How to Configure a Site-to-Site IPsec IKEv1 VPN Tunnel

https://campus.barracuda.com/doc/73719165/

The Barracuda CloudGen Firewall can establish IPsec VPN tunnels to any standard-compliant, third-party IKEv1 IPsec VPN gateway. The Site-to-Site IPsec VPN tunnel must be configured with identical settings on both the CloudGen Firewall and the third-party IPsec gateway. The Barracuda CloudGen Firewall supports authentication with a shared passphrase as well as X.509 certificate-based (CA-signed as well as self-signed) authentication. To allow traffic into the VPN tunnel, an access rule is required.

Before You Begin

- If you are using a dynamic WAN IP address, go to **CONFIGURATION > Configuration Tree> Box > Virtual Server > your virtual server > Assigned Services > VPN > VPN Settings**. In the **Advanced Tab** of the **Server Settings** set **Use IPsec dynamic IPs** to **Yes**. This will create an IPsec VPN listener on 0.0.0.0/0.
- If no already present, configure the **Default Server Certificate** in **CONFIGURATION > Configuration Tree> Box > Virtual Server > your virtual server > Assigned Services > VPN > VPN Settings**. For more information, see VPN Settings

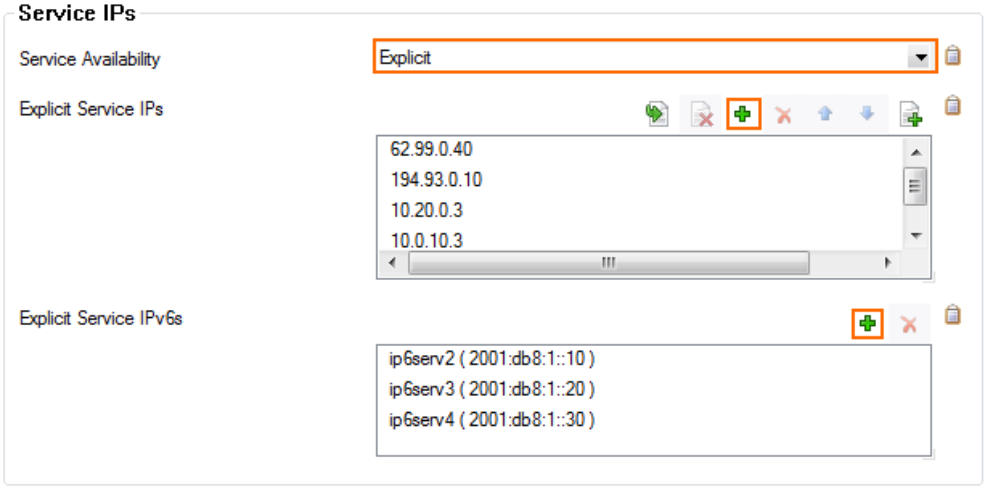
Step 1. Configure the VPN Service Listeners

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

1. Go to **CONFIGURATION > Configuration Tree> Box > Virtual Server > your virtual server > Assigned Services > VPN > Service Properties**.
2. Click **Lock**.
3. From the **Service Availability** list, select the source for the IPv4 listeners:
   - **First+Second-IP** – The VPN service listens on the first and second virtual server IPv4 address.
   - **First-IP** – The VPN service listens on the first virtual server IPv4 address.
   - **Second-IP** – The VPN service listens on the second virtual server IPv4 address.

- **Explicit** – For each IP address, click **+** and enter the IPv4 Addresses in the **Explicit Service IPs** list.

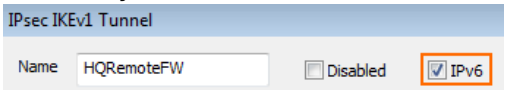
4. Click **+** to add an entry to the **Explicit IPv6 Service IPs**.
5. Select an IPv6 listener from the list of configured explicit IPv6 virtual server IP addresses.



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

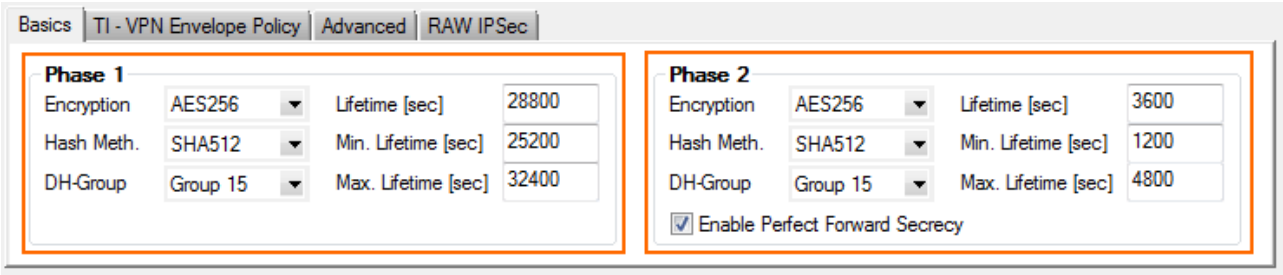
Step 2. Create an IKEv1 IPsec Tunnel on the CloudGen Firewall

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > VPN-Service > Site to Site**.
2. Click the **IPSEC IKEv1 Tunnels** tab.
3. Click **Lock**.
4. Right-click the table and select **New IPSec IKEv1 tunnel**. The **IPsec Tunnel** window opens.
5. Enter a **Name** for the tunnel.
6. (IPv6 only) If IPv6 addresses are used, click the **IPv6** check box.

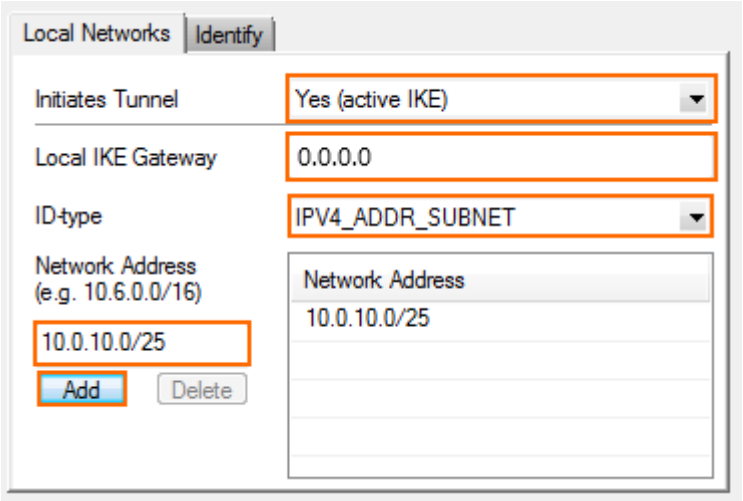


7. Select the **Phase 1** settings:
   - **Encryption** – Select the encryption algorithm: **AES**, **AES256**, **3DES**, **CAST**, **Blowfish** or **DES**.
   - **Authentication** – Select the hashing algorithm: **MD5**, **SHA**, **SHA256**, or **SHA512**.
   - **DH-Group** – Select the Diffie-Hellman Group. The Barracuda CloudGen Firewall supports **Group1** to **Group 18**.
   - **Lifetime [sec]** – Enter the phase 1 lifetime in seconds. Default: 28800
   - **Min. Lifetime [sec]** – Enter the phase 1 minimum lifetime in seconds. Default: 25200
   - **Max. Lifetime [sec]** – Enter the phase 1 maximum lifetime in seconds. Default: 32400
8. Select the **Phase 2** settings:
   - **Encryption** – Select the encryption algorithm: **AES**, **AES256**, **3DES**, **CAST**, **Blowfish**, **DES**, or **Null**.
   - **Authentication** – Select the hashing algorithm: **MD5**, **SHA**, **SHA256**, or **SHA512**.
   - **DH-Group** – Select the Diffie-Hellman Group. The Barracuda CloudGen Firewall supports

Group1 to **Group 18**.
- **Lifetime [sec]** – Enter the phase 1 lifetime in seconds. Default: 3600
- **Min. Lifetime [sec]** – Enter the phase 1 minimum lifetime in seconds. Default: 1200
- **Max. Lifetime [sec]** – Enter the phase 1 maximum lifetime in seconds. Default: 4800
- **Enable Perfect Forward Secrecy** – Enable if the remote VPN gateway supports perfect forward secrecy (PFS).

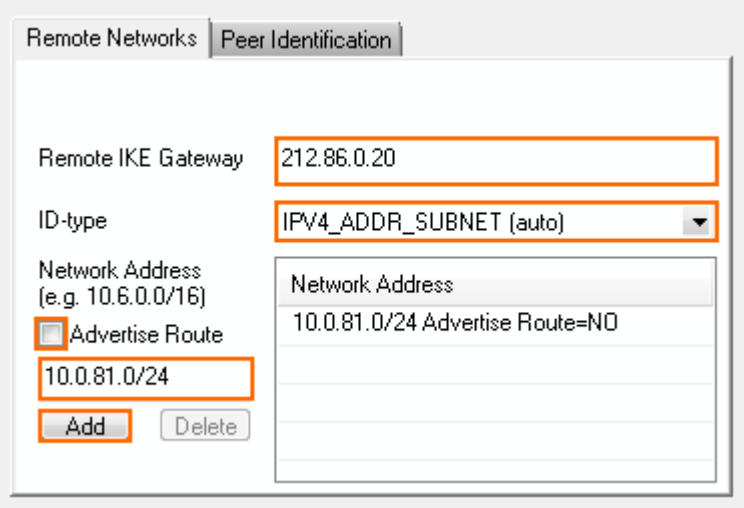


9. Click the **Local Networks** tab and configure the following settings:
   - **Initiates Tunnel**– Select **Yes (active IKE)** for the Barracuda CloudGen Firewall to initiate the VPN Tunnel.
   - **Local IKE Gateway** – Enter the IPv4 or IPv6 address the VPN service is listening on. If you are using a dynamic WAN IP address, enter `0.0.0.0` , or ::0.
   - **ID-type** – Select the IPsec ID-type. For more information, see IPsec IKEv1 Tunnel Settings.
   - **Network Address** – Add the local networks you want to reach through the VPN tunnel, and click **Add**.

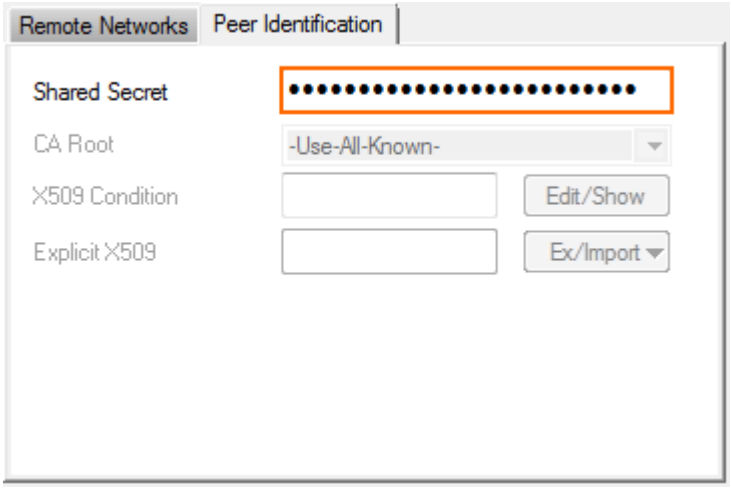


10. Click the **Remote Networks** tab, and configure the following settings:
    - **Remote IKE Gateway**
      You have two options to configure the remote IKE Gateway:
      - **Main mode** – Enter the hostname. If the remote appliance is using dynamic IP addresses, the hostname will be periodically resolved and the last dynamic assigned IP address of the remote gateway will be used.
      - **Aggressive mode** – Enter the IPv4 or IPv6 address the third-party appliance is listening on. If the remote appliance is using dynamic IP addresses, you can also enter `0.0.0.0/0` or ::0/0. In this case, you must use **aggressive mode**.
    - **ID-type** – Select the IPsec ID-type. For more information, see IPsec IKEv1 Tunnel Settings.
    - **Network Address** – Add the IP address of the remote network, and enable **Advertise Route** if you want to propagate it via RIP, OSPF, or BGP. (e.g., `10.0.81.0/24`). Enter the

address and then click **Add**.



11. Click the **Peer Identification** tab, and enter the shared passphrase in the **Shared Secret** field. The passphrase may not contain the hash (#) character.



12. If the remote IPsec gateway does not support Dead Peer Detection (DPD), disable it:
    1. Click the **Advanced** tab.
    2. In the **DPD interval (s)** field, enter `0`
13. Switch to aggressive mode if the remote IP address is unknown and you are using a **Shared Secret** to authenticate.
    1. Click the **Identity** tab.
    2. From the **Mode** list, select **Aggressive**
    3. Enter the **Aggressive-ID**.
14. Click **OK**.
15. Click **Send Changes and Activate**.

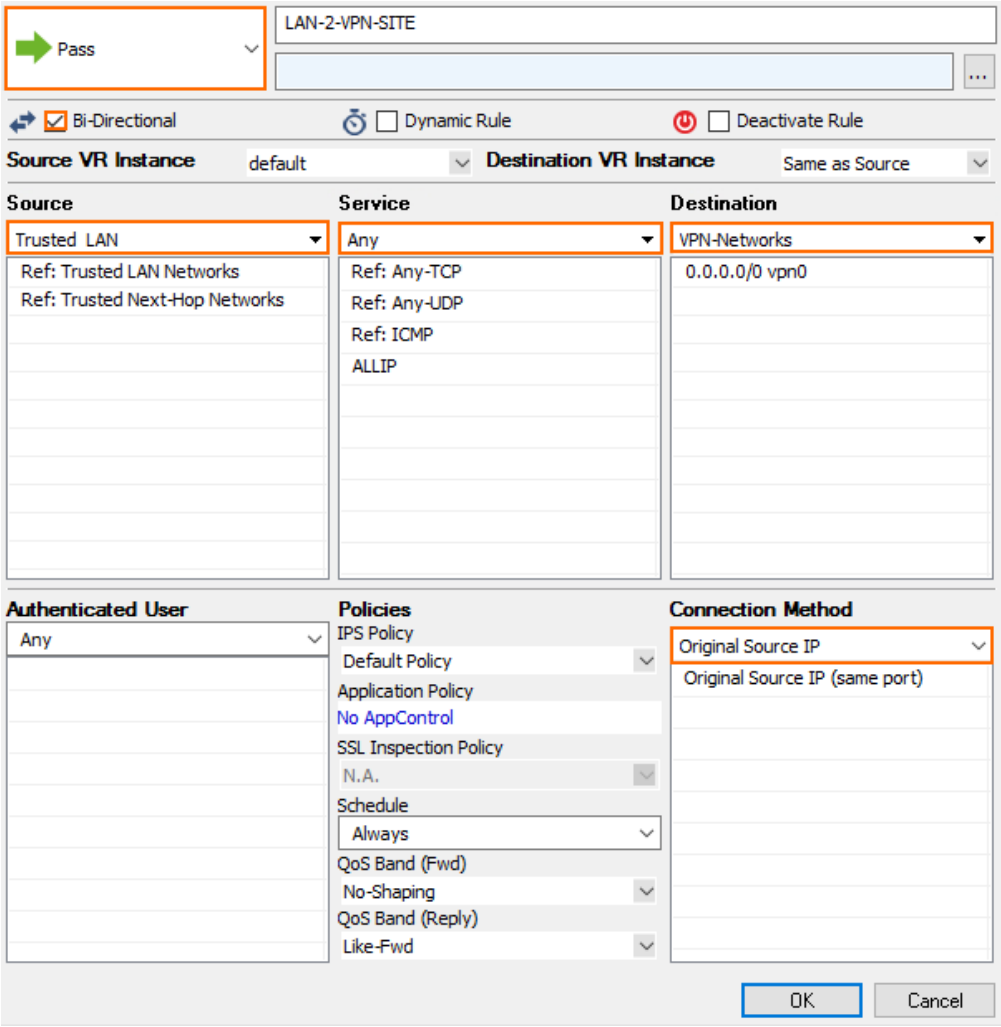
Step 3. Create an IPsec Tunnel on the Remote Appliance

Configure the remote CloudGen Firewall or third-party appliance as passive tunnel partner. The remote VPN gateway must be configured with the same encryption settings. Only the local and

remote networks and the IP address for the remote VPN gateway must be mirrored.

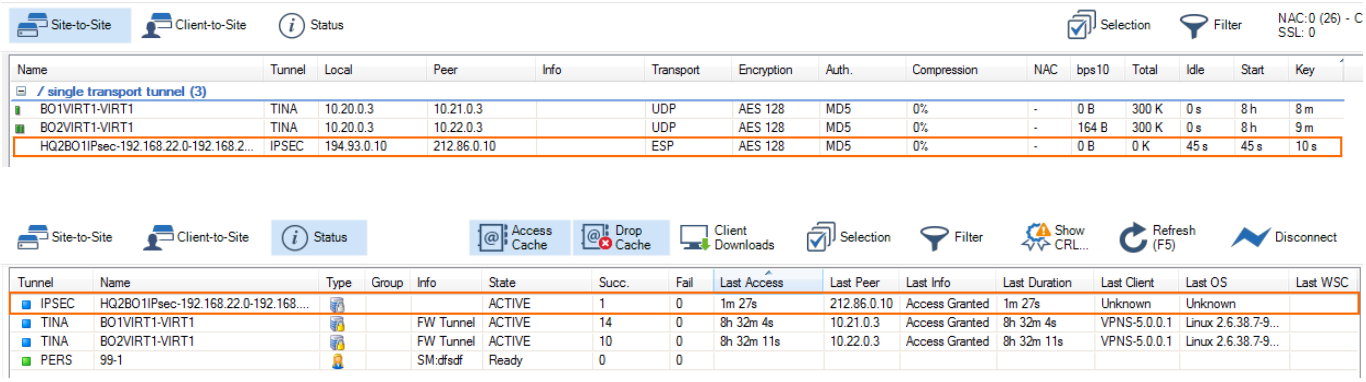
Step 4. Create Access Rules for VPN Traffic

To allow traffic in and out of the VPN tunnel, create a PASS access rule on the CloudGen Firewall. 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**.



Troubleshooting

- Ping a host in the remote network. If the network host is unavailable, attempt to ping the IP address of the remote IPsec gateway.
- Go to the **FIREWALL > Live** page and ensure that network traffic is matching the access rule created in Step 3.

Most of the IPsec implementations represent a single IP address as a network address in combination with a subnet mask (255.255.255.255). The IKE protocol is difficult to debug. Therefore, Barracuda CloudGen Admin displays a warning message if IPsec networks contain single IP addresses. If the IPsec connection cannot be established and the error **no compatible proposals chosen** is displayed,

- Verify that the IPsec settings on both IPsec peers match. (encryption, hash method, etc...).
- If you are using single IP addresses as the local or remote network, try to use network addresses (using netmask 255.255.255.252) for the local and remote network settings. If the tunnel can be be established, the third-party IPsec implementation most likely is not compatible with the use of single IP addresses. In this case, use a larger network as the remote and local network.

Checklist for Connecting to Third-party IPsec VPN Gateways

- Tunnel partners must be active at one end and passive at the other end.
- Phase 1 and Phase 2 settings must be identical on both VPN gateways.
- Do not use identical or overlapping remote networks when using multiple IPSec tunnels because the remote network is used for authentication.

When creating IPsec tunnels between CloudGen Firewall and third-party gateways, consider the following:

- Phase 1 and Phase 2 settings must match the requirements of the remote peer.

- Configure lifetimes, also known as tunnel rekeying times, in seconds and not as KB-values.
- The Phase 1 and Phase 2 lifetime must be different.
- Only use Dead Peer Detection if the remote VPN gateway also supports this feature.
- Supernetting is not supported
- Do not use IPsec-SA bundling.

Figures