Seismic Network Security

- On site
  - Networking
  - Servers
  - Sys-admin
- Off-site
  - “The Cloud”
  - Instruments
  - vNets
  - vpn’s
  - Add-on network hardware

PNSN
Pacific Northwest Seismic Network

Security vs. Usability

- The correct balance will be situation dependent and only probabilistically optimal.
- Where do we draw the line?
- Security adds complexity. Affects:
  - Scalability
  - Maintainability
  - Fragility
  - Usability
  - Resiliency

PNSN
Pacific Northwest Seismic Network

Motivators / vulnerabilities

- Why are they interested?
  - Anonymizing network connection
  - Plentiful sparsely monitored distributed DDOS attack sources
  - Processing power
  - Fun and reputation
  - Targeted
- Why do we care?
  - Induced failure
  - Bandwidth
  - Blacklisting
  - Escalation

PNSN
Pacific Northwest Seismic Network

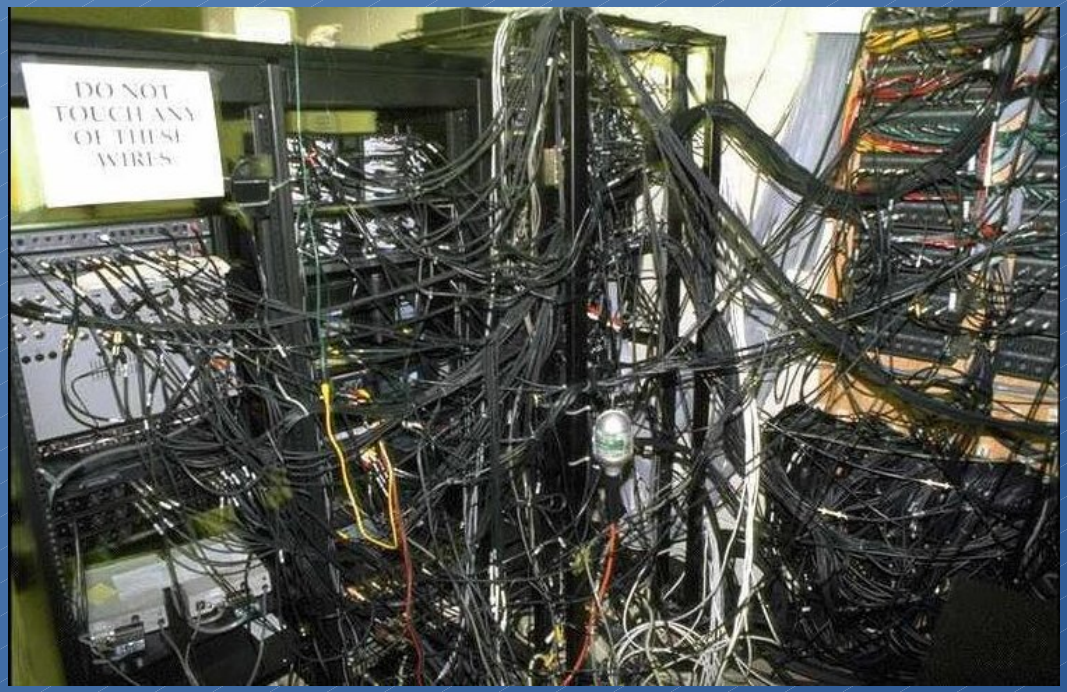
On-site security

- Perimeter firewalls
  - Filtering
  - NAT
- Private networks
- Host-based firewalls
- SELinux

