PowerShell Get-Help on command 'New-NetIPsecQuickModeCryptoProposal'

PS C:\Users\wahid> Get-Help New-NetIPsecQuickModeCryptoProposal

NAME

New-NetIPsecQuickModeCryptoProposal

SYNOPSIS

Creates a quick mode cryptographic proposal that specifies a suite of cryptographic protocols to offer in IPsec quick mode negotiations with other computers.

SYNTAX

New-NetIPsecQuickModeCryptoProposal [-AHHash {None | MD5 | SHA1 | SHA256 | SHA384 | AESGMAC128 | AESGMAC192 | AESGMAC256}] [-ESPHash {None | MD5 | SHA1 | SHA256 | SHA384 | AESGMAC128 | AESGMAC192 | AESGMAC256}] [-Encapsulation {None | AH | ESP}] [-Encryption {None | DES | DES3 | AES128 | AES192 | AES256 | AESGCM128 | AESGCM192 | AESGCM256}] [-MaxKiloBytes <UInt64>] [-MaxMinutes <UInt64>] [<CommonParameters>]

DESCRIPTION

The New-NetIPsecQuickModeCryptoProposal cmdlet creates a single cryptographic proposal to be used in quick mode negotiations.

A NetIPsecQuickModeCryptoProposal object provides the necessary security parameters for the negotiation of a quick mode security association (SA). The IPsec protocol, either AH or ESP, is provide in the Encapsulation parameter, the hashing algorithm for data integrity and authentication in the AHHash and ESPHash parameters, and the algorithm for encryption, if requested, in the Encryption parameter.

Multiple NetIPsecQuickModeCryptoProposal fields are grouped into a single NetIPsecQuickModeCryptoSet object. The quick mode exchange will use the first proposal that the peers have in common. A NetIPsecPhase2AuthSet object and a NetIPsecMainModeCryptoSet object get associated to a NetIPsecRule object to provide all the necessary SA parameters for customized quick mode negotiations.

PARAMETERS

-AHHash <HashAlgorithm>

Specifies the proposed hash algorithm for data integrity and authentication. The acceptable values for this parameter are: None, MD5, SHA1, SHA256, AESGMAC128. AESGMAC192, or AESGMAC256. The default value is None.

-ESPHash <HashAlgorithm>

Specifies the proposed hashing algorithm for data confidentiality and authentication. The acceptable values for this parameter are: None, MD5, SHA1, SHA256, AESGMAC128. AESGMAC192, or AESGMAC256. If the Encapsulation parameter is specified as AH is used, then the acceptable values for this parameter are: AESGMAC128, AESGMAC192, AESGMAC256, MD5, SHA1, or SHA256. If the Encapsulation parameter is specified as ESP or AH,ESP, then the acceptable values for this parameter are: AESGMAC128, AESGMAC192, AESGMAC256, MD5, SHA1, or SHA256. The default value is None.

-Encapsulation <IPsecEncapsulation>

Specifies the IPsec protocol method. The acceptable values for this parameter are: None, AH, AH,ESP, or ESP. AH (authentication header) and ESP (encapsulating security payload) can both be specified or None can be specified.

- AH,ESP: Supported in all platforms.

- None: Supported in firstref_server_7 and Windows Serverr 2012.

- AH: Supported in nextref_server_7 and Windows Server 2012.

The default value is None. AH is not supported with the transport mode IKEv2 keying module.

-Encryption <EncryptionAlgorithm>

Specifies the value for a main or quick mode cryptographic proposal. The acceptable values for this parameter are: None, DES, DES3, AES128, AES192, AES256, AESGCM128, AESGCM192, or AESGCM256. GCM encryption is not supported in phase 1 authentication for nextref_server_7 and Windows Server 2012. AESGCM128, AESGCM192, and AESGCM256 are not supported for IPsec main mode security association negotiations.

