

Construct and mitigating security vulnerabilities and weaknesses

by Ayush Kumar

Submission date: 05-May-2023 10:38PM (UTC+0100)

Submission ID: 204995506

File name:

45492_Ayush_Kumar_Construct_and_mitigating__security_vulnerabilities_and__weaknesses_497076_1139712376.docx (1.88M)

Word count: 8474

Character count: 50088



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Construct and mitigating security vulnerabilities and
weaknesses

By

Ayush Kumar

Lecturer: Dr Carlene Campbell

Report submitted as part of the requirements for the
award of MSc Computer networks and Cyber Security

May 2023

Table of Contents

Abstract.....	4
1. Introduction.....	5
1.1 Aim.....	5
1.2 Objectives	5
2. Laboratory Task (Part 1)	6
2.1 Security threats facing modern network infrastructures	6
a. Network security	6
b. Various types of threats and attacks.	7
c. Mitigating Malware and Network Attacks	8
d. Essential Principles for Securing a Computer Network	9
e. Mitigating the Impact of Network Attacks in Small to Medium-Sized Enterprises 	10
f. Enhancing Network Security with Cisco Network Foundation Protection Framework	11
g. Managing the Fallout from Malware in Small to Medium-Sized Businesses	12
h. Endpoint Security: Understanding Vulnerabilities and Protection Methods	13
2.2 Secure Cisco Routers	14
2.3. Implementing AAA on Cisco Routers with Local and External Server Database	16
a. Enhancing Network Security with AAA Framework	16
2.4 Use ACLs to mitigate attacks to Cisco routers and networks.....	18

2.5 Best Practices for Secure Management, Network Design and Reporting.....	20
a. Implementing a Security Policy for an Organization.....	20
b. Techniques and Tools for Network Security Testing.....	20
2.6 Mitigating Layer 2 Attacks: Best Practices and Strategies	22
a. Understanding Network Vulnerabilities and Mitigation Techniques	22
2.7 Implementing Cisco IOS IPS for Network Security	23
a. Strengthening Network Security with Network-Based Intrusion Prevention Systems	23
b. Detecting Malicious Network Traffic with Signature-Based Methods.....	23
c. Cisco IOS IPS operations using CLI.....	24
2.8 Implementing Site-to-Site VPN for Secure Remote Access.....	25
a. Understanding the Purpose and Benefits of Virtual Private Networks (VPNs) ...	25
b. Understanding the Operation of IPSec VPNs for Secure Remote Access.....	26
c. The Synergy of Encryption, Hashing, and Digital Signatures for Data Security .	28
d. Ensuring Data Integrity and Authentication with Cryptographic Hashes.....	29
f. Enhancing Data Security with Public Key Infrastructure for Confidentiality and Authentication.....	30
2.9 Cisco ASA Deployment for Robust Firewalling and NAT/PAT Services	32
a. Functionality of Cisco ASA as an Advanced Stateful Firewall	32
3. Secure Network Infrastructure (PART 2)	33
3.1 Blueprint Design	33
3.2 Proposal.....	33

3.3. Invoice	39
4. Conclusion and Recommendation	41
5. References	42

Table of Figure

Figure 1: R3 and PC-C, Management and securing of network device.....	14
Figure 2: R1 control plan security	14
Figure 3: R2 Control plane security	15
Figure 4: R3 control plane security.....	15
Figure 5: PC-C AAA authentication	17
Figure 6: R1 AAA authorization and accounting	17
Figure 7: R3 (ACLs) to filter traffic and mitigate network attacks	18
Figure 8: R3 classic firewall	18
Figure 9: R3 Zone-Based Policy Firewall	19
Figure 10: R3 signature configure	24
Figure 11: R2 and PC-C ping verify	25
Figure 12: Site-to-site IPsec VPN.....	27
Figure 13: Verifying ping from PC-A, PC-B, PC-C with using tracert.....	28
Figure 14: A2Z Technologies Ltd blueprint design with Swansea, Cardiff map	33

Abstract

Completing Part 1 of the assignment has proven to be an extremely valuable experience, providing me with critical, hands-on practical skills, and experience in successfully implementing and securing computer network infrastructures. The laboratory tasks were well-structured, allowing for a clear understanding and appropriate application of network security concepts. I acquired vital knowledge and skills, such as configuring network devices, troubleshooting network issues, and implementing security controls to protect against various cyber threats. My proficiency in utilizing tools and technologies to monitor and manage network traffic, detect anomalies, and respond to security incidents also significantly improved. This strengthened my underlying knowledge of network security and thoroughly increased my confidence in successfully implementing and securing network infrastructures.

Part 2 of the assignment was a challenging yet fulfilling experience, as it introduced me to the process of proposing a secure network infrastructure for a hypothetical organization based on a specific scenario. Through detailed analysis of the organization's requirements and potential security risks, I was able to design an effective multi-layered defence strategy that included appropriate security controls and technologies to mitigate various cyber threats. Furthermore, the proposed network infrastructure design was scalable, resilient, and easily manageable, with a focus on minimizing downtime and ensuring high availability of critical services. The comprehensive disaster recovery plan ensured seamless business continuity in the event of any unforeseen incidents. By applying the knowledge and skills obtained from Part 1 of the assignment and other Cisco Cybersecurity courses, I was able to develop my ability to analyse complex scenarios, propose effective solutions, and communicate my findings clearly and confidently to stakeholders. Overall, this assignment proved to be an exceptional learning experience that has equipped me with essential skills and knowledge necessary to succeed in network security and provided valuable insights that will enable me to excel in my career.

1. Introduction

The purpose of this assignment is to equip budding Network Security professionals with the essential competencies and practical experience required to competently handle real-world network security scenarios. It comprises two parts, each with a distinct focus on facets pertinent to network security.

1.1 Aim

Aim of this assignment is to give a complete and integrated approach to network security, encompassing procedural and troubleshooting expertise, implementation and fortification of computer network infrastructures using diverse tools and configurations, and devising robust network infrastructure proposals that address specific scenarios.

1.2 Objectives

Specifically, this assignment endeavours to achieve the following objectives:

- Foster technical aptitude in network security.
- Foster risk management skills, enabling identification and mitigation of potential threats and vulnerabilities.
- Foster the capacity to design secure network infrastructures that satisfy particular organizational requirements.

2. Laboratory Task (Part 1)

2.1 Security threats facing modern network infrastructures

a. Network security

The modern digital landscape has brought with it a host of unprecedented security threats that affect network infrastructures. Tackling such threats requires a multifaceted approach that involves a combination of technical and administrative controls. The practice of network security involves safeguarding computer networks against unauthorised access, misuse, alterations. At its core, network security entails implementing a set of security measures and protocols to safeguard the integrity, confidentiality and availability of data transmitted over a network. This is achieved through strategies such as encryption, intrusion detection and authentication, access control, prevention systems, firewalls and vulnerability management, which work together to prevent unauthorized access, detect network-based attacks and minimize the impact of security incidents [1].

It is imperative for organizations to adopt a comprehensive and proactive approach to network security, involving regular risk assessments, security audits, and updates to security policies and procedures. The increased risk of attacks has made network security a critical aspect of information security, and organizations must prioritize it to protect sensitive data, maintain business operations, and comply with regulatory requirements [2].

b. Various types of threats and attacks.

The contemporary world of interconnectivity exposes computer networks and systems to a broad spectrum of security threats and attacks. It is imperative to delineate the multiple kinds of threats and attacks that plague these systems. Some of the most widely prevalent include Malware attacks, which comprise software specifically designed to corrupt computer systems, thief data, or gain unauthorized access, encompassing viruses, worms, and Trojan horses. Phishing attacks are a category of social engineering attack which entails the duping of customers into disclosing private information like credit card numbers and login passwords, or personal details, through deceitful emails or websites. DoS attacks entail overwhelming the target system with traffic, resulting in it being unavailable to users. Man in the middle attacks involve the interception and alteration of data during transmission between two parties, enabling attackers to pilfer sensitive data. Password attacks entail endeavouring to crack or guess user passwords to achieve unauthorized entry into the system. Insider threats encompass employees or other trusted personnel who manipulate their authorized access to the system or data for malicious motives. Employing effective security measures like firewalls, anti-malware prevention systems and intrusion detection software can safeguard against these and other forms of threats and attacks. Regular user education and awareness training will also help users identify and avoid potential threats. A layered approach to security is critically crucial in safeguarding against an ever-evolving landscape of threats and attacks [3] [4].

c. Mitigating Malware and Network Attacks

In order to counter the adverse effects of malware and common network attacks, it is integral to employ effective tools and procedures designed to prevent, detect, and respond to security breaches. These attacks can significantly harm computer systems and networks; therefore, the implementation of mitigation measures is crucial [5].

