

Top Layer Keeps ISP Running in Face of Adversity

Background

SDV Plurimedia is one of France's largest Internet Service Providers (ISPs), offering customers Internet and Intranet networking, e-commerce capabilities, graphic design, systems engineering, and news publication services.

A 15 year-old company, SDV has a well-developed relationship with its customers, providing various press and media, banks, insurance agencies, SMEs and local authorities hosted and managed media solutions. SDV offers around-the-clock services and promises complete reliability and security.

As SDV provides Internet solutions for high profile customers, including international firms such as BNP Paribas and French daily newspapers including *Le Figaro*, it is essential that SDV ensure 24/7 uptime and complete protection against security threats. Media sources are highly visible targets for attacks, with brute force cyber attacks and defacement attempts as regular occurrences. With these potential attacks a real threat, it is essential that media sources maintain their reputations and integrity and ensure they're not presented as unreliable news sites. This concern led SDV to approach Top Layer to deploy its Intrusion Prevention System (IPS) 5500 solution and unique Three Dimensional Protection (3DP) technology to ensure total peace of mind.

The Challenge

SDV was subjected to a number of high volume rate-based attacks targeted at its newspaper customers. Any attack aimed at SDV's network, upon reaching a certain threshold, would affect all of SDV's customers, thereby violating their service provision contracts. SDV had worked hard over the previous 15 years to develop a solid reputation and relationship with its customers, and it was not prepared to compromise this in any way.

"The initial challenge for SDV was to find an attack mitigation solution that could not only handle the current peak load of 500Mbps, but would also quickly scale to fit a higher bandwidth requirement when necessary,"



explained Mark Armitage, EMEA Technical Director, Top Layer Networks. "SDV anticipated a doubling of peak load over the coming year, and an upgrade of their current 650Mbps feed. It was crucial to know that if a flood attack occurred, they could cope without affecting customers' services and damaging their reputation, ensuring business continuity from rate-based attacks."

SDV serves over 40 million page hits per month, and run an industry-leading data centre in Strasbourg that is as diverse as the needs of its many customers. Through its doors can be found over 150 servers, running AIX, Linux, Advanced Pick, Oracle, Windows 2000 and Apple, with a combined storage capacity of over eight terabytes. Not only was it a challenge to find an IPS that could handle gigabit wire-speeds, it was also a challenge to find an IPS that was aware of multi-vendor environments and could offer zero-day attack protection for all of their servers and applications.

SDV's infrastructure is built for speed, with redundant, multi-gigabit technology used throughout to ensure its users and hosted servers get guaranteed network availability. SDV would not accept inline security devices that could slow down the network performance or affect availability. In particular, with such a large distributed network, achieving low-latency would be key as delays are amplified by the size of a network.

In order to meet the hosting service level agreements, it was crucial for SDV to find a solution that offered zero packet loss and 100% accuracy to block and mitigate all attacks regardless of the network load.

Salim Gasmi, CTO from SDV explained, “We approached a number of IPS vendors that all claimed gigabit performance, but in reality, none of them could even handle an attack based on fast Ethernet speeds. These are the reasons why we turned to Top Layer.”

The Solution

SDV decided to deploy a Top Layer IPS 5500-1000 HA cluster, as it provides Top Layer’s 3DP, the most accurate, highest performing protection against content-based, rate-based, and unauthorized access attacks.

3DP takes existing principles of IPS to a new level, introducing for the first time three orthogonal planes of inspection. 3DP goes beyond just deep packet inspection, examining all seven OSI layers, integrating higher level decodes than the traditional methods of inspection. The depth capabilities enable the second of three planes of inspection: Context.

By analyzing the use and abuse of network and application protocols, it is possible to spot the ‘contextual fingerprints’ of single or blended threats. Top Layer’s 3DP solution looks for deviations from the rules that define both ordered and dynamically normalized protocols. Contextual fingerprints are backed up by binary signatures matched with known threats.

Contextual fingerprints are further strengthened by Top Layer’s solution if analytical information is maintained over time, the third plane. “Time” means maintaining stateful information about users, connections and flows for significant durations, although this is not a lengthy analysis.

Top Layer has coordinates in all three planes, and using contextual fingerprints is highly effective and ensures reliability at wire-speed, with worst-case packet latency of just 50µs. However, solutions providers who omit one or two of these planes will find the reliability of contextual fingerprints is weakened.



“ With Top Layer’s 3DP, we are now insured against the three levels of intrusion, all at gigabit speeds, without affecting network performance or availability. SDV can rest assured knowing that the Top Layer IPS 5500 covers all that and the other growing threats out there. ”

**— Salim Gasmi
CTO, SDV Plurimedia**

SDV wanted the implementation of the IPS to be immediate, so the 5500-1000 cluster was installed between the Internet connection and the perimeter firewall with virtually no downtime. Within minutes, SDV were provided with SYN, TCP and UDP flood protection, and, by following a simple-to-use GUI, all FTP, DNS, HTTP, SMTP, CIFS, and RPC protocols were also enabled for advanced intrusion protection.

“Initially we were looking for a specific defense solution. However, we quickly realized that we needed a complete protection mechanism. With Top Layer’s 3DP, we are now insured against the three levels of intrusion, all at gigabit speeds, without affecting network performance or availability. SDV can rest assured knowing that the Top Layer IPS 5500-1000 covers all that and the other growing threats out there,” said SDV’s Gasmi.

“SDV had concerns for the security and the service level agreements with its customers, and required a solution that offered complete security from attacks without affecting business continuity. SDV have a high standard of service to live up to, and we offered a solution that could support its excellent reputation, ensuring there would be no down-time or inconsistencies to the systems,” said Armitage.

The Result

Top Layer’s 3DP is now an integral part of SDV’s security infrastructure, and, as a result, SPV can confidently offer high-profile hosting services, without the risk of malicious content on network traffic and inappropriate rates, potentially bringing its system, and therefore the customers’ networks, to a standstill.

Top Layer has helped SDV preserve its excellent reputation as a resilient and reliable Internet Service Provider. “We are now able to do business without our SLAs being at risk of attack. For an ISP, this is essential and Top Layer has instilled confidence in our security system and ensures continuity and performance of our network,” said Gasmi.

“SDV is very happy with the IPS 5500 and is currently talking to Top Layer about installing further units to cater to our growing networking needs. SDV can now offer the best levels of protection and service uptime for all of our customers, and ensure that our clients’ reputations and online presence are maintained at the highest degree, guaranteeing total peace of mind.”



“SDV is very happy with the IPS 5500 and is currently talking to Top Layer about installing further units to cater to our growing networking needs. SDV can now offer the best levels of protection and service uptime for all of our customers.”

**— Salim Gasmi
CTO, SDV Plurimedia**

About Top Layer

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. Our family of IPS appliances is designed with “Three Dimensional Protection” that provides the most advanced protection capabilities against known and unknown attacks at the highest tested performance rates. Top Layer Networks is headquartered in Massachusetts USA with sales and support presence in Canada, France, Germany, Japan, Korea, The Netherlands and the United Kingdom.



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

www.TopLayer.com