LO 1: Examine network security principles, protocols and standards.

P1 Discuss the different types of network security devices.

Introduction to Network Security

Network security is the act of defending computer networks against any unauthorized access, misuse, malfunction, alteration, destruction, or inappropriate exposure. It entails enforcing policies, processes and technologies to make sure that organizational data and systems are not at risk due to internal and external attacks.

I am a Network Security Engineer at Myanmar Tech Solutions (MTS), which growing technology firm with its main office in Yangon and planning to expand a new branch office in Naypyidaw. During the company expansion, it encounters more cybersecurity issues, including unauthorized access, data breach, and derailment of key business processes.

To deal with these risks, I will create and establish a secure network infrastructure that will guard confidential information, facilitating secure communication among branches and facilitating streamlined departmental activities. This will entail installation of necessary network security equipment like firewalls, intrusion protection and prevention, secure routers, VPNs and VLAN enabled switches. These technologies will collaborate to protect the financial information, customer information, and in-house communication both internally and externally. This report will give an analysis of the principle of network security, protocols, devices and cryptography techniques and how they contribute towards the development of a secure and reliable network framework of MTS.

Importance of Network Security in Organizations

Network security is of high importance to a company such as Myanmar Tech Solutions (MTS) that is expanding since sensitive financial data, customer data, and internal communications should be secure against cyberattacks. Lack of appropriate protection, may lead to disruption of day-to-day operations, loss of finances or the reputation of the company.

Goals of Network Security (CIA Triad)

The key goals of network security are based on CIA triad. The confidentiality can be exploited to ensure that the information is only accessed by authorized users. Integrity will make certain that the data is correct and consistent and that no person will alter the information. Availability is the provision of systems and resources at the time of need. Focusing on these principles, MTS will have an opportunity to establish a secure and resilient IT infrastructure to support its growth and minimize the risks of cybersecurity.

Key Principles of Network Security

The key concepts used in the network security form the fundamentals of prevention of the information systems being compromised by the unauthorized individuals, malicious individuals or even by disruption. These principles ensure the networks are not just operational but they are also resistant to internal and external attacks. To make strong defense, organizations can focus on such aspects as verifying the identities of the user, access control, securing information with encrypted information, responsibility of individuals in their activities and system design security. All of these principles together form a paradigm to make sure that there is confidentiality, integrity, and availability and retains trust and reliability in online communications.

Authentication

Authentication refers to the act of establishing the identity of both the users and the devices prior to their accessibility to a network or a system. This assures that the company resources are only used by authorized users.

Secure credentials can be mandated to access internal systems where employees are required to use such credentials as strong passwords or multi-factor authentication (MFA).

Authorization & Access Control

The Authorization determines what an authenticated user can be allowed to do and the access control determines the roles and duties. This value is used to ensure that users can only receive information that is relevant to their work functions.

Role-based access can be utilized in a manner whereby the HR members can access employee records, Finance access accounting information and IT access network settings so that cross-departmental access is prevented.

Encryption

Data is encrypted to provide security by converting data into an incomprehensible form which can only be decrypted using the correct decryption key. It guarantees security of the information in its transmission and also at the storage level.

Encryption of customer details, financial records and email messages can be done such that even upon stolen, the data will not be read and will not be abused.

Non-repudiation

Non-repudiation gives evidence of user activities with the individuals being unable to refute that they have done a certain activity like sending an email, approving a transaction or accessing confidential files.

MTS can use digital signatures and secure audit logs to monitor activities such as approving financial transactions or updating the HR records.

Security by Design (Defense-in-Depth)

Security by design incorporates the security at all levels of the network not as an extra feature of the network. Defense-in-depth uses layers of protection with the view of ensuring that a failure in one control does not mean failure of defense because other controls will defend.

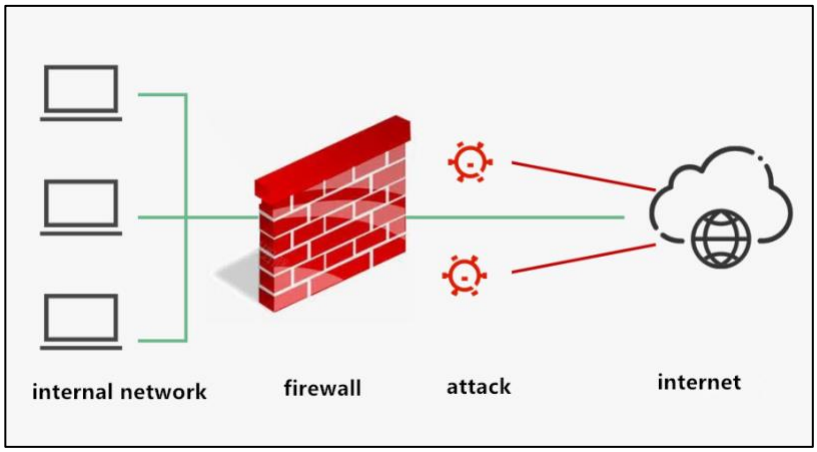
MTS can be used to implement firewalls, intrusion detection system (IDS), antivirus and network segmentation. Such a security layered system will force attackers to work very hard to break down the whole network.

Network Security Devices

Network security devices are a specific equipment that is used to guard the computer networks against unauthorized access, malicious code, and computer breaches. They offer protection through traffic control, threat administration and secure communication. Such devices are the key elements in establishing a secure and dependable network infrastructure.

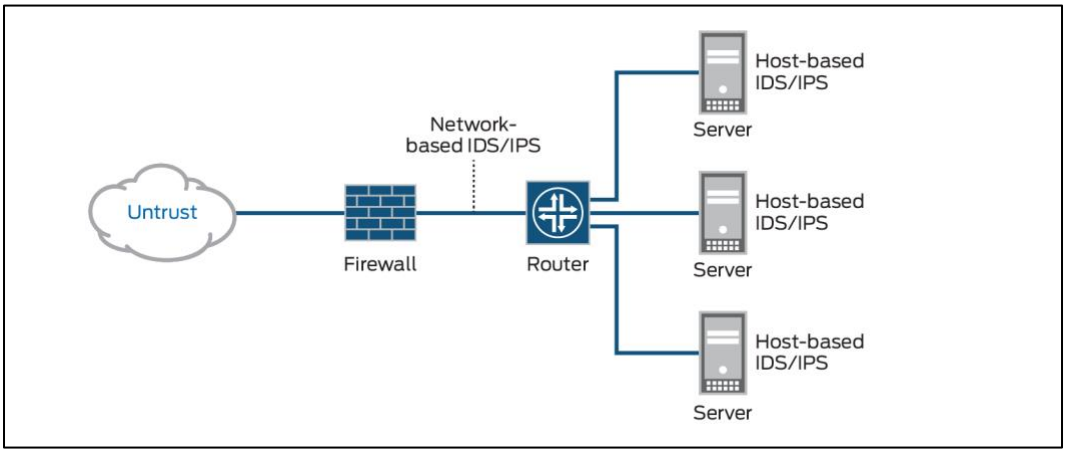
Firewalls

Firewalls can be described as security systems, which filter the incoming and outgoing network traffic, according to the defined rules. They can function as packet filtering firewalls, that is, data packets are analyzed individually, or as stateful inspection firewalls, that is, connections are observed in action, or next-generation firewalls (NGFWs) can be used that could use new features like application filtering and intrusion prevention.



Intrusion Detection & Prevention Systems (IDS/IPS)

IDS and IPS are used to scan network traffic and detect possible suspicious or malicious activity. An Intrusion Detection System (IDS) is used to spot and notify the administrator about the possible threat, whereas an Intrusion Prevention System (IPS) is implemented to prevent or stop identified malicious behaviors.

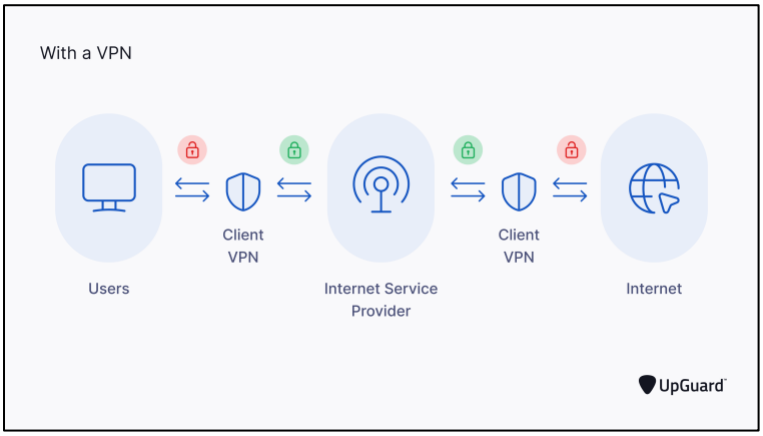


Routers with Security Features

Routers run the traffic of data between the various networks and may include security measures. Access Control Lists (ACLs) and traffic division are among the features that can control and access network communication to increase the general security.

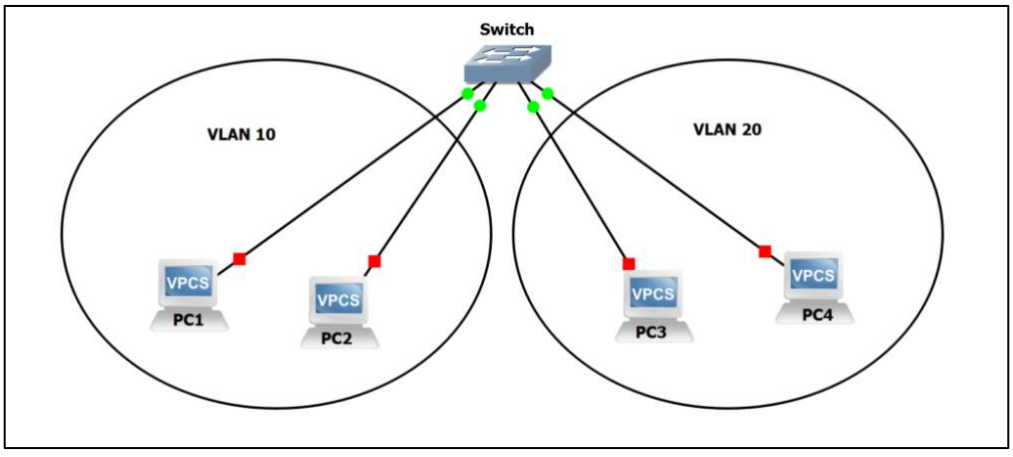
Virtual Private Network (VPN)

VPN creates a secure encrypted network between networks or users across the net. It will provide the security of confidentiality and integrity of data dispatched over a public or unreliable network.



Switches with VLANs

Switches connect various devices of a local network and may be set up with Virtual Local Area Networks (VLANs). VLANs divide the network into smaller and isolated networks and this enhances security because the sensitive flow of data is separated to the general data flow of the network.



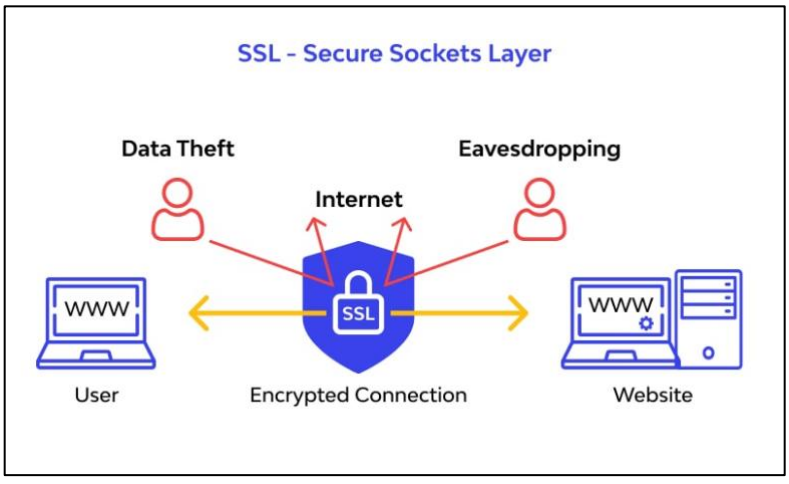
P2 Examine network security protocols and the use of different cryptographic types in network security.

