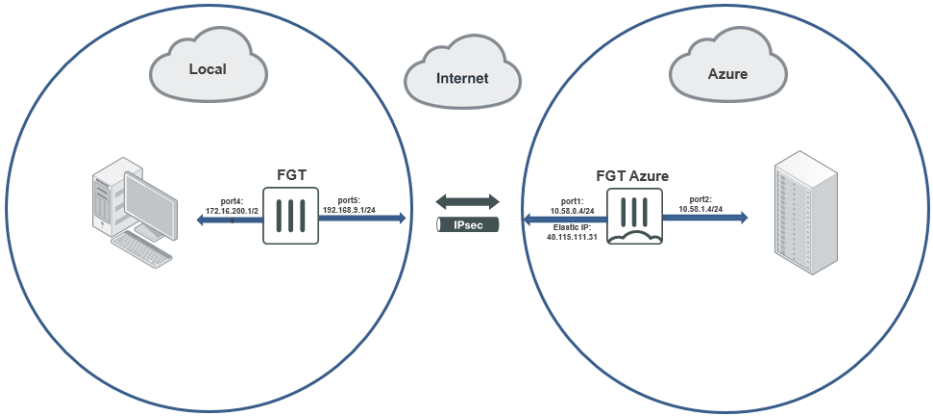
How to: Configure site-to-site VPN with local FortiGate to Azure FortiGate VM

By Elias Georgiou – System Consultant

FortiGate are next generation network firewalls manufactured from Fortinet that provide security for your network and unmatched threat protection for businesses of any kind or size. FortiGate is suitable small networks and can support up to hyperscale datacenters and are ideal for hybrid environments as well. FortiGate can be hardware, virtual and as we will see below a combination of both.

The following guide will provide a sample configuration scenario for a site to site VPN connection with a local FortiGate to an Azure FortiGate using IPsec VPN with static routing.

The following image shows the sample topology for this configuration:



As per the above diagram the topology is consisted of a local FortiGate in a local environment with port5 configured as WAN and port 4 as LAN and a FortiGate located in Azure with port1 connected to WAN and port 2 connected to LAN.

The configuration guide using the GUI is consisted of the below steps:

1. **Configure the local FortiGate:**
    a. Configure the interfaces.
    b. Configure a static route to connect to the Internet.
    c. Configure IPsec VPN.
2. **Configure the Azure FortiGate:**
    a. Configure the interface.
    b. Configure IPsec VPN.
3. **Bring up the VPN tunnel on the local FortiGate.**
4. **Verify the VPN tunnel on both the local FortiGate and the Azure FortiGate.**

Configure the local FortiGate

To configure the interfaces:

1. In FortiOS on the local FortiGate, go to *Network* > *Interfaces*.
2. Edit *port5*. Set the role to *WAN* and set an *IP/Network Mask* of 192.168.5.1/255.255.255.0. This is for the interface connected to the Internet.

3. Edit *port4*. Set the role to *LAN* and set an *IP/Network Mask* of 172.16.200.1/255.255.255.0. This is for the interface connected to the local subnet.

To configure a static route to connect to the Internet:

1. Go to *Network > Static Routes*.
2. Click *Create New*.
3. Set the *Destination* to 0.0.0.0/0.0.0.0.
4. For the *Interface*, select *port5*.
5. Set the *Gateway Address* to 192.168.9.254.

To configure IPsec VPN:

1. Go to *VPN > IPsec Wizard*.
2. Configure *VPN Setup*:
    a. Enter the desired VPN name. In the example, this is "to_cloud".
    b. For *Template Type*, select *Site to Site*.
    c. For the *Remote Device Type*, select *FortiGate*.
    d. For *NAT Configuration*, select *This site is behind NAT*. For non dial-up situations where your local FortiGate has a public external IP address, you must choose *No NAT between sites*.
    e. Click *Next*.
3. Configure *Authentication*:
    a. For *Remote Device*, select *IP Address*.
    b. Enter an IP address of 40.115.111.31, which is the Azure FortiGate's port1 public IP address.
    c. For *Outgoing Interface*, select *port5*.
    d. Set the *Authentication Method* to *Pre-shared Key*.
    e. Enter a pre-shared key of 123456.
    f. Click *Next*.
4. Configure *Policy & Routing*:
    a. For *Local Interface*, select *port4*.
    b. FortiOS automatically populates *Local Subnets* with 172.16.200.0/24.
    c. Set the *Remote Subnets* to 10.58.1.0/24, which is the Azure FortiGate's port2 subnet.
    d. For *Internet Access*, select *None*.
    e. Click *Create*.

