

## How to Configure Automatic Connectivity to Azure Virtual WAN

<https://campus.barracuda.com/doc/17957/>

VPN connections from a CloudGen Firewall to the Azure Virtual WAN hub are provisioned automatically. The automatic configuration provides a robust and redundant connection by introducing two active-active IPsec IKEv2 VPN tunnels for each ISP with the respective BGP setup and fully automated Azure Virtual WAN site creation on Microsoft Azure. All necessary services on the CloudGen Firewall (BGP and VPN) are created and configured automatically. The finished deployment allows for both branch-to-branch and branch-to-cloud connections. If you disable or delete the configuration on your CloudGen Firewall, make sure to delete the resources in Azure as soon as Virtual WAN is no longer needed.



## Before You Begin

- For CC admins to be able to trigger the virtual WAN configuration, cloud integration permissions are required. For the CC admin to be able to see the automatically created services, read permissions for VPN and BGP services are required. The automation service itself is not run in the scope of the CC admin that triggered the connection.
- Create an Azure service principal to allow the firewall to authenticate to the Azure Virtual WAN APIs. For more information, see [How to Create a Service Principal for Azure Virtual WAN](#).
- Verify that Barracuda Online Services can be accessed by the appliance. For more information, see [Best Practice - Hostname List for Barracuda Networks Online Services](#).

Azure Virtual WAN connectivity is not possible with the distributed firewall service.

## Before You Connect a Firewall Hosted in the Public Cloud to Azure Virtual WAN

Before you start with Step 1, configure the following on firewalls hosted in the public cloud:

- The firewall virtual machine must have multiple network interface cards (at least 2). Those network interface cards must be attached to different subnets.
- Each network interface card used for the connection to the Virtual WAN needs its own public IP

address.

- Configure **Direct Internet Access** for each interface used for the connection to the Virtual WAN. See Step 1.

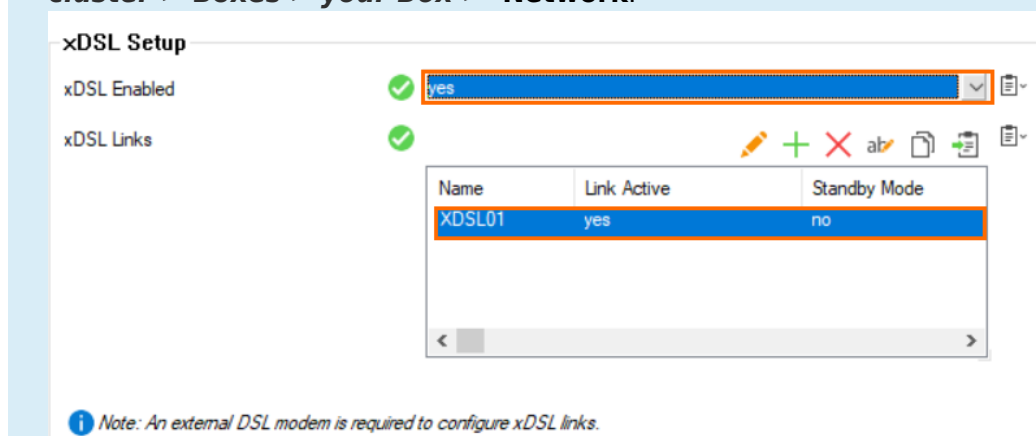
Azure Virtual WAN connectivity is not possible with the distributed firewall service.

## Step 1. Configure WAN Connection

You must have a static IPv4 public IP address. Your links must have similar bandwidth and latency if you want to use more than one ISP. The management interface can not be used as an ISP link port.

1. Configure your ISP. For more information, see [How to Configure an ISP with Static IP Addresses](#), [How to Configure an ISP with Dynamic IP Addresses \(DHCP\)](#), [xDSL WAN Connections](#) or [WAN Connections](#).
2. Verify that the setting **Direct Internet Access** is enabled in your ISP configuration, unless you are using xDSL.

