Design and Analysis of Real-time Network Intrusion Detection and Prevention System using Open Source Tools

Ammad Uddin
Department of Computer System Engineering,
University of Engineering and Technology,
Peshawar, Pakistan

Laiq Hasan, PhD
Department of Computer System Engineering,
University of Engineering and Technology,
Peshawar, Pakistan

ABSTRACT
Intrusion detection and prevention is one of the most important and fundamental task in an organization's computer network. Commercially available intrusion detection and prevention systems are costly and overkill for small and medium sized organizations. This paper describes the design and analysis of a network intrusion detection system (NIDS) and network intrusion prevention system (NIPS) using open source tools. The study also describes an open source Database to store the alerts and an open source front end management console application to view the alerts and logs from the proposed Database in any of the modern day web browser. In this particular research Snort was used as an NIDS to detect intrusions and attacks. Snort is a popular open source NIDS with signature based rules for detecting thousands of known attacks. The rules are regularly updated by Snort team to include new attacks and intrusions. SnortSam was used as an NIPS to act upon the alerts detected by Snort. SnortSam blocks the intrusions by sending intruders and attacker's source IP addresses to firewall in real time. MySQL was used as the Database to store alerts and BASE (Basic Analysis and Security Engine) was chosen as the open source management console application. Juniper Networks switch EX-3200 and Firewall SSG-20 were used as the network devices for connectivity and working of the system. Any other vendor network devices can also effectively be used in design and configuration of the system. The design successfully detected and prevented network intrusions and same can be implemented in any small and medium sized organization for protection of their Computer Networks.

Keywords
BASE (Basic Analysis and Security Engine), MySQL, NIDS, NIPS, Snort, Snortsam.

1. INTRODUCTION
INTRUSION detection and prevention is one of the top priority of each organization due to increase number of attacks and intrusions in computer networks. A network intrusion detections system (NIDS) is an application software or hardware designed to monitor network traffic and detect unauthorized users and malicious traffic [1]. A network intrusion prevention system (NIPS) is a system that works along NIDS and blocks intrusion into a network, often in real time [2]. Traditionally, Firewalls were used as the main protection systems against cyber-attacks and intrusions. But with the passage of time, the attacks are becoming more and more complex and increasing in number. Firewalls alone no longer provide full proof security to an organization's computer networks. To fill this gap, many commercial security systems including NIDS and NIPS have been developed and are available in the market. Many of these commercial security systems are quite sophisticated and intelligent as compared to traditional firewalls. These complex security systems are good for large organizations but not suited for small and medium sized organizations due to financial constraints.

This research proposes the design of a real time self-defending

System for small and medium organizations using open source tools. The design integrates open source tools including Snort NIDS, Snortsam NIPS, BASE console and MySQL Database into a composite real time self-defending security system. The security design can be implemented in any small and medium sized organization with minimum effort and cost. The security system inspects all the In / Out traffic through the network for intrusions and then sends the source IP address of any intruder or attacker to the edge router or firewall for blocking. This particular research uses Juniper Networks Firewall SSG-20 as the edge firewall for blocking the source IP addresses of intruders. Besides Juniper, Snortsam NIPS supports real-time IP address blocking on many other software and hardware based devices both for windows and Unix / Linux based Operating Systems such as Cisco Routers, Cisco Pix firewalls, Checkpoint Firewall-1, WatchGuard Firebox firewalls, 8signs firewalls (Windows), IP Filter (ipf), Linux IPTables, MS ISA Server firewall for windows, Linux IPchains, Linux EBTables and OpenBSD's packet filter.

Many researchers have done a considerable work in the field of intrusion and detection prevention. Chang-Su Moon in [3] focuses on an integrated security system with main focus on Deep Packet Inspection (DPI). The paper proposes Network security solutions including IPS, IDSS, firewall, network access control system, integrated risk management system, and VPN. Although the paper effectively suggests the design of an integrated security system, it doesn't cover or suggest the practical implementation using any of the available open source tools.

