Computer Engineering Department
Faculty of Engineering
Deanery of Higher Studies
Islamic University – Gaza
Palestine

# Developing Security-Enhanced Model For Enterprise Network

# تطوير نموذج آمن للشبكات المؤسساتية

**By**
**Khaled W. Alnaji**

**Supervisor**
**Dr. Aiman Abu Samra**

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Engineering

1435H (2014)

# Dedication

*To my beloved father Waleed*

*To my beloved mother Sawsan*

*To my beloved wife Manar*

*To my sister Yasmin*

*To my brothers Mohamed, Abedalhadi, and Rashad*

*To my daughters Sawsan and Yara*

*To my son Waleed*

# Acknowledgment

Praise is to Allah, the Almighty for having guided me at every stage of my life.

I would like to express my special appreciation and thanks to my advisor Dr. Aiman Abu Samra, for his guidance, support, motivation, enthusiasm, and immense knowledge during working on my thesis. I would like to thank you for encouraging my research and for allowing me to grow as a research scientist. I would also like to thank Dr. Hasan Qunoo, your guidance helped me in all the time of research and writing of this thesis. Continuing my thanks to thesis committee, both Dr. *Yousuf Abu Shaaban* and Dr. Hasan Qunoo for their suggestions and recommendations which assisted in developing this research.

A special thanks to my family. Words cannot express how grateful I am to my father, my mother, for all of the sacrifices that you've made on my behalf. Your prayer for me was what sustained me thus far. I would also like to thank all of my friends who supported me in writing, and incented me to strive towards my goal. At the end I would like express appreciation to my beloved wife who spent sleepless nights with and was always my support in the moments when there was no one to answer my queries.

# TABLE OF CONTENTS

# List Of Figures

# List Of Tables

# ملخص

تدعم الشبكات المؤسساتية الآلاف من المستخدمين عبر مواقع مختلفة ، و تربط العديد من الشبكات التي يتم توزيعها جغرافيا عبر المسافات الشاسعة, حيث تستضيف الشبكات المؤسساتية العديد من أجهزة الخادمات التي تقدم الكثير من الخدمات مثل تطبيقات الويب وقواعد البيانات و البريد الإلكتروني وغيرها. تختلف الشبكات المؤسساتية عن غيرها من الشبكات من حيث الاختلاف في حجمها ، وإدارة الموارد ، والأمن, حيث تشمل الشبكات المؤسساتية على عدد كبير من الشبكات المحلية و الموسعة و اللاسلكية ، هذا بالإضافة إلى احتوائها على عدد من بروتوكولات الاتصالات المختلفة لربط تلك الشبكات مع بعضها البعض, كذلك تعمل الشبكات المؤسساتية على تسهيل و تبسيط عمليات الاتصال بين مختلف الأجهزة و الأنظمة المحوسبة, حيث يتم مراقبتها بشكل مستمر من أجل توفير إدارة خارجية و داخلية للشبكات المؤسساتية. كما تقوم الشبكات المؤسساتية على تكامل أنظمة التشغيل المختلفة مثل الويندوز و اللينكس والهواتف الذكية و غيرها العديد, علاوة على توفير تكامل بشكل كبير بين بروتوكولات وخدمات الاتصالات. تمثل التهديدات الأمنية مشكلة كبيرة للشبكات المؤسساتية حيث أنها تحاول تدمير خدمات الشبكات المؤسساتية و كذلك إلحاق الضرر بسمعتها و تعطيل الخدمات المقدمة للمستخدمين من خارج و داخل الشبكة. يعتبر APT من التهديدات الثابتة المتقدمة التي تشكل هجمات الكترونية معقدة تستهدف الحكومات والمنظمات و الشركات ، وبالتالي أمن الشبكات المؤسساتية. إن توفير الأمان للشبكات المؤسساتية يساعد في صد تلك الهجمات الالكترونية و بالتالي الصمود أمام تلك الهجمات التي تحاول سرقة البيانات ، من المهم جدا للشبكات المؤسساتية الحفاظ على التواصل المستمر بين المستخدمين و الخادمات والشبكات, لقد أصبحت عملية توفير أداء عالي و موثوقية قوية و خدمات متوفرة باستمرار و انتشار واسع عملية كبيرة ومعقدة .

سوف نقترح في هذه الأطروحة البحثية نموذج آمن محسّن للشبكات المؤسساتية و مما لاشك في أن هذا النموذج من النماذج القليلة التي تعمل على صد و منع الهجمات المعقدة و المتمثلة في التهديدات المستمرة و المتقدمة APT. يوفر النموذج المقترح الأمن في طبقات مختلفة من النموذج المرجعي OSI حيث يتم استخدام العديد من الأجهزة والأدوات البرمجية لتحقيق هذا الغرض. النموذج المقترح يعمل على تكامل كل من الأجهزة و الحلول البرمجية في تطبيق النموذج المقترح علما بأن معظم النماذج السابقة تفتقر لهذا التكامل. لقد قمنا في أطروحتنا البحثية بإجراء تقييم الدفاع للنموذج الآمن المقترح حيث أظهرت النتائج على مقدرة النموذج المقترح على كشف ومنع عدد كبير من الهجمات الالكترونية و الرموز الخبيثة وكذلك هجوم الأورورا Aurora attack بطريقة فعالة . كما أظهر تقييم الأداء أن تطبيق النموذج المقترح له آثار قليلة على استخدام عرض النطاق الترددي ، وبالتالي أداء الشبكة.

الكلمات الرئيسية: الشبكات المؤسساتية ونموذج الأمن و SNORT و OSSEC و كشف التسلل و هجمات APT.

# Abstract

Enterprise network (EN) supports thousands of users across different locations, it interconnects many networks that are geographically distributed through vast distance. EN hosts hundreds of servers that provide several services such as web applications, databases, E-mail, and others.

ENs are different from other networks such as LAN, MAN, and WAN, this difference is represented in its size, resource management, and security.

It includes a large number of LAN and WAN networks, it uses different communication protocols to interconnect LANs. EN facilities system and device interoperability, it is tightly controlled to support internal and external enterprise data management. Usually, EN integrates different operating systems such as Windows, Linux, mainframes, smart phones and tablets. Moreover EN integrates a large number of communication protocols and services.

Security threats represent a big problem to enterprise network, they try to damage enterprise confidentiality, integrity, and availability. Advanced Persistent Threat APT are complex attacks that target governments, organizations, companies, and hence ENs.

Security provides protection against attacks, hacking, and data theft, while failover technique provides a high available services of EN. Other techniques such as fault tolerance and load balancing are used to maintain a robust EN. As EN needs to maintain a continuous communication between users, servers, and networks, the task of providing performance, reliability, scalability, redundancy, and security become large and complicated.

In this research thesis, we propose a security-enhanced model of enterprise network (SEEN).SEEN is one of few security model that are proposed for protection against APT attacks. The proposed model provides security at different layers of the OSI reference model. It uses devices and software tools to achieve this purpose. We integrate both hardware and software solutions in the proposed model, most previous proposed security model lack this integration.

In our thesis, we perform a defense evaluation for the proposed security model, the results show that it is able to detect and prevent a large number of attacks and malicious

codes as well as Aurora attack in an effective way. Performance evaluation shows that applying proposed security model has little effects on bandwidth utilization and hence network performance.

**Keywords:** Enterprise network, security model, SNORT, OSSEC, intrusion detection/prevention, APT attacks.

# CHAPTER 1: Introduction

In this chapter, we will introduce enterprise network to discover its components, services, equipments, and requirements. Also we will talk about network security and security model and its importance to enterprise network.

In section 1.1, we will discover the concept of Enterprise Network (EN). Also we will see the components of EN in more detail such as devices, operating systems, network equipments, and others. Service that are provided by EN are described in detail through section 1.1, these services are hosted in different location of EN. In section 1.1, we will define several branches networks of EN as well as users that are participated in EN. Enterprise Network management is describe through section 1.1.

We will introduce importance of network security of EN in section 1.2, improper configuration of security compromise enterprise confidentiality and halt its business. Security threats will be discussed in section 1.2, we will define its generation, types, detection, and prevention. Also we will explain security model and discover its importance, function, and components. Through section 1.2, we will introduce the main components used in implementing security of EN. These components could be hardware equipments and software tools. Transmission security is introduced latter in section 1.2.

In section 1.3, we will present our contribution to develop and implement a security-enhanced model of enterprise network. Finally section 1.4 provides thesis structures of coming chapters.

## 1.1 Enterprise Network

Enterprise Network EN is composed of a distributed infrastructure that connects different users, devices and branches networks. It includes high performance computing servers and massive storage solutions that depend on huge information, efficient infrastructure, and speed network for both local area network and wide area network [1]. Even enterprise network should meet a set of technical goals, it should also meet the business needs [2]of the enterprise. Enterprise network contains hundreds of network

devices such as routers[3]and switches [4], which connect users, devices, and branches networks to EN. It integrates multiple technologies, protocols, software, applications, and vendors, this integration permits for using variety numbers of network devices from different vendors. We can have routers from Cisco while have switches from 3Com, or even a firewall from Juniper. Moreover, users can have different operation systems, they may have Windows OS, Linux OS, and Apple computers.

EN includes data center that hosts different services such as web, E-mail, DNS, FTP, and other services. Some of these services are accessed by public user via Internet, while others are accessed via internal network. It is possible to have services that can be accessed by both public and internal networks. For example, web-based services could be accessed by different users from different networks, they can also access other services like database services. Users from Internet, internal network, and branches networks can access their e-mail and FTP accounts. For security reasons, access to database servers is restricted from internal network, it should not be accessed from public network. EN contains different networks, each network has its function, users, devices, and technology. EN includes Demilitarized Zone (DMZ) network[5], internal network, external network, and branches networks, it may include other special networks such as management and monitoring networks. DMZ is a network that hosts services accessed through public network. Services such as web, FTP, e-mail, and DNS are hosted in DMZ network. DMZ network requires a special care, we should filter traffic that enters and leaves it. The next section provides detail about securing DMZ network. Internal network contains personal computers, printers, laptops, and other related devices, it connects end users to enterprise services. Any user outside EN is considered an external user, there are different types of external users. Partners, customers, and remote users all require access to the EN, they are classified as external users. Some branches networks are connected to EN through WAN services such as VPN [6], Leased Line [7], and Frame Relay [8] while others may be connected using wireless technology such as Wi-Fi, WiMAX, and microwave. It is important to provide a secure connection from branches networks to data center in order to avoid intrusions and attacks. Securing servers of EN is essential, they must be available and secure. Enterprise network has different requirements, it needs availability, scalability, security, and mobility. Users at any time and from anywhere

should be able to connect to services hosted at EN. There are different technology that should be implemented within EN to maintain availability[9]. Unavailability of services harms enterprise reputation, it compromises its business. Fast restore will avoid service unavailability, business cannot tolerate failure, it costs many. Different technology and mechanisms are used to overcome this shortcut, failover technology is such one. It becomes more difficult to maintain availability as more services are distributed in EN. Accelerated growth in EN is critical, EN should be able to connect more branches networks. WAN devices such as routers should be scale enough to connect new branches, we need not to change the whole infrastructure of the EN. Moreover, EN requires a scalable wireless network, so it can connect new wireless sites. Scalability allows expansion without need to change EN infrastructure. Today most users have smart phones like Android, iPhone, these phones require wireless connection. EN should support mobility for wireless devices in order to enable mobile users to access EN service from anywhere and at anytime. There are different wireless technologies that can be used in EN. Wi-Fi [10] is a wireless technology that intents to connect user inside EN, they usually used for indoor connection. It may be possible to use Wi-Fi to connect branches networks but it still limited in distance that it covers. On the other hand, WiMAX[10] is used to connected branches networks of large distance, it needs more equipments and devices than Wi-Fi. WiMAX connectsboth sites and remote users to EN. Providing secure EN is not easy job, it needs more efforts, money, and devices. We cannot imagine EN without security, it will be a big problem. Network security and security models will be discussed in the following section.

Enterprise network management is an important task that administrators should care about it. Analysis and collecting information from different networking devices and users are necessary for monitoring and controlling EN. Most monitoring devices use SNMP[12] protocol to collect information about network devices, they may also need to enable syslog service as well. Authors in [11]proposed an Enhancing Enterprise Network Management using SMART, they try to make management of heterogeneous devices flexible and reliable. The paper used mobile agent technology for enterprise network in order to design a hierarchical network management framework. It aims to manage

dynamic evolving network components using distributed network management, flexible coordination and runtime topology discovery.

## 1.2 Network Security and Security Model

Securing network services and devices is the most important task of enterprise network., all data traffic is passed through network devices [13][14]. We need to secure routers, switches, personal computers, servers, operating systems, and any components in the EN. Without adequate protection many individuals, businesses, and governments are at risk of losing their asset[15], network security will protect confidentiality, maintain integrity, and assure availability for EN. EN should deploy network security to provide integrity for information data, they must be correct and protected against corruption and unauthorized change. Encryption provides confidentiality, authenticated users can only access and view information data. EN includes huge information that stores massive amount of sensitive data. Theft of these data exposes EN to compromise and even to damage business. EN should be protected from intrusions and attacks which are originated from internal and external network. Compromising enterprise network would be costly, it will halt enterprise reputation which will affect on business. EN security devices should have the latest updated signatures, they should fix vulnerability of the systems, monitor traffic, log network traffic activity. We need an updated security model that reflects changes in technology and services, we have to build and maintain a robust network security for end users and servers. As EN expands to include new technology, services, and systems, the likelihood of emerging new vulnerability with different degree of weakness increases. In general, security threats are arisen due to vulnerabilities, which represent the degree of weakness in software and hardware. Vulnerabilities are appeared due to different reasons, mis-configuration of hardware or software is a common one. Administrators should avoid default configurations, they should spend more time to secure configuration. Well network design will avoid potential vulnerabilities, proper placement of network security devices is essential through design. As new attacks are arisen, the challenge become bigger. EN should has an effective detection and prevention system against zero-day attacks. Intrusions try to steal data of EN, they intend to compromise EN. Today attack become complicated, they depend on attacker with high

skills. APT-based attacks [16] become a serious attack against EN, they are funded by governments and organizations. They represent cyber attack that requires special awareness and early alerts. There are different types of APT-based attacks, Aurora operation and RSA attack are common examples. Security threats are generated from different sources, Internet is the most common one. Attacks use malicious code to compromise victim host and hence distributed across EN to compromise the whole EN.

Implementing defense in depth is essential for EN, it provides security at many layer. Firewall and NIPS/NIDs are used to provide security for network devices, while HIPS are used to provide security for hosts and servers. Antivirus application is used at end user level, it must be updated daily. Having all security services in one device represents a single point of failure while distributed security system provides alternative efficient solution. Providing security at more than one level/layer will minimizing the likelihood of leaving breach undetected.

Security model determines which application/protocol should enter and leave EN. It secures DMZ and Internal networks from potential attacks, different hardware and software solutions can be used to achieve security task. Monitoring security is essential , it guarantees the continuity of having an updated security model. Securing DMZ network requires effective access control lists that filter inbound/outbound traffic. Users from public network such as Internet should access web server, e-mail server, and other services in a secure way, these servers should be under monitor to prevent potential intrusion. Internal network should be secured from both external and internal attacks. Public users should not access internal devices directly, they should be authenticated by intermediate security devices such as authentication servers. They should have least privilege permission that help them accomplishing their tasks. Moreover, security model determines how to access data , by whom, and its transmutation way. Monitoring and logging are the most important role of security model , without monitoring we cannot track attackers. There are many ways to protect EN services from intrusions, most of these ways depend on firewall and NIPS systems. Security model applies a real-time traffic monitoring and analysis, many tools and devices could be used to achieve this purpose. Many vendors like Cisco, Juniper, and Fortigate offer hardware solution for monitoring real time traffic. In the same time, there are open source tools such as SNORT

[17] that acts as NIDS and NIPS to monitor and prevent intrusions and attacks against network devices like routers and switches. HIPSs are used to protect individual host such as web server, e-mail server, and database server, they monitor resources, registry, and OS activity for each host with HIPS installed. OSSEC[18] is an open source tool that is used as HIPS Log files store security events that require deep analysis to detect malicious activity. Syslog is a UNIX program that should be enabled on network device in order to examine logs for monitoring and logging purpose. Intrusion Prevention Sensors (IPS) are used in EN as inline which enable them to monitor and analysis network traffic as it occurs. NIPS compares each packet that passed through it with pre-defined signatures. NIPS can take many action when it detect a malicious activity, it sends alerts to network administration and may drop the connection. On the other hand, NIDS will send an alarm when detecting an intrusion, it can also block malicious activity if it were configured as active response. Routers can be configure as NIPS if their IOS support.

Perimeter security is used to filter traffic that passed from and to EN depending on many factors such as user, IP address, protocol, application, time of day, etc. Usually, firewall is used to provide perimeter security, it filters each packet entering and leaving it. According to a predefined rule, firewall can deny or permit the coming packet. Administrators maintain these rule according to the need of EN.

Firewall[19] can act as NIPS if it has a IPS module inside it. It can be use to protect internal and DMZ networks, it has a specific port for each one. It can be used to provide other functions besides filtering inbound/outbound traffic. Content/URL filtering, virus scanning and SPAM filtering are additional functions that firewall provides. firewall is a central security device in EN, it should eliminate potential intrusion from affecting internal and DMZ networks. Multiple vendors provide integrated security devices that integrates IDS/IPS inside the firewall.

Transmission security on the other hand ensures data integrity and securing transmitting data. Virtual Private Networks (VPNs) are used to secure connection between two remote sites. They use encryption and authentication to secure connection, VPN creates tunnel through public network such as Internet to transmitted data. There are many VPN

protocols that are used for VPN connection. Point two Point tunneling protocol PPTP is one of the oldest VPN protocol, it is the least secure protocol. Layer 2 Tunneling Protocol with IPSec provides better security, it support encryption of header and payload. L22TP/IPSec is secure than PPTP. Open VPN is another VPN protocol, it is the most used protocol today. In our research thesis, we propose a security-enhanced model of enterprise network that treats network security integrally.

## 1.3 Our Contribution

The contribution of our research thesis is to propose a security-enhanced model for enterprise network. In our contribution, we recognize enterprise network as a special case. It is a real network that is in use until developing the proposed security-enhanced model. We use both hardware devices and open source tools to implement our proposed security model. Performing deep inspection of traffic that passes through EN represents an important step. We need to provide secure connection between branches networks and EN services, only authenticated users are allowed to access EN critical data. The proposed security model takes into account the defense in depth strategy, we implement security at more than one level. We do implementation to our proposed model using open source tool such as SNORT, OSSEC, and Splunk. We use SNORT as network intrusion detection system, while OSSEC as host intrusion prevention system. Also we use Splunk as monitoring and analysis server that reads logs from both SNORT and OSSEC. The proposed model provides a defense system against different attacks and intrusions, it detects and prevents Aurora attack. To evaluate our proposed model, we use two different evaluation which are defense and performance evaluations. We use Metasploit which is a free, open source penetration testing solution for defense evaluation, while FreeMeter for performance evaluation.

## 1.4 Thesis Structure

The rest of the research thesis is organized as the following: chapter 2 talks about related work, it discuses some related security models. Chapter 3 explains our Enterprise

Network Model (ENM) in more detail. It discuss the services provided by EN, and its requirements. We also talk about difficulties that faces applying these requirements, potential threats against EN are also described in chapter 3. It introduces the basic concepts related to the enterprise network as well as the EN topology.

In chapter 4, We do traffic analysis of enterprise network model, also we browse the most common traffic analysis tools. We discuss the results of traffic analysis to discover the nature of EN traffic. Chapter 4 explains Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), we explain both SNORT as open source NIDS/NIPS and OSSEC as HIPS. Latter in chapter 4, we describe our proposed security-enhanced model of EN.

In chapter 5, we do implementation of our proposed security-enhanced model, we use Metasploit tool to evaluate defense of our proposed model, while we use FreeMeter to evaluate network performance. Results are discussed latter in chapter 5. Finally, in chapter 6 we present conclusion and future works.

# CHAPTER 2: Related Work

In this section, we will review previous related security models, we will discuss each of them to see its advantage and disadvantage. There are number of security models that are designed for enterprise network. Some of them depend on firewall and routers in their design while others depend on intrusion detection/prevention system. There are different factors that affected on security model design such as number of users, supported services, and others.

In [22], author improved a new more initiative distributed network of safety warning model P2DWR2, the proposed model depends on the P2DR model. P2DR model is dynamic self-adaptive network security model, it uses dynamic detection to determine the status of network security. P2DR model suffers from different limitations, it does not support active early warning. It needs an interaction from human to provide a dynamic security model, there is no active cooperation between security components. It supports small-scale distributed network rather than large-scale distrusted network.

The proposed model P2DWR2 enhances and improves the P2DR model, it provides an active early warning model. Security policy is considered as the core of P2DWR2 model. Having an active cooperation between security components, P2DWR2 supports large-scale distributed network. Proposed model provides an automate response to security incident, while reduces human interaction. P2DWR2 supports automatic distribution, it enables self-adaptive management functions. It is composed of five components as shown in figure 2.1, the components are protection, detection, early warning, response, and recovery. It uses encryption, firewall, intrusion prevention system to protect the distributed network. Intrusion detection systems, vulnerability assessment, and other systems are used to detect potential attacks, it sends information about detected attack to defense system for early warning. Once it detects an attack, it response in a timely manner according to predefined security policy. Damaged information are restored by upgrading components of distributed network such as systems, software, security components, and other components.

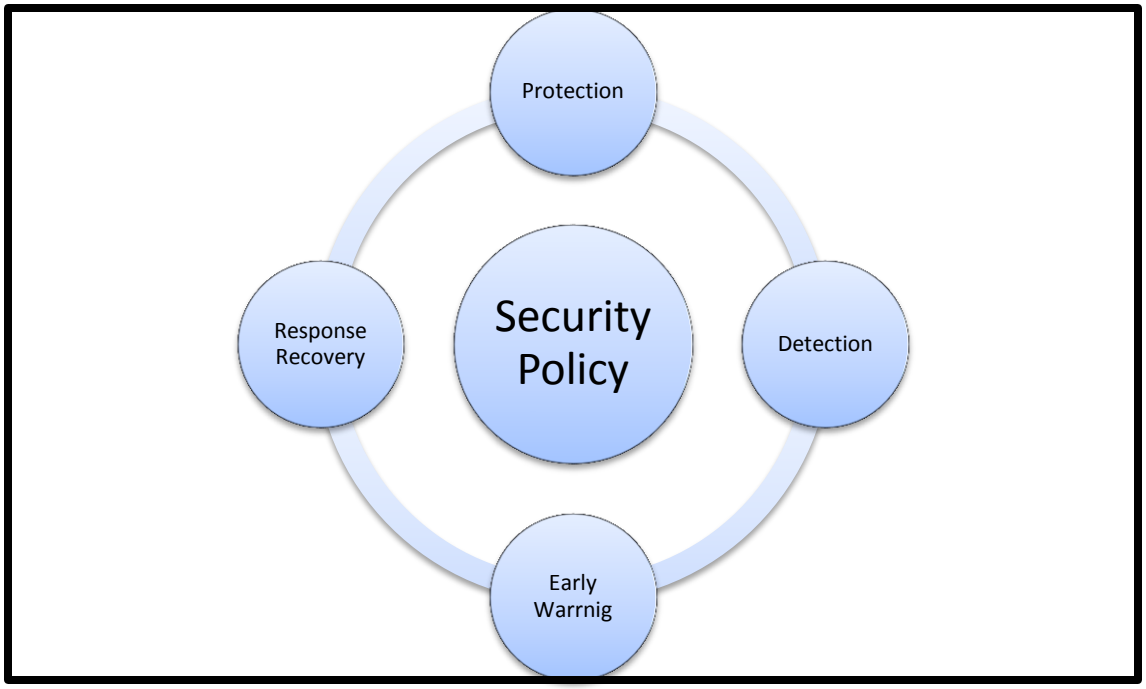



Figure 2.1: Components of P2DWR2 model.

ZhaoyangQu and Jia Yan proposed a design of network security model of active defense [24]. The new design proposed a new dynamic model WP2DR2C that overcomes the limitation of self-adopting network security model P2DR. Authors provided a dynamic response against attacks. The proposed paper designed network intrusion prevention system NIPS gateway using both intrusion detection system and traffic traction. Authors proposed dynamic diffluence algorithm that depends on the feature of NIPS gateway system. Traffic traction is virtually an equipment of diffluence that diffluence traffic based on certain strategy. The model uses strategies of diffluence to determine if the traffic is normal or abnormal. Normal traffic will be redirect to Intranet while abnormal will be send to other subsystems. Subsystems are determined according to attacked degree, for example it will send abnormal traffic to honeynet when it matches predefine rules of NIPS gateway. The model aims to find new vulnerabilities and bugs of Internet servers and equipments as quickly as possible. Figure 2.2 shows the proposed model, it is consisted of seven components which are warning, policy, protection, detection, response, recovery and counterattack.

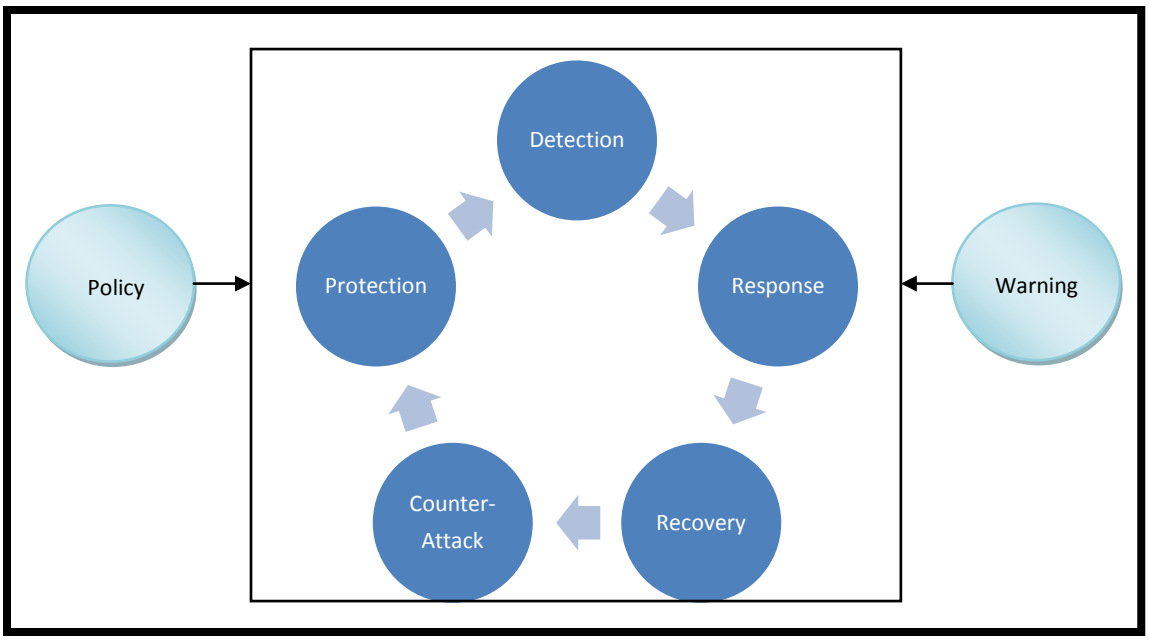



Figure 2.2: The proposed model WP2DR2C.

To provide protection, different components such as intrusion prevention system, security strategy, and encryption technology are used in cooperation with IPS. Security holes are discovered using intrusion detection, intrusion deception, hole-scanning. The system model will responds quickly when intrusion is detected. NIPS gateway is the core of the whole defending, NIPS gateway connects five different subsystem as shown in figure 2.3. The subsystems are Internet, Intranet, Honeynet, warning system, and counterattacking system.

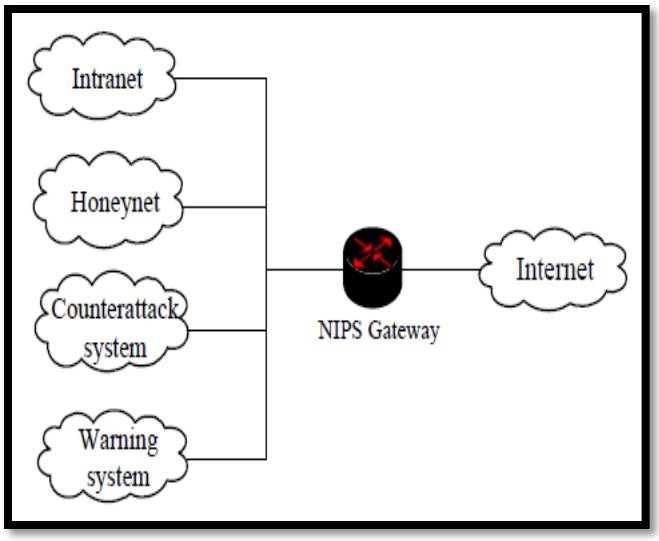



Figure 2.3: NIPS gateway of proposed model WP2DR2C.

Traffic that comes from Internet will be checked before getting to Intranet network. Once the proposed model detects an attack, it will send a warning. The response depends on the security strategy. Experimental results showed that the proposed model provided an effective defense system.

In [25], the paper proposed a new security model that is implemented with connectivity fault management (CFM). CFM is IEEE 802.1ag, it provides an end-to-end traffic carrier in the metro Ethernet domain. CFM defines protocols and practices of Operations, Administration, and Maintenance OAM for paths through 802.1 bridges and LANs. The proposed model provides an effective and reliable isolation of individual traffic flows and the associated LANs using CFM. OAM is consider to be as a policy and regulation agent in the Metro Ethernet service model. Even CFM is an effective fault manager, isolator, and indicator, the proposed model intends to use CFM as a tool for packet security. The proposed model is designed to eliminate and prevent attacks in Metro Ethernet.

Paper in [26] proposed a design for an enterprise network information detection system using embed processor. The proposed system can get detailed log messages of enterprise network at anytime, it is used as an node of great network. Figure 2.4 shows the hardware structure of the proposed system, it is connected to firewall devices directly.

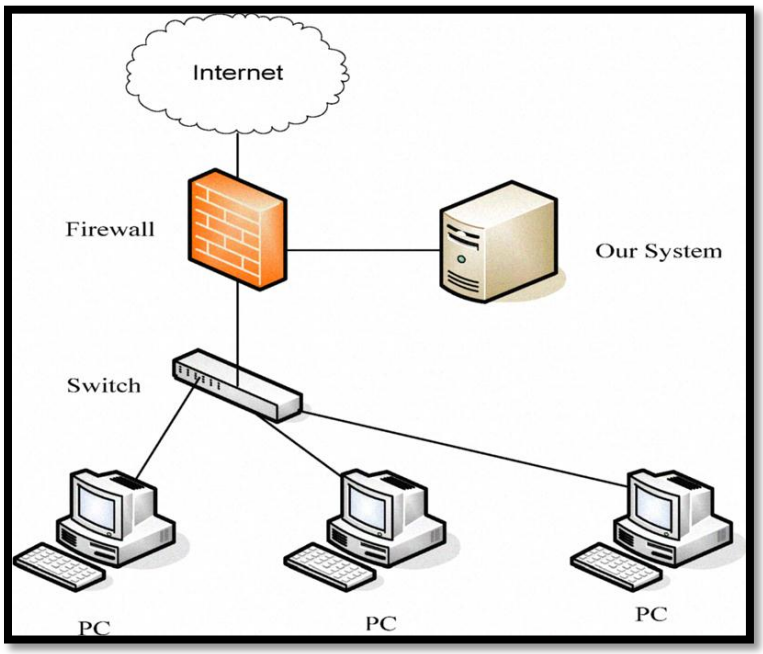



Figure 2.4: The hardware structure of proposed detection system using embed processor.

Figure2.5 shows the system software structure. The proposed system uses policy to determine which traffic to monitor. It can monitor HTTP, SMTP, FTP, URL blacklist, and others. Each packet is analyzed to extract each field of the packet header, content recovery module takes the extracted file as input. It can recover network data according to configuration file. The proposed system audits the network traffic by policy to check if it is normal, it checks the visiting URL against blacklist. It also do a content auditing for the captured data, it checks whether there is confidential or unauthorized information.

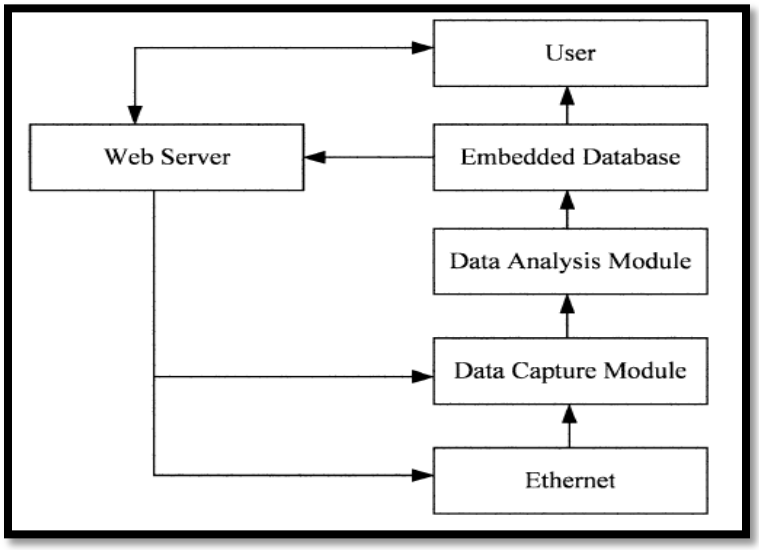



Figure 2.5: Software structure of proposed detection system using embed processor.

Paper in [23] proposed a new network security model using static VLAN and TACACS+ AAA server. The model aims to protect layer 2 of the OSI reference model from threats and attacks. Routers and AAA server are used in the proposed security model as shown in figure 2.6. TACACS+ is used as AAA server that encrypts the entire TACACS+ packet. AAA server is used to authenticate user before getting access to network, each user has specific access to network according to predefine policy. AAA is used to provide an extra level of protection, it uses policy to control user access. AAA server provides secure access to network and remote management of network devices.

Remote access to network device such as routers and switches is encrypted, the proposed model suggested to use SSH protocol, or IPSec encryption. In order to reduce attacks, the proposed model disables any unused protocols. Access Control Lists (ACL) are used to filter traffic that entering and leaving the network, traffic between VLANs is also filtered

using ACL. Securing VLANs requires changing the default VLAN, native VLAN, and management VLAN. It shutdown all unused switches interfaces.

The model suggested to enable port security configuration for all switches interfaces, it will restrict users who can connect to LAN networks. Other related configuration such as DHCP snooping are used to protect network from DHCP starvation and DHCP spoofing.

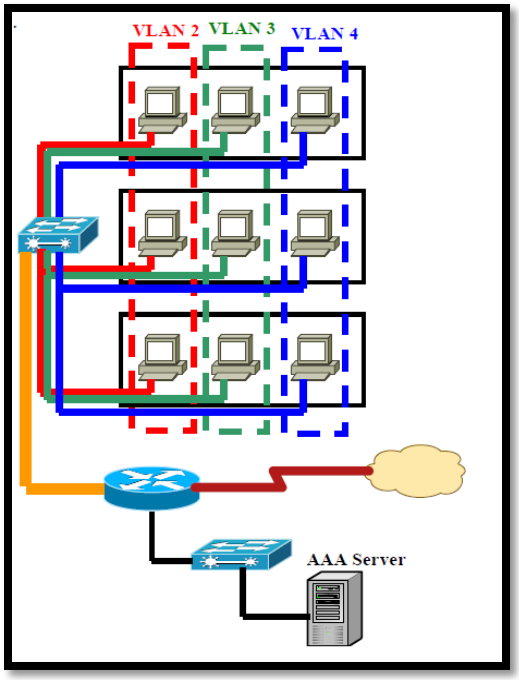



Figure 2.6: The proposed network security model using VLAN and TACACS+ AAA server.

Authors in [27] proposed a network security model that is supported by different network devices. Authors build their proposed model depending on analyzing security characteristics for physical layer, network layer, system layer, application layer, and management layer of the network. Different network devices support the model, routers are used at network layer, while switches are used at data link layer of the OSI reference model. Firewall, network management, and operational platform all support the proposed model. Experimental results show that security model provides perfect defense, it merges many different security aspects to provide effective security. It uses access control list to filter traffic entering and leaving the network, authentication is used to provide access for legal users. The model provides attack detection function, it scans the network for vulnerability and security holes. Physical layer security includes securing data center room, network devices, and other related equipments. Threats such as fire, earthquake, flood represent environmental threat, while mis-configuration and attacks represent

human threats. Securing network layer requires intrusion detection system, antivirus software, and access control lists. System layer security includes securing operating systems and software using updates and hot fixes. Securing web services and mail services is essential to application layer security, on the other hand management layer security ensures that management of network devices is done through secure connection. The model uses VPN networks to provide secure connection through encryption, it also provides different policies to determine the access permissions of resources in the network. Figure 2.7 shows the proposed network security defense model.

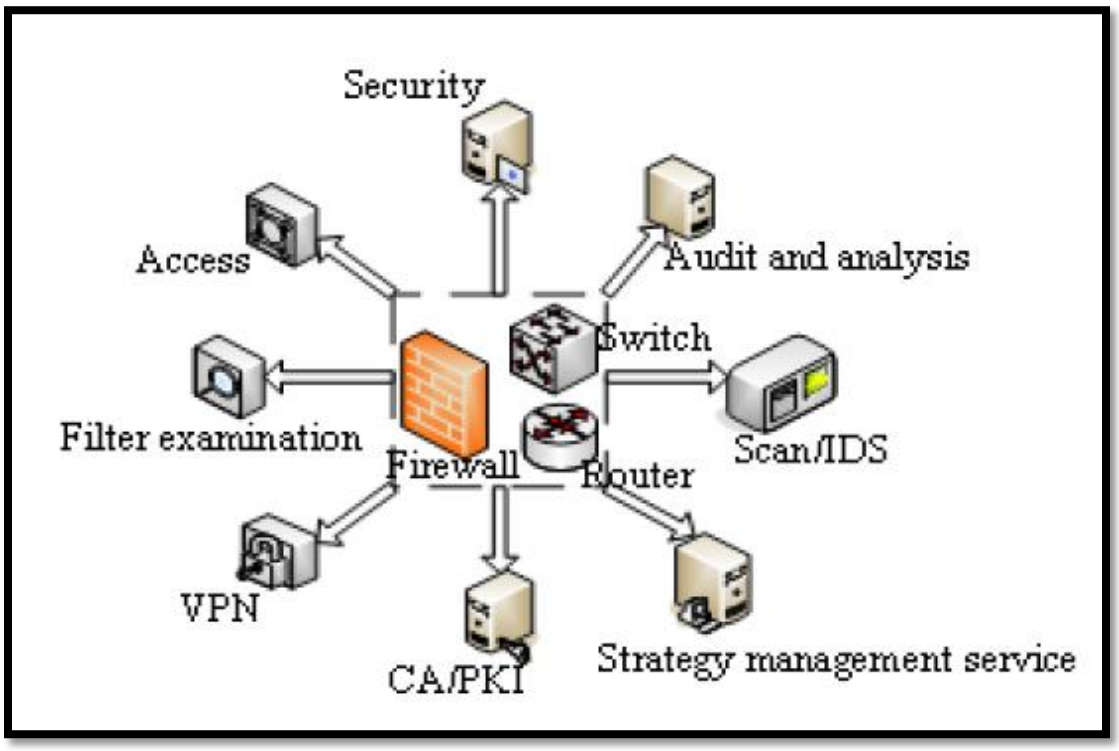



Figure 2.7: The proposed network security defense model.

