Skillet for PAN-OS

AWS Virtual Private Gateway

IKE/IPSec and BGP configuration for PAN-OS

https://github.com/cestebanez91/AWS-VGW-PANOS

Last Update: May 2019

Table of Contents

1. Presentation of the Skillet

This skillet will configure IKE/IPSec parameters and BGP in order to connect PAN-OS to AWS Virtual Private Gateway (VGW).

This skillet will be used to connect your Palo Alto Network device (physical or VM-series) to any AWS IPSec Gateway to establish a secure VPN connection.

By default, AWS propose two IPSec tunnel for each configured connection, this skillet will configure both tunnels.

Based on parameters given by AWS configuration file.

It will create two new IKE gateways and two new Ipsec tunnels, whatever these are already existing, iteration is possible up to four IKE gateways and four IPSec tunnels.

IKE and IPSec profile are compliant to AWS crypto profiles expectations.

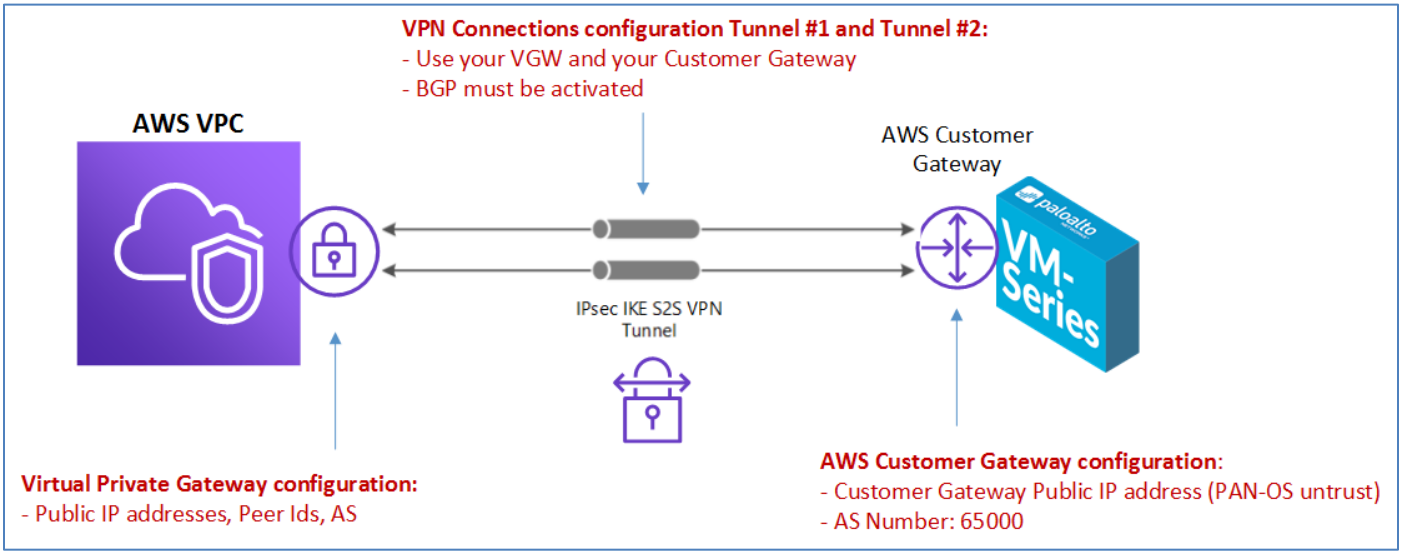
This skillet will configure PAN-OS with following features:

- IKE crypto profile compliant with AWS VGW
- IPSec crypto profile compliant with AWS VGW
- IKE gateway to connect to AWS gateway IP 1
- IKE gateway to connect to AWS gateway IP 2
- IPSec tunnel 1 and 2
- Tunnel interfaces, and Zone “VPN »
- Routing and BGP configuration with distribution profile activated for connected routes

Content is the following:

- ikecrypto.xml will configure IKE crypto profile
- ipseccrypto.xml will configure IPSec crypto profile
- ikeprofile.xml will configure IKE gateways with iteration
- ipsecprofile.xml will configure IPSec tunnels with iteration
- interface.xml will configure tunnels
- zone.xml will configure zones
- routing.xml will configure BGP parameters to exchange routes