There is no **Direct Internet Access** setting in the xDSL menu. xDSL will automatically be used as an uplink for Microsoft Azure virtual WAN if **xDSL Enabled** is set to **yes** and an xDSL link is configured and active in the **xDSL Links** section. To configure those settings, go to **CONFIGURATION > Configuration Tree > Multi Range > your range > your cluster > Boxes > your Box > Network**.



Name	Link Active	Standby Mode
XDSL01	yes	no

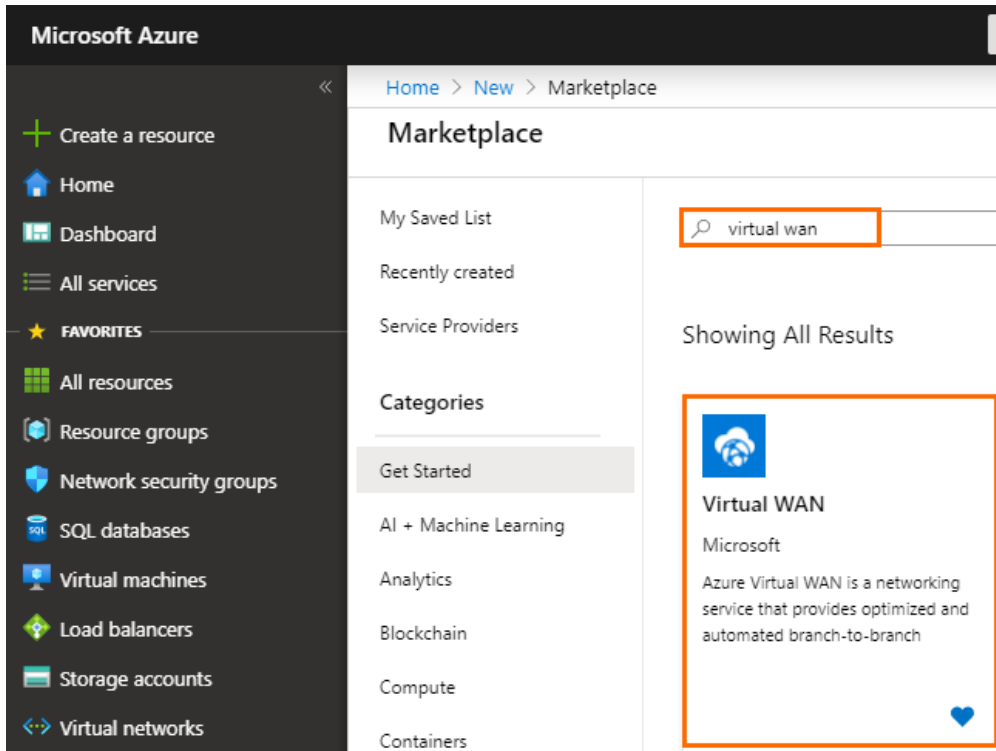
*Note: An external DSL modem is required to configure xDSL links.*

3. Configure direct attached routes to announce the local networks that should have access to cloud resources. For more information, see the **Advertise Route** setting in [How to Configure Directly Attached Routes](#).

## Step 2. Create Virtual WAN Service in Microsoft Azure

1. Log into the Azure portal: <https://portal.azure.com>

2. In the left menu, click **Create a resource** and search for **Virtual WAN**.
3. Click **Virtual WAN**.



4. In the next blade, click **Create**.
5. In the Create WAN blade, specify values for the following:
  - **Resource Group** – Select an existing resource group from the drop-down menu, or create a new one.

The resource group must be the same one as used by the service principal. Otherwise, the firewall will not have sufficient permissions to authenticate to Azure Virtual WAN APIs that enable automated connectivity. For more information, see [How to Create a Service Principal for Azure Virtual WAN](#).
  - **Resource group location** – Select the region of the Virtual WAN, e.g., West Europe .
  - **Name** – Enter a name for your Virtual WAN.
  - **Type** – Select **Standard** if you want to use multiple ISP for the connection of your firewall to Microsoft Azure Virtual WAN or hub-to-hub/routing mesh for peered VNets, or if you want to connect the hubs in Azure. Otherwise, select **Basic**.

