Infraestructura Segura - Infrastructure as Code

Sareak eta Sistemak Gotortzea - Zabala Gailetak

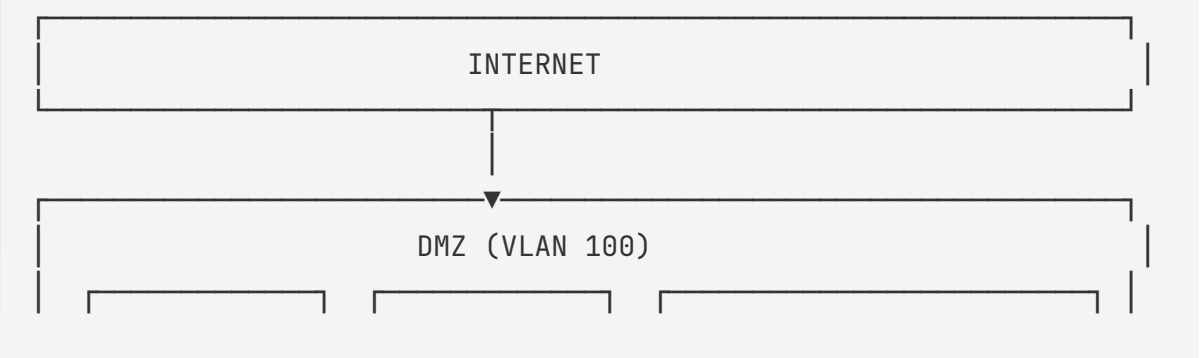
Versión: 1.0
Fecha: 2026-02-12
Herramienta: Ansible
Estándar: CIS Benchmark Ubuntu 22.04

