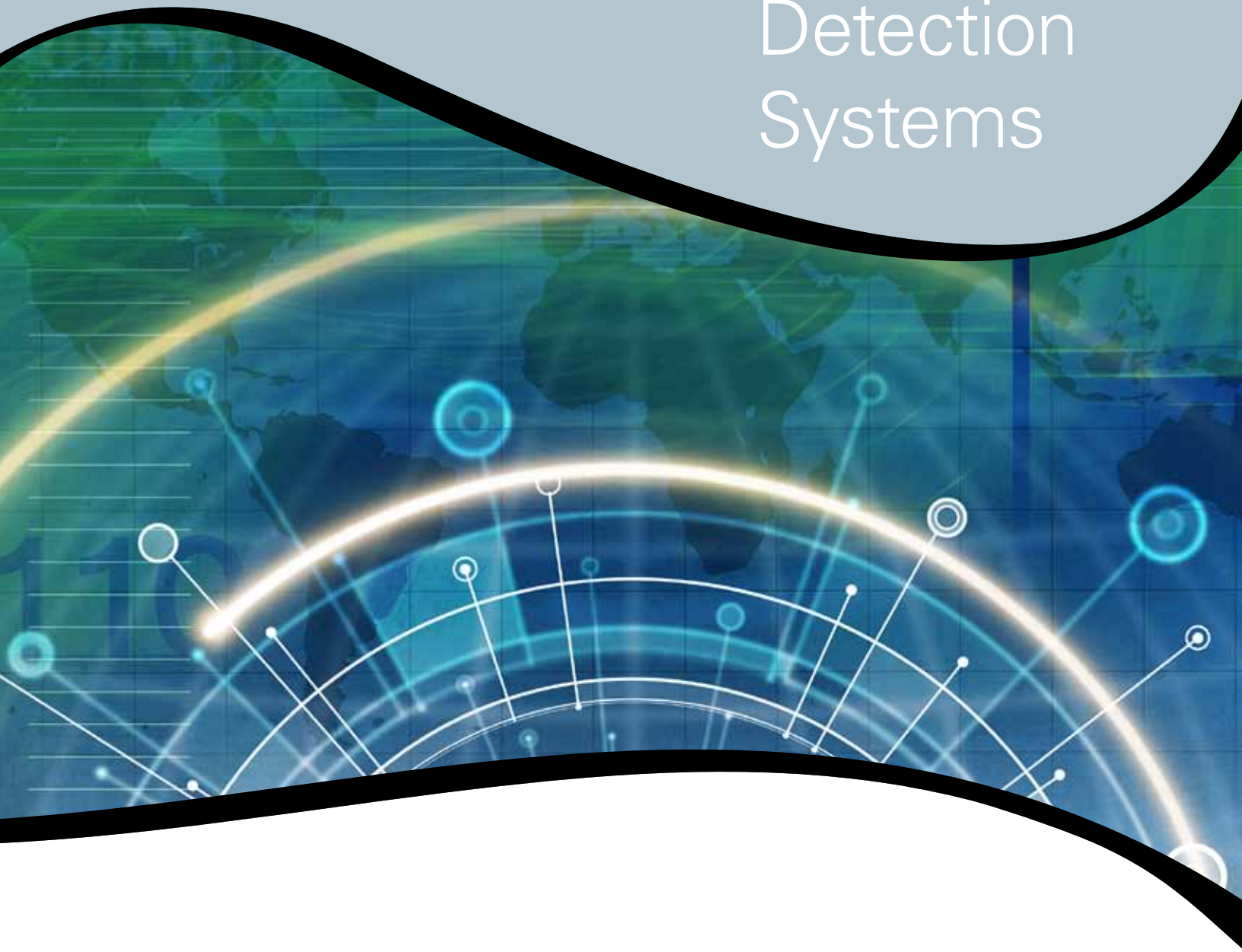
Tools

Information Assurance Tools Report

Sixth Edition

September 25, 2009

Intrusion Detection Systems



IATAC

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED *(From - To)*
25-09-2009	Report	25-09-2009

4. TITLE AND SUBTITLE
Information Assurance Technology Analysis Center (IATAC)

Information Assurance Tools Report – Intrusion Detection Systems. Sixth Edition.

5a. CONTRACT NUMBER
SPO700-98-D-4002

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Revision by Tzeyoung Max Wu

5d. PROJECT NUMBER

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
13200 Woodland Park Road
Herndon, VA 20171

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
IATAC is operated by Booz Allen Hamilton, 8283 Greensboro Drive, McLean, VA 22102.

14. ABSTRACT
This Information Assurance Technology Analysis Center (IATAC) report provides an index of Intrusion Detection System (IDS) tools. It summarizes pertinent information, providing users a brief description of available IDS tools and contact information for each. IATAC does not endorse, recommend, or evaluate the effectiveness of any specific tool. The written descriptions are based solely on vendors' claims and are intended only to highlight the capabilities and features of each firewall product. The report does identify sources of product evaluations when available.

15. SUBJECT TERMS
IATAC Collection, Intrusion Detection Systems (IDS)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
					Tyler, Gene
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	None	93	703-984-0775

Table of Contents

SECTION 1 ▸ **Introduction**

The Information Assurance Technology Analysis Center (IATAC) provides the Department of Defense (DoD) with emerging scientific and technical information to support Information Assurance (IA) and defensive information operations. IATAC is one of 10 Information Analysis Centers (IAC) sponsored by DoD and managed by the Defense Technical Information Center (DTIC). IACs are formal organizations chartered by DoD to facilitate the use of existing scientific and technical information. Scientists, engineers, and information specialists staff each IAC. IACs establish and maintain comprehensive knowledge bases that include historical, technical, scientific, and other data and information, which are collected worldwide. Information collections span a wide range of unclassified, limited-distribution, and classified information appropriate to the requirements of sponsoring technical communities. IACs also collect, maintain, and develop analytical tools and techniques, including databases, models, and simulations.

IATAC's mission is to provide DoD with a central point of access for information on emerging technologies in IA and cyber security. These include technologies, tools, and associated techniques for detection of, protection against, reaction to, and recovery from information warfare and cyber attacks that target information, information-based processes, information systems, and information technology. Specific areas of study include IA and cyber security threats and vulnerabilities, scientific and technological research and development, and technologies, standards, methods, and tools through which IA and cyber security objectives are being or may be accomplished.

As an IAC, IATAC's basic services include collecting, analyzing, and disseminating IA scientific and technical information; responding to user inquiries; database operations; current awareness activities (*e.g.,* the IAnewsletter, IA Digest, IA/IO Events Scheduler, and IA Research Update); and publishing State-of-the-Art Reports, Critical Review and Technology Assessments reports, and Tools Reports.

The IA Tools Database is one of the knowledge bases maintained by IATAC. This knowledge base contains information on a wide range of intrusion detection, vulnerability analysis, firewall applications, and anti-malware tools. Information for the IA Tools Database is obtained *via* open-source methods, including direct interface with various agencies, organizations, and vendors. Periodically, IATAC publishes a Tools Report to summarize and elucidate a particular subset of the tools information in the IATAC IA Tools Database that addresses a specific IA or cyber security challenge. To ensure applicability to Warfighter and Research and Development Community (Program Executive Officer/Program Manager) needs, the topic areas for Tools Reports are solicited from the DoD IA community or based on IATAC's careful ongoing observation and analysis of the IA and cyber security tools and technologies about which that community expresses a high level of interest.

Inquiries about IATAC capabilities, products, and services may be addressed to:

Gene Tyler, Director
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171
Phone: 703/984-0775
Fax: 703/984-0773

Email: *iatac@dtic.mil*
URL: *http://iac.dtic.mil/iatac*
SIPRNET: *https://iatac.dtic.mil*

1.1 Purpose

This report provides a brief explanation of why intrusion detection (ID) and intrusion prevention tools are necessary, and an index of various available tools. For this report, an Intrusion Detection System (IDS) is a device that attempts to detect intrusion into a computer or network by observation or audit. An Intrusion Prevention System (IPS) goes one step further and not only detects attacks but attempts to prevent them as well.

This report provides a summary of the characteristics and capabilities of publicly available IDS and IPS tools. IATAC does not endorse, recommend, or evaluate the effectiveness of any specific tools. The written descriptions are based solely on the suppliers' claims and are intended only to highlight the capabilities and features of each tool. These descriptions do not reflect the opinion of IATAC. It is up to the readers of this document to assess which product, if any, might best meet their needs. Technical questions concerning this report may be addressed to *iatac@dtic.mil*.

SECTION 2 ▸ Intrusion Detection/Prevention Overview

2.1 Definition

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies. Many IDS tools will also store a detected event in a log to be reviewed at a later date or will combine events with other data to make decisions regarding policies or damage control. An IPS is a type of IDS that can prevent or stop unwanted traffic. The IPS usually logs such events and related information.

2.2 Technologies

Several types of IDS technologies exist due to the variance of network configurations. Each type has advantages and disadvantage in detection, configuration, and cost. Specific categories will be discussed in detail in Section 3, Technologies.

2.2.1 Network-Based

A Network Intrusion Detection System (NIDS) is one common type of IDS that analyzes network traffic at all layers of the Open Systems Interconnection (OSI) model and makes decisions about the purpose of the traffic, analyzing for suspicious activity. Most NIDSs are easy to deploy on a network and can often view traffic from many systems at once. A term becoming more widely used by vendors is "Wireless Intrusion Prevention System" (WIPS) to describe a network device that monitors and analyzes the wireless radio spectrum in a network for intrusions and performs countermeasures.

2.2.2 Wireless

A wireless local area network (WLAN) IDS is similar to NIDS in that it can analyze network traffic. However, it will also analyze wireless-specific traffic, including scanning for external users trying to connect to access points (AP), rogue APs, users outside the physical area of the company, and WLAN IDSs built into APs. As networks increasingly support wireless technologies at various points of a topology, WLAN IDS will play larger roles in security. Many previous NIDS tools will include enhancements to support wireless traffic analysis.

2.2.3 Network Behavior Anomaly Detection

Network behavior anomaly detection (NBAD) views traffic on network segments to determine if anomalies exist in the amount or type of traffic. Segments that usually see very little traffic or segments that see only a particular type of traffic may transform the amount or type of traffic if an unwanted event occurs. NBAD requires several sensors to create a good snapshot of a network and requires benchmarking and baselining to determine the nominal amount of a segment's traffic.

2.2.4 Host-Based

Host-based intrusion detection systems (HIDS) analyze network traffic and system-specific settings such as software calls, local security policy, local log audits, and more. A HIDS must be installed on each machine and requires configuration specific to that operating system and software.

2.3 Detection Types

2.3.1 Signature-Based Detection

An IDS can use signature-based detection, relying on known traffic data to analyze potentially unwanted traffic. This type of detection is very fast and easy to configure. However, an attacker can slightly modify an attack to render it undetectable by a signature-based IDS. Still, signature-based detection, although limited in its detection capability, can be very accurate.

2.3.2 Anomaly-Based Detection

An IDS that looks at network traffic and detects data that is incorrect, not valid, or generally abnormal is called anomaly-based detection. This method is useful for detecting unwanted traffic that is not specifically known. For instance, an anomaly-based IDS will detect that an Internet protocol (IP) packet is malformed. It does not detect that it is malformed in a specific way, but indicates that it is anomalous.

2.3.3 Stateful Protocol Inspection

Stateful protocol inspection is similar to anomaly-based detection, but it can also analyze traffic at the network and transport layer and vender-specific traffic at the application layer, which anomaly-based detection cannot do.

2.4 False Positives and Negatives

It is impossible for an IDS to be perfect, primarily because network traffic is so complicated. The erroneous results in an IDS are divided into two types: false positives and false negatives. False positives occur when the IDS erroneously detects a problem with benign traffic. False negatives occur when unwanted traffic is undetected by the IDS. Both create problems for security administrators and may require that the system be calibrated. A greater number of false positives are generally more acceptable but can burden a security administrator with cumbersome amounts of data to sift through. However, because it is undetected, false negatives do not afford a security administrator an opportunity to review the data.

2.5 System Components

IDSs are generally made up of the following main types of components—

- **Sensors—**These are deployed in a network or on a device to collect data. They take input from various sources, including network packets, log files, and system call traces. Input is collected, organized, and then forwarded to one or more analyzers.
- **Analyzers—**Analyzers in an IDS collect data forwarded by sensors and then determine if an intrusion has actually occurred. Output from the analyzers should include evidence supporting the intrusion report. The analyzers may also provide recommendations and guidance on mitigation steps.
- **User interface—**The user interface of the IDS provides the end user a view and way to interact with the system. Through the interface the user can control and configure the system. Many user interfaces can generate reports as well.
- **Honeypot—**In a fully deployed IDS, some administrators may choose to install a "honeypot," essentially a system component set up as bait or decoy for intruders. Honeypots can be used as early warning systems of an attack, decoys from critical systems, and data collection sources for attack analyses. Many IDS vendors maintain honeypots for research purposes, and to develop new intrusion signatures. Note that a honeypot should only be deployed when the organization has the resources to maintain it. A honeypot left unmanaged may become a significant liability because attackers may use a compromised honeypot to attack other systems.

SECTION 3 ▸ Technologies

3.1 Network Intrusion Detection System

3.1.1 An Overview of the Open Systems Interconnection Model

A NIDS is placed on a network to analyze traffic in search of unwanted or malicious events. Network traffic is built on various layers; each layer delivers data from one point to another.

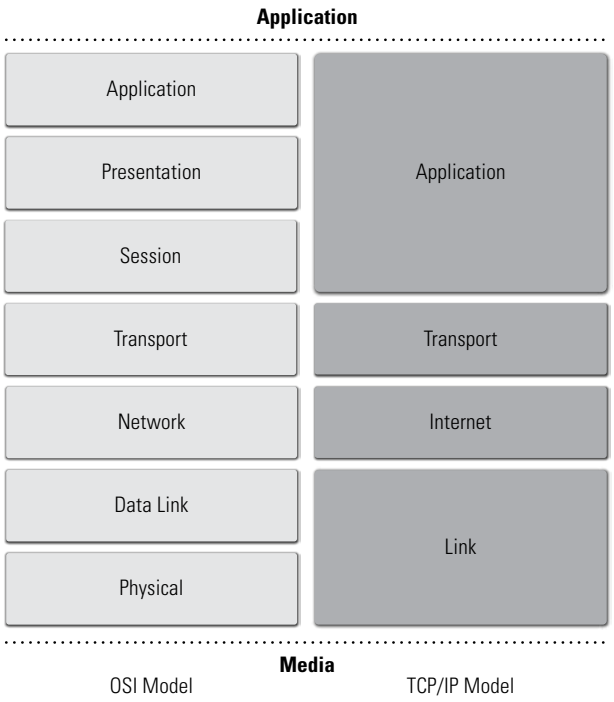


Figure 1 OSI and TCP/IP models

The OSI model and transmission control protocol (TCP)/IP model show how each layer stacks up. (See Figure 1.) Within the TCP/IP model, the lowest link layer controls how data flows on the wire, such as controlling voltages and the physical addresses of hardware, like mandatory access control (MAC) addresses. The Internet layer controls address routing and contains the IP stack. The transport layer controls data flow and checks data integrity. It includes the TCP and user datagram protocol (UDP). Lastly, the most complicated but most familiar level is the application layer, which contains the traffic used by programs. Application layer traffic includes the Web (hypertext transfer protocol [*HTTP]),* file transfer protocol *(FTP),* email, *etc.* Most NIDSs detect unwanted traffic at each layer, but concentrate mostly on the application layer.

