DEPLOYMENT GUIDE

FortiGate and Microsoft Azure Virtual WAN Integration

Table of Contents

1. Microsoft Azure Virtual WAN Introduction

Microsoft Azure Virtual WAN is an Azure-managed service that provides automated branch connectivity to, and through, Azure. You can leverage the Azure backbone to connect branches and enjoy branch-to-virtual network connectivity. Azure regions serve as hubs that you can use to connect your branches to.

This guide explains how to configure FortiGates to connect to the Azure Virtual WAN service. It also explains how to access virtual networks in Azure and employ branch-to-branch connectivity.

2. Virtual WAN Architecture Diagram

The Azure Virtual WAN architecture consists of the following important resources:

Virtual WAN. A virtual WAN resource is a virtual overlay of the Azure network. It contains resources that include all of the links to the virtual WAN hub.

Virtual hub. A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). There can only be one hub per Azure region. When a virtual WAN hub is created from the portal, it creates a virtual hub virtual network (VNet) and a virtual hub VPN gateway.

A hub gateway is not the same as a virtual network gateway that is used for ExpressRoute and VPN gateway. For example, when using virtual WAN, you do not create a site-to-site connection from the on-premises site directly to the virtual network. Instead, you will create a site-to-site connection to the hub, so the traffic always passes through the hub gateway. This means that your VNets do not need their own virtual network gateway. Virtual WAN allows your VNets to take advantage of scaling easily through the virtual hub and the virtual hub gateway.

Hub VNet connection. The hub VNet connection resource is used to connect the hub seamlessly to the VNet. Only the virtual networks that are within the same hub region can be connected to the virtual WAN hub.

Sites. A site resource is used for site-to-site connections only. The site resource is **vpnsite**. It represents your on-premises VPN device and its settings.

The Azure Virtual WAN architecture diagram below represents remote sites Tempe and Folsom, which connect to the virtual WAN hub. The hub virtual network is connected to two VNets: B and C. Connecting to the virtual WAN hub enables the sites Tempe and Folsom to access both VNets in Azure and to connect with each other through the virtual WAN hub.

There are redundant VPN tunnels from each branch to the virtual WAN hub to enhance connectivity. Routing is handled by Border Gateway Protocol (BGP).

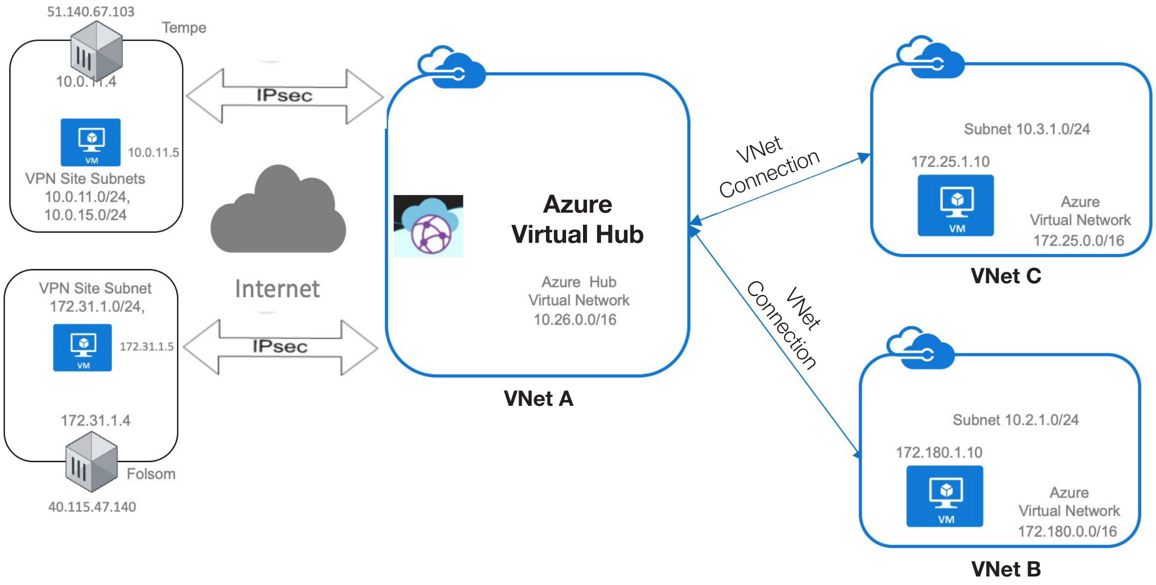


Figure 1: FortiGate(s) and Azure Virtual WAN architecture.

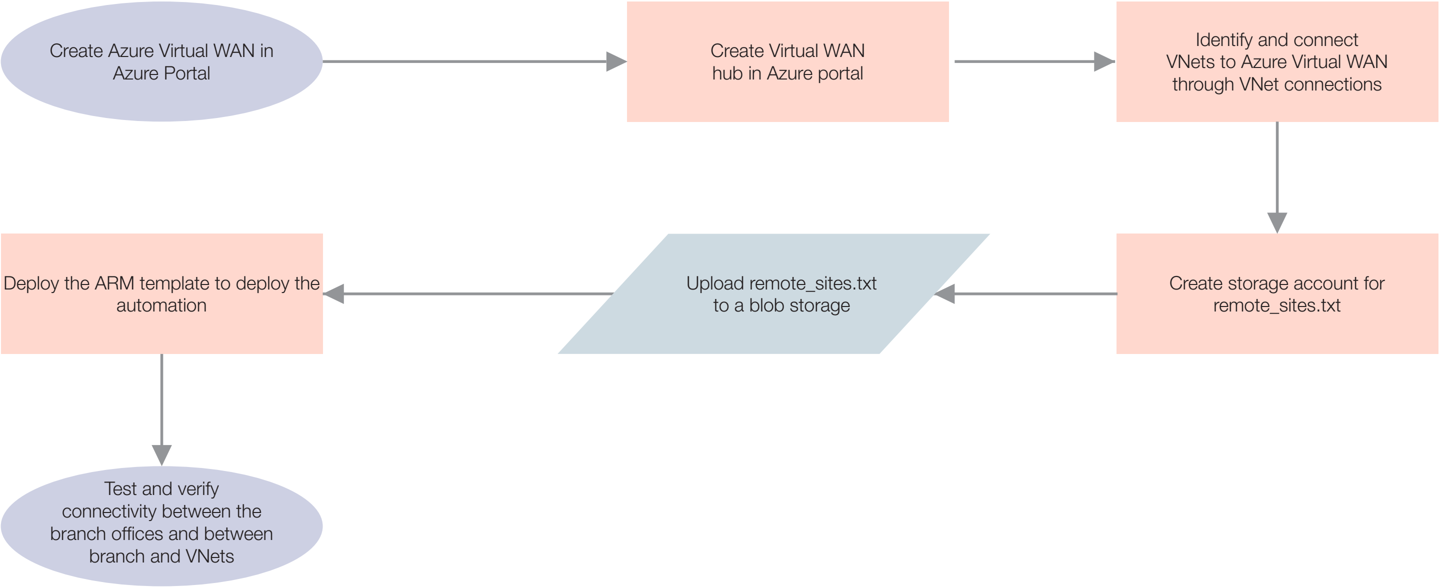

Create Azure Virtual WAN in Azure Portal
Create Virtual WAN hub in Azure portal
Identify and connect VNets to Azure Virtual WAN through VNet connections
Create storage account for remote_sites.txt
Upload remote_sites.txt to a blob storage
Deploy the ARM template to deploy the automation
Test and verify connectivity between the branch offices and between branch and VNets

