<https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk101275>

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | Rate This |

[Email](mailto:?subject=Check%20Point%20SecureKnowledge%20Solution&body=Solution%20Title:%20How%20to%20setup%20Site-to-Site%20VPN%20between%20Microsoft%20Azure%20and%20an%20on%20premise%20Check%20Point%20Security%20Gateway%0D%0ASolution%20ID:%20sk101275%0D%0ASolution%20Link:%0D%0Ahttps://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails%3D%26solutionid%3Dsk101275%20%20%20%20%0D%0A-------------------------------------------------------------%20%0D%0AFor%20Disclaimer%20of%20Warranty%20and%20Copyright%20info:%20http://www.checkpoint.com/copyright.html)[Print](https://supportcenter.checkpoint.com/supportcenter/portal/media-type/html/role/supportcenterUser/page/print.psml?action=portlets.SearchResultMainAction&eventSubmit_doPrintsolution=&solutionid=sk101275)

|  |  |
| --- | --- |
| Solution ID | sk101275 |
| Technical Level |  |
| Product | IPSec VPN |
| Version | R77, R77.10, R77.20, R77.30, R80.10, R80.20, R80.30, R80.40 |
| Platform / Model | Azure |
| Date Created | 14-Jun-2014 |
| Last Modified | 23-Feb-2020 |

**Solution**

**Note:** This article deals with setting up a VPN tunnel between Microsoft Azure and an on-premises Check Point Security Gateway. If you are interested in setting up a VPN tunnel between a **Check Point Security Gateway in Azure** and an on-premises Check Point Security Gateway, then refer to [sk109360 - Check Point Reference Architecture for Azure](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk109360).

For a detailed walk through on setting up a Site-to-Site VPN, refer to [sk53980 - How to set up a Site-to-Site VPN with a 3rd-party remote gateway](http://supportcontent.checkpoint.com/solutions?id=sk53980).

When setting up the tunnel with Microsoft Azure, you will need to use the following settings. These settings are required by Microsoft Azure. For more information, refer to [About VPN Devices for Virtual Network](https://azure.microsoft.com/en-gb/documentation/articles/vpn-gateway-about-vpn-devices/).

**Notes:**

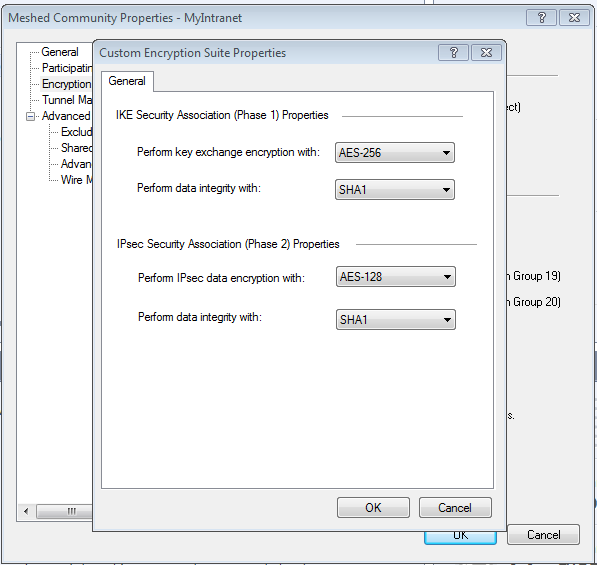
* While establishing a VPN with Microsoft Azure VPN Gateway, Check Point recommends configuring the VPN using Domain Based VPN
* Refer to <https://docs.microsoft.com/en-gb/azure/vpn-gateway/vpn-gateway-about-vpn-devices>
* For information about TCP MSS clamping, also refer to <https://docs.microsoft.com/en-gb/azure/vpn-gateway/vpn-gateway-about-vpn-devices>

