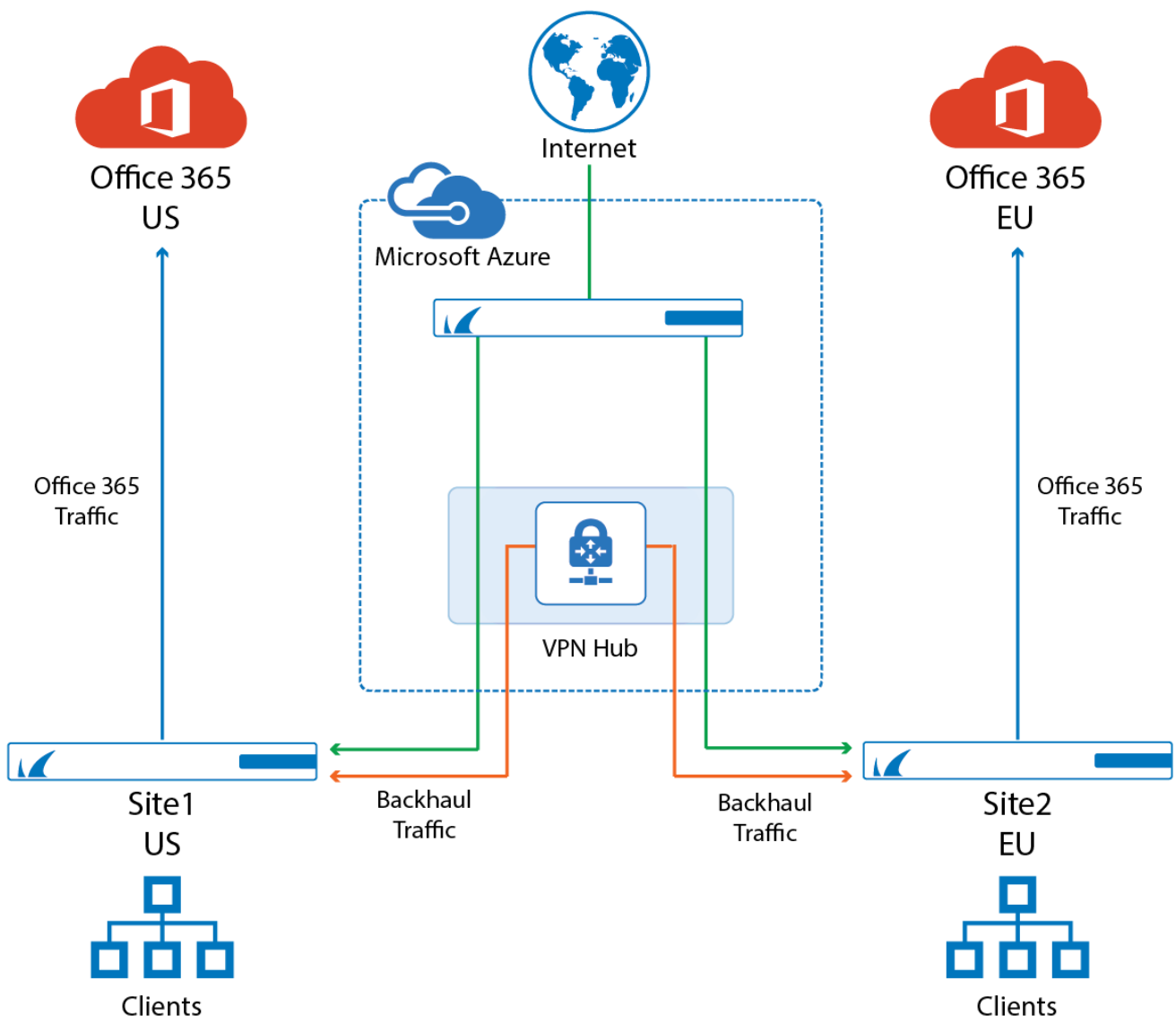


How to Configure Automatic Connectivity to Azure Virtual WAN with Selective Traffic Backhauling

<https://campus.barracuda.com/doc/80248877/>

Connecting Barracuda CloudGen Firewalls to a Microsoft Azure Virtual WAN hub can be done automatically. The automatic configuration provides robust and redundant connections 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 for selective traffic backhauling. Selective traffic backhauling means that all network traffic, except connections to Office 365, will be routed to the Microsoft Azure public cloud. However, for compliance and regional experience, Office 365 traffic routing will be enforced by the Azure Virtual WAN settings to be routed to the regional Office 365 datacenters of your on-premises sites.

