PROYECTO TÉCNICO

Despliegue de Firewall UTM Perimetral

Sede Central — 60 puestos de trabajo

Integración con la infraestructura de Red Telemática existente

Autor: Enrique Calabozo Orea

Administrador de Sistemas TIC / Project Manager

Fecha: Agosto 2026

Versión: 1.0

Índice

1. Introducción

El presente documento constituye la Memoria Técnica del proyecto “Despliegue de Firewall UTM Perimetral – Sede Central (60 puestos)”, cuyo objeto es dotar a la infraestructura de red ya implantada en la sede central de una capa de seguridad perimetral unificada (UTM: Unified Threat Management), situada entre la conexión a Internet y el Switch Core L3 del edificio.

Este proyecto se concibe como cierre natural del proceso de securización de la sede central, y se integra de forma coherente con los proyectos previamente documentados: la Implantación de Red Telemática (60 puestos), el despliegue de VoIP/Centralita IP, la interconexión VPN Site-to-Site con la sucursal remota, el sistema de videovigilancia IP (CCTV) y la red Wi-Fi corporativa. El UTM pasa a ser el punto único de control de todo el tráfico entrante y saliente de la organización, así como el extremo de cabecera de la VPN Site-to-Site existente.

El documento sigue la estructura habitual de la documentación técnica de proyecto empleada en las certificaciones profesionales IFCT0410 / IFCT0510, e incluye memoria técnica, anexos numerados correlativamente y anexos de soporte a la ejecución, operación y aceptación del sistema.

2. Objetivos del Proyecto

2.1. Objetivo general

Desplegar un equipo UTM en el perímetro de la red de la sede central que centralice y unifique las funciones de firewall, IPS/IDS, antivirus de pasarela, filtrado de contenidos y control de aplicaciones, protegiendo todas las VLAN existentes y sirviendo de cabecera VPN, sin degradar el rendimiento ni la disponibilidad de los servicios actuales.

2.2. Objetivos específicos

- Sustituir/complementar el router de borde del operador por un firewall UTM de nueva generación (NGFW) con capacidad de inspección profunda de paquetes (DPI).
- Definir zonas de seguridad (Untrust, Trust, DMZ, VPN) y aplicar el principio de mínimo privilegio en las reglas de firewall por zona y por VLAN.
- Habilitar IPS/IDS, antivirus de gateway, filtrado web/DNS y control de aplicaciones (Application Control) sobre todo el tráfico de la sede.
- Publicar de forma segura los servicios que deban ser accesibles desde el exterior mediante DNAT, sin exponer directamente los servidores internos.
- Garantizar la continuidad de la VPN Site-to-Site con la sucursal remota, migrando la cabecera VPN al nuevo UTM.
- Evaluar e implementar, si el presupuesto lo permite, alta disponibilidad activo-pasivo (HA) para eliminar el punto único de fallo que supone el perímetro.
- Integrar el UTM en la VLAN de gestión (VLAN 99) y centralizar logging y alertas en el sistema de monitorización (syslog/NMS) de la organización.
- Minimizar el impacto de la inspección SSL sobre la experiencia de usuario y sobre aplicaciones sensibles, definiendo excepciones justificadas.
- Dejar documentado un procedimiento de operación, mantenimiento y respuesta ante incidentes para el personal de sistemas.

3. Antecedentes y Situación Actual

La sede central dispone de una red telemática ya implantada y operativa para 60 puestos de trabajo, estructurada mediante un Switch Core L3 ubicado en el MDF, que realiza el enrutamiento inter-VLAN, y una serie de switches de acceso en los racks secundarios (IDF). El esquema de VLAN actualmente en producción es el siguiente:

VLAN	Nombre	Red / Máscara	Descripción
10	Datos	10.10.10.0/24	Puestos de usuario, equipos de oficina
20	Voz	10.10.20.0/24	Telefonía IP / centralita virtual
30	Wi-Fi Corporativo	10.10.30.0/24	Acceso inalámbrico de empleados
40	Wi-Fi Invitados	10.10.40.0/24	Acceso inalámbrico de visitantes (aislado)
50	Vídeo / CCTV	10.10.50.0/24	Cámaras IP, NVR/VMS
60	Servidores	10.10.60.0/24	Servidores internos y aplicaciones corporativas
99	Gestión	10.10.99.0/24	Gestión de electrónica de red (out-of-band lógica)

Asimismo, se encuentra desplegada (o prevista a corto plazo) una VPN Site-to-Site IPsec entre la sede central y una sucursal remota, actualmente terminada en el router/firewall de borde del cliente. Dicho equipo de borde, de prestaciones limitadas, únicamente realiza funciones básicas de NAT y filtrado por puerto, careciendo de IPS/IDS, antivirus de pasarela, control de aplicaciones e inspección SSL.

Esta carencia de inspección avanzada en el perímetro constituye el principal riesgo de seguridad identificado sobre la infraestructura actual, y es el problema que este proyecto resuelve.

4. Descripción General del Proyecto

El proyecto consiste en el diseño, suministro, instalación, configuración y puesta en producción de un equipo firewall UTM que se ubicará físicamente en el rack principal (MDF) de la sede central, en línea entre la salida a Internet (router del operador / ONT) y el Switch Core L3.

El alcance del proyecto comprende:

- Definición de la arquitectura de zonas de seguridad y su relación con las VLAN existentes.
- Selección de requisitos mínimos del equipo UTM (dimensionamiento por throughput, sesiones concurrentes y usuarios).
- Configuración de interfaces, zonas, objetos de red y políticas de firewall por zona y VLAN.
- Configuración de NAT (SNAT para salida a Internet, DNAT para publicación de servicios).
- Activación de los módulos de seguridad: IPS/IDS, antivirus de gateway, filtrado web/aplicaciones e inspección SSL con excepciones controladas.
- Migración de la VPN Site-to-Site existente al nuevo UTM sin interrupción prolongada del servicio.
- Integración en VLAN de gestión, configuración de logging remoto (syslog) y alertas.
- Evaluación de alta disponibilidad activo-pasivo (opción presupuestada de forma independiente).
- Pruebas de aceptación (UAT), documentación final y entrega formal mediante Acta de Recepción Provisional.

Quedan fuera de alcance: la renovación del cableado estructurado, la sustitución del Switch Core, y la securización de endpoints (EDR/antivirus de puesto), que se consideran proyectos independientes.

5. Solución Técnica Propuesta

5.1. Modo de despliegue

Se recomienda el despliegue en modo enrutado (routed / NAT mode) frente al modo transparente. El modo enrutado permite que el UTM asuma el rol de puerta de enlace perimetral, realice NAT, termine la VPN Site-to-Site y aplique políticas por zona/VLAN de forma nativa, con una gestión de logs más clara. El modo transparente se descarta porque obligaría a mantener el direccionamiento actual sin visibilidad de capa 3 en el propio firewall, dificultando el filtrado por VLAN y la terminación VPN.

5.2. Zonas de seguridad

Zona	Interfaz	Descripción
Untrust (WAN)	WAN1 (+ WAN2 opcional)	Conexión a Internet a través del router/ONT del operador
Trust (LAN/Core)	Subinterfaces 802.1Q hacia Core	VLAN 10, 20, 30, 60, 99 (tráfico interno de confianza)
Guest	Subinterfaz VLAN 40	Wi-Fi invitados, aislada del resto de zonas Trust
CCTV	Subinterfaz VLAN 50	Vídeo/CCTV, sin salida a Internet salvo actualizaciones controladas
DMZ	Interfaz dedicada / VLAN DMZ	Servicios publicados al exterior (si aplica: correo, portal, VPN de acceso remoto)
VPN	Interfaz túnel IPsec	Tráfico cifrado hacia la sucursal remota

5.3. NAT y publicación de servicios

Se configurará NAT de origen (SNAT/PAT) para la salida a Internet de las VLAN 10, 20, 30, 60 y 99. La VLAN 40 (invitados) dispondrá de su propia salida NAT independiente y sin visibilidad hacia el resto de VLAN. Para los servicios que deban ser accesibles desde el exterior (p. ej. correo corporativo, portal web, acceso VPN de usuario remoto) se aplicará NAT de destino (DNAT) hacia la DMZ, evitando en todo momento la publicación directa de servidores de la VLAN 60.

