

ADA University
School of Information Technology and Engineering



Senior Design Project

FINAL REPORT

Project Title: **Automated Cybersecurity Event Analysis**

Authors:

1. Nuray Gurbanova [CS]
2. Azarin Bayali [CS]
3. Gabil Gurbanov [CS]

Project Advisor: [ADA, Instructor] Nariman Aliyev

Industry Mentor: [Code Academy] Natig Zeynalzade

Industry Mentor: [ADA, Lead Infrastructure Manager] Orkhan Mammadov

Baku, May 2024

Table of Contents

LIST OF FIGURES.....	3
ABSTRACT.....	4
1. INTRODUCTION.....	4
1.1 DEFINITION	4
1.2 PURPOSE	5
1.3 PROJECT OBJECTIVES, SIGNIFICANCE, NOVELTY.....	6
1.4 PROBLEM STATEMENT	8
2. LITERATURE REVIEW	9
2.1 A FIREWALL: WHAT IS IT?	9
2.2 TIMELINE: FIREWALL IN THE 80S	9
2.3 TIMELINE: FIREWALL IN THE 90S	9
2.4 TIMELINE: FIREWALL SINCE 2000	10
3. DESIGN CONCEPTS.....	11
3.1 ALTERNATIVE SOLUTIONS	11
<i>Network design alternatives</i>	<i>12</i>
<i>Security tool alternatives.....</i>	<i>13</i>
3.2. DETAILED DESCRIPTION OF TECHNOLOGIES OF CHOICE	14
<i>VMWare Workstation.....</i>	<i>14</i>
<i>OPNsense firewall</i>	<i>14</i>
<i>Wazuh.....</i>	<i>26</i>
<i>Splunk (SIEM).....</i>	<i>29</i>
3.3. ENGINEERING STANDARDS (IF APPLICABLE)	32
<i>ISO/IEC 27001 Controls implemented:.....</i>	<i>32</i>
<i>NIST Controls implemented:</i>	<i>33</i>
3.4. RESEARCH METHODOLOGY AND TECHNIQUES	34
3.5. ARCHITECTURE, MODEL, DIAGRAM DESCRIPTION	35
<i>Diagrams.....</i>	<i>37</i>
3.6. ECONOMIC ANALYSIS	40
4. IMPLEMENTATION.....	41
4.1. HARDWARE DESIGN	41
<i>OPNsense</i>	<i>41</i>
<i>Staff and Client Servers.....</i>	<i>42</i>
<i>Splunk Server.....</i>	<i>43</i>
<i>Wazuh.....</i>	<i>44</i>
<i>Student Kali Machine</i>	<i>44</i>
<i>DMZ interface Servers</i>	<i>45</i>
4.2. ESSENTIAL COMPONENTS OF THE PROJECT	45
4.3. TIMELINE OR GANTT CHART	49
4.4. TESTING/VERIFICATION/VALIDATION OF RESULTS	49
<i>Wazuh Testing:</i>	<i>49</i>
WHAT ACHIEVED:.....	53
BEFORE:	53

AFTER:	53
5. CONCLUSION	53
5.1 DISCUSSION OF RESULTS	53
5.2 FUTURE WORK	54
6. ACKNOWLEDGEMENT	54
7. REFERENCES	54
8. ABBREVIATIONS	54

List of Figures

FIGURE 1: ARPANET INFRASTRUCTURE, MARCH 1977	7
FIGURE 2: OPNSENSE GUIDELINE BOOK	11
FIGURE 3: QUESTIONNAIRE IN REDDIT PLATFORM AND SPLUNK EMPLOYEE RESPONSE	12
FIGURE 4: VMWARE WORKSTATION PRO VIRTUALIZATION VERSION17	14
FIGURE 5: NTOPNG LIVE TRAFFIC MONITORING	16
FIGURE 6: THE STORAGE SPACE BEING USED	16
FIGURE 7: DESCRIPTION ANOMALIES AND MTU	17
FIGURE 8: DEFAULT HTTPS PORT CHANGING IN THE FIREWALL	18
FIGURE 9: ENABLING NGINX PLUGIN IN FIREWALL	18
FIGURE 10: UPSTREAM SERVER SELECTION	19
FIGURE 11: ADDING A WEB SERVER AS AN UPSTREAM SERVER	19
FIGURE 12: VERIFICATION OF UPSTREAM	20
FIGURE 13: SUCCESSFUL CONFIGURATION OF UPSTREAM	20
FIGURE 14: WEB ATTACK FLOWS	21
FIGURE 15: IMPLEMENTING PROTECTION RULES FOR SQL INJECTION IN WAF	22
FIGURE 16: ESTABLISHMENT OF WAF MODULE NAXSI	23
FIGURE 17: HTTPS LOCATION CONFIGURATION	24
FIGURE 18: HTTPS MONITORING	25
FIGURE 19: WAZUH WORKING PRINCIPLE	26
FIGURE 20: WAZUH INTEGRITY MONITORING	27
FIGURE 21: WAZUH SECURITY CONFIGURATION ASSESSMENT	28
FIGURE 22: WAZUH SSH HARDENING	28
FIGURE 23: SPLUNK MOBILE DASHBOARD	31
FIGURE 24: SPLUNK MOBILE WIDGETS FIGURE 25: SPLUNK MOBILE TICKETING	31
FIGURE 26: SPLUNK TICKETING INTEGRATION WITH SLACK	32
FIGURE 27: DETAILED CAMPUS TOPOLOGY	37
FIGURE 28: OPNSENSE WORKFLOW	37
FIGURE 29: NTOPNG WORKFLOW	37
FIGURE 30: SYSTEM INFRASTRUCTURE AND GPO RELATIONS	38
FIGURE 31: WAZUH WORKFLOW	38
FIGURE 32: RELATION TO HOW SPLUNK WORKS WITH OPNSENSE, WAZUH AND SLACK	39
FIGURE 33: RELATION BETWEEN WAF AND OPNSENSE	39
FIGURE 34: RELATION BETWEEN SPLUNK, OPNSENSE AND SLACK	40
FIGURE 35: VMNET AND IP CONFIGURATIONS	42
FIGURE 36: MEMORY AND RAM USAGES	42

FIGURE 37: STAFF SERVER DETAILS	FIGURE 38: CLIENT SERVER DETAILS.....	43
FIGURE 39: SPLUNK MEMORY AND RAM USAGES		44
FIGURE 40: WAZUH MEMORY AND RAM USAGES.....		44
FIGURE 41: KALI MACHINE DETAILS		45
FIGURE 42: WEB SERVER DETAILS	FIGURE 43: MAIL SERVER DETAILS.....	45
FIGURE 44: SPLUNK ALERT TICKETING SYSTEM		47
FIGURE 45: GANTT CHART		49
FIGURE 46: CHANGING SSH PORT		49
FIGURE 47: SSH PORT CONFIGURED TO 2244.....		50
FIGURE 48: VERIFICATION OF PORT CHANGE		51
FIGURE 49: VERIFICATION OF PORT CHANGE		51
FIGURE 50: TIME INTERVAL OF SCANNING MACHINE		52
FIGURE 51: VALIDATION OF SCI REPORT		52

Abstract

ABSTRACT - The project “Automated Network Analysis” examines campus network topology and integrates the implementation of both Data Analytics and Cybersecurity fundamentals including offensive and defensive strategies. Besides the establishment of virtual campus network topology and execution of cyberattacks, the project aims to implement best practices evolving rulesets, mitigation tools, and to automate the detection phase. “Automated Network Analysis” brings a clear view of automation monitoring in the network and achieves to identify various threats with precise rates. The development period combined experimentation of several technologies to determine significant distinctions and the most suitable services for the topology. Researching best practice methods against popular vulnerabilities for campus network topology led to finding optimal solutions to mitigate them with low cost of MTTR of technical scope and business cost. The project contributes to network security by enlarging the threat detection capabilities of the system.

1. Introduction

1.1 Definition

Every organization has a network topology that ensures business continuity. From small such as coffee shops to large companies start their businesses by designing and implementing the network infrastructure. In every organization, devices that are operating for the company should have a centralized management point to serve according to the needs of that

specific organization. Additionally, for an organization to be organized, it should have identified types of members that are in the network meaning categorization of the people based on their role and importance level. As a security backbone CIA triangle is introduced to identify security threats and categorize them. In campus network topology we divided the staff and student categories as distinct servers to measure their role in the network and give system permissions according to the significance of their role. The group of the users that are given higher permissions due to their administrative roles has been targeted in the attacks mostly. The logic of the attacker behind this action is to exfiltrate data and take advantage of sensitive information. From another point of view, we suppose mentioned critical attack vectors are protected securely for most type of attacks, and we consider other parts of the network infrastructure that have access to the outside of the network. The part of the network that is contained with internal servers (Web and Mail servers), in our case, is called DMZ meaning that a specific portion of the network infrastructure needs to have access to the outside of the network the services may include FTP servers, DNS servers, mail servers, web servers and so on can be covered according to the network topology. DMZ as mentioned above is a combination of network components that should have access to the external network which brings the possibility of various attack types with itself. Moreover, to become aware of and mitigate attacks the network should be analyzed and determine critical threats that vulnerabilities may lead to. Besides the internal threats, external threats targeting the availability portion of the CIA triangle are the most common type of attacks occurring in the campus network infrastructure. Examples of these attack types include DoS/DDoS, DNS amplification, application layer attacks, physical attacks, etc. Indicated attack types may lead to system crashes and downtime affecting financial position, loss of productivity, and loss of reputation of the organization.

1.2 Purpose

Every network topology belonging to a specific organization needs to be designed well considering scalability, performance requirements, redundancy, availability, security, cost, efficient management, compliance, and documentation. Organizations may grow and spread around various geographical places, in this case, network scalability should be available to the company to continue its operation successfully as it was before. Moreover, scalability refers to the ability of network topology to handle business growth and increased demand without compromising performance, reliability, or efficiency. It covers both vertical scalability which is adding more resources to the existing network component, and horizontal scalability which is meant to add additional devices to the network. Performance requirements in network topology design include supporting smooth experience for devices that are connected to the network with an identified speed rate which is required for continuity of the bandwidth efficiency. Another significant term mentioned is redundancy, which is about adding redundant resources or links to guarantee network infrastructure is backed up and provides failover capabilities. In IDS/IPS

system architecture, availability is the capacity of a network service to have low MTTR and high durability for user applications. To accurately reflect MTTR, these metric measures downtime as a percentage of total operational time within a specific period. Security, which we focused on mostly, is aimed at protecting sensitive data, preventing unauthorized access ensuring the confidentiality, integrity, and availability of the network resources or components. To provide network security, several measures need to be taken to mitigate risks, vulnerabilities, and threats which is crucial to provide secure network infrastructure. One of the most widely used mitigation methods includes the configuration of IDS systems as mentioned before in network infrastructure. An IDS monitors network traffic, system logs, and events in real-time to alert incidents or anomalies in the network. By developing a customized IDS, dedicated to our network structure, which is the university campus network topology, our purpose is to increase the security posture and durability of the constructed network topology. The customized IDS system is established and configured to meet campus network demands including its student and staff base and whole traffic patterns.

1.3 Project Objectives, Significance, Novelty

Our project objectives are as follows:

- Construction of common campus network topology
- Identification of DMZ zone
- Establishment of a dedicated IDS system for campus network topology
- Reduce constant security incidents by network log analysis, deployment, and integration
- Create from scratch ticketing system that shows alerts with log statistics and link pointer to the Splunk

In current era, the implementation of network topology is crucial for all countries including Azerbaijan. The carefully configured network infrastructure contains a base for the utilization of technology in our daily lives. Network infrastructure determines the specific local or wide area and devices that are belonging these areas. It maintains the organization and allows everyone in OU to be able to perform specific tasks and communicate with each other. Network devices changed over time relatedly based on shifting new devices and physical layer technologies security threats also evolved and changed during this period. The first constructed network is called ARPANET which adopted a communications model designed and developed by Robert Kahn and Vinton Cerf in 1983.

ARPANET LOGICAL MAP, MARCH 1977

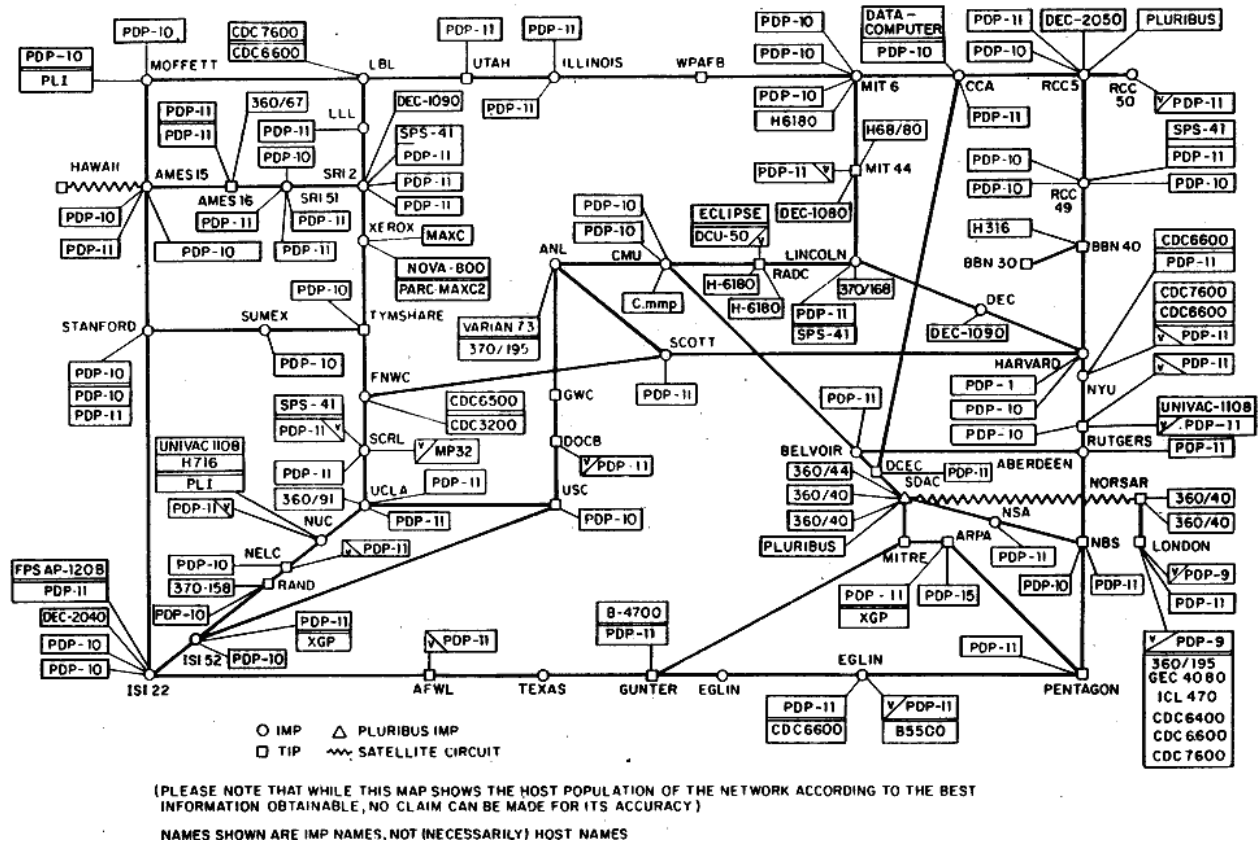


Figure 1: ARPANET infrastructure, March 1977

From their initiation, the modern internet was born. As mentioned, if we have a technology, it means we have threats as well. The first attack which is occurred 5 years after the establishment of the first network, called “The Morris Worm” named after the implementer Robert Tappan Morris. The novelty that we initiate is to have Automated Data Analytics to IDS system based on the network infrastructure. According to network topology, our IDS system can recognize anomalies of certain attacks and create a ticket. To achieve this, we simulate the specific types of common attacks occurring in campus network topology and collect traffic logs by doing so, our system achieves to identify patterns namely the type of attack.

1.4 Problem Statement

There are several obstacles facing today's network architecture in businesses, especially university campus networks, especially when it comes to availability assurance inside the CIA triangle. Modern networks are so sophisticated that they require a strong security architecture to protect against a variety of internal and external attacks. Attacks that aim to compromise network resource availability continue to exist despite attempts to strengthen network security, posing serious hazards to organizational continuity and operations.

Example Situation Case: To best illustrate the development of our college during the difficult times of the COVID-19 pandemic, we need to speak about a quick shift to a remote learning style. Fewer face-to-face interactions result in less time for the professors to monitor students which may lead to deterioration in the success of students. The sudden switch is a stunt that unveiled the weak points of the present structure of cybersecurity and showed that the university has turned to be a target to the propagation of cyberattacks. DDoS attacks and brute-force login attempt of distributed seemingly parallel technologies brought core university functions to corrupt, rather than had been just a side-effect due to a consequent domino effect. The issue also affected the University staff, for example Security and IT characteristics, and instructors; due to these disruptions, they were not as effective in supporting the virtual slate as they should. Insufficiency of the current monitoring protocols was demonstrated when these were unable to efficiently cope with the growing problem. This demonstrated an evident security need for a SIEM solution that would add up to the initial security configuration procedures, helping avoid vulnerabilities and subsequently recover from an attack as quickly as possible.

