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	Ho Quang Minh	**Student ID**	GCD210513
Class	GCD1104	**Assessor name**	Tran Thanh Truc

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:		

Table of Contents

I. Identify types of security threat to organisations. Give an example of a recently publicized security breach and discuss its consequences (P1)

1. Define threats

- In RFC 4949, IETF defines a threat as: A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.

- In SP8000-160, NIST defines it as: An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss.

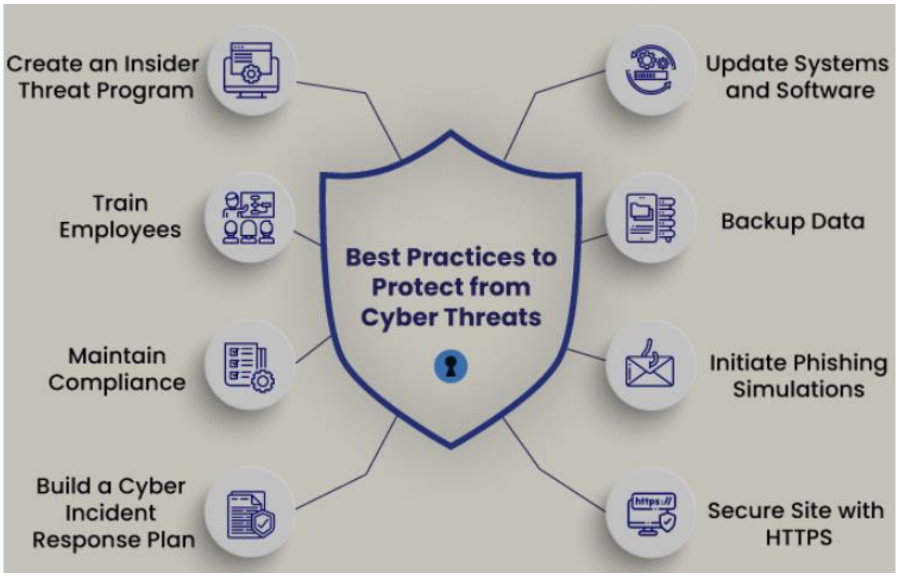

Best Practices to Protect from Cyber Threats
Create an Insider Threat Program
Train Employees
Maintain Compliance
Build a Cyber Incident Response Plan
Update Systems and Software
Backup Data
Initiate Phishing Simulations
Secure Site with HTTPS

Figure 1: Threats

2. Threat agents to organizations

- Malicious software: Malicious software, often referred to as "malware," is any software or code specifically designed to infiltrate, damage, or gain unauthorized access to computer systems, networks, or devices without the knowledge and consent of the user or owner.

- Hardware or software failure: Hardware and software failures refer to malfunction or failure of components in a computer system, resulting in the inability of the system or specific software applications to function as intended.

- Internal attacker: An insider, also known as an insider threat, refers to an individual who has access to an organization's systems, networks, or sensitive information due to their position within the organization. These individuals can be employees, contractors, business partners, or any other employee with legitimate access to the organization's resources.

- Equipment theft: An insider, also known as an insider threat, refers to an individual who has access to an organization's systems, networks, or sensitive information due to their position within the organization. These individuals can be employees, contractors, business partners, or any other employee with legitimate access to the organization's resources.

- External attacker: An individual, group, or entity that attempts to gain unauthorized access to, control over, or exploitation of computer systems, networks, or digital assets belonging to a company, person, or entity from outside their security perimeter is referred to as an external attacker in the context of cybersecurity and network security. These attackers frequently carry out their harmful operations with the purpose to hurt, steal sensitive information, disrupt services, or obtain unlawful benefits because they do not have authorized access to the target systems.

- Natural disaster: A natural catastrophe is a catastrophic event that happens as a result of natural processes and can result in substantial harm, devastation, and fatalities. These occurrences are frequently caused by geological, hydrological, meteorological, or climatic processes and are typically out of human control. Natural catastrophes can have catastrophic effects on local economies, communities, and the environment.

- Industrial espionage: Industrial espionage, sometimes referred to as corporate espionage or economic espionage, is the illegal and clandestine act of acquiring proprietary or secret information from one organization by another with the goal of gaining a business advantage or financial gain. Trade secrets, knowledge used in research and development, customer lists, marketing tactics, manufacturing procedures, and other sensitive corporate data may all have been stolen.

- Terrorism: The use of violence, intimidation, or coercion for ideological, political, religious, or other goals is referred to as terrorism. It entails using violence or threatening to use violence in order to spread fear, panic, and commotion inside a society in order to further a particular cause, impose beliefs, or accomplish particular political goals. Often, terrorist attacks target civilians or non-combatants in an effort to cause the most deaths and stir up widespread dread and worry.

3. List type of threats that organizations will face

- Viruses and worms: 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.

- 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. 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 operations, and produce malicious traffic for distributed denial-of-service assaults.

- Drive-by download attacks: In a drive-by download attack, 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 viewing 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 acquire personal information.

