# Personal VPN using SSH Dynamic Tunneling

Gary Meyer Ed Wehner

# SSH Dynamic Port Forwarding

- Dynamic port forwarding configures a local port for tunnelling data to multiple remote IP Addresses/Ports.
- The client application connecting to local port use the SOCKS protocol.
- The SOCKS proxy is located on the client side to specify where the traffic should be sent when it leaves the other end of the ssh tunnel.
- This technique is support with open/free software on virtually all platforms that supports ssh and firefox.

## How it works



http://chamibuddhika.wordpress.com/2012/03/21/ssh-tunnelling-explained/

#### Android Example

- What you need:
  - ConnectBot Google Play
  - Firefox Google Play

# Android Setup

- Install ConnectBot & Firefox
- Configure a Dynamic Tunnel to your ssh server
  - Local port 8080
- Configure Firefox to use a socks proxy to localhost port 8080
- Configure Firefox for DNS Lookup through the proxy server
- Test your IP addres

**ConnectBot: Hosts** 

ssh

íì

Ē

bud socks tunnel 26 minutes ago

ed@dexter01 18 days ago

edw@bud.sluug.org:2206

🔤 🖸 🔂 🖬 84° 2:48 🤝 🕌 » 🗎

# Last login: Sat Oct 5 21:17:08 2013 from 71-85-250-89. dhcp.stls.mo.charter.com



ConnectBot: Port forwards (edw@bud.sluug.org:2206)

Ŀ

Menu

Tap Menu to create port forwards.



Add port forward

エン

🗵 🔁 🖪 84° 2:48 📚 💾 » 🖬

#### ConnectBot: Port forwards (edw@bud.sluug.org:2206)



📼 🖸 🖸 🔂 🔂 🔂

ConnectBot: Hosts		1	
bud socks t	edw@bud.sluug.org:2206	•	
ed@dexter0	Disconnect	$\bigcirc$	
edw@bud.s	Edit host		
	Edit port forwards		
ssh 👻 eq	Delete host		
		Saving screenshot Screenshot is being saved.	

Long Press to Select Connection

ConnectBot

```
Color category
```

gray

```
Font size (pt)
```

Use pubkey authentication

Use SSH auth agent

No

#### **Post-login automation**

Commands to run on remote server once authenticated

23 🔁 🛋 84° 2:50 📚 💾 » 🛢

You can configure Pubkey authentication! Use Post-login automation to run a command on connect.

#### ConnectBot

#### Compression This may help with slower networks Start shell session Disable this preference to only use port forwards Stay connected Try to reconnect to host if disconnected DEL Key Delete Encodina 2:50 📚 🕌 » 🗎

Remove Start Shell for Tunnel Only, Stay connected will retry if tunnel closes



There are no user settable proxy settings available with FF Android

<b>ⓑ</b> ← ♂ about:config	C' ★ 🗄
proxy	
Add a New Setting	
network.http.max-persistent-connections-per-proxy	
20	
Modify Reset	
network.http.proxy.pipelining	
true	
Toggle Reset	
network.http.proxy.version	
1.1	
Modify Reset	
network.proxy.autoconfig_retry_interval_max	
300	
Modify Reset	
network.proxy.autoconfig_retry_interval_min	
5	
Modify Reset	
network.proxy.autoconfig_url	
Modify Reset	
network.proxy.failover_timeout	
	🔁 🖬 84° 2:52 📚 🕌 » 🗎

FF supports proxy, but you have to set the values through about:config

Blank		
	network.proxy.http	
1. 10	Modify Reset	
100	network.proxy.http_port	
	3128	
	Modify Reset	
	network.proxy.no_proxies_on	
	localhost, 127.0.0.1	
	Modity Reset	
	network.proxy.socks	
	Iocainost Medify Recet	
	Mouny neset	
Match Tun-	network.proxy.socks_port 8080	
nel Port	Modify Reset	
	network.proxy.socks_remote_dns	
Set True	true	
	Toggle Reset	
	network.proxy.socks_version	
	5 Medify Depart	
Plank	Modify Reset	
	network.proxy.ssl	

FF supports proxy, but you have to set the values through about:config

60 - 1	localhost, 127.0.0.1		
193	Modify Reset		
1 Gal.	network.proxy.socks		
11 1 10	localhost		
100	Modify Reset		
	network.proxy.socks_port		
	8080		
	Modify Reset		
	network.proxy.socks_remote_dns		
	true		
	Toggle Reset		
	network.proxy.socks_version		
	5		
	Modify Reset		
Blank	network.proxy.ssl		
	Modify Reset		
	network.proxy.ssl_port		
	3128		
	Modify Reset	=none	
Must he 1	network.proxy.type		
	Modify Reset 5	s=System	
	<ul> <li>► ☆ ⋳</li> </ul>		- Al 84° 2.53 😪 📑 » 🛔

