

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



ANONYMOUS

Because none of us are as cruel as all of us.



ANONYMISS

Girls on the internets... expect us.

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

How Tor Works: 1

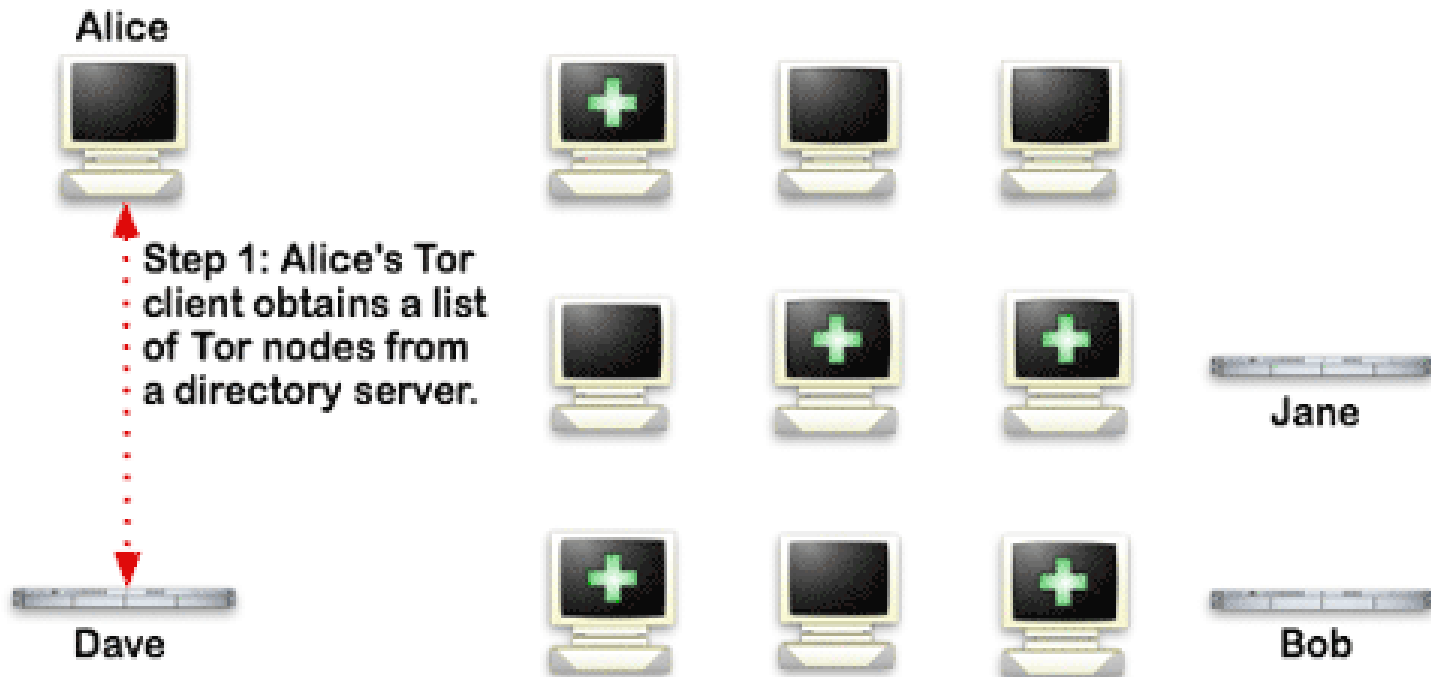
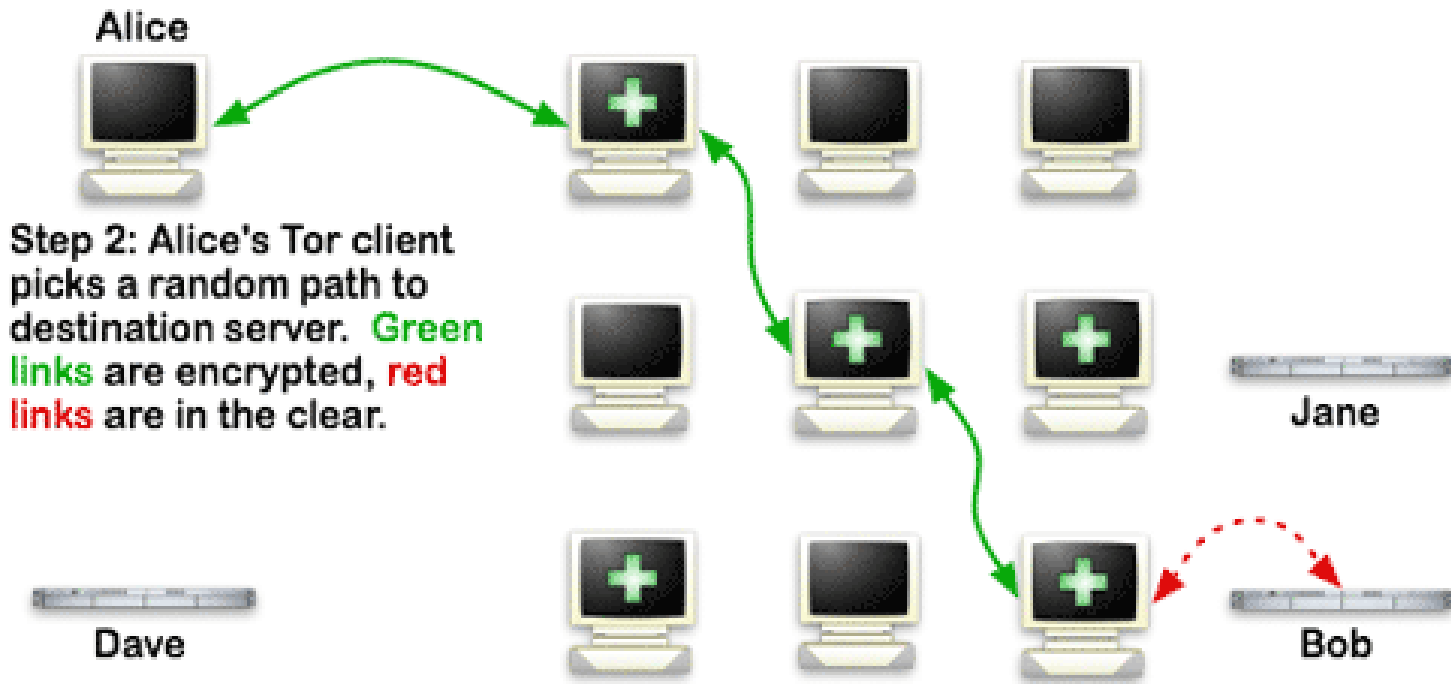


