Thesis Report



Name: Umair Ahmad

Student ID: N0955729

**Declaration**

I hereby declare that I am the sole author of this report. I authorize Nottingham Trent University to lend this report to other institutions or individuals for the purpose of scholarly research.

I also authorize the Nottingham Trent University to reproduce this report by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.



Signature:



Umair Ahmad

**Abstract**

In current times where more business are moving towards online solutions and many small to medium scale companies are working to increase their productivity and further expand their business but also need a secure network of protect their assets and development secrets. As these assets are very important and their businesses are solely depending on privacy of their products and creations. If their plans are reviled to other companies or competitors, they can replicate them similarly if destroyed can also cause a major setback. Hence these businesses need to maintain a decent level of security of internal and external networks.

This project purposes a fairly decent network design that can help small scale companies to protect their assets from intruders and prevent any data loss and isolate different departments or groups to certain limits. Some controls will be placed like firewall, IPS and data loss prevention that will help keep checks on everyone and only allow access to resources that they need and keep private information safe and also if an intruder penetrate the network, he cannot access all the information.

This solution was created for BYG systems, but it can be adopted by other companies to suit their needs with modifications according to their assets. Further work and development is also possible to enhance the network.

**Acknowledgement**

I would like to thank Dr. Nigel King for his continuous support and advice during the completion of this project. I would also like to thank my father and my cousin Jawad Mehdi for the encouragement, motivation, and emotional support they have provided during this period.

Contents

[Chapter 1: Introduction 7](#_Toc113029495)

[**1.1 Introduction** 7](#_Toc113029496)

[**1.2 Reason of project:** 8](#_Toc113029497)

[**1.3 Aims and Objectives:** 8](#_Toc113029498)

[**1.3.1Objectives** 8](#_Toc113029499)

[Chapter 2 Planning 9](#_Toc113029500)

[**2.1 Introduction** 9](#_Toc113029501)

[**2.2 Tasks** 9](#_Toc113029502)

[**2.3 Resources** 9](#_Toc113029503)

[**2.3.1 Diagramming tools** 9](#_Toc113029504)

[**2.3.2 Monitoring tools and firewall** 9](#_Toc113029505)

[**2.3.3 Virtual environment** 10](#_Toc113029506)

[**2.4 Project Risks** 10](#_Toc113029507)

[**2.5 Professional Issues** 11](#_Toc113029508)

[**2.6 Time Plan** 11](#_Toc113029509)

[Chapter 3 Literature Survey 12](#_Toc113029510)

[**3.1 Introduction** 12](#_Toc113029511)

[**3.2 Principles of secure design** 12](#_Toc113029512)

[**3.3 Information security Classification** 15](#_Toc113029513)

[**3.4 Network segmentation, IPS and firewall** 16](#_Toc113029514)

[**3.5 Conclusion** 17](#_Toc113029515)

[Chapter 4 Designing, Testing and Recommendation 18](#_Toc113029516)

[**4.1 Introduction** 18](#_Toc113029517)

[**4.2 Methodology** 18](#_Toc113029518)

[**4.3 Company Assets** 18](#_Toc113029519)

[**4.4 Information security classification** 19](#_Toc113029520)

[**4.5 Risk Classification** 19](#_Toc113029521)

[**4.6 Classification Table** 20](#_Toc113029522)

[**4.11 Network Diagram** 35](#_Toc113029523)

[**Chapter 5 Conclusion & Future work** 39](#_Toc113029524)

# Chapter 1: Introduction

## **1.1 Introduction**

Computer networks are a backbone of modern-day communications whether it is a simple email or sharing resources like storage, printer etc. (Kizza, 2005) defines computer network as a distributed system consisting of computers that are interconnected through a medium. It can be wired or wireless depending on your needs. Security is a very important aspect of networks. As networks allow to access multiple devices across the globe or different locations it is important to place controls that allow only authorized personals to access the network. To protect networks from unauthorized access many techniques and controls were developed and put in place to ensure the safety of all. Due to advancement of knowledge and research many techniques were made as a standard to uphold a certain level of security with the option to add more should the need arise. In 1960s when networks were rapidly spreading, governments, military and public sectors were establishing networks many incidents were witnessed where data was stolen, or system was rendered useless because of very little or no security at all. By 1980 the networks had spread across the entire world, and it was known as internet and as a result the threats rose to an exponential number. Government agencies worked with other users of network to develop CERT Computer Emergency Response Team to mitigate the threats and research way to prevent such attacks (radware.com). With the increase in technological advancement more sophisticated controls are being placed to strengthen the security of networks but here is a limit to how much security can be placed on existing networks. It is essential to take security controls in account when designing a network rather then design a network and then implement security when it comes under attack. According to (Patnaik, 2021) It is mandatory to consider the following when developing a secure network:

1. Confidentiality: Means that information should be held private
2. Integrity: Ensure that the data is correct, and no alterations has occurred.
3. Authentication: To verify that users are who they say they are.
4. Access: Only authorized users can have access to the resources.
5. Non-repudiation: Ensure that users can not deny the use of network.

Network security can be enhanced by assessing the company’s attack surface meaning that how many assets does the company has and what are the access points. Identifying the risks and then combining the security solutions to come up with a design to secure the assets based on their priority or likely hood of getting attacked is a good way to develop a strategy to counter any attacks against a network. As stated by (Dowd, McHenry, 1998) “With the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack an effective network security plan is developed.”

## **1.2 Reason of project:**

In the modern era of communication where computer are interconnected over the world and have instant access to resources, with this advancement comes some risks as well such as confidential information and information if leaked can cause privacy concerns. Similarly in an organization there is sensitive information and other resources that need to be kept confidential except for few position holders in a company. A secure network is needed to protect company network and resources from outside world and some controls inside the company to keep the valuable assets secured and prevent any unauthorized access.

The project is being developed for BYG Systems which is an e-learning company that creates e-learning solutions for companies and clients. They also design new learning materials and come up with fun ways to make the learning easy and fun. Many of its customers register and take courses to learn new skills. Since it is a small-scale company and does not have a secure network to protect its resources this design will provide a decent and very cost-effective solution.

