Case Study of Intrusion Detection and Prevention Techniques And Case Studies

By

Somboon Ingsakulsomboon

ID: 4229811

Project Proposal

Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Engineering in Telecommunication Management

Assumption University

November, 2004

Project Title: Intrusion Detection and Prevention

Name: Mr.Somboon Ingsakulsomboon

Project Advisor: Dr.Sudhiporn Patumtaewapibal

Academic Year: 2004

The Faculty of Engineering, Assumption University had approved this final report of the six credit course, TM 6900 Master Project, submitted in partial fulfillment of the requirements for the degree of Master of Science in Telecommunications Management.

Approval Committee :

(Dr.Sudhiporn Patumtaewapibal) (Asst.Prof.Dr.Kittiphan Techakittiroj)

Chairman / Advisor Member

(Assoc.Prof.Dr.Kobchai Dejhan)

MUA Representative

November 2004

Case Study of Intrusion Detection and Prevention Techniques And Case Studies-

By

Somboon Ingsakulsomboon

ID: 4229811

Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Engineering in Telecommunication Management

Assumption University

November, 2004

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The writer desires to express his most sincere appreciation and thanks to Dr.Sudhiporn Patumtaewapibal and Asst.Prof.Dr.Kittiphan Techakittiroj for their encouragement and advice through the course of this study and for their help in the preparation of this project.

LIST OF FIGURES

ABSTRACT

In network security has been critical after there are Internet connections. The security may speak like the word as "CONTROLABLITY". If you lost of the control that means you lost of security too. Everyone want the security for protect them from unwanted traffic that it may be the bother message until to the engine that can damage the system.

In the real-world, no security can protect a hundred percents, because the new attack was occurred everyday, every-minute, or every-second. The vulnerability has occurred if the programmer can't produce the product that hasn't the bug. However, we can find the best security in each environment.

The Security of one product isn't a total security. One product may be appropriate with one environment, but not appropriate with other. Before the Internet boom, we heard a virus attack that they were occurred on a standalone PC. We wanted only antivirus to prevent it. After the Internet boom, system connected the system to Internet. There were many unwanted traffics to the system. That time, a traffic control tool was used to block the unwanted traffics. The access-list was a simple tool in the router that done it. However, the access-list was difficult to manage the bi-directional traffics. This problem has happened until there is a stateful firewall technology.

Firewall market grown rapidly. Everyone wanted a firewall to protect their system for unwanted-traffics from Internet. Firewall was a solution of security but was not the end answer in today because it was filtering only unwanted traffics, but the vulnerability in application hasn't been protected. Therefore, security want have more a tool. There are many tools that provide security such as Encryption tool, Authentication tool, Intrusion Detection tool, Vulnerability Assessment tool, Database

Integrity tool and others. Each tool has a difference method. Intrusion Prevention tool is a new generation tool that it doesn't monitor only, but it has yet prevented the attacks. However, it must detect previously.

The project describes a history of security, vulnerabilities on today, and the market of IDS/IPS. Finally, we will see the Intrusion detection research and products in market that they are tested and announce a report from a trusted organization. We will have sample configurations of IDS/IPS on each strategy.

CHAPTER 1:INTRODUCTION THE SECURITY

1.1 History of Internet Security

The Internet began in 1969 as the ARPANET, a project funded by the Advanced Research Projects Agency (ARPA) of the U.S. Department of Defense. One of the original goals of the project was to create a network that would continue to function even if major sections of the network failed or were attacked. The ARPANET was designed to reroute network traffic automatically around problems in connecting systems or in passing along the necessary information to keep the network functioning. Thus, from the beginning, the Internet was designed to be robust against denial-of-service attacks, which are described in a section below on denial of service.

The ARPANET protocols (the rules of syntax that enable computers to communicate on a network) were originally designed for openness and flexibility, not for security. The ARPA researchers needed to share information easily, so everyone needed to be an unrestricted "insider" on the network. Although the approach was appropriate at the time, it is not one that lends itself to today's commercial and government use.

As more locations with computers (known as *sites* in Internet parlance) joined the ARPANET, the usefulness of the network grew. The ARPANET consisted primarily of university and government computers, and the applications supported on this network were simple: electronic mail (E-mail), electronic news groups, and remote connection to other computers. By 1971, the Internet linked about two dozen research and government sites, and researchers had begun to use it to exchange information not directly related to the ARPANET itself. The network was becoming an important tool for collaborative research.

During these years, researchers also played "practical jokes" on each other using the ARPANET. These jokes usually involved joke messages, annoying messages, and other minor security violations. Some of these are described in Steven Levy's *Hackers: Heroes of the Computer Revolution.* It was rare that a connection from a remote system was considered an attack, however, because ARPANET users comprised a small group of people who generally knew and trusted each other.

In 1986, the first well-publicized international security incident was identified by Cliff Stoll, then of Lawrence Berkeley National Laboratory in northern California. A simple accounting error in the computer records of systems connected to the ARPANET led Stoll to uncover an international effort, using the network, to connect to computers in the United States and copy information from them. These U.S. computers were not only at universities, but at military and government sites all over the country. When Stoll published his experience in a 1989 book, *The Cuckoo's Egg,* he raised awareness that the ARPANET could be used for destructive purposes.

In 1988, the ARPANET had its first automated network security incident, usually referred to as "the Morris worm". A student at Cornell University (Ithaca, NY), Robert T. Morris, wrote a program that would connect to another computer, find and use one of several vulnerabilities to copy itself to that second computer, and begin to run the copy of itself at the new location. Both the original code and the copy would then repeat these actions in an infinite loop to other computers on the ARPANET. This "self-replicating automated network attack tool" caused a geometric explosion of copies to be started at computers all around the ARPANET. The worm used so many system resources that the attacked computers could no longer function. As a result, 10% of the U.S. computers connected to the ARPANET effectively stopped at about the same time.

By that time, the ARPANET had grown to more than 88,000 computers and was the primary means of communication among network security experts. With the ARPANET effectively down, it was difficult to coordinate a response to the worm. Many sites removed themselves from the ARPANET altogether, further hampering communication and the transmission of the solution that would stop the worm.

The Morris worm prompted the Defense Advanced Research Projects Agency (DARPA, the new name for ARPA) to fund a computer emergency response team, now the CERT Coordination Center, to give experts a central point for coordinating responses to network emergencies. Other teams quickly sprang up to address computer security incidents in specific organizations or geographic regions. Within a year of their formation, these incident response teams created an informal organization now known as the Forum of Incident Response and Security Teams (FIRST). These teams and the FIRST organization exist to coordinate responses to computer security incidents, assist sites in handling attacks, and educate network users about computer security threats and preventive practices.

In 1989, the ARPANET officially became the Internet and moved from a government research project to an operational network; by then it had grown to more than 100,000 computers. Security problems continued, with both aggressive and defensive technologies becoming more sophisticated. Among the major security incidents were the 1989 WANK/OILZ worm, an automated attack on VMS systems attached to the Internet, and exploitation of vulnerabilities in widely distributed programs such as the sendmail program, a complicated program commonly found on UNIX-based systems for sending and receiving electronic mail. In 1994, intruder tools were created to "sniff' packets from the network easily, resulting in the widespread disclosure of user names and password information. In 1995, the method that Internet computers use to

name and authenticate each other was exploited by a new set of attack tools that allowed widespread Internet attacks on computers that have trust relationships with any other computer, even one in the same room.

As of 1996, the Internet connected an estimated 13 million computers in 195 countries on every continent, even Antarctica. The Internet is not a single network, but a worldwide collection of loosely connected networks that are accessible by individual computer hosts in a variety of ways; including gateways, routers, dial-up connections, and Internet service providers. The Internet is easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries or time of day.

However, along with the convenience and easy access to information come new risks. Among them are the risks that valuable information will be lost, stolen, corrupted, or misused and that the computer systems will be corrupted. If information is recorded electronically and is available on networked computers, it is more vulnerable than if the same information is printed on paper and locked in a file cabinet. Intruders do not need to enter an office or home, and may not even be in the same country. They can steal or tamper with information without touching a piece of paper or a photocopier. They can create new electronic files, run their own programs, and hide evidence of their unauthorized activity.

1.2 Basic Security Concepts

Three basic security concepts important to information on the Internet are confidentiality, integrity, and availability. Concepts relating to the people who use that information are authentication, authorization, and nonrepudiation.

When information is read or copied by someone not authorized to do so, the result is known as *loss of confidentiality.* For some types of information, confidentiality is a very important attribute. Examples include research data, medical and insurance records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals. This is particularly true for banks and loan companies; debt collectors; businesses that extend credit to their customers or issue credit cards; hospitals, doctors' offices, and medical testing laboratories; individuals or agencies that offer services such as psychological counseling or drug treatment; and agencies that collect taxes.

Information can be corrupted when it is available on an insecure network. When information is modified in unexpected ways, the result is known as *loss of integrity.* This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting.

Information can be erased or become inaccessible, resulting in *loss of availability.* This means that people who are authorized to get information cannot get what they need.

Availability is often the most important attribute in service-oriented businesses that depend on information (e.g., airline schedules and online inventory systems). Availability of the network itself is important to anyone whose business or education relies on a network connection. When a user cannot get access to the network or specific services provided on the network, they experience a *denial of service.*

To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. *Authentication* is proving that a user is whom he or she claims to be. That proof may involve something the user knows (such as a password), something the user has (such as a "smartcard"), or something about the user that proves the person's identity (such as a fingerprint). *Authorization* is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Authentication and authorization go hand in hand. Users must be authenticated before carrying out the activity they are authorized to perform. Security is strong when the means of authentication cannot later be refuted - the user cannot later deny that he or she performed the activity. This is known as *nonrepudiation.*

1.3 Why care about Security

It is remarkably easy to gain unauthorized access to information in an insecure networked environment, and it is hard to catch the intruders. Even if users have nothing stored on their computer that they consider important, that computer can be a "weak link", allowing unauthorized access to the organization's systems and information.

Seemingly innocuous information can expose a computer system to compromise. Information that intruders find useful includes which hardware and software are being used, system configuration, type of network connections, phone numbers, and access and authentication procedures. Security-related information can enable unauthorized individuals to get access to important files and programs, thus compromising the security of the system. Examples of important information are passwords, access control files and keys, personnel information, and encryption algorithms

Judging from CERT® Coordination Center (CERT/CC) data and the computer abuse reported in the media, no one on the Internet is immune. Those affected include banks and financial companies, insurance companies, brokerage houses, consultants, government contractors, government agencies, hospitals and medical laboratories, network service providers, utility companies, the textile business, universities, and wholesale and retail trades.

The consequences of a break-in cover a broad range of possibilities: a minor loss of time in recovering from the problem, a decrease in productivity, a significant loss of money or staff-hours, a devastating loss of credibility or market opportunity, a business no longer able to compete, legal liability, and the loss of life.

CHAPTER 2: INCIDENTS AND VULNERABILITY

2.1 Network Security Incidents

A *network security incident* is any network-related activity with negative security implications. This usually means that the activity violates an explicit or implicit security policy. Incidents come in all shapes and sizes. They can come from anywhere on the Internet, although some attacks must be launched from specific systems or networks and some require access to special accounts. An intrusion may be a comparatively minor event involving a single site or a major event in which tens of thousands of sites are compromised. (When reading accounts of incidents, note that different groups may use different criteria for determining the bounds of an incident.)

A typical attack pattern consists of gaining access to a user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites. It is possible to accomplish all these steps manually in as little as 45 seconds; with automation, the time decreases further.

2.2 Incidents Growth

Since the CERT® Coordination Center began operating in 1988, the number of security incidents reported to the center has grown dramatically, from less than 10 in 1988 to almost 140,000 in 2003, the last year for which complete statistics are available. Through 1994, the increase in incident reports roughly parallels the growth of the size of the Internet during that time. Figure 2-1 shows the growth in security incidents.

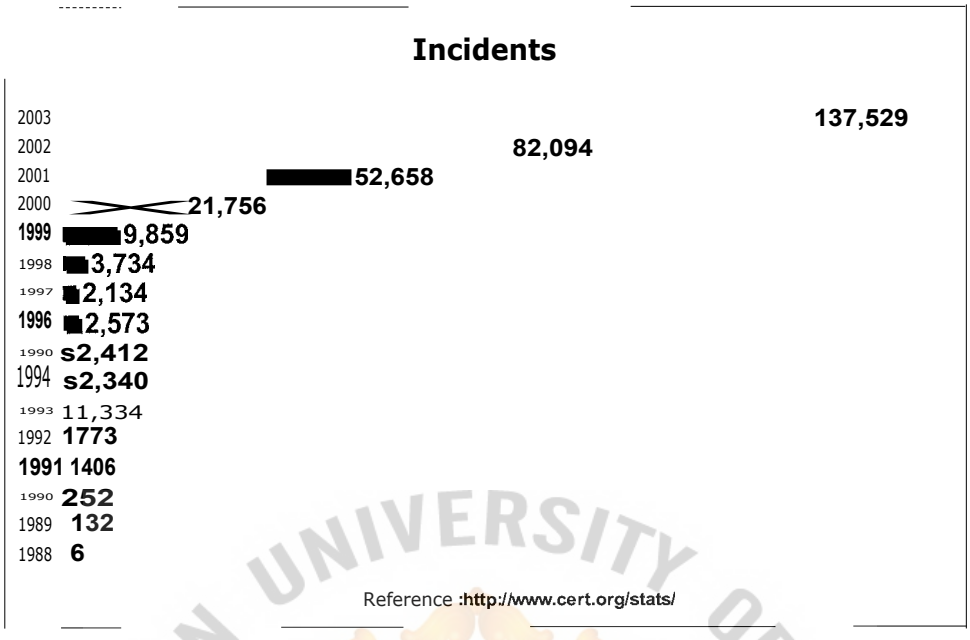


Figure 2-1 Growth in Security Incidents

The data for 1994 to 1997 show a slowing of the rate at which incidents are reported to the CERT/CC (perhaps because of sites' increased security efforts or the significant increase in other response teams formed to handle incidents). However, the rate continues to increase for serious incidents, such as root compromises, services outages, and packet sniffers.

In the late 1980s and early 1990s, the typical intrusion was fairly straightforward. Intruders most often exploited relatively simple weaknesses, such as poor passwords and misconfigured systems, which allowed greater access to the system than was intended. Once on a system, the intruders exploited one or another well-known, but usually unfixed, vulnerability to gain privileged access, enabling them to use the system as they wished.

There was little need to be more sophisticated because these simple techniques were effective. Vendors delivered systems with default settings that made it easy to break

into systems. Configuring systems in a secure manner was not straightforward, and many system administrators did not have the time, expertise, or tools to monitor their systems adequately for intruder activity.

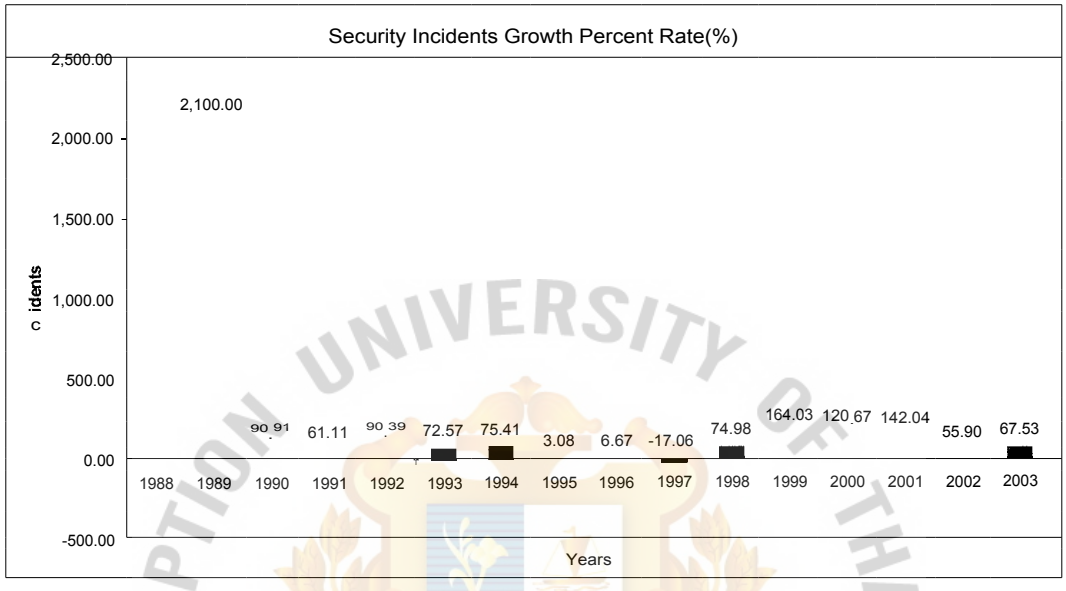


Figure 2-2 Security Incidents growth percent rate (%)

Unfortunately, all these activities continue in 1996; however, more sophisticated intrusions are now common. In eight years of operation, the CERT Coordination Center has seen intruders demonstrate increased technical knowledge, develop new ways to exploit system vulnerabilities, and create software tools to automate attacks. At the same time, intruders with little technical knowledge are becoming more effective as the sophisticated intruders share their knowledge and tools.

2.3 Internet Vulnerabilities

Vulnerability is a weakness that a person can exploit to accomplish something that is not authorized or intended as legitimate use of a network or system. When vulnerability is exploited to compromise the security of systems or information on

those systems, the result is a security incident. Vulnerabilities may be caused by engineering or design errors, or faulty implementation.

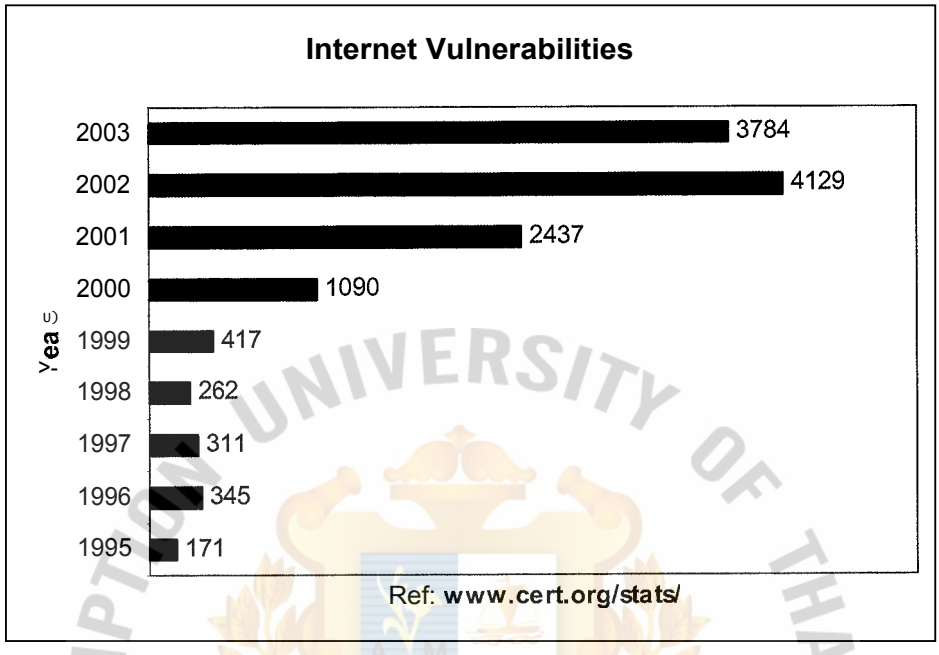


Figure 2-3 Internet Vulnerabilities

2.4 Why the Internet is vulnerable

Many early network protocols that now form part of the Internet infrastructure were designed without security in mind. Without a fundamentally secure infrastructure, network defense becomes more difficult. Furthermore, the Internet is an extremely dynamic environment, in terms of both topology and emerging technology.

Because of the inherent openness of the Internet and the original design of the protocols, Internet attacks in general are quick, easy, inexpensive, and may be hard to detect or trace. An attacker does not have to be physically present to carry out the attack. In fact, many attacks can be launched readily from anywhere in the world - and the location of the attacker can easily be hidden. Nor is it always necessary to

"break in" to a site (gain privileges on it) to compromise confidentiality, integrity, or availability of its information or service.

Even so, many sites place unwarranted trust in the Internet. It is common for sites to be unaware of the risks or unconcerned about the amount of trust they place in the Internet. They may not be aware of what can happen to their information and systems. They may believe that their site will not be a target or that precautions they have taken are sufficient. Because the technology is constantly changing and intruders are constantly developing new tools and techniques, solutions do not remain effective indefinitely.

Since much of the traffic on the Internet is not encrypted, confidentiality and integrity are difficult to achieve. This situation undermines not only applications (such as financial applications that are network-based) but also more fundamental mechanisms such as authentication and nonrepudiation. As a result, sites may be affected by a security compromise at another site over which they have no control. An example of this is a packet sniffer that is installed at one site but allows the intruder to gather information about other domains (possibly in other countries).

Another factor that contributes to the vulnerability of the Internet is the rapid growth and use of the network, accompanied by rapid deployment of network services involving complex applications. Often, these services are not designed, configured, or maintained securely. In the rush to get new products to market, developers do not adequately ensure that they do not repeat previous mistakes or introduce new vulnerabilities.

Compounding the problem, operating system security is rarely a purchase criterion. Commercial operating system vendors often report that sales are driven by customer

demand for performance, price, ease of use, maintenance, and support. As a result, off-the-shelf operating systems are shipped in an easy-to-use but insecure configuration that allows sites to use the system soon after installation. These hosts/sites are often not fully configured from a security perspective before connecting. This lack of secure configuration makes them vulnerable to attacks, which sometimes occur within minutes of connection.

Finally, the explosive growth of the Internet has expanded the need for well-trained and experienced people to engineer and manage the network in a secure manner. Because the need for network security experts far exceeds the supply, inexperienced people are called upon to secure systems, opening windows of opportunity for the intruder community.

2.5 Types of Technical Vulnerabilities

The following taxonomy is useful in understanding the technical causes behind successful intrusion techniques, and helps experts identify general solutions for addressing each type of problem.

2.5.1 Flaw in Software on Protocol Designs

Protocols define the rules and conventions for computers to communicate on a network. If a protocol has a fundamental design flaw, it is vulnerable to exploitation no matter how well it is implemented. An example of this is the Network File System (NFS), which allows systems to share files. This protocol does not include a provision for authentication; that is, there is no way of verifying that a person logging in really is whom he or she claims to be. NFS servers are targets for the intruder community.

When software is designed or specified, often security is left out of the initial description and is later "added on" to the system. Because the additional components

were not part of the original design, the software may not behave as planned and unexpected vulnerabilities may be present.

2.5.2 Weaknesses in how Protocols and Software are implemented

Even when a protocol is well designed, it can be vulnerable because of the way it is implemented. For example, a protocol for electronic mail may be implemented in a way that permits intruders to connect to the mail port of the victim's machine and fool the machine into performing a task not intended by the service. If intruders supply certain data for the "To:" field instead of a correct E-mail address, they may be able to fool the machine into sending them user and password information or granting them access to the victim's machine with privileges to read protected files or run programs on the system. This type of vulnerability enables intruders to attack the victim's machine from remote sites without access to an account on the victim's system. This type of attack often is just a first step, leading to the exploitation of flaws in system or application software.

Software may be vulnerable because of flaws that were not identified before the software was released. This type of vulnerability has a wide range of subclasses, which intruders often exploit using their own attack tools. For readers who are familiar with software design, the following examples of subclasses are included:

- race conditions in file access
- non-existent checking of data content and size
- non-existent checking for success or failure
- inability to adapt to resource exhaustion
- incomplete checking of operating environment
- inappropriate use of system calls
- re-use of software modules for purposes other than their intended ones

By exploiting program weaknesses, intruders at a remote site can gain access to a victim's system. Even if they have access to a nonprivileged user account on the victim's system, they can often gain additional, unauthorized privileges.

2.5.3 Weaknesses in System and Network Configurations

Vulnerabilities in the category of system and network configurations are not caused by problems inherent in protocols or software programs. Rather, the vulnerabilities are a result of the way these components are set up and used. Products may be delivered with default settings that intruders can exploit. System administrators and users may neglect to change the default settings, or they may simply set up their system to operate in a way that leaves the network vulnerable.

An example of a faulty configuration that has been exploited is anonymous File Transfer Protocol (FTP) service. Secure configuration guidelines for this service stress the need to ensure that the password file, archive tree, and ancillary software are separate from the rest of the operating system, and that the operating system cannot be reached from this staging area. When sites misconfigure their anonymous FTP archives, unauthorized users can get authentication information and use it to compromise the system.

2.6 How to Hack

2.6.1 Intruders' Technical Knowledge

Intruders are demonstrating increased understanding of network topology, operations, and protocols, resulting in the infrastructure attacks. Instead of simply exploiting well-known vulnerabilities, intruders examine source code to discover weaknesses in certain programs, such as those used for electronic mail. Much source code is easy to obtain from programmers who make their work freely available on the Internet.

Programs written for research purposes (with little thought for security) or written by naive programmers become widely used, with source code available to all. Moreover, the targets of many computer intrusions are organizations that maintain copies of proprietary source code (often the source code to computer operating systems or key software utilities). Once intruders gain access, they can examine this code to discover weaknesses.

