

# EASTERN INTERNATIONAL UNIVERSITY

**SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY**

## DEPARTMENT OF COMPUTER NETWORKS AND DATA COMMUNICATIONS

**CSE 420**

**INTERNSHIP PROJECT REPORT**

Integrated System Management: Combining Local Networks and Cloud Platforms

**Students**

**HA QUANG MINH** - 1931220012

**Supervisor**

**DR**. **PHAN VAN VINH**

**Binh Duong, SEPTEMBER , 2025**

EASTERN INTERNATIONAL UNIVERSITY

## SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY



# PROJECT EVALUATION FORM

### General information

* Project title: Integrated System Management: Combining Local Networks and Cloud Platforms
* Student name and ID:
  + **HA QUANG MINH - 1931220012**
* Supervisor name: **Dr. Phan Van Vinh**

### Descriptive comments

* 1. *Presentation (layout, format, style, confidence)*

This report has been written with good layout and format effectively.

* 1. *Content (Originality and contribution)*

The content of this report has satisfied the requirement of the first project.

* 1. *Outcome (Creativity and practice)*

This project has good achievements and expected outcomes.

* 1. *Performance during questions and answers*

During the time of this project, these student have shown there strong interest and good working attitude to complete the requirements of the project.

### Suggestion for improvement

Need to enhance the web interface design and database dessign to get better performance in data visualization.

**Total Score: …/100 Binh Duong, Date:**

**Phan Van Vinh**

# ABSTRACT

This report is about finding out how to mix local network tools with cloud services in a basic IT system. I mainly worked with **pfSense** for firewall and routing, where I tried basic setups like assigning IP addresses, creating firewall rules, and enabling DHCP. For monitoring, I used **Zabbix** with **Grafana** to track CPU, bandwidth, and uptime, and to build simple dashboards. On the cloud side, I tested free-tier services from **AWS, Google Cloud, and Microsoft Azure**, where I created small virtual machines and practiced adjusting basic security rules.

To make things more like a real-life situation, I created a small mixed setup with a pretend client called Athena. Since I didn’t have access to real company systems, I learned mainly by researching and building practice labs. Although I didn’t get to fully put the system into action, this project showed me a lot about how to organize IT systems using both local hardware and cloud platforms, this experience gave me a clear view of how system management can be planned in both local and cloud contexts **[1], [2].**

# ACKNOWLEDGEMENT

I want to thank my supervisor, Dr. Phan Van Vinh, for his support and advice throughout my internship. His feedback helped me stay on track with my research and practice. I’m also thankful to the School of Computing and Information Technology at **Eastern International University** for letting me do this project and for providing the resources I needed.

I appreciate my classmates and friends as well, who shared ideas with me and helped me test out lab setups on my own computer. Even though this project isn’t perfect, working on it was a valuable experience for me, and I’m grateful for all the help and encouragement I got along the way.

# TABLE OF CONTENTS

Contents

[EASTERN INTERNATIONAL UNIVERSITY 1](#_Toc207777318)

[DEPARTMENT OF COMPUTER NETWORKS AND DATA COMMUNICATIONS 1](#_Toc207777319)

[SCHOOL OF COMPUTING AND INFORMATION TECHNOLOGY 2](#_Toc207777320)

[PROJECT EVALUATION FORM 2](#_Toc207777321)

[1. General information 2](#_Toc207777322)

[2. Descriptive comments 2](#_Toc207777323)

[3. Suggestion for improvement 2](#_Toc207777324)

[ABSTRACT 1](#_Toc207777325)

[ACKNOWLEDGEMENT 2](#_Toc207777326)

[TABLE OF CONTENTS 3](#_Toc207777327)

[LIST OF FIGURES 4](#_Toc207777328)

[LIST OF ABBREVIATIONS 5](#_Toc207777329)

[CHAPTER 1 : INTRODUCTION 6](#_Toc207777330)

[1.1 Background and Motivation 6](#_Toc207777331)

[1.2 Problem statement 6](#_Toc207777332)

[1.3 Objectives 7](#_Toc207777333)

[1.4 Scope & Limitations 7](#_Toc207777334)

[CHAPTER 2 : TOOLS AND TECHNOLOGIES OVERVIEW 9](#_Toc207777335)

[2.1 pfSense 9](#_Toc207777336)

[2.2 Zabbix and Grafana 9](#_Toc207777337)

[2.3 Cloud Platforms (AWS, Google Cloud, Microsoft Azure) 10](#_Toc207777338)

[2.5 Vmware Workstation 11](#_Toc207777339)

[CHAPTER 3: METHODOLOGY 13](#_Toc207777340)

