

How to Connect Barracuda SecureEdge to Teridion via Dynamic Routing (BGP) over IPsec

<https://campus.barracuda.com/doc/101713064/>

Barracuda SecureEdge Manager allows you to connect SecureEdge to Teridion via BGP over IPsec. Teridion Connect provides numerous PoPs (Points of Presence) across the globe, including China, to allow access to their network backbone. Barracuda SecureEdge can connect to the TCR (Teridion Cloud Router) deployed in one of the PoPs by using IPsec to leverage their backbone to improve connectivity. For more information, visit the [Teridion website](#).

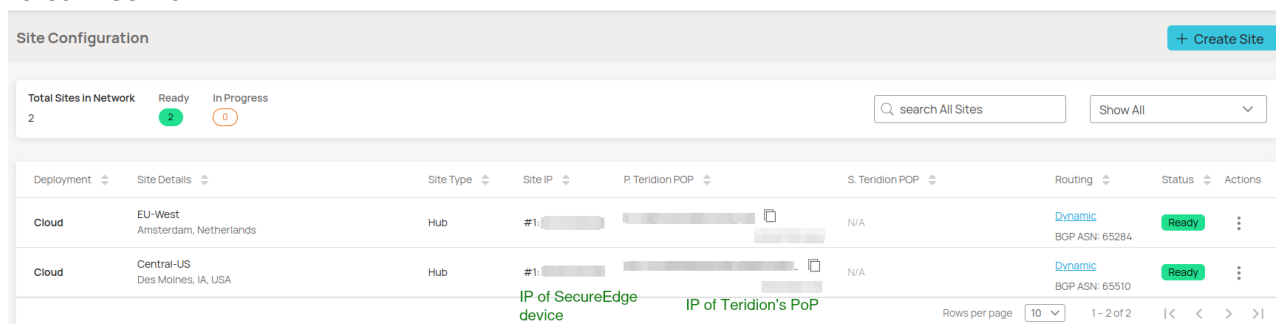
Before You Begin

- Deploy and set up your Teridion infrastructure. For assistance on the Teridion setup, please [contact Teridion](#).

Step 1. Collect Site Information

Log into your Teridion portal and collect the following information:

1. From the **Site Configuration** page, collect the information on the PoE IP from the site you need to connect to.



Deployment	Site Details	Site Type	Site IP	P. Teridion POP	S. Teridion POP	Routing	Status	Actions
Cloud	EU-West Amsterdam, Netherlands	Hub	#1: [redacted]	[redacted]	N/A	Dynamic BGP ASN: 65284	Ready	⋮
Cloud	Central-US Des Moines, IA, USA	Hub	#1: [redacted]	[redacted]	N/A	Dynamic BGP ASN: 65510	Ready	⋮

IP of SecureEdge device IP of Teridion's PoP

Site Details

Site Configuration ▶ View & Edit EU-West SAVE CHANGES ✕

Site Details Tunnel Type High Availability Gateways Site Type Routing IPSEC Bandwidth

1

Step 1 Site Name

Select a name for your site

EU-West

Alphabetic characters and special symbols [~!@#%^&*] only, must start with a character. Min 5 characters.

Step 2 Site Location

Select a location for your site

Amsterdam, Netherlands

• Tunnel type

Site Configuration ▶ View & Edit EU-West SAVE CHANGES ✕

Site Details Tunnel Type High Availability Gateways Site Type Routing IPSEC Bandwidth

2

Tunnel Type

Select a tunneling type for your site

☒ IPSEC

☐ GRE

Routing Method

Select a routing type for your site

☐ Route Based

☒ Dynamic (BGP)

☐ Policy Based

IPSEC (Internet Protocol Security) is a secure network protocol suite that authenticates and encrypts the packets of traffic to provide secure communication between two nodes over an IP network.

BGP traffic is routed through the tunnel based on dynamic protocol.

Site to Internet (BGP) the default Gateway is published by Teridion.

• High Availability (Optional)

• Gateways

◦ FQDN

Site Configuration ▶ View & Edit EU-West SAVE CHANGES ✕

Site Details Tunnel Type High Availability Gateways Site Type Routing IPSEC Bandwidth

4

FQDN

GW #1

FQDN Identifier

Create FQDN for Teridion POP/s

Primary FQDN

P - .d1.teridioncloud.net

Secondary FQDN

S - .d1.teridioncloud.net

Teridion Local ID

Select an option for local ID per your router settings

Gateway #1

☒ FQDN ☐ Send as text

FQDN ID is recommended enter a string for FQDN creation to be used for connecting to Teridion POPs, if not filed, Teridion will provide you with one. When configuring the site Gateway, use the Teridion Router FQDN for the IPsec connection IP and ID.