Paper in [28] introduced a new concept which is network business security. Using the proposed concept, the paper defines the object of information security in three parts which are data security, network system security, and network business security.

The concept of network business security provides theoretical basis for security defense of enterprise automatic production system and enterprise management information system. One important element of the proposed concept is the confidentiality and integrity constraints between network businesses of different security levels. According to paper, enterprise network information system is a platform for enterprise production

automation system and enterprise management system that are working together. Security of network business provides confidentiality, integrity, continuity and real-time of network business. The paper provides a formal description of network business and network business security model. Authors suggested that network business is composed of the network process sets, data sets and process operation sequence sets. Hence, network business security is represented by both network process sets and data sets. Network processes runs and writes operation on data sets.

Authors in [29] proposed a network security model for the campus network. Campus network is a special network, it is a type of enterprise network. Internet access exposes Campus network to attacks and intrusions. It becomes so important to provide a secure campus network that has ability to defense against intrusions and attacks.

The defense model proposed in [29] is composed of five components which are security management, protection, detection, response, and security services. Security management is responsible about monitoring network, dealing with security incidents, auditing, and analyzing security logs. Protection can be done by using host intrusion prevention system and network intrusion prevention system, while detection is done using intrusion detection system at the borders to provide real time detection. IDS and IPS are work together to prevent attacks, it provide real time protection. Security policy determines the response that will be applied after detection intrusion. The proposed model includes six modules, each of them provides a specific function. The modules are data collection module, firewall module, intrusion detection module, intrusion prevention module, analysis module integration and management control module. Figure 2.8 shows the modules of the proposed security model.

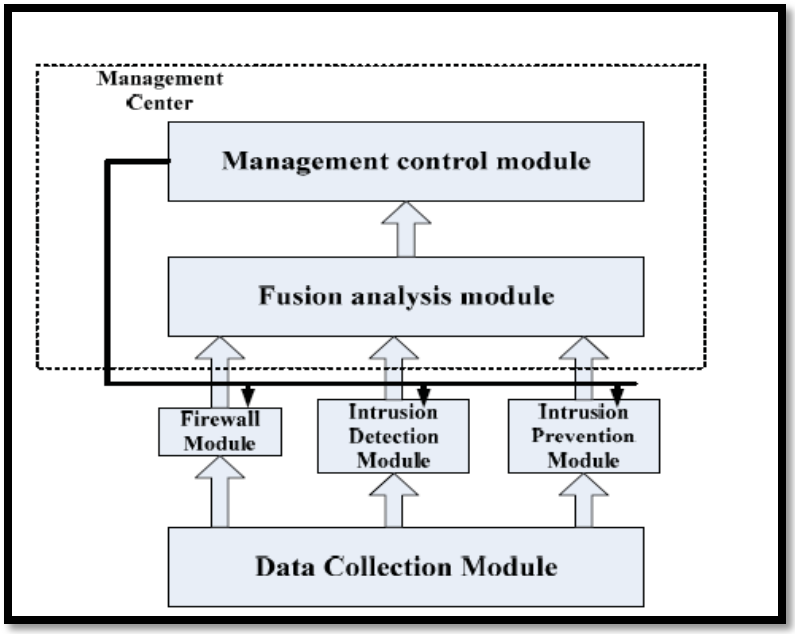



Figure 2.8: Modules of campus network security model.

Data collection module is the basis of the proposed model, it is located in the firewall, IDS and IPS detection. Firewall module is used to filter traffic between internal and external networks, it authenticates users to get access of network resources. Intrusion detection module provides real time monitoring for traffic passing through internal and external networks, while intrusion prevention module stops malicious activity and attacks. Management center includes tow module, it integrates analysis and management control module.

Salah Alabady in [15] used routers and firewalls to design and implement a network security model for cooperative networks. Author listed the network security vulnerabilities in routers and firewalls, he discussed prevention mechanism against different types of threats and attacks. The model used Packet Shaper which is a traffic management appliance in order to monitor and control network traffic passing over wide-area networks. Figure 2.9 shows the structure of the proposed network security model.

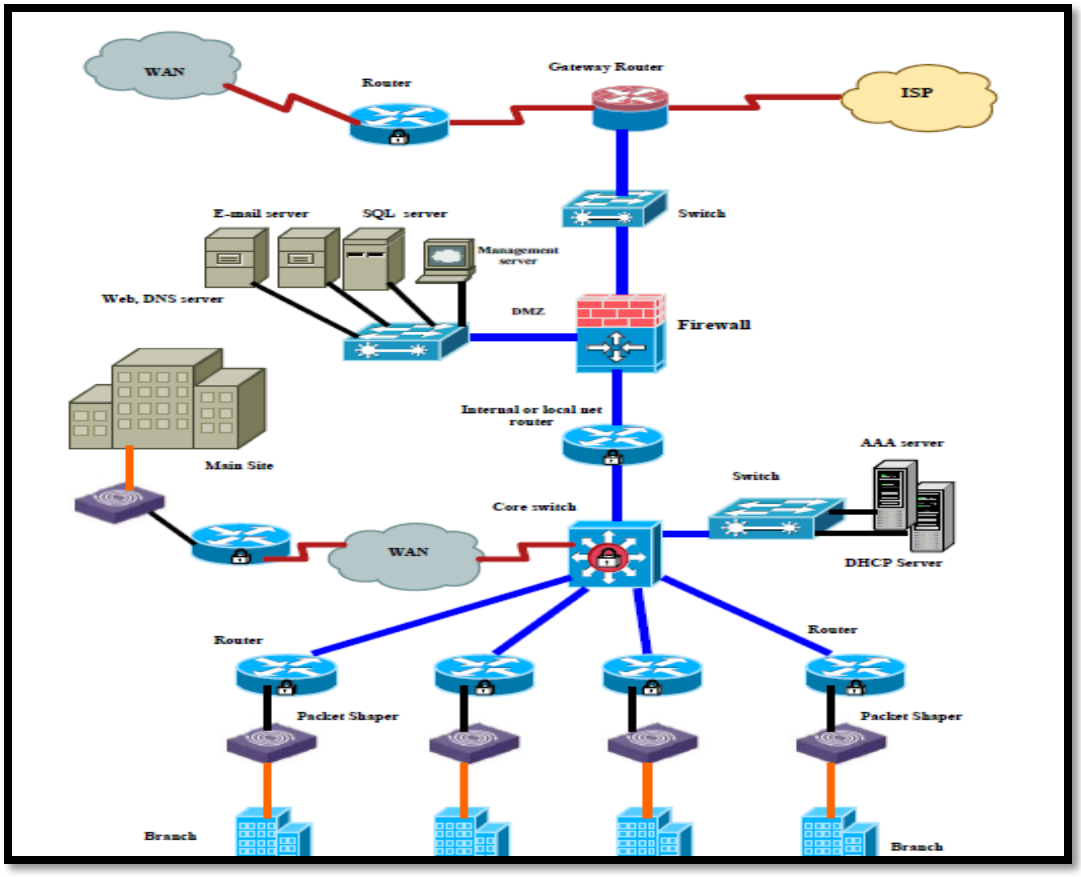



Figure 2.9 :Structure of the proposed cooperative network security model.

Author used security policy as evaluation way to check whether network devices implement the recommend configuration or not. The paper provided the recommended configuration for network devices to prevent potential attacks, threads, and hackers. It is important to follow these recommend configurations for routers and firewall, poor configurations expose network to attacks and hackers. The paper conducted that vulnerabilities are due to technology weaknesses , configuration weaknesses, and Security policy weaknesses. TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses are examples of technology weaknesses, while unsecured user accounts, simple password, mis-configuration are sample examples of configuration weaknesses. Security policy weaknesses includes absent of disaster recovery plan, lack of continuity and written security policy. Attackers use different tools to get illegal access to internal network. They use password sniffers to hack users password, also they use IP snooping and e-mail phishing to steal sensitive information in cooperative network. There are different threats against cooperative network such as

unauthorized access, session hijacking, rerouting, masquerading, denial of service (DoS), eavesdropping, and information theft. The proposed model suggested to disable services that are rare in use such as Cisco Discovery Protocol (CDP), Finger server, HTTP server, Bootp server, IP source routing, proxy ARP, IP directed broadcast, and SNMP Service. The proposed security model defined a security policy with different rules that should be adhered to provide the best practice network security. Security policy suggested to use SSH protocol for router management as well as to disable unused services and protocols. Author proposed a test bed to test security of the proposed model, Figure 2.10 shows this test bed. The test bed includes two Cisco router 2811 acts as internal and gateway routers. Cisco firewall (PIX) 516E is used between internal and external network, while Cisco switches 2960 connect LAN users to cooperative network. Test bed uses AAA server with TACACS+ protocol for authentication, and better auditing. The model used two workstations to simulate real attacks, they installed Ethereal program to simulate real reconnaissance network attacks. Other programs such as Super Scanner program and Dsniff programs are used to simulate a real access attacks to discover open ports and active IPs on the target network.

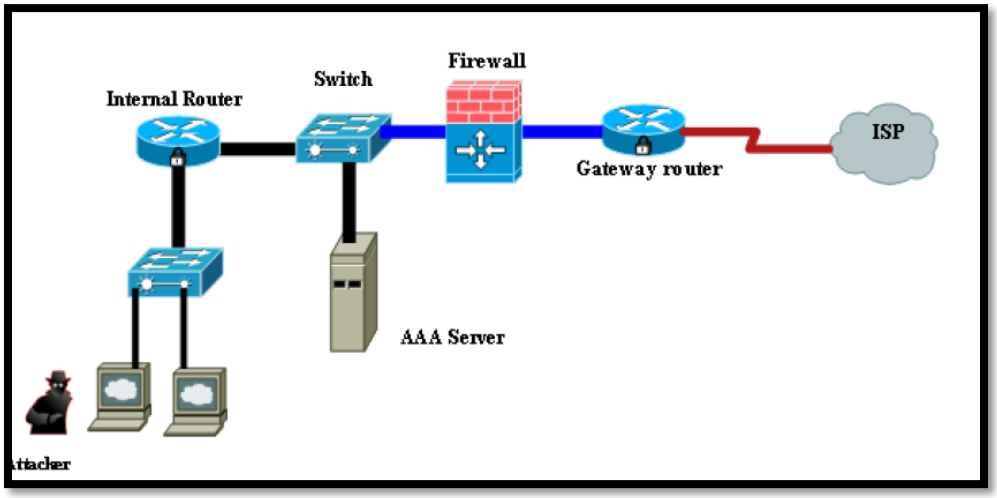



Figure 2.10 :The proposed test bed of proposed cooperative network security model.

Jack TIMOFTE in [30] proposed an intrusion detection system using open source tools, he used three open source IDS tools which are SNORT, OSSEC and Prelude. OSSEC is used as host intrusion prevention system, it is an open source tool. OSSEC provide real time monitoring for individual host such as server, it can monitor operating system registry. OSSEC can detect and prevent malicious activity once it detected. Prelude is a

framework that allow other application to send their reports to a centralized system. Prelude system is composed of more than components which are the Prelude library , Prelude manager, Prelude-LML, PreludeDB library and Prewikka. Events that received by one or a set of prelude managers are read by sensors. Sensors are created by the Prelude library. The Prelude Manager collects and normalizes information from distributed sensors, they use database to store collected information. Syslog messages for malicious activity are received by the Prelude LML, it monitors log files. The Prelude LML is considered as a signature-based log analyzer. Prewikka is a console that provides contextual filtering, aggregation, etc. Snort provides an open source intrusion detection and prevention system that used to prevent intrusions and attacks.

Paper in [31] proposed a new network intrusion detection system using Snort and NTOP. Experimental results shows that the proposed system can detect intrusions and attacks in efficient way. Figure 2.11 shows the structure of the proposed system.

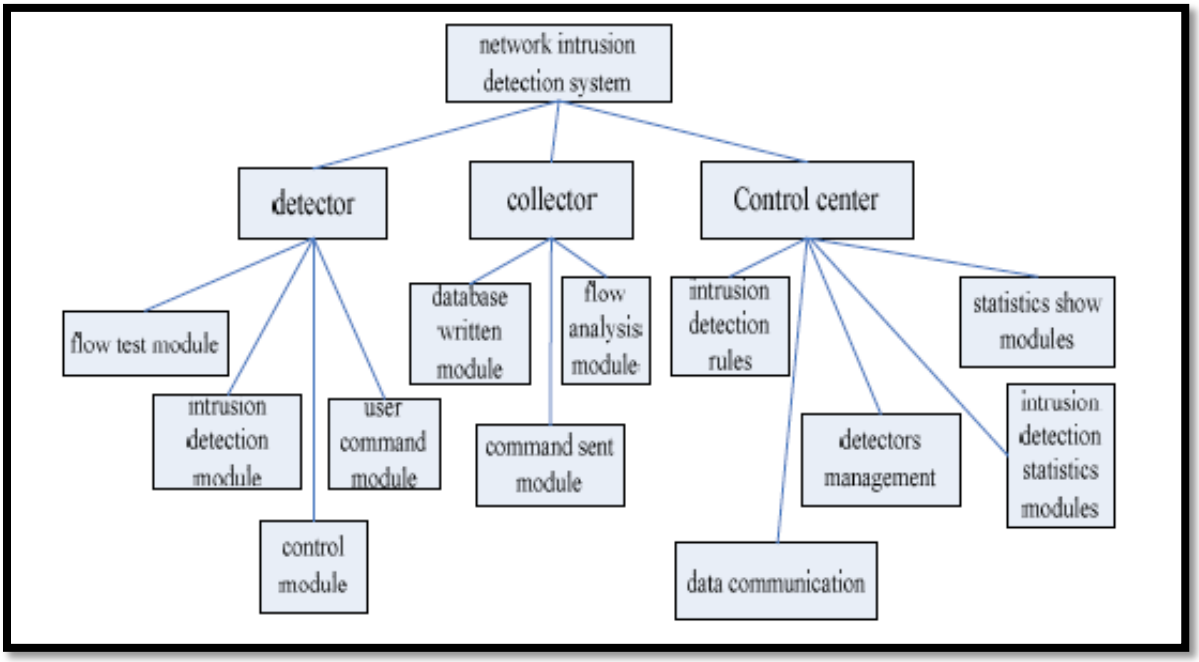



Figure 2.11 :The proposed network intrusion detection system using SNORT and NTOP.

SNORT is an open source intrusion prevent and detection system, it includes four components which are packet sniffer, pre-processor, detection engine, and warning and logs. On the other hand, NTOP is a tool of monitoring network, it can determine the existing problems of network. NTOPS has the ability to solve the problem of local

network by monitoring. NTOPS convert intercepted packets into the format for easy identification, it analyzes communication failure in the network, and record the network communication time and process.

The proposed system is composed of three components which are detectors, collector, and control center. By referring to Figure 2.11, the detector is composed of the flow test module, intrusion detection module, control module and user command module, detector gets data information of proposed system. Collector is composed of three modules which are database written module, command sent module and flow analysis module. Analyzing data processing is done by Collector. The control center is composed of data communication, intrusion detection rules, detectors management, statistics show modules, and intrusion detection statistics modules. Control center is used to send and receive command as well as to display data. it is GUI interface between network administrator and software. The proposed system used SNORT to implement intrusion detection module, while used NTOP to implement flow test module. Experimental results showed that high network flow leads to increase lost package rate. Packet loss rate was at about 5% when flow is 60 M.

The previous research papers have some drawbacks, we intent to overcome them in our research thesis. Papers in [22][24][29] did not provide a security solution for branches networks, the proposed models did not have a clear implementation of intrusion detection/prevention systems. They do not provide either defense evaluation or performance evaluation. Paper in [23] provides security only for layer2 of the OSI reference model, it does not care about other layers such as layer 3, layer 4, and layer 7. Even some proposed models [22][30] provide intrusion detection and prevention mechanism, they still lack management center to collect and analysis logs from network devices. It will be difficult to monitor enterprise network without management center. Proposed security model in [25] did not provide real implementation of network security concepts, it was just a group of deductions. On the other hand, paper in [28] provides formal description of network business security model, there is no practical implementation using either hardware or software. It is not sufficient to use only routers and firewall to provide network security [15], we need more devices and tool to provide better security model. Although security model in[31] provides intrusion detection

system for network devices, it fail to provide intrusion detection system for individual host such as servers. Unfortunately, all previous researches do not provide a security solution against Advanced Persistent Threat APT-based attacks such as Aurora attack.

# CHAPTER 3: Enterprise Network Model ENM

In this chapter, we will discuss our Enterprise Network Model (ENM) in order to discover its services, requirements, related difficulties, potential threats, and components. In section 3.1, we will introduce some basic concepts related to the enterprise network mode such as layer 2 switches, routers, firewall, and others. Section 3.2will describe the services provide by our ENM, requirements of the ENM will be discussed in section 3.3. It may be important to answer the question about difficulties to apply these requirements to ENM, answer will be found in sub-section 3.3.2.Threats on the ENM will be discussed in section 3.4, also we will see how to eliminate these threats as possible as we can. We will investigate the topology of our ENM in section 3.5, we will list the main components of the ENM as well as discuss topology of the ENM. Along the section, we will discover the function of each component in the ENM, and its effects on the ENM.

## 3.1 Basic Concepts Related To Enterprise Network Model:

In this section, we will define some basic concepts that are related to our ENM. It may be good to have a look on LAN devices such as layer 2 switches and layer 3 switches. Also we will see WAN devices such as routers and firewall, WAN services such as Leased Line, Frame Really, and VPN will be introduced through this section. Section 3.3 will discuss functions of some security devices such as firewall and intrusion detection system as well as zones types used in firewall device. SNMP protocol will be explained latter in this section to investigate its function in ENM.

**Layer 2 switch**: is a traditional switch which is a multiport bridge [33]. Switching and filtering are based on the Layer 2 MAC addresses. Unmanaged layer 2 switches did not need additional configuration, user can simply plug his/her network cable into layer 2 switch to get LAN connection. Due to its simplicity, layer 2 switch is considered the best choice. Layer 2 switches are used to interconnect PCs, printers, workstations of the same LAN, so it is usually used in local area network.

**Layer 3 switch**: is a network device that operates on both physical and network layer of OSI model. Unlike layer 2 switch, layer 3 switch can make both switching and filtering decision based on IP and MAC address. It uses both IP and MAC address to decide

whether to switch or route the incoming packets. Due to its high switching process, layer 3 switching is the favorite for highly scalable, resilient networking. Even layer 3 switch has faster switching than traditional router; traditional router still has a distinct feature in WAN service. Traditional routers support WAN services such as leased line, VPN, Frame Relay, and others, while layer 3 switches do not.

**Router**: is a network device used to interconnect distinguishing networks, and it is usually used in WAN networks[3]. Router has the tasks of best path selection, pack forwarding, and optionally packet filtering. The software architecture of a router is composed of three interdependent functional blocks connected by interfaces [34] which are data plane (forwarding plane), control pane (routing protocols), and management plane. There are many vendor of routers such as Cisco, 3come, HP, and others, but the most famous one is Cisco company.

**Firewall**: is placed at the point of entry between inside network and the outside Internet such that all incoming and outgoing packets have to pass through it. Firewall [19] will inspect each packet in both directions inbound and outbound in order to take a decision of dropping or allowing it. This decision depends on predefined rules; rules will determine the policy of enterprise network. Packets inspection related to source IP, destination IP, source port, destination port, protocol type, and other criteria. Firewall is a critical component in enterprise network; it is the first defense device in EN to protect against attacks. Firewall can be implemented as hardware appliance or a software application. Also firewall can be configured to protect both the whole enterprise network and a single personal computer. Firewall is offered by several vendors such as Cisco ASA, Juniper firewall, Fortinet, and others.

**Intrusion Detection System (IDS)**: The main function of IDS is to discover threats and detect attacks in enterprise network [12], attacks detection depends on predefined signatures. Once an IDS detects an attack, it will sent an alert to network administrator and block connection. When IDS works in promiscuous mode it does not take action by itself , but it notifies other blocking devices to take action such as firewall or router. IDS can be implemented using software such as SNORT (open source IDS/IPS) which is

installed and configured over a Linux distribution. IDS can be also a hardware appliance such Cisco IDS, Juniper IDS, and others.

**VPN**: Virtual Private Network is a computer network in which data traffic between nodes is carried by open connections or virtual circuits in public networks, such as Internet [6].

VPN is used to provide secure connections between enterprise branches via low-cost lines using Internet. VPN creates a tunnel between the sender and receiver, where data pass through this tunnel is encrypted. There are many protocols used in VPN such as PPTP, L2TP, Open VPN, and SSTP.

**Leased Line**[7]: is a WAN service provided by ISP. It is used to interconnect branches sites to the main data center through ISP network. Because Leased Line provides a dictated bandwidth one to one, it is usually expensive. Leased lines enable transmission of data at medium and high speeds (64 Kbps to 140 Mbps) by point to point or multipoint connection.

**Frame Relay**[8]: is WAN service provided by ISP. It is used to interconnect branches sites to the main data center through ISP network. Frame Relay is considered a packet switching methodology, which provides shared bandwidth. it is less expensive than Leased Line due to shared bandwidth.

**SNMP**: is a Simple Network Management Protocol (SNMP) used for managing devices in IP networks. Devices such as routers, switches, wireless access points and PCs all act as SNMP client that contact with the SNMP server. SNMP uses a fetch and store model in which each server maintains a variable that include statistics such as count of packet received [35]. SNMP helps us to detect which network devices are up and which are down. Moreover, we can detect the status of each network devices using SNMP.

**HTTP/HTTPS protocols:** is Hypertext Transfer Protocol (HTTP), it operates on application layer of OSI model. The default port of HTTP is 80, HTTP protocol is used to send and receive information across Internet. All web browsers application such as Internet Explorer, Mozilla Firefox, and Google Chrome use HTTP protocol. HTTP protocol is not a secure protocol, it does not provide either encryption or authentication via digital certificates. On the other hand, HTTPS is Hypertext Transfer Protocol over

Secure Socket Layer, or HTTP over SSL. HTTPS protocol is simply a secure HTTP, it operates at transport layer of OSI model. The default port of HTTPS is 443, it provides encryption and authentication through digital certificate. HTTPS protocol is used for securing websites such as banks website, payment websites, it encrypts transmitted data between web server and client web browser.

**Internal Zone**: It is also known as trust network or inside network. It contains local traffic that generates from the trust users or/and applications within internal network. It is usually connect to firewall for protection purpose against external attacks. Internal zone consists of different LANs and branches.

**External zone**: It is also known as Untrust network or outside network. This network contains local traffic that generates from the Untrust users or/and applications. Internet is the main source of traffic generates from this zone. It is usually connect to firewall for protection purpose; each packet from Internet is passed through firewall for filtering against attacks. Enterprise network must be protected from outside traffic and must apply the suitable filtering policy in external traffic.

**DMZ zone**: Demilitarized Zone is a network of servers that offers services to users via public network such as Internet [5]. It enables users from outside EN to access services in the DMZ. By having DMZ network, we add additional layer of security. We separate local area network from DMZ network, we limit public users via Internet to access only DMZ services. Services published to public network are vulnerable to attacks and hacking. It is so important to secure these services from attacks and eliminated their effects on LAN if the attacks success. Even users in internal network can access services in DMZ, this access should be filtered using firewall device. DMZ network should has a limited access to LAN network to avoid attacks and hacking to internal network.

We use firewall device to filter inbound/outbound traffic that passes from:

- DMZ network to internal network and vice versa.
- DMZ network to external network and vice versa.
- Internal network to external network and vice versa.

Any services needed to be access via public network such as Internet should be placed in DMZ network. Services which usually placed in DMZ network are:

- Web servers.
- Mail servers.
- FTP servers.
- Proxy Servers.
- DNS servers.
- Web-based application servers.

Web servers host websites of EN, these websites contain many web pages. Users can access these web pages via public network, also they can interactive with their associated web services. Web servers may require access to database servers, access can be done directly or indirectly through a firewall devices. Since database servers hold so sensitive data, they should be placed in internal network.

Although mail servers are exposed to public network, its database is not. This database hold mail messages and other related folder associated with users of EN.

FTP servers enable file exchange (download and upload) between DMZ network and external network. Users in public network represent client side who can send and receive files/folders from FTP servers in DMZ network. FTP servers authenticate users using username/password, each user has a unique username with a specific permission.

Proxy servers are placed in DMZ network in order to allow internal users to access Internet. Proxy servers filter incoming traffic by applying predefined rules and policies. They are intermediate between user (who request a specific website) and outside servers (which host public websites).

EN may provide access to application servers via public network, web-based applications are common one. They can be administrative, financial, and educational. Users in public network can interactive with these applications from anywhere that provide Internet connection. We should have an efficient design of DMZ network, it should be secured from outside attacks. There are two most common way to design DMZ network. The first one is by using only one firewall while the other is by using dual firewalls.

Figure 3.1 shows the DMZ design using a single firewall [38].

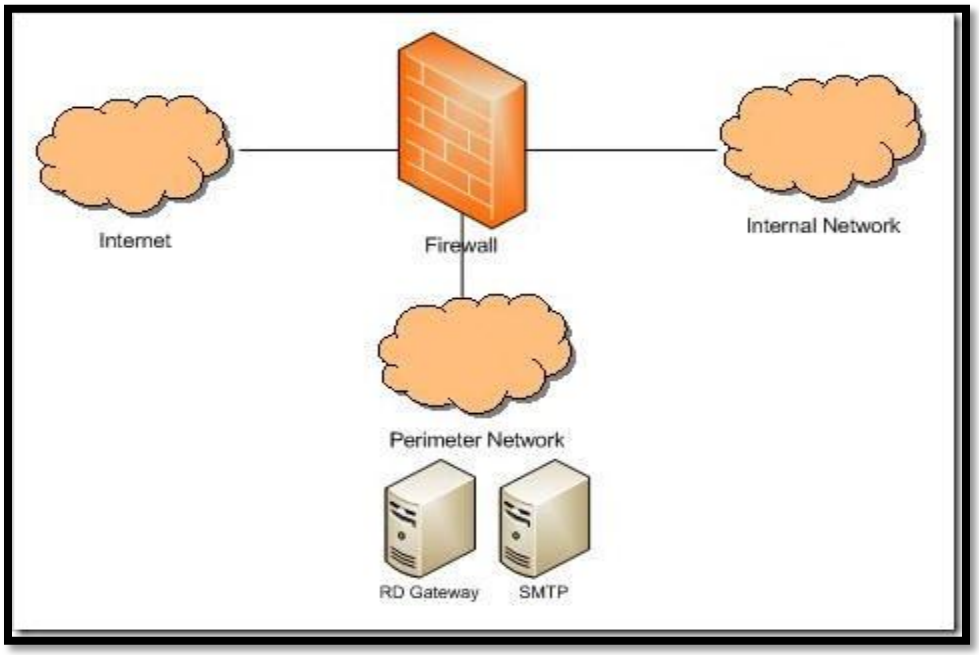



Figure 3.1: Design DMZ using a single firewall.

The Figure shows a single firewall with three interfaces, it also shows three types of networks DMZ network, internal network, and external network. In this design, we use the first interface to connect internal network (LANs), the second interface is used to connect public network (WAN), DMZ network is connected to the third interface. In this design, firewall represents a single point of failure, there is no backup one when the primary fails. Figure 3.2 shows DMZ design using a dual firewall [36].

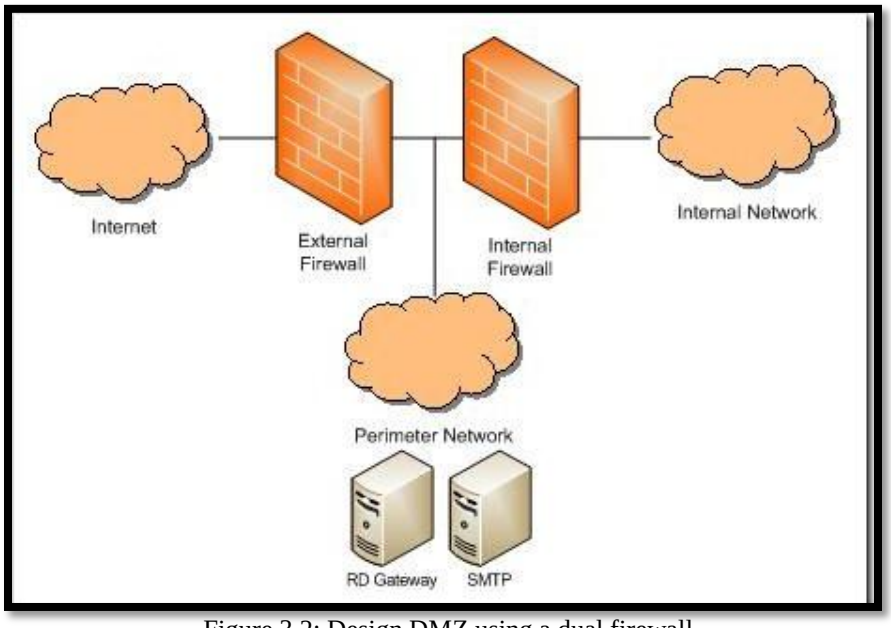



Figure 3 2: Design DMZ using a dual firewall.

Dual firewalls provide a high secure design, DMZ network is placed between the external and internal firewalls. The external firewall (also know front-end firewall) connects external network and DMZ network, it filters traffic between these networks. The internal firewall (also know back-end firewall) connects internal network and DMZ network, it filters traffic between these networks. This design avoid single point of failure, and provides dual protection against attacks.

## 3.2 Enterprise Network Model Services

ENM used in our research depends on a real enterprise network; many services are available through this EN. Services provided by the EN are centralized, they are hosted at data center. Public users connected via Internet can browse web pages hosted at the EN, internal users use domain services, e-mail, and file services, Also branches network get benefits of services of the EN such as connecting to Internet, file service, and database services. Here we list some of these services:

- Interconnection between distributed branches networks and data center, this interconnection depends on different Wide Area Network (WAN) services such as Leased Line, VPN over SHDSL, and Frame Relay.
- E-mail services.
- Domain Names Service (DNS) used for IP resolving into host names.
- Web hosting, hosting includes management and maintains.
- File service and identity authentication.
- Proxy server.9
- Certificate Authority (CA).
- E-services that are provided to partners and customers.

## 3.3 Enterprise Network Model Requirements And Difficulties

In this section, we will discuss the requirements of ENM, main requirements such as availability, redundancy, reliability, scalability, and security will be investigated for more details through subsection 3.3.1. Difficulties in applying these requirements will be explained in subsection 3.3.2.

### 3.3.1 Enterprise Network Model Requirements

ENM requirements include availability, redundancy, reliability, scalability, and security. Each one of these requirements depends on the other, they are not separate. An efficient ENM should care about these requirements, it should apply them at many levels (from user level to application level). Requirements should be refined around the time to get benefits of new technology when applying them in the ENM.

**Availability:**

The ENM should has high availability, we want to have continuously operation EN for a long period of time. The ENM should provide services all the time with the least down time, even it may be seems difficult but it should be five nine 99.999 percent availability possible. We have to achieve availability at different levels, this can be done using different techniques. For example, we can provide availably at devices, services, application levels. Failover cluster is a technique used to provide high availability HA. It includes a group of servers that provide high availability services. Once one server fails the other immediately takes its workload and continues to provide service. Figure 3.1 shows an example of failover cluster. It contains two node high availability cluster[9].Server 1 represents node 1 while server 2 represents node 2. When server 1 fails, server 2 will immediately takes its workload without downtime. It is usually to use more than two nodes for efficient HA. Also Figure 3.3 shows a shared storage which is necessary in designing HA.

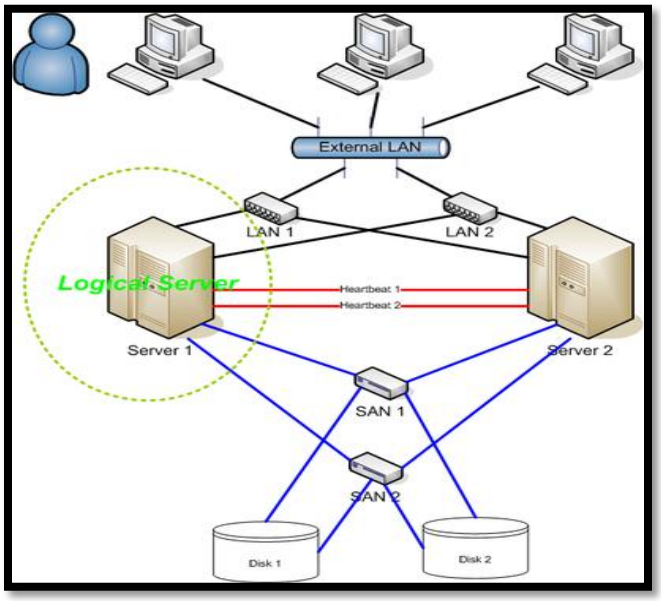



Figure 3.3: An example of two node Failover Cluster (HA).

**Redundancy:**

ENM should also provide redundancy, it should be implemented in network topology. Redundancy is the basic block in implementing fault tolerance, it enables EN to continue operating in the event of the failure. Redundancy enhances network reliability, it helps us to have a continuous operating network. Achieving redundancy requires high cost (double cost), since each device should has a backup one. Due to its high cost, we can achieve redundancy for core devices such as core routers and switches, while keep end devices such as printers, personal without. Core devices interconnect individual users, printers, and wireless access point into the EN. Redundancy can be implemented not only for network devices, but also for cables, UPS, and other network equipments. Figure 3.4 shows an example of a redundant network[32]. As we can see each network devices (firewall, routers, and switches) has a backup one, even cables have a backup one.

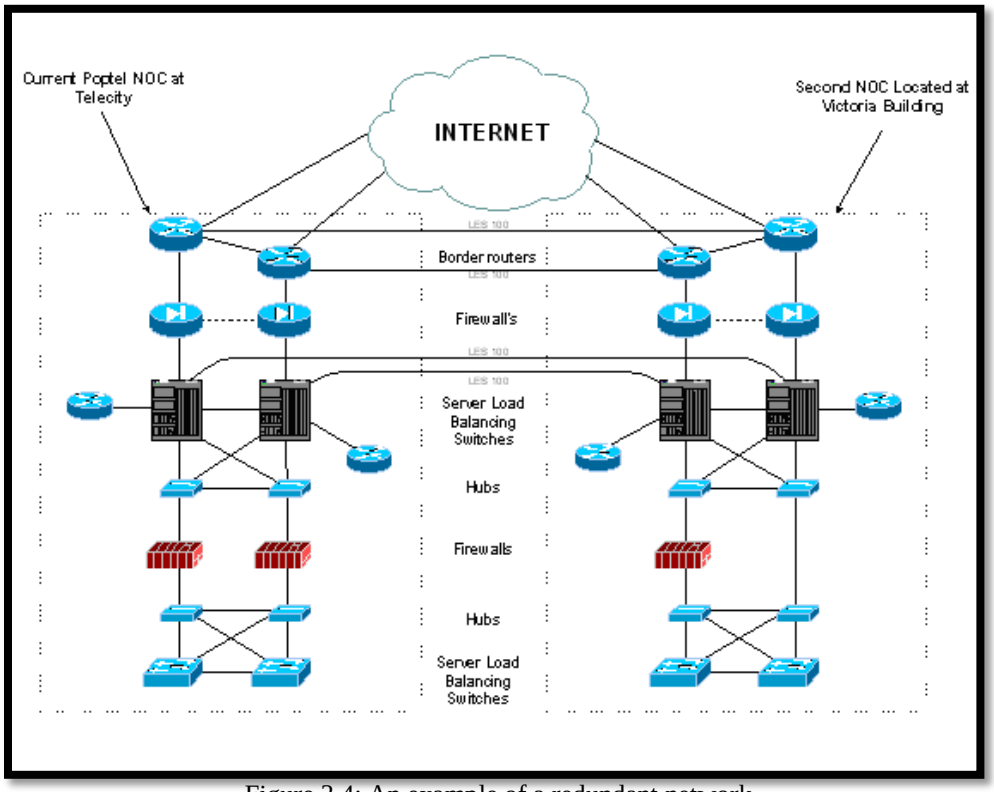



Figure 3.4: An example of a redundant network.

**Scalability:**

The ENM should be scale enough, so it can expand quickly to join new users and applications. This expanding must not affect performance of services available to existing users. Scalability is affected by the topology design of EN, so it is important to be careful when designing EN for scalability. The ENM should provide scalability for Local Area Network (LAN) and Wide Area Network (WAN). For LAN, we should use modular switches which can be expanded for future growth by adding extra interfaces. Also wireless LAN should be designed for scalability, wireless access point should be distributed in a manner that cover more area for future connection. Scalability should be designed for WAN devices, we should select modular routers. They provide capability to expand network when needed in the future without affecting on current operations. Also they should has a scalable IOS based features and protocols such as scalable routing protocols.

**Security:**

The ENM security is essential, we should keep data as secure as possible. We have to classify our data and assets to determine which access permissions and security policy to

use. There are many ways to classify data, a common one is to classify them into public, private, secret, and top secret. This classification determines the way to secure data, securing data can be done using encapsulation and encryption. The ENM should has a written security policy, it should be complete, stable, and clear to all employees in the EN. Security policy should be refined continuously, it is a living a document that reflects changes in the EN. It defined the policies that must be followed in order to protect assets of EN (data, devices, and anything owned by EN). Security policy are written for managers, technical, and end users, it includes many sub-documents. These documents define remote access policy, backup policy, e-mail policy, and other related policies. Network administrator should apply security policy carefully, they should test them before getting them in production network. EN should authenticate users before they get access to EN. It should use strong encryption algorithms to encrypt transmitted data. Security should be implemented at many levels, starting from end user level to application level. Securing user level requires using a trust antivirus that is updated daily. Network devices such as switches and routers should apply secure policy and access control list. They should allow only authenticate users to get connection to EN. WAN devices such as routers should apply access control lists to filter inbound/outbound traffic. Firewall is an important component in EN, it filters all incoming traffic that passes through it. Also network intrusion detection/network intrusion prevention systems are very important to detect and prevent attack and intrusions. Securing connection to branches network using VPN protocols is essential, it uses tunnel to hide transmitted data. The ENM should has a secure deign for interconnection branches network via WAN services. Also we should use a secure wireless network which depend on strong encryption algorithm. They should be tested before use, they should be difficult to penetrate by attackers and hackers. EN should account users, log events, and apply auditing at different levels. Logging helps network administrator in troubleshooting and tracing problems, while accounting users reflects the behavior of users in using resources of EN. Figure 3.5 shows an example of secure network[4]. The figure shows a firewall that it used to protect DMZ network and internal network from outside network. Also the network contains NIPS/NIDS sensors to prevent attacks and hacking.

