



Simbari & Associates

NETmind Management Appliance

Simbari & Associates's (Simbari) integrated network troubleshooting and security solutions enable organizations to protect productivity gains and reduce operating costs.

The NETmind Management appliance is a turnkey Network Troubleshooting and Security System. It works in concert with all of its other components to efficiently protect your data infrastructure. With the increased complexity networks today, and the threat of security threats, achieving efficient network optimization and intrusion security solutions is critical to maintaining a high level of network protection and performance. Vigilant network protection and ensures business continuity and minimizes the effect of costly intrusions. Optimal network efficiency ensures a high level of productivity.

Simbari's NETmind Management solution not only enables organizations to protect their connected business assets from threats and increase the operating efficiency of intrusion protection, but also aids in providing a network that is running at optimal efficiency.

Features and Benefits

Web Based Packet Capture

Managing today's complex and widespread enterprise network has never been more challenging. As an IT professional, how can you ensure that your network and the applications it supports deliver the availability, security, and reliability that your business requires to succeed in this highly competitive world—24x7? NETmind helps you meet these formidable challenges by providing a fault and network performance management solution that you can deploy across your entire enterprise. It delivers unparalleled network monitoring, protocol decodes, to all key segments, e.g., Local Area Network (LAN) including Ethernet, Fast Ethernet, Gigabit Ethernet, Wireless, etc.

This powerful combination of standards-based monitoring and web based packet capture makes NETmind the ideal solution to proactively manage today's multi-protocol distributed networks. With NETmind you can monitor, validate, and evaluate your entire network infrastructure operations—from troubleshooting and baselining—to real-time and historical analysis. Armed with these insights, you can identify and correct network performance problems and bottlenecks—before they impact your users.

NETmind Packet Capture also gives you distributed, secure, and easy information access. With its browser-based UI, you can access NETmind appliances anytime, from anywhere. Now your network engineering team can monitor and troubleshoot your network without incurring the travel expenses involved in on-site problem diagnosis and resolution.

Web Based Packet Capture Protocol Decodes:

- TCP and UDP over IP, Voice-over-IP including: H.323, H.225, H.245, RAS, SIP, SCCP, (Cisco Skinny)
- Novell (IPX and NetWare 5)
- Microsoft
- Database (Oracle, Sybase, and MS-SQL Server)
- Wireless
- RTP/RICP, and SDP/SAP, • MPLS, RSVP-TE and many more

Intrusion Detection

The Intrusion detection module consists of two different application functions. The IDS module provides Intrusion Detection database reporting. The Security Audit module provides vulnerability scanning and reporting. The IDS module provides real-time traffic analysis and packet logging on IP networks. It also performs protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts and much more. The Intrusion Detection module can be deployed in a centralized approach where one IDS appliance monitors a single Internet connection. It can also be deployed in a distributed approach where multiple IDS sensors are distributed throughout the enterprise network and report back to a centralized console for administration/review. An example deployment is pictured below.

All alerts are stored in a database contained on each NETmind appliance. The alerts can also be forwarded to a central database, contained on another NETmind appliance or a corporate database server. For corporate database integration, the following databases are supported: MySQL, Microsoft SQL Server or Oracle. Once an alert is received within the NETmind appliance, the following actions can be taken; Email the alert to a pre-defined list of users, send a snmp trap to the organization network management station, generate a syslog message. This ability allows third party software integration for automatic trouble ticketing or automatic paging of admin staff, which in the end enhances problem notification/resolution.

The administration of each IDS sensor is done through a web based interface that can be accessed from anywhere in the network. The administrative interface enables all aspects of sensor support, including rule creation, rule modification, plug-in support, sensor status, etc. Each sensor can be administered individually through the NETmind User Interface or can be done through a centralized console. The centralized console approach simplifies sensor management and ensures that each sensor in the network has the exact same configuration. The NETmind appliance will not only support NETmind IDS sensors, but will also support existing Snort IDS sensors already deployed in the network.

Security Audit

The Intrusion Detection module is integrated with NESSUS and NMAP to offer a complete security scanning and auditing solution for the enterprise network. The interface to NESSUS and NMAP is completely web based. Because of the sensitivity of the data of this area the Security Audit information is password protected using a local password database that is stored on the NETmind appliance.

