# Implementation of an Intrusion Detection System

**SAIDI BEN BOUBAKER Ourida [1]**

**[1] Computer Science Departement, Hifgh Institute of Management, University of Tunis**
**44, Av. de la liberté , Bardo/Tunis, Tunisa**

**Abstract**
Securing networks and data is among interesting issues of computer science research and practice. Many approaches and techniques have been developed to secure computer architectures, they addressed several layers, e.g, physical security, applications and encryption algorithms, etc. In this paper, we address the problem of securing large networks with complex architectures, based on intrusion detection systems. Based on the experimentations performed, we demonstrated the efficiency of our solution.
***Keywords:*** Information Systems Security, Intrusion Detection, Networks.

## 1. Introduction:

### 1.1. Definition of an intrusion detection system:

An intrusion detection system is a system that can analyze in real time or delayed events from a computer system. It detects overflows[1], among other rights and prevents visible signs of attacks against information systems. It's sort of a device to monitor the activity of a machine or network to detect intrusion attempts and generate alerts for possible against reactions and procedures.

### 1.3. Importance of intrusion detection system in a computer archi tecture:

An architecture is always likely to be attacked especially when dealing with a network architecture in which information flows across all segments and thus presenting vulnerabilities allowing an attacker to enter and enforce illegal actions generating anomalies in the network, hence the need to implement a solution for analyzing network traffic to detect and thwart a possible intrusion. This system will detect portions malicious network traffic from the Internet generally. It can also be used to detect viruses that try to attack computers in a LAN. It records the systematic attempts to connect from outside, which often indicate that someone is trying to find open ports on the host. The intrusion detection system stops the malicious packets for these ports open.
The intrusion detection system analyzes the content and information from the header of an IP packet and compares this information with signatures of known attacks. When information is similar or identical to a known attack, the intrusion detection system issues a warning and performs the action planned.

## 2. Specification of the project addressed:

### 2.1. Description of the network topology:

The network has two different topologies:
- A star topology built through a switch (switch) used for the interconnection of different parts of networks also connected with a level-2 switch for linking the physical positions of the segments. These connections using RJ45 connections for lines less than 85 meters and connections for fiber-optic lines over 100 meters.
- A Wireless Network that works around a number of access points distributed over many locations and connected physically to switches in order to address the problem of the scope which should not exceed fifty meters.
In addition to this topology, the network operatesas follows:
-The entire network has a dynamically assigned IP address through a DHCP server to avoid conflicts.
- The network uses a firewall to block unauthorized access and protect the internal network attacks.
- A dematerialized zone (DMZ) is used to install internal servers such as Web server and FTP server accessible from the internal and external network.
Access to the Internet is through a remote proxy used to identify the network user.

