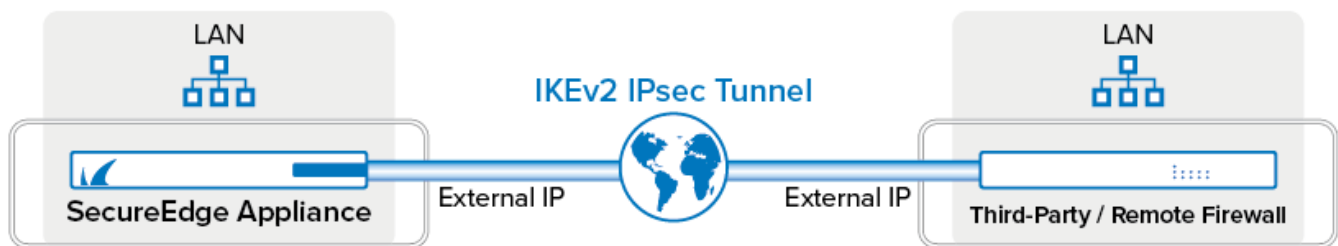


How to Configure a Site-to-Site IPsec IKEv2 VPN Tunnel on SecureEdge Using Static Routing

<https://campus.barracuda.com/doc/100370688/>

The Barracuda SecureEdge Manager allows you to configure a site-to-site IPsec IKEv2 tunnel on SecureEdge devices. You can connect to remote appliances or to third-party deployments that are capable of using IPsec IKEv2. IPsec IKEv2 tunnels can be created on all types of site devices, hardware or virtual. However, they cannot be created on IoT devices such as the Barracuda Secure Connector. You can also configure IPsec tunnels for all Edge Services: the Hosted Edge Service, Private Edge Service, and Edge Service for Virtual WAN. You can configure IKEv2 tunnels both for static routing and dynamic routing, where the remote networks will be propagated within SecureEdge via the Border Gateway Protocol (BGP). Only one IPsec IKEv2 tunnel can be configured for the same source and destination in the SecureEdge Manager.

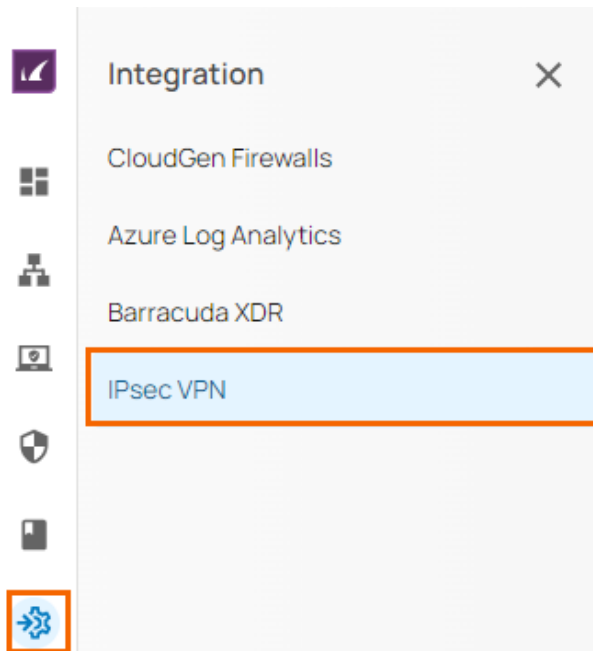


Requirements and Limitations

- For IPsec traffic, do not configure your SD-WAN policy with **ACTION** set to **PIN**; otherwise, site-to-site traffic over IPsec tunnels might be blocked.
- If you want to connect the stand-alone site to the Edge Service for vWAN for an IPsec tunnel using BGP, you must first delete the stand-alone site configuration completely and re-configure the same settings via the new site setup wizard.
- If you configure an IPsec IKEv2 VPN tunnel with BGP enabled, you can add more than one destination. However, you must ensure that two destinations of the same tunnel do not have the same remote gateway value.

Step 1. Create an IKEv2 IPsec Tunnel on SecureEdge

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace you want to configure the IPsec IKEv2 tunnel for.
3. Go to **Integration > IPsec VPN**.



