



# F5 BIG-IP and Azure Virtual WAN Integration

## WHAT'S INSIDE

- 2 Topology Used in This Deployment Guide
- 3 Prerequisites
- 3 Deployment Guide
- 4 Azure Virtual WAN Setup
- 5 Azure Hubs Setup
- 10 Virtual Network Connections Setup
- 14 VPN Site Setup
- 18 F5 BIG-IP Setup

## Introduction

### WHAT IS AZURE VIRTUAL WAN?

Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface.

These functionalities include branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE), site-to-site VPN connectivity, remote user VPN (point-to-site) connectivity, private (ExpressRoute) connectivity, intra-cloud connectivity (transitive connectivity for virtual networks), VPN ExpressRoute inter-connectivity, routing, Azure Firewall, and encryption for private connectivity.

#### More information about Azure Virtual WAN:

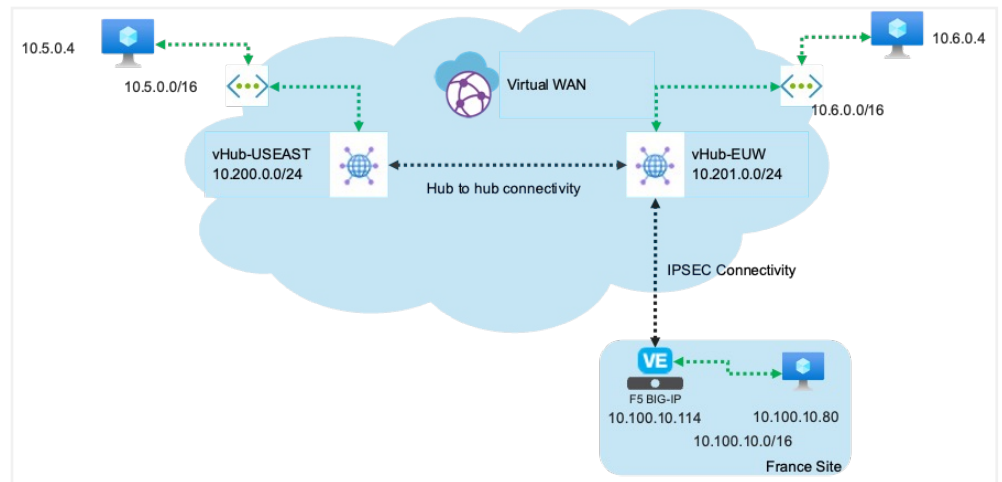
<https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about>.

### USING BIG-IP TO CONNECT TO AZURE VIRTUAL WAN

You can leverage F5® BIG-IP® to establish site-to-site connectivity via Internet Protocol Security (IPsec). This gives you the ability to establish a secure access between any remote site and your Azure Virtual WAN environment.

In this deployment guide, we'll use Terraform to automatically connect your BIG-IP to the targeted Virtual WAN environment.

## TOPOLOGY USED IN THIS DEPLOYMENT GUIDE



**Figure 1:** The diagram above illustrates an Azure Virtual WAN with two hubs and a remote site.

In the diagram above, we highlight the following resources:

- **Virtual WAN:** The Virtual WAN resource represents a virtual overlay of the Azure network and is a collection of multiple resources. It contains links to all your virtual hubs that you would like to have within the Virtual WAN. Virtual WAN resources are isolated from each other and cannot contain a common hub. Virtual hubs across Virtual WAN do not communicate with each other
- **Hub:** A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity. From your on-premises network (VPN site), you can connect to a VPN Gateway inside the virtual hub. Multiple virtual hubs can be created in the same region.
- **Hub-to-hub connection:** Hubs are all connected to each other in a Virtual WAN. This implies that a branch, user, or VNet connected to a local hub can communicate with another branch or VNet using the full mesh architecture of the connected hubs.
- **IPsec connectivity or site:** This resource is used for site-to-site connections only. The site resource is a VPN site. It represents your on-premises VPN device and its settings. By working with a Virtual WAN partner, you have a built-in solution to automatically export this information to Azure. You can connect to your resources on Azure over a site-to-site IPsec/IKE (IKEv2) connection. This is what we'll use with the F5 BIG-IP platform.

This deployment guide shows how to create and configure a Virtual WAN and connect to a remote site in Europe.

## PREREQUISITES

In this deployment guide, we'll consider the following have already been set up:

- Virtual networks and Ubuntu instances (or something else). We consider that you've already created the following resources:
  - Virtual networks in US EAST and West Europe (10.5.0.0/24 and 10.6.0.0/24 respectively).
  - Instances leveraging those VNets and hosted in US EAST and West Europe.
- Remote site. We consider that your remote site is already set up.
  - BIG-IP is set up and licensed.
  - You have one instance that can be used to test connectivity with resources hosted on Azure.
- Terraform is already set up to have access to your Azure environment. If you need assistance on this, please refer to this link: [https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/guides/service\\_principal\\_client\\_secret](https://registry.terraform.io/providers/hashicorp/azurerm/latest/docs/guides/service_principal_client_secret).

## Deployment Guide

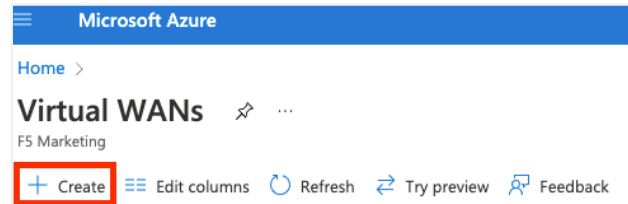
This is a summary of the steps covered in this deployment guide:

Step	Task	Description
1	Azure Virtual WAN Setup	Set up an Azure Virtual WAN resource on Azure that will host your hubs and be used to establish connectivity between hubs
2	Azure Hubs Setup	Set up two hubs tied to your Virtual WAN resource. One hub in US EAST and one hub in West Europe

## AZURE VIRTUAL WAN SETUP

Connect to your Azure portal via <https://portal.azure.com/>. Once connected, go to **Virtual WANs**, select **+Create** to open the **Create WAN** page.

Virtual WANs, + Create



You'll need to specify the following information:

### Project details

- Subscription: Select the relevant subscription
- Resource group: Specify if you want to use a new Resource group or an existing one.

