

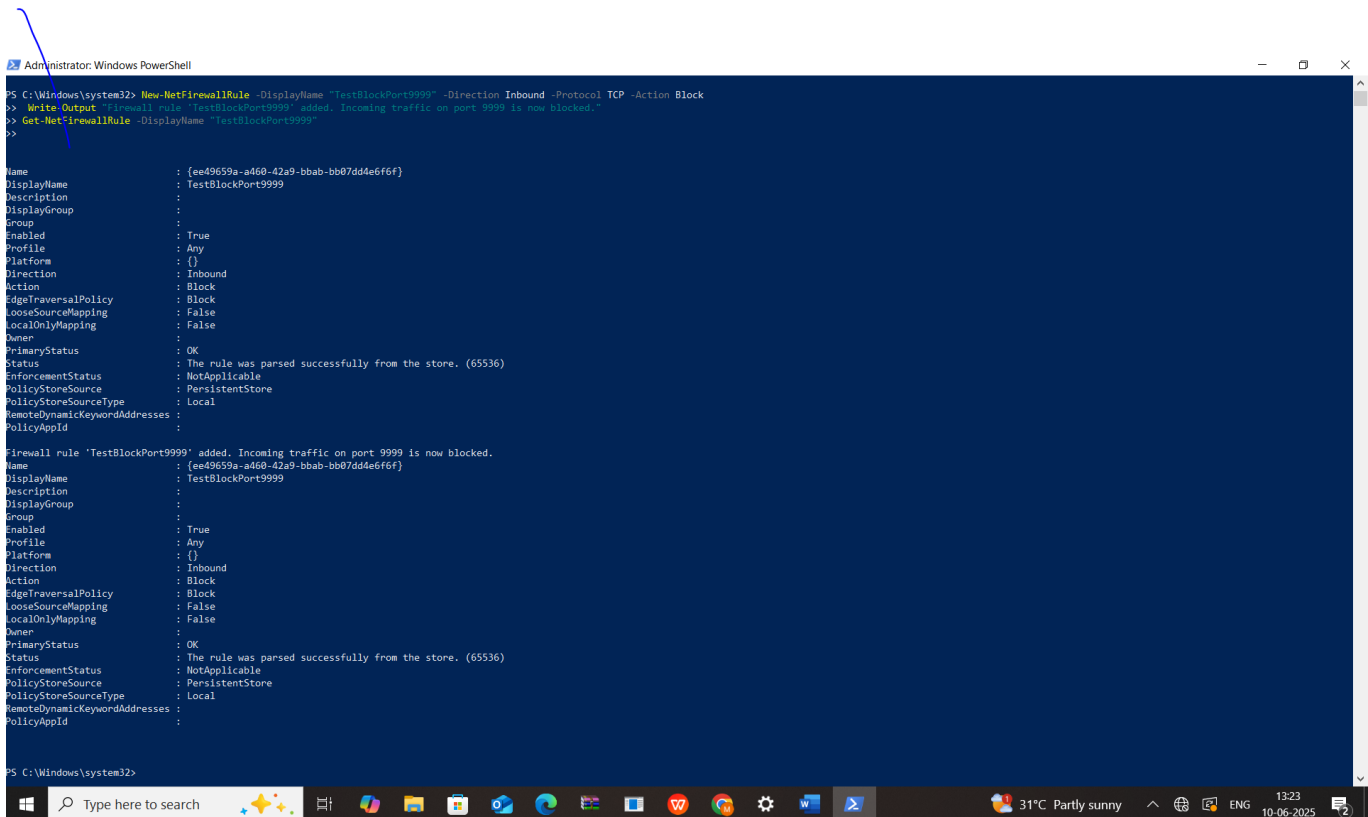
# Managing Windows Firewall Rules Using PowerShell

## Step 1: Add a New Firewall Rule to Block Port 9999

Command Used:

```
New-NetFirewallRule -DisplayName "TestBlockPort9999" -Direction Inbound -Protocol TCP -Action Block
```

