IDS and it's New Features (IPS)

Felipe Signoretti Bueno de Almeida

GSEC Practical Assignment Version 1.4b Option 1

September 25, 2003

Abstract

This paper will give the reader general information about a Intrusion detection and intrusion prevention systems. It provides an explanation about the architecture of the systems and how it work, the places were Intrusion detection system should be placed, and what you need to know about them to monitor and prevent attacks. Shows the advantages and disadvantages of different types of IDS[1] as well as IPS[2], and compare both solutions.

Introduction

With the growing of the internet organizations need a complete solution to implement security scenarios, many people say that the first thing that should be done regarding security is placing a firewall to protect your entire network, but many techniques can be used to bypass a firewall, so for a complete solution in security network it is necessary to implement a good security policy to protect your network, therefore one security policy must be complaint with a good solution to protect your internal DMZ network and your critical servers. I will present in this paper a solution for security improvement of your network, called Intrusion Detection Systems. It's concepts, implementation, issues, and the types of IDS that

[1] IDS means Intrusion Detection System.
[2] IPS means Intrusion Prevention System.

exists in the marked, as well as, the future of IDS, which is the Intrusion Prevention System (IPS) that can protect your entire network against different kinds of attacks. I will present a comparison for what type of solutions are best to apply to obtain a complete security policy with it's advantages and disadvantages.

What is Intrusion Detection?

The intrusion detection system is a start point to monitor and possibly prevent all kinds of events that occur in your network and systems, by analyzing the signs of intrusion. "An intrusion is somebody (A.K.A. "hacker" or "cracker") attempting to break into or misuse your system". [1]

Why is it important to use an IDS?

An IDS is a very important feature to detect the attacks that most firewalls don't detect. [2] In many Firewall implementation the web servers, mail servers and other application servers that need direct connection to the internet, will not have the related ports protected by the firewall, so malicious users may be able to bypass the security of your web server and run attacks against it. So an IDS can detect and possible prevent these types of attacks like someone trying to port scan your web server, Syn flood attacks, win nuke attacks and the attacks that occurs in your internal network.

IDS Analysis

There are two primary approaches to analyzing events to detect attacks: misuse detection and anomaly detection.

Misuse Detection

Misuse Detector is an IDS analysis that can look for an event that matches a predefined pattern of events, sometimes misuse detection is called Signature-based detection, because the IDS compares the events with the signatures previously configured in the sensor, with misuse detection all known attacks that match with a signature in the sensor are blocked, but the difficult approach is block the unknown attacks. [3]

Approaches

- Expert Systems
- Keystroke monitoring
- Model Based Intrusion Detection [4]

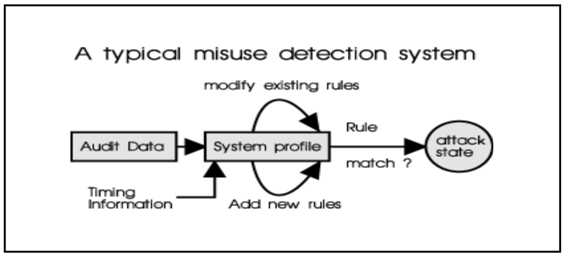

Figure 1 [4]

Anomaly Detection

“Anomaly detectors is designed to uncover abnormal patterns of behavior” [3] (anomalies) on a host or network, through this analysis the IDS generates a profile of the normal activities of the system and any suspicion activity that doesn’t match this profile, and this generates an alarm, while misuse detection only detects known attacks (attacks that matches your signature installed) the anomaly detection can detect both knows and unknowns attacks like new attacks that don’t match the current profile.

Approaches

- Statistical Approach
- Predictive Pattern Generation [4]

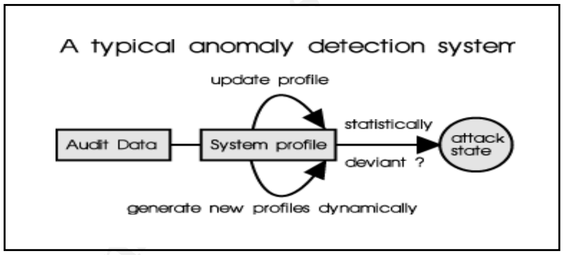

Figure 2 [4]

What type of Intrusion Detection is available?

