

**Helps build secure network infrastructure to reduce risks and losses associated with cyber threats.**



### Product Highlights

#### • **Three Dimensional Protection**

Protection against malicious content, undesired access, and rate-based attacks.

#### • **Performance**

High throughput and leading stateful session setup rates ensure excellent network performance.

#### • **Lowest Network Latency**

At <50 uSec there's no interruption to critical applications like VoIP.

#### • **Reliability and High Availability**

ProtectionCluster H/A configurations, port bypass and redundant power ensure reliability.

#### • **Easy to Deploy and Manage**

Protecting network within 30 minutes.

#### • **TopResponse™ Update Service**

Automated Protection Pack updates keep threat information current.

Cyber crimes and threats result in dramatic financial losses each year. In the 2006 CSI/FBI Computer Crime and Security Survey, three of the top five "Dollar Amount Losses by Type" were viruses, unauthorized access, and Denial of Service (DoS) attacks.

The existing security infrastructure in many organizations is no longer sufficient to protect against increasingly intelligent, high-volume, hybrid attacks which interrupt business operations. Hybrid attacks combine multiple techniques that can get around traditional security measures. For example, Nimda was a textbook example of a hybrid attack; SQL Slammer exploited a vulnerability and caused a DoS condition; and MyDoom contained elements of a virus, a DoS attack, and a backdoor Trojan.

The IPS 5500 E-Series is Top Layer's most advanced family of Intrusion Prevention Systems, designed to deliver non-disruptive protection against constantly-evolving cyber threats. It provides maximum protection for critical IT assets while allowing full access to legitimate users and applications. The IPS 5500 offers Three Dimensional Protection (3DP), that uniquely provides the broadest range of protection including:

- Protection against malicious content through advanced IPS technology
- Protection against undesired access through stateful firewall filtering
- Protection against rate-based attacks through DDoS mitigation



### Ensuring Business Continuity and Minimizing Risks and Losses

With the IPS 5500 in the network, risks and losses are minimized by:

- Reduction in IT hours devoted to fixing/remediating systems infected by viruses, worms, and spyware
- Reduction of downtime from DDoS attacks and Zombie threats
- Protection against theft of intellectual property due to undesired access
- Regulatory compliance through protection of confidential data
- Proactive protection from threats while patches are being tested and deployed
- Improved security posture through acceptable application usage enforcement

### Robust Protection without Sacrificing Network and Application Availability

Top Layer's purpose-built ASIC and FPGA-based architecture, featuring Gigabit speed TopInspect™ deep packet inspection algorithms, provides real-world protection at real-world performance levels. To properly protect networks and critical online assets from today's cyber threats, Top Layer delivers high levels of inline protection at industry-leading performance levels while minimizing latency, a critical factor when deploying security devices in a network. The IPS 5500 line includes products ranging in performance and capacity to handle throughputs from 100Mbit/sec to 2Gbit/sec, with transaction rates up to 50,000 stateful sessions/sec.

### The Most Awarded IPS:



# IPS 5500 E-SERIES INTRUSION PREVENTION SYSTEM

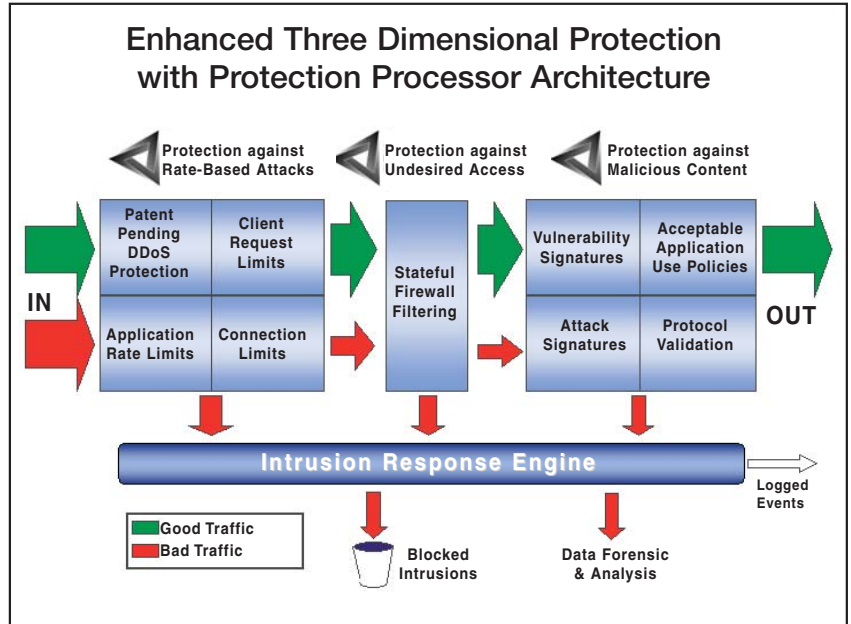
## Comprehensive Network Security through Three Dimensional Protection