5.4. Seguridad avanzada

- IPS/IDS: firmas actualizadas automáticamente, aplicadas sobre todo el tráfico Untrust ↔ Trust y en los flujos hacia la DMZ.
- Antivirus de gateway: inspección de ficheros en protocolos HTTP/HTTPS, SMTP, FTP.
- Filtrado de URL/aplicación: categorías de riesgo y productividad bloqueadas por defecto; VLAN de invitados con perfil restrictivo propio.
- Inspección SSL (SSL/TLS Inspection): activada de forma selectiva sobre categorías de riesgo elevado; se definen excepciones para banca, salud y sitios con certificate pinning, evitando roturas de aplicaciones críticas.
- Control de aplicaciones: identificación y limitación de aplicaciones P2P, proxies/anonimizadores y VPN no corporativas.

5.5. VPN Site-to-Site

El UTM asume el rol de cabecera IPsec, sustituyendo al router de borde actual. Se mantiene la topología existente (sede central – sucursal remota) descrita en el proyecto de VPN Site-to-Site, migrando el túnel IKEv2 con los mismos parámetros de direccionamiento remoto, ajustando únicamente el extremo local. Se define una ventana de migración con router de respaldo para minimizar el corte de servicio.

5.6. Alta disponibilidad (opcional)

Se plantea, como opción presupuestada de forma independiente, el despliegue de un segundo equipo UTM idéntico en clúster activo-pasivo (HA), con sincronización de sesiones y configuración, e interfaz dedicada de heartbeat. Esta opción elimina el punto único de fallo del perímetro y se recomienda si la organización considera crítica la disponibilidad de la salida a Internet y la VPN. En caso de no aprobarse, se recomienda contratar un contrato de soporte con sustitución de hardware en 24h (NBD) como mitigación parcial.

5.7. Gestión, logging y cumplimiento

El equipo se integrará en la VLAN 99 de gestión, con acceso administrativo restringido por IP de origen y doble factor de autenticación. Todos los eventos de firewall, IPS, VPN y sistema se enviarán en tiempo real a un servidor syslog/NMS centralizado, con retención mínima de 12 meses en línea con el criterio orientativo de buenas prácticas del ENS (Esquema Nacional de Seguridad) y con los principios de minimización y trazabilidad del RGPD, sin que ello suponga una certificación formal de cumplimiento normativo.

6. Especificaciones Técnicas

Requisitos mínimos orientativos del equipo UTM, dimensionados para 60 puestos + invitados + servicios publicados:

Parámetro	Requisito mínimo orientativo
Throughput Firewall (UDP)	≥ 2 Gbps
Throughput con IPS activado	≥ 800 Mbps
Throughput con NGFW (IPS+App Control)	≥ 600 Mbps
Throughput VPN IPsec (AES-256)	≥ 500 Mbps
Sesiones concurrentes	≥ 250.000
Nuevas sesiones/segundo	≥ 8.000
Interfaces	≥ 8 x 1GbE (2 SFP+ recomendables para futura ampliación)
VLAN / subinterfaces 802.1Q	≥ 20
Túneles VPN IPsec simultáneos	≥ 25
Usuarios soportados (licencia)	≥ 75 (60 puestos + margen de crecimiento)
Alta disponibilidad	Activo-pasivo (opcional, ver 5.6)
Gestión	GUI web HTTPS, CLI SSH, API REST, soporte SNMPv3
Logging	Exportación syslog (TCP/TLS) a servidor NMS centralizado

7. Plan de Ejecución y Cronograma

El proyecto se ejecuta en 7 fases a lo largo de 7 semanas. El detalle de tareas, duración y diagrama se recoge en el Anexo 3 – Cronograma.

