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: Mr. Nariman Aliyev
Industry Mentor: [Code Academy] Natig Zeynalzade
Industry Mentor: [ADA, Lead Infrastructure Manager] Orkhan Mammadov

Baku, May 2024

## Table of Contents

References

Appendices

1. List and description of sub-components used in the project
2. System block diagram
3. Circuit diagrams
4. Flowcharts
5. In-depth description of technologies used it the project
6. Program codes
7. Images of the final product
8. Screen shots of the software interface

## 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 lead to finding optimal solutions to mitigate them with low cost of MTR 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, this 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

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.

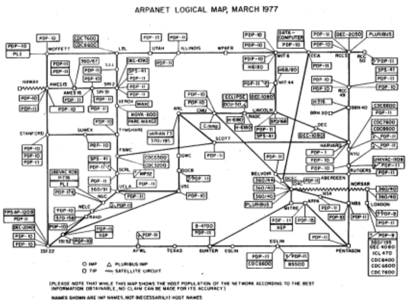


*Figure 1) ARPANET infrastructure, March 1977*

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: The COVID-19 pandemic necessitated a rapid transition to a virtualized environment for our university. This swift shift exposed critical vulnerabilities within the existing cybersecurity infrastructure, leaving the university susceptible to a surge in cyberattacks. Distributed Denial-of-Service (DDoS) attacks and brute-force login attempts significantly disrupted core university functions, creating a domino effect. Students faced difficulties registering for courses and accessing essential online learning platforms like Blackboard, MicrosoftTeams etc, fluctuating their academic progress. University staff, including security personnel, IT professionals, and instructors, were also impacted by the disruptions, hindering their ability to effectively support the virtual learning environment. The inadequacy of the current monitoring systems became apparent, as they were unable to efficiently detect and respond to these evolving threats. This highlighted the urgent need for a robust Security Information and Event Management (SIEM) solution, coupled with enhanced security configurations, to proactively mitigate vulnerabilities and expedite recovery procedures in the event of an attack.

The significant problem statement arises from actions that include attacks targeting the availability component of the CIA triangle. Attacks continue to occur even after classifying network users and putting security measures in place, including creating a Demilitarized Zone to protect vital assets. Vulnerabilities in the internal network architecture are typically overlooked in favor of protecting vital attack routes from outside threats.

As a result, hackers take advantage of these weaknesses to target user groups with greater levels of authority to obtain administrative access and maybe steal confidential information. The fact that assaults targeting availability continue to occur despite security measures being put in place and an Intrusion Detection System that has been specially designed to fit the network architecture of the institution highlights the necessity of a thorough approach to threat analysis and mitigation. To solve this issue and maintain network availability and uninterrupted operations within university campus networks, a comprehensive understanding of both internal and external vulnerabilities, proactive threat identification, and the implementation of targeted security measures are all necessary.

By implementing such a system, the university can ensure a more secure and resilient virtual environment, safeguarding the integrity of its online services and protecting the academic experience of students and staff.

## 2. Literature Review

The most recognizable component of security architecture is the firewall, a word that is frequently used in the information security industry. Moreover, it is not unexpected that while the view has changed much throughout time, the concept has not. Firewalls have always been a part of business environments, even with the increase of new capabilities in the perimeter security sector.

### 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.

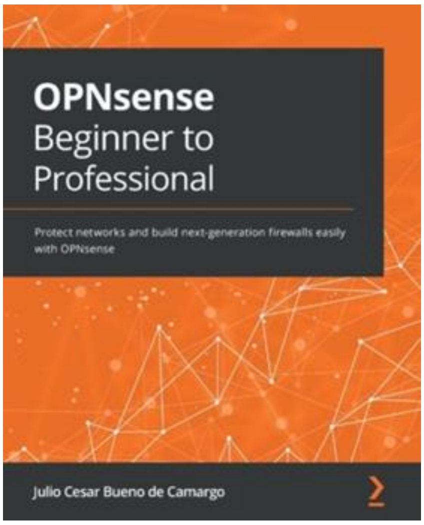

OPNsense
Beginner to Professional
Protect networks and build next-generation firewalls easily with OPNsense
Julio Cesar Bueno de Camargo

figure 2) OPNsense guideline book.

Date of Publication: 24 June 2022

ISBN-13 = 978-1801816878

ISBN-10 = 1801816875

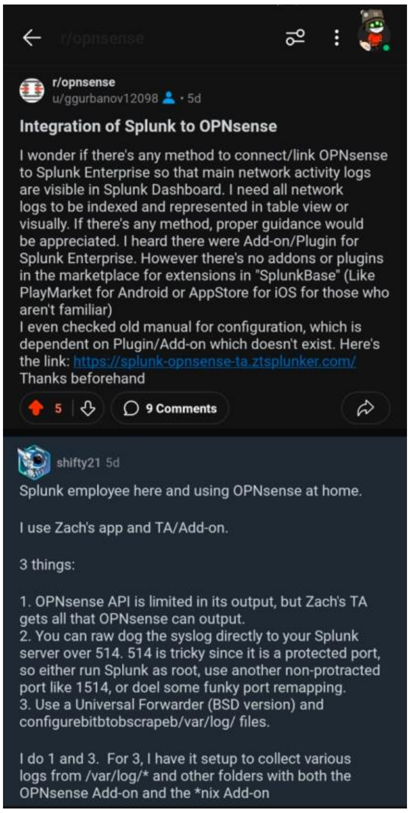
## 3. Design Concepts

### 3.1 Alternative Approaches

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 is capable of running 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 chat on Reddit platform for integrating OPNSense with Splunk, since we could not find valid documentation about it.



r/opnsense
u/ggurbanov12098 · 5d

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 PlayMarket 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-ta.ztsplunker.com/
Thanks beforehand

shifty21 5d

Splunk employee here and using OPNsense at home.

I use Zach's app and TA/Add-on.

3 things:

1. OPNsense API is limited in its output, but Zach's TA gets all that OPNsense can output.
2. You can raw dog the syslog directly to your Splunk server over 514. 514 is tricky since it is a protected port, so either run Splunk as root, use another non-protracted port like 1514, or doel some funky port remapping.
3. Use a Universal Forwarder (BSD version) and configurebitbtobscrapeb/var/log/ files.

I do 1 and 3. For 3, I have it setup to collect various logs from /var/log/* and other folders with both the OPNsense Add-on and the *nix Add-on

figure 3) Questionaree 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 similar to 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, whereis 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 version 17.

### 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 is set up with several interfaces connected to above given IP ranges accordingly, each designated for specific roles such as Staff, Student, DMZ, and SIEM, ensuring clear segmentation of network traffic and roles. This

**Commented [1]:** 3.2. Detailed Description of Solutions multi-interface setup is central to network security and traffic balancing.

### Advanced Port Management

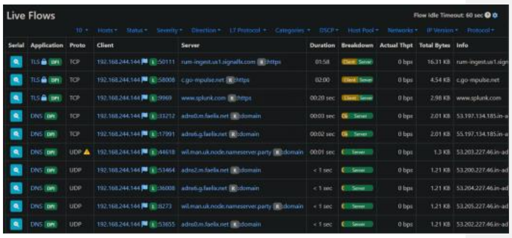
OPNSense is configured to provide GUI access via the Staff interface on port 8443 and SSH access on port 2244, showcasing best practices in changing default ports to reduce the likelihood of automated attacks. By allowing administrative access through a single interface and user, it effectively demonstrates user access control and the principle of least exposure.

### Ntopng

In the enhancement of the campus network's security posture, OPNSense was incorporated with Ntopng (a high-performance network traffic analysis tool) on 172.16.10.2 on port 3000. Ntopng is built-in service of OPNSense, pivotal for its advanced monitoring capabilities, providing with detailed insights into network usage and behavior.

