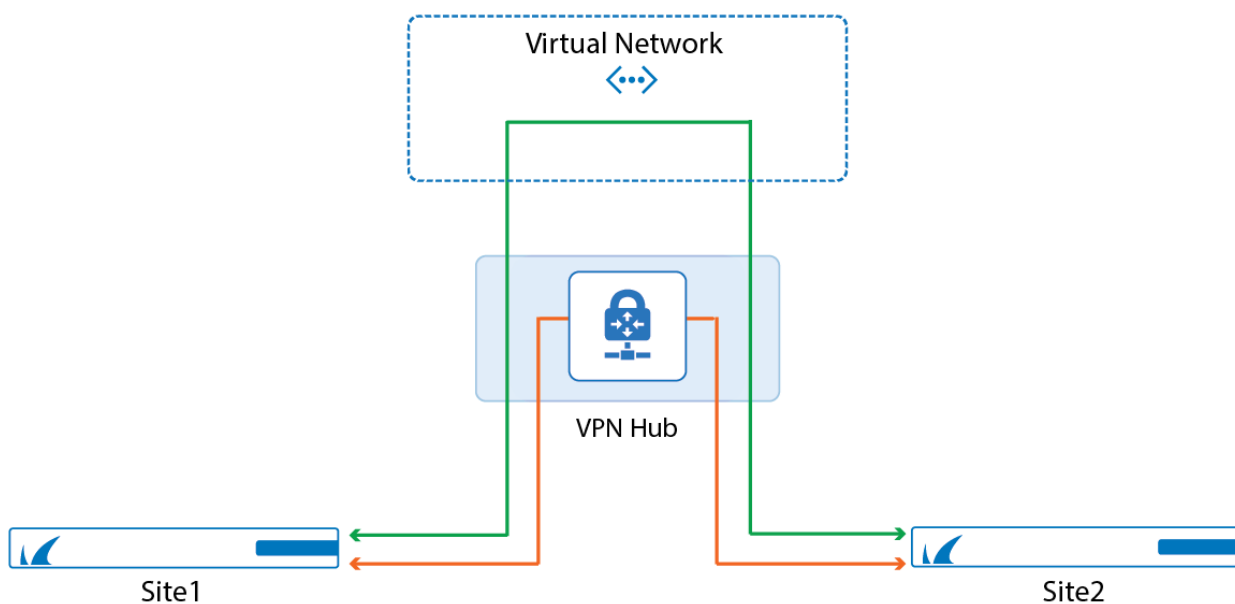


How to Configure Automatic Connectivity to Azure Virtual WAN

<https://campus.barracuda.com/doc/78808340/>

VPN connections from a CloudGen Firewall to the Azure Virtual WAN hub can be provisioned automatically. The automatic configuration provides a robust and redundant connection by introducing two active-active IPsec IKEv2 VPN tunnels with the corresponding BGP setup and fully automated Azure Virtual WAN site creation on Microsoft Azure. The finished deployment allows for both branch-to-branch and branch-to-cloud connections.



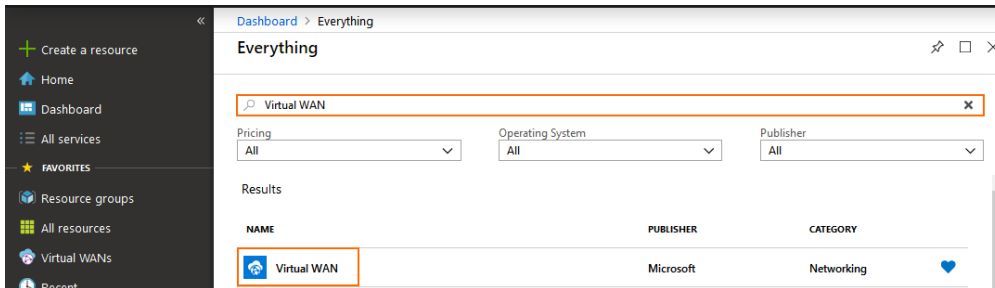
Before You Begin

- 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](#).
- 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 Direct Attached Routes](#).

