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

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

SYNOPSIS

Creates a policy setting for the firewall policy

SYNTAX

New-AzApplicationGatewayFirewallPolicySetting [-CustomBlockResponseBody <System.String>] [-CustomBlockResponseStatusCode <System.Nullable`1[System.Int32]>]

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

<System.Nullable`1[System.Boolean]>] [-DisableRequestBodyCheck] [-DisableRequestBodyEnforcement <System.Nullable`1[System.Boolean]>] [-LogScrubbing

<Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallPolicyLogScrubbingConfiguration>] [-MaxFileUploadInMb <System.Int32>] [-MaxRequestBodySizeInKb

<System.Int32>] [-Mode {Prevention | Detection}] [-RequestBodyInspectLimitInKB <System.Nullable`1[System.Int32]>] [-JSChallengeCookieExpirationInMins
<System.Nullable`1[System.Int32]>] [-State {Disabled | Enabled}] [<CommonParameters>]

DESCRIPTION

The New-AzApplicationGatewayFirewallPolicySetting creates a policy settings for a firewall policy.

PARAMETERS

-CustomBlockResponseBody <System.String>

Custom Block Response Body in policy settings of the firewall policy.

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

-CustomBlockResponseStatusCode <System.Nullable`1[System.Int32]>

Custom block response status code in policy settings of the firewall policy.

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

-DisableFileUploadEnforcement <System.Nullable`1[System.Boolean]>

Disable file upload enforcement limits for WAF.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DisableRequestBodyCheck <System.Management.Automation.SwitchParameter>

Diables the requestBodyCheck in policy settings of the firewall policy.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-DisableRequestBodyEnforcement <System.Nullable`1[System.Boolean]>

Disable request body enforcement limits for WAF.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-LogScrubbing

<Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallPolicyLogScrubbingConfiguration>

To scrub sensitive log fields

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MaxFileUploadInMb <System.Int32>

Maximum fileUpload size in MB.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MaxRequestBodySizeInKb <System.Int32>

MaxRequestBodySizeInKb in policy settings of the firewall policy.

Required? false

Position? named

Default value 128

Accept pipeline input? False

Accept wildcard characters? false

-Mode <System.String>

Firewall Mode in policy settings of the firewall policy.

Required? false

Position? named

Default value Detection

Accept pipeline input? False

Accept wildcard characters? false

-RequestBodyInspectLimitInKB <System.Nullable`1[System.Int32]>

Max inspection limit in KB for request body inspection.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-JSChallengeCookieExpirationInMins <System.Nullable`1[System.Int32]>

Web Application Firewall JavaScript Challenge Cookie Expiration time in minutes.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-State <System.String>

State variable in policy settings of the firewall policy.

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.PSApplicationGatewayFirewallPolicySettings

NOTES

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

$condition = New-AzApplicationGatewayFirewallPolicySetting -State $enabledState -Mode $enabledMode -DisableRequestBodyCheck -MaxFileUploadInMb $fileUploadLimitInMb

-MaxRequestBodySizeInKb $maxRequestBodySizeInKb

The command creates a policy setting with state as $enabledState, mode as $enabledMode, RequestBodyCheck as false, FileUploadLimitInMb as $fileUploadLimitInMb and

MaxRequestBodySizeInKb as $maxRequestBodySizeInKb. The new policySettings is stored to $condition.

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

$condition = New-AzApplicationGatewayFirewallPolicySetting -State $enabledState -Mode $enabledMode -DisableRequestBodyCheck -MaxFileUploadInMb $fileUploadLimitInMb

-MaxRequestBodySizeInKb $maxRequestBodySizeInKb -LogScrubbing $logScrubbingRuleConfig

The command creates a policy setting with state as $enabledState, mode as $enabledMode, RequestBodyCheck as false, FileUploadLimitInMb as $fileUploadLimitInMb and

MaxRequestBodySizeInKb as $maxRequestBodySizeInKb with a scrubbing rule as $logScrubbingRuleConfig. The new policySettings is stored to $condition.

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

$condition = New-AzApplicationGatewayFirewallPolicySetting -State $enabledState -Mode $enabledMode -DisableRequestBodyEnforcement true -RequestBodyInspectLimitInKB

2000 -DisableRequestBodyCheck -MaxFileUploadInMb $fileUploadLimitInMb -DisableFileUploadEnforcement true -MaxRequestBodySizeInKb $maxRequestBodySizeInKb

The command creates a policy setting with state as $enabledState, mode as $enabledMode, RequestBodyEnforcement as false, RequestBodyInspectLimitInKB as 2000,

RequestBodyCheck as false, FileUploadLimitInMb as $fileUploadLimitInMb, FileUploadEnforcement as false and MaxRequestBodySizeInKb as $maxRequestBodySizeInKb. The new

policySettings is stored to $condition.

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

$condition = New-AzApplicationGatewayFirewallPolicySetting -State $enabledState -Mode $enabledMode -DisableRequestBodyCheck -MaxFileUploadInMb $fileUploadLimitInMb

-MaxRequestBodySizeInKb $maxRequestBodySizeInKb -JSChallengeCookieExpirationInMins $jsChallengeCookieExpirationInMins

The command creates a policy setting with state as $enabledState, mode as $enabledMode, RequestBodyCheck as false, FileUploadLimitInMb as $fileUploadLimitInMb and

MaxRequestBodySizeInKb as $maxRequestBodySizeInKb, JSChallengeCookieExpirationInMins as $jsChallengeCookieExpirationInMins. The new policySettings is stored to

$condition.

RELATED LINKS

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