Anti-malware software serves as a critical component in the fight against malware, allowing for the detection and removal of malware from infected systems and the prevention of further infections. Firewalls act as a powerful tool, blocking unauthorized network access and preventing various types of attacks, including DDoS attacks. Intrusion Detection and Prevention Systems help to identify and respond to attacks in real-time, acting as a proactive line of defence against cyber threats [6] [7].

User education and awareness constitute vital measures in combating cyber threats, educating users on the risks of malware and common network attacks, presenting valuable insights that can help them recognize and prevent potential threats. The implementation of strong password policies and regular backups of vital data can also serve to mitigate the effects of cyber threats.

Overall, a comprehensive and proactive approach to security, encompassing a combination of technical controls and user education, is fundamental to the mitigation of the effects of malware and common network attacks [8].

d. Essential Principles for Securing a Computer Network

In ensuring the security of networks, a fundamental set of principles serve as guidelines, aimed at protecting the network from unwanted access, threats and data breaches.

The principle of defence in depth is a critical component, necessitating the implementation of multiple layers of security measures that can offer protection against diverse types of threats. Defensive measures may include firewalls, as well as anti-malware software.

The principle of least privilege involves the restriction of sensitive resources access based on user identity and role. This proactive approach can limit the damage that may arise from a compromised user account.

Encryption serves as another fundamental principle, focused on securing sensitive data during transmission over a network, preventing unauthorized access.

Adequate access controls are likewise, essential for implementing network security, preventing unauthorized access to critical systems and data that could serve as a vulnerability, opening up the network to potential cyber-attacks.

Finally, keeping software and firmware updates and patches, serves as a final line of defence against cyber-attacks, ensuring that known vulnerabilities are adequately addressed.

Adhering to these fundamental principles, organizations can take proactive measures to secure their networks, protecting against common cyber threats [9].

e. Mitigating the Impact of Network Attacks in Small to Medium-Sized Enterprises

Alleviating the outcome of common network attacks in a small to medium-sized business can be quite daunting; however, there are numerous measures that can be put in place to diminish the likelihood of successful attacks [10].

Firstly, it is crucial to execute fundamental safety measures such as anti-malware software, firewalls, intrusion detection, anti-virus, and prevention systems. These tactics can aid in detecting and dissuading various types of attacks before any substantial impairment occurs.

Secondly, regular user education and awareness training can ensure that personnel are cognizant of the hazards associated with common attacks, such as phishing and social engineering. These educational sessions can encompass instruction on how to detect and refrain from dubious emails, links, and attachments [11].

Thirdly, implementing robust password policies and mandating frequent password alterations can restrict password assaults. Two-factor authentication can also be utilized to provide an additional layer of security.

Fourthly, regular backups of critical data can diminish the effects of attacks such as ransomware by enabling data restoration in the event of an attack.

Lastly, it is essential to undertake periodic reviews and upgrades of security measures to ascertain that they remain effective against advancing threats. By adopting these methods, small to medium-sized businesses can aid in mitigating the impact of common network attacks and fortify their vital data and systems [12] [13].

f. Enhancing Network Security with Cisco Network Foundation Protection Framework

The Cisco Network Foundation Protection framework is a formidable security solution that offers widespread protection against an array of network threats and attacks. It encompasses various critical components that work collectively to create a layered approach towards securing networks [14].

Foremost, the NFP framework comprises sophisticated capabilities for detecting and preventing threats, including firewalls, intrusion detection and prevention, and malware detection technology. These capabilities efficiently identify and hinder known and unknown threats before they can inflict damage.

Furthermore, the NFP framework includes network segmentation and access control mechanisms that limit the propagation of attacks, as well as prevent unauthorized access to essential resources. Additionally, this framework integrates identity and access management solutions that facilitate the management of user identities, and control access to network resources based on levels of authorization.

Lastly, the NFP framework is equipped with advanced monitoring and reporting capabilities that provide real-time visibility into network activity, and aid organizations in identifying and responding to security incidents promptly and effectively [15].

Leveraging the Cisco NFP framework, organizations can establish a highly secure network that is resistant to a wide range of threats and attacks. This comprehensive, integrated security solution can be customized for the unique requirements of any organization, regardless of size or complexity [16].

g. Managing the Fallout from Malware in Small to Medium-Sized Businesses

A combination of both technical and non-technical approaches must be employed.

First and foremost, modern anti-virus and anti-malware software must be installed across all network-connected devices. This will assist in the detection and removal of any dangerous software before it is able to inflict any significant damage.

The regular application of software updates and patches should also be prioritized so that known vulnerabilities can be swiftly addressed and thus minimized [13].

It is also strongly recommended that all employees undergo regular education and training sessions aimed at promoting awareness and understanding of the risks associated with viruses, worms, and Trojan horses. This may include specialized training on the identification and avoidance of suspicious emails, links, and attachments as added measures of defence.

Restricting access permissions and controls can also limit the risk of these types of malware being able to rapidly spread throughout a network.

Finally, it is crucial to ensure that critical data is regularly backed up in order to facilitate swift and effective restoration in the event of an attack. By implementing such measures, small to medium-sized businesses can take proactive steps towards mitigating the effects of viruses, worms, and Trojan horses, thereby ensuring that their vital systems and data remain optimally protected [17].

h. Endpoint Security: Understanding Vulnerabilities and Protection Methods

Endpoint vulnerabilities and protection techniques are topics of significant importance in the realm of network security. Endpoints encompass various devices, such as laptops, desktops, smartphones, and tablets, that are interconnected with a network. These devices are often targeted by threat actors to exploit vulnerabilities and gain unauthorized access or steal confidential information. Thus, safeguarding endpoints is essential for maintaining the integrity and security of networks [18].

To protect endpoints against malicious attacks, it is vital to implement advanced antivirus software that can detect and remove malware. EDR tools can also aid in identifying and responding to threats in real-time. Organizations can take a more comprehensive approach to endpoint protection by utilizing endpoint protection platforms that include features such as firewall, intrusion prevention, and data loss prevention.

Strengthening access controls and permissions is also crucial in preventing unauthorized access to critical systems and data. Regular security awareness training for employees can also facilitate awareness of the potential dangers of common threats like phishing and social engineering.

Lastly, applying regular software updates and patches to all endpoints can address any known vulnerabilities effectively. By following these best practices, organizations can reduce the risk of endpoint attacks, ensuring robust network security and protecting sensitive data [19].