## **1.3 Aims and Objectives:**

The aim of this project is to design a secure network that prevents intruder from access the resources and create and isolate network segment and prevent data loss with the help of several network security controls.

### **1.3.1Objectives**

* Identify the risks and classifying the assets on priority basis.
* To analyze and find the best principles to implement for secure network design.
* Implementation of Network segmentation
* Analysis of monitoring tools and use the ones best suited for our needs.
* Testing the network and provides its capabilities and limits.
* Preparing documentation and recommendation.

# Chapter 2 Planning

## **2.1 Introduction**

This chapter explains the tasks and how the design of network will be made and what steps are involved. The resources used and professional issue that may encounter during the development period also it lists timeline of start of the project and stages it goes through till end result is achieved.

## **2.2 Tasks**

* List down assets and resources and classify them.
* Design the actual network.
* Apply Network Segmentation
* Test IPS, firewall and data loss prevention tools in virtual environment and place them on appropriate places.
* Develop firewall and IPS rules.
* Provide the benefits and limits of the network design.

It is important to identify the resources we need to protect in order to place security controls. Dividing network into smaller junctions so that even one junction is penetrated other junctions remain unharmed and still keeping resources safe. Intrusion prevention and data loss prevention controls monitor the traffic and detect any unauthorized access and block it. Data loss prevention control ensures that data is not lost or misused. Firewall ensure that only specific requests are allowed into the network and others will be denied.

## **2.3 Resources**

In order to design the network and test its capabilities there are some sources that are required.

### **2.3.1 Diagramming tools**

I need to find and select the best diagramming tool or network mapper that will be used to show the entire network. It will be used to virtual lay down the entire network and test some degree of its connectivity and capabilities. Some tools even allow to place any controls and monitoring tools as well so it will be very useful.

### **2.3.2 Monitoring tools and firewall**

There are many monitoring tools available, but I need to keep in mind the ones best suited for small level organization and cost effective. Some tools may even combine the features of others so it can be helpful in cutting the cost. Incase of firewall it all depends on the rules, there is not much difference in capabilities of different vendors.

### **2.3.3 Virtual environment**

It will be very useful in testing the features and limits of tools and firewall rules we can attempt attacks and try to bypass the security checks to ensure that the controls are working the way we want them to.

## **2.4 Project Risks**

During the development of this project, we can assume some risks that can affect the outcome or cause the project completion to delay.

*Table 1: Shows the Project Risks*

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Description | Scale | Solution |
| Accidental damage to computer or loss of data | It is possible to get the system damaged or stollen which was being used to carry out the project. | Low | Keep back up in cloud or separate external hard drive to ensure nothing goes wrong. |
| Tools may not be compatible with network configuration or combination with other tools. | Some tools have some bugs or dependencies that can cause them to deteriorate or not perform as expected. | Medium | Gather as much information about them as possible and look for reviews before hand to avoid using such tools or find a fix for them to work. |
| Insufficient knowledge of the task | It is likely to encounter a situation I have very little knowledge of, and it may halt the progress. | Medium | In this case first discuss with supervisor and look for professionals or experts that have specialties in that area and ask for their advice. |
| Increased or additional requirements that are added later on | Client may add some additional requirement and making room for it during the project can disrupt the timeline. | Medium | Discuss with the supervisor and look into the details and adjust them accordingly. |

## **2.5 Professional Issues**

The project will be completed under the supervision of assigned supervisor and taking ethics legal issues into account, and it will be developed with software and information freely available. It will be used for academic purposes and provide recommendations with its limits and abilities.

## **2.6 Time Plan**

The project is divided into tasks and assigning time to each tasks helps devise a plan to complete them in time.

*Timeline, waterfall chart

Description automatically generatedFigure 1: Displays Gantt Chart*

# Chapter 3 Literature Survey

## **3.1 Introduction**

Internet is vast collection of networks in which millions of computers communicate using some set of rules also known as protocols. Internet is expanding steadily over the time (Mowery et al. 2002). Internet and networks we see today were created to connect different computers together to exchange information. By the time internet was open to public and being used widely some security related issues arise as well. When Internet was not developed security wasn’t the concern it was deemed necessary with information was being compromised. Networks are more vulnerable, furthermore all most common attacks originate from some part of networks and effect another network around the globe. Network security is one of the fastest growing fields in technology (Michael Wood, 2020). There is an ever-growing demand for development and implementation of secure networks. There are certain steps to bear in mind while designing a secure network. The first and crucial step is to follow the latest principles of secure design. Which includes identifying what we are trying to protect and from what. How to implement tools like IPS, IDS and configure a firewall. Another important point to remember is information security classification which means dividing information into groups and identify which data can be public means No risk if it is compromised and then official means low risk some personal or business information and then sensitive information which is confidential information like company records and all personal information which poses high risk if it is revealed. According to Bhaskaran There can be many techniques to design a secure network but it all depends on the organization and its needs. Network segmentation is a security measure in networks that divides the network into segments and enforces certain rules on each segment to restrict the access in case of a cyber-attack. It is safe to say that if a network designer includes all the steps while designing a network it will be very difficult for attackers to gain access and steal or compromise information. Security is all about adding more layers and make it difficult for attackers to reach the critical resources.

## **3.2 Principles of secure design**

The network architecture is constantly changing and evolving over the time. That means new technologies are being invented and being used in networks to make them secure, so it is crucial to incorporate the latest security principals while designing a network. Network protections are first barrier in protecting resources from outside threats like intruders, malicious code etc. for example use of firewalls, Intrusion detection and prevention system (IDS and IPS), and content control systems like anti-virus, anti-malware, and URL filtering. A combination of Hardware and software solutions should be used. While designing a network following IT fundamental security principles should be considered.