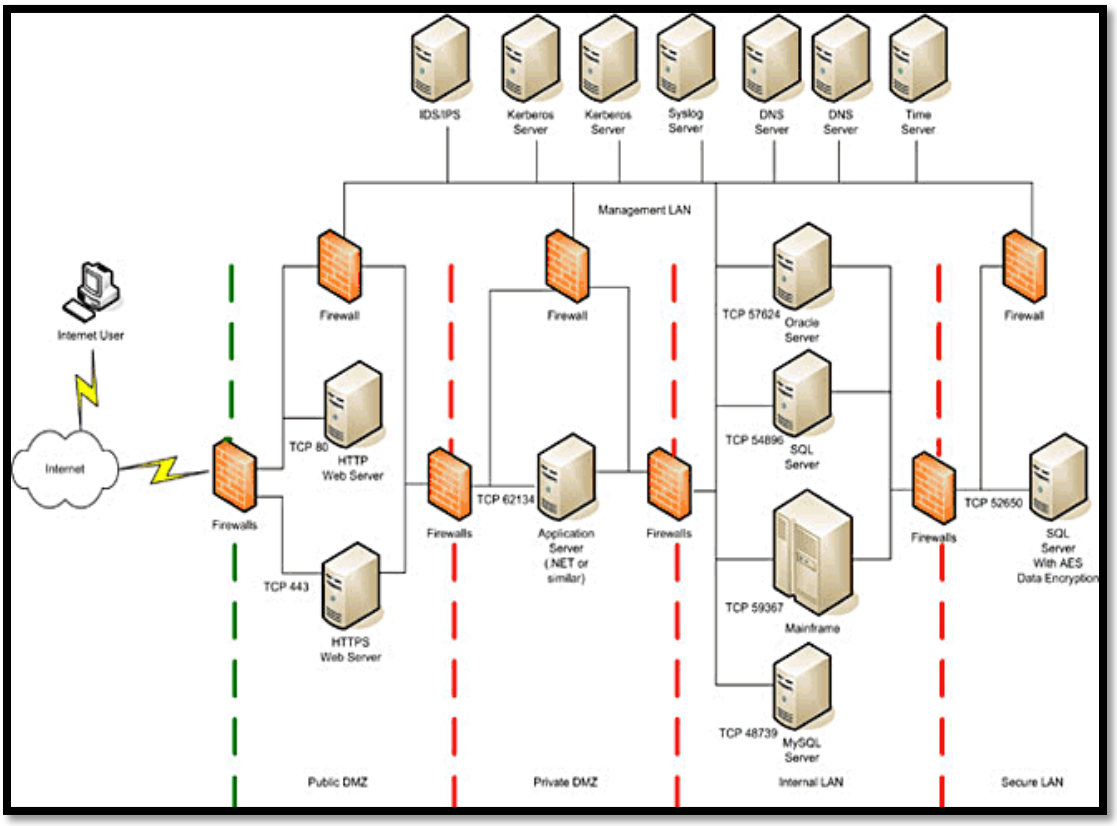



Figure 3.5: An example of secure network.

### 3.3.2 Difficulties In Applying ENM Requirements:

This section discuss the difficulties of applying ENM requirements. Even is not easy job to apply ENM requirement, but it is not impossible.

Since our ENM offers services over Internet for a large number of users, we should care about HA. Public users via Internet access services hosted in the EN, also branches networks get benefits of these services. Downtime should be as minimum as possible, it should be eliminated by failover technology. ENM provides large number of services that require more management, cost, and technical support. As more web services are include, we need an efficient high availability. Each service need a specific configuration for availability, it may also need additional network devices. Monitoring around a clock is important, it guarantees continuous operating services. Getting HA requires a well training staff, who is responsible to keep services available all the time without stopping. High cost needed of providing HA is consider a big problem for EN.

We need a well designed network topology for our ENM, it should care about data center and branches networks. Data center should be always online, each device in data center should has a backup one. No one can doubt that redundancy is costly but it is necessary to eliminated downtime. Moreover, different branches networks with different connection types (use different WAN services) represent a common problem in applying redundancy. Each branch network should has a backup connection when the primary one fails.

We need a scalable ENM, which enables future expansion without changing the network topology. Scalability should be implemented for data center, LANs, and Branches networks. we should have modular switches in data center to enable future growths, modular switches should be used for DMZ and core switches. Other network devices like firewall and routers should be scalable enough. LANs should use modular switches, they will enable new users to connect in easily and conveniently way. Even no additional configuration is needed for scalability, cost is the common problem. Cost is the dominant factors in applying scalability, it is less cost to buy 24-port switch than 48-port switch. More ports/interfaces on the network devices mean more cost. Scalability should be considered when designing the topology of ENM.

Security should be configured carefully, it must be tested before applying. It should be implemented at services level, operation systems level, and devices level. Since our ENM hosted many services that access via Internet, we should secure these services as possible. We need a written security policy documents, that determines access permissions. Devices such as firewall, IPS/IDS are essential to filter incoming traffic, detect attack, and prevent attack. Our ENM provides different services, each service requires a specific security configuration. Services related to database should be secured enough to prevent steal and corruption of data. Providing security for each devices depends on the its function and location. Different branches networks increase overload on the administrators, there is no enough information technology staff in branches networks. Connection between branches networks and data center should be secured, we can use encryption, tunnels for this purpose. Management of security policy, security auditing, user accounting requires an expert security staff.

## 3.4 Threats On Enterprise Network Model

In this section we will discuss the potential threats that may halt EN. Usually security threats exploit vulnerabilities in EN, vulnerabilities indicate the degree of weakness whether in network devices, operating systems, configurations, security policy or network protocols.

Network devices such as routers, switches, servers all may have vulnerabilities, as well as network protocols such as routing protocols, FTP protocol, and HTTP protocol. Mis-configuration of network devices and security policy represent weakness which could be exploited by attackers. Moreover, Operating systems have vulnerabilities that should be solved and fixed in order to avoid attacks and hacking. Since threats try to get over these vulnerabilities to halt our EN, we should address these vulnerabilities to eliminated them.

It is important to secure our EN from physical threats which try to compromise network devices physically. Physical threats include hardware threats, environmental threats, electrical threats, and maintenances threats. Hardware threats halt network devices such as routers, switches, servers, and any hardware devices in EN. They should be mitigated by securing server room through limiting entrance to only authenticated users, using security cameras, and monitoring corridors towards servers room.

On the other hand, environmental threats can be mitigated using temperature control, positive air flow, humidity control, and others. We can use UPS, generators sets, and redundant power supply to eliminate electrical threats that have a dangerous effects on EN operations. Imagine what happen if the main source of electricity fails and we don't have a backup one. The results will be so bad, servers room will get down. It is so bad to hear that some network administrators do not care about maintenance these threats. Poor cabling, poor labeling, and poor handle of electrical components are examples of maintenance threats. Network administrators should label every devices, equipments, and even cables in the server rooms, they should electrostatic discharge procedures to avoid maintenance threats.

In addition to physical threats, we have another type of threats that are classified according to it source. Internal threats are generated from internal network, they are dangerous than external threats that are generated from public network. Internal users are trust to network administrators, they know details of the internal network. Moreover, they

have authorized access to internal network, they represent a big problem in mitigation internal threats. While effects of external threats may be destructive, they still depend on the expertise of the attacker-either amateurish (unstructured) or expert (structured) [39].

One of the most popular threat is social engineering. It is so basic, it does not need deep skills or even experts. The main purpose of social engineering threat is to steal credit cards, users passwords, and detection users files/folders. Social engineering threat try to trick users using e-mail or any type of other messages, fake e-mail seems to be from a trust company. In fact this e-mail is from attacker in order to trick users. We can eliminate social engineering threat by educated users to avoid open e-mail from unknown senders, Also network administrators can use security devices to filter e-mail that are generated from a specific website.

## 3.5 Enterprise Network Model Topology

Here we will introduce the topology of our ENM and explain its each component. We will also discover functions of these components deeply and its effects on ENM. Figure 3.6 shows the topology of our ENM.

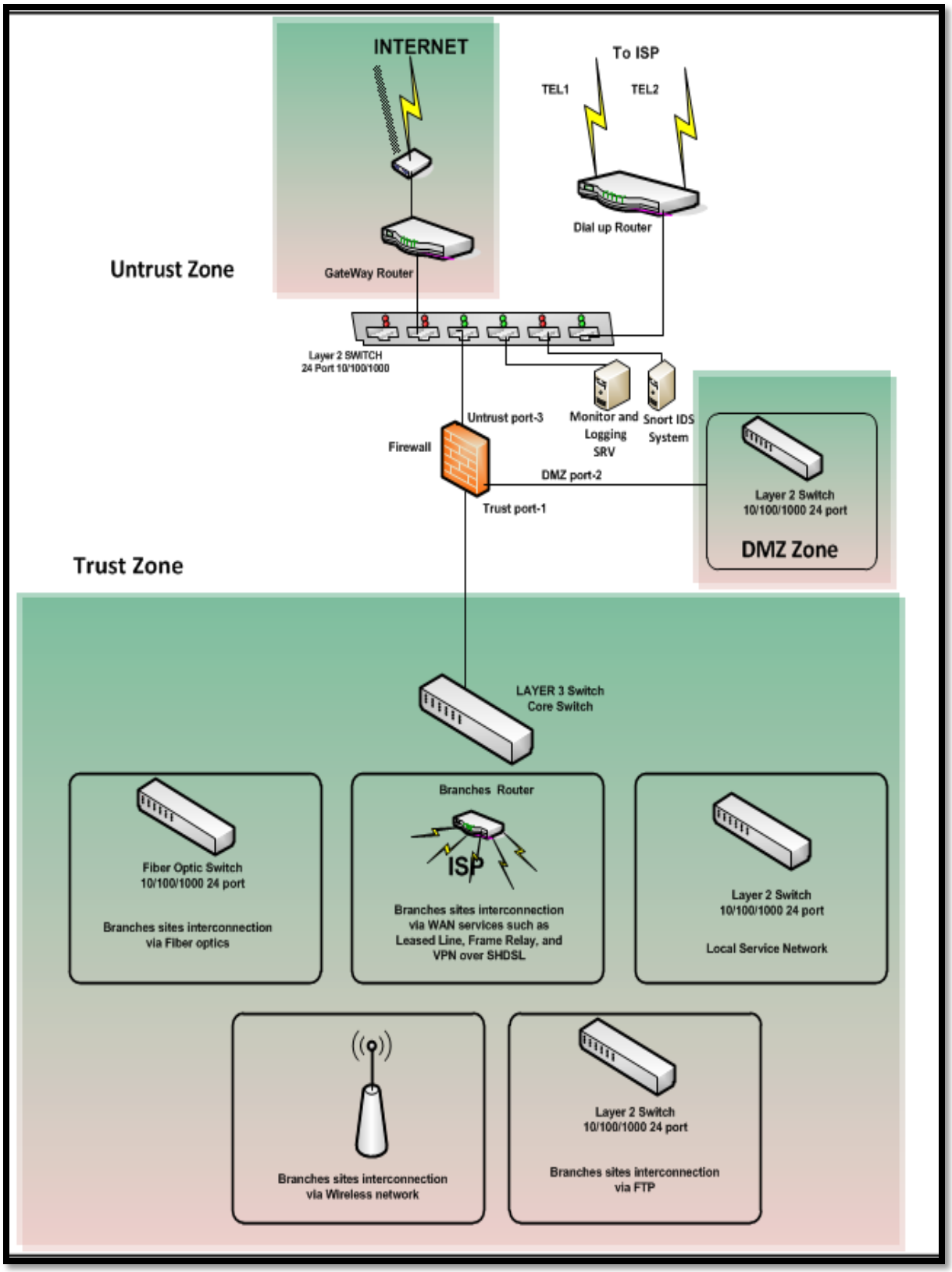



Figure 3.6: The topology of our ENM.

The topology of our ENM is built from three main zones which are DMZ zone (as explained in section 3.1), internal zone, and external zone. Each zone has a specific function, it includes various devices and services. For more detail about services that are hosted in DMZ network, please refers to section 3.2.DMZ zone is connected directly to firewall in order to inspect each incoming packet passes to it using filtering rules. It includes a layer 2 switch and servers. Servers are used to host EN services while Layer 2 switch is used to interconnect these servers. Figure 3.7 shows an example of DMZ network [40]. as it shown, public servers (which are accessed via Internet) are grouped together in DMZ network. It is connected to firewall interface for traffic filtering and access control.

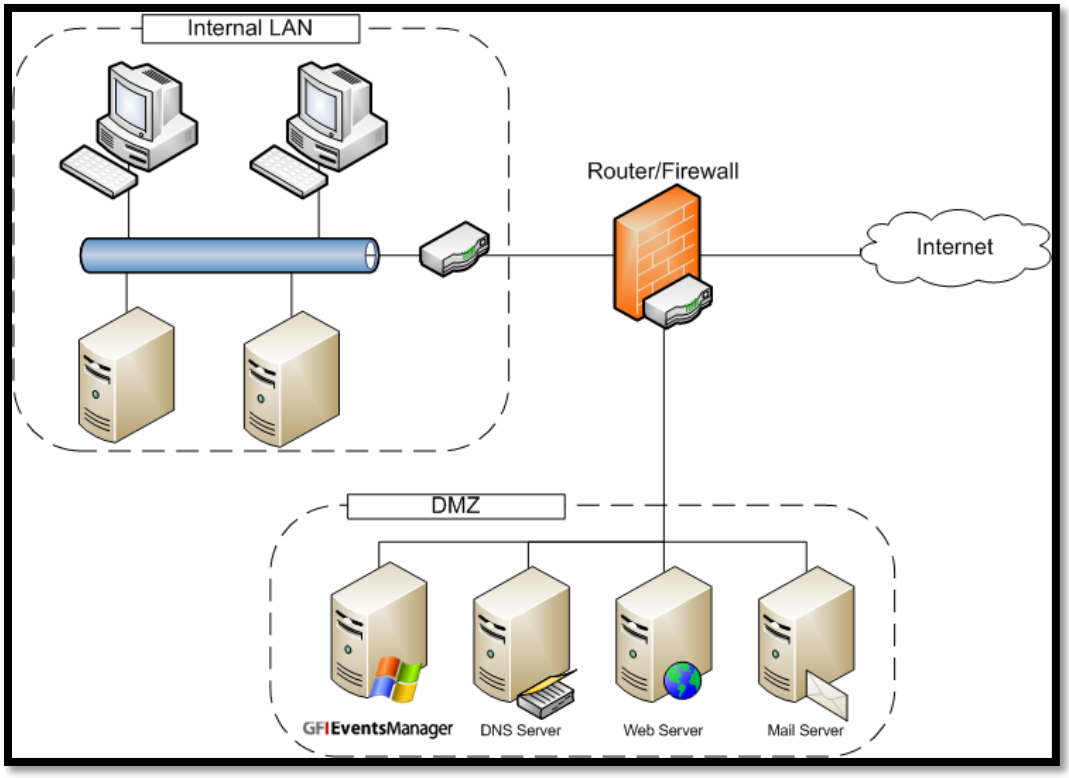



Figure 3.7: An example of DMZ network.

Internal zone is also known as trust zone, it includes local service network and branches networks. Branches networks are connected to EN using Foil Twisted Pair FTP cables, wireless connection, fiber optic cable, and WAN services.

Local service network provides local services for users of local area network. The common services that are used in LAN are: local Domain Name System (DNS) service, Dynamic Host Configuration Protocol(DHCP)service, domain controller service, Internet service (proxy server), local database service, and monitoring service.

FTP cables are used to connect closed buildings and branches to EN data center. Enterprise network uses category CAT 7 for FTP connection, it provides high transmission speed of 10 Gigabit per second. Wireless networks are used to connect other buildings and branches to EN using wireless technology. Enterprise network uses different wireless technology that depends on Wi-Fi networks. It also uses microwave transmission for connecting distant branches. Fiber optic cables are used to connect very distant buildings and branches to EN data center. Fiber optic single mode is used to interconnect very distant branches with high data rate 10 Gigabit per second.WAN services are used to connect buildings and branches to EN using services provided by local Internet Service Provides ISP. WAN services include leased line, frame relay, VPN over SHDSL, and others.

Internal zone is also includes layer 3 switch, it is a core switch that interconnects all branches networks as well as local services of EN. It is connected directly to firewall through internal zone. Layer 3 switch interconnects wireless branches, FTP branches, Fiber optic branches, and other branches to EN data center and its local services. We use layer 3 switch to control access and filter traffic between branches networks on the one hand and between branches networks and EN datacenter on the other hand. Branches Router interconnects branches that connected via WAN service to EN data center. Also, it applies access control lists to filter traffic inbound and outbound between branches and data center.

External zone is also known as outside zone or public zone. it includes the following components: gateway router, firewall, layer 2 switch, dial-up router, Intrusion Detection System (IDS), monitoring/logging server, and Internet service from local ISP.

Gateway router is used to connect enterprise network to outside public network (Internet). A number of access control lists are applied to gateway router for filtering incoming traffic and enhancing security of EN. Firewall does filtering for each packet

passes into internal and DMZ zones. Action are executed according to predefined rules and policies, they could permit or deny traffic.

Layer 2 switch is also known as untrust switch, it connects gateway router to firewall. It is used to connect IDS/IPS devices and monitoring and logging server. Dial-up router is used in emergency for management and to connect to EN. Intrusion Detection System is implemented using open source software SNORT (open source IDS/IPS) and configured over CentOS Linux distribution. Monitoring and logging Server is used in enterprise network for monitoring and logging outside traffic.

## 3.6 Summary

In chapter 3, we explained basic concepts related to our enterprise network. We talked about different devices, network equipments, protocols, and networks. Enterprise network includes different network devices such as layer 2 switches and layer 3 switches that are used as access, distributed, and core devices. On the other hand, router is used to connect distinguishing networks, it is used for WAN services connection. Other devices such as firewalls are used to filter inbound and outbound traffic passing through them from and to different networks such as external, internal, and DMZ networks. Intrusion prevention system is used to detect and prevent potential attacks according to predefined signatures. Also we introduced different connection such as Frame Relay, Leased Line, and VPN. While Frame relay provides shared bandwidth, Leased Line provides dedicated bandwidth for connected network. VPN presents a secure, cheap solution for connecting branches networks to enterprise networks, it establishes private network via public network such as Internet. Also we discussed different protocols such as HTTP/HTTPS, SNMP, and others. HTTP/HTTPS are the most used protocols in enterprise networks, all web services applications use HTTP/HTTPS. HTTPS provide encryption and authentication while HTTP is not. We introduced DMZ network which includes public services that allow public user (via Internet) to access them. DMZ network hosts web server, E-mail server, DNS server, FTP server, Web-based application, and others.

As we discussed before, there are different requirements of enterprise network such as availability, security, redundancy, reliability, scalability. These requirements are essential to provide continues and reliable services of enterprise network. We also explained

different security threats that may compromise network, these threats could be so complex such as APT-based attacks. Also this chapter implied the importance of designing an efficient and secure model of enterprise network. Finally, we discussed our enterprise network topology, we discovered each components in detail. It is very important to understand each components of enterprise network topology in order to build a secure model.

# CHAPTER 4: Security Enhanced Model For ENM

In this chapter, Proposed security-enhanced model of ENM will be explained through chapter 4 as well as its implementation details. We will do deep inspection of traffic passing through enterprise network. Inbound and outbound traffic will be analyzed to determine the most used traffic (protocols) through different working time. Also we will explain how to detect and prevent APT-based attacks such as Aurora attack.

In section 4.1, we will describe our proposed security enhanced model of EN in more details, we will investigate its components, topology, procedures, and other related topic. In section 4.2, we will describe various traffic analysis tools, There are many traffic analysis tools such as NetFlow, NFSen, IPFIX, SiLK, and others. In our traffic analysis, we will use NetFlow tool to inspect traffic. Analysis of bandwidth usage of EN will be discussed in section 4.3, MRTG tool will be used for this purpose. In section 4.4, we will do deep analysis of HTTP/HTTPS traffic using Fiddler2 tools, it can inspect encrypted HTTPS traffic. Section 4.5 will introduce intrusion detection and prevention system and its role in our proposed security-enhanced model. Advanced Persistent Threat will be discussed in section 4.6, Aurora attack is considered as APT-based attack. Our proposed model is designed to detect and prevent APT-based attack in smart and efficient way. Aurora attack prevention using our proposed model will be discussed in section 4.7, we will introduce the require signatures and rules to detect and prevent such attack.

## 4.1 Our Proposed Security-Enhanced Model

In this section, we will discuss our proposed security-enhanced model. We will explain implementation details and design issues, as well as tools that used in our proposed model.

### 4.1.1 Security-Enhanced Model Components

Our proposed model includes nine modules which are: external data module, branches networks module, secure connection module, analysis and deep inspection module, network intrusion detection/prevention module, host intrusion prevention and antivirus

module, firewall and web contents filtering module, management module, and real time response module. Figure 4.1 shows modules of our proposed model.

External module includes traffic coming from external network such as Internet. Traffic from external network contains different types of applications/protocols, HTTP/HTTPS traffic is the most commonly used. Other traffic are used in less common, data stream traffic such as video and voice are popular example. External module also contains traffic which is used by network administrators to manage enterprise network remotely through external network.

Branches networks module represents branches networks that are connect through WAN services such as leased line, frame relay, and VPN service. Also it contains branches networks that are connected through wireless connection such as Wi-Fi, WiMAX and microwave.

Secure connection module uses encapsulation and encryption to secure connection to branches networks. We intent to provide security for branches using routers that have IOS with network intrusion prevention system.

Analysis and deep inspection module provides deep inspection of each data packet that entering or leaving enterprise network. Different tools can be used for traffic analysis, section 4.2.1 explains the most common traffic analysis tools. Moreover, we can use network intrusion detection system such as SNORT [17] and host intrusion detection system such as OSSEC [18] for the same purpose.

Network intrusion detection/prevention module detects and prevents potential attacks and hackers from compromising enterprise network. It provides a secure layer against attacks and intrusions, this module can be implements using hardware or software solution. In our proposed model, we implement software solution using open source tool SNORT.

Host intrusion prevention and antivirus module detects and prevents potential attacks and hackers from compromising individual hosts. This module can be implemented using hardware or software solution, we implement software solution using open source tool OSSEC in our proposed model.

Firewall and web contents filtering module provides security at layer 3,4,5 and 7 of the OSI reference model. It scans each packet against predefine signatures in order to detect attacks, firewall is a core security device in enterprise network.

Management module collects logs and events from different network devices and analysis them for attacks and malicious activity. It is considered as a feedback for network security components in enterprise network, each network device is configured to transfer its logs to management center. It monitors and audits security events once they occur, we depend on management module to refine and update security policy of enterprise network model. We use Splunk server [20] in our proposed model to collect and mange logs from network devices. Management module sends and receives different information from analysis and deep inspection module.

Finally we have real time response module which is responsible about taking actions against attacks and intrusions existences. There are different actions that can be applied, we can stop malicious activity by blocking it as well as sending alert to administrators. Real time response module can log, alert, block, deny, reset malicious connection, actions are different according to predefined configurations.

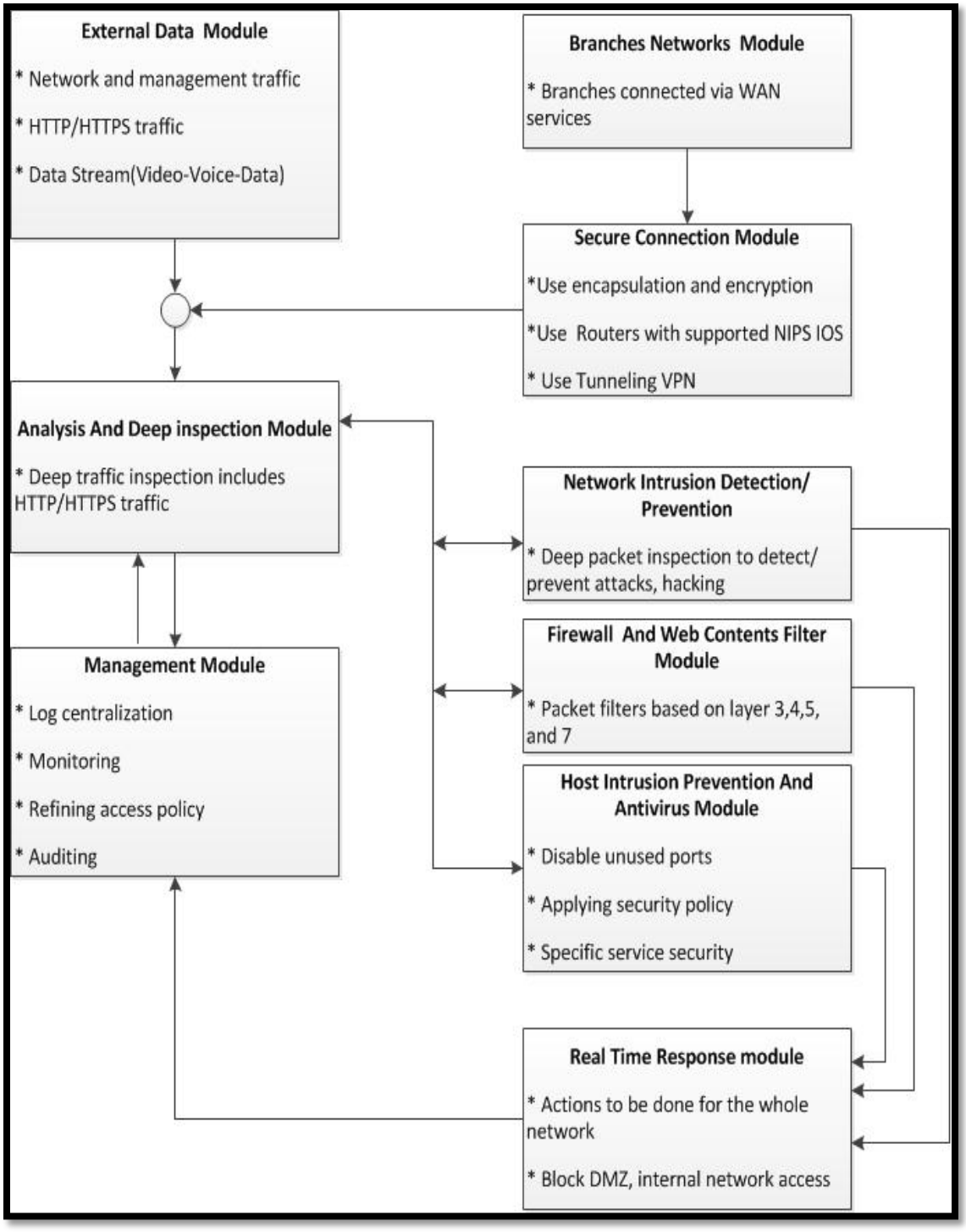



Figure 4.1: Modules of our proposed security-enhanced model.

### 4.1.2 Techniques And Tools Used In Security-Enhanced Model

In our proposed security-enhanced model, we will use SNORT as NIDS, we will configure SNORT NIDS as active response. In case of detecting intrusion SNORT NIDS, we will do the following: send alarms to administrator, send e-mail messages, log entries, and reconfigure gateway router to block connection and prevent intrusion through Access Control Lists (ACLs).

Since we have more than NIDS systems in our enterprise network, we will use SnortCenter [53] for central management of rule sets/signatures and snort configuration files. SnortCenter provides flexible management of distributed SNORT NIDS, it is a Web-based management application that uses PHP/MySQL web interface. SnortCenter provides the following features: SNORT daemon up or down status indicator, remote SNORT stop/start/restart functionality, access control for SnortCenter users, and sensor groups.

In our proposed security- enhanced model, we will provide efficient and secure enterprise network. We use hardware firewall in our proposed model, it includes NIPS system module inside. We prefer to place NIPS module inside firewall for the following reasons:

- Reducing budgets, we need one appliance rather than two appliance (firewall and NIPS).
- Reduce false positive alarms that are generated where there is no intrusion or attacks.
- Simplifying determination of attacks using real IP addresses and by avoiding IP with NAT option.
- Providing intrusion prevention for DMZ network and Internal network.

Also in our model, we don't only depend on NIPS module, but we use SNORT NIDS to monitor and analysis traffic from/to DMZ and Internal networks. We intend to get deep inspection of traffic that pass through DMZ and internal networks. SNORT NIDS will have no effects on network performance, since it just receive a copy of traffic pass from/to DMZ and Internal networks. Moreover, we run SNORT NIDS in active response mode in order to prevent potential intrusions and attacks as explained in section 4.7.

Figure 4.2 shows the proposed security-enhanced model of enterprise network, it shows the placement of NIPS and NIDS in EN. As it shown from the figure, we place NIPS system module inside the firewall. SNORT NIDS are distributed to monitor real time traffic for DMZ and internal Network. The first SNORT NIDS has two network interface cards NICs, one interface (first NIC) is connected to Switched Packet Analyzer Port (SPAN) of DMZ layer2 switch while the other one is connected to the management network. SPAN are special port on layer 2 switch, it has no IP address. Management network is used to connect monitor and logging devices, we prefer to separate it from other networks for security and management issues. The second SNORT NIDS has two network interface cards NICs, one NIC is connected to SPAN port of Internal layer 3 switch while the other NIC is connected to the management network.

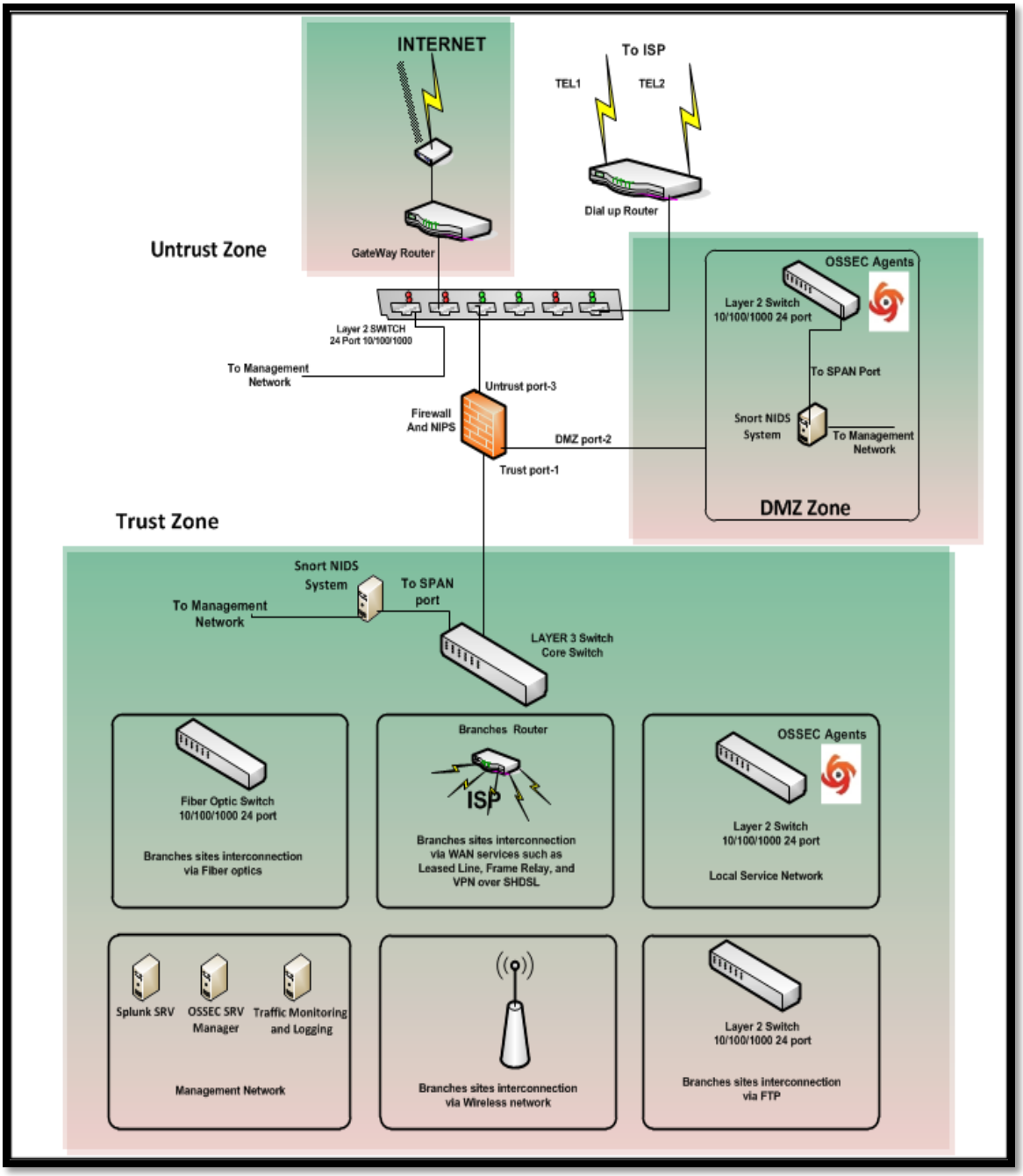



Figure 4.2: The proposed security-enhanced model of enterprise network.

It is necessary to provide security for branches networks. Our enterprise networks includes a large number of branches networks, we cannot provide NIPS for each branches due to management needs and cost requirement. Implementing NIPS for each branch requires a well trained staff for monitoring and analysis, we will need to buy a NIPS appliance for each branch. Due to these previous difficulties, we use NIPS module inside

router at each branch network. Monitoring and management of routers are done remotely from EN management network.

Our proposed model provides a complete security solution for enterprise network, NIDS and NIPS are not sufficient. We need Host Intrusion Prevention System (HIPS) for individual hosts, We want to provide security at servers and hosts level.

In our model, we use HIDS to monitor the following:

- The sate of host by monitoring, logging, and analyzing behavior of hosts.
- Real time traffic that pass in/out host though NICs.
- The way the host store its information, it tries to detect if there is abnormal behavior due to potential intrusion.
- Applications/service that consumed resources such as RAM and CPU, it identify how and which resources are consumed and by whom.
- Detecting violation of security policy that host must has.
- Detecting intrusions/attacks that try to change registry keys.
- Stopping attempted to change operating system or applications by a intruder or malware.

We use HIPS to protect servers which host services of enterprise network, HIPS will protect our servers from zero-day attacks. HIPS uses anomaly detection which provides ability to stop unknown attacks. As is shown in Figure 4.2, we implement OSSEC on each server of our enterprise network, also we will have OSSEC server as central management sever for monitoring and analysis real time traffic received from servers devices (OSSEC agents). Also we configure OSSEC manger in active response in order to stop malicious activity. The following servers of DMZ and internal networks will have OSSEC agent installed:

- WEB hosting server.
- FTP server.
- Mail server.
- Public DNS server.
- Backup server.

- Database server.
- Local DNS server.
- DHCP server.
- Domain controller server.
- Proxy server.

## 4.2 Traffic Analysis Of Enterprise Network Model

Traffic analysis is considered as the starting point for design a security model of ENM. It can be done using many different tools; these tools depend on packet sniffing. Packet sniffer is also known as protocol analyzer or Ethernet sniffer [12], it is a program running in a network device that passively receives all data link layer frames passing through its network adapter. Figure 4.3 shows data travels from application layer to the network interface card [12].

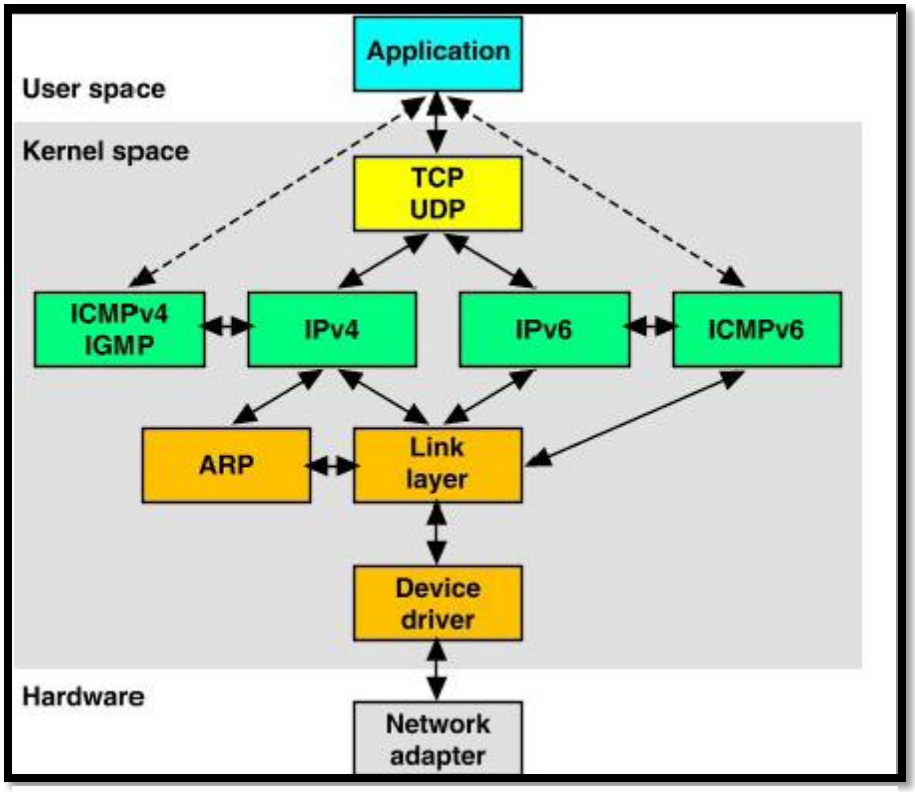



Figure 4.3: Data flow from application layer to network interface card.

Packet sniffer tries to capture data that is address to other machines, it saves it for latter analysis. Network administrators use packet sniffer for monitoring network traffic, troubleshooting network, identifying bottlenecks, and enhancing data transmitting in network. Unfortunately, packet sniffer can be used in hacking networks; it can steal sensitive information such as credit cards and passwords. Many tools such as traffic analysis tools and intrusion detection systems are depend on packet sniffer in their work. In this research, we will use packet sniffer to do traffic analysis of EN.

### 4.2.1 Common Traffic Analysis Tools

There are many tools used for capturing network traffic, it is captured as flow records [41]. Most of these tools support network traffic analysis using graphical interfaces. Here we list the most popular tools used for network traffic analysis.

