**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** |  | **Student ID** |  |
| **Class** |  | **Assessor name** |  |
| **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:** |
| **Signature & Date:** | | |

Contents

**No table of contents entries found.**

1. **INTRODUCTION**

My article will talk about how to prevent cybercriminals. Part one covers the types of risks that organizations often face. Part two talks about the organization Security procedures. The second part talks about the harms of misconfiguring firewall policies and VPNs, and the final comparison of Network Security technologies.

1. **CONTENT**

**LO1. ASSESS RISKS TO IT SECURITY**

1. **Identify types of security risks to organizations (P1).**

There is no business is totally safe from attackers. every computer has its own threats. If you are a business even small business, IT criminals will try to exploit your system and take important information and using it in order to threating you.



1. **Identify all security threats in the organization**

* Threats can come from many kinds of form, some of which you may not recognize them and they have been called as malware. Malware is a software application specifically designed to break, corrupt or gain unauthorized access to the most popular computer systems and delivery methods via email and suspicious websites.
* **Types of malware**
* **Virus** - The classic malware that most people have heard, a virus can attach itself to other programs and copy itself when files are opened or transferred from one computer to another



* **Worm** - A program that can actively copy to other computers on the network, usually by exploiting vulnerabilities in other systems.



* **Trojan horse** - A Trojan horse camouflage to something different which not easy to recognize. Often found in unlocking software downloaded from unauthorized sources. 
* **Rootkit** - Software designed to attack administrator on the computer without being detected. It is very difficult to track them. When rootkit is set, it can be used to access to the computers and steal



* **Spyware** - An application collecting information about a person or organization.



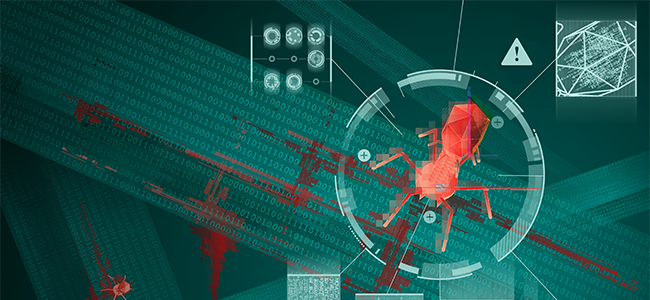
* **Adware** - often installed with other established applications, the adware will add some advertisements into the user's browser.



* **Ransomware** - It is a software designed to exploit a known Windows vulnerability. Ransomware can pass through the antivirus protection and administer malware to the victim's computer. From this point, it starts encrypting all user files and locks the victim out of their computer, ask them to pay to unlocking the computer.



* **Polymorphic malware** - An advanced type of special malware that changes its own code when copying, making it difficult for anti-malware programs to detect infection.



* **How to reduce malware.**

When there is an attack on any business or organization, it will have a very high level of risk that makes the organization stop working immediately, here are some tips to reduce risks.



* Install antivirus software and make sure the software is updated daily.
* Be careful with the email attachments you open or the websites you visit. As a rule of thumb, you should not open attachments or click links in emails from people you do not know.
* Always scan all-flash drives with antivirus software before you open any files on them because malware can hide somewhere in that file.
* The firewall should be always in on mode.
* In brief, these are just some of the threats to a security breach that you need to know, to ensure that your organization is safe and reduces data security risks in the safest way.

Security breaches and all types of organizational security risks are something very important issue in nowadays system security. Although there are many stories about security leaks and distributed denial of service (DDOS) (Schiff, 2015) attacks and repetitive alerts from security experts that businesses and individuals need to concern about. In order to better protect sensitive data, many businesses have not been properly prepared or protected from a variety of security threats.

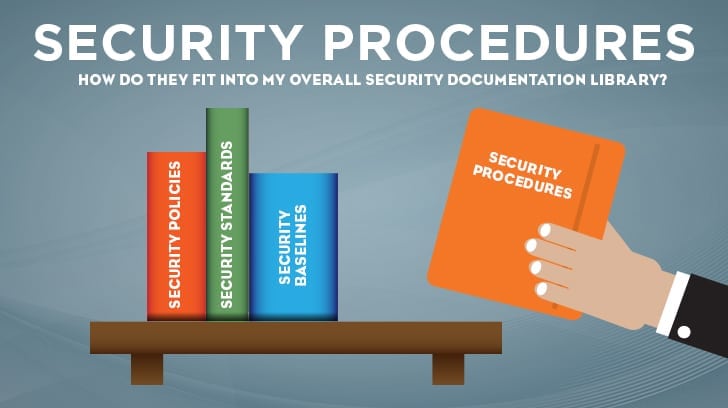
* **Identify other security threats in the organization**