PNSN
Pacific Northwest Seismic Network

On-site network

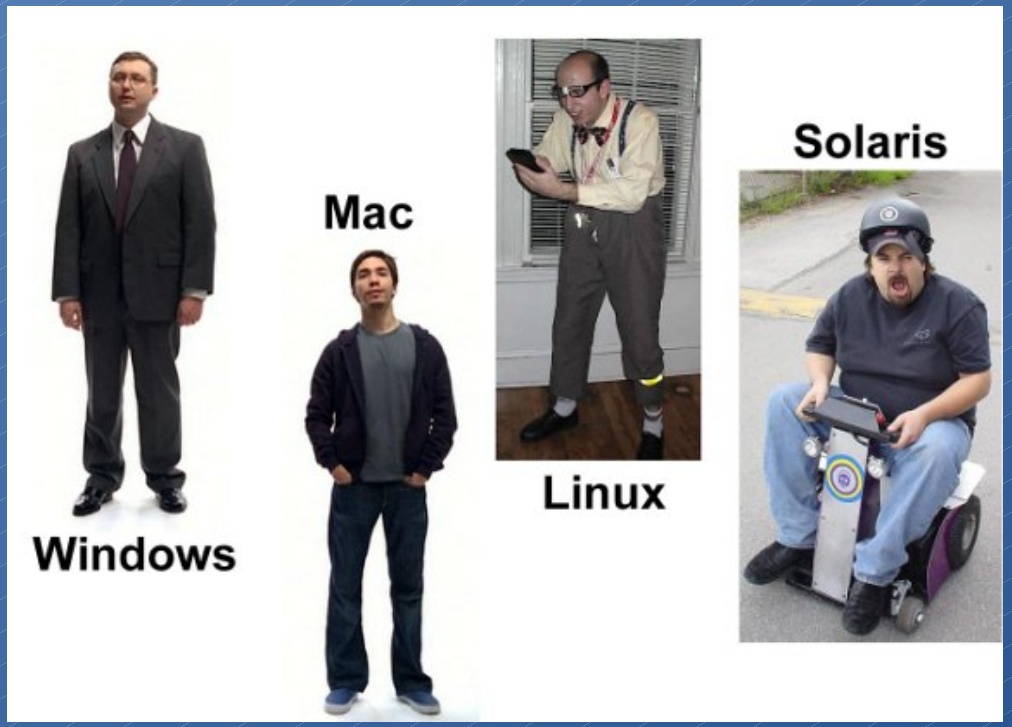
- Mix of public, NAT, and private networks
  - No Hardware Firewall
  - Software firewalls on all !!
  - “Zero Trust” config
  - IPv4 only (for now)
- Private networks
  - Carrier Grade NAT
  - Isolated Data Networks



PNSN
Pacific Northwest Seismic Network

On-site computing

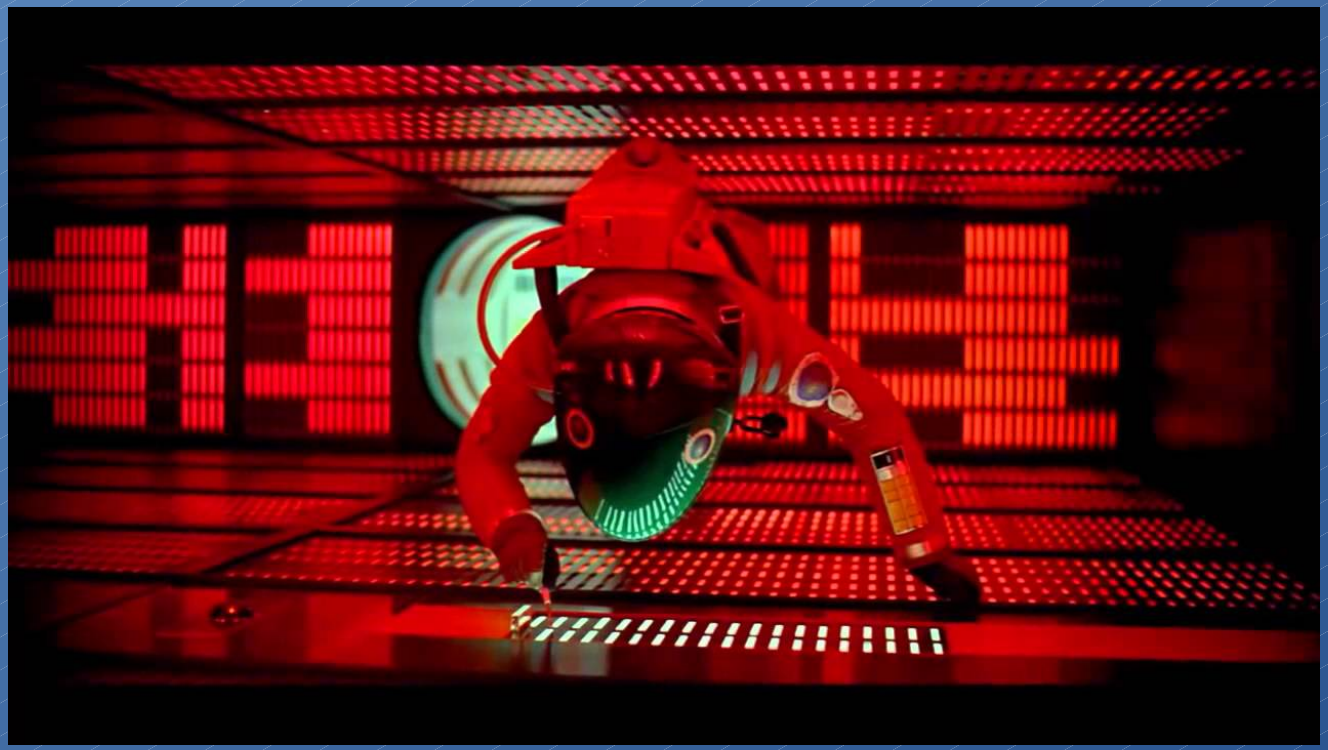
- Mostly bare hardware servers, some virtual
- Mostly CentOS-7
  - Software “iptables” firewall on all !!
  - SELinux !!
  - “Zero trust” config
- AWS cloud for web
  - Keep Web traffic offsite



