UNIT 19

Security

ASSIGNMENT

No.1

Learner’s name: Võ Thị Quỳnh Như

Assessor name: Ho Hai Van

Class: GCS0801A

Learner’s ID: GCS18612

Subject’s ID: 1623

Assignment due: Assignment submitted:28/4/2020

Assessment Brief 1

Qualification	**BTEC Level 5 HND Diploma in Computing**		
Unit number	Unit 5: Security		
Assignment title	Security Presentation		
Academic Year	2019 – 2020		
Unit Tutor	Ho Hai Van		
Issue date		**Submission date**	28/4/2020
IV name and date			

Submission Format

The submission is in the form of two documents/files:

1. A ten-minute Microsoft® PowerPoint® style presentation to be presented to your colleagues. The presentation can include links to performance data with additional **speaker notes** and a **bibliography using the Harvard referencing system.** The presentation slides for the findings should be submitted with speaker notes as one copy.
2. A detailed report that provides more thorough, evaluated or critically reviewed technical information on all of the topics.

You are required to make use of the font **Calibri, Font size 12, Line spacing 1.5, Headings,** P**aragraphs**, S**ubsections and illustrations** as appropriate, and all work must be **supported with research and referenced** using the **Harvard referencing system.**

Unit Learning Outcomes

LO1 Assess risks to IT security.

LO2 Describe IT security solutions.

LO3 Review mechanisms to control organizational IT security.

LO4 Manage organizational security.

All the business organizations should always monitor their computer networks to block potential unauthorized access and other kind of attacks. It is also important to establish a secured network and security support system due to the following reasons:

1. To protect Client Data and information:
2. Keep Shared Data safe and secure:
3. Protect Computer systems From Harmful Spyware:
4. To Comply with Ethical Responsibilities and Regulatory Requirements:
5. Increase Network Performance:

Network Security and support system is one of the most vital factors to consider, no matter how big or small a business organization is!

Assignment Brief and Guidance

SCENARIO:

You work as an IT Security Specialist for APPLE Corporation and as part of your role, you have been asked to prepare a presentation to help junior staff members on the tools and techniques associated with identifying and assessing IT security risks together with the organizational policies to protect business critical data and equipment's.

Prepare a presentation that will include:

1. Security legislation, types of security risks, describe the organizational security procedure and method to asses and treat security risk. Also in your report provide solutions and the management associated with operating effective IT security procedures.

2. Describe IT security solution, by giving a review of different security technologies supported with the tools and software used to develop effective IT security practice in an organization. Identify the potential impact to IT security of incorrect configuration of firewall policies and third- party VPNs. Your report should clearly show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security. Your report should be summarized by discussing three benefits to implement network monitoring systems with supporting reasons.

"Having organizational policies related to IT security is essential".

3. Review mechanisms to control organizational IT security : Discuss risks assessment procedures and explain data protection processes and regulations as applicable to an organization IT Security Audits.

4. List and justify the main components in a company disaster recovery plan. Choose a company of your choice and evaluate the suitability of the tools used in their security policy. Based on your findings, design a security policy and discuss with the management the implementation process.

On this task, you should define business continuity planning and testing process. This process involves the procedures of backup/restoration of data and security audits. In addition, you should provide testing procedures for an organization data, network, and systems.

Assessment Criteria		
Pass	**Merit**	**Distinction**
LO1: Assess risks to IT security		

P1 Identify types of security risks to organizations. **P2** Describe organisational security procedures.	**M1** Propose a method to assess and treat IT security risks.	**D1** Investigate how a 'trusted network' may be part of an IT security solution.
LO2: Describe IT security solutions		
P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third- party VPNs. **P4** Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.	**M2** Discuss three benefits to implement network monitoring systems with supporting reasons.	

Contents

P1 Identify types of security risks to organizations

The risks that Apple may face:

No.	Type of risk	Description	Asset affected	Severity when risk happened
1	Phishing attacks	Hackers often send spam emails or impersonate other legitimate corporations / banks / organizations to steal data. Be careful before clicking on suspicious links in emails, especially emails asking for personal information or payments. Remember that legitimate businesses that provide payment options will always have an SSL (HTTPS) digital certificate.	Staff from computer or total computers in the company.	Computers will not work or will be stolen information, virus can lose data
2	Weak password	In fact, there are many people who don't care about password security. However, after a series of security incidents in 2014 so far, password security has become more urgent. With technological advances, hackers can crack most passwords. Even according to an article, 90% of passwords can be cracked in seconds.	User	Hired account, revealing or losing personal information or confidential information of the business.
3	The device has not been patched	All of the hardware and software used by small businesses carries the risk of hacker intrusion. According to Shlomi Boutnaru, co-founder and CTO of CyActive, hackers can take advantage of the following devices to exploit data: • Network devices such as routers, servers, and printers that have software in the operating system. • Patch vulnerabilities have not been updated or their hardware is not designed to be updated after a security vulnerability has been discovered.	Staff from computer or total computers in the company.	Computers will not work or will be stolen information
4	Do not encrypt data	In the era of mobile, BYOD and Big Data, information is increasingly exchanged easily. Hackers will have more chances to attack your company's data.	Staff from computer or total computers in the company.	Data may be exposed or lost.

5	USB	Hackers will pretend to drop the USB containing spyware in a company's parking lot. If someone else picks it up and installs it on the computer, the software will be activated. At this point, hackers will invade your computer to exploit company resources. Although not new, but still many people fall victim to this trick.	Staff from computer or total computers in the company.	Computers will not work or will be stolen information, virus can lose data
6	Insider	A disgruntled employee can also become a threat to information security, even for small businesses. According to Cortney Thompson, CTO of Green House Data, “Internal attacks are one of the biggest threats to data and systems. Insider, especially IT employees - who have access to the network, data centers, administrative accounts, can cause serious damage.	Confidential information, creations, company assets.	Data may be exposed or lost.
7	Malware	Malware is a major threat to small businesses. Through ads and malicious download files, it can cause viruses to enter the computer, risking data loss. Small businesses are at greatest risk when the budget for firewalls and antivirus tools is limited. So, make sure all your software, applications, email programs and browsers are updated regularly.	Staff from computer or total computers in the company.	Computers will not work or will be stolen information

How to fix those risks?

1. Phishing attacks

Deploying a firewall for desktop / network or anti-spam software will limit the possibility of this type of attack.

2. Weak password

Use passwords that are more complicated, have more special characters, and are case-sensitive.

3. The device has not been patched

Regularly check and repair milk and equipment related to data to promptly detect and repair holes.

4. Do not encrypt data

Data encryption and authentication is a necessary security measure. One suggestion for you is security Two-step verification.

5. USB

Do not use storage devices and transfer data of unknown origin.

6. Insider

Human resources department should focus on checking the resume before hiring as well as care for the employee's compensation needs.

7. Malware

Businesses need to train their employees to know how to minimize the risk of malware attacks:

- Install anti-virus software and ensure it is up to date and safe.

- Always review the email files you open or websites you visit. As a general rule, you should

Do not open the file or click the link in the email from those you do not

- know or even from people you know, but from people you didn't expect

- Attachments or links.

P2 Describe Organizational security procedures

Security Procedure

A security procedure is a fixed sequence of the activities required to perform a particular security task or function. Procedures are usually designed to be followed as a sequence of steps as a consistent and repetitive path or cycle to achieve an end result. Once implemented, security procedures provide a set of established actions for conducting the security affairs of the organization, which will facilitate training, process auditing, and process improvement. Procedures provide a point of departure for enforcing the continuity required to eliminate variability in security procedures, which improves security control within the organization. Decreasing variability is also a good way to reduce duplication, improve efficiency and increase safety department performance.

Privacy policies and procedures are a major part of any organization. These steps are essential for implementing IT security management: delegating security roles and responsibilities to various security personnel; set rules for expected behavior from users and security role players; set up rules for business continuity; and more. The security policy should be agreed upon by most employees in the organization and should be supported by top management. This helps to prioritize at the overall organizational level.

The following list is an overview of some of the issues that an organization's policies are supposed to tackle. Remember, however, that the universal list is virtually infinite, and the list of each company will include issues depending on a variety of factors like their size and importance and responsiveness. Knowledge which it contains or processes. Such important issues protected by most privacy policies are:

- Access control standards. These are standards on controlling the access to various systems. These include password change standards.
- Accountability. Every user should be responsible for her own accounts. This implies that any activity under a particular user ID should be the responsibility of the user whose ID it is.
- Audit trails. There should be an audit trail recorded of all the activities under a user ID. For example, all the login, log-out activities for 30 days should be recorded. Additionally, all unauthorized attempts to access, read, write, and delete data and execute programs should be logged.
- Backups. There should be a clearly defined backup policy. Any backups should be kept in a secure area. A clear policy on the frequency of the backups and their recovery should be communicated to the appropriate personnel.
- Disposal of media. A clear policy should be defined regarding the disposal of media. This includes a policy on which hardware and storage media, such as disk drives, diskettes, and CD-ROMs, are to be destroyed. The level and method of destruction of business-critical information that is no longer needed should be well defined and documented. Personnel should be trained regularly on the principles to follow.
- Disposal of printed matter. Guidelines as to the disposal of printed matter should be specified and implemented throughout the organization. In particular, business-critical materials should be disposed properly and securely.
- Information ownership. All the data and information available in the organization should have an assigned owner. The owner should be responsible for deciding on access rights to the information for various personnel.
- Managers’ responsibility. Managers at all levels should ensure that their staff understands the security policy and adheres to it continuously. They should be held responsible for recording any deviations from the core policy.
- Equipment. An organization should have specific guidelines about modems, portable storage, and other devices. These devices should be kept in a secured physical environment.

- Communication. Well-defined policy guidelines are needed for communication using corporate information systems. These include communications via emails, instant messaging, and so on.
- Work procedures and processes. Employees of an organization should be trained to secure their workstations when not in use. The policy can impose a procedure of logging off before leaving a workstation. It can also include quarantining any device (such as a laptop) brought from outside the organization before plugging it into the network.

P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and third- party VPNs

Network security is the process of taking measures to prevent security or virus vulnerabilities contained in software, applications, websites, servers, data ... in order to protect network infrastructure. Or it can also be understood that the concept of network security is the prevention of unauthorized access, misuse, against modification, destruction or improper disclosure of information, network security should be ensured. Information, data in the safest condition.

Firewall Policy

A firewall is an appliance (a combination of hardware and software) or an application (software) designed to control the flow of Internet Protocol (IP) traffic to or from a network or electronic equipment. Firewalls are used to examine network traffic and enforce policies based on instructions contained within the Firewall's Ruleset. Firewalls represent one component of a strategy to combat malicious activities and assaults on computing resources and network-accessible information. Other components include, but are not limited to, antivirus software, intrusion detection software, patch management, strong passwords/passphrases, and spyware detection utilities.

Firewalls are typically categorized as either “Network” or “Host”: a Network Firewall is most often an appliance attached to a network for the purpose of controlling access to single or multiple hosts, or subnets; a Host Firewall is most often an application that addresses an individual host (e.g., personal computer) separately. Both types of firewalls (Network and Host) can be and often are used jointly.

This policy statement is designed to:

Provide guidance on when firewalls are required or recommended. A Network Firewall is required in all instances where Sensitive Data is stored or processed; a Host Firewall is required in all instances where Sensitive Data is stored or processed and the operating environment supports the implementation. Both the Network and Host Firewalls afford protection to the same operating environment, and the redundancy of controls (two separate and distinct firewalls) provides additional security in the event of a compromise or failure.

Raise awareness on the importance of a properly configured (installed and maintained) firewall.

Policy Statement:

Where Electronic Equipment is used to capture, process or store data identified as University “Legally/Contractually Restricted” and the Electronic Equipment is accessible via a direct or indirect Internet connection, a Network Firewall appropriately installed, configured and maintained is required.

All installations and implementations of and modifications to a Network Firewall and its Configuration and Ruleset are the responsibility of the authorized Northwestern University Information Technology (NUIT) Firewall Administrator, with this exception: maintenance of a Network Firewall Ruleset may be performed by other than NUIT personnel where permitted by a documented agreement between NUIT and the School/Department/Business Unit assuming the Firewall Administrator’s responsibilities.

Where Electronic Equipment is used to capture, process or store data identified as University “Legally/Contractually Restricted” and the Electronic Equipment is accessible via an Internet connection, a Host Firewall appropriately installed, configured and maintained is required where the operating environment supports that installation. The maintenance of the Host Firewall’s Configuration and Ruleset is the responsibility of that system’s administrator.

Where Electronic Equipment is used to capture, process or store data identified as University “Internal” or “Public” and the Electronic Equipment is accessible via an Internet connection, a Host and/or Network Firewall is recommended.

Use of a Host Firewall is recommended for any individual Host with access to the Internet; its maintenance is the responsibility of the individual user or designated support personnel.

The potential impact to IT security of incorrect configuration of firewall policies

1. Non-standard authentication can get the impact of failure of the firewall. The wrong remote controls, results in traffic not achieving your target, when the process doesn't work it can be detected very quickly.

