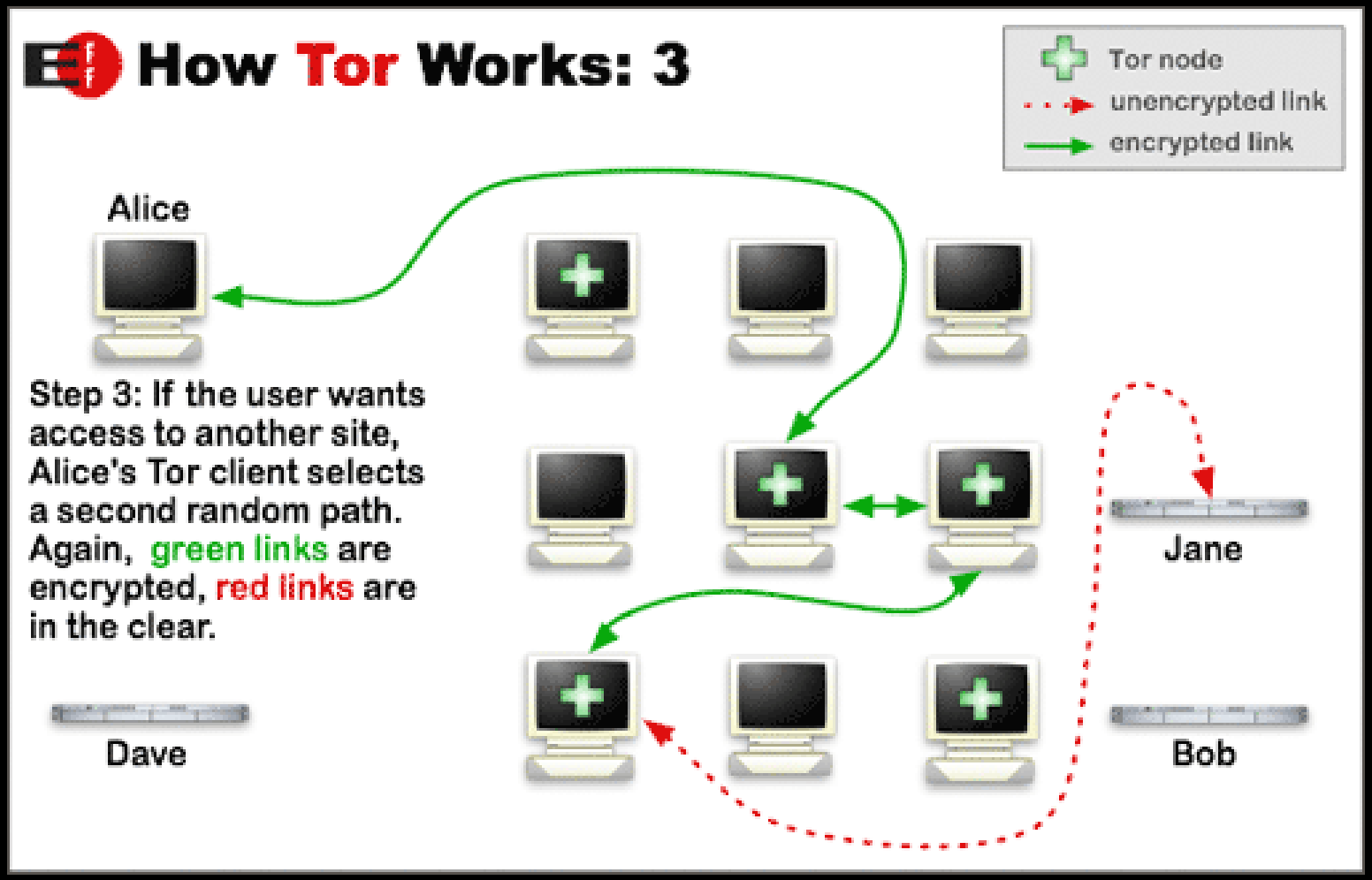


Image from http://www.torproject.org/overview.html.en

Layout to connect to Hidden Sevice

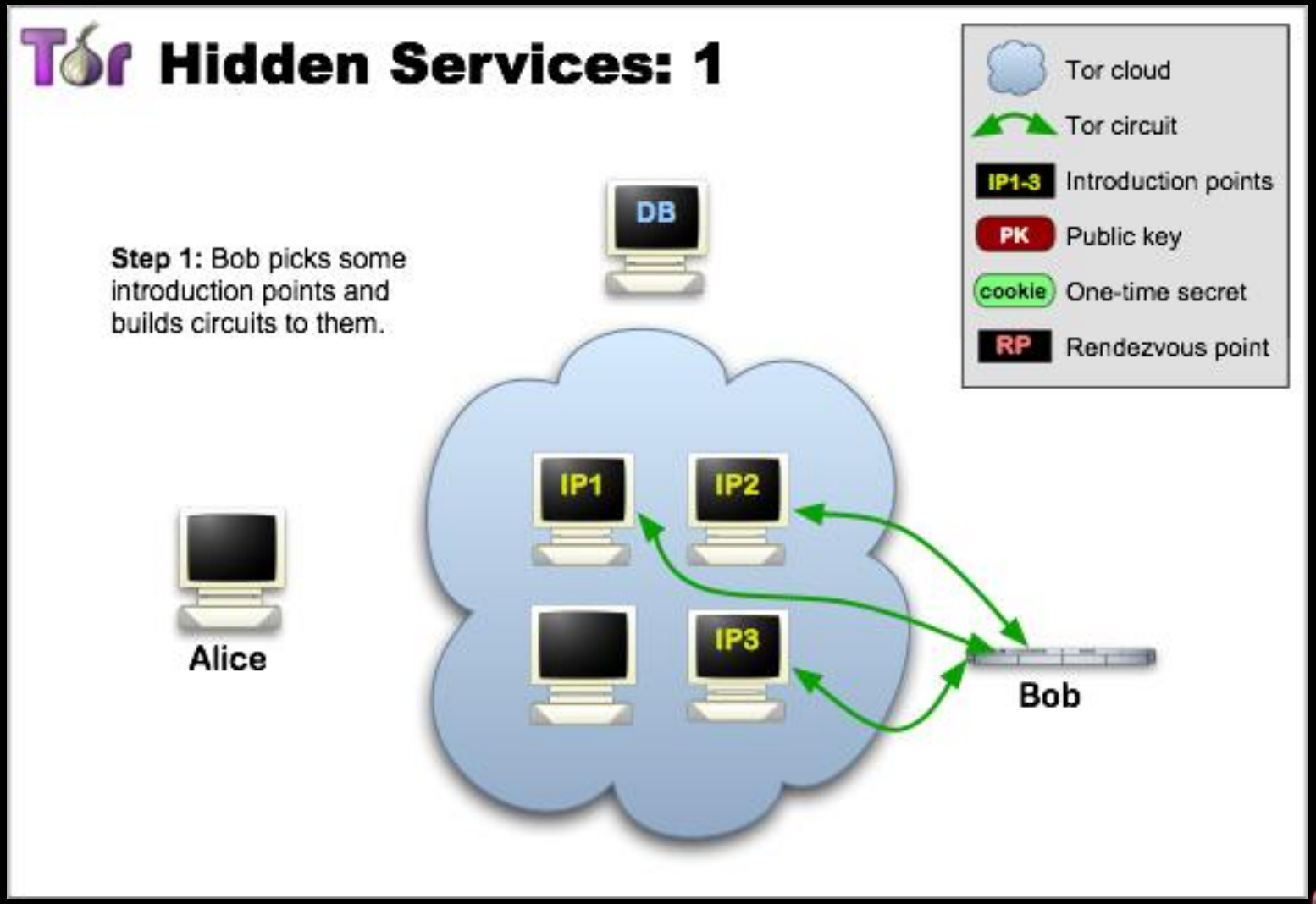


Image from http://www.torproject.org/hidden-services.html.en

Layout to connect to Hidden Sevice

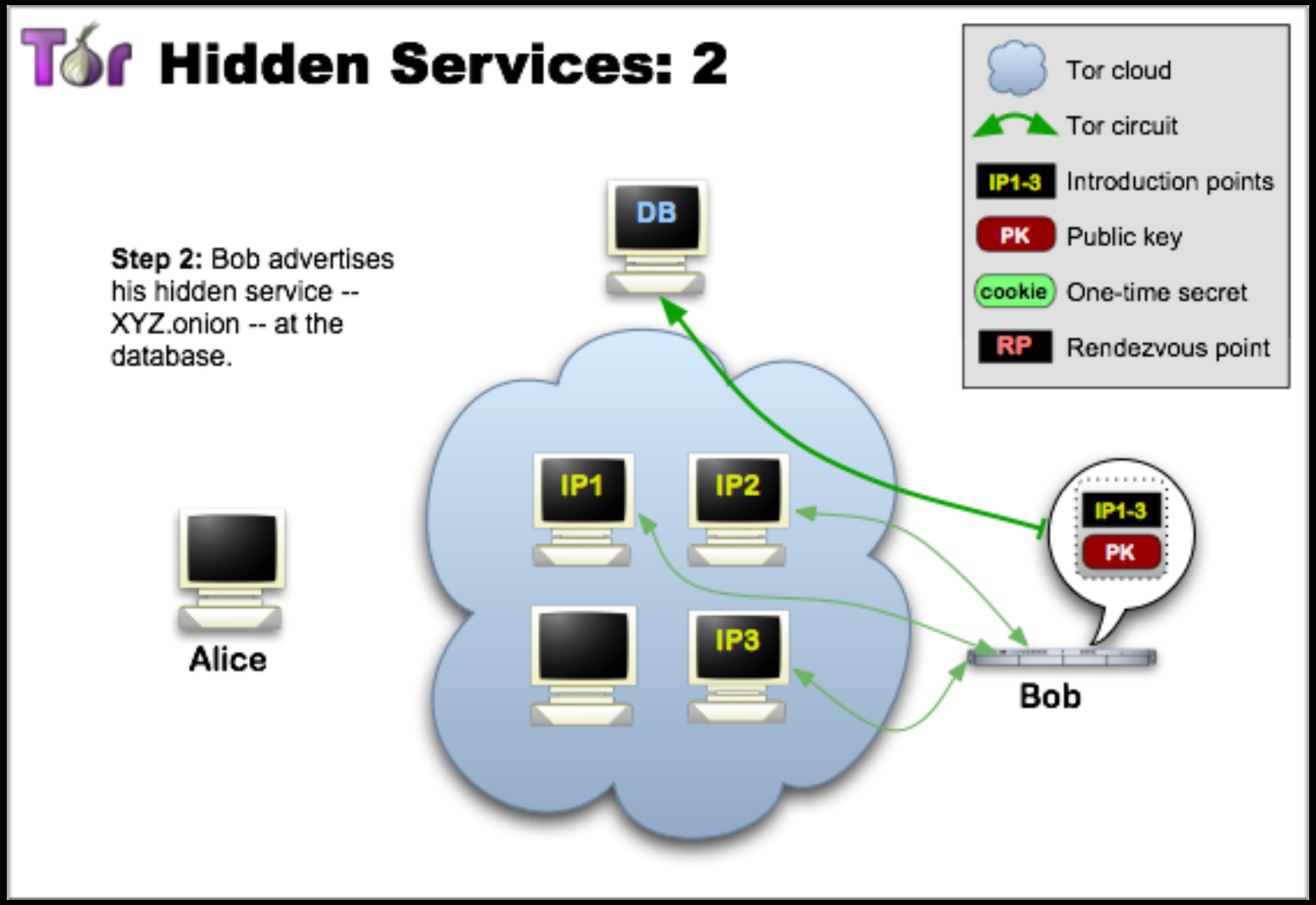


Image from http://www.torproject.org/hidden-services.html.en

Layout to connect to Hidden Sevice

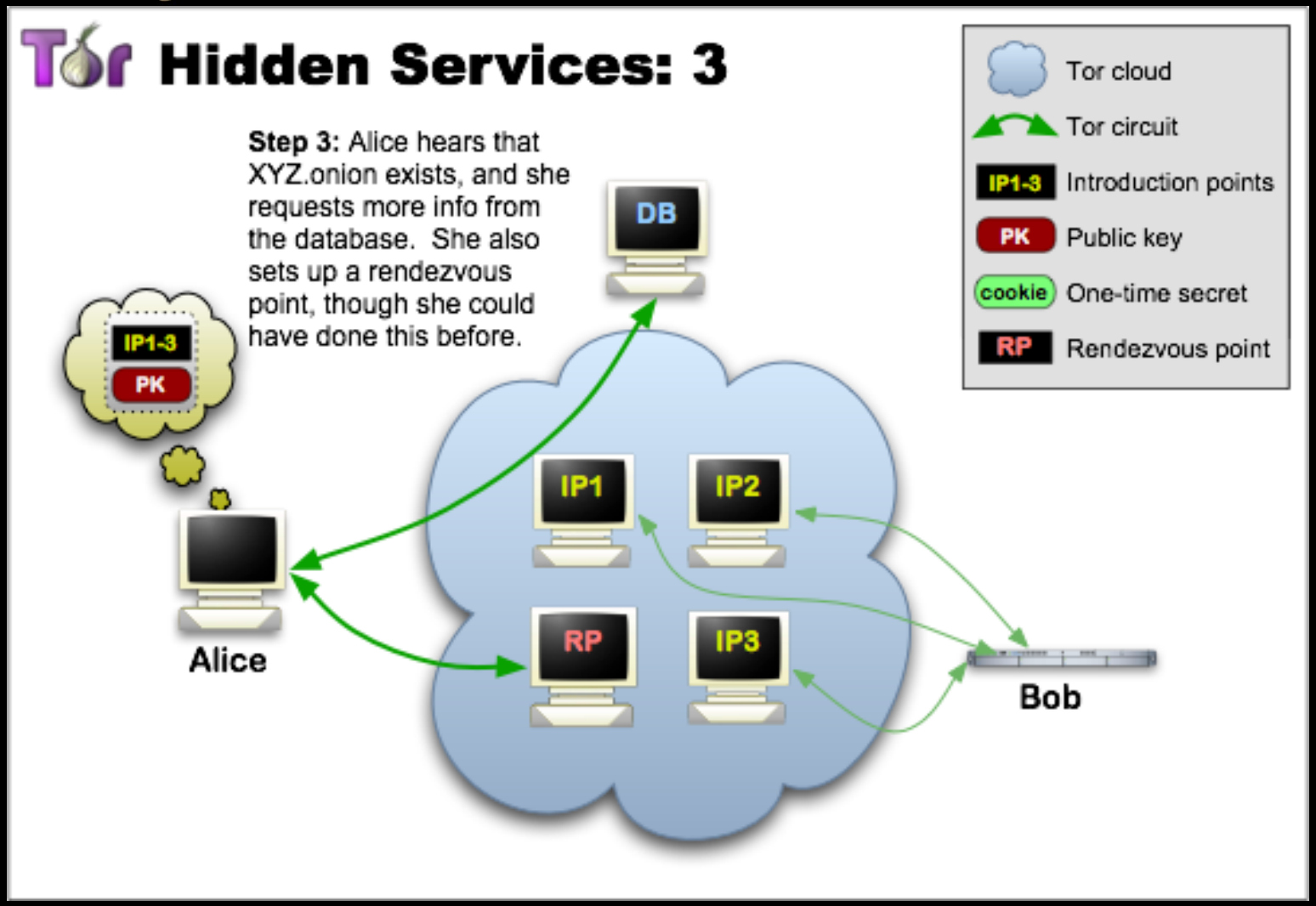


Image from http://www.torproject.org/hidden-services.html.en

Layout to connect to Hidden Sevice

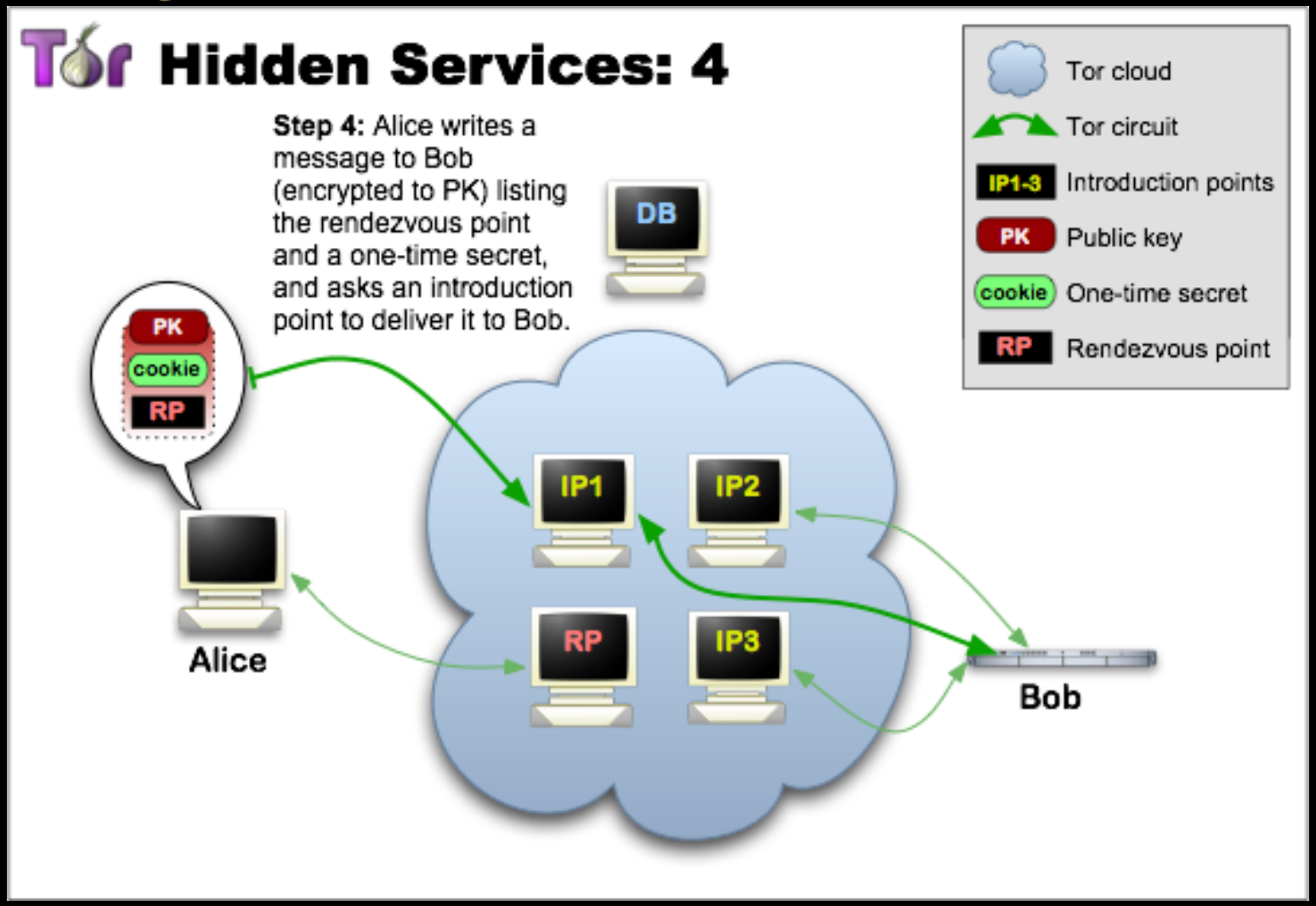


Image from http://www.torproject.org/hidden-services.html.en

Layout to connect to Hidden Sevice

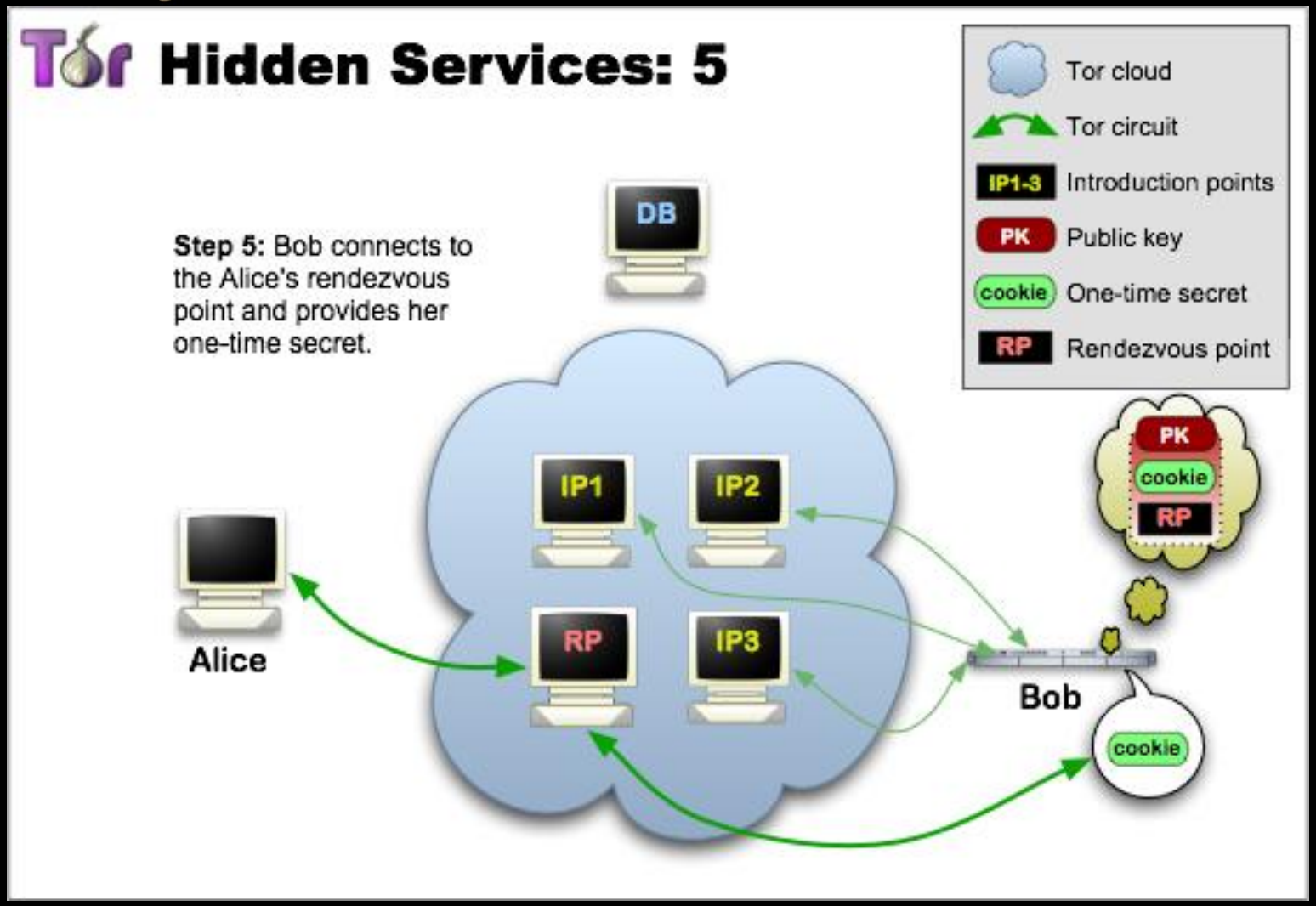


