**ASSIGNMENT FRONT SHEET**

|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | **Unit 5: Security** | | |
| **Submission date** |  | **Date Received 1st submission** | 12/9/2020 |
| **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:** | | |

|  |
| --- |
| **Unit Learning Outcomes** |
| **LO1** Assess risks to IT security. **LO2** Describe IT security solutions. |
| **Assignment Brief and Guidance** |
| You 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 your role, your manager Jonson has asked you 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.  In addition to your presentation you should also provide a detailed report containing a technical review of the topics covered in the presentation.  Your presentation should:   1. **Identify** the security threats FIS secure may face if they have a security breach. Give an example of a recently publicized security breach and discuss its consequences 2. **Describe** a variety of organizational procedures an organization can set up to reduce the effects to the business of a security breach. 3. **Propose** a method that FIS can use to prioritize the management of different types of risk 4. **Discuss** three benefits to FIS of implementing network monitoring system giving suitable reasons. 5. Investigate network security, **identifying** issues with firewalls and **IDS** incorrect configuration and **show** through examples how different techniques can be implemented to improve network security. 6. **Investigate** a ‘trusted network’ and through an analysis of positive and negative issues determine how it can be part of a security system used by FIS.   Your detailed report should include a summary of your presentation as well as additional, evaluated or critically reviewed technical notes on all of the expected topics. |

|  |  |  |
| --- | --- | --- |
| Learning Outcomes and Assessment Criteria | | |
| Pass | Merit | Distinction |
| **LO1** Assess risks to IT security | | **LO1 & 2 D1** Investigate how a ‘trusted network’ may be part of an IT security solution. |
| **P1** Identify types of security threat to organisations.  Give an example of a recently publicized security breach and discuss its consequences.  **P2** Describe at least 3 organisational security procedures. | **M1** Propose a method to assess and treat IT security risks. |
| **LO2** Describe IT security solutions | |
| **P3** Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS.  **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. |

**TABLE OF CONTENTS**

[**P1 Identify types of security threat to organizations. Give an example of a recently publicized security breach and discuss its consequences. 6**](#_Toc29421)

[What is a security threat? 6](#_Toc27478)

[What are Physical Threats? 6](#_Toc24847)

[What are Non-physical threats? 6](#_Toc3004)

[Viruses 7](#_Toc11803)

[Worms 7](#_Toc19964)

[Trojan Horses 7](#_Toc20172)

[Rootkit 7](#_Toc2735)

[Spyware 8](#_Toc15612)

[Adware 8](#_Toc20838)

[Ransomware 8](#_Toc15018)

[Careless employees 8](#_Toc21000)

[Natural disaster 9](#_Toc32350)

[**P2 Describe at least 3 organizational security procedures. 10**](#_Toc7736)

[**P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS. 15**](#_Toc7045)

[Firewall: 15](#_Toc27324)

[IDS: 17](#_Toc20145)

[Incorrect configuration of firewall policies and IDS: 18](#_Toc31030)

[**P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security. 19**](#_Toc21736)

[DMZ: 19](#_Toc21694)

[Static IP address: 20](#_Toc28265)

[NAT: 21](#_Toc8210)

[**References 23**](#_Toc28811)

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

**[What is a security threat?](https://debricked.com/blog/2019/05/29/what-is-a-security-threat/" \l ":~:text=Defining a security threat&text=A potential for violation of,event that could cause harm.&text=The threat is not a,that can violate the security.)**

It is known as a risk that can potentially harm computer systems and organization. The cause could be physical such as someone stealing a computer that contains important data. The cause could also be non-physical such as a virus attack and worms[1]

**What are Physical Threats?**

It is a potential cause of an incident that may result in loss or physical damage to the computer systems. There’re three main categories:

* Internal: The threats include fire, unstable power supply, humidity in the rooms housing the hardware,...
* External: These threats include Lightning, floods, earthquakes,…
* Human: These threats include theft, vandalism of the infrastructure and/or hardware, disruption, accidental or intentional errors.