### Virtual WAN details

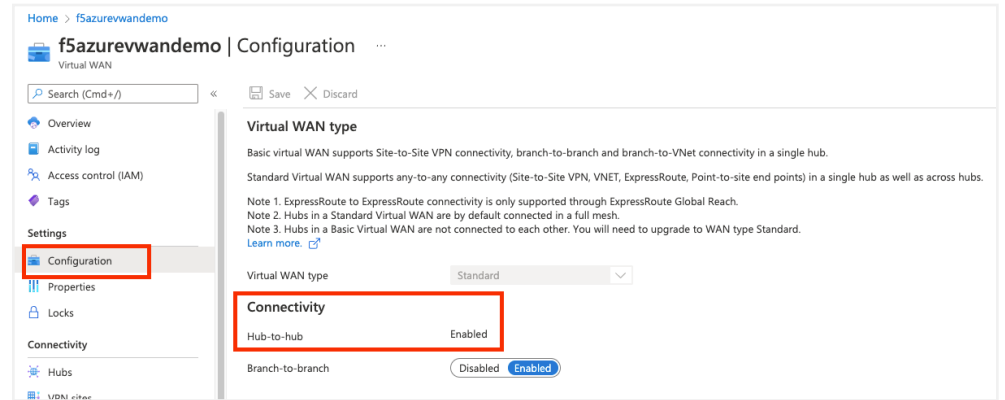
- Resource group location: we will use East US2
- Name: we will use f5azurevwandemo
- Type: Select **Standard**. This is required for the topology. If you want hub to hub connectivity, you need to select Standard.

Create WAN, Basics

A screenshot of the 'Create WAN' page in the Azure portal. The page has a title 'Create WAN' with a menu icon. Below the title, there are two tabs: 'Basics' (selected) and 'Review + create'. A descriptive text states: 'The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. [Learn more](#)'. The form is divided into two sections. The 'Project details' section contains two dropdown menus: 'Subscription \*' with the value 'f5-AZR\_5603\_MKTG\_AOTeam' and 'Resource group \*' with the value '(New) f5azurevwandemo-rg'. There is a 'Create new' link below the resource group dropdown. The 'Virtual WAN details' section contains three dropdown menus: 'Resource group location \*' with the value 'East US 2', 'Name \*' with the value 'f5azurevwandemo' (marked with a green checkmark), and 'Type' with the value 'Standard'.

## Virtual WAN, Configuration

Once your Virtual WAN is created, you can make sure connectivity is setup as expected. Navigate to **Virtual WAN** resource, select **Configuration** and review your connectivity. Confirm that **hub-to-hub** connectivity is enabled.



## AZURE HUBS SETUP

On the Virtual WAN page in the Azure portal, create two hubs:

Name	Region	Address Space	Site to Site	Point to Site	ExpressRoute
vhub-USEAST	East US	10.200.0.0/24	Disabled	Disabled	Disabled
vhub-EUW	West Europe	10.201.0.0/24	Enabled	Disabled	Disabled

## US EAST Hub Setup

In the Azure portal, on the **Virtual WAN** page, select **Hubs** and choose **+New Hub** to open the **Create virtual hub** page.

On the **Create virtual hub** page **Basics** tab, use the following configuration for vhub-USEAST.

## Create virtual hub, Basics (US East)

**Basics**
Site to site
Point to site
ExpressRoute
Tags
Review + create

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). [Learn more](#)

**Project details**

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

Subscription: f5-AZR\_5603\_MKTG\_AOTeam

Resource group: f5azurevwandemo

**Virtual Hub Details**

Region \*: East US

Name \*: vhub-USEAST

Hub private address space \*: 10.200.0.0/24

On the **Site to site** tab, select the following:

---

#### Create virtual hub, Site to site

---

Basics **Site to site** Point to site ExpressRoute Tags Review + create

You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Site to site (VPN gateway)?

Yes

No

On the **Point to site** tab, select the following:

---

#### Create virtual hub, Point to site

---

Basics Site to site **Point to site** ExpressRoute Tags Review + create

If you plan to use this hub with Point-to-site connections, you will need to enable Point-to-site gateway before connecting end-user devices. You can do this after hub creation, but doing now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Point to site (User VPN gateway)?

Yes

No

---

#### Create virtual hub, ExpressRoute

---

Basics Site to site Point to site **ExpressRoute** Tags Review + create

If you plan to use this hub with ExpressRoutes, you will need to enable an ExpressRoute gateway before connecting to ExpressRoute circuits. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create an ExpressRoute gateway? ⓘ

Yes

No

Select **Review + create** to validate. Once validation passes, select **Create**.

Create virtual hub, Review + create

✔ Validation passed

Basics

Site to site

Point to site

ExpressRoute

Tags

Review + create

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

Basics

Region

East US

Name

vhub-USEAST

Hub private address space

10.200.0.0/24

Site to site

Site to site (VPN gateway)

Disabled

Point to site

Point to site (VPN gateway)

Disabled

ExpressRoute

ExpressRoute gateway

Disabled

i

Creating a hub with a gateway will take 30 minutes.

Create

Previous

Next

Download a template for automation

## WEST Europe Hub Setup

Create another hub for West Europe and enable site-to-site connectivity (this is the hub that will be used by the remote site to establish IPsec connectivity).

Choose + **New Hub** to open the **Create virtual hub** page.

### Create virtual hub, Basics (West Europe)

**Basics** Site to site Point to site ExpressRoute Tags Review + create

A virtual hub is a Microsoft-managed virtual network. The hub contains various service endpoints to enable connectivity from your on-premises network (vpnsite). [Learn more](#)

**Project details**

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

Subscription f5-AZR\_5603\_MKTG\_AOTeam

Resource group f5azurevwandemo

**Virtual Hub Details**

Region \* West Europe

Name \* vhub-EUW

Hub private address space \* 10.201.0.0/24

On the **Site to site** tab, select **Yes** to enable the VPN Gateway. Since this is a lab environment, we will set up the Gateway with a **1 scale unit**.

### Create virtual hub, Site to site

**Basics** **Site to site** Point to site ExpressRoute Tags Review + create

You will need to enable Site to site (VPN gateway) before connecting to VPN sites. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Site to site (VPN gateway)? **Yes** No

AS Number 65515

\*Gateway scale units 1 scale unit - 500 Mbps x 2

Routing preference ☐ Microsoft network ☒ Internet



Note: We won't be using **Point to site** or **ExpressRoute** for this hub.

