

# Intrusion Prevention System (IPS)

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



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 Enterasys 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 Enterasys Secure Networks<sup>™</sup> 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 Enterasys Secure Networks architecture. When deployed in combination with Enterasys SIEM and NMS Automated Security Manager (ASM), it facilitates the automatic identification, location, isolation, and remediation of security threats. Enterasys IPS also integrates seamlessly with Enterasys Network Access Control (NAC) for post-connect monitoring of behavior once network access has been granted.

Enterasys 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, Enterasys 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<sup>™</sup> policy rules. Enterasys IPS leverages a comprehensive library of vulnerability and exploit-based signatures.

Enterasys' 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 Enterasys 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 Enterasys 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.

## 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, and 10 Gigabit performance

### 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

**There is nothing more important than our customers.**

---

Enterasys 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. Enterasys 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.

**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 100 Mbps, 250 Mbps, 500 Mbps, 1 Gbps, and Multi-Gigabit deep packet inspection throughput rates.

- Multi-Gigabit Network Sensors are appliances for high-performance data centers. They support Multi-Gigabit data rates and include two onboard ports. The two rack unit (2RU) appliance offers 10 GbE and 1 GbE network connectivity options.
- Gigabit Network Sensors are appliances for high-performance data centers. They support 1 Gbps data rates and include two onboard ports plus two dual-port fiber or two dual-port 10/100/1000 copper LAN interfaces.
- GE500 Network Sensors appliances support 500 Mbps data rates and include two onboard ports plus one dual-port fiber or one dual-port 10/100/1000 copper LAN interface.
- GE250 Network Sensors are appliances for regional office and similar locations. They support 250 Mbps data rates and include two onboard ports plus one dual-port fiber or one dual-port 10/100/1000 copper LAN interface.
- FE Network Sensors are appliances for branch office and similar locations. They support 100 Mbps data rates and include two onboard ports plus one dual-port 10/100/1000 copper LAN interface.

#### **Host-Based Threat Prevention**

Enterasys Host Sensors are security applications used to detect attacks on a network server in real time. Host intrusion detection is particularly valuable in environments where AES, SSL, IPsec, or other encryption schemes are deployed because the sensor analyzes the decrypted data. Enterasys 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, checking the integrity of critical configuration files, and checking for kernel level compromises. This hybrid approach helps organizations meet compliance requirements mandated by regulations including PCI, HIPAA and Sarbanes-Oxley.

---

Enterasys 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
- Monitor the kernel to detect suspicious privilege escalations and other signs of kernel-level compromises such as rootkits.

Enterasys 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 Enterasys 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)**

Enterasys Enterprise Management Server (EMS), with its client-server architecture, offers efficient, centralized management for all of the components offered with Enterasys IPS. The EMS provides reporting and management services for all deployed network and host sensors. Management services include binary 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 Enterasys 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 Enterasys Security Information & Event Manager solution for more advanced reporting capabilities.

#### **Event Flow Processor**

Event Flow Processor (EFP) is a security appliance used to scale Intrusion Prevention deployments for very large networks. Event flow processors are strategically placed on the network to aggregate event data from multiple network and host sensors, and report to the centralized Enterprise Management Server. This is particularly useful for organizations with multiple high traffic remote sites.

#### **Certifications and Partnerships**

Enterasys Intrusion Prevention has achieved Common Criteria certification. The Common Criteria evaluation process ensures IT products conform to international security standards. The program is a partnership between the public and private sectors in the United States and Europe designed to help government organizations select commercial IT products that meet strict security requirements.

Enterasys 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.

# Specifications\*

## Network Sensor 1U Appliances

(Revision 5x appliances)

### Chassis

Form Factor: 1U Rack  
Height: 1.68" (4.27 cm)  
Width: 17.60" (44.70 cm)  
Depth: 21.50" (54.61 cm)  
Weight: ~ 26.0 lbs. (11.80kg)

### Power

Single power supply (345W)

### Environmental

Operating Temperature: 10° to 35°C (50° to 95°F)  
Operating Relative Humidity: 20% to 80% (non-condensing) with a maximum humidity gradation of 10% per hour  
Operating Maximum Vibration: 0.25 G's 0-Peak, 3-200 HZ sweep @ 1/2 Octaves/minute  
Operating Maximum Shock: 31G, 2.6ms, 20inch/sec, bottom side  
Operating Altitude: -16 to 3048 m (-50 to 10,000 ft.)  
Storage Temperature: -40° to 65°C (-40° to 149°F)  
Storage Relative Humidity: 5% to 95% (non-condensing)  
Storage Maximum Vibration: 1.54 GRMS - 6 sides @ 15 min/side  
Storage Maximum Shock: 71G, 2ms, 35inch/sec, 6 sides; 32G, 2ms, 270inch/sec, 6 sides  
Storage Altitude: -16 to 10,600 m (-50 to 35,000 ft.)

