ASSIGNMENT 1 FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	Unit 5: Security		
Submission date	5th/08/2022	**Date Received 1st submission**	3rd/08/2022
Re-submission Date	20th/08/2022	**Date Received 2nd submission**	15th/08/2022
Student Name	Bùi Hương Linh	**Student ID**	GBH200662
Class	GCH1002	**Assessor name**	Michael Omar
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	Linh

Grading grid

P1	P2	P3	P4	M1	M2	D1

☼ Summative Feedback:	☼ Resubmission Feedback:

Grade:	Assessor Signature:	Date:
Lecturer Signature:		

Table of Contents

Introduction

In today's data-driven and globally connected society, data frequently travels freely between people, organizations, and enterprises. Data has significant monetary value, which cybercriminals are well aware of. As a result of the ongoing rise in cybercrime, the demand for security experts to secure and defend an organization from attack is increasing. This report will discuss some fundamentally basic theories of security, such as identifying types of security threats to organizations, organizational security procedures, firewall policies and IDS, DMZ, static IP, and NAT in a network, to help me gain a deeper understanding in this field.

Task 1 - Identify types of security threat to organizations. Give an example of a recently publicized security breach and discuss its consequences (P1)

I. Define threats

Threats are security conditions that could have negative effects on people's lives or property. It could take the form of physical or verbal warnings intended to frighten a specific demographic. (Igi-global, 2022)

Figure 1: Threats (Source: Internet)

II. Identify threats agents to organizations

1. Nation States
    - Companies involved in certain industries such as telecommunications, oil and gas, mining, power generation, and national infrastructure are targeted by foreign countries to disrupt their current operations or disrupt their country's operations during difficult times to come. may become. stop.

- From alleged Russian meddling in the US presidential election, to Sony's claims that North Korea was responsible for hacking his website in 2014, and more recently, Huawei's 5G network provides The concern is because it may be able to provide information. to the Chinese government.
  (Matthew Lamb, 2022)

2. Non-target specific (Ransomware, Worms, Trojans, Logic Bombs, Backdoors and Viruses perpetrated by vandals and the general public).
   - I've been told this many times by companies “Oh we’re not going to be a target for hackers because….”. However, the number of random attacks that occur every day is so large (I don't have exact statistics to share here) that any organization can become a victim.
   - The most famous example of a non-targeted attack is the WannaCry ransomware incident, which affected over 200,000 computers in 150 countries. In the UK, the NHS has been shut down for several days.
     (Matthew Lamb, 2022)
3. Employees and Contractors
   - Machines and software programs are well protected against malware, as long as it's not a zero-day virus. Humans, either maliciously or accidentally, are often the weakest link in security systems.
   - Common mistakes like sending an email to the wrong person happen, but you can usually spot the mistake quickly and correct the situation. Simple measures like password-protecting files can also help reduce the impact of such errors.
     (Matthew Lamb, 2022)
4. Terrorists and Hacktivists (political parties, media, enthusiasts, activists, vandals, general public, extremists, religious followers)
   - Similar to the threat posed by nation states, the level of threat posed by these agents depends on your activity. However, the threat of indiscriminate attacks may continue as some terrorists seek to target specific industries and countries.
   - Perhaps the most famous example of this is the 2010 WikiLeaks disclosure of diplomatic cables and other documents related to the conflicts in Iraq and Afghanistan.
     (Matthew Lamb, 2022)
5. Organised crime (local, national, transnational, specialist)
   - Criminals target personal data for a variety of reasons. Credit card fraud, identity theft, bank account fraud, and more. These crimes are now being carried out on an industrial scale. Methods vary from phishing attacks to "watering hole" sites, but the end result is the same. You and your data are extracted and used for malicious purposes.

- According to the Credit Industry Fraud Avoidance (Cifas) Fraudscape Report 2018, the number of identity fraud cases rose again in 2017, with about 175,000 recorded. This is only a 1% increase for him compared to 2016, but a 125% increase for him compared to 10 years ago, and 95% of these cases involve the identity of innocent victims. It is related.
  (Matthew Lamb, 2022)

6. Natural disasters (fire, flood, earthquake, volcano)
   - While not cyberattacks, these events can have the same impact on your ability to conduct business. Even if you can't access files stored in your office, data center, or cloud, there's a data disaster to consider. Earthquake risk is very low in the UK, but every year we see images of cities underwater. (Matthew Lamb, 2022)
7. Corporates (competitors, partners)
   - The threat of competitors stealing your IP is obvious, but we are increasingly working with a number of partner organizations to fill skill and resource gaps, or simply provide services. Depending on their motives, these partner companies may unknowingly or maliciously steal or disclose your intellectual property or personal information held by you.
   - The 2013 attack on the US retailer Target may be the best illustration of how partner organizations can be the source of a breach. The hackers specifically targeted (pardon the pun!) suppliers before discovering a weak spot with the HVAC company Fazio Mechanical. In order to gain access to Target's point-of-sale systems, the hackers eventually sent a phishing email to a Fazio employee. They were now able to access up to 40 million credit and debit cards belonging to customers who had stopped by its stores over the 2013 holiday shopping season. Target has lost more than $200 million as a result of this.
     (Matthew Lamb, 2022)

III. List type of threats that organizations will face

1. Advanced Persistent Threats (APT)
   - APT is used to detect individuals or groups gaining unauthorized access to a network, deploying custom malicious code on multiple computers for specific tasks, and searching for as long as possible to obtain specific tasks. A covert ongoing computer network attack to prevent Collect and access sensitive confidential information. Traditionally, APTs have been associated with governments, but in recent years there have been several examples of large, non-government-backed groups conducting large-scale targeted intrusions for other reasons. (Security, 2021)

Figure 2: APT (Source: Internet)

- There are typically five progressions a persistent targeted attack goes through to maximize damage:
  - Access Infiltration: APT attackers try to infiltrate systems through phishing, Trojan, or malware. They can also exploit human vulnerabilities, so cybersecurity training should be in place within organizations to counter these threats.
  - Strengthening of Grip: Advanced Persistent Threat's strength is its ability to gain a foothold within an organization. You must find unique ways to enter and exit the system unnoticed. Cybercriminals use their digital backdoors and tunnels to accomplish this.
  - Infesting the system: APT attackers will begin hacking the system by gaining administrator rights and cracking passwords left and right once they have complete freedom of movement. They can gather their target data with little resistance if they have this kind of access.
  - Lateral activity: At this point, the company is a cybercriminal's playground. Explore other sections of the system to access other secure databases and servers nearby. They use malware to collect data and transfer it out of the network through established backdoors. Break starts here.
  - Deep machinations: During this phase, the APT attackers have complete control of the enterprise, erasing all traces of their hacking activity and establishing a reliable backdoor for future use.
    (Security, 2021)

2. Distributed Denial of Service (DDoS)
   - The disruption of a website is the primary goal of cybercriminals when they deploy Distributed Denial of Service or DDOS. (Security, 2021)

- In a DDoS attack, an attacker attempts to prevent intended users from accessing a machine or network resource by temporarily or indefinitely disrupting the service of an Internet-connected host. DDoS is typically accomplished by flooding the target computer with redundant requests from many different sources, overloading the system and preventing some or all legitimate requests from being executed. (Security, 2021)

