Palo Alto Networks Virtual Private Network Automation with Microsoft Azure Virtual WAN

Author: Vinay Venkataraghavan

Change Log:

Date	Description	Author(s)
9/4/2018	V1.0: First version describing the automation framework and usage guidelines.	Vinay Venkataraghavan

Overview

Enterprises leveraging public clouds are increasingly find the need to connect branch and remote sites to virtual networks in the cloud. Currently the only way to connect the branch to the cloud is by the creation of VPN tunnels between the two ends.

This document describes the process of automating the creation of VPN tunnels between Palo Alto Networks VM-Series platform devices and peer VPN devices (most likely residing in a public cloud environment).

Important:
This document is restricted to describing the configuration of the Palo Alto Networks firewall portion of the VPN configuration. (There will be another document that describes the automation tool for the creation of various resources on the Microsoft Azure side of the VPN connection).

Theory of Operation

Concepts

The most important concept to note in using the VPN automation tool is that it is input driven. A user need only provide the various configuration parameters in a JSON file and the tool takes care of all aspects of the configuration and interaction with the Palo Alto Networks firewall device.

Components

The Palo Alto Networks VPN automation tools consists of two components:

- Python program

  The python program that performs all aspects of interacting with Palo Alto devices to create the entities required to create a VPN connection with a peer VPN device.

- Configuration files

  The configuration files define the parameters which will be consumed by the program to create the entities and objects

  Specifically, there are two configuration files:

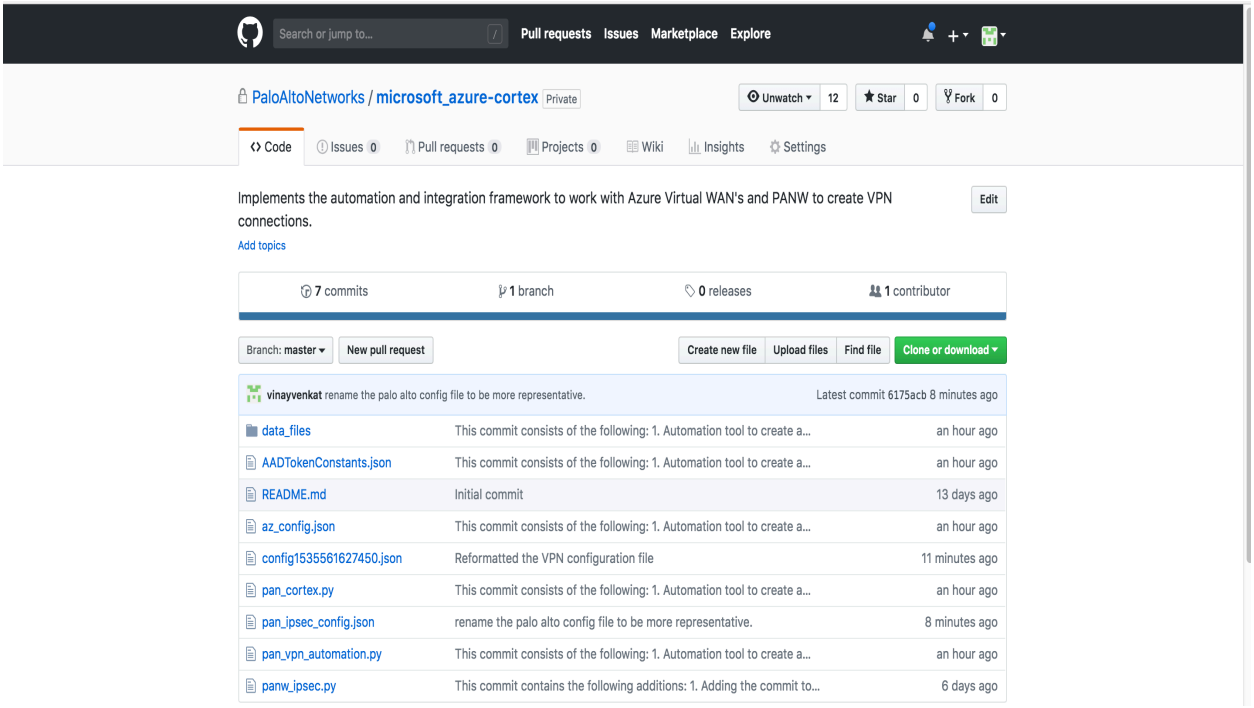
- A configuration file to define the various IKE, IPSec, IKE Gateway and IPSec tunnel configurations.
- The VPN configuration file downloaded from Microsoft Azure, defining the various VPN properties.

