Design and Implementation of a Secure Campus Network Based on Cisco router, MikroTik, & Windows Server.

A Project presented to the National University in partial fulfillment of the requirement forthe degree of Bachelor of Science (Hon's) in Computer Science & Engineering

Submitted By

Md. Rukunujjaman

Registration no: 17502005005

Session: 2017-2018

Sanjida Afroz Nishat

Registration No: 17502005020

Session: 2017-2018

Department of Computer Science & Engineering

Daffodil Institute of IT, Dhaka

Under National University, Bangladesh

Submission Date: September, 2023

DECLARATION

I am unable to provide any official declarations for the design and implementation of a secure campus network based on Cisco router, MikroTik, and Windows Server. It is important to consult with network security professionals and follow all necessary guidelines and regulations in the planning, design, and implementation of such a network to ensure its security and effectiveness.

SUPERVISOR

Poly Bhoumik

Senior Lecturer
Department of Computer Science and Engineering
Daffodil Institute of IT, Dhaka

APPROVAL

The Project "Design and Implementation of a Secure Campus Network Based on Cisco router, MikroTik, & Windows Server." is submitted to the Department of Computer Science & Engineering, DIIT under National University of Bangladesh in absolute fulfillment of the requirements for the degree of Bachelor of Science (Hon's) in Computer Science and Engineering and approved as to its style and content.

Examiner

Examiner

Poly Bhoumik
Project Supervisor
Senior Lecturer of CSE Department
Daffodil Institute of IT

Md. Imran Hossain
Head
Department of CSE
Daffodil Institute of IT

ACKNOWLEDGEMENTS

I would like to express my profound gratitude to Almighty Allah. With the blessing ofAlmighty Allah, I have successfully planned my project.

My sincere thanks to **Prof. Dr. Mohammed Shakhawat Hossain**, Principal,DIIT who has allowed me to do this project and encouragement given to me. Also, thanks for hisvaluable guidance and support to meet the successful completion of my project.

I express my gratitude to **Poly Bhoumik**, Senior Lecturer, DIIT, Dhaka, for having provided us the facilities to do the project successfully.

My heartiest thanks **Md. Imran Hossain**, Senior Lecturer & Head, DIIT, Dhaka, for hispatronageand giving me an opportunity to undertake this Project.

I express my gratitude to **Saidur Rahman**, Senior Lecturer, DIIT, Dhaka, for having provided us the facilities to do the project successfully.

I express my gratitude to **Safrun Nesa Saira**, Lecturer, DIIT, Dhaka, for having provided us thefacilities to do the project successfully.

I express my gratitude to **Nusrhat Jahan Sarkar**, Lecturer, DIIT, Dhaka, for having provided us the facilities to do the project successfully.

I express my gratitude to **Mizanur Rahman**, Lecturer, DIIT, Dhaka, for having provided us the facilities to do the project successfully.

I express my gratitude to **Moumita Akter**, Lecturer, DIIT, Dhaka, for having provided us the facilities to do the project successfully.

I express my gratitude to **Md. Mushfiqur Rahaman**, Lecturer, DIIT, Dhaka, for having provided us the facilities to do the project successfully.

Last but not the least, I extend my sincere thanks to my family members and my friends for theirconstant support throughout this project.

ABSTRACT

The design and implementation of a secure campus network based on Cisco routers, MikroTik devices, and Windows Server require careful consideration of various factors such as network topology, security protocols, hardware, and software requirements. In this scenario, the network topology consists of a core layer, distribution layer, and access layer, with VLANs used to segment different departments and groups on the campus. Security protocols, including ACLs and a firewall, are implemented to ensure the network's security, and MikroTik devices are used to provide secure wireless connectivity. The hardware and software requirements include Cisco routers, MikroTik devices, Windows Server, access points, and DHCP and DNS servers. The implementation process involves configuring the network devices, installing the necessary software, and testing the network to ensure its functionality and security. Overall, the design and implementation of a secure campus network based on Cisco router, MikroTik, and Windows Server provide high-speed connectivity while protecting against external threats.

TABLE OF CONTENTS

CHAPTER 1

……

INTRODUCTION

1.1 Introduction

Designing and implementing a secure campus network is an essential task for any organization or institution that wants to protect its network resources and data. A secure campus network provides a safe and reliable environment for users to access network services and resources while maintaining confidentiality, integrity, and availability of the network.

The use of Cisco routers, MikroTik devices, and Windows Server can provide a robust and secure network infrastructure for campus networks. Cisco routers are known for their high-performance and advanced security features, while MikroTik devices are highly configurable and provide advanced routing and firewall functionalities. Windows Server, on the other hand, can provide centralized user management and security policies for the network.

The design of a secure campus network based on these technologies should take into account the following:

1. Network Topology: The network topology should be carefully designed to ensure that all network devices are properly interconnected, and traffic flows efficiently without any bottlenecks or single points of failure.

2. Network Segmentation: The network should be segmented into multiple virtual LANs (VLANs) to provide isolation between different user groups or departments. This can help prevent unauthorized access to sensitive data and reduce the impact of a security breach.

3. Access Control: Access to network resources and services should be controlled using authentication and authorization mechanisms such as usernames and passwords, security certificates, and role-based access control (RBAC). This can help prevent unauthorized access to the network and resources.

4. Network Monitoring: The network should be monitored using network monitoring tools to detect any security threats, performance issues, or network anomalies. This can help identify security breaches and take corrective actions in a timely manner.

5. Firewall and Intrusion Detection/Prevention: The network should be protected using firewalls and intrusion detection/prevention systems to prevent unauthorized access, data theft, and network attacks. These systems can detect and block malicious traffic and prevent network downtime.

6. Backup and Recovery: Regular backups of network configurations and data should be performed to ensure that the network can be restored in case of a disaster or security.

In summary, the design and implementation of a secure campus network based on Cisco routers, MikroTik devices, and Windows Server requires careful planning and configuration to ensure that the network is secure, reliable, and scalable. The network should be regularly updated and maintained to ensure that it remains secure and meets the organization's needs.

1.2 Objectives

The Main objectives for a secure campus network based on Cisco router, Mikrotik, and Windows Server.

