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-NetFirewallSecurityFilter'

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

NAME

Get-NetFirewallSecurityFilter

SYNOPSIS

Retrieves security filter objects from the target computer.

SYNTAX

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

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

Get-NetFirewallSecurityFilter [-AsJob] [-Authentication {NotRequired |
Required | NoEncap}] [-CimSession <CimSession[]>] [-Encryption {NotRequired |
Required | Dynamic}] [-GPOSession <String>] [-LocalUser <String[]>]
[-OverrideBlockRules <Boolean[]>] [-PolicyStore <String>] [-RemoteMachine
<String[]>] [-RemoteUser <String[]>] [-ThrottleLimit <Int32>]

[<CommonParameters>]

DESCRIPTION

The Get-NetFirewallSecurityFilter cmdlet returns security filter objects associated with the input firewall rules.

Security filter objects represent the security conditions associated with firewall rules. The Authentication , Encryption , OverrideBlockRules , LocalUser , RemoteUser , and RemoteMachine parameters of a single rule are represented in a separate NetFirewallSecurityFilter 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 security settings associated with firewall rules. This allows for rule querying based on the Authentication , Encryption , OverrideBlockRules , LocalUser , RemoteUser , and RemoteMachine parameters; this cmdlet returns filter objects that may be further queried with the Where-Object (https://go.microsoft.com/fwlink/?LinkID=113423)cmdlet. The cmdlet also allows the interface type filters to be obtained by filter object query. The resultant filters are passed into the Get-NetFirewallRule cmdlet to return the rules queried by security settings.

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

The array of NetFirewallSecurityFilter 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 interface properties can be configured.

Alternatively, piping the array of NetFirewallSecurityFilter objects directly into the Set-NetFirewallSecurityFilter cmdlet allows the Authentication ,

Encryption , OverrideBlockRules , LocalUser , RemoteUser , and RemoteMachine parameters of the rules to be modified.

PARAMETERS

-All [<SwitchParameter>]

Indicates that all of the security 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 security 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.

-Authentication <Authentication[]>

Specifies that authentication is required on firewall rules. The acceptable values for this parameter are: NotRequired, Required, or NoEncap.

- NotRequired: Any network packet matches this rule, that it is protected by IPsec. This option is the equivalent of not selecting the allow only secure connections option in the Windows Firewall with Advanced Security MMC snap-in. - Required: Network packets that are authenticated by IPsec match this rule. A separate IPsec rule must be created to authenticate the traffic. This option is the equivalent of the allow only secure connections option in the Windows Firewall with Advanced Security MMC snap-in. - NoEncap: Network connections that are authenticated, but not encapsulated by Encapsulating Security Payload (ESP) or Authentication

Header (AH) match this rule. This option is useful for connections that must be monitored by network equipment, such as intrusion detection systems (IDS), that are not compatible with ESP NULL-protected network packets. The initial connection is authenticated by IPsec by using AuthIP, but the quick mode SA permits clear-text traffic. To use this option, you must also configure an IPsec rule that specifies authentication with encapsulation none as a quick mode security method. In the Microsoft Management Console (MMC), authentication and encryption are combined into one set of radio buttons. In Windows Management Instrumentation (WMI) or Windows PowerShellr, authentication and encryption are given as two separate options. The default value is Required. A rule can be queried for this condition, or modified by using the security filter object.

-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.

-Encryption <Encryption[]>

Specifies that encryption in authentication is required on firewall rules. The authentication is done through a separate IPsec or main mode rule. The acceptable values for this parameter are: NotRequired, Required, or Dynamic.

- NotRequired: Encryption is not required for authentication.

- Required: Encryption is required for authentication through an IPsec rule.

- Dynamic: This is `authdynenc` in the netsh command-line.

The default value is NotRequired. A rule can be queried for this condition, or modified by using the security filter object.

-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.

-LocalUser <String[]>

Specifies the principals for which the network traffic this firewall rule should apply. This is an SDDL string. The principals, represented by SIDs in the SDDL string, can be services, users, application containers, or any other SID that network traffic could be associated with. This parameter specifies that only network packets that are authenticated as coming from or going to a principal identified in the list of accounts (SID) match this rule. Querying for rules with this parameter can only be performed using filter objects.

-OverrideBlockRules <Boolean[]>

Allows matching network traffic that would otherwise be blocked. The network traffic must be authenticated by using a separate IPsec rule. If the Direction parameter is set to Inbound, then this parameter is valid only for rules that have one or more accounts listed in the RemoteUser parameter and optionally the RemoteMachine parameter. Network packets that

match this rule and that are successfully authenticated against a computer account specified in the RemoteUser parameter and against a user account identified in the RemoteMachine parameter are permitted through the firewall. If this parameter is specified, then the Authentication parameter cannot be set to NotRequired. This parameter is equivalent to the override block rules checkbox in the Windows Firewall with Advanced Security MMC snap-in. For computers that are running firstref_client_7 or firstref_server_7, this parameter is permitted on an outbound rule. Selecting this parameter on an outbound rule causes matching traffic to be permitted through this rule even if other matching rules would block the traffic. No accounts are required in the RemoteMachine or RemoteUser parameter for an outbound bypass rule, however, if authorized or excepted computers are listed in those groups the rules will be enforced. This parameter is not valid on outbound rules on computers that are running nextref_vista or earlier. Querying for rules with this parameter can only be performed using NetFirewallSecurityFilter objects.

-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 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.

-RemoteMachine <String[]>

Specifies that matching IPsec rules of the indicated computer accounts are retrieved. This parameter specifies that only network packets that are authenticated as incoming from or outgoing to a computer identified in the list of computer accounts (SID) match this rule. This parameter value is specified as an SDDL string. Querying for rules with this parameter can only be performed using filter objects.

-RemoteUser <String[]>

Specifies that matching IPsec rules of the indicated user accounts are retrieved. This parameter specifies that only network packets that are authenticated as incoming from or outgoing to a user identified in the list of user accounts (SID) match this rule. This parameter value is specified as an SDDL string. 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-NetFirewallSecurityFilter -PolicyStore ActiveStore

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

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

This example retrieves the security conditions associated with all 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 "Contoso Messenger" | Get-NetFirewallSecurityFilter

This example gets the security properties of a particular firewall rule.

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

PS C:\>Get-NetFirewallSecurityFilter -OverrideBlockRules $True | Get-NetFirewallRule

This example gets all of the authenticated bypass rules in the persistent store.

---------- Example 4 ----------

PS C:\>Get-NetFirewallSecurityFilter -Authentication Required | Where-Object -Property { $_.RemoteUser -Eq "$secureUserGroupSDDL" } | Get-NetFirewallRule

This example gets the firewall rules that require authentication by a specified user group.

REMARKS

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

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

For technical information, type: "get-help Get-NetFirewallSecurityFilter

-full".

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