

Southern California University Turns Back Denial of Service Attacks with TippingPoint™ Intrusion Prevention Systems

CASE STUDY



The Challenge

Deploying its first network in 1999 brought University of Redlands (www.redlands.edu) a lot more than connectivity to support its 5,000 faculty, students and staff. It also triggered the onset of crippling Denial of Service (DoS) attacks that compromised the Southern California liberal arts and sciences institution's academic research and communications.

Launched as far away as China and Poland, the DoS attacks were cloaked in email attachments that infected Redland's networked PCs. The menacing programs would then command the PCs to send a flood of traffic over the university's Internet portal, ultimately crashing Internet service at its main campus and seven satellite sites, plus its Web site. At these times, students were hard pressed to complete assignments and research. Staff struggled to conduct routine administrative tasks, and no one could send or receive e-mail. Even the university's environmental systems, e911 capability and important bank transactions were affected as IT personnel worked frantically to restore connectivity.

By the fall of 2004, as many as three DoS attacks a day penetrated Redlands' three Cisco firewalls protecting the school's local area and wide area network (LAN/WAN). Even the virtual LAN (VLAN) the IT department established to segregate infected PCs and protect healthy systems failed to neutralize the attacks. "We tried everything, from isolating switch-to-switch traffic, individual MAC addresses and infected PCs to using access control lists (ACLs)," said Matt Riley, associate IT director, University of Redlands. "Our IT staff was constantly trying to fix infected PCs, which compromised our overall technical support."

With its firewalls clearly unable to combat the DoS threats, the Redlands IT department

sought an alternative solution that would provide the comprehensive and pervasive protection it required, but with one important caveat. The security solution also had to interoperate seamlessly with the university's Cisco Gigabit network. "Being a smaller institution with fewer resources than larger universities, we needed a solution to stop the attacks affordably as well as effectively," Riley said.

Why TippingPoint

At first the IT department considered an intrusion detection system from Cisco. However, the product could only alert network administrators of an attack after it had violated the university's network. Ultimately, the IT department learned of the TippingPoint Intrusion Prevention System (IPS) from 3Com.

"The TippingPoint IPS has the capabilities and the track record we wanted at the affordable price point we needed," Riley said. "After surveying the field, we found it was the only product that could give us the proactive protection we required, but we still wanted to make sure," Riley said.

To test the system, the university deployed a single IPS in November 2005 between its two core routers and behind the firewalls guarding its 15 megabits per second (Mbps) DS3 Internet connection. "Installation was truly 'turnkey' right out of the box. The TippingPoint IPS interoperates beautifully

"Since we put in the TippingPoint IPS, we have not incurred even one successful DoS attack. The system provides us with complete in-line protection, something that no other product could do. Even if an attack starts internally, it may hit our switch, but the TippingPoint IPS will stop it."

*Matt Riley
Associate IT Director
University of Redlands*

with our pre-existing switches and routers, and the results were immediate and conclusive," Riley said. "We knew we made the right decision as soon as we plugged it in."

Today, the TippingPoint IPS proactively protects Redlands' networks, applications, and inbound and outbound traffic from malicious packets at line-rate Gigabit speeds. It blocks DoS attacks, spyware, worms, viruses, phishing and Trojans, while allowing legitimate traffic to pass uninhibited. It also protects all network components such as routers, switches and VoIP systems from targeted attacks and traffic anomalies.

Most importantly, the days of crippling attacks have ended for the University of Redlands. "Since we put in the TippingPoint IPS we have not incurred even one successful DoS attack," Riley said. "The system provides us with complete in-line protection, something that no other product could do. Even if an attack starts internally, it may hit our switch, but the TippingPoint IPS will stop it."

The IPS also prevents the school's non-critical applications from degrading performance and impeding the flow of important voice, data and video communications. Concurrently, the system's real-time Digital Vaccine® service ensures that the IPS is constantly updated to guard against the latest threats. The innovative service

automatically delivers new filters to Redlands' IPS's weekly or immediately in urgent situations, providing a powerful layer of safeguards for servers and desktops and fully inoculating them in virtually every case before an attack.

"The Digital Vaccine service helps us prevent emerging attacks by recognizing patterns and blocking malicious traffic," Riley said. "It offers the extra measure of protection we need to secure our network."

In addition, because the solution features parallel processing, traffic moves through the IPS with latency of less than 215 microseconds, regardless of the number of filters applied. Thus, a large number of simultaneous incidents will not impede traffic flow, enabling the campus community to continue working without interruption.

The Benefits

With the TippingPoint IPS guarding its network, University of Redlands today has the reliable communications its students, faculty, and administrators require. "Our Internet connection is now free from intrusions and always available for our users," Riley said. In addition, the university's VoIP solution, which it deployed at one residence hall location about the same time it began using the IPS, has not had one intrusion from a cyber attack, according to Riley.

The TippingPoint solution also is boosting the productivity of IT staff exponentially, enabling them to better support the campus community. "At the height of our outbreaks, we were too busy troubleshooting and fixing infected PCs to help students with applications and other issues. Now we're always there when they need us," Riley said.

IT staff also is able to devote more time developing applications that benefit the university, Riley said. The IT department, for example, recently installed virus protection with automatic updates on every university and student machine.

"The TippingPoint system has given us the freedom and time to re-evaluate traffic on a regular basis and give higher priority to high-use applications like VoIP," Riley says. "Most importantly, the TippingPoint system has allowed us to spend more of our valuable time helping the administration and serving the academic community."