There are two types of Intrusion detection, one is Network Intrusion detection and the other is Host based Intrusion detection.

1 - **Network Intrusion Detection (NIDS)** ⇒ This kind of IDS monitor your network segment for possible attacks that could compromised your network, like network scans, someone trying to connect a non open port, and others. The NIDS can be utilized in two modes: a normal mode that can monitor and analyze events destined for ip address of the network interface and network interface in promiscuous mode, that monitor and analyze the network traffic in real time as it crosses the network. Once an attack is recognized an NIDS utilizes many types of response, to inform the administrator, like sending an e-mail message, an snmp trap message, a log, an alert or a user response action. [5]
NIDS can have many advantages from HIDS

Lower cost of ownership - Because NIDS can be installed in your network segment and can protect this segment without installing anything in your server.

Detect attacks that HIDS systems miss - NIDS can detect attacks that HIDS don't because it examines the packet header, some types of attacks like Denied Of Service (DOS) can only be identified by looking at the packet header.

Difficult to an attacker to remove the evidence – Considering that the attackers know the audit logs of the system, they can corrupt or change this logs. With NIDS the attacker doesn’t have a chance to compromise it.

Real time detection and Response - Because NIDS detects an attack in the exact moment that it occurs, for example: If an attacks initiates a network based denied of service (DOS) the NIDS can send a TCP Reset to terminate the connection, while HIDS does not recognized as a attack until a log entry has been created.

Detect unsuccessful attacks - Because NIDS can be placed outside of a firewall to detect attacks intended to use and explore resources behind the firewall, while HIDS can only detect attacks that go to servers where it has been installed.

There are many places that you can put your NIDS. I will demonstrated bellow:

- Between the Internet router and the Firewall. This type of installation is good if you want to know what kind of packtes reaches your network.

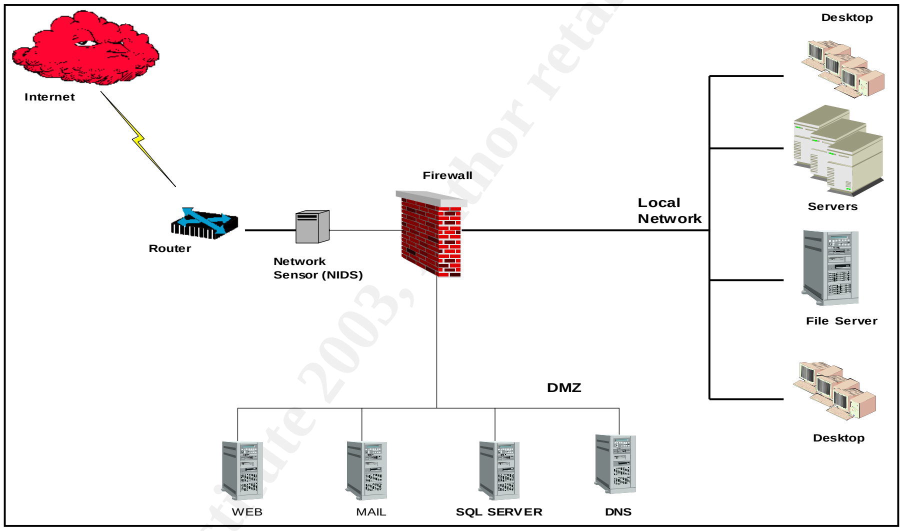

Figure 3: NIDS between the Internet router and Firewall

Advantage: You monitor what kind of packet reach your firewall and your internal network, in this scenario the attack can be identified at the exact moment that it enters your network and identifies the types of attacks that an intruder is trying to do in your system.