**What are Non-physical threats?**

A non-physical threat also known as logical threat, is a potential cause of an incident that may result in:

* Loss or corruption of system data
* Disrupt business operations that rely on computer systems
* Loss of sensitive information
* Illegal monitoring of activities on computer systems
* Cyber Security Breaches

An organization’s network is the lifeline that employees rely on to do their jobs and subsequently make money for the organization. Therefore it’s important to recognize that your IT infrastructure is an asset that requires top security. Thus we need to know what we’re secure against[1] Here’s some examples:

**Viruses** - It is a software program that can spread from one computer to another computer or one network to another network without the user’s knowledge and performs malicious attacks which execute when a document or program is opened. It has capability to corrupt or damage organization’s sensitive data, destroy files,  and format [hard drives](https://en.wikipedia.org/wiki/Hard_disk_drive)[1]

There are more different ways that a virus can be spread or attack, like:

Installing free software and apps, visiting an infected and unsecured website, clicking on advertisement, using of infected removable storage devices, such [USB drives](https://en.wikipedia.org/wiki/USB_flash_drive), opening spam email or clicking on URL link or downloading free games, media players and other software.

**Worms** - Worms is a type of [malicious software](https://enterprise.comodo.com/blog/what-is-malicious-software/) or program that spreads within its connected network and copies itself from one computer to another computer of an organization. Worms are usually distributed via e-mail attachments as separate executable programs. Usually, reading the e-mail message activate the worm. And if the worm does not start automatically, attackers can trick the user to start the program and launch the worm[1]

It can then spread without any human assistance and exploit the security holes of the software and trying to access for stealing sensitive information, corrupting files and installing a back door for remote access to the system.

**Trojan Horses** - Trojan Horse is a [malicious code](https://cyberthreatportal.com/malware-definition-and-example/) or program that developed by hackers to disguise as legitimate software to gain access to organization’s systems. It has designed to delete, modify, damage, block, or some other harmful action on your [data](https://en.wikipedia.org/wiki/Data) or [network](https://en.wikipedia.org/wiki/Computer_network)[1]

How Trojan Horse normally attack is the victim will receive an email with an attachment file which is looking as an original official email. The attachment file can contain malicious code that is executed as soon as when the victim clicks on the attachment file. In that case, the victim does not suspect or understand that the attachment is actually a Trojan horse.

**Rootkit** - Rootkit is a malicious program that installs and executes malicious code on a system without user consent in order gain administrator-level access to a computer or network system. There are different types of Rootkit virus such as Bootkits, Firmware Rootkits, Kernel-Level Rootkits and application Rootkits[1]

It can be infected in a computer either by sharing infected disks or drives. It is typically installed through a stolen password or installed through by exploiting system vulnerabilities, social engineering tactics, and phishing techniques without the victim’s knowledge.

**Spyware** - Spyware is unwanted types of security threats to organizations which installed in user’s computer and collects sensitive information such as personal or organization’s business information, login credentials and credit card details without user knowledge[1]

This type of threats monitor your internet activity, tracking your login credentials, and spying on your sensitive information.

**Adware** - Adware is a [software program](https://www.techopedia.com/definition/25084/software-program) that contains commercial and marketing related advertisements such as display advertisements through pop-up windows or bars, banner ads, video on your computer screen. Its main purpose is to generate revenue for its developer (Adware) by serving different types advertisements to an internet user[1]

When you click on that type of advertisements then it will redirect you to an advertising websites and collect information from to you. It can be also used to steal all your sensitive information and login credentials by monitoring your online activities and selling that information to the third party.

**Ransomware** - Ransomware is type of security threats that blocks to access computer system and demands for bitcoin in order to access the system. The most dangerous ransomware attacks are  [WannaCry](https://en.wikipedia.org/wiki/WannaCry_ransomware_attack), Petya, Cerber, Locky and [CryptoLocker](https://en.wikipedia.org/wiki/CryptoLocker),…[1]

It usually happened when you either download and open a malicious email attachment, install an infected software or apps, visit a malicious or vulnerable [website](https://en.wikipedia.org/wiki/Website) or click on an untrustworthy web link or images.

**Careless employees** - Employees are the greatest security risk for any organization, because they know everything of the organizations such as where the sensitive information is stored and how to access it. In addition to malicious attacks, careless employees are other types of cyber security threats to organizations. They use very simple password to remember their mind and also share passwords. Another common problem is that employees opening suspicious email attachments, clicking on the link or visit malicious websites, which can introduce malware into the system[1]

**Natural disaster** - sometimes natural disaster occur suddenly and have a chance of destroy the hardware of the organization, usually this can be prevented by making backups and have them securely protected.

