CSI3670
VPN

Erik Fredericks (fredericks@oakland.edu)

But first

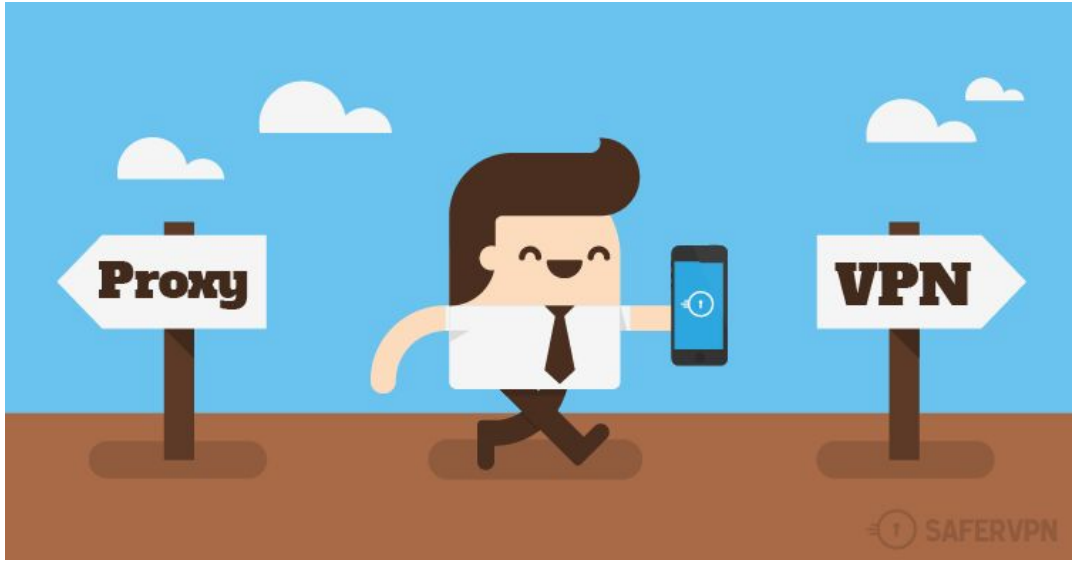
https://www.youtube.com/watch?v=Jct8VugYkis

