



## Top Layer Networks Attack Mitigator IPS 5500 Highlights

### The News

- Top Layer is announcing a new family of products – Attack Mitigator IPS 5500-100, IPS 5500-500 and IPS 5500-1000.
- The Attack Mitigator IPS 5500 platform is part of Top Layer's strategy to provide enterprises, service providers and government institutions with an innovative intrusion prevention solution that protects critical on-line assets from the growing number of network and application level cyber threats.
- Result: Attack Mitigator IPS 5500 is the first high performance, Non-Stop Protection platform for network-level and application-level threats.

### Innovative Non-Stop Protection Approach

- Architected from the ground up for intrusion prevention based upon experience gained over two years of in-line IPS deployments, the IPS 5500 incorporates stateful firewall technology with advanced deep packet inspection and intrusion prevention algorithms and is built upon a robust, high-performance, expandable platform.
- Contrast with the in-line IDS approach, which is costly due to its use of exploit detection versus vulnerability protection methodology, large log files and manual intervention.
- Contrast with a firewall that attempts to bolt on intrusion prevention technology, which lacks significant application-level protection, operates poorly under volume attacks and suffers from performance impacts.
- Result: Superior high-performance protection against network- and application-level threats which can expand to meet critical-asset-specific protection requirements.

### Non-Stop Protection

- **Advanced Network and Application-Level Protection** — Safeguards on-line assets from critical network- and application-level threats by blending protection from known and unknown attacks on critical vulnerabilities with protection against application-specific threats.
  - TopInspect™ Deep Packet Inspection technology combined with, proven stateful analysis, advanced protocol validation and acceptable use algorithms, industry leading DDoS protection and expandable application-specific protection.
- **Industry-Leading Performance** — High performance is delivered via the ASIC-based architecture, resulting in low-latency, high-throughput (2 gigabit speeds) and high connection rates.
  - 60,000 stateful connections per second (2 to 5 times industry state-of-art) with switch-like network latency and high throughput
  - 1,500,000 SYNs per second from distributed sources (3 to 10 times industry state-of-art).
- **Non-Stop Reliability** — High reliability system design and execution of security policies with minimal operator intervention provides non-stop attack mitigation to help ensure business continuity around the clock.
  - Reliable network operation provided by high-MTBF ASIC-based hardware design, redundant, hot swappable power supplies, and hot swappable fan-tray, along with secure custom O/S, and flexible port-bypass capabilities.

## Examples of Attack Protection

- The Attack Mitigator IPS 5500 platform:
  - Prevents undesired access
  - Filters illegal packets (such as LAN.d attacks) and illegal headers (such as IP options)
  - Stops network attacks (such as fragmentation attacks) and denial of service attacks (such as SYN Flood)
  - Prevents exploits of critical vulnerabilities (such as SQL Slammer, MS-Blaster and other worms)
  - Mitigates service overload attacks (such as SPAM-load artifacts)
  - Thwarts application-level attacks (such as reverse directory traversal exploits)

## Product Family Details

- Attack Mitigator IPS 5500-100
  - 100 Mbps networks (200 Mbps full duplex)
  - 4 10/100 Int./Ext. ports and 4 management ports
- Attack Mitigator IPS 5500-500
  - Gigabit networks (1 Gbps full duplex)
  - 4 GBIC Int./Ext. ports, 4 10/100 ports and 4 management ports
- Attack Mitigator IPS 5500-1000
  - Gigabit networks (2 Gbps full duplex)
  - 4 GBIC Int./Ext. ports, 4 10/100 ports and 4 management ports

## Deployment Scenarios

- Network Perimeter
  - In front of existing perimeter firewall: Increases protection against targeted DDoS attacks and application-level threats.
  - Behind VPN concentrator: Protect the network from cyber threats that may traverse the VPN link.
- Critical On-Line Asset Protection
  - In front of critical assets: Protects assets from network and application level threats regardless of whether they originate from outside or from within.
  - Internal network: Used to protect network segments from threats and provide containment of “infected” segments from other segments.