



Double NSS Approved

## 2005 NSS Test Report For The Attack Mitigator IPS 5500

*The Only IPS to Ever Receive a Coveted Double NSS Approved Award in a Single Test*

This briefing document summarizes the 2005 NSS Group Test Results for Top Layer's flagship Gigabit IPS product, the Attack Mitigator IPS 5500.

As more vendors market their products as Intrusion Prevention Systems ("IPS"), there are few comprehensive product evaluation methodologies that focus on the key attributes necessary for a true IPS product. NSS has become a leading authority for developing the most comprehensive test suite for IPS products. NSS conducted its first IPS test on the first generation IPS products in 2003. The 2005 test report has taken this IPS evaluation process to a new level and is highly regarded by organizations looking to purchase an IPS solution in 2005 as a significant influence on their purchasing decision.

### Test Overview

IPS products have matured significantly since NSS conducted its first test in 2003. This second and most comprehensive IPS group test to date pitted the newest, most advanced IPS products available in the market today against each other. The Attack Mitigator IPS 5500, Top Layer's flagship IPS product, was subjected to a barrage of over 1,600 individual tests (compared to 750 in the 2003 NSS test).

This test evaluated Performance, Reliability, Security Effectiveness, and Usability of the IPS products. NSS deems an IPS product "NSS Approved" if the IPS performed exceptionally well and NSS are confident in their recommendation of the product to others.

Top Layer's Attack Mitigator IPS 5500 achieved a standard never seen before for any IPS product – to be awarded a coveted **double "NSS Approved" sticker**. This accolade was awarded in recognition of the fact that the Attack Mitigator IPS is the first, and only in-line IPS product to successfully integrate multi-gigabit protection for both content-based and rate-based attacks while never blocking legitimate traffic and providing true "switch-like" latency.

It is widely regarded by industry experts that this updated IPS test methodology will become the *de facto* standard test for in-line IPS devices and the "NSS Approved" logo will be an essential requirement for organizations that purchase these products. This year, Top Layer's new Attack Mitigator IPS 5500 achieved a

standard never achieved before – to be awarded a double “NSS Approved” sticker. This accolade was awarded in recognition of the fact that the Attack Mitigator IPS is the first, and only in-line IPS product to successfully integrate multi-gigabit protection for both content-based and rate-based attacks while never blocking legitimate traffic and performing at the lowest latency levels ever seen in an IPS product.

The NSS IPS test methodology measures the effectiveness of the IPS against all of the attributes that are necessary for this network device to provide protection against cyber attacks, with a particular emphasis on:

- **In-Line Operation** – only by operating in-line can an IPS device perform true protection, by discarding all malicious packets immediately
- **Reliability and Availability** – an extremely low failure rate is very important in order to maximize up-time
- **Resilience** – an IPS needs to offer High Availability to ensure it does not become a single point of failure in the network
- **Low latency** – it is essential that the IPS has a minimal effect on the overall network performance, meaning the device should offer latency as close as possible as a layer 2/3 device, like a switch
- **High Performance** – packet processing rates must be at the rated speed of the device under real-life traffic conditions with all protection mechanisms enabled
- **Unquestionable Accuracy** – It is imperative that the device does not generate false positives that may lead to a denial-of-service condition
- **Fine Grained Granularity and Control** – to decide exactly which malicious traffic is blocked, it is vital that the IPS be able to be fine tuned by attack, by policy or right down to the individual host level

## Executive Summary

The following comments were taken from the Executive Summary section of the NSS Report, (note – any comments referred to in quotes are those of Bob Walder, Director of NSS Group):

- The Attack Mitigator IPS 5500 was launched in Q4, 2004. “The IPS 5500 is the first ever device to be tested against both our content-based IPS and rate-based IPS methodologies, and it performed extremely well in both.” At the time of writing, the Attack Mitigator IPS 5500 is the only IPS product capable of passing both tests in the Gigabit class of products. This best in class award represents an important shift in the IPS product space because it now means that there is a single IPS product that is NSS certified to protect against both classes of attack at the same time.

According to Bob Walder, Director of NSS, “Overall, the performance of the IPS 5500 is very impressive, combining almost flawless detection rates at Gigabit wire speed with some of the lowest latency figures we have seen under any traffic condition. We also found the IPS 5500 to be very stable, surviving our extended reliability tests without missing a beat, and without blocking any legitimate traffic or succumbing to common evasion techniques.”

- The NSS test validates Top Layer's claim that the Attack Mitigator IPS 5500 operates at an industry leading 50,000 sessions (connections) per second for a single device. The Attack Mitigator IPS 5500 is the only IPS that can scale performance and capacity for any network size using Top Layer's ProtectionCluster™ solution.
- "Top Layer's second-generation ASIC technology and mitigation algorithms integrate Stateful analysis techniques with its new TopInspect™ deep packet inspection technology and Denial of Service attack protection to provide comprehensive protection from Internet-based and internal threats."
- "Overall, the performance of the IPS 5500 is very impressive, combining almost flawless detection rates at Gigabit wire speed with some of the lowest latency figures we have seen under any traffic condition."
- "We also found the IPS 5500 to be very stable, surviving our extended reliability tests without missing a beat, and without blocking any legitimate traffic or succumbing to common evasion techniques."
- In the first NSS test in 2003, the first generation Attack Mitigator was an impressive rate-based solution. Top Layer have taken their leading rate-based technology and now combined it with their new content-based technology. In this second generation product, "its rate-based attack mitigation and bandwidth management features remain as impressive as ever."
- "The new Central Management System provides more extensive management features, albeit at an additional cost."

## Verdict

The following comments were taken from the Verdict section of the NSS Report

- A single IPS 5500 device is rated for a single Gigabit link (2Gbps aggregate throughput) and was tested to 1Gbps by NSS. "It turned in an outstanding performance in all our tests, achieving 100% detection rates across the board, and clearly with some headroom to spare. We would be more than happy to rate this device at a minimum of 1Gbps under **all** network loads." Although not specifically tested, Top Layer's ProtectionCluster™ provides a scaleable IPS solution that not only increases capacity, but provides better protection in real world environments through advanced state sharing and awareness.

According to Walder, "The IPS 5500 was one of the few devices we have tested in our labs which has achieved zero packet loss and low latency at all packet sizes up to 1Gbps. Overall, latency figures were considered to be outstanding, almost switch-like, under all traffic loads and packet sizes. Clearly this device can be placed anywhere on the corporate network – from the perimeter to a heavily-loaded high-speed backbone – without impacting overall network performance in any way."

- "Basic latency figures were outstanding – almost switch-like – across the board under all traffic loads. They ranged from 20µs to 41µs with between 250Mbps

(256 byte packets) to 1Gbps (1000 byte packets). Behavior throughout the tests with no background traffic was extremely constant and predictable, hardly increasing at all as additional network load was applied from 250Mbps to 1Gbps."

- "The IPS 5500 was also one of the few devices we have tested in our labs which has achieved zero packet loss and low latency at all packet sizes up to 1Gbps. Overall, latency figures were considered to be outstanding for a device of this type under all traffic loads and packet sizes. Clearly this device can be placed anywhere on the corporate network – from the perimeter to a heavily-loaded high-speed backbone – without impacting overall network performance in any way."
- "The IPS 5500 performed consistently and completely reliably throughout our tests, continuing to block attack traffic in a consistent manner whilst passing 100% of the legitimate traffic, even when under extended attack."
- "In the rate-based attacks, the IPS 5500 performed equally well. Mitigating high-volume rate-based attacks is a different prospect to detecting and blocking single-packet exploits, and often two different devices are deployed to achieve both. The Top Layer device is currently one of only a few devices on the market capable of completing both our content- and rate-based methodologies. Performance at all levels of our load tests was impeccable, with 100% of all attacks being detected and mitigated under all load conditions, and no interruptions to legitimate sessions. Latency too was very low across all tests, even when under heavy DoS attack."
- "The IPS 5500 is rated for DDoS protection at up to 500,000pps and the ProtectionCluster features can be used to scale this to higher rates. The device performed almost impeccably up to the 600Mbps level of attack traffic."
- "Top Layer has made significant additions to its protocol decode and validation modules, and significant enhancements to its signature set for this release. The IPS 5500's resistance to false positives is good and resistance to known evasion techniques was excellent, with the IPS 5500 achieving a clean sweep across the board. Performance in the high volume detection/mitigation test was almost impeccable across the board, with perfect detection and mitigation at all load levels."
- "The main job of the IPS 5500 is to stop malicious traffic or suspicious traffic, and it performs its blocking and mitigation tasks well. Most users would probably be content to leave it at the fact that the bad traffic never made it onto their network, but for those who want additional forensic analysis on the mitigated traffic, the IPS does provide the forensic port to route traffic to Top Layer's SecureCommand+™, CMS or other third party collection and analysis product."
- "The learning curve is steep and day to day running of the device is well catered for by the Management Application."

- “It is important with in-line devices such as this that sufficient features are given over to the task of traffic profiling, and the Attack Mitigator IPS 5500 does provide good graphical monitoring tools to help determine optimum bandwidth and connection rates for various applications before limiting traffic.”
- Deployment of the Attack Mitigator typically requires no changes to network topology and can be installed in minutes. Once installed, users can select from several predefined Protection Configurations with one click of a button. Unlike competitive products that claim to have broad protection capabilities, but only enable a small sub-set for fear of generating false positives, the Attack Mitigator can be set to block attacks in minutes because of its more intelligent protection mechanisms.

## **Conclusion**

The Attack Mitigator IPS 5500 is the world’s only IPS to provide Non-Stop Protection against network-level and application-level attacks. The Attack Mitigator seamlessly integrates protection, performance, management and reliability to create the only solution to provide Total Network Integrity by allowing good traffic to reach its destination when under attack. The powerful integration of these components means that the Attack Mitigator IPS provides the best protection at the highest throughput and lowest latency of any IPS product in the market.

Protecting against today’s sophisticated attacks is easy with the Attack Mitigator, which can be deployed to provide full protection within minutes, even in networks that need the high availability ProtectionCluster™ solution that operates at an unprecedented throughput of 8.8Gbps. NSS’s unprecedented double approval of the Attack Mitigator IPS 5500 is a testament to the power of the solution.

## **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](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)

A copy of the 80 page NSS Lab report on the Attack Mitigator IPS 5500 can be obtained upon request.

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

Phone: 508-870-1300, Fax: 508-870-9797, [www.TopLayer.com](http://www.TopLayer.com)