

Project Report on

**SecuLab: Deployment of Secured and Monitored Infrastructure using Virtualization**

**Submitted by**

**Chinmay Patil (250244223012)**

**Manu Sharma (250244223028)**

**Vaishnavi Mehar (250244223054)**

**Aparna Korade (250244223023)**

Under the guidance of

**Mr. Sandeep Walvekar**

**In partial fulfillment of the award of** **Post Graduate Diploma in**

**IT Infrastructure, Systems and Security**

**(PG-DITISS)**



**Sunbeam Institute of Information Technology,**

**Pune (Maharashtra)**

**PG-DITISS -2025**

# DECLARATION

We declare that this written submission represents our ideas in our own words and where others ideas or words have been included; we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed**.**

Place: Pune

Date:

**Chinmay Patil Manu Sharma Vaishnavi Mehar Aparna Korade**

**(250244223012) (250244223028) (250244223054) (250244223023)**

# CERTIFICATE

This is to certify that the project report entitled **“SecuLab: Deployment of Secured and Monitored Infrastructure using Virtualization”**, submitted by **Chinmay Patil** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

# CERTIFICATE

This is to certify that the project report entitled **“SecuLab: Deployment of Secured and Monitored Infrastructure using Virtualization”** submitted by **Manu Sharma** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

# CERTIFICATE

This is to certify that the project report entitled **“SecuLab: Deployment of Secured and Monitored Infrastructure using Virtualization”** submitted by **Vaishnavi Mehar** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

# CERTIFICATE

This is to certify that the project report entitled **“SecuLab: Deployment of Secured and Monitored Infrastructure using Virtualization”** submitted by **Aparna Korade** is the bonafide work completed under our supervision and guidance in partial fulfillment for the award of Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

**Mr. Sandeep Walvekar Mr. Vishal Salunkhe**

Guide Course Coordinator

**Mr. Nitin Kudale**

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

# APPROVAL CERTIFICATE

This Project II report entitled **“SecuLab: Deployment of Secured and Monitored Infrastructure using Virtualization”** by **Chinmay Patil (250244223012)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

# APPROVAL CERTIFICATE

This Project II report entitled **“SecuLab: Deployment of Secured and Monitored Infrastructure using Virtualization”** by **Manu Sharma (250244223028)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

# APPROVAL CERTIFICATE

This Project II report entitled **“SecuLab: Deployment of Secured and Monitored Infrastructure using Virtualization”** by **Vaishnavi Mehar (250244223054)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

# APPROVAL CERTIFICATE

This Project II report entitled **“SecuLab: Deployment of Secured and Monitored Infrastructure using Virtualization”** by **Aparna Korade (250244223023)** is approved for Post Graduate Diploma in IT Infrastructure, Systems and Security (PG-DITISS) of Sunbeam Institute of Information Technology, Pune (M.S.).

Place: Pune

Date:

Examiner:

**(Signature)**

**(Name)**

# CONTENTS

|  |  |
| --- | --- |
| **TITLE** | **PAGE NO** |
| **Declaration** |  |
| **Certificate** |  |
| **Approval Certificate** |  |
| **Abstract** | i |
| **1.INTRODUCION** | 1 |
| 1.1 Applications | 2 |
| **2. LITERATURE SURVEY** | 4 |
| Paper 1 | 4 |
| Paper 2 | 4 |
| Paper 3 | 5 |
| **3. SYSTEM DEVELOPMENT AND DESIGN** | 6 |
| 3.1 Proposed System | 6 |
| 3.2 Architecture Diagram | 7 |
| 3.3 Technology used | 8 |
| 3.3.1 VMware Workstation Pro | 8 |
| 3.3.2 Debian and Rocky Linux | 8 |
| 3.3.3 Apache HTTP Server | 8 |
| 3.3.4 Postfix and Dovecot | 9 |
| 3.3.5 Snort | 9 |
| 3.3.6 Nagios XI | 10 |
| 3.3.7 FortiGate Firewall | 10 |
| **4. PROJECT OUTPUT** | 11 |
| **5. CONCLUSION** | 14 |
| 5.1 Conclusion | 14 |
| 5.2 Future Scope | 14 |
| **REFERENCES** | 15 |

# ABSTRACT

This project simulates an enterprise-style IT infrastructure with a focus on secure communication, network segmentation, and monitoring. The setup uses VMware-based virtual machines to implement a layered network architecture featuring a DMZ, internal LAN, and segregated services. Key components include Web, Mail, DNS/DHCP, Database, and File servers, as well as a Nagios XI monitoring system, FortiGate firewall, and Snort IDS. The project demonstrates secure access control, SSL certificate deployment, traffic inspection, and alert-based monitoring.

