Setting Up Exit Node on Ubuntu Server:

Reference: https://tailscale.com/docs/features/exit-nodes?tab=linux

Enable IP forwarding to advertise your Linux device as an exit node.

If your system has a `/etc/sysctl.d` directory, use:

```
echo 'net.ipv4.ip_forward = 1' | sudo tee -a /etc/sysctl.d/99-tailscale.conf
echo 'net.ipv6.conf.all.forwarding = 1' | sudo tee -a /etc/sysctl.d/99-tailscale.conf
sudo sysctl -p /etc/sysctl.d/99-tailscale.conf
```

Otherwise, use:

```
echo 'net.ipv4.ip_forward = 1' | sudo tee -a /etc/sysctl.conf
echo 'net.ipv6.conf.all.forwarding = 1' | sudo tee -a /etc/sysctl.conf
sudo sysctl -p /etc/sysctl.conf
```

Securing Your Ubuntu Home Server as an Exit Node:

Why This Matters:

When you enable an exit node on your home server, it acts as a network gateway open to the internet, which creates MAJOR security issues. Open ports are easily targeted by hackers:

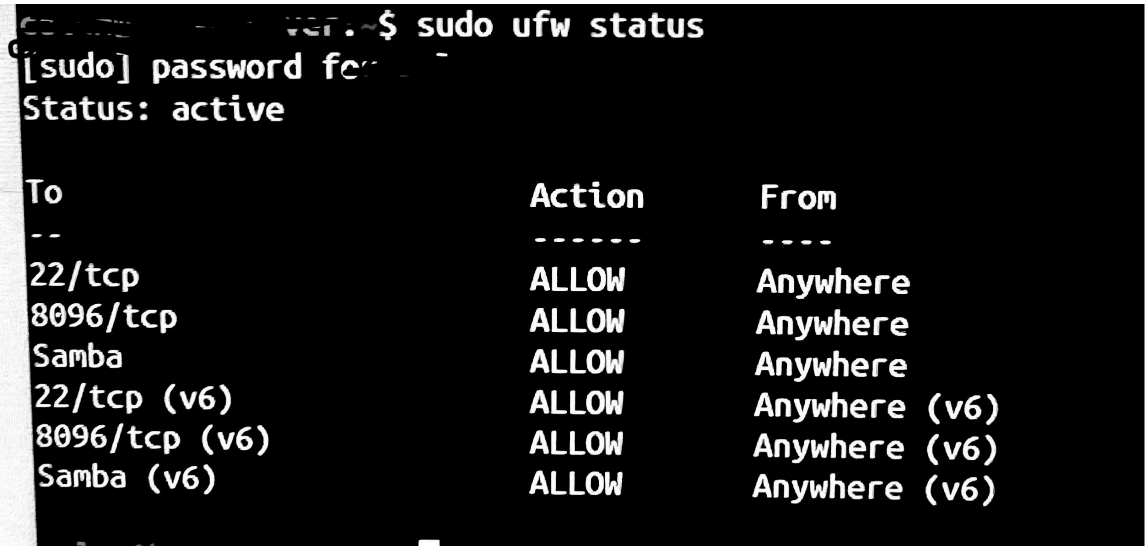
In case you have not had firewall installed on your home server, then following these command

To install Firewall:

- Ensure your package list is updated: `sudo apt update`
- Install Firewall: `sudo apt install ufw`
- Enable the Firewall: `sudo ufw enable`
- Check that the firewall is active: `sudo ufw status (verbose)`

But if you already have firewall install, then use this command to check `sudo ufw status (verbose)`

For example i have SSH, JellyFin, Samba port allowed in my home server



```
[redacted]:~$ sudo ufw status
[sudo] password for [redacted]
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
8096/tcp                   ALLOW       Anywhere
Samba                      ALLOW       Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
8096/tcp (v6)              ALLOW       Anywhere (v6)
Samba (v6)                 ALLOW       Anywhere (v6)
```

Seeing that Anywhere is actually a security risk, because "Anywhere" = Anyone on the internet can access, it is okay if you just use in local, however once you use home server as an exit node, your home server will be on the internet and when that happen:

- SSH (22/tcp) - Open to entire internet → Brute force attacks
- Jellyfin (8096) - Open to entire internet → Probably not needed publicly
- Samba - Open to entire internet → CRITICAL RISK - File sharing should NEVER be public

What You Want:

Only Tailscale or local network access, not "Anywhere" (anyone on the internet).