**NetFlow**[40]**:** is a network protocol designed by Cisco systems, it allows Cisco routers and switches to export and generate a flow record into a traffic analyzer server. In order to use NetFlow protocols, we need to configure Cisco routers and switches firstly. NetFlow analyzer is available for Windows and Linux platforms. Most common NetFlow versions are version 5 and version 9.

**NetFlow Version 5:**is widely used by researchers and network administrators to monitor network usage [46]. The most widely used tool is NetFlow version 5, it uses static NetFlow format [47]. There are many available GPL tools that process, analyze and present NetFlow version 5 format.

**NetFlow Version 9**[48]**:**is the latest Netflow version introduced by Cisco for the network monitoring and analysis purposes. Netflow Version 9 format is a template-based, it is a distinct feature from previous versionNetflowV5. Netflow Version 9 is the basic of an IETF standard. The template-based provides an extensible design to record format, which will allow for future enhancement to NetFlow services without requiring concrete changes to the basic flow-record format.

**IPFIX** [41]**:** is an open standard defined by the IETF based on NetFlow v9. It is used widely in different network traffic analysis application.

**NfSen**[42]**:**is a graphical based tool for network traffic analysis, it can understand NetFlow format. NfSen can be used to create history as well as a continuous profile, it can also set alerts based on various conditions. NfSen is a graphical web-based front end for the nfdump netFlow tools. NfSen displays NetFlow data from many sources is available using flows, packets and bytes, easily navigate through the NetFlow data, also we can process the NetFlow data within the specified time span. NfSen is available for Linux platforms.

**Flow-tools** [45]**:**are group of programs which are used for capturing and processing NetFlow v5 flow records. The group include 24 separate tools, flow-tools use UNIX pipes to make these tools work together. Not only flow-tools can capture traffic but also can read, filter and print flow records. They are saved in a fixed-size format. Flow-tools are available for Linux platforms

**Nfdump**[42]**:**It can capture, collect, and process NetFlow traffic on command line. Nfdump supports NetFlow v5, v7 and v9,it can analyze previous data traffic as well as track interesting patterns continuously. Before analyzing, all data are stored to disk, they are organized in a time based fashion.

**SiLK**[43]**:**is the System for internet-Level Knowledge, it was developed by CERT in order to simplify security analysis of large networks. SiLK contains a collection of traffic analysis tools. It provides an efficient way of collecting, storage, and analysis of network flow data which enables network security analysis to rapidly query large historical data sets. SiLK installation consists of two kinds of application which are packing system and analysis suite. We can install SiLK on Linux operating system.

**FlowScan**[44]**:**it contains a flow collection engine, a high performance database, and a visualization tool, it can analyze traffics and reports on Internet protocols (IP). FlowScan produces a graphic image that displays network traffic, consumed bandwidth, and other statistics. FLowScan is available for Linux distribution.

**AutoFocus**[49]**:**is an automatic traffic analysis and reporting tool. It analyzes network traffic and provides both textual reports and time series plots. It is available for Linux distribution.

**MRTG:** Multi Router Traffic Graph is a free software for monitoring and measuring traffic load on the network [51]. MRTG generates a graphic view about usage traffic (bandwidth) along time. It display traffic load of network every 5 minutes by default. MRTG allows user to print reports about usage traffic every day, week, and year, it can be used to measure traffic load of any network devices. MRTG graphs can be accessed through web browsers.

In our research, we use NetFlow analyzer professional plus as a traffic analysis tool to perform network traffic analysis. We also use SNMP service to get names of devices (routers and switches) and associated interface which are under analysis.

NetFlow analyzer professional plus provides the following features [50]: simplified bandwidth monitoring, in-depth traffic analysis, QoS validation using Cisco CBQoS, alerting based on thresholds, departmental bandwidth usage, custom reports, reduced operational costs, reduced training costs, effective data storage, and completely web based management.

### 4.2.2 Configuring NetFlow Export On Network Devices

To get start with NetFlow analyzer professional, we have to configure both NetFlow analyzer server and NetFlow export on network devices that we will be analyzed. We configure a laptop with 5.88 GHz Intel core i5 processor and 6G byte memory as NetFlow analyzer server, it runs Windows 7 as operating system. NetFlow analyzer server integrates both flow collector and analyzer. Since routers and switches of enterprise network model are from Cisco vendor, we have to do additional configurations on these devices before doing traffic analysis. For more detail about these configurations please refer to appendix A.

## 4.3 Network Traffic Analysis

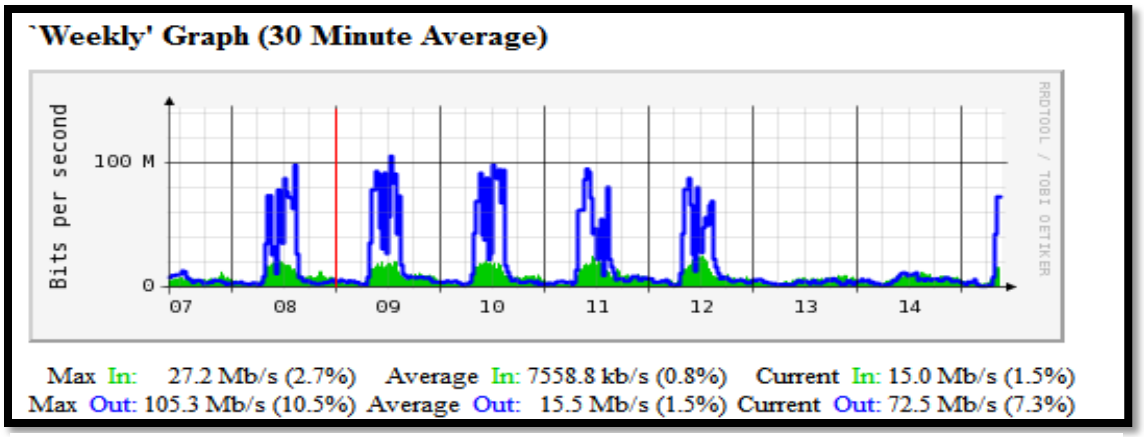
In this section, we will discuss the results of network traffic analysis, it will help us to determine the bandwidth usage of EN and types of applications/protocols being used. Services such as Internet, WAN connections (it is used for branches interconnection), and local services within a specific LAN (each branch contains a LAN) consume different

bandwidth. We expect to have a deep view about types of applications/protocols being used by users of EN.

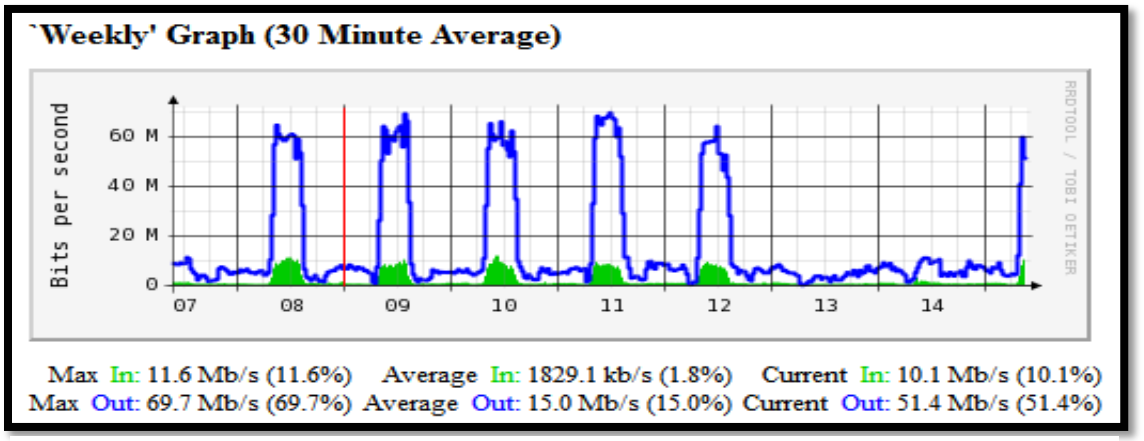
Traffic analysis is done during one week through a full-time work days, we started analysis from 7/9/2013 to 14/9/2013. Full-time work begins on Sunday at 8:00 am and ends on Thursday at 3:00 pm, Saturday and Friday are weekly vacation days.

We use two different tools for traffic analysis, MRTG and NetFlow. MRTG is used to determine bandwidth usage while NetFlow is used to discover types of applications/protocols being used.

Figure 4.4 shows bandwidth usage in EN during a week. Bandwidth usage is divided into inbound bandwidth ( denoted by green color) and outbound bandwidth (denoted by blue color). The Figure shows date of traffic analysis which is from 7-14/9/2013.




**(a)**




**(b)**

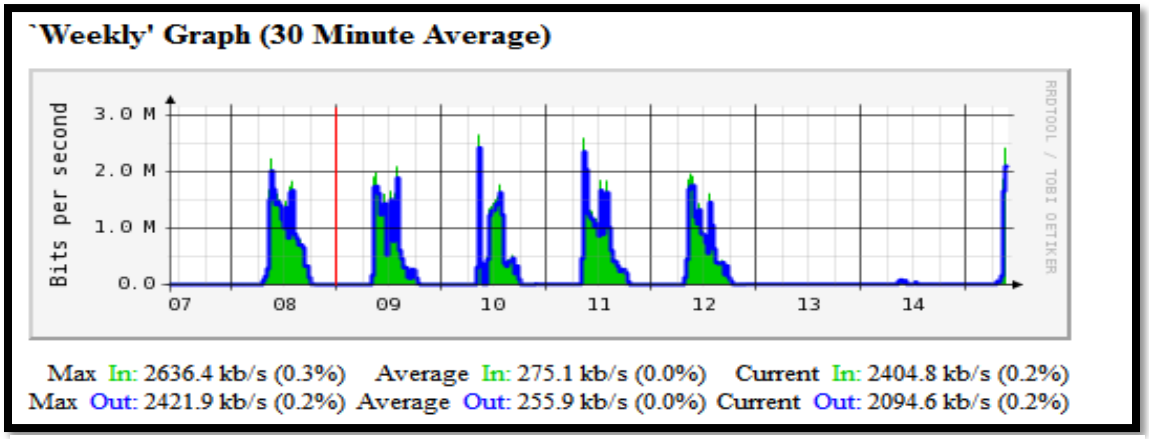



Figure 4.4: Bandwidth usage (a) Internet usage in EN during a week. (b) Bandwidth usage by branches networks during one week. (c) Bandwidth usage by one branch network during one week.

EN has Internet bandwidth of 150 Mbps, which is provided by a local Internet Service Provider ISP. Internet usage during one week is shown in figure 4.4(a), inbound bandwidth represents uploaded traffic. It is generated when users upload files/folders

from internal network and/or DMZ network to public network (Internet). On the other hand, outbound bandwidth represents downloaded traffic which is generated when users download files/folders from public network (Internet) to internal network and/or DMZ network. The maximum inbound traffic of Internet usage is about 27.2 Mbps (2.7%), while the maximum outbound traffic is about 105.3 Mbps (10.5%). Also it can be shown from Figure 4.4(a), the average inbound traffic of Internet usage is about 7.5588 Mbps (0.8%), where the average outbound traffic is about 15.5 Mbps (1.5%). It is clear that inbound traffic (upload) of Internet usage is less than outbound traffic (download). Also we observe that Internet usage is nearly the same for most work days of the week. Internet usage is almost non-exists in vacation days (which are Saturday and Friday-day 13 and 14) and in duration between 3:00 pm and 8:00 am. We prefer to do backup operation after 3:00 pm and before 8:00 am since this duration has the least consumption of Internet bandwidth.

EN interconnects its branches via WAN services thought bandwidth of 90 Mbps, which is provided by a local Internet Service Provider ISP. Bandwidth usage by branches networks during one week is shown in Figure 4.4(b), inbound bandwidth represents uploaded traffic which is generated when users upload files/folders from a branch network to DMZ network, another branch network, local services network, and public network (Internet). Outbound bandwidth represents downloaded traffic which is generated when users download files/folders from DMZ network, another branch network, local services network, and public network (Internet) to the branch network.

The maximum inbound traffic used by branches networks is about 11.6 Mbps (11.6%), while the maximum outbound traffic is about 69.7 Mbps (69.7%). Also it can be shown from Figure 4.4(b), the average inbound traffic used by branches networks is about 1.8291 Mbps (1.8%), while the average Outbound traffic is about 15 Mbps (15%). It is clear that outbound traffic (download) used by branches networks is more than inbound traffic (upload). Also we observe that the traffic used by branches networks is nearly the same for most work days of the week. Unlike Internet usage, There is a bit small amount of traffic in vacation days (which are Saturday and Friday-day 13 and 14) and in duration between 3:00 pm and 8:00 am. It is observed that inbound traffic used by branches networks is limited only to working days, specifically between 8:00 am and 3:00 pm.

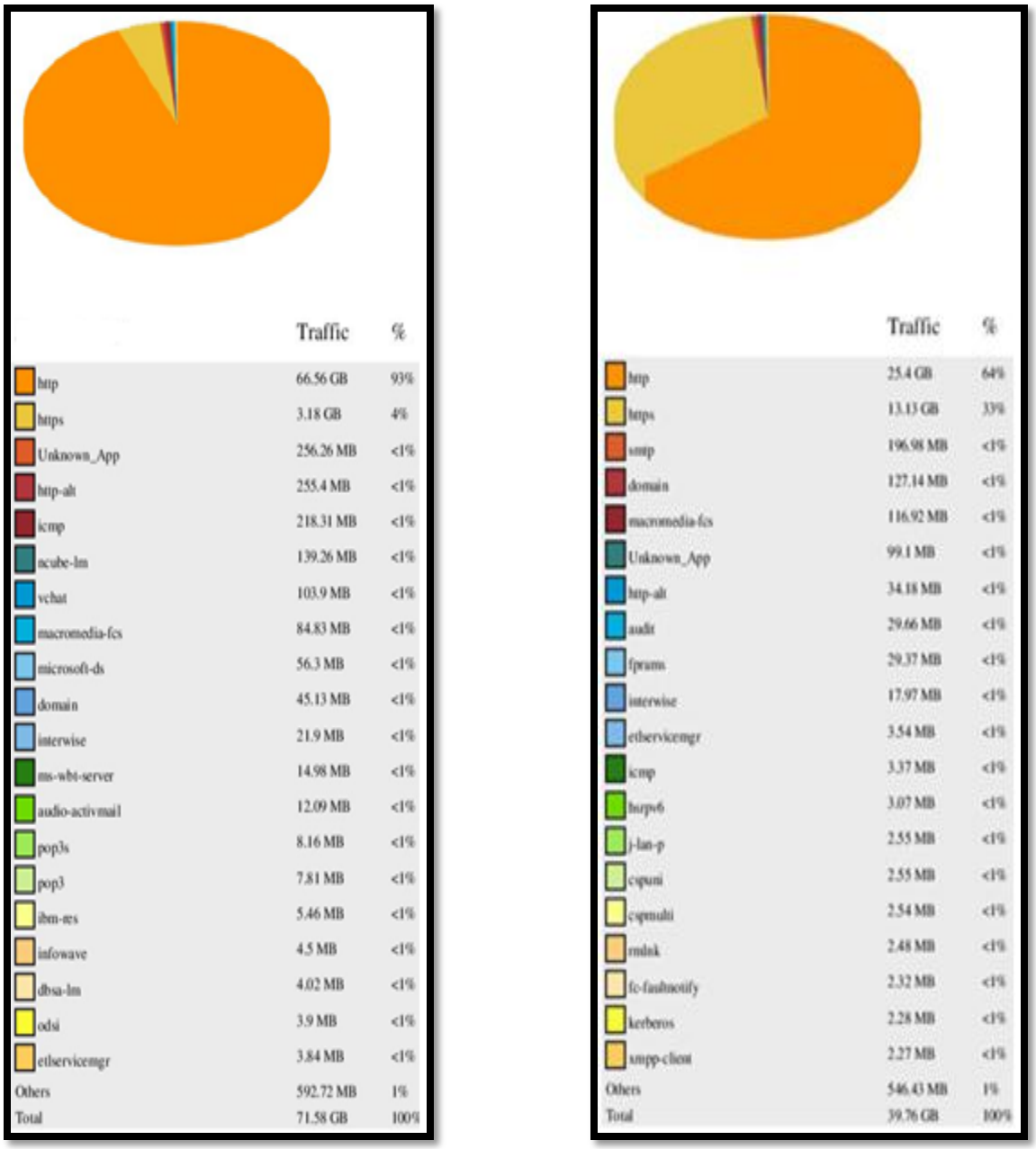
This may due to nature of ENM, branches networks have local database that could be accessed only during working hours and from internal network, other branches networks, and DMZ network. They cannot be accessed via public network such as Internet. Moreover Internet is used only during working hours (8:00 am to 3:00 pm).

Figure 4.4(c) shows traffic usage in a branch network during one week, which is connected to the EN through VPN over SHDSL(WAN service. Inbound bandwidth represents uploaded traffic which is generated when users upload files/folders from the branch network to DMZ network, another branch network, local services network, and public network (Internet). Outbound bandwidth represents downloaded traffic which is generated when users download files/folders from DMZ network, another branch network, local services network, and public network (Internet) to the branch network.

The maximum inbound traffic used by the branch network is about 2.6364 Mbps (0.3%), while the maximum outbound traffic is about 2.4219 Mbps (0.2%). Also it can be shown from Figure 4.4(c), the average inbound traffic used by the branch network is about 0.2751 Mbps (less than 1%), while the average outbound traffic is about 0.2559 Mbps (less than 1%). We observe that the traffic used by the branch network is nearly the same for most work days of the week. It is observed that inbound traffic used by the branch network is limited only to working days, specifically between 8:00 am and 3:00 pm. As we see there is no traffic in vacation days (which are Saturday and Friday-day 13 and 14) and in duration between 3:00 pm and 8:00 am. Some of the branches networks get down after 3:00 pm, which results in absence of traffic between 3:00 pm and 8:00 am. It is possible for other branches networks to work after 3:00 pm, this depends on the nature of services provided by the branch network.

We need additional traffic analysis to understand user usage of applications/protocols and discovering its traffic usage. For this purpose, we use NetFlow traffic analyzer.

Figure 4.5 shows the percentage of traffic usage by different applications/protocols. The Figure investigates traffic usage of inbound applications/protocols from: public network (Internet), branches networks, and a specific branch network.



| | Traffic | % |
|---|---|---|
| http | 66.56 GB | 93% |
| https | 3.18 GB | 4% |
| Unknown_App | 256.26 MB | <1% |
| http-alt | 255.4 MB | <1% |
| icmp | 218.31 MB | <1% |
| ncube-lm | 139.26 MB | <1% |
| vchat | 103.9 MB | <1% |
| macromedia-fcs | 84.83 MB | <1% |
| microsoft-ds | 56.3 MB | <1% |
| domain | 45.13 MB | <1% |
| interwise | 21.9 MB | <1% |
| ms-wbt-server | 14.98 MB | <1% |
| audio-activmail | 12.09 MB | <1% |
| pop3s | 8.16 MB | <1% |
| pop3 | 7.81 MB | <1% |
| ibm-res | 5.46 MB | <1% |
| infowave | 4.5 MB | <1% |
| dbsa-lm | 4.02 MB | <1% |
| odsi | 3.9 MB | <1% |
| etservicemgr | 3.84 MB | <1% |
| Others | 592.72 MB | 1% |
| Total | 71.58 GB | 100% |

| | Traffic | % |
|---|---|---|
| http | 25.4 GB | 64% |
| https | 13.13 GB | 33% |
| smtp | 196.98 MB | <1% |
| domain | 127.14 MB | <1% |
| macromedia-fcs | 116.92 MB | <1% |
| Unknown_App | 99.1 MB | <1% |
| http-alt | 34.18 MB | <1% |
| audit | 29.66 MB | <1% |
| fpnms | 20.37 MB | <1% |
| interwise | 17.97 MB | <1% |
| etservicemgr | 3.54 MB | <1% |
| icmp | 3.37 MB | <1% |
| hsrpv6 | 3.07 MB | <1% |
| j-lan-p | 2.55 MB | <1% |
| cspuni | 2.55 MB | <1% |
| cspmulti | 2.54 MB | <1% |
| rmlnk | 2.48 MB | <1% |
| fc-fauthnotify | 2.32 MB | <1% |
| kerberos | 2.28 MB | <1% |
| xmpp-client | 2.27 MB | <1% |
| Others | 546.43 MB | 1% |
| Total | 39.76 GB | 100% |

Figure 4.5: Percentage of traffic usage cont. (a) Percentage of traffic usage by applications/protocols in EN. (b) Percentage of traffic usage by applications/protocols in branches networks.


Figure 4.5: Percentage of traffic usage. (c) Percentage of traffic usage of applications/protocols in one branch network.

Figure 4.5(a) shows the percentage of traffic usage by applications/protocols of public network (Internet) by internal network and/or DMZ network. HTTP applications/protocols occupy the most percentage of the total traffic, it is about 93% of the traffic. HTTP traffic is access by users through web browser applications such as Internet Explorer, Mozilla Firefox, and others. HTTPS application/protocol is considered to be the second one to consume traffic with about 4% of the total traffic. HTTPS traffic is a secure HTTP traffic, it signals the browser to use added encryption layer of SSL/TLS to protect HTTP traffic. It is clear that users in the EN access few secure website when compare with unsecure websites (which use HTTTP protocol).

Hint: For more detail about HTTP/HTTPS please refer to section 3.1.

Other applications/protocols consume less than 1% of the total traffic, These applications/protocols are:

- Mail services (use SMTP, POP3).
- Windows authentication (use Kerberos).
- Network troubleshooting and management (use SNMP and ICMP).
- Domain services (use Domain, LDAP, and Microsoft-ds).
- Video Conferencing application (use vchat).
- Macromedia application (use macromedia-fcs).

Figure 4.5(b) shows the percentage of traffic usage by applications/protocols from branches network to public network (Internet) and/or DMZ network. HTTP applications/protocols occupy the most percentage of the total traffic, it is about 64% of the traffic. Users in the branches networks use HTTP protocol to reach public network such as Internet. HTTPS application/protocol is considered to be the second one to consume traffic with about 33% of the total traffic. We observe that HTTPS traffic is fairly large. Branches networks access web-based application that are hosted in the EN data center. All web-based applications use HTTPS protocol for security issue. Other applications/protocols (as we stated previously) consume less than 1% of the total traffic.
Figure 4.5(c) shows the percentage of traffic usage by applications/protocols from one branch network to public network (Internet) and/or DMZ network. HTTP applications/protocols occupy the most percentage of the total traffic, it is about 74% of the traffic. Users in the branches networks use HTTP protocol to reach public network such as Internet. HTTPS applications/protocols are considered to be the second one to consume traffic with about 5% of the total traffic. The Branch network accesses web-based application via HTTPS protocol which are hosted in the EN data center. Domain services occupy about 2% of the total traffic, they are used by domain controller for domain management. We have 2% of traffic consumed by Oracle applications, it uses ncube-lm-licenser manager- at port 1521.Oracle applications need connection to Oracle databases that are hosted in local services network. Custom applications are denoted by others in Figure 4.5(c), these applications use a user-defined ports. They are programmed

and developed by programmers of enterprise network, they consume less than 1% of the total traffic.

## 4.4 Deep Analysis Of HTTP/HTTPS Traffic

In this section, we will discover applications that use HTTP/HTTPS protocol. According to our previous network traffic analysis, we observed that HTTP and HTTPS are the dominant traffic of the total traffic. We will perform a deep inspection of HTTP/HTTPS traffic, so we get deep understand about the nature of this traffic. Many applications use HTTP/HTTPS Protocols, we should distinct between legal application and illegal one. Understanding HTTP/HTTPS traffic provides the basic step to classify applications which are used in EN. Once we classify our applications, we can rank theses application according to its importance and its need for security. Deep analysis of HTTP/HTTPS traffic will help us to develop an security-enhanced model of our EN.

There are many tools used to inspect HTTP/HTTPS traffic deeply. Fiddler2 tool is a powerful HTTP/HTTPS traffic inspector, it is a free tool.Fiddler2 tool provides the following features [52]:capture all HTTP/HTTPS traffic, deep dive into session metrics, filter captured traffic, archive and playback recorded traffic.

We do HTTP/HTTPS traffic analysis during one week through a full-time work days, we started analysis from 7/9/2013 to 14/9/2013. Full-time work begins on Sunday at 8:00 am and ends on Thursday at 3:00 pm, Saturday and Friday are weekly vacation days.

Figure 4.6 shows result summarization after running Fiddler2 for IN/OUT traffic of enterprise network.

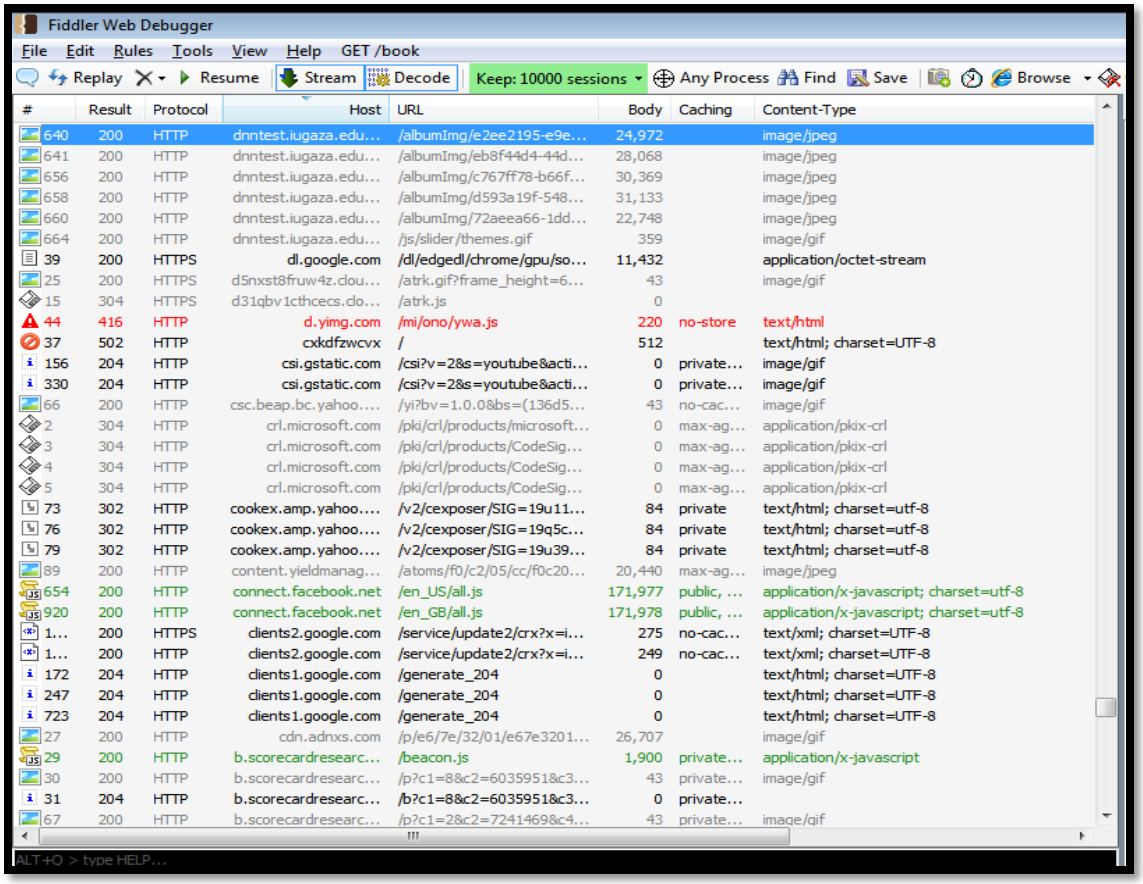



Figure 4.6: Results summarization after running Fiddler2 for IN/OUT traffic of Enterprise Network EN.

Figure 4.6 provides a clear view about the nature of HTTP/HTTPS traffic, we can detect applications that use HTTP/HTTPS protocol. The Figure lists file types which are send/received using HTTP/HTTPS traffic. Every row in the figure represents HTTP or HTTPS session, which can be used for more details. For each session we can fetch the following information:

- Protocol type (HTTP or HTTPS)
- Web server name which host the HTTP/HTTPS webpage..
- URL-Uniform Resource Location which represents the web address.
- Body size in bytes.
- Content type such as XML, JPEG, JavaScript, HTML, and others.

By referring to Figure 4.6, we do deep investigation on HTTP/HTTPS sessions. The main sources of these sessions are studied carefully, we list the most prominent sources as the following:

- Web sites browsing: there are many request/response HTTP headers that contain URLs of different web pages. They are hosted in Internet such as www.facebook.com, www.yahoo.com, and others.
- Web services hosted in enterprise network: HTTP traffic contains requests to web services hosted in EN, web services include:
    - E-login use HTTPS protocol.
    - Most of administrative transactions such as secretary, archiving, employment, vacations, etc.
    - Most of finance transactions such as salaries, payment, accounting, etc.
- Some websites of EN use digital certificate for authentication, they use HTTP over SSL (HTTPS) protocol.
- Meeting and training use IP-based applications such as Skype which uses HTTP traffic.
- Software updates are done via Internet; they use HTTP/HTTPS traffic. Updates are done for IOS, operating systems, antivirus programs, and other software.
- Also e-mail service uses HTTP/HTTPS traffic, since e-mail service is a web-based application access via local area network and Internet.
- Management devices such as IP power devices uses HTTP traffic.
- Network devices configurations use HTTP/HTTPS traffic, for example wireless access points, Cisco routers/switches all are configured using HTTP/HTTPS traffic via LAN or Internet.

## 4.5 Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

Intrusion Detection Systems IDS and Intrusion Prevention Systems IPS are available as hardware devices and software applications. There are many vendors who offer hardware IDS/IPS solution such as Cisco and Juniper, while software IDS/IPS systems are available as open source and commercial software. The use of IDS/IPS systems is different according to its placement and its implementation, IDS/IPS systems can be used to protect both the whole enterprise network and/or individual hosts. Network IDS/IPS systems are used to protect enterprise network while Host IDS/IPS systems are used to protect individual hosts. In our security-enhanced model, we will use both network IDS/IPS and host IDS/IPS systems. Network IDS will be used to monitor and analysis real time traffic of DMZ network, internal network, and external network, also we will use network IPS to protect the DMZ and internal networks from potential intrusions coming from external network. On the other hand, Host IDS/IPS will be used to monitor and prevent malicious traffic that aims to infect and penetrate servers, personal computers, switches, and routers. Intrusion prevention system (IPS) is known as intrusion detection and prevention system (IDPS), we will refer to network IDS/IPS as IDPS. We will use IDPS in our enterprise network as in-line, it will monitor and analysis real time traffic. IDPS detects malicious and anomaly traffic (potential intrusions), logs malicious behavior, blocks malicious traffic , and generates report about malicious traffic. We want to prevent intrusions from compromise integrity, confidentiality or availability of our enterprise network and its hosted services. According to our previous traffic analysis of our enterprise network, we observed that most traffic is represented by HTTP/HTTPS applications/protocols. IDPS can inspect layer 7 applications/protocols like HTTP, FTP, and SMTP. Once IDPS detects intrusion, it will apply corresponding actions that we previously defined. IDPS has different response, it may drop packets, correct CRC, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options. Even IDPS provides additional security layer to our enterprise network, we cannot use it alone. We will use firewall beside IDPS system to provide defense in depth strategy for our enterprise network. NIDS never replace firewall device, encryption, and other authentication methods. NIPS systems use different

detection methods , the most commonly used are signature-based and statistical anomaly-based. In signature-based mode, NIPS will monitor traffic passed through it, it will compare captured traffic against predefine signatures. NIPS maintains an updated database of signatures, when captures traffic match one of these signatures, the corresponding rule set will be applied. Rule sets can drop, block, or terminate TCP connection. Signature-based mode cannot detect zero-day attaches, since its signatures are not yet available. On the other hand, statistical anomaly-based will monitor behavior of traffic, it will classify traffic into normal and abnormal one. Normal traffic is defined using baseline which identify used protocols, used ports, used applications, and normal bandwidth usage. NIPS will send an alarm to the administrator when captured traffic contains abnormal behaviors that differs from the baseline.

## 4.6 Advanced Persistent Threat (APT)

APT will be introduced in this section, we will see its purpose and motivation. We will explain operation aurora, as APT-based attack in section 4.6.1.

APT is a network attack that intend to compromise enterprise network in order to get unauthorized access to network resources. APT is done by well trained attackers, they are supported by organizations, governments and states. APT attackers have a specific mission to achieve, they aim to steal data of enterprise network. APT attacks are produces against organization and big company such as Google, Yahoo, and others. It is a cyber attack that need foundation and support for completing its planned missions. Even we have NIDS system in enterprise network, it is still difficult to detect these APT attacks without additional devices and tools. APT uses social engineering tries to avoid detection by NIDS, it seems as legitimate activity to NIDS. Once APT attack gets access to victim host in enterprise network, it will immediately establish a backdoor hole. APT attacker hope to get more access to other hosts in enterprise network by moving from the compromised host to other through establishing more backdoors for future access.

### 4.6.1 Operation Aurora

Operation Aurora represents one of APT based attacks against enterprise network. It compromises the software-configuration management (SCM) systems that held

proprietary information of big companies such as Google, Adobe and others. Figure 4.7 shows steps that aurora attack follows in order to compromise a victim host [16]. As APT attack, operation aurora uses social engineering to gain access to victim host. When victim host receives an email, it seems as normal one. In fact this email contains a URL of malicious code such as JavaScript, attacker tries to exploit an Internet Explorer vulnerability . Each time the victim access Internet Explorer, it will access memory and hence triggers exploit. Aurora attack tries to download more malicious codes to victim host, which will enforce victim host to establish an encryption SSL connection to attacker network. Bu inducing a backdoor connection to victim host, attacker tries to compromise other hosts in order to steal sensitive information of enterprise network. Aurora attack uses RAR files to obscure the removal of data in enterprise network, it uses FTP to transfer RAR files to outside enterprise network. It will be impossible to detect Aurora attack without predefined signatures or rule sets.

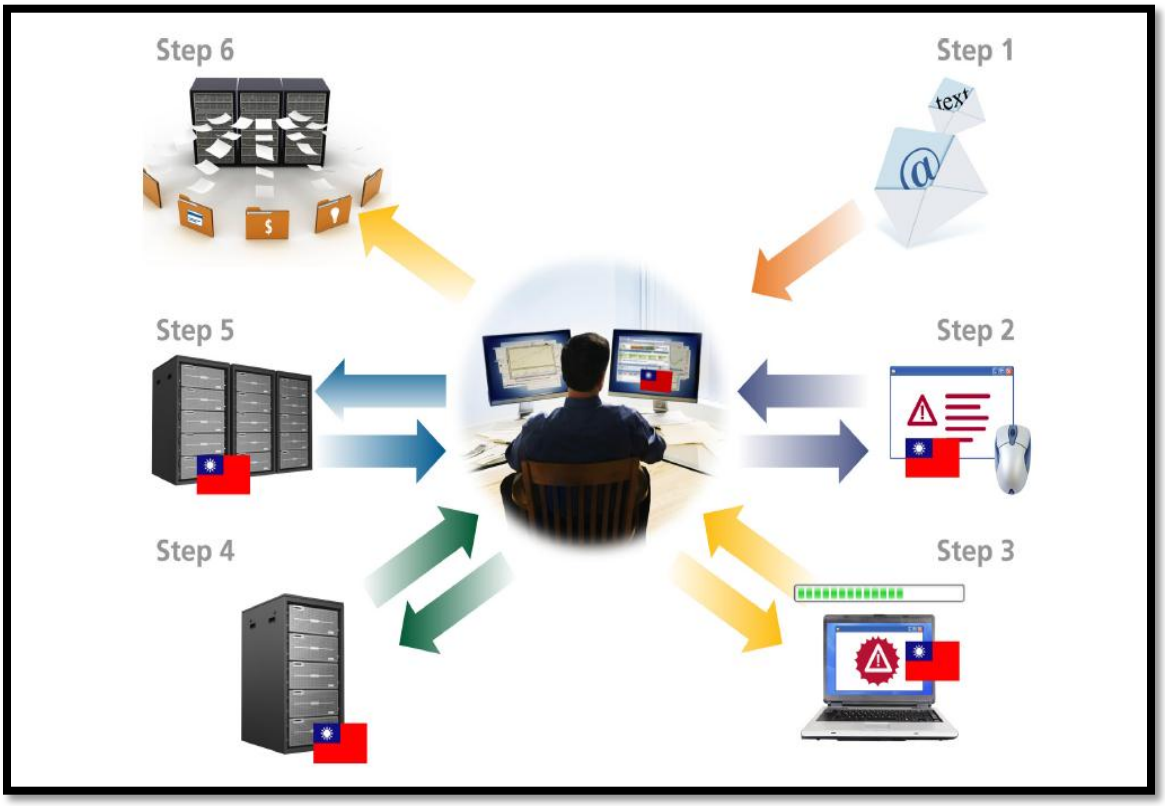



Figure 4.7: Steps of Aurora attack.

## 4.7 Aurora Attack Prevention Using Our Proposed Security-Enhanced Model

At this time, our proposed model can detect and prevent different number of attacks. We use SNORT as NIDS/NIPS with updated rule sets to detect intrusions and attacks, also we use OSSEC as HIPS to protect severs of enterprise network. Also we use Splunk as monitoring and logging server to track and monitor malicious activity, it collects logs from SNORT and OSSEC. What about APT-based attacks? how we can detect them? In the previous section, we describe Aurora attack as APT based-attack, the next step is how we will prevent this attack. In this section, we will modify SNORT configuration to detect and prevent Aurora attack. Aurora attack uses social engineering to compromise victim host by using false email to track victim. Social engineering uses phishing campaigns to get sensitive information such as user traditional, passwords, and other related data. We block phishing campaigns by using rule sets of phishing-spam. rules, which are created by the Sourcefire Vulnerability Research Team (VRT) . We enable these rules in blocking mode in order to detect phishing campaigns. Please refer to appendix B for more detail about phishing-spam. rules. Prevention phishing campaigns is not sufficient, we need to continue in monitoring malicious behavior using Splunk tool. Once we detect anomaly activity, it must be prevented using SNORT NIPS/NIDS and OSSEC HIPS.

We have to do modification to SNORT configuration in order to be able to detect Aurora attack. The default configuration of SNORT ignore encrypted traffic due to performance issues and reduce false positive. SNORT has SSL/TLS preprocessor, which is known as SSL Dynamic Preprocessor (SSLPP) . SSLPP can decode SSL and TLS traffic. As we explained in section 3.1, HTTPS traffic uses SSL to secure HTTP traffic, it uses SSL over port 443. The default configuration of SNORT inspect only SSL handshake of each HTTPS connection, it does not inspect encrypted payload of the traffic.