The alarming issue is associated with attack conducts that are often in the field of acting on the availability knob of the CIA components. Classification of user networks not only constitutes a lack of protection that is manifested by attacks unabated, but also does it lead to the Head Zone demilitarization to keep core assets protected. The internal network infrastructure is an area in the TCSP environment which can often be forgotten about while focus most directly outside threats. These failures have enabled the hackers to utilize them for targeting groups of users who possess a high rank of authorities to obtain administrative permissions and ultimately, they might have secret sensitive content in their possession. the fact that although the attacks are happening the intrusion detection system, is put in place to deal with the matter, the architectural design of the network, separates the institution from the rest points out on the importance of the comprehensive analysis of threats and the mitigation measures to be taken. The matter of boosting network resilience within university campus networks is not only the issue of ensuring continuous uptime of the devices, but rather a problem of understanding both internal and external vulnerabilities, running proactive security tests, and finally implementing targeted measures.

This would be made possible by its system-based approach which would ensure the security as well as safety of the virtual environment, thereby safeguarding the academic environment of students and staff alike.

2. Literature Review

Probably, the most distinct part of infrastructure in information security is a barrier. One hears this word a lot in this industry. Along with that, it is understandable that during the time the view has changed from much to very less, the concept has not. In the business context the basics of perimeter security to protect mission critical assets e.g., firewalls have been a part of business environments even aside with the advancement of various capabilities in this industry.

2.1 A firewall: what is it?

All that a firewall is a concept applied to software, or a combination of hardware and software, with the goal of providing security features and network connections by controlling all traffic going through it in accordance with pre-established regulations. Also, a firewall has an advantage over a traffic-tunneling architecture that is strategically located since it may permit or prohibit communication continuity if it doesn't provide an inconsistent or dangerous risk to the network. In many kinds of enterprises, firewalls are a common security measure. They are usually positioned in a topology between private networks (internal network segments) and public networks (the Internet). Realization of the challenges that have emerged throughout time and how the market and business have changed and developed into a better business model for a world that is becoming more linked is possible by having an overview of the past.

2.2 Timeline: Firewall in the 80s

A firewall is not a novel idea; its intrinsic qualities helped it gain popularity along with the growth of the TCP/IP protocol stack. IP presents a danger of unwanted access, data breach, and other scenarios because of its interoperable nature, which leaves networks with disparate functions or domains (businesses, academic institutions, etc.) without any oversight. So, establishing a wall between the public and private network segments—which are overseen by major telecom firms and local providers—and the public portion of the Internet's interconnection constitutes perimeter security. Information is sent from one location to another via packets in computer networks. Every packet is a unit that is autonomously routed via the Internet and comprises data (content) and a piece of identifying information (header). Jeff Mogul of Digital Equipment Corp. (DEC) developed the initial idea for a firewall, or packet filter, in 1989; this was the first generation of firewalls.

2.3 Timeline: Firewall in the 90s

In 1991, Steve Bellovin and Bill Cheswick assisted AT&T Bell Labs in developing the initial idea for what would eventually be referred to as stateful packet filtering, or simply stateful firewall.

This phase was identified as the firewall's second generation. The third generation of firewalls quickly appeared with the commercialization of DEC SEAL for its contemporary application proxy features. The term "hybrid firewall" is becoming more used in the industry and in academic circles due to the integration of packet filtering and proxy servers into a single system. Checkpoint introduced Firewall-one in 1994, which had a significant impact on the growth of the security industry, the inventive GUI idea, and other security-related technology. A few similar initiatives, including Squid (1996) and Snort (1998), emerged in the second part of the 1990s. These projects' primary objective was the gradual development and maturity of concepts and solutions rather than their commercialization. Both free and commercial security solutions still make extensive use of these programs today. Simultaneously, more firms formed, and the systems received enhancements with additional security measures, therefore becoming ever more hybrid. With the help of features like VPN, URL filtering, quality of service, antivirus integration or inclusion, WAF, and other solutions, organizations can now create environments that are more reliably secure.

2.4 Timeline: Firewall since 2000

The acronym UTM (Unified Threat Management) was initially used by IDC in 2004 with the introduction of new security solutions for firewalls. This phrase is the perfect way to describe how firewalls have changed throughout time. Numerous apps and services started to consolidate their operations on the network because of the Internet's growing popularity. Because of this change, it is now much more important to safeguard certain HTTP-based systems. Web application firewalls (WAFs) first appeared as a stand-alone product in 2006, but they were also made available as a UTM resource. Despite being well-known for integrating a variety of features and security measures into a single solution, UTMs' high resource requirements hindered their performance. Palo Alto Networks introduced Next Generation Firewalls (NGFW) to the market in 2008. NGFWs solve the UTM performance issue and add an essential feature: application-based visibility and control. Gartner then went on to identify the next generation of firewalls in 2009. To stay up to date with the trends they want to follow in the upcoming years, several providers have undergone both technical and commercial adjustments. As with NGIPS, many other known features have been updated to the next generation, the majority of which are exclusively available for purchase. The Internet has been a major factor in the convergence of information and knowledge in the electronic world over the past few years, which has resulted in significant changes to the technology supporting firewall solutions. The Internet of Things (IoT) will undergo significant changes in the upcoming years, along with a host of other new difficulties for mobile devices, which are currently extensively used in business settings. The construction of history never ends.

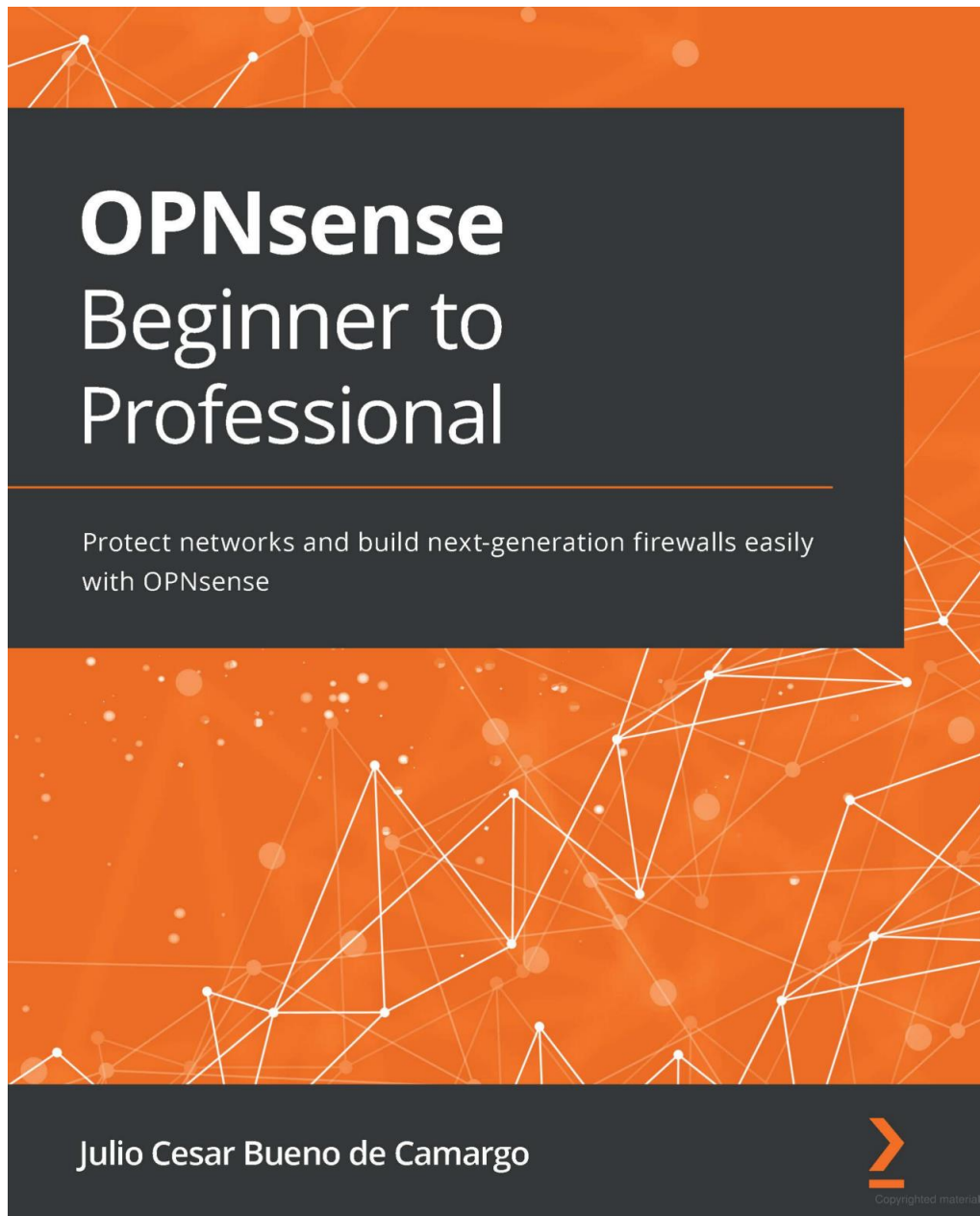


Figure 2: OPNsense Guideline Book

3. Design Concepts

3.1 Alternative Solutions

When it comes to fortifying network infrastructure, various strategies and technologies there are other approaches and technologies for achieving secure network infrastructure. Although technologies and approaches that are used in the project are highly satisfactory from our side, research of the alternative solutions helped us to improve our knowledge of cybersecurity.

Network design alternatives

For virtualization of all machines, we utilized VMware Workstation, particularly for user friendly configurations. However, alternative virtualization technologies include Oracle VM VirtualBox or Xen project. Xen project is known for its high performance in server virtualization scenarios. Both Oracle VM VirtualBox and Xen project are open-source virtualization solutions. However, the Xen project is considered to be complex to configure because of the lack of user-friendly interface. Moreover, Oracle VirtualBox even though can run on various operating systems like windows, macOS, Solaris, basic configurations like network or bridged network configurations are complex enough. For firewall we initially used Pfsense, where our biggest advantage was rich availability of documentation options for Pfsense. OPNsense on other hand, is a new version of Pfsense, thereby there are very few documentations available for it. However, this made us true explorers, while digging into newer and updated features of OPNsense from Pfsense. Furthermore, we conducted a discussion on Reddit platform for integrating OPNsense with Splunk, since we could not find valid documentation about it.

Our post in reddit which is a great platform for open-source project discussions. Integration of Splunk to OPNsense: “I wonder if there's any method to connect/link OPNsense to Splunk Enterprise so that main network activity logs are visible in Splunk Dashboard. I need all network logs to be indexed and represented in table view or visually. If there's any method, proper guidance would be appreciated. I heard there were Add-on/Plugin for Splunk Enterprise. However there's no addons or plugins in the marketplace for extensions in "SplunkBase" (Like Play Market for Android or AppStore for iOS for those who aren't familiar) I even checked old manual for configuration, which is dependent on Plugin/Add-on which doesn't exist. Here's the link: <https://splunk-opnsense-la.ztsplunker.com/> Thanks beforehand”

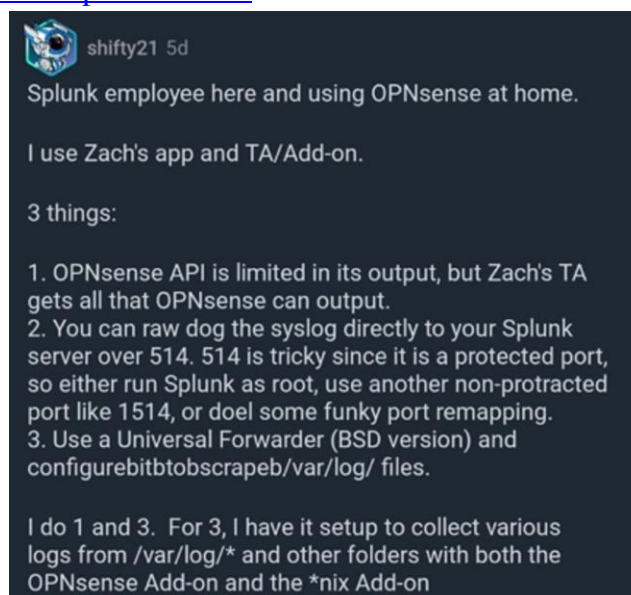


Figure 3: Questionnaire in Reddit Platform and Splunk Employee Response

src:https://www.reddit.com/r/opnsense/comments/1c9oj2x/integration_of_splunk_to_opnsense/

As a vulnerable web server, we used a JuiceShop, which was interesting to exploit. An alternative Webgoat could be used, which is like JuiceShop vulnerable web application and as useful as JuiceShop to perform a wide range of web application attacks for learning and testing purposes. Similarly, DVWA (Damn Vulnerable Web Application) can be used for simulating web-based penetration testing. Webgoat and DVWA are both supported by OWASP, which is a strong community of security professionals. However, Webgoat is requiring regular maintenance to address updated security flaws, whereas DVWA was very simplistic for simulating penetration testing attacks.

Security tool alternatives

In our topology we configured WAF service inside OPNsense firewall to secure web application servers. This allows centralized management and configuration of firewall rules, including WAF rules, within the OPNsense administration interface. Deploying Nginx with a WAF module involves setting up and configuring Nginx web server software on a standalone machine or virtual machine and can be an alternative way of setting up a WAF for Web Server. This way WAF functionality is provided by a third-party module, so-called ModSecurity, which must be installed and configured separately from Nginx.

In our infrastructure, we integrated Splunk with OPNsense firewall providing powerful capabilities for monitoring and analyzing network security events. Splunk offers a wide range of data analytics and monitoring solutions beyond SIEM. Moreover, it provides comprehensive documentation, training resources, and community support for users. Developed by IBM, QRadar is a dedicated SIEM solution within IBM's security portfolio. Splunk's licensing model is based on data volume indexed, with options for term-based licenses. QRadar's licensing model typically includes appliance-based pricing, where users purchase hardware appliances or virtual machine licenses based on the size and capacity of the deployment. This makes Splunk more advantageous than QRadar. For integrity monitoring we used Wazuh, one of the most powerful Open-Source SIEM tools, with its wide range of documentation. Wazuh dashboard and Wazuh indexer are applications based on OpenSearch Dashboards and OpenSearch distributions, which are forks of Kibana and Elasticsearch (v7.10.2). However, Elasticsearch itself can be used as an alternative SIEM tool for Wazuh. Among other alternatives of Wazuh are Splunk, QRadar, SolarWinds and so on. Even though we already used Splunk as SIEM tool as well, in our topology Wazuh and Splunk has different functionalities and roles

3.2. Detailed description of Technologies of choice



Figure 4: VMware Workstation Pro virtualization version17

VMWare Workstation

In our project we use VMware Workstation for all the virtualizations. VMware Workstation is an industry leader in desktop virtualization technology, enabling the creation and management of multiple operating systems on a single physical workstation. It provides a secure and isolated environment where various network topologies can be simulated without impacting the host machine. It allows users to emulate complex network infrastructures, complete with custom networking configurations such as VLAN tagging, network latency simulation, and detailed network performance monitoring. These functionalities enable users to set up environments that closely mimic real-world network operations. For educational environments, VMware's snapshot and revert functionality is invaluable. It is especially important when using hard core programs, that when there is a crash on a program we can revert to previous backup and continue to work or troubleshoot the problem.

OPNsense firewall

OPNsense is a security-centric, open-source firewall that delivers the versatility required for a virtual campus network. In the project, it is not only a gateway but also a comprehensive educational tool that enables the demonstration of complex network security concepts and the application of real-world cybersecurity techniques. Within the virtual campus network, the OPNsense firewall is configured to enable interface access exclusively for administrative purposes through the Staff interface, with IP gateway 172.16.10.2 and port 8443, leveraging its customizable web interface for secure and manageable control.

Multi-Interface Configuration

The firewall set with multiple interfaces linked to addresses designed as stated below acts with roles: Staff, Student, Subnet, and IT control as clearly distinct segmentation of network traffic. This multi-link infrastructure will play a big part on one's network security and traffic balancing.

Advanced Port Management

OPNsense is utilized to give access to Interface Staff on port 8443 and port 2244 to provide the SSH service, which is a security best practice of changing the default ports that will prevent the bots from attack resulting to a serious threat. Listening to this, I would say administrative access through a single interface and account can clearly exhibit the control over user access and the concept of the least access.

Ntopng

On top of the campuses network security posture, OPNsense was added with Ntopng (ng is a network High performance traffic analysis tool) on port 3000 on 172.16.10.2. Ntopng is a service in OPNsense toolset with major contribution to OPNsense's advanced network monitoring abilities. It provides with in-depth insights on network traffic as well as its behavior. Ntopng on OPNsense gives to us the option to observe and analyze network traffic data in detail, while looking real time flows occur on the campus network. Ntopng does the work of saving a huge amount of traffic logs which is an integral part of investigation when a security event takes place. This helps in procedure of log analysis which is useful for DoS and Brute Force kind of attacks. Recording feature lets to do the monitoring of the network statistics and filtration which allows to reveal the patterns that could be signs of security threats or network misuse. By using as Wireshark and JSON formats the data can be downloaded and analyzed in more detail.