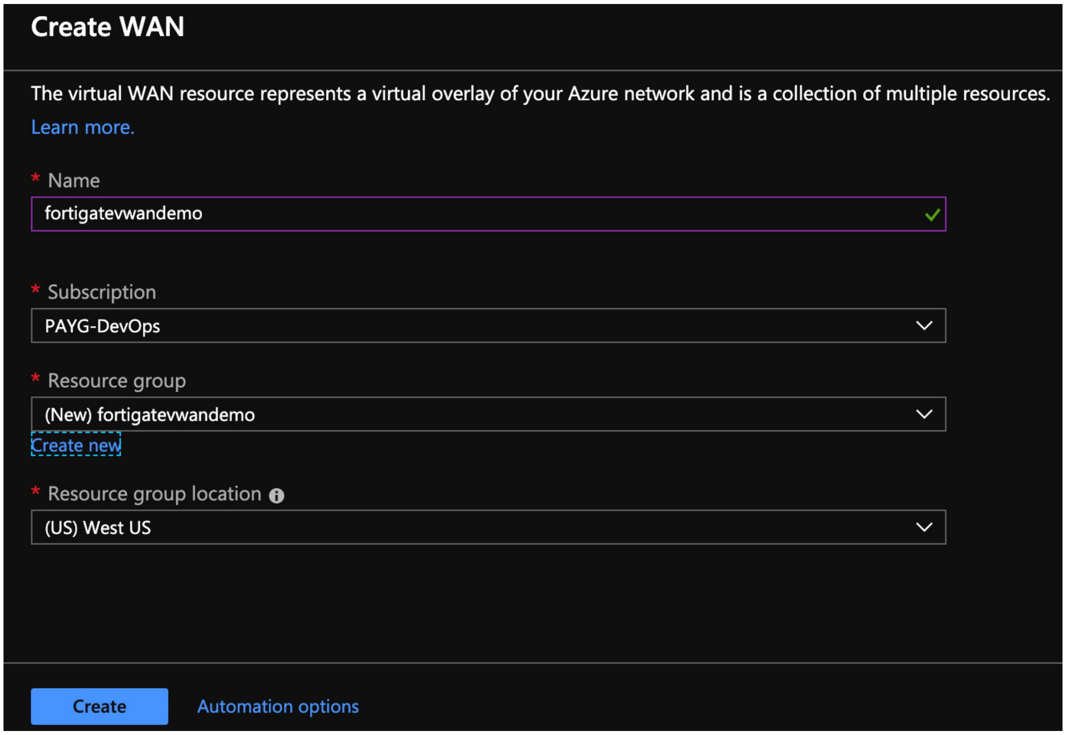
Figure 2: Process flow diagram of Azure Virtual WAN integration with FortiGate(s).

3. Creating the Azure Virtual WAN

First, the Azure Virtual WAN hub needs to be created within your subscription via the portal: https://portal.azure.com.

At this time, use of special characters or upper case letters is not supported for the name of the virtual WAN and also the resource group.

Once logged into the portal, click on **Create a new resource** and select **Virtual WAN**. Once the required information such as the name, region, resource group, and the subscription are chosen, the Azure Virtual WAN creation process will be completed.



Create WAN

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources.
Learn more.

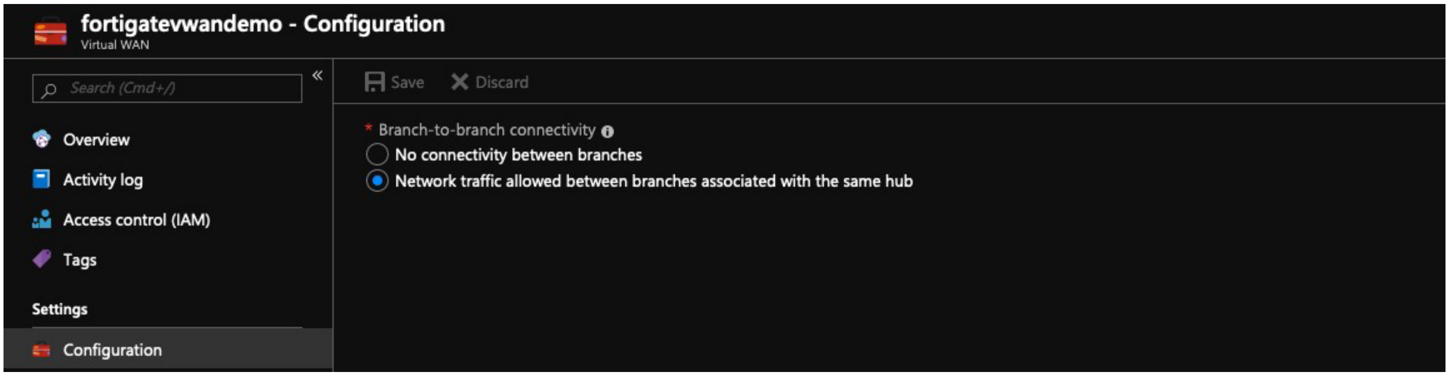
* Name
fortigatevwandemo

* Subscription
PAYG-DevOps

* Resource group
(New) fortigatevwandemo
Create new

* Resource group location
(US) West US

You can choose to enable branches to communicate with each other through the virtual WAN hub at this stage. Select **Network traffic allowed between branches associated with the same hub** under Configuration.



* Branch-to-branch connectivity

○ No connectivity between branches

● Network traffic allowed between branches associated with the same hub

The next step is to create a new virtual WAN hub.

To create a virtual WAN hub, navigate to **Hubs** and click on **+New Hub** to create a new hub.

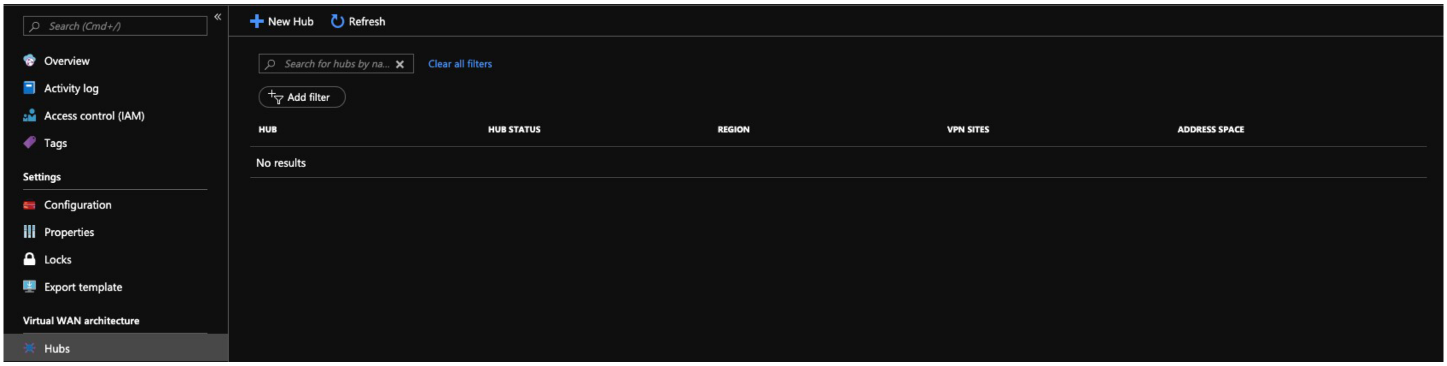
In the architecture discussed, site-to-site connectivity is used for connecting branch offices to the virtual WAN hub through IPsec VPNs. It requires creation of a VPN gateway, which can be created when the hub is created.