Muhammad Naveed proposes Network Intrusion Prevention by Configuring ACLs on the Routers, based on Snort IDS alerts [4]. His research discusses prevention of intrusions using Snort IDS with Cisco routers. The research discusses intrusion detection using Snort but doesn't mention any open source IPS for intrusion prevention. The design suggested also lacks an open source console application for viewing the alerts. Bhavini Ahir in Open Source Intelligent Network Intrusion Detection System Analyzer [5] proposed an approach for analysing the log file created by Snort IDS. The proposed system basically acts upon on the log file created by Snort during intrusion detection. Various data mining

tools are used to generate reports and the reports are then analysed to update the rule base of Snort. The study proposes a manual approach to analyse logs for intrusion detection generated by open source tool Snort. This manual configuration of Security Information and Event Manager (approach of intrusion finding from Snort log files in a tedious and inefficient job. Jonathan Sweeny in his research described how one can use open source tools to create Security Information and Event Manager (SIEM) and an incident response toolkit [6]. A significant piece of this toolkit is a Security Information and Event Manager (SIEM), or the ability to store and process event logs. The study mainly concentrated on how to configure security information and event manager (SIEM). The paper covers theoretically the SIEM) and an incident response toolkit but doesn't test and implement one using any of the available open source tools. Intrusion detection and prevention in computer network is also discussed in [7], [8], and [9].

2. DESIGN OF THE PROPOSED INTRUSION DETECTION AND PREVENTION SYSTEM

Main purpose of this study was to design a real-time network intrusion detection and prevention system using open source tools. The First part was to explore and evaluate open source tools available on the web and choose the best ones for final design implementation. The second part of the research was to integrate the tools selected into real-time network intrusion detection and prevention system. Both these stages are explained in next few paragraphs.

2.1 Analysis and Selection of Open Source Tools

Selection of most suitable tools and applications is the key to the efficiency and performance of the intrusion detection and prevention. Different tools are studied and tested in virtual environment using Oracle Virtual Box before selecting them in the final design implementation.

The study proposes following tools in the design of the network intrusion detection and prevention system.

2.1.1 OS

Operating system was one of the main and critical components of this design. Since the main idea behind the design is to use open source tools, selection of operating system is carried out keeping same in mind. After studying and testing few Operating systems, Kali Linux is selected as the OS in our study. Selection of kali is carried because it has some of the pre-requisite and plugins pre-installed that are required by the NIDS and NIPS applications. Besides this installation and configuration of NIDS, NIPS, MySQL and Console application works smoothly and without any trouble on Kali Linux.

2.1.2 NIDS

Intrusion detection is the first step in securing computer networks and preventing intrusion. Some of the well-known open source NIDSs were analyzed and considered for our work such as Bro, Suricata and Snort [10]. After studying different NIDS applications, Snort was selected as the NIDS for our research based on overall performance and advantage. Although latest Snort version 2.9.7.3 was available, we used Snort version 2.5.3 in our study due to its compatibility with the NIPS application used in our design.

2.1.3 NIPS

NIPS is the part of the system that will actually block the intrusions that have been detected by the NIDS. Snort, selected as NIDS tool in our research, can also be used and configured as an NIPS. However, when using Snort as an IPS, it is configured as Inline NIPS. Snort can be used as Inline NIPS and integrated with IPTables on Linux systems. However we are not using Snort as Inline IPS since there are some issues associated with this approach. In this approach the Linux system running IPTables has to placed and configured as the gateway of the network. Although this is an acceptable option but generally routers or firewalls from Juniper, Cisco and Linksys are much faster gateways as compared to IPTables running on Linux system. These routers and firewalls are easy to troubleshoot and require very less maintenance and support.

Because of the above limitations, we are using another more flexible NIPS tool, SnortSam for our design. SnortSam is more flexible and easy to use as compared to IPTables.

SnortSam will send the intruder's source IP addresses to firewall for blocking in real-time. Currently the SnortSam supports automatic blocking of IP addresses on following firewalls [11].

- Cisco Routers
- Juniper's Netscreen firewalls
- Cisco Pix firewalls
- Checkpoint Firewall-1
- WatchGuard Firebox firewalls
- CHX Packet filter
- 8signs firewalls (Windows)
- IP Filter (ipf)
- Linux IPTables
- MS ISA Server firewall for windows
- Linux IPchains
- Linux EBTables
- OpenBSD's packet filter (pf)
- FreeBSD's ipfw2

Besides automatic blocking of IP addresses, SnortSam NIPS has other features and capabilities such as:

- Email notification and file logging of events
- It supports TwoFish encrypted communication from Snort and itself during the blocking request by SnortSam output plugin.

