

Grocery Gateway Turns to Top Layer to Deliver Protection from Growing Threats on the Internet

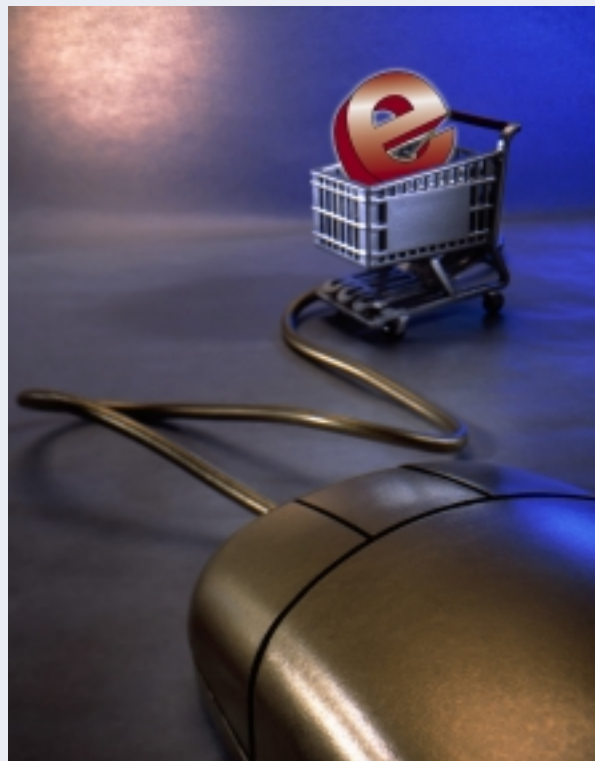
Solution Overview

Profile: Grocery Gateway has thousands of satisfied customers across its two businesses — home grocery delivery and 3rd Party Logistics (3PL). The 3PL business is serviced under the Gateway Delivery banner, which provides B2B and B2C delivery services for clients such as Staples Canada.

Challenge: Grocery Gateway had witnessed the growth in cyber threats on the Internet, and decided it was time to layer its security infrastructure to optimize its overall protection. The challenge for Grocery Gateway was to identify an intrusion prevention solution that would complement existing security devices and policies, without directly replacing or negatively impacting its present security investments. With a focused IT team, Grocery Gateway needed a solution that would offer solutions and automatically fix problems, instead of merely identifying threats.

Solution: Grocery Gateway conducted extensive research, canvassing the industry and holding discussions with service providers, and Top Layer Networks' Attack Mitigator™ IPS continuously came up as a potential solution. After evaluating a demo unit in the lab, the Attack Mitigator IPS worked well — blocking malicious traffic without negatively impacting network performance. The combination of deep packet inspection techniques, anti-DDoS capabilities and easy integration of logs into Grocery Gateway's existing management framework put the Attack Mitigator IPS at the top of the list.

Benefits: Top Layer's Attack Mitigator IPS helped Grocery Gateway meet its layered security goals by providing the active intrusion prevention mechanism that seamlessly works within its existing infrastructure — IDS, firewalls, routers, etc. In addition, the Attack Mitigator brought with it a built-in redundant power supply, and fail-open capabilities to ensure network connectivity. By strategically placing the Attack Mitigator IPS within its network, Grocery Gateway can rest assured that the box is effectively protecting its systems from the growing number of cyber threats that are evident today. Not only did the box provide seamless installation with zero latency, but it also alleviated the traffic load that Grocery Gateway's firewall and servers had previously borne the brunt of, improving overall network performance.



