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-AzFirewallNetworkRule'

*PS:\>Get-HELP New-AzFirewallNetworkRule -Full*

WARNING: The names of some imported commands from the module 'Microsoft.Azure.PowerShell.Cmdlets.Network' include unapproved verbs that might make them less discoverable.

To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.

NAME

   New-AzFirewallNetworkRule

SYNOPSIS

   Creates a Firewall Network Rule.

SYNTAX

   New-AzFirewallNetworkRule [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Description <System.String>]

   [-DestinationAddress <System.String[]>] [-DestinationFqdn <System.String[]>] [-DestinationIpGroup <System.String[]>] -DestinationPort <System.String[]> -Name

     <System.String> -Protocol {Any | TCP | UDP | ICMP} [-SourceAddress <System.String[]>] [-SourceIpGroup <System.String[]>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzFirewallNetworkRule cmdlet creates an network rule for Azure Firewall.

PARAMETERS

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with azure.

Required?                false

Position?                named

Default value            None

Accept pipeline input?     False

Accept wildcard characters?  false

-Description <System.String>

Specifies an optional description of this rule.

Required?                false

Position?                named

Default value            None

Accept pipeline input?     False

Accept wildcard characters?  false

-DestinationAddress <System.String[]>

The destination addresses of the rule

Required?                false

Position?                named

Default value            None

Accept pipeline input?     False

Accept wildcard characters?  false

-DestinationFqdn <System.String[]>

The destination FQDN of the rule


Required?              false

Position?              named

Default value          None

Accept pipeline input?      False

Accept wildcard characters?  false


-DestinationIpGroup <System.String[]>

The destination ipgroup of the rule


Required?              false

Position?              named

Default value          None

Accept pipeline input?      False

Accept wildcard characters?  false


-DestinationPort <System.String[]>

The destination ports of the rule


Required?              true

Position?              named

Default value          None

Accept pipeline input?      False

Accept wildcard characters?  false


-Name <System.String>

Specifies the name of this network rule. The name must be unique inside a rule collection.


Required?              true

Position?              named

Default value          None

Accept pipeline input?     False

Accept wildcard characters?  false


-Protocol <System.String[]>

Specifies the type of traffic to be filtered by this rule. Possible values are TCP, UDP, ICMP and Any.


Required?             true

Position?             named

Default value         None

Accept pipeline input?     False

Accept wildcard characters?  false


-SourceAddress <System.String[]>

The source addresses of the rule


Required?             false

Position?             named

Default value         None

Accept pipeline input?     False

Accept wildcard characters?  false


-SourceIpGroup <System.String[]>

The source ipgroup of the rule


Required?             false

Position?             named

Default value         None

Accept pipeline input?     False

Accept wildcard characters?  false


-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required?                    false

Position?                    named

Default value                False

Accept pipeline input?       False

Accept wildcard characters?  false


-WhatIf <System.Management.Automation.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.Azure.Commands.Network.Models.PSAzureFirewallNetworkRule


NOTES

--------- Example 1: Create a rule for all TCP traffic ---------

```
$rule = New-AzFirewallNetworkRule -Name "all-tcp-traffic" -Description "Rule for all TCP traffic" -Protocol TCP
-SourceAddress "*" -DestinationAddress "*"
  -DestinationPort "*"
```

This example creates a rule for all TCP traffic. User enforces whether traffic will be allowed or denied for a rule based on the rule collection it is associated with.

Example 2: Create a rule for all TCP traffic from 10.0.0.0 to 60.1.5.0:4040

```
$rule = New-AzFirewallNetworkRule -Name "partial-tcp-rule" -Description "Rule for all TCP traffic from 10.0.0.0 to
60.1.5.0:4040" -Protocol TCP -SourceAddress
  "10.0.0.0" -DestinationAddress "60.1.5.0" -DestinationPort "4040"
```

This example creates a rule for all TCP traffic from 10.0.0.0 to 60.1.5.0:4040. User enforces whether traffic will be allowed or denied for a rule based on the rule

collection it is associated with.

Example 3: Create a rule for all TCP and ICMP traffic from any source to 10.0.0.0/16

```
$rule = New-AzFirewallNetworkRule -Name "tcp-and-icmp-rule" -Description "Rule for all TCP and ICMP traffic from any
source to 10.0.0.0/16" -Protocol TCP,ICMP
  -SourceAddress * -DestinationAddress "10.0.0.0/16" -DestinationPort *
```

This example creates a rule for all TCP traffic from any source to 10.0.0.0/16. User enforces whether traffic will be allowed or denied for a rule based on the rule

collection it is associated with.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.network/new-azfirewallnetworkrule

New-AzFirewallNetworkRuleCollection

New-AzFirewall

Get-AzFirewall