PowerShell Get-Help on command 'Set-NetIPsecDospSetting'

PS C:\Users\wahid> Get-Help Set-NetIPsecDospSetting

```
NAME
    Set-NetIPsecDospSetting


SYNOPSIS
    Modifies existing IPsec Dos protection settings.



SYNTAX
    Set-NetIPsecDospSetting [-AsJob] [-CimSession <CimSession[]>] [-Confirm]
    [-DefBlockExemptDscp <UInt16>] [-DefBlockExemptRateLimitBytesPerSec <UInt32>]
    [-EnabledKeyingModules {None | IkeV1 | IkeV2 | AuthIP}] [-FilteringFlags {None
    | DisableDefaultBlock | FilterBlock | FilterExempt}] [-IcmpV6Dscp <UInt16>]
    [-IcmpV6RateLimitBytesPerSec <UInt32>] -InputObject <CimInstance[]>
    [-IpV6FilterExemptDscp <UInt32>] [-IpV6FilterExemptRateLimitBytesPerSec
    <UInt32>] [-IpV6IPsecAuthDscp <UInt16>] [-IpV6IPsecAuthRateLimitBytesPerSec
    <UInt32>] [-IpV6IPsecUnauthDscp <UInt32>]
    [-IpV6IPsecUnauthPerIPRateLimitBytesPerSec <UInt32>]
    [-IpV6IPsecUnauthRateLimitBytesPerSec <UInt32>] [-MaxPerIPRateLimitQueues
    <UInt32>] [-MaxStateEntries <UInt32>] [-PassThru]
    [-PerIPRateLimitQueueIdleTimeoutSeconds <UInt32>] [-PrivateInterfaceAliases
    <WildcardPattern[]>] [-PrivateV6Address <String>] [-PublicInterfaceAliases
    <WildcardPattern[]>] [-PublicV6Address <String>] [-StateIdleTimeoutSeconds
    <UInt32>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

    Set-NetIPsecDospSetting [-Name] <String[]> [-AsJob] [-CimSession
    <CimSession[]>] [-Confirm] [-DefBlockExemptDscp <UInt16>]
    [-DefBlockExemptRateLimitBytesPerSec <UInt32>] [-EnabledKeyingModules {None |
    IkeV1 | IkeV2 | AuthIP}] [-FilteringFlags {None | DisableDefaultBlock |
    FilterBlock | FilterExempt}] [-IcmpV6Dscp <UInt16>]
    [-IcmpV6RateLimitBytesPerSec <UInt32>] [-IpV6FilterExemptDscp <UInt32>]
    [-IpV6FilterExemptRateLimitBytesPerSec <UInt32>] [-IpV6IPsecAuthDscp <UInt16>]
    [-IpV6IPsecAuthRateLimitBytesPerSec <UInt32>] [-IpV6IPsecUnauthDscp <UInt32>]
    [-IpV6IPsecUnauthPerIPRateLimitBytesPerSec <UInt32>]
    [-IpV6IPsecUnauthRateLimitBytesPerSec <UInt32>] [-MaxPerIPRateLimitQueues
    <UInt32>] [-MaxStateEntries <UInt32>] [-PassThru]
    [-PerIPRateLimitQueueIdleTimeoutSeconds <UInt32>] [-PrivateInterfaceAliases
    <WildcardPattern[]>] [-PrivateV6Address <String>] [-PublicInterfaceAliases
    <WildcardPattern[]>] [-PublicV6Address <String>] [-StateIdleTimeoutSeconds
    <UInt32>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]
```

DESCRIPTION

The Set-NetIPsecDospSetting modifies existing IPsec Dos protection settings.

The settings cannot be queried by property in this cmdlet. The Get-NetIPsecDospSetting cmdlet returns the queried settings and pipes the settings into this cmdlet.

