Project Report on

Securing Web Application Infrastructure: A Multi-Layered Approach

Submitted by

Ankur Garg	**(250244223008)**
Mayuri Bhalerao	**(250244223010)**
Pawankumar Shedage	**(250244223041)**
Rishikesh Kumar	**(250244223043)**

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 -2023

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: 11th August, 2025

Ankur Garg	**Mayuri Bhalerao**	**Pawankumar Shedage**	**Rishikesh Kumar**
(250244223008)	**(250244223010)**	**(250244223041)**	**(250244223043)**

CERTIFICATE

This is to certify that the project report entitled **"Securing Web Application Infrastructure: A Multi-Layered Approach"**, submitted by **Ankur Garg** 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: 11th August, 2025

Mr. Sandeep Walvekar

Guide

Mr. Vishal Salunkhe

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 **"Securing Web Application Infrastructure: A Multi-Layered Approach"**, submitted by **Mayuri Bhalerao** 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: 11th August, 2025

Mr. Sandeep Walvekar

Guide

Mr. Vishal Salunkhe

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 **"Securing Web Application Infrastructure: A Multi-Layered Approach"**, submitted by **Pawankumar Shedage** 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: 11th August, 2025

Mr. Sandeep Walvekar

Guide

Mr. Vishal Salunkhe

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 **"Securing Web Application Infrastructure: A Multi-Layered Approach"**, submitted by **Rishikesh Kumar** 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: 11th August, 2025

Mr. Sandeep Walvekar

Guide

Mr. Vishal Salunkhe

Course Coordinator

Mr. Nitin Kudale

CEO

Sunbeam Institute of Information Technology

Pune (M.S.) – 411057

APPROVAL CERTIFICATE

This Project II report entitled **"Securing Web Application Infrastructure: A Multi-Layered Approach"** by **Ankur Garg (250244223008)** 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: 11th August, 2025

Examiner: _____

(Signature)

_____

(Name)

APPROVAL CERTIFICATE

This Project II report entitled **"Securing Web Application Infrastructure: A Multi-Layered Approach"** by **Mayuri Bhalerao (250244223010)** 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: 11th August, 2025

Examiner: _____

(Signature)

_____

(Name)

APPROVAL CERTIFICATE

This Project II report entitled **"Securing Web Application Infrastructure: A Multi-Layered Approach"** by **Pawankumar Shedage (250244223041)** 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: 11th August, 2025

Examiner: _____

(Signature)

_____

(Name)

APPROVAL CERTIFICATE

This Project II report entitled **"Securing Web Application Infrastructure: A Multi-Layered Approach"** by **Rishikesh Kumar (250244223043)** 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: 11th August, 2025

Examiner: _____

(Signature)

_____

(Name)

CONTENTS

TITLE	PAGE NO
Declaration	
Certificate	
Approval Certificate	
Abstract	i
1.INTRODUCION	1
1.1 Applications	1
1.2 Organization and Project Plan	3
2. LITERATURE SURVEY	4
Paper 1	4
Paper 2	4
Paper 3	4
3. SYSTEM DEVELOPMENT AND DESIGN	5
3.1 Proposed System	6
3.2 Flow Chart	7
3.3 Technology used	6
3.3.1 pfSense with Suricata IDS/IPS	6
3.3.2 PRTG Network Monitor	7
3.3.3 Grafana with Loki & Promtail	8
3.3.4 MySQL Database with Backup Automation	8
3.3.5 Backup Server	9
3.3.6 Telegram Integration	10
4. PROJECT OUTPUT	11
5. CONCLUSION	15
5.1 Conclusion	15
5.2 Future Scope	15
REFERENCES	16

ABSTRACT

This project presents a fully integrated network security, monitoring, and alerting architecture using open-source and automation-driven tools. The primary objective is to ensure real-time intrusion prevention, performance visibility, log analysis, and secure backup management across all infrastructure components. Network traffic first traverses a pfSense firewall, where Suricata IDS/IPS performs deep packet inspection to detect and block malicious activities instantly. Custom security rules enhance detection for targeted threats specific to the deployment environment.

System performance is continuously tracked using PRTG Network Monitor, which gathers metrics such as CPU load, memory usage, disk capacity, and network throughput from all connected devices, including the Web Server and MySQL Database Server. These performance statistics and event logs are forwarded to Grafana, which acts as the central visualization dashboard for both real-time and historical data.

To extend monitoring capabilities, Loki and Promtail are integrated for log aggregation, enabling efficient search and correlation of system events. This allows administrators to quickly trace incidents and identify the root cause of anomalies. In addition to visual dashboards, the system includes an advanced alerting mechanism. Both Grafana and PRTG generate alerts based on predefined thresholds and anomaly patterns, sending instant notifications via Telegram bot and email. This ensures prompt response, even when administrators are offsite.

The MySQL database, used for storing configuration data and application-related records, is hosted on a secure private network segment. Automated backup scripts generate encrypted database dumps, which, along with collected logs and dashboard configurations, are transferred to a dedicated backup server. This backup strategy guarantees data redundancy, integrity verification, and fast disaster recovery in case of system failure.

