



The Critical Importance of Three Dimensional Protection (3DP) in an Intrusion Prevention System

Top Layer Networks, Inc.

Enterprises without a sound intrusion prevention strategy across the three threat dimensions - undesired access, malicious content, and rate-based attacks - open the door to unacceptable risks and costs, especially from hybrid attacks. Top Layer's unique Three Dimensional Protection (3DP) approach provides the most comprehensive IPS protection for clients, servers, and network infrastructure, while maximizing bandwidth for mission-critical traffic.

Table of Contents

| | |
|--|----------|
| INTRODUCTION | 3 |
| ONE APPROACH..... | 4 |
| THE INTEGRATED SOLUTION: TOP LAYER'S IPS 5500 | 5 |
| PROTECTING AGAINST UNDESIREED ACCESS WITH STATEFUL FIREWALL TECHNOLOGY .. | 6 |
| STOPPING MALICIOUS CONTENT | 6 |
| DENYING DISTRIBUTED DENIAL OF SERVICE (DDoS) AND OTHER RATE-BASED ATTACKS | 7 |
| THE TOP LAYER DELIVERY APPROACH | 8 |
| WHY TOP LAYER?..... | 9 |

Introduction

When organizations first began experiencing the insecurity of networking, they placed barriers to entry on their networks – firewalls. Firewalls completely bar those entrances through which no traffic should be allowed to pass. In addition, they enforce access control over the ports they leave open, so that only traffic from desired IP addresses gets through. For these reasons, firewalls have proven effective against many types of intrusions. Of course, organizations can't use a firewall to block everything from passing through, as the organization would not remain in business for very long. We have learned that attackers will learn to exploit any entry left open. Because they attack in multiple ways against which the firewall - with its access control emphasis - are not built to protect, hybrid attacks, Denial-of-Service (DoS) attacks, application level attacks and protocol anomalies get through most firewall deployments.

Many companies also employ network intrusion detection systems, which inspect the network traffic and report their findings to log files and databases. IDS tools have been instrumental in providing forensics about attacks and in determining over time what areas of the network become compromised. While IDSs enable record-keeping, an alarm function, and eventual analysis and remediation, they do not stop or mitigate damage from malicious attacks in real time.

An increasing number of organizations, therefore, are using network intrusion prevention systems in addition to other network security measures to mitigate information security risks. This is a generally positive development, as inline intrusion prevention systems with deep packet inspection capabilities are critical to protecting corporate networks. However, even among those forward-looking companies that have adopted IPS, too many are doing so in an incomplete fashion, focusing only on certain risks that have top-of-mind currency, thereby exposing them to serious varieties of risks they had not considered.

Enterprises must have a sound intrusion prevention strategy across the three threat dimensions: **Undesired access**, wherein intruders gain access to such invaluable assets as proprietary intellectual property or customer identity/credit information, as we have seen in several high profile financial services attacks over the last eighteen months; **malicious content**, including viruses, spyware and other types, which can cause troubles that range from mild annoyances to cost-prohibitive extended network downtime and loss of stored material; and **rate-based attacks** which intentionally overload computers or networks with garbage traffic for the purpose of preventing legitimate traffic from reaching its destination, resulting in lost revenue and brand

damage for the attacked. A three-dimensional approach which addresses all three of these attack techniques is critical to prevent being hurt by complex hybrid attacks that use multiple techniques to quickly spread malicious executables, techniques that can beat traditional security point measures.

Some of the most damaging attacks ever orchestrated, such as Nimda, which infected over 2.2 million PCs and servers in 24 hours after its release in September 2001 (Computer Economics), causing an estimated \$530M or more in damages because of downtime and clean-up costs, have been hybrids. Code Red, even more significantly, was responsible for an estimated \$2.6 billion of damage. Other well-known cases of intelligent hybrid attacks that traditional security approaches were unable to prevent include SQL Slammer (which exploited a vulnerability and caused a DoS condition), and MyDoom (which contained elements of a virus, a DoS attack, and a backdoor Trojan).

More recently, the Zotob worm and its variants took advantage of a vulnerability in Microsoft's plug-and-play architecture by gaining undesired access to Windows desktops and servers through Port 445. Once the worm found a vulnerable system, it made an FTP connection to download a malicious content payload from an attacking computer. The worm also modified the host's files to prevent access to Web sites, including many antivirus and security sites. Finally, it created a backdoor that allowed for full remote command and control, adding to the potential for costly exploits.