Image from http://www.torproject.org/hidden-services.html.en

Layout to connect to Hidden Sevice

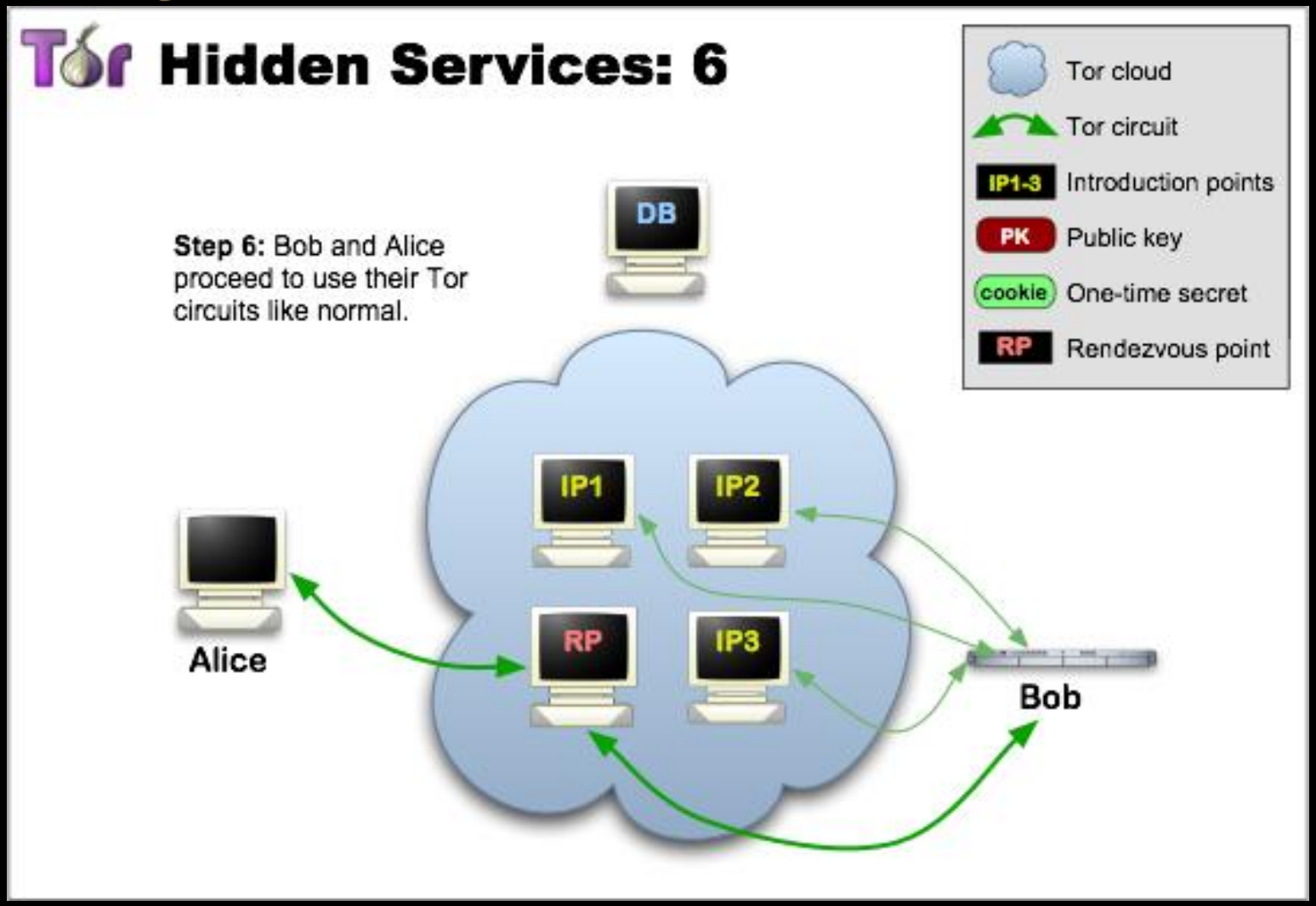


Image from http://www.torproject.org/hidden-services.html.en

Node types

- Client
  Just a user
- Relays
  These relay traffic, and can act as exit points
- Bridges
  Relays not advertised in the directory servers, so harder to block
- Guard Nodes
  Used to mitigate some traffic analysis attacks
- Introduction Points
  Helpers in making connections to hidden services
- Rendezvous Point
  Used for relaying/establishing connections to hidden services

What does it look like to the user?

Irongeek.com - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://www.irongeek.com/