1. Defense in depth

This approach is based on multiple layers in order to keep the network secure. According to (Wood C. 1990) better protections is achieved by adding redundant controls to protect a single asset. For example, a nuclear power plant has a fence as on outer perimeter and then combination of sensors and concrete wall to protect power plant form an invasion. If outer fence is compromised the other defenses are still active a penetration is not successful. Defensive depth can be implemented with use of single redundant security measure or combination of different measures. It all depends on the situation and how controls are placed with strong knowledge of the system. (Stawowski M. 2007) suggests that protection of IT system is based on security layers. The following rules should be considered

* Layered protection

Security layers should be associated with each other so that if one layer is by passed the other catches on to it and generate alert.

* Defense in multiple places

Security controls should be placed strategically in the IT system rather than in one place. So, the attacker does not know what he will encounter and where.

* Defense through diversification

Safeguards put in place to protect the IT system should consist of different types for example if firewall is being used, they should come from different vendors to enhance the security of the network or IT system.

The defense in depth methods should be used with cautions as adding more layers and security controls can make the system complex. Management and maintenance are also going to be difficult and costly.

1. Weakest Link

According to Cisco the system security is only as effective or efficient as its weakest link. Which unfortunately points to humans as they are often the weakest link in the chain. According to (Sasse et al. 2001) it is widely known in psychology of cyber security that users are the weakest link rather than the computer systems. The users sometime lack the judgment necessary to prevent an attack form happening and that causes the entire network breach. (Yan Z. et al. 2018) adds that Kevin Mitnick one of the famous hackers offered an insider’s view when he testified in the congress saying that “The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure devices, and its money is wasted, because none of these measures addresses the weakest link in the security”. (Standage, 2002, p. 1)

(Pfleeger S. et al 2014) The security staff should be encouraged to use simple and fundamental process to protect themselves. Company should summarize the findings in social psychology about moral values and habit formations and then combine then into guideline for the staff to transform them into better security experts. (Stawowski M. 2007) adds that when designing a network Separation of duty and job rotation should be accounted for as it limits employee’s ability to neglects and break the policy of IT system. Separation of duty states that critical tasks or commands should be executed by two or more employees. And job rotation dictates that there should be rotation between important positions of employees. Attackers most often attack the weakest link in the network and if it secure then entire system is secure and could withstand many attacks.

1. Least privileges

This security principles states that only authorized users and programs can access the resource. Privileges are set of policies that determine whether an action can be performed or not. If a user or program attempts to access the assets a request is sent to resource monitor that checks the privileges against that program or user if they are given the authority, then request will pass otherwise it will be denied and they cannot access the information or resources. (Wood C. 1990) states that least privilege is a very powerful security principle it indicates that access to information, the ability to execute and other system privileges should be restricted only designated users are given the access. According to (Schneider, F.B. 2003) Every user and program must have minimum set of permissions required in order to complete a task. It limits the damage in case of an attack or mistake it also reduces the interactions with privileged programs to avoid unnecessary use of privileges.

(Jero et al. 2021) dictates that least privilege is a significant security-design principle, but it does not protect against all threats therefore it is important to consider what threat and risks it is designed to respond. When we apply principle of least privilege or PoLP to an operating system the permissions and capabilities of the system are limited. If an attacker gain access to system process it limits his scope for example if attacker hacks into car’s head unit, he is limited to it only and cannot access the car’s steering. But there are other threat models in which system is compromised like corrupt system integrity, export data or consuming resources without providing desired output. So, it is important to place other principles to avoid the situations where PoLP is not very useful.

## **3.3 Information security Classification**

Information security is an important part of network design. It is crucial to differentiate sensitive and general information. (Collared et al., 2017) defines the information security classification a traditional informatics security concept. According to (JTC, 2013) All assets should clearly be identified, and they should be owned by appointed part of the organization, Information should be classified in terms of its value and sensitivity to the organization. A set of security measures shall be placed according to organization’s classification scheme.

According to (Agrawal, C, 2007) An organization creates and stores a large amount information, and it needs to be accessed a number of employees and even other organizations. Therefore, it is important to highlight the information that needs to be protected ad what level of protection should be provided. Information security classification is based on level of sensitivity and its effect on the organization in case it is disclosed. Information security classification helps in deciding the level of security measure to protect the information. Information classification also consists of associated systems, recovery plans and operational procedures rather the just files and databases.

What classifications or title be used to identify the sensitivity of information. There are no specific rules about titles used as it depends entirely on the organization although they should clear so it’s easily understandable. Nottinghamshire County council uses three information security classifications.

* Public: This includes general information that is already known and there is no point in securing that.
* Official: This includes some degree of personal and business information
* Official-sensitive: This will include top secret information and more personal data and requires high level of security also referred to as confidential.

(Woodbury C,2007) defines Information classification as a process of determining the importance and value of information and then assigning to a category. Due to breaches and the disclosure of vital information organization across the globe realized the importance data or information thus increasingly classifying the data and taking measures to ensure the safety of information. When classifying data following rules apply

* Who can access data

Assign roles and privileges to people who can access the data and what level of access is granted to them. For example, HR managers can view phone numbers and related information of staff while accounting clerks can only view payable accounts.

* How data is secured

It defines whether data is generally available or off limits by default. Specified people have access to data, and they further have restrictions imposed. For example, some are only allowed to view the data while other can view and modify.

* Data need to be encrypted or not

It depends on the organization policies whether data needs to be encrypted or not. For example, payment card industry encrypts data as it contains very sensitive information about customers.

All these rules help in classifying information and develop company’s security policy.

## **3.4 Network segmentation, IPS and firewall**

As its name suggest segmentation means divide the network into smaller chunks known as segments. This security measure focuses on splitting and dispersing the asset. According to (Wagner et al., 2016) Network segmentation partitions the network to restrict access of attacker and prevent him from gaining access to valuable resources. Different software and hardware are placed to monitor and communicate between segments.

Intrusion Prevention System or IPS is a protection measure that helps ward off intrusions. It can be a software or hardware. These products are used to continuously monitor the network and detect any attack and block the attackers (Daya B, 2013).

Firewalls is very important and recommended security measures while a designing any network that needs decent security. But as stated by (Lyu, and Lau, 2000) seeking a firewall and setting it up is not a fancy thing rather than the set of rules and policy are what make the firewall a truly secure measure. On a large-scale performance of firewall may affect the system so it is wise to choose a product that suits the company criteria.

