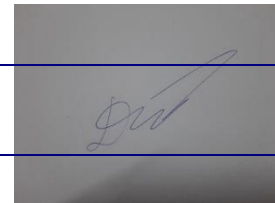




ASSIGNMENT 1 FRONT SHEET

Qualification	BTEC Level 5 HND Diploma in Computing		
Unit number and title	Unit 5: Security		
Submission date	23/2/2022	Date Received 1st submission	<div style="border: 2px solid red; width: 150px; height: 30px;"></div>
Re-submission Date		Date Received 2nd submission	
Student Name	Mai Thế Đức	Student ID	GCH200681
Class	GCH0907	Assessor name	Michael Omar
Student declaration <p>I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.</p> <div style="text-align: right;">1.1</div>			
		Student's signature	

Grading grid

P1	P2	P3	P4	M1	M2	D1
						

⚙ Summative Feedback:**⚙ Resubmission Feedback:**

2.1

Grade:**Assessor Signature:****Date:****Lecturer Signature:**

TABLE OF CONTENTS

I. Introduction	4
II. Types of security threat to organisations	4
II.1. Define threats	4
II.2. Threat agents	4
II.3. Type of threats that organisations will face	5
II.4. Security breaches	6
II.5. Solutions	8
III. Organisational security procedures	9
IV. THE potential impact to IT security of incorrect configuration of firewall policies and IDS.....	10
IV.1. How does a firewall provide security to a network?	10
IV.2. The potential impact of a firewall if it is incorrectly implemented.....	12
IV.3. IDS	12
IV.4. The potential impact of a IDS if it is incorrectly implemented.....	13
V. DMZ, static IP and nat in a network.....	14
V.1. DMZ	14
V.1.1. Usage	15
V.1.2. Security Functions	16
V.2. Static IP.....	16
V.2.1. Usage	17
V.2.2. Security Functions	17
V.3. NAT.....	18
V.3.1. Usage	18
V.3.2. Security Functions	19
VI. Conclusion.....	19
VII. References.....	20

I. INTRODUCTION

In this assignment, the scenario put in a role of trainee IT Security Specialist for Security consultancy in Vietnam called FPT Information security (FIS). My task is to train staff member on the tools and techniques associated with identifying and assessing IT security risks together with the organizational policies to protect business critical data and equipment.

II. TYPES OF SECURITY THREAT TO ORGANISATIONS

II.1. Define threats

Several definitions of the phrase can be found in the literature. The Internet Engineering Task Force (IETF) and the National Institute of Standards and Technology (NIST) both have texts that are rather short and simple.

In RFC 4949, IETF defines a threat as:

"A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm."

NIST, in SP800-160, defines it as:

"An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss."

II.2. Threat agents

Threat Agent is any person or thing that acts (or has the power to act) to cause, carry, transmit, or support a threat. Examples of threat agents are malicious hackers, organised crime, insiders (including system administrators and developers), terrorists, nation states, and even natural disasters (Fandom, 2022).

National States: Companies in specific industries, such as telecommunications, oil and gas, mining, power generation, national infrastructure, and so on, may become targets for foreign countries, either to disrupt operations today or to provide that nation a future hold in times of crisis (Lamb, 2019).

Insiders: Unless it's a Zero-day virus, machines and software programs are rather good at protecting themselves from malware. Humans are frequently the weakest link in the security system, whether intentionally or unintentionally. We all make mistakes, such as sending an email to the wrong person, but we typically catch ourselves and are able to correct the issue promptly. Simple safeguards, such as password-protecting data, can help to limit the consequences of such errors. Unfortunately, there are some disgruntled employees who intentionally destroy organizations from within for many reasons. There are instances when businesses want specialized assistance and hire contractors or external agencies who require access to their systems or data. These third parties are frequently the source of problems since their devices may not have the same degrees of security as the controller's data (Lamb, 2019).

Terrorists: similarly to the threat posed by nation states, the level of threat posed by these actors is dependent on your actions. However, some terrorists choose to target specific industries or countries, so you may face a constant fear of a random attack (Lamb, 2019).

Organised crime: Criminals are after personal information for a variety of purposes, including credit card fraud, identity theft, and bank account fraud. These crimes are now being carried out on a large basis. The methods employed vary, from phishing attempts to 'Watering Hole' websites, but the end result is the same: your data and you are being harvested and used for evil purposes (Lamb, 2019).

Natural disasters: Although not a cyber assault, these occurrences can have a similar impact on your ability to conduct business. If you can't get into your offices, data centers, or cloud-based information, you're still dealing with a data disaster, which must be considered (Lamb, 2019).

II.3. Type of threats that organisations will face

1. Computer viruses

A virus is a piece of software that can spread from one computer to another, or from one network to another, without the user's awareness and carry out hostile activities. It has the capacity to corrupt or harm important data in organizations, as well as delete files and format hard drives (Touhid, 2019).