Most Visited | Getting Started | Latest Headlines | Google | Google AdSense - Re... | Relaxing music, sleep...

Irongeek.com

Irongeek.com Hello Tor User :)

62.141.58.13
gpftor3.privacyfoundation.de
Windows NT 5.1
Mozilla/5.0 (Windows; U; Windows 5.1; en-US; rv:1.9.1.3) Gecko/2 Firefox/3.5.3 (.NET CLR 3.5.307
Amsterdam NL

Help Ironge
bandwidth and re

Ads by Google | It Security Jobs | Storage Security | Ag

Irongeek Security | Hacking Illustrated Videos | InfoSec Art
Reviews | RSS | Your IP | Podcasts | Hoosier Hackers
Nutrition | Supplements | Humor | Advertise | Hire Me
About

Sponsored by: SANS

Web Apps Performance
Better Manage Your Web Applications Read th
www.ca.com

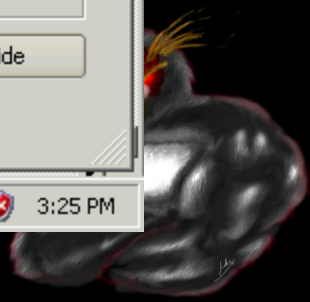
Vidalia Control Panel

Status
Connected to the Tor network!