Intruders keep up with new technology. For example, intruders now exploit vulnerabilities associated with the World Wide Web to gain unauthorized access to systems.

Other aspects of the new sophistication of intruders include the targeting of the network infrastructure (such as network routers and firewalls) and the ability to cloak their behavior. Intruders use Trojan horses to hide their activity from network administrators; for example, intruders alter authentication and logging programs so that they can log in without the activity showing up in the system logs. Intruders also encrypt output from their activity, such as the information captured by packet sniffers. Even if the victim finds the sniffer logs, it is difficult or impossible to determine what information was compromised.

2.6.2 Techniques to exploit vulnerabilities

As intruders become more sophisticated, they identify new and increasingly complex methods of attack. For example, intruders are developing sophisticated techniques to monitor the Internet for new connections. Newly connected systems are often not fully configured from a security perspective and are, therefore, vulnerable to attacks.

The most widely publicized of the newer types of intrusion is the use of the packet sniffers described in the section above on packet sniffers. Other tools are used to

construct packets with forged addresses; one use of these tools is to mount a denial-of-service attack in a way that obscures the source of the attack. Intruders also "spoof' computer addresses, masking their real identity and successfully making connections that would not otherwise be permitted. In this way, they exploit trust relationships between computers.

With their sophisticated technical knowledge and understanding of the network, intruders are increasingly exploiting network interconnections. They move through the Internet infrastructure, attacking areas on which many people and systems depend. Infrastructure attacks are even more threatening because legitimate network managers and administrators typically think about protecting systems and parts of the infrastructure rather than the infrastructure as a whole.

In the first quarter of 1996, 7.5% of 346 incidents handled by the CERT Coordination Center involved these new and sophisticated methods, including packet sniffers, spoofing, and infrastructure attacks. A full 20% involved the total compromise of systems, in which intruder gain system-level, or root, privileges. This represents a significant increase in such attacks over previous years' attacks, and the numbers are still rising. Of 341 incidents in the third quarter of 1996, nearly 9% involved sophisticated attacks, and root compromises accounted for 33%.

2.6.3 Intruders use of software tools

The tools available to launch an attack have become more effective, easier to use, and more accessible to people without an in-depth knowledge of computer systems. Often a sophisticated intruder embeds an attack procedure in a program and widely distributes it to the intruder community. Thus, people who have the desire but not the technical skill are able to break into systems. Indeed, there have been instances of

intruders breaking into a UNIX system using a relatively sophisticated attack and then attempting to run DOS commands (commands that apply to an entirely different operating system).

Tools are available to examine programs for vulnerabilities even in the absence of source code. Though these tools can help system administrators identify problems, they also help intruders find new ways to break into systems.

As in many areas of computing, the tools used by intruders have become more automated, allowing intruders to gather information about thousands of Internet hosts quickly and with minimum effort. These tools can scan entire networks from a remote location and identify individual hosts with specific weaknesses. Intruders may catalog the information for later exploitation, share or trade with other intruders, or attack immediately. The increased availability and usability of scanning tools means that even technically naive, would-be intruders can find new sites and particular vulnerabilities.

Some tools automate multiphase attacks in which several small components are combined to achieve a particular end. For example, intruders can use a tool to mount a denial-of-service attack on a machine and spoof that machine's address to subvert the intended victim's machine. A second example is using a packet sniffer to get router or firewall passwords, logging in to the firewall to disable filters, and then using a network file service to read data on an otherwise secure server.

The trend toward automation can be seen in the distribution of software packages containing a variety of tools to exploit vulnerabilities. These packages are often maintained by competent programmers and are distributed complete with version numbers and documentation.

A typical tool package might include the following:

- network scanner
- password cracking tool and large dictionaries
- packet sniffer
- variety of Trojan horse programs and libraries
- tools for selectively modifying system log files
- tools to conceal current activity
- tools for automatically modifying system configuration files
- tools for reporting bogus checksums

CHAPTER 3 IMPROVING SECURITY

In the face of the vulnerabilities and incident trends discussed above, a robust defense requires a flexible strategy that allows adaptation to the changing environment, well-defined policies and procedures, the use of robust tools, and constant vigilance.

It is helpful to begin a security improvement program by determining the current state of security at the site. Methods for making this determination in a reliable way are becoming available. Integral to a security program are documented policies and procedures, and technology that support their implementation.

3.1 Security Plan

3.1.1 Security Policy

A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology-specific issues.

A security policy covers the following (among other topics appropriate to the organization):

- high-level description of the technical environment of the site, the legal environment (governing laws), the authority of the policy, and the basic philosophy to be used when interpreting the policy
- risk analysis that identifies the site's assets, the threats that exist against those assets, and the costs of asset loss
- guidelines for system administrators on how to manage systems

- definition of acceptable use for users
- guidelines for reacting to a site compromise (e.g., how to deal with the media and law enforcement, and whether to trace the intruder or shutdown and rebuild the system)

Factors that contribute to the success of a security policy include management commitment, technological support for enforcing the policy, effective dissemination of the policy, and the security awareness of all users. Management assigns responsibility for security, provides training for security personnel, and allocates funds to security. Technological support for the security policy moves some responsibility for enforcement from individuals to technology. The result is an automatic and consistent enforcement of policies, such as those for access and authentication. Technical options that support policy include (but are not limited to)

- challenge/response systems for authentication
- auditing systems for accountability and event reconstruction
- encryption systems for the confidential storage and transmission of data
- network tools such as firewalls and proxy servers

There are many books and papers devoted to site security policies, including requests for comments RFC 1244 and RFC 1281, guidelines written by the Internet Engineering Task Force.

3.1.2 Security related procedures

Procedures are specific steps to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling, using encryption, authentication for issuing accounts, configuration, and monitoring.

3.1.3 Security practices

System administration practices play a key role in network security. Checklists and general advice on good security practices are readily available. Below are examples of commonly recommended practices:

- Ensure all accounts have a password and that the passwords are difficult to guess. A one-time password system is preferable.
- Use tools such as MD5 checksums, a strong cryptographic technique, to ensure the integrity of system software on a regular basis.
- Use secure programming techniques when writing software. These can be found at security-related sites on the World Wide Web.
- Be vigilant in network use and configuration, making changes as vulnerabilities become known.
- Regularly check with vendors for the latest available fixes and keep systems current with upgrades and patches.
- Regularly check on-line security archives, such as those maintained by incident response teams, for security alerts and technical advice.
- Audit systems and networks, and regularly check logs. Many sites that suffer computer security incidents report that insufficient audit data is collected, so detecting and tracing an intrusion is difficult.

3.2 Security Technology

A variety of technologies have been developed to help organizations secure their systems and information against intruders. These technologies help protect systems and information against attacks, detect unusual or suspicious activities, and respond to events that affect security. In this section, the focus is on two core areas: operational technology and cryptography. The purpose of operational technology is to maintain

and defend the availability of data resources in a secure manner. The purpose of cryptography is to secure the confidentiality, integrity, and authenticity of data resources.

3.2.1 Operational Technology

Intruders actively seek ways to access networks and hosts. Armed with knowledge about specific vulnerabilities, social engineering techniques, and tools to automate information gathering and systems infiltration, intruders can often gain entry into systems with disconcerting ease. System administrators face the dilemma of maximizing the availability of system services to valid users while minimizing the susceptibility of complex network infrastructures to attack. Unfortunately, services often depend on the same characteristics of systems and network protocols that make them susceptible to compromise by intruders. In response, technologies have evolved to reduce the impact of such threats. No single technology addresses all the problems. Nevertheless, organizations can significantly improve their resistance to attack by carefully preparing and strategically deploying personnel and operational technologies. Data resources and assets can be protected, suspicious activity can be detected and assessed, and appropriate responses can be made to security events as they occur.

3.2.1.1 One-Time Passwords

Intruders often install packet sniffers to capture passwords as they traverse networks during remote log-in processes. Therefore, all passwords should at least be encrypted as they traverse networks. A better solution is to use one-time passwords because there are times when a password is required to initiate a connection before confidentiality can be protected.

One common example occurs in remote dial-up connections. Remote users, such as those traveling on business, dial in to their organization's modem pool to access network and data resources. To identify and authenticate themselves to the dial-up server, they must enter a user ID and password. Because this initial exchange between the user and server may be monitored by intruders, it is essential that the passwords are not reusable. In other words, intruders should not be able to gain access by masquerading as a legitimate user using a password they have captured.

One-time password technologies address this problem. Remote users carry a device synchronized with software and hardware on the dial-up server. The device displays random passwords, each of which remains in effect for a limited time period (typically 60 seconds). These passwords are never repeated and are valid only for a specific user during the period that each is displayed. In addition, users are often limited to one successful use of any given password. One-time password technologies significantly reduce unauthorized entry at gateways requiring an initial password.

3.2.1.2 **Firewalls**

Intruders often attempt to gain access to networked systems by pretending to initiate connections from trusted hosts. They squash the emissions of the genuine host using a denial-of-service attack and then attempt to connect to a target system using the address of the genuine host. To counter these address-spoofing attacks and enforce limitations on authorized connections into the organization's network, it is necessary to filter all incoming and outgoing network traffic.

A firewall is a collection of hardware and software designed to examine a stream of network traffic and service requests. Its purpose is to eliminate from the stream those packets or requests that fail to meet the security criteria established by the

organization. A simple firewall may consist of a filtering router, configured to discard packets that arrive from unauthorized addresses or that represent attempts to connect to unauthorized service ports. More sophisticated implementations may include bastion hosts, on which proxy mechanisms operate on behalf of services. These mechanisms authenticate requests, verify their form and content, and relay approved service requests to the appropriate service hosts. Because firewalls are typically the first line of defense against intruders, their configuration must be carefully implemented and tested before connections are established between internal networks and the Internet.

3.2.1.3 Monitoring Tools

Continuous monitoring of network activity is required if a site is to maintain confidence in the security of its network and data resources. Network monitors may be installed at strategic locations to collect and examine information continuously that may indicate suspicious activity. It is possible to have automatic notifications alert system administrators when the monitor detects anomalous readings, such as a burst of activity that may indicate a denial-of-service attempt. Such notifications may use a variety of channels, including electronic mail and mobile paging. Sophisticated systems capable of reacting to questionable network activity may be implemented to disconnect and block suspect connections, limit or disable affected services, isolate affected systems, and collect evidence for subsequent analysis.

Tools to scan, monitor, and eradicate viruses can identify and destroy malicious programs that may have inadvertently been transmitted onto host systems. The damage potential of viruses ranges from mere annoyance (e.g., an unexpected "Happy Holidays" jingle without further effect) to the obliteration of critical data resources. To ensure continued protection, the virus identification data on which such tools

depend must be kept up to date. Most virus tool vendors provide subscription services or other distribution facilities to help customers keep up to date with the latest viral strains.

3.2.1.4 Security Analysis Tools

Because of the increasing sophistication of intruder methods and the vulnerabilities present in commonly used applications, it is essential to assess periodically network susceptibility to compromise. A variety of vulnerability identification tools are available, which have garnered both praise and criticism. System administrators find these tools useful in identifying weaknesses in their systems. Critics argue that such tools, especially those freely available to the Internet community, pose a threat if acquired and misused by intruders.

3.2.2 Cryptography

One of the primary reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. When you consider the millions of electronic messages that traverse the Internet each day, it is easy to see how a well-placed network sniffer might capture a wealth of information that users would not like to have disclosed to unintended readers. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of cryptography, to prevent intruders from being able to use the information that they capture.

Encryption is the process of translating information from its original form (called *plaintext*) into an encoded, incomprehensible form (called *ciphertext*). Decryption

refers to the process of taking ciphertext and translating it back into plaintext. Any type of data may be encrypted, including digitized images and sounds.

Cryptography secures information by protecting its confidentiality. Cryptography can also be used to protect information about the integrity and authenticity of data. For example, checksums are often used to verify the integrity of a block of information. A checksum, which is a number calculated from the contents of a file, can be used to determine if the contents are correct. An intruder, however, may be able to forge the checksum after modifying the block of information. Unless the checksum is protected, such modification might not be detected. Cryptographic checksums (also called message digests) help prevent undetected modification of information by encrypting the checksum in a way that makes the checksum unique.

The authenticity of data can be protected in a similar way. For example, to transmit information to a colleague by E-mail, the sender first encrypts the information to protect its confidentiality and then attaches an encrypted digital signature to the message. When the colleague receives the message, he or she checks the origin of the message by using a key to verify the sender's digital signature and decrypts the information using the corresponding decryption key. To protect against the chance of intruders modifying or forging the information in transit, digital signatures are formed by encrypting a combination of a checksum of the information and the author's unique private key. A side effect of such authentication is the concept of nonrepudiation. A person who places their cryptographic digital signature on an electronic document cannot later claim that they did not sign it, since in theory they are the only one who could have created the correct signature.

Current laws in several countries, including the United States, restrict cryptographic technology from export or import across national borders. In the era of the Internet, it

is particularly important to be aware of all applicable local and foreign regulations governing the use of cryptography.

CHAPTER 4 INTRODUCTION OF INTRUSION DETECTION

4.1 Why we need intrusion system

The Firewall is the security equivalent of a security fence around your property and the guard post at characters out, but cannot necessarily tell what is going on inside the compound. Intrusion detection systems are the equivalent of multi-sensor video monitoring and burglar alarm systems. They centralize this information, analyze it for patterns of suspicious behavior in much the same way a guard at a monitoring post watches the feeds from security cameras, and in some cases, deals with problems they detect. Most loss due to computer security incidents is still due to insider abuse. Intrusion detection systems, not firewalls, are capable of detecting this category of security violation. Perhaps more importantly, firewalls are subject to circumvention by a variety of well-known attacks.

Firewalls are subject to many attacks. The two considered most worrisome are tunneling attacks and application-based attacks.

Tunneling attacks arise due to a property of network protocols. Firewalls filter packets, and make pass/block decisions base on the network protocol. Rules typically check a database to determine whether a particular protocol is allowed, if so, the packet is allowed to pass. This represents a problem when an attacker masks traffic that should be screened by the firewall by encapsulating it within packets corresponding to another network protocol.

Application-Based attacks refer to the practice of exploiting vulnerabilities in applications by sending packets that communicate directly with those applications. Therefore, one could exploit a problem with Web software by sending an HTTP

command that exercises a buffer overflow in the web application. If the firewall is configured to pass HTTP traffic, the packet containing the attack will pass.

4.2 Intrusion Detection Research

Research is underway to improve the ability of networked systems and their managers to determine that they are, or have been, under attack. Intrusion detection is recognized as a problematic area of research that is still in its infancy. There are two major areas of research in intrusion detection: anomaly detection and pattern recognition

Research in anomaly detection is based on determining patterns of "normal" behavior for networks, hosts, and users and then detecting behavior that is significantly different (anomalous). Patterns of normal behavior are frequently determined through data collection over a period of time sufficient to obtain a good sample of the typical behavior is highly variable based on a wide variety of innocuous factors. Many of the activities of intruders are indistinguishable from the benign actions of an authorized user.

The second major area of intrusion detection research is pattern recognition. The goal here is to detect patterns of network, host, and user activity that match known intruder attack scenarios. One problem with this approach is the variability that is possible within a single overall attack strategy. A second problem is that new attacks, with new attack patterns, cannot be detected by this approach.

Finally, to support the needs of the future internet, intrusion detection tools and techniques that can identify coordinated distributed attacks are critically needed, as are better protocols to support traceability.

4.3 The Basic Concept in Intrusion Detection

The basic intrusion detection concept can be depicted with relative ease. Such straightforward depiction may be misleading however, as we will show throughout this document, because the practical implementation of this basic concept is anything but simple. We've found in our lecturing that the topic of intrusion detection can be introduced by the following Figure 4-1

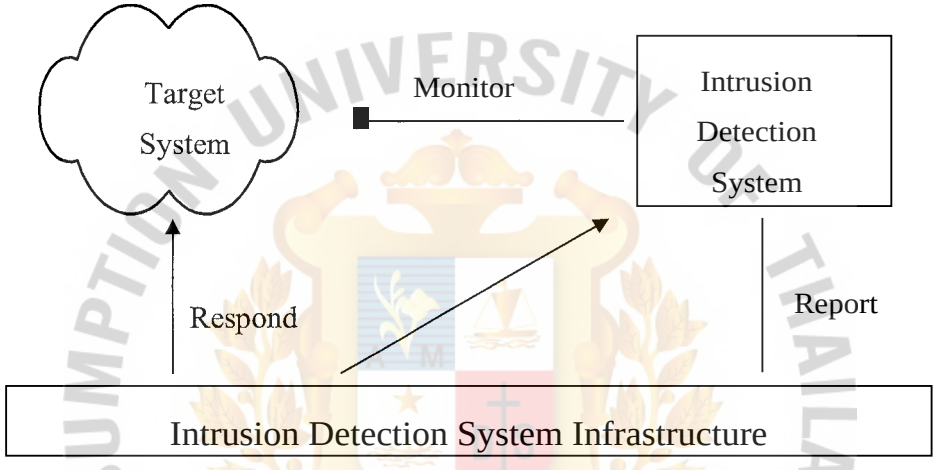


Figure 4-1 Simple Depiction of Intrusion Detection Concept

The diagram in Figure 4-1 introduces three critical functions in the basic intrusion detection concept

4.3.1 Monitor

Intrusion Detection systems examine and process information about target system activity. Many technical and operational issues arise in this monitoring function including timeliness of detection, confidence in information obtained, and processing power required to keep up with monitored activity. The degree to which these factors are properly handled will determine how successfully the intrusion detection system can detect actual intrusions.

4.3.2 Report

Intrusion detection systems report information about monitored systems into a system security and protection infrastructure. This infrastructure can be embedded in the intrusion monitoring component or can be done separately. In either case, the manner in which derived information about an intrusion is processed, stored, protected, shared, and used as the basic for risk mitigation is the most challenging aspect of practical intrusion detection.

4.3.3 Response

The purpose of intrusion detection —ultimately- is to reduce security risk. When risk-related information is made available by the intrusion detection system, an associated response function initiates mitigation activities. Response actions introduce a myriad of factors related to the timeliness and appropriateness of the activities initiated by the intrusion detection system to deal with an incident. Response is an extremely challenging process that requires attention to many technical and non-technical issues.

It's worth mentioning that the simplistic drawing in figure 4-1 often suggests a rather mundane function for intrusion detection systems. Intrusion detection is one of those rare topics that become more fascinating as one considers the topic in more detail. This may explain the growing emphasis on this technology in research and engineering circles.

Furthermore, the depth of interest in intrusion detection is equally rich in the areas of monitoring, reporting, and response.

4.4 Methods are used by Intrusion Detection Systems

Obviously, different intrusion detection systems will employ different methods. This is true in currently available and should continue in the future. We believe that as intrusion detection becomes a more attractive product option, particularly for major workstation, server, switch, firewall, and router vendors, differentiation of methods will be an important selling and marketing point. This is already happening. Just scan some of the marketing and advertising literature available for intrusion detection products. You will find their on-the-fly processing capability. Different intrusion detection methods are also prevalent in the various research intrusion detection systems that are being reported in the security conferences. Some focus on graph-oriented processing techniques, others focus on statistical correlation, and so on.

In spite of this difference in various products and systems, we can identify a collection of common methods that are generally present on a given intrusion detection system. These methods are neither mutually exclusive nor mutually dependent. Instead they comprise a collection of security protection strategies that are available to the intrusion detection system designer for use in a given product.

4.4.1 Audit Trail Processing

The method of processing an audit trail may be the most commonly used intrusion detection technique. This was certainly the first application of intrusion detection that emerged in the community and it is likely to remain important in the future. Figure 4-2 depicts a high-level view of the audit trail processing method of intrusion detection.

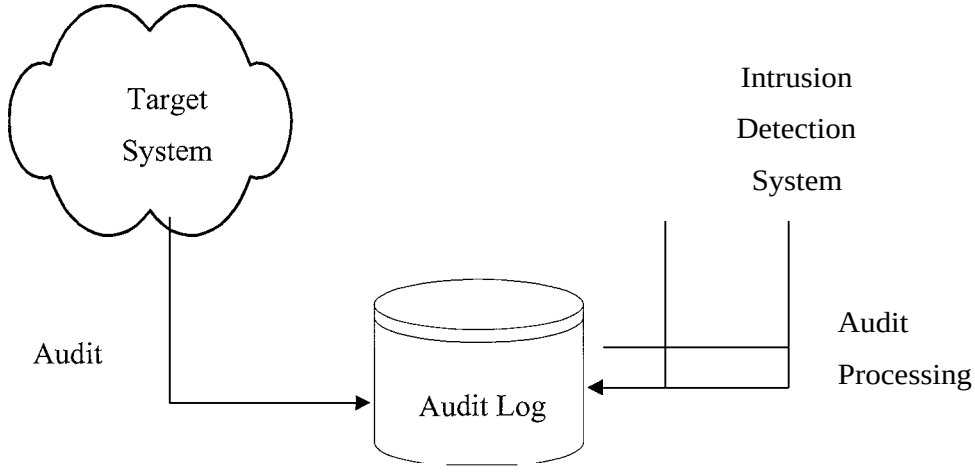


Figure 4-2 High-Level Depiction of Audit Trail Processing Method

The idea in audit trail processing is that an existing log in available for parsing and interpretation by an intrusion detection system. This method is typically performed off-line and rarely involves any real-time analysis. Such processing introduces issues of audit trail formats, storage techniques, archival policies, and real time auditing standards. It also raises issues in an intrusion-processing center of the manual processes required by human beings involved in the audit trail processing, particularly for archived data. Unfortunately, the security community has been negligent in the area of developing standard formats and techniques for audit trails.

Note that in current Internet and Intranet environments, audit trail information is readily available from operating system (e.g. UNIX syslog), network systems, routers, firewalls, switches, applications, and other components. As a result, in many environments, the desire to perform intrusion detection via audit trail analysis is great because the data is already being collected. It's worth noting, however, that very few environments exist where audit data is properly collected, stored, and protected. The enormous volume of audit data generated in a typical environment doesn't help matters.

4.4.2 On-The-Fly Processing

This method, sometime called network intrusion detection, involves the monitoring the traffic so that real-time or near real-time analysis can be done with respect to appropriate detection algorithms Specified strings of characters are often used in this method as a means for parsing traffic for so-called "dirty words". These dirty words might include '/etc/passwd', '/etc/shadow', of other sequences one might consider suspicious to be passing through an intrusion detection system.

The on-the-fly method complements audit trail processing in the most effective intrusion detection environments. Both techniques have the capability to detect a given intrusion, but the method of detection will differ in each case as will the information used for processing. Figure 4-3 depicts a high-level view of the on-the-fly processing method.

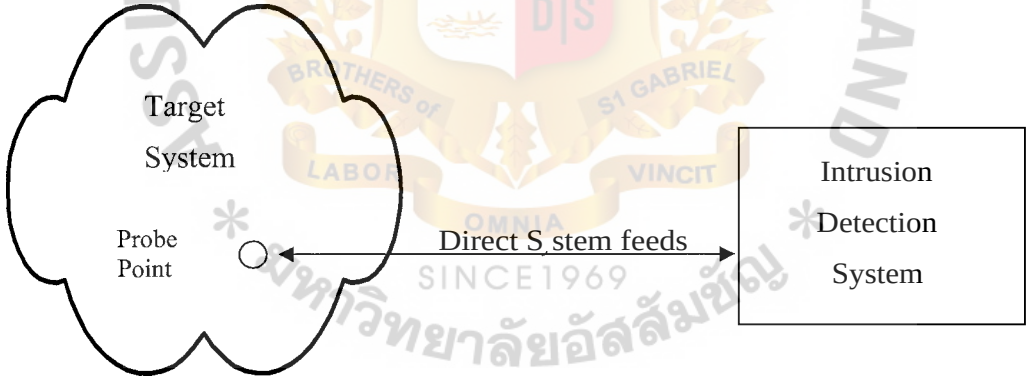


Figure 4-3 High-Level Depiction of On-the-fly Processing Method

One point worth highlighting with respect to the on-the-fly method is that it requires access to network traffic. Packets that pass through the target of the intrusion detection system are typically sniffed and passed to the on-the-fly system for real-time analysis. As more Intranet environments are designed around gateway choke points

with routers and firewalls, this often provides the type of network access required. One should expect on-the-fly intrusion detection systems, router processing, and firewall processing methods to be integrated more closely by vendors for this reason. The recent acquisition of the WheelGroup by Cisco Systems would certainly suggest that this might be true for at least one major vendor.

4.4.3 Profile of Normal Behavior

Profiles of normal behavior are used in intrusion detection to capture expectations about user and system computing and networking activity. This follows the basic paradigm of comparing expectations about behavior with actual observations. The creation of such profiles involves at least the following three basic concerns - it involves much more, but these are the big ones.