Home > New > Marketplace > Virtual WAN > Create WAN

## Create WAN

[Basics](#) [Review + create](#)

The virtual WAN resource represents a virtual overlay of your Azure network and is a collection of multiple resources. [Learn more](#)

**Project details**

Subscription \*

Resource group \*  [Create new](#)

**Virtual WAN details**

Resource group location \*

Name \*

Type

[Review + create](#) [Previous](#) [Next : Review + create >](#)

6. Click **Review + Create**.
7. Click **Create** to finish Virtual WAN creation.

### Step 3. Create a Hub in Your Azure Virtual WAN

Creating a hub takes between 30 and 50 minutes.

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services** and search for **Resource groups**.
3. Click on the resource group your vWAN is attached to. See Step 2.
4. Click on your vWAN created in Step 2.
5. On the left side, click **Hubs**.
6. In the next blade, click **+ New Hub**.

Home > Resource groups > RG-Campus-VWAN > Campus-VWAN - Hubs

## Campus-VWAN - Hubs

Virtual WAN

Search (Ctrl+/) << + New Hub Refresh

Search for hubs by name X Clear all filters

+ Add filter

Hub	Hub status
No results	

**Settings**

- Configuration
- Properties
- Locks
- Export template

**Connectivity**

- Hubs**
- VPN sites
- User VPN configurations
- ExpressRoute circuits
- Virtual network connections

7. The **Create virtual hub** blade opens. Specify values for the following:
- **Region** – Select a region from the drop-down list, e.g., **West Europe** .
  - **Name** – Enter a name for the hub, e.g., doc-vwan-hub .
  - **Hub private address space** - Enter the hub's address range in CIDR, e.g., 10.0.0.0/24. Select a unique network that is dedicated for the hub only.

Home > Resource groups > RG-Campus-VWAN > Campus-VWAN - Hubs > Create virtual hub

## Create virtual hub

[Basics](#) [Site to site](#) [Point to site](#) [ExpressRoute](#) [Routing](#) [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). The hub is the core of your network in a region. There can only be one hub per Azure region. When you create a hub using Azure portal, it creates a virtual hub VNet and a virtual hub vpngateway. [Learn more](#)

### Project details

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

Subscription \*

Resource group \*

### Virtual Hub Details

Region \*

Name \*

Hub private address space \* ⓘ

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

[Review + create](#) [Previous](#) [Next : Site to site >](#)

8. Click **Next: Site to site >**.

9. The **Site to site** blade opens. Specify the values for the following:

- **Do you want to create a Site to site (VPN gateway)** - Select **Yes**.
- **Gateway scale units** - Select a scale unit from the drop-down menu according to your requirements.

Home > Resource groups > RG-Campus-VWAN > Campus-VWAN - Hubs > Create virtual hub

### Create virtual hub

Basics Site to site Point to site ExpressRoute Routing 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 ⓘ

