رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Implementing a Secure Multi-Branch Office Network

DEPI Graduation Project

Fortinet Cybersecurity Engineer (ONL3_ISS8_S2)

Supervised By:

Eng. Alhussieny Ali

Team Members

Abdulrahman mohamed kamel

Mustafa Abdelhady Mohammed

Ahmed Zakaria Ismail

Abdelwahab Nabil Zakaria

Abdelrhman Badr metwaly

Mustafa Hesham Mustafa


Agenda
Project Scenario
Architecture
VLANs
DMZ
Firewall
NAT
ISP & VPN

Scenario

A **Company** With A Main Office And Branch Office.

Company Requires Reliable Connectivity, Secure Communication, And Internet Access.

The **Company** Also Needs Secure And Protection Against Cyber Threats.

Requirements

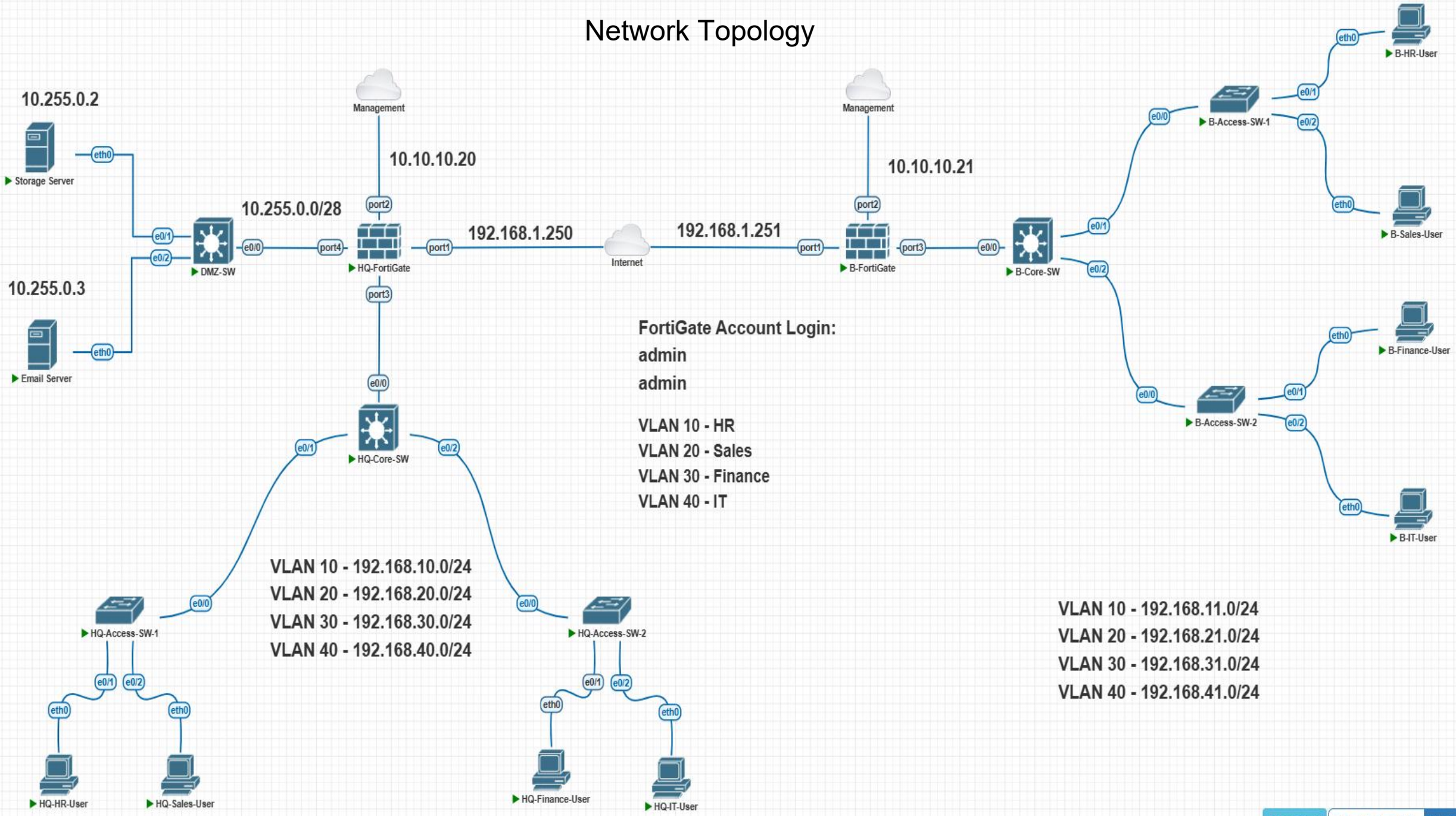
Network
Segmentation For
Different Departments

Secure
Site-to-site VPNs.