**- To protect computer systems from the above mentioned physical threats, an organization must have physical security control measures:**

**Internal:** Fire threats could be prevented by the use of automatic fire detectors and extinguishers that do not use water to put out a fire. The unstable power supply can be prevented by the use of voltage controllers. An air conditioner can be used to control the humidity in the computer room.

**External:** Lightning protection systems can be used to protect computer systems against such attacks. Lightning protection systems are not 100% perfect, but to a certain extent, they reduce the chances of Lightning causing damage. Housing computer systems in high lands are one of the possible ways of protecting systems against floods.

**Humans:** Threats such as theft can be prevented by use of locked doors and restricted access to computer rooms.

**- The following list also shows some of the possible measures that can be taken to protect cyber security threats:**

**To protect against viruses, Trojans, worms, etc. an organization can use anti-virus software:** In additional to the anti-virus software, an organization can also have control measures on the usage of external storage devices and visiting the website that is most likely to download unauthorized programs onto the user’s computer.

**Unauthorized access to computer system resources can be prevented by the use of authentication methods:** The methods can be, in the form of user ids and strong passwords, smart cards or biometric,…

There are much more kinds of thread for the organizations, so what every organization or individual usually do is to take an action to prevent from them by using anti-virus, firewall and download software from trusted sources. We also have some examples of a recently publicized security breach:

**- Twitter (2020):**

The social media platform suffered a breach where the hackers verified Twitter accounts of high profile US personalities like Barack Obama, Elon Musk, Joseph R. Biden Jr., Bill Gates, and many more.

Out of 130 targeted accounts, hackers were able to reset 45 user accounts’ passwords. Hackers posted fake tweets from these accounts, offering to send $2000 for $1000 sent to an unknown Bitcoin address. Reportedly, the [Twitter breach](https://www.kratikal.com/blog/biggest-twitter-breach-accounts-of-us-high-profiles-hacked-in-bitcoin-scam/) well-coordinated scam made attackers swindle $121,000 in Bitcoin through nearly 300 transactions.

According to the [Twitter Support](https://twitter.com/TwitterSupport/status/1289000138300563457?ref_src=twsrc%5etfw|twcamp%5etweetembed|twterm%5e1289000208701878272|twgr%5e&ref_url=https://www.theverge.com/2020/7/30/21348974/twitter-spear-phishing-attack-bitcoin-scam), “the attack on July 15, 2020, targeted a small number of employees through a phone spear-phishing attack. This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to our internal systems.”

**- Marriott(March 31st, 2020)**

The hotel chain Marriott disclosed a security breach that impacted the data of more than 5.2 million hotel guests who used their company’s loyalty application.

Hackers obtained login credentials of two accounts of Marriott employees who had access to customer information regarding the loyalty scheme of the hotel chain. They used the information to siphon off the data approximately a month before the breach was discovered.

The data accessed in the breach involved personal details such as names, birth-dates, and telephone numbers, travel information, and loyalty program information.

According to the Marriot, hackers might have obtained credentials of their employees either by credential stuffing or phishing. Previously, the hotel giant announced a data breach in late 2018 in which up to 500 million guests were impacted.

**P2 Describe at least 3 organizational security procedures.**

What is security procedure? A security procedure is a set sequence of necessary activities that performs a specific security task or function. Procedures are normally designed as a series of steps to be followed as a consistent and repetitive approach or cycle to accomplish 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 starting point for implementing the consistency needed to decrease variation in security processes, which increases control of security within the organization[2] Here are some organizational security procedures as examples:

**Security Policy from University of Notre Dame:**

- Purpose: to protect Notre Dame’s information resources from accidental or intentional unauthorized access, modification, or damage, while also preserving the open information sharing requirements of its academic culture.

- Policy Statement:

Information that Notre Dame or its agents use in the course of conducting University business is an institutional resource. Although individuals, offices, departments, programs, or schools may have responsibilities for creating and maintaining portions of University information and University records, the University itself retains ownership of, and responsibility for, the information.

Information handling standards and classifications will be created and maintained by the Information Governance Committee in partnership with Data Stewards responsible for specific data and data elements in order to properly protect University data.

