2016

Design of an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) for the EIU Cybersecurity Laboratory

Adekunle Adeyemo
Eastern Illinois University

The Graduate School
EASTERN ILLINOIS UNIVERSITY™

Thesis Maintenance and Reproduction Certificate

FOR: Graduate Candidates Completing Theses in Partial Fulfillment of the Degree
Graduate Faculty Advisors Directing the Theses

RE: Preservation, Reproduction, and Distribution of Thesis Research

Preserving, reproducing, and distributing thesis research is an important part of Booth Library's responsibility to provide access to scholarship. In order to further this goal, Booth Library makes all graduate theses completed as part of a degree program at Eastern Illinois University available for personal study, research, and other not-for-profit educational purposes. Under 17 U.S.C. § 108, the library may reproduce and distribute a copy without infringing on copyright; however, professional courtesy dictates that permission be requested from the author before doing so.

Your signatures affirm the following:

- The graduate candidate is the author of this thesis.
- The graduate candidate retains the copyright and intellectual property rights associated with the original research, creative activity, and intellectual or artistic content of the thesis.
- The graduate candidate certifies her/his compliance with federal copyright law (Title 17 of the U. S. Code) and her/his right to authorize reproduction and distribution of all copyrighted materials included in this thesis.
- The graduate candidate in consultation with the faculty advisor grants Booth Library the non-exclusive, perpetual right to make copies of the thesis freely and publicly available without restriction, by means of any current or successive technology, including by not limited to photocopying, microfilm, digitization, or internet.
- The graduate candidate acknowledges that by depositing her/his thesis with Booth Library, her/his work is available for viewing by the public and may be borrowed through the library's circulation and interlibrary loan departments, or accessed electronically.
- The graduate candidate waives the confidentiality provisions of the Family Educational Rights and Privacy Act (FERPA) (20 U. S. C. § 1232g; 34 CFR Part 99) with respect to the contents of the thesis and with respect to information concerning authorship of the thesis, including name and status as a student at Eastern Illinois University.

I have conferred with my graduate faculty advisor. My signature below indicates that I have read and agree with the above statements, and hereby give my permission to allow Booth Library to reproduce and distribute my thesis. My adviser's signature indicates concurrence to reproduce and distribute the thesis.

Graduate Candidate Signature

Faculty Adviser Signature

Printed Name

Printed Name

Technology

Graduate Degree Program

may 5th /2016.

Date

Please submit in duplicate.

Design of an Intrusion Detection System (IDS) and an Intrusion

Prevention System (IPS) for the EIU Cybersecurity Laboratory

(TITLE)

BY

Adekunle Adeyemo

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

Masters Degree In Science M.Sc.

IN THE GRADUATE SCHOOL, EASTERN ILLINOIS UNIVERSITY
CHARLESTON, ILLINOIS

2016

YEAR

I HEREBY RECOMMEND THAT THIS THESIS BE ACCEPTED AS FULFILLING
THIS PART OF THE GRADUATE DEGREE CITED ABOVE

	/2016.		5/2/16
THESIS COMMITTEE CHAIR	DATE	DEPARTMENT/SCHOOL CHAIR OR CHAIR'S DESIGNEE	DATE
	5/2/2016		
THESIS COMMITTEE MEMBER	DATE	THESIS COMMITTEE MEMBER	DATE
	5/2/2016		
THESIS COMMITTEE MEMBER	DATE	THESIS COMMITTEE MEMBER	DATE

Abstract

Cyber Security will always be a subject of discussion for a long time to come. Research has shown that there is massive growth of cyber-crime and the currently available number of Cyber Security experts to counter this is limited. Although there are multiple resources discussing Cyber Security, but access to training in practical applications is limited. As an institution, Eastern Illinois University (EIU) is set to start Masters of Science in Cyber Security in Fall 2017. Then the challenge is how EIU will expose students to the practical reality of Cyber Security where they can learn different detection, prevention and incidence analysis techniques of cyber-attacks. In addition, students should have the opportunity to learn cyber-attacks legally. This research proposes a solution for these needs by focusing on the design of firewall architecture with an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) for the EIU Cyber Security Laboratory. This thesis explores different up to date techniques and methods for detection and prevention of cyber-attacks. The overall outcome of this research is to design a public testing site that invites hackers to attack for the purpose of detection, prevention and security incidence analysis. This public firewall might empower students and instructors with practical cyber-attacks, detection techniques, prevention techniques, and forensics analysis tools. It may also provide the knowledge required for further research in the field of Cyber Security.

Dedication

I dedicate this thesis to God Almighty for His love for me and to the entire members of my family for their unfailing love, sacrifices, prayers, and support.

Acknowledgements

First, I sincerely thank and appreciate my supervisor Dr. Rigoberto Chinchilla, for his supervision, input, and effort in ensuring that this thesis achieves its aim and set objectives. I appreciate his precious time and commitment to providing critical review and guidance for my thesis. I am also grateful to members of my thesis committee; Dr. Israr Toqeer and Dr. Wutthigrai Boonsuk for accepting to serve on my committee and for providing valuable suggestions for my thesis. My special thanks also go Dr. Wafeek Wahby whose words of encouragement and believe in my abilities cannot be overemphasized. Also thanks to Dr. Odai Y. Khasawneh, who is always asking about my thesis and offering suggestions. I also appreciate Dr. Jerry Cloward for his smiles and readiness to listen anytime I have to talk to him and to the coordinator of my program, Dr. David Melton who is always ready to assist and always play pranks on me anytime we meet.

My gratitude to Randy Ethridge, David Smith and their team at the Information Technology Services (ITS) department for their help in providing Internet resources for the thesis. I am also indebted to Becky Shew at the student services office whose help in ensuring I get the resource I needed was timely.

I thank my family: my mother, Ruth Mogbonjubola Okesooto Adeyemo, my brothers Ipadeola, Banji, Niyi and sisters Bisi, Iyabo for educating me on aspects of both moral and religion, for unconditional support and encouragement to pursue my interests and dreams, even when the interests went beyond boundaries of language, field, and geography. To them I am highly indebted. In addition, I thank my nieces Mayowa, Seyi,

and Sayo for believing so much in their uncle and I also thank my cousin Nike Oladipo. I also thank my in-laws Jumai, Bola, Toun, and Shina.

I cannot also quantify the encouragement and support I received from Dr. Victor Ola-Akande, TPL Adebisi Adedire, Dr. Lakin Adeshina, Bukky Falomo, Oluwaseun Fatoba, Ogunyemi Mayowa, Seyi Soyinka and Kemi Soyinka. I will forever be grateful to a friend, a sister and a confidant, Oyindamola Idowu for her magnanimous contributions towards the success of this journey. I am also grateful to her husband Ola and their son Ayomi.

My gratitude also goes to Adeyemi Oluwadayo, Omolayole Ige, Ekundayo Simon, Opeyemi Onifade, Fabuluje Abiodun, Fatoba Wale and Wunmi Fatoba for their prayers, encouragement and support for me. I equally appreciate and say a big thank you to Beluchukwu Ebede for his help and spending hours with me in the laboratory during this research. To all my friends, I cannot list all your names but I appreciate you for making my experience at EIU a memorable one. Lastly, I appreciate everyone that has influenced my life.

Table of Contents

List of Figures

CHAPTER ONE

1.0 Introduction

The increasing nature of cyber-attacks is very worrisome and poses a major threat to both economic and social development. Between the year 2008 and 2013, the number of cyber threats increased from 2.37 million to 5.2 million. Also, there is an increase of over 100,000 new malicious programs daily from the 200,000 daily reported in 2012[1]. As reported by Net Losses: [2], cyber-attacks will continue to grow as more businesses go online and as we gravitate towards "Internet of Things". In addition, cyber-attacks have equally grown to become more sophisticated in nature.

The sophisticated nature of cyber-attacks on computer networks these days has rendered traditional firewalls inefficient; even the most complex ones are insufficient in protecting attacks from penetrating computer networks [3]. As a result, there is a need for better and more effective solutions for detecting and preventing attacks. The subject of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) has drawn the attention of both the academic and corporate world. An IDS is mainly a defensive mechanism that gives alerts, and log the information when it detects an attack or any malicious activity in a passive system, while in a reactive mode, the IDS can log off the malicious user or issue a command for the firewall to reconfigure itself to block such traffic from malicious user [4].

However, taking a step further, a more proactive approach is needed which not only detect but can also prevent the attacks from invading the computer networks. Such a device is referred as an IPS, and according to Conklin and White [5], "IPSs are merely expansions of existing IDS capabilities". They argued that a true IPS must be able to block, reject or redirect traffic in real time. An IDS that monitors a single host system is a Host Intrusion detection Systems (HIDS) while IDS that monitors an entire network is a Network Intrusion Detection Systems (NIDS) [42]. In this research, IDS is conceptualized as an NIDS.

The detection, sensor monitoring, and alert mechanism techniques of an IDS help also the IPS to discover new patterns of attack or malicious behavior. The IDS evolution allows both the IPS and IDS to share what they have learned with other connected networks or systems, thus increasing its effectiveness against attacks [6][7]. They also prevent malicious activities from bringing damage to the network [8]. Hence, the deployment of modern IDS and IPS in a network offers an advantage of dual intrusion detection and prevention. The IPS/IDS combination provides the best security architecture for an in-depth defense [9].

Some literatures refer to the combination of IDS and IPS as Intrusion Detection and Prevention System (IDPS). Korčák et al [10] research on IDS/IPS for a WIFI networks environment shows that there was about 95% decrease in the number of attacks compared to a network without the deployment of their proposed IDPS solution. Therefore, it may be concluded that the security been provided by an IDS/IPS security system could be a discouraging factor for some hackers to launch attacks, and most hackers would rather launch attacks against most vulnerable networks.

1.1 Justification of the Study

Kelvin G. Coleman [11] reported that Casteel the manager of SCADA and security business development at Emerson Process Management said: "we would never be able to completely get ahead of cyber criminals perpetuating cyber-attacks". If hackers would not rest, then it is very reasonable that researchers continue to research, design and implement security techniques to equip people on combating security attacks. Also according to McGettrick [12], the continuing expansion of technology invariably leads to continuing growth of cyber-attacks, which also calls for the need for more skilled people to combat this menace. The available pool of people with strong cyber security skill sets is quite low, thereby resulting in difficulties as private sectors and government agencies such as United States Department of National Defense and Department of Homeland Security jostle to engage competent individuals to fight cyber-crime [12].

Educational institutions, especially the universities, should be the ones providing leadership when it comes to combatting cyber-attacks. In designing Cyber Security curriculum, both theoretical and practical knowledge are essential to produce individuals that are able to understand the nitty gritty of cyber-attacks and how they should be prevented, hence, able to sufficiently get above the hackers game but quite often, the academic environment separates these two from another [12]. In the area of fighting cyber-attacks, theories are good as they provide the basic underlying principles; however, these are usually not sufficient for employment. Providing laboratory training would further reinforce and expose students to several technologies used by most organizations [13].

It is possible that many industries have been disappointed with the practical experience of students graduating in this field, hence, the reason they demand extra qualifications in the name of certifications during employment process [14]. In addition, according to the

Change the Equation (CTEq), a methodology that aims at improving the quality of STEM program in the United States, there are shortages of STEM talent. The reason is that fewer people are pursuing degrees in the areas of Cyber Security, computer science and IT related courses, and these degrees rarely encompass recent Cyber Security contents [14][15].

1.2 Overall aim

This study will propose a solution for the new Master of Science program in Cyber Security at EIU: To provide students with practical cyber-attacks detection, prevention and incidence analyzes experience and skills that will bridge the gap between academic education and practical training.

1.3 Objectives

1. To design a firewall architecture with an Intrusion Detection System (IDS) and Intrusion Prevent System (IPS) for the Cyber Security Laboratory at EIU.
2. To use the developed firewall architecture as a public testing site by inviting hackers to attack the system in other to analyze hacking activities.
3. To provide the prospective MSc Cyber Security students at EIU the practical realities of cyber-attacks, threats analysis, detections and preventions in other to bridge the gap between theoretical knowledge and practical training.

1.4 Hypotheses

The intent of this research is to ascertain the following:

It is possible to:

1. Develop firewall architecture with an IDS/IPS that would offer a high resiliency to cyber-attacks within the academic setting of the EIU telecommunication's laboratory.
2. Provide students with real cyber-attacks experiences in order to empower them to research and to improve Cyber Security systems based on the EIU Cyber Security laboratory experience.
3. Operate a physical Cyber Security laboratory with intrusion detection and intrusion prevention capabilities that attract prospective students to the MSc. program and in turn give EIU recognition among schools offering Cyber Security programs.

1.5 Delimitation

This research would strictly provide a firewall architecture design with an IDS/IPS for the purpose of intrusion detection, prevention and security incidence analysis, and would not discuss the speed or the full implementation of the designed system. The implementation of a honeypot is out of the scope of this research work. In addition, this research will not focus on detecting or preventing internal attacks. This research design would serve as a public testing site that invites outside hackers to launch attacks. It is possible that hackers launch sophisticated attacks that can break the security of designed system. However, it is also very possible that we catch/log all the activities that these hackers did to break the system, which is ultimately one of the goals of this research

CHAPTER TWO

2.0 Literature Review

This chapter provides background information and a theoretical justification for the firewall architecture with an IDS/IPS for the MSc. Cyber Security at EIU.

2.1 Cyber Security and its Challenges

Fisher [16] defines Cyber Security as a way of protecting and securing information and communication technology systems. The advent of information communication technology and its growth has continuously raised concern for data privacy protection, authorized information sharing and data integrity [16]. According to Baylon [17], the cyberspace users have tremendously increased and this has incidentally resulted in its continuous expansion, which has had a consequential reduction in the cost of Internet access. Baylon [17] argued further that cyber criminals have taken advantage of this growth to create cheap software which basically requires no technical know-how for whoever, to be able to launch cyber-attacks. Based on these arguments, one can conclude that cyber-attacks might not be on the decline anytime soon. In addition, the heavy dependent on technology and the Internet for the continuous sustenance of businesses, government, and individual needs has opened up new vulnerabilities and opportunities for hackers to further their criminal acts [18].

The growing nature of the electronic world is characterized by different networks and interconnected devices, the need to store and interact with a huge amount of data especially via an online platform and the cloud has resulted into the complex nature of the computer networks [18]. As a result of this complexity characterized by physical, logical and social layers, managing Cyber Security has been difficult as vulnerabilities are not easily detected, and attackers are able to exploit these vulnerabilities to launch attacks in an invisible manner [19][20]. In recent times, the Internet of Things (IoT) has been one of the major subjects in the IT world. With the reality of IoT, we can expect more complexity, as more devices would be interconnected. Folk et al [20] put the number of these devices at over 50 billion, and with this comes unimaginable exploits, vulnerabilities, and attacks. In a research conducted by the office of the privacy commissioner of Canada [18], by the year 2017, the total number of operational mobile devices would outnumber the population of the world. This fact supports the above security concerns. According to a research conducted by Check Point software Technologies Limited, there is a growing security concern with mobile devices [21]. The report shows that there was 63% increase in security risks of Android mobile platform [21].

The Cyber Security war will be difficult to defeat, as even the custodians of the law have found it to be a weapon to achieve illegal gains. This is evident as some states often times engage the services of hackers in order to accomplish evil agendas [22]. It is very alarming to see different countries using sophisticated malware, spear phishing and denial distributed of service against one another [23]. I perceive this as some sort of cyber war or cyber terrorism, which definitely would be deadlier than terrorism. In 2011, the pentagon noted that any act of attack or sabotage arriving from another country is a possible act of war [24]. Miller [25] described this as the militarization of cyber-attacks using highly trained hackers to access critical resources and information. In addition, the organized nature of cyber-crime has made the fight against cyber-crime difficult.

According to a review in 2012, organized hacking constituted 80% of cyber-crime activities [22]. In 2014, a first of its kind, a massive and sophisticated attack was launched against Sony. This level of attack reflects the highly and strategical organizational structure of an organized attack attributed to the Korean government [23][24]. Theophany [24] referred to this nature of attack as information warfare, that is, one that involves countries, government and big corporations in a bit to disrupt national security. Ferrillo [25] pointed to a recent release by FBI stating that China alone accounted for 95% of data breaches coming from foreign countries.

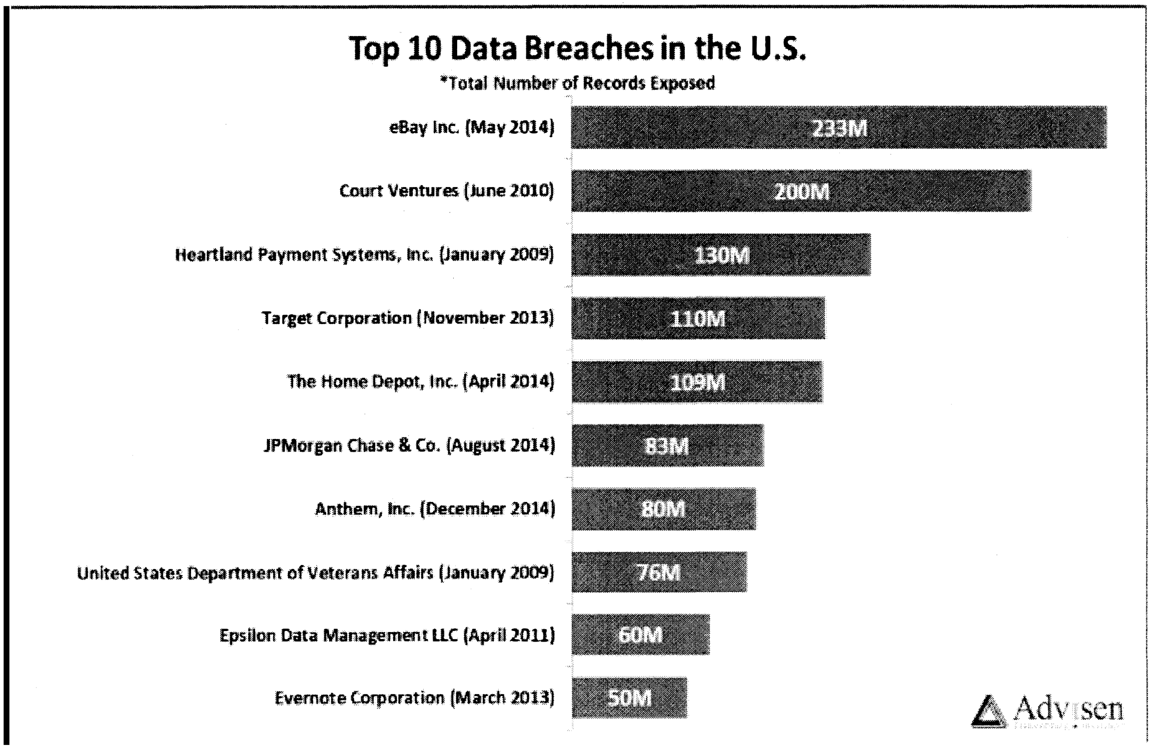


Figure 2.1: Showing the Top 10 Data Breaches in the U.S

Taking a critical look at data and figures resulting from successful cyber-attacks and data breaches, one can easily conclude that fighting cyber-attack would require huge financial budgeting and continuous spending. In Figure 2.1 above, as reported by Ferrillo [25], one can conclude that big corporations and companies would continually experience attacks. The 2015 information security breaches survey carried out by PWC in conjunction with info security, shows that 90% of large organizations representing about 11% from the previous year's breaches and about 74% of small businesses representing about 23% increase from the previous year's breaches were victims of cyber-attacks [26]. The significance of this is very symbolic, meaning that if these breaches continue at this rate, businesses would continue to incur heavy cost and reputation damages. In 2014 alone, large organizations lost to security breaches summed up to an average range between $2.05 million to $4.5 million [26]. In a world development report, Bauer & Dutton reported the global cost implication of cyber-crime to be at $445 billion [27].

2.2 Major Cyber Attacks

Hackers have developed several mechanisms ranging from simple to sophisticated techniques to perpetuating their criminal acts. In addition, the majority of them, leverage on the loopholes found in some of the hardware and software components of the interconnected network systems. Jun et al [23] noted that the biggest and the most commonly exploited platform for Cyber Security breaches is the point-of-sale (POS). Jun et al [23] also stressed that POS are basically attacked by gaining access to the credit card processing system of a retailer and installing several variants of malware on it, which usually goes unnoticed for a longer period of time. Malware's invisible capabilities make them unsuspicious spies on computer and network resources [28]. This malware does manifest as viruses, worms, spyware, adware, Trojan, and bots. Miller [29] described another form of attack called advanced persistent threats that has been around for long but have gained more attention due to the consistent changing sophisticated nature of cyber-attacks and the fast changing nature of the threat actors behind these attacks.

In the Fortinet white paper titled “anatomy of botnets”, the author identified distributed denial of service, spamming, financial fraud, search engine optimization poisoning, pay-per-click, cooperate and industrial espionage and bitcoin mining as several techniques hackers deploy in using botnets to generate money [30]. After a successful installation, the working operation of a botnet is such that it creates a backdoor, an avenue it uses to communicate or transfer stolen sensitive information and other details used to identify the infected system to its master [30]. Kamal et al [28] stressed that bots are the greatest threats and risks to users, computers and networks in recent times, because of their highly destructive nature. According to a white paper by McAfee, malware can exhibit polymorphism characteristics when hackers designed them to exist in a different form via regular updates, thereby making it difficult to be detected by signature updates techniques [31].

SQL injection attacks on web applications operated by retail stores are quite popular owing to the sensitive information in their database [25]. Different services like the emails, e-commerce, social media, television media that majorly use these applications to service their teeming clients are the major target of SQL injection attacks. SQL injection attack, if successful, can make an attacker bypass authentication, evade detection, perform data modification and extraction amongst other things, and these explain why they are very popular [32]. It has grown and become one of the key attack mechanisms of hackers, that the Open Web Application Security Project (OWASP) rated it number one web application vulnerability in 2013 [33].

Another dreaded attack is the zero day attack. A zero-day attack is an exploitation of vulnerability also referred to as a hole in software [25]. This form of attack is deadly because there is no way to protect or defend against this nature of attack [34]. In 2010, windows operating system, Adobe reader, and Adobe Flash Player were major vulnerable victims of the 14-day zero attack that made the high-profile attack using Stuxnet worm and Hydraq Trojan to be successful [34]. Egelman et al [35] focused on explaining the new security paradigm of zero-day exploits markets and raises an argument for and against this new paradigm shift. They concluded that these markets have gained so much popularity and attention and thus have consequential implications on the software manufacturing companies.

Hedge [36] identified Mac (MAC) spoofing as one of the major causes of denial of service attacks (DoS), man in the middle attack, dynamic name service (DNS) attack and address resolution protocol (ARP) poisoning. Man in the middle attack gives listening functionality to an intruder and allows such an intruder to listen to every communication traversing the network. DoS take advantage of the weaknesses of the IP protocol stack to disrupt the flow of traffic or services in a network [37]. Farraposo [37] categorizes DoS attack into normal DoS attack if attacks originate from a single computer system and distributed denial of service (DDoS) if attacks originate from multiple computer systems. A DNS attack can be launched indirectly or directly, an indirect attack is launched by registering a domain name deliberately for the purpose of stealing victim's identity and redirecting traffic [38], while a direct attack executes against DNS infrastructure using DoS, DDoS, and DNS cache poisoning, the later redirects legitimate traffic to hackers' websites [38]. Gangan [39] mentioned that ARP cache poisoning and session hijacking are causes of man in the middle attacks. Hackers use different tools such as Cain and able, Ettercap, Dsniff, etc to update an ARP cache table in order to redirect ARP responses to themselves and then be able to extract the necessary information that is needed to further perpetuate crime [39]. Session hijacking attacks an application layer by taking control of the HTTP session to obtain information about session ID and at the network layer of the OSI model by intercepting communication between the client and the server, leveraging on the unawareness and non-security consciousness of users [40].

