Regras de Bloqueio de tráfego

Perfeito 👍
Esse é um cenário **clássico de rede TI com acesso unidirecional**.
Vamos montar **do jeito certo**, simples e sem pegar tráfego indevido.

🎯 Objetivo

- ❌ VLANs **10, 20, 30, 50 NÃO podem acessar** a VLAN **60 (TI)**
- ✅ VLAN **60 (TI) PODE acessar** as VLANs **10, 20, 30, 50**
- ✅ Respostas (return traffic) devem funcionar normalmente

📌 Premissas (ajuste se necessário)

- VLAN 60 → `192.168.60.0/24`
- VLANs bloqueadas:
  - VLAN10 → `192.168.10.0/24`
  - VLAN20 → `192.168.20.0/24`
  - VLAN30 → `192.168.30.0/24`
  - VLAN50 → `192.168.50.0/24`

✅ Regras CORRETAS de Firewall (MikroTik)

🔹 **1️⃣ Sempre permitir conexões estabelecidas**

> **ESSENCIAL**

```
/ip firewall filter
add chain=forward action=accept connection-state=established,related com

```

🔹 **2️⃣ Permitir VLAN 60 acessar TODAS as outras VLANs**

```
add chain=forward action=accept \
    src-address=192.168.60.0/24 \
    dst-address=192.168.0.0/16 \
    comment="TI (VLAN60) -> Outras VLANs"

```

> Se quiser ser mais restrito, dá pra listar rede por rede.

🔹 **3️⃣ Bloquear VLANs 10,20,30,50 acessando a VLAN 60**

aqui eu criei uma Address list e coloquei todas a redes nelas e criei uma regra so

```
add chain=forward action=drop \
    dst-address=192.168.60.0/24 \
    src-address=192.168.10.0/24 \
    comment="Block VLAN10 -> VLAN60"

add chain=forward action=drop \
    dst-address=192.168.60.0/24 \
    src-address=192.168.20.0/24 \
    comment="Block VLAN20 -> VLAN60"

add chain=forward action=drop \
    dst-address=192.168.60.0/24 \
    src-address=192.168.30.0/24 \
    comment="Block VLAN30 -> VLAN60"

add chain=forward action=drop \
    dst-address=192.168.60.0/24 \
    src-address=192.168.50.0/24 \
    comment="Block VLAN50 -> VLAN60"

```

🔁 Ordem FINAL das regras (muito importante)

```
1. Accept established,related
2. Accept VLAN60 → VLANs
3. Drop VLANs → VLAN60

```

Se inverter a ordem, **quebra tudo**.

🧠 Dica profissional (mais limpo)

Você pode usar **address-list** para facilitar manutenção:

📋 Criar lista das VLANs não-TI

```
/ip firewall address-list
add list=VLANs-Usuarios address=192.168.10.0/24
add list=VLANs-Usuarios address=192.168.20.0/24
add list=VLANs-Usuarios address=192.168.30.0/24
add list=VLANs-Usuarios address=192.168.50.0/24

```

🔐 Bloqueio com uma única regra

```
/ip firewall filter
add chain=forward action=drop \
    src-address-list=VLANs-Usuarios \
    dst-address=192.168.60.0/24 \
    comment="Block VLANs -> VLAN60"

```

🧪 Testes esperados

Origem	Destino	Resultado
VLAN60	VLAN10/20/30/50	✅ OK
VLAN10/20/30/50	VLAN60	❌ BLOQUEADO
VLAN60	Internet	✅ OK

VLANs	Internet	✅ OK

Se quiser, posso:

- Ajustar isso **por interface (in-interface vlanX)**
- Criar exceção (ex: impressora, servidor, Zabbix)
- Validar com `torch` / `connection print`

Só me diga 👌