


ASSIGNMENT FRONT SHEET

Qualification	BTEC Level 5 HND Diploma in Computing		
Unit number and title	Unit 5: Security		
Submission date	14 - 2 - 2021	Date Received 1st submission	15 - 2- 2021
Re-submission Date	Not yet	Date Received 2nd submission	3 - 3 - 2021
Student Name	Duong Duc Anh	Student ID	GCH18611
Class	GCH0901	Assessor name	Michael Omar
Student declaration I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.			
		Student's signature	

Grading grid

P1	P2	P3	P4	M1	M2	D1

<input type="checkbox"/> Summative Feedback:			<input type="checkbox"/> Resubmission Feedback:		
Internal Verifier's Comments:					
Signature & Date:					

I.	INTRODUCTION	6
II.	P1 IDENTIFY TYPES OF SECURITY THREAT TO ORGANISATIONS.	6
1.	THREATS	6
2.	IDENTIFY THREATS AGENTS TO ORGANIZATIONS.....	6
3.	LIST TYPE OF THREATS THAT ORGANIZATIONS WILL FACE.....	7
4.	WHAT ARE THE RECENT SECURITY BREACH? LIST AND GIVE EXAMPLES WITH DATES.....	10
5.	DISCUSS THE CONSEQUENCES OF THESE BREACH.....	11
6.	SUGGEST SOLUTIONS	11
III.	P2 DESCRIBE AT LEAST 3 ORGANIZATIONAL SECURITY PROCEDURES.	11
IV.	M1 PROPOSE A METHOD TO ASSESS AND TREAT IT SECURITY RISKS.....	12
1.	DISCUSS METHODS REQUIRED TO ASSESS IT SECURITY THREAT?	12
2.	WHAT IS THE CURRENT WEAKNESS OR THREAT OF THE ORGANIZATION?	13
3.	WHAT TOOLS WILL YOU PROPOSE TO TREAT THE IT SECURITY RISK?.....	13
V.	D1 INVESTIGATE HOW A ‘TRUSTED NETWORK’ MAY BE PART OF AN IT SECURITY SOLUTION.	15
VI.	P3 IDENTIFY THE POTENTIAL IMPACT TO IT SECURITY OF INCORRECT CONFIGURATION OF FIREWALL POLICIES AND IDS. 17	
1.	FIREWALL AND POLICIES	17
2.	HOW DOES A FIREWALL PROVIDE A SECURITY TO A NETWORK?	19
3.	EXAMPLE.....	20
4.	IDS.....	20
5.	WRITE DOWN THE POTENTIAL IMPACT (THREAT-RISK) OF FIREWALL AND IDS INCORRECT CONFIGURATION TO THE NETWORK	21
VII.	P4 SHOW, USING AN EXAMPLE FOR EACH, HOW IMPLEMENTING A DMZ, STATIC IP AND NAT IN A NETWORK CAN IMPROVE NETWORK SECURITY	22
1.	DMZ	22
2.	STATIC IP	23
3.	NAT	24
VIII.	M2 DISCUSS THREE BENEFITS TO IMPLEMENT NETWORK MONITORING SYSTEMS WITH SUPPORTING REASONS ...	25
1.	NETWORKING MONITORING DEVICES	25
2.	WHY DO YOU NEED TO MONITOR NETWORK?	28
3.	WHAT ARE THE BENEFITS OF MONITORING A NETWORK?	29
IX.	CONCLUSION	30
X.	EVALUATION	30
1.	EVALUATION.....	30
2.	SLIDE.....	31
XI.	REFERENCES	42

FIGURE 1 - COMPUTER VIRUTS	8
FIGURE 2 – TROJAN HORSE	9
FIGURE 3 - ADWARE	9
FIGURE 4 - INTRUDER	14
FIGURE 5 - MALWAREBYTES.....	15
FIGURE 6 - MMC	17
FIGURE 7 - MMC	18
FIGURE 8 – MMC	18
FIGURE 9 - HOW DOES THE FIREWALL WORK.....	20
FIGURE 10 – IDS	21
FIGURE 11 - DMZ	22
FIGURE 12 - STATIC IP CONFIGURATION	23
FIGURE 13 - NAT	24
FIGURE 14 – SOLARWIND.....	25
FIGURE 15 – SOLARWIND.....	26
FIGURE 16 – PRTG.....	27
FIGURE 17 - 24X7.....	28
FIGURE 18 - SLIDE 1.....	31
FIGURE 19 - SLIDE 2.....	31
FIGURE 20 -SLIDE 3	32
FIGURE 21 - SLIDE 4.....	32
FIGURE 22 - SLIDE 5.....	33
FIGURE 23 - SLIDE 6.....	33
FIGURE 24 - SLIDE 7	34
FIGURE 25 - SLIDE 8.....	34
FIGURE 26 - SLIDE 9.....	35
FIGURE 27 - SLIDE 10.....	35
FIGURE 29 - SLIDE 11.....	36
FIGURE 28 - SLIDE 12.....	36
FIGURE 31 - SLIDE 13.....	37
FIGURE 30 - SLIDE 14.....	37
FIGURE 32 - SLIDE 15.....	38
FIGURE 33 - SLIDE 16.....	38
FIGURE 34 - SLIDE 17.....	39
FIGURE 35 - SLIDE 18.....	39
FIGURE 36 - SLIDE 20.....	40
FIGURE 37 - SLIDE 19.....	40
FIGURE 38 - SLIDE 21.....	41

I. Introduction

I work as a trainee IT Security Specialist for a leading Security consultancy in Vietnam called FPT Information security FIS. FIS works with medium sized companies in Vietnam, advising and implementing technical solutions to potential IT security risks. Most customers have outsourced their security concerns due to lacking the technical expertise in house. As part of my role, my manager Jonson has asked me to create an engaging presentation to help train 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. As a guide I need to explain the underlying issues in security: threats, security methods, security tools, enterprise security vulnerabilities, security benefits ... I proceed to make reports to clarify the above.

II. P1 Identify types of security threat to organisations.

1. Threats

Threats are acts of hostility to harm or endanger a person or an organization, it can also be retaliation or an intentional act that has serious consequences.

Example:

- ✓ Arm conflict .
- ✓ Acts of God (Nature) e.g. Earthquake, flood.
- ✓ Arm robbery.

Each threat has a different treatment, but most threats are hostile and can cause great harm to an organization or individuals.

2. Identify threats agents to organizations

- ✓ Nation state.
- ✓ SLEPT (Social, Legal, Economical, Political, Technology).

- ✓ Internal and External.
- ✓ Employee.

Threats to an organization negatively affect the organization's productivity and give it a bad reputation.

According to (Akhil, 2019):

Most of business transactions operate over a network environment, so the terrorists want to attack and exploit that vulnerability. therefore, if we own a business then we should not ignore those threats. It is really important that we understand about the most common threat to information security in an organization so that we can take proper precautions and safeguard the data privacy and security within our organization.

