Secure Cybersecurity Home lab

(Front Page)

Project Report submitted to

St. Xavier's College – Autonomous Mumbai

For the partial fulfilment for the award of the degree of

Bachelor of Science (BSc) in

Information Technology

By

Neev Jain

(UID. : 215003)

Under the Supervision of

Mr. Aaron Johns

INFORMATION TECHNOLOGY

ST. XAVIER'S COLLEGE (AUTONOMOUS),

MUMBAI-400001, INDIA

April 2024

PROJECT CERTIFICATE

This is to certify that the project entitled _____ undertaken at the Information Technology Department of St. Xavier's College – Autonomous Mumbai has been submitted by: **Neev Jain (UID No: 215003)**, in partial fulfilment of Bachelor's in Information Technology degree (Semester VI) Examination. It is further certified that they have completed all required phases of the project.

Signature	Signature	Signature
(Internal Guide)	(Internal Examiner)	(External Examiner)

Signature	College Seal
(HOD – Information Technology department)	

Student Declaration

I, **Neev Jain (UID No: 215003)** do hereby, certify that:

1) that the project report titled, "Secure Cybersecurity Home Lab" which is being submitted in partial fulfillment of the requirements for the Degree of Bachelor of Science with a specialization in Information Technology is the result of the **original work** carried out by us under the guidance of the Prof Mr. Aaron Johns, faculty of Information Technology Department, St. Xavier's College, Mumbai-01.
2) This project has not previously formed the basis for the award of any degree, diploma, or certificate of this college or of any other college or university.
3) Whenever we have used materials (data, theoretical analysis, and text) from other sources, we have given due credit to them by providing references of them in the project documentation.

Date:

Place:

_____

Neev Jain

UID: 215003

Table of Contents

Brief Synopsis

My final year project introduces an innovative framework designed to bolster network security and monitoring capabilities through the seamless integration of multiple cutting-edge technologies. At its core lies a meticulously crafted amalgamation of pfSense firewall, Zenarmor Next Generation Firewall (NGFW), Wazuh Security Information and Event Management (SIEM) system, an offline AI solution, and a Kali Linux machine, each playing a pivotal role in fortifying the network's defenses and ensuring real-time threat detection and response.

The project begins by establishing pfSense as the cornerstone of the network architecture, serving as the central gateway tasked with enforcing robust security policies and facilitating secure internet access for connected virtual machines. Leveraging the power of Snort, an open-source intrusion detection and prevention system, pfSense enhances its capabilities, enabling proactive monitoring and defense against a myriad of potential threats.

In parallel, the integration of Zenarmor NGFW introduces a new dimension to the network's security posture. With its intuitive graphical user interface (GUI) and advanced traffic monitoring capabilities, Zenarmor empowers administrators to gain unprecedented visibility into network activities, swiftly identifying and mitigating potential security breaches in real-time. This sophisticated firewall solution also helps streamlines policy enforcement, ensuring adherence to organizational security protocols.

Complementing Zenarmor's real-time monitoring prowess is the incorporation of the Wazuh SIEM system, which serves as the centralized nerve center for

logging, analysis, and response. By aggregating and correlating data from various sources, including Zenarmor's logs, Wazuh provides invaluable insights into emerging threats and anomalous activities, enabling administrators to formulate custom response strategies tailored to their organization's unique security requirements. Additionally, Wazuh's flexibility allows for the development of custom rules, further enhancing its ability to detect and mitigate evolving threats effectively.

Furthermore, the project introduces an offline AI solution, addressing the critical need for safeguarding sensitive data processing in environments where internet connectivity may pose privacy and security risks. This standalone AI system operates independently of external networks, ensuring the confidentiality and integrity of sensitive information, making it an invaluable asset for scenarios such as exam environments or research facilities where data privacy is paramount.

The inclusion of a Kali Linux machine adds an additional layer of versatility to the project, provides a platform for conducting security assessments, penetration testing, and vulnerability analysis. By using its robust suite of tools and utilities, administrators can proactively identify and address security weaknesses within the network, further bolstering its resilience against potential cyber threats.

In summary, my project represents a holistic approach to network security and monitoring, leveraging the collective strengths of pfSense, Zenarmor NGFW, Wazuh SIEM, an offline AI solution, and Kali Linux to create a robust defense-in-depth strategy. By integrating these cutting-edge technologies, I aim to empower organizations with the tools and insights needed to safeguard their digital assets effectively in an ever-evolving threat landscape.

Problem Statement

In today's digital landscape, the proliferation of cyber threats poses a significant challenge to organizations seeking to safeguard their sensitive data and digital assets. Traditional security measures often fall short in providing comprehensive protection against evolving threats, leaving networks vulnerable to infiltration, data breaches, and malicious activities.

The lack of integrated solutions that offer real-time monitoring, proactive threat detection, and centralized management exacerbates this challenge, hindering organizations' ability to effectively identify and respond to security incidents in a timely manner. Additionally, the increasing complexity of network infrastructures and the diverse array of cyber threats further compound the issue, making it increasingly difficult for administrators to maintain a robust security posture.

Furthermore, the advent of sophisticated attack vectors, such as zero-day exploits, advanced persistent threats (APTs), and insider threats, underscores the need for innovative approaches to network security that go beyond traditional perimeter defenses and reactive security measures.

In educational settings, particularly during exams, ensuring academic integrity and preventing cheating among students is paramount. With the rise of remote learning and online exams, traditional methods of proctoring are no longer sufficient to deter cheating effectively. As a result, there is a growing demand for advanced proctoring solutions that leverage technology to monitor student activities during exams and prevent unauthorized behavior.

Therefore, in addition to addressing the broader challenges of network security and threat detection, this project aims to develop and implement a comprehensive solution for exam proctoring in educational institutions. By integrating advanced security technologies such as Zenarmor NGFW, Wazuh SIEM, and an offline AI solution, the project seeks to create a robust exam proctoring system capable of monitoring student activities in real-time, detecting unauthorized behaviour, and ensuring academic integrity.

For example, during a college exam conducted remotely, the integrated framework can monitor students' internet usage, flagging any attempts to access unauthorized resources or websites. The Wazuh SIEM system can analyse network traffic and user behaviour patterns, alerting proctors to suspicious activities such as copying and pasting from external sources or using unauthorized software. The offline AI solution can further enhance exam security by detecting and preventing attempts to use AI-powered cheating tools or accessing prohibited materials stored locally on students' devices.

Overall, the project seeks to address the dual challenges of network security and academic integrity by developing an integrated solution that not only protects sensitive data and digital assets but also ensures fairness and honesty in educational assessments. By leveraging advanced technologies and innovative approaches, the project aims to empower educational institutions with the tools and capabilities needed to maintain a secure and trustworthy exam environment in today's digital age.

Objective & Scope

Objective:

The primary objective of this project is to design, develop, and implement an integrated network security and monitoring framework that addresses the challenges of modern cybersecurity while also providing advanced proctoring capabilities for educational institutions. The project aims to achieve the following specific objectives:

- Develop a comprehensive understanding of network security principles, technologies, and best practices.
- Design and implement an integrated framework comprising pfSense firewall, Zenarmor NGFW, Wazuh SIEM, an offline AI solution, and a Kali Linux machine.
- Enhance network security through proactive threat detection, real-time monitoring, and centralized management capabilities.
- Develop custom rules and policies for intrusion detection, response, and mitigation based on threat intelligence and organizational requirements.
- Integrate advanced proctoring capabilities into the framework to monitor student activities during exams and prevent cheating.
- Test and evaluate the effectiveness of the integrated framework in simulated and real-world scenarios, including educational environments.

Scope:

The scope of this project encompasses the design, development, implementation, and evaluation of an integrated network security and monitoring framework with advanced proctoring capabilities. The project will focus on the following key areas:

- Network Security Components:
    - Configuration and deployment of pfSense firewall as the central gateway for network security.
    - Integration of Zenarmor NGFW for real-time monitoring, threat detection, and policy enforcement.
    - Implementation of Wazuh SIEM for centralized logging, analysis, and response.
    - Deployment of an offline AI solution for sensitive data processing and privacy protection.
    - Utilization of Kali Linux for security assessments, penetration testing, and vulnerability analysis.

- Proctoring Capabilities:
    - Development of proctoring features to monitor student activities during exams, including internet usage, software usage, and behavior patterns.
    - Integration of AI-based algorithms for detecting cheating behaviors, such as copying from external sources or using unauthorized tools.
    - Implementation of real-time alerts and notifications to proctors for suspicious activities during exams.

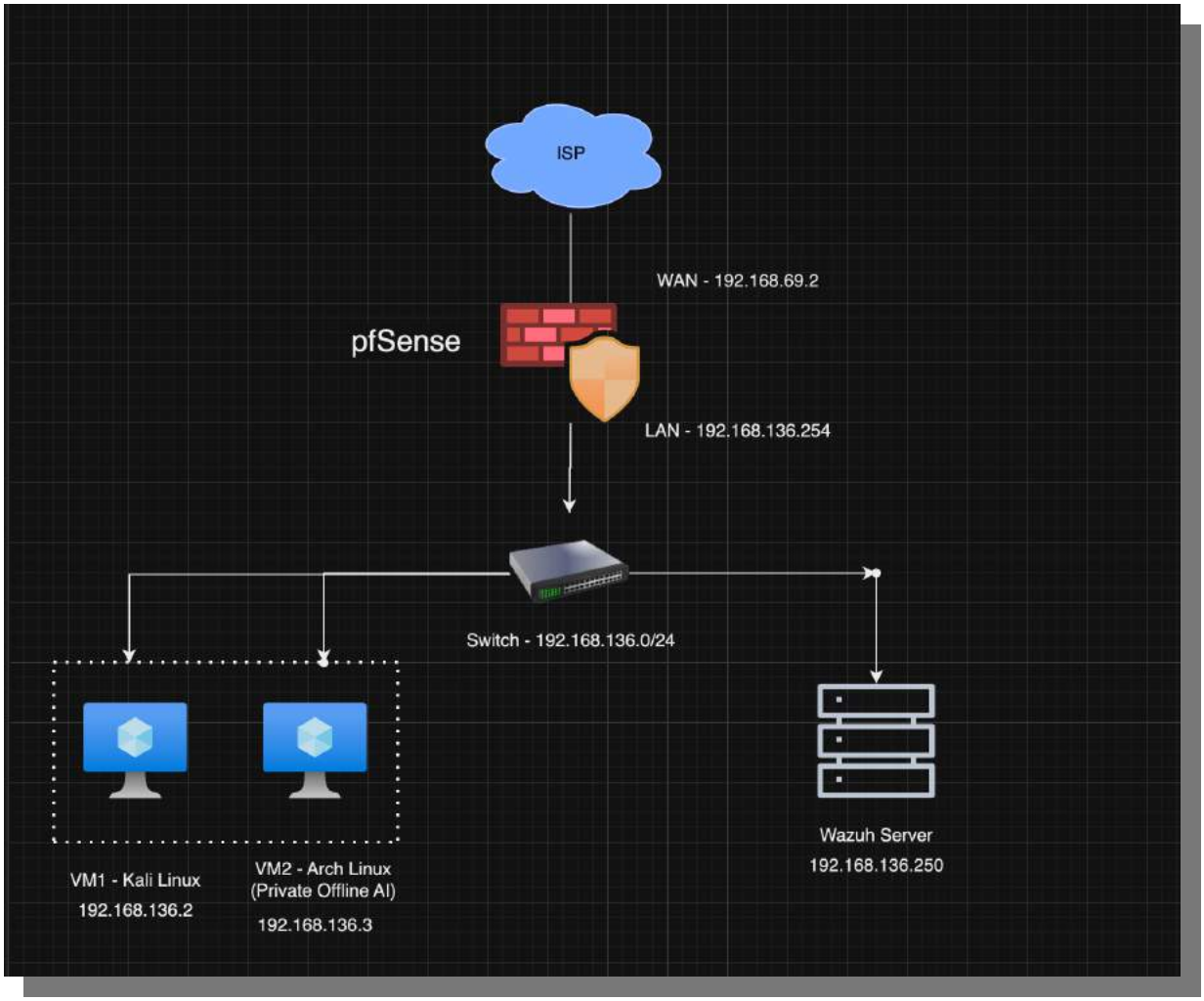
- Customization and Adaptation:
    - Customization of rules, policies, and configurations to meet the specific security requirements and operational needs of educational institutions.

    - Adaptation of the framework to different network environments, educational settings, and use cases, ensuring scalability and flexibility.

- Evaluation and Testing:
    - Evaluation of the integrated framework's effectiveness in detecting and mitigating cyber threats, as well as preventing cheating during exams.
    - Testing the framework in simulated and real-world environments to assess its performance, reliability, and usability.
    - Gathering feedback from stakeholders, including educators, students, and IT administrators, to identify areas for improvement and refinement.

Overall, the project aims to deliver a robust and versatile solution that not only enhances network security and monitoring capabilities but also addresses the specific challenges of exam proctoring in educational institutions.

System Design & Analysis



- **pfSense Firewall (Virtual Machine):**
  - **IP Address (LAN):** 192.168.136.254
  - **Gateway:** N/A (Acts as the central gateway)
  - **Functionality:**
    - Provides firewall, routing, and VPN services.
    - Acts as the primary point of entry/exit for network traffic.
    - Configured with Snort for intrusion detection and prevention.
    - Manages internet access for connected virtual machines.