- **Estimation of Initial Profiles.** Initial profiling for new users and systems requires estimation of expected behavior. Such estimation is nontrivial and makes profiling vulnerable to malicious teaching approaches by intruders (i.e., by altering initial behavior to set-up an intrusion profile to support a subsequent attack). One way to deal with such initial profiling problems is to maintain a stealth intrusion detection system so that new users are not aware that their behavior is being profiled. This raises all sorts of legal, ethical, and organizational policy issues that may make such a method unacceptable. This initial state problem may become less serious as more empirical evidence emerges for a given monitored environment.
- **Fine-Tuning of Profiles.** Observed user and system behavior provides basis for fine-tuning existing profiles. Proper fine-tuning is also nontrivial, as it requires attention to statistical concerns about probability of occurrences and regularity of events. In the best case, fine-tuning would be automated, but

manual techniques must be developed for this before such automation can be considered trusted. This fine-tuning is also vulnerable to malicious teaching approaches by profiled users or systems.

- **Profiling Using All-Source Information.** Information should be used from any relevant source to more accurately predict expected behavior. These sources do not have to be based on computing or networking information. In fact, some of the most powerful profiling information is derived from sources that are out of band with respect to any computer or network (e.g., personal characteristics and habits).

These intrusion detection system profiling concerns are depicted in the diagram in Figure 4-4

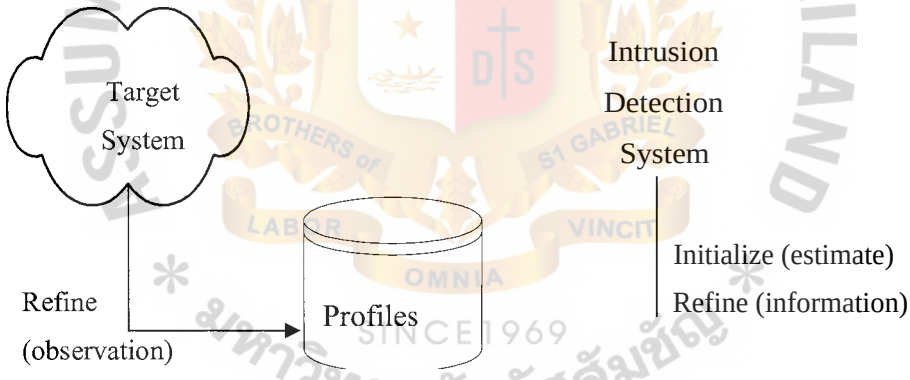


Figure 4-4 Intrusion Detection Profiling Method

The profiling approach is one of the most mature intrusion detection methods available, primarily because it is used extensively in telephony-based service provision environments. A technique for toll fraud mitigation by service providers is an example of a stable application of this method that has been used successfully to mitigate security risk.

4.4.4 Signatures of Abnormal Behavior

The use of abnormal behavioral signatures, also called attack signatures in some security books and research articles, is particularly common in on-the-fly intrusion detection systems. These abnormal behavior signatures generally come in one of two different flavors:

- **Known Attack Descriptions.** Dynamic Descriptions of related activity patterns that might constitute a security problem. These descriptions of known attacks are often referred to at attack signatures. Databases of these descriptions are reminiscent of virus databases in virus detection software.
- **Suspicious String Patterns.** Designated character string (like '/etc/shadow', `top secret', or ' proprietary') that correspond to traffic content that must be considered suspicious. These are often determined locally by security administrators.

The use of abnormal behavior signatures for intrusion detection is depicted in Figure 4-5

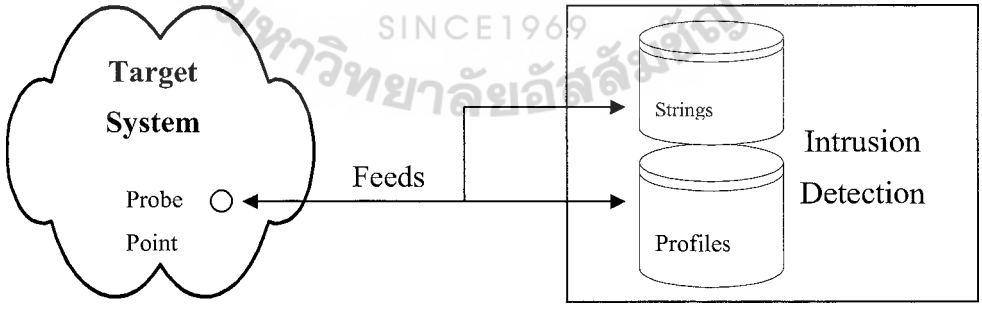


Figure 4-5 Abnormal Behavior Signature Method

The greatest challenge in abnormal behavior signatures is that the intrusion detection system must have advance knowledge of the attack to be detected. As any Internet security expert will attest, new attack methods are invented every day, and intrusion detection systems relying solely on this method will always, by definition, be slightly out of date. Users of virus detection software should be familiar with this basic problem. Very few of us have the patience and resolve to ensure that our virus checking software is always up-to-date with the latest viruses. Abnormal behavior signature checking methods will be vulnerable to this as well.

4.4.5 Parameter Pattern Matching

This method involves the use of day-to-day operational experience as the basis for detecting anomalies. From a logical perspective, this method can be viewed as a special case of the normal profiling method. It is separated out here because the explicit development of user and system security profiles may not be included in the approach. Instead, operators doing normal system and network management activity might, or might not, detect some sort of change in the parameters they typically monitor – hence our use of the pattern matching term for this method. Actually, one of the more attractive characteristics of this method is that the administrators are not specifically targeting security issues. This introduces a more robust environment in which anomalies and patterns might be detected and matched.

Such pattern matching constitutes an especially powerful processing approach because it provides an intrusion detection capability for attacks that might not be predictable. In fact, human operators in a network operations center might detect subtle changes as part of their normal security and network management operations that they can neither explain nor understand. It is these types of unpredictable change,

however, that could lead to detection of a problem. A high-level view of the method is depicted in Figure 4-6

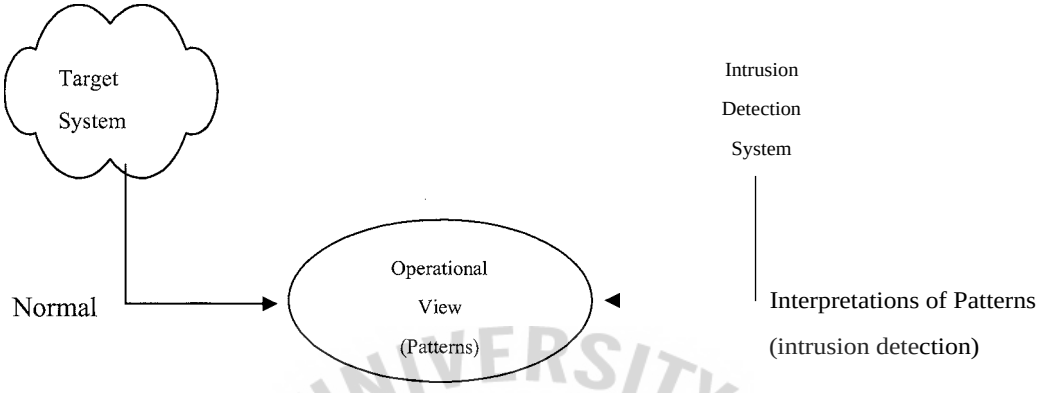


Figure 4-6 Pattern Matching Method of Intrusion Detection

4.5 Detection and Prevention

On the surface, intrusion detection and intrusion prevention solutions appear competitive. After all, they share a long list of similar functions, like packet inspection, Stateful analysis, fragment reassembly, TCP segment reassembly, deep packet inspection, protocol validation, and signature matching. But these capabilities take a backseat to the starkly different purposes for which they are deployed. An IPS operates like a security guard at the gate of a private community, allowing and denying access based on credentials and some predefined ruleset, or policy. An IDs works like a patrol car within the community, monitoring activities and looking for abnormal situations. No matter how strong the security at the gate is, the patrols continue to operate in a system that provides its own checks and balances.

4.6 Intrusion Detection Product

The purpose of intrusion detection is to provide monitoring, auditing, forensics, and reporting of network activity. It operates on the packets that are allowed through an

access control device. Because of reliability constraints, internal threats, and healthy does of skepticism, intrusion prevention must allow some "gray area" attacks through to protect against false positives. IDS solutions, on the other hand, are loaded with intelligence, using many different techniques to identify potential attacks, intrusions, exploits, and abuses. IDS have the luxury of being out-of-band and can therefore perform its operations without affecting the computing & networking architectures.

The passive nature of IDS is what provides the strength to conduct intelligent analysis of the packet stream. That positions IDS well to identify:

- Known attacks via signatures and rules.
- Variations in traffic volume and direction using complex rules and statistical analysis.
- Communication traffic pattern variations using flow analysis
- Anomalistic activity detection using baseline deviation analysis
- Suspicious activity detection using heuristics, flow analysis, statistical techniques, and anomaly detection

Some attacks are just plain hard to detect with any degree of certainty, and most can only be detected by methods that are non-deterministic in nature. That is, they are not suitable for a policy-driven blocking decision

4.7 Intrusion Prevention Product

Intrusion prevention solutions are intended to provide protection for assets, resources, data and networks. The primary expectation is that they will reduce the threat of attack by eliminating the harmful and / or malicious network traffic while continuing to allow legitimate activity to continue. The goal is a perfect system – no false positives that reduce end user productivity and no false negatives that create undue

risk within the environment. Perhaps a more crucial role is the need to be reliable; to perform in the expected manner under any conditions. In order to accomplish this goal, IPS solutions must be deterministic in nature.

Deterministic capabilities imbue the confidence required for a "hard" decision. This means that intrusion prevention solutions are ideally positioned to deal with :

- Undesired applications and active Trojan horse attacks against private networks and applications, by using deterministic rules and access control lists.
- Attack packets like those from LAND and WinNuke by using high-speed packet filters.
- Protocol abuse and evasive actions – network protocol manipulations like Fragroute and TCP overlap exploits – by using intelligent reassembly
- Denial of service(DOS/DDOS) attacks such as SYN and ICMP floods by using threshold-based filtering algorithms
- Application abuse and protocol manipulations – known and unknown attacks against HTTP, FTP, DNS, SMTP etc. – by using application protocol rules and signatures
- Application overload or abuse attacks by using threshold-based resource consumption limits

All of these attacks and the vulnerable state that allows them to happen are well-documented. In addition, the aberrations in communications protocols from network through application layer have no place in any sort of legitimate traffic, making the faults self-selective in a deterministic context.

4.8 False and Noise

Fundamentally, all IDS embody a trade-off between being too sensitive and annoying their users and being too narrow-focused and missing an important event. Figure 4-7 illustrates the estimated trade-off based on the author's practical experience. Note that the rate at which false positives are generated drops off fairly sharply as the signature set adds state or error checking and becomes more precise. The rate of false negatives is not believed to be symmetrical but is actually unknown since the number of unknown attacks is an unknown. However, a signature that does protocol correctness checking to any significant degree dramatically increases the likelihood of catching a large number of unknown attacks -- while a single correction to a signature may only remove a single false positive.

Figure 4-7 Relationship of signature quality to IDS responsiveness

When an IDS designer produces a signature set and detection logic in a product, it embodies their assessment of how their end-users adjudge the relative value of false positives, noise, and false negatives. In today's IDS product market, the designers' ability to judge these values has been somewhat hampered by the way in which customers and trade journal reviewers have been performing IDS tests.

The typical IDS test consists of running a baseline traffic mix and injecting attacks into it. The IDS is then scored based on how many attacks it saw; attacks missed are psychologically weighted more heavily in readers minds because, after all, if the IDS can't detect a known attack, it can't be very accurate, can it?

So goes the logic, anyhow. The end result is that most vendors will prefer to produce a few more false positives than risk a poor showing in a product review. The noise level an IDS produces has less to do with the quality of its signature set and more to do with the environment in which it is deployed and its ability to capture site-specific knowledge.

4.8.1 False Positives

An alarm generated by an IDS in which the IDS alerts to a condition that is actually benign. In other works, the IDS made a mistake. A typical example of a false positive would be a case when an IDS raises a “SYN Flood" alarm because it sees a large number of SYN packets directed at a busy web server and mistakenly concludes it is under attack. Another example of a false positive would be an IDS raising a “SMTP Wiz attack" alarm when it observes the string "DEBUG" in the body of an SMTP message.

4.8.2 False Negatives

A non-event in which an IDS fails to generate an alarm when an alert-worthy condition is in effect. A typical example of a false negative might be an IDS' failure to capture all the packets necessary to accurately reassemble an attacker's action due either to network load or changes in routing topology.

4.8.3 Noise

An alarm in which the IDS sends an alert on a condition that is non-threatening or not applicable to the site that is being monitored, but which is correctly diagnosed. The IDS did not make a mistake but the alarm is of questionable value. For example, the IDS might identify a Windows/Intel-based buffer overrun against a Solaris/SPARC system that will not be affected by the attack. Anothre example of noise might be an alarm in which an IDS outside a firewall correctly identifies hostile scanning activity that the site administrator knows will not penetrate past the firewall. In the first example, the IDS correctly identified an event of possible interest – site administrators will most likely react with varying levels of concern depending on the origin, persistence, or target of the attack. In the second example, since the IDS is out side the firewall, a certain amount of hostile traffic is expected, even if it is ignored or deemed insignificant. Some sites employ IDS specifically to collect statistics regarding attacks lunched against their outer perimeter —the "noise level".

4.9 Product Approach

4.9.1 Host -Based Approach

Host-based Intrusion Detection agents collect information reflecting the activity that occurs a particular system. This information is some times in the form of operating system audit trails. It can also include system logs, other logs generated by operating system processes, and contents of system objects not reflected in the standard operating system audit and logging mechanisms.

Advantages:

- Systems can monitor information access in terms of "who accessed what"
- Systems can map problem activities to a specific user id

- Systems can track behavior changes associated with misuse
- Systems can operate in switched network environments
- Systems can distribute the load associated with monitoring across available hosts on large networks, thereby cutting deployment costs

Disadvantages:

- Network activity is not visible to host-based detectors
- Running audit mechanisms can incur additional resource overhead
- When audit trails are used as data sources, they can take up significant storage
- Operating system vulnerability can undermine the integrity of host-based agents and analyzers
- Host-based agents must be more platform-specific, which adds to deployment costs
- Management and deployment costs associated with host-based systems are usually greater than in other approaches

4.9.2 Network -Based Approach

Network-based intrusion detection sensors collect information from the network itself. This information is usually gathered by packet sniffing, using network interfaces set in promiscuous mode; however, some agents are integrated in network hardware devices.

Advantages:

- The data come without any special requirement for auditing or logging mechanisms; in most case collection of network data occurs with the configuration of a network interface card.
- The insertion of a network-level agent does not affect existing data sources.

- Network-level agents can monitor and detect network attacks.(e.g., SYN flood and packet storm attacks).

Disadvantages:

- Although some network-based systems can infer from network traffic what is happening on hosts, they cannot tell the outcome of commands executed on the host. This is an issue in detection, when distinguishing between user error and malfeasance.
- Network-based agents cannot scan protocols or content if network traffic is encrypted.
- Network-based monitoring and intrusion detection becomes more difficult on modern switched network. Switched networks establish a network segment for each host; therefore, monitoring a single host. Network switches that support a monitoring or scanning port can at least partially mitigate this issue.
- Current network-based monitoring approaches cannot handle high-speed networks.

CHAPTER 5 IDS/IPS MARKET

5.1. Market Trends and Forecasts

The total World managed security services market was worth $497.1 Million in 2002, and is expected to grow at a CAGR (Compound Annual Growth Rate) of 24.1 percent through 2009. The value proposition of the MSSP (Managed Security Service Providers) remains strong, and is aimed at a market in which clients are growing increasing weary of accepting the burden of securing their own networks. This market has felt the prejudice of being the newcomer without experience and proven competencies, but the solid growth rates represent a shifting mindset toward higher acceptance levels as the market matures and dispels the attitudes against outsourced security.

Year	Revenues ($ Million)	Revenue Growth Rate (%)
1999	95.8	-
2000	226.4	136.3
2001	348.2	53.8
2002	497.1	42.7
2003	687.3	38.3
2004	909.2	32.3
2005	1,157.5	27.3
2006	1,431.6	23.7
2007	1,716.5	19.9
2008	1,987.9	15.8
2009	2,254.0	13.4

Compound Annual Growth Rate(2002-2009): 24.1%
Note : All figures are rounded the base year is 2002.
Source:Frost & Sullivan

Figure 5-1 Total MSSP Market: Revenue Forecasts(World), 1999-2009

Major market growth will come from the undeniable value proposition of offering more for less in economies that are facing tightened budgets. The severe damage that continues to occur from insecure networks is multiplied by the increased amount of

information and systems that are managed electronically to yield a massive market with decreasing faith in their own ability to secure their own networks.

The world market's revenue growth is also attributable to the recurring revenue model of the services industry. The high customer satisfaction rates have led to high retention rates industry wide. This model gives MSSPs the freedom to grow organically without winning all of their business again each year.

Moreover, with high customer satisfaction and retention, MSSPs can increase revenues from existing customers annually by positioning themselves as a solutions partner instead of a services provider. These tighter relationships facilitate growth from within MSSPs' existing customer base as their service capabilities and the number of devices monitored increases.

5.2 Asia Pacific MSSP Markets

Vendors have noted some difficulty in penetrating Asia Pacific markets with managed security services. These markets are younger with a less robust economy, and therefore most businesses cannot afford the prices charged by MSSPs. Also cultural and geographic disparateness adds difficulty to reaching this market. The MSSPs that are addressing this market are doing so largely through partners who provide a much easier entry into the region, although regional acquisitions that further the same goals are not uncommon. The Asia Pacific MSSP market generated just over $21 Million worth of security services in 2002 as noted in Figure 5-2

Year	Revenues ($ Million)	Revenue Growth Rate (%)
1999	-	
2000	1.7	-
2001	9.7	470.0
2002	21.1	116.5
2003	38.4	81.9
2004	62.7	63.3
2005	88.4	41.1
2006	119.9	35.6
2007	157.2	31.1
2008	198.7	26.4
2009	239.8	20.7

Compound Annual Growth Rate(2002-2009): 41.5%
Note : All figures are rounded the base year is 2002.
Source:Frost & Sullivan

Figure 5-2 Total MSSP Market: Revenue Forecasts (Asia Pacific), 1999-2099

The difficulties mentioned above, coupled with the relatively limited installed base of enterprise networks limits the relative representation of the Asia Pacific market to less than 10 percent of the world market until the last year of the forecast period. However, the growth rates associated with this market are considerable because the market is growing from a smaller base, yielding a 41.5 percent CAGR for the region through 2009.

5.3 IDS/IPS Market Growth

The early stages of the MSSP market offered a more limited service portfolio than today's market. MSSPs are continuing to add services that they can scale into their operations profitably. The growth of service offerings is a natural evolution of the market, but will not occur quickly or haphazardly, because integrating new technologies into service offerings requires infrastructure buildout, training in new technologies, and correlation of the results with the information received from more

traditional firewall, VPN and IDS offerings. New technologies must have scalable management platforms to even be considered in an MSSP environment.

As noted in Figure, the MSSP market in 2000 was heavily focused on firewall and VPN, since these technologies comprised the majority of the potential market's security interest.

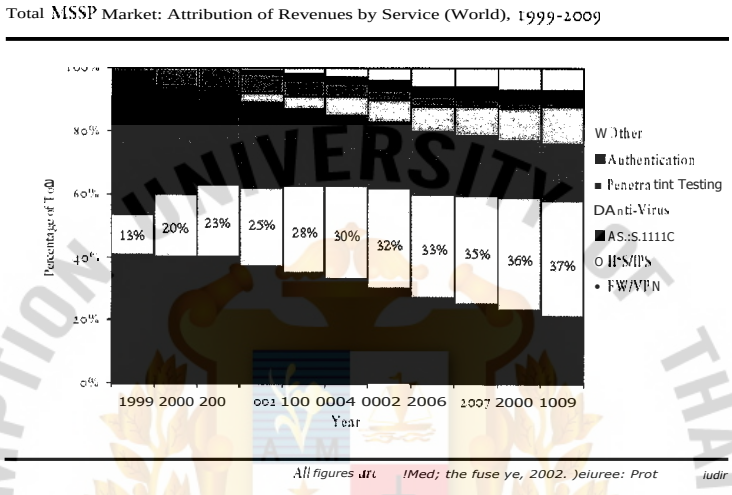


Figure 5-3 Total MSSP Market: Attribution of Revenues by Service(World),1999-2009

Managed firewall was the primary service offered as vendors initiated their operations. Even then, the market's demand was pushing MSSPs towards intrusion detection monitoring and management.

The nature of IDS technology commands constant attention in order to be utilized effectively. Here, monitoring services are critical in addition to the management of the device. As the market matured, customers demanded IDS monitoring, and have been accommodated by the vast majority of the market that now offers firewall, VPN, and IDS monitoring and management as a standard practice.

In the last 18 months, a renewed attention has been given to the IDS technology. Start ups have taken aim at the lack of development in IDS technology by bringing new host-based technologies, new attack recognition technologies, and intrusion prevention technologies to the marketplace. The entrance of these companies to the market has consequently refuelled demand for IDS/IPS technology, causing vendors to expand their services even farther.

For many providers, IDS/IPS difficulties have been the underlying catalyst that stimulates the idea of outsourcing. Increasingly, a customer's interest in outsourcing is piqued by the troubles with IDS, then is upsold other services as an add on. This trend coupled with the augmented amount of attention that IDS/IPS services require lends to the amplified representation of IDS/IPS services later in the forecast period.

CHAPTER 6 IDS/IPS PRODUCT IN THAILAND

6.1 Cisco IDS 4200 Products

6.1.1 Product Description

The Cisco IDS 4200 Series Sensors are used in the Cisco Intrusion Protection System. These intrusion detection system sensors work in concert with the other components to efficiently protect your data and information infrastructure. With the increased complexity of security threats, achieving efficient network intrusion security solutions is critical to maintaining a high level of protection. Vigilant protection ensures business continuity and minimizes the effect of costly intrusions.

Additionally, Cisco's flexible deployment options allow businesses to businesses to minimize the total cost of ownership of their IDS deployments by delivering :

- Unprecedented price/performance ratios
- The ability to simultaneously protect multiple network subnets through the support for multiple sniffing interfaces, thereby delivering up to five sensors in one
- A wide array of performance options
- Investment protection by delivering modular, upgradeable components
- Support for multi-VLAN traffic
- Embedded web-based management solutions packaged with the IDS sensors

6.1.2 About Cisco System Inc.

Cisco Systems, Inc. is the worldwide leader in networking for the Internet. Today, networks are an essential part of business, education, government and home

communications, and Cisco Internet Protocol-based (IP) networking solutions are the foundation of these networks. Cisco hardware, software, and service offerings are used to create Internet solutions that allow individuals, companies, and countries to increase productivity, improve customer satisfaction and strengthen competitive advantage. The Cisco name has become synonymous with the Internet, as well as with the productivity improvements that Internet business solution provide. At Cisco, our vision is to change the way people work, live, and learn.

Cisco was founded in 1984 by a small group of computer scientists from Standard University. Since the company's inception, Cisco engineers have been leaders in the development of Internet Protocol (IP)-based networking technologies. This tradition of IP innovation continues with industry-leading products in the core areas of routing and switching, as well as advanced technologies in areas such as:

- Home Networking
- IP Telephony
- Optical
- Network Security
- Storage Networking
- Wireless LAN

6.2 **Proventia** Product

6.2.1 Product Description

Internet Security Systems' Proventia products provide unprecedented network protection and cost efficiencies by performing the functions of multiple security technologies from a single protection engine. Proventia is available as network

appliances or software agents, spanning gateway, network, server, desktop and application levels to protect organizations from the gateway to the core.

Proventia identifies and blocks network attacks, intrusions, viruses and malicious code, and filters unwanted traffic and spam without user intervention, thus eliminating the need for stand-alone security products. Organizations can tailor Proventia to suit specific security needs, choosing from firewall, virtual private network (VPN), antivirus, intrusion detection and prevention, application protection, content filtering and anti-span protection functions.

6.2.2 About Internet Security System Inc.

Internet Security System, Inc. (ISS) is the trusted expert to global enterprises and world governments, providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise for more than 11,000 customers' world wide. ISS products and services are based on the proactive security intelligence conducted by ISS' X-Force research and development team – the unequivocal world authority in vulnerability and threat research. Headquartered in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East.

6.3 **Interspect** Product

6.3.1 Product Description

Check Point InterSpect is an internal security gateway that blocks the spread of worms and attacks inside the network and provides network zone segmentation. Based on Check Points proven security technologies : INSPECT, Stateful Inspection

and Application Intelligence , and SMART (Security Management Architecture), InterSpect is built specifically for internal network security. InterSpect provides :

- **Intelligent Worm Defender;** Blocks the spread of worms and attacks inside the network
- **Network Zone Segmentation;** Segments the internal network into organizational security zones
- **Quarantine of Suspicious Computers;** Isolates attacks and compromised devices
- **LAN Protocol Protection;** Provides the deepest and most comprehensive support for Microsoft and other LAN protocols
- **Pre-emptive Attack Protection;** Provides proactive defenses against vulnerabilities and attacks before they are exploited

6.3.2 About Check Point Software Technologies Inc.

Check Point Software Technologies is the worldwide leader in securing the Internet. It is the confirmed market leader of both the worldwide VPN and firewall markets. Through its Next Generation product line, the company delivers a broad range of Perimeter, Internal and Web security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from over 350 leading companies, Check Point solutions are sold, integrated and serviced by a network of over 2,300 Check Point partners in 92 countries.

