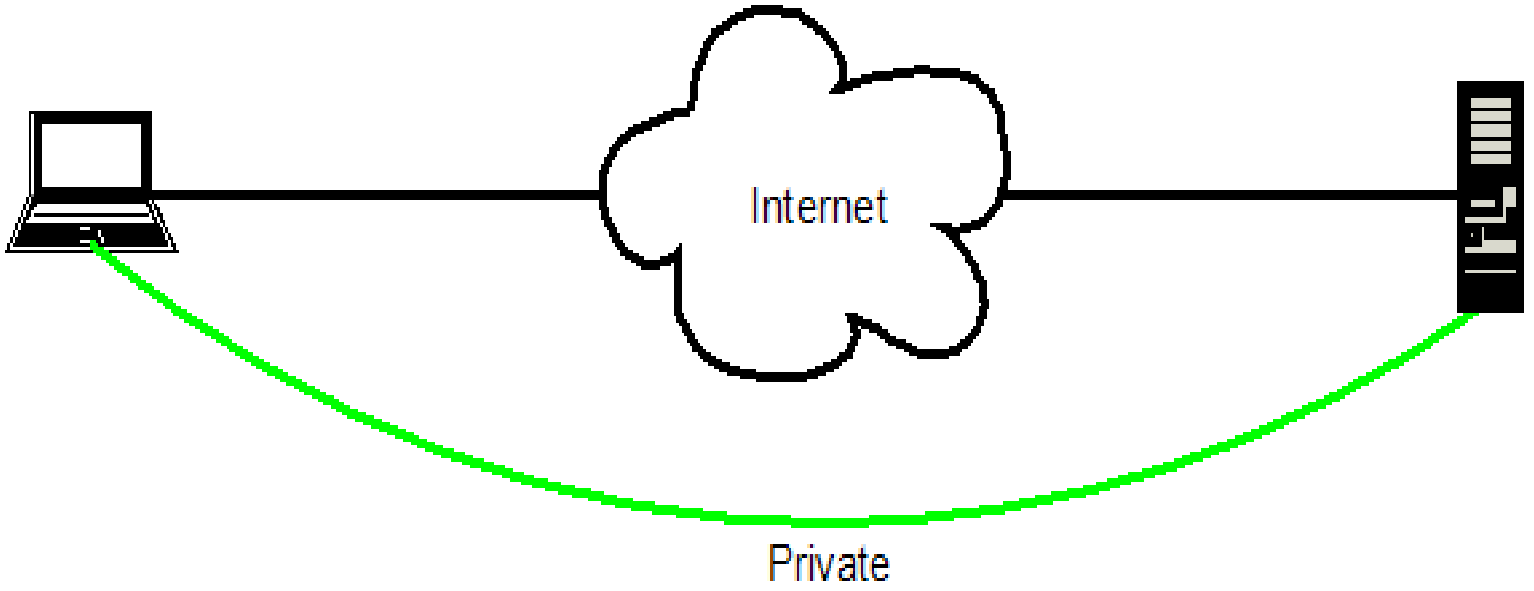
Open Source Enterprise VPN Solution
with OpenVPN and OpenBSD

Oscar Knight
John Pertalion
15.May.2008

VPN

- VPN – Virtual Private Network
  - A network just for me!

