Assignment Brief 1 (RQF)

Higher National Certificate/Diploma in Computing

|  |  |
| --- | --- |
| **Student Name/ID Number:** | **GCS20036/NGUYEN NHAT HAO** |
| **Unit Number and Title:** | **Unit 5: Security** |
| **Academic Year:** | **2021 – 2022** |
| **Unit Assessor:** | **SAM** |
| **Assignment Title:** | **Security Presentation** |
| **Issue Date:** | **April 1st, 2021** |
| **Submission Date:** | **22/8/2022** |
| **Internal Verifier Name:** |  |
| **Date:** |  |

|  |
| --- |
| **Submission Format:** |
| *Format:*   * The submission is in the form of an individual written report. This should be written in a concise, formal business style using single spacing and font size 12. You are required to make use of headings, paragraphs and subsections as appropriate, and all work must be supported with research and referenced using the Harvard referencing system. Please also provide a bibliography using the Harvard referencing system.   *Submission*   * Students are compulsory to submit the assignment in due date and in a way requested by the Tutor. * The form of submission will be a soft copy posted on <http://cms.greenwich.edu.vn/>. * Remember to convert the word file into PDF file before the submission on CMS.   *Note:*   * The individual Assignment *must* be your own work, and not copied by or from another student. * If you use ideas, quotes or data (such as diagrams) from books, journals or other sources, you must reference your sources, using the Harvard style. * Make sure that you understand and follow the guidelines to avoid plagiarism. Failure to comply this requirement will result in a failed assignment. |
| **Unit Learning Outcomes:** |
| **LO1** Assess risks to IT security.  **LO2** Describe IT security solutions. |
| **Assignment Brief and Guidance:** |
| **Assignment scenario**  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.  **Tasks**  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:   * 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 * Describe a variety of organizational procedures an organization can set up to reduce the effects to the business of a security breach. * Propose a method that FIS can use to prioritize the management of different types of risk * Discuss three benefits to FIS of implementing network monitoring system giving suitable reasons. * 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. * 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 (Assignment 1):** | | | |
| Learning Outcome | Pass | Merit | Distinction |
| **LO1** | **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. | **D1** Investigate how a ‘trusted network’ may be part of an IT security solution. |
| **LO2** | **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

[1 P1 Identify types of security threat to organisations. Give an example of a recently publicized security breach and discuss its consequences. 5](#_Toc112443207)

[Define threats 5](#_Toc112443208)

[Identify threats agents to organizations 5](#_Toc112443209)

[List type of threats that organizations will face 6](#_Toc112443210)

[Botnet 6](#_Toc112443211)

[Cryptojacking 6](#_Toc112443212)

[Ransomware 7](#_Toc112443213)

[Phishing 7](#_Toc112443214)

[DDoS (Distributed Denial of Service) Attack 7](#_Toc112443215)

[APT (Advanced Persistent Threats) 7](#_Toc112443216)

[What are the recent security breaches? List and give examples with dates 8](#_Toc112443217)

[CAM4 data breach 8](#_Toc112443218)

[Yahoo data breach 2017 9](#_Toc112443219)

[Aadhaar data breach 9](#_Toc112443220)

[First American Financial Corp. data breach 10](#_Toc112443221)

[Verifications.io data breach 11](#_Toc112443222)

[LinkedIn data breach 2021 11](#_Toc112443223)

[Discuss the consequences of this breach 12](#_Toc112443224)

[Reputational damage 12](#_Toc112443225)

[Theft 13](#_Toc112443226)

[Financial losses 13](#_Toc112443227)

[Fines 13](#_Toc112443228)

[Below-the-surface costs 14](#_Toc112443229)

[Suggest solutions to organizations 14](#_Toc112443230)

[2 P2 Describe at least 3 organisational security procedures. 14](#_Toc112443231)

[Credit Card Processing Procedures 15](#_Toc112443232)

[Vulnerability Management Procedure 17](#_Toc112443233)

[Patch Management Process 19](#_Toc112443234)

[3 P3 Identify the potential impact to IT security of incorrect configuration of firewall policies and IDS. 22](#_Toc112443235)

[Discuss briefly firewalls and policies, their usage and advantages in a network 22](#_Toc112443236)

[II. How does a firewall provide security to a network? 27](#_Toc112443237)

[III. IDS 27](#_Toc112443238)

[IV. The potential impact (Threat-Risk) of a firewall and IDS if they are incorrectly configured in a network 29](#_Toc112443239)

[4 Task 4 - Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security (P4) 30](#_Toc112443240)

[I. Define and discuss with the aid of diagram DMZ. Focus on its usage and security function as advantage 30](#_Toc112443241)

[II. Define and discuss with the aid of diagram static IP. Focus on its usage and security function as advantage 33](#_Toc112443242)

[III. Define and discuss with the aid of diagram NAT. Focus on its usage and security function as advantage 35](#_Toc112443243)

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

## Define threats

Two rather short and concise can be found in documents from IETF and NIST.

* In [RFC 4949](https://tools.ietf.org/html/rfc4949), IETF defines a threat as

A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm.

* NIST, in [SP800-160](https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final), defines it as

An event or condition that has the potential for causing asset loss and the undesirable consequences or impact from such loss.

Cyber threats are sometimes incorrectly confused with vulnerabilities. Looking at the definitions, the keyword is “potential”. The threat is not a security problem that exists in an implementation or organization. Instead it is something that *can* violate the security. This can be compared to a vulnerability which is an actual weakness that can be exploited. The threat always exist, regardless of any countermeasures. However, countermeasures can be used to minimize the probability of it being realized.

Identify threats agents to organizations

Identify threat agents as specific organizations or individuals, like Anonymous, or we may classify them by goals or methods of operation (MOs). For example, shoplifters are a class of threat agent that attacks retail stores.

A threat agent has the following properties:

* A set of goals – these may be political, financial, religious, or reflect other personal or community values.
* A level of motivation – these indicate the types of risks  the agent is willing to take and levels of damage willing to cause in pursuing the goals. These are discussed below.
* Assets and resources – these indicate the types and amount of effort the agent may expend. Effort may be spent on training or collecting data for an attack as well as the costs of the attack itself.
* Method of operation/MO – these are the typical features of the agent’s attacks.

The levels of motivation contain two scales. The lower three levels reflect risks in typical social environments, like households or small businesses. The higher three levels represent risks faced in the world at large.

* Unmotivated – Potential threat agents are not at all motivated to attack.
* Scant motivation – Threat agents may take advantage of unprotected assets if the risk of detection are small. Attacks won’t occur unless they can succeed with little or no effort or sophistication.
* Stealth motivation – Threat agents may be motivated to invest in and use established techniques to attack assets, as long as the risk of detection is small.
* Low motivation – willing to cause detectable damage of limited scope.
* Moderate motivation – willing to cause damage, though not to cause significant damage or serious injury to people.
* High motivation – willing to cause significant damage, including death or serious injury of people.

List type of threats that organizations will face

### Botnet

A combination of the words “robot” and “network”, a Botnet is a group of private computers infected with malicious software and controlled as a group without the owners' knowledge. They’re often used to deliver large volumes of spam, carryout DDoS attacks (see below), and steal data/credentials. Botnets have the collective computing power to act as a force multiplier for groups looking to disrupt or break into targets’ systems.

### Cryptojacking

Crypto jacking is the unauthorized use of someone else’s computer to mine cryptocurrency. Hackers usually trick the victim into clicking on a malicious email link which loads crypto mining code on the computer, or by infecting a website or online ad with code that auto-executes once loaded in the victim’s browser. The crypto mining code then works in the background as unsuspecting victims use their computers normally. The victim may notice the computer’s slower performance while they’re working, but otherwise it can go undetected. The uptick in crypto jacking in 2019 is simply the promise of more money for less risk.

### Ransomware

Ransomware is malicious malware that threatens to publish or steal victims’ data or prevents users from accessing their systems until a ransom is paid. Ransomware has grown to be one of the biggest problems in network security because it can paralyze large organizations and even whole cities, with [Atlanta](https://www.nc4.com/blogs/we-need-to-talk-about-the-cyber-attack-on-atlanta/) and [Baltimore](https://www.celerium.com/blog/what-happened-in-baltimore) as recent examples. The infection often starts with someone clicking on what looks like an innocent link or attachment, then turns into a disaster for companies of all sizes when vital files and documents are suddenly inaccessible and held for ransom. However, sometimes paying the ransom won’t fix the problem. Sometimes cybercriminals demand ransom even though the data they took is already destroyed.

4. Worms

A worm is self-replicating malware that duplicates itself to spread to uninfected computers. Its primary function is to infect other computers while remaining active on infected systems. Worms spread by exploiting vulnerabilities in operating systems; this kind of attack literally worms its way into systems by finding cracks and replicating itself over and over.

