EDGE

Segmentation & Security in a Tertiary Education Network

Presenter: Michael Harlow (Network Architect)

Co-Author: Ryan Minty (Senior Systems Administrator MS/Cloud)

Co-Author: Mark Zimmerli (ICT Security Manager)

EDGE – WHAT IS IT?

- The name of the most significant network and security project undertaken at the University of Tasmania:
  - A project that re-architected the University network
  - Introduced segmentation and security controls
  - Introduced significant security controls and concepts and features
  - Provided flexibility for University operations

THE RECOGNISED PROBLEMS

- Impact of de-centralised IT function
- Inconsistent processes
- Poor vulnerability management
- Vastly different approaches to risk acceptance
- Several security incidents
- Out of support equipment
- The rise of IoT
- Too much trust – Too much traffic mixing

CHANGE IN THE WINDS

- In 2010 the University began changing the way it thought about IT risk
  - Brought about by a change in senior management
- Restructured parts of the University structure to centralise key functions, and allow greater consistency in Policy and risk management
- Moved from ‘check box’ audits to penetration testing
  - Highlighted issues with machine configuration, consistency, and trust in the network
  - Changes needed
- Made funding available in 2014 to address issues highlighted by audits
- Elevated project profile, increased authority to implement changes

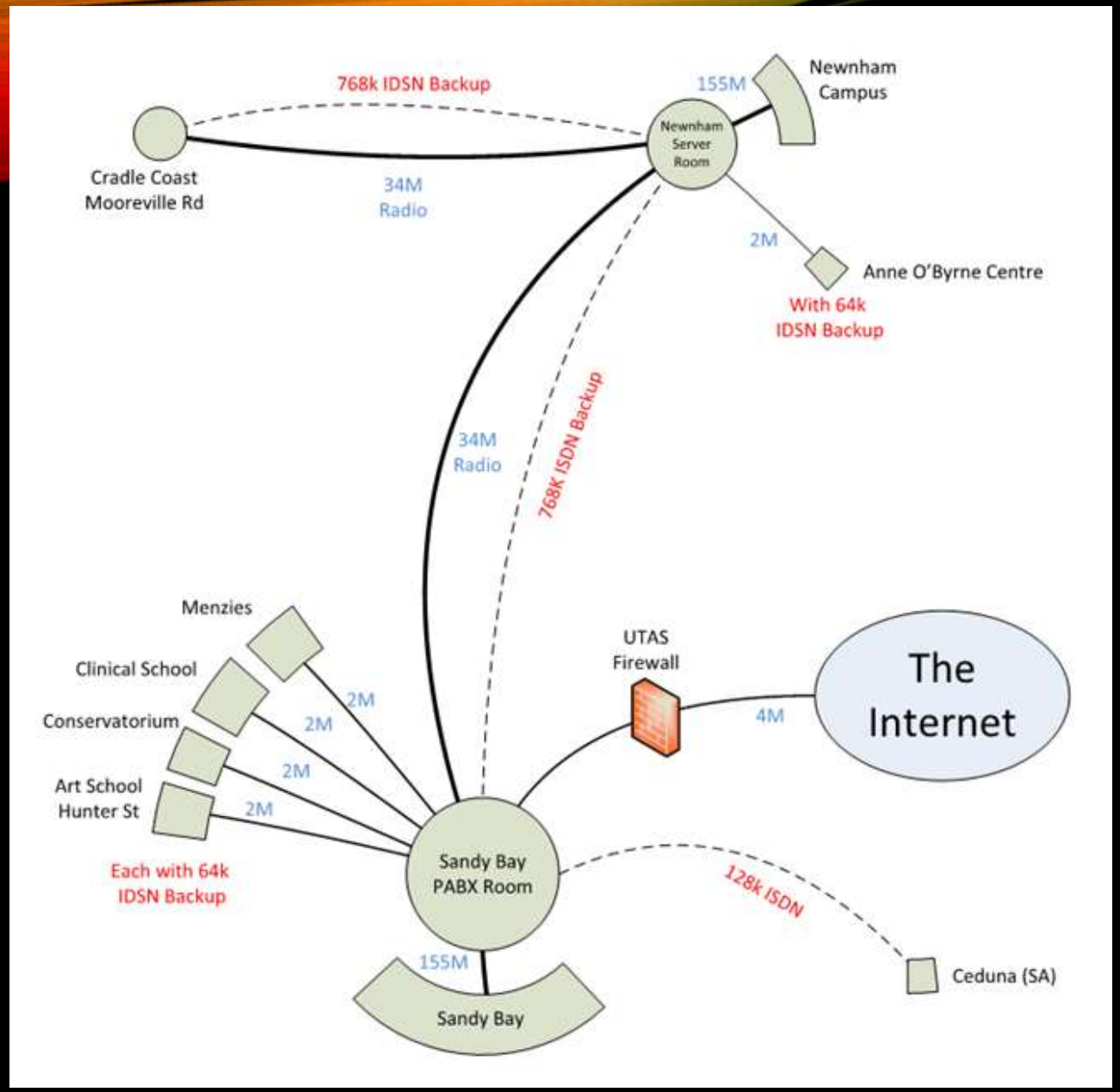
BUT FIRST…SOME UTAS BACKGROUND

- Only University operating in Tasmania
  - Results in broad curriculum/subjects
  - Collaboration with State and Federal agencies
- Operates three major campuses in Tasmania
- Two teaching (Nursing) sites in NSW
- Many medium, small and specialist sites
  - Short term accommodation
  - Remote research locations
  - Remote health sites/clinics
- Network presence in over 60 locations
  - Everyone wants a similar/transparent experience

