

## How to Configure a Site-to-Site IPsec IKEv2 VPN Tunnel

<https://campus.barracuda.com/doc/79462888/>

The Barracuda CloudGen Firewall can establish IPsec VPN tunnels to any standard compliant IKEv2 IPsec VPN gateway. The site-to-site IPsec VPN tunnel must be configured with identical settings on both the firewall and the third-party IKEv2 IPsec gateway.



### Before You Begin

If not already present, configure the **Default Server Certificate** in **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**. For more information, see [VPN Settings](#).

### Step 1. Configure the VPN Service Listeners

Configure the IPv4 and IPv6 listener addresses for the VPN service.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Service Properties**.
2. Click **Lock**.
3. From the **Service Availability** list, select the source for the IPv4 listeners of the VPN service.
  - When selecting **Explicit**, click **+** for each IP address and enter the IPv4 addresses in the **Explicit Service IPs** list.
4. Click **+** to add an entry to the **Explicit IPv6 Service IPs**.
5. Select an IPv6 listener from the list of configured explicit IPv6 service IP addresses.

**Service IPs**

Service Availability: Explicit

Explicit Service IPs

62.99.0.40
194.93.0.10
10.20.0.3
10.0.10.3

Explicit Service IPv6s

ip6serv2 ( 2001:db8:1::10 )
ip6serv3 ( 2001:db8:1::20 )
ip6serv4 ( 2001:db8:1::30 )

6. Click **Send Changes** and **Activate**.

## Step 2. Create an IKEv2 IPsec Tunnel on the CloudGen Firewall

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. Enter a **Tunnel Name**.
6. Set **Initiates Tunnel**:
  - **Yes** - The firewall is the active unit and continuously attempts to connect to the remote VPN gateway until a VPN tunnel is established.
  - **No** - The firewall is the passive unit and waits for connection attempts from the remote VPN gateway.
7. Set **Restart SA on Close**:
  - **Yes** - Restart the connection if the tunnel terminates unexpectedly.
  - **No** - Close the VPN connection if the tunnel terminates unexpectedly.

**General**

Tunnel name	<input type="text" value="ExampleIKEv2Tunnel"/>	Initiates tunnel	<input checked="" type="radio"/> Yes	<input type="radio"/> No
Enabled	<input checked="" type="radio"/> Yes	Restart SA on Close	<input checked="" type="radio"/> Yes	<input type="radio"/> No

The combination of **Restart SA on Close** and **IKE Reauthentication** is not supported. This configuration needs to be avoided on both sides of the tunnel to achieve a stable connection.

8. Select the **Authentication Method**:
  - **Pre-shared key** - Enter the **Shared Secret** to use a shared passphrase to authenticate.
 

The shared secret can consist of small and capital characters, numbers, and non alpha-numeric symbols, except the hash sign (#).
  - **CA certificate** - Select a **Server Certificate**, **CA Root** certificate, and enter a **X509 Condition** to use certificate authentication.

- o **X509 certificate (explicit)** – Select a **Server Certificate** and import an **Explicit X509** certificate.

Authentication			
Authentication Method:	Pre-shared key	CA Root	-Use-All-Known-
Shared Secret	••••••••	X509 Condition	<input type="text"/> <input type="button" value="Edit/Show"/>
Server Certificate	-Use-Default-	Explicit X509	<input type="text"/> <input type="button" value="Ex/Import"/>

9. Select the **Phase 1** settings:

- o **Encryption** – Select the encryption algorithm: **AES, 3DES, Blowfish, or AES256.**
- o **Hash** – Select the hashing algorithm: **MD5, SHA, SHA256, or SHA512.**
- o **DH-Group** – Select the Diffie-Hellman Group. Supported groups are: 1, 2, 5, 14 - 30.
- o **Proposal Handling**
  - **Strict** – The effective encryption is strictly determined by the proposed set of **Encryption, Hash and Group.** The communication partner must agree with the proposed set; otherwise, no communication will be established due to a missing common encryption agreement.
  - **Negotiate** – This option lets a communication partner decrease the strength of the encryption if it cannot support the proposed encryption from the initiator.
- o **Lifetime (seconds)** – Enter the number of seconds until the IPsec SA is re-keyed.  
Default: 28800