Disadvantage: Encrypted packages coming directly from the host are not detected by the NIDS. The NIDS doesn't monitor internal traffic and possible attacks.

- In the DMZ: This type of installation is good if you want to know what kinds of packtes reach your Demilitarized zone (DMZ).

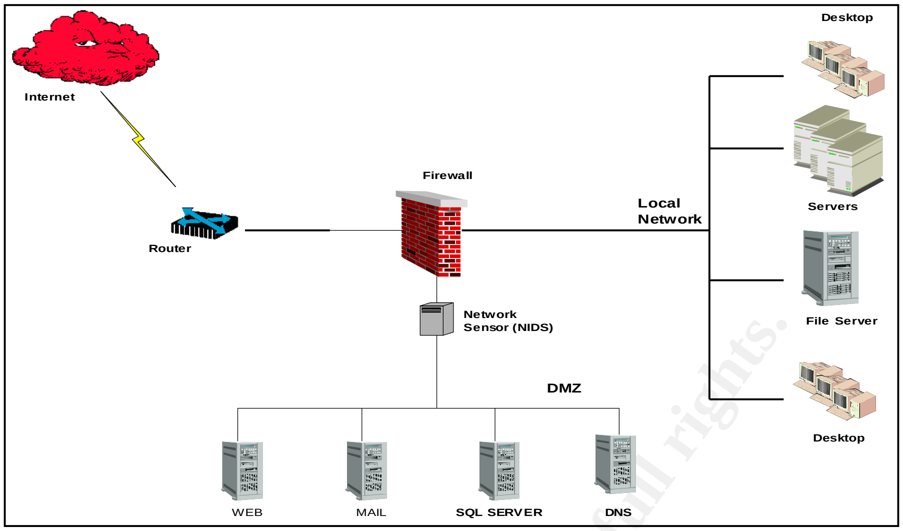

Figure 4: NIDS in the DMZ

Advantage: You monitor the kind of packets that reach your server in your Demilitarized Zone (DMZ). You can protect your server against known CGI, Unicode and DOS vulnerabilities that an intruder can use to bypass your security and explore your servers.

Disadvantage: Encrypted packages coming directly from the host are not detected by the NIDS. The NIDS doesn't monitor internal traffic and possible attacks.

- In the Internal Network: This type of installation is good if you want to monitor your internal traffic.

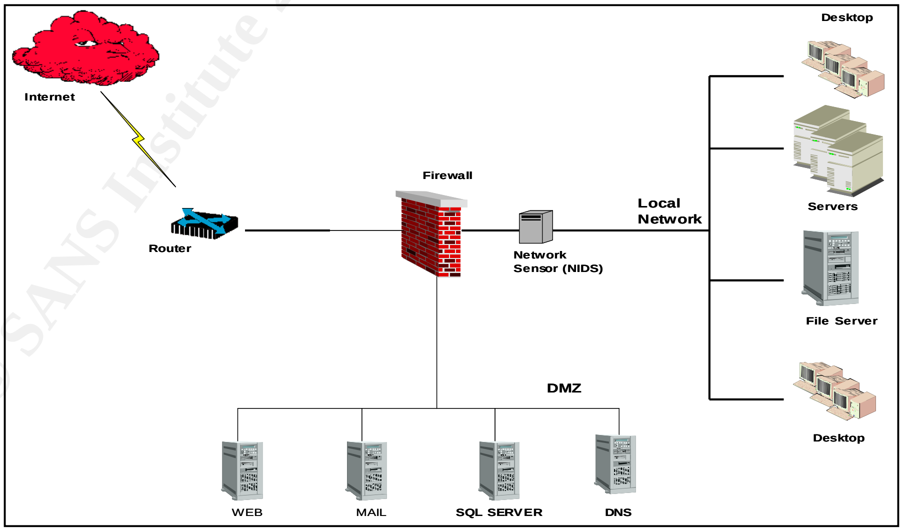

Figure 5: NIDS in the Internal Network

Advantage: You can monitor what kind of packets reach your internal network and what kind of action your users is trying to do.