Overall, the proposed solution ensures continuous infrastructure monitoring, proactive intrusion prevention, high system visibility, and secure data retention. By combining IDS/IPS, network monitoring, centralized log management, and multi-channel alerting, this architecture offers a robust and scalable approach to maintaining security and operational efficiency in modern network environments.

1. INTRODUCTION

In today's interconnected IT environments, the deployment, monitoring, security, and maintenance of network services have become critical for ensuring reliability and operational efficiency. This project presents an integrated approach to building a secure and high-performing infrastructure by implementing PRTG for real-time monitoring, Suricata as an Intrusion Detection and Prevention System (IDS/IPS), a centralized backup system using rsync over SSH, and Apache with MySQL/MariaDB for web and database hosting.

Monitoring with PRTG:

PRTG Network Monitor serves as the backbone for performance oversight, enabling administrators to track uptime, bandwidth usage, and the health of all critical services. Configured alerts and interactive dashboards facilitate early detection of anomalies, ensuring that potential issues are addressed before they affect service availability.

Network Security with Suricata IDS/IPS:

Security is a top priority in any modern infrastructure. Suricata provides deep packet inspection and advanced traffic analysis, operating in both IDS and IPS modes. This allows for the detection of malicious patterns and the blocking of suspicious activities, protecting against both internal and external threats.

Centralized Backup System:

A robust backup strategy ensures data resilience and disaster recovery readiness. Using rsync over encrypted SSH channels, this project implements a centralized backup solution that performs automated scheduled backups of configuration files, application data, and critical databases, safeguarding against accidental loss or corruption.

Web and Database Hosting:

The Apache web server delivers reliable and scalable hosting for applications, while MySQL/MariaDB provides a secure, high-performance backend for data management. Both services are configured for optimized performance, ensuring smooth delivery of web-based services.

By integrating monitoring, security, backup, and hosting services, this project demonstrates a scalable and secure infrastructure capable of meeting enterprise-level requirements for performance, availability, and data protection. The subsequent sections explore each component in detail, providing configuration insights, best practices, and implementation guidelines.

1.1 Applications

- Enterprise Networks: Ideal for organizations requiring continuous monitoring, data security, and high-availability hosting of business-critical applications..

- Educational Institutions: Supports secure hosting of learning platforms, centralized backup of academic resources, and proactive monitoring of IT infrastructure.

- E-Governance Systems: Ensures uninterrupted operation of government portals with secure data handling and real-time performance oversight.

- Research and Development Labs: Facilitates secure hosting of internal tools, protection of sensitive research data, and rapid recovery in case of system failures.

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 Use-Case view as per project				
5	Design Block diagram as per project				
6	Second review with PPT presentation				
7	Selection				
8	Final review with PPT presentation				
9	Implementation coding as per project				
10	Testing, Troubleshooting with different techniques				
11	Created Soft copy of project and then final hard copy				

2. LITERATURE SURVEY

Paper 1: - VINEVI: A Virtualized Network Vision Architecture for Smart Monitoring of Heterogeneous Applications and Infrastructures

Author: Rodrigo Moreira, Hugo G. V. O. da Cunha, Larissa F. Rodrigues Moreira, Flávio de Oliveira Silva

Description: This paper introduces a novel architecture—VINEVI—for seamless, detailed monitoring of both physical and virtualized infrastructures. It integrates real-time traffic classification agents with Prometheus and VictoriaMetrics to enable multi-tiered monitoring across diverse environments. The approach enhances visibility from hardware up through application layers.

Paper 2: - P4-NIDS: High-Performance Network Monitoring and Intrusion Detection in P4

Author: aying Chen, Siamak Layeghy, Liam Daly Manocchio, Marius Portmann

Description: This study presents a high-throughput, in-band monitoring and IDS solution built using the P4 programming language, designed for cloud-scale environments. It achieves ultra-low latency and high accuracy on real P4-capable hardware even at rates up to 8 million packets per second, offering a significant performance advantage over traditional out-of-band methods.

Paper 3: - Research and Build Cloud Servers Using Suricata to Detect and Respond to Cybersecurity Threats

Author: James Rebert, Poppy James, Victor Ogunrinde

Description: This paper explores the deployment of Suricata as an intrusion detection/prevention solution within cloud environments. It offers a practical framework for implementing Suricata on cloud servers, covering architectural design, rule management, automation, and orchestrated threat response. The study demonstrates how Suricata's deep packet inspection and real-time alerting can be optimized to secure cloud workloads effectively.

2. SYSTEM DEVELOPMENT AND DESIGN

3.1 Proposed System

We propose a comprehensive network security and monitoring framework that combines several open-source tools for intrusion detection, performance analysis, log handling, and data backup. Incoming network traffic is first directed through a router into a **pfSense firewall** equipped with **Suricata IDS/IPS**, enabling real-time detection and prevention of malicious activities.

System performance metrics and device status are gathered by **PRTG Network Monitor**, which monitors all connected devices, including the **Web Server** and the **MySQL Database** operating within a secure private network. PRTG forwards operational data and event logs to **Grafana**, which functions as the primary visualization and analytics platform.