### Regulatory

FCC Part 15 Class A  
EN61000-3-2, A1, A2: Current Harmonics  
EN61000-3-3: Voltage Flicker  
EN55022: 1998 and CISPR 22: 1997 Class A  
VCCI Class 1  
MIC Class A  
BSMI  
EN55024: 1998 and CISPR 24: 1997  
IEC 61000-4-2: Electrostatic Discharge specification  
IEC 61000-4-3: Radiated Immunity  
IEC 61000-4-4: EFT/Bursts Immunity  
IEC 61000-4-5: Surge Immunity  
IEC 61000-4-6: Conducted Immunity 0.15-80MHz  
IEC 61000-4-8: Power Frequency H-Field  
IEC 61000-4-11: Voltage Dips/Interrupts/Variations  
EN60950-1, First Edition: Standard for Information Technology Equipment - Safety-Part 1: General Requirements  
IEC 60950-1, First Edition (2001)  
UL/CSA 60950-1, First Edition: Standard for Information Technology Equipment -Safety-Part 1: General Requirements  
EK1-ITB 2000:2003: Ergonomics  
ISO 9241: VDT Ergonomic Requirements  
ZH1/618:GS-VW-SG7:1997: Ergonomics  
ISO 13406-2: Ergonomic requirements for work with visual displays based on flat panels  
ISO 7779: Sound Pressure at Operator Position (Acoustics)  
MsanPiN 001-96: Interstate Sanitary rules and norms (Acoustics)

\*Specifications refer to Enterasys appliance revision 6A or higher unless otherwise noted. Enterasys reserves the right to substitute alternative hardware that meets or exceeds the specifications in this datasheet.

## Network Sensor 2U Appliances

### EMS with Dual Power 2U Appliance

### Chassis

Form Factor: 2U Rack  
Height: 3.4" (8.64cm)  
Width: 17.44" (44.31cm) without latches  
Depth: 26.8" (68.07cm)  
Weight: 57.54 lbs (26.1 Kg), maximum configuration

### Power

Dual power supplies (570W)

### Environmental

Operating Temperature: 10° C to 35° C (50° F to 95° F)  
Storage Temperature: -40° C to 65° C (-40° F to 149° F)  
Operating Relative Humidity: 20% to 80% non-condensing  
Maximum humidity gradient: 10% per hour, operational and non-operational conditions.  
Storage Relative Humidity: 5% to 95% non-condensing  
Operating Altitude: -16 to 3,048m (-50 ft to 10,000 ft) Storage Altitude: -16m to 10,600m (-50 ft to 35,000 ft)

### 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

## EMS with Dual Power 1U Appliance

### Chassis

Form Factor: 1U Rack  
Height: 1.68" (4.26cm)  
Width: (42.4cm) without rack latches  
Depth: 30.4" (77.2cm)  
Weight: 39 lbs (17.7 Kg), maximum configuration

### Power

Dual power supplies (502W)

### Environmental

Operating Temperature: 10° C to 35° C (50° F to 95° F)  
Storage Temperature: -40° C to 65° C (-40° F to 149° F)  
Operating Relative Humidity: 20% to 80% non-condensing  
Maximum humidity gradient: 10% per hour, operational and non-operational conditions.  
Storage Relative Humidity: 5% to 95% non-condensing  
Operating Altitude: -16 to 3,048m (-50 ft to 10,000 ft) Storage Altitude: -16m to 10,600m (-50 ft to 35,000 ft)

## 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

## Ordering Information

### IPS Network Sensors

Part Number	Description
DIPA-MG	Network Multi-Gigabit IPS Appliance (NICs ordered separately)
DIPA-GIG-TX	Network GIG IPS Appliance - includes two 2 port Copper Fail-safe bypass NICs
DIPA-GIG-SX	Network GIG IPS Appliance - includes two 2 port Fiber Fail-safe bypass NICs
DIPA-GE500-TX	Network GE500 IPS Appliance - includes 2 port Copper Fail-safe bypass NIC
DIPA-GE500-SX	Network GE500 IPS Appliance - includes 2 port Fiber Fail-safe bypass NIC
DIPA-GE250-TX	Network GE250 IPS Appliance - includes 2 port Copper Fail-safe bypass NIC
DIPA-GE250-SX	Network GE250 IPS Appliance - includes 2 port Fiber Fail-safe bypass NIC
DIPA-FE-TX	Network Fast Ethernet IPS Appliance - includes 2 port Copper Fail-safe bypass NIC