https://www.youtube.com/watch?v=zcqxCeYkkhk

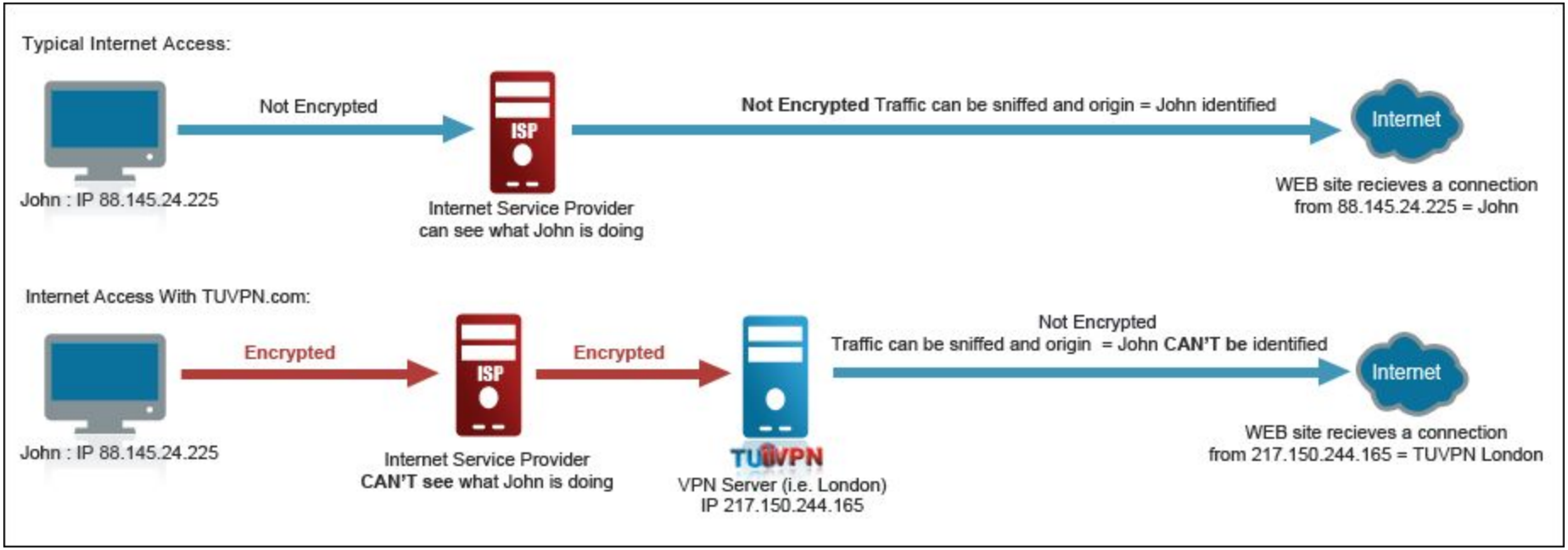
Overview

VPN

Enabling Technologies



Traditional Connectivity vs. VPN



VPN

Private line of communication via public lines of communication

E.g., via Internet

Popular to enable *private* remote access

Handy to have if you want to secure your communication when working on public WiFi

Case Study: Firesheep

Extension for Firefox browser

Packet sniffer

- Intercepts unencrypted data (cookies) from public websites
  - E.g., Twitter, Facebook

Enables person to easily hijack your account

https://en.wikipedia.org/wiki/Firesheep

Demo

https://www.youtube.com/watch?v=ZtZPR-TAEZw

(Starts at about 1:50)

Published in 2010, but still relevant?

This is basically Wireshark!

How to Counteract?

Use HTTPS (secured HTTP protocol) site-wide

(Watch video again, at 4:00)

Have a password-protected network (preferably not WEP)

Doesn’t help if you give your attacker the password!

VPN

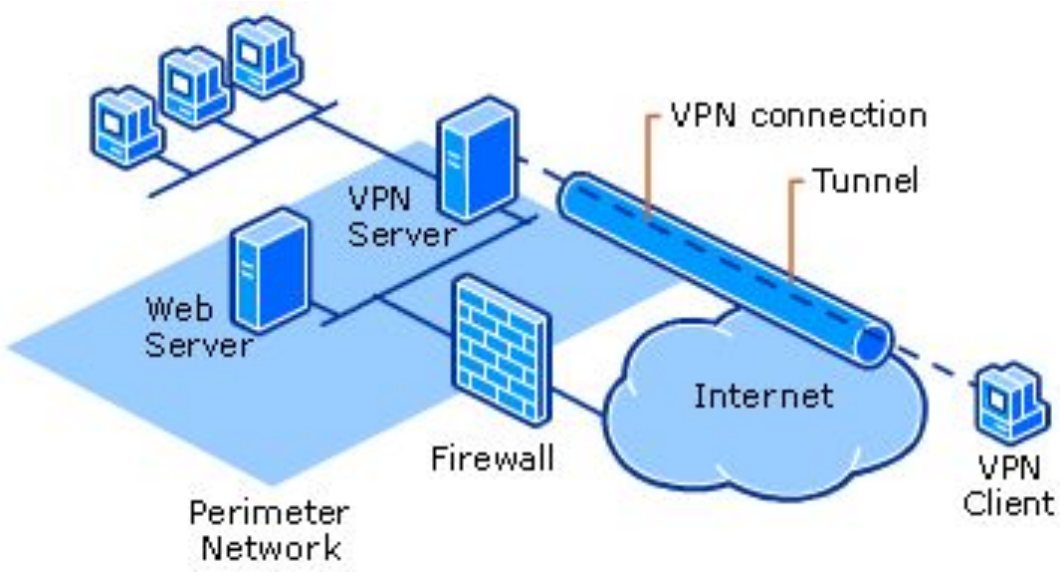
VPN

Access intranet remotely

Much more secure as you’re using your own network

Scalable

VPN


VPN connection
Tunnel
VPN
Server
Web
Server
Internet
Firewall
VPN
Client
Perimeter
Network