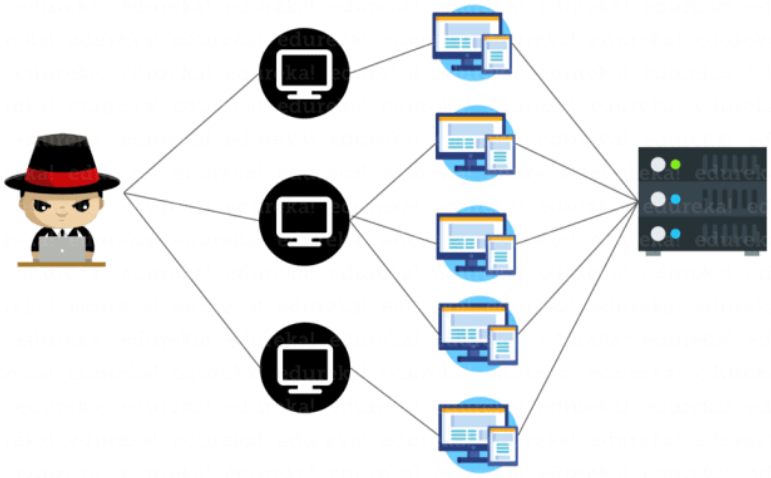


Figure 3: DDoS (Source: Internet)

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

1. Define security breaches

   A security breach is an incident that causes unauthorized access to computer data, applications, networks, or devices. This leads to unauthorized access to information. Usually occurs when an intruder is able to bypass security mechanisms. (Kaspersky, 2022)

2. Types of security breaches
   - Exploits attack vulnerabilities in systems such as outdated operating systems.
   - Weak passwords can be cracked or guessed. Some people still use the password "password", but "pa$$word" is not as secure.
   - Malware attacks such as phishing emails can be used to infiltrate. An employee simply clicks on a link in her phishing email and malicious software spreads throughout the network.
   - Drive-by downloads use viruses or malware delivered from compromised or fake websites.
   - Access can also be obtained using social engineering. For example, an intruder calls a company pretending to be her IT helpdesk employee and asks for a password to "fix" a computer.

(Kaspersky, 2022)

3. List and give examples with dates
    - Name: August 2022: QuestionPro Extortion Attempt Goes Public
        - Day: May 2022
        - A hacker using the alias "pompompurin" contacted QuestionPro in May 2022 and demanded money, claiming to have obtained 22 million email addresses and other pieces of information from the business. QuestionPro declined the hacker's demands for money in the form of Bitcoin.

          In August 2022, "pompompurin" notified Have I Been Pwned of the breach after QuestionPro turned down his payment request. QuestionPro has not formally acknowledged the breach as of yet. It's probable that the hacker that attacked the FBI and Robinhood earlier managed to access QuestionPro.
    - Name: July 2022: Neopets Data Breach Exposes Data on 69 Million Accounts
        - Day: July 19, 2022
        - A hacker put information on 69 million Neopets members up for sale on a website forum on July 19, 2022. Personal information including name, email address, date of birth, zip code, and others were exposed along with 460 MB of the compressed source code for the Neopets website. The Neopets team tweeted a confirmation of the data leak.

          Over the years, Neopets has had various breaches. The source code and user datasets have been accessed by numerous hackers and Neopets users. If you ever used Neopets, it could be a good idea to delete your account to guard against data breaches in the future.
    - Name: March 2022: Microsoft Breached by Lapsus$ Hacker Group
        - Day: March 20, 2022
        - The hacking collective Lapsus$ said that they have infiltrated Microsoft via a screenshot that was sent to their Telegram channel on March 20, 2022. The screenshot, which was obtained in the Microsoft collaboration tool Azure DevOps, showed that Bing, Cortana, and other projects had been affected by the intrusion.

          Microsoft released a statement on March 22 acknowledging the assaults had taken place. According to Microsoft's explanation, only one account was taken over in the attack, and the company's security staff was able to stop it before Lapsus$ could infiltrate further into their organization, they claimed that no customer data had been accessed.

          Lapsus$ is "a large-scale social engineering and extortion campaign against several enterprises with some seeing signs of harmful aspects," according to the security team at Microsoft. They go on to give a thorough description of the

group's strategies, proving that Microsoft had been closely researching Lapsus$ prior to the incident.

Lapsus$, on the other hand, has frequently asserted that they are only acting for commercial gain: Remember: We have no political motivations; money is our only purpose. They recently released a message encouraging tech professionals to hack their workplaces, showing that they appear to take advantage of insider threats.

- Name: January 2022: Over $30 Million Looted in Crypto.com Breach
  - Day: January 17, 2022
  - On January 17, 2022, hackers on Crypto.com gained access to the wallets of 483 individuals and stole a total of almost $18 million in bitcoin, $15 million in ethereum, and other cryptocurrencies. In order to access these individuals' wallets, it appears that the hackers were able to get around two-factor authentication.

    As soon as the breach occurred, Crypto.com called it a "incident" rather than a hack and said that none of its users' money had been taken. A few days later, they made it clear that money had been taken in the breach and said they had compensated the users who had been impacted. They added that they were striving to strengthen their security after auditing their systems.

(Firewall Times, 2022)

V. Discuss the consequences of this breach

- The impact on organizations exposed to data breaches is severe and growing. This is primarily due to the increased regulatory burden of notifying individuals whose data has been compromised. Notification requirements and penalties for organizations affected by a data breach vary by domestic and international jurisdictions in the United States and Canada.
- A company that experiences a customer data breach must determine where the customer lives and which regulator is responsible. Regulations define the types of data that must be reported after a breach, who must be notified, how the report should be made, and whether certain authorities must be notified. Violations related to personal, financial, and health information are generally subject to reporting requirements, although the exact definition varies by jurisdiction. Companies that operate internationally have customers in many countries and may need to meet different requirements. The cost of such a process, coupled with legal sanctions, potential damages claims, and resulting lawsuits, can be prohibitive and pose an existential threat to some businesses.

- Data breaches that affect other types of data can have a significant impact on a company's reputation and business health. In addition to the contractual obligations that may be affected, the proposed company sale could be jeopardized by a data breach, as happened recently with Verizon's acquisition of Yahoo. If your competitors become familiar with your business strategy and are able to sell similar products at lower prices, your business may not survive.
  (CloudMask , 2022)

VI. Suggest solutions to organizations

- You can maintain perimeter security and other protections, but you also need a data-centric solution that allows you to precisely control who can read specific files and records. Encryption gives you that kind of control, but it has to be the right kind of encryption. If a particular file or email is properly encrypted, you can control who can read it at any given time. Even if a data breach occurs in your IT system and an unauthorized person gains access to the data, they will not be able to read it and a data breach related to this data will be avoided. Such applications can reduce the risk of data breaches to an acceptable level and protect your business from catastrophic data breach costs.
- Train Your Workforce: Organizations can use security awareness training programs to educate employees about the importance of data security. Curricula CEO Nick Santora recommends that companies start by forming a team to create a strategic plan for their security awareness training program. Buy-in from the top is essential in this type of program, so the team should include both senior management and initiative leaders.
  (BISSON, 2022)

Task 2 - Describe at least 3 organizational security procedures (P2)