[3.1 Research Process 13](#_Toc207777341)

[3.2 Lab Setup Using VMware 13](#_Toc207777342)

[3.3 Network Simulation with Packet Tracer 13](#_Toc207777343)

[3.4 pfSense Configuration 14](#_Toc207777344)

[3.5 Zabbix and Grafana Integration 14](#_Toc207777345)

[3.6 Exploring Cloud Platforms 14](#_Toc207777346)

[3.7 Summary of Approach 15](#_Toc207777347)

[CHAPTER 4 : SYSTEM DESIGN AND ANALYSIS 16](#_Toc207777348)

[4.1 Assumed Requirements of Athena 16](#_Toc207777349)

[4.2 Proposed Hybrid System Architecture 16](#_Toc207777350)

[4.3 Network Design Diagram 17](#_Toc207777351)

[4.4 Summary of Tools and Their Roles 18](#_Toc207777352)

[4.5 Notes on Practicality 18](#_Toc207777353)

[CHAPTER 5: RESULTS AND DISCUSSION 19](#_Toc207777354)

[5.1 What Was Done 19](#_Toc207777355)

[5.2 What Worked and What Didn’t 19](#_Toc207777356)

[5.3 Lessons learned 19](#_Toc207777357)

[5.4 Challenges Faced 20](#_Toc207777358)

[CHAPTER 6: CONCLUSION AND FUTURE WORK 21](#_Toc207777359)

[6.1 Conclusion 21](#_Toc207777360)

[6.2 Recommendations 21](#_Toc207777361)

[6.3 Future Work 21](#_Toc207777362)

[REFERENCES 22](#_Toc207777363)

# LIST OF FIGURES

[Figure 1: Local Network Diagram 6](#_Toc207777364)

[Figure 2: pfSense VM 8](#_Toc207777365)

[Figure 3: Setup a small lab from Athena 8](#_Toc207777366)

[Figure 4: Firewall rules on pfSense 9](#_Toc207777367)

[Figure 5: The interface Zaabix 10](#_Toc207777368)

[Figure 6: The interface Grafana 10](#_Toc207777369)

[Figure 7: AWS tests 11](#_Toc207777370)

[Figure 8: Microsolf Azure Experiment 11](#_Toc207777371)

[Figure 9: Vmware ruuning 12](#_Toc207777372)

[Figure 10: Athena Hybrid Network Diagram 14](#_Toc207777373)

[Figure 11: Creating a new user 15](#_Toc207777374)

[Figure 12: Hybrid Architecture 17](#_Toc207777375)

# LIST OF ABBREVIATIONS

|  |  |
| --- | --- |
| **Abbreviation** | **Meaning** |
| AWS | Amazon Web Services |
| GCP | Google Cloud Platform |
| Azure | Microsoft Azure |
| pfSense | An open-source firewall/router software |
| Zabbix | A monitoring tool for IT infrastructure |
| Grafana | A tool for visualizing metrics & logs |
| VM | Virtual Machine |
| LAN | Local Area Network |
| IP | Internet Protocol |
| DNS | Domain Name System |
| NAT | Network Address Translation |
| GUI | Graphical User Interface |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# CHAPTER 1 : INTRODUCTION

## 1.1 Background and Motivation

These days, most companies no longer rely only on their own servers. Instead, they use a hybrid setup where some parts of their IT are on local machines, and others are on the cloud. This approach gives more flexibility, but also creates new issues, especially for monitoring, configuration, and security **[1], [2].**

During my internship, I wanted to see how different tools could work together in this kind of environment. I mainly used pfSense for firewalls and routing, Zabbix and Grafana for monitoring, and I tested free options from AWS, Google Cloud, and Microsoft Azure. My goal was simply to get real-world experience with these tools and understand how they can be used in a basic hybrid setup, not to become an expert.

A diagram of cloud computing

Description automatically generated

Figure 1: Local Network Diagram

## 1.2 Problem statement

A common challenge for many small and medium-sized businesses is that their IT systems can be **difficult to monitor and manage**. While there are tools available, choosing the right ones and integrating them effectively is often unclear. Small teams with limited budgets or expertise frequently find it hard to keep an overview of both their local and cloud environments **[3].**

To tackle this in a straightforward way, I created a simulated client named Athena to represent a medium-sized business. Using Athena’s basic requirements, this project suggests a simple **hybrid model** that links local network tools with cloud services, aiming to create a system that is easier to manage and maintain.