- It supports multi-threading for fast processing and simultaneous blocking on many devices.
- The agent support White-list, IP addresses that are never blocked.
- It supports a mechanism to stop repetitive blockage of same IP addresses with a customizable windowing for improving performance.
- An SID filter list of allowed or denied SIDs based upon reporting entity.
- It supports a time over ride list.
- Flexibility of per rule blocking specification.
- Maximum and minimum block time ceiling for reporting entities.

2.1.4 Analysis Console

By default, Snort stores the intrusion detection alerts in a log file on the same system on which it is configured. Although this approach is simple to configure and use, it is not user friendly to view alerts in a text file especially when the file is several hundreds or thousands lines long. To make this process more flexible and user friendly, a separate console application is proposed in our study for viewing the alerts. We propose an open source Database application MySQL to store the Snort alerts. Primarily Snort stores the alerts to a log file locally. Another open source application Barnyard2 is used to store the alerts from log file to MySQL Database [12]. A console application is used to view the alerts from MySQL Database in a Web Browser. Following are some of the well-known console products that we analyzed for usage in our design [13].

1. ACID
2. SGUIL
3. SNORBY
4. BASE

Based upon our analysis and overall advantage, we chose BASE (Basic Analysis and Security Engine) as our console application in our design. BASE is written in PHP and is basically derived from the code of ACID console which is now almost obsolete [14]. Following are the some of the advantages and reasons, based upon which we chose BASE as the console product for our design.

- BASE is one of the most widely used open source console for Snort NIDS.
- BASE has a large user base and support manuals are available for configuration with Snort.
- It is very user friendly and can be used with any modern day Web browser.
- BASE has the capability to view and generate alerts using different criteria such as source or destination IP addresses, source or destination ports etc.

2.2 System Design and Integration

The tools and applications selected in the first part of our study are integrated into one cohesive network intrusion detection and prevention system as show in Fig 1. That system can be effectively and efficiently used by small and medium sized organizations for the security of their networks.

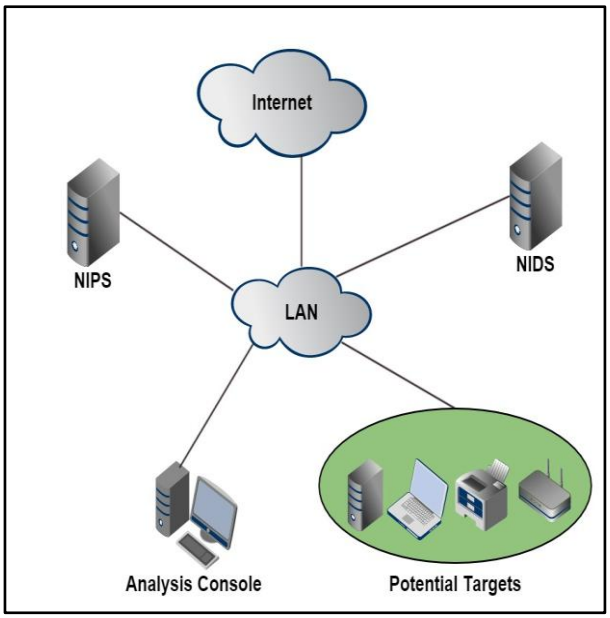

Fig. 1 System Design and Integration

Juniper's Networks devices, EX-3200 Switch [15] and SSG 20 Firewall [16] are used to connect and configure the traffic flows between all the components of the system. The connectivity between different components of the system using Juniper Networks Switch and Firewall is shown in Fig 2. Snort NIDS checks for any intrusion in the network traffic. Any intrusion detected by Snort NIDS is logged in MySQL Database and sent to SnortSam Firewall agent. SnortSam Firewall agent sends the intruder's IP address to the Juniper's Firewall for blocking. The mechanisms used for intrusion detection and prevention processes are explained further in the next paragraphs.