Networking Security Protocols

Network security protocols are standard procedures and rules that direct the transmission, authentication, and protection of data over the communication networks. They provide privacy, integrity and secure access by encrypting traffic, authentication and interception prevention. Through such protocols, organizations can protect web-based services, remote administration, wireless network, and intra-branch communication that provide a formidable base of credible and secured operations.

SSL/TLS

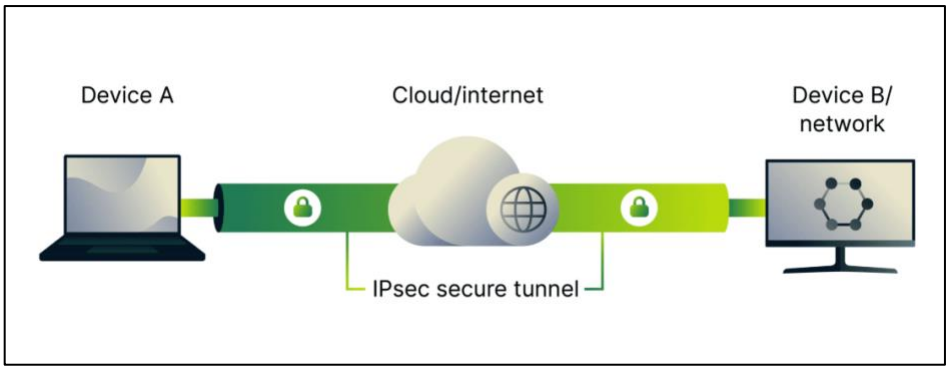
Secure Socket Layer (SSL) and its successor, Transport Layer Security (TLS), are cryptography protocols allowing secure communication over the internet to be possible. They assist in transferring encrypted data between a client and a server, in which important information such as login credentials, payment details and personal information cannot be duplicated to the third party. The most famous version of TLS to the world is HTTPS, HTTPS, which is the encrypted version of HTTP.



IPSec

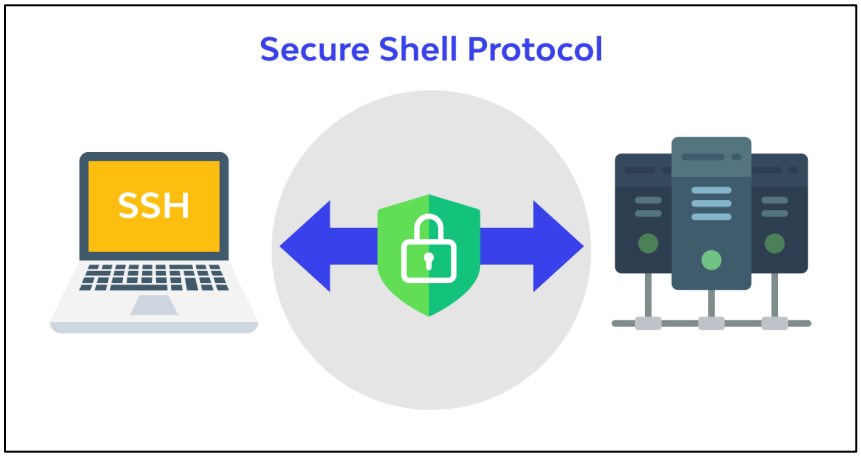
Internet Protocol Security (IPSec) refers to a set of protocols that are employed to encrypt the communications at the network layer. It gives the IP packets encryption, authentication and integrity which makes it suitable in the establishment of site-to-site Virtual Private Networks

(VPNs). IPSec secures that data sent between two locations in the network is secret and inaccessible by other parties.



SSH

Secure Shell (SSH) is a protocol which uses an unsecured network and enables secure access to remote systems. It provides a more secure substitute to older insecure systems like Telnet where encryption is used to secure login credentials and commands. Administrators commonly use SSH to remotely configure, manage and, troubleshoot servers and networking equipment in a secure way.



WPA2/WPA3

Wi-Fi Protected Access (WPA2 and WPA3) are security measures that ensure security of wireless networks. WPA2 also added strong encryption with AES (Advanced Encryption Standard), and WPA3 added further anti-guessing measures to password protection as well as stronger encryption to public Wi-Fi. Such standards are useful in preventing unauthorized users to gain access to wireless networks and also to keep the data that are sent over them confidential.

Cryptographic Techniques of Network Security

Cryptographic techniques have become very vital in modern network security as they guarantee that sensitive information is not available to unauthorized parties, that this information has been well integrated and that they provide safe means of authentication. These are mathematical algorithm-based methods of encrypting, decrypting, and authenticating data and are essential in the security of communications as well as the safety of stored information as well as authenticity of identity of the user. Different cryptographic methods are used in other types of work like fast encryption of information and the secure authentication of the online transactions.

Symmetric Encryption

Symmetric encryption applies one common key in encryption and decryption. It is quick and effective hence applicable in encrypting huge amounts of information. The problem is however, in key management as the distribution and storage of shared key can be complex. The most common symmetric encryption algorithm in the current networks is AES (Advanced encryption standard).

Asymmetric Encryption

Asymmetric encryption employs two keys, which include public and private key to encrypt and decrypt messages respectively. This does not require the use of a single secret key. Common algorithms used in protocols like the SSL/TLS and VPNs, include RSA and Elliptic Curve Cryptography (ECC), used to communicate the protocol and exchange encryption keys.

Hashing Functions

Hashing is a cryptographic method of one-way hash, which transforms data into a constant-size hash. It is not reversible to show original data thus it is best used in password storage, integrity tests and data forensics. Such functions as the SHA-256 are popular to check whether the data has been modified during its transportation or storage.

Digital Signatures and Certificates

Digital signatures are based on asymmetric cryptography to test the integrity and authenticity of digital message or document. Certificates are used together with digital signatures and they are issued by the reputed Certificate Authorities (CAs) so as to authenticate users and

servers. They are vital in certain protocols such the SSL/TLS where they check authenticity of websites and ensure safe communications.

M1 Compare and contrast at least two major network security protocols.

Comparison of Two Major Protocols (SSL/TLS vs IPSec)

A network security is the area where there exist a number of protocols which are used to protect the communication and two of the most popular protocols are the IPSec and the SSL/TLS. They can both be used to serve the same purpose namely to provide security to the data transmission but act at different levels of OSI system and are applicable to various applications. SSL/TLS is increasingly used to secure application-level traffic such as web abilities and email where IPSec is more suitable when the aim of the system is to safeguard all network layer IP packets, such as a VPN, or in inter-site connection. Each of the protocols has its strengths, weaknesses, and use, and this is why one should understand how they are different. Comparison between SSL/TLS and IPSec Comparative analysis of the two-SSL/TLS and IPSec is thoroughly depicted in the sections as follow.

Secure Socket Layer (SSL)

Cryptographic protocols Secure Socket Layer (SSL) and its successor, Transport Layer Security (TLS), provide security to internet-based communication between applications. They prevent the interception of intercepting and modification of sensitive data that might be pass codes, monetary records and personal data by encrypting data over insecure network. SSL/TLS was created to work on the application layer and creates an encrypted connection between a client (such as a browser) and a server (such as a web page). They are most frequently used in HTTPS, a system that ensures web-browsing, e-business contacts and web mail, as well as utilizing the cloud service.

Internet Protocol Security (IPSec)

The Internet Protocol Security (IPSec) is the set of protocols, which also provides security to IP communications at the network layer. It is simply meant to capture every traffic that is flowing through an IP network regardless of the application that is generating that traffic.

The IPSec also safeguards the network conveyance to employ encryption, verification, and integrity checks. It is also widely used as a way of building Virtual Private Networks (VPNs), site-to-site and remote access where it supports encrypted tunnels amongst multiple sites or users on to a corporate network. Contrary to the situation with the CSS/TLS, IPSec is not application-specific and in fact secures the entire IP packets passed over it.

Differences Between SSL/TLS and IPSec

The two protocols share the same objectives of data transmission security, but in different layers, meet different tasks, and are involved in various applications. SSL/TLS is also incorporated in offering security to the chosen application traffic and IPSec offers cover through the network.

Feature	**SSL/TLS (Application Layer)**	**IPSec (Network Layer)**
Definition	Cryptographic protocol for securing communication between applications	Protocol suite securing all IP communications across a network
Layer of Operation	Application layer (OSI layer 7)	Network Layer (OSI Layer 3)
Purpose	Secure specific application sessions (e.g., web, email)	Secure all IP traffic regardless of application
Usage	HTTPS, email, cloud apps	VPNs, site-to-site and remote access

Purpose and Layer of Operation

SSL/TLS provides confidentiality and integrity of application specific traffic, including a user logging in to a site or online banking, and operates on the application layer. By comparison, IPSec provides end-to-end security over whole networks, including communication between two offices, and it operates at the network layer.

Use Cases

SSL/TLS can be best used to protect web-based applications like online shopping, email servers and cloud applications. It is easy, popular and simple to use. IPSec is, however, best suited to organizational networks in which there is a need to protect entire streams of data between sites or users over the network. As an example, it is applied to ensure the communication between the offices of the branches or to give the employees in the remote offices access to the internal resources in an encrypted manner.

Vulnerabilities

There are advantages and disadvantages to both protocols, and it is imperative to know their weaknesses. There is no perfect security measure; both the SSL/TLS and IPSec might be

threatened in case of misconfiguration and in case of using the outdated version. Historically, SS/TLS has been attacked by bugs such as Heartbleed and weak ciphers, and IPSec by complexity and vulnerability to brute-force and downgrade attacks.

Protocol	Common Vulnerabilities
SSL/TLS	SSL/TLS Old outdated SSL versions (SSLv2, SSLv3), insecure ciphers, timeout in Heartbleed bug in OpenSSL, man-in-the-middle attacks (MITM) when certificates are not verified
IPSec	IPSec Complex configuration mistakes, vulnerabilities in key management, exposure to brute force resistance of pre-shared keys, in some systems downgrade attacks.

Performance

SSL/TLS tends to be a lightweight protocol since it only protects particular application traffic. It adds overhead to web sessions but is tuned to be fast and does not show up to most users. IPSec, on the other hand, encrypts every IP traffic and this could increase the computational and bandwidth load. This causes IPSec to be a heavier resource demand, especially in high volume settings, but it has greater coverage.

Advantages & Limitations

A benefit of SSL/TLS is that it is a fairly simple protocol to implement with web applications, it is strongly encrypted, authenticated, and has integrity at the application layer. Nevertheless, its key weakness is that it only protects certain categories of traffic, as web or email, and does not offer security to any network forms of communication. Instead, IPSec offers end-to-end protection at the network layer so that it can readily protect any IP-based traffic irrespective of the application. It is very effective in VPN connections, but has several distinct disadvantages including the complexity in configuration and control, and the possible performance cost of encryption.

