DARKNETS: FUN AND GAMES WITH ANONYMIZING PRIVATE 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

What is this talk about

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

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

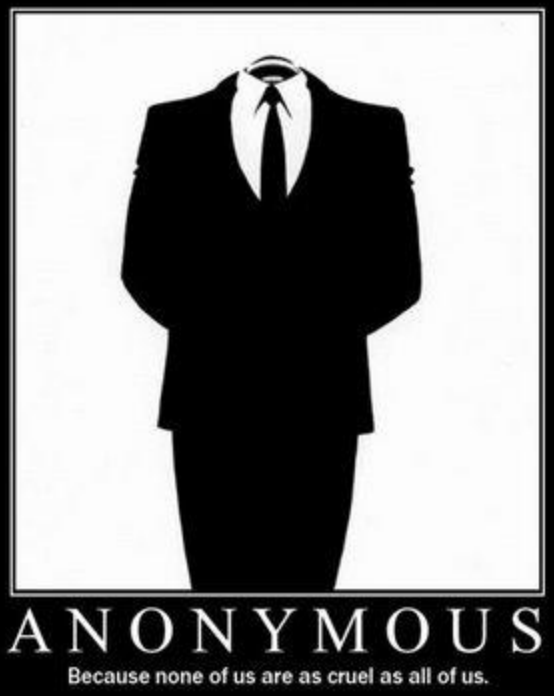
Who cares?

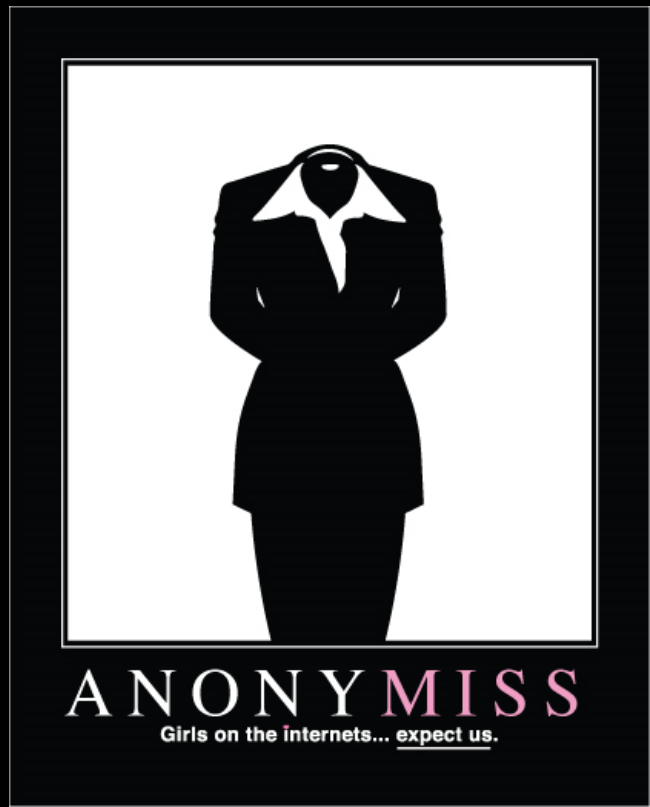
- Privacy enthusiasts and those worried about censorship
- Firms worried about policy compliance and leaked data
- Law enforcement

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

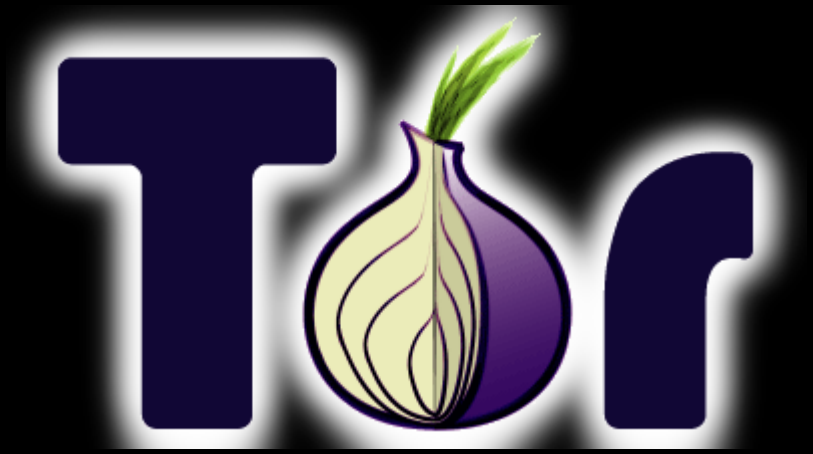
Law Enforcement
Why do you care?

