Windows PowerShell Get-Help on Cmdlet 'Set-NetFirewallHyperVRule'

PS:\>Get-HELP Set-NetFirewallHyperVRule -Full

NAME

Set-NetFirewallHyperVRule

SYNOPSIS

Modifies existing Hyper-V firewall rules.

SYNTAX

Set-NetFirewallHyperVRule [-Action {NotConfigured | Allow | Block}] [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Direction {Inbound | Outbound}] -DisplayName

<String> [-Enabled {True | False}] [-LocalAddresses <String[]>] [-LocalPorts <String[]>] [-Name <String>] [-NewDisplayName <String>] [-Protocol <String>]

[-RemoteAddresses <String[]>] [-RemotePorts <String[]>] [-RulePriority <uint16>] [-VMCreatorId <String>] [-Profiles {Any | Domain | Private | Public | NotApplicable}]

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

DESCRIPTION

The Set-NetFirewallHyperVRule cmdlet modifies existing Hyper-V firewall rule properties. This cmdlet gets one or more rules to be modified using the Name parameter or

the DisplayName parameter.

Rules cannot be queried by property in this cmdlet, but the querying can be done by the Get-NetFirewallHyperVRule cmdlet and piped into this cmdlet. The remaining

parameters modify the properties of the specified rules.

PARAMETERS

-Action <Action>

Updates the Action value for the matching Hyper-V firewall rules. This parameter specifies the action to take on traffic that matches this rule. The acceptable

values for this parameter are: Allow or Block.

- Allow: Network packets that match all criteria specified in this rule are permitted through the firewall. This is the default value. - Block: Network packets

that match all criteria specified in this rule are dropped by the firewall.

Required? false

Position? named

Default value None

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

-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

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Direction <Direction>

Updates the Direction value for the matching Hyper-V firewall rules. This parameter specifies which direction of traffic to match with this rule. The acceptable

values for this parameter are: Inbound or Outbound.

Required? false

Position? named

Default value Inbound

Accept pipeline input? False

Accept wildcard characters? false

-DisplayName <String>

Specifies that only matching Hyper-V firewall rules of the indicated display name are updated.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Enabled <Enabled>

Updates the Enabled value of the matching Hyper-V firewall rules. This parameter specifies that the rule object is administratively enabled or administratively

disabled. The acceptable values for this parameter are: - True: Specifies the rule is currently enabled.

- False: Specifies the rule is currently disabled.

Note that the type of this parameter is not Boolean, therefore `$true` and `$false` variables are not acceptable values here. Use "True" and "False" text strings

instead.

A disabled rule will not actively modify computer behavior, but the management construct still exists on the computer so it can be re-enabled.

Required? false

Position? named

Default value True

Accept pipeline input? False

Accept wildcard characters? false

-LocalAddresses <String[]>

Updates the LocalAddresses value for the matching Hyper-V firewall rules. This parameter specifies that network packets with matching IP addresses match this

rule. This parameter value is an IPv4 or IPv6 address, hostname, subnet, or range. The acceptable formats for this parameter are:

- Single IPv4 Address: 1.2.3.4

- Single IPv6 Address: fe80::1

- IPv4 Subnet (by network bit count): 1.2.3.4/24

- IPv6 Subnet (by network bit count): fe80::1/48

- IPv4 Subnet (by network mask): 1.2.3.4/255.255.255.0

- IPv4 Range: 1.2.3.4-1.2.3.7

- IPv6 Range: fe80::1-fe80::9

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

-LocalPorts <String[]>

Updates the LocalPorts value for the matching Hyper-V firewall rules.

This parameter specifies that network packets with matching IP local port numbers match this rule. The acceptable values are: - Port range: 0-65535

- Port number: 80

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <String>

Specifies that only matching Hyper-V firewall rules of the indicated name are updated.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-NewDisplayName <String>

Updates the DisplayName of the matching Hyper-V firewall rules.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Protocol <String>

Updates the protocol value of the matching Hyper-V firewall rules.

This parameter specifies that network packets with matching IP protocol match this rule. The acceptable values for this parameter are: - Protocols by number:

0-255.

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

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RemoteAddresses <String[]>

Updates the RemoteAddresses value of the matching Hyper-V firewall rules. This parameter specifies that network packets with matching IP addresses match this

rule. This parameter value is an IPv4 or IPv6 address, subnet, or range. The acceptable formats for this parameter are:

- Single IPv4 Address: 1.2.3.4

- Single IPv6 Address: fe80::1

- IPv4 Subnet (by network bit count): 1.2.3.4/24

- IPv6 Subnet (by network bit count): fe80::1/48

- IPv4 Subnet (by network mask): 1.2.3.4/255.255.255.0

- IPv4 Range: 1.2.3.4-1.2.3.7

- IPv6 Range: fe80::1-fe80::9

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RemotePorts <String[]>

Updates the RemotePorts value of the matching Hyper-V firewall rules. This parameter specifies that network packets with matching IP port numbers match this rule.

The acceptable values are: - Port range: 0-65535

- Port number: 80

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RulePriority <uint16>

Updates the RulePriority value of the matching Hyper-V firewall rules. This parameter specifies the order in which rules are evaluated. A lower priority rule is

evaluated before a higher priority rule.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-VMCreatorId <String>

Updates the VMCreatorId value of the matching Hyper-V firewall rules. This parameter specifies that network packets originating from a VM matching this

VMCreatorId matches this rule. The format for this value is a GUID enclosed in brackets: '{9E288F02-CE00-4D9E-BE2B-14CE463B0298}'.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Profiles <Profiles>

Specifies one or more profiles to which the hyper-v firewall rule is assigned. The rule is active on the local computer only when the specified profile is

currently active. This relationship is many-to-many and can be indirectly modified by the user, by changing the Profiles field on instances of rules. Only one

profile is applied at a time. The acceptable values for this parameter are: Any, Domain, Private, Public, or NotApplicable. The default value is Any. Separate

multiple entries with a comma and do not include any spaces.

Required? false

Position? named

Default value Any

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,

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

-WhatIf [<SwitchParameter>]

Shows what would happen if the cmdlet runs. The cmdlet is not run.

Required? false

Position? named

Default value False

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

None

OUTPUTS

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

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 ----------

PS C:\> Set-NetFirewallHyperVRule -Name DisplayName "Block Outbound to My Servers" -RemoteAddresses

"10.0.0.0/32"

This example modifies the existing Hyper-V firewall rules with DisplayName "Block Outbound to My Servers" and updates the RemoteAddresses condition.

RELATED LINKS

Online Version: https://docs.microsoft.com/powershell/module/netsecurity/set-netfirewallhypervrule?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

New-NetFirewallHyperVRule

Get-NetFirewallHyperVRule

Enable-NetFirewallHyperVRule

Disable-NetFirewallHyperVRule

Remove-NetFirewallHyperVRule

Rename-NetFirewallHyperVRule

Get-NetfirewallHyperVVMCreator