Disadvantage: Your DMZ and your firewall could be compromised and alerts be blocked. Web servers, mail and other servers could be compromised without the administrators knowledge.

- A solution that includes all Network Intrusion detection System that was showed above, with this solution all events that get inside your network are monitored by NIDS.

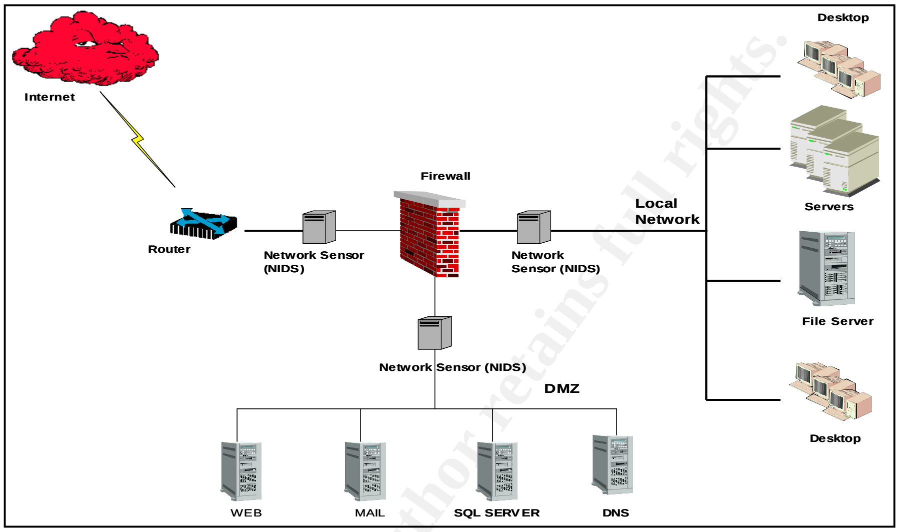

Figure 6: NIDS in all parties of the Network

Advantage: This solution is beneficial to your network, because you can monitor all types of packages that are transported in your entire network including packets that reaches your firewall.

Disadvantage: Is much more expensive to implement a complete solution with NIDS and also this type of implementation can generate to much false positives alerts.

2 – **Host based Intrusion Detection (HIDS)** ⇒ This kind of IDS is designed to run into the hosts for monitor system, events, all logs and if anyone of these items matches with your attack signature the HIDS responds with an action previously configured in your host based intrusion detection system. It's is very important when you want to know a suspicious root activity, and monitor your files in the servers protected with HIDS, the HIDS can be implemented in all server in your network but in most times it's implemented in web server to detect suspicious activities in it.

> Host-based IDSs normally utilize information sources of two types, operating system audit trails, and system logs. Operating system audit trails are usually generated at the innermost (kernel) level of the operating system, and are therefore more detailed and better protected than system logs. [5]

HIDS can have many advantages from NIDS

Verifies success or failure of an attack - Because HIDS check their logs for something that has actually occurred eliminating many false positives alerts that NIDS generate.

Monitor specific system activities - Because HIDS monitor file access activities, logon attempts and suspicious administrator activities that NIDS can't do.

Detect attacks that NIDS miss - Because HIDS can detect attacks in server console, like someone trying to access the system locally.

Near Real Time Detection and Response - Because HIDS can receive an interrupt from operation system when new log entry is generated, this type near the real time detection.

Requires no additional hardware - Because HIDS is implemented in a production server that resides in the network it didn't need any additional hardware.

