

### *University of Westminster Puts Its Trust in Top Layer*

#### Summary

The University of Westminster is one of the most popular universities in the UK with over 20,000 students, 700 teaching staff and up to 1,000 visiting academics. Spread over four campuses, with a unique size and topology, the network is a real challenge to secure. With the help of Top Layer and its Three Dimensional Protection (3DP) technology, the University of Westminster has become one of the first organizations in the UK to fully embrace network Intrusion Prevention Systems (IPS).

#### Background

Until recently, to maintain the University's philosophy of encouraging academic freedom, any security measures had to facilitate rather than restrict this requirement and hence only basic firewall protection had been deployed to protect the network and its users. But a rising web presence and dependency made the University vulnerable, both as a target and a source, to an increasing number of HTTP worms, zero day exploits, Distributed Denial of Service (DDoS) attacks, and other sophisticated cyber threats. A drive to address compliance issues also contributed to the University's decision to consider an IPS solution, which would protect against illegal traffic and undesired access and, ultimately, secure the network from the perimeter to the core.

The University specifically required that the IPS would have to be highly accurate in identifying bad traffic, thus preventing false positive events from being created and legitimate traffic from being restricted, and have the best zero day protection to mitigate any new threat. This improved protection was not to be at the expense of network availability and performance, which, in the University's, current 24/7 network environment needed to be guaranteed.

#### The Solution

Top Layer's IPS 5500-500 was chosen because of its low latency, ASIC architecture and its high performance with the ability to comfortably cope with the network's volume of traffic at high speeds. By using Top Layer's unique 3DP technology, it would ensure that the University network would be protected from content-



based attacks, such as virulent worm propagation (to which it had been susceptible), as well as DDoS and other rate-based attacks, and undesired internal or external access - all without compromising freedom of access and network performance.

The design plan was modularized to place an IPS 5500-500 unit inside the University network to protect the existing firewall and identify and block the spread of worm-infected hosts and any 'creative' students testing their skills by using university resources to attack hosts on the Internet.

The second part of the design was to place an IPS 5500-500 at the perimeter to protect the network and Internet presence from attacks from the outside, as the University had been witnessing a lot of DDoS attacks, which were taking its firewall offline frequently.

This design allowed for an overall connection setup rate of ~100K connections per second and two million concurrent flows, plus the ability to do integrated inspection on the three planes of 3DP - depth, context and time - on all traffic at 60K connections per second with flow table capacity of two million sessions.

## CASE STUDY - UNIVERSITY OF WESTMINSTER

---

Top Layer's 3DP technology identifies the 'contextual fingerprints' against the three dimensions of cyber threats – rate- and content-based attacks plus undesired access. This procedure enables the University to mitigate attacks by blocking all genuine threats and, with an unerring 100% accuracy in identifying malicious traffic; all false positive events were eliminated.

Based upon multi-dimensional analysis of traffic, as opposed to relying on matching binary signatures, 3DP's flexibility allows a focus on protecting against vulnerabilities in applications, which has given the University the very best protection against brand new and evolving threats, such as zero day attacks on the network.

"The Top Layer device was fast and easy to install without adversely impacting on the network, whilst company personnel were very accommodating, worked to our timelines and understood our concerns for a phased-in approach. Top Layer took good care of us on this project and helped out with all aspects, including onsite training and help with implementation and tuning," said Judie Ayoola, Network Security Officer at the University of Westminster.

"The automatic 'Top Response' security advisories service are also essential and comforting", Ayoola continued, "as we are protected from the latest security threats by a dedicated team researching vulnerabilities and pushing out policy updates that we have the option of implementing if we feel the threat affects our network."



### The Result

The deployment of the IPS 5500-500 instantly improved network traffic visibility and control, helping the University to achieve compliance with data protection guidelines. Crucially, Top Layer's 3DP technology has given the University of Westminster the confidence that its network is now protected from all forms of attack and cyber threats. It is highly accurate, and the University can be sure it has the solution in place to block and mitigate zero day attacks. In keeping with the University's goals, user access is guaranteed and network performance and availability have been maintained.

"We are very confident in the stability and accuracy of the Top Layer IPS 5500," said Judie Ayoola, Network Security Officer, University of Westminster. "The ability to be protected in the event of a new exploit spreading before the security community has time to address it was crucial."

### About Top Layer Security

Top Layer is dedicated to its role as the leading global provider of Network Intrusion Prevention Systems (IPS), developing and bringing to market network security infrastructure solutions that help commercial and government organizations protect their critical on-line assets from the losses and risks associated with cyber threats. Top Layer is headquartered in Massachusetts, USA with sales and services support worldwide.



**Top Layer Networks, Inc.** 2400 Computer Drive • Westboro, MA 01581 USA • +1.508.870.1300 • Fax +1.508.870.9797

[www.TopLayer.com](http://www.TopLayer.com)