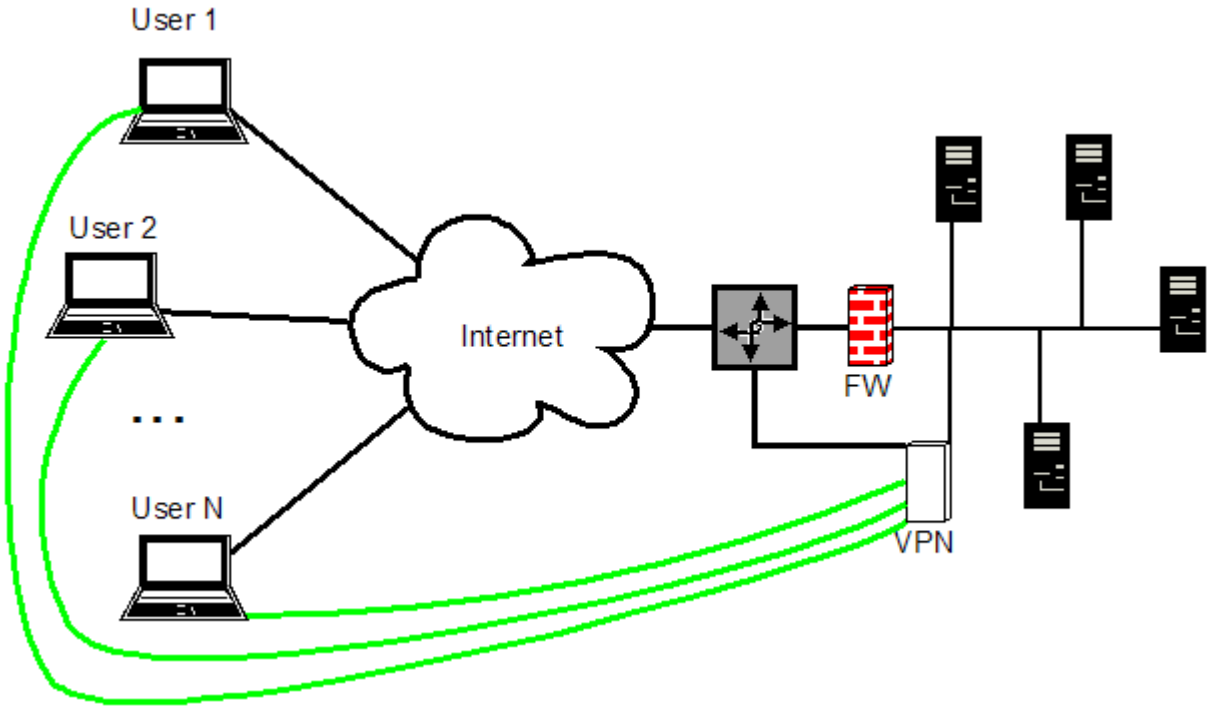


VPN Design

- Design Factors
  - Method of authentication
  - User affiliation types
  - Routed (Layer 3) or Bridged (Layer 2)
  - Client platforms
  - Number of users
  - Number of remote sites
  - Amount of network traffic

