PROYECTO TÉCNICO

Despliegue de Firewall UTM Perimetral

Sede Central — 60 puestos de trabajo

Integración con la infraestructura de Red Telemática existente

Enrique Calabozo Orea
Administrador de Sistemas TIC / Project Manager
Agosto 2026 • v1.0

Situación Actual

Red telemática de 60 puestos ya desplegada, con Switch Core L3 y VLAN segmentadas. El perímetro carece de inspección avanzada.

VLAN 10	VLAN 20	VLAN 30	VLAN 40	VLAN 50	VLAN 60	VLAN 99
Datos	Voz	Wi-Fi Corp.	Wi-Fi Invitados	Vídeo/CCTV	Servidores	Gestión
10.10.10.0/24	10.10.20.0/24	10.10.30.0/24	10.10.40.0/24	10.10.50.0/24	10.10.60.0/24	10.10.99.0/24

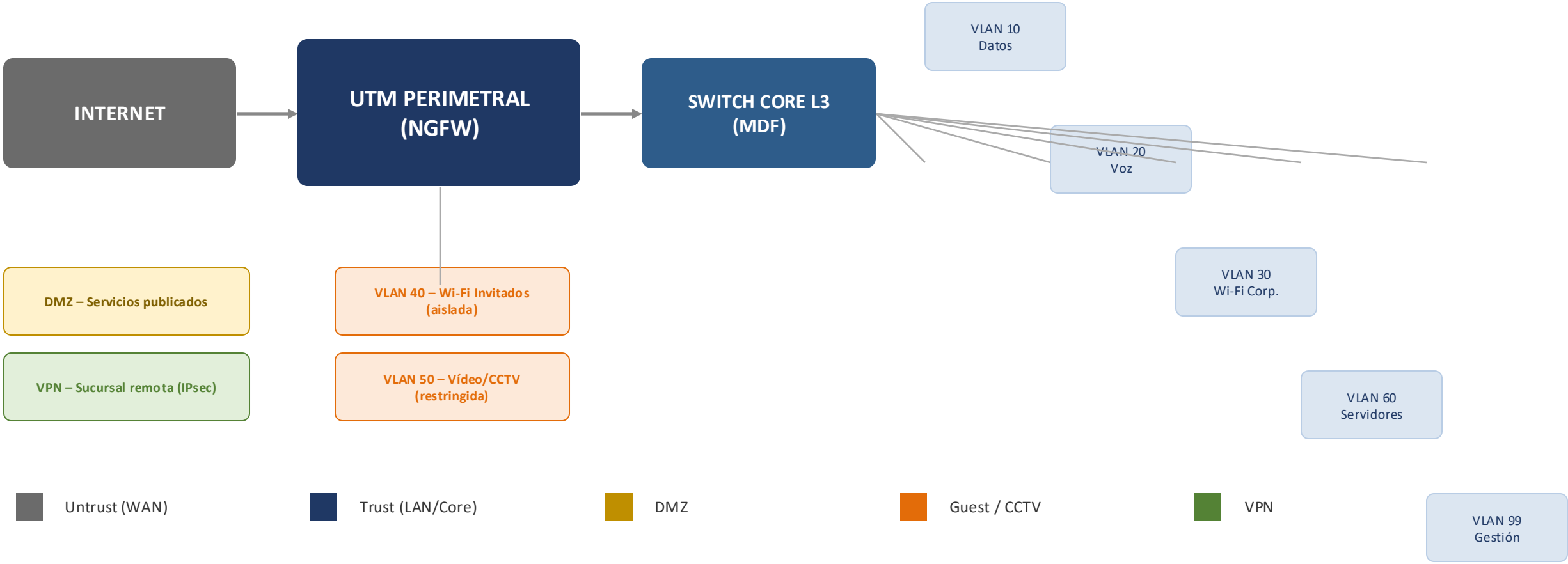
Problema identificado

El router/firewall de borde actual sólo realiza NAT y filtrado por puerto: sin IPS/IDS, sin antivirus de gateway, sin control de aplicaciones ni inspección SSL.

Objetivos del Proyecto

1. Sustituir el router de borde por un UTM/NGFW con inspección profunda de paquetes.
2. Zonas de seguridad (Untrust/Trust/DMZ/VPN) con mínimo privilegio por VLAN.
3. IPS/IDS, antivirus de gateway, filtrado web y control de aplicaciones.
4. Publicación segura de servicios mediante DNAT, sin exponer servidores internos.
5. Migrar la VPN Site-to-Site con la sucursal remota al nuevo UTM.
6. Evaluar alta disponibilidad activo-pasivo (HA) para eliminar el punto único de fallo.

Arquitectura de Zonas de Seguridad



Modo de despliegue: enrutado (routed/NAT). Deny-all por defecto en toda regla no contemplada.

Módulos de Seguridad Avanzada

1

IPS / IDS

Firmas actualizadas a diario; bloqueo de severidad media-alta en modo prevención.