CASE STUDY - ATTACK MITIGATOR IPS

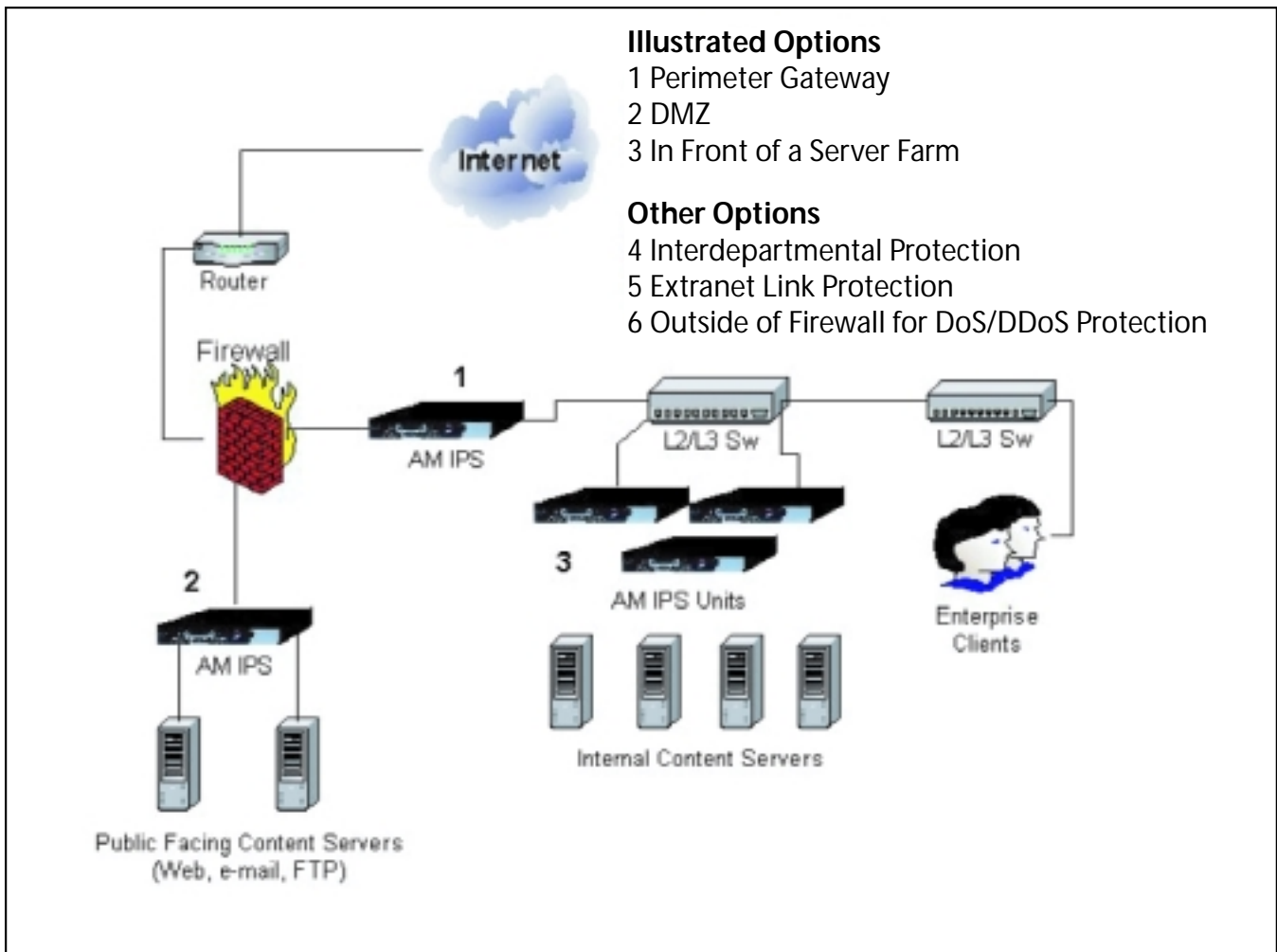
Full Case Study

Grocery Gateway was founded by a group of entrepreneurs with the idea that people had better things to do than shop for groceries. In business since 1998, Grocery Gateway has thousands of satisfied customers. The company started with a handful of employees and a couple of rented trucks. Now, it employs hundreds, manages a fleet of 100 trucks with climate zone compartments, and maintains a 280,000 square foot Market Centre in Downsview, Ontario, Canada with operations offices in Mississauga. Grocery Gateway consists of two businesses — home grocery delivery and 3rd Party Logistics (3PL). The 3PL business is serviced under the Gateway Delivery banner, which provides B2B and B2C delivery services for clients such as Staples Canada.

Grocery Gateway observed the significant growth in cyber threats on the Internet in recent years and decided it was time to layer its security infrastructure for

better overall protection and eliminate any single points of failure. The primary obstacle for Grocery Gateway was to identify an intrusion prevention solution that would complement existing security devices and policies, without directly replacing or negatively impacting its security investments already in place. With a focused IT team, Grocery Gateway needed a solution that would automatically fix problems, rather than merely identifying threats.

“Our security infrastructure was solid, but we felt that as Internet threats evolved, so should our security needs. It was time for Grocery Gateway to consider intrusion prevention, as the technology had finally matured to the point where it was an infrastructure necessity,” said Todd Norton, Network Engineer, Grocery Gateway. “The research our team did was extensive and Top Layer Networks continuously appeared on the radar screen.”