The most usual place that you can put HIDS in your network is in the Delimited Zone, that is showed above:

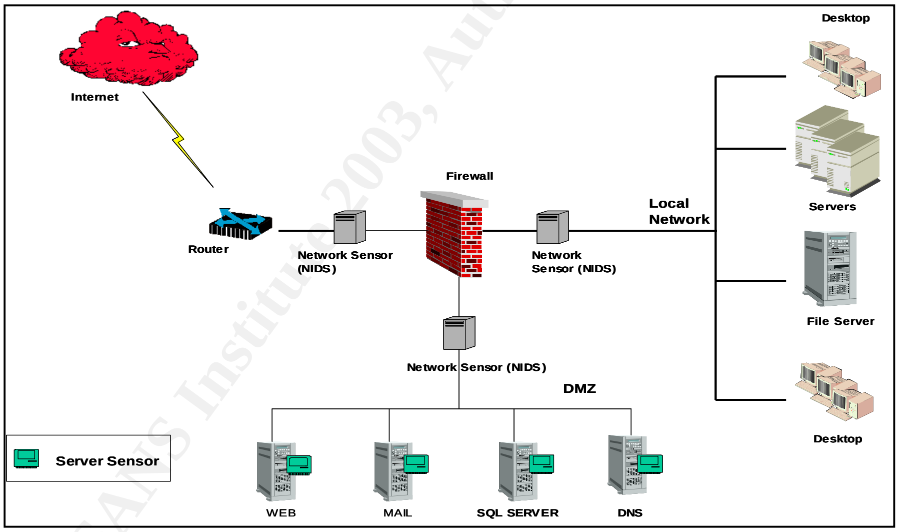

Figure 7: NIDS in all parties of the Network and HIDS in all DMZ Servers

3 – **Distribute Intrusion Detection System (dIDS)** Þ

A distributed IDS (dIDS) consists of multiple Intrusion Detection Systems (IDS) over a large network, all of which communicate with each other, or with a central server that facility advanced network monitoring, incident analysis, and instant attack data. By having these co-operative agents distributed across a network, incident analysts, network operations, and security personnel are able to get a broader view of what is occurring on their network as a whole. [6]

The complete IDS solution for an entire network, this solution needs the one central server with a complete database to collect all events from the other IDS systems, in each IDS system have one agent that communicate with the central server to send the events.

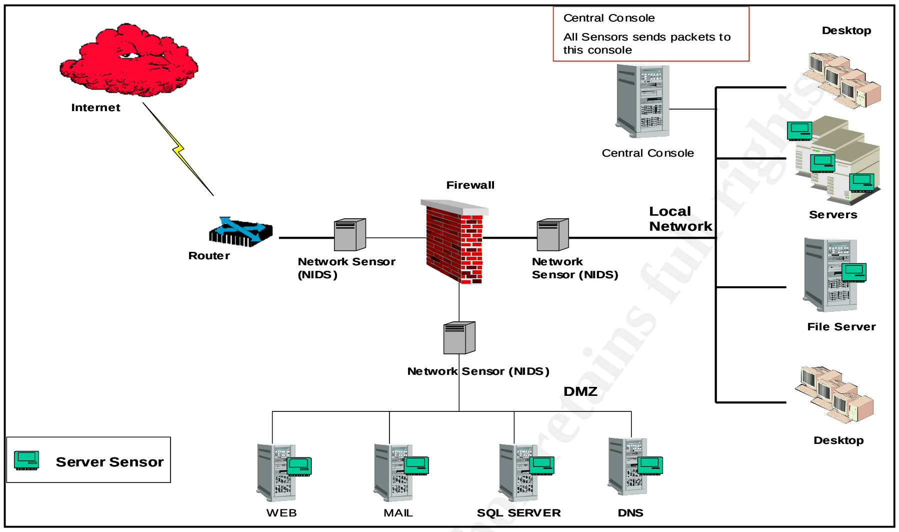

Figure 8: Distribute Intrusion Detection System (dIDS)

Advantages:

➢ One Central Console

All the management of this suite of products can be managed by one central location, making possible one central point of management. The security team can manage all sensors remotely and generate a list of reports in the central console; with this characteristics the events could be correlated to know principal types of attack.

➢ Easy Installation and Deployment.

With this suite of products it’s possible to install all agents remotely in the network, it’s easy to apply a rule that consist in protect all sensor with an easy deployment.