Step 1. Configure Microsoft Azure Virtual WAN Service

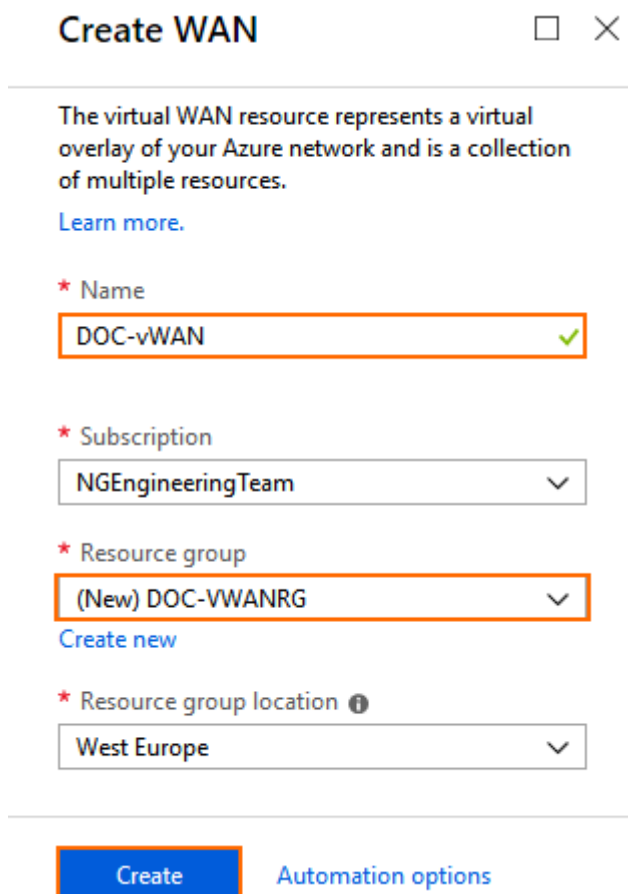
1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **Create a resource** and search for **Virtual WAN**.

3. Click **Virtual WAN**.



4. In the next blade, click **Create**.

5. In the **Create WAN** blade, enter the Virtual WAN **Name** and select an existing **Resource Group** or create a new one.



The screenshot shows the 'Create WAN' blade. It contains the following fields:

- Name:** DOC-vWAN (with a green checkmark)
- Subscription:** NGEEngineeringTeam
- Resource group:** (New) DOC-VWANRG (with a green checkmark)
- Resource group location:** West Europe

At the bottom, there is a blue 'Create' button and a link for 'Automation options'.

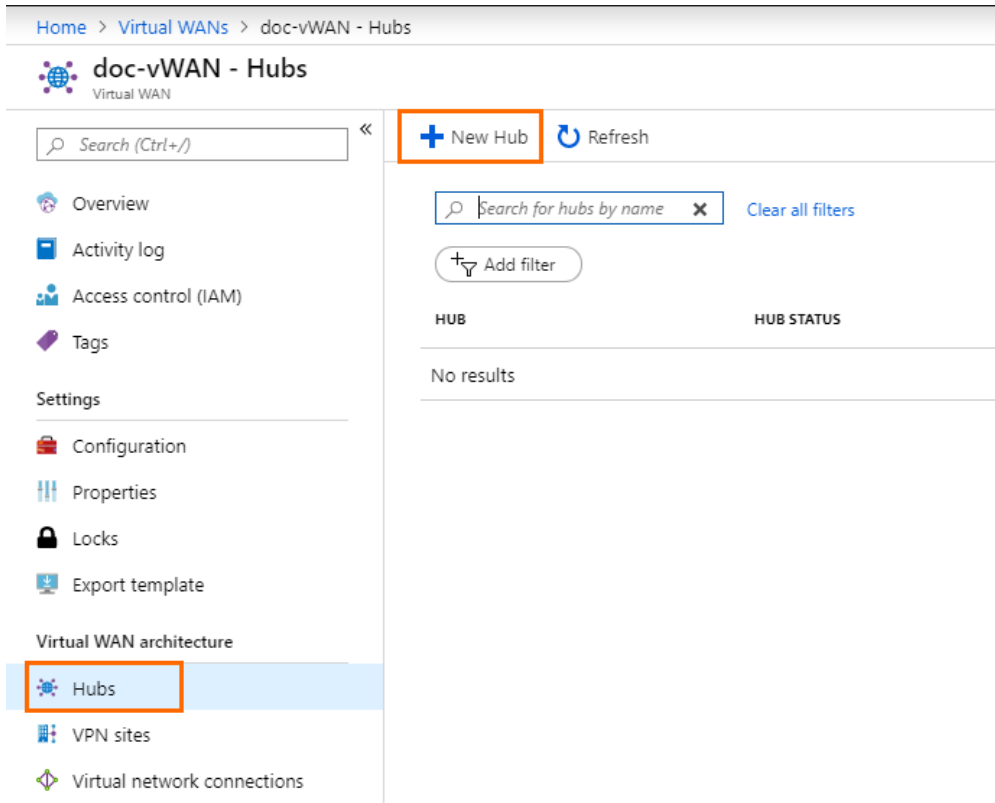
6. Click **Create** to finish Virtual WAN creation.

