ASSIGNMENT 1 FRONT SHEET

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number and title	Unit 5: Security		
Submission date	12/08/2022	**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	
Student Name	LE TRUNG TAI	**Student ID**	GBD201817
Class	GCD0905	**Assessor name**	Tran Trong Minh
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	Tai

Grading grid

P1	P2	P3	P4	M1	M2	D1

☐ Summative Feedback:	☐ Resubmission Feedback:	
Grade:	**Assessor Signature:**	**Date:**
Lecturer Signature:		

Table of Contents

Table of figure....4

A. Identify types of security threat to organizations. Give an example of a recently publicized security breach and discuss its consequences (P1).....5

I. Defining security threat.....5

II. Threats agents to organizations.....6

1. Nation states.....6

2. Non-target specific (Ransomware, Worms, Trojans, Logic Bombs, Backdoors and Viruses perpetrated by vandals and the general public).....6

3. Employees and Contractors.....6

4. Terrorists and Hacktivists (political parties, media, enthusiasts, activists, vandals, general public, extremists, religious followers).....7

5. Organized crime (local, national, transnational, specialist).....7

6. Natural disasters (fire, flood, earthquake, volcano).....7

7. Corporates (competitors, partners).....7

III. Types of information security threats.....7

1. Insider threats.....7

2. Viruses and worms.....8

3. Botnets.....8

4. Drive-by download attacks.....9

5. Phishing attacks.....9

6. Distributed denial-of-service (DDoS) attacks.....10

7. Ransomware.....10

8. Exploit kits.....11

9. Advanced persistent threat attacks.....11

10. Malvertising.....11

IV. (Jennings, n.d.)The recent security breaches.....11

1. Crypto.com.....11

2. Microsoft.....12

3. News Corp 12
4. Red Cross 12
5. The consequences of this breach 13
V. Solutions to reduce security threat 13
B. Describe at least organizational security procedures (P2) 14
I. Acceptable Use Policy (AUP) 14
II. Access Control Policy (ACP) 15
III. Change Management Policy 15
IV. Information Security Policy 15
V. Incident Response (IR) Policy 15
VI. Remote Access Policy 16
VII. Email/Communication Policy 16
VIII. Disaster Recovery Policy 16
IX. Business Continuity Plan (BCP) 16
C. Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS (P3) 17
I. Firewall 17
1. Definition 17
2. Usage and advantage of firewall in a network 17
II. Intrusion detection system (IDS). 20
1. Definition 20
2. The usage of IDS 21
III. The potential impact (Threat-Risk) of a firewall and IDS if they are incorrectly configured in a network. 21
D. Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security (P4). 23
I. Demilitarized zone (DMZ). 23
1. Definition 24
2. The usage and security function of DMZ 24

II. Static Internet Protocol Address (static IP) 25
1. Definition 25
2. The usage and security function of static IP 26
III. Network address translation (NAT) 27
1. Definition 27
2. The usage and security function of NAT 27
References 29

Table of figure

Figure 1 Data security threats 5
Figure 2 Botnets 9
Figure 3 Ransomware 10
Figure 4 Organizational security procedures 14
Figure 5 Firewall 17
Figure 6 The working of firewall 20
Figure 7 Usage of IDS 21
Figure 8 DMZ 24
Figure 9 Static IP 25
Figure 10 NAT 27

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

I. Defining security threat

Although the phrases security threat, security event, and security incident are connected, they have diverse connotations in the field of cybersecurity.

A security threat is a harmful act committed with the intent of corrupting or stealing data or disrupting an organization's systems or the entire company. A security incident is an occurrence in which a company's data or network may have been compromised. A security incident is an event that results in a data or network compromise.

Enterprise IT must remain cautious in securing their data and networks as cybersecurity attacks change and become more sophisticated.

(Anon., n.d.)

Figure 1 Data security threats

II. Threats agents to organizations

I've researched and learned a lot of information, but now I'd want to discuss a specific topic; there are a number of 'Threat Agents' there that we should keep in mind while looking at cybersecurity, or rather complete a risk assessment. Of course, it will rely on what your business does in terms of the degree and thus the hazards outlined below, but one thing is certain: one of them will have an impact on security: security, integrity, or availability of your data.

1. Nation states

Companies in specific areas, such as telecommunications, oil and gas, mining, power production, national infrastructure, and so on, may become targets for other governments, either to disrupt operations today or to provide that nation a future grip in times of crisis.

2. Non-target specific (Ransomware, Worms, Trojans, Logic Bombs, Backdoors and Viruses perpetrated by vandals and the general public)

The number of random assaults that occur every day is so large (there are no reliable numbers to publish here) that any organization can become a victim.

3. Employees and Contractors

Unless it is a Zero-day virus, machines and software programs are highly capable of guarding against malware. Humans are frequently the weakest link in the security system, whether intentionally or unintentionally.

Common errors, such as sending an email to the wrong person, occur, but we typically recognize the error immediately and are able to correct the problem. Simple precautions, such as password-protecting data, can also assist to limit the consequences of such errors.

Unfortunately, there are also unhappy individuals who actively undermine organizations from inside. A dissatisfied internal auditor recently downloaded payroll and other HR personal data from Morrisons and released it on the internet. The ex-employee was convicted and sentenced to jail, but Morrisons was also penalized for failing to put in place the necessary technological and organizational safeguards to prevent this crime (note that Morrisons is currently appealing against the fine).

There are other situations when organizations require specialized assistance and must rely on contractors or outside entities with access to their systems or data. Third parties are frequently the source of problems since they may not have the same standards of security on their devices that have access to the controller’s data.

4. Terrorists and Hacktivists (political parties, media, enthusiasts, activists, vandals, general public, extremists, religious followers)

The amount of harm posed by these agents is dependent on your behavior, similar to the threat posed by nation governments. However, because some terrorists want to target certain industries or nations, there remains a continual potential of a random strike against you.

5. Organized crime (local, national, transnational, specialist)

Criminals seek personal data for a variety of purposes, including credit card fraud, identity theft, and bank account fraud. These crimes are now being committed on a large basis. Methodologies differ, but the final effect is the same: you and your data are being collected and utilized for evil purposes.

6. Natural disasters (fire, flood, earthquake, volcano)

While not a cyber assault, these occurrences can have a similar impact on your capacity to do business. If you are unable to access your offices, data centers, or information saved in the cloud, you are still facing a data catastrophe, and this must be considered.