## 1.3 Objectives

The project was never intended to create a fully operational system. Instead, its main goal was to learn the fundamentals and understand how various tools can be combined. The key objectives included:

* Gaining hands-on experience with local network management by using pfSense for routing and firewall, along with Zabbix and Grafana for monitoring **[1].**
* Exploring the essential features of cloud platforms by experimenting with AWS, Google Cloud, and Microsoft Azure for small-scale setups **[2].**
* Building small-scale simulations using Cisco Packet Tracer and VMware to create a test environment resembling a real business scenario.
* Designing a simple hybrid model to propose a basic system management approach suitable for small or medium-sized companies like Athena.

By the end of the project, the goal was not to become an expert, but to have a clearer picture of how local and cloud systems can fit together for SMEs.

## 1.4 Scope & Limitations

This project was mainly research-based, supported by several small lab simulations done on my personal computer. The primary goal was to understand how the tools function rather than build a system ready for production use.

* + - **Scope :**
    - Learn and experiment with open-source tools like **pfSense, Zabbix, and Grafana,** and practice network scenarios using Packet Tracer.
    - Explore basic features of cloud platforms such as **AWS, Google Cloud, and Azure** through free-tier accounts.
    - Setup a small lab environment on my laptop using **VMware** to mimic real-world conditions as closely as possible.
    - Analyze the requirements of a simulated SME client named Athena and propose a high-level hybrid model that integrates local and cloud tools.
      * **Limitations:**
      * No direct access to real company infrastructure, so all environments had to be recreated in the lab.
      * Cloud usage was limited to **free-tier services**, restricting the scope of testing.
      * Security enhancements and performance testing were beyond the project’s scope due to limited resources and access.

A screenshot of a computer

Description automatically generated

Figure 2: pfSense VM

A diagram of a router

Description automatically generated

Figure 3: Setup a small lab from Athena

# CHAPTER 2 : TOOLS AND TECHNOLOGIES OVERVIEW

This chapter summarizes the main tools and platforms used during my internship. Since the focus was on learning rather than creating a large system, I explored each tool with basic, hands-on practice. Most were tested in a VMware lab setup or through free-tier cloud accounts.

## 2.1 pfSense

**pfSense** is a popular open-source firewall and router system commonly used in small and medium business networks **[4]**. It supports routing, NAT, VPN, and firewall rules.  
In this project, I installed pfSense as a virtual machine on VMware Workstation. I practiced tasks such as assigning static IP addresses, setting up port forwarding, and creating simple firewall rules. The aim was not advanced security, but to learn how pfSense can serve as the main control point in a local network.

A screenshot of a computer

Description automatically generated

Figure 4: Firewall rules on pfSense

## 2.2 Zabbix and Grafana

**Zabbix** is an open-source monitoring tool that collects data on system performance like CPU usage, memory, and network traffic **[5].** Grafana is a visualization platform that works with Zabbix to display the data in clear dashboards **[6]**

I set up a small **Zabbix server** on a VM and connected it to pfSense for monitoring. Then, **Grafana** was linked to **Zabbix** to display real-time charts of CPU and network activity. Though a small setup, it demonstrated how monitoring tools help IT teams maintain system control.