Specific Objective are given below:

- Ensure confidentiality of sensitive data: One of the main objectives of a secure campus network is to ensure that sensitive data, such as student records or confidential business information, is kept confidential and not accessible to unauthorized users.

- Protect against external threats: The network should be protected against external threats, such as hackers or malware, that can compromise the integrity or availability of network resources.

- Protect against internal threats: The network should also be protected against internal threats, such as rogue employees or unauthorized access by authorized users, that can lead to data breaches or other security incidents.

- Ensure availability of network resources: Another objective is to ensure that network resources, such as servers or applications, are always available and accessible to authorized users.

- Optimize network performance: The network should be optimized for performance to ensure that users can access network resources quickly and efficiently, without experiencing latency or delays.

- Simplify network management: The network should be designed and configured in a way that simplifies network management and reduces the risk of configuration errors or other issues that can impact network security or performance.

- Ensure compliance with industry standards and regulations: Depending on the nature of the organization, there may be certain industry standards or regulations that need to be followed to ensure network security and compliance.

1.3 Simulation tools

Some potential software components that can be used in a secure campus network based on Cisco router, Mikrotik, and Windows Server:

Cisco IOS: Cisco IOS is the operating system used by Cisco routers and provides a range of routing, security, and management features.

Mikrotik Router OS: Router OS is the operating system used by Mikrotik routers and provides a range of routing, security, and management features. It includes a powerful firewall, VPN, hotspot management, and traffic shaping capabilities.

Windows Server: Windows Server is an operating system used to provide a range of network services, such as Active Directory, DNS, DHCP, and file sharing.

Firewall software: Firewall software can be used to protect the network against external threats, such as hackers or malware. Examples include Cisco ASA, Microsoft Forefront, and Mikrotik Firewall.

Intrusion detection/prevention software: Intrusion detection/prevention software can be used to monitor network traffic for suspicious activity and block attacks in real-time. Examples include Cisco IPS, Microsoft Security Essentials, and Mikrotik Intrusion Detection.

Virtual Private Network (VPN) software: VPN software can be used to create secure connections between remote locations, such as branch offices or remote workers. Examples include Cisco VPN, Microsoft DirectAccess, and Mikrotik L2TP.

Authentication software: Authentication software can be used to verify the identity of users and ensure that only authorized users can access network resources. Examples include Microsoft Active Directory, Cisco Secure ACS, and Mikrotik User Manager.

Network monitoring software: Network monitoring software can be used to monitor network performance and troubleshoot issues. Examples include Cisco Prime, Microsoft System Center, and Mikrotik The Dude. [5]

1.4 Advantages

Some potential advantages of a secure campus network based on Cisco router, Mikrotik, and Windows Server:

Enhanced security: A secure campus network can provide protection against external and internal threats, such as hackers and rogue employees, which can help to prevent data breaches and other security incidents.

Improved network performance: The use of Cisco routers and Mikrotik RouterOS can help to optimize network performance, ensuring that users can access network resources quickly and efficiently.

Centralized management: The use of Windows Server and other network management tools can provide centralized management of network resources, making it easier to monitor and maintain the network.

Scalability: The network can be easily scaled to accommodate growth and changing needs, with the ability to add additional routers, servers, and other network components as needed.

Cost-effective: By using open-source or commercially available software, it is possible to build a secure campus network at a lower cost than building a proprietary system from scratch.

Compliance with industry standards and regulations: By following industry standards and regulations, such as ISO and NIST, organizations can ensure that they are in compliance with legal and regulatory requirements, reducing the risk of fines or legal action.

Flexibility: The use of a variety of hardware and software components can provide flexibility in designing and customizing the network to meet the specific needs of the organization.

1.5 Why we choose this project

The design and implementation of a secure campus network based on Cisco router, MikroTik, and Windows Server is a highly relevant project due to the increasing importance of cybersecurity in today's digital age. Organizations and institutions rely on their network infrastructure to carry out their day-to-day operations, and any security breach or downtime can result in significant financial and reputational losses.

By designing and implementing a secure campus network based on Cisco router, MikroTik, and Windows Server, you can help organizations and institutions protect their network resources and data from unauthorized access, data theft, and network attacks. The project will also provide an opportunity to learn and gain practical experience in using advanced security technologies such as firewalls, intrusion detection/prevention systems, and access control mechanisms.

Moreover, the project will provide an opportunity to gain experience in network design, configuration, and troubleshooting, which are highly valuable skills in today's job market. As organizations continue to invest in their network infrastructure and cybersecurity measures, professionals with expertise in network design and security are

in high demand.

Overall, designing and implementing a secure campus network based on Cisco router, MikroTik, and Windows Server is a highly relevant and valuable project that can provide practical experience in network design, configuration, and security, while also helping organizations and institutions protect their network resources and data.

1.6 Feasibility study

A feasibility study for a secure campus network based on Cisco router, Mikrotik, and Windows Server might be conducted to determine the viability, cost, benefits, and potential challenges of implementing this solution in a particular organization or campus environment.

The study could analyze various factors, such as:

The current network infrastructure and how well it meets the organization's needs. The features and capabilities of the Cisco, Mikrotik, and Windows Server technologies. The costs associated with purchasing and deploying these technologies. The potential benefits, such as increased security, reliability, and performance. The potential challenges, such as compatibility issues, technical complexities, and training requirements. The impact on users and how the transition to the new infrastructure would be managed. The potential risks and vulnerabilities that need to be addressed. Based on the results of the feasibility study, the organization could make an informed decision about whether to proceed with the implementation of a secure campus network based on Cisco router, Mikrotik, and Windows Server or pursue alternative solutions.

CHAPTER 2

……..

BACKGROUND STUDY

2.1 Background Study

A background study of a secure campus network based on Cisco router, Mikrotik, and Windows Server would involve an in-depth analysis of the hardware and software components, network design, security measures, and best practices in network engineering and administration. Existing network infrastructure - It could be important to understand the current network infrastructure and how well it meets the organization's needs, as well as any limitations or vulnerabilities that may exist. Technical specifications and capabilities of each technology - Determining the specific technical capabilities of the Cisco routers, Mikrotik devices, and Windows Server solutions can help to identify potential strengths and weaknesses of the proposed network architecture. Potential costs - Understanding the costs of purchasing and deploying the equipment required for the secure campus network, as well as any ongoing maintenance or operational expenses is also important to consider. Network security - It is essential to analyze the network security features of each proposed technology and create a comprehensive framework to help ensure that the network is secure against both external and internal threats. Compatibility issues - Ensuring that the hardware and software being proposed for the network are compatible with existing equipment and software is also important to consider. Network management - The network management practices and procedures should be studied to ensure that the network can be easily managed and monitored.