Ntopng Configurations:

Live Flows

Flow Idle Timeout: 60 sec

10 ▾ Hosts ▾ Status ▾ Severity ▾ Direction ▾ L7 Protocol ▾ Categories ▾ DSCP ▾ Host Pool ▾ Networks ▾ IP Version ▾ Protocol ▾

Serial	Application	Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
	TLS DPI	TCP	192.168.244.144 L-50111	rum-ingest.us1.signalfx.com R:https	01:58	Client Server	0 bps	16.31 KB	rum-ingest.us1.sign
	TLS DPI	TCP	192.168.244.144 L-58008	c.go-mpulse.net R:https	02:00	Client Server	0 bps	4.54 KB	c.go-mpulse.net
	TLS DPI	TCP	192.168.244.144 L-9969	www.splunk.com R:https	00:20 sec	Client Server	0 bps	2.98 KB	www.splunk.com
	DNS DPI	TCP	192.168.244.144 L-33212	adns0.m.faelix.net R:domain	00:03 sec	Client Server	0 bps	2.01 KB	53.197.134.185.in-a
	DNS DPI	TCP	192.168.244.144 L-17991	adns6.g.faelix.net R:domain	00:02 sec	Client Server	0 bps	2.01 KB	55.197.134.185.in-a
	DNS DPI	UDP	192.168.244.144 L-44618	wil.man.uk.node.nameserver.party R:domain	00:01 sec	Server	0 bps	1.3 KB	53.203.227.46.in-ad
	DNS DPI	UDP	192.168.244.144 L-53464	adns2.m.faelix.net R:domain	< 1 sec	Server	0 bps	1.21 KB	53.200.227.46.in-ad
	DNS DPI	UDP	192.168.244.144 L-36008	adns6.g.faelix.net R:domain	< 1 sec	Server	0 bps	1.21 KB	53.204.227.46.in-ad
	DNS DPI	UDP	192.168.244.144 L-8273	wil.man.uk.node.nameserver.party R:domain	< 1 sec	Server	0 bps	1.21 KB	53.205.227.46.in-ad
	DNS DPI	UDP	192.168.244.144 L-53655	adns0.m.faelix.net R:domain	< 1 sec	Server	0 bps	1.21 KB	53.202.227.46.in-ad

Figure 5: Ntopng Live Traffic Monitoring

PID (Process ID)	55919
Alerts	Queries: 136495 / Stored: 0 / Dropped: 0
Storage Utilization	Volume: /var/db/ntopng (/dev/gpt/rootfs) <ul style="list-style-type: none"> em4 (7.25 MB) em3 (6.71 MB) em1 (6.47 MB) em2 (6.02 MB) em0 (5.65 MB) lo0 (3.71 MB) System (1.86 GB) Available (52.21 GB) - Total: 54.11 GB
Last Log Trace	<pre> 29/Apr/2024 00:01:24 [fetch_blog_feed.lua:15] [blo 29/Apr/2024 00:00:48 [housekeeping.lua:37] [lists_ 29/Apr/2024 00:00:48 [housekeeping.lua:37] [lists_ b.com/ntop/ntopng 29/Apr/2024 00:00:43 [housekeeping.lua:37] [lists_ 1/blocklist-ipsets/master/dshield_7d.netset]... OK 29/Apr/2024 00:00:43 [housekeeping.lua:37] [lists_ e/]... OK 29/Apr/2024 00:00:41 [housekeeping.lua:37] [lists_ ts/CTU-AIPP-Blacklist/Todays-Blacklists/AIP_histor 29/Apr/2024 00:00:40 [housekeeping.lua:37] [lists_ </pre>

Figure 6: The Storage Space Being Used

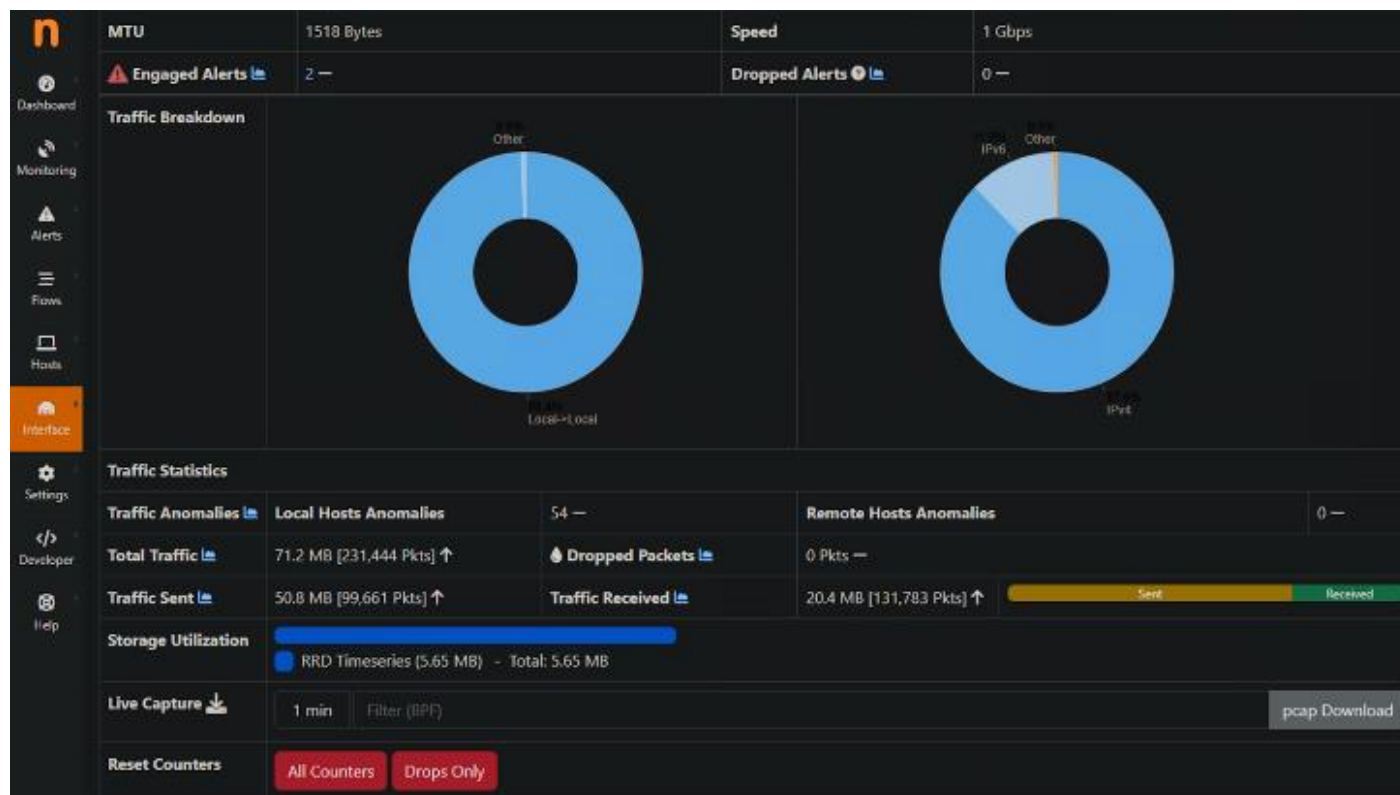


Figure 7: Description Anomalies and MTU

WAF

For WAF (web application firewall), we configured Nginx, built-in service on OPNsense.

With the Nginx in place, the load on the OPNsense system can be significantly reduced and it will be able to provide web applications firewall as well. It is a vital service because it takes care of a lot of vulnerabilities and deters threats that may be targeted at your campus site. Nginx has been equipped with a WAF tool which can proactively screen and filter malicious traffic in real time, and thereby, prevention attacks such as XSS, SQL injection, and many other exploits from occurring would keep the network/system more robust and safer.

Configurations:

Changing the Default HTTPS Port

From a security protocol aspect and for other services not to clash, HTTPS default port was changed. This one is critical because it contributes towards the materialization of this goal by inscribing a password that would safeguard the interface from automated scans that target by default ports.

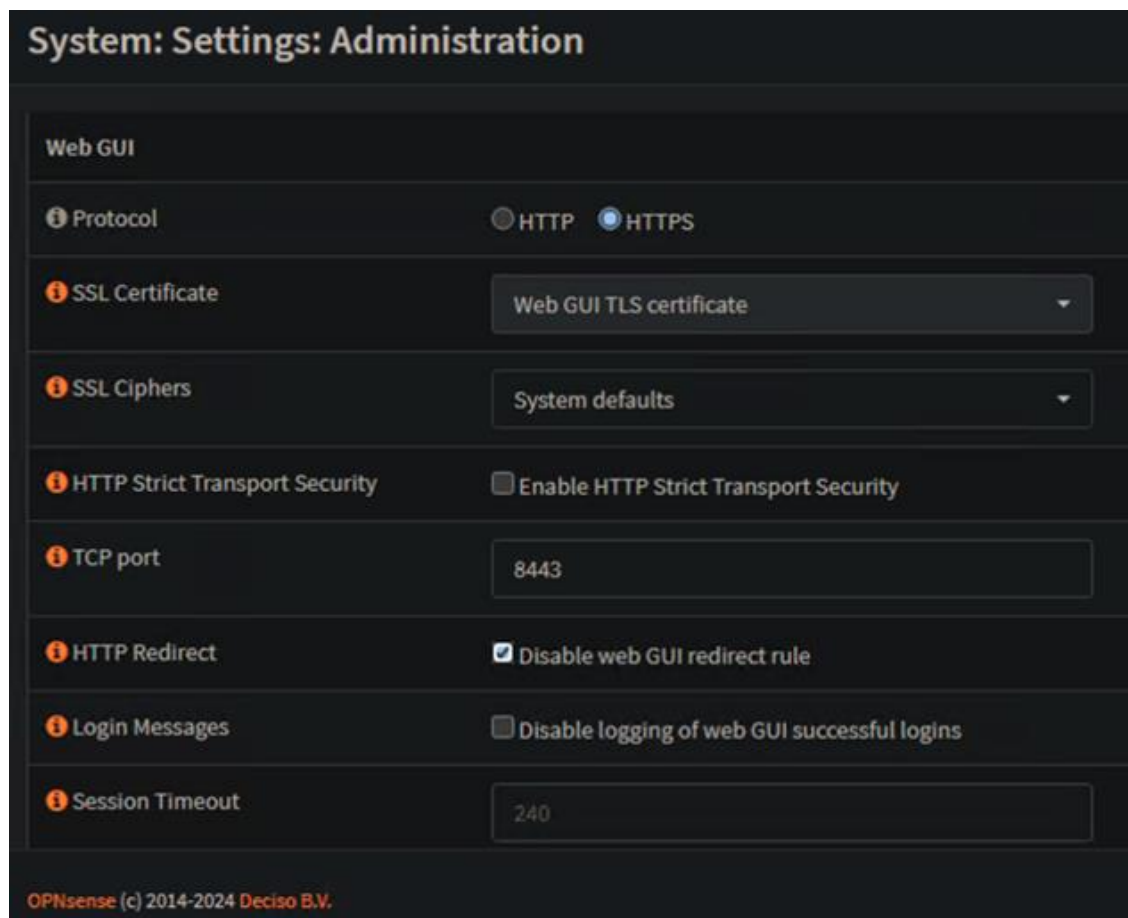


Figure 8: Default HTTPS Port Changing in the Firewall

Enabling Nginx on OPNsense

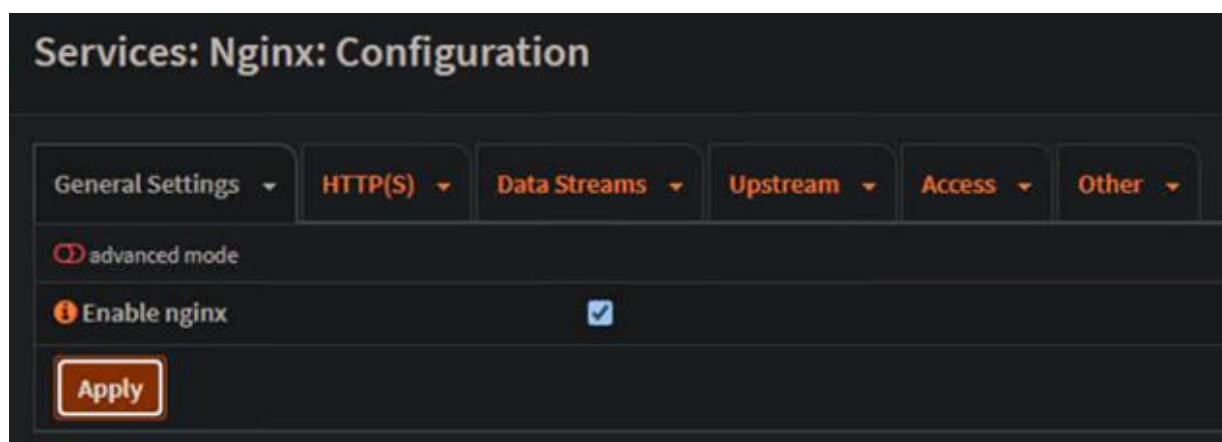


Figure 9: Enabling Nginx Plugin in Firewall

Upon the Services menu, under Nginx Configuration, you can find the Nginx button which will activate it. This setup is a prerequisite for us to benefit from WAF supported part of Nginx.

Upstream Server Configuration

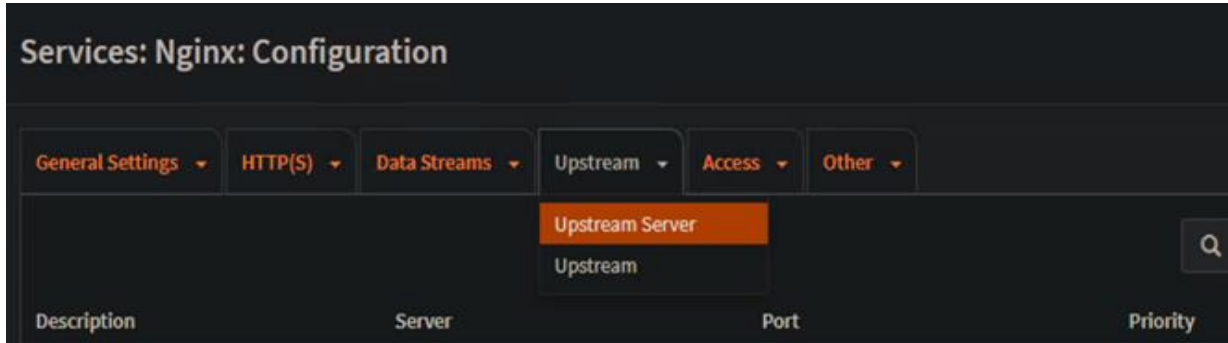


Figure 10: Upstream Server Selection

NGINX

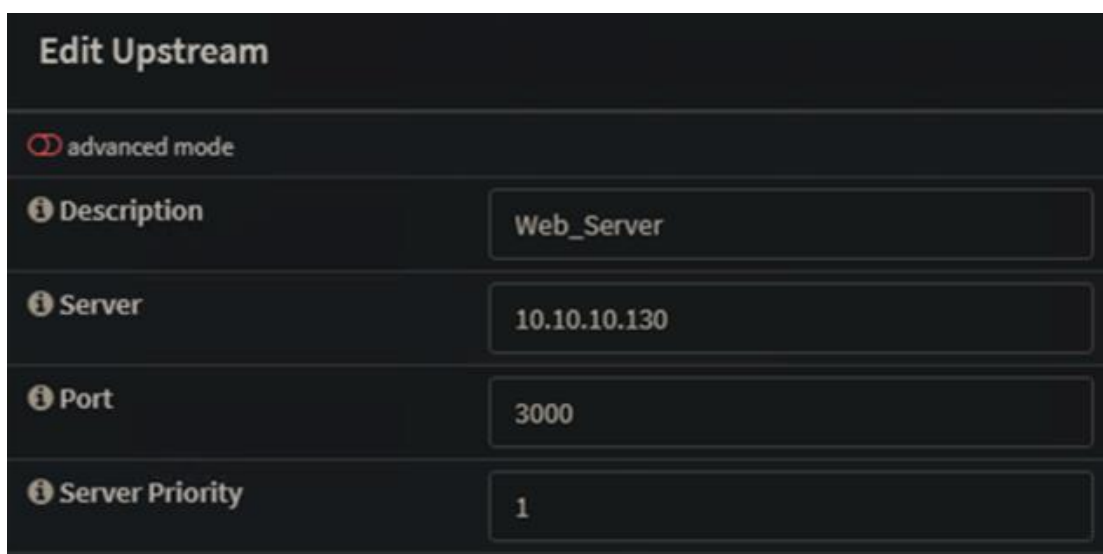
The image shows a form titled 'Edit Upstream'. At the top left, there is a checkbox labeled 'advanced mode' which is currently unchecked. Below this are four rows, each with a label and an input field: 'Description' with the value 'Web_Server', 'Server' with the value '10.10.10.130', 'Port' with the value '3000', and 'Server Priority' with the value '1'. Each label has an information icon (i) to its left.

Figure 11: adding a web server as an upstream server

Upstream addresses will be defined in the nginx.conf file. This file will handle the traffic load on backend servers. This configuration represents a fundamental as it provides with an answer as to how requests will be routed to the web applications and services behind the web application firewall.

