


ASSIGNMENT FRONT SHEET

Qualification	BTEC Level 5 HND Diploma in Computing		
Unit number and title	Unit 5: Security		
Submission date		Date Received 1st submission	
Re-submission Date		Date Received 2nd submission	
Student Name	NGUYEN CAO TRI	Student ID	GCS16241
Class	1623	Assessor name	LE HUYNH QUOC BAO
Student declaration <p>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.</p>			
		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
<p>You work as a trainee IT Security Specialist for a leading Security consultancy in Vietnam called FPT Information security FIS.</p> <p>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.</p> <p>In addition to your presentation you should also provide a detailed report containing a technical review of the topics covered in the presentation.</p> <p>Your presentation should:</p> <ol style="list-style-type: none"> 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. <p>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.</p>

Learning Outcomes and Assessment Criteria		
Pass	Merit	Distinction
LO1 Assess risks to IT security		

<p>P1 Identify types of security threat to organisations.</p> <p>Give an example of a recently publicized security breach and discuss its consequences.</p>	<p>M1 Propose a method to assess and treat IT security risks.</p>	<p>LO1 & 2</p> <p>D1 Investigate how a ‘trusted network’ may be part of an IT security solution.</p>
<p>LO2 Describe IT security solutions</p>		
<p>P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS.</p> <p>P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.</p>	<p>M2 Discuss three benefits to implement network monitoring systems with supporting reasons.</p>	

Contents

P1 Identify types of security threat to organizations. Give an example of a recently publicized security breach and discuss its consequences.	7
CYBER-ATTACKS:	7
COMPUTER VIRUSES	7
WORM	7
TROJANS HORSE	7
SPYWARE	8
ADWARE	8
DENIAL-OF-SERVICE (DOS) ATTACKS	9
PHISHING	9
SQL INJECTION	9
MALWARE	10
PHYSICAL THREATS	10
Canva	10
Sina Weibo	11
LinkedIn	11
P2 Describe at least 3 organizational security procedures.	12
1. Acceptable Use Policy (AUP)	12
2. Access Control Policy (ACP)	12
3. Change Management Policy	12
4. Information Security Policy	12
5. Incident Response (IR) Policy	13
6. Remote Access Policy	13
7. Email/Communication Policy	13
8. Disaster Recovery Policy	13
P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS.	13
1. Broad policy configurations	14
2. Risky rogue services and management services	14
3. Non-standard authentication mechanisms	14
4. Test systems using production data	15
5. Log outputs from security devices	15
P4 Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security.	15

DMZ	15
NAT	17

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

There are many security threats that an organization can face we can sort it in to two main categories: Cyber-attack and physical threat. Cyber-attacks are day by day changing their attacking techniques and gaining access of an organizations system. There are different **types of security threats to organizations**, which can affect business continuity of an organization. So, there is no way to be completely sure that an organization is free from cyber security threats or attacks.

CYBER-ATTACKS:

COMPUTER VIRUSES

A virus 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.

It has capability to corrupt or damage organization's sensitive data, destroy files and format hard drives.

There are different ways that a virus can be spread or attack, such as:

- Clicking on an executable file
- Installing free software and apps
- Visiting an infected and unsecured website
- Clicking on advertisement
- Using of infected removable storage devices, such USB drives
- Opening spam email or clicking on URL link
- Downloading free games, toolbars, media players and other software.

WORM

Computer worm is a type of malicious software or program that spreads within its connected network and copies itself from one computer to another computer of an organization.

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

TROJANS HORSE

Trojan horse is a malicious code 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 or network.

- The victim receives 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.

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.

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

So, every organization or individual should take an action to prevent from spyware by using anti-virus, firewall and download software from trusted sources.

It can be automatically installs itself on your computer or hidden component of software packages or can be install as traditional malware such as deceptive ads, email and instant messages.

ADWARE

Adware is a 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.

- When you click on that type of advertisements then it redirects 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 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, Petya, Cerber, Locky and CryptoLocker etc.

All types of threats typically installed in a computer system through the following ways:

- When download and open a malicious email attachment
- Install an infected software or apps
- When user visit a malicious or vulnerable website
- Click on untrusted web link or images

DENIAL-OF-SERVICE (DOS) ATTACKS

Denial-of-Service is an attack that shut down a machine or network or making it inaccessible to the users. It typically flooding a targeted system with requests until normal traffic is unable to be processed, resulting in denial-of-service to users.