Implementation / Code Artifacts, Usage and Guidelines

Code Repository

The code for the Palo Alto VPN Automation Framework can be found at:

https://github.com/PaloAltoNetworks/microsoft_azure-cortex



Code Elements

The main components of the tool are:

```panw_ipsec.py```:

This file implements the functionality required to interact with the Palo Alto Networks firewall devices to create VPN tunnels.

```<ipsec configuration file>```:

This file contains all the parameters required for the creation of the IKE profile, IPSec profile, IKE gateway and the IPSec tunnel.

Note: The example file provided in the repo is called ```pan_ipsec_config.json```

```<cloud vpn configuration file>```:

This file is typically downloaded from Microsoft Azure. It contains all the required properties and parameters required for a remote VPN device to establish a VPN connection with the Azure Virtual WAN.

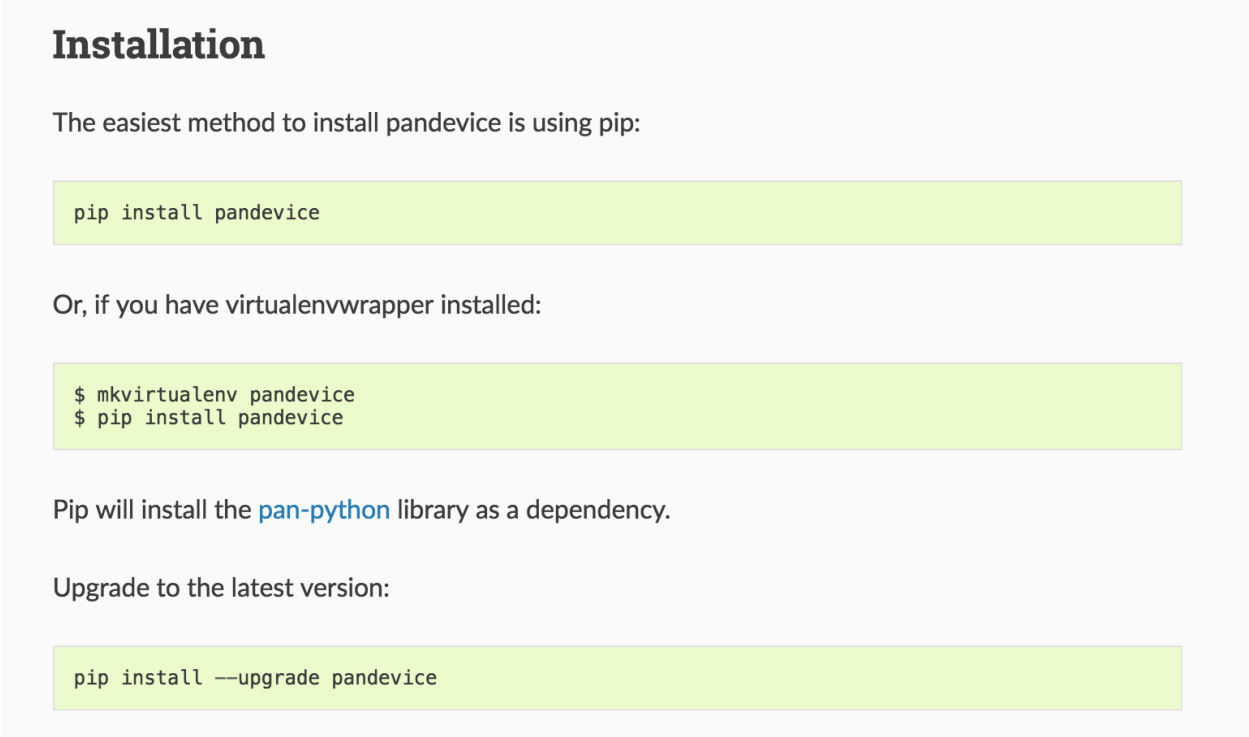
Note: The example file provided in the repository is called ```config1535561627450.json```

Pre-requisites / Assumptions

1. A system which supports the execution of python.
2. Python2.7 is installed on the system.
3. The execution of the ```panw_ipsec.py``` program requires the installation of the following dependencies:

   ```**pandevice**``` python package.