Vidalia Shortcuts
Stop Tor | Setup Relaying
View the Network | Use a New Identity
Bandwidth Graph | Help | About
Message Log | Settings | Exit

Show this window on startup | Hide

Exotic_Liability_34.mp3 - ... | Vidalia Control Panel | 3:25 PM



http://Irongeek.com

Applications/Sites

- Anonymous proxy to the normal web
  http://www.irongeek.com/i.php?page=videos/tor-1
- Hidden services
  Normally websites, but can be just about any TCP connection
  http://www.irongeek.com/i.php?page=videos/tor-hidden-services
- Tor2Web Proxy
  http://tor2web.com
- Tor Hidden Wiki:
  http://kpvz7ki2v5agwt35.onion
- Onion Cat
  http://www.cypherpunk.at/onioncat/

Tor Pros and Cons

Pros

- If you can tunnel it through a SOCKS proxy, you can make just about any protocol work.
- Three levels of proxying, each node not knowing the one before last, makes things very anonymous.

Cons

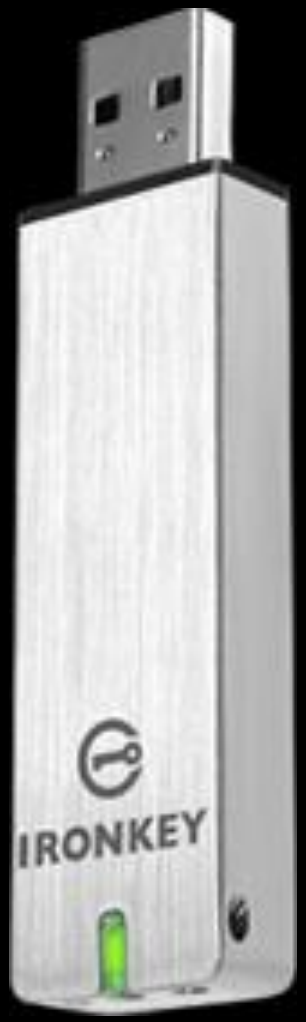
- Slow
- Do you trust your exit node?
- Semi-fixed Infrastructure:
  Sept 25th 2009, Great Firewall of China blocks 80% of Tor relays listed in the Directory, but all hail bridges!!!
  https://blog.torproject.org/blog/tor-partially-blocked-china
  http://yro.slashdot.org/story/09/10/15/1910229/China-Strangles-Tor-Ahead-of-National-Day
- Fairly easy to tell someone is using it from the server side
  http://www.irongeek.com/i.php?page=security/detect-tor-exit-node-in-php

What does the traffic look like?

(Keep in mind, this is just the defaults)

- Local
  9050/tcp Tor SOCKS proxy
  9051/tcp Tor control port
  8118/tcp Polipo
- Remote
  443/tcp and 80/tcp mostly
  Servers may also listen on port 9001/tcp, and directory information on 9030.
- More details
  http://www.irongeek.com/i.php?page=security/detect-tor-exit-node-in-php
  http://www.room362.com/tor-the-yin-or-the-yang

Private Tor based network



- Ironkey's Secure Sessions
  https://www.ironkey.com/private-surfing
- Much faster than the public Tor network
- How much do you trust the company?

ANONET

Roll your own, with OpenVPN and BGP routers

http://Irongeek.com

Overview

- **Who?**

  AnoNet 1/2: Good question
  http://www.anonet2.org
  http://anonetnfo.brinkster.net

- **Why?**

  To run a separate semi-anonymous network based on normal Internet protocols. Started using 1.0.0.0/8 because it was unused at the time, but that was allocated January 2010 to APNIC.

- **What?**

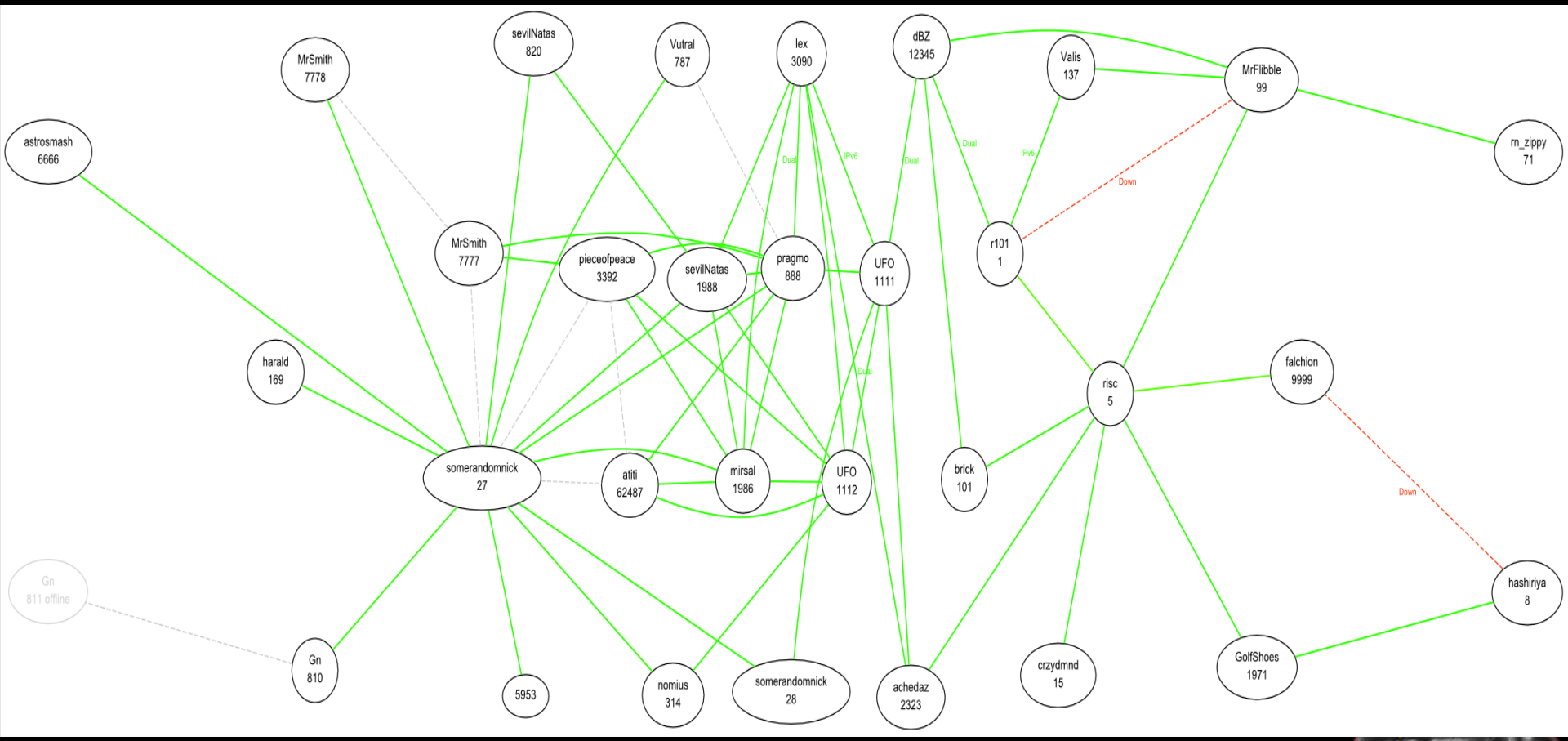
  Other sites and services internal to the network, but gateways to the public Internet are possible.

- **How?**

  OpenVPN connection to the network. Peering could be done with other VPN like tinc or QuickTun.