Local ID the Teridion router will always use the designated FQDN for its local ID. If the gateway software is not able to resolve the ID field FQDN to IP, select "send as text" option; in that case, the Teridion Router will send/validate its own FQDN as a text string for IPsec ID.

◦ Gateways IPs

Site Configuration ▶ View & Edit EU-West SAVE CHANGES ✕

Site Details Tunnel Type High Availability Gateways Site Type Routing IPSEC Bandwidth

✓ ✓ ✓ 4 ✓ ✓ ✓ ✓

FQDN

GW #1

General

Monitoring

Tunnels

General Details
Set up Gateway #1

Gateway #1 IP address / FQDN ✓ Entry IP is pingable
Must be a valid IP address / FQDN

IP of the SecureEdge device

Remote ID Resolve as IP / FQDN

Pre-shared secret

• Transfer Network

Site Configuration ▶ View & Edit EU-West SAVE CHANGES ✕

Site Details Tunnel Type High Availability Gateways Site Type Routing IPSEC Bandwidth

✓ ✓ ✓ 4 ✓ ✓ ✓ ✓

FQDN

GW #1

General

Monitoring

Tunnels

Teridion Primary POP 169.254.0.1

P. Tunnel Subnet 169.254.0.0 /30

GW #1 169.254.0.2 ☐ Monitor

✕ ————— ✕

• Dynamic Routing with BGP

Site Configuration ▶ View & Edit EU-West SAVE CHANGES ✕

Site Details Tunnel Type High Availability Gateways Site Type Routing IPSEC Bandwidth

✓ ✓ ✓ ✓ 6 ✓ ✓ ✓

General

Route Controls

BFD

Dynamic (BGP) Routing
Please set the BGP values for your site

Route Hops ☒ Single Hop ☐ Multi Hop

Site ASN 65534 Teridion ASN 64512

Keepalive (Sec) 3 Hold-time (Sec) 15

BGP password
Password may contain letters or digits, and be 0

Routing Hops Setup according to your CPE settings. Please note that hop settings affect both BGP & BFD on Teridion side.

Single-hop means that the TCP session must be established between the directly connected BGP peers.

Multi-hop means that BGP peers are not directly connected to each other, and the TCP session is established between them using an intermediate device or router.

• IPsec IKEv2 Settings

◦ IPsec Phase 1

Site Configuration ▶ View & Edit EU-West **SAVE CHANGES** ✕

Site Details Tunnel Type High Availability Gateways Site Type Routing IPSEC Bandwidth

✓ ✓ ✓ ✓ ✓ 7 ✓

IPSEC

☐ Default ☒ Custom

Phase 1

IKE version
☐ 1 ☒ 2

DPD delay/interval (Sec)

Encryption

Diffie-Hellman group

IPSEC mode
☒ N/A

DPD timeout (Sec)

Authentication

Lifetime (Sec)

Phase 1 is used to protect IKE messages that are exchanged between two IKE peers, or security endpoints.

Phase 2 is used to protect IP traffic, as specified by the security policy for a specific type of traffic, between two data endpoints.

IKEv2
 DPD delay/interval Sets the duration of tunnel idleness before liveness check is triggered.
 DPD timeout Sets the retransmissions timeout of the liveness-check.
 The tunnel will be considered down after DPD delay/interval + DPD timeout

IPsec Phase 2

Site Configuration ▶ View & Edit EU-West **SAVE CHANGES** ✕

Site Details Tunnel Type High Availability Gateways Site Type Routing IPSEC Bandwidth

✓ ✓ ✓ ✓ ✓ 7 ✓

Diffie-Hellman group Lifetime (Sec)

☒ Responder only

Phase 2

Encryption Authentication

PFS group (Sec) Lifetime (Sec)

The tunnel will be considered down after DPD delay/interval + DPD timeout

In this example, we have collected the following settings:

- **PoE (IP Teridion Router):** 52.252.228.31
- **SiteID (Firewall Internal IP):** 10.2.0.4
- **Gateway #1 IP (Firewall Public IP):** 23.99.253.105
- **Transfer Network TCR IP:** 169.254.0.1/30
- **Transfer Network Gateway IP:** 169.254.0.2/30

IKEv2 Authentication Settings

Phase 1		Phase 2	
Encryption	AES128	Encryption	AES256
Hash	MD5	Hash	MD5
DH-Group	Group 5	DH-Group	Group5
Proposal Handling	Strict	Proposal Handling	Strict
Lifetime [s]	28800	Lifetime	3600

BGP

- **Teridion ASN:** 64512
- **Site ASN:** 65534

Step 2. Configure IPsec IKEv2 over BGP

On Barracuda SecureEdge, do the following:

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 (Wantl)	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. In the **General** tab, specify values for the following:
 - **Enable** – Click to enable tunnel status.
 - **Initiates** – Initiates tunnel. Click to enable.