Faults in configuration:

- It was blocked
- Get wrong limiting, too much or too little network traffic passed the firewall.
- Policy configuration is too large
- Change it to the wrong destination.
- Could not be found.

2. Open Policy Configurations

Firewalls that allow traffic from any source to any destination pose a security risk. IT teams often use open policy configurations when they aren't sure what they need, since starting with broad rules makes it easy to tweak firewall configurations later. However, too many IT teams never get around to defining more specific firewall policies, leaving the network exposed to risks.

Your IT team should give the minimum level of privilege that users and services need to function normally. Regularly revisit firewall policies to find out how applications are being used, so you can reassess the privileges they need.

3. Risky Management Services

Leaving unnecessary services running on the firewall compromises security. Common offenders are dynamic routing and rogue DHCP servers that distribute IP addresses, which can lead to IP conflicts.

Once again, the solution is to follow the principle of granting the lowest level of privileges required for the services to function. Configure devices based on the functions you need them to complete, since allowing too many services to run adversely affects performance and increases network load.

Problems of misconfiguration VPN:

1. Evil hackers outside the firewall are able to hack devices inside the firewall
2. If you have public servers inside the firewall, say a web server, the public outside the firewall will not be able to access those servers.
3. Users inside the firewall are not able to access certain websites (or even all websites) on the public internet.
4. Users inside the firewall get very slow access to websites on the public internet.
5. Often a company has multiple offices in various cities that communicate with each other through VPNs set up in a firewall at each office. Misconfiguration could prevent 2 or more offices from communicating with each other.

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

1. DMZ

STRENGTHENING THE INTERNAL NETWORK SYSTEM WITH DMZ

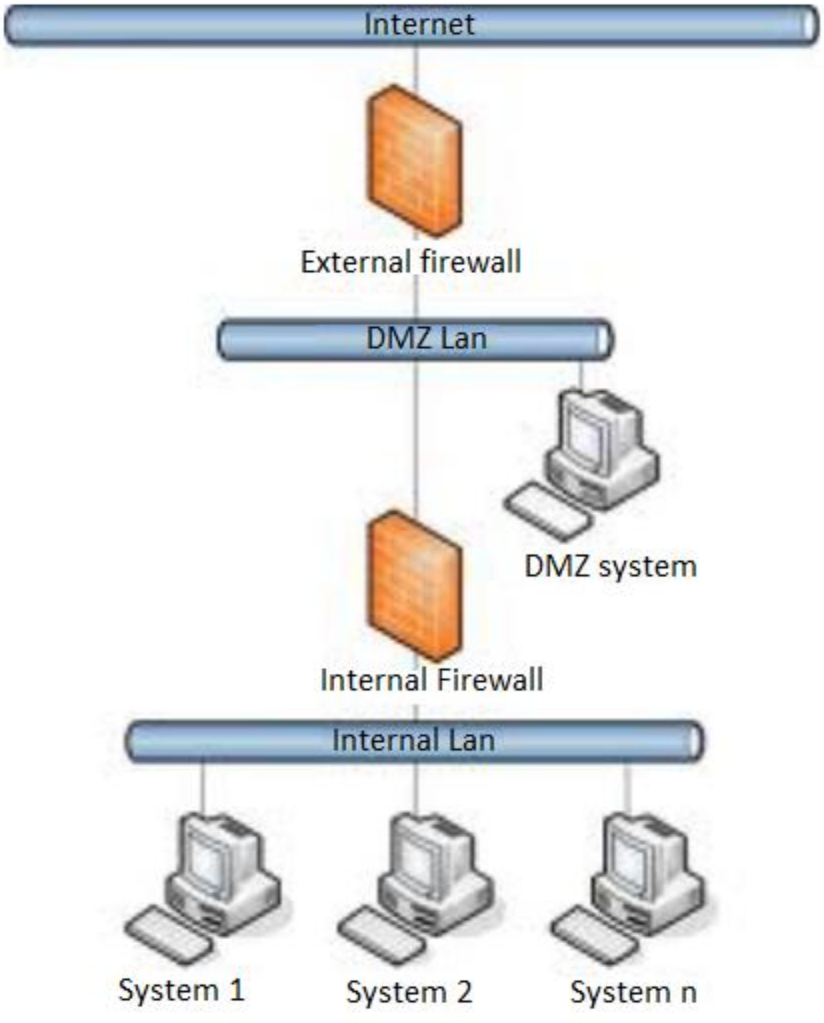


Figure 1: STRENGTHENING THE INTERNAL NETWORK SYSTEM WITH DMZ

Demilitarized Zone, also known as DMZ, is an area between the Local Area Network and the Internet. This is a place for servers and provides services for hosts on the LAN as well as other hosts from external LAN. The last step that data packets go through before transmitting out to the Internet. This is also the first place that packets arrive before being on the LAN.