In addition to the risks outside the organization when being attacked into the data system, we also have some reasons for the inside of the organization and when attached to the system it is even more dangerous when being tons of curves with external viruses. We have a few cases:

* **Staff dissatisfied**
* Employees are the biggest security risk for any organization because they know where the company's valuable data is stored and how to access it. If a trusted employee is against you, the result may be disastrous. Some ways to prevent an internal attack are:
* If something changes in personnel, remember to change your password, authenticate and authenticate information as well.
* Monitor and manage access information very closely and ensure privileged account log activity and monitor unusual behaviour.
* **Careless staff**
* In addition to malicious attacks, irresponsible employees bring many network security risks. For example, people in the company often put the password or important information in a place where easy to find. Another common problem is that employees open suspicious email attachments or surf malicious websites, which can bring malware into the system.
* The solution is to helps them know about simple security. Remind them about the importance of security. Encrypting the data so it becomes harder to steal even if the system is hacked.
* **Outdated software**
* A network security vulnerability is very common in all networks that are outdated software. More and more viruses and malware are born every day. Operating systems must be updated periodically with security patches. Obsolete and customized software can also contain serious network security issues, for example: BKAV antivirus software if not updated every day to recognize all new viruses will be attacked right away. Your best strategy now is to ensure that all patches and software definitions are constantly updated, even for business software.

1. **Describe organisational security procedures (P2).**

The security process in the organization is extremely important because all of these security procedures help an organization reduce a lot of risks that may threaten to data system and help an organization can develop as smoothly as possible. If any organization does not have security procedures, the organization may have a lot of risks.



1. **What is the security procedure?**

The security procedures in the organization are important part of instructions about implementing all the security controls listed from your organization's security policies and as detailed as possible. The security procedures contain all hardware and software components required to support your business processes as well as any security-related business processes.

1. **Why are security processes and purposes necessary in the organization?**

The purpose and processes of organizational security procedures are protecting and reducing risks in implementing security controls. They must be enforced every time a security control or business process is followed by all of these procedures. For example, when you enter a highly secure place you must follow all the checklists before get inside there. In simple thinking, they do it to make sure that everything must be safe from bad factors. Although security is stringent and armed to ensure safety, they still follow the checklist. Following the checklist can keep safe and avoid some unexpected risks. In addition, if the process is not followed in the database, the system administrator may skip a step that leads to the server or data being unacceptable and facing a very dangerous risk in organizational security.

1. **What is the relationship between security policy and security procedures?**
2. **Security procedures are built based on the organization's privacy policy.**

Organizational security policies are an important platform for an organization's security program. The important principles of all security policies are required to guide the implementation of all of the organization's security policies. Like all security policies, all security processes must also be focused on organizational behaviour. In addition, all privacy policies once mentioned who, what and why are required, all security procedures must notify all individuals in the organization at the same time. To help focus on implementing all security procedures in the organization, all the best standards must be enforced and the baseline is also required to be clearly defined. In addition, all standards and baselines should be geared towards technology to implement within an organization, while all policies and processes must focus on guiding behaviours.

To better understand the organization's security process, imagine that in your organization, any policies that have been defined and related to creating backups for important information of team users Your position. The organization's security process will be required to support and determine when all backups are made, to the same location and backup media will be recorded as well as all individual steps will be made backup. In summary, keep in mind that all procedural steps will be required to guide all an individual's behaviours to get the most clear and desirable end result in an organization.

1. **Organization security procedures must have all the details.**

The organization's security policy must contain all security requirements in a general or advanced way. In addition, all security procedures must provide the most detailed and understandable for an individual who is not familiar with the privacy policy process to achieve the desired results in the organization's privacy policy, because if the privacy policy is too difficult to understand, anyone will not understand, and they will cause many risks in the organization's privacy policy.

1. **All of the organization's security procedures include problems**

Without any organization without an organization's own security policies and procedures in the organization's and post-data systems, one of the most popular organization's security policies includes:

* **Organization information**

The purpose of this information is to declare all of the organization's privacy policies and all of these policies belong to the organization's ownership of your organization.

* **Apply policy**

The purpose of the application This policy will apply to all information created, received, stored and for the organization's data and applications including: Use, management and storage, information and data. The application of this policy covers all areas, such as: Access control, information security incident management, development and maintenance.

