UNIVERSITY of GREENWICH
Alliance with FPT Education

BTEC

Assignment 1

Systems Security

(Hoàng Quảng Quyền GCS210314)

Date: (15/12/2022)

Ho Chi Minh City

ASSIGNMENT 1 FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	Unit 5: Security		
Submission date		**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	Hoàng Quảng Quyền	**Student ID**	GCS210314
Class	GCS1003A	**Assessor name**	Nguyễn Xuân Sâm
Student declaration 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.			
		Student's signature	

Grading grid

P1	P2	P3	P4	M1	M2	D1

☼ Summative Feedback:	☼ Resubmission Feedback:

Grade:	Assessor Signature:	Date:
Lecturer Signature:		

Higher National Certificate/Diploma in Computing

Student Name/ID Number:	
Unit Number and Title:	**Unit 5: Security**
Academic Year:	**2022 – 2023**
Unit Assessor:	
Assignment Title:	**Security Presentation**
Issue Date:	**April 1st, 2021**
Submission Date:	
Internal Verifier Name:	
Date:	

Submission Format:

Format:

- The submission is in the form of an individual written report. This should be written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research and referenced using the Harvard referencing system. Please also provide a bibliography using the Harvard referencing system.

Submission

- Students are compulsory to submit the assignment in due date and in a way requested by the Tutor.
- The form of submission will be a soft copy posted on http://cms.greenwich.edu.vn/.
- Remember to convert the word file into PDF file before the submission on CMS.

Note:

- The individual Assignment *must* be your own work, and not copied by or from another student.
- If you use ideas, quotes or data (such as diagrams) from books, journals or other sources, you must reference your sources, using the Harvard style.
- Make sure that you understand and follow the guidelines to avoid plagiarism. Failure to comply this requirement will result in a failed assignment.

Unit Learning Outcomes:

LO1 Assess risks to IT security.

LO2 Describe IT security solutions.

Assignment Brief and Guidance:

Assignment scenario

You work as a trainee IT Security Specialist for a leading Security consultancy in Vietnam called FPT Information security FIS.

FIS works with medium sized companies in Vietnam, advising and implementing technical solutions to potential IT security risks. Most customers have outsourced their security concerns due to lacking the technical expertise in house. As part of your role, your manager Jonson has asked you to create an engaging presentation to help train junior staff members 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.

Tasks

In addition to your presentation, you should also provide a detailed report containing a technical review of the topics covered in the presentation.

Your presentation should:

- Identify the security threats FIS secure may face if they have a security breach. Give an example of a recently publicized security breach and discuss its consequences
- Describe a variety of organizational procedures an organization can set up to reduce the effects to the business of a security breach.
- Propose a method that FIS can use to prioritize the management of different types of risk
- Discuss three benefits to FIS of implementing network monitoring system giving suitable reasons.
- Investigate network security, identifying issues with firewalls and IDS incorrect configuration and show through examples how different techniques can be implemented to improve network security.
- Investigate a 'trusted network' and through an analysis of positive and negative issues determine how it can be part of a security system used by FIS.

Your detailed report should include a summary of your presentation as well as additional, evaluated or critically reviewed technical notes on all of the expected topics.

Learning Outcomes and Assessment Criteria (Assignment 1):			
Learning Outcome	Pass	Merit	Distinction

LO1	**P1** Identify types of security threat to organisations. Give an example of a recently publicized security breach and discuss its consequences. **P2** Describe at least 3 organisational security procedures.	**M1** Propose a method to assess and treat IT security risks.	**D1** Investigate how a 'trusted network' may be part of an IT security solution.
LO2	**P3** Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS. **P4** Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.	**M2** Discuss three benefits to implement network monitoring systems with supporting reasons.	

Table of Contents

Task 1 - Identify types of security threat to organisations. Give an example of a recently publicized security breach and discuss its consequences. 9
1. Definition of cyber threats 9
2. Threats agents to organizations 9
3. Type of threats that organizations will face 10
a. Insider threats 10
b. Viruses and worms 11
c. Botnets 11
d. Drive-by download attacks 12
e. Phishing attacks 12
f. Distributed denial-of-service (DDoS) attacks 13
4. The recent security breaches, consequences and solution to organizations. 13
a. Some recent security breaches and consequeces 13
b. Solution 14
Task 2 - Describe organisational security procedures 15
1. Security procedures 15
a. Definition 15
b. Purpose 16
2. Some security procedures 16
Task 3 - Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS 16
1. Firewall policies 16
a. Definition 16
b. Usage 17
c. Advantages in a network 17
2. How does a firewall provide security to a network 18
3. Diagrams the example of how firewall works 20
1. Firewall diagram 20
2. How does firewall work 20
4. IDS 21
a. Definition 21
b. Usage 21
c. Diagrams 22
5. The potential impact (Threat-Risk) of a firewall and IDS if they are incorrectly configured in a network 22

Task 4 - Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security....24
1.DMZ....24
a. Definition....24
b. Usage....24
c. Advantages....25
2. IP....26
a. Definition....26
b. Usage....26
c. Advantages....26
3. NAT....27
a. Definition....27
b. Usage....28
c. Advantages....28
REFERENCES....30

Table of Figure

Figure 1: Threats to network security....9
Figure 2: Threat Agent Categories....10
Figure 3: Insider threats....10
Figure 4: Computer Worms and Virus....11
Figure 5: Botnets....11
Figure 6: Drive-by download attacks....12
Figure 7: Phishing attacks....12
Figure 8: DDoS Attack....13
Figure 9: Firewall Policy....17
Figure 10: Firewall allowing Good Traffic....19
Figure 11: Firewall blocking Bad Traffic....19
Figure 12: Firewall Network Diagram....20
Figure 13: IDS....21
Figure 14: Diagram of IDS....22
Figure 15: DMZ Working....24
Figure 16: Usage of IP....26
Figure 17: Network address translation....27

Task 1 - Identify types of security threat to organisations. Give an example of a recently publicized security breach and discuss its consequences.

1. Definition of cyber threats

A malicious act that aims to destroy data, steal data, or otherwise interfere with digital life is referred to as a cyber or cybersecurity threat. Computer viruses, data breaches, DoS assaults, and other attack methods are examples of cyberthreats.

Figure 1: Threats to network security

Cyber threats also refer to the potential for a successful cyber assault with the intent of stealing sensitive data, damaging or disrupting a computer network, or gaining unauthorized access to an information technology asset. Cyberthreats may originate from a company's own trusted employees or may come from distant, unidentified parties.

2. Threats agents to organizations

A party who causes harm to an organization or attempts to do so is known as a threat actor or threat agent. Threat actors can have a variety of goals and might be internal, external, or partners in relation to their target.