7. Corporates (competitors, partners)

The fear of a rival stealing your intellectual property is evident, but we are increasingly collaborating with a wide range of partner organizations to address skills and resource gaps, or simply to deliver services. Depending on their motivations, these partner firms may steal or expose your intellectual property or personal data that you are keeping.

III. Types of information security threats

Enterprise IT must remain cautious in securing their data and networks as cybersecurity attacks change and become more sophisticated. To do so, companies must first understand the sorts of security dangers they face.

The top ten types of information security dangers that IT teams should be aware of are listed below.

1. Insider threats

An insider threat happens when someone close to a company who have authorized access to its network purposefully or accidentally misuse that access to harm the company's vital data or systems.

Insider dangers are created by careless workers who do not follow their businesses' business rules and regulations. Other insider dangers come from contractors, business partners, and third-party vendors.

Some insiders willfully circumvent security measures for the sake of convenience or in an ill-conceived attempt to become more productive. Malicious insiders deliberately circumvent cybersecurity procedures in order to erase data, steal data for later sale or exploit, disrupt operations, or otherwise harm the firm.

2. Viruses and worms

Viruses and worms are harmful software programs (malware) that are designed to destroy a company's systems, data, and network. A computer virus is a piece of harmful code that copies itself to another program, system, or host file. It remains dormant until it is activated, either intentionally or unintentionally, spreading the infection without the knowledge or approval of a user or system administrator.

A computer worm is a self-replicating software that spreads without the need for a host program or human intervention. Its primary goal is to spread infection to other computers while remaining active on the afflicted machine. Worms frequently propagate through automated and unnoticed portions of an operating system. When a worm enters a system, it instantly begins to replicate itself, attacking machines and networks that are not properly secured.

3. Botnets

A botnet is a network of Internet-connected devices, such as PCs, mobile devices, servers, and IoT devices, that are infected with and controlled remotely by a common form of malware. Typically, botnet malware scans the internet for susceptible devices. The threat actor that creates a botnet's purpose is to infect as many connected devices as possible, leveraging the computational power and resources of those devices for automated operations that are typically concealed from the devices' owners. The threat actors that operate these botnets, who are generally fraudsters, utilize them to transmit email spam, participate in click fraud operations, and create malicious traffic for distributed denial-of-service assaults.

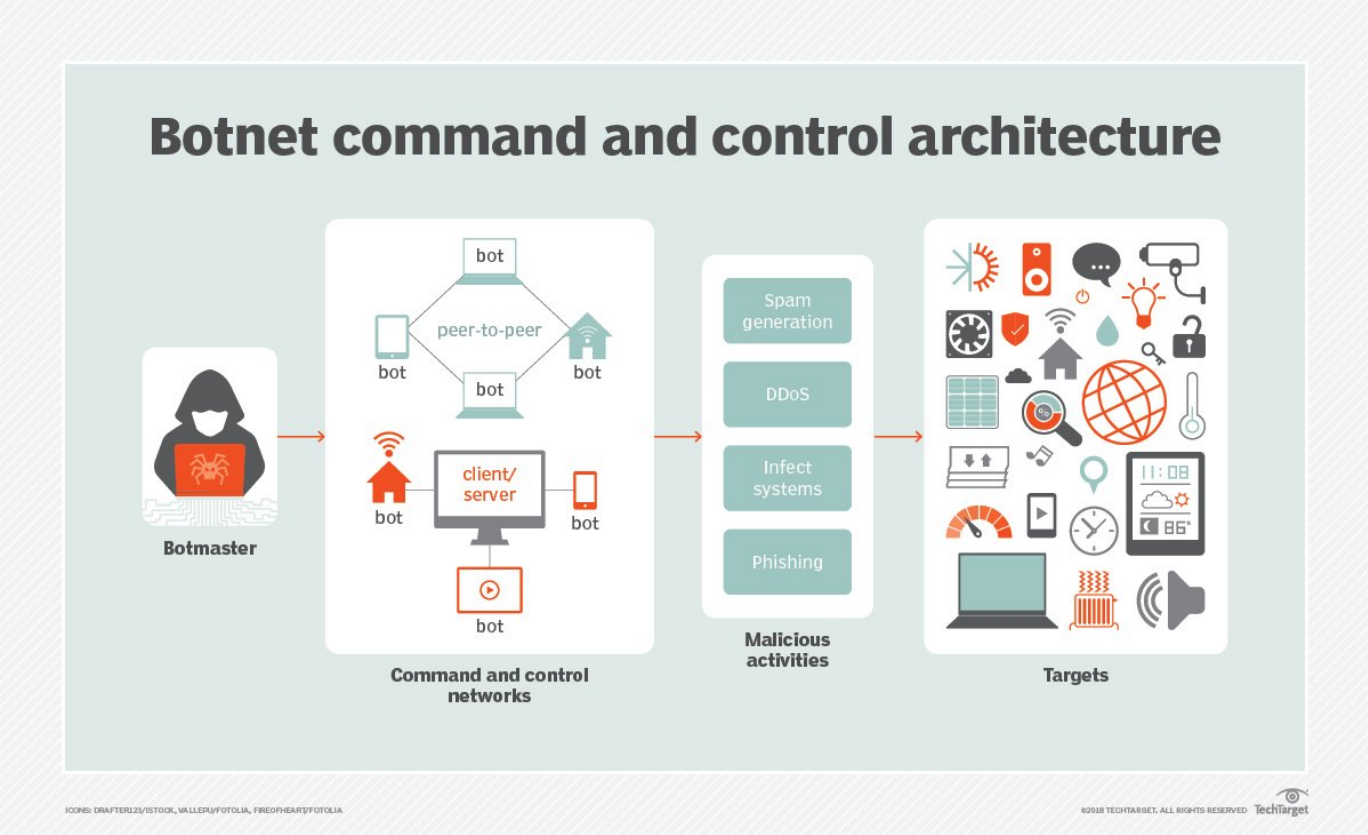


Figure 2 Botnets

(Rosencrance, n.d.)

4. Drive-by download attacks

In a drive-by download attack, malicious malware is downloaded from a website without the user's consent or knowledge via a browser, application, or integrated operating system. To start the download, the user does not need to do anything. Simply visiting or viewing a website might initiate a download. Drive-by downloads can be used by cybercriminals to inject banking Trojans, steal and collect personal information, and deploy exploit kits or other malware to endpoints.

