AUSTRALIA'S INNOVATIVE UNIVERSITY

MACQUARIE UNIVERSITY ~ SYDNEY

# The Great Paradox Cost-effective Security in a Permissive and Distributed Environment



AUSTRALIA'S INNOVATIVE UNIVERSITY

MACQUARIE UNIVERSITY ~ SYDNEY

- **The Great Paradox - Cost-effective Security in a Permissive and Distributed Environment**
- **Abstract:**
- With 7000 staff and 30,000 students, Macquarie University (MQ) faces increased threats from unauthorised access, virus and worms, and malicious attacks against its assets & systems. Any attacks launched from within its network to external global organisations have an equally detrimental impact on Macquarie University and so must also be contained.
- MQ's potential security model is complicated by the need to provide generally "open and liberal" access to many resources within the University and on the Internet, while supporting highly variable requirements to secure information and systems within the University across various School IT Departments and central IT Services Department (ITS).
- The requirement to enhance security posture within a largely permissive environment while managing the cost pressure of a large, distributed networking environment creates a true paradox.
- A Layered Security Architecture within a Flexible Security Framework
  Through an extensive consultative and trial process MQ opted for layered security architecture. By collapsing MQ's L3 backbone into a "Security Control Core" the majority of MQ's internal traffic and all external traffic can be directed through a centralised, extremely high performance, and highly resilient security infrastructure incorporating firewalls, traffic management and QoS enforcement points, as well as providing advanced session monitoring, analysis, and remediation. The development of an MQ Security Framework as outline in Diagram 1 allows for simplicity and ease of management, combined with a very high performance backbone infrastructure. It provides ITS with the ability to apply rigorous security policy to a large proportion of all traffic within the MQ systems.
- While the framework provides MQ with the ability to minimise costs, extend security policy and enforcement far beyond the normal reach of ITS is attractive, nothing in the proposed solution prevents MQ from using any of the technologies in a more distributed fashion around the MQ campus networks. In fact, specific high-risk areas such as the University library are locations for additional surveillance and enforcement points

# Overview

AUSTRALIA'S INNOVATIVE UNIVERSITY

- The Challenge
  - Macquarie University
  - Security Issues
- The Process
  - RFP & Selection Process
- The Solution
  - What & Why



# The Challenge
# Macquarie University

AUSTRALIA'S INNOVATIVE UNIVERSITY

- 30,000 students with more than a third post graduates
- 7,000 staff in university and affiliates
- Single campus – 135 hectares
- 18km north of Sydney CBD
- Extensive switched fibre network

AUSTRALIA'S INNOVATIVE UNIVERSITY

# The Challenge
# Macquarie University

- Rapid Uptake of Wireless Access
  - 25% of students using wireless
  - 5,000 plus uncontrolled laptops - growing
- Free – uncapped Internet access
- Campus network open to Internet – real world addresses
- Decentralized IT structure – no SOE
- Many users oblivious to security risks



AUSTRALIA'S INNOVATIVE UNIVERSITY

# The Challenge
# Security Issues

- Ethical hack highlighted enormous risks
- Secure Data Centre still vulnerable
- Traffic volumes exploding
- Peer to Peer, edonkey bit-torrent etc
- Mass storage devices
- Key loggers, worms, viruses, trojans, password resets, botnets, physhing, .Spam, D.O.S. attacks

AUSTRALIA'S INNOVATIVE UNIVERSITY

# The Challenge Security Issues

MACQUARIE UNIVERSITY ~ SYDNEY

- Unwanted attention & poor reputation
  - P2P servers, Credit Card Fraud, D.O.S., port scans






AUSTRALIA'S INNOVATIVE UNIVERSITY

# The Process

MACQUARIE UNIVERSITY ~ SYDNEY

- Request for Proposal
  - Deliberately vague and non-prescriptive
  - Identified problem and requested solutions
- Longer RFP process with much consultation – discovery workshops
- Confused some vendors
- Evaluation Committee from across divisions