\*Gateway scale units

**Review + create** Previous Next : Point to site >

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

10. Click **Review + create**.

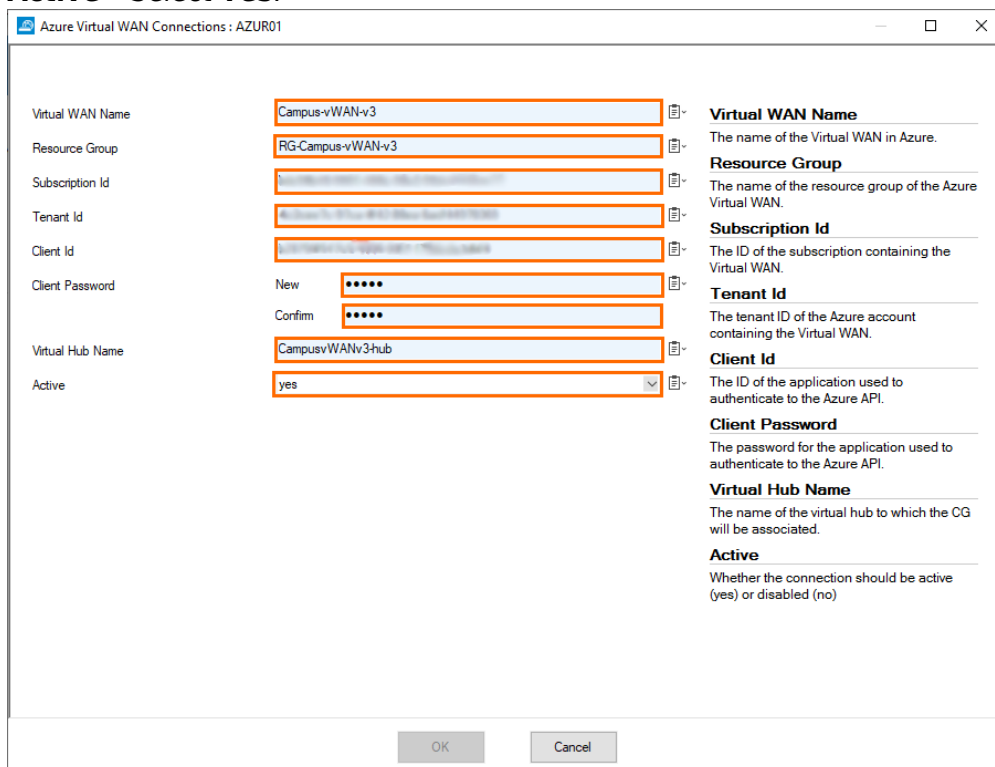
11. Review your settings and click **Create** to start the creation of the hub. This can take up to 30 minutes.

## Step 4. Trigger Virtual WAN connection

1. Log into the CloudGen Firewall with Firewall Admin.
2. Go to **CONFIGURATION > Configuration Tree > Multi Range > your range > your cluster > Boxes > your Box > Advanced Configuration > Cloud Integration**.
3. Select **Azure Virtual WAN** in the left menu.
4. Click **Lock**.
5. In the **Azure Virtual WAN Connections** section, click **+**.
6. Enter a name for your virtual WAN and click **OK**.
7. The **Azure Virtual WAN Connections** window opens. Specify values for the following:
  - **Virtual WAN Name** – Enter the name of the virtual WAN created in Step 2.
  - **Resource Group** – Enter the name of the resource group containing the virtual WAN.



- **Subscription Id** – Enter the ID of the subscription containing the Virtual WAN.
- **Tenant Id** – Enter the tenant ID of the Azure account containing the Virtual WAN.
- **Client Id** – Enter the ID of the application used to authenticate to the Azure API.
- **Client Password New** – Enter the password for the application used to authenticate to the Azure API.
- **Client Password Confirm** – Retype the password for the application used to authenticate to the Azure API.
- **Virtual Hub Name** – Enter the name of the hub created in Step 3.
- **Active** – Select **Yes**.



Virtual WAN Name	Campus-vWAN-v3	<b>Virtual WAN Name</b> The name of the Virtual WAN in Azure.
Resource Group	RG-Campus-vWAN-v3	<b>Resource Group</b> The name of the resource group of the Azure Virtual WAN.
Subscription Id	[redacted]	<b>Subscription Id</b> The ID of the subscription containing the Virtual WAN.
Tenant Id	[redacted]	<b>Tenant Id</b> The tenant ID of the Azure account containing the Virtual WAN.
Client Id	[redacted]	<b>Client Id</b> The ID of the application used to authenticate to the Azure API.
Client Password	New: [redacted] Confirm: [redacted]	<b>Client Password</b> The password for the application used to authenticate to the Azure API.
Virtual Hub Name	CampusvWANv3-hub	<b>Virtual Hub Name</b> The name of the virtual hub to which the CG will be associated.
Active	yes	<b>Active</b> Whether the connection should be active (yes) or disabled (no)

8. Click **OK**
9. Click **Send Changes** and **Activate**.

A VPN site entry is automatically created, and the firewall starts to check for an available configuration every 30 seconds. Wait for the new hub association to complete. The firewall automatically picks up the new configuration and connects to the Virtual WAN.

To change the **Virtual Hub** of an existing Virtual WAN configuration, first disable the Virtual WAN configuration, and then enter the new **Virtual Hub Name**.

