

SOLUTION BRIEF



CORPORATE ENTERPRISE SOLUTION

**Top
Layer**[™]

perfecting the art of network security

Contents

Top Layer Networks Attack Mitigator IPS 5500:.....	2
The Only True Enterprise-Class IPS.....	2
The Need for Speed.....	5
Slow and Steady.....	6
Investigating the Attack Mitigator IPS 5500	7
Best In Class for the Best Protection	8
Taking Packet Inspection Deeper	8
Limiting False Alarms	9
Performance Parameters	10
Easy Does It	11
Rapid Return on Investment	12

Top Layer Networks Attack Mitigator IPS 5500: The Only True Enterprise-Class IPS

As the cyber attacks relentlessly targeting the enterprise become more complex and dangerous, the tools used to detect and deter them must become increasingly sophisticated. The latest and best line of defense against cyber criminals is the Attack Mitigator™ IPS 5500 from Top Layer Networks, the only intrusion prevention system (IPS) engineered to overcome the specific security challenges of today's enterprise networks.

As security and IT managers know firsthand, each successive wave of Trojans, viruses, worms, and Distributed Denial of Service (DDoS) attacks is more virulent than its predecessor. What's more, the very nature of cyber crime is changing: Web-savvy professional criminals are adding extortion, protection rackets and theft to the extensive catalog of Internet threats. Typically, this new class of cyber criminals builds or leases a botnet, a network of robot PCs used to launch DDoS attacks. A simple demonstration of force is usually all that's needed to convince the victim to pay up. Such DDoS attacks can even be used to enable a potential break-in, where a small Trojan is masked by huge volumes of traffic and allows an outsider to get access to internal resources.

Meanwhile, security professionals still have to defend their companies against equally lethal attacks from "amateur" hackers. Their motives may not be clear, but their prowess is: So-called amateurs are responsible for Nimda, Code Red, Love Bug, MyDoom, Netsky, and SoBig—to name only a few of their more memorable contributions to online chaos. The sixth and final version of SoBig, for example, browned out e-mail servers worldwide. According to AOL, at its peak SoBigF was directly or indirectly responsible for three out of four e-mails on its network.

The world has already seen how ineffective firewalls and Intrusion Detection Systems (IDSs) are against these attacks, which penetrate security perimeters seemingly at will, speeding past firewalls and being detected by IDSs hours (or longer) later. According to security experts, however, an attack needs as little as six seconds to find and infiltrate an unprotected or inadequately protected system ("DDoS Threatens Financial Institutions—Get Prepared," white paper by Reymann Group).

In contrast, a true inline IPS like the IPS 5500, can identify and

neutralize incursions before they can reach a single server or desktop—in real time.

The right IPS can be equally adept at protecting enterprise organizations against threats from within. Security experts have long known that disgruntled employees can do far more damage than outsiders can. But what about perfectly happy employees, field engineers, consultants, partners, contractors, and visitors? Any of these laptop users can be unknowingly infected by some form of malware. When they plug into the corporate network, that malicious code goes to work. In the case of a DDoS, it can hijack thousands of desktops and servers, lurking invisibly in the heart of these machines until it's time to use them to launch a full-blown attack against a third party.

That type of hack is doubly dangerous in light of recent interpretations of tort law. If it's determined that proper precautions, like selecting an IPS, were not taken, companies whose networks are unwittingly and unwillingly used as a platform for a DDoS attack can now be considered as responsible as the cyber criminals who wrote and/or released the malicious code in the first place. And as "perpetrators," they can be—and have been—sued for damages ("Accounting for Internet Malice," a proprietary report by Top Layer).

At this point, it's virtually impossible to imagine a company, large or small, whose success isn't riding on its enterprise network. Given the inextricable interdependence of technology and business, any company that doesn't deploy an IPS is inviting trouble. Financial exposure, particularly for companies involved in e-commerce or online transaction processing, is a critical concern—but it's only one of many.

It's equally essential, in light of today's regulatory environment, for enterprise organizations to safeguard confidential data and servers. Ensuring the availability of these networked resources is another aspect of regulatory compliance. The Graham Leach Bliley Act (GLBA), for instance, requires financial firms to take proactive steps to ensure customer information is secure. Similarly, the Health Insurance Portability and Accountability Act (HIPAA) mandates that healthcare institutions must maintain the confidentiality, integrity, and availability of sensitive data. This includes patient health information (PHI), but also may cover payroll and employee records, business-strategy plans, and legal documents (such as pending lawsuits).