6.4 **Netscreen IDP** Product

6.4.1 Product Description

The Juniper Networks NetScreen Intrusion Detection and Prevention (NetScreen-IDP) integrates application and network visibility with incident investigation and remediation to help customers quickly and confidently deploy inline attack prevention. When deployed inline, NetScreen-IDP effectively identifies and stops network and application level attacks before they inflict any damages, minimizing the time and costs associated with intrusions. NetScreen-IDP not only helps protect your network against attacks, it provides you with information on rogue servers and applications that may have been added to the network without your knowledge. Armed with the knowledge that unauthorized applications such as peer-to-peer or instant messaging have been added to the network allows you to more easily enforce your security policy and maintain compliance with your corporate application use policy. Combined with a centralized, rule-based management approach, which offers granular control over the system's behavior and easy access to extensive logging and fully customizable reporting, it is easy to see why NetScreen-IDP is the best way to keep your critical information assets safe.

6.4.2 About Juniper

Juniper Networks transforms the business of networking. A leading global provider of networking and security solutions, Juniper Networks maintains an intense focus on customers who derive strategic value from their networks. Its customers include major network operators, enterprises, government agencies, and research and educational institutions globally. Juniper Networks delivers a portfolio of networking solutions that support the complex scale, security and performance of the world's most

demanding mission-critical networks, including the world's top 25 service providers and 8 of the top 15 Fortune 500 companies.

Juniper Networks was founded with a single mission - to anticipate and solve the industry's most difficult networking and security problems. Today, Juniper Networks is enabling customers worldwide to create competitive advantage by transforming the business of networking through:

- Securing networks against increasingly frequent and sophisticated attacks
- Leveraging networked applications and services that provide a competitive market advantage
- Providing secure and tailored access to remote resources for customers and business partners

Juniper Networks brings a new pace of innovation to the industry through purpose-built platforms and sophisticated software. It is recognized as a center of excellence in the development of silicon and software that support high- performance, intelligent networks, and remains at the forefront of industry initiatives that drive the continuing transformation of these networks and the businesses they support.

6.5 Snort 2.0

6.5.1 Product Description

Snort is a freeware Network Intrusion Detection System which was written for Unix/Linux systems and later ported to the Windows platform.

Snort is described as a cross-platform, lightweight network intrusion detection tool that can be deployed to monitor small TCP/IP networks and detect a wide variety of suspicious network traffic as well as outright attacks. There is nothing lightweight

about its flexibility and performance, however. It has a wealth of development effort behind it, in terms of both source code and attack signature production, and more often than not has the very latest attack signatures available for it before they are available for commercial IDS products.

Snort is available under the GNU General Public License, and is free for use in any environment, making the deployment of Snort as a network security system more of a network management and coordination issue than one of affordability.

6.5.2 About **Sourcefile**

Sourcefire is the world leader in real-time network defense solutions, transforming the way organizations manage and minimize network security risks. Sourcefire's ground-breaking 3D approach – Discover, Determine, Defend – is a comprehensive intelligent network defense system that unifies intrusion and vulnerability management technologies to provide customers with the most effective, real-time network security available for today's real world challenges. Sourcefire's products allow security practitioners and managers to better leverage essential security data, while reducing security costs and increasing overall effectiveness.

Sourcefire also helps drive compliance for recently legislated compliance laws including Sarbanes-Oxley, HIPAA, OCC Regulations, FISMA and FERCs Compliance, Gramm-Leach-Bliley and CA 1386.

Sourcefire was founded in 2001 by the creator of the popular Snort® open source Intrusion Detection technology, Martin Roesch. Today, with more than 2 million downloads, Snort is the single most widely deployed Intrusion Detection technology in the world.

CHAPTER 7 100MBPS IDS GROUP TEST REPORT BY NSS

7.1 About NSS

The NSS Group is the world's foremost independent security testing facility.

With security and network infrastructure testing facilities in the South of France, The NSS Group offers a range of specialist IT, networking and security-related services to vendors and end-user organizations world-wide.

The NSS Group security testing laboratories are available to vendors and end-users for fully independent testing of networking, communications and security hardware and software.

The NSS Group also operates certification schemes for vendors and certification bodies, and currently provides evaluation and certification of a wide range of security products, including IDS/IPS appliances, firewalls, VPN's, cryptographic devices and PKI products.

Output from the labs, including detailed research reports, articles and white papers on the latest network and security technologies, are made available on this site.

7.2 Testing Environments

The network is 100/1000Mbit Ethernet with CAT 5e cabling and a mix of Allied Telesyn AT-9816GB and AT-9812T switches. Software is installed on a tri-homed SuperMicro SuperServer 6012P-6 (the *"sensor"*, with dual 1.8GHz Pentium 4 processors and 2GB RAM) on the target subnet, or the IDS appliance is installed as provided by the vendor. Where specific network cards and drivers are not provided by the vendor, the Intel Pro/100 Server adapter is used for sensing, and the Intel Pro/100

desktop adapter is used for management. There is no firewall protecting the target subnet.

All "normal" network traffic, background load traffic and exploit traffic is mirrored to a single SPAN port, to which the sensor's detection interface is connected. An Adtech network monitoring device monitors the same mirrored traffic to ensure that the total amount of traffic never exceeds 100Mbps (which would invalidate the test run).

The IDS sensor is bound to the sniffing interface in "stealth mode" wherever that is supported (i.e. no IP address) and a second 100Mbit interface is used to connect the IDS sensor to the management console on a private subnet. This ensures that the IDS sensor and console can communicate even when the target subnet is subjected to heavy loads, in addition to preventing attacks on the console itself. The products that are under this test;

- CISCO IDS 4235
- ISS Proventia A201
- NFR NID 310
- Snort 2.0

7.3 Detection Engine Topic

The aim of this test is to verify that the sensor is capable of detecting a wide range of common exploits accurately, whilst remaining resistant to false positives. The latest signature pack is acquired from the vendor, and sensors are deployed with **all** available attack signatures enabled (some audit/informational signatures may be disabled).

7.3.1 Attack Recognition

7.3.1.1 Description

Whilst it is not possible to validate completely the entire signature set of any IDS sensor, this test attempts to demonstrate how accurately the sensor reports a wide range of common exploits, port scans, and Denial of Service attempts. All attacks are run with no load on the network and no IP fragmentation.

Our attack suite contains over 100 exploits covering the following areas: Backdoors, DNS, DOS, False negatives, Finger, FTP, HTTP, ICMP, Reconnaissance and RPC.

A wide range of vulnerable target operating systems and applications are used, and the majority of the attacks are successful, gaining root shell or administrator privileges on the target machine.

We expect all the attacks to be reported in as straightforward and clear a manner as possible (i.e. an "RDS MDAC attack" should be reported as such, rather than a "Generic IIS Attack"). Wherever possible, attacks should be identified by their assigned CVE reference. It will also be noted when a response to an exploit is considered too "noisy", generating multiple similar or identical alerts for the same attack.

The **"default"** *Attack Recognition Rating* (ARR) is expressed as a percentage of detected exploits against total number of exploits launched with the default signature set as received by NSS - this demonstrates how effective the sensor can be when simply deploying the default configuration.

Following the initial test run, each vendor is provided with a list of CVE references of the attacks missed, and then has 72 hours to produce an updated signature set. The sensor is then exposed to a second round of identical tests and the "custom" ARR is

determined. This demonstrates how effective the vendor is at responding to a requirement for new or updated signatures.

Both the *default* and *custom* ARR figures are reported.

7.3.1.2 Test Result

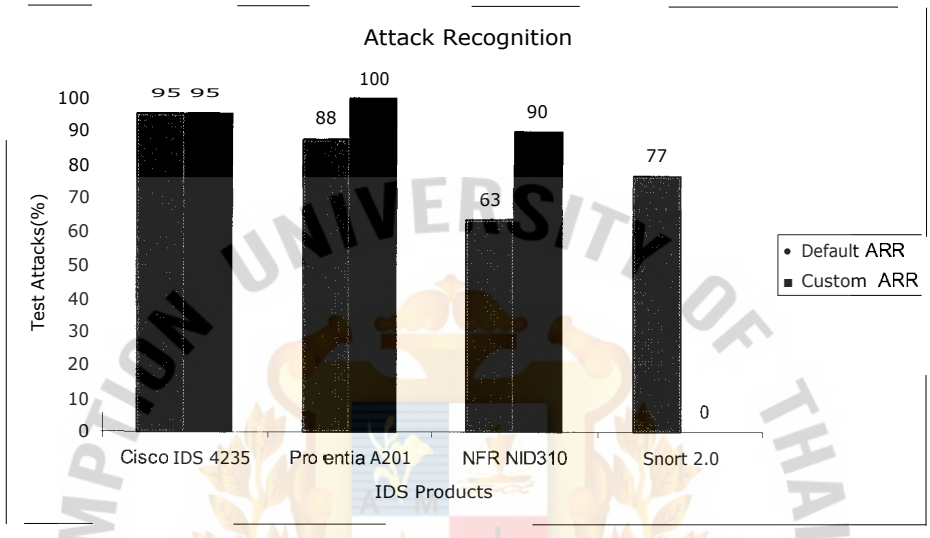


Figure 7-1 Attack Recognition

- All products didn't pass all with default configuration
- Proventia A201 passed all attacks when customized the configuration
- Cisco IDS 4235 didn't pass some of false negatives and RPC
- NFR NID310 didn't pass some of DOS, False negatives, HTTP and Reconnaissance
- Snort passed all of Reconnaissance and RPC, but passed some attack with the others
- Snort was the only product where we did not have the option to allow the vendor to produce a custom signature set

7.3.2 Resistance to False Positives

7.3.2.1 Description

The aim of this test is to demonstrate how likely it is that a sensor raises a false positive alert.

We have a number of trace files of normal traffic with "suspicious" content, together with several "neutered" exploits which have been rendered completely ineffective. If a signature has been coded for a specific piece of exploit code rather then the underlying vulnerability, or if it relies purely on pattern matching, some of these false alaims could be alerted upon.

The IDS attains a "PASS" for each test case if it does **not** raise an alert. Raising an alert on any of these test cases is considered a "FAIL".

7.3.2.2 Test Result

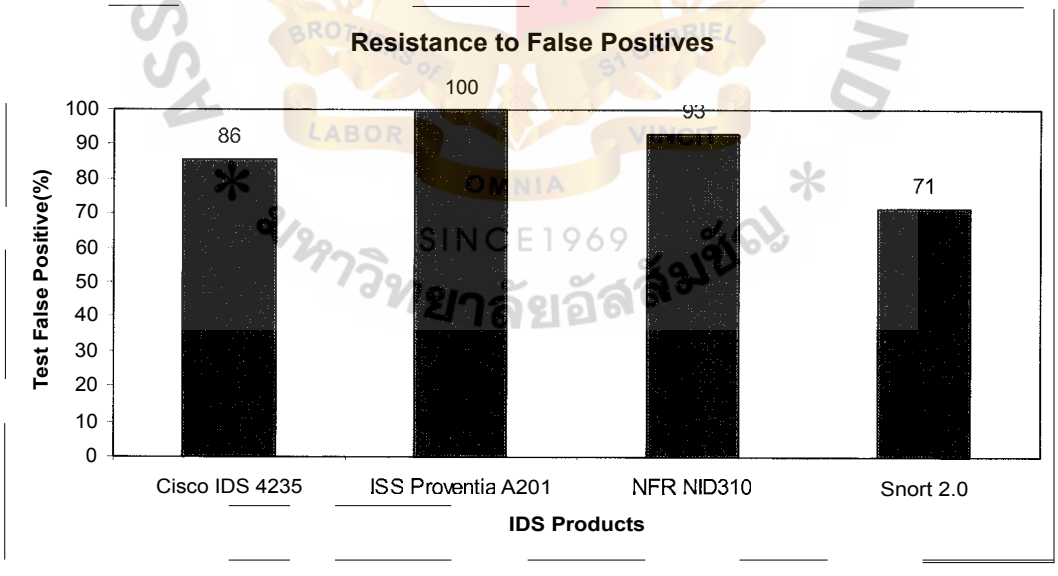


Figure 7-2 Resistance to False Positives

- Proventia A201 passed all testing

- NFR NID310 failed in
    - MSTREAM communications using invalid commands
- Cisco IDS 4235 failed in
    - MSTREAM communications using invalid commands
    - Normal directory traversal (below web root)
- Snort failed in
    - normal directory traversal (below web root),
    - MDAC heap overflow using GET instead of POST,
    - MSTREAM communications using invalid commands, and
- SNMP V3 packet with invalid request ID

7.3.3 Detection engine summary

As with our last round of tests, it was good to note that vendors are paying much more attention to *quality* of signatures rather than *quantity*, or *breadth of coverage.* False positives and information overload are the bane of the security administrators life - if alerts are not accurate the IDS becomes the equivalent of the boy who cried wolf. At best, the administrator will miss some attacks in the midst of the deluge. At worst, whole groups of signatures will be disabled, or the IDS simply ignored altogether. All three products showed good breadth of coverage (Proventia and Cisco being particularly good both out of the box and after a single update), with good resistance to false positives.

7.4 NIDS Performance Under Load Topic

The aim of this section is to verify that the sensor is capable of detecting exploits when subjected to increasing loads of background traffic up to the maximum bandwidth supported as claimed by the vendor.

The latest signature pack is acquired from the vendor, and sensors are deployed with all available attack signatures enabled (some audit/informational signatures may be disabled).

Our "attacker" host launches a fixed number of exploits at a target host on the subnet being protected by the NIDS sensor. An Adtech network monitor is configured to monitor an identically-mirrored combination of normal, exploit and background traffic to the IDS sensor, and is capable of reporting the total number of exploit packets seen on the wire as verification.

A fixed number of exploits are launched with zero background traffic to ensure the IDS sensor is capable of detecting our baseline attacks. Once that has been established, increasing levels of varying types of background traffic are generated in order to determine the point at which the sensor begins to drop packets and therefore miss attacks - all tests are repeated with 25Mbps, 50Mbps, 75Mbps and 100Mbps of background traffic.

At all stages, the Adtech network monitor verifies both the overall traffic loading and the total number of exploits seen on the target subnet. An additional confirmation is provided by the target host which reports the number of exploits which actually made it through.

The *Attack Detection Rate* (ADR) at each background load is expressed as a percentage of the number of exploits detected by the sensor against the number verified by the Adtech network monitor and target host.

For each type of background traffic, we also determine the maximum load the IDS can sustain before it begins to drop packets/miss alerts.

7.4.1 **UDP** Traffic to Random valid Ports

7.4.1.1 Description

This test uses UDP packets of varying sizes generated by a **SmartBits SMB6000** with LAN-3301A 10/100/1000Mbps **TeraMetrics** cards installed. A constant stream of the appropriate mix of packets - with variable source and destination IP addresses and ports - is injected onto the target segment.

Each packet contains dummy data, and is targeted at a valid port on a valid IP address on the target subnet. The percentage load and packets per second (pps) figures are verified by the Adtech network monitoring tool before each test begins. Multiple tests are run and averages taken where necessary.

This traffic does not attempt to simulate any form of "real world" network condition, and the aim of this test is purely to determine the raw sniffing speed of the IDS sensor, and its effectiveness at discarding "useless" packets quickly in order to pass potential attack packets to the detection engine.

- 64 byte packets – maximum 148,000 packets per second: This is our "sniffing torture test" with a background load made up of small packets in order to achieve the maximum packets per second throughput possible on a 100Mbps network. With hardware improving all the time, we expect even

commercial off the shelf servers to be capable of demonstrating a good level of performance in this test at 100Mbps.

- 440 byte packets - maximum 26,000 packets per second: This test has been included to provide a comparison with our "real world" packet mixes, since the average packet size is similar. No sessions are created during this test and there is very little for the IDS engine to do in the way of protocol analysis. This test provides a reasonable indication of the ability of an IDS to retrieve packets from the wire on an "average" network, and we would expect all products to demonstrate good performance levels.
- 1514 byte packets - maximum 8,172 packets per second: This test is the complete opposite of the 64 byte packet test, in that we would expect every single product to be capable of returning 100 per cent detection rates across the board when using only 1514 byte packets. We have included this test mainly to demonstrate how easy it is to achieve good results using large packets – beware of test results that only quote performance figures using similar packet sizes.

7.4.1.2 Test Result

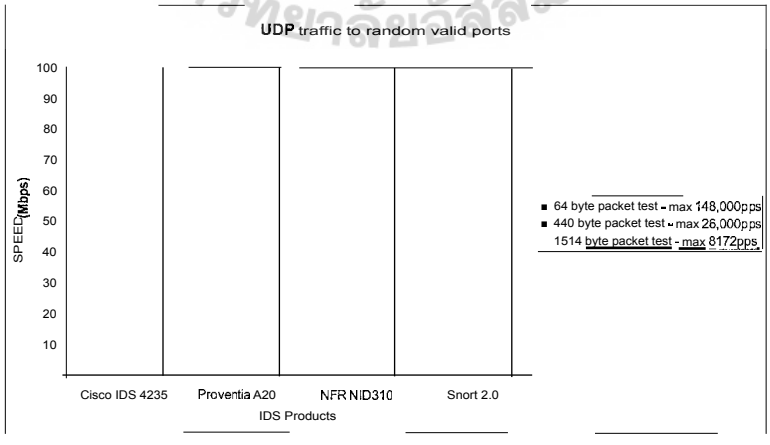


Figure 7-3 UDP Traffic to random valid ports

- Cisco IDS 4235 could handle all packets size.
- Proventia could handle 64 byte packets 95 %
- NFR could handle 64 byte packets 45 %
- SNORT could handle 64 byte packets 35 %

7.4.2 HTTP "Maximum Stress" Traffic with no Transaction Delays

7.4.2.1 Description

HTTP is the most widely used protocol in most normal networks, as well as being one of the most widely exploited. The number of potential HTTP exploits for the protocol makes a pure HTTP network something of a torture test for the average IDS sensor.

By creating genuine session-based traffic with varying session lengths, the IDS is forced to track valid sessions, thus ensuring a higher workload than for simple packet-based background traffic. This provides a test environment that is as close to "real world" as it is possible to achieve in a lab environment, whilst ensuring absolute accuracy and repeatability.

The aim of this test is to stress the HTTP detection engine and determine how the sensor copes with detecting exploits under network loads of varying average packet size and varying connections per second. Each transaction consists of a single HTTP GET request and there are no transaction delays. All packets contain valid payload (a mix of binary and ASCII objects) and address data, and this test provides an excellent representation of a live network (albeit one biased towards HTTP traffic) at various network loads.

- Max 250 new connections per second - average packet size 1200 bytes - maximum 10,000 packets per second.

- Max 500 new connections per second - average packet size 540 bytes - maximum 23,000 packets per second.
- Max 1,000 new connections per second - average packet size 440 bytes - maximum 28,000 packets per second.
- Max 2,000 new connections per second - average packet size 350 bytes - maximum 36,000 packets per second.

7.4.2.2 Test Result

HTTP "maximum stress" traffic with no transaction delays	Cisco IDS 4235	Proventia A201	NFR NID310	Snort 2.0
Max 250 connections per second – ave packet size 1200 bytes - max 10,000 packets per second	100Mbps	100Mbps	100Mbps	100Mbps
Max 500 connections per second - ave packet size 540 bytes - max 23,000 packets per second	100Mbps	100Mbps	100Mbps	100Mbps
Max 1000 connections per second - ave packet size 440 bytes - max 28,000 packets per second	100Mbps	100Mbps	100Mbps	100Mbps
Max 2000 connections per second – ave packet size 350 bytes - max 36,000 packets per second	100Mbps	100Mbps	100Mbps	100Mbps

7.4.3 HTTP "Maximum Stress" Traffic with Transaction Delays

7.4.3.1 Description

This test is identical to Test in 7.4.2 except that we introduce a 10 second delay in each transaction. This has the effect of maintaining a high number of open connections throughout the test, thus forcing the sensor to utilise additional resources to track those connections.

- Max 500 new connections per second - average packet size 540 bytes - maximum 23,000 packets per second - 10 second transaction delay - maximum 5,000 open connections.

- Max 1,000 new connections per second - average packet size 440 bytes - maximum 28,000 packets per second - 10 second transaction delay - maximum 10,000 open connections.

7.4.3.2 Test Result

HTTP "maximum stress" traffic with transaction delays	Cisco IDS 4235	**Proventia** A201	**NFR NID310**	Snort 2.0
Max 500 connections per second - ave packet size 540 bytes - max 23,000 packets per second - 10 sec delay - max 5,000 open connections	100Mbps	100Mbps	100Mbps	100Mbps
Max 1000 connections per second - ave packet size 440 bytes - max 10,000 packets per second - 10 sec delay - max 5,000 open connections	100Mbps	100Mbps	100Mbps	100Mbps

7.4.4 Protocol mix traffic

7.4.4.1 Description

Whereas 7.4.2 and 7.4.3 provide a pure HTTP environment with varying connection rates and average packet sizes, the aim of this test is to simulate more of a "real world" environment by introducing additional protocols whilst still maintaining a precisely repeatable and consistent background traffic load (something that is rarely seen in a real world environment).

The result is a background traffic load that, whilst less stressful than previous tests, is closer to what may be found on a heavily-utilised "normal" production network.

- 72% HTTP traffic (560 byte packets) + 20% FTP traffic + 6% UDP traffic (256 byte packets). Max 38 new connections per second - average packet size 555 bytes - maximum 2,200 packets per second - maximum 14 open connections.

7.4.4.2 Test Result

Protocol mix	Cisco IDS 4235	Proventia A201	NFR NID310	Snort 2.0
72% HTTP (540 byte packets) + 20% FTP + 4% UDP (256 byte packets). Max 38 connections per second - ave packet size 555 bytes - max 2,200 packets per second - max 14 open connections	100Mbps	100Mbps	100Mbps	100Mbps

7.4.5 "Real World" Traffic

7.4.5.1 Description

This is the closest we can come to a true "real world" environment under lab conditions.

For this test we eliminate the WebReflector device and substitute an IIS Web server installed on a dual P4 SuperMicro server with Gigabit interface. This server holds a copy of The NSS Group Web site, and is capable of handling 950Mbps of traffic.

We capture a typical browsing session on the NSS Group Web site, accessing a mixture of menu pages, lengthy text-based reports and multiple graphical images (screen shots) and have WebAvalanche replay multiple identical sessions from up to **25 new users per second.** It should be noted that whereas the goal of the previous tests is a very predictable, consistent and repeatable background load that never varies, the nature of this test means that traffic is much more "bursty" in nature.

- **Pure HTTP Traffic (simulated browsing session on NSS Web site):** Max 10 new connections per second - 3 new users per second - average packet size 1000 bytes - maximum 11,000 packets per second.

Note that the average packet sizes during this test do not match the various studies on Internet packet size distribution (we consider the average packet size to be in the

region of 440-550 bytes). However, given that this is a test which utilises real browsing sessions against a real server on a real network, the resulting packet distribution should be considered valid.

To gauge the effects of varying (smaller) packet sizes, connection rates and transaction delays, the results of tests in 7.4.2 – 7.4.4 should be examined.

7.4.5.2 Test Result

Real World traffic	Cisco IDS 4235	Proventia A201	NFR NID310	Snort 2.0
Pure HTTP (simulated browsing session on NSS Web site). Max 10 connections per second - 3 new users per second - ave packet size 1000 bytes - max 11,000 packets per second	100Mbps	100Mbps	100Mbps	100Mbps

7.4.6 NIDS Performance under load summary

Comparing the NFR against both the ISS and Cisco products in our 64 byte packets tests, for example, it is apparent that the NID-310 cannot match the other two in terms of raw sniffing speed. However, when it comes to our real world tests, and even HTTP stress tests, where raw packets-per-second performance is not as critical, the NFR product has no problems in handling everything we had to throw at it. As you would expect, the Cisco and Proventia also showed our real world and HTTP tests a clean pair of heals, with all three devices turning in a straight set of 100 percent detection rates across the board.

7.5 Network IDS Evasion Topic

The aim of this section is to verify that the sensor is capable of detecting basic exploits when subjected to varying common evasion techniques.

7.5.1 Evasion Baselines

7.5.1.1 Description

The aim of this test is to establish that the sensor is capable of detecting a number of common basic attacks (our baseline suite) in their normal state, with no evasion techniques applied.