   This package can be installed as follows:
   ```



Installation

The easiest method to install pandevice is using pip:

```
pip install pandevice
```

Or, if you have virtualenvwrapper installed:

```
$ mkvirtualenv pandevice
$ pip install pandevice
```

Pip will install the pan-python library as a dependency.

Upgrade to the latest version:

```
pip install --upgrade pandevice
```

Palo Alto Networks Firewall Pre-requisites:

- The user is expected to have pre-created the tunnel interface on the firewall device prior to its usage in the creation of the VPN configuration.

Usage

cmd_prompt > python panw_ipsec.py <ipsec configuration file> <cloud vpn configuration file> <Remote Site Name>

Note: <Remote Site Name> will be specified in the “Cloud VPN Configuration” file. This is the value that will need to input into the python program.

Example:

cmd_prompt > python panw_ipsec.py pan_ipsec_config.json config1535561627450.json AutomationVpnSite1

Note: The value “AutomationVpnSite1” is extracted from the “Cloud VPN Configuration” file. Please see the “Cloud VPN Configuration File” section below for more details.

Configuration File Description

IPSec Configuration File:

This file provides all the parameters which will be used by the Palo Alto Networks firewall device in order to create one end of the VPN connection. The contents of this file is shown below:

```
{
    "creds": {
        "fw_ip": "",
        "username": "",
        "password": ""
    },
    "ike_profile": {
        "name": "",
        "dh_group": "group2",
        "authentication": ["sha1"],
        "encryption": ["aes-256-cbc", "3des"],
        "lifetime_secs": ""
    },
    "ipsec_profile": {
        "name": "",
        "encryption": ["aes-128-cbc", "3des"],
        "authentication": ["sha1"],
        "dh_group": "no-pfs",
        "lifetime_hrs": "1"
    },
    "ike_gw": {
        "name": "ike_gw2",
        "protocol_version": "ikev2",
        "interface": "ethernet1/1",
        "auth_type": "pre-shared-key",
        "enable_passive_mode": true,
        "liveness_check": "5"
    },
    "ipsec_tunnel": {
        "name": "",
        "tunnel_interface": "tunnel.2",
        "key_type": "auto-key"
    }
}
```

The file shown above has the following configuration elements / sections:

“creds”:

This section provides the credentials to interact with the Palo Alto Networks firewall device.

“ike_profile”:

This section specifies the parameters required for the creation of the IKE profile. This includes specification of the protocols used for authentication, encryption etc.

“ipsec_profile”:

This section provides specifies the parameters required for the creation of the IPSec profile. This includes the specification of the protocols used for authentication, encryption etc.

“ike_gw”:

This section specifies the parameters required for the creation of the IKE gateway. The specification includes the authentication type, the interface to be used, the IKE protocol version etc.

“ipsec_tunnel”:

This section specifies the parameters required for the creation of the IPSec tunnel. It includes the tunnel interface to be used.

IMPORTANT: Please see section above “Palo Alto Network Firewall Pre-requisites”

Cloud VPN Configuration File:

This file is typically downloaded from Microsoft Azure upon completion of all the steps required to create and configure the Azure Virtual WAN.

The contents of the file are shown below:


```
[
  {
    "configurationVersion": {
      "LastUpdatedTime": "2018-08-29T16:54:02.3415379Z",
      "Version": "dd9c2ec8-fb96-4614-b907-6e260b5e79df"
    },
    "vpnSiteConfiguration": {
      "Name": "AutomationVpnSite1",
      "IPAddress": ""
    },
    "vpnSiteConnections": [
      {
        "hubConfiguration": {
          "AddressSpace": "10.7.0.0/16",
          "Region": "West US"
        },
        "gatewayConfiguration": {
          "IpAddresses": {
            "Instance0": "",
```

```
            "Instance1": ""
          }
        },
        "connectionConfiguration": {
          "IsBgpEnabled": false,
          "PSK": "msU",
          "IPsecParameters": {
            "SADataSizeInKilobytes": 102400000,
            "SALifeTimeInSeconds": 3600
          }
        }
      }
    ]
  }
]
```

Note: The most important section from a user perspective is the name of the site that needs to be configured. This entity is specified in the “vpnSiteConfiguration” section. The value specified here will be passed in as the third argument to the python program.