The Sarbanes Oxley (SOX) Act, which was enacted in the wake of

various high-profile financial scandals, legislates fiscal oversight of publicly held companies. SOX section 404 outlines a broad range of security components necessary for compliance. These include access control, data integrity, and system authentication, proper auditing and monitoring.

Top Layer's IPS 5500 helps companies establish single-platform regulatory compliance. By furnishing best-of-breed protection against DDoS attacks and remote exploits, it guarantees the security, confidentiality, and integrity of sensitive information. The IPS 5500 also detects and defeats an exhaustive array of cyber threats, including "invisible" malware and spyware that uses employee laptops to infect the enterprise.

In addition, the IPS 5500 contributes directly and indirectly to company profitability. It helps eliminate security-related downtime and lost opportunities, as well as the collateral damage that accompanies a major exploit. It prevents hackers from taking down corporate e-mail servers, cutting organizations off from partners, vendors, and customers. Most importantly, it enables a company to go about its business regardless of what sorts of attacks are leveled against it.

IPS or IDS: The Name Game

Finding the best *inline* IPS to safeguard an enterprise should be a relatively simple task, composed chiefly of comparing key parameters like performance, latency, scalability, reliability, and depth of protection. Unfortunately, the IPS market is already crowded with competitors, not all of whom are what they claim to be. Some IDS manufacturers, for instance, are modifying their *offline* products' software and selling them as inline IPSs. Thus, the first task facing security administrators and enterprise IT managers is separating the "real" IPSs from the "rebadged" IDSs.

That's more than a matter of semantics. A true IPS like the IPS 5500 is an inline device; it monitors and processes live traffic, just like a firewall or a router. An IDS, in contrast, works offline, analyzing traffic that's split off (mirrored) from the live packet stream. Attempts to use IDS in an online manner have historically proven to be a disaster for enterprises since they have quickly caused massive bottlenecks leading to poor network performance and application availability. In addition, they tend to generate reams of false positives, leaving administrators unsure of which signatures to enable.

The Need for Speed

Since it works with live traffic, an IPS is inherently a very-high-performance security appliance. It must instantly identify and deflect malicious packets—worms, viruses, DDoS attacks, application anomalies, and other security threats. To accomplish this, an IPS must employ a very streamlined decision-making process. Essentially, it decides if a packet is “good” or “bad.” The former are shunted onto the network; the latter are checked against predefined policies.

Clearly, a critical consideration when evaluating an enterprise IPS is performance, which ensures that IT managers don't simply trade one problem (security) for another (congestion). The IPS 5500's raw throughput is 4.4 Gbps, which can be doubled with the addition of special module. As a general rule of thumb, an IPS should be able to keep pace with a 10-Gbps link that's utilized at 80 percent to 90 percent capacity. Anything less, and the IPS is going to be a bottleneck. That plays havoc with delay-sensitive traffic like Voice over IP (VoIP) and also can cause dropped TCP/IP sessions and retransmissions.

There's something else to bear in mind: Despite their complex technologies and sophisticated algorithms, all inline security devices have a simple purpose: let legitimate traffic access the network and block bad packets. Once a bottlenecked IPS begins preventing legitimate packets from reaching their destinations, it's no longer a security device.

The other key IPS performance parameter is device latency. The IPS 5500 needs less than 50 *microseconds* to perform deep packet inspection. To put that number in perspective, an Ethernet network carrying VoIP traffic must converge around a failed device in less than 50 *milliseconds*; anything slower, and the quality of the call begins to degrade. The AM maintains this microsecond latency even while under heavy attack, enabling it to attain true switchlike performance. Most other IPSs claim microsecond or even millisecond latency, but that is typically under clean traffic conditions, not while under attack.

An IPS's high throughput and low latency help a company achieve its goals. Bottlenecks waste business cycles. They slow application performance and degrade network response time. All of these “microdelays” chip away at a company's ability to make the most efficient use of its information, risky behavior in a market that's

characterized by cutthroat competition and see-through profit margins.