NAT
traffic flow across network boundaries.

Network Architecture

Network Topology



VLANs

VLAN design demonstrates a solid understanding of network segmentation and access-control principles. The use of separate VLANs for HR, Sales, Finance, and IT across both HQ and Branch introduces a logical and highly secure structure. This segmentation minimizes broadcast domains, improves performance, and enforces separation between departments handling different types of data.


DMZ
Demilitarized Zone

Servers In the DMZ

Email Server

Manages and filters all inbound and outbound company emails.

Storage Server

central vault of the organization where critical data is stored, protected, and accessed on demand.

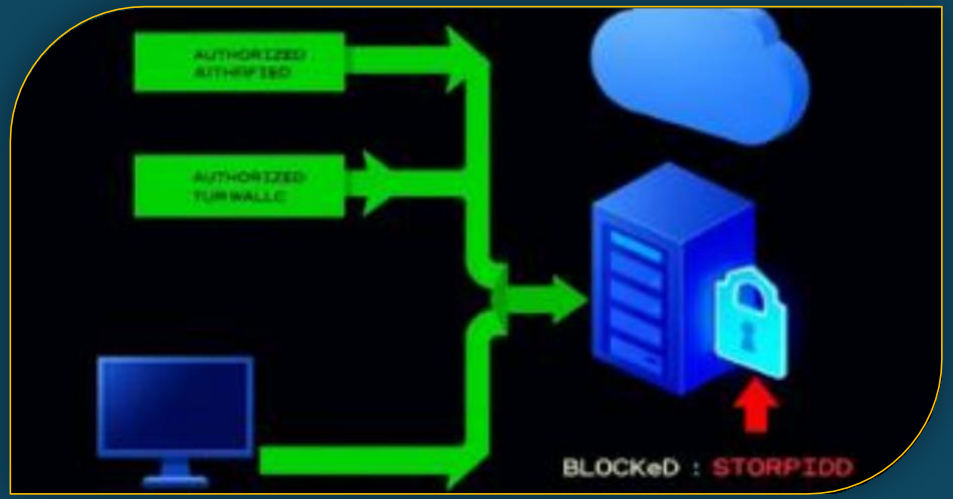
Firewall

Policies & Rules → Rounting Arch. → NAT

Firewall Security Polices

Firewall policy

act as the rule-based traffic controllers of the network, deciding what enters, what leaves, and what stays out .



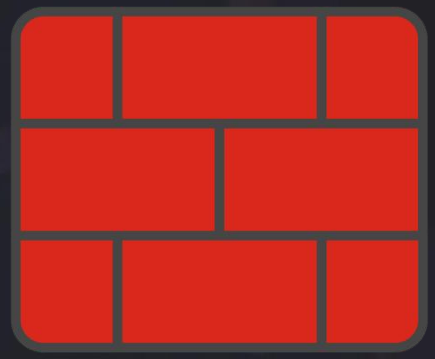
Authorized Traffic Only

Only essential services and approved directions are allowed per security requirements.

Firewall Security Rules

The FortiGate operates as:

- Primary security firewall.
- DHCP server for VLANs.
- Routing gateway for inter-VLAN communication.
- NAT device for internet access.
- Security inspection point (AV, IPS, Web Filter).