- Information Handling Standards:

The Information Governance Committee will create handling standards for each Highly Sensitive data element. Data stewards may create standards for other data elements under their stewardship. These information handling standards will specify controls to manage risks to University information and related assets based on their classification. All individuals at the University are responsible for complying with these controls.

The University’s policy is to comply with all applicable legislative, regulatory and contractual requirements concerning information security. University information security standards may exceed legally prescribed requirements.

- Limit:

This policy applies to faculty, staff, students, and all others granted use of University information or related assets and defines their responsibility for the protection and appropriate use of University information, applications, computer systems, and networks.

- Policy Enforcement: The Office of Information Technologies will investigate suspected violations, and may recommend disciplinary action in accordance with University codes of conduct, policies, or applicable laws. Sanctions may include one or more of the following:

1. Suspension or termination of access.
2. Disciplinary action up to and including termination of employment.
3. Student discipline in accordance with applicable University policy.
4. Civil or criminal penalties.

Report suspected violations of this policy to the Office of Information Technologies, or to the appropriate Data Steward. Reports of violations are considered Sensitive Information until otherwise classified.

**Security Policy of Bolton University:**

- Purpose: To set out the University’s intentions in managing information security as part of effective

governance. Provide guidance to users, administrators and developers of information systems on

appropriate behavior and controls required in order to maintain the integrity of information. To provide a comprehensive approach to information security across the University and set out the means by which information policies and are scrutinized, approved, revised, communicated and monitored.

To collects, processes, stores and uses information as part of its academic and

business processes. Information may be managed through computerized or manual systems. In all

cases the University needs to ensure that adequate controls are in place to ensure information is

appropriately available, accurate, secure, and complies with legislative requirements. This

information security policy provides management direction and support for information security

across the University.

- Limit: Applies to all staff, students, governors, consultants, contractors, partnership organizations

and partner staffs of the University of Bolton. Covers all information handled, stored, processed or shared by the University irrespective of whether that information originates with or is owned by the University. And also applies to all computer and non-computer based information systems owned by the University or used for University business or connected to University managed networks.

- The implementation of the Information Security Policy:

The University will ensure that all individuals who use information systems or handle sensitive information are aware of and understand the relevant policies that apply and the consequences of non-compliance.

When necessary, the University will implement appropriate physical and logical controls to restrict access to information systems and information to only authorized users.

Full account of the requirements of the Information Security Policy will be taken in planning, designing, implementing and using IT-based information systems. The University will use lawful means of monitoring the use of information systems and networks for the purposes of preventing, and detecting breaches of the information security policy.

To determine the appropriate levels of security measures applied to information systems, a process of risk assessment shall be carried out for each system to identify the probability and impact of security failures. All users will be required to abide by University policies before being authorized for access to University information systems.

Specialist advice on information security shall be made available throughout the University and the University will ensure that it maintains and applies up-to-date knowledge of risks and mitigation within its information management practices.

The University will establish and maintain appropriate contacts with other organizations, law enforcement authorities, regulatory bodies, and network and telecommunications operators in respect of its information security policy.

- Responsibilities:

The responsibility for ensuring the protection of IT based information systems and ensuring that specific security processes are carried out shall lie with the Head of Information Systems and Technology. While the information security working group, made up of key system administrators, managers and representatives from all relevant parts of the organization, shall devise and coordinate the implementation of information security controls. The implementation and effectiveness of the information security policy shall be reviewed periodically by the University’s internal audit function as part of its regular audit program.

**Security Policy from Smartwork:**

- Purpose: The purpose of Smartwork Information Security Policy is to protect employees, assets, customer information, integrity and reputation of the organization from potential security threats. Security threats can include confidentiality, integrity and availability.

- Limit: This policy applies to all Smartwork employees and third parties who interact with information held by Smartwork and assets used to store and process the information. All Smartwork employees must adhere to the code of conduct as well as the company's policies and procedures.

- Information Security Objectives:

The primary goals of the policy are to ensure that:

* Information that are only available to authorized users according to business needs and the information systems are used effectively and effectively in accordance with Smartwork policy.
* Information assets including data, computer systems, intellectual property, and IT equipment that are appropriately protected from damage, loss, improper modification, and unauthorized use or access.
* Comply with all legal and regulatory requirements related to information technology and data collection, processing, transmission, storage and disclosure. Raise corporate information security awareness as part of day-to-day operations and to ensure that all employees understand their responsibility for maintaining information security.
* Create detailed information security standards and procedures and ensure compliance with those standards and procedures.
* Provide guidance and direction to Smartwork and its employees to protect the organization's information systems from accidental, or intentional damage or destruction.