5. Phishing attacks

Phishing attacks are a type of information security threat that uses social engineering to trick users into violating normal security practices and disclosing sensitive information such as names, addresses, login credentials, Social Security numbers, credit card information, and other financial information. Most of the time, hackers send out bogus emails that appear to be from reputable sources such as financial institutions, eBay, PayPal, and even friends and coworkers.

In phishing attacks, hackers seek to persuade users to perform a certain action, such as clicking on links in emails that direct them to bogus websites that request personal information or install malware on their computers. Opening attachments in emails can potentially install malware meant to steal sensitive information on users' devices, , send emails to their contacts, or grant remote access to their devices.

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

A distributed denial-of-service (DDoS) assault involves numerous compromised devices attacking a target, such as a server, website, or other network resource, rendering the target unworkable. The deluge of connection requests, incoming messages, or malformed packets causes the target system to slow down or crash and shut down, depriving genuine users or systems of service.

7. Ransomware

A ransomware attack locks the victim's computer, usually by encryption, preventing the victim from utilizing the device or anything saved on it. To recover access to the device or data, the victim must pay the hacker a ransom, which is usually in the form of a virtual currency like Bitcoin. Malicious email attachments, corrupted software programs, infected external storage devices, and infiltrated websites may all be used to transmit ransomware.

(Rosencrance, n.d.)

Figure 3 Ransomware

8. Exploit kits

An exploit kit is a programming tool that allows someone with no programming skills to generate, tweak, and spread malware. Exploit kits are also known as infection kits, crimeware kits, DIY attack kits, and malware toolkits. These toolkits are used by cybercriminals to exploit system vulnerabilities in order to disseminate malware or participate in other harmful activities such as stealing business data, executing denial-of-service attacks, or constructing botnets.

9. Advanced persistent threat attacks

A targeted cyberattack in which an unauthorized intruder accesses a network and remains undiscovered for a lengthy period of time is known as an advanced persistent threat (APT). An APT attack's purpose, rather than inflicting harm to a system or network, is to observe network activities and acquire information to get access, including exploit kits and malware. APT attacks are generally used by cybercriminals to steal data from high-value targets such as major organizations and nation-states over a lengthy period of time.

10. Malvertising

Malvertising is a method through which fraudsters introduce harmful code into legitimate online advertising networks and web pages. Typically, this code links people to dangerous websites or installs malware on their computers or mobile devices. Even if users do not do anything to initiate the download, their devices may get infected. Malvertising may be used by cybercriminals to distribute a variety of money-making software, such as crypto mining scripts, ransomware, and banking Trojans.

Some well-known firms' websites, including Spotify, The New York Times, and the London Stock Exchange, have unintentionally featured harmful adverts, putting consumers at danger.

IV. (Jennings, n.d.)The recent security breaches

1. Crypto.com

Cryptocurrency is huge business, so it's no surprise that Crypto.com was hacked at the start of 2022. The hack occurred on January 17th and targeted almost 500 bitcoin wallets.

Despite the fact that the blockchain is a reasonably secure transaction system, the hackers employed a rather simple approach to accomplish their goal: they bypassed the site's two-factor authentication (2FA). They made off with $18 million in Bitcoin and $15 million in Ethereum.

Crypto.com initially classified the attack as an "incident" and denied any theft, but eventually confirmed the reality and paid the impacted individuals.

2. Microsoft

Microsoft is no stranger to cyberattacks, and on March 20, 2022, the company was targeted by a hacker organization known as Lapsus$. The gang released a screenshot on Telegram indicating that they had successfully hacked Microsoft and had compromised Cortana, Bing, and numerous other products.

The hackers also stole some Microsoft documents, however by March 22nd, Microsoft claimed that the hacking attempt had been quickly terminated and that just one account had been hacked.

Microsoft stated that no customer data had been taken, and Microsoft likely benefited from its strong security team - the Lapsus$ organization has previously attacked Nvidia, Samsung, and several other corporations, and the politically motivated group was already on Microsoft's radar.

3. News Corp

News Corp is one of the world's largest news companies, so it's no wonder that hackers are keen to compromise its security - and News Corp confirmed server vulnerabilities as early as February 2020.

News Corp promptly claimed that no customer data was obtained during the attack and that the company's normal operations were not hampered.

Instead, News Corp discovered proof that its journalists' emails had been taken. The burglars have not been identified, but News Corp has suggested that espionage is at the heart of this attack, which is not surprising given that News Corp systems contain a wealth of sensitive information.

4. Red Cross

Nobody would dream of attacking the Red Cross, yet that's exactly what happened in January 2022. More than 500,000 data were compromised in an assault on a third-party contractor, including papers classified as "extremely vulnerable" by the Red Cross.

Thousands of people had their sensitive data taken in the end, and the majority of the victims are presently categorized as missing or vulnerable. The Red Cross pulled systems offline to stop the attack and investigate this apparent political breach, but no perpetrator has been discovered.

5. The consequences of this breach

The ramifications of data breaches for corporations are serious and growing. This is mostly due to the increasing regulatory burden associated with notifying individuals whose data has been hacked. Notification procedures and sanctions for firms affected by a data breach vary by jurisdiction, both inside and outside of the United States and Canada.

Companies that suffer a data breach involving their customers must determine where their clients live and which regulatory entity has jurisdiction. Regulations specify the types of data that must be disclosed following a breach, as well as who must be contacted, how the notification must be carried out, and if certain authorities must be alerted. Personal, financial, and health data breaches are often subject to notification obligations, however specific definitions vary by state. Companies undertaking international commerce may have consumers in several jurisdictions and must meet a number of standards. The costs of such a procedure, including legal fines, potential reimbursement for damages, and any related litigation, might be too expensive for certain businesses.

Data breaches involving different sorts of data can have a significant impact on a company's reputation and economic status. In addition to contractual requirements, a data breach might jeopardize a company's planned sale, as happened recently with Verizon's acquisition of Yahoo. If your competitors learn about your business techniques and are able to offer items comparable to yours at a cheaper price, your company may fail.

V. Solutions to reduce security threat

While you can retain your perimeter security and other safeguards in place, you also need a data-centric solution that allows you to precisely manage who may view certain files and data sets. This type of control is provided via encryption, but it must be the correct form of encryption. You can always control who can read a given file or email if it is properly encrypted. Even if your IT system suffers a data breach and unauthorized persons obtain access to the data, they will be unable to read it, and a data breach with regard to that data is prevented. This type of application may minimize your data breach risks to manageable levels while also protecting your organization from ruinously high data breach costs.