If we do not take measures to faced against threats, these threats will seriously damage the organization or could go bankrupt. it is essential that we identify what those threats are? How do we deal with those threats?.

3. List type of threats that organizations will face

✚ One of the most common threats faced by organization is employees with a negative approach.

For example, a threat to the company might be a disloyal employee. Employees who come to the company just to make money are a major threat to the organization. If they don't contribute much to the organization, they're just a burden to the system.

✚ High attrition rate is another big threat to an organization.

For example, organizations will suffer great losses when talented employees quit their jobs and join competitors. That will lower corporate productivity and damage the ecosystem of the organization.

✚ Data and information loss.

For example, In large companies, data is crucial. The biggest flaw that drives the company out of business is data. If important data are acquired by the competing companies, Damage to the company is inevitable.

✚ Security issues pose a major threat to the organization.

Security problem is the biggest threat to organizations. Large organizations today can pay millions of dollars to hire good security. Make sure these security guards take safety measures against nature's forces such as tsunamis, earthquakes or hostile agents.

Some of security threats, According to (Touhit, 2019):

1. Computer viruses

Viruses can be infected from one computer to another. It could damage or steal important company data. subjects use this data to analyze and come up with solutions to threats to the organization.



Figure 1 - Computer viruts

Ways for viruses to attack:

- ❖ Clicking on an executable file.
- ❖ Installing free software and apps.
- ❖ Visiting an infected and unsecured website.
- ❖ Clicking on advertisement.

2. Trojan horse

This is a method in which hackers use malicious code to damage, modify, sabotage or otherwise do some harmful action on company data and network.



Figure 2 – Trojan horse

Ways for trojanhouse to attack:

- ❖ Using gmail to send malicious code
- ❖ Using communication methods on social networks such as messenger, zalo, ... to send malicious code

3. Adware

This is a way that hackers use advertisements on applications or websites to add malicious code or request to download malicious programs to a computer.



Figure 3 - Adware

Ways for trojanhouse to attack:

This is a method that companies can use to directly display advertising messages on users' computers. Its main purpose is to generate revenue for its developer (Adware) by serving different types advertisements to an internet user.

Lack of funds

Finance is a very important issue for the organization, it directly threatens the organization in all aspects. Therefore, it is necessary to carefully manage available capital to avoid future consequences.

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

Attack WHO by method Trojan horse

Recently, the outbreak of covid-19 has increased rapidly, which means that important information about it needs to be strictly protected. But as recently as April 2020, senior WHO officials were attacked by hackers to spread confidential data. Many email attacks WHO employees into accessing a malicious link in an email to download the malware onto their device.

According to Bloomberg, users of the internet forum 4chan published more than 2,000 passwords claimed to be associated with WHO email accounts. Details spread to Twitter and other social networking sites, where far-right political groups claim the WHO has been hacked to undermine the authenticity of public health guidelines.

The attack on FireEye revealed a series of US government agencies being compromised

When California-based cybersecurity firm FireEye found more than 300 of its proprietary cybersecurity products stolen, it discovered a massive hack that had been quietly going on for about nine months without any. was discovered.

Around 250 agencies directly under the US government, including the Treasury Department, the Department of Energy and even the Pentagon, were affected by the incident.

But the hack did not originate from FireEye but from SolarWinds, a company providing IT management software, was attacked. Some of its major customers were compromised, including Fortune 500

corporations such as Microsoft, Intel, Deloitte and Cisco. Hackers have launched a "supply chain" attack by hacking into a company's cybersecurity defenses leaving all of that company's customers affected by the domino effect.

According to Reuters reported in December 2020, hackers also tracked internal emails of the Treasury Department and the US Department of Commerce. US government officials and cybersecurity experts say Russia's Foreign Intelligence Service SVR is behind the attacks. Investigators are still stringing the details of the hack to determine the hackers' motives.

5. Discuss the consequences of these breach

Discuss 1: The form of attack by spreading malicious read paths over the network environment is now very popular. with just one click, all information on the user's computer can be lost. The bigger the company, the more important the data is. If it is lost to hackers like the above example, it may falsify the information given by WHO. The recent example in the US is that: some people misrepresent covid-19 that can spread via 5G: causing a series of smashing 5G broadcast stations in the US.

Discuss 2: The stolen proprietary cybersecurity products have serious consequences for the companies that use them. Companies that use this software as the US government leak confidential documents and criminals can use them to conduct terrorism.

6. Suggest solutions

Suggest 1: A security solution for organizations that depend on information data is to be secure in terms of security. We need to hire the people who can best protect the system even when we pay them high salaries.

Suggest 2: Before this incident, we should conduct a screening and remove the system that has been compromised by hackers.

III. P2 Describe at least 3 organizational security procedures.

1. All employees who want to enter the company must go through the checkpoint at the gate. Employees must present their ID and face card to prove they work in the company.

This first checkpoint is to identify and filter out people who have no position but still want to enter the company for information. Many companies use this procedure as it is effective for exclusion from the majority of outside parties. But this step is still just a simple administrative check (card check and eye check), the subjects can still fake identity cards.

2. Fingerprint check and face recognition.

This is an important security step in tech companies in Vietnam. we must use AI technology or machine learning to distinguish and make accurate decisions that the subjects is a person of our company. Anyone who fails this step will be arrested.

3. Changed accounts.

Company employees have their own accounts and passwords that are changed every day to use computers at work. Upon entering a department, employees are required to provide telephones or video recorders to the manager which will be returned at the end of the day. In addition, important departments will not have access to the internet.

IV. M1 Propose a method to assess and treat IT security risks

1. Discuss methods required to assess it security threat?

- Use people to monitor security

The most fundamental thing in assessing a security threat is using the people factor. Companies hire an organization or an individual to provide security for their company. These security guards have the ability to assess the situation and address possible threats to the company.

- Use tools to monitor security

Assistive tools for security threat assessment are the use of available data to analyze and filter out threats directly to the company.

- Uses AI technology to monitor security

AI technologies were developed to securely monitor everything in the company, analyze and evaluate without human impact.

2. What is the current weakness or threat of the organization?

Currently, there are 2 biggest weaknesses that directly affect the company: people and network security.

If the people in the company have bad intentions, it is very difficult to keep the company safe. The most important factor is the HR department must recruit people who are honest and loyal to the company. The company must also have incentives and a dynamic workplace to prevent employees from being bored.

The company's network security systems must be in good working order to avoid black hat hackers from breaking in and stealing information. Big companies in the world spend billions of dollars building safety systems for their companies.

3. What tools will you propose to treat the IT security risk?

➤ Intruder

The most popular cloud-based network vulnerability scanner that helps to find the cybersecurity weaknesses in the most exposed systems to avoid costly data breaches. It is the right solution for your cybersecurity issues. It helps to save time to a great extent. (SoftwareTestingHelp, 2021)



Figure 4 - Intruder

Features:

- ✓ Over 9,000 security vulnerabilities.
- ✓ Unlimited scans on demand.
- ✓ Unlimited user accounts.
- ✓ Checks for web application flaws such as SQL injection and Cross-site scripting.
- ✓ Emerging threat notifications.
- ✓ Smart Recon.
- ✓ Network view.
- ✓ PCI ASV scans available.

