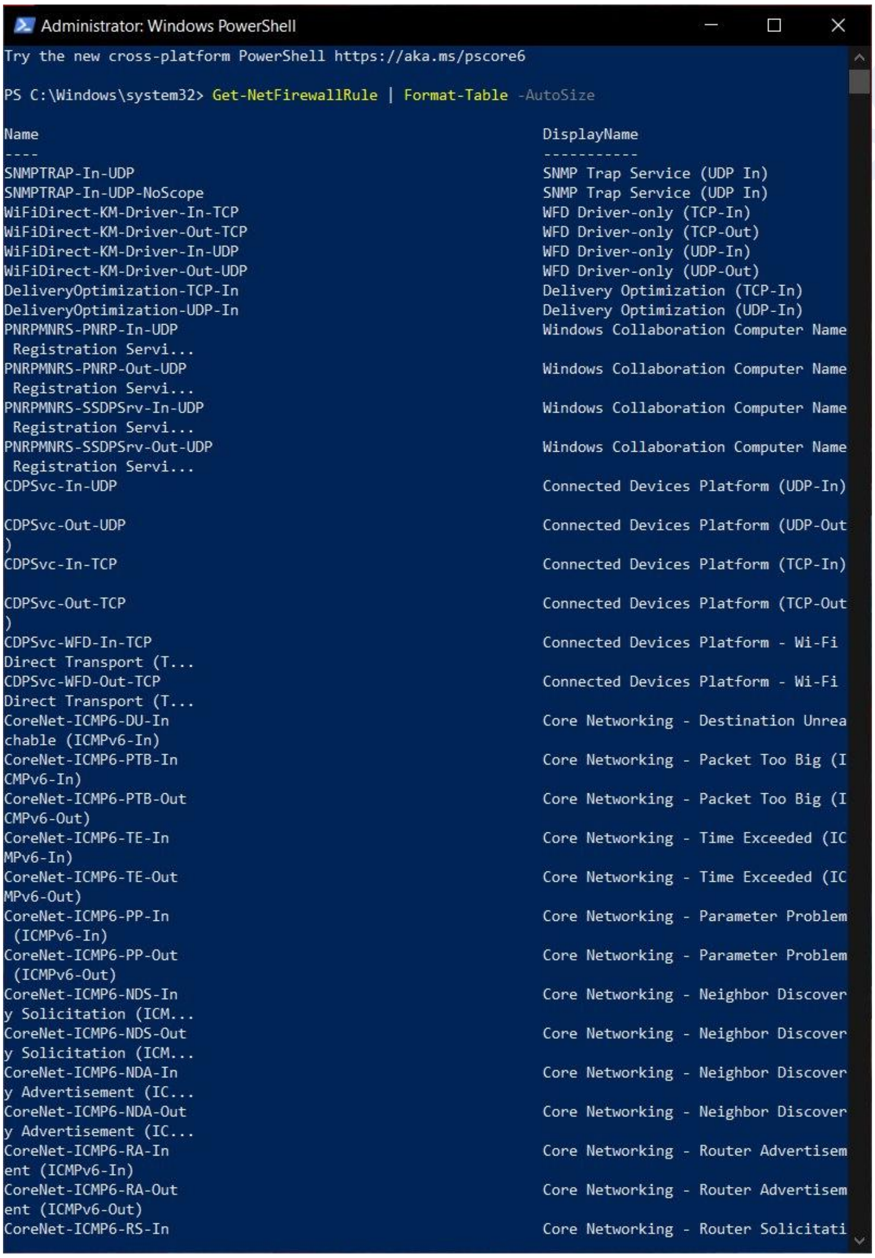
Firewall Configuration using Windows PowerShell and Linux iptables