Threat actors, also known as malevolent actors, can be individuals, teams, or entire entities. The most prevalent and dangerous actors are those who pose an external threat because, unlike other actors, the security events they cause are nearly always deliberate. Furthermore, external threat actors are more likely to act maliciously than maliciously for fun or "hacktivism"

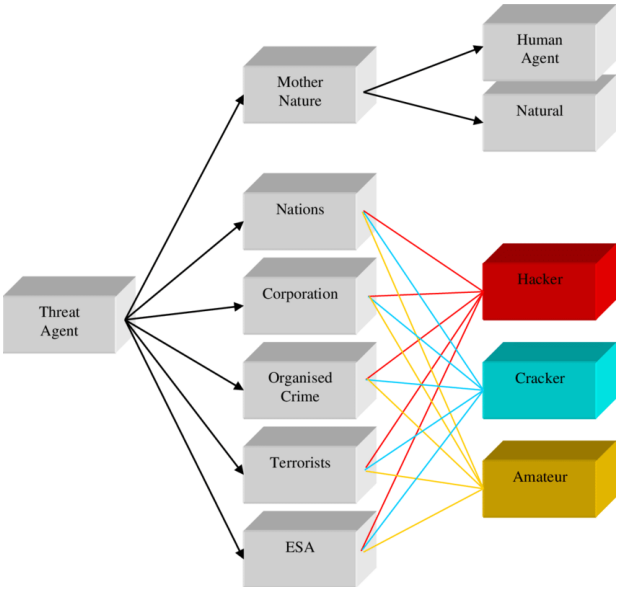

Figure 2: Threat Agent Categories

3. Type of threats that organizations will face

a. Insider threats

An insider threat arises when people affiliated with an organization who are granted permission to access its network inadvertently or intentionally misuse that access to harm the organization's vital information or systems.

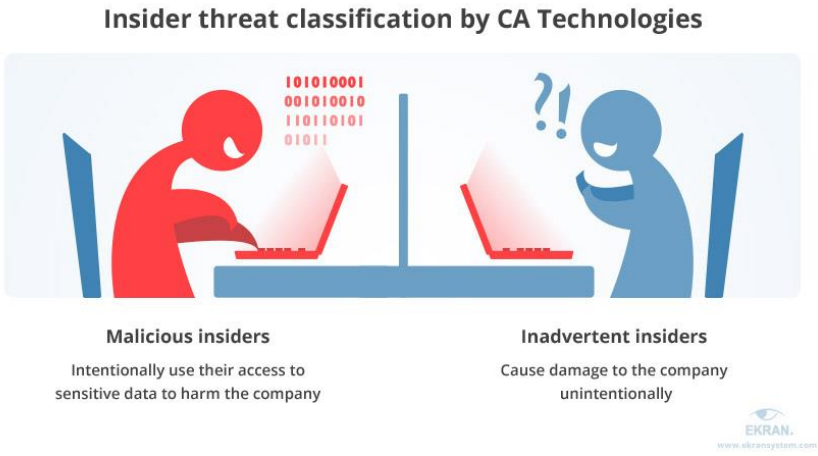

Figure 3: Insider threats

Insider threats are created by negligent employees that don't follow the business norms and regulations of their firms. For instance, individuals might unintentionally click on phishing links in emails, disclose their login information with others, or email consumer data to other parties. Other insider dangers come from vendors, partners in business, and contractors.

Some insiders purposefully evade security precautions out of convenience or inane attempts to increase productivity. Malicious insiders purposefully circumvent cybersecurity measures in order to destroy data, steal data to sell or exploit later, disrupt business operations, or do other harm.

b. Viruses and worms

Figure 4: Computer Worms and Virus

Malicious software (malware) such as viruses and worms is designed to harm a company's systems, data, and network. A computer virus is a piece of malicious software that spreads by copying itself onto a host file, system, or other application. It does not propagate until it is intentionally or unintentionally activated, without the knowledge or consent of a user or system administrator.

A computer worm is a self-replicating program that spreads without the need for human interaction or to copy itself to a host program. Its primary purpose is to spread infection while active on the compromised system. Invisible to the user, automatic operating system components are frequently used by worms to spread. When a worm enters a system, it immediately begins to replicate, infecting unprotected computers and networks.

c. Botnets

A group of Internet-connected devices, such as PCs, smartphones, servers, and IoT devices, that have been infected and are being remotely controlled by a common form of malware is known as a botnet. The botnet software typically scours the internet for susceptible devices.

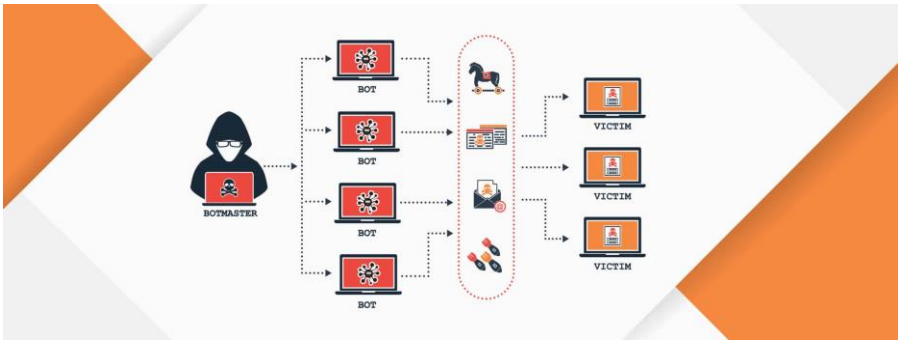

Figure 5: Botnets

The threat actor who builds a botnet wants to infect as many connected devices as they can, taking advantage of their computational power and resources for automated actions that are typically hidden from the users of the devices. These botnets are controlled by threat actors, who are frequently cybercriminals. They are used to send spam emails, run click-fraud campaigns, and produce malicious traffic for distributed denial-of-service attacks.

d. Drive-by download attacks

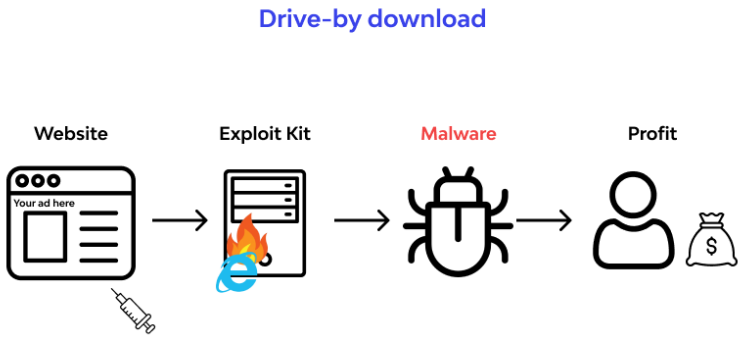

Figure 6: Drive-by download attacks

Malicious code is downloaded from a website using a browser, app, or integrated operating system in a drive-by download attack without the user's knowledge or consent. The download is activated without the user having to click on anything. A download can begin just by opening a website or browsing it. Drive-by downloads are a common method used by cybercriminals to infect endpoints with exploit kits, other malware, and banking Trojans as well as to steal and collect personal information.

e. Phishing attacks

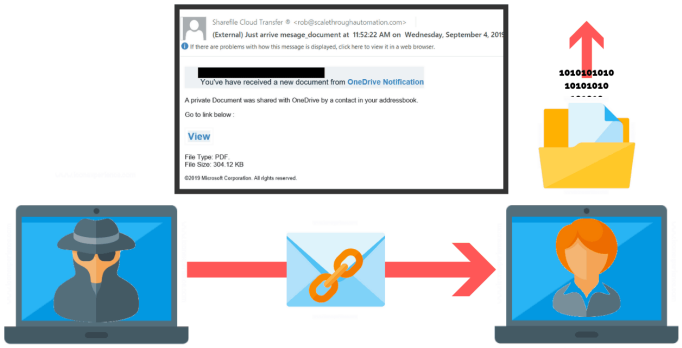

Figure 7: Phishing attacks

Phishing is a form of information security threat that uses social engineering to persuade users to disregard standard security procedures and divulge private data, including names, addresses, login credentials, Social Security numbers, credit card numbers, and other financial information. The majority of the time, hackers send out phony emails that appear to be from reliable sources like financial institutions, eBay, PayPal, and even friends and coworkers.

