Improving Security and Convenience with SSH Tunnels

Brett Viren

2008/03/19

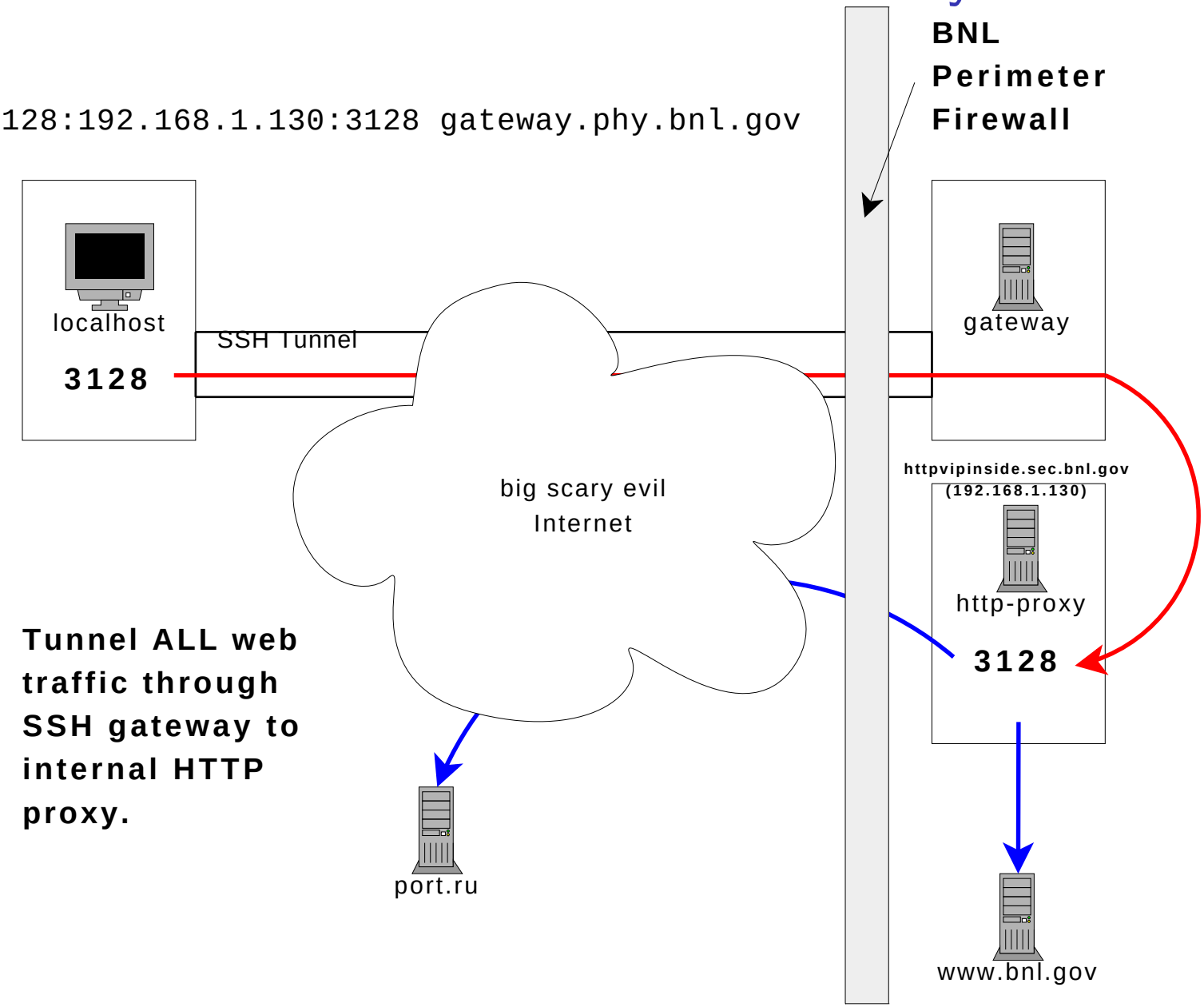
The problems

Some problems with Web, Email and other applications for mobile computing:

- Connecting with local, untrusted networks.
  - Exposure to additional attack vectors (DNS spoofing, man-in-the-middle).
  - Privacy compromised for all unencrypted communication.
  - Subject to local policy (sites blocked)
- Connecting to disparate networks
  - BNL internal, BNL wireless, home, hotel.
  - Constant configuration changes are annoying.
  - Must respect rules for acceptable behavior.