- **Zenarmor NGFW (Virtual Machine):**
    - **IP Address:** 192.168.136.254
    - **Gateway:** N/A (Acts as the central gateway)
    - **Functionality:**
        - Next-Generation Firewall providing real-time monitoring, threat detection, and policy enforcement.
        - Integrated with pfSense for seamless traffic filtering and policy enforcement.

- **Wazuh SIEM (Virtual Machine):**
    - **IP Address:** 192.168.136.250
    - **Gateway:** 192.168.136.254 (pfSense Firewall)
    - **Functionality:**
        - Security Information and Event Management (SIEM) system for centralized logging, analysis, and response.
        - Receives logs from pfSense Firewall and Zenarmor NGFW for analysis and threat detection.

- **Offline AI (Virtual Machine):**
    - **IP Address:** 192.168.136.3
    - **Gateway:** 192.168.136.254 (pfSense Firewall)
    - **Functionality:**
    - AI-powered solution for sensitive data processing without internet connectivity.
    - Detects cheating behaviours during exams and ensures data privacy.

- **Kali Linux (Virtual Machine):**
    - **IP Address:** 192.168.136.2
    - **Gateway:** 192.168.136.254 (pfSense Firewall)
    - **Functionality:**
    - Platform for security assessments, penetration testing, and vulnerability analysis.
    - Used by administrators for network testing and troubleshooting.

Internet Access Provision:

The pfSense Firewall (UTM VM) acts as the primary gateway and provides internet access to all connected virtual machines. It manages internet connectivity through its WAN interface, which is typically connected to the external network (e.g., ISP router or external modem). The pfSense firewall is responsible for routing internet-bound traffic from internal VMs to the external network and vice versa, ensuring secure and controlled internet access for the entire network.

With these configurations, the network is set up to ensure secure communication, effective threat detection, and controlled internet access for the virtual machines within the UTM Virtual Machine environment.

- **Comprehensive Network Security:**

By leveraging a UTM Virtual Machine environment with components like pfSense Firewall, Zenarmor NGFW, and Wazuh SIEM, the system offers a comprehensive approach to network security.

The integration of multiple security layers enables proactive threat detection, real-time monitoring, and centralized management, enhancing the overall security posture of the network.

- **Effective Threat Detection and Response:**

The combination of pfSense Firewall with Snort IDS/IPS, Zenarmor NGFW, and Wazuh SIEM facilitates effective threat detection and response.

Real-time monitoring and centralized logging allow for rapid identification of security incidents, while custom rule development enables tailored response actions to mitigate threats effectively.

- **Secure Internet Access Management:**

The pfSense Firewall serves as the central gateway for internet access management, ensuring controlled and secure connectivity for all connected virtual machines.

With its routing and firewall capabilities, pfSense enforces security policies, filters malicious traffic, and prevents unauthorized access to external networks, enhancing overall network security.

- **Enhanced Academic Integrity:**

The integration of an offline AI solution and proctoring features within the network architecture enhances academic integrity during exams.

The offline AI ensures sensitive data processing without internet connectivity, addressing privacy concerns and safeguarding against cheating behaviours.

Proctoring features enable real-time monitoring of student activities, detection of unauthorized behaviour, and prompt intervention to maintain exam integrity.

- **Scalability and Flexibility:**

The modular design of the UTM Virtual Machine environment allows for scalability and flexibility in adapting to evolving security requirements.

Additional virtual machines or security components can be integrated into the architecture as needed, ensuring the system remains adaptable to changing threats and organizational needs.

- **Centralized Management and Analysis:**

The centralized logging and analysis provided by Wazuh SIEM enable efficient management of security events and incidents.

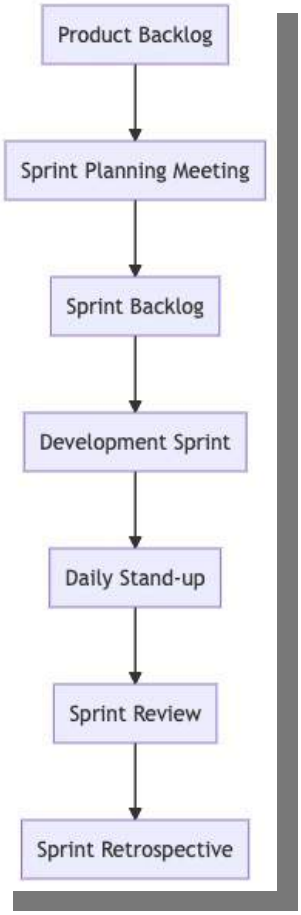
By correlating data from multiple sources, Wazuh SIEM provides valuable insights into emerging threats, facilitating informed decision-making and proactive security measures.

- **User-Friendly Configuration and Monitoring:**

The graphical user interface (GUI) of pfSense Firewall and Zenarmor NGFW simplifies configuration and monitoring tasks, making it accessible to administrators with varying levels of technical expertise.

Administrators can easily configure security policies, monitor network traffic, and respond to security incidents through intuitive interfaces, enhancing operational efficiency.

Software Engineering Paradigm



One software engineering paradigm that can be applied to the development and maintenance of the described system is the **Agile methodology**. Here's why Agile is suitable and how it can be implemented:

Why Agile:

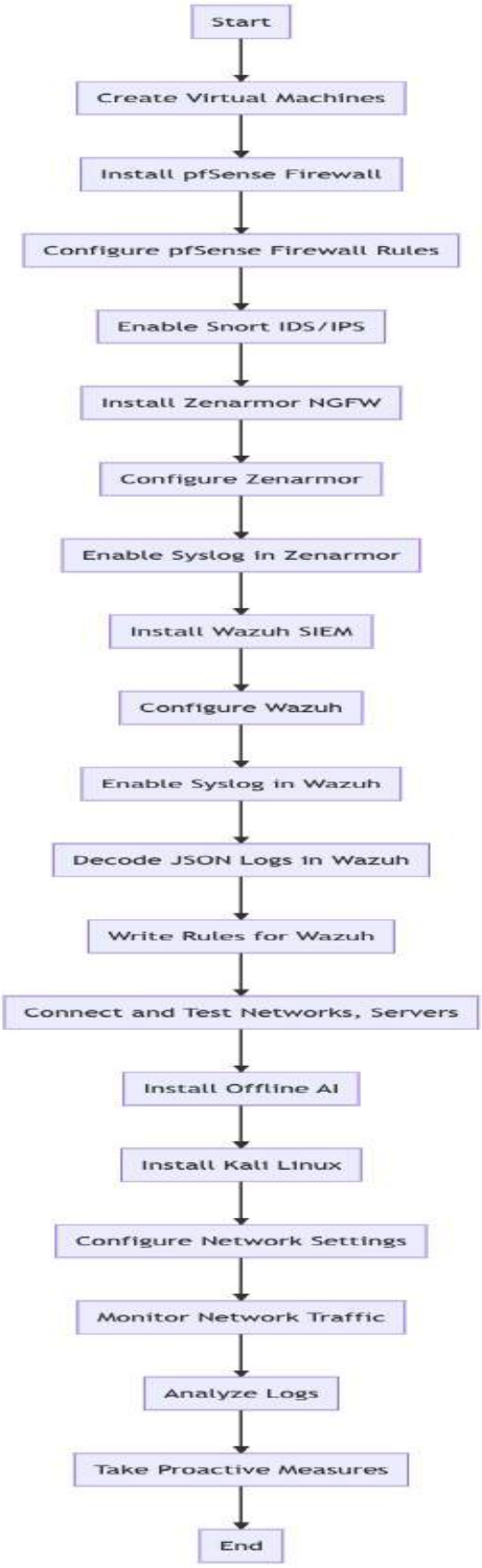
- **Iterative Development:** Agile promotes an iterative approach to development, allowing for incremental enhancements and adjustments based on feedback and changing requirements. This is particularly beneficial in the context of network security systems, where evolving threats and organizational needs necessitate continuous improvement and adaptation.
- **Flexibility:** Agile methodologies prioritize flexibility and responsiveness to change. Given the dynamic nature of cybersecurity and academic environments, where new threats emerge and requirements evolve rapidly, Agile enables teams to quickly pivot and adjust their approach to meet emerging challenges and user needs.
- **Collaboration and Communication:** Agile emphasizes collaboration and communication among team members, stakeholders, and end-users. In the context of developing a network security and proctoring system, close collaboration between security experts, educators, administrators, and students is essential to ensure that the system effectively addresses security concerns and meets user expectations.
- **User-Centric Design:** Agile encourages a user-centric approach to development, focusing on delivering value to end-users through continuous feedback and iteration. This is particularly relevant in the context of exam proctoring systems, where usability, accessibility, and adherence to academic integrity principles are paramount.

How Agile can be Implemented:

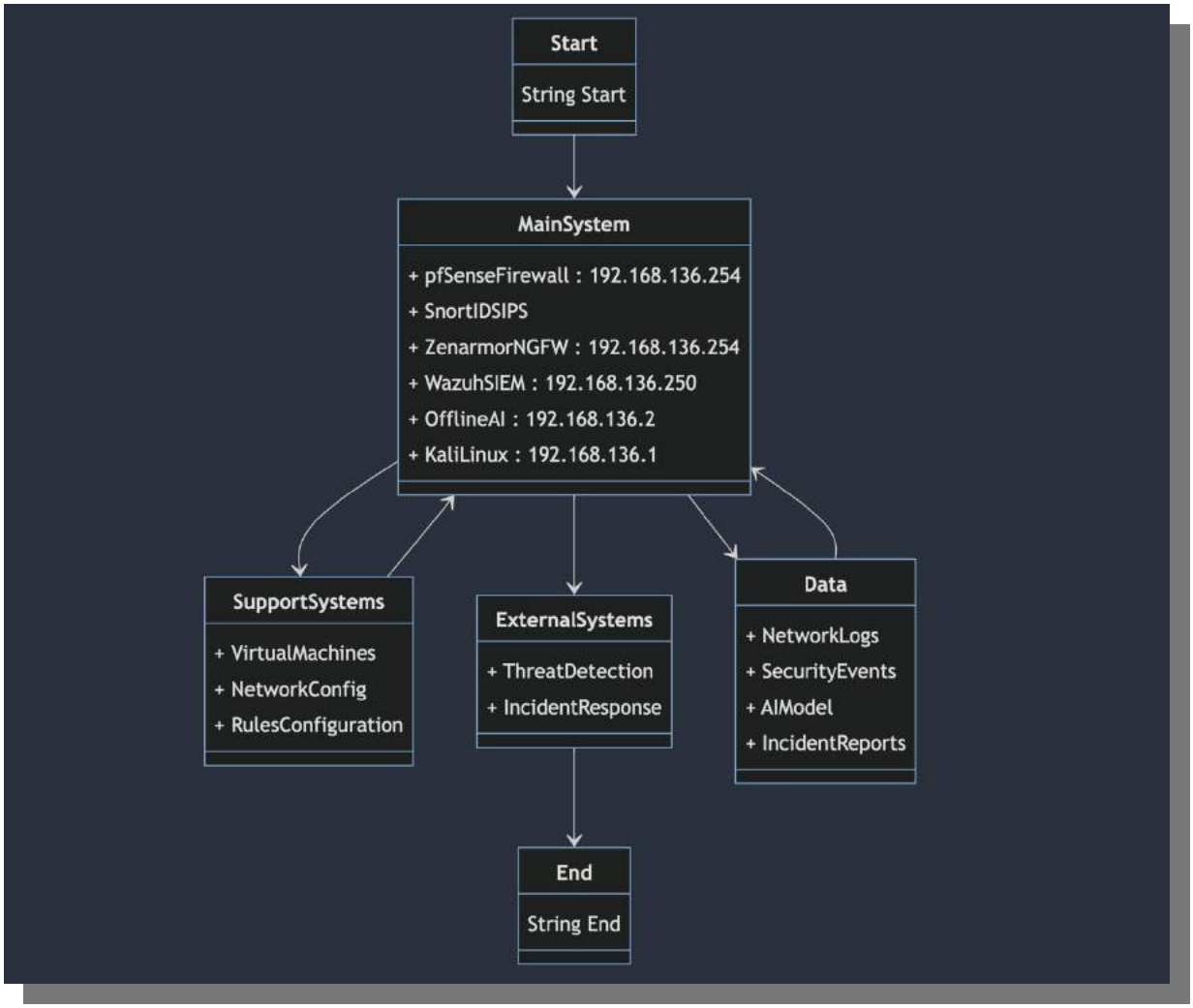
- **Scrum Framework:** Adopt the Scrum framework, which provides a structured approach to Agile development with defined roles, ceremonies, and artifacts. The Scrum framework includes regular sprint planning, daily stand-up meetings, sprint reviews, and retrospectives, enabling teams to manage their work effectively and deliver value incrementally.
- **User Stories:** Define user stories to capture user requirements and prioritize development efforts based on user needs and priorities. User stories should be clear, concise, and actionable, enabling the team to focus on delivering value to end-users with each iteration.
- **Sprint Planning:** Conduct regular sprint planning sessions to define the scope of work for each sprint based on prioritized user stories and feedback from stakeholders. Break down user stories into small tasks and estimate effort required to complete, ensuring that the team can deliver a potentially shippable product increment at the end of each sprint.
- **Continuous Integration and Testing:** Implement continuous integration and testing practices to ensure that changes are integrated into the system frequently and validated through automated testing. This helps identify and address issues early in the development process, minimizing the risk of defects and ensuring the stability and reliability of the system.
- **Iterative Feedback and Review:** Solicit feedback from stakeholders and end-users regularly throughout the development process. Conduct sprint reviews to demonstrate progress and gather feedback on the implemented features, enabling the team to make necessary adjustments and refinements based on user input.
- **Adaptation and Continuous Improvement:** Embrace change-adapt the development approach based on feedback, requirements, and evolving priorities. Continuously reflect on team performance and processes through sprint retrospectives, identifying areas for improvement and implementing changes enhancing productivity and effectiveness.