Key Takeaways

To conclude on the two security protocols, both are great security protocols, yet they are different in their functioning and are applied in various situations. SSL/TLS is most suitable where there is need to encrypt application-level communications i.e. web-browsing, email and online

transactions with a high level of encryption with minimal or no hassles. Instead, IPSec protects all IP traffic at the network layer, which is optimal with VPNs and site-to-site connections, but it is more complicated to implement and need not less resources. The decision to use them is based on the security policies and scope of protection and the performance of the environment where they are applied.

LO2 Design a secure network for a corporate environment

P3 Investigate the purpose and requirements of a secure network according to a given scenario.

Overview

Myanmar Tech Solutions (MTS) is a small, but expanding technology company which has its headquarters in Yangon and a new planned branch office at Naypyidaw. The company is further divides into five important departments namely; Finance, Human Resources, Sales and Marketing, Customer Support and Information Technology. Every department is handling sensitive information, including financial transactions, employee records, customer data, and internal communications, which are not to be left in unprotected access and cyber attacks. As the company expanded to Naypyidaw, the key factor will be inter-branch connectivity, network segmentation to ensure uninterrupted business operations, information confidentiality, and the stability of business operations.

Purpose of a Secure Network

The purpose of developing a secure network of Myanmar Tech Solutions (MTS) is to create reliable, secured, and efficient communications throughout its growing operations. As the new branch opens in Naypyidaw, MTS needs a network that will allow it to connect smoothly with the Yangon base and to avoid the transmission of sensitive data to unauthorized individuals. An impermeable design is also necessary to protect against increasing cyber threats like malware, phishing, and data breach, which may interfere with operations and result in loss of customer trust.

The company can protect confidential data and restrict the access to authorized personnel only by separating each department using VLANs and access control policies: Finance, Sales and Marketing, HR, Customer Support, and IT. Moreover, secure network improves the business continuity by minimizing the downtime, maintaining constant communication among sites, and deserving customer-facing services. It also assists the organization in meeting the compliance and data security standards minimizing legal and financial risks. Finally, a secure network design would enhance the overall cybersecurity status of MTS and allow it to grow in the future.

Requirements of a Secure Network

Myanmar Tech Solutions (MTS) is experiencing growth with its new division in Naypyidaw and creating a safe network infrastructure is a crucial need to protect confidential data and secure business continuity. As the number of cyber threats rises, securing financial records, customer details, and interdepartmental communication is necessary to ensure operational efficiency as well as retain trust of clients and other stakeholders. A safe net at MTS has to be formulated with multiple layers of defense and well-defined policies to curb any possible threats. The following are seven major requirements to be met to provide a robust cybersecurity framework at MTS –

1. Network Segmentation
2. Authentication and Access Control
3. Encryption
4. Firewalls and Intrusion Prevention Systems (IPS)
5. Virtual Private Network (VPN) for Branch Connectivity
6. Regular Security Updates and Patch Management
7. Security Policies and Employee Training

Network Segmentation

Network segmentation consists of breaking down the infrastructure of the company into independent, managed parts which include Finance, HR, Sales and Marketing, IT and Customer Support. Isolating the departmental networks will enable MTS to restrict unauthorized access, enhance monitoring and enable the attackers to move freely within the system in the event of a breach.

Authentication and Access Control

There should be strong authentication techniques such as multi-factor authentication (MFA) so that only authorized personnel get access to the critical systems. Role-Based Access Control (RBAC) allows users access only to the data and resources pertaining to their department, which leads to decreasing insider threats and the possibility of unauthorized actions inside the network.

Encryption

Encryption is important in the protection of data during transmission and rest. Using robust encryption, including AES, MTS will be able to safeguard customer information and financial data, as well as inter-office communications. Although data may be intercepted, encryption will make sensitive data unreadable and will not be exploited.

Firewalls and Intrusion Prevention Systems (IPS)

Firewalls can be used as a first line of defense against unauthorized traffic, Intrusion Prevention Systems (IPS) can detect and block suspicious traffic, malware infection or denial-of-service (DoS) attacks. Taken collectively, these devices offer a potent defense mechanism in the event an external threat to infrastructure of MTS is carried out.

Virtual Private Network (VPN) for Branch Connectivity

Since MTS is opening an office in Naypyidaw, there is a need to have a secure Virtual Private Network (VPN) that ensures that the communications between the headquarters and the new office remain encrypted. The VPNs also allow the remote employees to log into the company network securely, and classified information is relayed, over the unreliable internet systems.

Regular Security Updates and Patch Management

Old systems attract cybercriminals. In order to mitigate the vulnerabilities and exploiting it, software updating is needed on a regular basis along with automated patch management. As a result of keeping its systems updated, MTS will be in a position to maintain a better defence posture and reduce the likelihood of breaches because of the unpatched software.

Security Policies and Employee Training

Human error is one of the greatest risks facing cybersecurity. MTS should create efficient security policy, and provide employees with constant training on password-management, phishing-detection, and internet-safety. The initial defence is trained workers and the attackers are hard to have so that they can exploit the points of weakness in the company.

P4 Determine which network hardware and software to use in a secure network.

Introduction to Security Hardware and Software

The secure network infrastructure depends on both software and hardware components to ensure that sensitive information is not compromised and operations run smoothly. The physical basis of traffic control, network segmentation, and linking users is hard devices, and the security can be enhanced by software solutions which can operate with encryption, monitoring and controlling access. In the case of Myanmar Tech Solutions (MTS), it is important to select an appropriate mix of hardware and software to provide its headquarters in Yangon and the newly opened branch in Naypyidaw, as well as, support its five departments: Finance, HR, Sales and Marketing, Customer Support, and IT.

Hardware Requirements

Hardware requirements are needed in network security, and they are the hardware that allows routing, switching, wireless, and traffic control. These devices are not only important in ensuring that there is appropriate communication among the departments and branches but also in the implementation of security policies. Switches, routers, multilayer switches, wireless LAN controllers, and lightweight access points are used at MTS as the backbone of the secure infrastructure.

Routers (Cisco 2911 Router)

The Cisco 2911 Integrated Services Router is built to offer secure and scalable routing to medium sized organizations. It also provides progressive features like firewall, VPN, and built-in security. The 2911 router is aimed at routing efficiently data packets between the Yangon headquarters and the Naypyidaw branch as well as ensuring external connectivity to the internet. The router is important to facilitate MTS network site-to-site VPNs in communication that allows encrypted communication so that vital departmental information is not exposed during transit between the sites.

Switches (Cisco 2960 Switch)

Cisco 2960 Layer 2 access switch was a device employed to connect other devices in local area networks. It also provides Ethernet service, reliable and supporting VLANs. It is expected to separate traffic among departments and ensure the maintenance of a stable operation. The 2960 switch in MTS divides the departments such as Finance, HR and Sales and avoids the risk of internal data leakage or unauthorized access.

Multi-Layer Switch (Cisco 3560 Multilayer Switch)

Cisco 3560 is a multilayer switch which is a combination of Layer 2 switching as well as Layer 3 routing. It assists in routing of VLAN, access control lists (ACLs) and advanced security. It is directed to the increase in scalability and inter-VLAN communication. The 3560 switch ensures the safe inter-departmental communication, and it also places access control on sensitive systems in MTS.

Wireless LAN Controller

A Wireless LAN Controller (WLC) is used to control multiple wireless access points, with a centralized security policy, uniform configuration and predictable performance. It is meant to make the management of Wi-Fi easier and also implement encryption to all wireless users. At MTS, the WLC handles wireless connectivity at the Yangon and Naypyidaw offices, such that all Wi-Fi users are authenticated and secured.

Lightweight Access Point

A Lightweight Access Point (LWAP) makes the wireless access of the devices of employees accessible, but under the control of the WLC. LWAPs are also configured and monitored by the controller in contrast to autonomous access points. They are supposed to offer wireless coverage with centralized security. In the case of MTS, LWAPs are implemented in various departments in order to provide secure and flexible access to Wi-Fi without violating organizational policies.

Software Requirements

Although hardware provides security to the physical network infrastructure, software solutions have extra layers of protection to counter, prevent, and reduce cyber threats. Firewalls, VPN software and intrusion prevention systems (IPS) are the key software elements that MTS should have.

Firewall

Firewall software is developed with view to filtering and regulating network traffic according to security policies. It avoids unauthorized access, any malicious traffic and implementation of organizational policies. It is meant to act as the initial defense against cyberattacks. Firewall software is deployed at MTS to monitor and control the incoming and outgoing traffic with the aim of safeguarding sensitive departmental systems in the facility against external attacks.

Virtual Private Network (VPN)

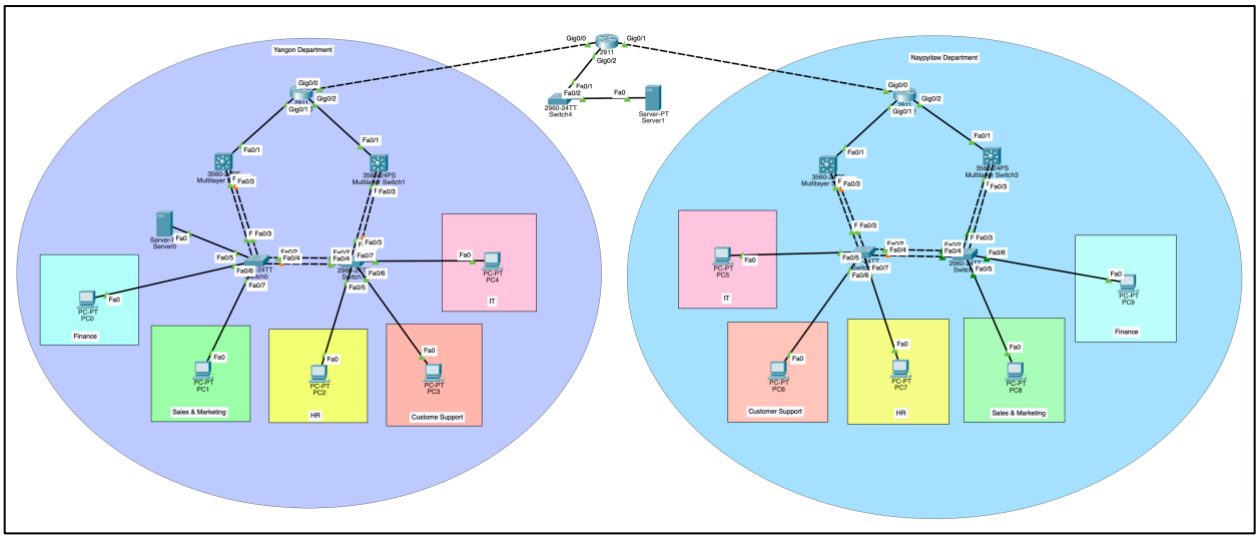
VPN programs provide secure and encrypted tunnels to transmit data on untrusted networks. It also guarantees confidentiality and integrity because sensitive information is secured in the process of remote access. It aims at allowing the employees and branch offices to access the main network safely. The VPN software at MTS will enable the Naypyidaw division and staff working remotely to connect to the corporate systems without exposing their important information to potential hackers.

Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) software will actively scan through network traffic in order to block malicious activities as they happen. It stops attacks like malware, brute-force attack

and denial-of-service (DoS) attack. It is intended to provide a proactive defense mechanism that is outside the firewall. At MTS, IPS software is used as an added protection level where suspicious traffic is detected and blocked before it can affect business processes or breach sensitive information.

M2 Create a design of a secure network according to a given scenario.



This architecture connects two sites, Yangon Department and Naypyitaw Department to an ISP WAN using site-to-site IPSec VPN. The perimeter of each site is configured with a Cisco 2911, core with a Cisco 3560 multilayer switch inter-VLAN routing through SVIs, and access switches at the endpoint with Cisco 2960. Departments co-reside in different VLANs (Finance, Sales and marketing, HR, Customer Support, IT), and shared services are configured in a special Server/DMZ VLAN.