Hackers use phishing attacks to trick users into performing a recommended action, such as clicking on links in emails that direct them to phony websites that solicit personal information or download malware onto their devices. Opening email attachments can also lead to the installation of malware on users' devices that is intended to gather private data, send emails to contacts, or grant remote access to their devices.

f. Distributed denial-of-service (DDoS) attacks

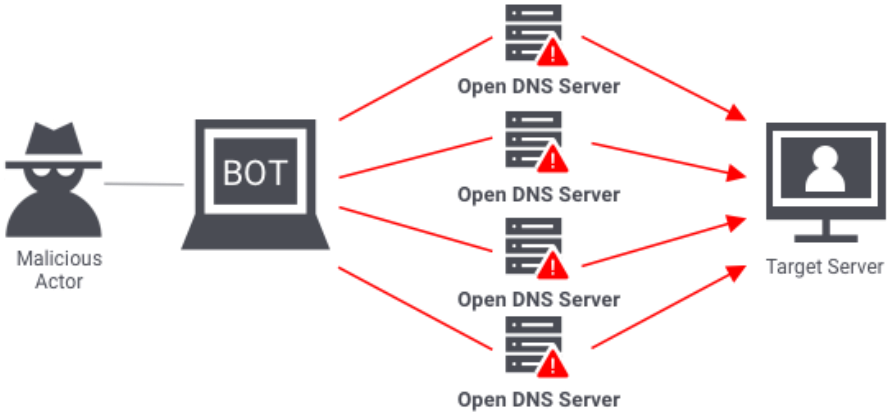

Figure 8: DDoS Attack

Multiple compromised machines attack a target, such as a server, website, or other network resource, in a distributed denial-of-service (DDoS) attack, rendering the target completely inoperable. The target system is forced to slow down or crash and shut down due to the barrage of connection requests, incoming messages, or malformed packets, depriving legitimate users or systems of service.

4. The recent security breaches, consequences and solution to organizations.

a. Some recent security breaches and consequeces

1. *MediBank: October 2022*

On October 25, 2022, health insurance MediBank disclosed that over 4 million of their clients' data had been compromised. The name, address, date of birth, and even the insurance card numbers might have been accessed, according to the Australian health insurer.

MediBank stated that it would provide compensation to people who were harmed as a result of their private information being obtained in order to set things right. Between $25M and $35M is the projected cost of this cyberattack to the business. After conducting an investigation and increasing network monitoring, they discovered the hacker was gone.

2. *Uber: September 2022*

Mid-September saw the announcement that one of the biggest companies in the world, Uber, had been hacked: "I am a hacker and Uber has suffered a data breach," followed by a number of emojis. In order to investigate the incident further, the company had to shut down its internal messaging system and engineering systems.

In addition, the hacker asserted that it was possible to access several of the company's databases, including the communications data. Uber contacted law enforcement after learning that a worker's account had been hijacked. Uber had previously experienced a cyber attack but failed to notify it, which resulted in a court dispute and costly fees. In an effort to prevent a repeat of this circumstance, they were honest and took the necessary safeguards this time.

3. *Plex: August 2022*

Millions of people use the media server app Plex, which suffered a data breach in August that exposed sensitive encrypted information about its users, including passwords, usernames, and emails. The access to the personal information of millions of people can harm a brand's reputation for years to come.

Despite the fact that the vulnerability has been fixed and secured, Plex continues to urge users to change their passwords and enable multi-factor authentication. To safeguard yourself against data breaches in 2022, this should once again be considered standard procedure.

4. Crypto.com Breach: January 2022

One of the most secure methods of transaction processing is the blockchain model, which has long been acknowledged as such. Despite this, hackers continue to try to breach crypto-based transactions. This was demonstrated by the attack on Crypto.com on January 17, 2022, which was directed at the wallets of 483.

Approximately $18 million worth of bitcoin and $15 million worth of Ethereum, along with other cryptocurrencies, were taken as part of this hack. The ability of the hackers to get past two-factor authentication and access users' wallets was largely responsible for this being made possible. Another illustration of the value of using a password manager.

Crypto.com initially brushed it off as merely a "incident," but later withdrew that claim, admitting that money had indeed been taken and that the affected users had been compensated. The business added that it had reviewed its systems and worked to strengthen its security posture.

Businesses need to understand the dangers of cryptocurrency theft. Having all sensitive data encrypted is the best defense against this kind of fraud.

b. Solution

1. Limit who has access to your most important data:

Previously, every employee had access to every file on their computer. Companies today are learning the hard way to restrict access to their more important data. There is no reason for a mailroom employee to see a customer's financial information, after all. You reduce the number of workers who might unintentionally click on a hazardous link by limiting who is permitted to read specific papers. Expect to see all corporate records partitioned off in the future so that only those who expressly require access will have it. One of those obvious fixes that businesses probably ought to have been using all along.

2. Third-party vendors must comply:

Every firm interacts with a variety of outside vendors. The need to understand who these people are has never been greater. Even permitting visitors onto their property might expose businesses to legal action. What if the person who delivers office supplies was recently released from jail? It's a thought to ponder. Also, make sure to restrict the kinds of documents that these vendors can access.

Although taking such steps can be a bother for the IT department, the alternative could be a data breach that costs millions of dollars. Demand transparency from the businesses that are permitted to access your sensitive information. Don't just assume that they are abiding by privacy laws; verify it. Request background checks from any outside vendors who frequently enter your business. If CEOs are serious about bringing about change, they must become tougher on security.

3. Conduct employee security awareness training:

Employees are the weakest link in the data security chain, according to recent research. Despite training, workers read dubious emails with the potential to download malware every day. Employers make the error of assuming that one cybersecurity training session is sufficient. Schedule regular classes every quarter or even monthly if you're serious about protecting your crucial data.

Employees have been known to leave those classes, head back to their offices, and open shady emails without a second thought. According to marketing studies, the majority of consumers must hear the same message at least seven times before their behavior starts to change.

4. **Update software regularl:**

Professionals advise routinely updating all operating systems and application software. When patches are available, install them. When programs aren't constantly patched and updated, your network is exposed. Baseline Security Analyzer, a product from Microsoft, can now be used to periodically check that all programs are patched and current. This is a simple and affordable way to fortify your network and thwart attacks before they start.

5. **Develop a cyber breach response plan:**

Few companies have a sound breach response plan in place. Employers should be very transparent concerning the scope of the breach. Developing a comprehensive breach preparedness plan enables both the employees and the employer to understand the damages that could occur. The government's OPM break-in was handled very poorly.

6. **Difficult to decipher passwords:**

Businesses rarely intervened in the frequency of password changes required of their employees in the past. Recent cyberattacks have altered everything. One thing that security professionals will emphasize when they visit your organization to train your staff is the importance of routinely changing all passwords. The majority of people are now aware of how crucial it is to make passwords challenging to crack. We have mastered the use of capital letters, numbers, and special characters when creating passwords, even on our home PCs. Make it as difficult as you can for burglars to enter and steal your belongings.