7.5.1.2 Test Result

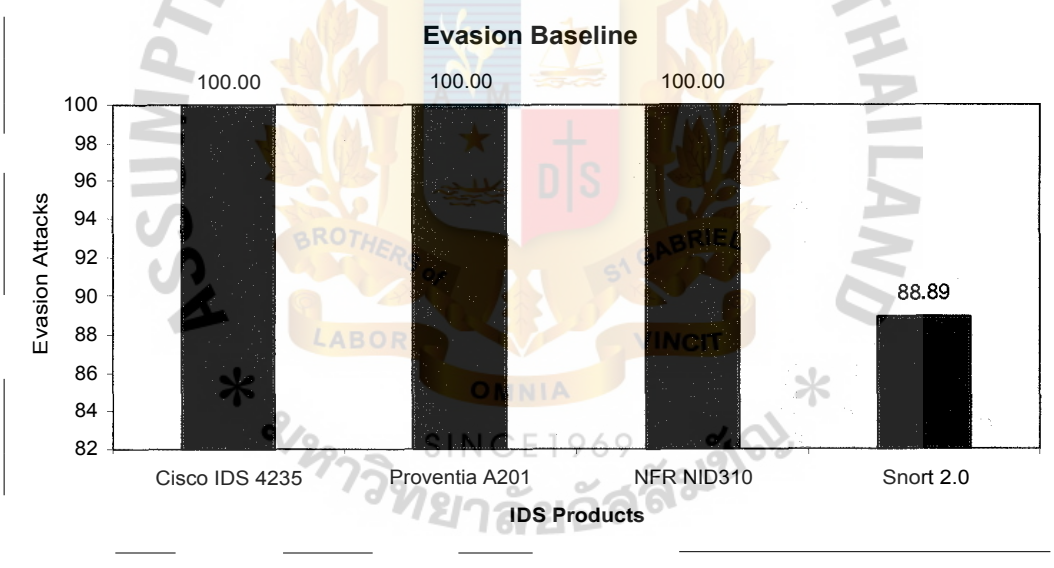


Figure 7-4 Evasion Baseline

- Commercial IDS products could detect the evasion baselines.
- Snort couldn't detect the PHF remote command execution

7.5.2 Packet Fragmentation and Stream Segmentation

7.5.2.1 Description

The baseline HTTP attacks are repeated, running them through fragroute using various evasion techniques, including IP fragmentation and TCP segmentation

For each of the evasion techniques, we note if

- The attempted attack is detected in any form, and
- If the exploit is successfully "decoded" to provide an accurate alert relating to the original exploit, rather than alerting purely on anomalous traffic detected as a result of the evasion technique itself.

7.5.2.2 Test Result

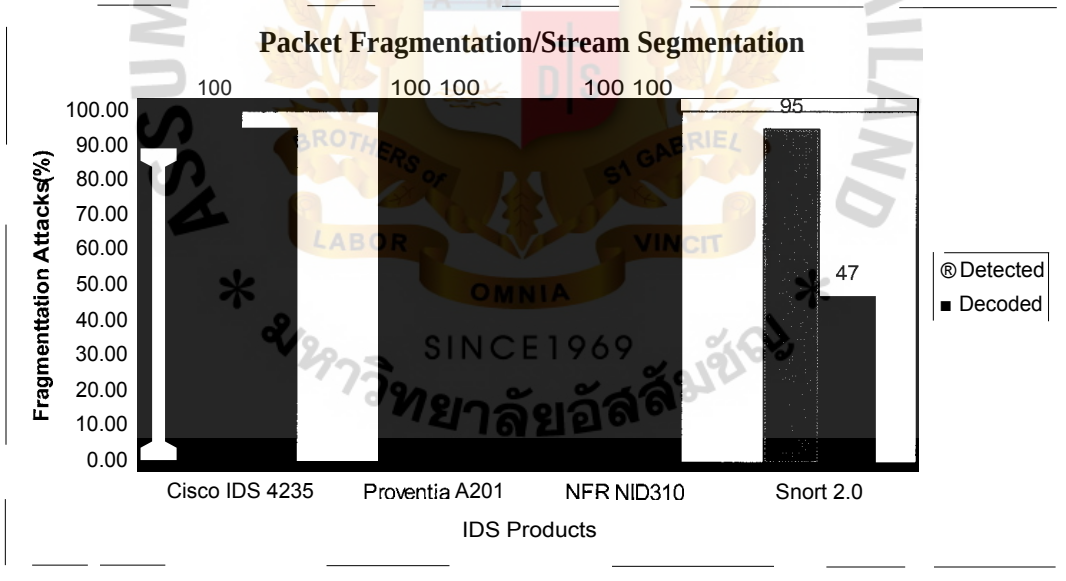


Figure 7-5 Packet Fragmentation/ Stream Segmentation

- Cisco didn't decoded for PAWS elimination although suspicious activity was detected

- Almost of the fragroute attacks were detected, Snort was difficulty in decoding

7.5.3 URL Obfuscation

7.5.3.1 Description

The baseline HTTP attacks are repeated, this time applying various URL obfuscation techniques made popular by the Whisker Web server vulnerability scanner, including:

- URL encoding
- /./ directory insertion
- Premature URL ending
- Long URL
- Fake parameter
- TAB separation
- Case sensitivity
- Windows \ delimiter
- Session splicing

For each of the evasion techniques, we note if

- The attempted attack is detected in any form, and
- If the exploit is successfully "decoded" to provide an accurate alert relating to the original exploit, rather than alerting purely on anomalous traffic detected as a result of the evasion technique itself.

7.5.3.2 Test Result

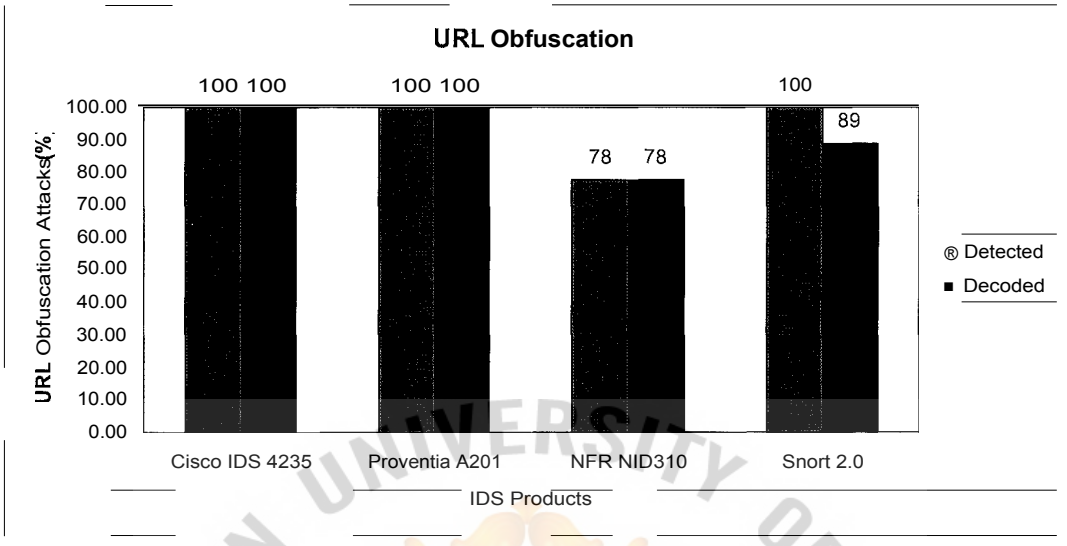


Figure 7-6 URL Obfuscation

- NFR didn't detect and decode
- Case Sensitivity
- Windows\delemiter
- Snort didn't decode the long url

7.5.4 Miscellaneous Evasion Techniques

7.5.4.1 Description

Certain baseline attacks are repeated, and are subjected to various protocol- or exploit-specific evasion techniques, including:

- Altering default ports
- Inserting spaces in FTP command lines
- Inserting non-text Telnet opcodes in FTP data stream
- Altering protocol and RPC PROC numbers

- RPC record fragging
- Polymorphic mutation (ADMmutate)

For each of the evasion techniques, we note if

- The attempted attack is detected in any form, and
- If the exploit is successfully "decoded" to provide an accurate alert relating to the original exploit, rather than alerting purely on anomalous traffic detected as a result of the evasion technique itself.

7.5.4.2 Test Result

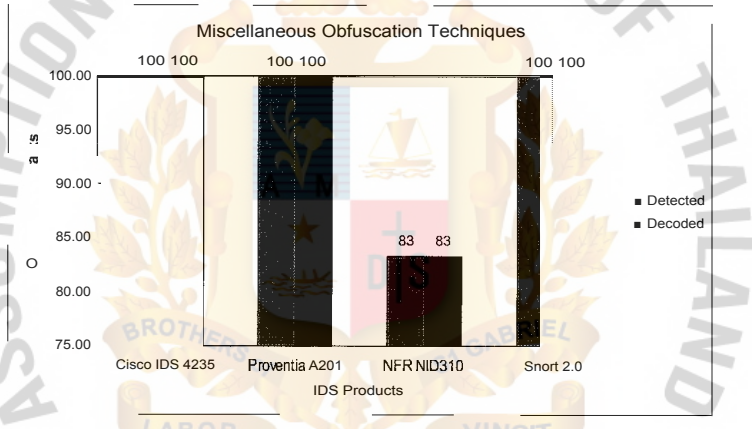


Figure 7-7 Miscellaneous Obfuscation Techniques

- NFR didn't detect and decode Alerting default ports

7.5.5 Network IDS Evasion Summary

Resistance to evasion techniques is one of those areas that seems to be susceptible to being "broken" each time an IDS product is updated in any significant way - thankfully, that does not seem to be the case this time around. Although the NFR NID-310 still has a blind spot with a couple of the Whisker evasion tests, resistance to evasion techniques is generally very good across all of the products under test, with

the majority of our fragroute, Whisker, and other miscellaneous techniques we employed being detected with few problems.

It is a fact that the majority of the traffic on the average corporate network today is HTTP. It is also a fact that the majority of the exploits and evasion/obfuscation techniques out there in the wild will also find their way onto our networks via the HTTP protocol. Thus, the processing power required to handle a fully-loaded network segment of HTTP traffic is significant, and the design of the HTTP detection engine is critical.

The extra work involved in performing HTTP traffic normalisation (eliminating the obfuscation techniques used by the likes of Whisker), executing a full protocol decode, and tracking large numbers of active sessions, tends to take its toll on all Network IDS products. Even those that can pull packets off the wire faster than anyone else can suddenly find themselves undone by a poorly implemented HTTP decode module or inefficient stateful analysis capabilities.

7.6 **Stateful** Operation Topic

The aim of this section is able to determine whether the IDS sensor is capable of monitoring stateful sessions at various traffic loads without either losing state or incorrectly inferring state.

7.6.1 Attack Replay

7.6.1.1 Description

This test determines whether the sensor is resistant to stateless attack flooding tools such as *Stick* and *Snot* - these utilities are used to generate large numbers of false alerts on the protected subnet using valid source and destination addresses and a range of protocols.

We run 15 seconds of Stick or Snot traffic past the sensor and note how many alerts are raised, whether a Denial of Service/flooding condition occurs between sensor and management server/console, and whether the sensor continues to detect genuine exploits whilst the flood is active.

- Snot test (15 seconds using default rule set)
- Stick test (15 seconds using default rule set)

7.6.1.2 Test Result

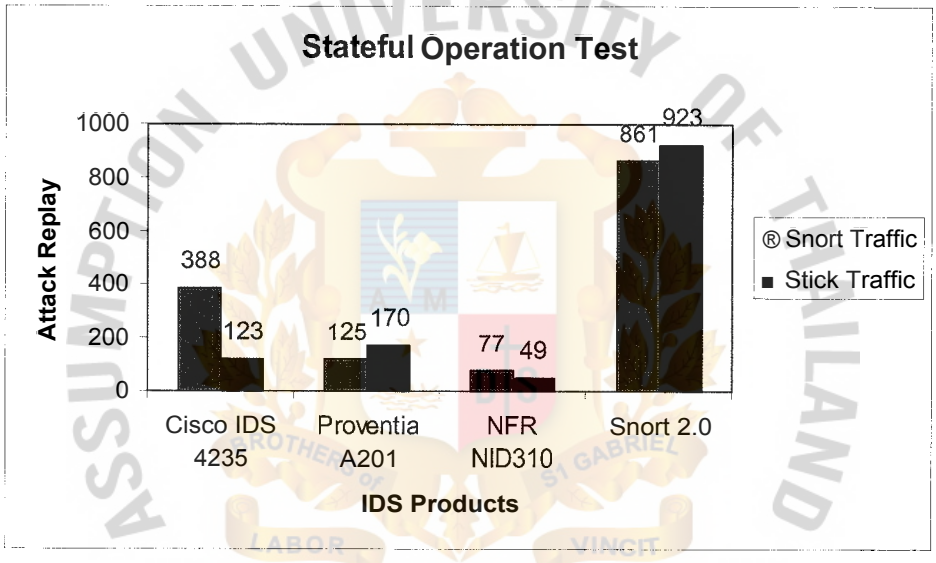


Figure 7-8 Stateful Operation Test

- This test determines whether the sensor is resistant to stateless attack flooding tools such as Stick and Snot
- Resistance to stick and snot of NFR was excellent, and Cisco and ISS was acceptable

7.6.2 Simultaneous Open Connections

7.6.2.1 Description

This test determines whether the sensor is capable of preserving state across increasing numbers of open connections, as well as continuing to detect new exploits when the state tables are filled. A legitimate HTTP session is opened and the first packet of a two-packet exploit is transmitted. The CAW WebAvalanche then opens various numbers of TCP sessions from 10,000 to 1,000,000 (one million). The initial HTTP session is then completed with the second half of the exploit and the session is closed. If the IDS is still maintaining state on the first session established, the exploit will be recorded. If the state tables have been exhausted, the exploit string will be seen as a non-stateful attack, and will thus be ignored.

Both halves of the exploit are required to trigger an alert - an IDS will fail the test if it fails to generate an alert after the second packet is transmitted, or if it raises an alert on either half of the exploit on its own. At each step, we ensure that the IDS engine is still capable of detecting freshly-launched exploits. This test is run using the default sensor settings.

- Attack Detection: This test ensures that the sensor continues to detect new exploits as the number of open sessions is increased in stages from 10,000 to 1,000,000
- State Preservation: This test ensures that the sensor maintains the state of pre-existing sessions as the number of open sessions is increased in stages from 10,000 to 1,000,000

7.6.2.2 Test Result

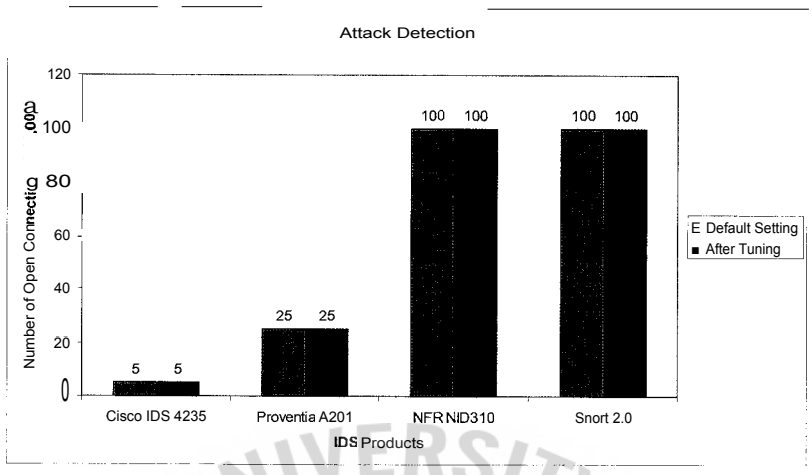


Figure 7-9 Attack Detection

- This test ensures that the sensor continues to detect new exploit as the number of open sessions is increased in stages from 10,000 to 1,000,000

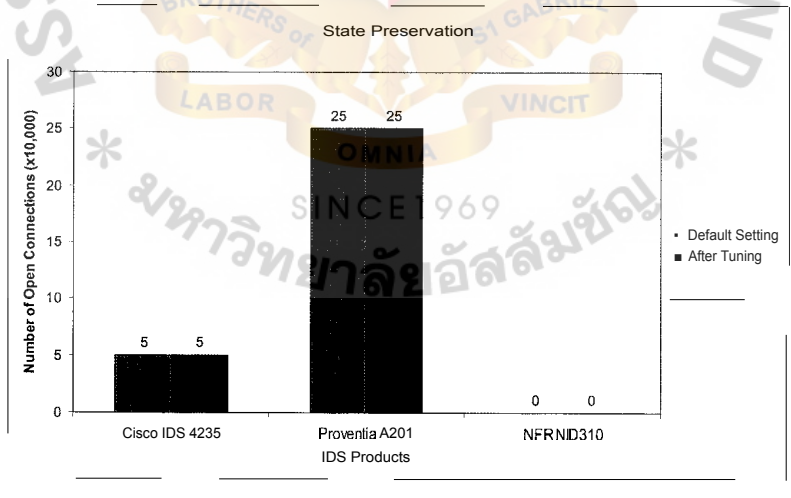


Figure 7-10 State Preservation

- This test ensures that the sensor maintains the state of pre-existing sessions as the number of open sessions is increased in stages from 10,000 to 1,000,000

- NFR is capable of maintaining state up to 50,000 open connections, but only for a maximum of around 30-60 Seconds
- Snort unable to run connections tests since there was no signature to handle the exploit used in these tests

7.6.3 Stateful Operation Summary

In terms of raw processing power coupled with the efficiency of the detection engine on a fully loaded 100Mbps segment, all three commercial products under test in this report appear to have got it right.

One area where none of them quite got it right first time was in handling large numbers of open connections. Both Cisco and Proventia demonstrated bugs during testing which prevented them from handling in excess of their default settings.

One thing that is worth noting is that you would be wise to configure Proventia to handle as many open connections as it can, since once that limit is reached, it is the only product of the three which drops *new* connections, setting it up for a possible evasion attempt at that point. The others under test here age out *old* connections when they reach their open connection limit and, whilst it is still technically possible to evade these products in such a situation, it is far more difficult to do so, and we feel that ageing out old connections is a better way to handle that particular condition. The NFR NID-310 also gave us cause for concern in this area due to the fact that it appears to age out existing connections far too aggressively when under stress, again setting itself up for a possible evasion attempt.

7.7 IDS Management Topic

Management and forensic reporting are becoming critical as IDS products are deployed more and more in large organisations - high speed switched networks mean

that a single IDS sensor simply cannot cut it any more in many implementations. The ability to fine-tune individual signatures or entire policies and then deploy them to multiple sensors at the click of a button is essential. As is the ability to filter the wheat from the chaff, allowing the administrator to slice and dice his data in a number of ways, mining the data to determine which alerts are the most significant.

New capabilities just beginning to appear in some products apply correlation techniques to match apparently disconnected events from different sensors, or match vulnerability scans to IDS alerts, in order to more accurately identify a real threat and alert the administrator accordingly.

Without a doubt, Proventia - with its SiteProtector management console - excelled in this area, demonstrating the most comprehensive and usable feature set when it comes to policy management and event handling. With the optional Security Fusion module providing advanced correlation, this is the one product that seems to have shown a real advance in management and analysis capabilities since our last test.

The Cisco management solution is also very good, while NFR lags behind in the feature stakes as we wait for its new console to appear.

CHAPTER 8 IDS/IPS DEPLOYMENT

The location of IDS/IPS is an important where it can sniff all packets. Network-Based IDS/IPS and Host-Based IDS/IPS will have a different capability. A deployment will concern the objective, performance and cost.

8.1 IDS/IPS Deployment Mode

8.1.1 Span Mode

Hub ports or SPAN ports from one or more network switches can be connected to the IDS system's detection ports. Response actions such as resetting a TCP connection can often be injected by the sensors using the same port

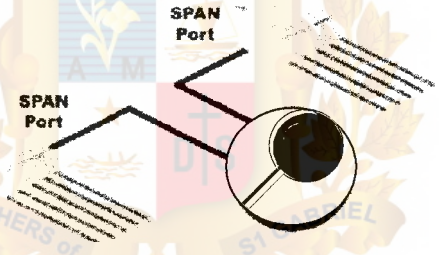


Figure 8-1 SPAN MODE

In the switched environment, we will use the mirror port or span port to sniff the traffic between the network devices. And for protect it; we should hide it with the stealth mode.

8.1.2 In-Line Mode

IDS/IPS sit in the data path, with active traffic passing through them. The IDS/IPS prevents network attacks by dropping malicious traffic in real time. Preventative action can be custom-defined at a highly granular level, including automated dropping of DoS Traffic intended for a specific Web Server. Wire speed prevention and highly available operation enable IDS/IPS deployment in mission-critical environments

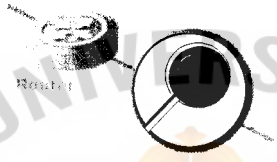


Figure 8-2 IN-LINE MODE

This mode is not only the monitoring tool; it has protected the attack with its algorithm method for depth security prevention. It will locate like the firewall.

8.2 Deployment Strategy

8.2.1 IDS/IPS Sensor in External Network

Objective:

To screen every packet from the Internet

Description:

The Network-Based IDS/IPS engine will sniff behide of the router with hide mode and the management server will locate in local network. The Network-Based IDS/IPS engine will be managed from management server via out-bound connection.

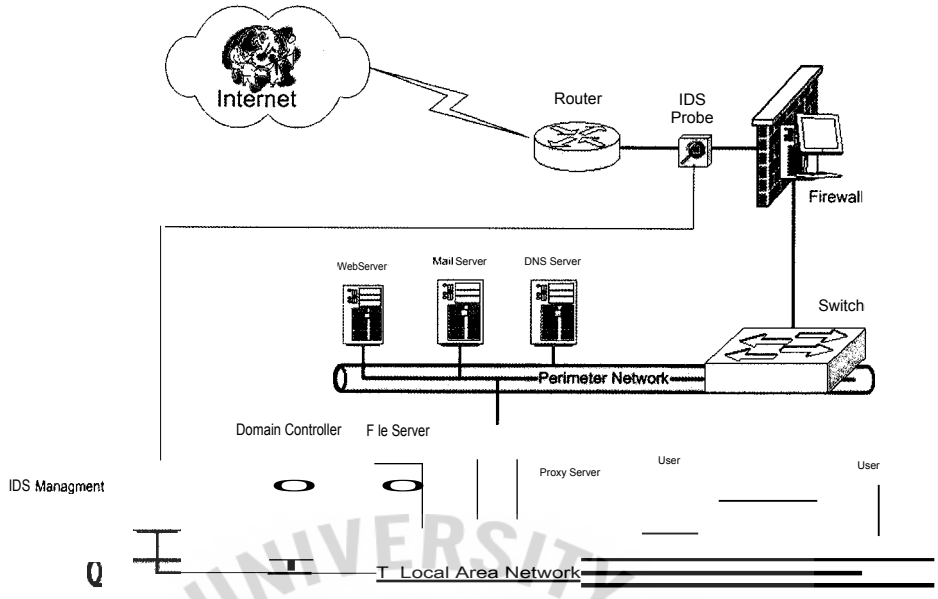


Figure 8-3 IDS/IPS sensor in external network

The Network-Based IDS/IPS engine will sniff between Internet Router and Firewall that the throughput will be limited by them. The fault-positive will be a bother message in this configuration.

Product Recommend:

Brand	Model	Performance	**Price(Baht)**	Remark
Cisco	IDS 4215	80 Mbps, 800 Connections	292,000	
ISS	Proventia G100	100Mbps	598,000	
Juniper	IDP 10	20 Mbps, 10K Sessions	470,000	

8.2.2 IDS/IPS Sensor in Perimeter network or DMZ Network

Objective:

To screen every packet from the Internet that pass through the firewall

Description:

The Network-Based IDS/IPS engine will sniff behide of the firewall with hide mode and the management server will locate in local network. The Network-Based IDS/IPS engine will be managed from management server via out-bound connection.

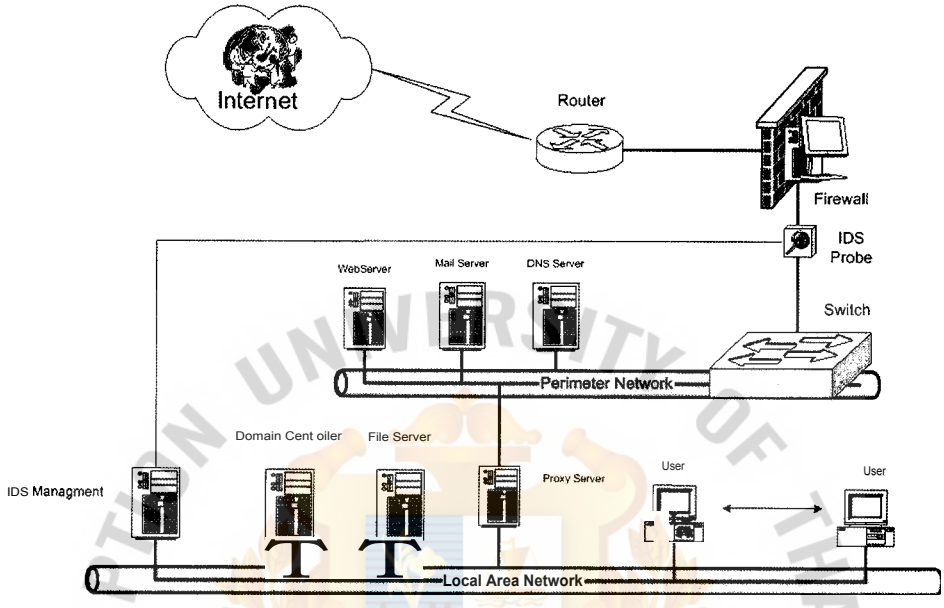


Figure 8-4 IDS/IPS sensor in perimeter network or dmz network

The Network-Based IDS/IPS engine will sniff the packets that pass through from firewall for inbound. However, when locate it in local network, it want more hardware specification for scan the network. The fault-positive will be least than fist configuration (Behide the router).

