Network Security

Thesis · November 2019

DOI: 10.13140/RG.2.2.19900.59526

1 author:

Alfred Tan Yik Ern
Asia Pacific University of Technology and Innovation
29 PUBLICATIONS **1** CITATION

SEE PROFILE

TECHNOLOGY PARK MALAYSIA
GROUP ASSIGNMENT
CT037-3-2-NWS

NETWORK SECURITY

UC2F1805IT(ISS)

NAME	TP NUMBER
TAN YIK ERN	TP046566
CHEA YAN SHAW	TP045215
GUO JUN HAO	TP046636

LECTURER: Nor Azlina Binti Abd Rahman
HAND OUT DATE: 1ST OCTOBER 2018
HAND IN DATE: 25th JANUARY 2019
WEIGHTAGE: 100%

INSTRUCTIONS TO CANDIDATES:

1. **Submit your assignment at the administrative counter.**
2. **Students are advised to underpin their answers with the use of references (cited using the Harvard Name System of Referencing).**
3. **Late submission will be awarded zero (0) unless Extenuating Circumstances (EC) are upheld.**
4. **Cases of plagiarism will be penalized.**
5. **The assignment should be bound in an appropriate style (comb bound or stapled).**
6. **Where the assignment should be submitted in both hardcopy and softcopy, the softcopy of the written assignment and source code (where appropriate) should be on a CD in an envelope / CD cover and attached to the hardcopy.**
7. **You must obtain 50% overall to pass this module.**

Contents

Section A

Guo Jun Hao (TP046636) Privacy network security (PNS)

Introduction

The privacy network is in a local geographical area (such as a school, factory and organization), generally a computer communication network consisting of various computers, external devices and databases connected within a few kilometers. It can be connected to a remote local area network, database or processing center through a data communication network or a dedicated data circuit to form a large-scale information processing system. Privacy network enables file management, application sharing, printer sharing, scanner sharing, scheduling within workgroups, email and fax communication services in your network. The privacy network is strictly closed. It can consist of several or even thousands of computers in the office. The main technical elements that determine the privacy network are: network topology, transmission medium and medium access control method. The privacy intranet belongs to a privatized regional network.

(Figure 1: Privacy network security) (Wolfe, 2019)

The privacy intranet computer uses a NAT (network address translation) protocol through a private the gateway accesses the Internet. A computer with a privacy network can send a connection request to other computers on the Internet, but other computers on the Internet cannot send connection requests to the computer of the privacy network and query any information about the

privacy network. In addition, the biggest problem with privacy network is network security. Even if it is a private network, it will always be attacked by this privacy network to get all the information in this privacy network. Network security means that the data in the hardware, software and systems of the network system is protected, and it is not damaged, changed or leaked due to accidental or malicious reasons. The system runs continuously and reliably, and the network service is not interrupted.

Security Features

(Figure 2: Automated document encryption) (Locklizard, 2019)

The internal intelligence information of the organization (school, company, government) to which the privacy network belongs must be encrypted and stored. Therefore, the privacy network system automatically encrypts each file and manages or modifies it through different levels of rights managers, which is the primary condition for document security protection. As long as the file is saved in plaintext, automatic encryption is maintained when stored in the privacy network system. When there is a hacker or an illegal organization attack, the file will be encrypted. If an illegal organization or a hacker cracks the encryption, the file will be destroyed automatically to ensure the confidentiality of the file and the information. There are many ways to leak secrets, and there are ways for criminals to obtain trade secrets. But even when an illegal organization conducts a

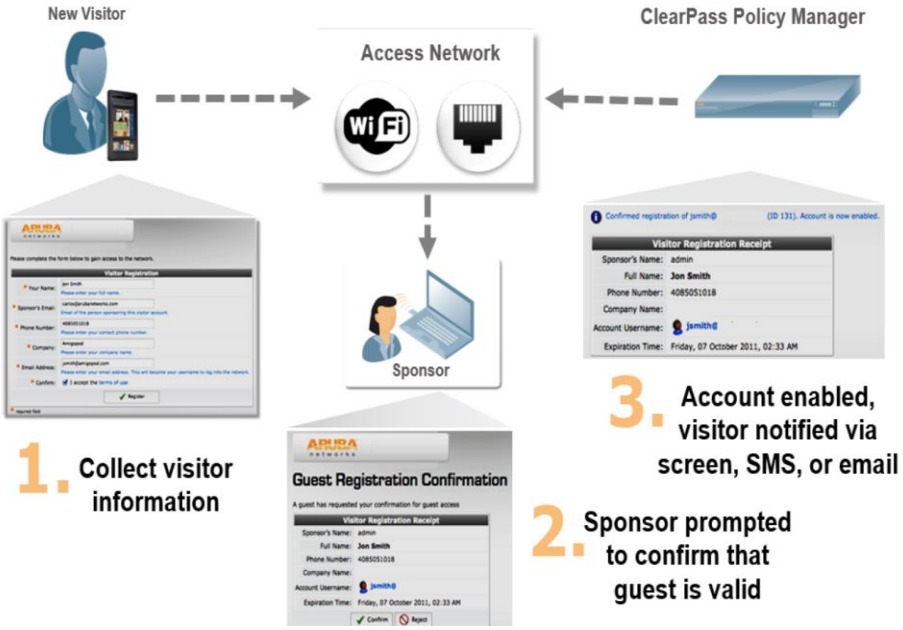
network attack, automated file encryption saves important protection information and privacy effects.

(Figure 3: Real-time control of authority) (ONLINE, 2019)

When you log in to your own privacy network organization account for activity, the network system records every activity that belongs to this privacy network. Top management (system top managers, company managers, learning management, etc.) has the authority to control all behaviors of each account in real time. When an account is found to be abnormal, the highest management can control the system account at any time and even limit the system account permissions. In order to avoid having to control the use of information materials after handing over the information to the other party, the user's authority can be controlled. For example: set which people can browse which files, can print files, save files, set the time limit for file use, the number of times users can browse, print or time range, prohibit user screen copying, use other auxiliary software to record screen, copy screen, Limit user reading conditions such as: specified machine, IP area restrictions. In this way, it not only ensures the safe use of the document in the shared state, but also completely controls the use permission of the document, effectively preventing the illegal dissemination of the electronic document, and even if it is spread out, it cannot be seen.

(Figure 4: Web security features) (laurenpoussard | creativestudio, 2019)

Given the increasing complexity of Web-based attacks, organizations must deploy a robust Web security solution. For many years, we have been using simple URL filtering, which is indeed a core part of Web security. But Web security is much more than just URL filtering. It also needs to inject AV scanning, malware scanning, IP reputation recognition, dynamic URL classification techniques and data leakage prevention. Attackers are attacking many high-profile websites at an alarming rate. If we only rely on URL black and white lists to filter, then we may only have whitelisted URLs available for access. Any web security solution must be able to dynamically scan web traffic to determine if the traffic is legitimate. Among the top 5 security solutions listed here, Web security is at the forefront of security technology development and costs the most. Most of the other solutions are quite mature. Web security should remove the illusion as soon as possible and return to the real world in order to withstand the attacks initiated by hackers.



(Figure 5: Symantec NAC Admission Control System Architecture) (Route XP, 2019)

NAC is a series of technologies and solutions proposed by Symantec for network security management and special protection of private network systems. NAC combines IEEE 802, lx technology to perform security policy checks on all devices attempting to access network computing resources. This limits emerging security threats such as viruses, worms, and spyware to compromise network security. Customers implementing NAC can only allow trusted terminal devices (PCs, servers, PDAs, etc.) that comply with security policies to access the network and control non-compliant or unmanageable devices to access the network, while supporting registration management of removable storage media. The NAC system mainly includes a terminal management server SEP, a terminal admission control server LANEnforcer, and a terminal management software Endpoint protection. The policy management server SEP is responsible for the unified management of security policies and end users: LAN Enforcer acts as an authentication server system and access switch in the IEEE 802.1x user identity authentication architecture. According to the authentication information of the terminal, the switch is enabled to open or close the port. The LAN Enforcer also periodically updates the security policy and terminal user information from the SEP. The EndPoint protection runs on the terminal device and checks whether the terminal device meets the security policy requirements according to the security policy of the SEP, and is in the IEEE 802. The .1x authentication process sends the security policy check

result and the profile information as authentication information to the LAN Enforcer through the EAPoL message.

The specific description of the terminal devices in the Symantec NAC system is as follows.

(1) The client sends the configuration file information and security policy check result information to the IEEE 802.1x-enabled network access switch before connecting to the network.

(2) The network switch forwards the information to the LAN Enforcer.

(3) The LAN Enforcer checks the client's profile information and security policy check results. If the profile information is illegal (such as a terminal device without Symantec EndPoint protection installed) or if the client

The endpoint did not comply with the security policy. Then the LAN Enforcer notifies the access switch to close the corresponding port to prevent it from accessing the network or placing it in the isolated network, where the computer can obtain remediation; if the profile information is legal and complies with the latest security policy on the SEP, the LAN Enforcer notifies the connection. The person switch opens the corresponding port to allow it to access the network.

(4) After the client remediates the computer and complies with the computer, the IEEE 802.1x protocol re-verifies the computer and grants the computer access to the network.

Privacy network security implemented in system

An organization (company, school, government) privacy network topology, in which the external network and LAN server (except the repair server) is a protected network, all computers on the intranet must be Symantec protection terminal software, the client access to the network needs to pass IEEE 802.1x authentication is successful only after access: To ensure that network printers, IP phones, video terminals and other devices that cannot install Symantec protection terminal software are used normally, the switch ports connected to them are not IEEE 802.1x enabled. Host Integrity Policy Configuration the following Host Integrity policies are configured in the LAN Enforcer as follows.

(1) The WSUS (Patch Distribution Server) client is installed.

(2) The WSUS client service is running.

(3) Prevent IP address changes.

(4) Disable Windows AutoPlay for all device types.

(5) Check if the Rising process is running.

(6) Enable logging and auditing.

(7) Enable security protection (the password complexity requirements and passwords are

Validity period requirements, disable default sharing, etc.)

(8) Disable the registry tool.

(9) Unregistered mobile storage devices are prohibited.

(10) Wireless modems are prohibited.

Expected result

- The terminal management server unifies the security policy and automatically distributes the server.
- To each client. The flexible and efficient management of the terminal security policy is realized.
- Because all access switch ports have IEEE802.1x enabled and associated with the access control server. The client needs to install the Symantec client software to gain access to the network through IEEE802.1x authentication. Thus, the Symantec client software enables the terminal to enforce the security policy defined on the terminal management server. The terminal security configuration is enhanced to ensure that the terminals in the access network have good security configurations, and the terminals that fail to reach the security configuration level are isolated from the information network.

- By enforcing the WSUS policy in the security policy, ensure that the terminal has system patches, and eliminate most of the sources from the source in a timely manner.
- A virus program that exploits system vulnerabilities. Reduce the administrator's operation and maintenance pressure.
- Through the management function of mobile storage devices, the trusted management of real mobile storage devices reduces the spread through mobile storage devices
- The possibility of viruses and non-unit personnel arbitrarily copying corporate information.
- Prohibit the implementation of wireless modems and eliminate illegal outreach

Impact of Privacy network security

According to data analysis, many organizations (schools, businesses, governments) have their own privacy networks. In particular, large and medium-sized enterprises have established their own private networks, and developed corresponding network security use systems for Internet users' operating systems. However, the security of application systems and networks is not perfect. At the same time, events such as terminal computer viruses, worms or Trojan horses, as well as information leaks, will still occur from time to time. The impact on the privacy network is as follows:

(1) Security policy has not been effectively implemented

For their own security risks, companies often develop a series of security policies and security systems to protect their network security. However, with the rapid increase in the size and complexity of intranets, these security strategies are increasingly difficult to implement effectively. Security policy assurance capabilities make it difficult for enterprise security policies to be fully monitored and enforced on large, dispersed hosts such as personal computers and mobile devices. For example, forcing

The virus firewall needs to be enabled to update the virus database in time, and force the user to modify the default unsafe configuration of the host system and monitor the execution results.

(2) The system did not fix the patch in time

The existence of host system vulnerabilities is the root cause of all security incidents. The most important factor leading to cybersecurity incidents is still "utilizing unpatched or unprotected software vulnerabilities", accounting for 50.3%, timely repair

Vulnerabilities in complex systems have become a way to protect internal networks.

(3) Lack of intranet access control

According to the famous "barrel principle", the security management of any access device is lacking. For example, if you have not upgraded the security patch in time, do not update the virus database or install unauthorized software, which can be fatal to the security of your company's intranet. Internal network access control checks the security status of the device when accessing the internal network. Only devices that meet security requirements are allowed to access the internal network. If an insecure device blocks access to the internal network, you can avoid security risks.

(4) Lack of effective control of mobile storage media

Mobile storage media, such as USB flash drives and mobile hard drives, are widely used due to their small size and large capacity. However, if uncontrolled, normal removable storage media will be connected to the confidential host or classified mobile device

Storage media is used for non-confidential hosts, which may result in business

Confidential information leaked.

(5) End-user illegal outreach

Due to imperfect management systems or lack of effective terminal monitoring technology, individual users in the internal network use telephone dial-up, plug-and-play Internet access devices. Privately operated external internet connection will blacken the look Guest attacks, viruses and Trojan horse attacks bypass the security barriers of current deployments. Lead to information disclosure and virus intrusion.

Recommendation

Network management

In the network environment of the manufacturing industry, due to the size of the unit and the needs of the office, there are many working areas, and even in the field, there are also their own offices and production workshops. In order to facilitate information sharing within the enterprise,

Generally, special lines or other network interconnection technologies are used to connect with the internal network to facilitate data management and office management within the unit. However, large-scale network environments and complex branches have brought great difficulties to network management. The distribution of devices is not clear; traffic management has no basis; for static IP address environment addresses, conflicts are also very difficult. The main aspects of network management include the following aspects:

Physical network topology

The internal network of the unit is set up by the cooperation of network devices. The main equipment's are: routers, switches, and HUBs. The core role of data interaction in the LAN is the switch.

The current network management software can draw the logical topology map and extract and control the panel information of the switch. However, the physical connection between the terminal device and the switch port cannot be seen, and the topology map cannot be seen.

Information about the connected device. How to establish the connection relationship between the switch port and the device is crucial, because the traffic information of the port is actually the traffic information of the device; if you want to control the device, just enter the switch port.

Line control is fine. Therefore, the physical topology diagram shows that the physical connection relationship between the device and the port brings great convenience to management.