**Basics** Site to site **Point to site** ExpressRoute Tags Review + create

If you plan to use this hub with Point-to-site connections, you will need to enable Point-to-site gateway before connecting end-user devices. You can do this after hub creation, but doing now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create a Point to site (User VPN gateway)? Yes **No**

**Basics** Site to site Point to site **ExpressRoute** Tags Review + create

If you plan to use this hub with ExpressRoutes, you will need to enable an ExpressRoute gateway before connecting to ExpressRoute circuits. You can do this after hub creation, but doing it now will save time and reduce the risk of service interruptions later. [Learn more](#)

Do you want to create an ExpressRoute gateway? Yes **No**

Select **Review + Create** to validate. Once validation passes, select **Create**.

Create virtual hub, Review + create

**Validation passed**

**Basics** Site to site Point to site ExpressRoute Tags **Review + create**

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

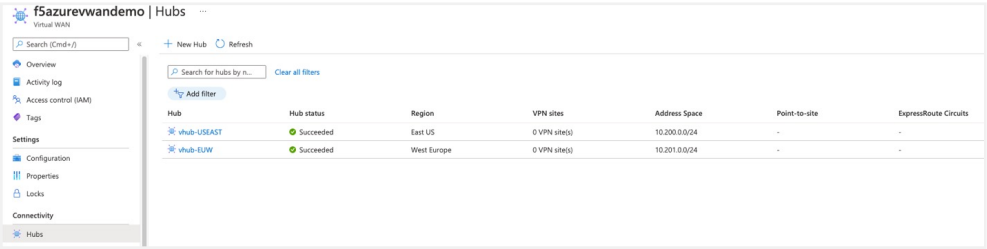
<b>Basics</b>	
Region	West Europe
Name	vhub-EUW
Hub private address space	10.201.0.0/24
<b>Site to site</b>	
Site to site (VPN gateway)	Enabled
AS Number	65515
Gateway scale units	1 scale unit - 500 Mbps x 2
<b>Point to site</b>	
Point to site (VPN gateway)	Disabled
<b>ExpressRoute</b>	

**i** Creating a hub with a gateway will take 30 minutes.

**Create** Previous Next [Download a template for automation](#)

Virtual WAN, Hubs

Your **Hubs** page should look as follows:



Hub	Hub status	Region	VPN sites	Address Space	Point-to-site	ExpressRoute Circuits
vhub-USEAST	Succeeded	East US	0 VPN site(s)	10.200.0.0/24	-	-
vhub-EUW	Succeeded	West Europe	0 VPN site(s)	10.201.0.0/24	-	-

Next, you'll attach the virtual subnets to the hubs.

VIRTUAL NETWORK CONNECTIONS SETUP

In this deployment guide, we consider that you have already created resources to attach to your US EAST and West Europe hubs.

To support this deployment guide, we've created the following resources:

US EAST

- Resource Group: f5demo-vwan-RG-USEAST
- Virtual network: subnet-vwandemo-useast  
Subnet: 10.5.0.0/16
- One Ubuntu instance for testing  
IP: 10.5.0.4

West Europe

- Resource Group: f5demo-vwan-RG-EUW
- Virtual network: subnet-vwandemo-euw  
Subnet: 10.6.0.0/16
- One Ubuntu instance for testing  
IP: 10.6.0.4

In this section, you'll create a connection between the VNet and your hubs.

Go to your **Virtual WAN**. On the **Virtual network connections** page, click **+Add connection**.

This is the setup to attach **subnet-vwandemo-euw** to the hub called **vhub-EUW**. Don't change the default routing configuration.

Virtual WAN, Virtual network connections, +Add connection (vhub-EUW)

### Add connection

Connection name \*

ConnectionvhubEUW

Hubs \* ⓘ

vhub-EUW

Subscription \*

f5-AZR\_5603\_MKTG\_AOTeam

Resource group \*

f5demo-vwan-RG-EUW

Virtual network \*

subnet-vwandemo-euw

Routing configuration ⓘ

Propagate to none

Yes No

Associate Route Table

Propagate to Route Tables

0 selected

Propagate to labels ⓘ

0 selected

Static routes ⓘ

Route name	Destination prefix	Next hop IP

Create

And, this is the setup to attach **subnet-vwandemo-useast** to the hub called **vhub-USEAST**. Don't change the default routing configuration.

Virtual WAN, Virtual network connections, +Add connection (vhub-USEAST)

### Add connection

Connection name \*

ConnectionvhubUSEAST

Hubs \* ⓘ

vhub-USEAST

Subscription \*

f5-AZR\_5603\_MKTG\_AOTeam

Resource group \*

f5demo-vwan-RG-USEAST

Virtual network \*

subnet-vwandemo-useast

Routing configuration ⓘ

Propagate to none

Yes No

Associate Route Table

Propagate to Route Tables

0 selected

Propagate to labels ⓘ

0 selected

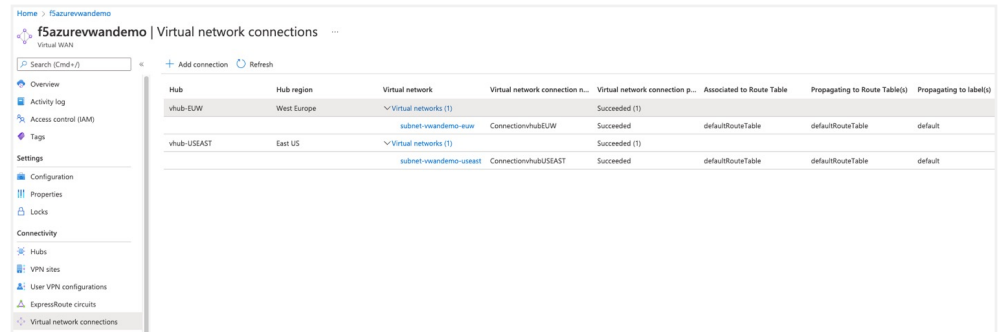
Static routes ⓘ

Route name	Destination prefix	Next hop IP

Create

Below is an overview of what we created:

## Virtual WAN, Virtual network connections



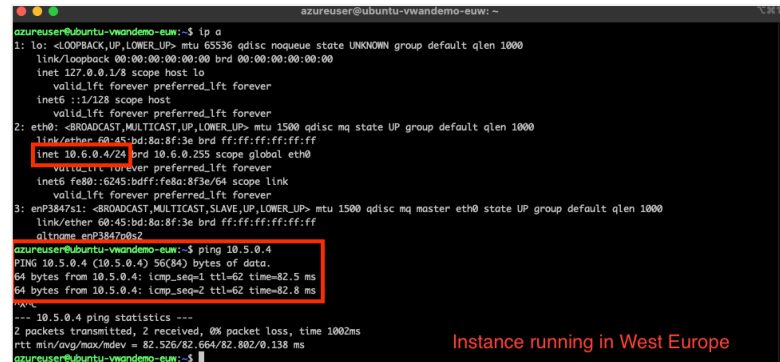
The screenshot shows the Azure portal interface for 'f5azurevwdemo' under 'Virtual network connections'. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Settings, Configuration, Properties, Locks, and Connectivity. The main area displays a table of virtual network connections.