1. Windows PowerShell Commands

# List all firewall rules

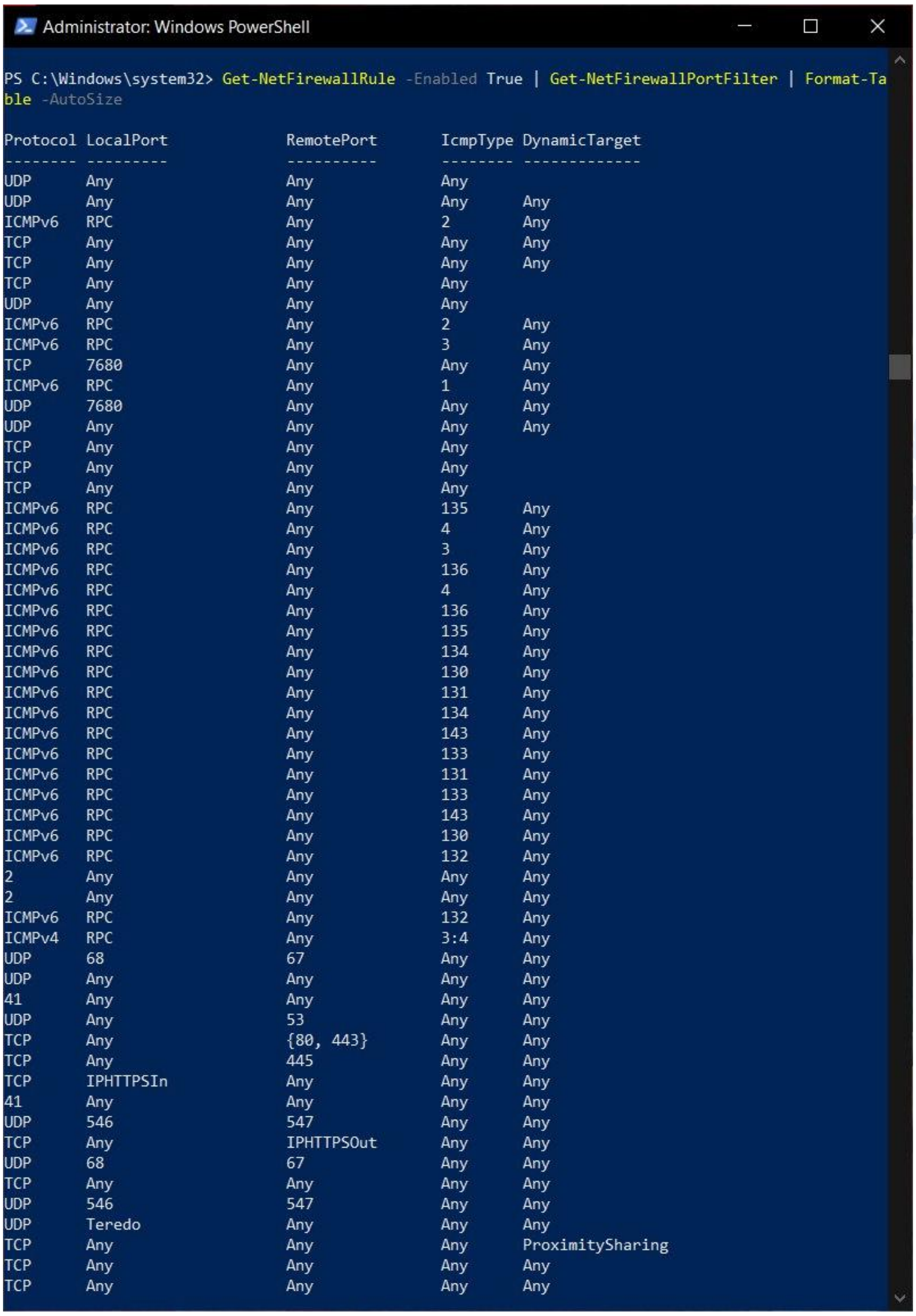
Get-NetFirewallRule | Format-Table -AutoSize



```
Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Get-NetFirewallRule | Format-Table -AutoSize

Name                                                          DisplayName
----                                                          -----------
SNMPTRAP-In-UDP                                               SNMP Trap Service (UDP In)
SNMPTRAP-In-UDP-NoScope                                       SNMP Trap Service (UDP In)
WiFiDirect-KM-Driver-In-TCP                                   WFD Driver-only (TCP-In)
WiFiDirect-KM-Driver-Out-TCP                                  WFD Driver-only (TCP-Out)
WiFiDirect-KM-Driver-In-UDP                                   WFD Driver-only (UDP-In)
WiFiDirect-KM-Driver-Out-UDP                                  WFD Driver-only (UDP-Out)
DeliveryOptimization-TCP-In                                   Delivery Optimization (TCP-In)
DeliveryOptimization-UDP-In                                   Delivery Optimization (UDP-In)
PNRPMNRS-PNRP-In-UDP                                          Windows Collaboration Computer Name
 Registration Servi...
PNRPMNRS-PNRP-Out-UDP                                         Windows Collaboration Computer Name
 Registration Servi...
PNRPMNRS-SSDPSrv-In-UDP                                       Windows Collaboration Computer Name
 Registration Servi...
PNRPMNRS-SSDPSrv-Out-UDP                                      Windows Collaboration Computer Name
 Registration Servi...
CDPSvc-In-UDP                                                 Connected Devices Platform (UDP-In)

CDPSvc-Out-UDP                                                Connected Devices Platform (UDP-Out
)
CDPSvc-In-TCP                                                 Connected Devices Platform (TCP-In)

CDPSvc-Out-TCP                                                Connected Devices Platform (TCP-Out
)
CDPSvc-WFD-In-TCP                                             Connected Devices Platform - Wi-Fi
Direct Transport (T...
CDPSvc-WFD-Out-TCP                                            Connected Devices Platform - Wi-Fi
Direct Transport (T...
CoreNet-ICMP6-DU-In                                           Core Networking - Destination Unrea
chable (ICMPv6-In)
CoreNet-ICMP6-PTB-In                                          Core Networking - Packet Too Big (I
CMPv6-In)
CoreNet-ICMP6-PTB-Out                                         Core Networking - Packet Too Big (I
CMPv6-Out)
CoreNet-ICMP6-TE-In                                           Core Networking - Time Exceeded (IC
MPv6-In)
CoreNet-ICMP6-TE-Out                                          Core Networking - Time Exceeded (IC
MPv6-Out)
CoreNet-ICMP6-PP-In                                           Core Networking - Parameter Problem
 (ICMPv6-In)
CoreNet-ICMP6-PP-Out                                          Core Networking - Parameter Problem
 (ICMPv6-Out)
CoreNet-ICMP6-NDS-In                                          Core Networking - Neighbor Discover
y Solicitation (ICM...
CoreNet-ICMP6-NDS-Out                                         Core Networking - Neighbor Discover
y Solicitation (ICM...
CoreNet-ICMP6-NDA-In                                          Core Networking - Neighbor Discover
y Advertisement (IC...
CoreNet-ICMP6-NDA-Out                                         Core Networking - Neighbor Discover
y Advertisement (IC...
CoreNet-ICMP6-RA-In                                           Core Networking - Router Advertisem
ent (ICMPv6-In)
CoreNet-ICMP6-RA-Out                                          Core Networking - Router Advertisem
ent (ICMPv6-Out)
CoreNet-ICMP6-RS-In                                           Core Networking - Router Solicitati
```