For log management, **Loki** paired with the **Promtail agent** is linked to Grafana, facilitating centralized log aggregation, fast searches, and event correlation. Periodic backups are carried out for Grafana and PRTG logs, as well as MySQL database dumps, storing them securely on a dedicated backup server to ensure data safety and quick recovery in case of failures.

This setup delivers continuous system oversight, early threat detection, and reliable data preservation, while providing clear visibility across all infrastructure layers.

3.2 Flow chart

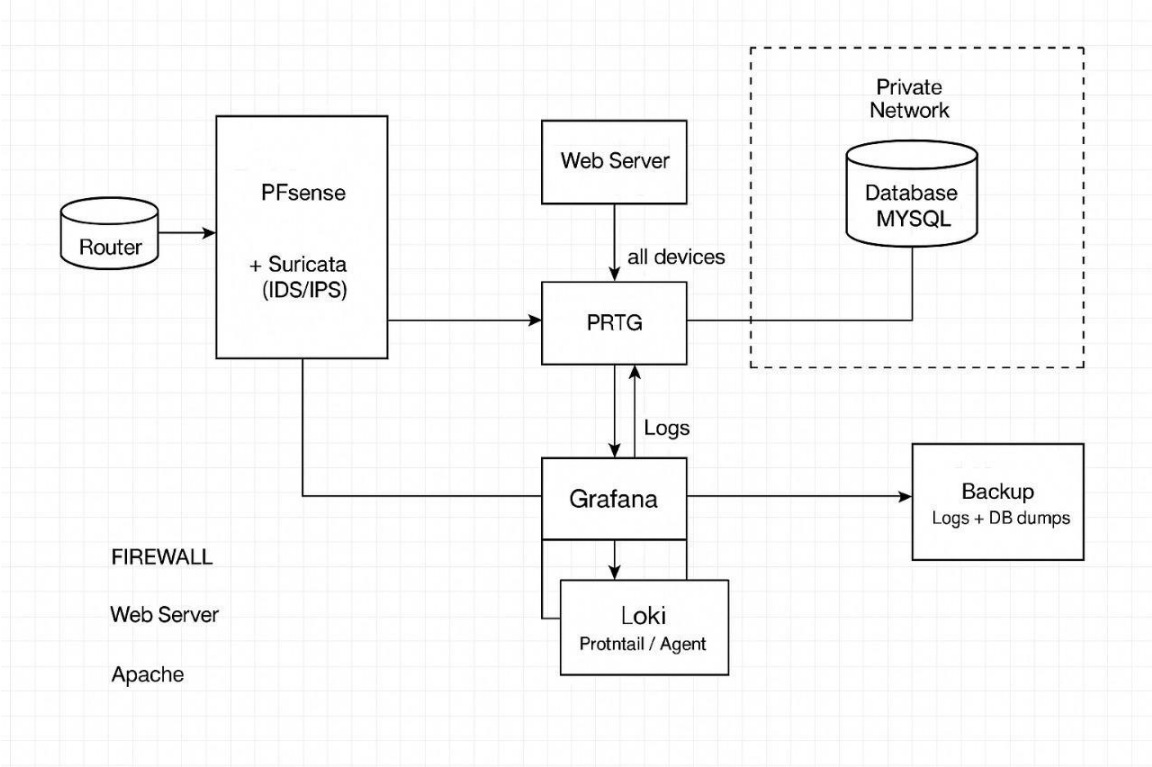


Figure: Flowchart

3.3 Technology used

3.3.1 pfSense with Suricata IDS/IPS

pfSense is an open-source firewall and router platform based on FreeBSD, offering enterprise-grade networking features with a user-friendly web interface. In this project, pfSense serves as the main network gateway and firewall, handling routing, NAT, and network segmentation. Integrated with **Suricata IDS/IPS**, pfSense performs deep packet inspection to detect and block malicious activities in real time.

Key features

- **Stateful Firewall:** Maintains state information about network connections, enabling advanced packet filtering and connection control.
- **Suricata Integration:** Provides signature-based and anomaly-based intrusion detection and prevention, blocking suspicious traffic instantly.
- **Custom Rules:** Allows the creation of project-specific security rules to detect targeted attacks on the infrastructure.
- **Traffic Shaping:** Prioritizes critical traffic, ensuring monitoring and security services always get bandwidth priority.
- **Secure Remote Management:** HTTPS and VPN-based admin access for secure configuration from remote locations.

3.3.2 PRTG Network Monitor

PRTG Network Monitor is a powerful infrastructure monitoring solution that collects performance data from devices, servers, and network interfaces. In this project, PRTG continuously monitors the health and status of the Web Server, MySQL Database Server, and the pfSense firewall itself.

Key features of PRTG Network Monitor:

- **Comprehensive Monitoring:** Tracks CPU usage, memory load, disk space, and network throughput for all connected devices.
- **Sensor-Based Data Collection:** Uses SNMP, WMI, and custom sensors to gather metrics from multiple platforms.
- **Threshold-Based Alerts:** Triggers alerts when performance metrics exceed pre-defined limits.
- **Integration with Telegram:** PRTG sends instant alerts to a configured **Telegram bot**, ensuring administrators are notified in real time.
- **Centralized Logging:** Performance data is forwarded to Grafana for visual analysis.

