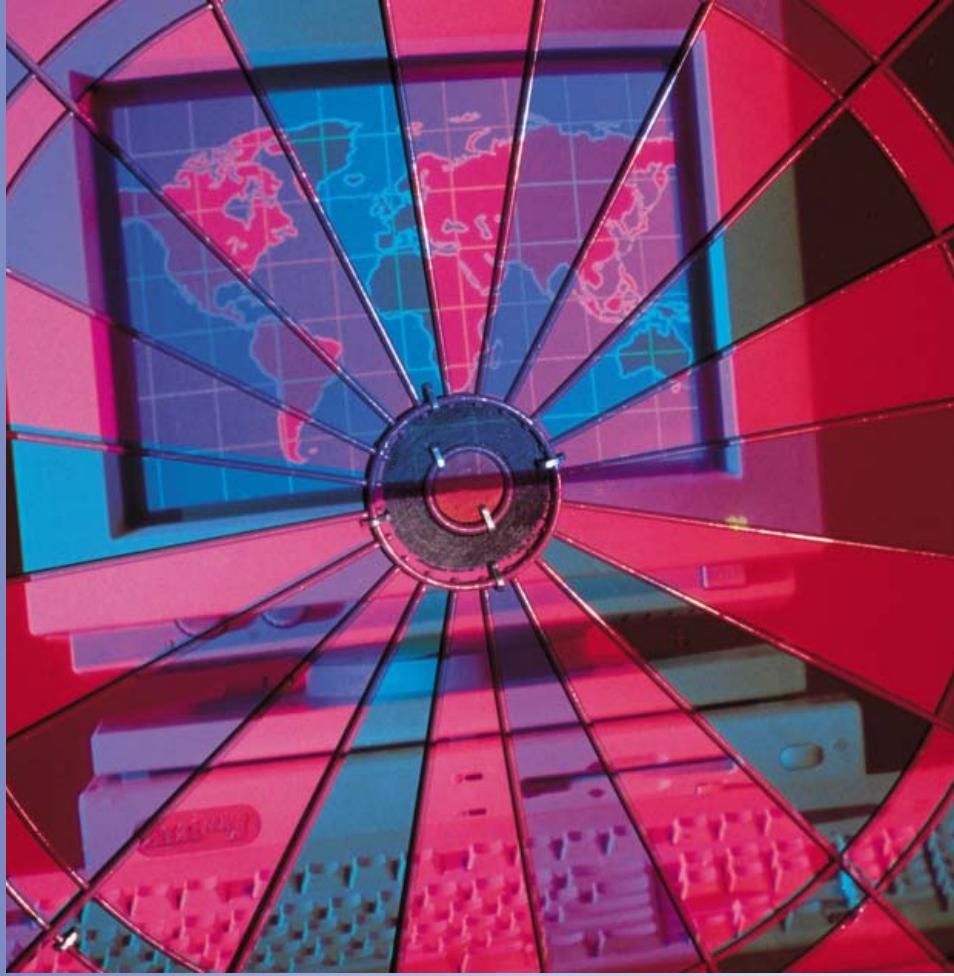


SOLUTION BRIEF



DDoS ATTACK SOLUTION



Double NSS Award

Denial-of-Service Protection Solution

Key Trends

Businesses have been embracing the Internet in record numbers to reach customers, partners, and suppliers. For several years now, Enterprises and xSPs have sought to create competitive advantage by utilizing the Internet to reach new levels of customer service and operational efficiency. More recently, many large, established companies have turned to the Internet to re-engineer key business processes, reduce costs, and increase customer satisfaction.

However, the ubiquitous nature of the Internet has also created new opportunities for cyber crime activities that seek to profit from the disruption of business activities by employing sophisticated, brute force Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks for both fun and profit.

A 2004 FBI/CSI survey concluded that DDoS attacks were the number one cause for financial losses for business.

Today, an attacker can hijack tens of thousands of compromised machines to launch an attack.

There is an increasing trend towards organized crime activities using DDoS attacks to extort money from businesses.

The growth of new Web sites over the past year has continued at a near-record pace of an average of 900,000 new sites per month, despite the steady drumbeat of security threats. In previous years, a methodical and sophisticated hacker could hijack perhaps 200 systems to launch a DDoS flood. Today, an attacker with even limited skills can assemble a botnet or zombie army of tens of thousands of compromised machines for launching gigabit-level attacks. Today's flood traffic can be comprised of anything from relatively simple SYN floods used by MafiaBoy in 2000 to take down Amazon, Yahoo and eBay, to more complex attacks, such as mimicking legitimate HTTP requests in order to overrun Web and application servers. More recently, there has been an increasing trend for attackers to profit from these attacks. There are the well-publicized and more discrete activities of domestic and overseas crime groups' intent on generating significant profits using new technologies to conduct good old fashioned extortion, often with a high degree of success.