IT INFRASTRUCTURE BACKGROUND

- Two major data centres greater Hobart area,
  - One local, one Co-Lo
  - 11/26km diverse 80G dark L2 interconnect
- 60 WAN links, Mostly dark fibre or managed.
- 600+ Ethernet switches (mostly 24/48 1RU in stacks rather than chassis)
- 2500+ servers (Majority ESX hosting MS and RHEL)
- 10,000 managed end points, 5000 IT controlled
- 25,000 active wireless devices
  - 8,000 simultaneous

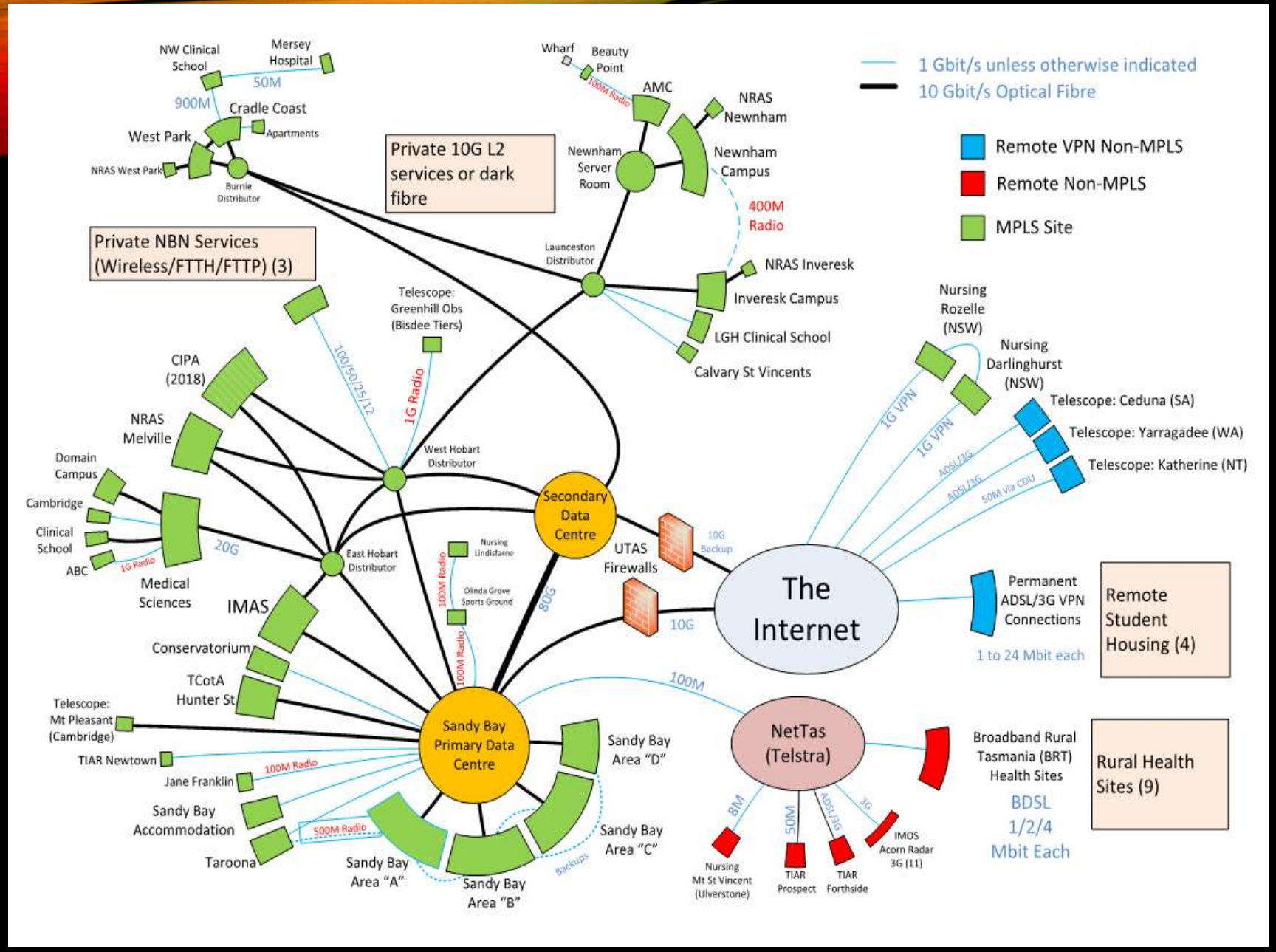
UTAS CIRCA 2001



- No Wireless
- No VPN
- No SLB
- No Australian Maritime College
- Mostly low-bandwidth radio
- Just 8 teaching locations
- 1 Interstate site
- 1 firewall – No DMZ

