

How to Create a TINA VPN Tunnel between CloudGen Firewalls

<https://campus.barracuda.com/doc/98216253/>

Since the TINA protocol offers significant advantages over IPsec, it is the main protocol used for VPN connections between CloudGen Firewalls. Many of the advanced VPN features, such as SD-WAN, are supported only for TINA site-to-site tunnels.



You must complete this configuration on both the local and the remote Barracuda CloudGen Firewall by using the respective values below:

Setting	Example values for the local firewall	Example values for the remote firewall
VPN local networks	10.0.10.0/25	10.0.81.0/24
VPN remote networks	10.0.81.0/24	10.0.10.0/25
External IP address (listener VPN service)	62.99.0.40	212.86.0.10

The following sections use the default transport, encryption, and authentication settings. For more detailed information, see [TINA Tunnel Settings](#).

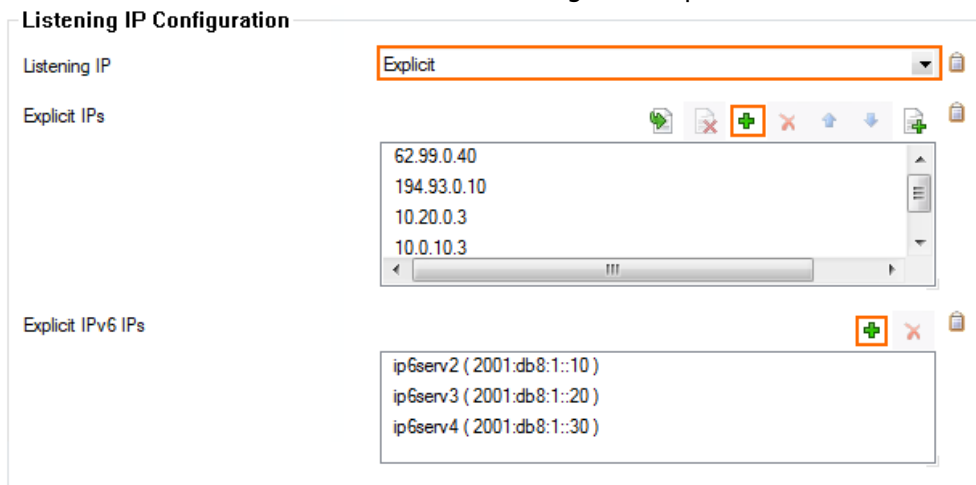
Before You Begin

If not already present, configure the **Default Server Certificate** in **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > VPN Settings > General**. For more information, see [VPN Settings](#).

Step 1. Configure the VPN Service Listeners

Configure the IPv4 and (optional) IPv6 listener addresses for the VPN service.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > Service Properties**.
2. Click **Lock**.
3. From the **Listening IP** list, select the source for the IPv4 listeners:
 - **First+Second IP** - The VPN service listens on the first and second Shared IP addresses.
 - **First IP** - The VPN service listens on the first Shared IP address.
 - **Second IP** - The VPN service listens on the second Shared IP address.
 - **Explicit** - For each IP address, click + and enter the IPv4 addresses in the **Explicit IPs** list.
 - **Device** - The VPN service listens on the interface(s) configured in the **Listening Device** table.
4. (optional) Perform the following subordinated steps optionally for IPv6:
 1. Click + to add an entry to the **Explicit IPv6 IPs**.
 2. Select an IPv6 listener from the list of configured explicit IPv6 Shared IP addresses.



Listening IP Configuration

Listening IP: Explicit

Explicit IPs:

- 62.99.0.40
- 194.93.0.10
- 10.20.0.3
- 10.0.10.3

Explicit IPv6 IPs:

- ip6serv2 (2001:db8:1::10)
- ip6serv3 (2001:db8:1::20)
- ip6serv4 (2001:db8:1::30)

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

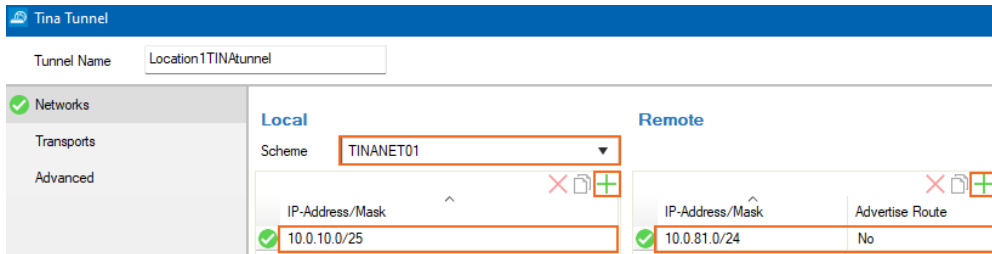
Step 2. Configure the TINA Tunnel at Location 1

For the firewall at Location 1, configure the network settings and export the public key. For more information on specific settings, see [TINA Tunnel Settings](#).