2

Antivirus de Gateway

Inspección de ficheros en HTTP/HTTPS, SMTP y FTP; cuarentena de adjuntos sospechosos.

3

Filtrado Web / DNS

Categorías de riesgo bloqueadas por defecto; perfil reforzado en Wi-Fi invitados.

4

Control de Aplicaciones

Bloqueo de P2P, proxies y VPN no corporativas.

5

Inspección SSL/TLS

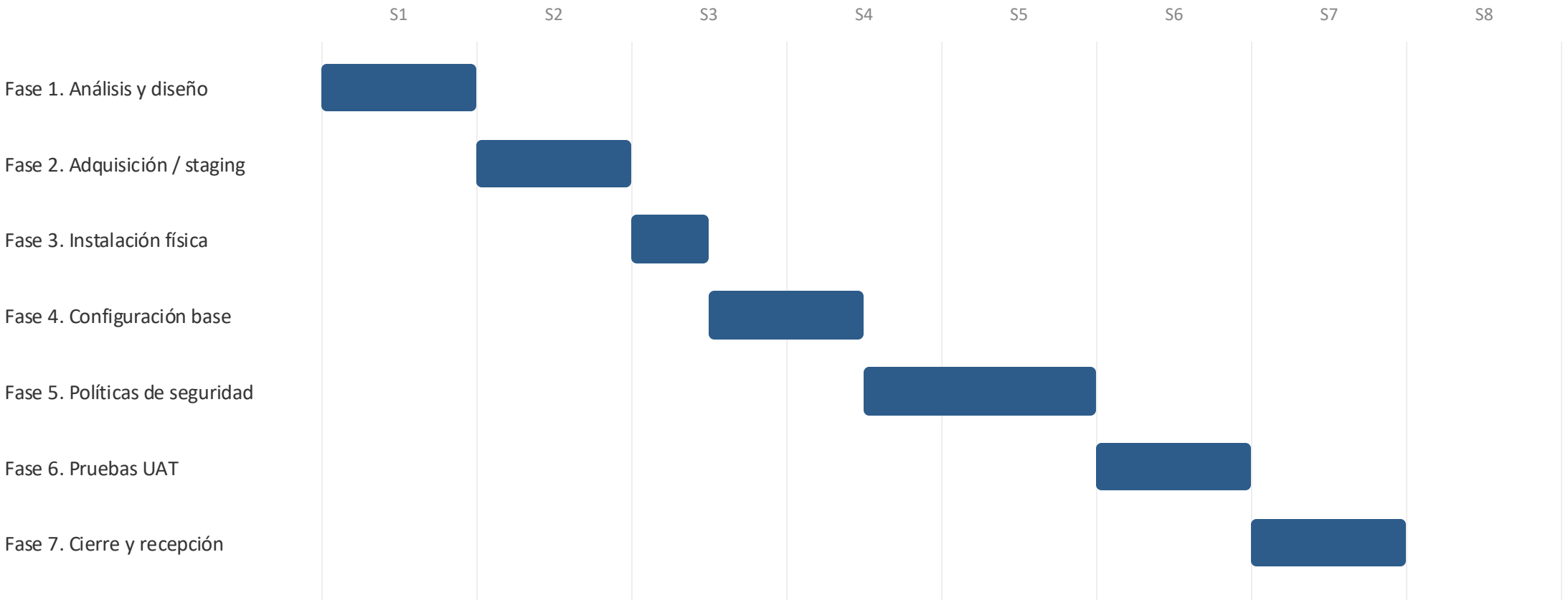
Activa salvo excepciones justificadas (banca, salud, certificate-pinning).