2.3 Different Techniques to Fight Cyber Attacks

There are several techniques or technologies that are always been deployed by the government, cooperate bodies and individuals in order to fight cyber-attacks and keep their network and resources save. A brief review of some of these technologies is given below.

2.3.1 Firewall Technologies

Tharaka et al [41] pointed out that a firewall does not necessary have the capability to handle or process malicious traffic but a combination of different firewall technologies may prove quite successful. They lamented the limited research activities on the subject of firewall technologies. A firewall filters packets separating the authentic ones from the malicious ones and then blocking the malicious ones. Tharaka et al [41] explore the combination of Network Address Translation (NAT), Virtual Private Network (VPN) and the packet filtering functionality of a firewall to propose a defense against cyber-attacks. NAT allows addresses to translate to another different address entirely. An example, private IP addresses translate to public IP addresses. This concept helps to hide private IP addresses from the public. It could be a one-to-one NAT or a dynamic NAT, where multiple IP addresses translate to a single IP address. In addition, the VPN is a very good secure point of communication, as it builds a tunnel, as a channel of communication and encrypting the traffic traveling through it using the most common form of encryption protocol like IPsec [42]. The firewall also provides the concept of security zones, where different resources could be placed on different zones based on how important they are, usually, the demilitarized zone (DMZ) houses the public webserver, while the very important company's information are kept in the trusted zone, and the access to the public network is kept in the untrusted zone [42].

Despite the security capability of firewalls, events, antecedents and research have proven that they would not be capable of solving all security issues and they might not be able to stop the new breed of sophisticated attacks. In lieu of this, Chopra [43] proposes the concept of distributed firewall architecture in order to mitigate sophisticated attacks. Chopra's research concluded on the note that distributed firewall techniques would create endpoint protection and at the same time enforce domain security using language and distribution policy control in conjunction with certificates for identity management of the domain members [43]. A report by Rajeswari [44] states that firewalls ability to serve as the first line of defense on a local area network (LAN) against attacks are limited to being able to watch or detect any malicious traffic coming from a Wi-Fi enabled device that is behind the LAN. The reason given for this is that firewalls would usually perform reverse tunneling, a process that allows devices to make outbound connections through a firewall.

Conklin et al [42] defined a perfect firewall as one that would not allow the passage of malicious or unauthorized packet. In the real world of security, I doubt if we would ever have a perfect firewall that is not susceptible to compromise. Although to a large extent, with constant monitoring of the firewall and proper configuration of security policies, firewalls could perform at their best. Firewalls do not perform filtering or check on traffic by default, they follow some sort of security policies configured by a network or systems administrator. Firewalls perform the function of traffic filtering following security policies configured by network administrators, how well these firewalls perform filtering is dependent on how well the security policies are configured [42].

2.3.2 Intrusion Detection Systems (IDS)

The awareness about the difficulty in achieving a perfect security of network resources must have given birth to the idea of detecting network intrusions either before attacks take place or after it has taken place. Patil et al [45] described an Intrusion Detection System (IDS) as a system or mechanism that identifies malicious packets or traffic that are both known and unknown. Conklin et al [42] define an IDS as a system that triggers an alarm when it sees an anomaly. In reality, triggering an alarm might not necessarily be indicative of a threat or attack. The administrator could further tune the IDS to reduce the rate of false alarms. Patil et al [45] in their research were able to show a reduction of about 10.02% in the false alarm rate of an IDS that uses clustering and classification hybrid techniques. Conklin et al [42] described in detail the workings of an IDS, the IDS uses traffic collectors to acquire traffic or packets and send them it to the analysis engine which inspects the traffic to see if there are known patterns of malicious traffic when compared to the traffic signatures that are in its database, and it finally passes the outcome to the user interface and report it appropriately.

In their work, Cepheli et al [46] proposed a hybrid intrusion detection framework to combat distributed denial of service attack (DDoS). They leveraged on both the anomaly and signature detection capability of an IDS to enhance the effectiveness of detection of DDoS attack. Das and Sarkar [47] gave a clear distinction between a firewall and an NIDS as many often regard them to be the same. They stated that firewall basically just stands as a guard that control traffic base on rule sets while NIDS is able to detect what is going on the inside of a network. Although they were quick to also point out that NIDS is not able to scan encrypted network traffic just in the same way a firewall could not as well [46]. Besides being able to identify and detect DDoS, Conklin et al [42] said the NIDS is capable of detecting other attacks such as port scans or sweeps, the presence of malicious content on data payload, Trojans, viruses, worms, tunneling, and brute-force. In another research conducted by Alkasassbeh et al [48], they incorporated different techniques such as multilayer perceptron (MLP), Naïve Bayes and Random Forest to improve the detection capability of an IDS, and they concluded that implementing the MLP delivered 98.63% detection accuracy.

The changing nature of attacks spurs researchers to constantly research techniques that can keep up with this development. Bini et al [49] described such techniques, namely; (i) "Data mining & forensics": an advantage of information in a repository or database to analyze attacks. (ii) "Intelligent agent and mining": intelligently learn new signature to detect attacks, a technique they claim reduces false positive and false negative, (iii) "Genetic algorithm": working is based on heuristic search method and (iv) "Fuzzy logic based alert optimization engine": an alert re-scoring technique that leads to a further reduction in the number alerts. They concluded that combining all of these techniques would result in more effective IDS. Another key thing to be considered is the placement of an IDS in a network. As shown in Fig 2.2 below, Conklin et al [42] described that placing an IDS before a firewall would make it see every traffic coming through the firewall and as such would report every alarm generated by itself and the firewall, hence overwhelming the administrator of such network with a huge number of alarms.

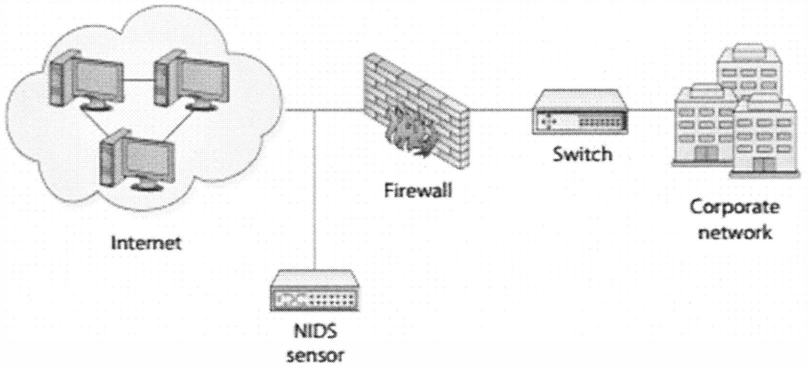


Figure 2.2: NIDS sensor placed before the firewall

Another option is shown in Figure 2.3 below, Conklin et al [42] explained that placing the IDS behind the firewall would reduce the huge alarm effect created in Figure 2.2 because it prevents the IDS from seeing attacks coming directly towards the firewall.

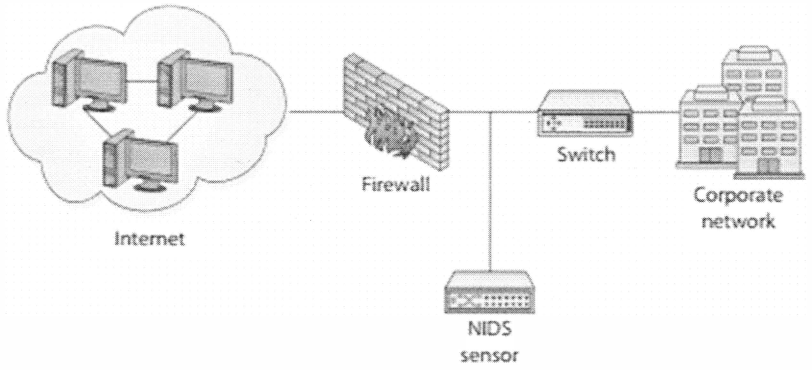


Figure 2.3: NIDS sensor placed behind the firewall

2.3.3 Intrusion Prevention System (IPS)

A modern intrusion prevention system could perform both functions of detecting and preventing malicious traffic as traffic traverses on a network, thereby making it an intrusion detection and prevention systems (IDPS) [47]. The different challenges such as speed, performance, scalability, flexibility and inability to proactively prevent malicious contents led to the development of such modern IPS [47][50]. An IPS is most effective when it can inspect protocols and analyze them. As an example, it might perform HTTP protocol inspection in order to be able to detect and prevent the popular URL encoding evasion technique [42]. Unlike the IDS, the IPS can perform a content inspection on traffic with the TLS protocol encryption, decrypt such traffic and take a decision on whether to allow it or not [42]. According to Korčák [10], an IDPS deployed to mitigate against DoS and ICMP flood attacks proved to be effective as it reduces traffic originating from an attacker by 95%. This shows the potential of an IPS system.

Kaur & Dhingra [51] proposed an algorithm for an IDPS in preventing SQL injection attacks against a database system by checking all database transactions before they are finally committed in order to prevent malicious transactions from being committed. In another research work, Ammad & Laiq [52] proposed a real-time IDPS that uses the Kali Linux operating system, an NIDS, and an IPS that blocks malicious traffic detected by the NIDS. This technique definitely offers a double detection advantage because the IPS also have the capability to detect before it prevents. This is a good way to affirm the integrity and accuracy of the NIDS and IPS that make up their design. Also critical to the success of an IPS is the ability to place an IPS inline in order for all traffic to flow through it and its ability to detect and stop against DoS attacks using rate-based monitoring even while being in the inline operation mode [42]. Intrusion prevention seems to be the way to go in safeguarding network resources. Holland & Shey in their publication forecasted that there would be 5% to 10% increase in intrusion prevention systems [53]. Although they pointed out that this prevention should not be limited to prevention techniques that are only signature based, but also endpoint protection and identity management technology that can identify even a hacker's infrastructure while offering protection.

2.4 The Need for Cybersecurity Knowledge

Despite the constantly developed techniques to combat the menace of cyber-attacks, there seems to be a gap in knowledge or the expertise required to complement these technologies. Most of these technologies still need human Cyber Security experts to configure and monitor these devices for optimal performance. According to a report by the Institute for Information Security & Privacy (IISP), there is a shortage of about one million information security specialists, and the worrisome thing about this is that the current trend does not guarantee that this problem would receive an immediate solution [54]. The report further stated that by 2020, there would be a shortage of 1.5 million workers with Cyber Security knowledge or expertise [54]. This is very alarming, and it raises a very serious concern. If winning the cyber war is necessary, then sophisticated technology to fight Cyber Security attacks and challenges, must continue to grow, as well as the number of Cyber Security experts. The same report says that there is no extensive class time in Cyber Security topics. Although in a separate report, Baeur & Dutton [27] reported that there has been an effort in some Northern American and Western European science departments to increase cyber learning and yet this is not enough to meet the global need.

The gap in knowledge or the required expertise in the field of Cyber Security forms the basis for this research work. A report by ACM stressed that Cyber Security as a discipline is lacking the necessary skills [55]. In the same report, a recommendation was made that Cyber Security at master's level should receive encouragement to attract prospective students to the field, and encourage professors to take an interest in embarking on Cyber Security projects. There should be aggressive Cyber Security research laboratories all over the world in order to keep up-to-date with current Cyber Security challenges and attacks. In reality, we probably do not need every graduate in technology or computer engineering to become Cyber Security experts, but we do need an appreciable number of graduates with such knowledge. This research aims to design an IDS/IPS system within firewall architecture in order to serve as a learning platform for students enrolling for the masters in Cyber Security program at EIU. This research work would have its webserver public IP address exposed to the public, and hence, it will be able to receive real attacks from external networks, hence student might learn with real and simulated cyber-attacks rather than only simulated laboratory created attacks.

CHAPTER THREE

3.0 Design Methodology

This chapter describes details of the methodologies and techniques deployed in order to achieve the objectives of this research.

3.1 The Topology of the Design

Figure 3.1 below depicts the design, which is reflective of a layered security approach characterized by different security devices with the sole aim of creating a strong defense in depth mechanism [42]. Security should be developed with the total awareness of the consequences of a single point of failure. Conklin et al [42] stressed that other security devices that form a whole security architecture could complement the inadequacies of a failed security device. Conklin et al[42] went further to advocate that network security systems or architecture should have the following techniques or methods: routers, firewalls, network segments which can also be referred to as perimeter security, IDSs, encryption, authentication software, physical security and traffic control to achieve layered security. According to Cleghorn [56], defense in depth would deter a casual attacker and a skilled hacker that lacks the continual motivation to perpetuate evil agenda as a result of several obstacles by different layers of security that needed to be overcome, and also prevent the invasion of automated attacks usually run by software programs targeted at public facing webservers.

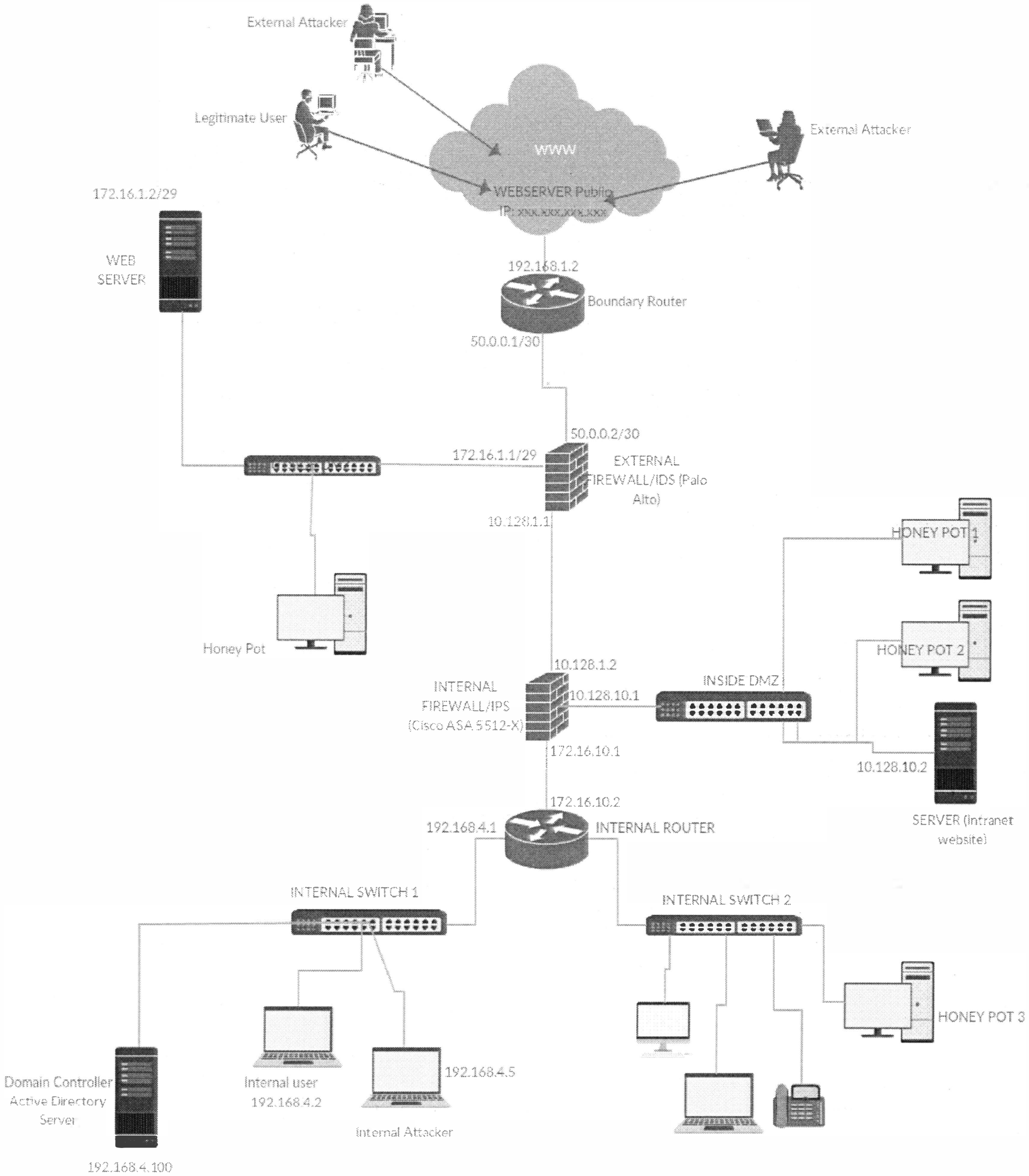


Figure 3.1: IDS/IPS design topology for EIU Cyber Security Laboratory

3.2 The Router

In this research work, the Cisco router 1941W is used. The Cisco 1941W has the capacity to deliver secured data and great mobility. It comes with two integrated 10/100/1000

Ethernet ports. In this topology, the cisco router provides the following functions:

3.2.1 The Cisco Router as a Boundary Router

The final essence of this research is to connect the developed design to an external network or to Internet in order for traffic to flow to and fro the external networks. In order to fulfill this, a router is needed to process and route traffic into the designed network, and also to process and direct traffic to the outside when originated by an inside user. As shown in Figure 3.1 above, the Gigabit Ethernet interface 0/0 (G0/0) connects to an ISP that provides Internet service for the designed topology. This interface plugs into a Cisco Bridge that connects wirelessly to a Verizon wireless hotspot for the purpose of Internet access. The Interface on the router is configured as a dynamic host configuration protocol client, which allows the router to automatically receive an IP address from the Verizon wireless through the Cisco Bridge connected to it.

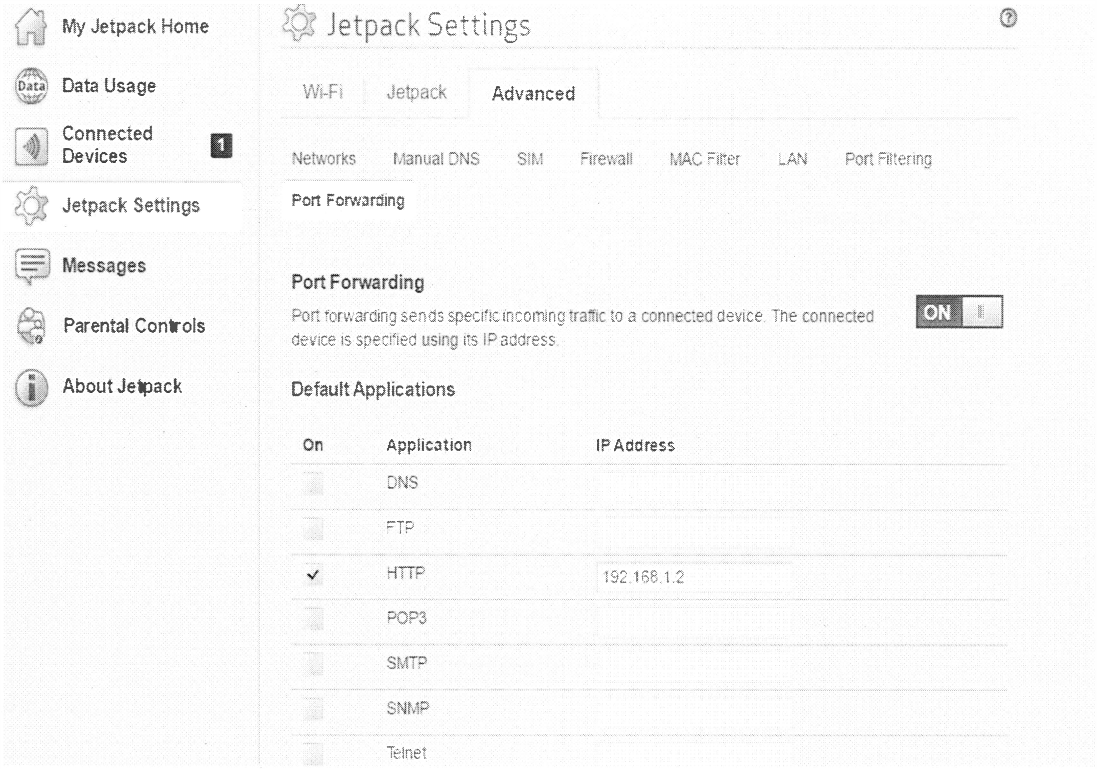
A network device would need a public IP address in order for it to be able to communicate with Internet. This means that Gigabit Ethernet interface 0/0 (G0/0) of the router needs a public IP address, but in this case, the Verizon hotspot assigned a private IP address to it in the range 192.168.1.0 subnet and through the process of network address translation (NAT), translates the private IP address to a public static IP address. NAT translate private IP addresses (non-routable) into public (routable) IP addresses and in doing that, it shields external network or external users from knowing the private IP addresses, thereby providing a form of security [42]. The NAT technique used by Verizon is referred to as port address translation (PAT) as it basically translates all the addresses in the 192.168.1.0 network into a single public IP address that would be used by any of the private IP addresses to get on the Internet. On the same router, the Gigabit

Ethernet interface 0/1(G0/1) is configured with a private IP address in the range 50.0.0.0/30 network. This interface connects directly to the Firewall/IDS.

3.2.2 Port Forwarding to the Webserver

The architecture of this design is such that a webserver is on the external DMZ of the network and would have a separate private IP address that is not known by the external users but has a public IP address representation. Users from the outside wanting to interact with this webserver would do so by sending traffic to the public webserver IP address. In order for the traffic sent to the webserver public address to hit the webserver on the inside of the network, the traffic would have to be in a format that the webserver would understand. Security is at the heart of the design hence, the webserver would only respond to a request or traffic coming from an IP address in its subnet range. In order for the traffic originating from the outside or Internet to communicate with the webserver, the following would have to take place:

1. Internet traffic destined for the webserver will first go to the webserver's public IP address.
2. Then this traffic forwards to the router's G0/0 interface. This is possible with the concept of port forwarding, directing Internet originating traffic to G0/0. In Figure 3.2 the Verizon Jetpack hotspot forwards traffic from Internet through port 80 to the IP address 192.168.1.2, which is the IP address on G0/0 of the router's interface.



Port Forwarding

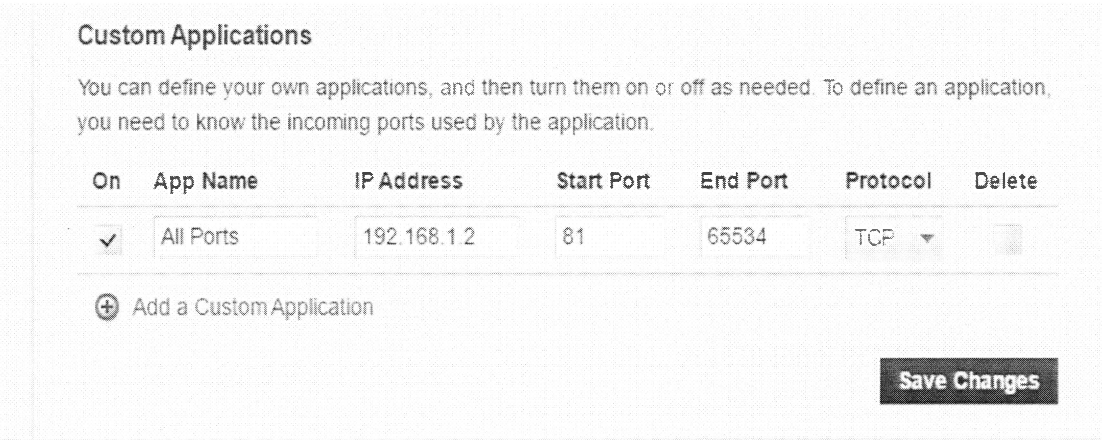
Port forwarding sends specific incoming traffic to a connected device. The connected device is specified using its IP address. ON

Default Applications

On	Application	IP Address
	DNS	
	FTP	
✓	HTTP	192.168.1.2
	POP3	
	SMTP	
	SNMP	
	Telnet	

Figure 3.2: Port Forwarding Configuration

Since the purpose of this design is to allow students experience different real cyber-attacks, Figure 3.3 shows how to allow traffic via a different range of ports.