- It occurs when an attacker prevents legitimate users from accessing specific computer systems, devices or other resources.
- The attacker sends too much traffic to the target server
- Overloading it with traffic and the server is overwhelmed, which causes to down websites, email servers and other services which connect to the Internet.

PHISHING

Phishing is a type of social engineering attack that attempt to gain confidential information such as usernames, passwords, credit card information, login credentials, and so more.

- In a phishing email attack, an attacker sends phishing emails to victim's email that looks like it came from your bank and they are asked to provide your personal information.
- The message contains a link, which redirects you to another vulnerable website to steal your information.
- So, it is better to avoid or don't click or don't open such type of email and don't provide your sensitive information.

SQL INJECTION

SQL injection is type of an injection attack and one of the most common web hacking techniques that allows attacker to control the back end database to change or delete data.

It is an application security weakness and when an application fails to properly sanitize the SQL statements then attacker can include their own malicious SQL commands to access the organization database. Attacker includes the malicious code in SQL statements, via web page input.

MALWARE

Malware is software that typically consists of program or code and which is developed by cyber attackers. It is types of cyber security threats to organizations which are designed to extensive damage to systems or to gain unauthorized access to a computer.

- There are different ways that a malware can infect a device such as it can be delivered in the form of a link or file over email and it requires the user to click on that link or open the file to execute the malware.
- This type of attack includes computer viruses, worms, Trojan horses and spyware.

PHYSICAL THREATS

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.

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. 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:

Canva

Date: May 2019

Impact: 137 million user accounts

Details: In May 2019 Australian graphic design tool website Canva suffered an attack that exposed email addresses, usernames, names, cities of residence, and salted and hashed with bcrypt passwords (for users not using social logins — around 61 million) of 137 million users. Canva says the hackers managed to view, but not steal, files with partial credit card and payment data.

The suspected culprit(s) — known as Gnosticplayers — contacted ZDNet to boast about the incident, saying that Canva had detected their attack and closed their data breach server. The attacker also claimed to have gained OAuth login tokens for users who signed in via Google.

The company confirmed the incident and subsequently notified users, prompted them to change passwords, and reset OAuth tokens. However, according to a later post by Canva, a list of approximately 4 million Canva accounts containing stolen user passwords was later decrypted and shared online, leading the company to invalidate unchanged passwords and notify users with unencrypted passwords in the list.

Sina Weibo

Date: March 2020

Impact: 538 million accounts

Details: With over 500 million users, Sina Weibo is China's answer to Twitter. However, in March 2020 it was reported that the real names, site usernames, gender, location, and -- for 172 million users -- phone numbers had been posted for sale on dark web markets. Passwords were not included, which may indicate why the data was available for just ¥1,799 (\$250).

Weibo acknowledged the data for sale was from the company, but claimed the data was obtained by matching contacts against its address book API. It also said that since doesn't store passwords in plaintext, users should have nothing to worry about. This, however, doesn't tally as some of the information being offered such as location data, isn't available via the API. The social media giant said it had notified authorities about the incident and China's Cyber Security Administration of the Ministry of Industry and Information Technology said it is investigating.

LinkedIn

Date: 2012 (and 2016)

Impact: 165 million user accounts

Details: As the major social network for business professionals, LinkedIn has become an attractive proposition for attackers looking to conduct social engineering attacks. However, it has also fallen victim to leaking user data in the past.

In 2012 the company announced that 6.5 million unassociated passwords (unsalted SHA-1 hashes) were stolen by attackers and posted onto a Russian hacker forum. However, it wasn't until 2016 that the full extent of the incident was revealed. The same hacker selling MySpace's data was found to be offering the email addresses and passwords of around 165 million LinkedIn users for just 5 bitcoins (around \$2,000 at the time). LinkedIn acknowledged that it had been made aware of the breach, and said it had reset the passwords of affected accounts.

These attacks not only make companies loss millions dollar, it also leak millions user detail, password onto internet.

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. Decreasing variation is also a good way to eliminate waste, improve quality, and increase performance within the security department.

1. Acceptable Use Policy (AUP)

An AUP stipulates the constraints and practices that an employee using organizational IT assets must agree to in order to access to the corporate network or the internet. It is standard onboarding policy for new employees. They are given an AUP to read and sign before being granted a network ID. It is recommended that an organizations IT, security, legal and HR departments discuss what is included in this policy. An example that is available for fair use can be found at SANS.