The CloudGen Firewall can now trigger the connection process to the Azure Virtual WAN.

Step 2. Create a Hub in Your vWAN

Creating a hub takes up to 30 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. It was created in Step 1.
4. Click on your vWAN created in Step 1.
5. On the left side, click **Hubs**.
6. In the next blade, click **New Hub**.



Home > Virtual WANs > doc-vWAN - Hubs

doc-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	

Overview
Activity log
Access control (IAM)
Tags

Settings

Configuration
Properties
Locks
Export template

Virtual WAN architecture

Hubs
VPN sites
Virtual network connections

7. The **Create virtual hub** blade opens.
 1. **Region** – Select a region from the drop-down list, e.g., West Europe.
 2. **Name** – Enter a name for the hub, e.g., doc-vwan-hub.
 3. **Hub private address space** – Enter the hub's address range in CIDR, e.g., 10.0.0.0/24.

[Home](#) > [Virtual WANs](#) > [doc-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	<input type="text" value="NGEngineeringTeam"/>
* Resource group	<input type="text" value="doc-vWAN_rg"/>

Virtual Hub Details

* Region	<input type="text" value="West Europe"/>
* Name	<input type="text" value="doc-vwan-hub"/>
* Hub private address space	<input type="text" value="10.0.0.0/24"/>

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


Home > clemens_vwan_test1009 - 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 ▾

 Creating a hub with a gateway will take 30 minutes.

Review + create

Previous

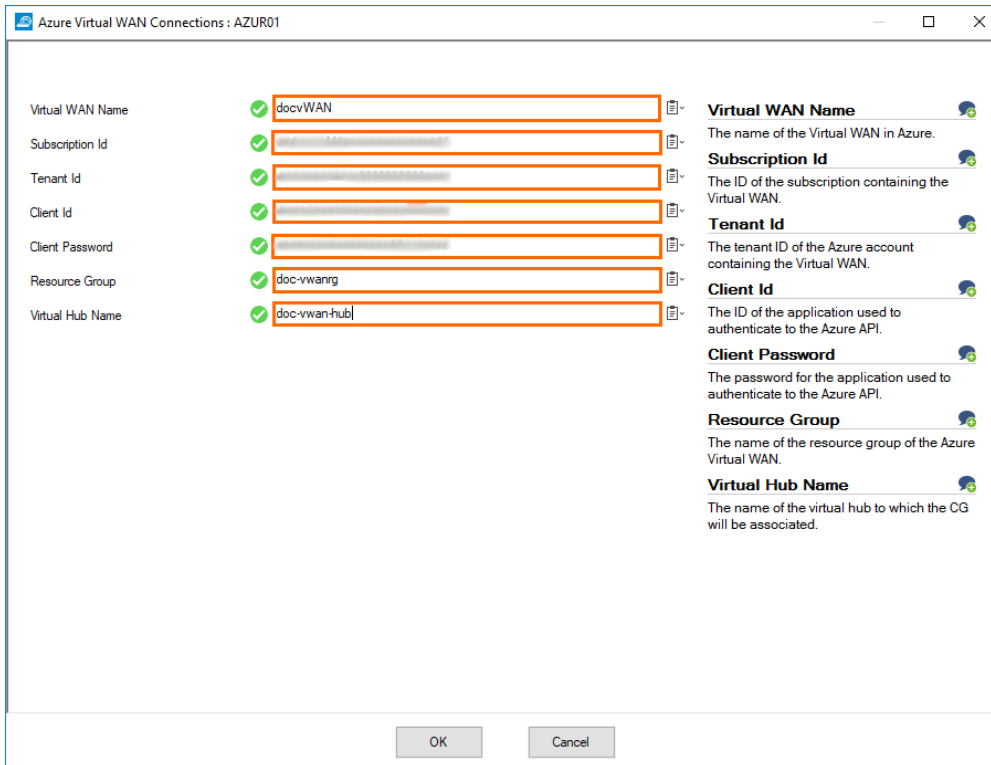
Next : Point to site >

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 3. Trigger Virtual WAN connection

1. Log into the CloudGen Firewall with CloudGen Admin.
2. Go to **CONTROL > Box**.
3. Click **Microsoft Azure Virtual WAN** and select **Connect to Virtual WAN**.
4. Enter the required information in the dialog to start automatic creation of the site. The site will be created and is then available in the Azure Virtual WAN **Settings**.