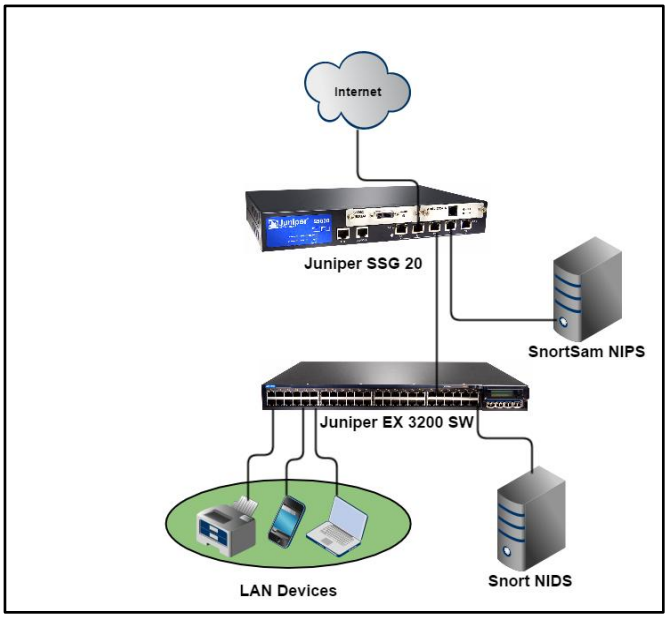

Fig. 2 Network Connectivity Diagram

2.2.1 Network Intrusion Detection

Snort is used as NIDS and is installed on Kali Linux OS. All the incoming and outgoing traffic is passed through the Snort NIDS using port mirroring on Juniper EX 3200 Switch.

Traffic generating from the within the LAN is also checked for intrusion detection which allows the detection of internal attacks and organization's own compromised devices that are zombies and part of Botnets. Any intrusion detected by Snort is stored in MySQL Database and sent to NIPS for blocking. The alerts and intrusions stored in MySQL Database can be viewed using the BASE console front end application in a web browser. Apache Web server was used on Kali Linux which enabled the console application to show alert in Web browser. Latest Snort rules were used for intrusion detection; however it is recommended that Snort rules are fine tuned to prevent false alerts generation.

2.2.2 Network Intrusion Prevention

This part of the system blocks any intrusion that is detected by Snort NIDS. SnortSam consists of two pieces of applications.

- SnortSam output plugin
- SnortSam firewall agent

2.2.2.1 SnortSam Output Plugin

The SnortSam output plugin is configured within Snort NIDS. We used the SnortSam output plugin version snortsam-2.9.5.3 keeping in mind our Snort version of Snort-2.9.5.3 to avoid any issues and problems during installation and configuration. The SnortSam output plugin is triggered when an intrusion is detected by Snort and sends information about the intrusion to SnortSam firewall agent for blocking.

2.2.2.2 SnortSam Firewall Agent

The SnortSam firewall agent resides on a host near the firewall. The SnortSam firewall agent listens for the blocking requests from the SnortSam output plugin and forwards it to the Juniper's firewall for blocking. The blocking request generated contains source IP address of the intruder and the command to login into the firewall and block the IP address from accessing the network.

2.3 Interface between NIDS and NIPS

Snort NIDS uses thousands of its rules for known intrusions. To enable SnortSam IPS blocking action for a particular attack, the detection Snort rule for that attack must be modified as show in Fig. 3. The modified rule includes the call to the SnortSam output plug-in. This rule tells SnortSam Output plugin to send a blocking request to SnortSam firewall agent for blocking the source IP address for the specified interval of time (5 minutes). This mechanism integrates NIPS and NIDS functionalities in our design. Instead of source (src), destination IP address or both source and destination IP addresses can be blocked.

Original Rule:

```
$HOME_NET any (msg:"SCAN nmap XMAS"; flow:stateless; flags:FPU,12;
reference:arachnids,30; classtype:attempted-recon; sid:1228; rev:7)
```

Changed Rule:

```
$HOME_NET any (msg:"SCAN nmap XMAS"; flow:stateless; flags:FPU,12;
reference:arachnids,30; classtype:attempted-recon; sid:1228; rev:7; fwsam: src, 5 minutes;)
```

Fig. 3 Interface between NIDS and NIPS

3. EXPERIMENTAL SETUP

The systems used in the implementation and experimental setup are show in Table 1. Mainly three laptops were used for implementation and experimentation. Out of these three laptops, one was used as the NIDS system on which Snort version 2.9.5.3 GRE (Build 132) on top of Kali Linux OS Version 1.1.0 was installed. MySQL and BASE Version 1.1.3 console applications were also installed on this system. The second system was used as the NIPS on which SnortSam firewall agent was installed on Kali Linux Version 1.1.0 OS inside Virtual Box. Main OS on this system was Windows 7. The third system was used as attacker for testing and experimenting the working and setup of the whole design.

