



Raven UTM Appliance

Raven UTM™ Appliance Capabilities



The Raven UTM (Unified Threat Management) 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 Raven UTM appliance consists of two small 1U half-depth hardened units. Included is a Manager Software unit, which implements many of the Raven 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 Raven 1100 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 the proprietary Promia Raven Sensor Unit. The Sensor Unit can be configured in either passive listening mode or in TAP mode which connects in-line in a network (failing open) and can optionally perform as an Intrusion Prevention System.

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 Raven software agents that have been placed at strategic locations on the network.

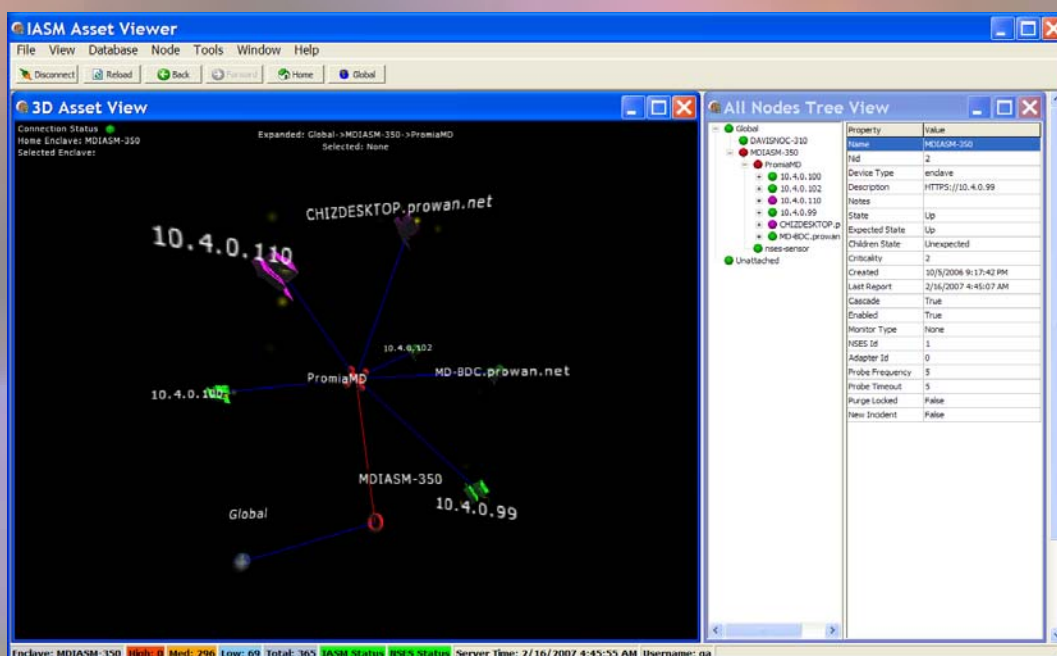
Another component is the Promia Raven Sensor unit, which currently has three network traffic sensors. One sensor passively identifies, fingerprints, and maps network assets while the second detects anomalous IP traffic – which often indicates previously unknown network attacks. The third sensor uses 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 Raven Sensor 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. The Raven Sensor Units have the capability to dynamically block network traffic based upon user set conditions.



Raven UTM Appliance

Promia Asset Viewer Graphical User Interface

The Raven UTM 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 Raven incidents and the operation status of the Raven appliance.

