Global Information Assurance Certification Paper

Fighting system intrusions: from detection to prevention

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Muriel BAUDRION
Location: SANS Conference – Amsterdam – September 2004

This paper is an overview of Intrusion Prevention Systems (IPS). It examines the various methods used by IPS to cope with attacks: signature recognition, anomaly detection, activity profile verification and file integrity checking are the most common one. The difference between an IPS and an Intrusion Detection System (IDS) is that the former is able to respond to attacks. This is accomplished in an active way by blocking malicious packets or application requests for instance.
IPS may be either Host IPS (HIPS) which consist in specialized software components (shims) running on the host to protect or Network IPS (NIPS) which are hardware devices or software programs sitting inline the network. Tarpits are an anecdotic additional category. Network sensors must be inserted at the right network location according to the type of protection searched for. IPS may be either isolated components or made of several entities in a layered architecture. Some famous commercial IPS products will be presented in the light of the explained concepts.

Table of Contents

List of Figures

1 Introduction

Intrusion detection is a key component of any serious security strategy in today IT infrastructures. Like other measures such as data encryption, access control and authentication, vulnerability scanning, anti-virus, firewall, .. It adds a necessary layer in a defense in depth strategy.
In the face of these protections, attacks tend to be more and more sophisticated. They no longer limit themselves in scanning networks to find open ports in order to compromise operating systems through simple strategies. They more and more target applications directly by means of complex approaches, while exploiting rapidly discovered software vulnerabilities.
Firewalls and Intrusion Detection Systems (IDS) are no longer sufficient to cope with these types of attack.
Firewalls only deny malicious traffic from an unauthorized source to pass through, such as a telnet access to a device coming from the internet, if it is prohibited by one packet filtering rule. But they don't have the capability to stop malicious traffic from authorized partners, such as web traffic in destination to an internal web server[1].
Moreover firewalls operate generally at the network perimeter, and are therefore of no help to protect against attacks coming from the inside.
IDS have the capability to detect potential attacks and fire alarms, but they are by no way able to prevent them, or stop them at their early stage: the attack is rightly detected, but may be to late when the network is already infected. In 2001, the Code Red II worm, and more recently, in 2003, the SQL Slammer or the Blaster worms spread so fast that they had infected a lot of systems before an alert could be processed. Security professionals are overwhelmed by the quantity of alarms raised by IDS and either don't analyze them in details or in the contrary, waste a precious time to study them, delaying the moment to intervene.

An Intrusion prevention system (IPS) has the capability of blocking offending operations. It shows a pro-active behaviour when the IDS one is only reactive: it prevents attacks by fighting them before they may cause damages to the network or hosts, rather than simply reacting to them. Attacks are answered in real time. (Zero day answer).
Moreover an IPS protects at the application layer level against attacks exploiting well known vulnerabilities relative to an application or an operating system. They may be tied to communication protocols such as http, ftp, sendmail… Such attacks use legitimate ports left open by a firewall for information exchange: for instance HTTP port (TCP 80) may be used for a web server attack behind a firewall.

According to Gartner Group, an IPS must meet three key criteria:[2]

- While it analyzes network traffic or data flow inside host, it must not block normal operations. But it has to perform blocking actions against suspicious activities. It must have a high level of performance and must perform accurate

[1] The NSS Group, "Intrusion Prevention Systems (IPS)" Introduction
[2] Pescatore John, "Enterprise Security Moves Toward Intrusion Prevention"

actions because bad attack identification will lead to a Denial Of Service (DOS).
- It must block malicious actions using signature based blocking of known attacks, as well as behavior and anomaly-based detection algorithms. These algorithms must operate at the application level in addition to standard, network-level firewall processing.
- It must detect and block higher percentage of attacks than firewalls.

The very first IPS notions appeared in the 1990s. At the beginning IPS products were no more than IDS products with additional IPS functional packages. The first "real" IPS appeared in 1999. It was called Stormwatch and was created by Okena systems. This IPS was based on their INCORE (Intercept Correlate Rules Engine) architecture. It was analyzing files and network activities and was performing real-time decisions based on application behaviour. CISCO systems acquired Okena in 2003 [3].

Many vendors have incorporated intrusion prevention features in their products such as firewalls, or intrusion detection systems. But these features, while they alter or block the network traffic are not initiated by an inline device. Such products are able to modify Access Control Lists (ACLs) on a router or packet filtering rules on a firewall to definitively block the IP address of the attacker but they are not able to prevent a SQL Slammer worm exploit packet from making it into the network.[4]

Attacks are more and more difficult to mitigate due to the complexity of today's network environment. So IPS uses more and more sophisticated analysis methods to detect a potential attack.

2 Intrusion Detection Methods

The basis for intrusion detection is analysis of data. Depending on the type of IPS these data correspond to:

- Network Intrusion Detection System (NIPS): traffic flowing through the network under scrutiny.
- Host Intrusion Detection System (HIPS): data exchange between well chosen processes or content of system events or log files.

Different methods of analysis may be used[5]:

2.1 Misuse – Signature – Rule-based Detection

This method is based on the search of known attacks represented by signatures saved in a database. A signature consist in many information, such as the source and/or the destination of the attack, the source and/or the destination service, the communication protocol used, the payload content…
IPS scans the incoming data in order to detect either a pattern (pattern matching) or a

[3] Endorf Carl, Schultz Eugene and Mellander Jim, "Intrusion detection and prevention" p 12
[4] Alder Raven et al., "Snort 2.1 Intrusion Detection" chap 12
[5] Endorf Carl, Schultz Eugene and Mellander Jim, "Intrusion detection and prevention" p 16-18

traffic stream (stateful pattern matching) already known in the signature database[6].

In a *pattern matching methodology*, a single packet is analyzed in order to find a fixed sequence of bytes. The pattern is often associated with a service or port, a source or destination IP address, and/or the analysis of a specific portion of the payload. For instance, IPS will identify an attack if a received packet is an UDP (User Datagram Protocol) with a destination port 564, and if the payload contains the string "attacksucceeded". But there are multiple protocols and attacks that do not use well-defined ports and the pattern matching solution has difficulty detecting such attacks. In addition, this method is not suitable to streamed based traffic such as HTTP.