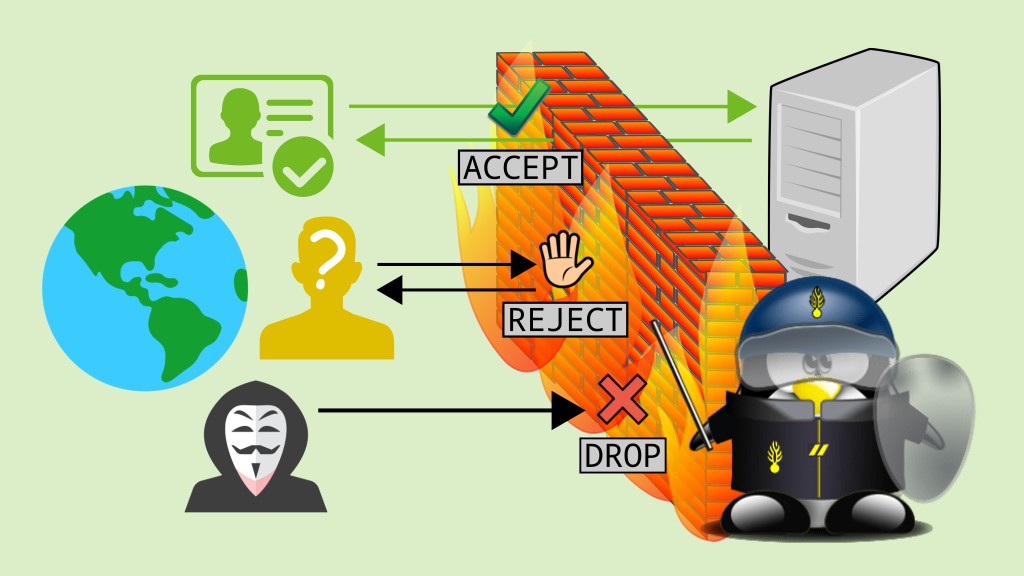
* **Policy principles**

The principle of an organizational security policy is to identify all the principles to establish all security measures to ensure the integrity of the organization security and reduce all security risks organization, such as: Take all appropriate control measures to protect information from being disclosed to the outside, delete or copy all information of the organization.

**LO2. DESCRIBE IT SECURITY SOLUTIONS**

1. **Identify the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs (P3).**
2. **Firewall**
3. **What is the Firewall**

A firewall is a piece of software that stands between a computer or network and the Internet. Connecting a computer directly to the global network is like leaving your front door open, allowing outsiders free access to your system. Any request will pass through to vulnerable systems, allowing unscrupulous third parties to exploit your computers for their own gain. A firewall serves to block these unauthorized requests, passing through only designated traffic.



1. **The purpose of the firewall**

* Firewalls prevent malicious programs from accessing and damaging your computer. Software firewalls provide another layer of security. They also prohibit malware on your own computer from being sent to others.
* It blocks incoming data that might contain a hacker attack.
* It hides information about the network by making it seem that all outgoing traffic originates from the firewall rather than the network. This is called Network Address Translation (NAT).
* It screens outgoing traffic to limit Internet use and/or access to remote

1. **About incorrect configuration**

* **Firewall policies:**

Non-standard authentication mechanisms will get the impact of failure firewall. Remote Control Gone Wrong so Traffic doesn’t reach it’s intended destination, it will likely be noticed fairly quickly when the process doesn’t work as expected.



* **Configuration mistakes:**
* Blocked
* Get wrong rare limiting, the number of data pass through the firewall are unstable
* Broad policy configurations
* Wrong destination.
* Hard to route

Unexpected traffic reaches a destination it should not. Get Risky rogue services, management services and a false sense of security it could generate, making troubleshooting another part of the system more difficult.

On bad standards/ instructions/ policy. Dangerous ports open (This is causing some negative consequences), it’s also attacking a vector for individuals with malicious intent (The cyber threat).

1. **VPN**
2. **What is the VPN**

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely.  VPN technology is widely used in corporate environments.