VPN Technology

Two connections made:

- One through the Internet
- One to the VPN host

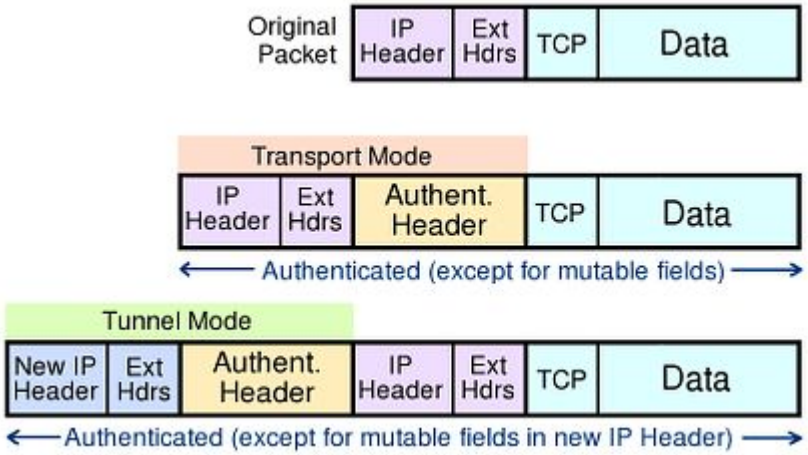
General steps:

1) Be online
2) Connect to VPN server (VPN gateway)
3) Authenticate user connection
4) Create VPN tunnel (encapsulating packets, etc.)

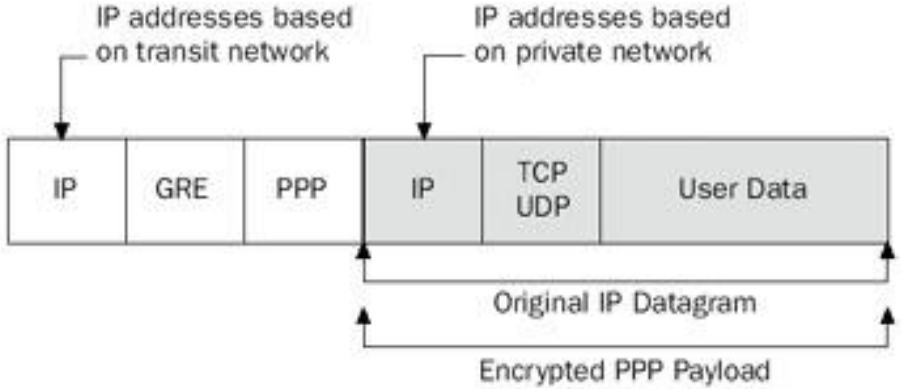
Packet Encapsulation

Different approaches (as if you expected anything different)

IPSec



PPTP



(Generic Routing Encapsulation header)

VPN Types

Hardware

- Router-based
  - ++ Network throughput
  - ++ Plug and play
  - ++ Dual-purpose (also a router)
  - -- Cost
  - -- Not terribly flexible

VPN Types

Software

- ++ Flexible (good for different domains / organizational units / multiple firewalls)
- ++ Relatively cheap (compared to hardware)

- -- Not as efficient
- -- Additional training required

VPN Requirements

User authentication

- Users are who they say they are!

Address management

- VPN clients need IP addresses (and private ones at that)

Encryption

- Anything in-between can’t read traffic!