PNSN
Pacific Northwest Seismic Network

On-site system administration

- Regular nmap scans, both internal and external.
- Tardis security scans
- System config audit & tracking



PNSN
Pacific Northwest Seismic Network

The Cloud

- Google*, Github, AWS, etc.
- Nominally as secure as site-hosted.
- Meltdown, Spectre, Rowhammer etc.
- More attractive target.
- Lots of major breaches in news. Mostly:
  - Simple configuration error.
  - Excessive sharing.
  - Phishing using data from LinkedIn, Facebook, organization web page etc.

PNSN
Pacific Northwest Seismic Network

Remote-site security

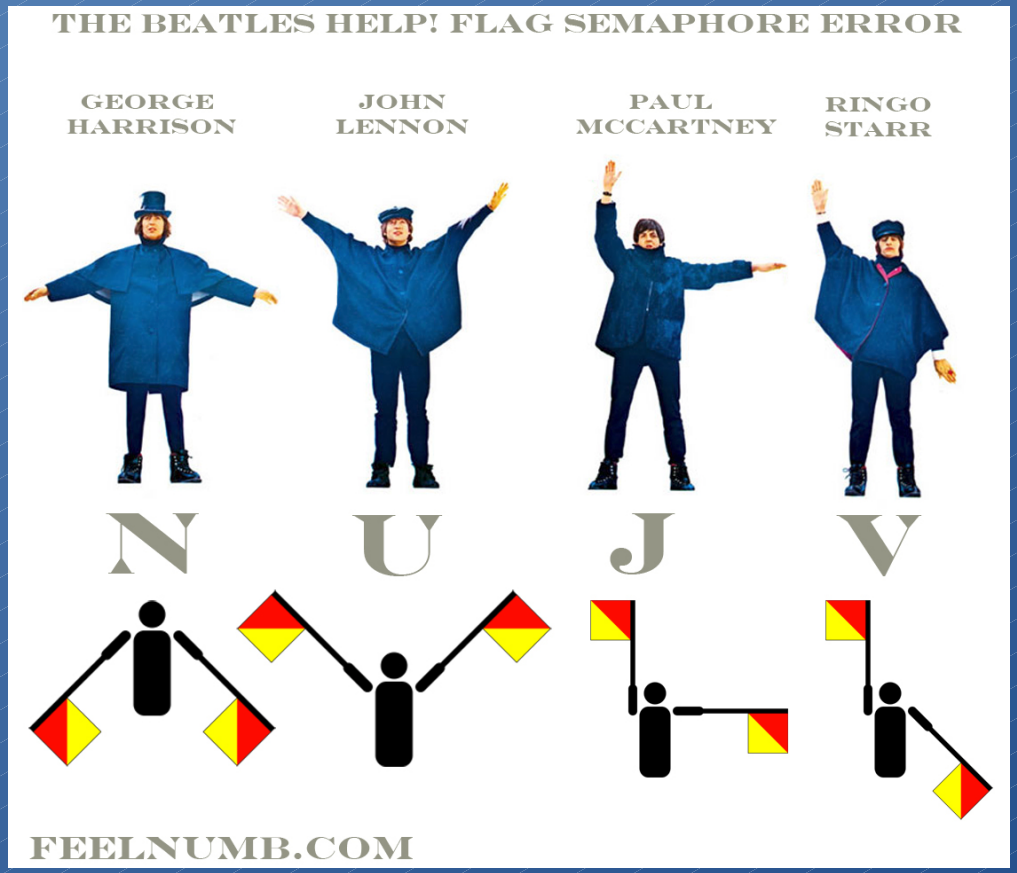
- Public network:
  - Host-based firewalls.
  - Turn off unnecessary and insecure services.
  - Move services to non-standard ports.
- Remote private networks:
  - External firewalls.
  - Port-forwarding NAT firewalls
  - Vnets
  - VPNs
  - Don’t expose unnecessary and insecure services.