Hub	Hub region	Virtual network	Virtual network connection name	Virtual network connection status	Associated to Route Table	Propagating to Route Table(s)	Propagating to label(s)
vhub-EUW	West Europe	Virtual networks (1)		Succeeded (1)			
		subnet-vwdemo-euw	ConnectionhubEUW	Succeeded	defaultRouteTable	defaultRouteTable	default
vhub-USEAST	East US	Virtual networks (1)		Succeeded (1)			
		subnet-vwdemo-useast	ConnectionhubUSEAST	Succeeded	defaultRouteTable	defaultRouteTable	default

Now the instances hosted in the virtual networks can communicate with each other.

Below is an example connectivity test from the instance in US EAST to the instance in West Europe:

## Instance running in West Europe



The terminal shows the network configuration for an instance in West Europe. The IP address 10.5.0.4 is highlighted. A ping test is performed to 10.5.0.4, showing successful connectivity with 0% packet loss.

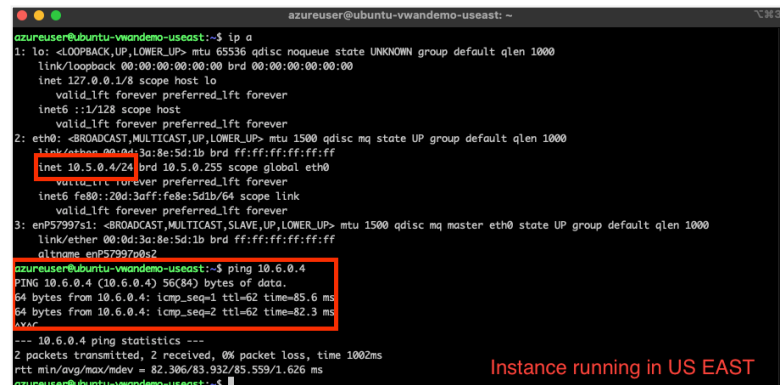
```
azureuser@ubuntu-vwdemo-euw:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 60:45:bd:8a:8f:3e brd ff:ff:ff:ff:ff:ff
    inet 10.5.0.4/24 brd 10.5.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::6245:bdf:fe8a:8f3e/64 scope link
        valid_lft forever preferred_lft forever
3: enp3847s1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc mq master eth0 state UP group default qlen 1000
    link/ether 60:45:bd:8a:8f:3e brd ff:ff:ff:ff:ff:ff
    altname enp3847o0s2

azureuser@ubuntu-vwdemo-euw:~$ ping 10.5.0.4
PING 10.5.0.4 (10.5.0.4) 56(84) bytes of data.
64 bytes from 10.5.0.4: icmp_seq=1 ttl=62 time=82.5 ms
64 bytes from 10.5.0.4: icmp_seq=2 ttl=62 time=82.8 ms
---
--- 10.5.0.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 82.526/82.664/82.802/0.138 ms
```

Instance running in West Europe

Below is an example connectivity test from the instance in West Europe to the instance in US EAST:

## Instance running in US EAST



The terminal shows the network configuration for an instance in US East. The IP address 10.6.0.4 is highlighted. A ping test is performed to 10.6.0.4, showing successful connectivity with 0% packet loss.

```
azureuser@ubuntu-vwdemo-useast:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0d:3a:8e:5d:1b brd ff:ff:ff:ff:ff:ff
    inet 10.6.0.4/24 brd 10.5.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20d:3aff:fe8e:5d1b/64 scope link
        valid_lft forever preferred_lft forever
3: enp5797s1: <BROADCAST,MULTICAST,SLAVE,UP,LOWER_UP> mtu 1500 qdisc mq master eth0 state UP group default qlen 1000
    link/ether 00:0d:3a:8e:5d:1b brd ff:ff:ff:ff:ff:ff
    altname enp5797o0s2

azureuser@ubuntu-vwdemo-useast:~$ ping 10.6.0.4
PING 10.6.0.4 (10.6.0.4) 56(84) bytes of data.
64 bytes from 10.6.0.4: icmp_seq=1 ttl=62 time=85.6 ms
64 bytes from 10.6.0.4: icmp_seq=2 ttl=62 time=82.3 ms
---
--- 10.6.0.4 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 82.386/83.932/85.559/1.626 ms
```

Instance running in US EAST

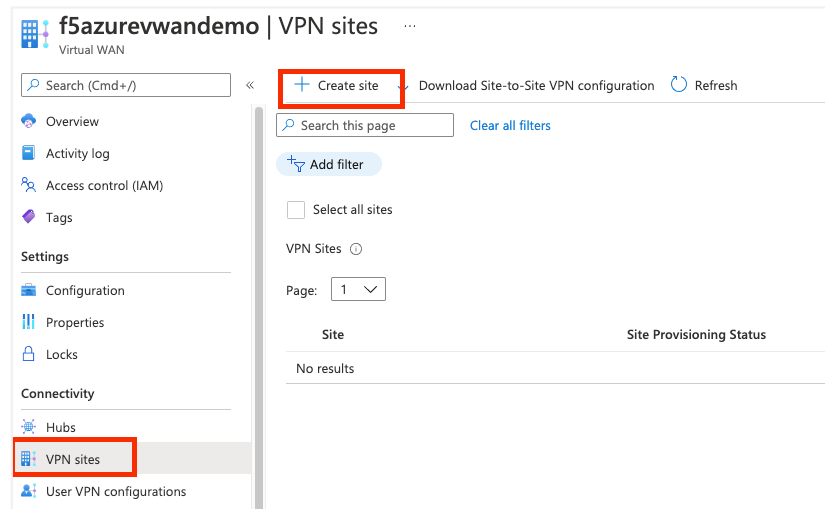
The instances can successfully communicate with each other. The next step will be to set up the VPN site to allow IPsec connectivity from the remote site.