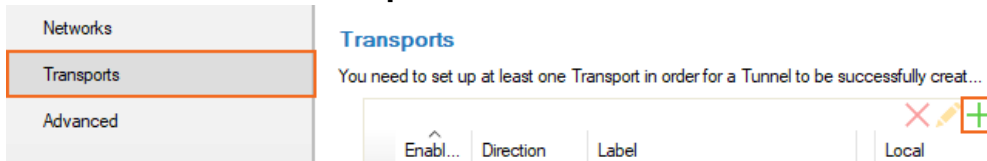
1. Log into the firewall at Location 1.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > Site to Site**.
3. Click **Lock**.
4. Click the **TINA Tunnels** tab.
5. Right-click the table and select **Add.New Tunnel**.
 1. Alternatively, you can click the + sign in the top-right corner of the window.
 2. Then, select **Add Tunnel**.
6. In the **Tunnel Name** field, enter a name for the new VPN tunnel.

7. For each local network, add the address in the **Local** section. E.g., 10.0.10.0/25
8. For each remote network, add the address in the **Remote** section. E.g., 10.0.81.0/24
9. (optional) To propagate the remote VPN network via dynamic routing, select **Yes** for **Advertise Route**

Route.

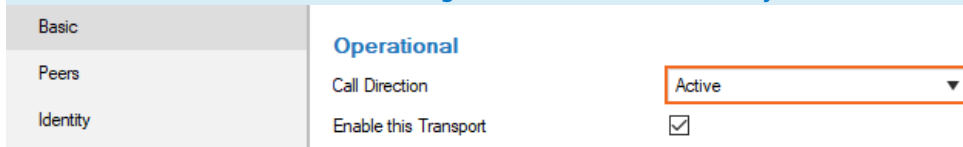


10. In the left menu, click **Transports**.



11. Click **+** to add a new transport for the VPN tunnel. The **New Transport for** window opens.
12. Select the **Call Direction**. (At least one of the firewalls must be active.)

Configure the CloudGen Firewall with a dynamic IP address to be the active peer. If both firewalls use dynamic IP addresses, a DynDNS service must be used. For more information, see [How to Configure VPN Access via a Dynamic WAN IP Address](#).

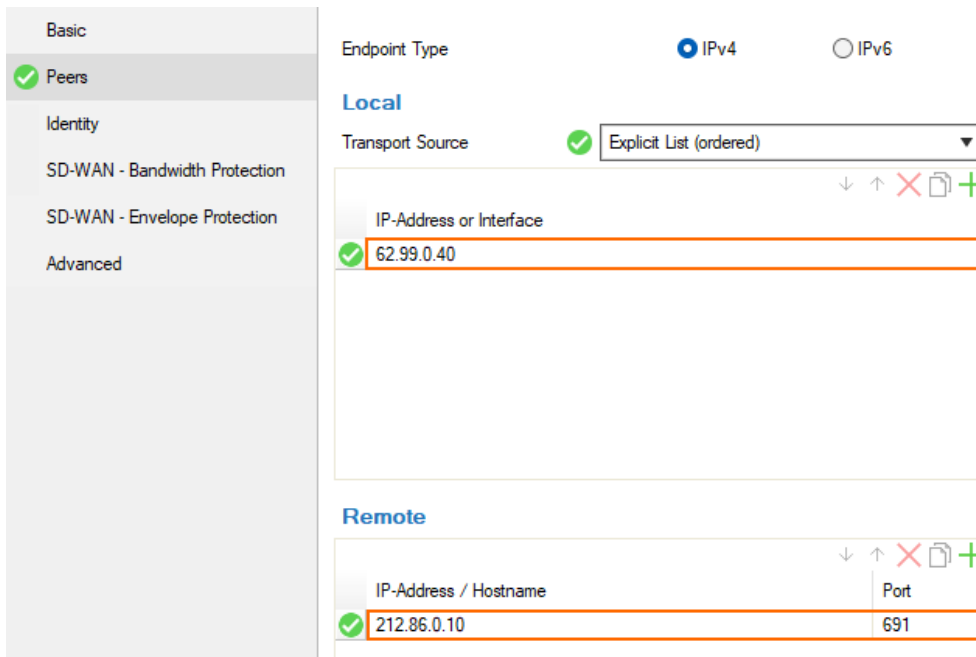


13. Configure the Basic transport settings. For more information, see [TINA Tunnel Settings](#).
 - **SD-WAN Class** – Depending on your requirements, select either **Bulk**, **Quality**, or **Fallback** from the list.
 - **Transport** – Select the transport encapsulation (recommended: **UDP**).
 - **Encryption** – Select the data encryption algorithm.
 - **Authentication** – Select the hashing algorithm for packet authentication.