3.3.3 Grafana with Loki & Promtail

Grafana is an open-source visualization and analytics tool used to display metrics from multiple data sources in real time. In this project, Grafana acts as the **central** monitoring dashboard, visualizing PRTG metrics and aggregated logs from Loki.

Key features of Grafana with Loki & Promtail:

- Custom Dashboards: Displays live graphs of CPU load, bandwidth usage, service uptime, and IDS/IPS alerts.
- Loki Log Aggregation: Loki collects logs from PRTG, pfSense, Suricata, and servers, while Promtail agents handle log forwarding.
- Efficient Log Querying: Fast searching and filtering of logs to identify incidents.
- Anomaly Detection: Patterns in logs can be used to detect unusual system behaviour proactively.
- Telegram Alerts: Grafana alerts are pushed directly to the Telegram bot when anomalies or security breaches occur.

.

3.3.4 MySQL Database with Backup Automation

The MySQL database in this project stores configuration data, logs, and application-related information. It runs on a private network segment for improved security, accessible only by authorized services.

Key features of MySQL Database with Backup Automation:

- Optimized Performance: Configured with tuning parameters to handle logging workloads efficiently.
- Automated Backups: Daily database dumps are created and sent to the backup server.
- Disaster Recovery: Backup strategy ensures minimal downtime and data loss in case of system failure.
- Access Control: Only PRTG and authorized scripts can query the database, reducing attack surface.
- Data Encryption: Backup files are encrypted before being stored remotely.

3.3.5 Backup Server

The backup server acts as a redundancy layer, storing system logs, PRTG data, Grafana configurations, and MySQL dumps.

Key features:

- Multi-Source Backup: Receives files from Grafana, PRTG, pfSense, and MySQL.
- Scheduled Synchronization: Cron jobs ensure timely transfers without human intervention.
- Data Integrity Checks: Verifies backups to prevent corruption or incomplete uploads.
- Disaster Recovery Testing: Regular test restores are conducted to ensure backup usability.

3.3.6 Telegram Integration

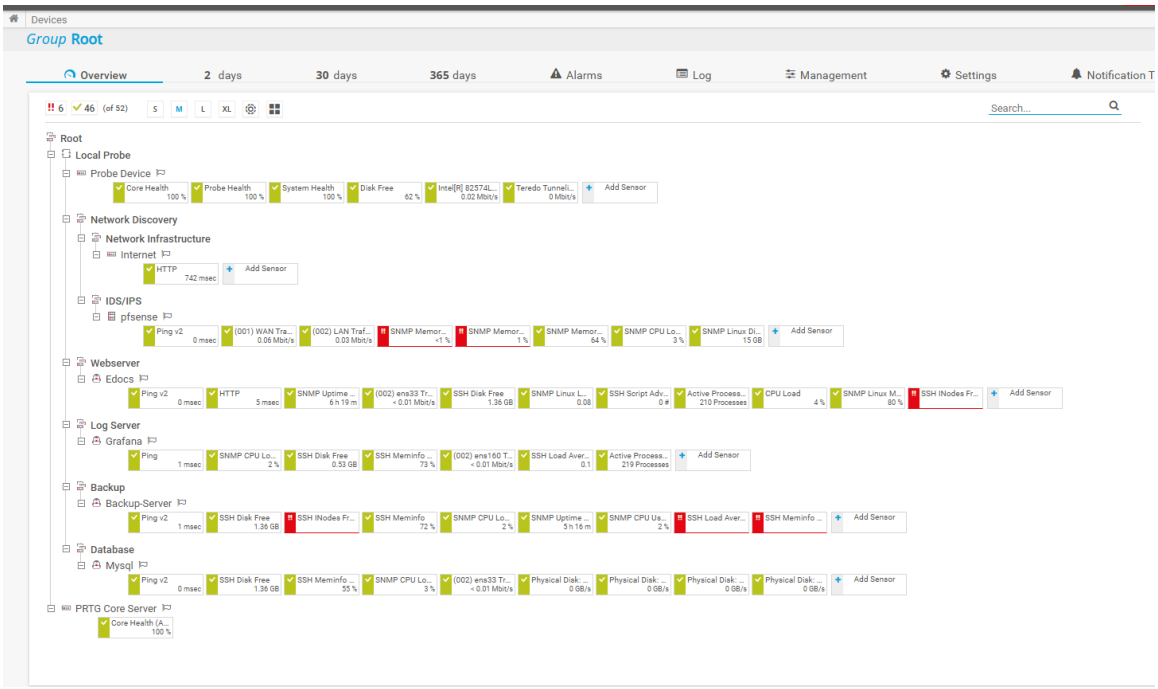
Telegram is used as a lightweight and secure notification channel for system alerts and security warnings.

Key features of Telegram Integration:

- Bot-Based Notifications: A Telegram bot is configured to receive messages from PRTG and Grafana alert systems.
- Real-Time Alerts: Instant push notifications on mobile devices, ensuring fast response to incidents.
- Secure API Communication: Bot API keys are stored securely to prevent unauthorized use.
- Custom Alert Formatting: Alerts include device name, metric exceeded, timestamp, and a quick link to the dashboard.