The simple times

2016

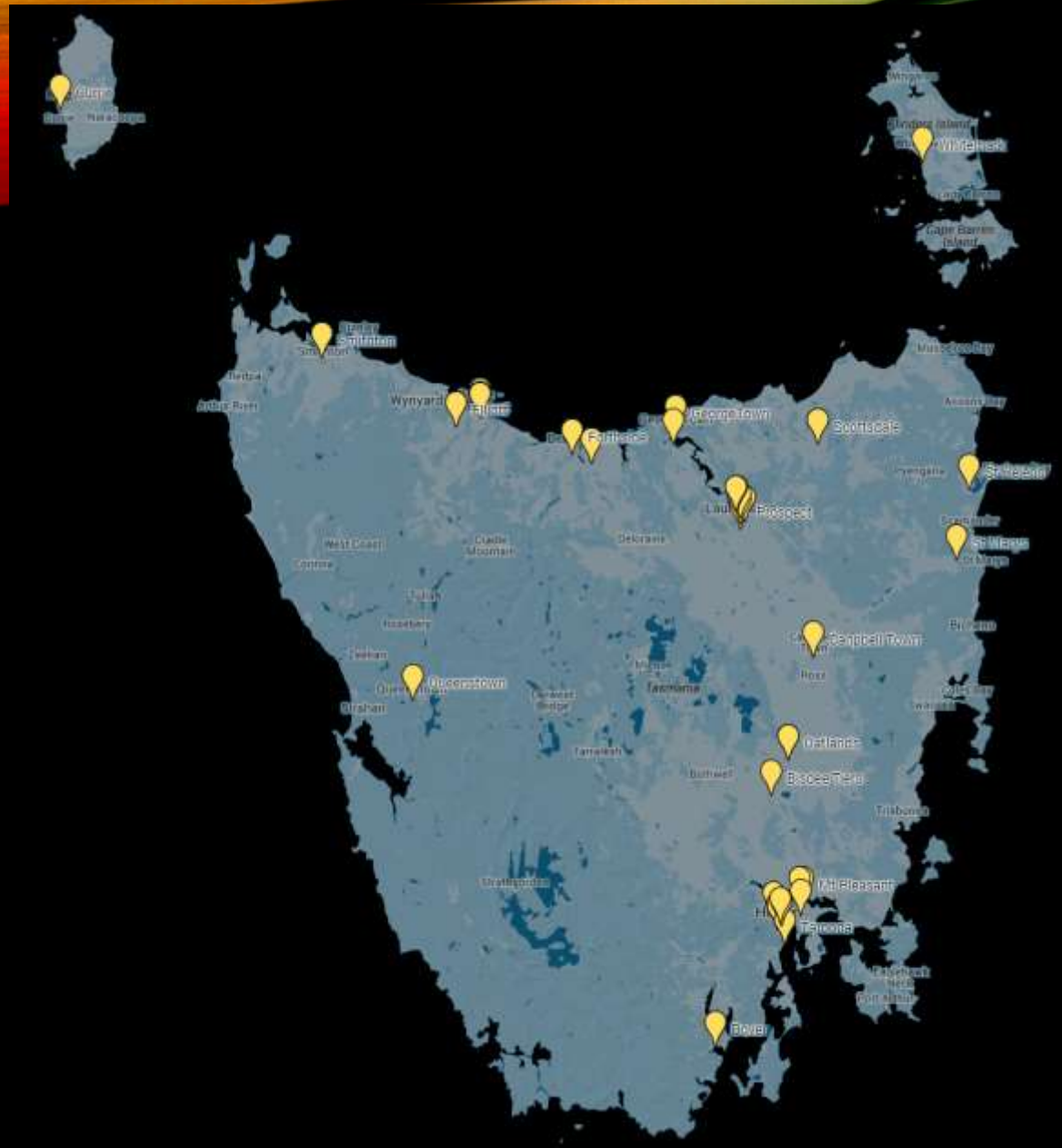


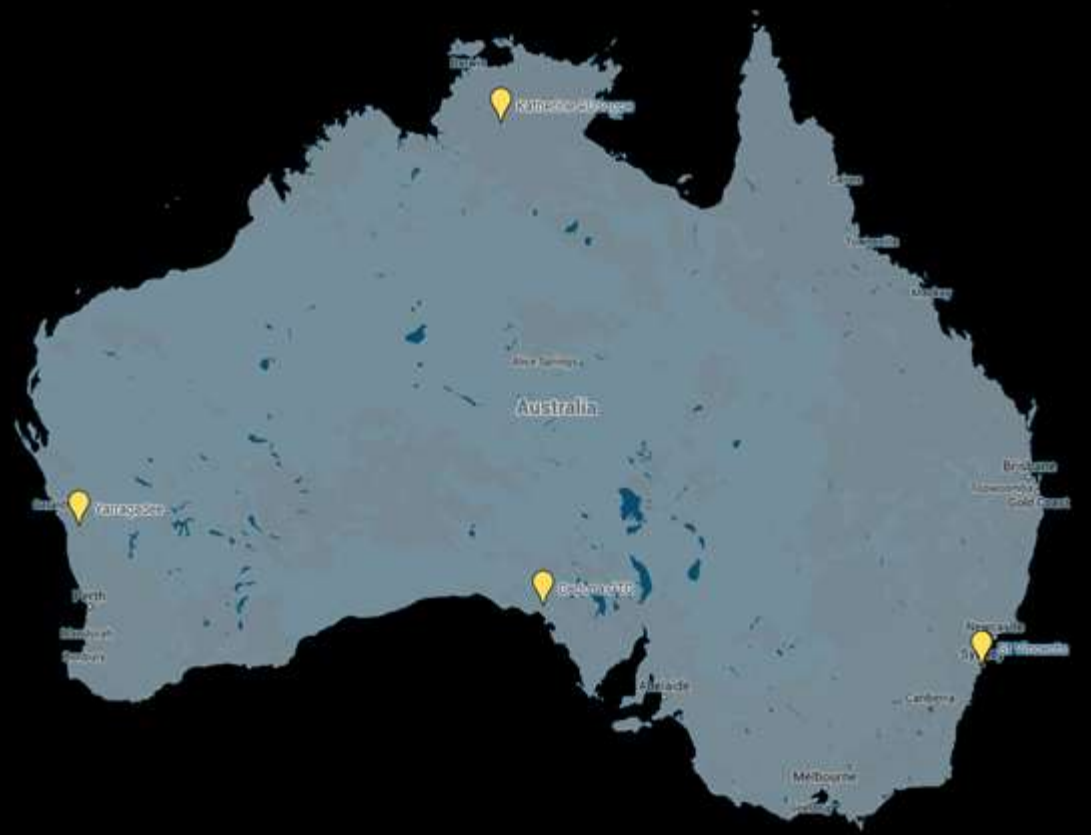
Things have changed

- Integration with AMC
- HPE MPLS network (2012)
- Large increase in sites
- Dual Internet connections
- Collaboration with Government agencies
- Radio Telescopes
- Wireless/VPN/Dorms
- Remote sites
- SLB/F5 ADC

