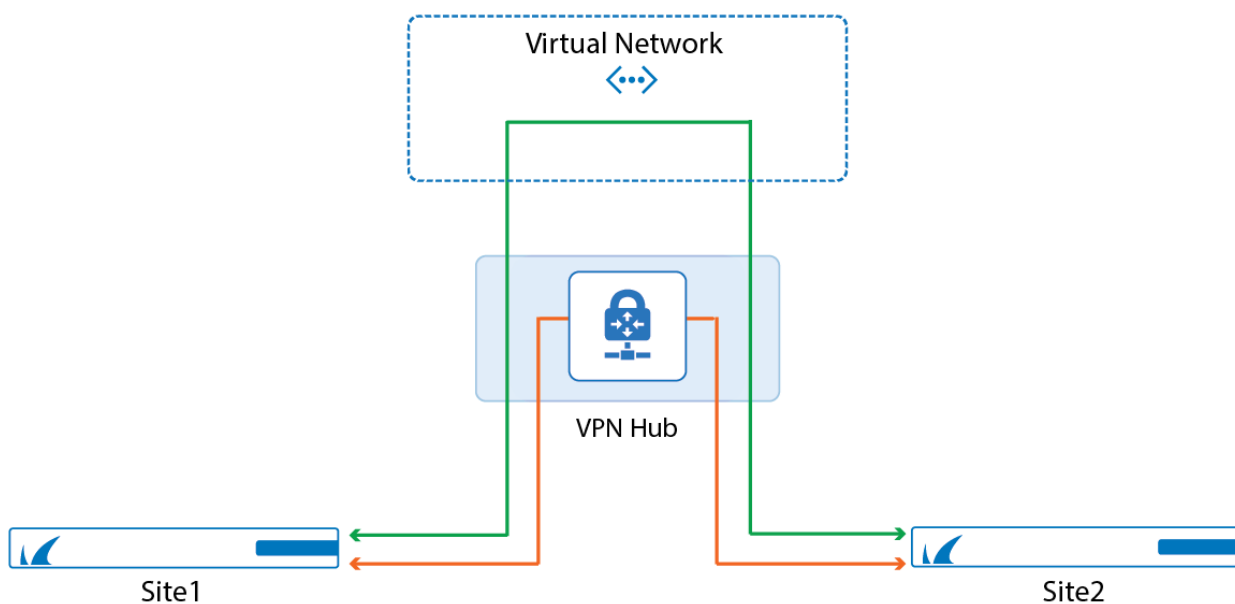


How to Configure Automatic Connectivity to Azure Virtual WAN

<https://campus.barracuda.com/doc/79463437/>

VPN connections from a stand-alone Barracuda 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 respective 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.



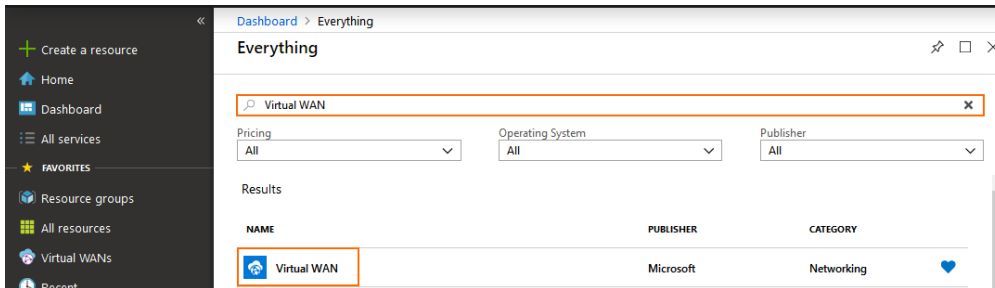
Before You Begin

- 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 **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 the **Resource Group**.

Create WAN □ ×

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

[Learn more.](#)

* Name
 ✓

* Subscription

* Resource group
 ▼

[Create new](#)

* Resource group location ⓘ

[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. 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 to the dialog to start automatic creation of the site. The site will be created and is then available in the Azure Virtual WAN **Settings**.

Automated Connectivity for Azure Virtual WAN

✕

Azure Authentication	
Tenant ID	5faff1ac-28ff-9d11-11hj666888459
Subscription ID	7ffaa7gc-55gj-2h77-63aj553311123
User ID	1ffc1dd-17ff-1d33-11hj666888459
Password	••••••••••

Azure Virtual WAN	
Virtual WAN Name	Campus-DOC-vWAN

Tenant ID Enter the Azure Active Directory Tenant ID of the Azure Account used for the Azure Virtual WAN.
Subscription ID Enter the subscription ID of the Azure account used for the Azure Virtual WAN.
User ID Enter the Azure Application ID of the Service Principal user for the Azure Virtual WAN.
Password Enter the Password of the Service Principal used to connect Firewalls to the Azure Virtual WAN.
Virtual WAN Name Optionally enter the name of the virtual WAN.

