



Windows PowerShell Get-Help on Cmdlet 'Get-NetFirewallInterfaceFilter'

PS:\>Get-HELP Get-NetFirewallInterfaceFilter -Full

NAME

Get-NetFirewallInterfaceFilter

SYNOPSIS

Retrieves interface filter objects from the target computer.

SYNTAX

```
Get-NetFirewallInterfaceFilter [-All] [-AsJob] [-CimSession <CimSession[]>] [-GPOSession <String>] [-PolicyStore  
<String>] [-ThrottleLimit <Int32>]  
[<CommonParameters>]
```

```
Get-NetFirewallInterfaceFilter [-AsJob] -AssociatedNetFirewallRule <CimInstance> [-CimSession <CimSession[]>]  
[-GPOSession <String>] [-PolicyStore <String>]  
[-ThrottleLimit <Int32>] [<CommonParameters>]
```

```
Get-NetFirewallInterfaceFilter [-AsJob] -AssociatedNetIPsecRule <CimInstance> [-CimSession <CimSession[]>]  
[-GPOSession <String>] [-PolicyStore <String>]  
[-ThrottleLimit <Int32>] [<CommonParameters>]
```

DESCRIPTION

The Get-NetFirewallInterfaceFilter cmdlet returns interface filter objects associated with the input rules.

Interface filter objects represent the interfaces associated with firewall and IPsec rules. The InterfaceAlias parameter of a single rule is represented in a separate

NetFirewallInterfaceFilter object. The filter to rule relationship is always one-to-one and is managed automatically. Rule parameters associated with filters can only be queried using filter objects.

This cmdlet displays the interface aliases associated with firewall and IPsec rules. This allows for rule querying based on the InterfaceAlias parameter; this cmdlet

returns filter objects that may be further queried with the Where-Object (<https://go.microsoft.com/fwlink/?LinkID=113423>)cmdlet. The resultant filters are passed to Get-NetFirewallRule or Get-NetIPsecRule cmdlet to return the rules queried by interface.

To modify the interface conditions, two methods can be used starting with the interface filters returned by this cmdlet and optional additional querying.

The array of NetFirewallInterfaceFilter objects can be piped to Get-NetFirewallRule or Get-NetIPsecRule cmdlet, which returns the rules associated with the filters.

These rules are then piped to Set-NetFirewallRule or Set-NetIPsecRule cmdlet where the interface properties can be configured.

Alternatively, piping the array of NetFirewallInterfaceFilter objects directly to the Set-NetFirewallInterfaceFilter cmdlet allows the Program and Package parameters of the rules to be modified.

PARAMETERS

-All [<SwitchParameter>]

Indicates that all of the interface filters within the specified policy store are retrieved.

Required?	false
Position?	named
Default value	False
Accept pipeline input?	False
Accept wildcard characters?	false

-AsJob [<SwitchParameter>]

Runs the cmdlet as a background job. Use this parameter to run commands that take a long time to complete.

Required?	false
Position?	named
Default value	False
Accept pipeline input?	False
Accept wildcard characters?	false

-AssociatedNetFirewallRule <CimInstance>

Gets the interface filter object associated with the specified firewall rule to be retrieved. This parameter represents a firewall rule, which defines how traffic is filtered by the firewall. See the `New-NetFirewallRule` cmdlet for more information.

Required?	true
Position?	named
Default value	None
Accept pipeline input?	True (ByValue)
Accept wildcard characters?	false

-AssociatedNetIPsecRule <CimInstance>

Gets the address filter objects that are associated, via the pipeline, with the input IPsec rule to be retrieved. A `NetIPsecRule` object represents an IPsec rule, which determines IPsec behavior. An IPsec rule can be associated with `Phase1AuthSet`, `Phase2AuthSet`, and `NetIPsecQuickMode` cryptographic sets. See the `New-NetIPsecMainModeRule` cmdlet for more information.

Required?	true
Position?	named
Default value	None
Accept pipeline input?	True (ByValue)
Accept wildcard characters?	false

-CimSession <CimSession[]>

Runs the cmdlet in a remote session or on a remote computer. Enter a computer name or a session object, such as the output of a New-CimSession

(<https://go.microsoft.com/fwlink/p/?LinkId=227967>) or

[Get-CimSession](<https://go.microsoft.com/fwlink/p/?LinkId=227966>)cmdlet. The default is the current session on the local computer.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-GPOSession <String>

Specifies the network GPO from which to retrieve the rules to be retrieved. This parameter is used in the same way as the PolicyStore parameter. When modifying

GPOs in Windows PowerShell, each change to a GPO requires the entire GPO to be loaded, modified, and saved back. On a busy Domain Controller (DC), this can be a

slow and resource-heavy operation. A GPO Session loads a domain GPO onto the local computer and makes all changes in a batch, before saving it back. This reduces

the load on the DC and speeds up the Windows PowerShell cmdlets. To load a GPO Session, use the Open-NetGPO cmdlet. To save a GPO Session, use the Save-NetGPO cmdlet.