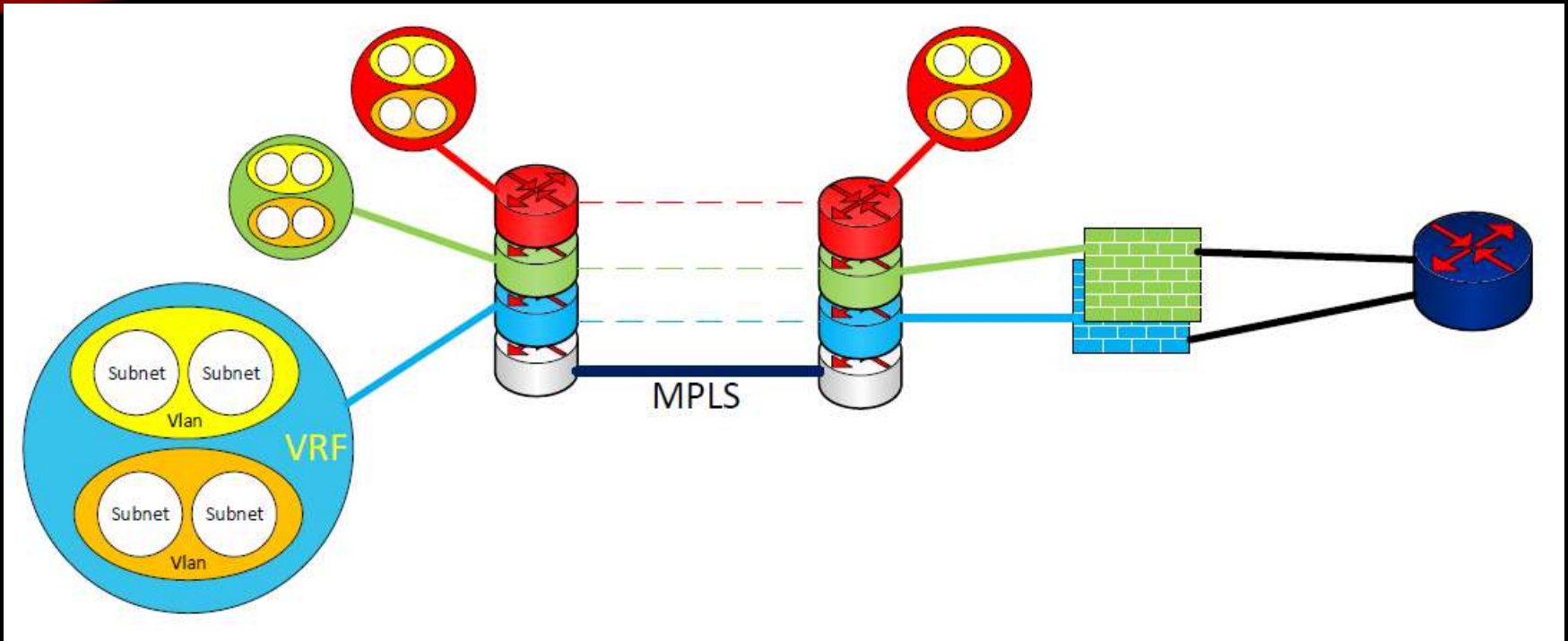
- BUSINESS & USER EXPECTATIONS

WHERE IS UTAS?





MPLS REFRESHER



- VRF – Virtual Routing and Forwarding - Group of vlans
- Totally isolated, or traffic via flow via shared router or firewalls
- MPLS allows sharing of links whilst maintaining separation

UTAS MPLS core

- Deployed 2012
- HPE A5800 1RU L3 switches – "Goldilocks"
- Mostly 1/10G fibre interconnects

PROJECT OBJECTIVES (1)

- Vulnerability management
- Procedural and change management improvements
- Centralisation of front line staff
- Reduction in distributed servers
- Standard desktop and server images
- Improved audit processes

