

# Build Secure Network Infrastructure and Reduce Risks and Losses Associated with Cyber Threats

## Product Highlights

- Threat 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 <35-60 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**  
 1U rack space for most models and low power consumption

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 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 Corero's most advanced generation family of Intrusion Prevention Systems. It is designed to deliver non-disruptive protection against constantly evolving threats. It provides maximum security for critical IT assets while allowing full access to legitimate users and applications.



Security threats are constantly changing and networks need to rapidly be protected from zero-day attacks. Corero's Threat Update Service provides an automated protection service, proactively safeguarding networks 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, botnet programs, and other malware
- Reduction of downtime from DDoS attacks and botnet threats

## Robust Protection without Sacrificing Network and Application Performance

Corero's purpose-built Tilera multicore processor architecture, featuring Gigabit speed deep packet inspection algorithms, provides real-world protection at real-world performance levels. To properly safeguard networks and critical online assets from today's threats, Corero delivers high levels of inline protection at industry-leading performance levels. It also minimizes 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 network throughputs from 600Mbit/sec to 10Gbit/sec, with transaction rates up to 250,000 stateful sessions/sec.

## Threat Update Research and Update Service

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

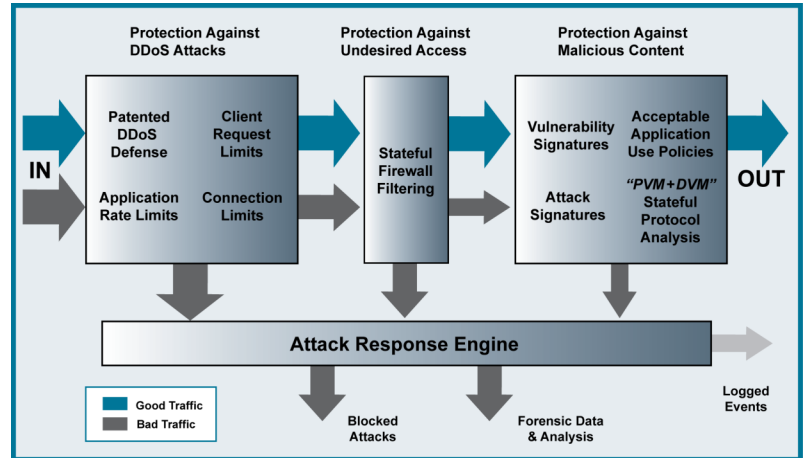
## Comprehensive Network Security through Three Dimensional Protection

Corero's ES-Series provides expanded Three Dimensional Protection (3DP) for servers and client desktops.

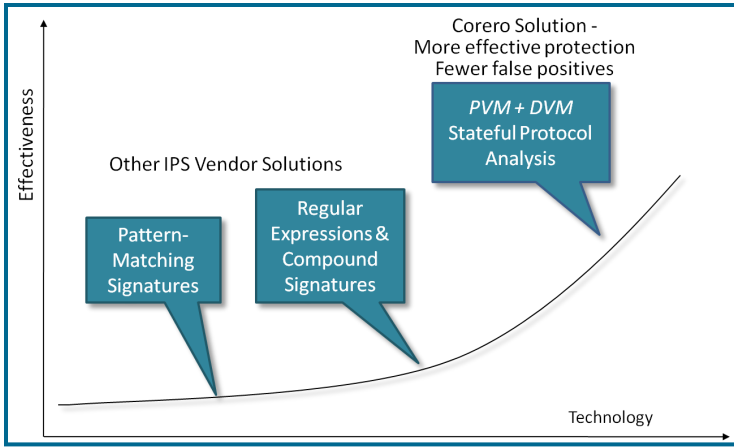
3DP is a multi-staged defense that ensures all traffic is properly and efficiently inspected in order to:

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

## Integrated Three Dimensional Protection



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	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