3.1.2 Component Types

Two main component types comprise a NIDS: appliance and software only. A NIDS appliance is a piece of dedicated hardware: its only function is to be an IDS. The operating system (OS), software, and the network interface cards (NIC) are included in the appliance. The second component type, software only, contains all the IDS software and sometimes the OS; however, the user provides the hardware. Software-only NIDSs are often less expensive than appliance-based NIDS because they do not provide the hardware; however, more configuration is required, and hardware compatibility issues may arise.

With an IDS, the "system" component is vital to efficiency. Often a NIDS is not comprised of one device but of several physically separated components. Even in a less complicated NIDS, all components may be present but may be contained in one device. The NIDS is usually made of components identified in Section 2.1.1, but more specifically, the physical components usually include the sensor, management sever, database server, and console—

- **Sensor**—The sensor or agent is the NIDS component that sees network traffic and can make decisions regarding whether the traffic is malicious. Multiple sensors are usually placed at specific points around a network, and the location of the sensors is important. Connections to the network could be at firewalls, switches, routers, or other places at which the network divides.
- **Management server**—As the analyzer, a management server is a central location for all sensors to send their results. Management servers often connect to sensors *via* a management network; for security reasons, they often separate from the remainder of the network. The

management server will make decisions based on what the sensor reports. It can also correlate information from several sensors and make decisions based on specific traffic in different locations on the network.

- **Database server**—Database servers are the storage components of the NIDS. From these servers, events from sensors and correlated data from management servers can be logged. Databases are used because of their large storage space and performance qualities.
- **Console**—As the user interface of the NIDS, the console is the portion of the NIDS at which the administrator can log into and configure the NIDS or to monitor its status. The console can be installed as either a local program on the administrator's computer or a secure Web application portal.

Traffic between the components must be secure and should travel between each component unchanged and unviewed. Intercepted traffic could allow a hacker to change the way in which a network views an intrusion.

3.1.3 NIDS Sensor Placement

Because a sensor is the portion of the NIDS that views network traffic, its placement is important for detecting proper traffic. Figure 2 offers an example of how to place a NIDS sensor and other components. There are several ways to connect a NIDS sensor to the network—

- **Inline**—An inline NIDS sensor is placed between two network devices, such as a router and a firewall. This means that all traffic between the two devices must travel through the sensor, guaranteeing that the sensor can analyze the traffic. An inline sensor of an IDS can be used to disallow traffic through the sensor that has been deemed malicious. Inline sensors are often placed between the secure side of the firewall and the remainder of the internal network so that it has less traffic to analyze.
- **Passive**—A passive sensor analyzes traffic that has been copied from the network versus traffic that passes through it. The copied traffic can come from numerous places—
- **Spanning port**—Switches often allow all traffic on the switch to be copied to one port, called a spanning port. During times of low network load, this is an easy way to view all traffic on a switch; however, as the load increases, the switch may not be able to copy all traffic. Also, if the switch deems the traffic malformed, it may not copy the traffic at all; the malformed traffic that may be the type the NIDS sensor must analyze.
- **Network tap**—A network tap copies traffic at the physical layer. Network taps are commonly used in fiber-optic cables in which the network tap is inline and copies the signal without lowering the amount of light to an unusable level. Because network taps connect directly to the media, problems with a network tap can disable an entire connection.

3.1.4 Types of Events

A NIDS can detect many types of events, from benign to malicious. Reconnaissance events alone are not dangerous, but can lead to dangerous attacks. Reconnaissance events can originate at the TCP layer, such as a port scan. Running services have open ports to allow legitimate connections. During a port scan, an attacker tries to open connections on every port of a server to determine which services are running. Reconnaissance attacks also include opening connections of known applications, such as Web servers, to gather information about the server's OS and version. NIDS can also detect attacks at the network, transport, or application layers. These attacks include malicious code that could be used for denial of service (DoS) attacks and for theft of information. Lastly, NIDS can be used to detected less dangerous but nonetheless unwanted traffic, such as unexpected services (*i.e.,* backdoors) and policy violations.

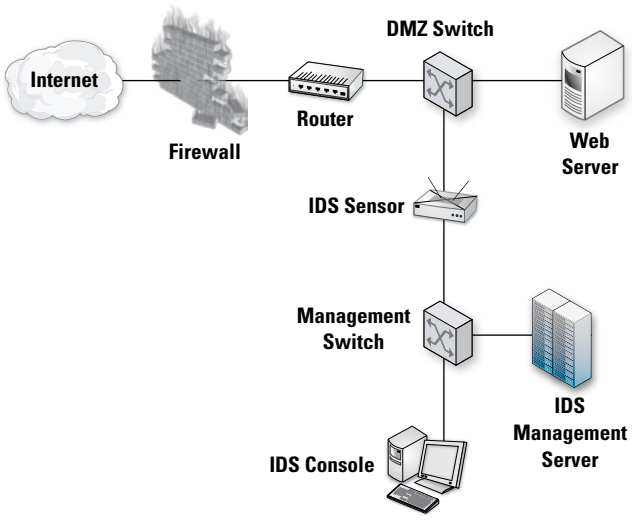


Figure 2 NIDS placement

3.1.5 Prevention

Although the detection portion of an IDS is the most complicated, the IDS goal is to make the network more secure, and the prevention portion of the IDS must accomplish that effort. After malicious or unwanted traffic is identified, using prevention techniques can stop it.

When an IDS is placed in an inline configuration, all traffic must travel through an IDS sensor. When traffic is determined to be unwanted, the IDS does not forward the traffic to the remainder of the network. To be effective, however, this effort requires that all traffic pass through the sensor. When an IDS is not configured in an inline configuration, it must end the malicious session by sending a reset packet to the network. Sometimes the attack can happen before the IDS can reset the connection. In addition, the action of ending connections works only on TCP, not on UDP or internet control message protocol (ICMP) connections. A more sophisticated approach to IPS is to reconfigure network devices (*e.g.,* firewalls, switches, and routers) to react to the traffic. Virtual local area networks (VLAN) can be configured to quarantine traffic and limit its connections to other resources.

3.2 Wireless

Because wireless technologies have become so popular, and with the nature of wireless communication blurring the borders between networks, special consideration is required. A wireless IDS is similar to an NIDS because the same types of network-based attacks can occur on wireless networks. However, because WLANs have other functionality and vulnerabilities, a WLAN IDS must monitor for network-based attacks as well as wireless-specific attacks.

For WLANs, Wireless sensors may be standalone devices that are used to monitor all wireless traffic but without forwarding the traffic. Sensors may also be built into wireless APs to monitor traffic as it connects to the wired network.

The location of a WLAN sensor is important because its physical location affects what a sensor can monitor. A sensor should be able to monitor traffic from devices that can connect to the wireless network. (See Figure 3.) This could involve having several sensors that extend past the normal field of operations. WLAN devices operate on one channel at a time, but can choose from several. Consequently, a WLAN sensor can listen on only one channel at a time. Sensors can listen to either one channel or to several channels by changing them periodically, as one would change channels on a television. Several sensors may be used for listening to several channels at once.

3.2.1 Components

A wireless IDS contains several components, such as sensors, management logging databases, and consoles, as does a NIDS. Wireless IDSs are unique in that they can be run centralized or decentralized. In centralized systems, the data is correlated at a central location and decisions and actions are made based on that data. In decentralized systems, decisions are made at the sensor.

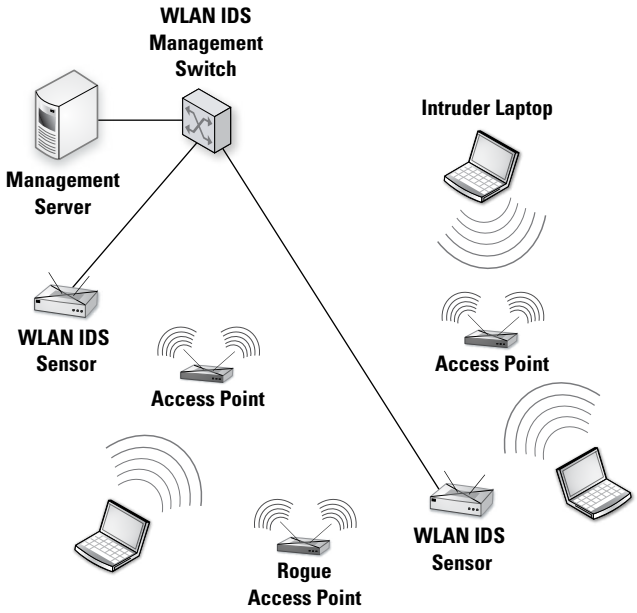


Figure 3 WLAN IDS placement

3.2.2 Types of Events

WLAN IDS sensors can monitor several types of events, such as those monitored on wired networks, and wireless specific events. WLAN sensors can detect anomalies such as unauthorized WLANs and wireless devices, poorly secured WLAN devices, unusual usage patterns, wireless scanners war driving tools, DoS attacks, and man in the middle (MITM) attacks. The limited scope of these events means that WLAN IDS results are usually more accurate than wired IDS results.

3.3 Network Behavior Anomaly Detection

NBAD is an IDS technology in which the shape or statistics of traffic, not individual packets, determines if the traffic is malicious. NBAD sensors are placed around a network in key places, such as at switches, at demilitarized zones (DMZ), and at locations at which traffic splits to different segments. Sensors then report on what type and amount of traffic is passing through. By viewing the shape of the traffic, an NBAD can detect DoS attacks, scanning across the network, worms, unexpected application services, and policy violations. NIDS and NBAD systems share some of the same components, such as sensors and management consoles; however, unlike NIDS, NBAD systems usually do not have database servers.

NBAD systems work best at determining when traffic deviates from the baseline. This is particularly useful for detecting DoS attacks and worms. As with other IDSs, NBADs can be used to prevent malicious traffic by stopping the traffic from passing through. If a network segment has been determined to be experiencing a DoS attack, the segment can be shut down or rerouted. NBADs do have a limitation in that the traffic causing the alert could also be the traffic that prevents a defensive mechanism. A DoS attack could prevent the NBAD system from reconfiguring a firewall or router, and the attack could then continue.

3.4 Host-Based Intrusion Detection System

HIDS comprises sensors that are located on servers or workstations to prevent attacks on a specific machine. A HIDS can see more than just network traffic and can make decisions based on local settings, settings specific to an OS, and log data.

Like other IDS configurations, HIDS have various device types. The sensor, or agent, is located on or near a host, such as a server, workstation, or application service. The event data is sent to logging services to record the events and possibly correlate them with other events.

HIDS agents can be placed on numerous host types. HIDS sensors can monitor servers, client hosts, and application servers. A server is typically a computer dedicated to running services in which clients connect to, send, or receive data, such as Web, email, or FTP servers. A client host is the workstation, such as a desktop or laptop, in which a user can connect to other machines. An application service is software that runs on a server, such as a Web service or database application. Because each host operates a different OS or service, the types of attacks that will affect the machines are specific to these machines.

Because the HIDS sensor monitors the machine, not solely the network traffic, the agent must be placed on the host as a piece of software. Logically, it is placed in a similar manner to that of a NIDS sensor, between the asset and outside network. However, instead of

being a network device, the HIDS sensor is a software layer through which the traffic must pass to get to the service. This layer is called a shim. (See Figure 4.)

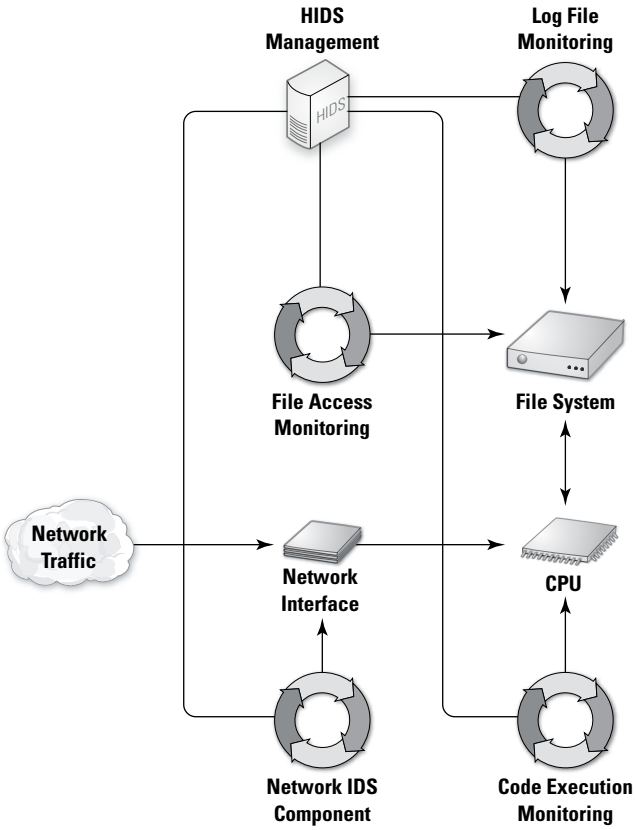


Figure 4 HIDS block diagram

3.4.1 Types of Events

A host-based IDS, such as a NIDS sensor, can monitor a system for network-based attacks and can also detect host-specific events. These host-specific events include code analysis, such as malicious code executes and buffer overflows; file system monitoring, including integrity and access; log analysis, during which host logs are reviewed; and lastly, network configuration monitor, during which the configuration of network settings (*e.g.,* wireless, VPN, and modem configurations) are reviewed for changes or improper settings.

3.4.2 Prevention

A HIDS monitors several host-specific events and, in turn, can defend a system from attacks of this type. When a malicious code event is detected, such as a buffer overflow, a HIDS can ensure that malicious code is not executed because of the buffer overflow. Also, when unexpected access to a file system occurs, the HIDS sensor can deny access. Because a HIDS sensor does not have to rely on network traffic to make decisions on malicious traffic or to stop network traffic, the HIDS IPS tactics can be performed very quickly and successfully.

SECTION 4 ▶ IDS Management

4.1 Maintenance

IDS maintenance is required for all IDS technologies. Because threats and prevention technologies are always changing, patches, signatures, and configurations must be updated to ensure that the latest malicious traffic is being detected and prevented. Usually a graphical user interface (GUI), application, or secure Web-based interface performs maintenance from a console. From the console, administrators can monitor IDS components to ensure they are operational, verify they are working properly, and perform vulnerability assessments (VA) and updates.

4.2 Tuning

To be effective, an IDS must be tuned accurately. Tuning requires changing settings to be in compliance with the security policies and goals of the IDS administrator. Scanning techniques, thresholds, and focus can be tuned to ensure that an IDS is identifying relevant data without overloading the administrator with warnings or too many false positives. Tuning is time-consuming, but it must be performed to ensure an efficient IDS configuration. Note that tuning is specific to the IDS product.