First, before intranet protection. Find out what it includes. The intranet system will include servers that provide basic services (Directory service, DNS, DHCP, File / Print Sharing, Web, Mail, FTP). In particular, Web Server, FTP, and Mail will usually have to provide their services to users inside and outside the local network.

Thus, if hackers from outside networks control Public Servers such as Web, Mail, and FTP, they will probably rely on these Servers to penetrate deeper into the workstations inside.

I said that if we want to secure the intranet system and reduce damage to hosts on the LAN, we will use DMZ. The DMZ will have different network paths or subnets than the internal network so hosts from other LANs will not be able to access the LANs but they can still use the services provided by the DMZ.

In the middle of the DMZ and the outside network we can put a firewall. It will control the connection from external network to DMZ. On the local network and DMZ, we can set another firewall to control the traffic from the DMZ to the internal network.

In protecting the local network, there are many ways to design DMZ, I send you two commonly used methods which are to use single firewall and dual firewall. Using a single firewall, there will be a device connected to the network interface card (NIC) to connect from the DMZ, LAN, and the Internet respectively. As for the use of dual firewalls, there are two firewall devices. Each device will have 2 NICs. Firewall 1 will connect to the Internet and DMZ, the second firewall will connect DMZ and LAN. This method is quite expensive compared to the first method. However, compared to the method of using a single firewall, it is much safer.

DMZ was created to secure the LAN network with two roles that are to provide services for hosts of LANs and hosts from other LANs, as well as to protect hosts in LANs from being hackers attack other LAN hosts.

2. NAT

NAT is a technique that allows one or more internal IP addresses to be converted to one or more external IP addresses. What is the abbreviated meaning of NAT? NAT or Network Address Translation makes the local network address (Private) accessible to the public network (Internet). The place to perform NAT technology is the edge router, where these two types of networks are connected.

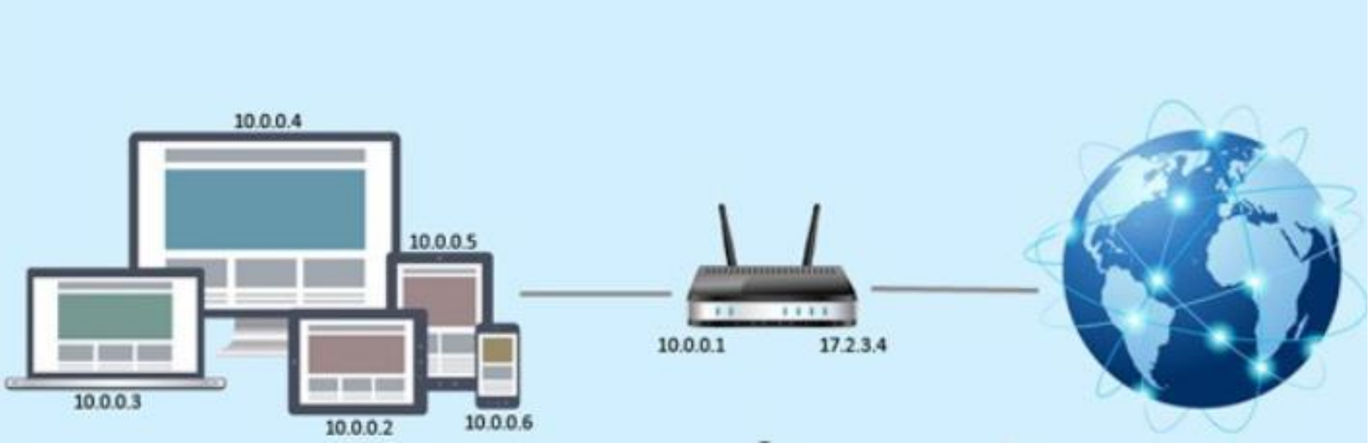


Figure 2: NAT-Network address translation

NAT mission:

NAT is responsible for transmitting packets from one network layer to another in the same network. NAT will make changes to the IP address inside the packet. Then move through routers and network devices.

When the packet is transmitted from the internet (public) back to the NAT, NAT will perform the task of changing the destination address to the IP address inside the local network and sending it.

NAT can act as a firewall. It helps users secure computer IP information. Specifically, if the computer is having trouble connecting to the internet, the public IP address (previously configured) will be displayed instead of the local network IP.