## **3.5 Conclusion**

Secure network design and development includes all the aspects discussed above. A secure and efficient network is balanced where it is easy to manage and maintain. First step is to design a secure network and implement it then constantly make if more efficient. A combination of different controls and good design can lead to a secure network able to withstand attacks and prevent any intruders to infiltrate. It is evident that threats will continue to evolve and someday bypass the security measures but so is the network security.

# Chapter 4 Designing, Testing and Recommendation

## **4.1 Introduction**

This chapter will explain the designing phase of the purposed secure network and also describe the limits and capabilities of the network design. Security controls will also be discussed that are used to provide security and demonstrate their working in virtual environments. Firewalls will be used to prevent filter the traffic and IPS (Intrusion prevention System) to prevent malicious traffic to enter the network. Data loss prevention system is used to prevent data form being lost or destroyed. A complete network is illustrated at the end.

## **4.2 Methodology**

The methodology used for the designing the network involves research in network designing, actual design, and implementation of security controls. The method is a bit different as it relies on previous research and then designing, testing, and improving the initial design as I dug deep into networks and studies. It also involves different security tools and how they work together with the network. As the overall objective is to provide demo to different security tools and recommend the best ones needed to deploy.

## **4.3 Company Assets**

Each company has assets or resources that are essential to their business. Assets include hardware, software, web services etc. It is very important to identify assets and then categorize them according to the risk they may face. BYG systems assets are listed below:

* Learning delivery: This asset encompasses of complete e-learning applications for users.
* Employees taking courses at a customer (customer learning system): As its name suggests this is the system used by customers that are taking some courses at BYG systems.
* Learning design: It includes the responsibility and curriculum that are used to design the learning materials
* Creative folks developing learning materials: This resource is being used by contractors who are hired by the company to develop the learning materials as designed by Learning design team.
* BYG Systems own data: This is the data server of the company, and it contains data about the company’s qualities and customer’s relation data etc.
* Private to company: This is information server, and it contains data that is used to target marketing or research purposes.
* Public data: This data includes all the information and services that are visible to General public so they can explore or purchase any products or services from the company.

## **4.4 Information security classification**

As earlier described in chapter 3 Information classification is an important part of network design. Generally, it is the process of assessing the assets and decide what level of protection it should be provided (Craigen et al.,2014). The system used in this design consists of four levels

* Public: This classification applies to information that is provided by the company and pose no such threat.
* Internal-only: This classification applies to data that is only used inside the company and only employees have access to it.
* Official: This classification applies to company’s information that is private and intended for internal use such as customer performance. Internal audit etc.
* Official-sensitive: This classification applies to confidential or sensitive information that needs to be monitored at all times. It can include strategies, reports, and research development etc.

These labels will used to identify the importance of assets and they will be placed in their appropriate segments.

## **4.5 Risk Classification**

According to (jouini et al., 2014) Information systems are constantly face several kinds of threats which can result in different types of damages and can lead to disastrous outcomes. The damages to these systems vary considerably as some target the confidentiality or integrity of the system while others can affect the availability of system or services. All these threats can cause small to large scale financial loss. To improve the security the experts developed risk classification that enables us to identify the assets or systems that face major risk or damage to them can cause big problems and others that might only have minor setback. Following are the labels are used to identify the likelihood of facing threats.

* High
* Medium
* Low

## **4.6 Classification Table**

After identifying the information classification and risks we can develop a table that reflects how assets are labeled. The table below shows all the assets and their labels.

Table 2: Classification table

|  |  |  |
| --- | --- | --- |
| **Assets** | **Risk classification** | **Information classification** |
| Learning delivery | Medium | Internal-only |
| customer learning system | Medium | Internal-only |
| Learning design | Medium | Internal-only |
| Developing learning materials | Medium | Internal-only |
| BYG Systems own data | High | Official |
| Private to company | High | Official-sensitive |
| Public data | Low | Public |

After constructing this table, we have identified the assets and classified them according to risk and Information classification techniques.

**4.7 Virtualization:**

Virtualization is an evolving technology in computing environment. It is used to consolidate workload and to make the environment flexible and use the resources to their fullest. It is used by engineers, developers, and security experts to conduct testing and performance tasks. According to (Kumar and Charu, 2015) Virtualization is a combination of hardware and software that creates Virtual machines (VMs) and enables us to run multiple operating systems on same physical system. It greatly helps us to test multiple controls like firewall and IPS systems. We will use this technology to implement firewalls and Intrusion prevention system. The software used for this purpose is Oracle VM virtual box.

**4.8 Firewalls**

Firewall is a network security control that helps in protecting our network from malicious traffic and hackers. It is first line of defense against any attacks that want to access or seek to destroy valuable resources in our network. Firewall is placed at a network junction so traffic incoming and outgoing traffic pass through the firewall and it allows or blocks the traffic using certain set of rules. Rules are setup by the network administrator or security expert. A firewall can be hardware, software, or both.

To demonstrate the firewalls, we used the virtual environment.

**4.8.1 IPFire**

IPFire is an open-source firewall which was built form scrap and its primary function was to work as a firewall. The reason why we choose IPFire is that first of all it is completely free and easy to deploy. It is regularly updated that keeps it very strong against new attack vectors. IPFire is Linux based firewall and needs to be deployed on a separate machine.

Now to setup the firewall we can download the image from the IPFire website and extract it after downloading completes. Now fire up the virtual box and select new option to create a VM and name it “IPFire” as Shown in figure below:

Graphical user interface, text, application

Description automatically generated

We can also see the specifications that are assigned to the VM. It has been assigned 2 GB of RAM and 8 GB of storage space. Now as we know that firewall is placed in between Internet and internal network, all the traffic passes through the firewall so for that we need two network adapters. In our case we created two virtual adapters to emulate the scenario. Now we can name these two adapters as “Red” and “Green”. The traffic is coming from red adapter and goes from green adapter. Moreover, the VM firewall is now placed ahead of our system and all the incoming and outgoing traffic of our system passes through the IPFire VM. The setup design of IPFire is displayed in figure below:

Diagram

Description automatically generated

The above diagram shows that setup design used to implement and test the firewall.