Ntopng on OPNSense offers granular visibility into network traffic, allowing us the real-time observation and analysis of data flows across the campus network. By collecting extensive logs, Ntopng aids in the retention of important traffic data, which is essential for forensic analysis in the event of a security incident, especially while making attacks like DoS and Brute Force it was crucial for log analysis. The service provides comprehensive network statistics and filtering making it possible to detect abnormal patterns that may indicate security threats or network misuse, furthermore to download as Wireshark and JSON formats for extensive analysis.

**Ntopng Configurations**:

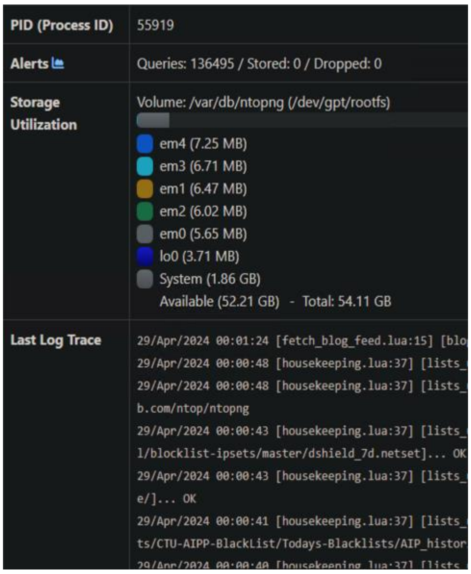


Live Flows

Flow Idle Timeout: 60 sec

| 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 | Cli 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 | Cli 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 | C 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 | C 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 | C 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 | C 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 | C 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)

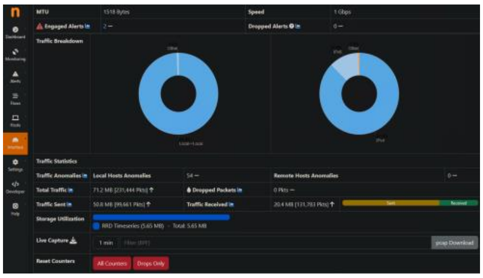
- em4 (7.25 MB)
- em3 (6.71 MB)
- em1 (6.47 MB)
- em2 (6.02 MB)
- em0 (5.65 MB)
- lo0 (3.71 MB)
- System (1.86 GB)

Available (52.21 GB) - Total: 54.11 GB

Last Log Trace

```
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_
```

figure 6) the storage space being used by Ntopng on data interfaces along with available storage space.



MTU 1518 Bytes | Speed 1 Gbps

Engaged Alerts 2 — | Dropped Alerts 0 —

Traffic Statistics

Traffic Anomalies: Local Hosts Anomalies 54 — | Remote Hosts Anomalies 0 —

Total Traffic 71.2 MB [231,444 Pkts] ↑ | Dropped Packets 0 Pkts —

Traffic Sent 50.8 MB [99,661 Pkts] ↑ | Traffic Received 20.4 MB [131,783 Pkts] ↑ | Sent | Received

Storage Utilization: RRD Timeseries (5.65 MB) - Total: 5.65 MB

Live Capture: 1 min

Reset Counters: All Counters | Drops Only

figure 7) Description anomalies and MTR.

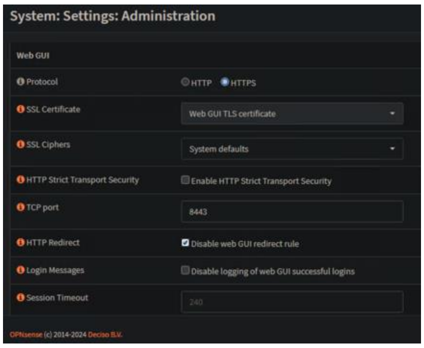
## WAF

For WAF (web application firewall), we configured Nginx, built-in service on OPNSense. The use of Nginx within OPNSense extends its capabilities to include a robust Web Application Firewall. This service is critical for protecting the campus network's web-facing services from a multitude of vulnerabilities and attacks. Nginx's WAF functionalities actively screen and filter out malicious web traffic, preventing common attacks such as XSS, SQL injection, and other exploits that could compromise the integrity of the network.

## Configurations:

Changing the Default HTTPS Port

For security best practices and to avoid conflict with other services, the default HTTPS port was changed. This is a fundamental step in hardening the firewall as it helps obscure the administrative interface from automated scans that typically target default ports.



System: Settings: Administration

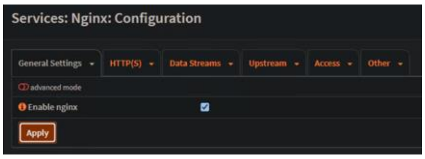
Web GUI

| | |
|---|---|
| Protocol | ○ HTTP ● HTTPS |
| SSL Certificate | Web GUI TLS certificate |
| SSL Ciphers | System defaults |
| HTTP Strict Transport Security | □ Enable HTTP Strict Transport Security |
| TCP port | 8443 |
| HTTP Redirect | ☑ Disable web GUI redirect rule |
| Login Messages | □ Disable logging of web GUI successful logins |
| Session Timeout | 240 |

OPNsense (c) 2014-2024 Deciso B.V.

figure 8) Default HTTPS port changing in Firewall.

### Enabling Nginx on OPNSense



Services: Nginx: Configuration

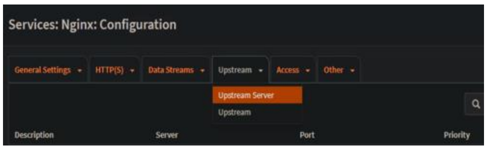
advanced mode

Enable nginx ☑

figure 9) Enabling nginx plugin in firewall.

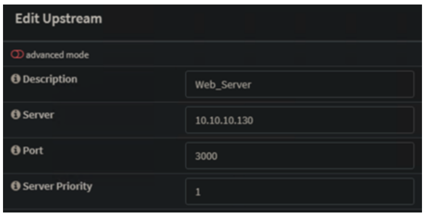
Nginx is activated via the Services menu, under the Nginx Configuration option. This step is essential for initializing the WAF functionalities that Nginx provides.

### Upstream Server Configuration



Services: Nginx: Configuration

| Description | Server | Port | Priority |
|---|---|---|---|

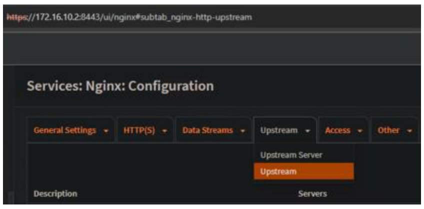


Edit Upstream

advanced mode

| | |
|---|---|
| Description | Web_Server |
| Server | 10.10.10.130 |
| Port | 3000 |
| Server Priority | 1 |

