DATA SHEET

Intrusion Prevention System

Distributed Intrusion Prevention & Response for Edge-to-Core and Data Center

Benefits

EXTENDS IPS PROTECTION TO THE NETWORK EDGE

- Protect networked resources by removing an attacker's ability to continue an attack or to mount a new attack
- Real-time dynamic attacker containment limits security incident impact
- Works with multi-vendor enterprise edge switching products

PROTECTS TODAY'S AND TOMORROW'S NEXT GENERATION NETWORKS

- Protection against emerging Voice over IP vulnerabilities, Day Zero threats, and advanced Denial of Service attacks
- Delivers leading price point and proven effectiveness at Gigabit, Multi-Gigabit
- Flexibly deployed as an appliance and/or virtual appliance enabling cost efficient threat detection and monitoring for both the physical and virtual networks
- Supports inspection and reporting for IPv6 networks extending IPS/IDS capabilities into next generation networks

INDUSTRY-LEADING INTRUSION PREVENTION AND RESPONSE

- Unmatched threat detection and containment that leverages sophisticated signature, application, protocol, and behavioral analysis
- Unique host-based and network-based protection deployment options

LEVERAGES YOUR EXISTING INFRASTRUCTURE INVESTMENTS AND IT EXPERTISE

- Ready to protect "out-of-the-box" with powerful configuration tools for customization and advanced control
- No fork lift upgrades – works with your existing network switches, routers, wireless access points, and security appliances

Threat containment that leverages existing network investments

In-line Intrusion Prevention deployment to provide advanced security in a specific location

Patented Distributed Intrusion Prevention deployment to automate response to threats in real-time

Out-of-band Intrusion Detection deployment that simultaneously utilizes multiple response technologies

Forensics tools for session reconstruction to simplify threat mitigation and resolution

Product Overview

The Extreme Networks Intrusion Prevention System (IPS) is unique in its ability to gather evidence of an attacker's activity, remove the attacker's access to the network, and reconfigure the network to resist the attacker's penetration technique. The IPS stops attacks at the source of the threat and can proactively protect against future threats and vulnerabilities. Offering an extensive range of detection capabilities, host-based and network-based deployment options, a portfolio of IPS appliances, and seamless integration with the Extreme Networks Secure Networks™ architecture, our IPS utilizes a state-of-the-art high-performance, multi-threaded architecture with virtual sensor technology that scales to protect even the largest enterprise networks.

The Intrusion Prevention System is a core component of the Extreme Networks Secure Networks architecture. When deployed in combination with Extreme Networks SIEM and NMS Automated Security Manager (ASM), it facilitates the automatic identification, location, isolation, and remediation of security threats. Extreme Networks IPS also integrates seamlessly with Extreme Networks Network Access Control (NAC) for post-connect monitoring of behavior once network access has been granted.

Extreme Networks advanced in-line Intrusion Prevention is designed to block attackers, mitigate Denial of Service (DoS) attacks, prevent information theft, and ensure the security of Voice over IP (VoIP) communications - while remaining transparent to the network. Built upon our award-winning intrusion prevention technology, Extreme Networks IPS can alert on the attack, drop the offending packets, terminate the session for TCP and UDP-based attacks, and dynamically

establish firewall or Secure Networks™ policy rules. Extreme Networks IPS leverages a comprehensive library of vulnerability and exploit-based signatures.

Extreme Networks' Distributed Intrusion Prevention (US Patent 7581249) and threat containment can block attackers at the source physical port for most multi-vendor edge switches. More granular business-oriented visibility and control based on user and application policy is provided when Extreme Networks switching products are deployed at the network edge. Effective threat containment requires the removal of the attacker's ability to continue the attack or to mount a new attack. The Extreme Networks Distributed Intrusion Prevention System identifies a threat or security event, locates the exact physical source of the event, and mitigates the threat through the use of enforceable bandwidth rate limiting policies, quarantine policies, or other port level controls.

Extreme Networks out-of-band Intrusion Detection is unmatched in detecting and reporting security events, including external intrusions, network misuse, system exploits, and virus propagations. It utilizes the industry's most sophisticated multi-method detection technologies by integrating vulnerability pattern matching, protocol analysis, and anomaly-based detection with specific support for VoIP environments. Application-based event detection detects non-signature-based attacks against commonly targeted applications such as HTTP, RPC, and FTP.