2. Worm

A computer worm is a sort of malicious software or program that spreads through an organization's network and replicates itself from one computer to another (Touhid, 2019).

3. Phishing

Phishing is a type of social engineering attack that tries to steal personal information such as usernames, passwords, credit card numbers, login credentials, and so on.

4. Malware

Malware is computer software that is often composed of a program or code that is created by cyber criminals. It is a class of cyber security risks aimed at causing significant harm to systems or gaining unauthorized access to a computer.

II.4. Security breaches

1. In May, 2021: security researchers revealed that multiple misconfigurations of cloud services had exposed the personal data of over 100 million Android users. The downloads, which ranged from 10,000 to 10 million and contained internal developer tools, were left unprotected in real-time databases utilized by 23 apps (Check Point, 2021).

Consequences: Names, email addresses, dates of birth, chat messages, location, gender, passwords, photographs, payment information, phone numbers, and push alerts were determined to be accessible by anyone, according to Check Point researchers.

2. In April, 2021: Alon Gal, a security researcher, uncovered a leaked Facebook database comprising 533 million accounts.

The data includes personal information from Facebook users in 106 countries, including over 32 million records for US users, 11 million for UK users, and 6 million for Indian users. Insider examined a sample of the leaked data and confirmed numerous records by cross-referencing known Facebook users' phone numbers with the data set's IDs. Insider also double-checked records by using email addresses from the data set in Facebook's password-reset feature, which may be used to expose a user's phone number in part (Holmes, 2021).

Consequences: "A database of that magnitude including the private information of a lot of Facebook's users, such as phone numbers, would almost likely lead to bad actors exploiting the data to undertake social-engineering assaults [or] hacking attempts," Gal says.

3. In June, 2021: Personal information from 700 million LinkedIn users, or almost 93 percent of the company's members, was available for purchase on the internet. With samples from 2020 and 2021, the data looked to be current. "We've examined, and there is no proof that this is fresh data or that the data is from 2020 and 2021," a LinkedIn spokeswoman told Fortune in a statement. The phone number, gender, inferred salary, and physical address in this data set did not come from LinkedIn, according to LinkedIn's current inquiry." (Morris, 2021)

Consequences: although the data did not contain login passwords or financial information, it did contain personal information that might be exploited to impersonate someone, such as:

- Full names
- Phone numbers
- Physical addresses
- Email addresses
- Geolocation records
- LinkedIn usernames and profile URLs
- Personal and professional experiences and backgrounds
- Genders
- Other social media accounts and usernames

All of the consequences are very impact on user online security. But not only clients are the ones who suffer, organisations will have to deal with many things after a successful breach happen. Financial loss and Reputational damage are two of biggest result from a data breach.

Financial loss: your personal information can be sold or used in an espionage scheme by a single criminal. The majority of the time, a cyber breach occurs so that thieves can profit. A data breach affects 100 firms in the United States every day. According to IBM, the average cost of a cyber breach in the United States in 2020 will be \$3.86 million. Aside from the financial expenses of a data breach, the consequences for

employees are equally frightening. When cybercriminals get access to employees' personal information, morale suffers.

Reputational loss: every data breach damages a company's brand, leading to client distrust. Customers will depart if they do not believe you are appropriately protecting them. Simultaneously, your competitors may approach your consumers to poach them as a result of the attention around your data breach.

II.5. Solutions

1. Implement a data security plan:

A thorough data security plan should be developed, implemented, and updated by each organization. This strategy should include a list of the many types of data that the business collects, stores, processes, or communicates (Matsuura, 2013).

2. Encrypt data:

For sensitive data, data security guidelines should mandate the use of strong encryption. When external parties are utilized to store data, the data should be encrypted before being sent to them, even if they are able to provide encryption services. In this situation, it is preferable to use your own encryption techniques rather than depending solely on encryption provided by service providers, which could be easily deciphered by government officials (Matsuura, 2013).

3. Use access controls and firewalls

Access restrictions should be a must in data security measures. Passwords, authentication requirements (e.g., challenge questions to validate user identity), and biometric systems should all be included in these controls (e.g., fingerprint readers). It's a good idea to employ a few different authentication techniques. The success of user authentication methods such as passwords is based on the behavior of all authorized users, according to data security policies and practices (Matsuura, 2013).

4. Keep some data off the network:

Data that is believed to be so sensitive that it should not be stored on computers connected to the Internet or other computer networks should be identified in data security strategies. It's likely that some very sensitive data shouldn't be maintained on machines that can be accessed through the Internet for security reasons. It's

critical that each organization assesses all of the many types of data it manages to see if part of it should be kept off of computers that may be accessed remotely (Matsuura, 2013).