By adopting Agile methodologies, teams can effectively manage the development of the network security and proctoring system, delivering value to end-users through iterative development, collaboration, and responsiveness to change.

Flowchart & Use Case Diagrams

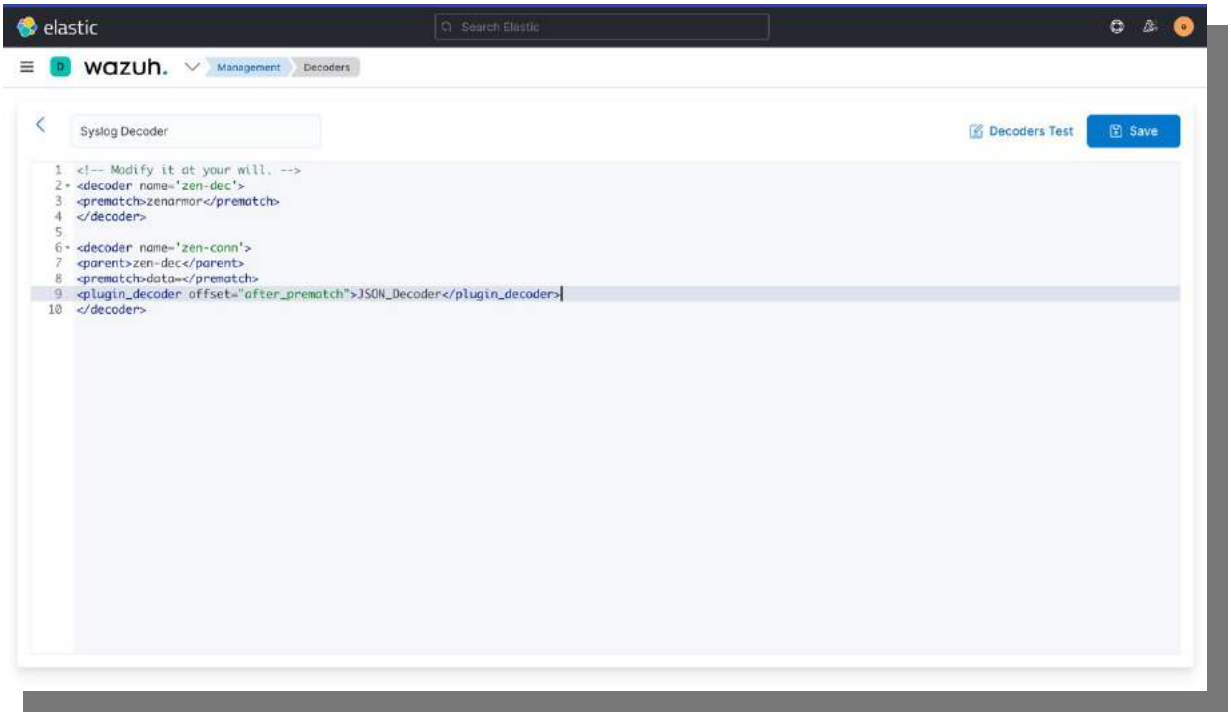


Use Case Diagram:

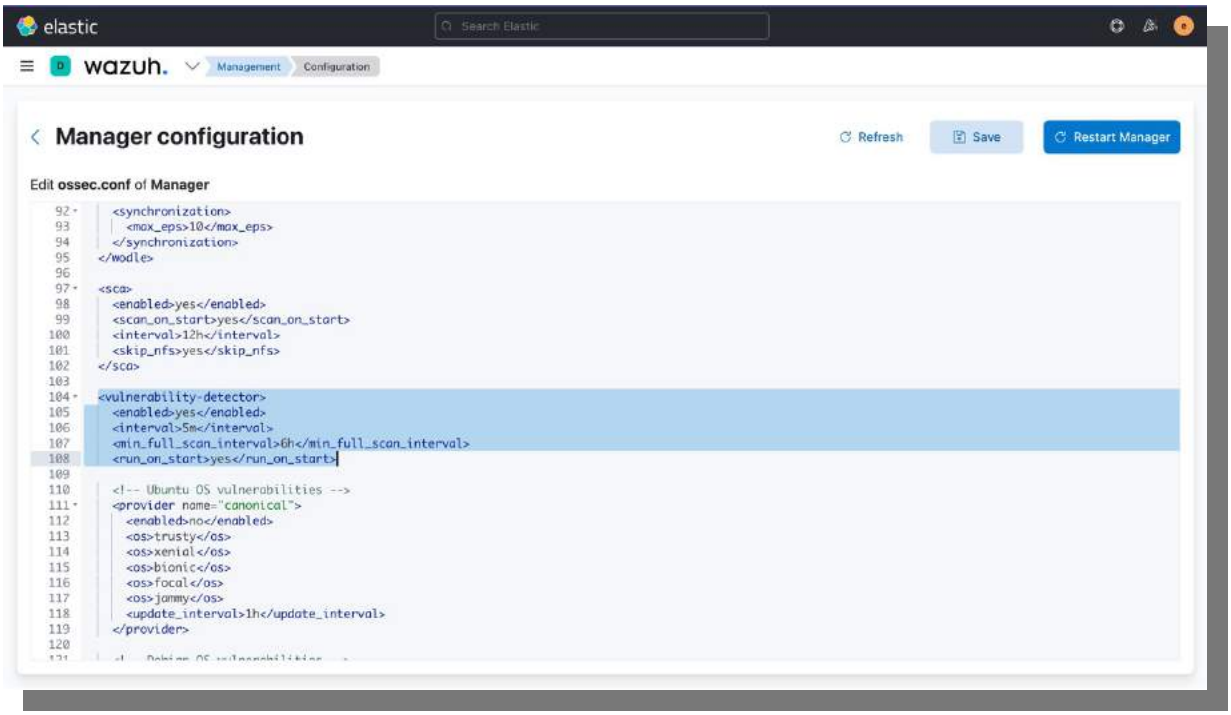


Code Snippets

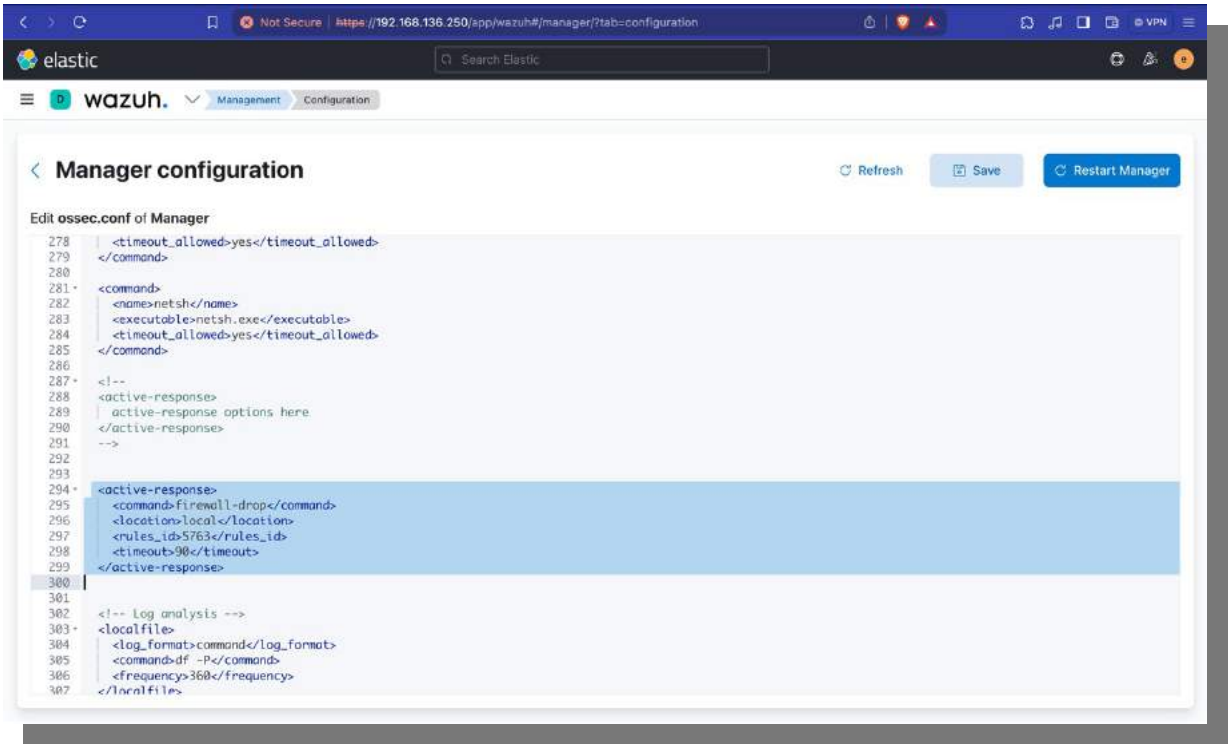
- **Code for Decoder (Decoding Syslog JSON)**



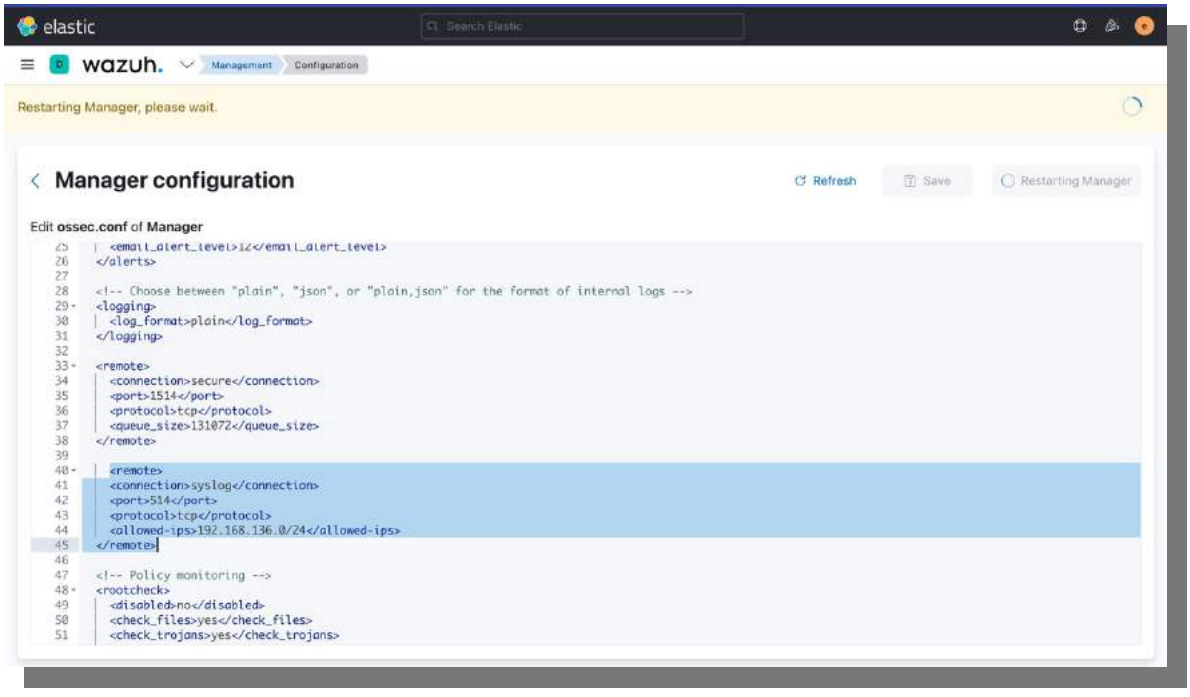
- **Code for Enabling Vulnerability Detector**