Intrusion Prevention sensors come ready to use "out-of-the-box" and easily integrate with your existing network infrastructure and security appliances. Extreme Networks Intrusion Prevention ships with a comprehensive set of pre-installed signatures, VoIP protocol decoders for SIP, MGCP, and H.323 protocols, and advanced detection of malformed messages to help prevent DoS attacks. Extreme Networks IPS supports both IPv4 and IPv6 networks.

Network Sensors are security appliances that offer market-leading deep forensics capabilities, including flexible packet capture and complete session reconstruction. Network Sensors are centrally managed via the Enterprise Management Server (EMS). EMS provides configuration management, status monitoring, live security updates, and a secure encrypted communications channel.

Network Sensors utilize an adaptive match engine and multi-threaded application execution to significantly enhance performance. Sensors support the use of multiple detection algorithms simultaneously, thereby optimizing traffic analysis to match the prevalent traffic type.

Security Administrators have broad flexibility in deploying Network Sensors. For example, a single sensor may operate as multiple "virtual sensors", each associated with a particular VLAN, Layer 3 network, physical switch port or TCP / UDP level application. Each virtual sensor can be configured with unique policies that define the analysis techniques used and alerts generated.

Network Sensors are available at 1 Gbps and Multi-Gigabit deep packet inspection throughput rates.

HOST-BASED THREAT PREVENTION

Extreme Networks Host Sensors are security applications used to detect attacks on a network server in real time. Extreme Networks Host Sensors monitor individual systems running today's most common operating systems for evidence of malicious or suspicious activity in real time. Host Sensors use a variety of techniques to detect attacks and misuse, including analyzing the security event log, and checking the integrity of critical configuration files. This hybrid approach helps organizations meet compliance requirements mandated by regulations including PCI, HIPAA and Sarbanes-Oxley.

Extreme Networks Host Sensors perform the following functions:

- Monitor file attributes such as file permission, owner, group, value, size increase, truncated and modification date
- Check file integrity to determine whether content of critical files was changed
- Continuously analyze log files using signature policies to detect attacks and/or compromises
- Monitor Windows event logs for misuse or attack
- Analyze Windows registry for attributes that should not be accessed and/or modified
- Perform TCP/UDP service detection for protection against backdoor services

Extreme Networks Host Sensors support custom module development using Microsoft's .NET Framework. This allows users to leverage the power and flexibility of the .NET framework to customize Extreme Networks functionality to meet their needs.

The optional Host Sensor Web Intrusion Prevention System (Web IPS) module protects against common attacks on web servers running Microsoft IIS and Apache. The Web IPS module works in conjunction with the Host Sensor to provide protection while operating with minimal overhead on the system. The Web IPS provides threat prevention for a large array of attacks and can terminate individual malicious sessions.

ENTERPRISE MANAGEMENT SERVER (EMS)

Extreme Networks Enterprise Management Server (EMS), with its client-server architecture, offers efficient, centralized management for all of the components offered with Extreme Networks IPS. The EMS provides reporting and management services for all deployed network and host sensors. Management services include remote sensor upgrades, signature updates, configuration updates and event alerting via email, Syslog, OPSEC, SNMPv1/v3 and custom scripting. Reporting services include real-time alerting, forensics, trend analysis and executive reporting. Distributed IPS is available via Extreme Networks NMS Automated Security Manager.

EMS configuration wizards and group policy rules simplify the configuration of network and host sensors. The EMS aggregates event reporting from individual network and host sensors. It can execute firewall rule changes, switch/router configurations, or other mitigation actions in response to attacks.

The EMS provides in-depth reporting and archiving of security event and network activity. This information may be used for regulatory compliance, audit trail analysis, forensics, and real-time trending. It is also tightly integrated with the Extreme Networks Security Information & Event Manager solution for more advanced reporting capabilities.