Configuring the Azure FortiGate

To configure the interface:

1. In FortiOS on the Azure FortiGate, go to *Network > Interfaces*.
2. Edit *port2*. Set the role to *LAN* and set an *IP/Network Mask* of 10.58.1.4/255.255.255.0. This is for the interface connected to the Azure local subnet.

To configure IPsec VPN:

1. Go to *VPN > IPsec Wizard*.
2. Configure *VPN Setup*:
    a. Enter the desired VPN name. In the example, this is "to_local".
    b. For *Template Type*, select *Site to Site*.
    c. For the *Remote Device Type*, select *FortiGate*.
    d. For *NAT Configuration*, select *This site is behind NAT*. For non dial-up situations where your local FortiGate has a public external IP address, you must choose *No NAT between sites*.
    e. Click *Next*.

3. Configure *Authentication*:
    a. For *Incoming Interface*, select *port1*.
    b. Set the *Authentication Method* to *Pre-shared Key*.
    c. Enter a pre-shared key of 123456.
    d. Click *Next*.
4. Configure *Policy & Routing*:
    a. For *Local Interface*, select *port2*.
    b. FortiOS automatically populates *Local Subnets* with 10.58.1.0/24.
    c. Set the *Remote Subnets* to 172.16.200.0/24, which is the local FortiGate's port4 subnet.
    d. For *Internet Access*, select *None*.
    e. Click *Create*.

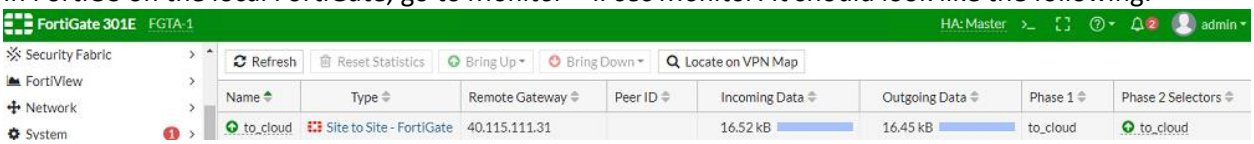
To bring up the VPN tunnel on the local FortiGate:

The tunnel is down until you initiate connection from the local FortiGate.

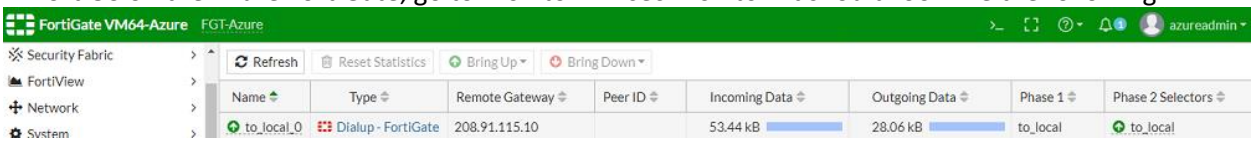
1. In FortiOS on the local FortiGate, go to *Monitor > IPsec Monitor*.
2. Click the to_cloud tunnel.
3. Click *Bring Up* to bring up the VPN tunnel.

To verify the VPN tunnel on both the local FortiGate and the Azure FortiGate:

In FortiOS on the local FortiGate, go to *Monitor > IPsec Monitor*. It should look like the following:



In FortiOS on the Azure FortiGate, go to *Monitor > IPsec Monitor*. It should look like the following:



Elias Georgiou is working for IBSCY for the last 4 years. He is working in the implementations department which consist of 4 people. His team is fully responsible for the implementations of new and existing clients in Cyprus and internationally. He holds several certifications from Microsoft, HPE, VMWare and other vendors.