Windows PowerShell Get-Help on Cmdlet 'New-AzApplicationGatewayWebApplicationFirewallConfiguration

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

SYNOPSIS

Creates a WAF configuration for an application gateway.

SYNTAX

New-AzApplicationGatewayWebApplicationFirewallConfiguration [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DisabledRuleGroup <Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallDisabledRuleGroup[]>] -Enabled <System.Boolean> [-Exclusion <Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallExclusion[]>] [-FileUploadLimitInMb <System.Int32>] -FirewallMode {Detection | Prevention} [-MaxRequestBodySizeInKb <System.Int32>] [-RequestBodyCheck <System.Boolean>] [-RuleSetType {OWASP}] [-RuleSetVersion <System.String>] [-Confirm] [-WhatIf]

[<CommonParameters>]

DESCRIPTION

The New-AzApplicationGatewayWebApplicationFirewallConfiguration cmdlet creates a web application firewall (WAF) configuration for an Azure application gateway.

PARAMETERS

-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

-DisabledRuleGroup <Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallDisabledRuleGroup[]>

The disabled rule groups.

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

-Enabled <System.Boolean>

Indicates whether the WAF is enabled.

Required? true
Position? named
Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Exclusion <Microsoft.Azure.Commands.Network.Models.PSApplicationGatewayFirewallExclusion[]>

The exclusion lists.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-FileUploadLimitInMb <System.Int32>

Max file upload limit in MB.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-FirewallMode <System.String>

Specifies the web application firewall mode. The acceptable values for this parameter are: - Detection

- Prevention

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MaxRequestBodySizeInKb <System.Int32>

Max request body size in KB.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RequestBodyCheck <System.Boolean>

Whether request body is checked or not.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RuleSetType <System.String>

The type of the web application firewall rule set. The acceptable values for this parameter are: - OWASP

Required? false

Position? named

Default value OWASP

Accept pipeline input? False

Accept wildcard characters? false

-RuleSetVersion <System.String>

The version of the rule set type.

Required? false

Position? named

Default value 3.0

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.PSApplicationGatewayWebApplicationFirewallConfiguration

NOTES

Example 1: Create a web application firewall configuration for an application gateway

```
$disabledRuleGroup1 = New-AzApplicationGatewayFirewallDisabledRuleGroupConfig -RuleGroupName "REQUEST-942-APPLICATION-ATTACK-SQLI" -Rules 942130,942140
$disabledRuleGroup2 = New-AzApplicationGatewayFirewallDisabledRuleGroupConfig -RuleGroupName "REQUEST-921-PROTOCOL-ATTACK"
$firewallConfig = New-AzApplicationGatewayWebApplicationFirewallConfiguration -Enabled $true -FirewallMode "Prevention" -RuleSetType "OWASP" -RuleSetVersion "3.0"
-DisabledRuleGroups $disabledRuleGroup1,$disabledRuleGroup2
```

The first command creates a new disabled rule group configuration for the rule group named "REQUEST-942-APPLICATION-ATTACK-SQLI" with rule 942130 and rule 942140
being disabled. The second command creates another disabled rule group configuration for a rule group named "REQUEST-921-PROTOCOL-ATTACK". No rules are specifically
passed and thus all rules of the rule group will be disabled. The last command then creates a WAF configuration with firewall rules disabled as configured in
$disabledRuleGroup1 and $disabledRuleGroup2. The new WAF configuration is stored in the $firewallConfig variable.

RELATED LINKS

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

Get-AzApplicationGatewayWebApplicationFirewallConfiguration

Set-AzApplicationGatewayWebApplicationFirewallConfiguration