In a *stateful pattern matching methodology*, IPS searches unique sequences spread across multiple packets within a stream of data. For this purpose, the session context has to be kept. From the preceding example, the improvement comes from the fact that the researched string can be detected even if “attack” is located in one packet and “succeeded” in another one. Even if more sophisticated than pattern matching, this method is also vulnerable to false positives due to attack types variants. Moreover this method requires more resources as more data has to be saved before it can be decided if an attack has occurred or not.

Figure 1 shows an example of a signature in the Snort product. The signature is specified by the keyword “alert”. Then the type of protocol is specified (TCP) along with:

- The source: any TCP port from $EXTERNAL_NET IP address
- And the destination: “$HTTP_PORTS” port to “$HTTP_SERVERS” IP address.

The “msg” field indicates which type of message to look for: in this case a connection through the Common Gateway Interface (CGI) of a web server to get the “passwd.txt” file. The “content field” contains the searched data string.

```
alert :

tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS

(msg :"WEB-CGI /wwwboard/passwd.txt access";

content :"/wwwboard/passwd.txt";
```

Figure 1: Intrusion signature example (Snort Signature SID 807 [7])

The IPS may analyze the payload and header of the incoming packet (content based signature) or only the packet header (context based signature).

This detection method is very similar to those used by antivirus tools. In the same way the signature database must be updated in accordance with new discovered

[6] The NSS Group, “Gigabit Intrusion detection systems”
[7] Alder Raven et al. “Snort 2.1 Intrusion Detection” chap 12

vulnerabilities. Vendors often offer this capability via internet and the user may even frequently personalize it according to its own needs.

The main advantage of signature detection is the low rate of false positives. But obviously it does not permit to detect unknown attacks. In addition, the update of the database with the new signatures is not so easy as it is closely tied to the targeted environment: operating system and applications software.

2.2 Anomaly – Profile-based detection

This method is based on the comparison of networks or host data against a set of profiles representing the "normal" state of the network's traffic activities, user's activities or application activities. The profiles may be comprised of statistical behaviour, such as "the system TCP traffic doesn't exceed 60 % of the capacity" and of qualitative behaviour such as "the user TOTO never FTP files outside of the company". First, there is a learning phase during which the IPS builds the profiles. During this stage, the system must not be submitted to intrusive attacks in order that they should not be recorded as "normal" conditions.
Once profiles are built, IPS will monitor network or host data and compare their state to the already defined profile. If there is a deviation from this profile, it considers that there is an anomaly.
There are three main categories of anomaly detection:
- *Behavioural analysis:* the IPS looks for deviations against the profiles.
- *Protocol Decode-Based Checking*: the IPS looks for network protocol violations or misuse as defined by Requests for Comment (RFC). If this method is effective for well-defined protocols because it reduces false positive, this is not the case if the protocol is loosely defined.
- *Traffic Pattern analysis*: the IPS searches for suspect patterns linked to specific protocols to guarantee that they are not used by attackers. This comes from the fact that some vendors do not implement protocols according to RFCs.

Using this method, IPS are able to discover unknown attacks. But this could require a lot of CPU power. Moreover specifying correct thresholds value is not an easy task[8]: too low values may result in many false positive events while too high one in undetected real attacks. Finally profiles must be updated frequently because normal state may vary over time.

2.3 Target Monitoring

This method relies on system integrity: most attacks are leaving traces on systems. By using this method, an IPS is looking for changes that may occur in files (creation, modification, or file attribute change) located on system under surveillance.
This checking is based on the assumption that the analyzed system is safe at the time the integrity checking computes beforehand cryptographic hash for each file using a specific algorithm. 128 bits key MD-5 described in RFC1321 [9] was the very first

[8] Lukatsky Alex, "Protect Your Information with Intrusion Detection" chap 4
[9] IETF, "RFC 1321"

algorithm used[10]. It is now replaced by SHA-1 described in Federal Information Processing Standards FIPS PUB 180-1 or SHS [11]. At regular intervals of time, a new hash is computed and compared to the reference hash. Any difference means a modification of a file. It may be CPU and resource intensive if there are a lot of files to analyze.

2.4 Stealth Probes – Wide area correlation

The purpose of this method is to detect attacks occurring over a long period of time. It combines anomaly and misuses detection. It needs to collect a wide variety of data throughout the system to discover any related attacks.

2.5 Heuristic-Based Analysis

This method is based on expert systems which rely on existing security rules to classify events. Expert system can be used either for misused detection as well as for anomaly detection. Their artificial intelligence allows them to have a heuristic approach in the search for intrusions.

2.6 Hybrid approach

As attack may be very complex, IPS generally combines most of the previous detection methods in order to be more effective. Using a hybrid approach eliminates many more false positive and false negative.

3 Kinds of Intrusion responses

Once an IPS has detected malicious activities, it has to block the attack immediately, without any manual intervention. IPS has the capability to block the attack at different levels associated to a layer of the protocol stack.

3.1 Active response

Today, many Intrusion Detection Systems implement responses. But their responses are only associated to layer 2 to 4 of the protocol stack. This type of response cannot guarantee that the attack will be stopped, but it is frequently integrated in IPS responses.

Hereunder are some possible IPS responses depending on the layer where they occur:

- **Data Link layer:** IPS disables the port on which the attack is carried on.
- **Network layer:** IPS shuns hostile IP address by reconfiguring a firewall packet filtering rules or router Access Control List (ACL) in order to definitively block packets to or from the attacker's IP address. However, if this method is effective,

[10] Evangelista Thierry, "Détection et prévention des intrusions" Partie II : Comment détecter une intrusion?
[11] FIPS PUB 180-1 "SECURE HASH STANDARD"

it can be used by the attacker to block legitimate users by sending packets with a source spoofed IP address.

- **Transport layer:** IPS kills established TCP or UDP connections (session sniping) either by:
    - Sending a TCP reset to mitigate TCP based attacks. The TCP reset packet must contain the appropriate port and source addresses, as it was generated by the host targeted by the attacker, and not by the IPS itself. If the attacker does not handle the received packets, the TCP reset may be ignored.
    - Or by sending an ICMP unreachable messages to answer UDP or ICMP based attacks. The attacker may ignore an ICMP unreachable message too.