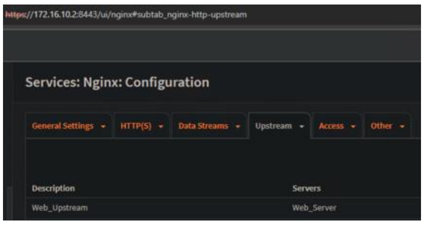
An upstream server is defined to manage the backend servers that Nginx protects. This configuration is crucial as it determines how Nginx routes requests to the web applications and services behind the WAF



https://172.16.10.2:8443/ui/nginx#subtab_nginx-http-upstream

Services: Nginx: Configuration

| Description | Servers |
|---|---|

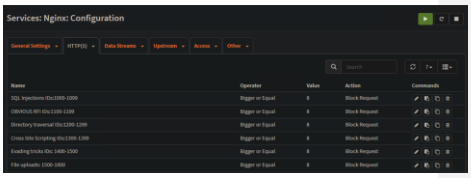


https://172.16.10.2:8443/ui/nginx#subtab_nginx-http-upstream

Services: Nginx: Configuration

| Description | Servers |
|---|---|
| Web_Upstream | Web_Server |

### Naxsi Rules Integration



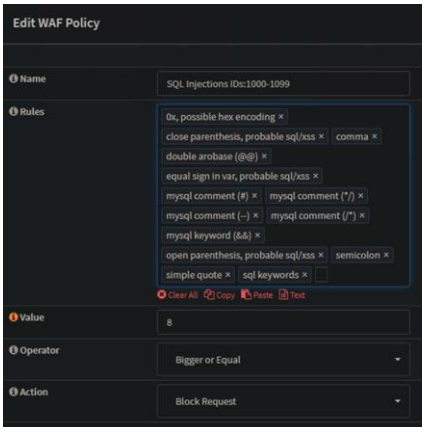
Services: Nginx: Configuration

| Name | Operator | Value | Action | Commands |
|---|---|---|---|---|
| SQL Injections IDs:1000-1099 | Bigger or Equal | 8 | Block Request | |
| OBVIOUS RFI IDs:1100-1199 | Bigger or Equal | 8 | Block Request | |
| Directory traversal IDs:1200-1299 | Bigger or Equal | 8 | Block Request | |
| Cross Site Scripting IDs:1300-1399 | Bigger or Equal | 8 | Block Request | |
| Evading tricks IDs: 1400-1500 | Bigger or Equal | 8 | Block Request | |
| File uploads: 1500-1600 | Bigger or Equal | 8 | Block Request | |

To enhance the security measures, Naxsi rules were downloaded and implemented. Naxsi is an open-source WAF module for Nginx, designed to protect web applications against various types of attacks, including SQL injection, cross-site scripting, and others.

The use of Naxsi rules within Nginx's WAF enables a robust set of predefined security policies that can be customized to meet the specific security needs of the campus network.

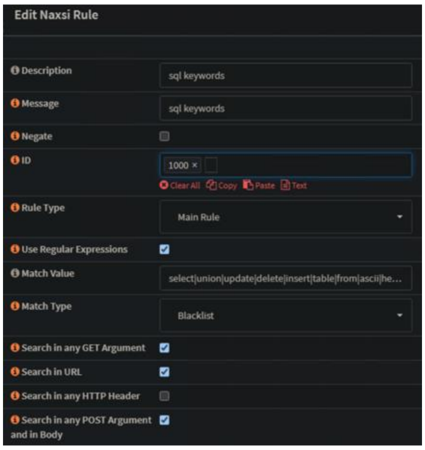
### SQL Injection (SQLi) Protection Rules



Edit WAF Policy

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

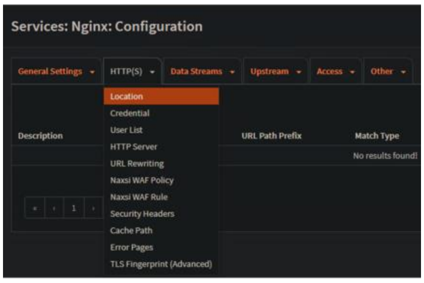
Specific rules against SQLi attacks were implemented as an example of the granular level of protection that can be achieved. SQLi is a prevalent and dangerous type of attack that the WAF configuration is designed to thwart, preventing unauthorized access to databases and the potential exfiltration of sensitive data.

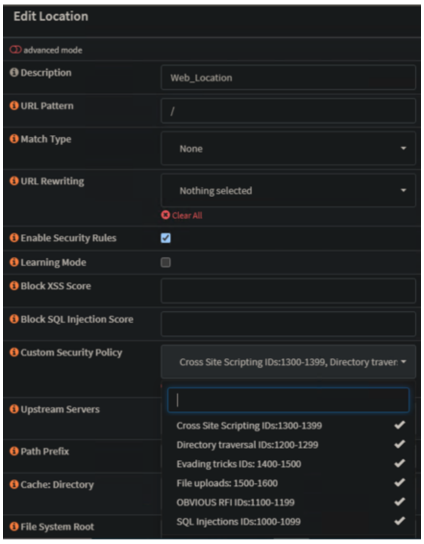


Edit Naxsi Rule

| | |
|---|---|
| Description | sql keywords |
| Message | sql keywords |
| Negate | □ |
| ID | 1000 ×<br>Clear All Copy Paste Text |
| Rule Type | Main Rule |
| Use Regular Expressions | ☑ |
| Match Value | select\|union\|update\|delete\|insert\|table\|from\|ascii\|he... |
| Match Type | Blacklist |
| Search in any GET Argument | ☑ |
| Search in URL | ☑ |
| Search in any HTTP Header | □ |
| Search in any POST Argument and in Body | ☑ |

## HTTPS Location and Configuration





Edit Location

advanced mode

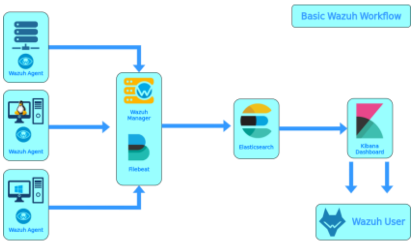
| | |
|---|---|
| Description | Web_Location |
| URL Pattern | / |
| Match Type | None |
| URL Rewriting | Nothing selected<br>Clear All |
| Enable Security Rules | ☑ |
| Learning Mode | □ |
| Block XSS Score | |
| Block SQL Injection Score | |
| Custom Security Policy | Cross Site Scripting IDs:1300-1399, Directory traver |
| Upstream Servers | Cross Site Scripting IDs:1300-1399 ✓<br>Directory traversal IDs:1200-1299 ✓ |
| Path Prefix | Evading tricks IDs: 1400-1500 ✓ |
| Cache: Directory | File uploads: 1500-1600 ✓<br>OBVIOUS RFI IDs:1100-1199 ✓ |
| File System Root | SQL Injections IDs:1000-1099 ✓ |

The HTTPS location block in Nginx was meticulously configured to define how HTTPS requests are handled. This includes the application of SSL/TLS settings, which ensure that the data transmitted is encrypted and secure.

The HTTPS location configuration also incorporates the application of the Naxsi rules, aligning the HTTPS traffic handling with the overall security strategy.

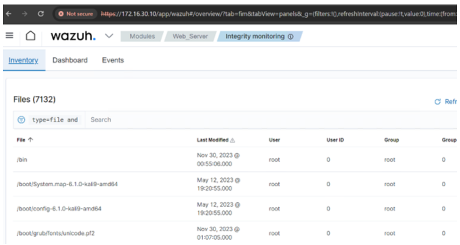
## Wazuh

Wazuh is an open-source security platform that provides a seamless and powerful solution for threat prevention, detection, and response. Its robust capabilities extend beyond simple log analysis, offering features like integrity monitoring, security configuration assessment, and active response. These functionalities make Wazuh a comprehensive tool for maintaining the security and compliance of the campus network.



**Integrity Monitoring**:

One of Wazuh's standout features is its file integrity monitoring system, which is critical for ensuring the security and consistency of the data that we used within our  campus network.



https://172.16.30.10/app/wazuh#/overview/?tab=fim&tabView=panels&_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:

Files (7132)

type=file and  Search

| File | Last Modified | User | User ID | Group | Group |
|---|---|---|---|---|---|
| /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 |

**Continuous Surveillance**:

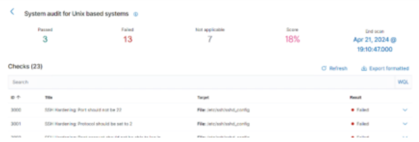
Wazuh's agent-based model allows it to constantly monitor and validate the integrity of system files and directories across network endpoints, detecting unauthorized changes in real time.

**Inventory Assessment**:

The integrity monitoring functionality is complemented by an inventory capability that records and tracks changes to the file system, thereby providing a transparent view of the integrity status of monitored systems.