Point-to-site is for connecting end-user devices to the virtual WAN hub using OpenVPN and other VPN clients. Similarly, if ExpressRoutes are to be connected to the virtual WAN hub, an ExpressRoute gateway must be created.

Since the architecture here only pertains to site-to-site connections, point-to-site and ExpressRoute gateway creation will be disabled.

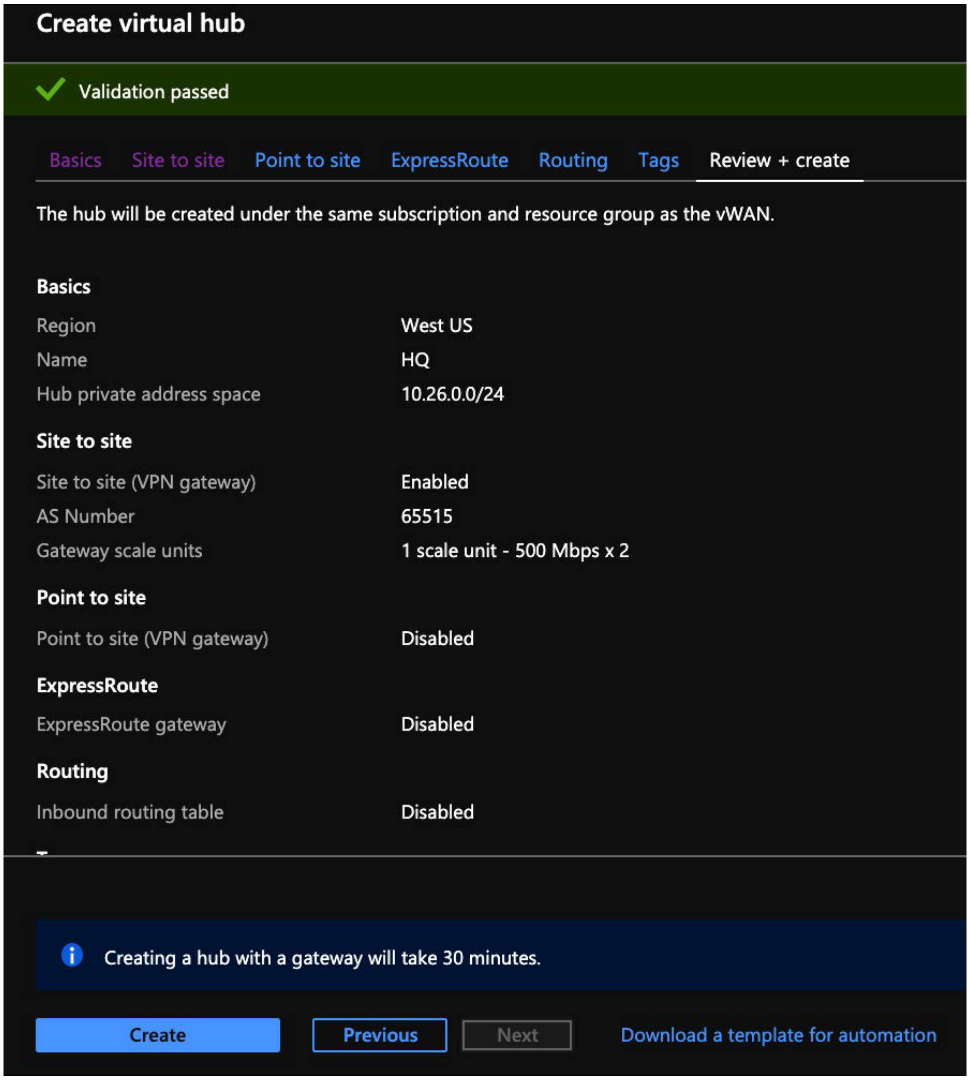
For advanced routing using the hub, routing tables must be set up. In this example, routing using the hub is not used, so route tables do not need to be enabled.

Creating a virtual WAN hub can take up to 30 minutes.



HUB	HUB STATUS	REGION	VPN SITES	ADDRESS SPACE
No results				

The following settings are used for site-to-site connectivity. The gateway scale units can be chosen depending on the traffic needs.



Create virtual hub

Validation passed

The hub will be created under the same subscription and resource group as the vWAN.

Basics

Region	West US
Name	HQ
Hub private address space	10.26.0.0/24

Site to site

Site to site (VPN gateway)	Enabled
AS Number	65515
Gateway scale units	1 scale unit - 500 Mbps x 2

Point to site

Point to site (VPN gateway)	Disabled

ExpressRoute

ExpressRoute gateway	Disabled

Routing

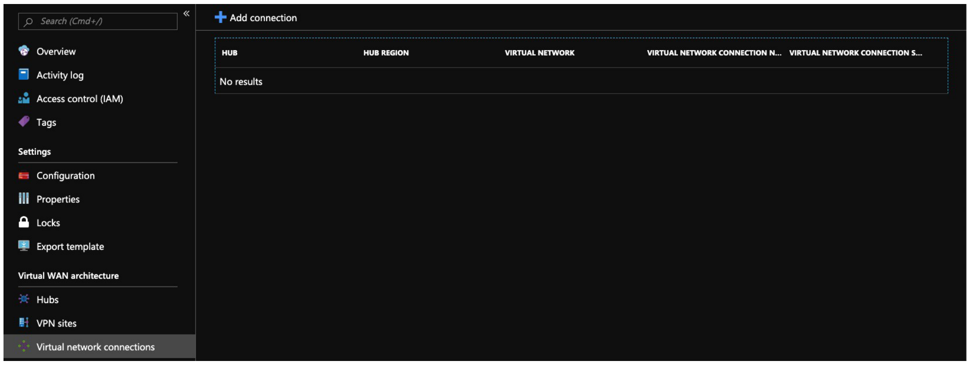
Inbound routing table	Disabled

Creating a hub with a gateway will take 30 minutes.