➤ Malwarebytes

Malwarebytes provides the cybersecurity solution for home and businesses. It can prevent threats in real-time and defend against harmful sites. (SoftwareTestingHelp, 2021)

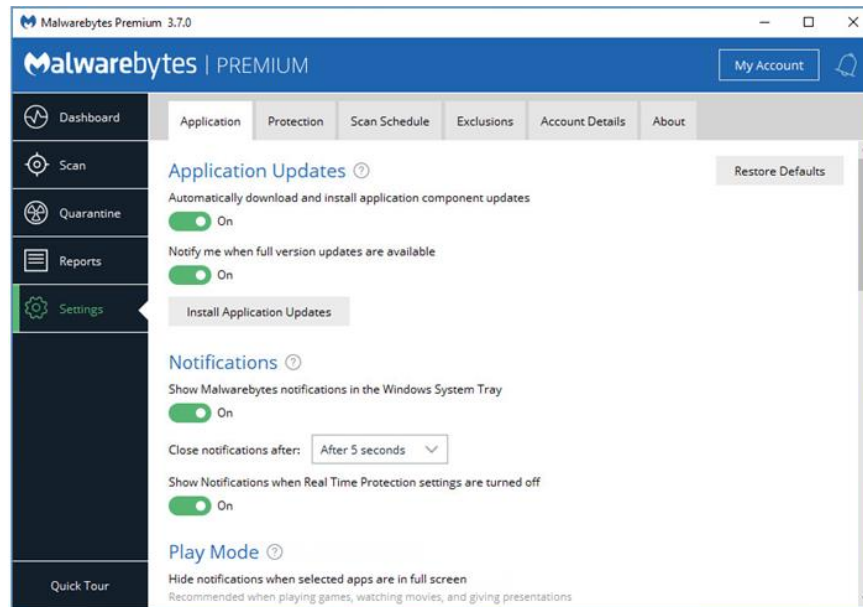


Figure 5 - Malwarebytes

Features:

- ✓ Malwarebytes makes the use of anomaly detection, behavior matching, and application hardening to protect from malware.
- ✓ It can clean up the infected devices.
- ✓ Malwarebytes will shut down the attack vectors from every angle regardless of the device you are using, Windows, Mac, or Android.
- ✓ It can provide multi-layered protection with endpoint detection and response for Windows.
- ✓ It can prevent threats in real-time.

V. D1 Investigate how a 'trusted network' may be part of an IT security solution.

A Trusted Network of a company is a network that the company uses to conduct its internal business. In many cases, the Trusted Network is by default defined in the organization as 'Secure'. The Trusted Network typically supports the backend systems, internal-only intranet web pages, data processing, messaging, and in some cases, internal instant messaging. In many companies the Trusted Network is allowed to interact

between systems directly, without encryption. The problem with the definition above is that many assumptions are being made at these companies. A Trusted Network is not always a secure network. In fact, in many cases the Trusted Network cannot be trusted. The reason is that an internal network comprises many different networks. These include new acquisitions, old acquisitions, international access points, and even several access points to the outside world. A common practice is to define the Trusted Network as the network that internal employees use when at the office or via a secure controlled dial-in mechanism. A single access point is established to the outside world via a mechanism called the Demilitarized Zone (DMZ) (Joseph Steinberg, Tim Speed, n.d.)

Example:

Duc Anh recently graduated from cybersecurity and was recruited to work at FPT. The manager asked him to do a project. he finds reliable network to have the following features:

- ✓ Authentication: the network should require users to login so that only authenticated users are allowed to use the network
- ✓ Encryption: the data should be encrypted so that secure data cannot be intercepted and transmitted to unauthorized users
- ✓ Firewall: the computers and servers on the trusted network should include hardware like a firewall, which is a software program or piece of hardware that helps screen for security
- ✓ Private Network: the computers and servers on the trusted network should be equipped with software like virtual private network (VPN), which allows for remote work with secure data transmission

In information technology security, the trusted network system is capable of protecting the network system in the company better. Access from outside is not possible, hackers only have the ability to enter when connected to the internal network in the company. That reduces the ability to attack from the outside.

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

1. Firewall and policies

A firewall is a piece of hardware or software that controls the flow of data packets, and it is critical on modern computer systems. It protects private networks and devices from malicious actions coming from public networks in the same way a physical firewall prevents fire from spreading from one area to another. A firewall acts as a defense mechanism which controls network traffic according to the implemented firewall rules. (GIS, 2019)

Computers behind a firewall cannot receive data until the data passes all filters. This enhances security by a large margin and reduces the risk of unauthorized access to private networks. A proper firewall configuration provides your system with a crucial layer of security and lowers the risk of successful hacking attacks.

MMC 3 way to access the firewall in window:

- Use the Server Manager to access the firewall MMC. Once the window opens, go to Tools on the top right side, and locate the Windows Firewall with Advanced Security option toward the bottom of the list.

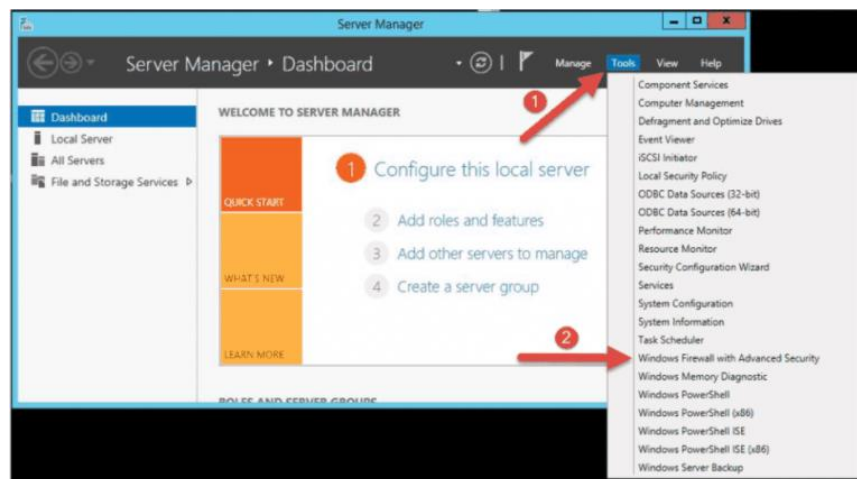


Figure 6 - MMC

- Open the Start menu (use the Windows key on keyboard) and type “firewall”. We should see the Windows Firewall with Advanced Security icon appear as one of the search results.



Figure 7 - MMC

Use the Run box to launch Windows Firewall with Advanced Security. Press Win + R keys, type in msc and hit Enter to load the console. You can also use Command Prompt or Windows PowerShell to run this command.

