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 rule locally
nc -vz localhost 23

# Test rule remotely
nc -vz <target-ip> 23
nmap -p 23 <target-ip>

# 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

# Reset all iptables rules (full flush)
sudo iptables -F
sudo iptables -X
sudo iptables -t nat -F
sudo iptables -t nat -X
sudo iptables -t mangle -F
sudo iptables -t mangle -X
sudo iptables -P INPUT ACCEPT
```

```
sudo iptables -P FORWARD ACCEPT
sudo iptables -P OUTPUT ACCEPT

# Verify all rules cleared
sudo iptables -L -n -v

# Apply safe default firewall rules
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# Check active rules after applying secure baseline
sudo iptables -L -n -v
```