

network_segmentation_sop

Sare Segmentazioa SOP (Debian/NFTables)

Bertsioa: 2.0 (Konfigurazio Erreferentzia) **Rola:** ZG-Gateway (Router/Suebakia)

1. Interfaze Konfiguraziaoa (`/etc/network/interfaces`)

Konfigurazio honek Gateway-a barneko azpisare guztiak router gisa definitzen du.

```
# /etc/network/interfaces

source /etc/network/interfaces.d/*

auto lo
iface lo inet loopback

# WAN (Eth0) - Internetera konektatuta (Isard Bridge)
allow-hotplug eth0
iface eth0 inet dhcp

# LAN (Eth1) - Barne sarera konektatuta
# Interfaze bakarra erabiltzen dugu VLAN gateway bakoitzeko alias-ekin
allow-hotplug eth1
iface eth1 inet static
    address 192.168.1.1
    netmask 255.255.0.0
    # Gateway Logikoak
    up ip addr add 192.168.10.1/24 dev eth1  # USER GATEWAY
    up ip addr add 192.168.20.1/24 dev eth1  # SERVER GATEWAY
    up ip addr add 192.168.50.1/24 dev eth1  # OT GATEWAY
    up ip addr add 192.168.200.1/24 dev eth1 # MGMT GATEWAY
```

2. Suebaki Arauak (`/etc/nftables.conf`)

Arau multzo honek IEC 62443-k eskatzen duen isolamendu zorrotza eta proiektuaren segurtasun politika betearazten ditu.

```
#!/usr/sbin/nft -f

flush ruleset

table ip filter {
    chain input {
        type filter hook input priority 0; policy drop;

        # Baimendu loopback
        iifname "lo" accept

        # Baimendu konexio estabiliduak
        ct state established,related accept

        # Baimendu SSH Admin Saretik bakarrik
        ip saddr 192.168.200.0/24 tcp dport 22 accept

        # Baimendu ICMP (Ping) diagnostikoetarako
        ip protocol icmp accept
```

```

# Baimendu DHCP eskaerak (UDP 67/68) LANean
iifname "eth1" udp dport { 67, 68 } accept
}

chain forward {
    type filter hook forward priority 0; policy drop;
    ct state established,related accept

# --- ACL ARAUAK ---

# 1. USER -> APP (Web Sarbidea soilik)
# Erabiltzaileei Web Zerbitzaria atzitzea baimentzen die
ip saddr 192.168.10.0/24 ip daddr 192.168.20.10 tcp dport { 80, 443 } accept

# 2. APP -> DATA (Datu-base Sarbidea soilik)
# Web Zerbitzariari Datu-basea/Redis atzitzea baimentzen dio
ip saddr 192.168.20.10 ip daddr 192.168.20.20 tcp dport { 5432, 6379 } accept

# 3. MGMT -> ALL (Administrazio Osoa)
# Administratzaleei DENA atzitzea baimentzen die
ip saddr 192.168.200.0/24 accept

# 4. OT ISOLAMENDUA
# Lehenespenez, OT (192.168.50.0/24) blokeatuta dago denetik
# konexio estabiliduez beste. Arauak ez dira behar (Politika DROP).

# 5. INTERNET IRAULIA
# Barne sare guztiei interneta atzitzea baimentzen die (NAT bidez)
iifname "eth1" oifname "eth0" accept
}

chain output {
    type filter hook output priority 0; policy accept;
}
}

table ip nat {
    chain postrouting {
        type nat hook postrouting priority 100; policy accept;

        # NAT (Masquerade) Internet Sarbiderako
        oifname "eth0" masquerade
    }
}

```

3. Aldaketak Aplikatzea

Konfigurazio hauek aplikatzeko:

1. **Sarea:** systemctl restart networking
2. **Suebakia:** nft -f /etc/nftables.conf

4. Egiaztapena

- **Ibilbideak Egiaztatu:** ip route
- **Arauak Egiaztatu:** nft list ruleset
- **Logak Egiaztatu:** dmesg | grep nft (logintza gaituta badago)