

How to Connect the Barracuda CloudGen Firewall to Teridion via GRE Tunnel

<https://campus.barracuda.com/doc/99123636/>

Teridion Connect provides numerous PoPs (Points of Presence) across the globe, including China, to allow access to their network backbone. The Barracuda CloudGen Firewall can connect to the TCR (Teridion Cloud Router) deployed in one of the PoPs by using IPsec or GRE tunneling to leverage their backbone to improve the connectivity. In addition, BGP can be used as a dynamic routing protocol to learn and propagate networks. For more information, visit the [Teridion website](#).

Connect a Barracuda CloudGen Firewall to the Teridion Network via GRE Tunnel

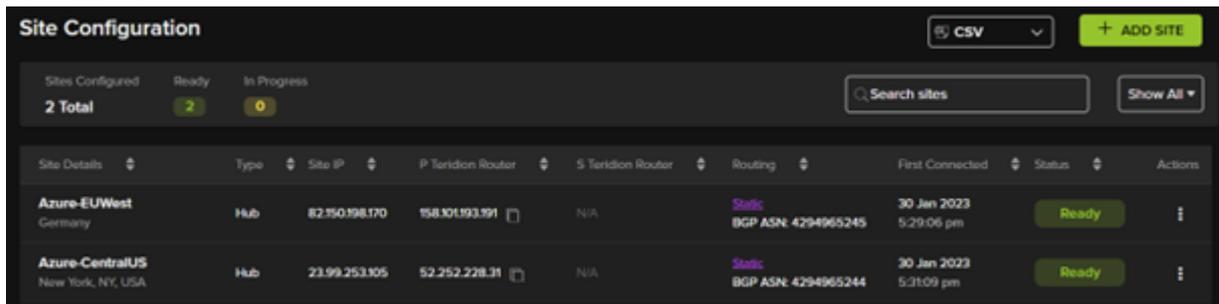
Before You Begin

- 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:

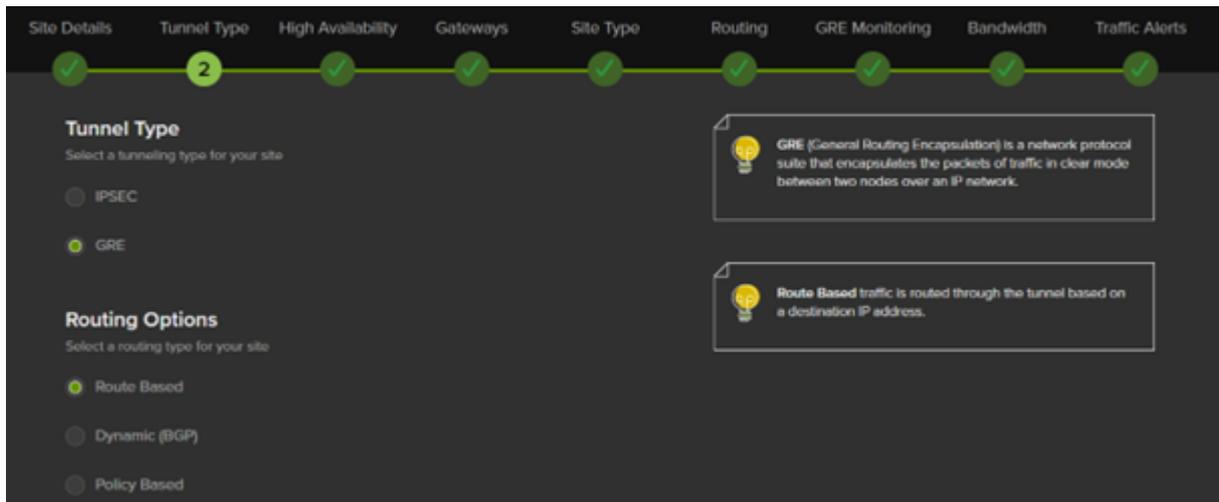
1. From the **Site Configuration**, collect the information on the PoE IP from the site you need to connect to.



