Project Report: Enterprise Network Security Architecture

1. Executive Summary

This project aims to design, simulate, and secure a scalable enterprise network connecting a Headquarters (HQ) and a Branch Office via a simulated ISP backbone. The architecture utilizes Fortinet FortiGate Next-Generation Firewalls (NGFW) to establish perimeter security, network segmentation (LAN/DMZ), and traffic management.

Key achievements include the configuration of ISP-level routing, implementation of strict firewall policies for outbound traffic (SNAT), and the secure publishing of internal services using Destination NAT (DNAT/Port Forwarding).

2. Network Topology & Architecture

The simulated infrastructure consists of three main zones:

A. ISP Backbone (Internet Simulation)

Device: Cisco c7200 Router.

Function: Simulates the public internet, handling routing between sites and providing public IP addressing.

Configuration: Configured with specific gateways for each site (11.11.11.1 and 22.22.22.1).

B. Headquarters (HQ - Site A)

Gateway: FortiGate VM (Forti-1).

WAN IP: 22.22.22.2/24.

Internal Network (LAN): 20.20.20.0/24 (Employee Zone).

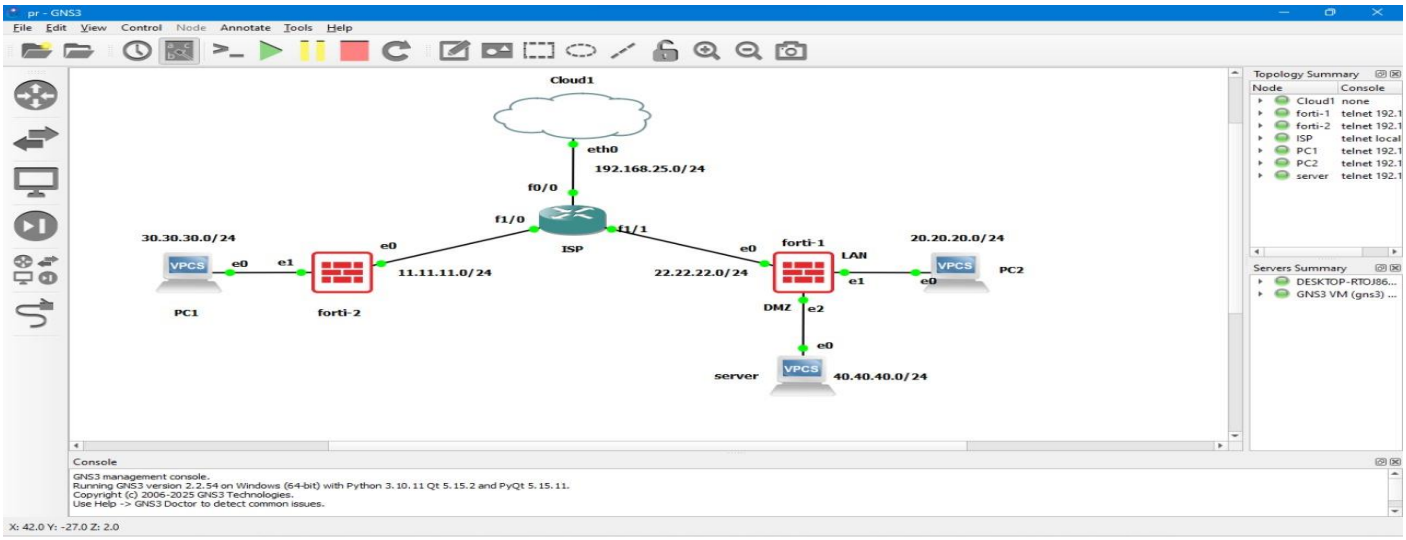
Demilitarized Zone (DMZ): 40.40.40.0/24 (Server Zone).

C. Branch Office (Site B)

Gateway: FortiGate VM (Forti-2).

WAN IP: 11.11.11.2/24.

Internal Network (LAN): 30.30.30.0/24.