Virtual WAN Name	✓ docvWAN	Virtual WAN Name The name of the Virtual WAN in Azure.
Subscription Id	✓ [Redacted]	Subscription Id The ID of the subscription containing the Virtual WAN.
Tenant Id	✓ [Redacted]	Tenant Id The tenant ID of the Azure account containing the Virtual WAN.
Client Id	✓ [Redacted]	Client Id The ID of the application used to authenticate to the Azure API.
Client Password	✓ [Redacted]	Client Password The password for the application used to authenticate to the Azure API.
Resource Group	✓ doc-vwanrg	Resource Group The name of the resource group of the Azure Virtual WAN.
Virtual Hub Name	✓ doc-vwan-hub	Virtual Hub Name The name of the virtual hub to which the CG will be associated.

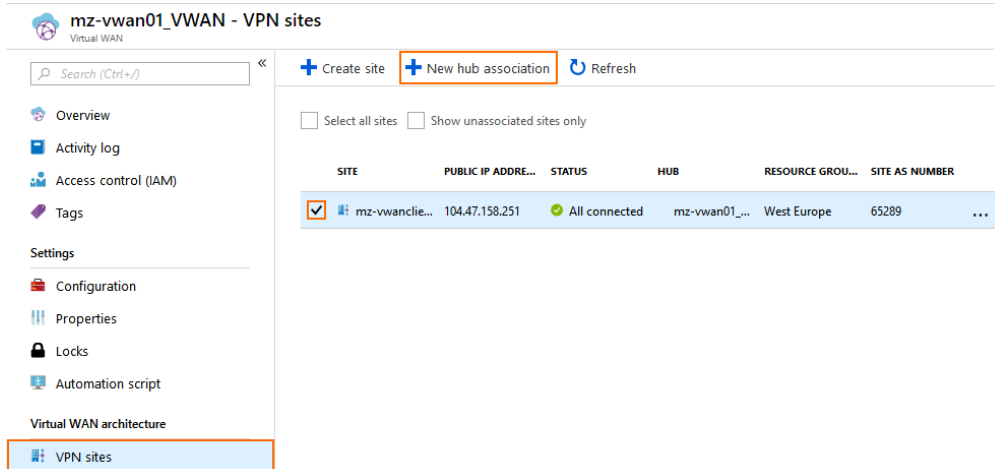
5. Click **Connect** to start the automatic site configuration process on Microsoft Azure.

A VPN site entry is automatically created, and the firewall starts to check for an available configuration every 30 seconds. To view the connection log, click **Check Connection Status**. Repeat as needed to update the status log messages.

Step 4. Associate Site to the Hub

The Virtual WAN VPN site must be associated to the geographically nearest Virtual WAN hub by the admin.

1. Log into the Azure portal: <https://portal.azure.com>
2. In your Azure Resource group, open your **Azure Virtual WAN**.
3. In the left menu of the Virtual WAN blade, click **VPN Sites**.
4. Select the check box of the Virtual WAN VPN site created by the firewall in Step 2 and click **New hub association**. The **Associate site with one or more hubs** blade opens.



mz-vwan01_VWAN - VPN sites

Virtual WAN

Search (Ctrl+/) << + Create site + **New hub association** Refresh

Select all sites Show unassociated sites only

SITE	PUBLIC IP ADDR...	STATUS	HUB	RESOURCE GROU...	SITE AS NUMBER
<input checked="" type="checkbox"/> mz-vwanclie...	104.47.158.251	All connected	mz-vwan01_...	West Europe	65289 ...