4. Adding Virtual Network Connections to the Virtual WAN Hub

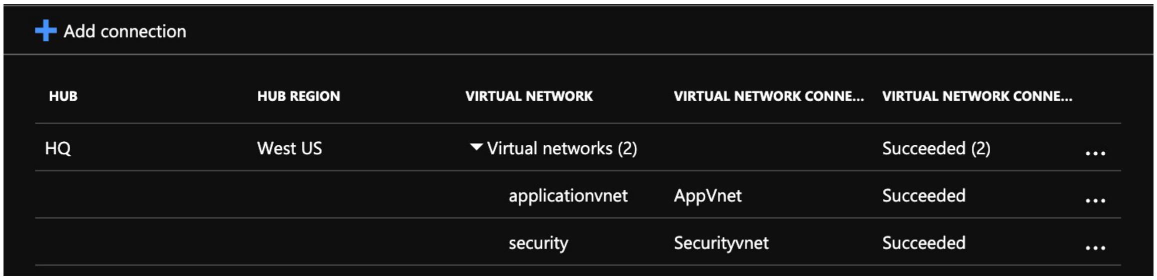
Once the Azure Virtual WAN is created, the next step is to identify the customer VNets that need to be connected to enable end-to-end connectivity.

In this example, there are two VNets, applicationvnet and security. To add them to the virtual WAN hub, start at the virtual WAN page. Navigate to the **Virtual Network Connections** tab, and click on **Add connection** to select the VNets that will connect to the virtual WAN hub.



HUB	HUB REGION	VIRTUAL NETWORK	VIRTUAL NETWORK CONNECTION N...	VIRTUAL NETWORK CONNECTION S...
No results				

Once the VNets are connected to the virtual WAN hub, they will appear as connections.



+ Add connection

HUB	HUB REGION	VIRTUAL NETWORK	VIRTUAL NETWORK CONNE...	VIRTUAL NETWORK CONNE...	
HQ	West US	▾Virtual networks (2)		Succeeded (2)	...
		applicationvnet	AppVnet	Succeeded	...
		security	Securityvnet	Succeeded	...

5. Deployment of the Azure Virtual WAN ARM Template

5.1 Prerequisites for the deployment

Before the Azure Resource Manager (ARM) template can be deployed, the following prerequisites must be met:

- Service principal
- Details about the virtual WAN
- Storage blob that contains the remote_sites.txt file

Service principal

1. Log into your Azure account. If you do not already have one, create one by following the on-screen instructions.
2. Create a service principal, making note of the following items as they will be needed to deploy the Function App:
   - Tenant ID (used for the Tenant ID parameter). This is under **Azure Active Directory > Properties > Directory ID**. This is not required for the hybrid licensing deployment.
   - Application ID (used for the Rest App ID parameter). This is under **Azure Active Directory > App registrations > {your-app}**.
   - Application secret (used for the Rest App Secret parameter). The application secret only appears once and cannot be retrieved.

Details about virtual WAN

The following information is needed about the Azure Virtual WAN service :

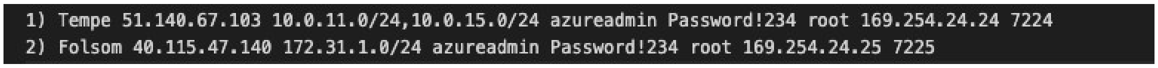
- Virtual WAN name
- Name of the resource group

Remote_sites.txt

This is the main file that serves as the input for Azure functions. This contains the information about all of the sites that want to connect to the Azure Virtual WAN service. This file is stored in a storage blob. The following information is required:

- Name of the site (to be used as an identifier in Azure)
- Public IP address of the FortiGate
- Internal networks behind the FortiGate that need access to the virtual WAN
- The BGP ASN and BGP peering IP address to use
- VDOM
- Login credentials

Contents of a sample remote_sites.txt file format is shown below.

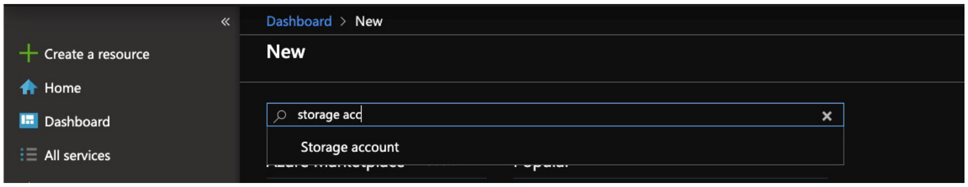


```
1) Tempe 51.140.67.103 10.0.11.0/24,10.0.15.0/24 azureadmin Password!234 root 169.254.24.24 7224
2) Folsom 40.115.47.140 172.31.1.0/24 azureadmin Password!234 root 169.254.24.25 7225
```

5.2 Storage account and remote_sites.txt upload

Once the remote_sites.txt file is populated, it needs to be uploaded to the Azure blob storage in a storage account. The following steps explain how to create a storage account and store the remote_sites.txt file in the blob storage.

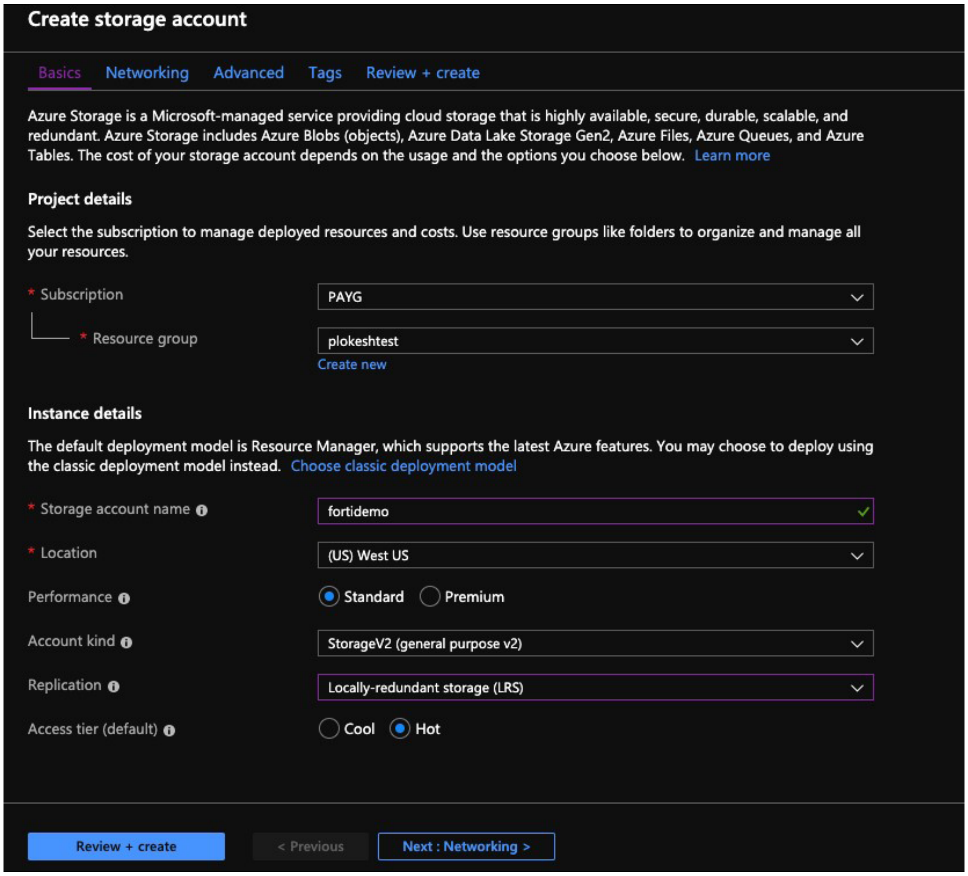
To create a storage account from the Azure portal, click on **Create a resource**, type "storage account" and select the storage account resource creation. Click **Create**.



storage acc

Storage account

In the following screen, select a **Resource group**, or create a new one. This is the location where the storage account will reside. A unique name for the storage account is required, as each storage account URL is unique. The other fields can be left as default. The replication can also be set to locally redundant storage.



Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

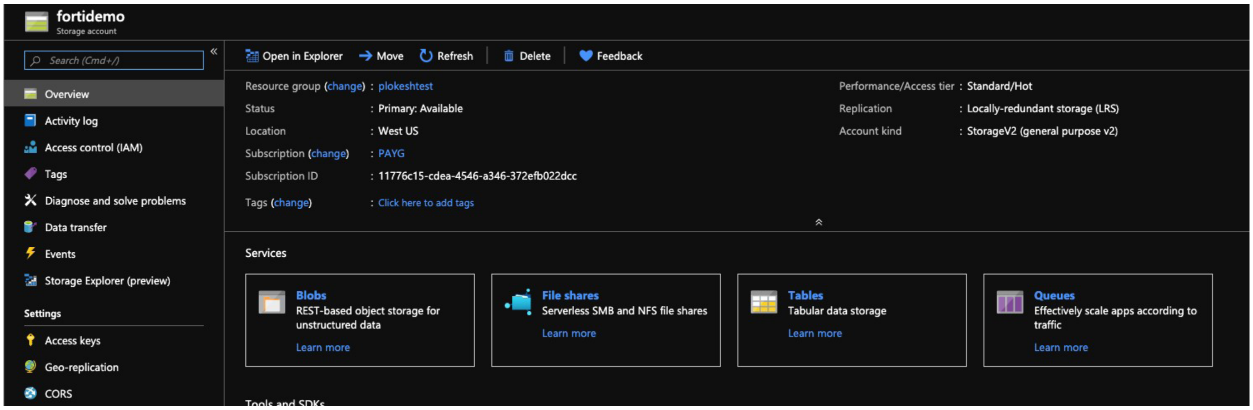
* Subscription	PAYG
* Resource group	plokeshtest Create new

Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. Choose classic deployment model

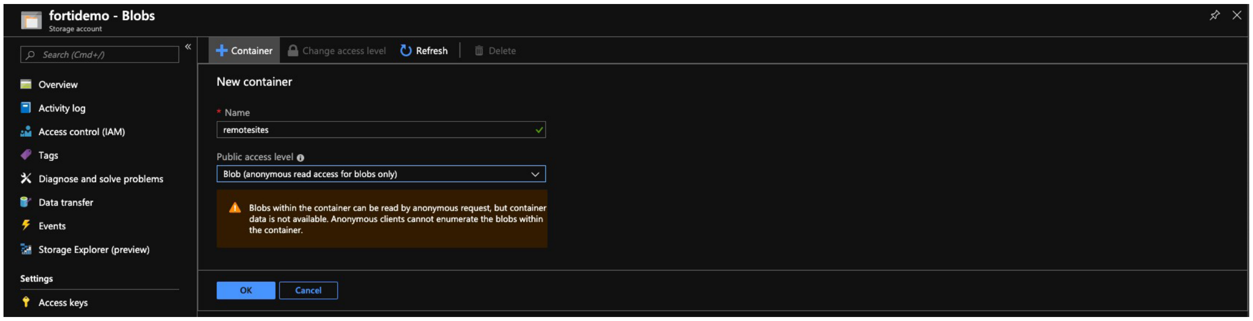
* Storage account name	fortidemo ✓
* Location	(US) West US
Performance	● Standard ○ Premium
Account kind	StorageV2 (general purpose v2)
Replication	Locally-redundant storage (LRS)
Access tier (default)	○ Cool ● Hot

Everything in the **Advanced** and **Tags** sections can also be left as default. Click on **Review + create** to create the storage account.



Resource group (change) : plokeshtest
Status : Primary: Available
Location : West US
Subscription (change) : PAYG
Subscription ID : 11776c15-cdea-4546-a346-372efb022dcc
Tags (change) : Click here to add tags
Performance/Access tier : Standard/Hot
Replication : Locally-redundant storage (LRS)
Account kind : StorageV2 (general purpose v2)

Once the storage account is configured, navigate to the **Blobs** section of the storage account and create a container by clicking on **+Container**. Create a container that enables read access to blobs.



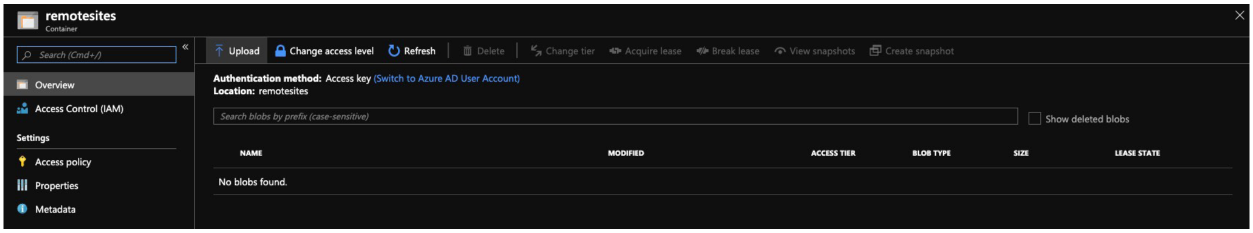
New container

* Name: remotesites

Public access level: Blob (anonymous read access for blobs only)

Blobs within the container can be read by anonymous request, but container data is not available. Anonymous clients cannot enumerate the blobs within the container.

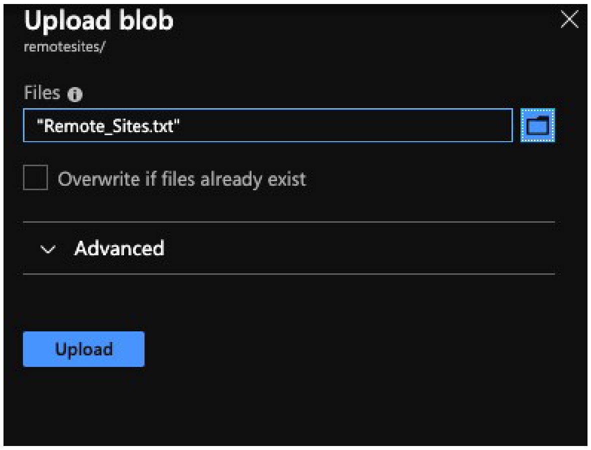
Once the container is created, click on the container name, then click **Upload** to upload the remote_sites.txt file.



Authentication method: Access key (Switch to Azure AD User Account)
Location: remotesites

NAME	MODIFIED	ACCESS TIER	BLOB TYPE	SIZE	LEASE STATE
No blobs found.					