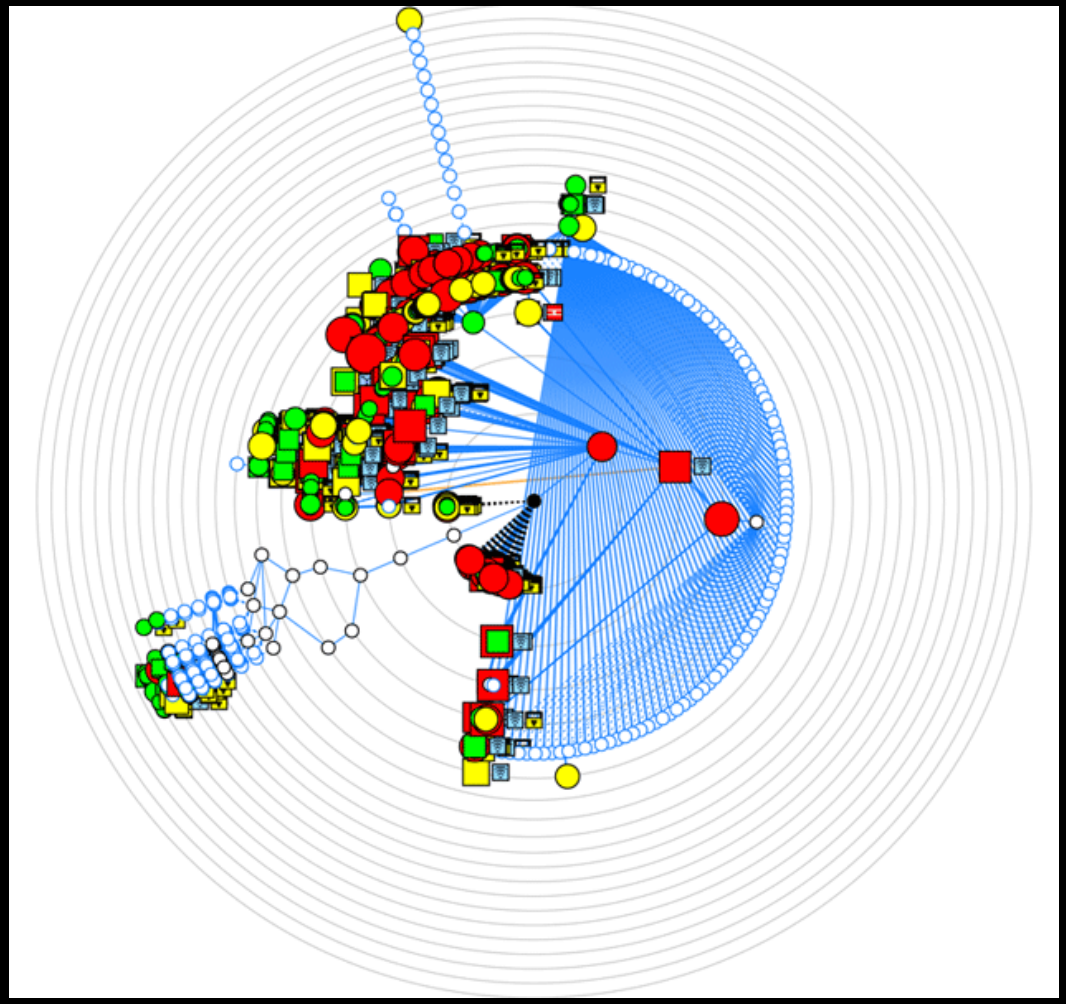
BGP peering and routing

- From: http://1.3.9.1/.stats/anonet.svg



Nmap scan using UFO client port

- Thanks to Alex Kah of Question-defense.com for the render, my computer had issues. ☺



Tools links to get started

- Read
  http://www.anonet2.org/
- Client ports
  (UFO client port)
  http://ix.ucis.nl/clientport.php
- OpenVPN
  http://openvpn.net/
- VNE/DNRouter
  http://wiki.ucis.nl/VNE/DNRouter
- QuickTun
  http://wiki.gontrol.nl/QuickTun
- HTTP access to the git repository
  http://anogit.ucis.ano/
- Outside access via Internet proxy
  http://powerfulproxy.com/
- List of some services
  http://www.anonet2.org/services/
  http://www.sevilnatas.ano/

Anonet and DarkNET Conglomeration Pros and Cons

Pros

- Fast
- Just about any IP based protocol can be used

Cons

- Not as anonymous as Tor since peers “know” each other
- Not a lot of services out there (DC)
- Entry points seem to drop out of existence (AN)

What does the traffic look like?

(Keep in mind, this is just the defaults)

- Whatever the OpenVPN clients and servers are configured for. I've seen:
- AnoNet
  5555/tcp
  5550/tvp
  22/tcp

Similar networks

- Darknet Conglomeration
  http://darknet.me
- Dn42
  https://dn42.net
- VAnet
  http://www.vanet.org
- ChaosVPN
  http://wiki.hamburg.ccc.de/index.php/ChaosVPN
  http://chaosvpn.net
  http://www.youtube.com/watch?v=Lx2w9K6a6EE

FREENET

All the world will be your enemy, Prince of a Thousand enemies. And when they catch you, they will kill you. But first they must catch you…

~ Watership Down

http://Irongeek.com

Overview

- **Who?**

  The Freenet Project, but started by Ian Clarke.
  http://freenetproject.org/

- **Why?**

  "Freenet is free software which lets you anonymously share files, browse and publish "freesites" (web sites accessible only through Freenet) and chat on forums, without fear of censorship."

- **What?**

  Documents and Freenet Websites for the most part, but with some extensibility.

- **How?**

  Locally run proxy of a sort (FProxy) that you can connect to and control via a web browser.

Layout

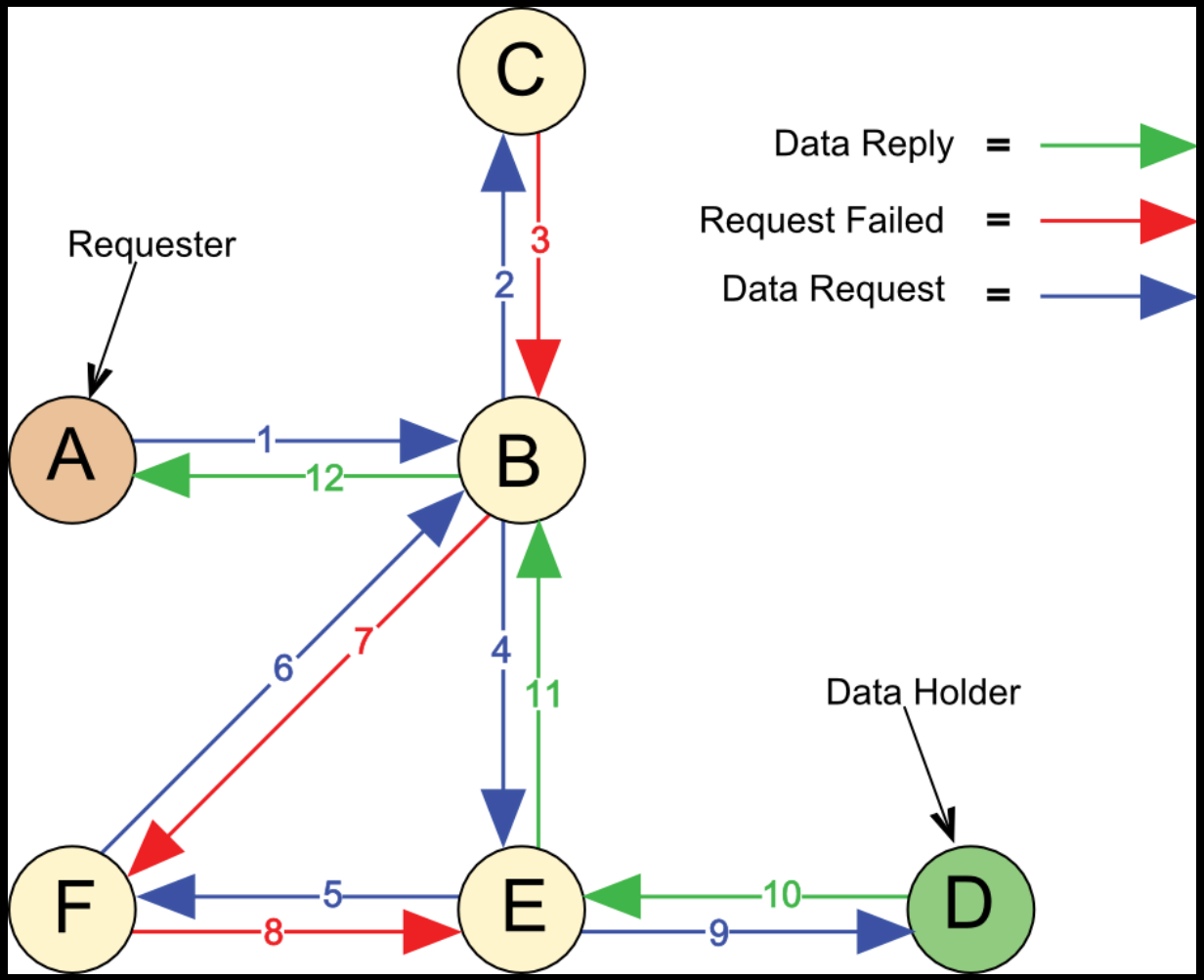


Image from http://en.wikipedia.org/wiki/File:Freenet_Request_Sequence_ZP.svg

What does it look like to the user?

Browse Freenet (Node id|-1349278091658394251) - Freenet - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://127.0.0.1:8888/

Most Visited | Getting Started | Latest Headlines | Google | Google AdSense - Re... | Relaxing music, sleep...

Browse Freenet (Node id|-13492780...

Browse Freenet (Node id|-1349278091658394251)

English | Switch to advanced mode | Security levels: NORMAL LOW LOW | 40 Peers

Browsing | Filesharing | Friends | Discussion | Status | Configuration

Search Freenet

Searching can be slow at the moment, so this will open a new window for the search, you should have a look at the index sites below while you wait for the search to complete.

Search Freenet!

Freesite subscriptions[Edit]

Indexes of freesites (in-Freenet web sites)

The Ultimate FreeNet Index

Freenet Activelink Index Text Version (should load relatively quickly)

Freenet Activelink Index (SLOW: graphical index, preloads all the sites, so takes *ages* to load)

Done | Proxy: Tor

Key types

- URI Example:
  http://127.0.0.1:8888/USK@0I8gctpUE32CM0iQhXaYpCMvtPPGfT4pjXm01oid5Zc,3dAcn4fX2LyxO6uCnWFTx-2HKZ89uruurcKwLSCxbZ4,AQACAAE/Ultimate-Freenet-Index/52/

- **CHK** - Content Hash Keys
  These keys are for static content, and the key is a hash of the content.
- **SSK** - Signed Subspace Keys
  Used for sites that could change over time, it is signed by the publisher of the content. Largely superseded by USKs.
- **USK** - Updateable Subspace Keys
  Really just a friendly wrapper for SSKs to handle versions of a document.
- **KSK** - Keyword Signed Keys
  Easy to remember because of simple keys like “KSK@myfile.txt” but there can be name collisions.

