HOLISTIC CYBER DEFENCE NETWORK MODEL

Author: Mohamed Khaled Mahmoud
Supervisor: Dr. Sahar Ashraf Al-Shazly

OCTOBER 26, 2024
NATIONAL TELECOMMUNICATION INSTITUTE - NTI
Egypt Makes Electronics (EME) Initiative - 4M (Cybersecurity-Blue Team Cyber Security Boot Camp)

Abstract

This project outlines a comprehensive strategy for designing and securing a network infrastructure with a focus on critical security objectives. By employing secure routing, VLAN segmentation, and firewall integration, the project aims to create a resilient network foundation. Key configurations such as TACACS+, RADIUS, and NTP are used to enhance access control and ensure reliable time synchronization across network devices.

Additional advanced features, including IPsec VPN, Dynamic ARP Inspection (DAI), and role-based access control, are implemented to protect against potential internal and external threats. These configurations ensure that the network meets industry standards for security while maintaining accessibility for authorized users. Integration of Syslog and other logging mechanisms further supports monitoring and incident response.

The effectiveness of these configurations was verified through extensive testing, demonstrating the network's ability to withstand various security challenges. This project provides a strong foundation for secure, scalable network solutions and exemplifies the best practices for enterprise-grade network hardening and security management.

Acknowledgment

I would like to express my deepest appreciation to everyone who contributed to the successful completion of this project. Their support and guidance were instrumental, and I am truly grateful for their encouragement throughout this journey.

First and foremost, I extend my heartfelt gratitude to my esteemed instructor, **Dr. Sahar Ashraf Al-Shazly**, whose expertise, patience, and insightful feedback consistently guided me forward. Her mentorship inspired me to approach challenges with confidence and to strive for excellence. I am thankful for her unwavering belief in my potential and the academic growth she facilitated.

I am also profoundly grateful to the National Telecommunication Institute (NTI) for their support through the Egypt Makes Electronics (EME) Initiative. The resources and learning environment provided by NTI were invaluable in shaping my technical skills and advancing my knowledge in network security.

To my family and friends, I am deeply thankful for their constant encouragement and belief in me. Their support was a driving force, reminding me to persevere and remain focused on my goals.

Finally, I extend my thanks to everyone involved in this project. Their contributions have been vital to my academic journey, and their support has provided me with a strong foundation for future endeavors.