Routing Architecture

Default Route Propagation

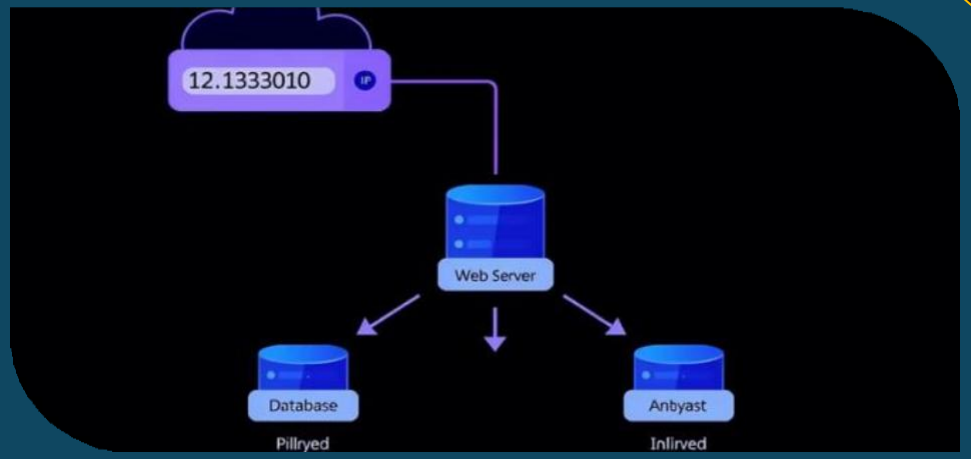
Routing is performed by FortiGate:

- Static routes for upstream gateways.
- Default route → ISP router.
- Optional routes to remote sites.

Ensures Seamless Connectivity

Maintains consistent and secure access to internet resources across the network.

NAT



- The **HQ** FortiGate firewall utilizes **Dynamic NAT** configuration specifically for the IT department (VLAN 40) to access the internet.

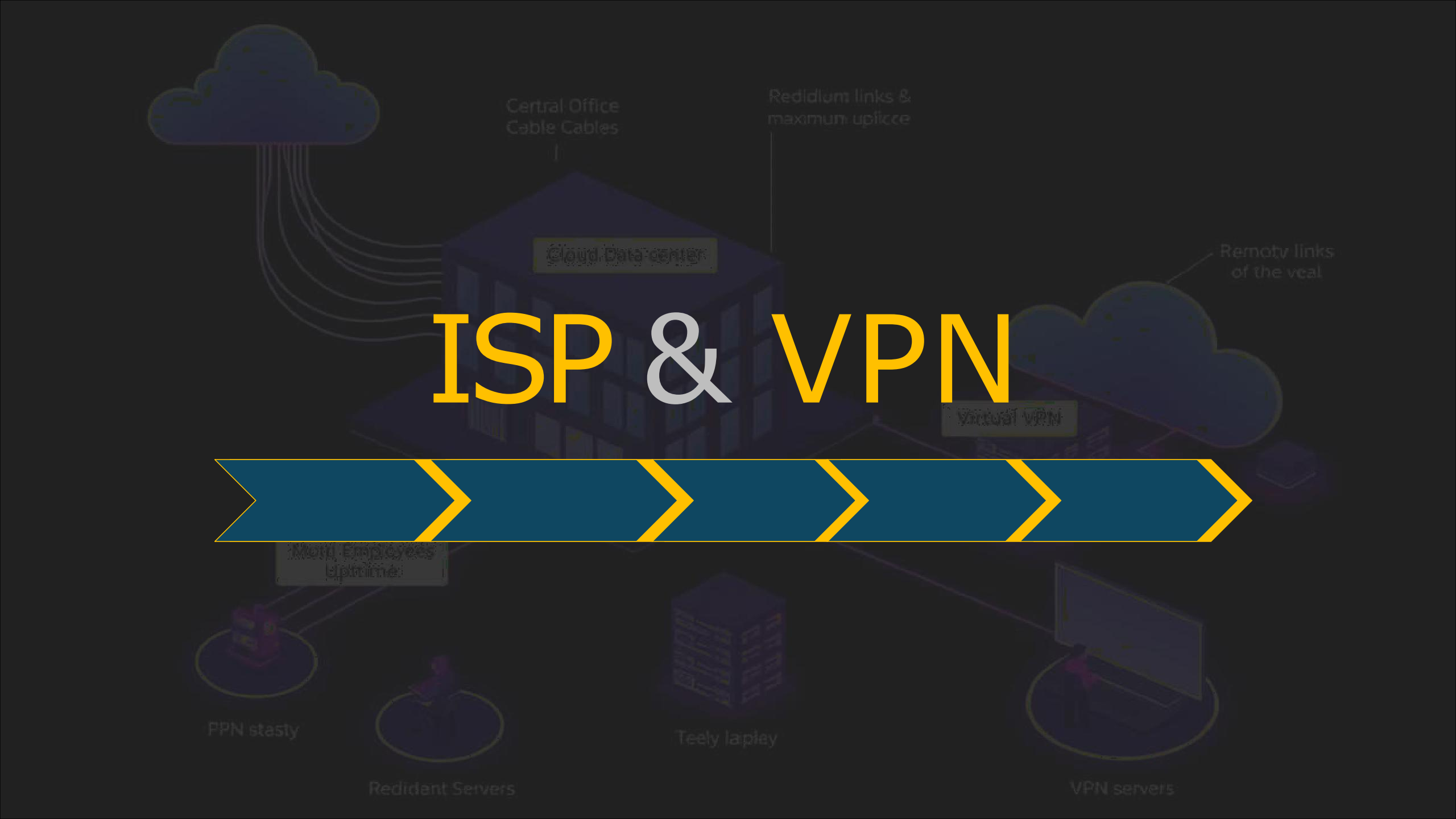
- Policy Name: IT TO internet .
- Source: IT (VLAN 40) .
- Destination: WAN (port1) .