Contraband and bad people everywhere

- 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

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

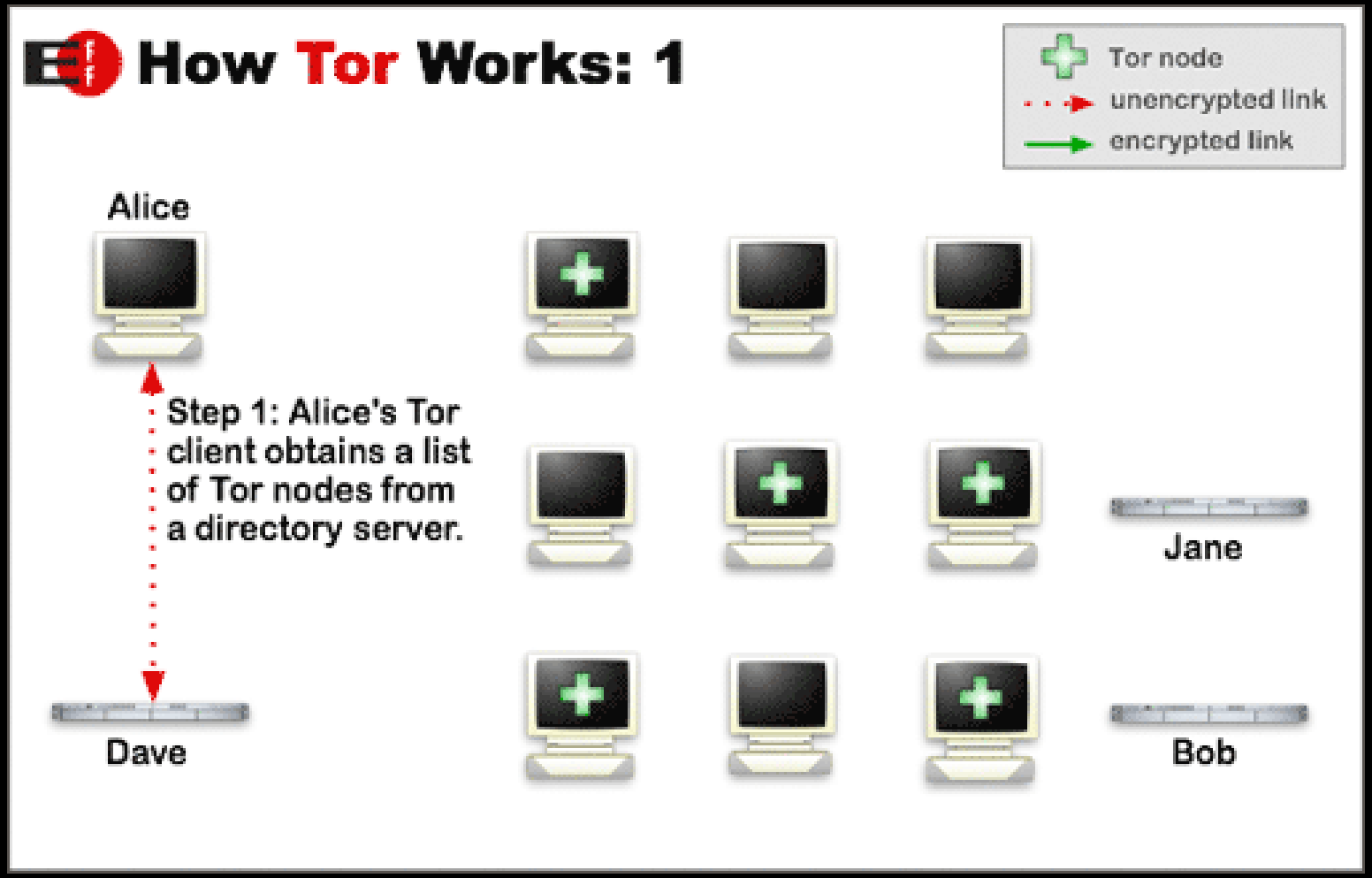


Image from http://www.torproject.org/overview.html.en

Layout

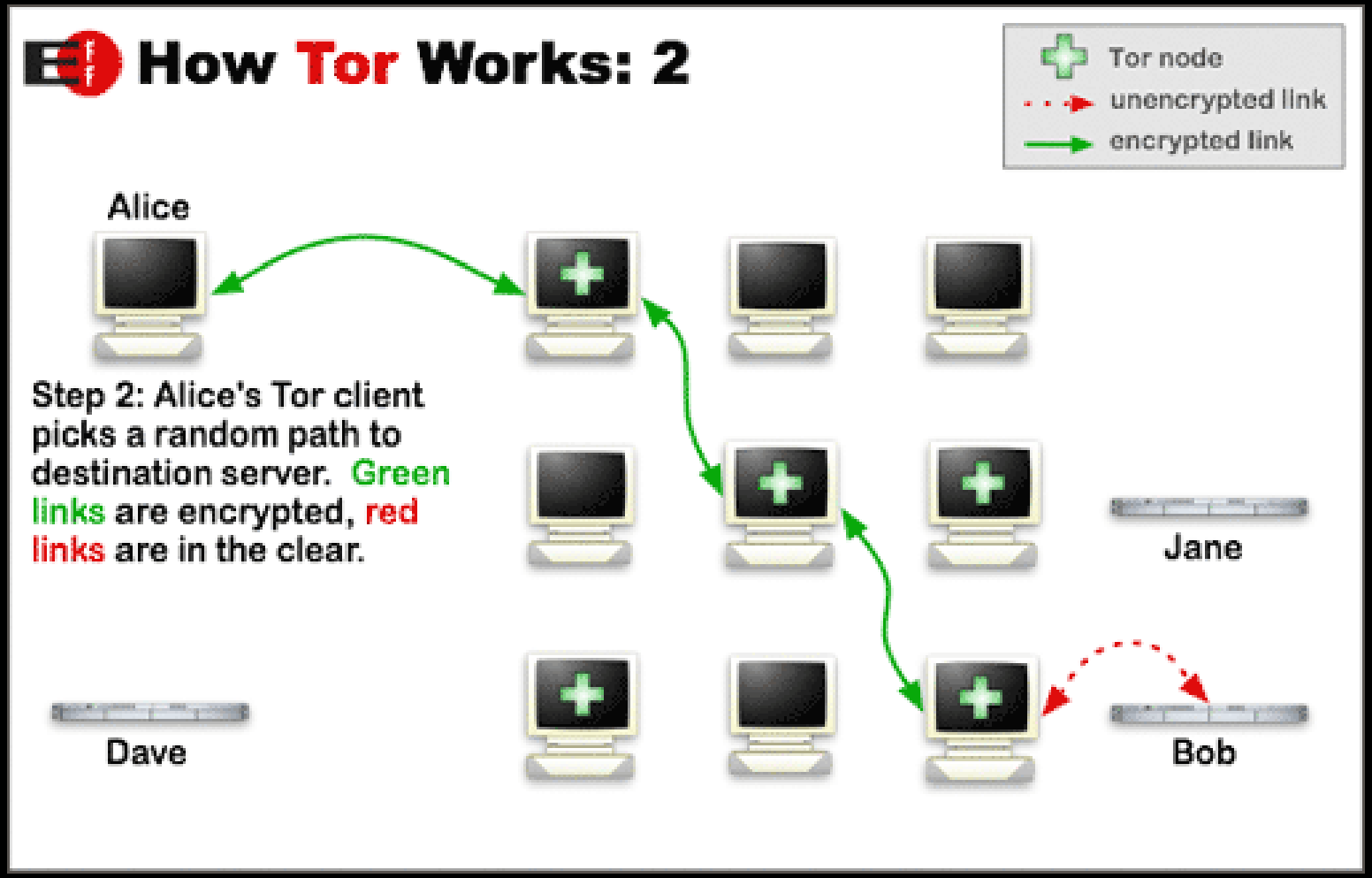


Image from http://www.torproject.org/overview.html.en

Layout

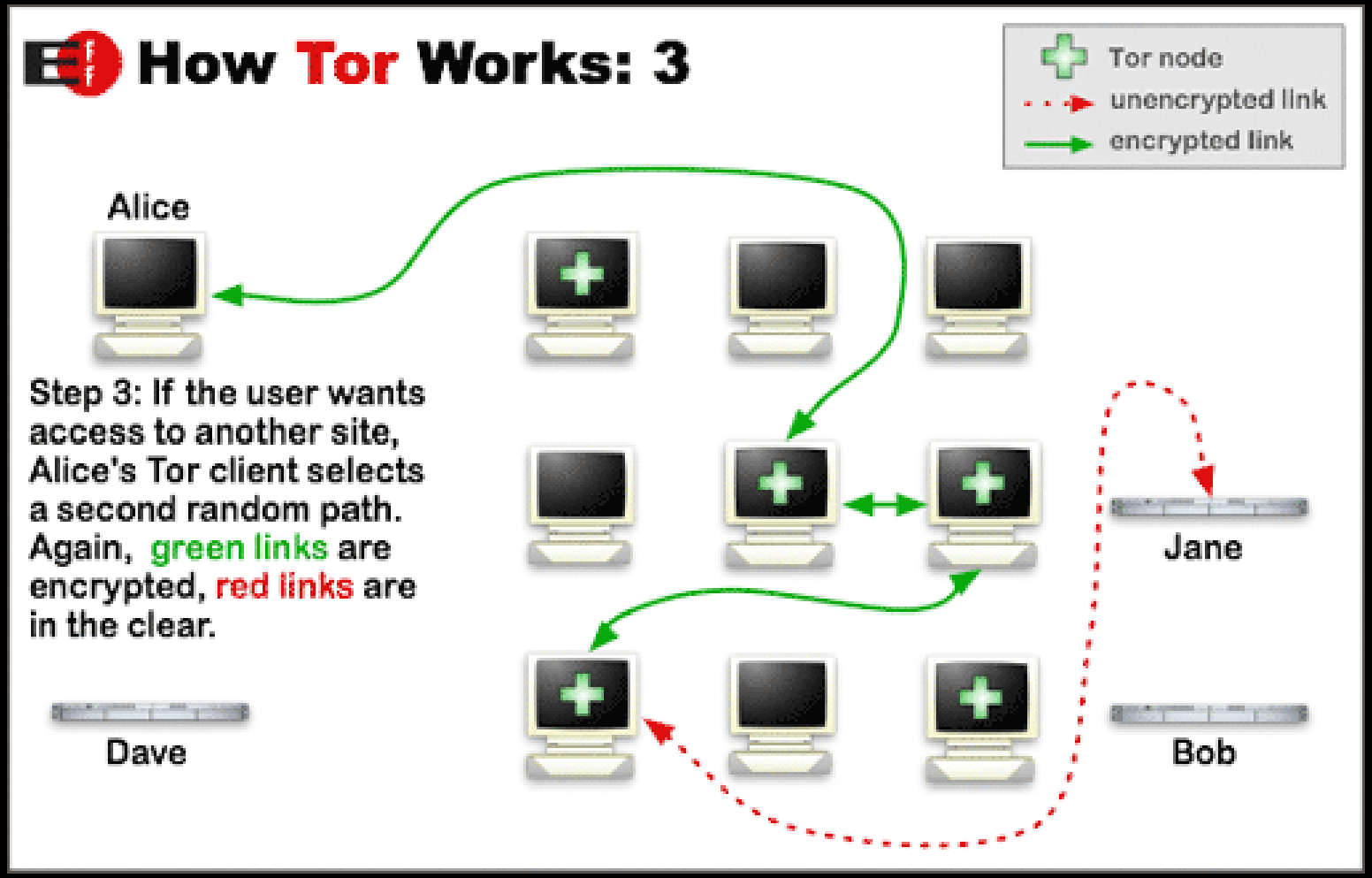
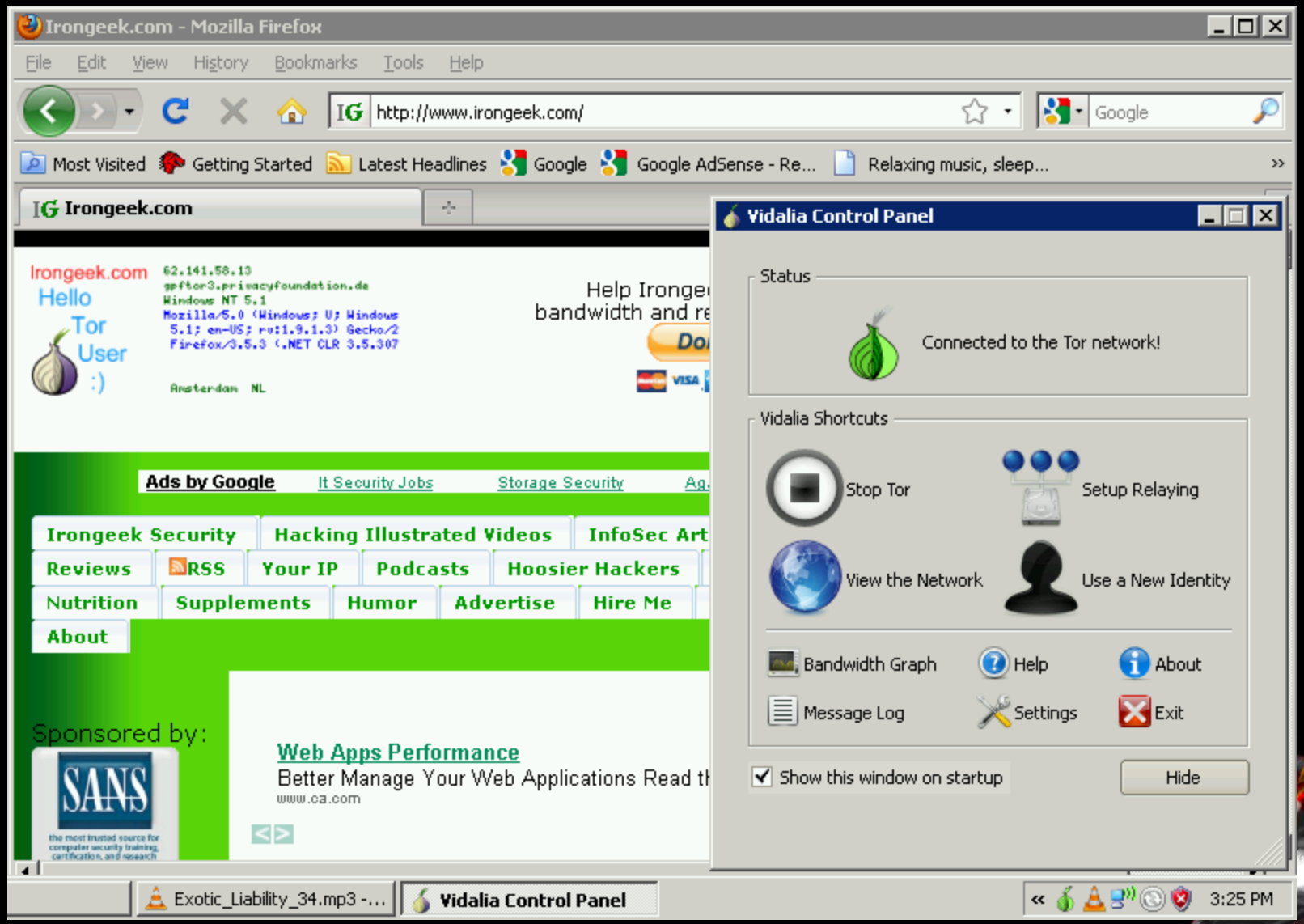


Image from http://www.torproject.org/overview.html.en

What does it look like to the user?



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 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?
- 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 Privoxy
- 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

ANONET AND DARKNET CONGLOMERATION

Roll your own, with OpenVPN and BGP routers

http://Irongeek.com

Overview

- **Who?**

  AnoNet: Good question
  http://anonetnfo.brinkster.net
  DarkNET Conglomeration: BadFoo.NET, ReLinked.ORG, SmashTheStack.ORG, and SABS (perhaps a few others).
  http://darknet.me

- **Why?**

  To run a separate semi-anonymous network based on normal Internet protocols.