- 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 banking institutions, eBay, PayPal, and even friends and coworkers.

- Distributed denial-of-service (DDoS) attacks: In a distributed denial-of-service (DDoS) attack, multiple infected machines assault a target, such as a server, website, or other network resource, in a distributed denial-of-service (DDoS) attack, rendering the target completely unworkable. The target system is forced to slow down or crash and shut down due to the barrage of connection requests, inbound messages, or malformed packets, depriving genuine users or systems of service.

- Ransomware: In a ransomware attack, the victim's computer is usually encrypted and locked, preventing them from accessing the system or the data that is stored on it. The victim is required to pay the hacker a ransom, generally in a digital currency like Bitcoin, in order to recover access to the device or data. Malicious email attachments, corrupted software programs, infected external storage devices, and compromised websites can all transmit ransomware.

- Exploit kits: A programming tool called an exploit kit lets someone without any prior experience writing software code to create, alter, and spread malware. A few other names for exploit kits are infection kits, crimeware kits, DIY attack kits, and malware toolkits. These toolkits are used by cybercriminals to distribute malware, perform denial-of-service attacks, create botnets, and steal corporate data by exploiting system weaknesses.

- Advanced persistent threat attacks: A targeted cyberattack known as an advanced persistent threat (APT) occurs when an unauthorized intruder breaches a network and does so while going unnoticed for a considerable amount of time. An APT attack aims to observe network activity and steal data to acquire access, using exploit kits and malware, rather than harming a system or network. APT attacks are generally used by cybercriminals to steal data over an extended period of time from high-value targets like large businesses and nation-states.

- Malvertising: Malvertising is a method used by online thieves to insert malicious code into trusted websites and online advertising networks. Typically, this code infects computers or mobile devices with malware or drives people to harmful websites. Even if users don't do anything to begin the download, their computers could still become infected. Malvertising is a technique used by cybercriminals to spread many types of lucrative malware, such as cryptomining scripts, ransomware, and banking Trojans.

Some of the websites of well-known companies, including Spotify, The New York Times and the London Stock Exchange, have inadvertently displayed malicious ads, putting users at risk.

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

Security breach: Any incident that allows unauthorized access to computer data, applications, networks, or devices is referred to as a security breach. As a result, unapproved access to information occurs. Usually, it happens when a burglar is able to get past security measures.

List some security breaches and example with dates

- June 2023: Report Identifies Over 101k Hacked ChatGPT Accounts

A threat intelligence team at Group-IB released a report indicating that over 101,000 ChatGPT credentials were stolen by malware over a 12-month period. These researchers found these accounts on the dark web, available for sale alongside other stolen data.

These accounts were compromised by malware on users' devices; they were not hacked due to a breach of ChatGPT itself.

- July 2023: Chinese Hackers Breach U.S. Agencies Via Microsoft Cloud.

On July 11, Microsoft publicly disclosed that a group of Chinese hackers had spied on U.S. government agencies via a vulnerability in Microsoft's cloud services. The attack was first detected in June, by an unnamed government agency which proceeded to inform Microsoft and the Department of Homeland Security of the incident.

The hacking group in question, deemed "Storm-0558" by Microsoft, appears to be linked to the Chinese government. Their attacks targeted State and Commerce department emails, ahead of U.S. Secretary of State Antony Blinken's visit to China in June. U.S. officials have stated that sensitive data was not compromised in this email breach.

- July 2023: More Victims Emerge from MOVEit Attacks.

July saw even more damage from the MOVEit attacks, which have now compromised over 200 companies. New victims include Radisson Hotels; a spokesperson said that "a limited number of guest records" were exposed, but did not detail exactly how many were affected.

The attacks also compromised data pertaining to 43,000 employees of real estate company Jones Lang LaSalle. Several universities were impacted, including the University of Illinois, the University of Colorado, and Johns Hopkins University. Other notable victims include Deutsche Bank, UofL Health, and the New York Department of Education.

All in all, sensitive records pertaining to millions of people have been implicated in this string of attacks. More details continue to emerge, and we will keep this article updated as more information comes to light.

- July 2023: Microsoft Denies Purported Data Breach.

On July 2, hacktivist group Anonymous Sudan claimed to have hacked Microsoft and pilfered data pertaining to over 30 million Microsoft accounts. The group provided a sample of the data, but so far it has not been determined where exactly the data came from.

A Microsoft spokesperson said that these claims of a data breach were not legitimate and stated that Microsoft had seen “no evidence that our customer data has been accessed or compromised.”

5. Discuss the consequences of this breach

Some consequence of security breaches:

- June 2023: Report Identifies Over 101k Hacked ChatGPT Accounts

Consequence:

The reported identification of over 101,000 hacked ChatGPT accounts in June 2023 would have several significant consequences:

Security worries: The breach would draw attention to weaknesses in the safeguards defending ChatGPT accounts. As a result, users may lose faith in the platform's capacity to protect their private information and data.

Users' confidential communications and possibly sensitive information could be compromised, raising privacy issues. Personal information may have been exposed in this incident, which might have serious repercussions for anyone who were personally impacted.