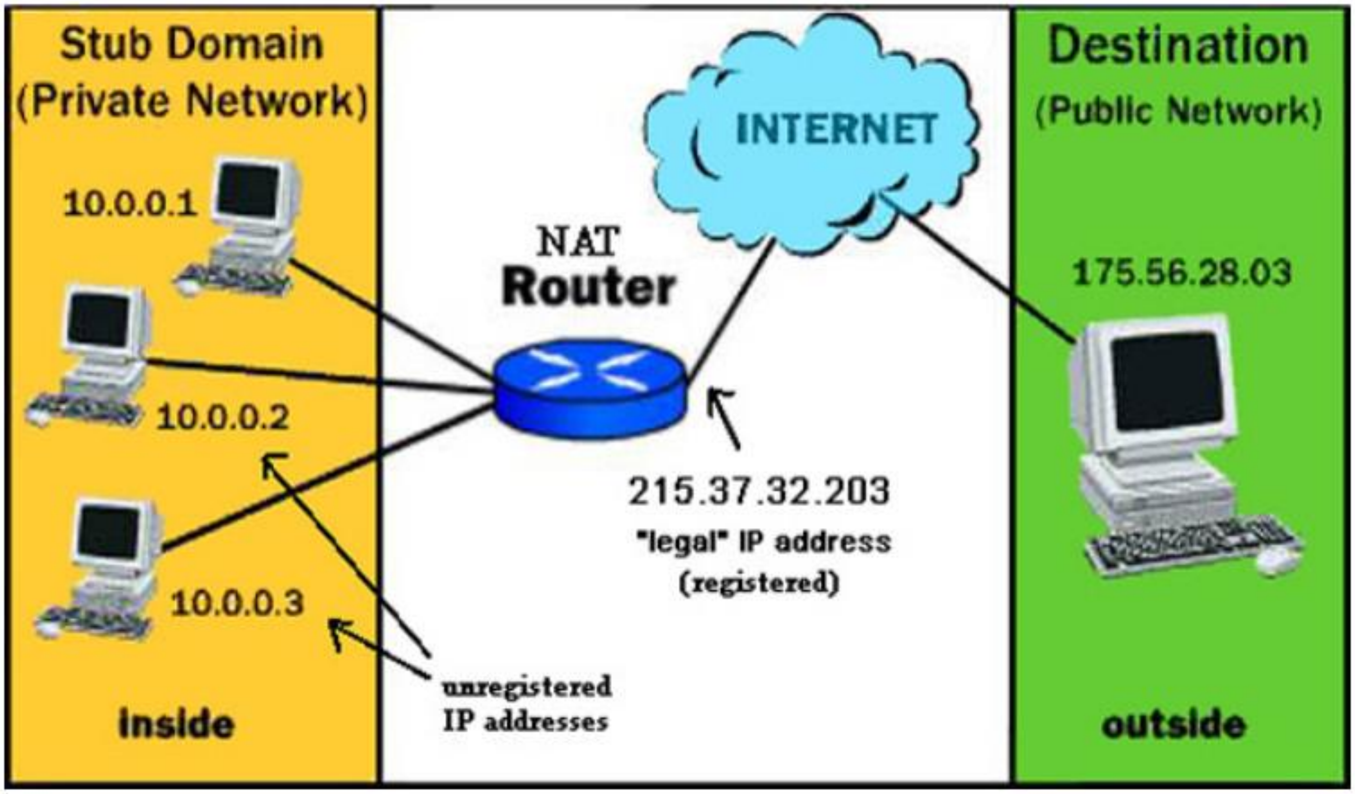


Figure 3: NAT mission

What are the advantages of NAT?

Saving IPv4 addresses: The number of users accessing the internet is increasing. This leads to the risk of IPv4 address shortages. NAT technology will help minimize the number of IP addresses to use.

Helps hide IP inside LAN.

NAT can share internet connection for many different computers and mobile devices in LAN with a single public IP address.

NAT helps network administrators filter incoming packets and approve public IP access to any port.

What are the disadvantages of NAT?

Besides the noticeable advantages, NAT also has some disadvantages and limitations:

When using NAT technology, the CPU will have to check and take time to change the IP address. This increases the latency during switching. Affect the internet connection speed.

NAT has the ability to hide IP addresses in LANs, so technicians will have difficulty in checking the origin of IP or tracing packets.

NAT hides the IP address, so some applications that need to use IP cannot work.