4.3 Detection Accuracy

The accuracy of an IDS depends on the way in which it detects, such as by the rule set. Signature-based detection detects only simple and well-known attacks, whereas anomaly-based detection can detect more types of attacks, but has a higher number of false positives. Tuning is required to minimize the number of false positives and to make the data more useful.

SECTION 5 ▶ IDS Challenges

It is important to remember that an IDS is only one of many tools in the security professional's arsenal against attacks and intrusions. As with any tool, all IDS have their own limitations and challenges. Much depends on how they are deployed and used, but in general, IDS should be integrated with other tools to comprehensively protect a system. Even more importantly security should be planned and managed. Personnel must be trained to have healthy security habits and to be wary of social engineering.

IDS technologies continue to evolve. As limitations are realized, new detection tools are being developed. Forensic technology has been a promising new source of detection strategies. Host Based Security Systems (HBSS) are also rising in popularity. The focus of HBSS-based systems security is migrating from strictly perimeter management to security management at the hosts.

5.1 Attacks

5.1.1 Tools Used in Attacks

As the world becomes more connected to the cyberworld, attackers and hackers are becoming increasingly sophisticated, especially in the use of automated tools to penetrate systems. At the same time, cybercriminals are becoming more organized and can engineer highly coordinated and intricate attacks. The following are general types of tools that attackers utilize—

- **Scanning Tools**—These tools allow attacks to survey and analyze system characteristics. These tools can determine the OS used by network devices, and then identify vulnerabilities and potential network ports to use for an attack. Some tools can also perform slowly timed surveys of a target system in order to not trigger an IDS.
- **Remote Management Tools**—Remote management tools are used often by systems administrators to manage a network by managing and controlling systems devices from a remote location. However, the same tools can be used by attackers to similarly take control of target devices, sometimes covertly.

Additionally, attackers have been creating various types of malware to carry out attacks. Malware can include trojan horses, Rootkits, Backdoors, spyware, keystroke loggers, and botnets.

5.1.2 Social Engineering

Despite the existence of sophisticated technical tools, social engineering remains one of the most effective methods of attacks to infiltrate systems. The most carefully secured system in the world using the latest technologies can be broken when employees are tricked into revealing passwords and other sensitive information. Besides physically securing systems, security professionals must ensure that staff and personnel are trained to recognize social engineering techniques such as phishing attacks. Personnel should also develop safe habits such as locking computer screens when idle, being careful when discarding notes that have sensitive information, and heeding warnings given by browsers when perusing Web sites. However, the problem is exacerbated when organizations using different networks must share potentially sensitive information. Trust between the organizations not to reveal one another's data can become a large issue.

5.2 Challenges in IDS

5.2.1 IDS Scalability in Large Networks

Many networks are large and can even contain a heterogeneous collection of thousands of devices. Sub-components in a large network may communicate using different technologies and protocols. One challenge for IDS devices deployed over a large network is for IDS components to be able to communicate across sub-networks, sometimes through firewalls and gateways. On different parts of the network, network devices may use different data formats and different protocols for communication. The IDS must be able to recognize the different formats. The matter is further complicated if there are different trust relationships being enforced within parts of the network. Finally, the IDS devices must be able to communicate across barriers between parts of the network. However, opening up lines of communication can create more vulnerabilities in network boundaries that attackers can exploit.

Another challenge in a large network is for the IDS to be able to effectively monitor traffic. NIDS components are scattered throughout a network, but if not placed strategically, many attacks can altogether bypass NIDS sensors by traversing alternate paths in a network. Moreover, although many IDS products in the market are updated to recognize attack signature of single attacks, they may fail to recognize attacks that use many attack sources. Many IDS cannot intelligently correlate data from multiple sources. Newer IDS technologies must leverage integrated systems to gain an overview of distributed intrusive activity.

5.2.2 Vulnerabilities in Operating Systems

Many common operating systems are simply not designed to operate securely. Thus, malware often is written to exploit discovered vulnerabilities in popular operating systems. Depending on the nature of the attack, many times if an operating is compromised, it can be difficult for an IDS to recognize that the operating system is no longer legitimate. Moving forward, operating systems must be designed to better support security policies pertaining to authentication, access control, and encryption.

5.2.3 Limits in Network Intrusion Detection Systems

NIDS analyze traffic traversing network segments at the network layer. At that level, attacks can be observed when it may be difficult if only observing at an application level. However, there may be traffic passing within the network that may not be fully visible to the NIDS. This happens especially when secure encrypted tunnels and VPNs are deployed. Unless it knows how to decrypt and re-encrypt data, such traffic remains fully opaque to the NIDS. Secure sockets layer (SSL) traffic over hypertext transfer protocol secure *(HTTPS)* connections can be used by attackers to mask intrusions.

Another limitation to NIDS manifests as bandwidth rates increase in a network. Especially when the amount of traffic also increases, it becomes a challenge for NIDS to be able to keep up with the rate of traffic and analyze data quickly and sufficiently. Finally, in a large network with many paths of communication, intrusions can bypass NIDS sensors.

5.2.4 Signature-Based Detection

A common strategy for IDS in detecting intrusions is to memorize signatures of known attacks. The inherent weakness in relying on signatures is that the signature patterns must be known first. New attacks are often unrecognizable by popular IDS. Signatures can be masked as well. The ongoing race between new attacks and detection systems has been a challenge.

5.2.5 Challenges with Wireless Technologies

Wireless technologies are becoming increasingly ubiquitous in modern networks; however, this new technology comes with its own set of challenges. Wireless networks are inherently 'open' and viewable by all network scanners. There are no physical barriers between data sent through the air. As such, it is relatively easy to intercept data packets in a wireless network.

One of the challenges with wireless is that the new technology come with its own set of protocols for communication that break the traditional OSI layer model. IDS must learn new communication patterns. Also, as open as wireless communication is, devices on such networks rely on established trust relationships between identified systems; however, if one system is already compromised before rejoining a network, it may be difficult for the IDS to detect intrusive activity from a trusted source.

5.2.6 Over-Reliance on IDS

IDS themselves may be used improperly within an organization. In general, an IDS is an important tool for security administrators to detect intrusions and attacks on a system. It is even more important for administrators to properly secure the system in the first place. When administrators focus too much on relying on IDS to catch intrusions, they can overly focus on symptoms of network's vulnerabilities rather than fixing the root causes of the security issue. Over-reliance on IDS can become a problem especially when commercial IDS vendors overhype features in the race to sell products on the market. Sometimes IDS capabilities claims are over-exaggerated and should be tested with skepticism. Administrators should thoroughly check IDS output and use competent judgment when analyzing reports.

It is important to recognize that the IDS is only one tool in an administrator's arsenal in properly securing a network. Using an integrated approach to security, administrators should come up with an overall plan, properly lock down systems, and leverage multiple types of tools such as firewalls, vulnerabilities scanners, and more.

SECTION 6 ▶ **Conclusion**

Intrusion detection and prevention systems are important parts of a well-rounded security infrastructure. IDSs are used in conjunction with other technologies (*e.g.,* firewalls and routers), are part of procedures (*e.g.,* log reviews), and help enforce policies. Each of the IDS technologies—NIDS, WLAN IDS, NBAD, and HIDS—are used together, correlating data from each device and making decisions based on what each type of IDS can monitor. Although IDSs should be used as part of defense in depth (DiD), they should not be used alone. Other techniques, procedures, and policies should be used to protect the network. IDSs have made significant improvements in the past decade, but some concerns still plague our security administrators. These problems will continue to be addressed as IDS technologies improve.

SECTION 7 ▸ **IDS Tools**

This section summarizes pertinent information, providing users a brief description of available IDS tools and vendor contact information. Again, IATAC does not endorse, recommend, or evaluate the effectiveness of these tools. The written descriptions are drawn from vendors' information such as brochures and Web sites, and are intended only to highlight the capabilities or features of each product. It is up to the reader to assess which product, if any, may best suit his or her security needs.

Trademark Disclaimer

The authors have made a best effort to indicate registered trademarks where they apply, based on searches in the U.S. Patent and Trademark Office Trademark Electronic Search System (TESS) for "live" registered trademarks for all company, product, and technology names. There is a possibility, however, that due to the large quantity of such names in this report, some trademarks may have been overlooked in our research. We apologize in advance for any trademarks that may have been inadvertently excluded, and invite the trademark registrants to contact the IATAC to inform us of their trademark status so we can appropriately indicate these trademarks in our next revision. Note that we have not indicated non-registered and non-U.S. registered trademarks due to the inability to research these effectively.

Legend For Tables

For each tool described in this section, a table is provided that provides certain information about that tool. This information includes—

Type	The type of tool, or category in which this tool belongs, *e.g.*, "Web Application Scanning"
Operating System	The operating system(s) on which the tool runs. If the tool is an appliance, this field will contain a "not applicable" symbol (N/A) because the operating system is embedded in the tool.
Hardware	The third-party hardware platform(s) on which the tool runs, plus any significant additional hardware requirements, such as minimum amount of random access memory or free disk space. If the tool is an appliance, this field will contain a "not applicable" symbol (N/A) because the hardware is incorporated into the tool.
License	The type of license under which the tool is distributed, *e.g.*, Commercial, Freeware, GNU Public License
NIAP Validated	An indication of whether the product has received a validation by the National Information Assurance Partnership (NIAP) under the Common Criteria, Federal Information Processing Standard 140, or another certification standard for which NIAP performs validations. If no such validation has been performed, this field will be blank.
Common Criteria	If the tool has received a Common Criteria certification, the Evaluation Assurance Level and date of that certification. If no such certification has been performed, this field will be blank.
Developer	The individual or organization responsible for creating and/or distributing the tool
URL	The Uniform Resource Locator (URL) of the Web page from which the tool can be obtained (downloaded or purchased), or in some cases, the Web page at which the supplier can be notified with a request to obtain the tool

IATAC does not endorse any of the following product evaluations.

AIDE—Advanced Intrusion Detection Environment

Abstract

AIDE is a free replacement for Tripwire®, which operates in the same manner as the semi-free Tripwire, but provides additional features. AIDE creates a database from the regular expression found in a customizable configuration file. Once this database is initialized, it can be used to verify the integrity of the files. It has several messages digest algorithms (md5, sha1, rmd160, Tiger®, Haval, *etc.*) that are used to check the integrity of the file. More algorithms can be added with relative ease. All the usual file attributes can be checked for inconsistencies, and AIDE can read databases from older or newer versions.

AIDE—Advanced Intrusion Detection Environment

Type	HIDS
Operating System	All BSD Platforms (FreeBSD/NetBSD/ OpenBSD/Apple Mac® OS X), All POSIX (Linux/BSD/UNIX-like OSes), Linux, Solaris®, IBM® AIX, Other
Hardware	Required
License	Open Source
NIAP Validated	
Common Criteria	
Developer	madhack, rvdb
URL	*http://sourceforge.net/projects/aide*

CSP Alert-Plus®

Abstract

Alert-Plus protects Hewlett-Packard® (HP) NonStop systems by providing real-time intrusion protection on systems running Safeguard. Alert-Plus is a rules-based system that compares events recorded in a Safeguard audit trail against custom-defined rules and automatically invokes a response when it detects an event of interest. Alert-Plus can detect an intrusion attempt and actually help to block it.

Alert-Plus includes a Windows® GUI, which allows a user to perform all Alert-Plus functions more directly from the GUI. Functions include the following—

- Creating, editing, and compiling rules;
- Observing on console windows the events detected by the Alert-Plus monitor;
- Defining actions to be taken;
- Starting and stopping the Alert-Plus monitor;
- Configuring log files;
- Seeing who is logged on;
- Accessing the spooler.

BUILTINS

BUILTINS are new in Alert-Plus and allow defining a complete rule in a single statement, monitoring up to 20 security vectors, and invoking 12 different responses, including audible announcements. Security vectors include suspicious logon activity and access attempts.

Threat Board

Threat Board is an optional component that can be added to an Alert-Plus installation. Threat Board works in conjunction with Alert-Plus to analyze patterns within multiple events and map them to threat indicators based on category, frequency, and customized thresholds.

Alert-Plus

Type	HIDS
Operating System	Windows
Hardware	Required
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Computer Security Products® (CSP®), Inc.
URL	*http://www.tandemsecurity.com/solution_3.php*

eEye® Retina®

Abstract

Retina Network Security Scanner provides vulnerability management and identifies known and zero day vulnerabilities, plus provides security risk assessment, enabling security best practices, policy enforcement, and regulatory audits.

Features

- **Network Security Scanner**—Enables prioritized policy management, patch management, and vulnerability management
- **Network Vulnerability Assessment**—Identifies network security vulnerabilities, missing application updates, and zero day threats
- **Network Discovery and Policy Assessment**—Discovers all devices, operating systems, applications, patch levels, and policy configurations
- **Vulnerability Management**—Enables prioritized policy management, patch management, and vulnerability assessment
- **Fast and Accurate Scans**—Accurately scans a Class C network of devices, operating systems and applications in ~15 minutes
- **Policy Compliance**—Identifies and simplifies corporate and regulatory requirements (SOX, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Gramm-Leach-Bliley Act of 1999 (GLBA), Payment Card Industry (PCI) and others)

eEye Retina

Type	HIDS
Operating System	Windows
Hardware	Required
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	eEye Digital Security
URL	*http://www.eeye.com/html/Products/Retina/index.html*

eEye SecureIIS Web Server Protection

Abstract

SecureIIS Web server security delivers integrated multi-layered Windows server protection. It provides application layer protection *via* integration with the IIS platform as an Internet Server Application Programming Interface (ISAPI) filter, protecting against known and unknown exploits, zero day attacks, and unauthorized Web access.

Features

- **Application Layer Protection**—SecureIIS inspects requests as they come in from the network layer, as they are passed up to the kernel, and at every level of processing in between. If at any point SecureIIS detects a possible attack, it can take over and prevent unauthorized access and/or damage to the Web server and host applications.
- **IIS ISAPI Integration**—SecureIIS was developed as an ISAPI filter, which allows for a tighter integration with the Web server as compared to other application firewalls. It monitors data as it is processed by IIS and can block a request at any point if it resembles one of many classes of attack patterns, including SQL injection and cross-site scripting.
- **Zero Day Protection**—Unlike network firewalls and intrusion detection systems, SecureIIS does not rely upon a database of attack signatures that require regular updating. Instead, it uses multiple security filters to inspect Web server traffic that could cause buffer overflows, parser evasions, directory traversal, or other attacks. Therefore, SecureIIS is able to block entire classes of attacks, including those attacks that have not yet been discovered.
- **Compatibility and Key Features**—SecureIIS works with and protects all common Web-based applications such as Flash, Cold Fusion, FrontPage, Outlook Web Access, and many third-party and custom applications. Configurations can be modified without having to restart the Web server, thus preventing disruption of the active Web site. SecureIIS runtime logs provide detailed explanations as to why requests were denied and allow for data to be exported in any number of different formats, including tab delimited, text, and Excel. This activity can also be graphed in real-time based on class of attack.

