MyWebUniversity
python
PowerShell Get-Help cmdlet
PS C:\> Get-Help
FPDF Library
PDF generator
FPDF
Full credit is given to all the above companies including
the Operating System that this PDF file was generated!

Windows PowerShell Get-Help on Cmdlet 'New-NetIPsecDospSetting'

PS:\>Get-HELP New-NetIPsecDospSetting -Full

NAME

New-NetIPsecDospSetting

SYNOPSIS

Creates an IPsec DoS protection setting and adds the setting to the target computer.

SYNTAX

```
        New-NetIPsecDospSetting [-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>]
-Name <String> [-PerIPRateLimitQueueIdleTimeoutSeconds
       <UInt32>] -PrivateInterfaceAliases <WildcardPattern[]> [-PrivateV6Address <String>] -PublicInterfaceAliases
<WildcardPattern[]> [-PublicV6Address <String>]
```

[-StateIdleTimeoutSeconds <UInt32>] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The New-NetIPsecDospSetting cmdlet creates an IPsec DoS protection setting and adds it to the target computer.

The NetIPsecDospSetting configurations affect only IPv6-based connections that are protected by using Encapsulating Security Payload (ESP), and the IPsec negotiation

traffic and ICMPv6 traffic that is required to establish those connections.

Architecturally, the computer on which IPsec Dosp is configured using this cmdlet is located on the network edge and is in the path for any native IPv6 traffic and

IPv6 traffic encapsulated inside tunnels such as Teredo, 6to4, and IP-HTTPS. The computer can be the same computer as the Teredo relay, 6to4 gateway or relay, or

IP-HTTPS server. In those cases, the IPsec DoS protection feature intercepts the forwarded packets after the packets are extracted from the tunnel. The only exception

is that the IPsec DoS protection feature cannot be deployed on an IPsec gateway, because IPsec tunnel traffic bypasses the IPsec DoS protection feature. To protect an

IPsec gateway, place the IPsec DoS protection feature on a separate computer that is between the Internet and the IPsec gateway.

By default, no interfaces are assigned to the IPsec DoS protection feature. At least one public interface using the PublicInterfaceAliases parameter and one internal

interface using the PrivateInterfaceAliases parameter for the feature must be added to be operational. Those features that are not specified are assigned the default

values. By default, AuthIP only is allowed to all internal addresses.

This cmdlet has no effect on existing IPsec connections; it only affects IPsec negotiation traffic that uses IKEv1, IKEv2 or AuthIP. ICMPv6 network traffic is always

allowed to enable Teredo and other advanced network scenarios to work.

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 DefBlockExemptRateLimitBytesPerSec , IcmpV6RateLimitBytesPerSec,

IpV6FilterExemptRateLimitBytesPerSec , IpV6IPsecAuthRateLimitBytesPerSec , IpV6IPsecUnauthPerIPRateLimitBytesPerSec , and IpV6IPsecUnauthRateLimitBytesPerSec

parameters limit the rate of inbound traffic of the specified type flowing from the public to the internal interface. You can specify an overall rate for all traffic

of a specified type, or you can limit the rate of the specified traffic to a specified IP address.

The following two prerequisite steps must be taken for this cmdlet to succeed. - `Set-NetIpv4Protocol -CimSession $session -GroupForwardedFragments

Enabled$sessionEnabled`

- `Set-NetIpv6Protocol -CimSession $session -GroupForwardedFragments Enabled$sessionEnabled`

- `New-NetIPsecDospSetting -CimSession $session -Name "Enforce IPsec DoS protection" -PublicInterfaceAliases $publicInterface -PrivateInterfaceAliases

$privateInterface$session"Enforce IPsec DoS protection"$publicInterface$privateInterface`

PARAMETERS

-AsJob [<SwitchParameter>]

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

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-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. The default value is 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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required? false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-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.

Required?   false

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-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. The default value is Disabled.

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

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-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.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-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. The default value is

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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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. The default value is Disabled. - 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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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. The default value is 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.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-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.