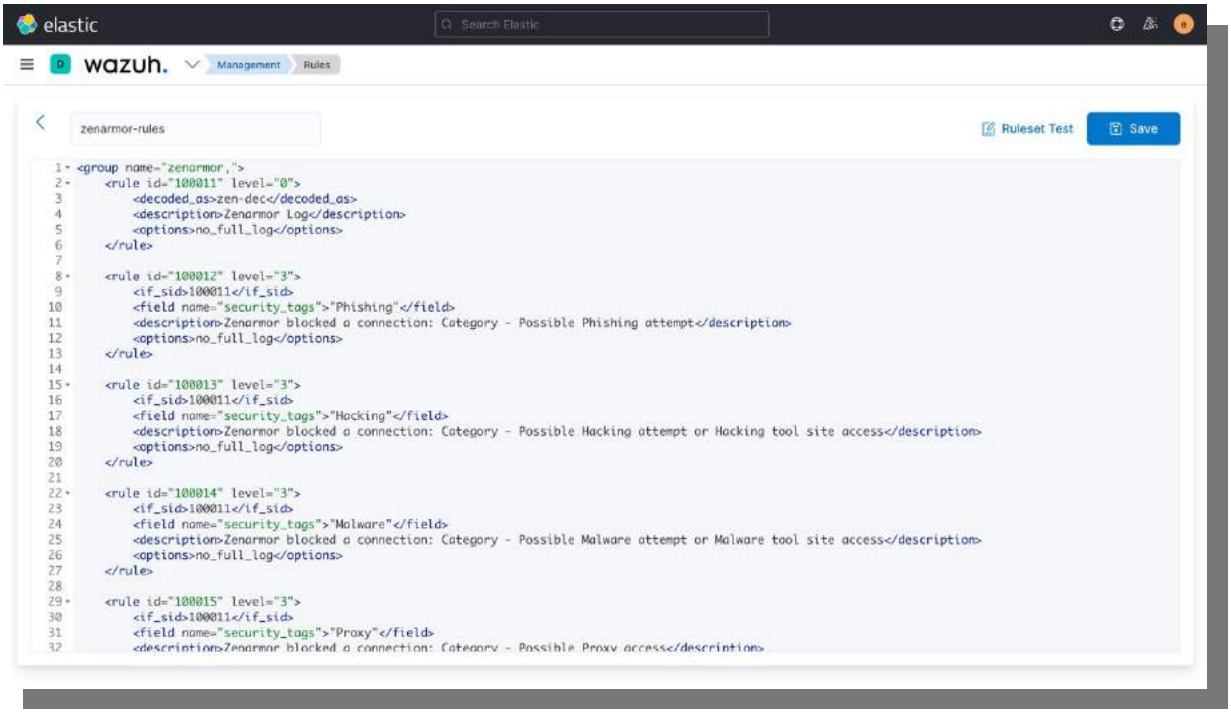
- **Code for Active Response**



- **Code for Activating Syslog**



- **Code for Custom Ruleset**



- **Code for Private Offline AI**

```
curl -fsSL https://ollama.com/install.sh | sh
```

```
neevjain@Neevs-MacBook-Air ~ % ollama run llama2-uncensored
pulling manifest
pulling 6aa74acf170f...   0% |              | 9.4 MB/3.8 GB  2.2 MB/s  28m50s
```

References –

- Wazuh Documentation -https://documentation.wazuh.com/current/user-manual/ruleset/custom.html
- Ollama - https://github.com/ollama/ollama

Testing Reports

Introduction:

The testing phase of the Secure Cybersecurity Home Lab aimed to validate the reliability, functionality, and security of its components. This report details the testing procedures, methodologies, and outcomes to ensure the system's readiness for deployment in educational environments.

Scope of Testing:

The testing scope encompassed an evaluation of system functionality, integration, security, and performance. This included assessing components such as pfSense Firewall, Snort IDS/IPS, Zenarmor NGFW, Wazuh SIEM, and Offline AI, as well as their interaction within the overall system architecture.

Testing Procedures:

Functionality Testing:

Each system component underwent rigorous functionality testing. pfSense Firewall was tested by configuring firewall rules, verifying network connectivity, and conducting ping tests to ensure proper routing. Additionally, network adapters were added, IPs and gateways were changed, and connectivity was verified to assess flexibility and robustness. Snort IDS/IPS functionality was evaluated by simulating network attacks and monitoring Snort alerts to validate threat detection capabilities. Similarly, Zenarmor NGFW underwent testing for policy configuration, network traffic monitoring, and application control features. Wazuh SIEM functionality was verified by deploying agents on systems, monitoring logs, and generating alerts based on predefined rules. The Offline AI's functionality was validated by inputting sample data and assessing response accuracy.

Integration Testing:

Integration tests were conducted to ensure seamless communication and data exchange between system components. Syslog data was transmitted from Zenarmor NGFW to Wazuh SIEM, and log ingestion and analysis were verified. Integration between pfSense Firewall and Snort IDS/IPS was tested to ensure effective threat detection and prevention mechanisms.

Security Testing:

Security tests were performed to identify vulnerabilities and strengthen security measures. Penetration testing was conducted to assess the system's resilience against potential entry points and attacks. Vulnerability scanning tools were utilized to identify security loopholes and weaknesses in system configurations. Additionally, network stress tests were performed to evaluate system performance under heavy loads and assess responsiveness.

Performance Testing:

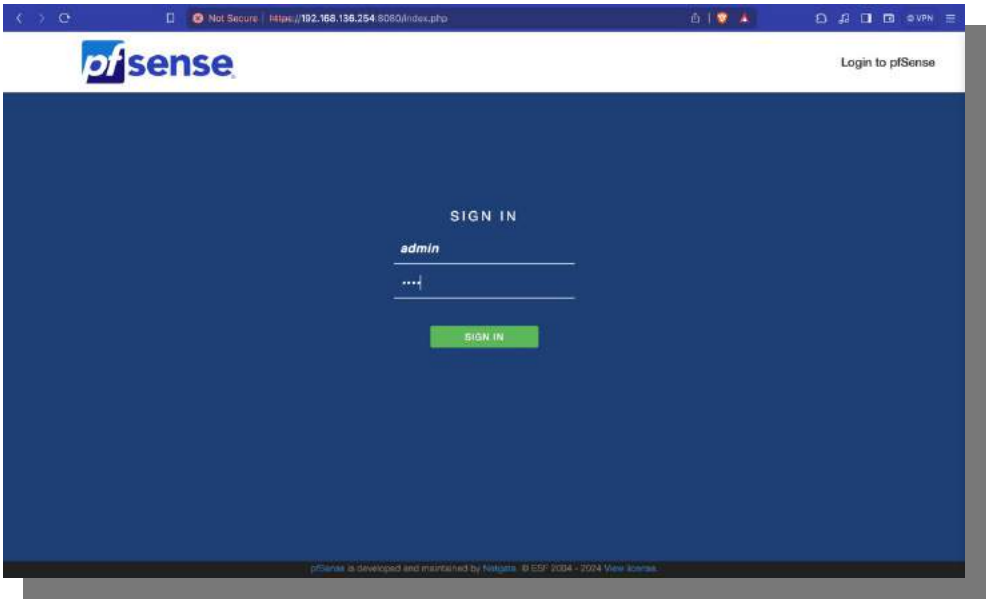
Performance tests were conducted to evaluate system responsiveness and scalability. Network stress tests were executed to assess system performance under varying loads, while monitoring tools were used to measure resource utilization and identify potential bottlenecks.

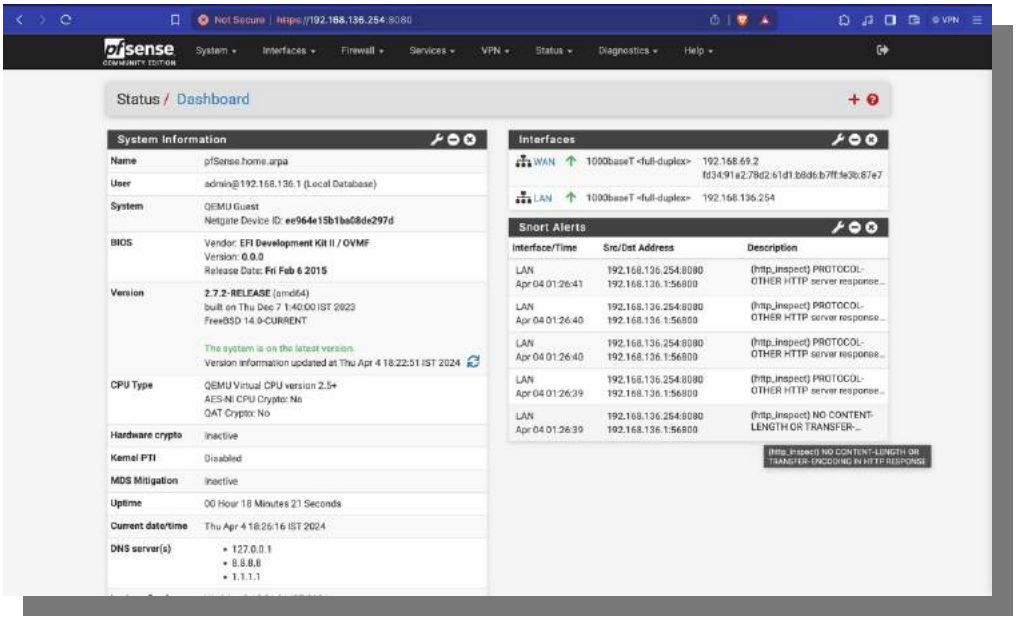
Overall Test Results:

The testing phase confirmed the reliability, functionality, and security of the College Exam Proctoring System. All system components demonstrated satisfactory performance, with minor vulnerabilities promptly addressed. Integration tests validated seamless communication between components, while security tests identified and mitigated potential risks. Performance tests indicated satisfactory system responsiveness and scalability under varying loads.

