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

PowerShell Get-Help on command 'Copy-NetFirewallRule'

PS C:\Users\wahid> Get-Help Copy-NetFirewallRule

NAME

Copy-NetFirewallRule

SYNOPSIS

Copies an entire firewall rule, and associated filters, to the same or to a different policy store.

SYNTAX

Copy-NetFirewallRule [-Action {NotConfigured | Allow | Block}] [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-Description <String[]>] [-Direction {Inbound | Outbound}] [-DisplayGroup <String[]>] [-EdgeTraversalPolicy {Block | Allow | DeferToUser | DeferToApp}] [-Enabled {True | False}] [-Group <String[]>] [-LocalOnlyMapping <Boolean[]>] [-LooseSourceMapping <Boolean[]>] [-NewGPOSession <String>] [-NewName <String>] [-NewPolicyStore <String>] [-Owner <String[]>] [-PassThru] [-PolicyStore <String>] [-PolicyStoreSource <String[]>] [-PolicyStoreSourceType {None | Local | GroupPolicy | Dynamic | Generated | Hardcoded}] [-PrimaryStatus {Unknown | OK | Inactive | Error}] [-Status <String[]>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Copy-NetFirewallRule [-All] [-AsJob] [-CimSession <CimSession[]>] [-Confirm]
[-NewGPOSession <String>] [-NewName <String>] [-NewPolicyStore <String>]
[-PassThru] [-PolicyStore <String>] [-ThrottleLimit <Int32>]
[-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Copy-NetFirewallRule [-AsJob] -AssociatedNetFirewallAddressFilter
<CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-NewGPOSession
<String>] [-NewName <String>] [-NewPolicyStore <String>] [-PassThru]
[-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf]
[<CommonParameters>]

Copy-NetFirewallRule [-AsJob] -AssociatedNetFirewallApplicationFilter
<CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-NewGPOSession
<String>] [-NewName <String>] [-NewPolicyStore <String>] [-PassThru]
[-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf]
[<CommonParameters>]

Copy-NetFirewallRule [-AsJob] -AssociatedNetFirewallInterfaceFilter
<CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-NewGPOSession
<String>] [-NewName <String>] [-NewPolicyStore <String>] [-PassThru]
[-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf]
[<CommonParameters>]

Copy-NetFirewallRule [-AsJob] -AssociatedNetFirewallInterfaceTypeFilter
<CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-NewGPOSession
<String>] [-NewName <String>] [-NewPolicyStore <String>] [-PassThru]
[-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf]
[<CommonParameters>]

Copy-NetFirewallRule [-AsJob] -AssociatedNetFirewallPortFilter <CimInstance>
[-CimSession <CimSession[]>] [-Confirm] [-NewGPOSession <String>] [-NewName
<String>] [-NewPolicyStore <String>] [-PassThru] [-PolicyStore <String>]
[-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Copy-NetFirewallRule [-AsJob] -AssociatedNetFirewallProfile <CimInstance>
[-CimSession <CimSession[]>] [-Confirm] [-NewGPOSession <String>] [-NewName
<String>] [-NewPolicyStore <String>] [-PassThru] [-PolicyStore <String>]
[-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Copy-NetFirewallRule [-AsJob] -AssociatedNetFirewallSecurityFilter
<CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-NewGPOSession
<String>] [-NewName <String>] [-NewPolicyStore <String>] [-PassThru]
[-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf]
[<CommonParameters>]

Copy-NetFirewallRule [-AsJob] -AssociatedNetFirewallServiceFilter
<CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-NewGPOSession
<String>] [-NewName <String>] [-NewPolicyStore <String>] [-PassThru]
[-PolicyStore <String>] [-ThrottleLimit <Int32>] [-TracePolicyStore] [-WhatIf]
[<CommonParameters>]

Copy-NetFirewallRule [-AsJob] [-CimSession <CimSession[]>] [-Confirm]
-DisplayName <String[]> [-NewGPOSession <String>] [-NewName <String>]
[-NewPolicyStore <String>] [-PassThru] [-PolicyStore <String>] [-ThrottleLimit
<Int32>] [-TracePolicyStore] [-WhatIf] [<CommonParameters>]

