ANEXO 8 – Configuración Base del UTM

Plantilla orientativa de configuración (sintaxis genérica tipo CLI), a adaptar al fabricante finalmente seleccionado.

8.1. Interfaces y zonas

```
interface WAN1   zone UNTRUST   ip address dhcp   # o IP fija asignada por el operador
interface LAN-TRUNK.10   zone TRUST   vlan-id 10   ip address 10.10.10.1/24  interface
LAN-TRUNK.20   zone TRUST   vlan-id 20   ip address 10.10.20.1/24  interface LAN-
TRUNK.30   zone TRUST   vlan-id 30   ip address 10.10.30.1/24  interface LAN-TRUNK.40
zone GUEST   vlan-id 40   ip address 10.10.40.1/24  interface LAN-TRUNK.50   zone CCTV
vlan-id 50   ip address 10.10.50.1/24  interface LAN-TRUNK.60   zone TRUST-SERVERS
vlan-id 60   ip address 10.10.60.1/24  interface LAN-TRUNK.99   zone MGMT   vlan-id 99
ip address 10.10.99.1/24  interface DMZ1   zone DMZ   ip address 172.16.1.1/28
```

8.2. Objetos de red

```
object network NET_DATOS       10.10.10.0/24 object network NET_VOZ
10.10.20.0/24 object network NET_WIFI_CORP   10.10.30.0/24 object network NET_WIFI_GUEST
10.10.40.0/24 object network NET_CCTV        10.10.50.0/24 object network NET_SERVERS
10.10.60.0/24 object network NET_MGMT        10.10.99.0/24 object network NET_SUCURSAL
192.168.100.0/24   # red remota VPN object network SRV_CORREO_DMZ  172.16.1.10/32 object
network SRV_WEB_DMZ     172.16.1.11/32
```

8.3. NAT

```
# SNAT salida a Internet (PAT sobre IP de WAN1) nat source
NET_DATOS,NET_VOZ,NET_WIFI_CORP,NET_SERVERS,NET_MGMT \     -> interface WAN1 (PAT) nat
source NET_WIFI_GUEST -> interface WAN1 (PAT, pool independiente)  # DNAT publicación de
servicios nat destination WAN1:443  -> SRV_WEB_DMZ:443     service HTTPS nat destination
WAN1:25   -> SRV_CORREO_DMZ:25   service SMTP nat destination WAN1:587  ->
SRV_CORREO_DMZ:587  service SMTP-SUBMISSION
```

8.4. VPN IPsec Site-to-Site

```
vpn ike-gateway SUCURSAL   interface WAN1   peer-ip <IP_PUBLICA_SUCURSAL>   ike-version
v2   auth-method pre-shared-key   encryption aes-256   hash sha-256   dh-group 14
lifetime 28800  vpn ipsec-tunnel SUCURSAL   gateway SUCURSAL   local-network
NET_DATOS,NET_SERVERS   remote-network NET_SUCURSAL   encryption aes-256-gcm   pfs-group
14   lifetime 3600
```

8.5. Perfiles de seguridad (resumen)

- Perfil IPS: modo prevención, severidad media-alta bloqueada, severidad baja en modo log.
- Perfil Antivirus: bloqueo de malware conocido en HTTP/HTTPS/SMTP/FTP, cuarentena de adjuntos sospechosos.
- Perfil Web Filter: categorías bloqueadas por defecto (malware, phishing, adultos, anonimizadores); perfil reforzado para VLAN 40.
- Perfil SSL Inspection: activo salvo lista de exclusión (banca, salud, certificate-pinning conocido).
- Perfil Application Control: bloqueo de P2P y proxies/VPN no corporativas; resto en modo monitorización.