UNIVERSITY of GREENWICH

Alliance with FPT Education

BTEC

# ASSIGNMENT FRONT SHEET

| | | | |
|---|---|---|---|
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number and title** | **Unit 5: Security** | | |
| **Submission date** | 12/10/2020 | **Date Received 1st submission** | |
| **Re-submission Date** | | **Date Received 2nd submission** | |
| **Student Name** | LE CHI KHAI | **Student ID** | GCC19095 |
| **Class** | GCC0801 | **Assessor name** | LE HUYNH QUOC BAO |
| **Student declaration**<br>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: | | |

# Assessment Brief

| | | | |
|---|---|---|---|
| **Qualification** | **BTEC Level 5 HND Diploma in Computing** | | |
| **Unit number** | Unit 5: Security | | |
| **Assignment title** | Security Presentation | | |
| **Academic Year** | 2020 | | |
| **Unit Tutor** | | | |
| **Issue date** | | **Submission date** | |
| **IV name and date** | Khoa Canh Nguyen, Michael Omar, Nhung 9th/01/2020 | | |

| **Submission Format** |
|---|
| The submission is in the form of two documents/files:<br>1. A ten-minute Microsoft® PowerPoint® style presentation to be presented to your colleagues. The presentation can include links to performance data with additional **speaker notes** and a **bibliography using the Harvard referencing system.** The presentation slides for the findings should be submitted with speaker notes as one copy.<br>2. A detailed report that provides more thorough, evaluated or critically reviewed technical information on all of the topics.<br>You are required to make use of the font **Calibri, Font size 12, Line spacing 1.5, Headings,** P**aragraphs**, S**ubsections and illustrations** as appropriate, and all work must be **supported with research and referenced** using the **Harvard referencing system.** |

## Unit Learning Outcomes

**LO1** Assess risks to IT security.

**LO2** Describe IT security solutions.

## 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**<br>**D1** Investigate how a 'trusted network' may be part of an IT security solution. |
| **P1** Identify types of security threat to organisations.<br>Give an example of a recently publicized security breach and discuss its consequences.<br>**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.<br>**P4** Show, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve Network Security. | **M2** Discuss three benefits to implement network monitoring systems with supporting reasons. | |

# Contents

# 1. The P1: Identify Types of Security Threat to Organization

The threat of information insecurity:

- The risk of information insecurity from the physical aspect is the risk of power failure, unsecured temperature, humidity, fire, natural disasters, damaged hardware equipment, destructive elements such as bad personnel. inside and thief outside.

- Risk of loss, damage, modification of information content: Users may accidentally reveal passwords or not operate properly, creating opportunities for bad guys to use them to steal or damage information. Hackers can use their own tools or techniques to change the content of information (files) in order to incorrectly order the information of the rightful owner.

- Risk of attack by malware: Malware attacks by many different methods to penetrate the system with different purposes such as viruses, Worm, spyware,…

- Risk of penetration from security holes: Security vulnerabilities are often caused by programming errors, bugs or software problems, located in one or more components that make up the operating system or in programs installed on the computer.

- Risk of information insecurity due to using e-mail: A targeted attack by email is an attack with a fake email like an email sent from an acquaintance, which can be attached file to make the infected with a virus.

- Risk of information insecurity during transmission: In the process of circulating and transacting information on the internet, the risk of information insecurity in the transmission process is very high because hackers block the transmission line and change or destroy the content of the information and then send it to the recipient.

*(Zucker, 2016)*

Factors causing information insecurity:

- The rather common cause of information insecurity is the lack of awareness and awareness of users of information technology equipment, arbitrary use of internet services to connect, receive and transfer documents over the network. .

- Agencies and units have not paid attention to building regulations on management of staff using telecommunications services as well as strictly managing confidential documents.

- The development or application of information security policies have not been concerned; the compliance and compliance with information security standards are not correct, creating loopholes in the information system.

- Using computers connected to the internet without safe protection solutions to compose and store information with sensitive content.

- Using software with security vulnerabilities, especially unlicensed software, while "patching" security vulnerabilities that are not given adequate attention, will create loopholes for hackers to steal. information is easy.

- Information insecurity occurs from updating malicious information on information systems ... Due to the user's subjectivity not to scan for malicious code before uploading it to the systems.

- Using transmission lines without encryption and information authentication. In addition to the attack of stealing information directly from users' servers and computers, the opponent can intercept information on transmission lines, if sensitive information is not encrypted and authenticated, completely. can be stolen.

- Loss of information security through information or data copying devices (USB, memory stick,...). This is a highly sophisticated case of information theft that users least expect even if their computer is completely independent from the internet.

- No explicit authorization: the administrator has not explicitly authorized the member. Taking advantage of this, internal employees can steal, exchange, and change company information.

- Vulnerabilities in the system: because the units do not regularly scan for vulnerabilities, assess the system's security, leading to the risk of great financial losses.

*(Zucker, 2016)*

Solutions to ensure information security:

- Preventing the risk of information insecurity in terms of physical aspects such as: UPS, temperature and humidity system installation. Always have fire extinguishing equipment, do not place chemicals near the system. Regularly back up data. Use the correct system operating policies for procedures, safety and security.

- Data backup: this is a fairly good and popular method of data protection.

- Set strong passwords: accounts on social networks, websites, and applications need strong passwords. Password should contain underscores or @, numbers, alphanumeric characters. Individuals should avoid putting in easy passwords like 123456, 123456789, iloveyou, name + date of birth,...

- Data encryption: For important and intimate information, we should encrypt it before sending it. The purpose of information encryption is to avoid hackers' eavesdropping.

- Software update: One of the best solutions to avoid loss of information is to install software. You can install antivirus software, attack warning software, system monitoring software,...

- Install anti-virus software: Installing intrusive antivirus software is also a recommended solution by experts. Note, users should scan for viruses before downloading the software to the computer. Some online tools help check online malware such as virus total, 6scan security, sitecheck.

- Use software with clear origin: Ensuring that all software and applications on your device have a clear origin will help limit the risk of information insecurity.

- Control permissions on the device: Divide permissions clearly among members and relatives on your device.

- Perform two-factor authentication for the email account

- Turn off Wi-Fi, Bluetooth, NFC connections when not in use: after entering the network, we must turn off Wifi, bluetooth, NFC connections to avoid the risk of leaking passwords, documents and personal information.

- Strengthening the capacity for members to stand out incidents of information safety and security; enhancing sharing and learning experiences to promptly prevent risks occurring.

*(Zucker, 2016)*

Some examples of public security breaches:

- Microsoft database leaked because of employee negligence:

+ Content: In late December 2019, a security researcher discovered a publicly accessible Microsoft customer support database

+ Cause of the incident: In early December 2019, Microsoft implemented a new version of the Azure security rules. Microsoft employees misconfigured those rules and caused the leak.

+ Consequences: A leaked database containing 250 million entries was accumulated over 14 years. The database includes support cases and details, customer email and IP address, customer geolocation, and notes taken by Microsoft support personnel. The database has been publicly accessible for about a month. Microsoft secured it the same day the breach was reported.

- Marriott leaked data due to a compromised third-party app:

+ Content: In January 2020, hackers misused a third-party app that Marriott used to provide services to guests. The attackers gained access to the 5.2 million Marriott guests' records.

+ Cause of the incident: Attackers compromised the credentials of two Marriott employees to log into one of the chain's third-party apps. Marriott's cybersecurity system has not noticed suspicious activity on these employees' records for two months.

