

Top Layer Attack Mitigator™ Helps State IT Department Reduce Threat Exposure and Costs

Solution Overview

Profile: Government for an east-coast state. The IT department provides services to more than 70 percent of state employees using 30,000 IP addresses, 100 routers, a fractional T3 link, 100 Mbps LANs, and Gigabit Ethernet.

Challenge: Numerous vulnerabilities left network resources exposed. Attack traffic was consuming bandwidth, SYN floods every five minutes, ICMP floods several times a minute. One attack crippled 17 Windows NT servers, requiring rebuilds from scratch. Sluggish performance and increasing bandwidth led the state to contemplate capacity upgrades.

Solution: After the state did an extensive security evaluation, they installed Top Layer's Attack Mitigator to sit between their firewall and router. The Attack Mitigator was proven to stop the time consuming and costly attacks that had been haunting their network and allowed them to monitor the traffic patterns and uncover other abnormal anomalies that were hampering performance (i.e. redundant paths, unwanted IP addresses).

Benefits: The state profited from increased security, significantly improved performance of their firewall, and less time being spent to fend off attacks. The Attack Mitigator also postponed their firewall upgrade as well as purchases of new servers and additional T3 bandwidth. The agency was able to offer improved SLA performance and can now confidently serve a greater number of users.



It turns out that the old cliché is wrong: what you don't know can, indeed, hurt you. Attackers were targeting numerous vulnerabilities in the state's IT systems to interrupt service, surreptitiously consume bandwidth and

processing resources, and corrupt countless hardware and software systems requiring lengthy and expensive repair efforts.

Their solution: Attack Mitigator from Top Layer Networks. Shortly after deploying Attack Mitigator, the state was able to quickly identify and remedy various undetected attacks, improve performance, postpone network and server upgrades, and increase the reliability of its systems.

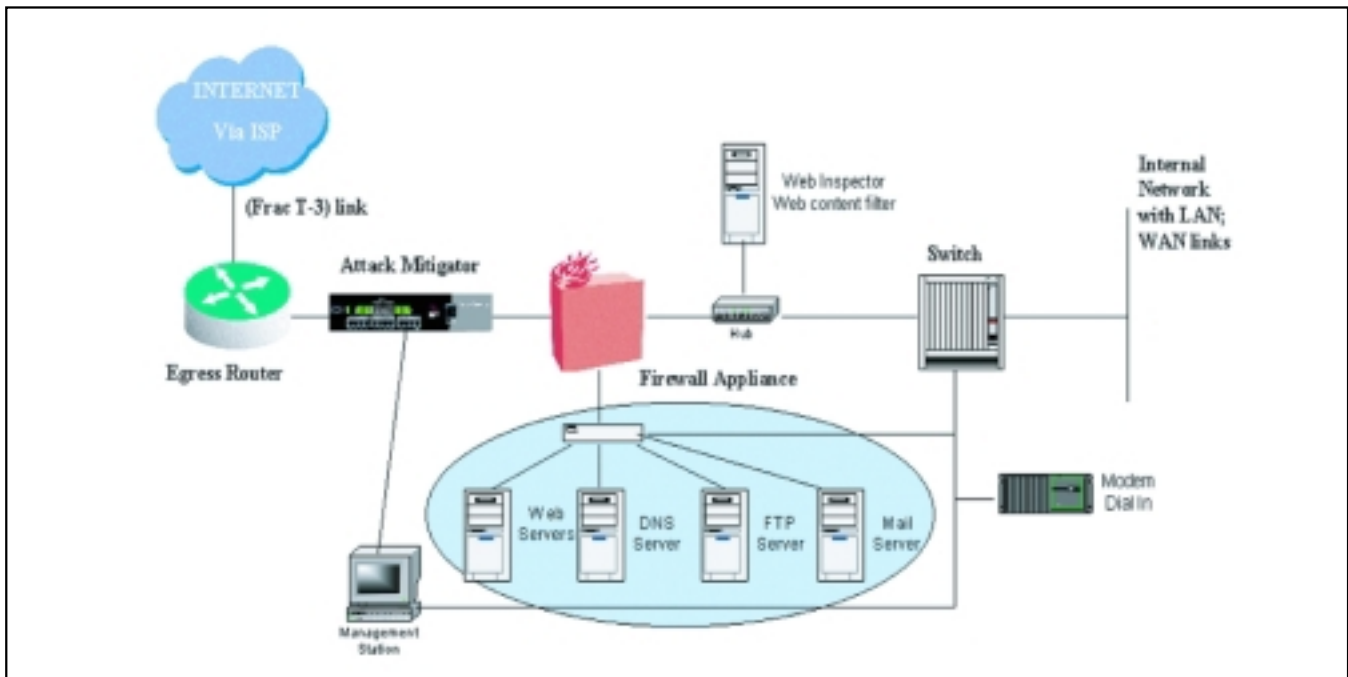
Supporting Dozens of Locations Statewide

Supporting the wide-area networking needs of multiple agencies in more than 100 locations across the state, the centralized IT services team has assembled a

formidable networking infrastructure rivaling that of the largest private enterprises:

- More than 100 routers in an internal network based on T1 links
- Internet access through a single fractional T3 (10Mbps) link
- Steady state bandwidth use of about 5Mbps
- Individual remote access provided by dial-up and VPN
- 100Mbps local LANs, some Gigabit Ethernet
- 30,000 IP addresses assigned for 70 percent of state employees
- Single public network hub for internal network
- DMZ with multiple Web servers
- Egress router, firewall, Web content inspector used for security infrastructure at network hub

CASE STUDY - ATTACK MITIGATOR



Central Site Topology

Unfortunately, with so many computing resources -- and fewer human resources to manage it all -- the state's IT network became a tempting target for hackers, crackers, and thieves. The state began to experience several attacks, usually against softened hosts in small numbers. Unbeknownst to the state's IT pros, numerous vulnerabilities were leaving their network resources exposed. Attack traffic was co-opting egress bandwidth and attacks such as SYN floods were occurring every three to five minutes. ICMP floods were happening several times a minute.

Initially, these were annoying -- but not debilitating events. But that perception changed significantly once the state endured a NIMDA attack that required the rebuilding -- from "scratch" -- of 17 Windows NT servers and numerous additional PCs. This watershed event, coupled with inconsistent availability, sluggish performance, and increasing bandwidth consumption forced the state to take aggressive steps.

Visibility Before Resolution

Knowing that major security problems existed -- but unsure about the extent and gravity of them -- the state undertook an extensive evaluation of commercial and public-domain intrusion detection systems (IDSs). While resolving security breaches was, of course, critical, the state felt that resolution could only occur after it achieved complete visibility into the problems.

Requirements during the selection process included the ability to mitigate SYN floods and ICMP floods, perform HTTP URI filtering, and limit connections and bandwidth rates for specific applications. Just as important, the IT group wanted a fast and simple implementation process that would not change its existing network equipment, design, and topology.

After completing its analysis, the state selected the Attack Mitigator from Top Layer Networks. Through a combination of custom ASICs, optimized packet inspection software, and an intuitive browser based configuration utility, the Attack Mitigator enables IT and network security professionals to protect their networks against attacks, resulting in an easy to use, high performance defense solution.

Attack Mitigator resides between the firewall and router and continuously watches for a comprehensive range of attacks by using a combination of packet filters, packet sequence signatures, HTTP URI filters, TCP connection counters, and threat-level assessment based on network connection behavior.

Fast Implementation, Immediate Results

The IT department installed the Attack Mitigator between its Cisco router and its firewall -- an installation that took a mere 15 minutes. The Attack Mitigator provides a Monitor mode that recognizes attacks and

CASE STUDY - ATTACK MITIGATOR

issues alarms or SNMP traps but does not touch the IP packets. This mode let the state ensure the new installation didn't disrupt its network and provided valuable logs of data on the constant attacks.

After just the first day, the IT group noticed that there were numerous anomalies to their network -- in addition to the attacks -- that were hampering performance. There were redundant paths, unwanted IP addresses, and unwanted management traffic from the Internet. After a week of "Monitor" mode to avoid false positives, the state began an iterative tuning and calibration process, configuring the Attack Mitigator to respond to the most obvious attack patterns.

Just weeks later, the state IT group had dramatically reduced ping attacks, SYN floods, and other extraneous traffic -- which created a significant improvement in the performance of its firewall. It also learned that the servers used by the state's taxation agency were a high-volume target as April 15 neared.

From an ROI perspective, the Attack Mitigator has been very successful. By reducing unauthorized traffic, the state has been able to postpone a "forklift upgrade" of its firewall, forego spending on new and additional servers, and hold off on expanding its T3 bandwidth. What's more, the agency can offer better SLA performance, serve greater numbers of users, and increase their own staff productivity by avoiding the time and cost of cleaning up after attacks. Without the Attack Mitigator, the state would have spent significantly more money-- and would not have anywhere near the same level of security it now enjoys.



“ From an ROI perspective, the Attack Mitigator has been very successful... Without the Attack Mitigator, the state would have spent significantly more money-- and would not have anywhere near the same level of security it now enjoys. ”

— State IT Director

About Top Layer

Since 1997, Top Layer Networks has delivered proven network security solutions worldwide, enabling enterprises to protect against cyber threats, and scale their infrastructure to meet new, ever increasing security demands. The Company's intrusion detection and prevention products are built on a patented, ASIC-based architecture. The products are engineered to block high-volume DoS and DDoS attacks, HTTP worms, traffic anomalies and unknown attacks; improve the effectiveness of intrusion detection systems through intelligent balancing and distribution of traffic; and enhance the availability and performance of firewalls through firewall/VPN balancing technology. Top Layer Networks is headquartered in Westboro, Massachusetts with sales and support presence in Australia, France, Germany, Japan, Korea, Malaysia, Singapore and the United Kingdom.

**Top
Layer™**

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

08-02 © 2002. 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, and SecureWatch 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.