4. Project Output

4.1 PRTG Network Monitor



4.2 PfSense with Suricata as IDS/IPS

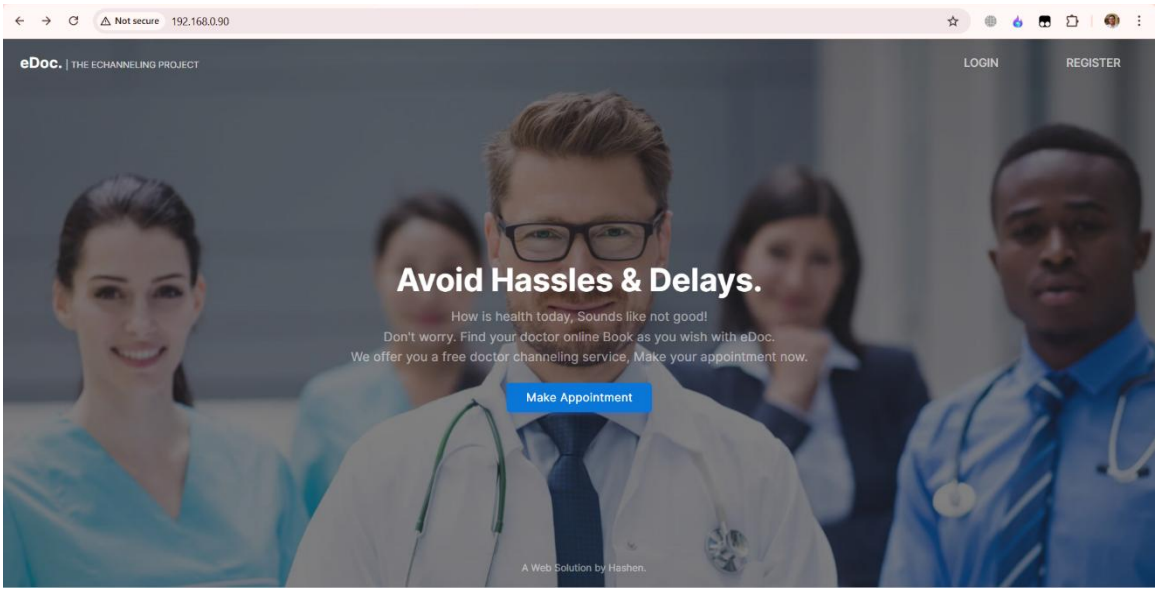
Alert Log View Filter

Last 250 Alert Entries. (Most recent entries are listed first)

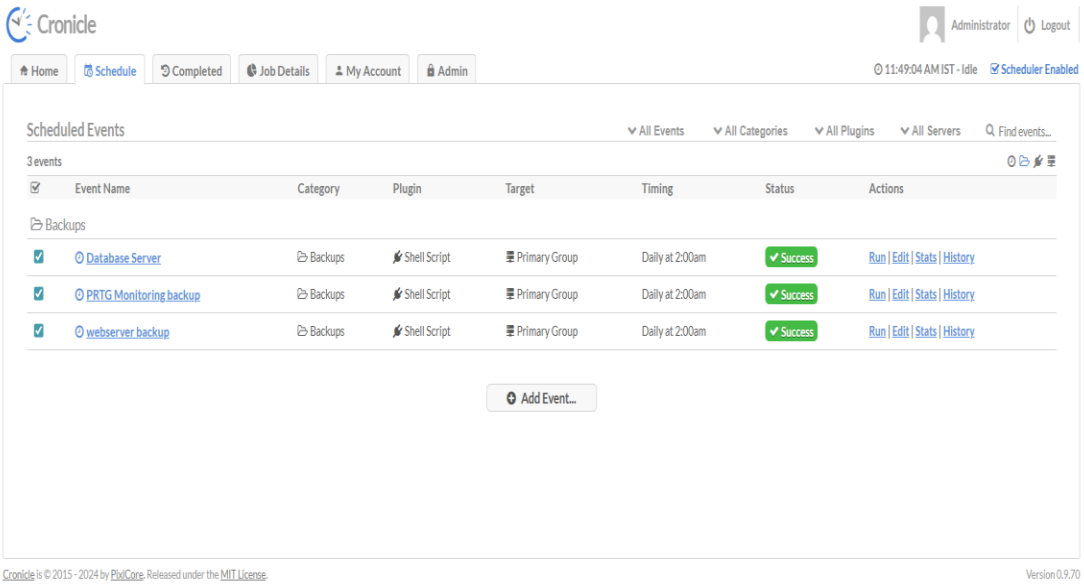
Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with highlighted rows below.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
08/11/2025 11:46:11		3	TCP	Generic Protocol Command Decode	192.168.0.90	80	192.168.0.181	31627	1:2260000	SURICATA Applayer Mismatch protocol both directions
08/11/2025 11:46:04		1	TCP	Web Application Attack	192.168.0.181	31623	192.168.0.90	80	1:2009358	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
08/11/2025 11:46:04		3	TCP	Generic Protocol Command Decode	192.168.0.90	80	192.168.0.181	31622	1:2260000	SURICATA Applayer Mismatch protocol both directions
08/11/2025 11:45:57		3	TCP	Generic Protocol Command Decode	192.168.0.90	80	192.168.0.181	31618	1:2260000	SURICATA Applayer Mismatch protocol both directions
08/11/2025 11:45:57		1	TCP	Web Application Attack	192.168.0.181	31617	192.168.0.90	80	1:2009358	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
08/11/2025 11:45:57		3	TCP	Generic Protocol Command Decode	192.168.0.90	80	192.168.0.181	31616	1:2260000	SURICATA Applayer Mismatch protocol both directions
08/11/2025 11:45:50		1	TCP	Web Application Attack	192.168.0.181	31612	192.168.0.90	80	1:2009358	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
08/11/2025 11:45:50		3	TCP	Generic Protocol Command Decode	192.168.0.90	80	192.168.0.181	31611	1:2260000	SURICATA Applayer Mismatch protocol both directions
08/11/2025 11:45:50		1	TCP	Web Application Attack	192.168.0.181	31610	192.168.0.90	80	1:2009358	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)
08/11/2025 11:45:50		3	TCP	Generic Protocol Command Decode	192.168.0.90	80	192.168.0.181	31609	1:2260000	SURICATA Applayer Mismatch protocol both directions
08/11/2025 11:45:50		3	TCP	Generic Protocol Command Decode	192.168.0.90	80	192.168.0.181	31608	1:2260000	SURICATA Applayer Mismatch protocol both directions
08/11/2025 11:45:43		1	TCP	Web Application Attack	192.168.0.181	31604	192.168.0.90	80	1:2009358	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)