In our model, we use SNORT to inspect only HTTPS traffic, we will ignore other traffic such as FTPS, POPS, and SMTPS. According to previous traffic analysis, the most usage traffic are HTTP and HTTPS..

We modify snort.conf file which is the configuration file of SNORT. We add the following SSL/TLS preprocessor to snort.conf file and enable it to inspect only HTTPS traffic:

Enable HTTPS inspections/decoding on port 443

preprocessor ssl: ports { 443 }

We have two rule options which are ssl_version and ssl_state. ssl_version determines version negotiated between the endpoints of the SSL encryption, while ssl_state tracks the state of the SSL encryption during the process of hello and key exchange. We have the following SSL version: sslv2, sslv3, tls1.0, tls1.1, and tls1.2. Also we have the following SSL state: client_hello, server_hello, client_keyx, and unknown.

We track all SSL versions and states by adding the following to preprocessor ssl:

version = "sslv2" | "sslv3" | "tls1.0" | "tls1.1" | "tls1.2"

state = "client_hello" | "server_hello" | "client_keyx" | "server_keyx" | "unknown"

In order to detect aurora attack, we use the followingSNORT signature[16].

1. `alert tcp $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ET TROJAN Aurora C&CCheckin"; flow:established,to_server; content:"|fffffffffff 00 00 feffffffffffffffff 88 ff|"; offset:0; depth:20; classtype:trojan-activity; reference:url,www.avertlabs.com/research/blog/index.php/2010/01/18/an-insight-into-the-aurora communication-protocol/; sid:10000000001; rev:1;)`
2. `alert $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ET TROJAN Aurora C&C CheckinResponse"; flow:established,to_server; content:"|cc cccccc cd cc cccc cd cc ccccccccccc|"; offset:0; depth:16; classtype:trojan-activity; reference:url, www.avertlabs.com/research/blog/index.php/2010/01/18/an-insight-into-the-aurora communication-protocol/; sid:10000000002; rev:1;)`

McAfee observed that backdoor is always sending the following 20 bytes to a command and control (C&C) server.

content:"|ffffffffffff 00 00 feffffffffffffffff 88 ff|"

We also use an additional SNORT rule set to detect RAR files leaving the network, Aurora attack uses RAR file to hide data theft.

The Emerging Threats group published a useful signatures for detecting RAR files leaving the network as the following:

- `alert tcpDMZ_Network any ->Public_Network any (msg:"ET POLICY RAR File Outbound"; flow: established; content:"|52 61 72 21|"; offset: 0; depth: 4; tag: session; classtype: not-suspicious; sid: 2001950; rev:3;)`

We implement previous signatures on eachSNORT NIDS of enterprise network.

## 4.8 Summary

In this chapter, we did network traffic analysis using different tools such as NetFlow, MRTG, Fiddler 2 to inspect traffic of enterprise network. We used NetFlow as network traffic analysis tool, while MRTG as bandwidth usage analysis tool . HTTPS traffic is analyzed using Fiddler 2 tool, it can inspect encrypted HTTP traffic. It is clear that HTTP/HTTPS represents the most used traffic in enterprise network due to incremental use of web-based applications and Internet. Bandwidth usage is different according to inbound and outbound access, it is consumed at different levels through working day. Also in this chapter, we propose a security-enhanced model of enterprise model, the proposed model uses different software tools and hardware. W used opens source SNORT as network intrusion detection and prevention system, while OSSEC as host intrusion prevention system. We used hardware firewall to filter inbound and outbound traffic passing through enterprise network. Also we used Splunk as central monitoring tool with high integration with SNORT and OSSEC. We also modified configuration of several software tools and hardware such as SNORT, OSSEC, Slunk, layer 3 switch, and

firewall. We added new signatures and rules to SNORT to detect and prevent APT-based attack such as Aurora attack. The proposed model suggests an efficient way to handle APT-based attack with minimum performance effect.

# CHAPTER 5: Implementation and Evaluation

The main purpose of this chapter is to implement our proposed security-enhanced model of enterprise network, implementation will be done using different devices and tools. In section 5.1, we will describe devices and tools that will be used in our implementation and performance evaluation. In section 5.2, we will see SNORT implementation as network intrusion detection system, OSSEC as host intrusion prevention system, and Slunk as logging and monitoring system. Latter in section 5.3, we will use Metasploit framework as penetrating test tool to evaluate our proposed model in detection Aurora attack. Finally, we will use bandwidth utilization as a metric to evaluate the overall performance of our proposed model.

## 5.1 Devices And Tools

In order to implement and evaluate performance of our proposed model, we need a number of devices and tools. To implement our proposed model, we use four servers and one firewall with NIPS module. There are different vendors who provide firewall device with NIPS module. FortiGate is one of them, it provides FortiGate-3140B firewall with NIPS module[55]. Implementing NIDS using SNORT requires two dictated servers, SRV-SNORT-DMZ is used for monitoring DMZ network while SRV-SNORT-Internal is used for monitoring internal network. The other two servers SRV-OSSEC, and SRV-SPLUNK are used to implement OSSEC server and Splunk server respectively. We install CentOS 6.3 [56]as operating system on all servers that we used in implementing our proposed model. CentOS (Community Enterprise Operating System ) is an open source operating system, it is an Enterprise-class Linux Distribution. It is full binary compatibility with its upstream source, Red Hat Enterprise Linux (RHEL).We use a personal computer PC1-OSSECwith OSSEC agent installed in order to assess performance impact of OSSEC on enterprise network. On the other hand, we use personal computer PC2to evaluate performance impact of SNORT on enterprise network, it has no OSSEC agent installed. OSSEC agent is an open source software that is used to monitor individual hosts, it establishes a connection with OSSEC manger for monitoring

hosts with OSSEC agent.PC1- OSSEC and PC2 both have Windows 7 as operating system in 64 bit.

We use Metasploit framework to evaluate capability of our proposed model in detection Aurora attack. Metasploitis a free open source penetrating test tool which is used to discover security vulnerability on enterprise network. It can be used to launch attacks and malicious codes to assess network security, it enable us to scan open ports on network devices. We use a personal computer PC3-Metasploit with MetasploitPRO version 4.7 installed.

FreeMeter tool is used to evaluate bandwidth utilization on PC1-OSSEC and PC2, it will help us to evaluate overall performance of proposed model. FreeMeter is free tool designed for Windows operating system, It is a graphic tool that shows upload and download activities in real time. Table 1 lists details of devices and tools that we used in our model for both implementation and evaluation.

Table 5.1: Description of devices and tools used in implementation and evaluation.

<table>
<tr><th>Device Name</th><th>Specification</th><th>Operating System</th><th>Installed Tools</th></tr>
<tr><td>PC1- OSSEC</td><td rowspan="3">• CPU: Core i5, 1.8 GHz<br>• RAM: 6GB</td><td rowspan="2">Windows 7 OS 64bit</td><td>• FreeMeter<br>• OSSEC Agent</td></tr>
<tr><td>PC2</td><td>• FreeMeter</td></tr>
<tr><td>PC3-Metasploit</td><td>CentOS 6.3</td><td>Metasploit PRO 4.7</td></tr>
<tr><td>SRV-SNORT-DMZ</td><td rowspan="2">Dell PowerEdge 2950 Server<br>• CPU: Intel Xeon 5300 Sequence: Dual Independent 1066MHz;<br>• RAM: 32GB</td><td rowspan="2">CentOS 6.3</td><td rowspan="2">SNORT 2.9.5.5</td></tr>
<tr><td>SRV-SNORT-Internal</td></tr>
<tr><td>SRV-OSSEC</td><td rowspan="2">Dell OptiPlex 755<br>• CPU: Core i5, 1.8 GHz<br>• RAM: 6GB</td><td rowspan="2">CentOS 6.3</td><td>OSSEC-hids-2.7.1</td></tr>
<tr><td>SRV-SPLUNK</td><td>Splunk-6.0</td></tr>
<tr><td>Firewall</td><td>FortiGate-3140B firewall with NIPS</td><td>FortiGate</td><td>FortiGate-3140B</td></tr>
</table>

## 5.2Implementation

### 5.2.1 Implementing Firewall With Integrated IPS

As we mention in chapter 4, we use a hardware firewall with integrated IPS module in our proposed model, it is FortiGate-3140B firewall.FortiGate-3140B provides up to 58 Gigabits per second (Gbps) firewall throughput, it includes integrated IPS, application control, user-based policies, and endpoint policy enforcement.

Figure 5.1 shows the IPS page of FortiGate-3140B, it includes the recent updates of IPS signatures. Also we observe the existence of Aurora.Backdoor.CC signature, it is used to detect and prevent Aurora attack. As it appears, firewall classifies Aurora attack as high severity, it targets server host that has Windows as operating system. The default action for firewall is to block Aurora attack once it detected.

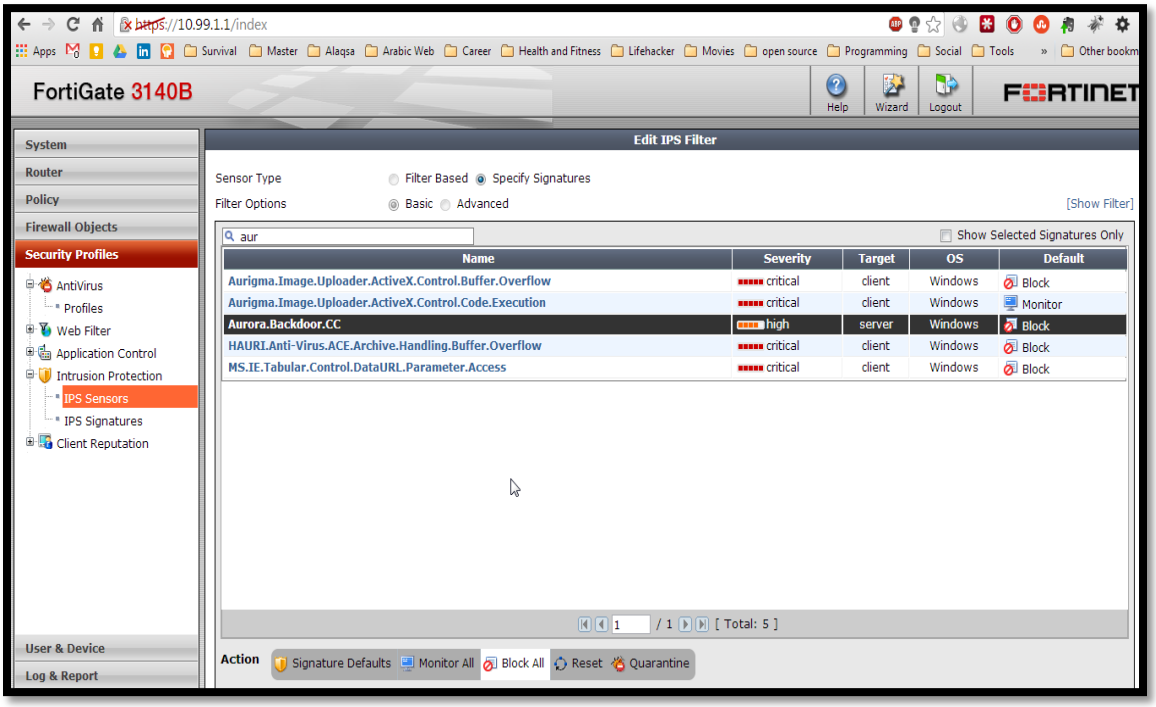



Figure 5.1: IPS Filter page of firewall FortiGate-3140B.

Since Aurora attack uses HTTPS reveres connection, It is important to enable SSL inspection specially for HTTPS traffic. In Figure 5.2, we enable HTTPS, FTPS, SMTPS, POP3S, and IMAPS inspection. For aurora attack detection, it is sufficient to enable just

HTTPS inspection. HTTPS inspection allows firewall to do deep filtering on encrypted HTTP traffic, and hence detects attack that uses HTTPS traffic.

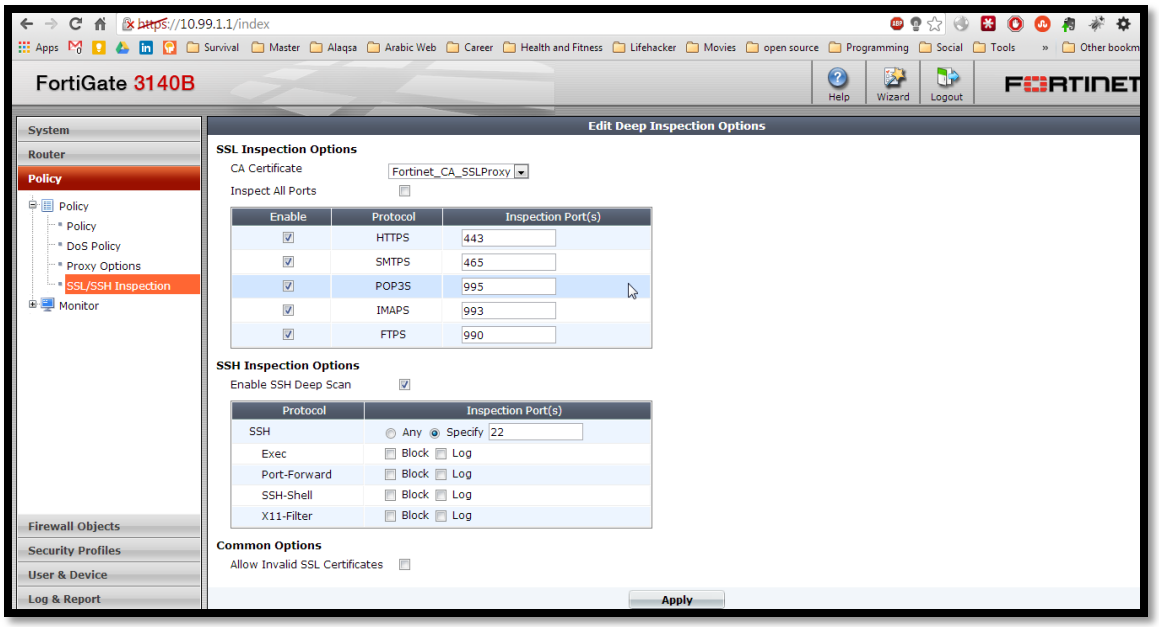



Figure 5.2: SSL inspection enabling on FortiGate-3140B.

## 5.2.2Implementing SNORT As Network Intrusion Detection System (NIDS)

In our security-enhanced model, we use SNORT as network intrusion detection system. SNORT is an open source tool with free source code, it is used as network intrusion prevention system (NIPS) and network intrusion detection system (NIDS).

We use SNORT to perform a real time traffic analysis and packet logging on enterprise network. SNORT provides multiple function, it can do protocol analysis, content searching, and content matching. Here we will give a detail view about how SNORT do its job as NIDS, SNORT architecture [57]is composed of five component as shown in Figure 5.3.

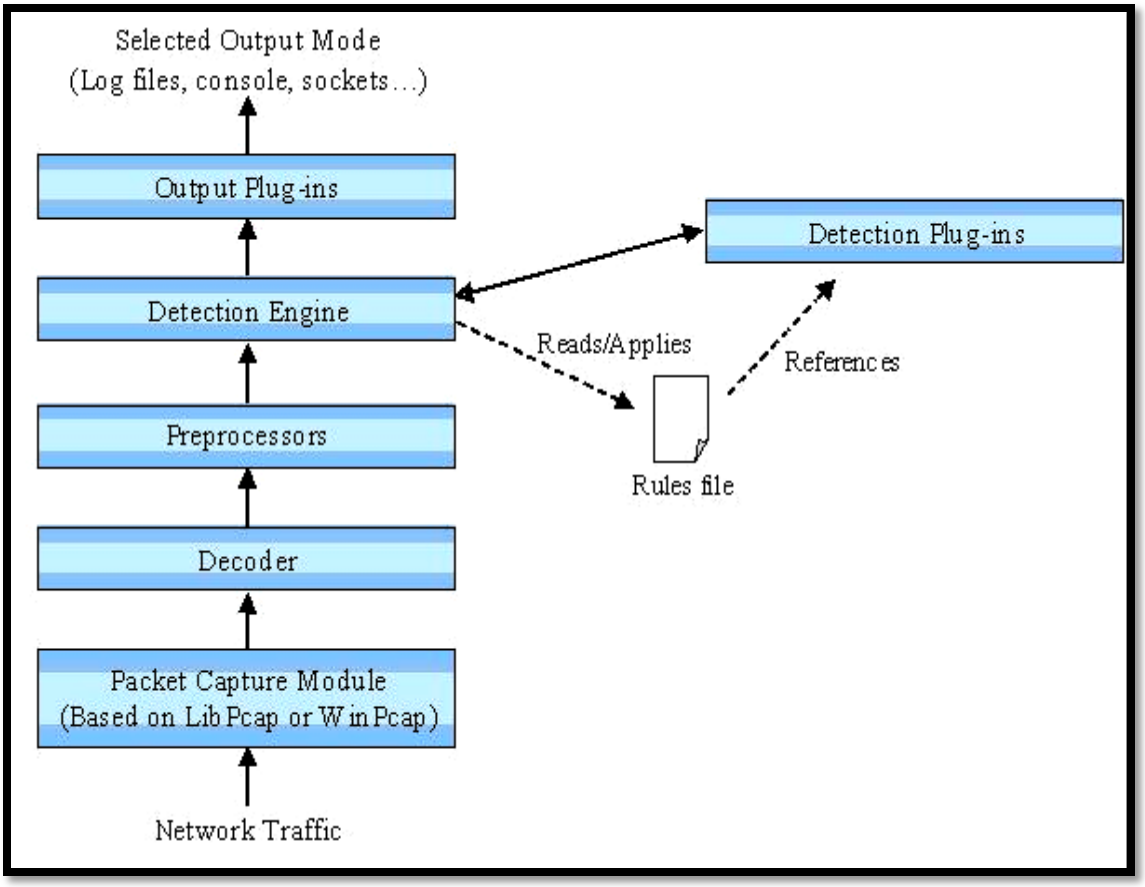



Figure 5.3: Internal Scheme of an SNORT intrusion detection system.

**Packet Decoder**: It captures network packets that pass through the SNORT, it collects these packets from different network interface cards. Packet decoder saves packets for future processing.

**Preprocessors:** They are used with SNORT to modify captured packets before sending them to detection engine. It takes the captured data packets and check them against sets of plug-ins such as RPC plug-in, HTTP plug-in, and port scanner plug-in. SNORT uses the plug-ins to check the contents of captured data packets for specific behavior. we can enable or disable these plug-ins according to our need.

**Detection Engine**: This is the most important component of SNORT, it applies the rule sets (signatures) on the captured packets. It will detect anomaly behavior according to its rule sets, rule sets or signatures are usually associated with a specific action. Sourcefire Vulnerability Research Team™ (VRT) Rules are the official rules of Snort. Each rule is developed and tested using the same rigorous standards the VRT uses for Sourcefire

customers. Rule sets or simply signatures are presented in three different way, Predefined signatures, SourceFire VDB signatures, and user-defined. Predefined and SourceFire VDB signatures are available when installing SNORT, they can be updated online via Internet, while user-defined signatures are written by security administrators.

**Logging and Alerting System**: The response of NIDS depends on the detection engine, it may produce alarms , send E-mail messages to administrator, and log entries of anomaly activity.

**Output Modules**: It defines the location to be used for storing the output of logging and alerting system of SNORT. We can store alerts on /var/log/snort/alerts file or some other file, also we can send messages to Syslog facility and Logging file to a database like MySQL or Oracle.

Figure 5.4 shows the base_main page of SNORT, it gives statistics about number of source IPs, destinations IPs, source ports, destination ports, number of unique alerts, total number of alerts, and many other statistics. As we can see, SNORT classifies traffic according to used protocols, TCP represents 83% of the total traffic, while UDP represents 17% of traffic. These percentage are expected, our previous traffic analysis shows that HTTP/HTTPS protocols/applications are the most frequent used traffic. It is known that HTTP/HTTPS protocols/ applications use TCP protocol.

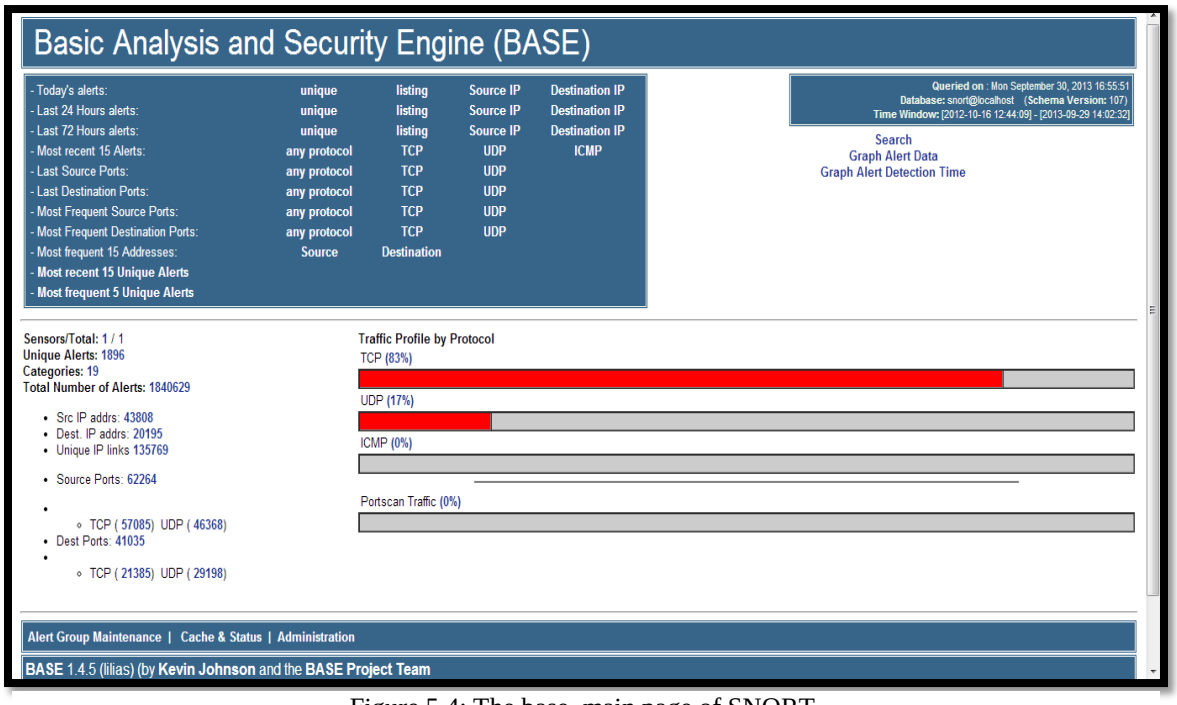


Figure 5.4: The base_main page of SNORT.

Figure 5.5 shows the last fifteen alerts that are generated by SNORT. SNORT filter each packet against predefined signature, it generate alerts when the corresponding signature fires. The alerts include name of signature, timestamp, source IP address, destination IP address, source port, destination port, and layer 4 protocol.

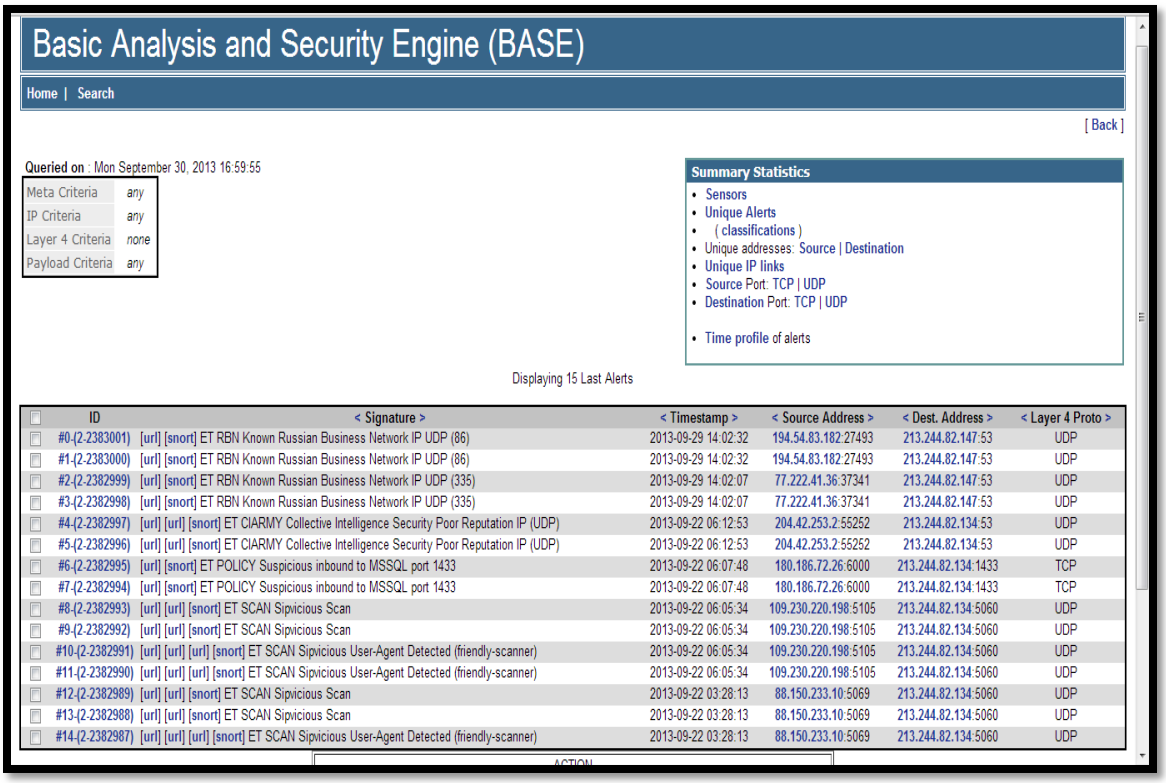



Figure 5.5: Last fifteen alert generated by SNORT.

Figure 5.6 shows the most frequent source IP addresses that are filtered by SNORT. The total number of most frequent source IP address is shown in the Figure as well as unique number of alerts for each source IP address. The Figure also displays the number of destination IP address that corresponding to each frequent source IP address.

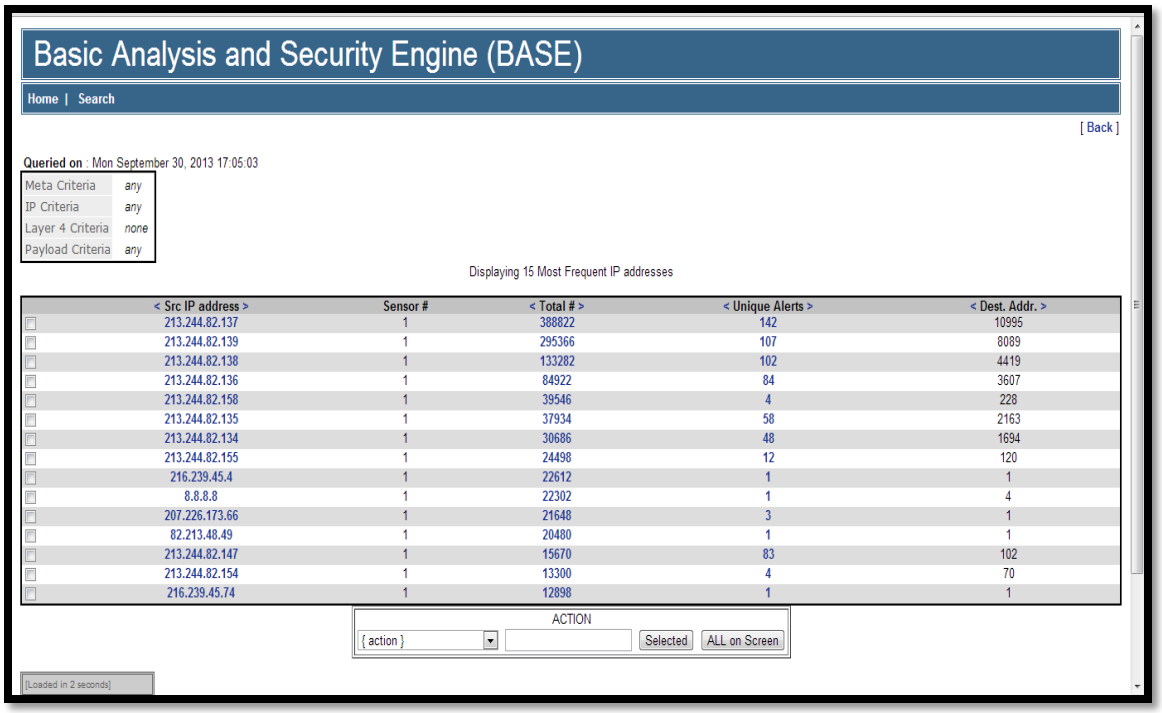



Figure 5.6: Most frequent source IP addresses filtered by SNORT.

### 5.2.3Implementing OSSEC As Host Intrusions Prevention System (HIPS)

There are many open source HIPS tool such as OSSEC, Samhain, and others, We use OSSEC as HIPS in our proposed model. OSSEC provides two working model which are local and client/server. Local model is used to monitor only one host while client/server model is used to monitor more clients using one server in centralized manner. We prefer OSSEC as HIPS for a lot of reasons, it has the ability to inspect encrypted protocols such as HTTPS traffic. OSSEC is a powerful correlation and analysis engine, it integrates log analysis and does file integrity checking. Moreover we can use OSSEC to monitor Windows registry, detect Rootkit using host-based anomaly detection and provide centralized policy enforcement.

AS HIPS system, OSSEC is composed of three components, each of them works together in order to detect intrusions. The main components of OSSEC HIPS are:

**Manager:** This is the central unit of OSSEC, it is really a manager. It simplifies management of OSSEC agents which make administration interesting and centralized. Also OSSEC managers store the following:

- File integrity checking databases for Unix and Windows

- Alerting when there is registry change for Windows OS.
- Logs
- Events
- System auditing entries

**Agents**: Are servers and hosts in enterprise network that we wish to monitor. Results of monitoring are transferred to mangers for analysis and events correlation. We install agent on each server in enterprise network in order to monitor its behavior and prevent potential intrusions. please refers to section 4.6 for more detail about OSSEC agents.

Figure 5.7 shows the architecture of OSSEC [58]. OSSEC agents like Linux OS, Windows OS, and even virtual machine send their events and logs to OSSEC manger that takes responsibility of analysis logs and correlate events for intrusion detection. Once intrusion is detected, OSSEC with active response will fire against intrusion in order to block, drop, and send alarm to administrators.

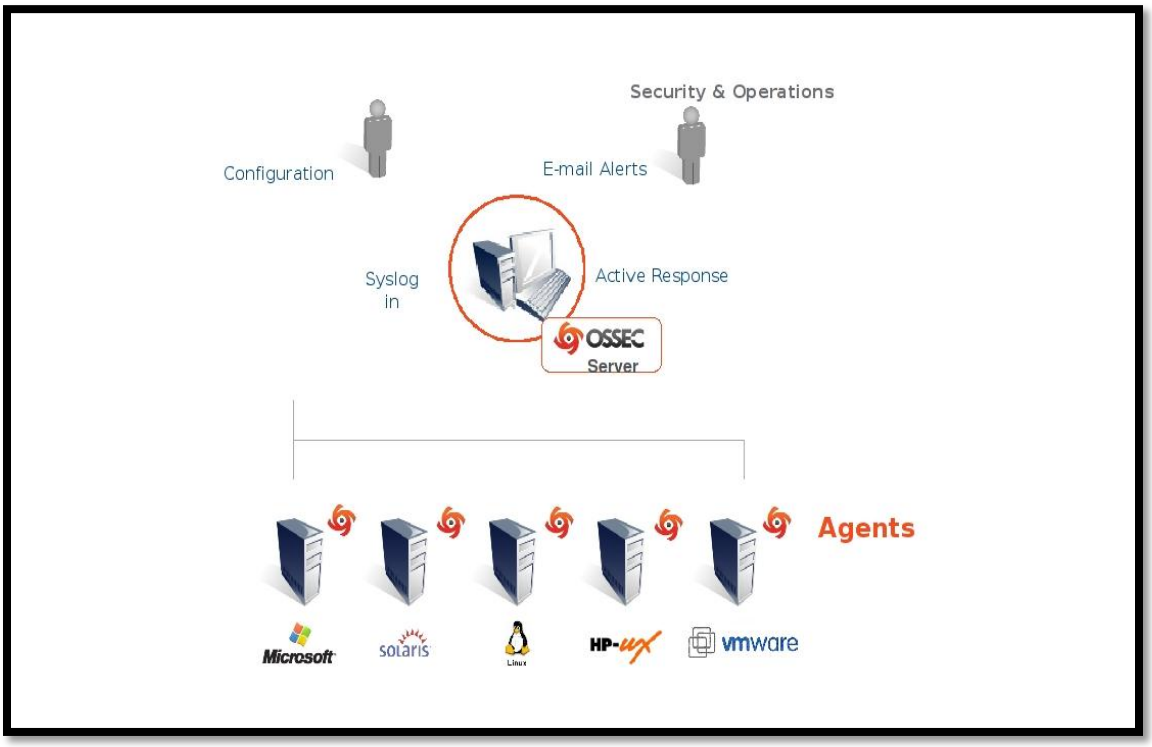



Figure 5.7: OSSEC architecture.

In our proposed model, we use OSSEC server with iptables service (Linux firewall) to implement and build host-based intrusion prevention system. In this case OSSEC will act

as HIDS, when OSSEC HIPS detects intrusion we will place the IP address into the iptables for a period of time. When no more scan activity is present the iptables will drop the IP address from the table.

Figure 5.8 shows the main page of OSSEC, it displays OSSEC agents that are added to OSSEC sever. We have two OSSEC agents which are OSSEC server known as local host and another server known as SRV_agent. Each agent includes IP address, name, last keep alive, and operating system type. The main page shows the latest events associated with OSSEC sever as well as the latest modified files.

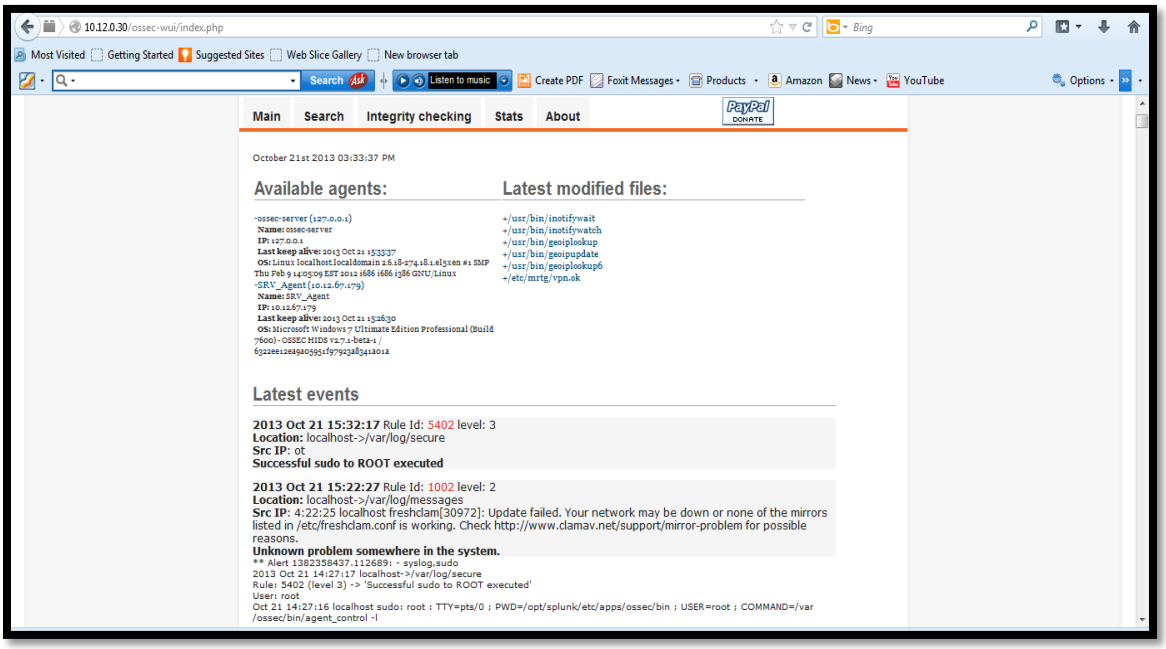



Figure 5. 8: Main page of OSSEC server.

Figure 5.9 shows the steps to add new agent to OSSEC server, we use the following command: //var/ossec/bin/manage_agents to add a new OSSEC agent. To add new OSSEC agent, we need to provide its IP address, name, and ID.

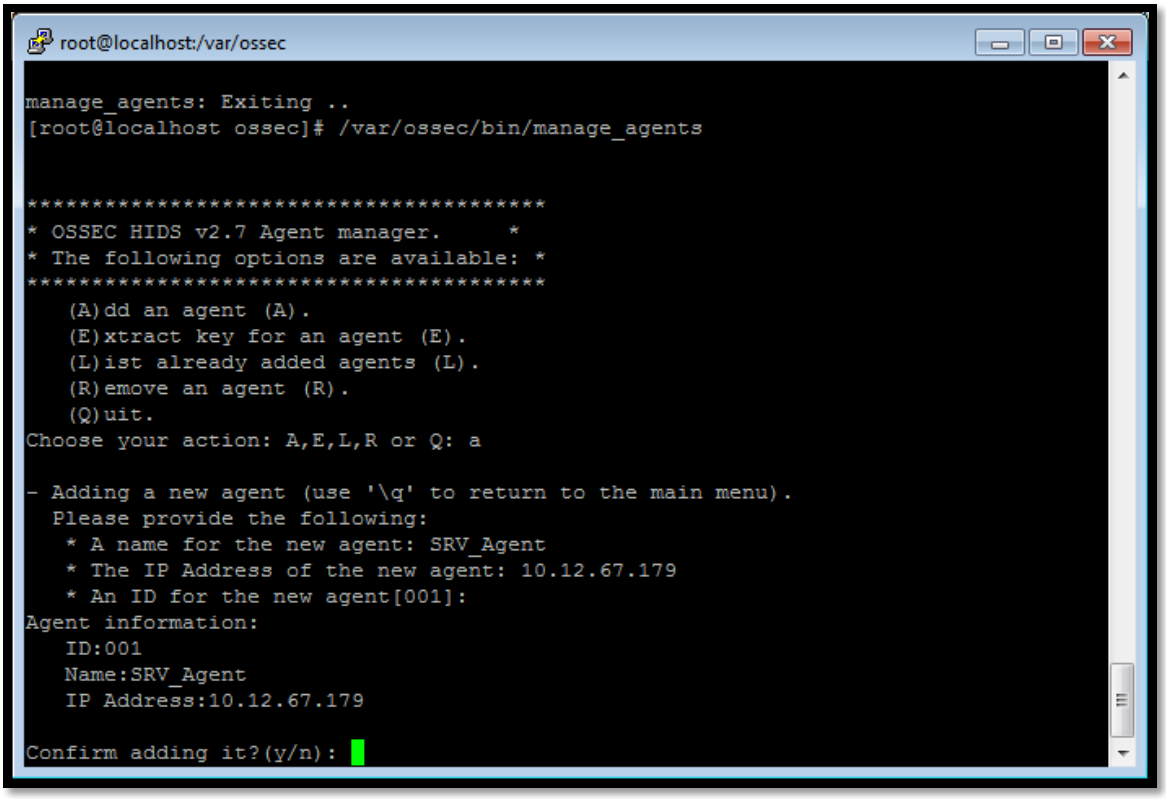



Figure 5.9: Steps to add new OSSEC agent.