### Phishing

A phishing attack involves using email to trick employees into believing a message is from a legitimate, trustworthy source. Then, when they click a link in the email or open an attachment, their computer becomes infected. The phisher could be someone pretending to be from the employee’s company, or perhaps a company he/she does business with. Sometimes the message will describe something the employee either wants or needs, or thinks they are expecting— a request from their bank, for instance. Whatever the masquerade, a sophisticated phishing attempt has the appearance of genuine communication but contains genuine harm.

### DDoS (Distributed Denial of Service) Attack

In a DDoS attack, the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the internet. DDoS is typically accomplished by flooding the targeted machine from many different sources with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

### APT (Advanced Persistent Threats)

APT is an undercover, ongoing computer network attack in which a person or group gains unauthorized access to a network with the goal of going undetected for the longest period possible in order to spy, place custom malicious code on multiple computers for specific tasks,  gather information, and access sensitive, classified information. Traditionally, APT was associated with governments, but over the last few years there have been multiple examples of non-state sponsored large groups conducting large-scale targeted intrusions for other reasons.

Cyber threats continue to become more and more sophisticated. Every employee of an organization must be educated and aware of the specific vulnerabilities and ongoing cyber threats to your network’s security. By ensuring that all the hardware and software on your network stays up to date and encouraging a culture of cyber security in the workplace, organizations can stay vigilant in the fight against threats.

What are the recent security breaches? List and give examples with dates

### CAM4 data breach

[[](https://www.upguard.com/security-report/cam4)](https://www.upguard.com/security-report/cam4" \t "_blank)

**Date:** March 2020

**Impact:** 10.88 billion records.

Adult video streaming website [CAM4](https://www.upguard.com/security-report/cam4) has had its Elasticsearch server breached exposing over 10 billion records.

The breached records included the following [sensitive information](https://www.upguard.com/blog/sensitive-data):

* Full names
* Email addresses
* Sexual orientation
* Chat transcripts
* Email correspondence transcripts
* Password hashes
* IP addresses
* Payment logs

Many of the exposed email addresses are linked to cloud storage services. If hackers were to launch successful [phishing attacks](http://www.upguard.com/blog/types-of-phishing-attacks) on these users, they could gain deeper access to personal photos and business information.

Due to the licentious connection of the breached database, compromised users could fall victim to blackmail and defamation attempts for many years to come.

### Yahoo data breach 2017

[[](https://www.upguard.com/security-report/yahoo)](https://www.upguard.com/security-report/yahoo" \t "_blank)

**Date:** October 2017

**Impact:** 3 billion accounts

[Yahoo](https://www.upguard.com/security-report/yahoo)disclosed that a breach in August 2013 by a group of hackers had compromised 1 billion accounts. In this instance, security questions and answers were also compromised, increasing the risk of [identity theft](http://www.upguard.com/blog/identity-theft). The breach was first reported by Yahoo while in negotiations to sell itself to Verizon, on December 14, 2016. Yahoo forced all affected users to change passwords and to reenter any unencrypted security questions and answers to re-encrypt them.

However, by October of 2017, Yahoo changed the estimate to 3 billion user accounts. An investigation revealed that users' passwords in clear text, payment card data and bank information were not stolen. Nonetheless, this remains one of the largest data breaches of this type in history.

### Aadhaar data breach

[[](https://www.upguard.com/security-report/uidau)](https://www.upguard.com/security-report/uidau" \t "_blank)

**Date:** March 2018

**Impact:** 1.1 billion people

In March of 2018, it became public that the personal information of more than a billion Indian citizens stored in the world’s largest [biometric](https://www.upguard.com/blog/biometrics) database could be bought online.

This massive data breach was the result of a [data leak](https://www.upguard.com/blog/data-leak) on a system run by a state-owned utility company. The breach allowed access to private information of [Aadhaar](https://www.upguard.com/security-report/uidau) holders, exposing their names, their unique 12-digit identity numbers, and their bank details.

The type of information exposed included the photographs, thumbprints, retina scans and other identifying details of nearly every Indian citizen.

### First American Financial Corp. data breach

[[](https://www.upguard.com/security-report/firstam)](https://www.upguard.com/security-report/firstam" \t "_blank)

**Date:**May 2019

**Impact:**885 million users

In May 2019, [First American Financial Corporation](https://www.upguard.com/security-report/firstam) reportedly leaked 885 million users' sensitive records that date back more than 16 years, including bank account records, social security numbers, wire transactions, and other mortgage paperwork.

### Verifications.io data breach



**Date:** February 2019

**Impact:**763 million users

In February 2019, email address validation service verifications.io exposed 763 million unique email addresses in a MongoDB instance that was left publicly facing with no password. Many records also included names, phone numbers, IP addresses, dates of birth and genders.

‍

### LinkedIn data breach 2021

[[](https://www.upguard.com/security-report/linkedin)](https://www.upguard.com/security-report/linkedin" \t "_blank)

**Date:** June 2021

**Impact:**700 million users

Data associated with 700 million LinkedIn users was posted for sale in a Dark Web forum on June 2021. This exposure impacted 92% of the total LinkedIn user base of 756 million users.

The data was dumped in two waves, initially exposing 500 million users, and then a second dump where the hacker "God User" boasted that they were selling a database of 700 million LinkedIn.



Preview of leaked data - Source: 9to5mac.com

The hackers published a sample containing 1 million records to confirm the legitimacy of the breach. The data included the following:

* Email addresses
* Full names
* Phone numbers
* Geolocation records
* LinkedIn username and profile URLs
* Personal and professional experience
* Genders
* Other social media accounts and details

The hacker scraped the data by exploiting LinkedIn's API.

LinkedIn claims that, because personal information was not compromised, this event was not a 'data breach but, rather, just a violation of their terms of service through prohibited data scraping.

Discuss the consequences of this breach

### Reputational damage

Loss of customer and stakeholder trust can be the most harmful impact of cybercrime, since the overwhelming majority of people would not do business with a company that had been breached, especially if it failed to protect its customers' data. This can translate directly into a loss of business, as well as devaluation of the brand you've worked so hard to build. Although on a case-by-case basis it’s difficult to quantify the erosion of reputation due to a data breach, according to one industry insider speaking with ITPro, “we see a 60% failure rate among SMBs after a company discloses a breach within 6-12 months, partly due to confidence issues and partly due to recovery challenges.” (7)

### Theft

While a cyber-raid on a big-name bank may net the attacker a sizeable haul, smaller businesses' defences are typically less sophisticated and easier to penetrate, making them a softer target. Cyber-enabled fraud leads to monetary losses, but stolen data can be worth far more to hackers, especially when sold on the Dark Web. A report by The Digital Shadows Photon Research team found that the average price for commercially traded logins on the Dark Web was a ‘modest’ $15.43; when it came to domain administrator accounts that give access to internal business networks, (typically sold by auction because of their value to hackers), the price spiked to an average of $3,139 and, in select cases, reached an eye-popping price of $120,000. (8) Intellectual property theft may be equally damaging, with companies losing years of effort and R&D investment in trade secrets or copyrighted material – and their competitive advantage.

### Financial losses

Cybercrime costs small businesses disproportionately more than big businesses when adjusted for organisational size. For a large corporation, the financial impact of a breach may run into the millions, but at their scale, the monetary implications are barely a blip on the radar. According to the latest data breach report by IBM and the Ponemon Institute, the average cost of a data breach in 2021 is $4.24M, a 10% rise from its average cost of $3.86M in 2019. Even more troubling is the report’s finding that the longer a breach remains undetected, the higher its financial impact. For example, data breaches that were identified and contained within 200 days had an average cost of $3.61 million. But breaches that took more than 200 days to identify ad contain had an average cost of $4.87 million ― a difference of $1.26 million. (9)

### Fines

As if direct financial losses weren't punishment enough, there is the prospect of monetary penalties for businesses that fail to comply with data protection legislation. In May 2018, the General Data Protection Regulation or GDPR went into effect in the EU. The enforcement powers associated with the law are significant. Fines for violations can reach up to 20 million Euros or 4% of a firm’s global annual revenue, per violation, whichever is larger. In 2020 European data agencies issued $193 million (€159 million) in fines in 2020 for violations of the General Data Protection Regulation where the single highest penalty imposed was a $57 million fine French authorities issued to Google. (10)

While in the US there is no true counterpart to GDPR, three states — California, Colorado and Virginia ― have enacted comprehensive consumer data privacy laws. The three laws have several provisions in common, such as the right to access and delete personal information and to opt-out of the sale of personal information, among others. (11)

### Below-the-surface costs

In addition to the economic costs of incident response, there are several intangible costs that can continue to blight a business long after the event itself. The impact of operational disruption tends to be woefully underestimated – especially among firms that have little in the way of formal business resilience and continuity strategies – and small organisations that already struggle to manage cash flow may face crippling rises in insurance premiums or see an increased cost to raise debt.

Cyber security and cyber incident recovery isn't an IT problem. Instead, it's a business imperative. Adopting a comprehensive security strategy today can help you avoid having to shut up shop if hackers strike tomorrow.