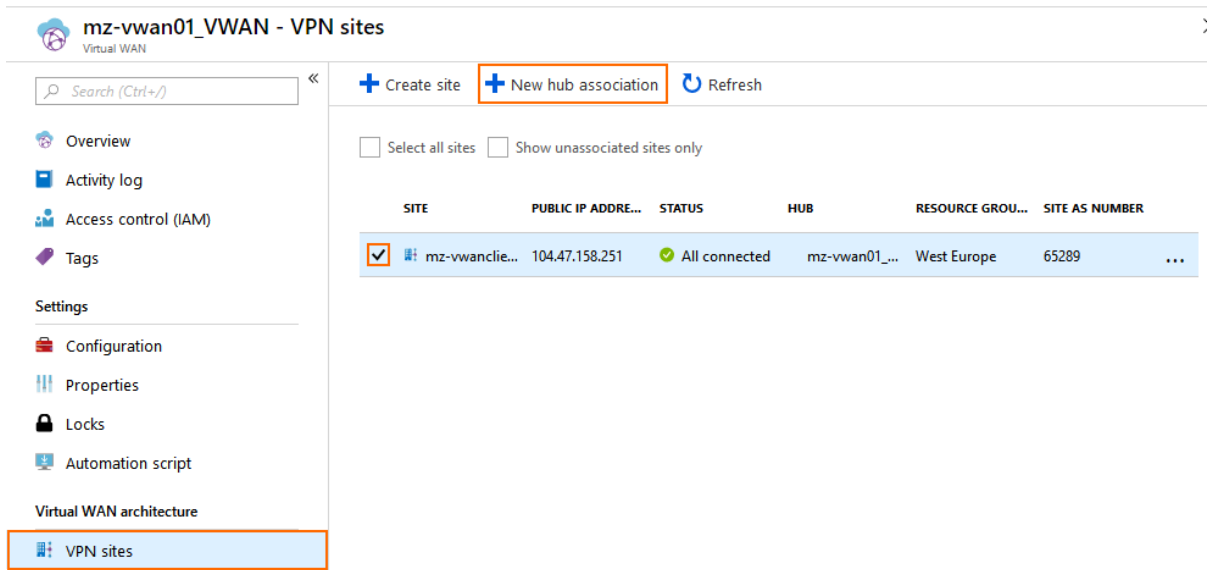
5. Click **Connect** to start the automatic site configuration process on Microsoft Azure.

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.

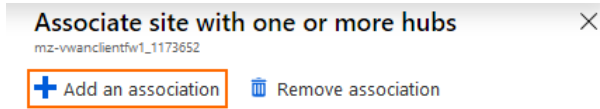
Step 3. Associate Site to the Hub

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.



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



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



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

Step 4. 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 NETWORK ACCESS CLIENT **VPN** LOGS STATISTICS EVENTS SSH

Site-to-Site Client-to-Site Status

Name	Tunnel	Local IP	Peer IP	Transport	Encryption	Compression	bit/s	Start
▲ AzureVWAN1	IPSec-IKEv2	0.0.0.0	0.0.0.0		No enc.	0%	1.0 K	05/09/2018 10:10:51
▲ AzureVWAN1	IPSec-IKEv2	109.224.194.153:4	13.69.99.10:4500	ESPoUDP	AES256	0%	1.0 K	05/09/2018 10:10:51
▲ AzureVWAN2	IPSec-IKEv2	0.0.0.0	0.0.0.0		No enc.	0%	0	05/09/2018 10:10:51
▲ AzureVWAN2	IPSec-IKEv2	109.224.194.153:4	13.69.96.109:4500	ESPoUDP	AES256	0%	0	05/09/2018 10:10:51

- 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 NETWORK ACCESS CLIENT VPN LOGS STATISTICS EVENTS SSH

Server Network Resources Licenses Box Sessions

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

Network

Network	Next Hop	Metric	Local Pref	Weight	Path	Origin
AS 65515						
Neighbor: 172.16.0.5						
Neighbor: 172.16.0.4						
PrefixesReceived: 4						
Up/Down-Time: 00:00:55						
Sent Messages: 5						
Received Messages: 2						
> 10.15.0.0/16	172.16.0.5		0	65515		IGP
> 172.16.0.0/24	172.16.0.5		0	65515		IGP
> 172.16.1.1/32	172.16.0.5		0	65515		IGP
> 172.16.2.1/32	172.16.0.5		0	65515		IGP
10.15.0.0/16	172.16.0.4		0	65515		IGP
172.16.0.0/24	172.16.0.4		0	65515		IGP
172.16.1.1/32	172.16.0.4		0	65515		IGP
172.16.2.1/32	172.16.0.4		0	65515		IGP

TABLES ALL

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table main, From all							
10.14.0.0/17	up	direct-b	eth0	10.14.42.156	0	-	boxnet
109.224.194.144/28	up	direct-b	eth3	109.224.194.153	0	-	IPV401
127.0.3.0/24	up	direct-k...	vpn1	127.0.3.1	0	-	
172.16.0.0/23	up	direct-k...	vpn1	172.16.1.2	0	-	
10.15.0.0/16	up	gateway...	vpn1	-	0	172.16.0.5	
172.16.1.1/32	up	gateway...	vpn1	-	0	172.16.0.5	
172.16.2.1/32	up	gateway...	vpn1	-	0	172.16.0.5	
Table default, From all							
0.0.0.0/0	up	gateway...	eth3	109.224.194.153	0	109.224.194.145	boxdev
Table vpnlocal, From all							
Table 5, From 172.16.1.2							
172.16.0.4/32	up	direct-b	vpn1	-	0	-	
172.16.0.5/32	up	direct-b	vpn1	-	0	-	

Step 5. 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. connect_fw.png
5. vwan2_03.png
6. vwan2_04.png
7. conn_routing.png
8. conn_routing01.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.