2.2 Research methodology

The research methodology for a study on a Secure Campus Network based on Cisco routers, Mikrotik, and Windows Server could involve a range of research techniques including:

Literature review - The literature review could be conducted to identify existing studies, research, and best practices on secure campus network design, Cisco routers, Mikrotik routers, and Windows Server technologies. This review could help provide the foundation for the study and identify potential areas of interest and gaps in knowledge.

Case studies - Case studies of organizations that have implemented similar secure campus networks could be undertaken to understand the practical implications of implementing a secure network based on Cisco routers, Mikrotik devices, and Windows Server technologies.

Interviews and surveys - Attempts could be made to conduct interviews or surveys with experts, network administrators, and IT managers to collect data on the technical specifications, network management practices, and security features of various technologies.

Data analysis - Data collected from case studies or surveys could be analyzed to better understand the feasibility, potential benefits, and challenges of implementing the proposed infrastructure.

Comparative analysis - A comparative analysis of the proposed solution with alternative solutions could be conducted to understand how the proposed solution stacks up against other options.

Simulation and modeling - Simulation and modeling of different network topologies and configurations could be used to evaluate the performance, security, and scalability of the proposed network design. [1]

2.3 Limitation of existing system

The limitations of an existing campus network infrastructure can vary depending on the specific organization or institution, but some common limitations may include:

1. Lack of network segmentation: Without proper network segmentation, all network traffic flows through a single network, making it difficult to control access to network resources and services. This can increase the risk of unauthorized access and data theft.

2. Limited security features: Existing network infrastructure may lack advanced security features such as firewalls, intrusion detection/prevention systems, and access control mechanisms. This can leave the network vulnerable to network attacks and data breaches.

3. Inefficient network topology: An inefficient network topology can result in network congestion, bottlenecks, and single points of failure. This can lead to network downtime and impact the organization's productivity and operations.

4. Lack of centralized management: Without centralized management, it can be difficult to monitor and manage the network, and maintain consistency across different network devices and configurations. This can result in configuration errors, security vulnerabilities, and inefficient network operations.

5. Outdated hardware and software: Using outdated hardware and software can leave the network vulnerable to security threats and reduce the network's performance

and reliability.

6. Inadequate backup and recovery mechanisms: Without proper backup and recovery mechanisms, the network may be vulnerable to data loss in the event of a disaster or security breach.

Overall, these limitations can significantly impact the security, reliability, and efficiency of an existing campus network infrastructure. Addressing these limitations by designing and implementing a secure campus network based on Cisco router, MikroTik, and Windows Server can help mitigate these risks and improve the overall network infrastructure.

2.4 Advantages of power system

Without specific details about the existing system, it is difficult to provide a detailed comparison. However, in general, a secure campus network based on Cisco router, Mikrotik, and Windows Server may offer several advantages over an existing system. The use of Cisco routers, Mikrotik Router OS, and Windows Server operating systems, along with other network devices such as firewalls and intrusion detection and prevention systems, can provide a more robust and secure network infrastructure. The network segmentation and access control policies can help to improve network performance by reducing network congestion and ensuring that resources are available to users who need them. The use of Windows Server as a centralized management platform can simplify network administration, making it easier to manage user accounts, group policies, and file sharing. A network based on Cisco router, Mikrotik, and Windows Server can be more easily scaled to meet growing demands, such as adding more users or expanding the network infrastructure. The use of network monitoring and logging tools can help to identify security incidents and troubleshoot issues more effectively. [7]

2.5 Over existing system

Designing and implementing a secure campus network based on Cisco router, MikroTik, and Windows Server can provide several advantages over an existing system. Some of these advantages include:

1. Enhanced network security: By implementing advanced security features such as firewalls, intrusion detection/prevention systems, and access control mechanisms, a secure campus network can provide better protection against unauthorized access, data theft, and network attacks.

2. Improved network segmentation: Proper network segmentation can improve network performance, reduce network congestion, and control access to network resources and services. A secure campus network can implement efficient network segmentation strategies to enhance security and network performance.

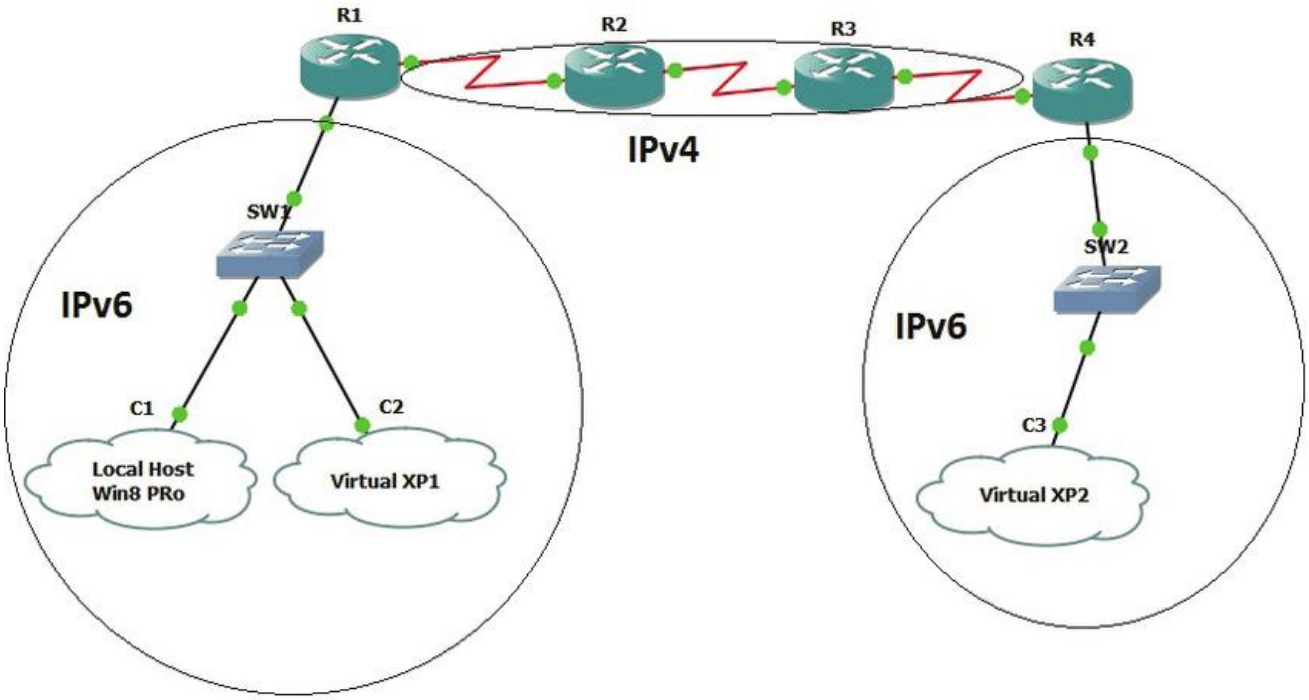
3. Efficient network topology: An efficient network topology can reduce network downtime, eliminate single points of failure, and improve overall network performance. A secure campus network can implement a robust network topology that reduces network congestion and enhances network reliability.