Contents

Holistic Cyber Defense Network Model

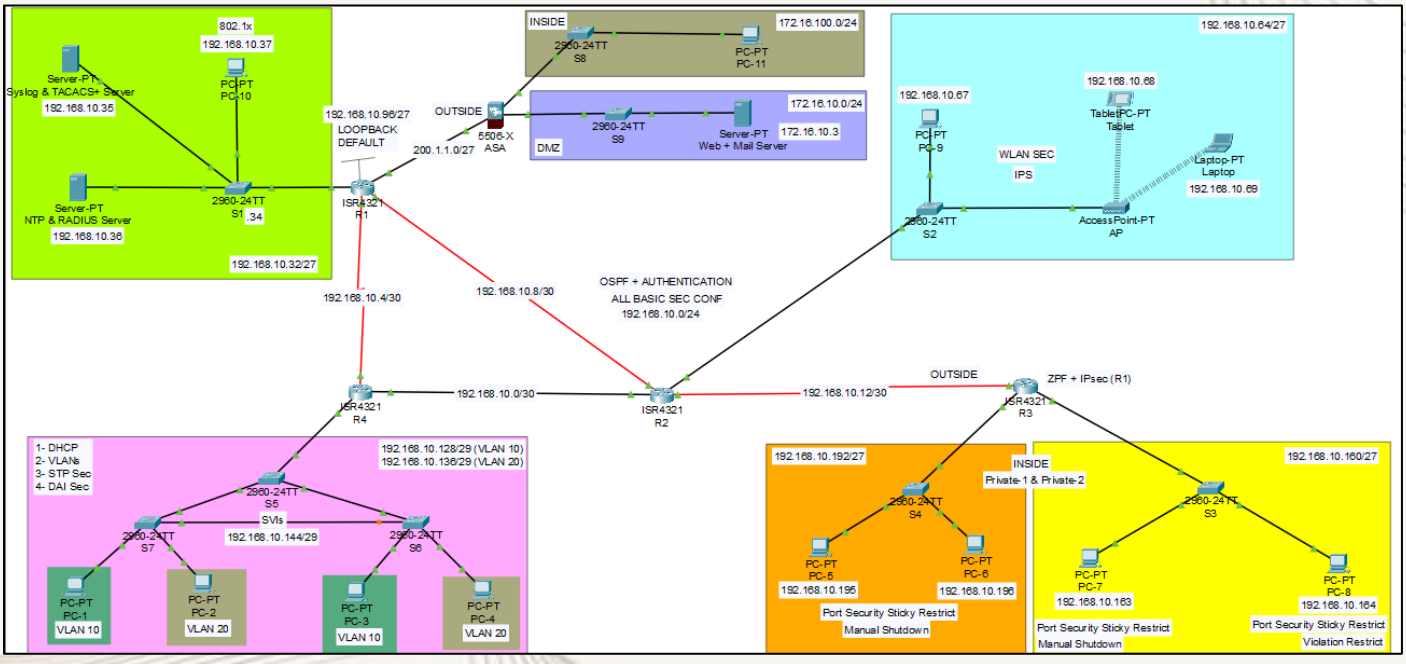
Introduction

The primary purpose of this project is to design and implement a secure and resilient network infrastructure tailored to meet the stringent security needs of an enterprise environment. By focusing on critical security configurations, this project aims to protect the network from a range of potential internal and external threats.

To achieve this, the project incorporates essential configurations such as **secure routing**, **VLAN segmentation**, and **firewall integration**. Advanced security protocols, including **TACACS+**, **RADIUS**, **IPsec VPN**, and **Dynamic ARP Inspection (DAI)**, are deployed to strengthen network integrity and manage access control effectively. Each component is carefully configured to optimize security and enhance overall network stability.

This project also includes comprehensive testing and validation to confirm the effectiveness of each security measure. By implementing best practices in network security, this project provides a robust framework for scalable, enterprise-grade security solutions.

Network Topology



Objectives

- **Basic Configuration (Routers & Switches).**
  - Use “192.168.10.0/24” to meet network addressing requirements.
  - Change Hostname.
  - Minimum password length = 10. (Router)
  - Create Encrypted Password for Privileged EXEC Mode.
  - Configure Domain Name, User and Password “Local DB” & RSA encryption.
  - Configure & Secure Console Port.

    - Configure & Secure AUX port. (Router)
    - Activate & Secure 5 VTY ports & enable SSH.
    - Prevent login brute force attack “block-for”. (Router)
    - Disable DNS lookup for unrecognized commands.
    - Banner Message.
    - Encrypt all passwords.
    - Configure Interfaces. (SVI-Switches)
    - Configure default gateway. (Switches)
    - Assign unused ports to unused VLAN and shut down. (Switches)
- **Configure Dynamic Routing Protocol (OSPFv2).**
    - Configure Passive Interfaces.
- **Configure OSPF MD5 authentication.**
- **Configure NTP Server & NTP Authentication (TACACS+).**
    - Pre-Shared Key in NTP server (cisco12345)
    - Configure routers to timestamp log messages
    - Configure TACACS+ (Port No, Client IP, Client Name, Server Type, Secret Key, User Setup)
- **Configure Syslog Server (RADIUS).**
    - Severity 7
    - Configure RADIUS (Port No, Client IP, Client Name, Server Type, Secret Key, User Setup)
    - Allow RADIUS EAP-MD5.
- **Configure PC-10 802.1X Port-based Authentication.**
- **Configure SVIs on all Switches.**
    - Unused Ports → Unused VLAN
    - Switch Port Access (End Devices).
    - Switch Port Trunk (Intermediate Devices).
    - Close DTP negotiation.
    - Close Unused ports.
- **Assign Static IPs for all PC & Server.**
- **Check the authentication key in Servers.**
- **ASA 5506-X:**
    - Configure Hostname.
    - Configure NTP & NTP Authentication.
    - Create Encrypted Password for Privileged EXEC Mode.
    - Configure Domain Name & Create an RSA key for SSH (1024).
    - Configure secure VTY 5 ports.
    - Configure interfaces & security level.
    - Configure default route.
    - Create LOCAL credential.
    - Configure AAA authentication.
    - NAT and ACL for INSIDE & DMZ.
        - ACL permit SMTP & HTTPS (ICMP for testing if you need).
    - Allow ICMP reply using “inspect”.
    - Configure DHCP & DNS.
- **R1 (Loopback 0) default route “Static” and publish it for all routers.**
    - Privilege level administrative access.
- **R2:**