4. The **IPsec VPN** page opens. To add tunnel, click **Add IPsec Tunnel**.

Demo Enterprises Inc/Production
Integration > IPsec VPN

Add IPsec Tunnel

Add filter Edit columns

NAME	ENABLED	SECUREEDGE PEER	REMOTE GATEWAY	TYPE
WestEurope	✓	Austria (Want)	myvpngateway2.westeurope.cl... myvpngateway1.westeurope.cl...	IPSec IKEv2
UAE	✓	Dubai (Etisalat)	20.35.72.11	IPSec IKEv2
EastUS	ⓘ	UnitedStates	myvpngateway.eastus.cloudap...	IPSec IKEv2
WestUS	✓	UnitedStates	myvpngateway.westus.cloudap...	IPSec IKEv2
BrazilSouth	✓	Brazil	myvpngateway.brazilsouth.cl...	IPSec IKEv2

5. The **Create IPsec Tunnel** window opens.

6. In the **General** tab, specify values for the following:

- **Enable** – Click to enable/disable tunnel status.
- **Initiates** – Initiates tunnel. Click to enable/disable.
 - If enabled, the appliance is the active unit and continuously attempts to connect to the remote VPN gateway until a VPN tunnel is established.
 - If disabled, the appliance is the passive unit and waits for connection attempts from the remote VPN gateway.

In the **GENERAL INFORMATION** section, specify values for the following:

- **Name** – Enter a unique tunnel name.
- **Description** – Enter a brief description.

In the **AUTHENTICATION** section, specify values for the following:

- **Authentication** – Select the authentication method from the drop-down menu.
- **Shared Secret** – Enter the shared secret to use a shared passphrase to authenticate.
 The shared secret can consist of small and capital characters, numbers, and non-alphanumeric symbols, except the hash sign (#).

Create IPsec Tunnel ×

1

2

3

4

5

General

Source/Destination

Phases

Network

Success

To create a new tunnel go through the following settings to configure it.

i

 Enable

☒

i

 Initiates

☐

GENERAL INFORMATION

i

 Name *

WestEurope

i

 Description

Campus IPsec

AUTHENTICATION

i

 Authentication *

Pre-shared key

i

 Shared Secret *

.....

Next

7. Click **Next**.

8. In the **Source/Destination** tab, specify values for the following:

- **Enable BGP** – Click to disable.

In the **SOURCE** section, specify values for the following

- **Type** – Select the type from the drop-down list. You can choose either **Edge Service** or **Site**.
- **Peer** – Select the peer from the drop-down list.
- **WAN Interface** – Select the WAN interface from the drop-down list.
- **Local ID** – Enter the local ID.
- **Network Addresses** – Add the IP address of the local network, and click +.

In the **DESTINATION** section, specify values for the following:

- **Remote Gateway** – Enter a remote gateway.
- **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 +.

Create IPsec Tunnel
✕

1 ☒ General
2 ☐ Source/Destination
3 ☐ Phases
4 ☐ Network
5 ☐ Success

Configure the source and destination of the tunnel that you want to add.

i
Enable BGP

☐

SOURCE

Type *

Edge Service

Peer *

Austria

WAN Interface

Wan1

i Local ID

WestEuropeWAN1

i Network Addresses *

10.14.40.0/24

✕

+

DESTINATION

i Remote Gateway *

myvpngateway1.westeurope.cl

i Remote ID

myvpngateway1.westeurope.cl

9. Click **Next**.

10. In the **Phases** tab, specify values for the following:

In the **PHASE 1** section, specify the values for the following:

- **Encryption** – Select the encryption algorithm from the drop-down list. You can choose between **AES**, **3DES**, **Blowfish**, or **AES256**.
- **Hash** – Select the hashing algorithm from the drop-down list. You can choose between **MD5**, **SHA**, **SHA256**, or **SHA512**.
- **DH-Group** – Select the Diffie-Hellman Group from the drop-down list. Supported groups are: 1, 2, 5, 14 - 24.
- **Proposal Handling** – Select the proposal handling from the drop-down list. You can choose between the following:
 - **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.

- **Lifetime** – Enter the number of seconds until the IPsec SA is re-keyed. Default: 28800

Create IPsec Tunnel ✕

✓ General
✓ Source/Destination
3 Phases
4 Network
5 Success

The Tunnel offers 2 phases. Setup your preferred security settings for each of these phases.