Inter-Site Connectivity

The two 2911 routers create IPSec site to site VPN encrypting only the private summaries of both sites. With summaries, crypto ACL complexity is minimized, inadvertent reachability is avoided, and processing overhead is minimized without losing cross-site services.

Implementation Summary

VLANs are configured on every 3560, IP-routing is configured and SVIs acquire the .254 addresses. The access ports on 2960s are configured in the appropriate VLANs; uplinks are configured to carry 802.1Q trunks, and only necessary VLANs permitted. DHCP issues address based on /24 with the SVI as the default routing table and site DNS resolver. Routing in between 2911 and 3560, passive interfaces are used with small OSPF domain or with static routes to site summary. NAT/PAT at the edge decides what internal networks are allowed to access the Internet (usually IT) and default route is sent to the ISP.

Security Measures

The security is designed on all levels. IP planning and subnetting give definite L3 boundaries; VLANs implement least privilege and isolate servers in a DMZ which only exposes services (e.g. DNS/HTTPS) which are needed. SVI ACLs restrict inter-VLAN traffic; edge ACLs default-deny unsolicited Internet traffic and allow VPN, established return traffic, NAT policies limit which sources are allowed to egress, minimizing exfiltration routes. Legislative protection: Layer-2 hardening, DHCP Snooping, Dynamic ARP Inspection, port-security with sticky MAC, BPDU Guard, storm-control and the closure of unused ports preventing the common attacks before they get to Layer-3.

IP Plan

The IP plan of both Yangon (HQ) and Naypyitaw (Branch) is also based on the same, department-per/24 model with the default gateway is configured as .254 on each SVI, independently using different non-overlapping private ranges to avoid conflict in the site-to-site VPN. Yangon has Finance, Sales and Marketing, HR, Customer Support, IT and Server/DMZ with contiguous /24s which Naypyitaw is adopting the same pattern with the same departments occupying their separate /24 block. This symmetry allows simplified scopes of DHCP, ACL design and troubleshooting; the contiguous addressing of each location also facilitates clean route summarization to the WAN/VPN, less routing chatter and attack surface, and allows growth without further redesign.

Yangon Department (Head Quarter)

Scope	VLAN ID	Network / Subnet	Gateway
Private	VLAN 10 – Finance	192.168.200.0/24	192.168.200.254
	VLAN 20 – Sales & Marketing	192.168.201.0/24	192.168.201.254
	VLAN 30 – HR	192.168.202.0/24	192.168.202.254
	VLAN 40 – Customer Support	192.168.203.0/24	192.168.203.254
	VLAN 50 – IT	192.168.204.0/24	192.168.204.254
	VLAN 60 – Server	192.168.205.0/24	192.168.205.254
Public	ISP (WAN)	203.0.113.4/30	203.0.113.6

Naypyitaw Department (Branch)

Scope	VLAN ID	Network / Subnet	Gateway
Private	VLAN 10 – Finance	192.168.210.0/24	192.168.210.254
	VLAN 20 – Sales & Marketing	192.168.211.0/24	192.168.211.254
	VLAN 30 – HR	192.168.212.0/24	192.168.212.254
	VLAN 40 – Customer Support	192.168.213.0/24	192.168.213.254
	VLAN 50 – IT	192.168.214.0/24	192.168.214.254
Public	ISP (WAN)	198.51.100 .4/30	198.51.100.6

Routing Policies & Summarization

Minimal advertising prefixes (HQ 192.168.200.0/21, Branch 192.168.208.0/21) over the VPN reduce the amount of routing information that is exposed and constrain the blast radius of errors. OSPF passive interfaces decrease adjacency that is unnecessary in addition to route filters, which make sure that only necessary networks are exported to the WAN and the other site.

Justification & Risk Reduction

ACLs and troubleshooting are simple when under pressure given the per-department /24s and the constant 254 gateways. Conflicts and asymmetric site ranges are avoided by non-overlapping site ranges and specific VPN selectors. Protections on each level such as defense in depth-L2, SVI ACLs and edge ACL/NAT limit the lateral movement and decrease the attack surface. Design is predictable: new departments are more merely new /24s on the same summaries, without altering the VPN model.

LO3 Configure Network Security measures for the corporate environment

P5 Configure network security for a network.

Inter-VLAN Routing Setup

```
Switch(config-vlan)#int vlan 10
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan10, changed state to up

Switch(config-if)#ip add 192.168.200.1 255.255.255.0
Switch(config-if)#int vlan 20
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan20, changed state to up

Switch(config-if)#ip add 192.168.201.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#int vlan 30
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

Switch(config-if)#ip add 192.168.202.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#
Switch(config-if)#int vlan 40
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan40, changed state to up

Switch(config-if)#ip add 192.168.203.1 255.255.255.0
Switch(config-if)#no shut
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 50
Switch(config-if)#ip add 192.168.204.1 255.255.255.0
Switch(config-if)#no shut
```

```
Switch(config-if)#ip add 102.168.204.1 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#int vlan 60
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan60, changed state to up

Switch(config-if)#ip add 192.168.205.1 255.255.255.0
Switch(config-if)#no shut
```

```
Switch(config-if)#no switchport
Switch(config-if)#ip add 192.168.20.2 255.255.255.0
Switch(config-if)#exit
Switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.1
Switch(config)#int f0/1
Switch(config-if)#no switchport
Switch(config-if)#
```

This is a VLAN setup and routing of a Cisco switch. It allocates the IP addresses of various VLANs, enables them and configures inter-VLAN routing to enable each department or subnet to communicate. The point is to isolate the network in terms of security and efficiency but still being able to connect to VLANs and the internet.

IP Addressing and Routing on Router

```
Router(config-if)#
Router(config-if)#exit
Router(config)#int g0/1
Router(config-if)#ip add 192.168.20.1 255.255.255.0
Router(config-if)#no shut
Router(config-if)#int g0/2
Router(config-if)#ip add 192.168.30.1 255.255.255.0
Router(config-if)#int g0/0
Router(config-if)#ip add 203.0.113.1 255.255.255.252
Router(config-if)#exit
Router(config)#ip route 192.168.200.0 255.255.255.0 192.168.20.2
Router(config)#ip route 192.168.201.0 255.255.255.0 192.168.20.2
Router(config)#ip route 192.168.205.0 255.255.255.0 192.168.20.2
Router(config)#ip route 192.168.202.0 255.255.255.0 192.168.30.2
Router(config)#ip route 192.168.203.0 255.255.255.0 192.168.30.2
Router(config)#ip route 192.168.204.0 255.255.255.0 192.168.30.2
Router(config)#
```

This is a router setup whereby various interfaces (g0/1, g0/2, g0/0) are assigned IP addresses in order to bridge different networks. The addition of the routing tables then follows where the router is aware of the path to all the VLAN networks by the appropriate next-hop IP. This is to facilitate the interconnection of the various subnets and to facilitate the proper data routing over the network of the organization.

VLAN Creation and Port Configuration on Switch

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#vlan 10
Switch(config-vlan)#vlan 20
Switch(config-vlan)#vlan 30
Switch(config-vlan)#vlan 40
Switch(config-vlan)#vlan 50
Switch(config-vlan)#vlan 60
Switch(config-vlan)#int f0/6
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#int f0/7
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#int f0/5
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 60
Switch(config-if)#int range f0/1,f0/3
Switch(config-if-range)#switchport mode trunk


Switch(config-if-range)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch(config-if-range)#switchport trunk allowed vlan 10,20,30,40,50,60
Switch(config-if-range)#
```

This configuration demonstrates the way of establishing VLANs and allocating them to the particular switch ports. Departments have access ports (f0/6, f0/7, f0/5 and others) that access a specific VLAN, and trunk ports (f0/1 and f0/3) are used to transmit a variety of VLANs across switches or to the router. It is meant to partition the network into various VLANs in order to manage it, enhance security, and inter-VLAN communication.

NAT Configuration on Router

```
Router(config)#int g0/0
Router(config-if)#ip add 203.0.113.2 255.255.255.252
Router(config-if)#int g0/1
Router(config-if)#ip add 198.51.100.2 255.255.255.252
Router(config-if)#int g0/2
Router(config-if)#ip add 192.168.200.1 255.255.255.0
Router(config-if)#
```

```
Router(config)#access-list 1 permit any
Router(config)#ip nat inside source list 1 interface g0/0 overload
Router(config)#int g0/0
Router(config-if)#ip nat outside
Router(config-if)#int g0/1
Router(config-if)#ip nat inside
Router(config-if)#int g0/2
Router(config-if)#ip nat inside
Router(config-if)#
Router(config-if)#
```

In this configuration, the IP addresses on router interfaces are configured and NAT (Network Address Translation) is also configured. The access-list permits any internal equipment and NAT overload is set up in such a way that several internal IPs may share a single external IP to access internet. This is to allow internal hosts to use personal addresses and still have the ability of accessing external networks safely.

Ether Channel

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range f0/2-3
Switch(config-if-range)#switchport mode trunk
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to
"trunk" mode.
Command rejected: An interface whose trunk encapsulation is "Auto" can not be configured to
"trunk" mode.
Switch(config-if-range)#switchport trunk encapsulation dot1q
Switch(config-if-range)#channel-protocol pagp
Switch(config-if-range)#channel-group 1 mode auto
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

Switch(config-if-range)#
```

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range f0/1,f0/3
Switch(config-if-range)#channel-protocol pagp
Switch(config-if-range)#channel-group 1 mode desirable
Switch(config-if-range)#
Creating a port-channel interface Port-channel 1

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/3, changed state to up

%LINK-5-CHANGED: Interface Port-channel1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Port-channel1, changed state to up

Switch(config-if-range)#int port-channel 1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

This setup establishes EtherChannel which will hold together several physical connections into a single logical connection to enhance bandwidth and offer redundancy. The switch ports are aggregated with pagp protocol and put in a Port-Channel interface and these ports are configured to trunk in order to support many VLANs. This is done to enhance the performance of their network, eliminate the chances of single-link failure, and facilitated efficient inter-switch communication.

