Network Intrusion Detection in Wireless Network based in Firewall Systems

Hussain Abo Surrah

College of Computers and Information Technology
Taif University
KSA
salama366@yahoo.com

ABSTRACT -**This is the purpose of applying intrusion detection system in firewall to identify the intruder, now a days we have a separate system for finding intruder in wire and wireless networks, however why we do not implement the intrusion detection systems in the firewall[1]. There is different firewall systems which is comes with the operating systems and there is some separate firewall systems to stop unwanted users. This firewall is used for blocking the intruder and we can set the permissions to access in out the network. There major challenges are in wireless network for intrusion detection systems (IDS) which attempt to identify suspected network traffic. Due to the high percentage of intruders alerts will generate by such systems. We present intelligent strategies for reduction of intrusion and infrastructure protection using a firewall in adaptive responses from firewall filters the packets in what we call, network quarantine channels (NQC). The paper is focus on the responses from the packet filters which is collaborate with the NQC to reply to suspicious hosts and they deny access to sensitive data servers in the infrastructure. The firewall packet filters can provide effective intelligent response by to granting access to the normal packets and denying malicious data access to the network, after the identity of the connections are verified through the statistical analysis in the NQC. These effective strategies reduce positives and increases detection capability of the IDS. A firewall is another important part of computer network security in intrusion detection systems; this can help strengthen network securities in all types. However, firewalls are differing from intrusion detection systems largely because they look outwardly for intrusions into a network in- order to stopping them from happening. A firewall intrusion detection system typically acts to prevent unauthorized access to networks. There are treats to the wireless local area networks are numerous and potentially developing. Security issues may occur from configured wireless access points (WAPs) to session hacking to Denial of Service (DoS) can plan a WLAN. Wireless networks are not only suitable to TCP/IP-based attacks native to wired networks; they are also subject to vary of the specified threats. To defend and detection of those threats in WLAN should employed a solution that including an intrusion detection system (IDS) in firewalls [2]. Even organizations without a WLAN are at risk of third party threats and should consider an IDS solution. This paper will describe the need for wireless intrusion detection in firewall provides an explanation of wireless intrusion detection systems, and identify the advantages and lacks of a wireless intrusion detection solution using in firewall [2]. The system can also determine the channel that a packet was transmitted on, versus the channel that it was received on. In addition, the system allows a user to create custom capture filters and attack signatures [4]. Some-times hackers can get in to the network and collapse the systems; there are many ways to prevent the external intrusion in wireless networks so the basic firewall must be strong with good antivirus to prevent.**

Keywords: **Intrusion detection system, Firewall configuration**.

I. INTRODUCTION

An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspected patterns that may indicate a network or system attack from someone attempting to break into or compromise a system [1].

There are several ways to categorize IDS:

1.1 Misuse detection vs. anomaly detection: in misuse detection, the IDS analyze the information it gathers and compares it to large databases of attack signatures. Essentially, the IDS look for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. In anomaly detection, the system administrator defines the baseline, or normal, state of the network traffic load, breakdown, protocol, and typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies [3].

Network-based vs. host-based systems: in a network-based system, or NIDS, the individual packets flowing through a network are analyzed. The NIDS can detect malicious packets that are designed to be overlooked by firewalls simplistic filtering rules. In a host-based system, the IDS examines at the activity on each individual computer or host.

1.2 Passive system vs. reactive system: in a passive system, the IDS detect a potential security breach, log the information and signal an alert. In a reactive system, the IDS respond to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source [3].

Though they both relate to network security, an IDS differs from a firewall in that a firewall looks out for intrusions in order to stop them from happening. The firewall limits the access between networks in order to prevent intrusion and does not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An

IDS also watches for attacks that originate from within a system [3].

An IPS, or intrusion prevention system is used in computer security. It provides policies and rules for network traffic along with an intrusion detection system for alerting system or network administrators to suspicious traffic, but allows the administrator to provide the action upon being alerted. Some compare an IPS to a combination of IDS and an application layer firewall for protection [3]. It is important to understand that most IDS architectural models are based on static, wired networks. These models alone are insufficient to help design IDS in a mobile, ad hoc network environment [6].

II. METHODOLOGY AND APPROACH

Every computer is always at risk for unauthorized access and intrusion; however, businesses with sensitive and private information are at a higher risk. While the occurrence of intrusions may be rare, this can be a costly problem for any size business as confidential and important information may be stolen or destroyed. It makes any organization vulnerable to theft or even legal action. This method can help improve your computer network security by using firewalls intrusion detection systems. Firewalls are set up at multiple levels to provide protection for servers, networks and individual devices [5].

Intrusion detection systems help information systems and networks to prepare for and deal with attacks by collecting information from a variety of network systems and analyzing and monitoring this information for possible security problems [5]. Firewalls are software or hardware based systems that act as a barrier against unauthorized access to a computer system. We can configure and managed firewalls intrusion detection systems for small, medium, and large size companies and organizations. I understand the importance for businesses to operate using fully secured networks. We can utilize our knowledge and experience to ensure your business' network is properly secured and protected from intrusion [5].

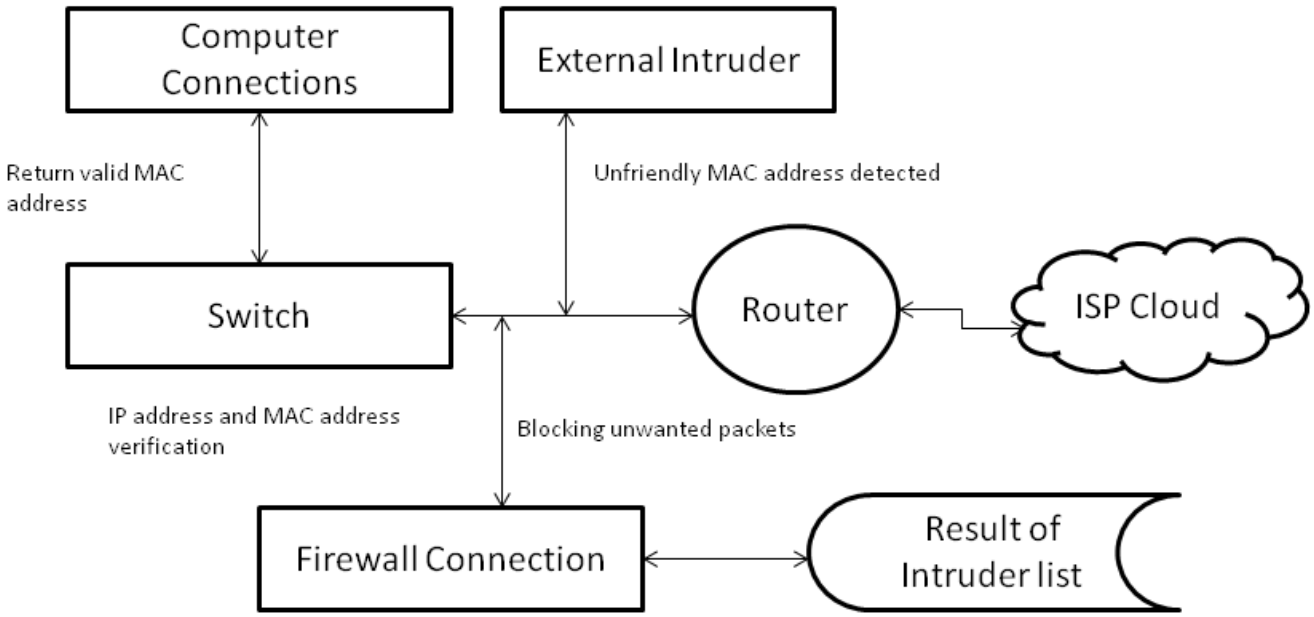

Figure 1 Blocking Intruders

III. IMPLEMENTING INTRUSION DETECTION SYSTEMS

Most of the computer network security services offers for small and mid-sized businesses are to implement and monitor intrusion detection systems. Intrusion detection systems monitor network and system activities in order to prevent attacks and malicious activities that can come from within a network. Typically, intrusion detection systems will notify the network administrator when suspected activity has been detected. In some cases, the intrusion detection systems can take action when problems are detected such as barring a user or IP address from accessing the system [5].As shown in the figure 1 I described the work flow of firewall to protect from the external intruder and unwanted packets.

Intrusion detection systems typically provide the following services:

3.1. Monitoring and analyzing user and system activity

This concept is helping us to monitoring the users in the network; those are trying to do the administration work in their local computer.

Remote server/desktop management tools, such as RDP and Team viewer, are typically used by support and IT professionals to work more efficiently [8].

3.2. Auditing system configurations and vulnerabilities

This is will make sure that we have installed good anti-virus to protect our network and our business. This will audit the performance of configurations and vulnerabilities.

3.3. Assessing the integrity of critical system and data files

The assessment of the systems and network it's depending on files, the integrity critical system has been assessing by scan to find viruses and loss of information.

3.4. Performing statistical analysis of activity patterns based on matching patterns with known attacks

The statistical report for activity of network has been generated from the log table, these information is very useful for find the attackers.

3.5. Analyzing abnormal activity

This case analyze from log to find abnormal activities in network and anti-virus date of expire and some extra details.

3.6. Operating system audits

In this case the network find malwares in operating system then audit the necessary updates which is available on operating systems.

Intrusion protection systems can be a good start to improving your organization's network security. However, these systems do have some limitations such as an inability to compensate for weak identification and authentication mechanisms, the inability to compensate for weaknesses in network protocols, and the inability to conduct investigations of attacks without human intervention. Because of these and the other limitations of intrusion detection systems, it is important to work with an experienced IT company for implementing and monitoring your network security on a regular basis. The Wireless Intrusion Detection System can be used to provide defense-in-depth protection for any wireless local area network [5].

IV. FIREWALL CONFIGURATION SERVICES

When implementing a firewall as part of your network security system, it is important to understand that a firewall must be configured properly in order for it to be effective. Steps involved in proper firewall configuration include setting firewalls to monitor incoming and outgoing packets, utilizing adequate firewall hardware or software for your needs, and standardizing wireless connections on a WPA. experienced IT professionals understand the importance of proper firewall configuration as it relates to network security issues. With all of our computer network security services, we can ensure that your business avoids major security breaches and other network problems in order to keep your business running smoothly [5].

Each node in the network will have an IDS agent running on it all times. This agent is responsible for detecting intrusions based on local audit data and participating in cooperative algorithms with other IDS agents to decide if the network is being attacked [6].

Host-based intrusion prevention system, HIPS is an IPS or intrusion prevention system designed for security over host-based systems where intrusions and infections are dealt with at the individual workstation le network-based intrusion prevention system, NIPS is an IPS or intrusion prevention systems designed for security over network-based systems. Well to provide a more effective level of security [7].

The next-generation firewall is well defined by Gartner as something new and enterprise-focused "incorporating full-stack inspection to support intrusion prevention, application-level inspection and granular policy control" [8]. Most network security vendors are now offering application visibility and control by either adding application signatures to their IPS engine, or offering you an add-on license for an application control modules. In either case, these options are additive to a port-based firewall, and do little to help you focus on the fundamental tasks your firewall is designed to execute [8].

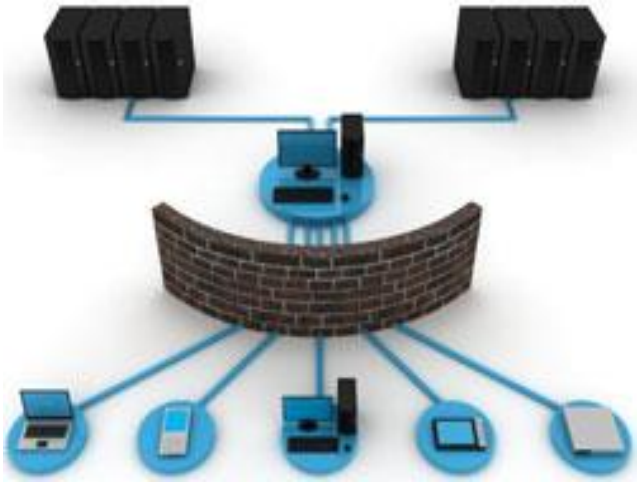

Figure 2: firewall configuration [5].

V. CONCLUSION

This paper presents the design and implementation of wireless network Intrusion detection, the evaluation of research determines to monitor the attacks using firewall, we summarize major contribution and make further work, the software successfully detecting the network intrusion in wireless network, the main advantage of our research to examine the traffic from one channel to other channel.

VI. FUTURE WORK

For future work, we suggest the following issues using firewall for disabled port of the network, for future the current prototype for the further development, we will find new types of attacks in wireless network.

ACKNOWLEDGEMENT

The wireless intrusion detection system research and development authors sincerely thank the anonymous

reviewers whose comments greatly helped clarify and improve this paper.

REFERENCES

[1]. "Defending Yourself: The Role of Intrusion Detection Systems", John McHugh, Alan Christie, and Julia Allen, Software Engineering Institute, CERT Coordination Center,S e p t e m b e r / O c t o b e r 2000 IEEE SOFTWARE.
[2]." Threats to wireless local area networks" Jamil Farshchi, SecurityFocus.com.
[3]."Vulnerabilities in wireless networks and intrusion detection", S L O B O D A N P E T R O V I ´C, Telektronikk 1.2005.
[4].Technology Profile Fact Sheet" Wireless Intrusion Detection System", Reference Number: 1514.
[5].http://www.forwardslashtechnology.com/firewall-intrusion-detection-prevention.html.
[6]. "Intrusion detection in wireless networks" Aparna Vattikonda, Ranjit Kumar Gampa, Vishnu Karunya Isukapalli, Viswanadha Raju Kakarlapudi.
[7]. "Ten Strategies of a World-Class Cybersecurity Operations Center". Carson Zimmerman, 2014 by the MITRE Corporation.
[8].10 Things Your Next Firewall Must Do, 2013, Palo Alto Networks, Inc.