

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



Product Highlights

• **TopResponse™ Update Service**

Automated Protection Pack updates keep threat information current.

• **Three Dimensional Protection**

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

• **Lowest Network Latency**

At <50-100 uSec there's no interruption to critical applications like VoIP.

• **Reliability and High Availability**

ProtectionCluster configurations, built-in port bypass and redundant power ensure reliability.

• **Easy to Deploy and Manage**

Small form-factor pluggable (SFP) ports simplify cabling; protecting networks within 30 minutes.

• **Green Design**

1 RU rack space and low power consumption preserve resources.

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 malware. 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 makes patching an ineffective defense.

The IPS 5500 ES-Series is Top Layer's most advanced 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 ES-Series in the network, risks and losses are minimized by:

- Proactive protection against 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 in IT hours devoted to fixing/remediating systems infected by viruses, worms, and spyware
- Reduction of downtime from DDoS attacks and Botnet threats

Robust Protection without Sacrificing Network and Application Performance

Top Layer's purpose-built Tiler multicore processor 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 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 ES-Series includes models ranging in performance and capacity to handle throughputs from 300Mbit/sec to 8Gbit/sec, with transaction rates up to 40,000 stateful sessions/sec.

The Most Awarded IPS:



Double NSS Awards

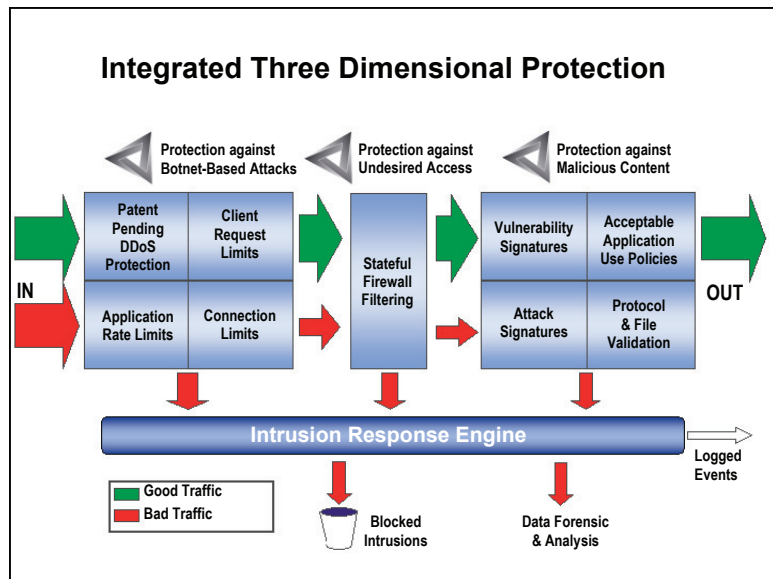


IPS 5500 ES-SERIES INTRUSION PREVENTION SYSTEM

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 is protected and operating at optimal performance.

Comprehensive Network Security through Three Dimensional Protection



Top Layer's ES-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
Prevents desktop computers and servers from being compromised by remote exploits and malware.	
Acceptable Application Use Policies	<ul style="list-style-type: none"> • Deep packet inspection for HTTP, FTP, DNS, SMTP, Telnet, SSH, MS-RPC, MS-CIFS, and other application protocols • Critical vulnerability protection against injection attacks, access attacks, DoS attacks, unauthorized servers, backdoors, etc. • Transaction and data protection rules for application-level checking of HTTP, FTP, DNS, SMTP, Telnet, SSH, MS-RPC, MS-CIFS, and other application protocols • 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
Protocol & File Validation	<ul style="list-style-type: none"> • Configurable transport layer protection rules for TCP and UDP including flexible enforcement criteria • Protocol normalization for reordering and coalescing IP fragments, and reordering TCP segments • Configurable file-format protection rules for files carried in protocol payloads • File format usage policies
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.
Prevents undesired access to business-critical systems, applications, and data.	
Stateful Firewall Filtering	<ul style="list-style-type: none"> • Policy-based undesired access protection through stateful firewall filtering with no performance degradation • Configurable data link protection against illegal or ill-formed MAC and data link headers, IEEE 802.1Q VLAN filters, MAC address filters • Configurable protection against attempts to use TCP retransmissions and segment overlap as evasion mechanisms • Configurable network protocol protection rules for IPv4, ICMP header fields, IP address filters
Ensures the availability of applications and services, even when under botnet-initiated attacks.	
Denial of Service & DDoS Protection	Patented algorithms for protection against SYN floods, ICMP floods, UDP floods, and application overload attacks
Policy-Based 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 ES-SERIES INTRUSION PREVENTION SYSTEM