HSRP

```
Switch(config)#interface Vlan10
Switch(config-if)# ip address 192.168.200.5 255.255.255.0
Switch(config-if)# standby 1 ip 192.168.200.1
Switch(config-if)# standby 1 priority 100
Switch(config-if)# standby 1 preempt
Switch(config-if)#
Switch(config-if)#interface Vlan20
Switch(config-if)# ip address 192.168.201.5 255.255.255.0
Switch(config-if)# standby 2 ip 192.168.201.1
Switch(config-if)# standby 2 priority 100
Switch(config-if)# standby 2 preempt
Switch(config-if)#
Switch(config-if)#interface Vlan30
Switch(config-if)# ip address 192.168.202.5 255.255.255.0
Switch(config-if)# standby 3 ip 192.168.202.1
Switch(config-if)# standby 3 priority 100
Switch(config-if)# standby 3 preempt
Switch(config-if)#
Switch(config-if)#interface Vlan40
Switch(config-if)# ip address 192.168.203.5 255.255.255.0
Switch(config-if)# standby 4 ip 192.168.203.1
Switch(config-if)# standby 4 priority 100
Switch(config-if)# standby 4 preempt
Switch(config-if)#
Switch(config-if)#interface Vlan50
Switch(config-if)# ip address 192.168.204.5 255.255.255.0
Switch(config-if)# standby 5 ip 192.168.204.1
Switch(config-if)# standby 5 priority 100
Switch(config-if)# standby 5 preempt
Switch(config-if)#
Switch(config-if)#interface Vlan60
Switch(config-if)# ip address 192.168.205.5 255.255.255.0
Switch(config-if)# standby 6 ip 192.168.205.1
Switch(config-if)# standby 6 priority 100
Switch(config-if)# standby 6 preempt
Switch(config-if)#
```

```
Switch(config)#interface Vlan10
Switch(config-if)# ip address 192.168.200.5 255.255.255.0
Switch(config-if)# standby 1 ip 192.168.200.1
Switch(config-if)# standby 1 priority 105
Switch(config-if)# standby 1 preempt
Switch(config-if)#
Switch(config-if)#interface Vlan20
Switch(config-if)# ip address 192.168.201.5 255.255.255.0
Switch(config-if)# standby 2 ip 192.168.201.1
Switch(config-if)# standby 2 priority 105
Switch(config-if)# standby 2 preempt
Switch(config-if)#
Switch(config-if)#interface Vlan30
Switch(config-if)# ip address 192.168.202.5 255.255.255.0
Switch(config-if)# standby 3 ip 192.168.202.1
Switch(config-if)# standby 3 priority 105
Switch(config-if)# standby 3 preempt
Switch(config-if)#
Switch(config-if)#interface Vlan40
Switch(config-if)# ip address 192.168.203.5 255.255.255.0
Switch(config-if)# standby 4 ip 192.168.203.1
Switch(config-if)# standby 4 priority 105
Switch(config-if)# standby 4 preempt
Switch(config-if)#
Switch(config-if)#interface Vlan50
Switch(config-if)# ip address 192.168.204.5 255.255.255.0
Switch(config-if)# standby 5 ip 192.168.204.1
Switch(config-if)# standby 5 priority 105
Switch(config-if)# standby 5 preempt
Switch(config-if)#
Switch(config-if)#interface Vlan60
Switch(config-if)# ip address 192.168.205.5 255.255.255.0
Switch(config-if)# standby 6 ip 192.168.205.1
Switch(config-if)# standby 6 priority 105
Switch(config-if)# standby 6 preempt
Switch(config-if)#
```

This setup establishes the HSRP (Hot Standby Router Protocol) in VLAN interfaces, to offer gateway redundancy. Virtual IPs are attached to each VLAN and two switches assume the functions of active and standby router with varied priorities. This is to allow the network to stay on, in case the gateway in service goes down, the backup gateway would automatically come into effect to maintain the flow of communication.

GRE TUNNEL

```
Router(config)#int tunnel 0

Router(config-if)#
%LINK-5-CHANGED: Interface Tunnel0, changed state to up

Router(config-if)#ip add 10.0.0.1 255.0.0.0
Router(config-if)#tunnel source g0/0
Router(config-if)#tunnel destination 198.51.100.1
Router(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0, changed state to up

Router(config-if)#ex
Router(config)#router rip
Router(config-router)#ver 2
Router(config-router)#network 10.0.0.0
```

Such a configuration enables a GRE (Generic Routing Encapsulation) tunnel on the router. Tunnel interface is established, which has an IP address and the source and destination are established to bridge remote networks across the internet. RIP routing is then made active on the tunnel network which enables the communication between the various sites in a safe manner as though they were on one local network.

IPSec

```
Router>
Router>
Router>en
Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 1
Router(config-isakmp)#authentication pres-share
                                   ^
% Invalid input detected at '^' marker.

Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#encryption aes 256
Router(config-isakmp)#hash sha
Router(config-isakmp)#group 5
Router(config-isakmp)#ex
Router(config)#crypto isakmp key cisco123 address 198.51.100.1
Router(config)#crypto ipsec transform-set test esp-aes 256 esp-sha-hmac
Router(config)#crypto map VPNmap 1 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#set peer 198.51.100.1
Router(config-crypto-map)#set transform-set test
Router(config-crypto-map)#match address 100
Router(config-crypto-map)#ex
Router(config)#access-list 100 permit gre host 203.0.113.1 host 198.51.100.1
Router(config)#int g0/0
Router(config-if)#crypto map VPNmap
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
Router(config-if)#ex
Router(config)#
```

This setup uses an IPSec VPN to encrypt communication between two routers using the internet. It establishes an isakmp policy which uses pre-shared authentication, AES encryption, and SHA hashing, and a transform set used in encryption and authentication. The router interface

is then encrypted with a crypto map so that the data passing between the known peers is encrypted and secured giving confidentiality and safe tunnelling to confidential data.

SSH – Telnet

```
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#line vty 0 3
Switch(config-line)#password telpa55
Switch(config-line)#login
Switch(config-line)#enable password enpa55
Switch(config)#int vlan 202
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#int vlan 30
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan30, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan30, changed state to up

Switch(config-if)#ip add 192.168.202.50 255.255.255.0
Switch(config-if)#no shut
Switch(config-if)#
```

```
C:\>telnet 192.168.202.50
Trying 192.168.202.50 ...Open


User Access Verification

Password:
Switch>en
Password:
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#username admin password telpa55
Switch(config)#hostname gw1
gw1(config)#ip domain-name info.com
gw1(config)#crypto key generate rsa
The name for the keys will be: gw1.info.com
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

gw1(config)#line vty 0 3
*Mar 1 1:50:30.348: %SSH-5-ENABLED: SSH 1.99 has been enabled
gw1(config-line)#transport input ssh
gw1(config-line)#ex
% Ambiguous command: "ex"
gw1(config-line)#ip ssh version 2
gw1(config)#ip ssh authentication-retries 3
gw1(config)#ip ssh time-out 60
gw1(config)#ex
gw1#!
```

The initial setting (on the switch) enables Telnet by enabling VTY lines using a password and allocating an IP address to VLAN30 in order to allow remote access. The second setup (terminal PC side) displays a Telnet connection with a switch environment in which further instructions are typed to activate SSH. SSH has been set up using domain name, RSA key generation as well as security options to offer more secure and encrypted remote management. The combination of this setup demonstrates that a switch can initially permit limited access of the plaintext Telnet, before being upgraded to SSH to enable safe access as an administration user.

Switchport Port Security

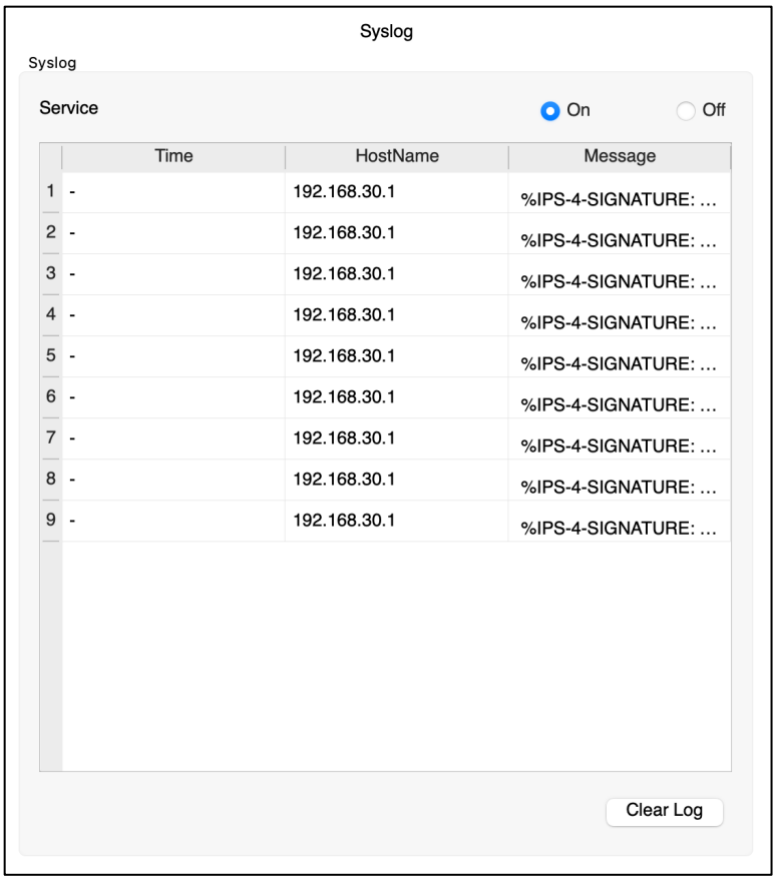
```
Switch(config)#In f0/6
Switch(config-if)#Switchport mode access
Switch(config-if)#Switchport access vlan 10
Switch(config-if)#Switchport port-security
Switch(config-if)#Switchport port-security maximum 1
Switch(config-if)#Switchport port-security mac-address sticky
Switch(config-if)#Switchport port-security violation shutdown
Switch(config-if)#No shu
Switch(config-if)#In f0/7
Switch(config-if)#Switchport mode access
Switch(config-if)#Switchport access vlan 20
Switch(config-if)#Switchport port-security
Switch(config-if)#Switchport port-security maximum 1
Switch(config-if)#Switchport port-security mac-address sticky
Switch(config-if)#Switchport port-security violation shutdown
Switch(config-if)#No shu
Switch(config-if)#exit
Switch(config)#
```

Such configuration allows port security of switch interfaces (f0/6 and f0/7). Each port will be configured to access mode; this will be assigned to a VLAN and will be limited to permit only one device sticky MAC address feature. In case the unauthorized device attempts to connect the port will automatically go dead. This is to safeguard the network by avoiding unauthorized access and making sure that the devices that are trusted can only access certain switch ports.

IOS IPS (Intrusion Prevention System)

```
Router>
Router>en
Router#show flash:

System flash directory:
File  Length   Name/status
  4   0        Show flash:
  3   33591768 c2900-universalk9-mz.SPA.151-4.M4.bin
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


Router#mkdir flash:
Create directory filename []?ipsdir
Created dir flash:ipsdir

Router#show flash

System flash directory:
File  Length   Name/status
  4   0        Show flash:
  3   33591768 c2900-universalk9-mz.SPA.151-4.M4.bin
  5   0        ipsdir
  2   28282    sigdef-category.xml
  1   227537   sigdef-default.xml
[33847587 bytes used, 221896413 available, 255744000 total]
249856K bytes of processor board System flash (Read/Write)


Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#ip ips config location flash:ipsdir
Router(config)#Ip ips name iosips
Router(config)#ip ips signature-category
Router(config-ips-category)#ip ips signature-category
Router(config-ips-category)#category all
Router(config-ips-category-action)#retired true
Router(config-ips-category-action)#exit
Router(config-ips-category)#category ios_ips basic
Router(config-ips-category-action)#retired false
Router(config-ips-category-action)#exit
Router(config-ips-category)#exit
Do you want to accept these changes? [confirm]
Applying Category configuration to signatures ...
%IPS-6-ENGINE_BUILDING: atomic-ip - 288 signatures - 6 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 30 ms - packets for this engine will be scanned

Router(config)#
```