Task 2 - Describe organisational security procedures

1. Security procedures

a. Definition

A security procedure is a predetermined flow of steps that must be taken in order to carry out a certain security duty or function. In order to achieve a goal, procedures are typically composed of a sequence of actions that must be carried out repeatedly and consistently. Security procedures offer a set of documented activities for managing the organization's security concerns after they are put into place, which will aid in training, process auditing, and process improvement. In order to establish the consistency required to reduce variation in security processes and strengthen control of security inside the business, procedures give a starting point. Another effective strategy for cutting waste, raising quality, and boosting productivity in the security division is to reduce variation.

b. Purpose

Security procedures are to be followed each time a security control or business process needs to be implemented. There is risk in relying on memory to execute the checklist as there could be some distraction. The best option would be to automate the hardening procedure through scripts or other automation tools.

2. Some security procedures

a. Change Management Policy

A structured procedure for making changes to IT, software development, and security services/operations is referred to as a "change management policy." An organization's proposed changes should be better known and understood throughout the organization, and all changes should be implemented systematically to reduce any negative effects on products and services.

b. Incident Response (IR) Policy

The incident response policy outlines how the business will handle incidents and lessen their negative effects on operations. CISOs wish they never had to apply this particular policy. The aim of this policy, however, is to outline the procedure for handling an incident with a view to minimizing harm to business operations and clients as well as to cut down on recovery time and costs.

c. Disaster Recovery Policy

The development of an organization's disaster recovery plan typically involves input from both the IT and cyber security teams and is a component of the larger business continuity plan. The incident response policy will be used by the CISO and teams to handle an incident. The Business Continuity Plan will be put into action if the incident has a significant financial impact.

Task 3 - Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS

1. Firewall policies

a. Definition

An program (software) or appliance (hardware and software) called a firewall is created to manage the flow of Internet Protocol (IP) traffic to and from a network or piece of electronic equipment. Using rules outlined in the firewall's ruleset, firewalls are used to inspect network traffic and enforce policies. A technique to stop criminal activity and attacks on computing resources and network-accessible data includes firewalls as one of its components. Antivirus software, intrusion detection software, patch management, secure passwords and passphrases, and spyware detection tools are a few additional elements.

Typically, firewalls fall under the "Network" or "Host" categories: A Host Firewall is typically an application that addresses a single host (such as a personal computer)

separately. A Network Firewall is typically an appliance connected to a network for the purpose of regulating access to one or more hosts, or subnets. Network and host firewalls can and frequently are used together.

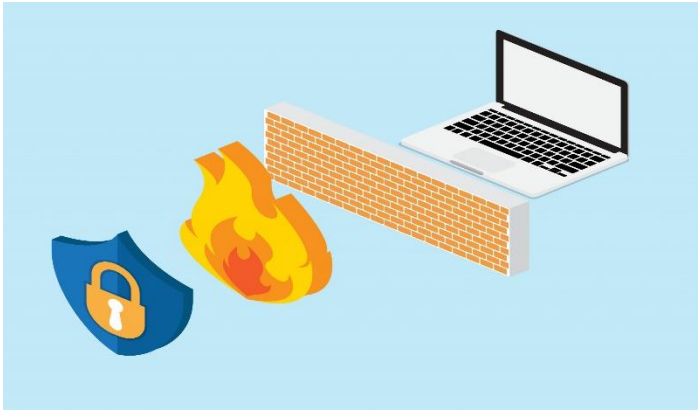

Figure 9: Firewall Policy

The purpose of this policy statement is to:

- Give instructions on when firewalls are necessary or advised. In all situations where sensitive data is kept or processed, a network firewall is necessary; in all situations where the operating environment permits the installation, a host firewall is necessary. The same operating environment is protected by both the Network and Host Firewalls, and the redundancy of controls (two separate and different firewalls) adds extra security in the case of a breach or failure.
- Inform people on the significance of a firewall that has been installed and maintained correctly.

b. Usage

Firewalls are used **to examine network traffic and enforce policies based on instructions contained within the Firewall's Ruleset**. Firewalls represent one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information.

c. Advantages in a network

1. Monitors Network Traffic

Monitoring network traffic is the first of many firewall security advantages. Threats have opportunities to compromise your operations thanks to the data that enters and leaves your systems. Firewalls use pre-made rules and filters by monitoring and analyzing network traffic to keep your systems safe. You can control your levels of protection based on what you see entering and leaving your firewall if your IT staff is properly trained.

2. Stops Virus Attacks

A viral attack can stop your digital operations more quickly and severely than anything else. You must set up the defenses to protect your systems because there are thousands of new threats created every single day. Controlling system entry points and preventing virus attacks is one of the most obvious advantages of firewalls. Depending on the virus, the damage caused by an attack on your systems could be immeasurably high.

3. Prevents Hacking

Unfortunately, as businesses increasingly rely on digital operations, thieves and other bad guys are encouraged to follow suit. Firewalls are now even more crucial as data theft and hostage-taking by criminals have increased because they stop hackers from accessing your data, emails, systems, and other things without your permission. A firewall can completely stop a hacker or convince them to pick an easier target.

4. Stops Spyware

Stopping spyware from entering your systems is a crucial benefit in today's data-driven society. The entry points criminals can use to access your systems increase as systems get more robust and complicated. The use of spyware and malware, which are programs made to infiltrate your systems, take control of your computers, and steal your data, is one of the most typical ways that unauthorized people gain access. An essential barrier against these malicious programs is provided by firewalls.

5. Promotes Privacy

The promotion of privacy is a general advantage. You create a private environment that your clients can rely on by actively trying to keep your data and the data of your customers secure. Nobody enjoys having their data stolen, particularly when it is obvious that precautions could have been taken to avoid the intrusion.

Upgraded data-protection systems can also give businesses a competitive edge and help them sell their services to clients and customers. The advantage grows as your company deals with more sensitive data.

2. How does a firewall provide security to a network

Firewalls within a private network filter network traffic, as was already explained. Based on a set of rules, it analyzes which traffic should be permitted or limited. Consider the firewall as a gatekeeper at the point where your machine enters the network, allowing only trusted IP addresses or sources to do so.

Only incoming traffic that has been set up to be accepted by the firewall is accepted. Based on previously set security criteria, it distinguishes between legitimate and malicious communication and either permits or bans particular data packets.

The source, destination, content, and other characteristics of the packet data are among the factors on which these rules are based. To stop cyberattacks, they restrict traffic coming from unknown sources.

For instance, the illustration below demonstrates how a firewall permits beneficial traffic to pass through to the user's private network.

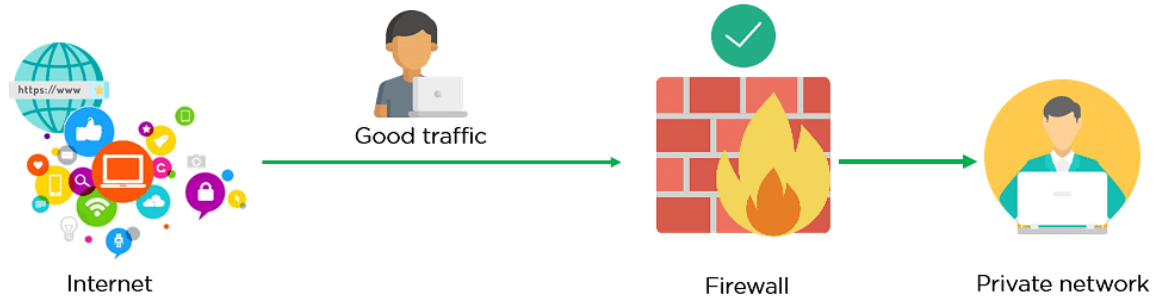

Figure 10: Firewall allowing Good Traffic

However, in the illustration below, the firewall prevents harmful traffic from gaining access to the private network, shielding the user's network from potential cyberattacks.

