

Top Layer Networks Helps Chicago Webs Avert Business Disaster

Solution Overview

Profile: Founded in 1998, Chicago Webs is one of the most recognized hosting providers on the Internet. Located in Illinois, the Company is considered one of the premier providers of shared hosting and dedicated servers, offering a range of web service solutions including Macromedia ColdFusion and Microsoft .NET. Chicago Webs has based its business on providing a solid, reliable network for programmers and developers to deploy their online applications and information. The availability and protection of their network is vital to its survival and success.

Challenge: Chicago Webs had experienced a severe Distributed Denial of Service (DDoS) attack that crippled their business, shutting down their network for 3 days. With their business and livelihood based upon providing reliable network capacity to customers, any sustained



downtime for Chicago Webs could result in considerable loss of business and customer goodwill. In addition, the man-hours spent on fixing networks and stopping the attacks drained valuable resources from other areas of the business, further hampering productivity. Chicago Webs' customers demand that the network be available to them 24 hours a day, making it critical that the current DDoS attack be stopped and future attacks prevented.

Solution: Patrick Stangler, CEO and president of Chicago Webs, had heard of Top Layer Networks and its Attack Mitigator[™] IPS solution through referrals from his customers. Given the severity of the attack and the need to get the network up and running quickly, Stangler didn't have time to shop around for other solutions, relying fully on 3rd party referrals to the product. Based on the feedback, Stangler felt that Top Layer Networks would provide him with the protection needed to thwart the current attacks, while better positioning him to prevent future assaults on his network. Three days after the attacks began, Stangler installed an Attack Mitigator IPS (Intrusion Prevention System) into his network.

Benefits: The benefits of the solution have been very significant. Within 20-30 minutes of installing the Attack Mitigator IPS into the network, Stangler noted that the DDoS attacks that had crippled Chicago Webs had been stopped and that his company was back in business. Additionally, Stangler notes that with the Attack Mitigator handling the malicious traffic on his network, his servers are able to work at full capacity, making his network faster than before the introduction of the Attack Mitigator IPS.