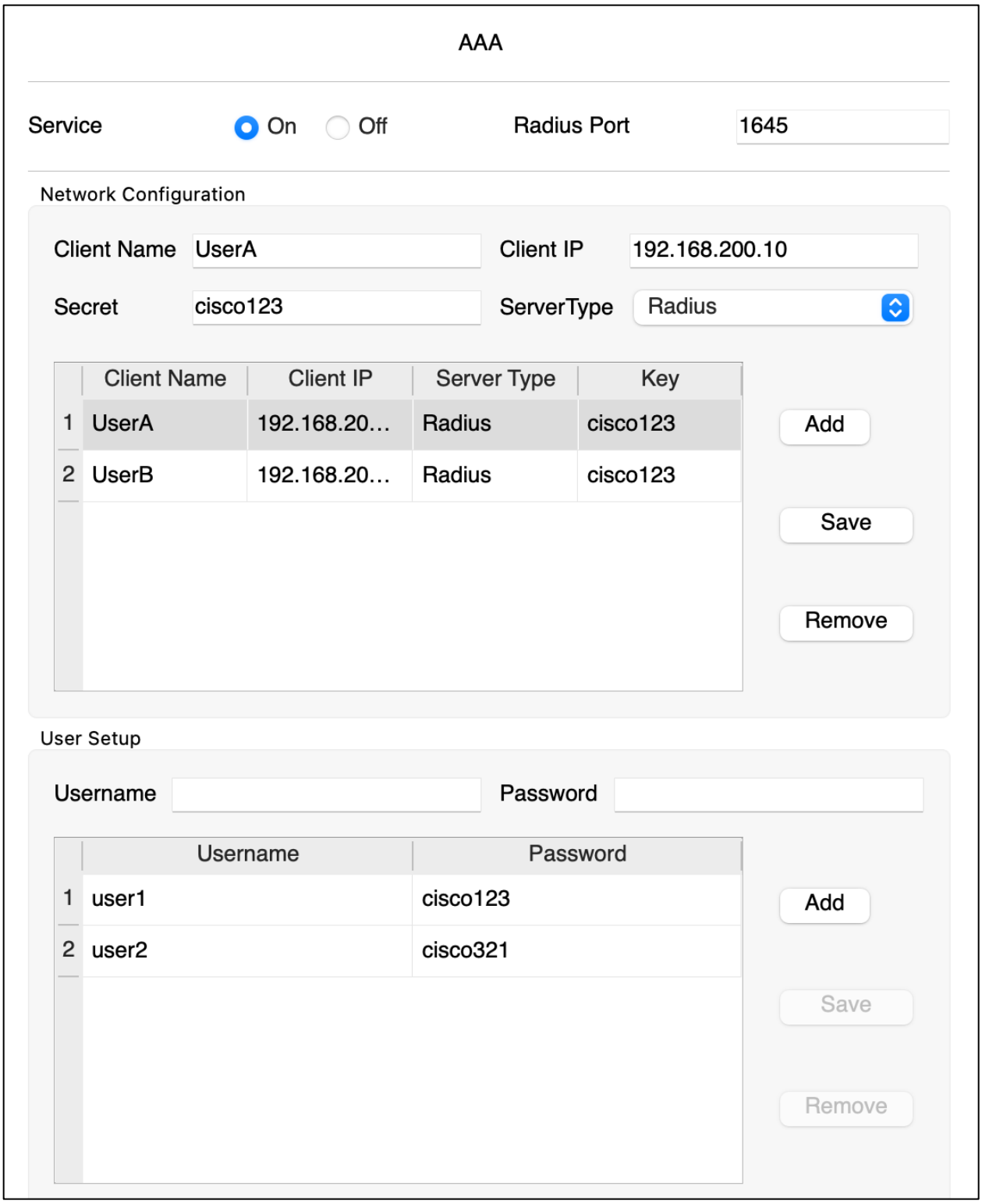
```
Router(config)#in g0/1
Router(config-if)#ip ips iosips out
Router(config-if)#ip ips signature-definition
Router(config-sigdef)#signature 2004 0
Router(config-sigdef-sig)#status
Router(config-sigdef-sig-status)#retired false
Router(config-sigdef-sig-status)#enable true
Router(config-sigdef-sig-status)#ex
Router(config-sigdef-sig)#engine
Router(config-sigdef-sig-engine)#event-action produce-alert
Router(config-sigdef-sig-engine)#event-action deny-packet-inline
Router(config-sigdef-sig-engine)#ex
Router(config-sigdef-sig)#ex
 %IPS-6-ENGINE_BUILDS_STARTED:  00:07:39 UTC Mar 01 1993

 %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines

 %IPS-6-ENGINE_READY: atomic-ip - build time 8 ms - packets for this engine will be scanned

 %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 8 ms

Router(config-sigdef)#exit
Do you want to accept these changes? [confirm]
%IPS-6-ENGINE_BUILDS_STARTED:
%IPS-6-ENGINE_BUILDING: atomic-ip - 303 signatures - 3 of 13 engines
%IPS-6-ENGINE_READY: atomic-ip - build time 480 ms - packets for this engine will be scanned
%IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 648 ms

Router(config)#
```

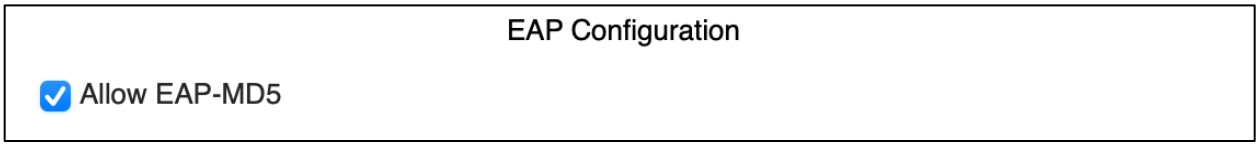


The combination of these three settings displays the configuration and monitoring of the IOS IPS (Intrusion Prevention System) on a Cisco router. The IPS signature files are initially stored and loaded out of the flash memory of the router. Then, rules are applied to interface (g0/1) with IPS, to identify and block suspicious traffic based on specified signatures. Lastly the Syslog is the output showing alerts that the IPS generate when possible threats are detected. This setup is to guard the network against malicious activity by identifying, recording and blocking harmful traffic in real-time.

NAC

```
Switch>
Switch>en
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int vlan 10
Switch(config-if)#no shu
Switch(config-if)#ip address 192.168.200.10 255.255.255.0
Switch(config-if)#ip default-gateway 192.168.200.1
Switch(config)#
Switch(config)#int vlan 20
Switch(config-if)#no shu
Switch(config-if)#ip address 192.168.201.10 255.255.255.0
Switch(config-if)#ip default-gateway 192.168.201.1
%LINK-5-CHANGED: Interface Vlan10, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up

%LINK-5-CHANGED: Interface Vlan20, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan20, changed state to up

Switch(config)#
```


AAA
Service
On
Off
Radius Port
1645
Network Configuration
Client Name
UserA
Client IP
192.168.200.10
Secret
cisco123
ServerType
Radius
Client Name
Client IP
Server Type
Key
1
UserA
192.168.20…
Radius
cisco123
2
UserB
192.168.20…
Radius
cisco123
Add
Save
Remove
User Setup
Username
Password
Username
Password
1
user1
cisco123
2
user2
cisco321
Add
Save
Remove


EAP Configuration
Allow EAP-MD5

```
Switch(config)#aaa new-model
Switch(config)#radius-server host 192.168.205.10 auth-port 1645 key cisco123
Switch(config)#aaa authentication dot1x default group radius
Switch(config)#dot1x system-auth-control
Switch(config)#in range fa0/6-7
Switch(config-if-range)#dot1x pae authenticator
Switch(config-if-range)#authentication port-control auto
Switch(config-if-range)#
```

These settings depict the application of AAA (Authentication, Authorization and Accounting) to the 802.1X authentication with a RADIUS server. The switch will be configured with VLAN IPs and attached to the RADIUS server that contains user credentials (such as user1 and user2). Authentication is permitted using the EAP-MD5 approach and the switch is configured using aaa new-model and connected to the RADIUS server. Lastly, ports are opened to 802.1X to ensure that the connection devices verify themselves with the RADIUS server before they are allowed to view the network. This will provide secure user management at the center and avoid unauthorized access.

M3 Justify the choices made in the implemented network security configuration.

EtherChannel

EtherChannel is a computer technological network where several physical Ethernet connections are integrated into a single logical channel. This enhances the bandwidth and enables traffic to pass more easily across the switches, routers or servers. In case one of them fails the rest of them will not fail and this makes the connection more stable. It also distributes traffic on all the operational links without overloading a single cable. EtherChannel is primarily used to enhance speed and to offer redundancy in company networks.

HSRP (Hot Standby Router Protocol)

The HSRP is a protocol used by Cisco to guarantee the availability of the gateway through the utilization of multiple routers. The router is configured as the active unit that processes traffic and the router is configured as the standby unit to come into play immediately the first router fails. This will eliminate network disconnection and keeps the users connected. HSRP is automatic in nature and offers automatic failover. It is principally used to ensure that the provision of high availability and the ongoing service of the important networks.

Switchport Port-Security

Switchport port-security is a switchport security protocol that limits access to a switch port. It operates by blocking unknown devices and specific MAC addresses. In case of an illegal laptop or gadget, the port may close or block. This prevents attacks like MAC flooding and also prevents intruders into the LAN. The objective of port-security is to render the local networks more controlled and secure.

Network Access Control (NAC)

Network Access Control is a mechanism that verifies machine access before fully permitting them to the entire network. It ensures that devices are compliant to standards like antivirus installed, updated software or standards set by the company regarding security. NAC may block or put a device in a restricted area as long as a device is not compliant. It is highly handy in

organizations having employees and visiting users. NAC is primarily used to make sure that safe and trusted devices are the only devices allowed to join the network.

GRE Tunnel (Generic Routing Encapsulation)

A GRE Tunnel is a protocol that provides a virtual private network between two networks that are far apart, which is situated on the internet. This tunnel is flexible to various applications as a number of different data and protocols can be sent within it. GRE however does not encrypt the traffic therefore it is commonly used with IPSec. GRE is used by businesses to connect their branch offices or remote locations. It is meant to offer easy and effective connectivity among untrusted networks.

IPSec (Internet Protocol Security)

IPSec is a set of protocols which provide security to data in transit over IP networks. It offers encryption as a measure of privacy protection, integrity verification as a measure of tampering and authentication as a measure of confirmation. VPNs have been popularly applied with IPSec, which provides remote employees and branch offices access to company resources in a secure manner. When information traverses the public internet, it is more crucial. The main function of IPSec is the provision of safe, confidential and trusted communication.

SSH (Secure Shell)

SSH is an insecure protocol that is used to administer devices and servers remotely. Contrary to Telnet that transmits data in plain text, all data is encrypted such that attackers cannot understand it in SSH. SSH helps administrators to log in, configure and trouble shoot routers, switches and servers without the danger of making them vulnerable. It is user friendly and compatible with nearly all systems. SSH is intended to encrypt and ensure safe remote control of network and system controls.

IOS IPS (Cisco IOS Intrusion Prevention System)

Cisco IOS IP is the default feature that can detect and prevent threats to one of the network devices. It captures real time traffic and compares this traffic with signatures to detect harmful patterns like worms, viruses or intrusion attacks. Suspicious activity may be blocked or alerted to the administrators when suspicious activity is detected. The direct placement of IPS on a router or

switch enhances network security at network points of entry. The primary role of IOS IPS is prevention of attacks.

Integrate Outcome

Combining EtherChannel, HSRP, Port-Security, NAC, GRE Tunnel, IPSec, SSH, IOS IPS, a network can perform well and be very secure. EtherChannel offers more rapid connection and reliability whereas HSRP offers persistent gateway connectivity. The control of the devices that are permitted is done by Port-Security and NAC to prevent any unauthorized access. GRE Tunnel and IPSec are used together in a bid to securely connect remote offices through the internet so that data remains confidential. SSH enables the administration to control devices securely, and IOS IPS incorporates the real-time threat identification. These technologies, when used together, form a safe, dependable and efficient network that minimizes downtime, attacks, and help to facilitate running of the business.