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 pre-shared key.
- **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 *

WestEuropeTunnel

i

 Description

SE-Teridion integration via BGP

AUTHENTICATION

i

 Authentication *

Pre-shared key

i

 Shared Secret *

.....

Next

6. Click **Next**.

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

- **Enable BGP** - Click to enable.

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

- **Type** - Select **Edge Service** or **Site**.
- **Peer** - Select the peer on which the tunnel will be configured from the drop-down list.
- **WAN Interface** - Select the WAN interface from the drop-down list. Note that this is not applicable for the Edge Service for Virtual WAN.
- **Local ID** - Enter the local ID.
- **Peering Address** - Enter the peering address of the Transfer Network in CIDR format: 169.254.0.2/30
- **ASN** - Enter the ASN of the local side, e.g., 65534

Create IPsec Tunnel ×

1

2

3

4

5

General

Source/Destination

Phases

Network

Success

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

Enable BGP ☒

SOURCE



Type *

Peer *

WAN Interface

Local ID


Peering Address *



ASN *  

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

- **Remote Gateway** - Enter your PoE IP for TCR, e.g., 52.252.228.31
- **Remote ID** - Enter your PoE IP for TCR, e.g., 52.252.228.31
- **Peering Address** - Enter the peering address of the Teridion BGP server, e.g., 169.254.0.1
- **ASN** - Enter the ASN of the remote side, e.g., 64512

DESTINATION

Destinations + 

52.252.228.31	<p>Remote Gateway *</p> <p>52.252.228.31</p> <p>Remote ID</p> <p>52.252.228.31</p> <p>Peering Address *</p> <p>169.254.0.1</p> <p>ASN *</p> <p>64512  </p>
---------------	--

Back **Next**

8. Click **Next**.

9. In the **Phases** tab, configure the following settings.

To configure **PHASE 1** encryption settings matching your Teridion setup, specify values for the following:

- **Encryption** – Select **AES**.
- **Hash** – Select **MD5**,
- **DH-Group** – Select **Group 5**.
- **Proposal Handling** – Select **Strict**.
- **Lifetime** – Enter 28800

To configure **PHASE 2** encryption settings matching your Teridion setup, specify values for the following:

- **Encryption** – Select **AES-256**
- **Hash** – **MD5**.
- **DH-Group** – Select **Group 5**.
- **Proposal Handling** – Select **Strict**.
- **Life time** – Enter 3600.
- **Traffic Volume Enabled** – Click to disable.

Create IPsec Tunnel ×

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

PHASE 1

i Encryption * AES

i Hash * MD5

i DH Group * Group 5

i Proposal Handling * Strict

i Lifetime * 28800

PHASE 2

i Encryption * AES256

i Hash * MD5

i DH Group * Group 5

i Proposal Handling * Strict

i Lifetime * 3600

10. Click **Next**.

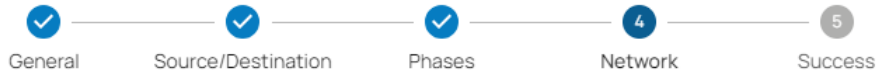
11. The **Network** blade opens. In the **NETWORK SETTINGS** section, specify values for the following:

- **Force UDP encapsulation** – Click to disable.
- **IKE Reauthentication** – Click to enable.

In the **DEAD PEER DETECTION** section, specify values for DPD to match your Teridion configuration.