➢ Remote application of signatures

Signatures can be applied remotely to all sensors in the network, the rules can be defined for an entire network and applied to all sensors in simplified way, and the signatures can be customized to reflect the current structure.

➢ Update of Logs in real time

The central console receives information’s in real time from the diverse installed components and consolidates these information’s in a local database.

Disadvantages:

- **The cost of Implementation**

The solution requires a qualified team for its implementation, as well the cost of the products.

- **False Positives**

One of the great problems of the IDS solutions consists of generating diverse alerts of false positives (false events that generate an alert of attacks).

- **Lose some bandwidth**

Lose some bandwidth because all ids need to send your information to a central server.

Intrusion Prevention System

What is IPS?

Intrusion Prevention System is a new module of Intrusion Detection System that can prevent known and unknown attacks, IPS monitor the traffic and based in your rules drop, reject or accept the packet. Sometimes IPS can be called an Intrusion Detection System (IDS) that incorporates a firewall solution in it, “when you blended your Intrusion Detection System with a Firewall system”. [7]

Why it’s important to use IPS?

Different from Intrusion Detection System (IDS) that only monitored the events, an Intrusion Prevention System (IPS) monitor and prevent suspicious events, An IPS solution is a new vision of IDS that exists in the market, with this solution we can analyze more accurate an specific type of attack before it arrive your target, besides to know if the target is vulnerable or not to this attack.

IPS Analysis

The two Intrusion Prevention System modes that is more implemented in the market is:

Inline Network Intrusion Detection System (NIDS)

> Inline NIDS will inspect the packet for any vulnerabilities that it is configured to look for. If a packet contains a piece of information that trips a signature, the packet can be forwarded or dropped and either logged or unlogged. Some Inline implementations can take it a bit further though: it has the added ability to rewrite the offending packet(s) to something that won’t work, a procedure known as packet scrubbing. This type of IPS is useful if you don’t want the attacker to know that their attacks are unsuccessful or if you want the attacker to continue to attack one of your systems in an attempt to gather more evidence. [7]

Inline NIDS can be implemented in network segments were old server like AS400 and Mainframe exists.

Application Firewall / IDS

The Application Firewall / IDS will create a profile of the machine to know which applications has been using in the system, based in this profile the IPS blocks the malicious packages against these applications, the Application Firewall /IDS looks for API calls, memory management and how the application interacts with the operation system. This type of solution is very important for web server, because this analysis comes with predefined solution for web server, for example ISS Desktop Protector in paranoid mode can detect and drop all malicious packets that is destined to the Internet Information Server (IIS).

What type of Intrusion Prevention is available?

Intrusion Prevention can be put in the same scenarios that an IDS system is, more than a general way the biggest implementations of IPS are related with the new concept (Dynamic thread Protection), this solution has applications firewall / IDS, IPS inline, network IDS, vulnerability scanners, correlated modules and one or more central console. I will show this solution bellow with your characteristics:

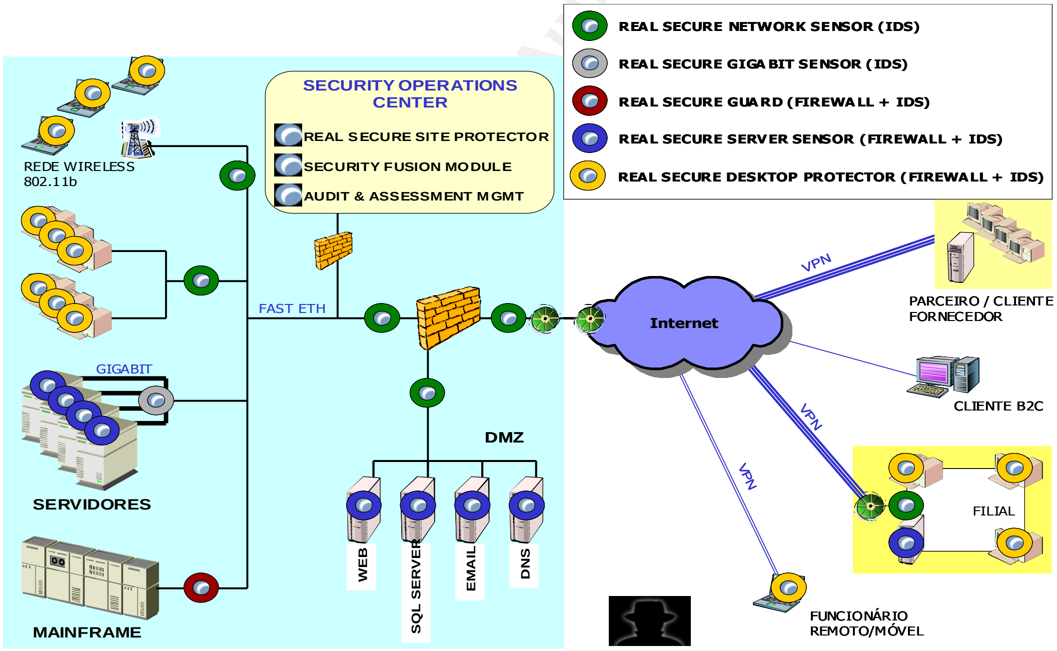
REAL SECURE NETWORK SENSOR (IDS)
REAL SECURE GIGABIT SENSOR (IDS)
REAL SECURE GUARD (FIREWALL + IDS)
REAL SECURE SERVER SENSOR (FIREWALL + IDS)
REAL SECURE DESKTOP PROTECTOR (FIREWALL + IDS)
SECURITY OPERATIONS CENTER
REAL SECURE SITE PROTECTOR
SECURITY FUSION MODULE
AUDIT & ASSESSMENT MGMT
REDE WIRELESS 802.11b
FAST ETH
GIGABIT
SERVIDORES
MAINFRAME
DMZ
WEB
SQL SERVER
EMAIL
DNS
Internet
VPN
PARCEIRO / CLIENTE FORNECEDOR
CLIENTE B2C
VPN
VPN
FILIAL
FUNCIONÁRIO REMOTO/MÓVEL

Figure 9 [12] (ISS Copright)

Characteristics:

The Dynamic Thread Protection utilizes modern correlations and analyses of data to determine fast automatically and the probability of success of an attack, from information of the vulnerability evaluation.

The attacks with high probability of success are shown in real time for the central console.
Dynamic thread Protection has an automatic criterion of classification for critical events of security.
All network assets include remote users are protect with this solution, if an intruder is trying to compromise a remote machine the sensor with firewall characteristics will block it.
Automatically correlates an attack with information of vulnerabilities on the target of the attack and assists the operators to determine the probability of success of the attack. [8]

Intrusion Detection System (IDS) vs. Intrusion Prevention System (IPS)

IDS can be considered as the last resource of network protection, being able to detect and some times eliminate the network attacks. IDS system can close a connection that it judges malicious by sending a tcp package with a Reset flag. One of the great problems that this systems is currently facing is the bad implementations of it, since the majority of times the companies do not have skilled people to manage an IDS system, generating a great low satisfaction of the security team in an IDS system. Another problem that the IDS systems face, are the extreme number of false positives and negatives that occur in this system.

IPS can be considered as an IDS system with Firewall characteristics, IPS works in active mode blocking know and unknown attacks that reaches the network. One of the IPS premises is to eliminate the great number of false positives alarms that had occurred in the IDS systems.
Inline IPS mode in many times can change the code of an attack, and block the ip address of the attacker, it’s so many times a bad thing, because IPS can block ip address of know machines in the network. [9]

The purpose of an IDS system is to alert the security team that an attack is reaching the network or network assets, it’s useful when you need to know what types of attacks are get into your network, [10] while IDS works in passive mode, the IPS system works in active mode. IDS systems alerts the security team about different types of attacks that reaches your network, while that the IPS besides alerting it they have the function to block these attacks through its proper configurations.