Custom Applications

You can define your own applications, and then turn them on or off as needed. To define an application, you need to know the incoming ports used by the application.

On	App Name	IP Address	Start Port	End Port	Protocol	Delete
✓	All Ports	192.168.1.2	81	65534	TCP	□

Figure 3.3: Showing configuration to open many ports

3.2.3 NAT Configuration and Filtering on the Boundary Router

The Gigabit Ethernet interface 0/1 (G0/1) of the router is configured with the IP address in the subnet 50.0.0.0/30. The G0/1 directly connects to the firewall/IDS. In order for traffic directed to the G0/0 interface of the router to go into the webserver, the following configuration is required on the router:

1. Network address translation is configured on the router for both interface G0/0 and G0/1 of the router to direct traffic in and out respectively. The IP address 192.168.1.2 on the G0/0 translates into the IP address 50.0.0.2 of the firewall/IDS that connects directly to the router.
2. The NAT inside command is configured on the G0/1 interface of the router while the NAT outside command is configured on the G0/0 interface of the router.

3.2.4 Access List Configuration to Prevent IP Spoofing

An attacker can pretend to be part of an internal network by trying to use an inside private IP address to communicate with internal users and resources. In order to prevent this, an access list is configured on the router to filter traffic and deny any traffic originating from non-routable IP addresses. Abderrahim [57] in his research termed this technique as network ingress filtering. Examples of IP addresses to be blocked are 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,127.0.0.0/8,169.254.0.0/16,224.0.0.0/4 [58]. All of these non-routable addresses are blocked by access list configuration on the router.

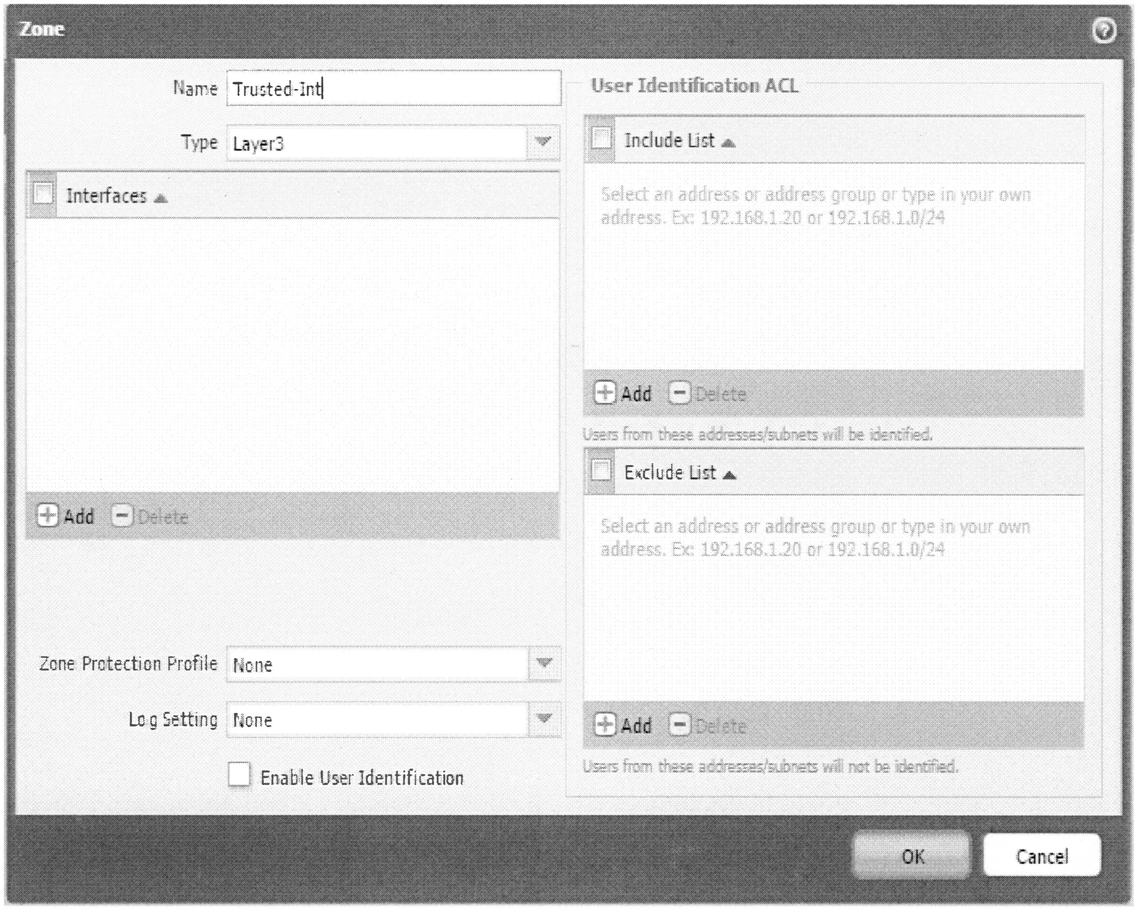
3.3 The Firewall/IDS

The Firewall/IDS in the design is a Palo Alto PA-200 device. The PA-200 has the capability to perform the function of both traffic filtering and an IDS. It has the ability to filter URL and block malicious websites. In addition, it comes with antivirus functionality that detects viruses and spyware. In order for this PA-200 to fulfill its purpose in this research work, the following configurations were set on it:

3.3.1 Zones and Interfaces configuration

There are three different zones configured on the Palo Alto. The security needs of the firewall/IDS design led to the creation of the three zones. The Ethernet interface 0/1 (E0/1) was configured as the untrusted zone because it connects to the boundary router, the Ethernet interface 0/3 (E0/3) as the DMZ zone and the Ethernet interface 0/2 (E0/2) as the trusted zone. The idea behind this network segmentation is to separate the webserver and place it on a DMZ to ensure that no traffic from Internet crosses that zone to the trusted zone. Figure 3.4 shows zone configuration while Figure 3.5 & Figure 3.6 show interface configuration. E0/3 is configured with an IP address in the subnet 172.16.0.0/24, the E0/2 is configured with an IP address in the subnet 10.128.10.0/24 and E0/1 is configured with an IP address in the subnet 50.0.0.0/30. The following steps show how to configure both zones and interfaces:

1. On the Palo Alto administration interface, click on the Network tab
2. Click on the zone on the left side panel
3. Click the add button to create a zone



Name: Trusted-Int

Type: Layer3

Zone Protection Profile: None

Log Setting: None

□ Enable User Identification

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

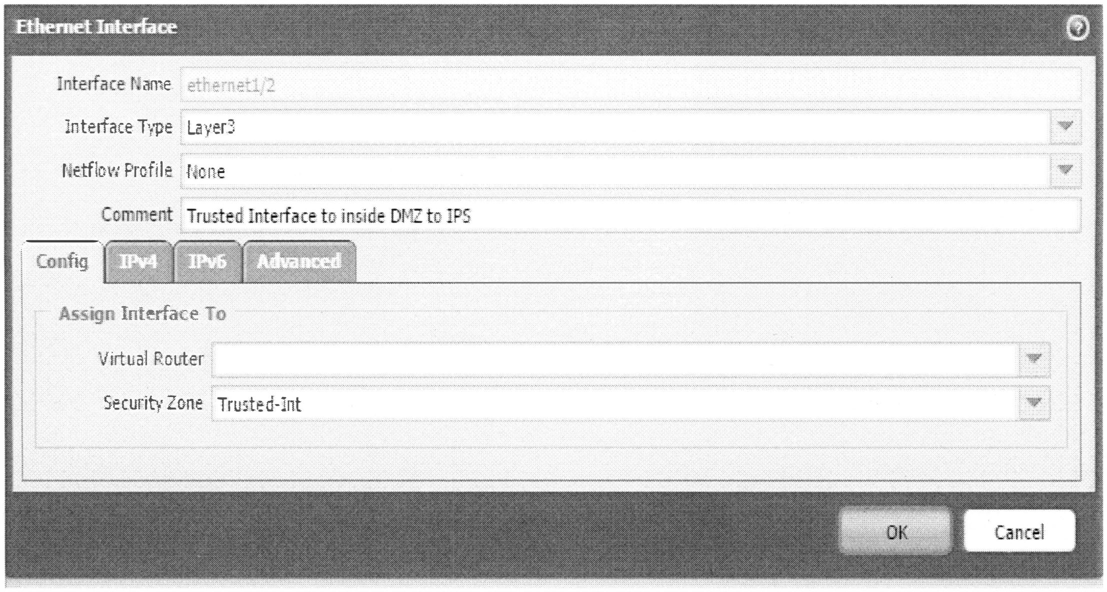
Users from these addresses/subnets will be identified.

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

Figure 3.4: Shows zone creation

4. Give it a name, then select type as layer3, then click ok
5. Then click on interfaces right above zones on the left side panel
6. Click on the interface to be configured
7. Select the specific security zone you want this interface to be associated with



Ethernet Interface

Interface Name ethernet1/2

Interface Type Layer3

Netflow Profile None

Comment Trusted Interface to inside DMZ to IPS

Assign Interface To

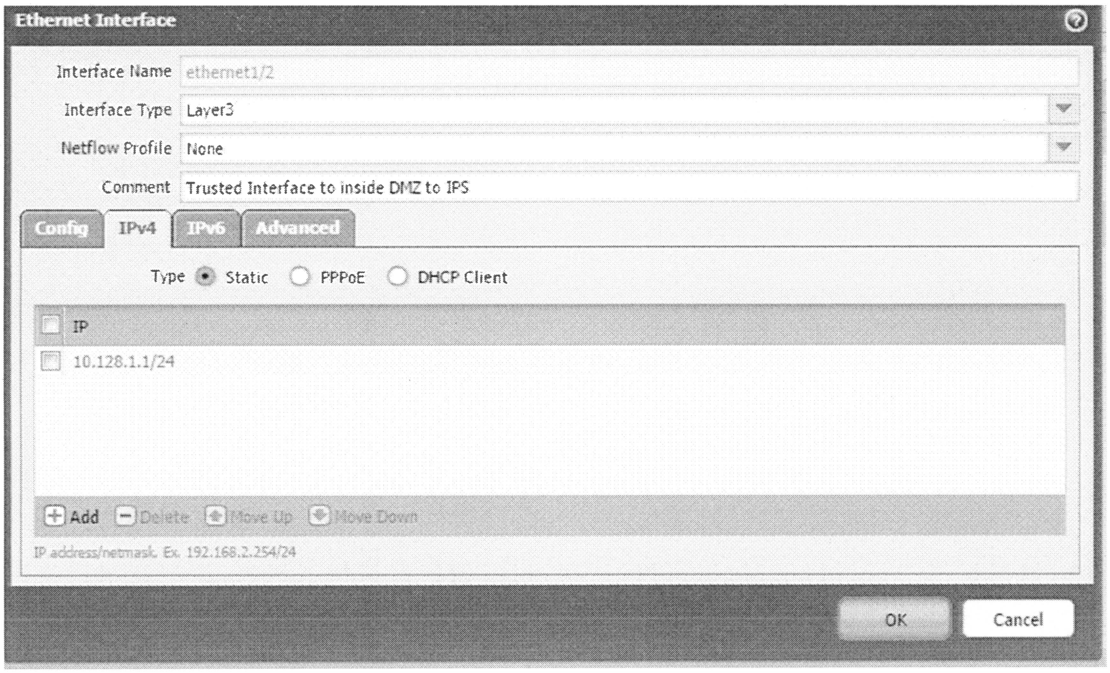
Virtual Router

Security Zone Trusted-Int

Figure 3.5: Showing interface configuration

8. Click on IPv4

9. Click on add to configure the IP address for this interface



Ethernet Interface

Interface Name ethernet1/2

Interface Type Layer3

Netflow Profile None

Comment Trusted Interface to inside DMZ to IPS

Type ● Static ○ PPPoE ○ DHCP Client

□ IP
□ 10.128.1.1/24

IP address/netmask. Ex. 192.168.2.254/24

Figure 3.6: Showing IP address configuration on the interface

10. Then click ok

Repeat the steps above to create the other two zones and interfaces.

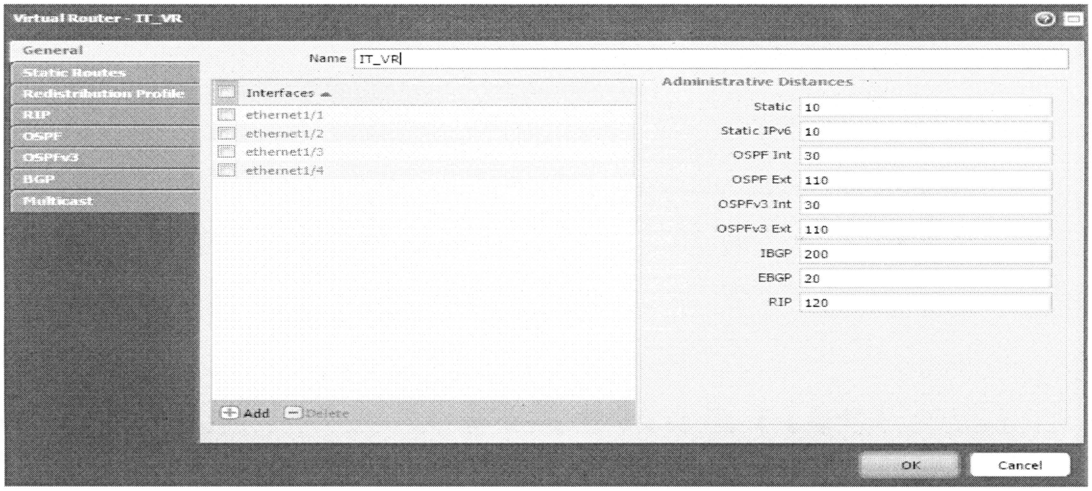
3.3.2 Virtual Router Configuration

The IDS needs to understand how to route traffic that is coming from both DMZ and from trusted zone to untrusted zone. The virtual router implements three static routes:

- The first route routes traffic to any destination on the Internet using the router's G0/1 interface IP address as the default gateway
- The second, routes traffic to the 172.16.10.0 network that is in between the IPS and the internal router by using the IPS outside interface G0/1 IP address as the default gateway)
- And the third one routes traffic to the 192.168.4.0 network using the IPS outside interface G0/1 IP address as the default gateway.

Figure 3.7 below shows the first route configuration. The Virtual router configuration steps are shown below:

1. Click on virtual routers
2. Click on add and give it any name you want it called as shown below



Name IT_VR

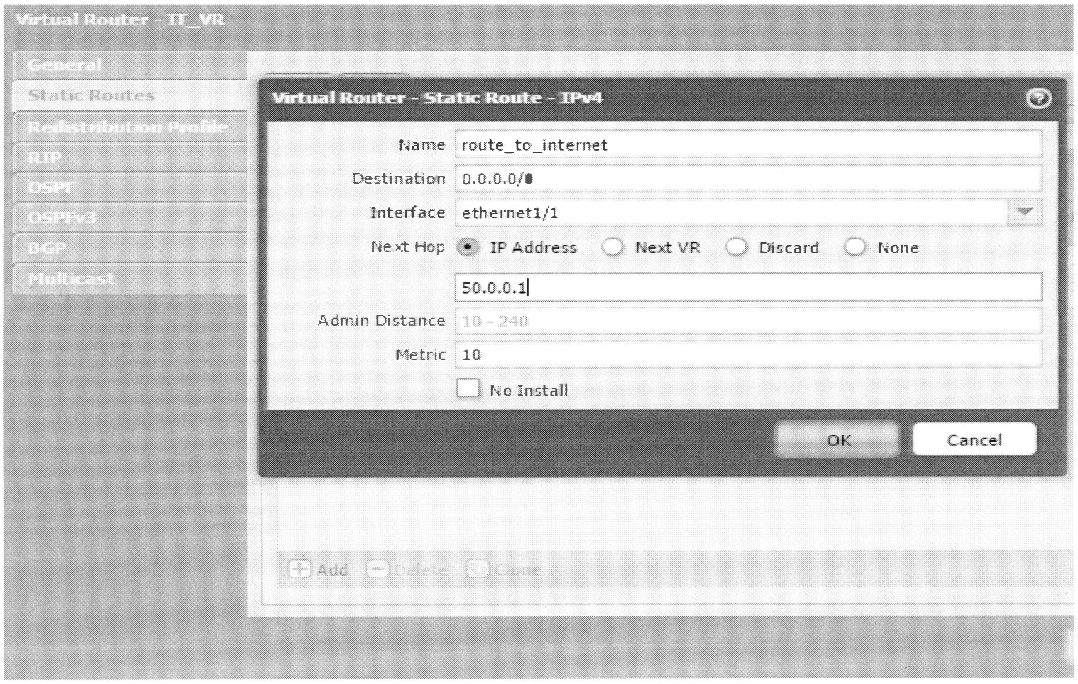
Interfaces
- □ ethernet1/1
- □ ethernet1/2
- □ ethernet1/3
- □ ethernet1/4

Administrative Distances

Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

Figure 3.7: Showing virtual router configuration

3. Click on static routes
4. Name your static route and enter the static route details as shown below
5. Then click ok



Name route_to_internet

Destination 0.0.0.0/0

Interface ethernet1/1

Next Hop ● IP Address ○ Next VR ○ Discard ○ None

50.0.0.1

Admin Distance 10 - 240

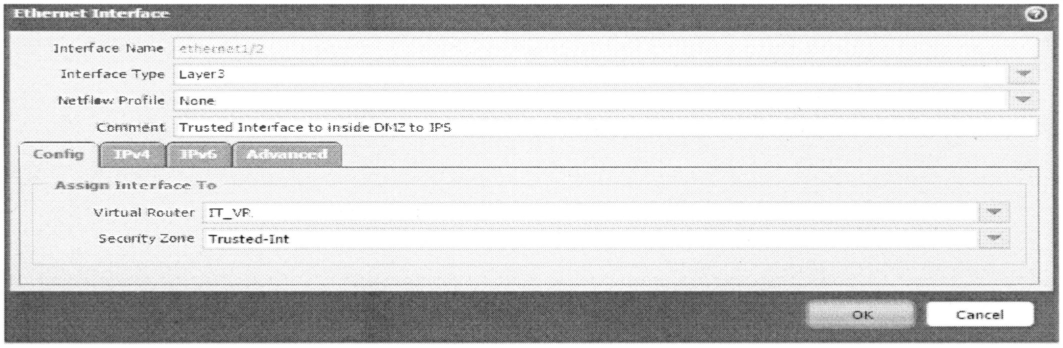
Metric 10

□ No Install

Figure 3.8: Shows how to set static route on a virtual router

Repeat all the steps above to create the other two static routes

The virtual router created has to be attached to the interfaces created. Click on the interfaces tab to select the virtual router created as shown in Figure 3.9



Interface Name: ethernet1/2
Interface Type: Layer3
Netflow Profile: None
Comment: Trusted Interface to inside DMZ to IPS

Assign Interface To
Virtual Router: IT_VR
Security Zone: Trusted-Int

Figure 3.9: Shows how to attach an interface to a virtual router

3.3.3 NAT Configuration

A bidirectional NAT is configured to translate the webserver IP address 172.168.1.2 to the IP address 50.0.0.2 on the untrusted zone of the IDS when traffic is originating or returning from the webserver, and also to translate 50.0.0.2 to 172.16.1.2 when traffic is destined to the webserver. The implication of this is that traffic directed towards the IP address 50.0.0.2 will translate to the 172.168.1.2 IP address. This is the point at which Internet traffic destined for the webserver that is port-forwarded to 192.168.1.2, and then changed to 50.0.0.2, will translate to 172.168.1.2. In addition, the NAT is configured to translate the IP address on the trusted zone to the untrusted zone so that traffic coming from the inside network outbound the trusted zone can find their path to either the webserver or the Internet depending on the traffic destination.

3.3.4 Firewall Security Policies

In this research, several security policies were configured to allow or deny traffic flowing from one zone to the other. The rules are shown below:

1. Allow traffic flow from the trusted zone to the untrusted zones
2. Deny traffic from the untrusted zone to the trusted zone
3. Allow traffic flow from the Internet inbound interface G0/0 of the router to the untrusted zone and then to the webserver via the DMZ. The policy is named UnT-DMZ
4. Allow traffic from the DMZ to the untrusted zone
5. Allow traffic flow from trusted to trusted zones
6. Allow traffic flow from the trusted zone to DMZ

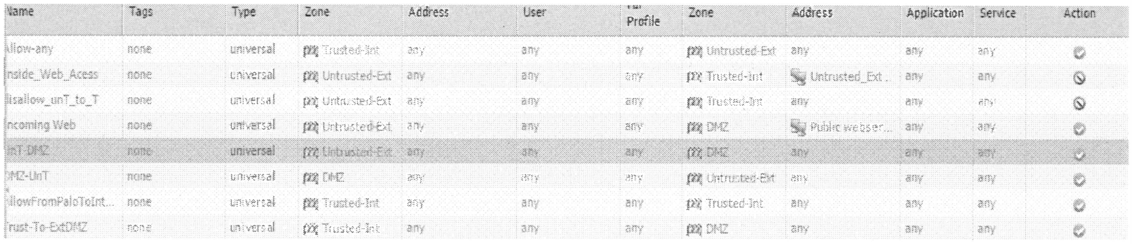
The essence of the security rules above is to deny unwanted traffic from one zone to the other and to allow legitimate traffic from one zone to the other.

The steps below show the creation of the third policy UnT-DMZ

1. Click on the policy tab
2. Click on the add button to create a policy
3. Under the general tab, name the policy
4. Click on the source, then click on the add to button under zone to add the source zone as untrusted
5. Click on user tab to add user, but this has been set to any in this configuration
6. Click on destination, then click on the add button under the destination zone as DMZ

7. Click on the application tab to specify an application, it has been configured to "any" in this configuration
8. Click on service/URL category, check any button under category
9. Click on the action tab and choose allow
10. Then click ok.