Image from <http://www.torproject.org/overview.html.en>

Layout

How Tor Works: 2



Step 2: Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.



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

Layout

How Tor Works: 3

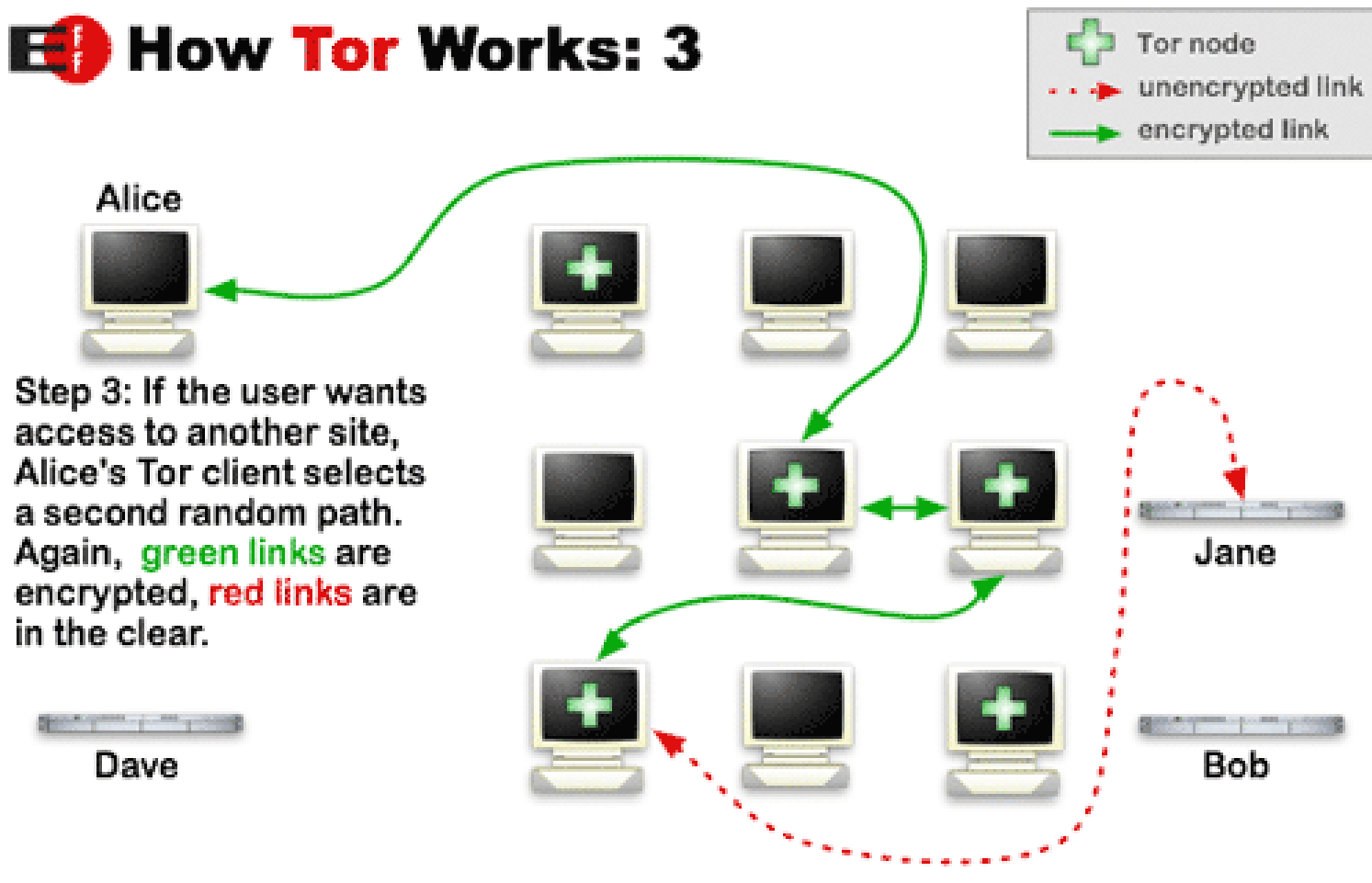
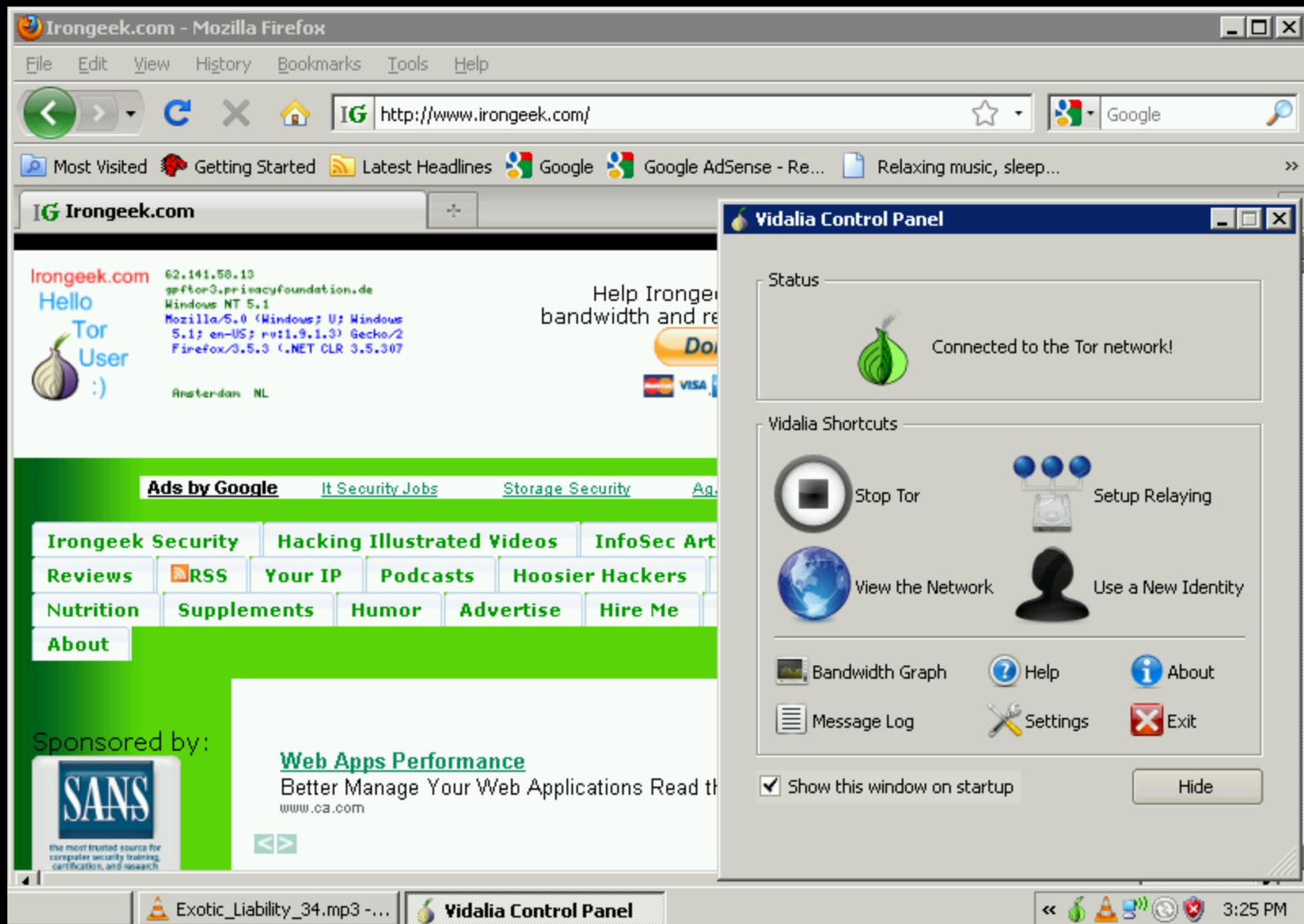