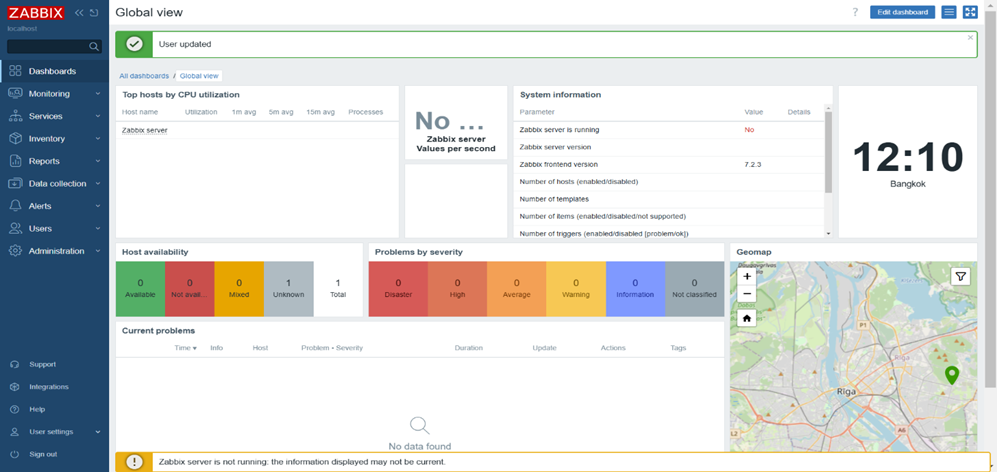


Figure 5: The interface Zaabix

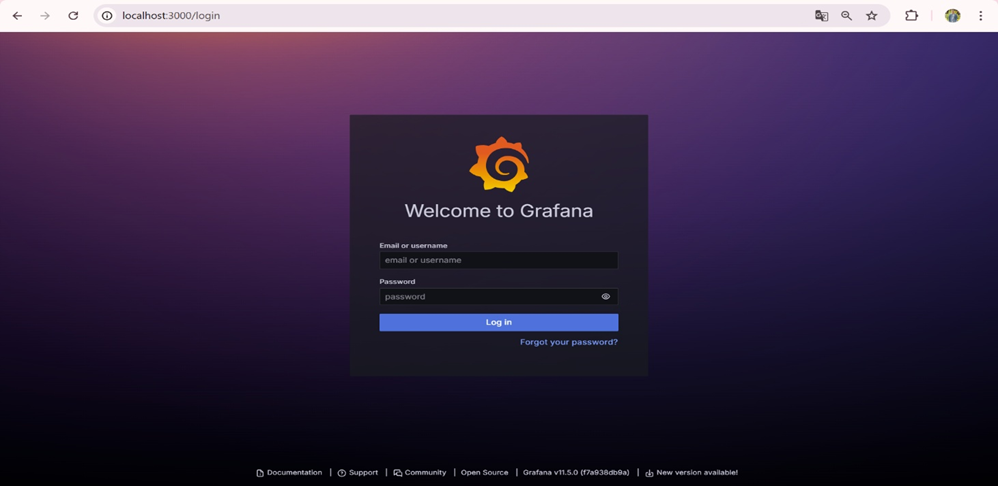


Figure 6: The interface Grafana

## 2.3 Cloud Platforms (AWS, Google Cloud, Microsoft Azure)

AWS, Google Cloud Platform (GCP), and Microsoft Azure are leading cloud providers offering compute, storage, networking, and monitoring services **[7].**

For this project, I created free-tier accounts on each platform to compare their dashboards, explore virtual network setups, and test basic monitoring features. The goal was to understand usability differences and find a good fit for the simulated client, Athena.

A screenshot of a computer

Description automatically generated

Figure 7: AWS tests

A screenshot of a computer

Description automatically generated

Figure 8: Microsolf Azure Experiment

## 2.5 Vmware Workstation

**VMware Workstation** is a virtualization tool that allows running multiple operating systems on one physical computer **[8].**

I used VMware to build my lab environment, running pfSense, Zabbix, Grafana, and a client-server test setup together without affecting my main system. This enabled me to simulate a small business network entirely on my laptop.

A screenshot of a computer

Description automatically generated

Figure 9: Vmware ruuning

# CHAPTER 3: METHODOLOGY

This chapter outlines the step-by-step approach I used during the internship project. Since the focus was on learning and testing, I combined research with small lab simulations on my laptop.

## 3.1 Research Process

At the start, I spent time studying books, documentation, and tutorials to build a solid foundation. My research covered how pfSense **[4]** works as a firewall and router , how Zabbix and Grafana **[5], [6]** manage system monitoring , , the core features of cloud platforms **[2]** like AWS, GCP, and Azure , as well as general ideas about hybrid IT infrastructure **[3].**

This preparation gave me a clear overview before starting lab configurations

## 3.2 Lab Setup Using VMware

After researching, I built a small lab environment with VMware Workstation **[8]** on my personal laptop. The setup included a VM running pfSense as firewall/gateway, a Zabbix server on Ubuntu, and a client VM to generate test traffic. All the VMs were connected via a virtual network, enabling me to test routing, firewall rules, and monitoring as a single system.

## 3.3 Network Simulation with Packet Tracer

Before setting up the VMs, I used Cisco Packet Tracer to design the network for the simulated client Athena. This helped me plan IP addressing, where to place firewalls and servers, and how to separate internal and external zones. Though Packet Tracer doesn’t provide real performance tests, it was useful to visualize the system design.