- Configure IPS (Allow inside ping and deny outside ping)
- WLAN Security.
- Connect Laptop.
- Role-based administrative access.

- **R3:**
  - ZPF (Private-1 & Private-2 & OUTSIDE)
  - VPN-IPsec.
  - Switches Port-Security
    - PC-8 (MAC Sticky Learn & Restrict & Maximum 3)
    - PC-7 (MAC Sticky Learn & Shutdown & Maximum 3)
    - PC-6 & PC-5 (MAC Sticky Learn & Shutdown & Maximum 3)
- **R4:**
  - VPN-IPsec.
  - 2 DHCP POOL.
  - DHCP Snooping.
  - VLAN security. <Done by configuration>
  - VLANs.
    - 10,20 Data.
      - 10 for SOC-Department.
      - 20 for IT-Department.
    - 30 Native.
    - 40 Unused Ports.
    - 99 Management SVI.
  - Mitigate STP Attacks.
    - Port Fast
    - BPDU guard
  - Configure Dynamic ARP inspection (DAI).
  - Create a Redundant Link between S6 and S7 (F0/3).

Addressing Table

Device	Interface	IP Address	Subnet/Prefix	Default Gateway
R1	G0/0/0	192.168.10.33	255.255.255.224	N/A
	S0/1/0	192.168.10.5	255.255.255.252	N/A
	S0/1/1	192.168.10.9	255.255.255.252	N/A
	Loopback 0	192.168.10.97	255.255.255.224	N/A
	G0/0/1	200.1.1.1	255.255.255.224	N/A
R2	G0/0/0	192.168.10.65	255.255.255.224	N/A
	G0/0/1	192.168.10.1	255.255.255.252	N/A
	S0/1/0	192.168.10.10	255.255.255.252	N/A
	S0/1/1	192.168.10.13	255.255.255.252	N/A
R3	S0/1/0	192.168.10.14	255.255.255.252	N/A
	G0/0/1	192.168.10.161	255.255.255.224	N/A
	G0/0/0	192.168.10.193	255.255.255.224	N/A
R4	S0/1/0	192.168.10.6	255.255.255.252	N/A