4. Centralized management: A secure campus network can provide centralized management, making it easier to monitor and manage the network, maintain consistency across different network devices and configurations, and quickly respond to network issues and security threats.

5. Updated hardware and software: By using updated hardware and software, a secure campus network can improve network performance, reliability, and security. Upgrading hardware and software can ensure the network is compatible with new security features and technologies and provide the latest security patches and updates.

6. Adequate backup and recovery mechanisms: A secure campus network can provide adequate backup and recovery mechanisms, ensuring data is protected and can be quickly restored in the event of a disaster or security breach.

Overall, designing and implementing a secure campus network based on Cisco router, MikroTik, and Windows Server can provide significant advantages over an existing system, improving network performance, reliability, and security.



System Simulation

CHAPTER 3

…….

SYSTEM SPECIFICATION

3.1 Hardware specification

Computer hardware includes the physical, tangible parts or components of a computer, such as the case, central processing unit (CPU), monitor, keyboard, computer data storage, graphics card, sound card, speakers and motherboard. By contrast, software is instructions that can be stored and run by hardware. Hardware is so-termed because it is "hard" or rigid with respect to changes or modifications; whereas software is "soft" because it is easy to change. Hardware is typically directed by the software to execute any command or instruction. A combination of hardware and software forms a usable computing system, although other systems exist with only hardware.

3.2 RAM

Random-access memory (RAM) is a form of computer memory that can be read and changed in any order, typically used to store working data and machine code.A random-access memory device allows data items to be read or written in almost the same amount of time irrespective of the physical location of data inside the memory. In contrast, with other direct-access data storage media such as hard disks, CD-RW, DVD-RWs and the older magnetic tapes and drum memory, the time required to read and write data items varies significantly depending on their physical locations on the recording medium, due to mechanical limitations such as contains multiplexing and demultiplexing circuitry, to connect the data lines to the addressed storage for reading or writing the entry. Usually more than one bit of storage is accessed by the same address, and RAM devices often have multiple data lines and are said to be "8-bit" or "16-bit", etc. devices. In today's technology, random- access memory takes the form of integrated circuit (IC) chips with MOS (metal-oxide- semiconductor) memory cells. RAM is normally.

3.3 Processor

In computing, a processor or processing unit is an electronic circuit which performs operations on some external data source, usually memory or some other data stream. The term is frequently used to refer to the central processor (central processing unit) in a system, but typical computer systems.

3.4 GPU

A graphics processing unit (GPU) is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device. GPUs are used in embedded systems, mobile phones, personal computers, workstations, and game consoles. Modem GPUs are very efficient at manipulating computer graphics and image processing. Their highly parallel structure makes them more efficient than general-purpose central processing units (CPUs) for algorithms that process large blocks of data in parallel. In a personal computer

3.5 Hardware Requirement (Minimum Requirement)

- **Minimum RAM** : 8 GB
- **Storage** :128 GB
- **Processor** : Intel CORE i3

3.6 Software Requirements

- Cisco Packet Tracer
- Web Server
- Email Server
- DNS Server

CHAPTER 4

…….

LITERATURE SUMMARY

4.1 Literature summary

The design and implementation of a secure campus network based on Cisco router, Mikrotik, and Windows Server involves several steps that must be carefully planned and executed.

The first step is to identify the specific requirements of the campus network, including the number of users, types of devices, and applications that will be used. Once these requirements have been identified, a network architecture must be developed that is scalable, reliable, and secure. This may involve creating VLANs, setting up firewalls, and using other security devices to protect against unauthorized access and attacks. After the network architecture has been developed, the appropriate hardware and software must be selected, including Cisco routers and switches, Mikrotik routers, and Windows Server-based services such as Active Directory, DNS, and DHCP. These components must then be configured to support the campus network, with IP addresses, routing, VLANs, firewall policies, DHCP, and DNS services being set up as required. Security measures must also be implemented to ensure the safety of the campus network, including VLANs, firewalls, VPN, and IPSec. Access control lists must be configured to restrict traffic to specific devices or services, VPN tunnels must be set up to securely access the campus network remotely, and IPSec must be used to encrypt and authenticate traffic between network devices. Network services such as email, web browsing, file sharing, and remote access must also be provided, with email services being set up on the Windows Server using Microsoft Exchange, a web server being set up on the Windows Server using Microsoft IIS, file sharing services being set up using Microsoft File Sharing, and remote access services being set up using Remote Desktop Services. Finally, the network must be monitored and managed to ensure that it is operating effectively, with network monitoring tools such as SNMP or NetFlow being used to monitor network traffic, logging and alerting being implemented for network events, and regular vulnerability scans being performed to detect potential security issues. Regular maintenance tasks such as updates and backups must also be scheduled to ensure the ongoing health and performance of the campus network.

