Everything You Need to Know About Intrusion Detection

NetProwler

2400 Research Boulevard

Rockville, MD 20850

1-888-44-AXENT

www.axent.com

Additional copies of this document or other AXENT publications may be ordered from your authorized distributor or directly from AXENT.

AXENT Technologies, Inc.
2400 Research Blvd. Suite 200
Rockville, MD 20850
1-888-44-AXENT
(301) 258-5043 (outside USA)
FAX: (301) 227-3745
Internet: www.axent.com

Table of Contents

1 Introduction

In recent years computer security has been a topic of great interest because of increased network usage and interconnectivity. Despite the undeniable progress made in network and computer security over the past few years, network devices and computers are still vulnerable from inside as well as outside attack.

Network Security: Still Incomplete

Increased exposure to the Internet has made most organizations aware of the dangers of a breach in network security. Most organizations have a defensive wall in the form of a firewall which protects against unwanted incoming traffic. However, network security solutions which can protect a network efficiently from Internet, do not work as well for Intranet security. Here are a few reasons why network security monitoring is becoming an essential component of keeping the network running smoothly:

Firewalls: An excellent first-line-of-defense

- Firewall are the first step towards implementing an organizational security policy
- Excellent perimeter security
- Mature products, proven techniques and useful enhancements such as VPN and remote user authentication
- However, Firewalls are mostly not suitable for high speed Intranets;
- Intranet security solution needs to be unobtrusive and transparent
- Current firewalls implementations can not keep up with Intranet (LAN) speeds
- Firewalls can not detect extensive Intranet attacks such information theft

Security Scanners: Finding holes yourself before an attacker does, could save the day

- Security assessment tools such as scanners provide the best way to evaluate OS and application security of critical resources
- Automated policy enforcement for security requirements such as software versions, password strengths etc.
- However, Most Scanners are
- not user friendly
- only report security holes, manual work required to correct them
- periodic execution required every time new OS, Server or App is installed on the network

Encryption/VPN: Best vehicle to transport sensitive application data

- Offers authentication of the sender/receiver, non-repudiation, reliability and integrity of the application data.

However, only the application data that uses VPN can be protected. All other traffic remains open and unprotected.

***Authentication and Authorization: If you are not allowed, YOU ARE NOT ALLOWED**

What acts as a catch-all for any activity that leaks through some or all of the above Security solutions?

To complete Network Security Monitoring and Enforcement, a tool is required which can passively monitor application and user sessions for unauthorized or malicious activity. Authorized and responsible users will see no impact on their application speed or access control. This maintains the openness of the Intranet. At the same time, as soon as a user becomes destructive, the user's application session can be terminated.

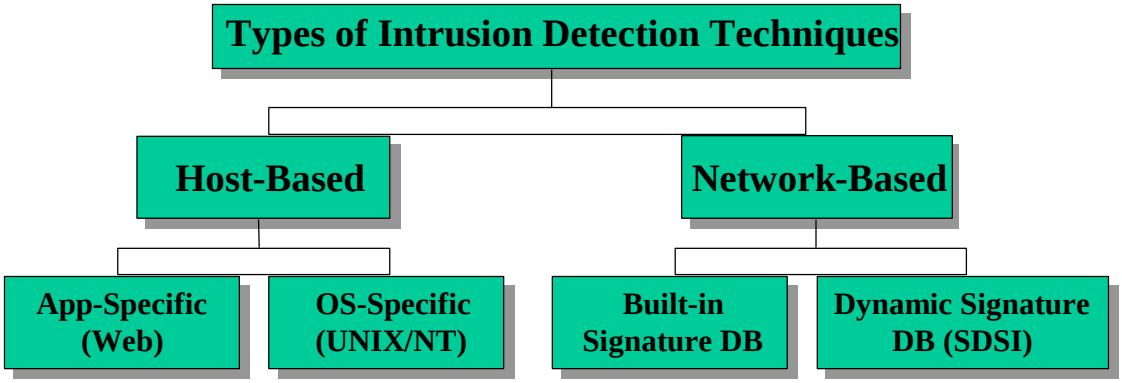
2 What is Intrusion Detection?

