VPNs – the promise and implications

or

How to get around annoyances like firewalls and access restrictions

Trevor Grove
CSCF Research Support, UW-DRCSCS

October 24, 2006

Overview

- What are VPNs?
- What are they good for?
- What do we have (what is the available technology)?
- What do I do if I want to use it?
- What’s next?
- Questions?

What are VPNs?

- VPN – Virtual Private Network
- Lots of definitions (Google "define: vpn"), most of which contain "tunnel", "public infrastructure", "encrypted", "remote access to corporate network", "private connection"
- My definition: a mechanism for teleporting a non-UW computer's network connection to UW
  - So that it has the effect of being plugged into an on-campus network port

What are they good for?

- Computers not located at UW are subject to various network restrictions:
  - IST firewall policies
  - Application access restrictions
  - Remote ISP policies
- Connecting a remote computer via a VPN makes the computer appear as if it’s on campus, so many restrictions are not applicable

What are they good for?

- Some of the facilities & services to which our VPN facilitates access (in no particular order):
  - Reading local newsgroups (see RT#41831)
  - Access to IST campus LDAP server:
    - uwldap.uwaterloo.ca; dc=uwaterloo, dc=ca; port 389
  - Access to mirror.cs for ISO images & online updates
  - OED lookups: http://www.lib.uwaterloo.ca/uwonly/weboed.html
  - UW pandemic "work from home" plan
  - Bypass email graylisting to on-campus addressees

What are they good for?

- More problems solved by a VPN:
  - UW library services (eg LexisNexis)
  - Windows xwin32 licencing (restricted to 129.97/16)
  - Access to cs-appserv (“asimov”)
  - ISP port 25 blocking and other ISP restrictions
  - IST firewall restrictions:
    - SMB/Samba, MySQL, X11, xdmcp: http://noc.uwaterloo.ca/cn/Stats/blocked
  - CSCF firewall: https://nsfw01.cs.uwaterloo.ca/index.html
  - Default domain becomes “uwaterloo.ca” – save typing!

What do we have?

- VPN server implementing PPTP (Point-to-Point Tunnelling Protocol):
  - Secure (encrypted) tunnelling mechanism to connect single systems to remote networks (eg home computer to UW network)
  - Encapsulates PPP (ISO layer 2) over an IP network using GRE protocol (Generic Routing Encapsulation, IP protocol # 47); like “dial-up PPP” but using an existing network instead of a phone-line
  - PPTP RFC 2637: http://www.ietf.org/rfc/rfc2637.txt
  - GRE RFC 2784: http://www.ietf.org/rfc/rfc2784.txt

What do we have?

