



IASM 3100 Appliance

IASM™ 3100 Appliance Capabilities

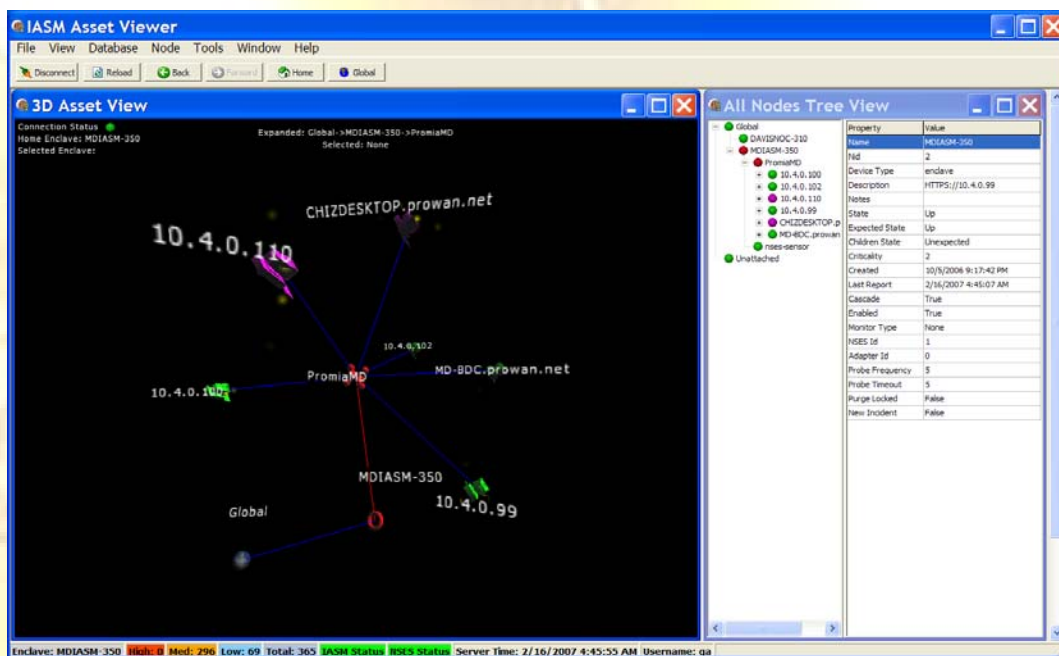


The IASM 3100 is hardened Security Asset, Event, and Incident Management appliance that was developed in collaboration with, and is scheduled for deployment to, U.S. Navy Carrier class ships. The IASM 3100 appliance consists of 4 distinct hardware units. The first is the Manager unit, which implements many of the IASM features, including Management, Analysis, and the Repository. The Management features includes both features for: identifying site-specific appropriate policy-driven responses, incident validation, and incident closure (after operator remediation of the problem) and the secure web-based IASM 3100 user interface for accessing those features. The Analytics feature runs software that detects operational and security incidents that would not otherwise be visible from any single sensor. The software uses a unique combination of expert system and statistical aggregation and correlation algorithms to analyze events from multiple sensor sources. An additional result of the algorithms is a natural language description of the kind of incident detected. The Repository feature consolidates and stores the logged event records from many commercial NIDS, HIDS, firewalls, VPN appliances, routers, host operating systems, and software applications into a unified online repository. The event records are actually collected, filtered, and forwarded by intelligent IASM software agents that have been placed at strategic locations on the network. The second is the Sony Lib-81 AIT-3 tape archival unit, to which operators can archive 180+ days of old incidents. The third is the Network Security Event Sensor (NSES) unit, which currently has three network traffic sensors. One sensor passively identifies, fingerprints, and maps network assets while the second detects anomalous IP traffic – which often indicates previously unknown network attacks. The third sensor uses the Snort engine to compare network packets with “Bleeding Edge” attack signature patterns that have been developed the Snort community and independently tested by Promia. The NSES unit includes filters that use local knowledge to eliminate false positive events, aggregate consecutive instances of the same event, and filter events according to white- and black-lists of IP addresses. Finally, the NSES unit also can record 1-60 second "snapshots" of IP traffic both before and after a security event for later remote forensic review by skilled incident analysis personnel. The fourth is a CISCO switch unit for interconnecting the appliance units and the protected network.



