

**Provides the most comprehensive real-time defense of critical IT assets through high performance inline network and application layer protection**



### Product Highlights

- **Comprehensive Infrastructure Security**

In-depth protection against network and application based threats including zero-day and unknown attacks

- **Performance**

Industry-leading inline inspection and real-time blockage of attacks ensuring business integrity

- **DDoS Protection**

Powerful protection from debilitating high-rate attacks such as SYN Floods and other network and application-based DoS attacks

- **Application Protocol Validation**

Stateful analysis and deep-packet inspection technologies combined with in-depth understanding of protocol, and application usage criteria and enforcement

- **Reliability**

Hardened custom-OS, flexible port-bypass capabilities

- **Easy to Deploy and Manage**

The IPS can be deployed and managed seamlessly and start protecting critical resources in less than 30 minutes

The Attack Mitigator™ IPS 5500 is the latest addition to Top Layer's globally proven set of inline Intrusion Prevention Systems (IPS). The IPS 5500 offers the best network and application assets protection against Distributed Denial of Service (DDoS), protocol, application and hacker attacks, and other malicious exploits such as Worms and Trojans. Top Layer's solution has been uniquely designed to defend against not only existing cyber threats but also provide protection from newly discovered "zero-day" exploits. In addition, Top Layer provides the capability to protect against high volume attacks effectively through rate-based controls.

The existing security infrastructure in many organizations – firewall and network intrusion detection – is no longer sufficient for the immediate blockage of high-volume and increasingly intelligent attacks that can interrupt business operations. To deliver protection against constantly evolving cyber threats requires a new class of intelligent, non-disruptive and highly reliable IT security solutions. These new solutions must provide the maximum amount of inline protection for critical IT assets while allowing full access to legitimate users and applications. The Attack Mitigator IPS 5500 family provides the most comprehensive protection from a wide variety of cyber threats, while also meeting today's requirements for performance and availability.

### Ensuring Business Continuity through Next Generation IT Resource Protection

By improving upon the most powerful characteristics of stateful inspection firewall technology and intrusion detection systems, Top Layer has developed the IPS 5500 in order to analyze and prevent attacks real-time with minimal interruption of legitimate traffic. Top Layer performs non-disruptive deep packet inspection and analysis coupled with intelligent blocking of attacks through TopFire™ second-generation ASIC technology. This architecture provides the high performance base required for real-time protection against today's threats along with the flexibility to integrate application-specific protection mechanisms that can immediately prevent zero-day exploits. With Top Layer's unique solutions, IT security costs are drastically reduced by:

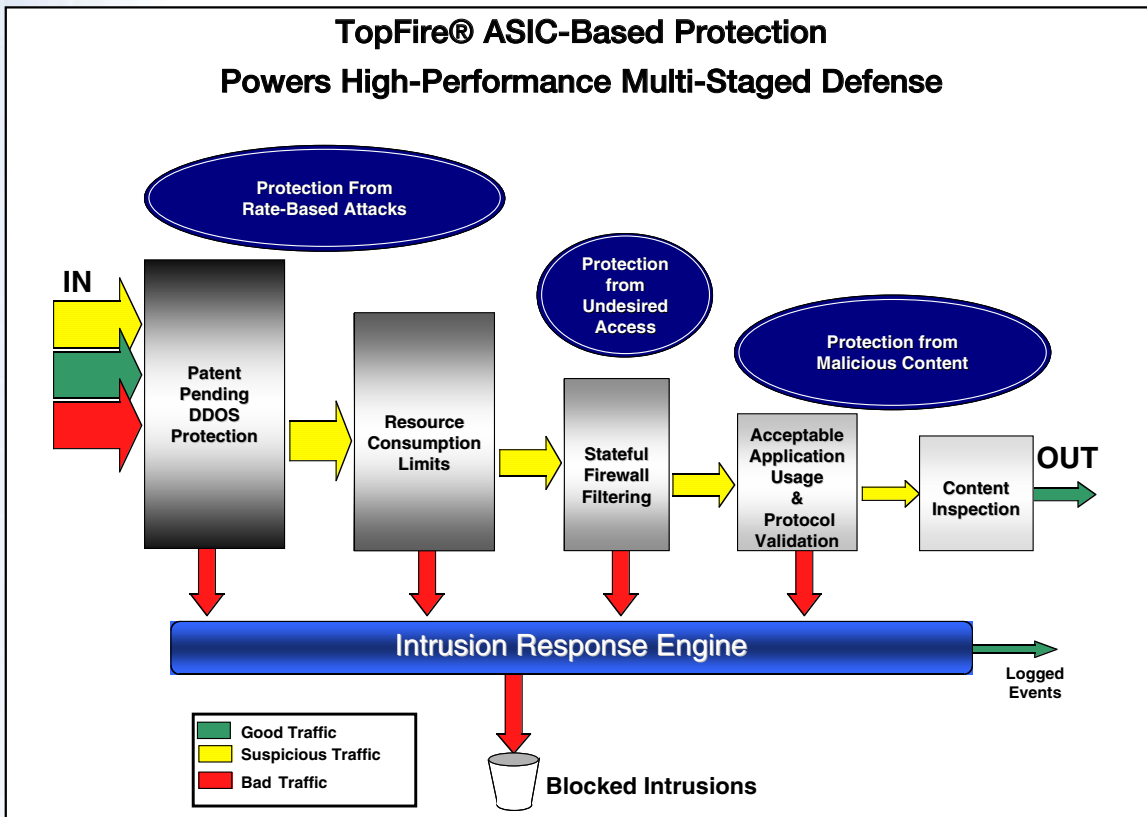
- Proactive protection from threats while patches are being tested and deployed
- Reduction in time spent by IT personnel fixing/remediating
- Protecting against exploits through acceptable application usage enforcement
- Reducing downtime from DDoS and Zombie threats
- Protection from theft of intellectual property

### Comprehensive Security through a Multi-Staged Defense

A Multi-Staged Defense ensures that all traffic can be properly and efficiently inspected in order to:

- Prevent undesired access
- Filter illegal packets and illegal headers
- Stop network attacks and DDoS attacks
- Prevent exploits of critical vulnerabilities
- Mitigate service overload attacks
- Thwart advanced hybrid and application level attacks





Top Layer has a unique approach to traffic inspection which is done by investigating not only intrusions based on suspicious and malicious content, but also resource attacks that employ extreme rates of traffic. Through the control of connection requests and allowed number of sessions, legitimate clients obtain full access to protected resources while being protected against flood-based attacks.

Top Layer has the most comprehensive solution for protecting your critical assets and thwarting attacks and intrusions. IPS 5500 provides network and application protection mechanisms that employ a wide variety of checks including packet filtering, full stateful firewall protection, rate-based filters, resource and bandwidth consumption enforcement, deep packet inspection, application usage checks, protocol validation and signature matching, all geared towards your specific environment.

<b>Data Link Protection</b>	Configurable checks for illegal or ill-formed MAC and data link headers, IEEE 802.1Q VLAN filters, MAC address filters
<b>Network Protocol Protection</b>	Configurable checks for IPv4, ICMP header fields, IP address filters
<b>Network Attack Protection</b>	Protects against attempts to use TCP retransmissions and segment overlap as evasion mechanisms
<b>Transport Layer Protection</b>	Configurable checks for TCP, UDP header fields, including flexible enforcement criteria
<b>Denial of Service &amp; DDoS Protection</b>	Patent pending protection against SYN floods, ICMP floods, application overload attacks
<b>Protocol Normalization</b>	Reordering and coalescing IP fragments, reordering TCP segments
<b>Access Control Protection</b>	ICSA compliant stateful firewall with up to 1000 rules with no performance degradation
<b>Resource Consumption Limits</b>	Per client and per client-group TCP connection limits, application rate limits, per client request limits
<b>User Specified Signatures</b>	Stateful matching signatures for IP, UDP, and reassembled TCP session payloads
<b>Critical Vulnerability Protection</b>	Protection against injection attacks, access attacks, DoS attacks, unauthorized servers, backdoors, etc.
<b>Acceptable Application Use Checks</b>	Deep packet inspection checks for HTTP, FTP, DNS, SMTP, Telnet, SSH, MS-RPC, MS-CIFS, and other application protocols. Call Top Layer for latest supported list.
<b>Transaction and Data Protection</b>	Application-level checking for HTTP transactions, FTP operations, and DNS transactions
<b>Response Mechanisms</b>	Packet filter, session filter, session reset, forensic redirection, transparent proxy
<b>Reporting Mechanisms</b>	SNMP traps and events, SysLog to logging servers and SEM/SIMs. Ability to provide forensic discard information.