Suggest solutions to organizations

The list of [things organizations can do](https://www.techtarget.com/searchsecurity/feature/Ten-ways-to-prevent-insider-security-threats) to minimize the [risks associated with insider threats](https://www.techtarget.com/searchsecurity/tip/Insider-threat-protection-Strategies-for-enterprises) include the following:

* limit employees' access to only the specific resources they need to do their jobs;
* train new employees and contractors on security awareness before allowing them to access the network. Incorporate information about unintentional and malicious insider threat awareness into regular security training;
* set up contractors and other freelancers with temporary accounts that expire on specific dates, such as the dates their contracts end;
* implement two-factor authentication, which requires each user to provide a second piece of identifying information in addition to a password; and
* install employee monitoring software to help reduce the risk of data breaches and the theft of intellectual property by identifying careless, disgruntled or malicious insiders.

# P2 Describe at least 3 organisational security procedures.

Credit Card Processing Procedures

* **Cardholder**

The cardholder (the buyer) presents a credit or debit card to the merchant for payment. This can happen directly, as when a card is swiped, tapped, chipped or inputted manually in a traditional brick-and-mortar store, or it can take place by phone or online.

* **Merchant**

The merchant (who the buyer is trying to pay) sends a request through a payment portal for the cardholder’s issuing bank to approve or decline the transaction. However, the authorization request doesn’t go directly to the cardholder’s bank. Instead, the merchant sends the required information through the merchant’s payment processor. (This is who a business hires to help them accept credit cards.)

* **Payment Processor**

The payment processor receives the merchant’s authorization request and transaction information and forwards it to the appropriate credit card network (Visa, MasterCard, American Express, or Discover).

* **Credit Card Network**

The credit card network receives the card information from the payment processor and forwards it to the cardholder’s issuing bank (in the case of Visa and Mastercard) for authentication and approval. This is the sense in which the credit card network is a “network”: it facilitates the transaction by acting as a highway along which transaction data travels back and forth between the payment processor and the issuing bank. American Express and Discover, however, are both card issuers and card networks.

* **Issuing Bank**

The issuing bank checks the card and transaction details against the cardholder’s line of credit (if the payment is made with a credit card) or the cardholder’s account balance (if a debit card), and then then approves or declines the transaction. The issuer then sends its response back to the credit card network. If it approves the transaction, the issuer also places a temporary hold on the cardholder’s account for the amount of the transaction.

* **Credit Card Network**

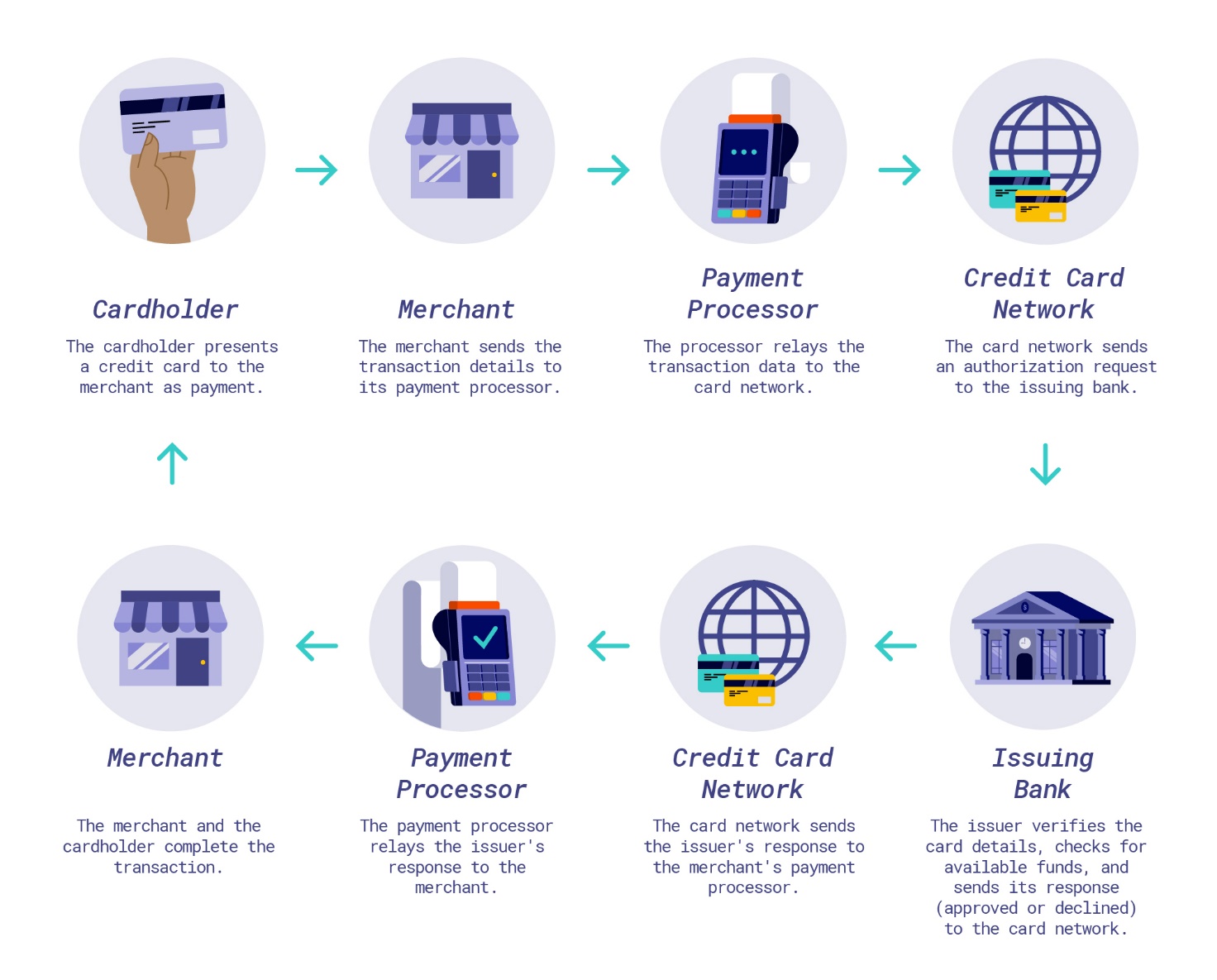
The credit card network sends the issuer’s response to the payment processor.

* **Payment Processor**

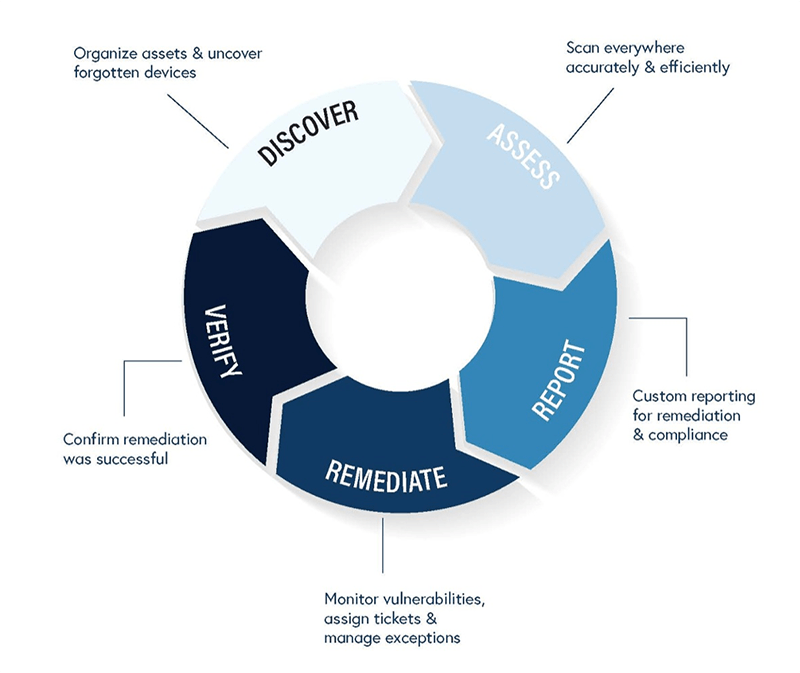
The payment processor transfers the issuer’s response to the merchant’s payment portal.

* **Back to Merchant**

The merchant receives the issuer’s response (approved or declined) and issues a receipt to the cardholder—which completes the transaction.



Vulnerability Management Procedure



**Stage 1: Discover**

The initial stage of the vulnerability management process is all about preparing for the vulnerability scans and tests and making sure your bases are covered. This means organizing all your company assets and uncovering any forgotten devices.

Compile all of the assets you need to test, determine their importance and who can access them (whether just administrators or your whole team). Work to maintain a continuously updated inventory so you can provide a map of the vulnerabilities throughout your network.

**Stage 2: Assess**

Once you’ve compiled all of your devices and inventory, the next stage involves the tests to make sure every device is scanned, both accurately and efficiently.

It’s not just about knowing the vulnerabilities, but gaining timely, efficient access to the information. If you aren’t receiving the data from a credible source, you might be wasting your time on false positives.

