HOW TO INTEGRATE FORTIGATE AND MICROSOFT AZURE VIRTUAL WAN

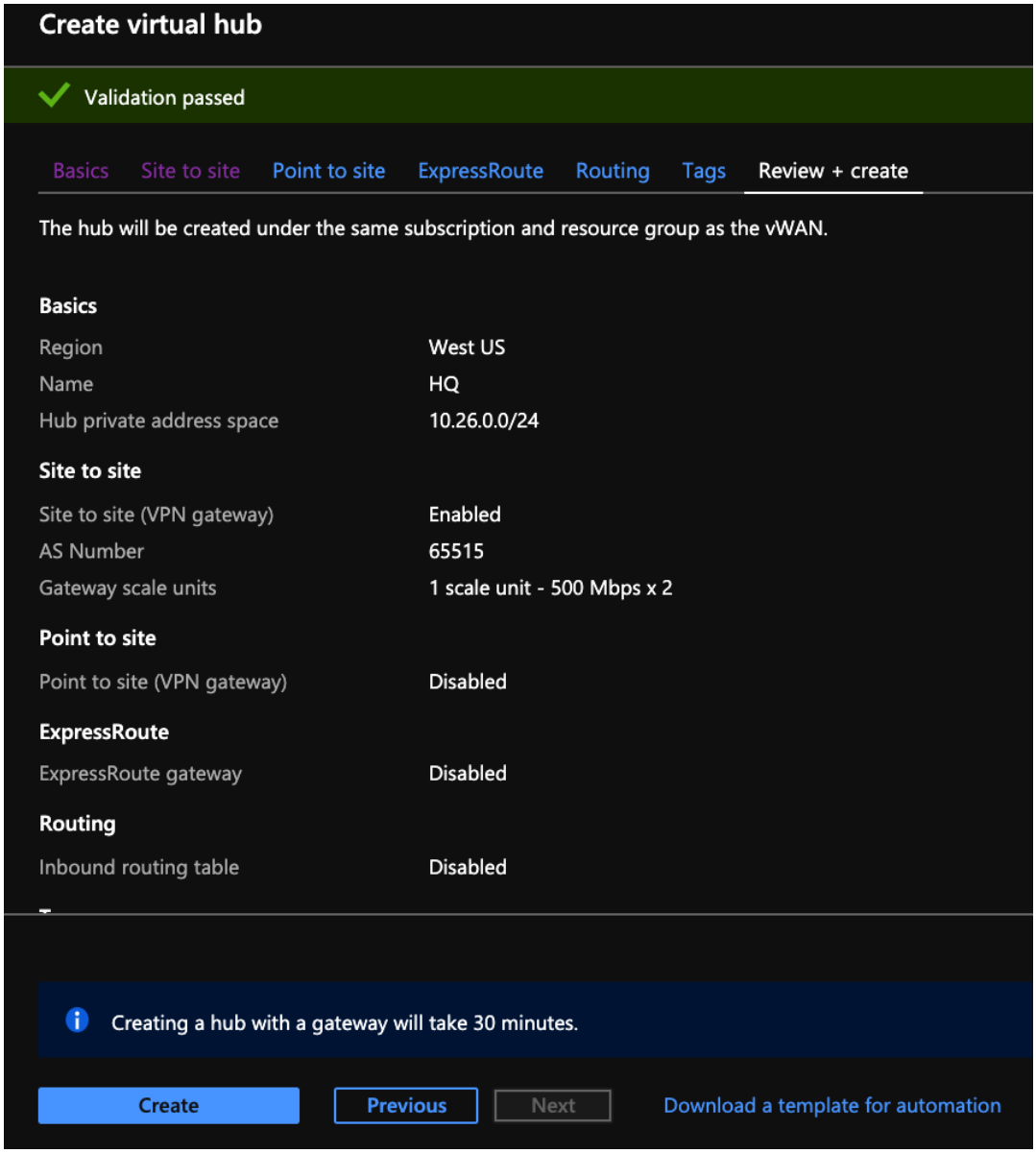
By Elias Georgiou – Team Leader – Implementation Services

WHAT IS AZURE VIRTUAL WAN?

