Class: BSCS-3B

Year: 2025 Fall

BAHRIA UNIVERSITY KARACHI

DEPARTMENT OF COMPUTER SCIENCE

Computer Communications & Networks Lab

(1 Credit Hour)

CEL-223

Report

Class: BSCS-3B

Year: 2025 Fall

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

TITLE: Smart Port Network Security Architecture – A Multi-Zone Defense-in-Depth Implementation

Table of Contents

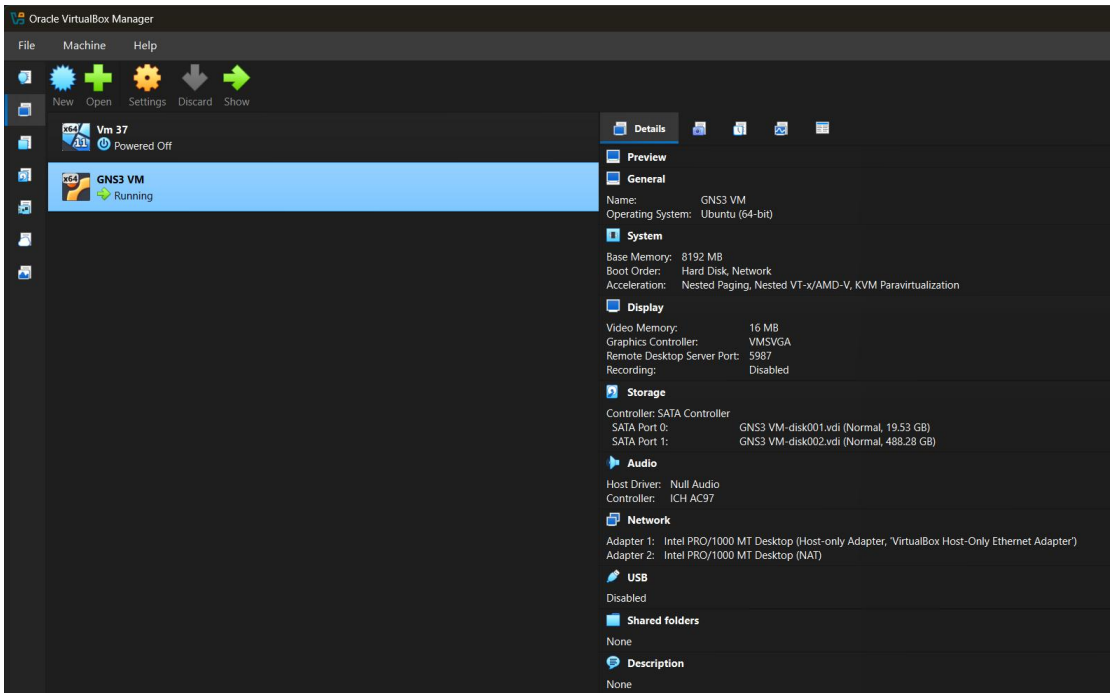
---

1. Executive Summary: The Real-World Scenario

This project replicates a **Real-World Smart Harbor** environment where digital surveillance, cargo tracking, and administrative operations are integrated into a single secure network. To address the problem of **Perimeter Vulnerability**, we utilize a **Defense-in-Depth** strategy. This ensures that no single failure—such as a compromised surveillance camera—can expose sensitive company data or the "Data Vault" [2]. The design utilizes **VLAN Segmentation** to stop lateral virus spread and **Stateful Firewall Policies** to block unauthorized entry[3].

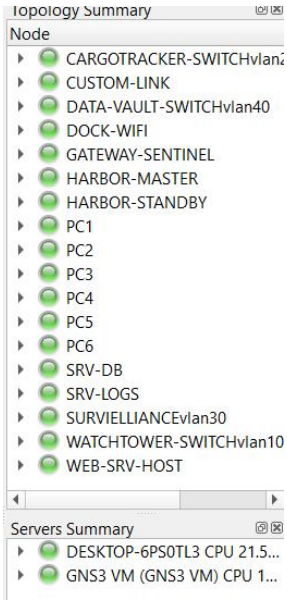
2. Infrastructure & Virtualization (GNS3 VM)

A critical technical highlight of this submission is the utilization of the **GNS3 VM (Oracle VirtualBox)**[4].