Data Misuse: Information from compromised accounts may be exploited for phishing, identity theft, or even information manipulation. Financial losses and reputational harm for those harmed could result from this.

Spam and Phishing Attacks: Hackers could use the compromised accounts to send spam messages, spread malware, or launch phishing attacks on other users. This could have a cascading effect, affecting not only the hacked accounts but also other users who might fall victim to these attacks.

Legal and Regulatory Ramifications: The company behind ChatGPT could face legal actions and regulatory fines for failing to protect user data adequately. Depending on the jurisdiction, they might be held accountable for the breach.

Loss of Trust and Reputation: The incident could severely damage the reputation of the platform, making users hesitant to continue using it or recommend it to others. Rebuilding trust after such a breach can be a long and challenging process.

Increased Security Measures: The company would likely need to implement stricter security measures, such as improved encryption, two-factor authentication, and regular security audits, to prevent future breaches. While this is a positive step, it might also inconvenience users with additional security measures.

Financial Impact: Dealing with the aftermath of a large-scale breach can be costly. The company might need to allocate significant resources to investigate the breach, notify affected users, provide support, and upgrade security systems.

User Awareness: The breach could serve as a wake-up call for users to take their online security more seriously. People might become more cautious about sharing personal information online and using strong, unique passwords.

Innovation and AI Development: The breach could prompt the AI development community to focus more on the security aspect of AI applications. Researchers and developers might work together to develop more secure and robust AI systems.

- July 2023: Chinese Hackers Breach U.S. Agencies Via Microsoft Cloud.

Consequence:

The Chinese Hackers Breach U.S. Agencies Via Microsoft Cloud in July 2023 would have several significant consequences:

Data Compromise: Breaches of U.S. agencies via a widely-used cloud provider like Microsoft could lead to the exposure of sensitive and classified information. This could include personal data of government employees, confidential diplomatic communications, and potentially even national security secrets.

National Security Concerns: Such a breach could have significant national security implications. Foreign hackers gaining access to government networks could potentially gather intelligence, conduct espionage, and gain insights into the nation's strategic plans and operations.

Diplomatic Tensions: If the attack is attributed to Chinese hackers, it could strain diplomatic relations between the United States and China, leading to political tensions and potential retaliatory measures.

Loss of Trust: The breach could erode public trust in government agencies' ability to protect sensitive information, as well as undermine confidence in the security of cloud services provided by tech companies.

Financial Impact: The aftermath of a cyberattack often involves substantial financial costs for investigating the breach, securing systems, and mitigating the damage. Additionally, affected agencies may need to invest in cybersecurity enhancements to prevent future breaches.

Legal and Regulatory Consequences: Depending on the circumstances, there could be legal and regulatory repercussions for both the hackers involved and the affected organizations. Regulatory bodies may impose fines for inadequate data protection measures.

Cybersecurity Policy Changes: High-profile breaches can lead to calls for stronger cybersecurity policies and regulations, potentially resulting in changes to how government agencies handle and protect sensitive information.

Escalation of Cyber Conflict: If the breach is part of a larger pattern of cyberattacks between nations, it could contribute to an escalation of cyber conflict, where countries engage in retaliatory or offensive cyber operations against each other.

6. Suggest solution to organizations

- June 2023: Report Identifies Over 101k Hacked ChatGPT Accounts

Notification and Communication: The platform that hosts ChatGPT would likely notify affected users about the breach, providing details about the incident, the potential impact, and recommended actions.

Account Recovery: Affected users would likely be advised to change their passwords immediately. The platform might also implement a forced password reset for all users to ensure the security of their accounts.

Investigation: The platform's security team would conduct a thorough investigation to determine the extent of the breach, how it occurred, and what data was compromised. This could involve working with cybersecurity experts and forensic analysts.

Mitigation: The platform would take steps to close the security vulnerabilities that allowed the breach to occur. This could involve patching software, improving security protocols, and enhancing monitoring systems.

Legal and Regulatory Compliance: The platform would need to adhere to data breach reporting requirements as dictated by relevant data protection laws. This might involve reporting the breach to regulatory authorities and affected users within a certain timeframe.

User Support: The platform would likely provide support to users who have been affected by the breach. This could include guidance on securing their accounts, monitoring for suspicious activity, and addressing any potential identity theft concerns.

Enhanced Security Measures: In response to the breach, the platform might implement additional security measures such as two-factor authentication (2FA), stricter password requirements, and more frequent security audits.

Communication Transparency: The platform would need to communicate transparently with its user base and the public about the breach, the steps taken to address it, and the measures being implemented to prevent similar incidents in the future.

Learning and Improvement: The breach would serve as a valuable lesson for the platform, prompting a review of their security practices and policies. They would likely identify areas for improvement and take steps to prevent similar breaches in the future.

- July 2023: Chinese Hackers Breach U.S. Agencies Via Microsoft Cloud.

Containment and Investigation: The first step would be to identify the extent of the breach and isolate affected systems to prevent further unauthorized access. A thorough investigation would be conducted to understand the methods used by the hackers and the data that might have been compromised.