PHASE 1

Encryption *	<div style="border: 1px solid orange; padding: 2px;">AES256 ▼</div>
Hash *	<div style="border: 1px solid orange; padding: 2px;">SHA256 ▼</div>
DH Group *	<div style="border: 1px solid orange; padding: 2px;">Group 24 ▼</div>
i Proposal Handling *	<div style="border: 1px solid orange; padding: 2px;">Strict ▼</div>
i Lifetime *	<div style="border: 1px solid orange; padding: 2px;">28800</div>

In the **PHASE 2** section, specify the values for the following:

- **Encryption** – Select the encryption algorithm from the drop-down list. You can choose between **AES**, **3DES**, **Blowfish**, or **AES256**.
- **Hash** – Select the hashing algorithm from the drop-down list. You can choose between **MD5**, **SHA**, **SHA256**, **SHA512**, or **GCM**.

Note that the GCM hash algorithm can be used only in combination with one of the AES encryption algorithms (such as AES, AES256, or AES512).

- **DH-Group** – Select the Diffie-Hellman Group from the drop-down list. You can choose either **Disable PFS** or supported groups. Supported groups are: 1, 2, 5, 14 - 24.
- **Proposal Handling** – Select the proposal handling from the drop-down list. You can choose between the following:
 - **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.
- **Life time** – Enter the number of seconds until the IPsec SA is re-keyed. Default: 3600.
- **Traffic Volume Enabled** – Click to enable/disable.
 - If enabled, specify the value for the following:
 - **Traffic Volume KB** – Enter the number of KB after which the IPsec SA is re-keyed.

PHASE 2

Encryption *	<input type="text" value="AES256"/>
Hash *	<input type="text" value="SHA256"/>
DH Group *	<input type="text" value="Disable PFS"/>
<i>i</i> Proposal Handling *	<input type="text" value="Strict"/>
<i>i</i> Lifetime *	<input type="text" value="3600"/>
<i>i</i> Traffic Volume Enabled	<input type="checkbox"/>

11. Click **Next**.

12. In the **Network** tab, specify the values for the following:

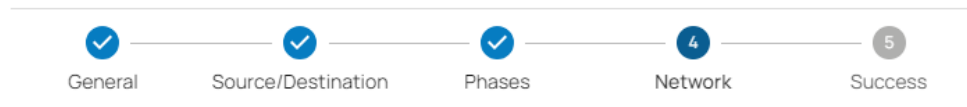
In the **NETWORK SETTINGS** section, specify the values for the following:

- **One VPN Tunnel Per Subnet Pair** – Click to enable/disable. This creates a dedicated security association for each subnet pair.
- **Universal Traffic Selectors** – Click to enable/disable. Instruct peer to route all traffic into tunnel.
- **Force UDP Encapsulation** – Click to enable/disable. Use UDP encapsulation (4500) for ESP traffic even if no NAT is detected.
- **IKE Reauthentication** – Click to enable/disable. Reauthenticate during every IKE rekeying. This setting must be disabled if the remote device is a Microsoft Azure Dynamic VPN Gateway.

In the **DEAD PEER DETECTION** section, specify the values for the following:


- **Action When Detected** – Select the action from the drop-down list. You can choose between the following:
 - **None** – Disable DPD.
 - **Clear** – Connection with the dead peer is stopped, and routes removed.
 - **Restart** – Connection is restarted.
- **Delay** – Enter the number of seconds after which an empty INFORMATIONAL message is sent to check if the remote peer is still available. Note: DPD Delay is required when detected DPD action is set anything other than **None**.

Create IPsec Tunnel



Configure the Network Settings. These are advanced options and is not mandatory for a general tunnel.

NETWORK SETTINGS

 One VPN Tunnel per Subnet Pair ☒

 Universal Traffic Selectors ☒

 Force UDP Encapsulation ☒

 IKE Reauthentication ☐

DEAD PEER DETECTION

 Action when detected

 Delay

[Back](#)[Save](#)

13. Click **Save**.

14. Verify that your IPsec tunnel configuration has been created successfully and click **Finish**.

Create IPsec Tunnel



New IPsec Tunnel successfully created

[Finish](#)

After the configuration is complete, you can see a new IPsec tunnel is shown on the **IPsec VPN** page, and the status of the field names (e.g., **Enabled**) can be verified.