Required?   false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-MaxPerIPRateLimitQueues <UInt32>

When using rate limits on unauthenticated traffic, this value specifies 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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-Name <String>

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

Required?	true
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-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.

Required?	false
Position?	named
Default value	None

Accept pipeline input?   False

Accept wildcard characters? false

-PrivateInterfaceAliases <WildcardPattern[]>

Adds the specified interface to the IPsec DoS protection configuration as an internal interface. 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.

Required?   true

Position?   named

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-PublicInterfaceAliases <WildcardPattern[]>

Adds the specified interface to the IPsec DoS protection configuration as a public interface. 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.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-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.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-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.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-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.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

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

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

<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

None

OUTPUTS

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\NetIPsecDospSetting[]

The `Microsoft.Management.Infrastructure.CimInstance` object is a wrapper class that displays Windows Management

Instrumentation (WMI) objects. The path after the

pound sign (`#`) provides the namespace and class name for the underlying WMI object.

NOTES

-------------------------- EXAMPLE 1 --------------------------

```
PS C:\>New-NetIPsecDospSetting -Name PubNet-CorpNet -PublicInterfaceAliases PubNet -PrivateInterfaceAliases
CorpNet
```

This example adds the public and internal network adapters as interfaces of the IPsec DoS protection feature.

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

```
PS C:\>New-NetIPsecDospSetting -Name IKEv1-PubNet-CorpNet -PublicInterfaceAliases PubNet
-PrivateInterfaceAliases CorpNet -EnabledKeyingModules IKEv1
```

This example enables IKEv1 negotiation traffic to all IPv6 addresses.

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

```
PS C:\>New-NetIPsecDospSetting -Name "IKEv1-PubNet-CorpNet-3ff3:401d:1f00:baa::1" -PublicInterfaceAliases PubNet
-PrivateInterfaceAliases CorpNet
    -EnabledKeyingModules IKEv1 -Privatev6Address 3ff3:401d:1f00:baa::1
```

This example enables IKEv1 negotiation traffic to a single IPv6 addresses.

-------------------------- EXAMPLE 4 --------------------------

```
PS C:\>New-NetIPsecDospSetting -Name "Block-3ffe:401d:1f00::/64-PubNet-CorpNet" -PublicInterfaceAliases PubNet
-PrivateInterfaceAliases CorpNet -FilteringFlags
    FilterBlock -Publicv6Address 3ff3:401d:1f00:baa::1
```

This example blocks all network traffic, even IPsec-protected traffic from the specified public IPv6 subnet.

-------------------------- EXAMPLE 5 --------------------------

```
PS C:\>New-NetIPsecDospSetting -Name PubNet-CorpNet-Unauth10 -PublicInterfaceAliases PubNet -PrivateInterfaceAliases CorpNet -IpV6IPsecUnauthDscp 10
```

This example marks all unauthenticated IPsec traffic with the value of 10.

-------------------------- EXAMPLE 6 --------------------------

```
PS C:\>New-NetIPsecDospSetting -Name PubNet-CorpNet -PublicInterfaceAliases PubNet -PrivateInterfaceAliases CorpNet -IpV6IPsecUnauthRateLimitBytesPerSec 2048
```

This example limits all IPsec unauthenticated network traffic to 2048 bytes per second.

-------------------------- EXAMPLE 7 --------------------------

```
PS C:\>New-NetIPsecDospSetting -Name PubNet-CorpNet -PublicInterfaceAliases PubNet -PrivateInterfaceAliases CorpNet -StateIdleTimeoutSeconds 480 -MaxStateEntries
100000
```

This example configures the IPsec DoS protection feature to stop tracking a connection after it is idle for 480 seconds, and to track a maximum of 100,000 connections.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/netsecurity/new-netipsecdospsetting?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

Get-NetIPsecDospSetting

Remove-NetIPsecDospSetting

Set-NetIPsecDospSetting