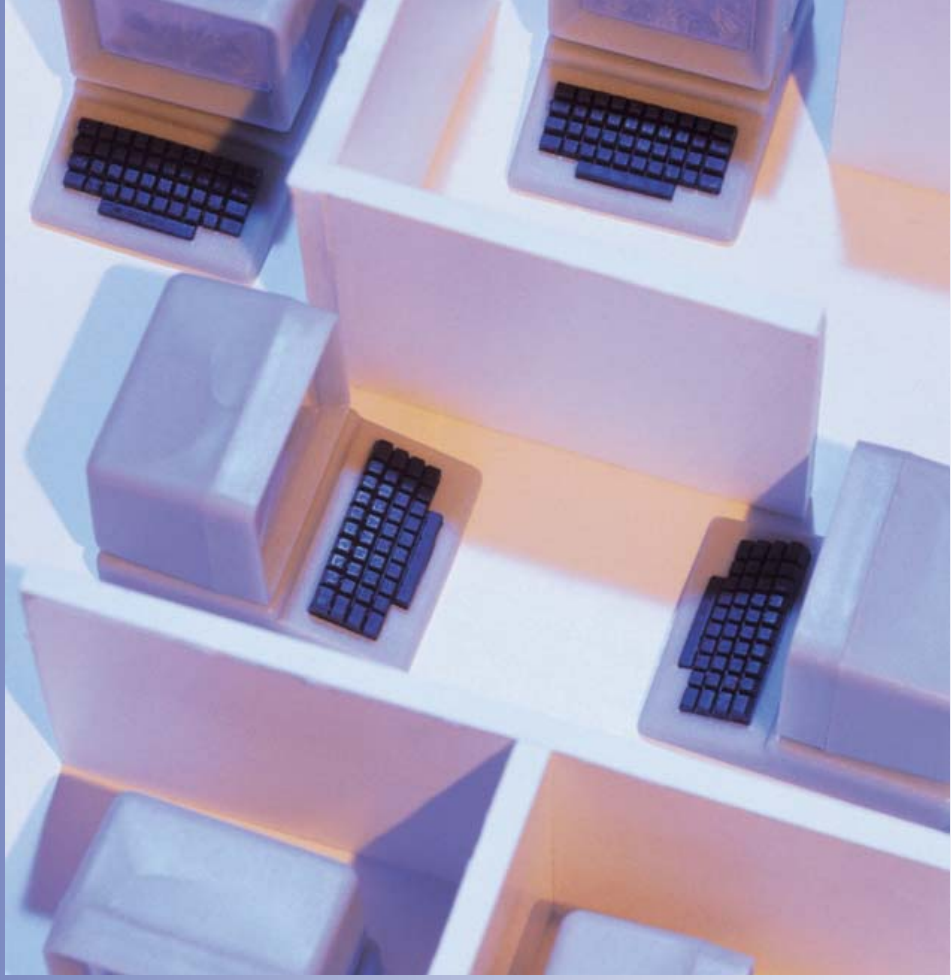


# SOLUTION BRIEF



## WEB SERVER PROTECTION SOLUTION



*perfecting the art of network security*

# Web Server Protection Solutions



## Key Trends

Organizations increasingly rely on the Internet to conduct business to drive their business strategies and increase operational effectiveness at a time when the global reach of transactions represents new opportunities for all organizations. E-Commerce web sites and partner collaboration portals enhance business opportunities and help organizations maintain real-time connectivity to their customers and partners. However, the ubiquitous nature of the Internet also creates new opportunities for cyber crime activities, which target the core infrastructure element for successful online business initiatives, the Web server.

The growth of new web sites has continued at a near-record pace despite the steady drumbeat of security threats. As businesses rely more heavily on new website infrastructure, the financial losses associated with cyber crime has scaled just as rapidly, thus requiring more advanced technologies to provide the necessary protection.