Once you’re aware of the potential risks on your devices, the next step is to prioritize those vulnerabilities. With the large number of vulnerabilities disclosed every day, it can seem impossible to manage them all, making it all the more significant to prioritize the biggest risks and resolve those first.

**Stage 3: Report**

All this data is then compiled into a custom report, giving details on the vulnerabilities and how to prioritize them. These reports will include recommendations as well as the best plan to triage the risks quickly and seamlessly.

It should include the actions to take and give step-by-step instructions to fix the problem. The purpose of the report is to significantly decrease the security risk that these vulnerabilities present in a practical way.

**Stage 4: Remediate**

In the stage of remediation, the goal is to monitor vulnerabilities, assign tickets, and manage exceptions.

As vulnerabilities are detected and reported, the next step in the vulnerability management process is to correct, monitor, or remove those vulnerabilities. This can be accomplished through the necessary updates and patches or workarounds to avoid the threat.

This stage is then repeated as new vulnerabilities are discovered. The network and its devices need to be continuously monitored to detect and find new vulnerabilities that might lead to potential, future threats.

**Stage 5: Verify**

The final step is to verify the success of the entire process. This step not only helps you see that the mitigation was successful but also maintains transparency and accountability across the company. The whole goal is to reduce the attack surface of a company, findings ways to minimize the threat of an attack by decreasing vulnerabilities.

Patch Management Process



1. **First, make a thorough inventory of the devices, services, and dependencies creating your IT infrastructure.**

This inventory should include what operating systems you’re using and which versions, and native and third-party applications. You should also be aware of what security systems you have in place, such as firewalls and anti-malware programs, including their configuration and latest version. When you have a clear inventory of what’s in your IT environment, you can make sure your patch management approaches are covering everything needing to be protected.

1. **Categorize your systems.**

To apply effective patch management processes, you need to have performed a clear risk assessment to ensure the highest-risk or most sensitive parts of your infrastructure are patched first. Having a more refined policy instead of a one-size-fits-all approach means you won’t be applying low-priority patches during the middle of the work day or failing to apply a critical patch when it’s necessary.

1. **It’s essential any patches be applied as soon as practically possible.**

The exact time frame will vary depending on how critical the application or service is, how severe the vulnerability is, and how much time it takes to test and deploy the patch itself. In all cases, patches to your operating system should be deployed immediately when they’re released, as operating system vulnerabilities can have serious and wide-reaching effects.

1. **All patches should be deployed to a test environment before you deploy them to the entire system.**

It’s possible to roll back patch deployments, but in the meantime a bad patch can break other parts of your system or even expose new vulnerabilities.

1. **For non-critical patches, a regular timeline should be established in which the patches are deployed, to minimize disruption to the business.**

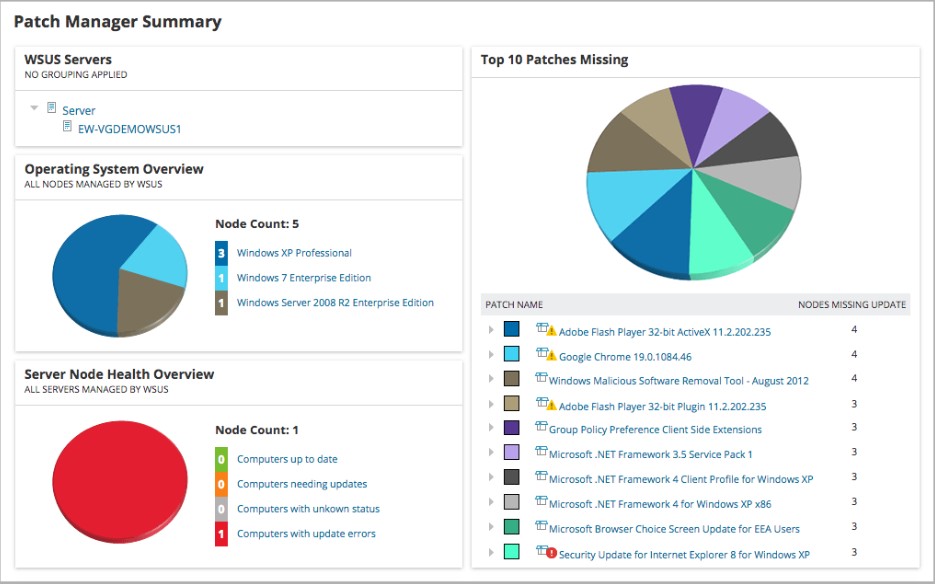
When a patch is deployed, this can slow down your business and network performance, so maintenance is best performed with automated systems during the lunch hour or overnight. Make sure you have an alerting system set up for patches deployed when you aren’t there, so if any part of the patch fails or any issue arises, you’ll be notified.

1. **Regularly scan and audit your systems for any vulnerabilities missed the first time around.**

The longer these security holes stay open, the more likely it is you’ll be the subject of an attack. Patch management should be a continuous process with regular and ongoing scanning.

1. **Use an automated tool or piece of software for the patch management process.**

Using software to manage and maintain your patches and updates can take a huge workload off your shoulders, and in many cases will be much more accurate and effective than trying to do things manually. My top choice of patch management tool is [SolarWinds Patch Manager](https://www.solarwinds.com/patch-manager/use-cases/computer-inventory-software?CMP=ORG-BLG-DNS-X_WW_X_NP_X_X_EN_X_X-PM-20210604_8PatchManagemen_X_X_VidNo_X-X).



Patch Manager has several features making it an excellent choice for maintaining your patch management processes. First, it **works with Microsoft WSUS and SCCM**, as well as third-party applications, to enhance your Windows patching tools. Second, it includes pre-built and tested **patches for third-party applications**, so you don’t need to spend as much time creating and testing these patches yourself. The Patch Manager dashboard is also excellent, as it displays the patch status of your entire environment. You can also see the top 10 missing patches, so you can focus on patching the most vulnerable parts of your software first.

1. **Undertake reporting and regular reviews to ensure your patch management processes and software are all working as expected.**

SolarWinds Patch Manager includes a utility capable of creating reports from your patch history, whether to demonstrate compliance with any legal or regulatory standards, or simply to show auditors or internal management you’re on top of security measures.

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

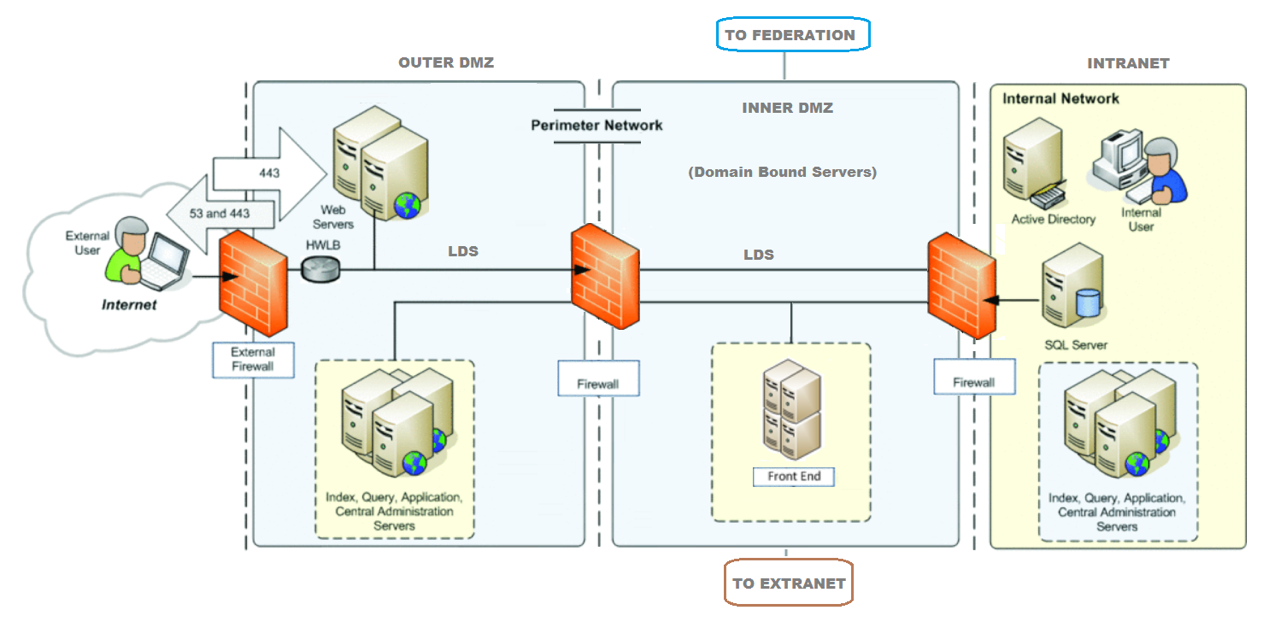
Discuss briefly firewalls and policies, their usage and advantages in a network