These types of responses are sometimes called as “passive responses”, because they may be ignored by the attacker or they may occur once the attack has been perpetrated and has reached its target.

Active response takes also place at the **application layer level**. As will be explained later on, they may be manifold.

Discarding or altering packets: the simplest active response is the IPS either discarding the malicious packet as well as all the next received packets belonging to the same session, or altering data portions of the offending packets before they reach the target. Obviously in the latter case the IPS has to recalculate the transport layer checksum.
For example, the IPS will modify a packet sent by an attacker containing a path to a shell ‘/bin/sh’ executable by a path that doesn’t exist on the target device, before the packet arrives at the target. In the same way, Figure 2 shows how the intrusion which has been detected as explained in Figure 1 is handled by changing the filename (“nofile.txt” instead of “passwd.txt”) searched for by the attacker:

alert :

```
tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-CGI /wwwboard/passwd.txt access";
content:"/wwwboard/passwd.txt";
```

replace :

```
"/wwwboard/nofile.txt"; nocase;
reference:arachnids,463; reference:cve,CVE1999-0953;
reference:nessus,10321; reference:bugtraq,649;
```

classtype :

```
attempted-recon;
sid:807;rev:7;)
```

Figure 2: Active response example (Snort Signature SID 807)

Protocol anomalies corrections: more sophisticated responses do exist, such as the IPS performing packet scrubbing[12] to remove protocol anomalies in the received packet, according to protocol specification standards.
Filtering conditions changes: Some IPS types may change their filtering decisions[13] during the course of the attack. The efficiency of the active response is measured in order to verify that it has nullified the attack. If it has succeeded, the response is maintained but it will be suppressed in the other case. IPS will then search a more appropriate measure to block the attack.
For example, if a user has been blocked due to malicious activity detection, IPS will start monitoring the user activity during a short period of time. If the activity is considered to be normal again, the user is released. Otherwise the user is definitively blocked.

Let think attack succeeded: Some IPS let the attacker think that its attack is successful in order to confirm the attack detection.

Block abnormal processes requests: A HIPS may block malicious application or operating system requests from succeeding. By this way it may prevent input data overflow from going into the stack or heap.

Because active response can in some cases generate a DOS against the network,

[12] The NSS Group, “Intrusion Prevention Systems (IPS)” Chapter “Network IPS(NIPS)"
[13] V-SECURE, “closed feedback module V secure”

many security professionals are reluctant to use it. Nevertheless the deployment of active response in an IT infrastructure must be tuned very carefully because of false positive events.

3.2 Passive response

IPS also has the capability of reporting alerts when malicious activity occurs. They are logged locally but are also sent to a management device to let the network administrator correlate all networks and hosts IPS alerts to analyze the attack. The IPS may send an e-mail with all the information to a predefined person, or perform customized actions such as generating SNMP trap.

4 Intrusion Prevention Systems types

There are three types of IPS [14].

- Host Intrusion Prevention Systems (HIPS) which are installed on hosts.
- Network Intrusion Prevention Systems (NIPS) inserted on network segments.
- Tarpits which are very specialized IPS

4.1 HIPS (Host Intrusion Prevention System)

4.1.1 HIPS presentation

A HIPS is a software installed on an individual system such as a server, a workstation or a notebook. Generally, it runs on critical business hosts. It detects and responds to malicious attacks that are moved towards the operating system or the application software. The data analyzed on the host to detect intrusions are among the following:

- The incoming and outgoing traffic that flows through the system.
- The audit log files.
- The creation, modification or suppression of files.
- The system environment of the applications. As an example, a HIPS may check the file location and settings of the registry of a Microsoft IIS a web server.
- The correct behavior of the operating system and its processes. System calls to the kernel, as well as APIs calls are monitored as they are used by applications when they request services to the operating system. This is executed by means of specialized software components called “software shims” which will be detailed later on.

4.1.2 HIPS operations

Upon attack detection, the HIPS either blocks the attack at the network interface level or generates commands to the application in order to nullify the attack.

[14] Andres Steven and Kenyon Brian “Security Sage’s Guide to Hardening the Network infrastructure” chap 9

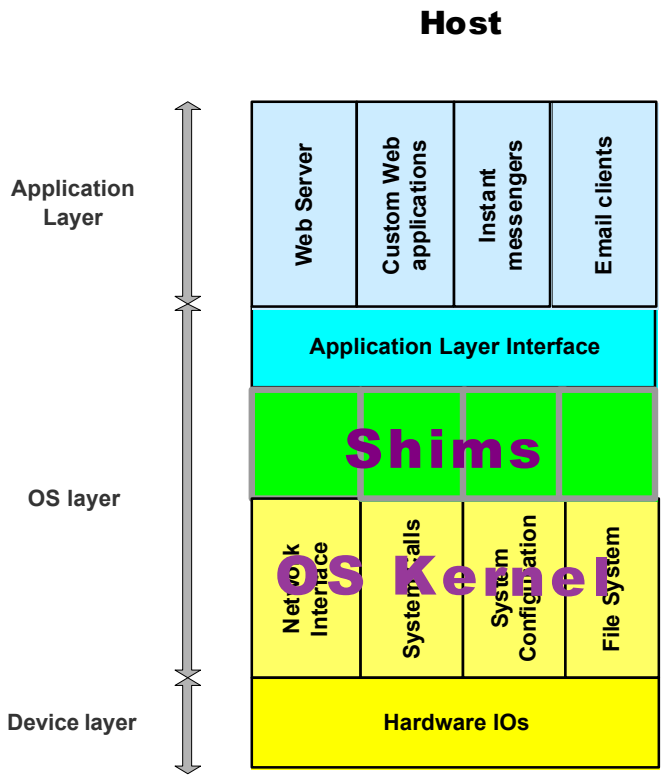

Figure 3: HIPS internal architecture

For that purpose, a HIPS may be composed of a set of shims that are inserted between the applications and the operating system. All data going through the shims are examined and analyzed according to a set of rules that define the type of actions authorized for a specific application. According to the rules, the corresponding action is allowed or denied.
There are various kinds of shims, each specialized in a type of application interaction[15]:

- A “network level shim” performs interface between application and the network.
- A “File system shim” provides file monitoring and integrity checking.
- A “Configuration shim” controls read/write access to the registry and configuration files.
- A “System call shim” that deals with application run-time environment. It has to intercept write memory requests, application illicit injection of code in another process and buffer overflow attacks.