## VPN SITE SETUP

We need to provide information related to the remote office to ensure IPsec connectivity. To do so, navigate to your **Virtual WAN**, select **VPN sites** and click **+Create site**.

Here you'll provide the topology information of your remote site:

Virtual WAN, VPN sites, +Create site



- Remote Site's region: West Europe
- Remote Site name: ParisOffice
- Device vendor: F5 BIG-IP
- Subnet(s): 10.100.10.0/24
- Link information:
  - Public IP is 13.38.18.23
  - Capacity: 10 (Mbps)
  - Link Provider Name: MyISPProvider

Create site, Basics

Create site, Links

Confirm your configuration passes validation, then select **Create**.

Create VPN site, Review + create

Create VPN site ...

✓ Validation passed

Basics

Links

Review + create

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

Basics

Region

West Europe

Name

ParisOffice

Device vendor

F5 BIG-IP

Private address space

10.100.10.0/24

Links

Link name

ISPLink

Link provider name

MyISPProvider

Link speed

10

Link IP address / FQDN

13.38.18.23

i

You can also work with a Virtual WAN partner to create multiple sites simultaneously. [Learn more.](#)

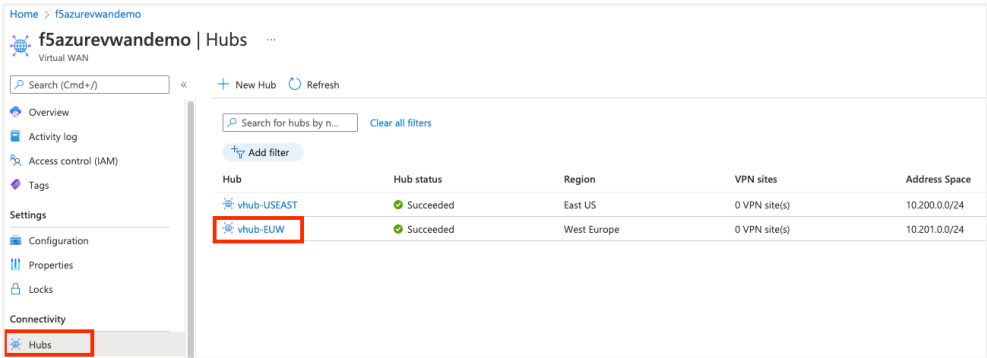
Create

Previous

Next

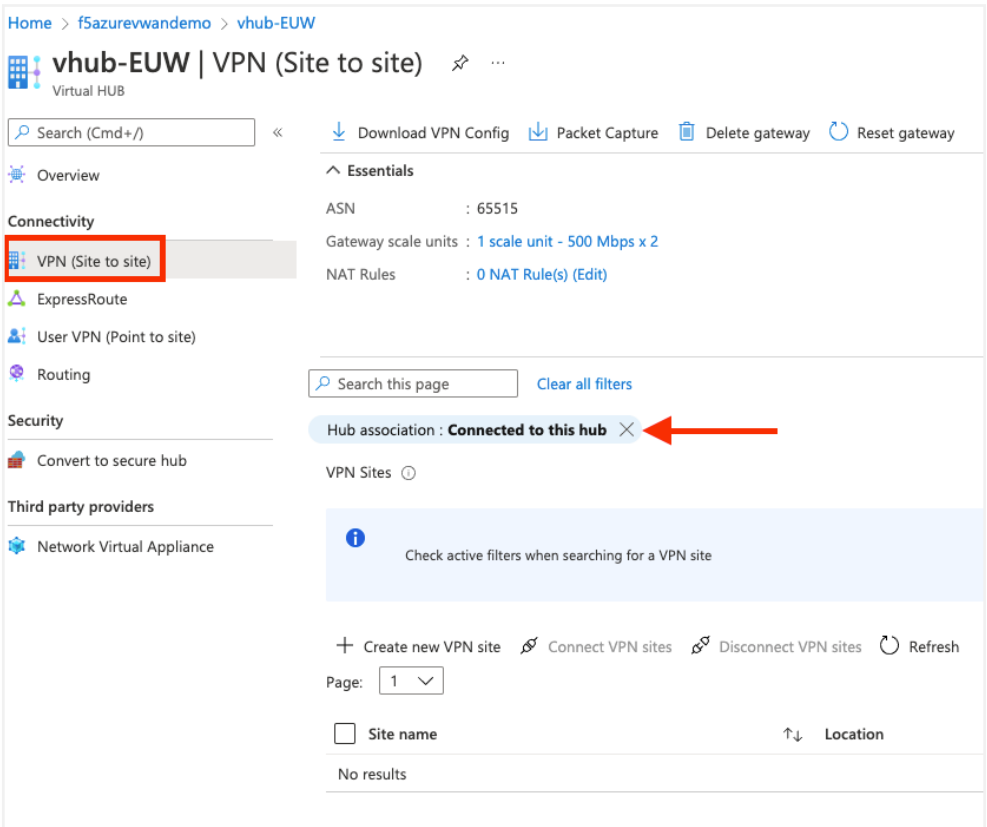
Once the VPN site is setup, you'll need to connect it to your hub. Go to your **Virtual WAN**, select **Hubs**, and choose **vhub-EUW**.

Virtual WAN, Hubs



Once in the **vhub-EUW** resource, choose **VPN (Site to site)**, and click the **X** in the **Hub association**: bubble to clear the filter. Once the filter has cleared, you can view your site. If you don't do this, you will not see the ParisOffice site.

Virtual HUB, VPN (Site to site)





Once the **ParisOffice** site is visible, select the checkbox next to the name of the site (don't click on the site name directly), then click **Connect VPN sites**.

#### Virtual HUB, VPN (Site to site), Connect VPN sites

The screenshot shows the Azure Virtual WAN portal for 'vhub-EUW | VPN (Site to site)'. The left sidebar contains navigation options: Overview, Connectivity (selected), ExpressRoute, User VPN (Point to site), Routing, Security, Convert to secure hub, Third party providers, and Network Virtual Appliance. The main area displays VPN site details: ASN (65515), Gateway scale units (1 scale unit - 500 Mbps x 2), and NAT Rules (0 NAT Rule(s) (Edit)). Below this is a search bar and a list of VPN sites. A red arrow points to the 'Connect VPN sites' button in the action bar. The table below shows one site, 'ParisOffice', with a checkbox selected and the location 'westeurope'.