DATA control

With the physical connection relationship of the devices on the physical network topology map, you can control the ports connected to the switch through the flow control of the switchable ports,

and close the ports or open the ports. However, it is impossible for all switches in the internal network environment to be network managed, and it is impossible for an administrator to open and close a port every day, unless such abnormal network attacks and congestion occur. Therefore, for daily control, the most effective method is to control the network card traffic of each terminal device. If the traffic of the device can be controlled within a certain range, the normal operation of the device is ensured.

It can also prevent congestion caused by illegal use of P2P download software to capture bandwidth and virus outbreaks, which is a practical management tool for management.

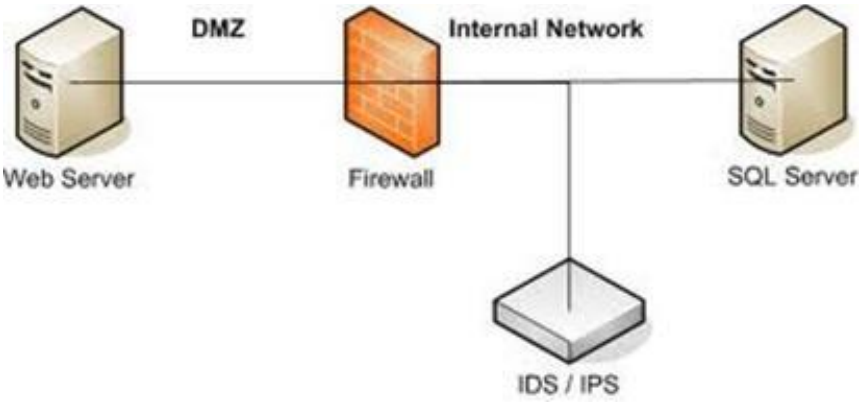
Conclusion

The results of the use of the system after operation indicate that the control system can be guaranteed by deploying privacy network security. The terminal device can effectively implement the security policy, reduce the probability that the terminal device suffers from the calculation of virus infringement and the infringement of the black guest, and provide a technical means for the security management of the computer terminal device, thereby effectively improving the security protection level of the intranet information.

Tan Yik Ern (TP046566) Intrusion Prevention System (IPS)

Introduction

Intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system (IDS) and attempt to stop possible incidents. Also known as a system that monitors a network for malicious activities such as policy violations and security threats. The main function of an IPS is to identify suspicious activity and log information, IPS will attempt to block the activity and then finally to report the malicious activities [1].



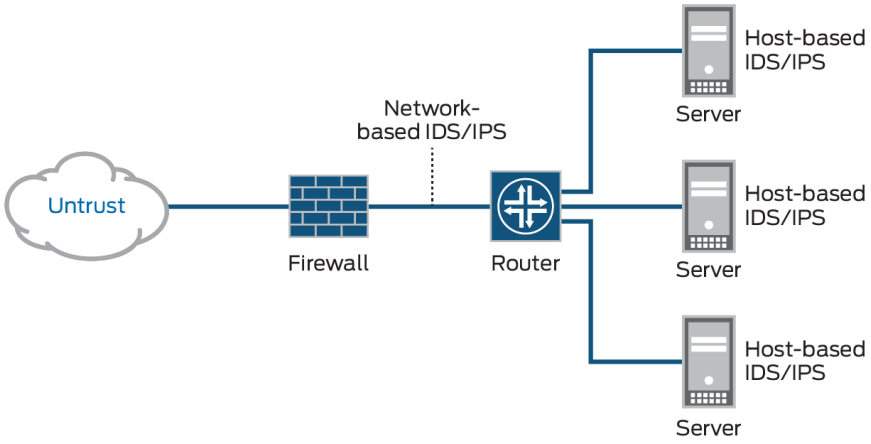
(Figure 1: IPS/IDS implement in system) (InfoSec Resources, 2019)

An IPS can implemented as a software or hardware device. The principle of IPS is filter the dirty traffic goes in and the clean traffic goes out. Intrusion prevention systems is an extensions of intrusion detection system. The difference between IPS and IDS are the main function of intrusion prevention system is actively block or prevent intrusions that are detected. For instance, IPS allowed to block the traffic an offending IP address and malicious packets.

(Figure 2: Cisco IPS hardware) (Services, 2019)

Security Features

Network Intrusion Prevention System (NIPS)



(Figure 3: Network intrusion prevention system) (Juniper.net, 2019)

Network intrusion prevention system (NIPS) used to monitor a network and protect the confidentiality, integrity and available (CIA) of the network. Its main functions are protecting the network from threat and malicious activity, such as denial of service (DoS), man-in-the-middle (MITM) and unauthorized usage. [1]

After the Intrusion prevention system installed in a network, it will be starting to scan the network packets in and out for suspicious traffic and malicious activity by analyzing the protocol

activity. IPS creates physical security zones to filter the network and make the network intelligent. IPS also used to defend the polymorphic threats, trojans, worms and viruses.

Intrusion prevention system is a real-time device for protect the network security. But the intrusion detection system is passive device, need to command it and IDS will start scanning the network. When a malicious activity and suspicious traffic occur, IPS will take action based on certain prescribed rules, such as clear the bad traffic or stop the network packets.

Wireless Intrusion Prevention System (WIPS)

(Figure 4: Wireless intrusion prevention system) (Watchguard.com, 2019)

Wireless intrusion prevention system (WIPS) is to prevent unauthorized network access to local area network and other information assets by wireless devices. WIPS operates at the Layer 2 level (data link layer) of the open system interconnection model (OSI). (website: gather.com)

WIPS can detect the denial of service (DoS), man-in-the-middle (MITM) and unauthorized usage. Improvement the wireless security and good data packets transfer by using wireless intrusion prevention system.

There are three measure to deploy a WIPS. The first, WIPS found at the lower-end of the market, known as time slicking or time sharing. This type of deployment, the wireless access point (AP) does double duty, providing network traffic with wireless connectivity while periodically scanning for rouge access points. [3]

Second, WIPS allowed to build in the authorized access point continually scans radio frequencies, looking for unauthorized access points. It also known as integrated WIPS. [3]

Third, wireless intrusion prevention system can sense the whole building to monitor radio frequencies. The sensor forwards the data they collect to a centralized server for further analysis, action and log achieving. To sense the whole building radio frequency requires dedicated hardware. Its also known as WIPS overlay. [3]

Network Behavior Analysis (NBA)

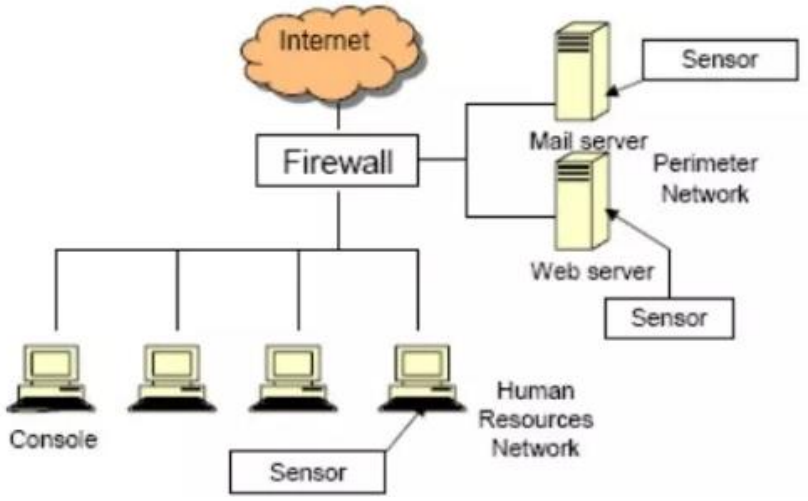
(Figure 5: Network Behavior Analysis) (Flowmon.com, 2019)

Network behavior analysis is a program to monitor throughout the network to ensure the security of a proprietary network. NBA helps in improving network safety by watching traffic and observing unusual activity and departures of a network operation. Common methods of defending a network against harmful data include signature recognition and packet checking and real-time blocking of malicious sites and data.

The program also checks and account for change in bandwidth and protocol being used during communication. This is particularly applicable in finding a potentially dangerous data source or website. The duty of an NBA program is to reduce the labor and time of network administrator

and network analysis to detect and resolve network issues. The NBA improved network protection along with firewalls, antivirus software and spyware detection tools. [4]

Host-based Intrusion Prevention System (HIPS)



(Figure 6: Host-based intrusion prevention system) (GBHackers On Security, 2019)

Host-based intrusion prevention system is a program to protect computer systems that contain crucial data against viruses and other internet malware. Scanning from the network layer, transport layer, session layer, presentation layer and application layer in the OSI model. [6] HIPS protect from known and unknown malicious attacks. HIPS often check every single host and the various events that occur within the host for suspicious activities.

The host-based intrusion prevention system can be implemented in workstations, computers and servers.

To detect and monitor the database of system objects about system calls, application logs and file-system modifications (access control lists, password files, binaries and capability databases). HIPS will create a checksum for the contents to remember each object's attributes. This information gets stored in a secure database for later analysis.

HIPS also check weather appropriate regions of memory have not been modified. Generally, it does not use virus patterns to detect malicious software but rather keeps a list of trusted

programs. A program that oversteps its permissions is blocked from carrying out unapproved actions.

The enterprise and home users have increased protection from unknown malicious attacks. HIPS use a peculiar prevention system that has a better chance of stopping such attacks as compared to traditional protective measures. Secondly, HIPS need to run and manage multiple security application to protect PCs, such as anti-spyware, anti-virus and firewalls. [5]

Intrusion Prevention System implemented in system

Positioning an IPS on the network

An intrusion prevention system (IPS) usually installs behind the firewall, adding another layer of analysis that removes malicious content from the data flow. The IPS installs in the communication path between the source and the destination, analyzing traffic and taking action. The system will give a notification or alert to user, dropping malicious packets, blocking traffic and resetting connections. So, IPS can result in degraded network performance if it hasn't been configured correctly. [7]

Connecting active directory to an IPS

Used IPS to track the user's identity, if a security event is triggered in IPS, user no necessary to deal with sifting through Active Directory logs to cross-reference users with IP address. The IPS systems allow you to gather identity information for the devices and applications attached to the network and traffic that is transmitted. User can gather this information using a number of different techniques with identity management systems including Active Directory and LDAP. [7]

Setting Up an IPS

Before user get started, user need to understand a few things about the network and traffic.

- How much traffic does it get?
- What type of traffic do you see?

- How many connections are there between the network and other networks? Include the internet.
- How complex is your network? How big?

This information will help user decide how many IPS devices you will need and what sort of hardware that user will need. First step, deploy your device with the default rules. This will give you a good baseline from which to work when the user tunes the device. Next step, tune the device to ensure that the alerts user see reflect actual, actionable events. For example, user can set the event action override to drop packets with a risk rating greater than 90% because if user have too many events, it quickly becomes unwieldy to determine which are false positives. If user have too few, then then the IPS is not doing its job and user runs the risk of getting false negatives. [7]

Setting up blocking rules for intrusion prevention system

Configuration the IPS blocking rules need slowly modify the rules until user get the blocking rules to where user want them. Basically, user looks for a balance between identifying threats and not affecting day-to-day business. Currently, most devices that monitor the network are limited in the amount of traffic they can monitor. This will require user to restrict what traffic have to monitor. For example, all the users will choose to monitor every external interaction with traffic inbound to your internal network. Additionally, specific services like email server and web server need to be monitored by relatively strict rules because they are often targeted for attack. [7]

Impact of intrusion prevention system

Wrong Source addresses

Intrusion prevention system implemented in firewall to prevent the network attack break the device or system’s firewall. Based on the network address that is associated with the IP packet that is sent into the network. This is good if the network address contained in the IP packet is

accurate, the address that is contained in the IP packet could be faked or scrambled. Here, we knew that IPS cannot detect the packet that is fake or scrambled. [8]

False notification

Intrusion prevention system are able to analysis the network behavior that is not normal for average network usage. While it is good to be able to detect abnormal network usage, the disadvantage is that the intrusion software can create a large number of false alarms. The number of user increase will impact the frequency of false alarm increase. So, the IT technician or IT professional must receive extensive training so that they can recognize what is true alarm and false alarm. [8]

Encrypted packets

The encrypted packets are not processed by the intrusion prevention system software. Hence, the encrypted packet can allow an intrusion to the network that is undiscovered until more significant network intrusions have occurred. Besides that, encrypted packets can also be set to be activated at a specific time or date once they have been planted into the network. This could liberate a virus or other software bug, which could be avoided if the intrusion prevention software was able to process encrypted packets. [8]

Analytical module

The analytical module has a limited ability to analyze the source information that is collected during intrusion detection and prevention. The result of this limit is that only a portion of the source information is buffed. Intrusion prevention system cannot point out where the abnormal behavior originated form. The response to this information can only be to try and stop the unauthorized network access. The IT technician and IT professional have to take defensive approach to prevent next network intrusion. [8]

System not install IPS

Intrusion prevention system not implemented behind the firewall to prevent the data and packet transfer from web server to SQL server will be endanger the whole device and system.

Cannot packet-filtering in firewall

Without installed IPS in firewall, there will let many unknown packet transport to the system through thr transport layer. IPS will provides network security by filtering network communication based on the information contained in the TCP/IP header of each packet. IPS not implemted affect the firewall cannot uses a filtering table to decide which packets must be discarded. [9]

Cannot detect malicious intrusion

Without installed IPS in system affect the device or system cannot detect malicious intrusion. For example, the malicious activity or event that done by hacker through network layer and data link layer. IPS will not allow or stop the traffic to gain access to its target network. Blocking from eavesdropping, hijacking, denial of service and man in the middle attack. [9]

Cannot alert indication of intrusions

File intrusion

- Cannot identification of unknown file and program on your system
- Cannot block unauthorized people to modify file permission
- Cannot explained modifications in file size
- Cannot identifications of storage file presence into system directories
- Cannot track the missing files

Network intrusion

- Unauthorized people can arbitrary log data in log files
- Unauthorized people can repeat probes of the existing services
- Sudden increase in bandwidth consumptions
- Unauthorized people can identifications of repeated attempts to log from remote locations

System intrusion

- System logs are deleted
- System performance decreased drastically
- Unusual display of graphics, pop-ups
- System crashes suddenly and reboots without user interventions
- System failure in identifying valid user
- Active access to unused logins
- Login during non-working hours
- New user account created automatically
- Modification in system software or configuration files

Recommendation

Analysis manually

Besides using the software liked Snort, Suricata or other IPS software, the network security analyst also has to scan the inbound and outbound traffic manually. Because the IPS software not enough humanize. So sometimes the hard to detect and prevent the malicious packet. For example, software needs to update to latest version. For example, IPS software developer need to update the latest information about the suspicious packet into the software. Network security scan the traffic meanwhile can analysis the and search for the anomaly packet.