- Policy statement:

Smartwork needs to identify security risks and their relative priorities, respond promptly and implement appropriate, effective, culturally and practically acceptable safeguards. All information, including third-party information, should be protected by appropriate security controls and handling procedures for its sensitivity and importance. Policy compliance will be monitored regularly and its measures should be periodically reviewed to protect the business. Information assets need to be protected and managed to meet contractual, legal, privacy, and ethical responsibilities. Third-party information assets need to be protected whether such protection is contractually, legally or ethically required.

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

**Firewall:**

A firewall policy defines how an organization's firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies[4]

System security improvements from firewall:

- Prevent invalid access to the system.

- Control address access, prohibit or allow the site to be accessed.

- User control over user access.

- Control content of information and packets circulating on the network.

- Filter packets based on source address, destination address, port number, protocol.

- Can be used to log all network access attempts and report to the administrator.

To prevent the case of choosing and setting Firewall incorrectly and effectively, we also have Firewall Policy. Normally the policy does the following two ways:

- Deny all, and allow only valid traffic.

- Allow all, and prohibit invalid traffic.

This work is part of the administration and security of the network, for example when creating a list of ports so that Trojans are not allowed to use,…then creating policies to block them. Otherwise, the valid traffic will be allowed.

There are many different components of the security policy that are commonly used:

- Acceptable Usage Statement: Some points to note in this component are:

+ Applications are not allowed to be installed (Internet, CD, USB or floppy disk).

+ The application backup installed on an organization's computer (decided by that organization).

+ Using accounts at computers, when there is no user, the machine must be locked and password

protected.

+ The computer and the applications installed on it are related only to the organization's activities. Not to be used to intimidate or harass any individual.

+ Email services are allowed.

- Network Connection Statement: This section is most enforced on the firewall, determining the

actual traffic of the network. Some ingredients to note are:

+ Only the administrator can perform network scans.

+ Users can access the FTP site to upload and download the required files, but the local computer

may not have the FTP server installed.

+ User can access WWW on port 80 and Email on port 25. But NNTP cannot be accessed on all

ports.

+ User sub-net 10.0.10.0 is allowed to use SSH for remote administration and vice versa.

+ User may not be able to run any Internet chat software.

+ Can’t download files larger than 5Mb

+ Anti-virus software must be installed, working well, updated weekly on the workstation and

updated daily on the server.

+ Only administrators are allowed to install new hardware on the computer (including NICs and

modems)

+ Prevent unauthorized connections to the internet in any way.

- Contracted Worker Statement:

+ There are no temporary or contractually unauthorized users who gain unauthorized access to resources, or perform network scans, copy data from the computer to any other device.

+ Cannot use FTP, telnet, or SSH without your text-based permission.

- Firewall Administrator Statement:

+ Firewall administrator must be certified by the firewall provider.

+ Must have SCNA certificate.

+ Must be familiar with the applications installed on the computers on the network.

+ Must report directly to the head of the security department.

+ Always be ready at anytime.

After building an overall security policy, it will cover many different issues, so the amount of

information will be very large Firewall[4]

**IDS:**

An intrusion detection system (IDS) is a device or [software application](https://en.wikipedia.org/wiki/Software_application) that monitors a [network](https://en.wikipedia.org/wiki/Computer_network) or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a [Security Information and Event Management](https://en.wikipedia.org/wiki/Security_information_and_event_management) (SIEM) system. A SIEM system combines outputs from multiple sources and uses [alarm filtering](https://en.wikipedia.org/wiki/Alarm_filtering) techniques to distinguish malicious activity from false alarms[5]

**IDS is divided into 2 categories based on the surveillance scope:**

- Network-based IDS (NIDS): These are IDSs that monitor the entire network. The primary source of information for the NIDS is the data packets circulating on the network. NIDS are usually installed at the entrance of the network, which may be in front of or behind the firewall.

- Host-based IDS (HIDS): These are IDSs that monitor the activities of each individual computer. Therefore, the main source of information of HIDS, in addition to data traffic to and from the server, also has system log data and system audit (system audit).