Show active rules with ports/protocols

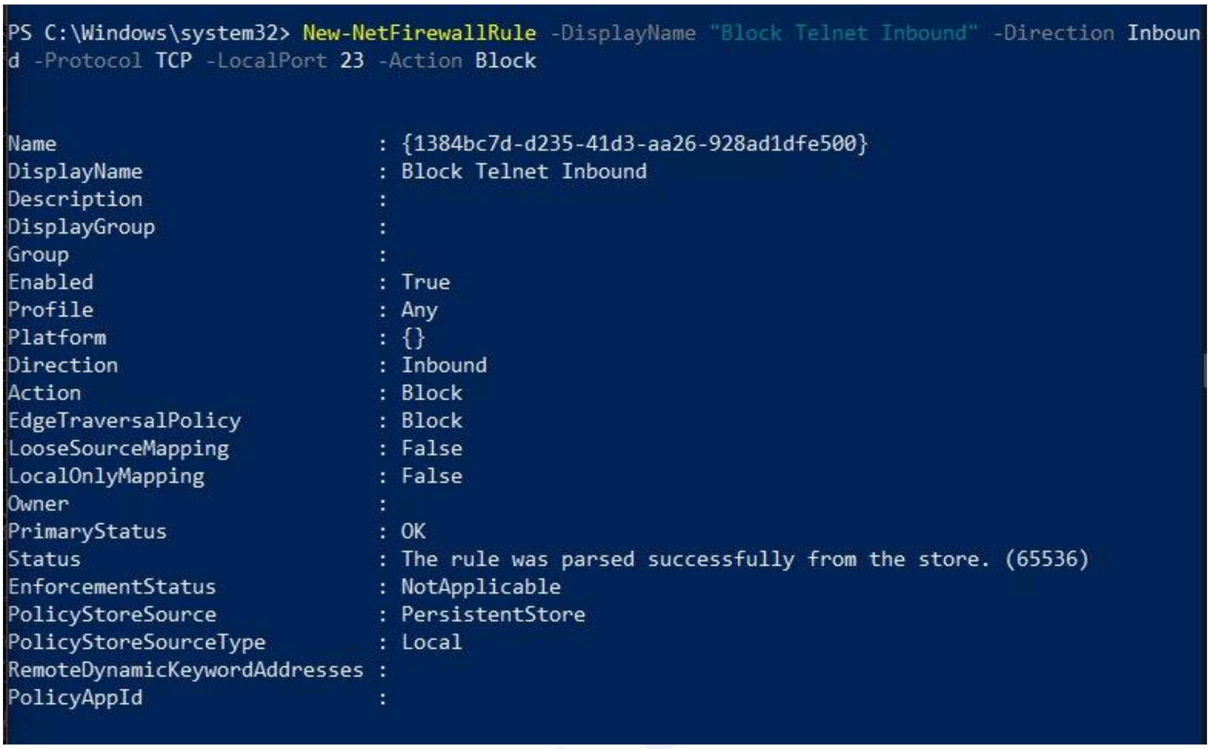
Get-NetFirewallRule -Enabled True | Get-NetFirewallPortFilter | Format-Table -AutoSize



```
PS C:\Windows\system32> Get-NetFirewallRule -Enabled True | Get-NetFirewallPortFilter | Format-Ta
ble -AutoSize

Protocol LocalPort             RemotePort       IcmpType DynamicTarget
-------- ---------             ----------       -------- -------------
UDP      Any                   Any              Any
UDP      Any                   Any              Any      Any
ICMPv6   RPC                   Any              2        Any
TCP      Any                   Any              Any      Any
TCP      Any                   Any              Any      Any
TCP      Any                   Any              Any
UDP      Any                   Any              Any
ICMPv6   RPC                   Any              2        Any
ICMPv6   RPC                   Any              3        Any
TCP      7680                  Any              Any      Any
ICMPv6   RPC                   Any              1        Any
UDP      7680                  Any              Any      Any
UDP      Any                   Any              Any      Any
TCP      Any                   Any              Any
TCP      Any                   Any              Any
TCP      Any                   Any              Any
ICMPv6   RPC                   Any              135      Any
ICMPv6   RPC                   Any              4        Any
ICMPv6   RPC                   Any              3        Any
ICMPv6   RPC                   Any              136      Any
ICMPv6   RPC                   Any              4        Any
ICMPv6   RPC                   Any              136      Any
ICMPv6   RPC                   Any              135      Any
ICMPv6   RPC                   Any              134      Any
ICMPv6   RPC                   Any              130      Any
ICMPv6   RPC                   Any              131      Any
ICMPv6   RPC                   Any              134      Any
ICMPv6   RPC                   Any              143      Any
ICMPv6   RPC                   Any              133      Any
ICMPv6   RPC                   Any              131      Any