Network misuse has become as pervasive as the computer networking itself. Intrusion Detection is a new, retrofit approach for assuring network security in existing networks, while allowing resources to operate in an "open" mode. The goal of network intrusion detection is to identify in real time unauthorized use, misuse and abuse of computer systems by both internal network users and external attackers. Intrusion Detection is a challenging task because of the proliferation of heterogeneous computer networks, operating systems, communication protocols and networked applications. Increased network connectivity offers greater access to outsiders and makes it easier for intruders to avoid identification. To identify such misuse or abuse of networks and computers, Intrusion Detection systems (IDS) are built-in on the belief that an intruder's behavior will be noticeably different from that of an authorized user.

Types of Intrusion Detection Techniques

Over the years, several different types of Intrusion Detection Systems have been researched and developed. Initial IDS research were focused on analyzing log files created by the operating system and by different applications running on the system. Depending on the assumption that an intruder behavior would be different from that of an authorized user, these systems were developed to find abnormalities in log files and then analyze them to detect a possible attack. However, these IDS were complicated and did not have access to enough data to decisively identify an attack. Attention has been diverted to more sophisticated intrusion detection techniques based on analyzing host or network data taken directly from the physical network being monitored or the host/application being monitored.

The following is a description of the most common Intrusion Detection Techniques, their advantages and disadvantages:

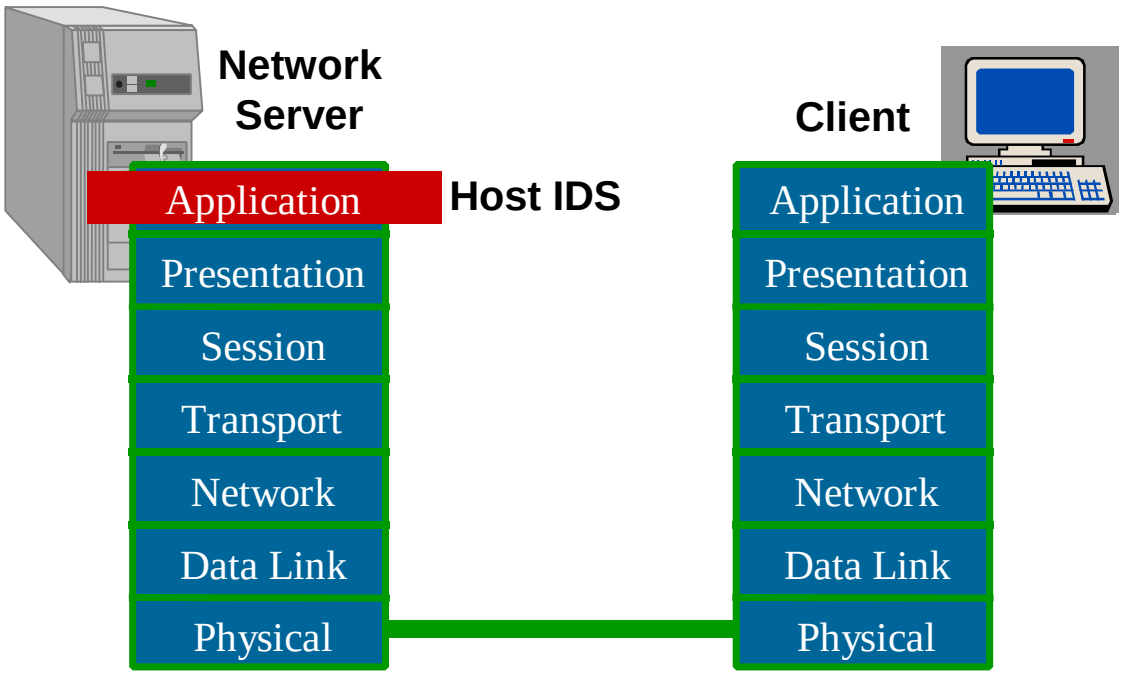


Host-Based Intrusion Detection

Some of the first IDS were built using Host-Based intrusion detection. An intelligent IDS agent runs on the host or server being monitored. The agent watches different aspects of the server security such as operating system log files, access log files, application log files etc. These forms of IDS thus depend on audit trails created by the OS or application servers. Typically Host-Based IDS employs an anomaly-detection model whereby a specific user's current session is statistically compared against the profile representing the user's normal behavior. Sophisticated algorithms are used to determine normal versus abnormal behavior. When a deviation from a normal user profile is observed, the IDS analyzes data to establish what it calls suspicious activity. Such information is forwarded to the appropriate network administrator as a suspected malicious session.