## Step 5. Configure Routes to Be Advertised via BGP

---

Only routes with the parameter **Advertise** set to **yes** will be propagated via BGP.

1. Go to **CONFIGURATION > Configuration Tree > Multi Range > your range > your cluster > Boxes > your Box > Network**.
2. Click **Configuration Mode**.
3. Click **Switch to Advanced**.
4. Click **Lock**.
5. (optional) Click **IP Configuration**. In the **Management Networks and IPs** section, set **Advertise Route** to **yes** in order to propagate the management network.
6. In the left menu, click **Advanced Routing**.
7. Double-click on the **Routes** you want to propagate, and set **Advertise Route** to **yes**.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

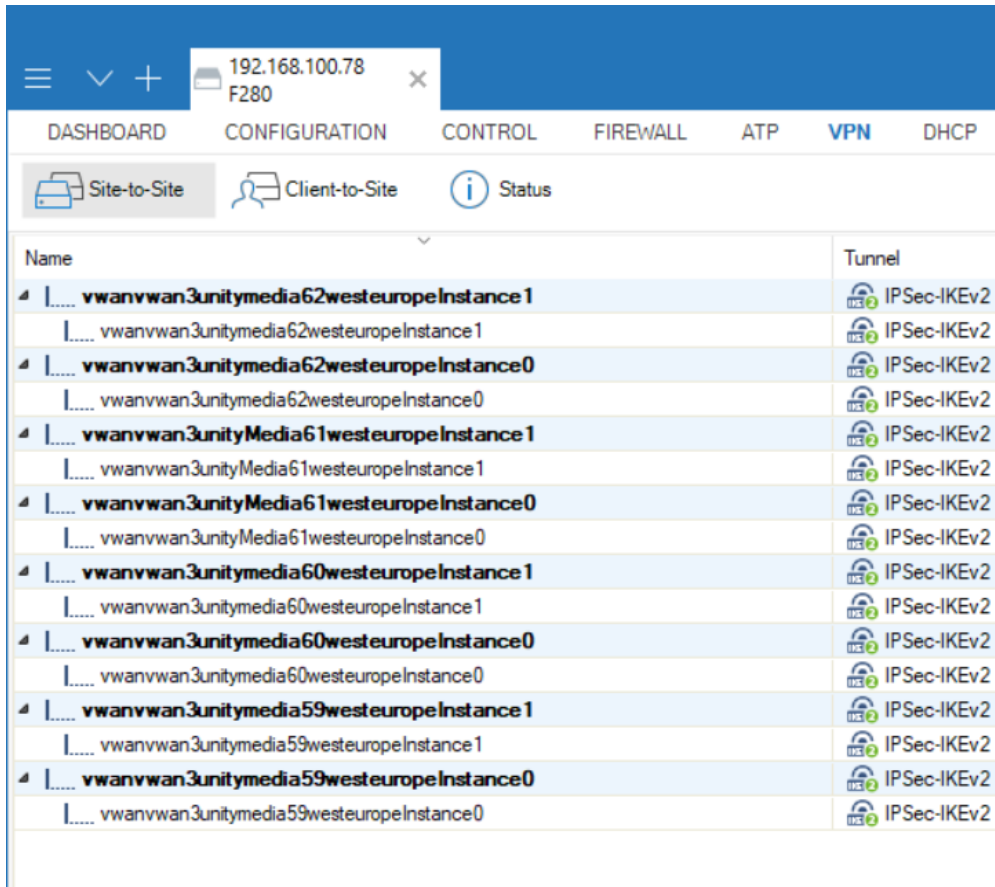
## Step 6. Verify Connectivity and Routing

---

For redundancy reasons, the CloudGen Firewall automatically creates two IPSec-IKEv2 VPN tunnels for each ISP and the required BGP routes to the Microsoft Azure Virtual Hub. Both tunnels for each ISP are in active-active mode. In case one tunnel fails, the routing is changed to automatically use the other tunnel. A failover can take up to 30 seconds, during which no traffic will be forwarded.

