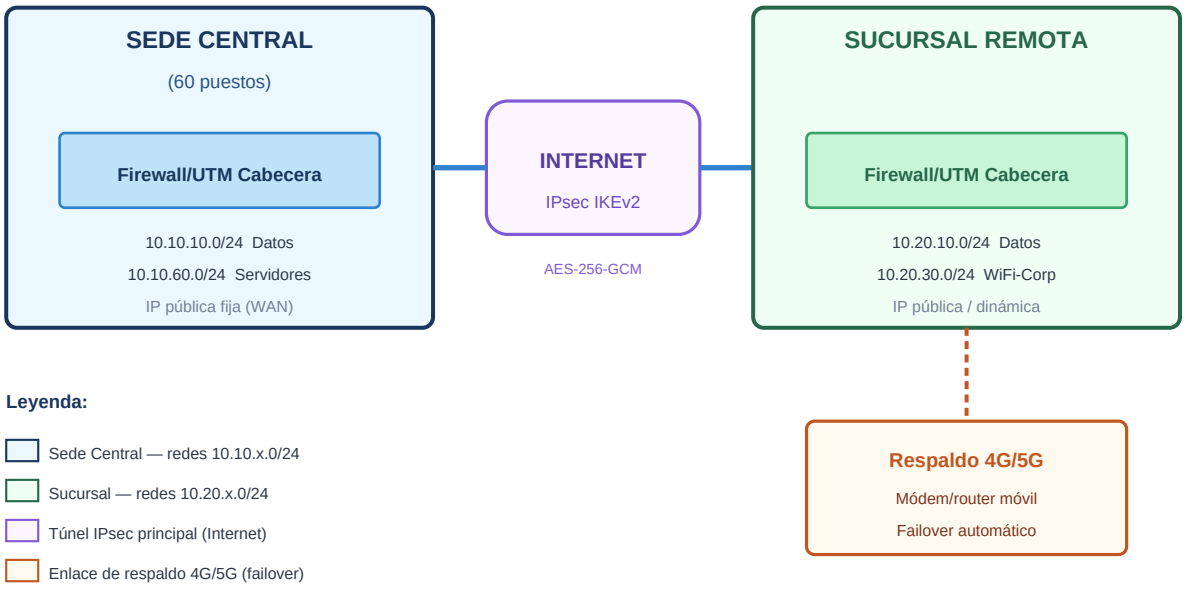
ANEXO 8

Diagrama de Arquitectura — VPN Site-to-Site

Proyecto: Interconexión Segura entre Dos Sedes (VPN Site-to-Site)
Fecha: Agosto 2026 · Versión: 1.0
Elaborado por: Enrique Calabozo Orea – Administrador de Sistemas TIC / Project Manager

Este anexo describe la topología física y lógica de la interconexión VPN Site-to-Site entre la sede central (60 puestos) y la sucursal remota, incluyendo el túnel IPsec principal sobre Internet y el enlace de respaldo 4G/5G.



1. Topología lógica

- Túnel IPsec Site-to-Site en modo túnel (ESP), IKEv2, AES-256-GCM, PFS Grupo 14, DPD habilitado.
- Redes de interés: 10.10.10.0/24 y 10.10.60.0/24 (central) ↔ 10.20.10.0/24 y 10.20.30.0/24 (sucursal).
- Tráfico entre sedes cifrado de extremo a extremo; tráfico a Internet de cada sede sale por su propia WAN (split-tunnel o full-tunnel según política).

2. Alta disponibilidad

- Enlace principal: Internet de cada sede (línea fija / FTTH o similar).
- Enlace de respaldo en sucursal: módem/router 4G/5G con conmutación automática (failover) ante caída de la WAN principal.
- Dead Peer Detection (DPD) para detección rápida de caída del peer y renegociación.

3. Seguridad perimetral

- Firewalls/UTM en ambas cabeceras con reglas de mínimo privilegio (solo tráfico entre redes de interés del túnel).
- Sin NAT del tráfico del túnel (tráfico interesante enrutado, no traducido).
- Logs y monitorización del estado del túnel y de intentos de conexión no autorizados.