When modifying the DSCP parameters including the DefBlockExemptDscp , IcmpV6Dscp , IpV6FilterExemptDscp , IpV6IPsecAuthDscp , and IpV6IPsecUnauthDscp parameters, the parameters are case sensitive and require Disabled to by specified using dot-notation.

PARAMETERS

-AsJob [<SwitchParameter>]

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

-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.

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

-DefBlockExemptDscp <UInt16>

Specifies the 6-bit value, specified as an integer from 1 to 63, that is placed in the differentiated services code point (DSCP) field of the IPv6 header when the traffic type matches traffic that is by default exempted from the default block behavior such as IPsec authenticated, IPsec unauthenticated, and ICMPv6 traffic. The DSCP value can be used in Quality of Service (QoS) implementations to prioritize network traffic and help ensure that less important network packets do not consume so much bandwidth that they interfere with the successful delivery of more important network packets. The acceptable values for this parameter are: 1 through 63, and Disabled.

- Disabled: This turns off DSCP marking for traffic that is by default exempted from the default block behavior. This includes IPsec authenticated, IPsec unauthenticated, and ICMPv6 traffic. This parameter is case sensitive and requires Disabled to be specified using dot-notation.

The default value is Disabled.

-DefBlockExemptRateLimitBytesPerSec <UInt32>

Specifies the maximum rate at which IPsec authenticated, IPsec unauthenticated, and ICMPv6 inbound network traffic such as traffic that is by default exempted from the default block behavior is forwarded from the public interface to the internal interface. The acceptable values for this parameter are: 1 through 4,294,967,295 bytes per second. The default value is 102400.

-EnabledKeyingModules <DospKeyModules>

Specifies the IPsec negotiation protocol, or keying module, to allow. The IPv6 address or subnet to which the specified IPsec negotiation protocol is allowed to be sent with the PrivateV6Address parameter can be optionally specified. By default, only IPsec negotiation traffic that uses AuthIP is allowed to all addresses. ICMPv6 network traffic is always allowed to enable Teredo and other advanced network scenarios to work. The IPsec-protected traffic that is part of an established connection that uses ESP is always allowed, as long as the connection has not been idle for more than the number of seconds specified with the StateIdleTimeoutSeconds parameter. The acceptable values for this parameter are: None, IkeV1, IkeV2, or AuthIP. The default value is AuthIP.

-FilteringFlags <DospFlags>

Specifies the action to take on network traffic that matches the Dosp setting address filters the public V6 address and the privateV6 address. Only one filter can be applied to a specific address or subnet. If a second Dosp setting with the exact same address or subnet parameter is created, then an error is displayed. If an address matches more than one filter, then the most specific match is selected and the corresponding filter is applied. For example, 2006:2006::2 matches a filter with the prefix 2006:2006::2/128 more closely than a filter with the prefix 2006:2006::2/64. The acceptable values for this parameter are:

- None: IPsec DoS protection feature drops all IPv4 traffic, and all non-IPsec IPv6 traffic (except ICMPv6) that is forwarded between a public interface and an internal interface.

- DisableDefaultBlock: IPsec DoS protection feature blocks no traffic.

- FilterBlock: Specifies that network traffic that matches the Dosp setting address filters using the PublicV6Address and PrivateV6Address parameters is blocked even if it is IPsec-protected. - FilterExempt: Specifies that IPv6 network traffic that matches the Dosp setting address filters using the PublicV6Address and PrivateV6Address parameters does not have to be IPsec-protected to be allowed through.

The default value is None.

-IcmpV6Dscp <UInt16>

Specifies that ICMPv6 protocol traffic is assigned the given DSCP value. This parameter specifies the 6-bit value, specified as an integer from 1 to 63, that is placed in the DSCP field of the IPv6 header, when the traffic type matches ICMPv6 protocol traffic. The DSCP value can be used in Quality of Service (QoS) implementations to prioritize network traffic and help ensure that less important network packets do not consume so much bandwidth that the packets interfere with the successful delivery of more important network packets. The acceptable values for this parameter are: 1 through 63, and Disabled.