### Step 6.1 Verify VPN Tunnels and Routing on Your Firewall

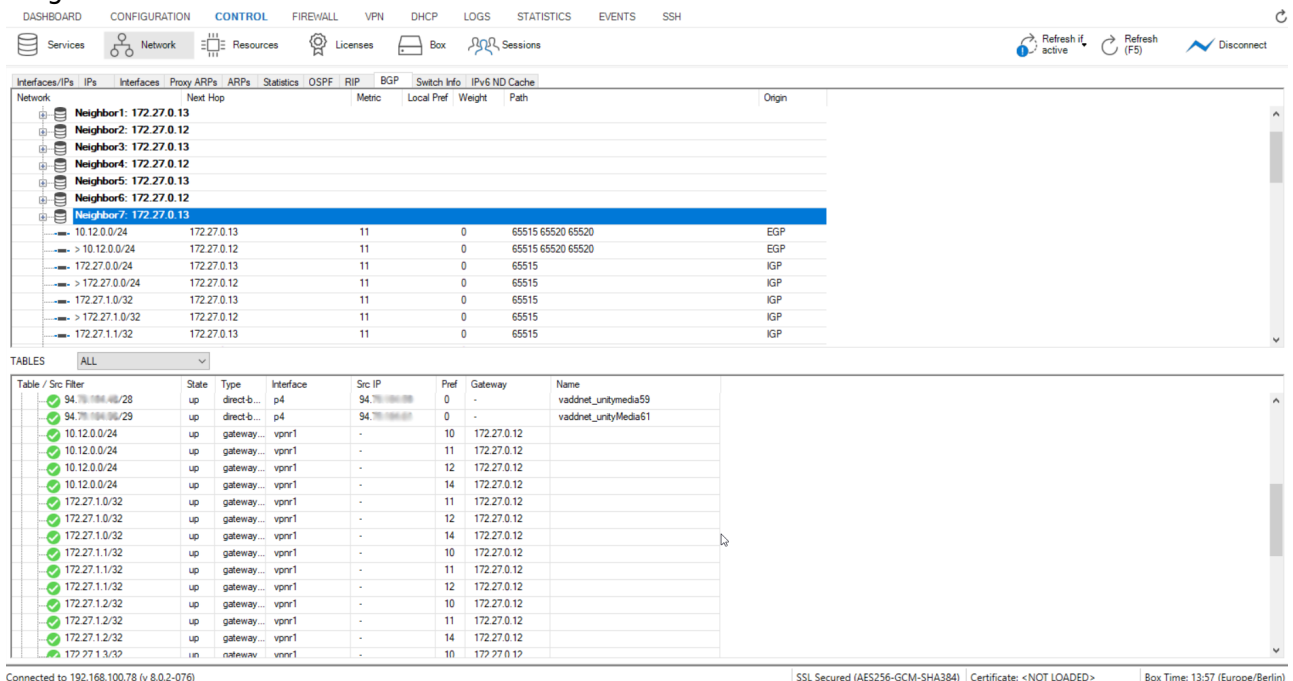
1. Log into the firewall.
2. Go to **VPN > Site-to-Site**.
3. Verify that two IPSec-IKEv2 tunnels for each ISP are up and running. In the example below, four ISPs are configured, resulting in eight tunnels (two tunnels for each link):



The screenshot shows the Barracuda CloudGen Firewall interface. At the top, there's a navigation bar with tabs: DASHBOARD, CONFIGURATION, CONTROL, FIREWALL, ATP, VPN, and DHCP. Below this, there's a sub-navigation bar with icons for Site-to-Site, Client-to-Site, and Status. The main content area displays a list of VPN tunnels. Each tunnel entry includes a Name and a Tunnel type (IPSec-IKEv2).

