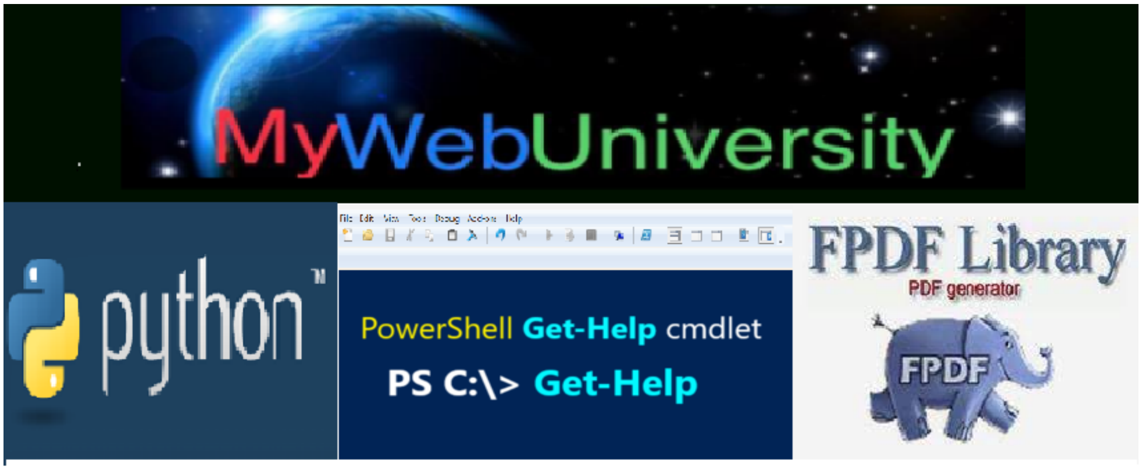

Full credit is given to all the above companies including the Operating System that this PDF file was generated!

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

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

NAME

New-NetFirewallHyperVRule

SYNOPSIS

Creates a new inbound or outbound Hyper-V firewall rule and adds the rule to the target computer.

SYNTAX

```
    New-NetFirewallHyperVRule [-Action {NotConfigured | Allow | Block}] [-AsJob] [-CimSession <CimSession[]>] [-Confirm]
[-Direction {Inbound | Outbound}] -DisplayName
      <String> [-Enabled {True | False}] [-LocalAddresses <String[]>] [-LocalPorts <String[]>] [-Name <String>] [-Protocol
<String>] [-RemoteAddresses <String[]>]
     [-RemotePorts <String[]>] [-RulePriority <uint16>] [-VMCreatorId <String>] [-Profiles {Any | Domain | Private | Public |
NotApplicable}] [-ThrottleLimit <Int32>]
    [-WhatIf] [<CommonParameters>]
```

DESCRIPTION

The New-NetFirewallHyperVRule cmdlet creates an inbound or outbound Hyper-V firewall rule and adds the rule to the target computer.

Some parameters are used to specify the conditions that must be matched for the rule to apply, such as the LocalAddress and RemoteAddress parameters.

Rules that already exist can be managed with the Get-NetFirewallHyperVRule and Set-NetFirewallHyperVRule cmdlets.

PARAMETERS

-Action <Action>

Specifies that matching Hyper-V firewall rules of the indicated action are created. 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.

The default value is Allow.

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>

Specifies that matching Hyper-V firewall rules of the indicated direction are created. This parameter specifies which direction of traffic to match with this

rule. The acceptable values for this parameter are: Inbound or Outbound.

The default value is Inbound.

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 created. Specifies the localized, user-facing name of the Hyper-V firewall

rule being created. When creating a rule this parameter is required. This parameter value is locale-dependent. When writing scripts in multi-lingual environments,

the Name parameter should be used instead, where the default value is a randomly assigned value. This parameter cannot be set to All.

Required?   true

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-Enabled <Enabled>

Specifies that matching Hyper-V firewall rules of the indicated state are created. 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.

The default value is True.

Required?   false

Position?   named

Default value   True

Accept pipeline input?   False

Accept wildcard characters? false

-LocalAddresses <String[]>

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

The default value is Any.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-LocalPorts <String[]>

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

- Port number: 80

The default value is Any.

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 created. This name serves as the unique identifier for this rule. This parameter

acts just like a file name, in that only one rule with a given name may exist in a policy store at a time.

The default value is a randomly assigned value.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-Protocol <String>

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.

The default value is Any.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-RemoteAddresses <String[]>

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

The default value is Any.

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

-RemotePorts <String[]>

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

- Port number: 80

The defauly value is Any.

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

-RulePriority <uint16>

Specifies the order in which rules are evaluated. A lower priority rule is evaluated before a higher priority rule.

The default value is based on the action of the rule. A rule with Action Allow is set to priority 2, and a rule with Action Block is 1. This configures, by

default, Block rules to take precedence over Allow rules.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-VMCreatorId <String>

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}'.

The default value is Any.

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:\> New-NetFirewallHyperVRule -DisplayName "Block Outbound Port 80" -Direction Outbound -LocalPorts 80 -Protocol TCP -Action Block
```

This example creates an outbound Hyper-V firewall rule to block all traffic from applicable Hyper-V VMs that originates on TCP port 80.

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

```
PS C:\> New-NetFirewallRule -DisplayName "Block HTTP from VM Creator" -Direction Outbound -Action Block -RemotePorts 443 -VMCreatorId
'{9E288F02-CE00-4D9E-BE2B-14CE463B0298}'
```

This example creates an outbound Hyper-V firewall rule to block HTTP traffic from VMs created by the input ID.

RELATED LINKS

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

Get-NetFirewallHyperVRule

Enable-NetFirewallHyperVRule

Disable-NetFirewallHyperVRule

Remove-NetFirewallHyperVRule

Rename-NetFirewallHyperVRule

Set-NetFirewallHyperVRule

Get-NetfirewallHyperVVMCreator