Basic solution: SSH Tunnel to HTTP Proxy

```
ssh -L 3128:192.168.1.130:3128 gateway.phy.bnl.gov
```



Comments on SSH Tunnel to HTTP Proxy

- **All** web traffic goes through tunnel.
- Browsing is fully encrypted: no snooping or tampering is possible by others between your laptop and the gateway.
- You can access internal sites (PeopleSoft, `intranet.bnl.gov`).
- Browsing will appear to originate on `gateway.phy.bnl.gov`.
- Your behavior is subject to BNL Computer Use Agreement!
- Need to start the tunnel and configure the browser.
- Same method can work for sending (SMPT) and getting (IMAP/POP) email, printing, mounting disks and just about anything else you normally expect LAN access.

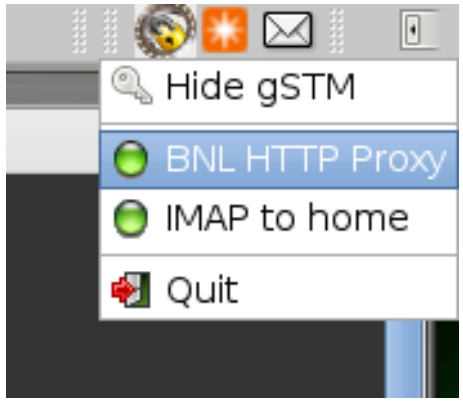
Adding convenience, SSH Tunnel Managers

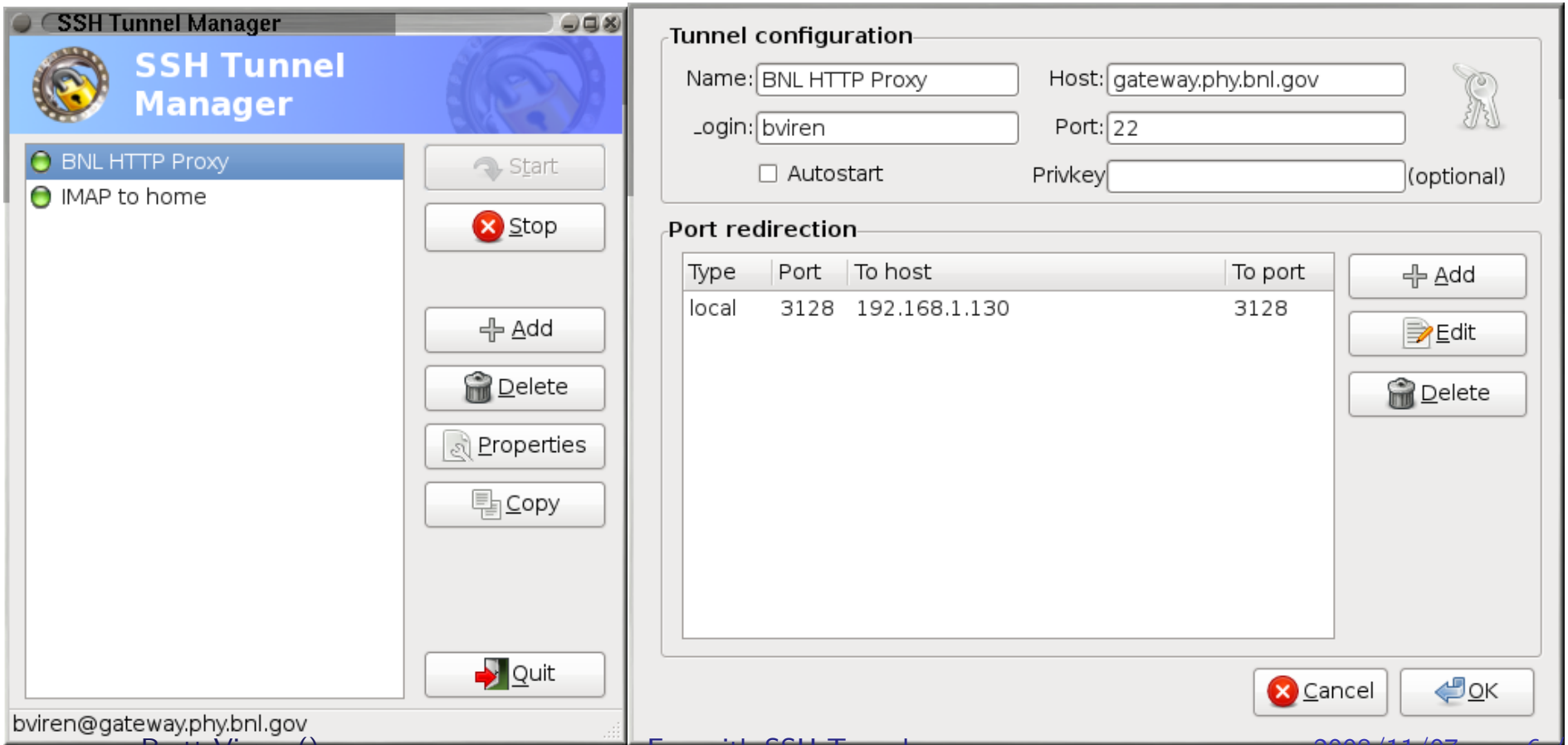
Use an SSH tunnel manager for convenience.