### IDS Network Sensors

Part Number	Description
DNSA-MG	Multi-Gigabit Network Sensor Appliance (NICs ordered separately)
DNSA-GIG-TX	Gigabit Network Sensor Appliance - includes two 2 port Copper NICs
DNSA-GIG-SX	Gigabit Network Sensor Appliance - includes two 2 port Fiber NICs
DNSA-GE500-TX	GE500 Network Sensor Appliance - includes 2 port Copper NIC
DNSA-GE500-SX	GE500 Network Sensor Appliance - includes 2 port Fiber NIC
DNSA-GE250-TX	GE250 Network Sensor Appliance - includes 2 port Copper NIC
DNSA-GE250-SX	GE250 Network Sensor Appliance - includes 2 port Fiber NIC
DNSA-FE-TX	Network Fast Ethernet IDS Appliance - includes 2 port Copper NIC

## Host Sensor

### System Requirements

Enterasys Host Based Sensors support Microsoft® Windows XP Professional, Windows Server 2003, Windows Vista, Linux, AIX, Solaris, Fedora Core, CentOS and HP-UX. The Host Sensor is also supported on any supported operating system that is running on a virtual machine of a VMware ESX Server v3.0 host.

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

### Host Sensors

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)
DSHSS7-WEBIPS	Host Sensor Software for Web IPS

### Enterprise Management Server (EMS)

Part Number	Description
DEMA-ME	Enterprise Management Server Appliance - Medium Enterprise, manages up to 25 nodes
DEMA-LE	Enterprise Management Server Appliance - Large Enterprise, manages up to 100 nodes
DEMA-U	Enterprise Management Server Appliance - Unlimited managed nodes
DEPA	Event Flow Processor Appliance
DISA-TX	Integrated Network Sensor/Server (Copper NIC), 250Mbps, contains EMS for up to 2 nodes
DISA-SX	Integrated Network Sensor/Server (Fiber NIC), 250Mbps, contains EMS for up to 2 nodes
DEMA-RED-U	Enterprise Management Server Appliance - Redundant power & drive, manages unlimited nodes
DEMA-6RED-U	Enterprise Management Server Appliance, 6X500 GB, manages unlimited nodes

## Network Interface Card (NIC) options for IPS appliances

Part Number	Description
<b>DNIC-2PORT-TX</b>	2-port, triple speed copper NIC
<b>DNIC-2PORT-SX</b>	2-port, fiber NIC
<b>DNICFO-2PORT-TX</b>	2-port, triple speed fail open copper NIC
<b>DNICFO-2PORT-SX</b>	2-port, fail open fiber NIC
<b>DNIC-4PORT-TX</b>	4-port, triple speed copper NIC
<b>DNIC-4PORT-SX</b>	4-port, fiber NIC
<b>DNICFO-4PORT-TX</b>	4-port, triple speed fail open copper NIC
<b>DNICFO-4PORT-SX</b>	4-port, fail open fiber NIC
<b>DNIC-2X10G-SR</b>	2-port, 10Gbps, fiber NIC (compatible with DIPA-MG and DNSA-MG only)
<b>DNICFO-2X10G-SR</b>	2-port, 10Gbps, fail open, fiber NIC (compatible with DIPA-MG and DNSA-MG only)

## Distributed Intrusion Prevention\*\*

Part Number	Description
<b>NS-AB-50</b>	Network Management Suite Advanced Bundle 50-devices (50 device Console license for 1 server plus 3 concurrent users with Policy Manager, Automated Security Manager, Inventory Manager, and NAC Manager)
<b>NS-AB-50FT</b>	Network Management Suite Advanced Bundle 50-devices FT (50 device Console license for 1 server plus 3 concurrent users, Policy Manager, Automated Security Manager, Inventory Manager, NAC Manager, a redundant NMS license for fault tolerance (manual failover), includes Lab License)
<b>NS-AB-U</b>	Network Management Suite Advanced Bundle Unrestricted (Unrestricted device Console license for 1 server plus 25 concurrent users with Policy Manager, Automated Security Manager, Inventory Manager, and NAC Manager)
<b>NS-AB-UFT</b>	Network Management Suite Advanced Bundle Unrestricted FT (Unrestricted device Console license for 1 server plus 25 concurrent users, Policy Manager, Automated Security Manager, Inventory Manager, and NAC Manager, a redundant NMS license for fault tolerance (manual failover), includes Lab License)

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

## Warranty

As a customer-centric company, Enterasys 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.

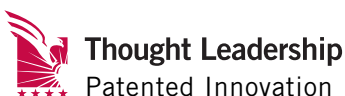
Enterasys Intrusion Prevention System appliances come with a one year warranty against manufacturing defects. For full warranty terms and conditions please go to: <http://www.enterasys.com/support/warranty.aspx>.

## Service and Support

Enterasys 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 Enterasys account executive for more information about Enterasys Service and Support.

## Contact Us

For more information, call Enterasys Networks toll free at **1-877-801-7082**, or +1-978-684-1000 and visit us on the Web at [enterasys.com](http://enterasys.com)



© 2010 Enterasys Networks, Inc. All rights reserved. Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications. Please visit <http://www.enterasys.com/company/trademarks.aspx> for trademark information.