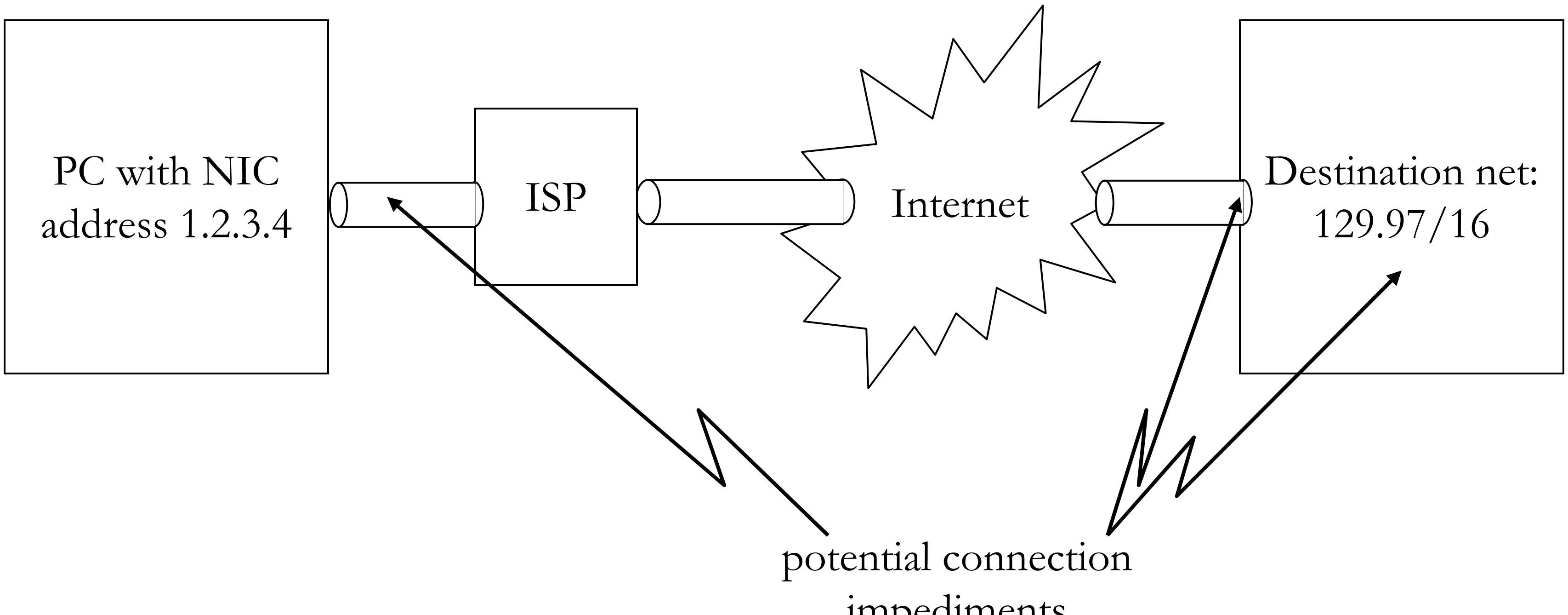
- PPTP informally:
  - Pick up network packets, NAT them to the assigned remote address, encapsulate and encrypt them, send them via the public Internet to the PPTP server, un-encapsulate the packets and deposit them on the remote network
  - Like a bridge for layer 3
- Not the same as IPSEC (layer 3) , L2TP (layer 2 PPTP + L2F à la Cisco), X11 tunnelling, proxy services

How does it work?

- On the client, create a virtual network interface at an address assigned by the VPN server
- That address is a PPP connection to the server (just like dialup)
- Client sends network traffic via that address to the server, which acts as a router for the traffic
  - Mac OSX client forces all traffic to go via the VPN, WinXP allows the client to make routing decisions (configure as "Use remote network")

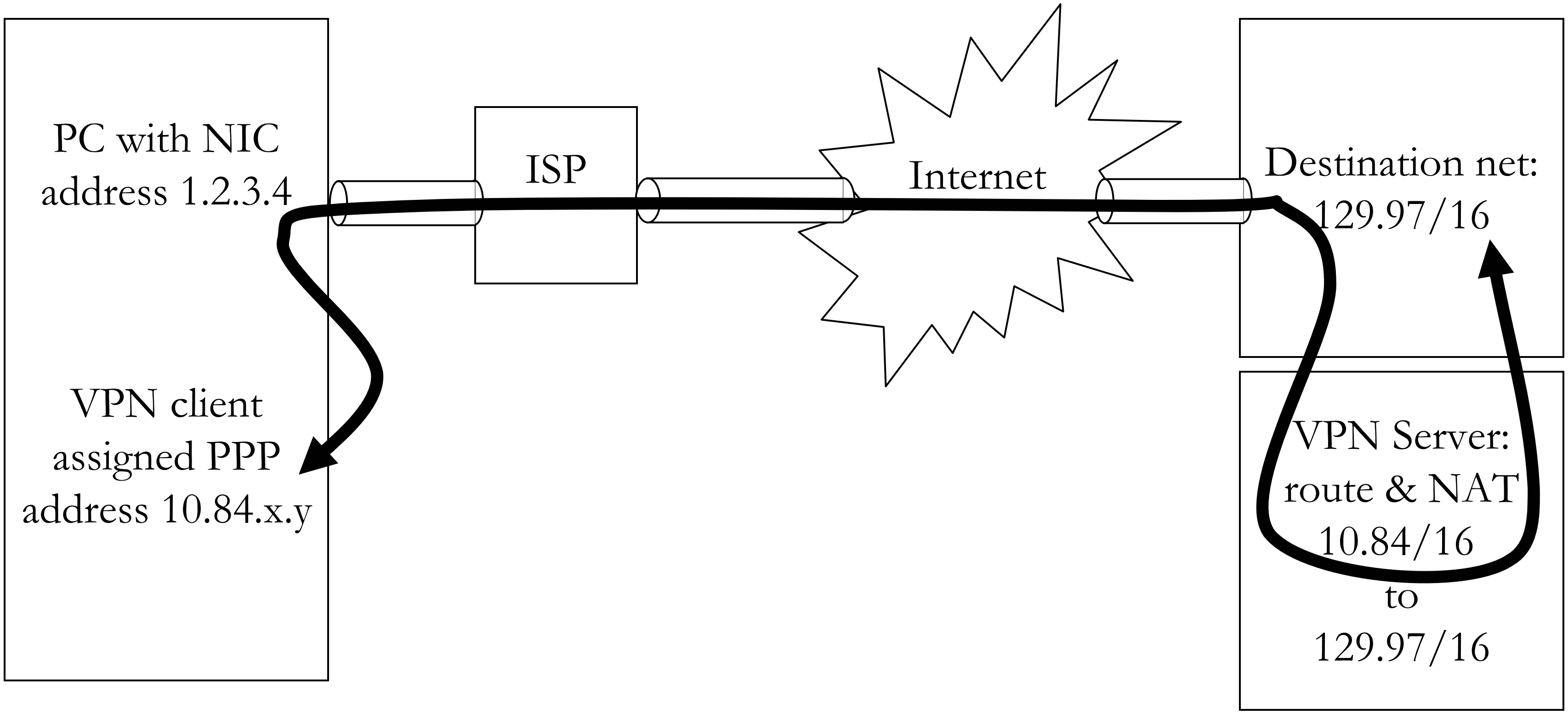
How does it work?