- **Linux** Gnome SSH Tunnel Manager (gstm) http://sourceforge.net/projects/gstm/
- **Mac** Mac SSH Tunnel Manager. http://projects.tynsoe.org/en/stm
- **Windows** PuTTY. http://www.chiark.greenend.org.uk/~sgtatham/putty/

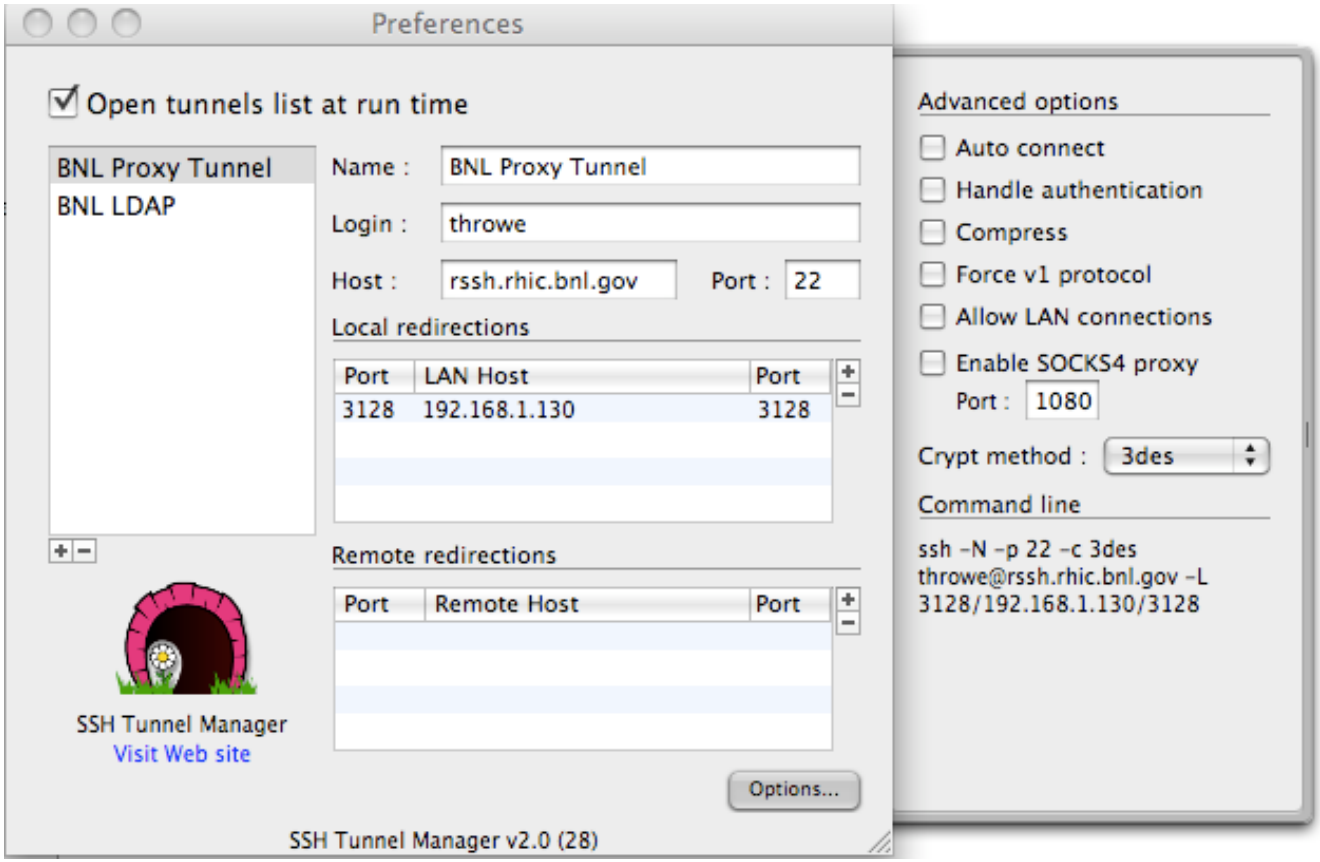
One time setup, thereafter just click a button.