Class: BSCS-3B

Year: 2025 Fall

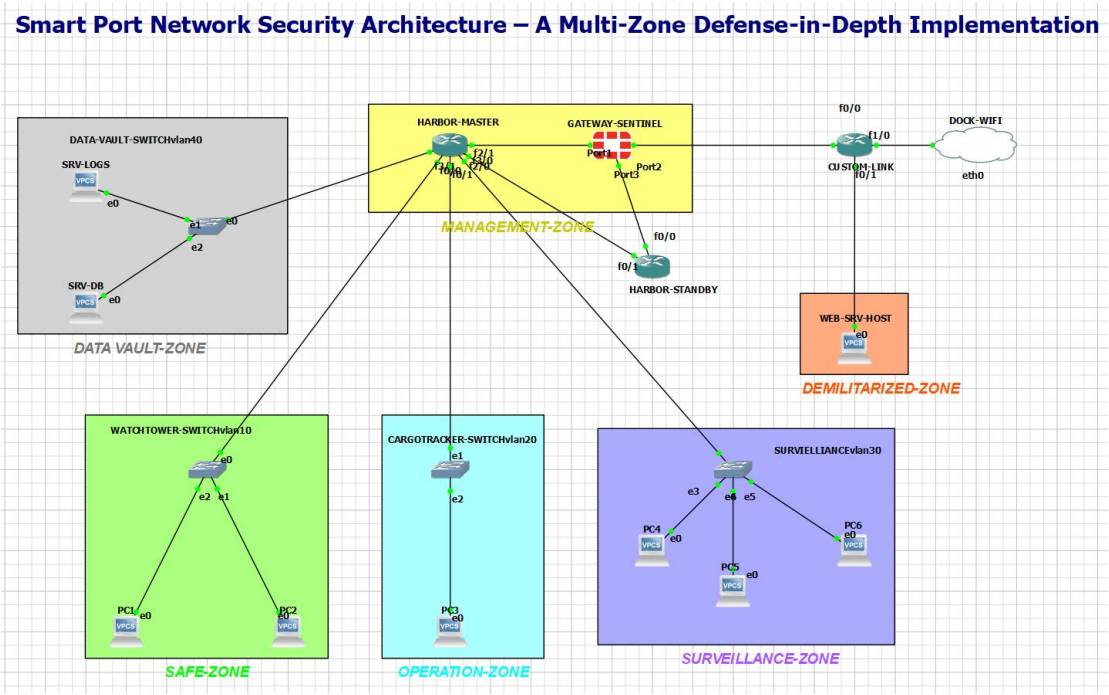


Resource Stability: The VM provides dedicated CPU and RAM for high-performance nodes like the **FortiGate VM** and **Cisco 7200** routers[5].

Performance: Despite having **15+ active nodes**, the topology runs mostly without lag as the VM manages hardware virtualization independently of the host OS[6].

3. Topology Overview

The architecture features a central **GATEWAY-SENTINEL** FortiGate firewall acting as the primary security barrier. Internal traffic is managed by the **HARBOR-MASTER** router, which serves as the gateway for all departmental subnets.



Class: BSCS-3B

Year: 2025 Fall

4. Security Zone Definitions

The network is segmented into five functional security zones based on trust levels:

Safe Zone (Green - 10.10.10.0/24): Includes **PC1**, **PC2**, and the Watchtower switch. This is the highest trust area for port control terminals.

Operations Zone (Blue - 10.10.20.0/24): Dedicated to **PC3** and cargo tracking readers. Logically separated to prevent internal lateral movement

.

Surveillance Zone (Purple - 10.10.30.0/24): High-traffic zone for IP cameras (**PC4, PC5, PC6**).

Data Vault Zone (Grey - 10.10.40.0/24): The most restricted zone, housing **SRV-LOGS** and **SRV-DB** (Databases).

Management & DMZ (Yellow/Orange): Includes the firewall transit link (**192.168.1.0/24**) and the **WEB-SRV-HOST** (**172.16.1.10**) in a zero-trust buffer zone.