# IPS 5500-50 INTRUSION PREVENTION SYSTEM

## Robust Protection without Sacrificing Network and Application Availability

Top Layer's unique ASIC and FPGA based architecture and specialized TopInspect™ deep packet inspection algorithms can provide real-world protection at real-world performance levels. Through this architecture the IPS 5500 supports true Gigabit-level deep packet inspection, which is required to properly protect networks and critical online assets from today's cyber threats.

In addition, Top Layer delivers high levels of inline protection at industry-leading performance while minimizing latency, a critical factor when deploying security devices in your network. The IPS 5500 family consists of four products ranging in performance and capacity to handle throughputs from 200Mbit/sec to 4.4Gbit/sec, with transaction rates up to 50,000 sessions/sec.

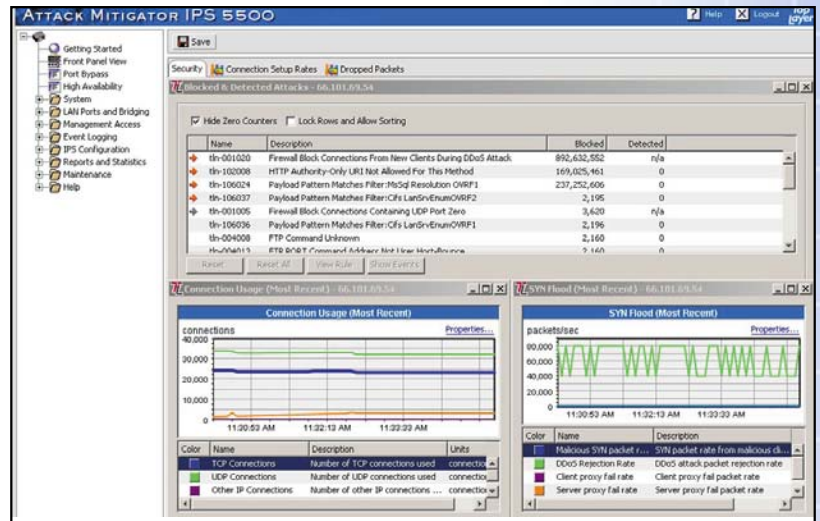
## Flexible Deployment and Simplified Management

Due to the flexible nature of the IPS 5500, the solution can be deployed at any number of key areas in your network infrastructure. The IPS 5500 is ideally suited for:

- Perimeter Security
- Protection of Critical Server Resources
- Remote Access and Extranet Protection
- Inter-Departmental Protection

The IPS 5500 combines the familiar ease-of-use in managing today's industry leading firewalls and the rich monitoring and reporting capability of today's leading intrusion detection systems. Through logical device management, all the relevant protection mechanisms, including access controls,

resource consumption limits, network attack mitigation, and protection against exploits of critical vulnerabilities and application level attacks, are right at your fingertips. Top Layer provides powerful policy-based management as well as keyword-based policy control to simplify management. In addition, Top Layer's Intrusion Response Engine provides an intuitive event-logging format for integration with leading event management tools.



## Intrusion Prevention Technical Support Service (IPTSS)

TopResponse IPTSS is a Top Layer technical support service that provides Attack Mitigator IPS customers with a comprehensive security support service that includes:

- E-mailed Security Advisories for newly discovered vulnerabilities, exploits, and threats that can be addressed by the IPS 5500
- Updated settings, signatures, rules and configurations to address vulnerabilities, exploits, and threats
- 24 x 7 Technical Assistance Center (TAC), including phone support
- Advanced notification of future software releases

## Why Top Layer

Top Layer provides high performance inline Intrusion Prevention Solutions that are widely deployed across the world today. The Attack Mitigator IPS's architecture leverages Top Layer's years of experience providing high-speed network security products to Global 2000 organizations. Top Layer has the most experience in in-line Intrusion Prevention with customer deployments worldwide and has certified compatibility with the leading security management providers.