# The Process

- Mandatory Requirements
  - Scalable & flexible
  - Able to be implemented into existing topology
  - High Availability and fault tolerance
  - Able to support differentiated levels of access and capabilities based on the user profile (i.e. student vs. admin staff, vs. researcher)
  - Protection from internal threats as well as external threats



# The Solution

- Successful bidder was

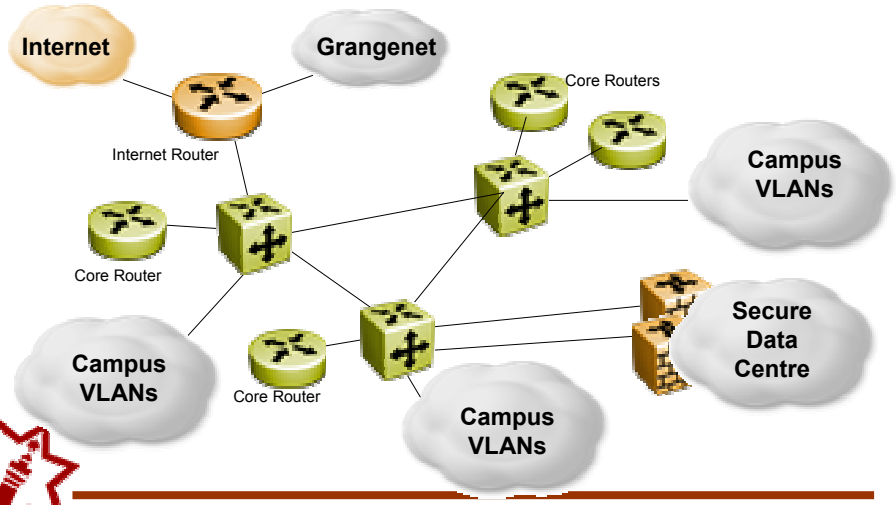
Nortel – 3D Networks consortium

# The Solution

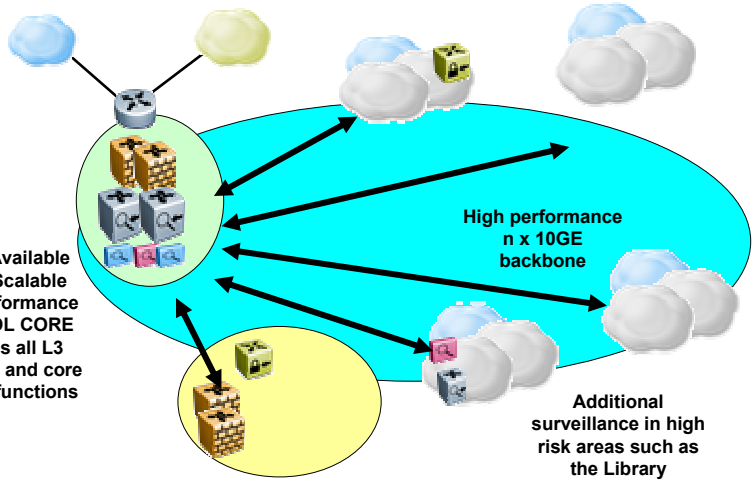
- 3D Networks & Nortel proposed an original and innovative architecture to address our issues
- The firewall cluster became the core of the network rather than a perimeter gateway
- The duplicated meshed design provides redundancy and high availability
- The consortium demonstrated a level of competence and understanding to successfully implement the solution