One Approach

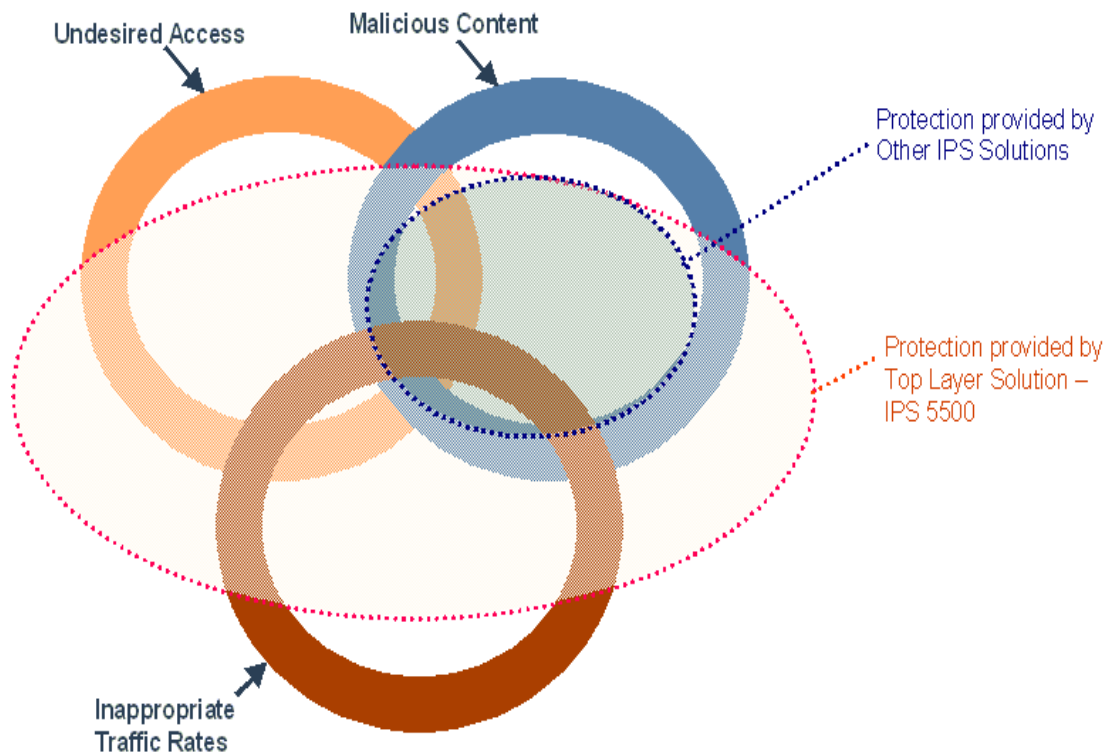
Such high-profile attacks have imprinted themselves in the enterprise's security worldview, and for good reason. According to Gartner's "Hype Cycle for Cyberthreats, 2005", "the majority of new attacks will use hybrid techniques." These hybrid attacks are proving themselves increasingly capable of propagating across an inadequately-protected network infrastructure. What typical security administrators consider as risks to protect against are what have been the traditional threats, usually malicious content. This is not all there is to worry about, however. Mass attacks such as worms and viruses – and universally visible, time consuming, potentially dangerous annoyances like spyware - get headlines because of widespread enterprise and consumer exposure.

Targeted attacks, which aim to achieve a specific negative impact against specific enterprises and are often executed through such means as undesired access to proprietary systems/files and SYN floods, which receive very little publicity because enterprises do not want to expose the nature and extent of the damage an attack may have caused, are more malicious and can be more harmful and cost even more money to redress. Enterprises, when they address only part of

the threat spectrum illustrated below, leave themselves open to these sophisticated, targeted attacks.

The challenge that the enterprise has faced is that employing point solutions to address these threat varieties across multiple fronts has proven costly, ineffective, difficult to manage, and reactive rather than proactive, remediating at great cost instead of preventing the damage from occurring.