- Before the VPN connection:



How does it work?

- After the VPN connection:



What do I do if I want to use it?

- Clients: built in to Windows XP, Mac OS X
  - Linux: pptpclient is a SourceForge project but we can't get it to work (routing problem)
    - And it looks like passwords are stored in plaintext ☹
- Server: vpn1.cscf.uwaterloo.ca
  - Uses standard CS AD authentication
    - Requires "dial-in" permission, which is denied by default
  - Client must be set up for secure authentication and secure connection (required by server)

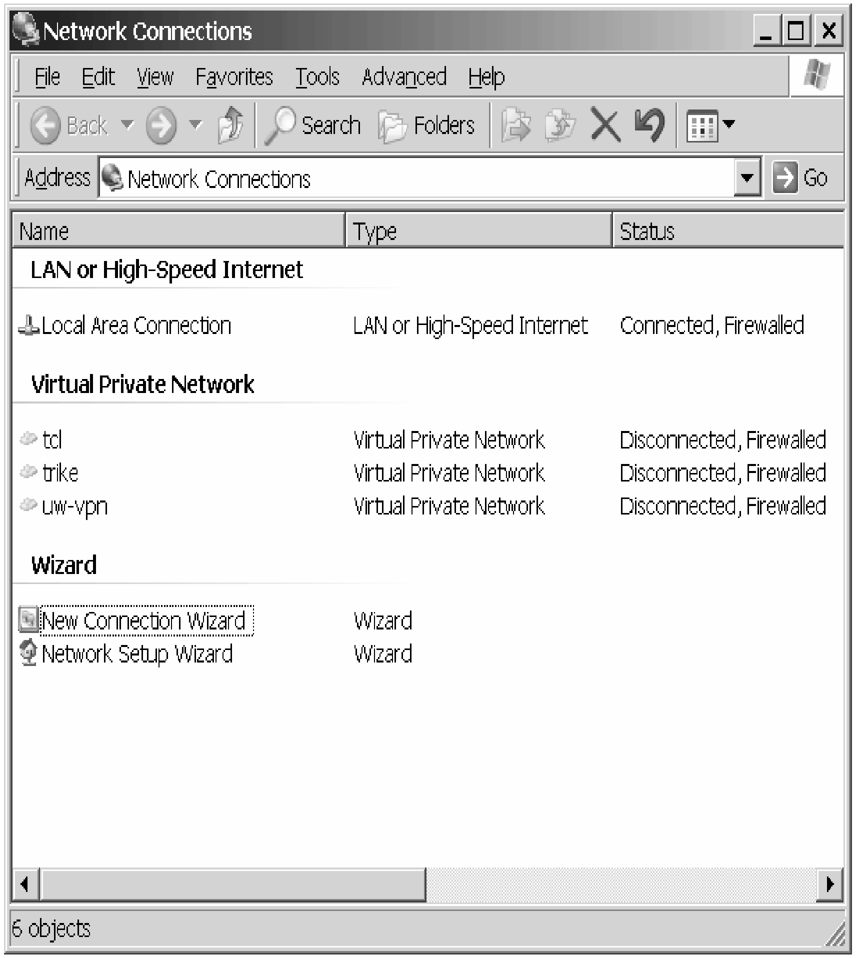
Client Setup (Windows)

