Pi-hole with Tailscale Security Setup

Important Notes

1. **Rule order matters** - iptables reads top-to-bottom, stops at first match

2. **ACCEPT** rules **MUST** come before **DROP** rules

3. **ts-input MUST** be the first rule in INPUT chain

4. Keep **"Permit all origins"** enabled in Pi-hole for Tailscale to work

5. Firewall blocks public access, Pi-hole setting allows Tailscale interface

Prerequisites

• Pi-hole installed and running

• Tailscale installed and connected

• **"Permit all origins"** enabled in Pi-hole settings

Step 1: Check Current Firewall Status

```
sudo iptables -L -n -v
```

Step 2: Install iptables-persistent

```
sudo apt install iptables-persistent -y
```

• Select **No** for both IPv4 and IPv6 prompts

Step 3: Add Firewall Rules

```
# Flush all INPUT rules

sudo iptables -F INPUT

# Re-add ts-input (MUST be first)
```

```
sudo iptables -I INPUT 1 -j ts-input

# DNS: ACCEPT localhost

sudo iptables -A INPUT -s 127.0.0.1 -p udp --dport 53 -j ACCEPT

sudo iptables -A INPUT -s 127.0.0.1 -p tcp --dport 53 -j ACCEPT

# DNS: ACCEPT Tailscale

sudo iptables -A INPUT -s 100.64.0.0/10 -p udp --dport 53 -j ACCEPT

sudo iptables -A INPUT -s 100.64.0.0/10 -p tcp --dport 53 -j ACCEPT

# DNS: ACCEPT local network

sudo iptables -A INPUT -s 192.168.1.0/24 -p udp --dport 53 -j ACCEPT

sudo iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 53 -j ACCEPT

# DNS: DROP everyone else

sudo iptables -A INPUT -p udp --dport 53 -j DROP

sudo iptables -A INPUT -p tcp --dport 53 -j DROP

# Web: ACCEPT Tailscale

sudo iptables -A INPUT -s 100.64.0.0/10 -p tcp --dport 80 -j ACCEPT

# Web: ACCEPT local network

sudo iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 80 -j ACCEPT

# Web: DROP everyone else

sudo iptables -A INPUT -p tcp --dport 80 -j DROP
```

Step 4: Save Rules

```
sudo netfilter-persistent save
```

Step 5: Verify Rules

```
sudo iptables -L -n -v
```

Expected order in **INPUT** chain:

1. **ts-input**
2. **ACCEPT** from **100.64.0.0/10** (udp/tcp port 53)
3. **ACCEPT** from **192.168.1.0/24** (udp/tcp port 53)
4. **DROP** all others (udp/tcp port 53)
5. **ACCEPT** from **100.64.0.0/10** (tcp port 80)
6. **ACCEPT** from **192.168.1.0/24** (tcp port 80)
7. **DROP** all others (tcp port 80)

Troubleshooting: Flush and Re-add Rules

If rules are in wrong order or duplicated:

```
# Flush all INPUT rules
sudo iptables -F INPUT
# Re-add Tailscale ts-input jump (MUST be first)
sudo iptables -I INPUT 1 -j ts-input
# DNS: ACCEPT Tailscale
sudo iptables -A INPUT -s 100.64.0.0/10 -p udp --dport 53 -j ACCEPT
sudo iptables -A INPUT -s 100.64.0.0/10 -p tcp --dport 53 -j ACCEPT
# DNS: ACCEPT local network
sudo iptables -A INPUT -s 192.168.1.0/24 -p udp --dport 53 -j ACCEPT
sudo iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 53 -j ACCEPT
# DNS: DROP everyone else
sudo iptables -A INPUT -p udp --dport 53 -j DROP
sudo iptables -A INPUT -p tcp --dport 53 -j DROP
```

```
# Web: ACCEPT Tailscale
sudo iptables -A INPUT -s 100.64.0.0/10 -p tcp --dport 80 -j ACCEPT
# Web: ACCEPT local network
sudo iptables -A INPUT -s 192.168.1.0/24 -p tcp --dport 80 -j ACCEPT
# Web: DROP everyone else
sudo iptables -A INPUT -p tcp --dport 80 -j DROP
# Save
sudo netfilter-persistent save
# Verify
sudo iptables -L -n -v
```

What Each Rule Does

ACCEPT = Allow traffic

DROP = Block traffic silently

100.64.0.0/10 = Tailscale IP range (covers 100.64.0.0 - 100.127.255.255)

192.168.1.0/24 = Local network subnet (adjust to match your network)

Port 53 = DNS queries

Port 80 = Pi-hole web interface