Top Layer's enhanced E-Series provides expanded Three Dimensional Protection (3DP) for servers and client desktops. The E-Series IPS uses a new IPS "Protection Processor" architecture with enhanced application payload inspection capabilities. 3DP is a multi-staged defense that ensures all traffic is properly and efficiently inspected in order to:

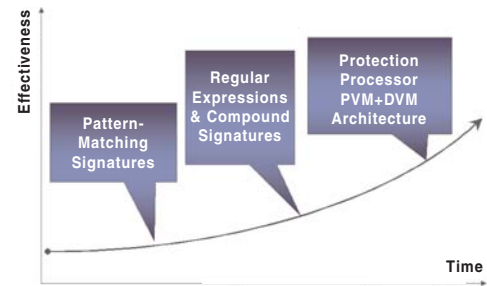
- Block network attacks and DDoS attacks
- Prevent undesired access
- Prevent exploits of critical vulnerabilities
- Thwart advanced hybrid and application level attacks
- Keep worms, viruses, and spyware out of your network
- Provide VoIP Protection with SIP PVM
- Provide P2P Security, blocking BitTorrent, Gnutella, eDonkey, Winny, Skype, and FastTrack.

Protocol Validation Modules (PVM) inspect protocol and identify payload content type.

Callable Data Validation Modules (DVM) inspect data with format-specific content rules, resulting in fewer signatures, quicker updates, and less false positives.



## Protection Processor Architecture Leads Evolution of Content-Based IPS Protection Capabilities



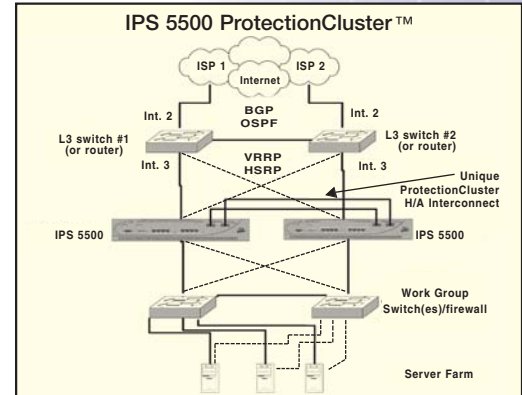
Protection Feature	Description
<b>Rate-Based Protection</b>	
Denial of Service & DDoS Protection	Patent pending algorithms for protection against SYN floods, ICMP floods, UDP floods, and application overload attacks
Application Rate Limits	Policy based rules that limit traffic rates
Connection Limits	Configurable rules that protect your network resources (such as servers and routers) from being overwhelmed by too many active connections
Client Request Limits	Configurable rules that limit the rate at which individual clients or groups of clients can initiate transactions
<b>Undesired Access Protection</b>	
Stateful Firewall Filtering	<ul style="list-style-type: none"> <li>• Policy-based undesired access protection through stateful firewall filtering with no performance degradation</li> <li>• Configurable data link protection against illegal or ill-formed MAC and data link headers, IEEE 802.1Q VLAN filters, MAC address filters</li> <li>• Configurable protection against attempts to use TCP retransmissions and segment overlap as evasion mechanisms</li> <li>• Configurable network protocol protection rules for IPv4, ICMP header fields, IP address filters</li> </ul>
<b>Malicious Content Protection</b>	
Acceptable Application Use Policies	<ul style="list-style-type: none"> <li>• Deep packet inspection for HTTP, FTP, DNS, SMTP, Telnet, SSH, MS-RPC, MS-CIFS, and other application protocols</li> <li>• Critical vulnerability protection against injection attacks, access attacks, DoS attacks, unauthorized servers, backdoors, etc.</li> <li>• Transaction and data protection rules for application-level checking of HTTP, FTP, DNS, SMTP, Telnet, SSH, MS-RPC, MS-CIFS, and other application protocols</li> <li>• Configurable data validation modules that inspect the content and format of known and unknown file types when carried as payloads of supported L3, L4, and L5 protocols</li> </ul>
Protocol Validation	<ul style="list-style-type: none"> <li>• Configurable transport layer protection rules for TCP and UDP including flexible enforcement criteria</li> <li>• Protocol normalization for reordering and coalescing IP fragments, and reordering TCP segments</li> </ul>
Attack Signatures	Stateful matching signatures for IP, UDP, and reassembled TCP session payloads. In addition to the factory provided signatures, users can add and edit their own signatures.
Vulnerability Signatures	Unlike the attack signatures, our vulnerability signatures provide protection against a whole group of attack variants, and are also very useful in providing protection against zero day attacks. For example, a vulnerability signature that simply checks that the HTTP host field length is smaller than 410 bytes can stop multiple known MS IIS exploits.