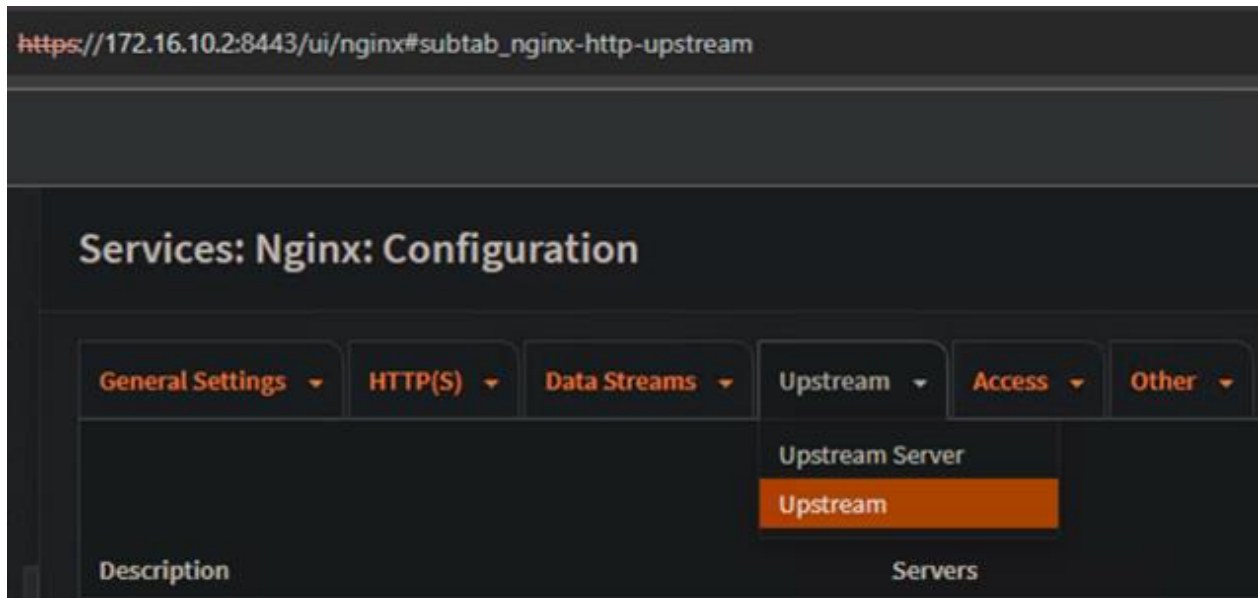


Figure 12: Verification of Upstream

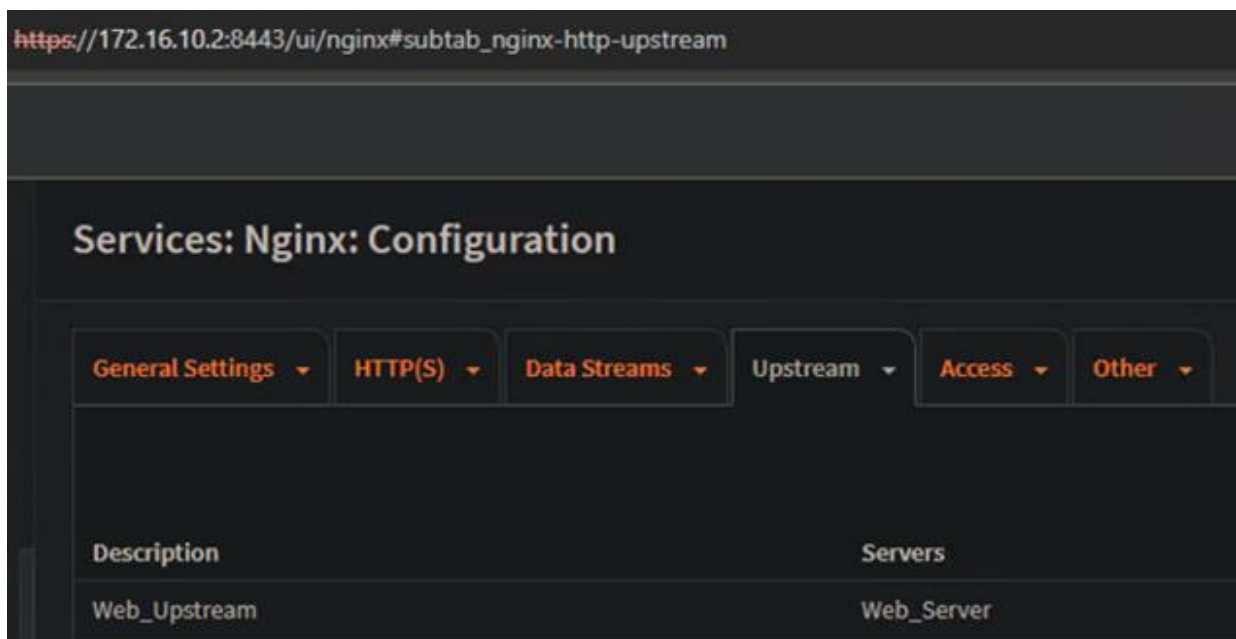


Figure 13: Successful Configuration of Upstream

Naxsi Rules Integration



Figure 14: Web Attack Flows

To enrich the security features of the site, Naxsi rules were uploaded and put into force. Naxsi as a Nginx open-source WAF module is majorly for the purpose of safeguarding web applications from SQL injection, cross-site scripting, and other types of attacks. The implementation of Naxsi rules in Nginx WAF provides a comprehensive filter pack and gives the ability to tune and adapt it to the precise needs of the campus network security.

SQL Injection (SQLi) Protection Rules

Edit WAF Policy

Name	SQL Injections IDs:1000-1099
Rules	<div> <div>0x, possible hex encoding ×</div> <div>close parenthesis, probable sql/xss × comma ×</div> <div>double arobase (@@) ×</div> <div>equal sign in var, probable sql/xss ×</div> <div>mysql comment (#) × mysql comment (*/) ×</div> <div>mysql comment (--) × mysql comment (/) ×</div> <div>mysql keyword (&&) ×</div> <div>open parenthesis, probable sql/xss × semicolon ×</div> <div>simple quote × sql keywords ×</div> </div> <div> Clear All Copy Paste Text </div>
Value	8
Operator	Bigger or Equal
Action	Block Request

Figure 15: Implementing Protection Rules for SQL Injection in WAF

Specific regulations for the prevention of SQLi attacks were implemented as one of the single examples of what can be done on a level of detail guards. Other than SQLi, there are many other common types of web application attacks, and this can be mitigated by the WAF configuration as it thwart this attack, prevent unauthorized access to databases and exfiltrated of sensitive data.

Edit Naxsi Rule

Description	sql keywords
Message	sql keywords
Negate	<input type="checkbox"/>
ID	1000 × <input type="text"/> Clear All Copy Paste Text
Rule Type	Main Rule ▼
Use Regular Expressions	<input checked="" type="checkbox"/>
Match Value	select union update delete insert table from ascii he...
Match Type	Blacklist ▼
Search in any GET Argument	<input checked="" type="checkbox"/>
Search in URL	<input checked="" type="checkbox"/>
Search in any HTTP Header	<input type="checkbox"/>
Search in any POST Argument and in Body	<input checked="" type="checkbox"/>

Figure 16: Establishment of WAF Module Naxsi



Figure 17: HTTPS Location Configuration

Edit Location

advanced mode

i Description

Web_Location

i URL Pattern

/

i Match Type

None

i URL Rewriting

Nothing selected

Clear All

i Enable Security Rules

☒

i Learning Mode

☐

i Block XSS Score

i Block SQL Injection Score

i Custom Security Policy

Cross Site Scripting IDs:1300-1399, Directory traver

i Upstream Servers

Cross Site Scripting IDs:1300-1399 ✓
 Directory traversal IDs:1200-1299 ✓
 Evading tricks IDs: 1400-1500 ✓
 File uploads: 1500-1600 ✓
 OBVIOUS RFI IDs:1100-1199 ✓
 SQL Injections IDs:1000-1099 ✓

i Path Prefix

i Cache: Directory

i File System Root

Figure 18: HTTPS Monitoring

The location block for the HTTPS query in Nginx was carefully configured to specify the handling of HTTPS requests. This includes encrypting the data that is transmitted with SSL/TLS settings, thus preventing any unauthorized access.

The application of the Naxsi rules is also a crucial constituent of the HTTPS location configuration, which is consistent with the overall security mission.

Wazuh

Wazuh is an open-source security platform which enables neat, responsive detection, response as well as risk aversion through single-hand. Its powerful tools provide for such log analysis, but they are not limited to this feature that are rich in functionality widespread with capability of integrity monitoring, security configuration assessment and active response. These features include performance and security as well as compliance, all thanks to which Wazuh helps to create manageable, secure and compliant campus networks.

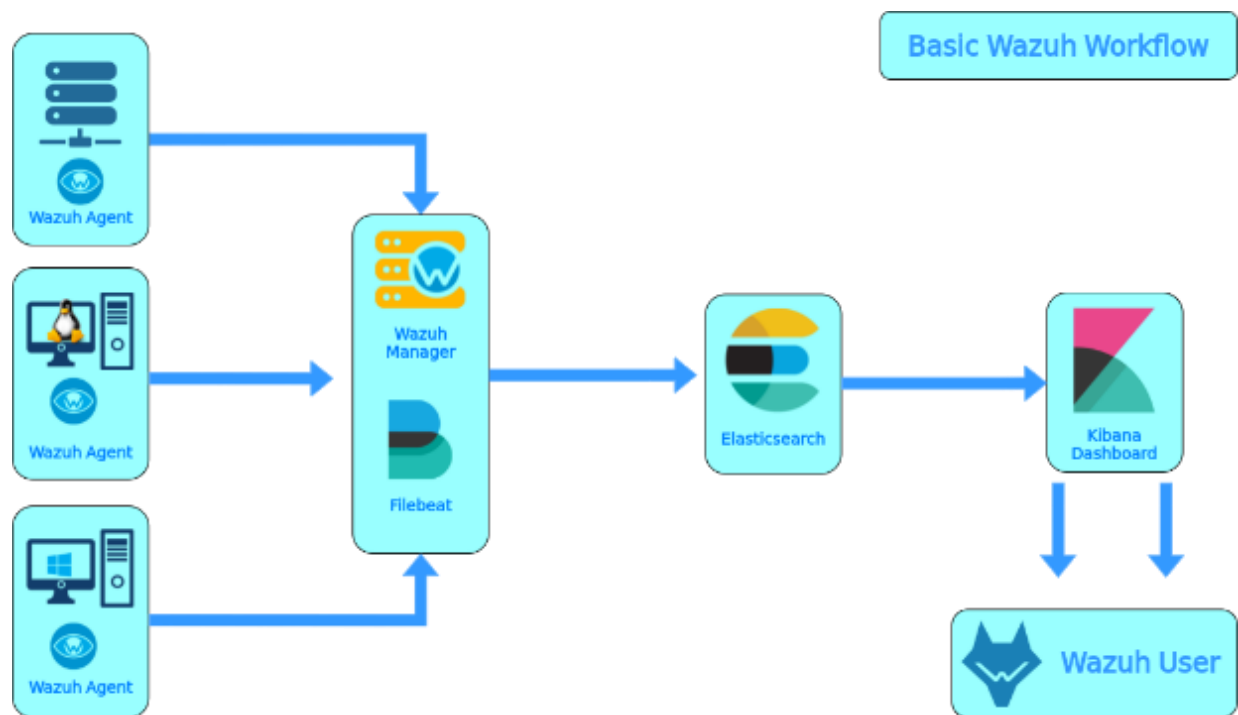
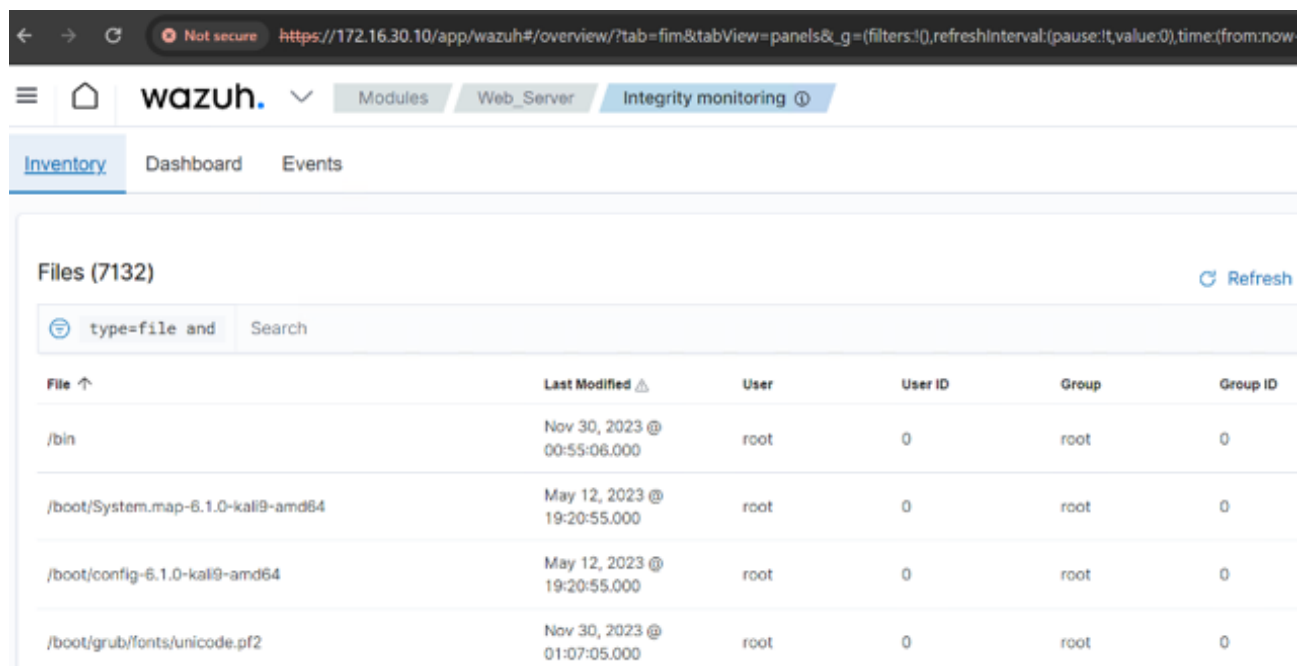


Figure 19: Wazuh Working Principle

Wazuh monitoring file integrity is not only integrated but also, one of the best features that it offers which is very critical for data and network security and consistency we use in our school campus.



The screenshot shows the Wazuh web interface at the URL `https://172.16.30.10/app/wazuh#/overview/?tab=fim&tabView=panels&_g=(filters:10,refreshInterval:(pause:1t,value:0),time:(from:now`. The navigation bar includes 'Modules', 'Web_Server', and 'Integrity monitoring'. The 'Inventory' tab is selected, showing a list of 7132 files. A search filter 'type=file and' is applied. The table displays columns for File, Last Modified, User, User ID, Group, and Group ID. The visible rows are:

File	Last Modified	User	User ID	Group	Group ID
/bin	Nov 30, 2023 @ 00:55:06.000	root	0	root	0
/boot/System.map-6.1.0-kali9-amd64	May 12, 2023 @ 19:20:55.000	root	0	root	0
/boot/config-6.1.0-kali9-amd64	May 12, 2023 @ 19:20:55.000	root	0	root	0
/boot/grub/fonts/unicode.pf2	Nov 30, 2023 @ 01:07:05.000	root	0	root	0

Figure 20: Wazuh Integrity Monitoring

Continuous Surveillance:

Wazuh is based on the agent model, therefore it can perform constant file integrity monitoring and directories validation across all available network endpoints and detect possible unauthorized changes on the fly.

Inventory Assessment:

The second step in the breach response plan is integrity monitoring. Wazuh also has an inventory capability that records and tracks changes to the file system, and it helps to make systems visibility process more transparent.

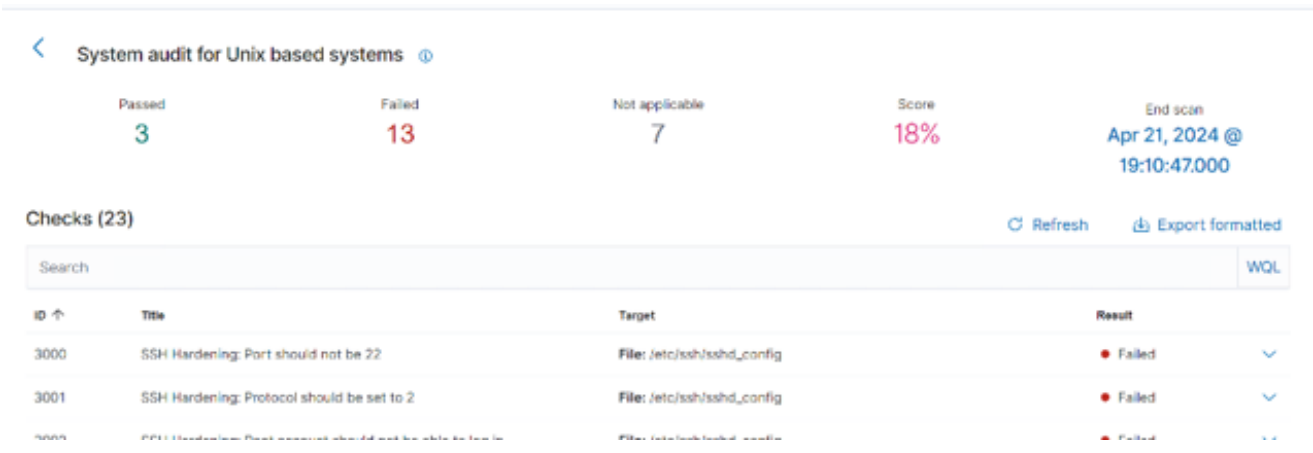


Figure 21: Wazuh Security Configuration Assessment

Vulnerability Identification:

SCA module assesses systems against predetermined security rules that aims at finding any misconfigurations or variations in settings which can expose the system to vulnerabilities.