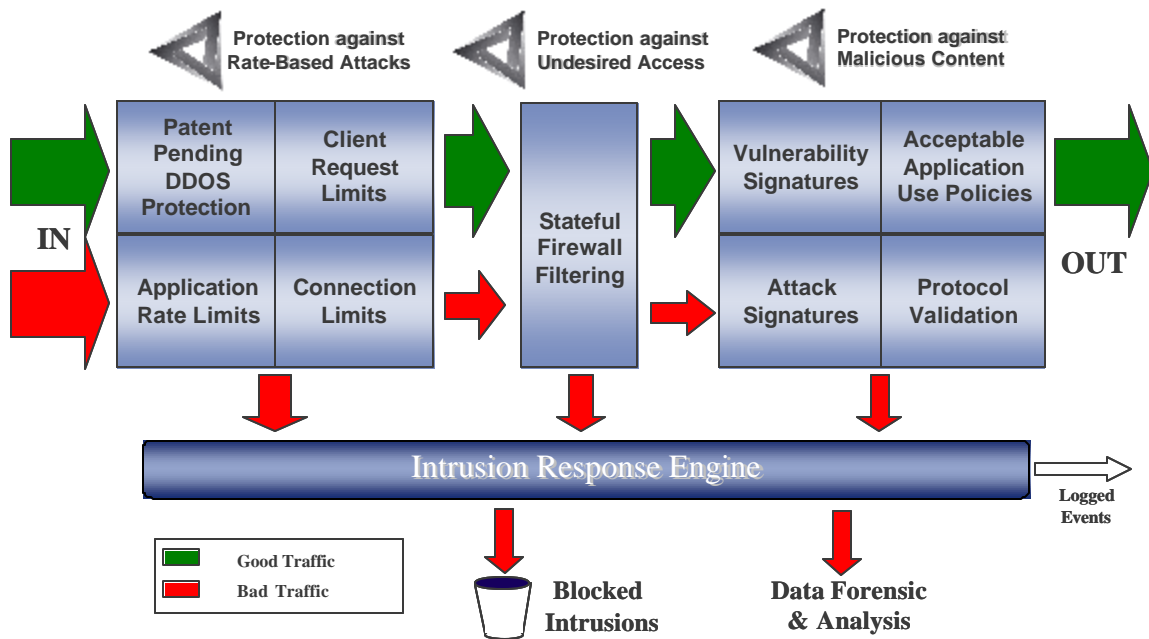
Figure 1: The Three Dimensions of Threat Activity



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



Protecting Against Undesired Access with Stateful Firewall Technology

In the first area of defense, Top Layer addresses the potential for undesired network and application access by adopting a stateful firewall stance. In the IPS 5500, Top Layer provides IP fragment abuse protection, Layer 2 and Layer 3 filtering, and stateful firewall filtering. Administrators can easily configure the IPS 5500's firewall filters to control who gets access to which servers and applications connected to the network, thereby preventing a malicious user from gaining entry to steal or destroy valuable intellectual property. Top Layer's stateful firewall approach separates it from IPS competitors, who do not have this level of protection from undesired access throughout a network available.

Stopping Malicious Content

Top Layer protects against malicious content with a multi-pronged approach: Acceptable application use policies, protocol validation, attack/vulnerability signatures, antivirus signatures, and spyware protection modules. Top Layer stops traffic that does not conform to an enterprise's application use rule set, which is easily-configurable. Network transactions that pass through this initial gate are then sent through a protocol anomaly detection engine to determine whether the packets meet standard protocol implementations, an approach that defines what is good, allowable traffic.

Because the IPS 5500 maintains more state, or context, than other IPS devices, it is better able to eliminate false positives by drawing more complex conclusions and detecting more subtle anomalies. Transactions that do not meet the acceptable protocol specifications (such as those containing buffer overflow attacks) are blocked and sent to a sophisticated identification and reporting engine for real-time reporting.

However, although this provides a powerful technique to detect and block many attacks, there are attacks that exhibit themselves as perfectly legitimate network traffic (such as some viruses, application logic attacks and reconnaissance methods). It is therefore important that seemingly legitimate traffic is subject to other protection mechanisms.

Packets that contain a file that may carry a malicious payload, such as a ZIP, JPEG, XML, or Microsoft Excel or Word files, are sent for further analysis of the body of the payload and matched against known exploits through attack signature pattern matching. This deep packet inspection and signature matching is performed without materially affecting network performance.