1. What is security procedures?
   Security procedures are detailed instructions for implementing, enabling, or enforcing the security controls outlined in your organization's security policy. Security procedures should cover the many hardware and software components that support business processes, as well as all security-related business processes themselves (such as onboarding new employees and assigning access rights). (DUNHAM, 2018)
2. Some organizational security procedures.
   - Acceptable Use Policy (AUP):
     - An AUP specifies the constraints and practices that an employee using organizational IT assets must agree to in order to access the corporate network or the internet. It is a standard onboarding policy for new employees. They are given

an AUP to read and sign before being given a network ID. It is recommended that organizations' IT, security, legal, and human resources departments discuss what is included in this policy. (Ninja, 2020)

- Access Control Policy (ACP):
  - The ACP specifies how employees can gain access to an organization's data and information systems. Access control standards, such as NIST's Access Control and Implementation Guides, are common topics covered in policies. Other issues covered in this policy include user access standards, network access controls, operating system software controls, and corporate password complexity. Other additions often outlined include how corporate systems are accessed and used, how unattended workstations should be secured, and how access should be secured when employees leave the company all frequently outlined. (Ninja, 2020)

- Business Continuity Plan (BCP):
  - The BCP will coordinate efforts throughout the organization and use the disaster recovery plan to restore hardware, applications, and data deemed critical to business continuity. Because they describe how the organization will operate in an emergency, BCPs are unique to each business. (Ninja, 2020)

- Disaster Recovery Policy:
  - The disaster recovery plan for an organization will typically include input from both the cyber security and IT teams and will be developed as part of the larger business continuity plan. The incident response policy will be used by the CISO and his team to manage an incident. The Business Continuity Plan will be activated if the event has a significant business impact. (Ninja, 2020)

Task 3 - Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS (P3)

I. Discuss briefly firewalls and policies, their usage and advantages in a network.

1. Firewall defined

   A firewall is a type of network security device that monitors incoming and outgoing network traffic and allows or denies data packets based on a set of security rules. Its purpose is to create a barrier between your internal network and incoming traffic from outside sources (such as the internet) in order to prevent malicious traffic such as viruses and hackers. (Forcepoint, 2022)

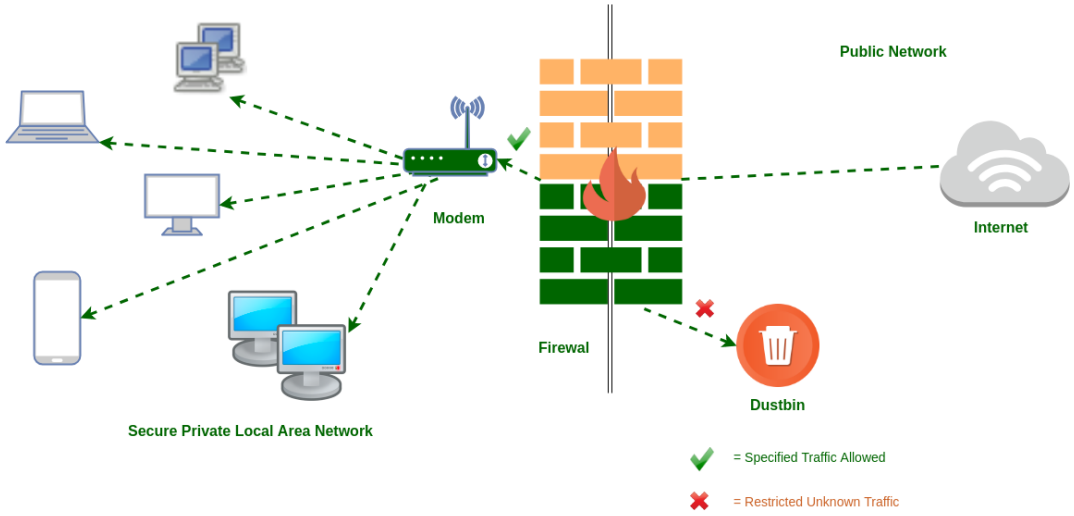


*Figure 4: Firewall (**Source**: Internet)*

2. Policy
    - Give instructions on when firewalls are required or recommended. A Network Firewall is required wherever Sensitive Data is stored or processed; a Host Firewall is required wherever Sensitive Data is stored or processed and the operating environment supports the implementation. Both the Network and Host Firewalls protect the same operating environment, and the control redundancy (two separate and distinct firewalls) adds extra security in the event of a compromise or failure.
    - Raise awareness about the importance of having a firewall that is properly configured (installed and maintained).
    (Northwestern , 2022)

3. Advantages of firewalls
    - Stops spyware: In a data-driven world, preventing spyware from accessing and infiltrating your system is a much-needed advantage. The more complex and robust a system is, the more access points criminals can use to gain access to it. One of the most common ways unwanted individuals gain access is through the use of spyware or malware (programs designed to infiltrate systems, control computers, and steal data). A firewall acts as an important block against these malicious programs.
    - Promotes privacy: An overarching benefit is the promotion of privacy. By proactively protecting your data and your customers' data, you can create a privacy environment your customers can trust. No one likes having their data stolen, especially when it's clear that steps can be taken to prevent an intrusion.

- Prevents hacking: Unfortunately, as companies increasingly move to digital operations, thieves and bad actors are doing the same. Data theft and the increasing hostage of systems by criminals have made firewalls even more important to prevent hackers from gaining unauthorized access to your data, emails, systems, and more. Firewalls can either stop hackers altogether or prevent them from choosing easier targets.
- Stops virus attacks: Nothing brings down digital operations faster and harder than a virus attack. With hundreds of thousands of new threats being developed every day, it's important to take measures to keep your system healthy. One of the most obvious benefits of a firewall is its ability to control entry points into your system and stop virus attacks. Depending on the type of virus, the cost of a virus attack on your system can be prohibitive.
- Monitors network traffic: The ability to monitor network traffic is the foundation of all firewall security benefits. Data flowing into and out of your systems opens the door for threats to compromise your operations. Firewalls protect your systems by monitoring and analyzing network traffic and applying predefined rules and filters. You can manage your levels of protection based on what you see coming in and out of your firewall with a well-trained IT team.
  (Fortinet , 2022)

II. How does a firewall provide security to a network?

1. Software firewalls

- A software firewall is a program your computer uses to inspect data entering and leaving your device. You can customize it to suit your needs. Similar to hardware firewalls, software firewalls filter data by checking if the data (or its behavior) matches a profile of malicious code.
- Software firewalls can also monitor traffic leaving your computer to prevent it from being used to attack other networks or devices. Each computer in the network must have a software firewall installed. A software firewall, as a result, can only protect one computer at a time.
- Firewalls use different methods to protect your network or computer:
  - Packet filtering
  - Proxy service
  - Stateful inspection

(Fortinet, 2022)

2. Hardware firewalls

- A hardware firewall is a system that works independently of the computer it is protecting by filtering information entering the system from the internet. A broadband internet router will almost certainly have its own firewall.