Now after setting up the firewall, we can start the firewall and configure it so we can monitor the traffic and view the web interface of the firewall. Once we start the firewall the bootup screen shows up

Graphical user interface, website

Description automatically generated

This the bootup screen of IPFire, press enter to start the firewall.

Now let the system start and then it will prompt for authentication username and password which is created during the installation phase. Once we are login the system displays a console which is shown in figure below:

Text

Description automatically generated

This is the main console which directly interacts with firewall, and we executed a simple command to display network adapters and their IP addresses. Like if we need to change adapters or edit any system configuration files or reboot and shutdown, we use this interface. This interface and can only be accessed on the system in our case it is VM so we have the access to system in other cases where it is deployed on a server, we can only access GUI and for console access we need a LAN cable so we don’t need this console to configure the firewall as it can be a bit complex. Instead, we use the Web interface that is on the WAN connection of the firewall. We can access the web GUI by typing the wan IP address in our browser and providing the port 444 as web GUI listens on this port. Once we provide the address the web interface prompts for authentication, and it is also setup during the installation process. After successful authentication the web interface is accessible as shown below.

Graphical user interface

Description automatically generated

We can view the internal and external net traffic graphs that shows the traffic on daily and weekly bases, and we can create rules and set actions. View firewall logs and check the firewall system status. It is fairly easy to use and configure but by no means IPFire is weak against attacks it is being used by many companies from small to large scale.

**4.8.2 pfSense**

PFsense is another great open-source firewall which is widely used all over the world. And it is regarded as one of the best open-source firewalls. It belongs to FreeBSD OS family and is tailored for use as a firewall and router. It is flexible and powerful furthermore regular updates keeps it secure and affective against new attacks. The best thing about PFsense is it easy to deploy and no knowledge of BSD is required to configure or use the firewall. Similar to IPFire, PFsense can also be deployed in virtual box, and we are going to create a VM for it and configure the firewall to start monitoring our traffic.

pfSense has same network configuration as IPFire and it also needs two adapters and needs 2 GB of RAM and 8GB of storage space to work. The network design of pfSense is shown below

A picture containing chart

Description automatically generated

This diagram shows how pfSense is physically setup and we will explain the firewall following this scenario.

Now to install pfSense we have to follow the same steps as IPFire and configure the network adapters. Then we can set up the LAN and WAN connections setup the authentication for root and web interface.

Text

Description automatically generated

This is the startup screen of pfSense once it boots up. We can see the WAN and LAN connections and some option that we can execute. pfSense also has a very easy interface but this console is only accessible with direct link to the machine. For the firewall configuration and status, we need to access the web interface that is available at the LAN connection of the firewall which is 192.168.1.176/24 in our case. We will type the address in web browser of our choosing. And it will ask for authentication we will enter the username and password of our choosing during the installation. Once authentication is successful, we can see the dashboard of pfSense firewall as shown in the figure below:

Graphical user interface, text, application

Description automatically generated

It shows the system information and interfaces that are connected and their status. Now we can configure the firewall rules for LAN and WAN connections. WAN is the outside traffic that is coming into our system also known as incoming traffic and also traffic that is going out known as outgoing. We can set different rules for WAN and LAN which is our internal network. As we can see I have already created few rules that will be compatible with the network design.

Graphical user interface, application

Description automatically generated

Now this window shows the rulesets that are created. I have created these rules to allow the following traffic that matches these conditions. First this is the ruleset for the LAN connection moreover the window shows 3 rules. The check box is for firewall log if the box is checked it will log all the traffic matching the rules. The green tick shows that traffic is allowed to pass next protocol we can explicitly define the protocol e.g., “TCP” or “UDP” and for IPv4 and v6. Source is where the traffic originates and next is its port or source port. Similarly with the destination. Gateway defines which path or route does traffic take to in and out of the network, Description shows what the rule means in English or human understandable. We can add as many rules as we want and easily delete any if we don’t need it anymore.

pfSense is great overall firewall with good performance and ease of use. It has many others features like VPN, routing capabilities and NAT address translator etc. The best thing about it is that its completely free and once deployed it very easy to maintain.

**4.8.3 OPNSense**

opnSense is another open-source and stateful firewall. It is also based on FreeBSD OS family. It includes many advanced features like VPN, hardware failover, Web filtering and IPS system. It contains everything to protect the network and free of cost. It is also considered as one of the best according to opnSense providers.

To setup opnSense we again deploy it in virtual machine and Assign 1 GB of RAM and 8 GB storage. Network adapters are again needed more then one and we created virtual adapters that bridged. So, the network design is similar to the previous firewalls.

Graphical user interface, text, application

Description automatically generated

The figure shows the specifications of the VM. Now we can boot it up and follow the steps to install the firewall. After installation we can boot up the firewall the boot up screen is shown in the figure below:

Text

Description automatically generated

It will automatically load all the drivers and services and then prompt to login. Once logged in using the username and password that was set during the installation process, we can see the following screen.

Text

Description automatically generated

The figure shows the opnsense website and blogs. Then it shows the LAN and WAN connection IP addresses. LAN address is used to access the web interface where we can configure the firewall and enable or disable any firewall rules or firewall itself. We can view the firewall status and dashboard once we access the web GUI. Enter the LAN IP address following HTTPS protocol as shown in figure

Graphical user interface, website

Description automatically generated

We can login using the web GUI username and password. This to protect the firewall configuration from unauthorized access. Although opnsense web GUI can only be accessed via LAN it still needs authentication to protect form inside access or access by mistake. Once logged in we can view the firewall dashboard which displays all the necessary information for quick monitoring.

Graphical user interface, application

Description automatically generated

As we know that firewall is only as powerful as its rules. So, it is very easy to create rules in opnsense. Now on WAN interface lets blocking all incoming and outgoing traffic that is the number protection after setting the firewall.