## Business Challenges

The moment you install a Web server, you've opened a window into your local network that the entire Internet can peer through. While most visitors are content to window shop, others prefer to vandalize or even force the window open and crawl inside. The results can range from the merely embarrassing, for instance the discovery one morning that your site's home page has been replaced by an obscene parody, to the damaging, for example the theft of your entire database of customer information. Another rapidly growing example of malicious behavior is blocking windows for fun or extortion purposes, each resulting in lost connectivity to customers.

Any organization using a Web server understands the importance of providing a rapid response time to customers, downtime means that the potential for lost profits is huge as well as running the risk of lost customer goodwill and trust in maintaining confidentiality.

## Understanding the Problem – Remote Exploits

Web servers provide a portal between your business and your customers and partners, so they require a more formidable and customized level of protection above and beyond what network firewalls or IDS' can provide. Firewalls are designed to allow traffic intended for the Web server to flow through to its destination with minimal scrutiny. Even next generation firewalls attempt to address the problem with poorly performing software patches and upgrades.

IDS solutions detect attacks based on known attack signatures, but are not architected for inline operation or proactive blocking of attacks. Even worse, an IDS that has been re-badged as an IPS can leave users helpless in the face of new web-specific attacks or attacks that attempt to slip through during peak usage. Code Red and Nimda are examples of worms that took advantage of Microsoft Web server vulnerabilities and inadequacies in firewalls and IDS solutions.

There are security risks that affect Web servers, the networks that host Web sites, and even innocent users of Web browsers. To ensure the success of commerce or partner portals, most businesses focus on securing the integrity of the data and the integrity of the transaction.

It is generally well known in system security and software development circles that large, complex programs contain bugs that cause security holes. Unfortunately, Web servers and web applications are large, complex programs that can (and in some cases have been proven to) contain security holes. Furthermore, the open architecture of Web servers allows arbitrary CGI scripts to be executed on the server's side of the connection in response to remote requests. Any CGI script installed at your site may contain bugs, and every such bug is a potential security hole. Many of these vulnerabilities can be remotely exploited, resulting in a compromised web site, lost business and potentially severe legal and financial ramifications due to lost or compromised data.

Finally, all organizations worry about the confidentiality of the data transmitted across the Internet. The TCP/IP protocol was not designed with security in mind; hence it is vulnerable to network eavesdropping. When confidential documents are transmitted from the Web server to the browser, or when the end-user sends private information to the server, someone may be listening in and have access to your data.

The critical areas of concern can be addressed by Intrusion Prevention System (IPS) technology. Left unprotected these Web site vulnerabilities allow unauthorized remote users to:

- Steal confidential documents not intended for their eyes.
- Execute commands on the server host machine, allowing them to modify the system.
- Gain information about the Web server's host machine that will allow them to break into the system.

## **Understanding the Problem – Denial of Service Attacks**

Along with the vulnerabilities listed above, businesses are also concerned with securing the integrity of the transaction. Cyber attacks that impact the performance and availability of the site cannot be tolerated. Distributed Denial of Service (DDoS) is an attack designed to render a computer or network incapable of providing normal services. The most common DDoS attacks will target the computer's network bandwidth or connectivity. A website DDoS attack is executed by flooding one or more of the site's web servers with so many requests that it becomes unavailable for normal use. If an innocent user makes normal page requests during a DDoS attack, the requests may fail completely, or the pages may download so slowly as to make the Website unusable. DDoS attacks typically take advantage of several computers which simultaneously launch hundreds of thousands of requests at the target Website. Connectivity attacks flood a computer with such a high volume of connection requests, that all available operating system resources are consumed and the computer can no longer process legitimate user requests (e.g., excessive HTTP Gets).

DDoS attacks are very hard to stop because of the large number of randomly distributed attacking sources, which renders conventional protection mechanisms useless. Connectivity attacks are equally devastating, as the web requests are legitimate in format, but overwhelming in volume.