Attack Mitigator IPS Deployment Options

Shopping for Attack Mitigation

Grocery Gateway conducted extensive research, canvassing the industry and holding discussions with service providers, and Top Layer Networks' Attack Mitigator IPS continuously came up as a potential solution. The other systems and proposed solutions that Norton's team evaluated required either multiple boxes to do the job, or required him to completely replace his existing devices — which didn't meet the company's layered security goals. Grocery Gateway decided to take a much closer look at Top Layer's Attack Mitigator IPS.

Norton contacted EdgeTech Services, a provider of enterprise security solutions that resells Top Layer's Attack Mitigator IPS product line. The combination of deep packet inspection techniques, anti-DDoS capabilities and easy integration into Grocery Gateway's existing management framework thrust the Attack Mitigator IPS to the top of the list. EdgeTech supplied Grocery Gateway with an Attack Mitigator IPS demo unit to evaluate in its lab. The Attack Mitigator IPS was impressive and met Norton's specific intrusion prevention needs — blocking malicious traffic without negatively impacting network performance and easily integrating into their existing infrastructure. "The Attack Mitigator was great at analyzing malformed HTTP packets, digging deep into the packet before passing it on — this was a key criterion for us to protect against DoS attacks, zero-day exploits, network traffic anomalies and other threats attempting to harm our network and online assets," explained Norton.

The Importance of Network Citizenship

After nearly two weeks in monitor mode to observe how the Attack Mitigator interacted with the network and traffic, Norton flipped the switch to mitigate mode. The integration of the Attack Mitigator into the existing network environment was seamless. Top Layer's Attack Mitigator IPS has enabled Grocery Gateway to meet its layered security goals by providing the active intrusion prevention mechanism that works seamlessly with its existing infrastructure — IDS, firewalls, routers, etc. Added Norton, "Many security devices claim to work well with others in the network. The Attack Mitigator met those claims where other alternative solutions fell short.

The Attack Mitigator brought with it a number of key benefits for Grocery Gateway:

- Built-in redundant power supply
- Fail-open capabilities to ensure network connectivity
- Deep-packet inspection techniques
- Unmatched anti-DDoS mechanisms
- Security logs that easily integrates into Grocery Gateway's firewall
- Zero-latency.

"We were clear in our objectives for attack mitigation technology — we didn't want to replace any of our existing systems and devices to rely on one single security gateway and have a single point of failure," explained Norton. "The Attack Mitigator performed as advertised, dropping malicious traffic immediately and working well with the other devices in the network. Also, the Attack Mitigator IPS activity log easily integrates into our firewall solution providing us with the intelligence we need to make better security decisions."

Beyond Attack Mitigation — Alleviating Stress

By placing the Attack Mitigator IPS between the ISP's router and all of Grocery Gateway's systems, the company can rest assured that the box is effectively protecting the company from the growing number of threats. "The Attack Mitigator IPS has been in place for nearly six months, and to date the system has blocked the many threats that are lurking in cyber space, including the Nachi, MS Blast and Welchia worms — thanks to a combination of effective technology and good security policies."

The architecture of the Attack Mitigator solution is what ensures effective protection. Not only is it good at deflecting DoS attacks, but it goes much further by protecting resources from attacks where signatures have not yet been created, helping companies like Grocery Gateway focus on its business operations instead of agonizing about zero-day exploit attacks, unknown attacks and other cyber threats that lurk around the Internet.

CASE STUDY - ATTACK MITIGATOR IPS



“ The Attack Mitigator performed as advertised, dropping malicious traffic immediately and working well with the other devices in the network. Also, the Attack Mitigator IPS activity log easily integrates into our firewall solution providing us with the intelligence we need to make better security decisions. ”

*— Todd Norton, Network Engineer
Grocery Gateway*

“I used to spend a lot of time sifting through activity logs and reports to identify infected hosts and network problems. With the Attack Mitigator in place, I can turn my attention to other network and IT projects that require attention without worrying about the onslaught of threats today’s companies are faced with.”

Not only did the box provide seamless installation with zero latency, but the solution also alleviated the traffic load that Grocery Gateway’s firewall and servers had previously been forced to handle, improving overall net-

work performance. In addition, Top Layer’s engineering and support teams have been fast to react, share information and ensure that Grocery Gateway is secure and happy. “Being a service business, Grocery Gateway knows how important it is to be responsive to customers, deliver the goods, and ensure satisfaction. Top Layer’s engineering and support team follows that philosophy and have enabled our business to operate effectively, and securely,” added Norton.

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 France, Germany, Japan, Korea, 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

06-04 © 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.