The NMAP integration allows for scanning of individual hosts or networks for open ports. Once the scan is complete a report is generated on the NETmind appliance showing which ports are open and what application is typically utilized over the particular port. This report is also emailed to the user that generates the report. All of the functions of NMAP that are available in the original application user interface are also available through the NETmind web based interface.

The NESSUS integration allows for scheduled vulnerability scanning of individual hosts or networks. Once the user defined schedule has been created, the NESSUS application will check each host for vulnerabilities against a local database of vulnerabilities. Once the NESSUS application is complete, a report is generated in HTML or PDF form detailing the host and all of the potential vulnerabilities that it may have. The vulnerability database that is located on the NETmind appliance is updated nightly from the NESSUS.com site. This ensures that when a host or network is scanned that it is checked against the latest vulnerabilities available.

The Security Audit module is user/profile based so users are only allowed to execute functions that are pre-defined by the administrator.

Real-Time Traffic Measurement

Network Management is becoming an increasingly complex task, requiring automated tools to support human effort. The Real-Time Traffic Measurement module is a simple portable traffic measurement and monitoring tool, which supports various management activities, including network optimization and planning.

The real-time measurement module is positioned in the network in the same way that the Packet Capture module is positioned. This module sits on the network and listens to all traffic on the network and stores it in a database contained on the NETmind appliance. Once this data is stored, it is broken down to provide web based reports for the end user. Some of the information contained in this module is:

Simbari & Associates LLC

All contents are Copyright © 2003 Simbari & Associates LLC, All rights reserved. Important Notices and Privacy Statement.

- Summary of traffic – local vs remote (Local network is defined by the end user)
- Summary of traffic based on protocol – IP, IPX, Appletalk, Decnet, LAT, etc.
- Summary of hosts, traffic destinations, destination ports.
- Summary of session information including source, destination, port, and latency of the connection.
- Amount of traffic each of the hosts are consuming on the network.
- Application Response Time.
- And much more

The real time traffic measurement module can also be used as a Netflow collector, where it will take flows from a Cisco router and export the information to a central Netflow analyzer like NetQoS or Ciscoworks. The Netflow support along with the low cost point of the NETmind appliance enables a more cost effective overall approach to Netflow collection and analysis.

Historical Analysis and Graphing

The Historical Analysis and Graphing module is based on the popular application Cacti. Cacti is a complete front-end to RRDTool. It stores all of the necessary information to create graphs and populate them with data in a database. The front-end is completely PHP driven. Along with being able to maintain Graphs, Data Sources, and Round Robin Archives in a database, Cacti handles the data gathering. There is also SNMP support for those familiar with creating graphs with MRTG.

Data Sources

To handle data gathering, you can feed cacti the paths to any external script/command along with any data that the user will need to "fill in". Cacti will then gather this data in a cron-job and populate a database with the round robin archives.

Data Sources which correspond to actual data on the graph, can also be created. For instance, if a user would want to graph the ping times to a host, you could create a data source utilizing a script that pings a host and returns its value in milliseconds. After defining options for RRDTool such as how to store the data, you will be able to define any additional information that the data input source requires, such as a host to ping in this case. Once a data source is created, it is automatically maintained at 5 minute intervals.

Graphs

Once one or more data sources are defined, an RRDTool graph can be created using the data. Cacti allows you to create almost any imaginable RRDTool graph using all of the standard RRDTool graph types and consolidation functions. A color selection area and automatic text padding function also aid in the creation of graphs to make the process easier.

Not only can you create RRDTool based graphs in Cacti, but there are many ways to display them. Along with a standard "list view" and a "preview mode", there is a "tree view", which allows you to put graphs onto a hierarchical tree for organizational purposes.

User Management

Due to the many functions of Cacti, a user based management tool is built in so you can add users and give them rights to certain areas of Cacti. This feature allows the ability for some users that can change graph parameters, while others can only view graphs.

Templating

Lastly, Cacti is able to scale to a large number of data sources and graphs through the use of templates. This allows the creation of a single graph or data source template which defines any graph or data source with which it is associated. Host templates enable you to define the capabilities of a host so cacti can poll it for information upon the addition of a new host.