## **Protecting Web Servers with Three Dimensional Protection (3DP)**

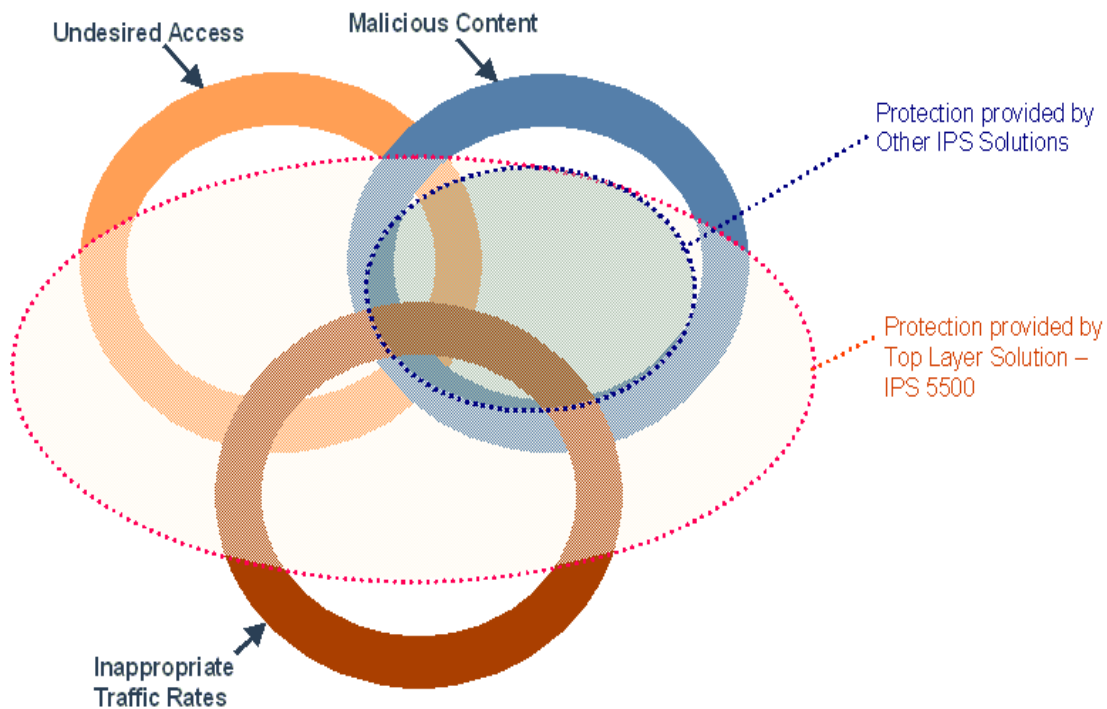
The Industry experts classify network security risks into three major threat categories:

- Malicious content in network traffic, including exploits of Microsoft vulnerabilities, worms, Spyware and other malware;
- Undesired access to networks or systems, including unauthorized or illegal access;
- Rate-based attacks on the infrastructure, such as SYN Floods, and other Denial of Service attacks.

In order to address these three major threat categories, an effective solution needs to comprise three protection mechanisms. These include:

- Content-based IPS protection;
- Stateful firewall filtering;
- And rate-based attack mitigation.

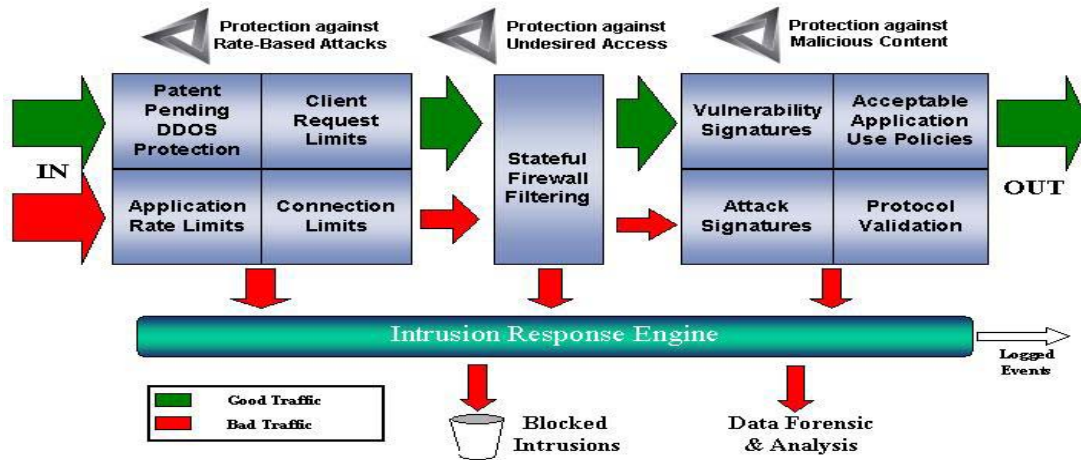
**Figure 1: Top Layer Networks' 3DP Protection**