- Disabled: Turns off DSCP marking for ICMPv6 protocol traffic. This parameter is case sensitive and requires Disabled to be specified using dot-notation.

The default value is Disabled.

-IcmpV6RateLimitBytesPerSec <UInt32>

Specifies the maximum rate at which ICMPv6 inbound network traffic is forwarded from the public to the internal interface. The acceptable values for this parameter are: 1 through 4,294,967,295 bytes per second. The default value is 10240.

-InputObject <CimInstance[]>

Specifies the input object that is used in a pipeline command.

-IpV6FilterExemptDscp <UInt32>

Specifies that IPv6 traffic with an IP address that is exempted by using an address filter is assigned the given DSCP value. To specify that the IPv6 network traffic that matches the Dosp setting address filters using the PublicV6Address and PrivateV6Address parameters does not have to be IPsec-protected to be allowed through set the FilteringFlags parameter to the filter exempt value. This parameter specifies the 6-bit value, specified as an integer from 1 to 63, that is placed in the DSCP field of the IPv6 header when the traffic type matches the exempted address filter traffic. The DSCP value can be used in Quality of Service (QoS) implementations to prioritize network traffic and help ensure that less important network packets do not consume so much bandwidth that they interfere with the successful delivery of more important network packets. The acceptable values for this parameter are: 1 through 63, and Disabled.

- Disabled: Turns off DSCP marking for traffic from the specified address filter, specified with the PrivateV6Address or PublicV6Address parameter. This parameter is case sensitive and requires Disabled to be specified using dot-notation.

The default value is Disabled.

-IpV6FilterExemptRateLimitBytesPerSec <UInt32>

Specifies the maximum rate at which inbound IPv6 network traffic, that is exempted by using an address filter, is forwarded from the public to the internal interface. To specify that the IPv6 network traffic that matches the Dosp setting address filters using the PublicV6Address and PrivateV6Address parameters does not have to be IPsec-protected to be allowed through set the FilteringFlags parameter to the filter exempt value. The acceptable values for this parameter are: 1 through 4,294,967,295 bytes per second. The default value is 102400.

-IpV6IPsecAuthDscp <UInt16>

Specifies that authenticated IPv6 IPsec-protected traffic is assigned the given DSCP value. This parameter specifies the 6-bit value, specified as an integer from 1 to 63, that is placed in the DSCP field of the IPv6 header, when the traffic type matches authenticated IPv6 IPsec-protected traffic. The DSCP value can be used in Quality of Service (QoS) implementations to prioritize network traffic and help ensure that less important network packets do not consume so much bandwidth that they interfere with the successful delivery of more important network packets.

- Disabled: Turns off DSCP marking for authenticated IPv6 IPsec-protected traffic. This parameter is case sensitive and requires Disabled to be specified using dot-notation. The default value is Disabled.

-IpV6IPsecAuthRateLimitBytesPerSec <UInt32>

Specifies the maximum rate at which authenticated IPv6 IPsec-protected inbound traffic is forwarded from the public to the internal interface.
The acceptable values for this parameter are: 1 through 4,294,967,295 bytes per second. The default value is 0, which disables the rate limit for this traffic.

-IpV6IPsecUnauthDscp <UInt32>

Specifies that unauthenticated IPv6 IPsec-protected traffic is assigned the given DSCP value. This parameter specifies the 6-bit value, specified as an integer from 1 to 63, that is placed in the DSCP field of the IPv6 header when the traffic type matches unauthenticated IPv6 IPsec-protected traffic. The DSCP value can be used in Quality of Service (QoS) implementations to prioritize network traffic and help ensure that less important network packets do not consume so much bandwidth that they interfere with the successful delivery of more important network packets. The acceptable values for this parameter are: 1 through 63, and Disabled.

- Disabled: Turns off DSCP marking for unauthenticated IPv6 IPsec-protected traffic. This parameter is case sensitive and requires Disabled to be specified using dot-notation.