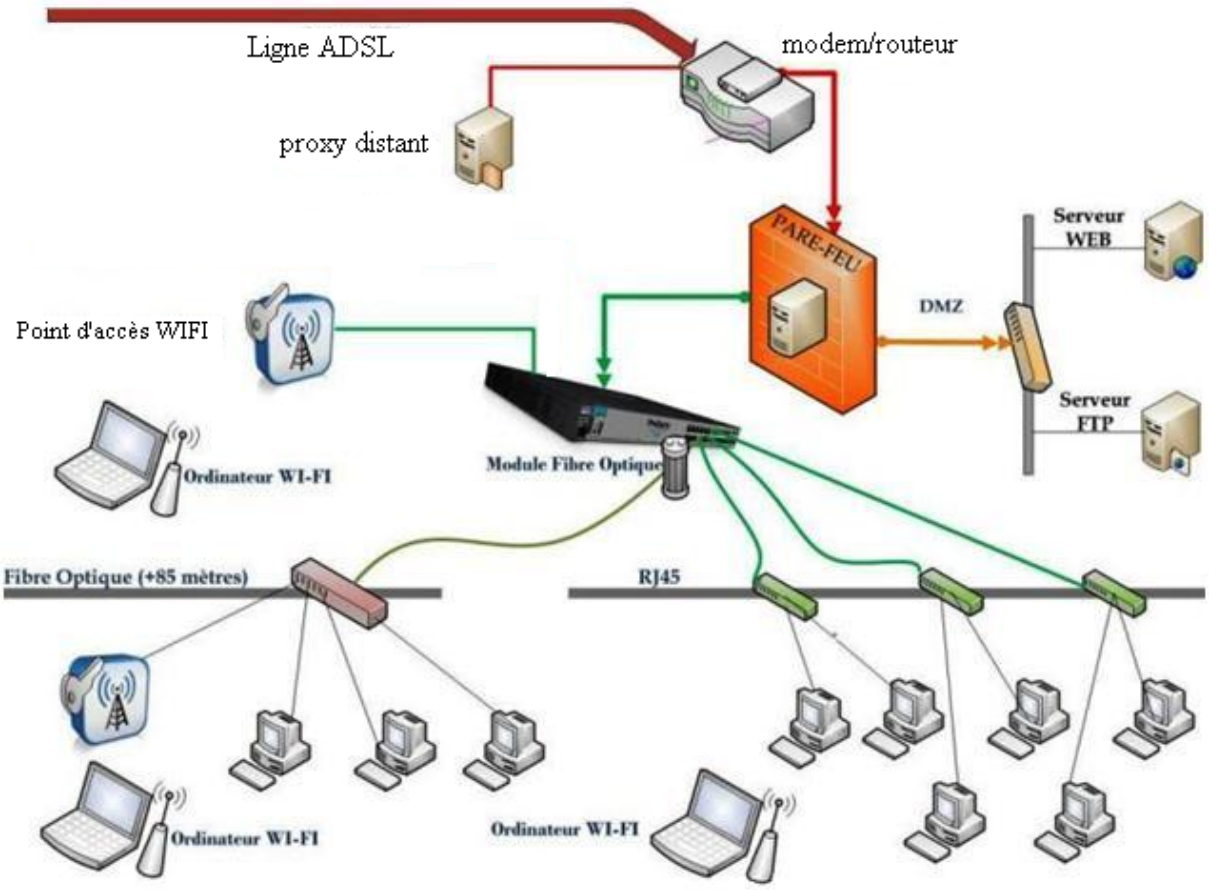



Figure 1: Network topology

**2.2. Security risks with this architectur e:**
Due to the very high number of computers connected to the network and benefiting from access to the Internet, our architecture presented the following security issues:
- Many passive attacks from the outside which can be summarized by the port scan to detect those who are open to change to active attacks.
- The download free software via the Internet has caused the infiltration of viruses into the network, which search for vulnerabilities in network and application layers in order to perform intrusions.
- The use of WEP encryption keys is a weak strategy which can be exploited by unregistered users because they can perform many intrusions such as scans of ports, retrieving addresses of access points and use keysdecryption utilities.
- While a firewall is in place to block a lot of malicious traffic, no functionality to alerts in case of existence of a new intrusion. In addition, the firewall installed operates on the lower layers of the OSI model and does not take into account the vulnerabilities of the application layer, which remains an important source of intrusion.

**2.3.Proposed Solution: IDS:**
In order to improve the security capabilities of our architecture and to ensure a more save network, we decided to implement an intrusion detection system. In what follows, we detail our solution.