McAfee STACK

Security Information & Event Management

Antivirus App Control

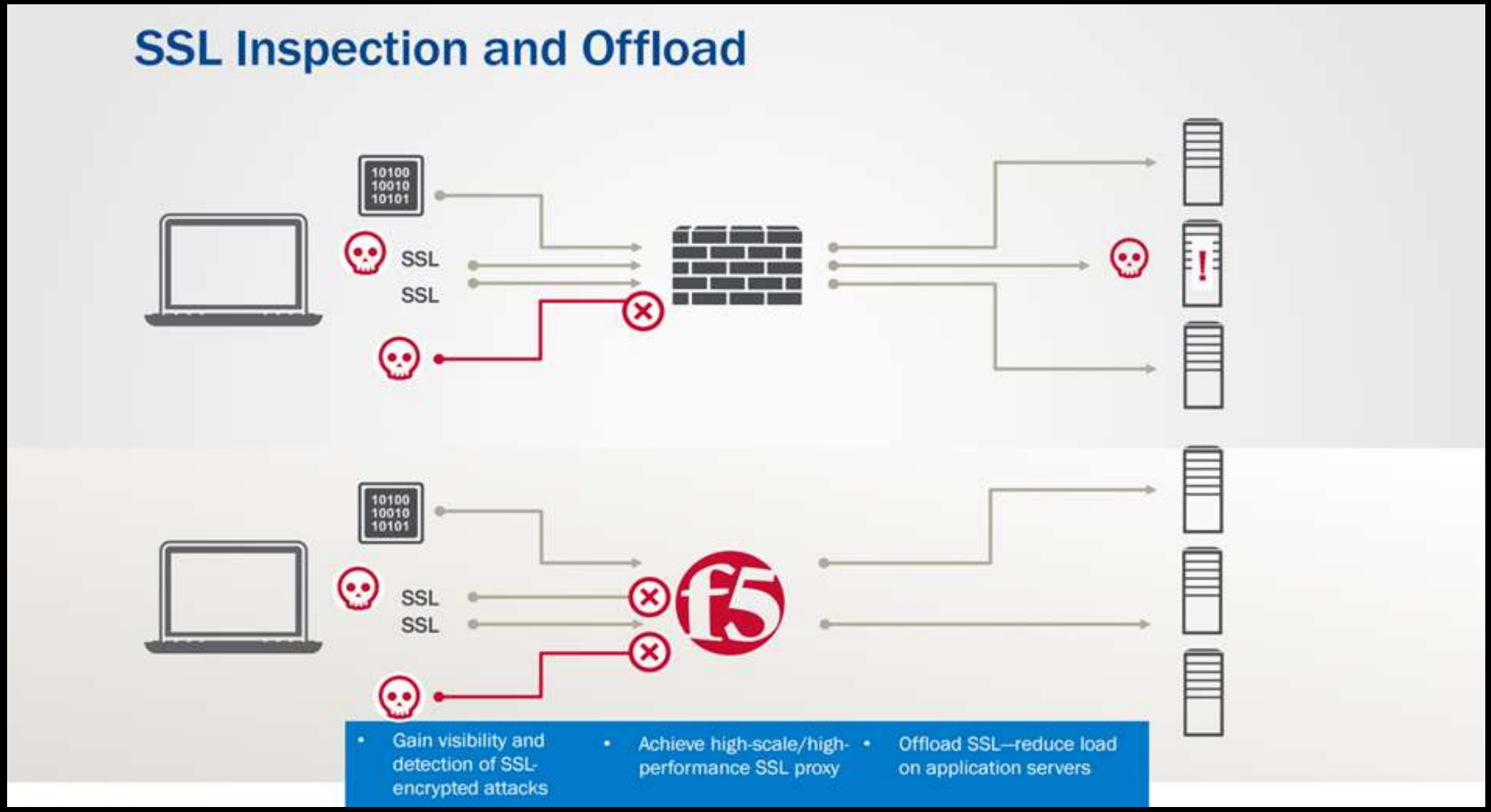
Disk Encryption

File Integrity Monitoring

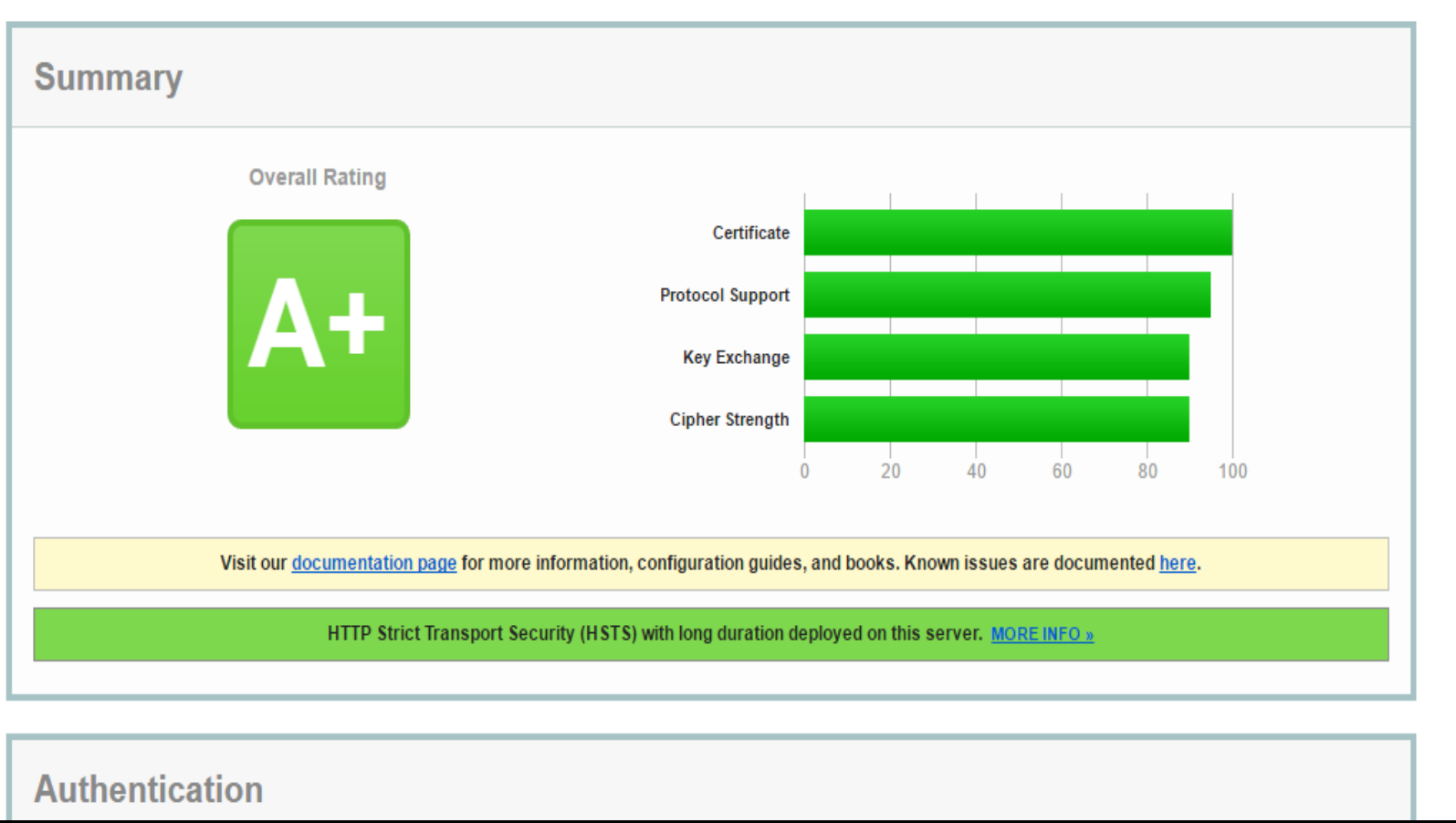
PROJECT OBJECTIVES (2)