Remove All Public-Facing Rules:

# Remove existing public rules

sudo ufw delete allow 22/tcp

sudo ufw delete allow 8096/tcp

sudo ufw delete allow Samba

# Set default policies

sudo ufw default deny incoming

sudo ufw default allow outgoing

# Allow Tailscale

```
sudo ufw allow in on tailscale0  # Allows everything via Tailscale
sudo ufw allow 41641/udp
```

# Allow all ports from local home network

```
sudo ufw allow from 192.168.1.0/24
```

For Specific Port Access (Optional):

Skip this step if you want all ports opened on both your home server's firewall and Tailscale's firewall. Use this approach if you only want specific ports accessible.

# Remove the broad rules

```
sudo ufw delete allow from 192.168.1.0/24
sudo ufw delete allow in on tailscale0
```

# Home network access (specific ports)

```
sudo ufw allow from 192.168.1.0/24 to any port 22
sudo ufw allow from 192.168.1.0/24 to any port 8096
sudo ufw allow from 192.168.1.0/24 to any port 8123
sudo ufw allow from 192.168.1.0/24 to any port 445
sudo ufw allow from 192.168.1.0/24 to any port 139
```

# Tailscale access (specific ports)

```
sudo ufw allow in on tailscale0 to any port 22

sudo ufw allow in on tailscale0 to any port 8096

sudo ufw allow in on tailscale0 to any port 8123

sudo ufw allow in on tailscale0 to any port 445

sudo ufw allow in on tailscale0 to any port 139
```

# Tailscale WireGuard

```
sudo ufw allow 41641/udp
```

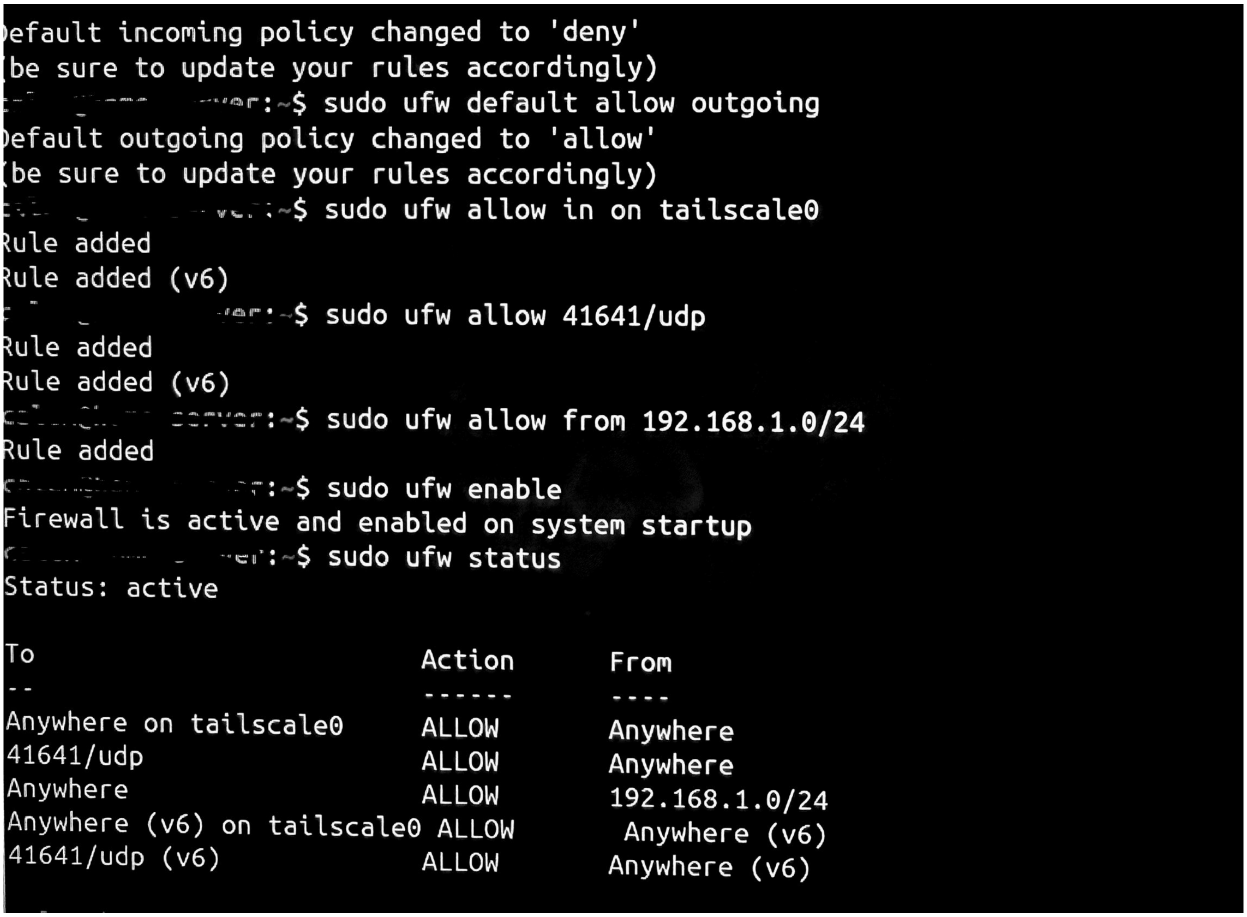
Enable firewall:

```
sudo ufw enable
```