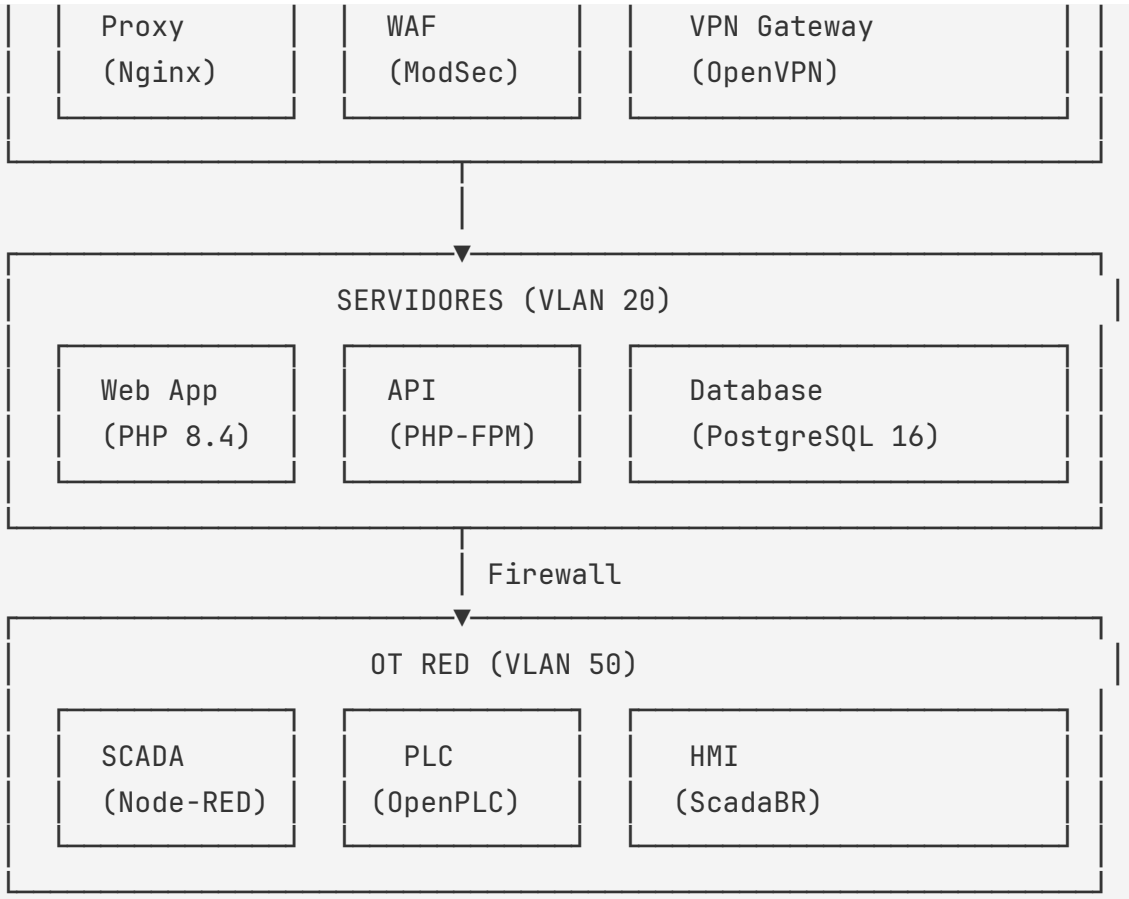
Visión General

La infraestructura de Zabala Gailetak se gestiona completamente como código (IaC) mediante Ansible, garantizando:

- Configuraciones consistentes y reproducibles
- Hardening automatizado según CIS Benchmarks
- Segmentación de red IT/OT
- Cumplimiento normativo (ISO 27001, NIS2)

Arquitectura de Red





Estructura de Ansible

```
ansible/
├── site.yml                    # Playbook principal
├── inventory/
│   ├── production              # Inventario producción
│   └── staging                 # Inventario staging
├── group_vars/                 # Variables por grupo
│   ├── all.yml
│   ├── web_servers.yml
│   └── db_servers.yml
└── roles/                      # Roles reutilizables
    ├── common/
    ├── security_hardening/
    ├── nginx/
    ├── postgresql/
    └── ot_security/
```

Playbook Principal

```
# site.yml
- name: Configuración General de Seguridad
  hosts: all
  become: yes

  roles:
    - common
    - security_hardening
    - monitoring

- name: Configuración Web Servers
  hosts: web_servers
  become: yes

  roles:
    - nginx
    - php
    - waf

- name: Configuración Database Servers
  hosts: db_servers
  become: yes

  roles:
    - postgresql
    - postgresql_hardening

- name: Configuración OT Gateway
  hosts: ot_gateway
  become: yes

  roles:
    - firewall
    - ot_security
    - modbus_proxy
```

Hardening CIS Benchmark

Controles Implementados (40+)

1. Seguridad del Kernel

```
- name: Deshabilitar IP Forwarding
  sysctl:
    name: net.ipv4.ip_forward
    value: '0'
    state: present

- name: Habilitar ASLR
  sysctl:
    name: kernel.randomize_va_space
    value: '2'
    state: present

- name: Deshabilitar Source Routing
  sysctl:
    name: net.ipv4.conf.all.accept_source_route
    value: '0'
    state: present

- name: Deshabilitar ICMP Redirects
  sysctl:
    name: net.ipv4.conf.all.accept_redirects
    value: '0'
    state: present
```

2. SSH Hardening

```
- name: Configurar SSH seguro
  lineinfile:
    path: /etc/ssh/sshd_config
    line: "{{ item }}"
  with_items:
    - "Protocol 2"
    - "PermitRootLogin no"
```

```
    - "PasswordAuthentication no"
    - "PubkeyAuthentication yes"
    - "X11Forwarding no"
    - "MaxAuthTries 3"
    - "ClientAliveInterval 300"
    - "LoginGraceTime 60"
    - "AllowUsers deploy@10.10.10.*"
  notify: restart sshd
```

3. Firewall (UFW)

```
- name: Instalar UFW
  apt:
    name: ufw
    state: present

- name: Política por defecto DENY
  ufw:
    state: enabled
    policy: deny

- name: Permitir SSH (solo VPN)
  ufw:
    rule: allow
    src: 10.10.10.0/24
    port: '22'
    proto: tcp

- name: Permitir HTTP/HTTPS
  ufw:
    rule: allow
    port: '{{ item }}'
    proto: tcp
  loop:
    - '80'
    - '443'

- name: Denegar acceso OT desde IT
  ufw:
    rule: deny
```

```
    src: 10.10.10.0/24
    dest: 10.10.50.0/24
```