Remediation Guidance:

Upon the detection of an SSH configuration issue, for example, Wazuh provides remediation instructions to quickly resolve security challenges in IT systems.



Figure 22: Wazuh SSH Hardening

Active Response for Real-Time Threat Mitigation

Wazuh implements active response as an active security measure to prevent active threats.

Automated Countermeasures:

At the point when a danger is identified, Wazuh can execute predefined actions to reduce or prevent the malicious activity, for example, interfere with an IP address or changing firewall rules.

Custom Response Scripts:

Administrators can define custom scripts that Wazuh will trigger upon specific alerts, enabling a dynamic defensive status against unique threats faced by the campus network.

Integration in Campus Network:

Wazuh's integration into the campus network security infrastructure enhances the overall security posture.

Compliance with Standards: The monitoring and assessment capabilities support compliance with industry standards and frameworks, vital for the protection of academic data.

Detailed Reporting: Through comprehensive reports and dashboards, Wazuh provides visibility into the security status of the network, facilitating informed decision-making by network security team.

Compared with Wazuh, it appears to be an independent security tool, that plays a very important role to defend any campus network. This relationship exactly complies with the aim of achieving security using advanced monitory methods, instant threat detection, and automated responses to ensure that the network remains full of all standards and reliable.

Splunk (SIEM)

Integration of a Ticketing System with Splunk for Enhanced Incident Response. To create smooth process pipeline for incident response workflows and facilitate real-time communication, integration of a ticketing system with our Splunk as an additional SIEM solution seemed optimal for our project. This integration contains Slack Bot as an intermediary bridge to the gap between Splunk's robust alerting capabilities and team-wide incident communication channels..

Technical Overview. The integration process considers majorly these key steps:

Slack App Creation: Creating a new Slack app with Incoming Webhooks. This will generate a unique webhook URL, which will be used by Splunk to push notifications to the designated Slack Bot for the "ADA Network" workspace.

Splunk Integration: We have installed the "Slack Notification Alert" app in SplunkBase. This app allows Splunk to send an alert over channels in Slack through messages under predefined conditions.

We establish the channel of communication by setting up our Slack app's webhook URL in this Splunk integration.

Alert Configuration:

Within Splunk, we have created alerts based on clearly important criteria for security. For example, failure to detect a heartbeat, which we housed alerts to run in cases where search patterns related to the data sources, we are monitoring get triggered.

We linked the newly defined alerts with the Slack integration, ensuring that a notification would be sent to the designated Slack channel when an alert is triggered.

Customization

We tailored the Slack notifications to provide essential incident details such as the event description, severity, and a link back to the relevant Splunk search results. This customization allows team members to quickly assess the situation and initiate response procedures.

Benefits of Integration

Centralized Monitoring: Splunk, as the primary SIEM solution, consolidates security data and generates alerts across our network infrastructure.

Real-time Collaboration: The seamless integration with Slack ensures that our development team and other relevant professionals receive notifications of critical incidents in real-time, fostering swift and collaborative responses.

Improved Incident Resolution: By streamlining communication and information sharing, this integration reduces incident resolution time, minimizing the potential consequences of security breaches or service disruptions.

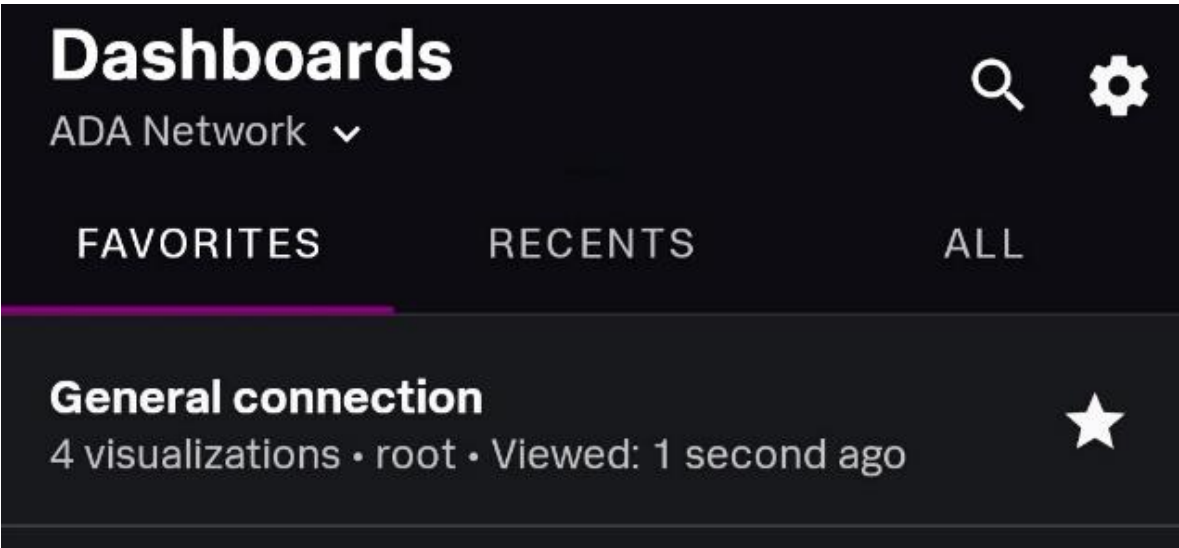


Figure 23: Splunk Mobile Dashboard

Mobile Widgets for smooth UI/UX

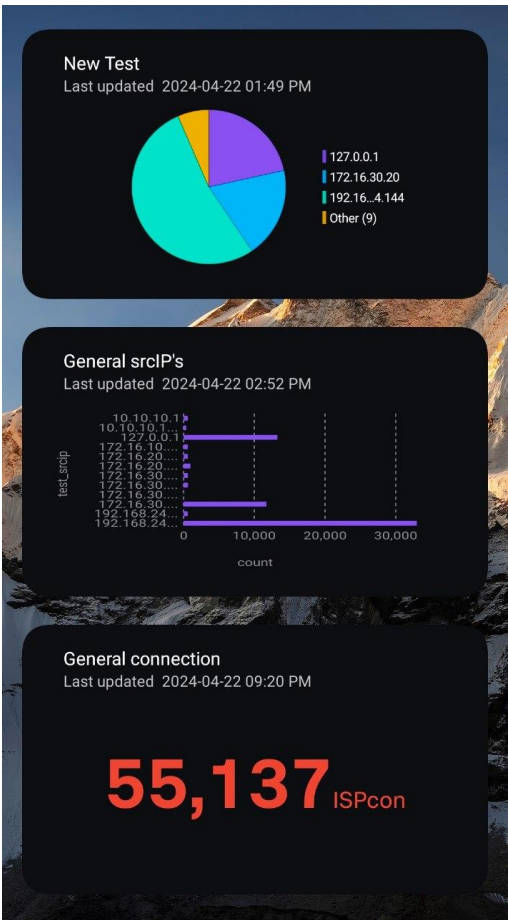


Figure 24: Splunk Mobile Widgets

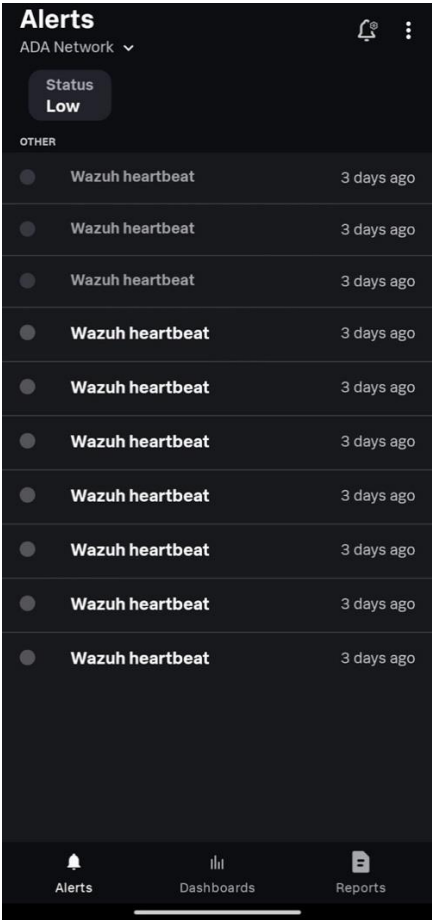


Figure 25: Splunk Mobile Ticketing

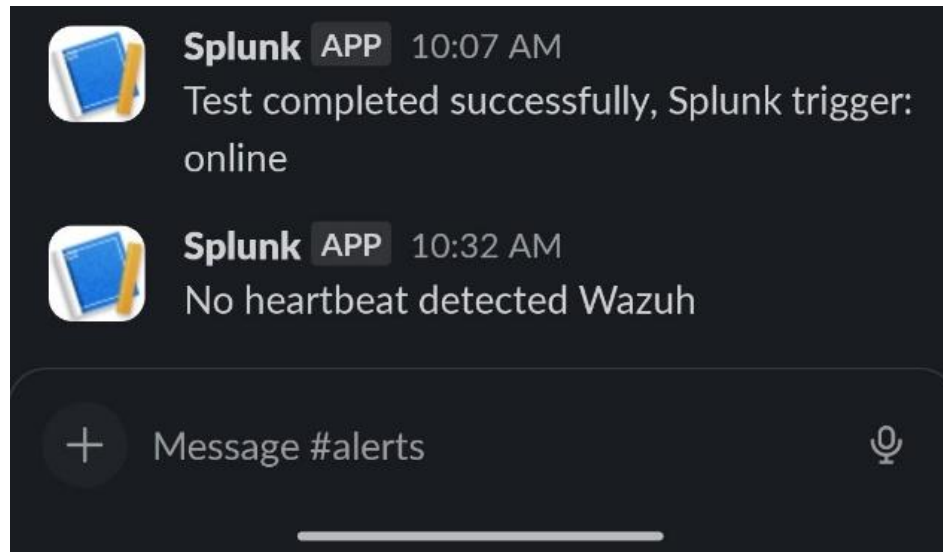


Figure 26: Splunk Ticketing Integration with Slack

Further Considerations:

While we used Slack in this implementation, the concepts and integration principles apply to a wide range of ticketing or collaboration platforms that support webhooks or similar API-based communication mechanisms. *Splunk Mobile* isn't an exception for direct alerting

3.3. Engineering Standards (if applicable)

The project adheres to ISO/IEC 27001 and NIST standards tailored to enhance the security. Mentioned standards are comprehensive frameworks for managing information security and risks. This standard is critical for managing sensitive data processed and logged by SIEM tools, ensuring the management of security risks, and maintaining data according to CIA triangle in the network infrastructure.

ISO/IEC 27001 Controls implemented:

- A.9.1.2 Access to Networks and Network Services
- A.12.1.2 Change Management
- A.12.3.1 Information Backup
- A.13.1.1 Network Security Management
- A.14.1.2 Securing Application Services on Public Networks
- A.14.2.5 Secure System Engineering Principles

NIST Controls implemented:

PR.DS-2 Cyber Incident Response

This IR process outlines 6 steps to effectively respond to security incidents:

1. **Preparation:** Establish teams, update tools & procedures.
2. **Identification:** Detect & categorize incidents (low, medium, high).
3. **Containment:** Isolate threats & gather attack information.
4. **Eradication:** Remove malicious elements from the network.
5. **Recovery:** Restore normal operations & fix vulnerabilities.
6. **Lessons Learned:** Analyze incidents to improve future responses.

PR.DS-8 system and information integrity

Software, Firmware, and Information Integrity:

- Use tools to detect unauthorized changes to defined software, firmware, and information.
- Ensure systems perform integrity checks at defined times.
- Include detection of unauthorized changes in incident response procedures.

Spam Protection:

- Use mechanisms at entry/exit points to detect and address spam.
- Update mechanisms with new releases according to configuration management procedures.
- Manage mechanisms centrally and ensure automatic updates.

Information Input Validation:

Check the validity of defined information inputs.

Offer a manual override capability for defined inputs, restricted to authorized personnel only.

- Audit the use of the manual override capability.
- Review and resolve input validation errors.
- Behave predictably when receiving invalid inputs.

Error Handling:

- Generate error messages with information for corrective actions without revealing exploitable information.
- Reveal error messages only to authorized personnel.

System-Generated Alerts:

- Ensure alerts from various sources (audit records, security mechanisms) are disseminated to authorized personnel/units for action.
- Transmit alerts via phone, email, or text message to designated personnel.

3.4. Research Methodology and Techniques

Structure

Restate the specific problem your project addresses within the university's cybersecurity context. Briefly outline the core technologies used in your solution (Suricata, ZenArmor, OPNsense).

Research Approach:

Our project likely leans towards qualitative analysis for collecting descriptive data about system performance and security insights.

Case Study Methodology:

We are using a case study approach by demonstrating our solution's efficacy in the university's environment.

Data Collection Techniques:

Our primary source of data will be the logs and alerts generated by Suricata and ZenArmor within OPNsense.

System Performance Metrics:

we will gather performance data (e.g., network traffic throughput, resource usage) to assess the impact of our security solution.

Performance Analysis:

Since this is a demo-focused project, we plan to assess our solution's improvement in terms of threat detection, incident response, and automation we have implemented.

Limitations

We acknowledge that our study is conducted within a specific test scenario, and real-world deployment might reveal additional challenges.

This project adopts a case study methodology to demonstrate the feasibility and effectiveness of the proposed cybersecurity automation solution. The primary data sources are security logs and alerts generated by Suricata and ZenArmor, integrated within the university's OPNsense firewall framework. These logs will be analyzed for patterns, suspicious activity, and potential threats. Additionally, system performance metrics will be collected to evaluate any impact of the solution on network throughput and resource utilization. Where possible, controlled security incident simulations may be performed to assess the system's response capabilities. Data analysis will involve a combination of log visualization tools, correlation techniques, and qualitative evaluation of the solution's benefits for faster threat detection and streamlined incident response processes.

3.5. Architecture, Model, Diagram description

Our network architecture employs a hybrid topology model, strategically combining elements of both mesh and star configurations to optimize connectivity, security, and operational efficiency. The heart of this architecture is a next-generation OPNsense firewall, enhanced with Zen Armor to provide a robust and multifaceted security foundation.

System Components and Services

OPNsense Firewall with Zen Armor: This core component establishes a centralized control point, enforcing security policies through stateful firewalling, intrusion detection/prevention (IDS/IPS), virtual private networking (VPN), and traffic shaping. The integration of Zen Armor further augments the firewall's capabilities with advanced web content filtering and application control mechanisms.

Two dedicated servers underpin essential university services

Web Server:

Responsible for hosting the university's public websites and web-based applications.

Mail Server:

Manages the university's email infrastructure, providing secure email storage, delivery, and user access.

Security Information and Event

Management (SIEM):

We leverage Splunk as our primary SIEM solution for comprehensive log aggregation, analysis, security monitoring, and incident response. To ensure high availability and resilience, Wazuh is implemented as a redundant SIEM solution.

Ticketing System Integration:

To streamline the management and resolution of security incidents, we have implemented ticketing systems that directly integrate with both Splunk and Slack. This integration fosters real-time collaboration between the development team and relevant professionals, facilitating rapid incident response and problem resolution.

Network Topology and Diagram

The hybrid topology model provides a balance between centralized control and partial redundancy. The OPNsense firewall serves as the central point, interconnecting and securing various network segments. A detailed network diagram visually represents the architecture, showcasing logical relationships, VLAN configurations, firewall rules, and security monitoring touchpoints.

Centralized Security Enforcement: The OPNsense firewall empowers us to establish and maintain network-wide security policies consistently.

Scalability and Flexibility:

The hybrid design supports future expansion and customization as required.

Operational Efficiency:

Centralized logging and ticketing systems improve the visibility, traceability, and resolution time of security events.

The inclusion of a well-developed network diagram with clear annotations will further strengthen this section of your report by providing a visual representation of the architecture's design and workflow.