## Corero's Protocol & File Validation Architecture

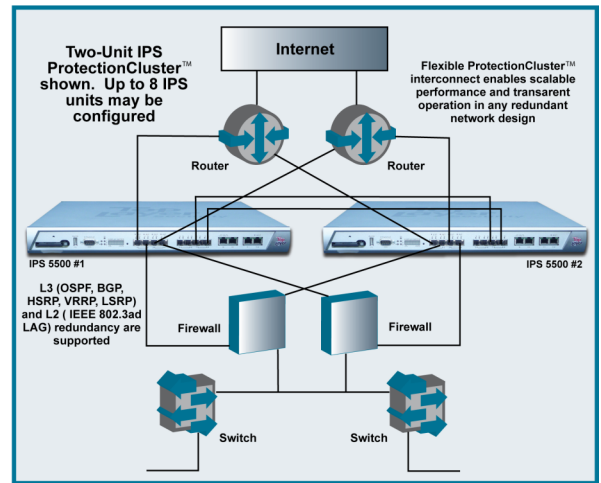
Unlike other IPS approaches, Corero's IPS uses a two-tiered "PVM+DVM" Stateful Protocol Analysis (SPA) implementation. This couples our industry-proven Protocol Validation Modules (PVM) with a set of file-format-specific Data Validation Modules (DVM). The benefits of "PVM+DVM" Stateful Protocol Analysis include increased protection against unknown (zero-day) attacks, fewer filters/signatures required for efficient and effective protection, and fewer false-positive indications.

- PVMs inspect protocol and identify file-types being carried as payloads
- DVMs inspect payload files with file-format-specific rules and signatures

## 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 system throughput up to 20 Gbit/Sec or more. With Corero'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 is designed to be a high performance switch-like device to ensure that it will not interrupt latency-sensitive applications such as VoIP, and guarantees 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 the network infrastructure, providing perimeter security, protection of critical servers, remote access and extranet entry points, and inter-departmental segmentation. Corero provides powerful policy-based IPS management in an easy-to-use firewall-like interface.

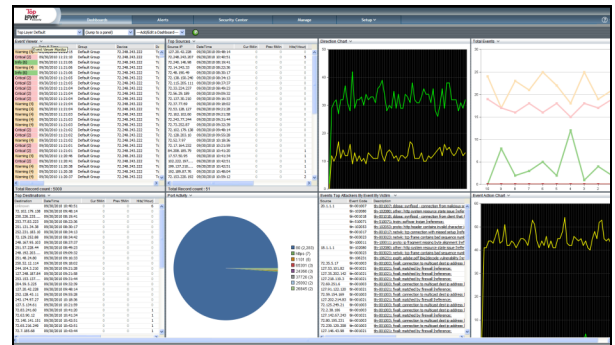
## Detailed Real-Time Incident Response

Corero's Attack 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 Information Event Management (SIEM) tools.

## Centralized Management System

Corero'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:

- Contextually aware high-level alerting
- 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