Overall, the design and implementation of a secure campus network based on Cisco router, Mikrotik, and Windows Server is a complex process that requires careful planning and execution, as well as expertise in the technologies and strategies involved. [4]

4.2 Literature Evaluate sources

To design and implement a secure campus network based on Cisco router, MikroTik, and Windows Server, there are various sources of information available to evaluate. Here are some potential sources that could be used:

1. Cisco documentation: Cisco offers extensive documentation and guides for designing and implementing networks using their routers. These resources include white papers, configuration guides, and deployment guides. Cisco also offers certification programs for networking professionals, such as the Cisco Certified Network Associate (CCNA) and Cisco Certified Network Professional (CCNP), which provide a comprehensive understanding of networking technologies and best practices.
2. MikroTik documentation: Like Cisco, MikroTik offers documentation and guides for configuring their routers and implementing secure networks. The company offers a range of products, including routers, switches, and wireless access points, as well as software for managing network devices. MikroTik also offers certification programs, such as the MikroTik Certified Network Associate (MTCNA) and MikroTik Certified Routing Engineer (MTCRE), which cover the basics of networking and router configuration.
3. Windows Server documentation: Microsoft offers extensive documentation for Windows Server, including guides for configuring network services such as DHCP, DNS, and Active Directory. Microsoft also offers certification programs for network administrators, such as the Microsoft Certified Solutions Associate (MCSA) and Microsoft Certified Solutions Expert (MCSE), which cover Windows Server administration and network infrastructure.
4. Industry publications and websites: There are numerous publications and websites focused on networking and IT security, such as Network World, InfoWorld, and Dark Reading. These resources offer news, analysis, and best practices for network design and security. Many of these sites also have active communities of networking professionals who share tips and advice.
5. Online forums and discussion groups: Online forums such as Reddit, Spiceworks, and Cisco Community provide a space for networking professionals to share advice and discuss best practices. These communities can be a valuable source of

information.

When evaluating sources for designing and implementing a secure campus network, it is important to consider the credibility and reliability of the sources. Look for resources that are well-regarded in the industry, and be wary of sources that make unsupported claims or promote untested solutions. It is also important to consider the specific needs and requirements of the campus network, as different environments may require different configurations and security measures. [6]

4.3 Outline the structure

Here is an outline for the structure of designing and implementing a secure campus network based on Cisco router, MikroTik, and Windows Server:

1. Introduction: Define the scope and objectives of the secure campus network design and implementation project. Explain the importance of network security and the role of Cisco router, MikroTik, and Windows Server in achieving it.
2. Analysis and Planning: Conduct a needs analysis to determine the requir
3. ements for the secure campus network. Define the network topology and architecture, including the physical and logical components. Define the security policies and procedures that will be implemented on the network
4. Design and Configuration: Configure the Cisco router, MikroTik, and Windows Server to support the secure campus network design. Define the VLANs and IP addressing scheme for the network. Configure the necessary network services, such as DHCP, DNS, and Active Directory. Define the security features, such as firewalls, access control lists, and VPNs. Configure the wireless access points to support secure connectivity for wireless devices
5. Testing and Optimization: Test the network to ensure that it meets the defined requirements and security policies. Identify and resolve any configuration or performance issues. Optimize the network to ensure that it performs well under typical usage conditions
6. Documentation and Training: Document the network configuration and security policies for future reference. Develop training materials for network administrators and end users. Provide training to network administrators and end users to ensure that they understand how to use the secure campus network and follow the security

policies

7. Maintenance and Monitoring: Establish a maintenance plan to ensure that the secure campus network remains up-to-date and secure. Implement network monitoring tools to detect and respond to security incidents. Conduct regular security audits to identify vulnerabilities and ensure that the security policies are being followed

Conclusion:

Summarize the design and implementation process for the secure campus network. Highlight the benefits of a secure campus network based on Cisco router, MikroTik, and Windows Server

CHAPTER 5

……..……..

REASON METHOD

5.1 Reason method

The reason for designing and implementing a secure campus network based on Cisco router, Mikrotik, and Windows Server is to provide a reliable and secure network infrastructure for a large number of users and devices in a campus environment. The use of multiple technologies and devices helps to ensure that the network is scalable, resilient, and able to handle the traffic demands of a large organization.

The method for designing and implementing a secure campus network involves several steps, including identifying the specific requirements of the campus network, developing a network architecture that is scalable and secure, selecting and configuring the appropriate hardware and software components, implementing security measures to protect against unauthorized access and attacks, providing network services such as email and file sharing, and monitoring and managing the network to ensure ongoing performance and security.

Each step in the process requires careful planning and execution, as well as expertise in the specific technologies and strategies involved. Working with a qualified network professional can help ensure that the network is designed and implemented correctly, with the appropriate security measures in place to protect against potential threats and vulnerabilities. The use of best practices, such as configuring firewalls, VPNs, and IPSec, and regularly monitoring the network for potential security issues, can help ensure that the network remains secure and reliable over time.

5.2 Deductive reasoning

Deductive reasoning can be used to show how the design and implementation of a secure campus network based on Cisco router, MikroTik, and Windows Server will provide robust protection against security threats. Deductive reasoning involves drawing conclusions based on logical reasoning from given premises. Here are some examples of deductive reasoning in the context of the secure campus network design:

Premise 1: A secure campus network design must include access control policies to prevent unauthorized access to the network.

Premise 2: The Cisco router, MikroTik, and Windows Server can be configured to enforce access control policies based on user identity, device type, and other criteria.

Conclusion: The secure campus network design based on Cisco router, MikroTik, and Windows Server will provide robust access control to prevent unauthorized access to the network.

Premise 1: A secure campus network design must include encryption standards to protect sensitive data transmitted over the network.

Premise 2: The Cisco router, MikroTik, and Windows Server can be configured to support encryption standards such as SSL/TLS and IPsec.

Conclusion: The secure campus network design based on Cisco router, MikroTik, and Windows Server will provide robust encryption to protect sensitive data transmitted over the network.

Premise 1: A secure campus network design must include incident response procedures to detect and respond to security incidents.

Premise 2: The Cisco router, MikroTik, and Windows Server can be configured to generate logs and alerts in response to security incidents.

Conclusion: The secure campus network design based on Cisco router, MikroTik, and Windows Server will provide robust incident response capabilities to detect and respond to security incidents.