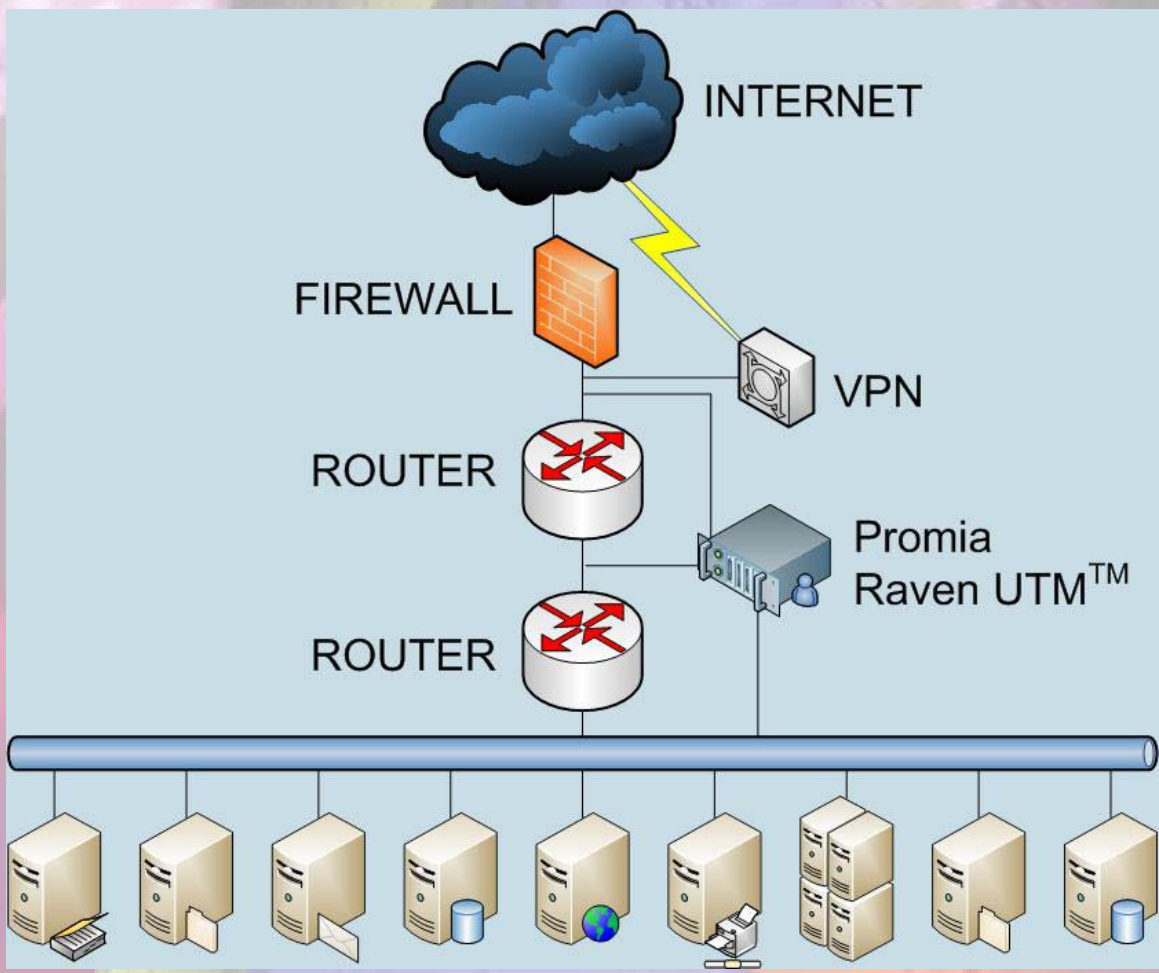


Regional or Departmental Security Management

The Raven UTM 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 Raven UTM 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.



Raven UTM 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



Raven UTM Appliance

Promia Raven UTM Appliance Technical Specifications Manager Unit

Form Factor	19" 1U chassis, P4 system platform with LAN bypass
LAN	PCI-E 10/100/1000Mbps LAN x 6 with dual latch GbE LAN bypass PCI 32bit/33MHz 10/100/1000Mbps LAN x 2
CF Socket	Onboard (Primary Channel)
Power Supply	350W ATX Power Supply
USB	USB 2.0 x 4 (2 at front, 1 optional at rear, 1 pin header)
LCM Support	Yes
CPU	Intel Pentium Core 2 Duo E6400 2.13GHz 1066MHz FSB 4MB L2 Cache
PCI Riser Card	PCI-X 64bit/133MHz 3.3V/5V PCI add-on card
Memory	2GB DDRII (1GB x 2)
Hard Drive	Seagate Barracuda 7200.8: 250GB SATAII 7200RPM 3.5"HDD

Promia Raven UTM Appliance Technical Specifications Sensor Unit

Form Factor	19" 1U chassis, P4 system platform with LAN bypass
LAN	PCI-E 10/100/1000Mbps LAN x 6 with dual latch GbE LAN bypass PCI 32bit/33MHz 10/100/1000Mbps LAN x 2
CF Socket	Onboard (Primary Channel)
Power Supply	350W ATX Power Supply
USB	USB 2.0 x 4 (2 at front, 1 optional at rear, 1 pin header)
LCM Support	Yes
CPU	Intel Pentium Core 2 Duo E6400 2.13GHz 1066MHz FSB 4MB L2 Cache
PCI Riser Card	PCI-X 64bit/133MHz 3.3V/5V PCI add-on card
Memory	2GB DDRII (1GB x 2)
Hard Drive	Seagate Barracuda 7200.8: 250GB SATAII 7200RPM 3.5"HDD