CCIE Security v6.1: The Unified Ultimate Lab

1. Lab Strategy and Architectural Scope

This lab scenario simulates a massive enterprise migration from legacy VPNs to a highly resilient, SD-WAN-ready architecture. You are tasked with managing three distinct layers of complexity simultaneously:

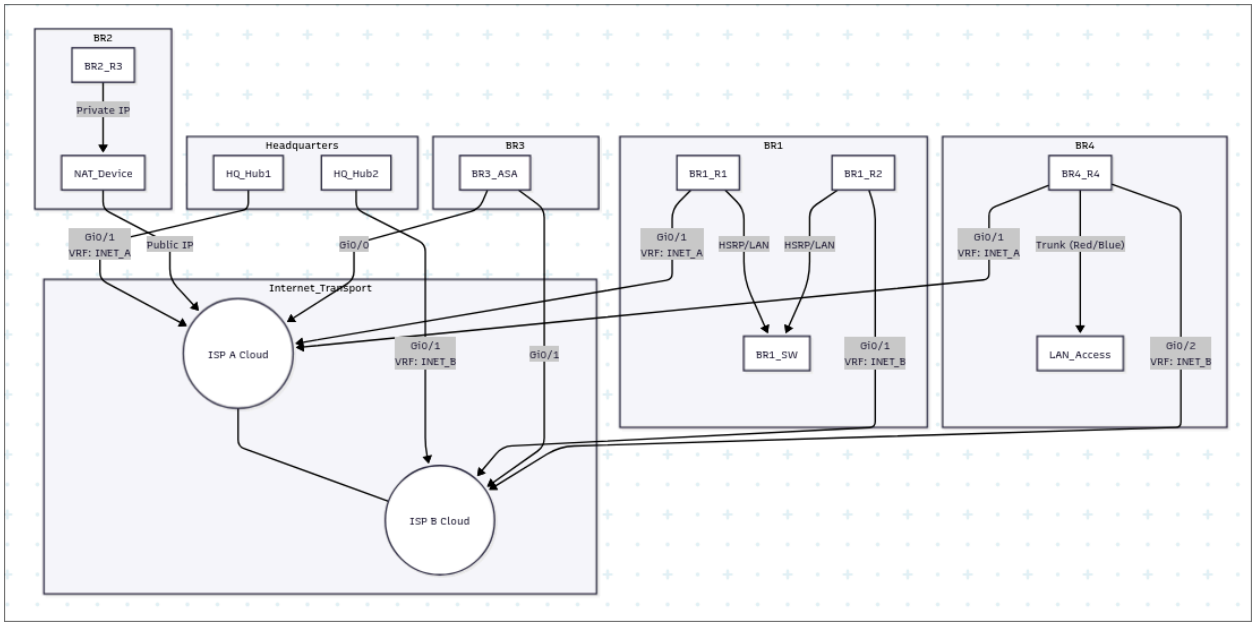
1. **Transport Redundancy:** Dual ISP Clouds with Dual Front Door VRFs.
2. **Service Segmentation:** Multi-Tenant (Red/Blue) traffic isolation using VRF-Lite.
3. **Protocol Diversity:** Hybrid Routing (BGP & EIGRP) and Advanced HA (ECMP vs. Clustering).

Key Design Constraints:

- **Dual Cloud Transport:** Two distinct clouds (**ISP A** and **ISP B**) with separate Front Door VRFs.
- **Multi-Tenancy: Branch 4** houses two tenants (**Red** & **Blue**) isolated across the WAN.
- **Routing Strategy:**
    - **VRF RED (Corporate):** Uses **iBGP** (Supports ASA & Routers).
    - **VRF BLUE (Tenant):** Uses **EIGRP** (Routers Only).
- **Availability Strategy:**
    - **Dual Uplink Sites (BR4):** Must use **ECMP** (Active/Active).
    - **Single Uplink Sites (BR2):** Must use **Failover/Clustering** (Active/Standby).

---

2. Master Topology Diagram



3. Phase 0: Infrastructure & Segmentation

Goal: Establish the "Dual FVRF" transport layer and "Multi-VRF" service layer.

3.0 Basic Connectivity

- **Objective 1:** On all devices, configure basic IP addressing
- **Objective 2:** On all devices, configure BGP for routing across INET_A and INET_B
- **Objective 3:** On **Branch 2**, configure basic PAT
- **Objective 4:** On **Branch 3**, configure HSRP

3.1 Dual Front Door VRF (FVRF)

- **Objective 1:** On **Branch 4**, configure VRF INET_A (for Gi0/1) and VRF INET_B (for Gi0/2).
- **Objective 2:** Configure separate default routes in each VRF pointing to the respective ISP gateways.
- **Objective 3:** Ensure BR4 can ping HQ-Hub1 *only* via INET_A and HQ-Hub2 *only* via INET_B.

3.2 Service Layer Segmentation

- **Objective 1:** Configure VRF_RED and VRF_BLUE on HQ and BR4.
- **Objective 2:** BR1, BR2, and BR3 participate only in VRF_RED (Corporate traffic).

3.3 Public Key Infrastructure

- **Objective 1:** Configure HQ-Hub1 as the Root CA.
- **Objective 2:** Enroll all spokes.
    - *Note:* Ensure BR4 enrolls using a source interface reachable by the CA, or enrolls twice if the CA is not reachable via both clouds.