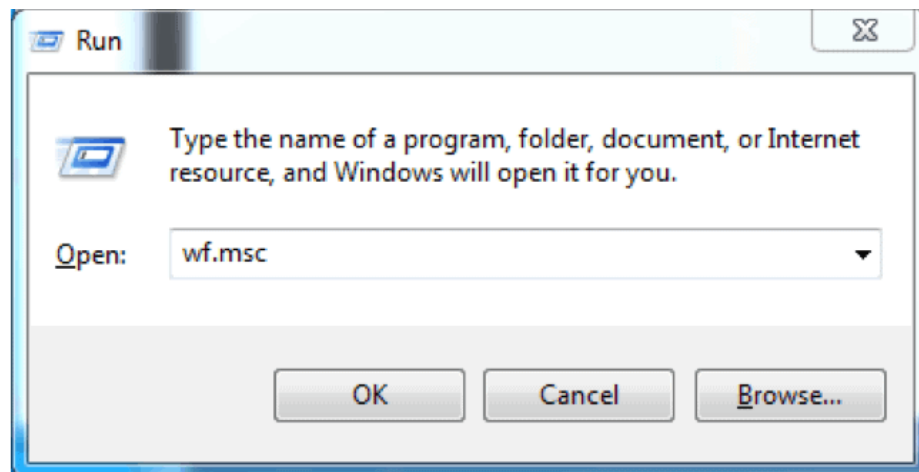


Figure 8 – MMC

Firewall policies:

- ✓ Firewall policies are stateful, meaning that they recognize flows in a network and keep track of the state of sessions.
- ✓ Firewall policies are bi-directional, meaning that they keep track of data connections traveling into or out of the network.
- ✓ Firewall policies are dynamic, meaning that address information in the policy rules can change as the policies are applied to users.

Firewall policies tend to forget that outbound traffic should not get a free pass. Rules in firewalls don't just have to block things, they can help you tag and categorize traffic that you allow through. This will allow to quickly determine which rules will work and which ones will not. (Branden R. Williams, Anton A. Chuvakin and Derek Milroy, n.d.)

Advantage and disadvantage of firewall:

Advantage	Disadvantage
Monitor Traffic	Cost
Protection against Trojans	User Restriction
Prevent Hackers	Performance
Access Control	Malware Attacks
Better Privacy	Complex Operations

(Room, 2020)

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

Firewalls work like a filter between computer/network and the Internet. we can program what we want to get out and what we want to get in. Everything else is not allowed. There are several different methods firewalls use to filter out information, and some are used in combination. These methods work at different layers of a network firewall, which determines how specific the filtering options can be. Firewalls can be used in a number of ways to add security to home or business.

3. Example

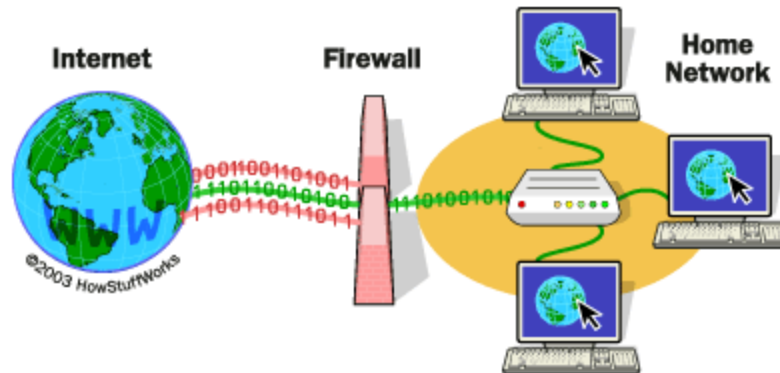


Figure 9 - How does the firewall work

4. IDS

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms (ashushrma378, 2020).

Type of IDS:

- ✓ Network Intrusion Detection System (NIDS).
- ✓ Host Intrusion Detection System (HIDS).
- ✓ Protocol-based Intrusion Detection System (PIDS).
- ✓ Application Protocol-based Intrusion Detection System (APIDS).
- ✓ Hybrid Intrusion Detection System.

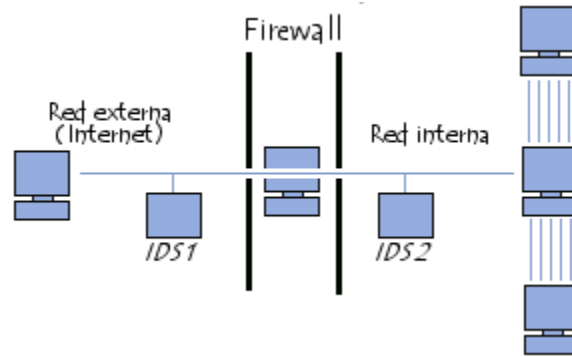


Figure 10 – IDS

5. Write down the potential impact (Threat-Risk) of FIREWALL and IDS incorrect configuration to the network

Even when a firewall is in place on network, and has all of the latest vulnerability patches, it can still cause problems if the firewall's configuration settings create conflicts. This can lead to a loss of performance on company's network in some cases, and a firewall outright failing to provide protection in others. (Dosal, 2018)

For example, dynamic routing is a setting that was long ago deemed a bad idea to enable because it results in a loss of control that reduces security. Yet, some companies leave it on, creating a vulnerability in their firewall protection.

Having a poorly-configured firewall is kind of like filling a castle's moat with sand and putting the key to the main gate in a hide-a-key right next to the entrance— just making things easier for attackers while wasting time, money, and effort on "security" measure.

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

1. DMZ

A demilitarized zone (DMZ) is a perimeter network that protects an organization's internal local-area network (LAN) from untrusted traffic.

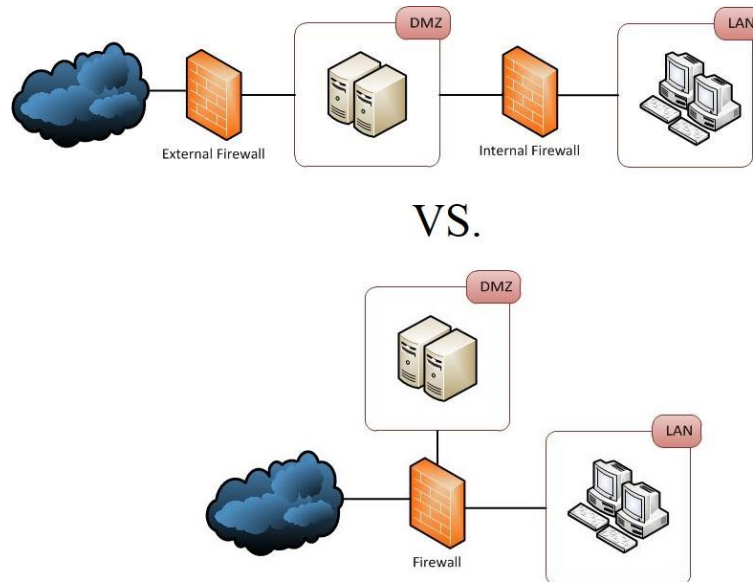


Figure 11 - DMZ

A DMZ network provides a buffer between the internet and an organization's private network. The DMZ is isolated by a security gateway, such as a firewall, that filters traffic between the DMZ and a LAN. The DMZ is protected by another security gateway that filters traffic coming in from external networks.