10. Select the **Phase 2** settings:

- o **Encryption** – Select the encryption algorithm: **AES, 3DES, Blowfish, or AES256.**
- o **Hash** – Select the hashing algorithm: **MD5, SHA, SHA256, or SHA512.**
- o **DH-Group** – Select the Diffie-Hellman Group. Supported groups are: 1, 2, 5, 14 - 30.
- o **Proposal Handling**
  - **Strict** – The effective encryption is strictly determined by the proposed set of **Encryption, Hash and Group.** The communication partner must agree with the proposed set; otherwise, no communication will be established due to a missing common encryption agreement.
  - **Negotiate** – This option lets a communication partner decrease the strength of the encryption if it cannot support the proposed encryption from the initiator.
- o **Lifetime (seconds)** – Enter the number of seconds until the IPsec SA is re-keyed.  
Default: 3600.
- o **Lifetime (KB)** – Enter the number of KB after which the IPsec SA is re-keyed.

Phase 1		Phase 2	
Encryption	AES	Encryption	AES
Hash	MD5	Hash	MD5
DH-Group	Group 2	DH-Group	Group 2
Proposal Handling	Strict	Proposal Handling	Strict
Lifetime (seconds)	28800	Lifetime (seconds)	3600
		Traffic Volume (KB)	<input checked="" type="checkbox"/> unlimited 0

11. Select the IP Version of the local listener and the remote gateway.

- o **IP Version** – Click **IPv4** or **IPv6** to match the **Local Gateway** and **Remote Gateway** IP address IP versions.

**Network Settings**

IP Version  IPv4  IPv6

One VPN Tunnel per Subnet Pair     Force UDP Encapsulation    Next Hop Routing

Universal Traffic Selectors     IKE Reauthentication    Interface Index

## 12. (optional) Select **Advanced Network Settings**

- **One VPN Tunnel per Subnet Pair** - Creates a dedicated security association for each subnet pair. This is needed if the remote device is a Cisco ASA.
- **Force UDP Encapsulation** - Use UDP encapsulation (4500) for ESP traffic even if no NAT is detected.
- **Universal Traffic Selector** - Instruct peer to route all traffic into tunnel. This is needed if the remote device is a Checkpoint firewall.
- **IKE Reauthentication** - Reauthenticate during every IKE rekeying. This setting must be disabled if the remote device is a Microsoft Azure Dynamic VPN Gateway.

The combination of **Restart SA on Close** and **IKE Reauthentication** is not supported. This configuration needs to be avoided on both sides of the tunnel to achieve a stable connection.

- **Next Hop Routing** - Sets the next hop IP address for routed VPN traffic.
- **Interface Index** - The number of the virtual interface to be used for routed VPN.

**Network Settings**

IP Version  IPv4  IPv6

One VPN Tunnel per Subnet Pair     Force UDP Encapsulation    Next Hop Routing

Universal Traffic Selectors     IKE Reauthentication    Interface Index

## 13. Enter the **Network Local** settings:

- **Local Gateway** - Enter the external IP address of the firewall. If you are using a dynamic WAN IP address, enter 0.0.0.0.
- **Local ID** - Enter an IP address, FQDN, email, or a distinguished name. If left blank, the local gateway IP is used.
- **Network Address** - Add the local networks you want to reach through the VPN tunnel, and click **Add**.

## 14. Enter the **Network Remote** settings:

- **Remote Gateway** - Depending on the setting of **Initiate Tunnel**, this edit field accepts different input:
  - **Initiate Tunnel = Yes** - The input must be a hostname or IP address. No network IPs in CIDR notation are allowed.
  - **Initiate Tunnel = No** - The input must be an IP address or network address. If the remote appliance is using dynamic IP addresses, enter 0.0.0.0/0.
- **Remote ID** - Enter a unique ID. VPN tunnels without remote ID will not establish successfully.
- **Network Address** - Add the IP address of the remote network, and click **Add**.

Network Local	Network Remote
Local Gateway: <input type="text" value="194.93.0.17"/>	Remote Gateway: <input type="text" value="64.99.0.40"/>
Local ID: <input type="text"/>	Remote ID: <input type="text"/>
Network address (e.g. 10.6.0.0/16) <span style="float:right">+ -</span>	Network address (e.g. 10.6.0.0/16) <span style="float:right">+ -</span>
<input type="text" value="10.0.10.0/25"/>	<input type="text" value="10.0.1.0/24"/>

15. Enter the **Dead Peer Detection** settings:

- **Action:**
  - **None** – Disable DPD.
  - **Clear** – Connection with the dead peer is stopped, routes removed.
  - **Hold** – Connection is put in hold state.
  - **Restart** – Connection is restarted.
- **Delay (seconds)** – Enter the number of seconds after which an empty INFORMATIONAL message is sent to check if the remote peer is still available.