2.2 Secure Cisco Routers

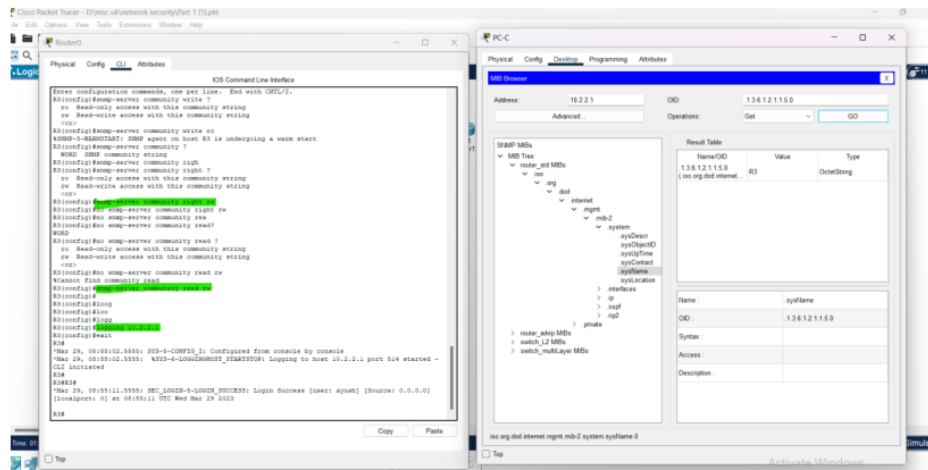


Figure 1: R3 and PC-C, Management and securing of network device

b. Control plane security

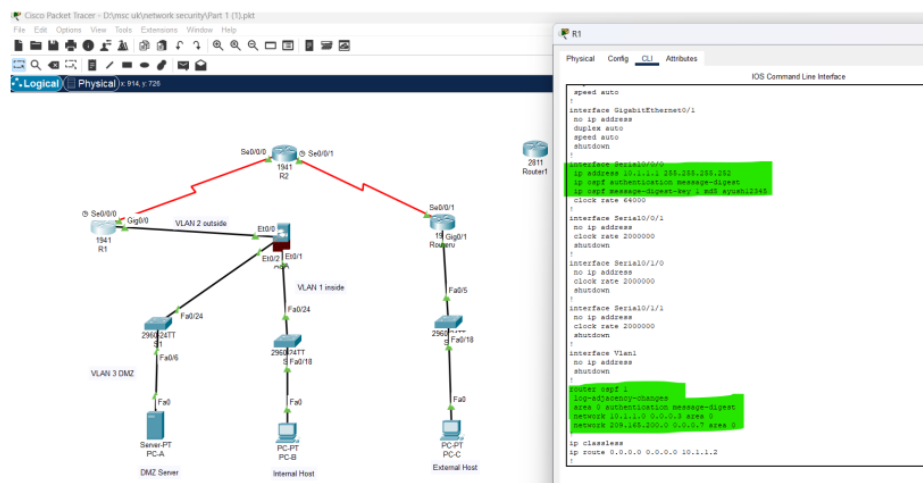


Figure 2: R1 control plan security

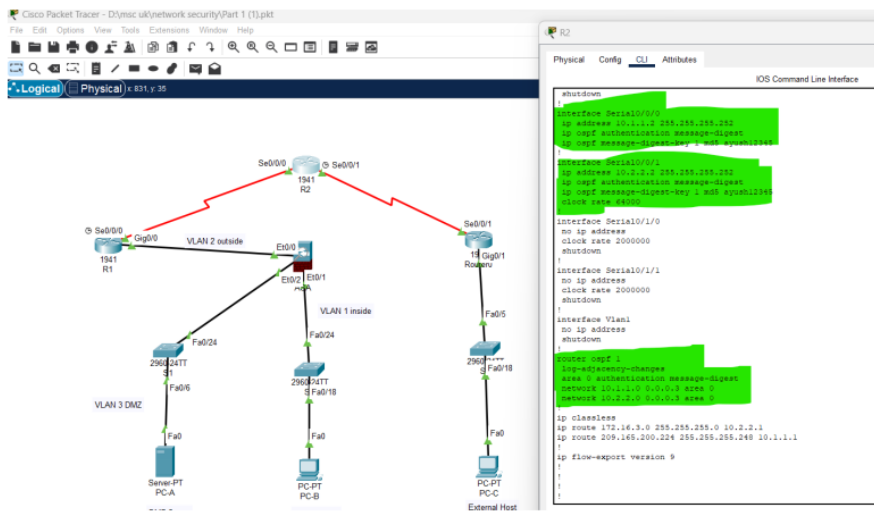


Figure 3: R2 Control plane security

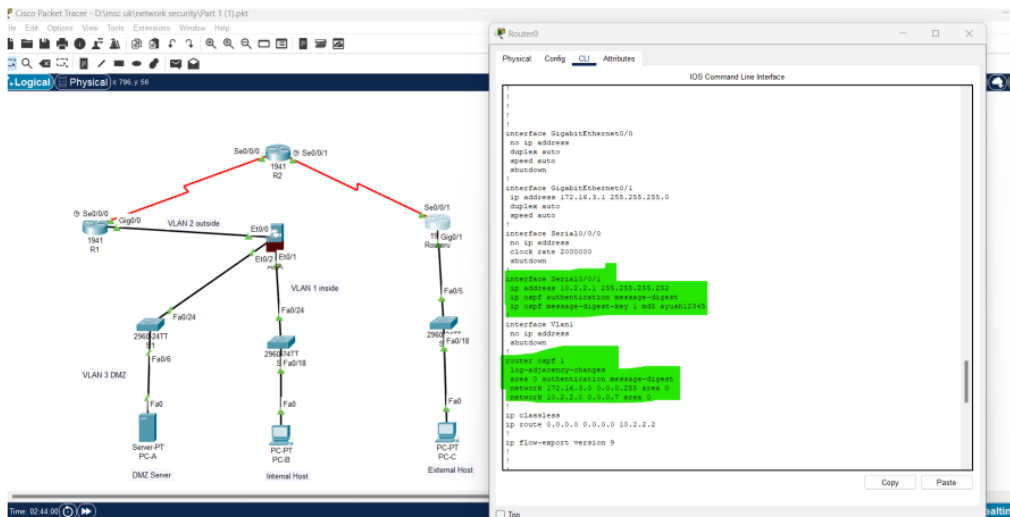


Figure 4: R3 control plane security

2.3. Implementing AAA on Cisco Routers with Local and External Server

Database

a. Enhancing Network Security with AAA Framework

The reinforcement of AAA (Authentication, Authorization, and Accounting) framework on Cisco routers utilizing a local router database alongside an external server is crucial in securing a network. The AAA methodology ensures network security by regulating access to network resources. It verifies users' identity, permits or denies access to resources based on user credentials, and regulates users' activity for accounting purposes [20].

The Authentication process in AAA guarantees users' identity before granting them access to network resources. It validates user credentials by cross-referencing them against a local or remote database. Authorization identifies a user's capabilities and sets restrictions on the resources they can access using access control lists. Accounting encompasses keeping a record of user activity to monitor the usage of resources and track security incidents or policy violations such as login attempts, resource usage, and command execution.

The implementation of AAA assists organizations in controlling access to network resources, preventing unauthorized access, and maintaining accountability for user activity. This increases network security, curtailing the likelihood of data breaches and other security incidents [21].

b. AAA authentication that validates users against a local database.