# INTRODUCTION

In modern enterprise environments, secure and efficient network infrastructure is critical for ensuring smooth operations, data protection, and reliable service delivery. This project focuses on the design and implementation of a simulated enterprise-grade network architecture that replicates real-world scenarios using virtualization. The network is built with a layered design, incorporating a Demilitarized Zone (DMZ) for public-facing services, an internal LAN for secure operations, and dedicated servers for specific roles.

The core objective is to integrate multiple essential services such as web hosting, email communication, database management, file sharing, domain resolution, DHCP allocation, and centralized monitoring within a controlled and secure setup. The entire infrastructure is virtualized using VMware Workstation Pro, allowing flexible deployment, rapid testing, and resource optimization without the need for extensive physical hardware.

Security is a key focus of the project. A Fortinet FortiGate Next-Generation Firewall is deployed to enforce strict access control policies, inspect network traffic at both the network and application layers, and enable port forwarding and DMZ segregation. The firewall works in conjunction with Snort-based Intrusion Detection to detect malicious activity targeting the web application hosted in the DMZ.

System monitoring is achieved using Nagios XI, which provides real-time host and service status tracking, automated alerts via email, and reporting capabilities. This ensures rapid identification and resolution of issues, improving system availability. Additional security is enforced through the implementation of SSL/TLS certificates using XCA for encrypted communication between services, enhancing confidentiality and integrity of data.

The project demonstrates a complete service lifecycle — from DNS resolution and DHCP assignment to secure application delivery, email communication, and file sharing — all within a controlled network. This setup not only mirrors real enterprise infrastructure but also provides a platform for experimenting with security policies, intrusion detection rules, and monitoring strategies.

By combining multiple technologies and following a structured network design, this project provides valuable hands-on experience in systems administration, cybersecurity, and IT infrastructure management, preparing for real-world enterprise deployment scenarios.

## Applications

The project hosts an Online Library Book Management System as the primary application in the DMZ web server. This application is developed using PHP for the backend logic and HTML/CSS/JavaScript for the frontend, running on an Apache HTTP server. The database backend is powered by MariaDB/MySQL, hosted on a separate database server within the internal LAN, ensuring data security and preventing direct public access.

The application allows library administrators and registered users to perform the following functions:

* Book Management – Add, update, and remove books from the catalog.
* User Account Management – Create and manage user profiles with authentication and role-based permissions.
* Book Issue/Return Tracking – Manage borrowing and returning of books, with due date tracking.

The separation of the web and database servers ensures better performance, scalability, and security. All connections between the application and the database are secured using SSL/TLS certificates, while firewall rules restrict database access only to the web server and authorized LAN devices.

## 1.2 Project Plan

**Table: Activities Details**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Sr.**  **No.** | **ACTIVITY** | **WEEK** | | | |
| **1** | **2** | **3** | **4** |
| 1 | Project group formation |  |  |  |  |
| 2 | Project work to be started in respective labs |  |  |  |  |
| 3 | First review with PPT presentation |  |  |  |  |
| 4 | Design Architecture Diagram as per project |  |  |  |  |
| 5 | Second review with PPT presentation |  |  |  |  |
| 6 | Selection |  |  |  |  |
| 7 | Final review with PPT presentation |  |  |  |  |
| 8 | Implementation and configuring as per project flow |  |  |  |  |
| 9 | Testing, Troubleshooting with different techniques |  |  |  |  |
| 10 | Created Soft copy of project and then final hard copy |  |  |  |  |

# 2. LITERATURE SURVEY

## **Paper 1**: - How to Maximize Performance in Nagios XI 2024

**Author:** Nagios

**Source:** Nagios Documents ([Link](https://assets.nagios.com/downloads/nagiosxi/docs/Maximizing-Performance-in-XI-2024.pdf))

**Description:** Nagios XI is a widely adopted monitoring platform that offers advanced alerting, custom dashboards, and agent-based or agentless monitoring. Its user-friendly web UI distinguishes it from Nagios Core by simplifying configuration and integration with plugins. Research such as 'Maximizing Performance in XI 2024' highlights how performance tuning and scalability can improve enterprise monitoring reliability. Additional studies emphasize Nagios’s ability to detect anomalies quickly, reducing downtime.