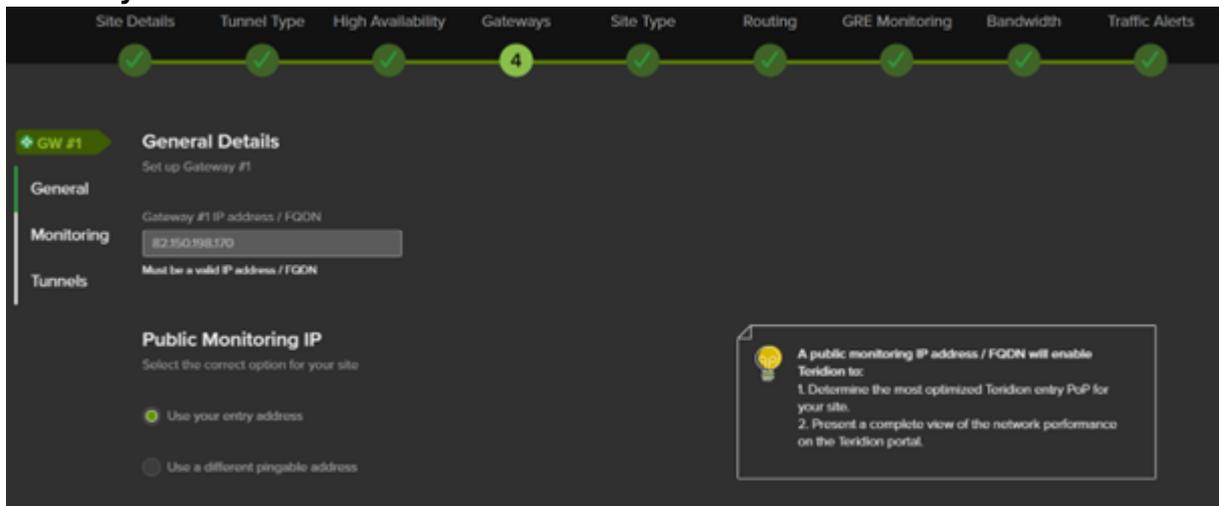
The screenshot shows the 'Site Configuration' interface in the Teridion portal. It features a table with columns for Site Details, Type, Site IP, IP Teridion Router, S Teridion Router, Routing, First Connected, Status, and Actions. Two sites are listed: 'Azure-EUWest' (Germany) and 'Azure-CentralUS' (New York, NY, USA). Both sites are marked as 'Ready'.

Site Details	Type	Site IP	IP Teridion Router	S Teridion Router	Routing	First Connected	Status	Actions
Azure-EUWest Germany	Hub	82.150.198.170	158.301.193.191	N/A	Static BGP ASN: 4294965245	30 Jan 2023 5:29:06 pm	Ready	
Azure-CentralUS New York, NY, USA	Hub	23.99.253.105	52.252.228.31	N/A	Static BGP ASN: 4294965244	30 Jan 2023 5:31:09 pm	Ready	