# Current Core Network



# New Architectural Model



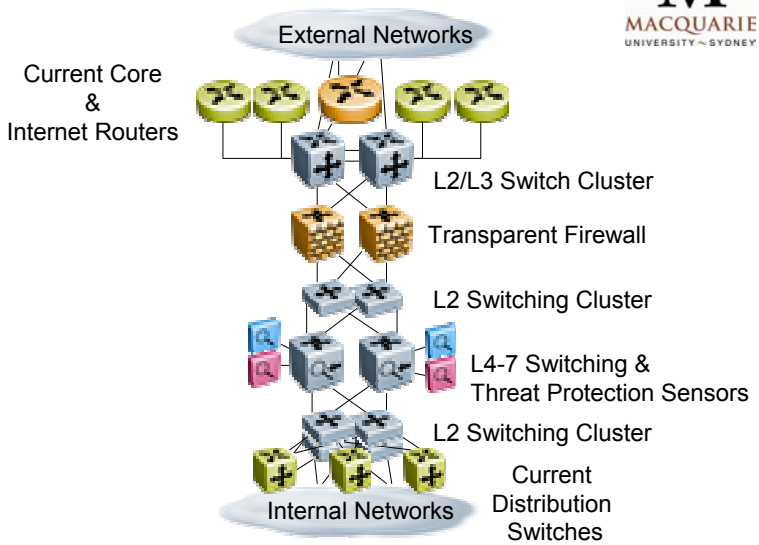



# The Products

- Nortel Switched Firewall
- Nortel Application Switch
- Nortel Threat Protection System
- Nortel VPN Router
- Switch Clustering
- Network Management

- Checkpoint
- Symantec First Attack Protection
- Enhanced Snort
- Integrated SSL-VPN
- SMLT - Multi-Link Trunking
- Nortel Enterprise Network Management System
- Checkpoint Smart Centre
- Nortel Defence Centre

# The Control Core






# The Solution

- Addresses MQ's great paradox
  - Cost effective security in an open and permissive environment.
  - Centralises control functions into a well defined "Control Core"
- Provides significantly reduced administrative and management overheads
  - "Flips" the traditional security management model.
- Meets and exceeds MQ's stated requirements.
  - Provides a platform for massively improved security, performance (n x 10GE) and scalability.

AUSTRALIA'S INNOVATIVE UNIVERSITY

MACQUARIE UNIVERSITY ~ SYDNEY

# Thankyou for your attention



AUSTRALIA'S INNOVATIVE UNIVERSITY

# The Solution in Greater Depth

MACQUARIE UNIVERSITY ~ SYDNEY

- The following slides explore the solution in greater depth.
- Further explanations would be best handled by contacting Nortel and 3D Networks directly at QuestNet stand.

3D Networks NORTEL

AUSTRALIA'S INNOVATIVE UNIVERSITY

# Nortel Switched Firewall

- Checkpoint security with high performance
  - Throughput up to 7 Gb/s
  - Session connections per second up to 100,000
  - Concurrent sessions up to 2,000,000
- Multi-layer packet inspection
- Switch-based acceleration
- Active-active configurations for 99.999% availability
- Integration with Threat Protection System

**Who's Done It**

- Finance
  - ComSec
- Governments
  - State Rail
- Automotive
  - Toyota
- Publishing
  - Fairfax
- Education
  - MQ
  - RMIT
  - Edith Cowan

Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.



AUSTRALIA'S INNOVATIVE UNIVERSITY

# Nortel Application Switch

## Intelligent Application Traffic Management

- Application layer inspection
- Application prioritization & traffic shaping
- Integrated Symantec First Attack Protection
- Flexible application flow manipulation
- Policy based QOS & rate-limiting
- Complete monitoring and reporting
- Scalable high performance hardware engine

**Who's Done It**

- Service Providers
  - Telstra
  - Optus
  - Vodafone
- Finance
  - Australian Stock Exchange
  - ComSec
- Insurance
  - GIO
  - AXA
- Education
  - RMIT

symantec.