FF supports proxy, but you have to set the values through about:config

#### Test your connection

🖸 🧲 🔺 what is my ip - Google Search		C	☆	÷
+You Search Images More -			Sign	in 🌣
Google what is my ip		×		2
Web Images Maps Shopping Applications More - Search tools				
Your public IP address is 206.196.99.162 - Learn more	Related searches			
What Is My IP <sup>®</sup>   Shows Your IP Address. www.whatismyip.com/ What Is My IP <sup>®</sup> - IP Address Lookup, Change IP, IP Whols Lookup, Internet Speed Test, Trace An Email, Host Name Lookup, User Agent, Server Headers IP Address Lookup - Internet Speed Test - How to Change Your IP Address - IP Tools	what is my ip <b>address and port</b> what is my ip <b>location</b> <b>speed test</b> what is my ip <b>speed</b> what is my ip <b>range</b>			
<ul> <li>What Is My IP Address? Lookup IP, Hide IP, Change IP, Trace IP and</li> <li>whatismyipaddress.com/</li> <li>IP address lookup, location, proxy detection, email tracing, IP hiding tips, blacklist check, speed test, and forums. Find, get, and show my IP address.</li> <li>IP Lookup - Blacklist Check - How do I change my IP address? - IP Address Tools 2,475 people +1'd this</li> </ul>	what is my <b>internal</b> ip what is my <b>router</b> ip what is my <b>local</b> ip			
IP Address Lookup - <b>What Is My IP</b> Address? whatis <b>myip</b> address.com/ <b>ip</b> -lookup Lookup details about an <b>IP</b> address including location, ISP, hostname, type, proxy, blacklist status and more. Trace, Track and Locate an <b>IP</b> address.				
What's My IP Address? Networking Tools & More	E <sup>→</sup> 84° <b>►</b> 2:	:55 <		»

Your IP Address should be the address of your ssh server

#### **Closing the Tunnel**

Last login: Mon Oct 7 Have a lot of fun	14:48:26 2013 from 71-	85-250-89.dhcp.stls.mo	.charter.com		
edw@bud:∼ \$					
$\times$			×	0	
$\sim$			C	~	
Disconnect	Сору	Paste	Port Forwards	URL Scan	Force Size
					84° 2:56 🛜 🔡 » 🛢

Go back to ConnectBot and tap menu and disconnect.

# **Closing the Tunnel**

ConnectBot: Ho	sts	
bud sock	s tunnel 34 minutes ago	$\bigcirc$
ed@dexte	er01 18 days ago	ightarrow
edw@buc	sluug.org:2206 1 minutes ago	0
ssh 🔻	username@hostname:port	
		Screenshot is being saved 📚 🕌 » 🗎

That's it!

#### Windows Approach

- What you need
  - Putty
  - Firefox
- We will assume you already have these.

# **Configure PUTTY session**

Real Putty Configuration		Reputty Configuration	? ×
Puttry Configuration         Category:         - Session         - Logging         - Terminal         - Keyboard         - Bell         - Features         - Window         - Appearance         - Behaviour         - Translation         - Selection         - Colours         - Connection         - Data         - Proxy         - Telnet         - Rlogin         - SSH         - Serial	Basic options for your PuTTY session         Specify the destination you want to connect to         Host Name (or IP address)       Port         bud.sluug.org       2206         Connection type:       Rlogin • SSH         Raw       Ielnet         Rlogin       SSH         Serial         Load, save or delete a stored session         Saved Sessions         Default Settings         Bud.Sluug.org Via Proxy         dexter01         dexter03         guardian         thepencilslinger.com         thepencilslinger.com Via Proxy         Clease window on exit	PuTTY Configuration         Category:         Category:         Terminal	ns controlling SSH port forwarding     accept connections from other hosts   ts do the same (SSH-2 only)   s:     Remove     ded port   8080   Add     Remote   IPv4   IPv4
	Close window on e <u>x</u> it. ⊚ Always	X11 Tunnels Bugs Serial	
About <u>H</u> elp	<u>Open</u> <u>Cancel</u>	About Help	Open <u>C</u> ancel