This command creates a new rule that blocks inbound TCP traffic on port 9999.



```
Administrator: Windows PowerShell
PS C:\Windows\system32> New-NetFirewallRule -DisplayName "TestBlockPort9999" -Direction Inbound -Protocol TCP -Action Block
> Write-Output "Firewall rule 'TestBlockPort9999' added. Incoming traffic on port 9999 is now blocked."
> Get-NetFirewallRule -DisplayName "TestBlockPort9999"
>

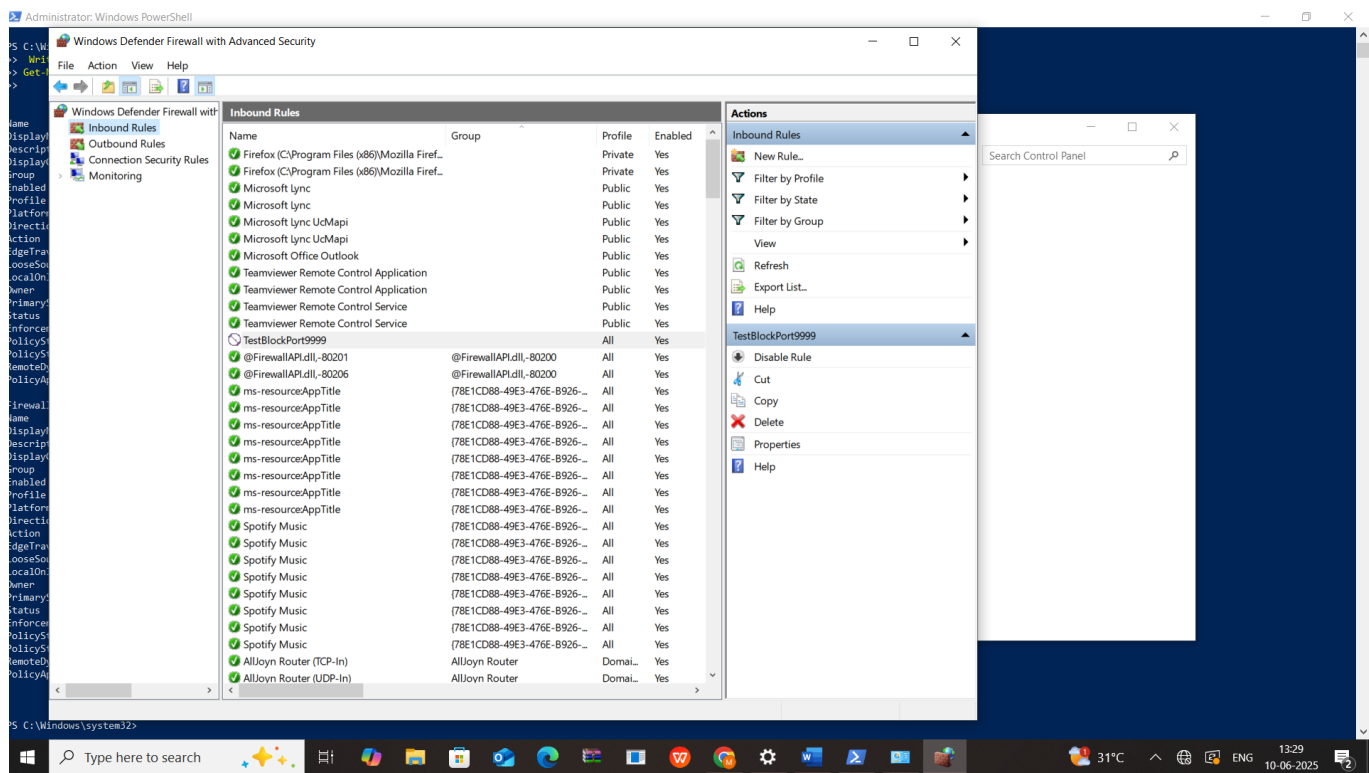
Name                           : {ee49659a-a460-42a9-bbab-bb07dde6f6f}
DisplayName                     : TestBlockPort9999
Description                     :
DisplayGroup                    :
Group                           :
Enabled                         : True
Profile                         : Any
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                     :

Firewall rule 'TestBlockPort9999' added. Incoming traffic on port 9999 is now blocked.
Name                           : {ee49659a-a460-42a9-bbab-bb07dde6f6f}
DisplayName                     : TestBlockPort9999
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                     :
```

## Step 2: Confirm Rule in Windows Defender Firewall

Open Windows Defender Firewall with Advanced Security.

Navigate to Inbound Rules and locate 'TestBlockPort9999' to confirm it has been added.



### Step 3: Remove the Firewall Rule

Command Used:

```
Remove-NetFirewallRule -DisplayName "TestBlockPort9999"
```

This command removes the rule and unblocks port 9999.

```
PolicyAppId :  
  
Firewall rule 'TestBlockPort9999' added. Incoming traffic on port 9999 is now blocked.  
Name : {ee49659a-a460-42a9-bbab-bb07dd4e6f6f}  
DisplayName : TestBlockPort9999  
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 :  
  
PS C:\Windows\system32> Remove-NetFirewallRule -DisplayName "TestBlockPort9999"  
PS C:\Windows\system32> Write-Output "Firewall rule 'TestBlockPort9999' removed."  
Firewall rule 'TestBlockPort9999' removed.  
PS C:\Windows\system32>  
PS C:\Windows\system32>
```