B. Describe at least organizational security procedures (P2)

Figure 4 Organizational security procedures

(Anon., n.d.)

I. Acceptable Use Policy (AUP)

An AUP specifies the restrictions and procedures that an employee who uses organizational IT assets must agree to in order to have access to the business network or the internet. It is normal new employee onboarding protocol. Before being assigned a network ID, they are given an AUP to read and sign. It is suggested that firms' IT, security, legal, and human resources departments consider what is included in this policy. SANS has an example that is available for fair use.

II. 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 subjects included in policies. This policy also addresses user access standards, network access restrictions, operating system software controls, and the difficulty of corporate passwords. Methods for monitoring how corporate systems are accessed and utilized are frequently mentioned, as well as how unattended workstations should be protected and how access is withdrawn when an employee departs the firm. IAPP is an outstanding illustration of this policy.

III. Change Management Policy

A change management policy is a systematic procedure for making changes to information technology, software development, and security services/operations. A change management program's purpose is to raise awareness and knowledge of planned changes within a company, and to guarantee that such changes are carried out systematically to minimize any negative impact on services and consumers. SANS has a fantastic example of an IT change management policy that is free to use.

IV. Information Security Policy

Information security rules are often high-level policies that encompass a wide range of security controls. The major information security policy is provided by the corporation to guarantee that all workers who utilize information technology assets within the organization or its networks adhere to the established rules and standards. Organizations have asked workers to sign this paper to confirm that they have read it (which is generally done with the signing of the AUP policy). This policy is intended to make workers aware that there are regulations to which they will be held accountable in terms of the sensitivity of business information and IT assets.

V. Incident Response (IR) Policy

The incident response policy is a systematic strategy to managing incidents and mitigating their impact on operations. It's the one policy that CISOs hope to never have to implement. However, the purpose of this policy is to explain the method of dealing with an event in order to reduce the impact on business operations and consumers while also lowering recovery time and costs. A high-level IR strategy is provided by Carnegie Mellon University, while a plan dedicated to data breaches is provided by SANS.

VI. Remote Access Policy

The remote access policy is a document that discusses and specifies allowed means of connecting to an organization's internal networks from a remote location. I've also seen addendums to this policy including rules for using BYOD assets. This policy is required for enterprises with scattered networks that might extend into unsecured network locations, such as the neighborhood coffee shop or unmanaged home networks. SANS provides an example of a remote access policy.

VII. Email/Communication Policy

A company's email policy is a document that explicitly defines how workers can use the company's preferred electronic communication medium. This policy appears to encompass email, blogs, social media, and chat technology. The major purpose of this policy is to inform employees on what constitutes acceptable and improper usage of company communication technologies. SANS provides an example of an email policy.

VIII. Disaster Recovery Policy

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

IX. Business Continuity Plan (BCP)

The BCP will coordinate activities throughout the firm, and the disaster recovery plan will be used to restore hardware, software, and data considered critical for business continuity. BCPs are unique to each company since they define how the company will function in an emergency. FEMA and Kapnick both have examples of BCPs that organizations may utilize to develop their own.

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

I. Firewall

(Anon., n.d.)

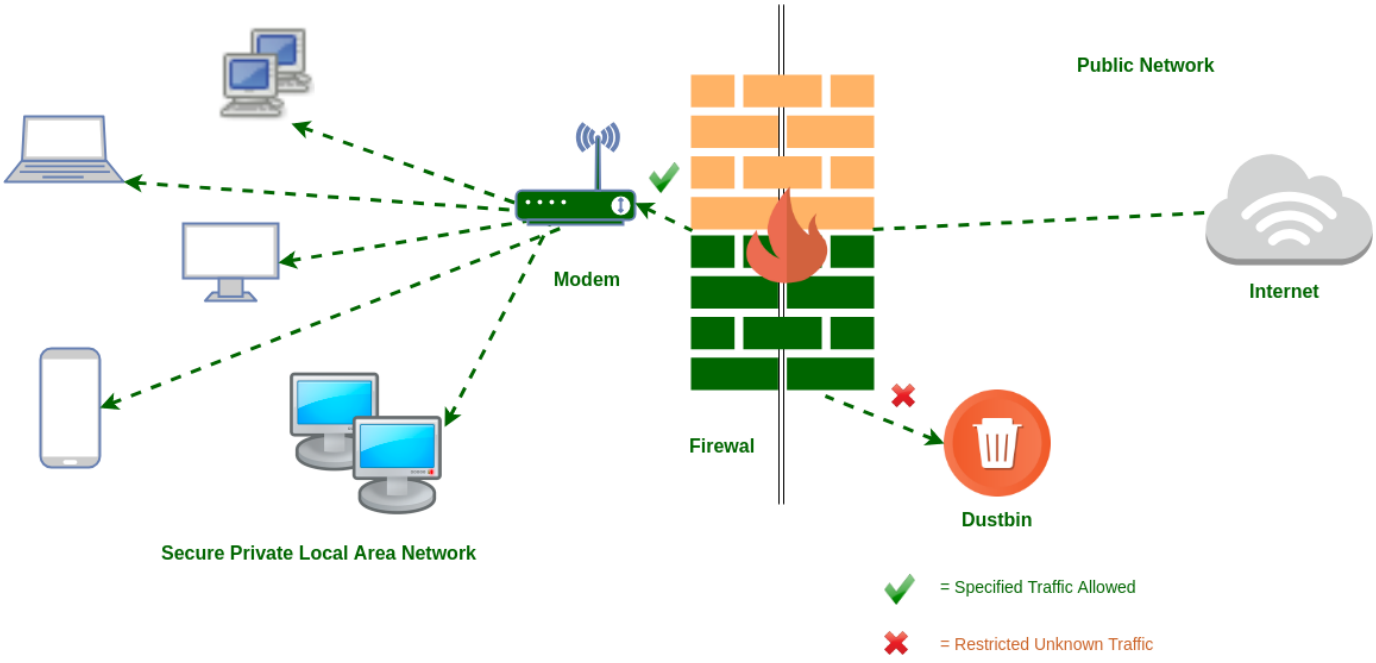


Figure 5 Firewall

1. Definition

A firewall is a network security system that utilizes rules to regulate traffic entering and exiting the system. It can be hardware or software-based. Firewalls serve as a barrier between the safe and unsecure networks. It regulates network resource access using a proactive control methodology. That is, only traffic that fits the firewall's rules may enter the network; all other traffic is blocked. As a consequence, our gadgets are safe from dangerous internet threats.