- Consistent SSL presentation utilising F5 as a ADC
- Network segmentation, separation of user and servers
- 2-Factor Authentication (2FA) for elevated access
- Firewall replacement (EoL) + VPN (EoL)
- Internet router replacement (EoL)

SSL INSPECTION AND OFFLOAD

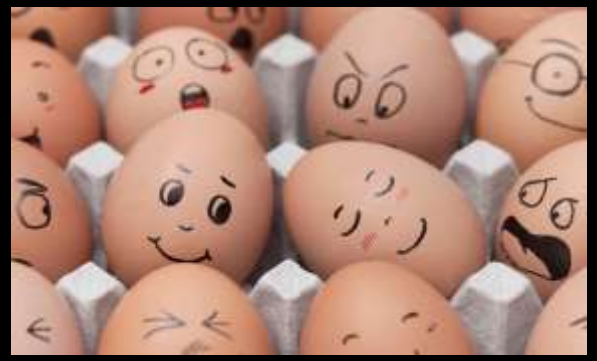


SSL MANAGEMENT



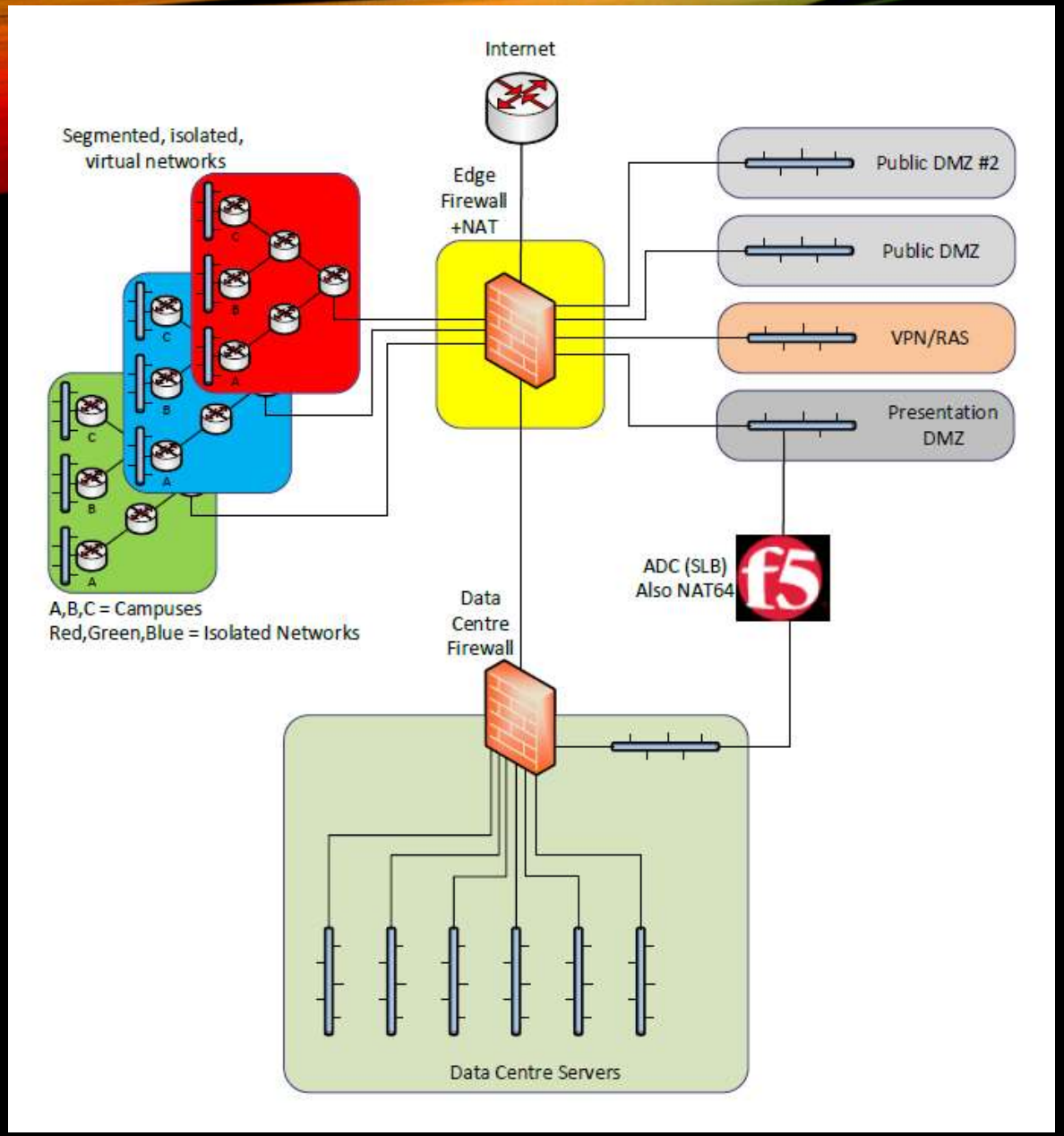
Time to respond to Heartbleed was ~2 weeks