Screenshots

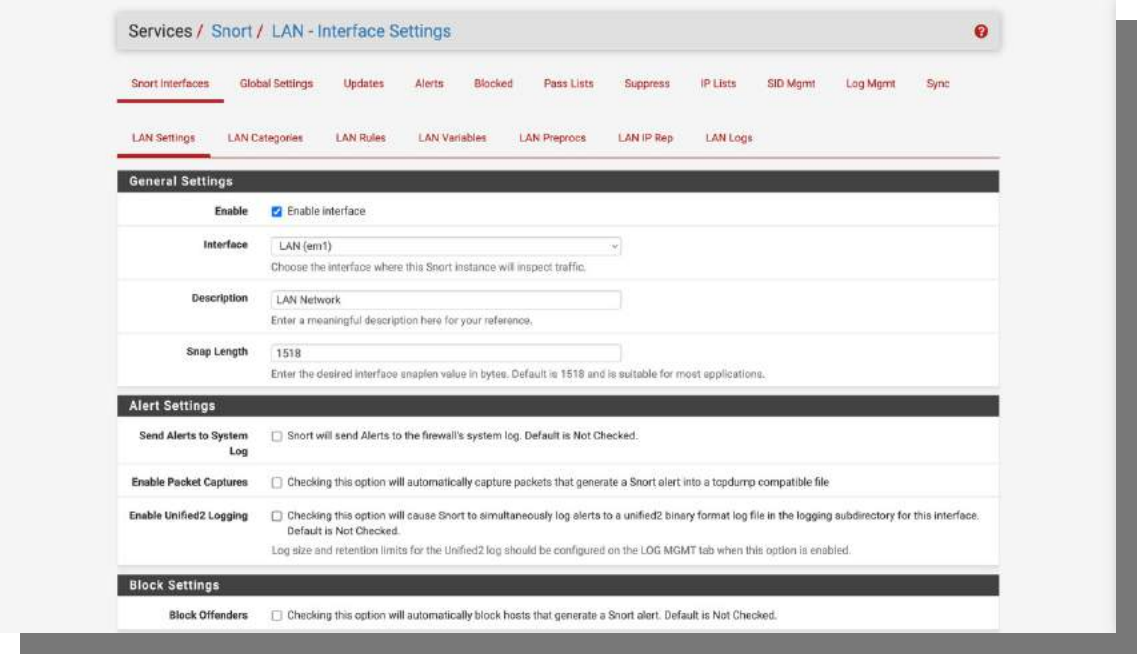
- **pfSense**

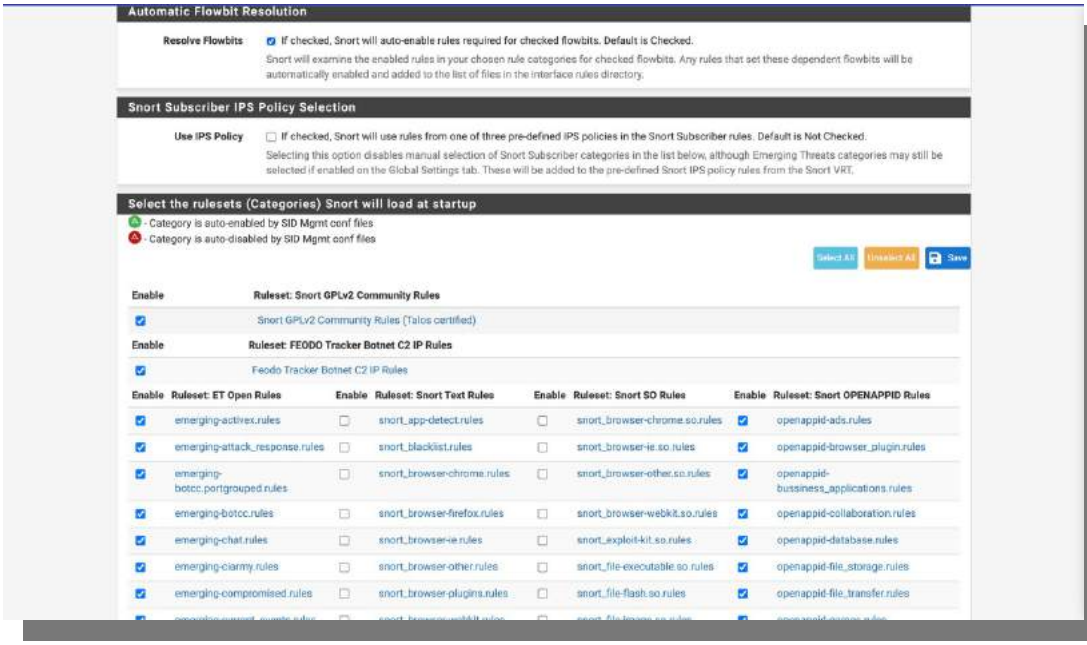


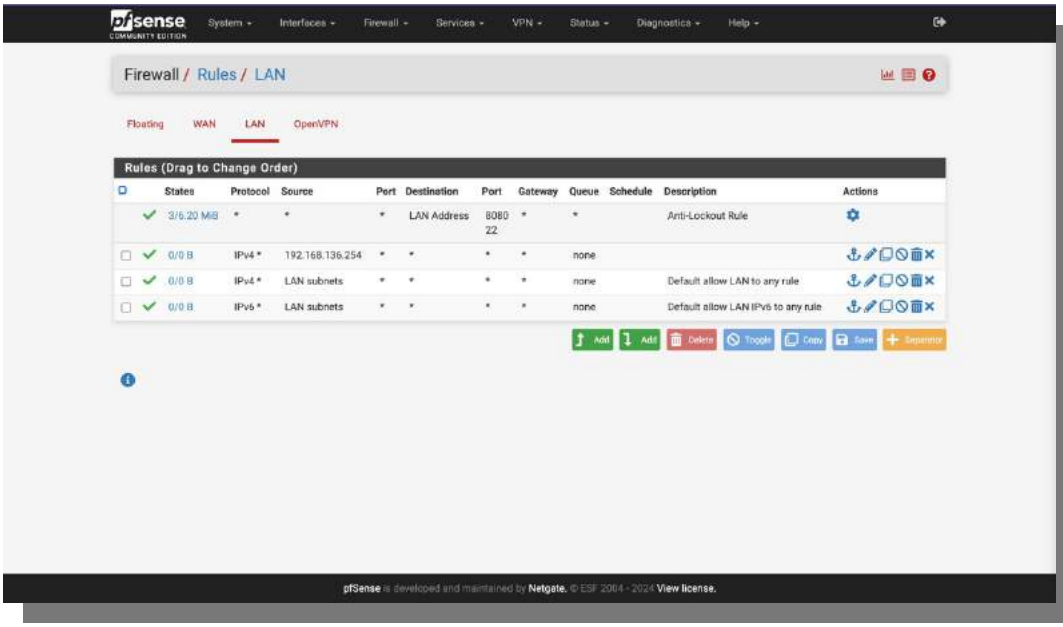


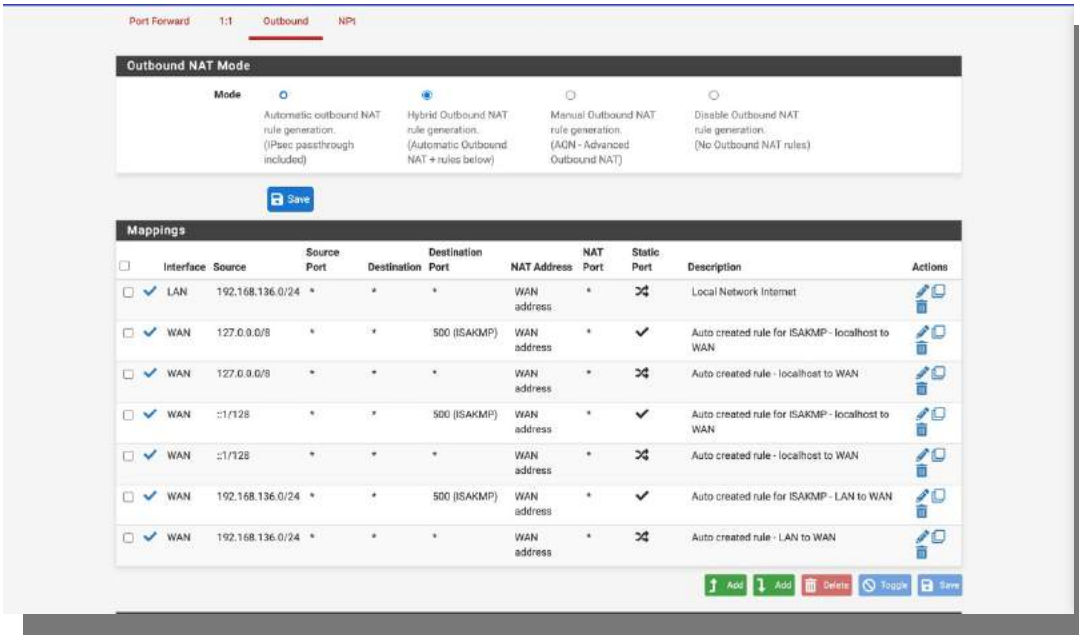
Snort Alerts

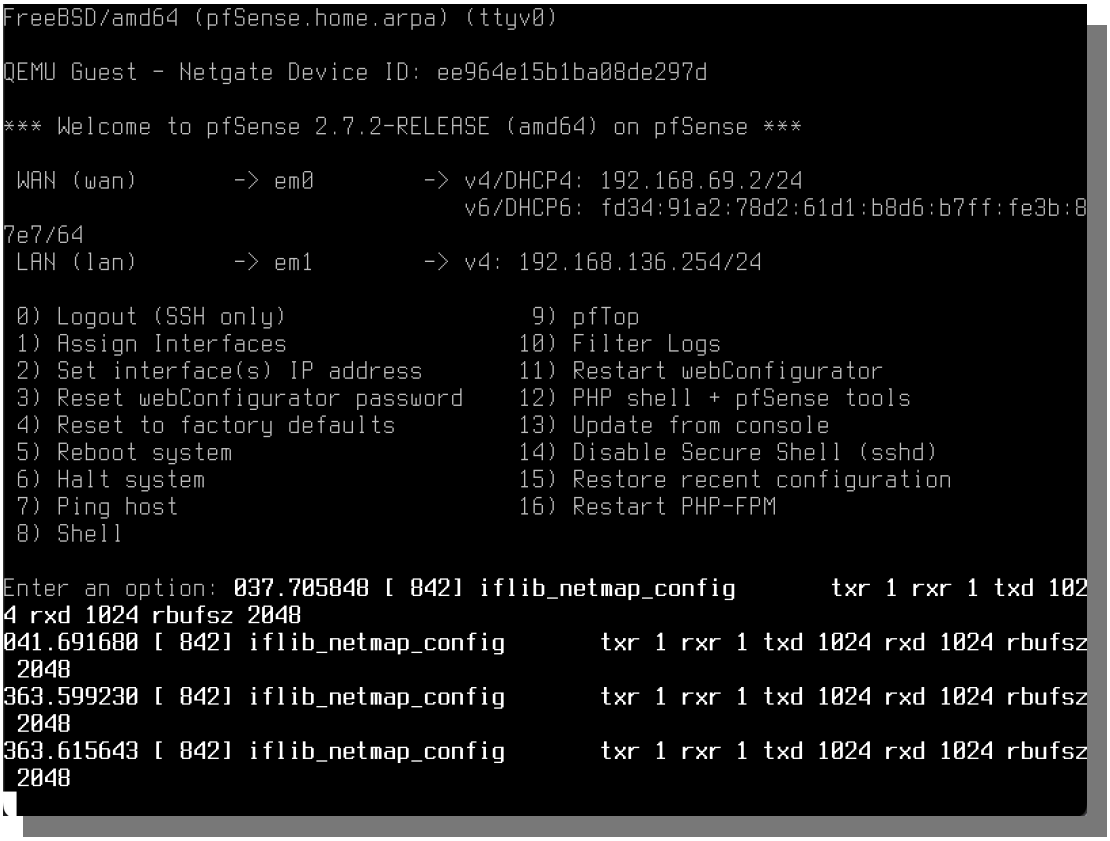
Interface/Time	Src/Dst Address	Description
LAN Apr 04 01:26:41	192.168.136.254:8080 192.168.136.1:56800	(http_inspect) PROTOCOL-OTHER HTTP server response...
LAN Apr 04 01:26:40	192.168.136.254:8080 192.168.136.1:56800	(http_inspect) PROTOCOL-OTHER HTTP server response...
LAN Apr 04 01:26:40	192.168.136.254:8080 192.168.136.1:56800	(http_inspect) PROTOCOL-OTHER HTTP server response...
LAN Apr 04 01:26:39	192.168.136.254:8080 192.168.136.1:56800	(http_inspect) PROTOCOL-OTHER HTTP server response...
LAN Apr 04 01:26:39	192.168.136.254:8080 192.168.136.1:56800	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-...



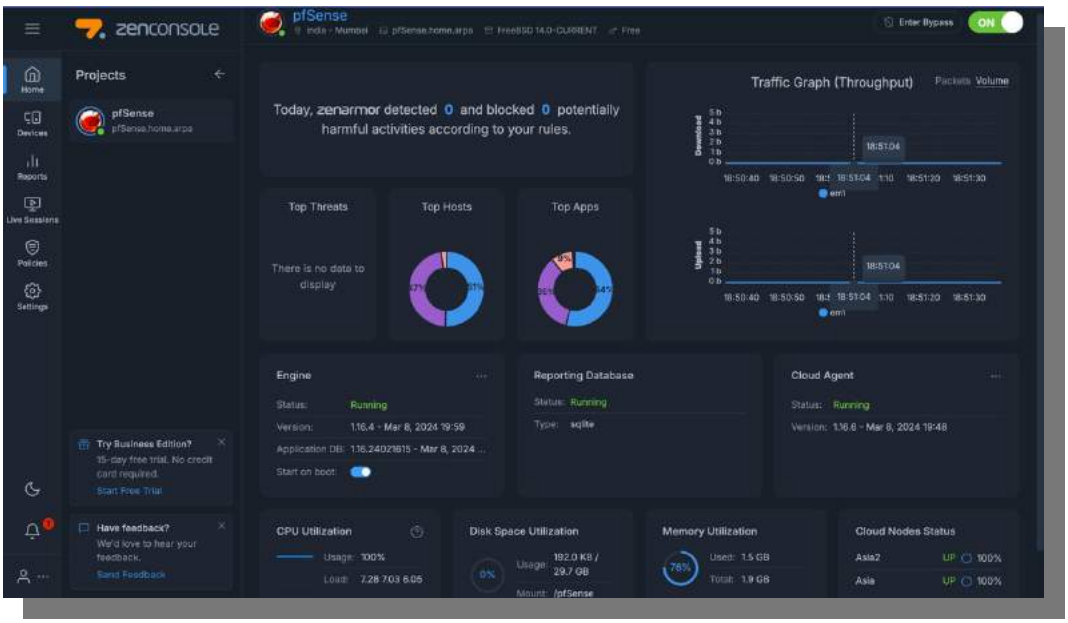

Automatic Flowbit Resolution
Resolve Flowbits
If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.
Snort Subscriber IPS Policy Selection
Use IPS Policy
If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.
Select the rulesets (Categories) Snort will load at startup
- Category is auto-enabled by SID Mgmt conf files
- Category is auto-disabled by SID Mgmt conf files
Select All
Unselect All
Save
Enable
Ruleset: Snort GPLv2 Community Rules
Snort GPLv2 Community Rules (Talos certified)
Enable
Ruleset: FEODO Tracker Botnet C2 IP Rules
Feodo Tracker Botnet C2 IP Rules
Enable
Ruleset: ET Open Rules
Enable
Ruleset: Snort Text Rules
Enable
Ruleset: Snort SO Rules
Enable
Ruleset: Snort OPENAPPID Rules
emerging-activex.rules
snort_app-detect.rules
snort_browser-chrome.so.rules
openappid-ads.rules
emerging-attack_response.rules
snort_blacklist.rules
snort_browser-ie.so.rules
openappid-browser_plugin.rules
emerging-botcc.portgrouped.rules
snort_browser-chrome.rules
snort_browser-other.so.rules
openappid-bussiness_applications.rules
emerging-botcc.rules
snort_browser-firefox.rules
snort_browser-webkit.so.rules
openappid-collaboration.rules
emerging-chat.rules
snort_browser-ie.rules
snort_exploit-kit.so.rules
openappid-database.rules
emerging-ciarmy.rules
snort_browser-other.rules
snort_file-executable.so.rules
openappid-file_storage.rules
emerging-compromised.rules
snort_browser-plugins.rules
snort_file-flash.so.rules
openappid-file_transfer.rules