Site name	Location
<input checked="" type="checkbox"/> ParisOffice	westeurope

Leave all the settings as-is and select **Connect** at the bottom of the page.

#### Virtual HUB, Connect sites

The screenshot shows the 'Connect sites' page for 'Virtual HUB'. It contains security settings for the connection: Pre-shared key (PSK), Protocol (IKEv2), IPsec (Default), Propagate Default Route (Disable), Use policy based traffic selector (Disable), and Configure traffic selector? (No). Below these settings, it states 'These sites will be connected to the [vhub-EUW] hub.' and shows a table with the 'ParisOffice' site in the 'westeurope' region. At the bottom, the 'Connect' button is highlighted with a red box.

Site name	Region
ParisOffice	westeurope

If you navigate back to the **Hubs** page in your **Virtual WAN**, you should see that one VPN site is tied to the **vhub-EUW** hub.

Virtual WAN, Hubs

Home > fsazurevwandemo

fsazurevwandemo | Hubs

Virtual WAN

Search (Cmd+J)

+ New Hub Refresh

Search for hubs by nar Clear all filters

Add filter

Hub	Hub status	Region	VPN sites	Address Space
vhub-USEAST	Succeeded	East US	0 VPN site(s)	10.200.0.0/24
vhub-EUW	Succeeded	West Europe	1 VPN site(s)	10.201.0.0/24

F5 BIG-IP SETUP

Retrieve F5 Terraform module for Azure Virtual WAN integration.

The Virtual WAN Terraform module can be located here: <https://github.com/F5Devcentral/bigip-vwan-module>.

Retrieve the repository on your Terraform system. Use git clone to clone the repository.

Note: If you intend to customize the solution, it would be better to fork the project into your repository and clone it.

Retrieve vWAN Terraform module

```
co@~/projects/tmp % git clone git@github.com:F5Devcentral/bigip-vwan-module.git
Cloning into 'bigip-vwan-module'...
remote: Enumerating objects: 79, done.
remote: Counting objects: 100% (79/79), done.
remote: Compressing objects: 100% (58/58), done.
remote: Total 79 (delta 30), reused 56 (delta 14), pack-reused 0
Receiving objects: 100% (79/79), 12.07 MiB | 1.91 MiB/s, done.
Resolving deltas: 100% (30/30), done.
```

Once you've imported the module into your system, you can set it up to automate the BIG-IP configuration based on your Virtual WAN setup.

F5 Terraform Module Setup

To set up the Terraform module, you need to update the following files:

- bigip-vwan-module/examples/main.tf
- bigip-vwan-module/examples/terraform.tfvars

---

## BIG-IP Provider definition

---

Use your favorite editor to update main.tf. In this file, update the “bigip” provider section to define access to your BIG-IP:

```
bigip-vwan-module > examples > main.tf
1
2 provider "bigip"
3   address = "xx.xxx.x.x"
4   port    = "443"
5   username = "admin"
6   password = "xxxxx"
7
8
9 module vwan {
10   source = "../"
11   azure_vwan_resourcegroup = var.azure_vwan_resourcegroup
12   azure_vwan_name          = var.azure_vwan_name
13   azure_vwan_vpnsite       = var.azure_vwan_vpnsite
14   bigip_local_ip_tunnel    = var.bigip_local_ip_tunnel
15   bigip_tunnel_selfip      = var.bigip_tunnel_selfip
16 }
```

Note: If you intend to tune the GitHub repository and Push your changes on GitHub, you should NOT send this updated file for security reason.

Next, you'll need to update terraform.tfvars. Provide the following information into this file:

- **azure\_vwan\_resourcegroup**: name of the Virtual WAN resource group you created. In this guide, it is **f5azurevwandemo**.
- **azure\_vwan\_name**: name of the Virtual WAN resource. In this guide, it is **f5azurevwandemo**.
- **azure\_vwan\_vpnsite**: name of the VPN site created for the remote office, **ParisOffice**.
- **bigip\_tunnel\_selfip**: the IP address you want BIG-IP to use within the IPsec tunnel. Since the VPN site is tied to the hub **vHub-EUW** (setup with a subnet of 10.201.0.0/24), we need to choose an IP within this subnet **10.201.0.37/24**.
- **bigip\_local\_ip\_tunnel**: the IP address of the BIG-IP that will be used to establish the IPsec tunnel **10.100.10.114**.

---

## Terraform module input parameters

---

```
bigip-vwan-module > examples > terraform.tfvars
1 azure_vwan_resourcegroup = "f5azurevwandemo"
2 azure_vwan_name          = "f5azurevwandemo"
3 azure_vwan_vpnsite       = "ParisOffice"
4 ##
5 ## We need to be able to specify:
6 ## - The Local address for the tunnel. In my situation it is the self IP that already exist
7 ## - The Public IP for the branch office that is used to establish the IPSEC tunnel
8 ## The only SelfIP We should create is the one part of the tunnel since it cannot be created before the tunnel is setup. All
9 ## the other SelfIPs should be created before using this solution
10
11 ##
12 ## This tunnel_selfip should be created
13 ##
14 bigip_tunnel_selfip      = "10.201.0.37/24"
15
16 ##
17 ## We should not try to create the next IP. This is for reference so that we can use it in our tunnel definition
18 ##
19 bigip_local_ip_tunnel    = "10.100.10.114"
```

---

#### Initialize Terraform working directory

---

The final step is to initialize Terraform within the repo. Get into the folder **bigip-vwan-module/examples** and run “**terraform init**”. You should see something like this:

```
Nico@~/projects/tmp/bigip-vwan-module/examples % terraform init
Initializing modules...
- vwan in ..

Initializing the backend...

Initializing provider plugins...
- Finding latest version of terraform-providers/bigip...
- Finding latest version of hashicorp/random...
- Installing terraform-providers/bigip v1.11.0...
- Installed terraform-providers/bigip v1.11.0 (signed by HashiCorp)
- Installing hashicorp/random v3.1.0...
- Installed hashicorp/random v3.1.0 (signed by HashiCorp)

Terraform has created a lock file .terraform.lock.hcl to record the provider
selections it made above. Include this file in your version control repository
so that Terraform can guarantee to make the same selections by default when
you run "terraform init" in the future.

Warning: Provider development overrides are in effect

The following provider development overrides are set in the CLI configuration:
- terraform-providers/bigip in /Users/N.Menant/projects/tests/test-terraform/terraform-provider-bigip-binary

Skip terraform init when using provider development overrides. It is not necessary and may error unexpectedly.

Warning: Additional provider information from registry

The remote registry returned warnings for registry.terraform.io/terraform-providers/bigip:
- For users on Terraform 0.13 or greater, this provider has moved to F5Networks/bigip. Please update your source in
required_providers.

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
```

## Execute Terraform Module

Now that everything is setup, we can execute the solution to connect BIG-IP to the Azure Virtual WAN via IPsec.