Product Recommend:

Brand	Model	Description	Price(Baht)	Remark
Cisco	IDS 4235	250Mbps, 3000 Connections	500,000	
ISS	Proventia A201	200Mbps	740,000	
ISS	Proventia G200	200Mbps	854,000	
Checkpoint	InterSpect 210	200Mbps	476,000	

Brand	Model	Description	Price(Baht)	Remark
Juniper	IDP 100	200Mbps, 70K Sessions	972,000	

8.2.3 IDS/IPS Sensor in Internal Network

Objective:

To screen packet from the local network

Description:

The Network-Based IDS/IPS engine will sniff front of the switch or uplink of user switch with hide mode and the management server will locate in save local network. The Network-Based IDS/IPS engine will be managed from management server via out-bound connection.

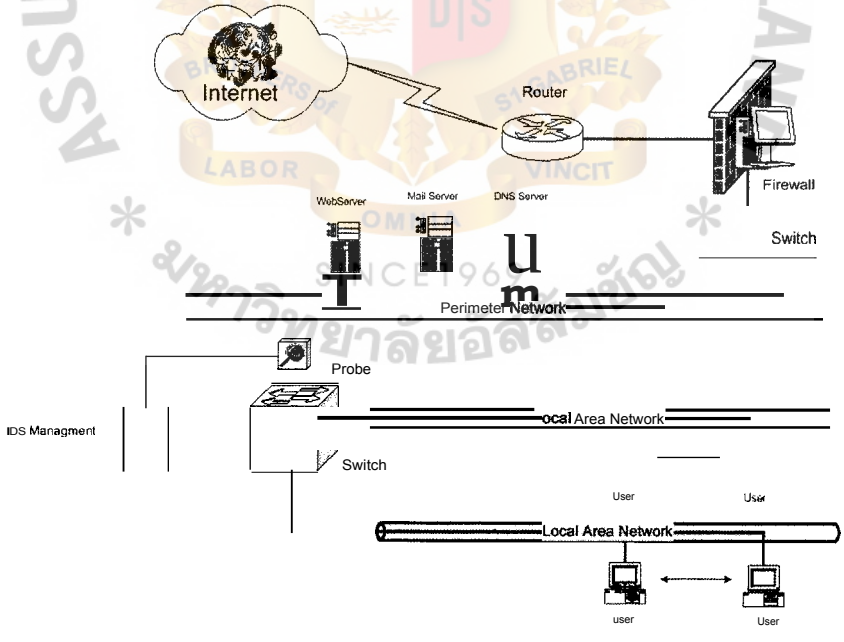


Figure 8-5 IDS/IPS sensor in internal network

The Network-Based IDS/IPS engine will sniff the packet that is sent from users. This configuration is appropriate the complicated network that there are many users in many network segments and difficult to control all user. This configuration may use many engine in each network segment. The Network-Based IDS/IPS should have enough the speed for local network.

Product Recommend:

Brand	Model	Description	**Price(Baht)**	Remark
Cisco	IDS 4250	500 Mbps, 5000 Connections	1,000,000	
ISS	Proventia A604	600Mbps	1,707,000	
Checkpoint	InterSpect 410	500Mbps	952,000	
Checkpoint	InterSpect 610	1Gbps	1,904,000	
Juniper	IDP 500	500Mbps, 220K Sessions	2,060,000	
Juniper	IDP 1000	1Gbps, 500K Sessions	4,000,000	

8.2.4 IDS/IPS Sensor in High Security Network

Objective:

To screen packet that come to the servers

Description:

This configuration will compound with Network-Based IDS/IPS engine and Host-Based IDS/IPS engine that they will sniff the packet from network segment and monitor the process in the servers. All engines will be managed from the centralized management.

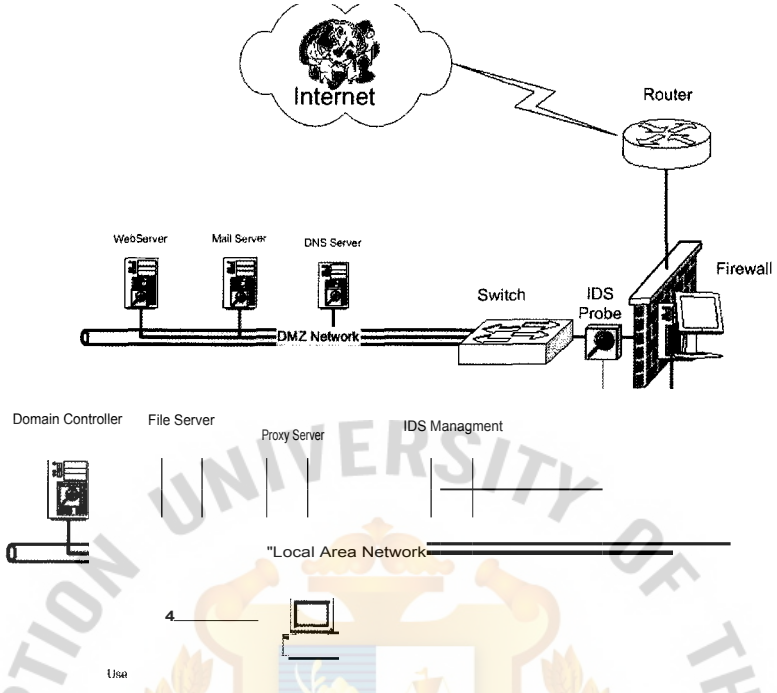


Figure 8-6 IDS/IPS sensor in high security network

The Network-Based IDS/IPS engine will prevent the malicious packet that pass through from firewall while the Host-Based IDS/IPS engine will prevent the malicious behavior that Network-Based engine can't prevent or malicious packet that be sent in own network.

Product Recommend:

Brand	Model	Description	**Price(Baht)**	Remark
Cisco	IDS 4250	500 Mbps, 5000 Connections	1,000,000	
ISS	Proventia A604	600Mbps	1,707,000	
ISS	Proventia A1204	1.2Gbps	3,072,000	
Checkpoint	InterSpect 410	500Mbps	952,000	
Checkpoint	InterSpect 610	1Gbps	1,904,000	

Brand	Model	Description	**Price(Baht)**	Remark
Juniper	IDP 500	500Mbps, 220K Sessions	2,060,000	
Juniper	IDP 1000	1Gbps, 500K Sessions	4,000,000	

8.2.5 IDS/IPS Sensor in Complicated Network

Objective:

To screen packet with separated sensors

Description:

The Network-Based IDS/IPS engine will sniff separately in Demilitarized Zone and Internal Server Zone. And Host-Based IDS/IPS engine will installed in each server. Central Management will manage all engines for high effectiveness.

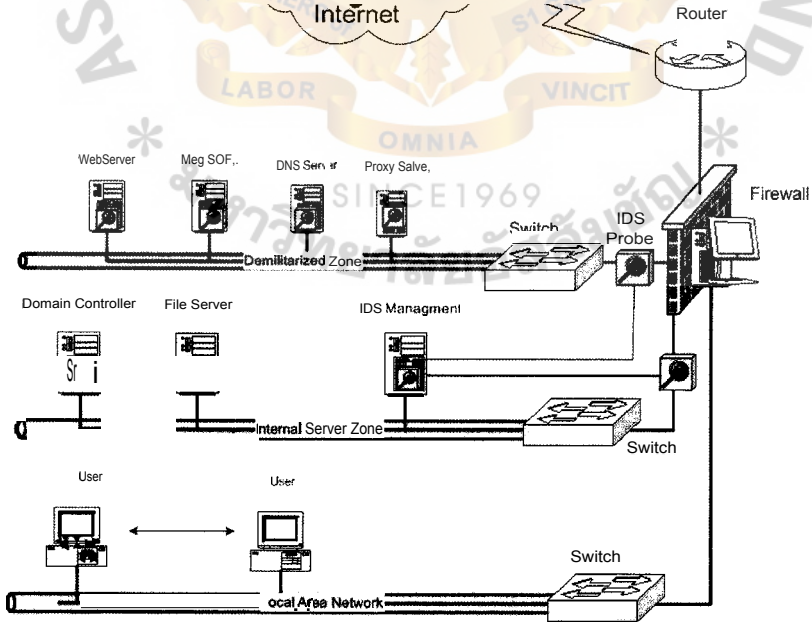


Figure 8-7 IDS/IPS sensor in complicated network

The separated network will be easy to manage the traffic. That means more security too. The Network-Based IDS/IPS will prevent the attack from other network and Host-Based IDS/IPS engine will prevent the attack that Network-Based IDS/IPS engine can't prevent or attack from local network segment pass through the server.

Product Recommend:

Brand	**Model**	**Description**	**Price(Baht)**	**Remark**
Cisco	IDS 4250	500Mbps, 5,000 Connections	1,000,000	
ISS	Proventia A604	600Mbps	1,707,000	
ISS	Proventia A1204	1.2Gbps	3,072,000	
Checkpoint	InterSpect 410	500Mbps	952,000	
Checkpoint	InterSpect 610	1Gbps, 3 Sensors	1,904,000	
Juniper	IDP 500	500Mbps, 220K Sessions	2,060,000	
Juniper	IDP 1000	1Gbps, 500K Sessions	4,000,000	

CHAPTER 9 CONCLUSION

The security and network have a different way because they have different objective. Network has an objective to serve the confidentiality, integrity and availability, but security has an objective to serve the speed and convenient of communication. This different objective must be optimized them together in real-world. That is mean the data will be sent while we can control it with rule.

The security tool are responsible the different method on different system. Today, the security doesn't be included in one product. The system may require one security tool, or more than one that depend on the requirement of security strength in the system.

- Antivirus is an integrity tool that everyone wants neither they will connect the network or not.
- Radius is an authentication or authorization tool on the multiple-user system.
- Firewall is an access control tool to limit the authorized accessing
- VPN is a confidentiality tool on Internet for encrypts the clear-text to unreadable (cipher-text).
- Vulnerability Assessment is an audit tool that find the vulnerability of system
- IDS/IPS is a monitoring tool that complements the network in depth security.

IDS and IPS has a different method. Intrusion Detection System can use non-deterministic methods to divine any sort of threat, or potential threat, from existing and historical traffic. This includes performing statistical analysis of traffic volume, traffic patterns, and anomalous activities. It is not for the faint of heart, nor should it be – it is for individuals who truly want to "know" what is happening on their networks.

Intrusion Prevention System, on the other hand, must be deterministic – correct – in all of its decisions in order to perform its function of scrubbing traffic. An IPS device is not supposed to take changes or react with some technical version of "gut instinct". It is supposed to work all of the time, and make access control decisions on the network. Firewalls provided the first deterministic approach to access control on the network, providing basic IPS capability. IPS devices add next-generation capability to these firewalls – still operating inline and providing the type of deterministic comfort required of an inline device that is making access control decisions.

Either IDS or IPS, it will be done the efficiency, if there is a traffic filtering such as the position will be located behide the firewall or router that filters the traffic with the access-lists.

BIBLIOGRAPHY

Information Technology-Essential but Vulnerable: Internet Security Trends, Richard D. Pethia, CERT Centers, November 2002

Security of the Internet, Marcel Dekker, The Froehlich/Kent Encyclopedia of Telecommunications vol. 15, 1997

Intrusion Detection Systems Test Edition 4, Group Test,The NSS Group Ltd., August 2003

Intrusion Prevention Systems (IPS): Next Generation Firewalls, Pete Lindstrom, A Spire Research Report, March 2004

False Positives: A User's Guide to Making sense of IDS Alarms, Marcus J. Ranum, ICSA Labs IDSC, February 2003

Intrusion Detection : An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response, Edward G.Amoroso, AT&T , June 1999

An Introduction to Intrusion Detection & Assessment, Rebacca Bace, ICSA Inc., March 1999

Next Generation Intrusion Detection Systems(IDS), Mcafee Security, November 2003

World Managed Security Service Provider Markets, Frost & Sullivan, 2003

WEBSITE REFERENCES

http://www.ietf.org/

http://www.cert.org/stats/

http://www.cisco.com

http://www.iss.net

http://www.nfr.com

http://www.checkpoint.com

http://www.juniper.net

http://www.sourcefire.com

http://www.spiresecurity.com

http://www.mcafeesecurity.com

APPENDIX A

PRODUCT DATASHEET

Data Sheet

Cisco IDS 4200 Series Sensors

Cisco integrated network security solutions enable organizations to protect productivity gains and reduce operating costs.

The Cisco IDS 4200 Series sensors are used in the Cisco Intrusion Protection System. These intrusion detection system sensors work in concert with the other components to efficiently protect your data and information infrastructure. With the increased complexity of security threats, achieving efficient network intrusion security solutions is critical to maintaining a high level of protection. Vigilant protection ensures business continuity and minimizes the effect of costly intrusions.

Additionally, Cisco's flexible deployment options allow businesses to minimize the total cost of ownership of their IDS deployments by delivering:

- unprecedented price/performance ratios
- the ability to simultaneously protect multiple network subnets through the support for multiple sniffing interfaces, thereby delivering up to five sensors in one
- a wide array of performance options
- investment protection by delivering modular, upgradable components
- support for multi-VLAN traffic
- embedded web-based management solutions packaged with the IDS sensors

Please refer to Table 1 for information on the characteristics of the Cisco IDS 4200 Series Sensors.

For details on the complete Cisco Intrusion Protection System, go to http://www.cisco.com/go/ids.

Deploying the Cisco IDS 4200 Series Sensors

The Cisco IDS 4200 Series includes four products: the Cisco IDS 4215, IDS 4235, IDS 4250 and IDS 4250-XL sensors. The Cisco IDS product line delivers a broad range of solutions that allow easy integration into many different environments, including enterprise and service provider environments. Each sensor addresses the bandwidth requirements at one of several speeds, from 80 Mbps to gigabits per second.

The Cisco IDS 4215 can monitor up to 80 Mbps of traffic and is suitable for T1/E1 and T3 environments. Additionally, multiple sniffing interfaces are supported on the IDS-4215 which allow the ability to simultaneously protect multiple subnets, thereby delivering five sensors in a single unit.

At 250 Mbps, the Cisco IDS 4235 can be deployed to provide protection in switched environments, on multiple T3 subnets, and with the support of 10/100/1000 interfaces it can also be deployed on partially utilized gigabit links.

The Cisco IDS 4250 supports a 500 Mbps speed and can be used to protect gigabit subnets and traffic traversing switches that are being used to aggregate traffic from numerous subnets. In addition, the Cisco IDS 4250 provides the flexibility to accommodate a simple hardware upgrade to scale to full line-rate gigabit performance.

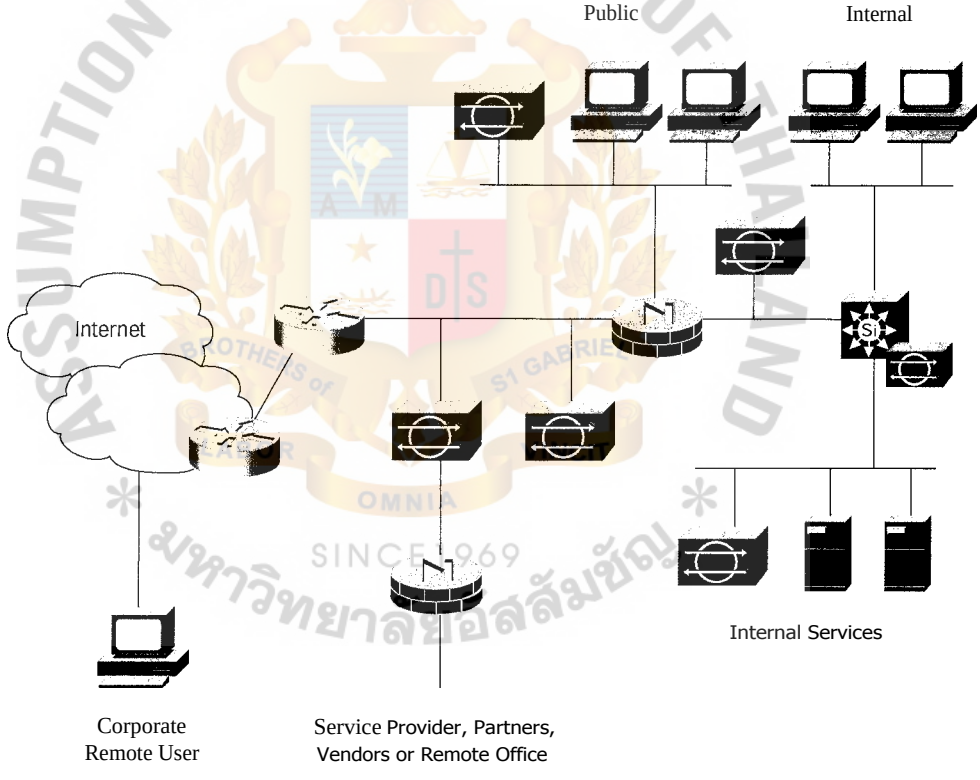
At 1 Gbps, the Cisco IDS 4250-XL provides unprecedented performance by providing customized hardware acceleration to protect fully-saturated gigabit links as well as multiple partially-utilized gigabit subnets.

As shown in Figure 1, sensors can be placed on almost any network segment of the enterprise-wide network where security visibility is required.

Please refer to Table 2 for ordering information for the Cisco IDS 4200 Series Sensors.

Figure 1

Deployment Scenarios for the 4200 Series Appliance Sensors



re

Product Specifications

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Performance	80 Mbps	250 Mbps	500 Mbps	1000 Mbps
Standard monitoring interface	10/100BASE-Tx	10/100/1000BASE-TX	10/100/1000BASE-TX	Dual 1000BASE-SX interface with MTRJ
Standard command and control interface	10/100BASE-Tx	10/100/1000BASE-TX	10/100/1000BASE-TX	10/100/1000BASE-TX
Optional interface	Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	-1000BASE-SX (fiber) -Four 10/100BaseTx (4FE) sniffing interfaces (allowing a total of 5 sniffing interfaces).	1000BASE-SX (fiber)
Performance upgradable	No	No	Yes	No
Form factor	One rack unit	One rack unit	One rack unit	One rack unit
Advanced protection algorithms				
Stateful pattern recognition	Yes	Yes	Yes	Yes
Protocol parsing	Yes	Yes	Yes	Yes
Heuristic detection	Yes	Yes	Yes	Yes
Anomaly detection	Yes	Yes	Yes	Yes
Attack protection				
Sweeps or floods	Yes	Yes	Yes	Yes
Denial-of-service (DoS) mitigation	Yes	Yes	Yes	Yes
Worms or viruses	Yes	Yes	Yes	Yes
Common gateway interface (CGI) or WWW attacks	Yes	Yes	Yes	Yes
Buffer overflow protection	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Remote-procedure call (RPC) attack detection	Yes	Yes	Yes	Yes
IP fragmentation attacks	Yes	Yes	Yes	Yes
Internet Control Message Protocol (ICMP) attacks	Yes	Yes	Yes	Yes
Simple Message Transfer Protocol (SMTP), Sendmail, Internet Message Access Protocol (IMAP), or Post Office Protocol (POP) attacks	Yes	Yes	Yes	Yes
File Transfer Protocol (FTP), Secure Shell Protocol (SSH), Telnet, and rlogin attacks	Yes	Yes	Yes	Yes
Domain Name System (DNS) attacks	Yes	Yes	Yes	Yes
TCP hijacks	Yes	Yes	Yes	Yes
Windows or NetBios attacks	Yes	Yes	Yes	Yes
TCP application protection	Yes	Yes	Yes	Yes
BackOrifice attacks	Yes	Yes	Yes	Yes
Network Timing Protocol (NTP) attacks	Yes	Yes	Yes	Yes
Customizable signatures using Signature Micro-Engine technology	Yes	Yes	Yes	Yes
Automated signature updates	Yes	Yes	Yes	Yes

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Alarm summarization	Yes	Yes	Yes	Yes
Support for 802.1q traffic	Yes	Yes	Yes	Yes
P2P / file sharing detection techniques	Yes	Yes	Yes	Yes
Secure communication				
IP Security (IPSec) or Secure Sockets Layer (SSL) between sensor and management console	Yes	Yes	Yes	Yes
Encrypted signature packages	Yes	Yes	Yes	Yes
SSH for remote administration	Yes	Yes	Yes	Yes
Serial Control Protocol (SCP) support for secure file transfer	Yes	Yes	Yes	Yes
IDS evasion protection				
IP fragmentation re-assembly	Yes	Yes	Yes	Yes
TCP stream re-assembly	Yes	Yes	Yes	Yes
Unicode deobfuscation	Yes	Yes	Yes	Yes
Active response actions				
Router access-control-list (ACL) modifications	Yes	Yes	Yes	Yes
Firewall policy modifications	Yes	Yes	Yes	Yes
Switch ACL modifications	Yes	Yes	Yes	Yes
Session termination via TCP resets	Yes	Yes	Yes	Yes
IP session logging or session replay	Yes	Yes	Yes	Yes

re

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

Active notification actions	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Alarm display	Yes	Yes	Yes	Yes
E-mail alerts	Yes	Yes	Yes	Yes
E-page alerts	Yes	Yes	Yes	Yes
Customizable script execution	Yes	Yes	Yes	Yes
Multiple alarm destinations	Yes	Yes	Yes	Yes
Third-party tool integration	Yes	Yes	Yes	Yes
IDS active update bulletins	Yes	Yes	Yes	Yes
Administration				
Web user interface (Secure Hypertext Transfer Protocol [HTTPS])	Yes	Yes	Yes	Yes
Command-line interface (CLI) (console)	Yes	Yes	Yes	Yes
CLI (Telnet or SSH)	Yes	Yes	Yes	Yes
CiscoWorks VPN Security Management Solution (VMS) support	Yes	Yes	Yes	Yes
High availability				
Redundant power supply	No	Yes	Yes	Yes
Failure detection				
Monitoring link failure detection	Yes	Yes	Yes	Yes
Communications failure detection	Yes	Yes	Yes	Yes
Services failure detection	Yes	Yes	Yes	Yes
Device failure detection	Yes	Yes	Yes	Yes
Dimensions				

Table 1 Characteristics of Cisco IDS 4215, 4235, 4250, and 4250-XL Sensors

	Cisco IDS 4215	Cisco IDS 4235	Cisco IDS 4250	Cisco IDS 4250-XL
Height	1.7 in. (4.37 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)	1.67 in. (4.24 cm)
Width	16.8 in. (42.72 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)	17.6 in. (44.70 cm)
Depth	11.8 in. (29.97 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)	27.0 in. (68.58 cm)
Weight	11.5 lb (4.11 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)	35 lb (15.88 kg)
Rack-mountable	Yes	Yes	Yes	Yes
Power				
Autoswitching	100V to 240V AC	110-220 VAC	110-220 VAC	110-220 VAC
Frequency	50 to 60 Hz	50-60 Hz	50-60 Hz	50-60 Hz
Operating current	1.5A	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V	2.7A at 115V 1.3A at 220V
Operating environment				
Operating temperature	+5°C to +40°C (+41°F to +104°F)	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)	10 to 35°C (50 to 95°F)
Nonoperating temperature	-25°C to +701/4°C (-13F to +1581/4°F)	-40 to 65°C (-40 to 149°F)	-40 to 65°C (-40 to 149°F)	-40 to 65°C (-40 to 149°F)
Operating relative humidity	5 to 95% (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)	8 to 80% (noncondensing)
Nonoperating relative humidity	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)	5 to 95% (noncondensing)
Heat dissipation (most severe case with full power usage)	410 Btu/hr (full power usage (65W))	983 Btu/hr (maximum)	983 Btu/hr (maximum)	983 Btu/hr (maximum)

Note:

- This 80-Mbps performance for the Cisco IDS 4215 is based on the following conditions:
  - 800 new TCP connections per second
  - 800 HTTP transactions per second

    Average packet size of 445 bytes,

    Running Cisco IDS 4.0 Sensor Software
- This 250-Mbps performance for the Cisco IDS 4235 is based on the following conditions:
  - 3000 new TCP connections per second
  - 3000 HTTP transactions per second
  - Average packet size of 445 bytes

- Running Cisco IDS 4.0 Sensor Software

- This 500-Mbps performance for the Cisco IDS 4250 is based on the following conditions:
  - 5000 new TCP connections per second
  - 5000 HTTP transactions per second
  - Average packet size of 445 bytes
  - Running Cisco IDS 4.1 Sensor Software
- This 1000-Mbps performance for the Cisco IDS 4250-XL is based on the following conditions:
  - 5000 new TCP connections per second
  - 5000 HTTP transactions per second
  - Average packet size of 595 bytes
  - Running Cisco IDS 4.0 Sensor Software

Regulatory Compliance

- EMC—FCC (CFR 47 Part 15) Class A, CISPR 22 Class A, EN 55022 Class A, EN 55024, EN61000-3-2, EN61000-3-3, VCCI Class A, AS/NZS 3548 Class A, CE marking
- Safety UL 60950, CSA 22.2 No.60950, IEC 60950, EN 60950, AS/NZS 3260, CE marking.