3. IP static

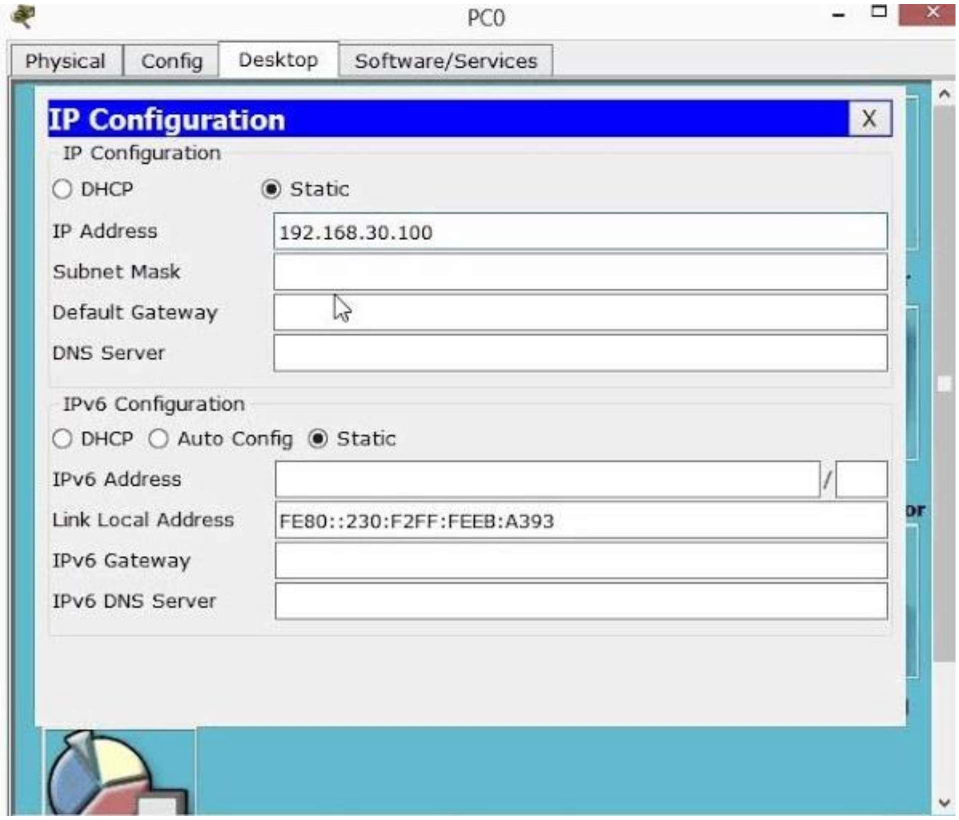
A static IP address is an IP address manually configured for a device compared to an address assigned via a DHCP server. It is called static because it does not change, as opposed to dynamically changing IP addresses.

Routers, phones, tablets, desktops, laptops, and any other device that can use an IP address can be configured with a static IP address. This can be done through devices that generate IP addresses (such as routers) or by manually entering the IP address into the device from the device itself.

Static IP addresses (sometimes called static IP addresses) are sometimes referred to as fixed IP addresses (dedicated IP addresses) or dedicated IP addresses (dedicated IP addresses).

Static IP addresses in network equipment and VPN tools, allowing everyone to access applications remotely. So, if you want to ensure that it is responding to queries, it needs to be associated with your static IP address in a format like 192.168.1.11. You can access your work computer when you are at home, set your computer up to use a static IP address that allows you to access your computer all the time, without the fear of changing your address and preventing you from accessing it.

Static IP addresses (also known as fixed IP addresses) are a constant number assigned to a computer or router. The internet service provider (ISP) assigns a public IP address to the router, while the router assigns an internal IP address to the connected devices.



IP Configuration

IP Configuration

○ DHCP ● Static

IP Address 192.168.30.100

Subnet Mask

Default Gateway

DNS Server

IPv6 Configuration

○ DHCP ○ Auto Config ● Static

IPv6 Address /

Link Local Address FE80::230:F2FF:FEEB:A393

IPv6 Gateway

IPv6 DNS Server

Figure 4: Set static IP for a PC using the router on Packet tracer

Why should you use a static IP address?

Static IP addresses are the same as email addresses or home addresses. These addresses never change - they are static, thus making it easy to contact or find someone.

Similarly, Static IP addresses become quite useful if you host a website at home, have a file server on the network using a networked printer, forward ports to specific devices, are running a print server or If you use remote access program. Because static IP addresses never change, other devices know exactly how to contact this static IP device.