Copy-NetFirewallRule [-AsJob] [-CimSession <CimSession[]>] [-Confirm]
-InputObject <CimInstance[]> [-NewGPOSession <String>] [-NewName <String>]
[-NewPolicyStore <String>] [-PassThru] [-ThrottleLimit <Int32>] [-WhatIf]
[<CommonParameters>]

Copy-NetFirewallRule [-Name] <String[]> [-AsJob] [-CimSession <CimSession[]>]
[-Confirm] [-NewGPOSession <String>] [-NewName <String>] [-NewPolicyStore
<String>] [-PassThru] [-PolicyStore <String>] [-ThrottleLimit <Int32>]
[-TracePolicyStore] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Copy-NetFirewallRule cmdlet copies a firewall rule and associated filters to a policy store, making a complete clone. When a new policy store is not specified, a firewall rule is copied to the same policy store with a new name specified by the user.

This cmdlet returns one or more firewall rules to be duplicated by specifying the Name parameter (default), the DisplayName parameter, the rule properties, or by associated filters or objects. The resulting queried rule is copied to a new policy store using the NewPolicyStore parameter, a new Group Policy Object (GPO) session using the NewGPOSession parameter, or to the same policy store using the NewName parameter. Only one firewall rule can be copied at a time when copying to the same policy store. This is because only a single firewall rule can use the unique identifier, or name, specified by the NewName parameter.

When copying a rule to a new policy store, the unique name of the set is preserved. This means that if the same set is copied twice, then the second attempt returns an error that the object already exists. To overwrite the target set, first run the Remove-NetFirewallRule cmdlet. If the object may already exist, then use the ErrorAction parameter to silently ignore these errors instead of running the Remove-NetFirewallRule cmdlet.

The associated filters (NetFirewallAddressFilter, NetFirewallApplicationFilter, and so on) have a one-to-one correspondence with each firewall rule and there is no need to copy the filter objects. For more information on filters, see the Get-NetFirewallRule cmdlet.

PARAMETERS

-Action <Action[]>

Specifies that matching firewall rules of the indicated action are copied.

This parameter specifies the action that the firewall will take on traffic that matches this rule. If multiple firewall rules are defined, then the order in which the firewall rules are evaluated for a match depends on the action specified in the rule. Firewall rules are evaluated in the following order:

- Allow if secured with override block rules (for rules with the Authentication field specified with any value other than NotRequired, and with the OverrideBlockRules field enabled).

- Block the connection.

- Allow the connection.

The Default profile behavior, allow or block as specified in the NetFirewallProfile object in the corresponding store. 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.

- 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.

-All [<SwitchParameter>]

Indicates that all of the firewall rules within the specified policy store are copied.

-AsJob [<SwitchParameter>]

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

-AssociatedNetFirewallAddressFilter <CimInstance>

Gets the firewall rules that are associated with the given address filter to be copied. A NetFirewallAddressFilter object represents the address conditions associated with a rule. See the Get-NetFirewallAddressFilter cmdlet for more information.

-AssociatedNetFirewallApplicationFilter <CimInstance>

Gets the firewall rules that are associated with the given application filter to be copied. A NetFirewallApplicationFilter object represents the application linked to a rule. See the Get-NetFirewallApplicationFilter cmdlet for more information.

-AssociatedNetFirewallInterfaceFilter <CimInstance>

Gets the firewall rules that are associated with the given interface filter to be copied. A NetFirewallInterfaceFilter object represents the interface conditions linked to a rule. See the Get-NetFirewallInterfaceFilter cmdlet for more information.

-AssociatedNetFirewallInterfaceTypeFilter <CimInstance>

Gets the firewall rules that are associated with the given interface type filter to be copied. A NetFirewallInterfaceTypeFilter object represents the interface conditions linked with a rule. See the Get-NetFirewallInterfaceTypeFilter cmdlet for more information.

-AssociatedNetFirewallPortFilter <CimInstance>

Gets the firewall rules that are associated with the given port filter to be copied. A NetFirewallPortFilter object represents the port conditions associated with a rule. See the Get-NetFirewallPortFilter cmdlet for more information.

