FortiGate Multi-Site Network Deployment with SD-WAN and HA

1. Project Overview

This repository documents a comprehensive, multi-site network infrastructure built using FortiGate virtual appliances (running FortiOS 7.0.5). The deployment is designed to showcase high availability (HA) at the Headquarters (HQ) and redundant connectivity across two Wide Area Network (WAN) links using Fortinet's **SD-WAN** feature to a remote German (DE) branch. A separate Data Center (DC) firewall manages internal transit traffic between corporate and demilitarized zone (DMZ) segments.

The primary goals of this project are:

- **High Availability (HA):** Implementing Active-Active HA at the HQ location for maximum uptime.
- **SD-WAN:** Utilizing dual WAN links for resilient, performance-driven IPsec VPN tunnels to the remote site.
- **Secure Segmentation:** Defining multiple VLANs and security zones (LAN, DMZ, Transit) with granular firewall policies.
- **Routing & Connectivity:** Establishing secure IPsec VPN tunnels (site-to-site) between HQ and the DE branch.

2. Network Topology

The network layout consists of four FortiGate appliances interconnecting three main sites: Headquarters (HQ), Data Center (DC), and a remote German Branch (FG-DE).

Key Network Segments & IP Schemes:

Network	Site	Subnet/VLAN	Purpose
Transit WAN 1	HQ, DE, DC	192.168.1.0/24	Primary external facing link (Simulated Internet)
Transit WAN 2	HQ, DE	192.168.75.0/24	Secondary external facing link (SD-WAN redundancy)

HQ LAN	HQ	10.1.1.0/24 (VLAN10)	User network
HQ LAN 2	HQ	10.1.2.0/24 (VLAN20)	Guest/Secondary User Network
DC DMZ	DC	10.1.3.0/24 (VLAN30)	Server/DMZ segment
DC DMZ 2	DC	10.1.4.0/24 (VLAN40)	Secondary Server/DMZ segment
DE Branch LAN	FG-DE	11.0.0.0/24	Remote Office Network

3. FortiGate Configurations Summary

The configurations provided (DC-FG.conf, FG-DE.conf, HQ-Firewall2.conf) define the core functionality of the security infrastructure.

A. Headquarters Firewall (HA Pair) - HQ-Firewall1/HQ-Firewall2

The HQ firewall uses an Active-Active (A-A) High Availability configuration for redundancy and load sharing.

Setting	**HQ-Firewall1 (Primary - Hypothetical)**	**HQ-Firewall2 (Secondary - Provided)**
Hostname	HQ-Firewall1	HQ-Firewall2
HA Group Name	HQ	HQ
HA Mode	Active-Active	Active-Active
Device Priority	150 (Primary)	100 (Secondary)
Heartbeat Interface	port3 (HA synchronization/heartbeat)	port3 (HA synchronization/heartbeat)
Interface HA Mgmt IP	port6 (Management IP setup for failover)	port6 (Management IP setup for failover)

SD-WAN Uplinks	port4 (192.168.1.50), port5 (192.168.75.3)	port4 (192.168.1.50), port5 (192.168.75.3)

Key Feature Highlights:

- **SD-WAN Configuration:** Traffic destined for the German Branch (11.0.0.0/24) is steered over the VPN links (VPN-To-DE-Wan1, VPN-To-DE-Wan2) as defined in the SD-WAN policies.
- **SD-WAN SLA:** Implicit use of Health Checks (Default_DNS, Default_Google Search, etc.) to monitor uplink performance.
- **Link Aggregation (LAG):** The internal LAN link (AggreLAN on ports 1 and 2) increases bandwidth and redundancy to the corporate switch infrastructure.
- **VLANs:** Internal network traffic is segmented across VLAN 10 and 20. Traffic transiting to the DC is routed through Transit VLANs 30 and 40.

B. German Branch Firewall - FG-DE.conf

The remote branch primarily acts as an endpoint for the SD-WAN resilient VPN connection back to HQ.

- **Local LAN:** port4 is the internal LAN interface (11.0.0.1/24).
- **SD-WAN SD-WAN SD-WAN Uplinks:** port1 (192.168.1.100), port5 (192.168.75.11).
- **IPsec VPN Tunnels:** Dual IPsec Phase 1/2 configurations (VPN-To-EG and VPNtoEG-wan2) anchor the SD-WAN members.
- **Static Routes:** Static routes point traffic for HQ networks (10.1.1.0/24, 10.1.2.0/24, etc.) into the SD-WAN tunnel zone (VPN-EG), allowing SD-WAN logic to select the best tunnel path.

C. Data Center Firewall - DC-FG.conf

The Data Center firewall manages segmentation between its WAN access (port2) and internal segmented DMZ/Transit networks (port1 with VLAN sub-interfaces).

- **WAN Uplink:** port2 (192.168.1.55/24).
- **Internal Interfaces:** VLAN30 (10.1.3.1), VLAN40 (10.1.4.1), Transit-V10 (10.1.1.99), TransitV20 (10.1.2.99).
- **Internal Routing:** Static routes push traffic destined for HQ/DE networks via the respective transit VLAN gateways (10.1.1.1, 10.1.2.1, etc.).

4. File Manifest

Filename	Description
README.md	This overview document.

HQ-Firewall2_7-0_0304_202505061929.conf	Original configuration of the secondary HQ FortiGate.
HQ-Firewall1_HA_Primary_Config_Template.conf	Template configuration for the primary HQ FortiGate (HA Master).
FG-DE_7-0_0304_202505061932.conf	Configuration for the German Branch FortiGate.
DC-FG_7-0_0304_202505061928.conf	Configuration for the Data Center FortiGate.
HA_Deployment_Notes.md	Detailed notes on HA and failover for the HQ cluster.
Cisco_Switch_Configuration_Template.txt	Template for the expected Cisco switch configuration supporting the VLANs and LAG.