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

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

NAME

New-NetFirewallRule

SYNOPSIS

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

SYNTAX

New-NetFirewallRule [-Action {NotConfigured | Allow | Block}] [-AsJob] [-Authentication {NotRequired | Required | NoEncap}] [-CimSession <CimSession[]>] [-Confirm]

[-Description <String>] [-Direction {Inbound | Outbound}] -DisplayName <String> [-DynamicTarget {Any | ProximityApps | ProximitySharing | WifiDirectPrinting |

WifiDirectDisplay | WifiDirectDevices}] [-EdgeTraversalPolicy {Block | Allow | DeferToUser | DeferToApp}] [-Enabled {True | False}] [-Encryption {NotRequired |

Required | Dynamic}] [-GPOSession <String>] [-Group <String>] [-IcmpType <String[]>] [-InterfaceAlias <WildcardPattern[]>] [-InterfaceType {Any | Wired | Wireless |

RemoteAccess}] [-LocalAddress <String[]>] [-LocalOnlyMapping <Boolean>] [-LocalPort <String[]>] [-LocalUser <String>] [-LooseSourceMapping <Boolean>] [-Name <String>]

[-OverrideBlockRules <Boolean>] [-Owner <String>] [-Package <String>] [-Platform <String[]>] [-PolicyStore <String>] [-Profile {Any | Domain | Private | Public |

NotApplicable}] [-Program <String>] [-Protocol <String>] [-RemoteAddress <String[]>] [-RemoteDynamicKeywordAddresses <String[]>] [-RemoteMachine <String>]

[-RemotePort <String[]>] [-RemoteUser <String>] [-Service <String>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-NetFirewallRule cmdlet creates an inbound or outbound 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. Other parameters

specify the way that the connection should be secured, like the Authentication and Encryption parameters. Rules that already exist can be managed with the

Get-NetFirewallRule and Set-NetFirewallRule cmdlets.

Filter objects, such as NetFirewallAddressFilter or NetFirewallApplicationFilter, are created with each firewall rule. The filter objects and rules are always

one-to-one and are managed automatically.

PARAMETERS

-Action <Action>

Specifies that matching 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. The OverrideBlockRules field changes an allow rule into

an allow bypass rule.

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

-Authentication <Authentication>

Specifies that authentication is required on firewall rules. The acceptable values for this parameter are: NotRequired, Required, or NoEncap.

- NotRequired: Any network packet matches this rule, that it is protected by IPsec. This option is the equivalent of not selecting the allow only secure

connections option in the Windows Firewall with Advanced Security MMC snap-in. - Required: Network packets that are authenticated by IPsec match this rule. A

separate IPsec rule must be created to authenticate the traffic. This option is the equivalent of the allow only secure connections option in the Windows Firewall

with Advanced Security MMC snap-in. This is the default value. - NoEncap: Network connections that are authenticated, but not encapsulated by Encapsulating

Security Payload (ESP) or Authentication Header (AH) match this rule. This option is useful for connections that must be monitored by network equipment, such as

intrusion detection systems (IDS), that are not compatible with ESP NULL-protected network packets. The initial connection is authenticated by IPsec by using

AuthIP, but the quick mode SA permits clear-text traffic. To use this option, you must also configure an IPsec rule that specifies authentication with

encapsulation none as a quick mode security method. In the Microsoft Management Console (MMC), authentication

and encryption are combined into one set of radio

buttons. In Windows Management Instrumentation (WMI) or Windows PowerShellr, authentication and encryption are given as two separate options. A rule can be

queried for this condition, or modified by using the security filter object. See the Get-NetFirewallSecurityFilter cmdlet for more information.

Required? false

Position? named

Default value None

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

-Description <String>

Specifies that matching firewall rules of the indicated description are created. Wildcard characters are accepted. This parameter provides information about the

firewall rule. This parameter specifies the localized, user-facing description of the IPsec rule.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Direction <Direction>

Specifies that matching 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 firewall rules of the indicated display name are created. Wildcard characters are accepted. Specifies the localized, user-facing

name of the firewall rule being created. When creating a rule this parameter is required. This parameter value is locale-dependent. If the object is not modified,

then this parameter value may change in certain circumstances. 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

-DynamicTarget <DynamicTransport>

Specifies a dynamic transport. The cmdlet adds the dynamic transport that you specify as a condition that must be matched for the firewall rule to apply. The

acceptable values for this parameter are:

- Any

- ProximityApps

- ProximitySharing

- WifiDirectPrinting

- WifiDirectDisplay

- WifiDirectDevices

The default value is Any.

