



Windows PowerShell Get-Help on Cmdlet 'Get-AzFirewall'

PS:\>Get-HELP Get-AzFirewall -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

Get-AzFirewall

SYNOPSIS

Gets a Azure Firewall.

SYNTAX

```

Get-AzFirewall [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-Name
<System.String>] [-ResourceGroupName
<System.String>] [<CommonParameters>]
```

DESCRIPTION

The Get-AzFirewall cmdlet gets one or more Firewalls in a resource group.

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

-Name <System.String>

Specifies the name of the Firewall that this cmdlet gets.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? true

-ResourceGroupName <System.String>

Specifies the name of the resource group that Firewall belongs to.

Required? false

Position? named

Default value None

Accept pipeline input? True (ByPropertyName)

Accept wildcard characters? true

<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

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSAzureFirewall

System.Collections.Generic.IEnumerable`1[[Microsoft.Azure.Commands.Network.Models.PSAzureFirewall,
Microsoft.Azure.PowerShell.Cmdlets.Network, Version=1.0.0.0,
Culture=neutral, PublicKeyToken=null]]

NOTES

---- Example 1: Retrieve all Firewalls in a resource group ----

Get-AzFirewall -ResourceGroupName rgName

Name : azFw

ResourceGroupName : rgName

Location : westcentralus

Id : /subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Micros
oft.Network/azureFirewalls/azFw

Etag : W/"00000000-0000-0000-0000-000000000000"

```

ResourceGuid      :
ProvisioningState  : Succeeded
Tags              :
IpConfigurations  : [
    {
        "Name": "AzureFirewallIpConfiguration",
        "Etag": "W/"00000000-0000-0000-0000-000000000000\"",
        "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/azureFirewalls/azFw/azureFirewallIpConfigurations/AzureFirewallIpConfiguration",
        "PrivateIpAddress": "x.x.x.x",
        "Subnet": {
            "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/virtualNetworks/vnetname/subnets/AzureFirewallSubnet"
        },
        "PublicIpAddress": {
            "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/publicIPAddresses/publicipname"
        }
    }
]

ApplicationRuleCollections : []
NatRuleCollections        : []
NetworkRuleCollections    : []
Zones                     : {}

Name                      : azFw1
ResourceGroupName         : rgName
Location                  : westcentralus
Id                        : /subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/azureFirewalls/azFw1
Etag                      : W/"00000000-0000-0000-0000-000000000000"
ResourceGuid              :

```

ProvisioningState : Succeeded

Tags :

IpConfigurations : [

```
{
  "Name": "AzureFirewallIpConfiguration",
  "Etag": "W/\"00000000-0000-0000-0000-000000000000\\\"",
  "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/azureFirewalls/azFw1/azureFirewallIpConfigurations/AzureFirewallIpConfiguration",
  "PrivateIpAddress": "x.x.x.x",
  "Subnet": {
    "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/virtualNetworks/vnetname/subnets/AzureFirewallSubnet"
  },
  "PublicIpAddress": {
    "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/publicIPAddresses/publicipname"
  }
}
```

ApplicationRuleCollections : []

NatRuleCollections : []

NetworkRuleCollections : []

Zones : {}

This example retrieves all Firewalls in resource group "rgName".

----- Example 2: Retrieve a Firewall by name -----

Get-AzFirewall -ResourceGroupName rgName -Name azFw

Name : azFw

```

ResourceGroupName      : rgName
Location               : westcentralus
Id                    : /subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Micros
                        oft.Network/azureFirewalls/azFw
Etag                   : W/"00000000-0000-0000-0000-000000000000"
ResourceGuid          :
ProvisioningState      : Succeeded
Tags                  :
IpConfigurations       : [
                        {
                          "Name": "AzureFirewallIpConfiguration",
                          "Etag": "W/"00000000-0000-0000-0000-000000000000\"",
                          "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/provi
                              ders/Microsoft.Network/azureFirewalls/azFw/azureFirewallIpConfigurations/AzureFirewallIp
                              Configuration",
                          "PrivateIpAddress": "x.x.x.x",
                          "Subnet": {
                            "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/pro
                              viders/Microsoft.Network/virtualNetworks/vnetname/subnets/AzureFirewallSubnet"
                          },
                          "PublicIpAddress": {
                            "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/pro
                              viders/Microsoft.Network/publicIPAddresses/publicipname"
                          }
                        }
                      ]
ApplicationRuleCollections : []
NatRuleCollections        : []
NetworkRuleCollections     : []
Zones                     : {}

```

This example retrieves Firewall named "azFw" in resource group "rgName".

----- Example 3: Retrieve all Firewalls with filtering -----

Get-AzFirewall -Name azFw*

```
Name           : azFw
ResourceGroupName : rgName
Location        : westcentralus
Id              : /subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/azureFirewalls/azFw
Etag            : W/"00000000-0000-0000-0000-000000000000"
ResourceGuid     :
ProvisioningState : Succeeded
Tags             :
IpConfigurations : [
    {
        "Name": "AzureFirewallIpConfiguration",
        "Etag": "W/"00000000-0000-0000-0000-000000000000\"",
        "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/azureFirewalls/azFw/azureFirewallIpConfigurations/AzureFirewallIpConfiguration",
        "PrivateIpAddress": "x.x.x.x",
        "Subnet": {
            "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/virtualNetworks/vnetname/subnets/AzureFirewallSubnet"
        },
        "PublicIpAddress": {
            "Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/publicIPAddresses/publicipname"
        }
    }
]
ApplicationRuleCollections : []
```