Trusted operating system: Some HIPS may use a trusted operating system built upon an improved system kernel with the following additional security controls[16]:

- Information compartmentalization.

[15] Cisco Systems, “Securing Host using Cisco Security Agent (HIPS)”
[16] Argus Systems Group “Trusted OS security: principles and practice”

System users have restricted access to information. Therefore a compromised application cannot be used to attack another application. This is achieved by means of:

  - Mandatory Access Controls (MAC):
    MAC assigns a sensitivity labels (SLs) on system objects such as users, files, directories, processes… Access to information is restricted by SL. For instance, the "root" account has the same level of restricted access as users.
  - Discretionary Access Control (DAC):
    Access to information is restricted regarding to user's identity and group membership. File permissions and Access Control Lists (ACL) are used for access restriction.

- Role Compartmentalization or Role Based Access Control (RBAC): It is based on the assumption that nobody can perform all system operations. Important system actions require confirmation of two users and root shell access does not allow full control of the system.
- Least Privilege: Processes have the lowest privilege level needed to perform their operations.
- Kernel-level enforcement: The kernel code is hardened by additional security controls so that no user action or application can thwart its integrity.

The "Sun Trusted Solaris 8" operating system is an example of such trusted operating systems[17].

Application Firewalls: These IPS only analyze API calls, memory management, the interactions of the application with the operating system and the user interactions with the application. They are dedicated to the protection of one application. They only look at Layer 7 data to detect malicious activities. These IPS create a profile resulting from this analysis and once an operation not defined in the profile is detected, it is stopped. Each application updates must conduct to a re-evaluation of the profiles. These IPS are very closely linked to the applications they protect and are able to detect many types of attacks such as buffer overflow, parameter manipulation, hidden form field manipulation, cross-site scripting, SQL injection, directory traversal and forceful browsing, authentication hijacking, error triggering information leaks, or server misconfiguration[18]. These IPS may be either software or an hardware appliance that is placed in front of the host it has to protect.

4.1.3 Advantages/ drawbacks

There are many advantages in installing a HIPS:

- First of them is the ability that has a HIPS to protect the network against internal attacks that are the most frequent:
  - IPS protects against local attacks. It prevents a person who has physical access to the system and who has gained "root" or "administrator"

[17] Sun microsystems, "Trusted Solaris Operating System"
[18] Andres Steven and Kenyon Brian "Security Sage's Guide to Hardening the Network infrastructure" chap 9

privileges to compromise other systems in the network.
    - It prevents attacks on systems located on the same network segment.
- A HIPS is useful for the protection of mobile systems once they are connected outside of the protected network.
- A HIPS also protects against attacks on systems part of an encrypted network, because it analyzes the traffic once it has been decrypted.
- A HIPS is the "Last Line of Defense" against attacks that have not been intercepted by other security tools.

However, there are also some drawbacks:

- A HIPS is generally closed to specific applications and operating systems and many types of HIPS may be required to protect the entire network.
- A HIPS is running on the host and can be resources consuming.
- As soon as the host has been compromised, a HIPS will no more be reliable.

4.2 NIPS (Network Intrusion Prevention System)

4.2.1 NIPS presentation

A NIPS is a software program or an hardware device that monitors traffic on a network segment. It protects all devices (hosts as well as networking devices, print servers) that are plugged on the same or downstream network segments. Like a firewall, it sits inline the network, so that it can prevent malicious traffic from passing through: a packet has to enter though one of the NIPS interface and exit through another to go to its destination. Placed on a strategic segment in the network, it provides a large coverage of protection.

4.2.2 NIPS operations

A NIPS has the ability to modify or discard packets it receives. As traffic passes through the NIPS, this latest must have high performance capabilities to guarantee that legitimate traffic will not be disrupted, or delayed causing the network to be blocked. Networks are running at Gigabits and NIPS have to incorporate custom integrated circuits (FPGAs or ASICs) in order to offset performance problems. However, if the NIPS fails, it must let the traffic flow through it, without blocking the network.
NIPS include a management interface which allows NIPS to transfer information to a centralized server for alerting purpose or global analysis.
A NIPS may be located in a switched network infrastructure. In this case it must have access to the traffic that is addressed to a given segment. For that purpose, the sensor monitoring interface has to be connected to a switch port that is performing "port mirroring": This switch port receives mirrored traffic from the switch ports that must be monitored. (Also called Switch Port Analyzer or SPAN). A difficulty may be experienced to reply to an attack if the switch, like many of them, prevents the monitoring port from sending data.

4.2.3 Advantages/ drawbacks

A NIPS presence provides the following advantages:

- A NIPS does not only protect hosts, it also protects other types of system such as firewalls, routers, switches or printers…
- The configuration of the network may be modified; the NIPS will always protect all the network attached devices.
- A HIPS does not support all existing operating systems. If the network contains one unsupported host, only a NIPS will help at protecting it.
- A NIPS has a global view of the network due to its placement and can therefore intercept network oriented attacks.
- A NIPS sensor has no IP address, MAC address, nor TCP/IP stack, so it will be difficult to initiate an attack against it.

However, there are also some drawbacks:

- A NIPS is not able to detect attacks hidden in encrypted traffic since it sits in the middle of the connections.
- A NIPS may also create bottleneck in the network as all traffic has to pass through it while being analyzed in real time.

4.3 Tarpits

The tarpit is a software program that runs on a host. The role of this kind IPS is to answer to the packets that are transmitted to unused IP addresses for which no connection is expected. Tarpits negotiate connection with low bandwidth and then responds very slowly in order to force the attacker to resend packets over and over. This is particularly efficient in case of worm attack because it will answer very slowly to the probe packets that are often sent before the attack.