## 3. Implementation of the IDS:

### 3.1. Techniques used:
The implementation of an intrusion detector is based on two important aspects[3]:

**3.1. Main approaches:**
According to its internal architecture, an intrusion detection system is based on a well-defined approach. There are here are two main approaches:
**- Behavioral Approach:**
This approach is based on tracking the behavior of a user, service or any application to infer a probable intrusion. If any of the entities mentioned above changes its behavior or the habits of its operation, the detector deduced that There's suspicious behavior and eventually transmit early warning. This approach itself uses either a probabilistic method in order to estimate a suspect traffic or a statistical method whose principle is to compare quantitatively the behavior of parameters related to the user such as the occupancy rate of bandwidth or the number of network access per day.
**- scenario based approach**:

The principle of this approach is based on known techniques used by hackers to perform intrusions, already enrolled in a signature, for comparison with the behavior of the user in question without recourse to its history and determine if this behavior is legal or not. The signature is actually a series of rules for analyzing packets that flow through the network (pattern matching) or the compliance of the protocol (protocol approach).
The use of both approaches in parallel will serve as a powerful solution for intrusion detection.

### 3.1. Types of IDS:

Intrusion detectors can operate in three possible methods[2]:
- H-IDS is a detector which, when installed on a local host, it operates as a service core to analyze traffic to that host, or to identify intrusion attempts.
- N-IDS is a detector which analyzes passively all incoming and outgoing traffic flowing through the network to detect the end of packet supposedly dangerous and generate alerts.
- Hybrid IDS: This is a sensor whose objective is to collect information via the various nodes placed on the network and hosts for analysis purposes. Using both H-IDS and N-IDS is a robust solution against several attacks.

### 3.2. Localization in the n etwork architecture:

It all depends on what you want to protect the location of the intrusion detector can be done in three possible positions:
- Upstream: This position is used to detect frontal attacks coming from outside and beyond the firewall to attack the internal network. It has the disadvantages of the large number of alerts that may occur to and are not detected by the firewall[5].

♣ Downstream: With this position, the intrusion detector is placed before the firewall allowing to detect intrusions from the outside but the problem is that the attacks on the internal network will not be detected.
♣ Before the DMZ: This position allows the IDS to detect intrusions that were not filtered by the firewall and protects the area against intruders. The downside is that the internal network is open to intrusion.

### 3.3. Technologies used to implement

The implementation of an intrusion detection system and after a study of existing software, the use of two types of intrusion detectors was an adequate solution to protect the network and its components. The solution is to install an antivirus internet security with the functionality of intrusion detection (IDS-H), which operates on the client / server architecture and a network intrusion detector (N-IDS) like Snort that uses the scenario approach and installed according to the three possible positions mentioned above.

### 3.4. Detailed steps of im plementation:

The implementation of the IDS required the main following two steps
**- Step 1:** This step is to install an antivirus internet security on a central server.♣ This antivirus has built-in intrusion detection system and its database alert rules are updated automatically through the official website. All computers connected to the network operate as clients and retrieve updates from the server including intrusion detection signatures. In this way, it provides the functionality of an intrusion detector host-reaction with H-IDS as it is not only to alerts but to intervene to block possible attacks on a component.
- Step 2: This step is to install an intrusion detection SNORT as alert nodes on different zones of the network in order to collect all the intrusion attempts that are logged to a log file. If this attempt is blocked automatically by the firewall, Snort does not, else, the intrusion detector alerts the attempt by placing an entry in the log file. By adding these signatures of intrusions into a guardian of active network that operates in parallel with SNORT, all attempts with the same signature will be blocked or rejected. The nodes are installed according to the following figure:

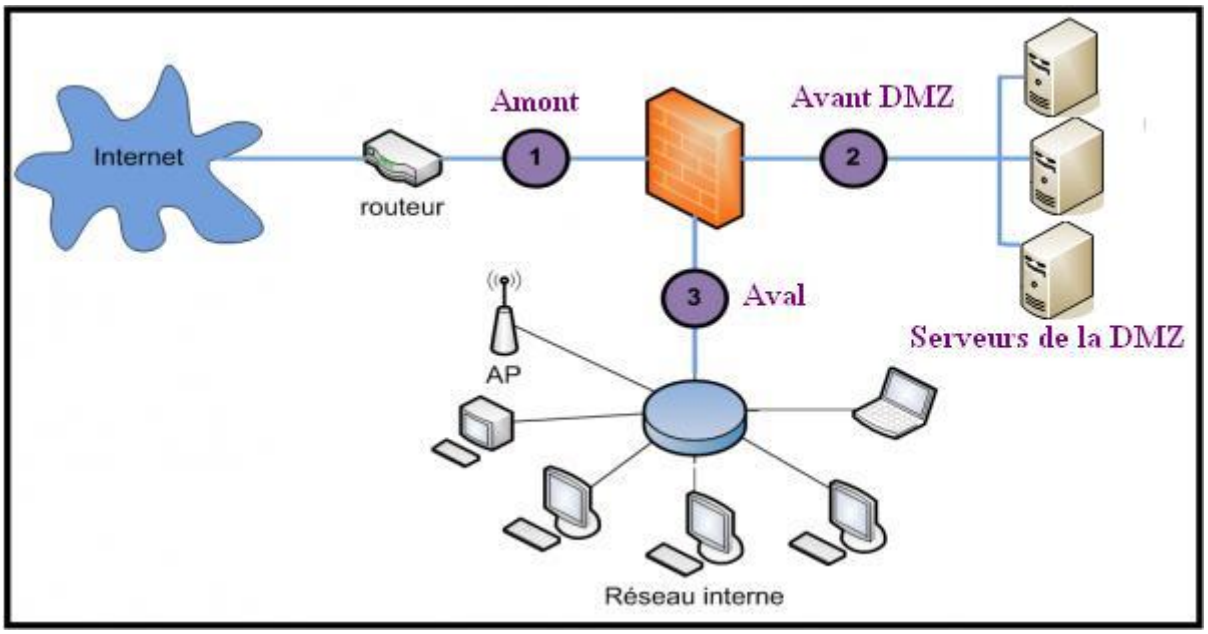



Figure 2: Positioning of nodes SNORT

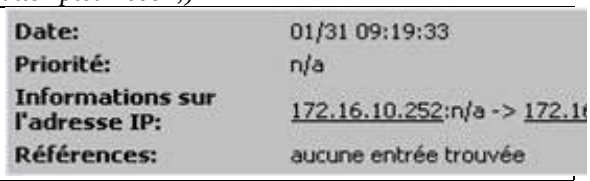
With this localization, intrusion detection will ensure[4]:
a. Intrusions from the Internet are detected before they are filtered by the firewall. This is the position upstream
b. Intrusions that exceed the firewall and whose direction is the internal network. This is the position downstream
c. Intrusions from the Internet and the internal network and that management is the DMZ are detected via the sensor installed before entering the area.
This facility provides an intrusion detection on all zones of the network and connected computers. To be updated with the new intrusions and detecting their signatures, updating the rules is very important and is available through the official website snort.org charge provided that is registered on this site. This record can acquire a code called Oink code used as an identifier and must be inserted on this page to be eligible for regular updating Snort certified rules.

### 3.5. Experimentations:

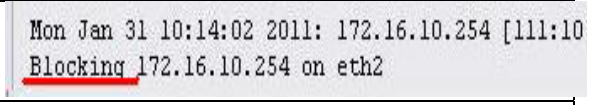
In order to test the firewall rules, intrusion sensor (Snort) and the controller of the network, some simulated attacks were performed. Normally intrusion attempts are filtered by the firewall rules in the first place and once they exceed these attempts, they will be analyzed by the detector of intrusions and subsequently filtered by the controller of the network.