Diagrams

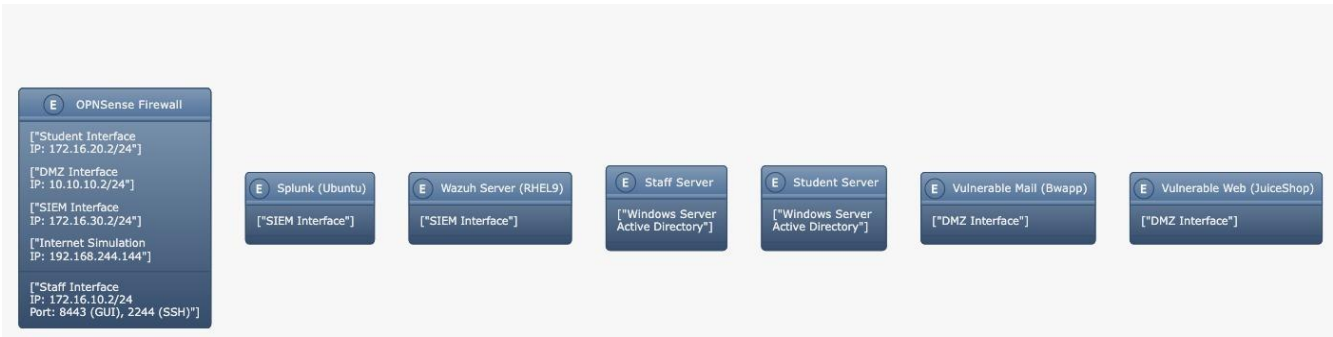


Figure 27: Detailed Campus Topology

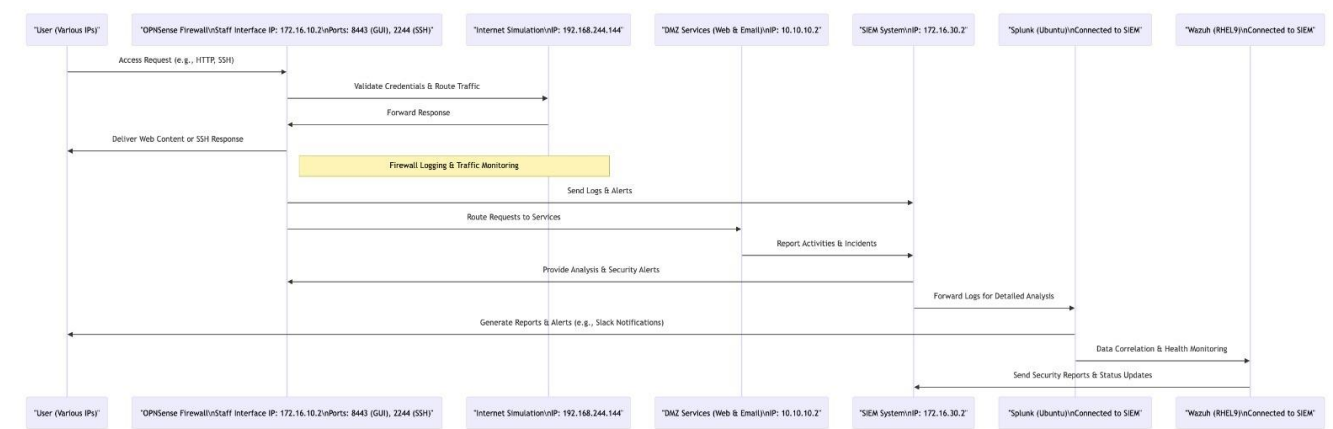


Figure 28: OPNSense Workflow

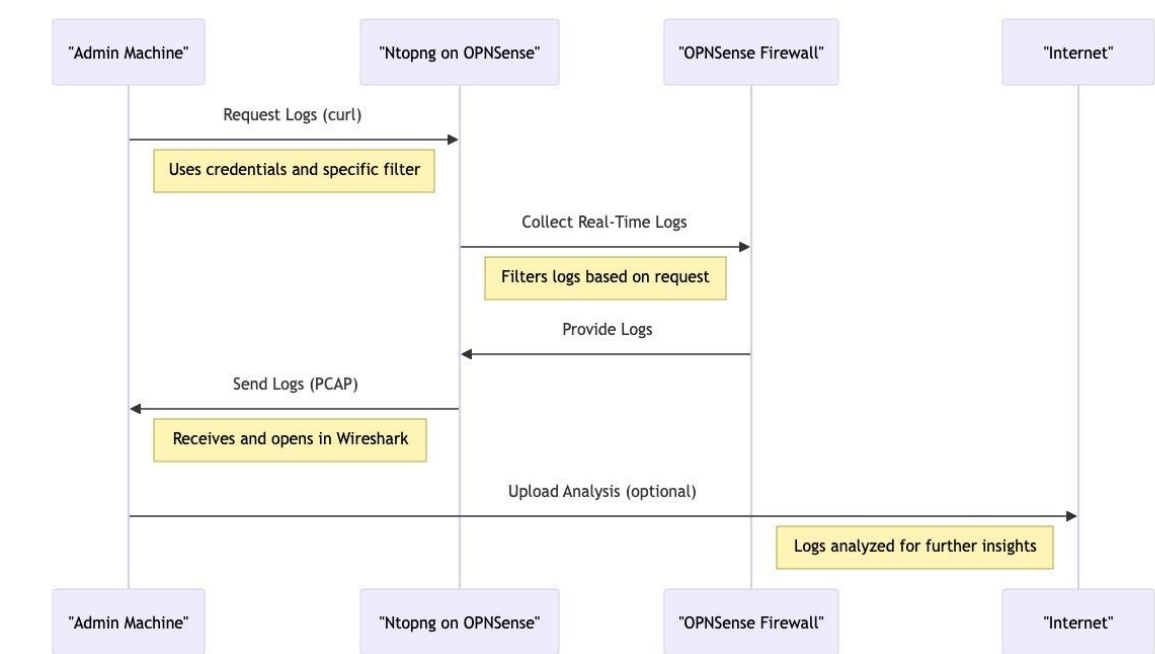


Figure 29: Ntopng Workflow

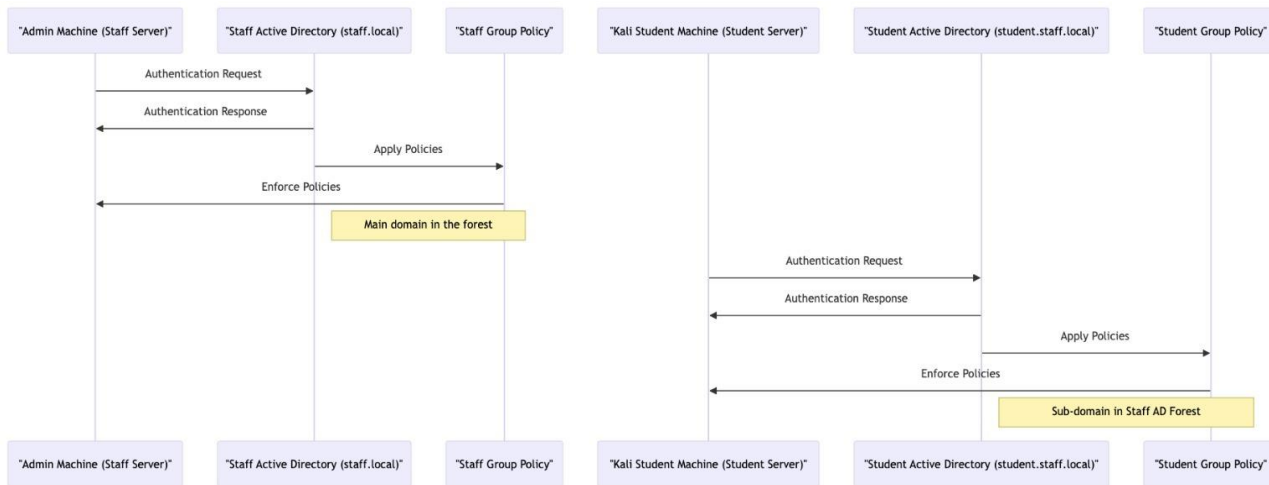


Figure 30: System Infrastructure and GPO Relations

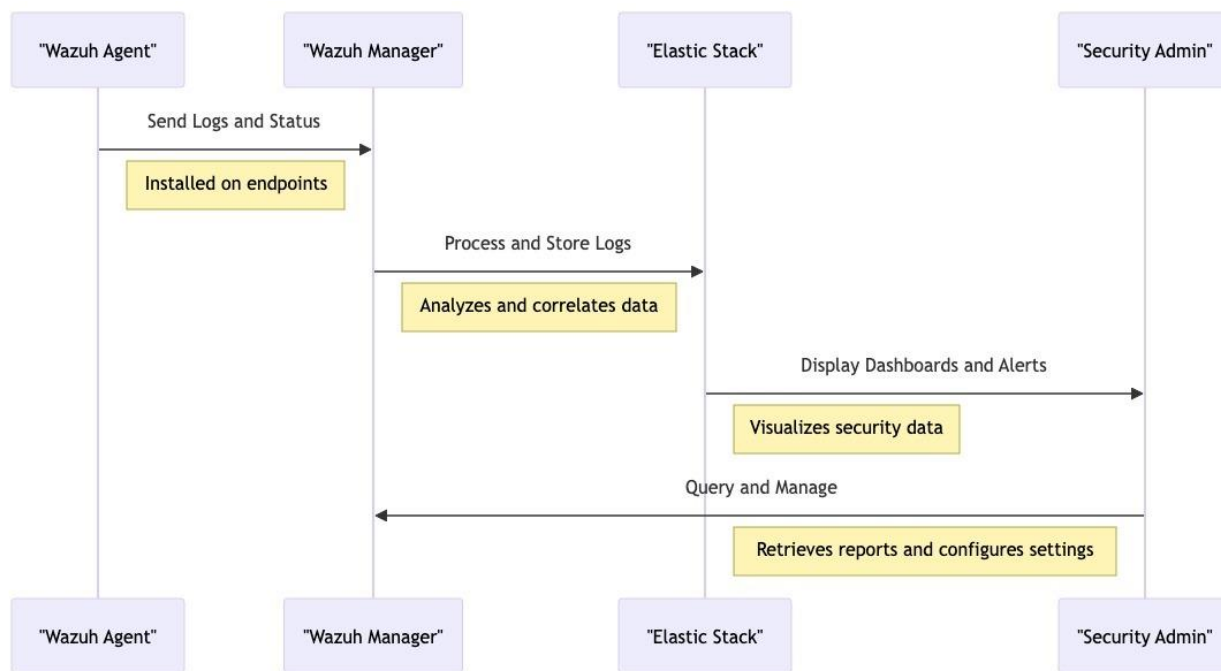


Figure 31: Wazuh Workflow

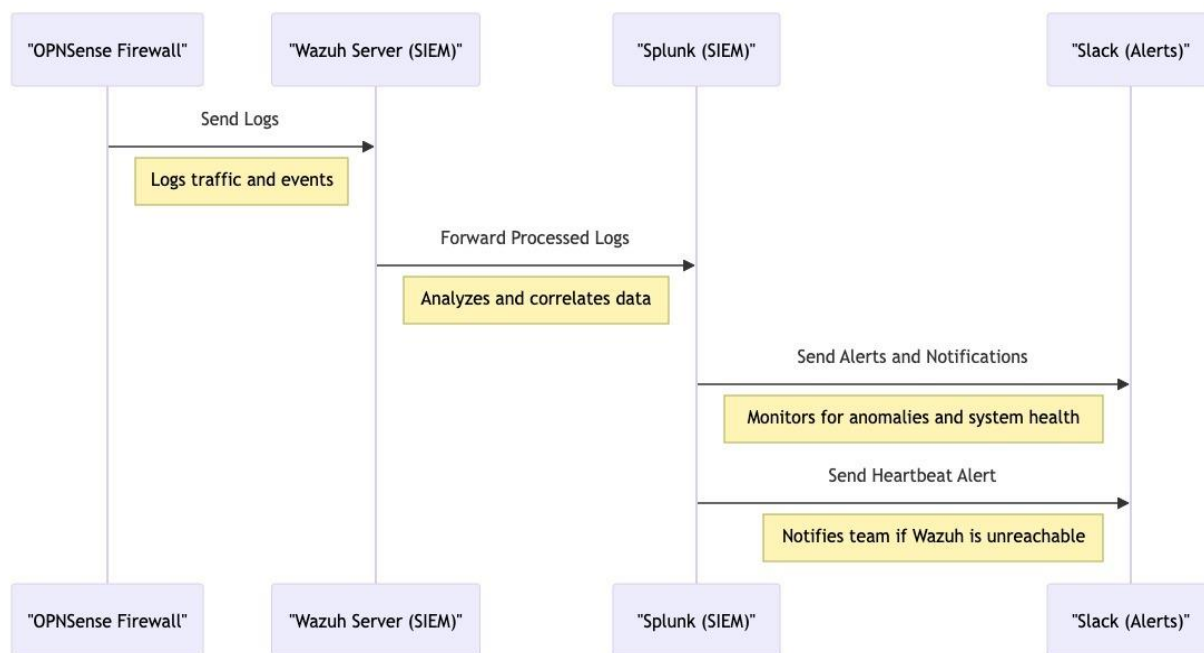


Figure 32: Relation to How Splunk Works with OPNsense, Wazuh and Slack

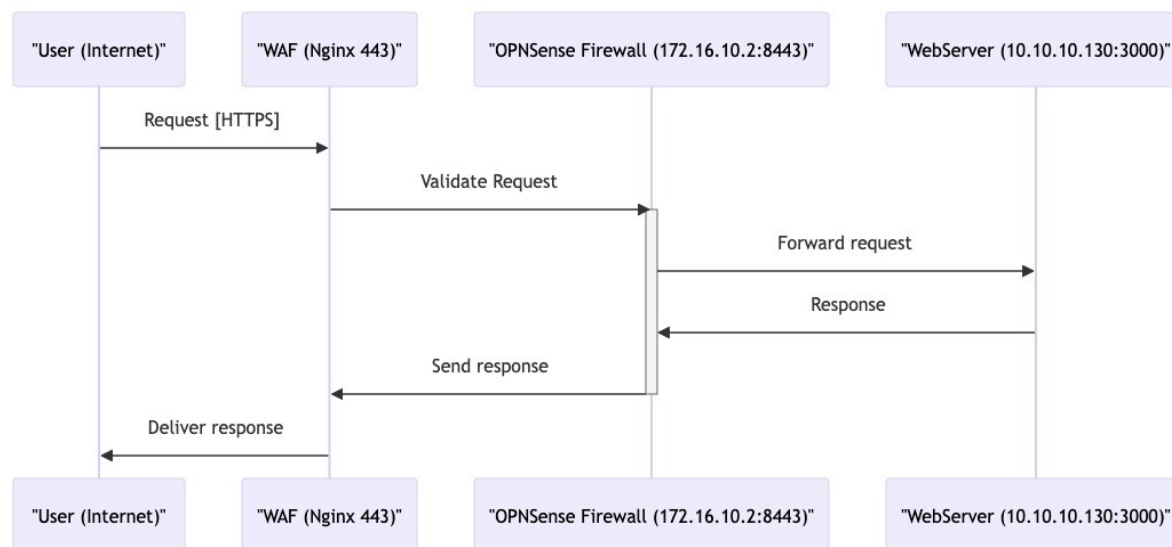


Figure 33: Relation Between WAF and OPNsense

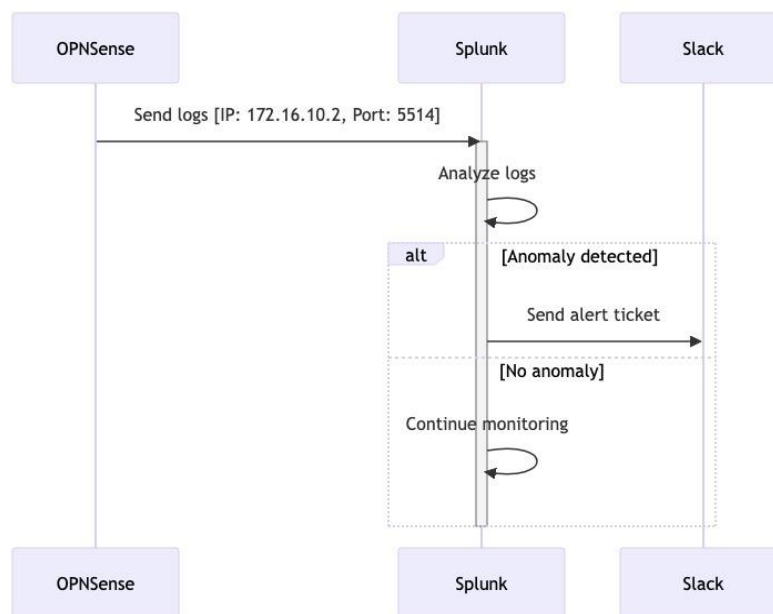


Figure 34: Relation between Splunk, OPNsense and Slack

3.6. Economic analysis

This project will put emphasis on the pathway of shortcut identification and response to the cybersecurity events. It will, therefore, minimize the involvement as well as the required engagement of network teams and other teams like “Staff”. Like this, the network is implemented considering a reduction in operational overhead, as well as the strengthened response to economic losses caused by service breakdown or hacker attacks. The conventional model of manual network and security monitoring calls for employment of a bigger team of experts resulting in higher numbered of personnel and consequently more expenses. Secondly, even longer times to react means rippling times on economic impacts. Examples of this include disputes with organizations and as a matter of fact, security breaches can happen due to non-compliance or financial penalties. Our project project’s core proceeds by applying open-source solutions to develop a cost-effective framework for the automation of real-time cyber intelligence event analysis. In contrast, such a choice relies on non-commercial community-grade platforms, thus avoiding the considerable investments characterizing enterprise-grade systems, which are usually associated with subscriptions, vendor support and practices, and frequently, expensive hardware upgrading. While the larger organizations with very vital uptime prescriptions usually need the solutions, the discovered open-source projects-based solutions can offer flexibility, thus the long-term cost efficiency to the smaller enterprises or institutions. That is, this project will be conducted in the form of OPNsense for stabilizing the firewall, Wazuh for complete SIEM system and Linux servers just to attend the system administration and maintenance issues. We not only get to use but also

participate in already existing software projects, effectively keeping our costs low. In addition, we contribute our own efforts in further development of these environments.

Key Economic Considerations:

Reduced Labor Costs:

Automation and increased efficiency reduce the need for constant human intervention, consequently decreasing general operational costs associated with network security.