5 Intrusion Prevention Systems topology

The efficiency of the IPS relies on its placement in the network[19]. This chapter will examine how a full intrusion detection solution requires installation of sensors, agents and managers in a multilayered architecture.

5.1 Network sensors placement

Network sensors must be inserted in the network in a way they can capture either external or internal traffic according to the needs. They should be located preferably at traffic concentration points to provide broader coverage. HIPS are generally installed on critical servers.

[19]Noonan Wesley J, “Hardening Network Infrastructure : Bulletproof your Systems Before You are hacked !” chap 4

Figure 4 shows the most frequent places where network sensors are plugged.

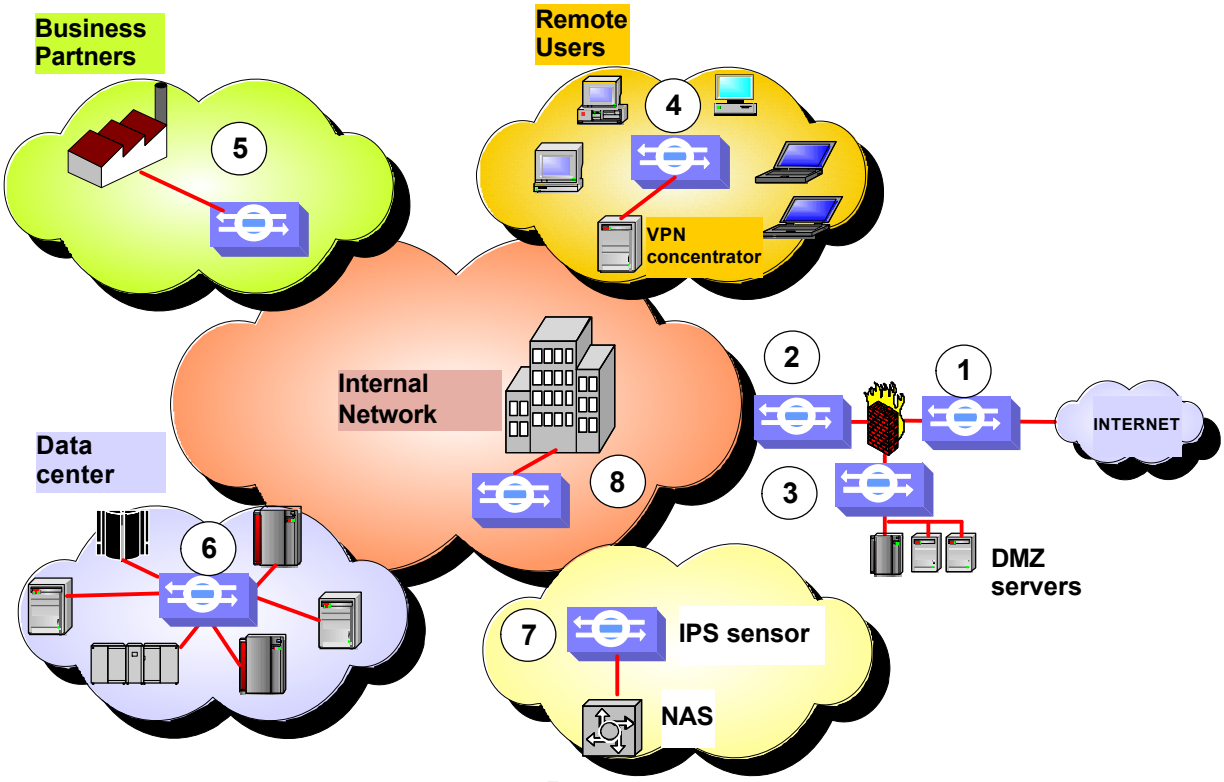

Figure 4: Network sensors placement

An IPS sensor may be placed:

- Just **in front of perimeter firewalls (1).** It gives there insight on which kind of traffic the firewalls have to cope with. In this case, it must be tuned in order not to respond to attacks that the firewall will block. It will give the network administrator precious information on how to define firewall packets filtering rules.

- **Behind the firewalls that provide access to a Demilitarized Zone (DMZ) (2) or the internal network (3).** Behind the perimeter firewall is the most commonly used location as all traffic will pass through it. In the presence of internet servers such as Web, DNS, FTP and SMTP servers located in a DMZ, a better alternative could be to install a HIPS on each of them to have a better protection.

  Sometimes IPS are **integrated into the gateway devices,** such as firewalls which generally have IPS functionalities built-in. It is an interesting solution for an IPS because it extends firewall blocking functionality.

- **Behind the VPN concentrators (4),** so that it may monitor the non–encrypted

traffic passing through it. As remote user access to the internal network is usually performed by means of VPNs, this kind of traffic will be taken into account too.

- **On the extranet connections (5)** between the internal network and business partners where implicit trust cannot be guaranteed. The IPS will be located either between the business partner facilities and the shared resources, or between the internal network and the extranet segment.

- **In front of the server segments (6) or Network Area Storage devices (7)** in order to protect valuable data residing on them from internal intrusion.

- **on any segment that contains or connects to critical resources (8)** such as the headquarter offices

5.2 Layered architecture

IPS may consist in one isolated component (single tiered architecture), but they are often implemented as hierarchical entities in a multi-tiered or peer to peer architecture.[20]

5.2.1 Single tiered architecture

The single tiered architecture is the less expensive one. Each IPS component analyzes the traffic on its own and does not communicate information to any other components. This can be an advantage if one IPS component is compromised as it will not compromise the other components.

5.2.2 Multi-tiered architecture

In a multi-tiered architecture, three components are involved:

- Sensors which either collect traffic from the network, or from log files, system calls…
- Agents that analyze input from sensors and perform attack detection. Each agent is dedicated to a specific function. For example, an agent may examine only HTTP traffic, while another agent examines FTP traffic. Agents are communicating with each other and when an agent suspects an attack, it immediately notifies other agents. The information given by other agents will help proving the attack. An agent may perform blocking functions.
- A Manager component which receives information from all agents. This latest analyzes information gathered from all the network components and correlates events in order to perform appropriate actions such as alerting, or sending request to components to perform specific prevention actions. The manager component generally centralizes and archives all data received from agents. It also distributes new policies to all agents. A management console is often attached to the manager component. Thanks to it, the security administrator

[20] Endorf Carl, Schultz Eugene and Mellander Jim, “Intrusion Detection and Prevention” Chap 6

interacts with the IPS. He accesses all alerts, IPS status, audit logs, and so forth.