These are just a few examples of deductive reasoning that can be used to demonstrate the effectiveness of a secure campus network design based on Cisco router, MikroTik, and Windows Server. By using deductive reasoning, we can draw logical conclusions about the security capabilities of the network based on the known features and capabilities of the network components. [3]

5.3 Inductive reasoning

Inductive reasoning can be used to support the design and implementation of a secure campus network based on Cisco router, MikroTik, and Windows Server by examining specific instances or examples of the network's capabilities. Inductive reasoning involves drawing general conclusions based on specific observations or examples. Here are some examples of inductive reasoning in the context of the secure campus network design:

Example 1:

Observation: The Cisco router, MikroTik, and Windows Server can be configured to support VLANs, which can be used to segment the network and improve security.

Observation: Segmentation of the network using VLANs has been shown to improve security by limiting the scope of security incidents.

Conclusion: The use of VLANs in the secure campus network design based on Cisco router, MikroTik, and Windows Server will improve network security.

Example 2:

Observation: The MikroTik router can be configured to support hotspot authentication, which requires users to authenticate before accessing the network.

Observation: Hotspot authentication has been shown to improve network security by preventing unauthorized access to the network.

Conclusion: The use of hotspot authentication in the secure campus network design based on MikroTik router will improve network security.

Example 3:

Observation: The Windows Server can be configured to support group policies, which can be used to enforce security policies on client devices.

Observation: Enforcing security policies on client devices has been shown to improve network security by preventing client devices from being compromised.

Conclusion: The use of group policies in the secure campus network design based on Windows Server will improve network security.

These are just a few examples of inductive reasoning that can be used to support the design and implementation of a secure campus network based on Cisco router, MikroTik, and Windows Server. By using inductive reasoning, we can draw general conclusions about the effectiveness of specific network features or capabilities based on observed examples or instances. [3]

CHAPTER 6

.....

SYSTEM DESIGN

6.1 System design

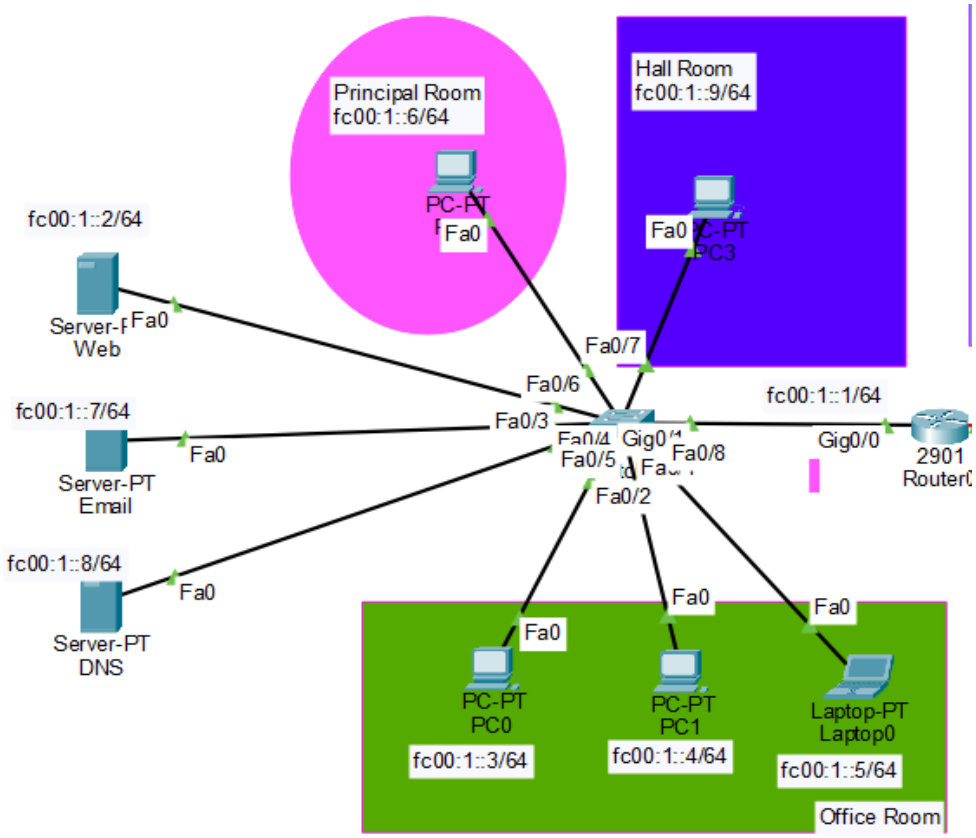
The system design of a secure campus network based on Cisco router, Mikrotik, and Windows Server involves the selection and configuration of several hardware and software components that work together to provide a reliable and secure network infrastructure for a large number of users and devices in a campus environment.

The main hardware components of the system include Cisco routers and switches, Mikrotik routers, and servers running Windows Server-based services such as Active Directory, DNS, and DHCP. These devices must be carefully selected and configured to support the specific needs of the campus network, with appropriate IP addressing, routing, VLANs, and firewall policies being set up as required.