Attribution: Determining the source of the attack is crucial. If the breach is indeed attributed to Chinese hackers, government agencies would work to gather evidence and confirm the origin of the attack.

Public Disclosure: Depending on the severity of the breach and the data involved, affected agencies might need to publicly disclose the incident. This helps in transparency and allows individuals to take necessary precautions if their data was compromised.

Communication: Government agencies would need to communicate internally and externally about the breach, its impact, and the steps being taken to address the situation. Clear and timely communication is important to manage public perception and address concerns.

Mitigation and Remediation: Efforts would be made to patch vulnerabilities and secure the compromised systems. This might involve working closely with the cloud provider (in this case, Microsoft) to address any security flaws.

Enhanced Security Measures: After the breach is contained, agencies would likely implement additional security measures to prevent future attacks. This could involve updating security protocols, enhancing employee training, and implementing stricter access controls.

Cooperation with Tech Companies: Collaboration with technology companies like Microsoft would be essential to understand how the breach occurred and to prevent similar incidents in the future. Tech companies might provide patches, updates, and guidance to improve system security.

Diplomatic Actions: If the breach is attributed to a foreign nation, diplomatic channels would be used to address the issue. This could involve diplomatic protests, discussions, and negotiations to prevent future breaches and maintain international norms in cyberspace.

Legal and Regulatory Responses: Governments might consider legal actions against the hackers involved, as well as review and potentially strengthen cybersecurity regulations and laws.

Lessons Learned: After the situation is under control, agencies would conduct a comprehensive review of the breach to identify what went wrong and how to improve future incident response and prevention.

II. Describe at least 3 organisational security procedures (P2)

- Security Awareness Training:

+ Security awareness training is a vital procedure that aims to educate employees and stakeholders about various security threats, best practices, and the organization’s security policies. This procedure involves:

+ Conducting regular training sessions on topics like phishing awareness, password hygiene, social engineering, and safe online practices.

+ Educating employees about the importance of protecting sensitive data and the potential consequences of security breaches.

+ Raising awareness about emerging threats and trends in cybersecurity to ensure that individuals remain informed and vigilant.

+ Providing guidelines for reporting security incidents, suspicious activities, or potential vulnerabilities.

- Vulnerability Management:

+ Vulnerability management is the process of identifying, assessing, mitigating, and monitoring vulnerabilities in an organization's systems, software, and networks. This procedure includes:

+ Regularly scanning systems and applications for known vulnerabilities using vulnerability assessment tools.

+ Prioritizing vulnerabilities based on severity and potential impact on the organization.

+ Developing a patch management strategy to ensure timely application of security patches and updates.

+ Establishing a process for addressing and remediating vulnerabilities, which may involve applying patches, configuration changes, or implementing compensating controls.

+ Continuously monitoring and reassessing the environment to identify new vulnerabilities as they emerge.

- Backup and Disaster Recovery:

+ Backup and disaster recovery procedures are essential for ensuring business continuity in the face of data loss, hardware failures, natural disasters, or cyberattacks. These procedures encompass:

+ Regularly backing up critical data, applications, and system configurations to secure off-site or cloud storage locations.

+ Creating and maintaining a well-documented disaster recovery plan that outlines roles, responsibilities, and steps to take in the event of a disruption.

+ Conducting regular testing and simulations of the disaster recovery plan to ensure its effectiveness and to identify any gaps or areas for improvement.

+ Implementing redundancy and failover mechanisms for mission-critical systems to minimize downtime.

+ Ensuring that personnel are trained on the disaster recovery plan and know how to execute it efficiently during emergencies.

-> The overall security posture of a company is influenced by these security measures as well as others like access control, incident response, and network segmentation. Maintaining a robust and resilient security environment requires adapting these procedures to the organization's specific threats, industry requirements, and technology landscape.

III. Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS (P3)

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

1.1 Firewall:

- Define: An organization's security policies are followed via a firewall, a network security device that monitors and filters incoming and outgoing network traffic. In essence, it serves as a barrier to protect a private internal network from the public Internet.

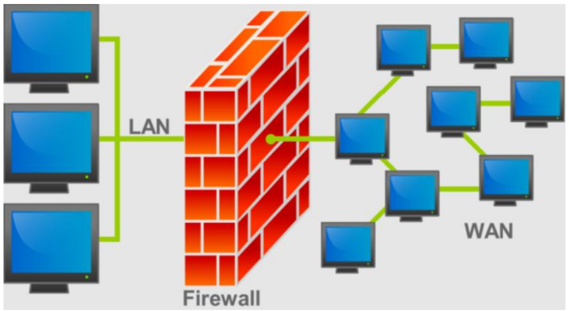


Figure 2: Firewall

- Types of firewalls:

+ Packet Filtering.

+ Proxy Service Firewall.

+ Stateful Inspection.

+ Next-Generation Firewall.

+ Unified Threat Management (UTM) Firewall.

+ Threat-Focused NGFW.

- Usage:

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.