- To protect your system, hardware firewalls inspect incoming data from different parts of the Internet to make sure it's safe. Hardware firewalls that use packet filters inspect every packet of data to check where the data is coming from and where it is going. The data collected by the firewall for each packet is checked against an authorization list to see if it matches a data profile that should be discarded. A hardware firewall can protect any computer connected to it, making it an easily scalable solution.
  (Fortinet, 2022)

Figure 5: Hardware firewall (Source: Internet)

III. How firewall works

First, the firewall system analyzes network traffic based on rules. A firewall only welcomes incoming connections that it is configured to accept. It does this by allowing or blocking specific data packets (units of communication sent over digital networks) based on predefined security rules. A firewall acts like a traffic monitor on your computer's entry points or ports. Only trusted sources or IP addresses are allowed. An IP address is important because it identifies a computer or source in much the same way that a mailing address identifies a place of residence. (Norton, 2022)

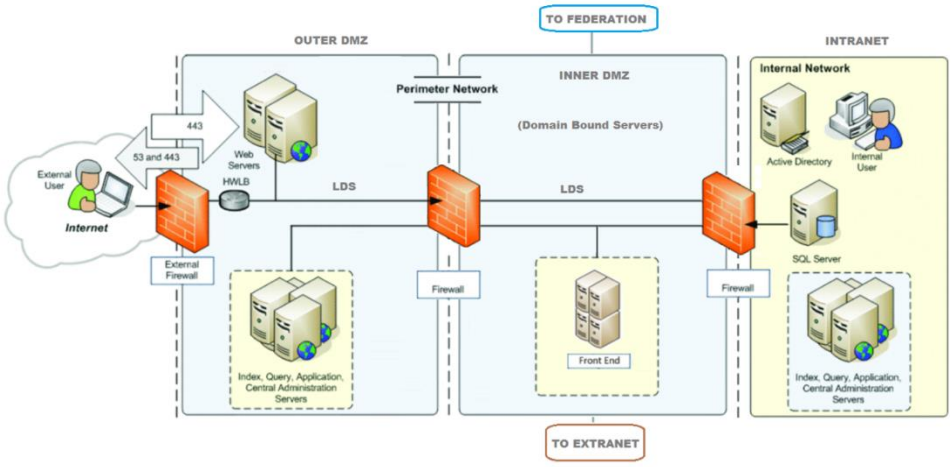


Figure 6: Firewall work (Source: Internet)

IV. Define IDS

An intrusion detection system (IDS) is a network security technology originally designed to detect the exploitation of vulnerabilities on targeted applications or computers. Intrusion prevention systems (IPS) have enhanced IDS solutions with the ability to block threats in addition to detection, and have become the primary deployment option for IDS/IPS technology.

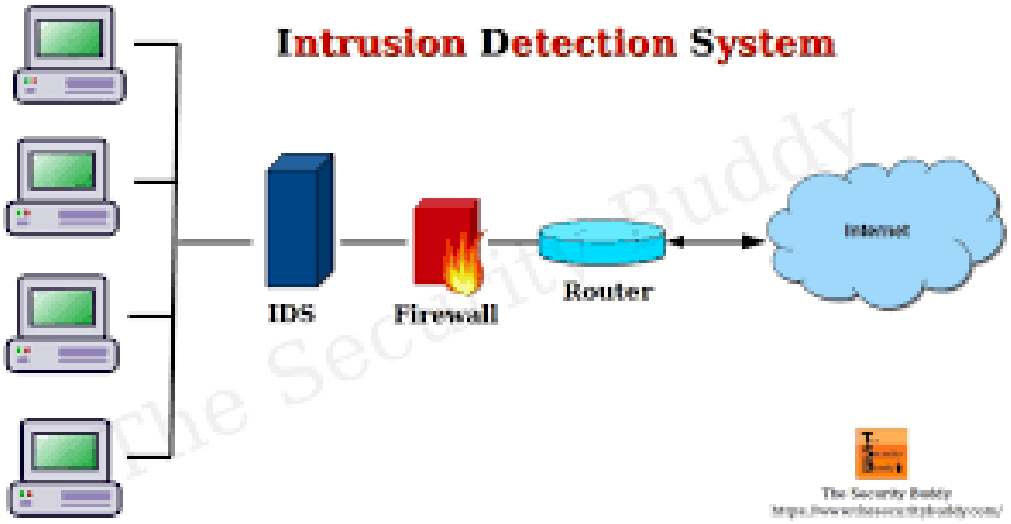


Figure 7: IDS (Source: Internet)

V. Firewall and IDS if they are incorrectly configured in a network

1. Firewall
    - Firewall issues are one of the main reasons this is the case.

- Through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws.
- Rapid change and accelerating hybrid cloud adoption make network security difficult to maintain.
- Many organizations try to protect themselves with network firewalls, increasing the risk of configuration errors and policy gaps.
  (Burton, 2020)

2. IDS
   - IDSs are prone to false positives (or false positives). As a result, the company has to make fine adjustments during the initial installation of his IDS product. This includes properly configuring intrusion detection systems to compare normal traffic on your network with potentially malicious activity.
     (Lutkevich, 2022)

Task 4 - Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security (P4)

I. Define and discuss DMZ

1. What is DMZ?
   A DMZ network is a perimeter network that protects an organization's internal local network from untrusted traffic and provides an additional layer of security. A shared DMZ is a subnetwork between the public internet and a private network. (Fortinet, 2022)

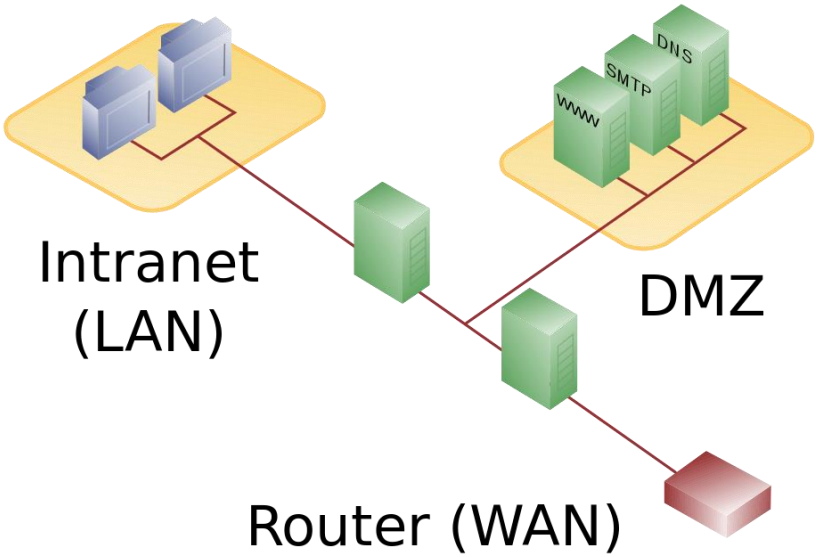


Figure 8: DMZ (Source: Internet)

2. How does a DMZ network work?

- The public servers are hosted on a network that is separate and isolated.
- A DMZ network acts as a barrier between the Internet and a company's private network. The DMZ is separated by a security gateway such as a firewall filtering traffic between the DMZ and the LAN. The default DMZ server is protected by another security gateway that filters incoming traffic from external networks.
- This is ideally placed between two firewalls and the DMZ firewall setup ensures that incoming network packets are checked by the firewall (or other security tool) before reaching the server hosted in the DMZ. will be This means that even if a sophisticated attacker manages to get past the first firewall, he would also need access to hardened services in the DMZ to cause damage to the organization.
- If an attacker penetrates the external firewall and compromises the systems in her DMZ, they must also penetrate the internal firewall to access the company's sensitive data. A highly skilled attacker may be able to breach her secure DMZ, but internal resources should trigger alarms that give enough warning that a compromise is underway.