Graphical user interface, text, application

Description automatically generated

As we can see in the figure above that all the incoming and outgoing is blocked. Now we can manually add the hosts or allow traffic on specific ports just like in figure I have created a rule to allow the IP address 192.168.10.15 to send and receive packets. This is how we can only allow trusted users to communicate with the network and access resources. The following table shows the comparison between the firewalls with windows default firewall.

*Table 3: Firewalls Comparison table*

|  |  |  |
| --- | --- | --- |
| Firewall Name | Features | Free |
| Windows Firewall | * Host based firewall * Two-way traffic filtration * IPsec to protect network against unauthorized access. * Can encrypt certain traffic. | Yes (Provided with Windows 10 and above server 2016 and above) |
| Pfsense | * IP and port filtering * Real time traffic monitoring * Network address translation * Stateful firewall | Yes |
| IPfire | * Stateful packet inspection firewall * Network address translation and port-forwarding rules can be created. * Based on packet filtering framework. * Intrusion prevention system can be integrated. | Yes |
| OPNSense | * Stateful firewall with ipv4 and v6 support * Integrated support for IPsec and OpenVPN * Two factor authentication * Web filtering * Integrated IPS and IDS | Yes |

**4.9 Intrusion prevention system**

IPS or Intrusion prevention system is another security tool that helps prevent intruders from breaking into the system. It basically scans every packet and blocks any suspicious packets or traffic that is generated intentionally. IPS is also called IDPS Intrusion detection and prevention system, as it first detects any malicious traffic and then generates alarm so that network administrator is notified that someone is trying to attack the network. Moreover, IPS blocks the traffic so that they cannot reach the system. It is very useful security tools and often used with the firewalls (Wang and Li, 2013). Usually, IPS is placed ahead of firewall, which is a very good technique whiling design a network as it provides an additional layer of defense.

**4.9.1 Suricata IPS**

Suricata is an excellent IPS with regular updates that keeps it up to date with new threats and attack patterns. It is also an opening source IPS, and it can be easily deployed. One of the major advantages of Suricata is that it can seamlessly embed with other open-source solutions like firewalls. Suricata IPS can be installed on both windows and Linux. But then we have to configure it by ourselves that can be bit complex and then to attach it with firewall can be difficult as well. Luckily IPFire and opnsense already have compatibility with Suricata and we can utilize the same functions without having to deal with technical configuration.

**4.9.1.1 Suricata with IPFire**

Suricata IPS is already combined with IPFire, but it is not activated by default. We have to set up the IPS. It also gives us the option to activate any of two. We can enable IPS and disable the firewall or just use the firewall and disable IPS. But the best case is if we use both together. But IPS is built ahead of firewall so once we enable the IPS all the traffic passes through the IPS and onto the firewall. We can enable IPS on web GUI of IPFire. It is easy to configure the rules and check the logs of both firewall and IPS as they are unified on the same web interface as shown in figure below:

Graphical user interface, application

Description automatically generated

The IPS offers monitoring on both interfaces red and green. It has built rules that are updated and can be immediately put on action to protect against all the known attacks. It also gives us the option to create any rules or monitor any specific type of traffic. For now, we have enabled the IPS ruleset of SSL connections with weak ciphers.

**4.9.1.2 Suricata with opnsense**

Similarly, with IPFire Suricata can be used with opnsense as well. Although the IPS is same, but the interface is different. As each vendor has its own way of placing things. In opnsense we have the option to enable IDS mode and IPS mode as separate option. The figure shows the IPS configuration page.

Graphical user interface, text, application, email, website

Description automatically generated

If we check the enable box it will enable the IDS mode of Suricata but if we check the IPS mode option, it will enable the blocking mode which is what prevents the traffic from passing through. We have the option to enable alerts and enable the logs that saves the alerts in a file, and it can be used for further improvement of rules. We can also specify the interfaces as well.

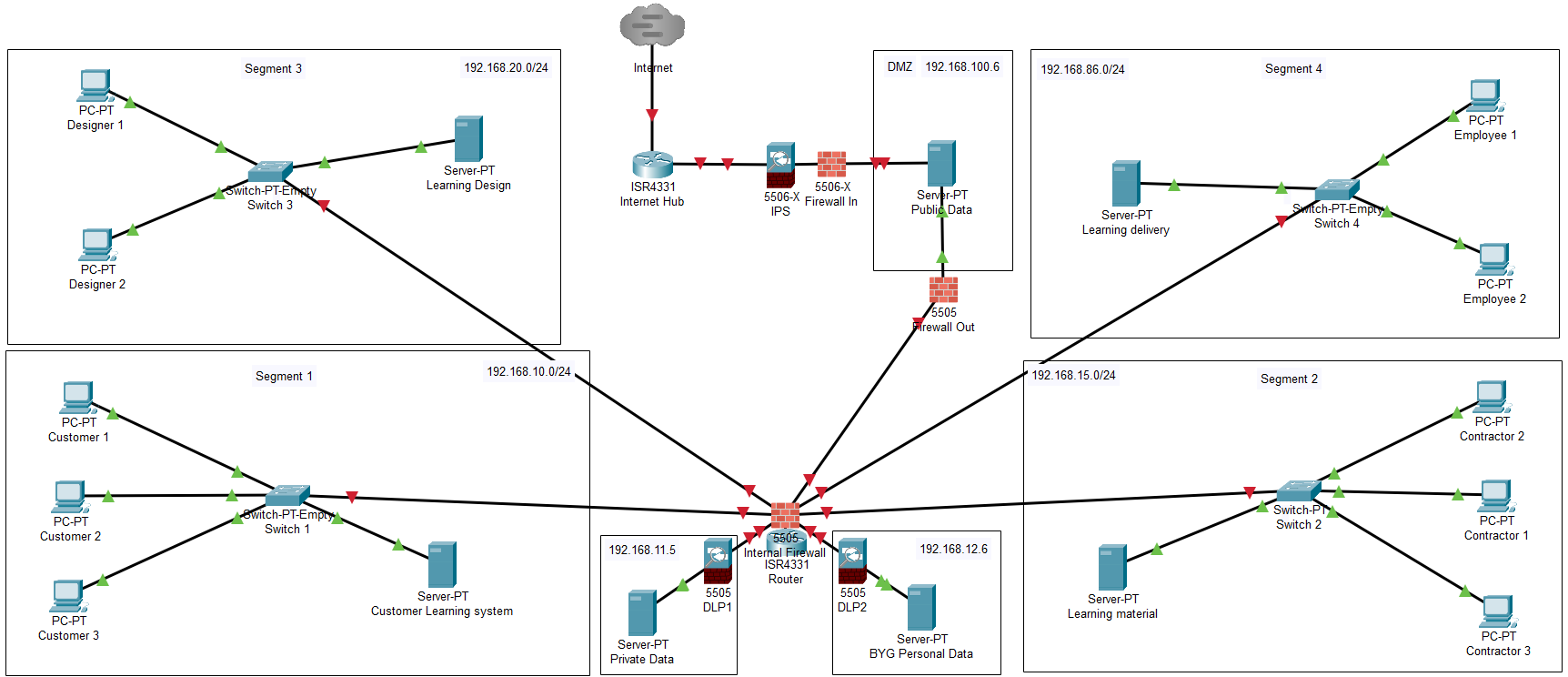
In download tab we have list of rules that many providers and community have built over the years by studying attack patterns. we have the option to enable the rules of our choice. It will take effect immediately and we can disable them at any time.