The default value is Disabled.

-IpV6IPsecUnauthPerIPRateLimitBytesPerSec <UInt32>

Specifies the maximum rate at which unauthenticated IPv6 IPsec-protected inbound traffic is forwarded from the public to the internal interface. If a per IP address rate limit is defined, then it is used instead of the global rate limit using the IpV6IPsecUnauthRateLimitBytesPerSec parameter. To rate limit on a per IP address basis, configure the number of per IP queues to support this by using the MaxPerIPRateLimitQueues parameter. The acceptable values for this parameter are: 1 through 4,294,967,295 bytes per second. The default value is 10240.

-IpV6IPsecUnauthRateLimitBytesPerSec <UInt32>

Specifies the maximum rate at which unauthenticated IPv6 IPsec-protected inbound traffic is forwarded from the public to the internal interface. This rate limit is applied on a per IP address basis, instead of network-wide. If a per IP address rate limit is defined using the IpV6IPsecUnauthPerIPRateLimitBytesPerSec parameter, then it is used instead of the global rate limit. To rate limit on a per IP address basis, configure the number of per IP queues to support this by using the MaxPerIPRateLimitQueues parameter. The acceptable values for this parameter are: 1 through 4,294,967,295 bytes per second. The default value is 10240.

-MaxPerIPRateLimitQueues <UInt32>

Specifies, when using rate limits on unauthenticated traffic, the maximum number of queues that can be used to hold traffic while it is delivered at the configured rate. The per IP address rate limit is defined with the IpV6IPsecUnauthPerIPRateLimitBytesPerSec parameter. The acceptable values for this parameter are: 1 through 4,294,967,295 queues. The default value is 50000.

-MaxStateEntries <UInt32>

Specifies the maximum number of connections that the IPsec DoS protection feature can track at one time. The acceptable values for this parameter are: 1 through 4,294,967,295 sessions. The default value is 75000.

-Name <String[]>

Specifies the unique identifier of the Dosp configuration setting. This parameter is mandatory.

-PassThru [<SwitchParameter>]

Returns an object representing the item with which you are working. By default, this cmdlet does not generate any output.

-PerIPRateLimitQueueIdleTimeoutSeconds <UInt32>

Specifies, when using rate limits on unauthenticated traffic on a per IP address basis, the timeout in seconds that the connection can be idle before the IPsec DoS protection feature treats the connection as stale and stops tracking the state. The per IP address rate limit is defined with the IpV6IPsecUnauthPerIPRateLimitBytesPerSec parameter. The acceptable values for this parameter are: 1 through 4,294,967,295 seconds. The default value is 360, or six minutes.

-PrivateInterfaceAliases <WildcardPattern[]>

Specifies the interface to the IPsec DoS protection configuration as an internal interface to be modified. At least one public interface using the PublicInterfaceAliases parameter and one internal interface using the PrivateInterfaceAliases parameter for the Dosp setting must be set to be operational.

-PrivateV6Address <String>

Specifies the internal IPsec address or subnet that matches the Dosp address filter. This parameter adds a filter that either blocks or allows via exempting the network traffic that is not IPv6 and IPsec-protected from the specified public address or subnet using the PublicV6Address parameter to the specified internal address or subnet using this parameter. This behavior, referring to blocking or exempting, is specified with the FilteringFlags parameter. Only one filter can be applied to a specific address or subnet. If a second rule with the exact same address or subnet parameter is created, then an error is displayed. If an address matches more than one filter, then the most specific match is selected and the corresponding filter is applied. For example, 2006:2006::2 matches a filter with the prefix 2006:2006::2/128 more closely than a filter with the prefix 2006:2006::2/64. If both the PublicV6Address parameter and this parameter are specified, then the Dosp rule treats the parameter values as a logical AND operator. Traffic matches the rule if it comes from an address with the specified public prefix and the traffic is destined for an address with the specified internal prefix. Network traffic of the specified protocol as specified using the EnabledKeyingModules parameter that is sent from an address or subnet not on the list is dropped. To specify a subnet, include the forward slash (/) followed by the number of digits that represent the network identifier.