CASE STUDY - ATTACK MITIGATOR IPS

Full Case Study

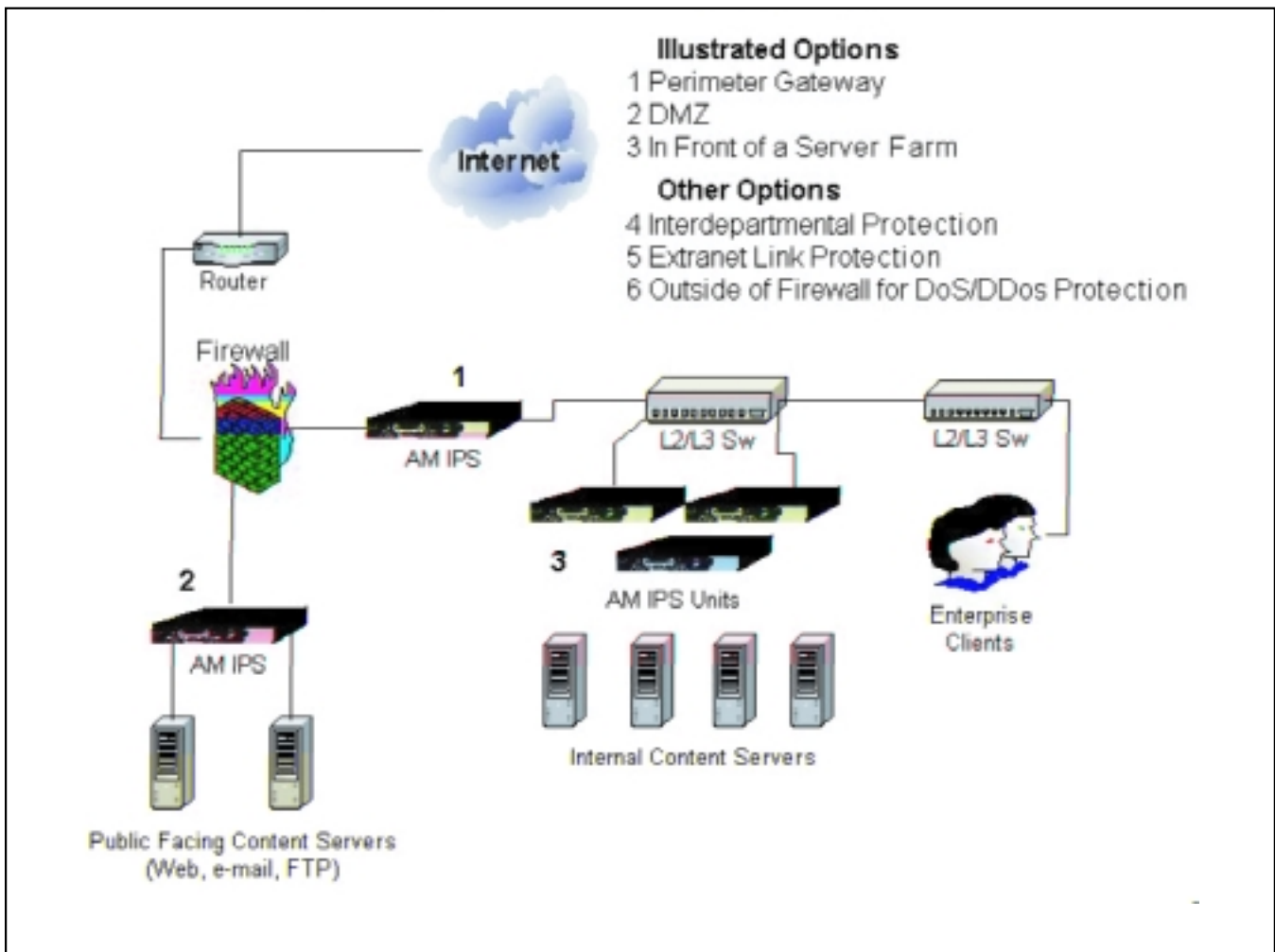
Founded in 1998, Chicago Webs is one of the most recognized hosting providers on the Internet. Located in Illinois, the Company is considered one of the premier providers of shared hosting and dedicated servers, offering a range of web service solutions including Macromedia ColdFusion and Microsoft .NET.

With a business model based upon ensuring that Web developers and online businesses have connectivity to the Internet to run their respective businesses, network performance and reliability are issues of paramount importance for Chicago Webs. Downtime for any reason on the Chicago Webs network not only costs them money, but costs their clients money as well. For all of these reasons, when the Distributed Denial of Service (DDoS) attacks came in against the Chicago Webs network, the effect was potentially crippling to its business, as well as to its customers businesses.

"As a company, we've always taken the proper steps to ensure the security of our network and our clients who use the network, so when the DDoS attacks came in and our network went down, it really brought us to a halt," said Patrick Stangler, CEO and President of Chicago Webs. "We needed a solution that would stop the attacks and enable us to get our network back up immediately, while providing us with long term security against futures attacks like this. And we needed it all immediately, because we were losing faith with our clients fast."

The Network Goes Dark

On a good day, the Chicago Webs network runs like a finely tuned machine. To provide access for over 3,000 domains, Chicago Webs utilizes 50-60 network devices and more than 50 servers. Traditional network defense consisted of properly securing a couple of routers and



Attack Mitigator IPS Deployment Options

firewalls. The Company had seen its network attacked before, but had always been able to thwart the attempts to compromise the system.

July 31st, 2003, began as any other day for Chicago Webs, only to end in disaster. During the early hours of the day, the Chicago Webs network experienced a highly targeted DDoS attack. In all, 2,100 servers from around the globe targeted Chicago Webs. The attack exploited the network's ports, http, e-mail, and various other applications to cripple the entire network.