SecureIIS Web Server Protection

Type	HIDS
Operating System	Windows
Hardware	Required
License	Commercial
NIAP Validated	
Common Criteria	
Developer	eEye Digital Security
URL	*http://www.eeye.com/html/products/secureiis/index.html*

GFI EventsManager

Abstract

GFI EventsManager is a software-based events management solution that delivers automated collection and processing of events from diverse networks, from the small, single-domain network to extended, mixed environment networks, on multiple forests and in diverse geographical locations. It offers a scalable design that enables you to deploy multiple instances of the front-end application, while at the same time, maintaining the same database backend. This decentralizes and distributes the event collection process while centralizing the monitoring and reporting aspects of events monitoring. GFI EventsManager includes—

- A performance-tuned event processing engine,
- A comprehensive set of event processing rules that are pre-configured and applicable to a wide variety of networks regardless of their size,
- A set of noise reduction features, critical in large complex networks,
- A centralized and user-friendly events browser that enables you to locate events that occurred on your network from a single console,
- Triggered-based alerts,
- Reporting features can be added by installing the GFI EventsManager ReportPack, a fully fledged reporting companion to GFI EventsManager.

GFI EventsManager

Type	HIDS
Operating System	Windows
Hardware	• Processor: 2.5 Gigahertz (GHz) or higher • Random access memory (RAM): 1024 Megabyte (MB) • Hard disk: 2 Gigabyte (GB) of available space
License	Commercial
NIAP Validated	
Common Criteria	
Developer	GFI Software
URL	*http://www.gfi.com/eventsmanager*

Hewlett Packard®-Unix (HP-UX®) 11i Host Intrusion Detection System (HIDS)

Abstract

HP-UX HIDS continuously examines ongoing activity on a system, and it seeks out patterns that suggest security breaches or misuses. Security threats or breaches can include attempts to break into a system, subversive activities, or spreading a virus. Once you activate HP-UX HIDS for a given host system and it detects an intrusion attempt, the host sends an alert to the administrative interface where you can immediately investigate the situation, and when necessary, take action against the intrusion. In addition, you can set up customized local responses to alerts.

HP-UX 11i HIDS

Type	HIDS
Operating System	Unix
Hardware	Required
License	Freeware
NIAP Validated	
Common Criteria	
Developer	Hewlett-Packard
URL	*http://h20338.www2.hp.com/hpux11i/cache/324806-0-0-0-121.html*

- HP-UX HIDS can provide notification in the event of suspicious activity that can precede an attack.
- HP-UX HIDS is useful for enterprise environments where centralized management tools control networks of heterogeneous systems. These environments can include Web servers, transaction processors, application servers, and database systems.
- HP-UX HIDS uses knowledge about how host systems, the network, or the entire enterprise can be exploited, and applies that expertise to the flow of system events. HP-UX HIDS uses known building blocks to protect resources against existing attack scenarios and unknown scenarios.
- HP-UX HIDS provides simplified administration through a secure GUI the HP-UX HIDS System Manager.
- HP-UX HIDS provides customizable intrusion response capabilities. Hosts always send alerts to the administration interface. You can augment these notifications with automated host-based response programs that you can customize for the host that is being monitored. HP provides a customized program for OpenView® Operations (OVO®) integration; you can also create your own.

IBM® RealSecure® Server Sensor

Abstract

IBM RealSecure Server Sensor provides automated, real-time intrusion protection and detection by analyzing events, host logs, and inbound and outbound network activity on critical enterprise servers in order to block malicious activity from damaging critical assets.

RealSecure Server Sensor applies built-in signatures and sophisticated protocol analysis with behavioral pattern sets and automated event correlation to help prevent known and unknown attacks.

Benefits

- **Server protection**—Designed to protect the underlying operating system by helping prevent attackers from exploiting operating system and application vulnerabilities
- **Web application protection**—Provides SSL) encrypted application layer intrusion monitoring, analysis, and response capability for both Apache and IIS Web servers
- **Advanced intrusion prevention/blocking**—Monitors all traffic to and from the server or network in order to detect and prevent inbound attacks as well as block new and unknown outbound attacks such as buffer overflows, Trojans, brute force attacks, unauthorized access and network worms
- **Console and network intrusion protection**—Provides the flexibility to detect and prevent both console and network-based attacks through log monitoring capabilities that detect malicious activity before it causes any damage
- **Broad platform coverage**—Provides you with the flexibility to grow their server protection strategy regardless of the environment: Windows, Solaris, HP-UX, AIX® and Linux
- **Windows Server 2003 and Windows 2000 Server certified**—This rigorous test is endorsed for business-critical applications by analysts and enterprise customers alike because it verifies features and functionality that make applications more robust and manageable.
- **Audit policy management**—Centralized management of operating system audit policy helps ensure that all critical servers have consistent and effective audit policy and allows for the management of true kernel-level auditing
- **Global technical support**—Provides customers with a wide array of support offerings, specifically designed to meet the cost and service demands of diverse networking environments

IBM RealSecure Server Sensor

Type	HIDS
Operating System	Windows, Sun Solaris, IBM AIX, HP-UX, VMware® ESX
Hardware	Required
License	Commercial
NIAP Validated	
Common Criteria	
Developer	IBM
URL	*http://www-935.ibm.com/services/us/index.wss/offering/iss/a1026960*

integrit

Abstract

integrit has a small memory footprint, uses up-to-date cryptographic algorithms, and has other features.

The integrit system detects intrusion by detecting when trusted files have been altered. By creating an integrit database (update mode) that is a snapshot of a host system in a known state, the host's files can later be verified as unaltered by running integrit in check mode to compare current state to the recorded known state. integrit can do a check and an update simultaneously.

integrit	
Type	HIDS
Operating System	All POSIX (Linux/BSD/UNIX-like OS)
Hardware	Required
License	Open Source
NIAP Validated	
Common Criteria	
Developer	Ed L. Cashin
URL	*http://integrit.sourceforge.net/texinfo/integrit.html* *http://sourceforge.net/projects/integrit/*

Lumension® Application Control

Abstract

Lumension Application Control (formerly SecureWave Sanctuary® Application Control) is a three-tiered client/server application that provides the capability to centrally control the programs and applications users are able to execute on their client computers. Application Control controls authorization of applications and executable files by maintaining a database of hashes of approved executables. When a user logs onto a client that is protected by Application Control, the client driver contacts the server and downloads the list of authorized hashes. Whenever the user attempts to execute a file on the client, the client driver intercepts the execution request at the operating system level, calculates the hash value of the file and searches for a match in the list of authorized hashes. If a match is found, execution of the file proceeds; otherwise, execution is blocked.

Three tiers of a Sanctuary Application Control Desktop (SACD) deployment comprise:

- **An SQL database**—The database management system (Microsoft® SQL Server 7.0 or higher, or MSDE version 1.0 or 2000) and underlying operating system (Windows 2000 Server or Professional, Windows XP Professional, or Windows Server 2003) are in the TOE environment.
- **One or more servers**—The Sanctuary Application Server (SXS) runs as a service on the underlying operating system (Windows 2000 Server or Professional, or Windows Server 2003).
- **Client kernel driver (SXD)**—This is installed on each of the client computers to be protected. Client kernel drivers are available for the following operating systems: Windows NT4 SP6a Server or Workstation; Windows 2000 Server or Professional; Windows XP Professional; or Windows Server 2003.
- **Administrative toolkit**—The kit is comprised of a GUI-based application (the SecureWave Management Console, or SMC) and various command-line tools. It also operates in the client tier, and is supported on Windows 2000 Server or Professional, Windows XP Professional, or Windows Server 2003.

Lumension Sanctuary Application Control

Type	HIDS
Operating System	Windows
Hardware	Required
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Lumension, Inc.
URL	*http://www.lumension.com/*

McAfee® Host Intrusion Prevention

Abstract

McAfee Host Intrusion Prevention (HIP) is a host-based intrusion prevention system designed to protect system resources and applications. It works to intercept system calls prior to their execution and network traffic prior to their processing. If the HIP Agent determines that a call or packet is symptomatic of malicious code, the call or packet can be blocked and/or an audit log created; if safe, it is allowed.

Host Intrusion Prevention uses multiple methods, including behavioral and signature analysis, a stateful firewall that sets security parameters based on how users connect to the network, and application control. Laptops are also protected. Different levels of protection are applied based on connection (corporate network, VPN®, or public network), and quarantine mode prevents remote users from accessing the network if their device fails checks. Automatic signature updates and zero-day protection provide advanced vulnerability-shielding capabilities, so that systems can be patched less often and less urgently.

Host Intrusion Prevention is part of McAfee Total Protection for Endpoint, which integrates with McAfee ePolicy Orchestrator® for centralized reporting and management that's accurate, scalable, easy to use and works with other McAfee and non-McAfee products.

Features

- Behavioral protection secures endpoints against unknown attacks; signature protection identifies and blocks known attacks; stateful firewall applies policies, bars unsolicited inbound traffic, and controls outbound traffic; application control specifies which applications can or cannot be run; custom, connection-based policies safeguard laptops when they are off the network
- Apply different levels of security using rules based on the endpoint's connection—on the corporate network, over VPN, or from a public network—with connection-aware protection; use quarantine mode to block remote users that fail security checks and prevent them from accessing the network management technology
- Access centralized event monitoring reports, dashboard, and workflow with ePolicy Orchestrator; deploy, manage, and update agents and policies across various operating system and administer endpoint protection with one Web-based console
- Collect attack details, complete with timestamps, for prompt compliance reporting, auditing, investigations, and response; customized dashboards deliver real-time compliance status and produce clear, easy-to-read reports for auditors and other stakeholders.
- Automatic security content updates target specific vulnerabilities and recognize unknown exploits and stop them from executing

McAfee Host Intrusion Prevention

Type	HIDS
Operating System	Windows
Hardware	Required
License	Commercial
NIAP Validated	True
Common Criteria	EAL3
Developer	McAfee
URL	*http://www.mcafee.com/us/enterprise/products/system_security/clients/host_intrusion_prevention_desktop_server.html*

NetIQ® Security Manager iSeries®

Abstract

NetIQ Security Manager satisfies compliance mandates by automating security activity reviews, log preservation, threat management, incident response, and change auditing. It provides strong protection of data residing on host systems, including servers, workstations, databases and the Active Directory infrastructure. NetIQ Security Manager provides out-of-the box support for a broad range of heterogeneous platforms, applications and devices, and includes these technical features:

Key Features and Benefits

- **Reduces exposure time**—Optimizes reaction times with real time monitoring for security incidents, extensive notification and information capabilities and automated responses.
- **Improves security knowledge**—Delivers a comprehensive Knowledge Base that automatically builds security knowledge and internalizes new and updated information. This helps ensure that the knowledge needed to understand and respond to incidents is available when needed.
- **Increases protection levels**—Integrates and correlates real time and archived data from all security systems and processes. By tracking incidents to ensure they are handled correctly and on time, customers achieve true incident life cycle management for optimal protection.
- **Boosts operational performance**—Improves ROI by consolidating security information from across the organization into a central location, filtering out noise and false positives, and presenting real incidents. This enables a focused monitoring and response capability.
- **Assures compliance**—Facilitates regular review and reporting on enterprise security information, monitors security controls to validate their effectiveness and provides real-time enforcement of policies and best practices.

NetIQ Security Manager Linux

Type	HIDS
Operating System	Linux, OS/400 and i5/OS V5R2 or later, Unix, Windows, OS/390
Hardware	• Dual processor dual-core (AMD®/Intel® recommended). Quad processors recommended for large environments. • 2 GB RAM (minimum); 4 GB RAM (recommended) • Windows Server 2003 • Microsoft SQL Server 2005 SP2 for the Database and Reporting Servers. Enterprise Edition is recommended for Reporting Server. Reporting Server also requires Microsoft SQL Server 2005 Analysis Services with Service Pack 2, Microsoft SQL Server 2005 Integration Services (SSIS) • IIS 5.0, IE 6.0, Office 2003 Web Components and more are required for Trend Analysis reports.
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	NetIQ
URL	*http://www.netiq.com/*

Osiris®

Abstract

Osiris is a host integrity monitoring system that can be used to monitor changes to a network of hosts over time and report those changes back to the administrator(s). Currently, this includes monitoring any changes to the file systems. Osiris takes periodic snapshots of the file system and stores them in a database. These databases, as well as the configurations and logs, are all stored on a central management host. When changes are detected, Osiris will log these events to the system log and optionally send email to an administrator.

In addition to files, Osiris has the ability to monitor other system information including user lists, group lists, and kernel modules or extensions.

Some integrity monitoring systems are signature-based—that is, they look for specific file attributes as a means of detecting malicious activity. Osiris is intentionally not like this. Osiris will detect and report changes to a file system and let the administrator determine what, if any, action needs to take place.

Osiris

Type	HIDS
Operating System	Linux, Unix, Windows
Hardware	Required
License	Open Source
NIAP Validated	
Common Criteria	
Developer	Schmoo
URL	*http://osiris.shmoo.com*

OSSEC HIDS

Abstract

OSSEC HIDS is an open-source HIDS. It performs log analysis, integrity checking, rootkit detection, time-based alerting, and active response.

For single-system monitoring, the OSSEC HIDS can be installed locally on that box and perform all functions from there; however, for additional systems, an OSSEC server may be installed with one or more OSSEC agents that forward events to the server for analysis.

OSSEC HIDS

Type	HIDS
Operating System	FreeBSD, Linux, OpenBSD, Solaris, AIX, HP-UX, MacOSX, VMWare ESX, Windows
Hardware	Required
License	Open Source
NIAP Validated	
Common Criteria	
Developer	Daniel B. Cid
URL	*http://www.ossec.net/*

PivX preEmpt®

Abstract

preEmpt uses Active System Hardening™ to protect Windows desktops and servers against new threats by blocking the underlying vulnerabilities exploited by worms and viruses. preEmpt includes a comprehensive management console for enterprise use and an easy to use interface for individual users.

preEmpt	
Type	HIDS
Operating System	Windows
Hardware	Required
License	Commercial
NIAP Validated	
Common Criteria	
Developer	PivX Solutions, Inc
URL	*http://www.pivx.com/HomeOffice*

Samhain

Abstract

Samhain is a file and host integrity and intrusion alert system suitable for single hosts as well as for large, UNIX-based networks. Samhain offers advanced features to support and facilitate centralized monitoring. In particular, Samhain can optionally be used as a client/server system with monitoring clients on individual hosts, and a central log server that collects the messages of all clients.

The configuration and database files for each client can be stored centrally and downloaded by clients from the log server. Using conditionals (based on hostname, machine type, OS, and OS release, all with regular expresions) a single configuration file for all hosts on the network can be constructed.

The client (or standalone) part is called Samhain, while the server is referred to as Yule. Both can run as daemon processes.

Features

- Centralized monitoring,
- Web-based management console,
- Multiple logging facilities,
- Tamper resistance.