* + 1. Definition

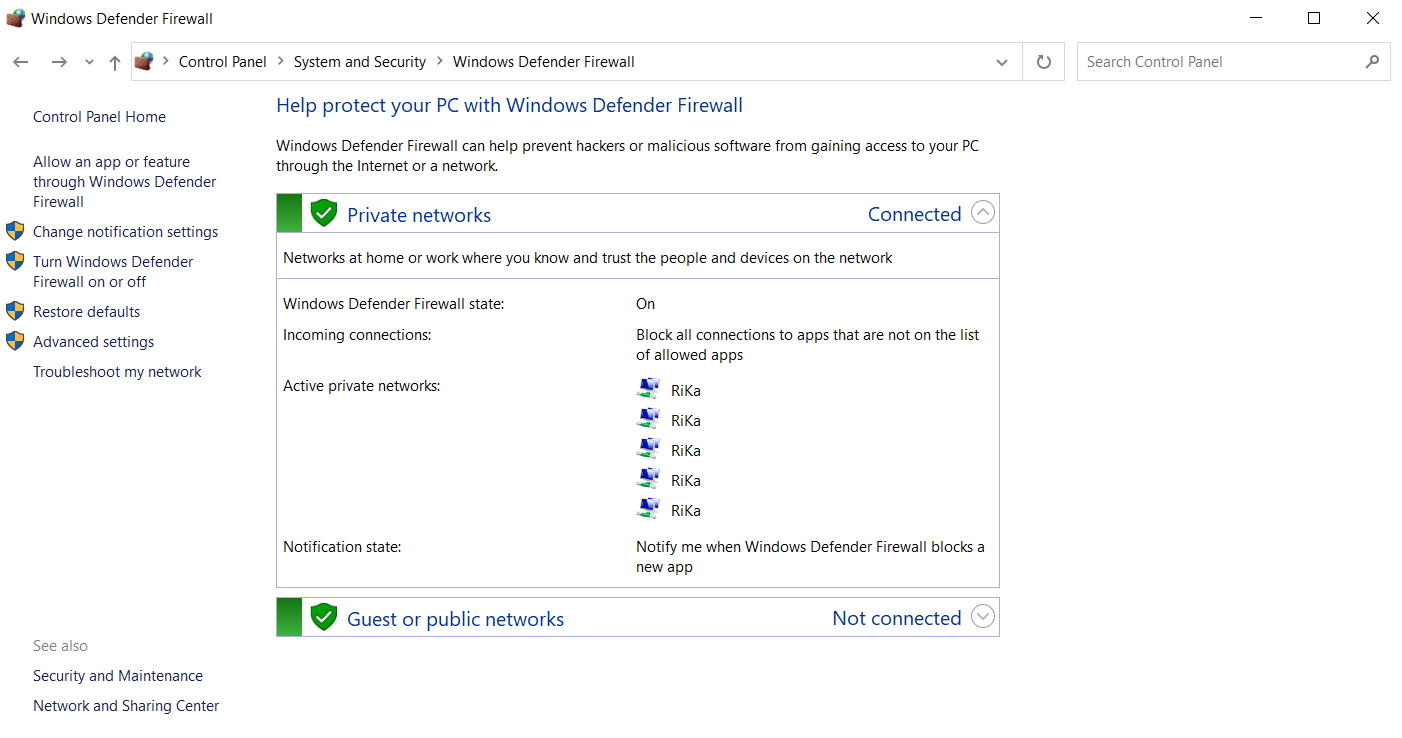
A firewall is a security device — computer hardware or software — that can help protect your network by filtering traffic and blocking outsiders from gaining unauthorized access to the private data on your computer.

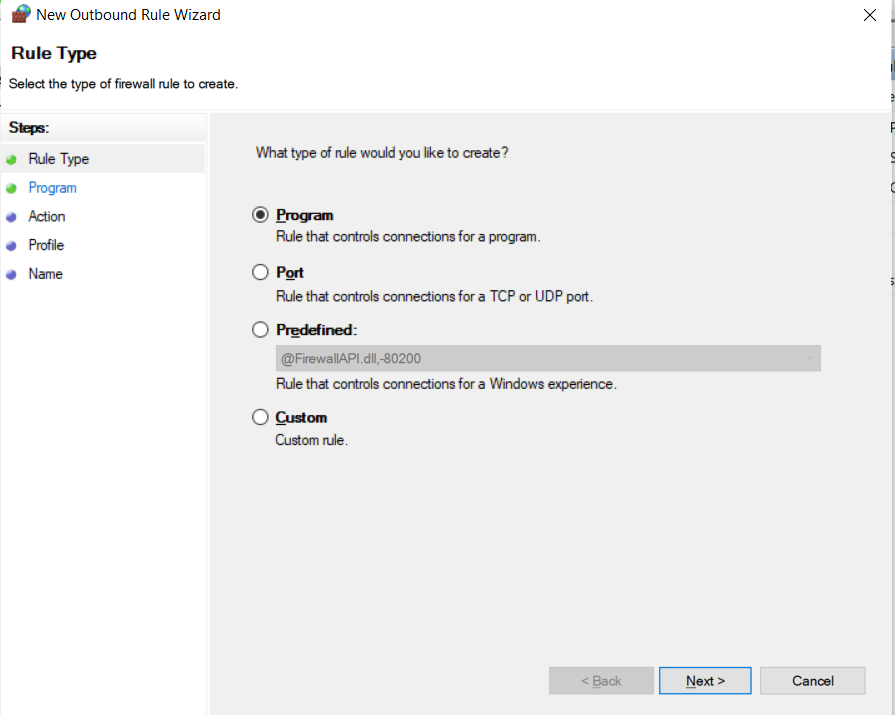
Not only does a firewall block unwanted traffic, it can also help block [malicious software](https://us.norton.com/internetsecurity-malware-how-can-i-tell-if-i-have-malware-and-what-can-i-do-about-it.html) from infecting your computer.

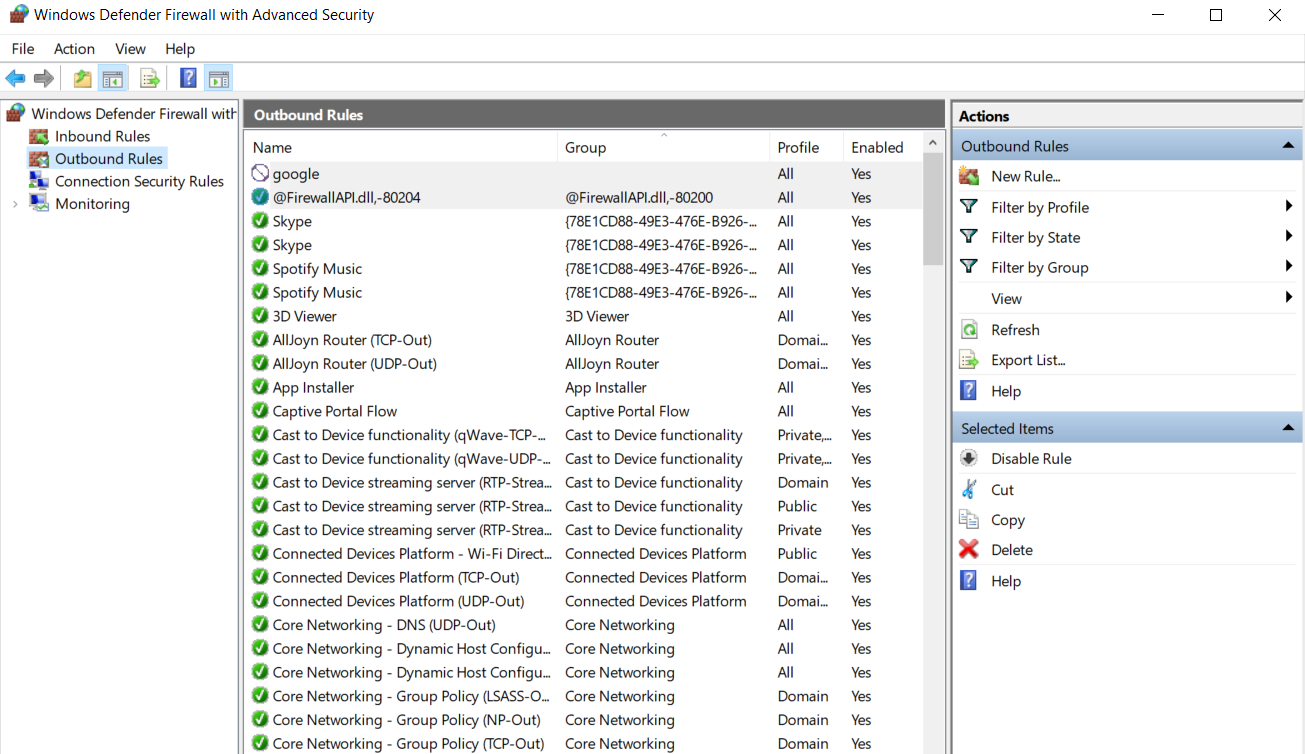
* + 1. Usage
* Constantly update your firewalls as soon as possible: Firmware patches keep your firewall updated against any newly discovered vulnerabilities.
* Use antivirus protection: In addition to firewalls, you need to use antivirus software to protect your system from viruses and other infections.
* Limit accessible ports and host: Limit inbound and outbound connections to a strict whitelist of trusted IP addresses.
* Have active network: To avoid downtime, have active network redundancies. Data backups for network hosts and other critical systems can help you avoid data loss and lost productivity in the case of a disaster.
  + 1. Advantages
* Firewalls play an important role in the companies for security management. Below are some of the important advantages of using firewalls.
* It provides enhanced security and privacy from vulnerable services. It prevents unauthorized users from accessing a private network that is connected to the internet.
* Firewalls provide faster response time and can handle more traffic loads.
* A firewall allows you to easily handle and update the security protocols from a single authorized device.
* It safeguards your network from phishing attacks.
  + 1. Diagrams the firewall works

