MyWebUniversity

python PowerShell FPDF Library PDF generator

Full credit is given to the above companies including the OS that this PDF file was generated!

PowerShell Get-Help on command 'Get-NetFirewallServiceFilter'

PS C:\Users\wahid> Get-Help Get-NetFirewallServiceFilter

NAME

Get-NetFirewallServiceFilter

SYNOPSIS

Retrieves service filter objects from the target computer.

SYNTAX

```
Get-NetFirewallServiceFilter [-All] [-AsJob] [-CimSession <CimSession[]>]
[-GPOSession <String>] [-PolicyStore <String>] [-ThrottleLimit <Int32>]
[<CommonParameters>]

Get-NetFirewallServiceFilter [-AsJob] -AssociatedNetFirewallRule <CimInstance>
[-CimSession <CimSession[]>] [-GPOSession <String>] [-PolicyStore <String>]
[-ThrottleLimit <Int32>] [<CommonParameters>]

Get-NetFirewallServiceFilter [-AsJob] [-CimSession <CimSession[]>]
[-GPOSession <String>] [-PolicyStore <String>] [-Service <String[]>]
[-ThrottleLimit <Int32>] [<CommonParameters>]
```

DESCRIPTION

The Get-NetFirewallServiceFilter cmdlet returns the service filter objects associated with the piped input firewall rules.

Service filter objects represent the Windows services associated with firewalls rules. The Service parameter of a single rule is represented in a separate NetFirewallServiceFilter object. The filter-to-rule relationship is always one-to-one and is managed automatically. Rule parameters associated with filters can only be queried using filter objects.

This cmdlet displays the service settings associated with firewall rules. This allows for rule querying based on the Service parameter. The resultant filters are passed into the Get-NetFirewallRule cmdlet to return the rules queried by service.

To modify the service conditions, two methods can be used starting with the service filters returned by this cmdlet. The array of NetFirewallServiceFilter objects can be piped into the Get-NetFirewallRule cmdlet, which returns the rules associated with the filters. These rules are then piped into the Set-NetFirewallRule cmdlet where the service properties can be configured. Alternatively, piping the array of NetFirewallServiceFilter objects directly to this cmdlet allows the Service parameter of the rules to be modified.

PARAMETERS

-All [<SwitchParameter>]

Indicates that all of the service filters within the specified policy store are retrieved.

-AsJob [<SwitchParameter>]

Runs the cmdlet as a background job. Use this parameter to run commands that take a long time to complete.

-AssociatedNetFirewallRule <CimInstance>

Gets the service filters associated with the specified firewall rule to be retrieved. This parameter represents a firewall rule, which defines how traffic is filtered by the firewall. See the New-NetFirewallRule cmdlet for more information.

-CimSession <CimSession[]>

Runs the cmdlet in a remote session or on a remote computer. Enter a computer name or a session object, such as the output of a New-CimSession (https://go.microsoft.com/fwlink/p/?LinkId=227967) or [Get-CimSession](https://go.microsoft.com/fwlink/p/?LinkId=227966)cmdlet. The default is the current session on the local computer.

-GPOSession <String>

Specifies the network Group Policy Object (GPO) from which to retrieve the rules to be retrieved. This parameter is used in the same way as the PolicyStore parameter. When modifying GPOs in Windows PowerShellr, each change to a GPO requires the entire GPO to be loaded, modified, and saved back. On a busy Domain Controller (DC), this can be a slow and resource-heavy operation. A GPO session loads a domain GPO onto the local computer and makes all of the changes in a batch, before saving it back. This reduces the load on the DC and speeds up the Windows PowerShell cmdlets. To load a GPO Session, use the Open-NetGPO cmdlet. To save a GPO Session, use the Save-NetGPO cmdlet.

-PolicyStore <String>

Specifies the policy store from which to retrieve the rules to be retrieved. A policy store is a container for firewall and IPsec policy. The acceptable values for this parameter are:

- PersistentStore: Sometimes called static rules, this store contains the persistent policy for the local computer. This policy is not from GPOs, and has been created manually or programmatically (during application installation) on the computer. Rules created in this store are attached to the ActiveStore and activated on the computer immediately. - ActiveStore: This store contains the currently active policy, which is the sum of all policy stores that apply to the computer. This is the resultant set of policy (RSOP) for the local computer (the sum of all GPOs that apply to the computer), and the local stores (the PersistentStore, the static Windows service hardening (WSH), and the configurable WSH). ---- GPOs are also policy stores. Computer GPOs can be specified as follows. ------ `-PolicyStore hostname`.

---- Active Directory GPOs can be specified as follows.

------ `-PolicyStore domain.fqdn.com\GPO_Friendly_Namedomain.fqdn.comGPO_Friendly_Name`.

------ Such as the following.

-------- `-PolicyStore localhost`

-------- `-PolicyStore corp.contoso.com\FirewallPolicy`

---- Active Directory GPOs can be created using the New-GPO cmdlet or the Group Policy Management Console. - RSOP: This read-only store contains the sum of all of the GPOs applied to the local computer.

- SystemDefaults: This read-only store contains the default state of firewall rules that ship with Windows Serverr 2012.

- StaticServiceStore: This read-only store contains all the service restrictions that ship with Windows Server 2012.

Optional and product-dependent features are considered part of Windows

Server 2012 for the purposes of WFAS. - ConfigurableServiceStore: This read-write store contains all the service restrictions that are added for third-party services. In addition, network isolation rules that are created for Windows Store application containers will appear in this policy store. The default value is PersistentStore. The Set-NetFirewallRule cmdlet cannot be used to add an object to a policy store. An object can only be added to a policy store at creation time with the Copy-NetFirewallRule cmdlet or with the New-NetFirewallRule cmdlet.

-Service <String[]>

Specifies the short name of a Windows Server 2012 service to which the firewall rule applies. If service is not specified, then network traffic generated by any program or service matches this rule. Querying for rules with this parameter can only be performed using filter objects.

-ThrottleLimit <Int32>

Specifies the maximum number of concurrent operations that can be established to run the cmdlet. If this parameter is omitted or a value of `0` is entered, then Windows PowerShellr calculates an optimum throttle limit for the cmdlet based on the number of CIM cmdlets that are running on the computer. The throttle limit applies only to the current cmdlet, not to the session or to the computer.

<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).

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

```
PS C:\>Get-NetFirewallServiceFilter -PolicyStore ActiveStore
```

This cmdlet shows the same information in a dynamically-sized, formatted table.

```
PS C:\>Get-NetFirewallServiceFilter -PolicyStore ActiveStore | Format-Table -
Property *
```

This example retrieves the service conditions associated with all of the firewall rules in the active store. Running this cmdlet without specifying the policy store retrieves the persistent store.

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

```
PS C:\>Get-NetFirewallRule -DisplayName "Wireless Portable Devices" |
Get-NetFirewallServiceFilter
```

This example gets the service associated with a firewall rule specified by using the localized name.

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

```
PS C:\>Get-NetFirewallServiceFilter -Service dnscache | Get-NetFirewallRule |
Where-Object -Property { $_.Enabled -Eq "False" }
```

This example gets the disabled firewall rules associated with the dnscache service from the persistent store.

REMARKS

To see the examples, type: "get-help Get-NetFirewallServiceFilter -examples".

For more information, type: "get-help Get-NetFirewallServiceFilter -detailed".

For technical information, type: "get-help Get-NetFirewallServiceFilter -full".

For online help, type: "get-help Get-NetFirewallServiceFilter -online"