Some types of dynamic transports, such as proximity sharing, abstract the network layer details. This means that you cannot use standard network layer conditions,

such as protocols and ports, to identify the dynamic transports.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-EdgeTraversalPolicy <EdgeTraversal>

Specifies that matching firewall rules of the indicated edge traversal policy are created. This parameter specifies how this firewall rule will handle edge

traversal cases. Valid only when the Direction parameter is set to Inbound. The acceptable values for this parameter are: Block, Allow, DeferToUser, or

DeferToApp. This parameter specifies that traffic that traverses an edge device, such as a network address translation (NAT)-enabled router, between the local

and remote computer matches this rule. If this parameter is set to DeferToUser or DeferToApp, then Windows allows the user or application to programmatically

register with the firewall to receive inbound unsolicited application traffic from the edge device.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Enabled <Enabled>

Specifies that matching 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.

Required? false

Position? named

Default value True

Accept pipeline input? False

Accept wildcard characters? false

-Encryption <Encryption>

Specifies that encryption in authentication is required on firewall rules. The authentication is done through a separate IPsec or main mode rule. The acceptable

values for this parameter are: NotRequired, Required, or Dynamic.

- NotRequired: Encryption is not required for authentication. This is the default value. - Required: Encryption is required for authentication through an IPsec

rule.

- Dynamic: Allows computers to dynamically negotiate encryption.

A rule can be queried for this condition, or modified by using the security filter object. See the Get-NetFirewallSecurityFilter cmdlet for more information.

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 created. 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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Group <String>

Specifies that only matching firewall rules of the indicated group association are copied. Wildcard characters are accepted. This parameter specifies the source

string for the DisplayGroup parameter. If the DisplayGroup parameter value is a localizable string, then this parameter contains an indirect string. Rule groups

can be used to organize rules by influence and allows batch rule modifications. Using the Set-NetFirewallRule cmdlets, if the group name is specified for a set of

rules or sets, then all of the rules or sets in that group receive the same set of modifications. It is a good practice to specify this parameter value with a

universal and world-ready indirect @FirewallAPI name. The DisplayGroup parameter cannot be specified upon object creation using the New-NetFirewallRule cmdlet,

but can be modified using dot-notation and the Set-NetFirewallRule cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-IcmpType <String[]>

Specifies the ICMP type codes. The key encoding is specified by running the Set-NetFirewallSetting cmdlet with the KeyEncoding parameter. The acceptable values

for this parameter are:

- ICMP type code: 0-255.

- ICMP type code pairs: 3:4.

- Keyword: Any.

A rule can be queried for this condition, modified by using the security filter object, or both. See the Get-NetFirewallPortFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InterfaceAlias <WildcardPattern[]>

Specifies the alias of the interface that applies to the traffic. Querying for rules with this parameter can only be performed using filter objects. See the

Get-NetFirewallInterfaceFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-InterfaceType <InterfaceType>

Specifies that only network connections made through the indicated interface types are subject to the requirements of this rule. This parameter specifies

different authentication requirements for each of the three main network types. The acceptable values for this parameter are: Any, Wired, Wireless, or

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

Get-NetFirewallInterfaceTypeFilter cmdlet for more information.

Required? false

Position? named

Default value Any

Accept pipeline input? False

Accept wildcard characters? false

-LocalAddress <String[]>

Specifies that network packets with matching IP addresses match this rule. This parameter value is the first end point of an IPsec rule and specifies the

computers that are subject to the requirements of this rule. This parameter value is an IPv4 or IPv6 address, hostname, subnet, range, or the following keyword:

Any. 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

Querying for rules with this parameter can only be performed using filter objects. See the Get-NetFirewallAddressFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-LocalOnlyMapping <Boolean>

Indicates that matching firewall rules of the indicated value are created. This parameter specifies the firewall rules for local only mapping, which describes

whether a packet must pass through a local address on the way to the destination. Non-TCP traffic is session-less. Windows Firewall authorizes traffic per

session, not per packet, for performance reasons. Generally, non-TCP sessions are inferred by checking the following fields: local address, remote address,

protocol, local port, and remote port. If this parameter is set to True, then the remote address and port will be ignored when inferring remote sessions.