- Advantage of firewall in a network:

+ Firewalls play an important role in the companies for security management. Below are some of the important advantages of using firewalls.

+ It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet.

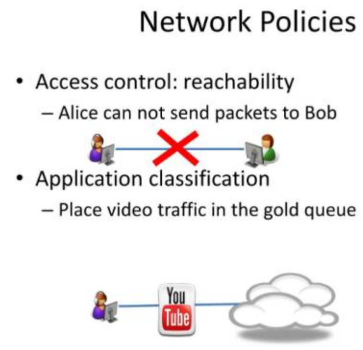
+ Firewalls provide faster response time and can handle more traffic loads.

+ A firewall allows you to easily handle and update the security protocols from a single authorized device.

+ It safeguards your network from phishing attacks.

1.2 Policies:

- Define: An organization's network resources should be accessed, used, and secured in accordance with its network security policies, which are a collection of standards, regulations, and procedures. These guidelines create a structure for preserving the confidentiality, integrity, and accessibility of network systems and data. They provide as a base for the implementation of security measures and controls to reduce risks and guarantee adherence to industry standards.



Network Policies

- Access control: reachability
  - Alice can not send packets to Bob
- Application classification
  - Place video traffic in the gold queue

Figure 3: Policies

- Usage:

Network security policies are used to guide the behavior and practices of individuals, systems, and devices within an organization's network environment. Some key areas where network security policies are applied include:

+ Access Control: Access rights to particular resources, networks, and data are governed by policies. They specify the access granting and revocation policies, authorization levels, and authentication techniques.

+ Password and Authentication: To prevent unwanted access, policies provide password complexity requirements, multi-factor authentication (MFA), and instructions for secure password management.

+ Data Handling and Encryption: Policies specify how private information should be handled, sent, and stored. To protect data while it is in transit and at rest, they could require encryption techniques.

+ Network Configuration: To make sure they are adequately secured and in line with best practices, policies control the installation and configuration of network equipment, including firewalls, routers, and switches.

+ Remote Access: Policies establish the use of Virtual Private Networks (VPNs), encrypted protocols, and authentication techniques in order to determine how remote users and devices can connect to the network.

- Advantage of policies in a network:

+ Consistency: By providing a uniform foundation for security procedures across the business, policies make sure that all personnel and technological systems follow the same security requirements.

+ Risk Mitigation: Policies aid in the prevention of security events and data breaches by recognizing and addressing potential security threats.

+ Compliance: In order to comply with industry standards and regulatory requirements and prevent negative legal and financial repercussions, well defined policies are essential.

+ Communication: Policies clear up ambiguities and raise security awareness by communicating security expectations to staff members, independent contractors, and third-party providers.

+ Efficiency: Policies reduce the need for ad hoc security measures by streamlining decision-making by providing set rules.

+ Incident Response: By putting incident response procedures in place, an organization can be sure that it is ready to react to security incidents in a way that minimizes harm and downtime.

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

By acting as a barrier between trusted internal networks and dubious external networks, such the internet, a firewall adds security to a network. Based on predetermined rules, it applies security policies to regulate the flow of incoming and outgoing network traffic. How a firewall improves network security is seen here:

- Packet Filtering: As data packets enter or exit the network, firewalls inspect them. They examine data such protocol kinds, port numbers, and source and destination IP addresses. A packet is only allowed to pass if it matches an allowed rule; otherwise, it is blocked. This stops harmful traffic and illegal access from accessing the network.

- Access Control: Firewalls implement access control rules that specify which users, gadgets, or programs are permitted access to particular network resources. This makes sure that only people with permission can access sensitive information and services.

- Stateful Inspection: Stateful inspection is a technique used by contemporary firewalls to monitor the status of active connections. This enables the firewall to decide whether to accept or restrict traffic with greater intelligence. It makes sure that only legitimate connections are made and kept up.

- Application Layer Filtering: At the application layer of the network stack, firewalls can function. This gives them the ability to recognize and manage particular programs or services (like email or web browsing) depending on their behavior or protocols. It assists in preventing the use of dangerous or unapproved programs on the network.

- Proxy Services: For specific types of traffic, some firewalls serve as proxies. They take requests from internal users, send them to an external server, get a response, and then send the internal user the information. This adds an additional layer of security and conceals internal IP addresses.

- Network Segmentation: Network segmentation, which divides the network into smaller pieces with their own security measures, is made possible by firewalls. In the event that one portion of the network is compromised, this stops attackers from moving laterally within it.

- Intrusion Detection/Prevention Systems (IDS/IPS): IDS/IPS capabilities can be included into firewalls to find and stop nefarious or suspicious activity. They look at the patterns and signatures of network traffic to spot potential risks and respond appropriately.

3. Show with diagrams the example of how firewall works

For example, the image depicted below shows how a firewall allows good traffic to pass to the user's private network.