- **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

 Force UDP Encapsulation ☐

 IKE Reauthentication ☒

DEAD PEER DETECTION

 Action when detected

 Delay

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

12. Click **Save**.

13. Verify that your IPsec tunnel configuration has been created successfully.

Create IPsec Tunnel



New IPsec Tunnel successfully created

[Finish](#)

14. Click **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](#)

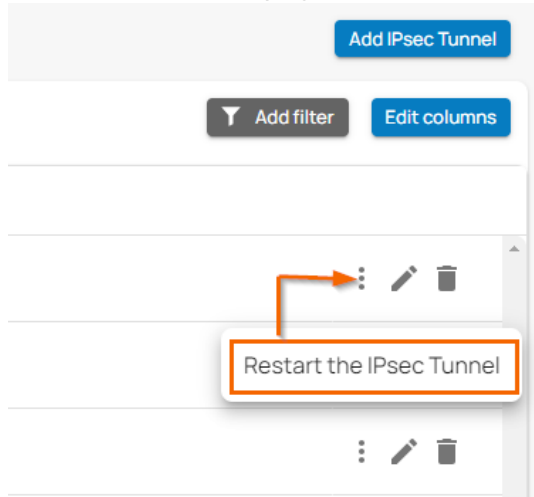
[Add filter](#) [Edit columns](#)

NAME	ENABLED	SECUREEDGE PEER	REMOTE GATEWAY	TYPE
WestEurope		Austria (Wan1)	myvpngateway2.westeurope.cl... myvpngateway1.westeurope.cl...	IPSec IKEv2
UAE		Dubai (Etisalat)	20.36.72.11	IPSec IKEv2
EastUS		UnitedStates	myvpngateway.eastus.cloudap...	IPSec IKEv2
WestUS		UnitedStates	myvpngateway.westus.cloudap...	IPSec IKEv2
BrazilSouth		Brazil	myvpngateway.brazilsouth.cl...	IPSec IKEv2

(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.

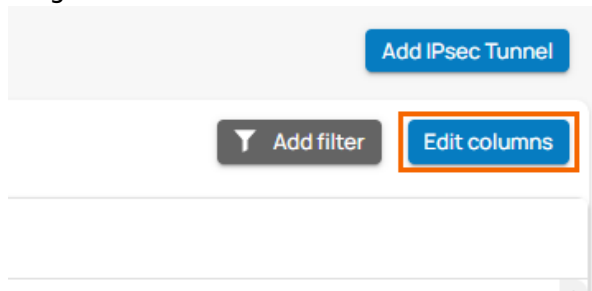


2. Click **Restart the IPsec Tunnel**.

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.

Edit Visible Columns ×

☐ Select All

<input checked="" type="checkbox"/> Name	<input type="checkbox"/> Description
<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> SecureEdge Peer
<input checked="" type="checkbox"/> Remote Gateway	<input checked="" type="checkbox"/> Type
<input type="checkbox"/> Local Networks	<input type="checkbox"/> Local BGP
<input type="checkbox"/> Remote Networks	<input type="checkbox"/> Remote BGP

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

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

NAME	ENABLED	SECUREEDGE PEER	REMOTE GATEWAY	TYPE	
WestEurope		Austria (Wan1)	myvpn-gateway2.westeurope.cl... myvpn-gateway1.westeurope.cl...	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.

- Go to **Integration > IPsec VPN**.
- 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	⋮ ✎ 🗑

- 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

- Click **Ok** to confirm.

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:

- Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
- In the left menu, click the **Tenants/Workspaces** icon and select the workspace containing your site.
- Go to **Infrastructure > Sites**. The **Sites** page opens.
- 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 VWAN	CONNECTION STATUS	PEERING ADDRESS	LANs	WANs
✓	Innsbruck	527457	T200C	Austria	Private Edge	Online	169.254.0.3	1014.01/24 1014.64/1/8	T-Mobile-Austria... Telekom-Austria... UPC-Austria (192...
✓	Johannesburg	714821	T200C	SouthAfrica	Private Edge	Online	169.254.0.2	1014.01/24 1014.64/1/8	Supersonic (Dyna... Vodacom (WWAN)

- 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

Figures

1. Site-Configuration.png
2. SiteNameLocation.png
3. DynamicBGP.png
4. TeridionLocalID.png
5. Gateways.png
6. TransferNetwork.png
7. ASN.png
8. IpsecPhase1.png
9. IpsecPhase2.png
10. AddTunnel.png
11. BGP-general.png
12. BGP-SourceSetting.png
13. BGP-DestinationSettings.png
14. Se-IPsec-phase.png
15. BGP-network.png
16. ClickFinish.png
17. IPsec VPN Tunnel.png
18. three.dots.png
19. EditColumn.png
20. ipsec-editcol.png
21. Ipsec-EditTunnel.png
22. Ipsec-DeleteTunnel.png
23. ClickOK.png
24. Sites.png
25. VPN-Status.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.