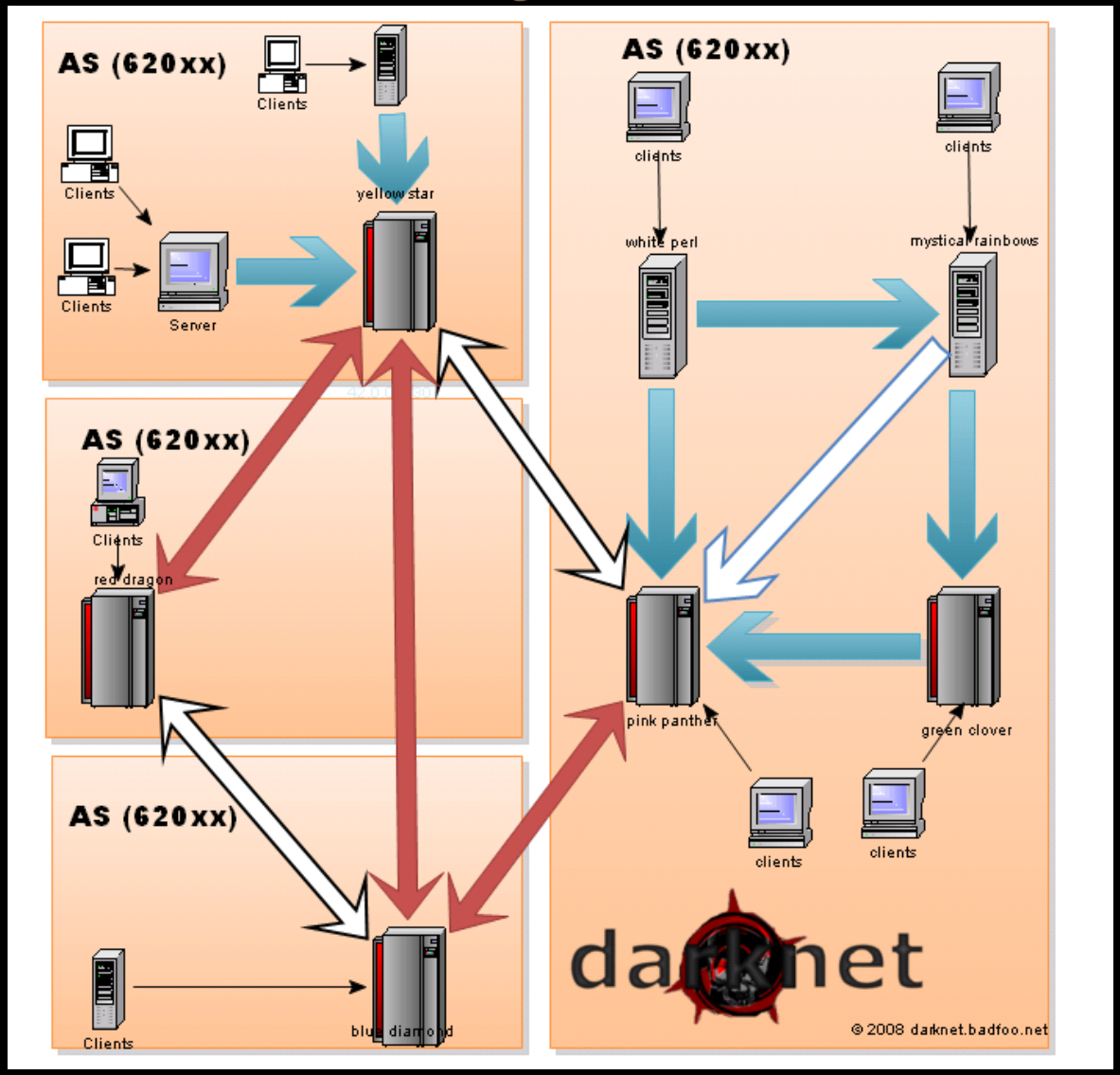
- **What?**

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

- **How?**

  OpenVPN connection to the network.

Layout



http://Irongeek.com

Image from http://darknet.me/whatthe.html

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 you can see whom you are peering with
- 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
  22/tcp
- Darknet Conglomeration
  2502/tcp

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

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 that you can connect to and control via a web browser.