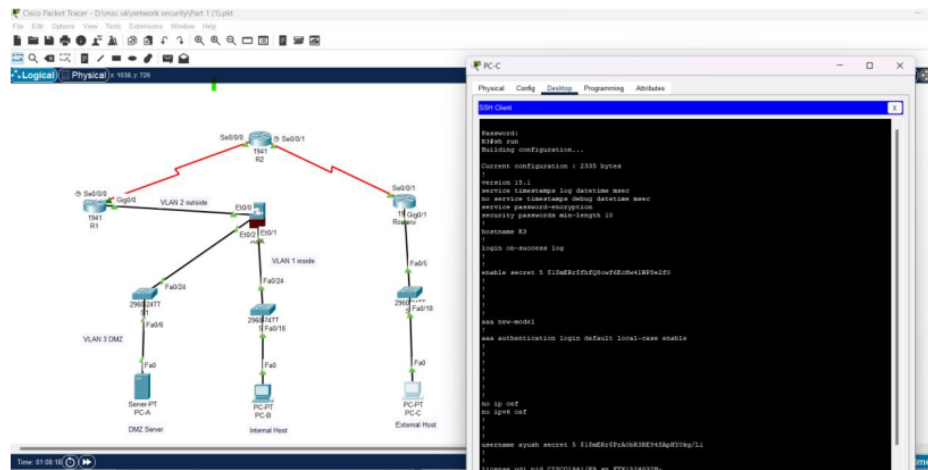


Figure 5: PC-C AAA authentication

c. Server-based AAA authorization and accounting

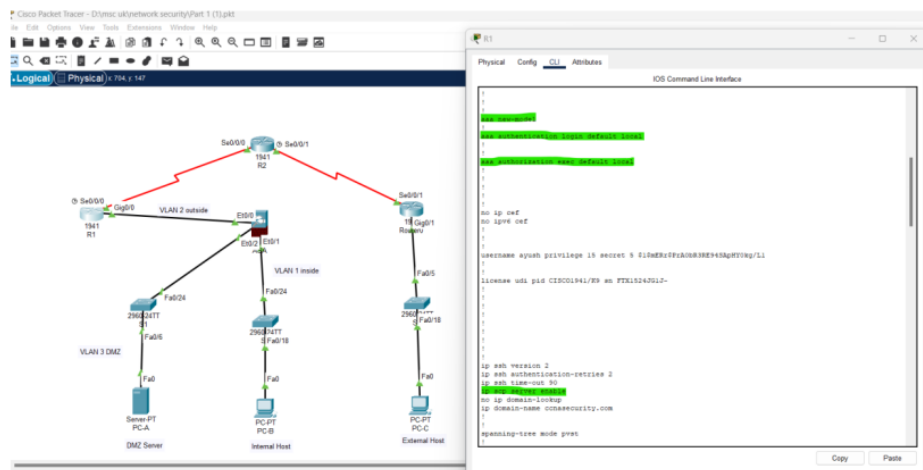


Figure 6: R1 AAA authorization and accounting

2.4 Use ACLs to mitigate attacks to Cisco routers and networks

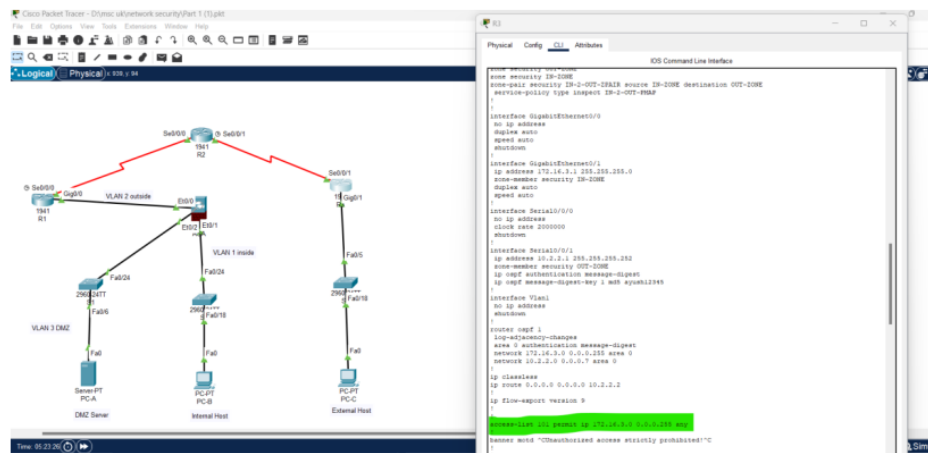


Figure 7: R3 (ACLs) to filter traffic and mitigate network attacks

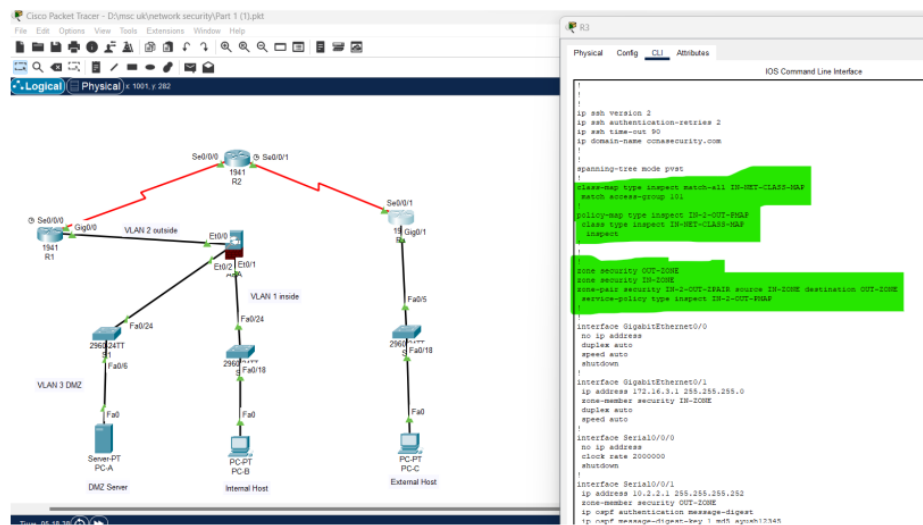


Figure 8: R3 classic firewall

```

R3#sh zon
R3#sh zone-
R3#sh zone-pair sec
R3#sh zone-pair security
Zone-pair name IN-2-OUT-2PAIR
    Source-Zone IN-ZONE Destination-Zone OUT-ZONE
    service-policy IN-2-OUT-PMAP

R3#sh pol
R3#sh policy-map ty
R3#sh policy-map type ins
R3#sh policy-map type inspect zon
R3#sh policy-map type inspect zone-pair se
R3#sh policy-map type inspect zone-pair sessions

policy exists on zp IN-2-OUT-2PAIR
Zone-pair: IN-2-OUT-2PAIR

    Service-policy inspect : IN-2-OUT-PMAP

        Class-map: IN-NET-CLASS-MAP (match-all)
            Match: access-group 101
            Inspect

        Class-map: class-default (match-any)
            Match: any
            Drop (default action)
                0 packets, 0 bytes
R3#sh zone
R3#sh zone secu
R3#sh zone security
zone self
    Description: System defined zone

zone OUT-ZONE
    Member Interfaces:
        Serial0/0/1

zone IN-ZONE
    Member Interfaces:
        GigabitEthernet0/1

```

Figure 9: R3 Zone-Based Policy Firewall

2.5 Best Practices for Secure Management, Network Design and Reporting

a. Implementing a Security Policy for an Organization

The implementation of a comprehensive security policy is paramount in safeguarding an organization's network and vital data. A security policy acts as a guiding framework, establishing a set of rules and guidelines to protect against unauthorized access, misuse, or theft of assets and sensitive information [22].

This measure requires coverage across all aspects of network security, focusing on access controls, user management, password policies, data encryption, backup and recovery procedures, and incident response protocols. The first step to implementing a comprehensive security policy involves conducting an in-depth risk assessment to identify possible vulnerabilities and threats. Based on this evaluation, organizations can develop policies and procedures to counter the identified risks and threats effectively.

The policy must be unambiguously communicated to all employees and stakeholders.

Adequate training should be provided to ensure that everyone understands their contribution to maintaining network security vigilantly. Regular reviews of the security policy must be conducted to ensure that it is up-to-date and pragmatic in addressing new and emerging threats and vulnerabilities [23].

b. Techniques and Tools for Network Security Testing

The process of network security testing holds immense significance when it comes to ensuring an organization's network infrastructure's reliability and security. There exist several tools and techniques that experts employ to achieve the objective of network security testing

effectively. One of such techniques includes vulnerability scanning that employs automated tools to scrutinize the network and establish a report of all vulnerabilities with their corresponding severity ratings [24].

Another technique, penetration testing, involves imitating an attacker's strategy to infiltrate a network's defence system to unveil vulnerabilities and evaluate the potential impact of a security breach. Network traffic analysis is yet another technique where experts analyse the network traffic to identify any suspicious activity that may suggest a security breach has occurred.

Password cracking tools, too, play a critical role in network security testing, and experts employ them to evaluate the passwords of the network users and identify weak passwords that may quickly succumb to a security breach. Web application security scanners are designed explicitly to scan web applications for security gaps, including cross-site scripting and SQL injection [25].

By leveraging these techniques and tools, network security experts can identify vulnerabilities and resolve them before attackers compromise an organization's critical infrastructure. In effect, it ensures that the network infrastructure remains protected and reliable against various threats, bolstering the overall security of the organization [26].

2.6 Mitigating Layer 2 Attacks: Best Practices and Strategies

a. Understanding Network Vulnerabilities and Mitigation Techniques

The Layer 2 framework of a network plays a crucial role in enabling communication among devices that belong to the same network segment. However, it also presents various susceptibilities that pose a threat to the security of the network. Common vulnerabilities include MAC address spoofing, ARP spoofing, VLAN hopping, and Spanning Tree Protocol (STP) attacks [27].

To curb these vulnerabilities, network administrators need to put in place different techniques. One such technique is to leverage port security to restrict the number of MAC addresses that can be learned on a given port, thus deterring MAC address spoofing attacks. Another practice is utilizing ARP inspection to authenticate ARP packets before forwarding them and prevent ARP spoofing attacks. VLAN hopping can also be prevented by using VLAN access control lists (ACLs) to constrain VLAN traffic, while BPDU guard can be employed to curb STP attacks through the disabling of ports that receive BPDU messages. Furthermore, network administrators can set up network segmentation, firewall rules, and access control policies to boost the security of the Layer 2 infrastructure.

As indicated, securing the Layer 2 infrastructure is fundamental to ensure overall network security. Network administrators must take a proactive stance by deploying relevant mitigation techniques that impede unauthorized access, data interception, and attacks [28] [29] [30].

2.7 Implementing Cisco IOS IPS for Network Security

a. Strengthening Network Security with Network-Based Intrusion Prevention Systems

Network-based Intrusion Prevention Systems (IPS) serve as a proactive measure by constantly surveillant and obstructing network traffic that overlaps with predefined attack signatures or abnormal behaviour patterns. In essence, an IPS functions similar to a highly evolved firewall that not only regulates traffic based on predetermined protocols but also scrutinizes it for known and unknown attacks in real-time.

In the event of an attack being identified by an IPS, it can adopt multiple courses of action such as halting the traffic, resetting connections, or generating an alert that warrants further investigation. IPS further proves to be an asset by furnishing network administrators with crucial feedback about the network's security continuity in identifying at-risk systems and traffic [31]. Furthermore, IPS systems can be integrated with additional tools like Security Information and Event Management (SIEM) systems to establish a holistic approach to network security. By employing IPS, network administrators can shore up network security fortifications to ward off a broad spectrum of attacks [32].

b. Detecting Malicious Network Traffic with Signature-Based Methods

A signature is a distinctive code or pattern unique to a specific malware or attack. Their creation can be done either by manual intervention by security experts or through the deployment of automated machine learning algorithms. When network traffic undergoes an analysis, the system compares it with a pre-existing database of signatures. In the event of a match being found, the system responds by identifying the traffic as malicious and executing the relevant actions such as alert generation or traffic blocking. Signatures are most

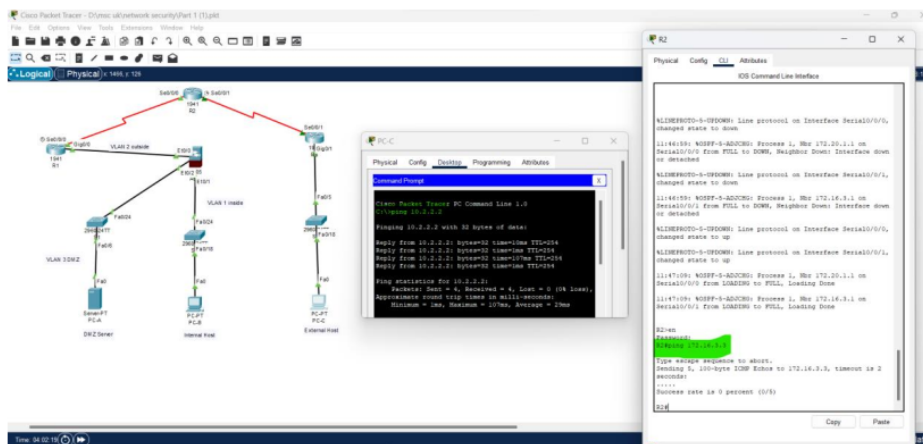


Figure 11: R2 and PC-C ping verify

2.8 Implementing Site-to-Site VPN for Secure Remote Access

a. Understanding the Purpose and Benefits of Virtual Private Networks (VPNs)

The fundamental aim of a Virtual Private Network (VPN) is to establish a secure and confidential connection amongst two or more remote networks over the internet. VPNs are prominently employed to enable remote workers to access the resources and services of a company's internal network comprehensively and securely from a remote location.