**4.10 Data Loss Prevention**

DLP or Data loss prevention is another security tool that is used to protect our data from being destroyed. Digital data can easily be destroyed during the transmission or while accessing the data. Any employee can by accident perform an operation that can result in data being altered or destroyed. To prevent this from happening DLP is placed on data servers which have sensitive information and must be protected against such mistakes.

## **4.11 Network Diagram**

Networks are design in network mapper tools. These tools visually show how computer and servers are placed. Cisco packet tracer is used to create the network diagram. After careful planning and following the research done in earlier chapters the network design is created. The figure shows the complete network.



This is the entire network design. There are multiple controls and check that makes the network secure and easy to understand. Some characteristics of these network are segmentation that makes the part of network isolated so they can only access the required resources. There are four segments that separate different departments of BYG systems. Segmentation helps to keep the network resources isolated from others in the network. DMZ demilitarized zone is also a segment, but it contains server which will be exposed to the public. As it is the entry point for all the public, we need to place certain checks so no malicious, or hackers can get into the network. The traffic is monitored by IPS and then passed to the firewall. There are two firewalls placed the “Firewall In” only allows the incoming traffic while no traffic can go out on the other hand the “Firewall Out” only allows the traffic to from internal network to the DMZ while blocking all the incoming traffic.

There are two types of networks internal and external. External network is where all the public has access to including the company employees. Internal can only be accessed by employee and it also has some resources which can only be accessed by authorized people. Let’s take a look at segment 1 as shown in figure:

Chart

Description automatically generated

In this diagram we have removed other segments to explain how segmentation will affect the network and how can they access the resources in the segment and outside the segment.

The segment 1 has the Network “10” in the top right corner it is written 192.168.10.0/24. This is an IP address, but it actually represents this whole network. Notice the last two part of the IP address they indicate network and host respectively. Customer1 and so on will have different IP addresses in the same network. The Server is connected through the switch. So, any of these customers can access the server as this is the customer learning system, they have to take courses which are available on the server. But they cannot access the private data server because they don’t need to access other servers so firewall on router has blocked their requests.

**4.12 Advantages of network**

The purposed network is an easy to implement and understandable design with an intermediate level of security to protect from outside threats. It has the following advantages

* Easy to deploy.
* Very cost effective in deploying the network as all of the security controls are open source.
* Ease of use as most interface don’t require background knowledge of Linux and FreeBSD.
* User friendly web interfaces to configure the firewalls and IPS.
* Maintenance is easy.
* Most of security are automatically updated so new attack are detected and can protect network form them.

The network consists of different security controls and techniques that are widely used all over the world. It provides a good security for a small-scale company with the ability to grow in future. It has an easy design which can be changed to accommodate new segments and policies.

**4.13 Limitations of network**

The purposed network use a lot of different security controls and other technical techniques like segmentation. It can be a little difficult to configure all of them. Since all the tools are open source there could be limited documentation and guides which might be needed in future to help resolve an issue. A dedicated network administrator maybe required to monitor the tools and respond in case of an issue with the connectivity.

Firewalls need to be configured properly and an individual with adequate knowledge of firewall maybe required. As rules may need a changing and in future if an old segment which no longer exists have to removed and for ruleset and a new segment is created it will need new set of rules. Because firewall can also be by passed and in that case, it poses a threat to the network.

Intrusion prevention system not only detects the attacks but prevents from, but it needs attention as it generate alerts if someone is trying to breach the network at first it may protect against the attack, but the attacker might use another technique was IPS is not capable of preventing but can detect it. So now it is up to the security team or person to handle the threat.

All these controls and devices need to be monitored as well because they can also experience some issue or an attack that might render them useless. Security of the network depends upon these tools. If anyone of these goes down either it can leave a huge vulnerability in the network, or it might take the network down.

**4.14 Recommendation**

There are many different vendors that created the firewalls, IPS and DLP each have some unique characteristics while they all protect our network against outside world. Some are better suited in some conditions while others are not. While deploying the purposed network the tools need to be configured and it is not easy to configure them. The best ones are those that are easy to configure and easy to use.

The recommended security tools to be used with the purposed network are listed below

* Use Suricata as an IPS for it is easy to configure and easy to use. Moreover, many rules are already built in, so we don’t need to create our own rules for protection against known attacks.
* The first firewall to be placed after the IPS and before the DMZ should be IPFire with default out going traffic to be blocked. And Local network access to be blocked as well.
* The second firewall will be pfSense as it also easy to use and reliable. It is widely used by many companies. This firewall will allow traffic from local area network into the DMZ but block traffic from DMZ into the internal network.
* DLP is configured on the Sensitive data servers only. As they need to be monitored and data loss is to be prevented.
* There are some switches that have routing capabilities, but it is better to place a router inside the internal network with firewall enabled.
* We can block the access to sensitive data server from others and only allow access from specific hosts only. So, the authorized people can only access the private data server and BYG data server.

