

Metropolitan Networks Case Study - University of Cambridge (Department of Physics)



Increased visibility brings increased security to University



UNIVERSITY OF CAMBRIDGE DEPARTMENT OF PHYSICS

Metropolitan Networks were able to bring visibility to the University of Cambridge's internet connection through the implementation of an effective traffic surveillance/ shaping tool from Netintact. This new found visibility offered protection from attacks, as well as making important publications available to the world for research.

"With Metropolitan Networks knowledge and assistance I have managed to condense what would have taken around eight hours a week into literally a 20 minute job."
Ian Mackey, IT Manager, University of Cambridge Cavendish Labs.

The Department is one of the top Physics departments in the world. There is over 600 staff, and around 3000 students on courses and academics. The Cavendish Laboratory has a 1 GB link to the University data network and the "outside world" and internally, multi-Gb trunked connections to adjacent institutes. With 58 * 48-port switches and 6 multi-frequency wireless access points the Laboratory needs automated security.

Issue:

As one of the worlds leading educational Physics laboratories, the University of Cambridge has research publications that are of interest to institutions and individuals all over the world. The different international research requirements necessitate massive bandwidth allowances at different times of the day, yet that information must be freely available 24 hours a day, seven days a week.

Not all interest in the University's data is from legitimate sources however. The University of Cambridge's status brings fame, and with that comes a certain amount of undesirable attention from individuals seeking to launch high profile attacks.

The challenge presented to the Physics department was how to monitor, assess and deal with un-authorized access attempts to potentially critical data, and at the same time allow freedom of access from around the world to research publications on an uninterrupted basis. All this without causing disruption to the 3000 students who use University bandwidth for educational and some recreational use.

Solution:

Metropolitan Networks recommended PacketLogic from Netintact as an effective solution to this problem. Its advanced traffic shaping tools enabled the University to allocate bandwidth discriminately for its mission critical applications. Powerful deep packet inspection capabilities offered the much needed surveillance to identify inbound and outgoing traffic in real time on a full Layer 7 analysis, collecting statistics and shaping or blocking as required.

Result:

The University of Cambridge were overjoyed with the result. Ian Mackey, IT Manager explains:

"Within one week we had identified and blocked no less than 220 intrusion attempts – some using normally acceptable ports. We had tangibly increased the speed of network access. We had isolated existing un-authorized software installations. We had saved an estimated 12k on human resources that would have been necessary to investigate these potential intrusions and development time monitoring and investigating Layer 4-7 access.

"By the end of the month I was able to present a breakdown of bandwidth use and abuse to the various management committees and demonstrate graphically how the network could be improved.

"We have since been able to utilize the PacketLogic with our IT intranet (primarily comprising of Extreme switches) to allow automated bandwidth allocations and QoS for specific research groups (averaging 380Tb data transfer) with no impact on other users.

"We have been able to maintain a high level of security even in high-bandwidth usage on normally innocuous traffic like port 80, 21, 23, 8080, etc and more especially secured or encrypted traffic on ports 443, 22, etc."

Summary:

It does what it says on the tin ... and more. Restricting what shouldn't be there, assisting what should, providing essential network management information and statistics of detailed packet-contents. *"With Metropolitan Networks knowledge and assistance I have managed to condense what would have taken around eight hours a week into literally a 20 minute job."*