2. Access Control Policy (ACP)

The ACP outlines the access available to employees in regards to an organization's data and information systems. Some topics that are typically included in the policy are access control standards such as NIST's Access Control and Implementation Guides. Other items covered in this policy are standards for user access, network access controls, operating system software controls and the complexity of corporate passwords. Additional supplementary items often outlined include methods for monitoring how corporate systems are accessed and used; how unattended workstations should be secured; and how access is removed when an employee leaves the organization. An excellent example of this policy is available at IAPP.

3. Change Management Policy

A change management policy refers to a formal process for making changes to IT, software development and security services/operations. The goal of a change management program is to increase the awareness and understanding of proposed changes across an organization, and to ensure that all changes are conducted methodically to minimize any adverse impact on services and customers. A good example of an IT change management policy available for fair use is at SANS.

4. Information Security Policy

An organization's information security policies are typically high-level policies that can cover a large number of security controls. The primary information security policy is issued by the company to ensure that all employees who use information technology assets within the breadth of the

organization, or its networks, comply with its stated rules and guidelines. I have seen organizations ask employees to sign this document to acknowledge that they have read it (which is generally done with the signing of the AUP policy). This policy is designed for employees to recognize that there are rules that they will be held accountable to with regard to the sensitivity of the corporate information and IT assets. The State of Illinois provides an excellent example of a cybersecurity policy that is available for download.

5. Incident Response (IR) Policy

The incident response policy is an organized approach to how the company will manage an incident and remediate the impact to operations. It's the one policy CISOs hope to never have to use. However, the goal of this policy is to describe the process of handling an incident with respect to limiting the damage to business operations, customers and reducing recovery time and costs. Carnegie Mellon University provides an example of a high-level IR plan and SANS offers a plan specific to data breaches.

6. Remote Access Policy

The remote access policy is a document which outlines and defines acceptable methods of remotely connecting to an organization's internal networks. I have also seen this policy include addendums with rules for the use of BYOD assets. This policy is a requirement for organizations that have dispersed networks with the ability to extend into insecure network locations, such as the local coffee house or unmanaged home networks. An example of a remote access policy is available at SANS.

7. Email/Communication Policy

A company's email policy is a document that is used to formally outline how employees can use the business' chosen electronic communication medium. I have seen this policy cover email, blogs, social media and chat technologies. The primary goal of this policy is to provide guidelines to employees on what is considered the acceptable and unacceptable use of any corporate communication technology. An example of an email policy is available at SANS.

8. Disaster Recovery Policy

An organization's disaster recovery plan will generally include both cybersecurity and IT teams' input and will be developed as part of the larger business continuity plan. The CISO and teams will manage an incident through the incident response policy. If the event has a significant business impact, the Business Continuity Plan will be activated. An example of a disaster recovery policy is available at SANS.

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

Firewalls are an essential part of your network security, and a misconfigured firewall can damage your organization and give easy access to an attacker. Yet misconfigurations are alarmingly common. In my work I come across lots of mistakes in firewall configurations. Below are five of the most common types that I encounter, along with advice on how you can avoid them.

1. Broad policy configurations

Firewalls are often set up with an open policy of allowing traffic from any source to any destination. This is because IT teams don't know exactly what they need at the outset, and therefore start with broad rules and work backwards. However, the reality is that due to time pressures or simply not regarding it as a priority, they never get round to defining firewall policies. This leaves the network in a perpetually exposed state.

Organizations should follow the principle of least privilege – that is, giving the minimum level of privilege that the user or service needs to function normally, thereby limiting the potential damage caused by a breach. It's also a good idea to regularly revisit your firewall policies to look at application usage trends and identify new applications being used on the network and what connectivity they require.

2. Risky rogue services and management services

Services that are left running on the firewall that don't need to be is another mistake I often find. Two of the main culprits are dynamic routing, which typically should not be enabled on security devices as best practice, and "rogue" DHCP servers on the network distributing IPs, which can potentially lead to availability issues as a result of IP conflicts. I'm also surprised to see the number of devices that are still managed using unencrypted protocols like telnet, despite the protocol being over 30 years old.

The answer to this problem is hardening devices and ensuring that configurations are compliant before the device is put into a production setting. This is something with which a lot of enterprises struggle. But by configuring your devices based on the function that you actually want them to fulfill and following the principle of least privileged access, you will improve security and reduce the chances of accidentally leaving a risky service running on your firewall.