To start the BIG-IP IPsec configuration, run the following command in your **bigip-vwan-module/examples** folder:

**terraform apply --auto-approve**

The following will take place:

1. Recovery of the expected VPN configuration (retrieved from Azure)
2. Analysis of the VPN configuration to set up BIG-IP accordingly
3. Creation of all the relevant objects on BIG-IP:
  - a. Creation of the IPsec policy
  - b. Creation of the IPsec tunnel
  - c. Creation of a forwarding VS to send traffic through the tunnel
  - d. Creation of routes to identify which subnets should be routed through the tunnel

**Note:** To retrieve the configuration, the process requires you to:

1. Push the VPN config in an Azure blob
2. Download the configuration from the blob

This process takes time. If you try to do consecutive Terraform plan and apply, you may receive the following error message:

---

Error message when triggering consecutive deployments

---

```
Error: => github.com/Azure/azure-storage-blob-go/azblob.NewStorageError, /Users/chinthalapalli/go/src/github.com/terraform-providers/terraform-provider-bigip/vendor/github.com/Azure/azure-storage-blob-go/azblob/zc_storage_error.go:42
===== RESPONSE ERROR (ServiceCode=ContainerBeingDeleted) =====
Description=The specified container is being deleted. Try operation later.
RequestId:6c42b3db-301e-0055-4c15-f8cbb4000000
Time:2021-12-23T15:57:50.4182696Z, Details:
  Code: ContainerBeingDeleted
  PUT https://f5storagevwdemo.blob.core.windows.net/myvpnsiteconfig?restype=container&timeout=61
  Authorization: REDACTED
  User-Agent: [Azure-Storage/0.13 (go1.16.3; darwin)]
  X-Ms-Client-Request-Id: [72fa0491-b096-4f34-4c23-ed364838b88c]
  X-Ms-Date: [Thu, 23 Dec 2021 15:57:50 GMT]
  X-Ms-Version: [2019-12-12]
  -----
  RESPONSE Status: 409 The specified container is being deleted. Try operation later.
  Content-Length: [252]
  Content-Type: [application/xml]
  Date: [Thu, 23 Dec 2021 15:57:49 GMT]
  Server: [Windows-Azure-Blob/1.0 Microsoft-HTTPAPI/2.0]
  X-Ms-Client-Request-Id: [72fa0491-b096-4f34-4c23-ed364838b88c]
  X-Ms-Error-Code: [ContainerBeingDeleted]
  X-Ms-Request-Id: [6c42b3db-301e-0055-4c15-f8cbb4000000]
  X-Ms-Version: [2019-12-12]

with module.vwan.data.bigip_vwan_config.vwanconfig,
on ../main.tf line 2, in data "bigip_vwan_config" "vwanconfig":
  2: data bigip_vwan_config vwanconfig {
```

If this happens, wait a few seconds, and try again.

The Terraform output should appear as follows:

Successful Terraform execution

```
Plan: 11 to add, 0 to change, 0 to destroy.
module.vwan.random_id.module_id: Creating...
module.vwan.random_id.module_id: Creation complete after 0s [id=Xng]
module.vwan.bigip_ipsec_policy.ipsec2azure_IPsec_policy: Creating...
module.vwan.bigip_ltm_virtual_server.forwarding_vs: Creating...
module.vwan.bigip_ipsec_policy.ipsec2azure_IPsec_policy: Creation complete after 1s [id=/Common/ipsec2azure_ipsecpolicy_5e78]
module.vwan.bigip_traffic_selector.azureVMAN_Trafficselector: Creating...
module.vwan.bigip_traffic_selector.azureVMAN_Trafficselector: Creation complete after 0s [id=/Common/ipsec2azure_trafficselector_5e78]
module.vwan.bigip_ipsec_profile.ipsec2azure_Profile: Creating...
module.vwan.bigip_net_ike_peer.ikepeer: Creating...
module.vwan.bigip_ipsec_profile.ipsec2azure_Profile: Creation complete after 1s [id=/Common/ipsec2azure_profile_5e78]
module.vwan.bigip_net_ike_peer.ikepeer: Creation complete after 1s [id=/Common/ipsec2azure_ikepeer_5e78]
module.vwan.bigip_net_tunnel.ipsec2azure_Tunnel: Creating...
module.vwan.bigip_net_tunnel.ipsec2azure_Tunnel: Creation complete after 1s [id=/Common/ipsec2azure_tunnel_5e78]
module.vwan.bigip_net_selfip_tunnel_self: Creating...
module.vwan.bigip_ltm_virtual_server.forwarding_vs: Creation complete after 3s [id=/Common/ipsec2azure_vsforward]
module.vwan.bigip_net_route.route[0]: Creating...
module.vwan.bigip_net_route.route[1]: Creating...
module.vwan.bigip_net_route.route[2]: Creating...
module.vwan.bigip_net_route.route[0]: Creation complete after 0s [id=/Common/ipsec2azure_route_0]
module.vwan.bigip_net_route.route[2]: Creation complete after 0s [id=/Common/ipsec2azure_route_2]
module.vwan.bigip_net_route.route[1]: Creation complete after 0s [id=/Common/ipsec2azure_route_1]

Apply complete! Resources: 11 added, 0 changed, 0 destroyed.
Nico@~/projects/tests/test-terraform/F5DemoAzureVMAN/bigip-vwan-module/examples %
```

Review your BIG-IP configuration.

IPsec Policy Configuration:

IPsec: IKE Peers

Network » IPsec : IKE Peers

⚙️

IKE Peer List

IPsec Policy List

Traffic Selector List

Manual Security Association List

Diagnostics

IKE Daemon

Create...

