

Globix Protecting Clients Internet Business

Globix is a Global Tier 1 Managed Service Provider offering application, media and infrastructure managed services to enterprises with business critical applications. It offers a comprehensive, single-source solution for every Internet need from management of web applications, servers and databases, to security, streaming, network bandwidth, and co-location facilities.

When Globix saw a rising trend in the frequency and complexity of DDoS attacks, it knew that traditional ISP methods of mitigating DDoS attacks were no longer going to provide adequate protection for its clients.

“Globix wanted to help its clients build a protection mechanism against the crippling effects of these DDoS attacks, which were having a devastating impact to our clients on-line business,” commented Brendan Slater, Director of Professional Services, Globix.

DDoS attacks are where a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

The DDoS threat affected two main areas of Globix’s business. Firstly, its network operations center, which manages its global network was impacted in that each attack targeted at one of its customers drove a huge amount of malicious traffic onto its backbone. The operations center had to respond quickly and effectively in order to manage its backbone traffic and maintain service not only to the victim of the attack, but to the rest of the Globix client base. These conflicting requirements meant that Globix could not always allow clients to weather the storm of a very large attack. In some cases black hole routes would be used to ban all traffic coming from the same part of the Internet as the attack.

Secondly, Globix’s security services department, already trusted with managing security for a large section of its client base, had to respond to this new threat by devising a response based on a sound technical solution and integrating this into the existing service delivery framework.

“Our primary requirements in the search for a suitable high capacity technology were that it was tried and tested from a vendor with a proven background in security and in particular, Intrusion Detection Systems (IDS) and



Intrusion Prevention System (IPS) solutions,” commented Brendan Slater. “The technology needed to be able to manage DDoS mitigation against the massive SYN flood and bogus *http* requests typical of the attack patterns experienced by our clients. At the same time we wanted to deploy a solution isolated from our existing network so that we could continue to provide service to other customers regardless of the attack size.”

At the time, DDoS attacks of this nature were relatively rare and could vary in execution greatly. Thus finding a suitable technology to protect against them was a difficult task. Previously, ISPs hadn’t dealt with this type of malicious attack pattern, so there was no basis for historical comparison. Normal network capacity and traffic management techniques were only partly effective – something new had to be found.

“Traditionally the ISP community has dealt with DDoS attacks by using techniques such as black hole routes or access control lists. However, this did not give us the granularity needed to stop the new, more complicated attack patterns. We needed a device capable of protecting customer’s web infrastructure on a per-connection basis; this is the only way to qualify which traffic is valid,” commented Slater.

After much product evaluation with a variety of vendors including Tipping Point, Globix chose Top Layer and its second-generation Attack Mitigator™ IPS 5500 technology capable of handling attack traffic speeds of up to 1Gbits per second.

“No other vendor has produced a second-generation product yet, so Globix was able to implement a technology developed from a research and development program built on real-world experience,” stated Slater.

“We particularly liked the Top Layer device’s ability to inspect each user connection for correct protocol usage

and then act based on the customer policy. The ruleset we have developed enables us to granularly control what constitutes normal service usage for each customer on a per-user basis to drop abusive or bogus traffic,” commented Slater.

Faced with an ever-present threat to their ongoing business Globix’s clients and the market wanted a solution immediately. Globix allocated a dedicated technical team to develop a solution which met the immediate need, but more importantly provided Globix with a platform upon which it could develop its product and service range in response to the changing threats and attack patterns.

Top Layer provided the technical hardware solution and also a great deal of intensive partner assistance. The partnership enabled Globix to initially launch the Network Defender 1000 solution. Based on Top Layer’s high capacity Attack Mitigator IPS 5500-1000 product, the solution is aimed at businesses experiencing or at risk of experiencing large-scale DDoS attacks and provides a high level of attack protection – and as a shared resource, offers real value for the money.

The service provides 100% inspection against a specific set of pre-determined rules. Any traffic that is identified as a threat is dropped, allowing only ‘cleansed traffic’ to be routed to the website ensuring clients continue to be served.

Implemented soon after was the complimentary Network Defender 100 service based on the Top Layer Attack Mitigator IPS 5500-1000. This solution will provide ‘always on’ protection with a custom protection policy fully managed by a Globix specialist. A combination of the two services plus the use of other Globix services provides the “defense in depth” strategy Globix see as critical if an organization is to protect its on-line assets as robustly as possibly.

“ Looking forward, we will be able to leverage the considerable capabilities presented by this technology to drive additional value for both our customers and Globix. ”

— Brendan Slater,
Director of Professional Services, Globix

The development of the Network Defender Service has been added to Globix’s security service portfolio and has not only enabled Globix to support the requirements of its existing client base, but also offer a new service to a wider market to win new customers. As a result, Globix’s security services division is experiencing substantial growth, and the company is now positioned as a leader in Intrusion Prevention Technology.

The project has been the catalyst for a broader review and development of Globix security services offerings to drive forward a product development roadmap which ensures its clients have the best possible security services available. This ability to support customer’s businesses has given Globix a competitive advantage in the market place.

“ Looking forward, we will be able to leverage the considerable capabilities presented by this technology to drive additional value for both our customers and Globix,” concluded Slater. “ With the help of Top Layer, we will always respond to our clients’ needs and build solutions to enable them to grow their business.”

About Top Layer

Founded in 1997, Top Layer Networks develops network security solutions that enable enterprises worldwide to protect their infrastructure and critical online assets from cyber threats. The Company’s patented, ASIC-based 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, Massachusetts with sales and support presence in Australia, Canada, France, Germany, Japan, Korea, Malaysia, the Netherlands, and the United Kingdom.



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

www.TopLayer.com

11-04 © 2004. Top Layer Networks, Inc. Attack Mitigator, DCFD, Flow Mirror, and IDS Balancer are trademarks of Top Layer. AppSafe, AppSwitch, SecureWatch, Top Layer, Top Layer Networks, TopFire, TopFlow, TopPath, TopView, and perfecting the art of network security 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.