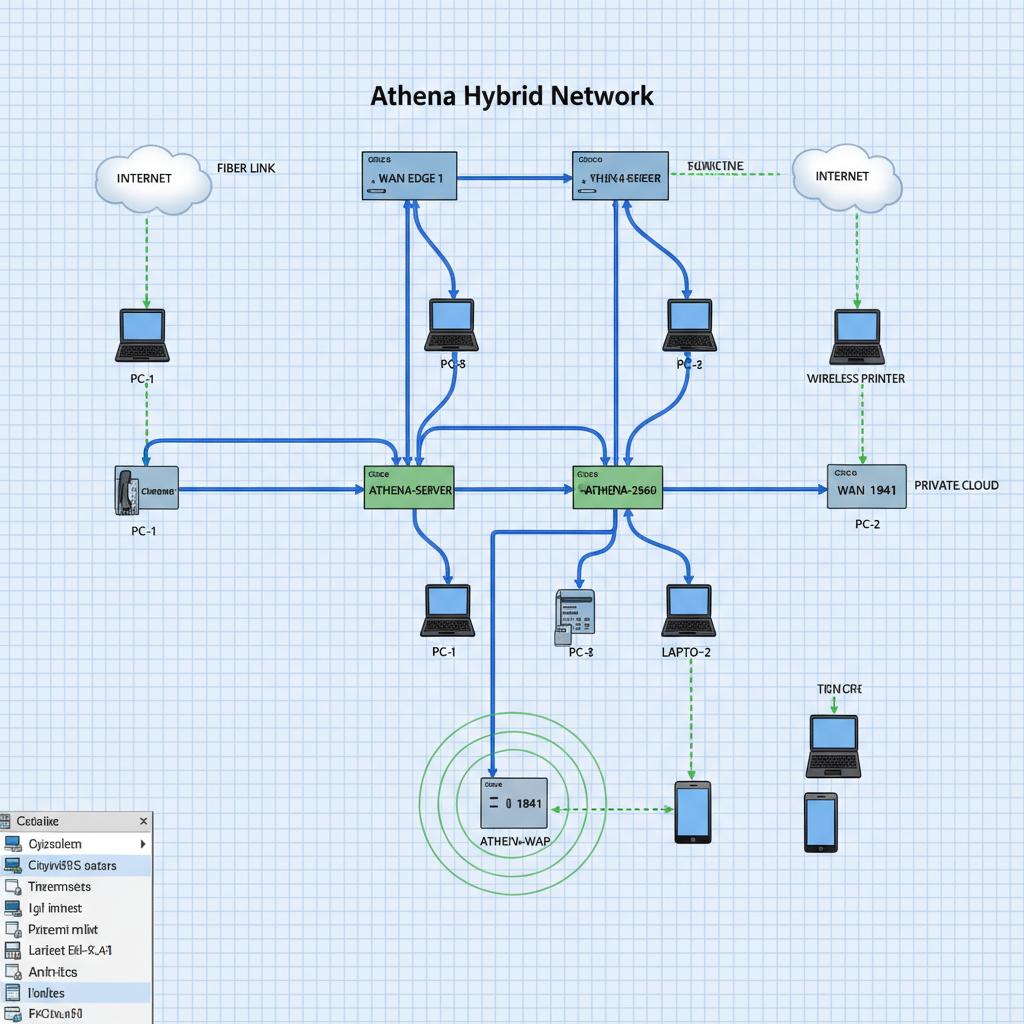


Figure 10: Athena Hybrid Network Diagram

## 3.4 pfSense Configuration

In pfSense, I practiced several important configurations:

* **Assigning static IPs** for WAN (e.g., 192.168.74.158) and LAN (e.g., 192.168.1.5).
* **Enabling DHCP** on the LAN interface so that client VMs could automatically receive IPs in a range I defined (192.168.10.100–192.168.10.200).
* **Creating firewall rules**: for example, allowing HTTP/HTTPS but blocking ICMP (ping) to test filtering.
* **Setting up NAT and port forwarding**: I redirected traffic from the WAN port 8080 to the internal client’s port 80, which allowed me to test web service access.

These activities showed how pfSense can act as the **central control point** for traffic in a small business network.

[📷 Insert Figure: pfSense Firewall Rules tab – showing allow/deny rules]  
[📷 Insert Figure: pfSense DHCP Server configuration page]  
[📷 Insert Figure: pfSense NAT Port Forward rule]

## 3.5 Zabbix and Grafana Integration

Next, I set up **Zabbix** on an Ubuntu VM and added both pfSense and a client VM as monitored hosts. The metrics I tracked included:

* CPU usage of the firewall VM,
* network bandwidth (incoming/outgoing),
* and uptime status of the client VM.

After this, I installed the **Grafana Zabbix plugin** and connected Grafana to Zabbix. I created simple dashboards with panels showing CPU load, memory usage, and network graphs. Even though this was a small setup, it made the monitoring results much clearer and closer to what IT managers would expect to see **[5], [6].**

[📷 Insert Figure: Zabbix Latest Data page showing monitored metrics]  
[📷 Insert Figure: Grafana dashboard with CPU and bandwidth graphs]

## 3.6 Exploring Cloud Platforms

To cover the cloud aspect, I created trial accounts on AWS and Microsoft Azure. I experimented with launching basic VMs, configuring virtual network settings, and exploring monitoring tools such as AWS CloudWatch, Google Operations Suite, and Azure Monitor **[2].** Due to free-tier limitations, I couldn’t run full setups, but this comparison helped me see how the providers differ.