EXTREME NETWORKS IPS VIRTUAL APPLIANCES

Extreme Networks IDS network sensor and Enterprise Management Server (EMS) can be deployed on VMware ESX™ servers. With these virtual machine options, enterprises gain additional, cost-efficient, network threat protection and the ability to monitor both the physical and virtual network. Leverage the enterprise's virtual environment for added security with the benefits of cost savings from using existing hardware, and reduced time to value.

CERTIFICATIONS AND PARTNERSHIPS

Extreme Networks is a partner in the Microsoft Active Protection Program (MAPP). This program, from the Microsoft Security Response Center (MSRC), provides detailed vulnerability information in advance of any public disclosure. This enables our research team to synchronize the availability of appropriate signatures with Microsoft vulnerability announcements, thereby bridging the gap between those announcements and security patch installation for IT departments.

Appliance Specifications

DRAGON IPS NETWORK SENSOR APPLIANCES		
MODEL	**DNIPS-A1-G**	**DNIPS-A1-MG**
IPS Throughput	1,200 Mbps	8,000 Mbps
Max I/O Modules	6	6
Bypass I/O Modules	4x1 Gbps copper, 4x1 Gbps fiber	n/a
Standard I/O Modules	4x1 Gbps copper, 4x1 Gbps fiber	4x1 Gbps copper, 4x1 Gbps fiber, 2x10 Gbps SR
Management Interfaces	4x1 Gbps copper	4x1 Gbps copper
Remote Console	Yes	Yes
Typical Latency	< 800 microseconds	< 300 microseconds
Processor	2 x E5-2603 Quad Core, 1.8 Ghz	2 x E5-2620 Hex Core, 2.0 Ghz
Memory	6 GB	12 GB
Hard Drives	2 x 1 TB SATA	2 x 1 TB SATA
Power Supplies	Dual 750W	Dual 750W
Dimensions (D x W x H in cm)	73.2 x 43.8 x 8.76	73.2 x 43.8 x 8.76
Shipping Weight (kgs)	28.1	28.1
Operating Temperature	10° c – 35° c	10° c – 35° c

AGENCY AND REGULATORY STANDARD SPECIFICATIONS

Safety: UL 60950-1, CSA 22.1 60950, EN 60950-1, and IEC 60950-1, NOM
EMC: FCC Part 15 (Class A), ICES-003 (Class A), BSMI, KCC, VCCI V-3, AS/NZS CISPR 22 (Class A), EN 55022 (Class A), EN 55024, EN 61000-3-2, EN 61000-3-3

DRAGON ENTERPRISE MANAGEMENT SERVER APPLIANCES		
MODEL	**DEMS-A1-25**	**DEMS-A1-U**
Management Capacity	25 Nodes	Unlimited (5000)
Management Interfaces	4x1 Gbps copper	4x1 Gbps copper
Remote Console	Yes	Yes
Processor	1 x E5-2620 Hex Core, 2.0 Ghz	1 x E5-2620 Hex Core,
Memory	12 GB	2.0 Ghz
Hard Drives	2 x 500 GB	12 GB
Power Supplies	Dual 750W	6 x 2 TB
Dimensions (D x W x H in cm)	73.4 x 43.8 x 4.32	Dual 750W
Shipping Weight (kgs)	23.1	73.2 x 43.8 x 8.76
Operating Temperature	10° c – 35° c	28.1

VIRTUAL APPLIANCES

System Requirements

The EMS and Network Sensor virtual appliances are packaged in the OVA file format, which is a one-file alternative to the Open Virtualization Format, an ANSI standard. Extreme Networks fully supports these virtual appliances when run on a VMware ESX or ESXi version 4.1 and higher with sufficient resources.

The EMS virtual appliance requires 4 GB of memory, two CPU cores, and 60 GB of thick provisioned hard drive space. The Network Sensor virtual appliance requires 2 GB of memory, two CPU cores, and 20 GB of thick provisioned hard drive space. Additional CPU and memory resources may enhance the performance of some configurations.

HOST SENSOR

System Requirement

Extreme Networks Host Based Sensors offer broad platform support including Microsoft® Windows, Solaris, Red Hat Enterprise Linux, HP-UX, Fedora Core, SUSE and AIX. Extreme Networks IPS Host Sensors are also supported when installed on any supported O/S that is itself running on a virtual machine of a VMware ESX Server, AIX 5.3 and 6.1 running in logical partitions (LPARS), and on Solaris 10 running in logical domains (LDOMS) on supported platforms.