-MaxKiloBytes <UInt64>

Specifies the maximum lifetime, in kilobytes, that the IKE message sender proposes for a security association to be considered valid after it has been created. The acceptable values for this parameter are: 20480 through 2147483647.

- A non-zero value specifies the desired lifetime, in kilobytes.

The default value is 100000.

-MaxMinutes <UInt64>

Specifies the number of minutes established for a quick mode security association before it expires and must be renegotiated. The acceptable values for this parameter are: 5 to 2879.

- A non-zero value specifies the desired minute lifetime.

The default value is 60 (minutes).

<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:\>$QMProposal = New-NetIPsecQuickModeCryptoProposal -Encapsulation ESP
-ESPHash SHA1 -Encryption AES128




PS C:\>$QMCryptoSet = New-NetIPsecQuickModeCryptoSet -DisplayName
"esp:sha1-des3" -Proposal $QMProposal




PS C:\>New-NetIPSecRule -DisplayName "Tunnel from HQ to Dallas Branch" -Mode
Tunnel -LocalAddress 192.168.0.0/16 -RemoteAddress 192.157.0.0/16
-LocalTunnelEndpoint 1.1.1.1 -RemoteTunnelEndpoint 2.2.2.2 -InboundSecurity
Require -OutboundSecurity Require -QuickModeCryptoSet $QMCryptoSet.Name
```

This example creates an IPsec tunnel that routes traffic from a private network (192.168.0.0/16) through an interface on the local computer (1.1.1.1) attached to a public network to a second computer through its public interface (2.2.2.2) to another private network (192.157.0.0/16). All traffic through the tunnel is integrity checked using ESP and SHA1, and encrypted using ESP and AES128.

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

This cmdlet illustrates how to include both AH and ESP protocols in a single suite.

```
PS C:\>$AHandESPQM = New-NetIPsecQuickModeCryptoProposal -Encapsulation AH,ESP
-AHHash SHA1 -ESPHash SHA1 -Encryption DES3
```

This cmdlet illustrates how to specify the use of the AH protocol only.

```
PS C:\>$AHQM = New-NetIPsecQuickModeCryptoProposal -Encapsulation AH -AHHash
SHA1 -ESPHash None -Encryption None
```

This cmdlet illustrates how to specify the use of the ESP protocol only, and uses the None keyword to specify not to include an encryption option, also known as "ESP null encryption".

```
PS C:\>$ESPQM = New-NetIPsecQuickModeCryptoProposal -Encapsulation ESP
-ESPHash SHA1 -Encryption None
```

This cmdlet illustrates how to use the None keyword to specify that ESP is used with an encryption protocol, but with no integrity protocol. This cmdlet also illustrates how to set a custom SA timeout using both time and data amount values.

```
PS C:\>$ESPnoAHQM = New-NetIPsecQuickModeCryptoProposal -Encapsulation ESP
-ESPHash None -Encryption AES256 -MaxKiloBytes 50000 -MaxMinutes 30
```

```
PS C:\>$QMCryptoSet = New-NetIPsecQuickModeCryptoSet -DisplayName "Custom
Quick Mode" -Proposal $AHandESPQM,$AHQM,$ESPQM,$ESPnoAHQM
```

```
PS C:\>New-NetIPsecRule -DisplayName "Domain Isolation Rule" -InboundSecurity
Require Request -OutboundSecurity Request -QuickModeCryptoSet $QMCryptoSet.Name
```

This example creates a domain isolation rule, but uses a custom quick mode proposal that includes multiple quick mode suites, separated by commas.

REMARKS

To see the examples, type: "get-help New-NetIPsecQuickModeCryptoProposal -examples".

For more information, type: "get-help New-NetIPsecQuickModeCryptoProposal -detailed".

For technical information, type: "get-help New-NetIPsecQuickModeCryptoProposal -full".

For online help, type: "get-help New-NetIPsecQuickModeCryptoProposal -online"