Verify firewall status:

```
sudo ufw status
```

It will look like this



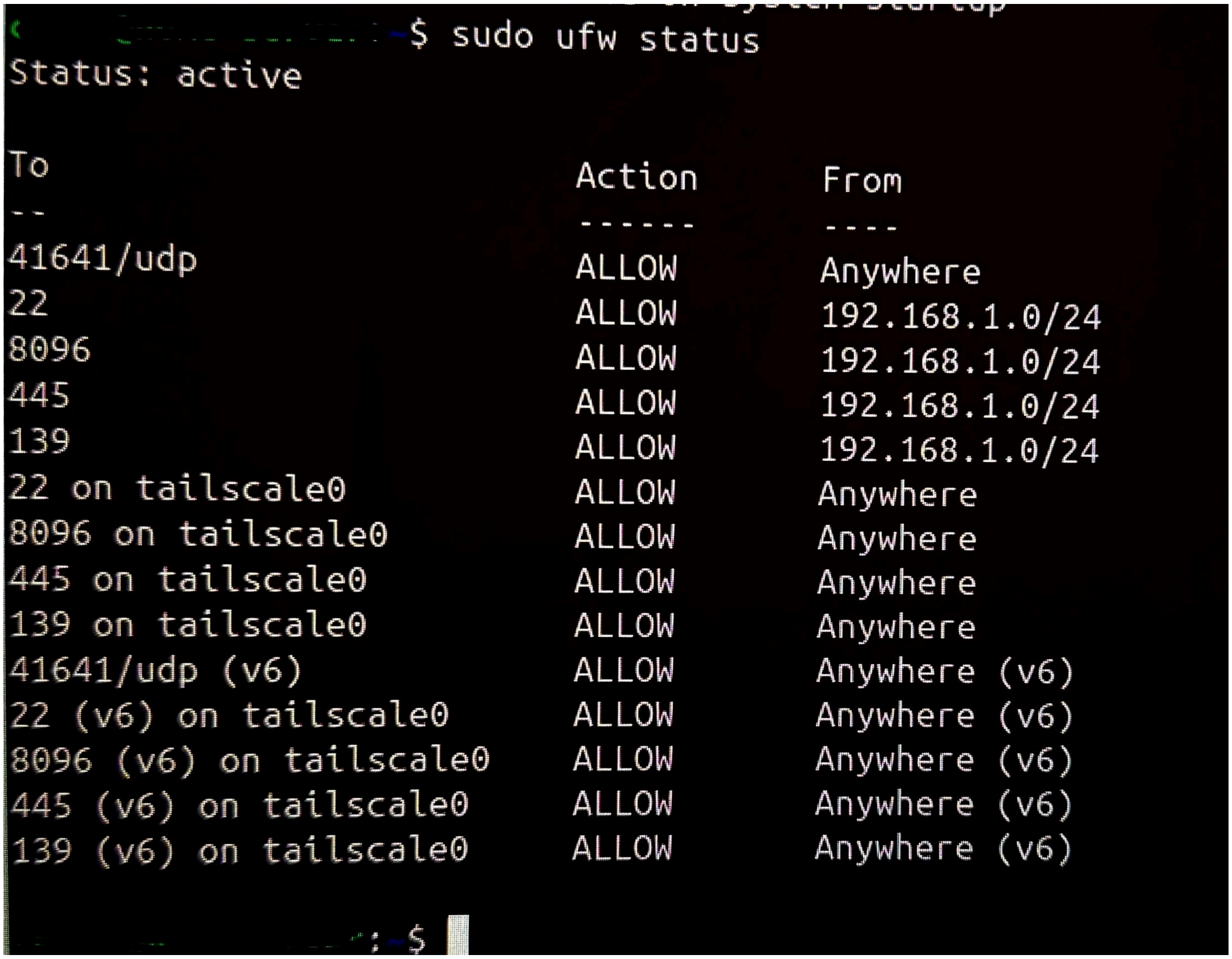
```
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
[redacted]:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
[redacted]:~$ sudo ufw allow in on tailscale0
Rule added
Rule added (v6)
[redacted]:~$ sudo ufw allow 41641/udp
Rule added
Rule added (v6)
[redacted]:~$ sudo ufw allow from 192.168.1.0/24
Rule added
[redacted]:~$ sudo ufw enable
Firewall is active and enabled on system startup
[redacted]:~$ sudo ufw status
Status: active

To                          Action      From
--                          ------      ----
Anywhere on tailscale0      ALLOW       Anywhere
41641/udp                   ALLOW       Anywhere
Anywhere                    ALLOW       192.168.1.0/24
Anywhere (v6) on tailscale0 ALLOW       Anywhere (v6)
41641/udp (v6)              ALLOW       Anywhere (v6)
```