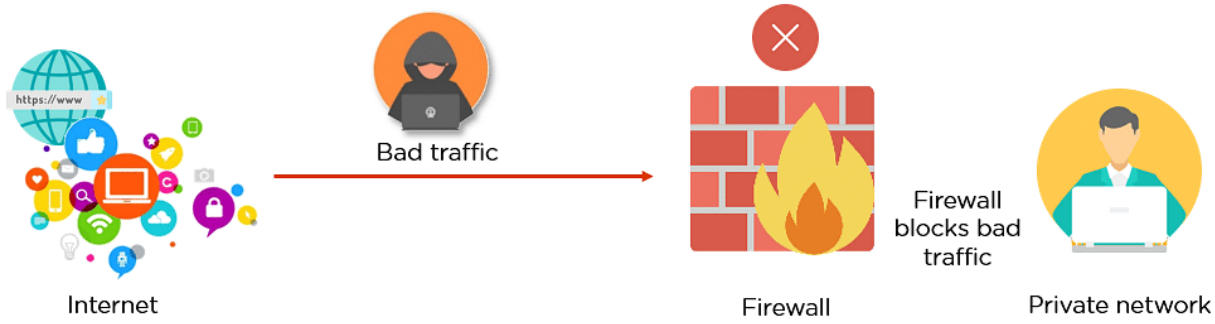

Figure 11: Firewall blocking Bad Traffic

A firewall performs fast analyses in this manner to find malware and other shady activity.

To read data packets at various network levels, there are numerous types of firewalls. You will now continue with this tutorial's following section and learn about the various kinds of firewalls.

3. Diagrams the example of how firewall works

1. Firewall diagram

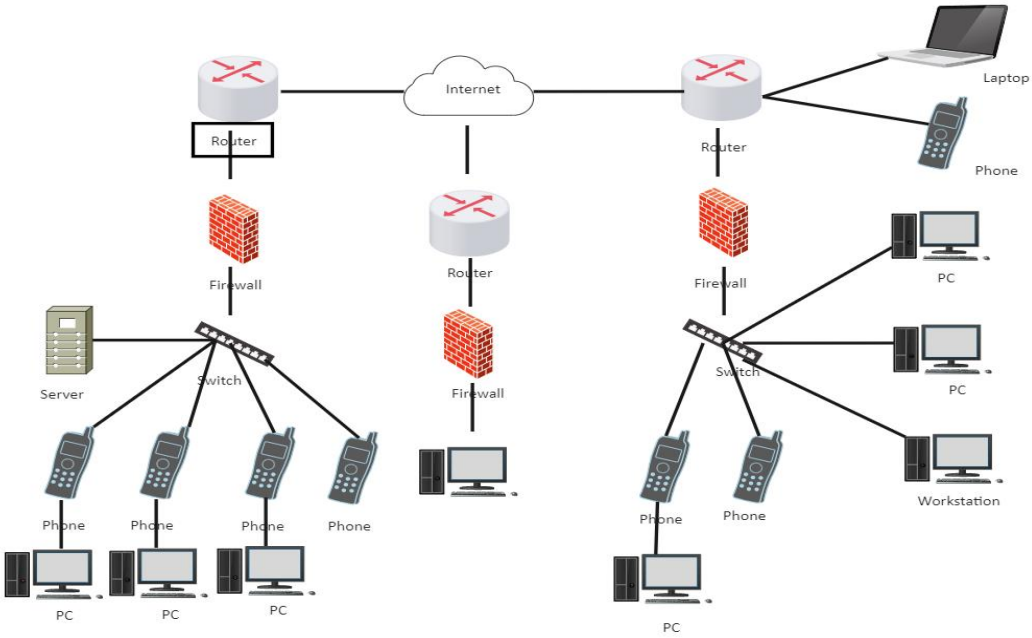

Figure 12: Firewall Network Diagram

2. How does firewall work

By blocking malicious or superfluous network traffic, firewalls defend your computer or network from outside cyberattacks. Additionally, firewalls can stop harmful software from connecting to a computer or network over the internet. Firewalls can be set up to permit relevant and essential data through while blocking data from specific locations (i.e., computer network addresses), applications, or ports. (For more information, see Understanding Denial-of-Service Attacks.)

4. IDS

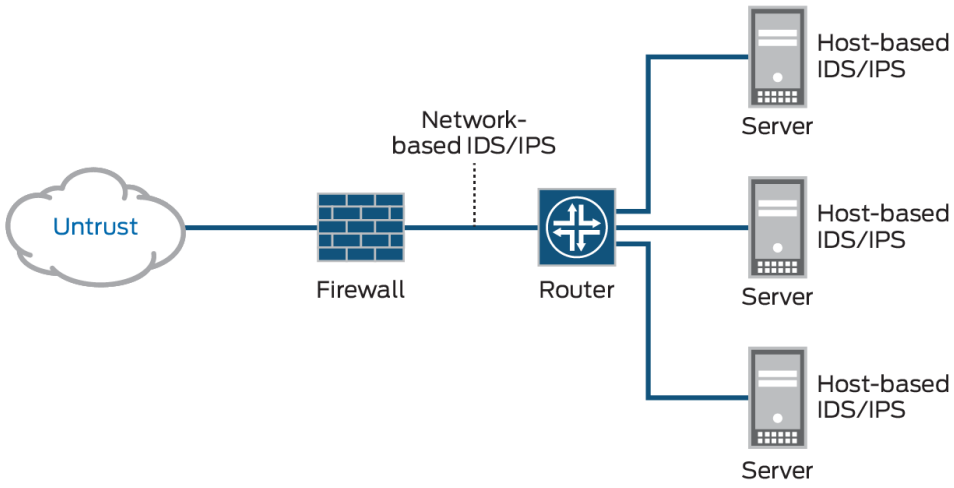

Figure 13: IDS

a. Definition

Software designed particularly to monitor network traffic and spot anomalies is known as an intrusion detection system (IDS). Network changes that are unexpected or inexplicable could be signs of malicious activity at any level, from the start of an assault to a full-blown breach. The two primary types of intrusion detection systems (IDS) are as follows:

- With the help of all packet metadata and contents, a network intrusion detection system (NIDS) detects intrusions throughout the whole network.
- A host-based intrusion detection system (HIDS) analyzes network traffic and system logs to and from a specific device and implements intrusion detection through a specific endpoint.

The best intrusion detection systems are designed to collect network traffic from all devices using NIDS and HIDS, increasing the likelihood that intrusions will be discovered throughout your IT infrastructure.

b. Usage

Before hackers may harm your network infrastructure, an intrusion detection system is a monitor-only application designed to find and report irregularities. IDS is either set up on a client system or your network (host-based IDS).

The majority of intrusion detection systems scan for well-known attack signatures or unusual departures from predetermined standards. The protocol and application layers of the OSI (Open Systems Interconnection) model are then contacted to further investigate these anomalous patterns in the network traffic.