Following all the steps above created all the rules as shown in Figure 3. 10 below



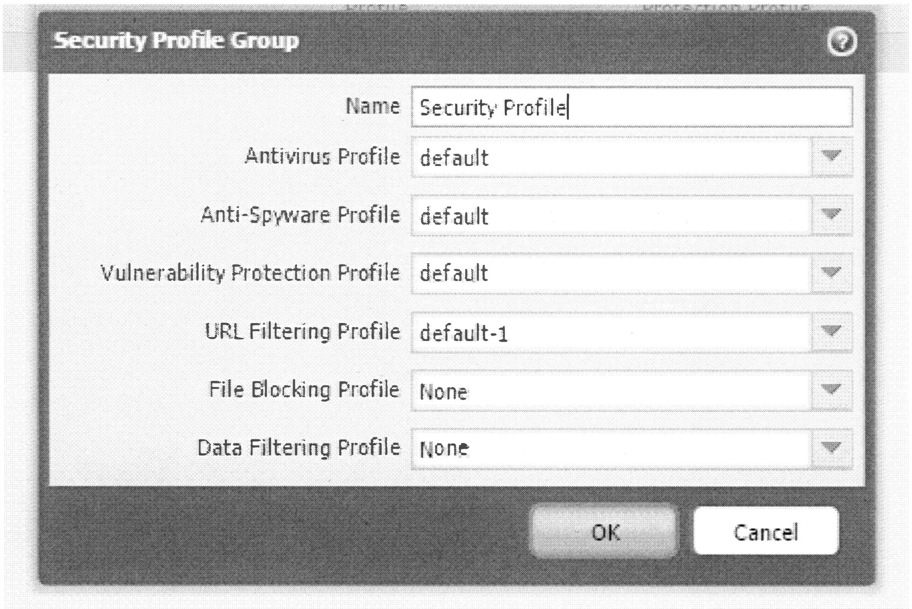
lame	Tags	Type	Zone	Address	User	Profile	Zone	Address	Application	Service	Action
llow-any	none	universal	Trusted-Int	any	any	any	Untrusted-Ext	any	any	any	✓
nside_Web_Acess	none	universal	Untrusted-Ext	any	any	any	Trusted-Int	Untrusted_Ext…	any	any	⊘
isallow_unT_to_T	none	universal	Untrusted-Ext	any	any	any	Trusted-Int	any	any	any	⊘
ncoming Web	none	universal	Untrusted-Ext	any	any	any	DMZ	Public webser…	any	any	✓
nT-DMZ	none	universal	Untrusted-Ext	any	any	any	DMZ	any	any	any	✓
MZ-UnT	none	universal	DMZ	any	any	any	Untrusted-Ext	any	any	any	✓
llowFromPaloToInt…	none	universal	Trusted-Int	any	any	any	Trusted-Int	any	any	any	✓
rust-To-ExtDMZ	none	universal	Trusted-Int	any	any	any	DMZ	any	any	any	✓

Figure 3.10: Shows the configured security policies

The steps above describe a policy that controls inbound traffic on the untrusted zone from the Internet entering the DMZ to access the webserver.

3.3.5 Profile Configuration

Profile configuration is where the IDS configuration is set to detect vulnerabilities, spyware, and viruses. In order for this configuration to be effective, the profile configuration has to be attached to a particular security rule. The profile created in this research is assigned to the UnT-DMZ security policy rule to monitor any traffic going through the untrusted zone in order to detect malicious traffic or vulnerabilities. Figure 3.11 below shows the profile configuration.



Security Profile Group

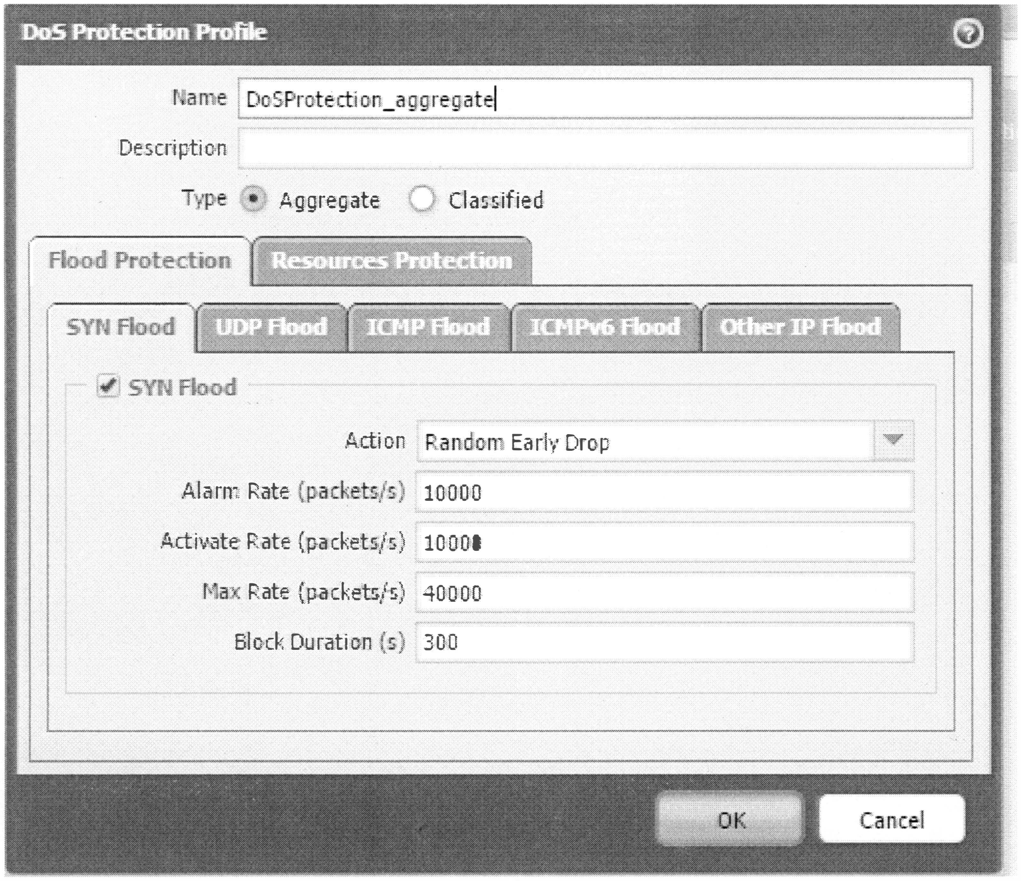
Name	Security Profile
Antivirus Profile	default
Anti-Spyware Profile	default
Vulnerability Protection Profile	default
URL Filtering Profile	default-1
File Blocking Profile	None
Data Filtering Profile	None

Figure 3.11: Showing profile configuration

3.3.6 DoS Protection

The IDS also is configured to mitigate denial of service attack. The detailed configuration is shown in Figure 3.12. The steps below show the configuration

1. Click on the objects tab
2. Click on DoS protection
3. Click on add
4. Give the DoS protection profile a name
5. Check the aggregate button
6. Under flood protection, check all of the buttons under SYN flood, UDP flood, ICMP flood and other IP flood tabs
7. Click on resource protection tab, and check the session button
8. Then click ok



DoS Protection Profile

Name DoSProtection_aggregate

Description

Type ● Aggregate ○ Classified

☑ SYN Flood

Action Random Early Drop

Alarm Rate (packets/s) 10000

Activate Rate (packets/s) 10000

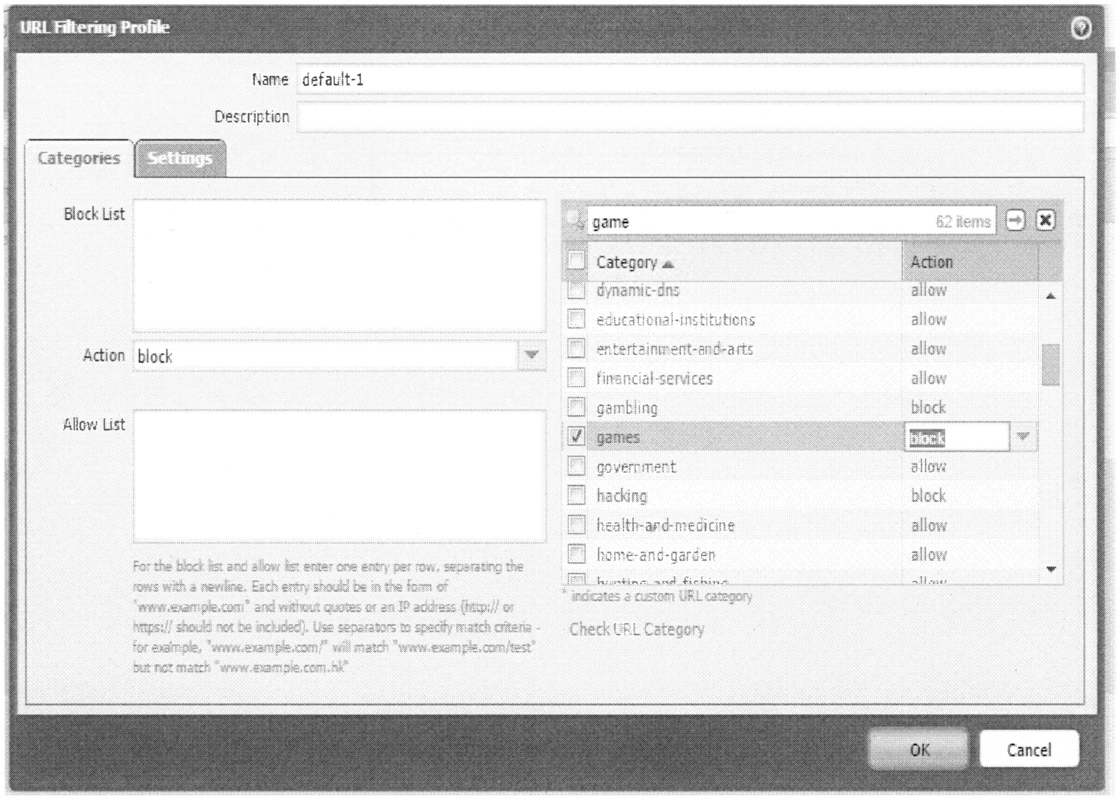
Max Rate (packets/s) 40000

Block Duration (s) 300

Figure 3.12: Showing DoS protection configuration

3.3.7 URL Filtering

URL filtering configured on the IDS blocks traffic from going to some websites that contain security risks. In addition, it helps to control the way users inside the network consumes network bandwidth. Websites like games websites are high bandwidth consumers and surfing these websites might make service unavailable to other users due to their high bandwidth usage. In addition, URL filtering would also prevent users from visiting websites with viruses and thus prevent ignorant virus downloads. The URL filtering configuration below blocks the games URL category.



Name: default-1

Description:

Block List:

Action: block

Allow List:

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

game — 62 items

	Category	Action
□	dynamic-dns	allow
□	educational-institutions	allow
□	entertainment-and-arts	allow
□	financial-services	allow
□	gambling	block
☑	games	block
□	government	allow
□	hacking	block
□	health-and-medicine	allow
□	home-and-garden	allow
□	hunting-and-fishing	allow

* indicates a custom URL category

Figure 3.13: Showing URL filtering

Steps to configure URL filtering to block games URL category

1. Click on objects
2. Click on URL filtering
3. Click on add
4. Give it a name
5. Select block under action
6. Select game under URL category and then select block action
7. Then click ok

3.4 Webserver Configuration

The webserver used in this design is a windows server 2012 R2. The robustness and high speed of the Windows Server 2012 R2 make it a good fit for this purpose. The system hosting this Windows Server is a core i7 Intel processor, with 8GB RAM and 1TB hard disk size machine. This system hosts the public webserver with the IP address 172.16.1.2 255.255.255.0. The content of this server loads whenever a request comes to the public webserver IP address. The web application (Damn Vulnerable Web Application) needed for the testing of the designed system runs well on Kali Linus Operating System. In order to achieve this, the Windows Server is virtualized using the Hyper-V functionality tool that comes with Windows Server 2012 R2, and Kali Linus operating system was installed on the virtualized server.

3.5 Firewall/IPS

The Firewall/IPS is a Cisco 5512-x device. This Cisco 5512-x device has an IPS sensor that comes with over 6000 signatures in its database. The IPS is capable of full network participation for global protection. Global protection is a service that allows the IPS to synchronize with the cloud in order to compare traffic signatures not just against its own database but also against signatures in the cloud. The advantage of this is that Cisco collects information about attacks that are detected on any of their IPSs and send it to the cloud in order for other IPSs to be aware of these threats. The IPS is configured in an inline mode in order to see through every traffic are that traversing the network. Configuration instructions are set on the IPS to allow traffic flow from the inside of the network and block traffic from coming in from the outside.

3.5.1 Interface Configuration of the Firewall/IPS

Three interfaces are configured on the firewall/IPS in order to segment traffic flow. The interface that connects directly to the IDS is E0/0 and has been configured as outside with security level of 0, this implies that whatever traffic coming from this interface should not be trusted. The interface E0/1 is configured as a DMZ with security level 50. The DMZ here host an intranet webserver and two honeypots. This aspect is outside the scope of this research but is included in the topology to make it obvious as a future recommendation. The intranet webserver is meant to be a decoy if peradventure an attacker is able to bypass the IDS and get to the IPS, the idea is to direct the attacker into this webserver to make the attacker feel he is already on the inside network. While the attacker does his/her hacking, the honeypots records and captures the details of the attacker's activities. E0/2 is configured with the security level of 100 since it is the interface that connects to the internal router.

3.5.2 Firewall Security Policies

Similar to policies on the IDS, policies are set on the IPS too in order to allow or deny traffic. The IPS has the following policies configuration:

1. Allow traffic from the inside network to go out to the Internet
2. Allow traffic from the DMZ to go out to the Internet
3. Deny traffic from the DMZ from going to the inside network
4. Deny traffic from the outside from going to the inside

Any other traffic that does not match the allow policies would be denied. The detailed configuration of this configuration is shown in the CLI commands in appendix B.

3.5.3 EIGRP Routing

EIGRP routing is configured on the firewall in order for it to advertise the networks on its interfaces. This is to enable communication between the firewall and the internal router. The good thing about this is that EIGRP protocol is not configured on the IDS and as such it does not get any advertisement or routing updates from the firewall/IPS.

3.5.4 IPS Sensor Configuration

Configuration for the IPS sensor could be through either the command line interface or the Cisco ASDM graphical user interface. The IPS sensor in the design is configured using the ASDM graphical user interface. Configuration details for the IPS sensor are on the appendix E page. As earlier mentioned, the IPS has over 6000 signatures that it uses to detect and prevent different attacks. In addition, it does anomaly detection as well. In this work, about 1000 signatures are enabled for testing.

3.6 Internal Router

The internal router is also a Cisco 1941W router just like the external router. The internal router serves as the gateway between the internal users and the outside network. In the design, a 24-port Cisco 1900 switch connects to the G0/0 of the internal router. The internal webserver hosting different resources and applications connects to a port on the switch. The internal router has EIGRP enabled on it to advertise its route. In addition, a static route is set on it to allow the internal network reach every network segment. The detailed configuration of the internal is on the appendix B page.

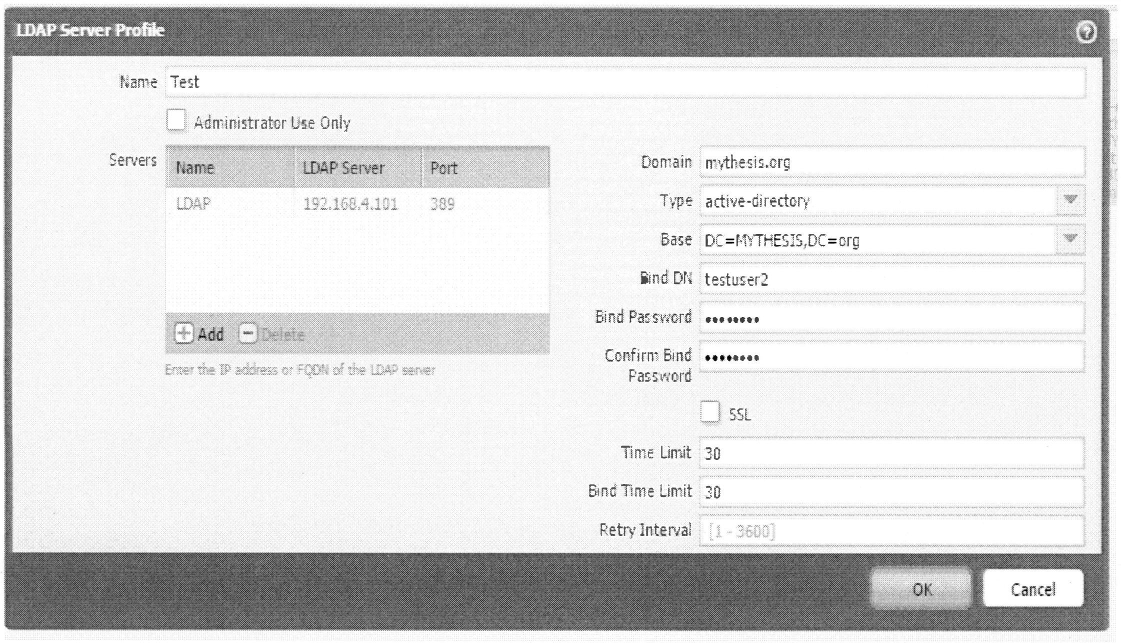
3.7 Internal Webserver

The internal webserver is also a virtualized version of windows server 2012 R2 just like the public webserver while the physical machine itself serves the purpose of a host. The Hyper-V functionality tool helps to achieve this as well. On this internal webserver, an active directory was setup, so also a domain controller, users in the inside network were added to the domain. This is to enable proper monitoring of internal users for auditing purpose. The idea behind this is to be able to identify who is accessing what resources on the network.

3.8 Lightweight Directory Access Protocol (LDAP) and Agentless User-ID

LDAP on the IDS synchronizes with the Active Directory Server in the internal network. It provides the following functions:

1. It allows any authorized user within the domain to authenticate into the IDS in other to manage it. This means that an administrator does not need to give out his/her password to anyone.
2. The LDAP enables the IDS to perform user identity mapping by configuring agentless identity mapping. The LDAP records users IP addresses as well as their profile, which include their name and the domain they belong to when they generate traffic on the network. This offers an advantage in the event of incidence analysis if an inside user has been collaborating with an external attacker. Figure 3.14 below shows how LDAP configuration is accomplished



LDAP Server Profile

Name: Test

□ Administrator Use Only

Servers

Name	LDAP Server	Port
LDAP	192.168.4.101	389

Enter the IP address or FQDN of the LDAP server

Domain: mythesis.org

Type: active-directory

Base: DC=MYTHESIS,DC=org

Bind DN: testuser2

Bind Password: ••••••••

Confirm Bind Password: ••••••••

□ SSL

Time Limit: 30

Bind Time Limit: 30

Retry Interval: [1 - 3600]

Figure 3.14: Shows LDAP configuration

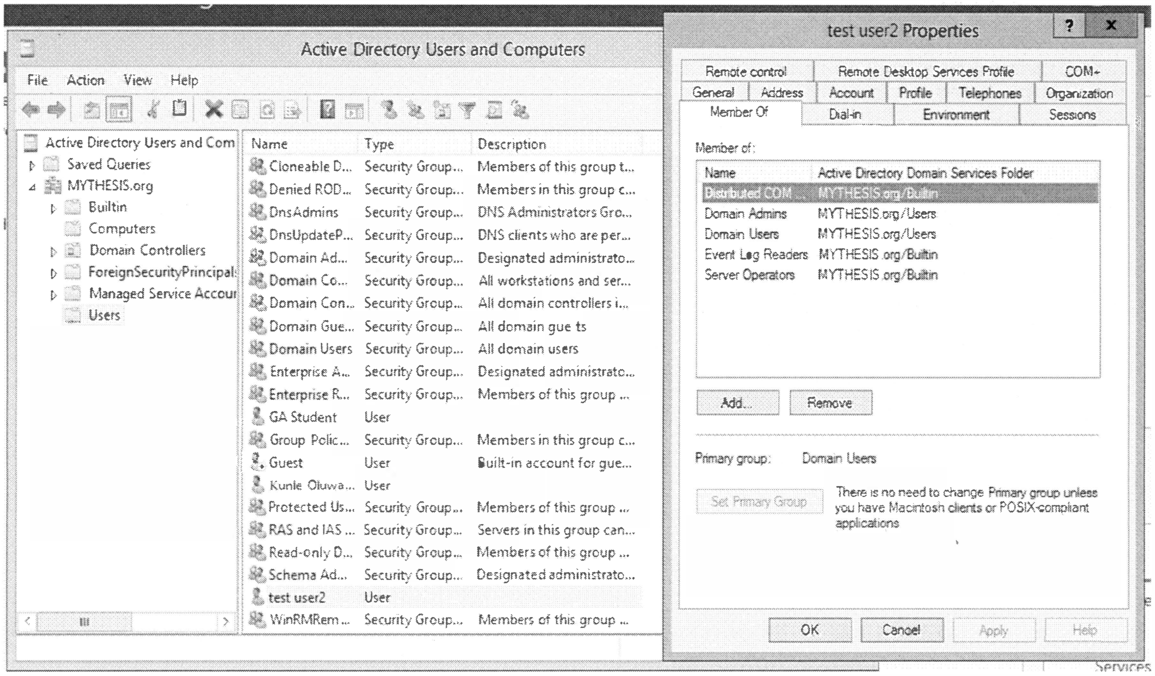
The steps to configure LDAP is shown below

1. Click on device tab
2. Under server profile in the left plane, click on LDAP
3. Click on add to add LDAP
4. Under servers click on add
5. Enter the IP address of the active directory server and use 389 for port number
6. Enter the domain name for your active directory and it will automatically populate the Base field
7. Enter your domain username and password
8. Then click ok

Steps to Configure Agentless User-ID

The Agentless User-ID is configured to monitor user session information from the active directory server. Steps to configure agentless user-id is shown below

1. Create service account in active directory. Add a user in the active directory to the Distributed COM users, Server Operators, and Event Log Readers Groups. Right click on the user as shown in Figure 3.15 below, select properties, then click member of, and use the add button to add the user to the groups mentioned above



Name	Type	Description
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain gue ts
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise R...	Security Group...	Members of this group ...
GA Student	User	
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Kunle Oluwa...	User	
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
test user2	User	
WinRMRem...	Security Group...	Members of this group ...

Member of:

Name	Active Directory Domain Services Folder
Distributed COM ...	MYTHESIS.org/Builtin
Domain Admins	MYTHESIS.org/Users
Domain Users	MYTHESIS.org/Users
Event Log Readers	MYTHESIS.org/Builtin
Server Operators	MYTHESIS.org/Builtin

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications

Figure 3.15: Shows how to add users to service accounts

The IDS uses WMI authentication and the user has to modify the security settings on CIMV2 security properties on the active directory server. Open the WMI by running wmimgmt.msc on windows command prompt, then right click on WMI control as shown in Figure. 3.16 below and then select properties.