# IPS 5500 E-SERIES INTRUSION PREVENTION SYSTEM

## High Availability with High Utility

With Top Layer's deep networking experience, the IPS 5500 offers the right solution for ensuring high availability and non-stop reliability:

- Active-Active and Active-Standby operation
- Asymmetric traffic handling
- Scalable performance and capacity
- Seamless fail-over that ensures non-stop protection
- Hot swappable power supply and fans
- No rotating media or chip fans



## Low Latency

The IPS 5500 has been designed to be a high performance switch-like device to ensure that it will not interrupt latency-sensitive applications such as VoIP, and will ensure speedy response times for all applications.

## Easy to Deploy and Manage

Due to the flexible nature of the IPS 5500, the solution can be deployed at any number of key areas in your network infrastructure, providing perimeter security, protection of critical servers, remote access and extranet entry points, and inter-departmental segmentation. Top Layer provides powerful policy-based IPS management in an easy-to-use firewall-like interface.

Row #	Segment	Client	Server	Service	Actions	Log Options	IPS Rule Set	IPS Treatment	Comment
1	Any	Forbidden_Hosts	Any	Any	[Icons]	[Icons]	-	-	Block forbidden clients
2	Any	Any	Forbidden_Hosts	Any	[Icons]	[Icons]	-	-	Block forbidden servers
3	Any	Any	Spyware_Sites	Any	[Icons]	[Icons]	-	-	Block spyware calling home
4	Any	Security_Scanners	Any	Any	[Icons]	[Icons]	All Rules Off	-	Don't interfere with vulnerability scanners
5	Outbound	Suspect_Hosts	Any	http/tcp80,ht...	[Icons]	[Icons]	Strict Server Protection	-	Be strict with suspect hosts using public services
6	Inbound	Desktop_Systems	Suspect_Hosts	Any	[Icons]	[Icons]	Strict Client Protection	-	Apply strict protection for clients using suspect services
7	Any	Any	Desktop_Systems	Any	[Icons]	[Icons]	-	-	Block desktop-deployed services
8	Any	Any	Public_Servers	http/tcp80,ht...	[Icons]	[Icons]	Recommended Server Protection	-	Access to public services
9	Any	Non_Routable_IP	Any	Any	[Icons]	[Icons]	Recommended Client Protection	-	Non-routable IP clients
10	Any	Any	Non-Routable_IP	Any	[Icons]	[Icons]	Recommended Server Protection	-	Non-routable IP servers
11	Inbound	Any	Any	Any	[Icons]	[Icons]	Recommended Client Protection	-	Outbound catch-all
12	Any	Any	Any	Any	[Icons]	[Icons]	Recommended Server Protection	-	Catch-all

## TopResponse Research and Update Service

TopResponse is a comprehensive service that provides customers with advanced security support services to maximize the security, availability, and performance of their networks. TopResponse's automated Protection Pack updates include updated signatures, rules, and configuration files to address the newest threats.

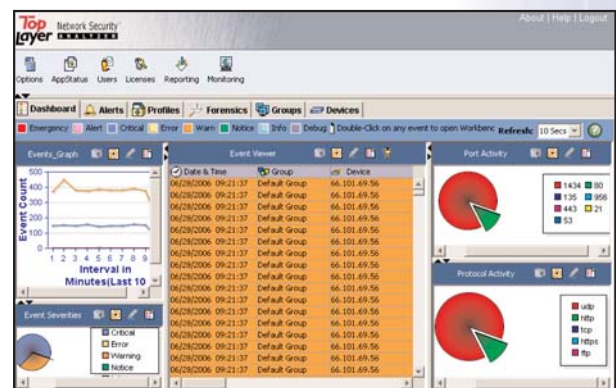
## Detailed Real-Time Incident Response

Top Layer's Intrusion Response Engine includes a built-in real-time Security Event Viewer that allows users to drill down and identify attackers, victims, and types of attacks and then take immediate action to block or mitigate the threat. In addition, it uses a flexible event-logging format for integration with leading security event management tools.