Required?	false
Position?	named
Default value	None

Accept pipeline input? False

Accept wildcard characters? false

-PolicyStore <String>

Specifies the policy store from which to retrieve the rules to be retrieved. A policy store is a container for firewall and IPsec policy. The acceptable values for this parameter are:

- PersistentStore: Sometimes called static rules, this store contains the persistent policy for the local computer. This policy is not from GPOs, and has been

created manually or programmatically (during application installation) on the computer. Rules created in this store are attached to the ActiveStore and activated

on the computer immediately. - ActiveStore: This store contains the currently active policy, which is the sum of all policy stores that apply to the computer.

This is the resultant set of policy (RSOP) for the local computer (the sum of all GPOs that apply to the computer), and the local stores (the PersistentStore, the

static Windows service hardening (WSH), and the configurable WSH). ---- GPOs are also policy stores. Computer GPOs can be specified as follows. -----

`-PolicyStore hostnamehostname`.

---- Active Directory GPOs can be specified as follows.

----- `-PolicyStore domain.fqdn.com\GPO_Friendly_Namedomain.fqdn.comGPO_Friendly_Name`.

----- Such as the following.

----- `-PolicyStore localhost`

----- `-PolicyStore corp.contoso.com\FirewallPolicy`

---- Active Directory GPOs can be created using the New-GPO cmdlet or the Group Policy Management Console. -

RSOP: This read-only store contains the sum of all

GPOs applied to the local computer.

- SystemDefaults: This read-only store contains the default state of firewall rules that ship with Windows Server 2012.
- StaticServiceStore: This read-only store contains all the service restrictions that ship with Windows Server 2012.

Optional and product-dependent features are considered part of Windows Server 2012 for the purposes of WFAS. -

ConfigurableServiceStore: This read-write store contains all the service restrictions that are added for third-party services. In addition, network isolation rules that are created for Windows Store application containers will appear in this policy store. The default value is PersistentStore. The Set-NetFirewallRule cmdlet cannot be used to add an object to a policy store. An object can only be added to a policy store at creation time with the Copy-NetFirewallRule cmdlet or with the New-NetFirewallRule cmdlet.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-ThrottleLimit <Int32>

Specifies the maximum number of concurrent operations that can be established to run the cmdlet. If this parameter is omitted or a value of `0` is entered, then Windows PowerShell calculates an optimum throttle limit for the cmdlet based on the number of CIM cmdlets that are running on the computer. The throttle limit applies only to the current cmdlet, not to the session or to the computer.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information, see about_CommonParameters (<https://go.microsoft.com/fwlink/?LinkID=113216>).

INPUTS

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\MSFT_NetConSecRule[]

The `Microsoft.Management.Infrastructure.CimInstance` object is a wrapper class that displays Windows Management Instrumentation (WMI) objects. The path after the pound sign (`#`) provides the namespace and class name for the underlying WMI object.

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\MSFT_NetFirewallRule

The `Microsoft.Management.Infrastructure.CimInstance` object is a wrapper class that displays Windows Management Instrumentation (WMI) objects. The path after the pound sign (`#`) provides the namespace and class name for the underlying WMI object.

OUTPUTS

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\MSFT_NetInterfaceFilter[]

The `Microsoft.Management.Infrastructure.CimInstance` object is a wrapper class that displays Windows Management Instrumentation (WMI) objects. The path after the pound sign (`#`) provides the namespace and class name for the underlying WMI object.

NOTES

----- EXAMPLE 1 -----

This cmdlet shows the same information in a dynamically-sized, formatted table.

```
PS C:\>Get-NetFirewallRule -PolicyStore ActiveStore | Format-Table
```

This example retrieves the interface aliases associated with all of the rules in the active store.

----- EXAMPLE 2 -----

```
PS C:\>Get-NetFirewallRule -DisplayName "Contoso Messenger" | Get-NetFirewallInterfaceFilter
```

This example gets the interface aliases associated with a particular firewall rule.

----- EXAMPLE 3 -----

```
PS C:\>Get-NetFirewallRule -DisplayName "Contoso Messenger" | Get-NetFirewallInterfaceFilter |  
Set-NetFirewallInterfaceFilter -InterfaceAlias Any
```

This cmdlet shows the same information in a dynamically-sized, formatted table.

```
PS C:\>Set-NetFirewallRule -DisplayName "Contoso Messenger" -InterfaceAlias Any
```

This example modifies the interface alias field of a particular firewall rule.

----- EXAMPLE 4 -----

```
PS C:\>Get-NetIPsecRule -Group "Wired Rules" | Get-NetFirewallInterfaceFilter | Where-Object -FilterScript {  
$_.InterfaceAlias -Eq "Wired2" } |  
Set-NetFirewallInterfaceFilter -InterfaceAlias Wired3
```

This example modifies a particular interface alias associated with all of the firewall rules in a specified group.

RELATED LINKS

Online

Version:

https://learn.microsoft.com/powershell/module/netsecurity/get-netfirewallinterfacefilter?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

Format-Table <https://go.microsoft.com/fwlink/p/?LinkId=113303>

Where-Object <https://go.microsoft.com/fwlink/p/?LinkId=113423>

Copy-NetIPsecRule

Get-NetFirewallApplicationFilter

Get-NetFirewallRule

Get-NetIPsecRule

New-NetFirewallRule

New-NetIPsecMainModeRule

New-NetIPsecRule

Open-NetGPO

Save-NetGPO

Set-NetFirewallInterfaceFilter

Set-NetFirewallRule

Set-NetIPsecRule