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

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

SYNOPSIS

Creates a new Azure Firewall Policy

SYNTAX

New-AzFirewallPolicy [-AsJob] [-BasePolicy <System.String>] [-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DnsSetting <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyDnsSettings>] [-ExplicitProxy <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyExplicitProxy>] [-Force] [-Identity <Microsoft.Azure.Commands.Network.Models.PSManagedServiceIdentity>] [-IntrusionDetection <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetection>] -Location <System.String> -Name <System.String> [-PrivateRange <System.String[]>] -ResourceGroupName <System.String> [-SkuTier {Standard | Premium | Basic}] [-Snat

<Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySNAT>] [-SqlSetting <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySqlSetting>] [-Tag <System.Collections.Hashtable>] [-ThreatIntelMode {Alert | Deny | Off}] [-ThreatIntelWhitelist <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyThreatIntelWhitelist>] [-TransportSecurityKeyVaultSecretId <System.String>] [-TransportSecurityName <System.String>] [-UserAssignedIdentityId <System.String>] [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-AzFirewallPolicy cmdlet creates an Azure Firewall Policy.

PARAMETERS

-AsJob <System.Management.Automation.SwitchParameter>

Run cmdlet in the background

Required? false
Position? named
Default value False
Accept pipeline input? False
Accept wildcard characters? false

-BasePolicy <System.String>

The base policy to inherit from

Required? false
Position? named
Default value None
Accept pipeline input? True (ByPropertyName)
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

-DnsSetting <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyDnsSettings>

The DNS Setting

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ExplicitProxy <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyExplicitProxy>

The Explicit Proxy Settings

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Force <System.Management.Automation.SwitchParameter>

Do not ask for confirmation if you want to overwrite a resource

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Identity <Microsoft.Azure.Commands.Network.Models.PSManagedServiceIdentity>

Firewall Policy Identity to be assigned to Firewall Policy.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-IntrusionDetection <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyIntrusionDetection>

The Intrusion Detection Setting

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Location <System.String>

location.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-Name <System.String>

The resource name.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-PrivateRange <System.String[]>

The private IP ranges to which traffic won't be SNAT'ed

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-ResourceGroupName <System.String>

The resource group name.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-SkuTier <System.String>

Firewall policy sku tier

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Snat <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySNAT>

The private IP addresses/IP ranges to which traffic will not be SNAT in Firewall Policy.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SqlSetting <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicySqlSetting>

The SQL related setting

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Tag <System.Collections.Hashtable>

A hashtable which represents resource tags.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ThreatIntelMode <System.String>

The operation mode for Threat Intelligence.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? false

-ThreatIntelWhitelist <Microsoft.Azure.Commands.Network.Models.PSAzureFirewallPolicyThreatIntelWhitelist>

The allowlist for Threat Intelligence

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TransportSecurityKeyVaultSecretId <System.String>

Secret Id of (base-64 encoded unencrypted pfx) 'Secret' or 'Certificate' object stored in KeyVault

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-TransportSecurityName <System.String>

Transport security name

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-UserAssignedIdentityId <System.String>

ResourceId of the user assigned identity to be assigned to Firewall Policy.

Required? false

Position? named

Default value None

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

System.String

System.Collections.Hashtable

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSAzureFirewall

NOTES

---------- Example 1: Create an empty policy ----------

New-AzFirewallPolicy -Name fp1 -ResourceGroupName TestRg

This example creates an azure firewall policy

--- Example 2: Create an empty policy with ThreatIntel Mode ---

New-AzFirewallPolicy -Name fp1 -ResourceGroupName TestRg -ThreatIntelMode "Deny"

This example creates an azure firewall policy with a threat intel mode

- Example 3: Create an empty policy with ThreatIntelWhitelist -

$threatIntelWhitelist = New-AzFirewallPolicyThreatIntelWhitelist -IpAddress 23.46.72.91,192.79.236.79 -FQDN microsoft.com

New-AzFirewallPolicy -Name fp1 -ResourceGroupName TestRg -ThreatIntelWhitelist $threatIntelWhitelist

This example creates an azure firewall policy with a threat intel allowlist

Example 4: Create policy with intrusion detection, identity and transport security

```
$bypass = New-AzFirewallPolicyIntrusionDetectionBypassTraffic -Name "bypass-setting" -Protocol "TCP" -DestinationPort "80" -SourceAddress "10.0.0.0"
-DestinationAddress "*"
$signatureOverride = New-AzFirewallPolicyIntrusionDetectionSignatureOverride -Id "123456798" -Mode "Deny"
$intrusionDetection = New-AzFirewallPolicyIntrusionDetection -Mode "Alert" -SignatureOverride $signatureOverride -BypassTraffic $bypass
$userAssignedIdentity =
'/subscriptions/9e223dbe-3399-4e19-88eb-0975f02ac87f/resourcegroups/TestRg/providers/Microsoft.ManagedIdentity/userAssignedIdentities/user-assign-identity'
New-AzFirewallPolicy -Name fp1 -Location "westus2" -ResourceGroupName TestRg -SkuTier "Premium" -IntrusionDetection $intrusionDetection -TransportSecurityName tsName
-TransportSecurityKeyVaultSecretId "https://<keyvaultname>.vault.azure.net/secrets/cacert" -UserAssignedIdentityId $userAssignedIdentity
```

This example creates an azure firewall policy with a intrusion detection in mode alert, user assigned identity and transport security

Example 5: Create an empty Firewall Policy with customized private range setup

```
New-AzFirewallPolicy -Name fp1 -ResourceGroupName TestRg -PrivateRange @("99.99.99.0/24", "66.66.0.0/16")
```

This example creates a Firewall that treats "99.99.99.0/24" and "66.66.0.0/16" as private ip ranges and won't snat traffic to those addresses

Example 6: Create an empty Firewall Policy with Explicit Proxy Settings

```
$exProxy = New-AzFirewallPolicyExplicitProxy -EnableExplicitProxy -HttpPort 100 -HttpsPort 101 -EnablePacFile
-PacFilePort 130 -PacFile
"sampleurlfortesting.blob.core.windowsnet/nothing"
New-AzFirewallPolicy -Name fp1 -ResourceGroupName TestRg -ExplicitProxy $exProxy


BasePolicy                : null
DnsSettings               : null
Etag                      : null
ExplicitProxy
 EnableExplicitProxy      : true
 EnablePacFile            : true
 HttpPort                 : 100
 HttpsPort                : 101
 PacFile                  : "sampleurlfortesting.blob.core.windowsnet/nothing"
 PacFilePort              : 130
Id                        : null
Identity                  : null
IntrusionDetection        : null
Location                  : "westus2"
Name                      : "fp1"
PrivateRange              : null
PrivateRangeText          : "[]"
ProvisioningState         : null
ResourceGroupName         : "TestRg"
ResourceGuid              : null
RuleCollectionGroups      : null
Sku
 Tier                     : "Standard"
Snat
 AutoLearnPrivateRanges : null
 PrivateRanges            : null
SqlSetting                : null
```

Tag : null

TagsTable : null

ThreatIntelMode : "Alert"

ThreatIntelWhitelist : null

TransportSecurity : null

Type : null

This example creates a firewall policy with explicit proxy settings

RELATED LINKS

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

New-AzFirewallPolicyExplicitProxy

New-AzFirewallPolicySnat