## **Paper 2:** **-** *FortiGate Firewall Complete Guide* (GitHub)

**Author:** Pavankumar Hegde

**Source:** GitHub repository ([GitHub](https://github.com/hegdepavankumar/Fortigate-Firewall-Complete-Guide))

**Description:** The GitHub repository **“FortiGate-Firewall-Complete-Guide”** by hegdepavankumar serves as a comprehensive, community-driven resource for mastering the FortiGate firewall platform. It delivers a structured, hands-on learning path crafted for virtual lab environments like EVE-NG hosted on VMware, providing practical exposure to:

* **Fundamentals and Interfaces**: Starting with firewall architecture, basic interface setup, and administrative access via CLI and GUI.
* **Security Operations & High Availability**: Details on configuring firewall policies, security profiles, authentication modules, and building HA clusters.
* **Logging, Monitoring & VPN**: Guidance on monitoring traffic and events, enabling logging, and setting up both IPsec and SSL VPNs.

## **Paper 3: -** Complete Guide to FortiGate Firewall

## Author: Axians UK Security Team.

**Source:** Article ([Link](https://www.axians.co.uk/news/completeguide-to-fortigate-firewall/))

**Description:** The Axians UK article *“Complete Guide to FortiGate Firewall”* offers a comprehensive explanation of Fortinet’s FortiGate platform, portraying it as more than just a traditional firewall. It is presented as a unified security solution that integrates multiple capabilities such as intrusion prevention, web filtering, antivirus, application control, and advanced threat detection into a single system. The article highlights its scalability and flexibility, with deployment options ranging from physical appliances to virtual machines and cloud instances, making it adaptable to a wide range of network environments. Emphasis is placed on its advanced threat protection features, including integration with FortiGuard Labs for real-time intelligence to counter emerging threats, and its centralized management through FortiManager, which enables streamlined policy enforcement across multiple devices. The piece also underlines FortiGate’s ability to reduce complexity and improve efficiency through automation and deep packet inspection, positioning it as a robust choice for both enterprise and hybrid networks, while supporting modern connectivity requirements with built-in SD-WAN capabilities.

# SYSTEM DEVELOPMENT AND DESIGN

## 3.1 Proposed System

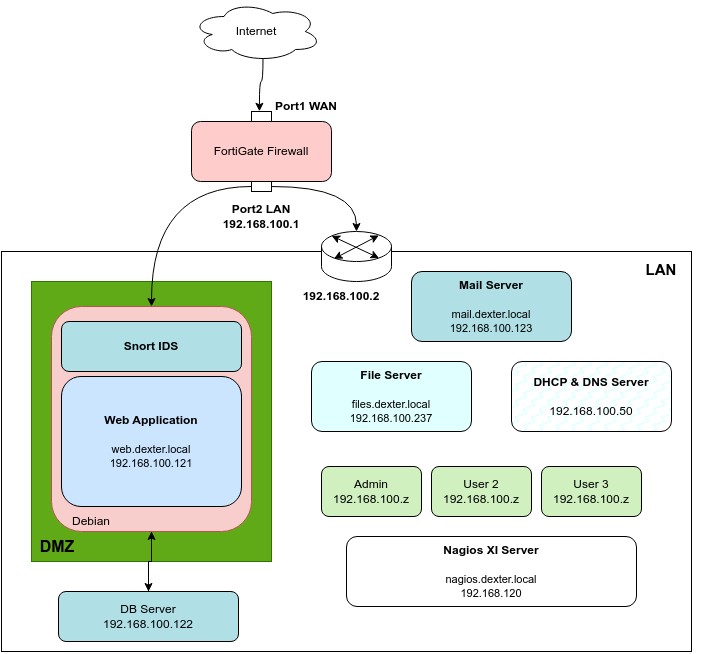
The proposed system aims to design and implement a secure, scalable, and enterprise-style network infrastructure within a virtualized environment using VMware Workstation Pro. The network architecture will follow a layered approach, incorporating DMZ (Demilitarized Zone) for public-facing services, an internal LAN for sensitive operations, and a firewall-based security perimeter for traffic inspection and control.