Samhain

Type	HIDS
Operating System	Cygwin/Windows, Linux, Unix
Hardware	Required
License	Open Source
NIAP Validated	
Common Criteria	
Developer	Samhain Labs
URL	*http://www.la-samhna.de/samhain/*

Tripwire® Enterprise

Abstract

The Tripwire Enterprise is a change audit assessment product that can ensure the integrity of critical data on a wide variety of servers and network devices (*e.g.,* routers, switches, firewalls, and load balancers) called nodes. It does this by gathering system status, configuration settings, file content, and file metadata on the nodes and checking gathered node data against previously stored node data to detect modifications.

The Tripwire Enterprise consists of a server application component (Tripwire Enterprise Server for Windows 2000, XP Professional, or 2003; Solaris 7, 8, or 9; or, Red Hat Enterprise Linux 3 or 4), a client application component (Tripwire Enterprise Agents for Windows 2000, XP Professional, and 2003; Solaris 8, 9, 10; Red Hat Enterprise Linux 3 and 4; SUSE® Enterprise Server 9; HP-UX 11.0, 11i v1, and 11i v2; and, AIX 5.1, 5.2, and 5.3), and a client administrative console application component (Tripwire Command Line Interface [CLI]). The Tripwire Enterprise Server utilizes the SSL mechanism provided by the Java Virtual Machine (JVM) in its information technology (IT) environment to facilitate *HTTPS* communication with the GUI and the CLI.

The product is also bundled with a database application (Firebird Database) to support the product's storage needs. The Firebird Database is considered part of the IT environment. While the product supports using the Firebird Database and the Tripwire Enterprise Server (TE Server) on different machines, they must run on the same machine in an evaluated configuration. The other Tripwire Enterprise components can run on different machines in various combinations. The Tripwire Enterprise Server is the only product installed and active on the machine in which it is running.

Tripwire Enterprise

Type	HIDS
Operating System	Linux, Unix, Windows
Hardware	**Windows and Linux** • 3.0 GHz x86 processor or compatible • 2 GB RAM • 2 SATA or SCSI hard drives • 3.2 GB free disk space • 4 GB Data storage space • 256-color display **900 MHz UltraSPARC III processor** • 2 GB RAM • 2 SATA or SCSI hard drives • 3.2 GB free disk space • 4 GB Data storage space • X-Windows capable display • 256-color display
License	Commercial
NIAP Validated	True
Common Criteria	EAL3
Developer	Tripwire, Inc.
URL	*http://www.tripwire.com/products/enterprise/*

Tripwire for Servers

Abstract

Tripwire for Servers is a file system integrity assessment tool designed to aid system administrators and users to monitor files for unauthorized or unexpected modification. Tripwire can ensure the integrity of critical data on the system(s) by detecting corrupted or altered files and reporting the occurrence to the system administrators, so corrective actions can be taken.

Tripwire Manager is a Java®-based application with a GUI that allows the administrator to manage multiple installations of Tripwire for Servers software from a central location. A Tripwire for Servers system can be managed by a single manager or multiple managers; however only one manager can issue commands to a Tripwire for Servers machine at a time. SSL is used to protect each communication link between the Tripwire Manager console and the Tripwire for Servers agents.

Following database initialization (creation of a data baseline in a known-good state), Tripwire for Servers conducts subsequent integrity checks, automatically comparing the state of the system with the baseline database. Any inconsistencies are reported to Tripwire Manager and to the host system's log file. Reports can also be emailed to an administrator. Additionally, Tripwire for Servers can execute commands automatically in response to violations or integrity checks.

Tripwire for Servers

Type	HIDS
Operating System	Compaq Tru64, IBM AIX, FreeBSD, Linux, Solaris, Windows
Hardware	**Tripwire for Servers** • Windows Intel Xeon and AMD Opteron (for x64 Edition) 128 MB RAM 12 MB disk space • Solaris® SPARC® 2-class processor or above Sun recommended current patch level for all versions 128 MB RAM 56 MB disk space • Solaris on x64/x86 Pentium® class processor or above 150 MB RAM 33 MB disk space • IBM AIX RS/6000 class processor or above 128 MB RAM 56 MB hard disk space • Linux Pentium-class processor or above Intel Xeon® and AMD® Opteron® (RHEL 3, 4 & 5, SUSE® EL 9) Intel Itanium® (for Red Hat Enterprise Linux® and SUSE® EL 9) Linux (x86) kernel 2.4 or higher glibc 2.3 and higher 128 MB RAM 25 MB disk space (Itanium II processor - 41 MB disk space) • FreeBSD 128 MB RAM 21 MB disk space • HP-UX PA-RISC 1.1 processor or higher 128 MB RAM 67 MB hard disk space • HP-UX 11i v2 (Itanium) Intel Itanium 128 MB RAM 82 MB hard disk space • Compaq® Tru64 UNIX S128 MB RAM 49 MB disk space

Hardware Cont.	**Tripwire Manager** • Windows Pentium IV class processor or above 1024 MB RAM 75 MB disk space (150 MB for installation) • Solaris Sun UltraSPARC II or higher processor 1024 MB RAM 86 MB disk space (229 MB for installation) X Window System • Linux Pentium IV class processor or above 1024 MB RAM 85 MB disk space (167 MB for installation) X Window System
License	Commercial
NIAP Validated	True
Common Criteria	EAL1
Developer	Tripwire
URL	*http://www.tripwire.com/products/servers/*

Arbor Networks Peakflow® X

Abstract

Peakflow X constructs a system-wide view of enterprise networks, auto-learning host behaviors to determine who talks to whom—and how. In addition to the real-time security information of Arbor's Active Threat Feed (ATF) service, Peakflow X also integrates data from Arbor's Active Threat Level Analysis System (ATLAS) —providing contextualized threat intelligence from a global and local perspective.

Peakflow X analyzes flow statistics to define normal network behavior. Then, in real time, its embedded network behavioral analysis (NBA) technology identifies abnormal activity that can indicate a developing security attack long before its signature is created.

Features

- **Built-in application intelligence**—With its integrated Application Intelligence collector, Peakflow X extends its network-wide visibility down to the application layer. This micro-level visibility helps maximize the performance, reliability and security of key applications; reduce cost and downtime by quickly resolving network issues; avoid over-provisioning a network to meet application demands; and expand application usage across geographically dispersed networks without risking bandwidth or security issues.
- **Network-wide visibility**—Leverage IP flow technology in existing network devices to achieve pervasive, cost-effective visibility and security of enterprise networks – including those based on MPLS.
- **Application intelligence**—Detect the applications on a network and identify who's using them – enabling you to improve the performance of critical business applications and form sound business reasons for network or application expansion and policy development.
- **Network behavioral analysis**—Understand the normal behavior of traffic including Voice over IP (VoIP) or P2P, and be alerted to abnormalities due to misconfigurations or malicious activity.
- **Layer 2 mitigation and visibility**—Quickly view where a host is connected to the network and stop them at the source, including auto-discovery of enterprise switches and elimination of troubled hosts from the network without affecting other hosts.
- **Zero-day protection**—Leverage anomaly detection to immediately identify zero-day threats.
- **Unrivalled threat analysis**—Optimize threat analysis and mitigation by combining unique Arbor capabilities: global visibility *via* ATLAS and local detection *via* ATF fingerprints.
- **Compliance assurance**—Monitor compliance with internal or external regulations (*e.g.,* SOX, GLBA, PCI) and be alerted to violations *via* network usage reports and audit trail.

Arbor Networks Peakflow X

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Arbor Networks
URL	*http://www.arbornetworks.com/*

ArcSight®

Abstract

The ArcSight product includes a security management software product designed to monitor, analyze, and report on network anomalies identified by third-party network monitoring devices (*e.g.,* IDS Sensors or IDS Scanners, firewalls). ArcSight then provides second-order IDS in that it provides enterprise-wide monitoring for sub-networks monitored by non-homogeneous network monitors. As such, ArcSight provides a solution for managing all network events and/or activities in an enterprise from a centralized view. ArcSight allows trusted users to monitor events, correlate events for in-depth investigation and analysis, and resolve events with automated escalation procedures and actions.

ArcSight Console is a centralized view into an enterprise that provides real-time monitoring, in-depth investigative capabilities, and automated responses and resolutions to events. The Console provides administrators, analyzer administrators, and operators with an intuitive interface to the Manager to perform security management functions that includes viewing the audit data.

ArcSight Manager is a high-performance engine that manages, cross-correlates, filters, and processes all occurrences of security events within the enterprise. The ArcSight Manager sits at the center of ArcSight and acts as a link between the ArcSight Console, ArcSight Database, and ArcSight SmartAgent.

The ArcSight Database is the logical access mechanism, particular schema, table spaces, partitioning, and disk layout. The ArcSight Database stores all captured events, and saves all security management configuration information, such as system users, groups, permissions, and defined rules, zones, assets, reports, displays, and preferences in an Oracle database.

ArcSight SmartAgent collects and processes events generated by security devices throughout an enterprise, such as routers, email logs, anti-virus products, firewalls, IDSs, access control servers, VPN systems, anti-DoS appliances, operating system logs, and other sources where information of security threats are detected and reported. Agents for the following products are included in the product—

- Nessus®, a vulnerability scanner that delivers its data as a report file;
- Check Point Firewall-1 NG OPSEC, a firewall that delivers its data *via* a proprietary, push protocol (OPSEC);
- Snort IDS DB, an intrusion detection system that delivers its data *via* a database (MySQL®).

ArcSight

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL3
Developer	ArcSight Inc.
URL	*http://www.arcsight.com*

Bro

Abstract

Bro is an open-source, Unix-based NIDS that passively monitors network traffic. Bro detects intrusions by first parsing network traffic to extract its application-level semantics and then executing event-oriented analyzers that compare the activity with patterns deemed troublesome. Its analysis includes detection of specific attacks (including those defined by signatures and by events) and unusual activities.

Bro uses a specialized policy language that allows a site to tailor Bro's operation, both as site policies evolve and as new attacks are discovered. If Bro detects something of interest, it can be instructed to either generate a log entry, alert the operator, or execute an operating system command. In addition, Bro's detailed log files can be particularly useful for forensics. Bro targets high-speed (Gigabytes per second [Gbps]), high-volume intrusion detection. By leveraging packet-filtering techniques, Bro is able to achieve the necessary performance while running on commercially available PC hardware.

Bro	
Type	NIDS
Operating System	Unix
Hardware	**Processor** • 1 GHz CPU (for 100 BT Ethernet with average packet rate <= 5,000 packets/second) • 2 GHz CPU (for 1000 BT Ethernet with average packet rate <= 10,000 packets/second) • 3 GHz CPU (for 1000 BT Ethernet with average packet rate <= 20,000 packets/second) • 4 GHz CPU (for 1000 BT Ethernet with average packet rate <= 50,000 packets/second) (Note: these are very rough estimates, and much depends on the types of traffic on your network [*e.g., HTTP, FTP,* email, *etc.*].) **Operating System** • FreeBSD 4.10 *(http://www.freebsd.org/)* Bro works with Linux and Solaris as well, but the performance is best under FreeBSD. In particular, there are some performance issues with packet capture under Linux. **Memory** • 1 GB RAM is the minimum needed, but 2–3 GB is recommended **Hard disk** • 10 GByte minimum, 50 GByte or more for log files recommended **Network Interfaces** • 3 interfaces are required: 2 for packet capture (1 for each direction), and 1 for host management. Capture interfaces should be identical.
License	Open Source
NIAP Validated	
Common Criteria	
Developer	Lawrence Berkeley National Laboratory
URL	*http://www.bro-ids.org/*

Check Point IPS Software Blade

Abstract

The Check Point IPS Software Blade provides complete, integrated, next generation firewall intrusion prevention capabilities at multi-gigabit speeds. The IPS Blade provides complete threat coverage for clients, servers, and OS. The Multi-Tier Threat Detection Engine combines signatures, protocol validation, anomaly detection, behavioral analysis, and other methods to provide IPS protection. The IPS Blade is supported by the global Check Point Research and Response Centers.

Benefits

- **Complete IPS protection**—A fully functioning IPS integrated into an existing firewall;
- **Dynamic management**—A complete set of management tools including real-time event views and an automated protection process;
- **Protection between patches**—Reinforces security during delays in the patching process.

Check Point IPS Software Blade

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Check Point Software Technologies, Inc.
URL	*http://www.checkpoint.com/products/softwareblades/intrusion-prevention-system.html*

Check Point VPN-1 Power

Abstract

VPN-1 Power security gateways provide an active defense. A central element of Check Point's unified security architecture, VPN-1 Power adapts as new applications are introduced and new threats appear. The result is an integrated firewall, VPN, and intrusion prevention solution. As part of Check Point's Unified Security Architecture, VPN-1 Power integrates with other Check Point solutions to simplify security management and deployment.

Benefits

- FireWall-1 security with integrated firewall, VPN, and intrusion prevention;
- Accelerated security up to 12 Gbps;
- Accelerated SmartDefense intrusion prevention up to 6.1 Gbps;
- Simple centralized management of a unified security architecture;
- Protection against new threats through SmartDefense Services.

Check Point VPN-1 Power

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL4
Developer	Check Point Software Technologies, Inc.
URL	*http://www.checkpoint.com/*

Check Point VPN-1 Power VSX

Abstract

The VSX security operations platform is a virtualized security gateway that enables the creation of hundreds of security systems on a single hardware platform. Based on VPN-1® Power, VSX provides firewall, VPN, URL filtering and intrusion prevention technology to multiple networks, securely connecting them to each other and shared resources, such as the Internet and DMZs. All security systems, virtual and real, are centrally managed through Check Point SmartCenter or Provider-1 management consoles. Turnkey VSX-1 appliances further reduce deployment cost while delivering carrier-class reliability and scalability.

Benefits

- Unique and comprehensive virtualized security solution with firewall, VPN, IPS, and URL filtering;
- Consolidate hundreds of security gateways to a single device, increasing device hardware utilization and reducing power, space, and cooling;
- Linear scaling of performance up to 27 Gbps;
- Flexible deployment options including software and a full line of turnkey appliances;
- Single proven security management architecture;
- Flexible Deployment Options.

Check Point VPN-1

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL4
Developer	Check Point Software Technologies Inc.
URL	*http://www.checkpoint.com/*

Cisco® ASA 5500 Series IPS Edition

Abstract

With its solid firewall and advanced application security capabilities, the Cisco ASA 5500 Series IPS Edition provides robust and stable policy enforcement. Intrusion prevention and antiworm capabilities enable the Cisco ASA 5500 Series IPS Edition to protect assets from sophisticated attacks.

Capabilities of the solution include:

- **Accurate, multi-vector threat protection**—The Cisco ASA 5500 Series IPS Edition combines inline intrusion prevention services with innovative technologies that improve accuracy.
- **Network integration and resiliency**—Building on Cisco networking expertise, the Cisco ASA 5500 Series IPS Edition provides tight integration with other network elements, increasing the effectiveness of security technologies.
- **Threat-protected VPN**—Building upon the market-proven VPN capabilities of the Cisco VPN 3000 Series Concentrator, the Cisco ASA 5500 Series IPS Edition provides secure site-to-site and remote-user access to corporate networks and services.
- **Complete incident life-cycle management**—The Cisco management and monitoring suite enables large-scale deployment and operation of the Cisco ASA 5500 Series IPS Edition. Also included with the solution is the Cisco Adaptive Security Device Manager, which provides a browser-based management and monitoring interface for individual devices.

Cisco ASA 5500 Series IPS Edition

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Cisco
URL	*http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_brochure0900aecd80402ef4.html*

Cisco Catalyst® 6500 Series Intrusion Detection System Services Module (IDSM-2)

Abstract

The Cisco® Catalyst® 6500 Series Intrusion Detection System Services Module (IDSM-2) is an IPS solution to safeguard organizations from costly and debilitating network breaches and help ensure business continuity. The second-generation Cisco IDSM2 protects switched environments by integrating full-featured IPS functions directly into the network infrastructure through the widely deployed Cisco Catalyst chassis. This integration allows a user to monitor traffic directly off the switch backplane—a logical platform for the additional services of a firewall, a VPN, or IPSs.

Cisco Intrusion Detection System Module (IDSM2)

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Cisco
URL	*http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/*

The Cisco IDSM2 with Cisco IPS Sensor Software v5.0 helps users through the use of the following elements—

- **Multi-vector threat identification**—Detailed inspection of Layer 2–7 traffic protects a network from policy violations, vulnerability exploitations, and anomalous activity.
- **Accurate prevention technologies**—Cisco Systems' innovative Risk Rating feature and Meta Event Generator provide the confidence to take preventive actions on a broader range of threats without the risk of dropping legitimate traffic.

When combined, these elements provide a comprehensive inline prevention solution to detect and stop malicious traffic before it affects business continuity.

Cisco Guard XT

Abstract

Working in concert with Cisco Traffic Anomaly Detectors, Cisco Guards detect the presence of a potential DDoS attack, and block malicious traffic in real time, without affecting the flow of legitimate, mission-critical transactions, thus ensuring availability and business continuity. The Cisco Guard XT diverts traffic destined for a targeted device under attack (and only that traffic) and subjects it to the unique Multi-Verification Process (MVP) architecture from Cisco.

The MVP architecture imposes multiple layers of defense designed to identify and block the specific packets and flows responsible for the attack while allowing legitimate transactions to pass, ensuring business continuity even while under attack.

The Cisco Guard XT delivers multi-gigabit performance to protect the largest enterprises and service providers from distributed denial-of-service (DDoS) attacks by performing per-flow-level attack analysis, identification and mitigation to block specific attack traffic.

Cisco Guard XT

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Cisco
URL	*http://www.cisco.com/en/US/products/ps5888/*

Cisco Intrusion Detection System Appliance IDS-4200

Abstract

The Cisco IDS can analyze both the header and content of each packet. The Cisco IDS can analyze single packets or a complete flow for attacks while maintaining flow state, allowing for the detection of multi-packet attacks. The Cisco IDS uses a rule-based expert system to interrogate the packet information to determine the type of attack, be it simple or complex.

The Cisco IDS is a standalone product in that all data collection and analysis is performed on one dedicated hardware platform. These units are to be placed at strategic points throughout a target IT system and interrogate passing network traffic. In response to an attack, the Cisco IDS has several options that include generating an alarm, logging the alarm event, and killing TCP sessions.

The Cisco IDS can be managed remotely in two ways. The first is *via* Web pages over a transport layer security connection. The second is through the CLI over an Secure Shell (SSH) connection.

Cisco Intrusion Detection System Appliance IDS4200

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Cisco
URL	*http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/*

Cisco IOS IPS

Abstract

Cisco IOS IPS is an inline, deep-packet inspection-based solution that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at data centers and corporate headquarters, distributing the network level defense to stop malicious traffic close to its entry point at branch or telecommuter offices is also critical.

Benefits

- Provides network-wide, distributed protection from many attacks, exploits, worms, and viruses exploiting vulnerabilities in operating systems and applications;
- Eliminates the need for a standalone IPS device at branch and telecommuter offices as well as small and medium-sized business networks;
- Unique, risk rating based signature event action processor dramatically improves the ease of management of IPS policies;
- Offers field-customizable worm and attack signature set and event actions;
- Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions;
- Works with Cisco IOS® Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router;
- Supports nearly 2,400 attack signatures from the same signature database available for Cisco IPS appliances.

Cisco IOS IPS

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Cisco
URL	*http://www.cisco.com/en/US/products/ps6634/index.html*

Cisco Security Agent

Abstract

Cisco Security Agent is an endpoint security solution that combines zero-update attack protection, data loss prevention, and signature-based antivirus in a single agent. This blend of capabilities defends servers and desktops against sophisticated day-zero attacks, and enforces acceptable-use and compliance policies within a simple management infrastructure.

Benefits

- Zero-update protection reduces emergency patching in response to vulnerability announcements, minimizing patch-related downtime and IT expenses;
- Visibility and control of sensitive data protects against loss from both user actions and targeted malware;
- Predefined compliance and acceptable use policies allow for efficient management, reporting, and auditing of activities;
- "Always Vigilant" Security—The system is always protected, even when users are not connected to the corporate network or lack the latest patches.

Cisco Security Agent

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Cisco
URL	*http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html*

Enterasys Dragon Network Defense

Abstract

The Enterasys® 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. When deployed in combination with Enterasys SIEM and NMS Automated Security Manager, IPS facilitates the automatic identification, location, isolation and remediation of security threats. IPS also integrates seamlessly with Enterasys Network Access Control for post-connect monitoring of behavior once network access has been granted.

The advanced in-line IPS is designed to block attackers, mitigate denial of service attacks, prevent information theft, and ensure the security of VoIP communications—while remaining transparent to the network. Built upon 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 role-based access control rules. IPS leverages thousands of vulnerability and exploit-based signatures.

Dragon Network Defense

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Enterasys Networks
URL	*http://www.enterasys.com/products/ids/DSIMBA7*

ForeScout CounterAct® Edge

Abstract

The CounterACT Edge (formerly ActiveScout) security appliance delivers an approach to preventing network intrusions. Stop attackers based on their "proven intent" to attack without using signatures, anomaly detection, or pattern matching of any kind.

Attackers follow a consistent pattern. To launch an attack, they need knowledge about a network's resources. Potential intruders, whether humans or self-propagating threats, compile vulnerability and configuration information through scanning and probing prior to an attack. The information received is then used to launch attacks based on the unique structure and characteristics of the targeted network.

ForeScout's patented ActiveResponse® technology detects attackers' reconnaissance and responds to them with counterfeit information. If an intruder attempts to use this information to attack the network, he has proven his malicious intent and can be blocked before the network is compromised.

By focusing on the "proven intent" of potential attackers, CounterACT Edge's dynamic intelligence ensures elimination of threats before they ever reach the network—without ever requiring signatures, deep packet inspection, anomalous behavior, or manual intervention.

CounterAct Edge

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL 2
Developer	ForeScout Technologies, Inc.
URL	*http://www.forescout.com/activescout/index.html*

IBM Proventia® SiteProtector

Abstract

The IBM Proventia Network IPS stops Internet threats before impact and delivers protection to all three layers of the network: core, perimeter, and remote segments. Preemptive protection, or protection that works ahead of the threat, is available from IBM Internet Security Systems through its proprietary combination of line-speed performance, security intelligence, and a modular protection engine that enables security convergence.

Proventia SiteProtector

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL 2
Developer	IBM
URL	*http://www-935.ibm.com/services/us/index.wss/offerfamily/iss/a1030570*

Highlights

The Proventia protection engine employs multiple intrusion prevention technologies working in tandem tomonitor,detectorblocktheseclassesofnetworkthreats—

- Application attacks,
- Attack obfuscation,
- Cross-site scripting attacks,
- Data leakage,
- Database attacks,
- DoS and DDoS attacks,
- Drive-by downloads,
- Insider threats,
- Instant messaging,
- Malicious document types,
- Malicious media files,
- Malware,
- Operating system attacks,
- Peer-to-peer,
- Protocol tunneling,
- SQL injection attacks,
- Web browser attacks,
- Web server attacks.

Imperva SecureSphere®

Abstract

Imperva SecureSphere 6 is an IDS/IPS that monitors network traffic between clients and servers in real-time, analyses that traffic for suspected intrusions, and provides a reaction capability. Reaction options include recording and monitoring suspected traffic and ID events, blocking traffic, and generating alarms containing event notifications. Database auditing allows the user to record selected user database queries for audit purposes. Web queries and responses can also be selectively recorded. In addition, monitored databases can be actively scanned to identify potential vulnerabilities.

SecureSphere	
Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Imperva, Inc.
URL	*http://www.imperva.com/*

Intrusion SecureNet IDS/IPS

Abstract

To identify and control threats from unauthorized users, backdoor attackers, worms, and other network malware, securing a network beyond firewalls requires visibility into the nature and characteristics of network traffic. The Intrusion SecureNet System provides critical, deep-packet analysis and application awareness and can be deployed passively for ID or actively for intrusion prevention.

The SecureNet System can be deployed with the broadest range of network configurations. Passive ID deployments are possible without costly switch and router resources or reconfiguration and without creating a failure point in the network. Intrusion prevention deployments can be configured to block or pass network traffic on failure, with the option for hot-standby and high availability.

Benefits

- Software and hardware appliance options;
- Available for 10, 100, 250, 1000 Mbit/s networks;
- Tweak, tune, and create pattern-matching and protocol-decode signatures;
- Highly scalable and flexible management with Provider interface.

When used for detection, prevention, or both, the Intrusion SecureNet technology accurately detects attacks and proactively reports indicators of future information loss or service interruption. By using pattern matching for performance and protocol decoding for detecting intentional evasion, polymorphic attacks, and protocol and network anomalies, the SecureNet System protectis critical networks and valuable information assets. The SecureNet family uses a hybrid detection model that permits quick and easy updating of network signatures. It also has a scripting language and graphical interface for tuning, tweaking, and creating highly accurate and very specific protocol-decode detection signatures.

SecureNet IDS/IPS

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Intrusion, Inc.
URL	*http://www.intrusion.com/*

iPolicy® Intrusion Prevention Firewall Family

Abstract

All iPolicy Networks Intrusion Prevention Firewalls support multiple security services delivered in parallel at very high performance made possible by iPolicy Networks' Single Pass Architecture™. Multiple defense mechanisms, including IPS/IDS, Layer 7 stateful firewall and URL filtering, are intrinsically built into the solution. They successfully block worms/botnets, server exploits, spyware and Trojans, mitigate DoS/DDoS attacks and prevent blended threats from entering the network in addition to providing access control.

Benefits

- Comprehensive security: Firewall, IPS/IDS, DoS/DDoS, URL filtering;
- Real-time worm, spyware and attack protection;
- Layer 3–7 firewall-based control;
- High-speed transparent URL filtering;
- VLAN and Network Address Translation (NAT) support in both transparent and gateway mode;
- Security domain (virtualization) for all security functions;
- High-availability support;
- Centralized management with hierarchical delegation;
- Web-based updates (software, attack signatures, URL database, *etc.*);
- Comprehensive real-time reporting and monitoring.

iPolicy Intrusion Prevention Firewall Family

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	
Common Criteria	
Developer	iPolicy Networks
URL	*http://www.ipolicynetworks.com/products/ipf.html*

Juniper Networks® IDP

Abstract

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances protects the network from a wide range of attacks. By using industry-recognized stateful detection and prevention techniques, the IDP Series provides zero-day protection against worms, trojans, spyware, keyloggers, and other malware.

Features

- **Stateful Signature Detection**—Signatures are applied only to relevant portions of the network traffic determined by the appropriate protocol context. This minimizes false positives.
- **Protocol Anomaly Detection**—Protocol usage against published RFCs is verified to detect any violations or abuse. Proactively protect network from undiscovered vulnerabilities.
- **Traffic Anomaly Detection**—Heuristic rules detect unexpected traffic patterns that may suggest reconnaissance or attacks. Proactively prevent reconnaissance activities or block DDoS attacks.
- **QoS/DiffServ Marking**—Packets are marked using DiffServ code point. Optimize network and ensure necessary bandwidth for business-critical applications.
- **VLAN-Aware Rules**—Unique policies are applied to different VLANs. Apply unique policies based on department, customer, and compliance requirements.
- **Role-Based Administration**—More than 100 different activities can be assigned as unique permissions for different administrators. Streamline business operations by logically separating and enforcing roles of various administrators.
- **Domains**—Enable logical separation of devices, policies, reports, and other management activities. Conform to business operations by grouping of devices based on business practices.
- **IDP Reporter**—Pre-configured real-time reporting capability available in each IDP appliance. Provide detailed real-time reports from each IDP appliance installed in the network without taxing the central IT organization.
- **Profiler**—Capture accurate and granular detail of the traffic pattern over a specific time period. Provide details on what threats are encountered by the network as well as the mix of application traffic.

Juniper Networks IDP

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL 2
Developer	Juniper Networks, Inc.
URL	*http://www.juniper.net/us/en/products-services/security/idp-series/*

Lancope® StealthWatch®

Abstract

Lancope delivers behavior-based, enterprise solutions that unify flow-based anomaly detection and network performance monitoring across physical and virtual networks to save limited resources.

Leveraging NetFlow, sFlow and packet capture, Lancope's StealthWatch System combines behavior-based anomaly detection and network performance monitoring to protect critical information assets and ensure network performance by preventing costly downtime, repair, and loss of reputation.

StealthWatch eliminates network blind spots and reduces total network and security management costs. Delivering unified visibility across physical and virtual networks, StealthWatch provides network, security, and IT administrators with an single platform of network intelligence for all parties.

StealthWatch	
Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Lancope, Inc.
URL	*http://www.lancope.com*

McAfee® IntruShield® Network IPS Appliances

Abstract

The IntruShield IDS system is composed of a family of stand-alone sensor appliances and IntruShield ISM system. The seven sensor appliances are the IntruShield 1200, IntruShield 1400, IntruShield 2600, IntruShield 2700, IntruShield 3000, IntruShield 4000, and IntruShield 4010. All other components of the product are software only components that run on a Windows workstation.

The ISM system is an IPS management solution for managing IntruShield sensor appliance deployments for large and distributed enterprise networks. The ISM operates with an MYSQL database to persist configuration information and alert data.

Features

- **Security Audit**—The IntruShield Intrusion Prevention system generates audit records related to the administration/management of the TOE and traffic logs for IDS information.
- **Identification and Authentication**—The IntruShield Intrusion Prevention system requires users to provide unique identification (user IDs) and authentication data (passwords) before any access to the TOE is granted.
- **Security Management**—The IntruShield Intrusion Prevention system provides a Web-based (using *HTTPS)* management interface for all administration, including the IDS rule set, user accounts and roles, and audit functions.
- **Protection of Security Functions**—The IntruShield Intrusion Prevention system protects the security functions it provides through a variety of mechanisms. These mechanisms include the requirement that users must authenticate before any administrative operations can be performed on the system. The encrypted data transferred between the ISM and sensor uses a proprietary SSL implementation.

Intrusion Prevention Functions

- **System Data Collection**—The IntruShield Intrusion Prevention system has the ability to set rules to govern the collection of data regarding potential intrusions.
- **System Data Analysis**—The IntruShield Intrusion Prevention system provides tools to analyze both IDS traffic log data as well as audit information.
- **System Data Review, Availability and Loss**—The IntruShield Intrusion Prevention system provides a user interface for menu selectable data review. The data stores of the raw collection data are limited only by the storage capacity of the platform and table management of the database.

McAfee IntruShield Network IPS Appliances

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL3
Developer	McAfee, Inc.
URL	*http://www.mcafee.com/us/enterprise/products/network_intrusion_prevention/index.html*

NIKSUN® NetDetector®

Abstract

NIKSUN's NetDetector is a full-featured appliance for network security surveillance, signature-based anomaly detection, analytics, and forensics. It complements existing network security tools, such as firewalls, intrusion detection/prevention systems and switches/routers, to help provide comprehensive defense of hosted intellectual property, mission-critical network services and infrastructure.

NetDetector alerts on defined signatures and traffic patterns. Built-in modules provide complementary signature and statistical anomaly detection, thus locating the proverbial "needles" of actionable information in the "haystack" of raw data. Advanced reconstruction capabilities allow for detailed review of Web, email, instant messaging, *FTP,* Telnet, and other application content. NetDetector's highly intuitive Web-based GUI eliminates the need for a special client application.

Key Benefits

- 100 percent real-time visibility into the network;
- Continuous, in-depth real-time surveillance;
- Capture network events the first time and store events for post-event analysis;
- Drill down forensic analysis down to packet level;
- Signature and statistical anomaly detection;
- Advanced reconstruction of Web, email, instant messaging, *FTP,* Telnet, VoIP and other TCP/IP applications;
- String search within application content;
- Advanced scheduled and on-demand reporting;
- Flexible and secure data export/import, including common third-party formats;
- Event Viewer with immediate paths from event to analysis, packet or statistical information, report generation or application reconstruction screen;
- Unlimited storage (add as you grow);
- Secure and easy-to-use Web interface with Role-Based Access Control;
- Cisco IDS, Micromuse NetCool, IBM/Tivoli Risk Manager and Arcsight integration.

NIKSUN NetDetector

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	False
Common Criteria	
Developer	NIKSUN
URL	*http://www.niksun.com/Products_NetDetector.htm*

NitroSecurity® NitroGuard® Intrusion Prevention System

Abstract

NitroSecurity's NitroGuard IPS may be used on its own or tightly integrated with the NitroView ESM Unified Security Information and Event Management solution. NitroGuard supports a default set of over 4,500 unique security rules.

Alone, NitroGuard supports—

- Native flow collection;
- Virtual IPS operation;
- Highly-tuned rules to block:
  - Worms, trojans, spyware and other malicious content;
  - Port scans, buffer overflow, DoS, and other attacks;
  - Protocol and traffic anomalies;
  - Malformed traffic, Invalid headers, a fragmentation attacks;
  - Obfuscations & evasions;
  - Zero-day attacks;
- Built-in analysis for:
  - Event management;
  - Anomaly detection;
  - Event and flow compression.

When used with NitroGuard Database Activity Monitor (DBM), the system provides:

- Edge-to-core network protection
- Edge defense—to prevent breaches at the network perimeter (IPS);
- Network visibility—to catch anomalies and determine vectors through the network;
- Core defense—to prevent breaches at the database itself (DBM).

When used with NitroView ESM, the total solution provides:

- Simple management of rules across all NitroGuard IPS devices,
- Precise network and event information collection,
- Forensic analysis,
- Network flow analysis,
- Physical event mapping, pinpointing events within your network topology,
- Correlation of NitroGuard flow and event data to other host, application, and third-party event data collected by NitroView receivers,
- Automated remediation, including black-list capabilities.

NitroSecurity Intrusion Prevention System

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL3
Developer	NitroSecurity, Inc
URL	*http://nitrosecurity.com/information-security/intrusion-prevention/*

PreludeIDS® Technologies

Abstract

The Prelude Open Source IDS was created in 1998. Since its creation, security engineers and specialists have enthusiastically contributed to Prelude in the spirit of Open Source. Prelude is a Universal Security Information Management system. Prelude collects, normalizes, sorts, aggregates, correlates, and reports all security-related events independently of the product brand or license giving rise to such events; Prelude is "agentless."

PreludeIDS Technologies

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	False
Common Criteria	
Developer	PreludeIDS Technologies
URL	*http://www.prelude-ids.com/*

Q1 Labs QRadar®

Abstract

The Q1 Labs® QRadar product is an administrator configurable network security management and response system. QRadar collects and processes data both from network taps and from event collectors installed on network devices. The product produces prioritized security events by real-time event matching and by comparing the collected data to historical flow-based behavior patterns. The security events are then correlated by the product to produce weighted alerts, which are sent to the product users.

Benefits

- Reads network data in real-time, including data from GB networks;
- Allows for amount of payload information to be configured by bytes per Collector;
- Analyzes vulnerability data by correlating the event with the various types of raw data, normalized data, and Offences. As a result, weighted Offence alerts can be generated;
- Provides behavioral and event correlation analysis on surveillance information;
- Records results by date, time, and type;
- Generates internal events and their associated violations;
- Sends alerts based on analysis of defense perspective data;
- Provides security responses to block network security threats based on analysis of defense perspective data;
- Generates automatic reports on defense perspective data;
- Provide administrators and users the ability to review the defense perspective data they are authorized to view.

QRadar

Type	NIDS
Operating System	
Hardware	Required
License	Commercial
NIAP Validated	True
Common Criteria	EAL 2
Developer	Q1 Labs, Inc.
URL	*http://www.q1labs.com/*

Radware DefensePro®

Abstract

Radware's DefensePro™ is a real-time IPS that maintains business continuity by protecting IP infrastructure against existing and emerging network-based threats that cannot be detected by traditional IPS, such as application misuse threats, SSL attacks, and VoIP service misuse. DefensePro features full protection against vulnerability-based threats through proactive signature updates, which safeguard against already known attacks including worms, trojans, botnets, SSL-based attacks, and VoIP threats. Unlike alternatives that rely on static signatures, DefensePro provides behavioral-based and automatically generated real-time signatures that prevent non-vulnerability-based threats and zero-minute attacks, such as application misuse attacks, server brute force attacks, application, and network flooding.

DefensePro offers adaptive, behavior-based protection capabilities at client, application server, and network levels. It immediately identifies and mitigates a wide range of network attacks (including non-vulnerability threats and zero-minute attacks) by automatically generating real-time signatures. The real-time signature "engine" is an adaptive multi-dimension decision engine that deploys fuzzy logic technology for accurate attack detection and mitigation without blocking legitimate user traffic.

DefensePro's behavior-based, self-learning mechanism proactively scans for anomalous network, server. and client traffic patterns. When detecting an attack, DefensePro characterizes the attack's unique behavior, establishes a real-time signature, and creates a blocking rule. A closed feedback mechanism dynamically modifies the signature characteristics as the attack unfolds and mutates, protecting against even the most sophisticated attacks with a high degree of accuracy. DefensePro rapidly and accurately distinguisesh between three broad categories of behavior: legitimate normal traffic, attack traffic and unusual patterns created by legitimate activity.

DefensePro

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	
Common Criteria	
Developer	Radware
URL	*http://www.radware.com/Products/ApplicationNetworkSecurity/DefensePro.aspx*

SecurityMetrics Appliance

Abstract

The SecurityMetrics Appliance is an integrated hardware and software solution that provides advanced ID and intrusion prevention functionality that analyzes network traffic and automatically stops attacks.

Features

- **Intrusion detection and prevention**—The SecurityMetrics Appliance is an integrated hardware and software solution. It provides advanced ID and intrusion prevention functionality that analyzes your network traffic and automatically stops attacks 24x7.
- **Vulnerability assessment**—Perform unlimited vulnerability assessment scanning of an entire network. Schedule the scans to run at off-peak hours, receive emails whenever computer risk increases, and receive repair instructions in each security report.
- **Firewall and router**—Optional firewall and router modules are provided with each appliance. These modules complement and are compatible with existing network infrastructure and security equipment.
- **Intelligent IDS technology**—Each attack is compared to the vulnerability assessment database to confirm it is a real threat. If the attack is not a real threat, then an alert is not sent. This saves time, reduces false positives, and alerts you only when real threats are occurring.

SecurityMetrics Appliance

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	False
Common Criteria	
Developer	SecurityMetrics, Inc.
URL	*https://www.securitymetrics.com/appliance_features.adp*

Snort®

Abstract

Snort is an open-source network intrusion prevention and detection system using a rule-driven language that combines the benefits of signature, protocol, and anomaly-based inspection methods.

Snort	
Type	NIDS
Operating System	Linux
Hardware	Required
License	Open Source
NIAP Validated	False
Common Criteria	
Developer	Marty Roesch
URL	*http://www.snort.org*

snort_inline

Abstract

snort_inline is a modified version of Snort that accepts packets from iptables and IP firewall (IPFW) *via* libipq(linux) or divert sockets(FreeBSD), instead of libpcap. It then uses new rule types (drop, sdrop, reject) to tell iptables/IPFW whether the packet should be dropped, rejected, modified, or allowed to pass based on a snort rule set. This acts as an IPS that uses existing IDS signatures to make decisions on packets that traverse snort_inline.

snort_inline	
Type	NIDS
Operating System	Linux
Hardware	Required
License	Open Source
NIAP Validated	False
Common Criteria	
Developer	William Metcalf
URL	*http://snort-inline.sourceforge.net*

Sourcefire 3D® Sensor

Abstract

Sourcefire 3D Sensors are purpose-built network security appliances available with throughputs from 5 Mbps up to 10 Gbps. 3D Sensors running Sourcefire's intrusion prevention (Sourcefire IPS™), network intelligence (Sourcefire RNA®), and user identity (Sourcefire RUA™) software can be deployed to protect all areas of a network—the perimeter, the DMZ, the core, and critical internal network segments.

Features

- **Fault Tolerance and High Availability**—3D Sensors are available with critical fault-tolerant features, such as fail-open copper and fiber ports, dual power supplies, and RAID drives, and each sensor supports an array of high availability configuration options. With up to 10 Gbps of IPS throughput, latency of less than 100 microseconds, and fully redundant configurations, 3D Sensors meet the requirements of today's largest networks.
- **Simple and Easy to Use**—The plug-and-protect nature of 3D Sensors with Sourcefire IPS enables customers to easily install and configure their IPS with minimal effort and training. For customers with limited IT security resources, the process of tuning an IPS can be fully automated to ensure that each IPS is continuously optimized to protect the dynamic network environment.

Using the powerful Sourcefire Defense Center™ management console, customers can centrally manage up to 100 3D Sensors, analyze events, configure and push IPS and RNA (Real-time Network Awareness) policies, automatically download and apply Sourcefire's Snort® rule updates, and much more. For larger deployments or distributed IT security teams, customers can leverage Sourcefire Master Defense Center technology to manage multiple defense centers and many hundreds of 3D Sensors across their entire organization.

Sourcefire Intrusion Detection Sensors

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Sourcefire, Inc.
URL	*http://www.sourcefire.com/products/3D/sensor*

Sourcefire® Intrusion Prevention System

Abstract

Built on the legacy of Sourcefire's Snort® rules-based detection engine, Sourcefire IPS™ uses a powerful combination of vulnerability- and anomaly-based inspection methods—at throughputs and line speeds up to 10 Gbps—to analyze network traffic and prevent critical threats from affecting a network. The Sourcefire solution is divided into three customer protection phases—IPS, Adaptive IPS, and Enterprise Threat Management (ETM)—with each phase building upon the benefits and features of the previous one, adding capabilities to optimize a company's network protection.

Based on the Snort detection engine, Sourcefire intrusion prevention system intrusion defense with extensive analytics, powerful reporting, and unrivaled scalability. Through the use of Sourcefire 3D® Sensors and one or more Sourcefire Defense Center® management consoles, the IPS phase enables you to detect and/or block attacks targeting thousands of vulnerabilities.

Sourcefire offers an Adaptive intrusion prevention system strategy. The Adaptive intrusion prevention system phase incorporates the real-time/all-the-time network intelligence from Sourcefire RNA® (Real-time Network Awareness) to enable automated threat impact assessment and automated intrusion prevention system tuning, saving considerable time and effort. Adding RNA to 3D Sensors significantly reduces false positives and false negatives and allows small-sized IT security staff to effectively monitor large networks.

Sourcefire's ETM phase provides all-the-time/real-time knowledge of attacks, targets, and the state of critical systems fully integrated into one system. It couples Sourcefire's IPS solution with additional ETM capabilities, including user identity tracking, NBA) and IT policy compliance. Sourcefire's ETM provides the tools necessary to defend a network before, during, and after the attack.

Sourcefire Intrusion Detection Sensors

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Sourcefire, Inc.
URL	*http://www.sourcefire.com/solutions/etm/ips*

StillSecure Strata Guard

Abstract

Strata Guard high-speed IDS/IPS gives a real-time, zero-day protection from network attacks and malicious traffic. Strata Guard protects an enterprise from the network perimeter to the core; including remote and internal segments. It monitors network traffic—in-line or out of band—anywhere the potential for attack exists: at the perimeter, internally, in the DMZ, and between strategic connections to un-trusted networks.

Strata Guard is deployable in both in-line and out of band configurations—

- In-line deployment:
  - True IPS functionality
  - React instantaneously to attacks; drop offending packets (Pre-emptive policies™)
  - Highest level of protection—attacks cannot penetrate the network
  - Allows you to move from IDS to IPS functionality at your own comfort level
  - Available with fail-open bypass switch

- Out-of-band deployment:
  - Triggers alerts and notifications of suspicious activity
  - Provides history of attack events
  - Forensic tracking

StrataGuard	
Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	False
Common Criteria	
Developer	StillSecure
URL	*http://www.stillsecure.com/strataguard/index.php*

Symantec® Critical System Protection

Abstract

Symantec Critical System Protection 5.1 protects against day-zero attacks, hardens systems, and helps maintain compliance by enforcing behavior-based security policies on clients and servers. A centralized management console enables administrators to configure, deploy, and maintain security policies; manage users and roles; view alerts; and run reports across heterogeneous operating systems.

Features

- Provides prevention techniques that shield operating systems, applications, and services by defining acceptable behaviors for each function;
- Protects systems from misuse by unauthorized users and applications through system and device controls that lock down configuration settings, file systems, and the use of removable media;
- Provides monitoring, notification, and auditing features that ensure host integrity, system, and regulatory compliance;
- Enables cross-platform server auditing and compliance enforcement with graphical reporting engine featuring multiple queries and graphic formats to visually highlight data.

Symantec Critical System Protection

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	False
Common Criteria	
Developer	Symantec
URL	*http://www.symantec.com/business/critical-system-protection*

TippingPoint® Intrusion Prevention System

Abstract

The TippingPoint IPS is an in-line device that is inserted seamlessly and transparently into the network. As packets pass through the IPS, they are fully inspected to determine whether they are legitimate or malicious. This instantaneous form of protection is an effective means of preventing attacks from ever reaching their targets.