**Security Configuration Assessment (SCA)**

Wazuh's Security Configuration Assessment tool is integral to maintaining security best practices across the campus network.



System audit for Unix based systems

| Passed | Failed | Not applicable | Score | End scan |
|---|---|---|---|---|
| 3 | 13 | 7 | 18% | Apr 21, 2024 @ 19:10:47.000 |

Checks (23)

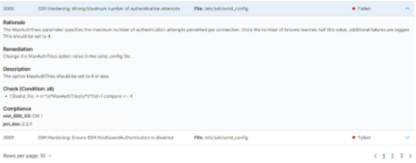
| ID | Title | Target | Result |
|---|---|---|---|
| 3000 | SSH Hardening: Port should not be 22 | File: /etc/ssh/sshd_config | Failed |
| 3001 | SSH Hardening: Protocol should be set to 2 | File: /etc/ssh/sshd_config | Failed |

**Vulnerability Identification:**

The SCA module analyzes systems against predefined security checks to identify misconfigurations or compliance drifts, which could potentially lead to vulnerabilities.

**Remediation Guidance:**

Upon detection of an issue, such as improper SSH configurations, Wazuh provides actionable recommendations for remediation, thus aiding in swiftly addressing security concerns.



3008 SSH Hardening: Wrong Maximum number of authentication attempts File: /etc/ssh/sshd_config ● Failed

**Rationale**
The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. Once the number of failures reaches half this value, additional failures are logged. This should be set to 4.

**Remediation**
Change the MaxAuthTries option value in the sshd_config file.

**Description**
The option MaxAuthTries should be set to 4 or less.

**Check (Condition: all)**
- f:$sshd_file -> n:^\s*MaxAuthTries\s*\t*(\d+) compare <= 4

**Compliance**
**nist_800_53:** CM.1
**pci_dss:** 2.2.4

3009 SSH Hardening: Ensure SSH HostbasedAuthentication is disabled File: /etc/ssh/sshd_config ● Failed

**Active Response for Real-Time Threat Mitigation:**

Active response is a reactive security measure that Wazuh implements to counteract active threats.

**Automated Countermeasures:**

When a threat is detected, Wazuh can execute predefined actions to mitigate the attack, such as blocking an IP address or modifying firewall rules.

**Custom Response Scripts:**

Administrators can define custom scripts that Wazuh will trigger upon specific alerts, enabling a tailored defensive stance 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 thorough 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 personnel.

Wazuh stands as an all-encompassing security tool that plays a vital role in protecting the campus network. Its deployment aligns with the objective of enhancing security through sophisticated monitoring, real-time threat detection, and automated responses, ensuring that the campus network remains secure and compliant with relevant standards.

### Splunk (SIEM)

Integration of a Ticketing System with Splunk for Enhanced Incident Response. To streamline incident response workflows and facilitate real-time communication, we integrated a ticketing system with our Splunk SIEM solution. This integration leverages Slack as an intermediary to bridge the gap between Splunk's robust alerting capabilities and team-wide incident communication channels.

**Technical Overview**. The integration process consists of the following key steps:

**Slack App Creation**:

We created a custom Slack app with Incoming Webhook functionality. This generated a unique webhook URL, which serves as the endpoint for Splunk to communicate with our designated Slack workspace.

**Splunk Integration**:

We installed the "Slack Notification Alert" integration from Splunkbase. This integration enables Splunk to send customized messages to Slack channels based on predefined alert conditions.

The webhook URL from our Slack app was configured within this Splunk integration, establishing the communication pathway.

**Alert Configuration**:

Within Splunk, we carefully defined alerts based on critical security criteria (e.g., failed heartbeat detection). These alerts were configured to trigger using search patterns relevant to the data sources we monitor.

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.

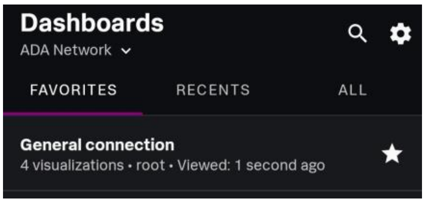
**Real-time Collaboration**:

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.

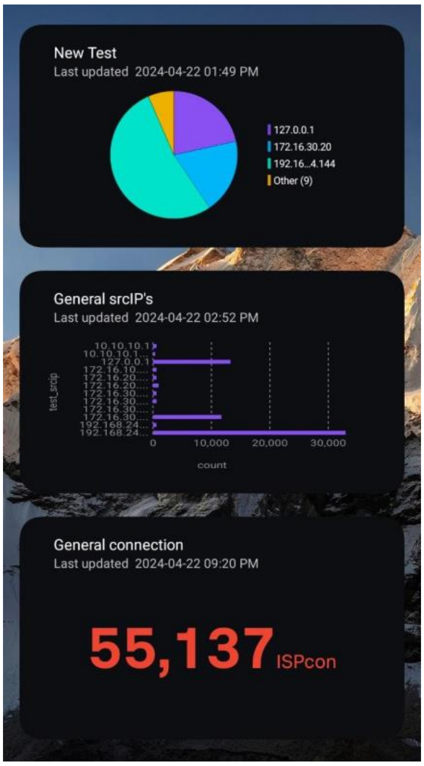
**Splunk Mobile Dashboards**:



Dashboards
ADA Network

General connection
4 visualizations • root • Viewed: 1 second ago

**Mobile Widgets for smooth UI/UX**

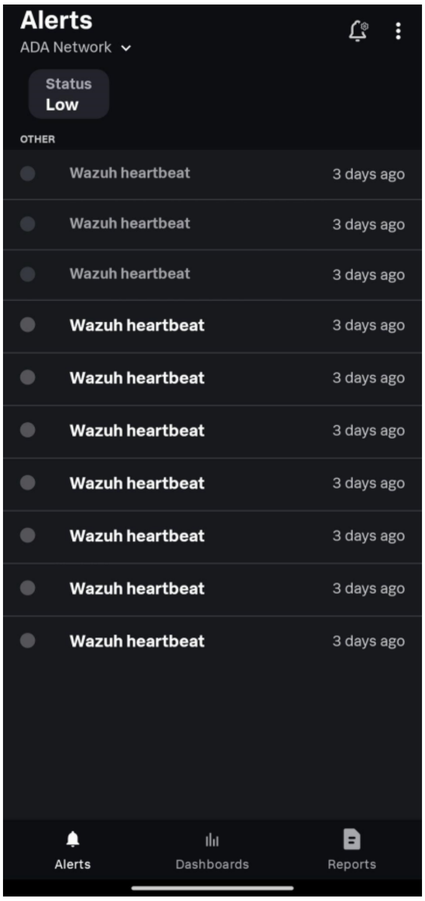


New Test
Last updated 2024-04-22 01:49 PM

General srcIP's
Last updated 2024-04-22 02:52 PM

General connection
Last updated 2024-04-22 09:20 PM

**Splunk Mobile Ticketing:**



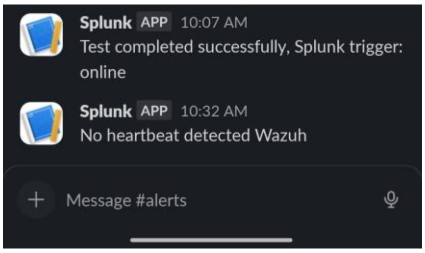
Alerts
ADA Network

Status
Low

OTHER

Wazuh heartbeat 3 days ago
Wazuh heartbeat 3 days ago
Wazuh heartbeat 3 days ago
Wazuh heartbeat 3 days ago
Wazuh heartbeat 3 days ago
Wazuh heartbeat 3 days ago
Wazuh heartbeat 3 days ago
Wazuh heartbeat 3 days ago
Wazuh heartbeat 3 days ago
Wazuh heartbeat 3 days ago

**Slack Ticketing integrated to Splunk:**



Splunk APP 10:07 AM
Test completed successfully, Splunk trigger: online

Splunk APP 10:32 AM
No heartbeat detected Wazuh

**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

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

## 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:**

evaluation of the solution's benefits for faster threat detection and streamlined incident response processes.

