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

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

SYNOPSIS

Creates a new Azure Firewall Policy Intrusion Detection to associate with Firewall Policy

SYNTAX

New-AzFirewallPolicyIntrusionDetection -Mode {Off | Alert | Deny} [-Profile {Basic | Standard | Advanced}] [-SignatureOverride

<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetectionSignatureOverride[]>] [-BypassTraffic

<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetectionBypassTrafficSetting[]>] [-PrivateRange <System.String[]>] [-DefaultProfile

<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-WhatIf] [-Confirm] [<CommonParameters>]

DESCRIPTION

The New-AzFirewallPolicyIntrusionDetection cmdlet creates an Azure Firewall Policy Intrusion Detection Object.

PARAMETERS

-Mode <System.String>

Intrusion Detection general state.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Profile <System.String>

Sets IDPS signatures profile.

Required? false

Position? named

Default value For newly created policy the default IDPS profile is ?Standard? and for existing policy without IDPS profile setting, the default is

?Advanced?

Accept pipeline input? False

Accept wildcard characters? false

-SignatureOverride <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetectionSignatureOverride[]>

List of specific signatures states.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-BypassTraffic <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetectionBypassTrafficSetting[]>

List of rules for traffic to bypass.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PrivateRange <System.String[]>

List of IDPS Private IP ranges.

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

-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

-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

<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.PSAzureFirewallPolicyIntrusionDetection

NOTES

------- Example 1: Create intrusion detection with mode -------

New-AzFirewallPolicyIntrusionDetection -Mode "Alert"

This example creates intrusion detection with Alert (detection) mode

Example 2: Create intrusion detection with signature overrides

$signatureOverride = New-AzFirewallPolicyIntrusionDetectionSignatureOverride -Id "123456798" -Mode "Deny"
New-AzFirewallPolicyIntrusionDetection -Mode "Alert" -SignatureOverride $signatureOverride

This example creates intrusion detection with specific signature override

Example 3: Create firewall policy with intrusion detection configured with bypass traffic setting

$bypass = New-AzFirewallPolicyIntrusionDetectionBypassTraffic -Name "bypass-setting" -Protocol "TCP" -DestinationPort "80" -SourceAddress "10.0.0.0"
-DestinationAddress "10.0.0.0"
$intrusionDetection = New-AzFirewallPolicyIntrusionDetection -Mode "Deny" -BypassTraffic $bypass
New-AzFirewallPolicy -Name fp1 -Location "westus2" -ResourceGroupName TestRg -SkuTier "Premium" -IntrusionDetection $intrusionDetection

This example creates intrusion detection with bypass traffic setting

Example 4: Create firewall policy with intrusion detection configured with private ranges setting

$intrusionDetection = New-AzFirewallPolicyIntrusionDetection -Mode "Deny" -PrivateRange @("167.220.204.0/24", "167.221.205.101/32")

New-AzFirewallPolicy -Name fp1 -Location "westus2" -ResourceGroupName TestRg -SkuTier "Premium" -IntrusionDetection $intrusionDetection

This example creates intrusion detection with bypass traffic setting

Example 5: Create firewall policy with intrusion detection profile setting

$intrusionDetection = New-AzFirewallPolicyIntrusionDetection -Mode "Deny" -Profile ?Advanced?

New-AzFirewallPolicy -Name fp1 -Location "westus2" -ResourceGroupName TestRg -SkuTier "Premium" -IntrusionDetection $intrusionDetection

This example creates intrusion detection with Alert and Deny mode and Advanced signatures Profile.

RELATED LINKS

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