Demo Enterprises Inc/Production
Integration > IPsec VPN Add IPsec Tunnel

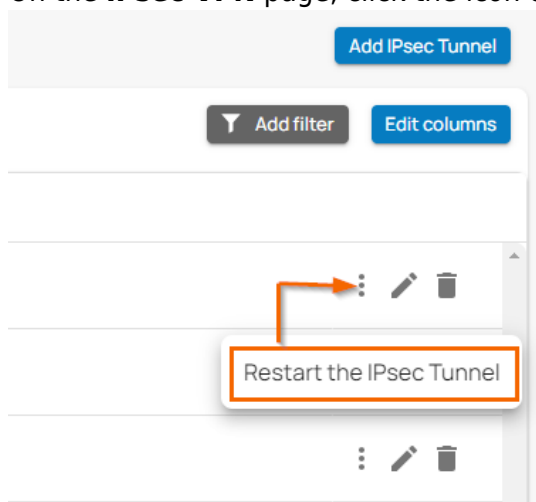
Add filter Edit columns

NAME	ENABLED	SECUREEDGE PEER	REMOTE GATEWAY	TYPE
WestEurope	✓	Austria (Wan1)	myprngateway2.westeurope.cl... myprngateway1.westeurope.cl...	IPSec IKEv2
UAE	✓	Dubai (Etisalat)	20.36.72.11	IPSec IKEv2
EastUS	ⓘ	UnitedStates	myprngateway.eastus.cloudap...	IPSec IKEv2
WestUS	✓	UnitedStates	myprngateway.westus.cloudap...	IPSec IKEv2
BrazilSouth	✓	Brazil	myprngateway.brazilsouth.cl...	IPSec IKEv2

(Optional) Restart the IPsec Tunnel

If you must restart the IPsec tunnel, proceed with the following steps:

1. On the **IPsec VPN** page, click the icon of three vertical dots to restart the IPsec tunnel.

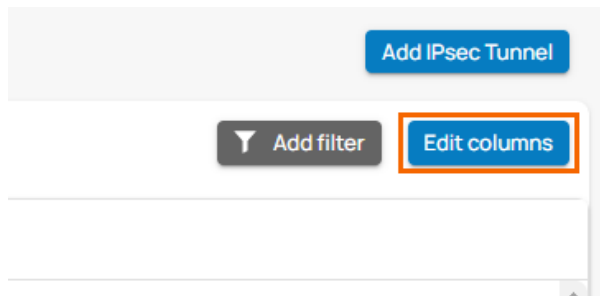


2. Click **Restart the IPsec Tunnel**.

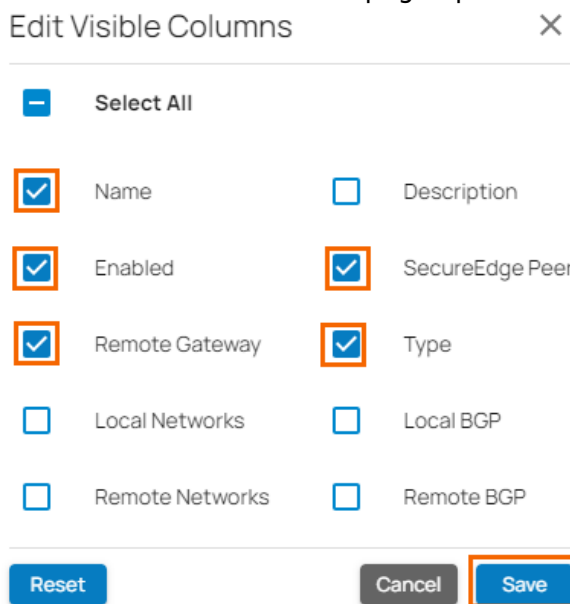
To restart the IPsec tunnel that is not initiated from the SecureEdge Manager, you may need to initiate the remote-side tunnel to bring the IPsec tunnel back up.

(Optional) Edit Visible Columns

1. To get more detailed information on IPsec VPN, click **Edit columns**.



2. The **Edit Visible Columns** page opens.



3. Select the field names you wish to display the columns for, and click **Save**.

Step 2. Create an IPsec Tunnel with the Remote Appliance

Configure the remote appliance 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. You can create a pass access rule on the remote appliance to allow traffic through the VPN tunnel.