Similarly, a sluggish IPS can suppress a Web or database server's ability to respond rapidly to customer requests. Internet consumers are accustomed to instant gratification; seven seconds is typically quoted as the length of time they'll wait for what they want. After that, they'll simply click over to a competitor's speedier site.

Slow and Steady

Since an IDS works offline, it doesn't have the same need for speed. Essentially, an IDS performs simple pattern matching against a very large database of exploit signatures. This is a time-consuming, CPU-intensive task. Unlike an IPS, which must make instant decisions, an IDS analyzes captured data and then generates a variety of reports that reveal attempted incursions, port scans, and potential security flaws.

That painstaking analyses are exactly why an IDS shouldn't be used inline. Think of it this way: An IDS knows what it knows. The only way to extend that knowledge is to add signatures to its database, and that can only be done after an attack. In addition, while most IDS-based IPSs claim a large database of signatures, only a very small subset can actually be used inline due to performance considerations. This gives the administrator the monumental task of picking and choosing a small subset of signatures to protect the entire enterprise. Signatures also are an inefficient primary defense mechanism since it takes time for security experts to create and test signatures for new threats. Given the speed at which viruses and worms jump from device to device, time is the one thing companies don't have.

Any company that unwittingly deploys a rebadged IDS is particularly vulnerable during the interval between the appearance of a new threat and the publishing of a new attack signature. The same goes for so-called copycat viruses, which resemble but are not identical to the original attack, and zero-day exploits. A rebadged IDS offers no protection against either.

It should be understood that this is not a criticism of IDSs in general. When they're deployed properly, these powerful security tools provide reams of valuable data to assist in tweaking security policies well after an attack has transpired. When vendors add new code to these devices and pass them off as IPSs, everyone suffers.

Investigating the Attack Mitigator IPS 5500

The Top Layer Attack Mitigator IPS 5500 is an ASIC-based inline solution that blocks network- and application-layer attacks. As Top Layer's second-generation IPS, the IPS 5500 also benefits from insights and experience gained from the first-generation product.

By using ASICs and FPGAs, Top Layer is architecturally committed to delivering the performance demanded on today's 1-Gbps and 10-Gbps enterprises, along with a high degree of programmability. General-purpose CPUs don't have the horsepower to do protocol validation, session reassembly, and deep packet inspection at high speeds. Employing them would represent an unacceptable compromise, trading off speed for stability.

As noted, an enterprise-class IPS should operate at or close to full wire speed. Further, those numbers should be clearly indicated on a product's spec sheet. Not all vendors publish real-world performance figures, which should be a tip-off that the IPS in question is a bottleneck in the making under any sort of loads or even with the smallest attacks. What's more, if performance falls off sharply when an IPS is under attack, it's a good bet that it isn't a true IPS in the first place.

Top Layer doesn't just disclose all stats on its spec sheets. It firmly believes that no other IPS appliance out there can touch the IPS 5500. Its performance figures aren't just theoretical maximums; they represent validated performance based on real-world traffic conditions and attack scenarios.

For example, the IPS 5500 is the *only* security appliance that can block incoming DDoS attacks while still allowing business-critical traffic to flow unimpeded. As noted, the reverse is also true: The IPS 5500 prevents hijacked network resources from being used to launch DDoS attacks against other organizations. Equally impressive, it gets these jobs done in real time. In fact, the IPS 5500 delivers the most extensive safeguards against all types of DoS and DDoS attacks. It's equally effective against hybrid attacks, picking out a single intruder while under a heavy load or while exploits are hidden in DDoS traffic.

DDoS protection is particularly important, since this type of incursion is growing more prevalent—with good reason. While it once took a modicum of programming talent to write the code for a distributed attack, would-be hackers can now download DDoS development kits

and detailed instructions. Further, the IPS 5500's powerful inline protection eliminates the need to deploy a separate DoS/DDoS solution to enhance firewalls or IDS/IPS solutions.

Best In Class for the Best Protection

Detecting and defeating DDoS attempts is just one example of the type of protection that only the IPS 5500 offers. Advanced protocol validation is another; this enables it to defend against zero-day exploits, which take advantage of unknown or unresolved vulnerabilities within applications themselves. Deep packet inspection and stateful analysis, meanwhile, make sure that cyber attacks can't be delivered in separate sessions, a favorite ploy that hackers use to outwit a firewall or an intrusion detection system. Even if these security devices could uncover these attacks, the bottleneck that would be created as they churn through packets would, ultimately, have the same effect as the attack: preventing valid user traffic from reaching its target.

