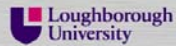


▶ Securing Information Systems and Widening Access: An Interesting Tautology

Matthew Cook
Senior IT Security Specialist
Security and Compliance Team



▶ Current Position

Security and Compliance Team

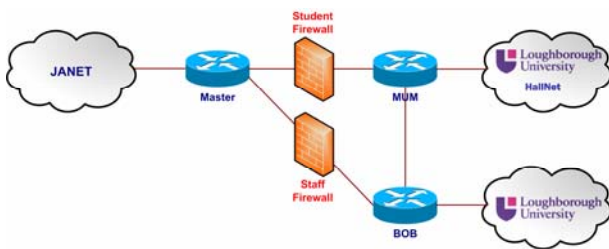
- ▶ Spoke about the firewall changes last year
- ▶ Improved campus security
 - ▶ Computers still compromised! :-)
- ▶ Migrating to dynamic rules, currently 1086
 - ▶ Investigation into chain grouping
- ▶ Servers protected on service VLANs
 - ▶ Firewall rules per net block
 - ▶ Router ACLs
 - ▶ Well configured servers (hopefully!)



2

▶ Topology

Security and Compliance Team



3

Developing a Strategy

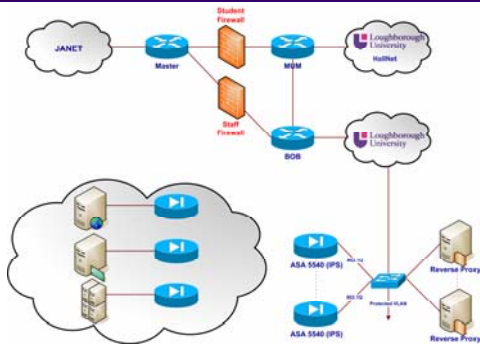
Security and Compliance Team

- ▶ Effectively create a DMZ
- ▶ Additional strict firewalling rules
 - ▶ On and off campus
- ▶ Concentrated inline IPS/IDS mitigation
- ▶ VPN termination
- ▶ Isolation of networks
- ▶ Replication on private netblocks/crossover cable
- ▶ Obfuscation of netblocks

7

Proposed Solution

Security and Compliance Team



8

Implementation

Security and Compliance Team

- ▶ Two Cisco ASA 5540
 - ▶ AIP SSM 20 IPS Module and 10 Context Licenses
- ▶ Virtual Contexts
 - ▶ Ten clusters of systems
 - ▶ Active/Active
- ▶ Outside 802.1q trunk with Internet IP Addresses
- ▶ Static NAT
- ▶ Inside 802.1q trunk to 10 VLANs
- ▶ Reverse proxy implementation as second stage

9

Problems and Issues

Security and Compliance Team

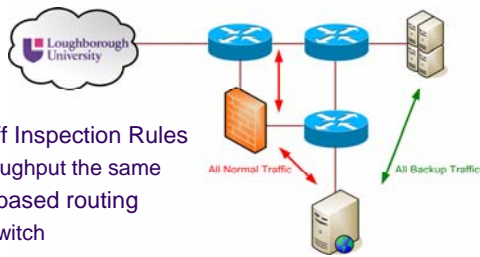
- ▶ No VPN termination at Layer2 (Bump in the Wire)
- ▶ Raw Throughput
 - ▶ Wirespeed 650Mb/sec
 - ▶ Inspection 450Mb/sec
 - ▶ Real life 420Mb/sec
- ▶ No A/V Content filtering, different SSM module
- ▶ Protected VLANs
 - ▶ VLAN hopping
 - ▶ Prefer physical interfaces (limitations)
- ▶ SSL Web VPN no longer free > v7.0 [7.2(2)14]

10

Backup Traffic

Security and Compliance Team

- ▶ Turn off Inspection Rules
 - ▶ Throughput the same
- ▶ Policy based routing
 - ▶ L3 switch
- ▶ Separate backup network
- ▶ Static route + network



11

Reverse Proxy

Security and Compliance Team

- ▶ Provide an additional layer of defence
 - ▶ Filter HTTP content, verbs etc
- ▶ Different solutions
 - ▶ Squid
 - ▶ Apache mod_security
 - ▶ Apache mod_backend
 - ▶ Apache mod_balance
 - ▶ Pound (<http://www.apsis.ch/pound/>)
- ▶ Acceleration of content, caching, gzip?

12

▶ **Futures**

Security and Compliance Team

- ▶ Replacement of main Campus firewalls [2007/08]
 - ▶ Bottleneck at 320Mb/sec
- ▶ Replacement of IDS [2008]
 - ▶ Problem with traditional hardware over 200Mb/sec
 - ▶ Optical/Wire taps
 - ▶ TCP offloading hardware
 - ▶ Snort acceleration cards
- ▶ Looking at the role of web caches/proxies
- ▶ Additional hardware in other datacenters

13



▶ **Questions:**

Matthew Cook
<http://escarpment.net/>