Ban malicious IP address

The auto intrusion prevention system cannot identify which IP address have to ban. Due to it cannot detect the real or fake inbound packet. The network analyst has to identify the inbound packet manually. After that, network security able to ban the IP address used the IPS software. To reduce the IPS software error ban the IP address, network security have to check manually to manage the IP address.

Conclusion

In-depth overview of intrusion prevention system (IPS) is protecting the network security. There are 4 main functions of IPS, such as network intrusion prevention system (NIPS), wireless intrusion prevention system (WIPS), network behavior analysis (NBA) and host-based intrusion prevention system. Installed the IPS in a right location can perform good security for network. To monitor hosts for system alteration or sniffs network packets off the wire, seeking for malicious contents. [9]

IPS and IDS should install together due to every single time packets transport to firewall, IDS will detect the packet. If IDS found suspicious packets, the job will pass to IPS try to prevent the suspicious packets such as blocking or ban the source of IP address. The biggest weaknesses are the high number of false-positives and the maintenance effort needed to keep signatures up to date and fine-tuned. [9]

Chea Yan Shaw (TP045215) DDoS Prevention

Introduction

Distributed Denial of Service (DDoS) is use a lot of zombie computers to either directly or indirectly to flood the targeted server, with a huge amount of information and choke it in order to cause legitimate users cannot access them. The owner of the zombie computer may not know that it is infected or that an attacker is using them to attack the target server.

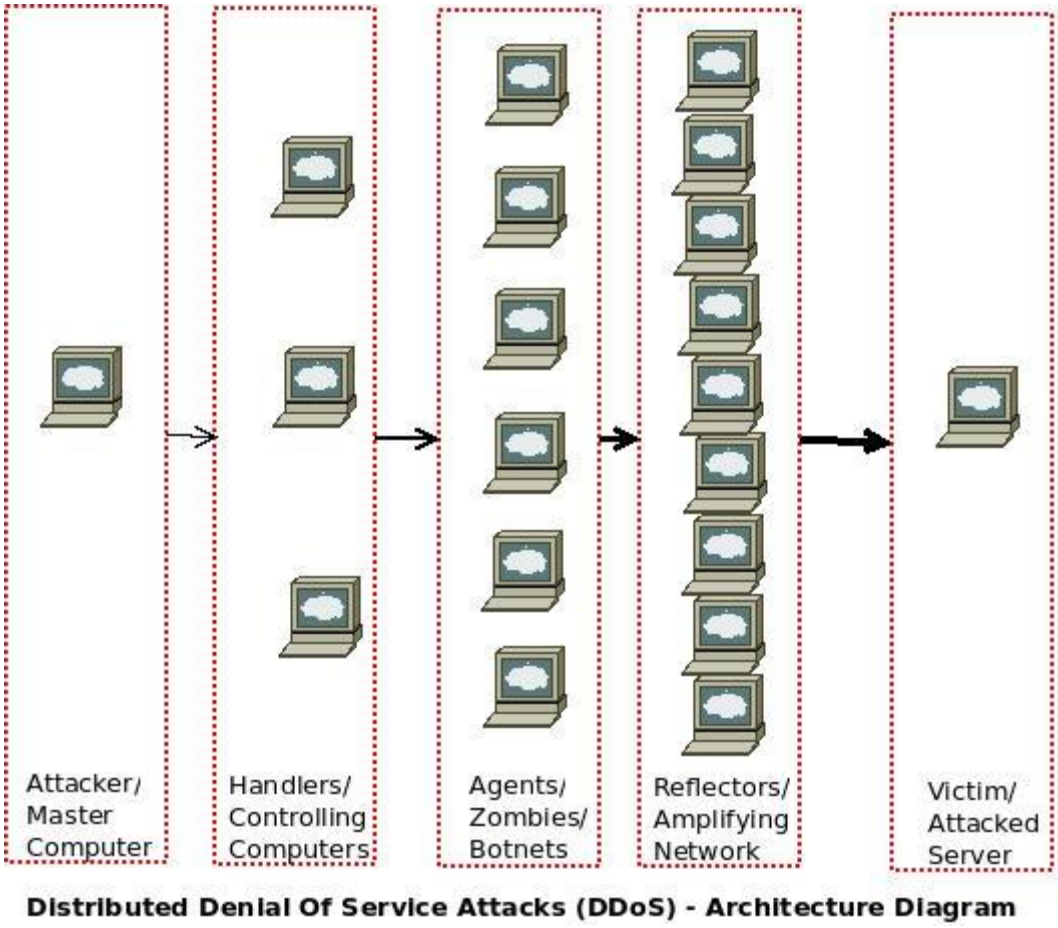


Figure 1: Architecture of DDoS (K, 2011)

The Attacker from where the attacks are initiated and the Victim server which comes under the attack makes it a Denial of Service attack (DOS). The middle three parts make it a distributed denial of service attack. A botnet is a computer that is responsible for performing DDoS attacks.

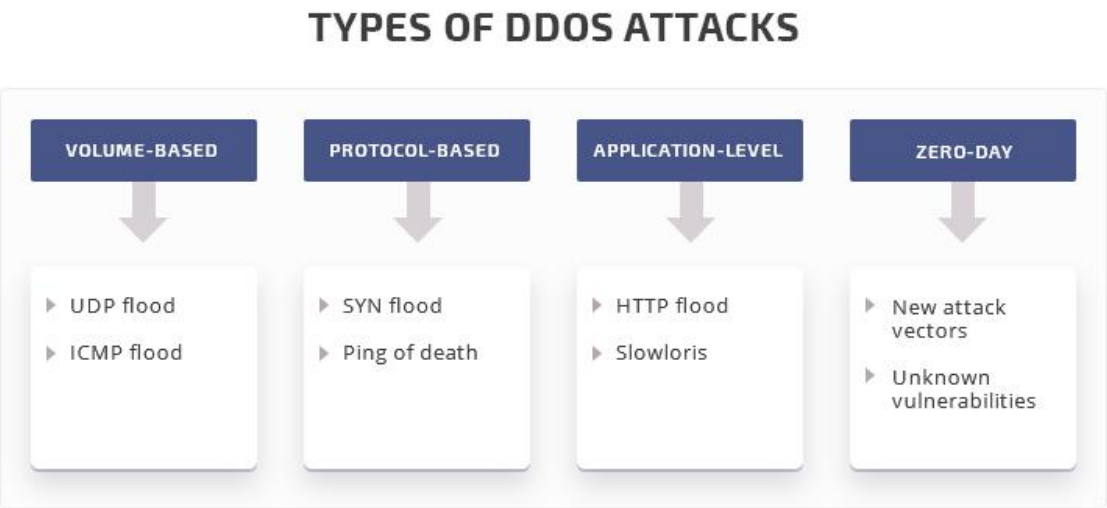


Figure 2: Classification of DDoS Attacks (apriorit, 2018)

Volumetric attacks: Try to block access to server resources with a lot of traffic, usually with botnets and amplification techniques. The most common types of capacity attacks are UDP floods and ICMP floods. (apriorit, 2018)

Protocol attacks: Attack against the weaknesses of the way the protocol works, and is the second most common attack vector. The most common types of protocol attacks are SYN flood and Ping of death. (apriorit, 2018)

Application attacks: Take advantage of weaknesses in the Level 6 and Level 7 protocol stacks for specific applications rather than the entire server. Usually targeted at common ports and services such as DNS or HTTP. The most common application-level attacks are HTTP flood and Slowloris. (apriorit, 2018)

Zero-day DDoS attacks: Using unknown software vulnerabilities that have not been patched or using less common attack vectors, making it harder to detect and protect (apriorit, 2018)

Distributed denial of service attacks is difficult to prevent/mitigate, but measures can be taken to prevent/identify/alleviate DDoS attacks. Some of these include identifying patterns of

DDoS attacks, applying load balancing, limiting maximum incoming traffic, Honeypots, and others.

Security Features

Anomaly detection

Network traffic is analyzed by statistical models and machine learning algorithms and traffic patterns are classified as normal or DDoS attacks. You can even search for anomalies in other network performance factors, such as device CPU utilization or bandwidth usage. (apriorit, 2018)

ACLs and firewall rules

In addition to ingress and egress traffic filtering, access control lists (ACLs) and firewall rules, it can also be used to enhance traffic visibility. You can analyze the ACL logs to understand the types of traffic that are running over the network. You can also configure a web application firewall to block suspicious incoming traffic based on specific rules, signatures, and patterns. (apriorit, 2018)

Intrusion prevention and detection system alarms

Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) provide server traffic visibility. Although false positives are high, their alerts can be an early indicator of anomalies and potentially malicious traffic. (apriorit, 2018)

Knowledge-based methods

Compare traffic to patterns of known DDOS attacks by using signature analysis, state transition analysis, expert systems, description scripts, and self-organizing maps. (apriorit, 2018)

DDoS Prevention implemented in system

Using firewalls

While firewalls don't protect your applications or servers from complex DDoS attacks, they can handle simple attacks efficiently.

Installing the latest security patches

Most attacks target software or hardware vulnerabilities, so all patches on time can help you reduce the risk of attack.

Disabling unused services

The fewer applications and services that may be hacked, the better. Be sure to disable all unwanted and unused services and applications to increase the security of your network.

Scale the load

Use load balancers and content distribution networks (CDNs) to mitigate the impact of attacks by balancing resource loads so that they remain online during an attack.

SIEM integration

It's important that your anti-DDoS solution integrates seamlessly with the SIEM system so that you can gather more information about the attack, analyze it and use it to enhance DDoS protection and prevent future attacks.

Impact of DDoS Prevention

User Experience Degradation

Redirecting to the cloud scrubbing center during a DDoS attack results in reduced throughput for existing legitimate connections. Re-establishing an existing TCP connection may result in packet loss. In addition, the scrubbing device cannot distinguish between existing connections and bad traffic, causing legitimate clients to be forced to reconnect. (Allot, 2018)

Incomplete detection

The cloud scrubbing center only samples input traffic without checking all incoming traffic, so the shunt mitigation solution does not provide 100% effective attack detection. In addition, Netflow cannot detect low-speed attacks based on applications. (Allot, 2018)

Relatively Slow Mitigation Due to Diversion Requirements

Netflow-based detection is slow, and it takes 2-3 minutes to propagate. The damage that can be caused by a flood attack is for a long time. For many new "hit and run" attacks, this delay is unacceptable. (Allot, 2018)

More Hardware Intensive

The inline DDoS protection solution monitors all traffic and performs mitigation at the checkpoint, thus requiring carrier-class capacity, throughput, reliability and scalability. It needs to be deployed in your network infrastructure, so it has a larger upfront capital expenditure than the scrubbing center solution. (Allot, 2018)

System not install IPS

Launching a DDoS attack is relatively inexpensive, but its impact on the business cannot be estimated. The mid-level DDoS attack lasts for about $500, and the loss of 24 hours of operator service is astronomical. In addition, the inability to provide services can damage a company's reputation and may have a more serious impact.

Service unavailability

The company to fail to meet its Service Level Agreement (SLA) with the customers. In November 2016, Google's availability issue in Central Europe cause all taxi services relying on Google Maps didn't work. (Kohout, 2018)

Data leakage

Attackers using DDOS to attack target servers cause their carrier firewalls to crash, and hackers illegally operate carrier servers without a firewall. In 2015, the British phone operator Carphone Warehouse became the target of the DDos attack, and hackers stole millions of customers' data on the carrier's servers and may publish them. (Toms, 2016)

Application is not efficient

In 2012, six US banks became the target of a series of DDoS attacks. Even if the bank can handle several types of DDoS attacks, it can't deal with other types of attacks. The system is slow to process, resulting in unpredictable losses. Such as the reduction in business transactions. (Toms, 2016)

Data lost

During the DDOS attack, if no precautions are taken, the normal traffic packets will not be transmitted and will be lost.

Recommendation

Add extra bandwidth

Provides extra time to identify and handle DDoS attacks. It also allows your server to adapt to a large number of traffic spikes and ease your strong attacks. (BENNETT, 2017)

Use a Content Delivery Network (CDN)

The CDN works by identifying traffic originating as part of a DDoS attack and transferring it to a third-party cloud infrastructure. (BENNETT, 2017)

Restricted area access

If the business is not an international business, there is no need to open access to all countries. Open access to countries in need, effectively reducing the possibility of DDOS attacks.

Make real-time adjustments

The attacker makes real-time changes to the attack target by waiting to see how the business responds and changes its methods accordingly. Therefore, by letting the server adjust the traffic in real time, it adapts to different attack methods of the attacker.

Conclusion

Hackers continue to make and improve DDOS attacks, targeting specific services, small businesses, large enterprises, and even public and non-profit organizations. Hacking is to exhaust the resources of the victim's server, causing their services, applications, or websites to crash.

Although there is no solution to completely prevent DDOS attacks, there are some effective DDOS attack protection techniques and methods. This strengthens the server infrastructure to protect against DDoS attacks and reduce their consequences.

Section B

Introduction

The project is creating a scenario from 2 location company, there are Company A and Company B, they are a food manufacturing company. Company A is based in KL and has 3 departments while Company B is in Singapore which is about 350 Kilometers away. Therefore, the purpose of this project is to allowed these 2 company's network connections established and secure the network. The main aim of this scenario and it is protecting the internal and DMZ hosts DNS as well, therefore, the exploitation of DMZ or any internal data would cause a severe loss in the aspects of financial and reputation to the companies.