Simply said, the IPS 5500 offers best-in-class protection against the types of attacks that security officers and IT managers face every day: undesired access, content- and rate-based attacks (including malformed packets), and well-known exploits such as Blaster, SQL Slammer, and many others.

That should not come as a surprise, since the IPS 5500 is the only 21st century security appliance built from the ground up to safeguard companies against 21st century cyber threats. That helps explain why the IPS 5500 is the *only* device to receive National Security Strategy Lab (NSS) approval as both an IPS and a DDoS solution in the recently concluded 2005 NSS Lab test. Others vendor claim both types of protection; however, the reality is only Top Layer has competitive industry validation of these claims.

Taking Packet Inspection Deeper

Accurately detecting and blocking the latest hybrid attacks and advanced hacker techniques necessitate a highly integrated multi-staged approach. The IPS 5500 inspects 100 percent of the packets it receives and integrates protection mechanisms like its Deep Packet Inspection and Stateful Analysis Engines to understand application behavior and usage across the entire session. While other vendors claim this level of inspection, they often can only perform this level of inspection part-time or when deployed offline to monitor. If these

mechanisms are actually active, legitimate traffic can be curtailed dramatically.

The most immediate benefit of this uncompromising approach to packet inspection is that IPS 5500 implements two-pass protection, which is twice as effective at discovering hidden threats. For starters, the IPS 5500's Deep Packet Inspection peers into every packet, quickly identifying and discarding any anomalous ones (even fragmented packets are reordered and reassembled with microsecond delay). Then, Top Layer's Advanced Protocol Validation Modules inspect every packet to determine if the stream that makes up a particular transaction complies with permitted protocol usage. Evaluating the entire stream, rather than just the individual packets, enables IPS 5500 to determine if any viruses or Trojans have been hidden across a number of packets, ready to be reassembled and launched once that stream gains access to the network.

Since they review application behavior in context, the IPS 5500's Advanced Protocol Validation Modules provide effective protection against zero-day attacks and unknown exploits. Both these incursions take advantage of recently discovered or unknown application vulnerabilities to launch attacks against enterprise resources. But to the IPS 5500, there are virtually no unknown application vulnerabilities. Similarly, it has recognized and moved to neutralize zero-day attacks long before vendors announce their existence. Even after vulnerabilities are announced, Top Layer provides prompt advisories and updates to customers as part of its Top Response service. Often, the advisories reveal that the IPS 5500 has been protecting customers all along, without requiring any updates! Once again, other vendors claim zero-day protection through advanced mechanisms that really boil down to signatures and signature updates, leaving customers exposed for lengthy periods.

Limiting False Alarms

IPSs that rely primarily on signatures are notorious for generating false positives. Since each of these inaccurate responses must be evaluated by security or IT personnel, they pull employees away from other responsibilities. At a time when many if not most IT and security departments are operating with a skeleton crew, false positives are more than annoying: They slow down or make it impossible to complete mission-critical tasks. The IPS 5500's Advanced Protocol Validation Modules virtually eliminate false positives. By doing its job accurately, IPS 5500 helps networking staff do their jobs as well.

What's more, given the IPS 5500's unprecedented speed, all of these safeguards can be invoked without any worries about degrading enterprise performance. That's a win-win situation for security and IT administrators; they get an unmatched level of protection at full enterprise speed.

Many attackers gain access to critical resources via compromised or firewalls. This is hardly surprising, since enterprise firewalls are difficult to configure correctly and unforgiving of mistakes. Even a seemingly small slip-up, if undetected, can transform a firewall into an open doorway to the enterprise.

Top Layer's tightly integrated Advanced Stateful Firewall Filters serve as a much-needed backup to misconfigured firewalls. And unlike their standalone counterparts, the IPS 5500's Stateful Firewall is a snap to set up.

In addition, the IPS 5500 maintains an order of magnitude more state than any other IPS. Continuous stateful operation is the only way to protect dynamic application environments, such as VoIP and file transfer protocol (FTP). This capability also is a crucial safeguard against slow but debilitating attacks. Further, it helps ensure highly accurate attack detection and uncovers evasive techniques used by hackers.

