ANEXO 5 – Políticas de Seguridad / Reglas de Firewall

Ejemplo de conjunto de reglas por zona/VLAN, aplicando el principio de mínimo privilegio. Todas las reglas no contempladas quedan denegadas por defecto (deny-all implícito).

#	Origen	Destino	Servicio	Acción	Inspección
1	VLAN 10 (Datos)	Zona Untrust	HTTP/HTTPS/DNS	Permitir	IPS + AV + Filtrado Web + SSL Insp.
2	VLAN 20 (Voz)	Proveedor SIP / Zona Untrust	SIP/RTP (UDP/TCP definidos)	Permitir	IPS (sin SSL insp. en RTP)
3	VLAN 30 (Wi-Fi Corp.)	Zona Untrust	HTTP/HTTPS/DNS	Permitir	IPS + AV + Filtrado Web
4	VLAN 30 (Wi-Fi Corp.)	VLAN 10/60 (Trust)	Cualquiera	Denegar	—
5	VLAN 40 (Wi-Fi Invitados)	Zona Untrust	HTTP/HTTPS/DNS	Permitir	Filtrado Web estricto
6	VLAN 40 (Wi-Fi Invitados)	VLAN 10/20/30/50/60/99	Cualquiera	Denegar	—
7	VLAN 50 (CCTV)	Zona Untrust	NTP/actualizaciones firmware (lista blanca)	Permitir	IPS
8	Zona Untrust	VLAN 50 (CCTV)	Cualquiera	Denegar	—
9	VLAN 10/30 (usuarios)	VLAN 60 (Servidores)	Puertos de aplicación corporativa (definidos)	Permitir	IPS
10	Zona Untrust	DMZ	HTTPS (443) / SMTP (25,587)	Permitir (DNAT)	IPS + AV
11	DMZ	VLAN 60 (Servidores)	Puertos específicos de backend (definidos)	Permitir	IPS
12	Zona Untrust	VLAN 99 (Gestión)	Cualquiera	Denegar	—
13	IP administrador (lista blanca)	VLAN 99 (Gestión)	HTTPS (GUI) / SSH	Permitir + MFA	—
14	Sucursal remota (túnel VPN)	VLAN 10/60 (recursos autorizados)	Puertos definidos por necesidad	Permitir	IPS
15	Cualquier zona	Cualquier zona	Cualquiera	Denegar (regla final)	Log activado

Principios aplicados

- Deny-all por defecto: sólo se permite explícitamente lo necesario.
- Segmentación estricta de VLAN 40 (invitados) y VLAN 50 (CCTV) respecto al resto de la red.
- Ninguna regla permite acceso directo desde Untrust hacia zonas Trust; toda publicación pasa por DMZ.
- El acceso administrativo al UTM requiere IP de origen en lista blanca y doble factor de autenticación.
- Todas las reglas quedan registradas (logging) para trazabilidad y auditoría.