Figure 5.10 shows the agent key information for OSSEC agent SRV_agent which has ID number 001. We use this key on SRV_agent host to connect with OSSEC server, it is used to authenticate agent to OSSEC server.

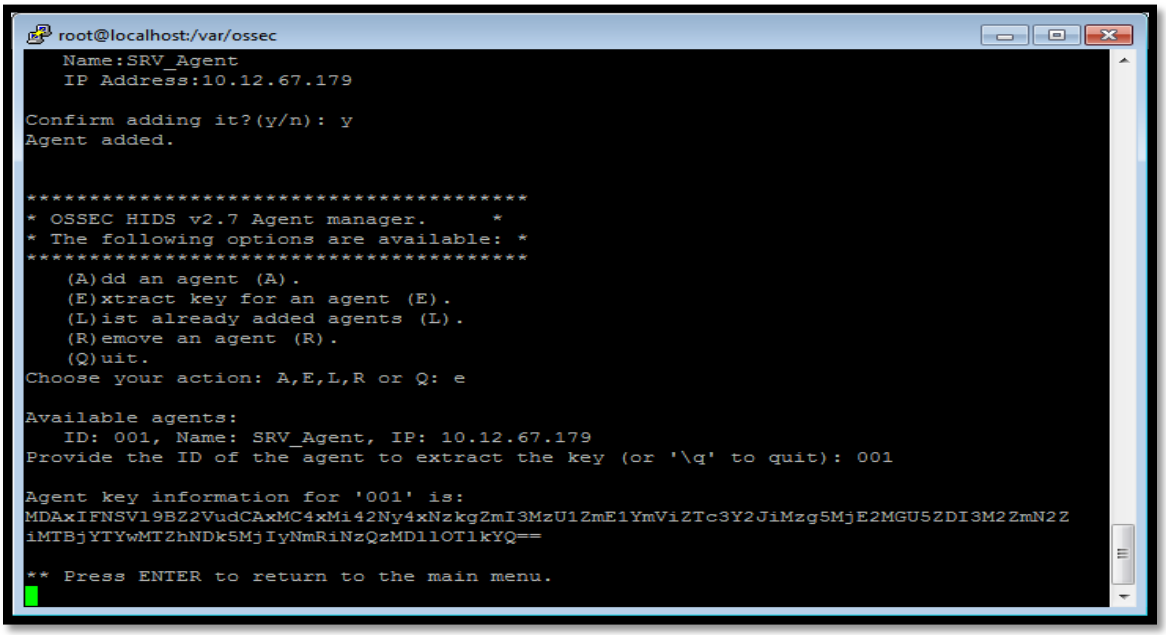



Figure 5.10: Agent key information for SRV_agent.

Figure 5.11 shows interface of OSSEC agent, we need to install OSSEC agent on SRV_agent to enable host intrusion prevention system. We have to fill both IP address and agent key for each OSSEC agent, where IP address is the OSSEC server. Once we start OSSEC agent, it will be connected to OSSEC server.

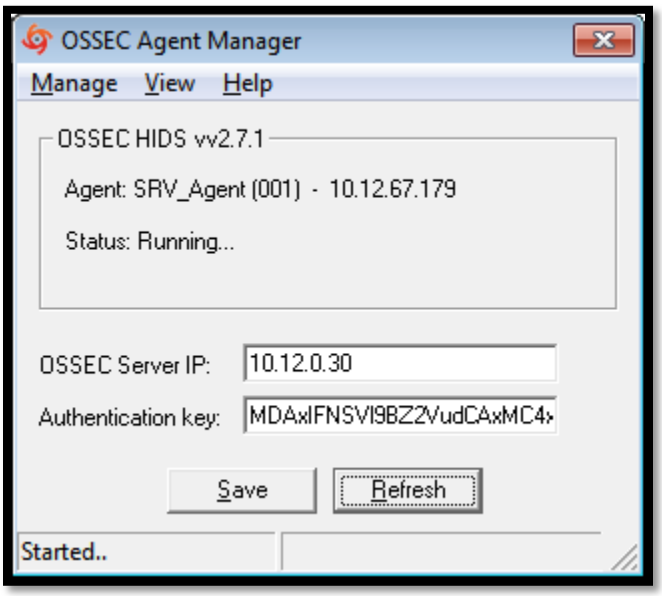



Figure 5.11: OSSEC agent manager.

Figure 5.12 shows log file of OSSEC agent, it contains log about host activity, windows registry, and other related information.

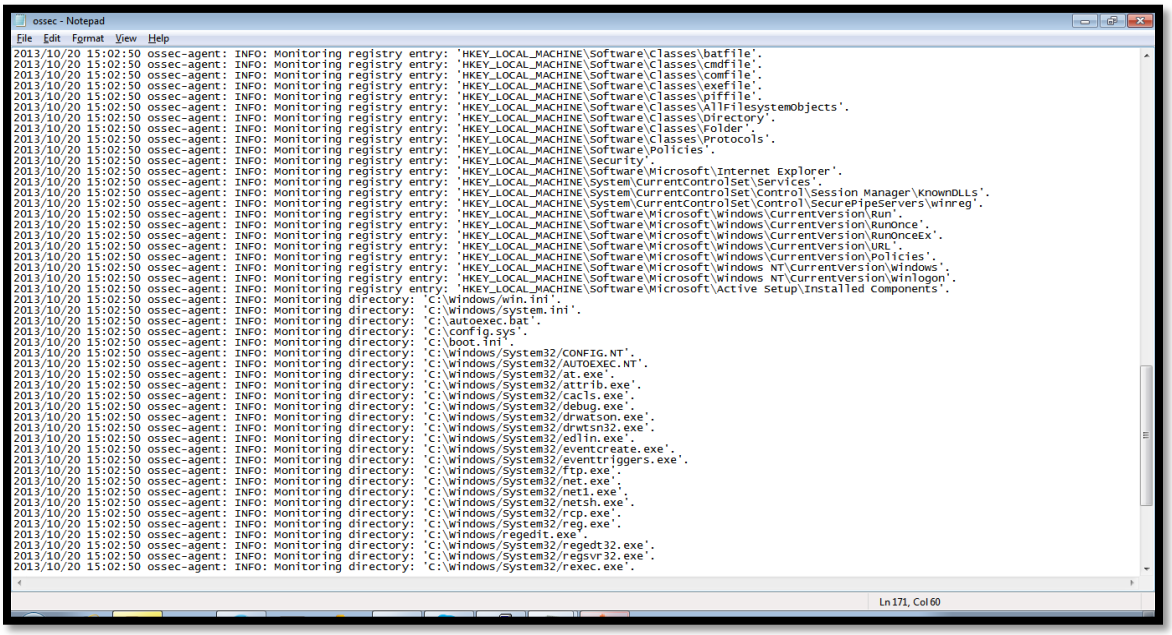



Figure 5.12: Log file of SRV_agent.

### 5.2.4 Implementing Splunk As Log Manager And Analyzer

There are several reporting, monitoring, and logging tools, which can be used to read SNORT log analysis. Some of these tools are commercial such as SourceFire, and Aanval, while others such as Sguil and Splunk are free and open source tools. We use free tools in our implementation of security-enhanced model of enterprise network. Splunk is an open free tool that can be integrated with both SNORT NIDS and OSSEC HIPS. When integrated with SNORT, Splunk provides field extractions for SNORT alert logs, dashboards, graphs, event types, tags, correlates real-time data, and reports. Also we can integrate Splunk with OSSEC for better correlation of alerts generated by OSSEC. Splunk generates reports for future analysis and management, it simplifies logs reading by transforming them in a graphic format. Figure 5.13 shows integration of OSSEC with Splunk [59]. As we stated previously, OSSEC agents are managed by OSSEC manger, they are connected to OSSEC manger for detecting and preventing malicious activity. All logs are stored in OSSEC meager since it is the central management of HIPS system. OSSEC manger collects logs data and transfers a copy to Splunk server.

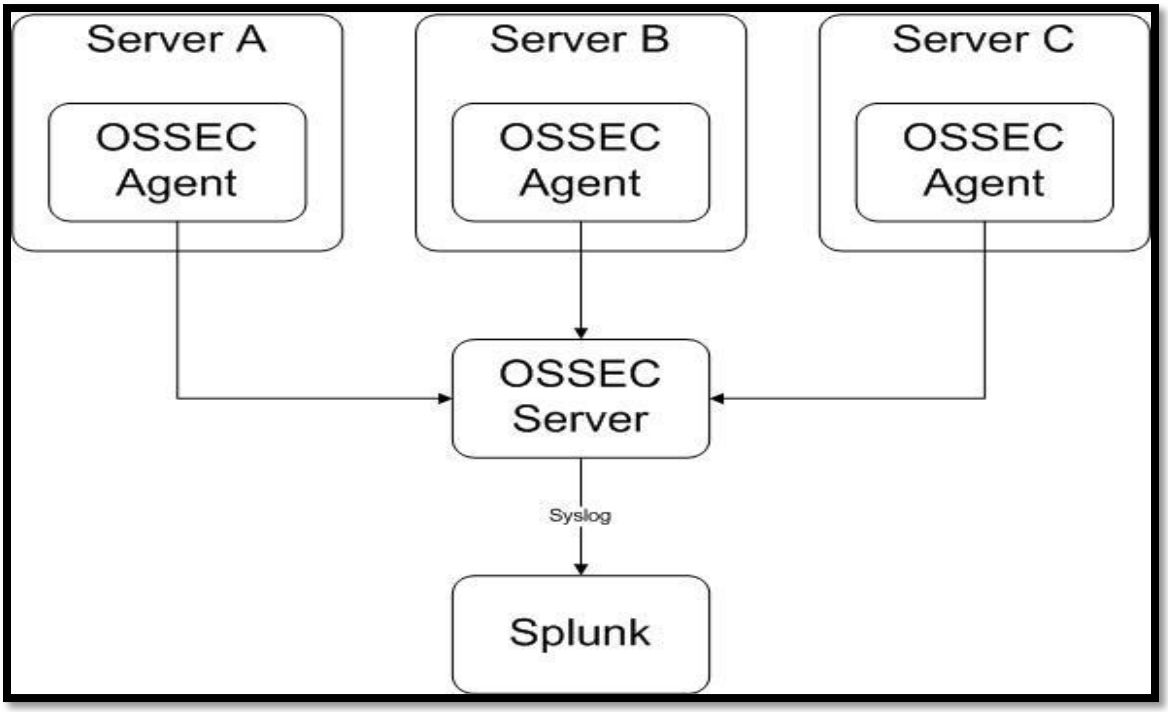



Figure 5.13: Splunk integration with OSSEC.

Figure 5.14shows the main page of Splunk tool, it contains three main sections which are Apps, Data, and Help. Apps section includes search, pivot, reports, alerts, and dashboard, while Data section provides adding and managing data. Help section provides additional tutorial about Splunk tool.

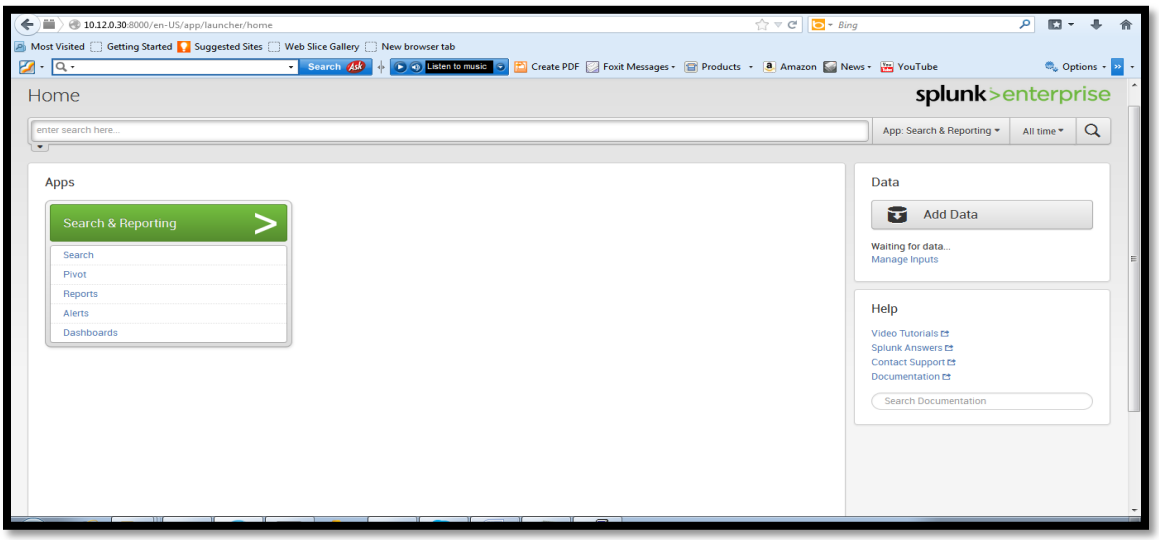



Figure 5.14: Main page of Splunk.

We do additional configuration to integrate OSSEC with Splunk, please refer to appendix C for more details about these configuration. Figure 5.15 shows the main page of Splunk after integrating Splunk for OSSEC.As we see, we have a new apps which is Splunk for OSSEC.

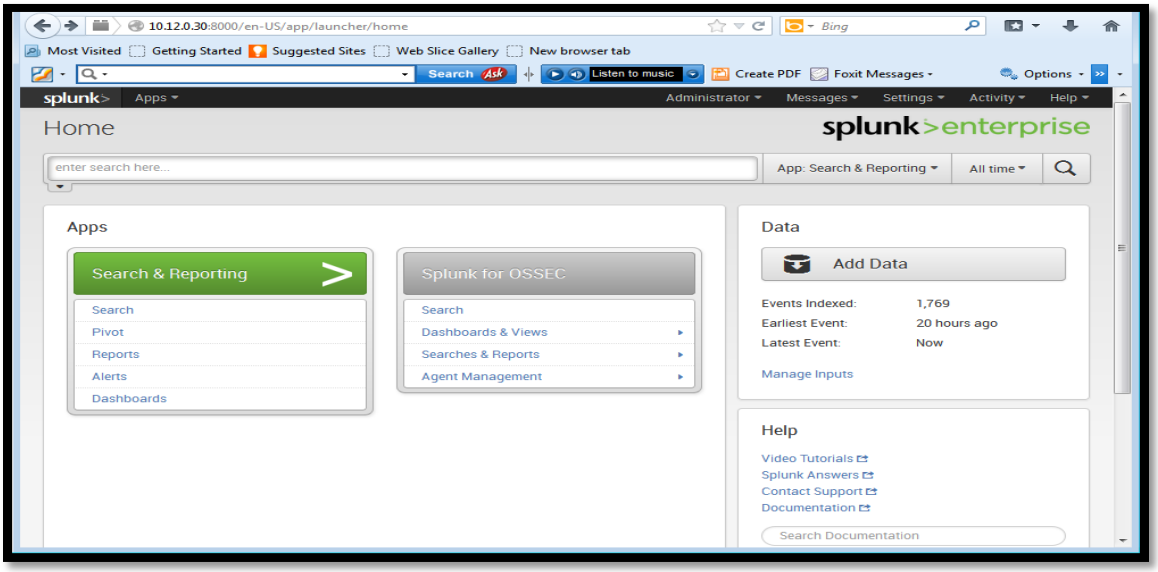



Figure 5.15: Splunk Integration with OSSEC.

Figure 5.16 shows the top signatures that fire over time period from 9 am to 10:30 am on OSSEC server. It can be seen that different signatures are fired such as login sessions open, OSSEC agent started, windows error events, windows login success, and others. Windows error event is the top signature that appears in OSSEC server. It appears between 9:20 am and 9:30 am.

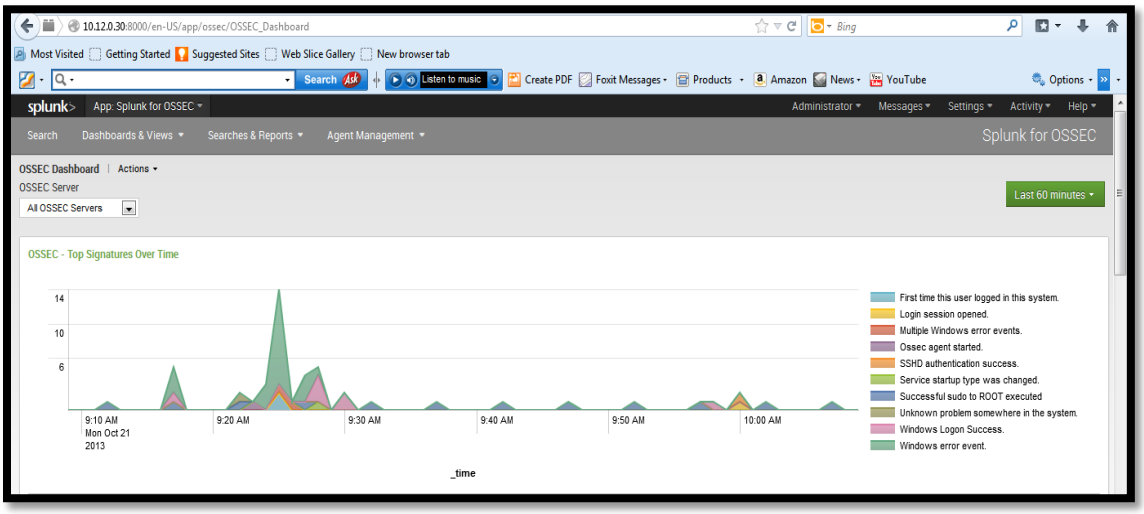



Figure 5.16: OSSEC top signatures.

Figure 5.17 shows the number of occurrence of top signatures between 9:00 am and 10:30 am.

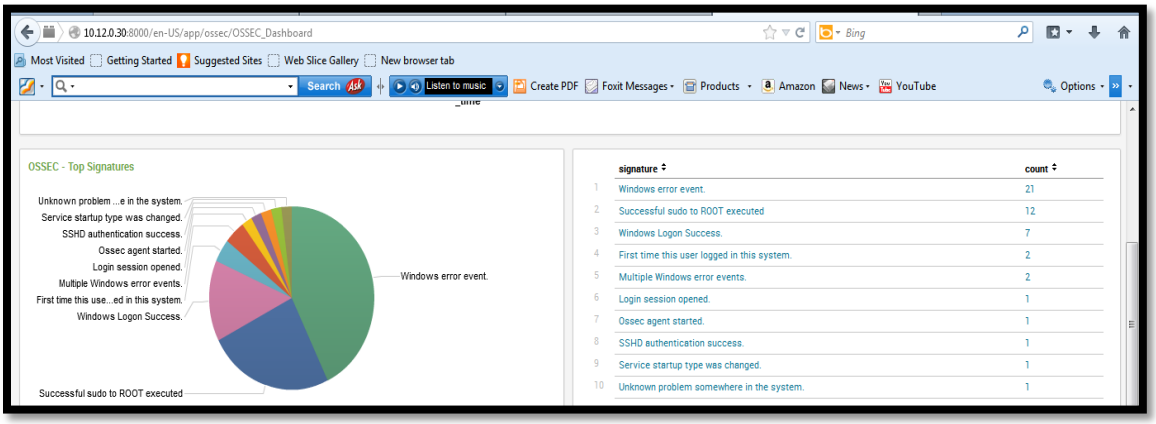



Figure 5.17: Number of occurrence of top signatures.

## 5.3 Evaluation

In this section, we evaluate both the defense and performance of our proposed security-enhanced model. For defense evaluation, we use Metasploit tool as penetrating test tool, while we use bandwidth utilization for performance evaluation.

### 5.3.1 Defense Evaluation

We use Metasploit framework to induce malicious codes and attacks to enterprise network, Figure 5.18 shows the launching process of malicious codes. Metasploit launches 688 different attacks in order to exploit security vulnerability of enterprise network, please see appendix D for more information about used attacks in defense evaluation. Our proposed model success in detection all of these attacks, we have recent update signatures for both firewall and SNORT NIDS.

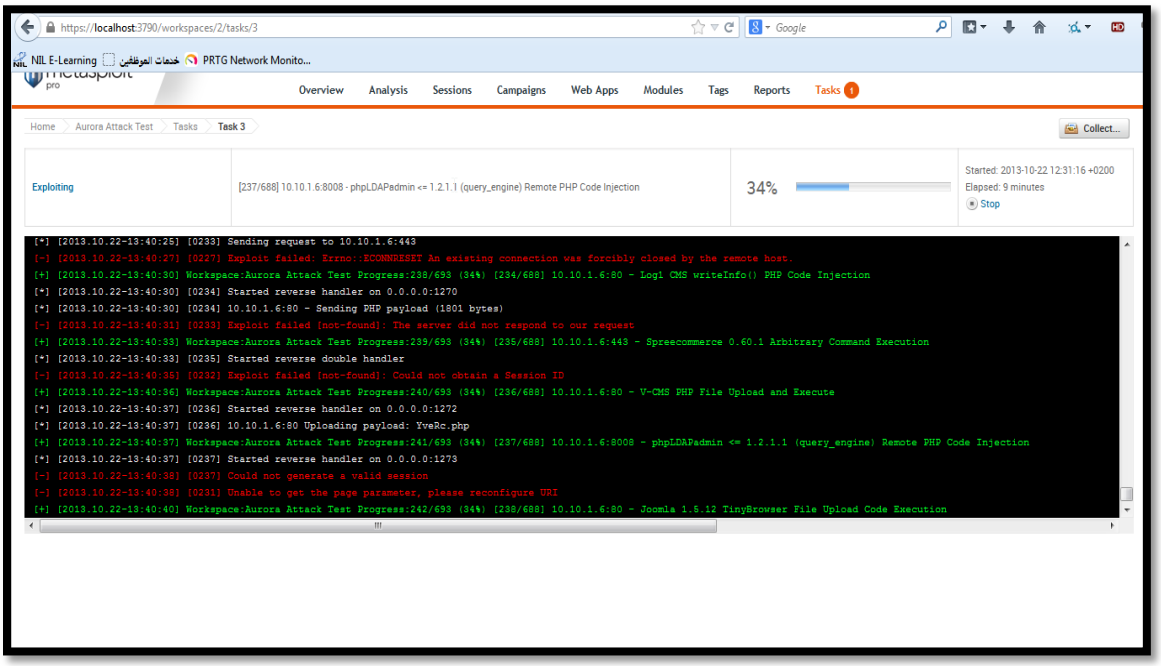



Figure 5.18: Launching malicious codes using Metasploit tool.

In order to evaluate detection of Aurora attack, we use Aurora Metasploit Module. We install this module on PC3 to launch aurora attack. Figure 5.19 shows the result of running the module, we use the resulted URL: https://10.99.1.2:8080/uH3JQkhD70c to launch Aurora attack. We access the previous URL on Internet Explorer to launch attack,

we intent to exploit vulnerability of Internet Explore. Since we have a firewall with NIPS module and SNORT NIDS, we need to do defense evaluating for both systems. The results were great, our proposed model detects Aurora attack. Firewall already has Aurora signature that fired once that attack is detected. SNORT NIDS uses rule sets that we defined in section 4.7 to detect Aurora attack as well new modification of HTTPS inspection.. SNORT logs the existence of Aurora attack, it sends an alert to administrator about attack detection.

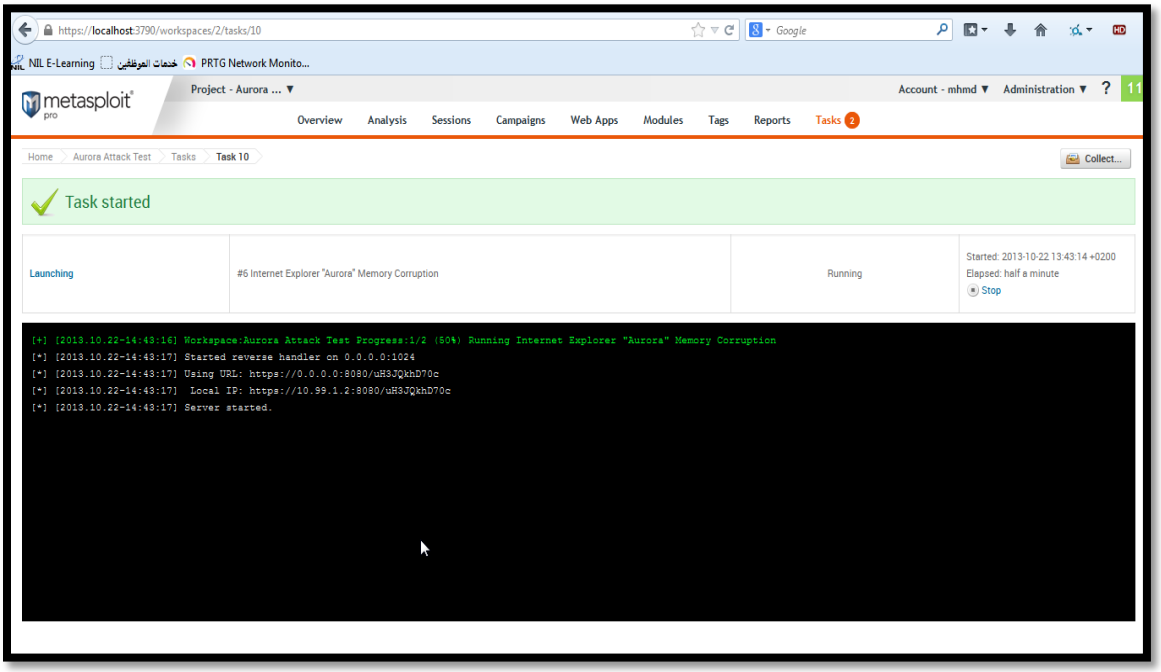



Figure 5.19: Launching Aurora attack using Metasploit tool.

### 5.3.2 Performance Evaluation

**Performance Evaluation Before Applying Our Proposed Model**

We use PC2 to evaluate bandwidth utilization before applying our proposed model, PC2 is connected directly to Internet service. It bypasses firewall and SNORT NIDS, It has no OSSEC agent.

Figure 5.20 shows the graph of bandwidth utilization of PC2, Y-axis represents time in seconds while X-axis represents bandwidth in Mega bits(Mb). We can observe that PC2 consumes bandwidth in different ways along time, but generally it consumes little bandwidth. There is no heavy consuming of bandwidth, it is restricted on users who access services in local area network LAN and Internet.

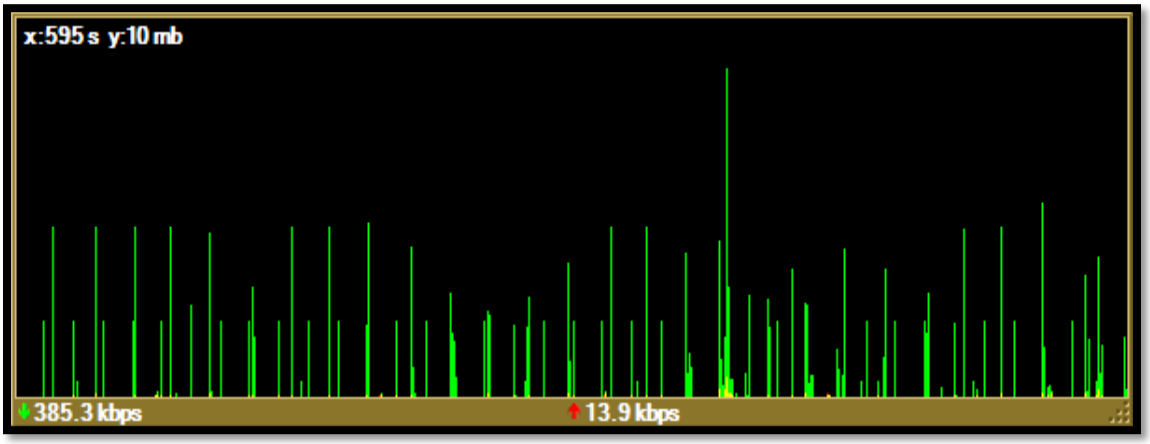



Figure 5.20: Bandwidth utilization before applying proposed model.

**Performance Evaluation Using Only Firewall**

Figure 5.21 shows bandwidth utilization using only firewall device. It is clear that firewall increases bandwidth consuming in a significant amount. Firewall filters each coming network packet against set of rules/signatures. Filtering needs extra bandwidth and hence it affects on network performance. Packets travel among different networks are filtered, firewall does deep inspection for SSL traffic. It does web content filtering at layer 7 of reference model IOS as well as for layer3,4, and 5.

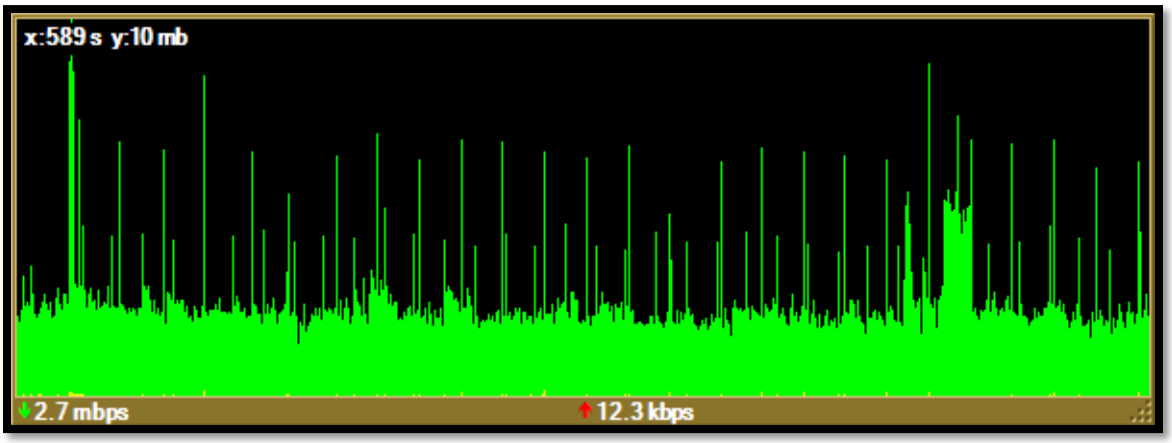



Figure 5.21: Bandwidth utilization using only firewall.

**Performance Evaluation Using Only SNORT NIDS And Firewall**

Figure 5.22 shows the graph of bandwidth utilization ofPC2. Even SNORT NIDS has so little effects on bandwidth consumption, firewall has more affects. When compared with

Figure 5.21, we conclude that firewall has the main performance impact on bandwidth consumption. SNORT NIDS has no observable effects, in our proposed model we use SNORT as NIDS. Network devices of enterprise network just send a copy of traffic to SNORT, it acts as a real time monitor.

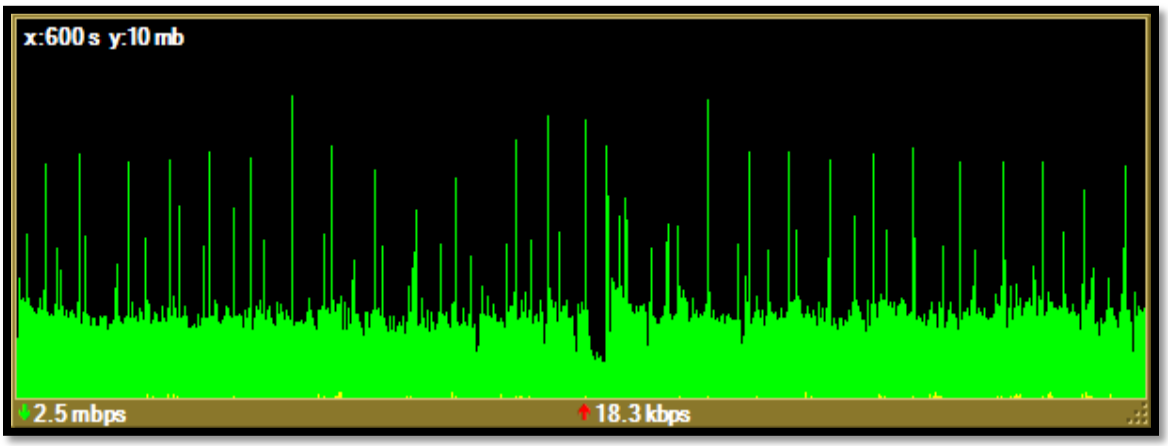



Figure 5.22: Bandwidth utilization using only SNORT NIDS and firewall.

**Performance Evaluation Using Only Firewall And OSSEC HIPS**

As we see in Figure 5.23, OSSEC has no observable effects on bandwidth utilization, it does not affects on network performance.

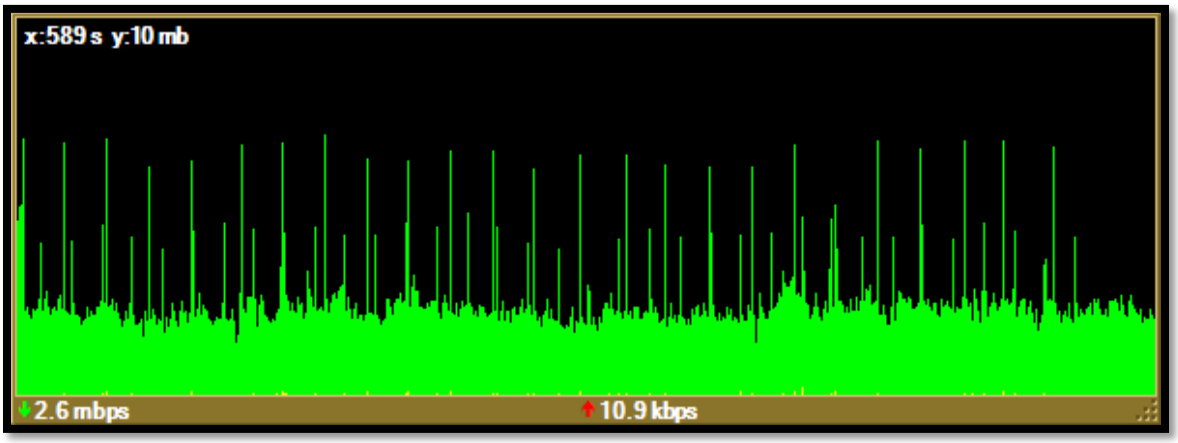



Figure 5.23: Bandwidth utilization using only firewall.

**Performance Evaluation Using Our Proposed Model**

Figure 5.24 shows the impact of applying our proposed security-enhance model on bandwidth utilization of enterprise network. Figure provides a graph of bandwidth utilization after implementing our proposed model, a quit few amount of bandwidth is

consumed. It is almost unnoticeable that OSSEC agent has effects on network bandwidth when compared with previous Figure 5.23. Firewall still has the most effects on network performance, we have to remember that firewall contains IPS module. OSSEC affects on CPU and RAM utilization rather than bandwidth utilization and hence network performance.

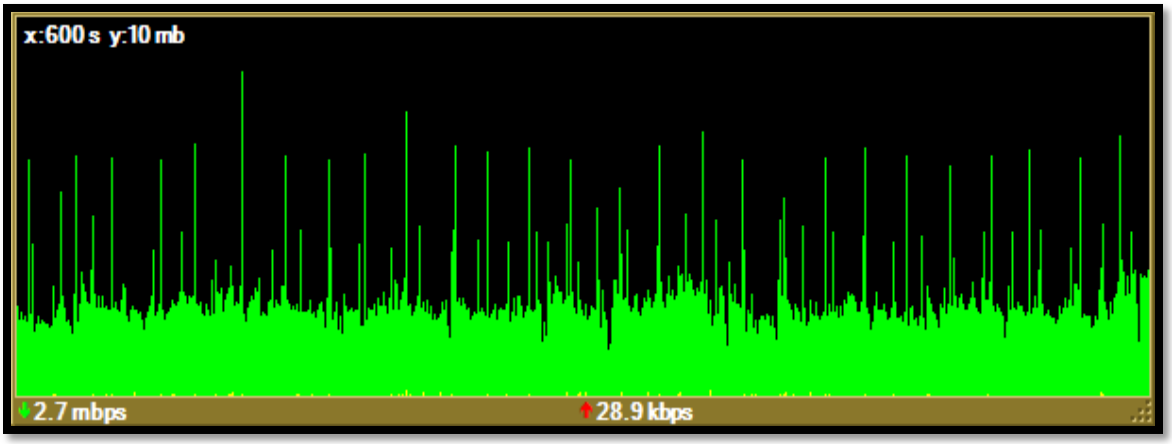



Figure 5.24: Bandwidth utilization using our proposed model.

# CHAPTER 6: Conclusion And Future Work

## 6.1 Conclusion

In our thesis research, we develop a security-enhanced model for a special enterprise network, we recognize it as a study case in our contribution. Enterprise networks includes different devices, equipments, protocols, and networks. Network devices are operated at different levels, Layer 2 switches are used to connect end users, printers, and wireless access point to EN. On the other hand, layer 3 switches are used as core switches, it interconnects different networks of different technology to EN. Firewalls are used to filter inbound and outbound traffic passing through them from and to different networks such as external, internal, and DMZ networks. DMZ network which includes public services that allow public user (via Internet) to access them. DMZ network hosts web server, E-mail server, DNS server, FTP server, Web-based applications, and others. Intrusion detection and prevention systems are used to detect and prevent malicious activity, they filter traffic according to predefined signatures and rules. Routers play a critical role in EN, they are considered as the main gateway of EN. They are used to interconnect distinguishing networks, it is used for WAN services connection. Moreover, host intrusion prevention systems are used to avoid personal computer compromising, it used to protect individual host. EN includes management and monitoring systems such as Splunk for integrating activity of SNORT and OSSEC.

EN interconnects different LAN and WAN using different connection such as Frame Relay, Leased Line, and VPN. Frame relay provides shared bandwidth, while Leased Line provides dedicated bandwidth for connected network. VPN presents a secure, cheap solution for connecting branches networks to enterprise networks, it establishes private network via public network such as Internet.

There are different requirements of enterprise network such as availability, security, redundancy, reliability, scalability. These requirements are essential to provide continues and reliable service of enterprise network.