After F5 reconfiguration time to respond to Freak/Logjam was 10 minutes



TIME TO DIVIDE

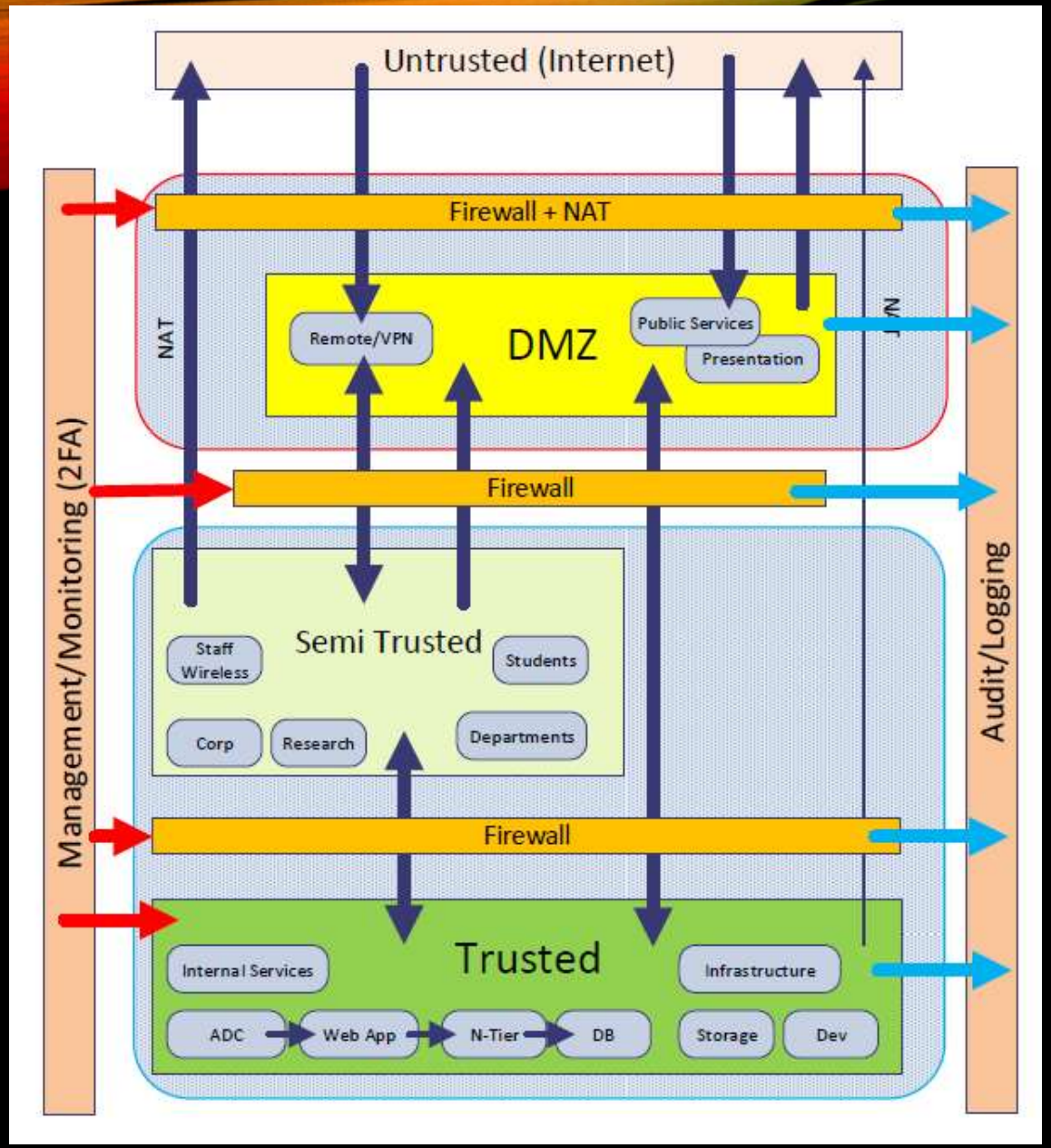
- Single organisation with single harden perimeter is no longer a suitable approach
- Adopt "Service Provider" mindset, not a single homogenous IT Department
- Diverse client base, with broad range of security requirements, risk profile and functional needs
- Segment and isolate to minimise risk, and reduce damage



SLICE'N'DICE

- Realisation that Users are untrusted and should be in the DMZ, not servers.
- In servers we trust, sort of.
- Increased segmentation inside DC.
- Grants visibility between application layers, multiple subnets/zones
- Traffic not controlled within subnet (yet). Future project (NSX?)