3. Non-standard authentication mechanisms

During my work, I often find organizations that use routers that don't follow the enterprise standard for authentication. For example, a large bank I worked with had all the devices in its primary data center controlled by a central authentication mechanism, but did not use the same mechanism at its remote office. By not enforcing corporate authentication standards, staff in the remote branch could access local accounts with weak passwords, and had a different limit on login failures before account lockout.

This scenario reduces security and creates more vectors for attackers, as it's easier for them to access the corporate network via the remote office. Organizations should ensure that all remote offices follow the same central authentication mechanism as the rest of the company.

4. Test systems using production data

Companies tend to have good governance policies requiring that test systems should not connect to production systems and collect production data. But in practice, this is often not enforced because the people who are working in testing see production data as the most accurate way to test. The problem occurs because when you allow test systems to collect data from production, you're likely to bring that data into an environment with a lower level of security. The data could be highly sensitive, and it could also be subject to regulatory compliance. So if you do use production data in a test environment, make sure that you use the correct security controls according to the classification of the data.

5. Log outputs from security devices

The issue that I see more often than I should is organizations not analyzing log outputs from their security devices -- or without enough granularity. This is one of the biggest mistakes you can make in terms of network security; not only will you *not* be alerted when you're under attack, but you'll have little or no traceability when you're investigating post-breach.

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

DMZ

In computer security a **DMZ** or **demilitarized zone** (sometimes referred to as a **perimeter network** or screened subnet) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted, usually larger, network such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. The DMZ functions as a small, isolated network positioned between the Internet and the private network.

The DMZ is seen as not belonging to either party bordering it. This metaphor applies to the computing use as the DMZ acts as a gateway to the public Internet. It is neither as secure as the internal network, nor as insecure as the public internet.

In this case, the hosts most vulnerable to attack are those that provide services to users outside of the local area network, such as e-mail, Web and Domain Name System (DNS) servers. Because of the increased potential of these hosts suffering an attack, they are placed into this specific subnetwork in order to protect the rest of the network should any of them become compromised.

Hosts in the DMZ are permitted to have only limited connectivity to specific hosts in the internal network, as the content of DMZ is not as secure as the internal network. Similarly, communication between hosts in the DMZ and to the external network is also restricted to make the DMZ more secure than the Internet and suitable for housing these special purpose services. This allows hosts in the DMZ to communicate with both the internal and external network, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients, and another firewall would perform some level of control to protect the DMZ from the external network.

A DMZ configuration provides additional security from external attacks, but it typically has no bearing on internal attacks such as sniffing communication via a packet analyzer or spoofing such as e-mail spoofing.

It is also sometimes good practice to configure a separate Classified Militarized Zone (CMZ), a highly monitored militarized zone comprising mostly Web servers (and similar servers that interface to the external world i.e. the Internet) that are not in the DMZ but contain sensitive information about accessing servers within LAN (like database servers). In such architecture, the DMZ usually has the application firewall and the FTP while the CMZ hosts the Web servers. (The database servers could be in the CMZ, in the LAN, or in a separate VLAN altogether.)

Any service that is being provided to users on the external network can be placed in the DMZ. The most common of these services are:

- Web servers
- Mail servers
- FTP servers
- VoIP servers

Web servers that communicate with an internal database require access to a database server, which may not be publicly accessible and may contain sensitive information. The web servers can communicate with database servers either directly or through an application firewall for security reasons.

E-mail messages and particularly the user database are confidential, so they are typically stored on servers that cannot be accessed from the Internet (at least not in an insecure manner), but can be accessed from email servers that are exposed to the Internet.

The mail server inside the DMZ passes incoming mail to the secured/internal mail servers. It also handles outgoing mail.