2. Usage and advantage of firewall in a network

- Usage of firewall:

The Windows firewall may be configured in a number of ways. The installation of the firewall, as well as the data and programs that it bans, may all be adjusted. You may manually block some apps, such as Microsoft Tips or Get Office, by default. By blocking them, these apps are effectively rendered inoperable. If you don't like the recommendations or reminders that appear when you buy Microsoft Office, you may disable them. Applications can transfer data to your computer at your choice; this is not possible by default. Because Windows need your permission to install and pass, this usually happens with third-party applications you install, such as iTunes. However, certain functions may be tied to Windows, such as the ability to utilize Hyper-V to construct virtual machines or Remote Desktop to remotely access your computer. You may also disable the firewall entirely if you wish to utilize a third-party security package, such as McAfee or Norton antivirus software. This is often a free trial service on new PCs, and people frequently sign up for it. If you have installed free software, you can also disable the Windows firewall.

- Advantage of firewall:
  - Versatility
    The ability to continuously upgrade and alter your network security in real time gives your IT staff a lot of freedom and variety. While your NGFW may include a hardware component, most modifications and upgrades may be handled from a single workstation. This allows you to stay more current with the evolving threat scenario. Furthermore, if your company's operations alter, you can more effectively regulate the flow of data and users.
  - Intelligence Port Control
    Typical network firewalls go beyond the traditional single-layer port method. NGFWs, on the other hand, provide multi-layered security by inspecting traffic at all levels of the network.

    Furthermore, NGFWs add application-level security to the mix, providing for greater control, greater transparency, and the ability to better regulate the data and information that enters and exits your network. The more intelligent your security system, the more effective it will be.
  - Simple Infrastructure
    The ease of use of the infrastructure is one of the primary benefits of NGFWs. By simplifying network security, your IT staff can much more easily deploy new policies across the whole network from a single device. Furthermore, transparency provides your team more control over what comes in and what gets out, which is the primary aim.
  - Updated Threat Protection

Businesses used to require separate firewalls, antivirus, ransomware protection, and intrusion detection systems. The fact that all security procedures are combined into a single seamless solution is a significant advantage of NGFWs. This not only makes life easier for your IT staff, but it also raises the overall degree of security through component collaboration.

NGFWs also go even further with deep packet inspection (DPI), which examines additional aspects of data entering your systems. As a result, decision-making about what to allow in and what to prohibit becomes more informed and effective. This, once again, contributes to the core objective of firewalls.

- Consistent Network Speed
  As previously stated, conventional firewalls can clog your systems as the scope of your defenses increases. A significant advantage is that you may continue to improve and increase the deployment of your security without sacrificing the speed of your network.

  The network's architecture encourages maximum possible throughput without sacrificing security. In layman's words, your systems remain secure, and your operations remain swift.

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

Network packets are used to transport data between networks. Along with the data, these packets carry information such as the source and destination addresses. These network packets are received by your computer via entry points known as ports.

The most straightforward analogy is to consider your computer to be your home. The IP address is your home's address, and the ports are the rooms in the building. You only let individuals inside your home whom you trust (source addresses) (destination address). The data is then further filtered, and only certain persons have access to particular rooms. You, as the owner, have access to all rooms (ports), but visitors are only permitted in select rooms (ports).

The firewall is responsible for monitoring all network packets entering and exiting your computer, analyzing them, and determining which packets are trustworthy and which are not. Based on a set of predefined rules, the firewall filters unprotected and suspicious communications.

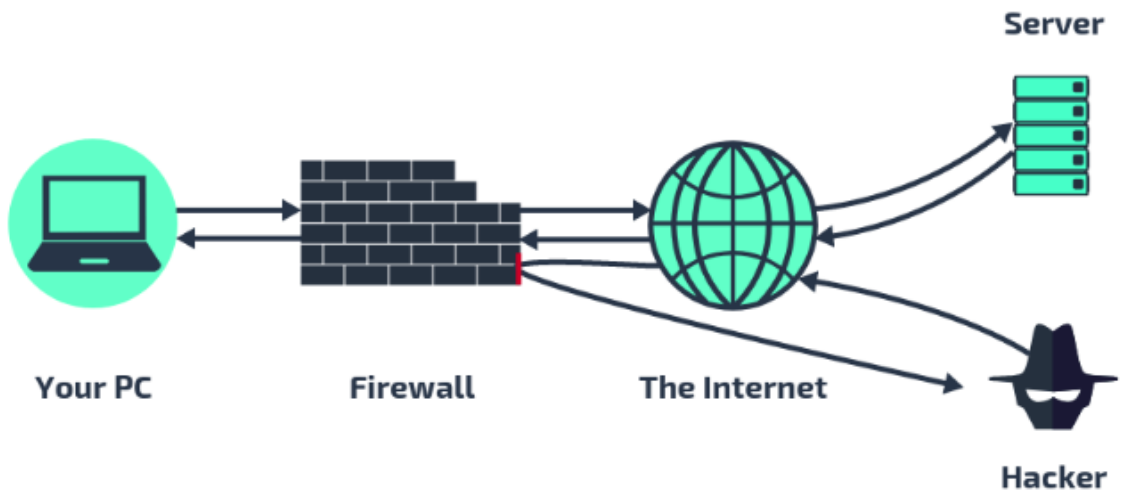


Figure 6 The working of firewall

A firewall's operation is based on the filtering of data packets. The IP address of the source or destination is the most important item a firewall looks at. If the IP address violates the set security standards, the data packet is denied, protecting you from harmful assaults.

Modern firewall software is more sophisticated, and it can filter traffic based on a variety of parameters, including keywords, domain names, apps, and individual data ports.

II. Intrusion detection system (IDS).

1. Definition

An Intrusion Detection System (IDS) is a network security solution designed to identify vulnerability exploits against a specific application or machine. Intrusion Prevention Systems (IPS) have become the main deployment choice for IDS/IPS technologies by extending IDS solutions with the capacity to prevent attacks in addition to detecting them. This post will go over the setup and functions that make up an IDS deployment.