Mitigation of Downtime Impacts:

The aim of proactive event detection and streamlined response workflows is to reduce the duration of service disruptions and their economic impact.

Reputation Protection:

A reputation helps to build trust in an organization; it prevents customers from leaving and, at the same time, avoids monetary loss because of the effect of a tarnished public image.

Open-Source Cost Optimization: The strategic use of open-source software lowers licensing fees and vendor lock-in, offering a flexible and cost-effective solution particularly suitable for smaller organizations or those operating on constrained budgets.

While a comprehensive cost-benefit analysis lies beyond the scope of this project, the qualitative economic advantages of our automated cybersecurity event analysis system are evident. Further research could quantify these benefits with greater precision, providing additional insights into the project's value proposition.

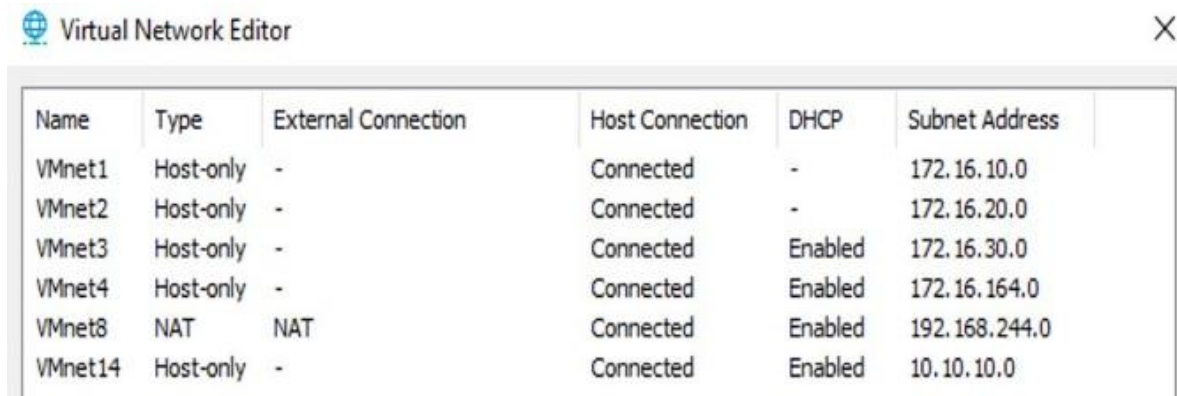
4. Implementation

4.1. Hardware Design

OPNsense

In our project we have used NAT instead of a bridged network, for internet simulation in Firewall. With bridged networking, the VM is accessible from the network. "NAT" on the other hand shares the hosts network connection by assigning the VMs an IP address from a private network and translates network requests from the guest. This way the host appears as a single system to the network. NAT connection on VMware on VMnet8 by default and the IP range is given by VMWare automatically, however it is possible to change if it is needed, in case it was with IP range 192.168.244.0/24. Additionally, we have created VMnet1 for Staff interface on Firewall with IP range 172.16.10.0/24, VMnet2 for Student interface with IP range 172.16.20.0/24,

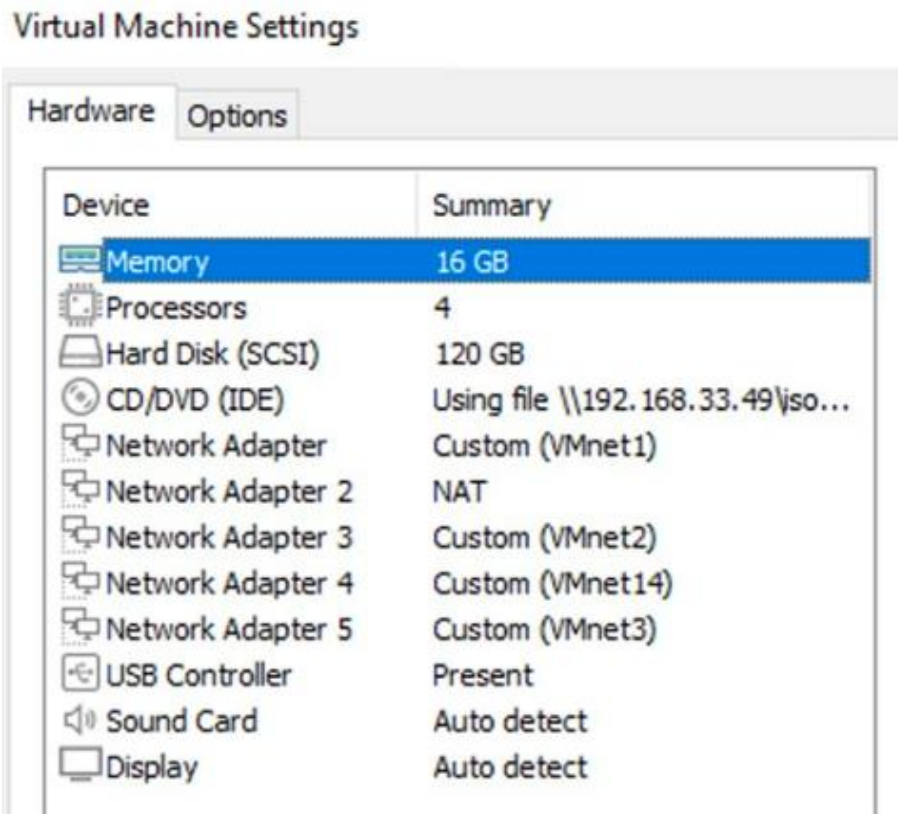
VMnet3 for SIEM interface where all SIEM machines are located with IP range 172.16.30.0/24, and DMZ interface with IP range 10.10.10.0/24.



Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet1	Host-only	-	Connected	-	172.16.10.0
VMnet2	Host-only	-	Connected	-	172.16.20.0
VMnet3	Host-only	-	Connected	Enabled	172.16.30.0
VMnet4	Host-only	-	Connected	Enabled	172.16.164.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.244.0
VMnet14	Host-only	-	Connected	Enabled	10.10.10.0

Figure 35: VMnet and IP Configurations

Furthermore, for OPNsense Firewall we used 16GB of RAM, 4 cores, and 120GB of Memory.



Device	Summary
Memory	16 GB
Processors	4
Hard Disk (SCSI)	120 GB
CD/DVD (IDE)	Using file \\192.168.33.49\iso...
Network Adapter	Custom (VMnet1)
Network Adapter 2	NAT
Network Adapter 3	Custom (VMnet2)
Network Adapter 4	Custom (VMnet14)
Network Adapter 5	Custom (VMnet3)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Figure 36: Memory and RAM Usages

Staff and Client Servers

For staff and Client servers we have used the default measures that VMWare provides according to chosen ISO file, in our case it was Windows Server 2022

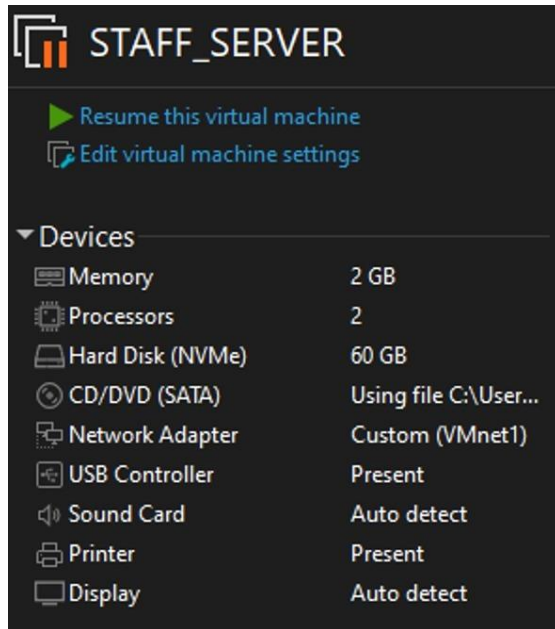


Figure 37: Staff Server Details

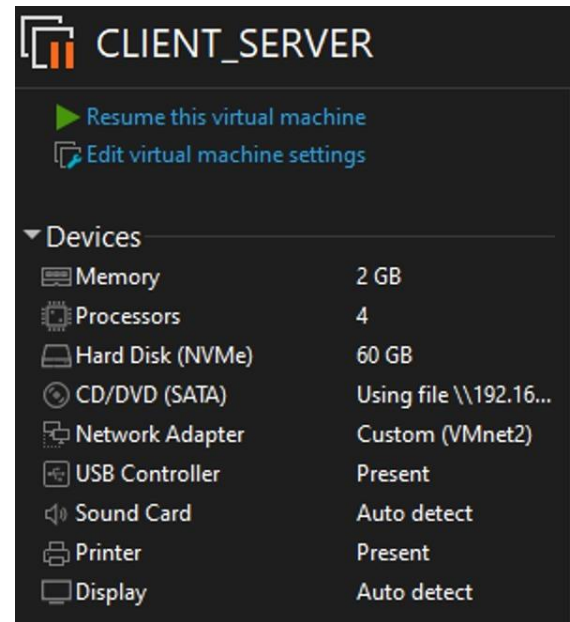


Figure 38: Client Server Details

Splunk Server

For the Splunk server we used default requirements that are given in Splunk documentations.

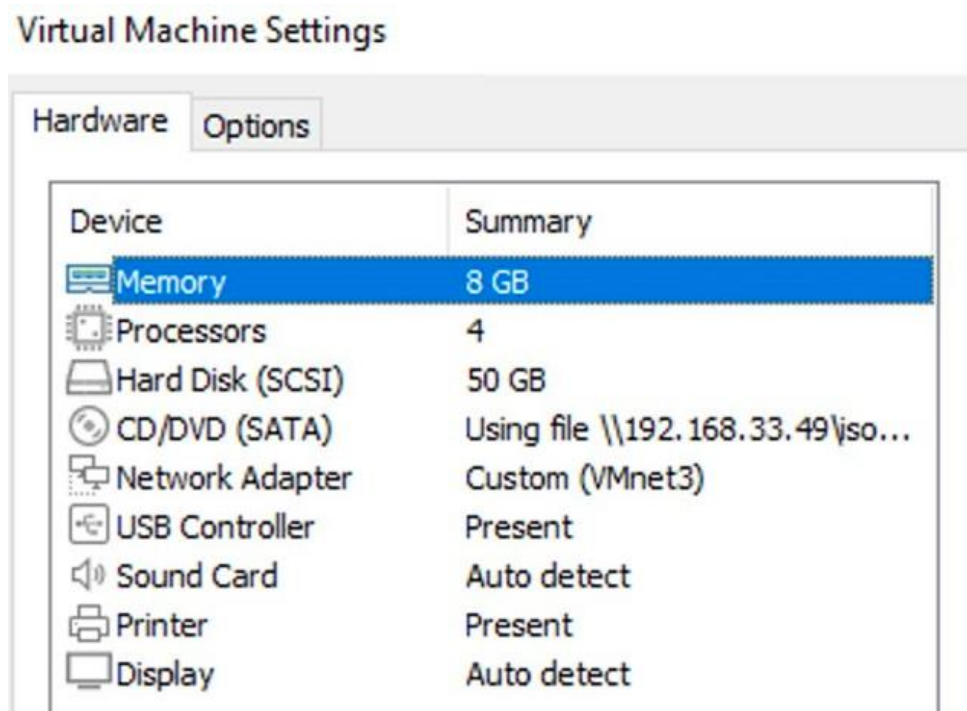


Figure 39: Splunk Memory and RAM Usages

Wazuh

For Wazuh also we used default requirements for Wazuh Server installation.



Figure 40: Wazuh Memory and RAM Usages

Student Kali Machine

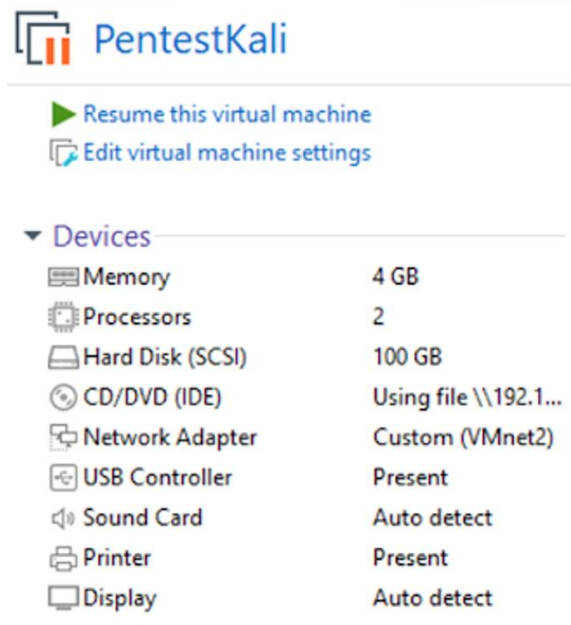


Figure 41: Kali Machine Details

DMZ interface Servers

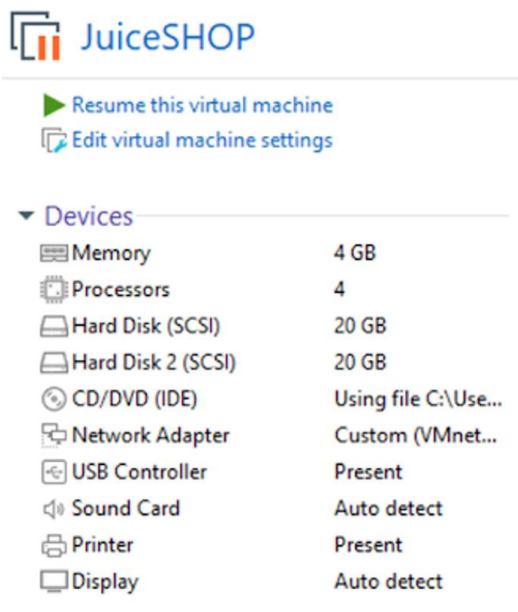


Figure 42: Web Server Details

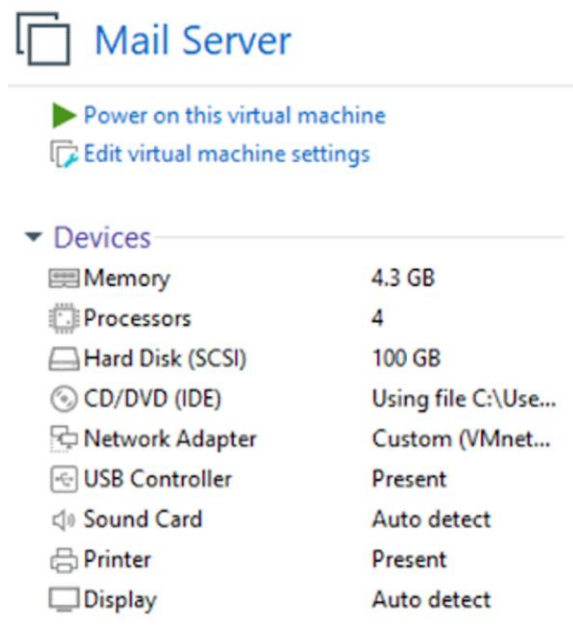


Figure 43: Mail Server Details

4.2. Essential Components of the Project

Our project encompasses the following essential components to establish an effective automated cybersecurity event analysis system within a small to medium-sized network environment:

Network Security Perimeter

- **Next-Generation Firewall (OPNsense):** Provides a robust perimeter security foundation with features including:
 - Stateful packet inspection (SPI)
 - Intrusion detection / prevention systems (IDS/IPS)
 - Web content filtering (with Zen Armor integration)
 - VPN capabilities for secure remote access
 - Traffic shaping for bandwidth prioritization



Centralized Monitoring and Analysis

- **SIEM (Splunk / Wazuh):** Aggregates and correlates logs from various network devices and security tools. Core functions include:
 - Real-time event monitoring
 - Security threat detection and alerting
 - Incident investigation and analysis
 - Visualization and reporting





Incident Response and Collaboration

- **Ticketing System Integration:** Streamlines incident management, providing:
 - Centralized ticket creation and tracking
 - Automated alert-based ticket generation
 - Enhanced problem resolution efficiency

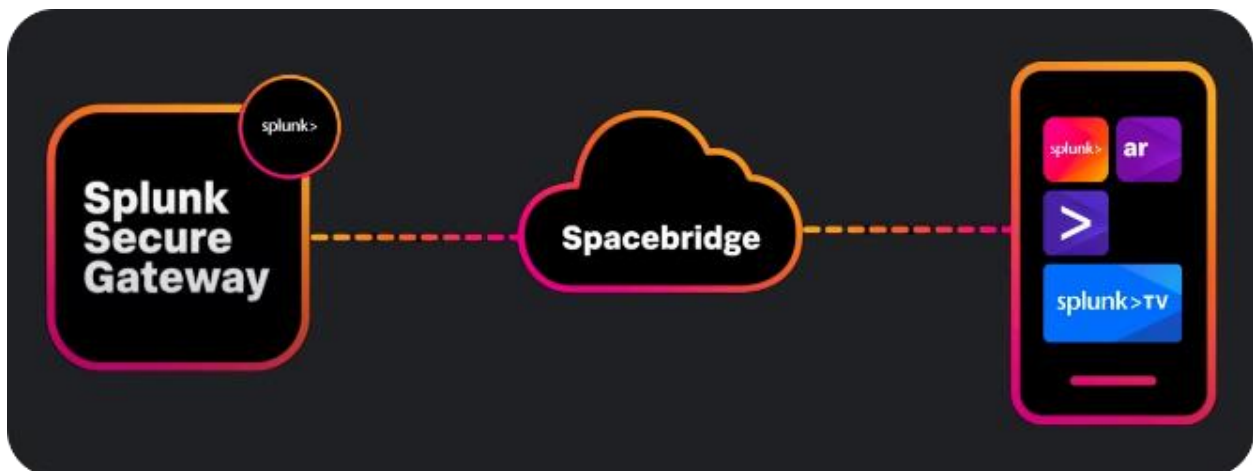


Figure 44: Splunk Alert Ticketing System

- **Communication Platform (SlackBot):** Facilitates real-time collaboration between security analysts, network engineers, and other relevant personnel.