+ Consequences: 5.2 million Marriott customer records were stolen. These profiles include contact information, gender, birthdays, loyalty account details and personal interests. Marriott's security team found suspicious activity and sealed off security breaches caused by insiders at the end of February 2020. Marriott is still battling a £99 milion GDPR fine (equivalent to $ 124 million) for a data breach in 2018.

- Twitter users were scammed because of employee fraud:

+ Content: By July 2020, hackers had access to 130 individual and corporate Twitter accounts with at least one million followers each. They used 45 of these accounts to promote a Bitcoin scam. The list of accounts hacked includes Barack Obama, Elon Musk, Bill Gates, Jeff Bezos, Michael Bloomberg, Apple, Uber, and other notable individuals and companies.

+ Cause of the incident: Twitter employees have fallen victim to a series of phishing attacks. Hackers gather information about company employees working from home, contact them, introduce themselves as Twitter IT administrators and request user credentials. Using these compromised accounts, the attackers then gained access to administrator tools. With these tools, they reset the accounts of popular Twitter users, change their login information and tweet phishing messages. Twitter did not notice suspicious activity in the admin tool until the phishing messages were published and press attention. Analyzing user and organization behavior and privileged access management solutions could have helped a company protect access to administrative tools and quickly detect unauthorized activity.

+ Consequences: Twitter users transferred Bitcoin equivalent of at least 180,000 USD to the scam account. Crypto exchange platform Coinbase blocked another $ 280,000 of transfers. After the incident, Twitter's share price fell 4%. The company stopped releasing its new API to update its security protocols and educate employees about social engineering attacks.

- The former Cisco employee intentionally crashes the cloud infrastructure

+ Content: A former Cisco employee had unauthorized access to the company's cloud infrastructure and deployed the malicious code that removed 456 virtual machines used for the Cisco WebEx Teams application. As a result, about 16,000 WebEx users were unable to access their accounts for two weeks.

+ Cause of the incident: Former Cisco employees used their knowledge of Cisco security mechanisms and abused their weaknesses to gain access to cloud infrastructure and deployment declare your code. Obviously, access to sensitive resources is not protected with two-factor authentication or other access management tools.

+ Consequences: Cisco has spent approximately $ 1.4 million of employee time to test their infrastructure and fix the damage. The company also has to pay a total of $ 1 million in compensation to affected users. The incident occurred in September 2018, but the case remains unsolved in court in December 2020. The attacker could face up to 5 years in prison and a $ 250,000 fine.

# 2. The P2: Organizations Security Policy

## 2.1. Policy Information Security of Celsia Organization

- Responsibilities in Information Security:  Celsia owns the information. The Company's vice-presidents are in charge of care and handling of this information. They are responsible for the custody of information generated by vicepresidencies considering its purpose and use. Vice-presidents must therefore be aware of the risks to which their information is exposed, so that they can act appropriately with their employees to decrease these risks.

- Contact with Authorities and Stakeholders: Celsia must maintain contact with authorities and stakeholders to keep up to date with regulatory changes in digital governance in Colombia and to identify trends in information security.

- Independent Revision in Information Security: Internal Auditing must implement and execute an internal information security auditing plan. This plan must be focused on revision of all security requirements (policies and procedures). The results must generate a security program that includes at least the following: Actions to be taken, schedules and responsible parties. The program must be approved by the Information Security Committee.

- Security in Access by Third Parties: The Technology Management Department must conduct a risk assessment to identify the risk of third parties accessing Celsia's information. Each vice - presidency must verify the implementation of agreements, monitor compliance with these, and manage changes to ensure that the services provided comply with the requirements agreed with the third parties.

## 2.2. Smarkwork Information Security Policy

- Purpose: The purpose of Smartworks 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 (people who improperly obtain or disclose information), integrity (information has been altered or misrepresented, even if intentional or accidentally) and availability (information not available on request).

- Limit:

+ This policy applies to all Smartworks employees and third parties who interact with information held by Smartworks and assets used to store and process the information.

+ All Smartworks 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 / information systems are only available to authorized users according to business needs and the information systems are used effectively and effectively in accordance with Smartworks policy.

+ Information assets include 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 Smartworks and its employees to protect the organization's information systems from accidental / intentional damage or destruction.

- Policy statement:

+ Smartworks 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.

+ Security 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.

## 2.3. University of Bolton Information Security Policy

- Purpose:

+ The University 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.

+ The Information Security Policy documentation serves these purposes:

- To set out the University’s intentions in managing information security as part of effective governance.
- To provide guidance to users, administrators and developers of information systems on appropriate behaviours and controls required in order to maintain the integrity of information.
- To provide a comprehensive approach to information security across the University.
- To set out the means by which information policies and are scrutinized, approved, revised, communicated and monitored.

- Scope of the information Security Policy: This Information Security Policy:

+ Applies to all staff, students, governors, consultants, contractors, partnership organisations and partner staff 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.

+ 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.

- Implementing 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.

+ Where necessary, the University will implement appropriate physical and logical controls to restrict access to information systems and information to only authorised 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.

+ 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 mitigations within its information management practices.

+ All users will be required to abide by University policies before being authorised for access to University information systems.

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

- Responsibilities for implementing the Information Security Policies:

+ An information security working group, made up of key system administrators, managers and representatives from all relevant parts of the organisation, shall devise and coordinate the implementation of information security controls.

+ 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.

+ 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 programme.

# 3. The P3: Impact of Misconfiguring The IDS and Firewall policies

## 3.1. Firewall

Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. A firewall typically establishes a barrier between a trusted internal network and an untrusted external network, such as the Internet *(Al-Shaer and Hamed, 2004)*

System security improvements:

- 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

*(Al-Shaer and Hamed, 2004)*

Before proceeding with the configuration, we need to have a Firewall Policy. To avoid the case of choosing and setting Firewall incorrectly and effectively.

A wall is designed and implemented correctly, must be based on a particular policy. That is part of the overall security policy of the organization that uses the firewall.

Usually the firewall policy does the following two ways:

- Deny all, allow only valid traffic.
- Allow all, prohibit invalid traffic.

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

There are many different components of the security policy that are common:

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

+ Applications are not allowed to be installed (From sources such as internet, CD, USB, floppy disk).

+ The application backup installed on an organization's computer (allow / not to be 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:

+ 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 subnet 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.

+ Do not 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)

+ Do not allow unauthorized connections to the internet in any way.

- Contracted Worker Statement: Some issues that need attention:

+ 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.

+ Do not 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 24/24

After building an overall security policy, it will cover many different issues, so the amount of information will be very large Firewall *(Al-Shaer and Hamed, 2004)*

## 3.2. Intrusion Detection System (IDS)

IDS is a system that detects signs of intrusion attacks, and can initiate actions on other devices to prevent attacks. Unlike firewalls, IDS does not prevent access but only monitors activities on the network to find out the signs of attack and alert the network administrator *(Ashoor and Gore, 2011)*

Based on the surveillance scope, IDS is divided into 2 categories:

- 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).

Based on implementation techniques, IDS is also divided into 2 categories:

- 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, ie monitoring the system's performance under normal conditions to record operational parameters, which is the basis for detection. later abnormalities *(Ashoor and Gore, 2011)*

## 3.3.Potential consequences of incorrect IDS configuration

Consequences of misconfiguring the IDS system: Misconfiguring the IDS system can lead to some serious consequences, such as:

- Some networks will intentionally take advantage of this misconfiguration error 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.

Consequences of Misconfiguration of Firewall: Similar to IDS, however misconfiguring the firewall can lead to some more serious consequences than IDS:

- Configuring a firewall incorrectly can cause 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 protects.

