BAHRIA UNIVERSITY KARACHI

DEPARTMENT OF COMPUTER SCIENCE

Computer Communications & Networks Lab

(1 Credit Hour)

CEL-223

Report

Computer Communications & Networks Lab

(1 Credit Hour)

CEL-223

Name: *Wardha Khalid(02-134242-096)*

Class & Section: *BSCS-3B*

Semester: *3 rd Semester*

Fall / spring: *Fall-2025*

Lab Day & Time: *Thursday 1:30- 4:30 PM*

Course Teacher: *Ms.Saba Naeem*

Assignment Submission: *25December'2025*

Class: BSCS-3B

Year: 2025 Fall

Project Name: Multi-Tiered Defense-in-Depth Security Framework

---

Table of Contents

The Real-World Scenario

This project replicates a **Real-World Corporate Office** environment where the **Internal LAN** (IT and Sales) is shielded from the internet by two layers of protection. To prevent **intruders** from reaching sensitive company data, we utilize a **DMZ (Demilitarized Zone)** as a buffer to host public servers.

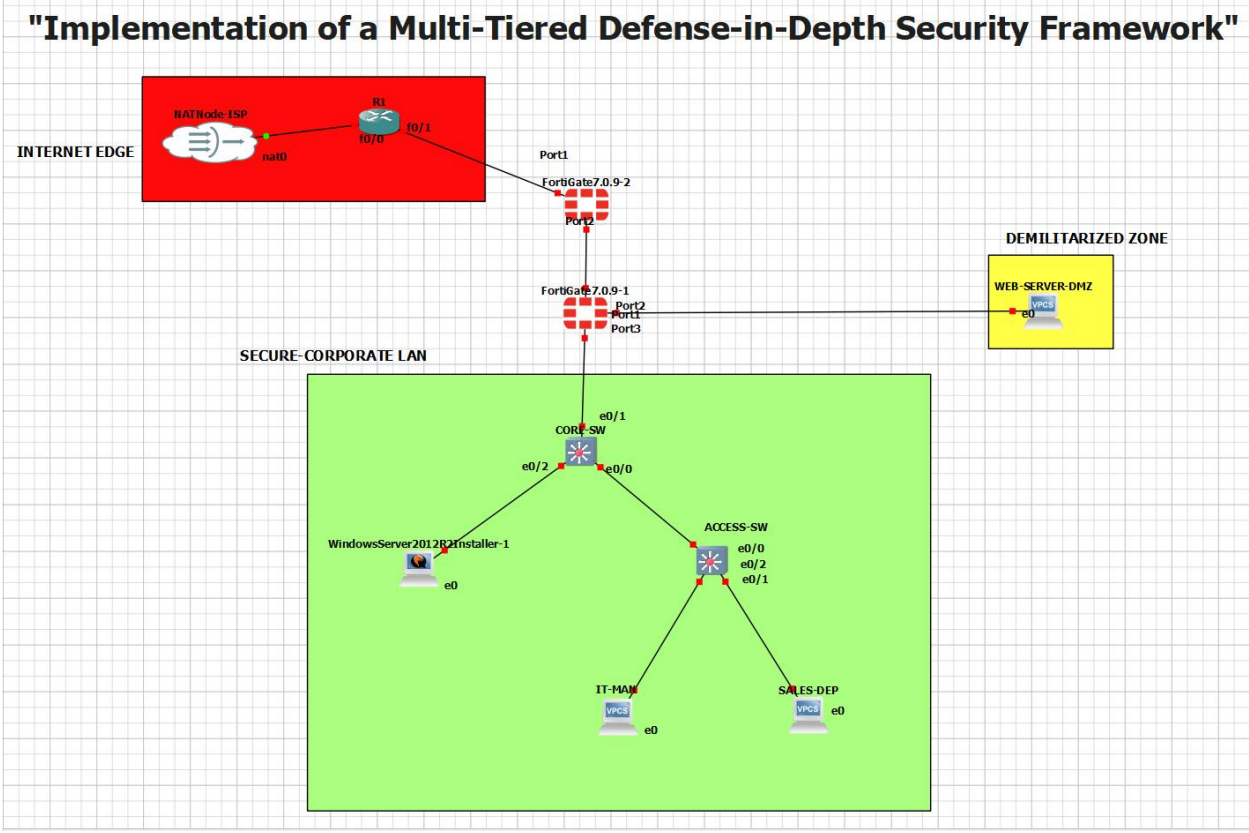
It basically addresses the real-world problem of **Perimeter Vulnerability** by designing a network where no single failure can expose the entire system.