AUSTRALIA'S INNOVATIVE UNIVERSITY

# Nortel Threat Protection System

- Intelligent Network and Application Threat Analysis
- Adaptive Defence System
- Threat Lifecycle Management
- Comprehensive Threat Reporting
- Centralised Management
- Based on enhanced Snort from Source Fire

**Who's Done It**

- Education
  - Coppin State University
- Utilities
  - Talisman Energy
- Tele Communications
  - Nortel

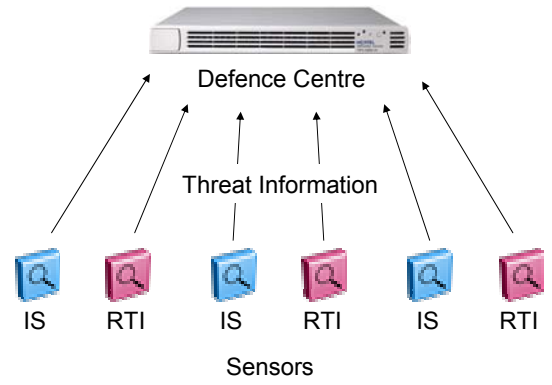
SOURCEfire Security for the real world.

SNORT.ORG

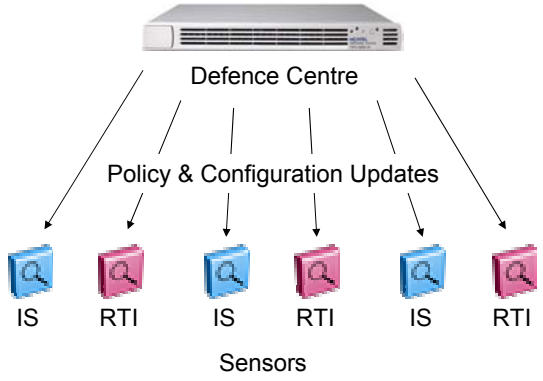


AUSTRALIA'S INNOVATIVE UNIVERSITY

# Scalable Distributed Solution



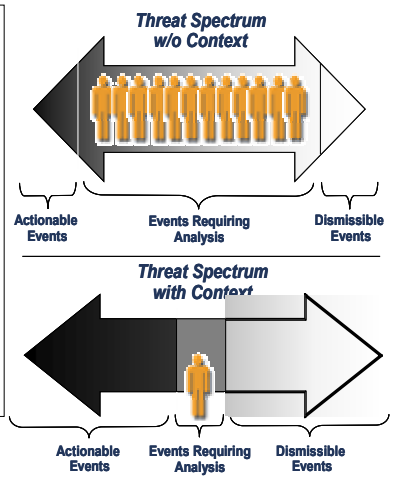
# Scalable Distributed Solution






# Real Time Threat Intelligence

- Reduces 'false positives' by providing behavioral context to intrusion detection
- Improved performance with 'target-aware' pre-processing of Threat Traffic
- Enables accurate automation and 'real-time' adaptive defense response



AUSTRALIA'S INNOVATIVE UNIVERSITY

# Universal Secure Access
## VPN Router with Integrated SSL-VPN

- Built for Security
- Flexible VPN Deployments
  - Multi-Platform Clients
  - Clientless Access
- Enables Secure Communities of Interest
- Role based access & QOS
- Full Firewall control within encrypted channels

**Who's Done It**

- Transport
  - Toll Holdings
- Education
  - Edith Cowan
- Finance
  - CommSec



AUSTRALIA'S INNOVATIVE UNIVERSITY

MACQUARIE UNIVERSITY ~ SYDNEY

*2000 IPSec Tunnels + 1000 SSL Tunnels*
*50-120 Mbps 3D NetworksES VPN*
*300 Mbps Firewall*

**IP Services Toolkit**

- VPN Services
- Routing Services
- Authentication
- Firewall Services
- QOS/ BWM
- Client Policy
- Audit/Accounting

# Nortel Switch Clustering

- Increased Scalability & Reliability
- Simplified network engineering
- Removes dependency on Spanning Tree Protocol
- Reduce link fail-over from 30s to 50ms
- Enabled 99.999% network availability