Infrastructure

- **Dedicated Servers:** Host essential university services:
 - Web Server
 - Mail Server



- **SIEM Servers:** Dedicated systems for running Splunk and Wazuh (for redundancy and load balancing purposes)

Project Workflow Outline:

1. **Network Segmentation:** Logically dividing the network to isolate critical assets, implement access controls, and enhance security posture.
2. **Firewall Configuration:** Developing and implementing firewall rules tailored to our network, balancing security and functionality.
3. **SIEM Deployment and Configuration:**
 - Installing and configuring Splunk and Wazuh as our primary and redundant solutions.
 - Defining log sources and relevant collection agents.
 - Developing custom dashboards and alerts relevant to our security requirements.
4. **Ticketing System Integration:** Establishing a seamless connection between our SIEM and ticketing system(s) for efficient incident management.
5. **Real-Time Communication Setup:** Integrating Slack to foster swift information sharing and response coordination.
6. **Testing and Refinement:** Rigorously testing the system under simulated incidents and adjusting configurations as needed.
7. **Documentation:** Creating comprehensive documentation covering system architecture, configuration, incident response procedures, and maintenance guidelines.

4.3. Timeline or Gantt chart

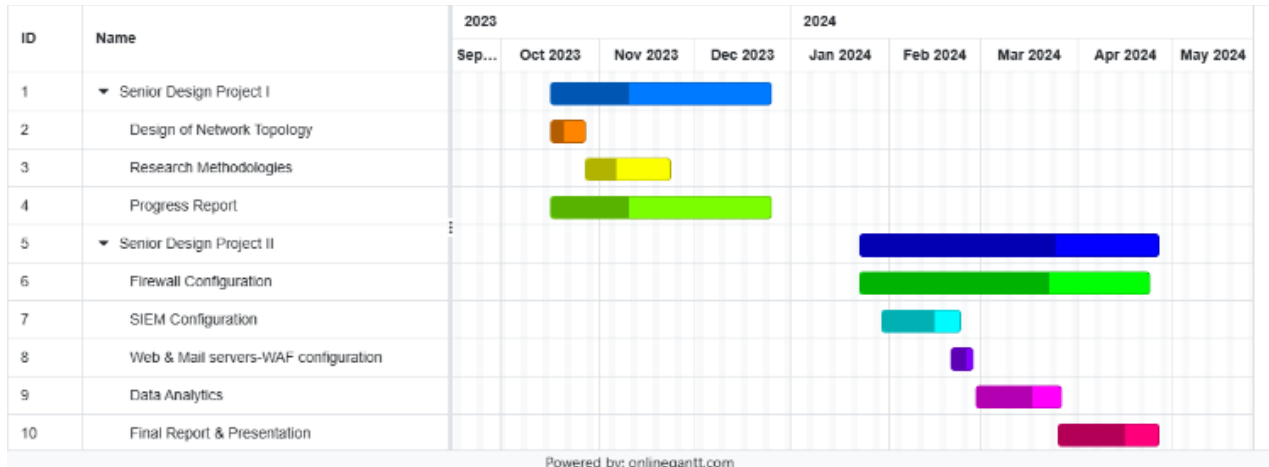


Figure 45: Gantt Chart

4.4. Testing/Verification/Validation of results

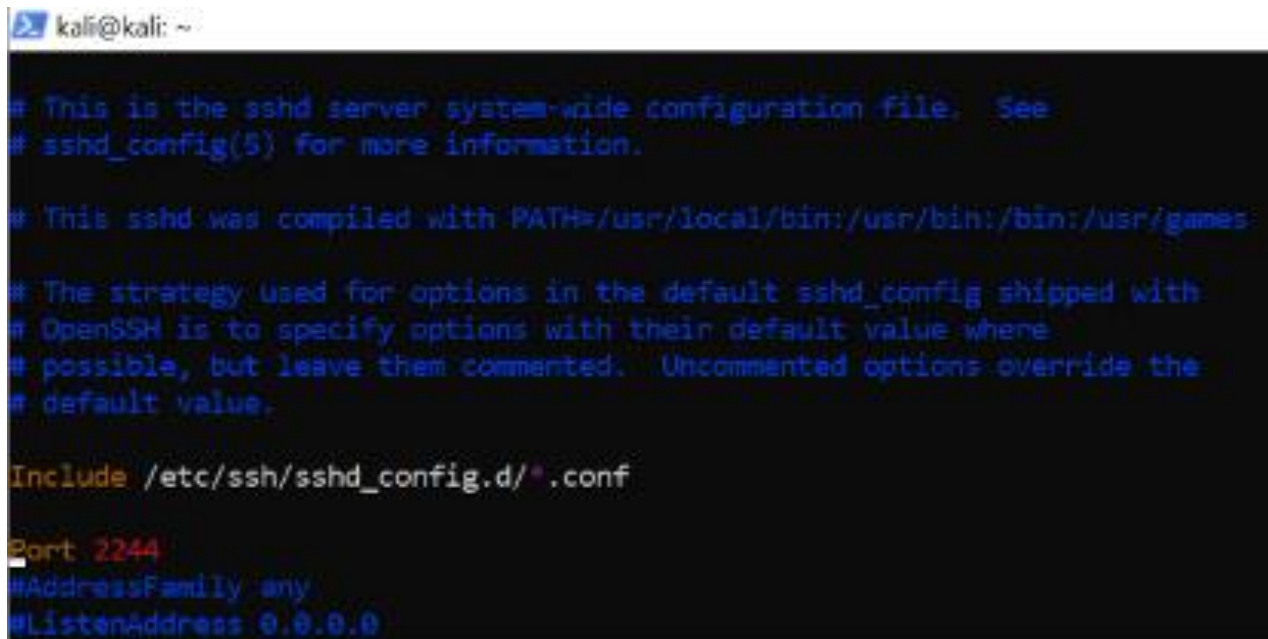
Wazuh Testing:

Below we see that our port is on default value 22, however according to security best practices we need to change it, so we follow the remediation.

ID ↑	Title	Target
3000	SSH Hardening: Port should not be 22	File: /etc/ssh/sshd_config
Rationale Changing the default port you may reduce the number of successful attacks from zombie bots, an attacker or bot doing port-		
Remediation Change the Port option value in the sshd_config file.		
Description The ssh daemon should not be listening on port 22 (the default value) for incoming connections.		
Check (Condition: all) • f:\$sshd_file → Ir:*# && r:Port && Ir:(s*)t*22\$		
Compliance nist_800_53: CM.1 pci_dss: 2.2.4		

Figure 46: Changing SSH Port

In /etc/ssh/sshd.config file we change port 22 to port 2244

A terminal window on a Kali Linux system showing the content of the /etc/ssh/sshd_config file. The text is displayed in a monospaced font with syntax highlighting. The 'Port' directive is highlighted in red and set to 2244. Other visible lines include comments about the configuration file, the PATH, and the strategy for options, as well as the 'Include' directive for the configuration directory and the 'AddressFamily' and 'ListenAddress' directives.

```
kali@kali: ~  
# This is the sshd server system-wide configuration file. See  
# sshd_config(5) for more information.  
  
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games:  
  
# The strategy used for options in the default sshd_config shipped with  
# OpenSSH is to specify options with their default value where  
# possible, but leave them commented. Uncommented options override the  
# default value.  
  
Include /etc/ssh/sshd_config.d/*.conf  
  
Port 2244  
#AddressFamily any  
#ListenAddress 0.0.0.0
```

Figure 47: SSH Port Configured to 2244

Now we cannot enter with the default port.

```

(kali@kali)-[~]
$ sudo vim /etc/ssh/sshd_config
[sudo] password for kali:

(kali@kali)-[~]
$ systemctl restart sshd
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'ssh.service'.
Authenticating as: kali,,, (kali)
Password:
==== AUTHENTICATION COMPLETE ====

(kali@kali)-[~]
$ systemctl restart ssh.service
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'ssh.service'.
Authenticating as: kali,,, (kali)
Password:
==== AUTHENTICATION COMPLETE ====

(kali@kali)-[~]
$ exit
Connection to 10.10.10.130 closed.
PS C:\Users\Azarin> ssh kali@10.10.10.130
ssh: connect to host 10.10.10.130 port 22: Connection refused
PS C:\Users\Azarin>

```

Figure 48: Verification of Port Change

But can connect with port 2244

```

PS C:\Users\Azarin> ssh kali@10.10.10.130 -p 2244
kali@10.10.10.130's password:
Permission denied, please try again.
kali@10.10.10.130's password:
Linux kali 6.1.0-kali9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1kali1 (2023-05-12) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Apr 21 12:10:57 2024 from 10.10.10.1
(kali@kali)-[~]
$

```

Figure 49: Verification of Port Change

In Webserver machine, we enter `/var/ossec/etc/ossec.conf` machine where we can find SCA section, we see that interval of scanning machine is every 12h, for big organizations it is normal, however, to see the result of our change in Events, we need to restart the wazuh_agent machine.

```
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>
```

Figure 50: Time Interval of Scanning Machine

After restarting we see that our frailer changed to passed.

Time	rule.description	rule.level	rule.id
Apr 21, 2024 @ 20:24:51	SCA summary: System audit for Unix based systems: Score less than 30% (25)	9	19005
Apr 21, 2024 @ 20:24:50.145	System audit for Unix based systems: SSH Hardening: Port should not be 22: Status changed from failed to passed	3	19010
Apr 21, 2024 @ 20:24:43.590	Host-based anomaly detection event (rootcheck).	7	510
Apr 21, 2024 @ 20:24:43.495	Host-based anomaly detection event (rootcheck).	7	510

Checks (23)

Refresh

Export formatted

ID ↑	Title	Target	Result
3000	SSH Hardening: Port should not be 22	File: /etc/ssh/ssh_config	Passed

Figure 51: Validation of SCA report

What Achieved:

Before:

Virtual Machines: with different OS and resources vulnerable varying levels beginning from the Application, Session, and other

Staff: No Active Directory Management, no DNS, NTP configuration

Student: No Active Directory Management

Firewall: No network segmentation, functionality, redundancy

SIEM: Absence of traffic control. No IDS, no usage of Splunk or Wazuh

Web and Mail: vulnerable in major layers (like Application, Session and etc)

After:

Packet Inspection for firewall tuning and feature extraction, Applied Rulesets (whitelists included) to arm empty firewall to NGFW, Active Directory Management, Ticketing System from scratch and application ready product to isolate the alert inspection from basic to advanced, contribution to open-source project for smooth integration and customization of add-on/plugins

5. Conclusion

5.1 Discussion of results

Our study on Automated cybersecurity event analysis resulted in considerable improvements in threat detection and overall security posture. The system's data analytics capabilities, when paired with a specific Intrusion Detection System (IDS), enabled more accurate identification of network abnormalities and suspicious behavior than typical human monitoring approaches. This resulted in speedier detection of possible attacks, allowing to perform more timely mitigation steps and reduce any possible damage. Furthermore, integrating security solutions such as Splunk and Wazuh enabled centralized management of logs and monitoring. This complete perspective of network operations speeds up the process of detecting and analyzing security issues. While the project had great outcomes, there is always place for improvement. Future developments might involve the integration of additional security technologies for a more comprehensive approach to security. Additionally, adding machine learning algorithms into the system may improve its capacity to identify cyberattacks. The system's ability to scale must be examined to guarantee that it can accommodate future campus expansion as well as the constantly evolving spectrum of cybersecurity threats.

5.2 Future Work

We want to mention that this project is a huge project needing more people involved in and cannot be completed in several months. For the future we plan to protect against emerging wireless assaults, switch the wireless network totally to WPA3, the latest and strongest Wi-Fi security standard. Furthermore, we will prioritize adding security measures that are expressly designed to reduce privilege escalation attempts. This could include enforcing the principle of least privilege for user accounts, using application whitelisting to limit unauthorized software execution, and implementing additional endpoint security controls to identify and avoid unusual behavior within user accounts with high privileges. Furthermore, we are planning to integrate Intrusion Prevention Systems (IPS) across the network in order to actively block anomaly detected traffic recognized by our detection systems. Also, a complete backup and disaster recovery strategy planned to be created. This strategy will include frequent backups of key data to secure remote locations, as well as well-defined protocols for recovering information and systems in the event of an attack or unexpected outage.

6. Acknowledgement

Special thanks to our supervisor Nariman Aliyev who led our project, Natig Zeynalzade for responsive validation and verification, and Orkhan Mammadov for resource optimization and other invaluable support which cannot be fully described here.

7. References

Julio Cesar Bueno de Camargo, "OPNsense Beginner to Professional: Protect networks and build next-generation firewalls easily with OPNsense"

M. Hristov, M. Nenova, G. Iliev and D. Avresky, "Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT"

T. Shanmugam and B. Malarkodi, "Analysis of Campus Network Management Challenges and Solutions"

8. Abbreviations

DMZ - **Demilitarized Zone**, isolated network that is placed between a trusted interior network and an outside network that is considered untrusted.

CIA - **Confidentiality, Integrity, Availability**, is the security model which focuses on the defense of the integrity, availability, as well as privacy of information systems and information.

MTU - **Maximum Transfer Unit**, the largest packet size that can be transmitted on a network.

FTP - **File Transfer Protocol**, network protocol for transferring files between computers.

DNS - **Domain Name System**, system that translates human-readable domain names into machine-readable IP addresses.

IDS - **Intrusion Detection System**, a system that checks the integrity of the network and alerts when suspicious activity occurs.

IPS - **Intrusion Prevention System**, a system that does nothing but stop the malicious traffic detected by an IDS in a preventive measure against such attacks.

MTTR - **Mean Time to Repair**, the mean duration an incident resolves.

OU - **Organizational Unit**, one of the ways to bond users, computers, and other resources in the network directory.

IT - **Information Technology**, the area in which one architects, builds, or maintains the computer systems.

TCP - **Transmission Control Protocol**, network protocol that provides the necessary measures to ensure highly reliable transmission.

IP - **Internet Protocol**, particular protocol which is used for communication on internet.

UTM - **Unified Threat Management**, it serves as a single security device to combine such security services as firewall, IPS, and web filtering.

GUI - **Graphical User Interface**, graphical user interface that replaces text-based commands with icons and menus.

VPN - **Virtual Private Network**, secure tunnel that allows encrypting data traffic over a public network.

IDC - **Internet Data Center**, site where computer systems and related equipment is located for the internet.

HTTP - **Hypertext Transfer Protocol**, the protocol used by the web servers and browsers while they communicate with each-other.

NGFW - **Next-Generation Firewall**, firewall with an extensive feature set that includes deep packet inspection as well as application control.

NGIPS - **Next-Generation Intrusion Prevention System**, an IPS that has great abilities to identify advanced threats.

IoT - **Internet of Things**, network of physical things with inner software, sensors and other technologies for transferring and processing data.

VM - **Virtual Machine**, a virtual computer that behaves as a physical computer.

DVWA - **Damn Vulnerable Web Application**, an intentionally vulnerable web application used for security testing.

OWASP - **Open Web Application Security Project**, non-profit organization promoting an open and impartial way of web security.

IBM - **International Business Machines**, multinational technology company.

SIEM - **Security Information and Event Management**, system that collects and analyzes security events from various sources.

SSH - **Secure Shell**, which is a secure protocol for accessing remote servers to run commands over the network

JSON - **JavaScript Object Notation**, simple but powerful data interchange format.

XSS - **Cross-Site Scripting**, certain types of web security vulnerabilities, enables the attackers to inject malicious scripts into the websites.

SQL - **Structured Query Language**, programming language which was developed to manipulate relational databases.

HTTPS - Hypertext Transfer Protocol Secure, securing data transfer in HTTP protocol, by using encryption.

SSL/TLS - Secure Sockets Layer/Transport Layer Security, communication protection protocol that is based on algorithms that secure communication between the client and server.

ISO/IEC - International Organization for Standardization/International Electrotechnical Commission, international standard-setting organizations that maintain highly comprehensive standards which cover almost all products and services.

NIST - National Institute of Standards and Technology, government agency that develops quality standards and calibrations for technology and measurements.

VLAN - Virtual Local Area Network, a logical bunching up of devices into a physical LAN that can be possibly treated as a different network.

NAT - Network Address Translation, technique for translating private IP addresses into public IP addresses.

RAM - Random Access Memory, not to be confused with ReadOnlyMemory, the computer's operational memory that stores data for temporary use.

SPI - Stateful Packet Inspection, firewall technique that uses a stateless inspection of network connection to enforce the control of traffic to determine if accepted.

SCA – Security Configuration Assessment, focuses on doing a check to ensure that the configuration is secure and not vulnerable to any known and relevant vulnerabilities. The checks in this kind of control system use a ground-rule to a system at a particular time.