High Speed Firewalls, VPN, IDS

Bryan Thompson

QUT Security Implementations

Firewalls

VPN

IDP (Proposed)

QUT Network Security Implementations

- Firewalls are being used to protect
  - PABX Infrastructure (IP Phones, Call Accounting)
  - Central Hosts (Web, E-mail etc.)
  - Management Network (Out of Band Network)

QUT Network Security Implementations

- Future IDP will be used to protect
  - Dial-in, VPN, Wireless, Laptop Access (Initially)
  - ISP Links – Max. 10Gig (Future)

QUT Network Security Implementations

- VPN solutions used to provide secure connection for
  - QUT Network (From ISP to QUT)
  - Wireless Network
  - Management Network (From Production Network)

High Speed Firewalls

Why the need for a High Speed Firewall?

- Originally for GrangeNet connection (1Gbps)
- Inter-campus 1Gbps links
- Future AARNet3 high speed links

High Speed Firewall Implementations

- High Speed Firewall (QUT Corporate Systems)
  - Current Status
    - Layer 3 Mode
    - Multiple gigabit connected hosts connected (incl. Web Servers, Backup storage nodes)
    - Migrating QUT Corporate Hosts to firewall network
  - Possible Future Upgrades
    - Transparent Firewall mode
    - Virtual Firewalls

Issues faced with High Speed Firewall Implementation

- Either "Big Bang" or "Host by host" approach to migrating hosts behind firewall (200+ hosts)
- Method for managing firewall rules
- Not all hosts/services are compatible with the firewall environment

"Big Bang" Migration Approach

- "Big Bang"
  - Disadvantages
    - High risk (Large volume of different services on different hosts)
    - Rollback procedure would include all hosts
  - Advantages
    - No change to IP address required
    - No DNS changes needed
    - No Host changes

"Host by host" Migration Approach

"Host by host"

- Disadvantages
  - Change of Host IP address required
  - DNS propagation delays
- Advantages
  - Rollback would only be for hosts with a problem (Quick)
  - Problems would be isolated to single hosts (Low Risk)

Method for managing firewall rules

- Centralised High Speed Firewall (Protect a large number of hosts)
  - System needed for easily managing rules in firewall
  - Use of virtual firewalls for segregating host groups

Method for managing firewall rules

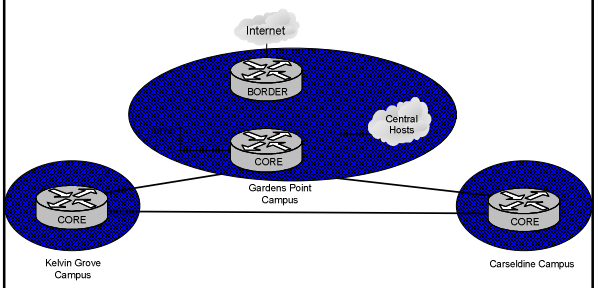
- Centralised High Speed Firewall (Protect a large number of hosts)
  - System needed for easily managing rules in firewall
  - Use of virtual firewalls for segregating host groups

QUT a university for the real world ® CRICOS No. 000213J

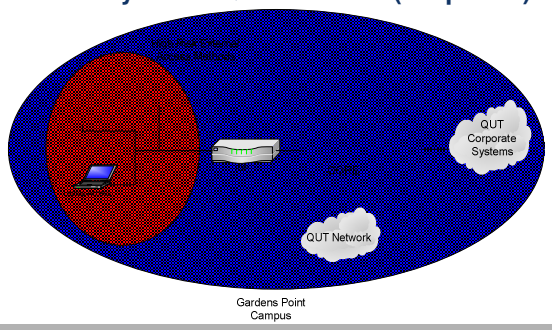
Not all hosts/services are compatible with the firewall environment

- Asynchronous routing
  - Hosts which currently have more than 1 network interfaces card
- Hosts running legacy applications (e.g. NFS over UDP)
  - May be blocked by inherent IDS features in firewall
- "Permit IP any any" != NO RULES!

Security in the QUT Network (Current)



Security in the QUT Network (Proposed)



Questions for the future???

- Will we be using IDPs vs Firewalls?
- Will we push more of the security protection back onto the user at the edge?
- Will the equipment we buy today be scalable for 10Gbps in the future?