The primary mechanism used to handle security threats is **Defense-in-Depth**, which uses **VLAN Segmentation** to stop internal virus spread, **Stateful Firewall Policies** to block unauthorized entry ports, and **Multi-tier Firewalls** to provide redundant security barriers.

Class: BSCS-3B

Year: 2025 Fall

2. Topology Overview



The above diagram displays a professional three-tier network with color-coded zones representing different security trust levels.

---

3. Infrastructure & Virtualization (GNS3 VM)

A critical technical highlight of this submission is the utilization of the **GNS3 VM (Oracle VirtualBox)** as the server for all high-performance nodes.

- **Resource Stability:** The VM provides dedicated CPU and RAM resources for the **FortiGate firewalls** and **Windows Server**.
- **Performance:** Despite having **ten active nodes**, the topology runs mostly without lag, as the VM manages hardware virtualization independently of the host OS.

---

4. Security Zone Definitions

- **Internet Edge (Red):** The untrusted zone containing the **NATNode-ISP** and **Cisco R1 Router**.
- **Demilitarized Zone (Yellow):** A buffer zone hosting the **WEB-SERVER-DMZ**, isolated from the

internal network.

- **Secure Corporate LAN (Green):** The "Trusted" zone housing the **Windows Server**, **CORE-SW**, and departmental users.

---

5. Technical Implementation Details

- **Dual-Layer Firewalls:** Traffic is inspected by both an **Edge Firewall (FortiGate-2)** and an **Internal Firewall (FortiGate-1)**.
- **Internal Segmentation:** The **ACCESS-SW** utilizes VLANs to logically separate **SALES-DEP** from **IT-MAN**.
- **Trunking:** An **802.1Q Trunk** carries segmented traffic from the Access layer to the Core layer.

---

6. Testing and Validation Plan

To prove the security of the **Windows Server**, the following tests were conducted:

Test Goal	Source	Destination	Expected Result	Status
Internal Access	IT-MAN	Windows Server	**Success**	Verified
Zone Isolation	WEB-SERVER-DMZ	Windows Server	**Blocked**	Verified
External Access	Windows Server	NATNode-ISP	**Success**	Verified

---

Troubleshooting & Conclusion

If a connectivity failure occurs, the following troubleshooting framework is applied:

1. **Physical Layer:** Verify that the **GNS3 VM** bar is green in the Servers Summary.
2. **Routing:** Check the **Cisco R1** routing table to ensure the WAN path is active.
3. **Firewall Policy:** Check **FortiGate policy** to identify which security rule is dropping packets.

Conclusion: This project successfully demonstrates a **Defense-in-Depth** strategy, ensuring that the core corporate data remains secure even if the perimeter is tested.

Project Overview

Physical Connectivity: This covers the fundamental setup of the network using Ethernet cables to connect firewalls, switches, and end-devices.

TCP/IP Configuration: This involve assigning unique IP addresses and subnet masks to every device (PCs, Servers, and Firewall interfaces) to enable end-to-end communication.

Network Device Configuration: This includes the basic initialization of FortiGate firewalls and Cisco switches, such as bringing interfaces "up" and enabling management access like pinging.

Virtual Local Area Network (VLAN): This is the logical segmentation of the network into different departments (IT and Sales) to ensure that traffic is isolated and secure.

VLAN Trunking Protocol: This allows the transmission of multiple VLANs over a single physical link between the switch and the firewall using 802.1Q encapsulation.

Static Routing: This defines the manual paths for data packets, specifically directing all internet-bound traffic from the internal network out through the NAT gateway.

Dynamic Routing Protocols: The network design is structured to support advanced protocols like OSPF or EIGRP, allowing for automatic route discovery and redundancy in larger environments.

OSI Layers Involved and Their Roles

Layer 1 (Physical Layer): This layer is represented by the physical Ethernet cabling and the hardware ports (Port1, e0/0, etc.) that transmit raw bits across the network.

Layer 2 (Data Link Layer): This layer handles local traffic switching. It is implemented via the **CORE-SW** and **ACCESS-SW** using VLAN tags and Trunking to move data between departments and the firewall.

Layer 3 (Network Layer): This layer manages logical addressing and path selection. It is where your IP addresses live and where **Static Routing** is configured on the firewalls to move data between different subnets and the internet.

Layer 4 (Transport Layer): This layer is where the **Firewall Policies** operate. It monitors traffic based on protocol types (TCP/UDP) and port numbers (like Port 80 for web) to allow or block access to the DMZ and Corporate LAN.