Modes of operation

- Opennet
  Lets any one in

- Darknet
  Manually configured “friend to friend”

Applications

- jSite
  A tool to create your own Freenet site
  http://freenetproject.org/jsite.html
- Freemail
  Email system for Freenet
  http://freenetproject.org/freemail.html
- Frost
  Provides usenet/forum like functionality
  http://jtcfrost.sourceforge.net/
- Thaw
  For file sharing
  http://freenetproject.org/thaw.html

Freenet Pros and Cons

Pros

- Once you inject something into the network, it can stay there as long as it is routinely requested
- Does a damn good job of keeping one anonymous
- Awesome for publishing documents without maintaining a server

Cons

- Slow
- Not really interactive
- Not used for accessing the public Internet
- UDP based, which may be somewhat more noticeable/NAT issues
- Not meant for standard IP protocols

What does the traffic look like?

(Keep in mind, this is just the defaults)

- Local

  FProxy: 8888/TCP (web interface)

  FCP: 9481

- Remote

  Random UDP for Opennet and Darknet modes?

~~Darknet FNP: 37439/UDP (used to connect to trusted peers i.e. Friends; forward this port if you can)~~

~~Opennet FNP: 5980/UDP (used to connect to untrusted peers i.e. Strangers; forward this port if you can)~~

~~FCP: 9481/TCP (for Freenet clients such as Frost and Thaw)~~

I2P

Invisible Internet Project

http://Irongeek.com

Overview

- **Who?**

  I2P developers, started by Jrandom.
  http://www.i2p2.de/

- **Why?**

  "I2P is an effort to build, deploy, and maintain a network to support secure and anonymous communication. People using I2P are in control of the tradeoffs between anonymity, reliability, bandwidth usage, and latency." ~ from the I2p web site

- **What?**

  Mostly other web sites on I2P (Eepsites), but the protocol allows for P2P (iMule, i2psnark), anonymous email and public Internet via out proxies.

- **How?**

  Locally ran proxy of a sort that you can connect to and control via a web browser.

Layout

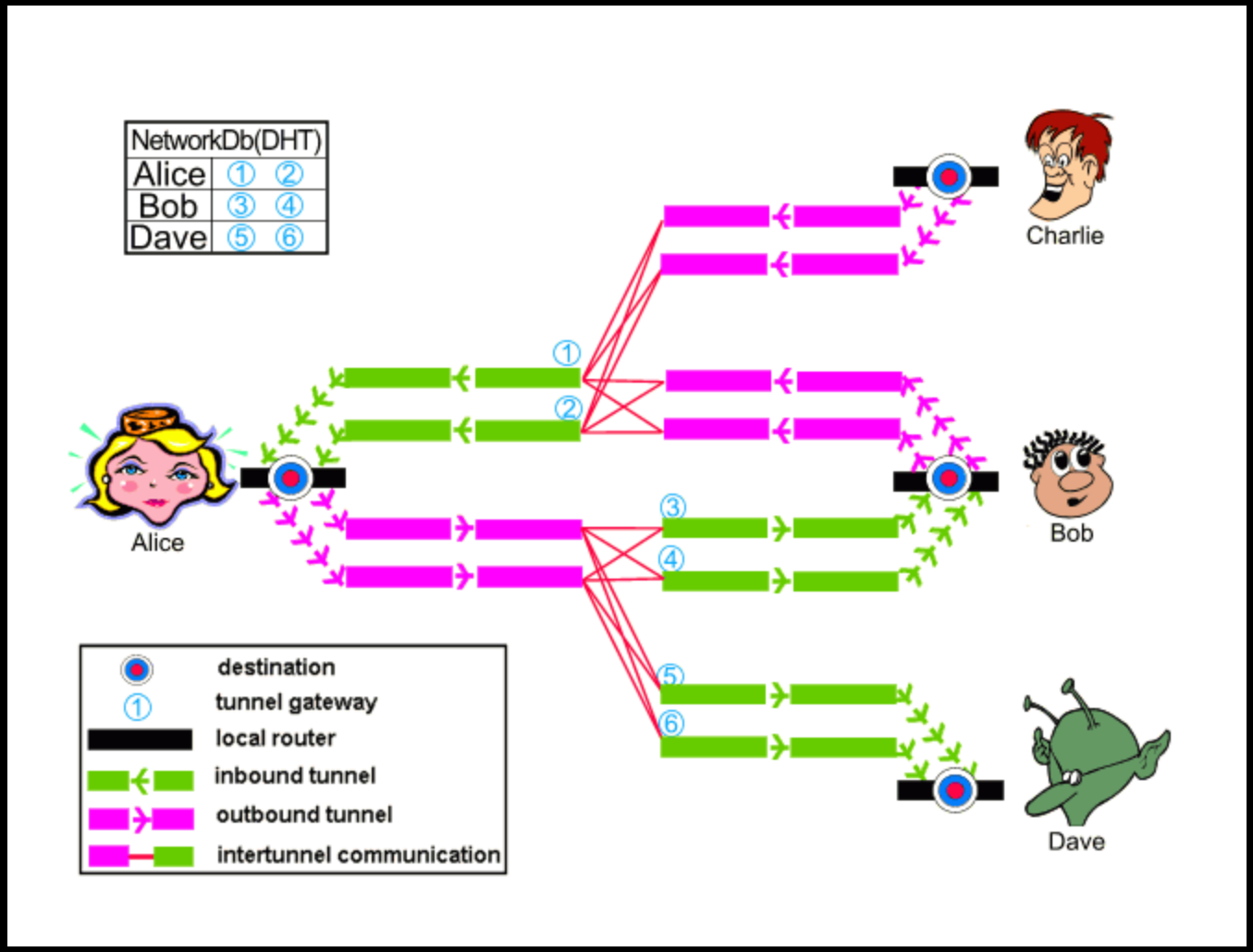


Image from http://www.i2p2.de/how_intro

Encryption Layers

- ElGamal/SessionTag+AES from A to H
- Private Key AES from A to D and E to H
- Diffie–Hellman/Station-To-Station protocol + AES

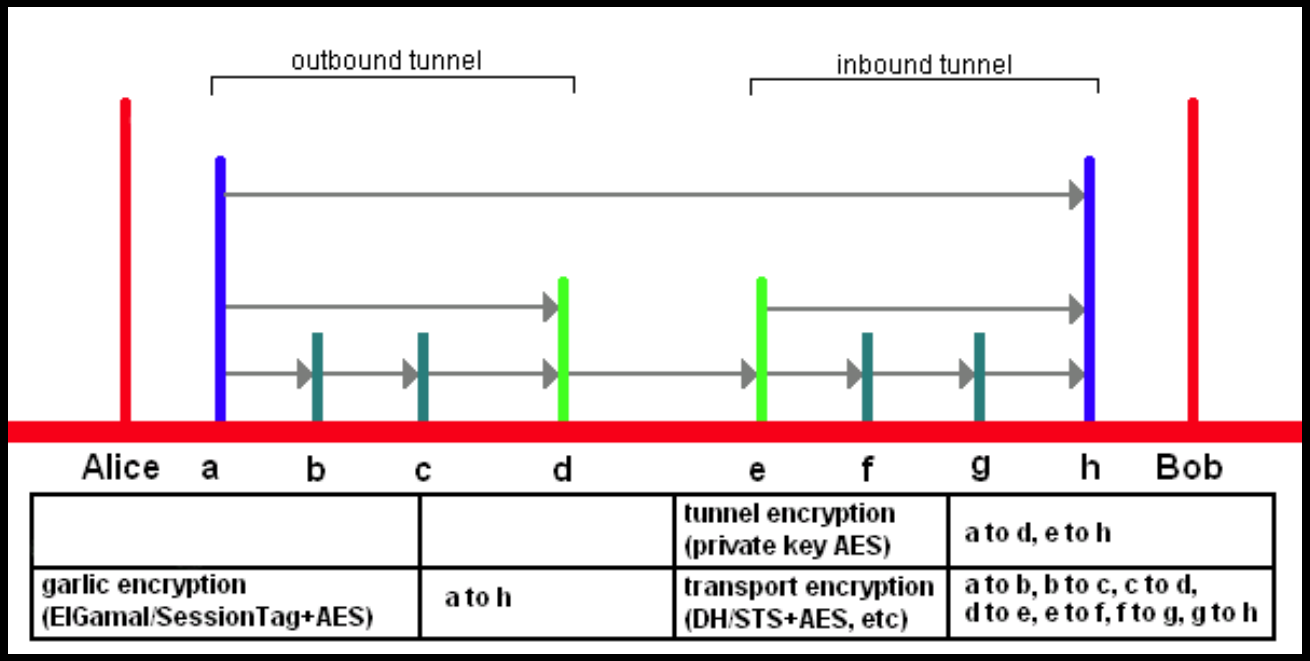
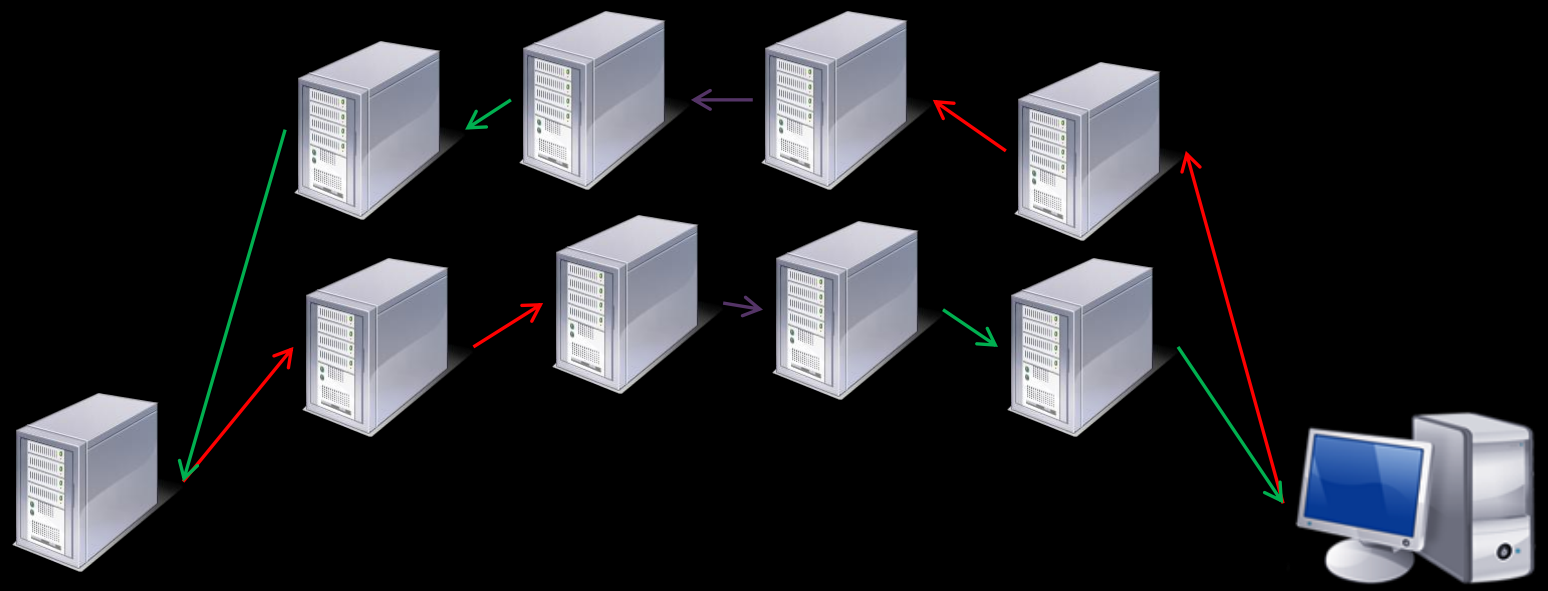


