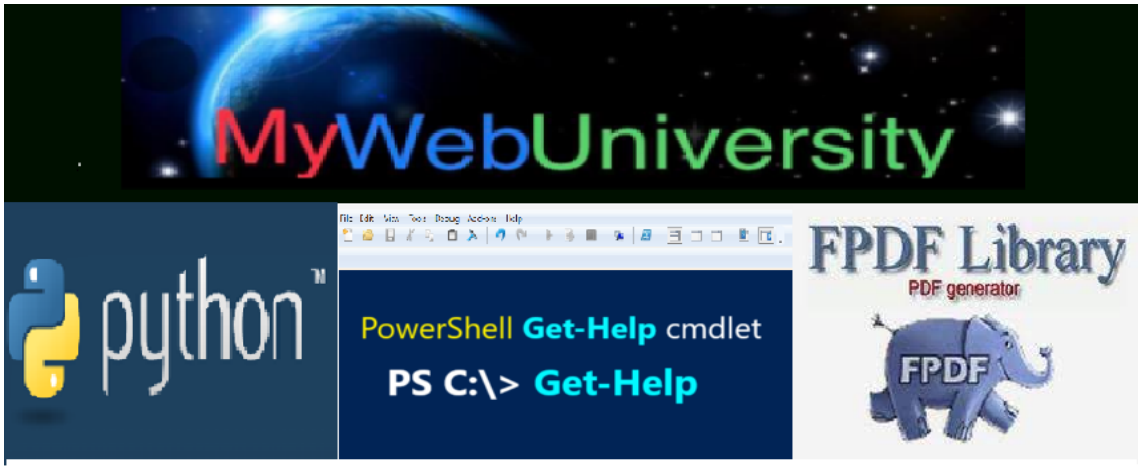

Full credit is given to all the above companies including the Operating System that this PDF file was generated!

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

PS:\>Get-HELP New-AzFirewallNetworkRuleCollection -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-AzFirewallNetworkRuleCollection

SYNOPSIS

Creates a Azure Firewall Network Collection of Network rules.

SYNTAX

New-AzFirewallNetworkRuleCollection -ActionType {Allow | Deny} [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] -Name <System.String> -Priority <System.UInt32> -Rule <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallNetworkRule[]> [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzFirewallNetworkRuleCollection cmdlet creates a collection of Firewall Network Rules.

PARAMETERS

-ActionType <System.String>

Specifies the action to be taken for traffic matching conditions of this rule. Accepted actions are "Allow" or "Deny".

Required?   true

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-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

-Name <System.String>

Specifies the name of this network rule collection. The name must be unique across all network rule collection.

Required?   true

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-Priority <System.UInt32>

Specifies the priority of this rule collection. Priority is a number between 100 and 65000. The smaller the number, the

```
higher the priority.


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


    -Rule <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallNetworkRule[]>
        Specifies the list of rules to be grouped under this collection.


        Required?                    true
        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.PSAzureFirewallNetworkRuleCollection

NOTES

---- Example 1: Create a network collection with two rules ----

```
$rule1 = New-AzFirewallNetworkRule -Name "all-udp-traffic" -Description "Rule for all UDP traffic" -Protocol UDP
-SourceAddress "*" -DestinationAddress "*"
-DestinationPort "*"
$rule2 = 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"
New-AzFirewallNetworkRuleCollection -Name RC1 -Priority 100 -Rule $rule1, $rule2 -ActionType "Allow"
```

This example creates a collection which will allow all traffic that matches either of the two rules. The first rule is for all UDP traffic. The second rule is for TCP

traffic from 10.0.0.0 to 60.1.5.0:4040. If there is another Network rule collection with higher priority (smaller number) which also matches traffic identified in

$rule1 or $rule2, the action of the rule collection with higher priority will take in effect instead.

---------- Example 2: Add a rule to a rule collection ----------

```
$rule1 = New-AzFirewallNetworkRule -Name "all-udp-traffic" -Description "Rule for all UDP traffic" -Protocol UDP
-SourceAddress "*" -DestinationAddress "*"
-DestinationPort "*"
$ruleCollection = New-AzFirewallNetworkRuleCollection -Name "MyNetworkRuleCollection" -Priority 100 -Rule $rule1
-ActionType "Allow"

$rule2 = 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"
$ruleCollection.AddRule($rule2)
```

This example creates a new network rule collection with one rule and then adds a second rule to the rule collection using method AddRule on the rule collection

object. Each rule name in a given rule collection must have a unique name and is case insensitive.

--------- Example 3: Get a rule from a rule collection ---------

```
$rule1 = New-AzFirewallNetworkRule -Name "all-udp-traffic" -Description "Rule for all UDP traffic" -Protocol UDP
-SourceAddress "*" -DestinationAddress "*"
-DestinationPort "*"
$ruleCollection = New-AzFirewallNetworkRuleCollection -Name "MyNetworkRuleCollection" -Priority 100 -Rule $rule1
-ActionType "Allow"
$getRule=$ruleCollection.GetRuleByName("ALL-UDP-traffic")
```

This example creates a new network rule collection with one rule and then gets the rule by name, calling method GetRuleByName on the rule collection object. The rule

name for method GetRuleByName is case-insensitive.

------- Example 4: Remove a rule from a rule collection -------

```
$rule1 = New-AzFirewallNetworkRule -Name "all-udp-traffic" -Description "Rule for all UDP traffic" -Protocol UDP -SourceAddress "*" -DestinationAddress "*"
-DestinationPort "*"
$rule2 = 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"
$ruleCollection = New-AzFirewallNetworkRuleCollection -Name "MyNetworkRuleCollection" -Priority 100 -Rule $rule1, $rule2 -ActionType "Allow"
$ruleCollection.RemoveRuleByName("ALL-udp-traffic")
```

This example creates a new network rule collection with two rules and then removes the first rule from the rule collection by calling method RemoveRuleByName on the

rule collection object. The rule name for method RemoveRuleByName is case-insensitive.

RELATED LINKS

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

New-AzFirewallNetworkRule

New-AzFirewall

Get-AzFirewall