With the advent of the IPS systems many companies are modifying your structure to this new system, But many questions exists that the companies need to answer to know which type of system that meet your needs:

How much money the company would like to invest?
What is the type of system profile the companies needs?
There are firewalls for first defense of your perimeter?
Is it necessary that the system alerting or blocking an attack?
There are skilled people to support the system?

There is the necessity of knowing an attack?
There is a consistent security police?
Where are the possible threads of your network?
What type of threads do you like to monitor or block?

Answer these question the companies can know which type of sensor can meet or needs, because the first thing that we need to know is if the company has worry about monitor, alert or block an specific packet.

Conclusion

Recently Gartner group publish one report of "Hype Cycle for Information Security, 2003" this report said that IDS system will be obsolete, and "this functionality is moving into firewalls, which will perform deep packet inspection for content and malicious traffic blocking." [11]

In my opinion Gartner group is wrong because exists so many facts that a firewall with IDS include can't prevent:

- The firewall can't prevent internal attacks
- How Firewalls will prevent attack to servers that is visible to Internet users
- If a firewall has been compromised your entire network will be too
- With Firewall you have one point of failure
- How firewall will prevent attacks to remote users that connect your network remotely

The IDS and IPS solution with firewall is a complete solution for your entire network, because you are protect in all segments and all hosts of your network, but the major problems in IDS implementation is that the companies doesn't have a skilled staff to manage the system and the great number of false positive alerts, in a solution that encloses IDS, IPS it's is minimized.

IDS and IPS can prevent and monitor events in your entire network, but IDS is a passive system, it only sniff the network to suspicious events and when it reaches a malicious packet, it sends a tcp Reset packet, therefore in many cases you need to know if the attack is accurate or not, IDS only close the tcp connections it didn't terminated the udp packets like DNS.

IPS is a new advantage of IDS, because it operates in inline mode that can drop the packet before it arrive your target, it's can be called a real time prevention.

References

1. Graham, Robert. “IDS Faq.” URL: http://www.robertgraham.com/pubs/network-intrusion-detection.html
(12 Dec. 2002)

2.“Intrusion Detection FAQ” URL: http://www.sans.org/resources/idfaq/index.php
(6 Jul. 2003)

3. Inella, Paul and McMillan, Oba; “An Introdution to Intrusion Detection System” URL: http://www.securityfocus.com/infocus/1520
(20 Nov. 2002)

4. Tidke, Sangram. “Intrusion Detection System.”
URL: http://netweb.usc.edu/cs558/IDS.ppt
(10 Aug. 2003)

5. Bace, Rebeca and Mell, Peter; “Intrusion Detection Systems” URL: http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf
(25 Mar. 2003)

6. Enwechter, Nathan; “An Introduction to Distributed Intrusion Detection Systems.” URL: http://www.securityfocus.com/infocus/1532
(6 Jun. 2003)

7. Desai, Neil; “Intrusion Prevention Systems: the Next Step in the Evolution of IDS.” URL: http://www.securityfocus.com/infocus/1670
(29 Jul. 2003)

8. ISS Copyright 2003. “Dynamic Thread Protection - A New Definition for Information Security.” URL:
http://documents.iss.net/whitepapers/DynamicThreatProtection.pdf
(30 Ago. 2003)

9. DeShon, Markus. “Intrusion Prevention versus Intrusion Detection” URL: http://www.secureworks.net/techResourceCenter/fullTechArticle.php?article=IpsVsIds
(1 Set. 2003)

10. Laing, Brian. “How to Guide: Intrusion Detection Systems” URL: http://www.snort.org/docs/iss-placement.pdf
(28 Nov. 2002)

11. V. Wheatman, R. Stiennon, R. Wagner, J. Pescatore, A. Hallawell, J. Girard, R. Witty, K. Kavanagh. “Hype Cycle for Information Security, 2003.” Gartner Research May 2003 (2003): 10 – 11.

12. Brito, Nelson. “RealSecure Protection System” ISS Copright - Customer Presentation.