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.

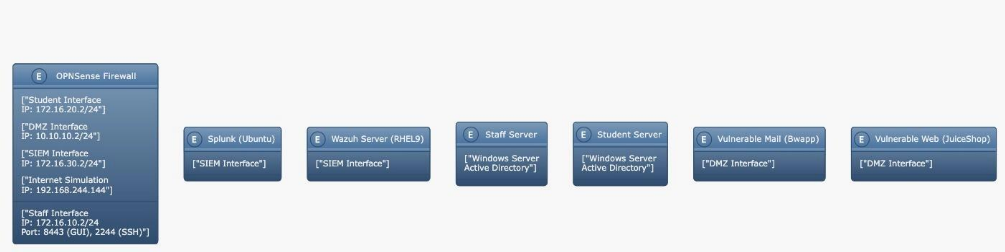
**Operational Efficiency:**

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

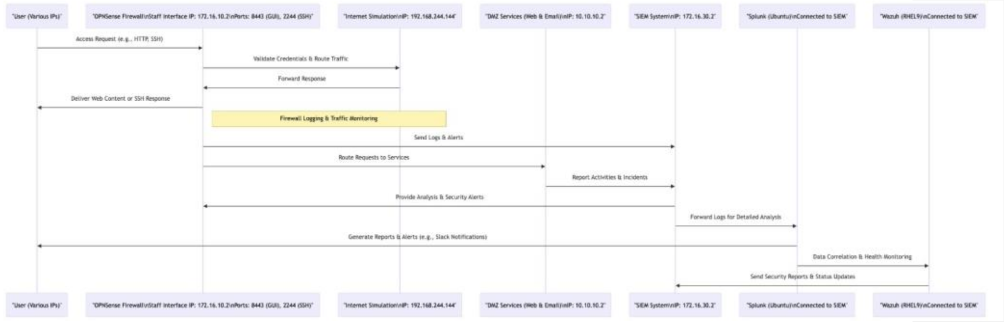
The inclusion of a well-developed network diagram with clear annotations will further strengthen this section of your report by providing a visual representation of the architecture's design and workflow.

## Diagrams:

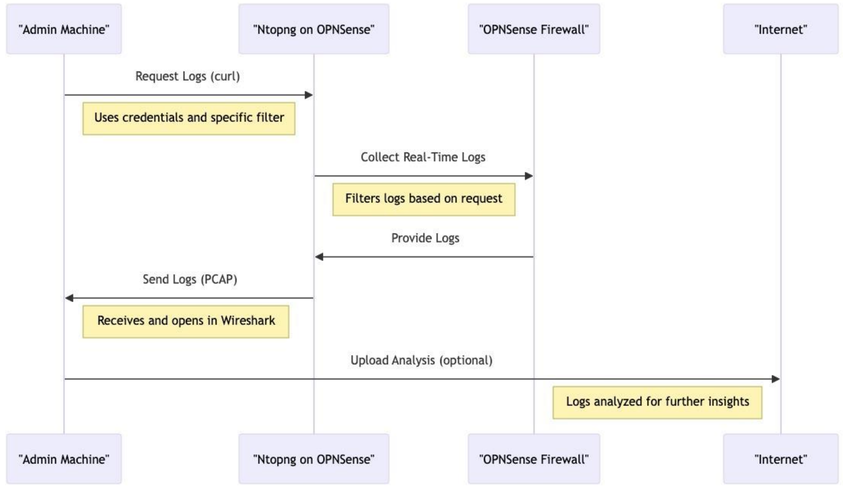
**Overall Topology:**



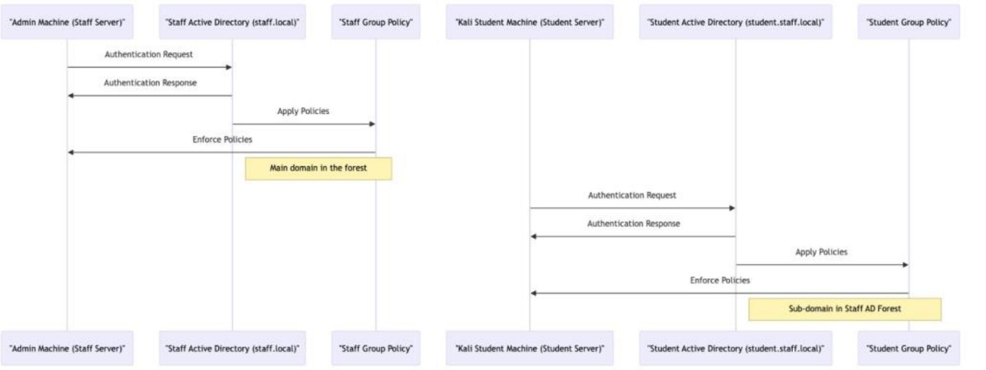
## OPNsense:


"User (Various IPs)"
"OPNSense Firewall\nStaff Interface IP: 172.16.10.2\nPorts: 8443 (GUI), 2244 (SSH)"
"Internet Simulation\nIP: 192.168.244.144"
"DMZ Services (Web & Email)\nIP: 10.10.10.2"
"SIEM System\nIP: 172.16.30.2"
"Splunk (Ubuntu)\nConnected to SIEM"
"Wazuh (RHEL9)\nConnected to SIEM"
Access Request (e.g., HTTP, SSH)
Validate Credentials & Route Traffic
Forward Response
Deliver Web Content or SSH Response
Firewall Logging & Traffic Monitoring
Send Logs & Alerts
Route Requests to Services
Report Activities & Incidents
Provide Analysis & Security Alerts
Forward Logs for Detailed Analysis
Generate Reports & Alerts (e.g., Slack Notifications)
Data Correlation & Health Monitoring
Send Security Reports & Status Updates

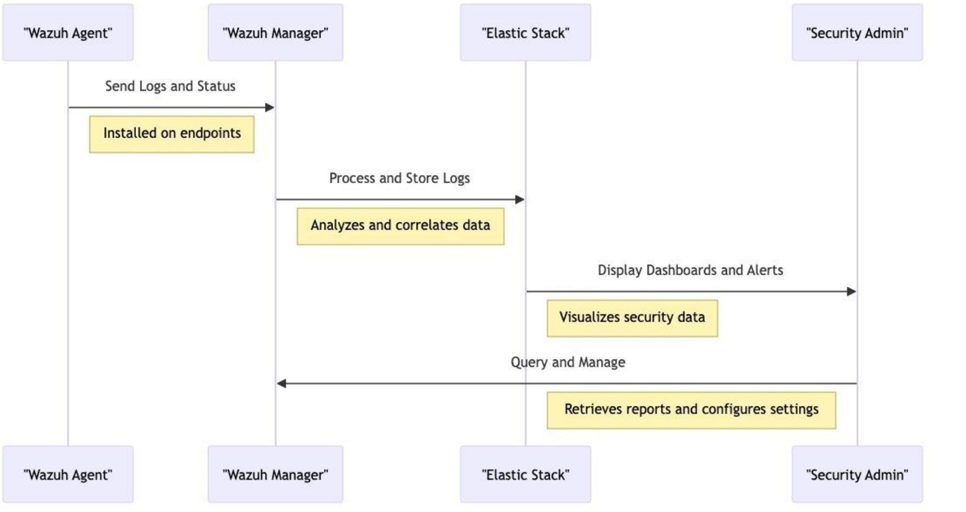
## Ntopng:


"Admin Machine"
"Ntopng on OPNSense"
"OPNSense Firewall"
"Internet"
Request Logs (curl)
Uses credentials and specific filter
Collect Real-Time Logs
Filters logs based on request
Provide Logs
Send Logs (PCAP)
Receives and opens in Wireshark
Upload Analysis (optional)
Logs analyzed for further insights