Key management

- Encryption keys between client/server must be managed

Advantages of VPN

Cost-savings

- Reduce expensive long-distance leased lines / telephone charges
- Support relegated to VPN provider

Scalability

- Easy to grow your userbase
- Ethernet can handle

VPN Applications

Site-to-site

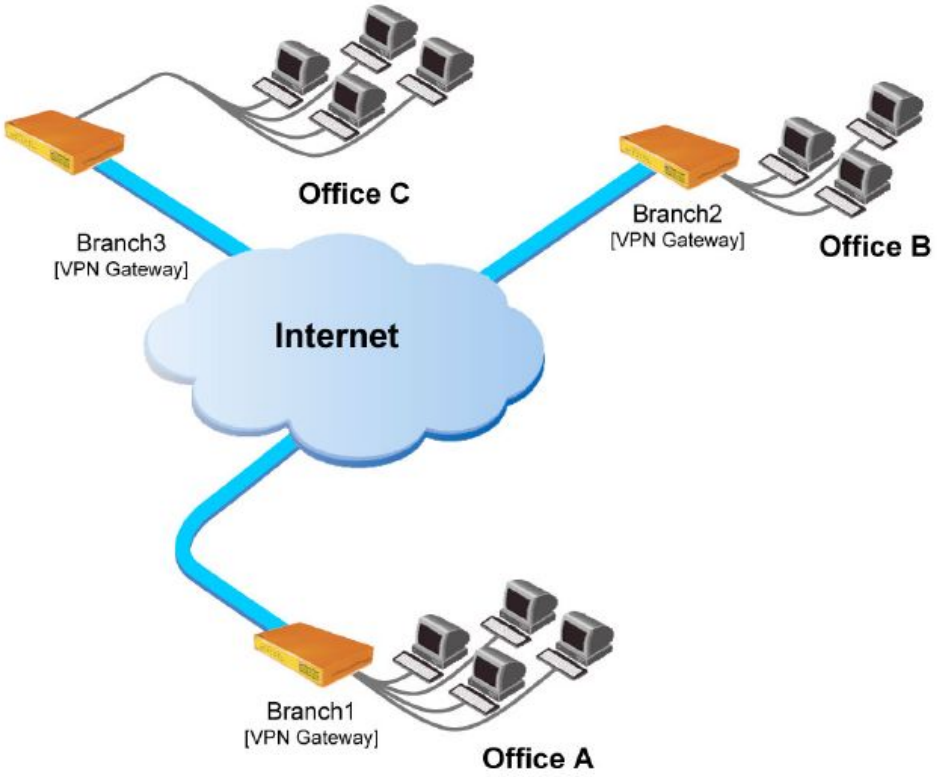
- Encryption between business offices
- Sent via branch office’s Internet to main office