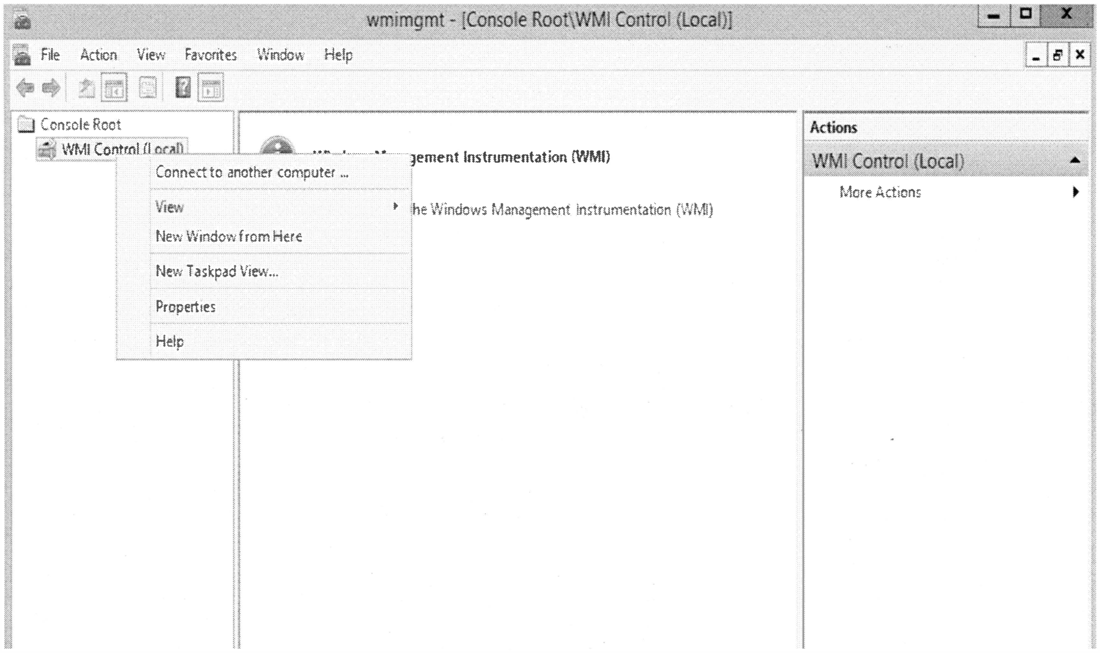
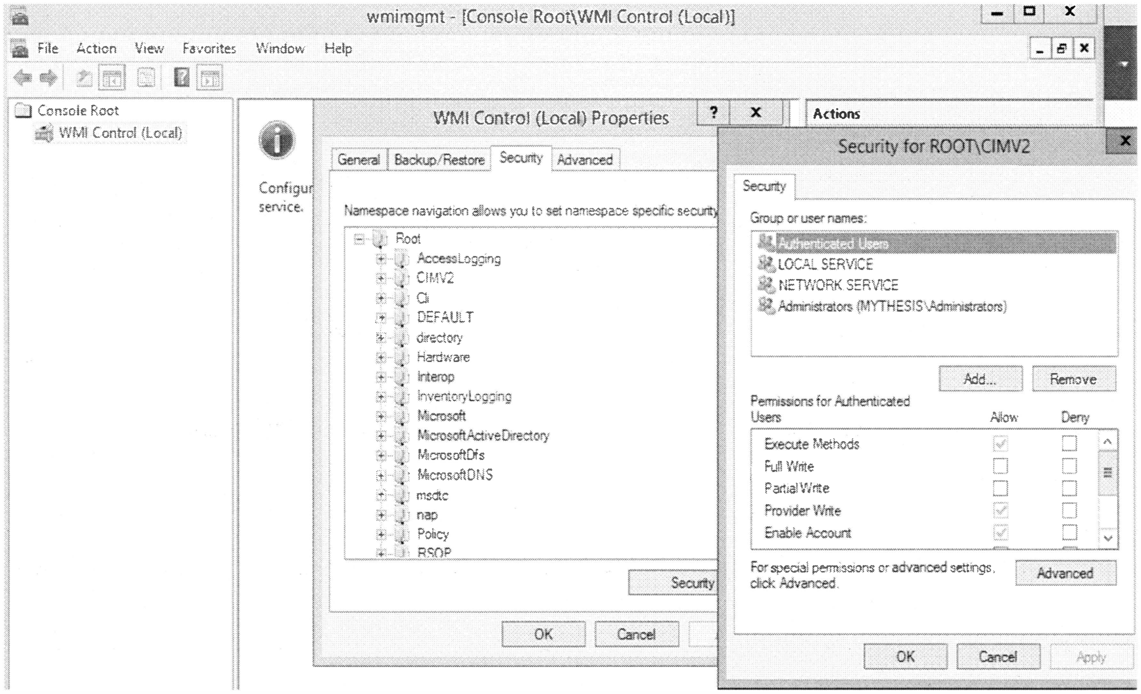


Figure 3.16: Shows WMI configuration

Then select the security tab and click on the root to expand it. Select the folder CIMV2, click the security tab and add the service account from step 1, and ensure you click enable account and remote enable as shown in Figure 3.17 below


wmimgmt - [Console Root\WMI Control (Local)]
File Action View Favorites Window Help
Console Root
WMI Control (Local)
Configur
service.
WMI Control (Local) Properties
General Backup/Restore Security Advanced
Security
OK Cancel
Actions
Security for ROOT\CIMV2
Security
Add... Remove
Advanced
OK Cancel Apply

Namespace navigation allows you to set namespace specific security

- Root
  - AccessLogging
  - CIMV2
  - Cli
  - DEFAULT
  - directory
  - Hardware
  - Interop
  - InventoryLogging
  - Microsoft
  - MicrosoftActiveDirectory
  - MicrosoftDfs
  - MicrosoftDNS
  - msdtc
  - nap
  - Policy
  - RSOP

Group or user names:

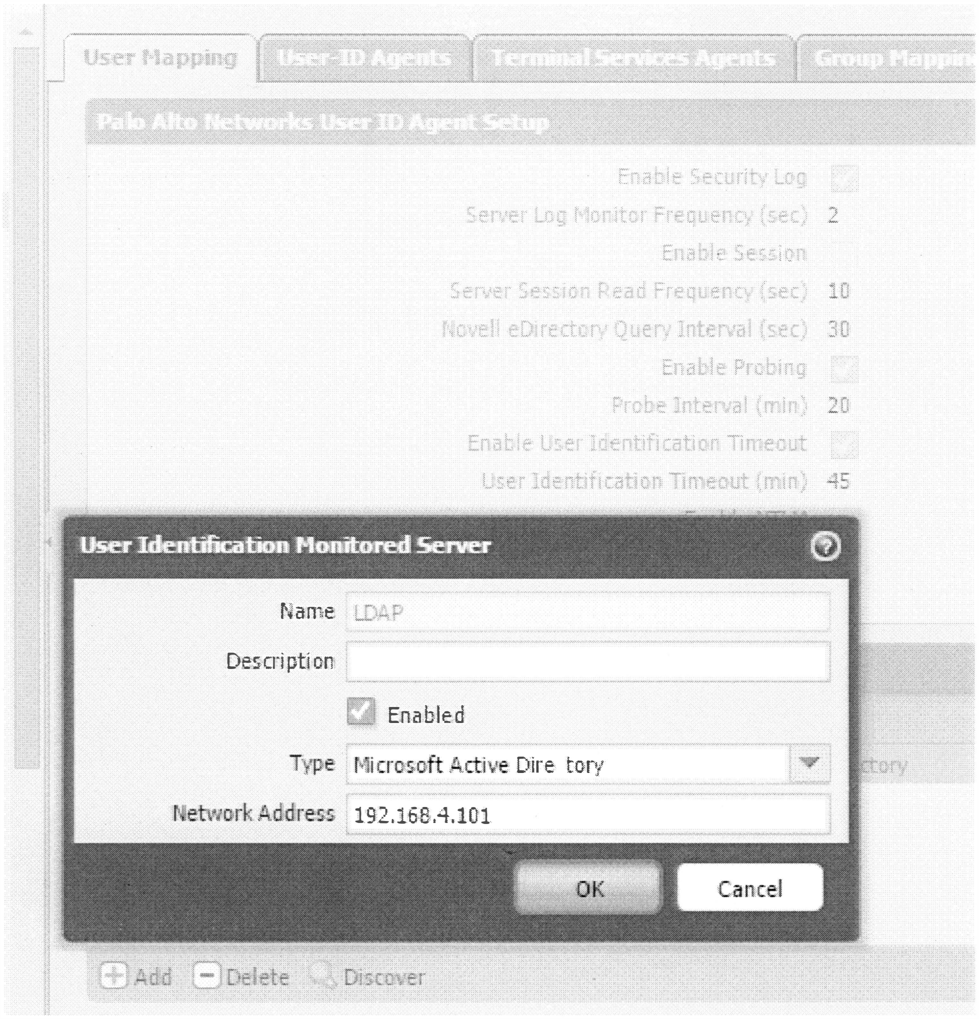
- Authenticated Users
- LOCAL SERVICE
- NETWORK SERVICE
- Administrators (MYTHESIS\Administrators)

Permissions for Authenticated Users	Allow	Deny
Execute Methods	☑	□
Full Write	□	□
Partial Write	□	□
Provider Write	☑	□
Enable Account	☑	□

For special permissions or advanced settings, click Advanced.

Figure 3.17: Shows how to add CIMV2 security to service account

2. Go to the IDS (Palo Alto) and click on the device tab, then select user mapping as shown in Figure 3.18 below, and then click the add button to enter a name for the server and enter the IP address for the active directory server.



Palo Alto Networks User ID Agent Setup

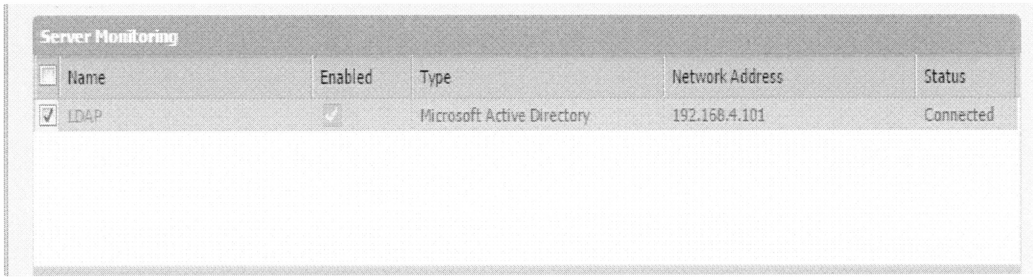
Enable Security Log ☑
Server Log Monitor Frequency (sec) 2
Enable Session
Server Session Read Frequency (sec) 10
Novell eDirectory Query Interval (sec) 30
Enable Probing ☑
Probe Interval (min) 20
Enable User Identification Timeout ☑
User Identification Timeout (min) 45

User Identification Monitored Server

Name LDAP
Description
☑ Enabled
Type Microsoft Active Dire tory
Network Address 192.168.4.101

Figure 3.18: Shows user-mapping configuration

If the above configuration is correct, you will see the server connected as shown below in Figure 3.19.

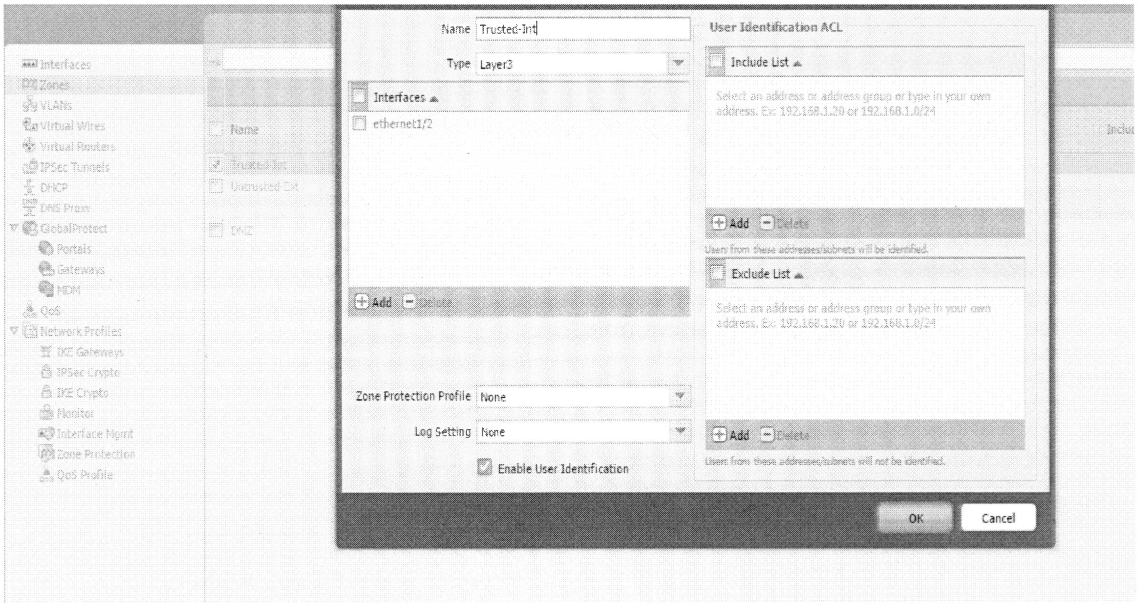


Server Monitoring

□	Name	Enabled	Type	Network Address	Status
☑	LDAP	☑	Microsoft Active Directory	192.168.4.101	Connected

Figure 3.19: Shows successful connection of active directory to LDAP

3. Then attach this user mapping to the trusted zone on the IDS as shown in Figure 3.20 below. Click on network tab, then click on the zone and select the zone as shown below, and check the button "enable user identification". Then click ok. Doing this will always capture every internal user that sends traffic out through the trusted zone.



Name: Trusted-Int

Type: Layer3

Interfaces: ethernet1/2

Zone Protection Profile: None

Log Setting: None

☑ Enable User Identification

User Identification ACL

Include List: Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will be identified.

Exclude List: Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

Users from these addresses/subnets will not be identified.

Figure 3.20: Shows enable user identification

CHAPTER FOUR

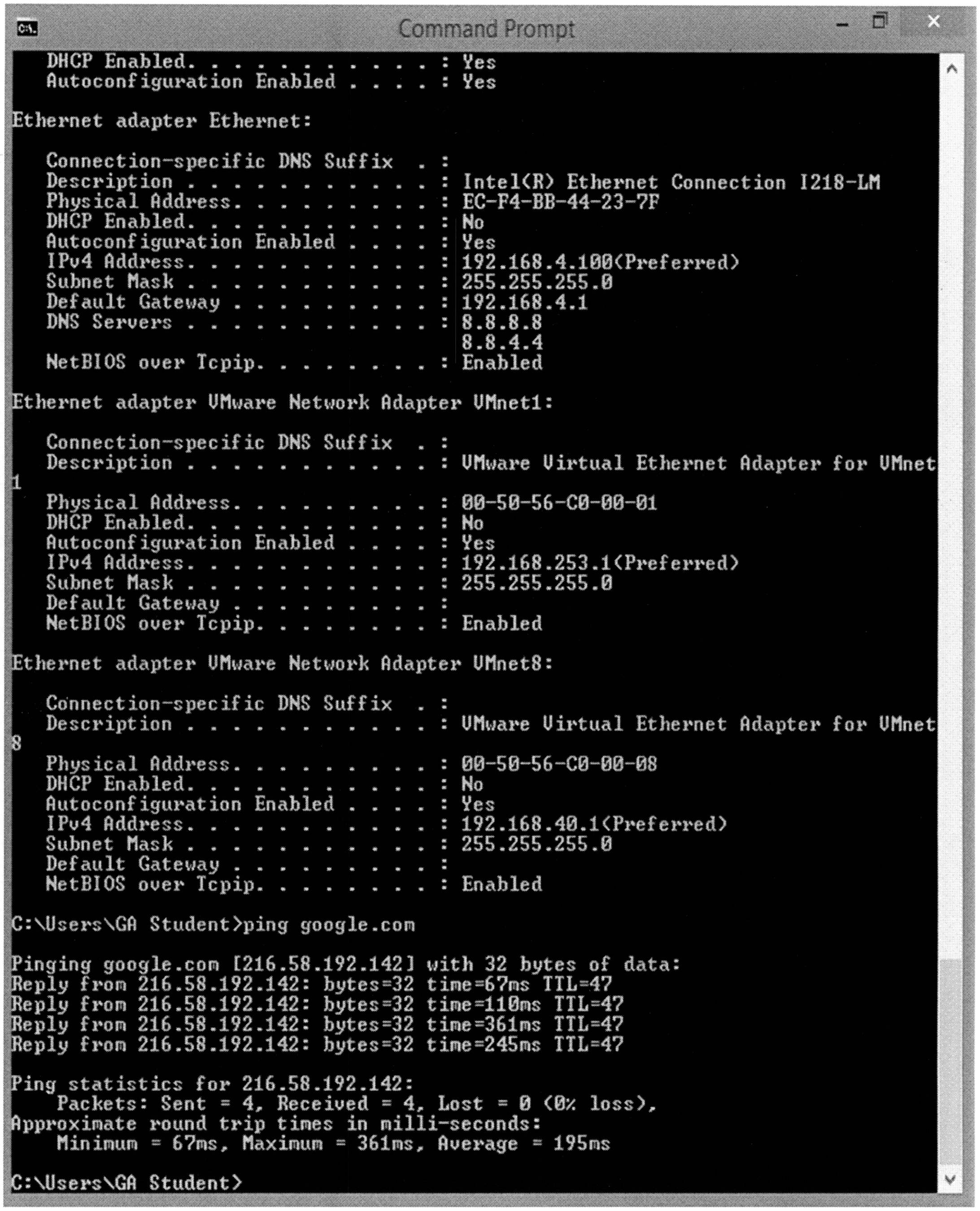
4.0 Results and Discussion, Conclusion & Recommendation

This research has accomplished the design for the IDS/IPS laboratory for the MSc Cyber Security program at EIU. The design was tested and worked as expected. All of the various network segments were able to communicate with themselves as expected. The laboratory design has its own network connection to the Verizon ISP, thereby isolating it from constituting a risk to the EIU network or any other public network. The internal users in the laboratory design are able to access the Internet with their own private IP addresses.

4.1 Results and Discussion

A major breakthrough of this design is that it was able to go online so it can serve the purpose of a public testing platform where hackers can launch different forms of attacks. This is very significant and it is a milestone. Students would have the privilege of working with real cyber-attacks and laboratory simulated attacks rather than only laboratory simulated attacks.

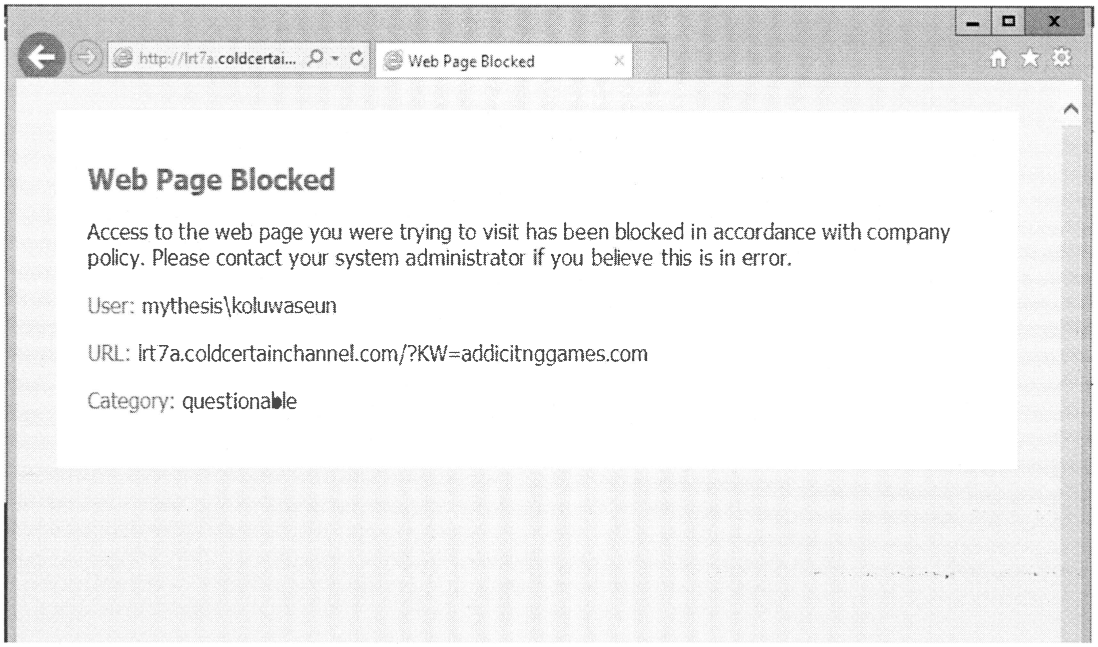
Figure 4.1 below shows an internal user with the IP address 192.168.4.100 pinging www.google.com. This is a proof that the internal users can access the external network.



```
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection I218-LM
   Physical Address. . . . . . . . . : EC-F4-BB-44-23-7F
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.4.100(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.4.1
   DNS Servers . . . . . . . . . . . : 8.8.8.8
                                       8.8.4.4
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet
1
   Physical Address. . . . . . . . . : 00-50-56-C0-00-01
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.253.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   NetBIOS over Tcpip. . . . . . . . : Enabled

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : VMware Virtual Ethernet Adapter for VMnet
8
   Physical Address. . . . . . . . . : 00-50-56-C0-00-08
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.40.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\GA Student>ping google.com

Pinging google.com [216.58.192.142] with 32 bytes of data:
Reply from 216.58.192.142: bytes=32 time=67ms TTL=47
Reply from 216.58.192.142: bytes=32 time=110ms TTL=47
Reply from 216.58.192.142: bytes=32 time=361ms TTL=47
Reply from 216.58.192.142: bytes=32 time=245ms TTL=47

Ping statistics for 216.58.192.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 67ms, Maximum = 361ms, Average = 195ms

C:\Users\GA Student>
```

Figure 4.1: Shows an internal user sending ping packets to google

However, users are restricted from accessing certain websites by configuring URL filtering. Figure 4.2 shows a user blocked when he/she tries to visit a questionable website.



Web Page Blocked

Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

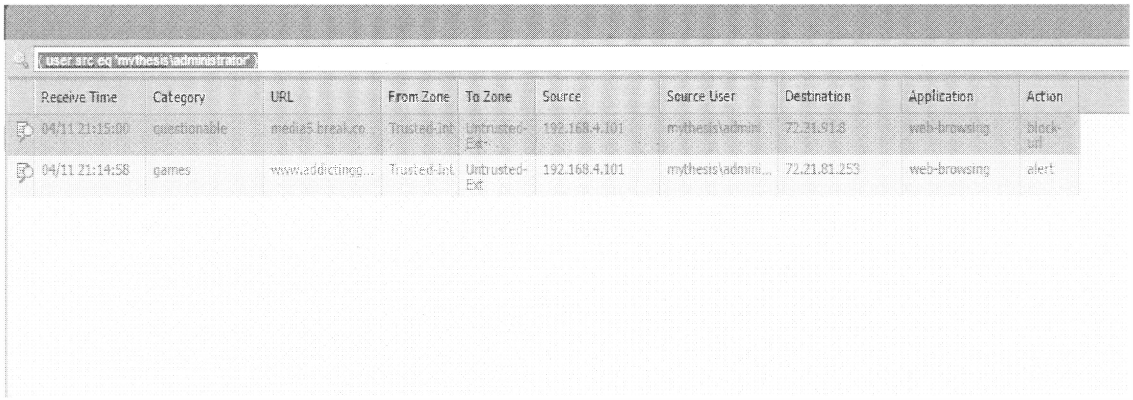
User: mythesis\koluwaseun

URL: lrt7a.coldcertainchannel.com/?KW=addicitnggames.com

Category: questionable

Figure 4.2: showing an internal user blocked from accessing forbidden website

An interesting part of this is that the agentless user-id mapping functionality would map such a user's ID and domain to that traffic so that appropriate actions is taken against such a user. Figure. 4.3 show how the IDS capture the details of the internal user trying to access a questionable website.