#### 3.5.1. Intrusion with port scanner (Advanced port scanner)

This is a network sniffer that detects open ports. This intrusion is detected by the signature *snmp.rules* having as filter rule: *alert tcp $ EXTERNAL_NET any -> $ HOME_NET 161 (msg: "SNMP request tcp"; stateless; reference: cve, CAN-20014-0012; reference: cve, CAN-20014-0013; sid: 1418, rev: 3; classtype : attempted-recon;)*



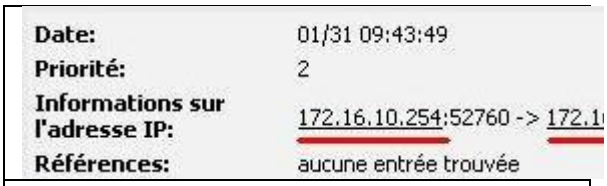

Ports Scan detected bu SNORT



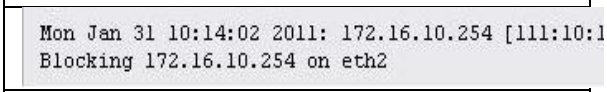

Attack block by the network controller

#### 3.5.2. Intrusion by netw ork sniffer (NMAP 5.21)

The sniffer NMAP is designed to detect vulnerabilities of a machine on the network by collecting all the information on the MAC address and open ports through which we can make an active attack.
This intrusion is detected by the signature *scan.rules* having as filter rule: *alert tcp $ EXTERNAL_NET any -> $ HOME_NET any (msg: "SCAN NMAP XMAS"; flags: FPU, reference: arachnids, 30; classtype: attempted-recon; sid: 1228, rev: 1;)*



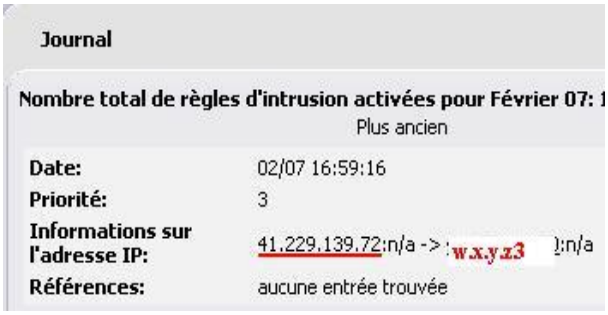

Intrusion detected by SNORT




Attempt blocked by network Controller

### 3.5.3. External intrusion attempt detect ed

This intrusion of type ICMP PING CyberKit 2.2 Windows comes from an external network and was detected by Snort and blocked by the controller of the network. Although this attempt is not very dangerous but it was possible to verify the proper operation of intrusion detection and response of the guardian of the network




The rule allowed the detection of this attempt is included in the Snort signature database with *SID No. 483* and which exists in the file *icmp.rules*. *alert icmp $ EXTERNAL_NET any -> $ HOME_NET any (msg: "ICMP PING CyberKit 2.2 Windows", itype: 8; content: "| AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA AA |", depth: 32, reference: arachnids, 154; classtype: misc-activity; sid: 483, rev: 5;)*

## 4.Conclusion:

To protect a network against attacks including intrusion, we must study its architecture, analyse vulnerabilities, up to date with new threats, a purpose to minimize the risks that may occur. In this paper, we proposed and implemented a solution for securing a network based on intrusion detection systems. We performed several experiments to validate our solution.

## References

[1] Denning D.“An Intrusion-Detection Model.” IEEE Transactions on Software Engineering, Vol. SE-13, No 2, 1987.
[2] ALAN BIVENS, CHANDRIKA PALAGIRI, “networkbased intrusion detection using neural Networks”, 2005.
[3] Hamdan.O.Alanazi, Rafidah Md Noor, B.B Zaidan, A.A Zaidan, “Intrusion Detection System: Overview”, in JOURNAL OF COMPUTING, VOLUME 2, ISSUE 2, FEBRUARY 2010
[4] Botha.M, Solms R, Perry K, Loubser E, Yamoyany G “The utilization of Artificial Intelligence in a Hybrid Intrusion Detection System”, *SAICSIT*, 149-155 2002
[5] Peter Lichodzijewski A.Nur Zincir-Heywood, Malcolm I. Heywood “Host-based Intrusion Detection using Self Organizing maps” *IEEE Communications* 2002.