



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 'Find-NetIPsecRule'

PS C:\Users\wahid> Get-Help Find-NetIPsecRule

NAME

Find-NetIPsecRule

SYNOPSIS

Gets IPsec rules that match specified criteria.

SYNTAX

```
Find-NetIPsecRule [-AsJob] [-CimSession <CimSession[]>] [-LocalAddress  
<String>] [-LocalPort <UInt16>] [-Protocol <String>] -RemoteAddress <String>  
[-RemotePort <UInt16>] [-ThrottleLimit <Int32>] [<CommonParameters>]
```

DESCRIPTION

The Find-NetIPsecRule cmdlet gets IPsec rules that match the criteria that you specify.

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.

-LocalAddress <String>

Specifies the local IP address of a connection. The cmdlet gets the IPsec rules that are matched to the IP address that you specify. This parameter value is the first end point of an IPsec rule and specifies the computers that are subject to the requirements of the rule. The acceptable values for this parameter are:

- Single IPv4 Address: 1.2.3.4
- Single IPv6 Address: fe80::1
- IPv4 Subnet (by network bit count): 1.2.3.4/24
- IPv6 Subnet (by network bit count): fe80::1/48
- IPv4 Subnet (by network mask): 1.2.3.4/255.255.255.0
- IPv4 Range: 1.2.3.4 through 1.2.3.7
- IPv6 Range: fe80::1 through fe80::9

-LocalPort <UInt16>

Specifies the local port of the connection. The cmdlet gets the IPsec rules that are matched to the IP port number that you specify. This

parameter value is the first end point of an IPsec rule. The acceptable values for this parameter are: a port, range, and keyword. The value depends on the protocol.

Protocol is TCP or UDP. The acceptable values for this parameter are:

- Port range: 0 through 65535
- Port number: 80
- Keyword: Any

Protocol is ICMPv4 or ICMPv6. The acceptable values for this parameter are:

- An ICMP type, code pair: 0, 8
- Type and code: 0 through 255
- Keyword: Any

No protocol is set. The acceptable values for this parameter are:

- Any
- RPC
- RPC-EPMAP
- IPHTTPS

IPHTTPS is supported only on Windows Server 2012.

-Protocol <String>

Specifies the protocol for an IPsec rule. The cmdlet gets the IPsec rules that use the protocol that you specify for the connection. The acceptable values for this parameter are:

- Protocols by number: 0 through 255

- Protocols by name: TCP, UDP, ICMPv4, or ICMPv6.

If a port number is identified by using port1 or port2, you must specify TCP or UDP for this parameter. The values ICMPv4 and ICMPv6 create a rule that exempts ICMP network traffic from the IPsec requirements of another rule.

-RemoteAddress <String>

Specifies the remote address of the TCP connection. The cmdlet gets the IPsec rules that are matched the IP address that you specify. This parameter value is the second end point of an IPsec rule and specifies the computer that is subject to the requirements of the rules.

The acceptable values for this parameter are: an IPv4 or IPv6 address, host name, subnet, range, or the following keyword: Any. The acceptable formats for this parameter are:

- Single IPv4 Address: 1.2.3.4

- Single IPv6 Address: fe80::1

- IPv4 Subnet (by network bit count): 1.2.3.4/24
- IPv6 Subnet (by network bit count): fe80::1/48
- IPv4 Subnet (by network mask): 1.2.3.4/255.255.255.0
- IPv4 Range: 1.2.3.4 through 1.2.3.7
- IPv6 Range: fe80::1 through fe80::9

-RemotePort <UInt16>

Specifies the remote port of the TCP connection. The cmdlet gets the IPsec rules that are matched to the remote port number that you specify. This parameter value is the second end point of an IPsec rule. The acceptable values for this parameter are: a port, range, and keyword. The value depends on the protocol.

Protocol is TCP or UDP. The acceptable values for this parameter are:

- Port range: 0 through 65535
- Port number: 80
- Keyword: Any

Protocol is ICMPv4 or ICMPv6. The acceptable values for this parameter are:

- An ICMP type, code pair: 0, 8
- Type and code: 0 through 255

- Keyword: Any.

No protocol is set. The acceptable values for this parameter are:

- Any

- RPC

- RPC-EPMAP

- IPHTTPS.

IPHTTPS is supported only on Windows Server 2012.

-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 PowerShell 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: Get an IPsec rule -----

PS C:\>Find-NetIPsecRule -RemoteAddress "131.107.33.200" -Protocol "TCP"

-RemotePort 80

IPsecRuleName : {c1988b9c-9546-4eea-bf64-fbe85ddbef8c}

DisplayName : External Traffic - Attempt IPsec

Description :

DisplayGroup : Protection for Internet Traffic

Group : Protection for Internet Traffic

Enabled : True

Profile : Domain

Platform : {6.2+}

Mode : Transport

InboundSecurity : Require

OutboundSecurity : Request

QuickModeCryptoSet : Msit-Qm-EspAes128Sha1-Or-AhSha1

Phase1AuthSet : Msit-Mm-Kerb-Or-CorpCertMap

Phase2AuthSet : Msit-Em-Kerb

KeyModule : Default

AllowWatchKey : False

AllowSetKey : False

LocalTunnelEndpoint :

RemoteTunnelEndpoint :

RemoteTunnelHostname :

ForwardPathLifetime : 0

EncryptedTunnelBypass : False

RequireAuthorization : False

User :

PrimaryStatus : OK

Status : The rule was parsed successfully from the store.

(65536)

EnforcementStatus : NotApplicable

PolicyStoreSource :

PolicyStoreSourceType : GroupPolicy

This command finds the IPsec rule that the system uses for conventional web traffic to the specified IP address. The command gets the IPsec rule that matches the TCP connection that has the remote address 131.107.33.200 and that uses the remote port 80. The command returns a WMIv2 IPsec rule object.

REMARKS

To see the examples, type: "get-help Find-NetIPsecRule -examples".

For more information, type: "get-help Find-NetIPsecRule -detailed".

For technical information, type: "get-help Find-NetIPsecRule -full".

For online help, type: "get-help Find-NetIPsecRule -online"