**Configuring the Palo Alto Networks Firewall**

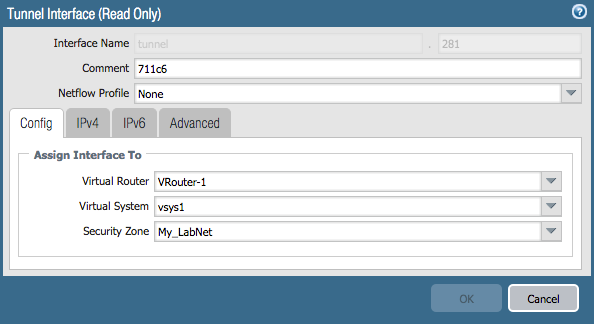
**Here' is a bit by bit guide on the most proficient method to set up the VPN for a Palo Alto Networks firewall.**

For this example, the following topology was used to connect a PA-200 running PAN-OS 7.1.4 to a MS Azure VPN Gateway.

For the PAN-OS IKEv2 Crypto Profile, you must select a combination of Microsoft Azure supported crypto parameters as stated in Microsoft’s IPSec Parameters (see first reference link above). Our example used the following IKE, IPSec, and crypto profile parameters.

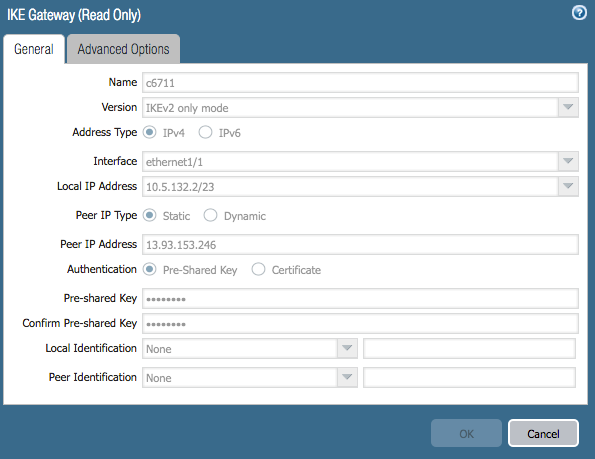
**Note:** Public IP addresses were changed for the purpose of this example.

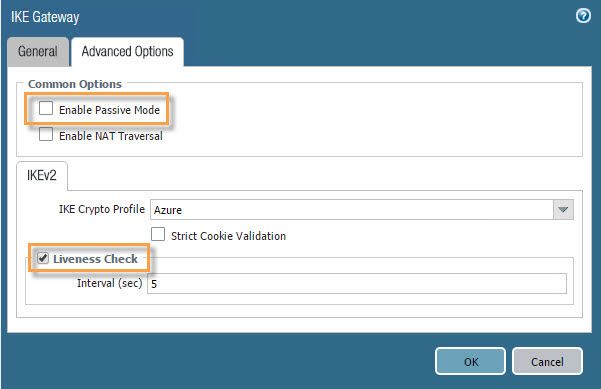
### ****Tunnel Interface****

1. Inside the WebGUI in **Network > Interfaces > Tunnel**, Add a new tunnel interface.  Select a virtual router and appropriate security zone.
2. **Optional**: Assign an IP on same subnet as the Azure Gateway for dynamic routing and/or tunnel monitoring inside the IPv4 tab.  
   

Tunnel Interface window

### ****IKE Gateway****

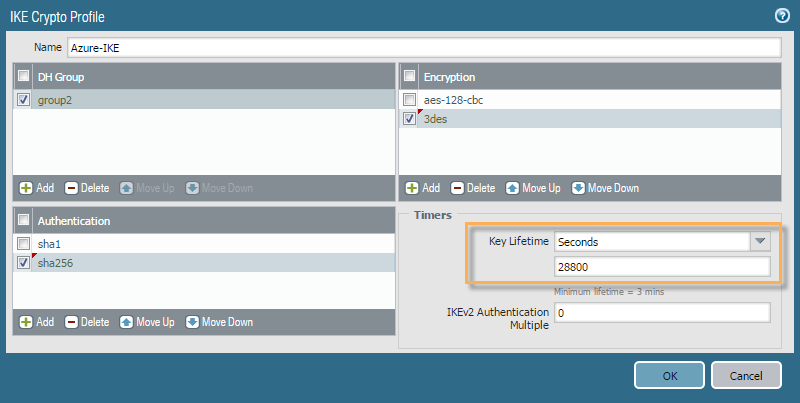
1. Add an IKE Gateway (**Network > Network Profiles >IKE Gateway**). The following values are to be configured:
   1. Version: Set to ‘**IKEv2 Only mode**’ OR ‘**IKEv2 preferred mode**’  
       IKE Gateway window
   2. **Interface**: Set to the public(internet) facing interface of the firewall used to connect to Azure.
   3. **Local IP Address**: IP address of the external interface of the firewall. If not behind a NAT device, this will be the VPN Gateway Address as configured in Azure.
   4. **Peer IP Address**: IP address of the Azure VPN Gateway. This can be obtained from the Azure Virtual Network dashboard. **Note**: Make sure you use the NAT-ed IP on Azure to define the peer IP.
   5. **Pre-shared Key**: Azure uses a **Pre-shared key**(PSK or Pre-Shared Secret) for authentication. The Key should be configured as the same value on Azure VPN settings and Palo Alto Networks’ firewall.  
      (**Note:** See links above for Azure configuration information)
   6. On the **Advanced Options** tab, leave the **Enable Passive Mode** (Set as responder) unchecked, and in the IKEv2 section leave **Liveness Check** enabled.