ICMPv6   RPC                   Any              133      Any
ICMPv6   RPC                   Any              143      Any
ICMPv6   RPC                   Any              130      Any
ICMPv6   RPC                   Any              132      Any
2        Any                   Any              Any      Any
2        Any                   Any              Any      Any
ICMPv6   RPC                   Any              132      Any
ICMPv4   RPC                   Any              3:4      Any
UDP      68                    67               Any      Any
UDP      Any                   Any              Any      Any
41       Any                   Any              Any      Any
UDP      Any                   53               Any      Any
TCP      Any                   {80, 443}        Any      Any
TCP      Any                   445              Any      Any
TCP      IPHTTPSIn             Any              Any      Any
41       Any                   Any              Any      Any
UDP      546                   547              Any      Any
TCP      Any                   IPHTTPSOut       Any      Any
UDP      68                    67               Any      Any
TCP      Any                   Any              Any      Any
UDP      546                   547              Any      Any
UDP      Teredo                Any              Any      Any
TCP      Any                   Any              Any      ProximitySharing
TCP      Any                   Any              Any      Any
TCP      Any                   Any              Any      Any
```

# Block inbound TCP port 23 (Telnet)

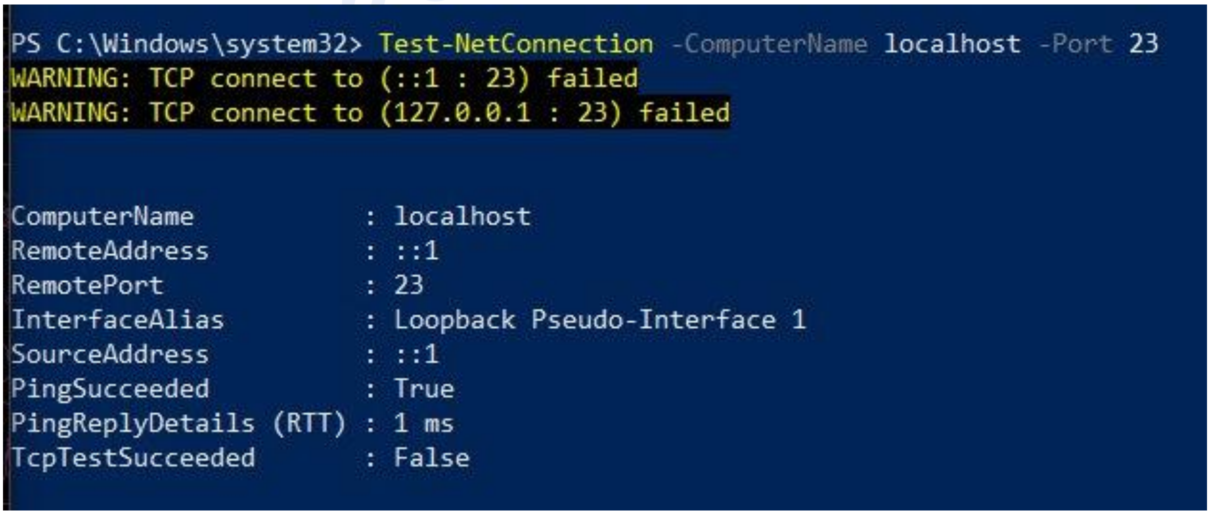
New-NetFirewallRule -DisplayName "Block Telnet Inbound" -Direction Inbound -Protocol TCP -LocalPort 23 -Action Block



```
PS C:\Windows\system32> New-NetFirewallRule -DisplayName "Block Telnet Inbound" -Direction Inboun
d -Protocol TCP -LocalPort 23 -Action Block


Name                          : {1384bc7d-d235-41d3-aa26-928ad1dfe500}
DisplayName                   : Block Telnet Inbound
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Block
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses :
PolicyAppId                   :
```