What Changed:

- ✅ SSH, Jellyfin, Samba no longer exposed to internet
- ✅ Only Tailscale and local home network (192.168.1.0/24) can access
- ✅ Both IPv4 and IPv6 covered
- ✅ Firewall enabled on startup

If you set specific ports to be opened on home server's firewall and tailscale's firewall, the status will look like this



```
[redacted]$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
41641/udp                  ALLOW       Anywhere
22                         ALLOW       192.168.1.0/24
8096                       ALLOW       192.168.1.0/24
445                        ALLOW       192.168.1.0/24
139                        ALLOW       192.168.1.0/24
22 on tailscale0           ALLOW       Anywhere
8096 on tailscale0         ALLOW       Anywhere
445 on tailscale0          ALLOW       Anywhere
139 on tailscale0          ALLOW       Anywhere
41641/udp (v6)             ALLOW       Anywhere (v6)
22 (v6) on tailscale0      ALLOW       Anywhere (v6)
8096 (v6) on tailscale0    ALLOW       Anywhere (v6)
445 (v6) on tailscale0     ALLOW       Anywhere (v6)
139 (v6) on tailscale0     ALLOW       Anywhere (v6)

[redacted]:~$
```

Final Step - Enable Exit Node:

1. Go to Tailscale Admin Console
2. Find your Ubuntu server
3. Click "Edit route settings" (3 dots menu)
4. Enable "Use as exit node"
5. Approve it

Additional Security - SSH Key Authentication:

For long-term security when using SSH:

```
# On your client device
```

```
        ssh-keygen

        ssh-copy-id user@server-ip


# On server, disable password authentication

        sudo nano /etc/ssh/sshd_config

# Set: PasswordAuthentication no

        sudo systemctl restart sshd
```

Important Note:

Question: Does this mean when I'm outside the home network, I can only access those ports and not browse the internet?

Answer: The exit node still works! Port restrictions only affect accessing services ON the server (SSH, Jellyfin, etc.).

Exit node functionality is separate:

- **Exit node** = Your client routes ALL internet traffic through the server
- **Port restrictions** = What services you can access on the server itself

You can still browse the internet through the exit node because:

- IP forwarding is enabled
- Default outgoing traffic is allowed (`sudo ufw default allow outgoing`)
- Exit node routing happens at network layer, not specific ports

With restricted ports:

- ✅ Browse internet via exit node when outside
- ✅ Access SSH/Jellyfin/Samba/Home Assistant via Tailscale
- ❌ Access other random ports on server via Tailscale