**It’s also divided into 2 categories based on implementation techniques:**

- Signature-based IDS: Signature-based IDS detects intrusions based on intrusions of intrusion, through analyzing network traffic and system logs. This technique requires maintaining a signature database, and this database must be updated regularly every time a new intrusion form or technique is introduced.

- Anomaly-based IDS: intrusion detection by comparing (statistically) current behavior with the normal operation of the system to detect anomaly that could be a sign of intrusion. For example, under normal conditions, the traffic on a server's network interface is approximately 25% of the maximum communication bandwidth. If at any point this traffic suddenly increases to 50% or more, then it can be assumed that the server is under a DoS attack. In order to function correctly, IDSs of this type must perform a "learning" process, monitoring the system's performance under normal conditions to record operational parameters, which is the basis for detection. later abnormalities [5]

**Incorrect configuration of firewall policies and IDS:**

When there’s incorrect configuration of firewall policies and IDS happening, many different things can happen, but it primarily results in two outcomes:

**- Desired traffic doesn’t reach it’s intended destination.**

The reason was because it was either  blocked, routed to the wrong destination or it couldn’t be routed at all. Usually it will likely be noticed fairly quickly when processes don’t work as expected.

**- Undesirable traffic reaches a destination that it should not.**

While it’s possible this could cause some negative consequence by accident, it’s also a possible attack vector for individuals with malicious intent like hacking and possible data corruption.

**In more details, incorrect configuration of the IDS system can lead to some serious consequences, such as:**

- Networks will intentionally take advantage of this to bypass IDS supervision to access the system that IDS protects.

- IDS will not be able to fully monitor or monitor the traffic accessing the system.

- The IDS system may fail and report on normal access.

- The IDS may misreport activities on the systems it protects.

**For firewall, incorrect configuration can lead to:**

- Causing a number of vulnerabilities in the firewall system. Hackers will take advantage of this vulnerability to destroy or steal data of the system that the firewall was trying to protect.

- Become inoperable or work against the rules desired by the one who do the configuration. For example, allow invalid accesses and block valid accesses.

- Configuring a firewall incorrectly can prevent the firewall from working. And then the system that the firewall protects will face the risk of crashing the system.

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

**DMZ:**

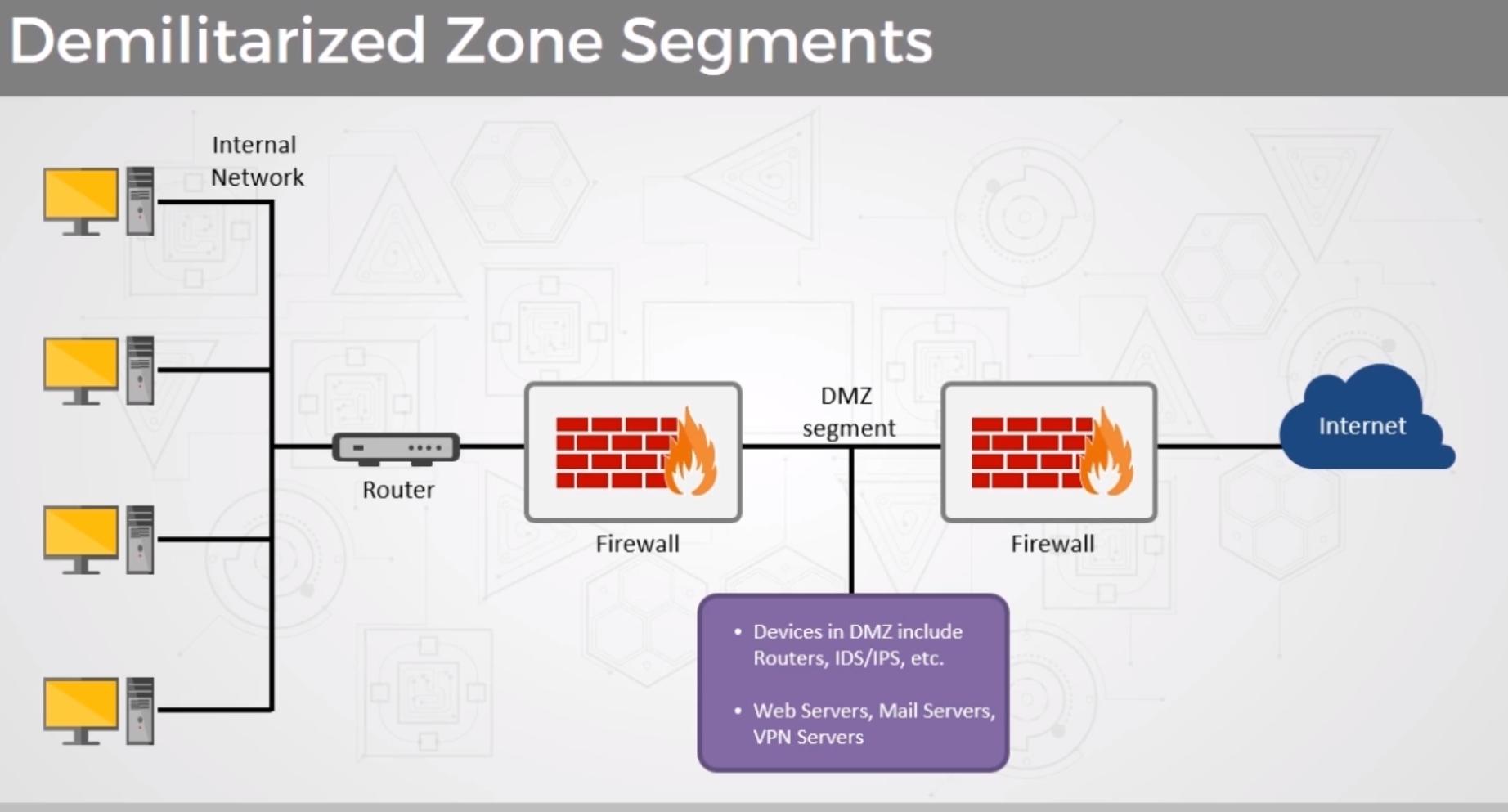
A demilitarized zone (DMZ) is a perimeter network that protects an organization’s internal local-area network (LAN) from untrusted traffic.

