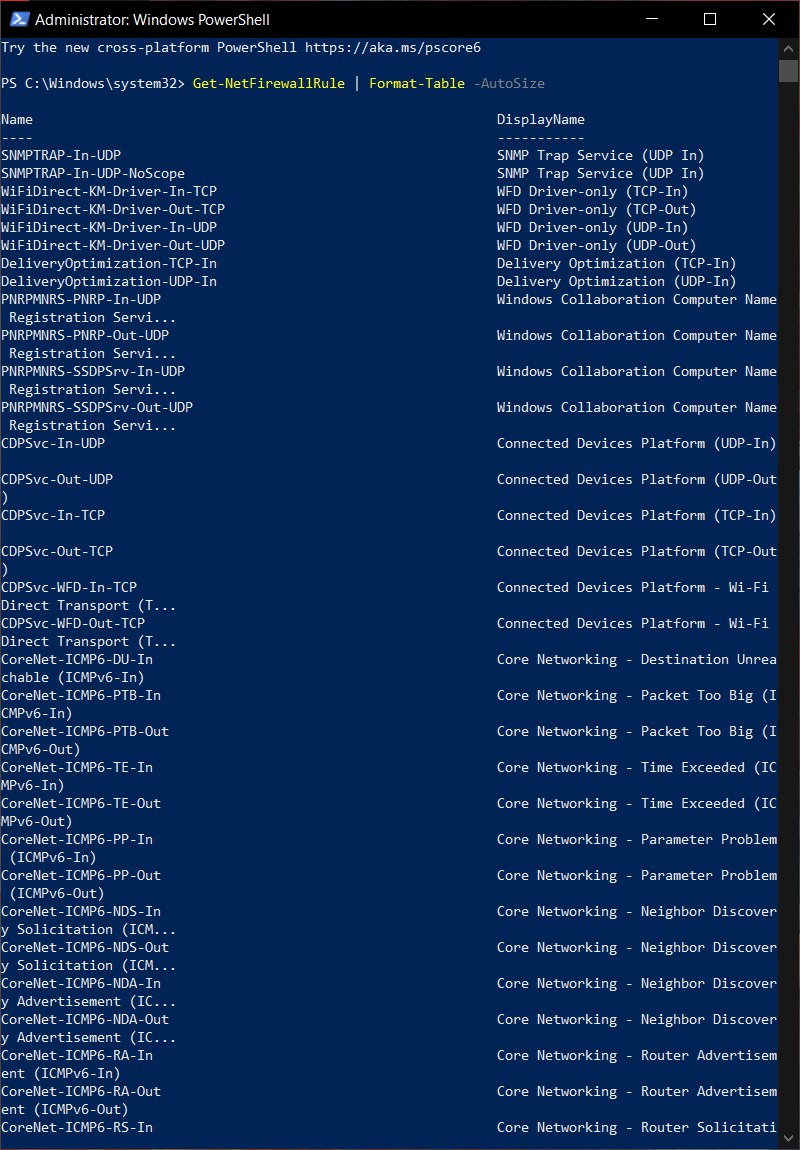
# **Firewall Configuration using Windows PowerShell and Linux iptables**