3. Technical Implementation

Phase 1: Infrastructure & Routing

The ISP router was configured to handle traffic between the two distinct WAN subnets.

Static Routing: Implemented on both FortiGate units to route traffic to the default gateway (ISP).

ISP NAT: Configured NAT overload on the ISP router to simulate real-world internet access for private networks.

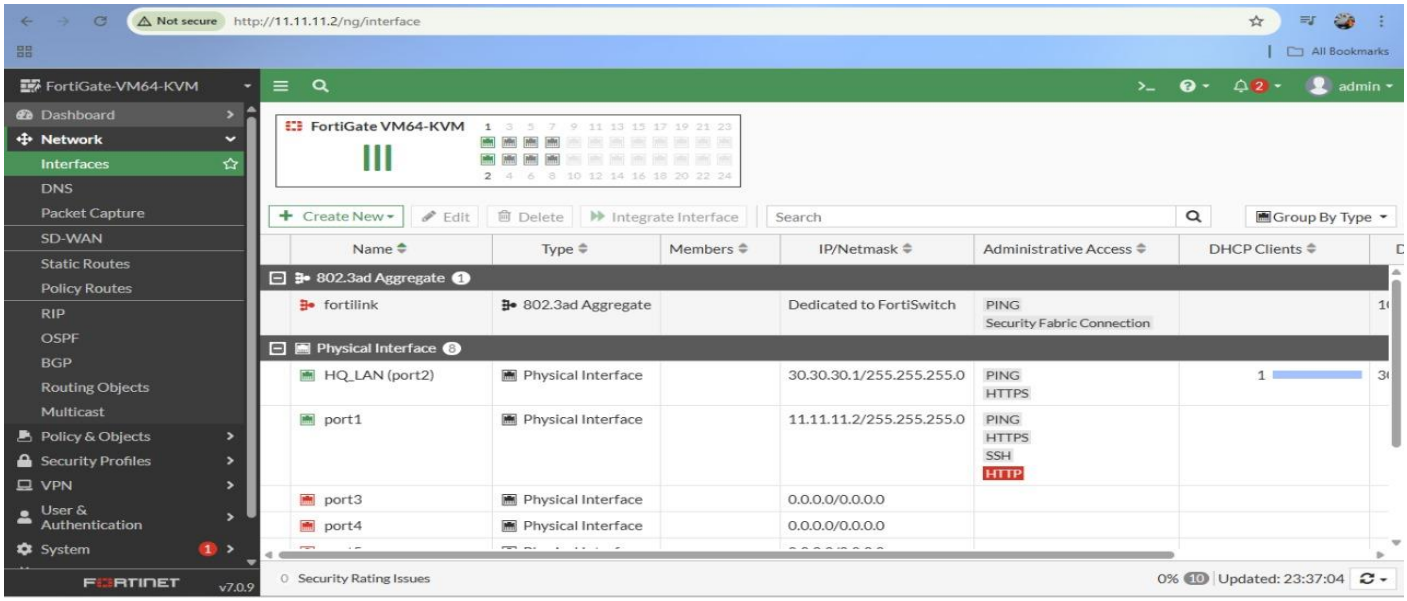
```
*Dec   3 08:40:19.999: %LINK-3-UPDOWN: Interface FastEthernet1/1, changed state to up
*Dec   3 08:40:20.007: %LINK-3-UPDOWN: Interface FastEthernet2/0, changed state to up
*Dec   3 08:40:20.015: %LINK-3-UPDOWN: Interface FastEthernet2/1, changed state to up
*Dec   3 08:40:21.311: %SYS-5-CONFIG_I: Configured from memory by console
*Dec   3 08:40:21.627: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
*Dec   3 08:40:21.631: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
*Dec   3 08:40:21.635: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/1, changed state to up
*Dec   3 08:40:21.635: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/0, changed state to down
*Dec   3 08:40:21.639: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet2/1, changed state to down
*Dec   3 08:40:21.915: %SYS-5-RESTART: System restarted --
Cisco IOS Software, 7200 Software (C7200-ADVENTERPRISEK9-M), Version 15.2(4)M7, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 25-Sep-14 10:36 by prod_rel_team
*Dec   3 08:40:21.999: %SNMP-5-COLDSTART: SNMP agent on host ISP is undergoing a cold start
*Dec   3 08:40:22.103: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
*Dec   3 08:40:22.107: %CRYPTO-6-GDOI_ON_OFF: GDOI is OFF
*Dec   3 08:40:23.099: %LINK-5-CHANGED: Interface FastEthernet2/0, changed state to administratively down
*Dec   3 08:40:23.235: %LINK-5-CHANGED: Interface FastEthernet2/1, changed state to administratively down
*Dec   3 08:40:31.651: %DHCP-6-ADDRESS_ASSIGN: Interface FastEthernet0/0 assigned DHCP address 192.168.25.147, mask 255.255.2
55.0, hostname ISP

ISP#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
ISP(config)#ex
% Ambiguous command:  "ex"
ISP(config)#end
ISP#
*Dec   3 08:41:22.775: %SYS-5-CONFIG_I: Configured from console by console
ISP#show ip inter bri
ISP#show ip inter brief
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.25.147  YES DHCP   up                    up
FastEthernet1/0            11.11.11.1      YES NVRAM  up                    up
FastEthernet1/1            22.22.22.1      YES NVRAM  up                    up
FastEthernet2/0            unassigned      YES NVRAM  administratively down down
FastEthernet2/1            unassigned      YES NVRAM  administratively down down
ISP#
```

