

Building an Intelligent Monitoring Layer Using the Top Layer IDS Balancer Ensures Full Security Coverage for University of California, Irvine

Solution Overview

Profile: With more than 1,200 faculty members, 7,900 staff and 27,000 students, UCI is the fourth-largest campus of the University of California system. Orange County's second-largest employer, UCI also is an economic engine powering prosperity in the region, generating an annual economic impact that exceeds \$2.65 billion. UCI is consistently ranked among the top universities in US News and World Report's annual college review, and was recently named by eWeek as one of the top 10 universities for IT education. <http://www.uci.edu>.

Security Challenges: Maintaining proper "defense in depth" security architecture against the rising number of new, complex, and elusive network-based attacks is a significant responsibility for UCI's Network and Academic Computing Services (NACS) security group, Network Planning and Security. Trying to keep up with cleaning the University systems that have been hacked or compromised started to become a major issue, requiring additional personnel to deal with the security breaches. Spending more time dealing with security issues also meant spending less time building the computing environment that the 27,000 students, faculty and researchers needed. With the existing infrastructure, the University had no easy, cost-effective way to monitor traffic in and out of the campus for attacks, or to do forensics after a system had been compromised. Network Planning and Security's Computer Security Officer, Mike Iglesias, decided to upgrade the security infrastructure at the campus border to improve NACS' ability to monitor network traffic while having no impact on network performance.

Solution: After researching and reviewing products and solutions from various security and network infrastructure vendors, UCI decided to take the following steps:

- Build an Intelligent Monitoring Layer using the Top Layer IDS Balancer.
- Install a Network IDS system from Enterasys Networks.
- Install a traffic monitoring system running Argus.
- Replace their 7513 border router with a Cisco Catalyst 6509.
- Install a Cisco Pix firewall.



Benefits: As part of a comprehensive overhaul of UCI's network security, building an **intelligent monitoring layer** with the use of a Top Layer IDS Balancer (3500 and 4508 product families) benefited the University in several ways:

- First, by having a centralized place to conduct all traffic monitoring, the University ensured that malicious traffic could be easily identified and isolated. Inbound/outbound traffic gets mirrored from the 6509 to the Top Layer IDS Balancer.
- By utilizing balancing technology to aggregate, filter and distribute traffic for analysis across multiple IDSes and traffic monitoring systems, thousands of dollars are saved that would have to be spent on additional IDSes and traffic monitoring devices to monitor each traffic segment.
- The fact that the IDS Balancer has the capability to produce multiple copies of the same traffic, allowed UCI to monitor traffic using different monitoring devices, such as the Enterasys IDS for intrusion detection and the Argus system for traffic anomalies.

- Adding new types of monitoring devices, such as new types of IDSes or “sniffer” type devices for network troubleshooting, now became very easy.
- Finally, the ease of management of the new network architecture enabled by the IDS Balancer improved efficiency across the University’s resources — network operations staff could ensure full, accurate network coverage and focus on real threats while spending more time doing what they should be doing rather than cleaning up hacked systems.

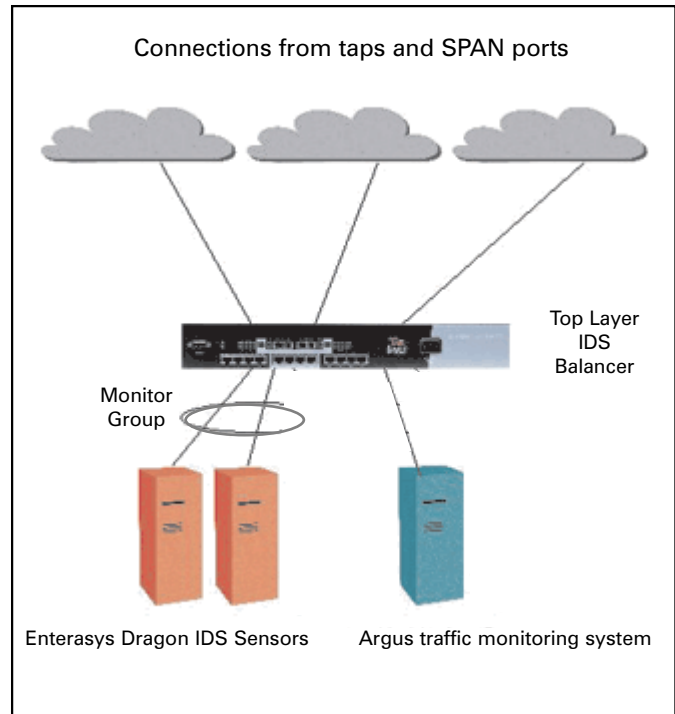
Full Case Study Details

Universities and businesses that have been around for many years generally build their network infrastructure on an ad-hoc basis — adding a component here, a connection and router there — as demand for bandwidth and services increases. They generally don’t have the time or budget to plan entire deployments in advance, or to do so with a holistic view of network security. This often poses the challenge of holes in network security that can prove very difficult to address.