# Test connectivity on port 23

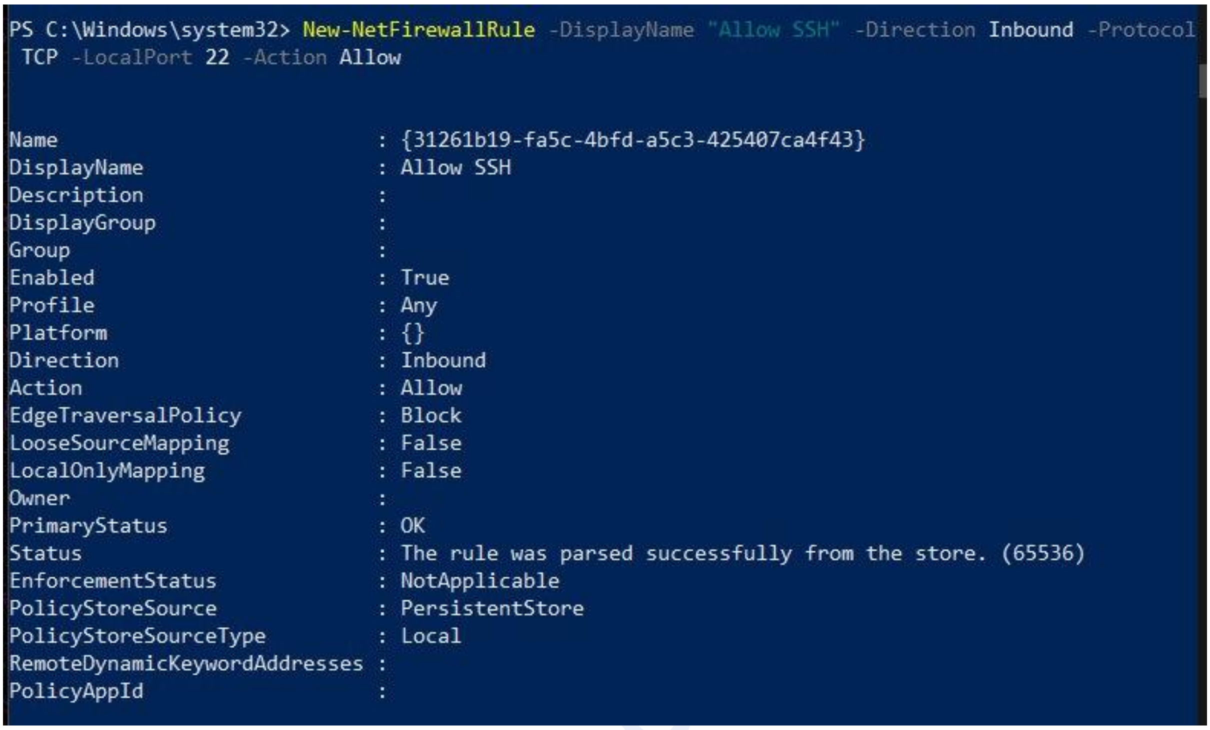
Test-NetConnection -ComputerName localhost -Port 23



```
PS C:\Windows\system32> Test-NetConnection -ComputerName localhost -Port 23
WARNING: TCP connect to (::1 : 23) failed
WARNING: TCP connect to (127.0.0.1 : 23) failed


ComputerName           : localhost
RemoteAddress          : ::1
RemotePort             : 23
InterfaceAlias         : Loopback Pseudo-Interface 1
SourceAddress          : ::1
PingSucceeded          : True
PingReplyDetails (RTT) : 1 ms
TcpTestSucceeded       : False
```