Monitoring a VPN Site-to-Site Tunnel

To verify that the VPN tunnel was initiated successfully and traffic is flowing, proceed with the following steps:

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace containing your site.

3. Go to **Infrastructure > Sites**. The **Sites** page opens.
4. Select the site you want to verify the status for. Click on the arrow icon next to the site.

demo Enterprises Inc Production





Infrastructure > Sites

[New site](#)

[Add filter](#) [Edit columns](#)

	NAME	SERIAL	MODEL	EDGE SERVICE	CLOUD WAN	CONNECTION STATUS	PEERING ADDRESS	LANS	WANS
✓	Innsbruck	327437	T200C	Austria	Private Edge	Online	169.254.0.3	10.14.0.1/24 10.14.64.1/18	T-Mobile-Austria... Telekom-Austria... UPC-Austria (192...
✓	Johannesburg	714821	T200C	South Africa	Private Edge	Online	169.254.0.2	10.14.0.1/24 10.14.64.1/18	Supersonic (Dyn... Vodacom (WWAN)

5. In the **Site** menu, the **Dashboard** page opens. You can see the status of all VPN tunnels for the corresponding sites.

VPN Tunnels				
STATUS	NAME	PEER	LOCAL	TYPE
 Up	wanhub-S5	109.224.194.180	172.16.10147	TINA Site-2-Site
 Up	wanhub-S5	109.224.194.148	172.16.10224	TINA Site-2-Site
 Up	wanhub-S5	109.224.194.114	172.16.1074	TINA Site-2-Site
 Up	wanhub-S5	109.224.194.107	172.16.1071	TINA Site-2-Site

Edit an Existing IPsec VPN Tunnel

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace you want to edit the IPsec IKEv2 tunnel for.
3. Go to **Integration > IPsec VPN**.
4. The **IPsec VPN** page opens. Click on the pencil icon next to the IPsec IKEv2 tunnel you want to edit.

Demo Enterprises Inc./Production

Integration > IPsec VPN

Add IPsec Tunnel

Add filter

Edit columns

NAME	ENABLED	SECUREDOE PEER	REMOTE GATEWAY	TYPE
WestEurope		Austria (Wan1)	<div>myvpngateway2.westeurope.cl...</div> <div>myvpngateway1.westeurope.cl...</div>	IPSec IKEv2
UAE		Dubai (Etisalat)	20.36.72.11	IPSec IKEv2

5. The **Edit IPsec Tunnel** window opens. Edit the value you are interested in.
6. Click **Save**.

Remove an Existing IPsec VPN Tunnel

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace you want to remove the IPsec IKEv2 tunnel for.
3. Go to **Integration > IPsec VPN**.
4. The **IPsec VPN** page opens. Click on the trashcan icon next to the IPsec IKEv2 tunnel you want to remove.

Demo Enterprises Inc/Production
Integration > IPsec VPN

Add IPsec Tunnel

Add filter Edit columns

NAME	ENABLED	SECUREEDGE PEER	REMOTE GATEWAY	TYPE	
WestEurope	✓	Austria (Wan1)	myvpngateway2.westeurope.cl... myvpngateway1.westeurope.cl...	IPsec IKEv2	⋮ ✎ 🗑
UAE	✓	Dubai (Etisalat)	20.36.72.11	IPsec IKEv2	⋮ ✎ 🗑

5. The **Delete IPsec Tunnel <Name of Tunnel>** window opens.

Delete IPsec Tunnel UAE

Are you sure you want to delete this IPsec Tunnel?

Cancel

Ok

6. Click **Ok** to confirm.

Figures

1. se_ipsec_ikev2.png
2. gotoIPSecVPN.png
3. AddTunnel.png
4. IPsec-general.png
5. ipsec-src-des.png
6. IPsec-phase1.png
7. Ipsec-phase2.png
8. NetworkSettings.png
9. ClickFinish.png
10. IPsec VPN Tunnel.png
11. three.dots.png
12. EditColumn.png
13. ipsec-editcol.png
14. Sites.png
15. VPN-Status.png
16. Ipsec-EditTunnel.png
17. Ipsec-DeleteTunnel.png
18. ClickOK.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.