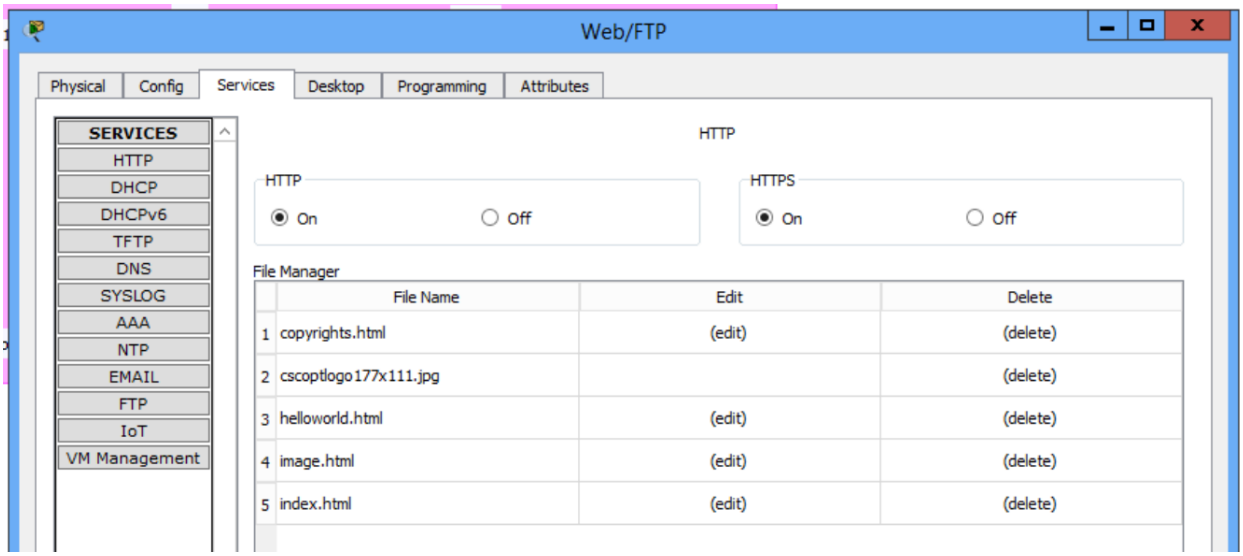
The diagram above is the network topology of the company. Next, the details information about the solution and configuration is shown below.

1. **Client workstations (sales, engineering and finance) must be able to access the web server at the DMZ over HTTP and HTTPS. The web server should be reachable from the external clients over HTTP and HTTPS only. (Solution and configuration)**

DMZ or demilitarized zone is protecting the internal Local Area Network from the untrusted internet. Here DMZ have to protect the web server, web mail and other DMZ could decrease the opportunity from hacker get into the system. (Rouse, 2017)

HTTP and HTTPS is hypertext transfer protocol is and application protocol and it runs on port 80. The function of HTTP is to transfer resources across the internet and it enables communication between physical dispersed system. HTTPS also same as HTTP but it more secure than HTTP. (Support, 2018) Because the S meant secure. This is also an encryption protocol to ensure that sensitive or confidential information are safe when the data transferring. (Pickaweb, 2018)

Below the diagram is configuration of activating HTTP and HTTPS.



(Diagram 1: Configuration of the Web/FTP)

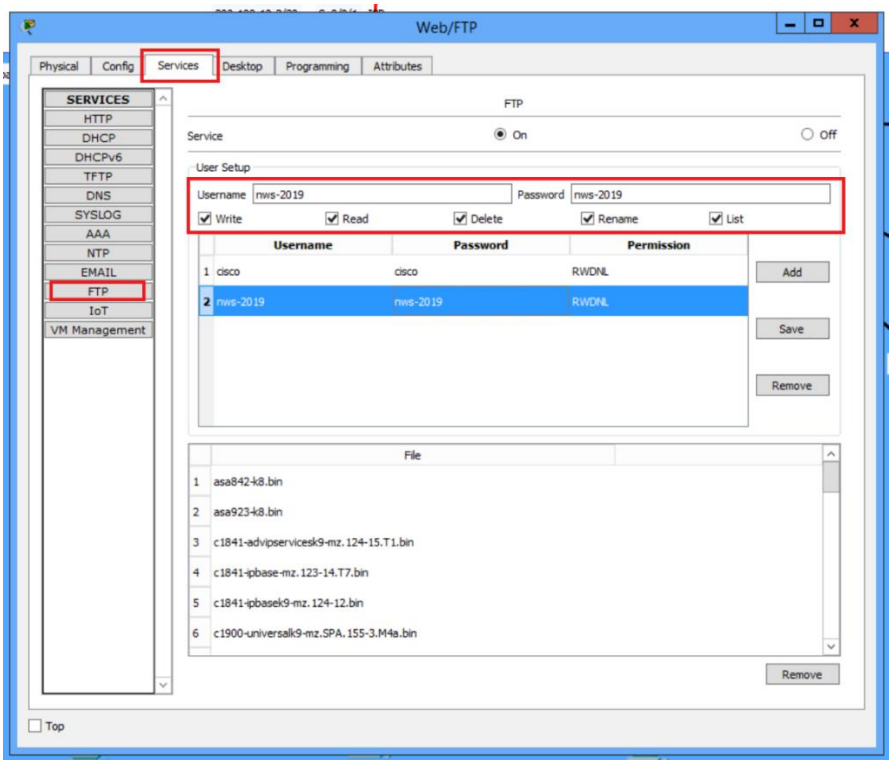
Open the web server and navigate to the config tab. Below the config tab categories choose form. Navigate to HTTP and HTTPS on to activate them.

2. <u>Clients should also be able to put and get files via FTP to the same server. The company requires implementing FTP with user and password is essential for each transaction. (Solution and configuration.)</u>

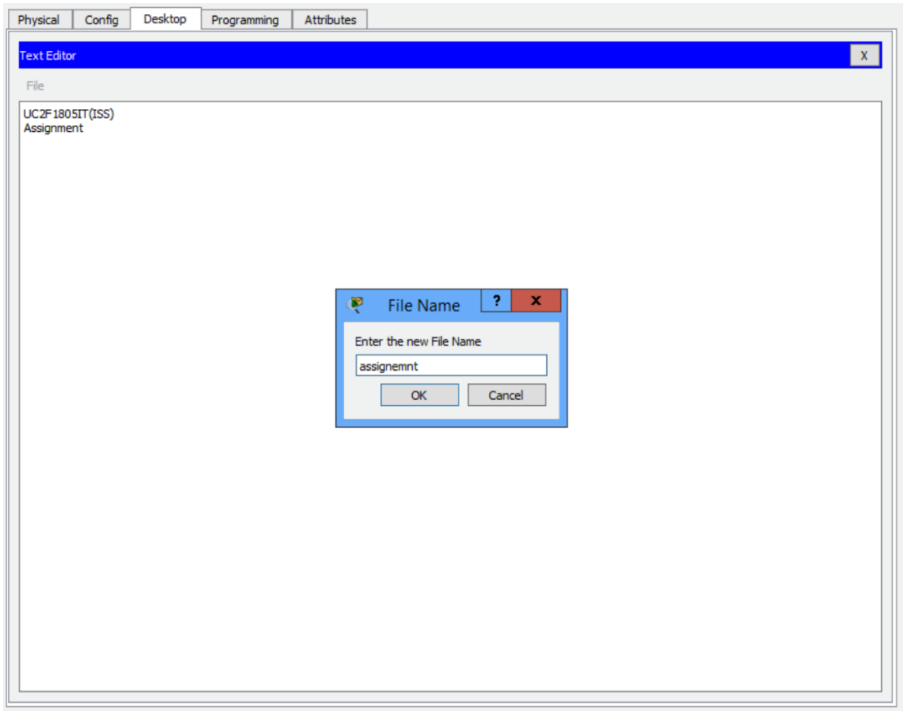
FTP stands for File Transfer Protocol, the function of it is allowed the client to upload and download files from the server. FTP also used for transfer files between client and client due to the computer can get the file through the server. (Justin , 2016)

The question 2, the client should to upload and download files through this protocol to access Web or FTP server. Implemented this protocol in the organization is because it will allow the users to share file between each other easily, so that it will improve the efficiently for the users to complete the assigned tasks. (Justin, 2016) The company need username and password to implement for each transaction in FTP to increase the security of the protocol.

Configuration

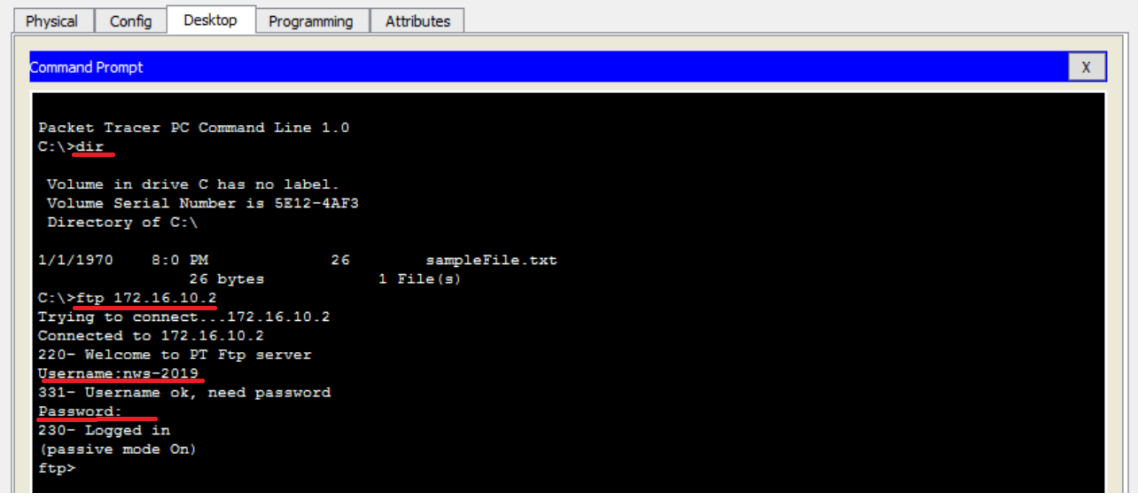


(Diagram 2: Configuration of the Web/FTP server)



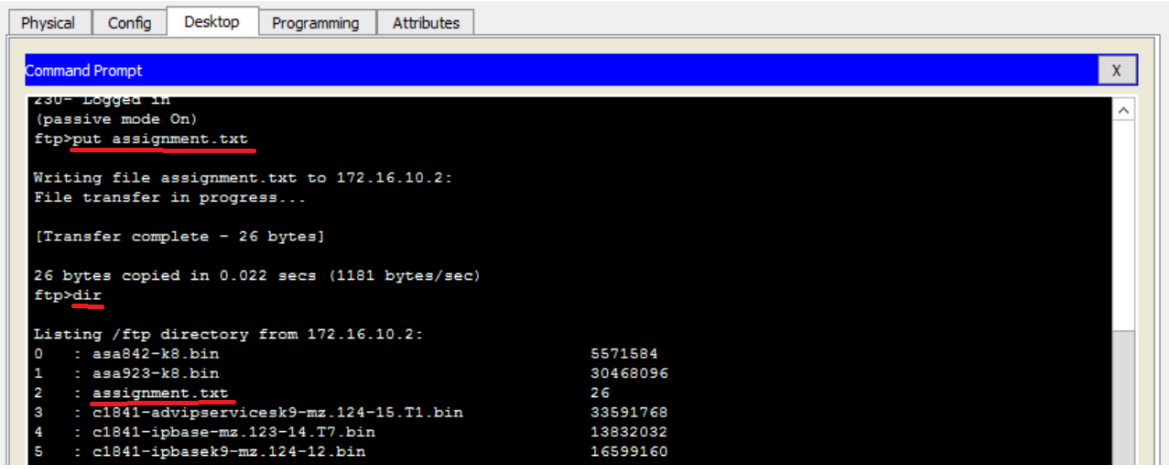
(Diagram 3: Provide information and save text file)

Choose a PC and click the desktop and then click on text editor. After that, just input the information that the user wants to share and save it.



(Diagram 4: Check PC directory and connect to FTP server)

Later on, proceed to the command prompt of the PC and check the directory of the PC using the command “dir”. Through this command, the user will able to figure out the file that the PC have. The user also needs to connect to the FTP server using the command “ftp IP address of the server” and username and password is required.



(Diagram 5: How to upload file to FTP and check the file)

After successfully connect to the FTP server, the user can just easily upload the file that he or she want to share by using the command “put filename”, which is shown in the diagram above. After the transfer is complete, the user can check the directory of the FTP to ensure the file is successfully upload.

Later on, proceed to the command prompt of the PC and check the directory of the PC using the command “dir”. Through this command, the user will able to figure out the file that the PC have. (BRAIN, 2017) The user also needs to connect to the FTP server using the command “ftp IP address of the server” and username and password is required.

(Diagram 4: How to upload file to FTP and check the file)

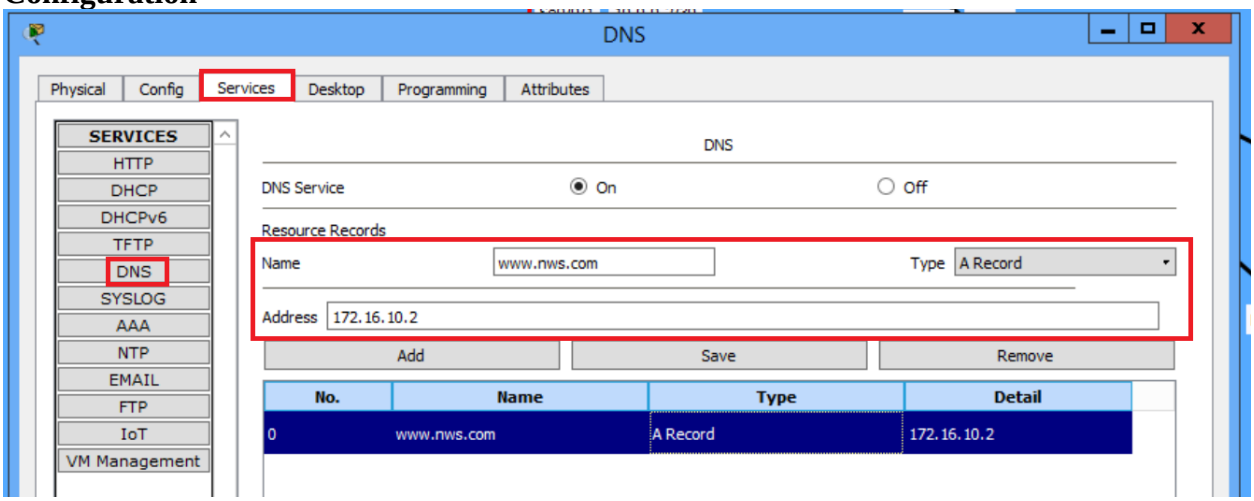
After successfully connect to the FTP server, the user can just easily upload the file that he or she want to share by using the command “put filename”, which is shown in the diagram above. After the transfer is complete, the user can check the directory of the FTP to ensure the file is successfully upload.

