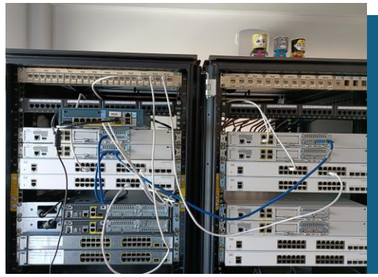
Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

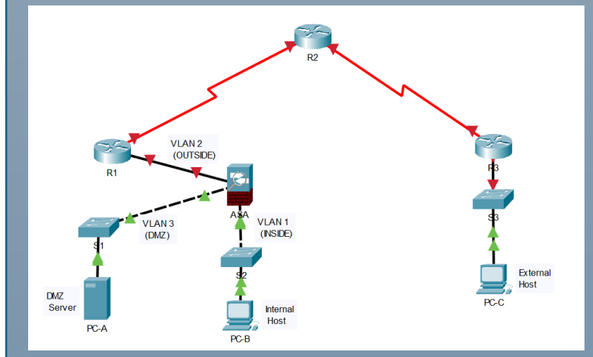


Firewall Configuration and Optimization

Author: Abdullah Azhar Cassim
BSc (Hons) Computing (Computer Networks and Cybersecurity)

Introduction

The main focus of this study is on testing the Cisco ASA 5505 firewall in a lab that was set up to simulate a real network. The main goal is to test the firewall's security features, performance, and dependability to make sure it works for small and medium-sized businesses. Setting up the firewall in a controlled lab environment, adjusting its settings, and running different tests on it, such as checking its security features in different situations, are all part of the project. The results are meant to give a full picture of the firewall's abilities and come up with the best ways to set it up and keep it running in a real-world setting



Project Goals

This project's main aim is to assess the capabilities of the Cisco ASA 5505 Firewall in a lab setting that mimics real-life scenarios. Assessing its security features, performance, and dependability is part of this to make sure it satisfies organisational security needs.

The general research question I'm attempting to address is: “How effective is the Cisco ASA 5505 firewall in terms of security features, performance, and dependability when subjected to real-life network scenarios?"
This question raises a number of important points:

Security Features: Evaluating the firewall's ability to keep threats, attacks, and unwanted access off a network. This involves assessing its capacity to manage and filter traffic for the prevention of malicious activity, as well as its capacity to manage and prevent intrusions and different security methods.

Performance: is the assessment of the firewall's effect on network performance. This involves timing, throughput, and the handling of simultaneous connections. It also involves understanding how various security policies or settings impact the network's responsiveness and speed.

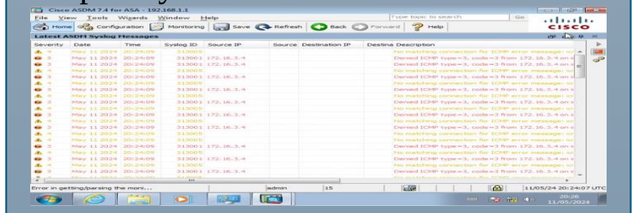
Dependability: is figuring out how reliable the firewall is in multiple operational environments. This covers its ability to keep network integrity and availability without regular downtimes or interruptions, its durability against different network threats, and its stability over long periods of time.

Implementation

The implementation of configuring and testing a Cisco ASA 5505 firewall in a simulated network environment :
Basic Configuration: Initial setup of the firewall, including hostname, domain name, interface security levels, and secure management access via SSH and HTTPS.
Network Scans: Conducted vulnerability scans using Nessus and Nmap from both internal and external networks to identify potential security issues.
Advanced Configuration: Set up a DMZ, configured NAT, and established access control lists (ACLs) to manage traffic between network zones.
DoS Attack Testing: Simulated a BlackNurse ICMP flood attack to evaluate the firewall's performance and response, monitoring CPU utilization and syslog messages.
The testing confirmed the firewall's ability to maintain internal network operations under attack, though it highlighted areas for potential configuration improvements.

Conclusions

Firewall Resilience: The firewall maintained internal network operations during a DDoS attack, indicating a level of resilience.
CPU Utilization: The firewall's CPU was heavily utilized during the attack, which could be a concern for sustained attacks over a longer period.
Intrusion Detection: The firewall's intrusion detection and prevention mechanisms were functional, as evidenced by the denied ICMP traffic, but the testing did not conclusively demonstrate an increase in detection capability with the complexity of the attack.



Overall, the tests were helpful in showcasing the firewall's capabilities and identifying areas for potential configuration improvements to enhance performance and security.