4.3 Web Application

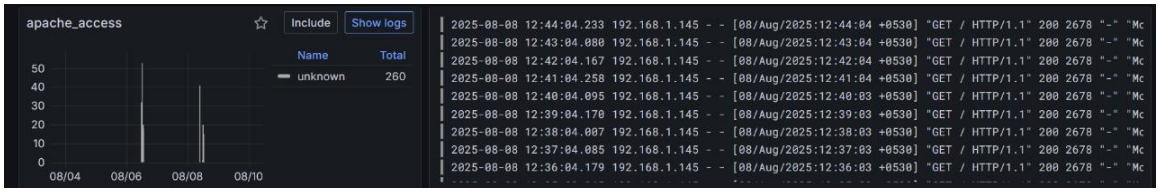


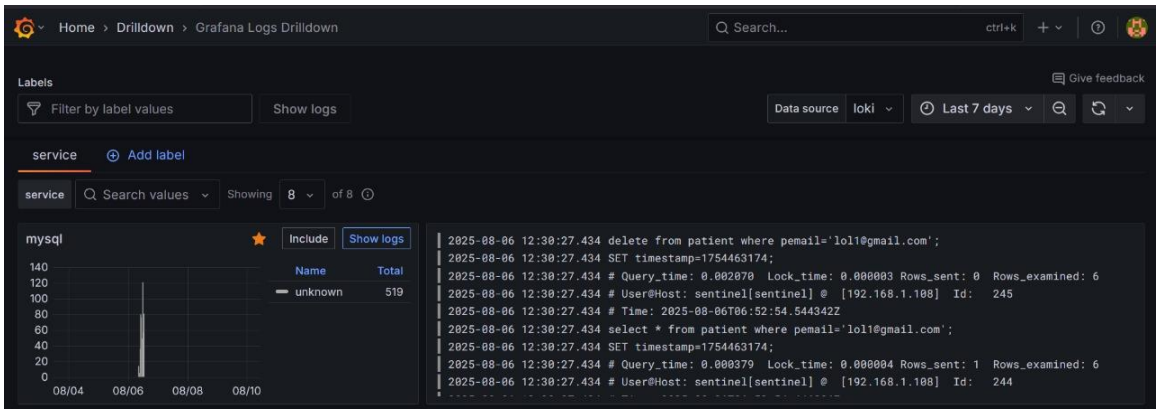
4.4 Backup Server

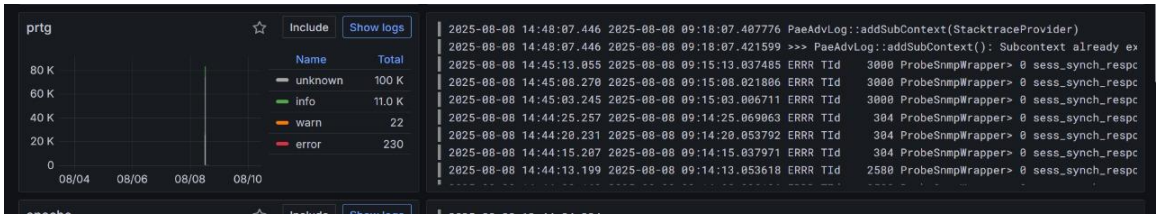


4.5 Grafana

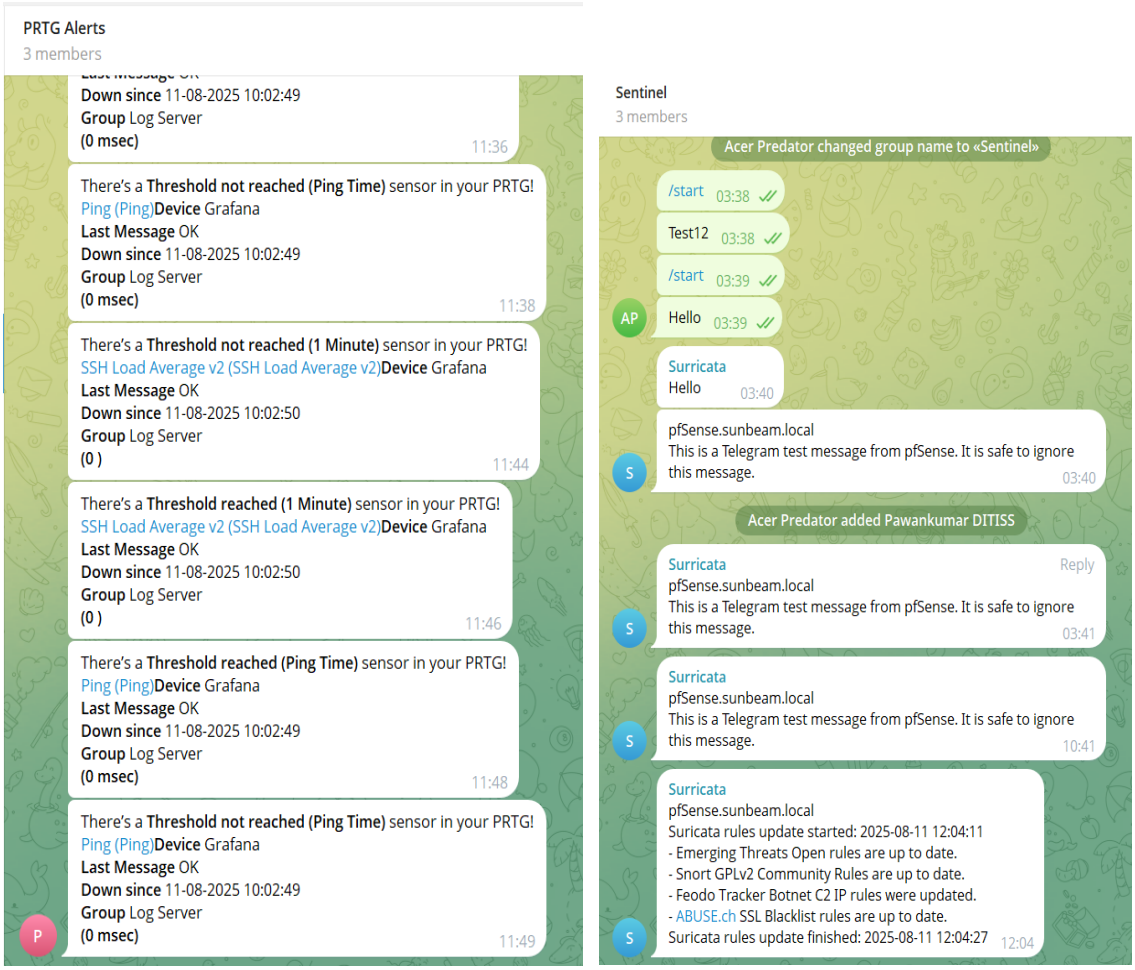

Home › Dashboards › My_apache_access1
Search...
Edit
Export
Share
Last 7 days
Refresh
Apache_access
11:40
11:50
12:00
12:10
12:20
12:30
12:40
12:50
13:00
13:10
13:20
13:30
09:40
11:50
12:00
12:10
12:20
12:30
12:40
Name
path
path


apache_access
Include
Show logs
Name
Total
unknown
260
08/04
08/06
08/08
08/10
2025-08-08 12:44:04.233 192.168.1.145 - - [08/Aug/2025:12:44:04 +0530] "GET / HTTP/1.1" 200 2678 "-" "Mc
2025-08-08 12:43:04.080 192.168.1.145 - - [08/Aug/2025:12:43:04 +0530] "GET / HTTP/1.1" 200 2678 "-" "Mc
2025-08-08 12:42:04.167 192.168.1.145 - - [08/Aug/2025:12:42:04 +0530] "GET / HTTP/1.1" 200 2678 "-" "Mc
2025-08-08 12:41:04.258 192.168.1.145 - - [08/Aug/2025:12:41:04 +0530] "GET / HTTP/1.1" 200 2678 "-" "Mc
2025-08-08 12:40:04.095 192.168.1.145 - - [08/Aug/2025:12:40:03 +0530] "GET / HTTP/1.1" 200 2678 "-" "Mc
2025-08-08 12:39:04.170 192.168.1.145 - - [08/Aug/2025:12:39:03 +0530] "GET / HTTP/1.1" 200 2678 "-" "Mc
2025-08-08 12:38:04.007 192.168.1.145 - - [08/Aug/2025:12:38:03 +0530] "GET / HTTP/1.1" 200 2678 "-" "Mc
2025-08-08 12:37:04.085 192.168.1.145 - - [08/Aug/2025:12:37:03 +0530] "GET / HTTP/1.1" 200 2678 "-" "Mc
2025-08-08 12:36:04.179 192.168.1.145 - - [08/Aug/2025:12:36:03 +0530] "GET / HTTP/1.1" 200 2678 "-" "Mc