3. **Engineering and sales workstations must be able to access the Internet (to reach company B) over HTTP and HTTPS with DNS. No other protocol access is allowed to the Internet. (Solution and configuration.)**

The third question of the scenario is the workstation (Engineering, Sales and Finance Department) which locate in Kuala Lumpur and Singapore can access the web server with URL instead of IP address. DNS server is a solution to suitable for this situation. (BRAIN, 2018) Domain name system is a system that store IP address and the domain name in the list like a “phonebook” in computing. Next, the Access Control List (ACL) will be made a block the services. The ACL will be configured to only permit external clients to access to web server.

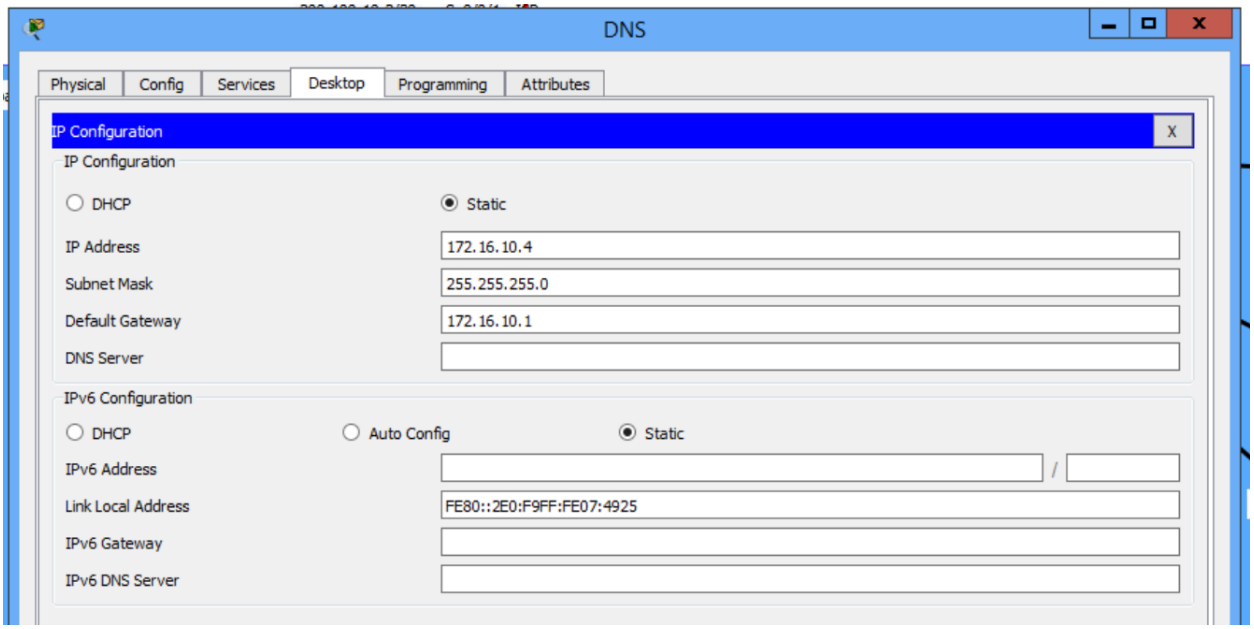
Setting up an idle location of DNS server is at DMZ. This is to ensure that the workstation in Singapore able to access it. After we assign the IP address for the DNS server, we need to point the client (workstation) to the DNS server IP address.

Configuration



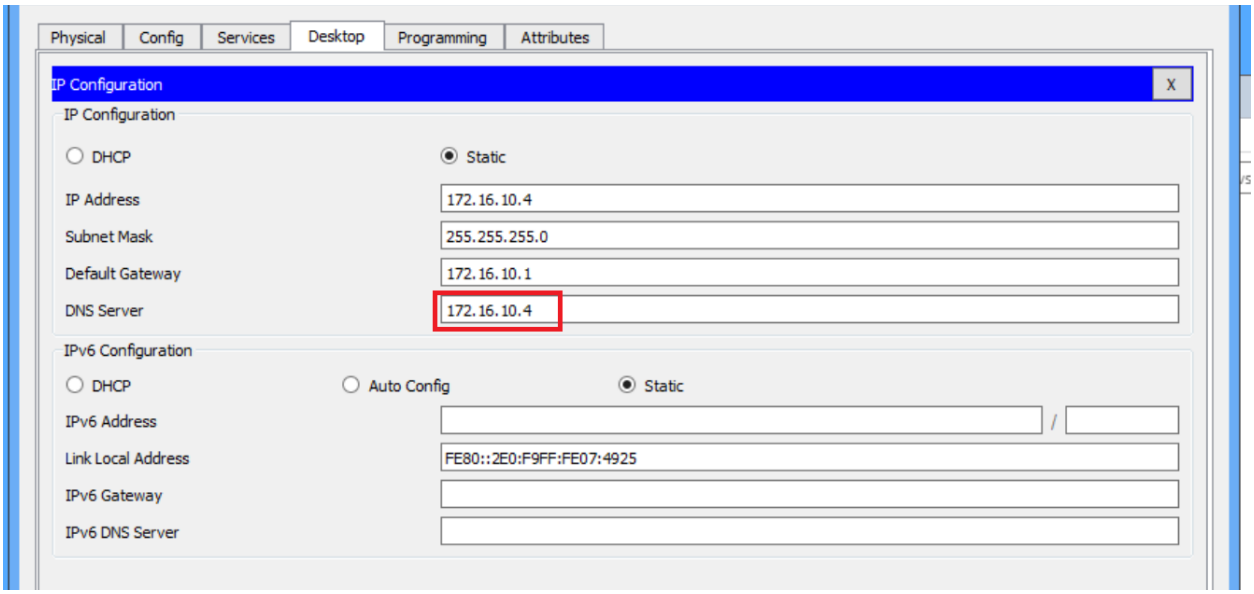
(Diagram 6: cisco packer)

1. From the DNS service we need to enable it and add the new name and insert the IP address into the list. For example, we add www.nws.com with IP address 172.16.10.2 (Webserver IP address).



(Diagram 7)

2. We also need to assign an IP address to the DNS server. For example, 172.16.10.4.



(Diagram 8)

3. From the client side (workstation), we need to add our DNS server IP address in the IP address configuration.

(Diagram 9)

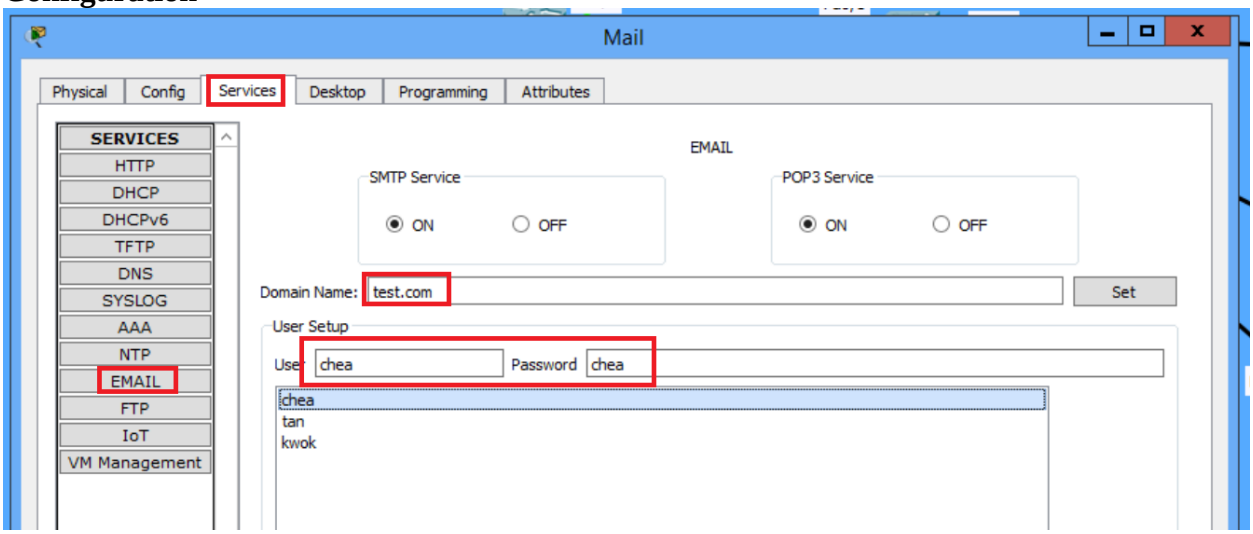
4. Now we can access the website through URL.

4. **Client workstations must be able to check their e-mail on the e-mail server at the DMZ. (Solution and configuration.)**

In case 4, checking and sending email on the email server at the DMZ through the Simple Message Transfer Protocol (SMTP). SMTP is a communication protocol for sending email messages on the internet. SMTP is usually used for sending email, while Post Office Protocol (PoP3) or Internet Message Access Protocol (IMAP) will be perform the task of receiving email. (Bradley, 2018)

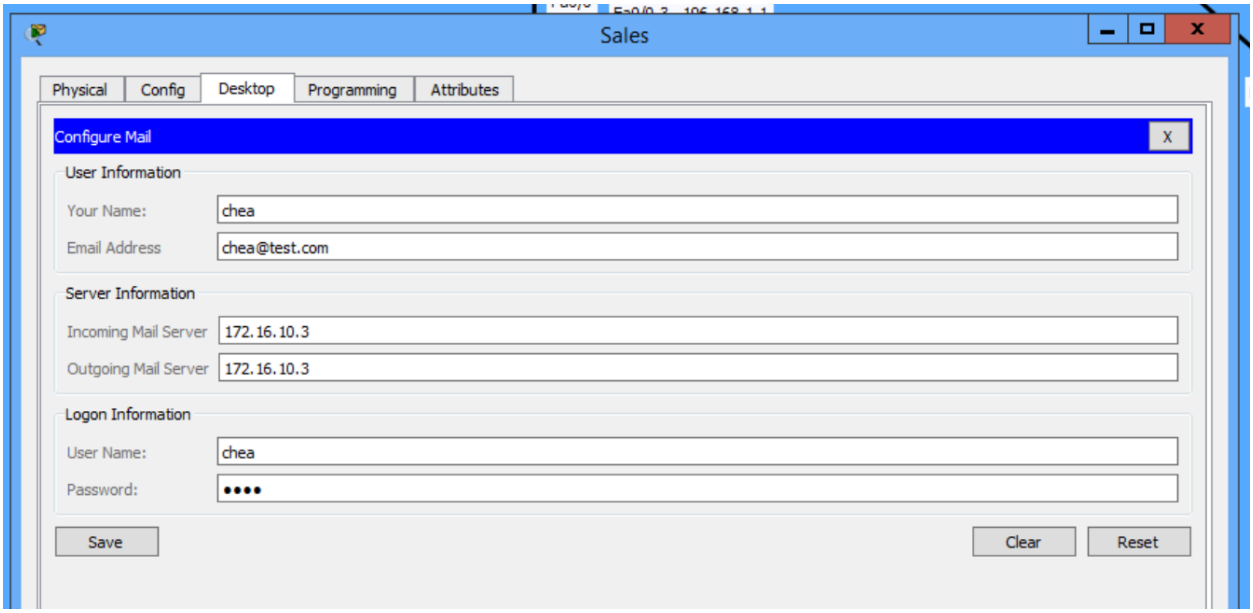
The email server is located inside the DMZ and the client workstations consists of three different department, there are sales department, engineering department and finance department. All the departments are located in the same company in Kuala Lumpur. Each PC in each department must able to send and check their email. (Bradley, 2018)

Configuration



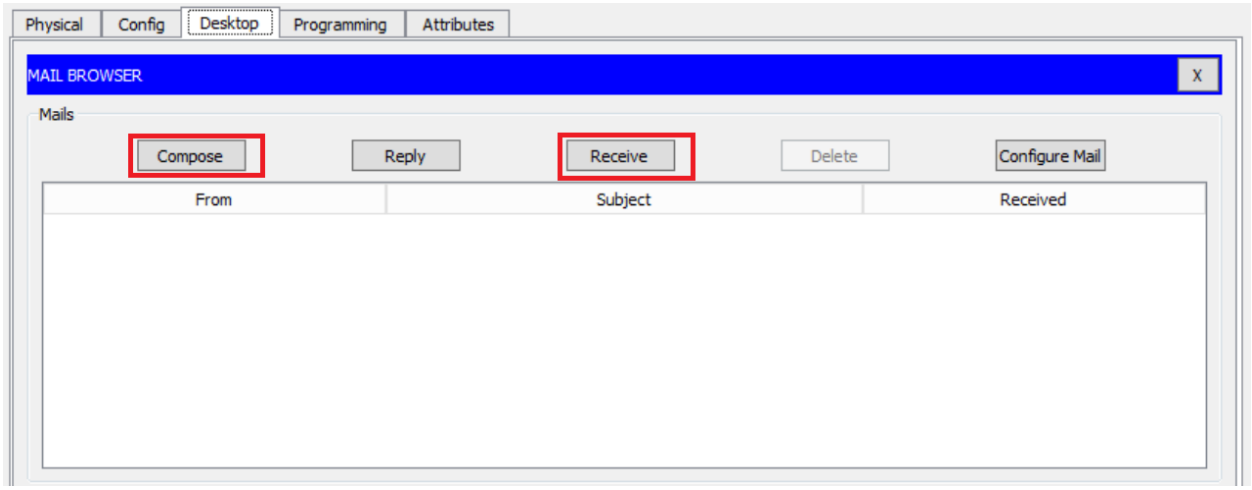
(Diagram 10)

Starting off with the configuration on the email server which is shown in the diagram above. The user needs to go to the email which is located in the services and provide a domain name such as test.com followed with the user setup by providing the username and password. At least two users are required to setup due to one of it is receiver while the second one is sender.



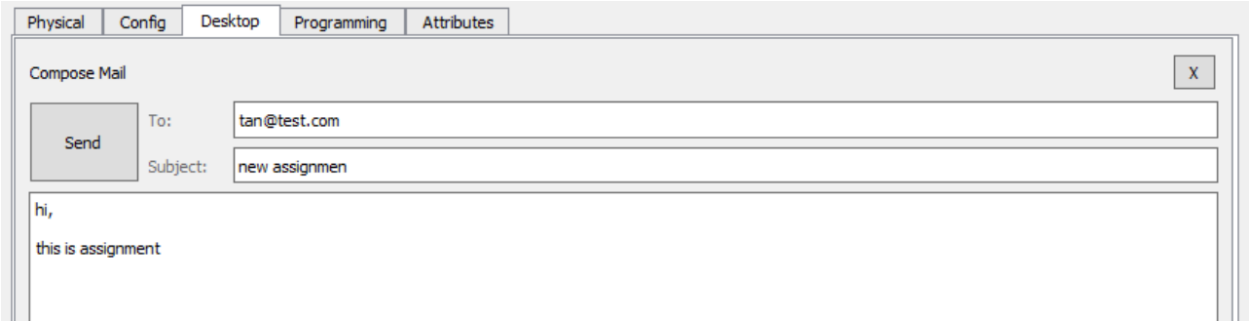
(Diagram 11)

After that, choose two PC and make some configuration on the Email which located in the Desktop section. The user information, server information and login information are required to configure when the PC access the email for the first time. the incoming mail server and the outgoing mail server will be the IP address of the email server.