At UCI, Michael Iglesias realized that the way the network had grown at the University gave him no single place to monitor network traffic for security problems, which potentially left the network open to an undetected attack.

Michael’s first thought was to install an IDS and a traffic monitoring system at each network segment. However, there were several fundamental issues with this approach:

- a) The cost of such a solution was very high since it required both an IDS and a traffic monitoring system for each segment, regardless of the volume of traffic in that segment.
- b) This solution was offering no redundancy. If one of the monitoring systems (IDS or traffic monitoring) failed, one of the network segments was becoming un-secure.
- c) Adding additional monitoring devices (such as network troubleshooting analyzers) was becoming an issue because of both the incremental high cost (one device per segment) as well as due to the fact that is not easy to tap a single segment multiple times. Using the SPAN/mirror ports of the switches in each segment was impossible since the switches usually have only one SPAN/mirror port.
- d) Management of this solution was becoming very complex due to the large number of devices that had to be managed.



Instead of installing multiple monitoring devices for each segment, Michael decided to build an **Intelligent Monitoring Layer** using the Top Layer IDS Balancer product family.

IDS Balancing Solution

The Top Layer IDS Balancer connects to the UCI network in a non-intrusive mode using taps and SPAN ports, **collecting and aggregating** data to be monitored from multiple Fast Ethernet and Gigabit Ethernet segments. **The ASIC-based Top Layer IDS Balancers, by using patented Flow Mirroring technology, filter and distribute the traffic in a load-balancing mode to the IDS sensors and the traffic monitoring systems.** The Top Layer IDS Balancers also offer **N+1 monitoring device redundancy**, so if one of the monitoring devices in a group fails; the Top Layer IDS Balancer detects that and automatically distributes the traffic to the remaining monitoring devices in that group.

By using the Top Layer IDS Balancer, UCI is able to monitor ALL network traffic in and out of the University. By using the Top Layer IDS Balancer, UCI saved thousands of dollars. Without the Top Layer IDS Balancer, UCI would have had to install many more IDS sensors and “traffic monitoring systems” to get coverage of all the network segments.

With the Intelligent Monitoring Layer in place, it became much easier to deal with device additions, moves or changes, as well as monitoring new segments or adding different IDS sensors or new monitoring devices (such as network analyzers). To accomplish this, all the University has to do in the new configuration is connect the new segment to an input port of the Top Layer IDS Balancer, connect the new monitoring device to an output port, and decide what data should go to the new monitoring port. Setting up, configuring and managing the Top Layer IDS Balancer is simple *via* the Web-based management interface.

“This is a great product! It is not very often that you come across a high-tech product that does exactly what it is supposed to do, and is very easy to use. I had it up and running the way I wanted within 30 minutes, pretty much without reading the documentation,” said Iglesias.

Cheaper, Simpler, Easy to Manage and Ready for Future Growth

The University immediately began realizing the benefits of the new configuration. Fewer systems have been compromised, and administrators are warned much earlier of potential attacks. Administrators are also able to review activity and do deep data forensics to determine “who did what to whom, and when.”

“Computing support staff all over campus can now spend more time doing the things they are supposed to be doing instead of cleaning up hacked systems,” said Iglesias. Iglesias is also considering adding additional IDS Balancers such as the IDSB 3500 and the IDSB

“ This is a great product!does exactly what it is supposed to do, and is very easy to use. I had it up and running the way I wanted within 30 minutes. Computing support staff can now spend more time doing the things they are supposed to be doing instead of cleaning up hacked systems.”

— Mike Iglesias, Manager

UCI Network and Academic Computing Services Team

4508, so that he can extend this successful network model to the dormitory networks and other network segments in the near future, thus affording them the same level of protection.

The Top Layer IDS Balancer improved security and manageability by giving UCI the ability to monitor **all** of their network traffic – something that would be dramatically more expensive if IDS had to be deployed on each segment.

About Top Layer

Founded in 1997, Top Layer Networks develops network security solutions that enable enterprises worldwide to protect their infrastructures and critical online resources from cyber threats. The Company's patented, ASIC-based security products are engineered to deliver accurate and reliable protection mechanisms while operating as robust in-line network devices. Top Layer Networks is headquartered in Westboro, MA, USA, with sales and support presence in France, Germany, Japan, Korea, and the United Kingdom.



perfecting the art of network security

Top Layer Networks, Inc. 2400 Computer Drive • Westboro, MA 01581 USA • 508.870.1300 • Fax 508.870.9797

www.TopLayer.com

09-03 © 2003. Top Layer Networks, Inc. All Rights Reserved. AppBalancing, AppSafe, Attack Mitigator, DCFD, Flow Mirror, IDS Balancer, perfecting the art of network security, Secure Balance, Top Layer, and Top Layer Networks are trademarks of Top Layer. AppSwitch, TopFire, TopFlow, TopPath, and TopView are registered trademarks of Top Layer. Unless otherwise indicated, Top Layer trademarks are registered in the United States and may or may not be registered in other countries. All other company and product names may be trademarks of the respective companies with which they are associated. Top Layer trademarks are registered in the U.S. Patent and Trademark Office.