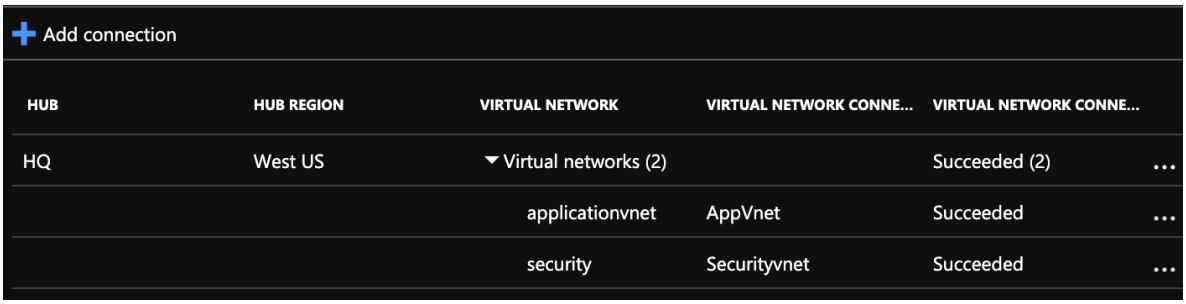
Microsoft Azure Virtual WAN is a managed networking service that combine networking, security, and routing capabilities to provide a single operational interface. This provides automated branch connectivity to, and through, **Azure**. The main features include Branch connectivity where you can connect branches and enjoy branch-to-virtual network connectivity by leveraging Azure backbone and Azure regions that serve as hubs which you can utilize to connect your branches to. Azure Virtual WAN also includes Site-to-Site VPN, Remote user VPN, Intra-cloud connectivity and VPN ExpressRoute.

Following is a detailed guide explaining how to configure **Fortinet**'s **FortiGate** to connect to the Azure Virtual WAN service. Moreover, it describes how to access Azure virtual networks and employ branch-to-branch connectivity.

1. First you need to create the Azure Virtual WAN in your Azure subscription. Click on Create a new resource and select Virtual WAN. Complete the fields as desired with all the required information such as the name, subscription, resource group and region.
2. Then enable communication between branches go to the newly created Virtual WAN and click on Allow branch to branch traffic under Configuration tab.
3. Next step is to create a Virtual WAN Hub. Navigate to Hubs and click on +New Hub. This configuration example connection to Azure is achieved using IPsec VPN so we need to create a VPN gateway on Site-to-site tab while creating the WAN Hub. Virtual Hub creation can take up to 30 minutes.



4. Next you must identify the Virtual Networks that should connect to the Virtual WAN Hub to enable end-to-end connectivity. Click on Virtual network connection, click Add connection and select the Virtual Networks.



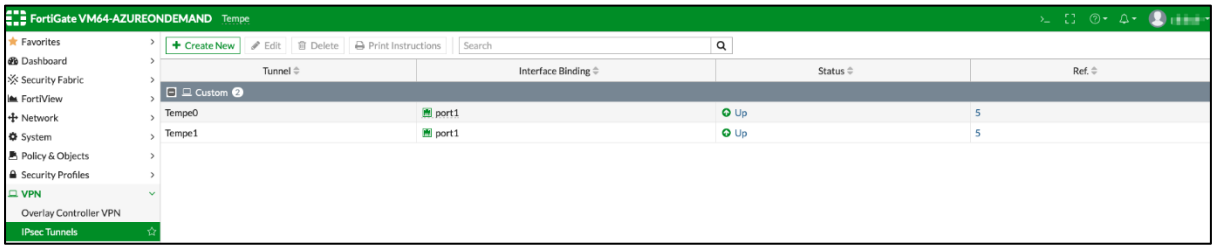
5. Following this we need to create an ARM template. To do so you must complete the following prerequisites, create a service principal, obtain Virtual WAN details, and create Remote_sites.txt file.
    a. **Create a service principal.** For this you need the Tenant ID (Azure Active Directory > Properties > Directory ID), Application ID (Azure Active Directory > App registrations > {your-app}) and Application secret which only appears once.
    b. **Obtain Virtual WAN details.** Name and resource group name.
    c. **Create the Remote_sites.txt file.** The Remote_sites.txt file serves as the input for Azure functions. The file contains information about all sites that want to connect to vWAN. You will store the file in a storage blob. You must include the following information in the file: Site name, FortiGate public IP address, internal networks behind FortiGate that will access the Virtual WAN, BGP ASN, peering IP address to use, VDOM and login credentials. An example is shown below:

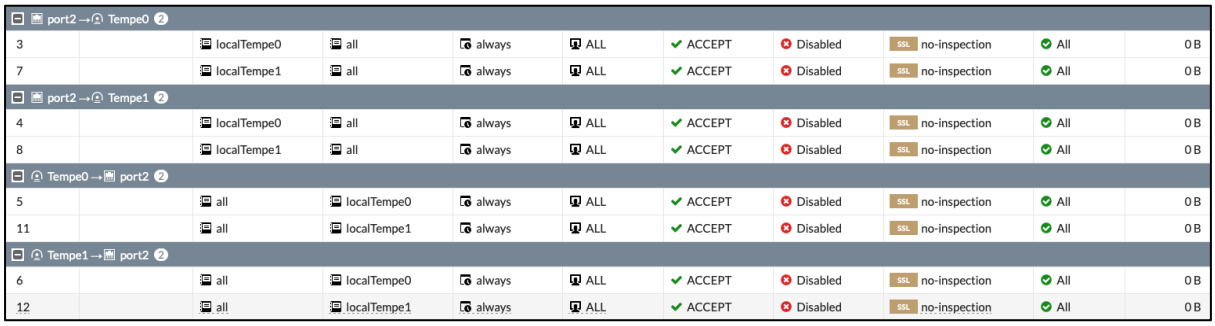
```
1) Tempe 51.140.67.103 10.0.11.0/24,10.0.15.0/24 azureadmin Password!234 root 169.254.24.24 7224
2) Folsom 40.115.47.140 172.31.1.0/24 azureadmin Password!234 root 169.254.24.25 7225
```

6. Then upload the ARM template to a Blob Container in a storage account.
7. Deploy the ARM template by clicking on Create new resource, select template deployment and Create. Click ***Build your own template in the editor***. In the editor, delete the default JSON content. Paste the **deploy_vwan_automation.json** file contents. Click ***Save***. The template to deploy the Virtual WAN solution appears and you can enter the parameters used to create the service principal. Click *Create*. Once Azure completes deployment, Azure displays a function app, its corresponding application lights, a storage account, and the service plan that Azure automatically generates for Linux function apps.
8. Following this you must associating the VPN sites with the Virtual WAN Hub. On the Virtual WAN page, go to the *VPN sites* tab and select the desired VPN sites, then click *New hub association. Then s*elect the desired Azure Virtual WAN hub and PSK. The default PSK chosen during Virtual WAN creation is used. Last click *Confirm*. Once Azure completes creating the association, the Azure VPN site status displays as shown.

SITE	PUBLIC IP ADDRESS	STATUS	HUB	RESOURCE GROUP LOCATION	SITE AS NUMBER
Folsom	40.115.47.140	See hub association status	1 hubs	West US	7225
			HQ - Connecting		
Tempe	51.140.67.103	See hub association status	1 hubs	West US	7224
			HQ - Connecting		

9. Finally, you need to verify the Virtual WAN configuration. The following shows FortiOS screenshots from a VPN site configured with Azure Virtual WAN automation. You can see that the redundant VPN tunnels, corresponding IPv4 policies, and BGP routing have been created.





The BGP routing table shows that this VPN site has access not only to the connected Virtual Networks on Azure, but also other remote sites.

Type	Network	Gateway IP	Interfaces	Distance
BGP	10.26.0.0/24	10.26.0.7	Tempe0	20
BGP	169.254.24.25/32	10.26.0.7	Tempe0	20
BGP	172.25.0.0/16	10.26.0.7	Tempe0	20
BGP	172.31.1.0/24	10.26.0.7	Tempe0	20
BGP	172.180.0.0/16	10.26.0.7	Tempe0	20

Pinging from one site to another succeeds, showing communication between the two branch offices.

```
Tempe #
Tempe # Tempe # execute ping-options source 10.0.11.4

Tempe # execute ping 172.31.1.5
PING 172.31.1.5 (172.31.1.5): 56 data bytes
64 bytes from 172.31.1.5: icmp_seq=0 ttl=63 time=282.7 ms
64 bytes from 172.31.1.5: icmp_seq=1 ttl=63 time=282.9 ms
64 bytes from 172.31.1.5: icmp_seq=2 ttl=63 time=282.9 ms
64 bytes from 172.31.1.5: icmp_seq=3 ttl=63 time=282.5 ms
64 bytes from 172.31.1.5: icmp_seq=4 ttl=63 time=283.0 ms

--- 172.31.1.5 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 282.5/282.8/283.0 ms
```

IBSCY Ltd is a Partner of Fortinet in Cyprus and Microsoft Solutions Partner for Azure Infrastructure in Cyprus providing excellent IT services with expertise to every business. Our employees are certified to sell, install, configure, and maintain all Microsoft Solutions and FortiGate devices in Cyprus.

Elias Georgiou is working for IBSCY for the last 6 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.