Fase	Descripción	Duración
1	Análisis, diseño de zonas y validación con red existente	1 semana
2	Adquisición y preparación del equipo (staging)	1 semana
3	Instalación física y cableado en MDF	0,5 semana
4	Configuración base: interfaces, zonas, objetos, NAT	1 semana

Fase	Descripción	Duración
5	Políticas de seguridad, IPS/AV/filtrado, migración VPN	1,5 semanas
6	Pruebas de aceptación (UAT) y ajuste fino	1 semana
7	Documentación final, formación y recepción provisional	1 semana

8. Presupuesto Estimado

El desglose completo se recoge en el Anexo 2. Resumen por partidas:

Partida	Importe (sin IVA)
Hardware UTM (equipo principal)	3.450,00 €
Licencias de seguridad (IPS/AV/Web/App, 3 años)	2.100,00 €
Opción HA (segundo equipo + licencias)	5.100,00 €
Instalación, configuración y migración	2.800,00 €
Documentación, pruebas y formación	900,00 €
TOTAL sin opción HA (sin IVA)	**9.250,00 €**
TOTAL con opción HA (sin IVA)	**14.350,00 €**
IVA (21%) – sin HA	1.942,50 €
TOTAL sin HA (con IVA)	**11.192,50 €**
TOTAL con HA (con IVA)	**17.363,50 €**

9. Gestión de Riesgos

La matriz completa de riesgos se detalla en el Anexo 4. Se identifican 10 riesgos, siendo los de mayor criticidad el fallo del UTM sin redundancia, la definición incorrecta de reglas de firewall y el impacto de la inspección SSL sobre aplicaciones críticas.

10. Plan de Calidad y Pruebas

Se define un Plan de Pruebas de Aceptación (UAT) con casos de prueba identificados (P-F01, P-F02…) y criterio PASS/FAIL medible, recogido en el Anexo 9. Las pruebas cubren: conectividad básica por VLAN, aplicación efectiva de reglas de mínimo privilegio, funcionamiento de IPS/antivirus/filtrado, publicación de servicios (DNAT), funcionamiento de la VPN Site-to-Site migrada, failover de HA (si aplica) y correcto envío de logs al NMS.

11. Documentación a Entregar

- Memoria técnica del proyecto (este documento).
- Anexo 1 – Diagrama de arquitectura / topología perimetral.
- Anexo 2 – Presupuesto detallado.
- Anexo 3 – Cronograma.
- Anexo 4 – Matriz de riesgos.
- Anexo 5 – Políticas de seguridad / reglas de firewall.
- Anexo 6 – Manual de Operación y Mantenimiento.
- Anexo 7 – Inventario detallado de equipos.

- Anexo 8 – Configuración base del UTM.
- Anexo 9 – Plan de Pruebas de Aceptación (UAT).
- Anexo 10 – Acta de Recepción Provisional.

12. Conclusiones

El despliegue del firewall UTM perimetral cierra la brecha de seguridad identificada en el perímetro de la sede central, aportando inspección avanzada de tráfico (IPS/IDS, antivirus de gateway, control de aplicaciones e inspección SSL) de la que carecía el equipo de borde actual. La solución propuesta es coherente con el direccionamiento IP y las VLAN ya desplegadas, no requiere modificar la electrónica de red existente y permite una migración ordenada de la VPN Site-to-Site sin rediseñar la arquitectura de la sucursal remota.

Se recomienda la adopción de la opción de alta disponibilidad (HA) siempre que el presupuesto lo permita, dado que el perímetro pasa a ser, tras este proyecto, el punto crítico de conectividad de toda la organización.

13. Anexos

Los anexos numerados del 1 al 10 se desarrollan a continuación de esta memoria.