The system will host multiple critical services including Web Server, Database Server, Mail Server, DNS/DHCP Server, File Server, and Network Monitoring Server (Nagios XI). A Snort-based IDS will be deployed to monitor and detect suspicious activity, while a FortiGate Firewall will be configured for network segmentation, port forwarding, DMZ creation, and policy-based access control at both network and application layers.

Secure communication between services will be ensured using SSL/TLS certificates generated through XCA, with chain certificates installed on both Linux servers and Windows clients. All services will be interconnected using domain-based resolution to provide easy access and centralized management.

The proposed setup allows external users to access only the public-facing web application through the firewall and DMZ, while sensitive backend systems like the database remain isolated from direct internet exposure. Internal users and developers will have restricted, secure access to backend resources via LAN, and administrators will monitor the entire infrastructure using Nagios XI with real-time alerts.

## 3.2 Architecture Diagram



**Figure: Architecture Diagram**

## 3.3 Technology used

### 3.3.1 VMware Workstation Pro

VMware Workstation Pro is a professional-grade virtualization platform that enables running multiple isolated operating systems on a single physical machine. It is widely used for development, testing, and training environments.

**Key Features:**

* Multi-VM Support – Run multiple virtual machines simultaneously.
* Networking Modes – Supports bridged, NAT, and host-only networking for flexibility.
* Snapshots & Cloning – Quickly revert or replicate environments for testing.

### 3.3.2 Debian & Rocky Linux

Debian and Rocky Linux are stable, open-source Linux distributions widely used in server environments. They provide reliability, long-term support, and compatibility with enterprise applications.

**Key Features:**

* Open-Source & Free – No licensing cost, fully community-driven.
* Stability – Proven reliability in production environments.
* Package Repository – Large software library with easy package management.

### 3.3.3 Apache HTTP Server

Apache HTTP Server is one of the most widely used open-source web servers, capable of serving static and dynamic content. It supports modular extensions and integrates easily with PHP.

**Key Features:**

* Cross-Platform – Runs on various operating systems.
* PHP Integration – Enables dynamic web application deployment.
* Module Support – Extend functionality with security, caching, and logging modules.

### 3.3.4 Postfix & Dovecot

Postfix is a mail transfer agent (MTA) for sending emails, and Dovecot is an IMAP/POP3 server for receiving and storing emails. Together, they provide a complete mail solution.

**Key Features:**

* Secure Email – SSL/TLS encryption for confidentiality.
* Efficient Delivery – Optimized for performance and reliability.
* Standards-Compliant – Works with most email clients and protocols.

### 3.3.5 Snort

### Snort is an open-source Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) that is widely used for network security monitoring. It helps detect and prevent unauthorized access, malicious activities, and security threats within network traffic. Snort is designed to analyze network packets in real-time and generate alerts when it identifies patterns that match known attack signatures or behavior anomalies.

**Key Features:**

* Signature-Based Detection – Identifies known threats via rule sets.
* Custom Rules – Tailor detection to specific network needs.
* Logging & Alerts – Records incidents for analysis and response.

### 3.3.6 Nagios XI

### Nagios is an open-source monitoring system that provides comprehensive monitoring and alerting capabilities for IT infrastructure components. It helps organizations monitor the health and performance of their networks, servers, applications, and services, enabling proactive identification and resolution of issues before they impact business operations.

### Key Features:

* Web-Based Management – Configure and monitor from the browser.
* Custom Alerts – Email and SMS notifications for issues.
* Reporting & Dashboards – Visual insights into system health.
  + 1. **FortiGate Firewall**

