ZABALA GAILETAK, S.A.

SAREAK ETA SISTEMAK GOTORTZEA

Sareak eta Sistemak Gotortzea — Txosten Nagusia

Sare Segmentazioa · Hardening · SIEM · OT Segurtasuna

Dokumentu Kodea:	HARD-ZG-001
Bertsioa:	1.0
Data:	2026-02-19
Ikasturtea:	2026
Sailkapena:	Heziketa — Barne Erabilera
Egilea:	Zabala Gailetak Zibersegurtasun Taldea

1. Sare Arkitektura eta Segmentazioa

Zabala Gailetak-ek Zero Trust printzipioan oinarritutako sare-arkitektura du, lau VLAN nagusirekin eta IT/OT banaketa zorrotzekin:

VLAN	Izena	Sareko Helbidea	Helburua	Babesbabesa
VLAN 10	Kudeaketa	10.10.10.0/24	Zerbitzari admin sarbidea	Restriczio gogorrak, VPN soilik
VLAN 20	IT/Enpresa	10.10.20.0/24	Langile ordenagailuak, aplikazioak	Firewall arau zorrotzak
VLAN 30	DMZ	10.10.30.0/24	Web zerbitzaria, DNS, HAProxy	Kanpotik ikusgai, baina mugatua
VLAN 50	OT/Industriala	10.10.50.0/24	PLC, SCADA, HMI gailuak	AIR-GAP, IT-tik guztiz isolatua

1.1 Firewall Arau Politika (Zerowireless First)

```
# pfSense — Oinarrizko arau-zerrenda (laburpena) # VLAN 50 (OT) → VLAN 20 (IT): DENY ALL [IT/OT bereiztzeko] # VLAN 20 (IT) → VLAN 30 (DMZ): ALLOW dport 443, 80 # Kanpoa → VLAN 30 (DMZ): ALLOW dport 443 # VLAN 10 → GUZTIA: ALLOW (kudeaketa sarbidea) # Default: DENY ALL — ez onartutakoa blokeatu
```

2. Zerbitzari Gotortzea (Server Hardening)

2.1 Linux Zerbitzariak — CIS Benchmark L2

- Sistema eguneratuak mantendu: apt update && apt upgrade -y astero.
- SSH root sarbidea desgaitu: PermitRootLogin no sshd_config-en.
- SSH pasahitz autentifikazioa desgaitu: PasswordAuthentication no — gako publikoak soilik.
- fail2ban instalatu SSH brute force erasoen aurkako babeserako.
- Beharrezkoak ez diren zerbitzuak desgaitu: systemctl disable.
- UFW suebakia konfiguratu: beharrezko portuak soilik ireki.
- auditd ezarri sistema-deiak eta fitxategi kritikoen aldaketak erregistratzeko.

```
# SSH konfigurazio segurua (/etc/ssh/sshd_config) PermitRootLogin no PasswordAuthentication no MaxAuthTries 3 LoginGraceTime 30 AllowUsers sysadmin deploy Protocol 2 Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com
```

3. Web Aplikazioaren Gotortzea

3.1 Nginx Segurtasun Goiburuak

```
# Nginx — Segurtasun goiburuak add_header Strict-Transport-Security 'max-age=63072000; includeSubDomains; preload' always; add_header X-Content-Type-Options 'nosniff' always; add_header X-Frame-Options 'DENY' always; add_header X-XSS-Protection '1; mode=block' always; add_header Referrer-Policy 'strict-origin-when-cross-origin' always; add_header Permissions-Policy 'geolocation=(), midi=(), camera=()' always; add_header
```

```
Content-Security-Policy "default-src 'self'; script-src 'self' 'nonce-{NONCE}'" always;
server_tokens off; # Nginx bertsioa ezkutatu
```

4. SIEM — ELK + Wazuh Inplementazioa

Security Information and Event Management (SIEM) sistema zentralizatua ELK Stack eta Wazuh-ekin ezarri da:

Osagaia	Rola	Portua
Elasticsearch	Log biltegiratze eta bilaketa	9200, 9300
Logstash	Log bilketa eta eraldaketa (ETL)	5044, 5000
Kibana	Dashboard eta bistaratze tresna	5601
Wazuh Manager	IDS/IPS + FIM + aktibo monitoreoa	1514, 1515
Wazuh Agents	Zerbitzari bakoitzean instalatua	1514 UDP
Filebeat	Log fitxategien bidalketa	5044

4.1 Alerta Arau Nagusiak

Araua	Trigerra	Larritasuna
Brute Force SSH	5 huts saiakera < 1 min IP beretik	■ Kritikoa
Privilege Escalation	sudo root komandoak	■ Kritikoa
FIM — /etc/passwd	Fitxategi aldaketa	■ Kritikoa
Port Scan	>50 portu < 30 seg IP beretik	■ Kritikoa
SQLi saiakera	Nginx access log — UNION SELECT	■ Kritikoa
New Admin User	/etc/group aldaketa — sudo taldea	■ Altua
Zaharkitu softw.	CVE datu-basea — CVSS > 8.0	■ Altua

5. OT Segurtasuna — IEC 62443 Gotortze Neurriak

IT/OT bereizpena derrigorrezkoa da fabrika ingurune seguruetarako:

- VLAN 50 (OT) guztiz isolatua — IT sarea eta OT sarea zuzenki konektatuta egon gabe.
- Unidirectional Security Gateway (data diode) OT telemtria IT SIEM-era bidaltzeko.
- USB portuen blokeo fisikoa PLCetan — badminton-en bakarrik SSP prozedurak.
- PLC sarbidea Engineers Only MAC whitelist-arekin.
- Honeypot Conpot gailua OT sarean mehatxu detekziorako.
- OT gailuetarako adabaki-kudeaketa: ekoizpen-geldialdietan soilik, probatuta.