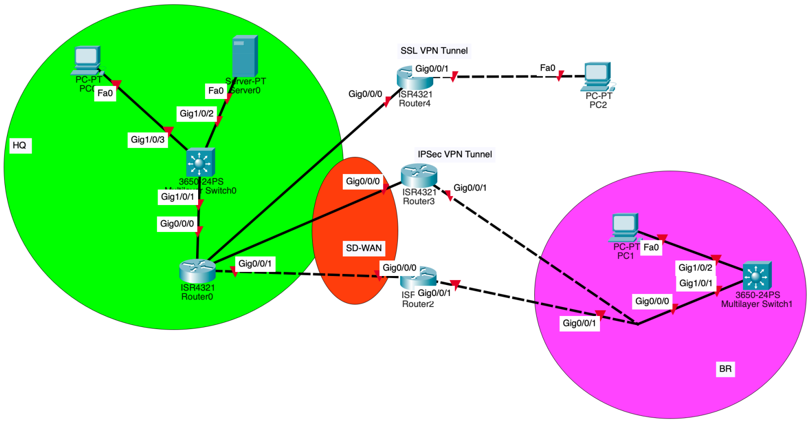
# VPN Project Topology Report

This report provides a complete and highly detailed explanation of the VPN topology. It covers all components including FortiGate firewalls, WAN routers, LANs, management networks, remote access, addressing schemes, routing, VPNs, policies, and traffic flows. The goal is to fully document the design as if for a professional deployment.

## 1. High-Level Overview



The topology has four main elements:
1. Headquarters (HQ): Main office with FortiGate, LAN, web server, and management network.
2. Branch Office (BR): Remote office with its own FortiGate, LAN, and management network.
3. WAN/ISP Routers: Devices simulating multiple ISPs and interconnections.
4. Remote Users: Connect via SSL-VPN into HQ securely.

Key features:
- Site-to-Site IPsec VPN: Connects HQ and Branch LANs.
- SSL-VPN: Allows remote users to securely access HQ LAN.
- SD-WAN: HQ uses two ISPs simultaneously with load-balancing and failover.
- Centralized Security: All traffic passes through FortiGates with policies and inspection.

## 2. Addressing Scheme

The design uses the private supernet 10.20.0.0/16, split using VLSM:

- HQ LAN: 10.20.3.0/24
- Branch LAN: 10.20.6.0/24
- HQ Mgmt: 10.20.99.0/28
- Branch Mgmt: 10.20.100.0/28
- SSL-VPN Pool: 10.20.200.0/28

- HQ–ISP1 (P2P): 10.20.254.0/30
- HQ–ISP2 (P2P): 10.20.254.4/30
- R3–ISP1 (P2P): 10.20.254.8/30
- R3–ISP2 (P2P): 10.20.254.12/30
- Branch–R3 (P2P): 10.20.254.16/30
- HQ–R4 (SSL Edge P2P): 10.20.254.20/30

## 3. Headquarters FortiGate

Role: Central firewall and VPN concentrator.

Interfaces:
- port1 (Mgmt): 10.20.99.1/28 – Admin access.
- port3 (LAN): 10.20.3.1/24 – Gateway for HQ LAN devices and servers.
- port5 (SSL Edge): 10.20.254.21/30 – Entry point for SSL-VPN.
- port4 (ISP1): 10.20.254.1/30 – Connected to R10 (ISP1).
- port2 (ISP2): 10.20.254.5/30 – Connected to R11 (ISP2).

Functions:
- Provides SD-WAN across port4 and port2.
- Hosts SSL-VPN service on port5 (TCP 10443).
- Establishes IPsec tunnel to Branch LAN.
- Defines static routes and firewall policies.

## 4. Branch FortiGate

Role: Protects Branch network and establishes VPN to HQ.

Interfaces:
- port1 (Mgmt): 10.20.100.1/28 – Admin access.
- port2 (LAN): 10.20.6.1/24 – Gateway for Branch LAN devices.
- port3 (WAN): 10.20.254.17/30 – Connected to R3.

Functions:
- Default route points to R3 (10.20.254.18).
- IPsec tunnel to HQ FortiGate.
- Security policies for Branch LAN ↔ HQ LAN communication.

## 5. WAN/ISP Routers

R3 (Core Router):
- Connects to Branch (10.20.254.18).
- Connects to R10 on 10.20.254.9/30 and R11 on 10.20.254.13/30.

R10 (ISP1 Router):
- Connects to HQ FortiGate (10.20.254.2).
- Connects to R3 (10.20.254.10).

R11 (ISP2 Router):
- Connects to HQ FortiGate (10.20.254.6).
- Connects to R3 (10.20.254.14).

R4 (SSL Edge Router):
- Connects to HQ FortiGate port5 (10.20.254.22).
- Provides edge connectivity for SSL-VPN services.

## 6. Endpoints and Services

- HQ Web Server: Inside 10.20.3.0/24, reachable from HQ, Branch, and SSL-VPN users.
- HQ Management PC: On 10.20.99.0/28 for FortiGate admin.
- Branch Management PC: On 10.20.100.0/28 for Branch FortiGate admin.
- Remote User: Connects via SSL-VPN and receives IP in 10.20.200.0/28.

## 7. VPN Configurations

SSL-VPN:
- Runs on port5 of HQ FortiGate.
- User pool: 10.20.200.0/28.
- Policies allow SSL-VPN users to access HQ LAN.

IPsec VPN:
- HQ–Branch tunnel.
- Phase-2 Selectors: HQ LAN (10.20.3.0/24) ↔ Branch LAN (10.20.6.0/24).
- Policies allow full LAN ↔ LAN traffic.
- Encryption, authentication, and key exchange parameters defined per best practices.

## 8. SD-WAN

The HQ FortiGate groups ISP1 and ISP2 into an SD-WAN interface:
- Members: port4 (10.20.254.1/30) and port2 (10.20.254.5/30).
- SLA Targets: e.g., 8.8.8.8.
- Strategy: Maximize Bandwidth with failover.
- Benefits: Resilient Internet connectivity, bandwidth aggregation, automatic failover.

## 9. Security Policies

HQ FortiGate:

- SSL-VPN → HQ LAN: allow, NAT off.
- HQ LAN ↔ Branch LAN via IPsec: allow, NAT off.

Branch FortiGate:

- Branch LAN ↔ HQ LAN via IPsec: allow, NAT off.

Implicit deny ensures all other traffic is blocked by default.

## 10. Traffic Flows

- Remote User: Connects via SSL-VPN, obtains IP in 10.20.200.0/28, reaches HQ LAN.
- HQ ↔ Branch: IPsec tunnel allows seamless communication between LANs.
- HQ → Internet: Uses SD-WAN to select optimal ISP path.
- Branch → Internet: Default route via R3.
- All flows inspected and enforced by FortiGate policies.

## 11. Verification and Testing

- Ping between HQ LAN (10.20.3.0/24) and Branch LAN (10.20.6.0/24).
- Connect SSL-VPN client and verify access to HQ Web Server.
- Simulate ISP failure to test SD-WAN failover.
- Review FortiGate IPsec Monitor and SSL-VPN logs.
- Verify management access from HQ and Branch PCs.