# Allow inbound SSH (port 22)

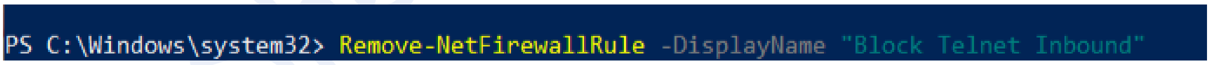
New-NetFirewallRule -DisplayName "Allow SSH" -Direction Inbound -Protocol TCP -LocalPort 22 -Action Allow



```
PS C:\Windows\system32> New-NetFirewallRule -DisplayName "Allow SSH" -Direction Inbound -Protocol
 TCP -LocalPort 22 -Action Allow


Name                          : {31261b19-fa5c-4bfd-a5c3-425407ca4f43}
DisplayName                   : Allow SSH
Description                   :
DisplayGroup                  :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Allow
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                 : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus             : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType         : Local
RemoteDynamicKeywordAddresses :
PolicyAppId                   :
```

# Remove Telnet block rule

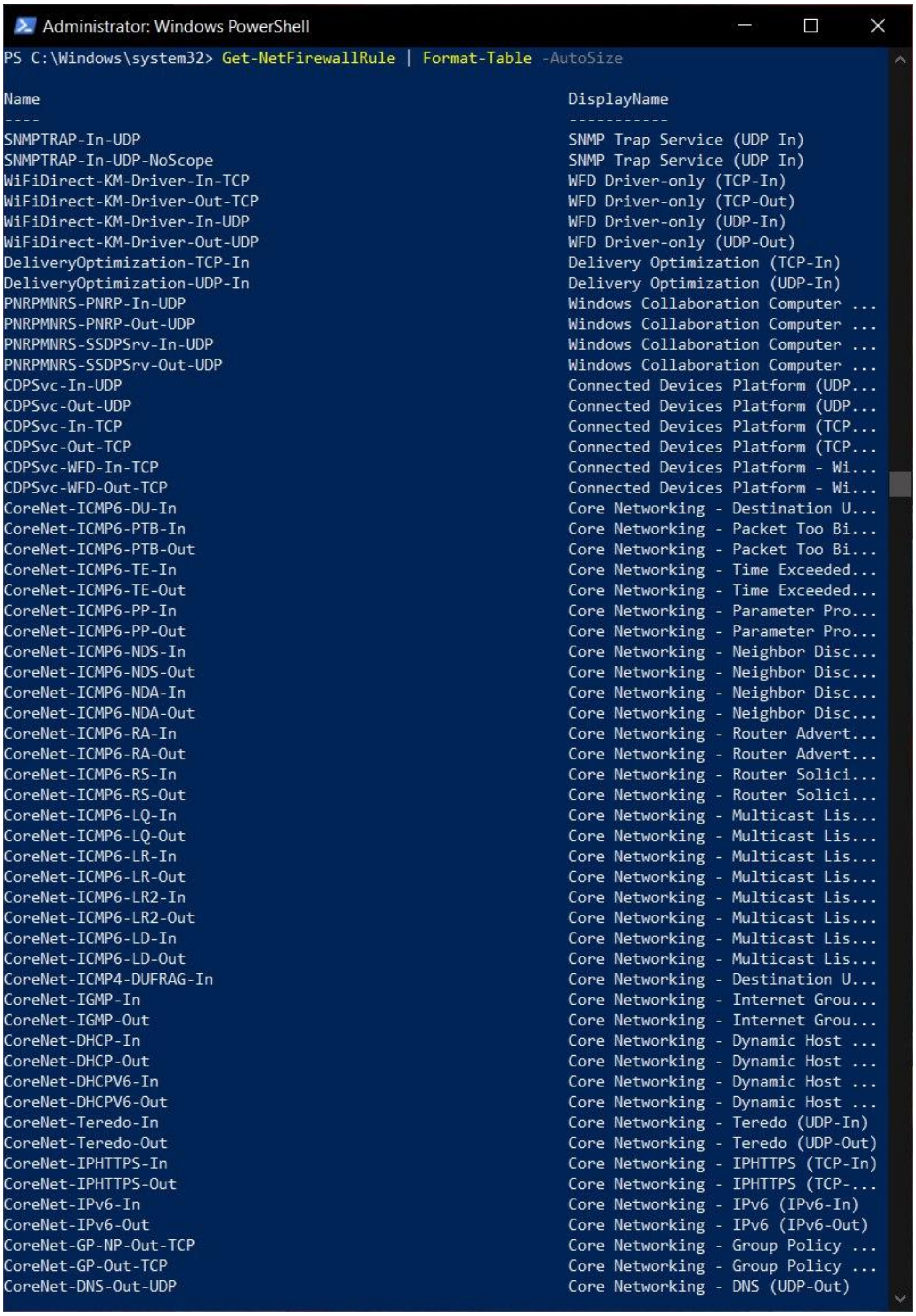
Remove-NetFirewallRule -DisplayName "Block Telnet Inbound"



```
PS C:\Windows\system32> Remove-NetFirewallRule -DisplayName "Block Telnet Inbound"
```