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
IDS-4215-K9	Cisco IDS 4215 Sensor (chassis, software, SSH, 2 onboard 10/100BASE-Tx interfaces with RJ-45 connector), 80-Mbps
IDS-4215-4FE-K9	Cisco IDS 4215 Sensor (chassis, software, SSH, 2 onboard 10/100BASE-Tx interfaces with RJ-45 connector plus 4FE interface card), 80-Mbps
IDS-4235-K9	Cisco IDS 4235 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
IDS-4250-TX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 10/100/1000BASE-T with RJ-45 connector)
IDS-4250-SX-K9	Cisco IDS 4250 Sensor (chassis, software, SSH, 1000BASE-SX with SC connector)
IDS-4250-XL-K9	Cisco IDS 4250-XL Sensor (chassis, software, SSH, hardware accelerator, with dual 1000BASE-SX and MTRJ connectors)
IDS-XL-INT=	Cisco IDS Accelerator Card with dual 1000BASE-SX interfaces and MTRJ connectors
IDS-4250-SX-INT=	1000BASE-SX monitoring interface with SC connector
IDS-4FE-INT=	Spare 4FE (10/100 BaseTx) sniffing interfaces for 4215, 4235, & 4250
IDS-PWR=	Spare power supply for the Cisco IDS 4235 and 4250 sensors
IDS-SCSI=	Spare Small Computer Systems Interface (SCSI) hard disk drive for Cisco IDS 4250 Sensor
IDS-RAIL-2=	Two post rail kits for the Cisco IDS 4235 and 4250 sensor platforms
IDS-RAIL-4=	Four post rail kits for the Cisco IDS 4235 and 4250 sensor platforms

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
CON-SNT-IDS4215XK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4215-K9)
CON-SNTE-IDS4215XK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4215-K9)
CON-SNTP-IDS4215XK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4215-K9)
CON-OS-IDS4215XK	Cisco SMARTnet Onsite support 8 x 5 x NBD (Cisco IDS 4215-K9)
CON-OSE-IDS4215XK	Cisco SMARTnet Onsite support 8 x 5 x 4 (Cisco IDS 4215-K9)
CON-OSP-IDS4215XK	Cisco SMARTnet Onsite support 24 x 7 x 4 (Cisco IDS 4215-K9)
CON-SNT-IDS4215-4FEXK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4215-4FE-K9)
CON-SNTE-IDS4215-4FEXK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4215-4FE-K9)
CON-SNTP-IDS4215-4FEXK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4215-4FE-K9)
CON-OS-IDS4215-4FEXK	Cisco SMARTnet Onsite support 8 x 5 x NBD (Cisco IDS 4215-4FE-K9)
CON-OSE-IDS4215-4FEXK	Cisco SMARTnet Onsite support 8 x 5 x 4 (Cisco IDS 4215-4FE-K9)
CON-OSP-IDS4215-4FEXK	Cisco SMARTnet Onsite support 24 x 7 x 4 (Cisco IDS 4215-4FE-K9)
CON-SNT-IDS4235K9	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4235)
CON-SNTE-IDS4235K9	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4235)
CON-SNTP-IDS4235K9	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4235)
CON-OS-IDS4235K9	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4235)
CON-OSE-IDS4235K9	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4235)
CON-OSP-IDS4235K9	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4235)
CON-SNT-IDS4250TK	Cisco SMARTnet support 8 x 5 x NBD (Cisco IDS 4250-TX)
CON-SNTE-IDS4250TK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-TX)
CON-SNTP-IDS4250T	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-TX)
CON-OS-IDS4250TK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-TX)
CON-OSE-IDS4250TK	Cisco SMARTnet onsite support 8 x 5 x 4 Cisco (IDS 4250-TX)
CON-OSP-IDS4250TK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-TX)
CON-SNT-IDS4250SK	Cisco SMARTnet support 8 x 5 x NBD Cisco (IDS 4250-SX)
CON-SNTE-IDS4250SK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-SNTP-IDS4250SK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-SX)
CON-OS-IDS4250SK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-SX)
CON-OSE-IDS4250SK	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4250-SX)
CON-OSP-IDS4250SK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-SX)
CON-SNT-IDS4250XK	Cisco SMARTnet support 8 x 5 x NBD Cisco (IDS 4250-XL)
CON-SNTE-IDS4250XK	Cisco SMARTnet support 8 x 5 x 4 (Cisco IDS 4250-XL)
CON-SNTP-IDS4250XK	Cisco SMARTnet support 24 x 7 x 4 (Cisco IDS 4250-XL)
CON-OS-IDS4250XK	Cisco SMARTnet onsite support 8 x 5 x NBD (Cisco IDS 4250-XL)
CON-OSE-IDS4250XK	Cisco SMARTnet onsite support 8 x 5 x 4 (Cisco IDS 4250-XL)
CON-OSP-IDS4250XK	Cisco SMARTnet onsite support 24 x 7 x 4 (Cisco IDS 4250-XL)

re

Table 2 Ordering Information for the Cisco IDS 4200 Series Sensor

Product number	Product description
CON-SNT-IDS4FE	Cisco SMARTnet support 8 x 5 x NBD (IDS-4FE-INT=)
CON-SNTE-IDS4FE	Cisco SMARTnet support 8 x 5 x 4 (IDS-4FE-INT=)
CON-SNTP-IDS4FE	Cisco SMARTnet support 24 x 7 x 4 (IDS-4FE-INT=)
CON-OS-IDS4FE	Cisco SMARTnet onsite support 8 x 5 x NBD (IDS-4FE-INT=)
CON-OSE-IDS4FE	SMARTnet onsite support 8 x 5 x 4 (IDS-4FE-INT=)
CON-OSP-IDS4FE	SMARTnet onsite support 24 x 7 x 4 (IDS-4FE-INT=)
CON-SNT-IDSXL	Cisco SMARTnet support 8 x 5 x NBD (IDS-XL-INT=)
CON-SNTE-IDSXL	Cisco SMARTnet support 8 x 5 x 4 (IDS-XL-INT=)
CON-SNTP-IDSXL	Cisco SMARTnet support 24 x 7 x 4 (IDS-XL-INT=)
CON-OS-IDSXL	Cisco SMARTnet onsite support 8 x 5 x NBD (IDS-XL-INT=)
CON-OSE-IDSXL	SMARTnet onsite support 8 x 5 x 4 (IDS-XL-INT=)
CON-OSP-IDSXL	SMARTnet onsite support 24 x 7 x 4 (IDS-XL-INT=)

Export Considerations

The Cisco IDS 4200 Series sensors are subject to export controls. Refer to the export compliance Web site for guidance at: http://www.cisco.com/wwl/export/crypto/.

For specific export questions, contact export@cisco.com.

Additional Information

For more information about the Cisco Intrusion Protection System, go to: http://www.cisco.com/go/ids

For more information about the CiscoWorks VMS Solutions (IDS management), go to: http://www.cisco.com/go/vms

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

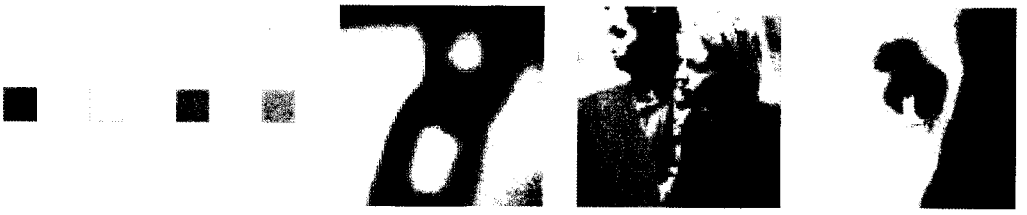
Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

RD/LW4599 0503

Check Point
SOFTWARE TECHNOLOGIES LTD

We Secure the Internet.



Check Point InterSpect

The Internal Security Gateway™

PRODUCT FEATURES:

- Intelligent Worm Defender
- Network Zone Segmentation
- Quarantine of Suspicious Computers
- LAN Protocol Protection
- Pre-emptive Attack Protection

PRODUCT BENEFITS:

- Blocks the spread of worms and attacks inside the network
- Segments the network into organizational security zones
- Isolates attacks and compromised devices
- Provides the deepest and most comprehensive support for Microsoft and other LAN Protocols
- Provides proactive defenses against vulnerabilities before they are exploited

Intelligent Security

YOUR CHALLENGE

To date, IT security organizations have focused on the network perimeter. However, many of today's attacks are introduced from inside the network. Laptops, PDAs and other devices travel into and out of the network daily, making it possible for legitimate users to infect the network or unwittingly grant attackers access to the network via a Trojan horse or other spyware.

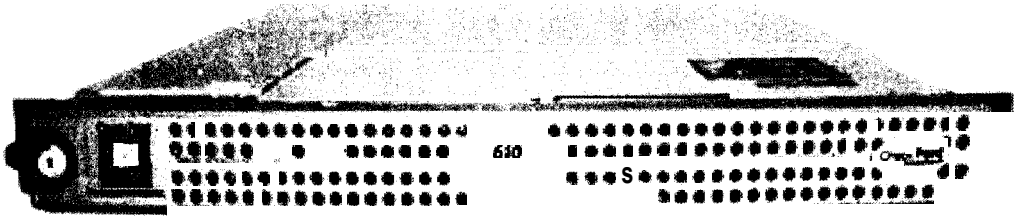
For example, many worms have propagated inside the network after being introduced by an internal source. Once a single network device has been infected, the entire network can be compromised very quickly. Fast-spreading worms, often called "flash" or "blitz" worms, can spread worldwide in a matter of minutes!

With such costly threats becoming increasingly common, organizations have come to realize that they must provide better defenses against worms, unauthorized access threats and other attacks within their internal network.

OUR SOLUTION

Check Point InterSpect™ is an internal security gateway that blocks the spread of worms and attacks inside the network and provides network zone segmentation. Based on Check Point's proven security technologies: INSPECT™, Stateful Inspection and Application Intelligence™, and SMART (Security Management Architecture), InterSpect is built specifically for internal network security. InterSpect provides:

- Intelligent Worm Defender™
  - Blocks the spread of worms and attacks inside the network
- Network Zone Segmentation
  - Segments the internal network into organizational security zones
- Quarantine of Suspicious Computers
  - Isolates attacks and compromised devices
- LAN Protocol Protection
  - Provides the deepest and most comprehensive support for Microsoft and other LAN protocols
- Pre-emptive Attack Protection
  - Provides proactive defenses against vulnerabilities and attacks before they are exploited



InterSpect is designed for flexible and non-disruptive deployment into existing network environments and includes a management interface tailored specifically for internal security.

FEATURES

Intelligent Worm Defender

The Intelligent Worm Defender provides the most powerful internal network worm protection by applying Check Point Stateful Inspection and Application Intelligence technologies. These technologies are based on INSPECT, which provides the most comprehensive and adaptive protection available. InterSpect is installed between protected network zones and prevents the spread of worms inside the network by inspecting the traffic from connected devices and blocking dangerous traffic.

Network Zone Segmentation

InterSpect segments the network into multiple administrator-defined security zones to prevent unauthorized access between zones. This prevents users or compromised computers on the network from accessing information and systems they are not authorized to view. Network zone segmentation also contains attacks within a sub-segment of the network.

Quarantine

InterSpect can identify suspicious or infected computers on the network and quarantine them, preventing the rest of the network from being compromised. InterSpect also allows the quarantine of computers during security patch deployment. This helps ease the risk of infection while network administrators identify, install and test patches.

InterSpect also has a unique user notification capability for quarantine. When a user's computer is quarantined, typically because the computer has been identified as infected, the user is notified via a customized dynamic web page. This notification helps to minimize the time spent troubleshooting the issue at the help desk, and also allows the network administrator to be made aware of the issue, reducing user downtime.

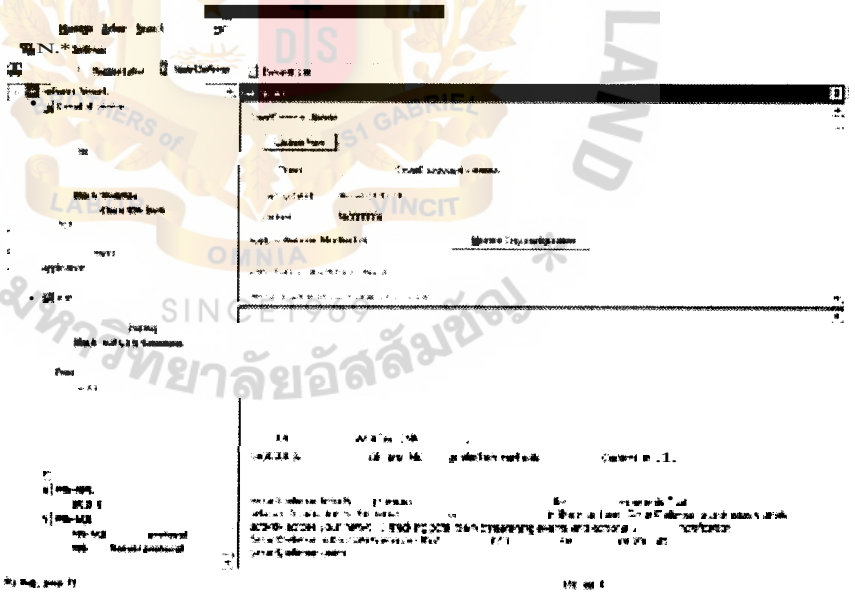
LAN Protocol Protection

InterSpect provides the deepest and most comprehensive protection for Microsoft protocols such as MS RPC, CIFS, MS SQL, and DOOM, as well as other LAN protocols such as Sun RPC, DCE RPC, and HTTP. InterSpect uses INSPECT technology to provide the industry's most adaptive security inspection capability. By taking advantage of INSPECT updates, available via SmartDefense™ subscription, InterSpect users can keep their internal security infrastructure up-to-date as new attacks and threats emerge.

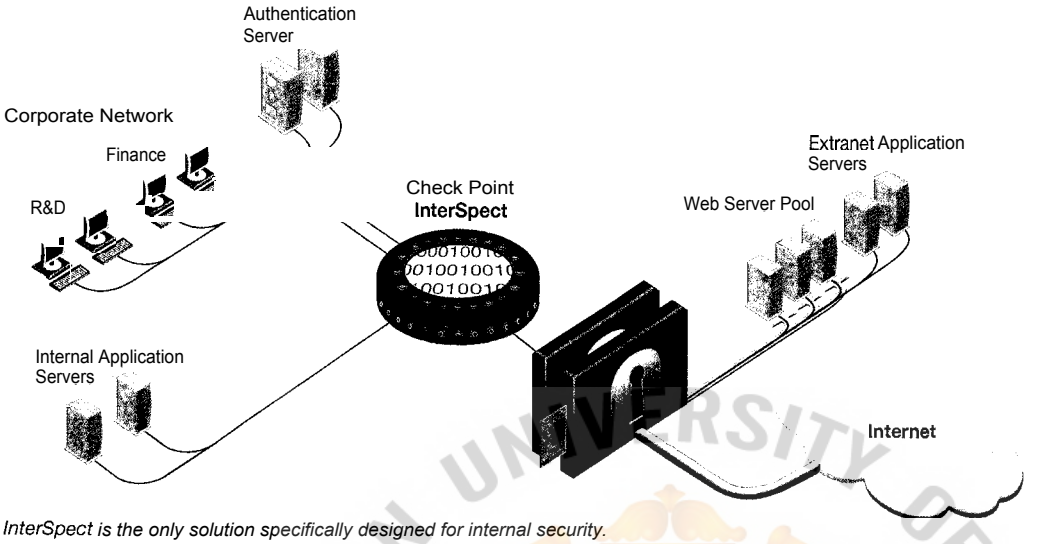
Pre-emptive Attack Protection

InterSpect provides proactive and dynamic protection for known and unknown attacks, enabling organizations to defend against vulnerabilities before they are exploited.

InterSpect includes a version of SmartDefense customized for internal network security that allows administrators to configure, enforce, and update all network and application attack defenses using Stateful Inspection and Application Intelligence, which are based on INSPECT, the industry's most intelligent and adaptive security inspection technology.



InterSpect includes SmartDefense for internal networks, providing pre-emptive protection for known and unknown attacks inside the network.

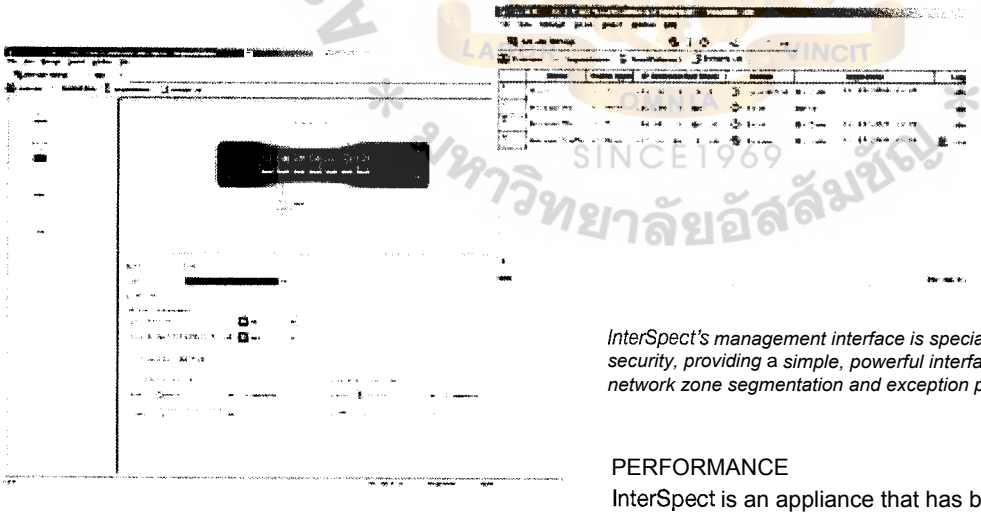


InterSpect is the only solution specifically designed for internal security.

Management Tailored for Internal Security

Managing InterSpect is made easy by using a management interface designed specifically for internal security. Based on SMART, this interface provides a powerful, easy-to-use interface to address the configuration and policy management issues unique to internal security.

Typically, network-level firewalls are configured to drop all traffic unless explicitly allowed. This can be quite complex to configure for internal deployments. But with Check Point, security segmentation is as simple as installing InterSpect into your network and defining your network security zones. InterSpect immediately begins inspecting traffic and dropping malicious content while allowing all common LAN traffic. Administrators can then explicitly disallow specific traffic patterns as well as configure internal security zones with an easy-to-use interface.



InterSpect's management interface is specialized for internal security, providing a simple, powerful interface for configuring network zone segmentation and exception policies.

PERFORMANCE

InterSpect is an appliance that has been designed to meet the performance demands of internal security. InterSpect is based on SecurePlatform, Check Point's hardened security operating system. To ensure the highest level of performance, InterSpect also includes Check Point's patented SecureXL™ security acceleration technology.

DEPLOYMENT MODES

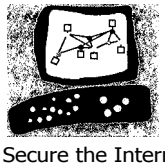
To support various deployments, InterSpect can work in three in-line operating modes (bridge, switch, and router mode). Monitor-only capability can be used with all modes.

Description	Primary Deployment Scenarios
Bridge mode InterSpect bridges one or more segments to the backbone and is invisible to the IP network	Transparent deployment of segmentation, worm defense and quarantine
Switch mode InterSpect acts as a multi-port bridge in which all ports are bridged together to make one zone	Transparent deployment of worm defense and quarantine when full segmentation is not required
Router mode InterSpect acts as a router, every active port is configured with a different IP address	Sophisticated network zone segmentation for multiple security zones
Monitor-only capability InterSpect inspects traffic without enforcing safeguards and defenses (Can be used with Bridge, Switch, or Router Modes)	Pilot deployments to understand InterSpect's effect on legacy applications prior to active, in-line deployment

SPECIFICATIONS

	InterSpect 210	InterSpect 410	InterSpect 610	InterSpect 610F
Target	One workgroup protection	Multiple workgroup protection	Gigabit network protection	Gigabit network protection
Operating Environment	Check Point SecurePlatform	Check Point SecurePlatform	Check Point SecurePlatform	Check Point SecurePlatform
Throughput	200 Mbps	500 Mbps	1000 Mbps	1000 Mbps
Fiber interfaces	N/A	Add-on available	Add-on available	Included
Expansions Slots	N/A	1	1	1
Inspection Ports	2	3-10	3-10	3-10
Management Port	1	1	1	1
Max ports	3	10	10	10
Interface speed	10/100 Mbps	10/100/1000 Mbps	10/100/1000 Mbps	10/100/1000 Mbps
VLAN Support	8 VLANs	128 VLANs	Unlimited VLANs	Unlimited VLANs
Redundant Power	No	Optional	Included	Included
SmartDefense Subscription	Included for 1st year	Included for 1st year	Included for 1st year	Included for 1st year
Width	16.7"/42.5 cm	17.61"/44.7 cm	17.61"/44.7 cm	17.61"/44.7 cm
Height	1.68"/4.2 cm (1U)	1.68"/4.2 cm (1U)	1.68"/4.2 cm (1U)	1.68"/4.2 cm (1U)
Depth	21.9"/55.5 cm	27"/68.3 cm	27"/68.3 cm	27"/68.3 cm
Weight	27 lbs/12.25 kg	35 lbs/15.9 kg	35 lbs/15.9 kg	35 lbs/15.9 kg
Power	100-220 Volts 50/60 Hz	100-220 Volts 50/60 Hz	100-220 Volts 50/60 Hz	100-220 Volts 50/60 Hz

Check Point'
SOFTWARE TECHNOLOGIES LTD.

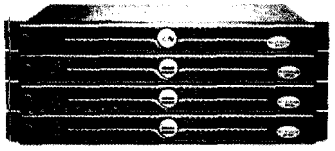


We Secure the Internet.