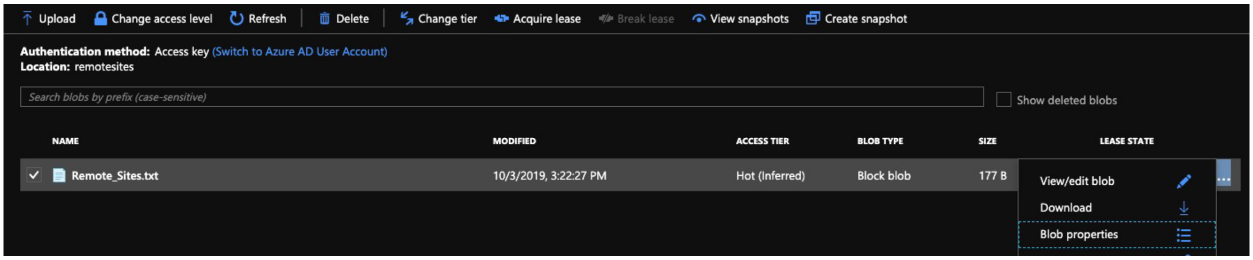
Select the **Remote_Sites.txt** file and click **Upload**.



Files: "Remote_Sites.txt"

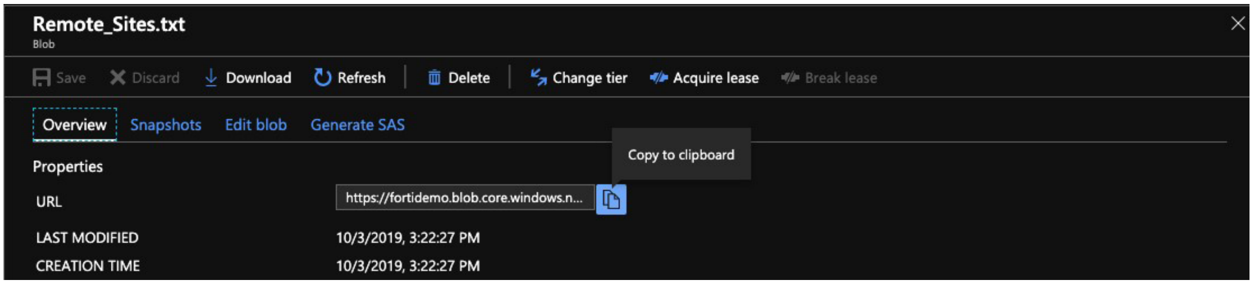
☐ Overwrite if files already exist

Once the file is uploaded, right click on the file and click on **Blob properties**. Copy the file URL. This is one of the parameters of the ARM template.



Authentication method: Access key (Switch to Azure AD User Account)
Location: remotesites

NAME	MODIFIED	ACCESS TIER	BLOB TYPE	SIZE	LEASE STATE
Remote_Sites.txt	10/3/2019, 3:22:27 PM	Hot (Inferred)	Block blob	177 B	



Properties

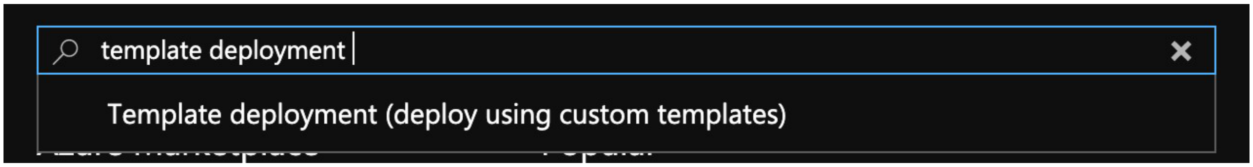
URL	https://fortidemo.blob.core.windows.n...
LAST MODIFIED	10/3/2019, 3:22:27 PM
CREATION TIME	10/3/2019, 3:22:27 PM

5.3 ARM template deployment

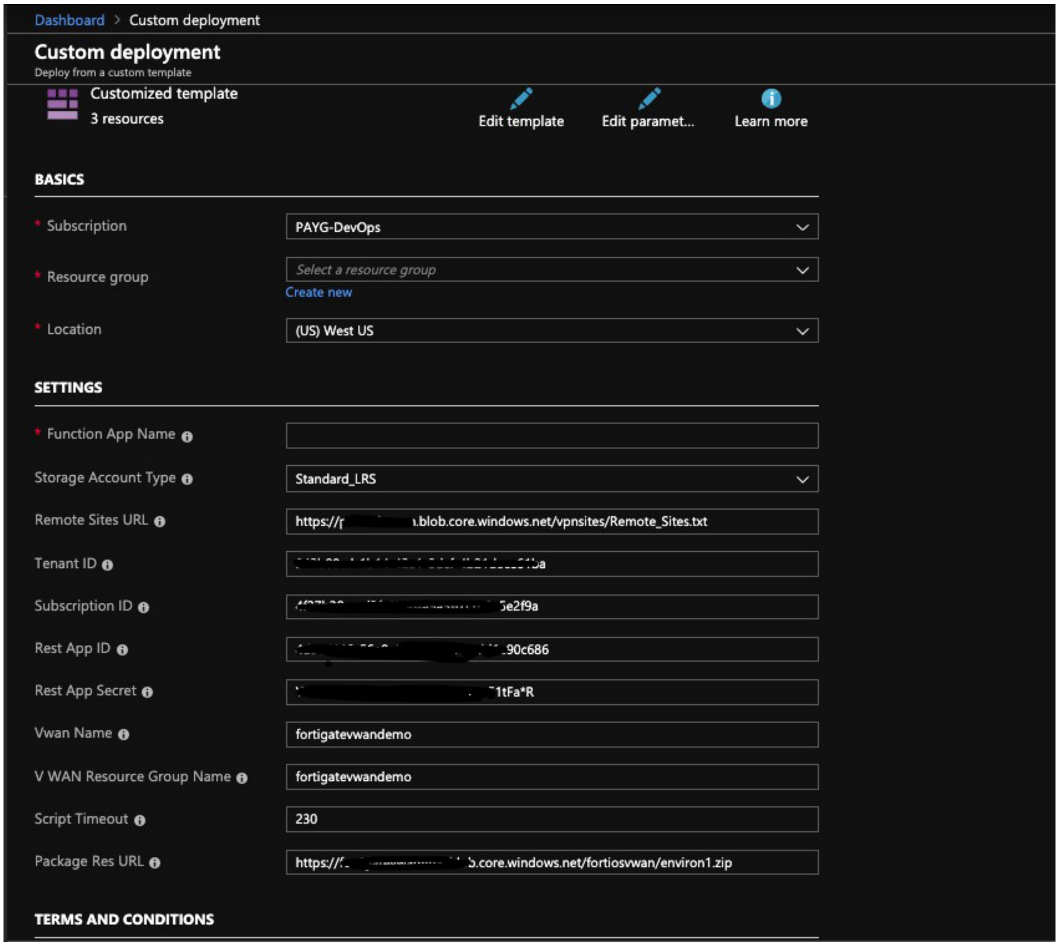
Once all the prerequisites are in place, the next step is to deploy the template. The template can be accessed in the following link:

https://fortigatevwanfinal.blob.core.windows.net/fortiosvwan/deploy_vwan_automation.json

Once the deploy_vwan_automation.json is downloaded, **log in** to the Azure portal and click on **Create New Resource**. Enter "template deployment", select the **Template deployment (deploy using custom templates)** option. Click **Create**.



In the following screen, click on **Build your own template in the editor**. In the editor window, **delete** the default **JSON** content, paste the contents of the deploy_vwan_automation.json file, and click on **save**. The template to deploy the virtual WAN solution **will appear and allow you** to enter the parameters that are discussed in the prerequisites.