III. ORGANISATIONAL SECURITY PROCEDURES

Security procedure refers to the security procedures that must be followed by Customer when issuing an Instruction and/or by Bank when receiving an Instruction in order for Bank to verify that the Instruction is authorized, as set forth in service level documentation in effect from time to time between the parties with respect to the services set forth in this Agreement, or as otherwise agreed in writing by the parties. Algorithms, codes, passwords, encryption, and telephone call backs are only a few examples of security procedures. Customer acknowledges that the purpose of Security Procedures is to verify the validity of Instructions rather than to find mistakes in them. For the avoidance of doubt, the parties agree that an authorized Instruction is a SWIFT message issued in Customer's name through any third party utility agreed upon by the parties as a way for giving Instructions and validated in accordance with such utility's ordinary procedures.

Some of Organisational security procedures:

- Acceptable Use Policy (AUP)
- Change Management Policy
- Disaster Recovery Policy

Discussion on Acceptable Use Policy:

An AUP outlines the restrictions and practices that employees who use organizational IT assets must accept in order to have access to the business network or the internet. It is standard procedure for new employees to be onboarded. Before being assigned a network ID, they must read and sign an AUP.

Discussion on Change Management Policy:

A structured method for making changes to IT, software development, and security services/operations is referred to as a change management policy. A change management program's purpose is to raise awareness

and knowledge of proposed changes throughout a business, as well as to ensure that such changes are implemented systematically to minimize any negative effects on services and consumers.

Discussion on Disaster Recovery Policy:

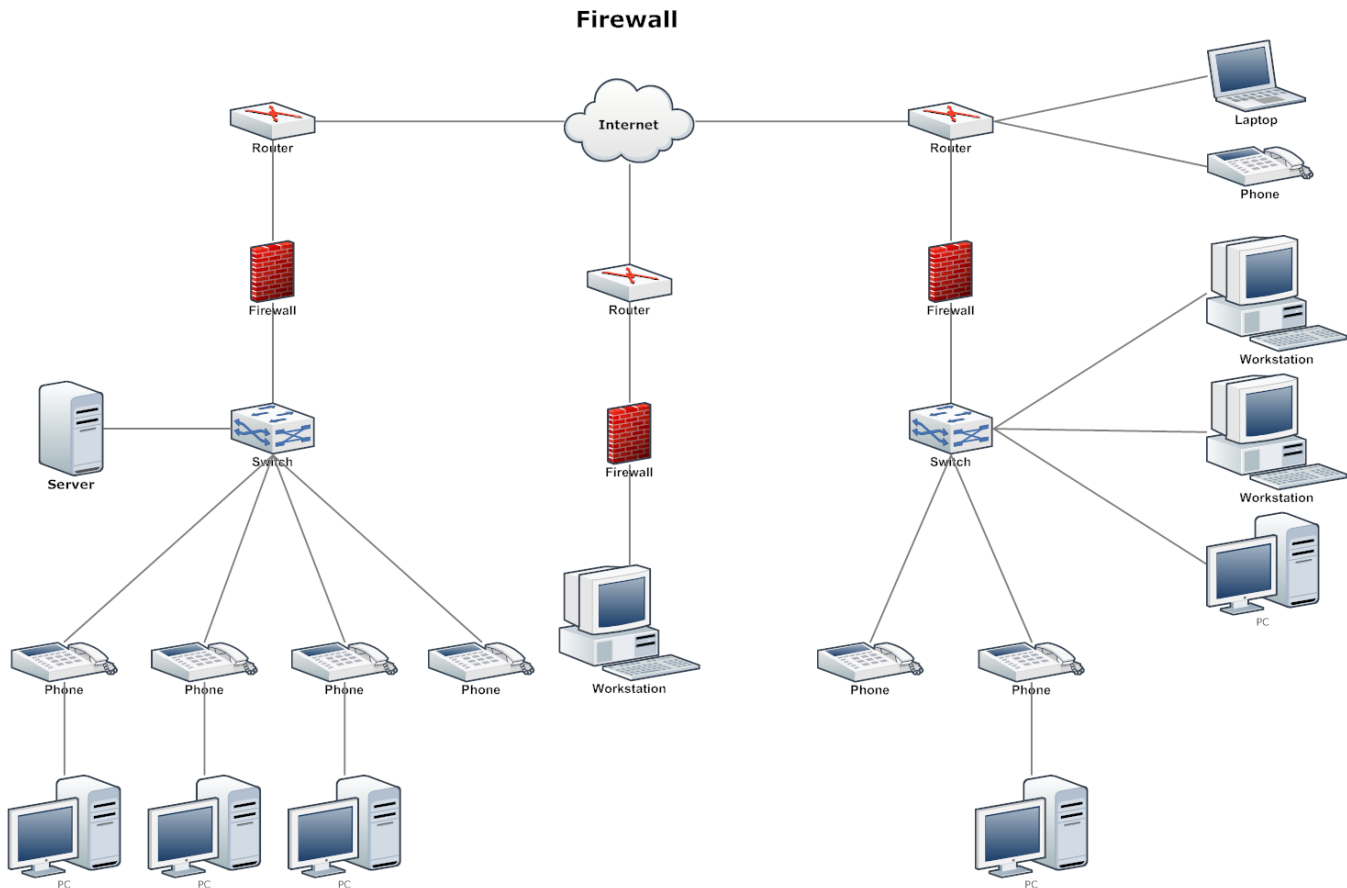
The disaster recovery plan for a company will often include input from both the cybersecurity and IT departments and will be established as part of the larger business continuity strategy. The incident response policy will be used by the CISO and his team to manage an occurrence. The Business Continuity Plan will be initiated if the event has a major business impact.