Technical Specifications IPS 5500 ES-Series Intrusion Prevention System

Order Part Number	IPS 5500-150ES	IPS 5500-500ES	IPS 5500-1000ES	IPS 5500-2000ES
Interfaces				
Copper 10/100/1000 Ethernet ports	4 MGMT			2 MGMT
Pluggable 1G Ethernet ports (SFP modules)	8			
Pluggable 10G Ethernet ports (SFP+ modules)				6
Other ports (Serial Console, Auth, Service)	1 Serial, 1 USB 2.0			
Performance/Capacity				
Target Network Capacity	In-line Gigabit Ethernet Network Light Utilization	In-line Gigabit Ethernet Network Moderate Utilization	In-line Gigabit Ethernet Network Heavy Utilization	In-line 10 Gigabit Ethernet Network Moderate Utilization
MAX Throughput	600+ Mbps	2400 Mbps	4400 Mbps	8000 Mbps
MAX Inspected Throughput	300+ Mbps	1000 Mbps	2000 Mbps	4000 Mbps
Typical Latency	< 50 uSec	< 50 uSec	< 50 uSec	< 50 uSec
Typical Inspected Latency	< 100 uSec	< 100 uSec	< 100 uSec	< 100 uSec
MAX Concurrent Sessions	256,000	1 Million	2 Million	4 Million ¹
MAX Session Setup/Teardown	40,000/Sec	40,000/Sec	40,000/Sec	50,000/Sec
MAX SYN Flood DoS Protection Rate	500,000/Sec	1,000,000/Sec	1,500,000/Sec	2,000,000/Sec
ProtectionCluster Capable	Yes	Yes	Yes	Yes
Device Management				
Management Interfaces	Four (4) switched 10/100/1000 Ports on isolated switch fabric with flexible assignment			Two (2) switched 10/100/1000 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 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, net-Forensics, Open Service, RSA Envision, Q1Labs, TriGeo			
Response Mechanisms	Packet filter, shun, 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			
Physical/Environmental				
Size (1RU)	4.4cm (H) x 44.0 cm (W) x 51.5cm (D)			
Weight	18.1 lbs. (8.2 Kgs)			
Operating Temperature	0 C to 40 C (32 F to 104 F)			
Storage Temperature	-25 C to 70 C (-13 F to 158 F)			
Humidity	5% to 95% non condensing			
MTBF Rating	>300,000 hours (25 deg. C ambient)			
Power & Cooling				
Power Supplies	Dual Hot-swappable Power Supply Units			
AC Input	100 to 240 VAC auto-ranging, 50-60Hz			
Max Power Consumption	< 100W			< 200W
Cooling	Hot-swappable N+1 fan tray			
Compliance & Approvals				
Compliance to EMC Emissions	FCC Part 15-7.10.2008, EN55022: 2006+A1:2007, CISPR22:2005+A1+A2:2005, VCCI-3 2009.04, AS/NZS CISPR22:2006, EN 61000-3-2:2006, EN61000-3-3:1995 +A1:2001+A2:2005, EN61000-3-11:2000, EN 61000-3-12:2005			
Compliance to EMC Immunity	EN55024:1998 including Amendment 1:2001 & Amendment 2:2003(CISPR24:1997 +A1:2001 +A2:2002), EN 61000-4-2:1995 +A1:1998 +A2:2001, EN 61000-4-3:2006, EN 61000-4-4:2004, EN 61000-4-5:2006, EN 61000-4-6:1996 +A1:2001, EN 61000-4-8:1993 +A1:2001, EN 61000-4-11:2004			
Compliance to Safety	UL 60950-1, 2 nd Ed., CSA C22.2 No. 60950-1, 2 nd Ed., EN 60950-1, 2 nd Ed., IEC 60950-1, 2 nd Ed.			
International Compliance Approvals	UL Listed, CUL, AS/NZS 3260, CE, FCC Class A, VCCI Class A, ICES-003 Class A			

¹Requires SWV7.X, otherwise 2 Million

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 known and zero-day threats 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. 1 Cabot Road • Hudson, MA 01749 USA • +1.978.212.1500 • Fax +1.978.212.1600 www.TopLayer.com

Rev 1.7 Dec-14 © 2010. Top Layer Networks, Inc. All Rights Reserved. Attack Mitigator, DCFD, Flow Mirror, IDS Balancer, TopInspect, TopMSS, SecureCommand+, and ProtectionCluster are trademarks of Top Layer. AppSafe, AppSwitch, SecureWatch, Top Layer, Top Layer Networks, TopFire, TopFlow, TopPath, TopView, and perfecting the art of network security are registered trademarks of Top Layer. Unless otherwise indicated, Top Layer trademarks are registered in the United States and may or may not be registered in other countries.