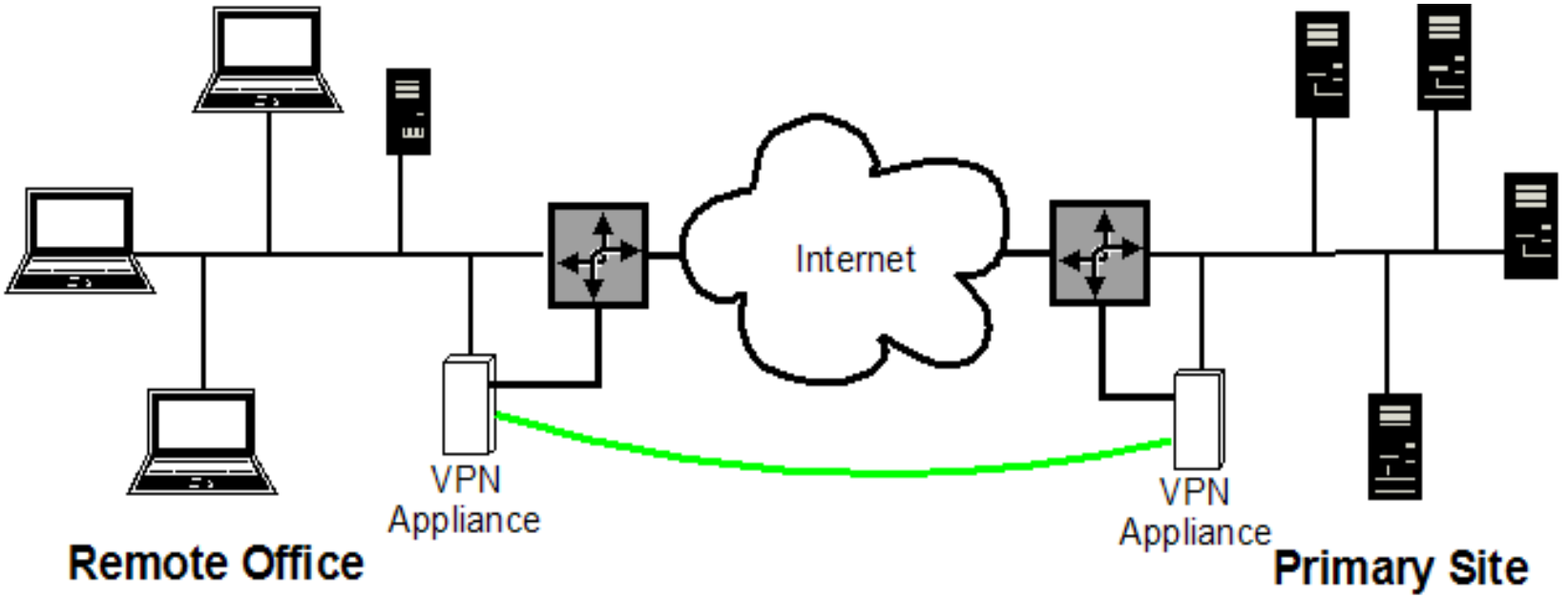
VPN – Road Warriors

- Road Warriors – Users that just want to connect their laptop/home computer. You'll have more than one! They will connect to may hosts.