Image from http://www.i2p2.de/

Ins and Outs

- Tunnels are not bidirectional



What does it look like to the user?

I2P Router Console - home - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://127.0.0.1:7657/index.jsp

Most Visited | Learn more about Tor | The Tor Blog | I2P Router Console - ... | Privacy | I2P | YaCy 'Eyacylator': Se...

Proxy: I2P HTTP | Apply | Status: Using I2P HTTP | Manage Proxies | Preferences

I2P Router Console - home

I2P

HELP & FAQ

I2P SERVICES

Addressbook Torrents Webmail Webserver

I2P INTERNALS

Tunnels Peers Profiles NetDB Logs Graphs Stats I2PTunnel

GENERAL

Local Identity: show
Version: 0.8.2-0
Uptime: 29 hours

Network: OK

Restart | Shutdown

PEERS

I2P ROUTER CONSOLE

2011-01-08: Tahoe-LAFS I2P released

The I2P release of the decentralized data store Tahoe-LAFS has been synchronized with upstream version 1.8.1 (and Foolscap 0.6.0). It is still in testing and a windows client is not yet released. Please join us on the #tahoe-lafs IRC channel for support and feedback.

2010-12-22: 0.8.2 Released

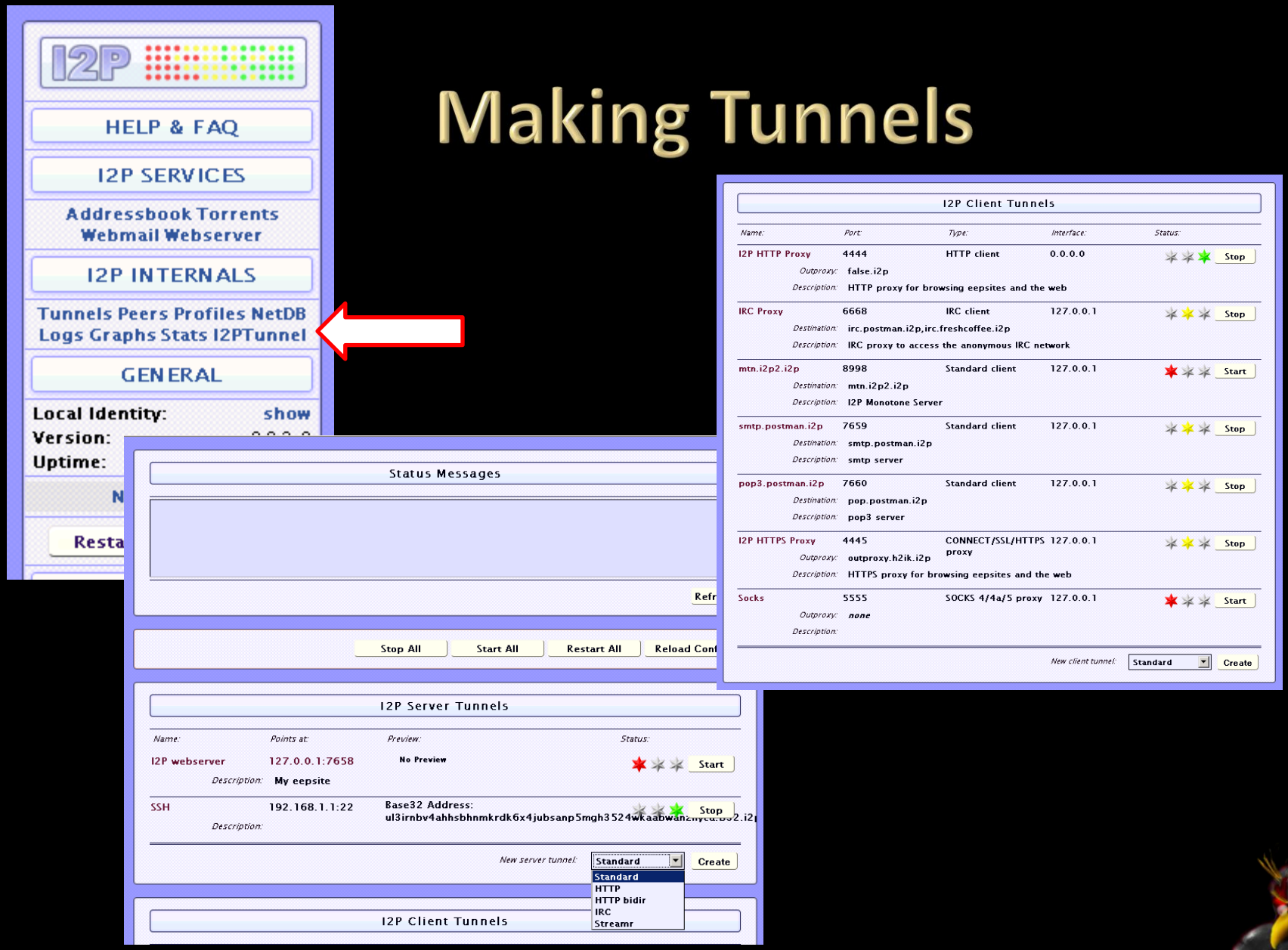
The 0.8.2 release includes extensive bug fixes and theme updates in the router and in i2psnark. There are also optimizations to reduce memory usage in i2psnark. The HTTP and SOCKS proxies now support local and remote authorization. As usual, upgrading is recommended.

I2P will be at 27C3 in Berlin the week of December 27th. Look for the I2P people there and ask for I2P stickers!

Please help grow the network. Say hello to the volunteers on the **#i2p-help IRC channel**. **Get involved**, spread the word, and **donate**! If you find a bug, please enter a report on **trac**. We are still looking for volunteers to work on new and existing translations. Please volunteer on **IRC #i2p**.

Done | Tor Disabled | Proxy: I2P HTTP

Making Tunnels



http://Irongeek.com

Making Tunnels

- Simple SOCKS client tunnel

I2P Tunnel Manager - Edit Client Tunnel - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://127.0.0.1:7657/i2ptunnel/edit?tunnel=7

Most Visited | Learn more about Tor | The Tor Blog | I2P Router Console - ... | Privacy | I2P | YaCy 'Eyacylator': Se... | The Hidden Wiki

Proxy: I2P HTTP | Apply | Status: Using I2P HTTP | Manage Proxies | Preferences

I2P Router Console - home | I2P Tunnel Manager - Edit Client ... | I2P Tunnel Manager - List

Edit proxy settings

Name:(N) Socks

Type: SOCKS 4/4a/5 proxy

Description:(E)

Access Point: Port: 5555

Reachable by(R): Locally (127.0.0.1)

Other(O):

Outproxies(x):

Shared Client(h): (Share tunnels with other clients and irc/httpclients? Change requires restart of client proxy)

Auto Start(A): (Check the Box for 'YES')

Advanced networking options

(NOTE: when this client proxy is configured to share tunnels, then these options are for all the shared proxy clients!)

Tunnel Options: Length(t): 2 hop tunnel (high anonymity, high latency) Variance(V): 0 hop variance (no randomisation, con

Count(C): 2 inbound, 2 outbound tunnels (standard b Backup Count(B): 0 backup tunnels (0 redundancy, no ad

Profile(f): bulk connection (downloads/websites/BT)

Delay Connect(y): (for request/response connections)

I2CP Options: Host(o): 127.0.0.1 Port(r): 7654

Reduce tunnel quantity when idle(d): Enable: Reduced tunnel count: 1 Idle minutes: 20

Done | Tor Disabled | Proxy: I2P HTTP

Making Tunnels

- SSH Example

I2P Tunnel Manager - Edit Server Tunnel - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://127.0.0.1:7657/i2ptunnel/edit?tunnel=8

Most Visited | Learn more about Tor | The Tor Blog | I2P Router Console - ... | Privacy | I2P | YaCy 'Eyacylator': Se... | The Hidden Wiki

Proxy: I2P HTTP | Apply | Status: Using I2P HTTP | Manage Proxies | Preferences

I2P Router Console - home | I2P Tunnel Manager - Edit Server...

