Windows PowerShell Get-Help on Cmdlet 'Get-NetIPsecQuickModeSA'

PS:\>Get-HELP Get-NetIPsecQuickModeSA -Full

NAME

Get-NetIPsecQuickModeSA

SYNOPSIS

Returns active quick mode security associations (SAs) from the target computer.

SYNTAX

Get-NetIPsecQuickModeSA [-All] [-AsJob] [-CimSession <CimSession[]>] [-ThrottleLimit <Int32>] [<CommonParameters>]

Get-NetIPsecQuickModeSA [-AsJob] -AssociatedNetIPsecMainModeSA <CimInstance> [-CimSession <CimSession[]>] [-ThrottleLimit <Int32>] [<CommonParameters>]

Get-NetIPsecQuickModeSA [-Name] <String[]> [-AsJob] [-CimSession <CimSession[]>] [-ThrottleLimit <Int32>] [<CommonParameters>]

DESCRIPTION

The Get-NetIPsecQuickModeSA cmdlet gets an active quick mode security association (SA). Two computers can

exchange network packets within the context of the quick

mode SA once established. This cmdlet is used for policy monitoring.

A quick mode negotiation establishes a secure channel between two computers to protect the user data that is exchanged between them. During a quick mode negotiation,

the keying material is refreshed or, if necessary, new keys are generated. A protection suite that protects the IP data traffic is also selected. The exchange of

information required to negotiate a quick mode SA is performed within the context of the main mode SA. After the quick mode SA is established, the two computers can

exchange network packets within the context of the quick mode SA. There is only one main mode SA between a pair of computers, but there can be many quick mode SAs.

Monitoring quick mode SAs can provide information about which peers are currently connected to this computer, and which protection suite is protecting the data

exchanged between them. Separate SAs are created for IPv4 and IPv6 connections.

PARAMETERS

-All [<SwitchParameter>]

Indicates that all of the quick mode security associations within the specified policy store are retrieved.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-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

-AssociatedNetIPsecMainModeSA <CimInstance>

Gets the quick mode security associations associated with the specified main mode security association.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

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

-Name <String[]>

Specifies that only matching quick mode cryptographic sets of the indicated name are retrieved. Wildcard characters are accepted. This parameter acts just like a file name, in that only one rule with a given name may exist in a policy store at a time. During group policy processing and policy merge, rules that have the same name but come from multiple stores being merged, will overwrite one another so that only one exists. This overwriting behavior is desirable if the rules serve the same purpose. For instance, all of the firewall rules have specific names, so if an administrator can copy

these rules to a GPO, and the rules will

override the local versions on a local computer. Since GPOs can have precedence, if an administrator that gives a rule with a different or more specific rule the

same name in a higher-precedence GPO, then it overrides other rules that exist. The default value is a randomly assigned value. When the defaults for quick mode

encryption are overridden, specify the customized parameters and set this parameter value, making this parameter the new default setting for encryption.

Required? true

Position? 0

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

<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

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\NetIPsecMainModeSA

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.

OUTPUTS

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

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:\>Get-NetIPsecQuickModeSA

This example gets all of the IPsec quick mode SAs on the local computer.

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

PS C:\>$computer1 = "RemoteMachineName"

PS C:\>Get-NetIPsecMainModeSA -Name "196511" -CimSession $computer1 | Remove-NetIPsecQuickModeSA -CimSession $computer1

This example removes all of the active main mode cryptographic sets associated with the specified quick mode SA on a remote computer.

RELATED LINKS

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

Remove-NetIPsecMainModeSA