IV. THE POTENTIAL IMPACT TO IT SECURITY OF INCORRECT CONFIGURATION OF FIREWALL POLICIES AND IDS.

A firewall serves as a barrier between two networks. It detects and inhibits attempts to obtain access to your operating system, as well as unwanted traffic from unidentified sources. A firewall can assist prevent dangerous malware from infecting your computer by blocking undesired traffic. Different levels of protection can be provided by firewalls. The key is to figure out how much protection you require.

IV.1. How does a firewall provide security to a network?

A firewalled system analyzes network traffic based on rules to begin with. Only those inbound connections that have been set to accept are accepted by a firewall. It accomplishes this by allowing or disallowing specific data packets — the units of communication that you send over digital networks — based on pre-determined security criteria. At your computer's entrance point, or port, a firewall acts as a traffic guard. Only IP addresses or trusted sources are permitted in. IP addresses are significant because they identify a computer or source, much like your postal address does (Johansen, 2021).



Example diagram of how firewall work

It's comparable to a security guard stationed at the door of a minister's residence. He maintains a close eye on everyone and personally inspects anybody who enters the house. It will not allow a person to enter if he or she is carrying a dangerous object, such as a knife or a gun. Similarly, even if the person does not have any prohibited items but appears suspicious, the guard has the authority to refuse access.

The firewall serves as a deterrent. It protects a corporate network by acting as a barrier between the inner and outside networks. All traffic must travel through the firewall in both directions. It then decides whether or not traffic should be permitted to move. The firewall can be implemented as hardware and software, or a combination of both.

IV.2. The potential impact of a firewall if it is incorrectly implemented

Firewall misconfigurations, however, might result in three major consequences. According to Wilson (2021):

- Compliance violation: In order to comply with PCI standards or laws in the retail, financial, or healthcare industries, firms must have a properly designed firewall. Fines apply to noncompliance.
- Breach avenues: A firewall misconfiguration that allows unauthorized access can lead to data loss, breaches, and stolen or ransomed IP.
- Unplanned outages: A misconfiguration may prevent a customer from engaging with a company, resulting in revenue loss. Large e-commerce companies, for example, could lose thousands, if not millions, of dollars until the problem is fixed.