A screenshot of a computer

Description automatically generated

Figure : Creating a new user from Microsoft Azure

[📷 Insert Figure: AWS EC2 instance details page (showing VM info + status)]

## 3.7 Summary of Approach

The project followed a simple cycle:

* Study theory
* Build the lab with Vmware
* Test and analyze what worked and what didn’t

The aim was not deep technical deployment but to build an understanding of how local and cloud tools can connect in a small business scenario like Athena.

# CHAPTER 4 : SYSTEM DESIGN AND ANALYSIS

This chapter describes how I designed the system for the simulated company Athena. Since I didn’t have access to a real system, the requirements were based on typical needs of a mid-sized business. The goal was to propose a simple hybrid setup that combines local tools with cloud services, supported by small test environments and diagrams.

## 4.1 Assumed Requirements of Athena

For the design, I imagined Athena needing:

* Firewall and basic network segmentation
* Simple monitoring for servers and devices
* Secure internet access with NAT and port control
* Easy-to-understand dashboards for system status
* The ability to migrate some services to the cloud in the future

The solution should be low-cost, easy to manage, and suitable for a small IT team **[3].**

## 4.2 Proposed Hybrid System Architecture

Based on these requirements, I proposed a **hybrid model** that includes:

* **pfSense** as the main firewall and router in the local network **[4],**
* **Zabbix** and **Grafana** for monitoring and visualization **[5], [6]**
* **Cloud integration** (GCP/AWS/Azure) for:
  + Off-site log backups
  + Optional cloud-based VM for remote access or failover
  + Monitoring cloud-side resources if needed later **[2].**

This model allows Athena to keep core services local while starting to integrate cloud solutions gradually.