Layout

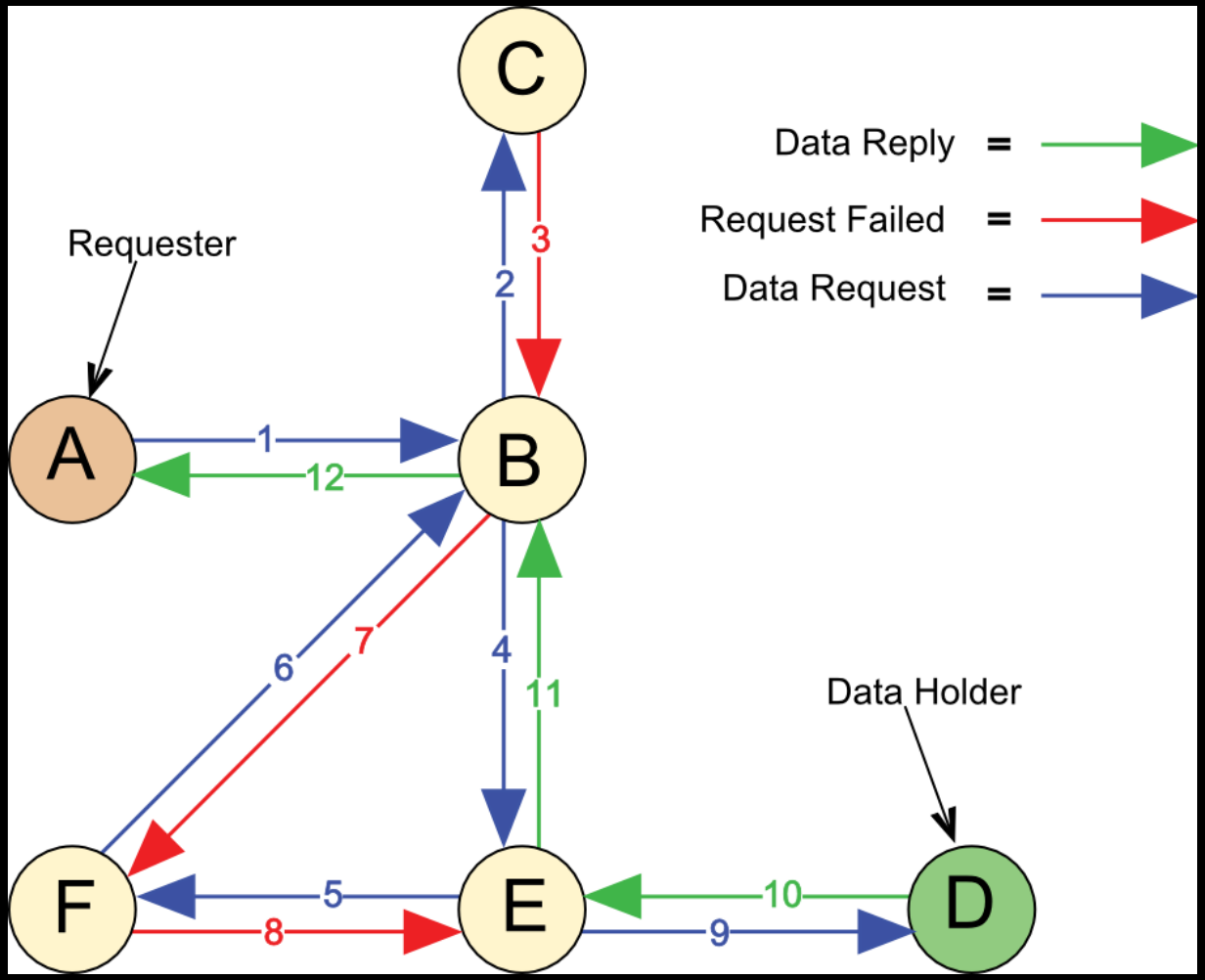
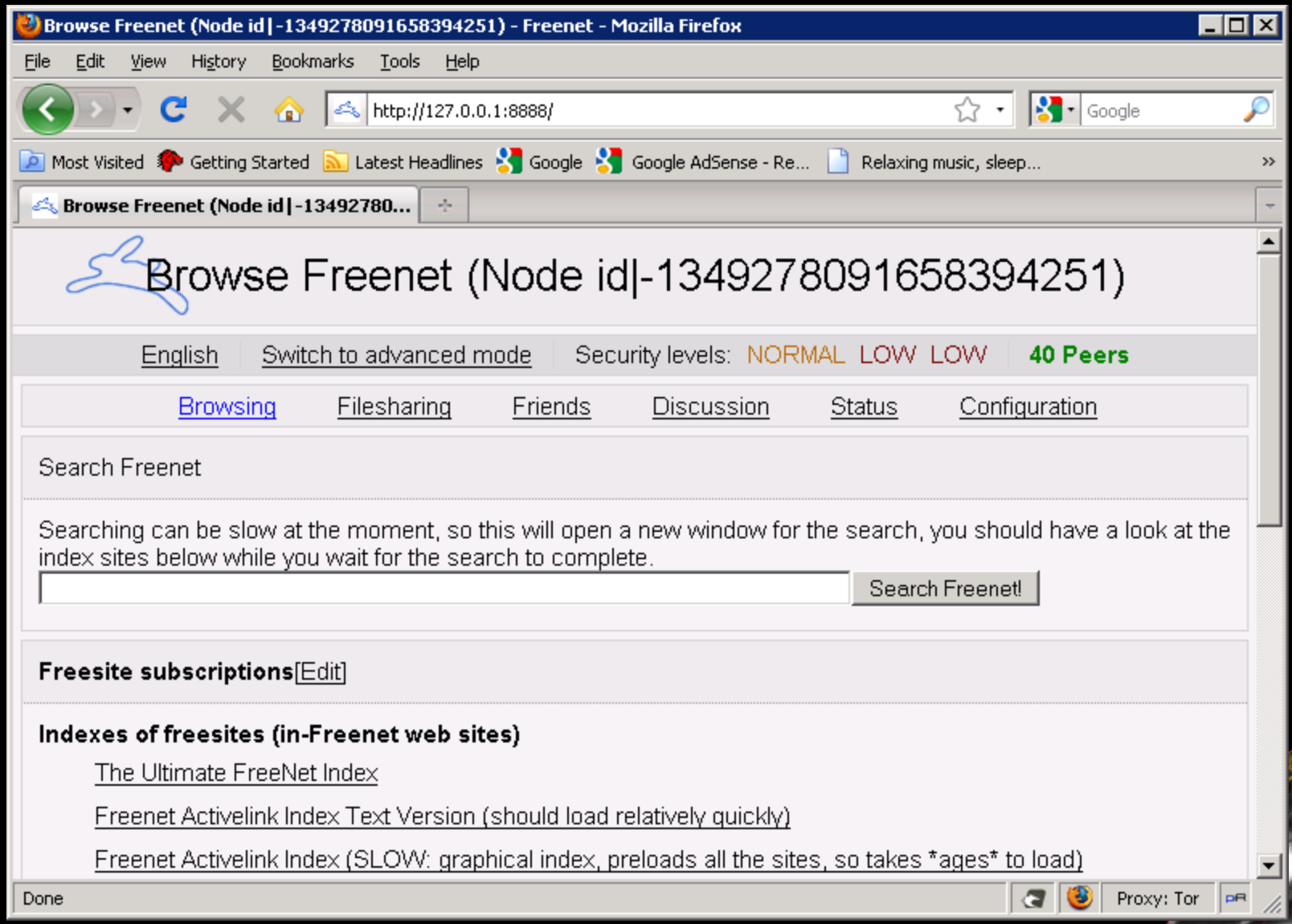


Image from http://en.wikipedia.org/wiki/File:Freenet_Request_Sequence_ZP.svg

What does it look like to the user?



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://freenetproject.org/frost.html
- 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

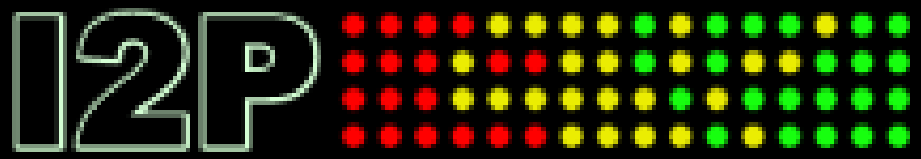
Cons

- 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)
- Remote
  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