# Verify firewall rules again

Get-NetFirewallRule | Format-Table -AutoSize

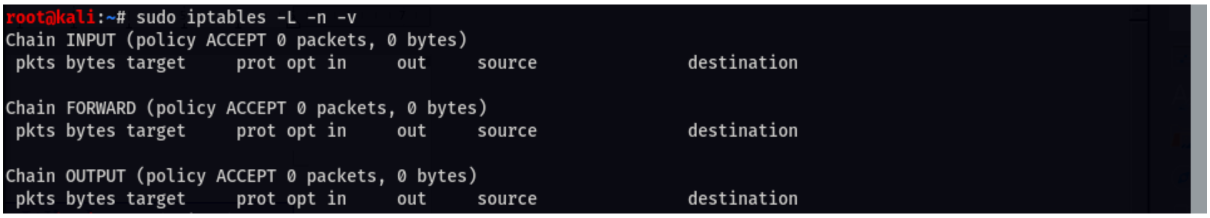


```
PS C:\Windows\system32> Get-NetFirewallRule | Format-Table -AutoSize

Name                                                          DisplayName
----                                                          -----------
SNMPTRAP-In-UDP                                               SNMP Trap Service (UDP In)
SNMPTRAP-In-UDP-NoScope                                       SNMP Trap Service (UDP In)
WiFiDirect-KM-Driver-In-TCP                                   WFD Driver-only (TCP-In)
WiFiDirect-KM-Driver-Out-TCP                                  WFD Driver-only (TCP-Out)
WiFiDirect-KM-Driver-In-UDP                                   WFD Driver-only (UDP-In)
WiFiDirect-KM-Driver-Out-UDP                                  WFD Driver-only (UDP-Out)
DeliveryOptimization-TCP-In                                   Delivery Optimization (TCP-In)
DeliveryOptimization-UDP-In                                   Delivery Optimization (UDP-In)
PNRPMNRS-PNRP-In-UDP                                          Windows Collaboration Computer ...
PNRPMNRS-PNRP-Out-UDP                                         Windows Collaboration Computer ...
PNRPMNRS-SSDPSrv-In-UDP                                       Windows Collaboration Computer ...
PNRPMNRS-SSDPSrv-Out-UDP                                      Windows Collaboration Computer ...
CDPSvc-In-UDP                                                 Connected Devices Platform (UDP...
CDPSvc-Out-UDP                                                Connected Devices Platform (UDP...
CDPSvc-In-TCP                                                 Connected Devices Platform (TCP...
CDPSvc-Out-TCP                                                Connected Devices Platform (TCP...
CDPSvc-WFD-In-TCP                                             Connected Devices Platform - Wi...
CDPSvc-WFD-Out-TCP                                            Connected Devices Platform - Wi...
CoreNet-ICMP6-DU-In                                           Core Networking - Destination U...
CoreNet-ICMP6-PTB-In                                          Core Networking - Packet Too Bi...
CoreNet-ICMP6-PTB-Out                                         Core Networking - Packet Too Bi...
CoreNet-ICMP6-TE-In                                           Core Networking - Time Exceeded...
CoreNet-ICMP6-TE-Out                                          Core Networking - Time Exceeded...
CoreNet-ICMP6-PP-In                                           Core Networking - Parameter Pro...
CoreNet-ICMP6-PP-Out                                          Core Networking - Parameter Pro...
CoreNet-ICMP6-NDS-In                                          Core Networking - Neighbor Disc...
CoreNet-ICMP6-NDS-Out                                         Core Networking - Neighbor Disc...
CoreNet-ICMP6-NDA-In                                          Core Networking - Neighbor Disc...
CoreNet-ICMP6-NDA-Out                                         Core Networking - Neighbor Disc...
CoreNet-ICMP6-RA-In                                           Core Networking - Router Advert...
CoreNet-ICMP6-RA-Out                                          Core Networking - Router Advert...
CoreNet-ICMP6-RS-In                                           Core Networking - Router Solici...
CoreNet-ICMP6-RS-Out                                          Core Networking - Router Solici...
CoreNet-ICMP6-LQ-In                                           Core Networking - Multicast Lis...
CoreNet-ICMP6-LQ-Out                                          Core Networking - Multicast Lis...
CoreNet-ICMP6-LR-In                                           Core Networking - Multicast Lis...
CoreNet-ICMP6-LR-Out                                          Core Networking - Multicast Lis...
CoreNet-ICMP6-LR2-In                                          Core Networking - Multicast Lis...
CoreNet-ICMP6-LR2-Out                                         Core Networking - Multicast Lis...
CoreNet-ICMP6-LD-In                                           Core Networking - Multicast Lis...
CoreNet-ICMP6-LD-Out                                          Core Networking - Multicast Lis...
CoreNet-ICMP4-DUFRAG-In                                       Core Networking - Destination U...
CoreNet-IGMP-In                                               Core Networking - Internet Grou...
CoreNet-IGMP-Out                                              Core Networking - Internet Grou...
CoreNet-DHCP-In                                               Core Networking - Dynamic Host ...
CoreNet-DHCP-Out                                              Core Networking - Dynamic Host ...
CoreNet-DHCPV6-In                                             Core Networking - Dynamic Host ...
CoreNet-DHCPV6-Out                                            Core Networking - Dynamic Host ...
CoreNet-Teredo-In                                             Core Networking - Teredo (UDP-In)
CoreNet-Teredo-Out                                            Core Networking - Teredo (UDP-Out)
CoreNet-IPHTTPS-In                                            Core Networking - IPHTTPS (TCP-In)
CoreNet-IPHTTPS-Out                                           Core Networking - IPHTTPS (TCP-...
CoreNet-IPv6-In                                               Core Networking - IPv6 (IPv6-In)
CoreNet-IPv6-Out                                              Core Networking - IPv6 (IPv6-Out)
CoreNet-GP-NP-Out-TCP                                         Core Networking - Group Policy ...
CoreNet-GP-Out-TCP                                            Core Networking - Group Policy ...
CoreNet-DNS-Out-UDP                                           Core Networking - DNS (UDP-Out)
```

