How to setup Site-to-Site VPN between Microsoft Azure and an on premise Hillstone Networks Security Gateway

I. Background

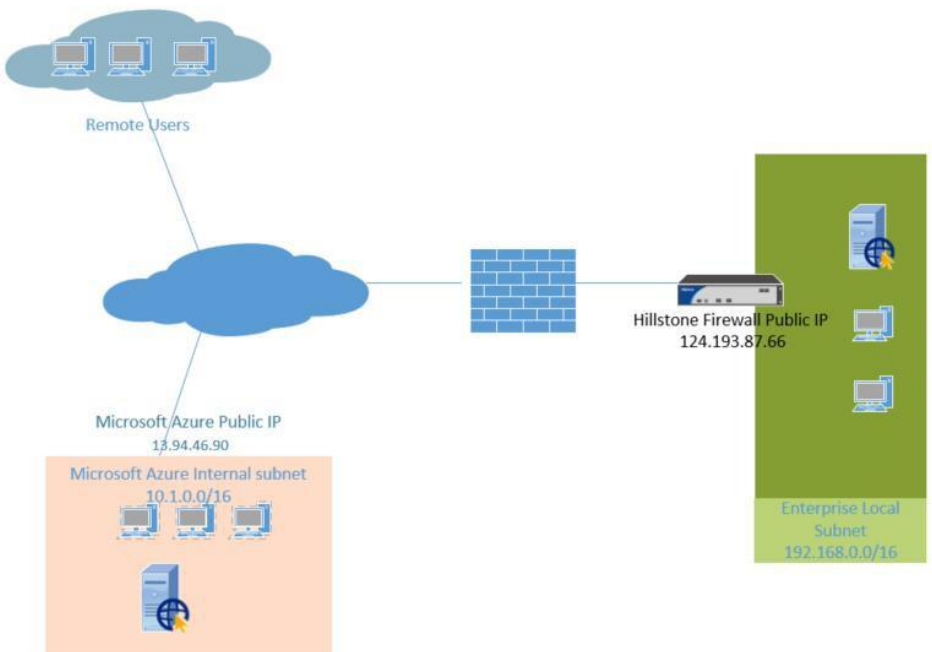
Today, more and more customers are using public cloud service providers such as Microsoft Azure to deploy their server or services, to get high performance, reliable services that are easy to deploy and get to market fastest.

But, these same customers still maintain local branch offices or datacenters. How do you securely connect local services with hosted cloud services? The solution is Hillstone Networks and this document outlines the steps to connect to Windows Azure.

Windows Azure has a relatively fixed setting on IKEv2. To set up an IPSEC tunnel between a Hillstone firewall and an Azure IPSEC service, simply do a match on the Hillstone device.

Below is a typical topology, with the following details as example:

- Hillstone Firewall Public IP: 124.193.87.66
- Hillstone side internal subnet: 192.168.0.0/16
- Azure side Public IP: 13.94.46.90
- Azure side internal subnet: 10.1.0.0/16



This article shows how to setup site-to-site VPN between Microsoft Azure and an on premise Hillstone Networks security gateway.

II. Notes

- IKEv2 can only be configured via **CLI** on Hillstone Networks device. WebUI configuration feature will be added in the future versions.
- The **"local-id"** and **"remote-id"** IPSec identifier flags for Phase 2 must be set to the local VPN public IP address and the Azure Gateway public IP address, respectively.
- You **cannot clear your IKEv2 IKE-SA's** via CLI nor via GUI in v5.5R7. This will be fixed later.
- You cannot use **SHA-256** as a hashing algorithm for Phase 1 (Main Mode), with the Hillstone VPN device. This will be fixed later.
- Refer to https://docs.microsoft.com/en-gb/azure/vpn-gateway/vpn-gateway-about-vpn-devices
- Refer to https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

III. Configuration

Configure Microsoft Azure

1. Create a virtual network

- Click Create a resource
- In *Search the Marketplace* field, search Virtual Network
- Click Create on Virtual Network page
- Fill in the following fields:
    - Name
    - Address space
    - Subscription (select an existing subscription to use)
    - Resource group (create a new group, or select an existing one)
    - Location (select from dropdown)
    - Subnet Name
    - Subnet Address range
- Click Create to create the virtual network

2. Create the gateway subnet

- Navigate to the virtual network for which you want to create a virtual network gateway
- Click Subnets
- Click +Gateway subnet

- Fill in the following fields:
    - Address range (CIDR block)
- Click OK to create the gateway subnet

3. Create the VPN gateway

- Click Create a resource
- In *Search the Marketplace* field, search Virtual Network Gateway
- Click Create on Virtual Network Gateway page
- Fill in the following fields:
    - Name
    - Gateway type: VPN
    - VPN type
    - SKU (Refer to https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings#gwsku)
    - Location (choose the one where your virtual network is located)
    - Virtual network (choose the one to which you want to add the gateway)
    - Public IP address (only dynamic Public IP address allocation is supported currently; input the public address name)
- Click Create and wait for the virtual network gateway deployment (it may take up to 45 minutes)
- After the virtual network gateway created, the public IP address will be assigned

4. Create the local network gateway

- Click Create a resource
- In *Search the Marketplace* field, search Local Network Gateway
- Click Create on Local Network Gateway page
- Fill in the following fields:
    - Name
    - IP address
    - Address space
    - Resource group
    - Location (can be different than the virtual network in step 1)
- Click Create to create the local network gateway

Configure Hillstone Networks device

5. Configure your Hillstone Networks device

- Setup IKEv2 proposal
    - ikev2 proposal “prop1”
    - hash sha
    - encryption 3des
    - group 2

- lifetime 10800
- exit

- setup IPSEC proposal
  - ikev2 ipsec-proposal "prop2"
  - hash sha
  - encryption aes
  - lifetime 3600
  - exit
- Setup IKEv2 peer
  - ikev2 peer "peer1"
  - interface ethernet0/1
  - match-peer "13.94.46.90"
  - ikev2-proposal "prop1"
  - local-id ip 124.193.87.66
  - ikev2-profile "esp-peer1"
  - remote id ip 13.94.46.90
  - remote key "key"
  - traffic-selector src subnet 192.168.0.0/16
  - traffic-selector dst subnet 10.1.0.0/16
  - exit
  - ikev2-profile "esp-peer1"
  - exit
  - exit
- Setup the IPSEC tunnel
  - tunnel ipsec "azure" ikev2
  - ikev2-peer "peer1"
  - ipsec-proposal "prop2"
  - auto-connect
  - exit
  - interface tunnel1
  - zone trust
  - tunnel ikev2 azure
  - exit
  - ip vrouter trust-vr
  - ip route 10.1.0.0/16 tunnel1
  - exit

(Note: the match-peer IP address and remote id IP address should be the Azure public IP address assigned in step 3; the local id IP address should be the local public IP address; the traffic-selector src subnet should be the local subnet; the traffic-selector dst subnet should be the Azure subnet; the remote key value should be the same to be configured on Azure)

Configure Microsoft Azure

6. Create the VPN connection

- Click the Virtual Network Gateway you want to use
- Click Connections

- Click Add
- Fill in the following fields:
    - Name
    - Connection type: Select Site-to-site(IPSec)
    - Virtual network gateway: fixed
    - Local network gateway: select the local network gateway created in step 4
    - Shared key (PSK): same as "key" in step 5
- Click OK to create the connection

After the configuration, you can check the VPN connection status.