Denying Distributed Denial of Service (DDoS) and other Rate-Based Attacks

With the IPS 5500 and its patent-pending algorithms, Top Layer Networks builds upon its industry leadership position in protecting against network- and application-level flood attacks and other attacks using inappropriate rates. The IPS 5500 does so by applying DoS/DDoS mitigation techniques, policy-based rate limits, and other resource-consumption limits.

The IPS 5500 uses purpose-built flexible programmable hardware to maximize good, or legitimate, network transactions (by blocking rate-based attacks) and maintain a real-time threat-level assessment of 2 million IP addresses (increasing to 5 million when an attack is detected). In addition, it provides advanced contextual information about traffic flowing through the device and distinguishes legitimate traffic from seemingly legitimate DDoS attack traffic.

The Top Layer Delivery Approach

Figure 3: Top Layer's IPS Solution



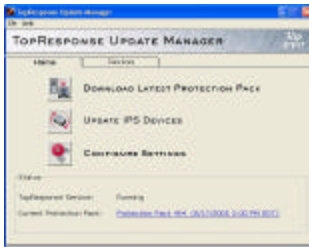
Central Management System

- Central Console for Multi-unit IPS Management
- Automatic Real-time Event Correlation
- Detailed and Trend Reporting



Network IPS Appliance

- Enforcement Point for Integrated Protection
- Full Product Family for Flexible Deployments
- Extensible Architecture for Investment Protection



Research and Automated Updates

- Subscription Update and Advisory Service
- Microsoft Updates
- Spyware Sites and Internet Topology Information

Top Layer has implemented its IPS 5500 solution on a purpose-built ASIC-based platform for high performance and reliability, resulting in the most effective holistic IPS solution architecture. When combined with the SecureCommand+ central management system and the TopResponse Automated Update Service, the IPS 5500 is easy to manage and always up-to-date as it delivers industry-leading Three Dimensional Protection.

Why Top Layer?

Top Layer's third generation intrusion prevention solution is widely acclaimed as the world's most powerful IPS product, combining top protection capabilities with unparalleled performance. The IPS 5500 has received the most awards in recognition. The IPS 5500 remains the only IPS product to receive dual NSS-approved awards in extensive lab tests among 23 IPS products. Also in 2005 the Top Layer IPS 5500 was named the winning IPS by *Information Security Magazine*, and received a five star rating from *SC Magazine* in its independent test of 12 leading IPS product. Other knowledgeable evaluators like The Tolly Group, *CRN*, *eWeek*, *IP World*, *Hosting Week*, and *Service Provider Week* have all approved and recommended the IPS 5500.

Complex attacks are becoming the weapon of choice among those who seek to hurt targeted enterprises and profit through these attacks. Most products in the IPS marketplace seek to detect and protect against facets of these attacks, but do not protect effectively across the threat spectrum of Undesired Access, Malicious Content, and Rate-Based Attack, as Top Layer's IPS 5500 does.

Even the best security, however, lacks meaning in the real world if network performance is crippled. Security cannot make it impossible to do business. The Top Layer IPS 5500 has the highest performance of any IPS product, with all models introducing less than 100 microseconds of network latency. The IPS 5500's hardware architecture makes it, according to the NSS 2005 tests, the only product that scales to multi-gigabit networks that will pass 100% of legitimate transactions, even while under a sustained attack.

Top Layer's IPS 5500 comes with a robust central management system, SecureCommand+ Centralized Management, that provides multi-unit configuration and policy management - which includes automatic correlation of IPS events, security events, and detailed reporting - Security Event Management capabilities, and integration with a wide variety of third party management tools and reports including Arcsight, CA, eIQ, HP Openview, IBM Tivoli, Network Intelligence, Open Service, Symantec, and others.

To enable Top Layer IPS 5500 Customers to achieve the highest levels of protection against newly discovered network-based threats, the TopResponse Research and Update service closely follows research and discoveries in vulnerability communities, hacker underground, software vendors, and media; interprets and assesses threat levels of newly discovered threats, vulnerabilities or incidents; and advises customers regarding the presence of these threats,

vulnerabilities or exploits, while automatically updating the IPS 5500 product to provide optimum protection against them.

Top Layer's IPS 5500 delivers the best defense against multi-faceted threats without sacrificing performance, and it can be deployed, managed, and updated with relative ease. Enterprises that are concerned about managing risk effectively and efficiently across the spectrum of potential attacks should seek out Three Dimensional Protection (3DP).