#### Port forward should look like this.

🔀 PuTTY Configuration		?
Category:	233	
Logging     Logging     Terminal     Keyboard     Bell     Features     Window     Appearance     Behaviour     Translation     Selection		Options controlling SSH port forwarding         Port forwarding         Local ports accept connections from other hosts         Remote ports do the same (SSH-2 only)         Forwarded ports:         D8080
Colours Connection Data Proxy Telnet Rlogin SSH	н	Add new forwarded port Source port Destination Local Remote Dynamic
Kex Auth TTY X11 Tunnels Bugs Serial	•	
About	<u>H</u> elp	<u>O</u> pen <u>C</u> ancel

Make what ever other changes are needed for Putty and save sessions

# **Check PUTTY Event Log**

PuTTY Event Log	
2013-10-07 15:56:56 2013-10-07 15:56:56 2013-10-07 15:56:56 2013-10-07 15:57:10 2013-10-07 15:57:10 2013-10-07 15:57:10 2013-10-07 15:57:10 2013-10-07 15:57:10 2013-10-07 15:57:10 2013-10-07 15:57:11	Reading private key file "C:\Users\ed\Documents\Putty\bigkey.ppk" Offered public key Offer of public key accepted Access granted Opened channel for session Requesting X11 forwarding Remote debug message: No xauth program; cannot forward with spo X11 forwarding refused Local port 8080 SOCKS dynamic forwarding Allocated pty (ospeed 38400bps, ispeed 38400bps) Started a shell/command
	C <u>o</u> py <u>C</u> lose

# Configure Firefox to use local Socks Proxy

Options							X
		页		90		$\bigcirc$	i i
General	Tabs	Content	Applications	Privacy	Security	Sync	Advanced
General Da	ata Choice	s Network	Update Certif	ïcates			
Connect	tion						
Configu	ire how Fire	efox connec	ts to the Interne	t		S <u>e</u> tti	ngs
Cached	Web Cont	ent					
						Clear	Now
Ove	erride auto	matic cache	management				
Lim	nit cache to		MB of space				
Offline	Web Conte	ent and User	Data				
			bulu			Clear	Now
Tell	me when	a website as	sks to store data	for offline	use	Except	tions
The foll	owina web	osites are all	owed to store d	lata for off	ine use:		
						<u>R</u> em	ove
				OK	Cance		Help
				UK	Cance		Telh

nfigure Proxies t	Access the Internet			
No proxy				
Auto-detect pr	oxy settings for this net <u>w</u> ork	c		
<u>U</u> se system pro	xy settings			
Manual proxy of	onfiguration:			
HTTP Proxy:			Port:	3128
	Use this proxy server for	or all protoco	ls	
SS <u>L</u> Proxy:			Port:	8080
ETP Proxy:			Port:	8080
SOCKS Host:	localhost		Por <u>t</u> :	8080
	SOCKS v4 SOCKS	<u>v</u> 5		
No Proxy for:				
localhost, 127	0.0.1, 192.168.2.0/24			
Example: .moz	lla.org, .net.nz, 192.168.1.0/	24		
Automatic prox	y configuration URL:			
	21/		F	Reload

## Set Firefox to use proxy for DNS

Firefox						X
e about:config	☆ マ C P + Search	٩	•	÷	♠	8
ĺ						
	This might void your warranty!         Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.					
	Show this warning next time I'll be careful, I promise!					
×					0	

## Set option to true

Firefox T					x
about:config +					
< 🕙 about:config			🏫 🔻 🙋 🔎 - Search	₽ 🖬 🕂 🏦	2
Search: dns					×
Preference Name	<ul> <li>Status</li> </ul>	Туре	Value		₽₽
network.dns.disableIPv6	default	boolean	false		
network.dns.disablePrefetch	default	boolean	false		
network.dns.ipv4OnlyDomains	default	string			
network.dnsCacheExpirationGracePeriod	default	integer	2592000		
network.proxy.socks_remote_dns	user set	boolean	true		
social.manifest.facebook	default	string	{"origin":"https://www.facebook.com","name":"Face	book Messenger","workerURL":"https://	/

#### Test your IP



## Warnings!

- These settings ONLY affect Firefox!
- Add-ons, such as Flash may bypass proxy settings!
- Other apps will not know about the proxy and may bypass it entirely leaving you defenseless.
- If you are rooted you can try tsocks to direct all traffic via socks. (I have never done this)
- For windows, there are several Socks Proxy Capture (SocksCap, WideCap, etc) to make non-socks apps socks complaint.