Multi-Branch Enterprise Network Project Documentation (I10 & D)

1. Introduction

1.1 Document Purpose

This document aims to provide comprehensive technical documentation for the design and implementation of the network infrastructure shown in the attached diagram. The documentation covers addressing details, network segmentation (VLANs), layered design, and inter-branch connectivity, with a focus on key security components.

1.2 Key Features

1. **Secure Site-to-Site VPN:** Secure connectivity between the main branch (I10) and the remote branch (D) is established over the Internet using two FortiGate devices, indicating the use of a VPN tunnel (likely IPsec) to ensure data confidentiality and integrity.
2. **Network Segmentation using VLANs:** The internal network in both branches is divided into Virtual Local Area Networks (VLANs) to enhance security, improve traffic management, and isolate departments.
3. **Demilitarized Zone (DMZ):** A DMZ is allocated in the main branch (I10) to host public servers (Storage Server, Email Server), isolating them from the internal network.
4. **Hierarchical Design:** The design follows a layered model (Core/Distribution/Access) to ensure scalability and improve performance.

1.3 Branches and Key Devices Table

Branch	Role	Key Security Devices	Management Network
I10	Main Branch / HQ	FortiGate (192.168.1.250)	10.10.10.20
D	Remote Branch	FortiGate (192.168.1.251)	10.10.10.21

---

2. Network Architecture

2.1 Topology Description

The network consists of two main branches connected over the Internet, with the two FortiGate devices acting as the main security gateways.

- **I10 Branch (Main):**
  - The FortiGate connects to the DMZ-GW, which in turn connects to the Storage and Email servers.
  - The FortiGate also connects to the I10-Core-GW, which distributes connectivity to the access switches (I10-Access-GW-1 and I10-Access-GW-2) serving end-users via VLANs.
- **D Branch (Remote):**
  - The FortiGate connects to the D-Core-GW, which distributes connectivity to the access switches (D-Access-GW-1 and D-Access-GW-2) serving end-users via VLANs.
- **Inter-Branch Connectivity:** This is established over the Internet between the two FortiGate interfaces (192.168.1.250 and 192.168.1.251), indicating a Site-to-Site VPN tunnel.

2.2 Network Diagram

(The original diagram is attached as part of the documentation)

---

3. IP Scheme and Network Segmentation (VLANs)

3.1 Virtual Network Segmentation (VLANs)

The network in both branches is divided into four functionally identical VLANs, but with different IP subnets to ensure proper routing.

VLAN ID	Department Name	I10 Branch Network (Main)	D Branch Network (Remote)
10	HR (Human Resources)	192.168.10.0/24	192.168.11.0/24
20	Sales	192.168.20.0/24	192.168.21.0/24

VLAN ID	Department Name	I10 Branch Network (Main)	D Branch Network (Remote)
30	Finance	192.168.30.0/24	192.168.31.0/24
40	IT (Information Technology)	192.168.40.0/24	192.168.41.0/24

3.2 Main Addressing Scheme

Zone	Network	Description
DMZ	10.255.0.0/28	Isolated server network in the I10 Branch.
Storage Server	10.255.0.2	IP address for the Storage Server in the DMZ.
Email Server	10.255.0.3	IP address for the Email Server in the DMZ.
Internet (I10)	192.168.1.250	External interface IP for the FortiGate in the I10 Branch.
Internet (D)	192.168.1.251	External interface IP for the FortiGate in the D Branch.
Management (I10)	10.10.10.20	IP address for the management interface in the I10 Branch.
Management (D)	10.10.10.21	IP address for the management interface in the D Branch.

---

4. Design and Configuration Notes

4.1 Inter-Branch Connectivity (VPN)

- **Technology:** Site-to-Site VPN (assumed IPsec) between the two FortiGate devices.
- **Objective:** To enable secure and encrypted communication between the internal networks of both branches (192.168.x.0/24 networks in I10 and 192.168.x.0/24 networks in D).
- **Endpoints:**
    - I10 Branch: 192.168.1.250
    - D Branch: 192.168.1.251

4.2 FortiGate Devices (Firewall)

The FortiGate devices function as the central firewall and VPN gateway.

- **Default Login Credentials:**
  - Username: `admin`
  - Password: `admin`
  - **Security Note:** The default login credentials must be changed immediately to a strong password.

4.3 DMZ Zone

- **Network:** 10.255.0.0/28.
- **Devices:** Storage Server (10.255.0.2) and Email Server (10.255.0.3).
- **Security Policies:** Strict firewall policies must be applied on the FortiGate to restrict access to the DMZ from the Internet, allowing only necessary protocols (e.g., HTTP/HTTPS, SMTP, etc.). Traffic from the DMZ to the internal network (VLANs) should also be restricted.

4.4 Inter-VLAN Routing

Routing between different VLAN subnets within each branch is handled by the Core-GW devices (I10-Core-GW and D-Core-GW), which act as the Default Gateways for each VLAN.

---

5. Security Policies

5.1 Firewall Policies

Firewall policies must be configured on the FortiGate to regulate traffic:

Source	Destination	Service	Action	Notes
Internet	**DMZ**	Public Services (Web, Mail)	Allow	Ports must be precisely defined (e.g., 80, 443, 25).
Internet	**Internal Network (VLANs)**	Any	Deny	Block all unwanted inbound connections.

Source	Destination	Service	Action	Notes
Internal Network (VLANs)	**Internet**	Any	Allow	With NAT (Network Address Translation) applied.
Internal Network (VLANs)	**DMZ**	Any	Allow	For internal access to servers.
I10 Internal Networks	**D Internal Networks**	Any	Allow	Via VPN tunnel.
D Internal Networks	**I10 Internal Networks**	Any	Allow	Via VPN tunnel.

5.2 VLAN Security

- **VLAN Isolation:** Ensure that Inter-VLAN routing occurs only through the Core-GW to enforce security policies.
- **Access Ports:** Each access port on the Access-GW switches must be assigned to a specific VLAN (10, 20, 30, 40) and Layer 2 security features like Port Security should be applied.

---

6. Backup and Maintenance Strategy

6.1 Configuration Backup

- **Devices:** FortiGate, Core-GWs, Access-GWs.
- **Procedure:** A periodic backup of the configurations for all key devices, especially the FortiGate, should be scheduled and stored in a secure, off-network location.

6.2 Maintenance and Troubleshooting

- **Management:** Devices are accessed via the Management Network (10.10.10.x) using the dedicated IP addresses (10.10.10.20 and 10.10.10.21).
- **Updates:** Firmware updates must be applied regularly to the FortiGate devices to maintain the highest level of security.
- **Monitoring:** Use protocols like SNMP and Syslog to monitor network performance and log security events.