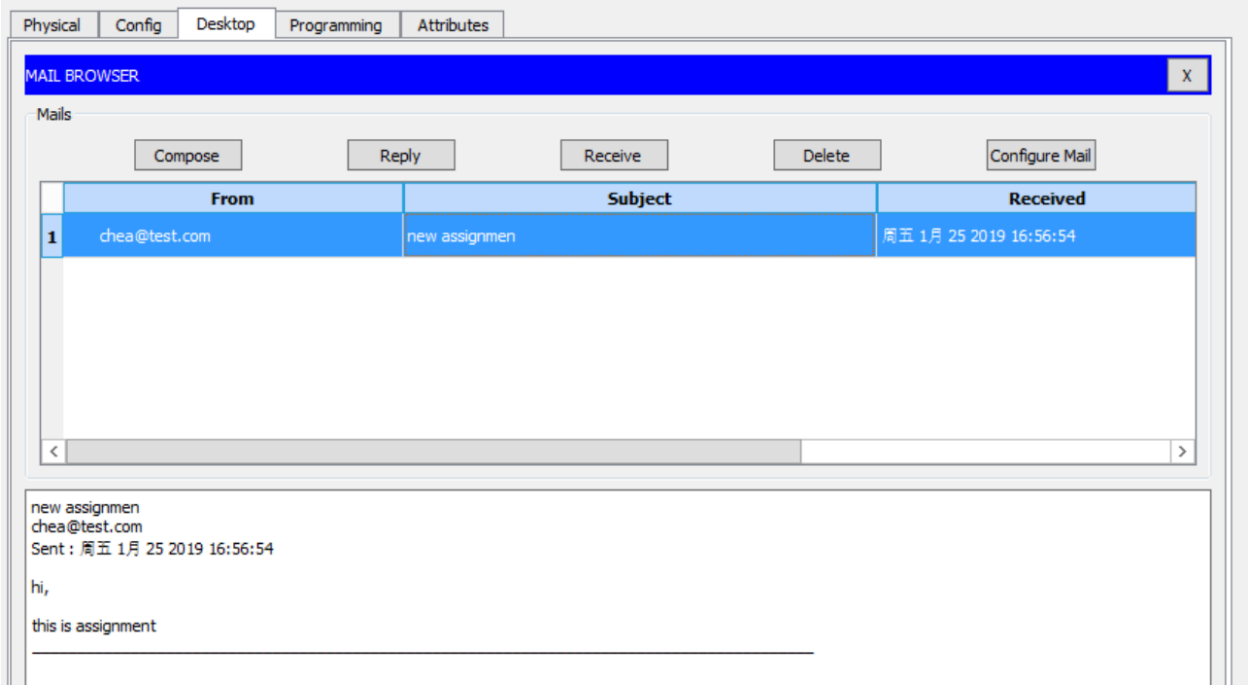
(Diagram 12)

After configuration as mention above is complete, the user will be guide to the mail browser. In the mail browser, the user can compose email, reply email, check received email and delete email but the main function that will be focused in this scenario is compose email and check received email.



(Diagram 13)

The diagram above shows how to compose an email. The recepient email will be the username that have been created previously together with the domain name. The user can just click send email to the recepient once everthing is done.



(Diagram 14)

After successfully send the email, the recipient can check the email by just click on the receive button to refresh the mail browser and the details of the email will be shown at the bottom of the mail browser.

5. **The e-mail server should be able to receive e-mail from external hosts over the simple mail transfer protocol (SMTP). (Solution.)**

Simple Mail Transfer Protocol (SMTP) is a communication protocol for sending email messages on the Internet and I usually used for sending email. Post Office Protocol (POP3) or Internet Message Access Protocol (IMAP) will be perform the task of receiving email. (Bradley, 2018)

To enable external hosts to send e-mail to email server using SMTP, the port of the SMTP in the router must be configured to permit while the other port in the router must be denied to ensure security as there might be external threats or external clients with intentions.

In question 5, the configuration can be made through access list as it could permit or deny specific port such as SMTP, FTP, HTTP. Therefore, the port number of each services should be acknowledged to prevent denying ports that should not be denied in order for the services to operate correctly. (Bradley, 2018)

The mail server to receive email from external hosts over SMTP and POP3 will considered as one of the methods because POP3 works as receiving email and therefore, the email server would able to receive email from the external hosts through this protocol.

6. **No client from sales, engineering and finance department is able to access clients in the other departments. (Solution and configuration.)**

Now, question 6 requirement need to block the workstation of Kuala Lumpur to access each other. The solution to solve this problem is Access Control List (ACL). Access control list is basically like rule for the connection, administrator can define the rules to permit or deny the end user to access some environment. The external Access Control List (ACL) is applied on the source router, it permits or deny the connection (packet) based on source and destination address. (Suman, 2016)

Question 6 have to applied external access control list due to need to specific the source and IP address. Inserted the wildcard mask when applied access control list to the router, wildcard mask is invert of subnet mask and it is use for matching a range IP address in access control list.

Configuration

1. In the source router, we need to add the extended access control list with the following command

```
R2>en
R2#config t
R2#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#access
R2(config)#access-list 100 deny ip 192.168.1.0 0.0.0.255
192.168.2.0 0.0.0.255
R2(config)#
```

(Diagram 15)

Enable Router for entering command.

CLI: en Go for the global configuration mode

CLI: configure terminal Insert the Extended Access Control List (the ID between 100 and 199)

CLI: access-list action(permit or deny) ip [source network id source wildcard mask] [destination network id destination wildcard mask]

For example: access-list 100 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255

2. We need to implement the access control list that we created to the specific interface on the router. In the scenario we have implemented INTER VLAN. So, we need to apply the rules to the logical interface instead of the physical interface

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#in
Router(config)#interface gi
Router(config)#interface gigabitEthernet 0/1.10
Router(config-subif)#ip access-group 100 in
Router(config-subif)#
```

(Diagram 16)

Specified the logical interface that need to apply the access control list

CLI: interface gigabitEthernet [port number]

For example: interface gigabitEthernet 0/1.10 Initiate the rule direction

CLI: ip access-group [ID] [Direction]

For example: ip access-group 100 in

3. We need to apply all the configuration from step 1 to 2 to all the network that need to be block access control (Engineering and Sales Department)

4. We confirm the extended access control list configuration with the following command (outside the configuration terminal of the router).

```
interface GigabitEthernet0/1.10
 encapsulation dot1Q 10
 ip address 192.168.1.1 255.255.255.0
 ip access-group 100 in
!
interface GigabitEthernet0/1.20
 encapsulation dot1Q 20
 ip address 192.168.2.1 255.255.255.0
 ip access-group 101 in
!
interface GigabitEthernet0/1.30
 encapsulation dot1Q 30
 ip address 192.168.3.1 255.255.255.0
 ip access-group 103 in
```

(Diagram 17)

CLI: show run

```
GigabitEthernet0/1.10 is up, line protocol is up (connected)
  Internet address is 192.168.1.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is 100
  Proxy ARP is enabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP Fast switching turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
```

(Diagram 18)

CLI: show ip interface

5. To proof that the access control list working we can try PING from Engineering Department to Sales Department and Finance Department. We will get destination host unreachable result because of we don't have any permission. We also need to confirm the workstation can access the webserver after applied the access control list.

```
FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::2D0:D3FF:FEE0:B32C
   IP Address.....: 192.168.2.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.2.1

C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(Diagram 19)

We need to go for the workstation of the Engineering Department and open Command Prompt to ping to Finance Department workstation.

CLI: ping [ip address]

For example: ping 192.168.1.2

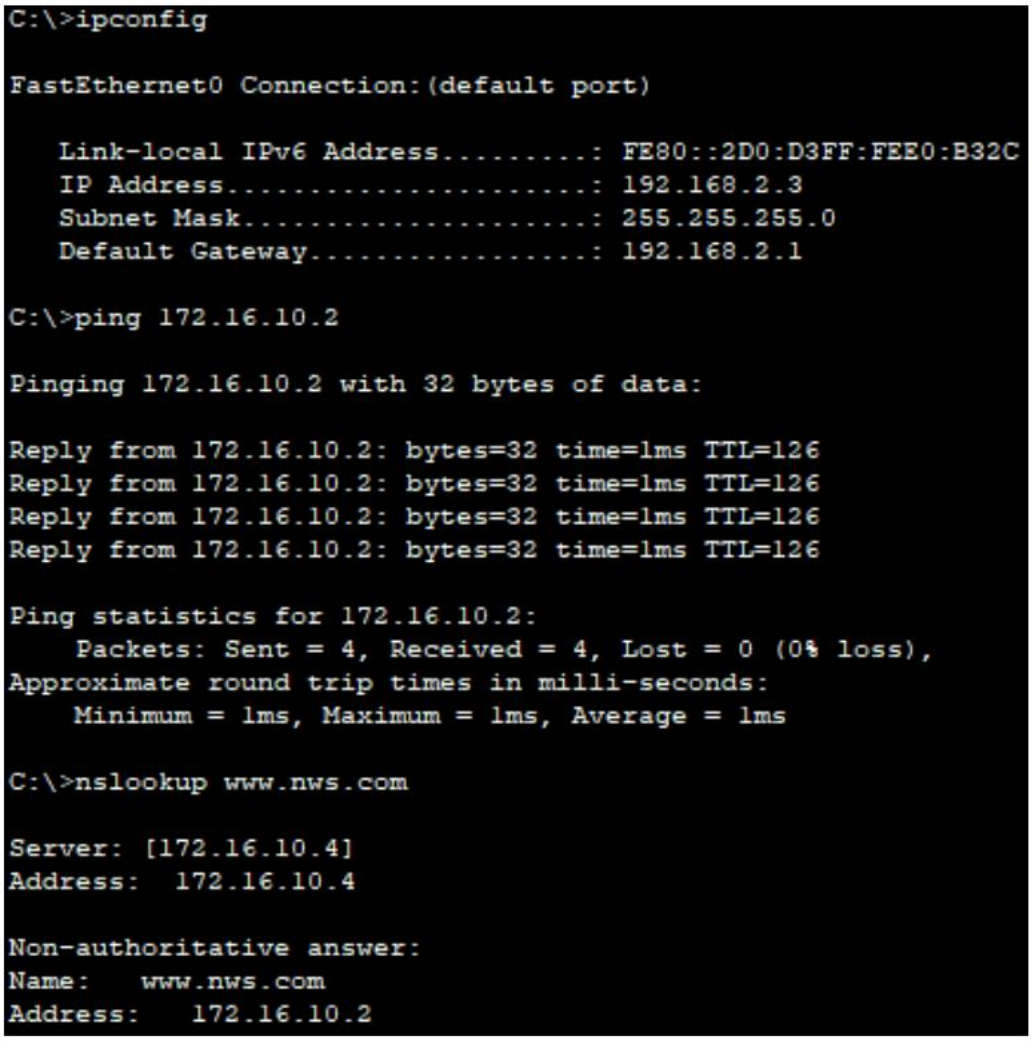
```
FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::2D0:D3FF:FEE0:B32C
   IP Address.....: 192.168.2.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.2.1

C:\>ping 192.168.3.2

Pinging 192.168.3.2 with 32 bytes of data:

Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.
Reply from 192.168.2.1: Destination host unreachable.

Ping statistics for 192.168.3.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(Diagram 20)

We need to go for the workstation of the Engineering Department and open Command Prompt to ping to Sales Department workstation

CLI: ping [ip address]

For example: ping 192.168.3.2



(Diagram 21)

We need to go for the workstation of the Engineering Department and open Command Prompt to ping to webserver and validate the IP address is our webserver with nslookup.

CLI: ping [ip address]

For example: ping 172.16.10.2

CLI: nslookup [domain address]

For example: nslookup www.nws.com

7. **Layer two securities is a requirement in the company-A LAN. (Solution and configuration.)**

The scenario needs to implement Layer 2 security. In OSI network model, layer 2 is data link layer also known as it responsible to transmit data and packet across physical network and it will be touching about the media access control (MAC) address and Logical Link Control (LCC). (Team, 2018) Implement the port security on the switch of each department. In port security, the switch of each department will collect the MAC address at the first time and register it in the switch for the specific port. Any of the Mac address did not register in the switch and to prevent unauthorize people access to internet. (Team, 2018)

Configuration

1. We need to insert the port security to the interface on the switch by using the following command in the configuration terminal.

CLI: interface range FastEthernet port number

For example: interface range FastEthernet 0/2-4

```
S1>en
S1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#in
S1(config)#interface fas
S1(config)#interface ran
S1(config)#interface range fas
S1(config)#interface range fastEthernet 0/2-4
S1(config-if-range)#sw
S1(config-if-range)#switchport po
S1(config-if-range)#switchport port-security
```

2. We need to limit the only one MAC address that register in the switch.

```
S1(config-if-range)#sw
S1(config-if-range)#switchport po
S1(config-if-range)#switchport port-security ma
S1(config-if-range)#switchport port-security maximum 1
S1(config-if-range)#w
S1(config-if-range)#sw
S1(config-if-range)#switchport po
S1(config-if-range)#switchport port-security mac
S1(config-if-range)#switchport port-security mac-address st
S1(config-if-range)#switchport port-security mac-address sticky
```

(Diagram 22)

CLI: switchport port-security maximum number

For example: switchport port-security maximum 1

CLI: switchport port-security mac-address action

For example: switchport port-security mac-address sticky

3. After configured the register MAC address into the switch, we need to restrict others MAC address to connect to the internet.

```
Switch(config-if-range)#switchport port-security violation rest
Switch(config-if-range)#switchport port-security violation
restrict
```

(Diagram 23)

CLI: switchport port-security violation action
For example: switchport port-security violation restrict

4. After implement the port security to the relevant port, we need to shut other unused port down.