Syslog Reporting

The Syslog Reporting module provides a fully functional Syslog server that stores all relevant Syslog information in a database. The Web based reporting engine provides an interface into the Syslog database that allows users to sort on date, host and message. The Syslog module can be used in a distributed approach where each NETmind appliance maintains its own Syslog database or in a centralized approach where each NETmind appliance sends its Syslog messages to a central NETmind appliance containing the Syslog database. The Syslog messages are stored in the database for 30 days and then are either archived to a backup database or automatically deleted. This functionality is fully configurable by the end user.

Web Based Administration

Each NETmind appliance is administered through a common web based interface. The web based interface provides a simplified approach to managing the Linux based operating system. Every aspect from starting and stopping the device, to user and group setup, to service/process administration, to application support is done through the Web User Interface. In the event that the web based interface is not available or is not desired by the support staff, the NETmind appliance can also be administered through a console or remotely via SSH (Secure Shell).

Wireless

The NETmind Wireless module is a 100% passive listening software, which looks at every single 802.11b frame transmitted across the air. It works by having the NETmind appliance deployed around the area where Access Points are located at, with two network interfaces, the wireless NIC (placed in promiscuous mode), and a standard Ethernet NIC that connects to the network backbone. In this setup, the wireless card sniffs on the air, registering every single packet in the air, and the standard Ethernet NIC waits for a connection from the "central appliance" and sends the current wireless activity statistic to the main server. The information registered is as follows:

Management Frames (key types such as beacons)

- registers number of packets
- registers total byte of packets
- registers Bandwidth used by management frames

Control Frames (key types such as Acknowledgement)

- registers number of packets
- registers total byte of packets
- registers Bandwidth used by control frames

Data Frames (differentiated between external/internal data)

- registers number of packets coming in from external connection
- registers total byte of packets from external connection
- registers number of packets coming from internally connected wireless nodes
- registers total byte of packets from internal connection
- registers total number of data packets
- registers total byte of data packets
- registers total Bandwidth of data frames

Overall Activity

- registers Total number of ALL packets
- registers Total bytes of ALL packets
- registers Total Bandwidth usage

Connected Nodes

- keeps track of connected "wireless" nodes
- remembers the MAC address of wireless nodes
- keeps track of incoming/outgoing traffic of wireless nodes
- keeps track of signal strength of wireless nodes
- keeps track of bandwidth usage by wireless nodes

And the above information is detected by a single NETmind appliance for ALL access points in the given area.

General Protocol Analysis System

- gives an overview of protocol activity in the wireless area
- view data link layer, network layer, transport layer info
- 802.11b breakdown, IP/IPv6/Other, TCP/UDP/ICMP/Other breakdown
- view count/byte, bandwidth usage, usage % statistics for all protocols

TCP Performance Analysis System

- target your investigation to individual wireless nodes
- view all TCP connections made to/from wireless node
- grouped under (IP, service port) pairs, view connection status,
- total packet/byte, incoming/outgoing packet/byte, retransmission
- rates, resource waste %, incoming/outgoing/RTT latencies, as well
- as incoming/outgoing/overall bandwidth (current, as well as highest observed).

NETmind Deployment

The NETmind appliance contains up to 3 10/100 Ethernet interfaces so that it can be deployed on a per segment basis. The NETmind appliance's can be deployed on the following segments:

Public:

On the public segment the NETmind appliance can be deployed in a variety of ways. First, the Intrusion Detection Module can be utilized for the following;

- 1. Accurate threat detection*—NETmind Intrusion Detection Module delivers the first step in providing a secure environment by comprehensively detecting all potential threats.
- 2. Intelligent threat investigation*—NETmind Intrusion Detection Module virtually eliminates false alarms, and automatically determines which threats need immediate attention to avoid costly intrusions.
- 3. Ease of management*—Browser-based tools simplify the user interaction, while providing powerful analytical tools that allow for a rapid and efficient response to threats.

Secondly, the Historical Graphing and Traffic Measurement modules can be utilized to measure the types and different types of traffic on the outside/Internet segment. This data is useful for architectural design and planning purposes for bandwidth sizing, etc. Thirdly, the Security Audit module can be utilized to provide out side look at the organization to determine which devices/networks are vulnerable to outside attacks. Finally, the packet analysis module can be utilized to troubleshoot Layer 1-7 problems on the outside/Internet segment.