Name	Tunnel
vwanvwan3unitymedia62westeuropeInstance1	IPSec-IKEv2
vwanvwan3unitymedia62westeuropeInstance1	IPSec-IKEv2
vwanvwan3unitymedia62westeuropeInstance0	IPSec-IKEv2
vwanvwan3unitymedia62westeuropeInstance0	IPSec-IKEv2
vwanvwan3unityMedia61westeuropeInstance1	IPSec-IKEv2
vwanvwan3unityMedia61westeuropeInstance1	IPSec-IKEv2
vwanvwan3unityMedia61westeuropeInstance0	IPSec-IKEv2
vwanvwan3unityMedia61westeuropeInstance0	IPSec-IKEv2
vwanvwan3unitymedia60westeuropeInstance1	IPSec-IKEv2
vwanvwan3unitymedia60westeuropeInstance1	IPSec-IKEv2
vwanvwan3unitymedia60westeuropeInstance0	IPSec-IKEv2
vwanvwan3unitymedia60westeuropeInstance0	IPSec-IKEv2
vwanvwan3unitymedia59westeuropeInstance1	IPSec-IKEv2
vwanvwan3unitymedia59westeuropeInstance1	IPSec-IKEv2
vwanvwan3unitymedia59westeuropeInstance0	IPSec-IKEv2
vwanvwan3unitymedia59westeuropeInstance0	IPSec-IKEv2

- Go to **CONTROL > Network** and open the **BGP** tab.
- Verify that, along with the VPN tunnels, all associated BGP autonomous systems and neighbors are present. In the example below, four ISPs are configured, resulting in eight BGP neighbor entries.

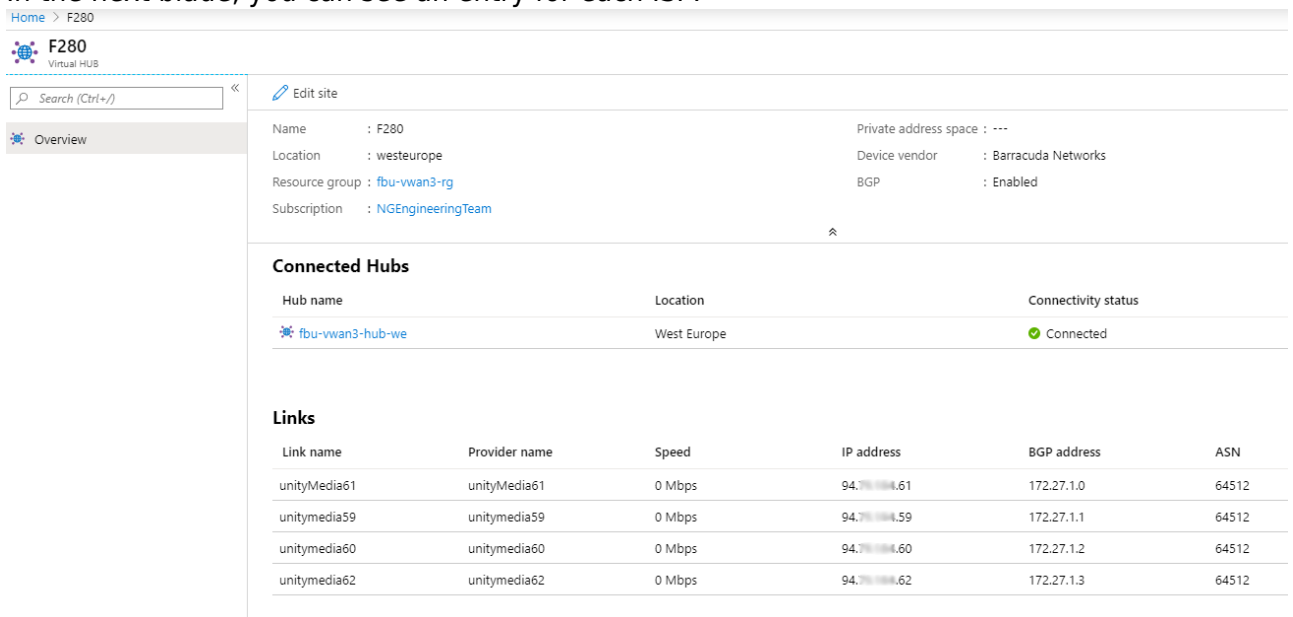


The screenshot shows the Barracuda CloudGen Firewall interface with the **CONTROL > Network** tab selected. The **BGP** sub-tab is active, displaying a list of BGP neighbors and their associated interfaces. Below the list, there's a table showing the configuration for each BGP neighbor.

