How to Connect the Barracuda CloudGen Firewall to Teridion via IPSec

https://campus.barracuda.com/doc/99123605/

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 IPSec

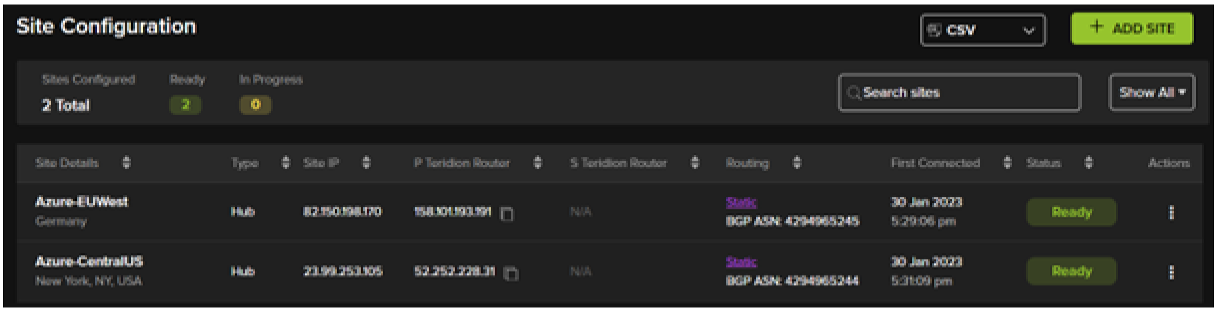
Before You Begin

- 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.

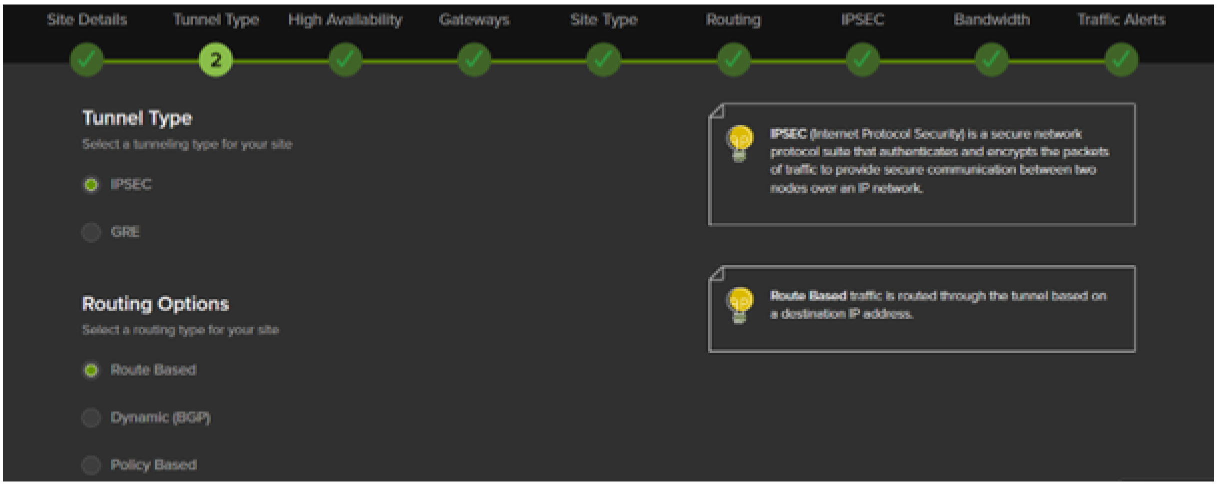


Site Configuration

Sites Configured: 2 Total | Ready: 2 | In Progress: 0

Site Details	Type	Site IP	P Teridion Router	S Teridion Router	Routing	First Connected	Status	Actions
Azure-EUWest Germany	Hub	82.150.198.170	158.101.193.191	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**



Tunnel Type

Select a tunneling type for your site

● IPSEC

○ GRE

Routing Options

Select a routing type for your site

● Route Based

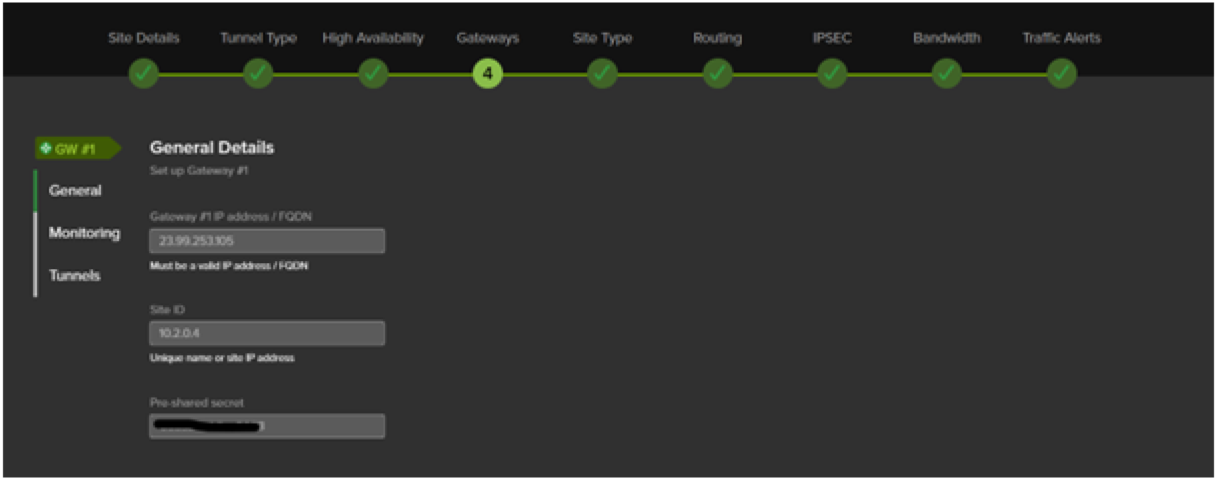
○ Dynamic (BGP)

○ 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.

Route Based traffic is routed through the tunnel based on a destination IP address.

- **High Availability (optional)**
- **Gateways IPs**



General Details

Set up Gateway #1

Gateway #1 IP address / FQDN: 23.99.253.105

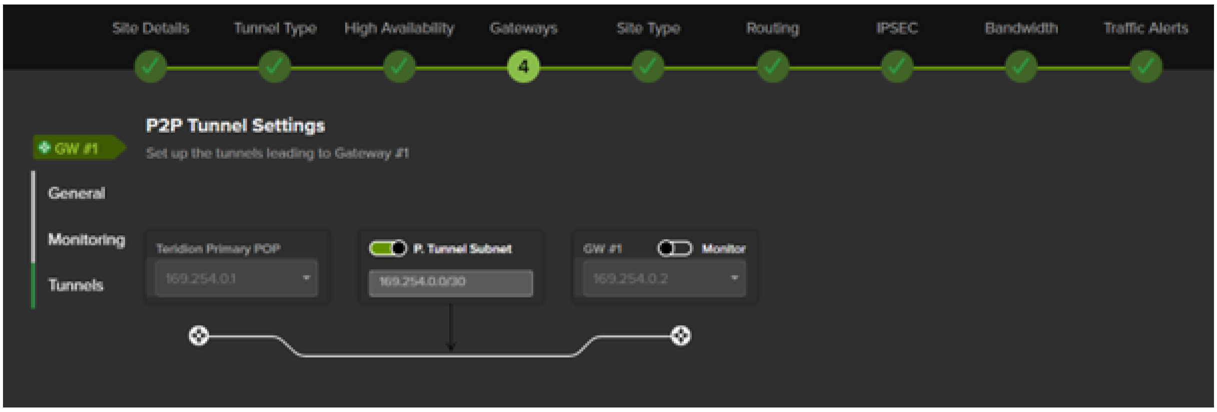
Must be a valid IP address / FQDN

Site ID: 10.2.0.4

Unique name or site IP address

Pre-shared secret: [redacted]

- **Transfer Network**



P2P Tunnel Settings

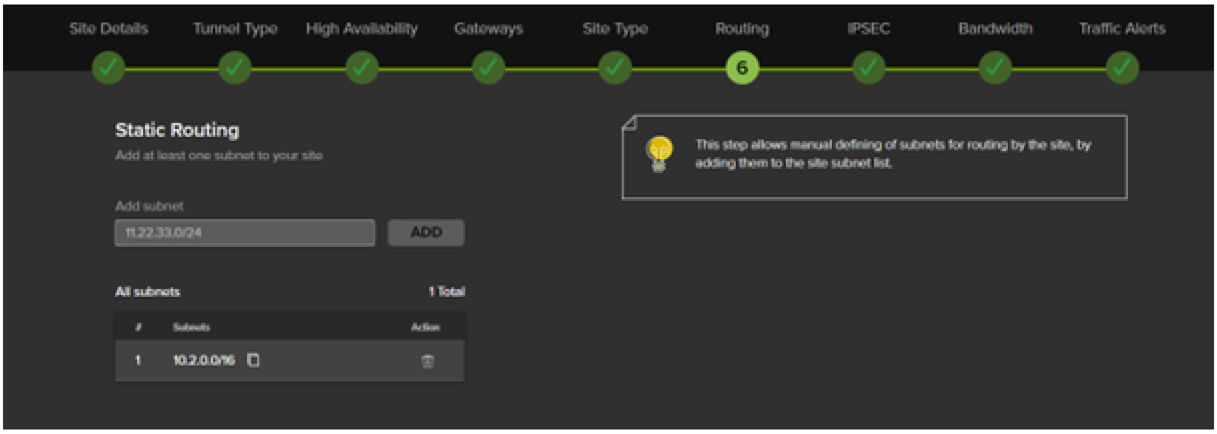
Set up the tunnels leading to Gateway #1

Teridion Primary POP: 169.254.0.1

P. Tunnel Subnet: 169.254.0.0/30

GW #1: 169.254.0.2 Monitor

- **Static Routing**



Static Routing

Add at least one subnet to your site

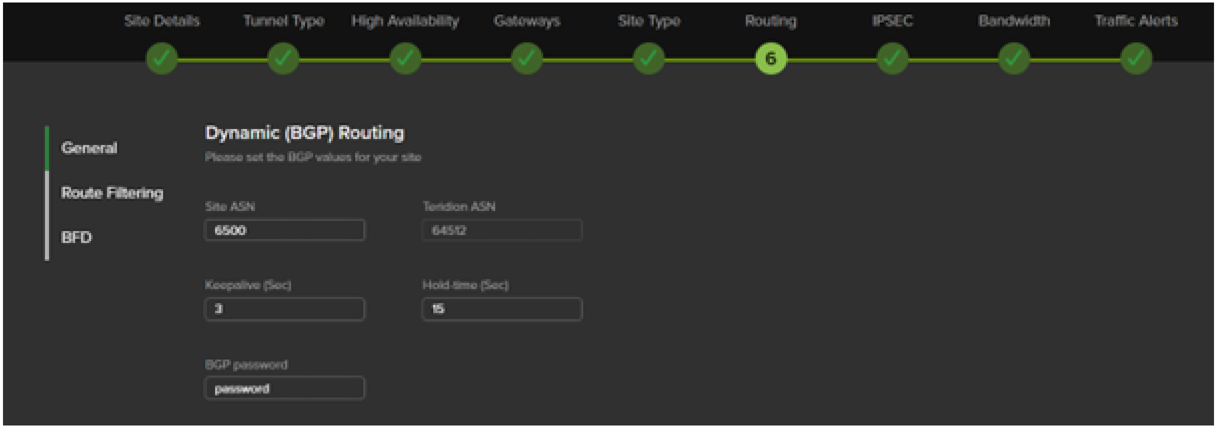
This step allows manual defining of subnets for routing by the site, by adding them to the site subnet list.

Add subnet: 11.22.33.0/24

All subnets — 1 Total

#	Subnets	Action
1	10.2.0.0/16	

- **Dynamic Routing with BGP (optional)**



Dynamic (BGP) Routing

Please set the BGP values for your site

Site ASN: 6500

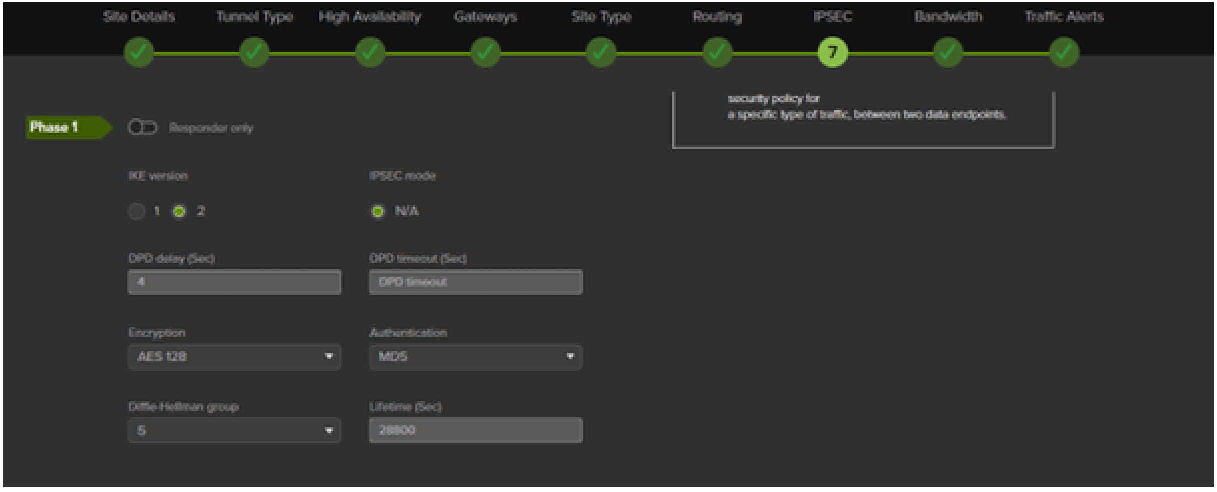
Teridion ASN: 64512

Keepalive (Sec): 3

Hold-time (Sec): 15

BGP password: password

- **IPSec IKEv2 Settings**



security policy for
a specific type of traffic, between two data endpoints.

○ Responder only

IKE version: ○ 1 ● 2

IPSEC mode: ● N/A

DPD delay (Sec): 4

DPD timeout (Sec): DPD timeout

Encryption: AES 128

Authentication: MD5

Diffie-Hellman group: 5

Lifetime (Sec): 28800

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

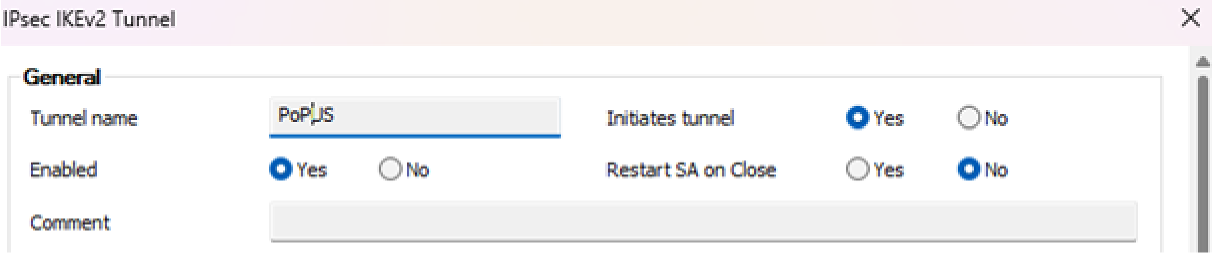
BGP (Optional)

- **Teridion ASN**: 64500
- **Site ASN**: 64512

Step 2. Configure IPSec IKEv2 Static Routing

On the Barracuda CloudGen Firewall, do the following:

1. Go to **Configuration > Configuration Tree > Box > Assigned Services > VPN Service > Site to Site**.
2. Click on the **IPSec IKEv2** tunnel tab.
3. Click **Lock**.
4. Right-click the table and select **New IKEv2 tunnel**. The **IKEv2 Tunnel** window opens.
5. In the **IKEv2 Tunnel Name** field, enter your tunnel name.
6. Set **Initiates Tunnel** to **Yes**.



IPsec IKEv2 Tunnel

General

Tunnel name: PoPUS

Initiates tunnel: ● Yes ○ No

Enabled: ● Yes ○ No

Restart SA on Close: ○ Yes ● No

Comment:

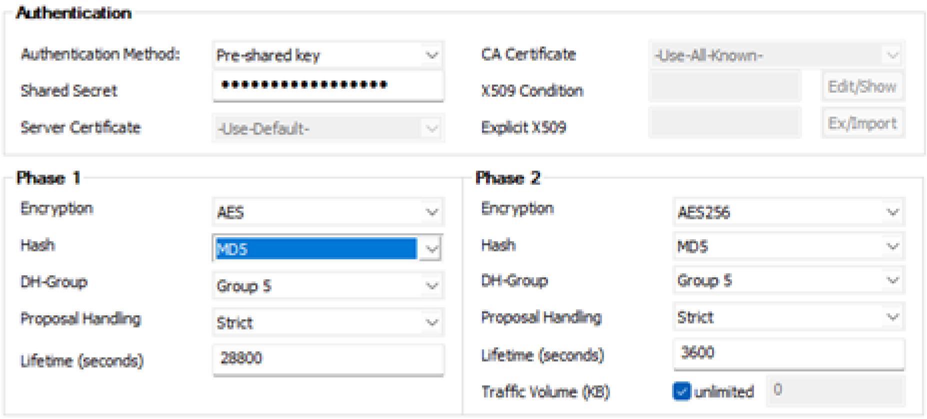
Step 3. Configure Authentication and Encryption

Step 3.1 Configure the Phase 1 encryption settings matching your Teridion setup

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

Step 3.2 Configure the Phase 2 encryption settings

- **Encryption** – Select **AES-256**.
- **Hash Meth.** – Select **MD5**.
- **DH Group** – Select **Group 5**.
- **Proposal Handling** – Select **Strict**.
- **Lifetime (seconds)** – Enter `3600`.
- **LIfetime (KB)** – Enter `0`.



Authentication

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

Phase 1

Encryption	AES
Hash	MD5
DH-Group	Group 5
Proposal Handling	Strict
Lifetime (seconds)	28800

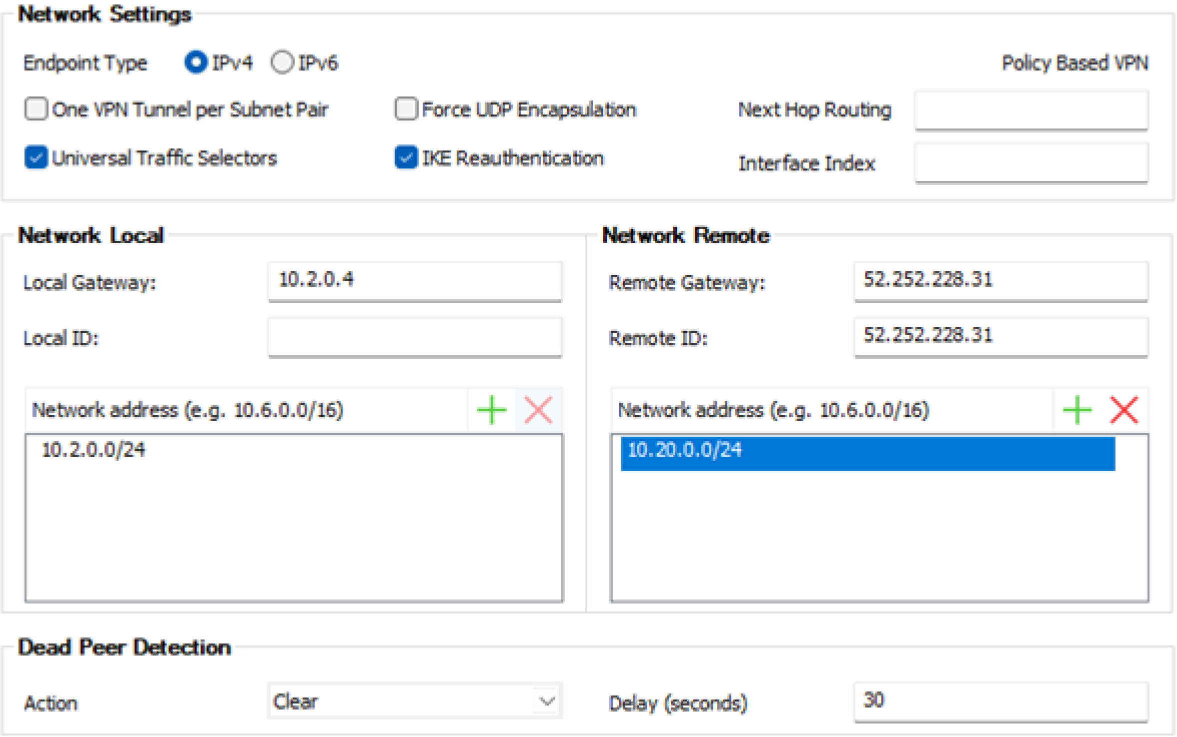
Phase 2

Encryption	AES256
Hash	MD5
DH-Group	Group 5
Proposal Handling	Strict
Lifetime (seconds)	3600
Traffic Volume (KB)	☑ unlimited 0

Step 4. Configure Network Settings

In the **Network Settings**, set the following values:

- **Universal Traffic selector** – Select the check box
- **IKE Reauthentication** - Select the check box
- **Local Gateway** – Enter your internal IP, e.g., `10.2.0.4`
- **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`
- Add your **Local Network**.
- Add your **Remote Networks** that are reachable via Teridion.
- Set up DPD to match your Teridion configuration.



Network Settings

Endpoint Type ● IPv4 ○ IPv6 — Policy Based VPN

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

☑ Universal Traffic Selectors — ☑ IKE Reauthentication — Interface Index:

Network Local

Local Gateway: 10.2.0.4

Local ID:

Network address (e.g. 10.6.0.0/16): 10.2.0.0/24

Network Remote

Remote Gateway: 52.252.228.31

Remote ID: 52.252.228.31

Network address (e.g. 10.6.0.0/16): 10.20.0.0/24

Dead Peer Detection

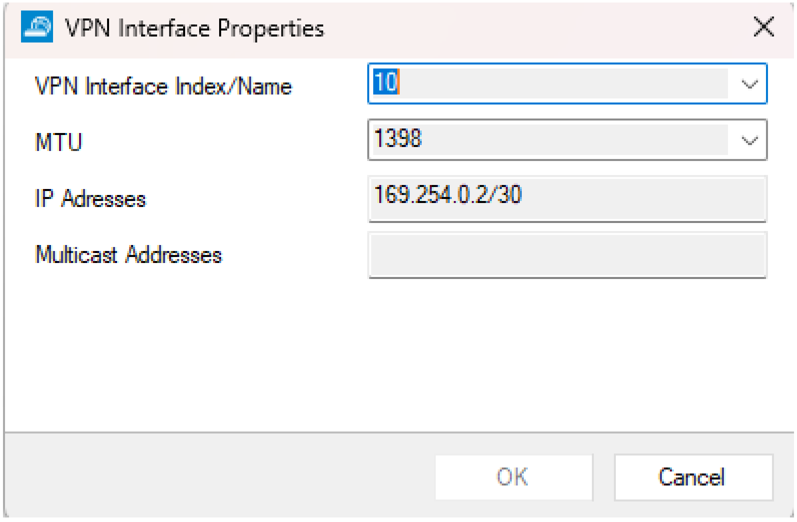
Action: Clear

Delay (seconds): 30

Step 5. Configure IPsec IKEv2 Dynamic Routing

Create a VPN next hop interface:

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the left menu, click **Routed VPN**.
4. Click **Add** in the **VPN Next Hop Interface Configuration** section.
5. Configure the following settings:
   - **VPN Interface Index** – Enter a number between 0 and 99. Each interface index number must be unique.
   - **MTU** – Enter 1398
   - **IP Addresses** – Enter **Transfer Network GW IP**, e.g., `169.254.0.2/30`



VPN Interface Properties

VPN Interface Index/Name: 10

MTU: 1398

IP Adresses: 169.254.0.2/30

Multicast Addresses:

6. Click **OK.**

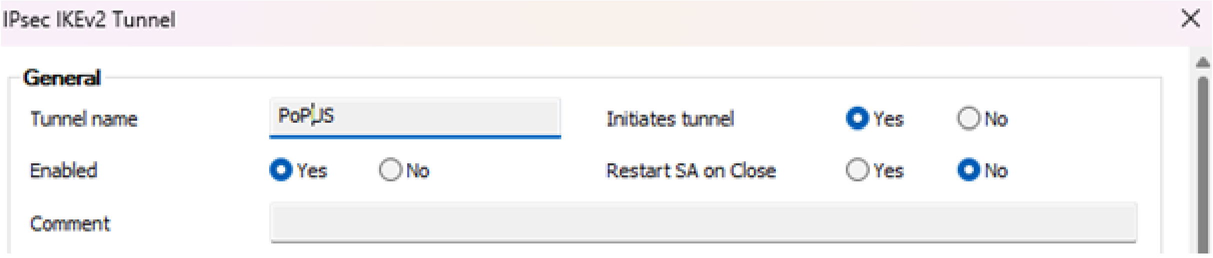
Step 5.1 Add the VPN next hop interface IP address to the shared IPs

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. In the left menu, click **IP Configuration**.
4. In the **Shared Networks and IPs** section, click **+**.
5. Enter a name for the shared IP address, and click **OK**.
6. The **Shared Networks and IPs** window opens. Configure the following settings:
    - **Interface** – Select **other** and enter `vpnr10`.
    - **Network Address** – Enter the network address of the Transfer Network in CIDR format: `169.254.0.0/30`.
    - Click **Shared IPs in this Network**. The **Shared IPs in this Network** window opens. Enter the following:
        - **IP Address** – Enter the IP address for the VPN interface of the CloudGen Firewall, e.g., `169.25.0.2`
        - **Alias for this IP** – Select **None**.
        - **Respond to Ping** – Select **yes**.
    - Click **OK**.
    - **Trust Level** – Select **Unclassified**.
    - **Active** – Select **Yes**.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Step 6. Configure the Site-to-Site IPSec IKEv2 VPN Service

1. Go to **Configuration > Configuration Tree > Box > Assigned Services > VPN Service > Site to Site**.
2. Click on the **IPSec IKEv2 tunnel** tab.
3. Click **Lock**.
4. Right-click the table and select **New IKEv2 tunnel**. The **IKEv2 Tunnel** window opens.
5. In the **IKEv2 Tunnel Name** field, enter your tunnel name.

6. Set **Initiates Tunnel** to **Yes**.



IPsec IKEv2 Tunnel

General

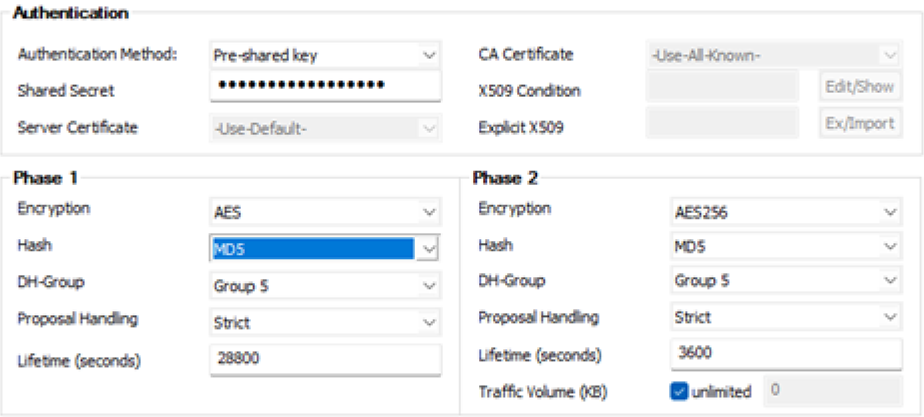
Tunnel name	PoP_US	Initiates tunnel	● Yes ○ No
Enabled	● Yes ○ No	Restart SA on Close	○ Yes ● No
Comment			

Step 6.1 Configure the Phase 1 encryption settings matching your Teridion setup

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

Step 6.2 Configure the Phase 2 encryption settings

- **Encryption** – Select **AES**.
- **Hash Meth.** – Select **MD5**.
- **DH Group** – Select **Group 5**.
- **Proposal Handling** – Select **Strict**.
- **LIfetime (KB)** – Enter `0`.



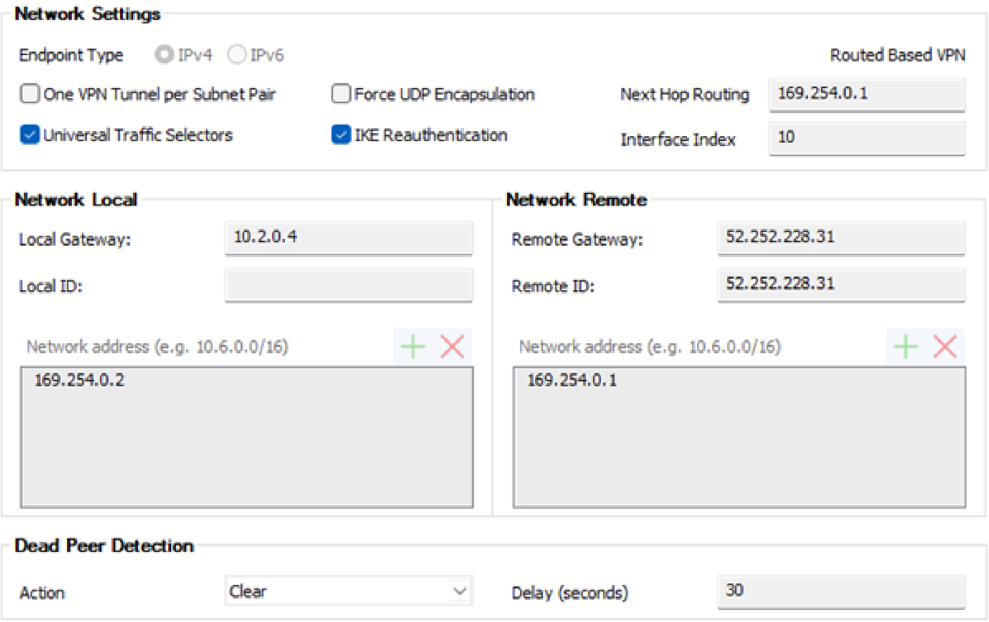
Authentication

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

Phase 1		Phase 2	
Encryption	AES	Encryption	AES256
Hash	MD5	Hash	MD5
DH-Group	Group 5	DH-Group	Group 5
Proposal Handling	Strict	Proposal Handling	Strict
Lifetime (seconds)	28800	Lifetime (seconds)	3600
		Traffic Volume (KB)	☑ unlimited 0

In the **Network Settings**, set the following values:

- **Universal Traffic selector** – Select the check box
- **IKE Reauthentication** - Select the check box
- **Next Hop Routing** – Enter the TCR IP collected in the beginning: `169.254.0.1`
- **Interface Index** – Enter the interface index created in Step 1.
- **Local Gateway** – Enter your internal IP, e.g., `10.2.0.4`
- **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`
- Set up DPD to match your Teridion configuration.



Network Settings

Endpoint Type ● IPv4 ○ IPv6

Routed Based VPN

□ One VPN Tunnel per Subnet Pair

□ Force UDP Encapsulation

Next Hop Routing: 169.254.0.1

☑ Universal Traffic Selectors

☑ IKE Reauthentication

Interface Index: 10

Network Local

Local Gateway: 10.2.0.4

Local ID:

Network address (e.g. 10.6.0.0/16): 169.254.0.2

Network Remote

Remote Gateway: 52.252.228.31

Remote ID: 52.252.228.31

Network address (e.g. 10.6.0.0/16): 169.254.0.1

Dead Peer Detection

Action: Clear

Delay (seconds): 30

9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Step 7. Configure the BGP Service

Configure BGP routing to learn the subnets from the remote BGP peer behind the Teridion network.

> Only routes with the parameter **Advertise** set to **yes** will be propagated via BGP.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. (optional) To propagate the management network, set **Advertise Route** to **yes**.
4. In the left menu, click **Advanced Routing**.
5. Double-click the **Routes** you want to propagate, and set **Advertise Route** to **yes**.
6. Click **OK.**
7. Click **Send Changes** and **Activate**.

Step 7.1 Enable BGP

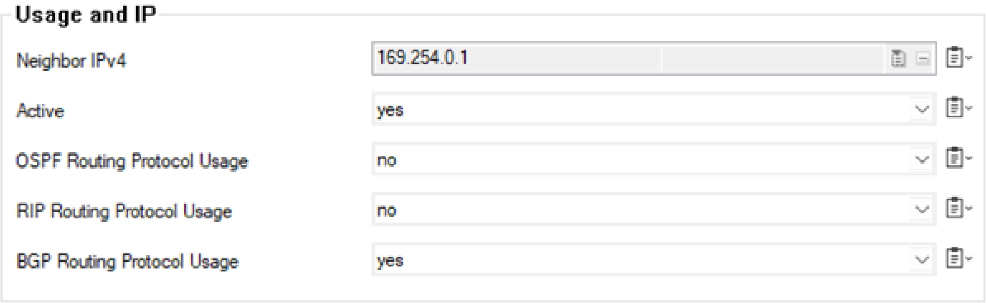
Configure the BGP setting for the BGP service on the firewall.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > OSPF-RIP-BGP-Service > OSPF/RIP/BGP Settings**.
2. In the left menu, click **BGP Router Setup**.
3. Enter the **AS Number** for your network, e.g., `64500`
4. In the **Terminal Password** fields, specify a password for connecting to the BGP router service via telnet from the shell of the Barracuda CloudGen Firewall.

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

Step 7.2 Configure the BGP Neighbor

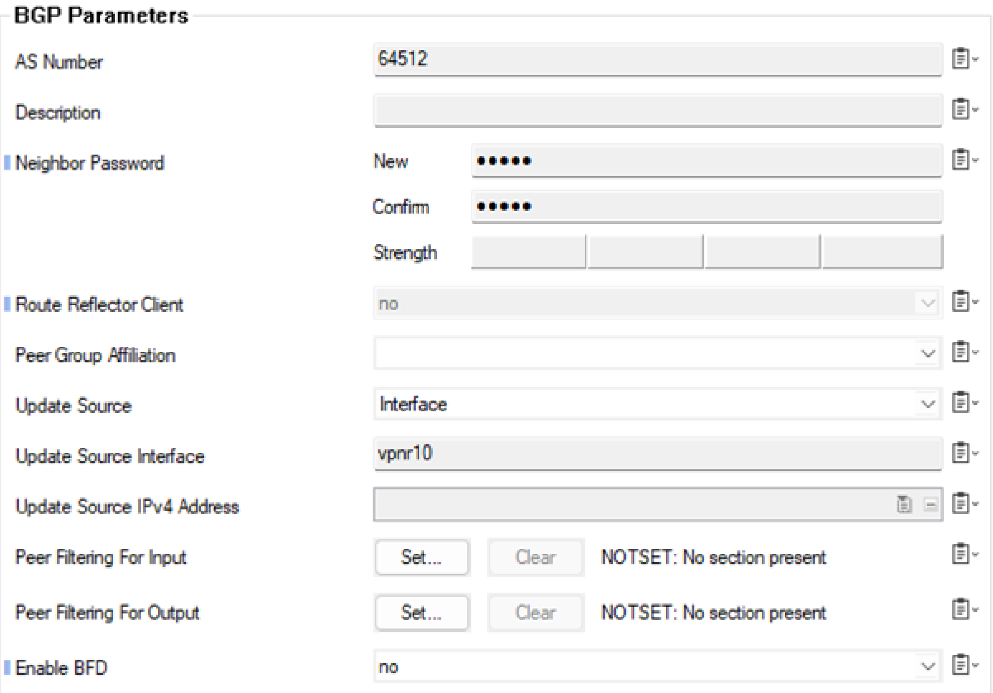
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Dynamic Routing (OSPF-RIP-BGP-Service) > OSPF/RIP/BGP Settings**.
2. In the left menu of the **OSPF/RIP/BGP Settings** page, click **Neighbor Setup IPv4**.
3. Click **Lock**.
4. In the left menu, expand **Configuration Mode** and click **Switch to Advanced Mode**.
5. Click **+** to add an entry to the **Neighbors** table. The **Neighbors** window opens.
6. Enter a **Name** and click **OK**.
7. In the **Neighbors** window, configure the following settings in the **Usage** and **IP** section:
    - **Neighbor IPv4** – Enter the remote BGP peer IP address, e.g., `169.254.0.1`
    - **OSPF Routing Protocol Usage** – Select **no**.
    - **RIP Routing Protocol Usage** – Select **no**.
    - **BGP Routing Protocol Usage** – Select **yes**.



Usage and IP

Neighbor IPv4	169.254.0.1
Active	yes
OSPF Routing Protocol Usage	no
RIP Routing Protocol Usage	no
BGP Routing Protocol Usage	yes

8. In the **BGP Parameters** section, configure the following settings:
    - **AS Number** – Enter the ASN for the remote network as collected in the preparation.
    - **Update Source** – Select **Interface**.
    - **Update Source Interface** – Enter the vpnr interface. E.g., `vpnr10`



BGP Parameters

AS Number	64512	
Description		
Neighbor Password	New	•••••
	Confirm	•••••
	Strength	
Route Reflector Client	no	
Peer Group Affiliation		
Update Source	Interface	
Update Source Interface	vpnr10	
Update Source IPv4 Address		
Peer Filtering For Input	Set... Clear	NOTSET: No section present
Peer Filtering For Output	Set... Clear	NOTSET: No section present
Enable BFD	no	

9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Additional Resources

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

Figures