# Network Topology Report – Dual ISP Architecture Using GNS3

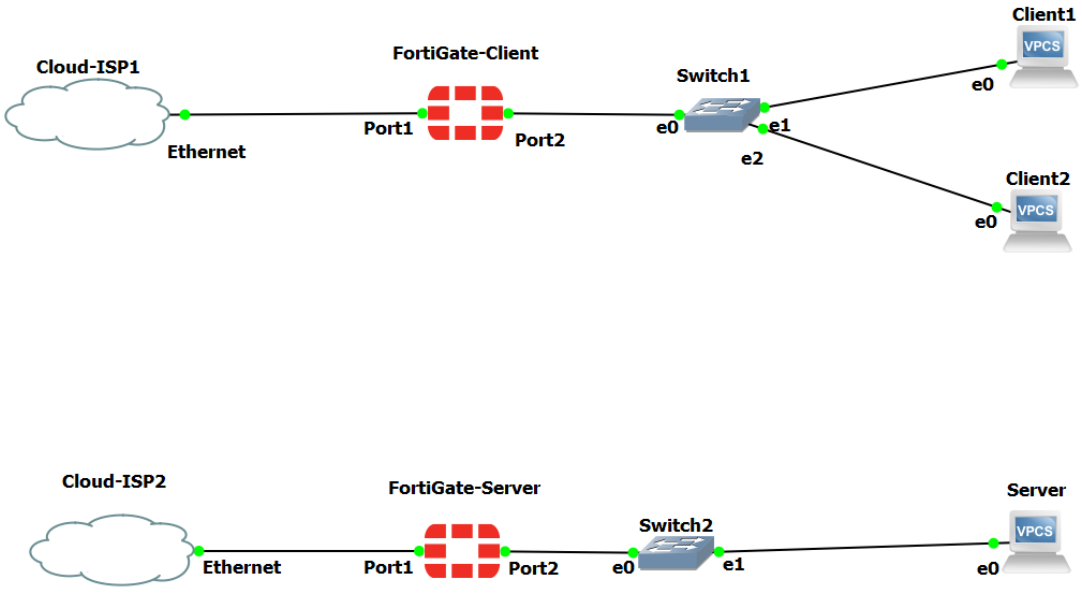
## 1. Overview

This report describes the design and implementation of a dual-ISP network topology using GNS3.

The setup includes two FortiGate firewalls, two Cloud nodes acting as separate ISPs, and two internal LAN segments for testing routing, NAT, and firewall policies.

The goal is to simulate a realistic environment where each FortiGate receives internet connectivity from a different ISP and provides secure access to internal devices.

## 2. Network Topology Diagram (Conceptual)



## 3. Components

### 3.1 FortiGate 1 (FG1)

- WAN Interface: Connected to Cloud 1 (ISP 1)

- LAN Interface: 10.0.1.1/24

- Purpose: Provide internet access to PC1 through NAT and security policies.

### 3.2 FortiGate 2 (FG2)

- WAN Interface: Connected to Cloud 2 (ISP 2)

- LAN Interface: 10.0.2.1/24

- Purpose: Provide internet access to a server through NAT and allow testing of DNAT/port forwarding.

### 3.3 Cloud Nodes (ISP Simulation)

- Cloud 1: Represents ISP 1 (via host network adapter 1 or virtual adapter)

- Cloud 2: Represents ISP 2 (via host network adapter 2 or loopback adapter)

- Both Clouds perform NAT, giving the FortiGate WAN interfaces real internet access.

### 3.4 End Devices

- PC (LAN1): 10.0.1.10/24

- Server (LAN2): 10.0.2.20/24 (HTTP/SSH for DNAT testing)

## 4. Configuration Summary

### 4.1 WAN Configuration on Both FortiGates

- Interface mode: DHCP Client

- Receives public NATed IP from the Cloud node

- Default route created automatically

### 4.2 LAN Configuration

**FG1 LAN:**

- IP: 10.0.1.1/24

- DHCP Server (optional)

### FG2 LAN:

- IP: 10.0.2.1/24

- DHCP Server (optional)

### 4.3 Security Policies

For both firewalls:

### 1. LAN → WAN Policy

- Allow outbound traffic

- Enable NAT (SNAT)

### 2. (Optional) WAN → LAN DNAT Policy (FG2)

- Configure Virtual IP (VIP) to publish Server services

- Allow external access to HTTP/SSH for testing

## 5. NAT Operation

### SNAT

- Internal devices use firewall's WAN IP to access the Internet

- Automatically applied through outgoing policies

### DNAT (on FG2)

- VIP translates WAN IP → Server private IP

- Used for testing:

  - Web server (TCP 80)

  - SSH server (TCP 22)

## 6. Testing Procedures

### 6.1 Connectivity Tests

- Ping from PC1 → 8.8.8.8

- Ping from Server → 8.8.8.8

- Verify routing table on both FortiGates

- Check WAN status receives DHCP address

### 6.2 DNAT Tests (FG2)

- From external network, attempt:
  - "http://<FG2-WAN-IP>"
  - "ssh <FG2-WAN-IP>"

### 6.3 Logs Verification

- Traffic logs on both firewalls
- NAT translations
- Firewall policy hits

## 7. Objectives Achieved

- Simulated two independent ISPs using dual Cloud nodes
- Deployed two FortiGate appliances in parallel
- Configured NAT, routing, firewall rules, and VIPs
- Validated outbound/inbound connectivity
- Created a realistic, multi-ISP environment for training and testing

## 8. Conclusion

The dual-ISP GNS3 topology successfully mimics a real-world network with separate internet providers, isolated LANs, and full firewall configuration.

This setup can be extended later for:

- SD-WAN
- Load balancing
- Failover
- Advanced security policies
- Red-team/blue-team simulations

It provides a strong foundation for practical network and security training.