When a VPN connection is initiated, all transmitted data between the remote device and the network is encrypted and conveyed through a secure tunnel [35]. Through this encryption, any unauthorized access to the data being transmitted is prevented, even in the possible event of interception by third parties. VPNs can also be utilized to circumvent geographical restrictions to access content that might be inaccessible in certain regions. By connecting to a VPN server situated in a different region, a user can obtain access to content that is typically unavailable in their location.

Overall, the goal of VPNs is to provide a secure and confidential connection that enables remote access to network resources and circumvents geographical restrictions. VPNs have become an indispensable tool for businesses and individuals who necessitate secure and confidential internet access [36].

b. Understanding the Operation of IPSec VPNs for Secure Remote Access

The fundamental aim of a Virtual Private Network (VPN) is to establish a secure and confidential connection amongst two or more remote networks over the internet. VPNs are prominently employed to enable remote workers to access the resources and services of a company's internal network comprehensively and securely from a remote location.

When a VPN connection is initiated, all transmitted data between the remote device and the network is encrypted and conveyed through a secure tunnel. Through this encryption, any unauthorized access to the data being transmitted is prevented, even in the possible event of interception by third parties. VPNs can also be utilized to circumvent geographical restrictions to access content that might be inaccessible in certain regions. By connecting to a VPN server situated in a different region, a user can obtain access to content that is typically unavailable in their location. Overall, the goal of VPNs is to provide a secure and confidential connection that enables remote access to network resources and circumvents geographical restrictions. VPNs have become an indispensable tool for businesses and individuals who necessitate secure and confidential internet access [37] [38].

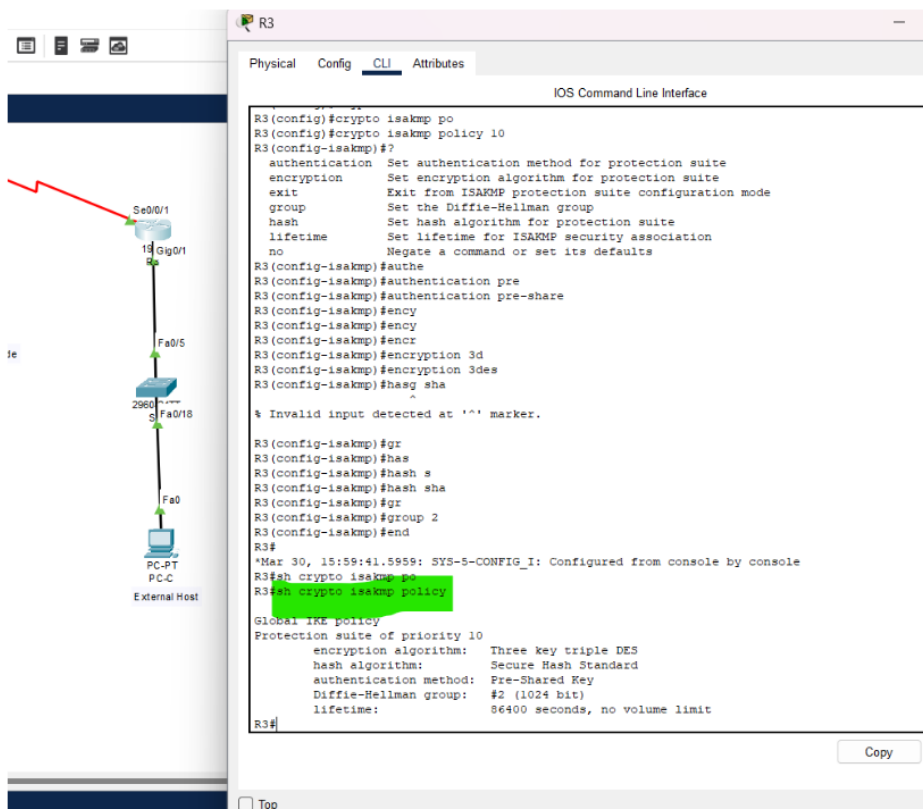


Figure 12: Site-to-site IPsec VPN

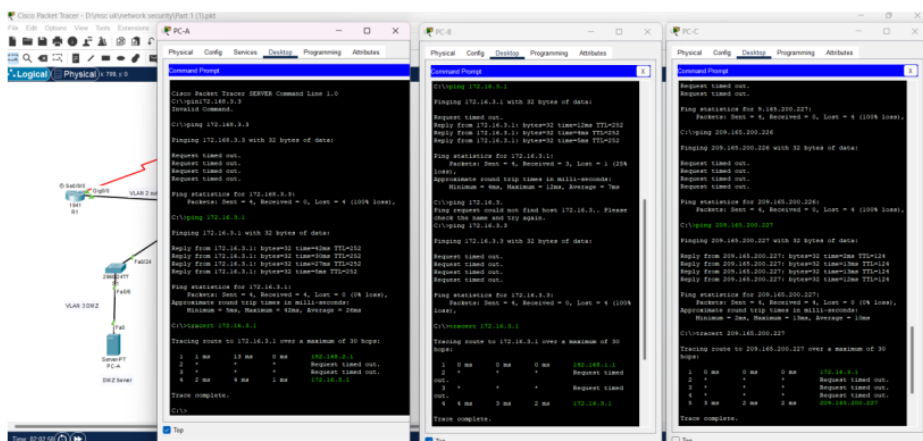


Figure 13: Verifying ping from PC-A, PC-B, PC-C with using tracert

c. The Synergy of Encryption, Hashing, and Digital Signatures for Data Security

Cryptographic techniques such as encryption, hashes, and digital signatures work in tandem to provide a robust framework for securing data through confidentiality, integrity, and authentication. Encryption involves the use of a secret key and an encryption algorithm to transform plaintext data into ciphertext that can only be decrypted with the same key. This ensures that only authorized parties can access confidential information.

In contrast, hashes employ one-way functions that convert any input into a fixed-length output, referred to as a digest or a message digest. The function is used to ascertain the integrity of data by contrasting the data's calculated hash to the expected hash. With any modification to the data, a unique hash value is created, making it possible to identify malicious tampering [39].

Digital signatures offer authentication by enabling the recipient to confirm the sender's identity and validate the message's integrity. These signatures' effectiveness relies on public-key encryption, which entails utilising the sender's private key to encrypt a message's hash. The recipient can then decrypt the hash using the sender's public key, compare, and ascertain its authenticity.

Overall, encryption, hashes, and digital signatures form the foundation of a secure data protection system. Encryption provides confidentiality, hashes ensure the data's integrity, while digital signatures provide authentication. They are fundamental tools in many applications, including secure communication, electronic transactions, and data storage [40].

d. Ensuring Data Integrity and Authentication with Cryptographic Hashes

The utilization of cryptographic hashes is a critical technique in modern cryptography to guarantee the integrity and authentication of data. Essentially, cryptographic hashes provide a digital fingerprint or checksum of a message or data, thereby ensuring that the data remains unaltered whilst in transit. This is accomplished through a hash function that takes an arbitrary-length input and generates an output of a fixed size that is unique to the input data. The resulting output, also known as a hash value or digest, represents the input data and is typically difficult to reverse-engineer or calculate in reverse.

To maintain data integrity, the original data's hash value is compared to the received data's hash value, enabling one to determine whether the data has been tampered with while in transit [41]. If the two-hash values match, it confirms the received data's authenticity, whereas non-matching hash values indicate that the data has been modified, thus compromising its integrity. In addition to ensuring data integrity, cryptographic hashes can also be employed to establish authentication. The process involves using the sender's private key to encode the hash value of the message, thus creating a digital signature. To ensure the message's authenticity, the recipient decrypts the encrypted hash value using the sender's public key and then compares it to the computed hash of the message. If the two-hash values match, it confirms that the message was indeed sent by the sender, thus verifying the source of the message and maintaining its integrity.

