Windows PowerShell Get-Help on Cmdlet 'Set-AzNetworkSecurityRuleConfig'

PS:\>Get-HELP Set-AzNetworkSecurityRuleConfig -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

Set-AzNetworkSecurityRuleConfig

SYNOPSIS

Updates a network security rule configuration for a network security group.

SYNTAX

Set-AzNetworkSecurityRuleConfig [-Access {Allow | Deny}] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>]

[-Description <System.String>] [-DestinationAddressPrefix <System.String[]>] [-DestinationApplicationSecurityGroup <Microsoft.Azure.Commands.Network.Models.PSApplicationSecurityGroup[]>] [-DestinationPortRange <System.String[]>] [-Direction {Inbound | Outbound}] -Name

<System.String> -NetworkSecurityGroup <Microsoft.Azure.Commands.Network.Models.PSNetworkSecurityGroup> [-Priority <System.Int32>] [-Protocol {Tcp | Udp | Icmp | Esp |

Ah | *}] [-SourceAddressPrefix <System.String[]>] [-SourceApplicationSecurityGroup

<Microsoft.Azure.Commands.Network.Models.PSApplicationSecurityGroup[]>

[-SourcePortRange <System.String[]>] [<CommonParameters>]

Set-AzNetworkSecurityRuleConfig [-Access {Allow | Deny}] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>]

[-Description <System.String>] [-DestinationAddressPrefix <System.String[]>] [-DestinationApplicationSecurityGroupId <System.String[]>] [-DestinationPortRange

<System.String[]>] [-Direction {Inbound | Outbound}] -Name <System.String> -NetworkSecurityGroup <Microsoft.Azure.Commands.Network.Models.PSNetworkSecurityGroup>

[-Priority <System.Int32>] [-Protocol {Tcp | Udp | Icmp | Esp | Ah | *}] [-SourceAddressPrefix <System.String[]>] [-SourceApplicationSecurityGroupId

<System.String[]>] [-SourcePortRange <System.String[]>] [<CommonParameters>]

DESCRIPTION

The Set-AzNetworkSecurityRuleConfig cmdlet updates a network security rule configuration for a network security group.

PARAMETERS

-Access <System.String>

Specifies whether network traffic is allowed or denied. The acceptable values for this parameter are: Allow and Deny.

Required? false

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

-Description <System.String>

Specifies a description for a rule configuration. The maximum size is 140 characters.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DestinationAddressPrefix <System.String[]>

Specifies a destination address prefix. The acceptable values for this parameter are: - A Classless Interdomain Routing (CIDR) address

- A destination IP address range

- A wildcard character (*) to match any IP address.

You can use tags such as VirtualNetwork, AzureLoadBalancer, and Internet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DestinationApplicationSecurityGroup <Microsoft.Azure.Commands.Network.Models.PSApplicationSecurityGroup[]>

The application security group set as destination for the rule. It cannot be used with 'DestinationAddressPrefix' parameter.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DestinationApplicationSecurityGroupId <System.String[]>

The application security group set as destination for the rule. It cannot be used with 'DestinationAddressPrefix' parameter.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DestinationPortRange <System.String[]>

Specifies a destination port or range. The acceptable values for this parameter are: - An integer

- A range of integers between 0 and 65535

- A wildcard character (*) to match any port

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Direction <System.String>

Specifies whether a rule is evaluated for incoming or outgoing traffic. The acceptable values for this parameter are: Inbound and Outbound.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

Specifies the name of the network security rule configuration that this cmdlet sets.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-NetworkSecurityGroup <Microsoft.Azure.Commands.Network.Models.PSNetworkSecurityGroup>

Specifies the NetworkSecurityGroup object that contains the network security rule configuration to set.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Priority <System.Int32>

Specifies the priority of a rule configuration. The acceptable values for this parameter are:An integer between 100 and 4096. The priority number must be unique

for each rule in the collection. The lower the priority number, the higher the priority of the rule.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Protocol <System.String>

Specifies the network protocol that a rule configuration applies to. The acceptable values for this parameter are: - Tcp

- Udp

- Icmp

- Esp

- Ah

- Wildcard character (*) to match all

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SourceAddressPrefix <System.String[]>

Specifies a source address prefix. The acceptable values for this parameter are: - A CIDR

- A source IP range

- A wildcard character (*) to match any IP address.

You can also use tags such as VirtualNetwork, AzureLoadBalancer and Internet.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SourceApplicationSecurityGroup <Microsoft.Azure.Commands.Network.Models.PSApplicationSecurityGroup[]>

The application security group set as source for the rule. It cannot be used with 'SourceAddressPrefix' parameter.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SourceApplicationSecurityGroupId <System.String[]>

The application security group set as source for the rule. It cannot be used with 'SourceAddressPrefix' parameter.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SourcePortRange <System.String[]>

Specifies the source port or range. The acceptable values for this parameter are: - An integer

- A range of integers between 0 and 65535

- A wildcard character (*) to match any port

Required? false

Position? named

Default value None

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

Microsoft.Azure.Commands.Network.Models.PSNetworkSecurityGroup

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSNetworkSecurityGroup

NOTES

Example 1: Change the access configuration in a network security rule

```
$nsg = Get-AzNetworkSecurityGroup -Name "NSG-FrontEnd" -ResourceGroupName "TestRG"
$nsg | Get-AzNetworkSecurityRuleConfig -Name "rdp-rule"
Set-AzNetworkSecurityRuleConfig -Name "rdp-rule" -NetworkSecurityGroup $nsg -Access "Deny"
```

The first command gets the network security group named NSG-FrontEnd, and then stores it in the variable $nsg. The second command uses the pipeline operator to pass

the security group in $nsg to Get-AzNetworkSecurityRuleConfig, which gets the security rule configuration named rdp-rule. The third command changes the access

configuration of rdp-rule to Deny. However, this overwrites the rule and only sets the parameters that are passed to the

Set-AzNetworkSecurityRuleConfig function.

NOTE: There is no way to change a single attribute

---------- Example 2 ----------

Set-AzNetworkSecurityRuleConfig -Access Allow -DestinationAddressPrefix * -DestinationPortRange 3389 -Direction Inbound -Name 'rdp-rule' -NetworkSecurityGroup <PSNetworkSecurityGroup> -Priority 1 -Protocol Tcp -SourceAddressPrefix 'Internet' -SourcePortRange *

---------- Example 3 ----------

Set-AzNetworkSecurityRuleConfig -Access Allow -Description 'Allow RDP' -DestinationAddressPrefix * -DestinationPortRange 3389 -Direction Inbound -Name 'rdp-rule' -NetworkSecurityGroup <PSNetworkSecurityGroup> -Priority 1 -Protocol Tcp -SourceAddressPrefix 'Internet' -SourcePortRange *

---------- Example 4 ----------

```
$nsg = Get-AzNetworkSecurityGroup -ResourceGroupName "MyResource" -Name "MyNsg"
($nsg.SecurityRules | Where-Object {$_.Name -eq "RuleName"}).SourceAddressPrefix = ([System.String[]] @("xxx.xxx.xxx.xxx"))
$nsg | Set-AzNetworkSecurityGroup | Get-AzNetworkSecurityRuleConfig -Name "RuleName"
```

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/az.network/set-aznetworksecurityruleconfig

Add-AzNetworkSecurityRuleConfig

Get-AzNetworkSecurityRuleConfig

New-AzNetworkSecurityRuleConfig

Remove-AzNetworkSecurityRuleConfig