BASICS

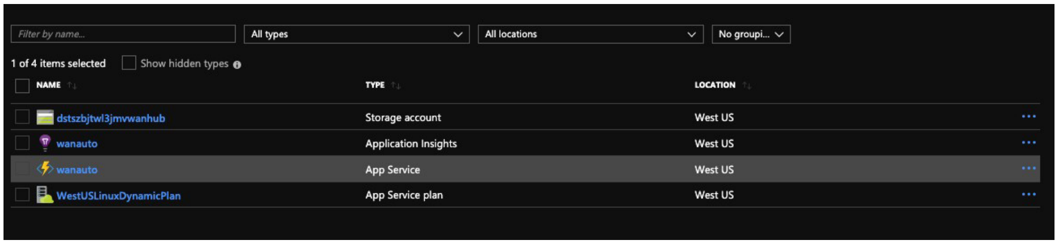
- * Subscription: PAYG-DevOps
- * Resource group: Select a resource group (Create new)
- * Location: (US) West US

SETTINGS

- * Function App Name:
- Storage Account Type: Standard_LRS
- Remote Sites URL: https://[redacted].blob.core.windows.net/vpnsites/Remote_Sites.txt
- Tenant ID: [redacted]a
- Subscription ID: [redacted]e2f9a
- Rest App ID: [redacted]90c686
- Rest App Secret: [redacted]1tFa*R
- Vwan Name: fortigatevwandemo
- V WAN Resource Group Name: fortigatevwandemo
- Script Timeout: 230
- Package Res URL: https://[redacted].core.windows.net/fortiosvwan/environ1.zip

TERMS AND CONDITIONS

Once all fields are completed, click on **Create** to deploy the template. Once the template is deployed, you will see a function app, its corresponding application insights, a storage account, and the service plan that is automatically generated for Linux function apps.

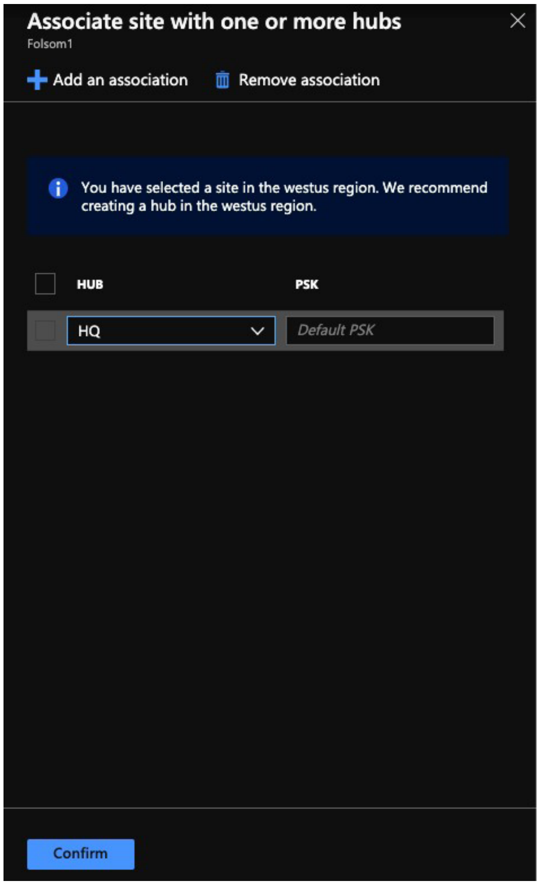


NAME	TYPE	LOCATION
dstszbjtwl3jmvwanhub	Storage account	West US
wanauto	Application Insights	West US
wanauto	App Service	West US
WestUSLinuxDynamicPlan	App Service plan	West US

6. Associating the VPN Sites with the Virtual WAN Hub

6.1 Adding hub association

Once the template is deployed, the VPN sites are created from the remote_sites.txt file. The next step is to associate it with the right virtual WAN hub. To do this, navigate to the **VPN sites** tab on your virtual WAN page, select the VPN site(s), and click on **Add an association**. Select the right virtual WAN hub and the PSK. The default PSK that was chosen during the virtual WAN creation will be used. Next, click on **Confirm** to create the association.



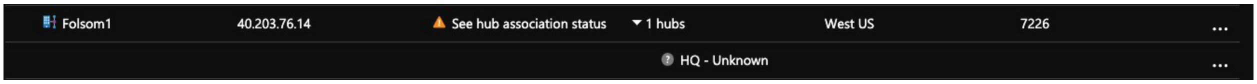
Associate site with one or more hubs

Folsom1

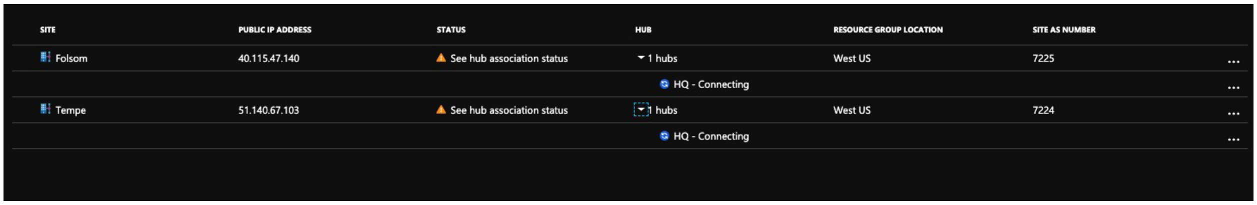
You have selected a site in the westus region. We recommend creating a hub in the westus region.

	HUB	PSK
□	HQ	Default PSK

After the association is complete, the status of the VPN site will update as pictured below.



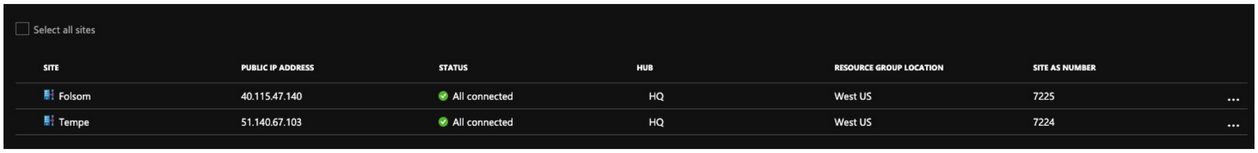
Folsom1	40.203.76.14	See hub association status	1 hubs	West US	7226	...
			HQ - Unknown			...



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			...

Once the hub association is complete, the Azure functions will configure the remote sites with the correct VPN, BGP, and firewall policies by logging into one of the FortiGates. It will check to see if there are any new remote sites and corresponding hub associations every 30 minutes. Azure functions will configure new sites and connect them to the virtual WAN solution.

After the configuration is complete, the status of VPN sites will change to **All connected**.