Looking back, cryptographic hashes are crucial in guaranteeing the genuineness and integrity of data in numerous applications, such as safeguarded communication, digital signatures, and data preservation. [42].

e. Protecting Data Confidentiality with Encryption Algorithms

Encryption algorithms are a paramount tool to safeguard data confidentiality as they convert plaintext or readable data into an unreadable format known as ciphertext. This impenetrable data becomes indecipherable to those lacking the decryption key, assuring that only authorized parties may access it. Encryption algorithms utilize complex mathematical functions and algorithms to transform data in such a way that it cannot be easily understood or read without the appropriate decryption key. The two primary encryption algorithms are symmetric key encryption, also called shared secret encryption, which employs the same key for encryption and decryption. Conversely, asymmetric key encryption (commonly recognized as public-key encryption) uses two keys - a public and a private key - for encryption and decryption, respectively. The public key distributes freely, while to keep the data safe, the private key must remain confidential. Encryption algorithms serve a wide variety of applications, including secure communication, data storage, and secure file transfer. They are indispensable in maintaining data confidentiality and blocking unauthorized access from sensitive information [43] [44] [45].

f. Enhancing Data Security with Public Key Infrastructure for Confidentiality and Authentication

Public Key Infrastructure comprises a suite of advanced technologies, protocols, and services that are employed to establish and manage digital certificates and public-private key pairs for secure communication purposes. By leveraging a trusted third party called a Certificate Authority, PKI facilitates data confidentiality and authentication. Specifically, digital certificates containing the recipient's public key are issued by the CA, which are then utilized to encrypt data. This encryption process enables only the intended recipient to decrypt the

message using their corresponding private key, thereby ensuring data privacy. Moreover, the digital certificate provides an added layer of authentication. By verifying the identity of the recipient and the authenticity of the public key, PKI builds a strong foundation of trust in the communication channel. The ability to revoke digital certificates in the event of loss, theft, or compromise ensures that fraudulent usage is prevented, thus increasing the reliability of this security infrastructure.

PKI finds extensive application in various sectors such as secure email, virtual private networks (VPNs), and online transactions. Its robustness and utility make it a crucial mechanism for ensuring data confidentiality and authentication in modern digital communications [46] [47].

2.9 Cisco ASA Deployment for Robust Firewalling and NAT/PAT Services

a. Functionality of Cisco ASA as an Advanced Stateful Firewall

It is a sophisticated stateful firewall that offers comprehensive security services for networks.

Operating at both the network layer and transport layer, the ASA employs stateful packet inspection to analyse traffic and maintain a record of connections passing through it. This capability enables it to identify and block unauthorized traffic that may pose a risk to the network. The ASA also includes access control lists (ACLs), which permit or deny traffic based on predefined rules [48].

In addition to packet filtering and access control, the ASA boasts advanced security features, including intrusion prevention, malware detection, and virtual private network (VPN) capabilities. To ensure maximum uptime and availability, the ASA supports high availability features such as failover, clustering, and load balancing.

Suitable for a range of network environments, from small businesses to large enterprises, the ASA is a versatile security appliance. Its advanced stateful firewall capabilities, coupled with its other security features, make it a powerful and effective tool for safeguarding networks against a wide range of potential threats [49] .

3. Secure Network Infrastructure (PART 2)

3.1 Blueprint Design

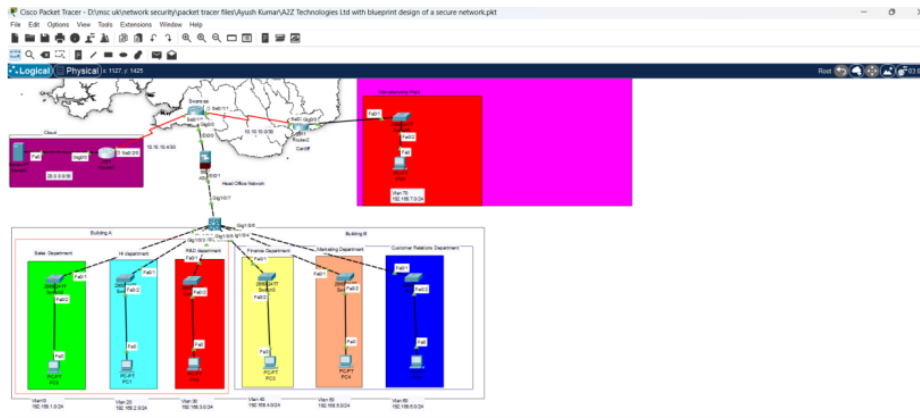


Figure 14: A2Z Technologies Ltd blueprint design with Swansea, Cardiff map

3.2 Proposal

A2Z Technologies Ltd currently faces a security threat with their network infrastructure, and thus, the company requires a more robust setup to safeguard their confidential data and resources. We suggest implementing a Hierarchical Network Design model that provides scalability, flexibility, and security.

Our proposed solution adheres to the framework of the Hierarchical Network Design model, which divides a network into three layers, stated below. Each layer operates with a specific function, facilitating easy scalability, redundancy, and security.

The **Access Layer** is responsible for connecting peripheral devices to the network. We propose creating IP networks for each department or faculty and setting up appropriate VLANs and security settings. It is necessary to configure switchport security or Port-Security on the switches to restrict unauthorized network access. In addition, host devices should be configured with strong passwords, allowing only authorized personnel access to the network.

The **Distribution Layer** should connect Access Layer Switches to Core Layer Routers. To facilitate communication between VLANs, Inter-VLAN Routing (Router on a stick) is proposed, along with DHCP server settings on the router to assign dynamic IP addresses to devices in building A.

The main purpose of the Core Layer is to establish fast connections between routers in the Distribution Layer. We suggest using either OSPF or RIPv2 as the routing protocol. RIPv2 will be used for the internal network, and static routing for external servers.

Secure Remote Access will be facilitated through configuring SSH, thus ensuring that only authenticated personnel can access the network. SSH provides exceptional network security, using encryption and authentication to prevent unauthorized network access.

In terms of cost analysis, the proposed solution would require the procurement of new networking equipment, including switches, routers, and cabling. A Network Security Engineer service is required to configure and setup the infrastructure. The estimated cost of implementing this network infrastructure is around £100,000. The procurement process should follow competitor analysis, and the best value-for-money vendor should be selected.

In order to effectively implement the recommended solution for A2Z Technologies Ltd, certain hardware and software components will be necessary. Specifically, the following network devices must be obtained:

Network Devices:

7 x Cisco Catalyst 2960 Series switches

3 x Cisco ISR 2911 routers

Cabling:

1000 ft. of Cat6 Ethernet cable

Copper Cross-over, Copper Straight-Through

Serial DCE, Serial DTE

Network Security:

1 x Cisco Adaptive Security Appliance (ASA) firewall

1 x 3650 24ps L3 switch

Network Management:

1 x Cisco Prime Infrastructure software

The total cost of these aforementioned hardware requirements will vary between £20,000 and £25,000, depending on the selected vendor and their pricing structure. Moreover, it is important to consider the additional cost of labour, specifically network engineer(s), that will be necessary for effectively configuring and deploying the network. Depending on the scope of work, the labour costs could range from £10,000 to £20,000.

It is highly recommended that A2Z Technologies Ltd gathers quotations from multiple vendors, and determines which vendor can offer the best value for the investment. We advise utilizing a Request for Quotation (RFQ) process to obtain quotations from various vendors, at which point they can be evaluated based on their pricing, warranties, and support options.

Overall, the total cost for implementing the proposed solution will likely fall between £30,000 and £45,000, dependent on the selected vendor and the specific scope of work required.

The proposed implementation of network infrastructure will span across a three-month period with a detailed project plan timeline that encompasses a range of tasks.

Project Plan Timeline:

The **first month** will involve the purchase and configuration of necessary hardware and software from chosen vendors. This will include configuring VLANs, assigning ports to appropriate VLANs for each department, configuring subnets and IP addresses, ensuring proper connectivity within the network, implementing router-on-a-stick for inter-VLAN routing, configuring DHCP server on the router, as well as switchport security to prevent unauthorized access.

During the **second month**, OSPF or RIPv2 will be set up as the routing protocol to provide dynamic routing of internal network traffic and static routing for external servers. Firewalls will also be configured to effectively restrict incoming and outgoing traffic. Anti-malware software and anti-virus will be implemented to protect the network from known threats, and

the entire network will be thoroughly tested for connectivity, security, and performance issues.

The **third month** of the project plan timeline will involve a comprehensive penetration testing to identify any vulnerabilities that may be exploited by attackers and remedial actions taken promptly. In addition, a vulnerability assessment will be conducted to ensure the network is protected against known vulnerabilities. Employee training on network security best practices will also be undertaken to reduce the risk of attacks due to potential human errors. Finally, the network will be regularly monitored and maintained to ensure optimal security and performance.