<input checked="" type="checkbox"/>	Name	Description	Address	Mode	Partition / Path
<input checked="" type="checkbox"/>	anonymous		Any		Common
<input type="checkbox"/>	ipsec2azure_ikepeer_5e78		20.47.118.63		Common

Delete...

IPsec: IPsec Policies

Network » IPsec : IPsec Policies

⚙️

IKE Peer List

IPsec Policy List

Traffic Selector List

Manual Security Association List

Diagnostics

IKE Daemon

Create...

<input checked="" type="checkbox"/>	Name	Description	Mode	Tunnel Local Address	Tunnel Remote Address	Partition / Path
<input checked="" type="checkbox"/>	default-ipsec-policy		Transport			Common
<input checked="" type="checkbox"/>	default-ipsec-policy-interface		IPsec Interface			Common
<input type="checkbox"/>	ipsec2azure_ipsecpolicy_5e78	IPSec policy	IPsec Interface			Common

Delete...

## IPsec Policy Configuration: ( Continued)

IPsec: Traffic Selectors

Network » IPsec : Traffic Selectors » ipsec2azure\_trafficselector\_5e78

⚙️ Properties

**General Properties**

Name	ipsec2azure_trafficselector_5e78
Partition / Path	Common
Description	<input type="text"/>
Order	<input type="text" value="0"/>

Configuration: Basic ▾

Source IP Address or CIDR	<input type="text" value="0.0.0.0/0"/>
Destination IP Address or CIDR	<input type="text" value="0.0.0.0/0"/>
Action	Protect
IPsec Policy Name	+ ipsec2azure_ipsecpolicy_5e78 ▾

Update Delete

## IPsec Tunnel Configuration:

Tunnels: Profiles: IPsec Interface

Network » Tunnels : Profiles : IPsec Interface » ipsec2azure\_profile\_5e78

⚙️ Properties

**General Properties**

Name	ipsec2azure_profile_5e78
Partition / Path	Common
Parent Profile	ipsec ▾
Description	<input type="text"/>

**Settings**

Traffic Selector	ipsec2azure_trafficselector_5e78 ▾
------------------	------------------------------------

Update Delete...

Tunnels: Tunnel List:

Network » Tunnels : Tunnel List » ipsec2azure\_tunnel\_5e78

⚙️

Properties

Configuration

Name	ipsec2azure_tunnel_5e78
Partition / Path	Common
Description	<div></div>
Profile	ipsec2azure_profile_5e78
Local Address	10.100.10.114
Remote Address	20.47.118.63
Mode	Bidirectional
MTU	0
Use PMTU	<input checked="" type="checkbox"/> Enabled
TOS	Preserve
Auto-Last Hop	Default

Update

Delete

Network, Self IPs

Network » Self IPs

⚙️

Self IP List

Search

Create...

<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input type="checkbox"/>	ipsec2azure_tunnelselfip_5e78		10.201.0.37	255.255.255.0	ipsec2azure_tunnel_5e78	traffic-group-local-only	Common
<input type="checkbox"/>	self_1nic		10.100.10.114	255.255.255.0	internal	traffic-group-local-only	Common

Delete...

Virtual Server and Routes Configuration:

Virtual Servers: Virtual Server List

Local Traffic » Virtual Servers : Virtual Server List

⚙️

Virtual Server List

Virtual Address List

Statistics

\*

Search

<input checked="" type="checkbox"/>	Status	Name	Description	Application	Destination	Service Port	Type
<input type="checkbox"/>		ipsec2azure_vsforward			Any IPv4	0 (Any)	Performance (Layer 4)

Enable

Disable

Delete...

Routes

Network » Routes

⚙️

Route List

<input checked="" type="checkbox"/>	Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource
<input type="checkbox"/>	default		Default IPv4		Partition Default Route Domain	Gateway	10.100.10.1
<input type="checkbox"/>	ipsec2azure_route_0		10.6.0.0	255.255.0.0	Partition Default Route Domain	Tunnel	ipsec2azure_tunnel_5e78
<input type="checkbox"/>	ipsec2azure_route_1		10.200.0.0	255.255.255.0	Partition Default Route Domain	Tunnel	ipsec2azure_tunnel_5e78
<input type="checkbox"/>	ipsec2azure_route_2		10.5.0.0	255.255.0.0	Partition Default Route Domain	Tunnel	ipsec2azure_tunnel_5e78

Delete...



## Validation - Connectivity Test From the Remote Site to Azure Resources

You can now use the resource in the remote site to test connectivity with your Azure resources. As a reminder, we have instances running in US EAST (10.5.0.4) and West Europe (10.6.0.4).

Connectivity tests from our remote site to resources running in different virtual hubs

```
ubuntu@UbuntuClientFrance:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc fq_codel state UP group default qlen 1000
    link/ether 0a:27:fb:94:94:76 brd ff:ff:ff:ff:ff:ff
    inet 10.100.10.80/24 brd 10.100.10.255 scope global dynamic eth0
        valid_lft 2182sec preferred_lft 2182sec
    inet6 fe80::822:fbff:fe94:9476/64 scope link
        valid_lft forever preferred_lft forever
ubuntu@UbuntuClientFrance:~$ ping 10.6.0.4
PING 10.6.0.4 (10.6.0.4) 56(84) bytes of data.
64 bytes from 10.6.0.4: icmp_seq=4 ttl=63 time=16.4 ms
64 bytes from 10.6.0.4: icmp_seq=5 ttl=63 time=16.7 ms
^X^C
--- 10.6.0.4 ping statistics ---
5 packets transmitted, 2 received, 60% packet loss, time 4066ms
rtt min/avg/max/mdev = 16.387/16.562/16.738/0.175 ms
ubuntu@UbuntuClientFrance:~$ ping 10.5.0.4
PING 10.5.0.4 (10.5.0.4) 56(84) bytes of data.
64 bytes from 10.5.0.4: icmp_seq=2 ttl=62 time=98.8 ms
64 bytes from 10.5.0.4: icmp_seq=3 ttl=62 time=98.2 ms
64 bytes from 10.5.0.4: icmp_seq=4 ttl=62 time=98.3 ms
^C
--- 10.5.0.4 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3022ms
rtt min/avg/max/mdev = 98.185/98.425/98.774/0.252 ms
```

Connectivity test to a  
resource running in West  
Europe

Connectivity test to a  
resource running in US  
EAST

To learn more, contact your F5 representative.