1. **The purpose of VPN**

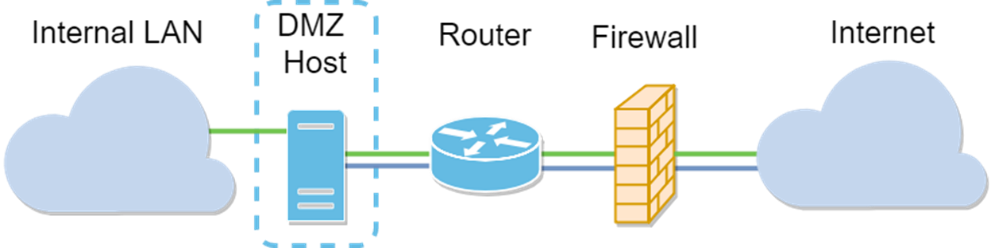
* VPN makes it difficult for hackers to infiltrate or interfere with the work of individuals or businesses.
* Hide browsing from your local network and ISP (internet provider)
* Securing access to internal systems of an enterprise
* Access geographically blocked websites

1. **Problems of misconfiguration VPN:**

* **Here are some VPN and related technical problems:**
* VPN client software must work on all user devices, such as a computer or mobile phone, this will help your company avoid a VPN security breach.
* VPN protocols must work end-to-end through firewalls, routers and switches.
* Must pick VPN devices that are compatible and interoperable with concentrators, appliances and servers.
* Balance security and protection against the ease and convenience of using your chosen VPN to avoid technical VPN issues.
* The data that can be used is limited.
* The speed of the internet is slow, ads are added with.
* The computer can be used with no allowance.

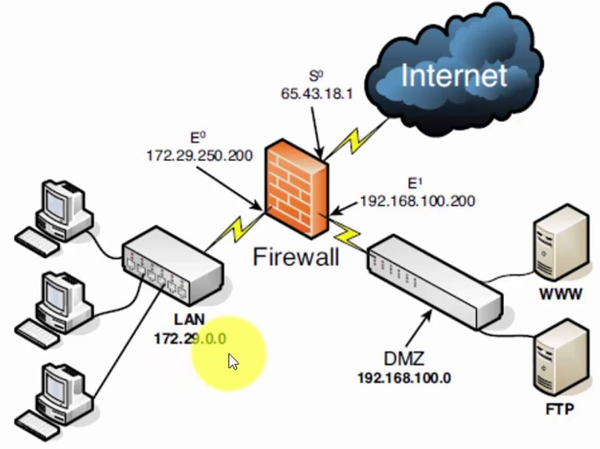
1. **Using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security (P4).**
2. **DMZ**
3. **Definition**

DMZ which stands for demilitarized zone is a network segment that is part of a local area network and separated from the other secure network segment. The devices included in the DMZ can be mail server, web server or public database. It is applied to office network or enterprise network in order to make sure that the entire network won’t be affected by any outside threats or danger



1. **How DMZ works**

A DMZ is a management server that is placed on the network that contains multiple network interfaces that play specific roles in protecting the local area network (LAN). IT administrators use a 4-port Ethernet card in the firewall to create a series of networks that include an internal trusted network, DMZ network, and the untrusted network which is the Internet.