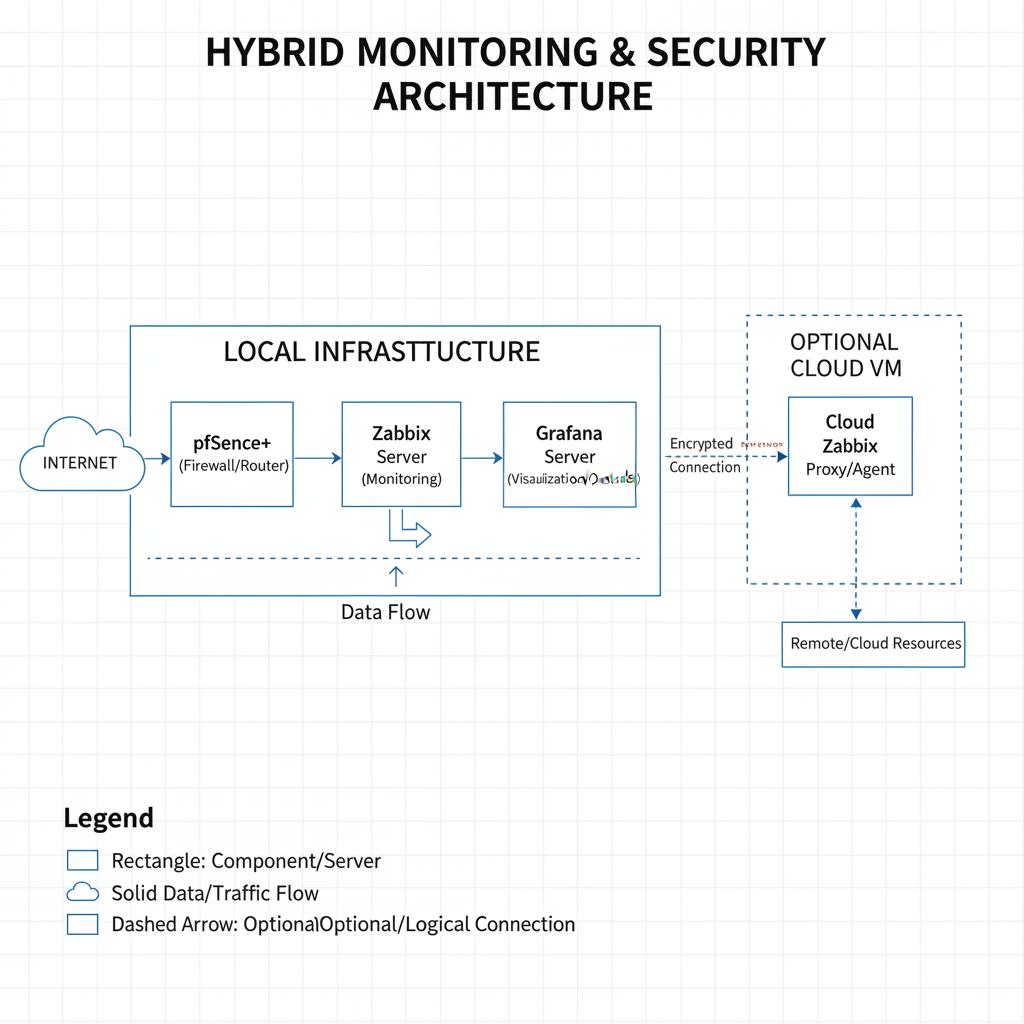
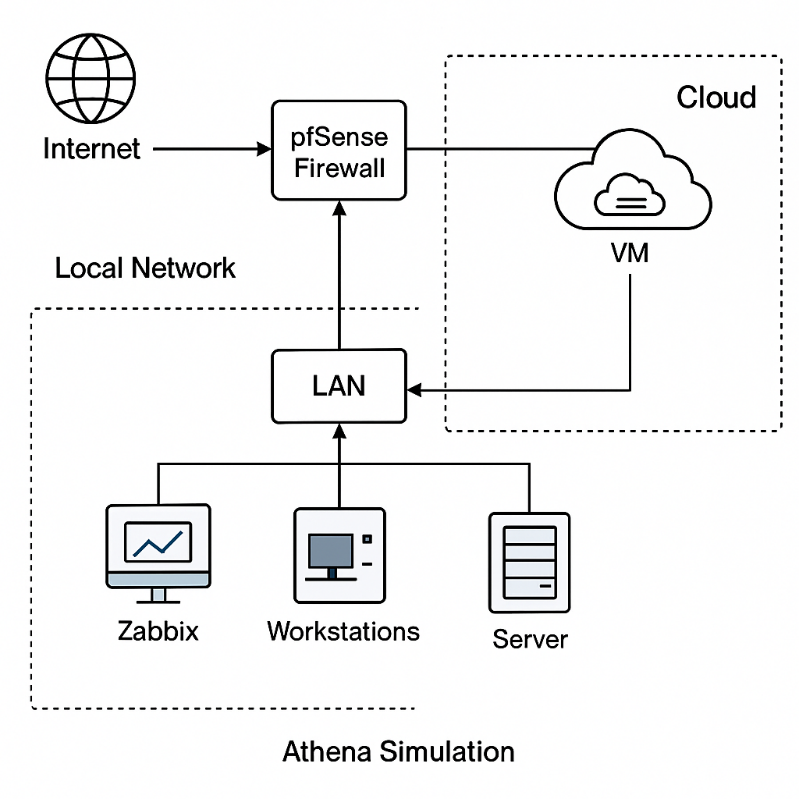


Figure 12: Hybrid Architecture

## 4.3 Network Design Diagram

To clarify the structure, I created a sample network diagram in **Cisco Packet Tracer** showing:

* A pfSense firewall between the internet and internal LAN
* A Zabbix server for monitoring internal systems
* Endpoints such as workstations and local servers
* And an **optional cloud VM** segment connected to the system



## 4.4 Summary of Tools and Their Roles

To measure the impact of the applied methodology, we define several evaluation criteria:

|  |  |
| --- | --- |
| **Tool** | **Role in the System** |
| PfSense | Firewall, routing, NAT, and port rules |
| Zabbix | Monitoring of system performance |
| Grafana | Visual dashboard for Zabbix data |
| Packet Tracer | Network design and planning |
| Vmware | Virtual lab environment |
| GCP / AWS / Azure | Optional cloud services (backup, VM) |

Each tool was tested or studied at a basic level to understand how it could support the proposed architecture.

## 4.5 Notes on Practicality

This model is not meant for production but as a learning example. Some features like cloud backups or deeper system integration were not implemented due to time and resource limits. Still, designing this system showed how different tools can work together, even on a small scale.

# CHAPTER 5: RESULTS AND DISCUSSION

This chapter reviews what I achieved during the internship, including successes, challenges, and key lessons learned. Since the project was mostly research-focused with small lab tests, the results are more about personal growth than production-ready outcomes.

## 5.1 What Was Done

During the internship, I was able to:

* Study how pfSense, Zabbix, and Grafana work in system management **[4–6]**
* Set up a virtual lab on VMware including pfSense firewall, a Zabbix server, and a client VM to generate traffic
* Athena’s network using Cisco Packet Tracer
* Explore basic features of AWS, GCP, and Azure **[2]**
* Create a Grafana dashboard linked to Zabbix data
* Propose a hybrid system architecture combining local and cloud services

All of these activities were done at a beginner level and were mainly focused on learning rather than deep technical implementation.

