Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'Get-NetFirewallPortFilter'

PS C:\Users\wahid> Get-Help Get-NetFirewallPortFilter

NAME

Get-NetFirewallPortFilter

SYNOPSIS

Retrieves port filter objects from the target computer.

SYNTAX

Get-NetFirewallPortFilter [-All] [-AsJob] [-CimSession <CimSession[]>]

[-GPOSession <String>] [-PolicyStore <String>] [-ThrottleLimit <Int32>]

[<CommonParameters>]

Get-NetFirewallPortFilter [-AsJob] -AssociatedNetFirewallRule <CimInstance>

[-CimSession <CimSession[]>] [-GPOSession <String>] [-PolicyStore <String>]

[-ThrottleLimit <Int32>] [<CommonParameters>]

Get-NetFirewallPortFilter [-AsJob] -AssociatedNetIPsecRule <CimInstance>

[-CimSession <CimSession[]>] [-GPOSession <String>] [-PolicyStore <String>]

[-ThrottleLimit <Int32>] [<CommonParameters>]

Get-NetFirewallPortFilter [-AsJob] [-CimSession <CimSession[]>]

[-DynamicTarget {Any | ProximityApps | ProximitySharing | WifiDirectPrinting | WifiDirectDisplay | WifiDirectDevices}] [-GPOSession <String>] [-PolicyStore <String>] [-Protocol <String[]>] [-ThrottleLimit <Int32>] [<CommonParameters>]

DESCRIPTION

The Get-NetFirewallPortFilter cmdlet returns the port filter objects associated with the input rules.

Port filter objects represent the port and protocol conditions associated with the firewall and IPsec rules. The Protocol, LocalPort , RemotePort , IcmpType and DynamicTransport parameters of a single rule are represented in a single rule are represented in a separate NetFirewallPortFilter 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 ports and protocols associated with firewall and IPsec rules. This allows for rule querying based on the Protocol , LocalPort , RemotePort , IcmpType and DynamicTransport parameters; this cmdlet returns filter objects that may be further queried with the Where-Object (https://go.microsoft.com/fwlink/?LinkID=113423)cmdlet. The cmdlet also allows the interface type filters to be obtained by Protocol , LocalPort , RemotePort , IcmpType and DynamicTransport parameter query. The resultant filters are passed into the Get-NetFirewallRule or Get-NetIPsecRule cmdlet to return the rules queried by port or protocol.

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

The array of NetFirewallPortFilter objects can be piped into the Get-NetFirewallRule or Get-NetIPsecRule cmdlet, which returns the rules associated with the filters. These rules are then piped to the Set-NetFirewallRule or Set-NetIPsecRule cmdlet where the interface properties

can be configured.

Alternatively, piping the array of NetFirewallPortFilter objects directly into the Set-NetFirewallInterfaceTypeFilter cmdlet allows the Protocol , LocalPort , RemotePort , IcmpType and DynamicTransport parameters of the rules to be modified.

PARAMETERS

-All [<SwitchParameter>]

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

-AsJob [<SwitchParameter>]

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

-AssociatedNetFirewallRule <CimInstance>

Gets the port 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.

-AssociatedNetIPsecRule <CimInstance>

Gets the phase 1 authentication sets 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.

-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.

-DynamicTarget <DynamicTransport[]>

Specifies an array of dynamic transports. The cmdlet returns port filter objects associated with the input rules that have the dynamic transports that you specify. The acceptable values for this parameter are:

- Any

- ProximityApps

- ProximitySharing

- WifiDirectPrinting

- WifiDirectDisplay

- WifiDirectDevices

Some types of dynamic transports, such as proximity sharing, abstract the network layer details, and you cannot use standard network layer conditions, such as protocols and ports, to identify the dynamic transports.

-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 PowerShellr, 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.

-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 hostname`.

---- 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 Serverr 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.

-Protocol <String[]>

Specifies that network packets with matching IP addresses match this rule. This parameter specifies the protocol for an IPsec rule. The acceptable values for this parameter are:

- Protocols by number: 0 through 255.

- Protocols by name: TCP, UDP, ICMPv4, or ICMPv6.

If a port number is identified by using port1 or port2, then this parameter must be set to TCP or UDP. The values ICMPv4 and ICMPv6 create a rule that exempts ICMP network traffic from the IPsec requirements of another rule.

The default value is Any. Querying for rules with this parameter can only be performed using filter objects.

-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 PowerShellr 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.

<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).

---------- Example 1 ----------

PS C:\>Get-NetFirewallPortFilter -PolicyStore ActiveStore

This cmdlet displays the same information in a dynamically sized formatted table.

PS C:\>Get-NetFirewallPortFilter -PolicyStore ActiveStore | Format-Table -Property *

This example retrieves the port conditions associated with all the rules in

the active store. Running this cmdlet without specifying the policy store retrieves the persistent store.

---------- Example 2 ----------

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

This example gets the port properties of a particular firewall rule.

---------- Example 3 ----------

```
PS C:\>Get-NetFirewallRule -DisplayName "Play To streaming server" |
Get-NetFirewallPortFilter | Set-NetFirewallPortFilter -LocalPort 10246
```

This task can alternatively be done with this cmdlet.

```
PS C:\>Set-NetFirewallRule -DisplayName "Play To streaming server" -LocalPort
10246
```

This example modifies the local port field of a particular firewall rule.

---------- Example 4 ----------

```
PS C:\>Get-NetFirewallPortFilter | Where-Object -Property LocalPort -EQ 10246
| Set-NetFirewallPortFilter -LocalPort Any
```

This example modifies all of the rules associated with a specific port.

---------- Example 5 ----------

```
PS C:\>Get-NetFirewallRule -DisplayGroup "File and Printer Sharing" |
Get-NetFirewallPortFilter | Where-Object -Property { $_.RemotePort -Eq "137" }
| Set-NetFirewallPortFilter -LocalPort Any
```

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

---------- Example 6 ----------

PS C:\>Get-NetFirewallPortFilter -DynamicTransport ProximitySharing |
Get-NetFirewallRule | Set-NetFirewall -Action Block

This example shows how to locate the built-in network isolation rule permitting ProximitySharing and blocks it so that the proximity pairing is disallowed.

REMARKS

To see the examples, type: "get-help Get-NetFirewallPortFilter -examples".
For more information, type: "get-help Get-NetFirewallPortFilter -detailed".
For technical information, type: "get-help Get-NetFirewallPortFilter -full".
For online help, type: "get-help Get-NetFirewallPortFilter -online"