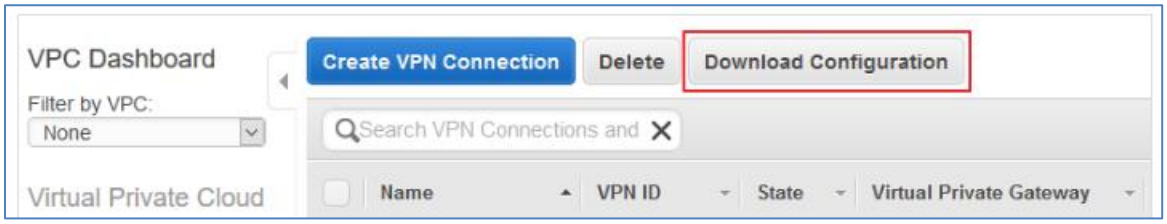
2. Diagram



To establish an IPSec connection to your AWS VGW, you will need to configure as a prerequisite:

- **AWS Virtual Private Gateway deployed and attached to a VPC**
- **AWS Customer Gateway configured (your on prem device running PAN-OS)**
- **AWS VPN Site-to-Site connection setup (to bind VGW and CGW)**
- **PAN-OS device 7.1 min**

Once you deployed 4 components, you will be able to download a configuration file, dedicated for PAN-OS devices:



This file contains all the important information to build the VPN connection.

You just need to fill the correct fields in your skillet and everything is configured.

This file is divided in two sections, one for each tunnel configuration:

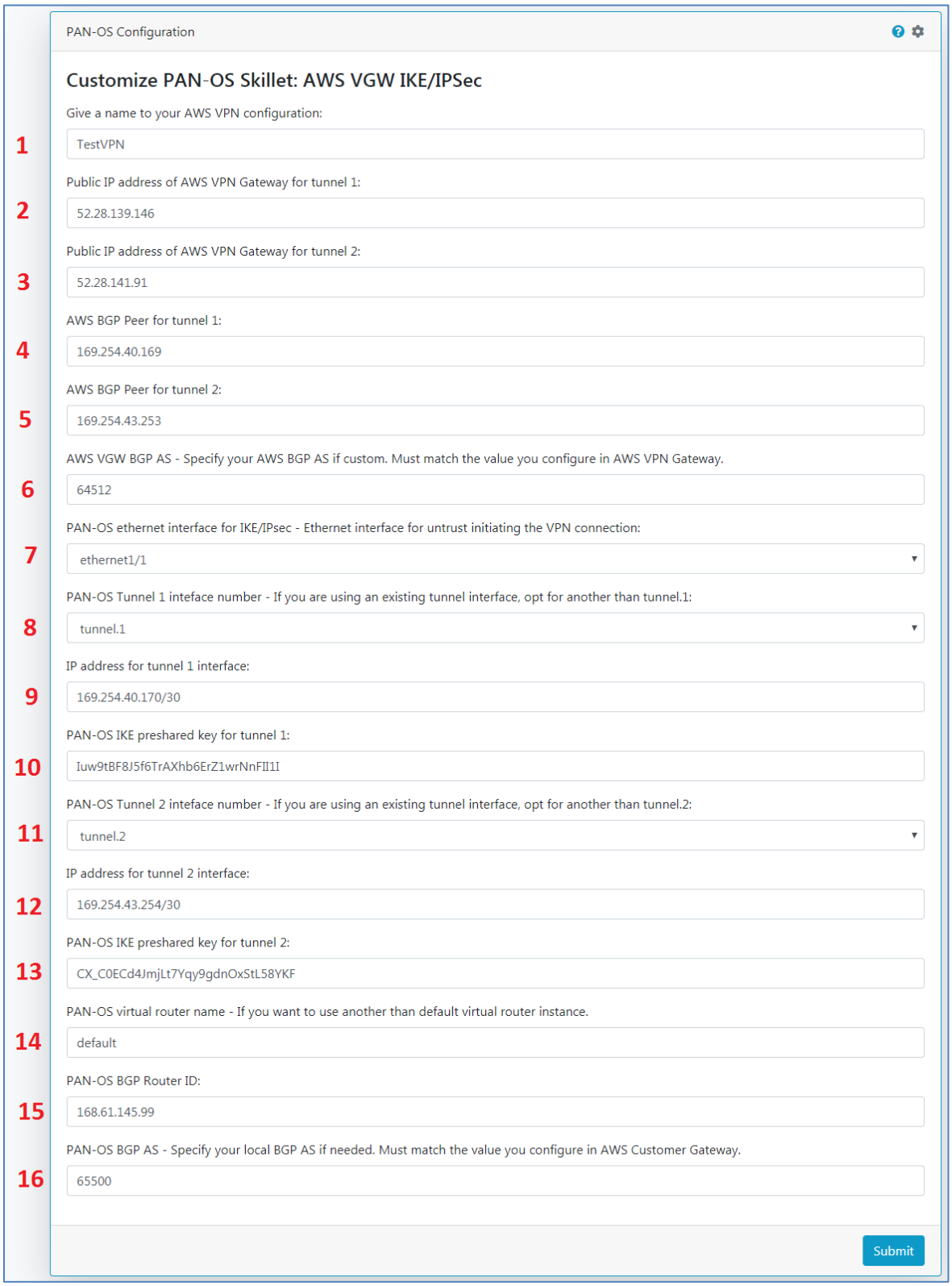
- IPSec Tunnel #1
- IPSec Tunnel #2

For each tunnel configuration, there are 4 sub sections:

- #1 IKE Configuration
- #2 IPSec Configuration
- #3 Tunnel Interface Configuration
- #4 BGP Configuration

3. Run Skillet

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



1: Give a name to your VPN connection, this name will prename all IKE and IPSec parameters to distinguish this VPN connection.

2: This is the AWS VPN gateway first Public IP address, this value can be found in section:

- IPSec Tunnel #1
  - #1 IKE configuration
    - set peer-address ip 52.28.139.146

3: This is the AWS VPN gateway second Public IP address, this value can be found in section:

- IPSec Tunnel #2
  - #1 IKE configuration
    - set peer-address ip 52.28.141.91

4: You need to define the AWS BGP Peer for tunnel 1, this value can be found in section:

- IPSec Tunnel #1
  - #4 BGP configuration
    - set peer-address ip 169.254.40.169

5: You need to define the AWS BGP Peer for tunnel 1, this value can be found in section:

- IPSec Tunnel #2
  - #4 BGP configuration
    - set peer-address ip 169.254.43.253

6: Fill with the AWS BGP AS number you defined in AWS console or CLI, if custom, this value can be found in section (same AS number for both tunnel configurations):

- IPSec Tunnel #1 (and #2)
  - #4 BGP configuration
    - set peer-as 64512

7: Choose from ethernet1/1 to ethernet1/4 on which PAN-OS interface your IKE gateway will terminate (commonly untrust interface is ethernet1/1)

8: For Tunnel #1, choose from tunnel.1 to tunnel.4 to create the new PAN-OS tunnel interface if tunnels are already existing.

9: Give an IP address to your Tunnel #1 tunnel interface, this value can be found in section:

- IPSec Tunnel #1
  - #3 Tunnel Interface Configuration
    - set ip 169.254.40.170/30

10: Preshared key for Tunnel #1 IKE gateway, can be found in section:

- IPSec Tunnel #1
  - #1 IKE configuration
    - Set authentication pre-shared-key key Iuw9tBF8J5f6TrAXhb6ErZ1wrNnFII1I

11: For Tunnel #2, choose from tunnel.2 to tunnel.5 to create the new PAN-OS tunnel interface if tunnels are already existing.

12: Give an IP address to your Tunnel #2 tunnel interface, this value can be found in section:

- IPSec Tunnel #2
  - #3 Tunnel Interface Configuration
    - set ip 169.254.43.254/30

13: Preshared key for Tunnel #2 IKE gateway, can be found in section:

- IPSec Tunnel #2
  - #1 IKE configuration
    - Set authentication pre-shared-key key CX_C0ECd4JmjLt7Yqy9gdnOxStL58YKF

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

15: Fill with the PAN-OS BGP Peer ID, this value is unique for both tunnels, this can be found in section:

- IPSec Tunnel #1 (or #2)
  - #4 BGP Configuration
    - set router-id 168.61.145.99

16: Local BGP AS Number for PAN-OS, by default 65000. This skillet will not update your AWS Customer Gateway configuration if different.

