

LARGE UK SCHOOL DEPLOYS PALO ALTO NETWORKS TO ACCOMPLISH THE ULTIMATE IN APPLICATION CONTROL

“We’ve achieved full control over our bandwidth, the ability to filter out applications we deem unsafe, and a robust first line of defence against student cyberbullying.”

— David Croft, Network Manager, Greenford High School

BACKGROUND

Established in 1939 initially as a mixed grammar school, Greenford High School today is a vibrant and successful seat of learning for over 1700 pupils aged 11 to 19. Greenford also has both ‘Specialist Language College’ and ‘Leading Edge School’ official status, and regularly achieves a high standard of academic results for its students.

THE CHALLENGE OF ‘OVER-RESOURCEFUL’ STUDENTS

Like many successful UK schools, Greenford prides itself on a strong commitment to investing in ICT as a learning resource. Indeed, each Greenford student benefits from a multitude of opportunities to access networked resources and to surf the Internet. In total, over 2,000 users (students and staff alike) enjoy these privileges, though all within the constraints of a carefully stipulated Internet safety policy.

A combination of alarming national press reports and anecdotal insights led Greenford to question whether their enforcement of these policies, which govern the ability of each user to access safe URLs and appropriate web-based applications/content, were as watertight as required. Particular concern was raised over the capacity of individual users to access web-based applications capable of ‘bypassing’ firewall controls, particularly via the use of proxy programs such as Ultrasurf. The issue compounded with the revelation that Greenford’s configuration of wireless users meant they do not need to be authenticated against Windows Active Directory (and thus be governed by Greenford’s own proxy controls) in order to reach the Internet.

“Essentially we had no control over wireless users and Active Directory users who would use their own proxy applications to bypass our controls,” said David Croft, Greenford High School Network Manager. “Controlling what users can access is essential. We cannot compromise on anything less than total responsibility when students – many of whom are under the age of 18 – are accessing materials through our networks.”



ORGANIZATION:

Greenford High School

INDUSTRY:

Education

CHALLENGE:

Mitigation of proxy programmes bypassing URL control mechanisms; controlling what students can access via the Internet for their own safety.

SOLUTION:

Implementation of a Palo Alto Networks PA Series next generation firewall, alongside an existing ISA server deployment, to enforce full application control over fixed and wireless users through seamless integration with Active Directory.

RESULTS:

- Higher productivity for students and staff.
- Reduced risk from threats.
- Maximum confidence in URL enforcement and application control policies.
- Flexibility to apply granular rule-sets to user groups and individuals.
- First line of defence against potential cyberbullying.

UNIQUE FIREWALL FUNCTIONALITY WITH UNPRECEDENTED APPLICATION CONTROL

Greenford was approached by Computrad Europe Ltd., a network integrator, who suggested an evaluation of Palo Alto Networks PA Series next-generation firewall technology. “We’d trialed several Open Source/Linux solutions; none of them were very intuitive or user-friendly,” added Croft. “Running the Palo Alto Networks device for just a week in TAP mode was extremely enlightening, and for the first time we could see how many users were bypassing our controls.”

Greenford employs a Microsoft ISA server as its Internet gateway and network firewall, so the next stage of evaluation was to drop the Palo Alto Networks firewall alongside it (in between the ISA server and Greenford’s core switch) in transparent mode. “After seeing the results and experiencing its ease-of-use, we decided to go for full deployment.”

OBJECTIVES REACHED PLUS EXTRA BENEFITS

According to Croft, the PA Series has met all of Greenford’s expectations and provided a platform for additional benefits. “The control we now have over blocking applications is critical to protecting students from inappropriate material, and important for the school’s reputation,” he added. “Users hate it, but I think that’s good news because it shows how effective we now are. We’ve achieved full control over our bandwidth, the ability to filter out applications we deem unsafe, and a robust first line of defence against student cyberbullying. The flexibility of creating granular controls and policies against different AD groups is an extremely powerful benefit.”

The enhanced granularity of application control and policy enforcement is now enabling Greenford to be both measured and dynamic in its response to new users, emerging applications and changing work/study practices. In any event, the intuitive usability of the PA Series allows Croft to easily manipulate the access criteria of individual applications on a user-by-user basis, via just a few mouse-clicks. Rather than the traditional firewall controls of ‘blocking or allowing’ applications, users or user groups can be designated with a breadth of distinct policy privileges such as – for example – disabling some aspects of application functionality or subjecting certain applications to high or low Quality of Service (QoS).

From an ROI/cost saving perspective, Croft is also pleased that he no longer needs to annually renew ISP-provided proxy services as he found the Palo Alto Networks appliance’s URL qualities to be far superior.