- Configuring a firewall incorrectly can cause it to become inoperable or work against the rules desired by the configurator. 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 system crash.

# 4. The P4: Implementing a DMZ, static IP and Nat

## 4.1. DMZ

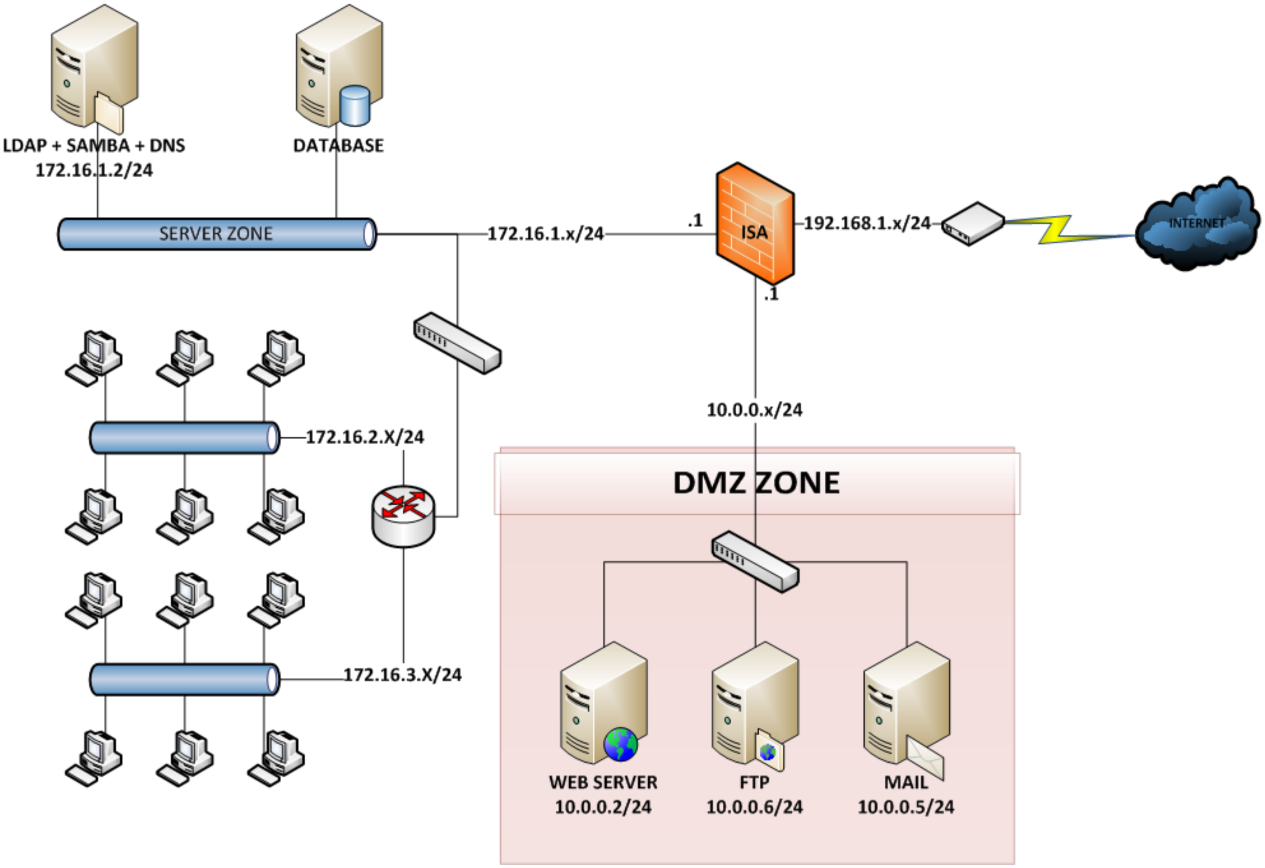
The DMZ is a neutral network area between the local network and the internet *(Crichigno, Bou-Harb and Ghani, 2018)*

Mission is a repository of information that allows users from the Internet to access and accept risks from Internet attacks *(Crichigno, Bou-Harb and Ghani, 2018)*

The function of the DMZ is the place to deploy services such as: Web server, Mail server, DNS server, FTP server,... *(Crichigno, Bou-Harb and Ghani, 2018)*

Mechanism: DMZs are designed to act as a sort of buffer between the public internet and the private network. Deploying a DMZ between two firewalls means all incoming network packets are screened using a firewall or other security device before they reach the servers that the organization hosts in the DMZ. If a better prepared threat agent gets past the first firewall, then they must gain unauthorized access to those services before they can do any damage and those systems are capable of Get hardened against such attacks *(Crichigno, Bou-Harb and Ghani, 2018)*

Example for DMZ:



Improvements in Information Security and Advantages when implementing DMZ:

- Avoid attacks from outside the internet or internal attacks.
- Add more layers of defense to the intranet.
- Reduce damage to hosts when attacked by hackers.

*(Crichigno, Bou-Harb and Ghani, 2018)*

## 4.2.Static IP

A static IP address is an IP address that is manually configured for the device, as opposed to an IP address assigned through a DHCP server. It is called a "static" address because it doesn't change. This is the complete opposite of dynamic IP addresses, which can be changed *(Bahl, Microsoft Corp, 2005)*

Function:

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

- Some services and games require a static IP address. That means the fixed IP address does not change, even after rebooting the model.

- Static IP addresses also help speed up web access and download torrent files

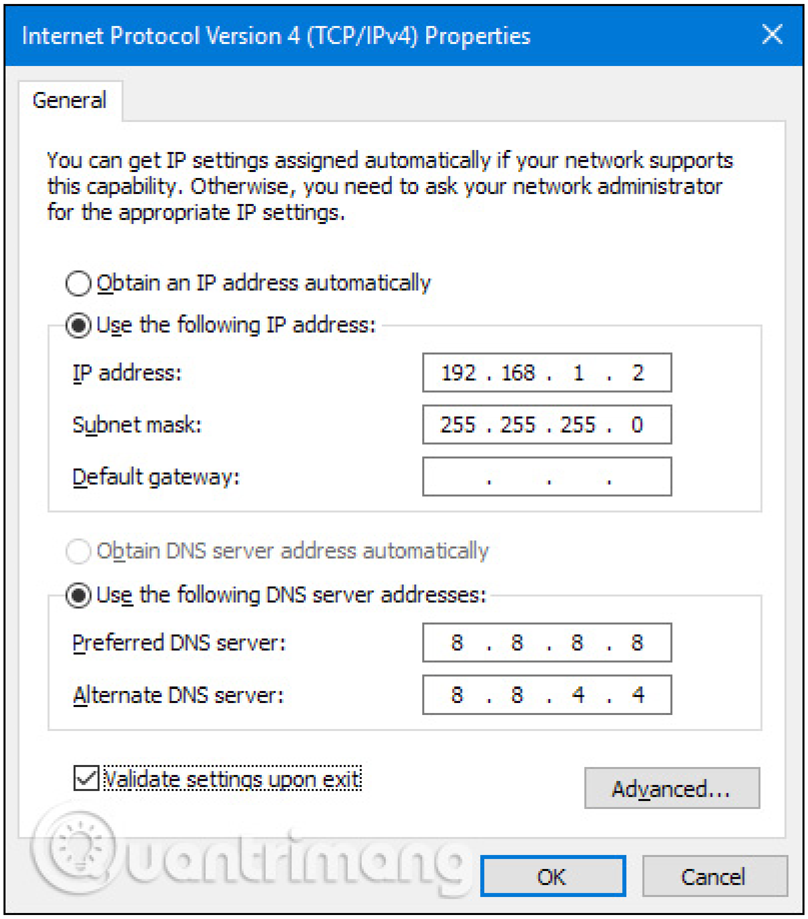
- Static IP address is essentially for stable communication with computers on the local network. For example, companies use network printers with static IP addresses.