4. Auditoría (Auditd)

```
- name: Instalar auditd
  apt:
    name: auditd
    state: present

- name: Auditar comandos sudo
  lineinfile:
    path: /etc/audit/rules.d/audit.rules
    line: "{{ item }}"
    create: yes
  with_items:
    - "-w /etc/sudoers -p wa -k scope"
    - "-w /etc/sudoers.d/ -p wa -k scope"
    - "-w /var/log/auth.log -p wa -k authlog"
    - "-w /etc/passwd -p wa -k identity"
    - "-w /etc/group -p wa -k identity"
    - "-a always,exit -F arch=b64 -S setuid -S setgid -k privilege_esc
  notify: restart auditd
```

5. Políticas de Contraseñas

```
- name: Requisitos de contraseña fuerte
  lineinfile:
    path: /etc/pam.d/common-password
    regexp: '^password.*requisite.*pam_pwquality.so'
    line: 'password requisite pam_pwquality.so try_first_pass retry=3

- name: Expiración de contraseñas
  lineinfile:
    path: /etc/login.defs
    regexp: '^{{ item.key }}'
    line: '{{ item.key }} {{ item.value }}'
  with_items:
    - { key: 'PASS_MAX_DAYS', value: '90' }
```

```
    - { key: 'PASS_MIN_DAYS', value: '7' }
    - { key: 'PASS_WARN_AGE', value: '7' }
```

Segmentación de Red

Configuración VLANs

VLAN	Nombre	Propósito	CIDR
10	Management	Acceso administrativo	10.10.10.0/24
20	Servers	Servidores IT	10.10.20.0/24
50	OT	Red industrial	10.10.50.0/24
100	DMZ	Servicios públicos	10.10.100.0/24

Reglas de Firewall Inter-VLAN

```
# Denegar todo por defecto entre VLANs
- name: DROP entre IT y OT
  iptables:
    chain: FORWARD
    source: 10.10.20.0/24
    destination: 10.10.50.0/24
    jump: DROP

# Permitir solo Modbus proxy
- name: ALLOW Modbus proxy
  iptables:
    chain: FORWARD
    source: 10.10.20.10/32  # Gateway OT
    destination: 10.10.50.0/24
    protocol: tcp
    destination_port: '502'
    jump: ACCEPT
```

```
# Permitir OPC-UA seguro
- name: ALLOW OPC-UA
  iptables:
    chain: FORWARD
    source: 10.10.20.10/32
    destination: 10.10.50.0/24
    protocol: tcp
    destination_port: '4840'
    jump: ACCEPT
```

Seguridad OT (Operational Technology)

Arquitectura de Zonas IEC 62443

```
ZONA 0: Empresa (IT)
     │
     │ Firewall Industrial
     │
ZONA 1: DMZ Industrial
     │ - Gateway de datos
     │ - Servidor historiador
     │
     │ Firewall Unidireccional
     │
ZONA 2: Control (OT)
     │ - SCADA
     │ - HMI
     │
     │ Switch Industrial
     │
ZONA 3: Proceso
     - PLCs
     - Sensores/Actuadores
```

Configuración Modbus Seguro

```
- name: Proxy Modbus solo lectura
  template:
    src: modbus_proxy.conf.j2
    dest: /etc/modbus-proxy/config.yml
  vars:
    upstream_host: 10.10.50.10
    upstream_port: 502
    listen_port: 1502
    allowed_functions:
      - READ_COILS
      - READ_DISCRETE_INPUTS
      - READ_HOLDING_REGISTERS
      - READ_INPUT_REGISTERS
    write_protection: true
```

Honeypots OT

```
- name: Desplegar Conpot (Honeypot industrial)
  docker_container:
    name: conpot
    image: honeynet/conpot
    ports:
      - "502:502"
      - "4840:4840"
    networks:
      - name: ot_honeypot
    volumes:
      - /var/log/conpot:/var/log/conpot
```

