Creating an IPSEC Tunnel with Microsoft Azure

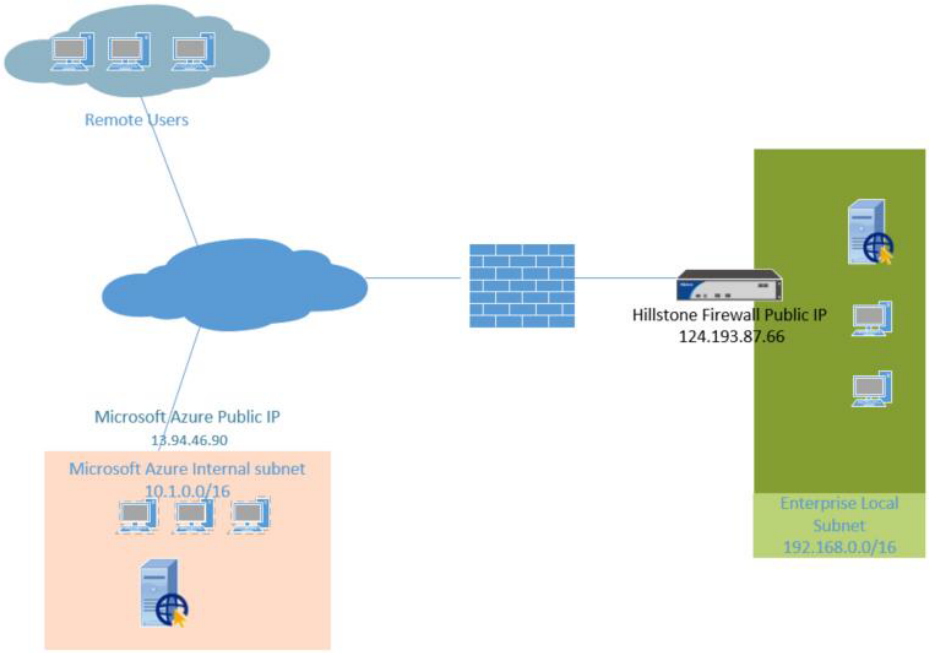
Today, more and more customers are using public cloud service providers such as Microsoft Azure to deploy their server or services, to get high performance, reliable services that are easy to deploy and get to market fastest.

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 configuration in 4 easy steps, with the following details:

- 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



Step1: Setup IKEv2 proposal

```
ikev2 proposal "prop1"
hash sha
encryption 3des
group 2
lifetime 10800
exit
```

Step2: setup IPSEC proposal

```
ikev2 ipsec-proposal "prop2"
hash sha
encryption aes
lifetime 3600
exit
```

Step3: 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
```

Step4: Setup the IPSEC tunnel

```
tunnel ipsec "azure" ikev2
ikev2-peer "peer1"
ipsec-proposal "prop2"
auto-connect
exit
```

After you complete Steps 1-4, the IKEv2 IPSEC tunnel between Hillstone and Azure will be complete. Admins can bind this tunnel to the routing table (routing based model) or Policy rule (Policy based model) of the firewall.