It is ideally located between two firewalls, and the DMZ firewall setup ensures incoming network packets are observed by a firewall—or other security tools—before they make it through to the servers hosted in the DMZ. This means that even if a sophisticated attacker is able to get past the first firewall, they must also access the hardened services in the DMZ before they can do damage to a business.

If an attacker is able to penetrate the external firewall and compromise a system in the DMZ, they then also have to get past an internal firewall before gaining access to sensitive corporate data. A highly skilled

bad actor may well be able to breach a secure DMZ, but the resources within it should sound alarms that provide plenty of warning that a breach is in progress.

Organizations that need to comply with regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), will sometimes install a proxy server in the DMZ. This enables them to simplify the monitoring and recording of user activity, centralize web content filtering, and ensure employees use the system to gain access to the internet.

2. Static IP

Static IP means an IP address set by the user, a fixed IP address reserved for one person, or a group of users whose internet-connected device is always assigned an IP address. . As usual, a static ip address is given to a dedicated server, so that many people can access it without interrupting the access process.

- ✓ Static ip address will help you connect to the internet quickly without having to re-issue a new IP address.
- ✓ Some services, and games, require a static ip address, meaning that the fixed ip address will not change, so that it is possible to restart the model.
- ✓ Static IP addresses also help to speed up web access and speed up torrent file downloads
- ✓ A static IP address is actually for stable communication with a computer on the internal network.
eg a company uses a network printer device with a static IP address.

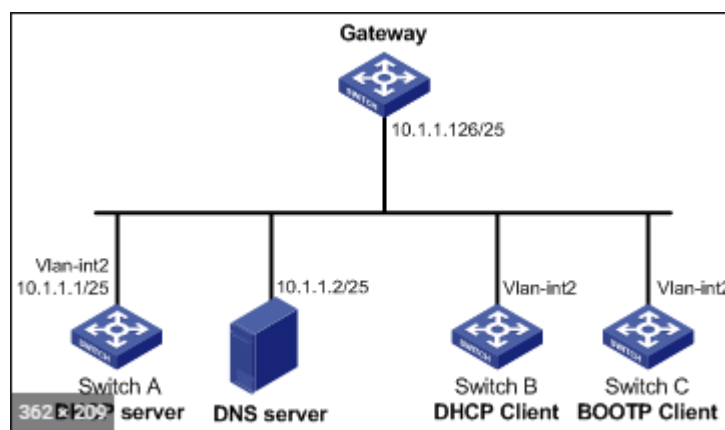


Figure 12 - Static IP configuration

Static IPs are more hackable: With a static IP address, hackers know exactly where your server is on the Internet. That makes it easier for them to attack it and become exposed to a higher security risk.

3. NAT

NAT is like a router, forwards packets between different network layers on a large network. NAT translates or changes one or both addresses within a packet as the packet passes through a router, or some other device. Typically NAT changes the address that is usually the private IP address of a network connection to a public IP (Public IP) address.

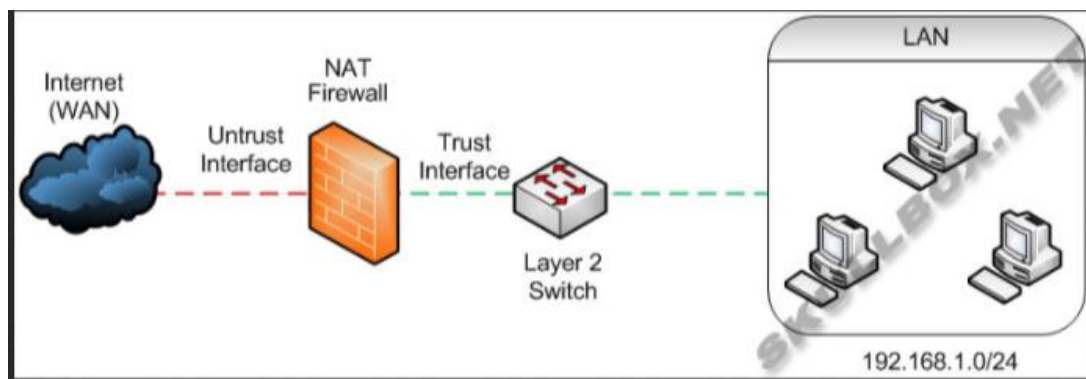


Figure 13 - NAT

NAT can also serve as a basic Firewall. NAT maintains a table of information about each packet passed. When a computer on the network connects to a website on the Internet the source IP address header is replaced by the pre-configured Public address on the NAT server, after the packet returns to NAT based on the record table it has. save the packets, change the destination IP address to the PC address on the network and forward it. Through this mechanism, the network administrator is able to filter packets sent to or from an IP address and allow or prevent access to a specific port.

NAT type:

- ✓ Static NAT
- ✓ Dynamic NAT
- ✓ Overloading NAT
- ✓ Overlapping NAT

VIII. M2 Discuss three benefits to implement network monitoring systems with supporting reasons

1. Networking monitoring devices

SolarWinds Network Performance Monitor

SolarWinds Network Performance Monitor is easy to setup and can be ready in no time. The tool automatically discovers network devices and deploys within an hour. Its simple approach to oversee an entire network makes it one of the easiest to use and most intuitive user interfaces.

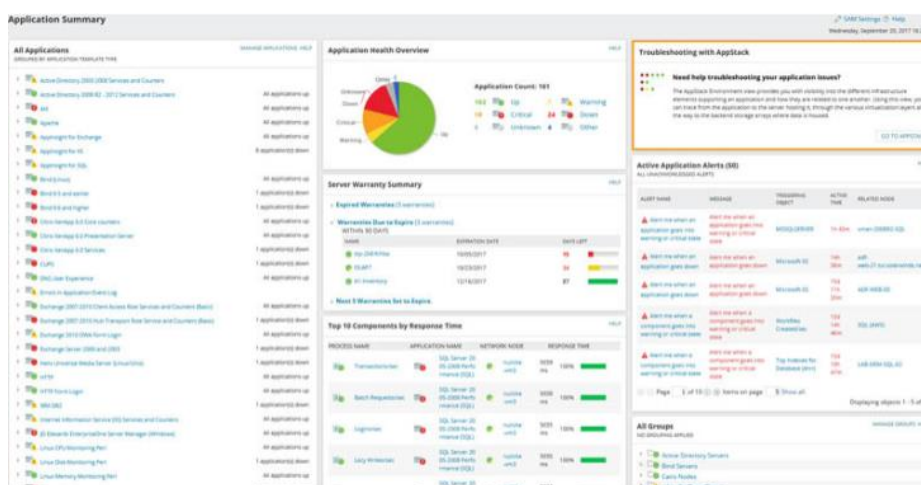


Figure 14 – Solarwind

SolarWinds NPM has an Extensive Feature list that make it One of the Best Choices for Network Monitoring, including:

- ✓ Automatically Network Discovery and Scanning for Wired and Wifi Computers and Devices
- ✓ Support for Wide Array of OEM Vendors
- ✓ Forecast and Capacity Planning
- ✓ Quickly Pinpoint Issues with Network Performance with NetPath™ Critical Path visualization feature
- ✓ Easy to Use Performance Dashboard to Analyze Critical Data points and paths across your network
- ✓ Robust Alerting System with options for Simple/Complex Triggers

- ✓ Monitor CISCO ASA networks with their New Network Insight™ for CISCO ASA.
- ✓ Monitor ACL's, VPN, Interface and Monitor on your Cisco ASA
- ✓ Monitor Firewall rules through Firewall Rules Browser
- ✓ Hop by Hop Analysis of Critical Network Paths and Components
- ✓ Automatically Discover Networks and Map them along with Topology Views
- ✓ Manage, Monitor and Analyze Wifi Networks within the Dashboard
- ✓ Create HeatMaps of Wifi Networks to pin-point Wifi Dead Spots
- ✓ Monitor Hardware Health of all Servers, Firewalls, Routers, Switches, Desktops, laptops and more.
- ✓ Real-Time Network and Netflow Monitoring for Critical Network Components and Devices

(Wilson, 2021)



Figure 15 – Solarwind



PRTG Network Monitor from Paessler

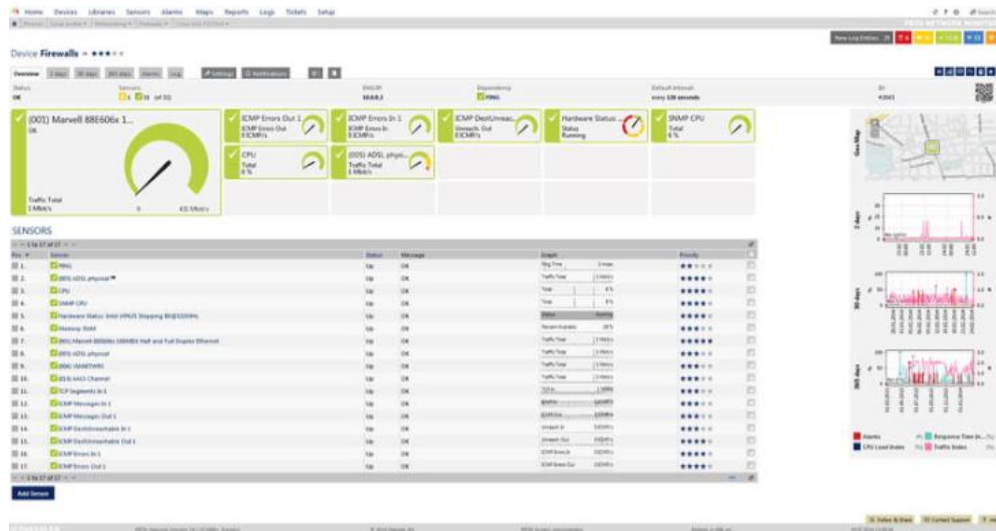


Figure 16 – PRTG

PRTG Network Monitor software is commonly known for its advanced infrastructure management capabilities. All devices, systems, traffic, and applications in your network can be easily displayed in a hierarchical view that summarizes performance and alerts. PRTG monitors IT infrastructure using technology such as SNMP, WMI, SSH, Flows/Packet Sniffing, HTTP requests, REST APIs, Pings, SQL. (Wilson, 2021)

 Site24x7 Network Monitoring

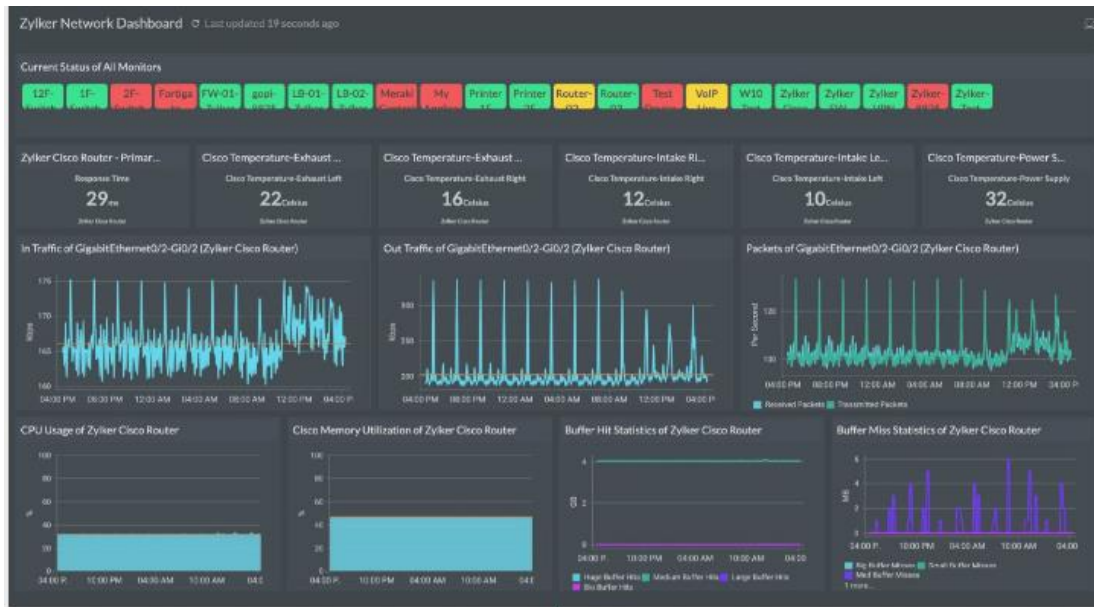


Figure 17 - 24X7

Site24x7 is a monitoring service that covers networks, servers, and applications. The network monitoring service in this package starts off by exploring the network for connected devices. It logs its findings in a network inventory and draws up a network topology map.

The Network Monitor uses procedures from the Simple Network Management Protocol (SNMP) to poll devices every minute for status reports. Any changes in the network infrastructure that are revealed by these responses update the inventory and topology map.

The SNMP system empowers device agents to send out a warning without waiting for a request if it detects a problem with the device that it is monitoring. Site24x7 Infrastructure catches these messages, which are called Traps, and generates an alert. This alert can be forwarded to technicians by SMS, email, voice call, or instant messaging post. (Wilson, 2021)

2. Why do you need to monitor network?

The need for ever-accessible software and resources continues to rise, making network availability monitoring a core necessity for modern data centers. Network monitoring systems provide the first line of protection as apps go down or when efficiency continues to deteriorate.

Network availability management systems allow networking teams to determine the health and availability of their network equipment, as well as the overall network. Network monitoring systems can track the bandwidth use, uptime, availability and response times of networked equipment, and offer comprehensive reporting and metrics that can help network administrators with troubleshooting.