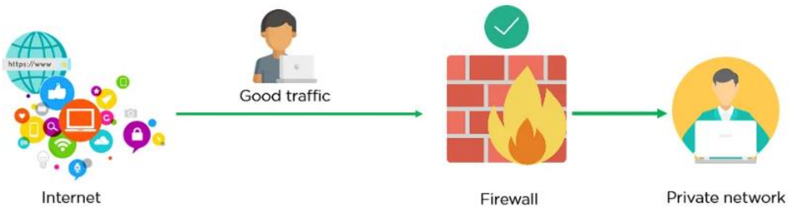


Figure 4: Firewall allowing Good Traffic

However, in the example below, the firewall blocks malicious traffic from entering the private network, thereby protecting the user's network from being susceptible to a cyberattack.

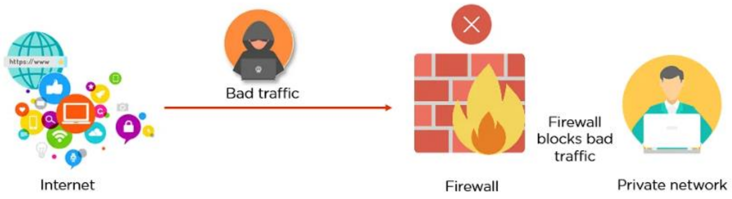


Figure 5: Firewall blocking Bad Traffic

4. Define IDS, its usage, and show it with diagrams examples

- Define: An intrusion detection system (IDS) monitors network traffic for malicious activity and immediately provides notifications if it detects anything suspicious. Software is used to look for malicious activity or policy violations on a network or system.

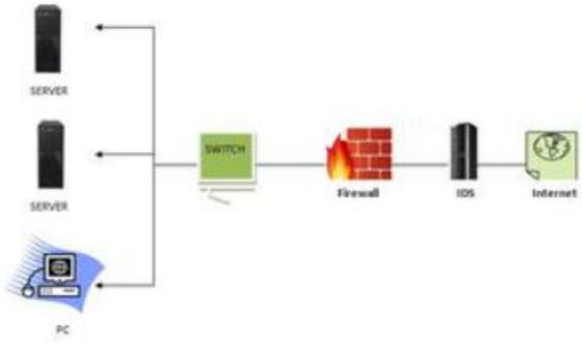


Figure 6: IDS

- Usage:

+ A computer network's traffic is monitored by an IDS (Intrusion Detection System) to look for any unusual activities.

+ The network's data is analyzed to seek for trends and indications of unusual behavior.

+ The IDS looks for any activity that might be a sign of an attack or intrusion by comparing the network activity to a set of predetermined rules and patterns.

+ The system administrator receives a notification if the IDS finds something that corresponds to one of these rules or patterns.

+ After looking into the alert, the system administrator can take appropriate measures to stop any harm or additional infiltration.

- Diagrams examples:

+ Network Intrusion Detection System (NIDS)

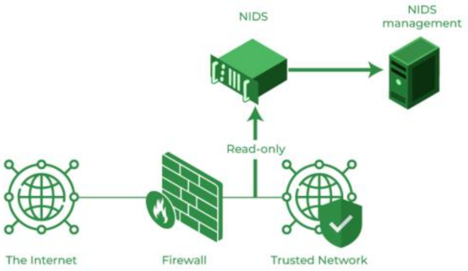


Figure 7: NIDS

+ Host Intrusion Detection System (HIDS)

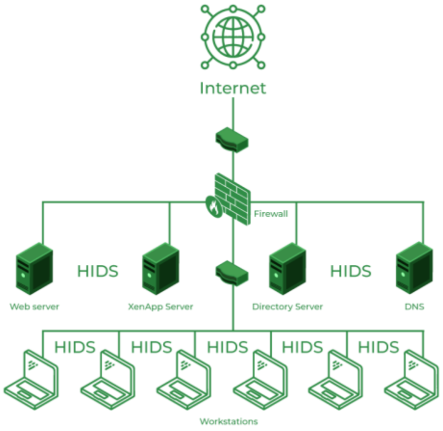


Figure 8: HIDS

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

Firewalls and Intrusion Detection Systems (IDS) that are improperly set can seriously harm a network's security posture. Here is a list of the possible dangers and risks connected to certain configuration errors:

- Reduced Security Effectiveness:

+ Threat: Incorrectly set firewalls may unintentionally let unauthorized traffic into the network or mistakenly block legal traffic.

+ Risk: Attackers could take advantage of these weaknesses to infiltrate the network, carry out malicious operations, steal data, or launch distributed denial-of-service (DDoS) assaults. Similar to how an IDS with bad rules could miss some threats or produce too many false positives, creating security holes or alert fatigue.

- False Sense of Security:

+ Threat: Incorrect firewall and IDS setups could deceive managers into thinking the network is secure when it isn't.

Risk: As a result, security on the network may not be monitored or maintained with the utmost care, leaving vulnerabilities open to attack.

- Performance Degradation:

+ Threat: Improperly designed firewalls and IDS may cause network devices to process data excessively.

+ Risk: As a result of these security procedures using an excessive amount of resources, there may be network slowdowns, packet losses, or even network outages.