Phase 2: Firewall Basic Configuration & Segmentation

Interfaces were configured and logically separated into Zones (LAN, WAN, DMZ) to ensure zero-trust security.

DHCP Services: Deployed on LAN interfaces to provide dynamic IP allocation for endpoints.

Outbound Policies: Created firewall rules (LAN_TO_INTERNET) allowing internal users to access the internet using Source NAT (SNAT) to hide internal IP addresses.

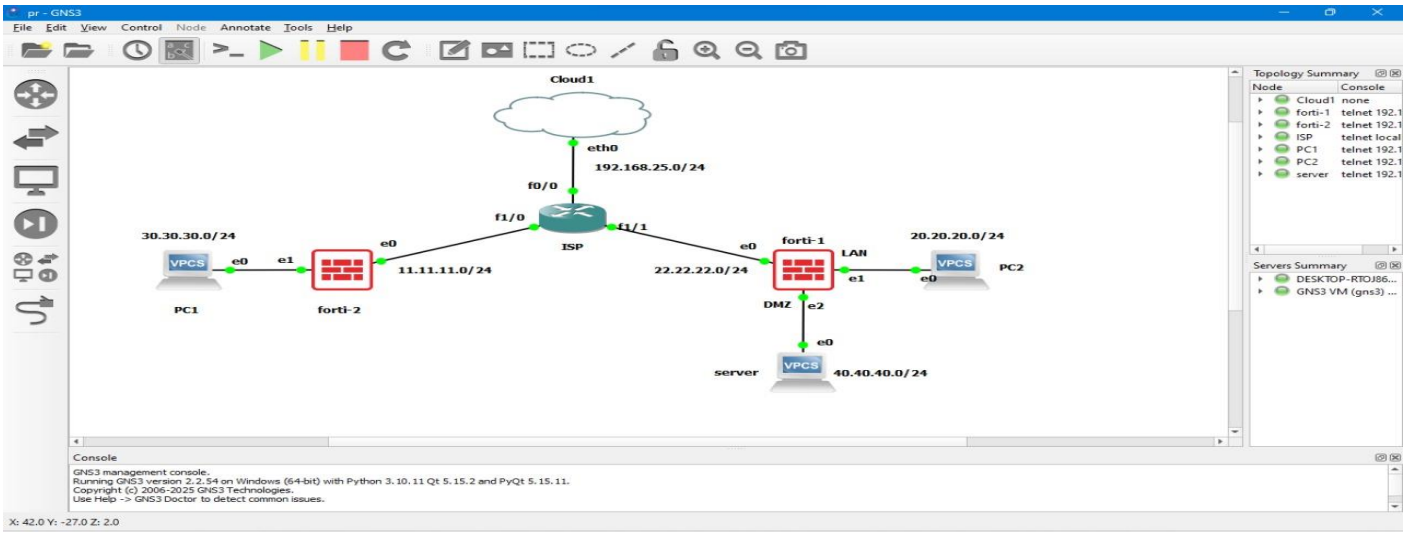


Phase 3: Secure Service Publishing (DNAT)

To enable external access to the internal Web Server (40.40.40.2) located in the DMZ without exposing the private network:

Virtual IP (VIP): Configured a Virtual IP object mapping the Public WAN IP (22.22.22.2) to the Private Server IP.

Inbound Policy: Implemented a specific firewall rule allowing traffic from the WAN to the DMZ only for specific services, utilizing the VIP object.



4. Testing & Validation

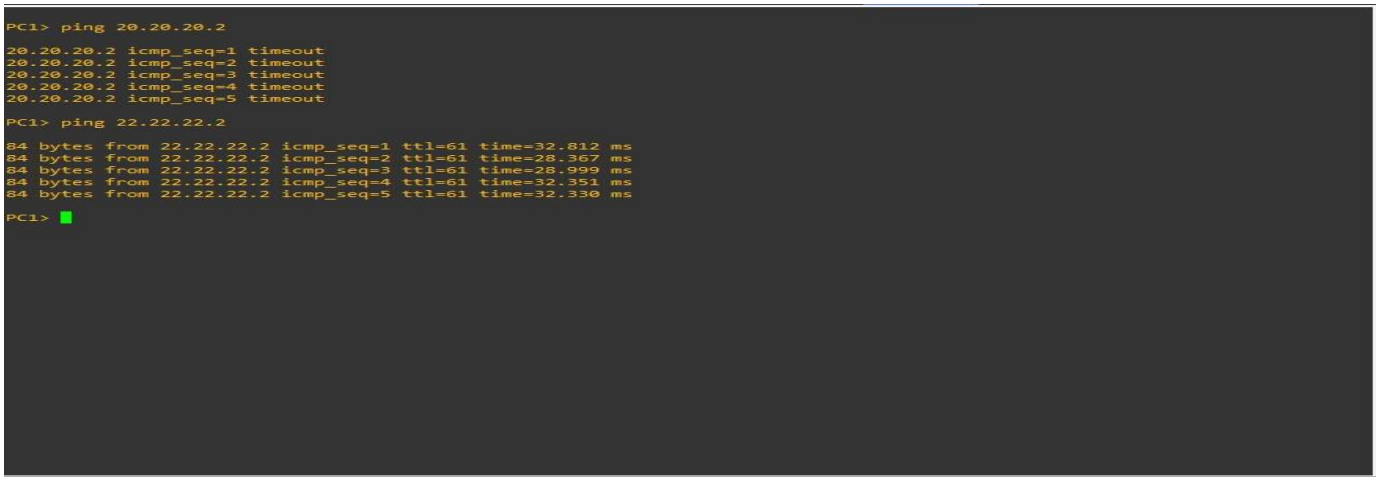
The network underwent rigorous testing to verify connectivity and security controls:

Test Case 1: Outbound Connectivity

Objective: Verify internal users can access the internet.

Result: The PC in the HQ LAN successfully pinged public DNS servers (8.8.8.8).

Status: Pass.