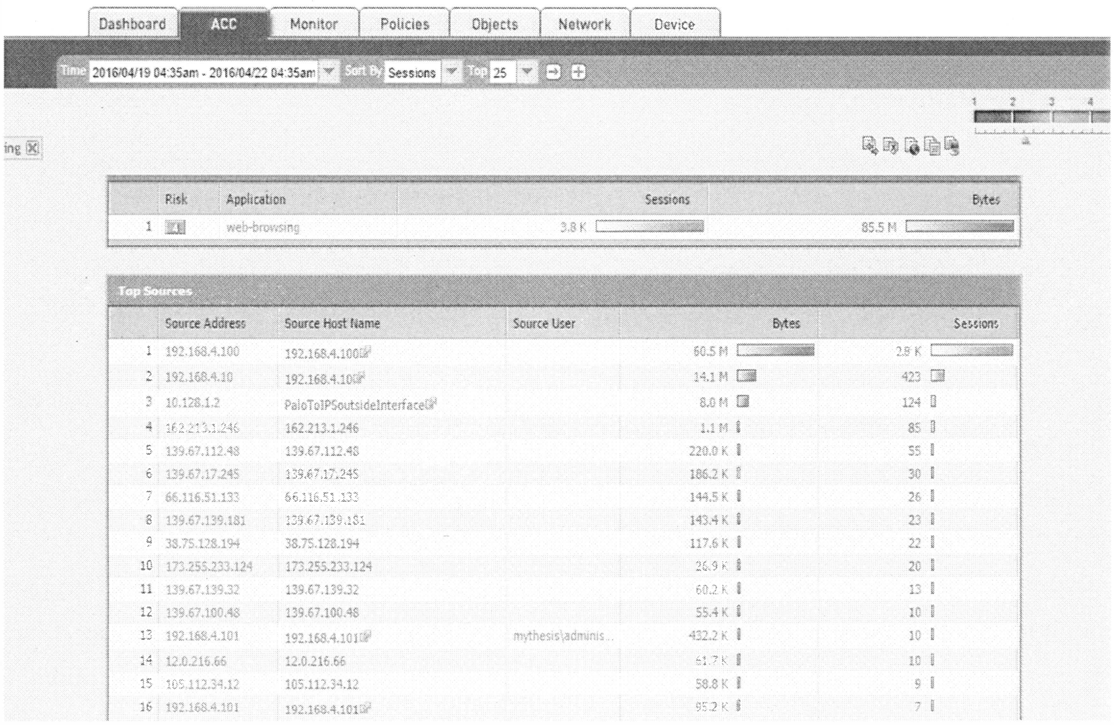


(user.src eq 'mythesis\administrator')

Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action
04/11 21:15:00	questionable	media5.break.co...	Trusted-Int	Untrusted-Ext	192.168.4.101	mythesis\admini...	72.21.91.8	web-browsing	block-url
04/11 21:14:58	games	www.addictingg...	Trusted-Int	Untrusted-Ext	192.168.4.101	mythesis\admini...	72.21.81.253	web-browsing	alert

Figure 4.3: Showing details of an internal user captured by the IDS

This is very significant in conducting incidence analysis in the event of a break in. The administrator can see which user originates what traffic and what website or IP addresses the internal user is sending traffic to. The ACC tab presents a better view of this visibility. The administrator is able to see what users are doing, what applications are consuming network bandwidth, and what threats are traversing the network, etc. Figure 4.4 shows how the ACC represents activities on the IDS.



Time 2016/04/19 04:35am - 2016/04/22 04:35am Sort By Sessions Top 25

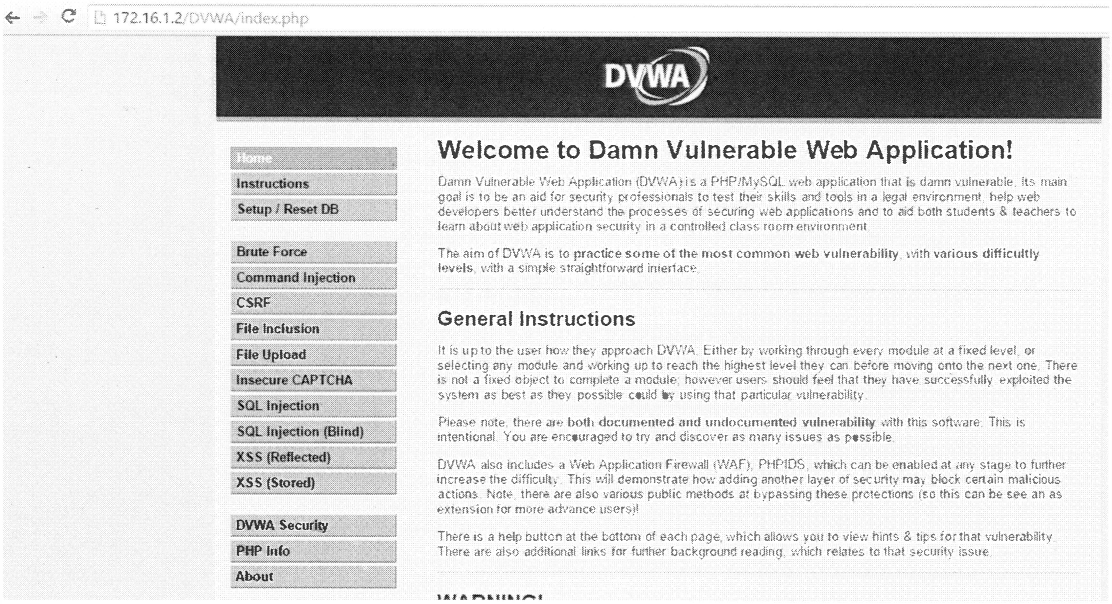
	Risk	Application	Sessions	Bytes
1		web-browsing	3.8 K	85.5 M

Top Sources

	Source Address	Source Host Name	Source User	Bytes	Sessions
1	192.168.4.100	192.168.4.100		60.5 M	2.8 K
2	192.168.4.10	192.168.4.10		14.1 M	423
3	10.128.1.2	PaloToIPSoutsideInterface		8.0 M	124
4	162.213.1.246	162.213.1.246		1.1 M	85
5	139.67.112.48	139.67.112.48		220.0 K	55
6	139.67.17.245	139.67.17.245		186.2 K	30
7	66.116.51.133	66.116.51.133		144.5 K	26
8	139.67.139.181	139.67.139.181		143.4 K	23
9	38.75.128.194	38.75.128.194		117.6 K	22
10	173.255.233.124	173.255.233.124		26.9 K	20
11	139.67.139.32	139.67.139.32		60.2 K	13
12	139.67.100.48	139.67.100.48		55.4 K	10
13	192.168.4.101	192.168.4.101	mythesis\adminis...	432.2 K	10
14	12.0.216.66	12.0.216.66		61.7 K	10
15	105.112.34.12	105.112.34.12		58.8 K	9
16	192.168.4.101	192.168.4.101		95.2 K	7

Figure 4.4: Shows ACC tab with web browsing activities details

In addition, the internal users are able to access the public webserver, which is resident on the DMZ segment of the IDS. This offers good security because the internal users do not need to go outside of the network or use the public IP address of the public webserver. The Figure 4.5 below shows a user accessing the public webserver using the private IP address of the webserver



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerability**, with **various difficultly levels**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

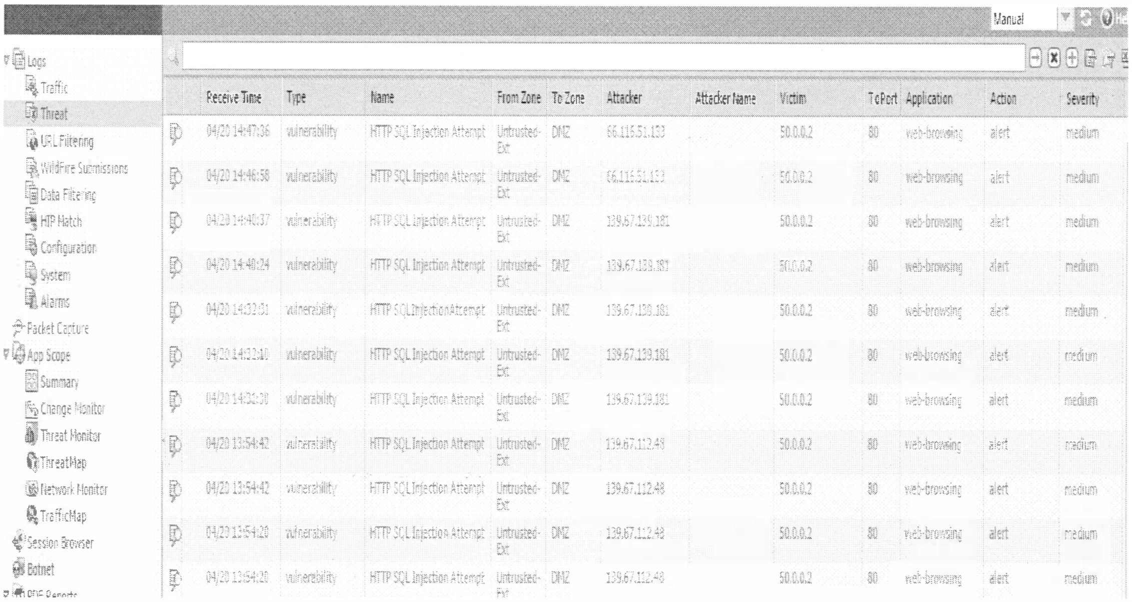
DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be see an as extension for more advance users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Figure 4.5: Internal access to webserver using the webserver's private IP address

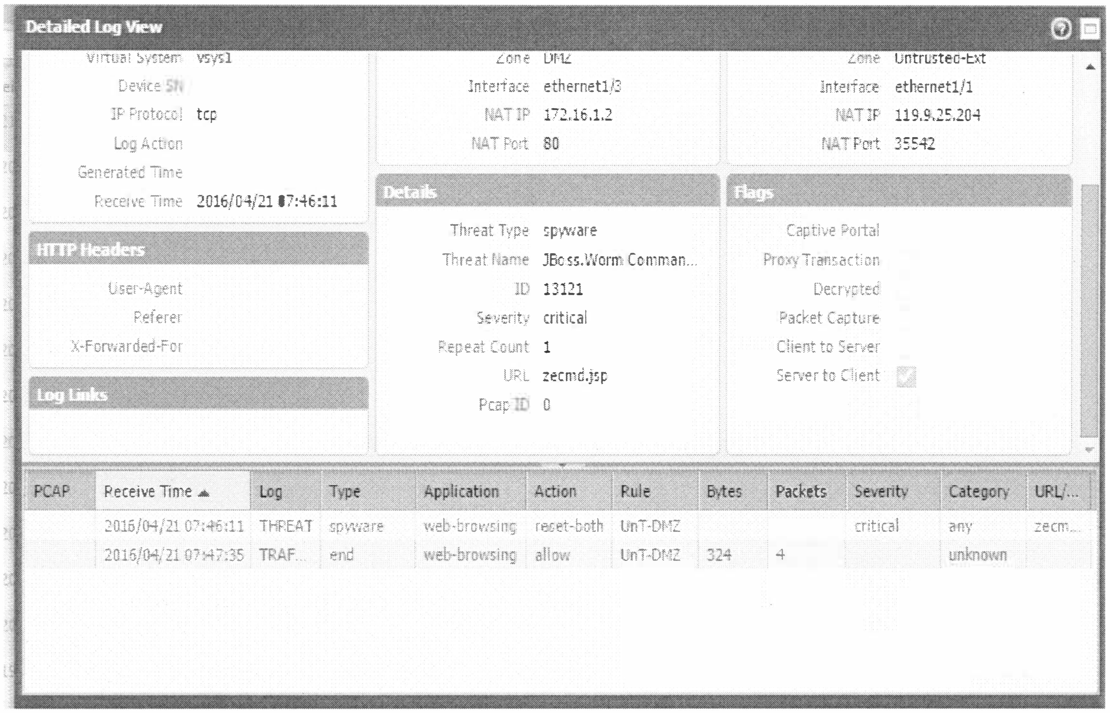
In order to test the functionality of the IDS/IPS developed, a vulnerable web application is hosted on the webserver. The result shows that SQL injection attacks were launched against the webserver frequently, and this was detected by the IDS as shown in Figure 4.6 below. In Figure 4.6 below, it can be observed that the victim's IP address isn't shown as the webserver IP address but rather as the IP of the untrusted zone on the IDS. This is a very good security feature because the webserver is being protected.



Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
04/20 14:47:36	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	66.115.51.133		50.0.0.2	80	web-browsing	alert	medium
04/20 14:46:58	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	66.115.51.133		50.0.0.2	80	web-browsing	alert	medium
04/20 14:40:37	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	139.67.139.181		50.0.0.2	80	web-browsing	alert	medium
04/20 14:40:24	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	139.67.139.181		50.0.0.2	80	web-browsing	alert	medium
04/20 14:32:01	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	139.67.139.181		50.0.0.2	80	web-browsing	alert	medium
04/20 14:32:10	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	139.67.139.181		50.0.0.2	80	web-browsing	alert	medium
04/20 14:31:30	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	139.67.139.181		50.0.0.2	80	web-browsing	alert	medium
04/20 13:54:42	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	139.67.112.48		50.0.0.2	80	web-browsing	alert	medium
04/20 13:54:42	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	139.67.112.48		50.0.0.2	80	web-browsing	alert	medium
04/20 13:54:20	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	139.67.112.48		50.0.0.2	80	web-browsing	alert	medium
04/20 13:54:20	vulnerability	HTTP SQL Injection Attempt	Untrusted-Ext	DMZ	139.67.112.48		50.0.0.2	80	web-browsing	alert	medium

Figure 4.6: Shows IDS capturing SQL Injection attacks

In another instance as shown in Figure. 4.7 below, the IDS detected a spyware JBoss.Worm Command and Control. According to Amazon Web Service, the JBoss.Worm Command and Control is a worm that runs on an infected host that scans other network and connects to unprotected JMX console in order to execute some codes on the victim [59]. The IDS identified this attack as critical and performed reset-both actions on it. An action that resets the connection if it is TCP based and drop the connection if it is UDP based. Because of this, a configuration is set on the IDS to block any such malicious traffic.



Virtual System vsys1
Device SN
IP Protocol tcp
Log Action
Generated Time
Receive Time 2016/04/21 07:46:11

User-Agent
Referer
X-Forwarded-For

Zone DMZ
Interface ethernet1/3
NAT IP 172.16.1.2
NAT Port 80

Zone Untrusted-Ext
Interface ethernet1/1
NAT IP 119.9.25.204
NAT Port 35542

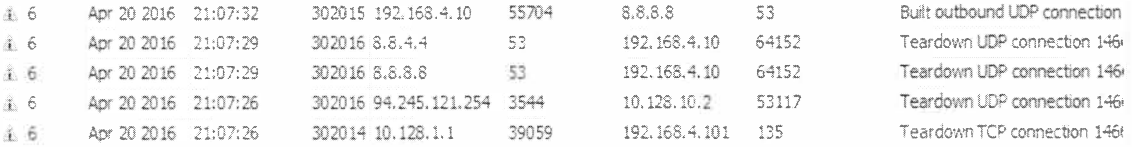
Threat Type spyware
Threat Name JBoss.Worm Comman...
ID 13121
Severity critical
Repeat Count 1
URL zecmd.jsp
Pcap ID 0

Captive Portal
Proxy Transaction
Decrypted
Packet Capture
Client to Server
Server to Client ☑

PCAP	Receive Time ▲	Log	Type	Application	Action	Rule	Bytes	Packets	Severity	Category	URL/...
	2016/04/21 07:46:11	THREAT	spyware	web-browsing	reset-both	UnT-DMZ			critical	any	zecm...
	2016/04/21 07:47:35	TRAF...	end	web-browsing	allow	UnT-DMZ	324	4		unknown	

Figure 4.7: Shows a detected spyware

The IDS/IPS design proved to be secure because there is no traffic able to breakthrough from Internet into the IPS, which directly connects behind the IDS. However, the IPS monitors all traffic leaving the internal network and prevents any suspicious response to traffic initiated from the inside. Figure. 4.8 shows a closed UDP session from an IP address 94.245.121.254 going to 10.128.10.2, which is a webserver on the DMZ interface of the IPS.



```
i 6   Apr 20 2016   21:07:32   302015 192.168.4.10     55704   8.8.8.8         53      Built outbound UDP connection
i 6   Apr 20 2016   21:07:29   302016 8.8.4.4          53      192.168.4.10    64152   Teardown UDP connection 146
i 6   Apr 20 2016   21:07:29   302016 8.8.8.8          53      192.168.4.10    64152   Teardown UDP connection 146
i 6   Apr 20 2016   21:07:26   302016 94.245.121.254   3544    10.128.10.2     53117   Teardown UDP connection 146
i 6   Apr 20 2016   21:07:26   302014 10.128.1.1       39059   192.168.4.101   135     Teardown TCP connection 146
```

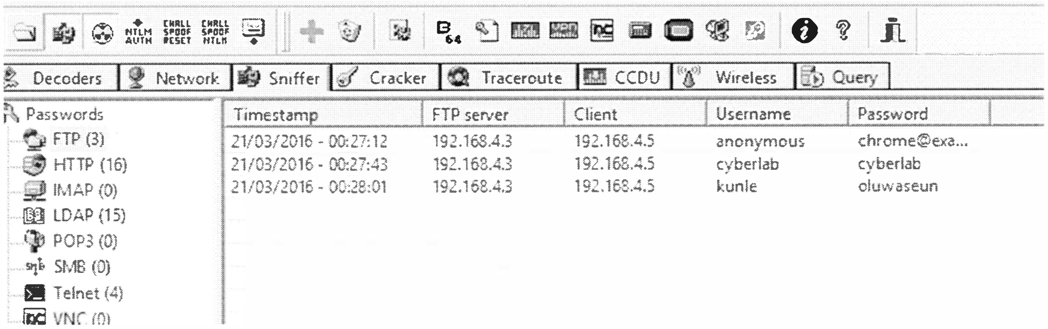
Figure 4.8: Shows a closed UDP session

4.2 Conclusion

The main purpose of this research is to research and propose an initial solution for the new Master of Science program in Cyber Security at EIU. This research fulfills this purpose. In addition, the research also fulfills all the set objectives set at the beginning. The design developed would afford student to learn real cyber-attacks detection and prevention techniques to complement Cyber Security theoretical knowledge. In addition, the public testing site would also allow students to learn both within and outside of the classroom. Furthermore, the public testing site would invite hackers and it is expected that new and sophisticated attacks might be detected and student can carry out further research on these attacks.

4.3 Recommendation

This design is subjected to the man in the middle attack by using IP spoofing techniques to poison the router's interface that connects to the internal switch. The result shows that the design could not stop this form of attack. Figure 4.9 below shows how an attacker was able to sniff FTP login details.



Timestamp	FTP server	Client	Username	Password
21/03/2016 - 00:27:12	192.168.4.3	192.168.4.5	anonymous	chrome@exa...
21/03/2016 - 00:27:43	192.168.4.3	192.168.4.5	cyberlab	cyberlab
21/03/2016 - 00:28:01	192.168.4.3	192.168.4.5	kunle	oluwaseun

Figure 4.9: Showing internal attacker capturing FTP credentials

Because of this, the recommendation for further research is to improve this design to detect and prevent internal attacks. In addition, a honeypot should be implemented on both the external DMZ and the internal network in order to have a repository that store attackers' activities for the purpose of thorough incidence analysis. Furthermore, subsequent research can focus on creating a VPN access for remote site users needing to communicate with the internal network from the outside over a public network.

In summary, it is my recommendation that the Firewall laboratory set up with IPS/IDS can be enhanced with additional research activities like:

- The design of an internal watchdog (IDS/IPS) to protect internal users or intruders from penetrating the systems in spite of the current protections.
- VPN access to at least the DMZ and Internal Zones to study the risk involved in this kind of activities as many companies allow some authorized employees to access internal servers.
- To launch a systematic attack (internal auditing) on the system by our own people to explore all the avenues or possible holes we have not identified yet.
- The hardening of the Windows servers to protect them if an intruder is able to reach them.
- The hardening of the switches to protect from internal attackers.
- Further research/implementation is necessary to ensure a well-protected log system that allows us to keep the records of the hacker's activities (in successful attacks) without allowing the hacker to delete the records.

- Access to the laboratory facilities also should be monitored (logins to the machines with additional security i.e biometrics) to ensure only authorized users can change our configurations.
- In the academic area, develop laboratory guidelines to set up and monitor
    - The Palo Alto Firewall (IDS)
    - The Cisco Firewall box (IPS)
    - The Windows servers
    - The Architecture as a whole (replication of the system with laboratory guidelines)

References

[1]B. Jasiul *et al.*, “Detection and Modelling of Cyber Attacks with Petri Nets”. *Entropy*, 16(12), 6602-6623. Doi:10.3390/e16126602, 2014.

[2]Center for strategic and International studies. “Net Losses: Estimating the Global Cost of Cybercrime”, 2014[online]. Available: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf. [Accessed: 21- Nov- 2015].

[3]N. Waisman *et al.*, “Methods and Apparatus for computer Network Security using Intrusion Detection and Prevention”. US Patent 7225468 B2, May 29, 2007.

[4]R. K. Singh, & T. Ramanujam, “Intrusion Detection System Using Advanced Honeypots”. *International Journal of Computer Science and Information Security*,*2*(1). 2009

[5]A. Conklin and G. White, “Principles of Computer Security”, 2010, pp. 333

[6]S. David *et al.*, “Efficacy of Attack Detection Capability of IDPS Based on Its Deployment in wired and Wireless Environment,” *International Journal of network Security & Its Applications*, vol. 5, March 2013.

[7]E. Schultz, “Intrusion prevention”. *Computers & Security*, 23. 265-266. Doi: 10.1016/j.cose.2004.04.004, 2004.

[8]S.A. Ashoor, & S. Gore, “Intrusion Detection System (IDS) & Intrusion Prevention System (IPS): Case Study”. *International Journal of Scientific Engineering Research, 2(7),* 1-3, 2011.

[9]N. Stanciu, “Technologies, Methodologies and Challenges in Network Intrusion detection and Prevention Systems”. *Informatica Economica*, 17(1), 144-156. Doi:10.12948/issn14531305, 2013.

[10]M. Korčák *et al.*, “Intrusion Prevention/Intrusion Detection System (IPS/IDS) for Wifi Networks”. *Internal journal of computer networks & communications (IJCNC).* 6(4). Doi: 10.5121/ijcnc.2014.64.07, 2014.

[11]N. Spring, “Cyber Security: Are We Doing Enough”? (Cover story). *Electric Light & Power*, 86(3), 20-26, 2008.

[12]A. McGettrick, “Toward Curricular Guidelines for Cybersecurity: Report of a Workshop on Cybersecurity Education and Training”. Retrieved from https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf. 2013

[13]J. A. Chisholm, “Analysis on the Perceived Usefulness of Hands-on Virtual Labs in Cybersecurity Classes”, 2015.

[14] HM Government. “Cyber Security Skills: Business perspectives and Government’s next steps”. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf, 2014.

[15]L. Saporito, “The Cybersecurity Workforce: States’ Needs and Opportunities” *(Washington, D.C.: National Governors Association Center for Best Practices).* 2014

[16]E.A Fisher, "Cybersecurity Issues and Challenges: In Brief ", Congressional Research Service, Dec. 2014

[17]C. Baylon, "Challenges at the intersection of cyber security and space security", Country and Institution perspectives, Dec. 2014

[18]Office of the privacy Commissioner of Canada, "Privacy and Cyber Security", Emphasizing Privacy Protection in Cyber Security Activities, 2014

[19]R.C. Armstrong, J.R. Mayo & F. Siebenlist, "Complexity Science Challenges in Cyber Security", Sandia national Laboratories, 2009

[20]C. Folk, D. Hurley, W. K. Kaplow and J. F.X. payne, The Security implications Of The Internet Of things, 2015.