Host-Based IDS are designed to monitor a single host on which the IDS agent resides. As shown in the figure, typically this kind of IDS is able to watch data available from higher levels of protocol stack (as shown in the ISO 7-layer model below), which restricts its ability to monitor activity to those audit trail made by OS or applications. It also can

detect the activities which occur locally on the monitored host, such as file permission modification, user account setup etc.



In the Client-Server communication scenario above, the activities of a client accessing an application server are logged by the server. The IDS agent polling these log files extracts user activity information and tries to match that data against a statistically known user's normal behavior profile. There are two major types of Host-Based IDS: Application Specific IDS and OS Specific IDS.

OS-Specific IDS:

Most Host-Based IDS are based on monitoring the Operating System audit trails created while a user session is established on the server being monitored. First, a behavioral model of a normal use profile is created using statistical information gathered from OS log files and audit trails.

Several criteria are employed, such as time of work, number and type of files created, number and type of files accessed, etc. During the detection process, current audit trails are refined to those sessions that can be identified as abnormal such as unsuccessful login attempts. These sessions are then compared against the normal usage behavior using specific algorithms (they vary depending on the implementation). Suspicious sessions then are classified and reported to the network administrator.

Application-Specific IDS:

This type of IDS is designed to monitor intrusion or attack on a specific application server. At several large companies whose business relies on uninterrupted Database operation, specific IDS have been designed to monitor intrusions that relate to a database server. Because of wide popularity of World Wide Web on the Internet, there are some Web-Specific intrusion systems now available commercially.

The specific details of the application monitored is analyzed, a set of rules which define abnormal activities are selected, and the IDS is implemented to periodically check if any of those rules are observed in the last time period. A simple example of this type of IDS is a web server monitoring system. First, web server log files are analyzed to syntax of the logged entries. Then, a set of suspicious-activity rules are defined: for example, if the web root directory is being removed or web-server configuration is being altered. The IDS is then implemented to watch for those rules in the server log file.

Analysis of Host-Based IDS:

Pros:

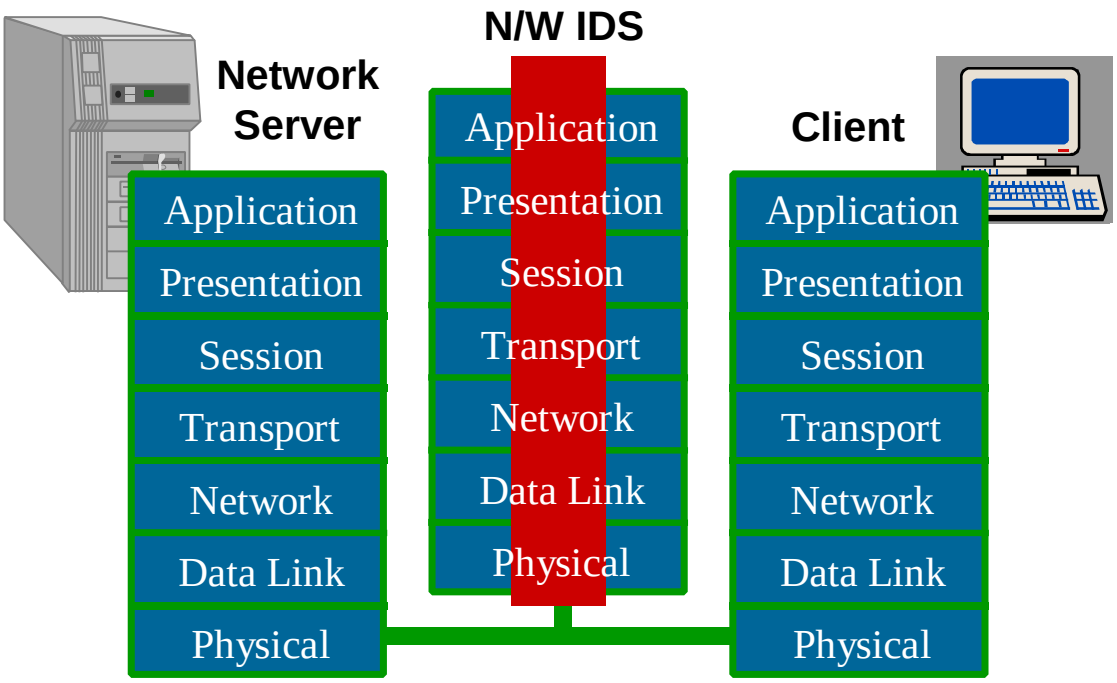
- Simpler to understand and configure for individual servers and applications.
- Tailored security since they are designed to monitor specific OS or Application.
- Only Host-Based IDS can detect an intrusion which occurs through

the local console.
- Only Host-Based IDS can enforce a User-based reaction policy when an attack is detected e.g. disable the user account, terminate user process etc.