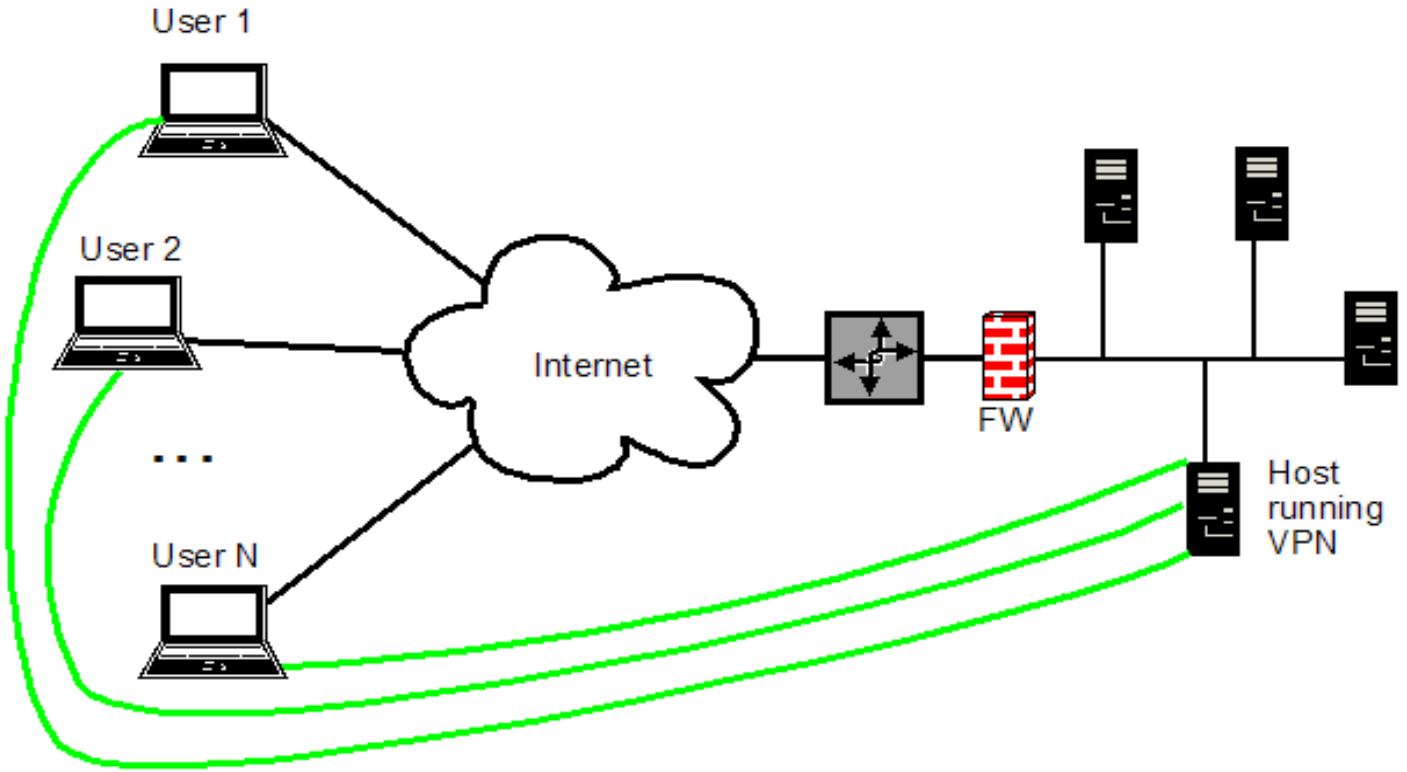
VPN – Site to Site

- Remote office with ***n*** employees & maybe a server.



VPN – One Host

- Special Case of road warriors
- User(s) just need access to one host



Road Warrior VPN History

- 2003 We Installed a commercial IPSec solution
  - Windows only client
  - Did not interoperate with anything
- 2004/5 Began searching for replacement
- 2006 first OpenVPN beta box
  - Ran this for about a year
  - It went well, not many users
- 2007 purchased new hardware
  - Training sessions
  - Small concurrent users, lots have tried

OpenVPN

- Runs on most platforms:
  - *BSD, Linux, Windows, Mac OS X
- Can be embedded
- Creates Layer 2 or Layer 3 VPNs, tun/tap driver
- Single binary for both server and client
- Works great even if client is NAT'ed

OpenVPN (cont)

- Authentication – one of two or both
  - Cert based, either on or off
  - username/password can be used with or in lieu of cert based authentication
- Authentication, additions possible via
  - Scripts
  - Plugins
- It just works!

Which OS

- We use OpenBSD for OpenVPN server OS
  - Pf
  - Carp
    - While pfsync will help pf, if you failover your users will need to reauthenticate.
  - Stability
- We will be replacing several small commercial firewalls with BSD/pf

VPN - Vendors

- Vendors that support systems at your site
- Most likely treated like road warriors
- Special because they are vendors!
- If possible limit access to just the nodes for which they are authorized
- Authenticate before network access, yes!

VPNs currently in use

- Enterprise
  - Road Warrior
  - Vendor Static
  - Vendor Road Warrior
- Commerce Unit 1
  - Bridged Instance
  - Routed Instance
- Commerce Unit 2
  - Routed
  - Clients run OpenVPN as service

Enterprise Road Warrior(instance)