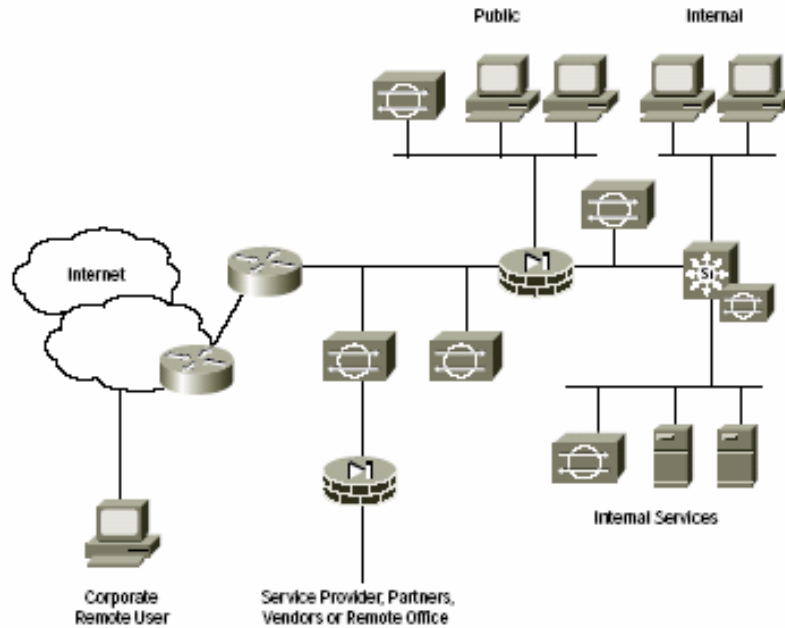


Figure 1 – NETmind Deployment Scenarios

Internal:

On the internal segment the NETmind appliance can be deployed in a variety of ways. First, the Intrusion Detection Module can be utilized to protect both the internal network, gaining the same benefits as on the public segment above. Secondly, the Historical Graphing and Traffic Measurement modules can be utilized to measure the types and different types of traffic on the various internal segments. This data is useful for architectural design and planning purposes for bandwidth sizing, etc. Thirdly, the Syslog module can be utilized to aid in fault analysis for network and system devices in the network that support Syslog. Fourthly, the Syslog module can be utilized to provide out side look at the organization to determine which devices/networks are vulnerable to outside attacks. Finally, the packet analysis module can be utilized to troubleshoot Layer 1-7 problems on the outside/Internet segment.

Technical Specifications

Part Numbers

- NETmind-1.0-IDS – NETmind Version 1.0 with IDS Module
- NETmind-1.0-Wireless – NETmind Version 1.0 with Wireless Module
- NETmind-1.0 – NETmind Version 1.0 without IDS
- NETmind-support – NETmind 1 year Support Contract

Form Factor

NETmind appliance is one rack unit (1RU) and will fit most 19” network racks.

LEDs

- Single indicator (LED)
- OFF—no power
 - YELLOW—booting up/standby
 - GREEN—application is running
 - RED—module fault located

Processor

Pentium 2.0 GHz on main board.

Operating System

Red Hat Linux 9.0

Memory

512MB RAM

Hard Disk

40 GB Hard Drive

Network Interfaces

NETmind w/IDS: 3 – 10/100 Ethernet Interfaces, Intel Chipset

NETmind w/Wireless – 2 - 10/100 Ethernet Interfaces and Cisco Aironet 350 PCI Wireless Card

NETmind - 2 – 10/100 Ethernet Interfaces, Intel Chipset

Traffic Capture Methods

SPAN

RSPAN

Any port mirror technology

Operating Environment

Operating temperature: 0 to 40°C (32 to 104.5°F)

Non-operating temperature: -40 to 70°C (-40 to 158°F)

Operating relative humidity: 10 to 90% (noncondensing)

Non-operating relative humidity: 5 to 95% (noncondensing)

Operating and non-operating altitude: sea level to 3050m (10,000 ft.)

Additional Information

For information about the NETmind Management Appliance please send email to sales@dynasolgrp.com or call 412.779-3790.