Cons:
- Computational overhead on mission-critical server whose security is being monitored since the IDS resides on the same server.
- Network-based attacks which exploit protocol vulnerabilities are impossible to be detected.
- Since they analyze data from the audit trails, reaction to an attempted intrusion may not be in real-time.
- Complexity of deployment and administration increases with number of servers for enterprise-wide monitoring.

Network-Based Intrusion Detection

The main limitation of Host-Based IDS is that the access to audit trails is available only at the OS level or at the application level. The evolution of large networks requires monitoring data at all levels of communication. This shortcoming led to the development of Network-Based IDS.



As shown in the figure above, the IDS sitting in the middle of the communication path between client and server has access to data at all layers of communication. Therefore this type of IDS can do extensive analysis for attack detection. Since the IDS is running on a computer other than the server being monitored, there is no performance impact on the server computer at all.

Network-Based IDS forms its attack detection upon a comparison of parameters of the user's session and the user's commands to a rule-base of techniques used by attackers to penetrate a system. These techniques, called Attack Signatures, are what Network-Based IDS look for in the user's behavior. Since this model searches for patterns known to cause security problems, it is called a misuse detection model.

Analysis of Networked-Based IDS:

Advantages of Network-Based IDS versus Host-Based IDS:

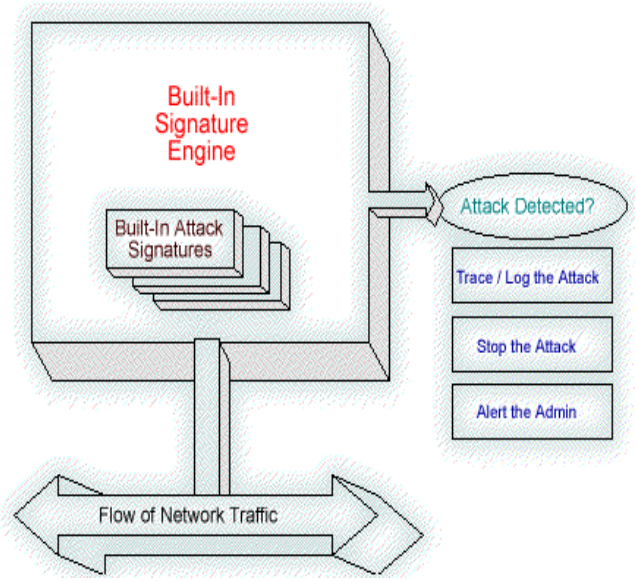
- No performance overhead on servers being monitored
- No overhead on the application sessions (completely transparent and unobtrusive)
- Intrusion Detection is in real-time and therefore immediate action (such as resetting the user session) can be taken
- Excellent overall security since it can monitor data at all 7-layers of OSI model

Network-Based IDS can be further divided in to two sub-categories, one that utilizes a built-in attack signature database, called Static Signature IDS, and the second which relies on signature information to be dynamically added in to the IDS, called Dynamic Signature IDS.

The Dynamic Signature IDS is the focus of discussion in this paper. However, to understand the architecture of Dynamic Signature IDS, it is useful to understand Static Signature IDS.

Built-in (Static) Signature Database IDS:

In the Network-Based IDS model, each attack signature is processed using a set of functions, which essentially represent a program, to detect that specific signature. The actual Static Signature or Built-in Signature database engine is a collection of such programs (processing functions), one for each attack signature which is built into the system. An attack signature can be any pattern or a sequence of patterns which constitutes a known security violation. These patterns are then monitored on the network data.



Built-In IDS:

- Each Attack Signatures is a pattern or set of patterns being matched in the network data.
- Processing of each attack signature is done through a separate processing function or functions.
- A new processing function(s) needs to be added every time a new signature is added in the engine.
- Most current Network-Based IDS are based on this technique

Pros:

- Most limitations of the Host-Based IDS are overcome

Cons:

- No real-time extensibility of new attack signatures. A new executable has to be deployed when new attacks are released
- Large overhead on the IDS performance because of sequential execution of processing functions.
- IDS Performance degrades further as more signatures are built-in

When such an attack signature is detected on any of the current user sessions, several actions can be taken to stop or trace the attacker.