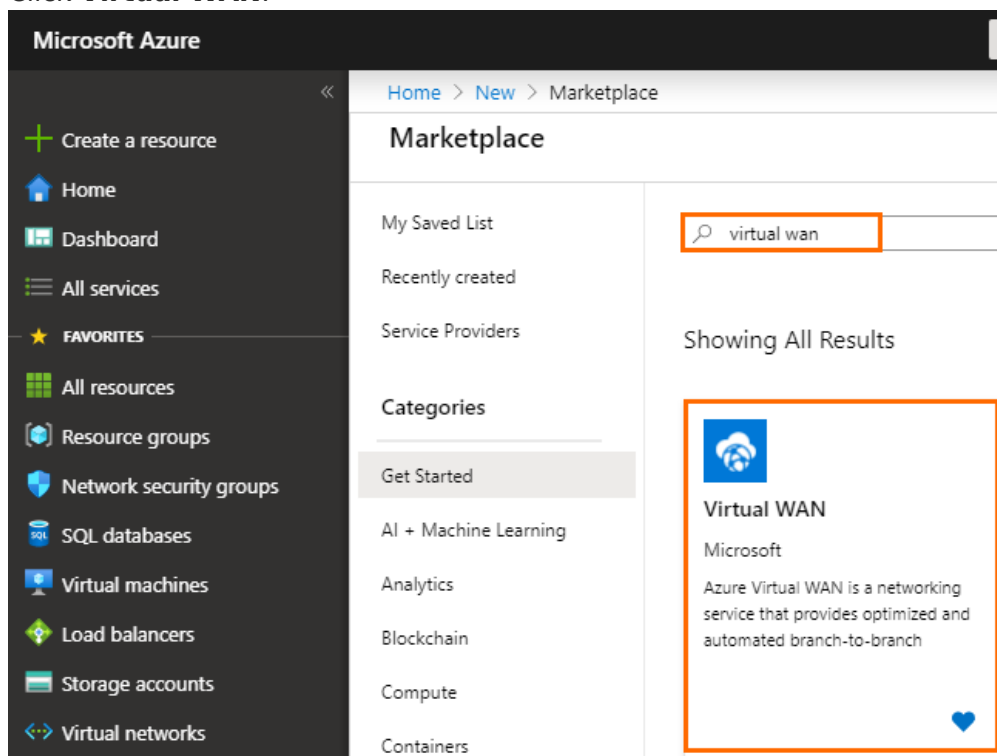


Before You Begin

- This configuration requires CloudGen Firewall 7.2.3, hotfix-896, and Barracuda Firewall Admin 7.2.3 - 207.
- 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](#).

Step 1. 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 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 >](#)

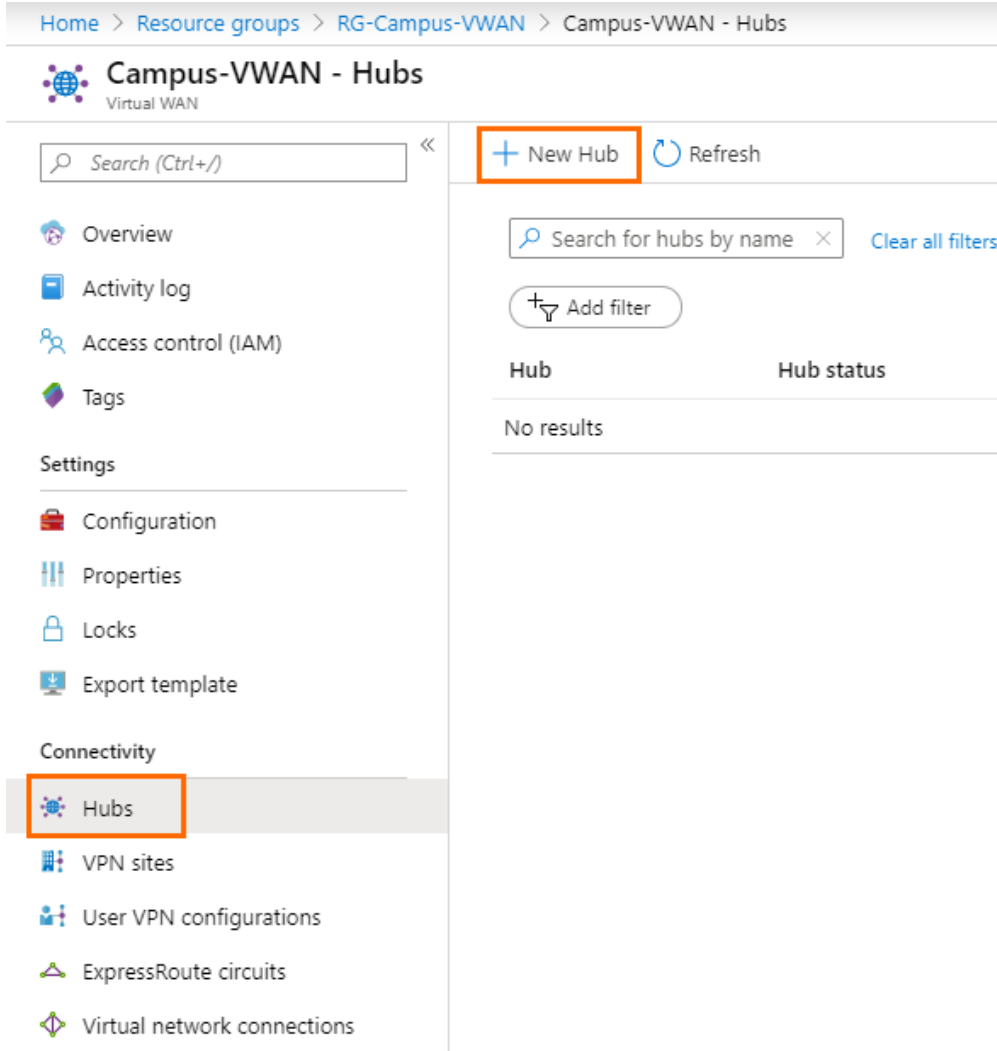
6. Click **Review + Create**.
7. Click **Create** to finish Virtual WAN creation.

Step 2. Create a Hub in Your Azure Virtual WAN

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

Campus-VWAN - Hubs

Virtual WAN

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

Overview
Activity log
Access control (IAM)
Tags

Settings

Configuration
Properties
Locks
Export template

Connectivity

Hubs
VPN sites
User VPN configurations
ExpressRoute circuits
Virtual network connections

Search for hubs by name X Clear all filters

+ Add filter

Hub	Hub status
No results	

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 .

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 ⓘ

65515

*Gateway scale units

1 scale unit - 500 Mbps x 2

 Creating a hub with a gateway will take 30 minutes.

[Review + create](#)

[Previous](#)

[Next : Point to site >](#)

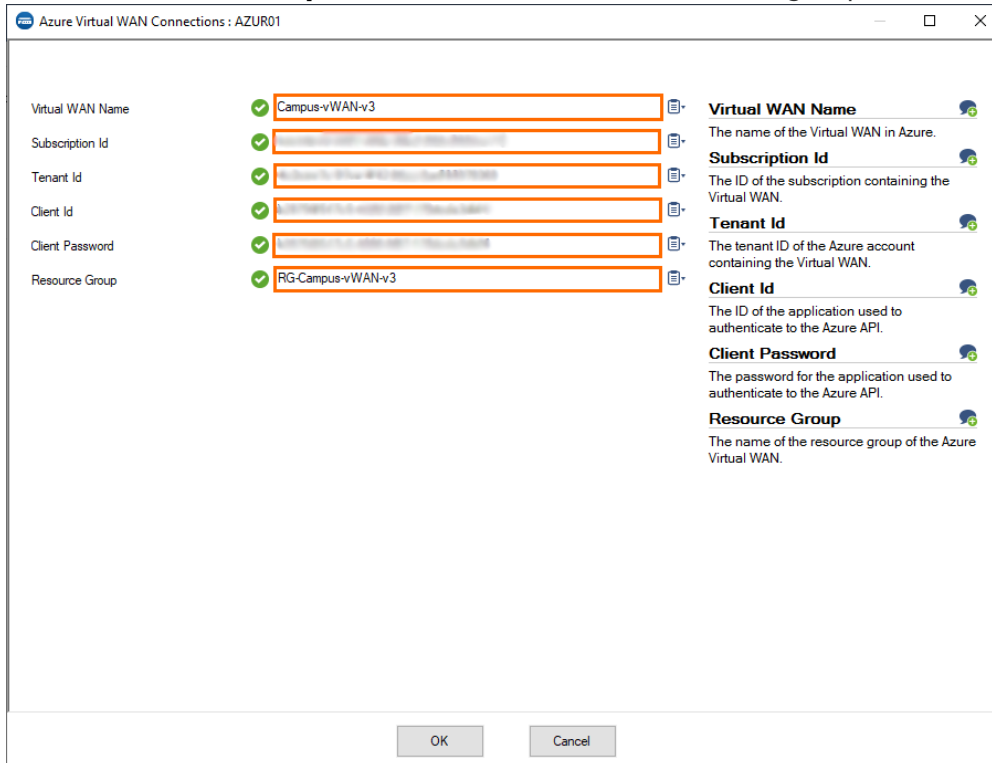
10. Click **Review + create**.

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 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.
 - **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** – Enter the password for the application used to authenticate to the Azure API.
- **Resource Group** – Enter the name of the resource group containing the Virtual WAN.



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

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** created in Step 1.
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 3 and click **New hub connection**.

Home > Resource groups > RG-Campus-vWAN-v3 > Campus-vWAN-v3 - VPN sites

Campus-vWAN-v3 - VPN sites
Virtual WAN

Search (Ctrl+/) << + Create site ↓ Download Site-to-Site VPN c... **+ New hub connection** ↻ Refresh

Search by site name × Clear all filters

+ Add filter

☐ Select all sites

VPN Sites ⓘ

Site	Site Provisioning Status	Hub
<input checked="" type="checkbox"/> = CGF_WOX7MT6YMY	Provisioned	> Connection needed

Overview
Activity log
Access control (IAM)
Tags
Settings
Configuration
Properties
Locks
Export template

5. The **Connect sites with one hub** blade opens.

1. Select the **Hub** created in Step 2 from the drop-down menu.
2. Select the check box of the Virtual WAN VPN site created by the firewall in Step 3.

Connect sites with one hub ×

1 Azure WAN sites

CampusvWANv3-hub

<input checked="" type="checkbox"/>	Site	PSK
<input checked="" type="checkbox"/>	801-CGF_...	Default PSK

Confirm

6. Click **Confirm**.

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

Step 5. Configure Routes to Be Advertised via BGP

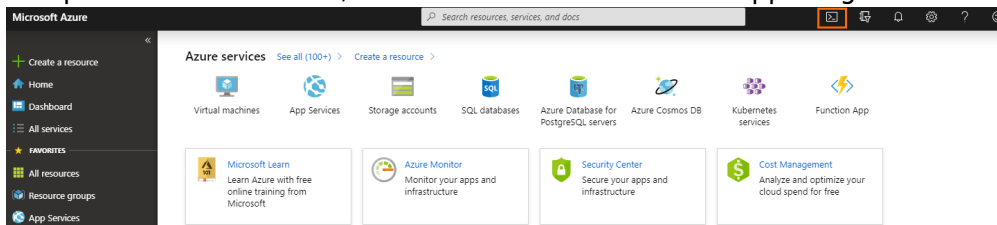
Only routes with the parameter **Advertise** set to **yes** will be propagated via BGP.

1. Go to **CONFIGURATION > Configuration Tree > Multi Range > your range > your cluster > Boxes > your Box > Network**.
2. Click **Configuration Mode**.

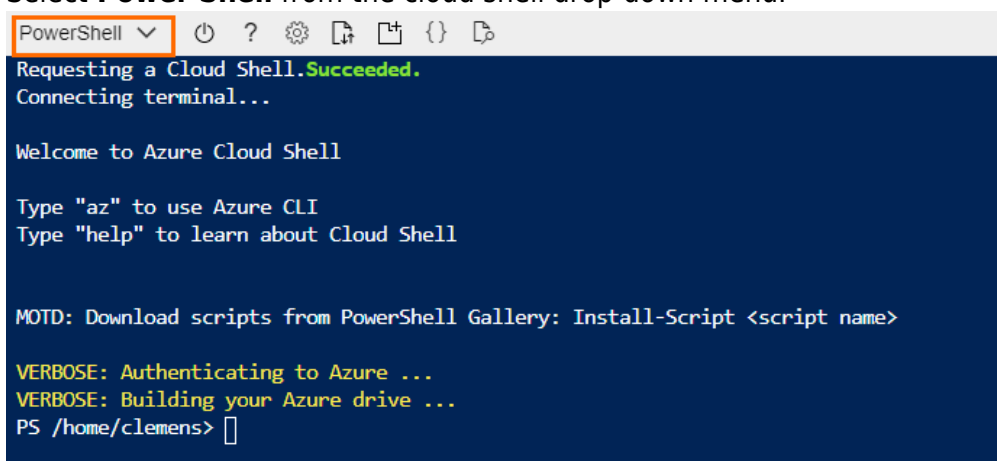
3. Click **Switch to Advanced**.
4. Click **Lock**.
5. (optional) Click **IP Configuration**. In the **Management IP and Networks** section, set **Advertise Route** to **yes** in order to propagate the management network.
6. In the left menu, click **Routing**.
7. Double-click on the **Routes** you want to propagate, and set **Advertise Route** to **yes**.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Step 6. Configure Local Breakout in Microsoft Azure Cloud Shell

1. Log into the Azure portal: <https://portal.azure.com>.
2. To open the **Cloud Shell**, click on the shell icon in the upper-right corner.



3. Select **Bash** in the **Cloud Shell** menu.
4. Select **Power Shell** from the cloud shell drop-down menu.



5. (Optional) If you have not installed the virtual WAN extension for Azure Power Shell, type `az extension add --name virtual-wan` and press enter to install the extension.

```
PowerShell | ? ? ? ? ? ? ? ? ? ?
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

MOTD: Manage Azure Active Directory: Get-Command -Module AzureAD*

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive
PS /home/clemens> az extension add --name virtual-wan
The installed extension 'virtual-wan' is in preview.
PS /home/clemens> |
```

6. Enter `az network vwan update --name <your_virtual_WAN_name> --resource-group <name_of_resource_group_containing_your_virtual_WAN> --office365-category <value>` to select the breakout category that meets your requirements.

```
PowerShell | ? ? ? ? ? ? ? ? ? ?
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

MOTD: Scripts installed with 'Install-Script' can be run from the shell

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/clemens> az network vwan update --name vWAN_catamaniuk --resource-group vWAN_rg_catamaniuk --office365-category 0
{
  "allowBranchToBranchTraffic": true,
  "allowWnetToVnetTraffic": false,
  "disableVpnEncryption": false,
  "etag": "W/XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX",
  "id": "/subscriptions/288b0000-0000-0000-0000-000000000000/resourceGroups/vWAN_rg_catamaniuk/providers/Microsoft.Network/virtualWans/vWAN_catamaniuk",
  "location": "westeurope",
  "name": "vWAN_catamaniuk",
  "office365LocalBreakoutCategory": "Optimize",
  "p2SvpnServerConfigurations": null,
  "provisioningState": "Succeeded",
  "resourceGroup": "vWAN_rg_catamaniuk",
  "securityProviderName": null,
  "tags": null,
  "type": "Microsoft.Network/virtualWans",
  "virtualHubs": null,
  "vpnSites": null
}
PS /home/clemens> |
```

7. After the update was successful, the new configuration is displayed on the command-line interface.

The following values are available:

Value	Name
0	optimize
1	optimize and allow
2	all
3	none

For more information on the categories, see Microsoft article

<https://docs.microsoft.com/en-us/cli/azure/ext/virtual-wan/network/vwan?view=azure-cli-latest> .

Step 7. Verify Connectivity and Routing

For redundancy reasons, the CloudGen Firewall automatically creates two IPsec-IKEv2 VPN tunnels and the required BGP routes to the Azure Virtual Hub. Both tunnels are in active-active mode while only one tunnel is tunneling data to the Azure Virtual WAN. The firewall automatically switches between the tunnels to ensure robust connectivity to Azure.

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

DASHBOARD	CONFIGURATION	CONTROL	FIREWALL	NETWORK ACCESS CLIENT	VPN	LOGS	STATISTICS	EVENTS	SSH
<div> <div>Site-to-Site</div> <div>Client-to-Site</div> <div>Status</div> </div>									
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	

4. Go to **CONTROL > Network** and open the **BGP** tab.
5. Verify that, along with the VPN tunnels, all associated BGP autonomous systems and neighbors are present.

Navigation: DASHBOARD | CONFIGURATION | **CONTROL** | FIREWALL | NETWORK ACCESS CLIENT | VPN | LOGS | STATISTICS | EVENTS | SSH

Server | **Network** | Resources | Licenses | Box | Sessions

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

Network | Next Hop | Metric | Local Pref | Weight | Path | Origin

AS 65515

Neighbor: 172.16.0.5
Neighbor: 172.16.0.4

Prefixes Received: 4
Up/Down-Time: 00:00:55
Sent Messages: 5
Received Messages: 2

Prefix	Next Hop	Metric	Local Pref	Weight	Path	Origin
> 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 8. 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: [Access Rules](#).

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_a_o365.png
2. marketplace_vwan1.png
3. create_vwan_blade.png
4. create_hubs_1.png
5. create_hub2.png
6. create_hub3.png
7. vwan_cgf.png
8. connect_hub.png
9. connecthub2.png
10. cloud_shell.png
11. ps.png
12. vwan_ext.png
13. updated.png
14. conn_routing.png
15. conn_routing01.png

© Barracuda Networks Inc., 2024 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.