Sessions will be grouped based on local address, protocol, and local port. This is similar to the LooseSourceMapping parameter, but performs better in cases

where the traffic does not need to be filtered by remote address. This could improve performance on heavy server workloads where UDP requests come from dynamic

client ports. For instance, Teredo relay servers.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-LocalPort <String[]>

Specifies that network packets with matching IP local port numbers match this rule. The acceptable value is a port, range, or keyword and depends on the

protocol. If the Protocol parameter value is TCP or UDP, then the acceptable values for this parameter are: - Port range: 0-65535.

- Port number: 80.

- Keyword: PlayToDiscovery or Any.

If the Protocol parameter value is ICMPv4 or ICMPv6, then the acceptable values for this parameter are: - An ICMP type, code pair: 0, 8.

- Type and code: 0-255.

- Keyword: Any.

If the Protocol parameter is not specified, then the acceptable values for this parameter are: RPC, RPCEPMap, Teredo, IPHTTPSIn, IPHTTPSOut, or Any. IPHTTPS is

only supported on Windows Server 2012. Querying for rules with this parameter can only be performed using filter objects. See the Get-NetFirewallPortFilter

cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-LocalUser <String>

Specifies the principals to which network traffic this firewall rule applies. Principals for which the network traffic this firewall rule should apply. The

principals, represented by security identifiers (SIDs) in the security descriptor definition language (SDDL) string, are services, users, application containers,

or any SID to which network traffic is associated. This parameter specifies that only network packets that are authenticated as coming from or going to a

principal identified in the list of accounts (SID) match this rule. Querying for rules with this parameter can only be performed using filter objects. See the

Get-NetFirewallSecurityFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-LooseSourceMapping <Boolean>

Indicates that matching firewall rules of the indicated value are created. This parameter specifies the firewall rules for loose source mapping, which describes

whether a packet can have a non-local source address when being forwarded to a destination. If this parameter is set to True, then the rule accepts packets

incoming from a host other than the one the packets were sent to. This parameter applies only to UDP protocol traffic. The default value is False.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <String>

Specifies that only matching firewall rules of the indicated name are created. Wildcard characters are accepted. 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. During group policy processing and policy merge, rules that have the same name but

come from multiple stores being merged, will overwrite one another so that only one exists. This overwriting behavior is desirable if the rules serve the same

purpose. For instance, all of the firewall rules have specific names, so if an administrator can copy these rules to a GPO, and the rules will override the local

versions on a local computer. GPOs can have precedence. So if an administrator has a different or more specific rule with the same name in a higher-precedence

GPO, then it overrides other rules that exist. The default value is a randomly assigned value. When the defaults for main mode encryption need to overridden,

specify the customized parameters and set this parameter, making it the new default setting for encryption.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-OverrideBlockRules <Boolean>

Indicates that matching network traffic that would otherwise be blocked are allowed. The network traffic must be authenticated by using a separate IPsec rule. If

the Direction parameter is set to Inbound, then this parameter is valid only for rules that have one or more accounts listed in the RemoteUser parameter and

optionally the RemoteMachine parameter. Network packets that match this rule and that are successfully authenticated against a computer account specified in the

RemoteUser parameter and against a user account identified in the RemoteMachine parameter are permitted through the firewall. If this parameter is specified,

then the Authentication parameter cannot be set to NotRequired. This parameter is equivalent to the override block rules checkbox in the Windows Firewall with