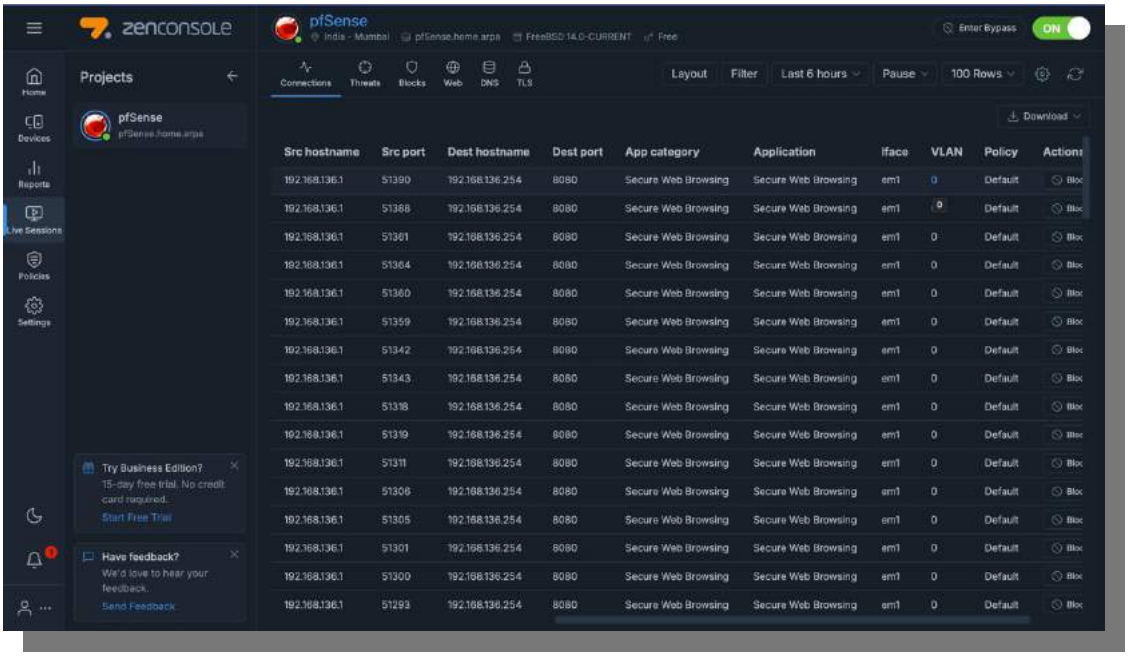

pfsense
COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Firewall / Rules / LAN
Floating
WAN
LAN
OpenVPN
Rules (Drag to Change Order)
States
Protocol
Source
Port
Destination
Port
Gateway
Queue
Schedule
Description
Actions
3/6.20 MiB
*
*
*
LAN Address
8080
22
*
*
Anti-Lockout Rule
0/0 B
IPv4 *
192.168.136.254
*
*
*
*
none
0/0 B
IPv4 *
LAN subnets
*
*
*
*
none
Default allow LAN to any rule
0/0 B
IPv6 *
LAN subnets
*
*
*
*
none
Default allow LAN IPv6 to any rule
Add
Add
Delete
Toggle
Copy
Save
Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2024 View license.


Port Forward
1:1
Outbound
NPt
Outbound NAT Mode
Mode
Automatic outbound NAT rule generation. (IPsec passthrough included)
Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
Disable Outbound NAT rule generation. (No Outbound NAT rules)
Save
Mappings
Interface
Source
Source Port
Destination
Destination Port
NAT Address
NAT Port
Static Port
Description
Actions
LAN 192.168.136.0/24 * * * WAN address * Local Network Internet
WAN 127.0.0.0/8 * * 500 (ISAKMP) WAN address * Auto created rule for ISAKMP - localhost to WAN
WAN 127.0.0.0/8 * * * WAN address * Auto created rule - localhost to WAN
WAN ::1/128 * * 500 (ISAKMP) WAN address * Auto created rule for ISAKMP - localhost to WAN
WAN ::1/128 * * * WAN address * Auto created rule - localhost to WAN
WAN 192.168.136.0/24 * * 500 (ISAKMP) WAN address * Auto created rule for ISAKMP - LAN to WAN
WAN 192.168.136.0/24 * * * WAN address * Auto created rule - LAN to WAN
Add
Add
Delete
Toggle
Save

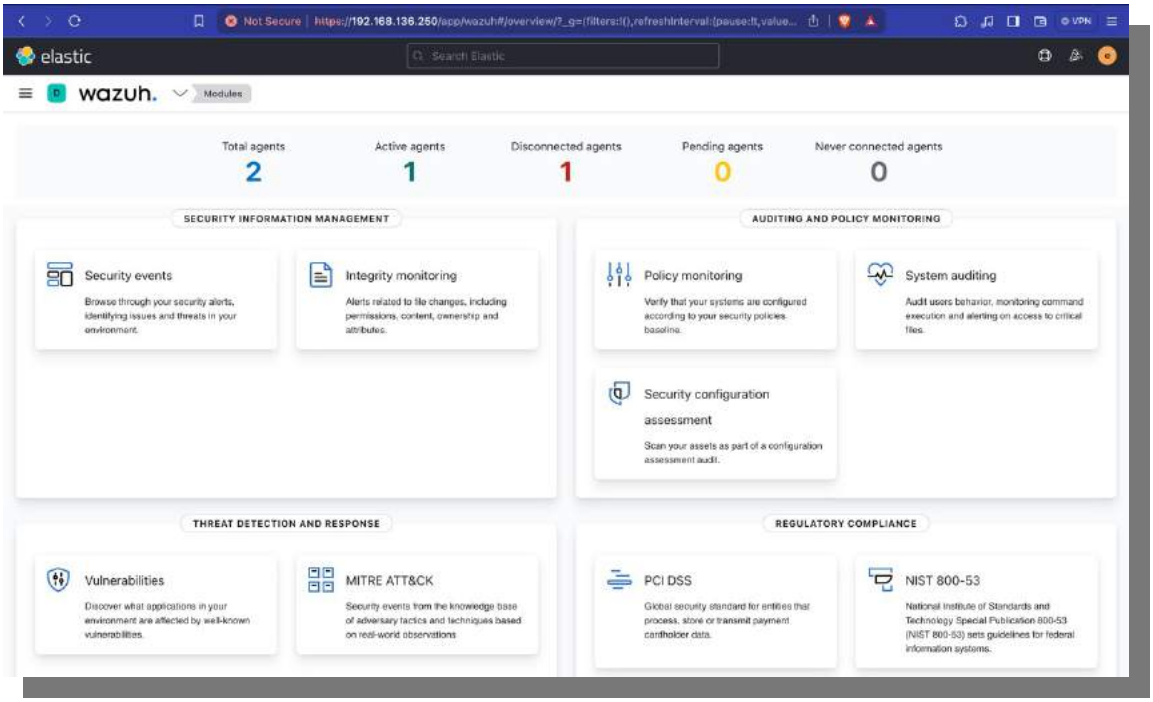

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
QEMU Guest - Netgate Device ID: ee964e15b1ba08de297d
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan) -> em0 -> v4/DHCP4: 192.168.69.2/24
v6/DHCP6: fd34:91a2:78d2:61d1:b8d6:b7ff:fe3b:87e7/64
LAN (lan) -> em1 -> v4: 192.168.136.254/24
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Disable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option: 037.705848 [842] iflib_netmap_config txr 1 rxr 1 txd 1024 rxd 1024 rbufsz 2048
041.691680 [842] iflib_netmap_config txr 1 rxr 1 txd 1024 rxd 1024 rbufsz 2048
363.599230 [842] iflib_netmap_config txr 1 rxr 1 txd 1024 rxd 1024 rbufsz 2048
363.615643 [842] iflib_netmap_config txr 1 rxr 1 txd 1024 rxd 1024 rbufsz 2048