Image from <http://www.torproject.org/overview.html.en>



What does it look like to the user?



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



Overview

▣ Who?

AnoNet: Good question

<http://anonetinfo.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.

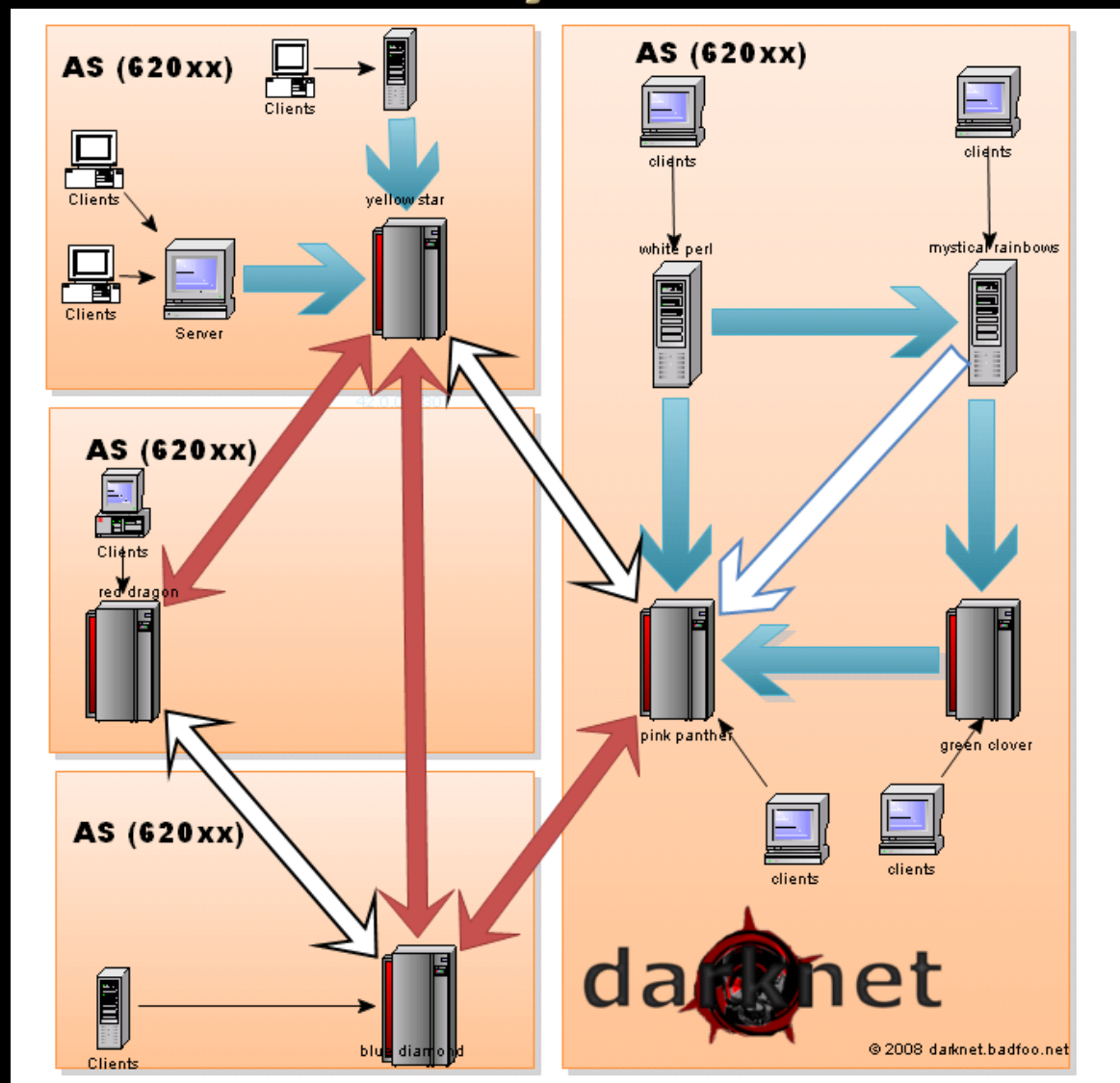
▣ How?

