MyWebUniversity

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

PowerShell Get-Help on command 'Get-NetFirewallAddressFilter'

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

```
NAME
    Get-NetFirewallAddressFilter


SYNOPSIS
    Retrieves address filter objects from the target computer.



SYNTAX
    Get-NetFirewallAddressFilter [-All] [-AsJob] [-CimSession <CimSession[]>]
    [-GPOSession <String>] [-PolicyStore <String>] [-ThrottleLimit <Int32>]
    [<CommonParameters>]


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


    Get-NetFirewallAddressFilter [-AsJob] -AssociatedNetIPsecMainModeRule
    <CimInstance> [-CimSession <CimSession[]>] [-GPOSession <String>]
    [-PolicyStore <String>] [-ThrottleLimit <Int32>] [<CommonParameters>]


    Get-NetFirewallAddressFilter [-AsJob] -AssociatedNetIPsecRule <CimInstance>
```

[-CimSession <CimSession[]>] [-GPOSession <String>] [-PolicyStore <String>]
[-ThrottleLimit <Int32>] [<CommonParameters>]

DESCRIPTION

The Get-NetFirewallAddressFilter cmdlet returns address filter objects associated with the input rules.

Address filter objects represent the local and remote addresses associated with the input rules. The LocalAddress and RemoteAddress parameters of a single rule are represented in a separate NetFirewallAddressFilter 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 retrieves the addresses associated with firewall, IPsec, and IPsec main-mode rules. This allows for rule querying based on address fields using the LocalAddress or RemoteAddress parameters; this cmdlet returns filter objects that may be further queried with the Where-Object (https://go.microsoft.com/fwlink/?LinkID=113423)cmdlet. The resultant filters are passed to the Get-NetFirewallRule, Get-NetIPsecRule, or Get-NetIPsecMainModeRule cmdlet to return the rules queried by address.

To modify rule address conditions, two methods can be used starting with the address filters returned by this cmdlet and optional additional querying.

- The address filter objects can be piped into the Get-NetFirewallRule, Get-NetIPsecRule, or Get-NetIPsecMainModeRule cmdlet, which returns the rule objects associated with the filters. These rules are then piped into the Set-NetFirewallRule, Set-NetIPsecRule, or Set-NetIPsecMainModeRule cmdlet where the address properties can be configured. - Alternatively, piping the address filter objects directly into the Set-NetFirewallAddressFilter cmdlet allows the LocalAddress and RemoteAddress parameters of the rules to be

```
    specified.



PARAMETERS
    -All [<SwitchParameter>]
        Indicates that all of the address 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 address filter object 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.

    -AssociatedNetIPsecMainModeRule <CimInstance>
        Gets the address filter objects that are associated, via the pipeline,
        with the input main mode rule to be retrieved.  A NetIPsecMainModeRule
        object represents a main mode rule, which alters the behavior of main mode
        authentications. Main mode negotiation establishes a secure channel
        between two computers by determining a set of cryptographic protection
        suites, exchanging keying material to establish a shared secret key, and
        authenticating computer and user identities. See the
        Get-NetIPsecMainModeRule cmdlet for more information.

    -AssociatedNetIPsecRule <CimInstance>
        Gets the address filter objects that are associated, via the pipeline,
        with the input IPsec rule to be retrieved.  A NetIPsecRule object
        represents an IPsec rule, which determines IPsec behavior. An IPsec rule
        can be associated with Phase1AuthSet, Phase2AuthSet, and NetIPsecQuickMode
```

cryptographic sets. See the New-NetIPsecMainModeRule 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 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 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 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.

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.

-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-NetIPsecRule -PolicyStore ActiveStore
```

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

```
PS C:\>Get-NetIPsecRule -PolicyStore ActiveStore | Format-Table
```

This example retrieves the addresses associated with all the rules in the active store. Running this cmdlet without specifying the policy store retrieves the persistent store.

-------------------------- EXAMPLE 2 --------------------------

```
PS C:\>Get-NetFirewallRule -DisplayGroup "Core Networking" |
Get-NetFirewallAddressFilter | Where-Object -FilterScript { $_.RemoteAddress
-Eq "LocalSubnet6" }
```

This example gets the address configurations associated with a particular IPsec rule.

-------------------------- EXAMPLE 3 --------------------------

```
PS C:\>Get-NetFirewallRule -DisplayGroup "Core Networking" |
Get-NetFirewallAddressFilter | Where-Object -FilterScript { $_.RemoteAddress
-Eq "LocalSubnet6" } | Set-NetFirewallAddressFilter -RemoteAddress LocalSubnet4
```

This is an alternate method with this cmdlet.

```
PS C:\>Get-NetFirewallRule -DisplayGroup "Core Networking" |
Get-NetFirewallAddressFilter | Where-Object -FilterScript { $_.RemoteAddress
-Eq "LocalSubnet6" } | Get-NetFirewallRule | Set-NetFirewallRule
-RemoteAddress LocalSubnet4
```

This example gets the filter objects associated with the firewall rules with a particular remote, second, endpoint belonging to the Core Networking group and modifies the second endpoint of those rules.

REMARKS

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

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

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

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