As proof of these disturbing trends, a 2004 FBI/CSI survey concluded that DDoS attacks were the number one cause for financial losses resulting from cyber crime.

Business Challenges

The moment you install any Internet-facing mission critical assets, you are susceptible to debilitating DDoS attacks. The motives behind the attacks can be varied, from extortion attempts, to political statements, to bragging rights. The bottom line is that any organization that connects to the Internet is highly susceptible to these attacks, resulting in financial losses, downtime, and even legal liability in some cases, not to mention the embarrassment and loss of customer and partner confidence.

Without adequate protection, any Internet-facing mission critical asset is susceptible to debilitating DDoS attacks.

While, even Low-level DDoS (under 100Mbit/s attacks can easily overwhelm gigabit firewalls and mission critical servers, attackers now have enormous armies of compromised machines to unleash massive attacks against any business.

In spite of vendor claims and even some dedicated solutions, DDoS attacks continue to be some of the most difficult attacks to defend against. While Firewalls are the traditional perimeter defense solution, they often become the first point of failure during an attack, rendering the organization "offline" until both the attack ceases and the firewall settings are reset. Worse yet, some firewalls become overwhelmed and can let more sophisticated attacks through. More advanced hybrid attacks are also becoming prevalent. These attacks involve a Worm or Trojan hidden amongst DDoS traffic in order to trick or heavily task the security solution; hoping the malicious code slips through undetected. Once this Trojan is installed, it can hijack a machine and even force it to participate in another DDoS attack that can target internal or external resources.

For many organizations, being offline for any period of time can result in a catastrophic loss of business. For those companies who rely on the Internet as a key source of information exchange and revenue, it is clear that customers who are unable to gain access to their critical information or pay for goods and services, may decide to pursue more reliable competitive choices. Consumer confidence is easily lost when connectivity to a particular Web site is down. You often hear, "if they cannot maintain a secure Web presence, why should I trust my credit card information with them?" Another key element is the performance of a Website. Studies have shown that people are not willing to wait, on average, more than seven seconds. If resources are tasked or made unavailable by an attack, the user will tend to click somewhere else, possibly a competitor.

Expecting your ISP to address the problem is not always the best option. It is very common for ISP's to pull the plug on customers who are subject to regular attacks, to prevent the attacks from impacting the Internet connectivity of the ISP's other customers. While the ISP is willing to absorb the hit, your business can be severely impacted. Since even low-level attacks can overrun firewalls or other security solutions and your mission critical servers, subscribing to more bandwidth is not a viable option.

Understanding the Problem

The business impact of DDoS attacks can be far reaching. Overall network performance can be compromised leading to customer dissatisfaction and lost productivity from employees. Even worse, a complete loss of Internet connectivity resulting from a large sustained attack can lead to lost profits and inefficiencies. For example, when remote sales staff, cannot gain access to their corporate networks for activities such as payment processing.

The figures are enormous. According to the Yankee Group, attacks against major sites in February 2000, including the likes of Yahoo and eBay caused an estimated cumulative loss over \$1 billion. The severity of the impact of an attack is so critical to businesses that this issue resonates through Boardrooms around the globe.

The traditional intent and impact of a DDoS attack is to prevent or impair the legitimate use of computers, servers, and network resources. It is important to understand infrastructure limitations that play into the hands of cyber criminals. Bandwidth, processing power, and storage capacities are all common targets for DDoS attacks by consuming enough of the targets resources to cause some level of service disruption. An abundance of well-engineered capacity may offset some of the impact of an attack, but newer and more sophisticated tools place even the most abundant resources at risk.

The most common DDoS attacks today involves sending a large number of packets (that can even reach multi-gigabit total bandwidth) to a destination, causing excessive amounts of network bandwidth and server processing capability to be consumed. These attacks are commonly referred to as packet flooding attacks. The packet types used for the attacks have varied over time, but it is safe to say that the sophistication and distributed nature of these attacks and the sheer volume at which they are launched is increasing, making it difficult to target the source. The more common attacks involve TCP floods, ping floods, and UDP floods.

How The Attack Mitigator IPS Solution Solves The Problem

The Attack Mitigator IPS is a hardware, ASIC-based inline solution designed to block DDoS attacks while allowing good transactions to continue to flow. The product can be installed and provide immediate protection using the preconfigured protection mechanisms that are preloaded with the device. Top Layer's Non-Stop Protection approach to IPS focuses on Protection, Performance, Management, and Reliability.

DDoS attacks at best will compromise overall network performance, and at worse render an organization offline for an extended time period, resulting in lost profits and customer dissatisfaction.

DDoS attacks are now a common security concerns in the Boardroom.