## 5.2 What Worked and What Didn’t

**What worked well:**

* pfSense setup and basic firewall rules within the Vmware lab.
* Zabbix monitoring between virtual machines
* Grafana dashboards for data visualization
* Network diagram design using Packet Tracer for Athena
* Comparing the interfaces of AWS, GCP, and Azure.

**What was limited or did not work::**

* Free-tier cloud accounts restricted advanced testing
* Zabbix configuration was sometimes complicated and required troubleshooting.
* Some integration ideas, such as remote logging to the cloud, were not completed due to time and resource limitations.

## 5.3 Lessons learned

* System management involves not just tools but also planning based on business needs **[3].**
* Even small lab setups provide valuable insights on how tools connect.
* pfSense is powerful but takes time and patience to master.
* Zabbix and Grafana work well together, though their setup can be complex.
* Cloud platforms share similarities but each handles networking and resources in unique ways **[2].**
* Creating diagrams early helped avoid confusion during implementation.

## 5.4 Challenges Faced

* Limited hardware: My personal laptop (8GB RAM) made it hard to run many VMs at once.
* Learning curve: Tools like Zabbix and pfSense had many settings and required time to learn.
* Time management: Balancing between learning theory and doing hands-on tasks was sometimes difficult.
* No real company access: Since Athena was a simulated client, all assumptions had to be made without real data.

# CHAPTER 6: CONCLUSION AND FUTURE WORK

## 6.1 Conclusion

This internship gave me the chance to learn the basics of system and network management using both local tools and cloud platforms. Most of the work involved small labs and simulations, through which I was able to:

* Understand key functions of pfSense as a firewall and route **[4].**
* Learn how Zabbix and Grafana work together for monitoring and visualization **[5], [6].**
* Explore networking concepts on cloud platforms like AWS, GCP, and Azure **[2].**
* Design a simple hybrid architecture for a simulated company (Athena).
* Practice using tools like VMware and Cisco Packet Tracer to test ideas in a safe environment.

Although the project did not involve real production deployment, it highlighted the importance of planning, visibility, and monitoring in IT systems. Overall, I gained a clearer understanding of how local and cloud tools can complement each other.

## 6.2 Recommendations

For students taking on similar internship projects, my advice is:

* Start with simple goals and build up gradually.
* Spend time reading official documentation — it really helps.
* Use diagrams to organize your ideas before building anything.
* Don’t worry about mastering every feature — focus on understanding the basics first.
* Use free-tier cloud services wisely to avoid unexpected charges.

## 6.3 Future Work

With more time and resources, I would like to:

* Explore automation tools like **Ansible** or **Terraform** to simplify system configuration.
* Try integrating cloud monitoring services (e.g., AWS CloudWatch) with local tools like Zabbix.
* Build a more complete demo that includes real-time alerting and log management.
* Study more about **network security**, including VPN, IDS/IPS, and zero-trust models.
* Combine this internship knowledge with future Capstone projects to build a more advanced system.

# REFERENCES

**[1]** A. Tanenbaum and D. Wetherall, *Computer Networks*, 5th ed. Pearson, 2010

<http://inf.ufsc.br/~bosco.sobral/ensino/ine5645/Computer-Networks---A-Tanenbaum---5th-edition.pdf>

**[2]** T. Erl, R. Puttini, and Z. Mahmood, *Cloud Computing: Concepts, Technology & Architecture*. Prentice Hall, 2013.

<https://ptgmedia.pearsoncmg.com/images/9780133387520/samplepages/0133387526.pdf>

**[3]** W. Stallings, *Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud*. Addison-Wesley, 2016.

<https://ptgmedia.pearsoncmg.com/images/9780134175393/samplepages/9780134175393.pdf>

**[4]** C. Buechler and J. C. Schneider, *pfSense: The Definitive Guide*. Reed Media Services, 2009.

<https://rom.lv/pfsense/pfSense_%20The%20Definitive%20Guide%20Version%202.1.pdf>   
**[5]** R. Pavlov, *Zabbix 6 IT Infrastructure Monitoring Cookbook*. Packt Publishing, 2022.

<https://github.com/PacktPublishing/Zabbix-6-IT-Infrastructure-Monitoring-Cookbook>   
**[6]** Grafana Labs, *The Art of Monitoring with Grafana*. Grafana Labs, 2021.

<https://grafana.com/tutorials/>   
**[8]** VMware, *VMware Workstation Pro Documentation*, 2023.

<https://www.vmware.com/docs/vmware-product-guide-december-2023>