```
Switch(config)#interface range fastEthernet 0/5-24
Switch(config-if-range)#shutdown

%LINK-5-CHANGED: Interface FastEthernet0/5, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/6, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/7, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/8, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/9, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/10, changed state to
administratively down

%LINK-5-CHANGED: Interface FastEthernet0/11, changed state to
administratively down
```

(Diagram 24)

CLI: interface range fastEthernet port number

For example: interface range fastEthernet 0/5-24
CLI: shutdown

8. **Bastion host works as an application proxy. You are required to explain the solution in detail. (Configuration is not required.)**

Some companies or organizations typically use proxy servers to improve network performance. Therefore, the proxy fee server becomes the medium for the client to connect to the Internet. System administrators can configure to allow or restrict specific protocols. The most common protocols are HTTP and HTTPS. It has good network defense and good encryption performance. When a client is operating on a proxy server, the system administrator can define a list of sites within the proxy server to prevent clients from accessing it. (Team, 2018) At the same time, the proxy server also saves browsing sites that are cached in local storage, so if the client accesses the same website, the Internet performance will be better. For example, jayden browsed www.youtube.com at 12 o'clock and TAN visited the same website at 10 o'clock, so TAN would get the website from the proxy server cache instead of Youtube's web server. (Tulley, 2018)

The bastion host is a dedicated computer located in the demilitarized zone (DMZ). The bastion host needs to be accessible from outside the network. It is often placed between internal and external firewalls. It is like a filter that monitors network traffic. For example, the bastion host is Mail, Domain Name System (DNS), Web and File Transfer Protocol (FTP). The bastion host can also act as a firewall and router, so it also has the dual functions of monitoring and protection. (Gremban, 2017)

The base host acts as the user's application proxy, which users can access outside the company, and all traffic can be logged in to the company's local storage. The bastion host can also have the same functionality as the proxy server. System administrators can define rules that allow or deny certain network activities. For example, a system administrator can restrict users from accessing File Transfer Protocol (FTP) to prevent users from changing content on the server. If the cache memory exists, the application will load faster. It is similar to a proxy server because the previous

user has previously browsed the same website, so the cache will be saved on the server and the next user will request the same page, which will be loaded from the proxy server instead of the original web server.

9. **Connectivity between company-A in Kuala Lumpur and company-B in Singapore is a requirement. What is the best solution? Elaborate on the solution. (Configuration is not required)**

10. **Data transmitted over the network must be kept disguised and only intended recipient can read it. Hackers are unable to understand the content even they are able to wiretap the communication. (Solution on the techniques, no configuration is required)**

According to the trend of modern science and technology, in this era, there are many illegal organizations or hackers who continue to carry out cyber security attacks for the sake of interest. Such attacks are becoming more and more powerful every day, and hackers simply transmit information transmitted online from one the place sneaked another place. When sensitive information transmitted across a company is crossed or leaked by an attacker, this will result in the disclosure of corporate network security and theft of confidential information, as it can result in significant loss of financial or reputational or trust to the customer or employee. (Gremban, 2017) Therefore, a secure but stable connection must be established to ensure that sensitive information being transmitted is inaccessible to hackers or encapsulated by adding encrypted content.

At the same time, many large organizations or methods currently in use in the market will be introduced and implemented to protect network security, and it is a VPN or virtual private network. Today, there are so many organizations that use VPN because it provides the ability to create secure and encrypted connections over the Internet, but this is a less secure network that can be exposed to many external threats, thus creating many network security issues. (Gremban, 2017) From a basic point of view, it extends the private network on the public network so that the users of company A actually belong to the same private network as the private networks in company B hundreds of kilometers away. In order to ensure the security of the network, the data will basically be tunneled, and the authentication method will also be used to ensure the true

identity of the user. For example, passwords, tokens, etc. Whenever a VPN client is started on a computer, the computer performs a trusted key exchange with the remote server (Rouse, 2018). Now, before entering the implementation location, it is important to consider the encryption on the VPN and the very important process of protecting the data and files transmitted over the mobile. Internet Protocol Security Protocol or IPSEC is used to protect traffic on IP networks and its function is to encrypt data between two devices, so only the target can view or understand the content held within the packet. It uses two types of sub-protocols to protect packets classified as encapsulated secure payloads or (ESP) and authenticated. Title or (AH). The main task of Tys is to use symmetric key encryption to transmit data, and the authentication header is responsible for modifying all hash operations of the packet header, so specific packet information will not be visible when transmitted to the destination. As a result, applications that use VPNs over the network benefit from the capabilities of a private network, ensuring network security and management while ensuring that data security is not compromised. (Rouse, 2018)

In order to achieve this function, a secure VPN tunnel can be implemented between the firewalls of company A and company B. For example, after the firewall, the data packet will reach the Internet containing many external threats, and the implementation of secure VPN tunnel rights will be behind the firewall. Ensure that information transmitted from the source to the destination is encapsulated and encrypted and can only be unlocked by its legal owner or recipient. (Tyson, 2011)

11. The company requires implementing intrusion detection systems (IDS). (No Configuration is required.)

Deciding to discuss the location of the intrusion detection system in the network topology itself, you must first understand the definition of network security and how to accurately detect the malicious activity and malware or any violation of computer security policies, acceptable usage policies or standards. Security practice. Assume that it is found in network traffic or in a computer system. If any malicious activity, malware or any offending signature matches the IDS database, how should the notification be sent to the network administrator and the suspicious activity is notified, then the network administrator can analyze it and stop and patch it in time This kind of activity can be prevented from happening again. (Scarfone, 2015)

After discussing the definition of network security, you can see the importance of IDS system in network security. For example, IDS system implements IDS system in a company network topology, which can prevent suspicious malware attacks or prevent violations. The rules set by the company. However, the location cannot be placed at will, because the IDS system's sensors are costly and difficult to configure, and IDS systems can easily trigger false positives and can cause legitimate traffic to be blocked, which can slow down the company's business processes and cause potential losses. The system is unreliable and network administrators also collect and analyze information in a time-consuming manner. Therefore, a strategic location should be set to reduce the maximum capacity of false alarms and reduce costs and time by implementing only a sufficient number of sensors. (Scarfone, 2015)

The best place to assign an IDS system and its sensors is behind the firewall but before the DMZ. The reason for implementing it behind a firewall is that because the IDS system can easily trigger false positives as described above, the firewall should filter all unnecessary packets into the DMZ and allow the IDS to check the remaining approved packets. Assigning on the DMZ will give the network administrator enough time to analyze the error and determine if it is a legitimate attack along with the severity of the attack, as if the IDS was assigned next to the internal network, stopping the legitimate attack while collecting the relevant attacks. More information about the source and the attack itself, but in order to take full advantage of IDS, priority should be given to preventive thinking rather than incident response.

12. **Implement VPN between Singapore and Kuala Lumpur. (Configuration is required.)**

Given the issues mentioned in questions 9 and 10, we can determine that the implementation of a VPN or virtual private network is definitely beneficial to the company or organization in terms of communication between the two authenticators, as it will be provided by applying encapsulation and encryption together. A protected and secure tunnel. Therefore, we recommend establishing a VPN tunnel between Singapore and Kuala Lumpur, and an Internet Protocol (IPSec) will be set up in the project, which will authenticate and encrypt each IP packet transmitted. (GZaetz, 2017)

On the other hand, before performing any configuration on the IPSec VPN tunnel, you must first configure an access list between the sender and receiver of the packet between the Internet, in which case it is two firewalls. Complete the access control list to allow traffic or matching traffic through the tunnel. At the same time, the ISAKMP policy and the ISAKMP key must be configured because it will define the process and packet format of the security association, which is a one-way relationship between the sender and the receiver. After the setup is complete, the ISAKMP conversion set should be set up. It is basically a set of protocols and algorithms specified on the gateway to protect data. (GZaetz, 2017). It consists of three factors, namely data encryption, data authentication and encapsulation mode. Once everything is configured, you can perform a crypto map and then bind everything together and allow it to be created and applied.

In the end, the conversion set consists of three factors, namely data encryption, data validation and encapsulation mode, so their use and why they are used have become a more secure recommendation for Kuala Lumpur and Singapore. One of the two VPN protocols used in this project is to encapsulate the security payload, and the reason for using it on the authentication header is because it provides a huge advantage in data encryption, which will ensure more secure data transmission and information security. (GZaetz, 2017).

Then, according to Cisco's Encryption Algorithm Configuration Guide, it is highly recommended to use the Advanced Encryption Standard or (AES) as the encryption algorithm. Therefore, AES will be used as a symmetric key in ESP so that authenticated parties encrypt and decrypt data before exchange. Use SHA-HMAC instead of MD5-HMAC because it is more secure than the usual MD5 because it produces a larger hash value.

13. Implement SSL encryption between Singapore and Kuala Lumpur. (Solution)

Hypertext Transfer Protocol (HTTP) is a protocol for communicating between a web server and a client on the web, and the communication is performed without any encryption, which allows for easy viewing during a wiretapping attack. Data that has been transferred between the server and the client has occurred. Therefore, it is important to implement Secure Sockets Layer (SSL) before Transport Layer Security (TLS). (Global Sign, 2018) Both protocols are cryptographic protocols that ensure communication security between clients so that the connection between the

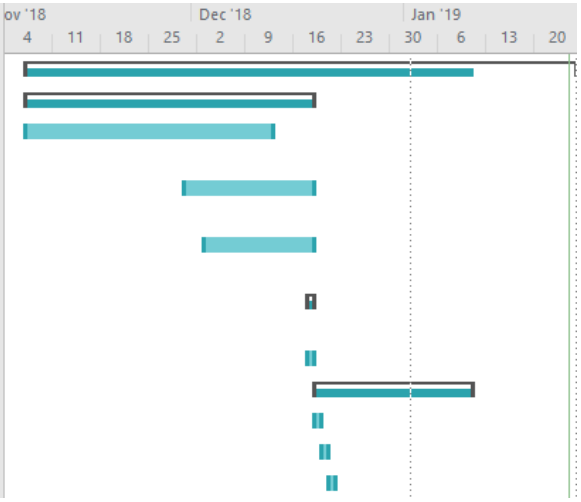
two devices is secure on the Internet. However, even if the SSL protocol is not recommended and the TLS protocol is not recommended, most people will still refer to SSL technology. If the website is implemented using the SSL protocol, the URL will be changed from HTTP to HTTPS, and the padlock symbol will be displayed in front of the URL of the browser used by the user.

Before implementing SSL, users need to obtain an SSL certificate, which is a digital certificate from a Certificate Authority (CA). The purpose of this certificate is to provide a secure session between the client and the server over an SSL connection. If there is no SSL certificate, a secure connection will not be established. Then we will explain the basic operation of SSL work. First, the client will use SSL protection to send a request to the server to identify itself. The server then sends the encrypted public key or certificate back to the client. The client will check if it is trusted. If the client chooses to trust the certificate, a message or encryption key is sent back to the server to confirm the server. If the client does not trust the certificate, the communication will fail. When the server receives an acknowledgment from the client, the server will send back a digitally signed acknowledgment to initiate an SSL encrypted session, and the encrypted data will be shared between the client and the server.

In the end, with the implementation of SSL, it will provide a secure environment for sharing information between companies in Kuala Lumpur and Singapore and ensure that data is more secure because information and data are encrypted.

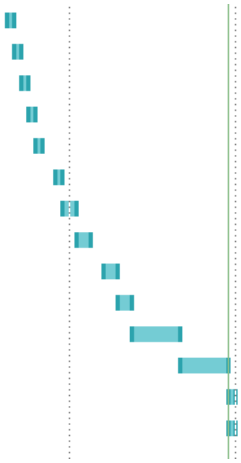
Gantt Chart

	Task Name	Duratic	Start	Finish
1	**network Security**	**58 days?**	**Wed 11/7/18**	**Fri 1/25/19**
2	**Individual Components**	**30 days**	**Wed 11/7/18**	**Tue 12/18/18**
3	Intrusion Prevention System	26 days	Wed 11/7/18	Wed 12/12/18
4	Privacy Network Security	13 days	Fri 11/30/18	Tue 12/18/18
5	Prevention Denail of Secvice	12 days	Mon 12/3/18	Tue 12/18/18
6	**Group Components Introduction**	**1 day**	**Tue 12/18/18**	**Tue 12/18/18**
7	Introduction	1 day	Tue 12/18/18	Tue 12/18/18
8	**Cisco Packet Tracer**	**17 days?**	**Wed 12/19/18**	**Thu 1/10/19**
9	Chapter 1	1 day	Wed 12/19/18	Wed 12/19/18
10	Chapter 2	1 day	Thu 12/20/18	Thu 12/20/18
11	Chapter 3	1 day	Fri 12/21/18	Fri 12/21/18



(Figure 1: Gantt chart)

12	Chapter 4	1 day	Mon 12/24/18	Mon 12/24/18
13	Chapter 5	1 day	Tue 12/25/18	Tue 12/25/18
14	Chapter 6	1 day	Wed 12/26/18	Wed 12/26/18
15	Chapter 7	1 day	Thu 12/27/18	Thu 12/27/18
16	Chapter 8	1 day	Fri 12/28/18	Fri 12/28/18
17	Chapter 9	1 day	Mon 12/31/18	Mon 12/31/18