	G0/0/1	192.168.10.2	255.255.255.252	N/A
	G0/0/0.1 (10)	192.168.10.129	255.255.255.248	N/A
	G0/0/0.2 (20)	192.168.10.137	255.255.255.248	N/A
	G0/0/0.99	192.168.10.145	255.255.255.248	N/A
ASA 5506-X	G1/1	200.1.1.2	255.255.255.224	N/A
	G1/2	172.16.100.1	255.255.255.0	N/A
	G1/3	172.16.10.1	255.255.255.0	N/A
S1	VLAN 1	192.168.10.34	255.255.255.224	192.168.10.33
S2	VLAN 1	192.168.10.66	255.255.255.224	192.168.10.65
S3	VLAN 1	192.168.10.162	255.255.255.224	192.168.10.161
S4	VLAN 1	192.168.10.194	255.255.255.224	192.168.10.193
S5	VLAN 99	192.168.10.146	255.255.255.248	192.168.10.145
S6	VLAN 99	192.168.10.147	255.255.255.248	192.168.10.145
S7	VLAN 99	192.168.10.148	255.255.255.248	192.168.10.145
S8	VLAN 1	172.16.100.2	255.255.255.0	172.16.100.1
S9	VLAN 1	172.16.10.2	255.255.255.0	172.16.10.1
Syslog & TACACS+ Server	NIC (Static)	192.168.10.35	255.255.255.224	192.168.10.33
NTP & RADIUS Server	NIC (Static)	192.168.10.36	255.255.255.224	192.168.10.33
Web + Mail Server	NIC (Static)	172.16.10.3	255.255.255.0	172.16.10.1
PC-1	NIC (DHCP)	----------	255.255.255.248	192.168.10.129
PC-2	NIC (DHCP)	----------	255.255.255.248	192.168.10.137
PC-3	NIC (DHCP)	----------	255.255.255.248	192.168.10.129
PC-4	NIC (DHCP)	----------	255.255.255.248	192.168.10.137
PC-5	NIC (Static)	192.168.10.195	255.255.255.224	192.168.10.193
PC-6	NIC (Static)	192.168.10.196	255.255.255.224	192.168.10.193
PC-7	NIC (Static)	192.168.10.163	255.255.255.224	192.168.10.161
PC-8	NIC (Static)	192.168.10.164	255.255.255.224	192.168.10.161
PC-9	NIC (Static)	192.168.10.67	255.255.255.224	192.168.10.65
PC-10	NIC (Static)	192.168.10.37	255.255.255.224	192.168.10.33
PC-11	NIC (DHCP)	172.16.100.3	255.255.255.0	172.16.100.1
Tablet	NIC (DHCP)	192.168.10.68	255.255.255.224	192.168.10.65
Laptop	NIC (DHCP)	----------	255.255.255.224	192.168.10.65

Subnetting Table

(192.168.10.0/24)

Network Number	Network Address	Broadcast IP	No. of Valid Hosts	First IP address	Last IP address
N1	192.168.10.0/27	192.168.10.31	30	192.168.10.1	192.168.10.30
N2	192.168.10.32/27	192.168.10.63	30	192.168.10.33	192.168.10.62
N3	192.168.10.64/27	192.168.10.95	30	192.168.10.65	192.168.10.94
N4	192.168.10.96/27	192.168.10.127	30	192.168.10.97	192.168.10.126
N5	192.168.10.128/27	192.168.10.159	30	192.168.10.129	192.168.10.158
N5-VLAN 10-20	192.168.10.128/29 192.168.10.136/29	192.168.10.135 192.168.10.143	6 6	192.168.10.129 192.168.10.137	192.168.10.134 192.168.10.142
N5-SVI	192.168.10.144/29	192.168.10.151	6	192.168.10.145	192.168.10.150
N5-(free)	192.168.10.152/29	192.168.10.159	6	192.168.10.153	192.168.10.158
N6	192.168.10.160/27	192.168.10.191	30	192.168.10.161	192.168.10.190
N7	192.168.10.192/27	192.168.10.223	30	192.168.10.193	192.168.10.222
N8	192.168.10.224/27	192.168.10.255	30	192.168.10.225	192.168.10.254
N1-WAN	192.168.10.0/30	192.168.10.3	2	192.168.10.1	192.168.10.2
N2-WAN	192.168.10.4/30	192.168.10.7	2	192.168.10.5	192.168.10.6
N3-WAN	192.168.10.8/30	192.168.10.11	2	192.168.10.9	192.168.10.10
N4-WAN	192.168.10.12/30	192.168.10.15	2	192.168.10.13	192.168.10.14

The routers & switches Username & Password:

User: admin
Any password: admin12345