Advanced Security MMC snap-in. For computers that are running Windowsr 7 or nextref_server_7, this parameter is permitted on an outbound rule. Selecting this

parameter on an outbound rule causes matching traffic to be permitted through this rule even if other matching rules would block the traffic. No accounts are

required in the RemoteMachine or RemoteUser parameter for an outbound bypass rule, however, if authorized or excepted computers are listed in those groups the

rules will be enforced. This parameter is not valid on outbound rules on computers that are running firstref_vista or earlier. Querying for rules with this

parameter can only be performed using filter objects. See the Get-NetFirewallSecurityFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Owner <String>

Specifies that matching firewall rules of the indicated owner are created. This parameter specifies the owner of the firewall rule, represented as an SDDL

string. All Windows Store applications that require network traffic create network isolation rules (normally through installing via the Store), where the user

that installed the application is the owner. This parameter specifies that only network packets that are authenticated as coming from or going to an owner

identified in the list of accounts (SID) match this rule.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Package <String>

Specifies the Windows Store application to which the firewall rule applies. This parameter is specified as a security identifier (SID). Querying for rules with

this parameter can only be performed using filter objects. See the Get-NetFirewallApplicationFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Platform <String[]>

Specifies which version of Windows the associated rule applies. The acceptable format for this parameter is a number in the Major.Minor format. The version

number of 6.0 corresponds to Vista (nextref_vista), 6.1 corresponds to Win7 (Windowsr 7 or firstref_longhorn), and 6.2 corresponds to Win8 (Windowsr 8 or Windows

Server 2012). If + is not specified, then only that version is associated. If + is specified, then that version and later versions are associated. Querying for

rules with this parameter with the Get-NetFirewallRule cmdlet cannot be performed.

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 created. 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

of the 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 this cmdlet or the New-NetFirewallRule cmdlet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Profile <Profile>

Specifies one or more profiles to which the 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 firewall 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. Use the keyword Any to configure the profile as Private, Public, Domain in the ConfigurableServiceStore.

Required? false

Position? named

Default value Any

Accept pipeline input? False

Accept wildcard characters? false

-Program <String>

Specifies the path and file name of the program for which the rule allows traffic. This is specified as the full path to an application file. Querying for rules

with this parameter can only be performed using filter objects. See the Get-NetFirewallApplicationFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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: 0-255.

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

If a port number is identified by using numeric values (80, 443, 8080, etc.), 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. See the Get-NetFirewallPortFilter cmdlet for more

information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RemoteAddress <String[]>

Specifies that network packets with matching IP addresses match this rule. This parameter value is an IPv4 or IPv6 address, subnet, range or keyword. 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

- Keyword: Any, LocalSubnet, DNS, DHCP, WINS, DefaultGateway, Internet, Intranet, IntranetRemoteAccess, PlayToDevice. NOTE: Keywords can be restricted to IPv4 or

IPv6 by appending a 4 or 6 (for example, keyword "LocalSubnet4" means that all local IPv4 addresses are matching this rule).

Querying for rules with this parameter can only be performed using filter objects. See the Get-NetFirewallAddressFilter cmdlet for more information.

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

-RemoteDynamicKeywordAddresses <String[]>

Specifies the dynamic keyword address IDs to be used for the remote host of the traffic matched by this rule.

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

-RemoteMachine <String>

Specifies that matching IPsec rules of the indicated computer accounts are created. This parameter specifies that only network packets that are authenticated as

incoming from or outgoing to a computer identified in the list of computer accounts (SID) match this rule. This parameter value is specified as an SDDL string.

Querying for rules with this parameter can only be performed using filter objects. See the Get-NetFirewallSecurityFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RemotePort <String[]>

Specifies that network packets with matching IP port numbers match this rule. This parameter value is the second end point of an IPsec rule. The acceptable value

is a port, range, or keyword and depends on the protocol. If the protocol is TCP or UDP, then the acceptable values for this parameter are:

- Port range: 0-65535

- Port number: 80

- Keyword: Any

If the protocol is ICMPv4 or ICMPv6, then the acceptable values for this parameter are: - An ICMP type, code pair: 0, 8

- Type and code: 0-255

- Keyword: Any.

