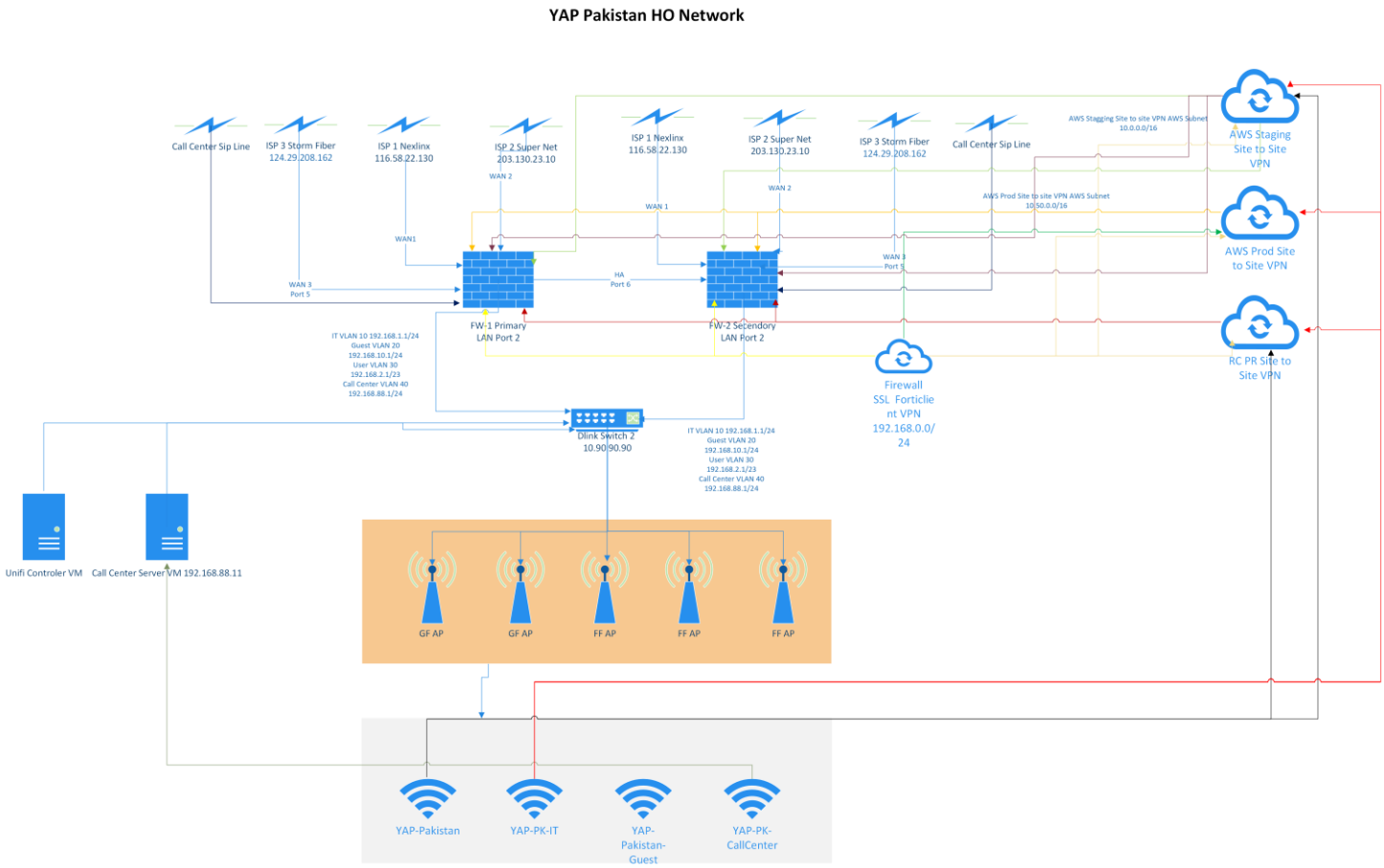
YAP Pakistan HO Network – Detailed Design Document



1. Network Overview

The YAP Pakistan Head Office (HO) network is designed for high availability, security, and scalability. It integrates multiple ISPs, redundant firewalls, VLAN-based segmentation, enterprise Wi-Fi, SSL VPN for remote users, and site-to-site VPN tunnels with AWS and RapidCompute (RC) cloud environments.

2. WAN & ISP Connectivity

- ISP 1 (Nexlinx) → Public IP: 116.58.22.130 (WAN1)
- ISP 2 (Super Net) → Public IP: 203.130.23.10 (WAN2)
- ISP 3 (Storm Fiber) → Public IP: 124.29.208.162 (WAN3)
- Call Center SIP Line → 124.29.208.162 (dedicated for VoIP traffic)

ISPs connect to dual FortiGate 81F firewalls configured in HA (High Availability) mode to ensure failover and redundancy.

3. Firewall & VPNs

- Primary Firewall (FW-1) and Secondary Firewall (FW-2) handle all WAN/LAN traffic.
- SSL VPN (FortiClient) allows secure remote user access → Subnet: 192.168.0.0/24.
- Site-to-Site VPNs:
  - AWS Staging → 10.0.0.0/16
  - AWS Production → 10.50.0.0/16
  - RapidCompute PR (RC) → RC-provided subnet

Routing policies ensure VLANs and SSL VPN users can access AWS/RC resources as required.

4. VLAN Segmentation

VLAN Name	Subnet	Purpose
IT VLAN 10	192.168.1.0/24	IT staff and admins – full access including AWS/RC
Guest VLAN 20	192.168.0.0/24	Visitors – Internet only, isolated from internal resources
User VLAN 30	192.168.2.0/23	General staff users – access to internal apps and selected AWS/RC resources
Call Center VLAN 40	192.168.88.0/24	Call Center and Internet

5. Wi-Fi SSIDs & VLAN Mapping

SSID	Mapped VLAN	Access Rights
YAP-Pakistan	User VLAN 30	Staff → Internet + AWS Staging (limited)
YAP-PK-IT	IT VLAN 10	IT team → Full internal + AWS Staging/Prod + RC
YAP-Pakistan-Guest	Guest VLAN 20	Internet only, no AWS/RC access
YAP-PK-CallCenter	Call Center VLAN 40	Call Center Application &

6. Servers & Core Systems

- Unifi Controller VM → Manages Wi-Fi APs.
- Call Center Server VM → 192.168.88.11 (Call Center VLAN).
- D-Link Core Switch (192.168.1.2) → Distributes connectivity to APs and VLANs.

7. VPN Access Policies

A. SSL VPN Users

- Subnet: 192.168.0.0/24
- Full access to internal VLANs + AWS/RC cloud.

B. Site-to-Site VPN Access

- AWS Staging VPN (10.0.0.0/16) → Accessible from IT VLAN, User VLAN, and SSL VPN (restricted).
- AWS Production VPN (10.50.0.0/16) → Accessible from IT VLAN, some instanced on User VLAN and SSL VPN users.
- RC VPN → Accessible only from IT VLAN, User VLAN (selected), and IT SSL VPN.