gSTM on Linux



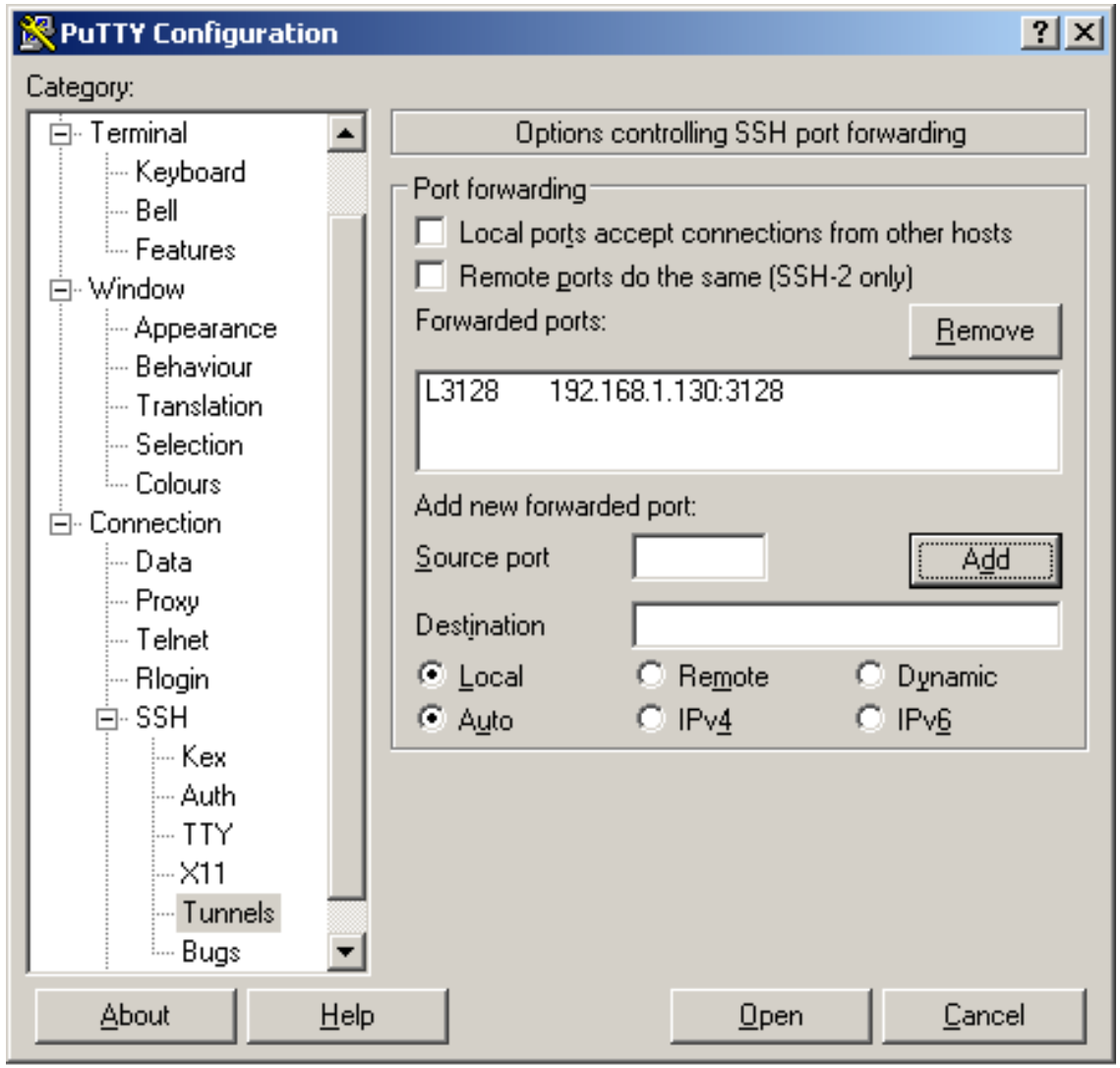


STM on Mac



`http://www.phy.bnl.gov/computing/index.php/Mac_SSH_Tunnel_Manager`

PuTTY on Windows



`http://www.phy.bnl.gov/computing/index.php/PuTTY_SSH_tunnel`

Adding convenience, FoxyProxy Firefox plugin

Allows URL-pattern based proxy definitions.

Home setup
- Send all `*.bnl.gov` requests through
- Everything else, unproxied ($\rightarrow$ note `tinyproxy`)

BNL wireless
- Proxy to `http://192.168.1.140:3128`, or
- Tunnel in and proxy to `localhost:3128`.

On travel
- Tunnel in and proxy everything to `localhost:3128`.

`https://addons.mozilla.org/en-US/firefox/addon/2464`