-AssociatedNetFirewallProfile <CimInstance>

Gets the firewall rules that are associated with the given firewall profile type to be copied. A NetFirewallProfile object represents the profile conditions associated with a rule. See the Get-NetFirewallProfile cmdlet for more information.

-AssociatedNetFirewallSecurityFilter <CimInstance>

Gets the firewall rules that are associated with the given security filter to be copied. A NetFirewallSecurityFilter object represents the security conditions associated with a rule. See the Get-NetFirewallSecurityFilter cmdlet for more information. The security conditions include the Authentication , Encryption , LocalUser , RemoteUser , and RemoteMachine parameters for a firewall rule.

-AssociatedNetFirewallServiceFilter <CimInstance>

Gets the firewall rules that are associated with the given service filter to be copied. A NetFirewallServiceFilter object represents the profile conditions associated with a rule. See the Get-NetFirewallServiceFilter 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.

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

-Description <String[]>

Specifies that matching firewall rules of the indicated description are

copied. Wildcard characters are accepted. This parameter specifies the localized, user-facing description of the rule. This parameter can be used to provide information about the rule, such as the rule owner, the rule requester, the purpose of the rule, a version number, or the date of creation.

-Direction <Direction[]>

Specifies that matching firewall rules of the indicated direction are copied. This parameter specifies which direction of traffic to match with this rule. The acceptable values for this parameter are: Inbound and Outbound. The default value is Inbound.

-DisplayGroup <String[]>

Specifies that only matching firewall rules of the indicated group association are copied. Wildcard characters are accepted. The Group parameter specifies the source string for this parameter. If the value for this parameter is a localizable string, then the Group parameter contains an indirect string. Rule groups can be used to organize rules by influence and allows batch rule modifications. Using the Set-NetFirewallRule cmdlet, 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 good practice to specify the Group parameter value with a universal and world-ready indirect @FirewallAPI name. This parameter cannot be specified upon object creation using the New-NetFirewallRule cmdlet, but can be modified using dot-notation and the Set-NetFirewallRule cmdlet.

-DisplayName <String[]>

Specifies that only matching firewall rules of the indicated display name are copied. Wildcard characters are accepted. This parameter specifies the localized, user-facing name of a rule. When creating a rule this parameter is required. This parameter value is locale-dependent, so this parameter value may change depending on the display language of the user.

When writing scripts that work with any language, consider using the Name parameter instead. This parameter cannot be set to All.

-EdgeTraversalPolicy <EdgeTraversal[]>

Specifies that matching firewall rules of the indicated edge traversal policy are copied. This parameter specifies how the firewall rule will handle edge traversal cases. Edge traversal allows the computer to accept unsolicited inbound packets that have passed through an edge device, such as a network address translation (NAT) router or firewall. This parameter applies to inbound rules only. The acceptable values for this parameter are:

- Block: Prevents applications from receiving unsolicited traffic from the Internet through a NAT edge device.

- Allow: Allows applications to receive unsolicited traffic directly from the Internet through a NAT edge device.

- DeferToUser: Allows the user to decide whether to allow unsolicited traffic from the Internet through a NAT edge device when an application requests it.

- DeferToApp: Allows each application to determine whether to allow unsolicited traffic from the Internet through a NAT edge device.

The default value is Block. The DeferToApp and DeferToUser options are only valid for computers running firstref_client_7, firstref_server_7, and Windows Serverr 2012.

-Enabled <Enabled[]>

Specifies that matching firewall rules of the indicated state are copied.

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. Enabling a rule causes the firewall to compare all network packets to the criteria in this rule and to perform the action specified with the Action parameter when a match is found. - False: Specifies the rule is currently disabled. Disabling the rule does not delete it, but instead causes the firewall to stop comparing network packets to the rule.

-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 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.

-InputObject <CimInstance[]>

Specifies the input object that is used in a pipeline command.

-LocalOnlyMapping <Boolean[]>

Indicates that matching firewall rules of the indicated value are copied. This parameter specifies the firewall rules for local only mapping, which describes whether a packet must pass through a local address on its 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, such as Teredo relay servers. The default value is False.

