



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

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

WARNING: The names of some imported commands from the module 'Microsoft.Azure.PowerShell.Cmdlets.Network' include unapproved verbs that might make them less discoverable.

To find the commands with unapproved verbs, run the Import-Module command again with the Verbose parameter. For a list of approved verbs, type Get-Verb.

NAME

New-AzVpnClientIpsecPolicy

SYNOPSIS

This command allows the users to create the Vpn ipsec policy object specifying one or all values such as IpsecEncryption,IpsecIntegrity,IkeEncryption,IkeIntegrity,DhGroup,PfsGroup to set on the VPN gateway. This command let output object is used to set vpn ipsec policy for both new / existing gateway.

SYNTAX

```
New-AzVpnClientIpsecPolicy [-DefaultProfile
<Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>] [-DhGroup {DHGroup24
| ECP384 |
ECP256 | DHGroup14 | DHGroup2}] [-IkeEncryption {GCM AES256 | GCM AES128 | AES256 | AES128}] [-IkeIntegrity
{SHA384 | SHA256}] [-IpsecEncryption {GCM AES256 | GCM AES128
```

| AES256 | AES128}} [-IpsecIntegrity {GCMAES256 | GCMAES128 | SHA256}} [-PfsGroup {PFS24 | PFSMM | ECP384 | ECP256 | PFS14 | PFS2 | None}} [-SADataSize <System.Int32>] [-SALifeTime <System.Int32>] [<CommonParameters>]

DESCRIPTION

This command allows the users to create the Vpn ipsec policy object specifying one or all values such as IpsecEncryption,IpsecIntegrity,IkeEncryption,IkeIntegrity,DhGroup,PfsGroup to set on the VPN gateway. This command let output object is used to set vpn ipsec policy for both new / existing gateway.

PARAMETERS

-DefaultProfile <Microsoft.Azure.Commands.Common.Authentication.Abstractions.Core.IAzureContextContainer>

The credentials, account, tenant, and subscription used for communication with Azure.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DhGroup <System.String>

The VpnClient DH Groups used in IKE Phase 1 for initial SA

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-IkeEncryption <System.String>

The VpnClient IKE encryption algorithm (IKE Phase 2)

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

-IkeIntegrity <System.String>

The VpnClient IKE integrity algorithm (IKE Phase 2)

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

-IpsecEncryption <System.String>

The VpnClient IPSec encryption algorithm (IKE Phase 1)

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

-IpsecIntegrity <System.String>

The VpnClient IPSec integrity algorithm (IKE Phase 1)

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

-PfsGroup <System.String>

The VpnClient PFS Groups used in IKE Phase 2 for new child SA

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SADataSize <System.Int32>

The VpnClient IPSec Security Association (also called Quick Mode or Phase 2 SA) payload size in KB

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SALifeTime <System.Int32>

The VpnClient IPSec Security Association (also called Quick Mode or Phase 2 SA) lifetime in seconds

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

None

OUTPUTS

Microsoft.Azure.Commands.Network.Models.PSIPsecPolicy

NOTES

----- Example 1: Define vpn ipsec policy object: -----

```
$vpnclientipsecpolicy = New-AzVpnClientIpsecPolicy -IpsecEncryption AES256 -IpsecIntegrity SHA256 -SALifeTime  
86472 -SADataSize 429497 -IkeEncryption AES256  
-IkeIntegrity SHA256 -DhGroup DHGroup2 -PfsGroup None
```

This cmdlet is used to create the vpn ipsec policy object using the passed one or all parameters' values which user can pass to param:VpnClientIpsecPolicy of PS

command let: New-AzVirtualNetworkGateway (New VPN Gateway creation) / Set-AzVirtualNetworkGateway (existing VPN Gateway update) in ResourceGroup :

Example 2: Create new virtual network gateway with setting vpn custom ipsec policy:

```
$vnetGateway = New-AzVirtualNetworkGateway -ResourceGroupName vnet-gateway -name myNGW -location $location  
-IpConfigurations $vnetIpConfig -GatewayType Vpn -VpnType  
RouteBased -GatewaySku VpnGw1 -VpnClientIpsecPolicy $vpnclientipsecpolicy
```

This cmdlet returns virtual network gateway object after creation.

Example 3: Set vpn custom ipsec policy on existing virtual network gateway:

```
$vnetGateway = Set-AzVirtualNetworkGateway -VirtualNetworkGateway $gateway -VpnClientIpsecPolicy $vpnclientipsecpolicy
```

This cmdlet returns virtual network gateway object after setting vpn custom ipsec policy.

Example 4: Get virtual network gateway to see if vpn custom policy is set correctly:

```
$gateway = Get-AzVirtualNetworkGateway -ResourceGroupName vnet-gateway -name myNGW
```

This cmdlet returns virtual network gateway object.

RELATED LINKS

Online Version: <https://learn.microsoft.com/powershell/module/az.network/new-azvpnclientipsecpolicy>