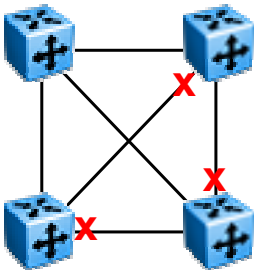
**Who's Done It**

- Finance
  - ASX
  - CommSec
  - St George
  - Westpac
- Education
  - Edith Cowan
  - RMIT
- Service Provider
  - Optus



# Traditional Meshed Network

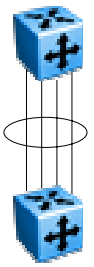
- Increased fault tolerance
- STP stops Ethernet loops



AUSTRALIA'S INNOVATIVE UNIVERSITY

# Multilink trunking / Ether Channel / 802.3ad

- Increase Bandwidth
- Link Fault Tolerance



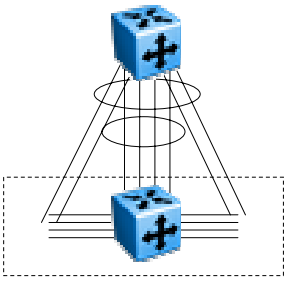


AUSTRALIA'S INNOVATIVE UNIVERSITY

# Switch Clustering

MACQUARIE UNIVERSITY ~ SYDNEY

- Increased Bandwidth
- Link Fault Tolerance
- Chassis Fault Tolerance
- Full mesh without loops



Switch Cluster

# Network Management

AUSTRALIA'S INNOVATIVE UNIVERSITY

- Network & Fault management
  - Nortel Enterprise Network Management System
  - Policy performance reporting
- Security Enforcement
  - Checkpoint Smart Centre
- Threat Analysis
  - Nortel Defence Centre



# Nortel Enterprise Network Management System

AUSTRALIA'S INNOVATIVE UNIVERSITY

- Know when new devices are added to the network
- Visualise network topology
- Fault aggregation
- Real-time network performance analysis
- Inventory Management

# Checkpoint Smart Centre

AUSTRALIA'S INNOVATIVE UNIVERSITY

- Single, unified console for campus wide policy management
- Ensures consistent policy enforcement
- Maximizes operational efficiency
- Currently deployed in MQ Secure Data Centre

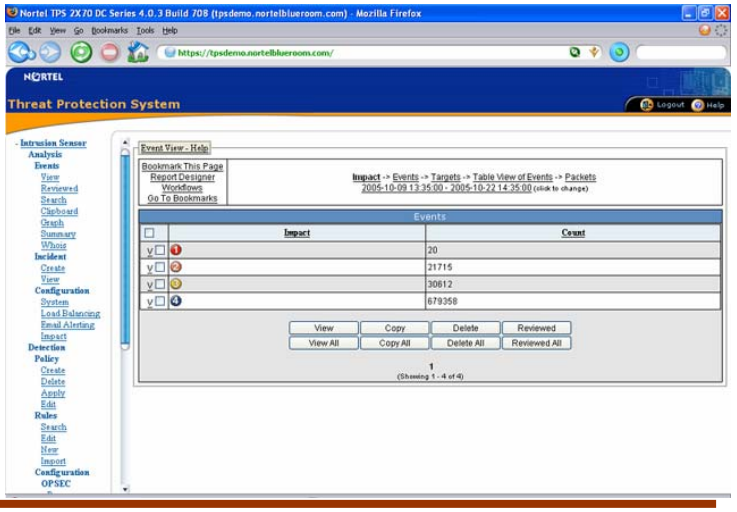


# Nortel Defence Centre

AUSTRALIA'S INNOVATIVE UNIVERSITY

- Sophisticated data analysis
- Event impact assessment & prioritization
- Policy management & configuration
- Manages response to critical threats

# Nortel Defence Centre






# Nortel Defence Centre