P/N 501210

Juniper NETWORKS

Juniper Networks **NetScreen-IDP 10/100/500/1000**



The Juniper Networks **NetScreen** Intrusion Detection and Prevention **(NetScreen-IDP)** integrates application and network visibility with incident investigation and **remediation** to help customers quickly and confidently deploy **inline** attack prevention. When deployed **inline**, **NetScreen-IDP** effectively identifies and stops network and application level attacks before they inflict any damages, minimizing the time and costs associated with intrusions. **NetScreen-IDP** not only helps protect your network against attacks, it provides you with information on rogue servers and applications that may have been added to the network without your knowledge. Armed with the knowledge that unauthorized applications such as peer-to-peer or instant messaging have been added to the network allows you to more easily enforce your security policy and maintain compliance with your corporate application use policy. Combined with a centralized, rule-based management approach, which offers granular control over the system's behavior and easy access to extensive logging and fully customizable reporting, it is easy to see why **NetScreen-IDP** is the best way to keep your critical information assets safe.

		orks /500/1000
Management Capabilities		
3 Tier System		Yes
User Interface Platforms	Windows	Yes
	Linux	Yes
Management Server latforms	Linux RedHat 7/8 RedHat Enterprise Server 3 Solaris 7/8	Yes Yes
ser Interface Mechanisms	Java Application Command Line Interface	Yes Yes
Number of Users		Unlimited
Centralized Management	Policy Management Log Viewing Incident Management	Yes Yes Yes
Logging		Over 50,000 logs per second
Log Exporting		PostgresSQL Database XMLFile CSVFile
Signature Updates		Yes; signature updates provided weekly
Reporting		
Quick reports		Yes
Fully customizable reports		Yes
Exportable (HTML)		Yes
System Status Monitoring		Yes
Sensor Software		
Detection Methods (8 methods)	Stateful Signature Detection	Yes
	Protocol Anomaly Detection	Yes
	Backdoor Detection	Yes
	Traffic Anomaly Detection	Yes
	IP Spoofing Detection	Yes
	DoS Detection	Yes
	Layer 2 Detection	Yes
	Network Honeypot	Yes

		Juniper Networks •1.0/ 10/500/t 00
Signatures	Stateful	Yes
	Number of contexts supported	500 +
	Compound (Stateful plus protocol anomaly)	Yes
	Open signature format	Yes
	Custom, user definable	Yes
	Parallel signature matching	Yes
Protocols supported		60
Traffic Interpretation	Reassembly	Yes
	Scrubbing	Yes
	Normalization	Yes
Active Responses	Drop Packet	Yes
	Drop Connection	Yes
Passive Responses	TCP Resets	Yes
	Close Client	Yes
	Close Server	Yes
	Close Connection	Yes
	IP Actions	Yes
Notification Methods	Built-in Log Viewer	Yes
	SMTP(Email)	Yes
	Custom Script	Yes
	SNMP trap	Yes
	SYSLOG	Yes
Packet Management	User-specified logging	Yes
	Built-in packet viewer	Yes
	3rd party compatibility	Yes
Operational Modes	Bridge	Yes
	Router	Yes
	Proxy-ARP	Yes
	Transparent	Yes
	Sniffer (Passive)	Yes
Enterprise Networking	802.1QVLAN Support	Yes
	SNMPMIB-II Support	Yes
Network Forensics/ Incident Response	Application (L7) information/awareness	Yes
	Network (L2-L4) information/awareness	Yes
	Policy violation visibility/awareness	Yes
	Incident correlation	Yes
	Policy refinement	Yes
	TruSecure incident remediation	Yes

Intrusion Detection and Prevention

Juniper Networks NetScreen-IDP 10/100/500/1000

Sensor Hardware	Juniper Networks NetScreen-IDP 10	Juniper Networks • I P 100	works P	Juniper Networks NetSc [illegible]	Juniper Networks NetScreen-IDP Bypass
Interfaces	2 Copper Gigabit and 1 10/100 Standard	2 Copper Gigabit and 2 10/100 Standard(1)	2 Copper Gigabit and 2 Fiber Gigabit Standard(2)	2 Copper Gigabit and 2 Fiber Gigabit Standard'	
Memory (RAM)	512 mb	1 Gb	4 Gb	4 Gb	
Maximum Session	10,000	70,000	220,000	500,000	
hroughput	Up to 20 mb/Sec Nominal(5)	Up to 200 mb /Sec	Up to 500 mb/Sec	Up to I Gb/Sec(4)	
igh Availability					
Standalone Failover	No	Yes	Yes	Yes	
HA Clustering	No	Yes	Yes	Yes	
Load Sharing	No	Yes	Yes	Yes	
3rd Party Failover	No	Yes	Yes	Yes	
Fail-Open	Yes'	Yes"	No	No	
Physical Redundancy					
Redundant Power	No	Optional	Yes	Yes•	
RAID	No	Optional	Yes	Yes	
Physical					
AC Power Wattage	230 Watts	275 Watts	275 Watts	325 Watts	12 Watts
AC Power Voltage	100/240 VAC, 2.0-1.0 A, 50/60 Hz	100/240 VAC, 3.9-2.0 A, 50/60 Hz	100/240 VAC, 3.9-2.0 A, 50/60 Hz	110/220 Volts	90-264 VAC
System Battery	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell	CR2032 3V lithium coin cell	3V coin cell	
Operating Temp	50° to 95°F	50° to 95°F	50° to 95°F	50° to 95°F	
Storage Temp	-40° to 149°F	-40° to 149°F	-40° to 149°F	-40° to 149°F	
Relative Humidity (Operating)	8% to 80% noncondensing	8% to 85% noncondensing	8% to 85% noncondensing	8% to 80% noncondensing	
Relative Humidity (Storage)	5% to 95% noncondensing	5% to 95% noncondensing	5% to 95% noncondensing	5% to 95% noncondensing	
Altitude (Operating)	-50 to 10,000 ft	-50 to 10,000 ft	-50 to 10,000 ft	-50 to 10,000 ft	
Altitude (Storage)	-50 to 35,000 ft	-50 to 35,000 ft	-50 to 35,000 ft	-50 to 35,000 ft	
Weight	27 lbs	35.27 lbs	35.27 lbs	35 lbs	1.5 lbs
Height	1.69 in. 1U	1.69 in. 1U	1.69 in. 1U	1.67 in. 1U	1.35 in.
Width	16.7 in.	19 in.	19 in.	17.61 in.	8 in.
Depth	23.1 in.	26.9 in.	26.9 in.	27 in.	5 in.

) Each 10/100 interface may be replaceable with an optional quad 10/100/1000 interface card (at extra cost). In total, the 2 standard 10/100 interfaces may be replaced with 8 10/100/1000 interfaces.
) Each Fiber Gigabit interface (Base-SX) may be replaceable with an optional quad 10/100/1000 interface card (at extra cost). In total, the 2 standard Fiber Gigabit (Base-SX) cards may be replaced with 8 10/100/1000 interfaces. Note: the Fiber Gigabit cards are for multimode (Base-SX) SC connectors only. If single mode is needed the user will need an external converter.
) The IDP-10 supports 20 MB/Sec of continuous throughput. however it can handle bursts at full line-speed.
ill As rested with 101' 3.0 software.
(11 Requires NetScreen-IDP Bypass unit, which is purchased separately.

Management server
IDP Management software runs on either Solaris 7/8 or Linux RedHat 7.2/8 or RedHat Enterprise Server 3. Recommended processor: 1GHZ (Linux), 400 MHZ (Solaris). Recommended capacities: 1GB RAM and 18 GB hard disk (minimums).

Management GUI client application
The client application is a Java-based application that runs on Windows2000, NT, XP and Linux RedHat 8 or RedHat Enterprise Server 3. JRE version 1.4.1 is included. Disk Requirements: 128 MBRAM Requirements: 256 MB (IDP 2.1), 512 MB (IDP 3.0)

Product	Part Number
NetScreen-IDP 10 Intrusion Detection and Prevention Appliance	NS-IDP-10
NetScreen-IDP 100 Intrusion Detection and Prevention Appliance	NS-IDP-100-002
NetScreen-IDP 500 Intrusion Detection and Prevention Appliance	NS-IDP-500-002
NetScreen-IDP 1000 Intrusion Detection and Prevention Appliance	NS-IDP-1000
Accessories	
NetScreen-IDP Bypass Fail-Open Device (IDP-10 and IDP-100 only)	NS-IDP-BYP
NetScreen-IDP Fiber Gigabit NICs (set of 2 Cards)*	NS-IDP-GB
NetScreen-IDP Quad 10/100/1000 NIC**	NS-IDP-QUAD-NIC
NetScreen-IDP Redundant Hard Drive (IDP 100 only)	NS-IDP-HD-002
NetScreen-IDP AC Power Supply (IDP 100 only)	NS-IDP-PWR-AC-002
NetScreen-IDP Rapid Rail Kit	NS-IDP-RCK-01
NetScreen-IDP Chatsworth Rail Kit	NS-IDP-RCK-02

*For NetScreen-IDP 100 only
**For NetScreen-IDP 100/500/1000 only

Juniper NETWORKS
1194 North Mathilda Avenue Sunnyvale, CA 94089 USA
Phone: 888-JUNIPER (888-586-4737) or 408-745-2000
Fax: 408-745-2100

Part Number 110010-001 Apr 2004

Proventia™ A Series

Built on the world's leading security intelligence and technologies, Internet Security Systems' Proventia™ A Series intrusion detection appliances reduce costs through simplified deployment, streamlined management and maximized protection.

Proventia A Series appliances, along with all Internet Security Systems' network, server and desktop protection agents, can be centrally-managed with SiteProtector™, a single security management platform. Ongoing X-Force™ security research results in X-Press Update™ enhancements to provide the most up-to-date protection against known and unknown attacks.

Proventia A Series models are available to meet a range of needs, including complete threat protection and full coverage from 200 Mbps to 1000 Mbps on one to four network segments.

The Proventia A Series Advantage

Integrated Protection Appliance
- Acquisition and 24/7 support from one security vendor
- Available for immediate deployment
- Get up and running quickly with minimal tuning and easy configuration for known and previously unknown attacks with unprecedented accuracy

Based on **RealSecure®** Technologies
- Unified protocol analysis and pattern matching that works even at high speeds
- Based on the same industry-proven technologies that have earned RealSecure Network Protection the top market position

Analyzes 100 network protocols catching even unknown attacks

Firewall Monitor

Protects against malicious network traffic that successfully passes through firewalls
- Offers essential added layers of protection

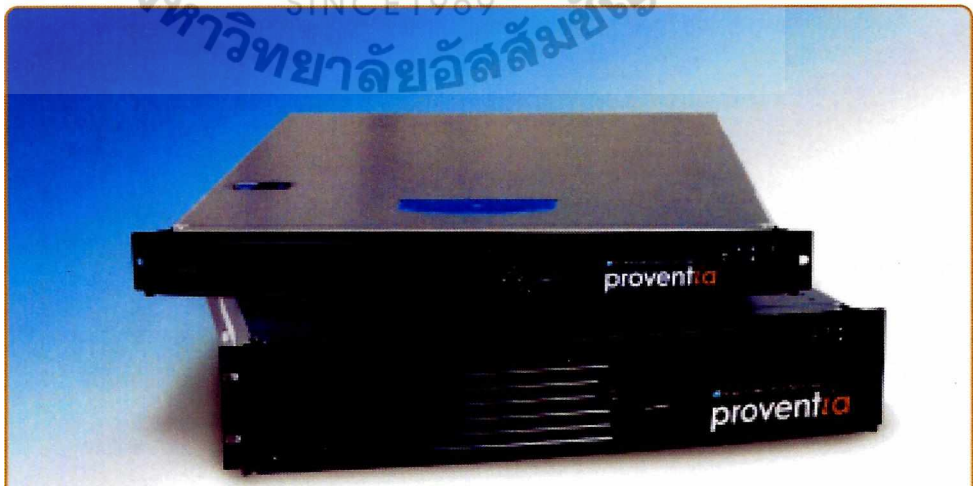
Centralized Management
- Simple, remote, centralized management with SiteProtector and the SiteProtector SecurityFusion™ module

Control, monitor and analyze with a minimum of staff and operational costs
- Advanced data correlation, impact analysis and attack pattern recognition

Optional Managed Protection Services

24/7 monitoring for security incidents
- Allows focus on core business instead of security
- Customer control of policy and online access to security events

Benefits
- Protection that reduces risk exposure - Essential complement to firewalls to increase success in ongoing business operations
- **Simplicity** that lowers cost - Simplifies deployment, streamlines management and reduces costs
- Optimized for enterprise networks - Maximum protection to meet a variety of enterprise needs



INTERNET SECURITY , SYSTEMS®

Proventia™ Intrusion Prevention Appliances

Internet Security Systems' (ISS) ***Proventia™ intrusion prevention appliances*** automatically block malicious attacks before they impact your organization, preserving network availability, reducing the burden on IT resources and preventing security breaches. Proventia intrusion prevention appliances sit inline on the network or at the gateway blocking intrusions, denial of service attacks, backdoors and hybrid threats that can paralyze an enterprise.

The Proventia appliances complement other Internet Security Systems network, server and desktop protection offerings, and are centrally administered through the SiteProtector™ management platform, eliminating the need for active administrator involvement. Ongoing **X-Force®** security research and development results in first-to-market **X-Press Update™** enhancements to provide the most current protection against known and unknown threats. ISS is the foremost provider of intrusion detection and prevention and the only company that preemptively protected against all of the last five major Internet worms - Sasser, MS Blaster, SQL Slammer, Nimda and Code Red.

The Proventia Advantage

Dynamic Blocking

- Enables an immediate and reliable blocking response to unwanted traffic
- Includes more than 225 default rules out-of-the-box that prevent the propagation of hybrid threats, such as Sasser, MS Blaster, SQL Slammer, Nimda and Code Red
- Allows legitimate traffic to pass unhindered without impacting network performance
- Immediately protects against known and unknown attacks without having to apply unscheduled manual patch updates or hotfixes

Proven Prevention Without False Positives

- Deep protocol analysis capabilities provide accurate and high-performance protection against known and unknown attacks.
  Analyzes more than 100 network protocols and includes more than 2,500 unique checks.
  The technology employed in Proventia intrusion prevention appliances earned the NSS Approved award in the NSS Group IPS Group Test (Edition 1). The Proventia G200 demonstrated 100 percent attack detection and blocking, 100 percent out-of-the-box resistance to false positives and 100 percent resistance to evasion techniques.[1]

Centralized Management with SiteProtector

- Control, monitor and analyze with minimum staff and operational costs
- Scales easily from small organizations to large, global enterprises
- Advanced data correlation, impact analysis and attack pattern recognition with the **SiteProtector SecurityFusion™** module

Flexible Deployment Options

- Up to four network segments monitored inline with single appliance (Proventia G1200 models)
- Out-of-the-box protection with minimal tuning and simple configuration to get up and running quickly
- Easily switches between detection and prevention without disrupting or blocking legitimate network traffic
- Three modes of operation include: Active (inline, blocking), Passive (offline, no blocking) Simulation (inline, no blocking)
- Native support for asymmetrically routed networks (Proventia G1200 models)

1 See www.nss.co.uk for the full report of more than 750 tests

NSS approved

Proventia G200
NSS Group, January 2004

Performance & Benefits:

Block known and *unknown* attacks before they do damage

X-Force **R&D** delivers immediate automatic updates

wer cost of ownership

tomated management

network protection | server protection | desktop protection | enterprise management

work protection server protection desktop protection enterprise management

	ISS Proventia A201	ISS Proventia A604	ISS Proventia A604-200	ISS Proventia A1204	ISS Proventia A1204F	ISS Proventia A1204F-400
Form Factor						
Appliance	1U	1U	1U	2U	2U	2U
Rack-mountable	X	X	X	X	X	
One-stop acquisition	X	X	X	X	X	
Plug and protect deployment	X	X	X	X		
Redundant power supply	----			X		
Redundant local storage						
Network Support						
1000BASE-T (gigabit copper - IEEE 802.3ab)						
1000-SX (gigabit fiber - IEEE 802.3z)						
Load-balanced networks		X				
Port aggregation (for asymmetric routing, etc.)		X	X	X		
Native full duplex support		X	X	X		
Protection Capacity						
Maximum segments protected per unit	1	4	4	4	4	4
Full coverage performance	200 mbps	600 mbps	200 mbps	1200 mbps	1200mbps	400mbps
Stealth mode operation						X
Based on *RealSecure* Technologies						
Embedded X-Force security knowledge	X	X	X			
Immune to IDS evasion techniques	X	X	X			
Full 7-layer, stateful protocol decoding and analysis	X	X	X	X	X	X
Fully analyzes at least 100 network and application layer protocols	X	X	X	X	X	X
Detects over 1700 known threats	X	X	X	X	X	X
Detects unknown threats	X					
Integrated with desktop, server and network protection						
SiteProtector Management						
Remote central management	X	X	X	X	X	X
Event aggregation, consolidation, filtering and analysis	X	X	X	X	X	X
Impact analysis	X	X	X	X	X	X
IDS/VA/OS correlation	X	X	X	X	X	X
Incident tracking	X	X	X	X	X	X
Attack pattern recognition	X	X	X	X	X	X
Custom reports, exportable to HTML, Word and RTF	X	X	X	X	X	X
Support						
Optional 24/7 Managed Protection Services	X	X	X	X	X	X
24/7 ISS Technical Support	X	X	X	X	X	
Advanced exchange for appliance replacement	X	X	X	X	X	
Automated security content and software updates	X	X	X	X	X	

6303 Barfield Road • Atlanta, GA 30328 • Tel: +1.404.236.2600 • Fax: +1.404.236.2626 • www.iss.net • MC-PROVA-DS-DOC

Performance and Reliability

Protects at wire speed without consuming network bandwidth or disrupting network availability

Allows traffic to pass in the event of power loss or other failure

Premium quality systems based on Intel server architecture that includes:

- Redundant internal cooling fans
- RAID (redundant) storage to prevent fatal hardware failures
- Hot swappable power supplies

Layer Two (bridge-mode) Intrusion Prevention

- Invisible to the monitored network and determined attackers
- Separate out-of-band management interface

Managed Protection Services (MPS)

- Guaranteed, performance-based Service Level Agreements (SLAs)
- Performance-based reporting
- Managed Service Customer Portal
- Bundled services (MPS Premium Service Only)

Proventia Intrusion Prevention Appliance Specification Details

Specifications Common To All Models	
Form Factor	2U (G100 and G200 = 1U)
Management Interface	One (1) 10/100/1000 **Mbps** Copper
Dedicated Kill Interface (passive mode only)	One (1) 10/100/1000 **Mbps** Copper
Inline Segment(s)	One (1) (G1200 models = 4 segments)
Bypass on failure	Yes (**G1000F**, **G1200F** and fiber segments of **G1200CF** require external bypass unit)
Centralized Management	Yes, **SiteProtector**
Redundant Storage	Yes
Redundant Power Supply	Yes (not G100 and G200)
Operating System	**Proventia** OS
Enclosure	Fits 19" rack
Serial Ports	One (1)
Lockable front bezel	Yes
Operating Temperature	10C to 35C (50F to 95F)
Non-Operating Temperature	-40C to 70C (-40F to 158F); relative humidity 95%; non-condensing at 30C
Emissions	FCC Class A

Model-Specific Details	Performance	Monitoring Interfaces	AC Power
G100	100 **Mbps**	Two (2) 10/100 **Mbps** Copper	100-127V (50-60Hz) 2 Amps
G200	200 **Mbps**	Two (2) 10/100/1000 **Mbps** Copper	200-240V (50-60 Hz) 2 Amps
G1000-400	400 **Mbps**	Two (2) 10/100/1000 **Mbps** Copper	
G1000F-400	400 **Mbps**	Two (2) 1000 **Mbps SX** Fiber (LC)	
G1200-400	400 **Mbps**	Eight (8) 10/100/1000 **Mbps** Copper	
G1200CF-400	400 **Mbps**	Four (4) 10/100/1000 **Mbps** Copper; Four (4) 1000 **Mbps SX** Fiber (LC)	100-127 V (50 - 60 Hz) 5.2 Amps 200-240 V (50 - 60 Hz) 2.6 Amps
G1200F-400	400 **Mbps**	Eight (8) 1000 **Mbps SX** Fiber (LC)	
G1000	1000 **Mbps**	Two (2) 10/100/1000 **Mbps** Copper	
G1000F	1000 **Mbps**	Two (2) 1000 **Mbps SX** Fiber (LC)	
G1200	1200 **Mbps**	Eight (8) 10/100/1000 **Mbps** Copper (50 - 60 Hz)	
G1200CF	1200 **Mbps**	Four (4) 10/100/1000 **Mbps** Copper; Four (4) 1000 **Mbps SX** Fiber (LC)	
G1200F	1200 **Mbps**	Eight (8) 1000 **Mbps SX** Fiber (LC)	

Get Started Today

To get started securing your information, contact an ISS security consultant at 800-776-2362 in the U.S. or +1 (404) 236-2600 outside the U.S., or visit the Internet Security Systems Web Site at http://www.iss.net.

About Internet Security Systems (ISS)

Internet Security Systems, Inc. (ISS) is the trusted expert to global enterprises and world governments providing products and services that protect against Internet threats. An established world leader in security since 1994, ISS delivers proven cost efficiencies and reduces regulatory and business risk across the enterprise for more than 11,000 customers worldwide. ISS products and services are based on the proactive security intelligence conducted by ISS' X-Force research and development team - the unequivocal world authority in vulnerability and threat research. Headquartered in Atlanta, Internet Security Systems has additional operations throughout the Americas, Asia, Australia, Europe and the Middle East. For more information, visit the Internet Security Systems Web site at www.iss.net or call 800-776-2362.

6303 Barfield Road • Atlanta, GA 30328 • Tel: +1.800.776.2362 • Fax: +1.404.236.2626 • www.iss.net • MC-DS-PROVG-504

RealSecure® Server Sensor

Every organization relies on servers to run applications and host data to drive their business. Any disruption of service can result in customer dissatisfaction, lost revenue and increased costs. New vulnerabilities, or exploits of existing vulnerabilities, put your systems at risk for intrusion and constantly threaten the vital operations of these key systems. Securing server environments, while enabling them to keep applications running, continues to be a challenge.

The Solution

RealSecure® Server Sensor protects servers from the growing threat spectrum while enabling them to keep data and applications reliable, available and confidential. This centrally-managed enterprise protection agent combines a proven intrusion prevention system with powerful firewall capabilities to protect servers. Real-time monitoring and analysis of the operating system, applications and network activity guard server environments from misuse and intrusions with little to no impact on the performance of the system.

Features & Benefits

RealSecure Server Sensor provides automated, real-time intrusion detection and protection by analyzing events, operating system logs and inbound/outbound network traffic on enterprise servers, blocking malicious activity from damaging critical assets. Utilizing the ISS Protocol Analysis Module (PAM), Server Sensor applies a combination of sophisticated protocol analysis with behavioral pattern sets and automated event correlation. This dramatically reduces security costs and downtime by preventing both known and unknown attacks.

Web Application Protection – Server Sensor protects Web applications by inspecting traffic for malicious activity and is capable of adding an additional level of protection to those applications running on both Apache and IIS Web servers by inspecting Secure Sockets Layer (SSL) encrypted traffic.

Benefits

Provides increased protection against complex Internet threats such as Nimda and Code Red

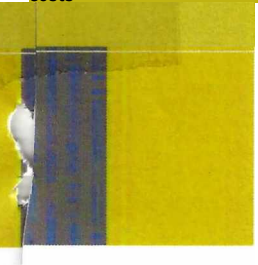
Safeguards confidential data from loss or theft

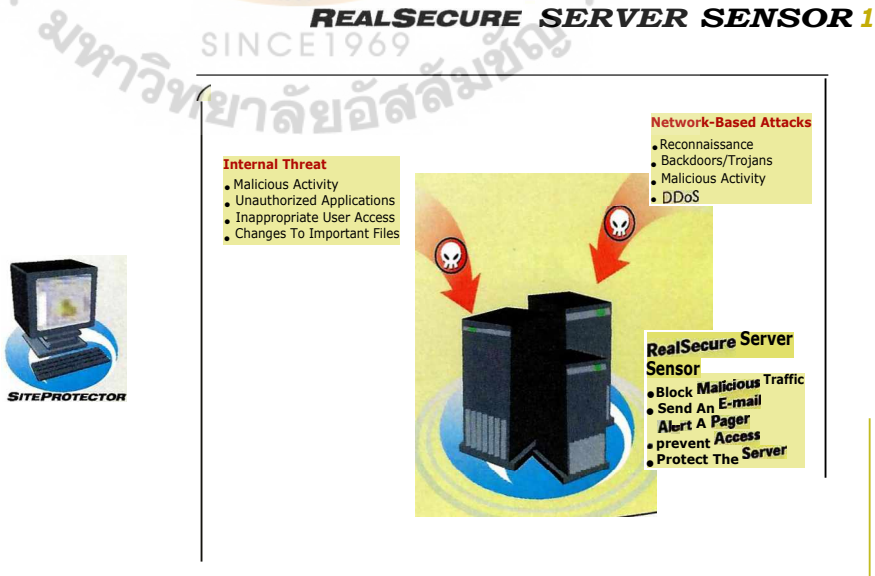
Allows you to enforce security according to policy

Prevents both console and network-based attacks

Maximizing system uptime

Reduces security related costs





Advanced Intrusion Prevention/Blocking – Monitors all inbound and outbound traffic to detect and prevent attacks, both known and unknown. This includes buffer overflows, Trojans, brute force attacks, unauthorized access and network worms, along with many other types of attacks.

Local and Network-Based Protection – Provides the flexibility to detect and protect from both local and network attacks through log monitoring capabilities. This prevents authorized users from attacking the system, while also preventing brute force attacks and unauthorized access to system resources that would otherwise compromise data confidentiality, integrity and accessibility.

Audit Policy Management – Centralized management of an OS audit policy ensures that all critical servers have a consistent and effective audit policy that allows for the management of true kernel-level auditing.

Centralized Management – Server Sensor is incorporated into Internet Security Systems' SiteProtector™ central management application. This management console unifies the administration of enterprise protection across gateways, networks, servers and desktops, significantly reducing demands on staff and other operational resources.

SiteProtector™ SecurityFusion™ Module – This plug-in module for SiteProtector uses built-in X-Force® security knowledge to dynamically escalate threatening security incidents while reducing false alarms. The module instantly correlates security data from multiple sources to escalate serious threats, such as an attack on a vulnerable asset or a covert, multi-step attack.

Backed by the X-Force® – Internet Security Systems' X-Force® organization is a leading group of security experts dedicated to proactive counter-intelligence and public education against online threats. X-Force researches security issues, tracks the evolution of threats through ISS' Global Threat Operations Center, and ensures that ISS is the first to bring new threat management solutions to market. With more than 250 years of combined experience, the X-Force organization possesses a wide range of expertise in security management strategies and tactics. This deep understanding of distributed computing, global networking, programming and forensics keeps the X-Force at the forefront for combating the latest developments in online security.

System Requirements

Operating Systems Supported

- Microsoft Windows Server 2003
- Microsoft Windows 2000
- Microsoft Windows NT 4.0
- Sun Solaris
- RedHat Linux
- IBM AIX
- Hewlett-Packard HP-UX

Refer to the *System Requirements* document for additional details on platforms supported.

Microsoft Windows Server 2003 and Windows 2000 Server Certified

RealSecure Server Sensor is certified on the following platforms by VeriTest, the authorized worldwide lab to test enterprise applications for Microsoft's "Certified for Windows" program:

- *Windows Server 2003 Standard Edition*
- *Windows Server 2003 Enterprise Edition*
- *Windows Server 2003 Datacenter Edition*
- *Windows 2000 Server*
- *Windows 2000 Advanced Server*
- *Windows 2000 Datacenter Server*

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.

The full Certification Report from VeriTest is available at: *http://cert.veritest.com/CfWreports/server/SearchResults.asp?co=1391&lo=0&bs=Search&pr=0&pc=0*

Doc. Rev 3.2

6303 Barfield Road • Atlanta, GA 30328 • Tel: +1.404.236.2600 • Fax: +1.404.236.2626 • www.iss.net • MC-SERSEN-DS-DOC