For security, compliance with legal standards such as HIPAA, and monitoring reasons, in a business environment, some enterprises install a proxy server within the DMZ. This has the following benefits:

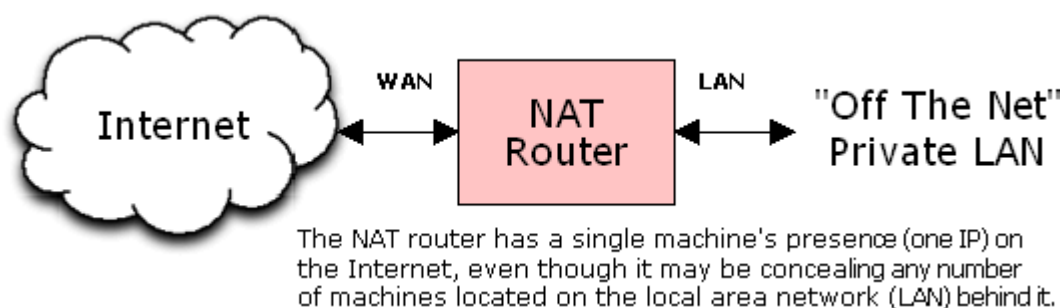
- Obliges internal users (usually employees) to use the proxy server for Internet access.
- Reduced Internet access bandwidth requirements since some web content may be cached by the proxy server.
- Simplifies recording and monitoring of user activities.
- Centralized web content filtering.

STATIC IP

NAT

A NAT router creates a local area network (LAN) of private IP addresses and interconnects that LAN to the wide area network (WAN) known as the Internet. The "Network Address Translation" (NAT) performed by the router allows multiple computers (machines) connected to the LAN behind the router to communicate with the external Internet.

The most common use for NAT routers is serving as an "interface" between the global public WAN Internet and a private non-public LAN:



One of the key benefits of NAT routers (and the main reason for their purchase by residential and small office users) is that the router appears to the Internet as a single machine with a single IP address. This effectively masks the fact that many computers on the LAN side of the router may be simultaneously sharing that single IP. This is good for the Internet since it helps to conserve the Net's limited IP space.

Although NAT routers are not generally purchased for their security benefits, all NAT routers inherently function as very effective hardware firewalls (with a few caveats examined below). As a hardware firewall they prevent "unsolicited", unexpected, unwanted, and potentially annoying or dangerous traffic from the public Internet from passing through the router and entering the user's private LAN network.

The reason they do this is very simple: With multiple "internal" computers on the LAN behind the router, the router must know which internal computer should receive each incoming packet of data. Since ALL incoming packets of data have the same IP address (the single IP address of the router), **the only way the router knows which computer should receive the incoming packet is if one of the internal computers on the private LAN FIRST sent data packets out to the source of the returning packets.**

Since the NAT router links the internal private network to the Internet, it sees everything sent out to the Internet by the computers on the LAN. It memorizes each outgoing packet's destination IP and port number in an internal "connections" table and assigns the packet its own IP and one of its own ports for

accepting the return traffic. Finally, it records this information, along with the IP address of the internal machine on the LAN that sent the outgoing packet, in a "current connections" table.

When any incoming packets arrive at the router from the Internet, the router scans its "current connections" table to see whether this data is **expected** by looking for the remote IP and port number in the current connections table. If a match is found, the table entry also tells the router which computer in the private LAN is expecting to receive the incoming traffic from that remote address. So the router re-addresses (translates) the packet to that internal machine and sends it into the LAN.

REFERENCE

Cyber Security Portal. 2020. *Common Types Of Security Threats To Organizations | Cyber Security Portal*. [online] Available at: <<https://cyberthreatportal.com/types-of-security-threats-to-organizations/>> [Accessed 10 December 2020].

Dark Reading. 2020. *5 Most Common Firewall Configuration Mistakes*. [online] Available at: <<https://www.darkreading.com/operations/5-most-common-firewall-configuration-mistakes-/a/d-id/1322225>> [Accessed 10 December 2020].

En.wikipedia.org. 2020. *DMZ (Computing)*. [online] Available at: <[https://en.wikipedia.org/wiki/DMZ_\(computing\)](https://en.wikipedia.org/wiki/DMZ_(computing))> [Accessed 10 December 2020].

Steve Gibson, G., 2020. *GRC | NAT - The Security Of Network Address Translation*. [online] Grc.com. Available at: <<https://www.grc.com/nat/nat.htm>> [Accessed 10 December 2020].

Swinhoe, D., 2020. *The 15 Biggest Data Breaches Of The 21St Century*. [online] CSO Online. Available at: <<https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>> [Accessed 10 December 2020].

Hayslip, G., 2020. *9 Policies And Procedures You Need To Know About If You'Re Starting A New Security Program*. [online] CSO Online. Available at: <<https://www.csoonline.com/article/3263738/9-policies-and-procedures-you-need-to-know-about-if-youre-starting-a-new-security-program.html>> [Accessed 10 December 2020].