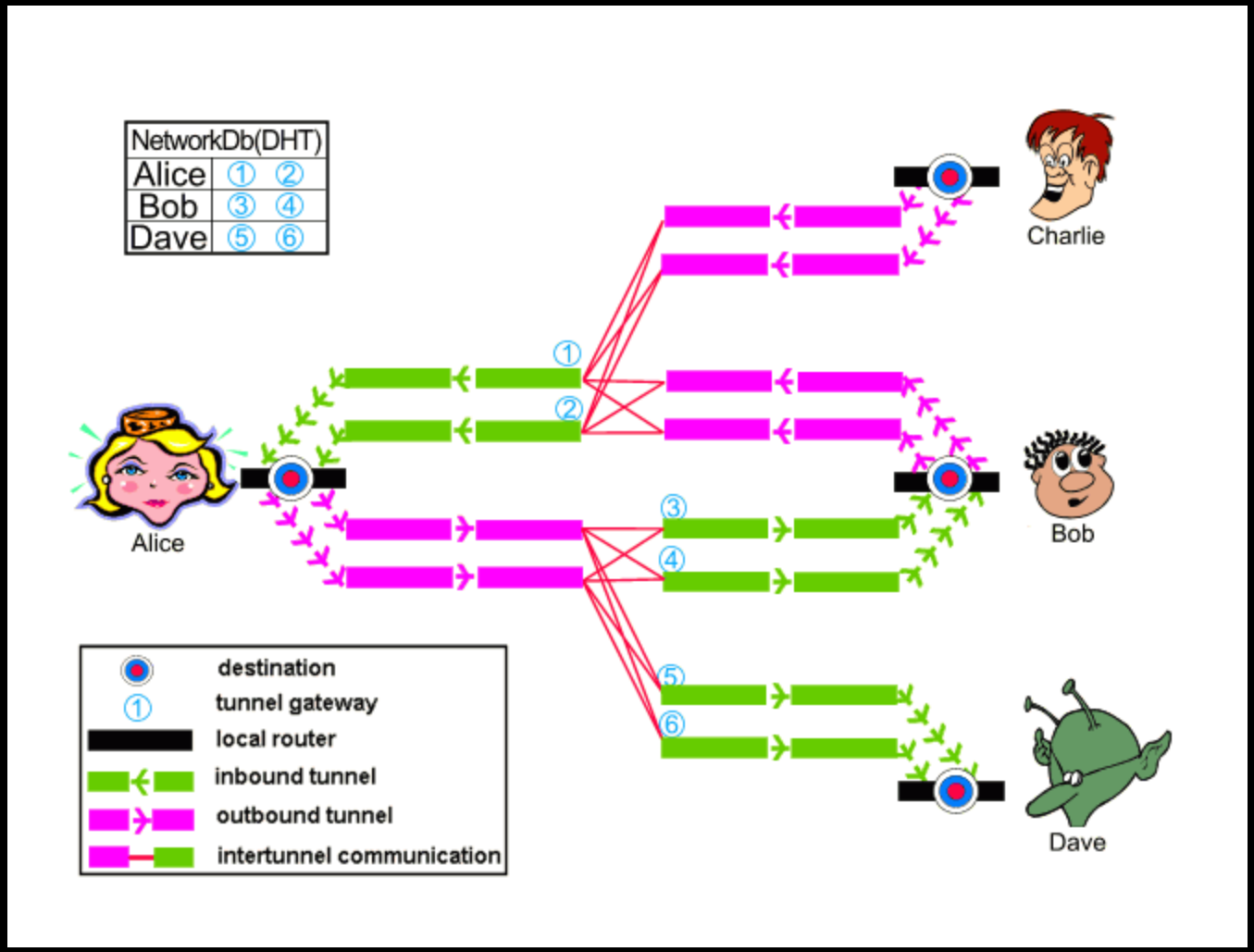
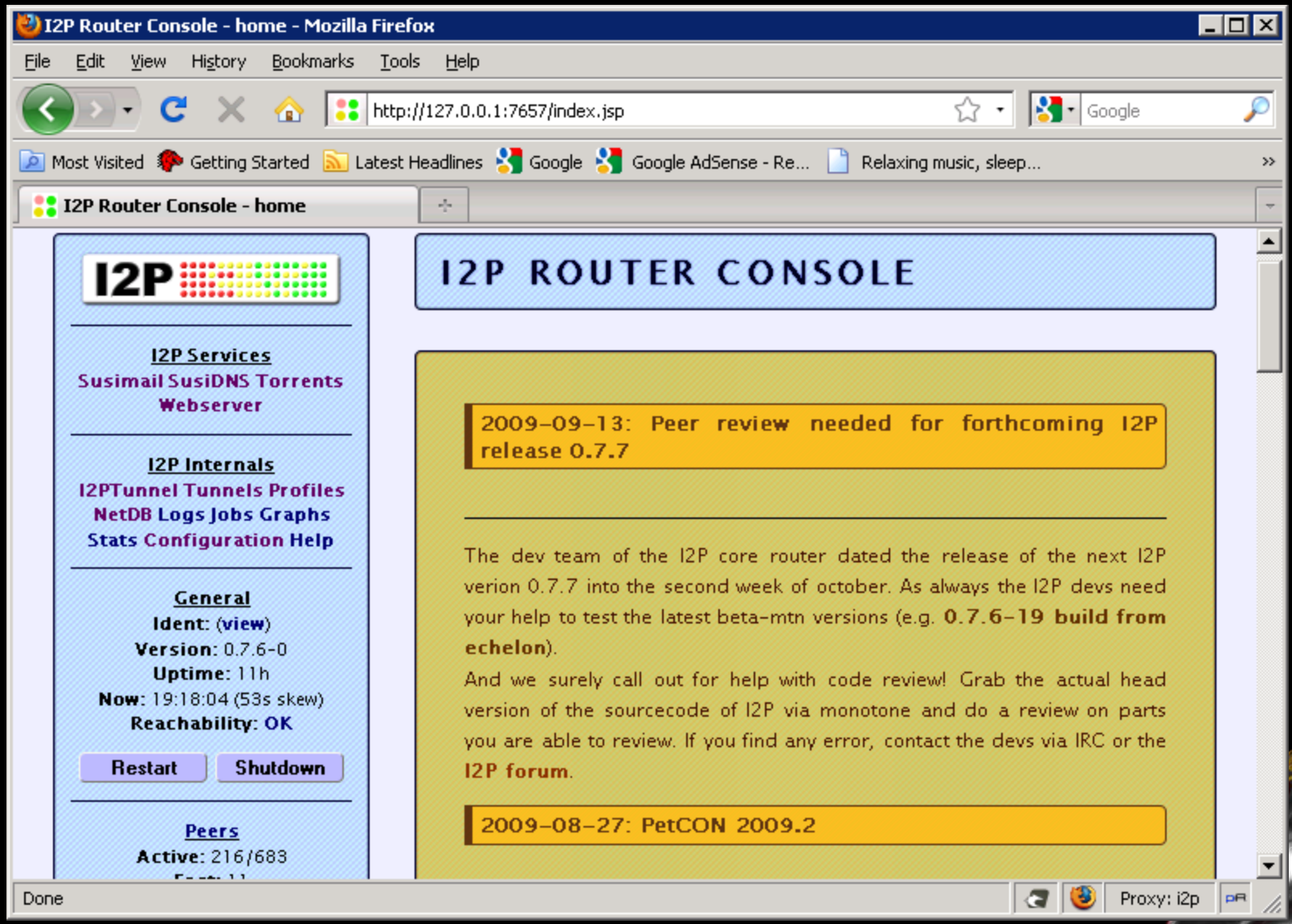
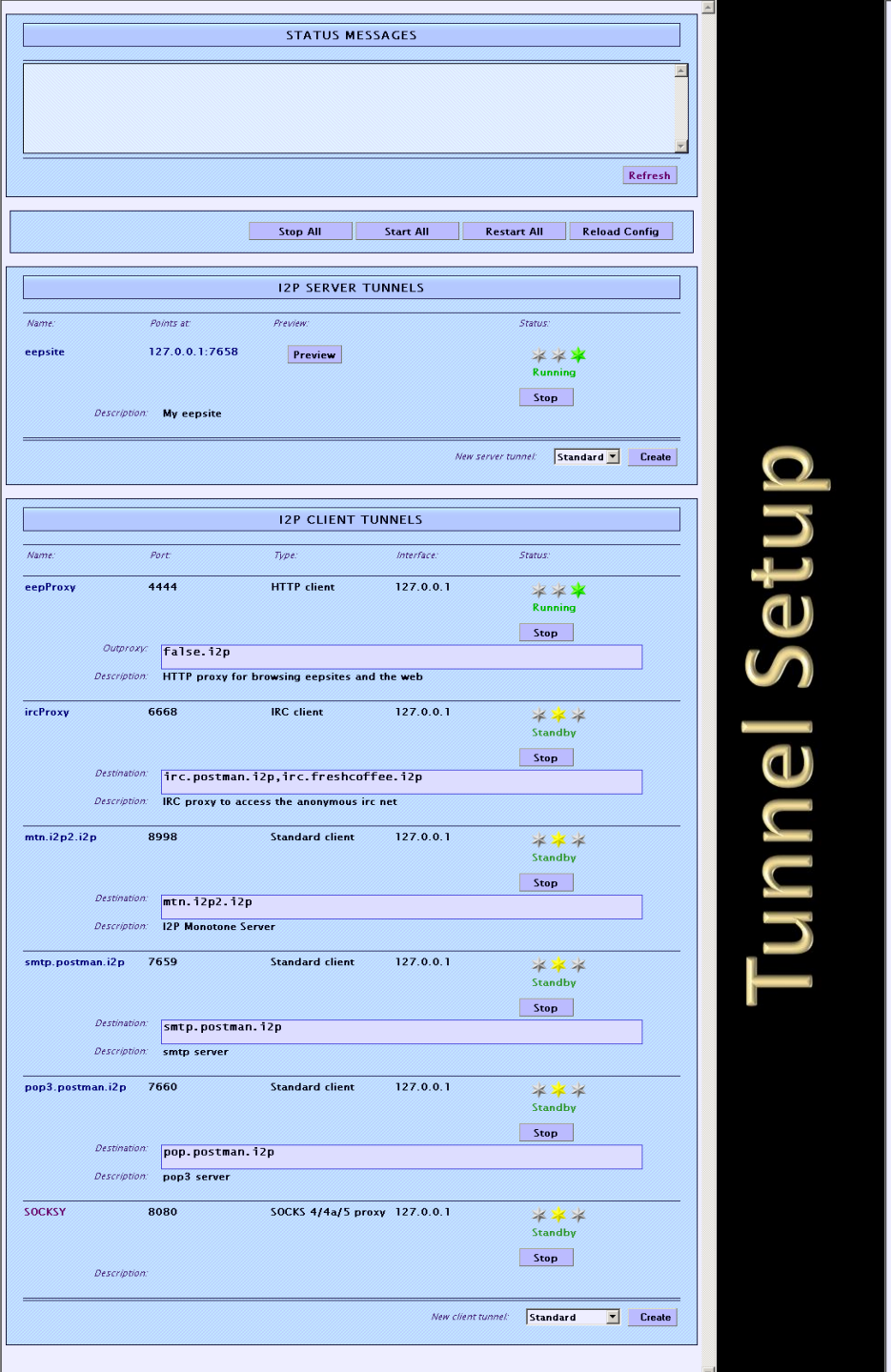