(Fortinet, 2022)

3. Benefits of DMZs
    - Enable access control: Organizations can allow users to access services outside their network perimeter over the public Internet. The DMZ grants access to these services while also implementing network segmentation to make it difficult for unauthorized users to reach your private her network. A DMZ can also include proxy servers that centralize the internal flow of traffic and facilitate monitoring and recording of that traffic.
    - Prevent network reconnaissance: By providing a buffer between the Internet and private networks, DMZs prevent attackers from performing reconnaissance efforts to find potential targets. Servers in the DMZ are publicly accessible, but an extra layer of security is provided by a firewall that prevents attackers from snooping into your internal network. Even if the DMZ system is compromised, an internal firewall separates and protects the private network from the DMZ, making it difficult for outside investigations.
    - Block Internet Protocol (IP) spoofing: Attackers try to gain access to your system by forging IP addresses and pretending to be authorized devices logged on to your network. A DMZ can detect and thwart such spoofing attempts when another service verifies the legitimacy of her IP address. A DMZ also provides network segmentation to organize traffic and create space for accessing public services outside the internal private network.

      (Fortinet, 2022)

II. Define and discuss static IP

1. What is static IP?

   A static IP address is an IP address that is manually configured for a device and not assigned by a DHCP server. It is called static because it does not change, unlike a dynamic IP address, which changes. (Kaspersky, 2022)

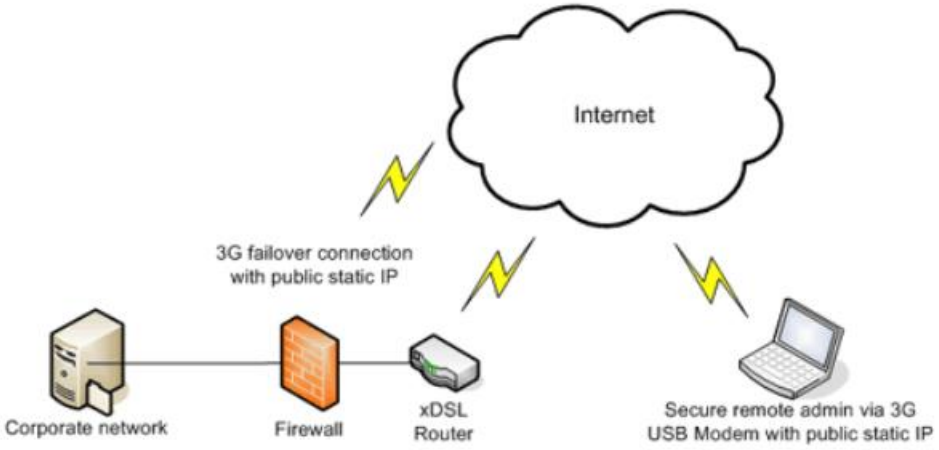


Figure 9: IP Addresses (Source: Internet)

2. How do IP addresses work?
   - Devices connect to the Internet indirectly by first connecting to an Internet-connected network. This will allow your device to access the internet.
   - If you're at home, that network is likely your Internet Service Provider (ISP). At work, it becomes a corporate network.
   - An IP address is assigned to your device by your ISP.
   - Internet activity is routed through his ISP and using your IP address. They provide you access to the Internet, so it's their job to assign IP addresses to your devices.
   - However, IP addresses are subject to change. For example, turning your modem or router on or off can change that. Alternatively, you can contact your ISP and ask them to change it for you.
   - If you take your device with you on the go, such as when you travel, you won't have your home IP address with you. It uses a different network (Wi-Fi in a hotel, airport, coffee shop, etc.) to access the internet, and uses a different (temporary) IP address assigned by your internet service provider. It's because Hotels, airports, coffee shops. (Kaspersky, 2022)
3. Benefits of IP addresses
   - Speed: Devices with static IP addresses tend to work faster because static IP addresses are less inconsistent. The difference in speed will be very noticeable only if you are

a broadband user, not for DSL connections. This is especially useful if you are constantly uploading and downloading files.

- Security: A static IP address always provides a higher level of security. A static IP address comes with an extra layer of protection that reliably prevents most security issues.
- Accessibility: Programs such as Virtual Private Networks (VPNs) allow remote access with static IP addresses. This means you can access your device from anywhere in the world. All information is accessible as long as the device is connected to the internet.
- Hosting: All types of hosting web servers, email servers, and other types of servers are now accepted with static IP addresses. Therefore, with a static IP address, all clients and customers can easily access his website. And even if you use a static IP address, your device can easily find and locate all servers around the world.
- Stability: All static IP addresses are known to be stable as they are protected from changes. Unlike dynamic IP addresses, they are not subject to common errors. Computers with the same IP address can quickly reconnect to the Internet after each restart.
- Accuracy: A static IP address is very accurate when it comes to geolocation data. All geolocation services can locate your exact business location. With this accurate information, your company will always be in the forefront. This is beneficial to businesses in many ways.
- Shared Resource: Some companies often share office resources with their employees. To do this, use a corporate network with devices with static IP addresses. Devices with static IP addresses are easier to find. Conversely, devices with dynamic IP addresses are notoriously difficult to discover.
  (HitechWhizz, 2022)

III. Define and discuss NAT

1. What is NAT?

   Network Address Translation (NAT) is the process of mapping one Internet Protocol (IP) address to another IP address by modifying the IP packet headers while in transit through a router. This improves security and reduces the number of IP addresses your organization needs. (Hanna, 2022)

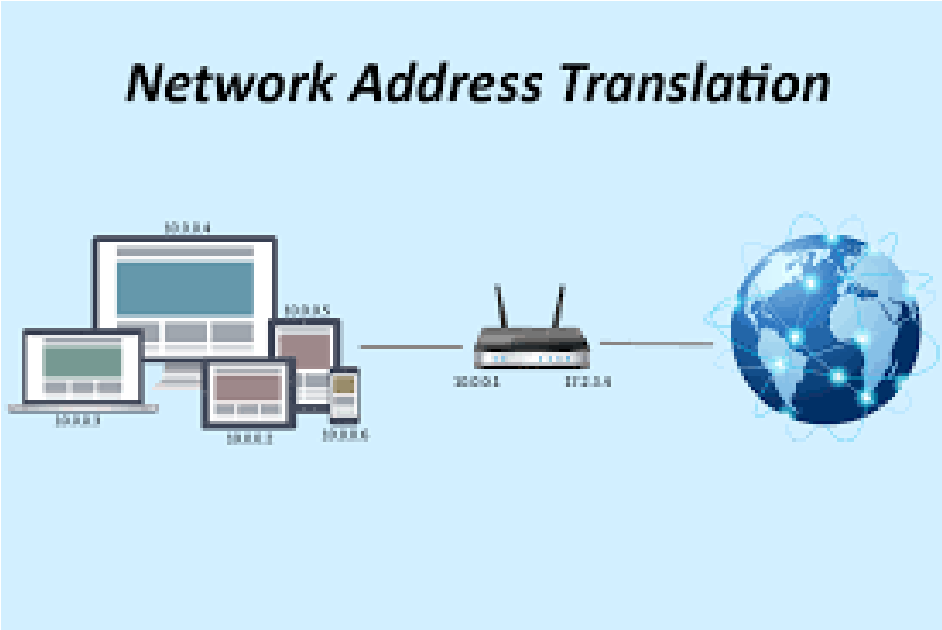


Figure 10: NAT (Source: Internet)

2. How does NAT work?
    - NAT works by choosing a gateway between two local networks (the internal network and the external network). Systems on the internal network are typically assigned IP addresses that are not routable to external networks (for example, networks within the 10.0.0.0/8 block).
    - Some externally valid IP addresses are assigned to the gateway. The gateway makes outgoing traffic from internal systems appear to originate from one of the valid external addresses. Accept incoming traffic destined for valid external addresses and send it to the correct internal system.
    - This contributes to security. Because every outgoing or incoming request has to go through a transformation process that offers the possibility to qualify or authenticate the incoming stream, compare it with the outgoing request, and so on.
    - NAT has done a lot to save on the number of globally valid IP addresses that organizations need and combined with Classless Inter-Domain Routing (CIDR), has done a lot to extend the useful life of IPv4. NAT is generally described in IETF RFC 1631.