Neighbor	Interface	State	Type	Interface	Src IP	Pref	Gateway	Name
Neighbor1: 172.27.0.13		up	direct-b...	p4	94.76.194.28	0	-	vaddnet_unitymedia59
Neighbor2: 172.27.0.12		up	direct-b...	p4	94.76.194.29	0	-	vaddnet_unityMedia61
Neighbor3: 172.27.0.13		up	gateway...	vpn1	-	10	172.27.0.12	
Neighbor4: 172.27.0.12		up	gateway...	vpn1	-	11	172.27.0.12	
Neighbor5: 172.27.0.13		up	gateway...	vpn1	-	12	172.27.0.12	
Neighbor6: 172.27.0.12		up	gateway...	vpn1	-	14	172.27.0.12	
Neighbor7: 172.27.0.13		up	gateway...	vpn1	-	11	172.27.0.12	
Neighbor8: 172.27.0.12		up	gateway...	vpn1	-	12	172.27.0.12	
Neighbor9: 172.27.0.13		up	gateway...	vpn1	-	14	172.27.0.12	
Neighbor10: 172.27.0.12		up	gateway...	vpn1	-	10	172.27.0.12	
Neighbor11: 172.27.0.13		up	gateway...	vpn1	-	11	172.27.0.12	
Neighbor12: 172.27.0.12		up	gateway...	vpn1	-	12	172.27.0.12	
Neighbor13: 172.27.0.13		up	gateway...	vpn1	-	14	172.27.0.12	
Neighbor14: 172.27.0.12		up	gateway...	vpn1	-	10	172.27.0.12	
Neighbor15: 172.27.0.13		up	gateway...	vpn1	-	11	172.27.0.12	
Neighbor16: 172.27.0.12		up	gateway...	vpn1	-	12	172.27.0.12	
Neighbor17: 172.27.0.13		up	gateway...	vpn1	-	14	172.27.0.12	
Neighbor18: 172.27.0.12		up	gateway...	vpn1	-	10	172.27.0.12	

**(Optional) Step 6.2 Verify Connectivity and Routing in Microsoft Azure**

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services** and search for **Virtual WANs**.
3. Click on your vWAN created in Step 2.
4. Click on your hub created in Step 3.
5. Click **VPN (Site to site)**.
6. Click on the entry of your CloudGen Firewall in the site list.
7. In the next blade, you can see an entry for each ISP:



Home > F280

**F280**  
Virtual WAN

Search (Ctrl+/) Edit site

Overview

Name : F280 Private address space : ---  
Location : westeurope Device vendor : Barracuda Networks  
Resource group : fbu-vwan3-rg BGP : Enabled  
Subscription : NGEngineeringTeam

**Connected Hubs**

Hub name	Location	Connectivity status
fbu-vwan3-hub-we	West Europe	Connected

**Links**

Link name	Provider name	Speed	IP address	BGP address	ASN
unityMedia61	unityMedia61	0 Mbps	94.7% 194.61	172.27.1.0	64512
unitymedia59	unitymedia59	0 Mbps	94.7% 194.59	172.27.1.1	64512
unitymedia60	unitymedia60	0 Mbps	94.7% 194.60	172.27.1.2	64512
unitymedia62	unitymedia62	0 Mbps	94.7% 194.62	172.27.1.3	64512

**Step 7. Configure the Forwarding Firewall Rule Set**

To manage and restrict network traffic from and to the Azure Virtual Hub, the forwarding firewall rule set needs to be adapted to allow traffic as required.

For more information, see [How to Create a Pass Access Rule](#).

**Next Steps**

Attach an Azure Virtual Network to the Virtual WAN hub to use the VPN connection for branch-to-cloud connectivity.

## Figures

1. vpn\_hub.png
2. xdsl\_config.png
3. marketplace\_vwan1.png
4. create\_vwan\_blade.png
5. create\_hubs\_1.png
6. create\_hub2.png
7. create\_hub3.png
8. cloud\_integration.png
9. ng\_admin4\_isps.png
10. control\_network\_bgp.png
11. azrue4isps.png

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.