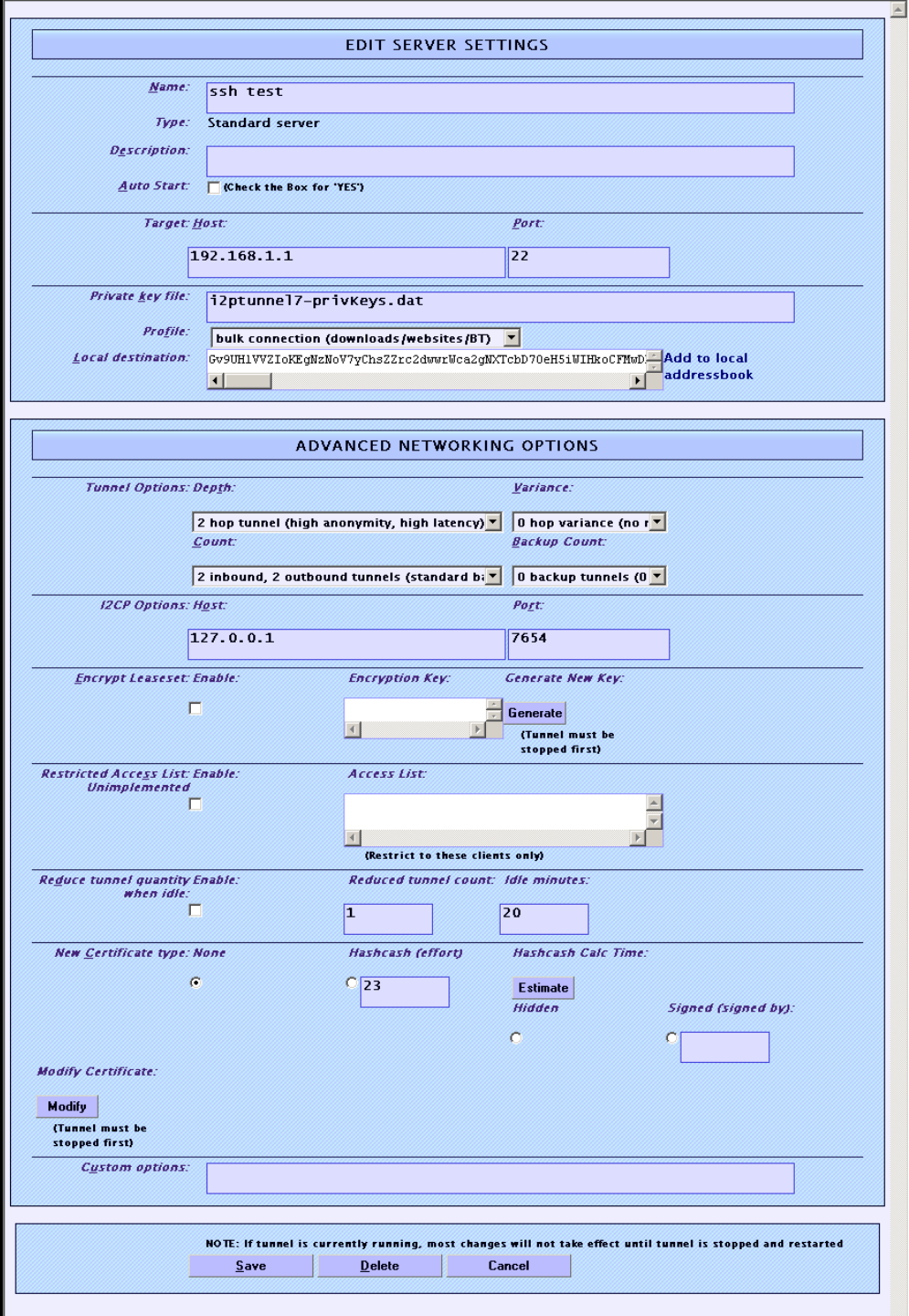
Image from http://www.i2p2.de/how_intro

What does it look like to the user?