Edit server settings

Name(N): SSH

Type: Standard server

Description(e):

Auto Start(A): (Check the Box for 'YES')

Target: Host(H): 192.168.1.1 Port(P): 22

Private key file(k): i2ptunnel8-privkeys.dat

Local destination(L): sCA0k5hzw9FnpsqfPw08KXt4IgStktW54jyHSbEMhXtlpKkjFYUNvXxvlcLCYll

Add to local addressbook

Advanced networking options

Tunnel Options: Length(t): 2 hop tunnel (high anonymity, high latency) Variance(V): 0 hop variance (no randomisation, con

Count(C): 2 inbound, 2 outbound tunnels (standard b Backup Count(B): 0 backup tunnels (0 redundancy, no ad

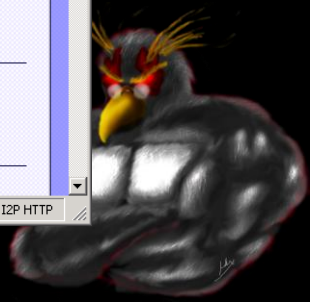
Profile(f): bulk connection (downloads/websites/BT)

I2CP Options: Host(o): 127.0.0.1 Port(r): 7654

Encrypt Leaseset(E): Enable: Encryption Key: Generate New Key: Generate (Tunnel must be stopped first)

Restricted Access List(s): Enable: Access List: (Restrict to these

Done | Tor Disabled | Proxy: I2P HTTP



Naming and Addresses

- Details
  http://www.i2p2.de/naming.html
- 516 Character Address
  -KR6qyfPWXoN~F3UzzYSMIsaRy4udcRkHu2Dx9syXSzUQXQdi2Af1TV2UMH3PpPuNu-GwrqihwmLSkPFg4fv4y
  QQY3E10VeQVuI67dn5vlan3NGMsjqxoXTSHHt7C3nX3szXK90JSoO~tRMDl1xyqtKm94-RpIyNcLXofd0H6b02
  683CQIjb-7JiCpDD0zharm6SU54rhdisIUVXpi1xYgg2pKVpssL~KCp7RAGzpt2rSgz~RHFsecqGBeFwJdiko-
  6CYW~tcBcigM8ea57LK7JjCFVhOoYTqgk95AG04-hfehnmBtuAFHWklFyFh88x6mS9sbVPvi-am4La0G0jvUJw
  9a3wQ67jMr6KWQ~w~bFe~FDqoZqVXl8t88qHPIvXelvWw2Y8EMSF5PJhWw~AZfoWOA5VQVYvcmGzZIEKtFGE7b
  gQf3rFtJ2FAtig9XXBsoLisHbJgeVb29Ew5E7bkwxvEe9NYkIqvrKvUAt1i55we0Nkt6xlEdhBqg6xXOyIAAAA
- SusiDNS Names
  something.i2p
- Hosts.txt and Jump Services
- Base32 Address
  {52 chars}.b32.i2p
  rjxwbsw4zjhv4zsplma6jmf5nr24e4ymvvbycd3swgiinbvg7oga.b32.i2p

Applications/Sites

Services

IRC on 127.0.0.1 port 6668

Syndie

Bittorent
http://127.0.0.1:7657/i2psnark /

eMule/iMule
http://echelon.i2p/imule/

Tahoe-LAFS

More plugins at
http://i2plugins.i2p/

Susimail
http://127.0.0.1:7657/susimail

Garlic Cat
http://www.cypherpunk.at/onioncat/wiki/GarliCat

eepSites

Project site
http://www.i2p2.i2p/

Forums
http://forum.i2p/
http://zzz.i2p/

Ugha's Wiki
http://ugha.i2p/

Search engines
http://eepsites.i2p/
http://search.rus.i2p/

General Network Stats
http://stats.i2p/

Site Lists & Up/Down Stats
http://inproxy.tino.i2p
http://perv.i2p

I2P.to, like Tor2Web, but for Eepsites
http://i2p.to
example: eepsitename.i2p.to

I2P Pros and Cons

Pros

- Lots of supported applications
- Can create just about any hidden service if you use SOCKS5 as the client tunnel
- Eepsites somewhat faster compared to Tor Hidden Services (Subjective, I know)

Cons

- ~~UDP based, which may be somewhat more noticeable/NAT issues~~
  Oops, I was wrong, it can use UDP but TCP is preferred
- Limited out proxies
- Out proxies don't handle all protocols (http/s should be good to go though)

What does the traffic look like?

These are defaults that can be changed in many cases

- Local
  1900: UPnP SSDP UDP multicast listener.
  2827: BOB bridge
  4444: HTTP proxy
  4445: HTTPS proxy
  6668: IRC proxy
  7652: UPnP HTTP TCP event listener.
  7653: UPnP SSDP UDP search response listener.
  7654: I2P Client Protocol port
  7655: UDP for SAM bridge
  7656: SAM bridge
  7657: Your router console
  7658: Your eepsite
  7659: Outgoing mail to smtp.postman.i2p
  7660: Incoming mail from pop.postman.i2p
  8998: mtn.i2p2.i2p (Monotone - disabled by default)
  32000: local control channel for the service wrapper
- Remote
  UDP from the random port (between 9000 and 32000) noted on the configuration page to arbitrary remote UDP ports, allowing replies
  TCP from random high ports (between 9000 and 32000) to arbitrary remote TCP ports
  UDP on port 123
- As copied from: http://www.i2p2.de/faq.html#ports but heavily edited. Check the I2P site for more details.

Some common Darknet weaknesses

Not all Darknets have all of these, but all of them have some of them ☺

Remote:

- Traffic analysis
- DNS leaks
- Cookies from when not using the Darknet
  http://www.irongeek.com/browserinfo.php
  http://irongeek.com/downloads/beenherebefore.php
  http://irongeek.com/downloads/beenherebefore.txt

- Plug-ins giving away real IP
  http://decloak.net/
  http://ha.ckers.org/weird/tor.cgi
  http://evil.hackademix.net/proxy_bypass/
  http://www.frostjedi.com/terra/scripts/ip_unmasker.php
  http://www.frostjedi.com/terra/scripts/phpbb/proxy_revealer.zip

Cookie Example

Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://irongeek.com/downloads/beenherebefore.php

Most Visited | Getting Started | Latest Headlines | Google | http://icache.i2p/?i2p... | Google AdSense - Re... | Relaxing music, sleep...

http://irongeek....nherebefore.php | http://www.frostje...r.php?mode=quirks

This is a simple script from Irongeek.com. It shows how cookies can be used to connect a Tor user with a real IP if the Tor user visits the same page more than once and they have cookies enabled.

```
You were here from 65.49.2.22 on Monday 26th of October 2009 02:41:19 PM
You were here from 65.49.2.22 on Monday 26th of October 2009 02:41:21 PM
You were here from 72.225.242.222 on Monday 26th of October 2009 02:41:46 PM and this IP is a Tor relay
```

Done | Proxy: Tor

Some common Darknet weaknesses

Not all Darknets have all of these, but all of them have some of them ☺

Remote (continued):

- Un-trusted exit points
  Dan Egerstad and the "Hack of the year“
  http://www.schneier.com/blog/archives/2007/11/dan_egerstad_ar.html
  http://encyclopediadramatica.com/The_Great_Em/b/assy_Security_Leak_of_2007
- The snoopers may not know what you are sending, or to who, but they may know you are using a Darknet and that could be enough to take action.
- Clock based attacks
- Metadata in files
- Sybil/infrastructure attacks
- Many more…
  http://www.i2p2.de/how_threatmodel.html

Local:

- Cached data and URLs (Privacy mode FTW)
  http://www.irongeek.com/i.php?page=videos/anti-forensics-occult-computing

I2P Specific attacks

- Darknets and hidden servers: Identifying the true IP/network identity of I2P service hosts http://www.irongeek.com/i.php?page=security/darknets-i2p-identifying-hidden-servers

Things to worry about if you decide to research Darknets (IANAL)

- Opening holes into your network
- Encryption laws of your country
  http://rechten.uvt.nl/koops/cryptolaw/
- Inadvertently possessing child porn/contraband
  - Wipe and forget?
  - Tell the authorities?
  - IANAL 18 USC § 2252

(c) Affirmative Defense.— It shall be an affirmative defense to a charge of violating paragraph (4) of subsection (a) that the defendant—

(1) possessed less than three matters containing any visual depiction proscribed by that paragraph; and

(2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any visual depiction or copy thereof—

(A) took reasonable steps to destroy each such visual depiction; or

(B) reported the matter to a law enforcement agency and afforded that agency access to each such visual depiction.

Other things to check out

- Tor Bundle
  http://www.torproject.org/projects/torbrowser.html.en
- Multiproxy Switch
  https://addons.mozilla.org/en-US/firefox/addon/7330
- Wippien
  http://www.wippien.com/
- Blackthrow/Svartkast/Pivot/Dropbox
  http://cryptoanarchy.org/wiki/Svartkast
- HP Veiled
  Matt Wood & Billy Hoffman's Blackhat Slides
  http://www.blackhat.com/presentations/bh-usa-09/HOFFMAN/BHUSA09-Hoffman-VeilDarknet-SLIDES.pdf

Events

- DerbyCon 2011, Louisville Ky
  Sept 30 - Oct 2
  http://derbycon.com/
- Louisville Infosec
  http://www.louisvilleinfosec.com/
- Other Cons:
  http://www.skydogcon.com/
  http://www.dojocon.org/
  http://www.hack3rcon.org/
  http://phreaknic.info
  http://notacon.org/
  http://www.outerz0ne.org/

QUESTIONS?

42

http://Irongeek.com