**Note**: Enable NAT traversal if the firewall is behind a NAT device.  
IKE Gateway window - advanced options

* 1. ‘**IKE Crypto Profile**’ is set to default. A new crypto profile can be defined to match the IKE crypto settings of Azure VPN.  
     **DH Group**: group2

**Encryption**: aes-256-cbc, 3des

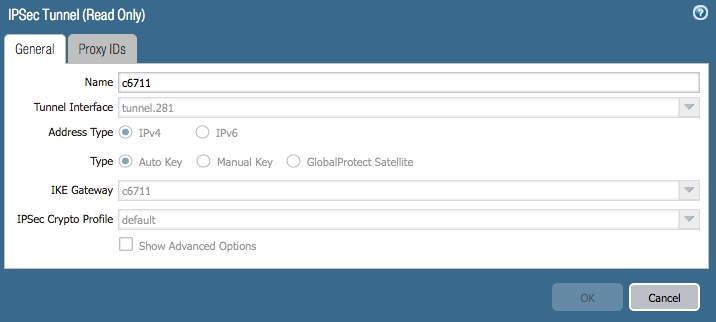
**Authentication**: sha1, sha256

**Note:**Set lifespans longer than Azure settings to ensure that Azure renews the keys during re-keying. Set phase 1 lifetime to 28800 seconds.  


PAN-OS IKEv2 Crypto Profile window.

**IPSec Tunnel**

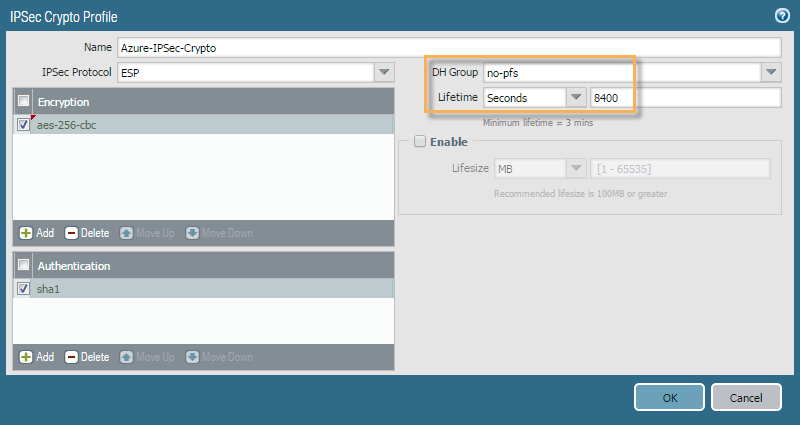
##### Add a new IPSec tunnel (**Network**->**IPSec Tunnels**). The following values are to be configured:

1. Tunnel Interface: Select the configured Tunnel Interface in Step 1. above.  
   **(Optional**: Use the ‘Show Advanced Options’ to configure tunnel monitoring, if desired.)  
   IPSec Tunnel window
2. IKE Gateway: Select the IKE Gateway configured in Step 2. above.
3. IPSec Crypto Profile:(**Network** > **Network Profiles** > **IPSec Crypto**) Select an ‘**IPSec Crypto Profile**’. This can be default if it matches the Azure settings, otherwise create a new one with **Add** at the bottom of the IPSec Crypto window.

**Encryption**: aes256-cbc

**Authentication**: sha1

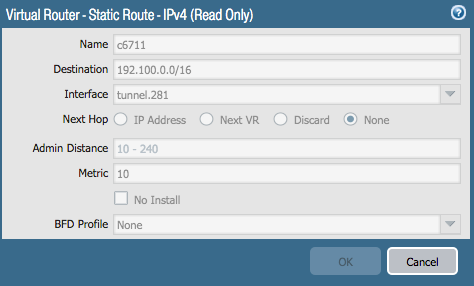
**DH Group**: no-pfs

**Note**: Set lifespans longer than Azure settings to ensure that Azure renews the keys during re-keying. Set IPSec (phase 2) lifetime to 8400 seconds  
 IPSec Crypto Profile window

##### **Network Reachability**

In ‘route based VPNs’, the routing engine of the device(s) is used to determine reachability even for any VPN networks.

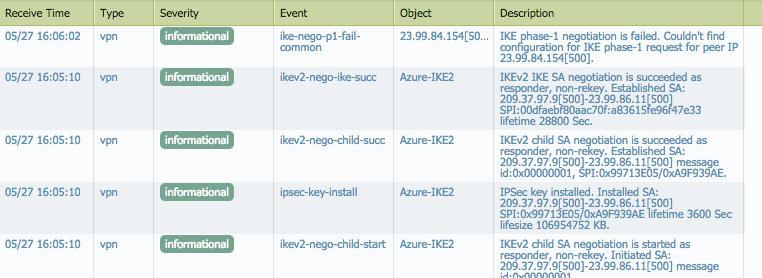
1. Use the ‘Virtual Router’ settings (Network->Virtual Router-><VR Name>) to add a Static Route for the remote network with the Interface set to being the Tunnel Interface configured in Step 1. This should match the local network settings on Azure.



Virtual Router window - Static Route - IPv4

##### **IPSec Tunnel Configuration**

You can optionally configure “Tunnel Monitor” to ping an IP address on the Microsoft Azure side.  You will also need to configure the necessary Proxy IDs (IP address ranges) for the local and remote networks using the Proxy ID tab.  This is how route-based VPNs are configured for “dynamic routing” in the Microsoft Azure environment.



##### **Checking the Connection**

On the PAN-OS firewall under the IPSec Tunnels menu option, check the UI to ensure that the tunnel you created is up and running. The status columns for the IKE Gateway and the Tunnel Interface should be green if IKEv2 negotiated correctly and the IPSec Phase 2 tunnel was brought up.

Bottom of Form