- The company can use the fax machine to observe the camera from outside when there is static IP.

*(Bahl, Microsoft Corp, 2005)*

Mission is to assign servers with a specific purpose (web server, mail server, ...) so that many people can access them without interrupting those processes *(Bahl, Microsoft Corp, 2005)*

Example for Static IP:



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

Alternate DNS server: 8 . 8 . 4 . 4

☑ Validate settings upon exit

Advantages of implementing static IP:

- Better DNS support.

- 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.

- More convenient in remote access.

- More reliable geolocation services and communications.

*(Bahl, Microsoft Corp, 2005)*

## 4.3. Nat

NAT (Network Address Translation) is a skill of allow an or many IP address local domain convert to a or many IP external domain addresses *(Malik, 2003)*

Function: NAT makes local network address accessible to the public network (Internet). The place to perform NAT technique is the router, connecting these two types of networks *(Malik, 2003)*

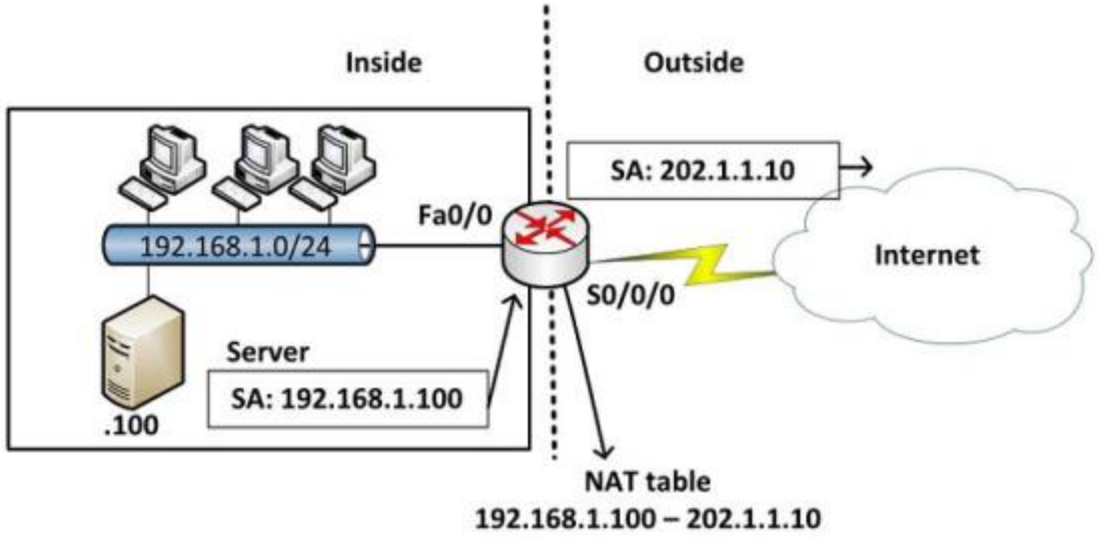
Mission:

- NAT is responsible for transferring packets from one network layer to another in the same system. NAT will make changes to the IP address inside the packet. Then switch over to the router and network devices.

- During the period when the packet is transferred from the Internet (public) back to the NAT, NAT will change the destination address to an IP address within the local network and move.

- NAT can act as a firewall. It helps users to secure computer IP information. Specifically, if the computer has problems while connecting to the internet, the public IP address (previously configured) will be displayed instead of the local network IP *(Malik, 2003)*

Example for NAT:



Advantages of implementing NAT:

- 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.

- Helps to conceal IP inside LAN.

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

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

*(Malik, 2003)*

Improved security when deploying NAT:

- Help administrators to remove packets containing malicious code or malware
- Help users conceal IP to avoid IP detection and avoid being tracked.
- Help users verify and prevent access with malicious intent.

*(Malik, 2003)*

# 5. The M1: Method to assess and treat IT security risks

## 5.1. Method to assess and treat risk

Step 1: List all the work or activities of the organization: The more detailed the listing, the more effective the evaluation can be, the more likely the listing might look like this:

- According to the administration function.
- According to geographic factories and offices.
- According to the organizational structure, functional departments.
- According to the execution order of processes, processes.

Step 2: Identify the potential risks and risks: For each job step listed; we need to identify the hazards that present risks. The hazard can be human, equipment, process, external, or possibly a combination of the above; It is then followed to identify the possible risks based on the above risks.

Step 3: The severity or ability to cause damage: To determine the severity; we have to judge against the history of the organization's operations, to see if that has happened. If it happened, it is easy to determine the extent of the damage, if it has not happened, it can be estimated, if it happened, how the damage will be and we have to divide the different levels of damage to make it easier. For ease of assessment, it is usually divided into 5 levels of damage from 1 ~ 5, depending on the size of the organization that defines the level of damage differently.

Step 4: Determine likelihood: To determine the likelihood, we also have to rely on the organization's operational history to see how often the problem occurs, from which we also divide into different levels to make it easier to hit price (reference example below). If the newly established organization has no data, we can refer to organizations in the same field, the same industry or the same operating environment.

| Level | Possibility | Explain |
|---|---|---|
| 1 | Very rare | Occurs 1 times in 5 years |
| 2 | Unlikely | Occurs 1 times in 3 years |
| 3 | Incident | Occurs 1 times in 1 years |
| 4 | It could very well happen | Occurs 1 times in quarter |
| 5 | Usually happen | Occurs 1 times in month |

Step 5: Determine the level of risk: It can be divided into 4 different levels that are low 1 ~ 4 points; medium 5 ~ 8 points, high 10 ~ 12 points and very high is 15~25 points.

| Possibility<br>Consequence | Very rare (1) | Unlikely (2) | Incident (3) | It could very well happen (4) | Usually happen (5) |
|---|---|---|---|---|---|
| Very Low (1) | 1 | 2 | 3 | 4 | 5 |
| Low (2) | 2 | 4 | 6 | 8 | 10 |
| Medium (3) | 3 | 6 | 9 | 12 | 15 |
| High (4) | 4 | 8 | 12 | 16 | 20 |
| Very High (5) | 5 | 10 | 15 | 20 | 25 |

Step 6: Justification must be resolved: Once the levels of risk have been identified, we have to implement the control measures with the priority based on the different levels of risk, the control measure can be the establishment of the risk assessment process. risks, guidelines, forms, regulations,... Normally, in order to minimize the system, we will prioritize risk control for activities at a high and very high level of risks, and for activities have a low level of risk, then we can consider it depending on the needs of the organization.

| Level of risk | | | |
|---|---|---|---|
| Very High 15 ~ 25 | Especially Dangerous | This is a catastrophic level risk, prevention methods need to be calculated in a certain time. Prioritize activities to control the risks and risks occurring. | Unacceptable risks |
| High 10 ~ 12 | Dangerous | | |
| Medium 5 ~ 8 | Relatively Dangerous | It is necessary to have handling measures such as improving security, assigning more system supervisors. Prioritize activities to control and reduce risks. | |
| Low 1 ~ 4 | Less Dangerous | Carry out data backup to prevent problems such as data loss, data changes,... | Risks can be accepted |

Step 7: Assign a conductor and follow-up to the evaluation: After completing the above assessment steps, this assessment will be reviewed and approved by the top management, and appointed people to implement the control measures as well as monitor and evaluate the effectiveness of the work. this. With this method, the organization can control the risks of all activities; it also helps to minimize the documentation system and improve efficiency.