An IDS is installed within your network infrastructure outside of the real-time communication band (a path connecting the information sender and receiver) to function as a detection system. In order to ensure that the streaming traffic is not malicious or otherwise spoofed, it instead uses a SPAN or TAP port for network monitoring and analyzes a copy of inline network packets (fetched through port mirroring). The IDS effectively detects infected components like corrupted data packets, DNS poisonings,

Xmas scans, and more that have the potential to affect the performance of your entire network.

c. Diagrams

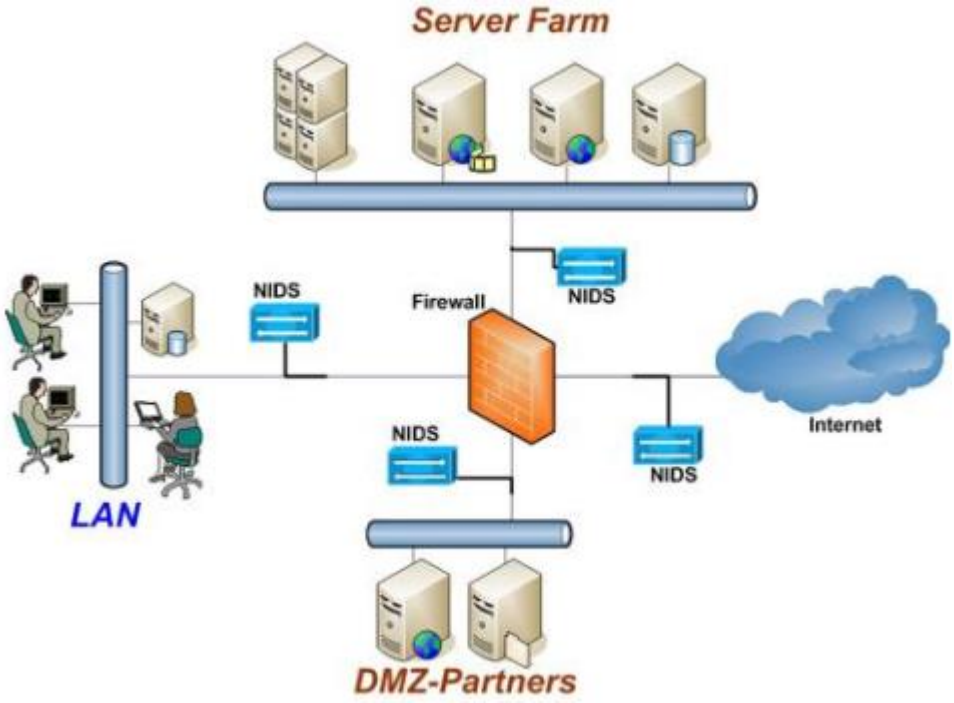

Figure 14: Diagram of IDS

5. The potential impact (Threat-Risk) of a firewall and IDS if they are incorrectly configured in a network

Insider Attacks:

An external network assault is one that a perimeter firewall is designed to thwart. What occurs then if the attack originates from within? Since the attacker is already on your system, the perimeter firewall usually becomes useless.

Firewalls can still be helpful, even if an attack comes from within your network, IF you also have internal firewalls in addition to perimeter firewalls. Internal firewalls aid in segmenting specific network assets so that attackers must exert more effort to transfer from one system to another. By doing this, you give yourself additional time to react to the attack while also extending the attacker's breakout time.

Missed Security Patches:

When network firewall software isn't correctly handled, this problem occurs. Attackers can take advantage of flaws in any software program; firewall programs are no different from other software in this regard. When firewall providers find these flaws, they often work to quickly develop a patch to address the issue.

The firewall application at your firm won't automatically receive the patch just because it exists. The vulnerability is still present and ready for exploitation by an arbitrary attacker up until the point at which that firewall software patch is actually applied.

The best solution to this issue is to establish and adhere to a rigid patch management schedule. According to such a schedule, you (or the person in charge of your cybersecurity) should regularly check for firewall software security updates and make sure to immediately install any that are available.

Configuration Mistakes:

Even if a firewall is installed on your network and has all the most recent vulnerability fixes installed, conflicts in the firewall's configuration settings might still arise and lead to issues. In certain circumstances, this can result in a decrease in network speed for your business, while in others, a firewall may completely stop offering security.

For instance, enabling dynamic routing was once thought to be a negative choice because it leads to a loss of control and lowers security. However, some businesses leave it on, leaving a gap in their firewall defense.

The key to the main gate is hidden in a hide-a-key right next to the entrance if your firewall is poorly configured; this only makes things easier for attackers while wasting time, money, and effort on your "security" measure.

A Lack of Deep Packet Inspection:

In order to approve or refuse a packet's travel to or from a system, next-generation firewalls use the stringent Layer 7 (also known as "deep packet") inspection inspection mode.

An attacker might easily spoof this information to get around a less sophisticated firewall that only checks the data packet's place of origin and destination before allowing or rejecting a request.

Using a firewall that can do deep packet inspection to scan information packets for known malware can be the best solution for this issue.

DDoS Attacks:

Attacks using distributed denial of service (DDoS) are common and are known for being very efficient and relatively inexpensive to carry out. The primary objective is to deplete a defender's resources and bring about a shutdown or extended inability to provide services. Protocol attacks are a type of attack that aim to exhaust the resources of load balancers and firewalls in order to prevent them from processing legitimate traffic.

Firewalls can reduce some DDoS attacks, but protocol attacks can still cause them to become overloaded.

There is no quick answer for DDoS attacks because there are several attack tactics that can take advantage of various network architectural flaws in your firm. Some cybersecurity service providers provide "scrubbing" services, in which they redirect incoming traffic away from your network and separate the DDoS activity from the traffic that is actually trying to get access to your system. Then, your network receives this legitimate traffic so you can carry on with your regular business.

Firewalls by themselves are unable to shield your network from all threats. However, they can be a crucial component of a more comprehensive cybersecurity plan to protect your company.

Want to know more about creating a reliable cybersecurity plan for your company? Visit the following link to download our free guide to cybersecurity fundamentals. You can also speak with a cybersecurity professional at Compuquip Cybersecurity right away to receive professional advice.

Task 4 - Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security

1.DMZ

a. Definition

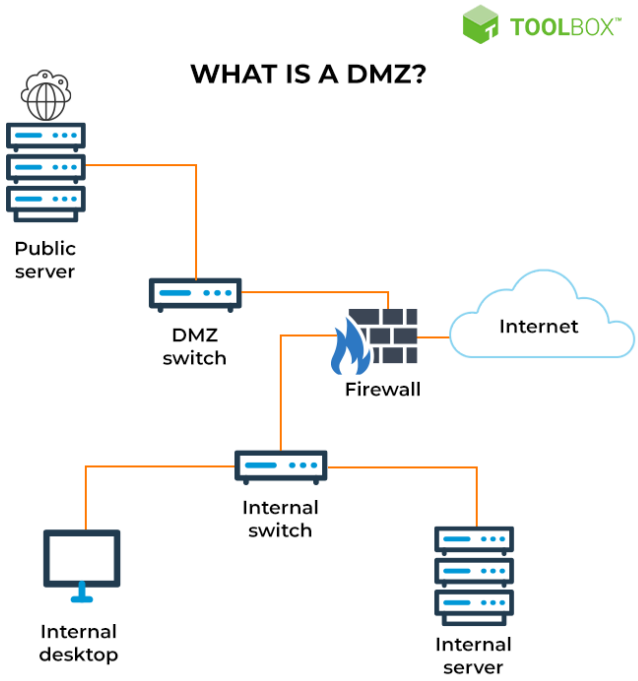

Figure 15: DMZ Working

A DMZ, or demilitarized zone, in computer security is a physical or logical subnetwork that houses and exposes an organization's external-facing services to an untrusted, typically bigger network like the Internet. It is also referred to as a perimeter network or screened subnet. A DMZ serves as an extra security measure for a company's local area network (LAN) because only the portions of the network that are exposed there can be accessed by outside network nodes, while the remainder of the network is shielded by a firewall. A small, segregated network called the DMZ serves as a bridge between the public Internet and the private network.

b. Usage

The DMZ Network was created to safeguard the hosts that are most susceptible to assault. These hosts typically host services that are accessible to users outside of the LAN, with email, web servers, and DNS servers serving as the most prevalent examples. They are put into the monitored subnetwork to help safeguard the rest of the network in case they are compromised due to the increased risk of attack.

