**VLAN/WAP2 Configuration**

Prince Mitchell C.E

Table of Contents

[Introduction 3](#_Toc204874799)

[Network Threats 3](#_Toc204874800)

[Tools and methods used 4](#_Toc204874801)

[Steps taken to complete the Task 4](#_Toc204874802)

# Introduction

In today's digital world and with artificial intelligence evolving, network security plays a crucial role in protecting sensitive data and ensuring the safe operation of digital communication. As cyber threats continue to grow, implementing robust security measures has become essential for preventing threats to your data and network infrastructure. This report defines several types of network threats and key security implementations, such as Access Control Lists (ACLs), IP routes, firewalls, WPA2 on wireless routers, and secure network configurations and static routing. Through a logical and structured approach, we explore the reasoning behind these security mechanisms, their implementation, and their impact on protecting the network over the Internet.

# Network Threats

A **network threat** is any potential danger or malicious activity that aims to compromise the **security**, **integrity**, **availability**, or **confidentiality** of a computer network and its data.

There are different categories of network threats, such as: Unauthorized Access, Denial of Service (DoS/DDoS) Attacks, Phishing & Social Engineering, Man-in-the-Middle (MITM) Attacks, Packet Sniffing, IP Spoofing, Zero-Day Exploits, and Malware-Based Threats. In each category of this threat mentioned are different types of threats cyber-attacks use to gain unauthorized data. Malware-Based Threats are threats such as: **Viruses**: These infect files and spread across systems, **Worms**: This works like viruses, but they spread through the network without user action, **Trojans**: The threat disguises itself as legitimate software but performs malicious actions. **Ransomware**: an attacker encrypts data and demands payment to decrypt it. The following category is Unauthorized Access. Under this category are **Hackers**, who gain unauthorized access to systems to steal, modify, or destroy data/information. **Insider Threats**: Occurs when employees or trusted users abuse their access to a company’s network. The next is Denial of Service (DoS/DDoS) Attacks, which involve overloading network resources to make services unavailable. Another is Phishing & Social Engineering, by tricking users into revealing sensitive info (passwords, banking details). Furthermore, **Man-in-the-Middle (MITM) Attacks** occur when an attacker intercepts communication through the session ID between two systems. **Packet Sniffing** occurs when attackerscapture and analyze network traffic to steal sensitive data. **IP Spoofing**, when a cyber attackerpretends to be a trusted device by faking an IP address. **Zero-Day Exploits,** Attacks unknown or unpatched software vulnerabilities on the victim’s system.

# Tools and methods used

Learning and understanding the different types of network threats is essential to building a secure network by implementing basic security measures. A virtual lab with a router and one or two connected devices will be used for the task. So, for this project, a Cisco Packet Tracer will be used for the virtual lab, displaying connections between network devices.

# Steps taken to complete the Task

The devices selected for this task were a router, a switch and six PCs, a laptop, a firewall, and a wireless router. Two different networks were created, the INSIDE and the OUTSIDE network. Configuring the devices to have general connectivity with other devices was the first step. This helps to trace a device in the network easily if one fails to respond to a type of network request, such as an ICMP echo. To achieve this, the IP address routes, ACLs were implemented on the switch and routers, the devices were assigned IP addresses, the inside network received the private IP addresses, and the outside network received the public IP addresses. The firewall was configured to accept packets between the divided networks and to recognize other network devices listed between these networks. A configuration for the latest Wi-Fi security (WPA2) was implemented on the wireless router.

After the first step was successfully implemented, the second step was to go through the configurations and network, but this time listing the devices that are allowed to exit and enter the network through the router and firewall. The INSIDE network is divided into three sections: HR, IT, and Sales. They are all connected to a switch but divided into three sections using the VLANs. Implementing this method improves security and mitigates security flaws for an attack; it is recommended and used in both larger and smaller networks. A few examples of the created ACL lists were the firewall, which was configured to only accept any traffic from the sales department and to transport the traffic to the other network, but the other departments were denied access. The HR department was denied access to the IT departments, but the IT and SALES departments were granted access to the HR department in the INSIDE network. The screenshots below display different VLANS connected to different departments, and the directions in which data flows. It equally displays the IP route and ACL configurations set on the router and firewalls, and finally, the implemented Wi-Fi security on a firewall.

A computer screen shot of a diagram

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.