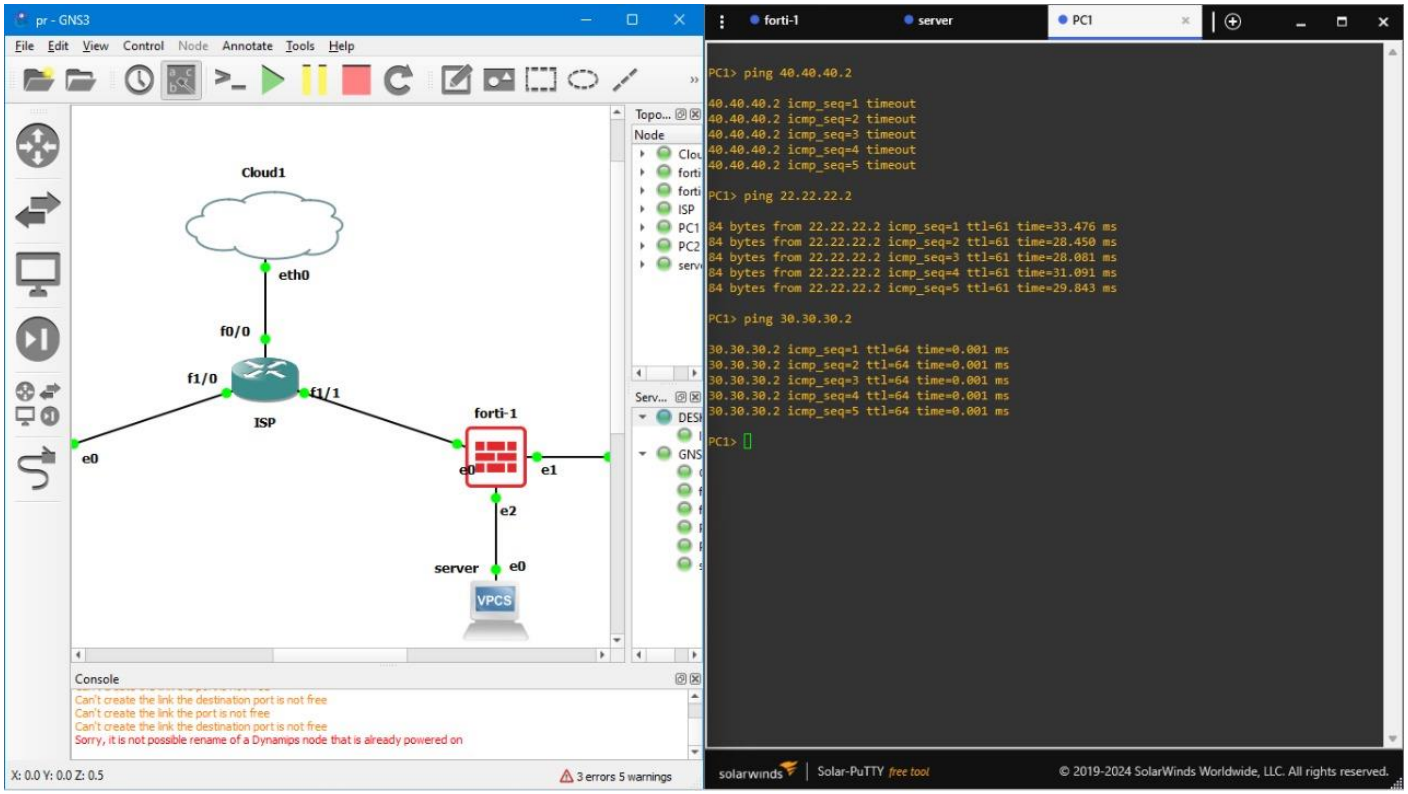


Test Case 2: Inbound Server Access (DNAT)

Objective: Verify external users can access the internal server via the Public IP.

Result: A PC from the external network successfully communicated with the server using the Public IP (22.22.22.2), while direct access to the private IP (40.40.40.2) was blocked by the firewall.

Status: Pass.



5. Conclusion

The project successfully demonstrates a secure, segmented, and functional enterprise network. The implementation of FortiGate firewalls ensures that internal assets are protected while maintaining necessary connectivity. The architecture is ready for future expansion, including Site-to-Site VPN tunneling and SD-WAN integration.