### **The Integrated Solution: Top Layer's IPS 5500**

In order to best combat the threats posed by undesired access, malicious content, and rate-based attacks (and complex hybrid attacks that use multiple elements of these to circumvent static, one-dimensional security tools), enterprises should select and deploy a network IPS solution that addresses all three in an integrated, mutually-reinforcing fashion – as Top Layer Networks does with its “Three Dimensional Protection” approach.

Figure 2: Top Layer Networks' 3DP Architecture



## Return on Investment

Most of our customers who use the IPS 5500 to protect their web servers tell us that the payback from their IPS investment is immediate. The following are often cited by customers as reasons for a rapid ROI:

- Eliminating Web server down time and therefore maximizing revenue
- Avoid hurried patching of compromised Web servers that may cause follow-on problems because of a lack of time to properly test patches
- 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
- Allowing 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 IPS 5500 to protect mission critical web servers is compelling and no other IPS solution can claim this level of ROI.

## Customer Success Story

One customer was able to show his management the immediate benefits of deploying the IPS 5500 from both the perspective of cost and security. The IPS 5500 allowed him to significantly reduce the time and cost associated with managing and maintaining old security technologies while providing the organization with a much higher level of overall security. The net result, higher customer satisfaction from being able to conduct transactions at any time which led to higher overall revenues, at the same time reducing network operating expenditures.

IPS 5500 customers depend upon Top Layer's IPS 5500 for Protection and realize immediate benefits from the IPS 5500. Below is a sample list of customers and Web site applications.

### Sample Customers

Top 3 US bank

Leading computer reseller

Leading online advertiser

### Application

Payment system protection

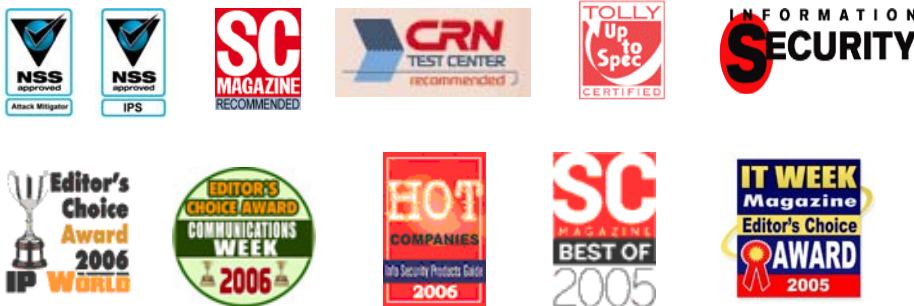
Customer ordering & support site protection

Datacenter web server farm protection

## Next Steps

To find out more about how Top Layer's award-winning IPS 5500 can help protect your network, call Top Layer at 1-508-870-1300, email [info@toplayer.com](mailto:info@toplayer.com), or locate your local sales office at [http://www.TopLayer.com/content/contact\\_us/offices/index.jsp](http://www.TopLayer.com/content/contact_us/offices/index.jsp)

*The IPS 5500 has won the most awards:*



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

Phone: 508-870-1300, Fax: 508-870-9797, <http://www.TopLayer.com/>