The attack began on a Friday and targeted specific RackShack servers, directly impacting customers. Williams' team was able to track the source of the attacks and beat them early on. "With 11 gigabits of transit through the Internet, volume wasn't the issue. Specific sources were what we had to look for and we did so effectively," said Stangler. The attack had accomplished its goal of making the network go dark, and Chicago Webs was under the strain of either getting the network backup and running immediately, or losing customers. As the downtime continued, the financial impact upon the business grew exponentially. With four developers working on the problem, and an assortment of people from premier partners such as Cable and Wireless in Chicago and Cisco, the costs began to mount for Chicago Web, yet no solution presented itself.

The crippled network also began affecting the customer base. With no end in sight, Chicago Webs starting seeing an exodus of their customers who needed Internet access for the success of their own businesses. In all, the Company lost between 70-100 unique accounts. Normal applications were halted as well, as daily e-mail went from 500 per day down to no e-mail communications at all.

"Being a smaller company, we took quite a big hit. Anytime you lose business, it hurts, but the network downtime had caused us to lose a chunk of business in a very short period," said Stangler. "And the scary thing was we hadn't been able to solve the problem. We needed to find a robust solution that would stop the attacks, and we had to do it immediately.

Flying for a Solution

After determining the cause of the network outage and the applications affected, Stangler knew that he needed to purchase an Intrusion Prevention System

(IPS) to stop the attacks and return his network to normal. A major stumbling block that was hampering this process was the fact that he had no time to perform the normal evaluation process that goes into such a major purchase.

Given the situation and the dire need for a fast solution, Stangler knew that he had to rely totally on word of mouth and third party reference to provide him direction in purchasing an IPS product. After discussions with premier partner Cable and Wireless, Stangler opted for Top Layer Networks' Attack Mitigator IPS.

"We didn't have the time to perform the normal due diligence, so we had to rely on what my trusted colleagues recommended," Stangler indicated. "Cable and Wireless is a Top Layer customer and they were extremely satisfied. That was good enough for us, so we went for it."

With the decision made to go with Top Layer Networks, the next step was to get actual product to implement. Given the urgency, Stangler took it upon himself to secure and deliver the product as soon as possible. Rushing to the airport, Stangler flew from St. Louis to Boston, where he met a Top Layer representative with the product. A few hours later, Stangler was back in line at the airport, hoping to return as quickly as possible to save his business.

"In my estimation, it certainly was a matter of life or death. The life or death of my business. We needed to get our network back up and running as quickly as possible," said Stangler. "Given the importance of the product, there was no way I was letting it out of my sight. Luckily for me, it fit in the overhead compartment on the airplane."

A Triumphant Return

Stangler had his solution, and wasted no time implementing it into his network. Within 20 minutes of putting the Attack Mitigator IPS on the internal side of the router, the DDoS attacks stopped entirely.

"I got back to Chicago, and we immediately went to work putting it in," said Stangler. "We set up and configured the Attack Mitigator IPS on the network, and within about 20 minutes, it was blocking the bad traffic. I couldn't believe it - we were up and running, mail was coming in, HTTP was back in service, and Chicago Webs was back in business. It was amazing."

CASE STUDY - ATTACK MITIGATOR IPS



“ If it weren’t for the Attack Mitigator IPS, I would be out of business. I couldn’t sleep at night without knowing the Attack Mitigator IPS was protecting my clients and our network. ”

*— Patrick Stangler, CEO and president
Chicago Webs*

As the Attack Mitigator IPS continued to stop the network attacks, Chicago Webs began noticing the immediate expected benefits, as well as some unanticipated benefits. With the network back up and running, Chicago Webs could begin the process of winning back customers that had been disenfranchised by the network downtime. Overall, the Company was able to win back over 80% of the clients that had left because of the outage.

Additionally, clients immediately noticed the positive effects the Attack Mitigator IPS had on overall network performance. After plugging the Attack Mitigator IPS

into the network, Stangler indicated that over a dozen customers proactively informed him that the network was noticeably better than at any previous time before the implementation.

“I can’t say enough about Top Layer Networks and this product – I literally owe my livelihood to them. If it weren’t for the Attack Mitigator IPS, I would be out of business,” said Stangler. “I couldn’t sleep at night without knowing the Attack Mitigator IPS was protecting my clients and our network.”

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

01-04 © 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.