However, the demand for network management solutions can be daunting, since there is a wide range of applications and embedded hardware equipment providing similar features but with different degrees of integration and performance. Some network availability monitoring tools have fully integrated architectures that require only a single piece of software, whereas other tools may include several individual components, such as a polling engine, a database, an analytics server or user console that must be installed and managed separately. Network monitoring systems can protect against malicious behavior targeted at the system.

3. What are the benefits of monitoring a network?

a. Stay ahead of outages

Causes of IT problems: human errors, configuration errors, or environmental factors. Performing network monitoring is the most basic step in preventing this problem from happening in the first place.

b. Fix issues faster

Under difficult circumstances, it will be very costly and time consuming. Network monitoring will speed up the process and reduce costs incurred.

c. Identify security threats

When the company doesn't have the budget for large security systems, but still wants a first-class approach to data protection, network surveillance can help protect critical data. When the company doesn't have the budget for large security systems, but still wants a first-class approach to data protection, network surveillance can help protect critical data.

IX. Conclusion

Today, technology is developing more and more and security is also invested more and more. Therefore, we need to keep up with that development and learn and research to become a good security engineer.

X. Evaluation

1. Evaluation

The report is completed and divided into categories that are reasonable and easy to find. All items have been specifically clarified about threats, corporate security procedures, method to assess and treat IT security risks, trusted network in security, DMZ, static IP, NAT, firewall and policies. The report is constantly being edited and completed in a very long time. The references are also carefully selected from 2018 to 2021. The information in the reference is also read first and a small part is extracted to support the report. In addition to supporting research I also read non-book references.

The examples I took directly around the world in 2020 from hackers attacked WHO and the US government.

- All of these sources have been verified as correct.

I think I will score D in this report because I have fulfilled criteria P, M, D.

2. Slide



Figure 18 - Slide 1



Figure 19 - Slide 2

Content

1. Threats
2. Organization procedures
3. Method to management risks
4. Benefit of networking monitoring
5. Firewall and IDS
6. Trusted network

3

Activate Windows

Figure 20 -Slide 3

Security threats

As a company specializing in security, security threats to the company are inevitable. we need to identify direct and indirect threats to our company. Some of threats:

- Hacker
- People working in our company
- Act of nature
- Profit

Each threat has a different treatment, but most threats are hostile and can cause great harm to an organization or individuals.

ADD A FOOTER

4

Activate Windows

Figure 21 - Slide 4

Example

Attack WHO by Trojan horse (4/2020)

April 2020, senior WHO officials were attacked by hackers to spread confidential data. Many email attacks WHO employees into accessing a malicious link in an email to download the malware onto their device.

- The form of attack by spreading malicious read paths over the network environment is now very popular. with just one click, all information on the user's computer can be lost. The bigger the company, the more important the data is. If it is lost to hackers like the above example, it may falsify the information given by WHO.
- The recent example in the US is that: some people misrepresent covid-19 that can spread via 5G: causing a series of smashing 5G broadcast stations in the US.

How to defence:

- ❖ Re-training human resources
- ❖ Control online activities in the company

5

Activate Windows

Figure 22 - Slide 5

Organizational procedures

Here are some of the procedures some companies use to minimize security breaches

1. All employees who want to enter the company must go through the checkpoint at the gate. Employees must present their ID and face card to prove they work in the company.

This first checkpoint is to identify and filter out people who have no position but still want to enter the company for information. Many companies use this procedure as it is effective for exclusion from the majority of outside parties. But this step is still just a simple administrative check (card check and eye check), the subjects can still fake identity cards.



6

Activate Windows

Figure 23 - Slide 6

Organizational procedures

Here are some of the procedures some companies use to minimize security breaches

1. Fingerprint check and face recognition.

This is an important security step in tech companies in Vietnam. we must use AI technology or machine learning to distinguish and make accurate decisions that the subjects is a person of our company. Anyone who fails this step will be arrested.



7

Activate Windows

Figure 24 - Slide 7

Organizational procedures

Here are some of the procedures companies use to minimize security breaches

3. Changed accounts.

Company employees have their own accounts and passwords that are changed every day to use computers at work. Upon entering a department, employees are required to provide telephones or video recorders to the manager which will be returned at the end of the day. In addition, important departments will not have access to the internet.



ComputerHope.com

8

Activate Windows

Figure 25 - Slide 8

Organizational procedures

Many companies are now using AI technology to replace people to protect companies from risks. This technology is designed to detect threats and bugs that arise in corporate security. In addition, this technology can also automatically analyze and evaluate problems without the need for human interaction.



9

Activate Windows

Figure 26 - Slide 9

Benefit of network monitoring system

1. Stay ahead of outages: Causes of IT problems: human errors, configuration errors, or environmental factors. Performing network monitoring is the most basic step in preventing this problem from happening in the first place.
2. Fix issues faster: Under difficult circumstances, it will be very costly and time consuming. Network monitoring will speed up the process and reduce costs incurred.
3. Identify security threats: When the company doesn't have the budget for large security systems, but still wants a first-class approach to data protection, network surveillance can help protect critical data. When the company doesn't have the budget for large security systems, but still wants a first-class approach to data protection, network surveillance can help protect critical data.

10

Activate Windows

Figure 27 - Slide 10

Network security

Network security is any activity designed to protect the usability and integrity of network and data

- ❖ It includes both hardware and software technologies
- ❖ It targets a variety of threats
- ❖ It stops them from entering or spreading on network
- ❖ Effective network security manages access to the network



11

Activate Windows

Figure 29 - Slide 11

Firewall

A firewall is a piece of hardware or software that controls the flow of data packets, and it is critical on modern computer systems. It protects private networks and devices from malicious actions coming from public networks in the same way a physical firewall prevents fire from spreading from one area to another. A firewall acts as a defense mechanism which controls network traffic according to the implemented firewall rules.

Computers behind a firewall cannot receive data until the data passes all filters. This enhances security by a large margin and reduces the risk of unauthorized access to private networks. A proper firewall configuration provides your system with a crucial layer of security and lowers the risk of successful hacking attacks.

12

Activate Windows

Figure 28 - Slide 12

Firewall

Advantage	Disadvantage
Monitor Traffic	Cost
Protection against Trojans	User Restriction
Prevent Hackers	Performance
Access Control	Malware Attacks
Better Privacy	Complex Operations

13

Activate Windows

Figure 31 - Slide 13

IDS

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.

It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms

14

Activate Windows

Figure 30 - Slide 14

Firewall and IDS incorrect configuring

Even when a firewall is in place on network, and has all of the latest vulnerability patches, it can still cause problems if the firewall's configuration settings create conflicts. This can lead to a loss of performance on company's network in some cases, and a firewall outright failing to provide protection in others. For example, dynamic routing is a setting that was long ago deemed a bad idea to enable because it results in a loss of control that reduces security. Yet, some companies leave it on, creating a vulnerability in their firewall protection.