## 5.2. Things that need security

Things that need security:

- Data: This is the top priority in everything that needs to be protected in the system. What individuals or organizations need to do is back up data and store it in a safe place.

- Hardware device: Hardware is a device used to store data and retrieve data. For server hardware, individuals or organizations need to put it in a separate room with secure system and a fire suppression system. Only provide permissions to the server room for individuals, staff with duties in the server room. Personal computer hardware should be kept in a dry, humid place, away from chemicals or inflammable and explosive materials.

- Software: Software is a collection of files that are related to each other and used to operate hardware. Software also needs to be protected. If the software fails, it will cause it to operate the hardware incorrectly or cause data loss. Software protection must be protected against external influences such as hackers because software is a crucial component in data storage and retrieval.

Security solution:

- About Data: To ensure the security of data, we need:

+ Data backup: copy all the data in the computer, server, server, ... and store it in one or more other storage devices for backup data.

+ Data encryption: converting data from one form to another or into a form of code that only someone with access to the decryption key or password can read.

- About Hardware:

+ The individual or organization should place it in a separate room with the safety system and fire suppression system.

+ Only grant the right to use the server room to individuals, employees with duties in the server room.

+ Install a cooling system for the server room to avoid overheating of server equipment leading to fire and explosion.

+ Regularly check and replace hardware components as needed.

+ Personal computer hardware should be kept in a dry place, not wet, away from chemicals or inflammable materials.

- About Software:

+ Regularly check software for security holes.

+ Regularly upgrade or update the software.

+ Using security software such as anti-virus, anti-malware, ...

Reassessment The risk assessment and treatment method is outlined in the previous section: The above method is an effective method. The above method has an assessment of the risk and damage levels based on the ISO 900 Assessment Criterion. The steps taken are also based on the logic of the ISO 9001 Evaluation Standard.

## 6. The M2: Network Monitoring Systems

Network monitoring system is a system that monitors the breakdown, performance, status of devices and computers in a network system. The system includes a recording software and helps system administrators to record and track the information passed through it *(Aki and Saito, Fujitsu, 2008)*

Core elements in network monitoring:

- Mastering tools, equipment, and software for monitoring, including internal and open software.

- Mastering parts, units, systems, services and equipment for monitoring.

- To use methodically tools and solutions to support the processing and analysis of monitoring results. Some tools like Snort, Wireshark, Nessus, Nmap,...

- Make sure the staff has a good knowledge of the field.

A network system is comprehensive, so network safety monitoring is very important, requiring you to know the components in the system such as:

- Server - the server

- Network infrastructure equipment such as:

+ Hub

+ Router

+ Switch

- Workstation, workstation model

- Devices and systems for network monitoring
- Software and applications in workstations and servers.

The nature of SIEM, also known as Security information and event management, is created with the main purpose of collecting data and information about security events. It is calculated from terminals to centralized storage. Thanks to the analysis results of network safety system tools, we can detect the risks of hacker attacks.

The main benefits of a network security monitoring system are:

- Helping manage more centralized
- SIEM can detect network penetration and attack problems that are difficult for conventional devices to detect.
- Makes troubleshooting simpler but more efficient
- Overall, SIEM is a great product for large organizations, enterprises, banks, corporations and government agencies.

Network monitoring software: One of the network monitoring software that many people use a lot is Splunk. Splunk is feature-based tool from Log analysis and design on Lucence, MongoDB platform. This tool specializes in finding, monitoring and analyzing large data of applications, systems, software and network infrastructure equipment.

Advantages of Splunk network monitoring tool:

- Support diverse on workstations, Firewall, IDS / IPS, Log Event ..
- Constantly updating data in real time
- Smart search engine includes keywords, search functions and structure, from which you can access everything you want.
- Automatically fix the problem

Disadvantages of Splunk network monitoring tool:

- Not suitable for high security systems

- Time to learn, use and operate quite a long time

- In particular, there must be a separate system large enough. And of course, Splunk is not suitable for medium to small scale systems.

In addition to Splunk there are network monitoring tools Syslog-Ng, Logzilla (Php Syslog-Ng), HP ArcSight Logger, Nagios, system monitoring service Loggly.

Solutions to strengthen the network system: There are 3 main solutions to help the surveillance system be secure, including:

- Solution to manage and analyze security events: is a combination of the two above solutions to overcome inherent limitations. So the documentation will be geared towards building this solution.

- Security information management solutions: focus on collecting and archiving logs.

- Security event management solution: focuses on analyzing and processing logs that have been collected to deliver alerts to users.

Problems occurring in the network system:

- Cannot grant or obtain an IP address.
- Can not connect to server.
- Printing errors.
- Poor quality cable.
- The transmission is slow.
- DNS error.
- The touch machine cannot connect to wifi.
- Low bandwidth.
- Device not working.

A network monitoring system is deployed to track problems:

- Bandwidth.
- The operational status of network devices.
- Connection between devices.
- Monitor unusual activities like hacking or monitoring invalid access.

Network monitoring system that supports system evaluation:

- About connection: Network monitoring system will monitor and report on the connection status between terminal and terminal.

- Network monitoring system: Network monitoring system will regularly collect data about bandwidth and report suspiciously low or high bandwidth transmission.

- Regarding access: The network monitoring system will record all access levels to the system and the exclusion into valid and invalid access.

*(Aki and Saito, Fujitsu, 2008)*

Reasons for choosing a network monitoring system:

- When the network monitoring system monitors in real time and detects any unusual events, the administrator will receive immediate notification via text message or email.

- Network monitoring system capable of finding the cause, analyzing and diagnosing problems.

- Can provide detailed insight into the problem, help assess its severity and estimate the time it takes to fix it.

- It is possible to monitor the status of a security system, evaluate its effectiveness and exploit this system more thoroughly.