OpenVPN connection to the network.

<http://Irongeek.com>



Layout



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?

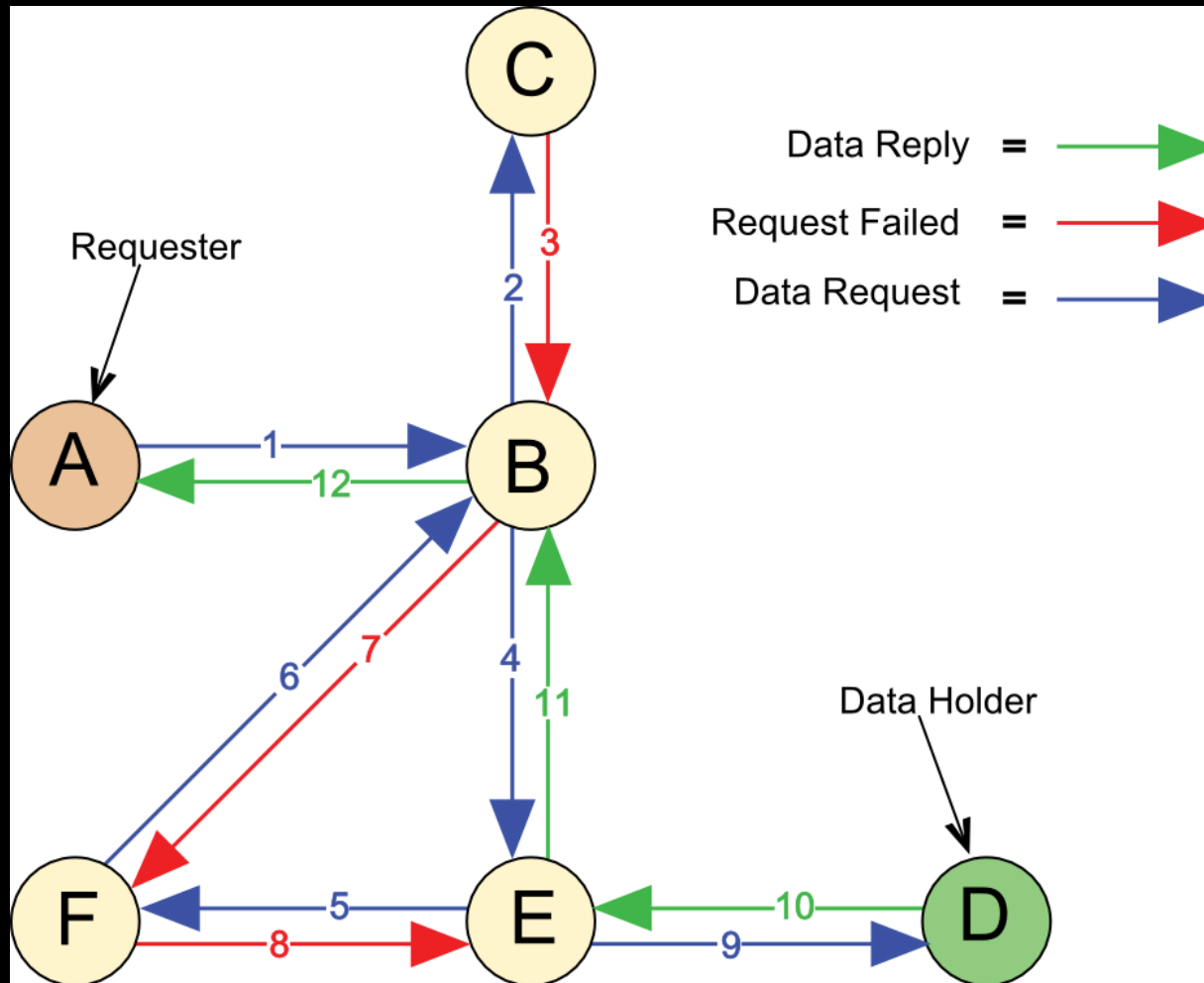
Documents and Freenet Websites for the most part, but with some extensibility.

▣ How?