4. Configuration file from AWS

You will find in the below copy of configuration file all important parameters you need, this is example for Tunnel #1.

```
This ! Amazon Web Services
! Virtual Private Cloud

! AWS utilizes unique identifiers to manipulate the configuration of
! a VPN Connection. Each VPN Connection is assigned an identifier and is
! associated with two other identifiers, namely the
! Customer Gateway Identifier and Virtual Private Gateway Identifier.
!
! Your VPN Connection ID           : vpn-08d6b84c2dba31d8b
! Your Virtual Private Gateway ID         : vgw-099e4f96ffa5be0dc
! Your Customer Gateway ID         : cgw-07b8fdf8f26de19c4
!
!
! This configuration consists of two tunnels. Both tunnels must be
! configured on your Customer Gateway.
!
! ------------------------------------------------------------------------
! IPSec Tunnel #1
! ------------------------------------------------------------------------
! #1: Internet Key Exchange (IKE) Configuration
!
! A policy is established for the supported ISAKMP encryption,
! authentication, Diffie-Hellman, lifetime, and key parameters.
! Please note, these sample configurations are for the minimum requirement of AES128, SHA1, and
DH Group 2.
! Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2,
and DH Group 14.
! You will need to modify these sample configuration files to take advantage of AES256, SHA256,
or other DH groups like 2, 14-18, 22, 23, and 24.
! Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
! The address of the external interface for your customer gateway must be a static address.
! Your customer gateway may reside behind a device performing network address translation (NAT).
! To ensure that NAT traversal (NAT-T) can function, you must adjust your firewall !rules to
unblock UDP port 4500. If not behind NAT, we recommend disabling NAT-T.

!

 configure
 edit network ike crypto-profiles ike-crypto-profiles vpn-08d6b84c2dba31d8b-0
  set dh-group group2
  set hash sha1
  set lifetime seconds  28800
  set encryption aes-128-cbc
  top

! With local-address IP please append the configured subnet mask (i.e, /30) on the VPN
initiating interface (i.e., ethernet 1/1)
! For example if you have /30 as subnet mask the local-address ip should be 168.61.145.99/30

 edit network ike gateway ike-vpn-08d6b84c2dba31d8b-0
  set protocol ikev1 ike-crypto-profile vpn-08d6b84c2dba31d8b-0 exchange-mode main
  set protocol ikev1 dpd interval 10 retry 3 enable yes
  set authentication pre-shared-key key Iuw9tBF8J5f6TrAXhb6ErZ1wrNnFII1I
  set local-address ip 168.61.145.99
  set local-address interface ethernet1/1
  set peer-address ip 52.28.139.146
```

```
 top


! #2: IPSec Configuration
!
! The IPSec transform set defines the encryption, authentication, and IPSec
! mode parameters.
!
! Category "VPN" connections in the GovCloud region have a minimum requirement of AES128, SHA2,
and DH Group 14.
! Please note, you may use these additionally supported IPSec parameters for encryption like
AES256 and other DH groups like 2, 5, 14-18, 22, 23, and 24.
! Higher parameters are only available for VPNs of category "VPN," and not for "VPN-Classic".
!
 edit network ike crypto-profiles ipsec-crypto-profiles ipsec-vpn-08d6b84c2dba31d8b-0
  set esp authentication sha1
  set esp encryption aes-128-cbc
  set dh-group group2 lifetime seconds 3600
 top



! ------------------------------------------------------------------------------
! #3: Tunnel Interface Configuration
!
! A tunnel interface is configured to be the logical interface associated
! with the tunnel. All traffic routed to the tunnel interface will be
! encrypted and transmitted to the VPC. Similarly, traffic from the VPC
! will be logically received on this interface.
!
! Association with the IPSec security association is done through the
! "tunnel protection" command.
!
! The address of the interface is configured with the setup for your
! Customer Gateway.  If the address changes, the Customer Gateway and VPN
! Connection must be recreated with Amazon VPC.
!


 edit network interface tunnel units tunnel.1
  set ip 169.254.40.170/30
  set mtu 1427
 top

!
! Tunnel interface needs to be associated to Zone, we are using untrust zone as an example,
please adjust according
!

set zone untrust network layer3 tunnel.1

!
! Tunnel interface needs to be associated to a virtual router, we are using default as an
example, please adjust accordingly
!

set network virtual-router default interface tunnel.1

 edit network tunnel ipsec ipsec-tunnel-1
  set auto-key ipsec-crypto-profile ipsec-vpn-08d6b84c2dba31d8b-0
  set auto-key ike-gateway ike-vpn-08d6b84c2dba31d8b-0
  set tunnel-interface tunnel.1
  set anti-replay yes
```

```
 top

! ------------------------------------------------------------------------------

! #4: Border Gateway Protocol (BGP) Configuration
!
! BGP is used within the tunnel to exchange prefixes between the
! Virtual Private Gateway and your Customer Gateway. The Virtual Private Gateway
! will announce the prefix corresponding to your VPC.
!
!
!
! The local BGP Autonomous System Number (ASN) (65000)
! is configured as part of your Customer Gateway. If the ASN must
! be changed, the Customer Gateway and VPN Connection will need to be recreated with AWS.
!


 edit network virtual-router default protocol bgp
  set router-id 168.61.145.99
  set install-route yes
  set enable yes
  set local-as 65000
   edit peer-group AmazonBGP
    edit peer amazon-vpn-08d6b84c2dba31d8b-0
     set peer-as 64512
     set connection-options keep-alive-interval 10
     set connection-options hold-time 30
     set enable yes
     set local-address ip 169.254.40.170/30
     set local-address interface tunnel.1
     set peer-address ip 169.254.40.169
     top
```