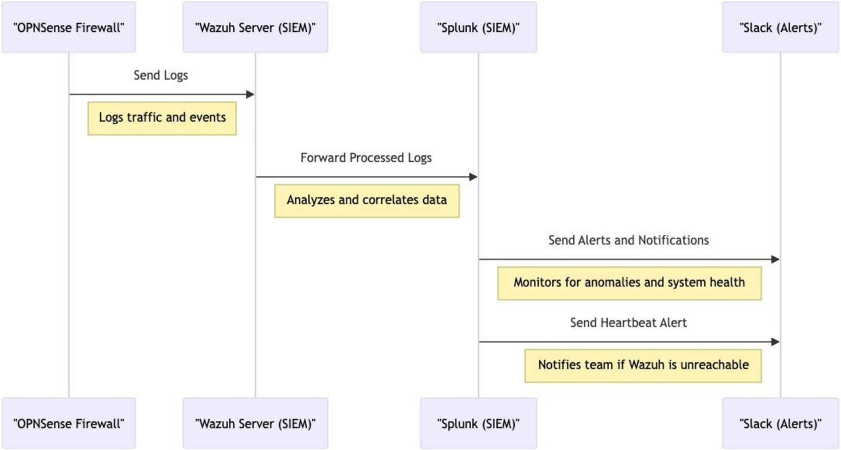
## System Infrastructure and GPO Relations:


"Admin Machine (Staff Server)"
"Staff Active Directory (staff.local)"
"Staff Group Policy"
"Kali Student Machine (Student Server)"
"Student Active Directory (student.staff.local)"
"Student Group Policy"
Authentication Request
Authentication Response
Apply Policies
Enforce Policies
Main domain in the forest
Authentication Request
Authentication Response
Apply Policies
Enforce Policies
Sub-domain in Staff AD Forest
"Admin Machine (Staff Server)"
"Staff Active Directory (staff.local)"
"Staff Group Policy"
"Kali Student Machine (Student Server)"
"Student Active Directory (student.staff.local)"
"Student Group Policy"

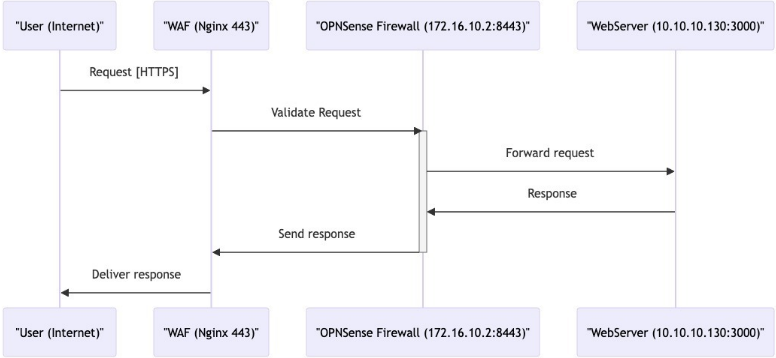
## Wazuh:


"Wazuh Agent"
"Wazuh Manager"
"Elastic Stack"
"Security Admin"
Send Logs and Status
Installed on endpoints
Process and Store Logs
Analyzes and correlates data
Display Dashboards and Alerts
Visualizes security data
Query and Manage
Retrieves reports and configures settings
"Wazuh Agent"
"Wazuh Manager"
"Elastic Stack"
"Security Admin"

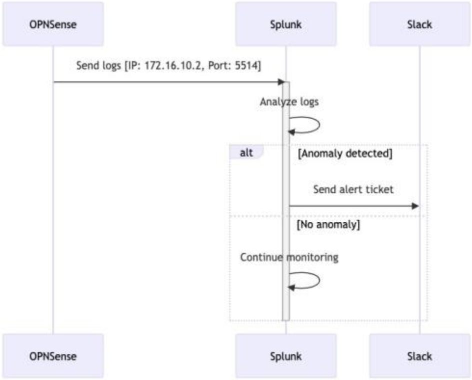
### Relation how Splunk works with OPNSense, Wazuh and Slack:



### Relation between WAF and OPNSense:



### Relation between Splunk, OPNSense and Slack:



## 3.6 Economic analysis

This project endeavors to streamline the identification and resolution of cybersecurity events, minimizing the required engagement of network teams and associated personnel. This optimization translates to a reduction in operational overhead and an enhanced ability to mitigate the potential economic fallout of service disruptions or security breaches.

Manual network and security monitoring necessitates a larger dedicated workforce, incurring substantial personnel costs. Furthermore, delays in responding to incidents can have cascading economic consequences. These may include reputational damage, data loss, financial penalties due to non-compliance, and direct revenue losses due to operational downtime. Our project uniquely leverages open-source solutions to provide a cost-effective foundation for automated cybersecurity event analysis. This approach stands in contrast to the substantial investments associated with commercial enterprise-grade systems, which frequently necessitate licensing fees, vendor support contracts, and recurring hardware upgrades. While such enterprise solutions are often indispensable for large organizations with strict uptime requirements, smaller businesses or institutions may find that developing a customized solution based on verified open-source projects offers greater flexibility and long-term cost efficiency.

Specifically, our project integrates OPNsense for robust firewall functionality, Wazuh for comprehensive Security Information and Event Management (SIEM), and Linux servers for system administration and maintenance. By contributing to and actively utilizing open-source projects, we not only gain access to powerful tools at minimal financial outlay, but also play a role in the ongoing development and improvement of these software ecosystems.

**Key Economic Considerations:**

**Reduced Labor Costs:**

Automation and enhanced efficiency lessen the need for continuous human intervention, lowering overall operational expenses related to network security.

**Mitigation of Downtime Impacts**:

Proactive event detection and streamlined response workflows aim to decrease the duration and economic consequences of service disruptions.

**Reputation Protection:**

A robust security posture bolsters the organization's reputation,

**Commented [2]:** burda ikinci detailed var preventing customer churn and potential financial losses associated with 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.

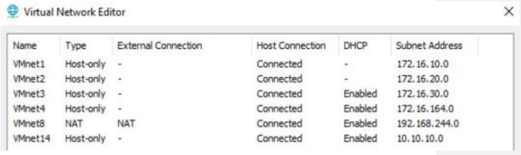
While a comprehensive cost-benefit analysis lies beyond the scope of this project, the qualitative economic advantages of our automated cybersecurity event analysis system are evident. Further research could quantify these benefits with greater precision, providing additional insights into the project's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

# 4. Implementation

## 4.1 Hardware Design

### OPNSense

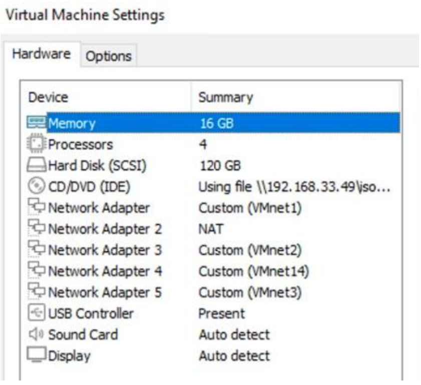
In our project we have used NAT instead of a bridged network, for internet simulation in Firewall. With bridged networking, the VM is accessible from the network. "NAT" on the other hand shares the hosts network connection by assigning the VMs an IP address from a private network, and translates network 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 VMent1 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.