Promia Asset Viewer Graphical User Interface

The IASM 3100 comes with the Promia Asset Viewer GUI, shown below, which presents a flexible, powerful, 3-Dimensional, consolidated visualization of all assets and incidents on the monitored network. The AV shows versions and patch levels of node operating systems, device and application status, ports in use, and other related information. The AV enables an operator to navigate among multiple network segments being monitored by Promia NSES appliances, thus exposing the contextual relationship between those segments. The AV provides a real-time tactical status view of the IASM incidents and the operation status of the IASM and NSES appliances.

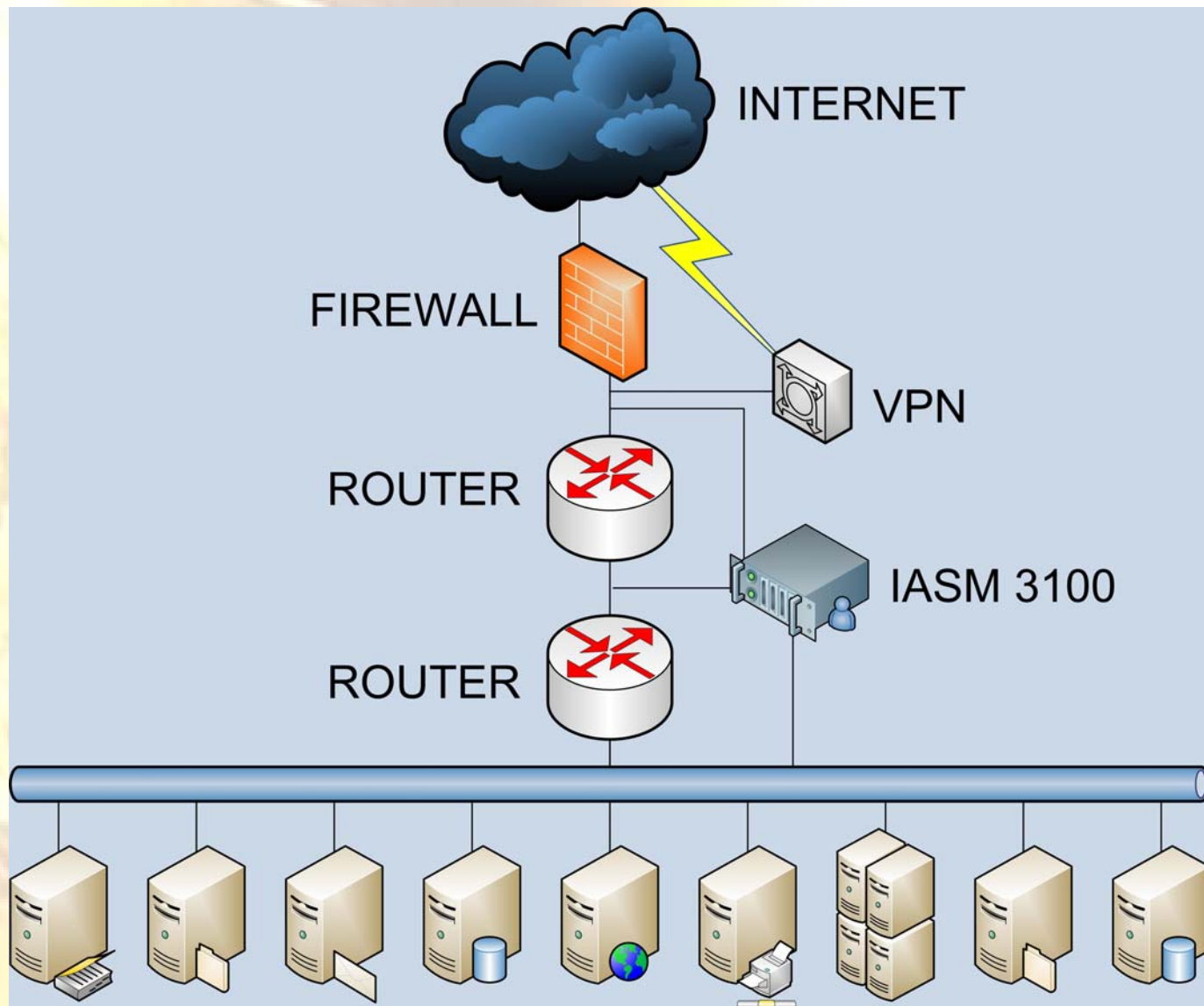


Regional or Departmental Security Management

The IASM 3100 Appliance is capable of monitoring and managing the regional or departmental security operations of a large enterprise. While it can be deployed alone for network protection of a medium-sized network, the IASM 3100 Appliance is most effective when used to consolidate events coming in from a group of individual network segments that are geographically or logically related to each other: as shown in the diagram, below.



IASM 3100 Appliance



For more information, please contact:

PROMIA, Inc

160 Spear Street, Suite 320

San Francisco, CA 94105

415-536-1600 (Phone)

415-536-1616 (Fax)

sales@promia.com



IASM 3100 Appliance

Promia IASM 3100 Appliance Technical Specifications

	IASM 3100 Manager Unit	IASM 3100 NSES Unit
Enclosure	2U Rack mount SATA Server Case with 400W Power Supply and 4 SATA Hotswap drive bays	1U Rack mount SATA Server Case with 400W Power Supply and 4 SATA Hotswap drive bays
