**Skillet for PAN-OS**



**Azure Virtual Network Gateway**

**IKE/IPSec and BGP configuration for PAN-OS**

<https://github.com/cestebanez91/Azure-VNG-PANOS>

Table of Contents

[1. Presentation of the Skillet 3](#_Toc10198339)

[2. Diagram 4](#_Toc10198340)

[3. Run Skillet 5](#_Toc10198341)

1. **Presentation of the Skillet**

This skillet will configure IKE/IPSec parameters and BGP in order to connect PAN-OS to Microsoft Azure VNG (Virtual Network Gateway).

This skillet will be used to connect your Palo Alto Network device (physical or VM-series) to any Microsoft Azure Virtual Network Gateway to establish an IPSec connection.

Based on parameters given by Azure (VNG public IP address, BGP peer and gateway subnet).

It will create a new IKE gateway and a new Ipsec tunnel, whatever this is already existing, iteration is possible up to four IKE gateways and four IPSec tunnels.

IKE and IPSec profile are compliant to Azure VNG expectations.

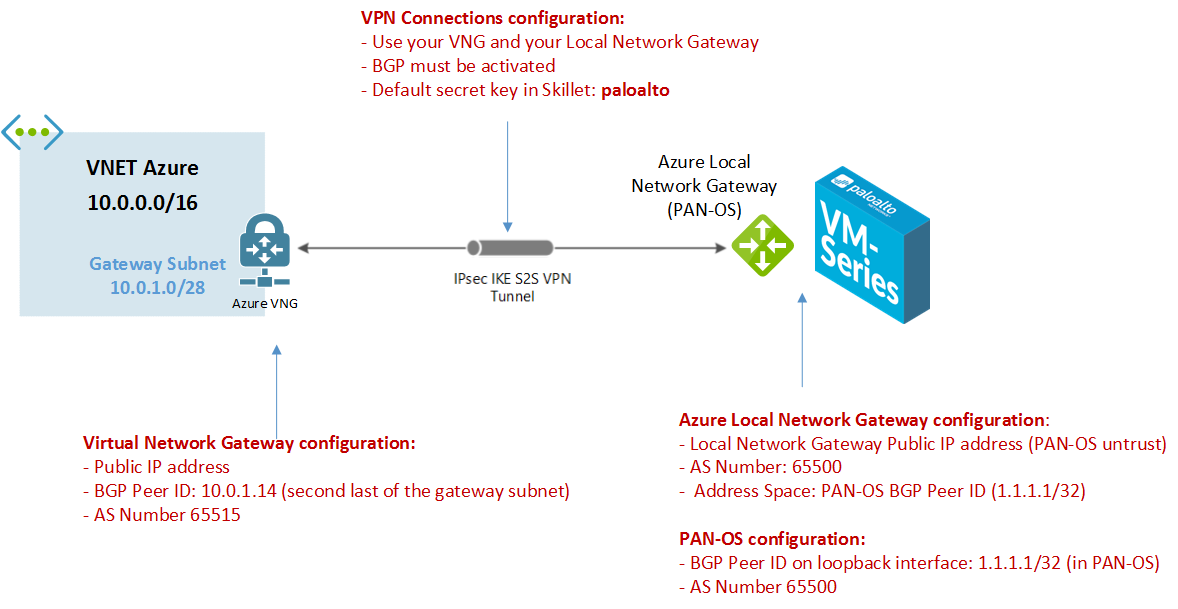
**This skillet will configure PAN-OS with following features:**

* IKE crypto profile compliant with Azure VNG
* IPSec crypto profile compliant with Azure VNG
* IKE gateway to connect to Azure VNG
* IPSec tunnel
* Tunnel interface, loopback interface for BGP and Zone
* Routing and BGP configuration with distribution profile activated

**Content is the following:**

* ikecrypto.xml will configure IKE crypto profile
* ipseccrypto.xml will configure IPSec crypto profile
* ikeprofile.xml will configure IKE gateway with iteration
* ipsecprofile.xml will configure IPSec tunnel with iteration
* interface.xml will configure tunnel and loopback interfaces
* zone.xml will configure zones
* routing.xml will configure BGP parameters to exchange routes

1. **Diagram**



To establish an IPSec connection to your Azure Vnet, you will need to configure:

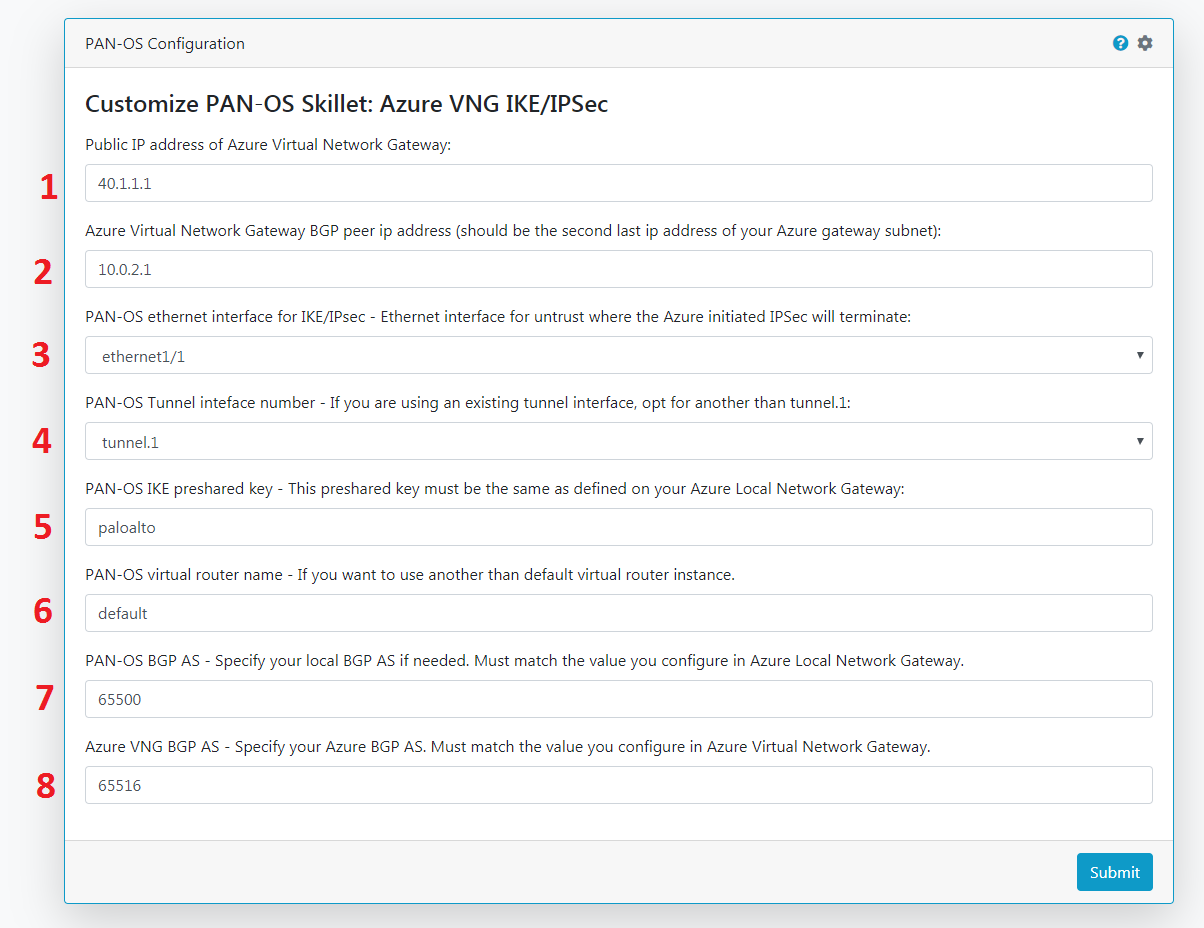
* **Azure Virtual Network Gateway (VNG)**
* **Azure Local Network Gateway (your on prem device running PAN-OS)**
* **Azure VPN connection (to bind VNG and LNG)**
* **PAN-OS device**

Once you deployed 4 components, you should get:

* **Azure VNG public IP address**
* **Azure VNET gateway subnet CIDR**
* **Azure VNG BGP Peer ID (second last IP address of your gateway subnet CIDR)**
* **Azure VNG BGP AS Number**
* **PAN-OS public IP address with default route to Internet**

1. **Run Skillet**

When you run exectue the skillet, you need to define these values:



1: This is the Public IP Address given by Azure when you create your Virtual Network Gateway.

2: This is the BGP Peer IP address given by Azure.

3: Choose from ethernet1/1 to ethernet1/4 on which interface you will connect your IPSec tunnel for untrust side.

4: Choose from tunnel.1 to tunnel.4 to create the new tunnel if tunnels are already existing.

5: This is the preshared ky used to authenticate the IKE, must match the one defined in your Azure VNG configuration (by default: paloalto).

6: Type in the name of your PAN-OS virtual router instance to be configured (by default: default).

7: Local BGP AS Number for PAN-OS, by default 65500. This skillet will not update your Azure configuration if different.

8: Azure Virtual Network Gateway BGP AS Number, given by Azure.