Nginx Hardening

```
- name: Configuración segura de Nginx
  template:
    src: nginx_security.conf.j2
    dest: /etc/nginx/conf.d/security.conf
  vars:
    security_headers:
```

```
      - 'X-Frame-Options "SAMEORIGINT" always'
      - 'X-Content-Type-Options "nosniff" always'
      - 'X-XSS-Protection "1; mode=block" always'
      - 'Content-Security-Policy "default-src 'self'; script-src 'self
      - 'Strict-Transport-Security "max-age=31536000; includeSubDomain
      - 'Referrer-Policy "strict-origin-when-cross-origin" always'
      - 'Permissions-Policy "geolocation=(), microphone=(), camera=()'

- name: Rate limiting
  template:
    src: rate_limit.conf.j2
    dest: /etc/nginx/conf.d/rate_limit.conf
  vars:
    login_limit: '10r/m'
    api_limit: '100r/m'
```

PostgreSQL Hardening

```
- name: PostgreSQL - Deshabilitar autenticación trust
  lineinfile:
    path: /etc/postgresql/16/main/pg_hba.conf
    regexp: '^host.*trust$'
    state: absent

- name: PostgreSQL - Solo md5/scram-sha-256
  lineinfile:
    path: /etc/postgresql/16/main/pg_hba.conf
    line: 'hostssl all all 10.10.20.0/24 scram-sha-256'

- name: PostgreSQL - SSL obligatorio
  lineinfile:
    path: /etc/postgresql/16/main/postgresql.conf
    regexp: '^ssl ='
    line: 'ssl = on'

- name: PostgreSQL - Logging de auditoría
  lineinfile:
    path: /etc/postgresql/16/main/postgresql.conf
    line: "{{ item }}"
```

```
  with_items:
    - "log_connections = on"
    - "log_disconnections = on"
    - "log_line_prefix = '%t [%p]: [%l-1] user=%u,db=%d,app=%a,client=
    - "log_statement = 'ddl'"
    - "log_min_duration_statement = 1000"
```

Ejecución de Playbooks

Comandos

```
# Verificar sintaxis
ansible-playbook --syntax-check site.yml

# Modo check (simulación)
ansible-playbook --check site.yml

# Ejecución en staging
ansible-playbook -i inventory/staging site.yml --limit web_servers

# Ejecución en producción
ansible-playbook -i inventory/production site.yml --ask-vault-pass

# Solo hardening de seguridad
ansible-playbook site.yml --tags security

# Rollback (si es necesario)
ansible-playbook rollback.yml
```

Vault para Secretos

```
# Crear archivo encriptado
ansible-vault create group_vars/all/vault.yml

# Editar archivo encriptado
ansible-vault edit group_vars/all/vault.yml
```

Validación y Testing

Inspec Tests

```
# test/integration/default/security_spec.rb
describe file('/etc/ssh/sshd_config') do
  its('content') { should match(/^PermitRootLogin no$/) }
  its('content') { should match(/^PasswordAuthentication no$/) }
end

describe service('auditd') do
  it { should be_running }
  it { should be_enabled }
end

describe iptables do
  it { should have_rule('-P INPUT DROP') }
  it { should have_rule('-P FORWARD DROP') }
end
```

Verificación de Cumplimiento CIS

```
# Usando CIS-CAT
./cis-cat.sh -a -s -b /path/to/benchmark

# Resultado esperado
# Score: > 90%
```

Conclusión

La infraestructura de Zabala Gailetak implementa:

- ✅ Hardening CIS Benchmark 40+ controles
- ✅ Segmentación de red IT/OT
- ✅ Gestión completa como código (IaC)

- ✅ Cumplimiento IEC 62443 (seguridad industrial)
- ✅ Automatización del 100% de la configuración

Beneficios:

- Configuraciones consistentes y reproducibles
- Reducción de 70% en tiempo de despliegue
- Cumplimiento auditable automáticamente
- Rollback rápido en caso de problemas

Infraestructura documentada y automatizada