CASE STUDY: Central School of Speech & Drama

ROYAL CENTRAL
SCHOOL OF SPEECH & DRAMA
UNIVERSITY OF LONDON

The Challenge

• Responding to an increase in student- and staff-owned mobile devices, CSSD required greater network resilience and cyber-security.

The Solution

• Network re-configuration to cope with high-density, high bandwidth, networking and data-hungry applications.
• A Palo Alto PA-500 Next-Generation firewall, handing the IT-team granular visibility in network security and performance.

The Results

• A simplified yet secure school wireless LAN, featuring prompt and effective threat prevention and granular network usage visibility.

Ensign Communications Ltd
20/21 Sandford Lane, Wareham
Dorset, UK, BH20 4DY

Tel: +44(0)1929 556 553

sales@ensign-net.co.uk
www.ensign-net.co.uk

LinkedIn   Google+   Twitter   Facebook

Ensign Delivers a Campus-Wide Network Overhaul and Next-Generation Firewall Solution to Prestigious London Performing Arts Facility

Founded in 1906, with a desire to advance the study of theatre as an academic discipline, *London's Central School of Speech and Drama (CSSD)* has evolved to become one of the most renowned and illustrious educational institutions in the country. Its alumni includes the likes of Lord Laurence Olivier and Dame Judi Dench, and the school has even received "Royal" status from Her Majesty the Queen in recognition of its world class facilities and contribution to the arts.

Ensign Communications were first approached by CSSD in 2009 after the school had been experiencing performance issues with their existing network. As is being observed by many educational facilities, the school's IT had witnessed a tremendous rise in the popularity and accessibility of mobile devices amongst students and staff members alike; a trend that can put conventional networks under a great deal of strain.

Acutely aware of the educational advantages to be had from offering high-performance wireless within an already rich teaching environment (not least as the often expansive acting 'spaces' do not lend themselves to Ethernet wired networking), the school required Ensign to re-configure the current wireless LAN in order to achieve higher levels of performance and resilience.

High-Density School Networking

Among many challenges for Ensign was the sheer number of devices; with around 500 students and 50-some staff members, all with at least one device (often more), the new network would have to be resilient enough to cope. High volumes of traffic, particularly during recreational periods, was not the sole concern; Ensign's network design would also need to be configured and optimised to deal with the high-bandwidth usage from video streaming and instant messaging that is characteristic of many school and educational Wi-Fi environments.

An important security consideration for CSSD was the requirement to segment the network into two, allowing distinctively different levels of access to staff, IT administrators and students. By splitting the roles and access rights in this way, the school would be able to isolate their business-critical data from that of their students and guests, and in doing so could mitigate the risk of cyber-attacks.

Security Focused

Once finalised, the school could boast a secure and professionally-structured enterprise network, which was not only highly resilient and secure but had the potential for increased performance, providing the building blocks for advanced network services and the expansion of the existing services offered to students.

In a dynamic wireless environment, such as CSSD, where the majority of end users are young and tech-savvy, keeping pace with their ever-changing needs and requirements, whilst maintaining a high performance and above all, secure, wireless network becomes a top priority.

Evolving Threat Landscapes

Visibility of enterprise networks has, in recent years, proven to be a core concern of many IT managers within academic establishments, as well as across many other sectors. The transformation of the threat landscape, as malware and hackers grow more sophisticated, has led to a demand for a new generation of network security solution that can safeguard against such onslaughts. As Gold Partners of Palo Alto Networks, market leaders in Next Generation threat prevention, Ensign could provide CSSD with the type of advanced solution that they required.

Jim Lucking, Technical Architect at Ensign, said: "Understanding CSSD's strict requirements for security and visibility was of great importance, especially due to the large amount of users the school has connecting to the network daily.

"With the ever changing way in which applications and users interact, and the evasiveness of modern malware, the market leading Palo Alto Next Generation Firewall was the obvious choice. The product provides the power, granularity and flexibility the School required to maintain the security and integrity of their network infrastructure and data resources, whilst being easy to manage with its intuitive interface."

The Solution

The Palo Alto Firewall is built upon three main pillars that make it the market leading Next Generation Firewall; Application-ID (App-ID), Content-ID, and User-ID.

- *App-ID is an innovative technology used to recognise, categorise and control traffic at the Application Layer, so rather than relying on ports and protocols - which can easily be bypassed by modern applications - the control of trusted and untrusted programs can be maintained to ensure that unknown traffic is not finding its way in (and crucially) out of the network.*
- *Content-ID technology enables the ability to recognise the nature of modern malware and provides the mechanisms to protect systems from the threats they can cause, however they are delivered, whilst working in conjunction with App-ID.*
- *User-ID is all about identifying the user as opposed to the IP address, linking into the existing database structures in Windows Active Directory, or by the use of client probing and guest portal authentication, to provide better visibility in dynamic client environments.*

Proof-of-Concept and Beyond

To showcase the capabilities of the Palo Alto firewall, Ensign ran a proof-of-concept with the school, a process which yields an in-depth AVR (Application, Visibility and Risk) report. The extensive report provided the schools' network managers with a detailed view of the types of traffic that were traversing their network, the applications being used and their relative security risk.

Opting for the PA-500 Next-Generation firewall, a unit capable of handling up to 64,000 simultaneous user sessions and up to 7,500 new sessions every second, CSSD now had the assurance that the Palo Alto could filter and control the school's thriving network traffic. Wayne Burgess, Systems and Network Administrator at the Central School of Speech and Drama, said of the Next-Generation Firewall solution:

"Since the installation of our Palo Alto firewall it has not only simplified but significantly improved our network security. We have a large number of student and staff personal devices which consist of Apple, Android, Windows and Blackberry, controlling what our students and staff can access is pivotal for both network performance and their on-going protection."

We have been amazed at the level of visibility it the Palo Alto allows; we can now take a granular look into how exactly our network is being used and by who, ensuring that threats are dealt with promptly and efficiently."