Because the data transported through the DMZ is less secure, hosts in the DMZ have strictly regulated access permissions to other services within the internal network. To further strengthen the secured border zone, communications between hosts in the DMZ and the outside network are also limited. The firewall divides and controls all traffic shared between the DMZ and the internal network, enabling hosts in the protected network to communicate with both the internal and external networks. The DMZ will often be shielded from access by everything on the external network by a second firewall.

If a DMZ is used, all services that users can access when communicating from an external network can be placed there, and they should. The most popular services include:

- **Web servers:** Web servers may need to be put into a DMZ if they are in charge of maintaining communication with an internal database server. This contributes to the security of the internal database, which frequently houses sensitive data. The internal database server can then be accessed by the web servers either directly or through an application firewall, all the while remaining protected by the DMZ.
- **Mail servers:** Individual emails and the user database created to store login information and private messages are typically kept on servers with no direct internet access. In order to interact with and access the email database without directly exposing it to potentially hazardous traffic, an email server will be created or installed inside the DMZ.
- **FTP servers:** These enable direct file interaction and can host important content on a website for an organization. An FTP server should therefore always be only partially connected to important internal systems.

Although a DMZ configuration offers extra protection from external attacks, it typically has no effect on internal attacks like communication sniffing using a packet analyzer or spoofing using email or other methods.

c. Advantages

The main advantage of a DMZ is to give an internal network a high level of security by limiting access to servers and sensitive data. A DMZ creates a barrier between website visitors and the company's private network so they can access some services. As a result, the DMZ also provides extra security advantages like:

- Access control: Organizations can give consumers access to services outside the boundaries of their network by using the open internet. While providing network segmentation to make it more difficult for an unauthorized user to access the private network, the DMZ allows access to these services. A proxy server, which centralizes internal traffic flow and makes it easier to monitor and record that traffic, may also be present in a DMZ.
- Network reconnaissance is prevented via a DMZ, which creates a barrier between the public internet and a private network to keep hackers from scouting out potential targets. Although servers in the DMZ are open to the public, a firewall that stops an attacker from seeing inside the internal network adds an additional degree of security. The internal firewall keeps the private network secure and makes it challenging for outside reconnaissance even if a DMZ system is compromised.
- Blocking Internet Protocol (IP) spoofing: By spoofing an IP address and pretending to be a trusted device logged in to a network, attackers try to identify ways to access systems. Such spoofing efforts can be detected and stopped by a DMZ while another service confirms the IP address's validity. In addition to network

segmentation, the DMZ offers a place for traffic organization and public services access that is separate from the internal private network.

2. IP

a. Definition

A device on the internet or a local network can be identified by its IP address, which is a special address. The rules defining the format of data delivered over the internet or a local network are known as "Internet Protocol," or IP.

IP addresses, which contain location information and make devices reachable for communication, are essentially the identifier that permits information to be sent between devices on a network. There must be a way for computers, routers, and websites to be distinguished on the internet. A method for doing this is provided by IP addresses, which are crucial to the operation of the internet.

b. Usage

An IP address is used to manage the connection between gadgets that send and receive data over a network. Without an IP address, it is impossible to communicate with any device connected to the internet. IP addresses allow computing devices (like PCs and tablets) to communicate with websites and streaming services, as well as inform websites of the identity of the connecting user.

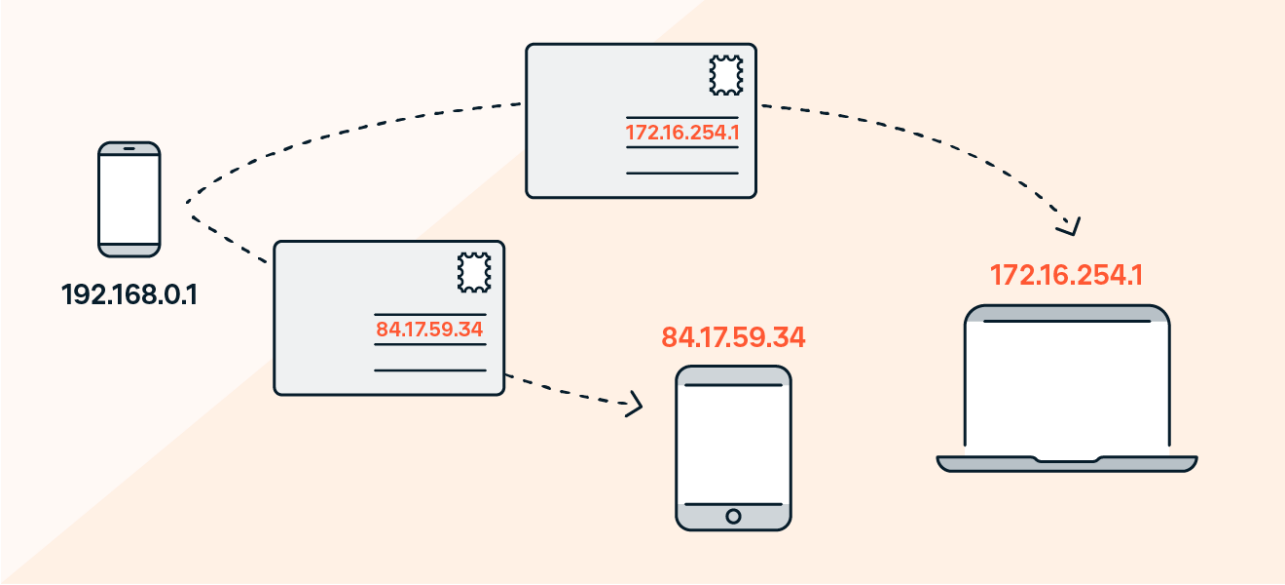

Figure 16: Usage of IP

An IP address functions similarly to a return address on mail. If you provide a return address on the envelope, you will receive the letter back if it is delivered to the incorrect address.

Email follows the same rules. Your IP address enables the business' mail server to send you a bounce message when you send an email to an invalid recipient (such as a former employee who no longer has a company email address). This message lets you know that your email wasn't delivered to the intended recipient.

c. Advantages

1.There are no additional costs associated with IP:

Every time you want to improve or adjust your business, there are no payments involved, so you can do it for free. But once the inventor has finished developing the product, it is always advised to seek for official patent protection.