Virtual Network Editor

| 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 |

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

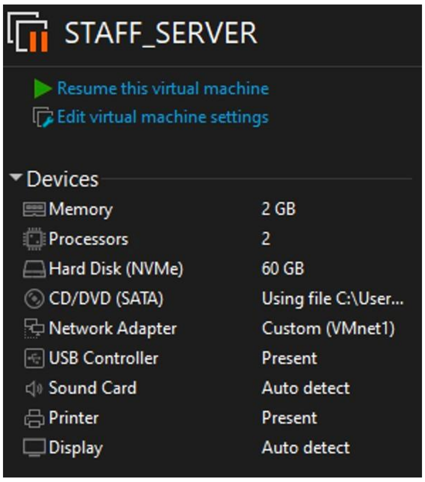


Virtual Machine Settings

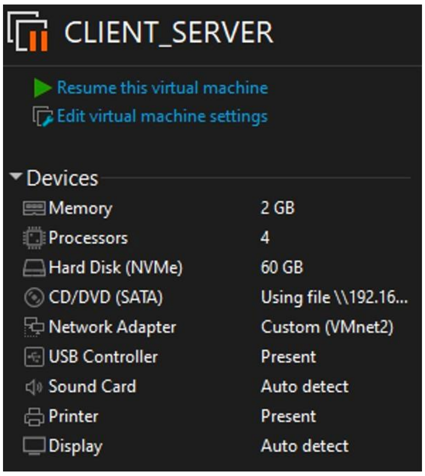
| Device | Summary |
|---|---|
| Memory | 16 GB |
| Processors | 4 |
| Hard Disk (SCSI) | 120 GB |
| CD/DVD (IDE) | Using file \\192.168.33.49\iso... |
| Network Adapter | Custom (VMnet1) |
| Network Adapter 2 | NAT |
| Network Adapter 3 | Custom (VMnet2) |
| Network Adapter 4 | Custom (VMnet14) |
|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

### 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



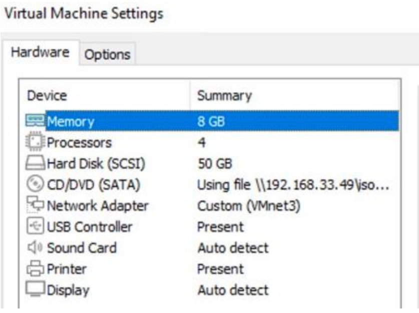
| | |
|---|---|
| Memory | 2 GB |
| Processors | 2 |
| Hard Disk (NVMe) | 60 GB |
| CD/DVD (SATA) | Using file C:\User... |
| Network Adapter | Custom (VMnet1) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |



| | |
|---|---|
| Memory | 2 GB |
| Processors | 4 |
| Hard Disk (NVMe) | 60 GB |
| CD/DVD (SATA) | Using file \\192.16... |
| Network Adapter | Custom (VMnet2) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

## Splunk Server

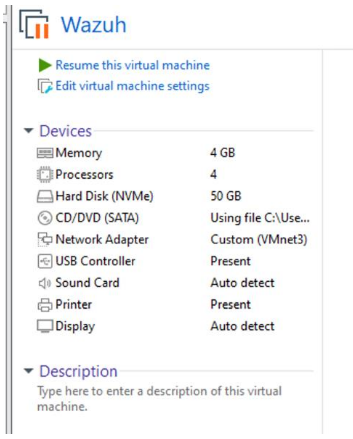
For the Splunk server we used default requirements that are given in Splunk documentations.



| Device | Summary |
|---|---|
| Memory | 8 GB |
| Processors | 4 |
| Hard Disk (SCSI) | 50 GB |
| CD/DVD (SATA) | Using file \\192.168.33.49\iso... |
| Network Adapter | Custom (VMnet3) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

## Wazuh

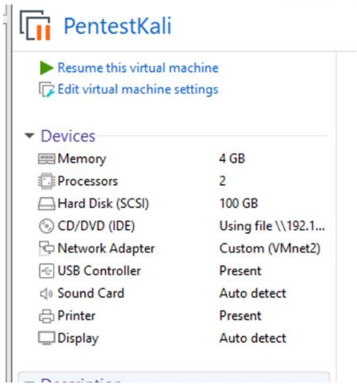
For Wazuh also we used default requirements for Wazuh Server installation.


Wazuh
Resume this virtual machine
Edit virtual machine settings
Devices

| | |
|---|---|
| Memory | 4 GB |
| Processors | 4 |
| Hard Disk (NVMe) | 50 GB |
| CD/DVD (SATA) | Using file C:\Use... |
| Network Adapter | Custom (VMnet3) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

Description
Type here to enter a description of this virtual machine.

## Student Kali Machine

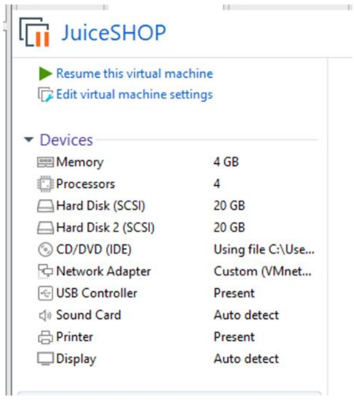


PentestKali

Devices

| | |
|---|---|
| Memory | 4 GB |
| Processors | 2 |
| Hard Disk (SCSI) | 100 GB |
| CD/DVD (IDE) | Using file \\192.1... |
| Network Adapter | Custom (VMnet2) |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

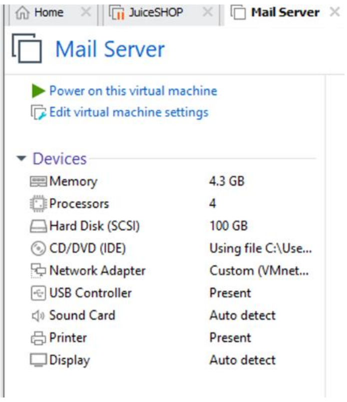
DMZ interface Servers



JuiceSHOP

Devices

| | |
|---|---|
| Memory | 4 GB |
| Processors | 4 |
| Hard Disk (SCSI) | 20 GB |
| Hard Disk 2 (SCSI) | 20 GB |
| CD/DVD (IDE) | Using file C:\Use... |
| Network Adapter | Custom (VMnet... |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |



Mail Server

Devices

| | |
|---|---|
| Memory | 4.3 GB |
| Processors | 4 |
| Hard Disk (SCSI) | 100 GB |
| CD/DVD (IDE) | Using file C:\Use... |
| Network Adapter | Custom (VMnet... |
| USB Controller | Present |
| Sound Card | Auto detect |
| Printer | Present |
| Display | Auto detect |

## 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**

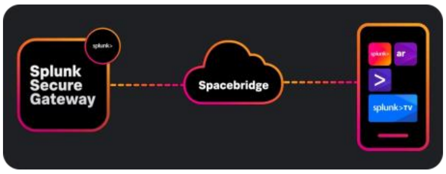
- **Next-Generation Firewall (OPNsense):** Provides a robust perimeter security foundation with features including:
  - Stateful packet inspection (SPI)
  - Intrusion detection / prevention systems (IDS/IPS)
  - Web content filtering (with Zen Armor integration)
  - VPN capabilities for secure remote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



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

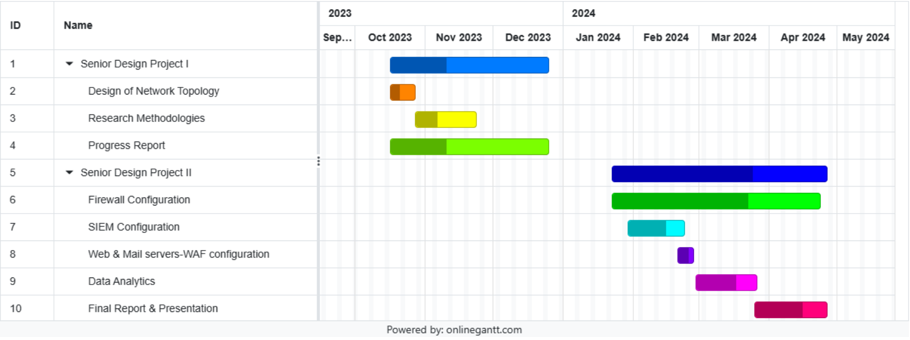
**Infrastructure**

- **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:**
   - o Installing and configuring Splunk and Wazuh as our primary and redundant solutions.
   - o Defining log sources and relevant collection agents.
   - o 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