Having a poorly-configured firewall is kind of like filling a castle's moat with sand and putting the key to the main gate in a hide-a-key right next to the entrance— just making things easier for attackers while wasting time, money, and effort on “security” measure.

15

Activate Windows

Figure 32 - Slide 15

Method to improve network security

1. Using Networking monitoring devices

The need for ever-accessible software and resources continues to rise, making network availability monitoring a core necessity for modern data centers. Network monitoring systems provide the first line of protection as apps go down or when efficiency continues to deteriorate.

Network availability management systems allow networking teams to determine the health and availability of their network equipment, as well as the overall network. Network monitoring systems can track the bandwidth use, uptime, availability and response times of networked equipment, and offer comprehensive reporting and metrics that can help network administrators with troubleshooting.

However, the demand for network management solutions can be daunting, since there is a wide range of applications and embedded hardware equipment providing similar features but with different degrees of integration and performance. Some network availability monitoring tools have fully integrated architectures that require only a single piece of software, whereas other tools may include several individual components, such as a polling engine, a database, an analytics server or user console that must be installed and managed separately. Network monitoring systems can protect against malicious behavior targeted at the system.

16

Activate Windows

Figure 33 - Slide 16

Method to improve network security

DMZ

A demilitarized zone (DMZ) is a perimeter network that protects an organization's internal local-area network (LAN) from untrusted traffic.

A DMZ network provides a buffer between the internet and an organization's private network. The DMZ is isolated by a security gateway, such as a firewall, that filters traffic between the DMZ and a LAN. The DMZ is protected by another security gateway that filters traffic coming in from external networks.

It is ideally located between two firewalls, and the DMZ firewall setup ensures incoming network packets are observed by a firewall—or other security tools—before they make it through to the servers hosted in the DMZ. This means that even if a sophisticated attacker is able to get past the first firewall, they must also access the hardened services in the DMZ before they can do damage to a business.

17

Activate Windows

Figure 34 - Slide 17

Method to improve network security

NAT

NAT is like a router, forwards packets between different network layers on a large network. NAT translates or changes one or both addresses within a packet as the packet passes through a router, or some other device. Typically NAT changes the address that is usually the private IP address of a network connection to a public IP (Public IP) address.

NAT can also serve as a basic Firewall. NAT maintains a table of information about each packet passed. When a computer on the network connects to a website on the Internet the source IP address header is replaced by the pre-configured Public address on the NAT server, after the packet returns to NAT based on the record table it has. save the packets, change the destination IP address to the PC address on the network and forward it. Through this mechanism, the network administrator is able to filter packets sent to or from an IP address and allow or prevent access to a specific port.

NAT type:

- Static NAT
- Dynamic NAT
- Overloading NAT
- Overlapping NAT

18

Activate Windows

Figure 35 - Slide 18

Trusted network

A Trusted Network of a company is a network that the company uses to conduct its internal business. In many cases, the Trusted Network is by default defined in the organization as 'Secure'. The Trusted Network typically supports the backend systems, internal-only intranet web pages, data processing, messaging, and in some cases, internal instant messaging. In many companies the Trusted Network is allowed to interact between systems directly, without encryption. The problem with the definition above is that many assumptions are being made at these companies. A Trusted Network is not always a secure network. In fact, in many cases the Trusted Network cannot be trusted. The reason is that an internal network comprises many different networks. These include new acquisitions, old acquisitions, international access points, and even several access points to the outside world. A common practice is to define the Trusted Network as the network that internal employees use when at the office or via a secure controlled dial-in mechanism. A single access point is established to the outside world via a mechanism called the Demilitarized Zone (DMZ)

19

Activate Windows

Figure 37 - Slide 19

Trusted network

Example:

Duc Anh recently graduated from cybersecurity and was recruited to work at FIS. The manager asked him to do a project. he plan that network to have the following features:

- ❖ Authentication: the network should require users to login so that only authenticated users are allowed to use the network
- ❖ Encryption: the data should be encrypted so that secure data cannot be intercepted and transmitted to unauthorized users
- ❖ Firewall: the computers and servers on the trusted network should include hardware like a firewall, which is a software program or piece of hardware that helps screen for security
- ❖ Private Network: the computers and servers on the trusted network should be equipped with software like virtual private network (VPN), which allows for remote work with secure data transmission

In FIS security, the trusted network system is capable of protecting the network system in the company better. Access from outside is not possible, hackers only have the ability to enter when connected to the internal network in the company. That reduces the ability to attack from the outside.

20

Figure 36 - Slide 20

THANK YOU!

Duong Duc Anh

Phone:

0913924185

Email:

anhddgch18611@fpt.edu.vn



Activate Windows

Figure 38 - Slide 21

XI. References

Akhil, 2019. *What is the Most Common Threat to Information Security in an Organization?*. [Online]
Available at: <https://www.techinpost.com/what-is-the-most-common-threat-to-information-security-in-an-organization/>
[Accessed 2021].

ashushrma378, 2020. *Intrusion Detection System (IDS)*, s.l.: s.n.

Branden R. Williams, Anton A. Chuvakin and Derek Milroy, n.d. *PCI Compliance, Understand and Implement Effective PCI Data Security Standard Compliance*. s.l.:s.n.

Dosal, E., 2018. *5 Firewall Threats and Vulnerabilities to Look Out For*, s.l.: s.n.

GIS, 2019. *How To Configure Windows Server 2012 Firewall*. [Online]
Available at: [https://phoenixnap.com/kb/how-to-configure-windows-server-2012-firewall#:~:text=Open%20the%20Start%20menu%20\(use%20the%20Windows%20key,msc%20and%20hit%20Enter%20to%20load%20the%20console.](https://phoenixnap.com/kb/how-to-configure-windows-server-2012-firewall#:~:text=Open%20the%20Start%20menu%20(use%20the%20Windows%20key,msc%20and%20hit%20Enter%20to%20load%20the%20console.)

Joseph Steinberg, Tim Speed, n.d. *SSL VPN : Understanding, evaluating and planning secure, web-based remote access*. A comprehensive overview of SSL VPN technologies and design strategies ed. s.l.:s.n.

MSG, n.d. *Common Threats to an Organization*, <https://www.managementstudyguide.com/common-threats-to-organization.htm>: s.n.

Pratt, M. K., 2018. *What is an intrusion detection system? How an IDS spots threats*, s.l.: s.n.

Room, M., 2020. *5 Advantages and Disadvantages of Firewall | Drawbacks & Benefits of Firewall*, s.l.: s.n.

SoftwareTestingHelp, 2021. <https://www.softwaretestinghelp.com/cybersecurity-software-tools/>. [Online].

Touhit, 2019. *COMMON TYPES OF SECURITY THREATS TO ORGANIZATIONS*. [Online]
Available at: <https://cyberthreatportal.com/types-of-security-threats-to-organizations/>
[Accessed 28 July 2021].

Wilson, M., 2021. *12 Best Network Monitoring Tools & Software of 2021*. [Online]
Available at: <https://www.pcworld.com/best-network-monitoring-tools-and-software>