- Windows setup:
  - New Connection wizard (in Network Connections)
  - Choose "Connect to the network at my workplace"
  - Choose "Virtual Private Network connection"
  - Enter an label for the connection
  - Choose "Do not dial the initial connection" (unless you actually are on a dialup ISP!)
  - Hostname: vpn1.cscf.uwaterloo.ca (129.97.152.21)
  - Add a shortcut if you want

Client Setup (Mac)

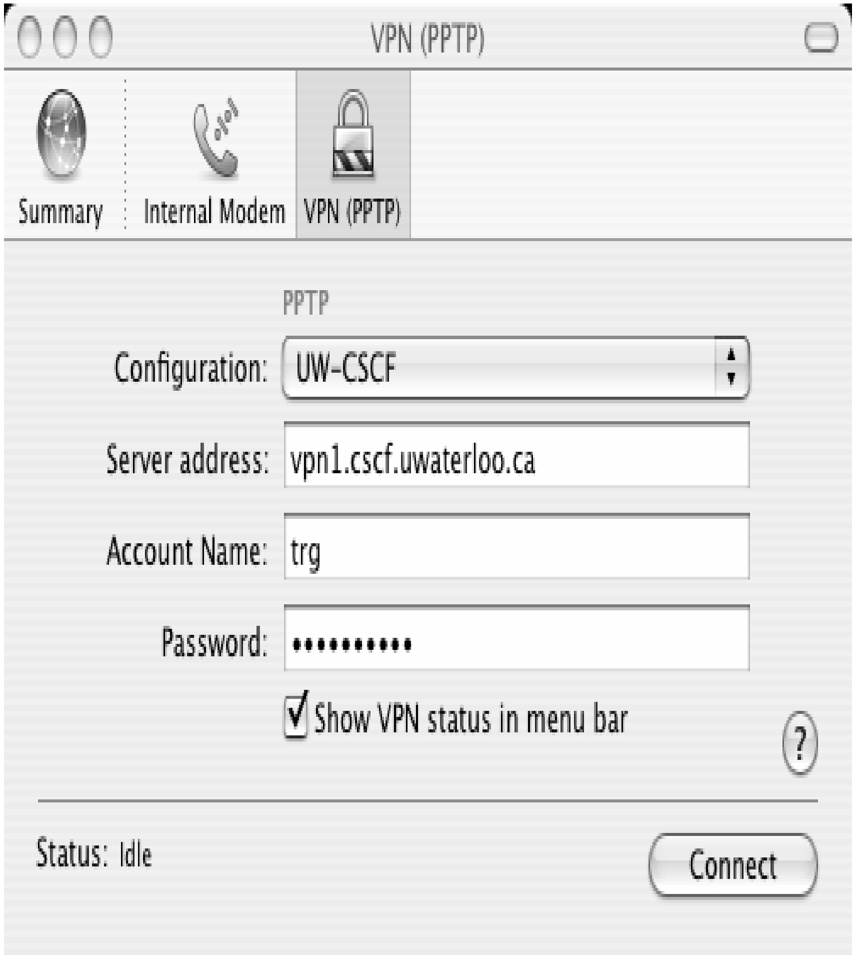
- Mac client setup:
  - Open "Internet Connect" in the Application folder
  - Click "VPN" on the toolbar
    - If you are asked for VPN type, choose PPTP
  - Fill in the server name (vpn1.cscf.uwaterloo.ca) and your CS-GENERAL AD credentials
  - Check the "Show VPN Status on menu bar" option
  - In the configuration selector, use the "Edit configurations" to set a meaningful label