[21]The Impact of Mobile Devices on Information Security: A Survey of IT AND Security Professionals. Check Point Software Technologies Limited, 2014, pp. 1-10.

[22]R. Broadburst, P. Grabosky, M. Alazab & S. Chon, "Organizations and Crime: An Analysis of The nature of Groups engaged in Cyber crime", International journal of cyber criminology, vol. 8, no.1, 2014

[23]J. Jun, S. lafoy and E. john, "The Organization Operations in North Korea", Center For Strategic & International Studies, 2014

[24]. C.A theophany, "Information warfare: Cyberattacks on Sony", 2015

[25]P. A. Ferrillo, Navigating The Cybersecurity Storm, Advisen, pp. 3-9, 2015

[26]HM Government, 2015 Information Security Breaches Survey, 2015

[27]J. Bauer and W. Dutton, "The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet", SSRN Electronic Journal, 2016.

[28]S. Uldun Mostfa Kamal, R. Jabbar Abd Ali, H. Kamal Alani and E. Saad Abdulmajed, "Survey and Brief History on Malware in Network Security Case Study: Viruses, Worms and Bots", ARPN Journal of Engineering and Applied Sciences, vol. 11, no. 1, pp. 683-695, 2016.

[29]R. Miller, The Changing Face of Cyber-Attacks: Understanding and preventing both external and insider security breaches, 1st ed. CA Technologies, 2016.

[30]Anatomy of Botnet, Fortinet White Paper, n.d

[31] Identifying and Thwarting Malicious Intrusions, McAFee White Paper, 2010

[32]M.A Lawal, A. Md Sultan and S. Ayanloye, "Systematic Literature Review on SQL Injection Attacks", International Journal of Soft Computing, vol. 11, no. 1, pp. 26-35, 2016.

[33]A. Chaturvedi, S. Bagdi and V. Choudhary, "Analysis of SQL Injections Attacks and Vulnerabilities", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, no. 3, pp. 106-109, 2016

[34]L. Bilge and T. Dumitras, "An Empirical Study of Zero-Day Attacks In The Real World", ACM, 2012

[35]S. Egelman, C. Herley and P.C Van Oorschot, "Markets for zero-day exploits: Ethics and Implication". Retrieved from http://dx.doi.org/10.1145/2535813.2535818, ACM, 2013

[36]A. Hegde, "MAC Spoofing Detection and Prevention", International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, no. 1, pp. 229-232, 2016.

[37]S. Farraposo, L. Gallon and P. Owezarski, *Network Security and DoS Attacks*, 1st ed. 2005, pp. 3-5.

[38]DNS: Types of attack and security techniques. AFNIC, 2009. Retrieved from (this reference has a different font???) https://www.afnic.fr/medias/documents/afnic-dns-attacks-security-guide-2009-06.pdf

[39]S. Gangan, A Review of Man-in-the-Middle Attacks, n.d

[40]L. Vishnoi and M. Agarwal, "Session Hijacking and its Countermeasures", International Journal of Scientific Research Engineering & Technology, vol. 2, no. 5, pp. 250-252, 2013.

[41]S.C Tharaka, R.L.C. Silva, S. Sharmila, S. U.I. Silva, K.L.D.N. Liyanage and A.A.T.K.K. Amarasinghe, D, "High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies", International Journal of Scientific and Research Publications, vol. 6, no. 4, pp. 504-508, 2016.

[42]W. Conklin, G. White, D. Williams, R. Davis and C. Cothren, Principles of computer security, 2016

[43]A. Chopra, "Security Issues of Firewall", International Journal of P2P Network Trends and Technology, vol. 22, no. 1, pp. 4-9, 2016.

[44]B. Rajeswari, "Addressing Security Challenges in Internet of Things", International Journal of Scientific Engineering and Applied Science, vol. 2, no. 3, pp. 393-395, 2016.

[45]R.P. Patil, Y. Sharma and M. Kshirasagar, "Performance Analysis of Intrusion Detection Systems Implemented using Hybrid Machine Learning Techniques", International Journal of Computer Applications, vol. 133, no. 8, pp. 35-38, 2016.

[46]O. Cepheli, S. Büyükçorak and G. Karabulut Kurt, "Hybrid Intrusion Detection System for DDoS Attacks", Journal of Electrical and Computer Engineering, vol. 2016, pp. 1-8, 2016.

[47]N. Das and T. Sarkar, "Survey on Host and Network Based Intrusion Detection System", Int. J. Advanced Networking and Applications, vol. 6, no. 2, pp. 2266-2269, 2016.

[48]M. Alkasassbeh, A.B.A. Hassanat, G. Al-Naymat and M. Almseidin, "Detecting Distributed Denial of Service Attacks Using Data Mining Techniques", International Journal of Advanced Computer Science and Applications, vol. 7, no. 1, pp. 436-445, 2016.

[49]V.C. Bini, A. Shaji, P. Jayakumar and M.K. Nimmi, "A Study on Intrusion Detection and Protection Techniques", IOSR Journal of Computer Engineering, pp. 7-10, 2016.

[50]N. Chakraborty, "Intrusion Detection System and Intrusion Prevention System: A Comparative Study", International Journal of Computing and Business Research, vol. 4, no. 2, 2013.

[51]H. Kaur and S. Dhingra, "A Review: Prevent SQL Injection Attacks Using IPS", International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 10, 2014.

[52]A. Uddin and L. Hasan, "Design and Analysis of Real-time Network Intrusion Detection and Prevention System using Open Source Tools", International Journal of Computer Applications, vol. 138, no. 7, 2016.

[53]R. Holland and H. Shey, Predictions 2016: Cybersecurity Swings To Prevention, Forrester, 2015.

[54]Institute for Information Security and Privacy, Emerging Cyber Threats Report 2016

[55]Toward Curricular Guidelines for Cybersecurity, 1st ed. Association for Computing Machinery, 2013.

[56]L. Cleghorn, "Network Defense Methodology: A Comparison of Defense in Depth and Defense in Breadth", *Journal of Information Security*, vol. 04, no. 03, pp. 144-149, 2013.

[57]M. Abderrahim, "THE FIGHT AGAINST IP SPOOFING ATTACKS: NETWORK INGRESS FILTERING VERSUS FIRSTCOME, FIRST-SERVED SOURCE ADDRESS VALIDATION IMPROVEMENT (FCFS SAVI)", *International Journal of Security, Privacy and Trust Management (IJSPTM)*, vol. 5, no. 1, 2016.

[58]M. Cotton and L. Vegoda, *Best Current Practices: Special Use IPv4 Addresses.* 2010.

[59]"JBoss Worm Spreading via Unpatched or Unsecured JBoss Application Server", *Amazon Webservices*, 2011. [Online]. Available: https://aws.amazon.com/security/security-bulletins/jboss-worm-spreading-via-unpatched-or-unsecured-jboss-application-server/. [Accessed: 21- Apr- 2016].

Appendices

Appendix A

Definition of Terms

Firewall: is a network device-hardware, software, or a combination thereof- whose purpose is to enforce a security policy across its connections by allowing or denying traffic to pass into or out of the network

Intrusion detection Systems (IDS): is a security system that detects inappropriate or malicious activity on a computer or network.

Intrusion Prevention System (IPS): An intrusion prevention system monitors network traffic for malicious or unwanted behavior and can block, reject, or redirect that traffic in real time.

Demilitarized Zone (DMZ): A DMZ sometimes referred to as a perimeter network is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet.

Router: A router is a device that forwards data packets along networks

ARP poisoning: is a type of attack in which a malicious actor sends falsified ARP (Address resolution Protocol) messages over a local area network.

Virtual Private Network (VPN): A VPN is a technology that creates an encrypted connection over a less secure network.

Internet of Things (IoT): IoT refers to the ever-growing network of physical objects that feature an IP address for Internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems.

Network Intrusion Detection Systems (NIDS): NIDS focuses on network traffic-the bits and bytes travelling along cables and wires that interconnect the systems.

Active Directory: Active Directory is a database that keeps track of all the user accounts and passwords in your organization. It allows you to store your user accounts and passwords in one protected location, improving your organization's security.

Domain Controller: a domain controller (DC) is a server that responds to security authentication requests (logging in, checking permissions, etc.) within a domain.

Virtualization: Virtualization refers to the act of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, operating systems, storage devices, and computer network resources.

WMI: Windows Management Instrumentation (WMI) is a set of specifications from Microsoft for consolidating the management of devices and applications in a network from Windows computing systems. WMI is installed on all computers with Windows operating systems.

CIMV2: CIMV2 is the default WMI namespace on Windows machines.

Spamming: This is the use of electronic messaging systems to send unsolicited message (spam), especially advertising, as well as sending messages repeatedly on the same site.

Bitcoin Mining: This is the process of transactions in the digital currency system, in which the records of current Bitcoin transactions, known as blocks, are added to the record of the past transactions, known as the block chain.

Industrial Espionage: Spying directed toward discovering the secrets of a rival manufacturer or other industrial company

Appendix B

Configuration for firewall/IPS

```
IPS# sh run
: Saved
:
ASA Version 9.1(2)
!
hostname IPS
enable password E.bgA9kfttKB/.vi encrypted
names
!
interface GigabitEthernet0/0
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface GigabitEthernet0/1
 nameif outside
 security-level 0
 ip address 10.128.1.2 255.255.255.0
!
interface GigabitEthernet0/2
 nameif DMZ
 security-level 50
 ip address 10.128.10.1 255.255.255.0
!
interface GigabitEthernet0/3
 nameif inside
 security-level 100
 ip address 172.16.10.1 255.255.255.0
!
interface GigabitEthernet0/4
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/5
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 speed 100
 management-only
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
ftp mode passive
clock timezone GMT 0
same-security-traffic permit inter-interface
object network DMZ_outside
 subnet 0.0.0.0 0.0.0.0
object network web-server-from-outside-thru-palo
 host 10.128.10.2
object network web-server-fromInside
 host 10.128.10.2
object network IntrnalRouterNetwork
 subnet 192.168.100.0 255.255.255.0
object network inside-network
 subnet 172.16.10.0 255.255.255.0
object network 10.128.1.1
 host 10.128.1.1
object network 172.16.10.2
 host 172.16.10.2
object network 10.128.1.0
 subnet 10.128.1.0 255.255.255.0
object network 10.128.1.2
 host 10.128.1.2
object network Nat_inIPSrouterToOutside
 subnet 172.16.10.0 255.255.255.0
object network IntASA
 subnet 0.0.0.0 0.0.0.0
object network officeLanToInside
 subnet 192.168.4.0 255.255.255.0
object network office_Lan
 subnet 192.168.4.0 255.255.255.0
object network Inside_going_Outside
 subnet 172.16.10.0 255.255.255.0
 description Inside traffic should go out
```

```
object network Inside_goingTO_InsideDMZ
 subnet 172.160.10.0 255.255.255.0
 description Inside traffic going to DMZ
object network Outside_DMZ
 subnet 176.16.1.0 255.255.255.0
 description The outside DMZ network
object network Inside_Going_Outside
 subnet 172.16.10.0 255.255.255.0
 description network address btw ASA and internal Router
object network Inside_Going_outside
 subnet 172.16.10.0 255.255.255.0
object network Network_Behind_Internal_Router
 subnet 192.168.4.0 255.255.255.0
 description Network_Behind_Internal_Router
object network Nat_Inside_To_DMZ
 subnet 172.16.10.0 255.255.255.0
access-list inside_access_in extended permit ip any any
access-list OutsideThruPaloToDMZ extended permit ip any host 10.128.10.2
access-list OutsideThruPaloToDMZ extended permit ip object 10.128.1.1 object
172.16.10.2
access-list inside_access_out extended permit icmp 10.128.10.0 255.255.255.0 object
Network_Behind_Internal_Router echo-reply
access-list inside_access_out extended permit ip any any
access-list inside_access_in_1 extended permit ip 172.16.10.0 255.255.255.0 any
access-list inside_access_in_1 extended permit ip object
Network_Behind_Internal_Router any
access-list ALLOW_OUT_IN extended permit icmp any any
access-list ALLOW_OUT_IN_echo extended permit icmp any any echo-reply
access-list ALLOW_OUT_IN_echo extended permit ip object 10.128.1.1 any
access-list DMZ_access_in extended permit ip 10.128.10.0 255.255.255.0 any
access-list DMZ_ALLOW_echo_Reply extended permit icmp 10.128.10.0 255.255.255.0
172.16.10.0 255.255.255.0 echo-reply log
access-list DMZ_access_in_1 extended permit ip any any
access-list DMZ_access_in_2 extended permit icmp 10.128.10.0 255.255.255.0
172.16.10.0 255.255.255.0 echo-reply
access-list DMZ_access_in_2 extended permit icmp 10.128.10.0 255.255.255.0 object
Network_Behind_Internal_Router echo-reply
access-list DMZ_access_in_2 extended deny ip any object
Network_Behind_Internal_Router
access-list DMZ_access_in_2 extended deny ip any 172.16.10.0 255.255.255.0
access-list DMZ_access_in_2 extended permit ip any any
pager lines 24
logging enable
logging asdm informational
mtu outside 1500
mtu DMZ 1500
mtu inside 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
!
object network DMZ_outside
 nat (DMZ,outside) dynamic interface
object network web-server-from-outside-thru-palo
 nat (DMZ,outside) static interface
access-group ALLOW_OUT_IN_echo in interface outside
access-group DMZ_access_in_2 in interface DMZ
access-group inside_access_in_1 in interface inside
access-group inside_access_out out interface inside
!
router eigrp 1000
 no auto-summary
 network 10.0.0.0 255.0.0.0
 network 172.16.0.0 255.255.0.0
!
route outside 0.0.0.0 0.0.0.0 10.128.1.1 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
```

```
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection scanning-threat
threat-detection statistics
threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400 average-rate 200
ssl encryption aes128-sha1 3des-sha1
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
  inspect icmp error
 class class-default
  ips inline fail-open
  user-statistics accounting
!
```

```
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
Cryptochecksum:060d16daa1e6364b4b88ace962b9c94e
: end
```

Appendix C

Boundary Router Configuration

```
Current configuration : 2022 bytes
!
! Last configuration change at 03:18:50 UTC Mon Apr 18 2016
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
service-module wlan-ap 0 bootimage autonomous
!
no ipv6 cef
ip source-route
ip cef
!
!
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
!
license udi pid CISCO1941W-A/K9 sn FTX152583HY
hw-module ism 0
!
!
Redundancy
!
!

interface GigabitEthernet0/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface wlan-ap0
 description Service module interface to manage the embedded AP
 no ip address
 arp timeout 0
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/1
 ip address 50.0.0.1 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface Wlan-GigabitEthernet0/0
 description Internal switch interface connecting to the embedded AP
!
interface Serial0/0/0
 no ip address
 shutdown
 no fair-queue
 clock rate 2000000
!
interface Serial0/0/1
 ip address 192.168.240.2 255.255.255.252
!
interface GigabitEthernet0/1/0
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface GigabitEthernet0/1/4
!
interface GigabitEthernet0/1/5
!
interface GigabitEthernet0/1/6
!
interface GigabitEthernet0/1/7
!
```

```
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat inside source list 101 interface GigabitEthernet0/0 overload
ip nat inside source static tcp 50.0.0.2 80 192.168.1.2 80 extendable
!
access-list 101 permit ip any any
ip access-list extended ingress-antispoof
 deny   ip 10.0.0.0 0.255.255.255 any
 deny   ip 172.16.0.0 0.15.255.255 any
 deny   ip 192.168.0.0 0.0.255.255 any
 deny   ip 127.0.0.0 0.255.255.255 any
 deny   ip 224.0.0.0 31.255.255.255 any
 deny   ip 169.254.0.0 0.0.255.255 any

control-plane
!
!
!
line con 0
line aux 0
line 67
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 login
 transport input all
!

scheduler allocate 20000 1000

end
```

Appendix D

Internal Router Configuration

```
Current configuration : 2494 bytes
!
! Last configuration change at 04:34:50 UTC Sat Apr 9 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname InternalRouter
!
boot-start-marker
boot-end-marker
!
!
no logging console
enable secret 5 $1$P17h$Tw9icjdxSyPtslSX3fU531
!
no aaa new-model
service-module wlan-ap 0 bootimage autonomous
!
ip cef
!
!
!
!
!
!
ip domain name mythesis.org
no ipv6 cef
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941W-A/K9 sn FTX18228352
hw-module ism 0
!
!
```

```
!
username cisco secret 5 $1$CW.o$G6yNKhr9Da84rpYnj/HQd0
!
!
ip ssh version 2
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 ip address 192.168.4.1 255.255.255.0
 duplex auto
 speed auto
!
interface wlan-ap0
 description Service module interface to manage the embedded AP
 no ip address
 arp timeout 0
 no mop enabled
 no mop sysid
!
interface GigabitEthernet0/1
 ip address 172.16.10.2 255.255.255.0
 duplex auto
 speed auto
!
interface Wlan-GigabitEthernet0/0
 description Internal switch interface connecting to the embedded AP
 no ip address
!
interface Serial0/0/0
 ip address 192.168.240.13 255.255.255.252
 clock rate 2000000
!
interface Serial0/0/1
 ip address 192.168.240.10 255.255.255.252
!
interface Vlan1
 no ip address
```

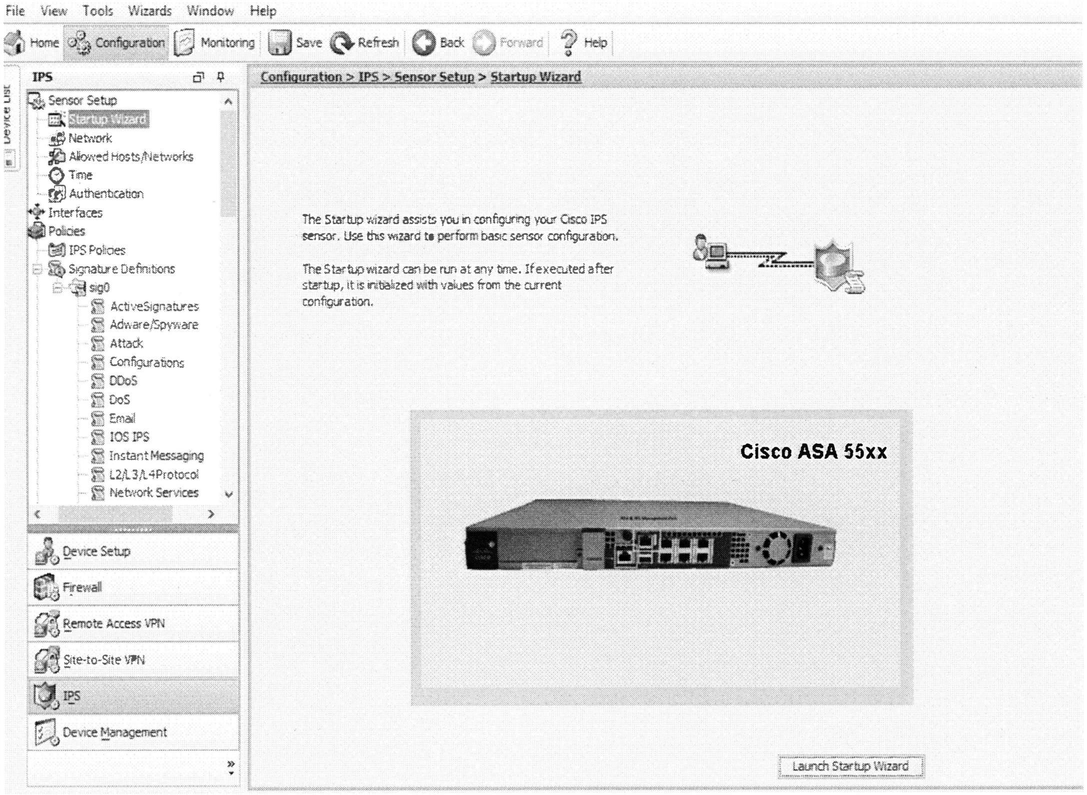
```
!
!
router eigrp 100
 network 192.168.240.0
!
!
router eigrp 1000
 timers active-time 30
 metric maximum-hops 50
 network 172.16.0.0
network 192.168.4.0
 !
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 172.16.10.1
ip route 10.128.1.0 255.255.255.0 172.16.10.1
ip route 10.128.10.0 255.255.255.0 172.16.10.1
ip route 50.0.0.0 255.255.255.252 172.16.10.1
ip route 172.16.1.0 255.255.255.0 172.16.10.1
!
!
!
control-plane
!
!
!
line con 0
 password cisco
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line 67
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
line vty 0 4
 password cisco
 login local
 transport input all
!
scheduler allocate 20000 1000
!
end
```

Appendix E

Configuration for IPS Sensor

The following are the steps to configure the IPS sensor

1. Click on IPS and then click on startup wizard



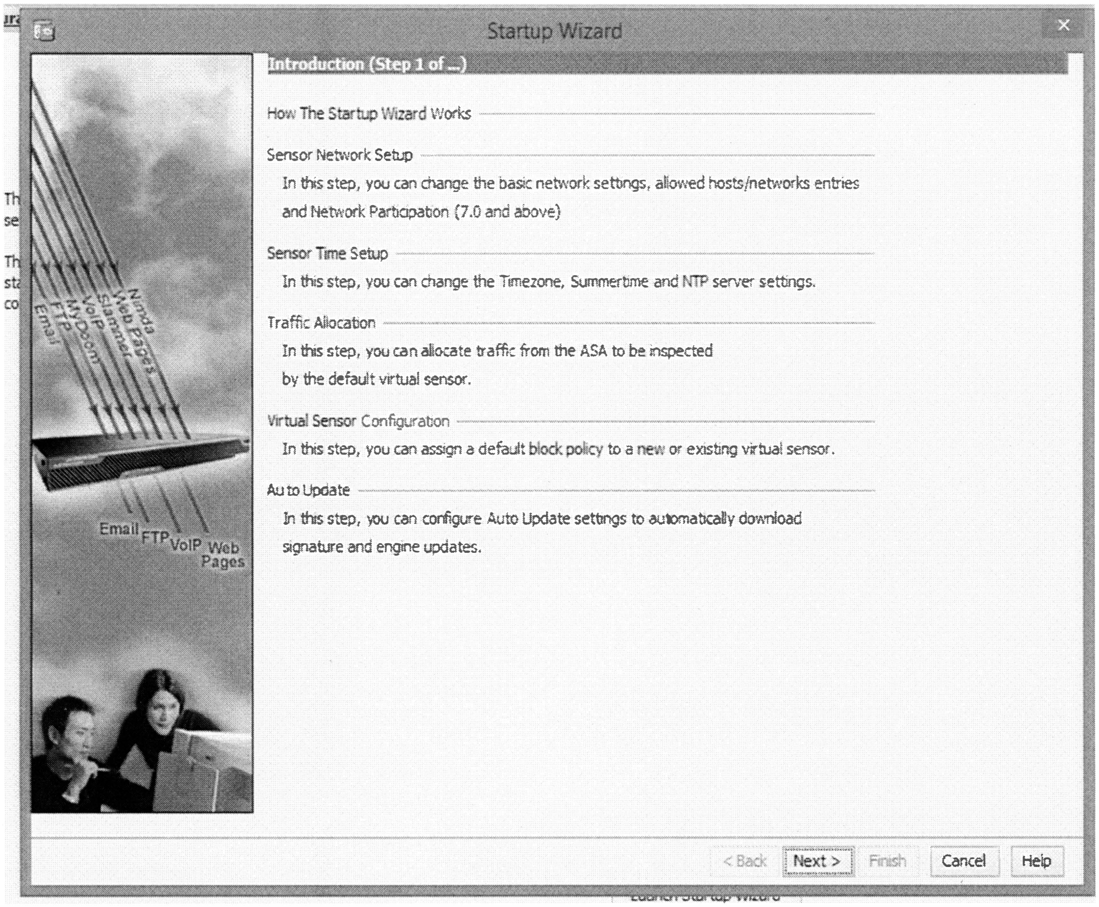
Configuration > IPS > Sensor Setup > Startup Wizard

The Startup wizard assists you in configuring your Cisco IPS sensor. Use this wizard to perform basic sensor configuration.

The Startup wizard can be run at any time. If executed after startup, it is initialized with values from the current configuration.

Figure E-1: Showing the startup wizard

2. Click on launch startup wizard



Introduction (Step 1 of ...)

How The Startup Wizard Works

Sensor Network Setup

In this step, you can change the basic network settings, allowed hosts/networks entries and Network Participation (7.0 and above)

Sensor Time Setup

In this step, you can change the Timezone, Summertime and NTP server settings.

Traffic Allocation

In this step, you can allocate traffic from the ASA to be inspected by the default virtual sensor.

Virtual Sensor Configuration

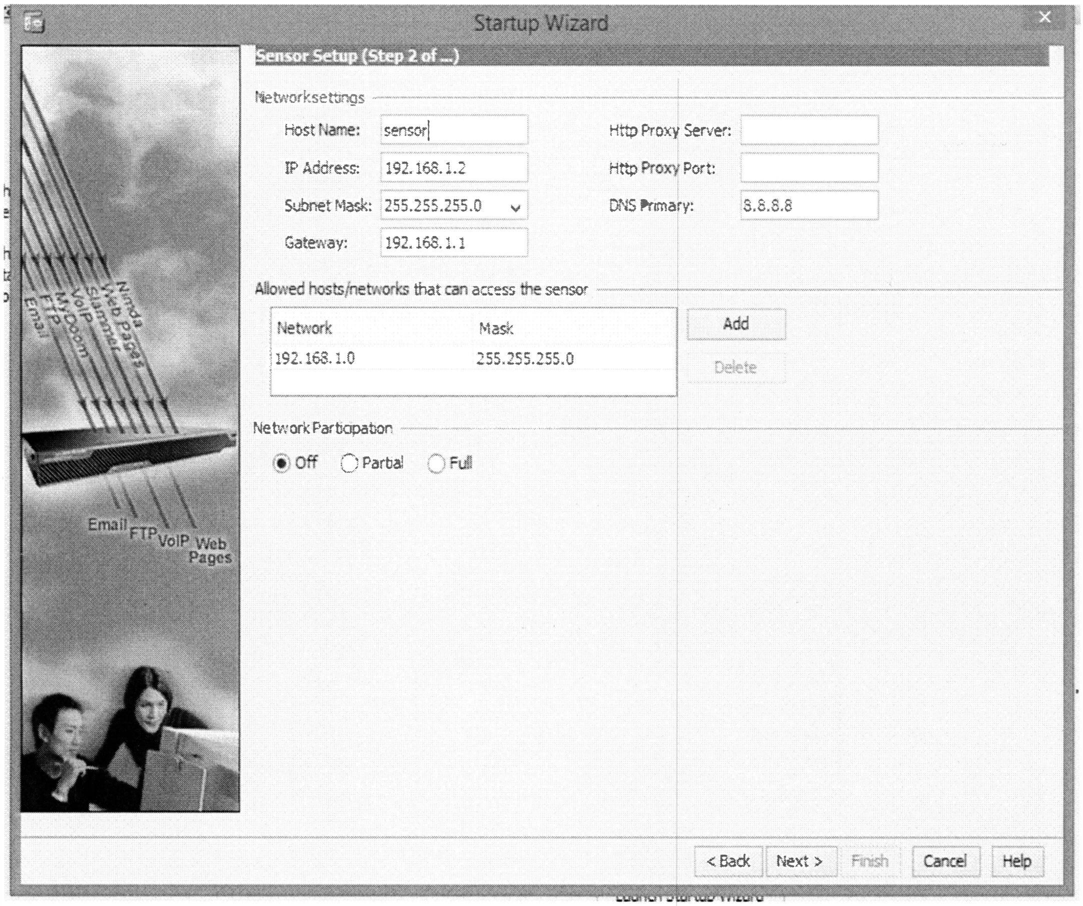
In this step, you can assign a default block policy to a new or existing virtual sensor.

Auto Update

In this step, you can configure Auto Update settings to automatically download signature and engine updates.

Figure E-2: Showing configuration information

3. Click next, enter the name for the IPS sensor, IP address in the same subnet range with the Cisco ASA (firewall) management interface because the IPS sensor shares same management interface with it. The default gateway will be the management interface IP address



Startup Wizard

Sensor Setup (Step 2 of ...)

Networksettings

Host Name: sensor

IP Address: 192.168.1.2

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.1

Http Proxy Server:

Http Proxy Port:

DNS Primary: 8.8.8.8

Allowed hosts/networks that can access the sensor

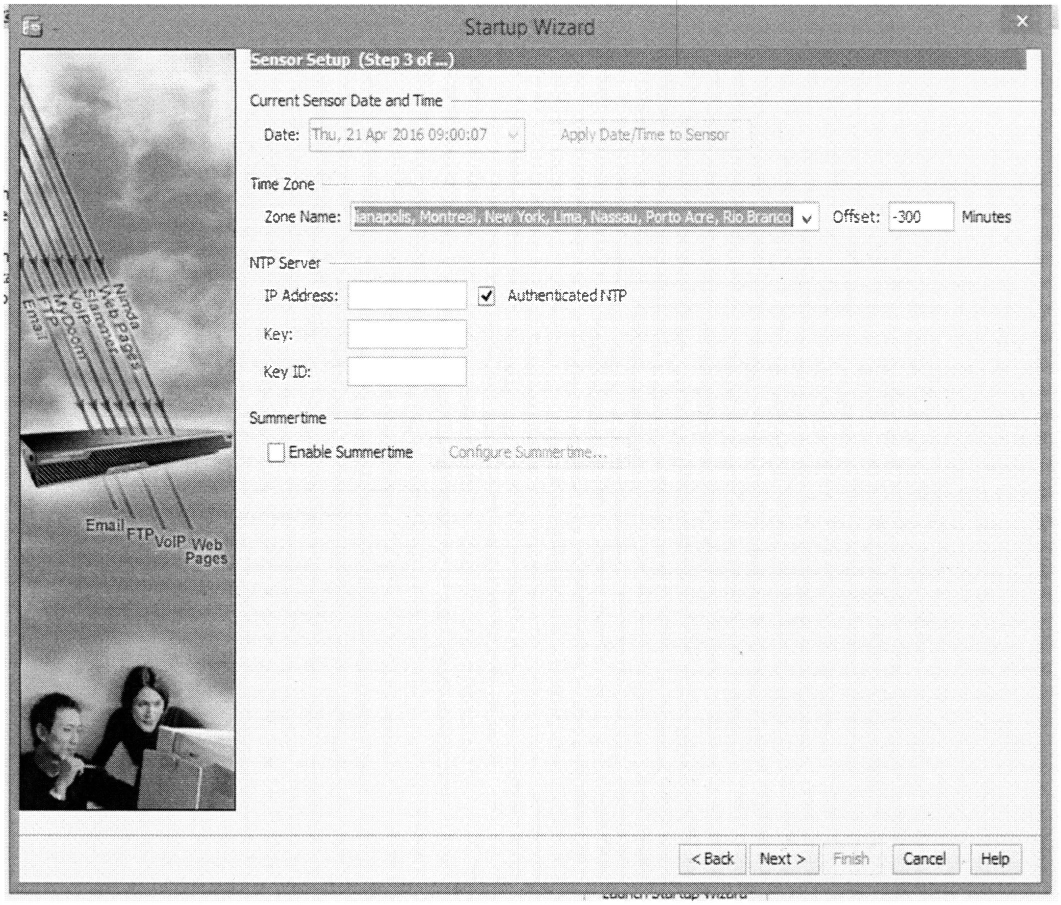
Network	Mask
192.168.1.0	255.255.255.0

Network Participation

● Off ○ Partial ○ Full

Figure E-3: Showing host name and IP address configuration

4. Click next to enter date and time information. You should leave the NTP server information blank except you have an NTP server


Startup Wizard

Sensor Setup (Step 3 of ...)

Current Sensor Date and Time

Date: Thu, 21 Apr 2016 09:00:07

Time Zone

Zone Name: ianapolis, Montreal, New York, Lima, Nassau, Porto Acre, Rio Branco

Offset: -300 Minutes

NTP Server

IP Address:

☑ Authenticated NTP

Key:

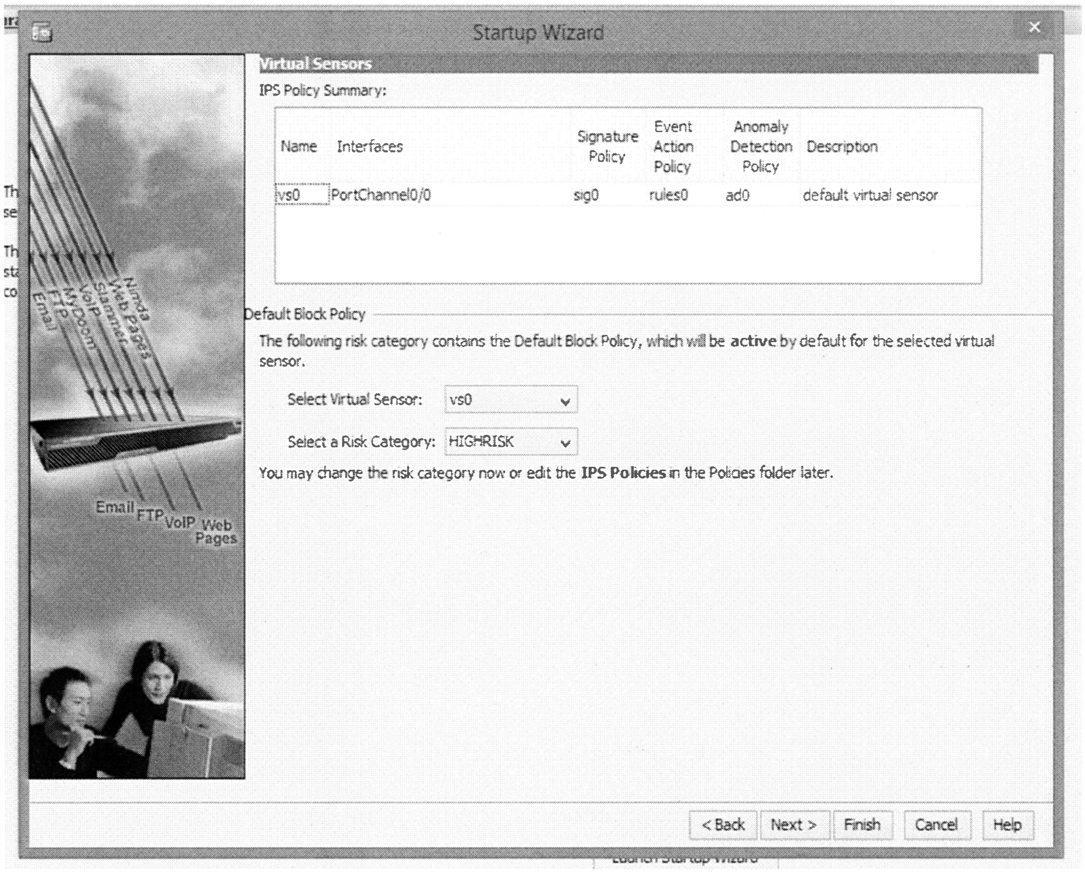
Key ID:

Summertime

□ Enable Summertime

Figure E-4: Showing the how to set date, time and enter NTP server information

5. Click next to see the default IPS policy that blocks HIGHRISK traffic.



Virtual Sensors

IPS Policy Summary:

Name	Interfaces	Signature Policy	Event Action Policy	Anomaly Detection Policy	Description
vs0	PortChannel0/0	sig0	rules0	ad0	default virtual sensor

Default Block Policy

The following risk category contains the Default Block Policy, which will be **active** by default for the selected virtual sensor.

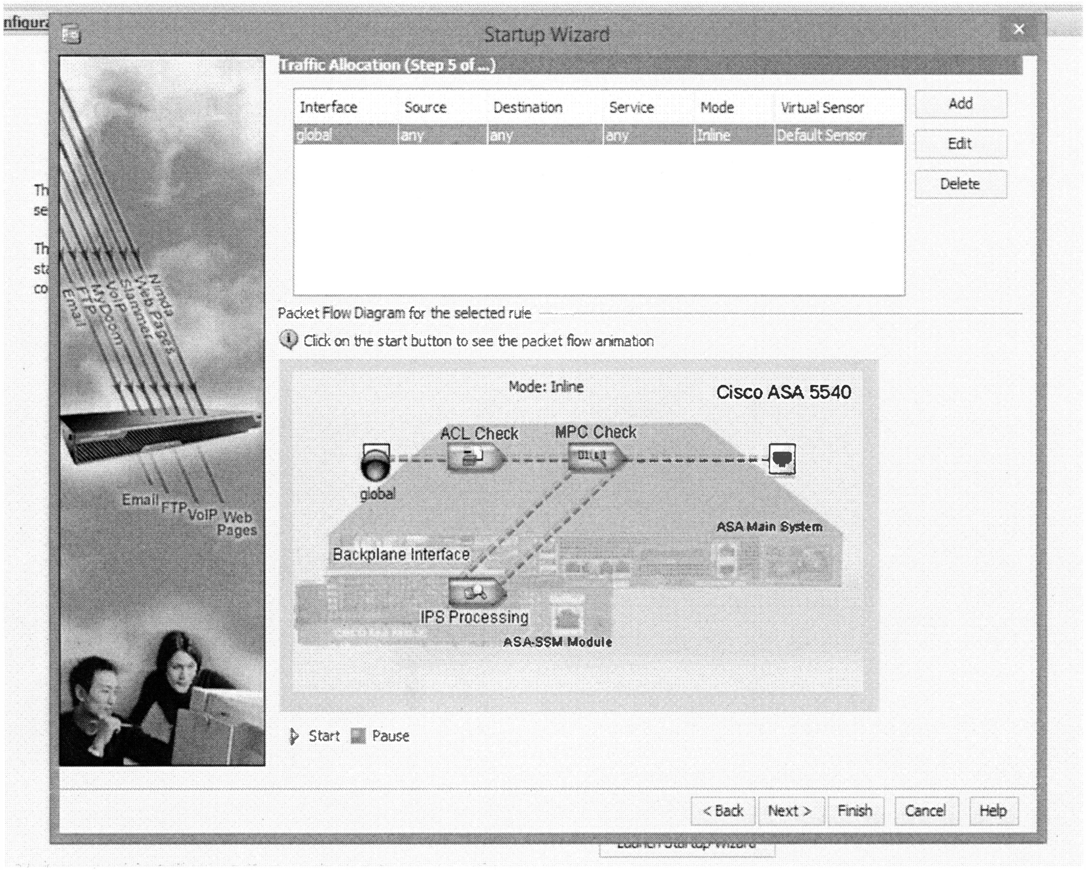
Select Virtual Sensor: vs0

Select a Risk Category: HIGHRISK

You may change the risk category now or edit the **IPS Policies** in the Policies folder later.

Figure E-5: Showing the IPS virtual sensor policy

6. Click next, to configure the IPS sensor to be in inline mode. As shown in the figure below, the rule is set to see traffic from any source going to any destination. You can add more rules here to apply to whatever direction of traffic.



Traffic Allocation (Step 5 of ...)

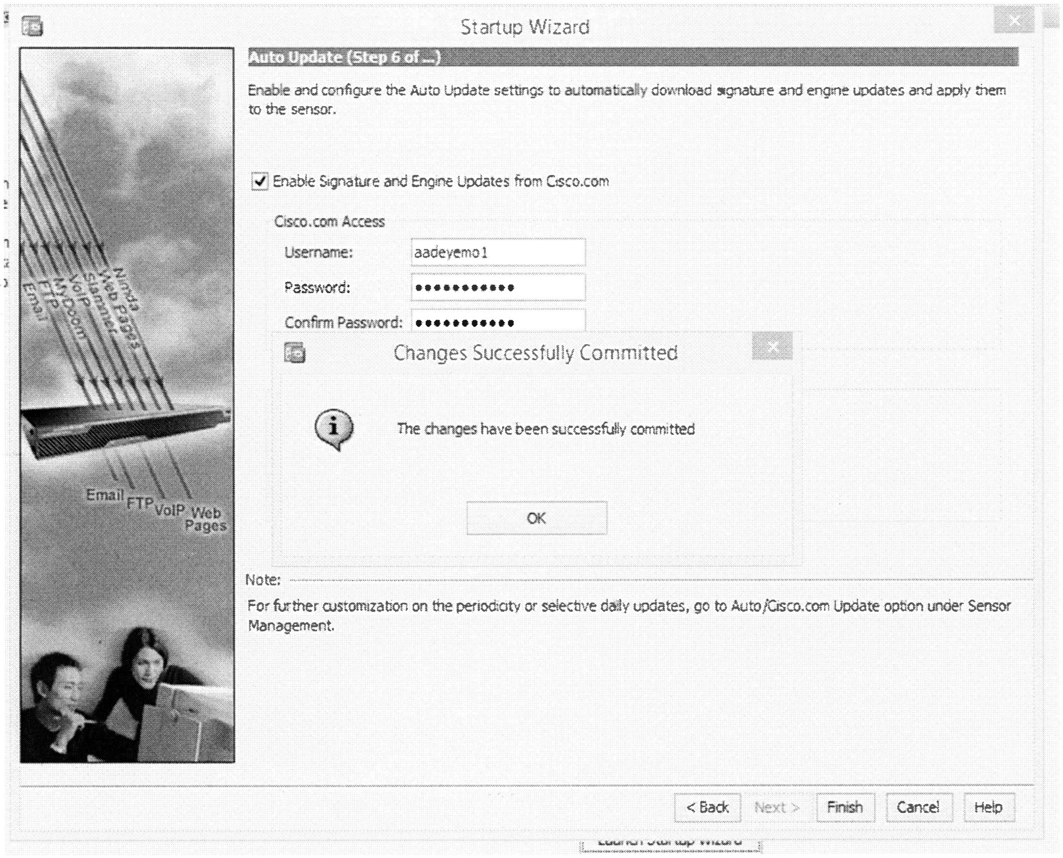
Interface	Source	Destination	Service	Mode	Virtual Sensor
global	any	any	any	Inline	Default Sensor

Packet Flow Diagram for the selected rule

Click on the start button to see the packet flow animation

Figure E-6: Showing the traffic allocation

7. Click next, and then check the enable signature and engine updates from cisco.com. You can create an account on cisco.com. Then enter the account login information as shown below. In addition, you will enter the time when you want the daily updates run. It is very important to enter the appropriate information. Then click next, it will prompt that you commit the saves, click ok. Then click finish.



Startup Wizard

Auto Update (Step 6 of ...)

Enable and configure the Auto Update settings to automatically download signature and engine updates and apply them to the sensor.

☑ Enable Signature and Engine Updates from Cisco.com

Cisco.com Access

Username: aadeyemo1

Password: ●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●

Changes Successfully Committed

The changes have been successfully committed

Note:

For further customization on the periodicity or selective daily updates, go to Auto/Cisco.com Update option under Sensor Management.

Figure E-7: Configuration to enable signature and engine updates from cisco.com

Appendix F

Photo of the IDS/IPS Design

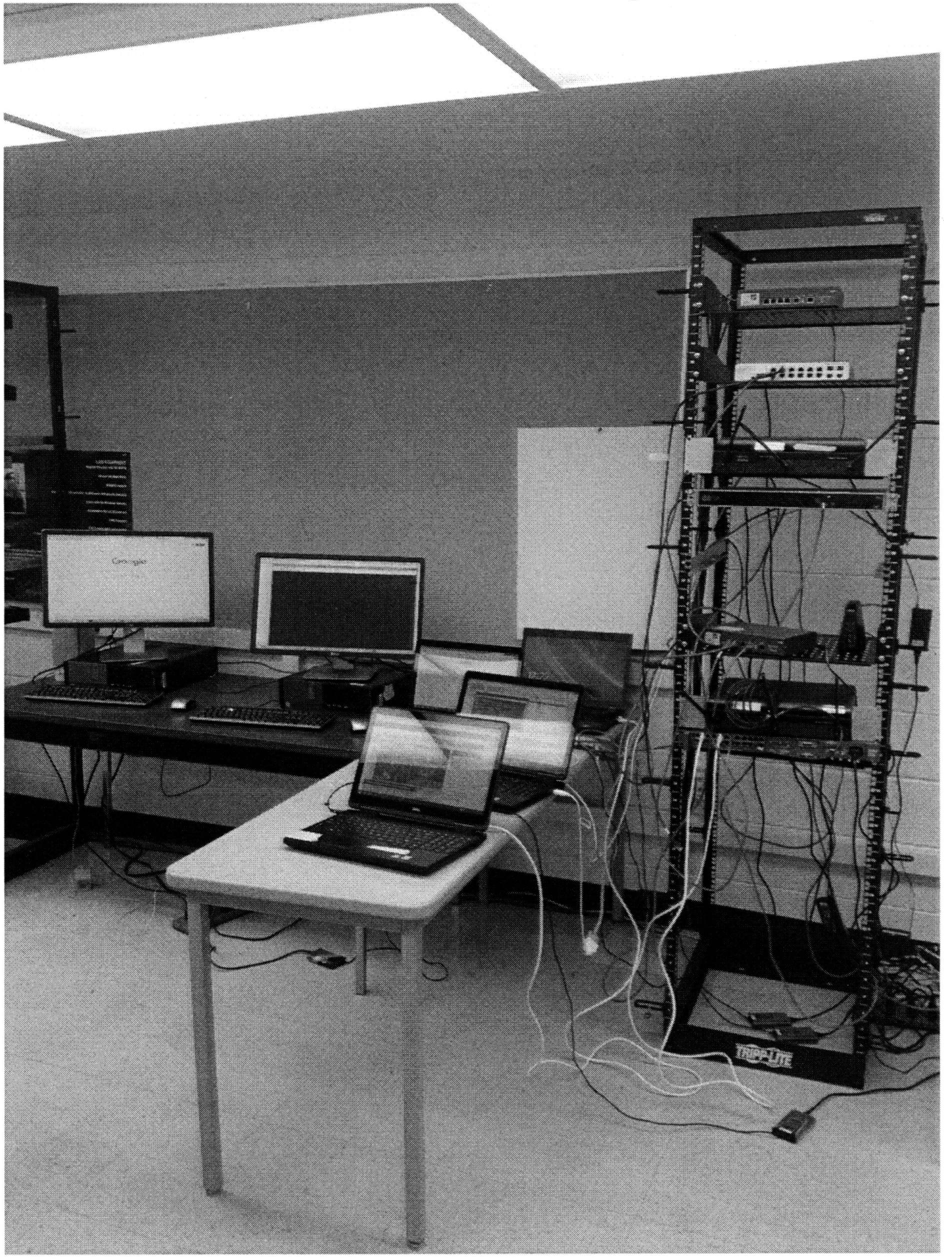


Figure E-8: Photo of Firewall Architecture with IDS/IPS