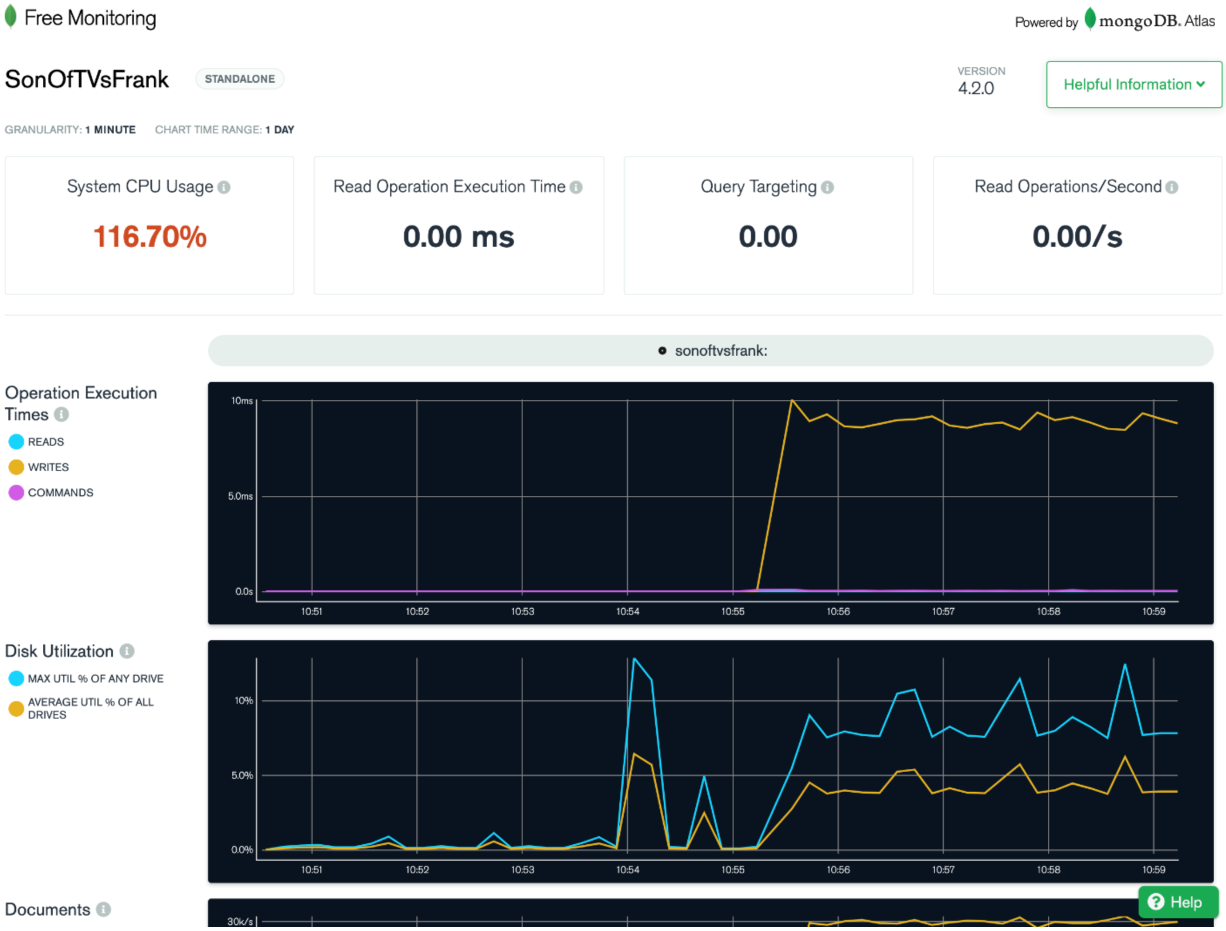
- Allows organizations or individuals to monitor and update, detect and correct application problems before users complain.

- Maximize system availability by monitoring all active devices in the network, including servers, workstations, network devices, and applications.

- Troubleshooting can be faster, easier, and reduces security risks compared to free software.

Some Software of Network Monitoring System:

- MongoDB Platform



Free Monitoring

SonOfTVsFrank STANDALONE

VERSION 4.2.0

GRANULARITY: 1 MINUTE CHART TIME RANGE: 1 DAY

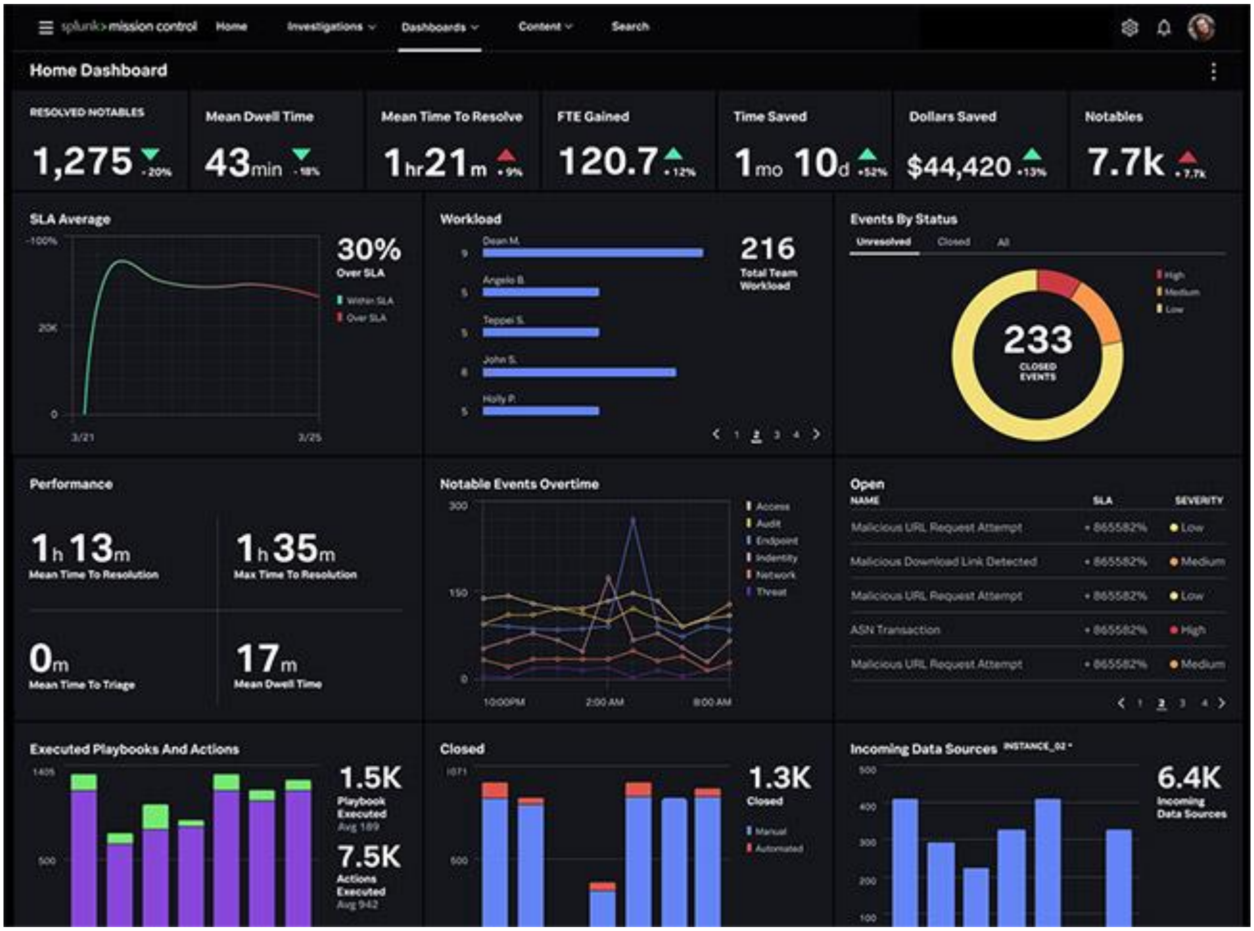
System CPU Usage 116.70%

Read Operation Execution Time 0.00 ms

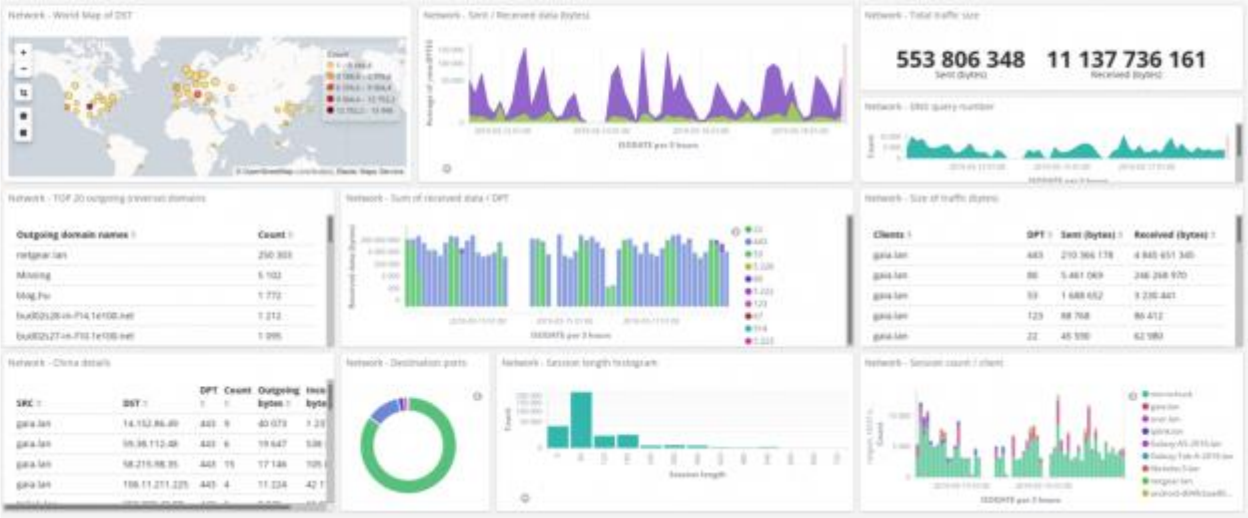
Query Targeting 0.00

Read Operations/Second 0.00/s

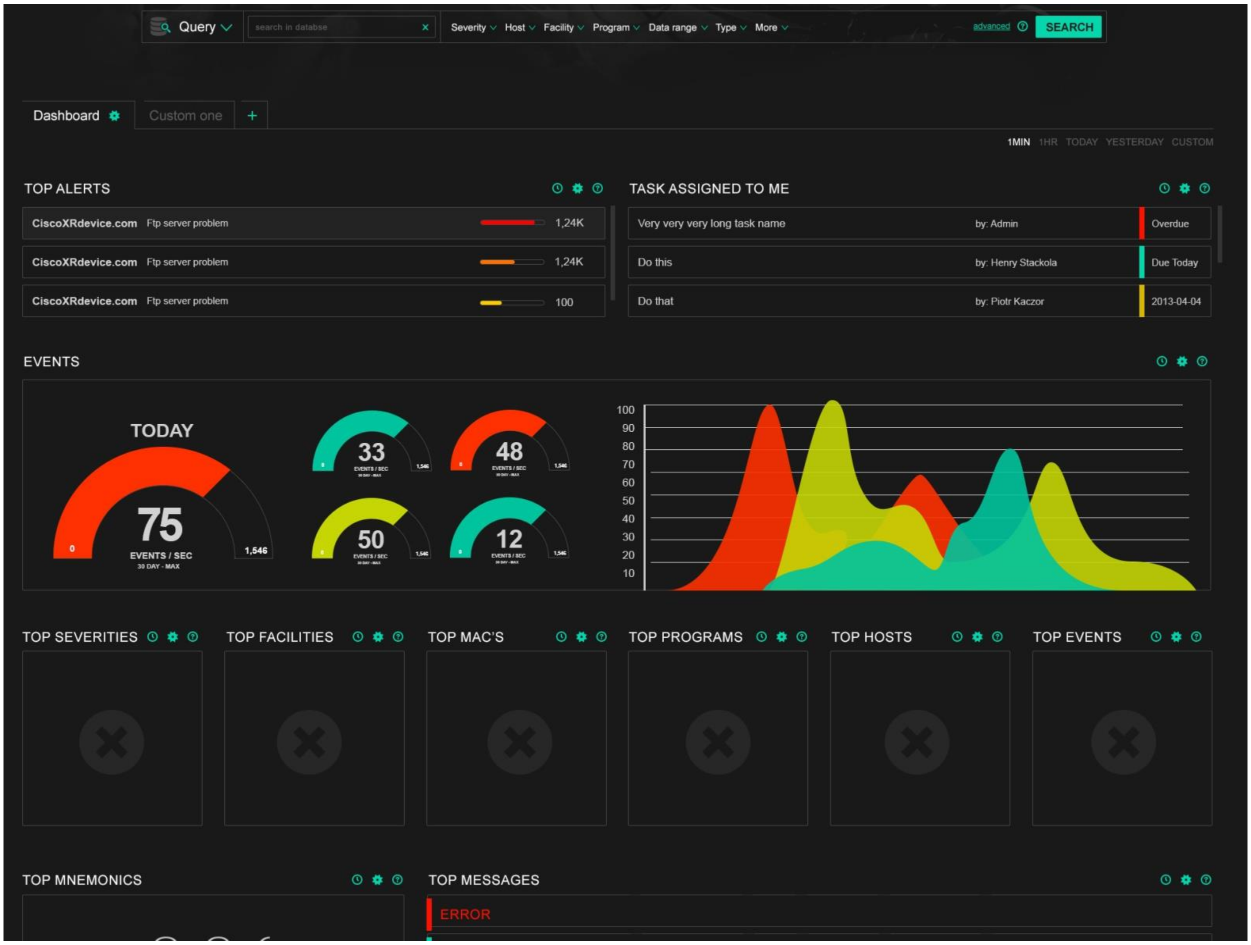
- Splunk



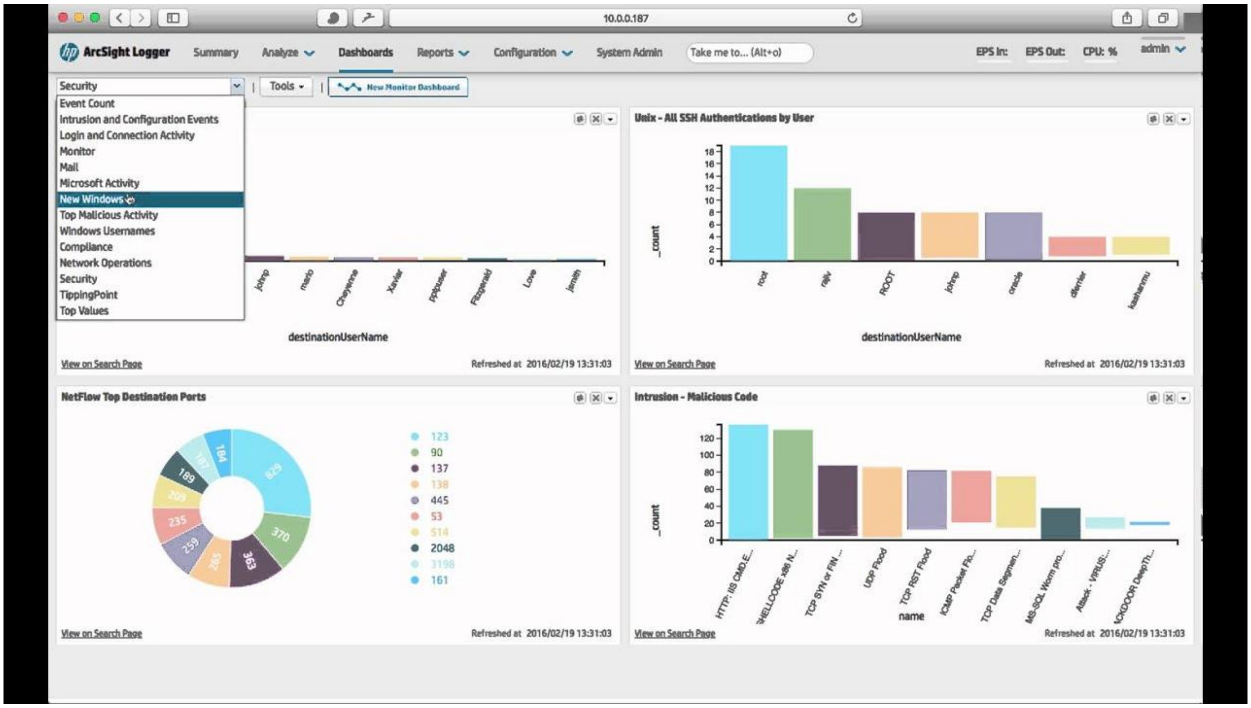
- Syslog-Ng



- Logzilla (Php Syslog-Ng)