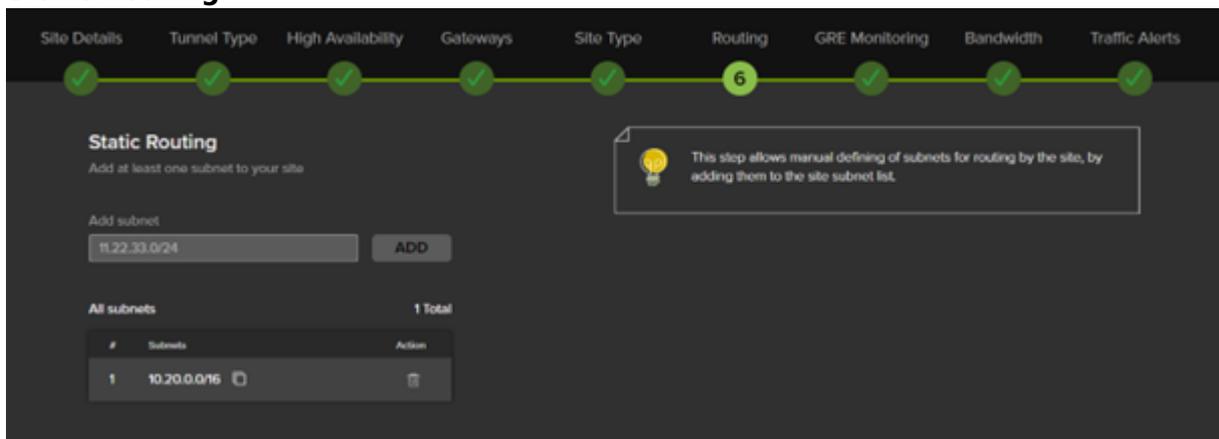
- **Tunnel Type**



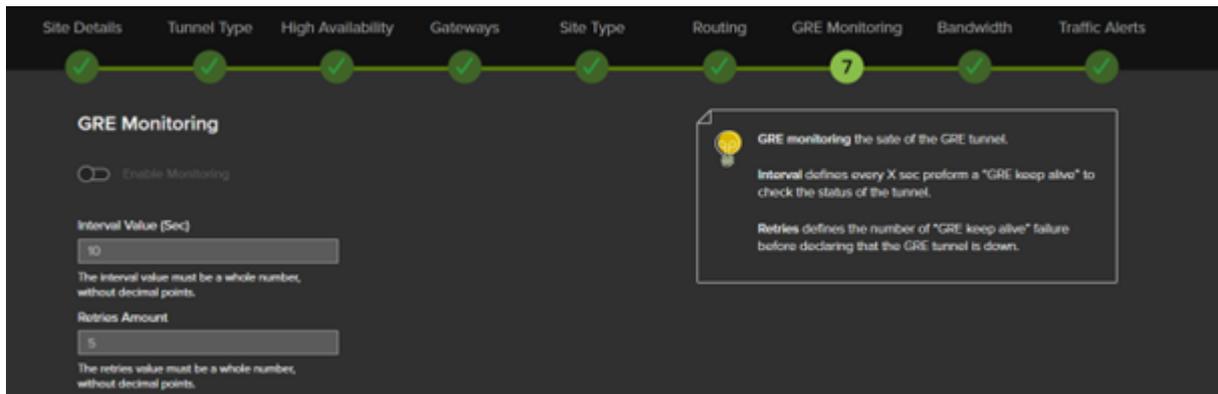
- High Availability (optional)
- Gateway IPs



- Static Routing



- GRE Monitoring - Must be deactivated.



- **IPSec IKEv2 Settings**

In this example, we have collected the following settings:

- **PoE (IP Teridion Router):** 158.101.193.191
- **Gateway #1 IP (Firewall Public IP):** 82.150.198.170
- **Routed Network:** 10.20.0.0/16

Step 2. Configure IP Tunneling

On the Barracuda CloudGen Firewall, do the following:

1. Go to **Configuration > Configuration Tree > Box > Network**.
2. In the left menu, select **IP Tunneling**.
3. Click **Lock**.
4. In the **IP Tunneling** section, click **+**.
5. Provide a meaningful **Name** for the **GRE Tunnel**.
6. Configure the remaining settings according to your setup:

Tunnel Configuration

Encapsulation Mode	GRE(47)
Tunnel TTL	
Set Multicast Flag	no
Source IP Type	BoxIP
Source IP	10.20.0.5
Source Mask	single-host
Route Metric	15
Remote End IP	158.101.193.191
Check Reachability	yes
Local End IP	82.150.198.170
Trust Level	Trusted (added to Trusted-LAN for Firewall)
Target Networks	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">10.2.0.0/24</div>
Advertise Route	no
Use Policy Routing	no
Table Placement	postmain
Use Table	
Source Networks	<div style="border: 1px solid #ccc; padding: 5px; min-height: 40px;">0.0.0.0/0</div>

- **Encapsulation Mode** - Select **GRE(47)**.
- **Source IP Type** - Select **Box IP**.
- **Source IP** - Use one of the box IP addresses that reside in the **Network (Static Routing - 4)** window of the Teridion setup (e.g: 10.20.0.5) .
- **Source Mask** - Select **single host**.
- **Remote End IP** - Enter the public IP of PoE, e.g, 158.101.193.191
- **Check Reachability** - Select **yes**.
- **Local End IP** - Enter the public IP of your CloudGen Firewall, e.g., 82.150.198.170
- **Trust Level** - Select **Trusted** or configure a firewall policy to allow the traffic
- **Target Networks** - Add networks that are are reachable through GRE tunnel /Teridion Network, e.g., 10.2.0.0/16

Additional Resources

- [How to Connect the Barracuda CloudGen Firewall to Teridion via IPSec](#)

Figures

1. gre1.png
2. gre2.png
3. gre3.png
4. gre4.png
5. gre5.png
6. gre6.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.