Tunnel Setup



Tunnel Setup

EDIT PROXY SETTINGS

Name: SOCKSY

Type: SOCKS 4/4a/5 proxy

Description:

Access Point: Port: 8080

Reachable by: Locally (127.0.0.1)

Other:

Profile: bulk connection (downloads/websites/BT)

Delay Connect: (for request/response connections)

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

Auto Start: (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: Depth: 2 hop tunnel (high anonymity, high latency)

Variance: 0 hop variance (no r

Count: 2 inbound, 2 outbound tunnels (standard b

Backup Count: 0 backup tunnels (0

I2CP Options: Host: 127.0.0.1

Port: 7654

Reduce tunnel quantity when idle: Enable:

Reduced tunnel count: 1

Idle minutes: 20

Close tunnels when idle: Experimental Enable:

New Keys on Reopen: Enable / Disable

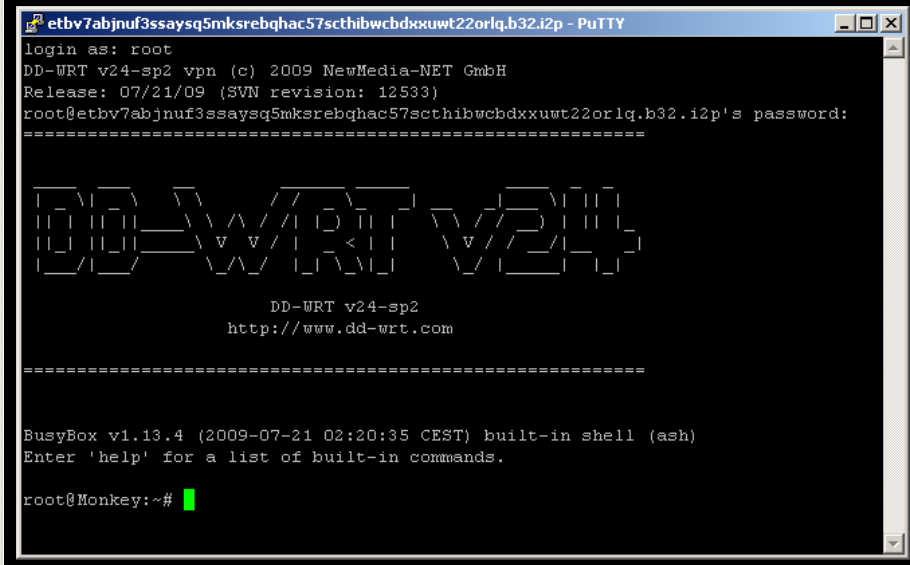
Idle minutes: 30

Delay tunnel open until required: Experimental Enable:

Custom options:

NOTE: If tunnel is currently running, most changes will not take effect until tunnel is stopped and restarted

Save | Delete | Cancel



Applications/Sites

- I2PSnark
  Built-in Bittorrent Client
- iMule
  Kad file sharing network client
  http://www.imule.i2p.tin0.de/
- Syndie
  Blogging application, very alpha
- I2PTunnel
  Built-in, allows for setting up arbitrary TCP/IP tunnels between nodes
- Out Proxies
  For connecting to the normal Internet
- Susimail
  Built-in mail client, but you need to register an account at *www.mail.i2p*
- InProxy I2P Eepsite
  http://inproxy.tino.i2p/status.php

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
- Limited out proxies
- Out proxies don't handle SSL (I'm not 100% on this)

What does the traffic look like?

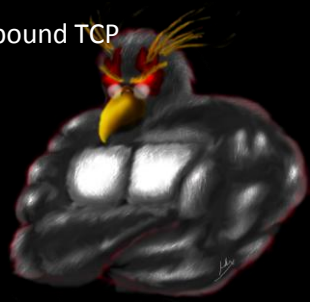
(Keep in mind, this is just the defaults)

- Local

  1900/udp: UPnP SSDP UDP multicast listener. Cannot be changed. Binds to all interfaces. May be disabled on config.jsp.
  2827: BOB bridge, a higher level socket API for clients Disabled by default. May be enabled/disabled on configclients.jsp. May be changed in the bob.config file.
  4444: HTTP proxy May be disabled or changed on the i2ptunnel page in the router console.
  6668: IRC proxy May be disabled or changed on the i2ptunnel page in the router console.
  7652: UPnP HTTP TCP event listener. Binds to the LAN address. May be changed with advanced config i2np.upnp.HTTPPort=nnnn. May be disabled on config.jsp.
  7653: UPnP SSDP UDP search response listener. Binds to all interfaces. May be changed with advanced config i2np.upnp.SSDPPort=nnnn. May be disabled on config.jsp.
  7654: I2P Client Protocol port, used by client apps. May be changed with the advanced configuration option i2cp.port but this is not recommended.
  7655: UDP for SAM bridge, a higher level socket API for clients Only opened when a SAM V3 client requests a UDP session. May be enabled/disabled on configclients.jsp. May be changed in the clients.config file with the SAM command line option sam.udp.port=nnnn.
  7656: SAM bridge, a higher level socket API for clients Disabled by default for new installs as of release 0.6.5. May be enabled/disabled on configclients.jsp. May be changed in the clients.config file.
  7657: Your router console May be changed in the clients.config file
  7658: Your eepsite May be disabled in the clients.config file
  7659: Outgoing mail to smtp.postman.i2p May be disabled or changed on the i2ptunnel page in the router console.
  7660: Incoming mail from pop.postman.i2p May be disabled or changed on the i2ptunnel page in the router console.
  8998: mtn.i2p2.i2p (Monotone - disabled by default) May be disabled or changed on the i2ptunnel page in the router console.
  32000: local control channel for the service wrapper

- Remote

  Outbound 8887/udp to arbitrary remote UDP ports, allowing replies
  Outbound TCP from random high ports to arbitrary remote TCP ports
  Inbound to port 8887/udp from arbitrary locations
  Inbound to port 8887/tcp from arbitrary locations (optional, but recommended by default, I2P does not listen for inbound TCP connections)
  Outbound on port 123/udp, allowing replies for I2P's internal time sync (via SNTP)



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
- Plug-ins giving away real IP
  http://ha.ckers.org/weird/tor.cgi
  http://evil.hackademix.net/proxy_bypass/
- Un-trusted peers
- Un-trusted exit points
- 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.

Local:

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

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
  - Wipe and forget?
  - Tell the authorities?
  - http://detroit.fbi.gov/crimes2.htm

Other things to check out

- HP Veiled
  http://www.internetnews.com/dev-news/article.php/3832326/HP+Veiled+A+Darknet+for+Browsers.htm
- FlashBlock
  https://addons.mozilla.org/en-US/firefox/addon/433
- Multiproxy Switch
  https://addons.mozilla.org/en-US/firefox/addon/7330
- Wippien
  http://www.wippien.com/

Events

- Free ISSA classes
- ISSA Meeting
  http://issa-kentuckiana.org/
- Louisville Infosec
  http://www.louisvilleinfosec.com/
- Phreaknic/Notacon/Outerz0ne
  http://phreaknic.info
  http://notacon.org/
  http://www.outerz0ne.org/

Thanks

- Folks at Binrev and Pauldotcom
- Louisville ISSA
- Hacker Consortium
- Free ISSA Classes

Helping with the free classes

- Got old hardware you would like to donate?
- Is there a subject you would like to teach?
- Let others know about upcoming classes, and the videos of previous classes.

QUESTIONS?

42