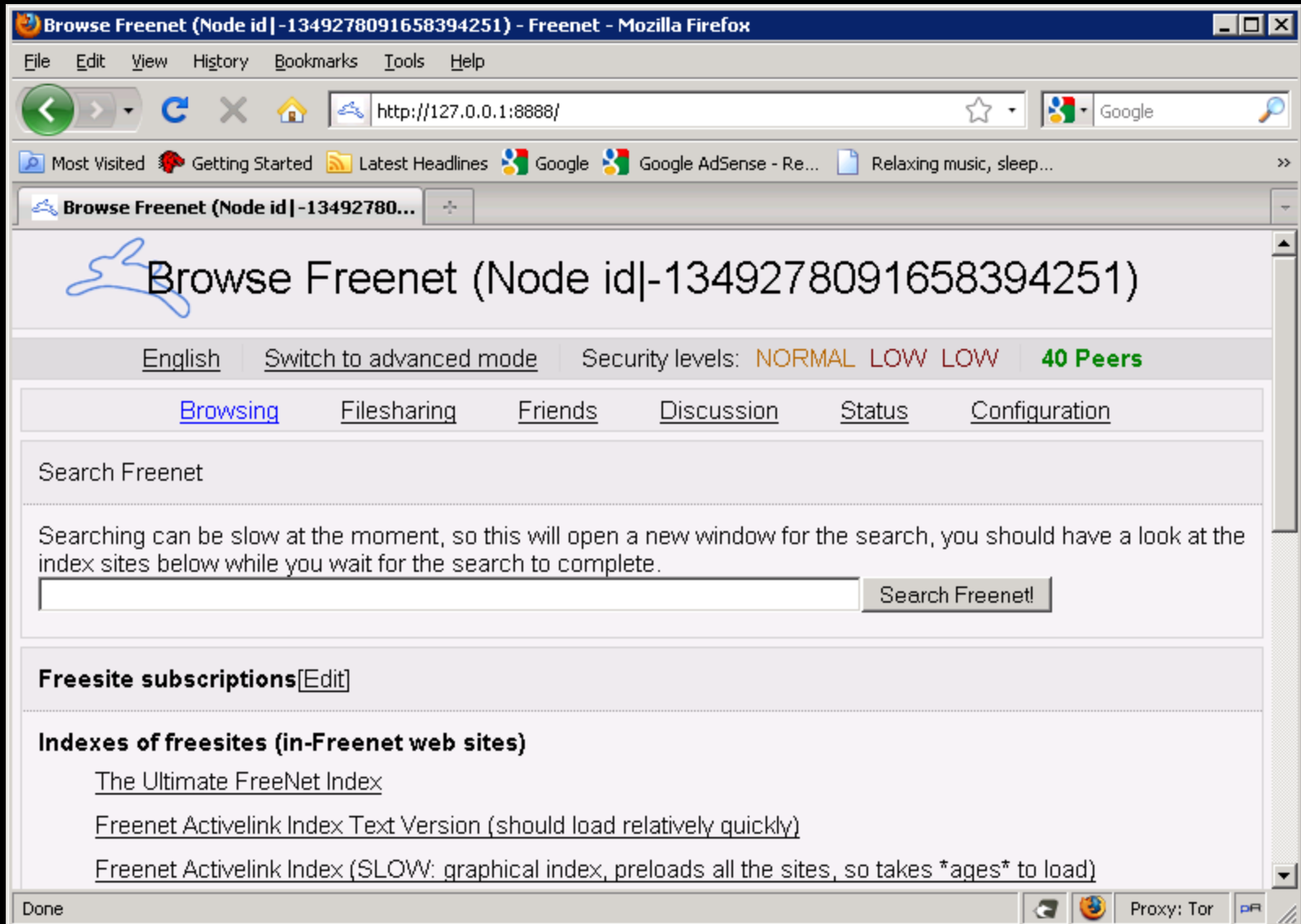
Locally run proxy of a sort that you can connect to and control via a web browser.



Layout



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)

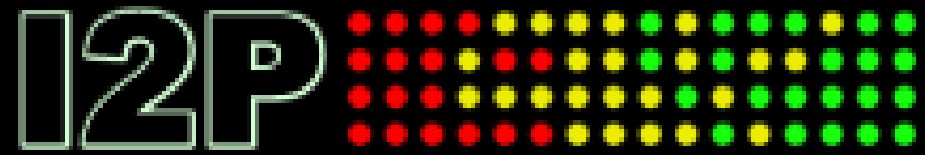
- ▣ Remote

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



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?