---

4. Phase 1: Legacy IPsec (Dual Cloud Awareness)

Goal: Establish static tunnels to verify basic connectivity and test explicit redundancy protocols.

4.1 Hub-to-Branch 1 (Split HA)

- **Objective 1:** Establish HQ-Hub1 (ISP A) <--> BR1-R1 (ISP A).
- **Objective 2:** Establish HQ-Hub2 (ISP B) <--> BR1-R2 (ISP B).
- **Objective 3:** Verify **HSRP failover** causes traffic to switch ISPs. When R1 fails, traffic flows via R2/ISP B.

4.3 Hub-to-Branch 3 (ASA Dual ISP)

- **Objective 1:** Configure BR3_ASA with **SLA Monitor**.
    - Primary Route: ISP A (Metric 1, Tracked).
    - Secondary Route: ISP B (Metric 254).
- **Objective 2:** Establish IPsec tunnel to HQ-Hub1. Verify failover to HQ-Hub2 (via ISP B) by shutting down the ASA's ISP A interface.

---

5. Phase 2: Dual Cloud DMVPN & Hybrid Routing

Goal: Deploy Dual-Cloud DMVPN. Implement **ECMP** for Dual-Link sites and **NHS Clustering** for Single-Link sites.

5.1 DMVPN Overlays (Multi-VRF)

- **Objective 1 (Red/BGP):** Configure **Tunnel 100** (Cloud A) and **Tunnel 200** (Cloud B) on Hubs and BR4.
    - Tunnel VRF: VRF_RED.
- **Objective 2 (Blue/EIGRP):** Configure **Tunnel 300** (Cloud A) and **Tunnel 400** (Cloud B) on Hubs and BR4.
    - Tunnel VRF: VRF_BLUE.

5.2 Branch 4 (Dual Uplink): Active/Active ECMP

- **Objective 1 (BGP):** On BR4 (VRF RED), configure iBGP to peer with both Hubs. Enable maximum-paths ibgp 2.
- **Objective 2 (EIGRP):** On BR4 (VRF BLUE), configure Named EIGRP to peer with both Hubs. Ensure delay/bandwidth metrics match.
- **Verification:** show ip route vrf RED and show ip route vrf BLUE must show two paths to HQ.

5.3 Branch 2 (Single Uplink): Active/Standby NHS Clustering

- **Objective 1:** BR2 has only one uplink (ISP A). Configure **Tunnel 100** (Red) to register with **both** Hubs over the single link.
- **Objective 2:** Configure **NHRP NHS Priority**:
    - ip nhrp nhs <Hub1> priority 0 (Preferred).
    - ip nhrp nhs <Hub2> priority 1 (Backup).
- **Objective 3:** Verify that BR2 registers with both, but only installs routes/shortcuts via Hub 1 under normal conditions.

5.4 ASA Legacy Integration

- **Objective 1:** Retain Phase 1 IPsec for BR3_ASA.
- **Objective 2:** Redistribute the ASA static route into the VRF_RED BGP process on HQ-Hub1 so DMVPN spokes can reach it.

---

6. Phase 3: FlexVPN with Hybrid ECMP & Client Failover

Goal: Migrate to a unified FlexVPN fabric. Replace Routing ECMP with IKEv2 Load Balancing where appropriate.

6.1 FlexVPN Hubs: IKEv2 Load Balancing

- **Objective 1:** Convert Hubs to FlexVPN (IKEv2).
- **Objective 2:** Configure an **IKEv2 Load Balancing Cluster** (Redirect).
    - HQ-Hub1: Priority 100 (Master).
    - HQ-Hub2: Priority 90.
- **Objective 3:** Configure a **Virtual IP (VIP)** for the cluster.

6.2 Branch 2 (Single Uplink): FlexVPN Client Failover

- **Objective 1:** Configure an **IKEv2 FlexVPN Client Profile** on BR2.
    - Peer 1: HQ-Hub1 (Tracked Object).
    - Peer 2: HQ-Hub2.
- **Objective 2:** Enable peer reactivate. This forces the router to tear down the tunnel and dial Peer 2 if Peer 1 fails (Protocol-level redundancy).

6.3 Branch 4 (Dual Uplink): Hybrid ECMP Spoke

- **Objective 1:** Configure **4 Static VTIs** on BR4:
    - Tu10: VRF RED -> Hub1 (ISP A) -> Run BGP.
    - Tu20: VRF RED -> Hub2 (ISP B) -> Run BGP.
    - Tu30: VRF BLUE -> Hub1 (ISP A) -> Run EIGRP.
    - Tu40: VRF BLUE -> Hub2 (ISP B) -> Run EIGRP.
- **Objective 2:** Verify **BGP ECMP** works over Tu10 and Tu20 (Red Tenant).
- **Objective 3:** Verify **EIGRP ECMP** works over Tu30 and Tu40 (Blue Tenant).

6.4 ASA FlexVPN Migration

- **Objective 1:** Migrate BR3_ASA to IKEv2 VTI.
- **Objective 2:** Peer BGP with HQ-Hub1 and HQ-Hub2.
- **Objective 3:** Configure BGP Local Preference to prefer the path via ISP A.

6.5 IPv6 Overlay & TrustSec

- **Objective 1:** Enable IPv6 on the VRF_RED tunnels. Configure BGP IPv6 Address Family.
- **Objective 2:** Enable **SGT Inline Tagging** on the FlexVPN VTIs. Verify SGTs are preserved across the dual-cloud overlay.