    (Hanna, 2022)
3. Benefits of NAT
    - This allows you to recover your private IP address.
    - It has excellent security features that enhance the security of private networks by isolating the internal network from the external network.

- Helps conserve IP address space. A large number of hosts can be connected to the global Internet using a small IP address.
  (GeeksforGeeks, 2022)

Conclusion

The essential security expertise is enumerated in this article: Threat agent for organizations, List the types of threats that organization will face, Discuss the consequences of this breach, ... Describe at least 3 organizational security procedures. Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS. Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.

References

BISSON, D., 2022. *5 Ways Your Organization Can Ensure Improved Data Security.* [Online] Available at: https://www.tripwire.com/state-of-security/security-data-protection/5-ways-you-can-ensure-improved-data-security/

Burton, D., 2020. *The Dangers of Firewall Misconfigurations and How to Avoid Them.* [Online] Available at: https://www.akamai.com/blog/security/the-dangers-of-firewall-misconfigurations-and-how-to-avoid-them

CloudMask , 2022. *Data Breaches: Threats and Consequences.* [Online] Available at: https://www.cloudmask.com/blog/data-breaches-threats-and-consequences#:~:text=Depending%20on%20the%20type%20of,and%20possibly%20compensate%20those%20affected.

DUNHAM, R., 2018. *Security Procedures – How Do They Fit Into My Overall Security Documentation Library?.* [Online] Available at: https://linfordco.com/blog/security-procedures/?fbclid=IwAR1Hrx2uMFJmtT9WSghprwoGyvdTDX7LbjF5nCVCczdby-V1AwQBUuHPz5g

Forcepoint, 2022. *What is a Firewall?.* [Online] Available at: https://www.forcepoint.com/cyber-edu/firewall?fbclid=IwAR1Hrx2uMFJmtT9WSghprwoGyvdTDX7LbjF5nCVCczdby-V1AwQBUuHPz5g

Fortinet , 2022. *Firewall Benefits: The Importance of Firewall Security.* [Online] Available at: https://www.fortinet.com/resources/cyberglossary/benefits-of-firewall

Fortinet, 2022. *How Does a Firewall Work?.* [Online] Available at: https://www.fortinet.com/resources/cyberglossary/how-does-a-firewall-work

Fortinet, 2022. *What is DMZ and hy would you use it?.* [Online] Available at: https://www.fortinet.com/resources/cyberglossary/what-is-dmz#:~:text=A%20DMZ%20Network%20is%20a,public%20internet%20and%20private%20networks.

GeeksforGeeks, 2022. *Advantages and Disadvantages of NAT.* [Online] Available at: https://www.geeksforgeeks.org/advantages-and-disadvantages-of-nat/

Hanna, K. T., 2022. *Network Address Translation (NAT).* [Online] Available at: https://www.techtarget.com/searchnetworking/definition/Network-Address-Translation-NAT#:~:text=A%20Network%20Address%20Translation%20(NAT,IP%20addresses%20an%20organization%20needs.

HitechWhizz, 2022. *7 Advantages and Disadvantages of Static IP Address | Drawbacks & Benefits of Static IP Address.* [Online]
Available at: https://www.hitechwhizz.com/2021/09/advantages-and-disadvantages-drawbacks-benefits-of-static-ip-address.html.html.html

Igi-global, 2022. *What is Threats.* [Online] Available at: https://www.igi-global.com/dictionary/threats/30044

Kaspersky, 2022. *What is a security breach?.* [Online] Available at: https://www.kaspersky.com/resource-center/threats/what-is-a-security-breach

Kaspersky, 2022. *What is an IP Address – Definition and Explanation.* [Online] Available at: https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address

Lutkevich, B., 2022. *intrusion detection system (IDS).* [Online] Available at: https://www.techtarget.com/searchsecurity/definition/intrusion-detection-system

Matthew Lamb, M. D., 2022. *7 Threat Agents Your Cyber Security Team Should Be Aware Of.* [Online] Available at: https://www.thedataguardians.co.uk/2019/02/27/7-threat-agents-your-cyber-security-team-should-be-aware-of/?fbclid=IwAR1JjI9w2qb1cQWVRJDEOADJP1P81ubzSS0x_vecCpC69jJw5OYjy5id3kc

Ninja, P., 2020. *9 Policies For Security Procedures Examples.* [Online] Available at: https://www.privacy.com.sg/resources/9-rules-security-procedures-examples/?fbclid=IwAR1Of4SiPMk8cm0bPEudrduOa-T4iymEsVYBUIe4tzN_ucrf-4iOjhsbssk

Northwestern , 2022. *Firewall Policy.* [Online] Available at: https://www.it.northwestern.edu/policies/firewall.html

Norton, 2022. *What is a firewall? Firewalls explained and why you need one.* [Online] Available at: https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html#

Security, R., 2021. *TYPES OF SECURITY THREATS TO ORGANIZATIONS.* [Online] Available at: https://blog.rsisecurity.com/types-of-security-threats-to-organizations/?fbclid=IwAR00TvzVRnCQMZvy9DnqDprfWBn06w-GssqW76yvc6-cL0i4anjOaZYzYlw

Presented by: Bùi Hương Linh
Class: GCH1002
Student ID: GBH200662
Tutor: Michael Omar

Security

Table of content

Task1: Identify types of security threat to organizations. Give an example of a recently publicized security breach and discuss its consequences

1. Define threats.

   Threats are security conditions that could have negative effects on people's lives or property. It could take the form of physical or verbal warnings intended to frighten a specific demographic.

2. Identify threats agents to organizations.

Organised crime: Criminals target personal data for a variety of reasons. Credit card fraud, identity theft, bank account fraud, and more. These crimes are now being carried out on an industrial scale. Methods vary from phishing attacks to "watering hole" sites, but the end result is the same. You and your data are extracted and used for malicious purposes.

3. List type of threats that organizations will face
   - Advanced Persistent Threats (APT)
   - Distributed Denial of Service (DDoS)

Task1: Identify types of security threat to organizations. Give an example of a recently publicized security breach and discuss its consequences

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

- Define security breaches:

A security breach is an incident that causes unauthorized access to computer data, applications, networks, or devices. This leads to unauthorized access to information. Usually occurs when an intruder is able to bypass security mechanisms.

- Types of security breaches:

Access can also be obtained using social engineering. For example, an intruder calls a company pretending to be her IT helpdesk employee and asks for a password to "fix" a computer.

5. Discuss the consequences of this breach

The impact on organizations exposed to data breaches is severe and growing. This is primarily due to the increased regulatory burden of notifying individuals whose data has been compromised.