Because an IDS only needs to identify threats, it is located out-of-band on the network infrastructure, which means it is not in the genuine real-time communication channel between the transmitter and receiver of information. Instead, IDS systems will frequently use a TAP or SPAN port to inspect a duplicate of the inline traffic stream (and thus ensuring that IDS does not impact inline network performance).

IDS was originally designed in this manner because the level of analysis necessary for intrusion detection at the time could not be completed at a rate that could keep up with components on the network infrastructure's direct communications channel.

As previously stated, the IDS is also a listen-only device. The IDS analyzes traffic and sends its findings to an administrator, but it cannot prevent a detected exploit from taking over the system automatically. Attackers can exploit weaknesses relatively fast once they reach the network, making the IDS an ineffective preventative mechanism.

2. The usage of IDS

Intrusion detection systems are used to detect abnormalities in order to capture hackers before they cause severe damage to a network.

Intrusion detection systems work by checking for signs of previously recognized assaults or deviations from normal activity. The protocol and application layers are moved up the stack to investigate these changes or anomalies. They are capable of detecting domain name system (DNS) poisonings and Christmas tree scans with high accuracy.

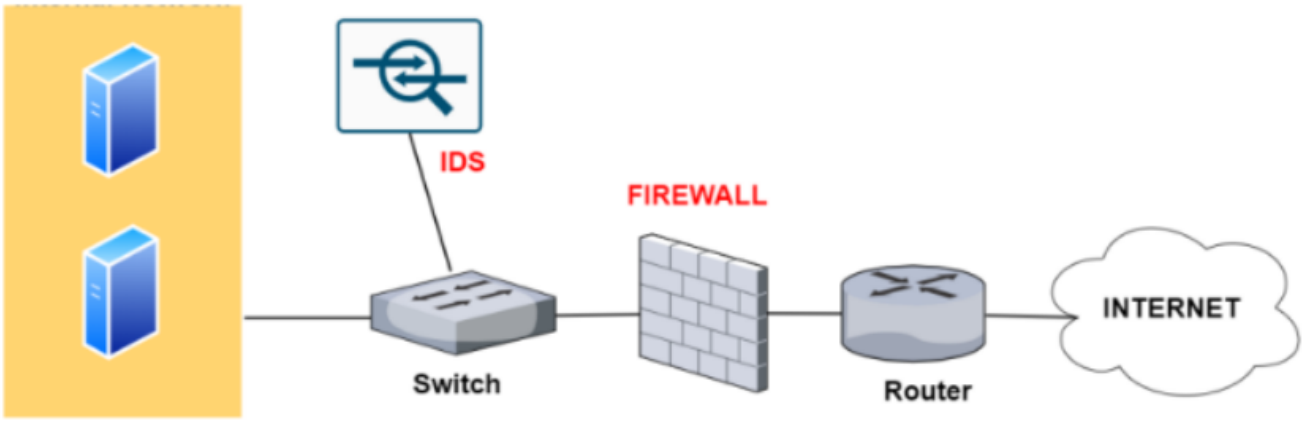


Figure 7 Usage of IDS

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

- A firewall will not protect you from inside threats.
  - The firewall cannot guard against assaults if they do not pass through it.
  - If the assault is absolutely new, the firewall cannot defend you.

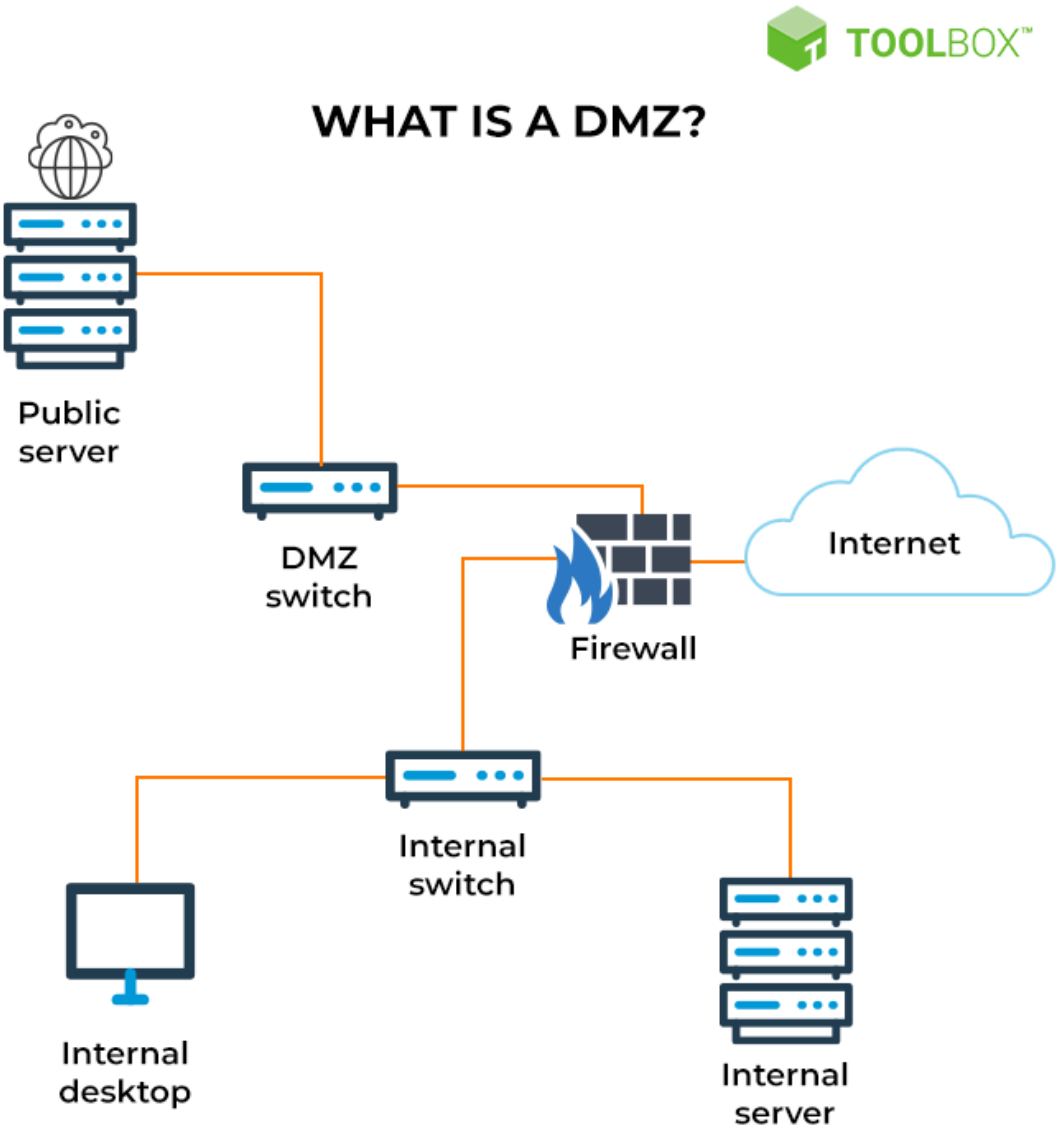
- A firewall cannot combat viruses.