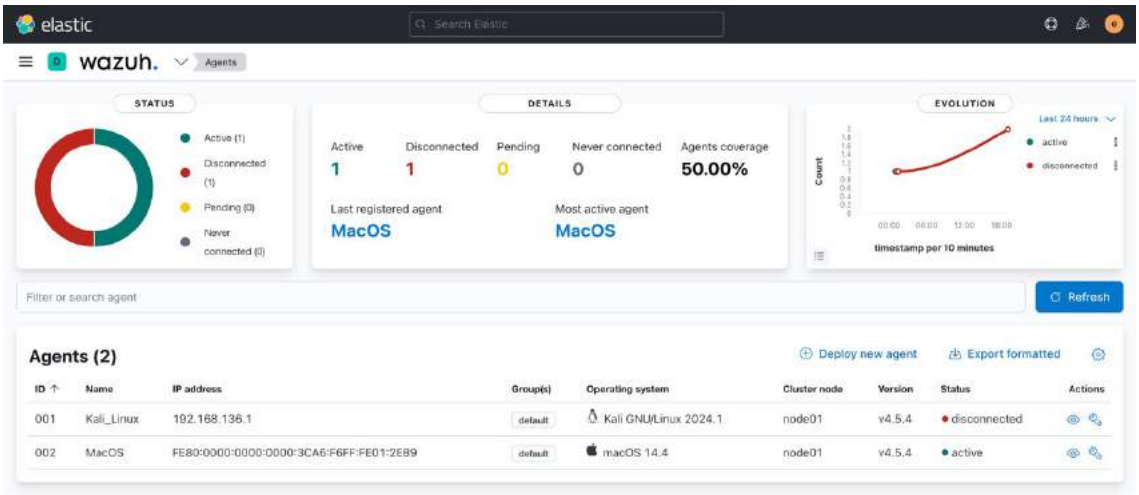
- **Zenarmor (NGFW)**

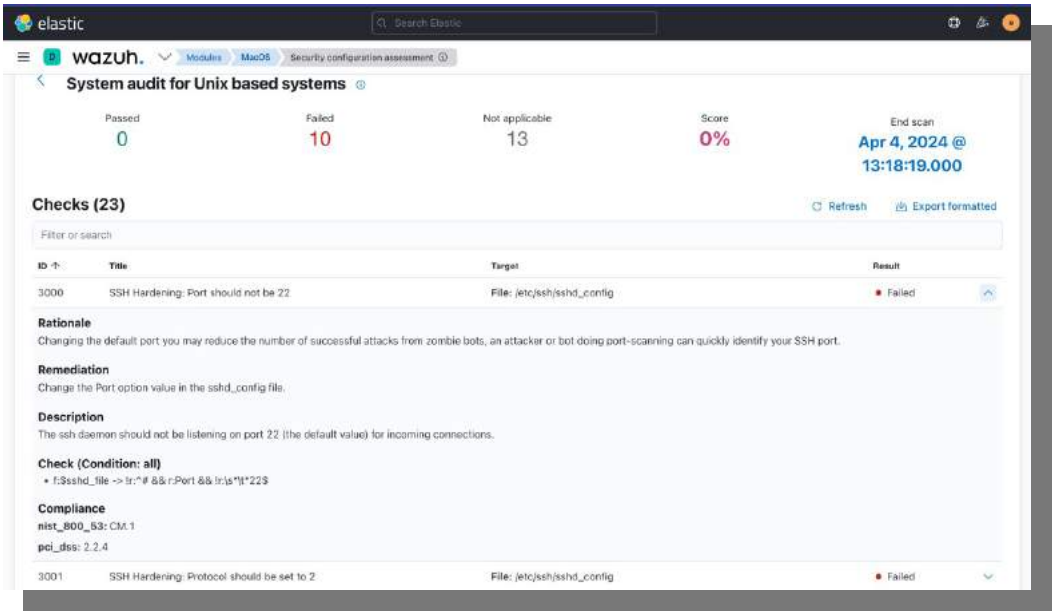


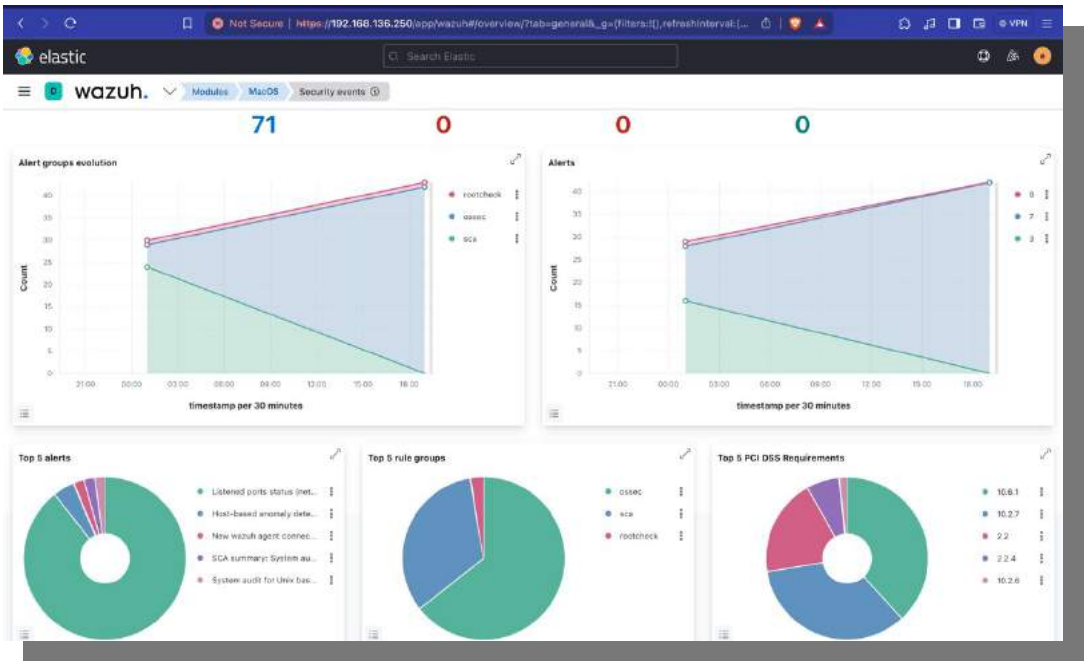


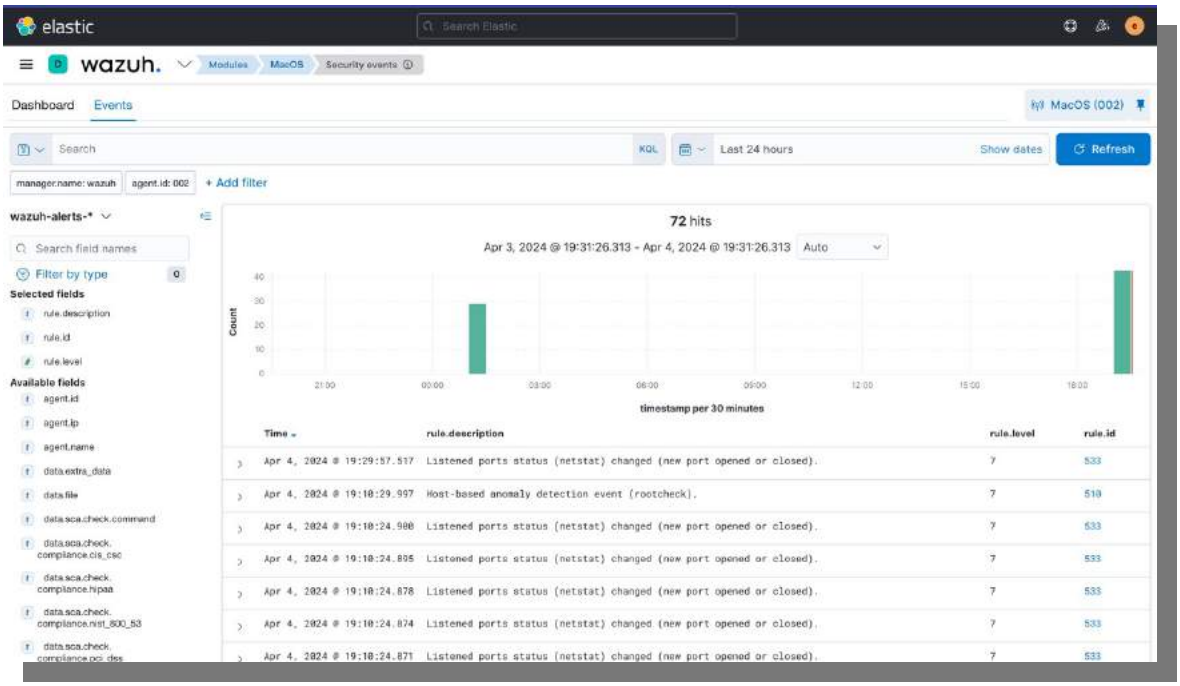
- **Wazuh**

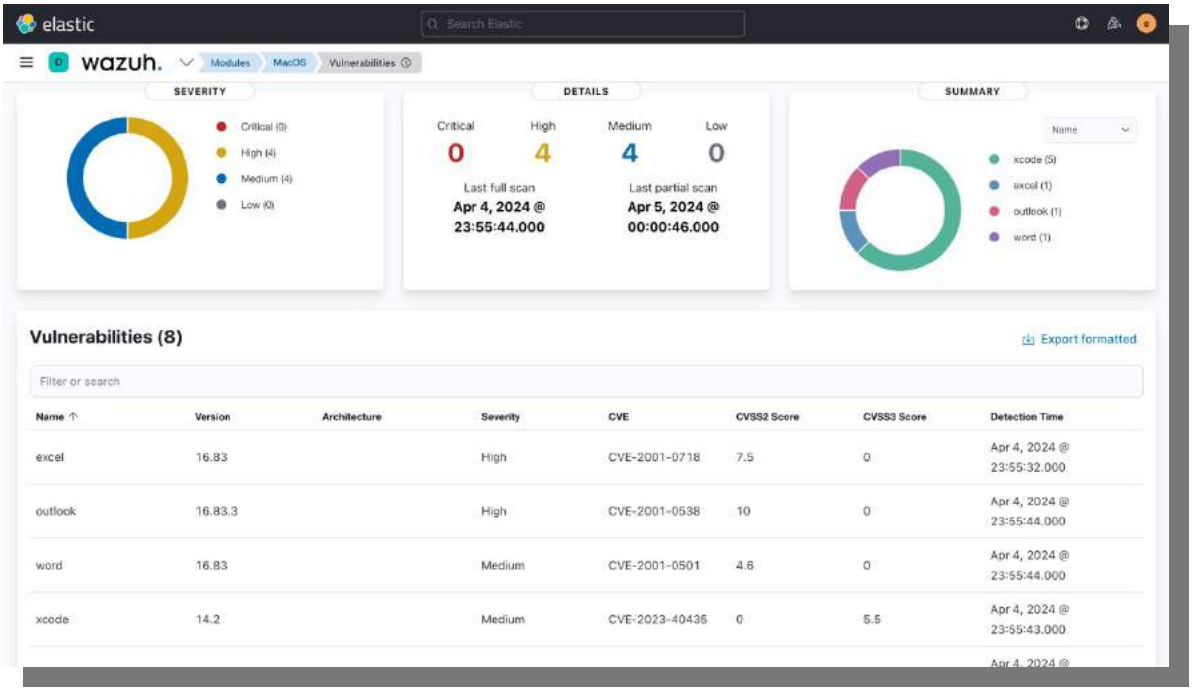

Not Secure
https://192.168.136.250/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value...
elastic
Search Elastic
wazuh.
Modules
Total agents
2
Active agents
1
Disconnected agents
1
Pending agents
0
Never connected agents
0
SECURITY INFORMATION MANAGEMENT
Security events
Browse through your security alerts, identifying issues and threats in your environment.
Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.
AUDITING AND POLICY MONITORING
Policy monitoring
Verify that your systems are configured according to your security policies baseline.
System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.
Security configuration assessment
Scan your assets as part of a configuration assessment audit.
THREAT DETECTION AND RESPONSE
Vulnerabilities
Discover what applications in your environment are affected by well-known vulnerabilities.
MITRE ATT&CK
Security events from the knowledge base of adversary tactics and techniques based on real-world observations
REGULATORY COMPLIANCE
PCI DSS
Global security standard for entities that process, store or transmit payment cardholder data.
NIST 800-53
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.


elastic
Search Elastic
wazuh.
Agents
STATUS
Active (1)
Disconnected (1)
Pending (0)
Never connected (0)
DETAILS
Active
1
Disconnected
1
Pending
0
Never connected
0
Agents coverage
50.00%
Last registered agent
MacOS
Most active agent
MacOS
EVOLUTION
Last 24 hours
active
disconnected
Count
timestamp per 10 minutes
Filter or search agent
Refresh
Agents (2)
Deploy new agent
Export formatted
ID
Name
IP address
Group(s)
Operating system
Cluster node
Version
Status
Actions
001
Kali_Linux
192.168.136.1
default
Kali GNU/Linux 2024.1
node01
v4.5.4
disconnected
002
MacOS
FE80:0000:0000:0000:3CA6:F6FF:FE01:2E89
default
macOS 14.4
node01
v4.5.4
active

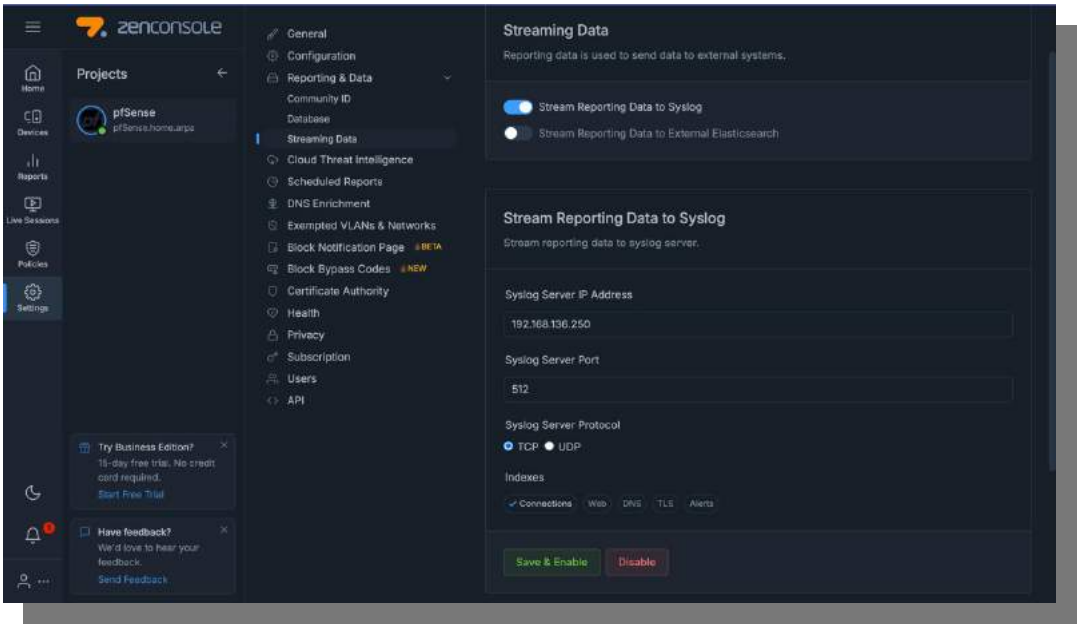

elastic
wazuh.
Modules
MacOS
Security configuration assessment
System audit for Unix based systems
Passed
0
Failed
10
Not applicable
13
Score
0%
End scan
Apr 4, 2024 @
13:18:19.000
Checks (23)
Refresh
Export formatted
Filter or search
ID
Title
Target
Result
3000
SSH Hardening: Port should not be 22
File: /etc/ssh/sshd_config
Failed
Rationale
Changing the default port you may reduce the number of successful attacks from zombie bots, an attacker or bot doing port-scanning can quickly identify your SSH 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
3001
SSH Hardening: Protocol should be set to 2
File: /etc/ssh/sshd_config
Failed

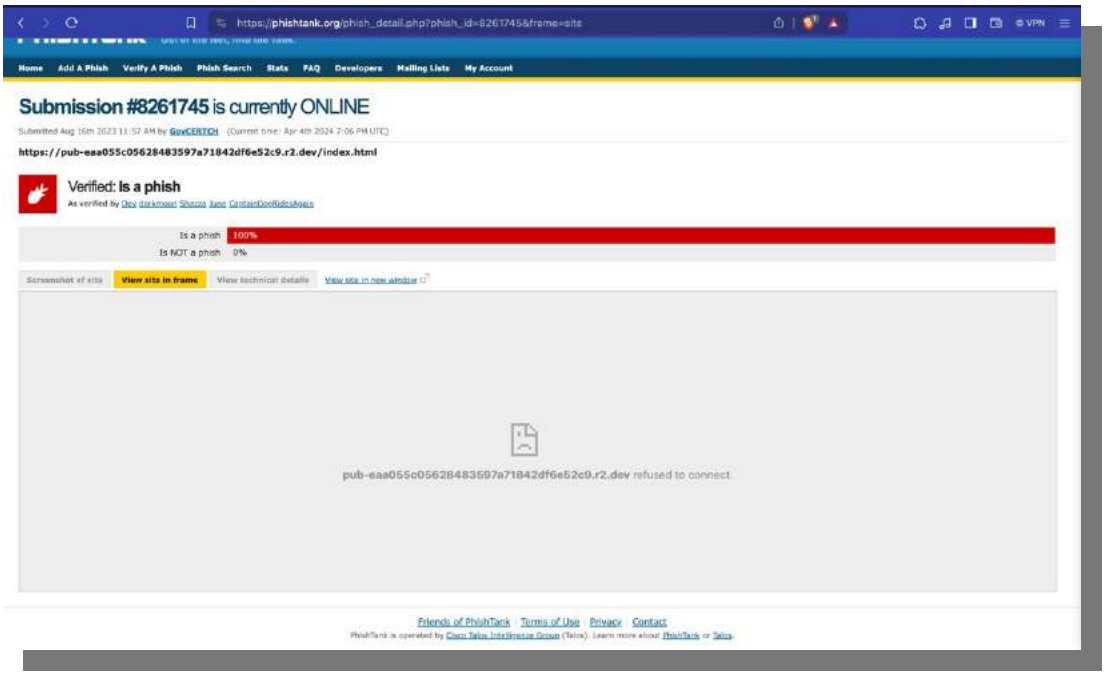

Not Secure
elastic
wazuh.
Modules
MacOS
Security events
71
0
0
0
Alert groups evolution
Alerts
Count
timestamp per 30 minutes
Top 5 alerts
Top 5 rule groups
Top 5 PCI DSS Requirements


elastic
Search Elastic
wazuh.
Modules
MacOS
Security events
Dashboard
Events
MacOS (002)
Search
KQL
Last 24 hours
Show dates
Refresh
manager.name: wazuh
agent.id: 002
+ Add filter
wazuh-alerts-*
Search field names
Filter by type
0
Selected fields
rule.description
rule.id
rule.level
Available fields
agent.id
agent.ip
agent.name
data.extra_data
data.file
data.sca.check.command
data.sca.check.compliance.cis_csc
data.sca.check.compliance.hipaa
data.sca.check.compliance.nist_800_53
data.sca.check.compliance.pci_dss
72 hits
Apr 3, 2024 @ 19:31:26.313 - Apr 4, 2024 @ 19:31:26.313
Auto
Count
timestamp per 30 minutes
Time
rule.description
rule.level
rule.id
Apr 4, 2024 @ 19:29:57.517 Listened ports status (netstat) changed (new port opened or closed). 7 533
Apr 4, 2024 @ 19:10:29.997 Host-based anomaly detection event (rootcheck). 7 510
Apr 4, 2024 @ 19:10:24.900 Listened ports status (netstat) changed (new port opened or closed). 7 533
Apr 4, 2024 @ 19:10:24.895 Listened ports status (netstat) changed (new port opened or closed). 7 533
Apr 4, 2024 @ 19:10:24.878 Listened ports status (netstat) changed (new port opened or closed). 7 533
Apr 4, 2024 @ 19:10:24.874 Listened ports status (netstat) changed (new port opened or closed). 7 533
Apr 4, 2024 @ 19:10:24.871 Listened ports status (netstat) changed (new port opened or closed). 7 533