Table 1. Hardware And Software Specifications

System	CPU	RAM	Hard Drive	OS	Applications
NIDS System	Core i3	2 GB	40 GB	Kali Linux	Snort , BASE, MySQL
NIPS System	Core 2 Duo	2 GB	40 GB	Win 7, Kali Linux	SnortSam V2.9.5.3
Intruder testing	Core 2 Duo	2 GB	20 GB	Win 7	-

4. CONDUCTION OF EXPERIMENT

Snort NIDS use rules for detection of attacks and anomalies. These rules are available online on snort official website and can be downloaded for Snort. The latest rules set downloaded for use in this design contains 27766 rules. These rules require fine tuning before deploying in an organization production environment to avoid false alarms generation.

To check the working of our system, we used a single ICMP rule for the sake of simplicity as show below. Instead of 27766 rules file, Snort was loaded with another file that contained the rule for detection of only ICMP Ping. The rule was used to check both the NIDS and NIPS functionalities of the system as shown below. The first line shows the ICMP traffic detection rule while the second line shows the modified rule having NIPS functionality depicted by bold words.

alert icmp any any -> any any (msg:"ICMP"; sid:10; rev:001)

alert icmp any any -> any any (msg:"ICMP"; sid:10; rev:001; ***fwsam: src, 5 minutes****;)*

5. RESULTS

As already discussed, there are thousands of Snort rules for known attack signatures and traffic anomalies. Many of these rules contain false alarms and require fine tuning before deployment to avoid legitimate traffic blocking. Initially traffic was passed through Snort IDS using the default rules set containing 27766 rules. The alerts detected by Snort are shown in Table II.

Table 2 Snort Alerts

Signature	No. of Packets	%age of Total Traffic
Sensitive data e-Mail address	3	1 %
Reset outside window	65	24 %
TCP small segment threshold exceeded	62	23 %
Data sent on stream after TCP reset	30	11 %
Bad Segment	4	1 %
Unknown method	24	9 %
Long header	1	0 %

The Snort NIDS was then run with the single ICMP rule. A target system was pinged from another attacking PC in the network, without first running the SnortSam NIPS system. The Snort logged the ICMP alerts to MySQL database. These alerts are viewed in browser using BASE console application as shown in Fig. 4.

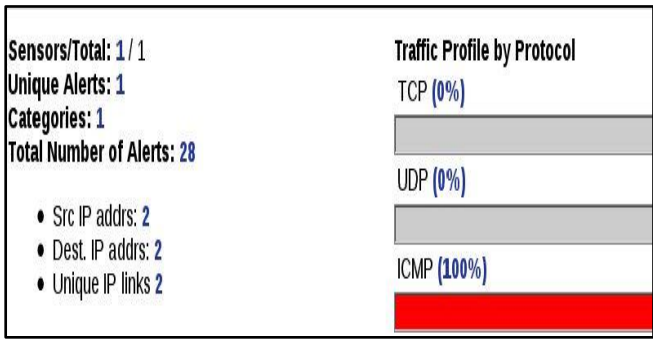

Fig. 4 BASE application showing Snort ICMP alerts

The SnortSam NIPS system was then turned on and SnortSam firewall agent was run. The SnortSam firewall agent sent the IP address of the attacker's PC to SSG 20 Firewall for blocking. The attacker's IP address was blocked and the attacker PC was no longer able to ping the target pc. Snapshot taken from Juniper's firewall lists the blocked IP addresses of the attacker shown in Fig. 5.

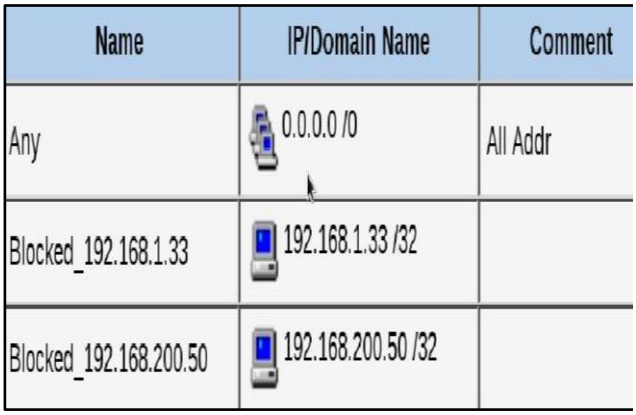

Fig. 5 Blocked IPs inside Juniper Firewall by SnortSam NIPS

6. CONCLUSION

Using open source tools and application provides an easy and cost effective way to design a network intrusion detection and prevention system. The system can be incorporated with any modern day switch and firewall that are already present in an organization network. The proposed system will provide a necessary security to an organization network provided the snort rules are fine-tuned as per the organization requirements.