5. Technical Implementation Details

VLAN Segmentation: Logical separation is maintained using **802.1Q encapsulation** on the HARBOR-MASTER router.

Point-to-Point Security: Direct connections between the firewall and DMZ router reduce the attack surface.

Static Path Selection: The firewall uses a static route (10.0.0.0/8) pointing to the internal gateway (192.168.1.2) to ensure return traffic finds the correct zone.

6. Testing and Validation Plan

To prove the security of the infrastructure, the following tests were conducted:

The Connectivity Test: Ping from PC1 to Harbour Master router

```
PC1> ping 10.10.10.1

10.10.10.1 icmp_seq=1 timeout
84 bytes from 10.10.10.1 icmp_seq=2 ttl=255 time=19.894 ms
84 bytes from 10.10.10.1 icmp_seq=3 ttl=255 time=11.382 ms
84 bytes from 10.10.10.1 icmp_seq=4 ttl=255 time=6.796 ms
84 bytes from 10.10.10.1 icmp_seq=5 ttl=255 time=11.334 ms
```

The Bridge Test: Ping from PC1 to Web Server.

```
PC1> ping 172.16.1.10

84 bytes from 172.16.1.10 icmp_seq=1 ttl=61 time=91.510 ms
84 bytes from 172.16.1.10 icmp_seq=2 ttl=61 time=40.279 ms
84 bytes from 172.16.1.10 icmp_seq=3 ttl=61 time=42.583 ms
84 bytes from 172.16.1.10 icmp_seq=4 ttl=61 time=33.241 ms
84 bytes from 172.16.1.10 icmp_seq=5 ttl=61 time=40.429 ms
```

Class: BSCS-3B

Year: 2025 Fall

The Security Test: Ping from Web Server to PC1

```
WEB-SRV-HOST> ping 10.10.10.11

10.10.10.11 icmp_seq=1 timeout
10.10.10.11 icmp_seq=2 timeout
10.10.10.11 icmp_seq=3 timeout
10.10.10.11 icmp_seq=4 timeout
10.10.10.11 icmp_seq=5 timeout
```

The Perimeter Reachability Test: Ping from PC1 to Gateway-Sentinel

```
PC1> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=254 time=31.316 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=254 time=17.843 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=254 time=19.263 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=254 time=15.607 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=254 time=13.721 ms
```

Perimeter Exit ValidationTest: Ping from PC1 to Custom-Link Router

```
PC1> ping 203.0.113.1

84 bytes from 203.0.113.1 icmp_seq=1 ttl=253 time=122.419 ms
84 bytes from 203.0.113.1 icmp_seq=2 ttl=253 time=57.485 ms
84 bytes from 203.0.113.1 icmp_seq=3 ttl=253 time=29.461 ms
84 bytes from 203.0.113.1 icmp_seq=4 ttl=253 time=24.635 ms
84 bytes from 203.0.113.1 icmp_seq=5 ttl=253 time=24.250 ms
```

7. Troubleshooting & Conclusion

If connectivity failures occur, we apply the following framework:

Physical Layer: Verify the **GNS3 VM** status bar is green in the Servers Summary[8].

Routing Audit: Check the **HARBOR-MASTER** routing table to ensure sub-interfaces are "Up"[9].

Firewall Policy: Inspect **FortiGate logs** to identify which security rule is dropping packets[10].

Conclusion: This project successfully demonstrates a **Defense-in-Depth** strategy, ensuring core database and port operations remain secure even if one zone is tested[11].

Class: BSCS-3B

Year: 2025 Fall

8. OSI Layer Mapping

Layer 1 (Physical): Hardware ports (FastEthernet, Port1) and Ethernet cabling[12].

Layer 2 (Data Link): Implemented via **VLAN tags and Trunking** on switches to isolate departments[13].

Layer 3 (Network): IP addressing and **Static Routing** on the FortiGate to manage cross-subnet paths[14].

Layer 4 (Transport): Firewall Policies monitoring traffic based on protocol types (TCP/UDP) and port numbers[15].