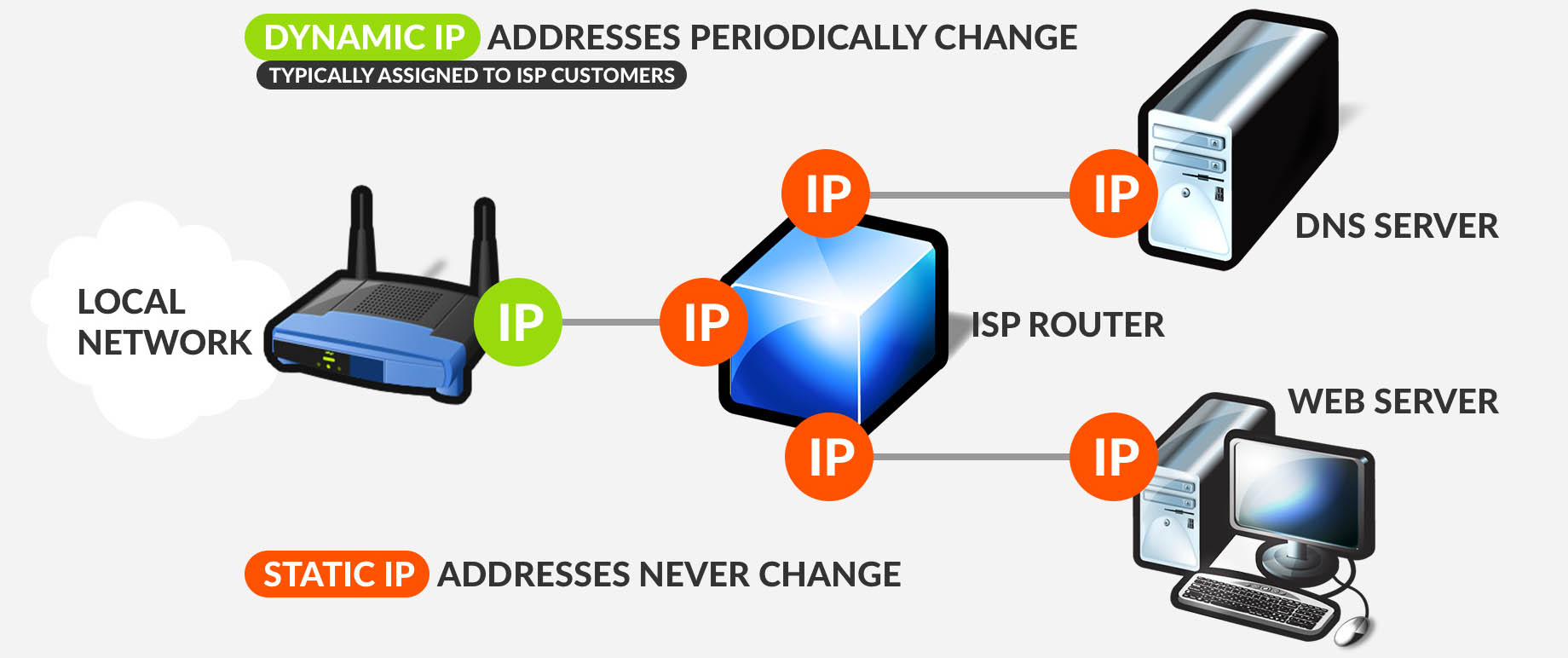


Multiple DMZ networks are created to reduce the impact of damage to the system in the event that one of the DMZ hosts is compromised for any reason. Although a regular network firewall is installed to provide protection for the local area network, a DMZ establishes rules for protecting the DMZ network from the Internet. It also establishes rules for protecting the local area network from the DMZ in the event the DMZ is compromised. This provides added protection against hackers that try to breach the local area network.

1. **Static IP**
2. **Definition**

A static IP address is an IP address that was manually configured for a device instead of one that was assigned by a DHCP server. It’s called static because it doesn't change a dynamic IP address, which does change.

Routers, phones, tablets, desktops, laptops, and any other device that can use an IP address can be configured to have a static IP address. This might be done through the device giving out IP addresses (like the router) or by manually typing the IP address into the device from the device itself.