The system has its advantages but few shortcomings too. The system detects the intrusion after few packets have already reached the target system. Hence intrusions within the first single or few packets can intrude the target system. The system was tested using static IP addresses and may not work with DHCP configuration in a network.

The system can be extended for large networks by using many NIDS and NIPS sensors. The system can also be used with software based firewall applications without the use of hardware firewall.

7. REFERENCES

[1] J. Gomez, C. Gil and N. Padilla, "Design of a Snort based Hybrid Intrusion Detection System" *International Work-Conference on Artificial Neural Networks*, , Salamanca, Spain, June 10-12, 2009, pp. *515-522.*

[2] Mike Smith, "A Design for Building an IPS Using Open Source Products," in *Sans Institute Information security reading room.*

[3] Chang-Su Moon and Sun-Hyung Kim. (*2014*). Integrated Security System based Real-time Network Packet Deep Inspection. *International Journal of Security and Its Applications,* pp. 123–135.

[4] Muhammad Naveed, "Network Intrusion Prevention by Configuring ACLs on the Routers, based on Snort IDS alerts," in *International Conference on Emerging Technologies*, Islamabad, 2010, pp. 234-239.

[5] Bhavini Ahir, Prache Tambakhe and Dr. Kalpesh Lad. (2012, December). Open Source Intelligent Network Intrusion Detection System Analyser. *Indian Journal of Applied Research.* [online]. *2(3).* Available: http://www.worldwidejournals.com/ijar/articles.php?val=ODY3&b1=109&k=28

[6] Jonathan Sweeny and Rob VandenBrink. (2011, June). The SANS Institute: Creating your own SIEM and Incidence Response Toolkit using open source tools. [online] Available : https://www.sans.org/reading-room/whitepapers/incident/creating-siem-incident-response-toolkit-open-source-tools-33689+&cd=1&hl=en&ct=clnk&gl=pk

[7] S. Vikrama Teja, S. Kranthi Kumar, T.V. Rao, G.Dayanandam. (2013, August). In-line Prevention System using Snort. *International Journal of Application and Innovation in Engineering management.* [online]. *2(3).* Available*:* www.ijaiem.org/volume2issue8/IJAIEM-2013-08-31-083.pdf

[8] N. Akhyari and S. Fahmy. (2014, January). Design of a Network Security Tool Using Open-Source Applications. *Australian Journal of Basic and Applied Sciences.* [online] . *8(4).* Available: http://connection.ebscohost.com/c/articles/95511258/design-network-security-tool-using-open-source-applications

[9] Sutapa Sarkar and Brindha.M. (2014, Julyl). High Performance Network Security using NIDS Approach. *International Journal of Information technology and Computer Science.* [online]. 6(7) . pp. 47-55. Available: www.mecs-press.org/ijitcs/ijitcs-v6-n7/IJITCS-V6-N7-7.pdf

[10] Joe Schreiber, "Open Source Intrusion Detection Tools: A Quick Overview" https://www.alienvault.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview

[11] Frank Knobbe, "SnortSam, A firewall blocking agent for Snort" SnortSam setup guides http://www.snortsam.net

[12] Noah Dietrich, "Snort 2.9.7.x on Ubuntu 12 and 14 with Barnyard2, PulledPork, and BASE". https://www.snort.org/.../snort-2-9-7-x-on-ubuntu-12-lts-and-14-lts

[13] Joel Else (2011). "GUIs for Snort IDS, The Official Blog of the World Leading Open-Source IDS/IPS Snort" GUIs for Snort http://blog.snort.org/2011/01/guis-for-snort.html

[14] Rafeeq Ur Rehman, "Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID", Bruce Perens's Open Source Series, 2003, Chapter 6.

[15] Juniper Networks EX Series Ethernet Switches http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/ex-series/product/

[16] Juniper Networks SSG 20 http://www.juniper.net/us/en/products-services/security/ssg-series/ssg20/