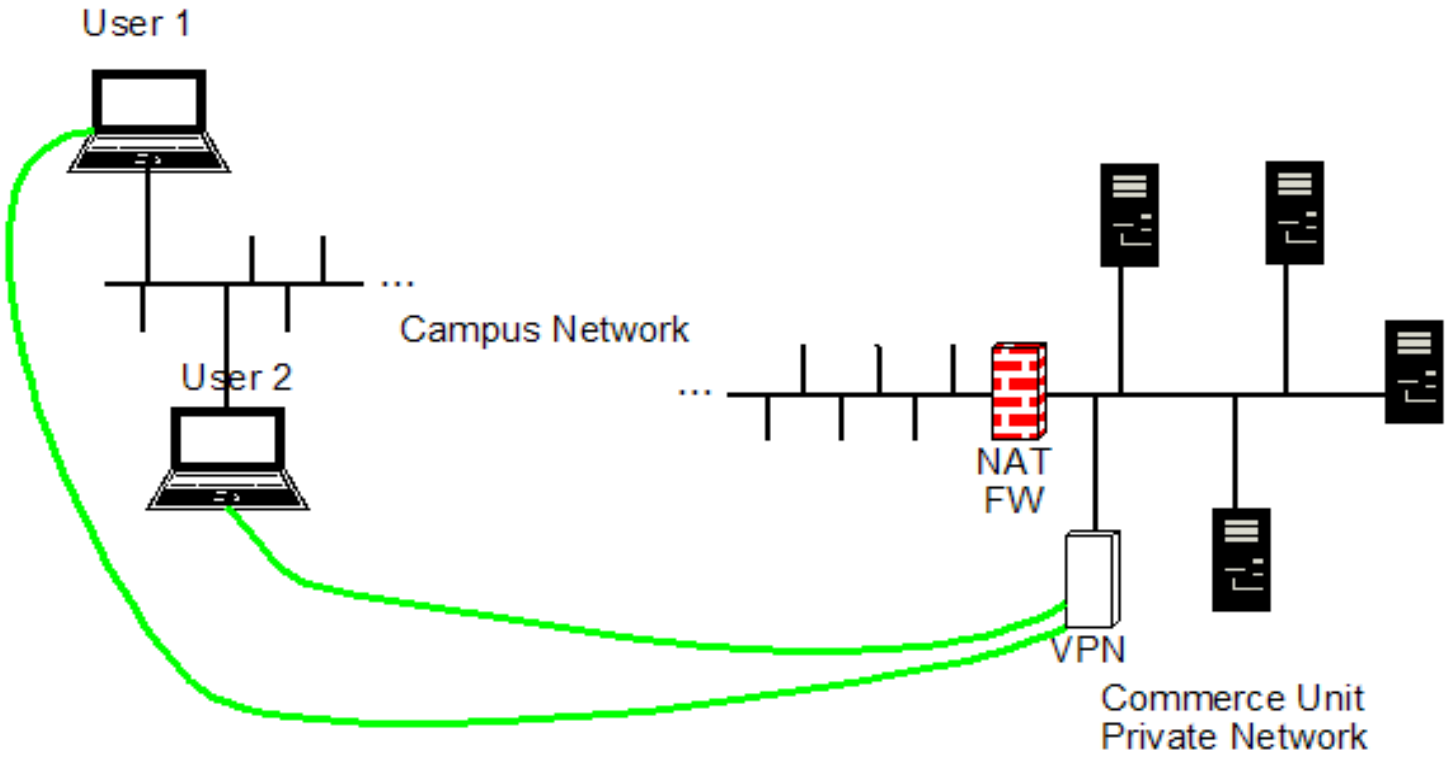
- For Faculty & Staff
- Username/Password authentication via LDAP
- Routed
- Traffic appears on the 'inside'
- NetReg is queried for IP of user's desktop machine(s). A pf anchor is created to allow access to user's desktop(s). Everyone wants access to their desktop!

Enterprise Vendor

- Static (instance)
  - For one external host to one or many internal hosts.
  - pf rules and routes are configured manually
  - Certificate based authentication
- Road Warrior (instance)
  - Leverged our NetReg system for addition vendor users and systems for which they have access
  - Process on VPN periodically pulls data from NetReg and creates config files
  - Username/password authentication

Commerce Units

- VPN has single network connection, DANGER!



Commerce Unit 1

- Two instances
  - Bridged
    - Cert based authentication
    - Bridges old IPX devices!
    - Soekris box is the remote device.
  - Routed
    - Username/Password authentication
    - Allows access to several servers on the private network

Commerce Unit 2

- One routed instance
- Private network has MS-Net Domain!
- Cert based authentication
- Clients run OpenVPN as client AND it starts as a service