Several proactive defensive mechanisms, including VLAN separation of departments to control access to sensitive information, firewalls to regulate incoming and outgoing traffic, and the implementation of anti-virus and anti-malware software will be applied to safeguard the network. Additionally, the use of switchport security or port-security on switches will prevent unauthorized network access.

An organization's network infrastructure is vulnerable to various types of cyber-attacks, and safeguarding it is crucial. An example of a network attack is a distributed denial-of-service (DDoS) attack that inundates a network with an overwhelming amount of traffic., rendering it inaccessible to users. Another type of network attack is phishing, where hackers deceive users into revealing confidential data, such as login credentials, or financial data through fraudulent emails or websites. Another form of attack is malware, which includes viruses, worms, and Trojan horses that infect systems and can steal or destroy data. It is of utmost importance to implement proper security measures that will prevent such attacks and ensure a secure network infrastructure.

It is crucial to undertake routine assessments after the proposed secure network infrastructure has been implemented to verify the effectiveness of the security measures. **There are three types of periodic tests that are recommended:**

Firstly, vulnerability assessment is essential since it examines the network for susceptibility and flaws that a hacker could exploit. This test can be performed using automated tools or manually to recognize and prioritize potential vulnerabilities.

Secondly, penetration testing recreates a real-world scenario where a network may be attacked. The aim is to locate and exploit any flaws in the system. A certified ethical hacker can conduct the test to discover weakness in the network's security measures.

Thirdly, conducting a security audit is necessary to ensure compliance with industry standards and best practices. The audit can be done internally or by external auditors. It involves an examination of the security policies and procedures to identify areas that require improvement and ensure the continued safety of the network.

There are also three types of testing that can be carried out to evaluate the network's security, including black box testing, grey box testing, and white box testing. Each test assesses various security threats that could establish evidence of any vulnerabilities in the system.

3.3. Invoice

Invoice Date: 05/04/2023

Invoice Number: 001

To: A2Z Technologies Ltd

Address: Wales, UK

Contact Person: XYZ

Email: XYZ@a2ztech.com

Dear A2Z Technologies Ltd,

I am writing to express my gratitude for your business and your trust in my professional consultancy services. It was a pleasure to work with you on the network infrastructure implementation project, which included designing and implementing a secure communication and data protection system that meets your specifications.

The project scope entailed designing a hierarchical network infrastructure, configuring VLANs and subnetting, configuring Inter-VLAN routing and DHCP server, configuring SSH for secure remote access, configuring OSPF or RIPv2 as the routing protocol, configuring switchport security or Port-Security on the switches, conducting penetration testing and vulnerability assessments.

As an esteemed client, please find enclosed the invoice for the services provided, with a total amount of £35,000. If you have any inquiries or doubts regarding the invoice, please feel free to reach out to me. I welcome the opportunity to address any issues and reassure your satisfaction.

I am looking forward to a continued business relationship with you and to working on future projects. Thank you again for your confidence in my skills and expertise.

Best regards,

Ayush Kumar,

Network Security Engineer

4. Conclusion and Recommendation

In conclusion, the network infrastructure design proposed for A2Z Technologies Ltd encompasses multiple layers of to safeguard the confidentiality, integrity, and availability of their data, companies implement security measures. The design involves firewalls, intrusion detection systems, access control lists, encryption, and secure remote access solutions. Furthermore, the proposed cost analysis provides a comprehensive estimation of expenses for both software and hardware, as well as for professional and consultancy services.

The project plan timeline for deploying the solution(s) specifies the hardware and software types to be employed, configurations to be applied, and protective measures to be enforced. The plan also outlines three types of testing to be carried out following the implementation to guarantee the network infrastructure's impregnability. To ensure the success of the project, we recommend the following:

1. Regular employee training and awareness programs on cybersecurity to minimize the risks of security breaches caused by human errors.
2. Frequent security audits to identify vulnerabilities and loopholes in the network infrastructure.
3. Periodic penetration testing to evaluate the efficiency of security measures can be assessed to identify any potential vulnerabilities. gaps or weaknesses.

Overall, the proposed network infrastructure design will provide A2Z Technologies Ltd with a secure and reliable network that meets their business needs. The amalgamation of multiple security measures and defensive mechanisms will prevent security breaches and protect the organization's valuable assets.

5. References

- [1] R. Hou, G. Ren, C. Zhou, H. Yue, H. Liu and J. Liu, "Analysis and research on network security and privacy security in ubiquitous electricity Internet of Things," *Computer communications*, vol. 158, pp. 64-72, 2020.
- [2] Y. Liu, L. Xu and J. Lin, "Remolding and Thinking of Network Security System in Intelligent Hospital," in *8th Annual International Conference on Network and Information Systems for Computers (ICNISC)*, Hangzhou, China, 2022.
- [3] A. K. Tyagi., *Handbook of research on technical, privacy, and security challenges in a modern world*, Information Science Reference, 2022.
- [4] S. Geetha and A. V. Phamila, *Countering Cyber Attacks and Preserving the Integrity and Availability of Critical Systems*, Hershey: IGI Global, 2019.
- [5] F. W. M. L. M. Skopik, "Detecting Unknown Cyber Security Attacks Through System Behavior Analysis," in *Cybersecurity of Digital Service Chains*, vol. 13300, Springer, Cham, 2022.
- [6] B. B. Gupta, *Advances in Malware and Data-Driven Network Security*, Kurukshetra, India: IGI GLobal, 2022, p. 304.
- [7] Y. Xie, M. Siponen, G. Moody and X. Zheng, "Discovering the interplay between defensive avoidance and continued use intention of anti-malware software among experienced home users: A moderated mediation model," *Information & management*, vol. 59, pp. 103586-, 2022.

- [8] A. Krkoleva Mateska, P. Krstevski and Borozan, "Overview and Improvement of Procedures and Practices of Electricity Transmission System Operators in South East Europe to Mitigate Cybersecurity Threats," vol. 9, pp. 39-, 2021.
- [9] K. J. E. H. M. Nisar, "A survey on the architecture, application, and security of software defined networking: Challenges and open issues," *Internet of Things*, vol. 12, p. 100289, 2020.
- [10] A. H. A. M. a. V. J. Sukumar, "Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors.," *Risk Analysis*, 2023.
- [11] F. L. B. S. MF Franco, "'SECProject: a Framework for the Management of Cybersecurity Projects in Small and Medium-sized Enterprises," 2022.
- [12] R. Sahay, W. Meng and Jensen, "The application of Software Defined Networking on securing computer networks: A survey," *Journal of network and computer applications*, vol. 131, pp. 89-108, 2019.
- [13] S. S. K. S. a. M. A. A. Mishra, "Multilayer self-defense system to protect enterprise cloud.," *Comput. Mater. Contin.*, pp. 71-85, 2021.
- [14] W. G. L. Shaorong, "Research on campus network security protection system framework based on cloud data and intrusion detection algorithm," *Soft computing*, vol. 27, no. 10, pp. 6835-6844, 2023.
- [15] A. Cartagena, G. Rimmer, T. v. Dalsen, L. Watkins and W. H. Robinson, "Privacy Violating Opensource Intelligence Threat Evaluation Framework: A Security

Assessment Framework For Critical Infrastructure Owners,” in *10th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2020.

- [16] V. A. a. S. S. Karam AbuAlnaaj, “A strategic framework for smart campus. In Proceedings of the International Conference on Industrial Engineering and Operations Management,” 2020.
- [17] A. Chidukwani, S. Zander and P. Koutsakis, ““A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations,” *n IEEE Access*, pp. 85701-85719, 2022.
- [18] G. S. R. A. Tan MK, “Understanding negotiated anti-malware interruption effects on user decision quality in endpoint security,” *Behaviour & Information Technology*, pp. 903-932, 4 Jul 2021.
- [19] E. a. M. A. Ozkaya, *Hands-On Cybersecurity for Finance: Identify vulnerabilities and secure your financial services from security breaches*, Packt Publishing Ltd., 2019.
- [20] J. E. Setiawan, “Wireless Network Security Information System on Banking Company with Radius Server Using Authentication, Authorization, Accounting (AAA),” *International Journal of Computer Science and Software Engineering*, vol. 7, no. 11, pp. 55-259, 2018.
- [21] A. Braeken and A. Touhafi, “AAA - autonomous anonymous user authentication and its application in V2G,” *Applied Mechanics and Materials*, vol. 30, no. 12, Concurrency and computation.