14. In the left menu, click **Peers**.

For Transport Source, select one of the following options:

- **First IP** – The connection gets established from the first Shared IP address.
 - **Second IP** – The connection gets established from the second Shared IP address.
 - **Dynamic (via routing)** – The firewall uses a routing table lookup to determine the IP address.
 - **Explicit List** – Enter one or more explicit IP addresses. Multiple IP addresses are tried in the listed order. Click **+** and add the IP address(es) or interface(s) used as tunnel address.
15. In the **Remote** section, add the external peer **IP Address / Hostname** for the tunnel destination.



Basic

☒ Peers

Identity

SD-WAN - Bandwidth Protection

SD-WAN - Envelope Protection

Advanced

Endpoint Type ☒ IPv4 ☐ IPv6

Local

Transport Source ☒ Explicit List (ordered)

IP-Address or Interface
<input checked="" type="checkbox"/> 62.99.0.40

Remote

IP-Address / Hostname	Port
<input checked="" type="checkbox"/> 212.86.0.10	691

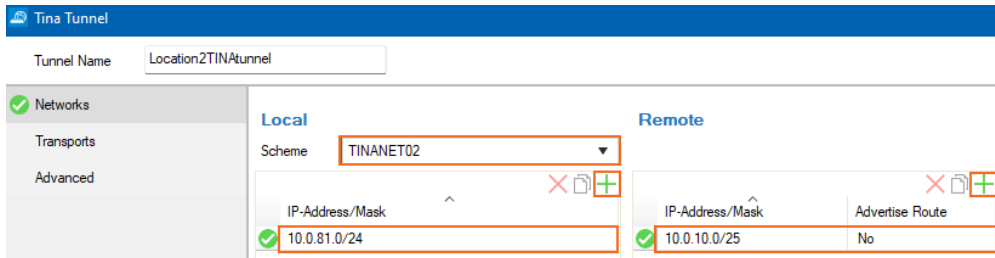
16. Configure **SD-WAN** and **Advanced** transport settings to match the settings configured for the local firewall. For more information, see the lower section in [TINA Tunnel Settings](#).

In the **Advanced** tab, you can select the **Accepted Algorithms**. To use a cipher, the list must match the **Encryption** settings configured in the **Basic** tab.

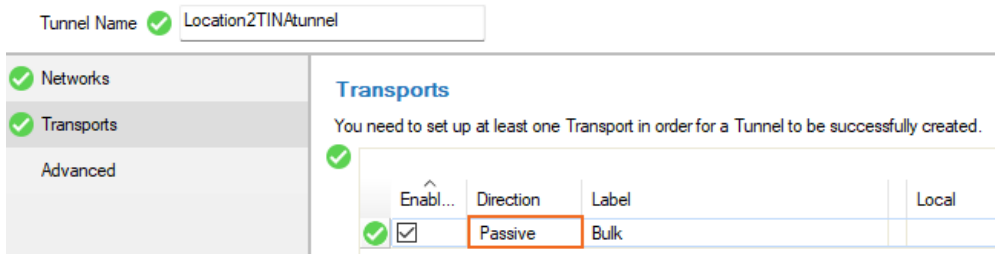
17. Configure the **Advanced** tunnel settings to match the settings configured for the local firewall. For more information, see the lower section in [TINA Tunnel Settings](#).
18. Click **OK**.
19. Click **Send Changes** and **Activate**.

Step 3. Create the TINA Tunnel at Location 2

1. Log into the firewall at Location 2.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > Site to Site**.
3. Click **Lock**.
4. Click the **TINA Tunnels** tab.
5. Right-click the table and select **Add new TINA Tunnel**. Alternatively, you can click the + sign in the top-right corner of the window.
6. Select **Add Tunnel**.
7. In the **Tunnel Name** field, enter a name for the new VPN tunnel.
8. Select a configured **Scheme** for the local network, or select **Explicit**.
9. For each local network at Location 2, add the address in the **Local** section. E.g., 10.0.81.0/24
10. For each remote network, add the address in the **Remote** section. E.g., 10.0.10.0/25



11. Configure the TINA tunnel settings to match the settings configured for Location 1. For more information, see the upper section in [TINA Tunnel Settings](#).
12. In the left menu, click **Transports**.
13. Click **+** to add a new transport. The **Edit Transport** window opens, showing the **Basic** tab.
14. Select the **Direction**. (At least one of the firewalls must be active.)