CPU/Motherboard	<ul style="list-style-type: none"> • Dual CPU Tyan Opteron EATX MB with 2 single-core 2.2 GHz Opteron processors • 16GB PC2700 ECC Registered DDR SDRAM (8 x 2GB packages) • 3Ware 8506-8 64-bit/66MHz PCI 8-channel SATA Raid C/C 	
Storage	<ul style="list-style-type: none"> • 8 x 250GB RAID SATA drives (7200 rpm, 8MB buffer) • 1 x Slim 8x DVD±RW Drive, Double Layer • 1 x Slim 3.5" 1.44MB Internal Floppy Disk Drive 	<ul style="list-style-type: none"> • 2 x 250GB RAID SATA drives (7200 rpm, 8MB buffer) • 1 x Slim 8x DVD±RW Drive, Double Layer • 1 x Slim 3.5" 1.44MB Internal Floppy Disk Drive
Interfaces	<ul style="list-style-type: none"> • 2 x USB 2.0 • 2 x RJ45 for 10/100/1000 MBs Ethernet 	<ul style="list-style-type: none"> • 2 x USB 2.0 • 6 x RJ45 for 10/100/1000 MBs Ethernet
Operating System	<ul style="list-style-type: none"> • Suse Linux Enterprise Server 9.0 Operating System <ul style="list-style-type: none"> ◦ Security hardened according to US DISA Linux STIG guidance 	
Java Runtime	<ul style="list-style-type: none"> • Sun Java Runtime Environment 5.0 Update 11 (Linux version) <ul style="list-style-type: none"> ◦ Security hardened according to US DISA JRE STIG guidance 	
Database	<ul style="list-style-type: none"> • PostgreSQL v8.2.3 <ul style="list-style-type: none"> ◦ Security hardened according to US DISA database STIG guidance 	
Proprietary	<ul style="list-style-type: none"> • Promia IASM 1.2.2 Core Services • Promia IASM 1.2.2 Analytic services • Promia IASM 1.2.2 Multi-collector services • Promia Asset Viewer v0.9 	<ul style="list-style-type: none"> • NSES Core v7.1

IASM 3100 Tape Archival Unit	IASM 3100 Network Switch Unit
<ul style="list-style-type: none"> • Sony Lib-81 AIT-3 Tape Archive System 	<ul style="list-style-type: none"> • CISCO 24-port switch