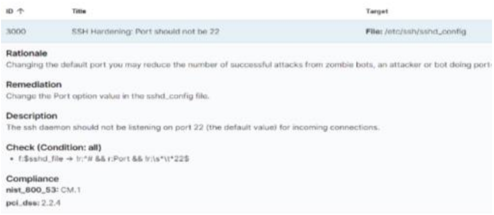


| ID | Name |
|---|---|
| 1 | Senior Design Project I |
| 2 | Design of Network Topology |
| 3 | Research Methodologies |
| 4 | Progress Report |
| 5 | Senior Design Project II |
| 6 | Firewall Configuration |
| 7 | SIEM Configuration |
| 8 | Web & Mail servers-WAF configuration |
| 9 | Data Analytics |
| 10 | Final Report & Presentation |

## 4.4 Verification and 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

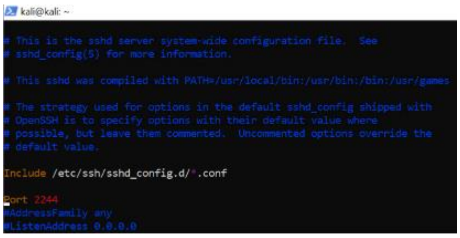
**Remediation**
Change the Port option value in the sshd_config file.

**Description**
The ssh daemon should not be listening on port 22 (the default value) for incoming connections.

**Check (Condition: all)**
- f:$sshd_file → !r:^# && r:Port && !r:\s*\t*22$

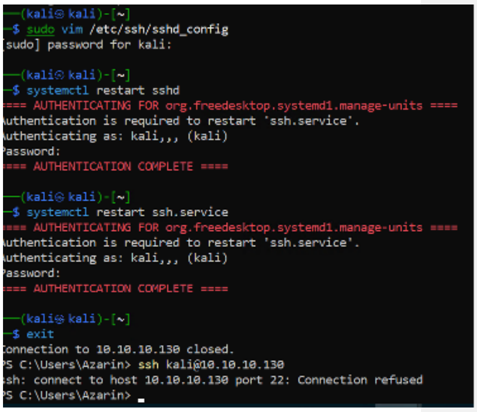
**Compliance**
**nist_800_53:** CM.1
**pci_dss:** 2.2.4

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



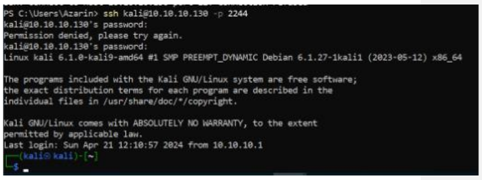
```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# 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
```

Now we cannot enter with the default port.



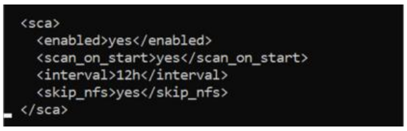
```
──(kali㉿kali)-[~]
─$ sudo vim /etc/ssh/sshd_config
[sudo] password for kali:

──(kali㉿kali)-[~]
─$ systemctl restart sshd
=== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
uthentication is required to restart 'ssh.service'.
uthenticating as: kali,,, (kali)
assword:
=== AUTHENTICATION COMPLETE ====

──(kali㉿kali)-[~]
─$ systemctl restart ssh.service
=== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
uthentication is required to restart 'ssh.service'.
uthenticating as: kali,,, (kali)
assword:
=== AUTHENTICATION COMPLETE ====

──(kali㉿kali)-[~]
─$ exit
onnection to 10.10.10.130 closed.
S C:\Users\Azarin> ssh kali@10.10.10.130
sh: connect to host 10.10.10.130 port 22: Connection refused
S C:\Users\Azarin> _
```

But can connect with port 2244



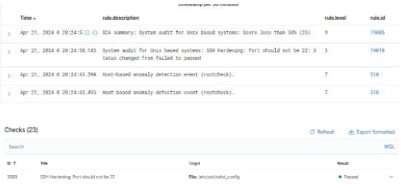
```
PS C:\Users\Azarin> ssh kali@10.10.10.130 -p 2244
kali@10.10.10.130's password:
Permission denied, please try again.
kali@10.10.10.130's password:
Linux kali 6.1.0-kali9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1kali1 (2023-05-12) x86_64

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)-[~]
└─$ _
```

In Web_Server 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>
```

After restarting we see that our frailer changed to passed.



|  | Time | rule.description | rule.level | rule.id |
|---|---|---|---|---|
| › | Apr 21, 2024 @ 20:24:5 | 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)

| ID ↑ | Title | Target | Result |
|---|---|---|---|
| 3000 | SSH Hardening: Port should not be 22 | File: /etc/ssh/sshd_config | ● Passed |

## 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. Abbreviations

DMZ - **Demilitarized Zone,** network segment that sits between a trusted internal network and an untrusted external network.

CIA – **Confidentiality, Integrity, Availability,** is a security model that emphasizes protecting the confidentiality, integrity, and accessibility of information systems and data.

MTR - **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,** system that monitors network traffic for suspicious activity.

IPS - **Intrusion Prevention System,** system that actively blocks malicious traffic detected by an IDS.

MTTR - **Mean Time to Repair,** the average time it takes to resolve an incident.

OU - **Organizational Unit,** way to group users, computers, and other resources in a network directory.

IT - **Information Technology,** the field dealing with the design, development, implementation, support or management of computer systems.

TCP - **Transmission Control Protocol,** network protocol that ensures reliable data transmission.

IP - **Internet Protocol,** the main communication protocol used on the internet.

UTM - **Unified Threat Management,** security appliance that combines multiple security functions like firewall, IPS, and web filtering.

GUI - **Graphical User Interface,** user interface that uses icons and menus instead of text commands.

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

IDC - **Internet Data Center,** facility that houses computer systems and related components for the internet.

HTTP - **Hypertext Transfer Protocol,** the protocol used to communicate between web servers and browsers.

NGFW - **Next-Generation Firewall,** firewall that offers advanced features like deep packet inspection and application control.

NGIPS - **Next-Generation Intrusion Prevention System, a**n IPS that provides advanced threat detection capabilities.

IoT - **Internet of Things,** network of physical devices embedded with software, sensors, and other technologies for connecting and exchanging data.

VM - **Virtual Machine,** a software computer that simulates a physical computer.

DVWA - **Damn Vulnerable Web Application,** a deliberately insecure web application used for security testing.

OWASP - **Open Web Application Security Project,** nonprofit organization that creates free and open standards for web application 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,** secure protocol for remote login and command execution.

JSON - **JavaScript Object Notation,** lightweight data interchange format.

XSS - **Cross-Site Scripting,** a type of web security vulnerability that allows attackers to inject malicious scripts into websites.

SQL - **Structured Query Language,** language used to interact with relational databases.

HTTPS - **Hypertext Transfer Protocol Secure,** the secure version of HTTP that uses encryption to protect data traffic.

SSL/TLS - **Secure Sockets Layer/Transport Layer Security**, encryption protocols that secure communication between a client and a server.

ISO/IEC - **International Organization for Standardization/International Electrotechnical Commission,** international organizations that set standards for a wide range of products and services.

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

VLAN - **Virtual Local Area Network,** logical grouping of devices within a physical LAN that can be treated as a separate network.

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

RAM - **Random Access Memory,** the computer's volatile memory that stores data for temporary use.

SPI - **Stateful Packet Inspection,** firewall technique that examines the state of a network connection to determine if traffic is allowed.