Pictures



Name	Type	Status
LAN or High-Speed Internet		
Local Area Connection	LAN or High-Speed Internet	Connected, Firewalled
Virtual Private Network		
tcl	Virtual Private Network	Disconnected, Firewalled
trike	Virtual Private Network	Disconnected, Firewalled
uw-vpn	Virtual Private Network	Disconnected, Firewalled
Wizard		
New Connection Wizard	Wizard	
Network Setup Wizard	Wizard	

6 objects



Configuration: UW-CSCF

Server address: vpn1.cscf.uwaterloo.ca

Account Name: trg

Password: ••••••••••

☑ Show VPN status in menu bar

Status: Idle

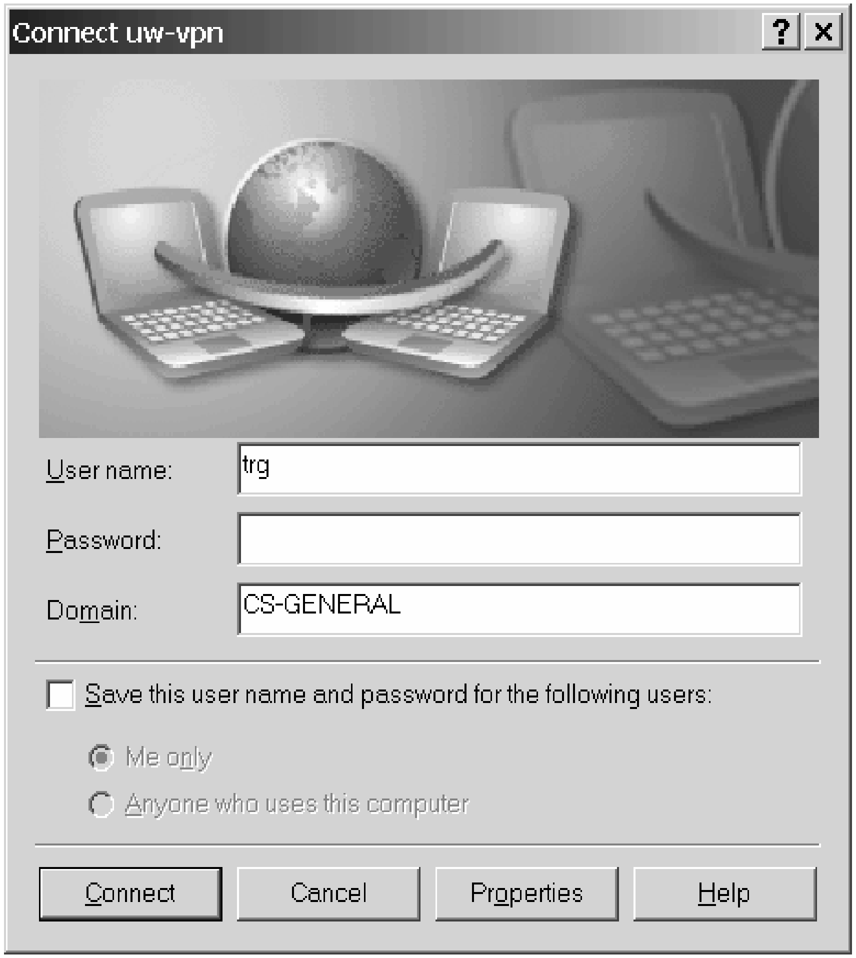
Client Activation (Windows)

- Using the Windows client:
  - Give yourself dial-in permissions in the AD (or ask a WWG member to do it for you)
  - Activate the connection you just created (via a desktop icon or the Network Connections)
  - Username: <your CS-GENERAL userid>
  - Password: <password for the preceding>
  - Domain: CS-GENERAL
  - Press “Connect”
  - Remember the authentication information, if you like