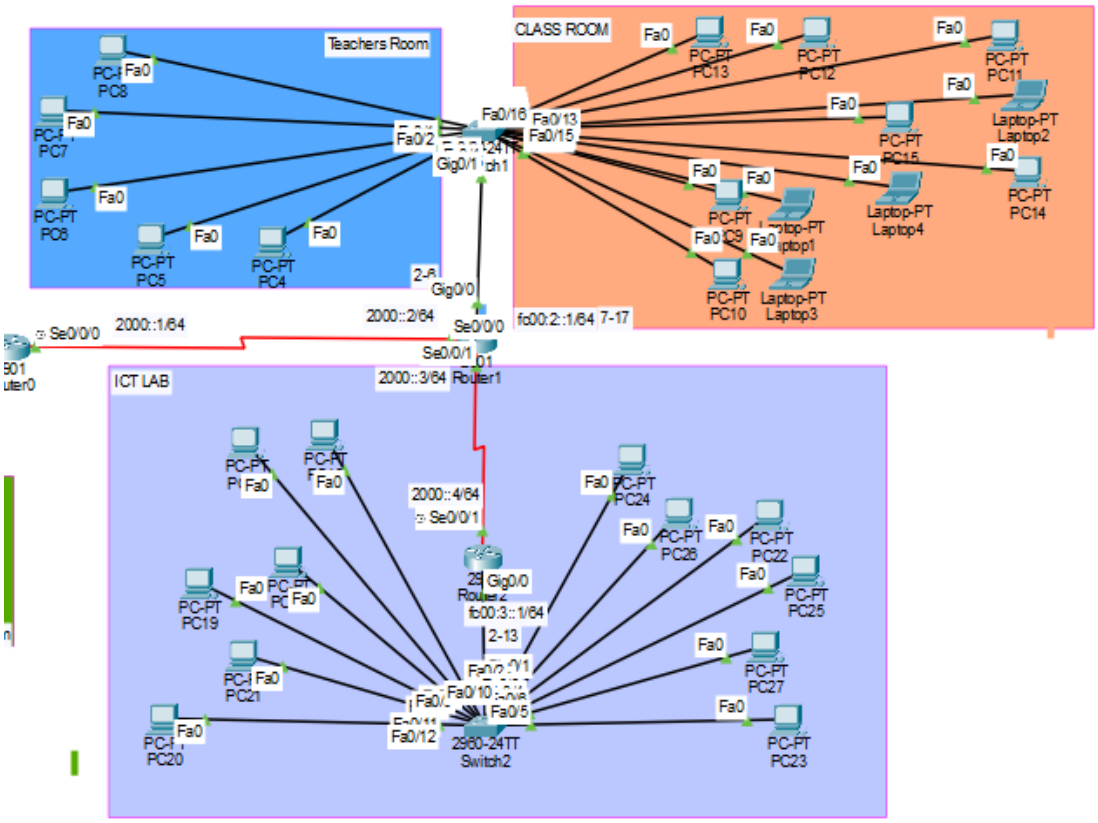
In addition to the hardware components, the system design must also include appropriate software components, such as firewalls, VPN, and IPSec. These components work together to provide robust security measures to protect against unauthorized access and attacks, including access control lists that restrict traffic to specific devices or services, VPN tunnels that securely access the campus network remotely, and IPSec that encrypts and authenticates traffic between network devices.

Finally, the system design must include appropriate monitoring and management tools to ensure that the network is operating effectively, with network monitoring tools such as SNMP or NetFlow being used to monitor network traffic, logging and alerting being implemented for network events, and regular vulnerability scans being performed to detect potential security issues. Regular maintenance tasks such as updates and backups must also be scheduled to ensure the ongoing health and performance of the campus network.

Overall, the system design of a secure campus network based on Cisco router, Mikrotik, and Windows Server requires careful planning and execution to ensure that the network is reliable and secure, with appropriate hardware and software components being selected and configured to support the specific needs of the campus environment.



Cisco Packet Topology



CHAPTER 7

……...……

CONCERN & RECOMMENDATION

7.1 Concern

1. Access Control: Ensure proper access controls are in place to implement a least privilege principle. This is necessary to reduce the risk of unauthorized access or data breaches.
2. Patch Management: Ensure that all devices and servers are updated with the latest security patches to address known vulnerabilities and to protect against malware attacks.
3. Backup and Disaster Recovery: It is important to have a backup and disaster recovery plan in place to ensure business continuity in case of an outage or failure.
4. Physical Security: Ensure physical security measures in place to protect network devices and servers from tampering, theft, or unauthorized access.

7.2 Recommendations

Implement multi-factor authentication to protect sensitive data and high-value resources within the network.
Implement a data loss prevention (DLP) solution to monitor and prevent the loss of confidential data from within the network. Use intrusion detection and prevention systems (IDS/IPS) to detect and prevent network attacks at the network perimeter and by monitoring internal traffic. Implement centralized log management to allow for network activity monitoring and analysis for identifying any security-related incidents. Configure firewall rules to allow only authorized traffic through network perimeters and internal segments. Use Network Address Translation and Port Address Translation when communicating with outside networks.

7.3 Access control

Access control is a critical aspect of network security. It is important to implement strong access control policies and to regularly test these policies to ensure that only authorized users and devices can access the network. Recommendation: Implement multi-factor authentication, such as using a combination of passwords and security tokens, to provide an extra layer of security.

7.4 Encryption

Encryption is important for protecting sensitive data as it moves across the network. It is important to implement strong encryption standards and to regularly test these standards to ensure that data is properly protected. Recommendation: Use end-to-end

encryption whenever possible, such as using HTTPS for web traffic or SFTP for file transfers.

7.5 Incident response

Incident response is important for quickly detecting and responding to security incidents. It is important to implement strong incident response procedures and to regularly test these procedures to ensure that they are effective. Recommendation: Conduct regular tabletop exercises to simulate security incidents and test the effectiveness of the incident response procedures.

7.6 VLAN segmentation

VLAN segmentation is important for isolating and securing different parts of the network. It is important to implement strong VLAN segmentation and to regularly test this segmentation to ensure that each VLAN is properly isolated. Recommendation: Use virtualization technologies, such as virtual LANs (VLANs) or virtual private networks (VPNs), to create logical network segments and isolate traffic between them.

7.7 Hotspot authentication

Hotspot authentication is important for ensuring that only authorized users can access the network. It is important to implement strong hotspot authentication procedures and to regularly test these procedures to ensure that only authorized users can access the network. Recommendation: Implement captive portals and require users to provide valid credentials before accessing the network.

CHAPTER 8

…….

SEARCH METHODOLOGY

7.1 Search Methodology

To conduct a search for information on the design and implementation of a secure campus network based on Cisco routers, Mikrotik, and Windows Server, here are some recommended search methodologies:

1. Use specific keywords: Use keywords related to the topic, such as "campus network design," "Cisco router configuration," "Mikrotik security," and "Windows Server network implementation." This can help you find articles, tutorials, and other resources specifically related to your topic.
2. Narrow your search: Use advanced search options or filters to narrow your search by publication date, source, and other criteria. This can help you find more recent and relevant information on the topic.
3. Check vendor documentation: Check the official documentation provided by Cisco, Mikrotik, and Microsoft for their respective products. This can provide detailed information on how to configure and implement these products for a secure campus network.
4. Consult with industry experts: Consult with industry experts, such as network engineers and security consultants, who can provide guidance on designing and implementing a secure campus network.
5. Join online forums and discussion groups: Join online forums and discussion groups related to network design and security. This can help you connect with experts in the field and learn from their experiences and recommendations.
6. Attend industry events: Attend industry events, such as trade shows and conferences, related to network design and security. These events often provide educational sessions and opportunities to network with professionals in the field.