- **NAT** Type: **Dynamic** IP NAT with "Overload" (Port Address Translation) enabled .

- IP Pool Range: The configuration uses a specific IP pool named internet access ranging from 192.168.192.100 to 192.168.192.150 .

- Similar to the HQ configuration, the B Branch FortiGate implements NAT to allow internet access for its IT department.
- Source: IT (VLAN 40) .
  Destination: WAN (port1) .

- NAT Type: Dynamic IP NAT with "Overload" enabled .
- IP Pool Range: The branch utilizes a distinct IP pool range from 192.168.192.151 to 192.168.192.200 .


Central Office
Cable Cables
Redidium links &
maximun upiicce
Remoty links
of the veal
PPN stasty
Teely lapley
VPN servers

ISP & VPN

VPN Setup with IPSec

Branch-to-HQ Security

B Branch connect securely to the main HQ.

Restricted Communication

IPsec Phase 2 Selectors: The tunnel is configured to allow specific private subnets to communicate across the link (e.g., HQ VLAN 10 to Branch VLAN 10)

Data Encryption

Critical data and shared servers are encrypted for safety.

IPSec VPN Data Protection

Secure Communication

Ensuring safe data exchange between HQ and branch offices

Data Encryption

Protecting confidentiality and integrity of network data

- **VPN (IPsec Site-to-Site Tunnel) :**

The network uses an IPsec Site-to-Site VPN to securely connect the Headquarters (HQ) and Branch internal networks.

- **Tunnel Endpoints :**

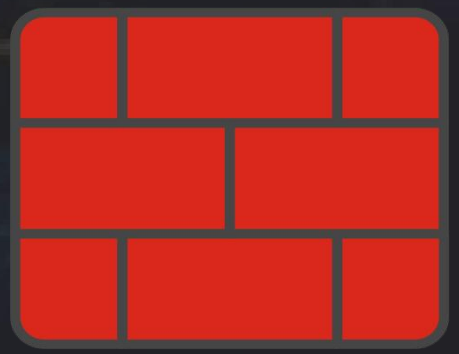
The VPN tunnels are established between the WAN interfaces of the two FortiGate firewalls:

Location	VPN Tunnel Name	FortiGate Public IP	Outgoing Interface
HQ FortiGate	B_VPN (Remote)	192.168.192.250	WAN (port1)
Branch FortiGate	HQ_VPN (Remote)	192.168.192.251	WAN (port1)

ISP &WAN Interface and Default Routing

The port1 interface on both FortiGate firewalls serves as the connection point to the WAN (ISP).

Location	Interface	IP Address/Mask	Default Route Next-Hop
HQ FortiGate	port1 (WAN)	192.168.192.250/24	192.168.192.2 (ISP Gateway)
Branch FortiGate	port1 (WAN)	192.168.192.251/24	192.168.192.2 (ISP Gateway)



ISP Network Connections

Branch Connectivity

Each branch is linked through the ISP with a fixed gateway.

Reliable Network

ISP infrastructure ensures seamless communication across branches.


Thank You :)