- HP ArcSight Logger



# 7. The D1: Trusted Network

A trusted network is one that is under the control of a network administrator or network administrator. Basically, this is the network that the network administrator trying to protect and define security parameters for the same. Therefore, it can also be said that trusted networks are within the security ring *(Josang, Hayward and Pope, 2006)*

Components of trusted networks include:

- Firewall
- Users computer, Phone,...
- Server
- Some connected devices such as: switch, Hub, Bridge, Cable, router

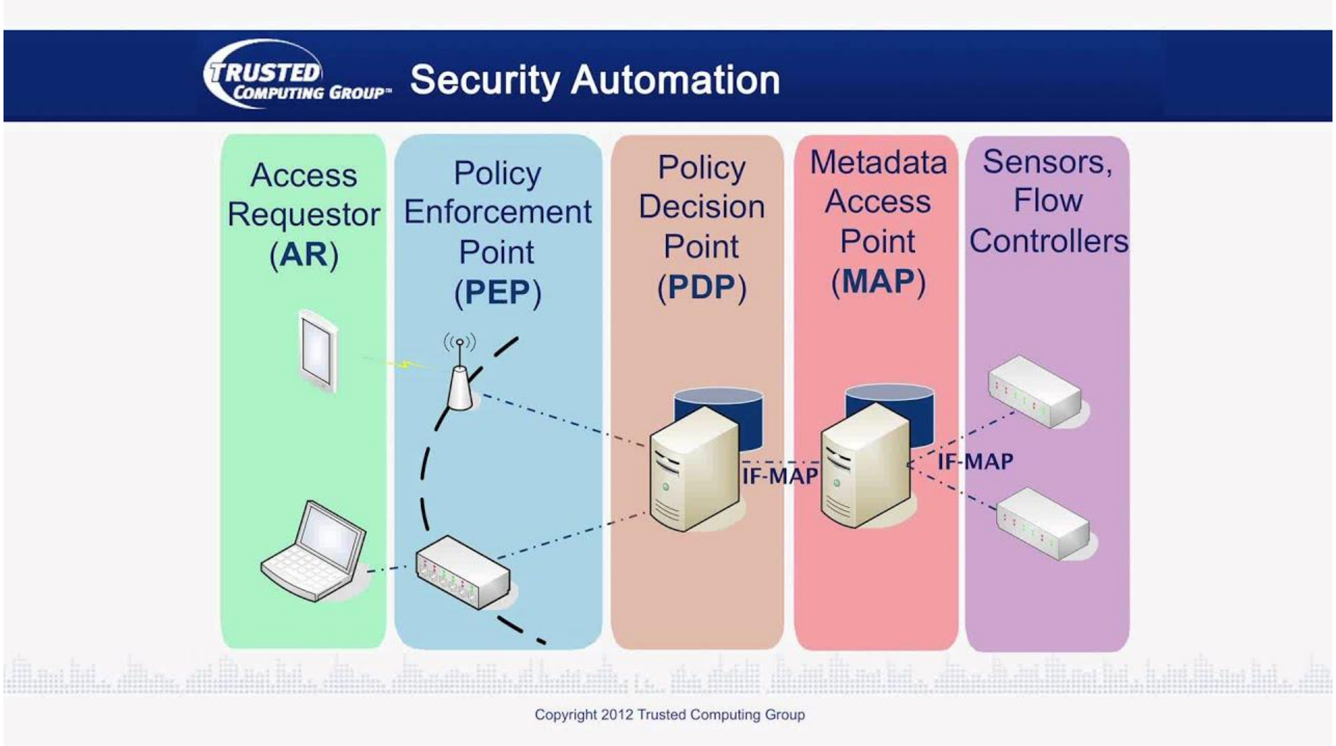
Trusted Network facilitates the gathering of information about an endpoint and securely distributing that information to other components in the environment. The Trusted Network architecture recognizes the following high-level roles for the entities involved in trusted network communication:

- An endpoint: any entity - physical or virtual - that can be connected to the network.
- Execution points: take access control decisions from the policy server and apply them to endpoint requests.
- Policy server: collect and evaluate endpoint posture information and / or make access control decisions based on endpoint context (including role, state, location, behavior, and factors) and communicating those decisions to execution points.
- Configuration Management Database (CMDB): stores the collected endpoint measurements.
- CMDB client: communicates endpoint information and consumes information from CMDB.
- Metadata Access Point (MAP): provides centralized coordination for security and network information manufacturers and consumers
- MAP client: publish, search, and subscribe to endpoint and environmental updates via MAP.

A single entity can assume multiple roles.

*(Josang, Hayward and Pope, 2006)*

For example, the policy server can also be a MAP client as well as a CMDB client. The following figure illustrates the relationship between roles in trusted networks:


TRUSTED COMPUTING GROUP
Security Automation
Access Requestor (AR)
Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
Metadata Access Point (MAP)
Sensors, Flow Controllers
IF-MAP
IF-MAP
Copyright 2012 Trusted Computing Group

The dangers that trusted networks prevent:

- Trust networks enhance the value of the Trusted Platform Module (TPM) by helping to establish a link to a decision point where integrity reports can be assessed. The use of a trusted network's TPM is optional, but for platforms with a TPM, the convenient reporting infrastructure allows for TPM reports to be included in compliance assessment and access control decisions. network. A system with TPM can protect sensitive data such as encryption keys and collected measurements. The TPM securely stores those measurements in a protected location until ready for reporting; when the trusted network allows for that report. Products based on a trusted network architecture can work in today's environments with and without TPM, but if so, there is a higher assurance that the integrity reports of the private network. Dependability is derived from the intended foundation.
- Endpoint antivirus and malware protection.
- Protection while browsing the web from threats like malware or phishing.
- Encrypt your data to avoid problems like data disclosure or data theft.
- Comprehensive reports on equipment to avoid failures and risks.
- Ensure that your network and IP data are not exposed.

Conclusion: Trusted networks can be part of information security.

*(Josang, Hayward and Pope, 2006)*

# 8. References

*Aki, Y. and Saito, H., Fujitsu Ltd, 2008. Network monitoring system. U.S. Patent 7,353,269.*

*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.*

*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.*

*Bahl, P., Microsoft Corp, 2005. System and method of assigning and reclaiming static addresses through the dynamic host configuration protocol. U.S. Patent 6,957,276.*

*Crichigno, J., Bou-Harb, E. and Ghani, N., 2018. A comprehensive tutorial on Science DMZ. IEEE Communications Surveys & Tutorials, 21(2), pp.2041-2078.*

*Josang, A., Hayward, R.F. and Pope, S., 2006. Trust network analysis with subjective logic.*

*Malik, S., 2003. Network security principles and practices. Indianapolis, Ind, Cisco.*

*Zucker, M., 2016. Information Insecurity. Science Scope, 39(8), p.73.*