Web IPS supports Apache with Linux servers, plus Microsoft IIS 5 and IIS 6 for Microsoft Windows 2000, Windows XP, and Windows 2003 servers.

Ordering Information

IDS NETWORK SENSOR SOFTWARE / VIRTUAL APPLIANCES

PART NUMBER	DESCRIPTION
DNIDS-V-100	Network IDS software, 100 Mbps limit
DNIDS-V-250	Network IDS software, 250 Mbps limit
DNIDS-V-500	Network IDS software, 500 Mbps limit
DNIDS-V-1000	Network IDS software, 1 Gbps limit

HOST SENSOR SOFTWARE

PART NUMBER	DESCRIPTION
DSHSS7-U-LIC	Host Sensor Software License (Unlimited pack)
DSHSS7-10K-LIC	Host Sensor Software License (10,000 pack)
DSHSS7-100-LIC	Host Sensor Software License (100 pack)
DSHSS7-1-LIC	Host Sensor Software License (Single)
DSHSS7-25-LIC	Host Sensor Software License (25 pack)
DSHSS7-500-LIC	Host Sensor Software License (500 pack)

ENTERPRISE MANAGEMENT SERVER (EMS) APPLIANCES

PART NUMBER	DESCRIPTION
DEMS-A1-U	EMS Appliance, 6 x 2 TB, Manages unlimited nodes
DEMS-A1-25	EMS Appliance, 2 x 500 GB, Manages up to 25 nodes

ENTERPRISE MANAGEMENT SERVER SOFTWARE / VIRTUAL APPLIANCES

PART NUMBER	DESCRIPTION
DSEMS7-ME	EMS Software - Medium Enterprise, manages up to 25 nodes
DSEMS7-LE	EMS Software - Large Enterprise, manages up to 100 nodes
DSEMS7-SE	EMS Software - Small Enterprise, manages up to 2 nodes
DSEMS7-U	EMS Software - Unlimited, no managed node limit

IPS NETWORK SENSOR APPLIANCES

PART NUMBER	DESCRIPTION
DNIPS-A1-G	Network GIG IPS Appliance
DNIPS-A1-MG	Network Multi-Gigabit IPS Appliance

NETWORK INTERFACE CARD (NIC) OPTIONS FOR GIG IPS APPLIANCES

PART NUMBER	DESCRIPTION
DNIC-4PORT-TX	4-port, triple speed copper NIC
DNIC-4PORT-SX	4-port, fiber NIC
DNICFO-4PORT-TX	4-port, triple speed fail open copper NIC
DNICFO-4PORT-SX	4-port, fail open fiber NIC

NETWORK INTERFACE CARD (NIC) OPTIONS FOR MG IPS APPLIANCES

PART NUMBER	DESCRIPTION
DNIC-HS2X10G-S	MG NIC, 2-port, 10 Gig SR
DNIC-HS4PORT-SX	MG NIC, 4-port fiber
DNIC-HS4PORT-TX	MG NIC, 4-port triple speed copper

DISTRIBUTED INTRUSION PREVENTION**

PART NUMBER	DESCRIPTION
NMS-XXX	Network Management Suite (NMS) with Console (including Wireless Management), Policy, Inventory, Automated Security (ASM), NAC, OneView and Mobility. Available for a range of licensed devices and thin APs.

***Requires at least one of the IPS or IDS Network Sensors*

Warranty

As a customer-centric company, Extreme Networks is committed to providing quality products and solutions. In the event that one of our products fails due to a defect, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired or media replaced as soon as possible.

Extreme Networks Intrusion Prevention System appliances come with a one year warranty against manufacturing defects. For full warranty terms and conditions please go to: http://www.ExtremeNetworks.com/support/warranty.aspx.

Service and Support

Extreme Networks provides comprehensive service offerings that range from Professional Services to design, deploy and optimize customer networks, customized technical training, to service and support tailored to individual customer needs. Please contact your Extreme Networks account executive for more information about Extreme Networks Service and Support.

Extreme networks

http://www.ExtremeNetworks.com/contact / Phone +1 408 579 2800