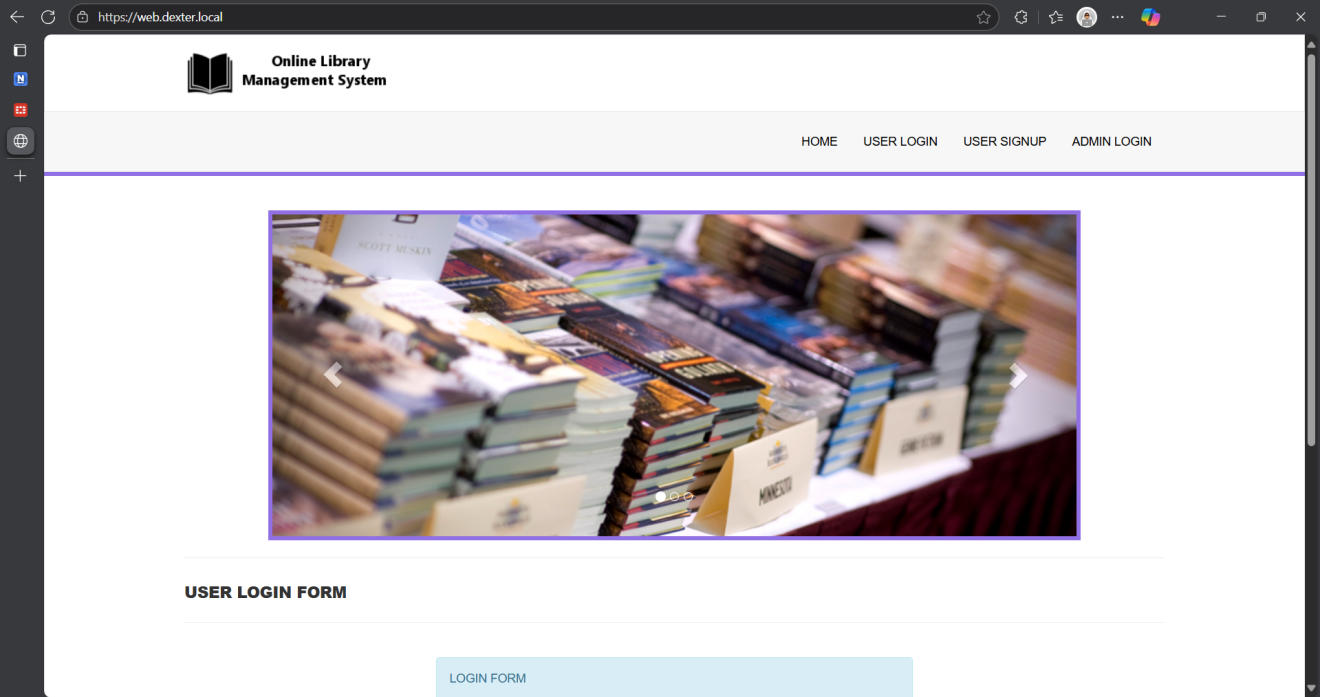
FortiGate is a next-generation firewall offering unified threat management (UTM) features for secure network operations.

**Key Features:**

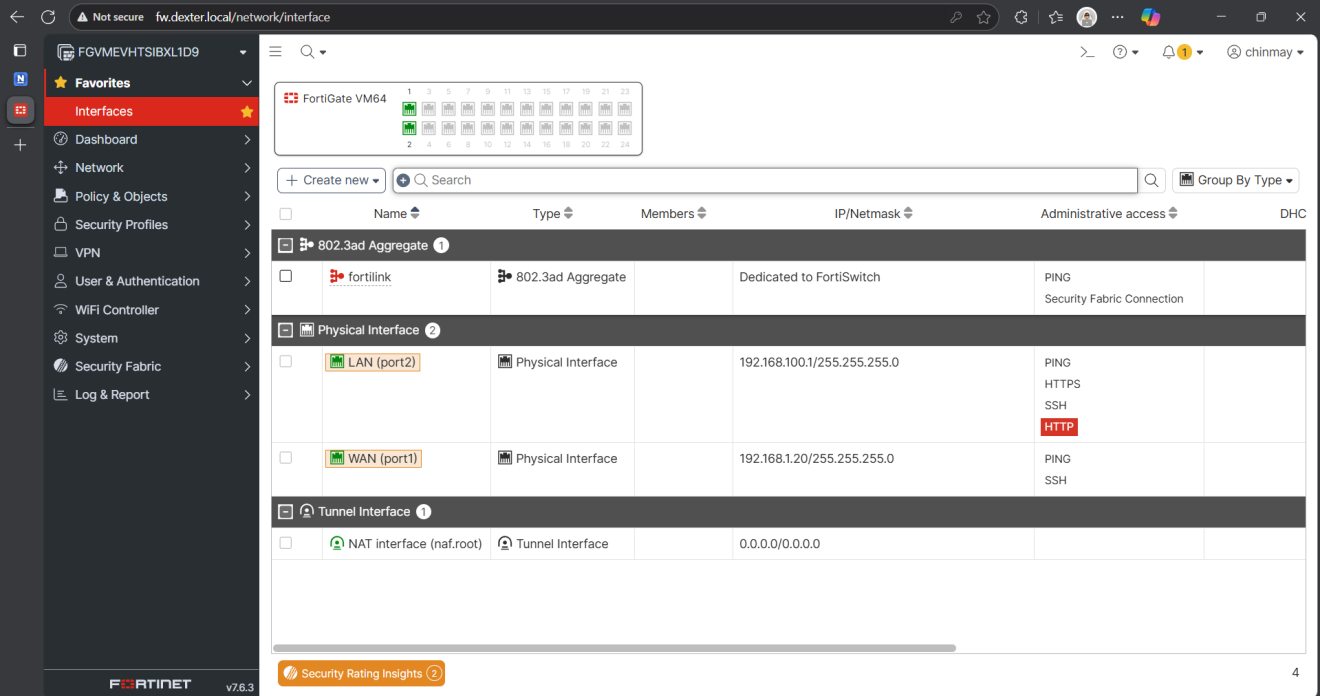
* Application & Network Layer Security – Filters traffic based on protocols and patterns.
* DMZ & Port Forwarding – Securely host public services.
* Intrusion Prevention – Detects and blocks malicious traffic.