- **Integrating Wazuh SIEM and Zenarmor (NGFW) with Syslog**





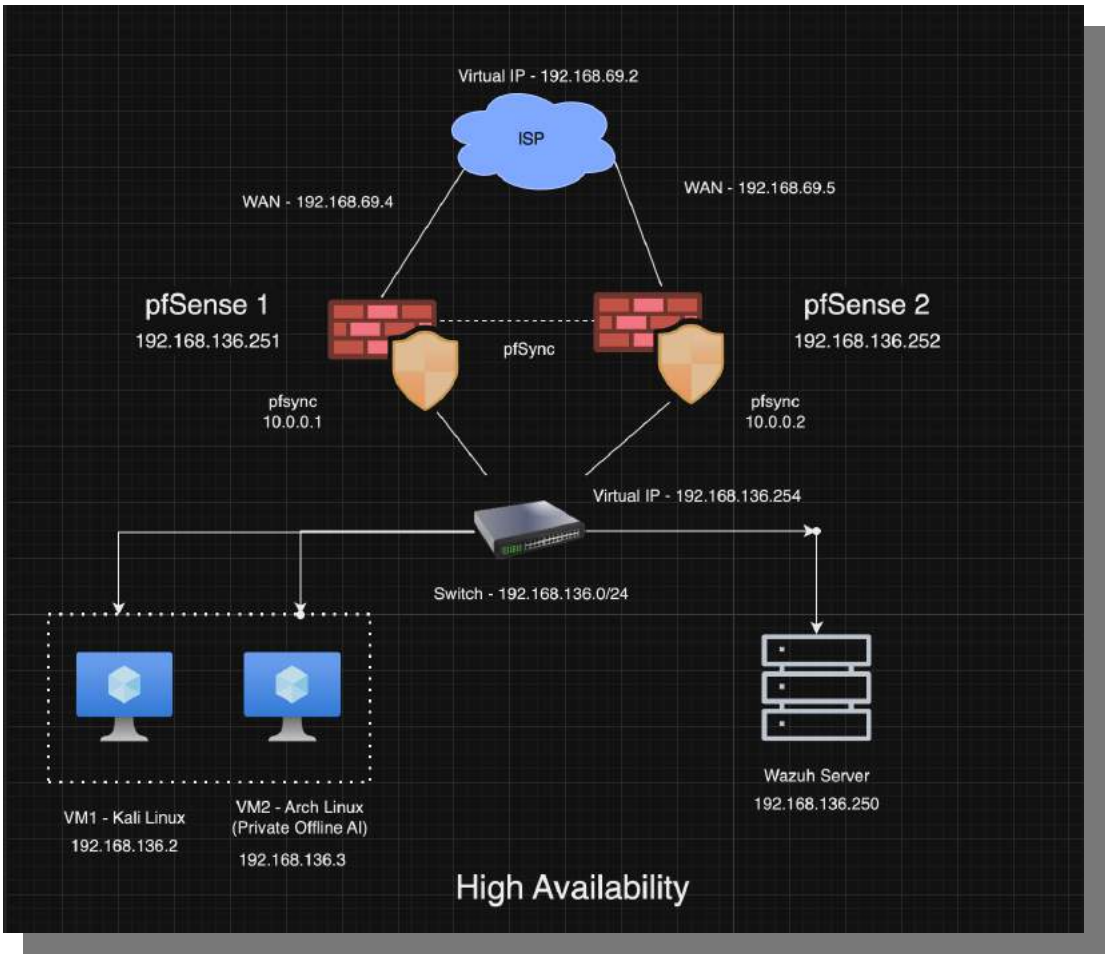
(Blocking the Phishing Website)

- **Private Offline AI**

```
>>> hello
Hi there!

>>> what is network security?
Network Security refers to the practices and technologies that are used to
protect networks, devices, data, and users from unauthorized access,
modification or destruction.
```

```
>>> do you know st. xavier's college, mumbai? describe the college
Yes, I do know St Xavier's College, Mumbai. It is a private autonomous
Catholic college located in Mumbai, India. The college was established in
1869 and offers undergraduate, postgraduate, and doctoral programs in
various fields such as arts, science, commerce, law, and education.

>>> how is the course b.sc. it in that college
The Bachelor of Science (B.Sc.) Information Technology program offered by
St Xavier's College Mumbai covers a wide range of topics such as operating
systems, networking, computer architecture, programming languages,
database management systems, software engineering, and artificial
intelligence. The program is designed to provide students with the
necessary skills and knowledge to pursue careers in IT fields such as
software development, system administration, network engineering,
cybersecurity, etc.

>>> Send a message (/? for help)
```

Future Enhancements



1. High Availability with Proxmox VM:

Integrating Proxmox Virtual Environment (PVE) as a bare-metal hypervisor type-1 can significantly enhance the system's performance and availability. By deploying the College Exam Proctoring System on Proxmox, we can leverage its robust virtualization features, including live migration, high availability clustering, and centralized management. This ensures seamless failover and minimal downtime, thereby enhancing the reliability and resilience of the system.

2. Scalability and Performance Improvements:

To cater to larger organizations, the system can be further enhanced for scalability and performance. This includes optimizing resource utilization, implementing load balancing mechanisms, and scaling out system components horizontally to accommodate a larger user base and higher network traffic.

3. Advanced Threat Detection and Incident Response:

For improved security, advanced threat detection mechanisms such as machine learning-based anomaly detection and behavior analysis can be integrated. Additionally, automated incident response capabilities can be developed using orchestration tools like Ansible or Puppet. This allows the system to automatically respond to security incidents based on predefined rules and policies, thereby reducing response time and minimizing potential impact.

4. Centralized Logging and Monitoring:

Implementing a centralized logging and monitoring solution, such as ELK Stack (Elasticsearch, Logstash, Kibana), can provide real-time visibility into system activities and security events. This enables proactive threat detection, forensic analysis, and compliance auditing across the entire infrastructure.

5. Multi-factor Authentication (MFA):

Enhancing user authentication with multi-factor authentication (MFA) adds an extra layer of security to the system. Integrating MFA solutions such as Google Authenticator or RSA SecurID ensures that only authorized users can access the system, mitigating the risk of unauthorized access and credential theft.

6. Redundant Network Infrastructure:

Implementing redundant network infrastructure with technologies like Virtual Router Redundancy Protocol (VRRP) or High Availability (HA) pairs ensures network resilience and uninterrupted connectivity. Redundant switches, routers, and network links can be deployed to eliminate single points of failure and maintain continuous network availability.

7. Disaster Recovery Planning:

Developing a comprehensive disaster recovery plan is essential for mitigating the impact of unforeseen events such as hardware failures, natural disasters, or cyber attacks. This involves regular backups, off-site storage, and predefined procedures for restoring operations in the event of a disruption.

Bibliography

- **pfSense Documentation** – https://docs.netgate.com/pfsense/en/latest/
- **Wazuh Documentation** - https://documentation.wazuh.com/current/getting-started/index.html
- **Sunny Valley Zenarmor** - https://sunnyvalley.io/
- **Introduction to pfSense** – https://youtu.be/lUzSsX4T4WQ?si=zOa0wxzhYnkdfPhO
- **Introduction to Wazuh** - https://youtu.be/Hq58_yGJwHk?si=dhaVz_1tGOajDVZ7
- **Private Offline AI** - https://docs.privategpt.dev/manual/general-configuration/configuration
- **Networking –** Head First Networking Book & Cisco Packet tracer
- **Private GPT** - https://youtu.be/WxYC9-hBM_g?si=uNQS7pSJvZiAXHkL

Glossary

- **pfSense Firewall:** An open-source firewall and router platform based on FreeBSD that provides advanced security features such as firewall rules, VPN support, and traffic shaping.
- **Snort IDS/IPS:** An open-source network intrusion detection and prevention system (IDS/IPS) that analyses network traffic and detects/signatures for suspicious activity or known threats.
- **Zenarmor NGFW:** Next-Generation Firewall (NGFW) solution providing features such as application control, intrusion prevention, and deep packet inspection to protect networks from cyber threats.
- **Wazuh SIEM:** An open-source Security Information and Event Management (SIEM) that collects, analyses, and correlates security events from various sources to detect and respond to security incidents.
- **Offline AI:** An artificial intelligence (AI) system deployed locally that performs specific tasks or analysis without requiring an internet connection, used for tasks such as exam proctoring or offline data analysis.
- **Kali Linux:** A Linux distribution designed for digital forensics and penetration testing, equipped with a wide range of tools for security testing and ethical hacking.
- **Virtual Machine (VM):** A software emulation of a physical computer that runs an operating system and applications in an isolated environment, allowing multiple virtual machines to run on a single physical host.
- **Bare Metal Hypervisor:** A type-1 hypervisor that runs directly on the physical hardware of a server, allowing for efficient virtualization and resource allocation without the need for a separate operating system.

- **Centralized Logging:** The process of collecting and storing log data from various sources (e.g., servers, network devices, applications) in a centralized location for analysis, troubleshooting, and compliance purposes.
- **Incident Response:** The process of identifying, assessing, and responding to security incidents, including steps such as detection, containment, eradication, recovery, and lessons learned.
- **Anomaly Detection:** A method of detecting deviations from normal behaviour or patterns within a system or network, often used for identifying potential security threats or malicious activities.
- **Machine Learning:** A subset of artificial intelligence (AI) that enables systems to learn from data and make predictions or decisions without explicit programming, often used for tasks such as anomaly detection and threat analysis.
- **Orchestration:** The automation and coordination of multiple tasks or processes to achieve a desired outcome, often used in incident response and security operations to streamline workflows and response efforts.
- **Compliance Management:** The process of ensuring that an organization adheres to relevant laws, regulations, and industry standards related to data security, privacy, and governance.
- **Threat Intelligence:** Information about potential or current cyber threats, including indicators of compromise (IOCs), attack patterns, and adversary tactics, techniques, and procedures (TTPs), used for proactive defense and threat analysis.
- **Rules:** In the context of network security, rules refer to predefined criteria or configurations used to govern the behavior of a firewall, intrusion detection system (IDS), or other security devices. These rules define which network traffic is allowed or blocked based on criteria such as source/destination IP addresses, ports, and protocols.

- **NAT (Network Address Translation):** A networking process that modifies network address information in packet headers while in transit, typically used to map private IP addresses to public IP addresses to facilitate communication between devices on different networks.
- **Custom Rules:** Rules created by users or administrators to tailor the behavior of security devices or systems according to specific requirements or policies. Custom rules can be defined to enforce additional security measures, allow or block specific traffic patterns, or trigger customized actions based on predefined conditions.
- **Syslog (System Logging Protocol):** A standard protocol used for forwarding log messages and event data from network devices, servers, and applications to a centralized logging server or collector for storage, analysis, and monitoring.
- **Decoder:** In the context of security information and event management (SIEM) systems, a decoder is a component responsible for parsing and interpreting incoming log data or event streams from various sources, transforming them into standardized formats for analysis and correlation.
- **High Availability (HA):** A design approach or architecture that aims to minimize downtime and ensure continuous availability of critical systems or services by deploying redundant components, failover mechanisms, and automated recovery processes.
- **Proxmox:** A virtualization platform that provides hypervisor-level virtualization capabilities, allowing users to create and manage virtual machines (VMs) and containers on a single physical host. Proxmox offers features such as live migration, high availability clustering, and centralized management for efficient virtualization deployment.

Gantt Chart

Task	Expected Start	Actual Start
Project Initiation	Dec 01	Jan 05
Research and Planning	Dec 16	Jan 21
Setting up Virtual Machines	Jan 11	Feb 06
Installing and Configuring pfSense	Jan 21	Feb 11
Configuring Rules in pfSense Firewall	Jan 31	Feb 21
Enabling Snort IDS/IPS	Feb 06	Feb 26
Installing Zenarmor NGFW	Feb 11	Mar 04
Configuring Zenarmor	Feb 21	Mar 11
Enabling Syslog in Zenarmor	Feb 26	Mar 16
Installing Wazuh SIEM	Mar 03	Mar 21
Configuring Wazuh	Mar 03	Mar 26
Enabling Syslog in Wazuh	Mar 06	Apr 01
Decoding JSON Logs in Wazuh	Mar 06	Apr 01
Writing Rules for Wazuh	Mar 08	Apr 03
Connecting and Testing Servers	Mar 10	Apr 04
Installing Offline AI	Mar 14	Apr 04
Installing Kali Linux	Mar 15	Apr 04
Configuring Network Settings	Apr 04	Apr 04