18	Chapter 10	2 days	Tue 1/1/19	Wed 1/2/19
19	Chapter 11	2 days	Thu 1/3/19	Fri 1/4/19
20	Chapter 12	2 days	Mon 1/7/19	Tue 1/8/19
21	Chapter 13	2 days	Wed 1/9/19	Thu 1/10/19
22	Recommendation	5 days	Fri 1/11/19	Thu 1/17/19
23	Network configurations	5 days	Fri 1/18/19	Thu 1/24/19
24	Conclusion	1 day	Fri 1/25/19	Fri 1/25/19
25	References	1 day	Fri 1/25/19	Fri 1/25/19



(Figure 2: Gantt chart)

References (Guo Jun Hao-Privacy Network Security (PNS))

1. laurenpoussard | creativestudio. (2019). *When in doubt - CALL ME - or secure your privacy settings - laurenpoussard | creativestudio*. [online] Available at: https://laurenpoussard.com/doubt-call-secure-privacy-settings/ [Accessed 24 Jan. 2019].
2. Krishnan, R. (2019). *Comodo's so-called 'Secure Internet Browser' Comes with Disabled Security Features*. [online] The Hacker News. Available at: https://thehackernews.com/2016/02/comodo-web-browser-security.html [Accessed 24 Jan. 2019].
3. OpenLearn. (2019). *Network security*. [online] Available at: https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-0 [Accessed 24 Jan. 2019].
4. Chamberagent.com. (2019). *Network Security & Privacy*. [online] Available at: http://www.chamberagent.com/products_business_network_security.asp [Accessed 24 Jan. 2019].
5. Secure2.mearie.ca. (2019). *Privacy, Cyber & Network Security*. [online] Available at: https://secure2.mearie.ca/imis15/MG/products/Commercial_Insurance/Privacy__Cyber__Network_Security_/MG/Products_M/Comm_Ins/Privacy__Cyber___Network_Security_.aspx?hkey=f1dc643b-a0bc-4635-b9ac-f4d3478e585e [Accessed 24 Jan. 2019].
6. Privacyinternational.org. (2019). *Privacy International | International Network*. [online] Available at: https://privacyinternational.org/partners [Accessed 24 Jan. 2019].
7. Support.symantec.com. (2019). *How Symantec Network Access Control works*. [online] Available at: https://support.symantec.com/en_US/article.HOWTO81731.html [Accessed 24 Jan. 2019].
8. Snyder, J. (2019). *Network access control authentication: Are you ready for 802.1X?*. [online] Computerworld. Available at: https://www.computerworld.com/article/2519270/security0/network-access-control-authentication--are-you-ready-for-802-1x-.html [Accessed 24 Jan. 2019].
9. Bordoni, S. (2019). *The importance of maintaining cyber security in your business*. [online] IT Pro Portal. Available at: https://www.itproportal.com/features/the-importance-of-maintaining-cyber-security-in-your-business/ [Accessed 24 Jan. 2019].

References (Intrusion Prevention System (IPS))

10. Techopedia.com. (2018). *What is an Intrusion Prevention System (IPS)? - Definition from Techopedia*. [online] Available at: https://www.techopedia.com/definition/15998/intrusion-prevention-system-ips [Accessed 29 Dec. 2018].
11. Harvey, C. (2018). *Intrusion Prevention Systems: Securing Your Network from Attacks*. [online] Esecurityplanet.com. Available at: https://www.esecurityplanet.com/network-security/intrusion-prevention-systems.html [Accessed 29 Dec. 2018].
12. WhatIs.com. (2018). *What is WIPS (wireless intrusion prevention system)? - Definition from WhatIs.com*. [online] Available at: https://whatis.techtarget.com/definition/WIPS-wireless-intrusion-prevention-system [Accessed 29 Dec. 2018].
13. Techopedia.com. (2019). *What is Network Behavior Analysis (NBA)? - Definition from Techopedia*. [online] Available at: https://www.techopedia.com/definition/16118/network-behavior-analysis-nba [Accessed 12 Jan. 2019].
14. Techopedia.com. (2019). *What is a Host-Based Intrusion Prevention System (HIPS)? - Definition from Techopedia*. [online] Available at: https://www.techopedia.com/definition/4290/host-based-intrusion-prevention-system-hips [Accessed 12 Jan. 2019].
15. Webopedia.com. (2019). *The 7 Layers of the OSI Model - Webopedia Study Guide*. [online] Available at: https://www.webopedia.com/quick_ref/OSI_Layers.asp [Accessed 12 Jan. 2019].
16. Spiceworks, I. (2019). *Tips for Implementing Your IDS/IPS*. [online] The Spiceworks Community. Available at: https://community.spiceworks.com/networking/articles/2471-tips-for-implementing-your-ids-ips [Accessed 12 Jan. 2019].
17. Anon, (2019). [online] Available at: https://www.techwalla.com/articles/the-disadvantages-of-intrusion-detection-systems [Accessed 12 Jan. 2019].
18. InfoSec Resources. (2019). *Network Design: Firewall, IDS/IPS*. [online] Available at: https://resources.infosecinstitute.com/network-design-firewall-idsips/#gref [Accessed 12 Jan. 2019].

References (DDos Prevention)

Anon., n.d. [Online]
Available at: Techopedia.com. (2018). What is an Intrusion Prevention System (IPS)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/15998/intrusion-prevention-system-ips [Accessed 29 Dec. 2018].

K, R., 2011. *An Introduction to DDoS.* [Online]
Available at: https://www.excitingip.com/1500/an-introduction-to-ddos-distributed-denial-of-service-attack/
[Accessed 20 1 2019].

Allot, 2018. *Inline DDoS Protection versus Scrubbing Center Solutions.* [Online]
Available at: https://www.allot.com/resources/SB-DDoS-Protection-inline-vs-scrubbing.pdf
[Accessed 21 1 2019].

Toms, L., 2016. *The Impact of Denial of Service Attacks.* [Online]
Available at: https://www.globalsign.com/en/blog/denial-of-service-in-the-iot/
[Accessed 21 1 2019].

apriorit, 2018. *Modern DDoS Protection Techniques: An Overview.* [Online]
Available at: https://www.apriorit.com/dev-blog/559-ddos-protection-techniques
apriorit, 2018. *Modern DDoS Protection Techniques: An Overview.* [Online]
Available at: https://www.apriorit.com/dev-blog/559-ddos-protection-techniques
[Accessed 21 1 2019].

BENNETT, A., 2017. *20 Ways to Prevent a Deadly DDoS Attack.* [Online]
Available at: https://techspective.net/2017/05/11/20-ways-prevent-deadly-ddos-attack/
[Accessed 22 1 2019].

Kohout, J., 2018. *How DDoS Attacks Can Sink Your Business · TeskaLabs Blog.* [Online]
Available at: https://teskalabs.com/blog/how-ddos-can-sink-your-business
[Accessed 22 1 2019].

References (Section B)

Commodo, 2017. What is Website Security. [Online] Available at: https://blog.comodo.com/web-security/what-is-website-security/ [Accessed 1 October 2018].

Connectify, 2016. Is there a limit to the number of clients on my Hotspot?. [Online] Available at: https://support.connectify.me/article/18-is-there-a-limit-to-the-number-of-clients-onmy-hotspot

Dargin, M., 2017. How to protect your data when using public Wi-Fi. [Online] Available at: https://www.networkworld.com/article/3194005/mobile-wireless/how-to-protectyour-data-when-using-public-wi-fi.html

Pinola, M., 2018. Life Wire. [Online] Available at: https://www.lifewire.com/rooting-and-jailbreaking-your-phone-or-tablet-2377406 [Accessed 10 9 2018].

Poole, I., 2018. Radio Electronic. [Online] Available at: https://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standardstutorial.php [Accessed 16 8 2018].

Publico, R., 2017. Global Sign. [Online] Available at: https://www.globalsign.com/en/blog/how-to-spot-a-fake-website/ [Accessed 3 10 2018].

Raphael, J., 2017. CSOOnline. [Online] Available at: https://www.csoonline.com/article/3241727/mobile-security/5-mobile-securitythreats-you-should-take-seriously-in-2018.html [Accessed 2 8 2018].

Rapid7, 2018. Man-in-the-Middle (MITM) Attacks. [Online] Available at: https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/ [Accessed 5 October 2018].

Rapid7, 2018. Phishing Attack. [Online] Available at: https://www.rapid7.com/fundamentals/phishing-attacks/ [Accessed 5 October 2018].

Rapid7, 2018. SQL Injection Attacks (SQLi). [Online] Available at: https://www.rapid7.com/fundamentals/sql-injection-attacks/ [Accessed 6 October 2018].

Dolly, J., 2018. Why you should never, ever connect to public WiFi. [Online] Available at: https://www.csoonline.com/article/3246984/wi-fi/why-you-should-never-everconnect-to-public-wifi.html

edGY, 2013. Mobile Hotspot in Malaysia: An Overview of Portable WiFi Services. [Online] Available at: https://www.expatgo.com/my/2013/08/25/mifi-malaysia/

Ed, H., 2018. Microsoft Takes Top Spot in Inaugural Phishers' Favorites Top 25 List. [Online] Available at: https://www.vadesecure.com/en/phishers-favorites-q2-2018/ [Accessed 5 October 2018].

Fruhlinger, J., 2018. CSOOnline. [Online] Available at: https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this

cyber-attack-works-and-how-to-prevent-it.html [Accessed 15 8 2018].
Global Sign, 2018. What is SSL?. [Online] Available at: https://www.globalsign.com/en/ssl-information-center/what-is-ssl/ [Accessed 6 October 2018]

Ibrahim, T., Furnell, S. M., Papadaki, M. & Clarke, N. L., 2008. Assessing the challenges of Intrusion Detection Systems. University of plymouth, pp. 1-11.

Jessica, O., 2018. The SiteLock Website Security Insider 2018. [Online] Available at: https://www.sitelock.com/blog/2018/09/website-security-insider-q2-2018/ [Accessed 1 October 2018].

Josh , F., 2018. What is phishing? How this cyber attack works and how to prevent it. [Online] Available at: https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-thiscyber-attack-works-and-how-to-prevent-it.html [Accessed 5 October 2018].

Joyce, T., 2018. Why do I need website security?. [Online] Available at: https://www.sitelock.com/blog/2018/07/why-do-i-need-website-security/ [Accessed 1 October 2018].

Support, 2018. What is HTTP?. [Online] Available at: https://www.pickaweb.co.uk/kb/what-is-http/ [Accessed 10 10 2018].

Team, C., 2018. Cisco. [Online] Available at: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/122/25ew/configuration/guide/conf/port_sec.html [Accessed 5 9 2018].

Team, G., 2018. Google. [Online] Available at: https://cloud.google.com/load-balancing/docs/ssl-certificates [Accessed 3 10 2018].

Team, J., 2018. Juniper Networks. [Online] Available at: https://www.juniper.net/documentation/en_US/junos/topics/concept/interfacesecurity-data-link-layer-understanding.html [Accessed 3 9 2018].

Team, K., 2018. Kapersky. [Online] Available at: https://www.kaspersky.com/resource-center/threats/top-seven-mobile-securitythreats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store [Accessed 25 8 2018].

Team, K., 2018. Kapersky. [Online] Available at: https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks [Accessed 12 9 2018].

Justin , P., 2016. WTF is FTP? The file transfer protocol, explained. [Online] Available at: https://www.digitaltrends.com/computing/what-is-ftp-and-how-do-i-use-it/ [Accessed 8 October 2018].

Khandelwal, S., 2018. The Hacker News. [Online] Available at: https://thehackernews.com/2018/06/4g-lte-network-hacking.html [Accessed 6 8 2018].

Mullins, M., 2014. Lock IT Down: Implementing an intrusion detection system on your network. [Online] Available at: https://www.techrepublic.com/article/lock-it-down-implementing-an-intrusiondetection-system-on-your-network/ [Accessed 5 10 2018].

Team, W., 2018. Webroot. [Online] Available at: https://www.webroot.com/us/en/resources/tips-articles/how-to-prevent-phonehacking-and-sleep-like-a-baby-again [Accessed 6 10 2018].

The Blog, 2018. 2017 Statistics about Web-based Attacks, Mobile Attacks, Data Breaches…. [Online] Available at: https://www.vaadata.com/blog/2017-statistics-web-based-attacks-mobile/ [Accessed 4 10 2018].

Tulley, J., 2018. 2012. [Online] Available at: https://blog.icorps.com/bid/120002/Understand-What-a-Bastion-Hosts-is-From-an-ITConsultant [Accessed 6 9 2018].

Tyson, J., 2011. How VPNs Work. [Online] Available at: https://computer.howstuffworks.com/vpn.htm [Accessed 10 10 2018].

Veracode Solutions, 2018. Man-in-the-middle (MITM) attack. [Online] Available at: https://www.veracode.com/security/man-middle-attack [Accessed 4 October 2018].

Marking Scheme

		Group (40%)				**Individual (60%)**				
	Names and TP number	Documentation (10)	Referencing (10)	Research and Investigation (10)	Diagram/Figures (10)	Critical Thinking and Applicability (20)	Analytical (20)	Configurations (10)	Presentations (10)	**Grand Total (100)**
1	Guo Jun Hao TP046636									
2	Tan Yik Ern TP046566									
3	Chea Yan Shaw TP045215									

Marking Scheme Rubrics

	1 to 3	4 to 7	8 to 10
Documentation (10)	All submission requirements were not adhered or poor writing or poor quality of contents.	All submission requirements were followed with well writing and proper formatting of document along with proper quality of the content.	All submission requirements were followed with very good writing and formatting. The quality of the content is very good. The document looks like a real world solution.
	1 to 3	4 to 7	8 to 10
Referencing (10)	None, very little, or wrong usage of citation or not following proper referencing format.	Proper, well formatted referencing with needed citations in all required places. Including needed copyright sign for used software.	Proper, well formatted referencing with needed citations in all required places. Including needed copyright sign for used software and terms with proper referencing for each one. Using a right bibliography
	1 to 3	4 to 7	8 to 10
Research and Investigation (10)	Poor research and investigation of the problem. Poor evaluation of the requirement.	Well research and investigation is done. Good evaluation of the requirements with proper reasoning with proper project planning and management.	Very well analysis and investigation of the problem. Outstanding evaluation of the requirements with proper reasoning. Outstanding project planning and management with the screenshots of used tools.

	1 to 3	4 to 7	8 to 10
Diagrams / Figures (10)	Failed to attach any diagrams and figures. Descriptions of diagrams are blurring.	Few diagrams and figures attached. Diagrams are lack of descriptions and labeling.	Proper and relevant diagrams and figures. Diagrams are labeled and well described. Sequence of diagrams is well organized.

	1 to 5	6 to 10	11 to 15	16 to 20
Critical Thinking and Applicability (20)	The judgment criteria are not relevant and the solution is not applicable.	The judgment is somehow relevant. The solution is applicable though it lacks in some parts.	The judgment is relevant.The solution is relevant though it lack of supporting factors.	Provided relevant criteria for making the judgment. Applicable methods or techniques are used for forming the judgment.
	1 to 5	6 to 10	11 to 15	16 to 20
Analytical (20)	Very poor or minimal analysis of the problem is done.	Analysis done with lack of tools and techniques. Insufficient descriptions on analysis results	Analysis is accurate and good use of the analysis tools and technique is made	Excellent analysis of the solution has been done. Proper usage of tools in analyzing and testing the accuracy of the solution.

	1 to 3	4 to 7	8 to 10
Configurations (10)	Failed to configure the required devices.	Partial configuration is done; some of the devices are not configured properly. The documentation of the configured devices is not complete.	Proper and full configuration of all of the devices with complete documentation of the configured devices.
	1 to 3	4 to 7	8 to 10
Presentations (10)	Fail to attend the presentations. Voice is hardly to be heard.	Attended presentation but voice is hard to be heard. Able to answer question but failed to	Attended presentation and able to attract audience's attentions. Voice is clear and loud. Able to answer

	Unable to answer questions	produce confirmed answers	all the questions without referring to notes.