

**Build secure network infrastructure and reduce risks and losses associated with cyber threats.**



#### Product Highlights

- **TopResponse<sup>TM</sup> Update Service**

Automated Protection Pack updates keep threat information current.

- **Three Dimensional Protection**

Protection against malicious content, undesired access, and botnet-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 networks within 30 minutes.

The existing security infrastructure in many organizations is no longer sufficient to protect against today's cyber threats. The continued discovery of vulnerabilities in commercially deployed software puts servers and client workstations at risk for becoming compromised by Spyware, viruses, botnet programs and other malicious code. The development of more targeted attack methods and clever social engineering makes it more likely that even careful educated users can become victims. Finally the appearance of true zero-day exploits of commonly deployed software such as the recent set of zero-day exploits in operating systems and other network infrastructure products, makes patching an ineffective defense.

The IPS 5500 E-Series is Top Layer's most advanced third generation family of Intrusion Prevention Systems, designed to deliver non-disruptive protection against constantly-evolving threats. It provides maximum protection for critical IT assets while allowing full access to legitimate users and applications.

Security threats are constantly changing and your network needs to rapidly be protected from zero-day attacks. Top Layer's TopResponse provides an automated protection service ensuring proactive protection for your network and assets.

#### Ensuring Business Continuity and Minimizing Risks and Losses

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

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

#### Robust Protection without Sacrificing Network and Application Performance

Top Layer's purpose-built ASIC and FPGA-based architecture, featuring Gigabit speed TopInspect<sup>TM</sup> deep packet inspection algorithms, provides real-world protection at real-world performance levels. To properly protect networks and critical online assets from today's 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 E-Series includes products ranging in performance and capacity to handle throughputs from 300Mbit/sec to 4.4Gbit/sec, with transaction rates up to 40,000 stateful sessions/sec.

#### The Most Awarded IPS:



# IPS 5500 E-SERIES INTRUSION PREVENTION SYSTEM

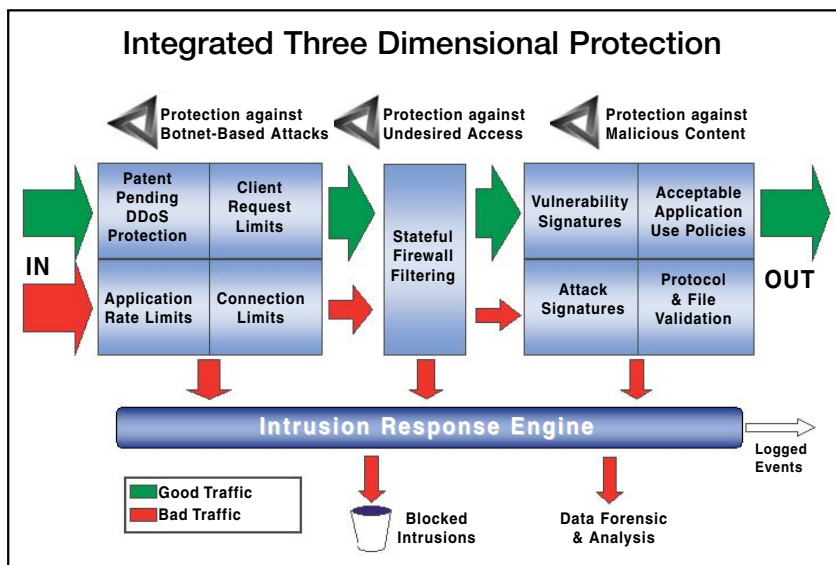
## TopResponse Research and Update Service

TopResponse is an Automated Protection Update Service that provides Top Layer IPS 5500 customers with advanced security services to maximize security, availability, and performance of their network. TopResponse offers customers proactive protection from zero-day threats and resolution to their security issues. Specifically, TopResponse provides automated updates, technical support, security advisory and software subscription services, along with access to Top Layer's Security Knowledge Base and special delivery programs. Customers will feel confident that their network's security is protected and operating at optimal performance.

## Comprehensive Network Security through Three Dimensional Protection

Top Layer's enhanced E-Series provides expanded Three Dimensional Protection (3DP) for servers and client desktops. 3DP is a multi-staged defense that ensures all traffic is properly and efficiently inspected in order to:

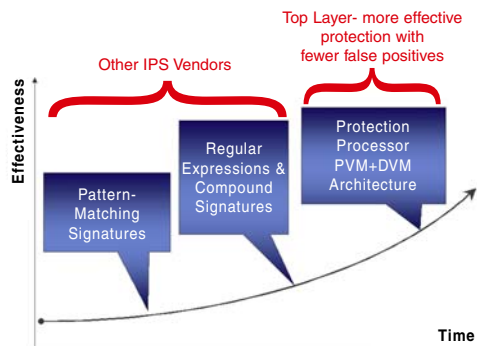
- Prevent exploits of critical vulnerabilities
- Keep Spyware, viruses, botnet programs and other malware out of your network
- Thwart advanced hybrid and application level attacks
- Provide P2P Security, blocking BitTorrent, Gnutella, eDonkey, Winny, Skype, and FastTrack
- Provide protection of VoIP infrastructure
- Block DDoS and botnet-based attacks
- Prevent undesired access