6

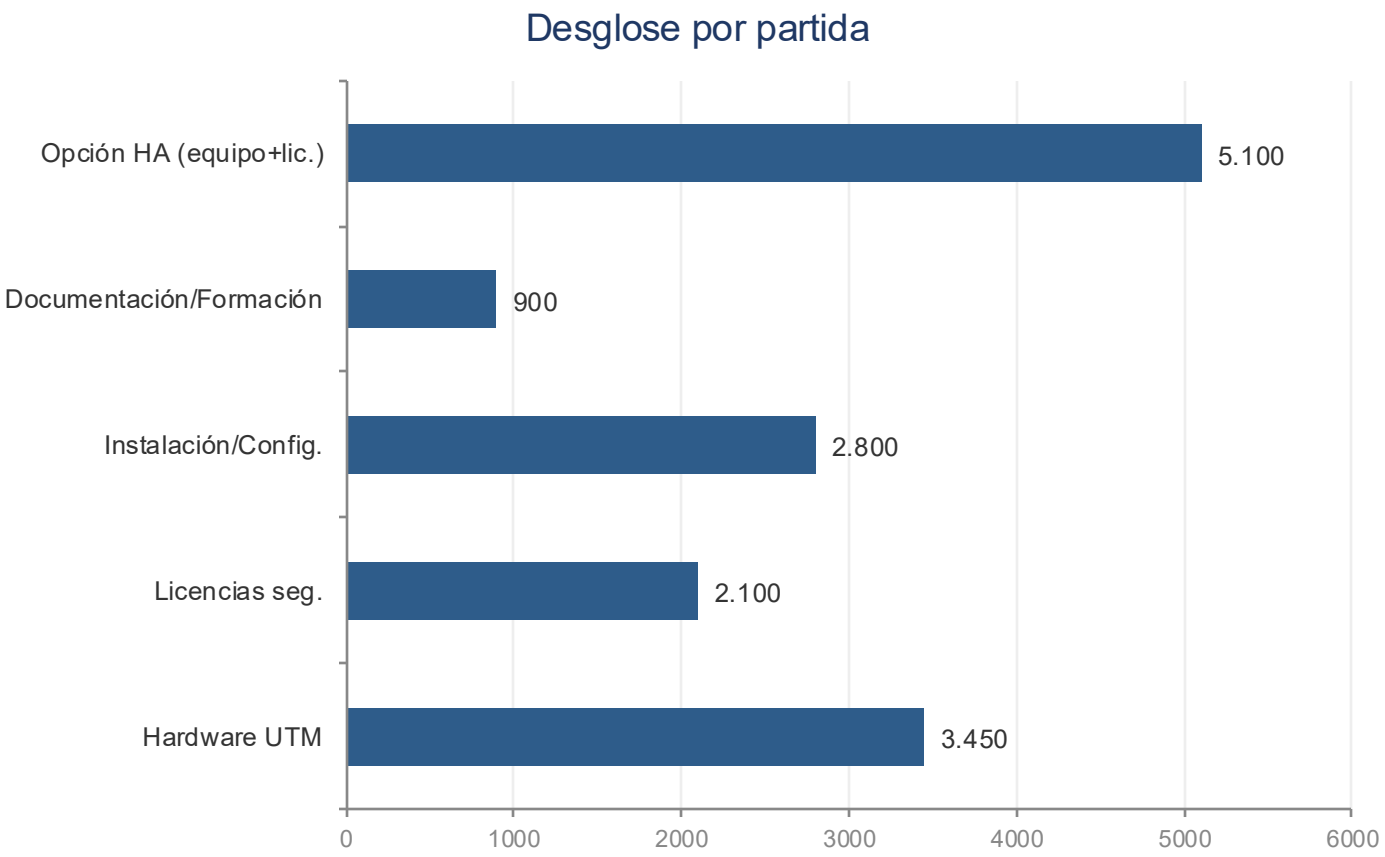
VPN Site-to-Site

Cabecera IPsec IKEv2, AES-256, migrada desde el router de borde actual.

Plan de Ejecución (7 semanas)



Presupuesto Estimado



TOTAL sin HA

11.192,50 €

(con IVA 21%)

TOTAL con HA

17.363,50 €

(con IVA 21%)

Se recomienda la opción HA para eliminar el punto único de fallo del perímetro.

Principales Riesgos

ID	Riesgo	Criticidad
R2	Reglas de firewall mal definidas	9
R1	Fallo del UTM sin redundancia	6
R3	Impacto de SSL Inspection en apps críticas	6
R4	Corte durante migración de VPN	4
R6	Retraso de entrega del hardware	4
R7	Errores de NAT en publicación de servicios	4
R10	Acceso no autorizado a gestión	3
R5	Dimensionamiento insuficiente	3
R8	Resistencia de usuarios (bloqueo de apps)	2
R9	Pérdida de logs / fallo de envío a NMS	2

Escala de criticidad

- Alta (6–9)
- Media (3–4)
- Baja (1–2)

Criticidad = Probabilidad × Impacto (escala 1–3 cada uno).

Pruebas de Aceptación (UAT)

12 casos de prueba (P-F01–P-F12) con criterio PASS/FAIL medible. Aceptación: 100% PASS antes de la recepción provisional.

- ☑ P-F01 Conectividad básica por VLAN
- ☑ P-F02 Aislamiento de VLAN de invitados
- ☑ P-F03 Bloqueo por defecto (deny-all)
- ☑ P-F04 Publicación de servicio (DNAT)
- ☑ P-F05 Detección IPS de firma conocida
- ☑ P-F06 Bloqueo por antivirus de gateway
- ☑ P-F07 Filtrado web de categorías de riesgo
- ☑ P-F08 SSL Inspection sin roturas en excepciones
- ☑ P-F09 VPN Site-to-Site operativa tras migración
- ☑ P-F10 Failover de alta disponibilidad (HA)
- ☑ P-F11 Envío de logs a syslog/NMS
- ☑ P-F12 Acceso administrativo restringido

Conclusiones

- ✓ Cierra la principal brecha de seguridad: falta de inspección avanzada en el perímetro.
- ✓ Coherente con el direccionamiento y VLAN ya desplegadas – sin rediseñar la red existente.
- ✓ Migración ordenada de la VPN Site-to-Site sin afectar a la sucursal remota.
- ✓ Se recomienda la opción de alta disponibilidad (HA) dado que el perímetro pasa a ser el punto crítico de conectividad.