Dead Peer Detection	
Action	<input type="text" value="Restart"/>
Delay (seconds)	<input type="text" value="30"/>

16. Click **OK**.

17. Click **Send Changes and Activate**.

### Step 3. Create an IPsec Tunnel on the Remote Appliance

Configure the remote firewall or third-party VPN gateway with the same settings. Only the local and remote networks and the IP address for the remote VPN gateway must be interchanged.

### Step 4. Create Access Rules for VPN Traffic

To allow traffic in and out of the VPN tunnel, create a **Pass** access rule.

For more information, see [How to Create Access Rules for Site-to-Site VPN Access](#).

### Monitoring a VPN Site-to-Site Tunnel

To verify that the VPN tunnel was initiated successfully and traffic is flowing, go to **VPN > Site-to-Site** or **VPN > Status**.

Site-to-Site		Client-to-Site		Status		Access Cache		Drop Cache		Client Downloads		Selection		
Tunnel	Name	Type	Group	Info	State	Succ.	Fail	Last Access	Last Peer	Last Info	Last Duration	Last Client	Last OS	Last WSC
IPSEC	v2-AWS2AzureVPNGW				ACTIVE	1031	0	1h 25m 43s	168.63.96.146	Access Granted	1h 25m 43s	Unknown	Unknown	

Go to **LOGS** and select the **/<your\_vpn\_service>/IKEv2** log file.

AWSVIRT1\AWSVPN\ikev2 <new Log>

Select Log File: AWSVIRT1\AWSVPN\ikev2 Reload Log File Tree

Time	Type	TZ	Message
2015 11 16 09:14:19	16[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [del_sa] dstaddr = 168.63.96.146
2015 11 16 09:14:19	16[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [del_sa] deleting SPI {112797247} failed: SPI not found
2015 11 16 09:14:19	16[IKE]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> establishing CHILD_SA IPSEC-v2-AWS2AzureVPNGW(2)
2015 11 16 09:14:19	16[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> getting SPI for reqid {2}
2015 11 16 09:14:19	16[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> got SPI for reqid {2} = {497813479}
2015 11 16 09:14:19	16[ENC]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> generating CREATE_CHILD_SA request 29 [ SA No KE TSi TSr ]
2015 11 16 09:14:19	16[NET]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> sending packet: from 127.0.0.9[4500] to 168.63.96.146[4500] (332 bytes)
2015 11 16 09:14:19	16[ENC]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> generating INFORMATIONAL response 326 [ D ]
2015 11 16 09:14:19	16[NET]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> sending packet: from 127.0.0.9[4500] to 168.63.96.146[4500] (76 bytes)
2015 11 16 09:14:19	09[NET]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> received packet: from 168.63.96.146[4500] to 127.0.0.9[4500] (348 bytes)
2015 11 16 09:14:19	09[ENC]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> parsed CREATE_CHILD_SA response 29 [ SA No TSi TSr KE ]
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [add_sa] ktina_tname = "IPSEC-v2-AWS2AzureVPNGW"
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [add_sa] mode = TUNNEL
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [add_sa] src = 168.63.96.146:4500, dst = 127.0.0.9:4500
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [add_sa] direction = inbound
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [add_sa] site2site
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [add_sa] updating existing transport
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [add_sa] hash name: sha
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [add_sa] cipher name: aes
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [add_sa] KTINA_IJOREQ_SPI_NEW: dir:1 addr:0x92603fa8 spi:497813479
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [add_sa] enabled SA: IPSEC-v2-AWS2AzureVPNGW lifetime: 2736 3600
2015 11 16 09:14:19	09[KNL]	+00:00	<IPSEC-v2-AWS2AzureVPNGW[1]> [phion_vpns_send] succeeded

## Figures

1. ipsec\_IKEv2.png
2. vpn\_service\_listeners.png
3. S2S\_IKEv2\_01.png
4. S2S\_IKEv2\_02.png
5. S2S\_IKEv2\_03.png
6. network\_settings\_ipvX.png
7. network\_setting\_others.png
8. S2S\_IKEv2\_04.png
9. S2S\_IKEv2\_05.png
10. S2S\_IKEv2\_monitor.png
11. S2S\_IKEv2\_logfile.png

© Barracuda Networks Inc., 2020 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.