6. Suggest solutions to organizations

-You can maintain perimeter security and other protections, but you also need a data-centric solution that allows you to precisely control who can read specific files and records. Encryption gives you that kind of control, but it has to be the right kind of encryption.

Task 2 - Describe at least 3 organizational security procedures

1. What is security procedures?

Security procedures are detailed instructions for implementing, enabling, or enforcing the security controls outlined in your organization's security policy. Security procedures should cover the many hardware and software components that support business processes, as well as all security-related business processes themselves (such as onboarding new employees and assigning access rights).

2. Some organizational security procedures.

- Acceptable Use Policy (AUP):
- Access Control Policy (ACP):
- Business Continuity Plan (BCP):
- Disaster Recovery Policy:

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

1. Discuss briefly firewalls and policies, their usage and advantages in a network.

- Firewall defined

A firewall is a type of network security device that monitors incoming and outgoing network traffic and allows or denies data packets based on a set of security rules. Its purpose is to create a barrier between your internal network and incoming traffic from outside sources (such as the internet) in order to prevent malicious traffic such as viruses and hackers.

- Advantages of firewalls
  - Stops spyware
  - Promotes privacy
  - Prevents hacking
  - Stops virus attacks
  - Monitors network traffic

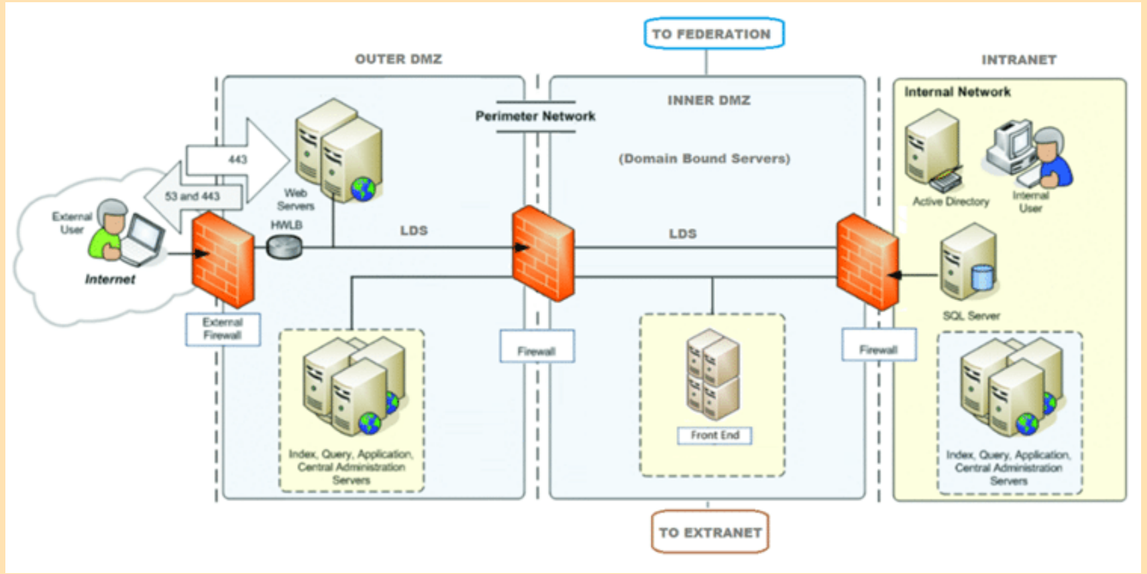
2. How does a firewall provide security to a network?

- Software firewalls
  - Firewalls use different methods to protect your network or computer:
    + Packet filtering
    + Proxy service
    + Stateful inspection
- Hardware firewalls
  - A hardware firewall is a system that works independently of the computer it is protecting by filtering information entering the system from the internet. A broadband internet router will almost certainly have its own firewall.

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

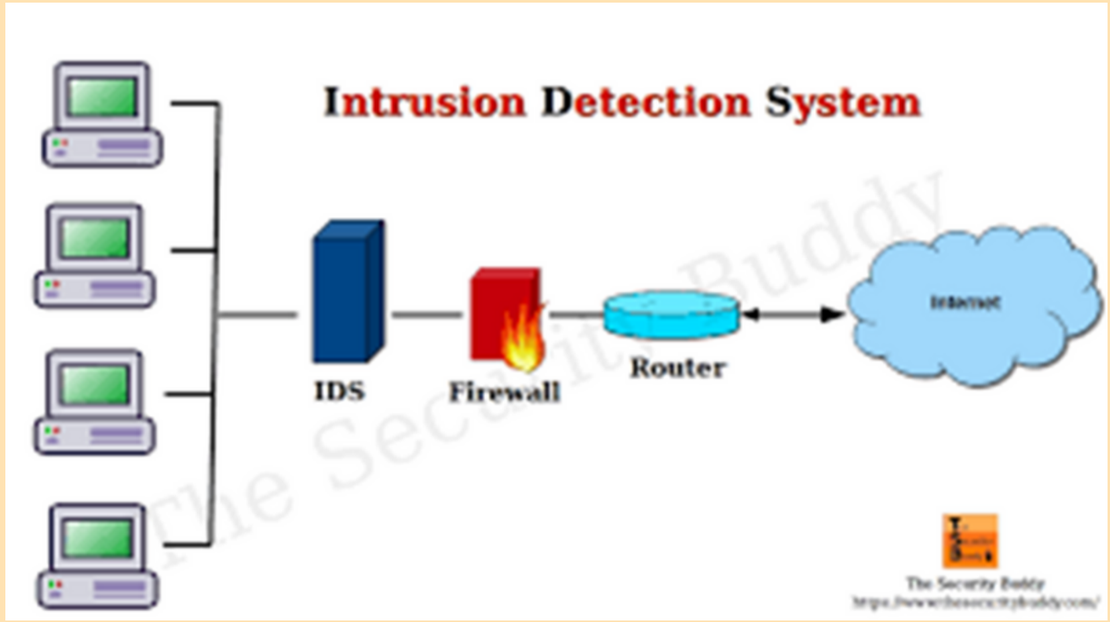
3. How firewall works

First, the firewall system analyzes network traffic based on rules. A firewall only welcomes incoming connections that it is configured to accept. It does this by allowing or blocking specific data packets (units of communication sent over digital networks) based on predefined security rules.



4. Define IDS

An intrusion detection system (IDS) is a network security technology originally designed to detect the exploitation of vulnerabilities on targeted applications or computers. Intrusion prevention systems (IPS) have enhanced IDS solutions with the ability to block threats in addition to detection, and have become the primary deployment option for IDS/IPS technology.



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

5. Firewall and IDS if they are incorrectly configured in a network

- Firewall
  + Firewall issues are one of the main reasons this is the case.
  + Through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws.
  + Rapid change and accelerating hybrid cloud adoption make network security difficult to maintain.
  + Many organizations try to protect themselves with network firewalls, increasing the risk of configuration errors and policy gaps.