## Centralized Management System

Top Layer's Network Security Analyzer provides security event management, real-time alerting, and flexible reporting. It saves time and effort in normal day-to-day security monitoring and incident response. It features:

- Enterprise-wide IPS security intelligence
- Real-time monitoring and correlated alerting
- Forensics and investigative root cause analysis
- Reporting and monitoring portals
- MSSP support with advanced user access controls
- Compliance audit lifecycle management



# IPS 5500 E-SERIES INTRUSION PREVENTION SYSTEM

## Technical Specifications - IPS 5500 E-Series Intrusion Prevention System

Order Part Number	IPS 5500-150E	IPS 5500-500E	IPS 5500-1000E
<b>Interfaces</b>			
Fast Ethernet ports (10BASE-T/100BASE-TX)	8 (4 INT/EXT + 4 MGMT)		
Gigabit Ethernet ports (GBIC)	4 INT/EXT		
H/A Interconnect (1000BASE-SX)	2		
Other ports (Serial Console, Auth, Service)	1 Serial, 2 USB 2.0		
<b>Performance/Capacity</b>			
Target Network Capacity	In-line 100BASE-TX Network & Lightly Loaded Gigabit Network	In-line Gigabit Ethernet Network 50% Load	In-line Gigabit Ethernet Network
Rated Firewall Throughput	300 Mbps	1000 Mbps	2000 Mbps
Raw Firewall Throughput	600 Mbps	2400 Mbps	4400 Mbps
Typical Device Latency (Stateful Firewall)	<50 uSec	< 50 uSec	< 50 uSec
Typical Device Latency (Deep Packet Inspection)	< 100 uSec	< 100 uSec	< 100 uSec
Concurrent Sessions	512,000	512,000	1,000,000
Session Setup/Tear Down (Stateful Firewall)	50,000/Sec	50,000/Sec	50,000/Sec
Session Setup/Tear Down (Deep Packet Inspection)	40,000/Sec	40,000/Sec	40,000/Sec
SYN Flood DoS Protection Rate	500,000/Sec	1,000,000/Sec	1,500,000/Sec
Protection Cluster Capable	Yes	Yes	Yes
<b>Device Management</b>			
Management Interfaces	Four (4) switched 10BASE-T/100BASE-TX Ports on isolated switch fabric with flexible assignment		
Out-Of-Band Access	Dedicated LAN ports, 9-pin D-Sub for Local Console		
Command Line	Yes, via local console or Telnet		
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	Optional Locking Compact Flash cover, console access token, tamper-evident seal		
Third Party Management Compatibility	ArcSight, Computer Associates, eIQ Networks, Forensics Explorer, GuardedNet, HP Openview, IBM Tivoli, netForensics, Network Intelligence, Open Service, Q1Labs, TriGeo		
Response Mechanisms	Packet filter, session filter, session reset, forensic redirection, transparent circuit proxy		
Reporting Mechanisms	SNMP traps and events, Syslog to logging servers and SEM/SIMs. Ability to provide forensic discard information.		
<b>Physical/Environmental</b>			
Size (2RU)	8.8cm (H) x 43.8cm (W) x 51.5cm (D)		
Weight	24 lbs.		28 lbs.
Operating Temp	0 C to 40 C (32 F to 104 F)		
Storage Temp	-25 C to 70 C (-13 F to 158 F)		
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		225W
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		

### About Top Layer

Top Layer is dedicated to its role as leading global provider of Network Intrusion Prevention Systems (IPS), developing and bringing to market network security infrastructure solutions that help commercial and government organizations protect their critical on-line assets from the losses and risks associated with cyber threats. Its family of IPS appliances is designed with "Three Dimensional Protection" that provides the most advanced protection capabilities against known and unknown attacks at the highest performance rates. Top Layer Networks is headquartered in Massachusetts USA with sales and support presence in Canada, Germany, Japan, Korea, The Netherlands and the United Kingdom.



perfecting the art of network security

Top Layer Networks, Inc. 2400 Computer Drive • Westboro, MA 01581 USA • +1.508.870.1300 • Fax +1.508.870.9797

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