If a protocol is not specified, then the acceptable values for this parameter are: Any, RPC, RPC-EPMap, or IPHTTPS. IPHTTPS is only supported on Windows Server

2012. Querying for rules with this parameter can only be performed using filter objects. See the Get-NetFirewallPortFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RemoteUser <String>

Specifies that matching IPsec rules of the indicated user accounts are created. This parameter specifies that only network packets that are authenticated as

incoming from or outgoing to a user identified in the list of user accounts match this rule. This parameter value is specified as an SDDL string. Querying for

rules with this parameter can only be performed using filter objects. See the Get-NetFirewallSecurityFilter cmdlet for more information.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Service <String>

Specifies the short name of a Windows Server 2012 service to which the firewall rule applies. If this parameter is not specified, then network traffic generated

by any program or service matches this rule. Querying for rules with this parameter can only be performed using filter objects. See the

Get-NetFirewallServiceFilter cmdlet for more information.

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 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.

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\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.

NOTES

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

PS C:\> New-NetFirewallRule -DisplayName "Block Outbound Port 80" -Direction Outbound -LocalPort 80 -Protocol TCP -Action Block

This example creates an outbound firewall rule to block all of the traffic from the local computer that originates on TCP port 80.

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

PS C:\> New-NetFirewallRule -DisplayName "Block WINS" -Direction Inbound -Action Block -RemoteAddress WINS

This example creates a firewall rule that blocks all inbound traffic from all WINS servers.

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

PS C:\> New-NetFirewallRule -DisplayName "Allow Messenger" -Direction Inbound -Program "C:\Program Files

(x86)\Messenger\msmsgs.exe" -RemoteAddress LocalSubnet

-Action Allow

This example creates an inbound firewall rule that allows traffic for the Windows Messenger program only from computers on the same subnet as the local computer.

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

PS C:\> New-NetFirewallRule -DisplayName "Allow Authenticated Messenger" -Direction Inbound -Program "C:\Program Files (x86)\Messenger\msmsgs.exe" -Authentication

Required -Action Allow

This example creates a firewall rule that allows inbound Windows Messenger network traffic only if the connection from the remote computer is authenticated by using a

separate IPsec rule.

---------- EXAMPLE 5 ----------

PS C:\> New-NetFirewallRule -DisplayName "Allow Only Specific Computers and Users" -Direction Inbound -RemoteMachine "D:(A;;CC;;;SIDforMachineGroupAccount)"

-RemoteUser "D:(A;;CC;;;SIDforUserGroupAccount)" -Action Allow -Authentication Required

This example creates a firewall rule that allows all of the network traffic from computers that are members of a specific computer group, and only from users that are

members of a specific user group. Both memberships must be confirmed by authentication using a separate connection security rule.

---------- EXAMPLE 6 ----------

PS C:\> New-NetFirewallRule -Name "Block Wireless In" -Direction Inbound -InterfaceType Wireless -Action Block

PS C:\> New-NetFirewallRule -Name "Block Wireless Out" -Direction Outbound -InterfaceType Wireless -Action Block

This example uses two cmdlets to create firewall rules that block all of the wireless network traffic.

---------- EXAMPLE 7 ----------

PS C:\> New-NetFirewallRule -DisplayName "Allow TCP 12345 and 5000-5020 over Teredo" -Direction Inbound -Action

Allow -EdgeTraversalPolicy Allow -Protocol TCP

-LocalPort 12345,5000-5020 -Program "C:\Program Files (x86)\TestIPv6App.exe"

This example creates a firewall rule to allow TCP traffic addressed to port 12345 and the range of ports 5000-5020 to a specific application from the computers on the

remote side of an edge (NAT) device, using the Teredo IPv6 interface.

RELATED LINKS

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

Copy-NetFirewallRule

Enable-NetFirewallRule

Disable-NetFirewallRule

Get-NetFirewallAddressFilter

Get-NetFirewallApplicationFilter

Get-NetFirewallInterfaceFilter

Get-NetFirewallInterfaceTypeFilter

Get-NetFirewallPortFilter

Get-NetFirewallRule

Get-NetFirewallSecurityFilter

New-NetFirewallDynamicKeywordAddress

Open-NetGPO

Remove-NetFirewallRule

Rename-NetFirewallRule

Save-NetGPO

Set-NetFirewallRule

Set-NetFirewallSetting

Show-NetFirewallRule