# 4. Project Output

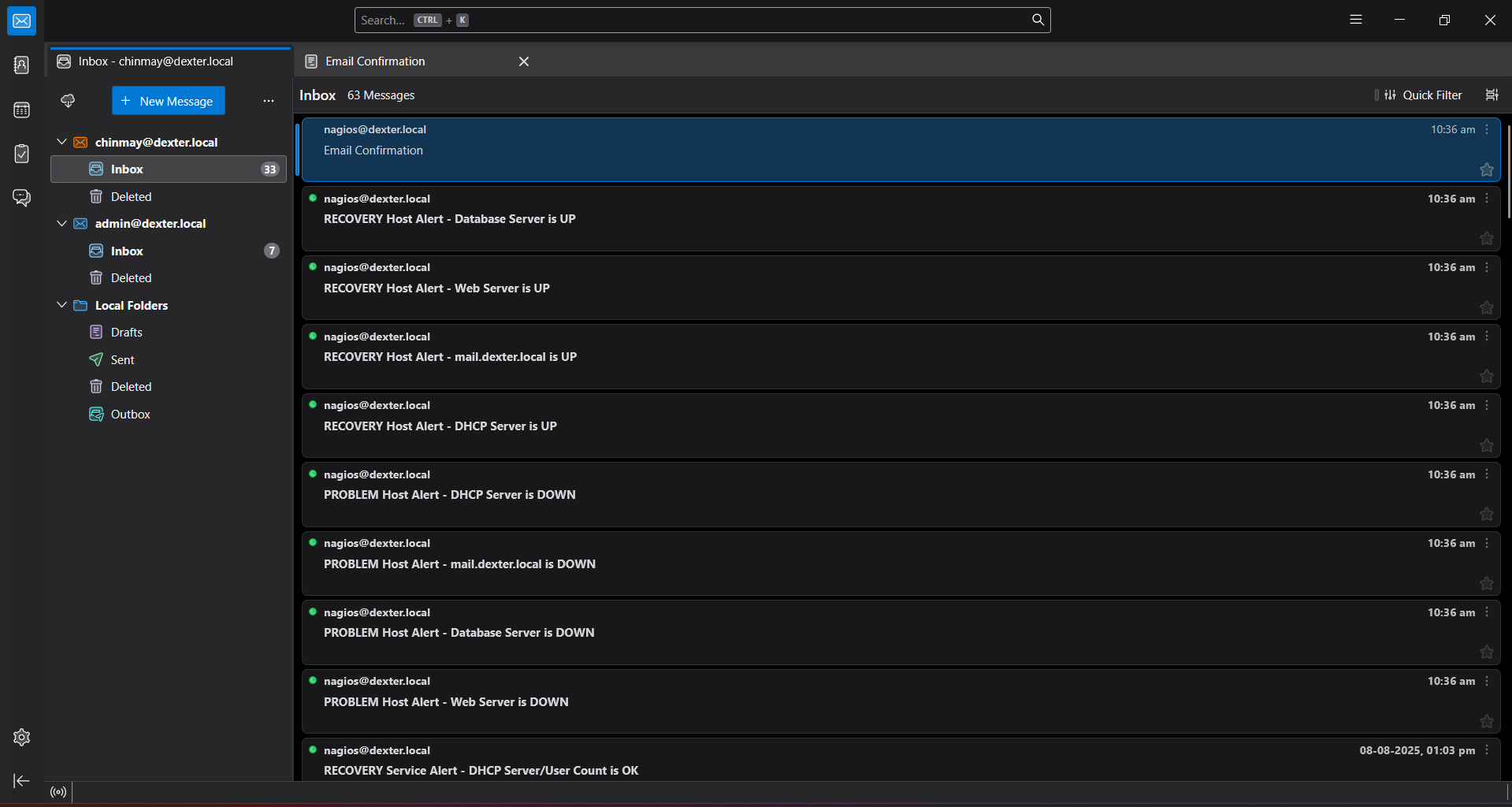
## Web Application with HTTPS



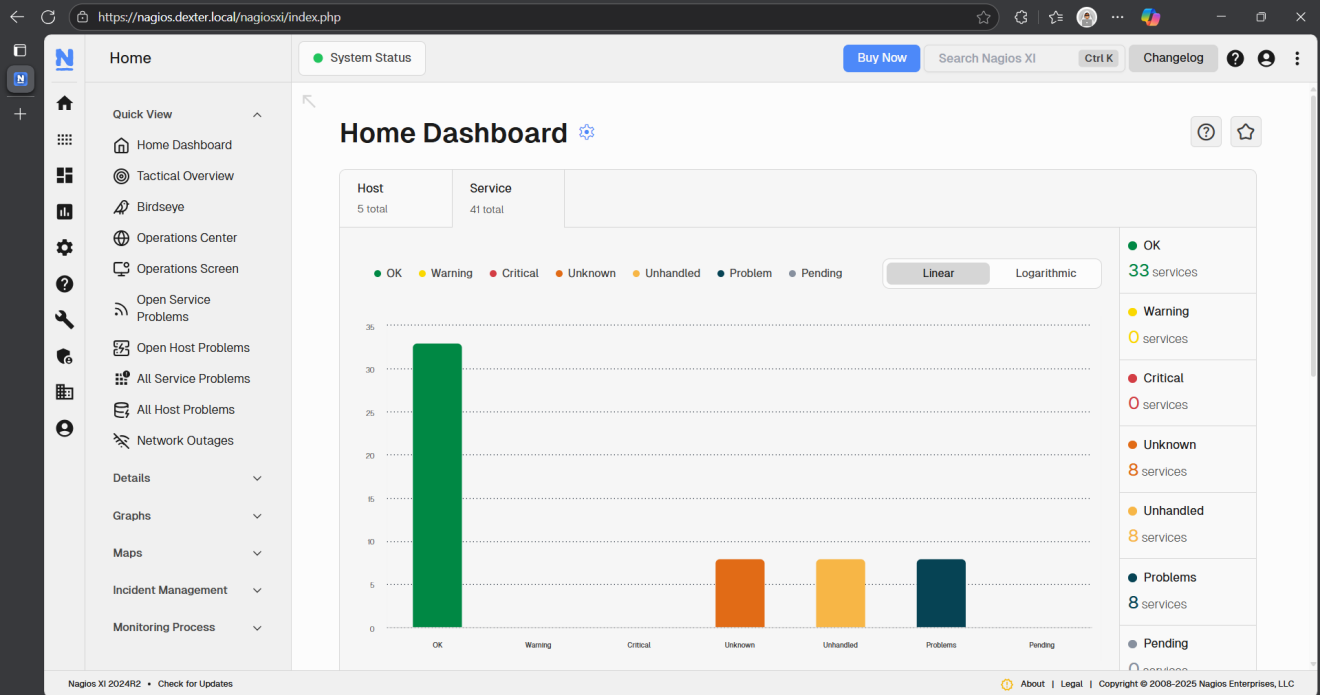
## Firewall Web Interface



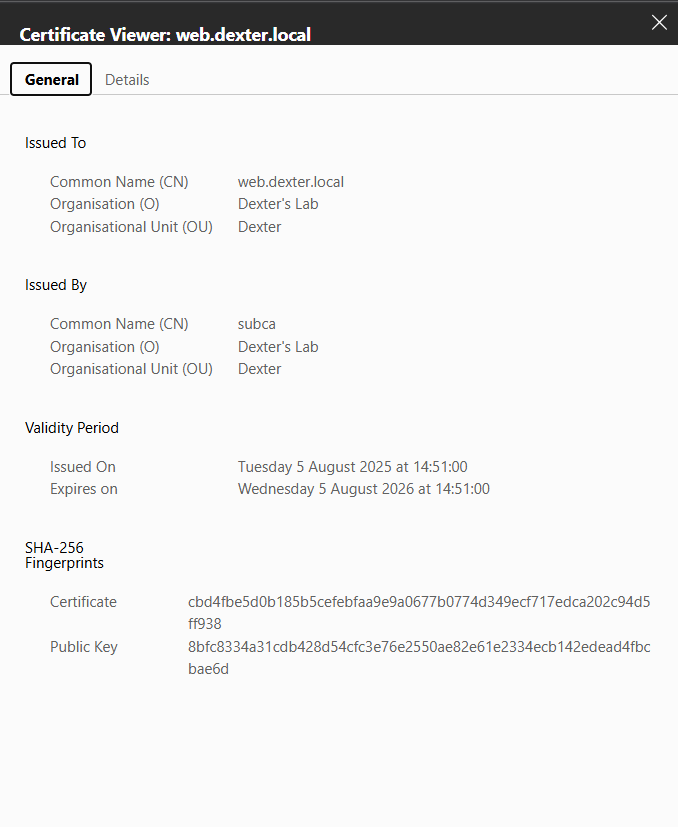
## Thunderbird Mail Client with Received Emails



* 1. **Nagios XI Monitoring Dashboard**

****

* 1. **SSL Certificates in Use**



# 5. CONCLUSION

## 5.1 Conclusion

The project successfully demonstrates the design, deployment, and management of a secure, monitored, and functional enterprise-style network infrastructure within a virtualized environment. By combining open-source tools such as Debian, Rocky Linux, Apache, MariaDB, Postfix, Dovecot, Snort, and Nagios XI with enterprise-grade security products like the FortiGate firewall, the setup achieves a well-structured and layered architecture that ensures network segmentation, threat detection, and secure communications across all services. The implementation of a DMZ, controlled access policies, SSL/TLS encryption, and intrusion detection mechanisms strengthens