A common DMZ meaning is a sub-network that sits between the public internet and private networks. It exposes external-facing services to untrusted networks and adds an extra layer of security to protect the sensitive data stored on internal networks, using firewalls to filter traffic[6]

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[6]

As an example, 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.



Improvements for implementing DMZ:

- Reduce damage to hosts when attacked by hackers.

- Add more layers of defense to the intranet.

- Avoid attacks from outside the internet or internal attacks.

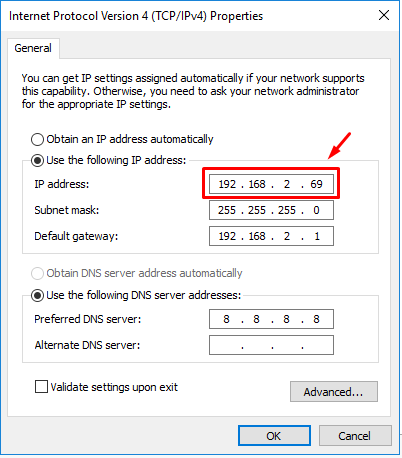
All in all, it helps enabling access control, preventing network reconnaissance, the servers within the DMZ are exposed publicly but are offered another layer of security by a firewall that prevents an attacker from seeing inside the internal network, and it also helps blocking Internet Protocol (IP) spoofing, a DMZ can discover and stall such spoofing attempts as another service verifies the legitimacy of the IP address. The DMZ also provides network segmentation to create a space for traffic to be organized and public services to be accessed away from the internal private network.

**Static IP address:**

A static IP is an IP address that is fixed, meaning that it never changes. If you are connected to an Internet connection that is “always on”, most likely you have a static IP address, although some of the “always on” connections use dynamic IP addressing to make the installation process easier[7]

For example, if a static IP address is set up for a computer in a home network. Once the computer has a specific address tied to it, a router can be set up to always forward certain inbound requests directly to that computer, such as [FTP](https://www.lifewire.com/ftp-defined-2654479) requests if the computer shares files over FTP.

Another example of a static IP address at work is with [DNS servers](https://www.lifewire.com/what-is-a-dns-server-2625854). DNS servers use static IP addresses so that devices always knows how to connect to them. If they changed often, you'd have to regularly [reconfigure those DNS servers on your router or computer](https://www.lifewire.com/how-to-change-dns-server-settings-2617979) to use the [internet](https://www.lifewire.com/difference-between-the-internet-and-the-web-2483335).



