PowerShell Get-Help on command 'Get-NetIPsecMainModeSA'

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

```
NAME
    Get-NetIPsecMainModeSA

SYNOPSIS
    Returns active main mode security associations (SA) from the target computer.


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

    Get-NetIPsecMainModeSA [-AsJob] -AssociatedNetIPsecQuickModeSA <CimInstance>
    [-CimSession <CimSession[]>] [-ThrottleLimit <Int32>] [<CommonParameters>]

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


DESCRIPTION
    The Get-NetIPsecMainModeSA cmdlet gets an active main mode security
    association (SA). This cmdlet is used for policy monitoring.
```

An SA is generated when main mode negotiation establishes a secure, authenticated channel between two computers. The SA is the information maintained about that secure channel on the local computer so that it can use the information for future network traffic to the remote computer.

An SA is the combination of a negotiated key, security protocol, and SPI, which together define the security used to protect the communication from sender to receiver. Therefore, by looking at the security associations for this computer, which computers have connections with this computer can be determined, which type of data integrity and encryption is being used for that connection, and other information. This information can be helpful when testing IPsec policies and troubleshooting access issues.

There are four mandatory parameters that negotiated as part of the main mode SA: - The computer authentication method: Kerberos v5, certificate, or pre-shared key (PSK) authentication, provided by the NetIPsecPhase1AuthSet object. - The encryption algorithm, provided by the NetIPsecMainModeCryptoSet object. - The hashing algorithm, provided by the NetIPsecMainModeCryptoSet object. - The Diffie-Hellman (DH) key exchange group to be used for the base keying material, provided by theNetIPsecMainModeCryptoSet object.

PARAMETERS

-All [<SwitchParameter>]

Indicates that all of the main mode security associations 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.

-AssociatedNetIPsecQuickModeSA <CimInstance>

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

-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.

-Name <String[]>

Specifies that only matching main mode rules 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 main mode encryption are overridden, specify the customized parameters and set this parameter value, making this parameter the new default setting for encryption.

-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-NetIPsecMainModeSA -PolicyStore ActiveStore
```

This example returns all of the active main mode cryptographic sets 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 quick mode cryptographic sets associated with the specified main mode security association on a remote computer.

REMARKS

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

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

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

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