-LooseSourceMapping <Boolean[]>

Indicates that matching firewall rules of the indicated value are copied. 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 True, then the rule accepts packets incoming from a host other than the one to which the packets were sent. This parameter applies only to UDP protocol traffic, as specified with the Protocol parameter. The default value is False.

-Name <String[]>

Specifies that only matching firewall rules of the indicated name are copied. Wildcard characters are accepted. This parameter acts just like a filename, 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.

-NewGPOSession <String>

Specifies the new GPO session for one or more firewall rules.

-NewName <String>

Specifies the new name for the firewall rule.

-NewPolicyStore <String>

Specifies the policy store for one or more firewall rules.

-Owner <String[]>

Specifies that matching firewall rules of the indicated owner are copied. 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.

-PassThru [<SwitchParameter>]

Returns an object representing the item with which you are working. By default, this cmdlet does not generate any output.

-PolicyStore <String>

Targets the policy store from which the firewall rules are copied.. 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 this cmdlet or the New-NetFirewallRule cmdlet.

-PolicyStoreSource <String[]>

Specifies that firewall rules matching the indicated policy store source are copied. This parameter contains a path to the policy store where the rule originated if the object is retrieved from the ActiveStore with the TracePolicyStoreSource option set. This parameter value is automatically generated and should not be modified. The monitoring output from this parameter is not completely compatible with the PolicyStore parameter. This parameter value cannot always be passed into the PolicyStore parameter. Domain GPOs are one example in which this parameter contains only the GPO name, not the domain name.

-PolicyStoreSourceType <PolicyStoreType[]>

Specifies that firewall rules that match the indicated policy store source type are copied. This parameter describes the type of policy store where the rule originated if the object is retrieved from the ActiveStore with the TracePolicyStoreSource option set. This parameter value is automatically generated and should not be modified. The acceptable values for this parameter are:

- Local: The object originates from the local store.

- GroupPolicy: The object originates from a GPO.

- Dynamic: The object originates from the local runtime state.

This policy store name is not valid for use in the cmdlets, but may appear when monitoring active policy. - Generated: The object was generated automatically. This policy store name is not valid for use in the cmdlets, but may appear when monitoring active policy. - Hardcoded: The object was hard-coded. This policy store name is not valid for use in the cmdlets, but may appear when monitoring active policy.

-PrimaryStatus <PrimaryStatus[]>

Specifies that firewall rules that match the indicated primary status are copied. This parameter specifies the overall enforcement state of the rule. - OK: Specifies that the rule works as specified.

- Inactive: Specifies that one or more parts of the rule is not enforced.

- Error: Specifies that the computer is unable to use the rule at all.

-Status <String[]>

Specifies that firewall rules that match the indicated status are copied. This parameter describes the status message for the specified status code value. The status code is a numerical value that indicates any syntax, parsing, or runtime errors in the rule or set. This parameter value should not be modified.

-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.

-TracePolicyStore [<SwitchParameter>]

Specifies that the name of the source GPO is set to the PolicyStoreSource

parameter value.

-WhatIf [<SwitchParameter>]

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

<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:\>Copy-NetFirewallRule -DisplayName "Require Outbound Authentication" -NewName "Alternate Require Outbound Authentication"

This example copies a firewall rule, found using the localized name, to the current policy store under a new unique identifier. The localized DisplayName parameter value remains the same.

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

PS C:\>Copy-NetFirewallRule -Group "@FirewallAPI.dll,-36501" -Enabled $False -PolicyStore domain.contoso.com\GPO_name -NewPolicyStore domain.contoso.com\new_gpo

This example copies a group of firewall rules that are currently disabled to a new policy store.

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

PS C:\>Get-NetFirewallProfile -Profile Domain -PolicyStore domain.contoso.com\GPO_name | Copy-NetFirewallRule -NewPolicyStore domain.example.com\new_gpo

This example copies all of the domain firewall rules of a specified GPO to a new policy store.

REMARKS

To see the examples, type: "get-help Copy-NetFirewallRule -examples".

For more information, type: "get-help Copy-NetFirewallRule -detailed".

For technical information, type: "get-help Copy-NetFirewallRule -full".

For online help, type: "get-help Copy-NetFirewallRule -online"