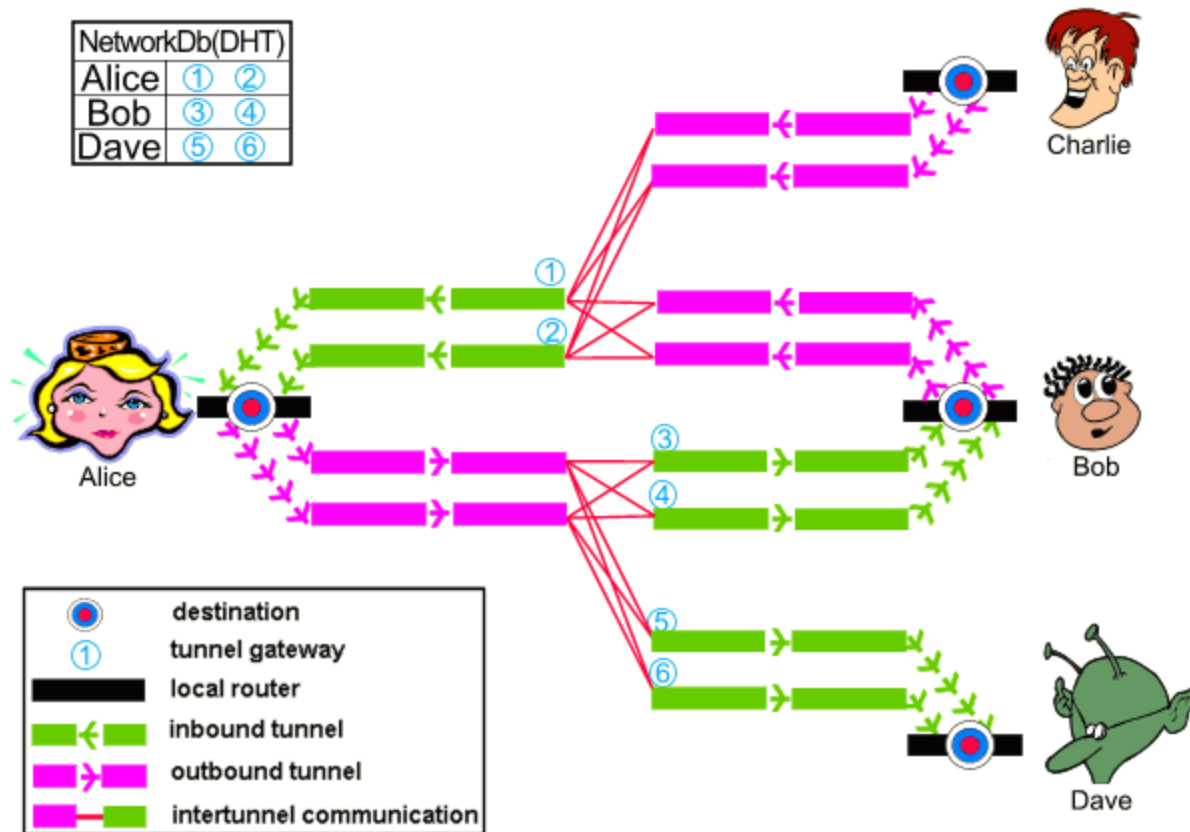
Mostly other web sites on I2P (Eepsites), but the protocol allows for P2P (iMule, i2psnark), anonymous email and public Internet via out proxies.

▣ How?

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



Layout



What does it look like to the user?

The screenshot shows a Mozilla Firefox browser window with the title "I2P Router Console - home". The address bar displays "http://127.0.0.1:7657/index.jsp". The browser's menu bar includes File, Edit, View, History, Bookmarks, Tools, and Help. The toolbar contains navigation buttons (back, forward, home, stop, reload) and a search bar with the Google logo. The bookmarks bar shows "Most Visited", "Getting Started", "Latest Headlines", "Google", "Google AdSense - Re...", and "Relaxing music, sleep...".

The main content area of the browser displays the I2P Router Console web interface. On the left side, there is a sidebar with the I2P logo and several sections:

- I2P Services**: [Susimail](#), [SusiDNS](#), [Torrents](#), [Webserver](#)
- I2P Internals**: [I2PTunnel](#), [Tunnels](#), [Profiles](#), [NetDB](#), [Logs](#), [Jobs](#), [Graphs](#), [Stats](#), [Configuration](#), [Help](#)
- General**:
 - Ident: [\(view\)](#)
 - Version: 0.7.6-0
 - Uptime: 11h
 - Now: 19:18:04 (53s skew)
 - Reachability: **OK**
 - [Restart](#) [Shutdown](#)
- Peers**:
 - Active: 216/683
 - Fast: 11

The main content area on the right is titled "I2P ROUTER CONSOLE" and contains two yellow boxes with news items:

- 2009-09-13: Peer review needed for forthcoming I2P release 0.7.7**
- 2009-08-27: PetCON 2009.2**

Below the first news item, there is a paragraph of text: "The dev team of the I2P core router dated the release of the next I2P version 0.7.7 into the second week of october. As always the I2P devs need your help to test the latest beta-mtn versions (e.g. **0.7.6-19 build from echelon**). And we surely call out for help with code review! Grab the actual head version of the sourcecode of I2P via monotone and do a review on parts you are able to review. If you find any error, contact the devs via IRC or the **I2P forum**."