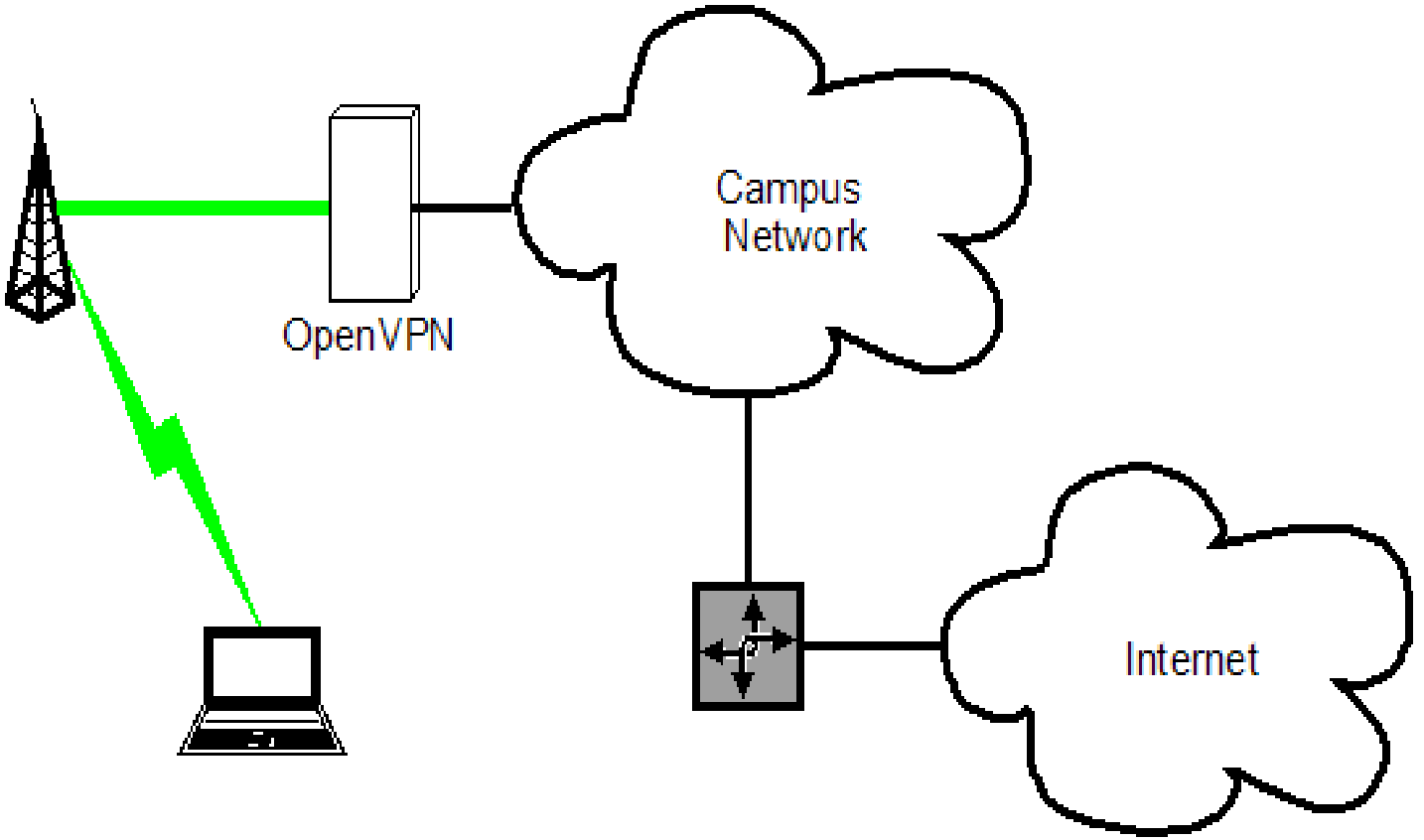
VPNs in progress

- Wireless
- Student

Wireless – in progress

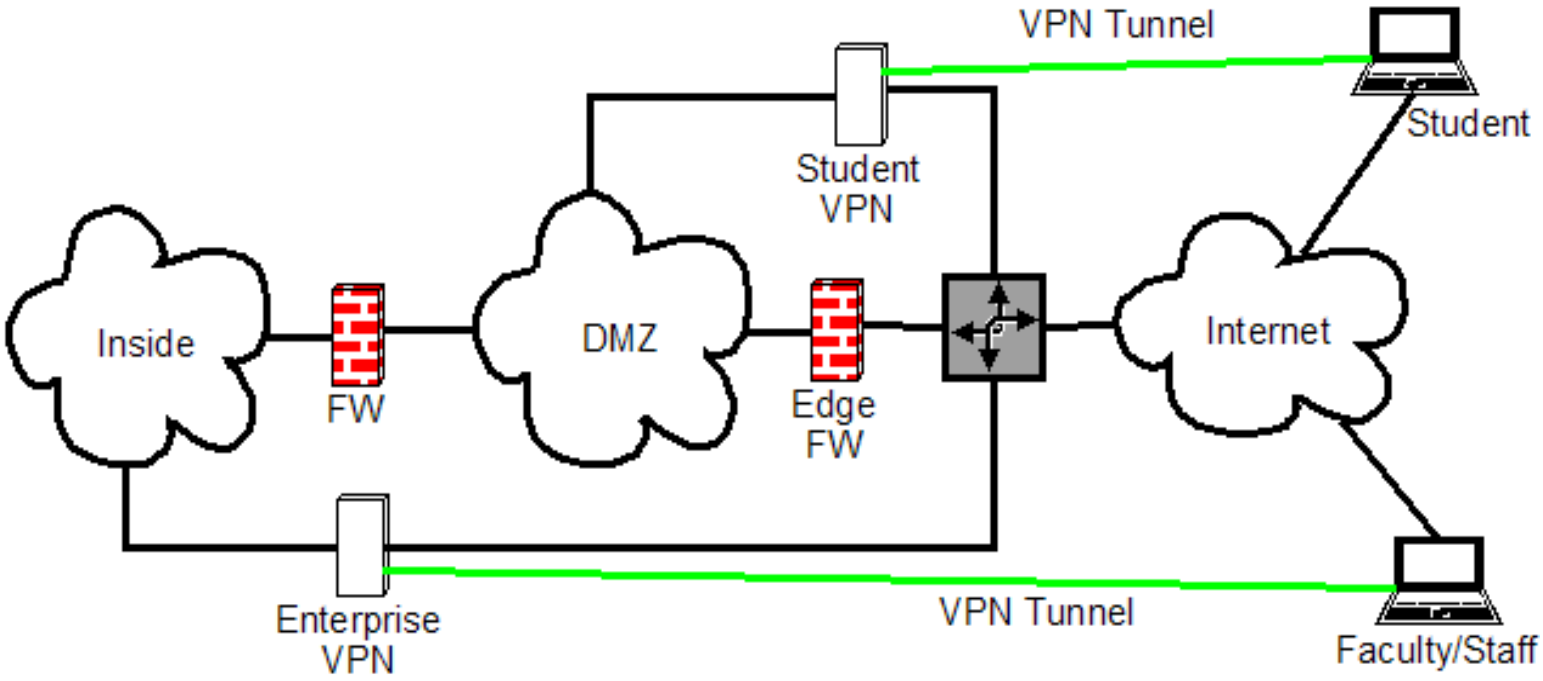
- Enterprise Wireless has multiple Networks
  - WPA
  - WEP
  - Guest – Captive portal, limited connectivity
  - Open – connection only with OpenVPN
- All wireless traffic is GRE tunneled back to central location. Different wireless networks are mapped to the appropriate VLAN.
- Open network is fronted with OpenVPN at this point.

Wireless (cont.)



Student – in progress

- Differs from Enterprise only in location in our network



OpenVPN/BSD/pf made possible

- Vendor Access
  - Multiple instances, Static and RW
  - Access limited by pf
    - Static it's manual
    - RW it's automatic
  - Access granted via custom Web interface
- Access to administrative desktops
  - pf anchors rule

Is OpenVPN secure?

- Peter Gutmann
  - http://www.cs.auckland.ac.nz/~pgut001/pubs/linux_vpn.txt
  - http://www.mail-archive.com/cryptography@metzdowd.com/msg05159.html
- While no one will bless OpenVPN, it's hard to find critics.
- There have been problems, most severe have been related to OpenSSL.
- Current stable 2.0.9 has seen few issues
- http://secunia.com/search/?search=openvpn

pfSense

- Check out pfSense
- A quick way to get openvpn up and running.

References

- www.openvpn.net
  - The HowTo really does tell you all you need to know.
- Book: OpenVPN -Building and Integrating Virtual Private Networks by Markus Feilner
- Book: The Book of PF by Peter N.M. Hansteen

Thanks!

- James Yonan, creator of OpenVPN
- All of the *BSD developers
- Dan Langille
- Everyone at BSDCan