**1. Windows PowerShell Commands**

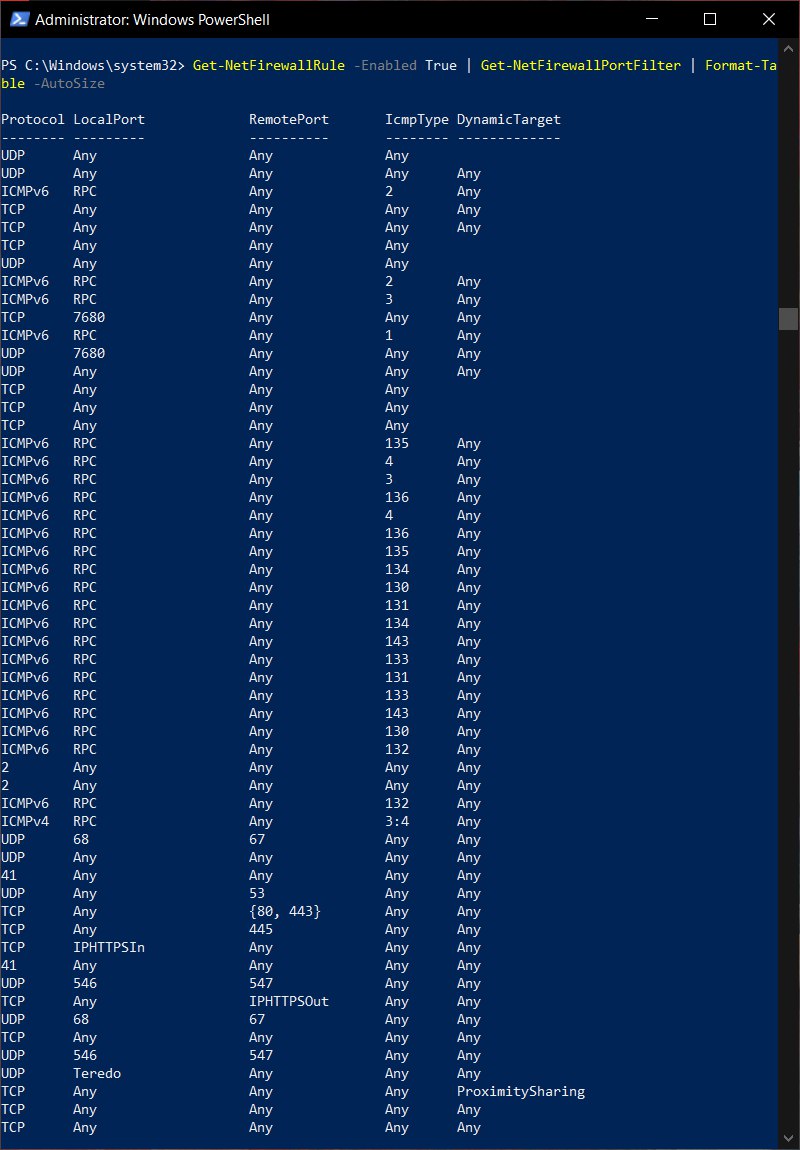
# List all firewall rules

Get-NetFirewallRule | Format-Table -AutoSize



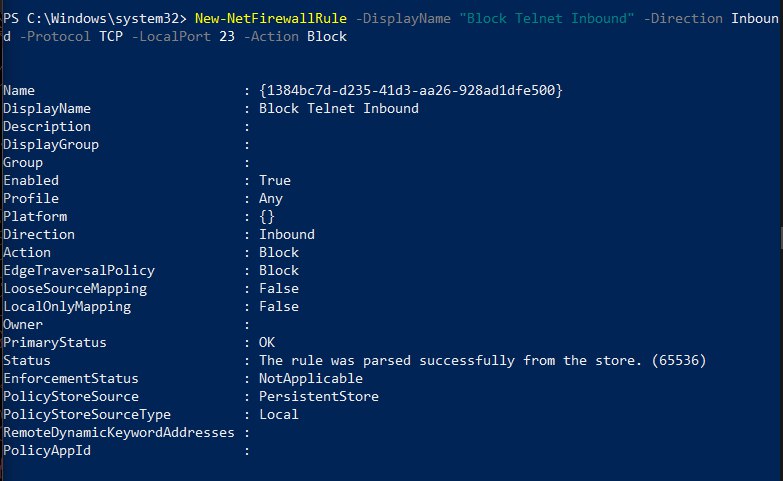
# Show active rules with ports/protocols

Get-NetFirewallRule -Enabled True | Get-NetFirewallPortFilter | Format-Table -AutoSize



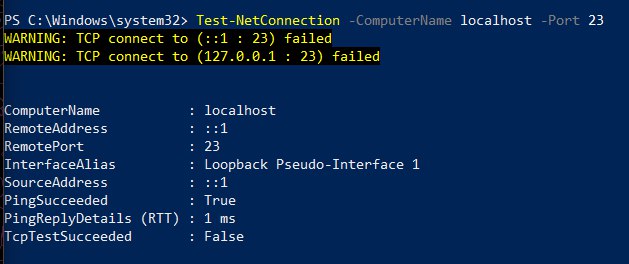
# Block inbound TCP port 23 (Telnet)

New-NetFirewallRule -DisplayName "Block Telnet Inbound" -Direction Inbound -Protocol TCP -LocalPort 23 -Action Block



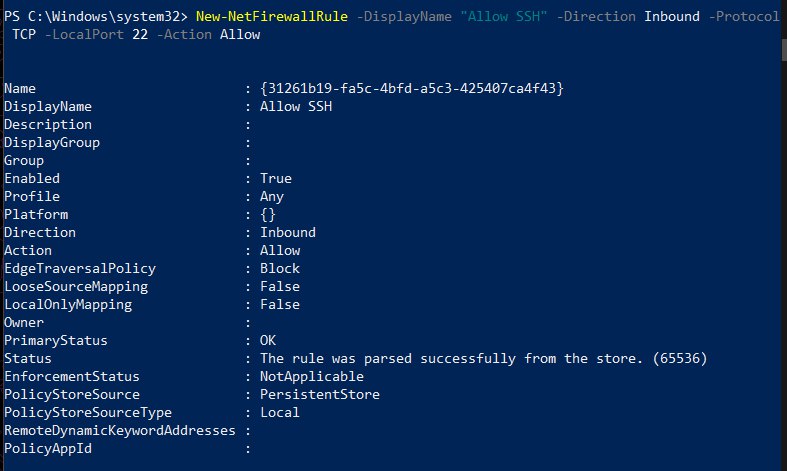
# Test connectivity on port 23

Test-NetConnection -ComputerName localhost -Port 23



# Allow inbound SSH (port 22)

New-NetFirewallRule -DisplayName "Allow SSH" -Direction Inbound -Protocol TCP -LocalPort 22 -Action Allow



