

network_topology

Sare Topologia eta Mapa - Zabala Gailetak

1. Topologiaren Deskribapena

Enpresak sare segmentatu bat ezarri du, segurtasuna bermatzeko.

Egitura Nagusia

- **DMZ (Gune Desmilitarizatua):**
 - Kanpotik eskuragarri egon behar diren zerbitzuak (Web zerbitzaria, Emaila, Honeypot).
 - Firewall bidez isolatuta barne aretik.
- **Barne Sarea (LAN):**
 - Erabiltzaileen ekipoak.
 - Inprimagailuak.
- **Sistemen Sarea (Server VLAN):**
 - Datu-baseak, Fitxategi zerbitzariak, Domeinu kontrolatzailea.
 - Sarbidea murritzuta (bakarrik beharrezko portuak).
- **OT Sarea (Industrial):**
 - PLC-ak (OpenPLC), HMI-ak, SCADA sistemak.
 - **Node-RED:** Datuen integrazioa eta fluxuen kudeaketa egiteko, sare berean kokatuta.
 - Makina fisikoen simulazioa (Factory I/O).
 - IT saretik guztiz isolatuta edo “Data Diode” / Firewall zorrotz baten bidez.

2. Sare Mapa (Irudiak)

Jarraian, dokumentaziotik ateratako sare mapak agertzen dira:

image2.png



image2.png

Oharra: Irudien edukia mantendu egin da jatorrizko formatuan, base64 kodeketa delako. Irudi honek sarearen topologia fisikoa erakusten du.

3. Sare Segmentazioa

VLAN Banaketa

VLAN ID	Izena	IP Tartea	Helburua
---------	-------	-----------	----------

10	Bulegoa	192.168.10.0/24	Langileen ekipoak
----	---------	-----------------	-------------------

20	Zerbitzariak	192.168.20.0/24	Aplikazio eta datu-base zerbitzariak
----	--------------	-----------------	--------------------------------------

VLAN ID	Izena	IP Tartea	Helburua
30	DMZ	192.168.30.0/24	Publikoki eskuragarri dauden zerbitzuak
40	OT/SCADA	192.168.40.0/24	Industria kontrol sistemak
99	Honeypot	172.16.99.0/24	Isolatutako honeypot sarea

Firewall Arau Nagusiak

Internet → DMZ (HTTP/HTTPS soilik)
allow tcp any to DMZ port 80,443

DMZ → Barne Sarea (debekatua)
deny any DMZ to LAN

DMZ → Zerbitzariak (mugatua)
allow tcp DMZ to SERVERS port 5432 (PostgreSQL)
allow tcp DMZ to SERVERS port 6379 (Redis)

Barne Sarea → Internet (HTTP/HTTPS)
allow tcp LAN to any port 80,443

OT Sarea → Internet (debekatua)
deny any OT to any

OT Sarea → Barne Sarea (debekatua)
deny any OT to LAN

Barne Sarea → OT Sarea (SCADA sarbide soilik)
allow tcp LAN to OT port 502 (Modbus TCP)

4. Segurtasun Neurriak

Sare Mailan

- **Firewall:** Fortinet FortiGate 200F
- **IDS/IPS:** Suricata/Snort integratua
- **VLAN Isolamendua:** Sare segmentazio zorrotza
- **Port Security:** MAC helbideen eta portuen lotura

Sistema Mailan

- **Antivirus:** ClamAV / Sophos
- **Host Firewall:** iptables/ufw gaituta
- **Logak:** Rsyslog bidez zentralizatuta SIEM-era
- **Monitorizazioa:** Nagios/Zabbix/Wazuh

Aplikazio Mailan

- **HTTPS:** TLS 1.3 edo altuena
- **HSTS:** HTTP Strict Transport Security gaituta
- **CSP:** Content Security Policy konfiguratuta
- **CSRF Token-ak:** Cross-Site Request Forgery babesia

5. Kontaktua eta Laguntza

Segurtasun gertaera bat detektatzen bada, jarri harremanetan:

- **Segurtasun Taldea:** security@zabala.gaietak.eus
- **24/7 Larrialdiak:** +34 600 XXX XXX
- **SIEM Alertak:** SOC@zabala.gaietak.eus