NatRuleCollections : []

NetworkRuleCollections : []

Zones : {}

Name : azFw1

ResourceGroupName : rgName

Location : westcentralus

Id : /subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/azureFirewalls/azFw1

Etag : W/"00000000-0000-0000-0000-000000000000"

ResourceGuid :

ProvisioningState : Succeeded

Tags :

IpConfigurations : [

{

"Name": "AzureFirewallIpConfiguration",

"Etag": "W/"00000000-0000-0000-0000-000000000000\"",

"Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/azureFirewalls/azFw1/azureFirewallIpConfigurations/AzureFirewallIpConfiguration",

"PrivateIpAddress": "x.x.x.x",

"Subnet": {

"Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/virtualNetworks/vnetname/subnets/AzureFirewallSubnet"

},

"PublicIpAddress": {

"Id": "/subscriptions/00000000-0000-0000-0000-000000000000/resourceGroups/rgName/providers/Microsoft.Network/publicIPAddresses/publicipname"

}

}

]

ApplicationRuleCollections : []

NatRuleCollections : []

NetworkRuleCollections : []

Zones : {}

This example retrieves all Firewalls that start with "azFw"

Example 4: Retrieve a firewall and then add a application rule collection to the Firewall

```
$azFw=Get-AzFirewall -Name "azFw" -ResourceGroupName "rgName"

$appRule = New-AzFirewallApplicationRule -Name R1 -Protocol "http:80","https:443" -TargetFqdn "*google.com",
"*microsoft.com" -SourceAddress "10.0.0.0"

$appRuleCollection = New-AzFirewallApplicationRuleCollection -Name "MyAppRuleCollection" -Priority 100 -Rule
$appRule -ActionType "Allow"

$azFw.AddApplicationRuleCollection($appRuleCollection)
```

This example retrieves a firewall, then adds a application rule collection to the firewall by calling method AddApplicationRuleCollection.

Example 5: Retrieve a firewall and then add a network rule collection to the Firewall

```
$azFw=Get-AzFirewall -Name "azFw" -ResourceGroupName "rgName"

$netRule = New-AzFirewallNetworkRule -Name "all-udp-traffic" -Description "Rule for all UDP traffic" -Protocol "UDP"
-SourceAddress "*" -DestinationAddress "*"
-DestinationPort "*"

$netRuleCollection = New-AzFirewallNetworkRuleCollection -Name "MyNetworkRuleCollection" -Priority 100 -Rule
$netRule -ActionType "Allow"

$azFw.AddNetworkRuleCollection($netRuleCollection)
```

This example retrieves a firewall, then adds a network rule collection to the firewall by calling method AddNetworkRuleCollection.

Example 6: Retrieve a firewall and then retrieve a application rule collection by name from the Firewall

```
$azFw=Get-AzFirewall -Name "azFw" -ResourceGroupName "rgName"  
$getAppRc=$azFw.GetApplicationRuleCollectionByName("MyAppRuleCollection")
```

This example retrieves a firewall and then gets a rule collection by name, calling method `GetApplicationRuleCollectionByName` on the firewall object. The rule collection name for method `GetApplicationRuleCollectionByName` is case-insensitive.

Example 7: Retrieve a firewall and then retrieve a network rule collection by name from the Firewall

```
$azFw=Get-AzFirewall -Name "azFw" -ResourceGroupName "rgName"  
$getNetRc=$azFw.GetNetworkRuleCollectionByName("MyNetworkRuleCollection")
```

This example retrieves a firewall and then gets a rule collection by name, calling method `GetNetworkRuleCollectionByName` on the firewall object. The rule collection name for method `GetNetworkRuleCollectionByName` is case-insensitive.

Example 8: Retrieve a firewall and then remove a application rule collection by name from the Firewall

```
$azFw=Get-AzFirewall -Name "azFw" -ResourceGroupName "rgName"  
$azFw.RemoveApplicationRuleCollectionByName("MyAppRuleCollection")
```

This example retrieves a firewall and then removes a rule collection by name, calling method `RemoveApplicationRuleCollectionByName` on the firewall object. The rule collection name for method `RemoveApplicationRuleCollectionByName` is case-insensitive.

Example 9: Retrieve a firewall and then remove a network rule collection by name from the Firewall

```
$azFw=Get-AzFirewall -Name "azFw" -ResourceGroupName "rgName"
```

```
$azFw.RemoveNetworkRuleCollectionByName("MyNetworkRuleCollection")
```

This example retrieves a firewall and then removes a rule collection by name, calling method `RemoveNetworkRuleCollectionByName` on the firewall object. The rule

collection name for method `RemoveNetworkRuleCollectionByName` is case-insensitive.

Example 10: Retrieve a firewall and then allocate the firewall

```
$vnet=Get-AzVirtualNetwork -Name "vnet" -ResourceGroupName "rgName"
```

```
$publicIp=Get-AzPublicIpAddress -Name "firewallpip" -ResourceGroupName "rgName"
```

```
$azFw=Get-AzFirewall -Name "azFw" -ResourceGroupName "rgName"
```

```
$azFw.Allocate($vnet, $publicIp)
```

This example retrieves a firewall and calls `Allocate` on the firewall to start the firewall service using the configuration (application and network rule collections)

associated with the firewall.

RELATED LINKS

Online Version: <https://learn.microsoft.com/powershell/module/az.network/get-azfirewall>

New-AzFirewall

Remove-AzFirewall

Set-AzFirewall