Home › Drilldown › Grafana Logs Drilldown
Search...
Labels
Give feedback
Filter by label values
Show logs
Data source
loki
Last 7 days
service
Add label
service
Search values
Showing
8
of 8
mysql
Include
Show logs
Name
Total
unknown
519
08/04
08/06
08/08
08/10
2025-08-06 12:30:27.434 delete from patient where pemail='lol1@gmail.com';
2025-08-06 12:30:27.434 SET timestamp=1754463174;
2025-08-06 12:30:27.434 # Query_time: 0.002070 Lock_time: 0.000003 Rows_sent: 0 Rows_examined: 6
2025-08-06 12:30:27.434 # User@Host: sentinel[sentinel] @ [192.168.1.108] Id: 245
2025-08-06 12:30:27.434 # Time: 2025-08-06T06:52:54.544342Z
2025-08-06 12:30:27.434 select * from patient where pemail='lol1@gmail.com';
2025-08-06 12:30:27.434 SET timestamp=1754463174;
2025-08-06 12:30:27.434 # Query_time: 0.000379 Lock_time: 0.000004 Rows_sent: 1 Rows_examined: 6
2025-08-06 12:30:27.434 # User@Host: sentinel[sentinel] @ [192.168.1.108] Id: 244


prtg
Include
Show logs
Name
Total
unknown
100 K
info
11.0 K
warn
22
error
230
08/04
08/06
08/08
08/10
2025-08-08 14:48:07.446 2025-08-08 09:18:07.407776 PaeAdvLog::addSubContext(StacktraceProvider)
2025-08-08 14:48:07.446 2025-08-08 09:18:07.421599 >>> PaeAdvLog::addSubContext(): Subcontext already ex
2025-08-08 14:45:13.055 2025-08-08 09:15:13.037485 ERRR TId 3000 ProbeSnmpWrapper> 0 sess_synch_respc
2025-08-08 14:45:08.270 2025-08-08 09:15:08.021806 ERRR TId 3000 ProbeSnmpWrapper> 0 sess_synch_respc
2025-08-08 14:45:03.245 2025-08-08 09:15:03.006711 ERRR TId 3000 ProbeSnmpWrapper> 0 sess_synch_respc
2025-08-08 14:44:25.257 2025-08-08 09:14:25.069063 ERRR TId 304 ProbeSnmpWrapper> 0 sess_synch_respc
2025-08-08 14:44:20.231 2025-08-08 09:14:20.053792 ERRR TId 304 ProbeSnmpWrapper> 0 sess_synch_respc
2025-08-08 14:44:15.207 2025-08-08 09:14:15.037971 ERRR TId 304 ProbeSnmpWrapper> 0 sess_synch_respc
2025-08-08 14:44:13.199 2025-08-08 09:14:13.053618 ERRR TId 2580 ProbeSnmpWrapper> 0 sess_synch_respc

4.6 Telegram Notification



5. CONCLUSION

5.1 Conclusion

In this project, we have successfully designed and deployed a robust, automated, and real-time network monitoring and intrusion detection system integrating multiple open-source and cloud-based tools. By leveraging AWS EC2 for scalable infrastructure, Docker for containerized deployment, and Jenkins with Git for CI/CD, we ensured streamlined development and automated updates. The combination of Snort IDS for packet inspection, Nagios for infrastructure health monitoring, and centralized logging provided by Loki/Grafana enabled comprehensive visibility into system activities. Furthermore, the integration of Telegram bots and email notifications ensured immediate alerts for potential threats or performance issues, significantly reducing incident response time. This end-to-end implementation not only strengthens the organization's security posture but also automates operational workflows, making the system resilient, scalable, and easy to maintain.

5.2 Future Scope

In the future, this system can be expanded to handle enterprise-scale deployments with high-volume traffic and multi-region AWS infrastructure. Advanced machine learning-based anomaly detection models can be integrated to detect zero-day threats and adapt to evolving attack patterns.

Support for automated incident response can be added, where detected threats trigger predefined mitigation actions (e.g., blocking IPs, isolating servers). Kubernetes orchestration could replace standalone Docker containers for better scalability and self-healing capabilities.

Additionally, integration with threat intelligence feeds would enhance Snort's detection accuracy, and extending the alerting system to include Slack, Microsoft Teams, or SMS gateways would provide even broader real-time communication coverage. Over time, the system could evolve into a fully autonomous Security Operations Center (SOC) framework capable of proactive defense, continuous compliance monitoring, and predictive analytics.

REFERENCES

Paper 1: - VINEVI: A Virtualized Network Vision Architecture for Smart Monitoring of Heterogeneous Applications and Infrastructures

Author: Rodrigo Moreira, Hugo G. V. O. da Cunha, Larissa F. Rodrigues Moreira, Flávio de Oliveira Silva

Paper 2: P4-NIDS: High-Performance Network Monitoring and Intrusion Detection in P4

Author: aying Chen, Siamak Layeghy, Liam Daly Manocchio, Marius Portmann

Paper 3: - Research and Build Cloud Servers Using Suricata to Detect and Respond to Cybersecurity Threats

Author: James Rebert, Poppy James, Victor Ogunrinde