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

Order Part Number	IPS 5500-150ES	IPS 5500-500ES	IPS 5500-1000ES	IPS 5500-2000ES	IPS 5500-2400ES
<b>Interfaces</b>					
Copper 10/100/1000 Ethernet ports	4 MGMT		2 MGMT		
Pluggable 1G Ethernet ports (SFP modules)	8				
Pluggable 10G Ethernet ports (SFP+ modules)					4
Other ports (Serial Console, Auth, Service)	1 Serial, 1 USB 2.0				2 Serial, 2 USB 2.0
<b>Performance/Capacity</b>					
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	In-line 10 Gigabit Ethernet Network Heavy Utilization
MAX Throughput	600+ Mbps	2.4 Gbps	4.4 Gbps	8 Gbps	10 Gbps
MAX Inspected Throughput	300+ Mbps	1.0 Gbps	2.0 Gbps	4 Gbps	8 Gbps
Typical Latency <sup>1</sup>	< 35 uSec	< 35 uSec	< 35 uSec	< 35 uSec	< 45 uSec
Typical Inspected Latency <sup>1</sup>	< 50 uSec	< 50 uSec	< 50 uSec	< 50 uSec	< 60 uSec
MAX Concurrent Sessions	256,000	1 Million	2 Million	4 Million <sup>2</sup>	8 Million <sup>2</sup>
MAX Session Setup/Tear-down	40,000/Sec	40,000/Sec	40,000/Sec	50,000/Sec	100,000/Sec
MAX SYN Flood DoS Protection Rate	500,000/Sec	1,000,000/Sec	1,500,000/Sec	2,000,000/Sec	3,000,000/Sec
Protection/Cluster Capable	Yes	Yes	Yes	Yes	Yes
<b>Device Management</b>					
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	Four (4) switched 10/100/1000 Ports on isolated switch fabric with flexible assignment
Network Standards	IEEE 802.3-2002, 802.3-2008, 10BASE-T, 100BASE-TX, 1000BASE-T with manual or auto-negotiated speed and duplex, 802.1Q-2003 Standards for supported SFP Modules			IEEE 802.3-2002, 802.3-2008, 10BASE-T, 100BASE-TX, 1000BASE-T with manual or auto-negotiated speed and duplex, 802.1Q-2003 Standards for supported SFP+ Modules & SFF-8431 Rev4.1 10GSFP+Cu (Direct Attach)	
Out-Of-Band Access	Dedicated Management Interfaces described above, 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 (SSL V3.1 / TLS V1.0) <sup>3</sup>				
Management Protocols	Yes, SNMPv1 standard MIB GETs, Traps, NTPv2, SYSLOG				
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, netForensics, Open Service, RSA Envision, Q1Labs,				
Response Mechanisms	Packet filter, shun, session filter, session reset, forensic redirection, transparent circuit proxy				
<b>Physical/Environmental</b>					
Size	1-RU 4.4cm (H) x 44.0 cm (W) x 51.5cm (D)				2-RU 8.8 x 44 x 51.5
Weight	18.1 lbs. (8.2 Kgs)				36.2 lbs. (16.4 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)		>200,000 hours (25 deg. C ambient)		>150,000 hours (25 deg. C ambient)
Operating Altitude	0-10,000 feet				
<b>Power &amp; Cooling</b>					
Power Supplies	Dual Hot-swappable Power Supply Units				Four Hot-swappable Power Supply Units
AC Input	100 to 240 VAC auto-ranging, 50-60Hz				
Max Power Consumption	< 100W		< 150W		< 300W
Cooling	Hot-swappable N+1 fan tray				2 Hot-swappable N+1 fan trays
<b>Compliance &amp; Approvals</b>					
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 <sup>nd</sup> Ed., CSA C22.2 No. 60950-1, 2 <sup>nd</sup> Ed., EN 60950-1, 2 <sup>nd</sup> Ed., IEC 60950-1, 2 <sup>nd</sup> Ed.				
International Compliance Approvals	UL Listed, CUL, AS/NZS 3260, CE, FCC Class A, VCCI Class A, ICES-003 Class A				

<sup>1</sup>Typical latency values measured for packet sizes up to 1518 Bytes

<sup>2</sup>Requires V7.X software, otherwise 2 million for Model 2000ES, 4 million for Model 2400ES

<sup>3</sup>Requires use of IPS Controller for management

## About Corero Network Security

Corero Network Security is a leading global provider of Network Intrusion Prevention Systems (IPS) and Distributed Denial of Service (DDoS) attack defense solutions that enable enterprise organizations to protect their critical on-line assets against risks associated with network-borne cyber threats. Corero, formerly Top Layer Security, is headquartered in Massachusetts, U.S. with sales and services support worldwide.

Corero Network Security, Inc. 1 Cabot Road • Hudson, MA 01749 USA  
+1.978.212.1500 • Fax +1.978.212.1600 www.Corero.com  
169 High Street • Rickmansworth • Hertfordshire WD3 1AY • +44.0.1923.897333  
Copyright 2011 Corero Network Security, Inc., All rights reserved.