- [22] L. H. W. X. L. A. I. A. M. a. Y. X. Li, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *International Journal of Information Management*., pp. 13-24, 2019.
- [23] G. S. H Aldawood, "Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues," *Future Internet*, p. 73, 2019.
- [24] L. Reznik., *Intelligent security systems : how artificial intelligence, machine learning and data science work for and against computer security*, Hoboken, New Jersey: Wiley, 2022.
- [25] E. A. Altulaihan, A. Alismail and M. Frikha, "A Survey on Web Application Penetration Testing,," *Electronics (Basel)*, vol. 12, no. 5, pp. 1229-, 2023.
- [26] M. C. Ghanem and T. M. Chen, "Reinforcement Learning for Efficient Network Penetration Testing," *Information (Basel)*, vol. 11, no. 1, pp. 6-, 2020.
- [27] S. Hijazi and M. S. Obaidat, "Address resolution protocol spoofing attacks and security approaches: A survey," *Security and privacy*., vol. 2, no. 1, pp. e49-, 2019.
- [28] Z. e. a. Liu, "Jaquen: A High-Performance Switch-Native Approach for Detecting and Mitigating Volumetric DDoS Attacks with Programmable Switches.,," *In USENIX Security Symposium*, pp. 3829-3846, August 2021.
- [29] M. Y. Y. E. Y. GUVEN, "A Survey on Backbone Attack,," in *7th International Symposium on Digital Forensics and Security (ISDFS)*, 2019.

- [30] A. a. J. T. Mileva, "Hiding Data in a Switched Network.," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, vol. 13, no. 3, pp. 37-49, 2022.
- [31] C. Cai, S. Mei and W. Zhong, "Configuration of intrusion prevention systems based on a legal user: the case for using intrusion prevention systems instead of intrusion detection systems," *Information technology and management*, vol. 20, no. 2, pp. 55-71, 2019.
- [32] M. Patel, "A Comparative Study Between Intrusion Detection System And Intrusion Prevention System," vol. 12, pp. 10-18, 2022.
- [33] M. Al-Asli and T. A. Ghaleb, "Review of Signature-based Techniques in Antivirus Products," in *2019 International Conference on Computer and Information Sciences (ICCIS)*, Sakaka, Saudi Arabia, 2019.
- [34] O. N. A. H. I. a. L. S. Savenko, "Dynamic Signature-based Malware Detection Technique Based on API Call Tracing," *In ICTERI Workshops* , pp. 633-643, 2019.
- [35] A. F. Gentile, P. Fazio and G. Miceli, "A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios," *Telecom (Basel)*, no. 4, pp. 430-445, 2021.
- [36] A. K. K Kaur, "A Survey of Working on Virtual Private Network," 2019.
- [37] H. Gunleifsen, T. Kemmerich and V. Gkioulos, ""Dynamic setup of IPsec VPNs in service function chaining," *Computer networks*, vol. 160, pp. 77-91, 2019.

- [38] F. Hauser, M. Haberle, M. Schmidt and M. Menth, "P4-IPsec: Site-to-Site and Host-to-Site VPN With IPsec in P4-Based SDN," *IEEE access*, vol. 8, pp. 139567-139586, 2020.
- [39] N. J. J. T. S. a. V. S. Gayathri, "DATA ENCRYPTION USING DIGITAL SIGNATURE IN BLOCKCHAIN TRANSACTIONS," in *In CONFERENCE SECRETARIAT*, 2021.
- [40] M. R. a. A. M. Alagheband, "Advanced digital signatures for preserving privacy and trust management in hierarchical heterogeneous IoT: taxonomy, capabilities, and objectives," *Internet of Things*, vol. 18, mMay 2022.
- [41] M. K. A. H. M. R. L. K. R. a. T. T. Islam, "Data security system for a bank based on two different asymmetric algorithm cryptography," in *In International Conference on Evolutionary Computing and Mobile Sustainable Networks*, 2020.
- [42] S. M. A. T. I. G. A. K. S. a. B. S. P. Agarwal, "Authenticating Cryptography over Network in Data,," in *International Conference on Intelligent Computing and Control Systems (ICCS)*, Madurai, India, 2019.
- [43] H. T. a. H. T. H. ALRikabi, "Enhanced data security of communication system using combined encryption and steganography," *International Journal of Interactive Mobile Technologies*, vol. 5, no. 16, p. 145, 2021.
- [44] J. Li, Z. Zhang, S. Li, R. Benton, Y. Huang, M. V. Kasukurthi, D. Li, J. Lin, G. M. Borchert, S. Tan, G. Li, B. Ma, M. Yang and J. Huang, "A partial encryption algorithm for medical images based on quick response code and reversible data hiding

technology,,” *BMC medical informatics and decision making*, vol. 20, pp. 297-297, 2020.

- [45] U. D. G. a. M. M. H. C. Biswas, “An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography,” in *International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Cox'sBazar, Bangladesh, 2019.
- [46] C. Techapanupreed and W. Kurutach, “Enhancing Transaction Security for Handling Accountability in Electronic Health Records,” *Security and communication networks*, pp. 1-18, 2020.
- [47] B. a. A. N. Ying, “Lightweight remote user authentication protocol for multi-server 5G networks using self-certified public key cryptography,” *Journal of network and computer applications*, pp. 66-74, 2019.
- [48] M. S. S. H. a. N. V. Y. Faizan, “Faizan, Mohammed, Sujay S. Hegde, and Nagaratna V. Yaligar.,” *IOSR Journal of Computer Engineering (IOSR-JCE)* , pp. 34-36, 2019.
- [49] H. a. R. L. Karrar, “CREATING AN INTEGRATED WIRELESS NETWORK AND ENCRYPT INFORMATION,” p. 80, 2020.

Construct and mitigating security vulnerabilities and weaknesses

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

77 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

PAGE 32

PAGE 33

PAGE 34

PAGE 35

PAGE 36

PAGE 37

PAGE 38

PAGE 39

PAGE 40

PAGE 41

PAGE 42

PAGE 43

PAGE 44

PAGE 45

GRADING FORM: L7 NS (ACCA7019)

AYUSH KUMAR

77

ENGAGEMENT WITH LITERATURE SKI

Your work must focus on variety of scanning and defence technologies available for you to choose for the given scenario. Your work must include articles published by peer reviewed journals, conference proceedings, books, and related website (e.g. IEEE, ACM, Science direct). Information from website such as ehow, wiki, forums, etc. will not be accepted. (10 marks)



You have research on security threats facing modern network infrastructures and other areas to aid solutions to part 1. Appropriate referencing done.

8

KNOWLEDGE AND UNDERSTANDING SK

Your work must demonstrate understanding of concepts and underlying principles. You should explain and analysis the chosen area in a meaningful way. (10 marks)



You have demonstrated understanding of the research.

8

COGNITIVE AND INTELLECTUAL SKI

Your work must demonstrate critical analysis and evaluation of the proposal. Your work must also justify your research findings and provide evidences. This will be assessed by the quality of your explanations, discussions, conclusions and recommendation, from part 1 and part 2: • The proposed choices and security measures. • The implementing the solution(s) cost. . • The three month project plan timeline for the implementation. • Three attacks that plagues organisations network infrastructure. • Three types of test to be conducted after the implementation. • Monitoring tools if considered. • Invoice for the professional/consultancy service. (25 marks)



Your abstract should be the last to be written to outline the key findings.

Your introductions need improvement. Your introduction should give a background to the work along with some general research information of the subject areas, followed by what the rest of the report will include. You have not done a conclusion.

You have Use the knowledge gain from part 1 to propose and implementation solution for A2Z:

- You have wrote the proposal explaining your choices but lacking critical analytic discussion.
- You have not done a proposed cost analysis for implementing the solution(s)
- You have not done the timeline for the implementation
- You have explained to A2Z at least three attacks that will plagues the organisations network infrastructure.
- You have explained three types of test to be conducted after the implementation to ensure the network infrastructure is secure.
- You have provided a sort of invoice.

18

PRACTICAL SKILLS

You will use Cisco Packet Tracer for part 1 or any equivalent tools to conduct the blueprint design for part 2. This will be assessed by:

- *Working Cisco packet tracer file and clearly state or indicate the devices the configuration files belong to.*
- *Clearly labelled blueprint design showing departments, manufacturing plant, types of connection internal, external, remotely etc.*
- *Application used and protocols involved*
- *Restricted access to the necessary site(s) (50 marks)*



You have submitted a Cisco Packet Tracer file along with the configurations embed in your report.

40

The knowledge and understanding gain from part 1 packet tracer implementation was used to:

- Implement a working Cisco packet tracer design (instead a constructed and label the blueprint design) for the given case study explanation. You could consider redundancy in your design.

TRANSFERABLE SKILLS FOR LIFE A

You must submit a report which should be approximately 6,000 words in length (remember diagrams/pictures worth a thousand words; these can be used to enhance your report). The report should be presented in an academic way and therefore must include an abstract, an introduction, a conclusion and a list of references. The report must be submitted via Turnitin and practical implementation along with configuration files must be uploaded to the Moodle link that will be provided. (5 marks)



Your report could do with some formatting alignment. Do not use first person tense in academic report example "me, I, etc"

3