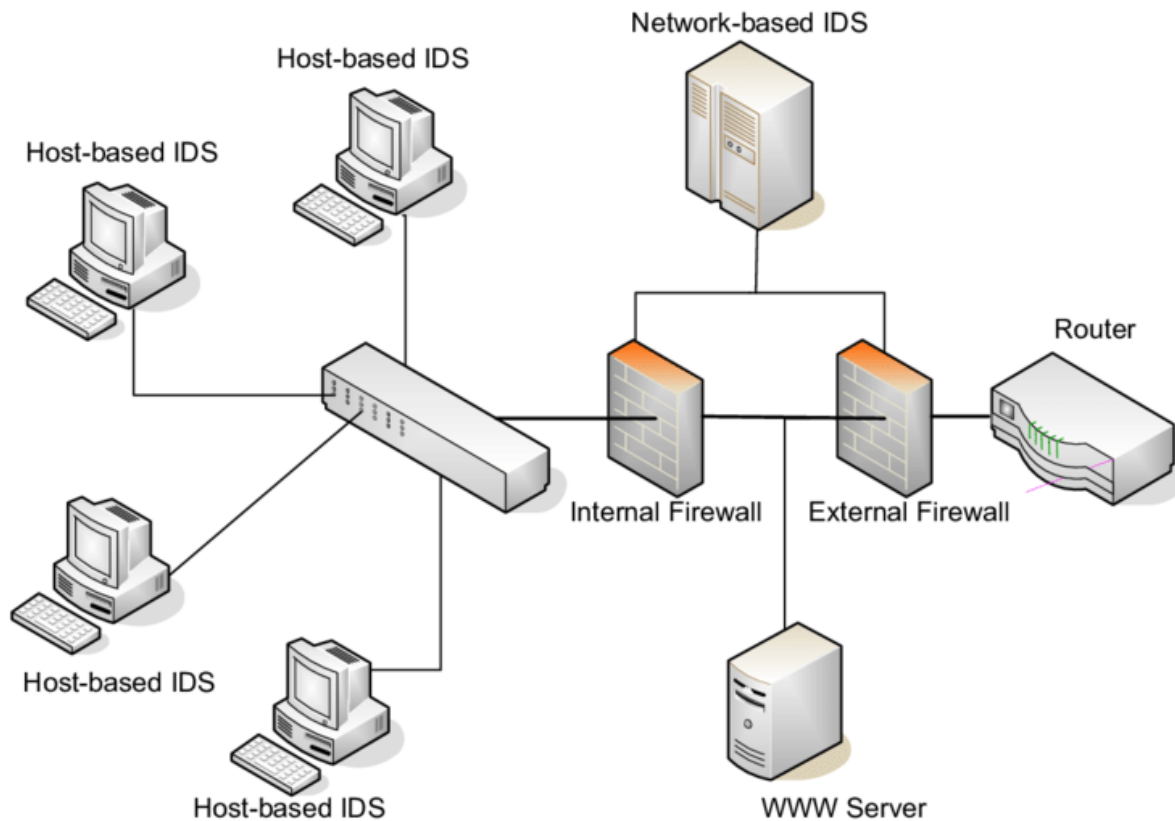
IV.3. IDS

An intrusion detection system (IDS) is a network traffic monitoring system that detects suspicious behavior and sends out alerts when it is found.

While anomaly detection and reporting are the major duties of an IDS, certain intrusion detection systems are capable of taking measures when malicious behavior or abnormal traffic is discovered, including blocking traffic coming from questionable Internet Protocol (IP) addresses (Lutkevich, DEFINITION, 2021).

Intrusion detection systems are used to detect irregularities in the network in order to catch hackers before they cause serious damage. Network-based IDSes and host-based IDSes are both possible. The client computer has a host-based intrusion detection system, while the network has a network-based intrusion detection system (Lutkevich, DEFINITION, 2021).

Intrusion detection systems detect assaults by looking for signatures of previous attacks or deviations from regular behavior. These anomalies are moved up the stack and investigated at the protocol and application layers. They are capable of detecting occurrences such as Christmas tree scans and DNS poisonings (Lutkevich, DEFINITION, 2021).



Example of host-based IDS and Network-based IDS

IV.4. The potential impact of a IDS if it is incorrectly implemented

1. To detect the most recent threats, the signature library must be constantly updated:

The signature library of an IDS determines how effective it is. It won't register the latest attacks if it isn't updated often, and it won't be able to warn you about them if it isn't updated frequently. Another issue is that until a new threat is introduced to the signature library, your systems are exposed, thus the most recent attacks will always be a major concern (Rapid7, 2017).

2. IP packets are still susceptible to forgery:

An IDS reads the data from an IP packet, but the network address can still be faked. When an attacker uses a false address, it makes it more difficult to detect and analyze the threat (Rapid7, 2017).

3. Protocol-based attacks are a threat to them:

Because an NIDS examines protocols as they are collected, it is vulnerable to the same protocol-based assaults that network hosts are. Protocol analyzer issues, as well as improper data, can cause an NIDS to crash (Rapid7, 2017).