This solution is the most commonly used. It allows having an in-depth analysis of the network security.

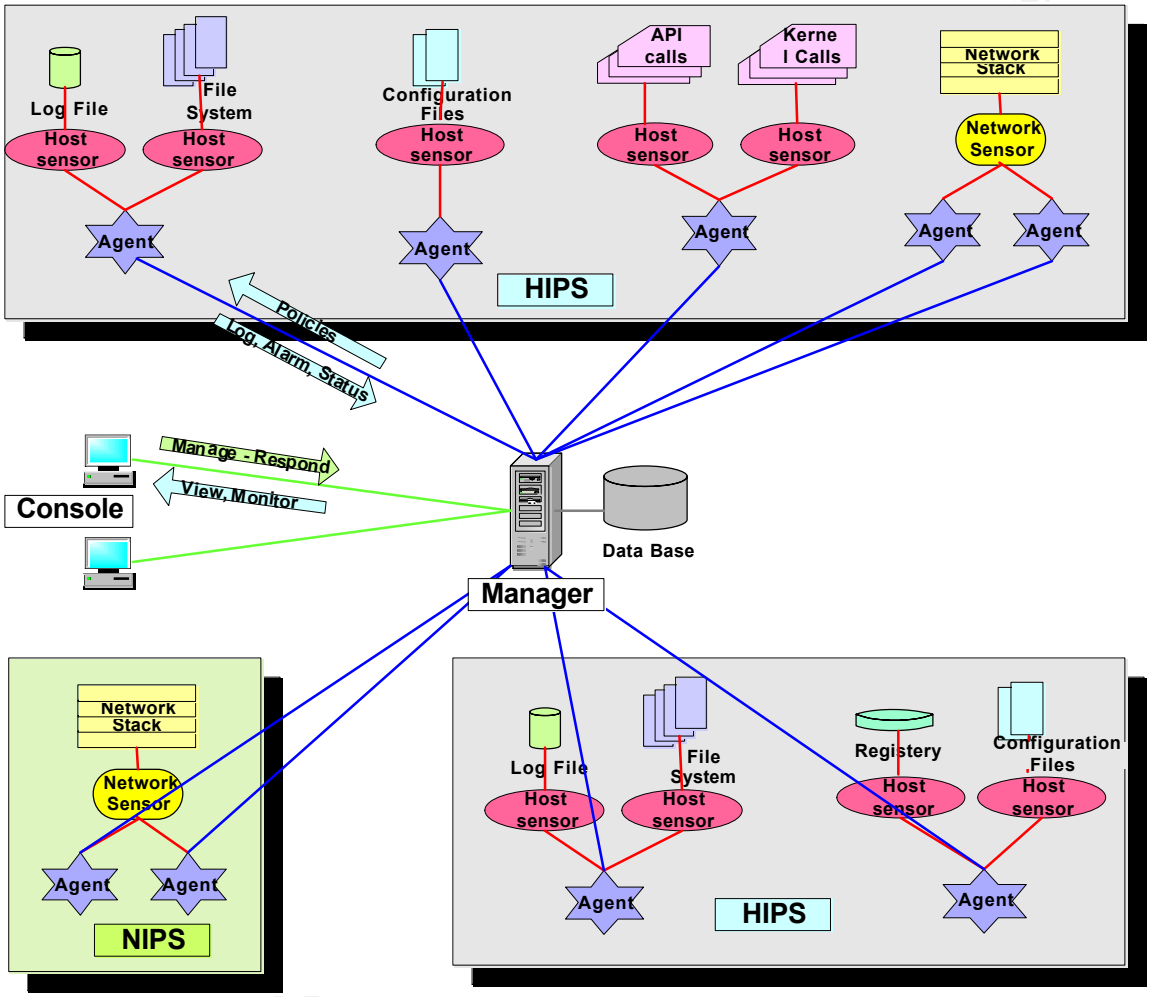

Figure 5: Multi-tiered architecture

5.1.3 Peer to peer architecture

In the peer to peer architecture, all peer components communicate with each other peers. They either notify other components about attacks or require actions from other components. This architecture is more effective than the single tiered architecture because all components have a more global view of the network. However, there is no centralized management component.

6 Some commercial products

This chapter will illustrate all the concepts explained here above by summarizing some HIPS and NIPS commercial solutions.

6.1 HIPS products

6.1.1 McAfee Entercept

McAfee Entercept[21] consists in three components: the agent which is installed on the host, the management server which manages up to 5000 agents and the console which is used for agent configuration. Each agent is designed for an application type:

- McAfee Entercept Standard Edition is dedicated to general purpose enterprise servers supporting lot of operating systems
- McAfee Entercept Web Server Edition (WSE) defends Web servers against buffer overflow and privilege escalation attacks by preventing any unauthorized server process.
- McAfee Entercept Database Edition locks down Microsoft SQL 2000 database to enforce correct behavior and block abnormal ones.

Mc Afee Entercept agent detects attacks using signature detection analysis and behavioural analysis. It includes firewall capabilities like blocking accesses at network level (by logical port, protocol, or IP Address) or blocking requests at applications or services level. It proposes a means to reduce the time required to configure the rules. Entercept 'adaptive auditing" functionality allows it to easily 'learn' the applications located on the servers. Entercept agent wraps a protective envelope around the processes so that each time an application tries to access the executing files, Entercept agent must approve the action.