2.competitive advantage over similar businesses:

IP protection invariably grants the capacity to have a competitive advantage over other businesses in the market that are identical to yours. Because the same firms in the market won't be able to replicate, use, or manufacture the same product, this will relieve stress for the companies with IP protection because it secures the running of their enterprises.

3. IP contributes to increasing a company's worth:

Through the sale or licensing of the invention, intellectual property aids in increasing revenue for the company.

4. IP helps the business market its goods and services:

It can assist in setting one business apart from the competition in order to draw in more potential clients. As a result, it helps the registered products market better.

5. Financing becomes simple to come by:

Since the IP protection increases credibility, it is simpler to get financing from financial organizations and lenders.

6. More export possibilities:

It improves one's ability to compete internationally and in export markets for goods and services

3. NAT

a. Definition

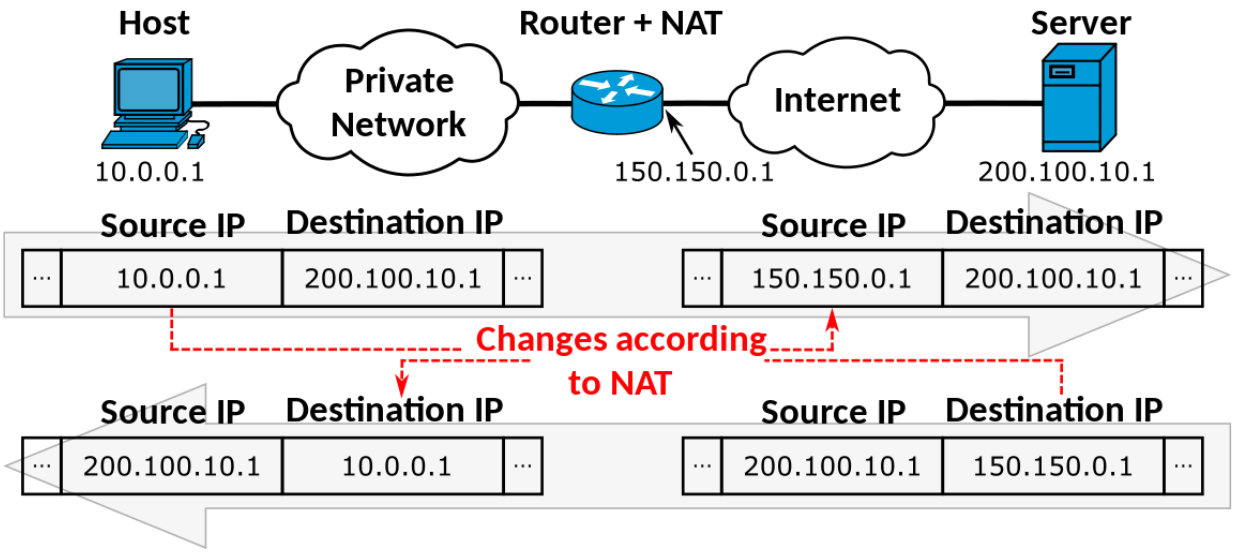

Figure 17: Network address translation

Network address translation is referred to as NAT. Before transferring the data, it is a way to map several local private addresses to a public one. Both most home routers and organizations that need multiple devices to share a single IP address use NAT.

b. Usage

Consider a laptop that is linked to a router at home. Someone uses the laptop to look up the location of their preferred restaurant. This request is sent from the laptop to the router as a packet, which the router then sends to the internet. To begin with, though, the router converts the outgoing IP address from a local private address to a public address.

Similar to sending physical mail and asking for return service but giving an anonymous return address, if the packet keeps a private address, the receiving server won't know where to send the information back to. Using NAT, the data will return to the laptop using the router's public address rather than the device's private one.

c. Advantages

1. Cost Savings

When using NAT with private IP addresses, the organizations don't need to purchase IP address for each and every computer out there. Same IP address can be used for multiple computers. Thus, this can lead to significant cost reduction.

2. Address Conserving

When the user uses NAT overload, NAT allows preserving the IPv4 address space by allowing the privatization of intranets. This especially happens through the process of Intranet Privatization. In this process all the addresses are saved by multiple applications at the port level.

3. Flexible Connection

By implementing multiple tools, backup tools and load balancing tools, NAT can overall increase the flexibility and reliability of the network. This happens when establishing to the public network or any other network connection.

4. Consistent Network

NAT provides a consistent network addressing scheme. Whenever there is a use of public IP address, there should be proper address space assigned. This is because if the network is enlarged, more of the IP address will be required.

5. Network Security

All the original source and destination address in NAT is hidden completely. Unless the user wants to, the hosts inside the NAT cannot be reached by hosts on other networks. Therefore, NAT provides additional layer of network security

6. Private Addressing

NAT has its own private IPv4 addressing system even if you move to a new public addressing scheme. Al though if you change the Internet Service Provider, the changes in the internal address will be prevented.

Network monitoring tools can compare data continuously and automatically when baseline data is available. You are notified when performance declines so you can take immediate action to fix the issue. You can compare historical data to determine the ideal network performance or spot subpar performance. You can use it to analyze network issues from the past.

REFERENCES

EDUCBA. (2022). *Network Monitoring Tools | List of Networking Monitoring Tools*. [online] Available at: https://www.educba.com/network-monitoring-tools/.
GeeksforGeeks. (2021). *Advantages and Disadvantages of NAT*. [online] Available at: https://www.geeksforgeeks.org/advantages-and-disadvantages-of-nat/.
EDUCBA. (2019). *What is NAT? | Working & Types | Advantages and Disadvantages*. [online] Available at: https://www.educba.com/what-is-nat/.
SearchSecurity. (n.d.). *What is a DMZ in Networking?* [online] Available at: https://www.techtarget.com/searchsecurity/definition/DMZ#:~:text=The%20primary%20benefit%20of%20a.
SearchSecurity. (n.d.). *What is an intrusion detection system (IDS)? Definition from SearchSecurity*. [online] Available at: https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system#:~:text=An%20IDS%20can%20be%20used.
support.huawei.com. (n.d.). *Firewall Security Policy: What It Is and How It Works - Huawei*. [online] Available at: https://support.huawei.com/enterprise/en/doc/EDOC1100172309.
Farrelly, J. (2022). *High-Profile Company Data Breaches 2022*. [online] Electric. Available at: https://www.electric.ai/blog/recent-big-company-data-breaches.
7 Threat Agents Your Cyber Security Team Should Be Aware Of (2019). *7 Threat Agents Your Cyber Security Team Should Be Aware Of | The Data Guardians*. [online] The Data Guardians. Available at: https://www.thedataguardians.co.uk/2019/02/27/7-threat-agents-your-cyber-security-team-should-be-aware-of/.
Rosencrance, L. (2021). *Top 10 types of information security threats for IT teams*. [online] SearchSecurity. Available at: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams.
https://uniserveit.com (n.d.). *How To Protect Your Business From Insider Threats | Uniserve IT*. [online] Uniserve IT Solutions. Available at: https://uniserveit.com/blog/how-to-protect-your-business-from-insider-threats.
Worm vs. Virus: What's the Difference and Does It Matter? (n.d.). *Worm vs. Virus: What's the Difference and Does It Matter?* [online] Available at: https://www.avast.com/c-worm-vs-virus.
www.hypr.com. (n.d.). *What is a Threat Actor? | Security Encyclopedia*. [online] Available at: https://www.hypr.com/security-encyclopedia/threat-agent.