❖ IDS.

- If the setting is not appropriate, it may result in false alarm status.
- The capacity to decrypt encrypted communications is limited.
- The system's deployment and operation costs are rather high.

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

I. Demilitarized zone (DMZ).



(Anon., n.d.)

Figure 8 DMZ

1. Definition

A DMZ Network is a perimeter network that protects and secures an organization's internal local-area network from untrusted traffic. A common DMZ is a subnetwork that connects the public internet to private networks.

A DMZ's ultimate purpose is to allow an organization to access untrusted networks, such as the internet, while keeping its private network or LAN safe. External-facing services and resources, as well as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers, are often stored in the DMZ.

These servers and resources are segregated and have limited LAN access to guarantee that they can be accessed through the internet but not the internal LAN. As a result, a DMZ strategy makes it more difficult for a hacker to acquire direct internet access to an organization's data and internal systems.

2. The usage and security function of DMZ

The fundamental advantage of a DMZ is that it adds an additional security layer to an internal network by restricting access to critical data and servers. A DMZ allows website visitors to access specific services while acting as a barrier between them and the organization's private network. As a result, the DMZ provides additional security advantages, such as:

- Enabling access control: Businesses can give consumers with access to services outside of their network's boundaries through the public internet. The DMZ allows access to these services while also employing network segmentation to make it more difficult for unauthorized users to get access to the private network. A proxy server may be included in a DMZ, which centralizes internal traffic flow and facilitates monitoring and recording of that traffic.
- Preventing network reconnaissance: By acting as a barrier between the internet and a private network, a DMZ stops attackers from conducting reconnaissance in search of possible targets. Servers in the DMZ are publicly accessible but are protected by a firewall, which prevents an attacker from seeing inside the internal network. Even if a DMZ system is hacked, the internal firewall keeps the private network safe and makes external spying impossible.
- Blocking Internet Protocol (IP) spoofing: Attackers try to obtain access to systems by spoofing an IP address and impersonating an authorized device connected to a network. A DMZ can detect and thwart such attempts while another service checks the authenticity of the IP address. The DMZ also allows network segmentation to establish a zone for traffic organization and access to public services apart from the internal private network.

A DMZ provides the following services:

- DNS servers
- FTP servers
- Mail servers
- Proxy servers
- Web servers

II. Static Internet Protocol Address (static IP)

(Anon., n.d.)

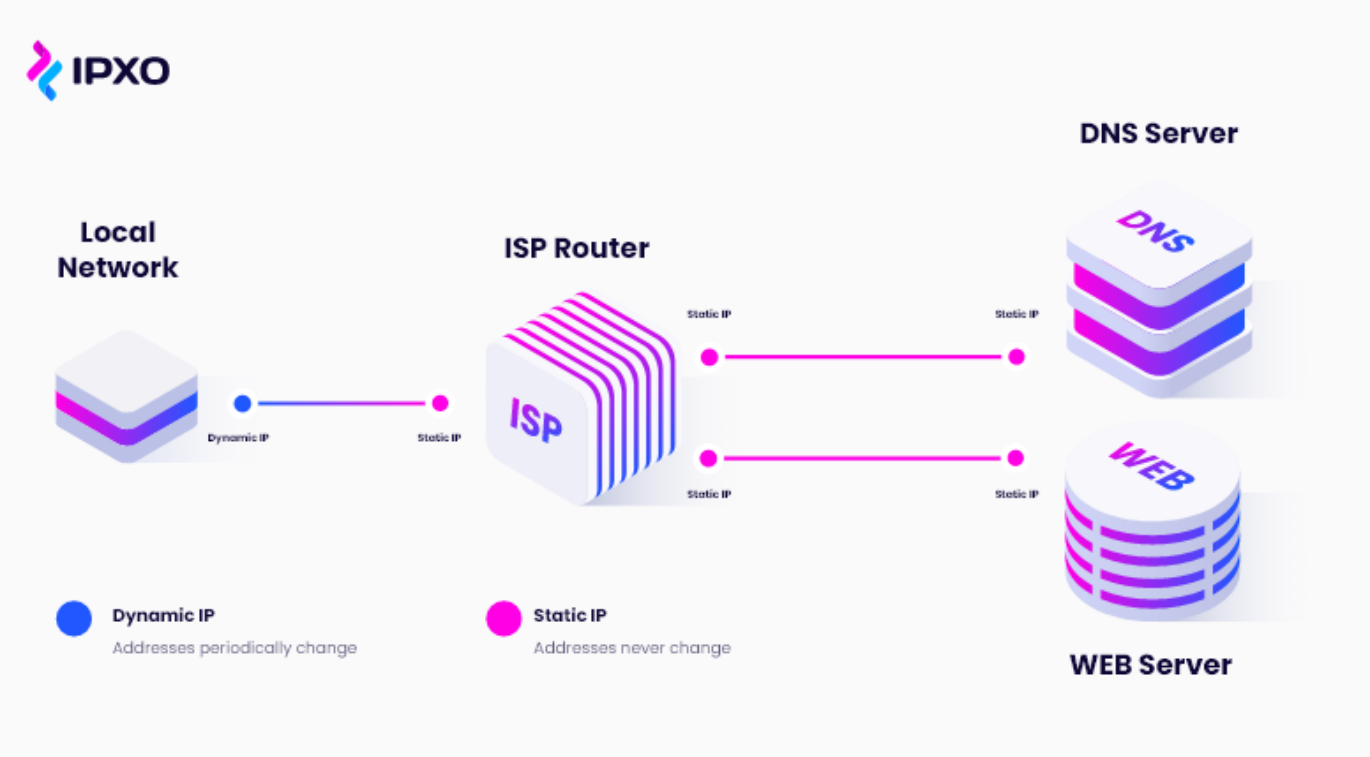


Figure 9 Static IP

1. Definition

A static Internet Protocol (IP) address is a unique number provided to a computer by an Internet service provider (ISP).