LO4 Undertake the testing of a network using a Test Plan

P6 Comprehensively test the network using a devised Test Plan

VLAN

```
10   Finance                          active    Fa0/6
20   SALE_AND_MKT                     active    Fa0/7
30   HR                               active
40   Customer_Support                 active
50   IT                               active
60   MM_Server                        active    Fa0/5
```

The implementation and verification of VLAN configuration has been done successfully. The switch ports are properly mapped and each department is allocated to VLAN. The VLANs are seen to be active and thus, the right set up and operation. As an illustration, VLAN 10 (Finance) is operational at port Fa0/6, VLAN 20 (Sales and Marketing) is operational at port Fa0/7 and VLAN 60 (Server) is operational at port Fa0/5. This output shows that the system is properly divided and is prepared to communicate on the safe side within departments.

Domain

```
ip domain-name info.com
```

The domain name info.com has been configured into the system and is successful. This validates the fact that the device is ready to support secure services e.g. generating SSH keys and authenticating. The domain name configuration is checked by the output to verify that it is activated and working as required.

Ether Channel

```
Switch#show ether summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-------------------------

1      Po1(SU)           PAgP   Fa0/2(P) Fa0/3(P)
```

The configuration and verification of the EtherChannel have been able to be done by using the following command show ether summary. The output verifies that Port-channel 1 (Po1) is active and it uses PAgP protocol and shares interfaces Fa0/2 and Fa0/3. Both ports indicate as in port-channel (P) and in use (U), which is evidence that the EtherChannel is operating properly to provide higher bandwidth and redundancy.

Access Mode for End Device

```
interface FastEthernet0/5
 switchport access vlan 60
 switchport mode access
```

Access mode configuration has been implemented successfully in order to interface FastEthernet0/5. The port is allocated to VLAN 60 and it is configured to access mode, which means that it is dedicated to one end device connection. This is to ensure that the interface is set up to bridge the end devices in the right VLAN segment with a secure connection.

Inter-VLAN Routing

```
Pinging 192.168.204.10 with 32 bytes of data:

Reply from 192.168.204.10: bytes=32 time<1ms TTL=127
Reply from 192.168.204.10: bytes=32 time<1ms TTL=127
Reply from 192.168.204.10: bytes=32 time=9ms TTL=127
Reply from 192.168.204.10: bytes=32 time=18ms TTL=127

Ping statistics for 192.168.204.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 18ms, Average = 6ms
```

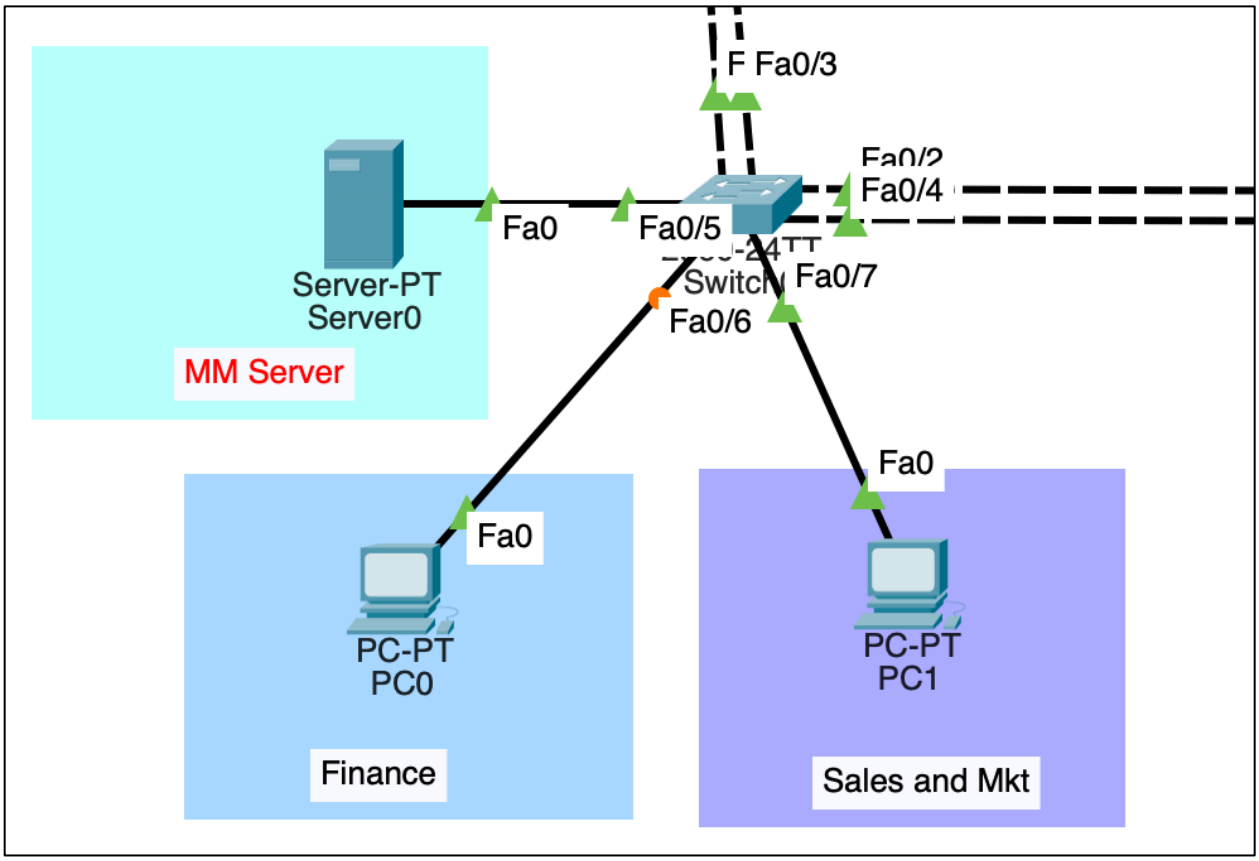
In the Inter-VLAN Routing set-up, pinging of the IP address of VLAN-50 192.168.204.10 has been tested. No lost packets in ping replies and this showed that VLANs are functioning properly. The values of the round-trip time (Minimum = 0ms, Maximum = 18ms, Average =6ms) suggest that devices in VLANs are consistently connected since the router can connect without any problem.

Port Security

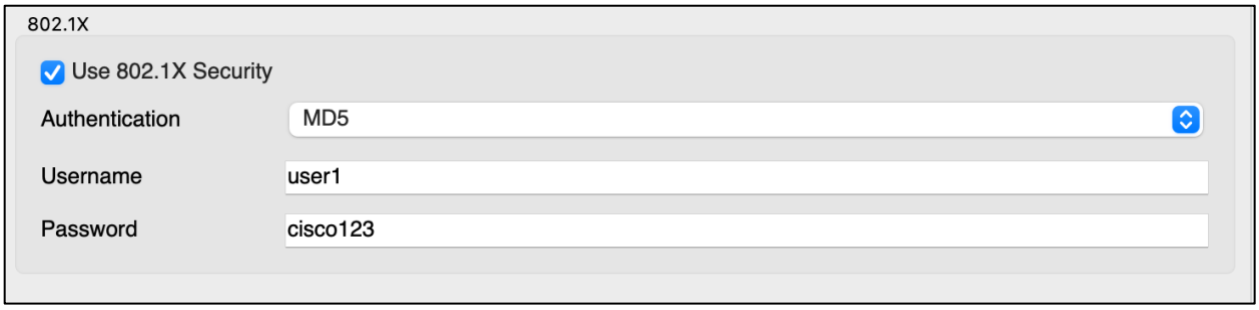
```
Switch#show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
               (Count)       (Count)        (Count)
-----------------------------------------------------------------------
        Fa0/6        1           1                0         Shutdown
        Fa0/7        1           1                0         Shutdown
-----------------------------------------------------------------------
```

The port-security configuration has been checked successfully by the help of the command show port-security. The result of the output indicates that in interfaces Fa0/6 and Fa0/7, only one secure MAC address is allowed, and the identified device is connected to the secure address. None of the security violations have been identified, and the security action, which is configured, will shut down in case of unauthorized access. This proves that port security is functioning in the right direction to prevent unauthorized devices.

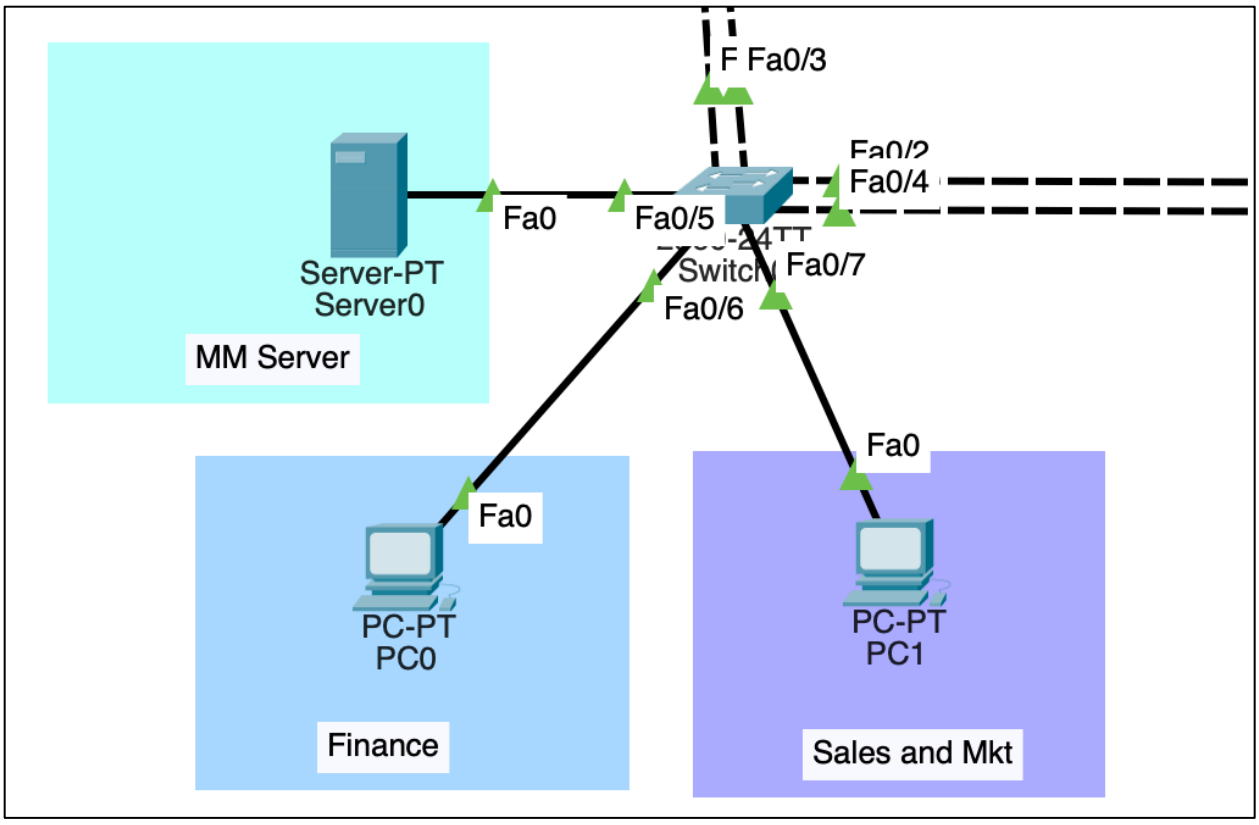
Port-Based Access



The 802.1X port-based access control configuration has been implemented and experimented successfully. At first, the end devices (Finance PC and Sales and Marketing PC) were attached to the switch and had to be authenticated prior to gaining access to the network.



Through the RADIUS server, the client authenticated using 802.1X security setup, whereby the usernames were user1 and cisco123 were used as the usernames and passwords respectively.



After the authentication was made, the devices were granted access to their respective VLANs and to the MM Server. This is the evidence that port-based authentication 802.1X is active and only the authorized users can access the network.