TRAFFIC CONTROL



- Discrete Management and Audit Zones, protected with 2FA
- Multiple “Semi-Trusted” user networks
- Trusted Data Centre Zone(s) including N-Tier traffic control

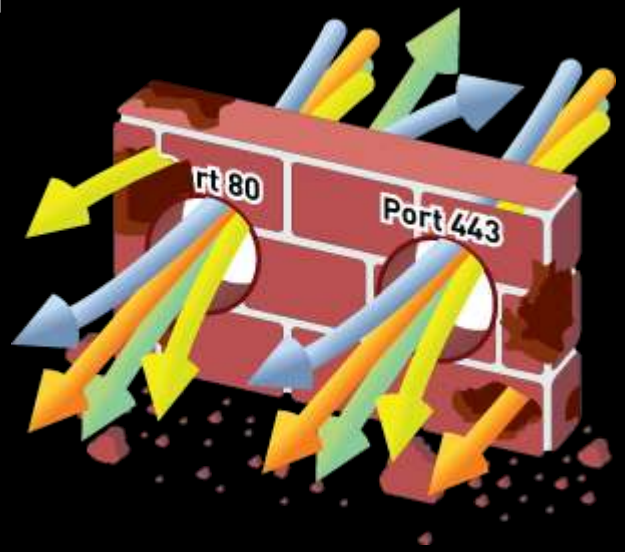
FIREWALL REPLACEMENT

- Functional requirements determined with professional services from external party
- Assisted in design of restructure of DMZ and Semi-Trust zones
- Vendor neutral tender for supply and implementation of new devices
- Internal PM resource assigned to assist with business interaction
- Successful tender by NTT was chosen
- Hardware was pairs of Palo Alto in HA split between DC
- PA-5050 pair for Internet connectivity PA-5060 pair for Data Centre control

NEXT GEN FIREWALLS

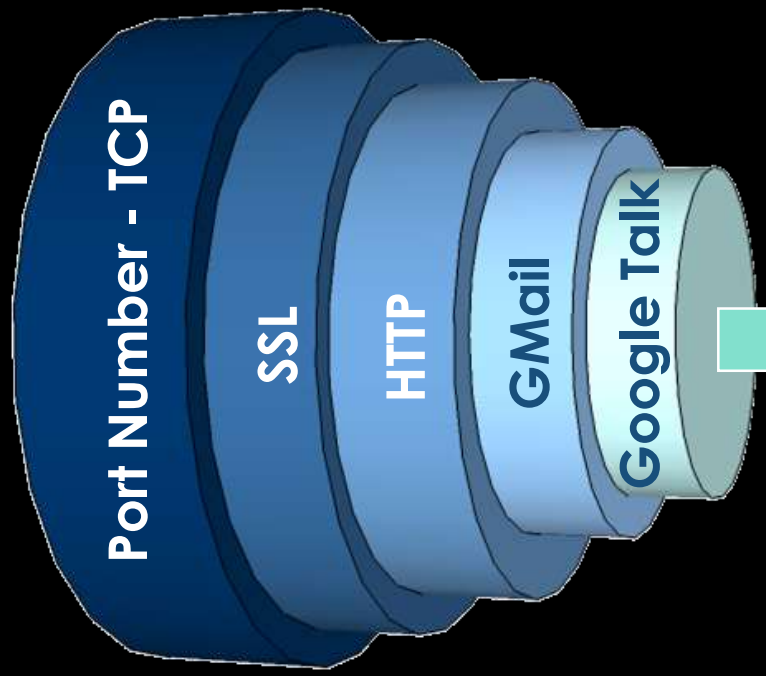
Need to move on from simple IP and Port rules

Ports ≠ Applications
IP Addresses ≠ Users
Packets ≠ Content



DETERMINE LEGITIMATE TRAFFIC

What is the traffic and is it allowed? (App-ID)	Allowed for this specific user or group? (User ID)	What risks or threats are in the traffic? (Content ID)



Inbound
Full cycle threat prevention

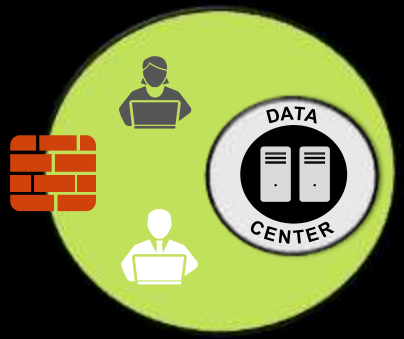
- Intrusion prevention
- Malware blocking
- Anti-virus control
- URL site blocking
- Encrypted and compressed files

Outbound
Data leakage control

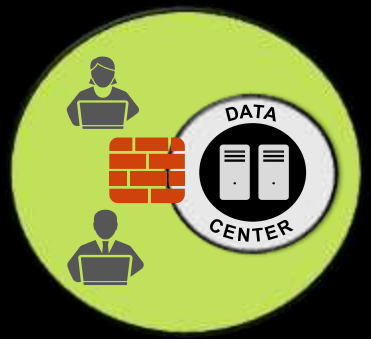
- Credit card numbers
- Custom data strings
- Document file types

DETECTING AND PREVENTING THREATS ACROSS THE UTAS NETWORK

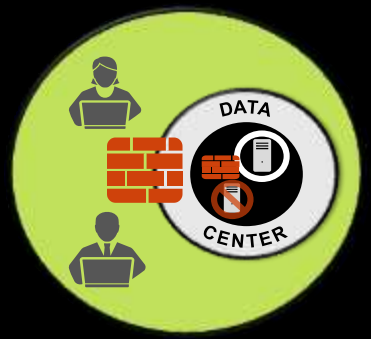
At the mobile device



At the internet edge



Between staff/students and devices within the LAN



At the data center edge, and between VM's

Within private, public and hybrid clouds

- 2 Factor Authentication is in deployment stage
- URL Policy is in final approval stage
- SSL Decryption awaiting signoff
- Rule migration still ongoing
- Always on VPN

Question Time