-PublicInterfaceAliases <WildcardPattern[]>

Specifies the interface to the IPsec DoS protection configuration as a public interface to be modified. At least one public interface using the PublicInterfaceAliases parameter and one internal interface using the PrivateInterfaceAliases parameter for the Dosp setting must be added to be operational.

-PublicV6Address <String>

Specifies the external IPsec address or subnet that matches the Dosp address filter. This parameter adds a filter that either blocks or allows via exempting the network traffic that is not IPv6 and IPsec-protected from the specified public address or subnet using this parameter to the specified internal address or subnet using the PrivateV6Address parameter. This behavior, referring to blocking or exempting, is specified with the FilteringFlags parameter. Only one filter can be applied to a specific address or subnet. If a second rule with the exact same address or subnet parameter is created, then an error is displayed. If an address matches more than one filter, then the most specific match is selected and the corresponding filter is applied. For example, 2006:2006::2 matches a filter with the prefix 2006:2006::2/128 more closely than a filter with the prefix 2006:2006::2/64. If both this parameter and the PrivateV6Address parameter are specified, then the Dosp rule treats the parameter values as a logical AND operator. Traffic matches the rule if it comes from an address with the specified public prefix and the traffic is destined for an address with the specified internal prefix. Network traffic of the specified protocol as specified using the EnabledKeyingModules parameter that is sent from an address or subnet not on the list is dropped. To specify a subnet, include the forward slash (/) followed by the number of digits that represent the network identifier.

-StateIdleTimeoutSeconds <UInt32>

Specifies the number of seconds that an IPsec session can be idle before the IPsec DoS protection feature stops considering it to be a valid IPsec-protected connection that is allowed by the feature. After the specified number of seconds, the IPsec session is considered stale, and traffic that is part of the session is no longer allowed through the feature by default. The acceptable values for this parameter are: 1 through 4,294,967,295 seconds. The default value is 360, or six minutes.

-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.

-WhatIf [<SwitchParameter>]

Shows what would happen if the cmdlet runs. The cmdlet is not run.

<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:\>Set-NetIPsecDospSetting -Name PubNet-CorpNet -PublicInterfaceAliases
PubNet2
```

This example modifies the internal interface of an IPsec DosP setting by using the rule name.

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

```
PS C:\>$nipDospSetting = Get-NetIPsecDospSetting




PS C:\>$nipDospSettingPubNet = Where-Object -FilterScript {
$_.PublicInterfaceAliases -Eq "PubNet" } -InputObject $nipSospSetting
```

```
PS C:\>Set-NetIPsecDospSetting -PublicInterfaceAliases PubNet2 -InputObject
$nipDospSettingPubNet
```

This cmdlet can be run using only the pipeline.

```
PS C:\>Get-NetIPsecDospSetting | Where-Object -FilterScript {
$_.PublicInterfaceAliases -Eq "PubNet" } | Set-NetIPsecDospSetting
-PublicInterfaceAliases PubNet2
```

This example modifies the internal interface of an IPsec DosP setting by querying by property.

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

```
PS C:\>$dosPSetting = Get-NetIPsecDospSetting -Name PubNet-CorpNet




PS C:\>$dosPSetting.IpV6IPsecUnauthDscp = "Disabled"
```

This example turns off DSCP marking for unauthenticated IPv6 IPsec-protected traffic for a particular DosP setting.

REMARKS

To see the examples, type: "get-help Set-NetIPsecDospSetting -examples".

For more information, type: "get-help Set-NetIPsecDospSetting -detailed".

For technical information, type: "get-help Set-NetIPsecDospSetting -full".

For online help, type: "get-help Set-NetIPsecDospSetting -online"