V. DMZ, STATIC IP AND NAT IN A NETWORK

V.1. DMZ

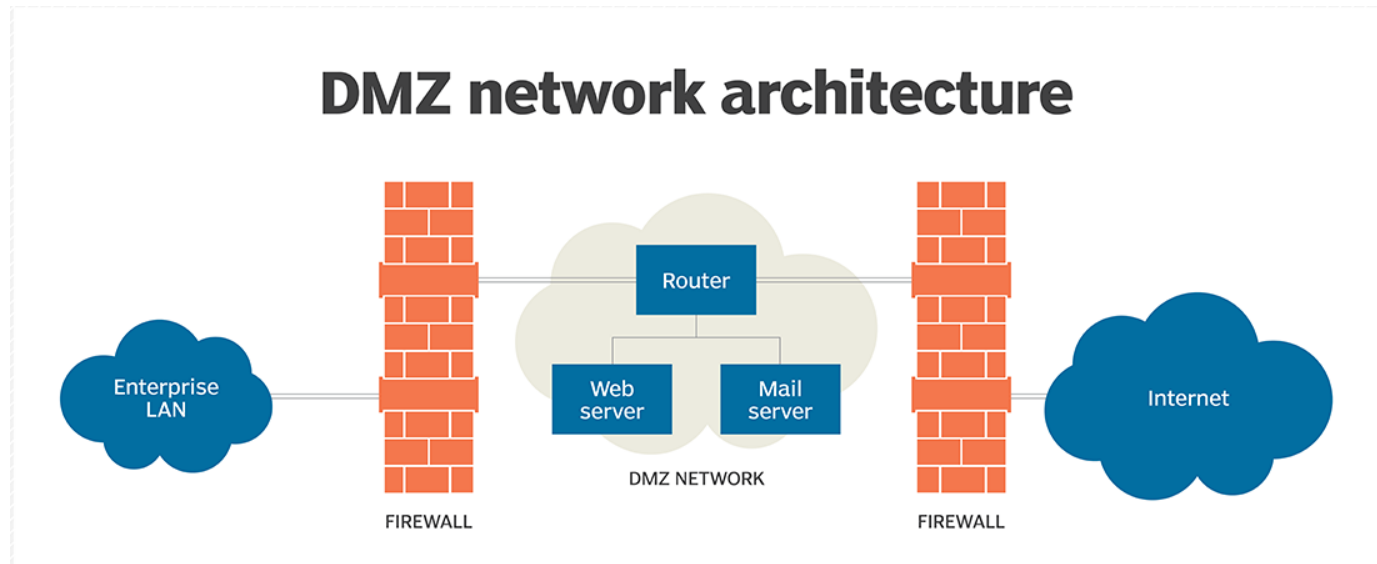
A DMZ, or demilitarized zone, in computer networks is a physical or logical subnet that separates a local area network (LAN) from other untrusted networks, most commonly the internet. Perimeter networks or screened subnetworks are other terms for DMZs (Lutkevich, DMZ in networking, 2021).

The DMZ network should contain any service supplied to users on the public internet. It's usually where external-facing servers, resources, and services are kept. Web, email, domain name systems, File Transfer Protocol, and proxy servers are some of the most common of these services.

The DMZ's servers and resources are available over the internet, but the remainder of the internal LAN is not. This method adds another layer of security to the LAN by preventing hackers from accessing internal servers and data directly from the internet.

How it works:

Between the public internet and the private network, DMZs serve as a buffer zone. Between two firewalls, a DMZ subnet is set up. Before reaching the servers in the DMZ, all inbound network packets are checked using a firewall or other security appliance.



V.1.1. USAGE

According to Lutkevich (2021), the following are common uses for DMZ networks:

- Separate possible target systems from internal networks.
- Limit and regulate external user access to those systems.
- Host business resources to make some of them available to approved external users.

V.1.2. SECURITY FUNCTIONS

According to Lutkevich (2021), this buffer has a number of security advantages, including the following:

- **Control of access:** A DMZ network controls access to services accessible from the internet outside of an organization's network perimeters. It also creates a layer of network segmentation, increasing the number of barriers a user must overcome before being granted access to an organization's private network.
- **Preventing network reconnaissance:** A DMZ also makes it impossible for an attacker to scout out potential targets on the network. The internal firewall protects the private network, which is separated from the DMZ, even if a system within the DMZ is compromised.
- **Protection against IP spoofing:** In some circumstances, attackers try to get around access control limits by impersonating another device on the network by spoofing a permitted IP address.

V.2. Static IP

A static IP address is a 32-bit number that is assigned to a computer to use as an internet address. An internet service provider will usually supply this number in the form of a dotted quad (ISP).

A device's IP address (internet protocol address) serves as a unique identity when it connects to the internet. IP addresses are used by computers to locate and communicate with one another over the internet, much like phone numbers are used by individuals to locate and communicate with one another over the phone. An IP address can reveal details about the hosting provider as well as geographic location data (Gillis, 2020).

V.2.1. USAGE

- Businesses that use IP addresses for mail, and web servers could have a single address that never changes.
- For hosting voice over IP, VPNs, and gaming, static IP addresses are preferred.
- They stable in the event of a connectivity outage, ensuring that packet exchanges are not missed.
- They enable speedier file uploads and downloads on file servers.
- A device with a static IP address does not need to make renewal requests.
- When it comes to maintaining servers, network administrators may find it easier to keep static IP addresses.
- Administrators can keep track of internet traffic and grant access to users depending on their IP addresses.