- Unintended Consequences:

+ Threat: Failure to fully comprehend the network's architecture and applications can have unforeseen effects while configuring firewalls or IDS.

+ Risk: Legal services could be restricted, disrupting communications or corporate operations. IDS false positives may also draw attention and resources away from true security issues.

- Network Isolation Issues:

+ Threat: Inadequate firewall rules may unintentionally isolate certain network segments.

+ Risk: Communication between crucial systems may be disrupted, impacting operations and the flow of information.

- Vulnerability Amplification:

+ Threat: Incorrect firewall configuration leaves internal services and systems vulnerable to outside attackers.

+ Risk: Attackers may use these weaknesses to intensify their attacks, compromise more systems, and possibly cause extensive harm.

- Limited Incident Analysis:

+ Threat: Security teams may have trouble analyzing real incidents if IDS generates too many false positives.

+ Risk: Real security issues may go unnoticed or unaddressed, allowing attackers to continue undetected.

- Resource Misallocation:

+ Threat: Inadequate IDS setups can waste resources by sending out too many alarms.

+ Risk: Instead of dealing with actual security events, network managers may spend their time and energy resolving erroneous alarms.

- Lack of Integration:

+ Threat: IDS and firewalls not being properly integrated with other security solutions.

+ Risk: The lack of a comprehensive understanding of the network's security posture may make it difficult to correlate attacks and respond to them effectively.

- Compliance Failures and Legal Consequences:

+ Threat: Non-compliance with regulations may result from improperly implemented security measures.

+ Risk: Due to poor security procedures, organizations run the risk of facing fines from the law, losing their business licenses, or contract violations.

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

1. Define and discuss with the aid of diagram DMZ. Focus on its usage and security function as advantage

- Define:

An organization's internal local-area network is shielded from unauthorized traffic by a perimeter network known as a DMZ, or demilitarized zone.

A demilitarized zone network's major objective is to provide access to untrusted networks, such as the internet, while maintaining the security of the organization's LAN or private network. The Domain Name System (DNS), File

Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers are just a few examples of servers that are commonly kept in the DMZ by organizations.

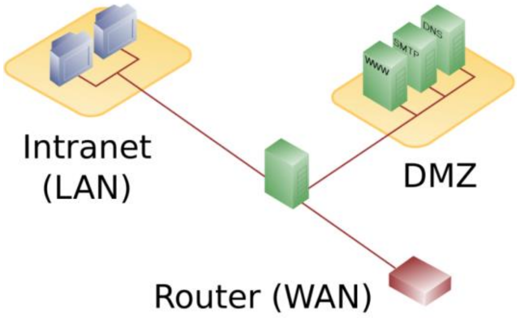


Figure 9: DMZ

- Usage:

+ Hosting Public Services: Public-facing services including web servers, email servers, and DNS servers are housed in DMZs. This protects sensitive internal resources by separating these services from the internal network.

+ External Access Points: DMZs are home to gateways that provide access to particular services for partners or external users while obstructing direct access to the internal network.

+ Intrusion Prevention: To monitor incoming and outgoing traffic for threats, a DMZ can be equipped with security tools like intrusion detection systems (IDS) and intrusion prevention systems (IPS).

+ Guest Networks: DMZs can be used to host guest networks, giving guests access to the internet without disclosing private information about the organization.

+ DMZs can be used to host authentication and authorization services for outside users, eliminating the need for direct access to internal authentication systems.

- Security of DMZ:

+ Isolation of Services: The potential impact of a compromise on critical internal resources is reduced by DMZs, which physically divide externally facing services from the inside network.

+ Reduced Attack Surface: The company limits the number of exposed services in the DMZ, cutting down on the number of possible entry points for attackers.

+ Traffic Scrutiny: Firewalls, IDS, and IPS, among other security tools, can watch and examine incoming and outgoing traffic in the DMZ before it enters the internal network.

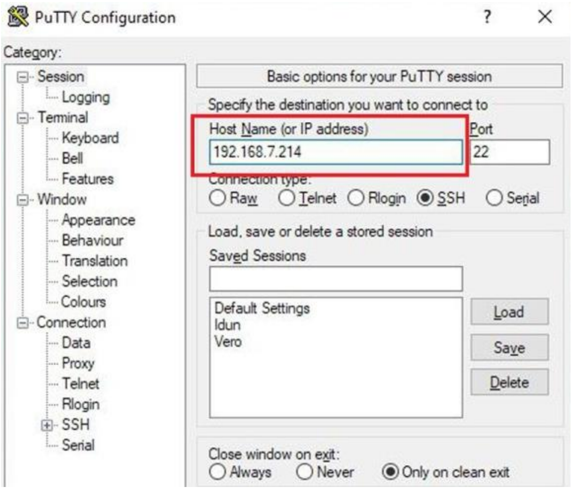
+ Access Control: What can be accessed directly from the DMZ is restricted by the use of access controls between the DMZ and the internal network.

+ Segregation of Networks: With the use of DMZs, networks can be divided, protecting sensitive information and important systems from unauthorized external networks.