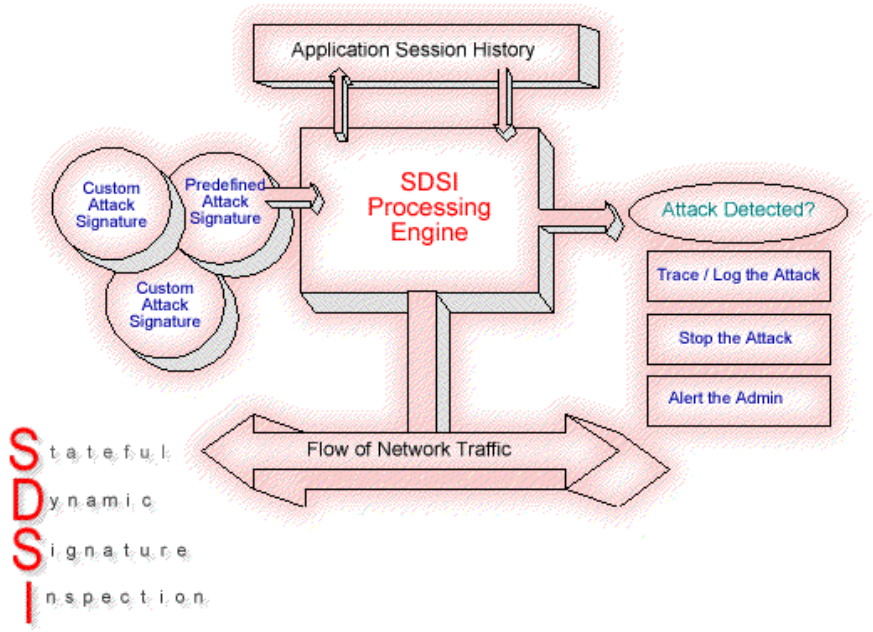
This type of IDS represents a major improvement over Host-Based IDS. However new limitations are imposed because of the architecture of the IDS engine. First, new attack signatures can not be deployed in real-time because the IDS has no processing function for them. Second, a new IDS engine has to be built and deployed
in order to add new attack signatures. The IDS performance also is impacted heavily because of the sequential execution of each processing function of the attack signatures. This overhead increases as the number of built-in signatures increase.

The built-in attack signature processing technique comes natural to all the vendors whose Intrusion Detection expertise is derived from their Security Scanner software. Since the knowledge of security holes is built into the Scanner software, which performs a security evaluation of networked hosts, similar techniques and signature knowledge is built into their IDS solution as well. That's why almost all currently available commercial solutions of Network-Based IDS utilize this technique.

3 Stateful Dynamic Signature Inspection (SDSI) IDS:

To overcome the limitations of extensibility and performance of the traditional Built-in Signature IDS, a new technique called Stateful Dynamic Signature Inspection has been developed by Internet Tools, Inc. With a strong background in Internet Security through experience in Firewall implementations, developers at Internet Tools, Inc. have designed a virtual processing machine that allows attack signatures to be executed as a set of instructions.

In this design each attack signature is a set of instructions which the SDSI virtual processor executes using a cache entry describing the current user session state and the current packet received from the network. Each network server being monitored will have a small set of associated attack signatures based on the Operating System of the server as well as Applications supported by the server.



As shown in the figure above, the SDSI virtual processor takes the current packet from the network data, brings in the state cache entry pertaining to the current user/application session, and then executes attack signatures from the signature cache which are optimized for the Server. When an attack is detected, the processor triggers the reaction module to take a set of actions against the attacker.

SSDI Pros

SDSI:

- A unique virtual processor design for Stateful Dynamic Signature Inspection
- Attack Signatures are represented as sophisticated instructions for the SDSI virtual processor
- SDSI processor is Stateful because it makes extensive use of optimized register cache entries which store application state information for the current application sessions.
- SDSI processor is Dynamic because new attack signatures can be added in real-time to the engine.

Pros:

Efficient:

- Utilizes optimized attack signature customization for server security based on OS and Apps supported
- High performance hashed state-cache lookup
- Register cache to store current info and instruction results

Extensible:

- Almost any type of attack signature can be configured using extensive instructions.
- New attack signatures can be added in real-time

Effective:

- Customized attack signatures can detect attacks on customer-specific resources
- Several Actions can be taken upon attack detection: Terminating the user session to prevent data theft or loss, recording a detailed log of the user session for later prosecution and others

Advantages of SDSI IDS versus Built-in Signature Engine IDS

- Powerful customer-specific resource security (such as customer Credit Card Database) through custom attack signatures
- Real-time addition of new and complex attack signatures
- Minimal performance impact of adding new attack signatures because of optimized look-ups and caching
- Completely extensible and customizable (new attacks can be defined in real-time)

SDSI thus offers the latest technological advancement in the Intrusion Detection Systems. SDSI technology overcomes all the restrictions of the Host-Based IDS as well as the Built-in Signature IDS.

Host-Based IDS using SDSI:

The Stateful Dynamic Signature Inspection (SDSI) technology is independent of whether it analyzes the network traffic or other data forwarding sources such as operating system audit trails or application log files. Therefore, it is feasible to build a host-based IDS with the server-based agents utilizing SDSI. The advantages here will be:

- SDSI brings extensibility, effectiveness and increased performance.
- Reduced resource impact on the server because of smaller foot-print of the SDSI engine and efficiency of signature execution.
- A tighter integration between Host and Network based IDS since they both use same underlying technology.

Comparing Various IDS:

A simple set of intrusion examples can explain limitations of each IDS described above. Assume a Hacker named Bob is trying to break in to the network.

App-Specific IDS:

Can Detect: A Web-Specific IDS can detect if Hacker Bob overwrites the web-server root directory with a set of dummy files.
Can't Detect: The same IDS can not detect if Hacker Bob deletes an important OS directory such as /etc on a UNIX server.

OS-Specific IDS:

Can Detect: AUNIX-OS-Specific IDS can detect if Hacker Bob deletes an important OS directory such as /etc on a UNIX server.
Can't Detect: The same UNIX-Specific IDS can not detect if Hacker Bob generates a network-based denial-of-service attack such as LAND (where an ill-formatted IP packet causes the server to go in an infinite loop consuming all it's protocol stack resources and unable to service any real user)

Built-in Signature IDS:

Can Detect: A network-based built-in signature IDS can detect if Hacker Bob generates a network-based denial-of-service attack such as LAND .
Can't Detect: The same IDS can not detect if Hacker Bob starts stealing customer credit cards information from an enterprise database.

SDSI IDS:

Can Detect: A hybrid network and host based SDSI IDS can detect all of the above attacks and more.

4 NetProwler: An SDSI Commercial Implementation for an Advanced Intrusion Detection System

NetProwler™ is a network intrusion detection and reaction system based on SDSI technology. It has the ability to monitor the traffic on the network for different kinds of intrusions regardless of whether the attack comes from an internal or an external attacker. It can be deployed on the network to monitor the Operating System as well as Application-specific security holes that can be exploited by an intruder. It coexists with other security products such as a Firewall on your network because it is completely unobtrusive. There is no performance penalty on the network because unlike Firewalls, all the data does not have to pass through the intrusion detection system.

- Is your Firewall protecting your network properly?
- Is there any internal misuse of the network resources?
- Are unauthorized users accessing sensitive information?
- Has someone broken in and changed your Web site or FTP site data?
- How can you enforce time-of-day accesses to your sensitive servers?
- If your network security is compromised, how can you trace the hacker and create an audit trail for legal action?

NetProwler Features

- ***Detection of over 200 well-known Internet attacks, including***
  - ***Port Scanning***
  - ***SYN Attacks***
  - ***Ping denial-of-service Attacks***
  - ***IP Address Spoofing***
- ***TCP sequence number Spoofing***
- ***Powerful Attack Detection Engine based on patent-pending SDSI technology***
- ***New attack signatures can be added and customized in real-time***

- ***Various actions can be taken upon attack detection such as stopping the session, taking full trace of the session, sending SNMP traps, email, page etc.***
- ***Data consistency checks for***
  - ***DNS server tables***
  - ***Router tables***
  - ***Web Server content***
  - ***FTP Server content***

- ***Inactive session purging***
- ***Time-of-day access for specific applications on servers***
- ***Completely transparent and non-obtrusive***
  Fully scalable to secure the complete Enterprise

