Network Infrastructure: Detecting sick hosts

Review: risks to/from hosts.

- Keystroke Loggers
- Bots
- Spam engines
- Misbehaved users/clients (PEBCAK)
- Social engineering

Logs

- Syslog (centralized)
- logwatch, swatch
- Key is to ensure you are informed of what is *important* as opposed to every possible event. (or you'll start to ignore the logs)

Trends and alerts

- Bandwidth usage: - cacti
- Network events: - nagios
- Packet analyzers/dumpers for tracking down individual events.
- All the above depend on sanely designed network infrastructure.

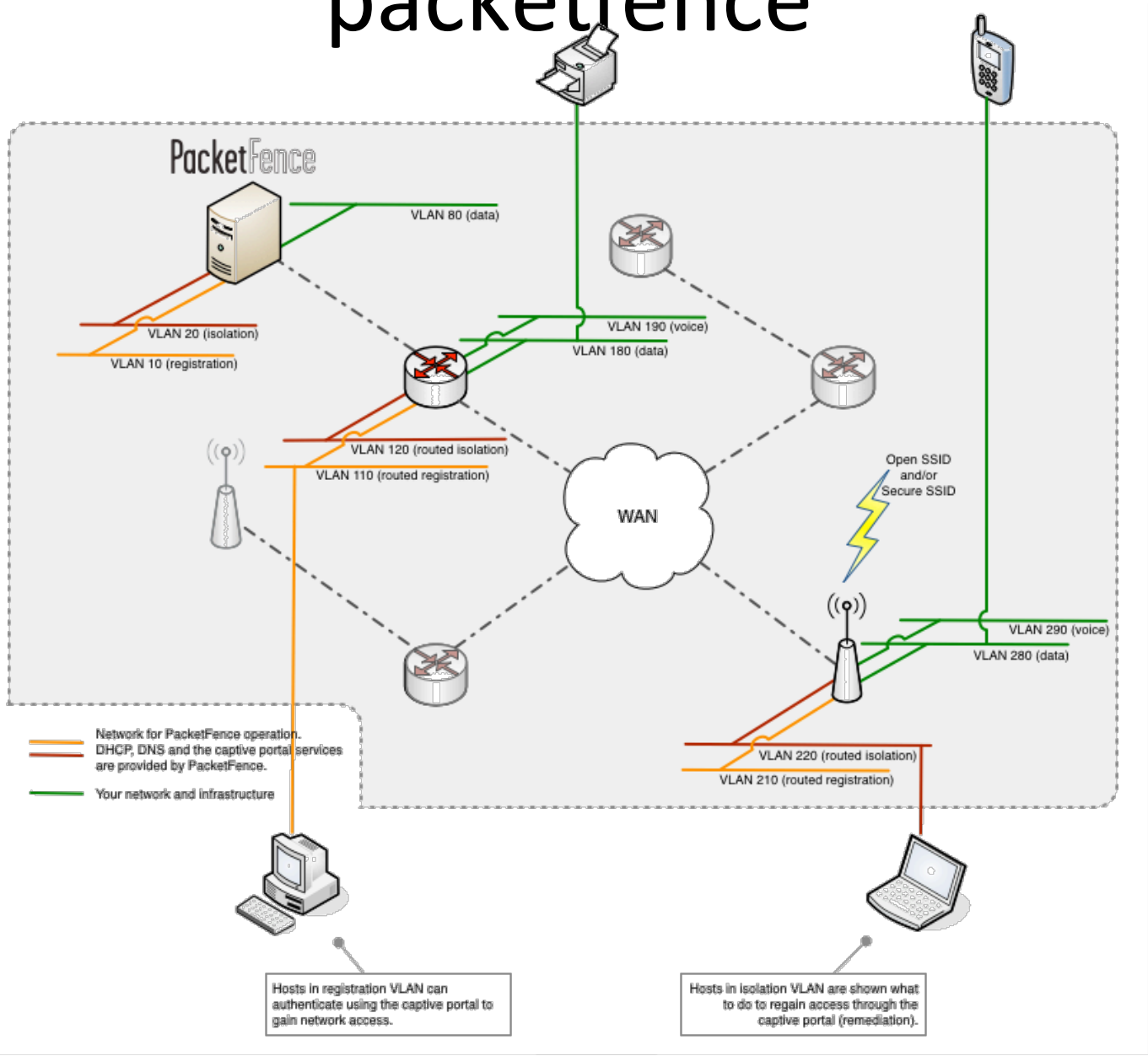
BAYU

- Be aware you are uploading:
- http://filesharing.uoregon.edu/bayu_notification.html
- On a single enterprise/campus network you may have the ability (think permission) to move users into a “disciplinary pen” if their machine misbehaves.
- ISPs should not do as much policing, but some is possible

Policies

- Submit to a “scan” on connection (using nessus or OpenVAS (Open Vulnerability Assessment System).
- Scan your own machines regularly.
- Run an IDS (talk about that tomorrow)
- What do you do with the results of that data. How do you scan?

packetfence



Principles

- Do not scan inline – you end up adding a point of failure as well as a bottleneck. You do need a “mirror” or “monitor” port
- Need supported hardware with SNMP (Ubiquity support still in progress)
- In ISPs you can trigger custom perl scripts based on particular “events” from network scanners.

Principles

- In enterprises you can drop the users access port in a VLAN with restricted filters.
- For scalability you could have more boxes in different parts of the network.
- FreeNAC is an alternative piece of software (also opensource)

Data gathering:

- IDS systems
- Active scanners
- Netflow

packetfence