Deep inspection of traffic passing through enterprise network is very important, it allows us to classify passing traffic. Inbound and outbound traffic will be analyzed to determine

the most used traffic (protocols) through different working time. There are a various number of traffic analysis tools, the following are most famous one: NetFlow, NFSen, IPFIX, and SiLK. NetFlow tool is used to inspect traffic. We do network traffic analysis using different tools such as NetFlow, MRTG, Fiddler 2 to inspect traffic of enterprise network. NetFlow is used as network traffic analysis tool, while MRTG as bandwidth usage analysis tool . Fiddler 2 tool is used to inspect HTTPS traffic, it can inspect encrypted HTTP traffic. Bandwidth usage is different according to inbound and outbound access, it is consumed at different levels through working day.

HTTP/HTTPS traffic is the most used protocols in enterprise networks, most applications of EN are web based. Even HTTP traffic is larger than HTTPS traffic, HTTPS provides encryption and authentication.

Security threats represent a big challenge to EN, these threats could be so complex such as APT-based attacks. The proposed model provides an efficient and secure solution of enterprise network. Security issues are critical to enterprise network, intrusions try to damage enterprise services such web services, mail service, e-services, file service, and others. Today, new complex attacks are arisen, they are performed by expert intruders with foundation from governments and organizations. Advanced Persistent Threat APT are a real example. In our thesis, we do a deep study about Aurora attacks, one main purpose of this thesis is to prevent such attack.

For management and monitoring purpose, we use Splunk tool, it provides an efficient integration with SNORT and OSSEC. It correlates and collects events and logs from network devices.

The proposed model uses different software tools and hardware. Opens source SNORT is used as network intrusion detection and prevention system, while OSSEC as host intrusion prevention system. We use FortiGate-3140B firewall with NIPS as hardware firewall to filter inbound and outbound traffic passing through enterprise network.

The proposed model has the ability to detect and prevent APT-based attack such as Aurora attack. By tuning SNORT, we can inspect HTTPS traffic and thus prevent Aurora attack. Also a firewall of updated signatures and rules decreases the likelihood of threats and attacks success. Metasploit framework is used as penetrating test tool in order to evaluate our proposed model in detection Aurora attack. Overall performance of our

proposed model is done using bandwidth utilization, it is a metric for performance evaluation.

The results of defense evaluation of the proposed security model proves that it has the ability to detect and prevent a large number of attacks and malicious codes. The defense evaluation is done over exploits listed in appendix D (table D.1). There is no guarantee that proposed security-enhanced model will detect new exploits, it should be updated to accomplish this task. The proposed security model can detect and prevent Aurora attack in effective way and using different network security devices and tools. Even results of performance evaluation shows that firewall has impact of network performance, this impact still limited and acceptable.

## 6.2 Future Work

According to performance evaluation in figure 5.24, we observe that firewall has a little impact on bandwidth utilization and so on network performance. We will try to use firewall from other vendors such as Cisco ASA, we used FortiGate-3140B firewall in our proposed model. We will work to develop and implement an awareness module to be added to proposed model. Again, we will use open source in implementing such a module, the main purpose of the module is to provide enough information about intrusions and attacks before they occur. We may need an advance wireless security module to protect branches networks connected through wireless networks. Finally for precision and deep log analysis, we may integrate SNORT with other monitoring and logging tools such as Squil.

# Appendices

## Appendix A

### NetFlow v5 Configuration On Cisco Router

We provide the necessary configurations that are needed to enable NetFlow V5 on Cisco routers. Table A.1 lists the configuration commands that should be configures on Cisco routers [60] to use NetFlow v5.

Table A. 1: Configuration commands list to enable NetFlow v5 on Cisco router.

| Configuration command | Command description |
|---|---|
| `router#configure terminal` | Enter Global configuration mode |
| `route(config)#interface FastEthernet 0/1` | Enter interface mode |
| `router(config-if)#ip route-cache flow` | • This will enable NetFlow export on the specified interface for example FastEtherent 0/1.<br>• We Apply this command on all interfaces of your device that is under traffic analysis. |
| `router(config-if)#exit` | |
| `router(config)#ip flow-export destination 192.168.1.10 9996` | • Exports the NetFlow cache entries to the specified IP address.<br>• Use the IP address of the NetFlow Analyzer server and the configured NetFlow listener port.<br>• The default port is 9996. |
| `router(config)#ip flow-export source Loopback 1` | • Sets the source IP address of the NetFlow exports sent by the device to the specified IP address. |

| | |
|---|---|
| | • NetFlow Analyzer will make SNMP requests of the device on this address. |
| `router(config)#ip flow-export version 5` | • Sets the NetFlow export version to version 5. NetFlow Analyzer supports only version 5, version 7 and #version 9 |
| `router(config)#ip flow-cache timeout active 1` | • Breaks up long-lived flows into 1-minute fragments.<br>• You can choose any number of minutes between 1 and 60. |
| `router(config)#ip flow-cache timeout inactive 15` | • Ensures that flows that have finished are periodically exported. The default value is 15 seconds.<br>• You can choose any number of seconds between 10 and 600. |
| `router(config)#snmp-server ifindex persist` | • Enables ifIndex persistence (interface names) globally.<br>• This ensures that the ifIndex values are persisted during device reboots. |

# Appendix B

## phishing-spam.rules

Phishing attacks and spam represent the main problem for modern inbox, they use malicious emails to steal users data such as password, credit card number, est.phishing-spam.rules are configured in SNORT system to look for domains being advertised in malicious emails.

These rule sets are available from the following website (last visit on Oct. 2013):

- http://cs.uccs.edu/~cs591/ids/snort/snort2_9_0/rules/phishing-spam.rules

# Appendix C

## Integration OSSEC with Splunk

We need to correlates and collected events that are generated from OSSEC server. The default installation of Splunk tool do not contain OSSEC Apps, we have to install OSSEC apps to integrate OSSEC with Splunk.

To integrate OSSEC with Splunk, we have to do the following

1. Enable syslog on OSSEC server by editing OSSEC configuration file /var/ossec/etc/ossec.conf and add the following lines:
    - `<syslog_output>`
    - `<server>xxxx.xxxx.xxxx.xxxx</server>#OSSEC server IP`
    - `</syslog_output>`
2. Edit the configuration file /opt/splunk/etc/system/default/inputs.conf and add the following lines:
    - `[udp://OSSEC_SERVER_IP:Default_PORT(10002)]`
    - `disabled = false`
    - `sourcetype = ossec`
3. Download and install Splunk v4 from http://apps.splunk.com/app/300/ website, Splunk v4 is Splunk for OSSEC package, it contains parsing logic, saved searches, and dashboards for monitoring the OSSEC Host-based Intrusion Detection System via Splunk.

# Appendix D

## Exploits created by Metasploit

Table D.1 describes exploits that we used in our defense evaluation. Exploits target different platform such as Windows, Linux, PHP, hardware, and others.

Table D.1: Exploits used in defense evaluation.

| # | Exploits Description | Platform |
|---|---|---|
| 1. | NTP daemon readvar Buffer Overflow | linux |
| 2. | Wireshark LWRES Dissector getaddrsbyname_request Buffer Overflow | linux |
| 3. | Mozilla Suite/Firefox InstallVersion->compareTo() Code Execution | windows |
| 4. | wu-ftpd SITE EXEC/INDEX Format String Vulnerability | linux |
| 5. | Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow | linux |
| 6. | Veritas Backup Exec Name Service Overflow | windows |
| 7. | Veritas Backup Exec Windows Remote Agent Overflow | windows |
| 8. | Windows Media Services ConnectFunnel Stack Buffer Overflow | windows |
| 9. | Microsoft Private Communications Transport Overflow | windows |
| 10. | WinComLPD <= 3.0.2 - Buffer Overflow | windows |
| 11. | NIPrint LPD Request Overflow | windows |
| 12. | Hummingbird Connectivity 10 SP5 LPD Buffer Overflow | windows |
| 13. | SAP SAPLPD 6.28 Buffer Overflow | windows |
| 14. | Timbuktu Pro Directory Traversal/File Upload | windows |
| 15. | Oracle 8i TNS Listener (ARGUMENTS) Buffer Overflow | windows |
| 16. | Oracle 8i TNS Listener SERVICE_NAME Buffer Overflow | windows |
| 17. | Oracle 10gR2 TNS Listener AUTH_SESSKEY Buffer Overflow | windows |
| 18. | Oracle Secure Backup NDMP_CONNECT_CLIENT_AUTH Buffer Overflow | windows |
| 19. | FutureSoft TFTP Server 2000 Transfer-Mode Overflow | windows |
| 20. | D-Link TFTP 1.0 Long Filename Buffer Overflow | windows |
| 21. | TFTPDWIN 0.4.2 - Long Filename Buffer Overflow | windows |
| 22. | 3CTftpSvc TFTP Long Mode Buffer Overflow | windows |
| 23. | Quick FTP Pro 2.1 Transfer-Mode Overflow | windows |
| 24. | TFTPD32 <= 2.21- Long Filename Buffer Overflow | windows |
| 25. | Allied Telesyn TFTP Server 1.9 Long Filename Overflow | windows |
| 26. | SIPfoundry sipXezPhone 0.35a CSeq Field Overflow | windows |
| 27. | SIPfoundry sipXphone 2.6.0.27 CSeq Buffer Overflow | windows |
| 28. | AIM Triton 1.0.4 CSeq Buffer Overflow | windows |
| 29. | Microsoft IIS ISAPI w3who.dll Query String Overflow | windows |
| 30. | Microsoft IIS ISAPI nsiislog.dll ISAPI POST Overflow | windows |

| | | |
|---|---|---|
| 31. | Microsoft IIS ISAPI FrontPage fp30reg.dll Chunked Overflow | windows |
| 32. | Microsoft IIS Phone Book Service Overflow | windows |
| 33. | Microsoft IIS ISAPI RSA WebAgent Redirect Overflow | windows |
| 34. | Microsoft WINS Service Memory Overwrite | windows |
| 35. | Microsoft Windows SMB Relay Code Execution | windows |
| 36. | Microsoft Print Spooler Service Impersonation Vulnerability | windows |
| 37. | Microsoft Server Service Relative Path Stack Corruption | windows |
| 38. | Microsoft Windows SRV2.SYS SMB Negotiate ProcessID Function Table Dereference | windows |
| 39. | Microsoft RRAS Service Overflow | windows |
| 40. | Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB) | windows |
| 41. | Microsoft Server Service NetpwPathCanonicalize Overflow | windows |
| 42. | Microsoft LSASS Service DsRolerUpgradeDownlevelServer Overflow | windows |
| 43. | Microsoft Services MS06-066 nwwks.dll | windows |
| 44. | Timbuktu <= 8.6.6 PlughNTCommand Named Pipe Buffer Overflow | windows |
| 45. | Microsoft NetDDE Service Overflow | windows |
| 46. | Microsoft Workstation Service NetpManageIPCConnect Overflow | windows |
| 47. | Microsoft Services MS06-066 nwapi32.dll | windows |
| 48. | Microsoft Windows Authenticated User Code Execution | windows |
| 49. | Microsoft RRAS Service RASMAN Registry Overflow | windows |
| 50. | Novell NetIdentity Agent XTIERRPCPIPE Named Pipe Buffer Overflow | windows |
| 51. | Microsoft ASN.1 Library Bitstring Heap Overflow | windows |
| 52. | Microsoft Workstation Service NetAddAlternateComputerName Overflow | windows |
| 53. | Microsoft Outlook Express NNTP Response Parsing Buffer Overflow | windows |
| 54. | CitectSCADA/CitectFacilities ODBC Buffer Overflow | windows |
| 55. | MOXA Device Manager Tool 2.1 - Buffer Overflow | windows |
| 56. | DATAC RealWin SCADA Server SCPC_INITIALIZE Buffer Overflow | windows |
| 57. | DATAC RealWin SCADA Server SCPC_INITIALIZE_RF Buffer Overflow | windows |
| 58. | DATAC RealWin SCADA Server SCPC_TXTEVENT Buffer Overflow | windows |
| 59. | DATAC RealWin SCADA Server Buffer Overflow | windows |
| 60. | D-Link DWL-G132 Wireless Driver Beacon Rates Overflow | windows |
| 61. | Omni-NFS Server Buffer Overflow | windows |
| 62. | Energizer DUO Trojan Code Execution | windows |

| | | |
|---|---|---|
| 63. | EMC AlphaStor Agent Buffer Overflow | windows |
| 64. | Microsoft SQL Server sp_replwritetovarbin Memory Corruption | windows |
| 65. | Microsoft SQL Server Resolution Overflow | windows |
| 66. | Microsoft SQL Server Payload Execution via SQL injection | windows |
| 67. | Microsoft SQL Server Payload Execution | windows |
| 68. | Microsoft SQL Server sp_replwritetovarbin Memory Corruption via SQL Injection | windows |
| 69. | Lyris ListManager MSDE Weak sa Password | windows |
| 70. | Microsoft SQL Server Hello Overflow | windows |
| 71. | Seattle Lab Mail 5.5 POP3 Buffer Overflow | windows |
| 72. | CA BrightStor ARCserve for Laptops & Desktops LGServer Buffer Overflow | windows |
| 73. | CA BrightStor ARCserve Message Engine Heap Overflow | windows |
| 74. | CA BrightStor HSM Buffer Overflow | windows |
| 75. | CA BrightStor Agent for Microsoft SQL Overflow | windows |
| 76. | Computer Associates ARCserve REPORTREMOTEEXECUTECML Buffer Overflow | windows |
| 77. | CA BrightStor Universal Agent Overflow | windows |
| 78. | CA BrightStor Discovery Service Stack Buffer Overflow | windows |
| 79. | CA BrightStor ARCserve Tape Engine Buffer Overflow | windows |
| 80. | CA BrightStor Discovery Service TCP Overflow | windows |
| 81. | CA BrightStor ARCserve for Laptops & Desktops LGServer Buffer Overflow | windows |
| 82. | Computer Associates Alert Notification Buffer Overflow | windows |
| 83. | CA BrightStor ARCserve for Laptops & Desktops LGServer Buffer Overflow | windows |
| 84. | CA BrightStor ARCserve Message Engine 0x72 Buffer Overflow | windows |
| 85. | CA BrightStor ArcServe Media Service Stack Buffer Overflow | windows |
| 86. | CA BrightStor ARCserve License Service GCR NETWORK Buffer Overflow | windows |
| 87. | CA BrightStor ARCserve for Laptops & Desktops LGServer (rxsSetDataGrowthScheduleAndFilter) Buffer Overflow | windows |
| 88. | CA BrightStor ARCserve for Laptops & Desktops LGServer Multiple Commands Buffer Overflow | windows |
| 89. | CA BrightStor ARCserve Tape Engine 0x8A Buffer Overflow | windows |
| 90. | CA BrightStor ARCserve Message Engine Buffer Overflow | windows |
| 91. | Mercury/32 <= 4.01b - PH Server Module Buffer Overflow | windows |
| 92. | Firebird Relational Database SVC_attach() Buffer Overflow | windows |
| 93. | FreeFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow | windows |
| 94. | PuTTy.exe <= 0.53 - Buffer Overflow | windows |
| 95. | ISS PAM.dll ICQ Parser Buffer Overflow | windows |

| | | |
|---|---|---|
| 96. | Kerio Firewall 2.1.4 Authentication Packet Overflow | windows |
| 97. | Microsoft IIS/PWS CGI Filename Double Decode Command Execution | windows |
| 98. | Microsoft IIS 4.0 .HTR Path Overflow | windows |
| 99. | Microsoft IIS 5.0 Printer Host Header Overflow | windows |
| 100. | Microsoft IIS 5.0 WebDAV ntdll.dll Path Overflow | windows |
| 101. | Microsoft IIS WebDAV Write Access Code Execution | windows |
| 102. | Microsoft IIS 5.0 IDQ Path Overflow | windows |
| 103. | Mercury/32 <= 4.01b - LOGIN Buffer Overflow | windows |
| 104. | Qualcomm WorldMail 3.0 IMAPD LIST Buffer Overflow | windows |
| 105. | MailEnable IMAPD (2.35) Login Request Buffer Overflow | windows |
| 106. | Mercur 5.0 - IMAP SP3 SELECT Buffer Overflow | windows |
| 107. | Mdaemon 8.0.3 IMAPD CRAM-MD5 Authentication Overflow | windows |
| 108. | Novell NetMail <= 3.52d IMAP SUBSCRIBE Buffer Overflow | windows |
| 109. | IMail IMAP4D Delete Overflow | windows |
| 110. | MailEnable IMAPD W3C Logging Buffer Overflow | windows |
| 111. | Mercur Messaging 2005 IMAP Login Buffer Overflow | windows |
| 112. | MDaemon 9.6.4 IMAPD FETCH Buffer Overflow | windows |
| 113. | Novell NetMail <= 3.52d IMAP STATUS Buffer Overflow | windows |
| 114. | Mercury/32 4.01a - IMAP RENAME Buffer Overflow | windows |
| 115. | MailEnable IMAPD 1.54 - STATUS Request Buffer Overflow | windows |
| 116. | Novell NetMail <= 3.52d - IMAP AUTHENTICATE Buffer Overflow | windows |
| 117. | Ipswitch IMail IMAP SEARCH Buffer Overflow | windows |
| 118. | Novell NetMail <= 3.52d IMAP APPEND Buffer Overflow | windows |
| 119. | RealVNC 3.3.7 Client Buffer Overflow | windows |
| 120. | UltraVNC 1.0.1 Client Buffer Overflow | windows |
| 121. | WinVNC Web Server <= 3.3.3r7 - GET Overflow | windows |
| 122. | Novell iPrint Client ActiveX Control ExecuteRequest debug Buffer Overflow | windows |
| 123. | EnjoySAP SAP GUI ActiveX Control Arbitrary File Download | windows |
| 124. | Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow | windows |
| 125. | Kazaa Altnet Download Manager ActiveX Control Buffer Overflow | windows |
| 126. | RealPlayer ierpplug.dll ActiveX Control Playlist Name Buffer Overflow | windows |
| 127. | EnjoySAP SAP GUI ActiveX Control Buffer Overflow | windows |
| 128. | Internet Explorer Unsafe Scripting Misconfiguration | windows |
| 129. | Hyleos ChemView ActiveX Control Stack Buffer Overflow | windows |
| 130. | Novell iPrint Client ActiveX Control call-back-url Buffer Overflow | windows |
| 131. | IBM Lotus Domino Web Access Upload Module Buffer | windows |

| | | |
|---|---|---|
| | Overflow | |
| 132. | Adobe Doc.media.newPlayer Use After Free Vulnerability | windows |
| 133. | Adobe util.printf() Buffer Overflow | windows |
| 134. | Facebook Photo Uploader 4 ActiveX Control Buffer Overflow | windows |
| 135. | Internet Explorer Daxctle.OCX KeyFrame Method Heap Buffer Overflow Vulnerability | windows |
| 136. | Microsoft Visual Studio Msmask32.ocx ActiveX Buffer Overflow | windows |
| 137. | Novell iPrint Client ActiveX Control Buffer Overflow | windows |
| 138. | Mozilla Firefox Interleaving document.write and appendChild Exploit | windows |
| 139. | McAfee Subscription Manager Stack Buffer Overflow | windows |
| 140. | Logitech VideoCall ActiveX Control Buffer Overflow | windows |
| 141. | Symantec AppStream LaunchObj ActiveX Control Arbitrary File Download and Execute | windows |
| 142. | Ultra Shareware Office Control ActiveX HttpUpload Buffer Overflow | windows |
| 143. | Novell iPrint Client ActiveX Control ExecuteRequest Buffer Overflow | windows |
| 144. | Worldweaver DX Studio Player <= 3.0.29 shell.execute() Command Execution | windows |
| 145. | Microsoft WMI Administration Tools ActiveX Buffer Overflow | windows |
| 146. | IBM Access Support ActiveX Control Buffer Overflow | windows |
| 147. | Chilkat Crypt ActiveX WriteFile Unsafe Method | windows |
| 148. | Yahoo! Messenger 8.1.0.249 ActiveX Control Buffer Overflow | windows |
| 149. | VeryPDF PDFView OCX ActiveX OpenPDF Heap Overflow | windows |
| 150. | Windows Media Encoder 9 wmex.dll ActiveX Buffer Overflow | windows |
| 151. | Yahoo! Messenger YVerInfo.dll ActiveX Control Buffer Overflow | windows |
| 152. | Novell iPrint Client ActiveX Control target-frame Buffer Overflow | windows |
| 153. | AwingSoft Winds3D Player SceneURL Buffer Overflow | windows |
| 154. | AOL Instant Messenger goaway Overflow | windows |
| 155. | Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (HTTP) | windows |
| 156. | Apple QuickTime 7.1.3 RTSP URI Buffer Overflow | windows |
| 157. | Symantec Altiris Deployment Solution ActiveX Control Buffer Overflow | windows |
| 158. | WinDVD7 IASystemInfo.DLL ActiveX Control Buffer Overflow | windows |
| 159. | mIRC IRC URL Buffer Overflow | windows |
| 160. | Winamp Playlist UNC Path Computer Name Overflow | windows |
| 161. | Internet Explorer XML Core Services HTTP Request Handling | windows |
| 162. | Internet Explorer CSS Recursive Import Use After Free | windows |

| | | |
|---|---|---|
| 163. | AtHocGov IWSAlerts ActiveX Control Buffer Overflow | windows |
| 164. | Trend Micro OfficeScan Client ActiveX Control Buffer Overflow | windows |
| 165. | Green Dam URL Processing Buffer Overflow | windows |
| 166. | Microsoft OWC Spreadsheet msDataSourceObject Memory Corruption | windows |
| 167. | McAfee Visual Trace ActiveX Control Buffer Overflow | windows |
| 168. | Creative Software AutoUpdate Engine ActiveX Control Buffer Overflow | windows |
| 169. | Zenturi ProgramChecker ActiveX Control Arbitrary File Download | windows |
| 170. | Internet Explorer Winhlp32.exe MsgBox Code Execution | windows |
| 171. | Novell iPrint Client ActiveX Control Date/Time Buffer Overflow | windows |
| 172. | SonicWALL Aventail epi.dll AuthCredential Format String Exploit | windows |
| 173. | Microsoft Help Center XSS and Command Execution | windows |
| 174. | Adobe FlateDecode Stream Predictor 02 Integer Overflow | windows |
| 175. | Internet Explorer Style getElementsByTagName Memory Corruption | windows |
| 176. | Amaya Browser 11.0 - bdo tag Overflow | windows |
| 177. | Internet Explorer isComponentInstalled Overflow | windows |
| 178. | WebDAV - Application DLL Hijacker | windows |
| 179. | Internet Explorer CSS SetUserClip Memory Corruption | windows |
| 180. | Husdawg, LLC. System Requirements Lab ActiveX Unsafe Method | windows |
| 181. | BaoFeng Storm mps.dll ActiveX OnBeforeVideoDownload Buffer Overflow | windows |
| 182. | America Online ICQ ActiveX Control Arbitrary File Download and Execute | windows |
| 183. | Internet Explorer 7 CFunctionPointer Uninitialized Memory Corruption | windows |
| 184. | XMPlay 3.3.0.4 (ASX Filename) Buffer Overflow | windows |
| 185. | Ask.com Toolbar askBar.dll ActiveX Control Buffer Overflow | windows |
| 186. | Apple QuickTime 7.6.6 Invalid SMIL URI Buffer Overflow | windows |
| 187. | Roxio CinePlayer ActiveX Control Buffer Overflow | windows |
| 188. | Autodesk IDrop ActiveX Control Heap Memory Corruption | windows |
| 189. | Internet Explorer COM CreateObject Code Execution | windows |
| 190. | Apple ITunes 4.7 Playlist Buffer Overflow | windows |
| 191. | Tumbleweed FileTransfer vcst_eu.dll ActiveX Control Buffer Overflow | windows |
| 192. | Internet Explorer WebViewFolderIcon setSlice() Overflow | windows |
| 193. | RKD Software BarCodeAx.dll 4.9 - ActiveX Remote Stack Buffer Overflow | windows |

| | | |
|---|---|---|
| 194. | CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow | windows |
| 195. | Internet Explorer Tabular Data Control ActiveX Memory Corruption | windows |
| 196. | Juniper SSL-VPN IVE JuniperSetupDLL.dll ActiveX Control Buffer Overflow | windows |
| 197. | Orbit Downloader Connecting Log Creation Buffer Overflow | windows |
| 198. | AwingSoft Winds3D Player 3.5 SceneURL Download and Execute | windows |
| 199. | iseemedia / Roxio / MGI Software LPViewer ActiveX Control Buffer Overflow | windows |
| 200. | GOM Player ActiveX Control Buffer Overflow | windows |
| 201. | Macrovision InstallShield Update Service Buffer Overflow | windows |
| 202. | Microsoft Windows Shell LNK Code Execution | windows |
| 203. | SAP AG SAPgui EAI WebViewer3D Buffer Overflow | windows |
| 204. | Persits XUpload ActiveX AddFile Buffer Overflow | windows |
| 205. | CA BrightStor ARCserve Backup AddColumn() ActiveX Buffer Overflow | windows |
| 206. | Internet Explorer createTextRange() Code Execution | windows |
| 207. | Oracle Document Capture 10g ActiveX Control Buffer Overflow | windows |
| 208. | HP Mercury Quality Center ActiveX Control ProgColor Buffer Overflow | windows |
| 209. | MS03-020 Internet Explorer Object Type | windows |
| 210. | Symantec BackupExec Calendar Control Buffer Overflow | windows |
| 211. | Internet Explorer Data Binding Memory Corruption | windows |
| 212. | RealPlayer rmoc3260.dll ActiveX Control Heap Corruption | windows |
| 213. | Sun Java Web Start Plugin Command Line Argument Injection | windows |
| 214. | RealNetworks RealPlayer SMIL Buffer Overflow | windows |
| 215. | Sun Java Runtime New Plugin docbase Buffer Overflow | windows |
| 216. | HP LoadRunner 9.0 ActiveX AddFolder Buffer Overflow | windows |
| 217. | Apple QuickTime 7.6.7 _Marshaled_pUnk Code Execution | windows |
| 218. | Winamp Ultravox Streaming Metadata (in_mp3.dll) Buffer Overflow | windows |
| 219. | Windows XP/2003/Vista Metafile Escape() SetAbortProc Code Execution | windows |
| 220. | Symantec ConsoleUtilities ActiveX Control Buffer Overflow | windows |
| 221. | Adobe Flash Player "newfunction" Invalid Pointer Use | windows |
| 222. | Microsoft DirectShow (msvidctl.dll) MPEG-2 Memory Corruption | windows |
| 223. | SonicWall SSL-VPN NetExtender ActiveX Control Buffer Overflow | windows |
| 224. | VUPlayer - M3U Buffer Overflow | windows |
| 225. | BlazeDVD 5.1 PLF Buffer Overflow | windows |

| | | |
|---|---|---|
| 226. | Adobe CoolType SING Table "uniqueName" Stack Buffer Overflow | windows |
| 227. | Media Jukebox 8.0.400 Buffer Overflow Exploit (SEH) | windows |
| 228. | Cacti graph_view.php Remote Command Execution | php |
| 229. | PHP XML-RPC Arbitrary Code Execution | php |
| 230. | Simple PHP Blog <= 0.4.0 - Remote Command Execution | php |
| 231. | TikiWiki jhot Remote Command Execution | php |
| 232. | AWStats (6.4-6.5) migrate Remote Command Execution | cgi |
| 233. | phpBB viewtopic.php Arbitrary Code Execution | php |
| 234. | QuickTime Streaming Server parse_xml.cgi Remote Execution | cgi |
| 235. | TWiki History TWikiUsers rev Parameter Command Execution | php |
| 236. | Barracuda IMG.PL Remote Command Execution | cgi |
| 237. | TWiki Search Function Arbitrary Command Execution | php |
| 238. | WordPress cache_lastpostdate Arbitrary Code Execution | php |
| 239. | vBulletin misc.php Template Name Arbitrary Code Execution | php |
| 240. | BASE base_qry_common Remote File Include | php |
| 241. | osCommerce 2.2 Arbitrary PHP Code Execution | php |
| 242. | PAJAX Remote Command Execution | php |
| 243. | CakePHP <= 1.3.5 / 1.2.8 Cache Corruption Exploit | php |
| 244. | OpenX banner-edit.php File Upload PHP Code Execution | php |
| 245. | Trixbox langChoice PHP Local File Inclusion | php |
| 246. | AWStats (6.1-6.2) configdir Remote Command Execution | cgi |
| 247. | Joomla 1.5.12 TinyBrowser File Upload Code Execution | php |
| 248. | Google Appliance ProxyStyleSheet Command Execution | hardware |
| 249. | Nagios3 statuswml.cgi Ping Command Execution | cgi |
| 250. | Coppermine Photo Gallery <= 1.4.14 picEditor.php Command Execution | php |
| 251. | TikiWiki tiki-graph_formula Remote PHP Code Execution | php |
| 252. | Mambo Cache_Lite Class mosConfig_absolute_path Remote File Include | php |
| 253. | PhpMyAdmin Config File Code Injection | php |
| 254. | Matt Wright guestbook.pl Arbitrary Command Execution | cgi |
| 255. | Dogfood CRM spell.php Remote Command Execution | php |
| 256. | ContentKeeper Web Remote Command Execution | hardware |
| 257. | Adobe ColdFusion - Directory Traversal | multiple |
| 258. | Sun Java Applet2ClassLoader Remote Code Execution Exploit | multiple |
| 259. | AstonSoft DeepBurner (DBR File) Path Buffer Overflow | windows |
| 260. | Mini-Stream 3.0.1.1 - Buffer Overflow Exploit | windows |
| 261. | CA Antivirus Engine CAB Buffer Overflow | windows |
| 262. | VideoLAN Client (VLC) Win32 smb:// URI Buffer Overflow | windows |
| 263. | Microsoft Visual Basic VBP Buffer Overflow | windows |
| 264. | Adobe Collab.getIcon() Buffer Overflow | windows |

| | | |
|---|---|---|
| 265. | Adobe PDF Escape EXE Social Engineering (No JavaScript) | windows |
| 266. | HTML Help Workshop 4.74 (hhp Project File) Buffer Overflow Exploit | windows |
| 267. | Destiny Media Player 1.61 PLS M3U Buffer Overflow | windows |
| 268. | MOXA MediaDBPlayback ActiveX Control Buffer Overflow | windows |
| 269. | Microsoft Word RTF pFragments Stack Buffer Overflow (File Format) | windows |
| 270. | Snortreport nmap.php and nbtscan.php Remote Command Execution | php |
| 271. | myBB 1.6.4 Backdoor Exploit | php |
| 272. | HP Power Manager 'formExportDataLogs' Buffer Overflow | cgi |
| 273. | phpLDAPadmin <= 1.2.1.1 (query_engine) Remote PHP Code Injection | php |
| 274. | phpScheduleIt PHP reserve.php start_date Parameter Arbitrary Code Injection | php |
| 275. | LifeSize Room Command Injection | hardware |
| 276. | Support Incident Tracker <= 3.65 Remote Command Execution | php |
| 277. | Java Applet Rhino Script Engine Remote Code Execution | multiple |
| 278. | CTEK SkyRouter 4200 and 4300 Command Execution | hardware |
| 279. | Family Connections less.php Remote Command Execution | php |
| 280. | Traq <= 2.3 Authentication Bypass / Remote Code Execution Exploit | php |
| 281. | PmWiki <= 2.2.34 (pagelist) Remote PHP Code Injection Exploit | php |
| 282. | LotusCMS 3.0 eval() Remote Command Execution | php |
| 283. | FreePBX 2.10.0 / 2.9.0 callmenum Remote Code Execution | php |
| 284. | Java AtomicReferenceArray Type Violation Vulnerability | multiple |
| 285. | Snort 2 DCE/RPC preprocessor Buffer Overflow | multiple |
| 286. | Dolibarr ERP & CRM 3 Post-Auth OS Command Injection | php |
| 287. | Mozilla Firefox Bootstrapped Addon Social Engineering Code Execution | multiple |
| 288. | V-CMS PHP File Upload and Execute | php |
| 289. | PHP CGI Argument Injection | php |
| 290. | WikkaWiki 1.3.2 Spam Logging PHP Injection | php |
| 291. | Squiggle 1.7 SVG Browser Java Code Execution | multiple |
| 292. | Active Collab "chat module" <= 2.3.8 - Remote PHP Code Injection Exploit | php |
| 293. | HP StorageWorks P4000 Virtual SAN Appliance Command Execution | hardware |
| 294. | appRain CMF Arbitrary PHP File Upload Vulnerability | php |
| 295. | WeBid converter.php Remote PHP Code Injection | php |
| 296. | PHP Volunteer Management System 1.0.2 - Arbitrary File Upload | php |

| | | |
|---|---|---|
| 297. | Log1 CMS writeInfo() PHP Code Injection | php |
| 298. | Apache Struts <= 2.2.1.1 - Remote Command Execution | multiple |
| 299. | Symantec Web Gateway 5.0.2.8 Arbitrary PHP File Upload Vulnerability | php |
| 300. | Symantec Web Gateway 5.0.2.8 ipchange.php Command Injection | php |
| 301. | F5 BIG-IP SSH Private Key Exposure | hardware |
| 302. | WordPress plugin Foxypress uploadify.php Arbitrary Code Execution | php |
| 303. | SugarCRM <= 6.3.1 unserialize() PHP Code Execution | php |
| 304. | Tiki Wiki <= 8.3 unserialize() PHP Code Execution | php |
| 305. | Basilic 1.5.14 diff.php Arbitrary Command Execution | php |
| 306. | Hastymail 2.1.1 RC1 Command Injection | php |
| 307. | EGallery PHP File Upload Vulnerability | php |
| 308. | CuteFlow 2.11.2 - Arbitrary File Upload Vulnerability | php |
| 309. | WebPageTest Arbitrary PHP File Upload | php |
| 310. | PHP IRC Bot pbot eval() Remote Code Execution | php |
| 311. | TestLink 1.9.3 - Arbitrary File Upload Vulnerability | php |
| 312. | E-Mail Security Virtual Appliance learn-msg.cgi Command Injection | cgi |
| 313. | XODA 0.4.5 Arbitrary PHP File Upload Vulnerability | php |
| 314. | MobileCartly 1.0 Arbitrary File Creation Vulnerability | php |
| 315. | JBoss DeploymentFileRepository WAR Deployment (via JMXInvokerServlet) | multiple |
| 316. | HP SiteScope Remote Code Execution | multiple |
| 317. | Sflog! CMS 1.0 - Arbitrary File Upload Vulnerability | php |
| 318. | PhpTax pfilez Parameter Exec Remote Code Injection | php |
| 319. | phpMyAdmin 3.5.2.2 server_sync.php Backdoor | php |
| 320. | qdPM 7.0 - Arbitrary PHP File Upload Vulnerability | php |
| 321. | Apple iOS MobileSafari LibTIFF Buffer Overflow | hardware |
| 322. | Apple iOS MobileMail LibTIFF Buffer Overflow | hardware |
| 323. | Project Pier Arbitrary File Upload Vulnerability | php |
| 324. | AjaXplorer checkInstall.php Remote Command Execution | php |
| 325. | ManageEngine Security Manager Plus 5.5 build 5505 SQL Injection | multiple |
| 326. | Java Applet JAX-WS Remote Code Execution | multiple |
| 327. | SAP DB 7.4 WebTools Buffer Overflow | windows |
| 328. | MaxDB WebDBM Database Parameter Overflow | windows |
| 329. | Sybase EAServer 5.2 - Remote Stack Buffer Overflow | windows |
| 330. | IA WebMail 3.x Buffer Overflow | windows |
| 331. | Trend Micro OfficeScan Remote Stack Buffer Overflow | windows |
| 332. | eDirectory 8.7.3 iMonitor Remote Stack Buffer Overflow | windows |

| | | |
|---|---|---|
| 333. | EasyFTP Server <= 1.7.0.11 list.html path Stack Buffer Overflow | windows |
| 334. | EFS Easy Chat Server Authentication Request Handling Buffer Overflow | windows |
| 335. | Novell eDirectory NDS Server Host Header Overflow | windows |
| 336. | HP OpenView NNM 7.53, 7.51 OVAS.EXE Pre-Authentication Stack Buffer Overflow | windows |
| 337. | Alt-N WebAdmin USER Buffer Overflow | windows |
| 338. | Free Download Manager Remote Control Server Buffer Overflow | windows |
| 339. | Race River Integard Home/Pro LoginAdmin Password Stack Buffer Overflow | windows |
| 340. | Now SMS/MMS Gateway Buffer Overflow | windows |
| 341. | CA iTechnology iGateway Debug Mode Buffer Overflow | windows |
| 342. | Webster HTTP Server GET Buffer Overflow | windows |
| 343. | Alt-N SecurityGateway username Buffer Overflow | windows |
| 344. | Belkin Bulldog Plus Web Service Buffer Overflow | windows |
| 345. | HP OpenView Network Node Manager OpenView5.exe CGI Buffer Overflow | windows |
| 346. | BadBlue 2.72b PassThru Buffer Overflow | windows |
| 347. | InterSystems Cache UtilConfigHome.csp Argument Buffer Overflow | windows |
| 348. | NaviCOPA 2.0.1 URL Handling Buffer Overflow | windows |
| 349. | IBM TPM for OS Deployment 5.1.0.x rembo.exe Buffer Overflow | windows |
| 350. | MDaemon <= 6.8.5 WorldClient form2raw.cgi Stack Buffer Overflow | windows |
| 351. | Novell NetMail <= 3.52d NMAP STOR Buffer Overflow | windows |
| 352. | Novell GroupWise Messenger Client Buffer Overflow | windows |
| 353. | Novell ZENworks 6.5 Desktop/Server Management Overflow | windows |
| 354. | Raidsonic NAS Devices Unauthenticated Remote Command Execution | hardware |
| 355. | Nodejs js-yaml load() Code Exec | multiple |
| 356. | Linksys WRT110 Remote Command Execution | hardware |
| 357. | VMware Hyperic HQ Groovy Script-Console Java Execution | multiple |
| 358. | D-Link DIR-605L Captcha Handling Buffer Overflow | hardware |
| 359. | Open Flash Chart 2 Arbitrary File Upload | php |
| 360. | vTigerCRM 5.3.0 5.4.0 - Authenticated Remote Code Execution | php |
| 361. | NAS4Free - Arbitrary Remote Code Execution | php |
| 362. | ISPConfig Authenticated Arbitrary PHP Code Execution | php |
| 363. | ProcessMaker Open Source Authenticated PHP Code Execution | php |
| 364. | Symantec Alert Management System Intel Alert Originator Service Buffer Overflow | windows |