NetProwler is a true Network-Based IDS based on SDSI Technology. It offers other unique features such as Data Consistency checks for various network resources such as web servers and routers. It can enforce Application specific time-of-day access for mission critical servers. NetProwler can be deployed Enterprise-wide to monitor intrusion at several strategic points. The centralized console allows a network administrator to monitor and deploy security policies across the Enterprise

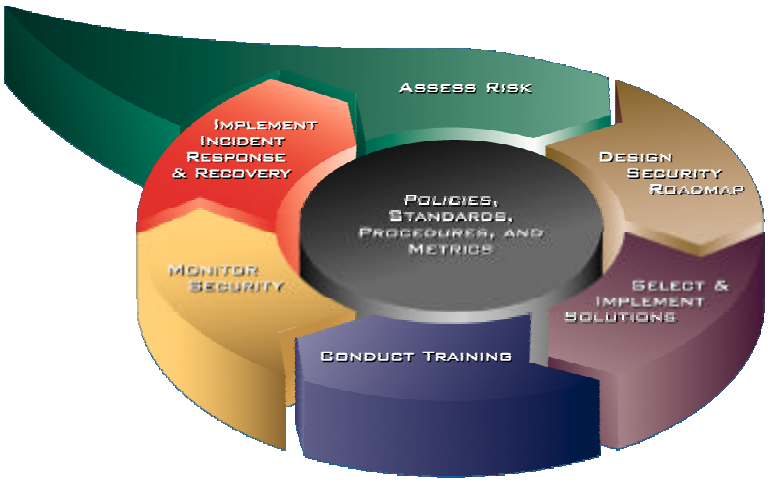
5 Summary

- Intrusion Detection is a retrofit approach to network security without having to change the existing network topology or resources.
- Several different types of IDS have been developed and are commercially available.
- Stateful Dynamic Signature Inspection (SDSI) is the most advanced IDS technology available in the industry.
- Extensibility of SDSI offers business advantage to Enterprise customers because of the ability to define new custom signatures which allows the IDS to monitor Enterprise-specific resource such as a proprietary database server or a manufacturing process plant.
- Hybrid IDS which make use of both Host and Network based components will be the future of intrusion detection systems

6 e-Security: Enabling E-Business

Lifecycle Security Solutions

Organizations are constantly adapting their information systems and networks to meet new business needs, particularly now since they are connected not only to employees, but to partners, customers and suppliers. Managing the risk associated with these changes requires a structured approach to assess information security issues. AXENT's Lifecycle Security™Model provides an organized methodology to understand the security needs of enterprise systems and networks. The Lifecycle Security Model allows companies to design, implement, maintain and modify their security architecture. With this model, a company can assess the information risk associated with business objectives and changes, then implement the "right" level of security for these conditions.



Only AXENT delivers e-security with our award-winning Lifecycle Security Solutions, a comprehensive approach based on our Lifecycle Security Methodology that takes into account all aspects of your dynamic business.

AXENT offers Lifecycle Security Solutions to:

-**ASSESS** vulnerabilities and ensure policy compliance
-**PROTECT** critical information systems
-**ENABLE** secure Internet usage
-**MANAGE** and administer users and resources

ASSESS

The first step to proactively reduce corporate risk is to effectively measure compliance to a business security policy and assess vulnerabilities where critical information resides. It is important to understand the effectiveness of a security policy, now and as it changes with businesses needs in order to properly define, manage and enforce business policies and assess possible threats.

Enterprise Security Manager™ manages and enforces your information security policy with one enterprise-wide security management solution. Enterprise Security Manager proactively checks the entire enterprise for security vulnerabilities, assesses security risks from one central console across tens of thousands of systems.

NetRecon™ leverages the latest technology to execute multiple scans simultaneously to quickly find, analyze and report perimeter and internal security vulnerabilities. NetRecon applies a unique patent-pending technology that operates in a collaborative tiger team approach to reveal hidden threats.

PROTECT

Organizations must protect information against unwanted users and hackers and control access to information to maintain business integrity.

Balancing these needs requires a solution set that protects data from within the perimeter, checks and detects attacks to the perimeter and controls access to information to assure customers that proprietary data is secured.

ntruder Alert™ monitors systems and networks in real-time to detect security breaches and suspicious activities and will respond automatically according to your established security policy. It works across your entire enterprise including LANs, WANs, intranets and the Internet.