Traditional security infrastructure plays into the hands of the attackers.

Protection is a key element of any solution designed to maximize mission critical Web server availability. The Attack Mitigator addresses protection in the following way:

- **Best In Class DDoS Protection** – Attacks against mission critical Internet-facing assets where there are no vulnerabilities are more prevalent now than ever before. The Attack Mitigator, using multiple patented DDoS protection mechanisms, offers the most comprehensive protection from all types of DoS and DDoS attacks.
- **Uncompromised Protection** – The latest hybrid attacks and advanced hacker evasion techniques necessitate a highly integrated multi-method approach to accurately detect and block cyber attacks. The Attack Mitigator inspects 100% of the packets and integrates many protection mechanisms, including its Deep Packet Inspection and Stateful Analysis Engines to understand application behavior and usage.
- **Continuously Stateful** – The Attack Mitigator maintains the most context (state) of any IPS device, by an order of magnitude. This is crucial for protection against slow, but debilitating attacks, ensuring high attack detection accuracy and avoiding hacker evasion techniques.

Performance is critical for an inline IPS. The key performance aspects for an inline IPS are latency, throughput, DDoS rejection rates, operation under load and scalability. The Attack Mitigator IPS 5500 delivers industry-leading performance across all the key attributes and in many cases operates at 3 – 5 times the performance levels offered by competitive products.

- **Industry Leading DDoS Rejection Rates** – Today, DDoS attacks can be launched simultaneously from computer armies of 35,000 compromised machines, delivering seemingly harmless legitimate traffic at rates approximating a gigabit per second. Only the most advanced DDoS capabilities, designed in hardware, can stop these attacks while allowing legitimate traffic to continue to flow to the intended destination. Top Layer has been at the leading edge of stopping high volume DDoS attacks for many years. The Attack Mitigator incorporates this technology in all of its IPS products and allows customers to combine traditional IPS protection features with full DDoS protection.
- **Lowest Latency Of Any IPS Device** – The Attack Mitigator is the first IPS to seamlessly integrate multiple protection mechanisms on a distributed ASIC platform. The result is that latency measurements are below 50 microseconds, even when all protection mechanisms are enabled.
- **Scaleable Performance and Capacity** – The Attack Mitigator ProtectionCluster™ provides the highest level of performance by using unique load sharing mechanisms. The ProtectionCluster™ provides a scaleable solution and since it shares state across multiple units, it provides better protection through more insight into conversations.
- **Outstanding Throughput** - It is very difficult for any security administrator to be able to characterize all of the traffic on their network with a high degree of accuracy. What is the average bandwidth? What are the peaks? Is the traffic mainly one protocol or a mix? What is the average packet size and level of new connections established every second? The Attack Mitigator has been designed to eliminate these concerns by being able to

operate in the most demanding networks with throughput of 8.8 Gbps with the ProtectionCluster™.

Performance When Under Attack – This is the one performance metric missing from most vendors datasheets. As a result of the tight integration of the protection mechanisms with the hardware architecture, datasheet performance for the Attack Mitigator is precisely that, even when under attack.

Return on Investment

Most of our customers who use the Attack Mitigator to defend against DDoS attacks tell us that the payback from their IPS investment is immediate. The following are often cited by customers as reasons for a rapid ROI:

- Eliminate mission critical server down time and therefore maximize revenue and maintain high customer satisfaction
- Blocking attacks allows for increased bandwidth availability
- Increase network performance by eliminating unwanted and malicious traffic
- Reduce operating expenses incurred by maintaining and running older, ineffective security solutions
- Allow legitimate transactions to continue to flow even in the face of the most brut force DoS attacks

Many customers tell us that even one of these reasons can result in a 100% payback in a very short time. When combined, the business case for deploying the Attack Mitigator to defend against DDoS attacks is compelling and no other IPS solution can claim this level of ROI.

Customer Success Story

An online gaming site that handles thousands of sport-related online wagers every day became a target for an increasingly disturbing trend amongst e-commerce sites. The customer received an email stating “We’ll take your network down unless \$30,000 is wired to a foreign country within a week.” Rather than pay the ransom and be labeled as a “payer”, this customer turned to Top Layer to protect them from this and any future threats. The customer stated, “The Attack Mitigator IPS has improved network reliability and availability dramatically, enabling rapid processing of online wagers and improving the bottom line, with little worry about additional attacks.”

Next Steps

To find out more about how the Attack Mitigator IPS 5500 can help protect your network, call Top Layer at 1 508-870-1300, email info@TopLayer.com or locate your local sales office at http://www.toplayer.com/content/contact_us/offices/index.jsp

Top Layer Networks, 2400 Computer Drive, Westboro, MA 01581

Phone: 508-870-1300, Fax: 508-870-9797, www.TopLayer.com