A static IP address is the inverse of a dynamic IP address and is also known as a fixed IP address or dedicated IP address.

When connecting to the Internet, a machine with a static IP address uses the same IP address.

Static IP addresses are important for gaming, website hosting, and Voice over IP (VoIP) services.

The major benefits are speed and dependability. Static IP addresses are subject to data mining and increased security issues since they remain consistent.

2. The usage and security function of static IP

Improved DNS support: With DNS servers, static IP addresses are considerably easier to set up and administer.

Server hosting: Having a static IP address makes it easier for consumers to discover you via DNS whether you operate a web server, email server, or any other type of server. In practice, this implies that clients with a static IP address will have an easier time accessing your websites and services.

Convenient remote access: Having a static IP address makes working remotely with a Virtual Private Network (VPN) or other remote access tools simpler.

Static IP addresses facilitate the usage of Audio over Internet Protocol (VoIP) for teleconferencing and other voice and video communications.

Improved geo-location services: With a static IP address, services can match the IP address to its actual location. For example, if you utilize a local weather service with a static IP address, you are more likely to receive the weather report you require rather than the one for the next city over.

III. Network address translation (NAT)

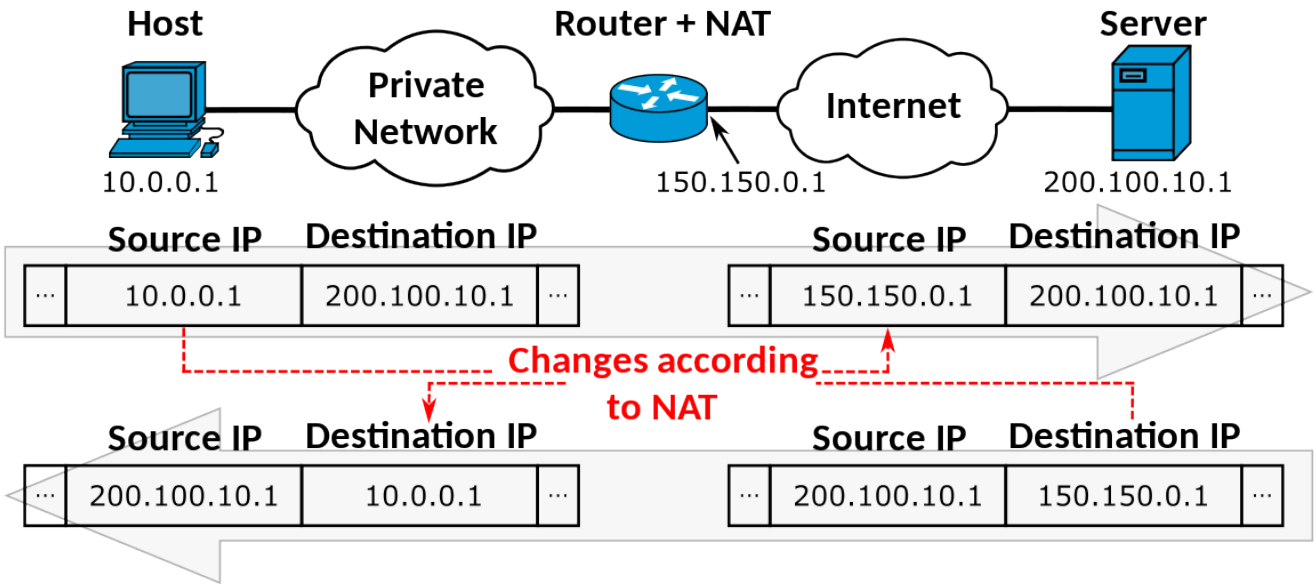


Figure 10 NAT

1. Definition

NAT (Network Address Translation) is a procedure that converts a single IP address space into a global address space. This works in conjunction with a router or firewall that links two networks. With the aid of a single public address, we may join several network address translations into an intranet. This approach is mostly used to avoid address space depletion.

Many firms adopted NAT because they wanted numerous devices to share a single IP address. It doubles the security of its features and addresses translation in networking systems. It will be beneficial in certain circumstances, but not in others.

2. The usage and security function of NAT

When you utilize NAT overload, you may keep the IPv4 address space, which gives you access to all the privileges of intranets. This is possible in this case because to Intranet Privatization. They used to save all of the addresses at the port level in numerous programs throughout this operation.

NAT includes a number of features, including load balancing and backup tools. These tools will aid in increasing the network's overall resilience and flexibility. It will happen when we build any link either in the public or any of their connections.

It employs a method known as consistent network addressing. It has a dedicated address space for the usage of public IP addresses. This occurs because as the network grows, more IP addresses are necessary.

All of your original source and destination addresses will be entirely masked using In-Network Address Translation. Without the user's authorization, so that other hosts in the network cannot contact the hosts inside them. This demonstrates that they have greater security.

They own and operate their own private IPv4 addressing system. So, even if you switch to a different addressing system, they will retain their existing addressing scheme. If the consumer switches internet service providers, it will prohibit them from changing their internal addresses.

References

Anon., n.d. [Online]
Available at: https://www.csoonline.com/article/3263738/9-policies-and-procedures-you-need-to-know-about-if-youre-starting-a-new-security-program.html

Anon., n.d. [Online]
Available at: https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/

Anon., n.d. [Online]
Available at: https://www.spiceworks.com/it-security/network-security/articles/what-is-demilitarized-zone/

Anon., n.d. [Online]
Available at: https://www.ipxo.com/blog/static-vs-dynamic-ip-address/

Anon., n.d. [Online]
Available at: https://thumbs.dreamstime.com/b/data-security-threats-infographics-information-r-risks-concept-technology-vector-illustration-black-neon-blue-color-background-106746653.jpg

Jennings, M., n.d. [Online]
Available at: https://www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022

Rosencrance, L., n.d. [Online]
Available at: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams#:~:text=A%20security%20threat%20is%20a,network%20may%20have%20been%20exposed.

Rosencrance, L., n.d. [Online]
Available at: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams#:~:text=A%20security%20threat%20is%20a,network%20may%20have%20been%20exposed.