- IDS

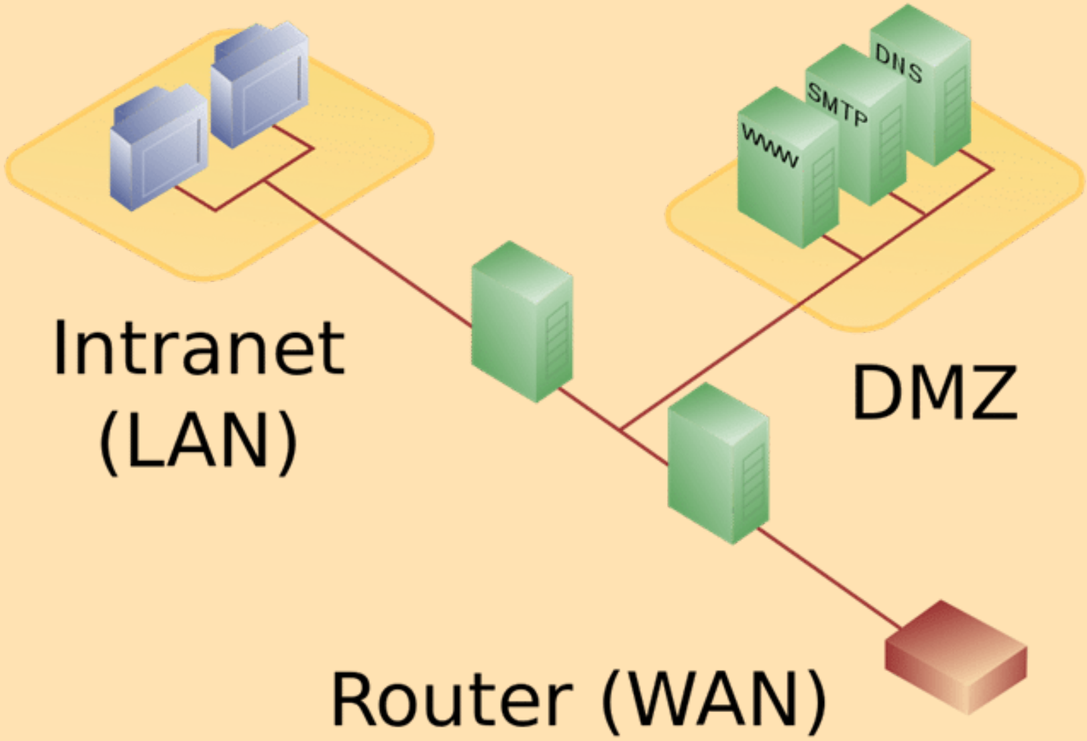
  IDSs are prone to false positives (or false positives). As a result, the company has to make fine adjustments during the initial installation of his IDS product. This includes properly configuring intrusion detection systems to compare normal traffic on your network with potentially malicious activity.

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

1. Define and discuss DMZ

- What is DMZ?

A DMZ network is a perimeter network that protects an organization's internal local network from untrusted traffic and provides an additional layer of security. A shared DMZ is a subnetwork between the public internet and a private network.



- Benefits of DMZs

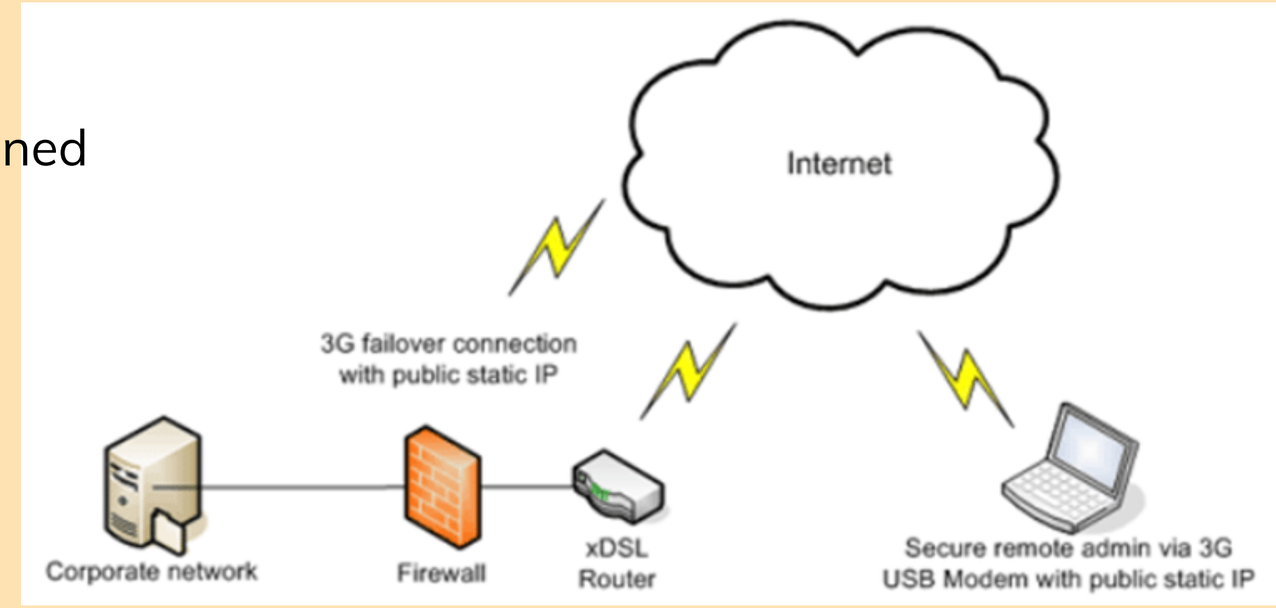
- Enable access control
- Prevent network reconnaissance
- Block Internet Protocol (IP) spoofing

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

2. Define and discuss static IP

- What is static IP?

A static IP address is an IP address that is manually configured for a device and not assigned by a DHCP server. It is called static because it does not change, unlike a dynamic IP address, which changes.



- Benefits of IP addresses

- Speed
- Security
- Accessibility
- Hosting
- Stability
- Accuracy
- Shared Resource

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

3. Define and discuss NAT

- What is NAT?

Network Address Translation (NAT) is the process of mapping one Internet Protocol (IP) address to another IP address by modifying the IP packet headers while in transit through a router. This improves security and reduces the number of IP addresses your organization needs.

- Benefits of NAT

- - This allows you to recover your private IP address
- It has excellent security features that enhance the security of private networks by isolating the internal network from the external network
- -Helps conserve IP address space. A large number of hosts can be connected to the global Internet using a small IP address.

References

BISSON, D., 2022. 5 Ways Your Organization Can Ensure Improved Data Security. [Online]
Available at: https://www.tripwire.com/state-of-security/security-data-protection/5-ways-you-can-ensure-improved-data-security/
Burton, D., 2020. The Dangers of Firewall Misconfigurations and How to Avoid Them. [Online]
Available at: https://www.akamai.com/blog/security/the-dangers-of-firewall-misconfigurations-and-how-to-avoid-them
CloudMask , 2022. Data Breaches: Threats and Consequences. [Online]
Available at: https://www.cloudmask.com/blog/data-breaches-threats-and-consequences#:~:text=Depending%20on%20the%20type%20of,and%20possibly%20compensate%20those%20affected.
DUNHAM, R., 2018. Security Procedures – How Do They Fit Into My Overall Security Documentation Library?. [Online]
Available at: https://linfordco.com/blog/security-procedures/?fbclid=IwAR1Hrx2uMFJmtT9WSghprwoGyvdTDX7LbjF5nCVCczdby-V1AwQBUuHPz5g
Forcepoint, 2022. What is a Firewall?. [Online]
Available at: https://www.forcepoint.com/cyber-edu/firewall?fbclid=IwAR1Hrx2uMFJmtT9WSghprwoGyvdTDX7LbjF5nCVCczdby-V1AwQBUuHPz5g

Thank for listening