PNSN
Pacific Northwest Seismic Network

Communication protocols

- Good:
  - SSH
  - SSL/TLS
  - HTTPS
- Securty through obscurity:
  - Earthworm:
    - Winston
    - waveserverV
    - Import/export
  - Many others
- Bad:
  - Telnet
  - FTP
  - HTTP
  - Proprietary

- Too soon to say
  - IPV6



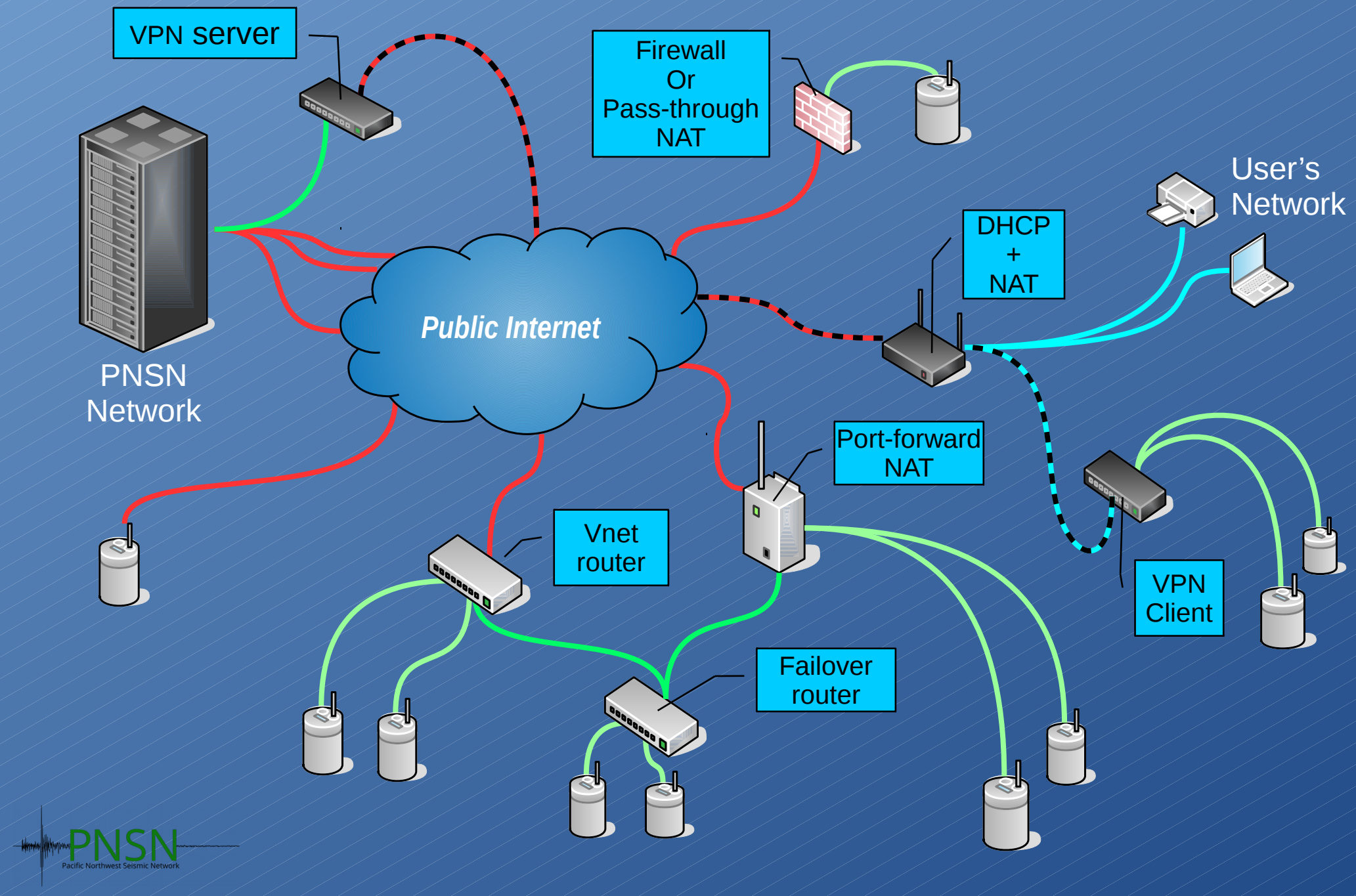
PNSN
Pacific Northwest Seismic Network

Instruments

- Vulnerabilities:
  - Vulnerable protocols
  - IOT scans
  - Hidden “features”
  - Back doors
  - DNS/MDNS
  - NTP
- Mitigations:
  - Firewalling
  - Non-standard ports
  - Requesting and using new features
  - Software and configuration fingerprinting
  - Additional hardware on-site.

PNSN
Pacific Northwest Seismic Network

Remote managed networks



PNSN
Pacific Northwest Seismic Network

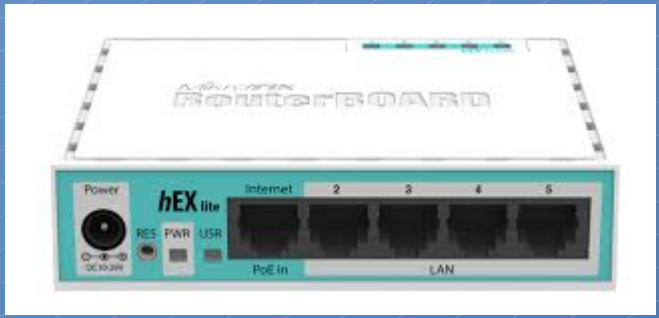
Raspberry Pi

- Simple but capable firewall
- Port-forwarding NAT
- Drop-in DHCP/NAT traversing OpenVPN client
- Other?

- Good:
  - Cheap
  - Powerful enough
  - Low power consumption
  - Easily configured/deployed
  - Flexible
  - Robust Linux OS
- Bad:
  - Hobby-grade construction
  - Hobby-grade accessories
  - Fabrication time

PNSN
Pacific Northwest Seismic Network

Mikrotik Routers



- Sophisticated firewall
- Port-forwarding NAT
- Pass-through NAT
- Virtual net router
- VPN client or server
- Failover routing
- Much much more...

- Good:
  - Powerful
  - Shockingly cheap
  - Compact
  - Flexible
  - Good construction
- Bad:
  - Powerful
  - Proprietary menu-based command structure.
  - Exposed proprietary communications protocols
  - Not ”mature” product
  - Complicated configuration: both too many options and not enough flexibility

PNSN
Pacific Northwest Seismic Network

Cell Modems and P2P radios

- Several useful security options:
  - Simple Firewall
  - Pass-through NAT
  - Port-forwarding NAT
  - VPN client (primitive)
  - Options improving with time

PNSN
Pacific Northwest Seismic Network

Discussion

PNSN
Pacific Northwest Seismic Network