# IPS 5500-50 INTRUSION PREVENTION SYSTEM

## Technical Specifications - IPS 5500 Intrusion Prevention System

IPS 5500-50	
<b>Interfaces</b>	
Fast Ethernet ports (10BASE-T/100BASE-TX)	8 (4 INT/EXT + 4 MGMT)
Gigabit Ethernet ports (GBIC)	0
H/A Interconnect (1000BASE-SX)	0
Other ports (Serial Console, Auth, Service)	1 Serial, 2 USB 2.0
<b>Performance/Capacity</b>	
Target Network Capacity	In-line 100BASE-TX Network at 50% load
Rated Firewall Throughput	100 Mbps
Raw Firewall Throughput	200 Mbps
Typical Device Latency (Stateful Firewall)	<50uSec
Typical Device Latency (Deep Packet Inspection)	< 100 uSec
Concurrent Sessions	128,000
Session Setup/Teardown (Stateful Firewall)	15,000/Sec
Session Setup/Teardown (Deep Packet Inspection)	15,000/Sec
SYN Flood DoS Protection Rate	150,000/Sec
<b>Device Management</b>	
Management Interfaces	Four (4) switched 10BASE-T/100BASE-TX Ports on isolated switch fabric with flexible assignment
Centralized Management	Yes, through Top Layer Networks SecureCommand+ CMS
Out-Of-Band Access	Dedicated LAN ports, 9-pin D-Sub for Local Console
Command Line	Yes, via local console, Telnet, or SSH
Web-Based	Yes, via Java Web Start application over HTTP, or SSL
SNMP	Yes, SNMPv1 standard MIB GETs, TRAPS
Software Upgrade	Remotely upgradeable image and configuration stored on internal Compact Flash
Secured Physical Access	Locking Compact Flash cover, console access token, tamper-evident seal
Management Partners	Open Service, eIQ Networks, IBM Tivoli, HP Openview, Forensics Explorer, GuardedNet, Q1Labs
<b>Physical/Environmental</b>	
Size (2RU)	8.8cm (H) x 43.8cm (W) x 51.5cm (D)
Weight	23 lbs.
Operating Temp	0 C to 40 C (32 F to 104 F)
Storage Temp	-25 C to 70C (-13 F to 158F)
Humidity	5% to 95% non condensing
MTBF	>100,000 hours (25 deg. C ambient)
<b>Power &amp; Cooling</b>	
Power Supply Type	Hot-swappable PSU (Optional dual PSU)
AC Input	100 to 240 VAC auto-ranging, 50-60Hz
Power Consumption	200W
Cooling	Hot-swappable N+1 fan tray
<b>Compliance &amp; Approvals</b>	
Compliance to EMC Emissions	FCC 47 CFR Part 15 Class A, EN55022: 1998 including CISPR 22 3rd Edition, EN61000-3-2: A1: 1998 and A2: 1998, EN61000-3-3: 1995
Compliance to EMC Immunity	EN55024: 1998 including CISPR 24 1st Edition
Compliance to Safety	UL 60950-1, 1st Edition, CSA C22.2 No. 60950, 3rd Edition, EN 60950/IEC 60950, 3rd Edition
International Compliance Approvals	UL Listed, CUL, AS/NZS 3260, CE, FCC Class A, VCCI Class A, ICES-003 Class A
<b>Planned Certifications</b>	
Common Criteria Evaluation	NIAP FW PP, EAL4
ICSA Firewall Certification	ICSA Firewall <i>Baseline + Corporate</i> 4.0

### Comint Systems And Solutions

Office No.1, 1st floor, #5-4-57 to 62

Sri Krishna Govinda Complex,

Distillery Road, Ranigunj

Secunderabad-500003

Tel: +91-40-27536034 Fax: +91-40-27536036

E-mail: [Comint@comintindia.com](mailto:Comint@comintindia.com)

Visit us at [www.comintindia.com](http://www.comintindia.com)



perfecting the art of network security

Top Layer Networks, Inc. 2400 Computer Drive • Westboro, MA 01581 USA • 508.870.1300 • Fax 508.870.9797

[www.TopLayer.com](http://www.TopLayer.com)