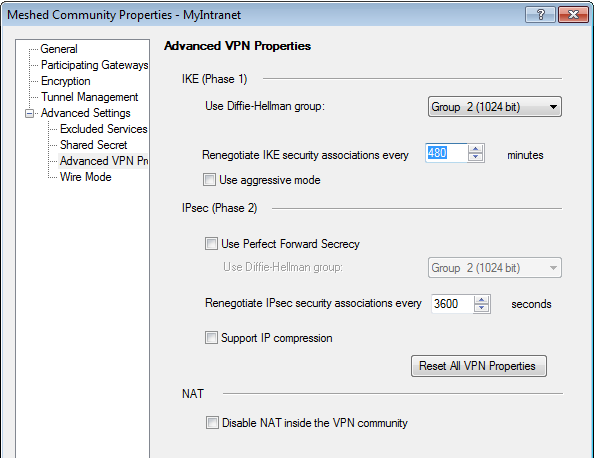
**IKE Phase 1 setup**

|  |  |  |
| --- | --- | --- |
| **Property** | **Static routing (PolicyBased) VPN gateway** | **Dynamic routing (RouteBased) VPN gateway** |
| IKE Version | IKEv1 | IKEv2 |
| Diffie-Hellman Group | Group 2 (1024 bit) | Group 2 (1024 bit) |
| Authentication Method | Pre-Shared Key | Pre-Shared Key |
| Encryption Algorithms | AES256 AES128 3DES | AES256 3DES |
| Data Integrity Algorithm  (**Important: Please note that in the current GUI HMAC-SHA1 is labeled SHA1.**) | HMAC-SHA1 | HMAC-SHA1 |
| Phase 1 Security Association (SA) Lifetime (Time) | 28,800 seconds  (480 minutes) | 28,800 seconds  (480 minutes)  Refer to [About VPN devices for Site-to-Site VPN Gateway connections](https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-about-vpn-devices) |

**IKE Phase 2 setup**

|  |  |  |
| --- | --- | --- |
| **Property** | **Static routing (PolicyBased) VPN gateway** | **Dynamic routing (RouteBased) VPN gateway** |
| IKE Version | IKEv1 | IKEv2 |
| Data Integrity Algorithm  **(Important: Please note that in the current GUI HMAC-SHA1 is labeled SHA1.)** | HMAC-SHA1 | HMAC-SHA1 |
| Phase 2 Security Association (SA) Lifetime (Time) | 3,600 seconds  (60 minutes) | 27,000 seconds  (450 minutes) |
| IPsec SA Encryption & Authentication Offers (in the order of preference) | ESP-AES256 ESP-AES128 ESP-3DES N/A | Refer to [Dynamic Routing Gateway IPsec Security Association (SA) Offers](https://azure.microsoft.com/en-gb/documentation/articles/vpn-gateway-about-vpn-devices/) |
| Perfect Forward Secrecy (PFS) | No | No |
| Dead Peer Detection | Not supported | Supported |





**Notes:**

* To configure Phase II properties for IKEv1 and IKEv2 in Check Point SmartDashboard: go to *IPSec VPN* tab - double-click on the relevant VPN Community - go to the *Encryption* page - in the section *Encryption Suite*, select *Custom* - click on *Custom Encryption...* button - configure the relevant properties - click on *OK* to apply the settings - install the policy.
* When setting up a Site-to-Site VPN with Azure, you will need to see if Azure is offering subnet-to-subnet or gateway-to-gateway VPN:
  + If Azure is using ***subnet-to-subnet***, then Check Point side must be configured in the following way in Check Point SmartDashboard: go to *IPSec VPN* tab - double-click on the relevant VPN Community - go to the *Tunnel Management* page - in the section *VPN Tunnel Sharing*, select ***One VPN tunnel per subnet pair*** - click on *OK* to apply the settings - install the policy.
  + If Azure is using ***gateway-to-gateway***, then Check Point side must be configured in the following way in Check Point SmartDashboard: go to *IPSec VPN* tab - double-click on the relevant VPN Community - go to the 'Tunnel Management' page - in the section *VPN Tunnel Sharing*, select ***One VPN tunnel per Gateway pair*** - click on *OK* to apply the settings - install the policy.
  + The ***subnet-to-subnet*** is what Azure calls "policy-based VPN" and ***gateway-to-gateway*** is what Azure calls "route-based VPN". This should help customers identify what they have on Azure against what they need to configure on the Check Point device.
  + Also, when using ***subnet-to-subnet,*** users can define one or more address prefixes to use in their virtual network, and then carve out multiple subnets within each prefix. Azure VPN in policy-based configuration will use the prefix pairs for the Traffic Selectors for the SA negotiation, not subnet ranges.
* Make sure the Networks in the respective encryption domains correspond to the settings configured at the Azure side (you may use the setting ***subnet\_for\_range\_and\_peer*** to make sure the subnets are negotiated as required - for details, refer to "*Scenario 1*" in [sk108600 - VPN Site-to-Site with 3rd party](https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108600#Scenario%201)).