Protection Benefits	Description
<b>Prevents desktop computers and servers from being compromised by remote exploits and malware.</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 & File 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> <li>• Configurable file-format protection rules for files carried in protocol payloads</li> <li>• File format usage policies</li> </ul>
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.
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.
<b>Prevents undesired access to business-critical systems, applications, and data.</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>Ensures the availability of applications and services, even when under botnet-initiated attacks.</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

# IPS 5500 E-SERIES INTRUSION PREVENTION SYSTEM

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



## E-Series File Validation Architecture

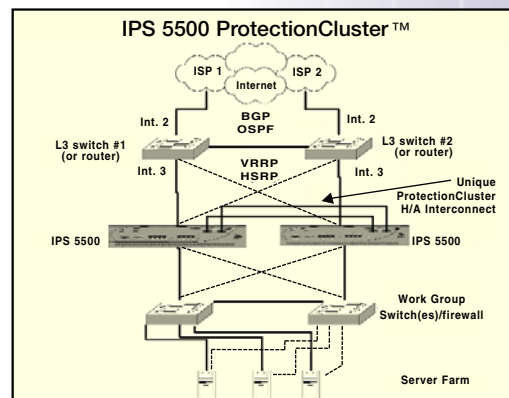
Top Layer's E-Series, unlike other approaches that are only signature-based, uses a new multi-tiered "Protection Processor PVM+DVM Architecture" which couples our industry-proven protocol validation modules (PVMs) with a set of new File-Format-Specific Data Validation Modules (DVMs). Deep File Inspection, such as looking for MS-Word exploits, occurs independently from the protocol which is used to transfer the file, requiring fewer filters than competitive approaches, and resulting in quicker updates and fewer false-positive indications.

- Protocol Validation Modules (PVM) inspect protocol and identify file-type being carried as payload
- Data Validation Modules (DVM) inspect payload files with file-format-specific rules

## ProtectionCluster™ – Scalable, Transparent High Availability

The IPS 5500 ProtectionCluster can be deployed in configurations of up to 8 parallel units and is recommended for deployments requiring greater than 10Gbit/sec of throughput. 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 policies 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.

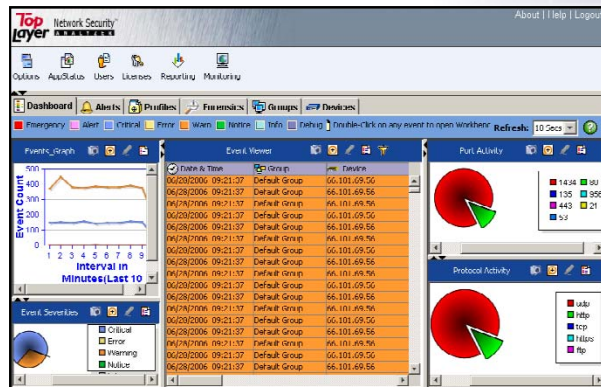
## Detailed Real-Time Incident Response

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:

- Automated security report delivery
- Compliance audit lifecycle management
- Enterprise-wide IPS security intelligence
- Real-time monitoring and correlated alerting
- Forensics and investigative root cause analysis



# 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 Utilized Gigabit Ethernet Network	In-line Gigabit Ethernet Network Moderate Utilization	In-line Gigabit Ethernet Network Heavy Utilization
Throughput	600+ Mbps	2400 Mbps	4400 Mbps
Inspected Throughput	300+ Mbps	1000 Mbps	2000 Mbps
Typical Latency	< 50 uSec	< 50 uSec	< 50 uSec
Typical Inspected Latency	< 100 uSec	< 100 uSec	< 100 uSec
Concurrent Sessions	512,000	512,000	1,000,000
Session Setup/Tear-down	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
ProtectionCluster 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 Supplies	Single Hot-swappable PSU (2nd PSU Optional)	Dual Hot-swappable Power Supply Units	
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 a leading provider of Network Intrusion Prevention Systems (IPS) that reduce organizations' risks and losses by protecting critical online assets against cyber threats. Its family of high performance IPS provides the most advanced protection against zero-day attacks at maximum throughput rates. Top Layer is headquartered in Massachusetts, USA, with Global Sales and Support throughout North America, Europe, Asia, and Japan.



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)