HSRP

Interface	Grp	Pri	P	State	Active	Standby	Virtual IP
Vl10	1	105	P	Active	local	192.168.200.5	192.168.200.1
Vl20	2	105	P	Active	local	192.168.201.5	192.168.201.1
Vl30	3	105	P	Active	local	192.168.202.5	192.168.202.1
Vl40	4	105	P	Active	local	192.168.203.5	192.168.203.1
Vl50	5	105	P	Active	local	192.168.204.5	192.168.204.1
Vl60	6	105	P	Active	local	192.168.205.5	192.168.205.1

HSRP (Hot Standby Router Protocol) was successfully experimented. As indicated in the output VLAN interfaces VLAN10-VLAN60 are pruned with priority 105 and in Active state in the local router. The VLANs are set with the virtual IP address, which is utilized in order to provide the redundancy of the gateway and there is always a standby router that would take up the role in the event the already in use router collapses. This is to indicate that HSRP is working correctly and this gives high availability and sustained network connection.

GRE Tunnel & IPSec VPN

```
Router#show int tunnel 0
Tunnel0 is up, line protocol is up (connected)
  Hardware is Tunnel
  Internet address is 10.0.0.1/8
  MTU 17916 bytes, BW 100 Kbit/sec, DLY 50000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 203.0.113.1 (GigabitEthernet0/0), destination 198.51.100.1
  Tunnel protocol/transport GRE/IP
    Key disabled, sequencing disabled
    Checksumming of packets disabled
  Tunnel TTL 255
  Fast tunneling enabled
  Tunnel transport MTU 1476 bytes
  Tunnel transmit bandwidth 8000 (kbps)
  Tunnel receive bandwidth 8000 (kbps)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 1
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 50 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     58 packets input, 9976 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
      0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

On the GRE tunnel, the IPSec VPN tunnel has been established and tested with a command show int tunnel 0. The output has proven that the tunnel 0 exists and protocol exists (connected) with source 203.0.113.1 and destination 198.51.100.1. The tunnel has been encapsulated using GRE over IP, and tested successfully with constant operation, no input/output errors, collisions and drops. The process of transmitting and receiving packets is functional which confirms that that the GRE tunnel and the IPSec VPN has been incorporated and that they are fully operational and ready to be used to conduct secure communications at the site to site level.

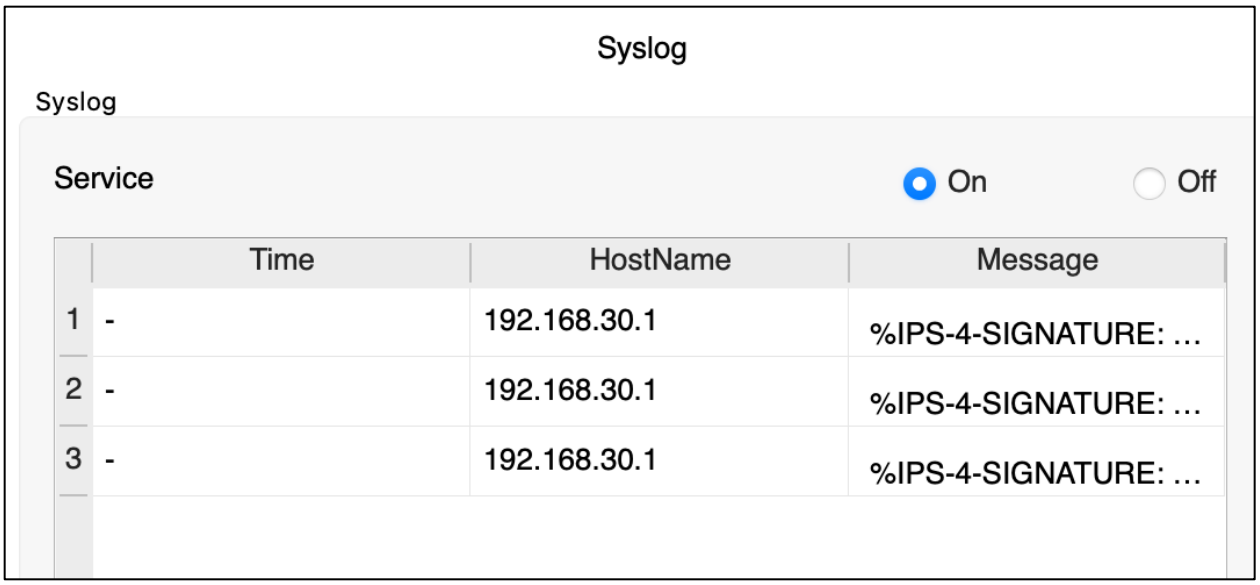
SSH

```
C:\>ssh -l admin 192.168.202.50

Password:



gw1>en
Password:
gw1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
gw1(config)# !
```

The SSH settings were also tested by connecting to the device remotely at 192.168.202.50. Authentication of passwords was provided and a session was allowed which provided secure access to privileged EXEC and configurations modes. This ensures the adequacy of SSH configuration and encrypted and secure remote control of network device.

IPS

```
C:\>ping 192.168.205.10

Pinging 192.168.205.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.205.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```



The set up of the IPS (Intrusion Prevention System) has been completed and tested. In trying to ping the target 192.168.205.10, all attempts to ping the target took 100 percent packet loss, indicating that IPS blocked the suspicious traffic. There is also proof of detection and prevention with Syslog output showing several IPS signature warnings of host 192.168.30.1. This confirms that IPS is vigilantly tracking, identifying and blocking malicious or unauthorized traffic as desired.

M4 Analyze the results of testing to recommend improvements to the network.

EtherChannel – Improvements Recommendation

The solution of EtherChannel proved to work well and interfaces Fa0/2, Fa0/3 were packaged into Port-Channel 1 with the PAgP providing redundancy and increased bandwidth. This ascertains the existence of load balancing of traffic as well as fault tolerance that improves the efficiency of the network. Yet, the use of PAgP alone can restrict the ability to connect with devices using standardized protocols, and no performance monitoring was evaluated. To optimize this setup, it is suggested to replace it with LACP to support more devices, activate periodic load balancing monitoring, and set up error detection systems to guarantee optimal failover and optimum usage of bandwidth capacity.

HSRP – Improvements Recommendation

Testing of HSRP was successful, the VLAN interfaces were configured and the local router was in the Active state to guarantee as much as possible redundancy in the gateway. This configuration reduces downtimes since the failing router can be replaced by a backup router, thereby enhancing availability. The problem is, however, that only one standby router was used and default timers were used, which might slow down the failover in the cases of actual incidents. This can be enhanced by setting up several standby routers, optimizing hello and hold timer to ensure faster recovery and using object tracking to track important interfaces so that failover is smarter and more reliable.

GRE Tunnel & IPSec VPN – Improvements Recommendation

The GRE tunnel across IPSec was functioning properly and the transmission was steady with no input or output errors identified which indicates that the site-to-site secure communication is in effect. This enhances connectivity among the branches and ensures encryption and secrecy by use of IPSec. The downside, however, is that GRE does not come with security and scalability was not applied to support the future growth. To improve on this solution, adapting DMVPN to a larger multi-branch scalability to provide a stronger IPSec algorithm such as AES with SHA-2 and the ability to provide a consistent performance monitoring and logging will aid in the long term scalable and effective tunnelling.

Switchport Port Security – Improvements Recommendation

The port security on Switchport port was configured and effective control was observed over guarding unauthorized access since no security breach was reported. This will ensure that VLAN segments are secure and rogue devices do not enter the network. The more important problem, however, is that the configuration is quite rigid; when the legitimate device is changed, the mode of shutdown violation might falsely interrupt the service. In an effort to augment this attribute, MAC addresses can be made to be sticky to dynamically learn legitimate machines, and restrict or protect violation modes can be used to eliminate downtime and still be able to block an intruder.

Network Access Control (802.1X) – Improvements Recommendation

The access control configuration that was implemented at the port was effective and provided access to devices after RADIUS authentication, which was effective in limiting the access of unauthorized connections. This is far better in enhancing security as verification is done on the users before they are allowed to join VLANs. However, the problem is that one RADIUS server poses a threat of service failure in the event of server downtime, and only password-based authentication would be used, and it would be possible to exploit it. A second backup RADIUS server should be installed to enhance reliability and security, integration with centralized directories such as active directory should be implemented to manage identities better and certificate-based authentication should also be introduced to enhance better validation.

IPSec – Improvements Recommendation

IPsec setting using the GRE tunnel worked well and encrypted traffic was confirmed, and no reports of errors, which assured confidentiality, integrity, and authentication of data traffic. This proves that VPN can secure remote connections. Nevertheless, there are possible limitations which may occur when using older algorithms like DES or MD5, and high traffic rates may negatively affect the work of the software-based routers. Improvements would be to implement stronger algorithms, such as AES-256 with SHA-2, implementing hardware-based VPN accelerators to make the throughput better, and revising the IPSec policy regularly to ensure that it provides a high level of protection to changes in cyber threats.

SSH – Improvements Recommendation

The SSH remote access was tested and proved successful since encrypted sessions were created and the password authentication was used to provide access to the device with high security, which removes the risks of plaintext management. This demonstrates the sufficiency of safe remote administration. The worry is that it uses password-based authentication and is still prone to brute-force attack, and that there is a risk of using older versions of SSH. It can be improved by ensuring the use of SSH version 2 exclusively and using ACLs to ensure that only certain management IPs can gain access to SSH which will combine to provide greater and more limited access to the remote devices.

IOS IPS – Improvements Recommendation

The IOS Intrusion Prevention System performed well, and it was able to block and identify the suspicious traffic, with the evidences provided in the syslog logs that the IPS is working, and malicious packets are getting blocked before reaching the internal devices. It proves that the system is defending the network actively. The issue is that false positives will potentially block legitimate traffic by accident, and outdated IPS signatures will diminish the accuracy of detection. Some improvements that can be made are regular updates of IPS signature database, better policies to minimize false alarms and incorporation of logs into a centralized SIEM to facilitate more effective monitoring, correlation and proactive response to threats.

References

Fortinet [Online] Available from:

https://www.fortinet.com/resources/cyberglossary/cia-triad

Accessed Date: 6.9.2025

IT Governance [Online] Available from:

https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important

Accessed Date: 6.9.2025

SecurityScorecard [Online] Available from:

https://securityscorecard.com/blog/what-is-the-cia-triad/

Accessed Date: 7.9.2025

NinjaOne [Online] Available from:

https://www.ninjaone.com/blog/ssl-vpn-vs-ipsec

Accessed Date: 7.9.2025

Lightyear.ai [Online] Available from:

https://lightyear.ai/tips/ipsec-versus-tls

Accessed Date: 7.9.2025

Medium (RocketMeUpCybersecurity) [Online] Available from:

https://medium.com/@RocketMeUpCybersecurity/comparing-ssl-tls-and-ipsec-choosing-the-right-protocol-for-your-network-needs-423b9f4aa218

Accessed Date: 7.9.2025

Privacy.com [Online] Available from:

https://www.privacy.com/blog/ssl-vpn-vs-ipsec

Accessed Date: 8.9.2025

ConnectWise [Online] Available from:

https://www.connectwise.com/blog/ssl-vs-ipsec-vpns

Accessed Date: 8.9.2025

GoodAccess [Online] Available from:

https://www.goodaccess.com/blog/ipsec-vpn

Accessed Date: 8.9.2025

ITBD.net [Online] Available from:

https://itbd.net/blog/noc/ssl-vpn-vs-ipsec-choosing-the-right-vpn-protocol-for-your-business/

Accessed Date: 8.9.2025