The browser's status bar at the bottom shows "Done" and "Proxy: i2p".

Tunnel Setup

STATUS MESSAGES

Refresh

Stop All

Start All

Restart All

Reload Config

I2P SERVER TUNNELS

Name: Points at: Preview: Status:

eebsite 127.0.0.1:7658 Preview Running

Description: My eebsite

Stop

New server tunnel: Standard Create

I2P CLIENT TUNNELS

Name: Port: Type: Interface: Status:

eeProxy 4444 HTTP client 127.0.0.1 Running

Outproxy: false.i2p

Description: HTTP proxy for browsing eebsites and the web

Stop

ircProxy 6668 IRC client 127.0.0.1 Standby

Destination: irc.postman.i2p,irc.freshcoffee.i2p

Description: IRC proxy to access the anonymous irc net

Stop

mtn.i2p2.i2p 8998 Standard client 127.0.0.1 Standby

Destination: mtn.i2p2.i2p

Description: I2P Monotone Server

Stop

smtp.postman.i2p 7659 Standard client 127.0.0.1 Standby

Destination: smtp.postman.i2p

Description: smtp server

Stop

pop3.postman.i2p 7660 Standard client 127.0.0.1 Standby

Destination: pop.postman.i2p

Description: pop3 server

Stop

SOCKSY 8080 SOCKS 4/4a/5 proxy 127.0.0.1 Standby

Description:

Stop

New client tunnel: Standard Create

EDIT SERVER SETTINGS

Name: ssh test

Type: Standard server

Description:

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

Target Host:

192.168.1.1

Port:

22

Private key file: i2ptunnel17-privkeys.dat

Profile: bulk connection (downloads/websites/BT)

Local destination: Gv9UH1VVZIoKEgNzNoV7yChsZZrc2dwwrWca2gNXTcbD70eH5iWlHkoCFMwD Add to local addressbook

ADVANCED NETWORKING OPTIONS

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: Hgst:

127.0.0.1

Port:

7654

Encrypt Leaseset: Enable:

☐

Encryption Key:

Generate

Generate New Key:

Generate

(Tunnel must be stopped first)

Restricted Access List: Enable: Unimplemented

☐

Access List:

(Restrict to these clients only)

Reduce tunnel quantity Enable: when idle:

☐

Reduced tunnel count: Idle minutes:

1

20

New Certificate type: None

☐

Hashcash (effort)

23

Hashcash Calc Time:

Estimate

Hidden

Signed (signed by):

Modify Certificate:

Modify

(Tunnel must be stopped first)

Custom options:

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

Save

Delete

Cancel

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:	<input type="checkbox"/> (for request/response connections)
Shared Client:	<input checked="" type="checkbox"/> (Share tunnels with other clients and irc/httpclients? Change requires restart of client proxy)
Auto Start:	<input checked="" type="checkbox"/> (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!)			
<u>Tunnel Options:</u> Depth:		<u>Variance:</u>	
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">2 hop tunnel (high anonymity, high latency) ▾</div>		<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">0 hop variance (no r ▾</div>	
<u>Count:</u>		<u>Backup Count:</u>	
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">2 inbound, 2 outbound tunnels (standard b ▾</div>		<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">0 backup tunnels (0 ▾</div>	
<u>I2CP Options:</u> Host:		<u>Port:</u>	
<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">127.0.0.1</div>		<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;">7654</div>	
<u>Reduce tunnel quantity Enable:</u> when idle:		<u>Reduced tunnel count:</u> Idle minutes:	
<input type="checkbox"/>		<div style="display: inline-block; width: 50px; border: 1px solid #ccc; text-align: center;">1</div> <div style="display: inline-block; width: 50px; border: 1px solid #ccc; text-align: center;">20</div>	
<u>Close tunnels when Enable:</u> idle: Experimental		<u>New Keys on Reopen:</u> Idle minutes:	
<input type="checkbox"/>		<div style="display: inline-block; width: 50px; border: 1px solid #ccc; text-align: center;">30</div>	
<u>Delay tunnel open until Enable:</u> required: Experimental			
<input type="checkbox"/>			
<u>Custom options:</u>			
<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>			
<div style="text-align: center; font-weight: bold; font-size: small;">NOTE: If tunnel is currently running, most changes will not take effect until tunnel is stopped and restarted</div>			
<div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #e6f2ff;">Save</div>		<div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #e6f2ff;">Delete</div>	
		<div style="border: 1px solid #ccc; padding: 2px 10px; background-color: #e6f2ff;">Cancel</div>	

[illegible]

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 Pauidotcom
- ▣ 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