2. Linux iptables Commands

# List current iptables rules

sudo iptables -L -n -v



```
root@kali:~# sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

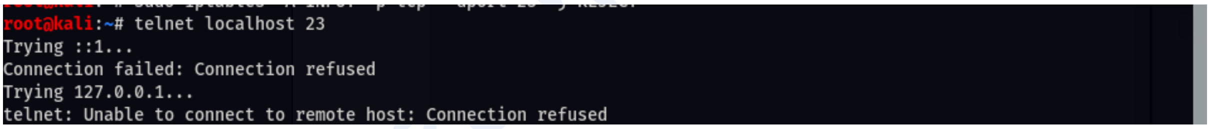
# Block incoming TCP traffic on port 23 (Telnet)

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

```
root@kali:~# sudo iptables -A INPUT -p tcp --dport 23 -j REJECT
```

# Test connectivity on port 23

telnet localhost 23



```
root@kali:~# telnet localhost 23
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

# Allow SSH (port 22)

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

```
root@kali:~# sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

# Remove Telnet block rule

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

```
root@kali:~# 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

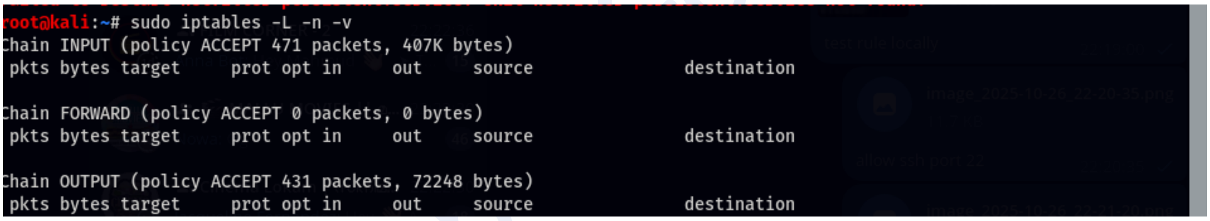
sudo iptables -P INPUT ACCEPT

sudo iptables -P FORWARD ACCEPT

sudo iptables -P OUTPUT ACCEPT

# Verify all rules cleared

sudo iptables -L -n -v



```
root@kali:~# sudo iptables -L -n -v
hain INPUT (policy ACCEPT 471 packets, 407K bytes)
 pkts bytes target     prot opt in     out     source               destination

hain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

hain OUTPUT (policy ACCEPT 431 packets, 72248 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

# 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