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

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

SYNOPSIS

Creates a new custom rule for the application gateway firewall policy.

SYNTAX

New-AzApplicationGatewayFirewallCustomRule -Action {Allow | Block | Log} [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-GroupByUserSession <Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallCustomRuleGroupByUserSession[]>] -MatchCondition <Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallCondition[]> -Name <System.String> -Priority <System.Int32> [-RateLimitDuration {OneMin | FiveMins}] [-RateLimitThreshold <System.Int32>] -RuleType {MatchRule | RateLimitRule} [-State {Disabled | Enabled}]

[<CommonParameters>]

DESCRIPTION

The New-AzApplicationGatewayFirewallCustomRule creates a custom rule for firewall policy.

PARAMETERS

-Action <System.String>

Type of Actions.

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

-GroupByUserSession

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

List of match conditions.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MatchCondition <Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallCondition[]>

List of match conditions.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Name <System.String>

The Name of the Rule.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Priority <System.Int32>

Describes priority of the rule. Rules with a lower value will be evaluated before rules with a higher value.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RateLimitDuration <System.String>

Describes duration over which Rate Limit policy will be applied. Applies only when ruleType is RateLimitRule.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RateLimitThreshold <System.Int32>

Describes rate limit threshold. Applies only when ruleType is RateLimitRule.Accepted range for this value is 1 - 5000.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RuleType <System.String>

Describes type of rule.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-State <System.String>

State variable of the custom rule.

Required? false

Position? named

Default value Enabled

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.PSApplicationGatewayFirewallCustomRule

NOTES

---------- Example 1 ----------

New-AzApplicationGatewayFirewallCustomRule -Name example-rule -Priority 1 -RuleType MatchRule -MatchCondition $condtion -Action Allow

Name : example-rule

Priority : 1

RuleType : MatchRule

MatchConditions : {Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallCondition}

Action : Allow

State : Enabled

MatchConditionsText : [

```
                {
                  "MatchVariables": [
                    {
                      "VariableName": "RequestHeaders",
                      "Selector": "Malicious-Header"
                    }
                  ],
                  "OperatorProperty": "Any",
                  "NegationConditon": false
                }
               ]
```

The command creates a new custom rule with name of example-rule, priority 1 and the rule type will be MatchRule with condition defined in the condition variable, the
action will the allow.

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

New-AzApplicationGatewayFirewallCustomRule -Name example-rule -Priority 2 -RuleType MatchRule -MatchCondition $condition -Action Allow -State Disabled

```
Name               : example-rule
Priority           : 2
RuleType           : MatchRule
MatchConditions    : {Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallCondition}
Action             : Allow
State              : Disabled
MatchConditionsText : [
                {
                  "MatchVariables": [
                    {
                      "VariableName": "RequestHeaders",
```

```
        "Selector": "Malicious-Header"
      }
    ],
    "OperatorProperty": "Any",
    "NegationConditon": false
  }
]
```


The command creates a new custom rule with name of example-rule, state as Disabled, priority 2 and the rule type will be MatchRule with condition defined in the

condition variable, the action will the allow.

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

New-AzApplicationGatewayFirewallCustomRule -Name RateLimitRule3 -Priority 3 -RateLimitDuration OneMin -RateLimitThreshold 10 -RuleType RateLimitRule -MatchCondition

$condition -GroupByUserSession $groupbyUserSes -Action Allow -State Disabled

```
Name               : RateLimitRule3
Priority           : 3
RateLimitDuration  : OneMin
RateLimitThreshold : 10
RuleType           : RateLimitRule
MatchConditions    : {Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallCondition}
GroupByUserSession : {Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallCustomRuleGroupByUserSession}
Action             : Allow
State              : Disabled
MatchConditionsText : [
                      {
                        "MatchVariables": [
                          {
```

```
                    "VariableName": "RequestHeaders",
                    "Selector": "Malicious-Header"
                  }
                ],
                "OperatorProperty": "Any",
                "NegationConditon": false
              }
            ]
  GroupByUserSessionText : [
              {
                "groupByVariables": [
                  {
                    "variableName": "ClientAddr"
                  }
                ]
              }
            ]
```


The command creates a new custom rule with name of RateLimitRule3, state as Disabled, priority 3, RateLimitDuration OneMin, RateLimitThreshold 10 and the rule type

will be RateLimitRule with condition defined in the condition variable, the action will the allow, the GroupByUserSession defined in the GroupByUserSession condition

variable.

RELATED LINKS

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