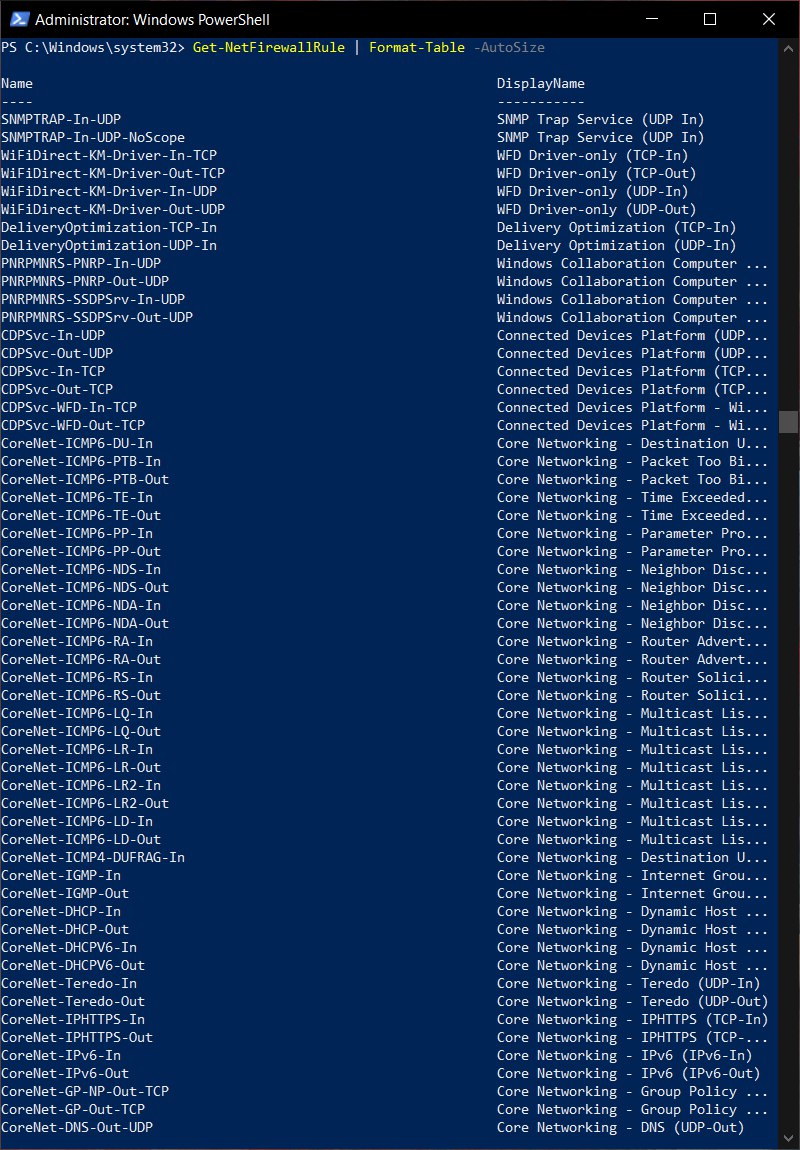
# Remove Telnet block rule

Remove-NetFirewallRule -DisplayName "Block Telnet Inbound"



# Verify firewall rules again

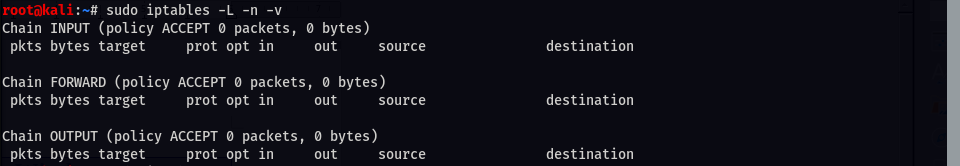
Get-NetFirewallRule | Format-Table -AutoSize



**2. Linux iptables Commands**

# List current iptables rules

sudo iptables -L -n -v



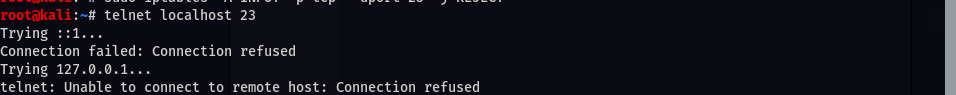
# Block incoming TCP traffic on port 23 (Telnet)

sudo iptables -A INPUT -p tcp --dport 23 -j REJECT



# Test connectivity on port 23

telnet localhost 23



# Allow SSH (port 22)

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT



# Remove Telnet block rule

sudo iptables -D INPUT -p tcp --dport 23 -j REJECT



# Verify all rules cleared

sudo iptables -L -n -v

