**Linux UFW (Uncomplicated Firewall) Configuration Guide**

This guide covers setting up and configuring UFW on Ubuntu and other Debian-based Linux distributions.

**Step 1: Install UFW**

# Ubuntu/Debian  
sudo apt update  
sudo apt install ufw

**Step 2: Check UFW Status**

# Check current status  
sudo ufw status  
  
# Check detailed status  
sudo ufw status verbose  
  
# Check numbered rules (useful for deletion)  
sudo ufw status numbered

**Step 3: Enable UFW**

# Allow SSH first

sudo ufw allow ssh  
# Enable UFW  
sudo ufw enable

**Step 4: List Current Rules**

# Show active rules  
sudo ufw status verbose  
  
# Show rules with numbers  
sudo ufw status numbered  
  
# Show raw iptables rules (advanced)  
sudo iptables -L -n -v

**Step 5: Block Telnet Traffic (Port 23)**

# Block incoming Telnet connections  
sudo ufw deny in 23/tcp  
  
# Alternative syntax  
sudo ufw deny telnet  
  
# Verify the rule  
sudo ufw status

**Step 6: Test the Telnet Block**

# Install telnet client if needed  
sudo apt install telnet  
  
# Test connection (should fail)  
telnet localhost 23  
  
# Test with timeout  
timeout 5 telnet localhost 23  
  
# Check with netcat  
nc -zv localhost 23  
  
# Check listening services  
ss -tlnp | grep :23

**Step 7: Allow SSH (Port 22)**

# Allow SSH (if not already done)  
sudo ufw allow ssh  
  
# Or be more specific  
sudo ufw allow in 22/tcp  
  
# Allow from specific IP only (more secure)  
sudo ufw allow from 192.168.1.100 to any port 22

**Step 8: Test SSH Access**

# Test SSH locally  
ssh localhost  
  
# Test from another machine  
ssh username@your-server-ip  
  
# Check SSH service  
systemctl status ssh

**Step 9: Document Current Configuration**

# Save current rules to file  
sudo ufw status verbose > ufw-rules-backup.txt  
  
# Save iptables rules (underlying rules)  
sudo iptables-save > iptables-backup.rules  
  
# View configuration files  
cat /etc/ufw/before.rules  
cat /etc/ufw/after.rules  
cat /etc/ufw/ufw.conf

**Step 10: Remove Test Rules**

# Remove Telnet block rule  
sudo ufw delete deny in 23/tcp  
  
# Alternative: use rule number  
sudo ufw status numbered  
sudo ufw delete [number]  
  
# Verify removal  
sudo ufw status verbose

**Advanced Configuration**

**Application Profiles**

# List available application profiles  
sudo ufw app list  
  
# Get info about specific app  
sudo ufw app info OpenSSH  
  
# Allow application  
sudo ufw allow OpenSSH

**Logging**

# Enable logging  
sudo ufw logging on  
  
# Set logging level  
sudo ufw logging medium  
  
# View logs  
sudo tail -f /var/log/ufw.log

**Default Policies**

# Set default policies  
sudo ufw default deny incoming  
sudo ufw default allow outgoing  
sudo ufw default deny forward

**Verification Commands**

# Check firewall status  
sudo ufw status verbose  
  
# Test specific ports  
nc -zv localhost 22 # SSH (should work)  
nc -zv localhost 23 # Telnet (should fail)  
  
# Check listening services  
ss -tlnp  
  
# View recent connections in log  
sudo tail -20 /var/log/ufw.log  
  
# Show iptables rules created by UFW  
sudo iptables -L ufw-user-input -v