

How to Make a CloudGen Firewall Centrally Manageable Without a Control Center

<https://campus.barracuda.com/doc/96026024/>

If you are managing only one or two remote Barracuda CloudGen Firewalls and are not using a Barracuda Firewall Control Center, use Site-to-Site VPN tunnels to securely manage the remote units. Exchange the box certificates to authenticate the Site-to-Site VPN tunnel.

Step 1. Export the Public Key

Export the box identification certificate from the remote box. The certificate is used to authenticate the remote Barracuda CloudGen Firewall.

1. Go to **CONFIGURATION > Configuration Tree > Box > Identity**.
2. From **Box Private Key**, click **Ex/Import** and select **Export Public to Clipboard**.

Step 2. Configure a Site-to-Site Tunnel at the VPN Server Peer

Configure the Site-to-Site VPN tunnel on the central unit. The remote management tunnel is a site-to-site tunnel.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Site to Site**.
2. Click **Lock**.
3. Right-click the table and select **New TINA tunnel**.
4. Enter a **Name** for the tunnel.
5. Under the **Local Networks** tab, select **Passive** from the **Call Direction** list.
6. In the **Network Address** section, enter the LAN and any other connected private subnets you wish to connect from, and click **Add**.
7. Click the **Local** tab.
8. In the **IP Address or Interface used** section, select or enter the external IP address that the remote box will connect to (reference: first or second server IP, or select **Explicit List (ordered)** and enter below).
9. Click the **Peer Identification** tab.
10. From **Public Key**, click **Ex/Import** and select **Import from Clipboard**.
 - If necessary, change **Identity > Identification Type: Public Key**.
11. Click the **Identify** tab.
12. From the **Server Protocol Key** list, click **Ex/Import** and select an RSA key or create a new key.

- Keys in the drop-down menu are created/imported under **VPN Settings > Service Certificates/Keys**.

13. In the **Server Protocol Key** section, export the public key to clipboard.
14. Click the **Remote** tab.
15. In the **Remote Peer IP Addresses** field, enter either 0.0.0.0/0 (if the remote partner uses a dynamic IP), or the external IP of the remote partner (if static), and click **Add**.
16. Click the **Remote Networks** tab.
17. Choose a free IP address for your virtual IP (VIP) address, enter this address in the **Remote Network** section, and click **Add**.

The VIP may be either routed (it is within a network range not used on either local or remote sites) or it may be part of the local LAN connected to your central firewall. In this case, you must create a Proxy ARP to be able to connect (see: [How to Create Proxy ARP Objects](#)). Do not use the remote Management IP from the remote LAN.
18. Click **OK**.
19. Click **Send Changes** and **Activate**.

For more information about TINA tunnels, see [How to Create a TINA VPN Tunnel between CloudGen Firewalls](#).

Step 3. Configure Remote Access

Configure the remote partner to connect to the central firewall:

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. In the left menu, select **Management Access**.
3. In the left menu, expand **Configuration Mode**, and click **Switch to Advanced**.
4. Click **Lock**.
5. From the **Enable Tunnel** list, select **yes**.
6. In the **Virtual IP (VIP)** field, enter the VIP address chosen in Step 2.17.
7. From **Tunnel Details**, click **Set**.
 1. From **VPN Server Key**, click **Ex/Import** and select **Import from Clipboard**.
 2. In the **VPN Server** table, add the point of entry to reach the central gateway (defined under Step 2.8).
 3. In the **Remote Networks** table, add the remote LANs (defined under Step 2.7).
 4. Add an IP address of the central firewall to the list of **Reachable IPs**. This IP address will be used as probing target to keep the tunnel alive. If no probing target is defined, the tunnel will be restarted periodically.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Go to **VPN > Status** and verify that the site-to-site tunnel is **ACTIVE** in the state column.

© 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.