2. Define and discuss with the aid of diagram static IP. Focus on its usage and security function as advantage

Define: A computer's static IP address is a 32-bit value that serves as its internet address. The internet service provider (ISP) often provides this number, which is represented as a dotted quadrilateral.

An internet-connected device's IP address, or "internet protocol address," serves as a special identification number. Similar to how individuals use phone numbers to locate and communicate with one another on the phone, computers use IP addresses to locate and communicate with one another online. An IP address might reveal details about the hosting company and location information.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.7.214
Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings
Idun
Vero

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 10: Static IP

- Usage:

+ Server Hosting: Hosting servers including web servers, email servers, and game servers frequently use static IP addresses. This is so that customers may connect to these services dependably, which requires a constant address.

+ Remote Access: Static IPs are frequently used by equipment that need remote access, such as security cameras, network routers, and Internet of Things (IoT) devices, to guarantee constant connectivity.

+ VPN and Remote Access: For devices connected through Virtual Private Networks (VPNs) or remote access solutions, static IP addresses are useful. This ensures that gadgets can always be accessed from a distance.

+ Network Devices: For management purposes, switches, routers, and firewalls frequently employ static IP addresses. Administrators may now regularly access these devices for configuration and maintenance thanks to this.

+ DNS Servers: DNS servers, which convert domain names into IP addresses, frequently employ static IP addresses to deliver trustworthy name resolution services.

- Security of static IP:

+ Stable Network Access: Static IPs give network devices a constant and unchanging address. For administrators and authorized users, secure device access is made simpler by this predictability.

+ Access Control: Firewalls and static IPs can be used to grant or refuse access based on IP addresses. This facilitates the implementation of granular access control policies.

+ Intrusion Detection and Monitoring (IDS) can concentrate on static IP addresses, which makes it simpler to track and examine potential threats and anomalies.

+ Authentication and Authorization: IP addresses are frequently used in access control as part of authentication systems. By guaranteeing consistent identification for authorized users, static IPs improve security.

3. Define and discuss with the aid of diagram NAT. Focus on its usage and security function as advantage

- Define: Private IP networks can use the internet and cloud thanks to a service called "Network Address Translation" (NAT). Before packets are delivered to an external network, NAT converts private IP addresses in an internal network to a public IP address.

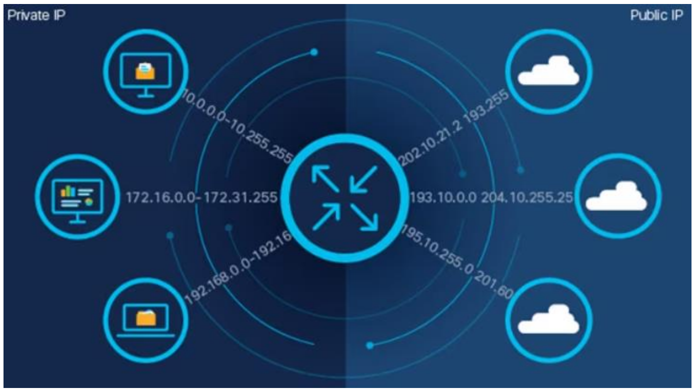


Figure 11: NAT

- Usage:

Network Address Translation (NAT) is a service that links private networks to open networks, such as the internet, using a router or edge platform. In order to offer internet access in core, campus, branch, and colocation sites, NAT is frequently used at the WAN edge router.

When connecting devices outside of its network, NAT allows an organization to represent an entire set of devices with just one IP address or one small public IP address. Using IP and port address translation, Port Address Translation (PAT) allows numerous hosts to share a single IP.

- Security of NAT:

+ IP address obfuscation: NAT conceals internal IP addresses from external networks, hindering attackers' ability to conduct reconnaissance and target particular devices.

+ Access Control: NAT serves as a wall separating internal networks from external networks, granting some form of access control. The attack surface is less since connections to internal devices cannot be started by external entities directly.

+ Prevention of Unsolicited Incoming Traffic: By default, NAT blocks incoming traffic that originates from outside sources. By doing this, the possibility of direct assaults like port scans or illegal access attempts is decreased.

+ Address Hiding: By assigning a single public IP address to a number of devices, NAT conceals the true number of devices that are protected by the firewall, making it more difficult for attackers to gauge the size of the network and possible targets.

References

cisco, 2023. [Online]
Available at: https://www.cisco.com/c/en/us/products/routers/network-address-translation.html#~features-and-benefits

Deshpande, C., 2023. [Online]
Available at: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall

fortinet, 2023. [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/what-is-dmz

Gillis, A. S., 2020. [Online]
Available at: https://www.techtarget.com/whatis/definition/static-IP-address

Heiligenstein, M. X., 2023. [Online]
Available at: https://firewalltimes.com/recent-data-breaches/

kaspersky, 2023. [Online]
Available at: https://www.kaspersky.com/resource-center/threats/what-is-a-security-breach

pp_pankaj, 2023. [Online]
Available at: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

Rosencrance, L., 2023. [Online]
Available at: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams