

How to Configure an IKEv2 IPsec Site-to-Site VPN to a Routed-Based Microsoft Azure VPN Gateway

https://campus.barracuda.com/doc/17396/

To connect to your Azure virtual network with your on-premises CloudGen Firewall, Microsoft offers the Azure VPN Gateway in two different versions: static and route-based. The route-based VPN Gateway allows connection for up to 10 on-premises firewalls. To connect to the VPN Gateway, configure an IPsec IKEv2 site-to-site VPN tunnel on your CloudGen Firewall. The CloudGen Firewall must be configured as the active partner. The following instructions are for Azure Resource Manager deployments.



Before You Begin

- You will need the following information:
 - VPN Gateway
 - Public IP address of your on-premises CloudGen Firewall
 - Remote and local networks.
- Install and configure Azure PowerShell 4.1.0 or higher.

Step 1. Create a Dynamic Microsoft Azure VPN Gateway Using Azure Resource Manager and PowerShell

Use Azure PowerShell to create a routed-based VPN Gateway.

- 1. Open Azure PowerShell.
- 2. Connect to your Azure account:

Login-AzureRmAccount

3. Enter your Azure account credentials and click Login.



4. Create a resource group:

```
New-AzureRmResourceGroup -Name YOUR_RESOURCE_GROUP -Location YOUR_LOCATION
```

5. Create the network configuration for the VPN gateway subnet and two Azure subnets. The VPN gateway subnet must use the name **GatewaySubnet**.

```
$vpnsubnet = New-AzureRmVirtualNetworkSubnetConfig -Name "GatewaySubnet"
-AddressPrefix 10.2.1.0/28
$subnet1 = New-AzureRmVirtualNetworkSubnetConfig -Name "Subnet1" -
AddressPrefix 10.2.2.0/24
$subnet2 = New-AzureRmVirtualNetworkSubnetConfig -Name 'Subnet2' -
AddressPrefix 10.2.3.0/24
```

6. Create the virtual network:

```
New-AzureRmVirtualNetwork -Name VNET_NAME -ResourceGroupName
YOUR_RESOURCE_GROUP -Location YOUR_LOCATION -AddressPrefix 10.2.0.0/16 -
Subnet $vpnsubnet,$subnet1,$subnet2
```

7. Create the local VPN Gateway configuration. Use the public IP address your firewall is using to connect to the Azure VPN Gateway. Replace the LOCAL_SUBNET variables with a list of the local subnets behind your firewall.

```
New-AzureRmLocalNetworkGateway -Name OnPremiseVPNGateway -
ResourceGroupName YOUR_RESOURCE_GROUP -Location YOUR_LOCATION -
GatewayIpAddress YOUR_PUBLIC_IP
-AddressPrefix @('LOCAL_SUBNET1','LOCAL_SUBNET2')
```

8. Create an Azure public IP address and store it in a variable for later use.

```
$gwpip = New-AzureRmPublicIpAddress -Name gwpip -ResourceGroupName
YOUR RESOURCE GROUP -Location YOUR LOCATION -AllocationMethod Dynamic
```

9. Create variables for virtual network, VPN subnet, and gateway IP configuration.

```
$vnet = Get-AzureRmVirtualNetwork -Name VNET_NAME -ResourceGroupName
YOUR_RESOURCE_GROUP
    $vpnsubnet = Get-AzureRmVirtualNetworkSubnetConfig -Name
'GatewaySubnet' -VirtualNetwork $vnet
    $gwipconfig = New-AzureRmVirtualNetworkGatewayIpConfig -Name
gwipconfig1 -SubnetId $vpnsubnet.Id -PublicIpAddressId $gwpip.Id
```

10. Create the routed-based (dynamic) VPN Gateway attached to the virtual network:

New-AzureRmVirtualNetworkGateway -Name VNET_GW_NAME -ResourceGroupName YOUR_RESOURCE_GROUP -Location YOUR_LOCATION -IpConfigurations \$gwipconfig -GatewayType Vpn -VpnType RouteBased

11. Create the VPN connection:



\$gateway1 = Get-AzureRmVirtualNetworkGateway -Name VNET_GW_NAME ResourceGroupName YOUR_RESOURCE_GROUP
\$local = Get-AzureRmLocalNetworkGateway -Name OnPremiseVPNGateway ResourceGroupName YOUR_RESOURCE_GROUP
New-AzureRmVirtualNetworkGatewayConnection -Name localtovpn ResourceGroupName YOUR_RESOURCE_GROUP -Location YOUR_LOCATION VirtualNetworkGateway1 \$gateway1 -LocalNetworkGateway2 \$local ConnectionType IPsec -RoutingWeight 10 -SharedKey YOUR_PASSPHRASE

Creating the VPN connection can take up to 30 minutes to complete. You can now configure the onpremises firewall to connect to the Azure VPN Gateway.

Step 2. Get the VPN Gateway Public IP Address

Get the public IP address allocated for the Azure VPN gateway.

- 1. Open Azure PowerShell
- 2. Get the IP address assigned to the VPN gateway:

```
Get-AzureRmPublicIpAddress -Name gwpip -ResourceGroupName
YOUR RESOURCE GROUP
```

Step 3. Configure IPsec IKEv2 Site-to-Site VPN on the CloudGen Firewall

Configure a site-to-site IKEv2 VPN tunnel on the CloudGen Firewall. The firewall is configured as the active partner.

- 1. Go to CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Site to Site.
- 2. Click the IPSEC IKEv2 Tunnels tab.
- 3. Click Lock.
- 4. Right-click the table and select **New IKEv2 tunnel**. The **IKEv2 Tunnel** window opens.
- 5. In the **Tunnel Name** field, enter your tunnel name.
- 6. Set Initiates tunnel to Yes.
- 7. Configure the **Authentication** settings:
 - Authentication Method Select Pre-shared key.
 - **Shared Secret** Enter the passphrase you used when creating the virtual network gateway connection in Step 1.11.

The shared secret can consist of small and capital characters, numbers, and nonalpha-numeric symbols, except the hash sign (#).



Authentication					
Authentication Method:	Pre-shared key	~	CA Root	-Use-All-Known-	\sim
Shared Secret	•••••		X509 Condition		Edit/Show
Server Certificate	-Use-Default-	\sim	Explicit X509		Ex/Import

- 8. Configure the **Phase 1** encryption settings:
 - Encryption Select AES-256.
 - Hash Meth. Select SHA.
 - DH Group Select Group 2.
 - Lifetime Enter 28800.
- 9. Configure the **Phase 2** encryption settings:
 - Encryption Select AES-256.
 - Hash Meth. Select SHA.
 - **DH Group** Select **Disable PFS**.
 - Lifetime Enter 3600.

Phase 1		Phase 2					
Encryption	AES256 🗸	Encryption	AES256 V				
Hash	SHA 🗸	Hash	SHA 🗸				
DH-Group	Group 2 🗸	DH-Group	Disable PFS 🗸 🗸				
Proposal Handling	Strict 🗸	Proposal Handling	Strict ~				
Lifetime (seconds)	28800	Lifetime (seconds)	3600				
		Traffic Volume (KB)	✓ unlimited 0				

- 10. In the **Network Settings** section, enable **Universal Traffic Selectors** to instruct the peer to route all traffic into the tunnel.
- 11. Configure the Local Network settings:
 - Local Gateway Enter the public IP address the Azure VPN Gateway is connecting to, or use 0.0.0.0 if you are using a dynamic IP address or if the appliance is hosted in Azure, AWS, or GCP.
 - **Network Address** Enter your local on-premise networks and click **Add**.
- 12. Configure the **Remote Network** settings:
 - **Remote Gateway** Enter the Gateway IP Address of the Azure VPN Gateway in Step 2.
 - **Network Address** Enter the Azure subnet(s) configured in the Azure Virtual Network and click **Add**.



Network Local			Network Remote		
Local Gateway:	0.0.0.0		Remote Gateway:	168.63.96.146	j
.ocal ID:			Remote ID:		
Network address (e.	g. 10.6.0.0/16)	+ ×	Network address (e.g	g. 10.6.0.0/16)	+ ×
10.0.1.0/24			10.2.1.0/28		
			10.2.2.0/24		

- 13. Click **OK**.
- 14. Click Send Changes and Activate.

Step 4. Create an Access Rule

Create a pass access rule to allow traffic from the local network to the remote network.

- 1. Go to CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Firewall Rules.
- 2. Click Lock.
- 3. Create a PASS access rule:
 - **Bi-Directional** Enable.
 - **Source** Select the local on-premises network(s).
 - Service Select the service you want to have access to the remote network, or select Any for complete access.
 - **Destination** Select the network object containing the remote Azure Virtual Network subnet(s).
 - Connection Method Select Original Source IP.

Barracuda CloudGen Firewall



_ \	Lan-2	-AzureVPNNetworks								
Pass Y	Allows	Allows unrestricted communication between TRUSTED LAN networks.								
🛹 🔽 Bi-Directional		💍 🗌 Dynamic Rule	2	🕘 🗌 Deactivate Rule						
Source VR Instance	default	✓ De	estination VR Inst	tance Same as Source Destination						
Source		Service								
Trusted LAN	-	Any	-	Azure Re	mote Networks	-				
Ref: Trusted LAN Networks		Ref: Any-TCP		172.16.0	0.0/24					
Ref: Trusted Next-Hop Netw	vorks	Ref: Any-UDP								
		Ref: ICMP								
		ALLIP								
Authenticated User		Policies		Connecti	ion Method					
	~	IPS Policy								
	-	Default Policy	\sim	Original S	source IP	~				
		Application Policy		Original	Source IP (sam	e port)				
		No AppControl								
		SSL Inspection Policy								
		N.A.	\sim							
		Schedule								
		Always	~							
		QoS Band (Fwd)								
		No-Shaping	\sim							
		QoS Band (Reply)								
		Like-Fwd	\sim							
					OK	Cancel				

- 4. Click **OK**.
- 5. Move the access rule up in the rule list, so that it is the first rule to match the firewall traffic.
- 6. Click Send Changes and Activate.

Your Barracuda CloudGen Firewall will now automatically connect to the Azure VPN Gateway.

Site-to-	Site Client-to-Site	(i) Status								@ Acce Cach	e Dro Cad	p che	Client Downloads	Selection
Tunnel	Name	Туре	Group	Info	State	Succ.	Fail	Last Access	Last Peer	Last Info	Last Duration	Last Client	Last OS	Last WSC
IPSEC	v2-AWS2AzureVPNGW	6			ACTIVE	1031	0	1h 25m 43s	168.63.96.146	Access Granted	1h 25m 43s	Unknown	Unknown	

Barracuda CloudGen Firewall



Figures

- 1. az_vpn_gw.png
- 2. GW_2.png
- 3. GW_3.png
- 4. GW_4.png
- 5. access rule01.png
- 6. GW_05.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.