# **Chapter 5 Conclusion & Future work**

**5.1 Conclusion:**

This project has purposed and shown how a secure network design and how it can be deployed. It has the potential to stop the intruders from accessing the valuable resources. It also ensures that only authorized party can access the sensitive information and isolated others to the resources that they need. The project has fulfilled its aim and objectives while discussing many security tools and following the best practices of placing the controls. This network design is completed by conducting research and into the secure network design principles, classifications and security tools that lead to secure network design.

**5.2 Future Work:**

The completion of this project also leads to future work. As the technology advances everyday new threats and problems arise with it. Now the network design can be secure for now, but it can be vulnerable in future. It may demand the network to upgrade and introduce new requirements.

The scope of this network design can be further expanded by using new and latest security tools that provide much better security and more features. We can add IPS on the internal network as well to monitor the internal network traffic as well. The security tools can also be paired with AI and machine learning to lessen the load on network administrator and security experts as it can handle threats and detect patterns by using algorithms and then incorporate them into the network.

The purposed network design is for small scale companies with limited resources and security controls. As small-scale companies can rise to medium or large scale their resources and network needs to be expanded as well. They can have multiple office or sites and they might need to connect to the others. Similarly, some employees could be working from home after the change in trend due to global pandemic. So, it opens multiple dimensions this project can proceed into.

**References**

Wood, C.C., 1990. Principles of secure information systems design. *Computers & Security*, *9*(1), pp.13-24.

<https://www.learncisco.net/courses/iins/common-security-threats/security-architecture-design-guidelines.html>

Wood, M., 2020. How SASE is defining the future of network security. *Network Security*, *2020*(12), pp.6-8.

V. Agrawal, "A Framework for the Information Classification in ISO 27005 Standard," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), 2017, pp. 264-269, doi: 10.1109/CSCloud.2017.13.

Mowery, D.C. and Simcoe, T., 2002. Is the Internet a US invention?—an economic and technological history of computer networking. *Research Policy*, *31*(8-9), pp.1369-1387.

Bhaskaran, A.P., Analyzing Effectiveness of Security by design Model in a Cloud application development lif ecycle which uses IAC (Infrastructure As Code).

Charles P. Pfleeger. 1988. *Security in computing*. Prentice-Hall, Inc., USA.

Stawowski, M., 2007. The principles of network security design. *ISSA Journal*, pp.29-31.

Wood, C.C., 1990. Principles of secure information systems design. *Computers & Security*, *9*(1), pp.13-24.

Yan, Z., Robertson, T., Yan, R., Park, S.Y., Bordoff, S., Chen, Q. and Sprissler, E., 2018. Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behavior*, *84*, pp.375-382.

Sasse, M.A., Brostoff, S. and Weirich, D., 2001. Transforming the ‘weakest link’—a human/computer interaction approach to usable and effective security. *BT technology journal*, *19*(3), pp.122-131.

Standage, T., 2002. The weakest link. *The Economist*, *365*(8296), pp.11-16.

Pfleeger, S.L., Sasse, M.A. and Furnham, A., 2014. From weakest link to security hero: Transforming staff security behavior. *Journal of Homeland Security and Emergency Management*, *11*(4), pp.489-510.

Schneider, F.B., 2003. Least privilege and more [computer security]. *IEEE Security & Privacy*, *1*(5), pp.55-59.

Jero, S., Furgala, J., Pan, R., Gadepalli, P.K., Clifford, A., Ye, B., Khazan, R., Ward, B.C., Parmer, G. and Skowyra, R., 2021, May. Practical Principle of Least Privilege for Secure Embedded Systems. In *2021 IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS)* (pp. 1-13). IEEE.

Woodbury, C., 2007. The Importance of Data Classification and Ownership. *no. C*, pp.1-4.

Agrawal, V., 2017, June. A framework for the information classification in ISO 27005 standard. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 264-269). IEEE.

Collard, G., Ducroquet, S., Disson, E. and Talens, G., 2017, May. A definition of information security classification in cybersecurity context. In *2017 11th International Conference on Research Challenges in Information Science (RCIS)* (pp. 77-82). IEEE

Joint Technical Committee ISO/IEC JTC1. Subcommittee SC 27, 2013. *Information Technology--Security Techniques--Information Security Management Systems--Requirements*. ISO/IEC.

Wagner, N., Şahin, C.Ş., Winterrose, M., Riordan, J., Pena, J., Hanson, D. and Streilein, W.W., 2016, December. Towards automated cyber decision support: A case study on network segmentation for security. In *2016 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1-10). IEEE.

Daya, B., 2013. Network security: History, importance, and future. *University of Florida Department of Electrical and Computer Engineering*, *4*.

Lyu, M.R. and Lau, L.K., 2000, October. Firewall security: Policies, testing and performance evaluation. In *Proceedings 24th Annual International Computer Software and Applications Conference. COMPSAC2000* (pp. 116-121). IEEE.

Kizza, J.M., 2005. *Computer network security* (pp. 440-455). New York: Springer.

Patnaik, D.P.C., Network Security: Concepts and Various Aspects for Treating the Attacks. *IJSDR2102055*.

Dowd, P.W. and McHenry, J.T., 1998. Network security: it's time to take it seriously. *Computer*, *31*(9), pp.24-28.

Craigen, D., Diakun-Thibault, N. and Purse, R., 2014. Defining cybersecurity. Technology Innovation Management Review, 4 (10), 13-21.

Jouini, M., Rabai, L.B.A. and Aissa, A.B., 2014. Classification of security threats in information systems. *Procedia Computer Science*, *32*, pp.489-496.

Wang, Z. and Li, X., 2013. Intrusion prevention system design. In Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012 (pp. 375-382). Springer, London.