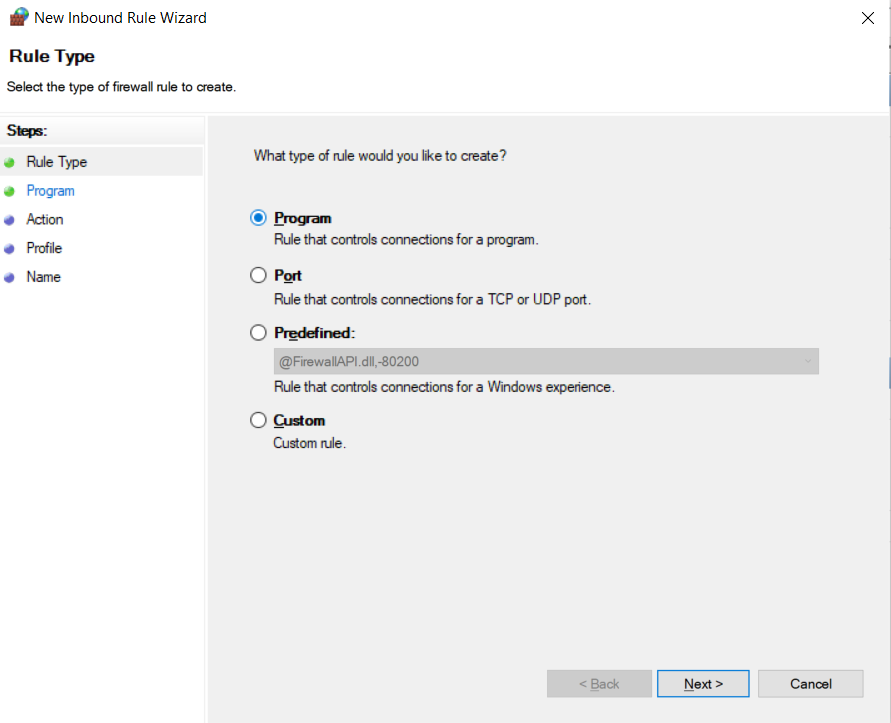


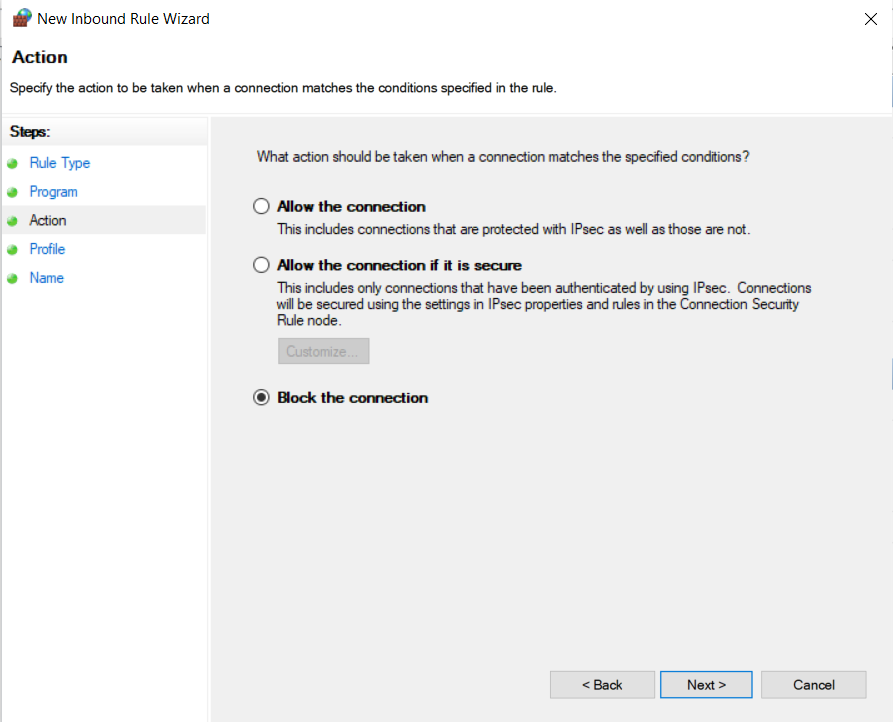
* + 1. Implement

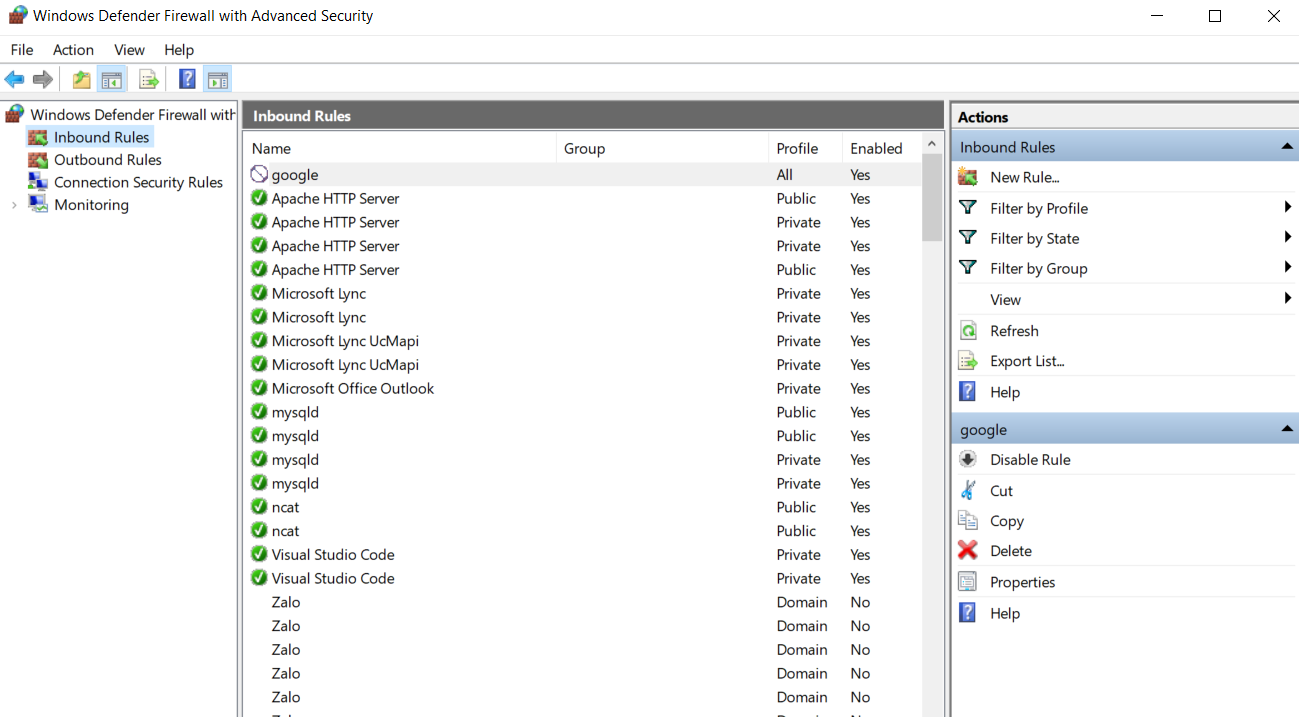


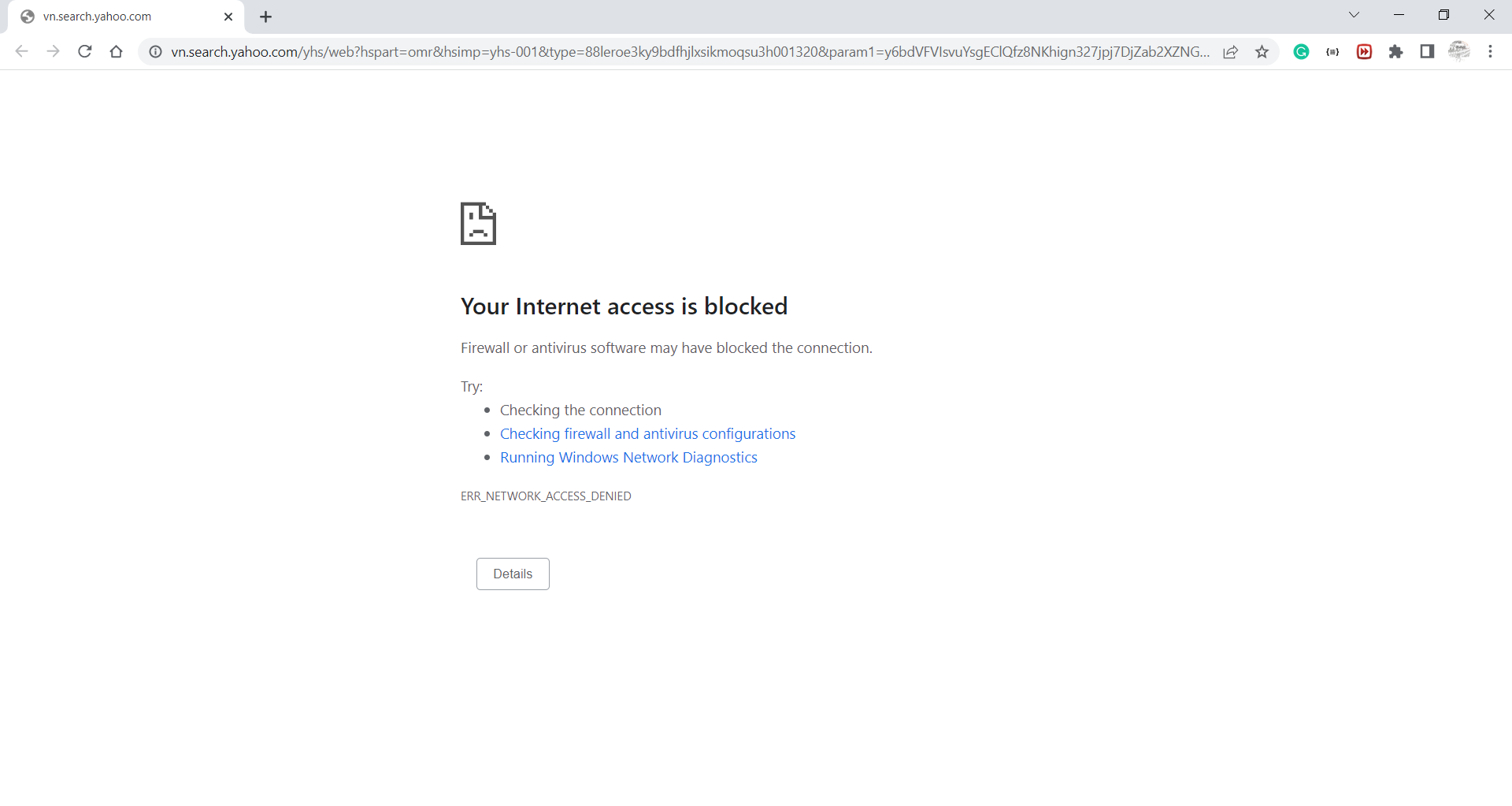












* 1. How does a firewall provide security to a network?

Network firewalls are security devices used to stop or mitigate unauthorized access to private networks connected to the Internet, especially intranets. The only traffic allowed on the network is defined via firewall policies – any other traffic attempting to access the network is blocked. Network firewalls sit at the front line of a network, acting as a communications liaison between internal and external devices.

A network firewall can be configured so that any data entering or exiting the network has to pass through it – it accomplishes this by examining each incoming message and rejecting those that fail to meet the defined security criteria. When properly configured, a firewall allows users to access any of the resources they need while simultaneously keeping out unwanted users, hackers, viruses, worms or other malicious programs trying to access the protected network.

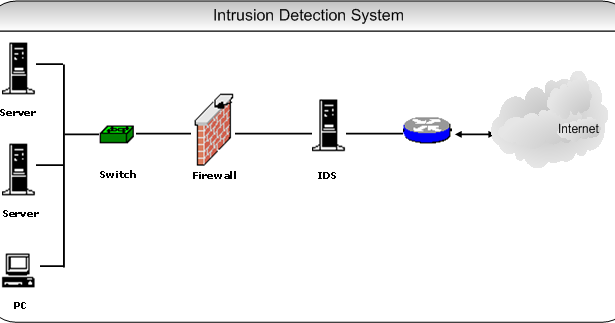
* 1. IDS
     1. Definition

An IDS is a passive monitoring device that detects potential threats and generates alerts, enabling security operations center ([SOC](https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/)) analysts or incident responders to investigate and respond to the potential incident. An IDS provides no actual protection to the endpoint or network. A firewall, on the other hand, is designed to act as a protective system. It performs analysis of the metadata of network packets and allows or blocks traffic based upon predefined rules. This creates a boundary over which certain types of traffic or protocols cannot pass.

* + 1. Usage

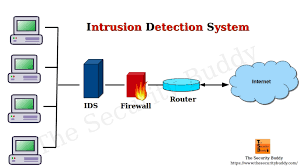
When placed at a strategic point or points within a network to monitor traffic to and from all devices on the network, an IDS will perform an analysis of passing traffic, and match the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.

* + 1. Diagram IDS work



When installed between the router and the firewall, the IDS is convenient for monitoring traffic in both directions. Although under great pressure in terms of traffic, in return, the IDS at the center of the router and firewall helps the system to monitor well and detect problems in a timely manner.

However, during the installation process, you need to choose a device with a high load capacity. If installed with the wrong type of equipment, they will not withstand extreme flow pressure.



In addition to the location between the router and the firewall, the IDS can also be located behind the firewall. This is the right position to monitor all traffic behind. For example, data fluctuates in the LAN, data moves from the LAN into or out of the DMZ.

* 1. The potential impact (Threat-Risk) of a firewall and IDS if they are incorrectly configured in a network
     1. Firewall
* **Compliance violations:** A properly configured firewall is necessary for businesses to comply with PCI standards or regulations in retail, finance or healthcare. Noncompliance leads to fines.