For example, suppose you set a static IP address for one of the computers in your home network. When the computer has a specific address attached to it, you can set up a router that always forwards certain requests to that computer, such as FTP requests if the computer shares files via FTP.

Not using a static IP address will cause problems if you are hosting a website, because for every new IP address the computer receives, you must change the settings. set your router to forward requests to that new address. If you do not do this, no one will be able to access your website because the router does not know which device on the network is a web server.

Disadvantages of using static IP address

The major disadvantage that static IP addresses cause is that you have to configure the devices manually. As in the examples given above, home web server and remote access programs require you to set the IP address for the device and configure the right router to communicate with that IP address.

These operations certainly require more work than simply plugging into a router and allowing it to dynamically assign IP addresses via DHCP.

Moreover, if you assign your device with an IP address like 192.168.1.110, but then you move to another network that only provides 10.XXX addresses, you won't be able to connect to your static IP. , instead, you'll have to reconfigure the device to use DHCP (or choose a static IP that works with that new network).

Security may be one thing you will have to be wary of using static IP addresses. The never-ending IP address will allow hackers to own a time frame long enough for them to find vulnerabilities in the device's network. Using dynamic IP addresses will cause an attacker to change the way he communicates with the device.

References

[1] Unit 5 - Security 2019, *Chapter 1 - Introduction to information security*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[2] Unit 5 - Security 2019, *Chapter 2 - Malware Attacks*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[3] Unit 5 - Security 2019, *Chapter 3 - Social Engineering attacks*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[4] Unit 5 - Security 2019, *Chapter 4 - Application attacks*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[5] Unit 5 - Security 2019, *Chapter 5 - Networking Based Attacks*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[6] Unit 5 - Security 2019, *Chapter 6 - Host, Application, and Data Security*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[7] Unit 5 - Security 2019, *Chapter 7 - Basic Cryptography*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[8] Unit 5 - Security 2019, *Chapter 8 - Network Security Fundamentals*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[9] Unit 5 - Security 2019, *Chapter 9 - Access Control Fundamentals*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[10] Unit 5 - Security 2019, *Chapter 10 - Wireless Network Security*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[11] Unit 5 - Security 2019, *Chapter 11 - Mobile device security*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

[12] Unit 5 - Security 2019, *Chapter 12 - Business Continuity*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.
[13] Unit 5 - Security 2019, *Chapter 13 - Risk Mitigation*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.
[14] Unit 5 - Security 2019, *Chapter 14 - Vulnerability Assessment*, University of Greenwich (Alliance with Vietnam FPT Education), United Kingdom.

Techblog của VCCloud. 2020. Địa Chỉ IP Tĩnh Là Gì? Cách Đặt Địa Chỉ IP Tĩnh Trong Windows 7, 8, 10 - Techblog Của Vccloud. [online] Available at: <https://tech.bizflycloud.vn/dia-chi-ip-tinh-la-gi-cach-dat-dia-chi-ip-tinh-trong-windows-7-8-10-2018101815070735.htm> [Accessed 28 April 2020].

Trung tâm hỗ trợ kỹ thuật | MATBAO.NET. 2020. NAT Là Gì? Hướng Dẫn Cách Kết Nối Mạng NAT Dễ Dàng. [online] Available at: <https://wiki.matbao.net/kb/nat-la-gi-huong-dan-cach-ket-noi-mang-nat-de-dang/> [Accessed 28 April 2020].

Garland, B., 2020. 4 Common Mistakes In Firewall Configuration. [online] Valasecure.com. Available at: <https://www.valasecure.com/blog/4-common-mistakes-in-firewall-configuration> [Accessed 28 April 2020].

It.northwestern.edu. 2020. Firewall Policy: Information Technology - Northwestern University. [online] Available at: <https://www.it.northwestern.edu/policies/firewall.html> [Accessed 28 April 2020].

Sciencedirect.com. 2020. Security Procedure - An Overview | Sciencedirect Topics. [online] Available at: <https://www.sciencedirect.com/topics/computer-science/security-procedure> [Accessed 28 April 2020].

Technology Diver. 2020. Top 7 Rủi Ro Bảo Mật Mà Các Doanh Nghiệp Nhỏ Phải Đối Mặt - Technology Diver. [online] Available at: <https://cuongquach.com/top-7-rui-ro-bao-mat-ma-doanh-nghiep-nho-phai-doi-mat.html> [Accessed 28 April 2020].