the security posture, while centralized monitoring through Nagios XI enhances visibility and proactive issue resolution. Furthermore, the deployment highlights best practices in server configuration, service hardening, and policy-based access control, making it a realistic simulation of modern organizational infrastructure. This comprehensive approach not only fulfills the functional requirements of hosting and securing critical services like web, mail, database, DNS/DHCP, and file sharing but also provides a strong foundation for scalability, advanced security integrations, and further automation in future enhancements.

## 5.2 Future Scope

In the future, the project can be enhanced by containerizing the web application using Docker, enabling efficient deployment, portability, and easier scalability. A honeypot can be integrated into the database server to attract, detect, and analyze malicious activities targeting database services, thus improving the overall threat intelligence capabilities. Implementing a forward proxy in the LAN will provide better control over outbound internet access, content filtering, and user activity logging. Additionally, secure protocols such as IMAPS, SMTPS, and POP3S can be enforced for mail services to ensure encrypted communication, while adopting minimal Linux installations will reduce the attack surface by removing unnecessary services and closing unused ports, further strengthening the system’s security posture..

# REFERENCES

**Paper 1: - How to Maximize Performance in Nagios XI 2024**

**Author:** Nagios

**Source:** Nagios Documents ([Link](https://assets.nagios.com/downloads/nagiosxi/docs/Maximizing-Performance-in-XI-2024.pdf))

**Paper 2: - *FortiGate Firewall Complete Guide***

**Author:** Pavankumar Hegde

**Source:** GitHub repository ([GitHub](https://github.com/hegdepavankumar/Fortigate-Firewall-Complete-Guide))

**Paper 3: - Complete Guide to FortiGate Firewall**

**Author:** Axians UK Security Team

**Source:** Article ([Link](https://www.axians.co.uk/news/completeguide-to-fortigate-firewall/))