□ Select all sites

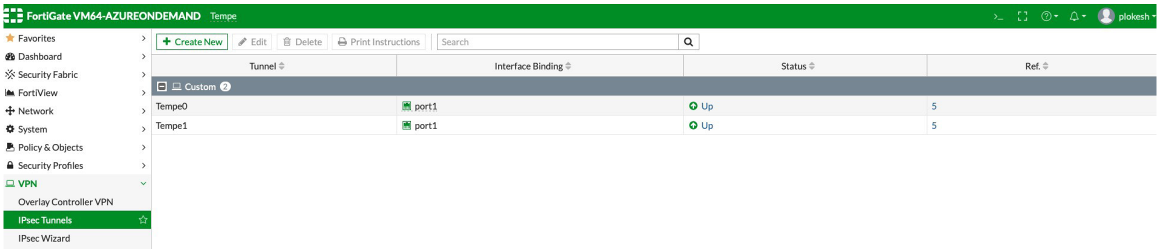
SITE	PUBLIC IP ADDRESS	STATUS	HUB	RESOURCE GROUP LOCATION	SITE AS NUMBER	
Folsom	40.115.47.140	All connected	HQ	West US	7225	...
Tempe	51.140.67.103	All connected	HQ	West US	7224	...

The access between the remote site and VNet resources, and the access between two remote sites, can also be verified.

7. Validation

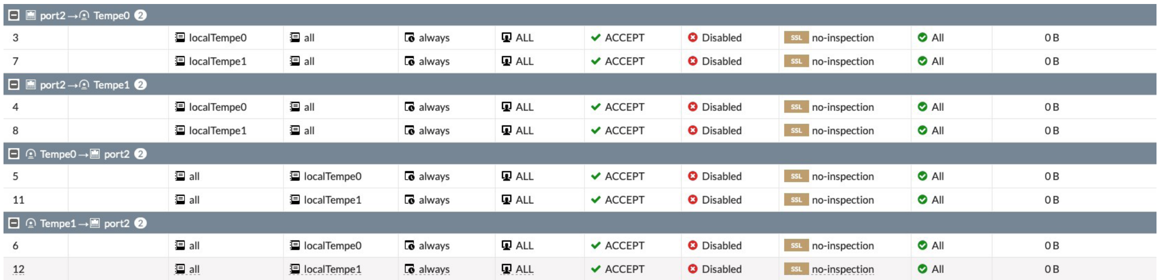
The following screenshots are from one of the VPN sites that the Azure Virtual WAN automation configured. It can be seen that the redundant VPN tunnels, corresponding IPv4 policies, and BGP routing have been created. The ping from one site to another site is successful, as shown below.

Redundant VPN tunnels to the virtual WAN hub:

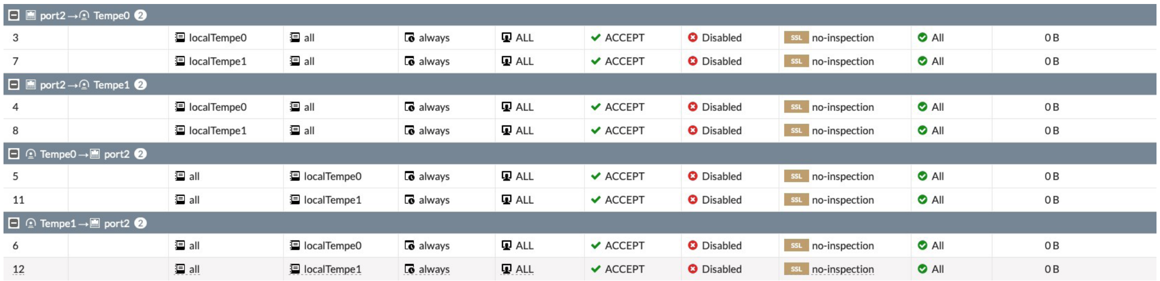


Tunnel	Interface Binding	Status	Ref.
Custom 2			
Tempe0	port1	Up	5
Tempe1	port1	Up	5

Firewall policies between the tunnel interfaces and the internal networks:

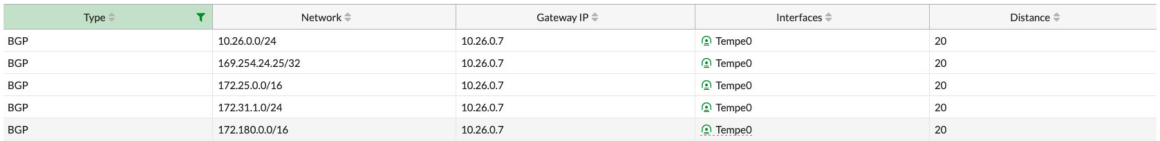


port2 → Tempe0 2										
3		localTempe0	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
7		localTempe1	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
port2 → Tempe1 2										
4		localTempe0	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
8		localTempe1	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
Tempe0 → port2 2										
5		all	localTempe0	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
11		all	localTempe1	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
Tempe1 → port2 2										
6		all	localTempe0	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
12		all	localTempe1	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B



port2 → Tempe0 2										
3		localTempe0	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
7		localTempe1	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
port2 → Tempe1 2										
4		localTempe0	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
8		localTempe1	all	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
Tempe0 → port2 2										
5		all	localTempe0	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
11		all	localTempe1	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
Tempe1 → port2 2										
6		all	localTempe0	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B
12		all	localTempe1	always	ALL	✓ ACCEPT	Disabled	SSL no-inspection	All	0 B

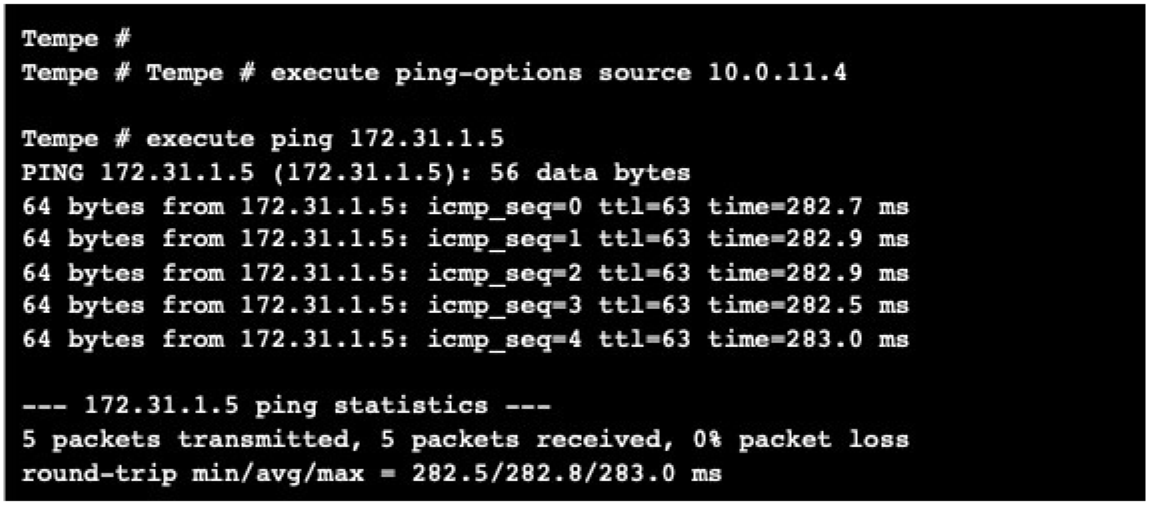
BGP routing from the routing monitor:



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

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

The successful ping shows 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
```