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

PS:\>Get-HELP New-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

New-AzNetworkSecurityRuleConfig

SYNOPSIS

Creates a network security rule configuration.

SYNTAX

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

<Microsoft.Azure.Commands.Network.Models.PSApplicationSecurityGroup[]>] [-SourcePortRange <System.String[]>]

[<CommonParameters>]

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

DESCRIPTION

The New-AzNetworkSecurityRuleConfig cmdlet creates an Azure 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 of the network security rule configuration to create.

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 on 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 creates.

Required? true

Position? named

Default value None

Accept pipeline input? False

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 new rule configuration applies to. The acceptable values for this parameter are: -Tcp

- Udp

- wildcard character (*) to match both.

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

None

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSSecurityRule

NOTES

---- Example 1: Create a network security rule to allow RDP ----

```
$rule1 = New-AzNetworkSecurityRuleConfig -Name rdp-rule -Description "Allow RDP" `
    -Access Allow -Protocol Tcp -Direction Inbound -Priority 100 -SourceAddressPrefix `
    Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 3389
```

This command creates a security rule allowing access from the Internet to port 3389

-- Example 2: Create a network security rule that allows HTTP --

```
$rule2 = New-AzNetworkSecurityRuleConfig -Name web-rule -Description "Allow HTTP" `
    -Access Allow -Protocol Tcp -Direction Inbound -Priority 101 -SourceAddressPrefix `
    Internet -SourcePortRange * -DestinationAddressPrefix * -DestinationPortRange 80
```

This command creates a security rule allowing access from the Internet to port 80

RELATED LINKS

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

Add-AzNetworkSecurityRuleConfig

Get-AzNetworkSecurityRuleConfig

Remove-AzNetworkSecurityRuleConfig

Set-AzNetworkSecurityRuleConfig