Improvements of implementing static IP:

- Better DNS support.

- More convenient in remote access.

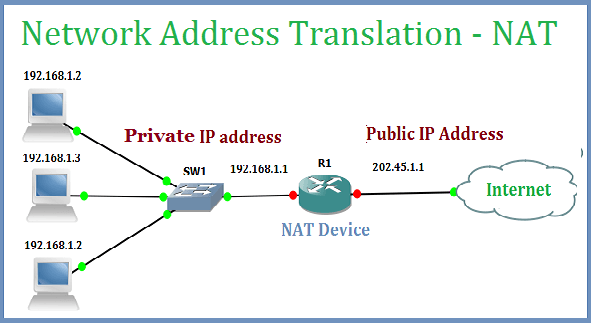
- Static IP address will help you connect to the Internet quickly without having to re-issue a new IP address.

- Static IP addresses also help to speed up access and download files.

**NAT:**

NAT (or Network Address Translation) translates the IP addresses of computers in a local network to a single [IP address](https://techterms.com/definition/ip_address). This address is often used by the [router](https://techterms.com/definition/router) that connects the computers to the Internet. This adds an extra level of security, since the router can be configured as a [firewall](https://techterms.com/definition/firewall), only allowing authorized systems to access the computers within the network. NAT makes computers outside the local area network ([LAN](https://techterms.com/definition/lan)) see only one IP address, while computers within the network can see each system's unique address. While this aids in network security, it also limits the number of IP addresses needed by companies and organizations[8]

For example, in some large networks, some servers may act as Web servers and require access from the Internet. These servers are assigned public IP addresses on the firewall, allowing the public to access the servers only through that IP address. However, as an additional layer of security, the firewall acts as the intermediary between the outside world and the protected internal network. Additional rules can be added, including which ports can be accessed at that IP address.



Advantages of implementing NAT:

- NAT can share internet connection for many different computers, mobile devices in LAN with only one public IP address.

- Saving IPv4 addresses: The number of users accessing the internet is increasing. This leads to the risk of IPv4 address shortages. The NAT technique helps to reduce the number of IP addresses to use.

- NAT helps network administrators filter incoming packets and verify public IPs access to any port.

- Helps to conceal IP inside LAN.

Improvement:

- Conceal IP to avoid IP detection and avoid being tracked.

- Remove packets containing malicious code or malware.

- Verify and prevent access with malicious intent[9]

NAT is a very important aspect of firewall security. It conserves the number of public addresses used within an organization, and it allows for stricter control of access to resources on both sides of the firewall.

**References**

1. Yeh, Q.J. and Chang, A.J.T., 2007. Threats and countermeasures for information system security: A cross-industry study. *Information & Management*, *44*(5), pp.480-491.
2. Yu, C.F., Verizon Laboratories Inc, 1990. *Distributed security procedure for intelligent networks*. U.S. Patent 4,919,545.
3. Peltier, T.R., 2016. *Information Security Policies, Procedures, and Standards: guidelines for effective information security management*. CRC Press.
4. Al-Shaer, E.S. and Hamed, H.H., 2004. Modeling and management of firewall policies. *IEEE Transactions on network and service management*, *1*(1), pp.2-10.
5. Ashoor, A.S. and Gore, S., 2011. Importance of intrusion detection system (IDS). *International Journal of Scientific and Engineering Research*, *2*(1), pp.1-4.
6. Iskandar, A., Virma, E. and Ahmar, A.S., 2019. Implementing DMZ in improving network security of web testing in STMIK AKBA. *arXiv preprint arXiv:1901.04081*.
7. Levy, S.B., Microsoft Corp, 2002. *Method using an assigned dynamic IP address and automatically restoring the static IP address*. U.S. Patent 6,466,981.
8. Smith, M. and Hunt, R., 2002, August. Network security using NAT and NAPT. In *Proceedings 10th IEEE International Conference on Networks (ICON 2002). Towards Network Superiority (Cat. No. 02EX588)* (pp. 355-360). IEEE.
9. Malik, S., 2003. Network security principles and practices. Indianapolis, Ind, Cisco.