Performance Parameters

The real test of IPS performance comes under duress in a production network. The IPS 5500's abilities are unmatched across all key attributes—latency, throughput, DDoS rejection, operation under load, and scalability. In many cases the Top Layer IPS 5500 delivers three to five times the performance achieved by competitors:

- The Attack Mitigator IPS 5500 is the first IPS to seamlessly integrate multiple protection mechanisms on a distributed ASIC platform. The result: latency below 50 microseconds with all protection mechanisms enabled.
- Top Layer's IPS ProtectionCluster™ not only increases capacity but also provides better protection through advanced state sharing and awareness.

- It's very difficult for security administrators to characterize network traffic with any degree of accuracy. Average and peak bandwidth? Single protocol or mix? Typical packet size and average number of new connections established every second? The IPS 5500 eliminates these concerns. Even on the most demanding networks, it delivers a steady 8.8 Gbps (with the ProtectionCluster implemented).
- DDoS attacks can be launched from 35,000 compromised machines, all of which deliver seemingly harmless traffic at nearly 1 Gbps. Only the most advanced hardware-based capabilities can stop these attacks from taking out e-commerce sites, e-mail servers, Domain Name System (DNS) servers, and VoIP providers—while allowing legitimate traffic to continue flowing. Top Layer has long been a leader when it comes to stopping high-volume DDoS attacks. IPS 5500 incorporates this proven technology, allowing customers to combine traditional IPS protection features with full DDoS protection.
- Performance under load is the one performance metric missing from most vendors' datasheets—for good reason. Not only is it available on the IPS 5500's spec sheet, the performance cited is what security and IT managers can expect when the Top Layer IPS 5500 is deployed in live networks, handling small packets, and even under attack.

Easy Does It

The Top Layer IPS 5500 can be set up in minutes using shrink-wrapped, yet custom, configurations that provide immediate protection as well as offering meaningful and actionable reporting.

Deploying the IPS 5500 typically requires no changes to the network topology. Once the IPS 5500 is installed, which takes only a few minutes, security administrators can select from several predefined Protection Configurations with the click of a mouse. Unlike competitive products that claim to have broad protection capabilities but only enable a small subset for fear of generating false positives or slowing their devices to a crawl thereby causing major bottlenecks, the IPS 5500 can be safely set to block all attacks.

The IPS 5500 is the only enterprise-class IPS that lets IT managers configure protection profiles for up to 64 departments or assets. Each also can have unique protection policies. In addition, special security

reports can be generated easily to give users meaningful protection information.

The IPS 5500's SecureCommand+™ Centralized Threat Management System, which employs Top Layer's unique Rapid Threat Recognition and Response Engine, reacts immediately to distributed and dynamic security threats using the industry's first Centralized Management and Security Event Correlation solution.

Top Layer's IPS 5500 can easily be deployed and managed in a High Availability Configuration that ensures ongoing protection in the event of a system failure or power loss. In addition, the IPS 5500 can handle asymmetric traffic without any performance degradation or changes to the routing infrastructure.

Attack Mitigator IPS 5500 has been built with long life in mind. There are no rotating storage media and no chip-mounted cooling fans. The IPS 5500 has redundant hot-swappable power supplies and fan trays.

Top Layer's TopResponse™ Service is key to providing customers with immediate protection against newly discovered vulnerabilities. The service draws upon the security expertise of Top Layer's Vulnerability Research Team, Network Security Research Team, Security Engineering Team, and Technical Research Team. In addition, Top Layer maintains relationships with a number of partners who typically see new attack types before they become widespread, allowing the team to provide better protection earlier.

Rapid Return on Investment

Most of Top Layer's Attack Mitigator IPS 5500 customers indicate that they see rapid ROI, sometimes reaching 100 percent in a very short time. No other IPS can claim this sort of ROI.

Among the more common reasons customers offer to explain their quick recoup:

- The IPS 5500 automatically blocks attacks, allowing the security team to adequately test patches before deployment.
- The ISP eliminates server downtime, thus maximizing revenue and maintaining high customer satisfaction.
- Blocked attacks ensure that more bandwidth is available.

Similarly, eliminating unwanted and malicious traffic improves network performance.

- Legitimate transactions continue to flow even in the face of brute-force DDoS 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