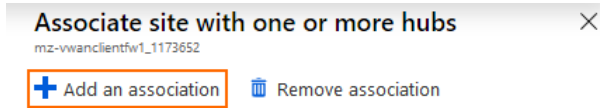
Settings

- Configuration
- Properties
- Locks
- Automation script

Virtual WAN architecture

- VPN sites**

5. Select the **Hub** from the list.
6. Select the check box for the hub and click **Add an association**.



Associate site with one or more hubs ×

mz-vwanclientfw1_1173652

+ Add an association Remove association

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

HUB PSK

mz-vwan01_HUB Default PSK

Wait for the new hub association to complete. The firewall automatically picks up the new configuration and connects to the Virtual WAN.

Step 5. Verify Connectivity and Routing

For redundancy reasons, the CloudGen Firewall automatically creates two IPSec-IKEv2 VPN tunnels and the required BGP routes to the Microsoft Azure virtual hub. Both tunnels are in active-active mode. In case one tunnel fails, the routing is changed to automatically use the other tunnel.

1. Log into the CloudGen Firewall.
2. Go to **VPN > Site-to-Site**.
3. Verify if two IPSec-IKEv2 tunnels are up and running.

DASHBOARD CONFIGURATION CONTROL FIREWALL **VPN** LOGS STATISTICS EVENTS SSH

Site-to-Site Client-to-Site Status

Name	Tunnel	Local IP	Peer IP	Transport	Encryption	Compression	bit/s	Start
▲ AzureVWAN-JTOyMOF142-01	IPSec-IKEv2	0.0.0.0	0.0.0.0		No enc.	0%	0	03.09.2019 14:46:18
└ AzureVWAN-JTOyMOF142-01	IPSec-IKEv2	127.0.0.9:4500	40.119.159.223:4500	ESPoUDP	AES256	0%	0	03.09.2019 14:46:18
▲ AzureVWAN-JTOyMOF142-02	IPSec-IKEv2	0.0.0.0	0.0.0.0		No enc.	0%	0	03.09.2019 14:48:53
└ AzureVWAN-JTOyMOF142-02	IPSec-IKEv2	10.1.16.4:4500	40.119.159.62:4500	ESPoUDP	AES256	0%	0	03.09.2019 14:48:53

- 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.

DASHBOARD CONFIGURATION **CONTROL** FIREWALL VPN LOGS STATISTICS EVENTS SSH

Services Network Resources Licenses Box Sessions

Interfaces/IPs IPs Interfaces Proxy ARPs ARPs Statistics OSPF RIP **BGP** Switch Info IPv6 ND Cache Azure UDR

Network	Next Hop	Metric	Local Pref	Weight	Path	Origin
AS 65515						
Neighbor: 10.17.94.7						
Neighbor: 10.17.94.6						
Prefixes Received: 2						
Up/Down-Time: 00:02:45						
Sent Messages: 6						
Received Messages: 5						
> 10.17.94.0/24	10.17.94.6			0	65515	IGP
> 10.17.95.1/32	10.17.94.6			0	65515	IGP

TABLES ALL

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table vpnllocal, From all							
Table 5, From 10.17.95.1							
10.17.94.6/32	up	direct-b...	vpn1	-	0	-	
10.17.94.7/32	up	direct-b...	vpn1	-	0	-	
Table dhcp1, From 10.1.16.4							
Table main, From all							
10.1.16.0/24	up	direct-k...	dhcp	10.1.16.4	0	-	
10.1.16.1/32	up	direct-b...	dhcp	10.1.16.4	0	-	
10.1.16.1/32	up	direct-k...	dhcp	10.1.16.4	0	-	
10.17.94.0/23	up	direct-k...	vpnr1	10.17.95.1	0	-	vaddnet_VWAN-JTOyMOF142
127.0.0.0/24	up	direct-b...	lo	127.0.0.2	0	-	boxnet
127.0.3.0/24	up	direct-k...	vpn1	127.0.3.1	0	-	
168.63.129.16/32	up	gateway...	dhcp	10.1.16.4	100	10.1.16.1	
169.254.169.254/32	up	gateway...	dhcp	10.1.16.4	100	10.1.16.1	
10.17.95.1/32	up	gateway...	vpnr1	-	0	10.17.94.6	
Table default, From all							
0.0.0.0/0	up	gateway...	dhcp	10.1.16.4	100	10.1.16.1	

Step 6. 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. vwan2_01.png
3. vwan2_02.png
4. create_hub.png
5. create_hub2.png
6. site to site vpn_gateway.png
7. vwan_config_cgf.png
8. vwan2_03.png
9. vwan2_04.png
10. vpn.png
11. cgf_network.png

© Barracuda Networks Inc., 2019 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.