V.2.2. SECURITY FUNCTIONS

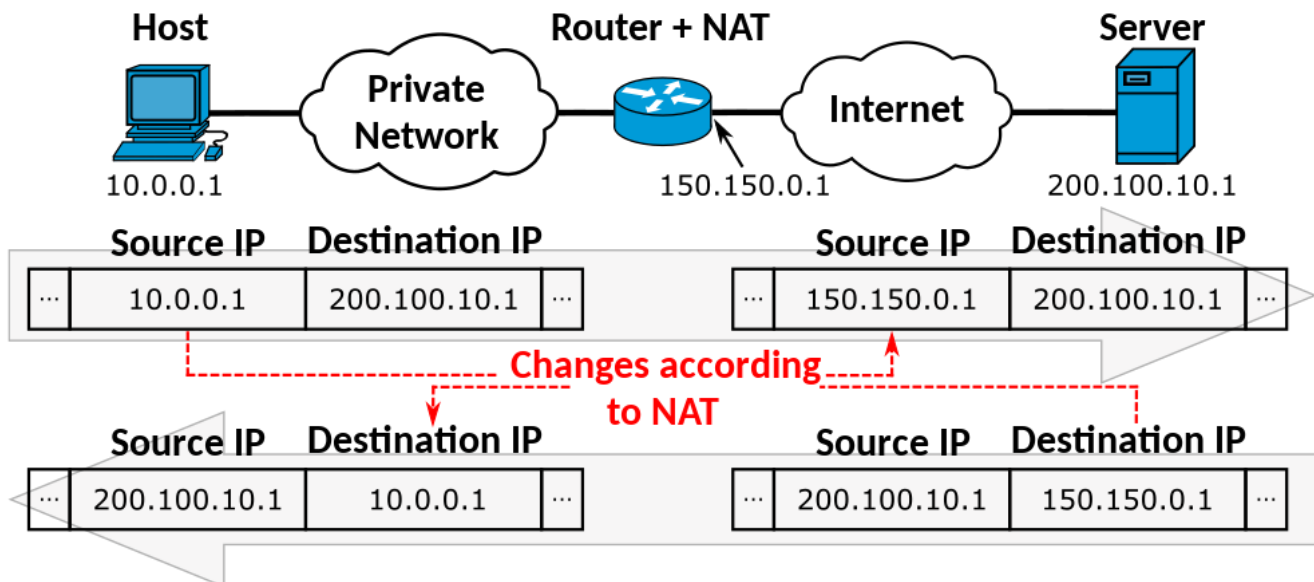
Implementing a router firewall, security suite, or VPN can assist alleviate security flaws discovered in dynamic IP addresses. A VPN, for example, might mask your network address, making it more difficult to track down a device's physical location (Gillis, 2020).

V.3. NAT

The goal of network address translation (NAT) is to allow many devices to connect to the Internet using a single public address. This necessitates the conversion of a private IP address to a public IP address. In order to give Internet connectivity to local hosts, Network Address Translation (NAT) is a procedure in which one or more local IP addresses are translated into one or more global IP addresses and vice versa (saurabhsharma56, 2021).

V.3.1. USAGE

NAT converts a local (private) IP address to a global (public) IP address when a packet travels outside the local (inside) network. The global (public) IP address of a packet is changed to a local (private) IP address when it reaches the local network. NAT generally operates on a router or firewall.



V.3.2. SECURITY FUNCTIONS

According to Saurabh Sharma (2021), NAT have three big advantage security function:

- NAT protects legitimately assigned IP addresses.
- It ensures anonymity by masking the device's IP address when sending and receiving traffic.
- When a network evolves, address renumbering is no longer necessary.

VI. CONCLUSION

In this report I have introduce about security threat, security procedures, firewall & IDS, and also DMZ, static IP, and NAT. All of the junior staff members will get to know how to identifying IT security risks together. My work here is done, I am looking forward to perform future projects.

VII. REFERENCES

- Check Point. (2021, May 20). *Misconfiguration of third party cloud services exposed data of over 100 million users*. Retrieved from Check Point:
<https://blog.checkpoint.com/2021/05/20/misconfiguration-of-third-party-cloud-services-exposed-data-of-over-100-million-users/>
- Fandom. (2022, February 20). *The IT Law Wiki*. Retrieved from Fandom:
https://itlaw.fandom.com/wiki/Threat_agent
- Gillis, A. S. (2020, March 15). *static IP address*. Retrieved from TechTarget:
<https://whatis.techtarget.com/definition/static-IP-address>
- Holmes, A. (2021, April 3). *533 million Facebook users' phone numbers and personal data have been leaked online*. Retrieved from Business Insider: <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4?r=DE&IR=T>
- Johansen, A. G. (2021, June 17). *What is a firewall? Firewalls explained and why you need one*. Retrieved from Norton: <https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html>
- Lamb, M. (2019, February 27). *7 Threat Agents Your Cyber Security Team Should Be Aware Of*. Retrieved from The Data Guardians: <https://www.thdataguardians.co.uk/2019/02/27/7-threat-agents-your-cyber-security-team-should-be-aware-of/>
- Lutkevich, B. (2021, October 15). *DEFINITION*. Retrieved from TechTarget:
<https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system>
- Lutkevich, B. (2021, July 15). *DMZ in networking*. Retrieved from TechTarget:
<https://www.techtarget.com/searchsecurity/definition/DMZ>
- Matsuura, C. J. (2013, September 1). *Corporate Counsel Connect collection*. Retrieved from Thomson Reuters: <https://store.legal.thomsonreuters.com/law-products/news-views/corporate-counsel/tips-for-protecting-your-organizations-data>
- Morris, C. (2021, June 30). *Massive data leak exposes 700 million LinkedIn users' information*. Retrieved from Fortune: <https://fortune.com/2021/06/30/linkedin-data-theft-700-million-users-personal-information-cybersecurity/>

Rapid7. (2017, January 11). *The Pros & Cons of Intrusion Detection Systems*. Retrieved from RAPID7:
<https://www.rapid7.com/blog/post/2017/01/11/the-pros-cons-of-intrusion-detection-systems/>

saurabhsharma56. (2021, December 13). *Network Address Translation (NAT)*. Retrieved from
GeeksforGeeks: <https://www.geeksforgeeks.org/network-address-translation-nat/>

Touhid. (2019, July 28). *Common Types of Security Threats to Organizations*. Retrieved from Cyber
Threat & Security Portal: <https://cyberthreatportal.com/types-of-security-threats-to-organizations/>

Wilson, B. (2021, May 12). *Why Firewall Misconfigurations Are Putting Your Clients At Risk*. Retrieved
from XAAS Journal: <https://www.xaasjournal.com/why-firewall-misconfigurations-are-putting-your-clients-at-risk-in-2020/>

Index of comments

1.1 You can remove the background of the signature with an online free background remover tool

2.1 The organizational academic Report structure is Recognized
#

Below are the comments based on your report.

P1

Identify the types of security threats to organizations.

Define threats:

Identify threats agents to organizations:

Threats agents

Mother nature

Human-agent

Natural Agents

Nations

Corporations

Organized crimes

Terrorists

Employee

List type of threats that organizations will face:

Crackers

Hackers

Malware

Viruses

What are the recent security breaches? List and give examples with dates:

Discuss the consequences of this breach:

Suggest solutions to organizations:

The threat was defined, Threats to the organization were identified in the report.

The recent security breach was listed with the date.

You did discuss the consequences and provide solutions for mitigation for the recently published breach.

P1 Pass

P2

Describe at least 3 organizational security procedures.

Organizational security procedure:

Incidence response policy

AUP Acceptable use policy

Security Policy

Human resource policy

BCP Business continuity policy

Your report did clearly iterate the policies, however, a few methods under the policy were mentioned and

Index of comments

discussed.

P2 Pass

P3

Identify the potential impact on IT security of incorrect configuration of firewall policies and IDS.

Discuss briefly firewalls and policies, their usage, and advantages in a network:
How does a firewall provide security to a network?

Show with diagrams the example of how a firewall works:

Define IDS, its usage, and show it with diagrams examples:

Write down the potential impact (Threat-Risk) of a firewall and IDS if they are incorrectly configured in a network:

Firewalls, policy, usage and advantages in a network setting were discussed. How firewalls provide security to the network was discussed. A diagram illustration was given for the firewall. The report did define IDS, usage illustrating with diagram example. The potential impact of an incorrectly configured firewall and IDS were mentioned in the report.

P3 Pass

P4

Show, using an example for each, how implementing a DMZ, static IP, and NAT in a network can improve Network Security.

Define and discuss DMZ:

DMZ usage and security function as an advantage:

Define and discuss static IP.

Static IP usage and security function as an advantage:

Define and discuss NAT:

NAT its usage and security function as an advantage:

Definition of DMZ with a brief discussion was given in the report. Usages, Security functions and advantages were all detailed in the report.

The report defined and discussed static IP with the aid of a diagram, an advantage was given for using static IP in the network environment.

NAT usage, security functions and advantages were provided in the report.

P4 Pass

M1

Propose a method to assess and treat IT security risks.

Not implemented

Index of comments

M2

Discuss three benefits to implementing network monitoring systems with supporting reasons

Not implemented

D1

Investigate how a 'trusted network' may be part of an IT security solution.

Not implemented

10 minutes of PowerPoint and additional speaker

The report contents are missing the PowerPoint presentation

Recommendation

You should be more focused on your studies, your report is having missing components.

Document formatting

Your document format, justification, fonts and size are ok.

Documents are justified.

References:

Index of comments

References are ok. However, they are not Harvard style

The report has references, however, the references provided did not conform to the Harvard style.

FrontPage:

Frontpage is ok. There are missing components such as submission dates.

You can remove the background of the signature with an online free background remover tool.

NOTE

All questions must be written clearly with the corresponding number such as P1, P2, P3, P4, followed by the answer.

All report questions must proceed with P1, P2, P3 etc.

File naming convention:

Your full name and student Id required with the course name

Filename

Assignment 1.pdf is not acceptable, please use the conventions on the right next time.

1623-GCH0123-Michael_Omar

Introduction/ Contents

The report is having an introduction.

The introduction is ok

Conclusions /

The report has a conclusion.

Your conclusion is short.