Remote access

- Encryption between mobile/remote users to office

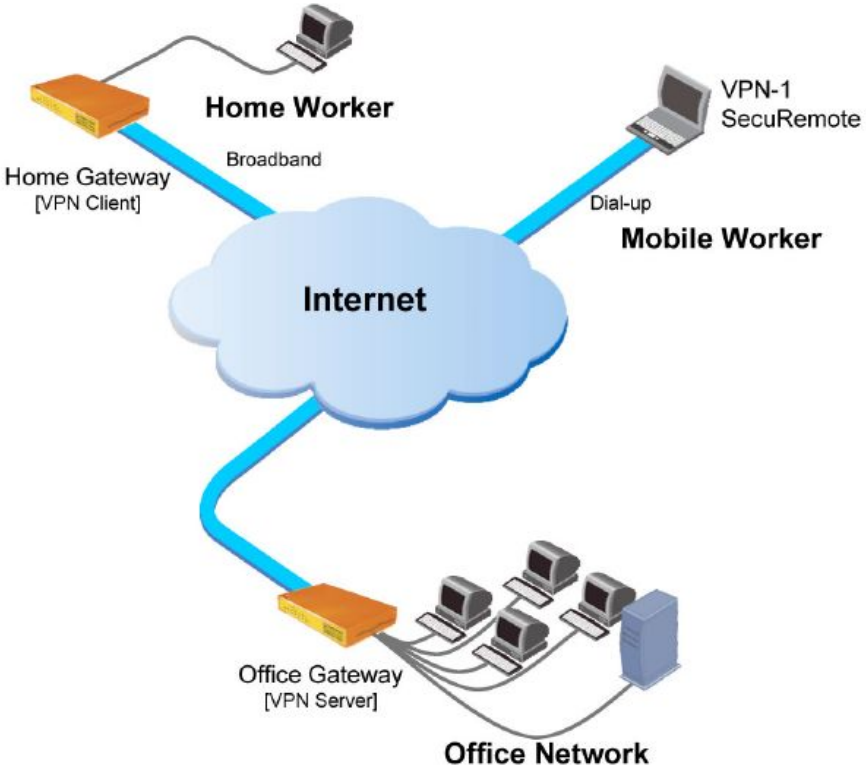
VPN Applications

Site-to-site



VPN Applications

Remote access



VPN vs. Proxy

Both conceal identity

Proxy server

- Intermediary between you and internet
- Any traffic from you will appear to come from the proxy server
- Generally *unencrypted* traffic

VPN vs. Proxy

Proxy server

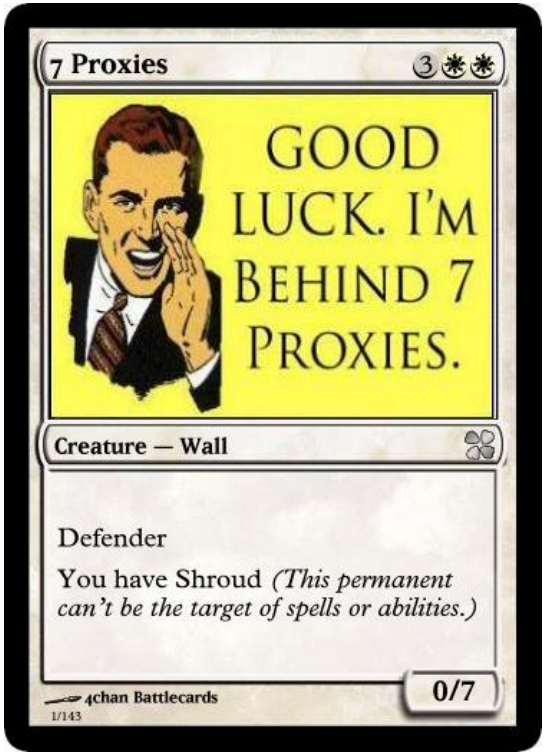
Generally inexpensive, sometimes free

Can be used to abstract your geographical location

E.g., purchasing violent Steam games in Germany

Many free public servers available

E.g., freeproxylists.net



VPN vs. Proxy

However,

- Only good for browsing the internet
- True location can be detected with JavaScript/Flash
- Not encrypted
  - ISP can see exactly what you’re doing
- Each browser must be configured

VPN vs. Proxy

VPN

- Encrypted tunnel from site to site
- ISP can only see that you’ve connected
  - Everything hidden behind VPN encryption protocol

VPN vs. Proxy

However,

- More expensive than proxies
- Can be slower
- VPN provider (if paid for) may log your activities

VPN (Windows)

1) Install VPN role
2) Enable Routing/Remote Access
3) Setup incoming IP addresses for clients
    a) Setup DHCP relay client, if auto-assigning
4) Setup Network Policy Server (authorization for remote clients)

http://techgenix.com/configure-vpn-windows-server-2012-r2/

VPN (Ubuntu)

OpenVPN

TLS/SSL VPN (certificates used to encrypt traffic)

1) Install OpenVPN
2) Configure certificate
   a) Build server and client certificates
3) Configure service
   a) Firewalls, IP forwarding, etc.
   b) Typically port 1194, but 443 is popular as well
      i) Popular because it's typically pre-opened in the firewall
4) Configure clients
   a) Directory structure, distribute certificates, etc.

https://www.digitalocean.com/community/tutorials/how-to-set-up-an-openvpn-server-on-ubuntu-18-04

Last-Minute Project Time!

Remember, presentations start **this Thursday**

Take the rest of class time to work on **this project**