6.1.2 Sana Primary Response

Sana Security Primary Response[22] software protects host applications such as Web server, Microsoft MS Exchange, Lotus Notes, SQL server, SAP .., or custom applications on Windows or Solaris platforms. Its detection method is exclusively profile based. The specificity of this HIPS comes from the in-depth inspection it performs at the lower levels of the operating system, learning normal applications behavior to build adaptive profiles. It continually monitors the system in order to update the application behavior profiles. Known as well as unknown malicious activities are blocked at kernel level. Primary Response solution is a multi tiered architecture and up to 7000 HIPS can communicate with the Primary Response Management Server to give the security administrator a global view of attacks detection and response.

6.1.3 Cisco Security Agent

Cisco proposes a solution based on a combined HIPS and NIDS. HIPS Cisco Security

[21] McAfee, "Entercept Host Intrusion Prevention System – Frequently asked questions"
[22] Sana Security " Sana Security Launches Suite of Innate Defense Modules for Personal Computers"

Agent[23] intercepts system resource calls to kernel by applications and authorizes or forbid them in real time according to application behavioral policies. It acts also as an intrusion prevention agent, a file integrity monitoring agent and an application sandbox. It deploys four interceptors:

- File system interceptor captures all read or write attempted file accesses and authorizes or blocks them according to the policy
- Network interceptor analyses packets at network interface level and enforces security.
- Configuration interceptor captures read/write requests to the registry on Microsoft Windows or rc files on Unix.
- Execution Space Interceptor blocks write requests to memory space not owned by the requesting application, application attempts to inject code in another process and buffer overflow attacks.

Note Sand boxing is a technique that prevents access to server resources not specifically allowed by the operating system or application.

6.1.4 eEye Digital Security SecureIIS

eEye with SecureIIS[24] is an application level firewall designed to protect a Microsoft Internet Information Server (IIS) Web Server. It is plugged into IIS and every time a Web request is received it checks it against known vulnerabilities and malformed data. Then it either forwards the request to IIS for execution, or blocks it. SecureIIS relies on heuristic attack detection. It is also able to monitor specific files for suspect creation, modification or deletion.

6.2 NIPS products

6.2.1 Snort_Inline

Snort_Inline[25] is built on the famous Snort IDS. It is usually deployed on a Linux system acting as a router or an Ethernet bridge between two network segments. It looks into the IP packets queues to detect intrusions and has the capability to respond to them.

6.2.2 McAfee Intrushield

Network Associate (NAI) Mc Afee proposes three models of sensors[26] depending on network bandwidth to deal with.

- Intrushied 1200 is designed to protect branch offices by handling up to 100 Mbps throughput.
- Intrushield 1600 protects enterprise perimeter with 600 Mbps throughput.
- Intrushield 1400 is a high end product for core networks allowing to handle up to 2Gbps throughput.

[23] Cisco Systems, “Securing Host using Cisco Security Agent (HIPS)”
[24] eEye Digital Security, “SecureIIS Web Server Protection”
[25] Alder Raven et al. “Snort 2.1 Intrusion Detection, second Edition” chap 12
[26] McAfee “Host and Network Intrusion Prevention White Paper”

Intrushield performs hybrid intrusion detection: signature detection and anomaly detection including statistical techniques.
Intrushield sensors are able to detect attacks on SSL encrypted traffic, as they may decrypt traffic with the private encryption keys if they have been previously stored on the sensors, obviously in a secure fashion.

6.2.3 Tipping Point Unity One

Tipping Point Unity One offers sensors[27] with a wide range of performance from the "Unity One 50" appliance intended for small offices with a throughput up to 50 Mbps, to the 5 Gigabits "Unity One 5000". All contain dedicated ASICs. They integrate a discovery tool that performs a network segment discovery of Windows and Unix servers to help in traffic analysis and in the reduction of false positive findings. Their signatures dictionary is built from the SANS, CERT and Securiteam. In case of failure, a sensor has the ability to transform itself to a switch, in order to not block the traffic.

6.2.4 Juniper Networks NetScreen-IDP

Juniper NetScreen-IDP 1000[28] is a three tiered architecture solution. This IPS has won the Network Computing "great IPS test" at the beginning of 2005, for its user friendly management interface that make it easier for the network administrator to understand the context of an attack and to customize the signatures in an easy way[29]. It uses Multi Method of Detection (MMD™) such as stateful pattern matching signature, protocol and traffic anomaly detection, backdoor detection and provides also network honeypot functionality. Another feature is that it can be attached in parallel mode on the network to improve effectiveness in case of high capacity network.

6.3 Tarpits

6.3.1 LaBrea

LaBrea[30] is a Linux based application which takes advantages of the Address Resolution Protocol (ARP) used by routers to answer ARP requests for which no physical device has answered (IP address not instantiated on an hardware MAC address) and creates a virtual machines associated to the unused targeted IP address. The virtual machines hold the connection open for a long time until it gets stuck. It is very effective in stopping or slowing down network scans. It can also be used in a switched environment.

7 Conclusion

Intrusion Prevention technology is yet in its early stage, but is in constant evolution.

[27] TippingPoint "UnityOne Intrusion Prevention Systems"
[28] Juniper Networks "Intrusion Detection and Prevention"
[29] NWC "Intrusion-Protection Systems. The Great IPS Test"
[30] LaBrea Technologies "Welcome To My Tarpit - The Tactical and Strategic use of Labrea"

Even terminology and concepts are not stabilized and may differ among authors and vendors. But there is no doubt that it becomes a hot topic and that IPS have a growing place in a “defense in depth” strategy.

An IPS is not a monolithic box like a router, performing every instant the same dumb job: it is rather a set of intelligent hardware (network sensors) and software components (shims, hosts agents) which can be associated in many ways to provide a complex solution tailored to the organization security threats and business needs. Intelligence is often spread between highly specialized sensors or agents, and a centralized server, offering unique means to cope with the most pernicious attacks. A state of the art solution combine NIPS for their capacity to defend the overall network, with HIPS for their ability, by being closely linked to hosts, to put them aside of any attack.
The IPS intrusion detection part consists of elaborate methods based on attacks signatures, activities profiling, rules deviations, anomalies follow up, which may be mixed together for more efficiency. These signatures, rules and profiles are constantly updated to cope with new threats, sometimes in an automatic fashion by the system itself. They may even be handled by Artificial Intelligence agents.
The IPS intrusion prevention part, unmatched by any other existing solution, may occur at network or host level depending on the attack and may also adapt itself to the efficiency of the response.