TippingPoint's IPSs provide application protection, performance protection, and infrastructure protection at gigabit speeds through total packet inspection. Application protection capabilities provide fast, accurate, and reliable protection from internal and external cyber attacks. Through its infrastructure protection capabilities, the TippingPoint IPS protects VoIP infrastructure, routers, switches, DNS, and other critical infrastructure from targeted attacks and traffic anomalies. TippingPoint's Performance Protection capabilities enable customers to throttle non-mission critical applications that hijack valuable bandwidth and IT resources, thereby aligning network resources and business-critical application performance.

The system is built upon TippingPoint's Threat Suppression Engine (TSE)—a highly specialized hardware-based intrusion prevention platform consisting of state-of-the-art network processor technology and TippingPoint's own set of custom application-specific integrated circuits (ASIC). The TippingPoint ASIC-based TSE is the underlying technology.

Through a combination of pipelined and massively parallel processing hardware, the TSE is able to perform thousands of checks on each packet flow simultaneously. The TSE architecture utilizes custom ASICs, a 20 Gbps backplane and high-performance network processors to perform total packet flow inspection at Layers 2-7. Parallel processing ensures that packet flows continue to move through the IPS with a latency of less than 84 microseconds, independent of the number of filters that are applied.

The TippingPoint TSE architecture also enables traffic classification and rate shaping. Sophisticated algorithms baseline "normal" traffic allowing for automatic thresholds and throttling so that mission-critical applications are given a higher priority on the network.

TippingPoint Intrusion Prevention System

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	TippingPoint Technologies, Inc.
URL	*http://www.tippingpoint.com/products_ips.html*

Top Layer IPS

Abstract

The Top Layer IPS™ solution includes (i) an in-line, transparent network appliance, (ii) Network Security Analyzer Software, a powerful real-time security event manager, (iii) IPS Controller software, a centralized management module for multi-device deployments and (iv) TopResponse™, a comprehensive threat update service together with (v) Hardware and software support and maintenance.

Top Layer's IPS appliances scale in performance from 300 Mbps to 4.4 Gbps. With Top Layer's ProtectionCluster™ capabilities, up to eight IPS appliances can be interconnected and provide transparent high-availability capabilities. The Top Layer IPS can be deployed in a variety of modes, including detection-only, pre-emptive blocking, or a combination of both. The Top Layer IPS detection/protection capabilities use an integrated three dimensional approach to perform thousands of inspections on each packet to filter out any malicious traffic.

Top Layer IPS

Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	False
Common Criteria	
Developer	Top Layer Security
Networks-URL	*http://www.toplayer.com/content/products/intrusion_detection/attack_mitigator.jsp*

Webscreen®

Abstract

Webscreen has been developed to ensure uninterrupted service and minimum performance degradation from an enterprise data centre and hosted service environments. Through its patented heuristic protocol, Webscreen intelligently monitors and filters Web traffic at the network perimeter, thereby maintaining connectivity for mission-critical services, and prioritizes bandwidth availability for core applications by identifying nonessential network traffic.

Webscreen	
Type	NIDS
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	False
Common Criteria	
Developer	Webscreen Technologies
URL	*http://www.webscreen-technology.com/*

AirMagnet®

Abstract

AirMagnet Enterprise provides a simple, scalable WLAN monitoring solution that enables any organization to proactively mitigate all types of wireless threats, enforce enterprise policies, prevent performance problems, and audit the regulatory compliance of all their WiFi assets and users worldwide. The enterprise WLAN monitoring solution offers complete visibility and control over the wireless airspace, enabling any enterprise to reliably deliver the same standards of security performance and compliance for their wireless networks as they expect from their wired networks.

New Improvements in Enterprise 8.0 Include:

- New security alarms,
- System-wide threat scoring,
- Spectrum forensics,
- Improved threat tracing,
- New overview page,
- Prioritized device monitoring,
- User impact analysis,
- Integration with AirMagnet survey,
- Streamlined workflow,
- System filtering,
- Automatic device classification,
- Association and roaming tracking,
- Report scheduling and delivery,
- Access control list (ACL) integration with Cisco controllers.

AirMagnet

Type	Wireless
Operating System	Windows
Hardware	AirMagnet Enterprise Server: • Intel® Pentium®-4 Processor 2.4 GHz or higher. (Dual Pentium®-4 Xeon Processor 3.0 GHz or higher recommended) • 1 GB of RAM (2GB recommended for larger deployments) • 20 GB Hard Disk Space • 10/100Mb Ethernet connection AirMagnet Enterprise Console: • Intel® Pentium®-Class Processor 2.0 GHz • 512 MB of RAM (1GB recommended) • 500 MB of hard disk space
License	Commercial
NIAP Validated	
Common Criteria	
Developer	
URL	*http://www.airmagnet.com/products/enterprise/*

AirSnare

Abstract

AirSnare is an IDS to help monitor a wireless network. AirSnare will generate alerts on to unfriendly MAC addresses and dynamic host configuration protocol requests. If AirSnare detects an unfriendly MAC address, it provides the option of tracking its access to IP addresses and ports or of launching Ethereal. Version 1.5 may include unspecified updates, enhancements, or bug fixes.

AirSnare

Type	Wireless
Operating System	Windows
Hardware	Required
License	Open Source
NIAP Validated	
Common Criteria	
Developer	
URL	*http://download.cnet.com/AirSnare/3000-2092_4-10255195.html*

AirTight® Networks SpectraGuard® Enterprise

Abstract

SpectraGuard Enterprise is a complete, end-to-end wireless intrusion prevention solution (WIPS). SpectraGuard Enterprise is suitable for customers who want to purchase the wireless security equipment and host it at their site.

SpectraGuard Enterprise is architected for maximum scalability and ease of deployment. It extends the trusted WIPS capabilities offered by AirTight.

Components

- **Server for Data Processing**—Processing of wireless security data is performed in server. Server can be set up in high availability mode to maximize up time.
- **SpectraGuard Managed Network Console (MNC)**—Console to manage multiple servers.
- **Wireless Scanners**—Wireless scanners for on-demand scanning and 24x7 monitoring. Wireless scanners scan wireless activity at locations where they are installed. Wireless scanner devices are also known as sensors. Wireless scanners transfer the scan data to the servers securely using industry standard AES encryption.
- **Web Browser**—Web browser to access user interface securely

AirTight Networks SpectraGuard Enterprise

Type	Wireless
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	True
Common Criteria	EAL2
Developer	Airtight Networks
URL	*http://www.airtightnetworks.com/*

Aruba® Wireless Intrusion Detection & Prevention (WIDP)

Abstract

Using existing access points, and sometimes dedicated sensors, Aruba's solution provides real-time wireless threat detection, attack prevention, policy enforcement, and compliance reporting.

Features

- Integration with Aruba's mobility infrastructure;
- Scanning several across the 802.11 frequency spectrum;
- Rogue AP & ad-hoc detection, location, classification, containment, and DoS detection;
- Fully automated threat prioritization and response;
- Pre-configured compliance reporting;
- Centralized and Web-accessible monitoring, troubleshooting, and analysis.

Aruba Wireless Intrusion Detection & Prevention (WIDP)

Type	Wireless
Operating System	N/A
Hardware	N/A
License	Commercial
NIAP Validated	
Common Criteria	
Developer	arubanetworks
URL	*http://www.arubanetworks.com/solutions/wids_widp.php*

Kismet

Abstract

Kismet is an 802.11 Layer 2 wireless network detector, sniffer, and IDS. Kismet will work with any wireless card that supports raw Radio Frequency Monitoring mode and can sniff 802.11b, 802.11a, and 802.11g traffic.

Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of non-beaconing networks *via* data traffic.

Kismet

Type	Wireless
Operating System	Linux
Hardware	Required
License	Open Source
NIAP Validated	
Common Criteria	
Developer	
URL	*http://www.kismetwireless.net*

Motorola® AirDefense® Mobile

Abstract

Motorola AirDefense uses collaborative intelligence with secure sensors that work in tandem with a hardened purpose-built server appliance to monitor all 802.11 (a/b/g) wireless traffic in real time.

Motorola AirDefense Mobile™ is a complementary solution to the AirDefense Enterprise monitoring platform, giving enterprises an AirDefense-powered mobile product to perform a real-time snapshot of all WLAN infrastructure and activity (802.11 a/b/g). This tool provides wireless device inventory, threat index analysis, location tracking, advanced rogue management and automated protection. Running on a Windows XP or 2000 platform, Motorola AirDefense Mobile installs on any laptop with an Atheros-based 802.11 a/b/g wireless card, such as Netgear (WAG511) or Cisco (CB21AG).

Motorola AirDefense Enterprise

Type	Wireless
Operating System	Windows
Hardware	
License	Commercial
NIAP Validated	True
Common Criteria	EAL 2
Developer	Motorola, Inc.
URL	*http://airdefense.net/products/admobile/index.php*

Functionality

Motorola AirDefense Mobile provides a real-time snapshotofall802.11a/b/gwirelessinfrastructure,including—

- Real-time device discovery and connection analysis,
- Advanced rogue management with threat indicators for rogue devices,
- Real-time threat detection and alarm expert help,
- Advanced location tracking including triangulation positioning,
- Automated protection with termination capabilities,
- Live view for traffic analysis,
- Wireless network usage statistics and health analysis,
- Capture file playback for off-site analysis and reporting,
- Advanced diagnostics tools for troubleshooting,
- Reporting capabilities.

Newbury Networks WiFi Watchdog™

Abstract

WiFi Watchdog is a server based software system that can be used "stand-alone" to enforce "No WiFi" policies as well as integrate with any existing Wi-Fi infrastructure (Cisco, Aruba, Symbol, Trapeze) to stop the increasing number of security threats not addressed by authentication, encryption. or VPNs.

Using Newbury's patented 802.11 device tracking capabilities, WiFi Watchdog precisely locates every WiFi device—in real-time, 24x7—to enforce the perimeter security of facilities and actively prevents neighboring users or skilled hackers from gaining unauthorized access to 802.11 WLAN resources.

WiFi Watchdog distinguishes legitimate clients from rogue access points, accurately characterizes weaknesses in a network; identifies and resolves security holes created by internal users or visitors; and alerts IT/security personnel with the precise physical location of vulnerabilities and attacks as soon as they appear.

WiFi Watchdog's flexible alerting architecture provides extensive intrusion detection capabilities. WiFi Watchdog identifies and locates an array of wireless attacks including MAC spoof, MAC storm, MITM, and DoS attacks. Alerts identify the physical location of the source of the attack. Watchdog supports real-time and rapid updates to attack signatures and integration with legacy network management tools.

WiFi Watchdog

Type	Wireless
Operating System	
Hardware	
License	Commercial
NIAP Validated	False
Common Criteria	
Developer	
URL	*http://www.newburynetworks.com/products-watchdog.htm*

SECTION 8 ▸ **Bibliography**

Allen, Julia; Christie, Alan; Fithen, William; McHugh, John; Pickel, Jed; Stoner, Ed. *State of the Practice of Intrusion Detection Technologies.* Pittsburg, PA: Carnegie Mellon Software Engineering Institute, January 2000

Base, Rebecca & Mell, Peter (2001). SP 800-31, *Intrusion Detection Systems.* Washington, DC: National Institute of Standards and Technology.

Kent, Karen & Mell, Peter (2006). SP 800-94, *Guide to Intrusion Detection and Prevention (IDP) Systems (DRAFT).* Washington, DC: National Institute of Standards and Technology.

Kent, Karen & Warnock, Matthew (2004). *Intrusion Detection Tools Report, 4th Edition.* Herndon, VA: Information Assurance Technology Analysis Center (IATAC).

Low, Christopher (2005). *Understanding wireless attacks & detection.* Bethesda, MD: The SANS Institute, Global Information Assurance Certification (GIAC) Security Essentials.

Thomas, Duncan. *http://compm067.paisley.ac.uk/notes/unit01.html.* ICT, Paisley University, 1999–2003.

SECTION 9 ▶ Definitions of Acronyms and Key Terms

Acronym or Term	Definition
3DP	Three Dimensional Protection
ACL	Access Control List
AIDE	Advanced Intrusion Detection Environment
AP	Access Point
ASIC	Application-Specific Integrated Circuit
ATF	Active Threat Feed
ATLAS	Active Threat Level Analysis System
BotNet	Robot Network
CLI	Command Line Interface
DDoS	Distributed Denial of Service
DiD	Defense in Depth
DMZ	Demilitarized Zone
DNS	Domain Name Server
DoD	Department of Defense
DOS	Disk Operating System
DoS	Denial of Service
DTIC	Defense Technical Information Center
EAL	Evaluation Assurance Level
ESM	Enterprise Security Manager
ETM	Enterprise Threat Management
FTP	File Transfer Protocol
Gbps	Gigabytes Per Second
GB	Gigabyte
GHz	Gigahertz
GIAC	Global Information Assurance Certification
GLBA	Gramm-Leach-Bliley Act of 1999
GUI	Graphical User Interface
HBSS	Host Based Security Systems
HIDS	Host-Based Intrusion Detection System
HIP	Host Intrusion Prevention
HIPS	Host-Based Intrusion Prevention System
HIPAA	Health Insurance Portability and Accountability Act of 1996
HP	Hewlett-Packard

Acronym or Term	Definition
HP-UX	Hewlett-Packard-UNIX
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IAC	Information Analysis Center
IATAC	Information Assurance Technology Analysis Center
ICMP	Internet Control Message Protocol
ID	Intrusion Detection
IDP	Intrusion Detection and Prevention
IDS	Intrusion Detection System
IDSM	Intrusion Detection System Module
IIS	Internet Information Server
IM	Instant Messaging
IO	Information Operations
IP	Internet Protocol
IPFW	IP Firewall
IPS	Intrusion Prevention System
ISAPI	Internet Server Application Programming Interface
IT	Information Technology
JVM	Java Virtual Machine
MAC	Mandatory Access Control
Mbps	Megabytes Per Second
MB	Megabyte
MITM	Man in the Middle
MVP	Multi-Verification Process
NAT	Network Address Translation
NBA	Network Behavioral Analysis
NBAD	Network Behavior Anomaly Detection
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NIDS	Network Intrusion Detection System
NSK	Non-Stop Kernel
Open SSL	Open Source Secure Sockets Layer
OS	Operating System
OSI	Open Systems Interconnection

Acronym or Term	Definition
PC	Personal Computer
PCI	Payment Card Industry
POSIX	Portable Operating System Interface
P2P	Peer-to-Peer
R&D	Research & Development
RAM	Random Access Memory
ROI	Return on Investment
SNMP	Simple Network Management Protocol
SOAR	State-Of-the-Art-Report
SOX	Sarbanes-Oxley Act
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
STI	Scientific and Technical Information
Syslog	System Log
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
Telnet	Telephone Network
TSE	Threat Suppression Engine
UDP	User Datagram Protocol
URL	Uniform Resource Location
VA	Vulnerability Assessment
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WIDP	Wireless Intrusion Detection & Prevention
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network