* **Breach avenues:** A firewall misconfiguration that results in unintended access can open the door to breaches, data loss and stolen or ransomed IP.
* **Unplanned outages:** A misconfiguration could prevent a customer from engaging with a business, and that downtime leads to lost revenues. For example, large e-commerce businesses could lose thousands or even millions of dollars until the error is corrected.

2. IDS

The configuration enables the IDS to detect a greater number of possible attacks, it also can leave the system open to a greater number of false positives.

False positives are the bane of the IDS world. There are two main errors you’ll encounter when working with IDSs: false positives and false negatives. A false positive occurs when the IDS reports a potential attack but there is actually no attack in progress. A false negative is when the IDS fails to report an attack when an attack is in progress. False negatives indicate a failure in the IDS itself, while the false positive shows the IDS is working exactly as it is configured to work.

The problem with false positives is that IDS admins begin receiving hundreds or thousands of alerts per day, overwhelming them and leading them to ignore it when the IDS reports a real attack because it has “cried wolf” so many times in the past. A good example of how this happens is when you’ve configured your IDS to liberally interpret port scans as attacks. Ports scans are going on all the time, and

most of them don’t result in actual intrusions. If you configure your IDS t report every port scan, you’ll probably soon find that you’re ignoring not only the port scan alerts, but any other alert that the IDS sends you. That’s human nature–but it can have disastrous results.

# Task 4 - Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security (P4)

* 1. Define and discuss with the aid of diagram DMZ. Focus on its usage and security function as advantage
     1. Definition

A **DMZ Network** is a perimeter network that protects and adds an extra layer of security to an organization’s internal local-area network from untrusted traffic. A common DMZ is a subnetwork that sits between the public internet and private networks.

The end goal of a DMZ is to allow an organization to access untrusted networks, such as the internet, while ensuring its private network or LAN remains secure. Organizations typically store external-facing services and resources, as well as servers for the Domain Name System (DNS), File Transfer Protocol (FTP), mail, proxy, Voice over Internet Protocol (VoIP), and web servers, in the DMZ.

These servers and resources are isolated and given limited access to the LAN to ensure they can be accessed via the internet but the internal LAN cannot. As a result, a DMZ approach makes it more difficult for a hacker to gain direct access to an organization’s data and internal servers via the internet.

* + 1. Usage

DMZ networks have been central to securing global enterprise networks since the introduction of firewalls. They protect organizations’ sensitive data, systems, and resources by keeping internal networks separate from systems that could be targeted by attackers. DMZs also enable organizations to control and reduce access levels to sensitive systems.