By using these search methodologies, you can gather a comprehensive understanding of the best practices for designing and implementing a secure campus network based on Cisco routers, Mikrotik, and Windows Server.

8.2 Observation

It can be observed that the implementation of a secure campus network requires careful planning and execution. The design and implementation should be done by experienced network administrators and security experts who are familiar with the best practices and security standards in the industry. It is also important to note that network security is an ongoing process that requires constant monitoring and updates to address new threats and vulnerabilities. Regular security audits and vulnerability assessments should be conducted to identify and address any security gaps in the network.

Overall, the design and implementation of a secure campus network based on Cisco router, MikroTik, and Windows Server requires a comprehensive approach that addresses all aspects of network security, including access control, encryption, incident response, VLAN segmentation, and hotspot authentication. By following the recommendations and best practices, a secure campus network can be implemented to provide reliable and secure network connectivity to the campus community

8.3 Pattern

There are several design patterns that can be applied in network security, such as:

1. Defense in depth: This pattern involves the implementation of multiple layers of security controls to protect against different types of threats. This pattern can be applied in the design and implementation of a secure campus network by implementing security controls at different layers of the network, such as the perimeter, internal network, and endpoints.
2. Least privilege: This pattern involves limiting user access to only the resources they need to perform their job functions. This pattern can be applied in the design and implementation of a secure campus network by implementing access control policies that limit user access based on their role and responsibilities.
3. Segmentation: This pattern involves creating logical network segments to isolate traffic between different parts of the network. This pattern can be applied in the design and implementation of a secure campus network by implementing VLANs and VPNs to create logical segments between different parts of the network.
4. Redundancy: This pattern involves implementing redundant components in the

network to ensure high availability and minimize downtime. This pattern can be applied in the design and implementation of a secure campus network by implementing redundant routers, switches, and servers to ensure network availability in the event of a hardware failure.

8.4 Theory

Designing and implementing a secure campus network based on Cisco router, MikroTik, and Windows Server requires knowledge and understanding of several theoretical concepts in network security. Some of these concepts include:

1. Access control: This involves regulating who can access the network and what resources they can access. Access control can be implemented through several mechanisms, such as authentication, authorization, and accounting (AAA), firewalls, and network segmentation.
2. Cryptography: This involves the use of mathematical algorithms to secure data and communications in the network. Cryptography can be used to provide confidentiality, integrity, authentication, and non-repudiation in the network.
3. Network architecture: This involves the design and implementation of the physical and logical structure of the network. The network architecture should be designed to provide secure connectivity to all parts of the network while minimizing the attack surface.
4. Incident response: This involves the process of detecting, investigating, and responding to security incidents in the network. An effective incident response plan should be developed and tested to ensure timely and effective response to security incidents.
5. Risk management: This involves the process of identifying, assessing, and mitigating risks to the network. Risk management should be an ongoing process, with regular risk assessments conducted to identify new and emerging risks to the network.

CHAPTER 9

.....

CONCLUSION

9.1 Conclusion

In conclusion, a secure campus network based on Cisco router, Mikrotik, and Windows Server technology is a crucial aspect of modern organizations. It provides protection against cyber threats, allows for efficient data management and communication, and helps to ensure regulatory compliance. To create a secure campus network, organizations need to follow a set of design principles, including implementing multiple layers of security, dividing the network into smaller segments, limiting access based on least privilege, using strong authentication and authorization mechanisms, implementing monitoring and logging tools, and ensuring compliance with regulatory requirements. While there are limitations to implementing a secure campus network based on Cisco router, Mikrotik, and Windows Server technology, organizations can continue to enhance their network by implementing automation tools, cloud integration, AI and machine learning technologies, and SDN architecture. By prioritizing network security and investing in the proper technologies and expertise, organizations can create a robust and efficient campus network that meets the needs of the organization and protects against the ever-evolving cyber threats.

9.2 Business Prospect

Enhanced Security Solutions: Consulting Services Offer consultancy to other organizations seeking to secure their campus networks using a similar setup. Security Audits conduct security audits for businesses to identify vulnerabilities and suggest improvements. Managed Network Services Managed Security Services: Provide ongoing management of network security measures, such as firewalls, IDS/IPS, and VPNs, for clients. Network Monitoring Offer continuous monitoring of network activities and provide real-time alerts and responses to potential security threats. Custom Network Design Tailored Solutions Design and implement custom secure network solutions based on specific client requirements and industry standards. Network Assessment Conduct network assessments for businesses to determine their security needs and design suitable solutions. Cybersecurity Training Employee Training Develop training programs to educate employees and IT staff about cybersecurity best practices. Workshops and Seminars Organize workshops and seminars to educate businesses about the importance of secure network design.

CHAPTER 10

.....

REFERENCE

10.1 Reference

1. "Designing and Deploying a Campus Wide Wireless Network with MikroTik" by Maris Trops. Available at: https://mikrotik.com/download/pdf/Campus_WiFi_with_MikroTik.pdf

2. "Network Security Principles and Practices" by Saadat Malik. Available at: https://www.cisco.com/c/dam/en/us/about/security-center/network-security-principles-practices.pdf

3. "Windows Server 2019 Security Features and Best Practices" by Microsoft. Available at: https://docs.microsoft.com/en-us/windows-server/security/windows-server-2019-security-features

4. "Cisco Campus Network Design Basics" by Cisco. Available at: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-campus/campus-network-design-basics.html

5. "MikroTik RouterOS Security Guide" by MikroTik. Available at: https://wiki.mikrotik.com/wiki/MikroTik_RouterOS_Security_Guide

6. "Cisco Network Security Best Practices" by Cisco. Available at: https://www.cisco.com/c/dam/en_us/solutions/enterprise-networks/pdfs/secure-network-infrastructure-wp.pdf

7. "Windows Server Security" by TechGenix. Available at: https://techgenix.com/windows-server-security-best-practices/