Client Activation (Mac)

- Using the Mac client:
  - Give yourself dial-in permissions in the AD (or ask a WWG member to do it for you)
  - Click "Connect" from the setup dialog
  - Or: click Connect from the menu bar icon you installed in the setup
  - Or: System Preferences -> Network -> Location: Automatic; Show: Network Status
    - Select the PPTP port and click "Connect"
  - Or: Apple -> Location -> Network Preferences {etc}

Pictures



User name: trg

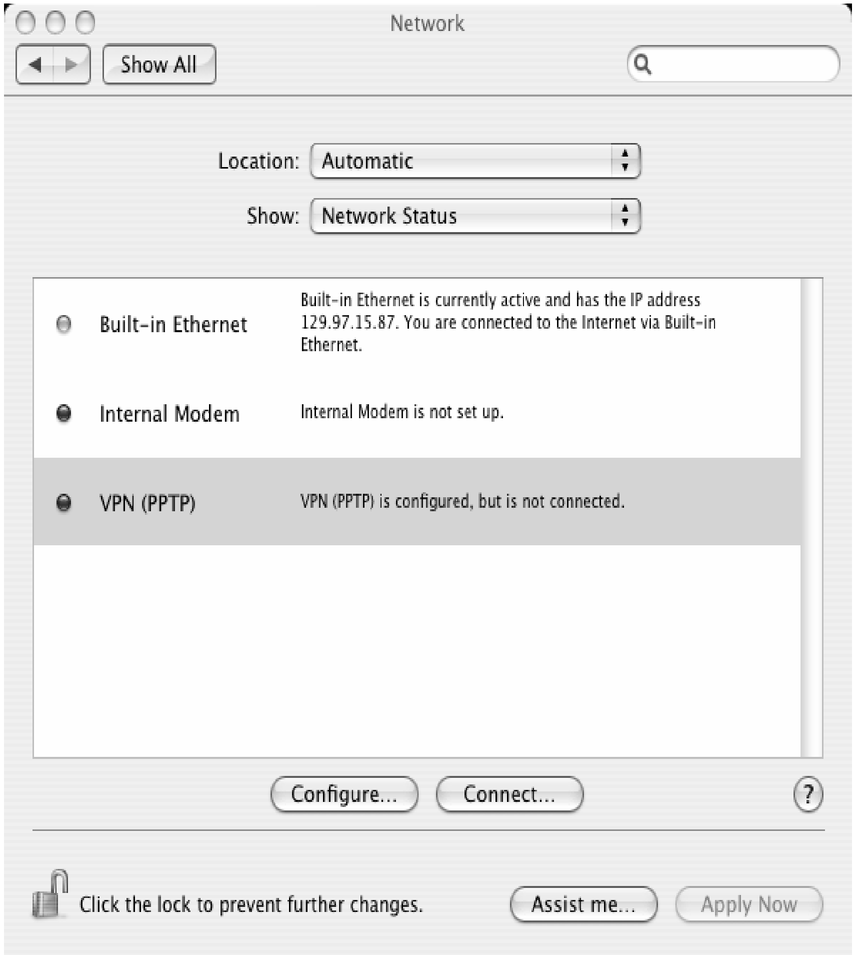
Password:

Domain: CS-GENERAL

□ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer



Location: Automatic

Show: Network Status

○	Built-in Ethernet	Built-in Ethernet is currently active and has the IP address 129.97.15.87. You are connected to the Internet via Built-in Ethernet.
●	Internal Modem	Internal Modem is not set up.
●	VPN (PPTP)	VPN (PPTP) is configured, but is not connected.

Click the lock to prevent further changes.

What’s next?

- Find a working solution for Linux clients
  - Get pptpclient figured out
  - The Linux community seems to favour an open-source (as opposed to open-standard) solution called OpenVPN: http://openvpn.net/
    - Builds connections tunnel using SSL, so it is a layer 4.5 solution
  - We could investigate running an OpenVPN server beside the PPTP server to serve Linux clients
- Expand the “internal” user community of the VPN
  - Within CSCF; DRCSCS
- Wait for the campus-wide solution

Questions?