It goes without saying that such complete security solutions are expensive and that their architecture and deployment must be carefully studied and planned. Skilled security professionals must also be in charge to finely configure the IPS according to the organization security policies and threats, and tune it over time. Performance issues must not be underestimated as IPS are often "inline": for high throughput requirements, products based on integrated circuits are a must.
Care must also be taken about the IPS capability to eliminate by itself false positive findings, as it is easy to understand that the amount of alerts generated by such a distributed and "surgical" system may quickly become a nightmare. False positive findings may also generate inappropriate reactions towards "innocent" devices. Undetected attacks are also a problem: the coverage of the IPS must be near 100 %. Vendors are actively working on these issues.

What about the future? Bob Geiger says[31] that the major improvement of IPS will not be in the “basic network and performance requirements” but in the “content, and expertise in the design of the products and in the security intelligence fed into the products in real time”. This will help IPS to cope with new areas of interest in the internet world, such as the rapid and uncontrolled spreading of adwares, spywares, key loggers and other hidden dialers. In the beginning of 2005, market leaders McAfee with its Intrushield and Tipping Point with is Unity One solutions have announced coming support in these domains[32].

[31] Geiger Bob “The future of Network Security :Intelligence Behind Intrusion Protection Systems”
[32] Messmer Ellen “IPS gets bigger role in spyware defense”

8 References

[1] [5] [12] The NSS Group. “Intrusion Prevention Systems (IPS)”. January 2004. February 28, 2005 <http://www.nss.co.uk/WhitePapers/intrusion_prevention_systems.htm>

[2] Pescatore John. Gartner Group. “Enterprise Security Moves Toward Intrusion Prevention”. September 25, 2003. February 28, 2005 <http://www.csoonline.com/analyst/report1771.html>

[3] [20] Endorf Carl, Schultz Eugene and Mellander Jim. Intrusion Detection and Prevention. New York: McGraw-Hill/Osborne. 2004

[4] [7] [25] Alder Raven et al. Snort 2.1 Intrusion Detection. Rockland: Syngress Publishing, Inc. Second Edition 2004

[6] The NSS Group. “Gigabit Intrusion detection systems”. January 2004. February 28, 2005 <http://www.nss.co.uk/WhitePapers/gigabit_ids.htm>

[8] Lukatsky Alex. Protect Your Information with Intrusion Detection. Wayne: A-LIST Publishing. 2003

[9] The Internet Engineering Task Force. "Request for Comments 1321". April 1992. February 28, 2005 <http://www.ietf.org/rfc/rfc1321.txt>

[10] Evangelista Thierry. “Détection et prévention des intrusions. Partie II : Comment détecter une intrusion ?". November 30, 2004. February 28, 2005 <http://www.vulnerabilite.com/dossier/?page_num=1&id=14>

[11] Federal Information Processing Standards FIPS PUB 180-1 “SECURE HASH STANDARD”. April 17, 1995. February 28, 2005 <http://www.itl.nist.gov/fipspubs/fip180-1.htm>

[13] V-SECURE. “Closed Feedback Module”. 2004. February 28, 2005 <http://www.v-secure.com/technology/feedback_module.asp>

[14] [18] Andres Steven and Kenyon Brian. Security Sage’s Guide to Hardening the Network infrastructure. Rockland: Syngress Publishing, Inc. 2004

[15] [23] Cisco Systems. Securing Hosts using Cisco Security Agent (HIPS). Student Guide. Version 1.0. KnowledgeNet.com, Inc. 2004

[16] Argus Systems Group. "Products White Papers PitBull Foundation and Foundation Suite". Trusted OS security: principles and practice. December 2004. February 28, 2005 <http://www.argus-systems.com/product/white_paper/pitbull/oss/2.shtml>

[17] Sun microsystems. "Trusted Solaris Operating System". February 28, 2005 <http://www.sun.com/software/solaris/trustedsolaris/index.xml>

[19] Noonan Wesley J. Hardening Network Infrastructure: Bulletproof Your Systems Before You Are Hacked!. New York: McGraw-Hill/Osborne 2004

[21] McAfee. "Entercept Host Intrusion Prevention System – Frequently asked questions". June 2004. February 28, 2005 <http://www.networkassociates.com/us/_tier2/products/_media/mcafee/entercept_faq_june_04.pdf>

[22] Sana Security. " Sana Security Launches Suite of Innate Defense Modules for Personal Computers". October 25, 2004. February 28, 2005 <http://www.sanasecurity.com/press/pressreleases/102504.php>

[24] eEye Digital Security. "SecureIIS Web Server Protection". February 28, 2005 <http://www.eeye.com/html/products/secureiis/index.html>

[26] McAfee. "Host and Network Intrusion Prevention White Paper". February 2005. February 28, 2005 <http://www.networkassociates.com/us/local_content/white_papers/wp_host_nip.pdf>

[27] TippingPoint. "UnityOne Intrusion Prevention Systems". February 28, 2005 <http://www.tippingpoint.com/products.html>

[28] Juniper Networks. "Intrusion Detection and Prevention". February 28, 2005 <http://www.juniper.net/products/intrusion/>

[29] Network Computing. "Intrusion-Protection Systems. The Great IPS Test" January 20, 2005. February 28, 2005 <http://www.nwc.com/showitem.jhtml?articleID=57700108&pgno=3>

[30] LaBrea Technologies. “Welcome To My Tarpit - The Tactical and Strategic use of Labrea”. February 28, 2005 <http://www.labreatechnologies.com/LaBrea_Tactics_And_Strategy.pdf>

[31] Geiger Bob. “The future of Network Security: Intelligence Behind Intrusion Protection Systems”. February 18, 2005. February 28, 2005 <http://www.dmreview.com/article_sub.cfm?articleId=1020435>

[32] Messmer Ellen. "IPS gets bigger role in spyware defense". NetworkWorldFusion News. January 17, 2005. February 28, 2005 <http://www.nwfusion.com/news/2005/011705mcaffee.html>

********** **END OF DOCUMENT**
****