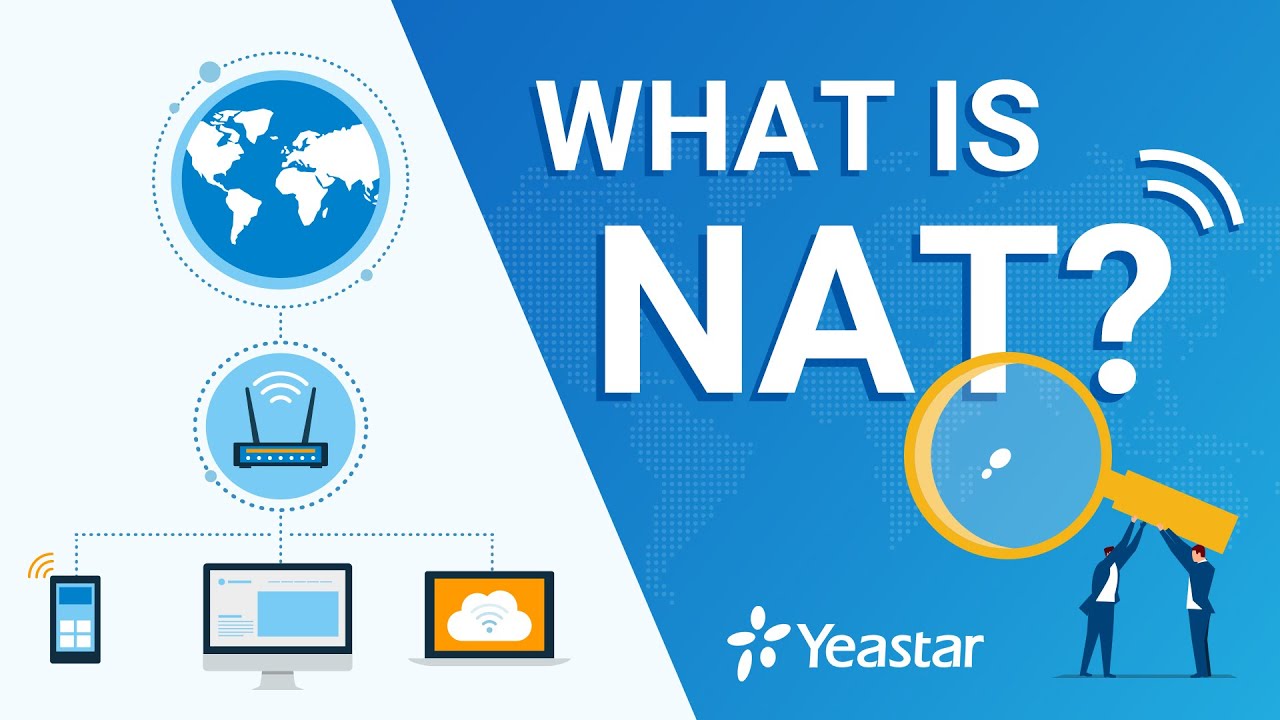
1. **How does static IP work?**

At the point when Static IP Addresses are used. Static IP locations are essential for gadgets that need steady access.

On the other hand, if the server were doled out a dynamic IP address, it would change infrequently which would keep your switch from knowing which computer on the network in the right server. People can use the static IP address to host a private file or FTP server, host a private website or domain name server or even a chat server.

1. **NAT (Network Address Translation).**
2. **Definition**

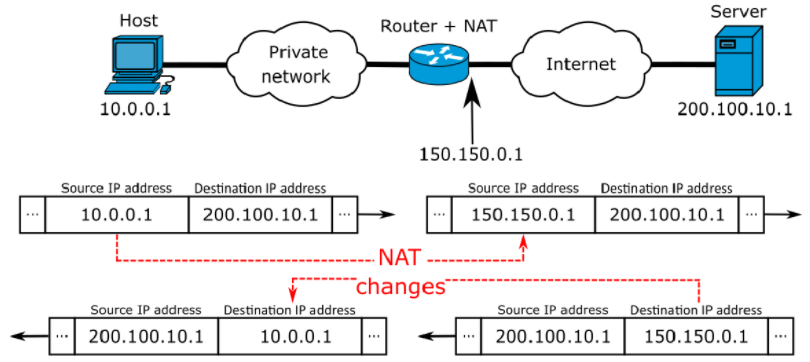
NAT stands for network address translation. It’s a way to map multiple local private addresses to a public one before transferring the information. Organizations that want multiple devices to employ a single IP address use NAT, as do most home routers.



1. **How NAT works**

Let’s say that there is a laptop connected to a home router. Someone uses the laptop to search for directions to their favorite restaurant. The laptop sends this request in a packet to the router, which passes it along to the web. But first, the router changes the outgoing IP address from a private local address to a public address.

If the packet keeps a private address, the receiving server won’t know where to send the information back to — this is akin to sending physical mail and requesting return service but providing a return address of anonymous. By using NAT, the information will make it back to the laptop using the router’s public address, not the laptop’s private one.



1. **CONCLUSION**

In this report, the importance of security especially security of networking. When understand the basic security, we can protect our information, important and sensitive information by ourselves.

Furthermore, this report also gives some kind of dangerous attackers who can able to store any data of any person. In this case, we can know how to avoid them by using some tips or reliable tools for our devices. Networking is not simple as we thought, you may get in trouble even though you only using a network for social purpose like Facebook or Twitter.

1. **REFERENCES**

**[1]**. ACADEMY, B. L.-2. (2009, 7 2). QUẢN TRỊ RỦI RO IT TRONG DOANH NGHIỆP HIỆN ĐẠI.Retrieved 7 2, 2009, from <https://infochief.com.vn>: https://infochief.com.vn/blog/quan-tri-rui-ro-trong-doanh-nghiep-hien-dai.html

**[2]**. BenSanders. (2017, June 16). Information Security Awareness: Identifying Security Threats and Vulnerabilities. Retrieved June 16, 2017, from https://www.digitalcraftsmen.com:https://www.digitalcraftsmen.com/information-security-awareness-identifying-security-threats- vulnerabilities/

**[3]**. McConnachie, L. (2019, Mar 19). 10 Cyber Security Threats In 2017 That You Can't Just Ignore... [How Vulnerable Are You?]. Retrieved Mar 19, 2019, from https://purplegriffon.com: https://purplegriffon.com/blog/10-cyber-security-threats-in-2017