| | | |
|---|---|---|
| 365. | Trend Micro ServerProtect 5.58 Buffer Overflow | windows |
| 366. | Trend Micro ServerProtect 5.58 CreateBinding() Buffer Overflow | windows |
| 367. | Trend Micro ServerProtect 5.58 EarthAgent.EXE Buffer Overflow | windows |
| 368. | Symantec Remote Management Buffer Overflow | windows |
| 369. | SafeNet SoftRemote IKE Service Buffer Overflow | windows |
| 370. | Snort Back Orifice Pre-Preprocessor Remote Exploit | linux |
| 371. | Madwifi SIOCGIWSCAN Buffer Overflow | linux |
| 372. | Cyrus IMAPD pop3d popsubfolders USER Buffer Overflow | linux |
| 373. | hplip hpssd.py From Address Arbitrary Command Execution | linux |
| 374. | NetSupport Manager Agent Remote Buffer Overflow | linux |
| 375. | Borland InterBase PWD_db_aliased() Buffer Overflow | linux |
| 376. | Borland InterBase open_marker_file() Buffer Overflow | linux |
| 377. | GLD (Greylisting Daemon) Postfix Buffer Overflow | linux |
| 378. | LPRng use_syslog Remote Format String Vulnerability | linux |
| 379. | Borland InterBase jrd8_create_database() Buffer Overflow | linux |
| 380. | Borland InterBase INET_connect() Buffer Overflow | linux |
| 381. | Poptop Negative Read Overflow | linux |
| 382. | UoW IMAP server LSUB Buffer Overflow | linux |
| 383. | Squid NTLM Authenticate Overflow | linux |
| 384. | Unreal Tournament 2004 "secure" Overflow (Linux) | linux |
| 385. | MySQL yaSSL SSL Hello Message Buffer Overflow | linux |
| 386. | MySQL yaSSL CertDecoder::GetName Buffer Overflow | linux |
| 387. | ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux) | linux |
| 388. | ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux) | linux |
| 389. | Berlios GPSD Format String Vulnerability | linux |
| 390. | PeerCast <= 0.1216 URL Handling Buffer Overflow (linux) | linux |
| 391. | Samba lsa_io_trans_names Heap Overflow | linux |
| 392. | Samba chain_reply Memory Corruption (Linux x86) | linux |
| 393. | Samba trans2open Overflow (Linux x86) | linux |
| 394. | ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD) | linux |
| 395. | Samba trans2open - Overflow (*BSD x86) | linux |
| 396. | HP Openview connectedNodes.ovpl Remote Command Execution | linux |
| 397. | SquirrelMail PGP Plugin command execution (SMTP) | linux |
| 398. | Mitel Audio and Web Conferencing Command Injection | linux |
| 399. | Oracle VM Server Virtual Server Agent Command Injection | linux |
| 400. | Citrix Access Gateway Command Execution | linux |
| 401. | DistCC Daemon Command Execution | linux |
| 402. | SpamAssassin spamd Remote Command Execution | linux |

| | | |
|---|---|---|
| 403. | ProFTPD-1.3.3c Backdoor Command Execution | linux |
| 404. | UnrealIRCD 3.2.8.1 Backdoor Command Execution | linux |
| 405. | ClamAV Milter Blackhole-Mode Remote Code Execution | linux |
| 406. | Exim4 <= 4.69 - string_format Function Heap Buffer Overflow | linux |
| 407. | Mercantec SoftCart CGI Overflow | windows |
| 408. | System V Derived /bin/login Extraneous Arguments Buffer Overflow | linux |
| 409. | Novell iPrint Client ActiveX Control <= 5.52 Buffer Overflow | windows |
| 410. | Oracle MySQL for Microsoft Windows Payload Execution | windows |
| 411. | Kolibri <= 2.0 - HTTP Server HEAD Buffer Overflow | windows |
| 412. | Foxit PDF Reader 4.2 Javascript File Write | windows |
| 413. | HP OpenView Performance Insight Server Backdoor Account Code Execution | windows |
| 414. | RealNetworks RealPlayer CDDA URI Initialization Vulnerability | windows |
| 415. | Adobe Flash Player AVM Bytecode Verification | windows |
| 416. | HP OpenView NNM nnmRptConfig nameParams Buffer Overflow | windows |
| 417. | HP NNM CGI webappmon.exe OvJavaLocale Buffer Overflow | windows |
| 418. | HP NNM CGI webappmon.exe execvp Buffer Overflow | windows |
| 419. | Distributed Ruby send syscall vulnerability | linux |
| 420. | PostgreSQL for Microsoft Windows Payload Execution | windows |
| 421. | HP OpenView NNM nnmRptConfig.exe schdParams Buffer Overflow | windows |
| 422. | HP OpenView Network Node Manager snmpviewer.exe Buffer Overflow | windows |
| 423. | HP OpenView Network Node Manager getnnmdata.exe (ICount) CGI Buffer Overflow | windows |
| 424. | HP OpenView Network Node Manager ovwebsnmpsrv.exe main Buffer Overflow | windows |
| 425. | HP OpenView Network Node Manager getnnmdata.exe (MaxAge) CGI Buffer Overflow | windows |
| 426. | HP OpenView Network Node Manager ovwebsnmpsrv.exe Unrecognized Option Buffer Overflow | windows |
| 427. | HP OpenView Network Node Manager ovwebsnmpsrv.exe ovutil Buffer Overflow | windows |
| 428. | HP OpenView Network Node Manager getnnmdata.exe (Hostname) CGI Buffer Overflow | windows |
| 429. | VLC AMV Dangling Pointer Vulnerability | windows |
| 430. | Distributed Ruby Send instance_eval/syscall Code Execution | linux |
| 431. | Real Networks Arcade Games StubbyUtil.ProcessMgr ActiveX Arbitrary Code Execution | windows |
| 432. | AOL Desktop 9.6 RTX Buffer Overflow | windows |
| 433. | IBM Lotus Domino iCalendar MAILTO Buffer Overflow | windows |

| | | |
|---|---|---|
| 434. | ManageEngine Applications Manager Authenticated Code Execution | windows |
| 435. | VeryTools Video Spirit Pro <= 1.70 .visprj Buffer Overflow | windows |
| 436. | Adobe Flash Player 10.2.153.1 SWF Memory Corruption Vulnerability | windows |
| 437. | Wireshark <= 1.4.4 packet-dect.c Stack Buffer Overflow | windows |
| 438. | Wireshark <= 1.4.4 packet-dect.c Stack Buffer Overflow | windows |
| 439. | eZip Wizard 3.0 Stack Buffer Overflow | windows |
| 440. | Black Ice Cover Page ActiveX Control Arbitrary File Download | windows |
| 441. | FactoryLink vrn.exe Opcode 9 Buffer Overflow | windows |
| 442. | Sielco Sistemi Winlog Buffer Overflow | windows |
| 443. | RealWin SCADA Server DATAC Login Buffer Overflow | windows |
| 444. | Lotus Notes 8.0.x - 8.5.2 FP2 - Autonomy Keyview (.lzh attachment) | windows |
| 445. | Siemens FactoryLink 8 CSService Logging Path Param Buffer Overflow | windows |
| 446. | Microsoft Office Visio VISIODWG.DLL DXF File Handling Vulnerability | windows |
| 447. | Citrix Provisioning Services 5.6 streamprocess.exe Buffer Overflow | windows |
| 448. | HP OmniInet.exe Opcode 27 Buffer Overflow | windows |
| 449. | HP OmniInet.exe Opcode 20 Buffer Overflow | windows |
| 450. | MicroP 0.1.1.1600 (MPPL File) Stack Buffer Overflow | windows |
| 451. | Blue Coat Authentication and Authorization Agent (BCAAA) 5 Buffer Overflow | windows |
| 452. | Mozilla Firefox "nsTreeRange" Dangling Pointer Vulnerability | windows |
| 453. | HP OpenView Network Node Manager Toolbar.exe CGI Buffer Overflow | windows |
| 454. | HP OpenView Network Node Manager Toolbar.exe CGI Cookie Handling Buffer Overflow | windows |
| 455. | Iconics GENESIS32 9.21.201.01 - Integer overflow | windows |
| 456. | PXE exploit server | windows |
| 457. | Mozilla Firefox 3.6.16 mChannel use after free vulnerability | windows |
| 458. | TeeChart Professional ActiveX Control <= 2010.0.0.3 Trusted Integer Dereference | windows |
| 459. | MS10-026 Microsoft MPEG Layer-3 Audio Stack Based Overflow | windows |
| 460. | HP Easy Printer Care XMLSimpleAccessor Class ActiveX Control Remote Code Execution | windows |
| 461. | Symantec System Center Alert Management System (xfr.exe) Arbitrary Command Execution | windows |
| 462. | Symantec System Center Alert Management System (hndlrsvc.exe) Arbitrary Command Execution | windows |
| 463. | RealVNC Authentication Bypass | windows |

| | | |
|---|---|---|
| 464. | Citrix Gateway ActiveX Control Stack Based Buffer Overflow Vulnerability | windows |
| 465. | DVD X Player 5.5 .plf PlayList Buffer Overflow | windows |
| 466. | Apple QuickTime PICT PnSize Buffer Overflow | windows |
| 467. | Procyon Core Server HMI <= 1.13 - Coreservice.exe Stack Buffer Overflow | windows |
| 468. | Apple Safari Webkit libxslt Arbitrary File Creation | windows |
| 469. | Cytel Studio 9.0 (CY3 File) Stack Buffer Overflow | windows |
| 470. | GTA SA-MP server.cfg - Buffer Overflow | windows |
| 471. | Mini-Stream 3.0.1.1 - Buffer Overflow Exploit | windows |
| 472. | MS11-021 Microsoft Office 2007 Excel .xlb Buffer Overflow | windows |
| 473. | Aviosoft Digital TV Player Professional 1.0 Stack Buffer Overflow | windows |
| 474. | Mini-Stream RM-MP3 Converter 3.1.2.1 - (.pls) Stack Buffer Overflow | windows |
| 475. | Viscom Image Viewer CP Pro 8.0/Gold 6.0 ActiveX Control | windows |
| 476. | Wireshark console.lua pre-loading vulnerability | windows |
| 477. | Viscom Software Movie Player Pro SDK ActiveX 6.8 | windows |
| 478. | Free MP3 CD Ripper 1.1 - (WAV File) Stack Buffer Overflow | windows |
| 479. | MS11-038 Microsoft Office Excel Malformed OBJ Record Handling Overflow | windows |
| 480. | Serv-U FTP Server < 4.2 - Buffer Overflow | windows |
| 481. | CCMPlayer 1.5 Stack based Buffer Overflow (.m3u) | windows |
| 482. | CoDeSys SCADA 2.3 - Webserver Stack Buffer Overflow | windows |
| 483. | Microsoft Internet Explorer JavaScript OnLoad Handler Remote Code Execution Vulnerability | windows |
| 484. | Adobe Reader U3D Memory Corruption Vulnerability | windows |
| 485. | XAMPP WebDAV PHP Upload | windows |
| 486. | Linux BSD-derived Telnet Service Encryption Key ID Buffer Overflow | linux |
| 487. | BS.Player 2.57 Buffer Overflow Exploit (Unicode SEH) | windows |
| 488. | McAfee SaaS MyCioScan ShowReport Remote Command Execution | windows |
| 489. | HP Easy Printer Care XMLCacheMgr Class ActiveX Control Remote Code Execution | windows |
| 490. | HP OpenView Network Node Manager ov.dll _OVBuildPath Buffer Overflow | windows |
| 491. | Gitorious Arbitrary Command Execution | linux |
| 492. | HP Diagnostics Server magentservice.exe Overflow | windows |
| 493. | MS12-004 midiOutPlayNextPolyEvent Heap Overflow | windows |
| 494. | Sunway Forcecontrol SNMP NetDBServer.exe Opcode 0x57 | windows |
| 495. | Icona SpA C6 Messenger DownloaderActiveX Control Arbitrary File Download and Execute | windows |

| | | |
|---|---|---|
| 496. | Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode 0x40020000 Buffer Overflow | windows |
| 497. | Adobe Flash Player MP4 SequenceParameterSetNALUnit Buffer Overflow | windows |
| 498. | Java MixerSequencer Object GM_Song Structure Handling Vulnerability | windows |
| 499. | Horde 3.3.12 Backdoor Arbitrary PHP Code Execution | linux |
| 500. | TrendMicro Control Manger <= 5.5 CmdProcessor.exe - Stack Buffer Overflow | windows |
| 501. | Orbit Downloader - URL Unicode Conversion Overflow | windows |
| 502. | Sun Java Web Start Plugin Command Line Argument Injection (2012) | windows |
| 503. | HP Data Protector 6.1 EXEC_CMD Remote Code Execution | windows |
| 504. | ASUS Net4Switch ipswcom.dll ActiveX Stack Buffer Overflow | windows |
| 505. | IBM Personal Communications I-Series Access WorkStation 5.9 Profile | windows |
| 506. | DJ Studio Pro 5.1 .pls Stack Buffer Overflow | windows |
| 507. | VLC Media Player RealText Subtitle Overflow | windows |
| 508. | Sysax 5.53 SSH Username Buffer Overflow (msf) | windows |
| 509. | Adobe Flash Player .mp4 'cprt' Overflow" | windows |
| 510. | NetDecision 4.5.1 HTTP Server Buffer Overflow | windows |
| 511. | Dell Webcam CrazyTalk ActiveX BackImage Vulnerability | windows |
| 512. | MS10-002 Internet Explorer Object Memory Use-After-Free | windows |
| 513. | Ricoh DC DL-10 SR10 FTP USER Command Buffer Overflow" | windows |
| 514. | UltraVNC 1.0.2 Client (vncviewer.exe) Buffer Overflow | windows |
| 515. | NetOp Remote Control Client 9.5 - Buffer Overflow', | windows |
| 516. | TRENDnet SecurView Internet Camera UltraMJCam OpenFileDlg Buffer Overflow | windows |
| 517. | Csound hetro File Handling Stack Buffer Overflow | windows |
| 518. | LANDesk Lenovo ThinkManagement Console Remote Command Execution | windows |
| 519. | IBM Tivoli Provisioning Manager Express for Software Distribution Isig.isigCtl.1 ActiveX RunAndUploadFile() Method Overflow | windows |
| 520. | Quest InTrust Annotation Objects Uninitialized Pointer | windows |
| 521. | CyberLink Power2Go name attribute (p2g) Stack Buffer Overflow Exploit | windows |
| 522. | GSM SIM Editor 5.15 Buffer Overflow | windows |
| 523. | TFTP Server for Windows 1.4 ST WRQ Buffer Overflow | windows |
| 524. | xRadio 0.95b Buffer Overflow | windows |
| 525. | Adobe Flash Player ActionScript Launch Command Execution Vulnerability | linux |
| 526. | MS12-027 MSCOMCTL ActiveX Buffer Overflow | windows |

| | | |
|---|---|---|
| 527. | Shadow Stream Recorder 3.0.1.7 - Buffer Overflow | windows |
| 528. | McAfee Virtual Technician MVTControl 6.3.0.1911 GetObject Vulnerability | windows |
| 529. | VLC MMS Stream Handling Buffer Overflow | windows |
| 530. | Solarwinds Storage Manager 5.1.0 - SQL Injection | windows |
| 531. | Firefox 7/8 (<= 8.0.1) nsSVGValue Out-of-Bounds Access Vulnerability | windows |
| 532. | Distinct TFTP 3.01 Writable Directory Traversal Execution | windows |
| 533. | Firefox 8/9 AttributeChildRemoved() Use-After-Free | windows |
| 534. | Oracle Weblogic Apache Connector POST Request Buffer Overflow | windows |
| 535. | Foxit Reader 3.0 Open Execute Action Stack Based Buffer Overflow | windows |
| 536. | FlexNet License Server Manager lmgrd Buffer Overflow | windows |
| 537. | OpenOffice OLE Importer DocumentSummaryInformation Stream Handling Overflow | windows |
| 538. | RabidHamster R4 Log Entry sprintf() Buffer Overflow | windows |
| 539. | quickshare file share 1.2.1 - Directory Traversal vulnerability | windows |
| 540. | Symantec Web Gateway 5.0.2.8 Command Execution Vulnerability | linux |
| 541. | ispVM System XCF File Handling Overflow | windows |
| 542. | MPlayer SAMI Subtitle File Buffer Overflow | windows |
| 543. | Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode 0x40020004 Buffer Overflow | windows |
| 544. | Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode 0x40020006 Buffer Overflow | windows |
| 545. | Citrix Provisioning Services 5.6 SP1 Streamprocess Opcode 0x40020002 Buffer Overflow | windows |
| 546. | GIMP script-fu Server Buffer Overflow | windows |
| 547. | Microsoft Windows OLE Object File Handling Remote Code Execution | windows |
| 548. | Sielco Sistemi Winlog Buffer Overflow 2.07.14 | windows |
| 549. | PHP apache_request_headers Function Buffer Overflow | windows |
| 550. | EZHomeTech EzServer <= 6.4.017 Stack Buffer Overflow Vulnerability | windows |
| 551. | Adobe Flash Player AVM Verification Logic Array Indexing Code Execution | windows |
| 552. | Adobe Flash Player Object Type Confusion | windows |
| 553. | Apple iTunes 10 Extended M3U Stack Buffer Overflow | windows |
| 554. | Apple QuickTime TeXML Stack Buffer Overflow | windows |
| 555. | HP Data Protector Create New Folder Buffer Overflow | windows |
| 556. | Irfanview JPEG2000 <= 4.3.2.0 - jp2 Stack Buffer Overflow | windows |
| 557. | IBM Rational ClearQuest CQOle Remote Code Execution | windows |
| 558. | Poison Ivy 2.3.2 C&C Server Buffer Overflow | windows |

| | | |
|---|---|---|
| 559. | AdminStudio LaunchHelp.dll ActiveX Arbitrary Code Execution | windows |
| 560. | ALLMediaServer 0.8 - Buffer Overflow | windows |
| 561. | Windows Escalate Task Scheduler XML Privilege Escalation | windows |
| 562. | Novell ZENworks Configuration Management Preboot Service 0x06 Buffer Overflow | windows |
| 563. | Novell ZENworks Configuration Management Preboot Service 0x21 Buffer Overflow | windows |
| 564. | Linux Kernel Sendpage Local Privilege Escalation | linux |
| 565. | Novell ZENworks Configuration Management Preboot Service 0x6c Buffer Overflow | windows |
| 566. | Novell ZENworks Configuration Management Preboot Service 0x4c Buffer Overflow | windows |
| 567. | Simple Web Server Connection Header Buffer Overflow | windows |
| 568. | Photodex ProShow Producer 5.0.3256 load File Handling Buffer Overflow | windows |
| 569. | Cisco Linksys PlayerPT ActiveX Control Buffer Overflow | windows |
| 570. | Symantec Web Gateway 5.0.2.18 pbcontrol.php Command Injection | linux |
| 571. | Microsoft Office SharePoint Server 2007 Remote Code Execution | windows |
| 572. | Microsoft Internet Explorer Fixed Table Col Span Heap Overflow | windows |
| 573. | Plixer Scrutinizer NetFlow and sFlow Analyzer 9 Default MySQL Credential | windows |
| 574. | NetDecision 4.2 TFTP Writable Directory Traversal Execution | windows |
| 575. | Cyclope Employee Surveillance Solution 6.0 - SQL Injection | windows |
| 576. | globalSCAPE CuteZIP Stack Buffer Overflow | windows |
| 577. | Windows Service Trusted Path Privilege Escalation | windows |
| 578. | Adobe Flash Player 11.3 Font Parsing Code Execution | windows |
| 579. | Sysax Multi Server 5.64 Create Folder Buffer Overflow | windows |
| 580. | Zabbix Server Arbitrary Command Execution | linux |
| 581. | SAP NetWeaver HostControl Command Injection | windows |
| 582. | SAP NetWeaver Dispatcher DiagTraceR3Info Buffer Overflow | windows |
| 583. | Symantec Messaging Gateway 9.5/9.5.1 SSH Default Password Security Bypass Vulnerability | linux |
| 584. | ActiveFax (ActFax) 4.3 Client Importer Buffer Overflow | windows |
| 585. | WAN Emulator 2.3 - Command Execution | linux |
| 586. | Openfiler 2.x - NetworkCard Command Execution | linux |
| 587. | Winamp MAKI Buffer Overflow | windows |
| 588. | InduSoft Web Studio Arbitrary Upload Remote Code Execution | windows |
| 589. | Avaya WinPMD UniteHostRouter Buffer Overflow | windows |
| 590. | NTR ActiveX Control StopModule() Remote Code Execution | windows |
| 591. | MS12-063 Microsoft Internet Explorer execCommand Use- | windows |

| | | |
|---|---|---|
| | After-Free Vulnerability | |
| 592. | NTR ActiveX Control Check() Method Buffer Overflow | windows |
| 593. | HP Application Lifecycle Management XGO.ocx ActiveX SetShapeNodeType() Remote Code Execution | windows |
| 594. | Windows Escalate UAC Execute RunAs | windows |
| 595. | MS11-080 AfdJoinLeaf Privilege Escalation | windows |
| 596. | Windows Escalate UAC Protection Bypass | windows |
| 597. | Avaya IP Office Customer Call Reporter ImageUpload.ashx Remote Command Execution | windows |
| 598. | Linux udev Netlink Local Privilege Escalation | linux |
| 599. | Samba SetInformationPolicy AuditEventsInfo Heap Overflow | linux |
| 600. | KeyHelp ActiveX LaunchTriPane Remote Code Execution Vulnerability | windows |
| 601. | Windows Escalate Service Permissions Local Privilege Escalation | windows |
| 602. | Turbo FTP Server 1.30.823 PORT Overflow | windows |
| 603. | HP Operations Agent Opcode coda.exe 0x8c Buffer Overflow | windows |
| 604. | HP Operations Agent Opcode coda.exe 0x34 Buffer Overflow | windows |
| 605. | Aladdin Knowledge System Ltd ChooseFilePath Buffer Overflow | windows |
| 606. | HP Intelligent Management Center UAM Buffer Overflow | windows |
| 607. | EMC Networker Format String | windows |
| 608. | WinRM VBS Remote Code Execution | windows |
| 609. | Oracle Database Client System Analyzer Arbitrary File Upload | windows |
| 610. | NFR Agent FSFUI Record File Upload RCE | windows |
| 611. | Narcissus Image Configuration Passthru Vulnerability | linux |
| 612. | NetIQ Privileged User Manager 2.3.1 ldapagnt_eval() Remote Perl Code Execution | windows |
| 613. | RealPlayer RealMedia File Handling Buffer Overflow | windows |
| 614. | IBM Cognos tm1admsd.exe Overflow Vulnerability | windows |
| 615. | Microsoft Internet Explorer Option Element Use-After-Free | windows |
| 616. | Honeywell Tema Remote Installer ActiveX Remote Code Execution | windows |
| 617. | Freesshd Authentication Bypass | windows |
| 618. | Nagios3 history.cgi Host Command Execution | linux |
| 619. | Windows Manage Memory Payload Injection | windows |
| 620. | VMWare OVF Tools Format String Vulnerability | windows |
| 621. | VMWare OVF Tools Format String Vulnerability | windows |
| 622. | Novell GroupWise Client gwcls1.dll ActiveX Remote Code Execution | windows |
| 623. | Foxit Reader Plugin URL Processing Buffer Overflow | windows |
| 624. | BigAnt Server 2 SCH And DUPF Buffer Overflow | windows |
| 625. | BigAnt Server DUPF Command Arbitrary File Upload | windows |

| | | |
|---|---|---|
| 626. | MS13-009 Microsoft Internet Explorer SLayoutRun Use-After-Free | windows |
| 627. | Honeywell HSC Remote Deployer ActiveX Remote Code Execution | windows |
| 628. | Sami FTP Server LIST Command Buffer Overflow | windows |
| 629. | Cool PDF Image Stream Buffer Overflow | windows |
| 630. | KingView Log File Parsing Buffer Overflow | windows |
| 631. | Mutiny Remote Command Execution | linux |
| 632. | ActFax 5.01 RAW Server Buffer Overflow | windows |
| 633. | HP Intelligent Management Center Arbitrary File Upload | windows |
| 634. | Java CMM Remote Code Execution | windows |
| 635. | HP System Management Homepage Local Privilege Escalation | linux |
| 636. | MongoDB nativeHelper.apply Remote Code Execution | linux |
| 637. | Synactis PDF In-The-Box ConnectToSynactic Stack Buffer Overflow | windows |
| 638. | MS13-009 Microsoft Internet Explorer COALineDashStyleArray Integer Overflow | windows |
| 639. | Novell Client 4.91 SP4 nwfs.sys Local Privilege Escalation | windows |
| 640. | ZPanel 10.0.0.2 htpasswd Module Username Command Execution | linux |
| 641. | HP System Management Homepage JustGetSNMPQueue Command Injection | windows |
| 642. | MoinMoin twikidraw Action Traversal File Upload | linux |
| 643. | ZPanel zsudo Local Privilege Escalation Exploit | linux |
| 644. | Windows EPATHOBJ::pprFlattenRec Local Privilege Escalation | windows |
| 645. | ABBS Audio Media Player .LST Buffer Overflow | windows |
| 646. | ERS Viewer 2013 ERS File Handling Buffer Overflow | windows |
| 647. | Corel PDF Fusion Stack Buffer Overflow | windows |
| 648. | Apple Quicktime 7 Invalid Atom Length Buffer Overflow | windows |
| 649. | HP Managed Printing Administration jobAcct Remote Command Execution | windows |
| 650. | Foreman (Red Hat OpenStack/Satellite) bookmarks/create Code Injection | linux |
| 651. | VMware vCenter Chargeback Manager ImageUploadServlet Arbitrary File Upload | windows |
| 652. | MS13-005 HWND_BROADCAST Low to Medium Integrity Privilege Escalation | windows |
| 653. | Firefox onreadystatechange Event DocumentViewerImpl Use After Free | windows |
| 654. | HP StorageWorks P4000 Virtual SAN Appliance Login Buffer Overflow | windows |
| 655. | Open-FTPD 1.2 - Arbitrary File Upload | windows |
| 656. | Intrasrv 1.0 - Buffer Overflow | windows |
| 657. | MiniWeb (Build 300) Arbitrary File Upload | windows |

| | | |
|---|---|---|
| 658. | Ultra Mini HTTPD Stack Buffer Overflow | windows |
| 659. | Chasys Draw IES Buffer Overflow | windows |
| 660. | Cogent DataHub HTTP Server Buffer Overflow | windows |
| 661. | Oracle Endeca Server Remote Command Execution | windows |
| 662. | VMWare Setuid vmware-mount Unsafe popen(3) | linux |
| 663. | HP LoadRunner lrFileIOService ActiveX Remote Code Execution | windows |
| 664. | Firefox XMLSerializer Use After Free | windows |
| 665. | MS13-059 Microsoft Internet Explorer CFlatMarkupPointer Use-After-Free | windows |
| 666. | HP LoadRunner lrFileIOService ActiveX WriteFileString Remote Code Execution | windows |
| 667. | IKE and AuthIP IPsec Keyring Modules Service (IKEEXT) Missing DLL | windows |
| 668. | Sophos Web Protection Appliance clear_keys.pl Local Privilege Escalation | linux |
| 669. | Sophos Web Protection Appliance sblistpack Arbitrary Command Execution | linux |
| 670. | Agnitum Outpost Internet Security Local Privilege Escalation | windows |
| 671. | HP ProCurve Manager SNAC UpdateDomainControllerServlet File Upload | windows |
| 672. | HP ProCurve Manager SNAC UpdateCertificatesServlet File Upload | windows |
| 673. | CA BrightStor ARCserve Tape Engine 0x8A Buffer Overflow | windows |
| 674. | MS13-069 Microsoft Internet Explorer CCaret Use-After-Free | windows |
| 675. | MS13-071 Microsoft Windows Theme File Handling Arbitrary Code Execution | windows |
| 676. | freeFTPd PASS Command Buffer Overflow | windows |
| 677. | Micorosft Internet Explorer SetMouseCapture Use-After-Free | windows |
| 678. | SIEMENS Solid Edge ST4 SEListCtrlX ActiveX Remote Code Execution | windows |
| 679. | HP LoadRunner magentproc.exe Overflow | windows |
| 680. | HP Data Protector Cell Request Service Buffer Overflow | windows |
| 681. | MS13-080 Microsoft Internet Explorer CDisplayPointer Use-After-Free | windows |
| 682. | Interactive Graphical SCADA System Remote Command Injection | windows |
| 683. | HP Intelligent Management Center BIMS UploadServlet Directory Traversal | windows |
| 684. | Zabbix Authenticated Remote Command Execution | linux |
| 685. | OpenMediaVault Cron Remote Command Execution | linux |
| 686. | Moodle Remote Command Execution | linux |
| 687. | GLPI install.php Remote Command Execution | php |
| 688. | Linksys WRT110 Remote Command Execution | hardware |

# References


[1] S. M. Nadaf, H. K. Rath, and A. Simha, "A novel approach for an enterprise network transformation and optimization," in *India Conference (INDICON), 2012 Annual IEEE*, 2012, pp. 317-322.

[2] M. Weinstein, "Planning enterprise networks to meet critical business needs," in *Enterprise Networking Mini-Conference, 1997. ENM-97. In conjunction with the ICC-97., First IEEE*, 1997, pp. 3-13.

[3] K. K. Nguyen and B. Jaumard, "Routing engine architecture for next generation routers: evolutional trends," *Network Protocols and Algorithms*, vol. 1, pp. 62-85, 2009.

[4] (2013, september 15). *The Ultra-Secure Network Architecture*. Available: http://mcgladrey.com/Risk-Advisory-Services/The-UltraSecure-Network Architecture.html.

[5] E. Dart, L. Rotman, B. Tierney, M. Hester, and J. Zurawski, "The science dmz: A network design pattern for data-intensive science," in *IEEE/ACM Annual SuperComputing Conference (SC13), Denver CO, USA*, 2013.

[6] B.-H. Kang and M. O. Balitanas, "Vulnerabilities of VPN using IPSec and defensive measures," *International Journal of Advanced Science and Technology*, vol. 8, pp. 9-18, 2009.

[7] E. Sutherland, "The regulation of leased lines," in *Telecommunication Techno-Economics, 2007. CTTE 2007. 6th Conference on*, 2007, pp. 1-5.

[8] D. B. Grossman, "An overview of frame relay technology," in *Computers and Communications, 1991. Conference Proceedings., Tenth Annual International Phoenix Conference on*, 1991, pp. 539-545.

[9] L.-G. Zhu, D.-z. Han, S.-Z. Zhou, and C.-S. Xie, "High availability cluster with combining NAS and ISCSI," in *Machine Learning and Cybernetics, 2006 International Conference on*, 2006, pp. 4455-4460.

[10] L. Yi, K. Miao, and A. Liu, "A comparative study of WiMAX and LTE as the next generation mobile enterprise network," in *Advanced Communication Technology (ICACT), 2011 13th International Conference on*, 2011, pp. 654-658.

[11] P. Saravanan, E. Reuter, and S. Verma, "Enhancing enterprise network management using smart," in *India Conference, 2008. INDICON 2008. Annual IEEE*, 2008, pp. 343-348.

[12] M. A. Qadeer, M. Zahid, A. Iqbal, and M. Siddiqui, "Network traffic analysis and intrusion detection using packet sniffer," in *Communication Software and Networks, 2010. ICCSN'10. Second International Conference on*, 2010, pp. 313-317.

[13] S. Chen, J. Xu, R. K. Iyer, and K. Whisnant, "Evaluating the security threat of firewall data corruption caused by instruction transient errors," in *Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on*, 2002, pp. 495-504.

[14] H. W. Kim and S. Lee, "Design and implementation of a private and public key crypto processor and its application to a security system," *Consumer Electronics, IEEE Transactions on*, vol. 50, pp. 214-224, 2004.
[15] S. Alabady, "Design and Implementation of a Network Security Model for Cooperative Network," *Int. Arab J. e-Technol.*, vol. 1, pp. 26-36, 2009.
[16] M. Labs and M. F. P. Services, "Protecting Your Critical AssetsLessons Learned from "Operation Aurora"," Santa Clara, CA2010.
[17] J. Xi, "A Design and Implement of IPS Based on Snort," in *Computational Intelligence and Security (CIS), 2011 Seventh International Conference on*, 2011, pp. 771-773.
[18] OSSEC. (2013, october 1). *OSSEC | Home | Open Source SECurity*. Available: http://www.ossec.net/
[19] K. Ingham and S. Forrest, "A history and survey of network firewalls," *University of New Mexico, Tech. Rep*, 2002.
[20] (2013, october 10). *Operational Intelligence, Log Management, Application Management, Enterprise Security and Compliance | Splunk*. Available: http://www.splunk.com/
[21] (2013, october 15). *Penetration Testing Software | Metasploit*. Available: http://www.metasploit.com/
[22] S. P. Ping, "An improved model of distributed network information security," in *Educational and Information Technology (ICEIT), 2010 International Conference on*, 2010, pp. V3-391-V3-393.
[23] S. A. J. Alabady, "Design and implementation of a network security model using static VLAN and AAA server," in *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, 2008, pp. 1-6.
[24] Z. Qu and J. Yan, "The Design of the Network Security Model of Active Defense," in *Wireless Communications, Networking and Mobile Computing, 2008. WiCOM'08. 4th International Conference on*, 2008, pp. 1-4.
[25] S. Singh, "EtherSec: An Enterprise Ether-network security model," in *Networks, 2008. ICON 2008. 16th IEEE International Conference on*, 2008, pp. 1-5.
[26] X. He, B. Yao, and W. Gao, "Design and implementation of Enterprise Network information monitoring system," in *Communications, Circuits and Systems, 2009. ICCCAS 2009. International Conference on*, 2009, pp. 326-330.
[27] J. Li, H.-x. Wang, R.-f. Han, and X.-p. Jing, "Construction and application of network security defense model," in *Wireless Communications, Networking and Mobile Computing, 2009. WiCom'09. 5th International Conference on*, 2009, pp. 1-3.
[28] W. Kehe, Z. Tong, L. Wei, and M. Gang, "Security model based on network business security," in *Computer Technology and Development, 2009. ICCTD'09. International Conference on*, 2009, pp. 577-580.
[29] W. Zongjiang, "A new type of intelligent network security model of the campus study," in *Computer Research and Development (ICCRD), 2011 3rd International Conference on*, 2011, pp. 325-329.

[30] J. Timofte, "Intrusion detection using open source tools," *Informatica Economica Journal Issn*, vol. 14531305, pp. 75-79, 2008.
[31] Y. Peng, "Research of network intrusion detection system based on snort and NTOP," in *Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on*, 2012, pp. 2764-2768.
[32] (2013, september 15). *Inter-Data Center Connectivity*. Available: http://archive.icann.org/en/tlds/org/applications/unity/III/C17.1.htm
[33] R. Singh, "LAYER 3 SWITCHING," *International Journal of Scientific Research Engineering & Technology (IJSRET)*, vol. 1, pp. 1-5, January 2013 2013.
[34] M. G. Gouda and A. X. Liu, "Structured firewall design," *Computer Networks*, vol. 51, pp. 1106-1120, 2007.
[35] R. Kohavi, "Scaling up the accuracy of naive-Bayes classifiers: A decision-tree hybrid," in *KDD*, 1996, pp. 202-207.
[36] R. Ganta. (2013, september 4). *RD Gateway deployment in a perimeter network & Firewall rules - Remote Desktop Services (Terminal Services) Team Blog - Site Home - MSDN Blogs*. Available:
http://blogs.msdn.com/b/rds/archive/2009/07/31/rd-gateway-deployment-in-a-perimeter-network-firewall-rules.aspx
[37] C. Academy, "Access the WANCCNA Exploration 4_English Version 4.," ed, 2007.

[38] GFI. (2013, september 15). *GFI EventsManager*. Available:
http://support.gfi.com/manuals/en/esm2011/esm2011manual.1.8.html
[39] V. Bajpai, J. Schauer, and J. Schönwälder, "NFQL: A Tool for Querying Network Flow Records," 2013.
[40] B. Claise, "Cisco systems NetFlow services export version 9," 2004.
[41] B. Claise, "Specification of the IP flow information export (IPFIX) protocol for the exchange of IP traffic flow information," 2008.
[42] P. Haag, "Netflow tools nfsen and nfdump," in *18th Annual FIRST Conference*, 2006.
[43] C. C. Center, "SiLK: System for internet-level knowledge," ed, 2004.
[44] D. Plonka, "FlowScan: A Network Traffic Flow Reporting and Visualization Tool," in *LISA*, 2000, pp. 305-317.
[45] M. Fullmer and S. Romig, "The OSU flowtools package and CISCO NetFlow logs," in *Proceedings of the 2000 USENIX LISA Conference*, 2000.
[46] Cisco. (2013, october 2). *Introduction to Netflow*. Available:
http://www.cisco.com/%20en/US/products/ps6646/products_ios_protocol_option_home.html
[47] (2013, October 2). *Netflow v 5 Format*. Available:
http://support.packeteer.com/documenttaios/packetguide/7.2/info/netflow5-header.html
[48] Cisco. (2013, september 4). *NetFlow version 9*. Available: http://www.cisco.com/en/US/products/ps6645/products_ios_protocol_option_home.html
[49] C. Estan and G. Varghese, "Autofocus: A tool for automatic traffic analysis," in *Proceedings of ACM SIGCOMM*, 2003.

[50] ManageEngine. (2013, september 4). *Top 10 reasons. NetFlow Monitoring | NetFlow Analysis | NetFlow Reporting :: NetFlow Analyzer*. Available: http://www.manageengine.com/products/netflow/top-10-reasons.html
[51] (2013, september 15). *MRTG - The Multi Router Traffic Grapher*. Available: http://www.mrtg.org/
[52] (2013, september 22). *Fiddler: HTTP/HTTPS traffic recording*. Available: http://fiddler2.com/features
[53] A. McCarty, "Distributed NIDS: A HOW-TO Guide," SANS Institute2003.
[54] E. Hjelmvik, "How to detect reverse_https backdoors - NETRESEC Blog," vol. 2013, ed, 2013.
[55] (2013, october 10). *FortiGate-3140B Next Generation Firewall (NGFW)*. Available: http://www.fortinet.com/products/fortigate/3140B.html
[56] (2013, october 1). *The Community ENTerprise Operating System*. Available: http://www.centos.org/
[57] J. Gómez, C. Gil, N. Padilla, R. Baños, and C. Jiménez, "Design of a snort-based hybrid intrusion detection system," in *Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing, and Ambient Assisted Living*, ed: Springer, 2009, pp. 515-522.
[58] (2013, october 1). *OSSEC Architecture â" OSSEC v2.7.0 documentation*. Available: http://www.ossec.net/doc/manual/ossec-architecture.html
[59] (2013, october 1). *Howto: Distributed Splunk Architecture*. Available: http://blog.rootshell.be/2012/12/22/howto-distributed-splunk-architecture/
[60] (2013, september 4). *Setting up Cisco NetFlow :: User Guide*. Available: http://www.manageengine.com/products/netflow/help/cisco-netflow/cisco-ios-netflow.html