NetProwler™ provides dynamic network intrusion detection that transparently examines network traffic to instantly identify, log and terminate unauthorized use, misuse and abuse of computer systems by internal saboteurs and external hackers. It's patent-pending SDSI™ virtual processor enable immediate deployment of customized attack signatures to terminate even the most sophisticated security violations.

Raptor® Firewall combines the highest level of perimeter security available with the performance, interoperability, scalability, and ease of use to meet your business goals. This award-winning firewall provides centralized, real-time enterprise security across the Internet, intranets, mobile computing and remote sites to give authorized users seamless, secure network access.

ENABLE

The Internet is an essential resource that enables organizations to communicate more efficiently reduce telecommunication costs and provides more timely information. It is critical to deliver information via the Internet to employees, partners and customers without compromising the security of that information. The Internet can help to enable new business opportunities and reduce operational costs.

Defender™ implements a two-factor authentication system to create one-time passwords that uniquely authenticates users and grants access

over dial-up, ISDN, Internet and on-LAN connections.

WebDefender™ provides secure single sign-on access control across a company's growing number of web applications and web servers. WebDefender centralizes the management of end user authentication and authorization to lower the cost of deploying your Web applications.

VPN Solutions (RaptorMobile™ & PowerVPN™) securely connect remote user, branch offices and third parties, to applications and data deep in a corporate network. Unlike traditional VPN products that only offer encrypted sessions, AXENT's VPN solutions enables the network manager to control, screen and granularly define where and what information an individual is allowed to access.

PassGo™ InSync provides enterprise password synchronization securely and quickly. PassGo InSync can be easily deployed producing immediate benefit of increased productivity through unified one-time password synchronization that can span multiple systems, servers, networks and applications.

PassGo SSO gives users a single point of access for business critical information. PassGo SSO is a fully customizable, flexible administration solution that verifies a user's credentials with the Authentication Service, which is used by all platforms to control access to the network and applications.

MANAGE

Today's enterprise computing environments consist of multiple operating systems running applications from different vendors and accessed by multiple client platforms. Organizations need a cost effective secure solution to manage and administer users and the computing resources from one central location. This streamlined administration allows organizations to manage more with fewer resources.

Enterprise Resource Manager™ greatly simplifies administrative

tasks for systems and security managers from one central repository. It provides enterprise-wide user and resource administration across distributed computing platforms, as well secure single sign-on to platforms and applications.

Resource Manager™ for UNIX® provides a graphical representation of system administration no matter what vendor's variation of UNIX you are using. As part of the comprehensive Enterprise Resource Manager family the Resource Manager for UNIX user interface provides full point-and-click use, drag and drop icons and on-line help. Managing UNIX system users across heterogeneous platforms has never been easier.

Privilege Manager™ for UNIX® controls access to root privileges with the first out-of-the-box solution. It allows delegation of UNIX root authority, so that you can implement reasonable security controls, without impacting the ability of users to perform their daily work.

Lifecycle Security Services

In addition to product solutions, AXENT provides services to effectively implement and deploy e-security solutions based on the Lifecycle Security approach. Our complete AXENT Services include top of the line Consulting, Education, and Customer Support to assist our customers before, during and after the implementation of security solutions.

Consulting: AXENT provides security services to effectively implement and deploy e-security solutions based on the Lifecycle Security Methodology. Through over 800 resellers and its independent subsidiary, Secure Network Consulting, Inc., AXENT offers a Lifecycle Security services program that includes on-site security consulting, assessment, integration, and training services. This program is business specific and scalable to suit each organization's individual dimensions.

Education: AXENT is dedicated to providing consistent, high-quality training to users of AXENT products. Our mission s to develop educational programs that help users increase their productivity through the effective use of AXENT products as the cornerstone of a comprehensive security solution.

Support: AXENT's skilled Customer Support team, help organizations attain the most value from their security software investment. They have access to the most current hardware and technical information available, which allows our teams to deliver a high degree of quality and responsive post-installation software support.

AXENT's products are used by 45 of the top Fortune 50 U.S. companies, five of the six largest public accounting firms, and industry leaders such as Sprint, OppenheimerFunds, Toronto Dominion Bank, Mobil, MCI and Unilever and government agencies including EPA and the U.S. Air Force.

For additional information, contact AXENT via e-mail at info@axent.com, or visit the company's Web site at www.axent.com