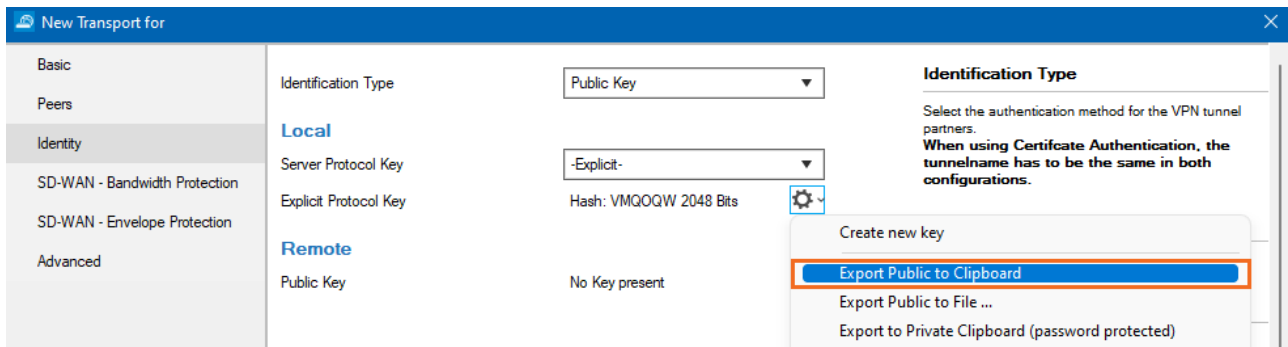


15. In the left menu, click **Peers**.
16. From the **Transport Source** list, select the IP address used to establish the VPN connection:
 - **First IP** – The connection gets established from the first Shared IP address.
 - **Second IP** – The connection gets established from the second Shared IP address.
 - **Dynamic (via routing)** – The firewall uses a routing table lookup to determine the IP address.
 - **Explicit List** – Enter one or more explicit IP addresses. Multiple IP addresses are tried in the listed order. Click **+** and add the addresses to the lists.
17. In the **Remote** section, add the tunnel destination network.
18. Configure the remaining transport and tunnel settings to match the configuration for Location 1. For more information, see the lower section in [TINA Tunnel Settings](#).

Step 4. Exchange the Public Keys Between the Local and Remote Firewall

Start with exporting the public key in the displayed window on the remote firewall.

1. Go to **CONFIGURATION > Configuration Tree > Box > your remote firewall > Assigned Services > VPN > Site to Site**.
2. Edit the transport for the TINA tunnel.
3. In the left menu, click **Identity**.
4. From the **Identification Type** list, select **Public Key**.
5. In the **Local** section, click the cog wheel icon next to **Server Protocol Key**, and export the public key to clipboard.



6. Click **OK** and close the **TINA Tunnel** configuration.
7. Go to **CONFIGURATION > Configuration Tree > Box > your local firewall > Assigned Services > VPN > Site to Site**.
8. Click **Lock**.
9. Select **TINA Tunnels**.
10. Open the configuration for the site-to-site tunnel transport created in Step 1.
11. In the left menu, click **Identity**.
12. In the **Remote** section, click the cog wheel icon next to **Public Key**, and import the key from the clipboard.

Remote

Public Key

No Key present



- Import from Microsoft Certificate Management...
- Import from Clipboard**
- Import from File...

13. Click **OK**.
14. Click **Send Changes** and **Activate**.
15. In the **Local** section, click the cog wheel icon next to **Server Protocol Key**, and export the key to the clipboard.
16. Click **OK** to close the **TINA Tunnel** window.
17. Go to **CONFIGURATION > Configuration Tree > Box > your remote firewall > Assigned Services > VPN > Site to Site**.
18. Click **Lock**.
19. Select **TINA Tunnels**.
20. Open the configuration for the site-to-site tunnel transport.
21. Click the **Identity** tab.
22. In the **Remote** section, click the cog wheel icon next to **Public Key**, and import the public key from the clipboard.
23. Click **OK** and close the **TINA Tunnel** window.
24. Click **Send Changes** and **Activate**.

After configuring the TINA VPN tunnel on both firewalls, you must also create an access rule on both systems to allow access to the remote networks through the VPN tunnel.

Next Step

Create access rules to allow traffic in and out of your VPN tunnel: [How to Create Access Rules for Site-to-Site VPN Access](#).

Figures

1. autovpn_tina.png
2. vpn_listeners_01.png
3. tina_net_90.png
4. trans01.png
5. call_active.png
6. transport_source_90_01.png
7. tina_net2_90.png
8. tina02_dir.png
9. export_public.png
10. import_public.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.