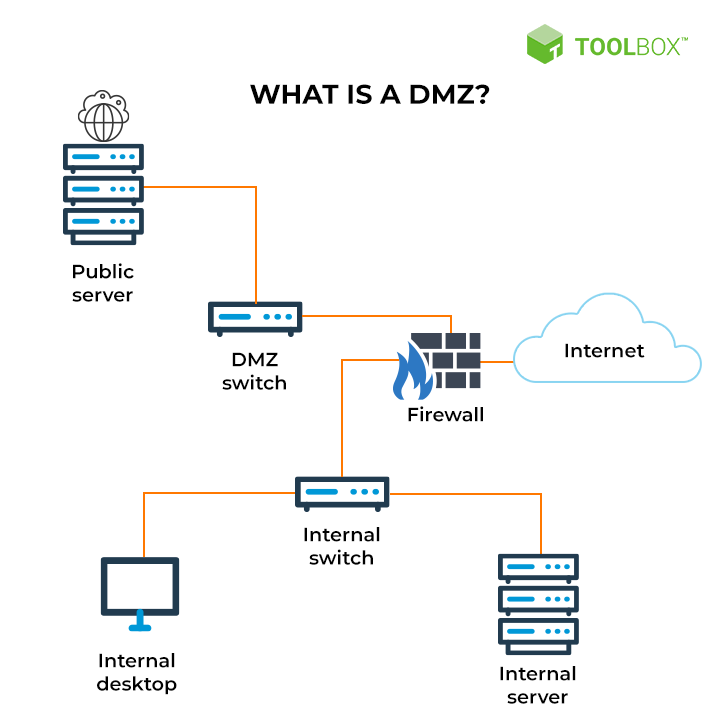
Enterprises are increasingly using containers and virtual machines (VMs) to isolate their networks or particular applications from the rest of their systems. The growth of the cloud means many businesses no longer need internal web servers. They have also migrated much of their external infrastructure to the cloud by using Software-as-a-Service (SaaS) applications.

Further, DMZs are proving useful in countering the security risks posed by new technology such as Internet-of-Things (IoT) devices and operational technology (OT) systems, which make production and manufacturing smarter but create a vast threat surface. That is because OT equipment has not been designed to cope with or recover from cyberattacks the way that IoT digital devices have been, which presents a substantial risk to organizations’ critical data and resources. A DMZ provides network segmentation to lower the risk of an attack that can cause damage to industrial infrastructure.

* + 1. Benefits of using a DMZ

The main benefit of a DMZ is to provide an internal network with an advanced security layer by restricting access to sensitive data and servers. A DMZ enables website visitors to obtain certain services while providing a buffer between them and the organization’s private network. As a result, the DMZ also offers additional security benefits, such as:

* Enabling access control: Businesses can provide users with access to services outside the perimeters of their network through the public internet. The DMZ enables access to these services while implementing network segmentation to make it more difficult for an unauthorized user to reach the private network. A DMZ may also include a proxy server, which centralizes internal traffic flow and simplifies the monitoring and recording of that traffic.
* Preventing network reconnaissance: By providing a buffer between the internet and a private network, a DMZ prevents attackers from performing the reconnaissance work they carry out the search for potential targets. 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. Even if a DMZ system gets compromised, the internal firewall separates the private network from the DMZ to keep it secure and make external reconnaissance difficult.
* Blocking Internet Protocol (IP) spoofing: Attackers attempt to find ways to gain access to systems by spoofing an IP address and impersonating an approved device signed in to a network. 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.
  + 1. Diagram DMZ



* 1. Define and discuss with the aid of diagram static IP. Focus on its usage and security function as advantage
     1. Definition

A static IP address is an IP address that was manually configured for a device instead of one that was assigned by a [DHCP](https://www.lifewire.com/what-is-dhcp-2625848) server. It's called static because it doesn't change vs. a [dynamic IP address](https://www.lifewire.com/what-is-a-dynamic-ip-address-2625857), which does change.

* + 1. Usage

a static IP address is useful if you host a website from home, have a file server in your network, use networked printers, forward ports to a specific device, run a print server, or use a remote access program. Because a static IP address never changes, other devices always know exactly how to contact a device that uses one.

Static IP addresses are also useful for when the device's domain name is inaccessible.

With remote access applications such as Windows Remote Desktop, using a static IP address means you can always access that computer with the same address.

* + 1. Advantage
* **Running servers**

A big advantage of utilizing a static IP address is that it can host servers, which other computers can access using their internet connection. Because static IP addresses do not change, they can be located from just about any area in the world. Different devices and operating systems can also gain remote access to networks using the IP address.

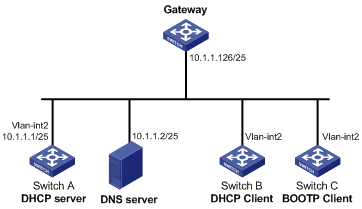
* **Stability**

These types of IP addresses also offer more stability, as they do not change like dynamic IP addresses. Dynamic IPs change often, sometimes every couple of hours, which can mean losses in connection while using the internet. You may find yourself having to reconnect while working on tasks and facing difficulties when reconnecting.

* **Faster download/upload speeds**

Depending on your network, the speed of a static IP can be drastically faster than a device with a dynamic IP. DSL connections may not produce noticeable differences in speed, but broadband users with [high speed connections](https://www.techguide.com.au/news/10-things-affecting-internet-speed/) may notice an increase in speed that is over 1 megabit. If you tend to download or upload a lot of files, documents, and data, you may want to compare static and dynamic speeds.

* + 1. Diagram static IP



* 1. Define and discuss with the aid of diagram NAT. Focus on its usage and security function as advantage
     1. Definition

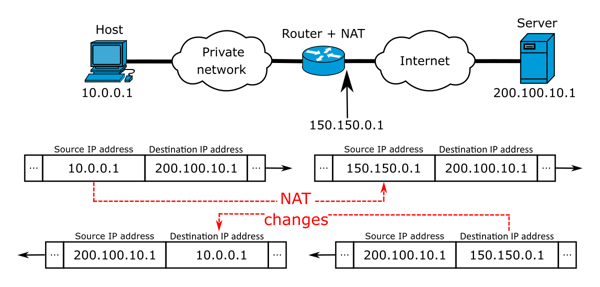
NAT is the process of reassigning the single IP address space into a further one by altering the network address data in the IP header of the data packet while they are traveling through a network towards the destination node.

Generally, NAT works on a router or gateway and interconnects two networks with each other by translating the private addresses into the registered addresses before the data being transmitted to another network.

NAT is having the potential to broadcast only one IP address to the public network on behalf of the entire internal network. This provisions the feature of security by efficiently hiding the overall IP address of the private network behind that solo address.

Thus NAT tenders the double feature of address translation and security for networking systems.

* + 1. Usage



In the above diagram, a host with a private IP address 10.0.0.1 wants to communicate over the internet with a server with the IP address 200.100. 10.1 , possibly to access some documents.

This would not be possible because private IP addresses cannot be used on the internet. But the ISPs now come in, using the NAT technique to map the private IP 10.0.0.1 to the public IP 150.150.0.1, enabling it to communicate with the server on the internet. This is possible because NAT masquerades private IP addresses with public ones.

This is achieved by using a routing table that holds a temporary record of all available, registered, public IP addresses that they have. It maps the public IPs to each private IP coming from clients who wish to access the internet.

A situation can arise whereby the IP addresses available to the service provider (using the NAT router) are grossly insufficient to accommodate the number of users that wish to access the internet through them. In this situation, they will employ the other technique we mentioned earlier, PAT.

* + 1. Advantage
* NAT conserves legally registered IP addresses.
* It provides privacy as the device’s IP address, sending and receiving the traffic, will be hidden.
* Eliminates address renumbering when a network evolves.

4. Diagram NAT

NAT (Network Address Translation) là gì? Những điều cần biết về NAT

REFERENCE

Sungardas.com Available at: <https://www.sungardas.com/en-gb/blog/the-consequences-of-a-cyber-security-breach/> [Accessed 20 Aug. 2022]

Cloudmask.com Available at: <https://www.cloudmask.com/blog/data-breaches-threats-and-consequences> [Accessed 20 Aug. 2022]

Upguard.com Available at: <https://www.upguard.com/blog/biggest-data-breaches> [Accessed 20 Aug. 2022]

Rsisecurity.com Available at: <https://blog.rsisecurity.com/types-of-security-threats-to-organizations/> [Accessed 20 Aug. 2022]

Celerium.com Available at: <https://www.celerium.com/blog/7-network-security-threats-to-your-organization-today> [Accessed 20 Aug. 2022]

Cryptosmith.com Available at: <https://cryptosmith.com/2016/01/31/threat-agents-and-levels-of-motivation/> [Accessed 20 Aug. 2022]

Techtarget.com Available at: <https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams> [Accessed 20 Aug. 2022]

Debricked.com Available at: <https://debricked.com/blog/what-is-security-threat/> [Accessed 21 Aug. 2022]

Nstec.com Available at: <https://www.nstec.com/a-firewall-misconfiguration-is-a-threat> [Accessed 21 Aug. 2022]

Fortinet.com Available at: <https://www.fortinet.com/resources/cyberglossary/what-is-dmz> [Accessed 21 Aug. 2022]