Barracuda CloudGen Firewall

How to Configure VPN Access via a Dynamic WAN IP Address

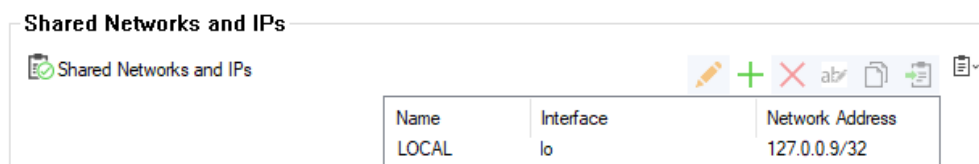https://campus.barracuda.com/doc/17389/

Services running on a firewall cannot be configured to listen on dynamic IP addresses on the box layer of the Barracuda CloudGen Firewall. To use a VPN service on a Barracuda CloudGen Firewall with dynamic WAN connections, configure the firewall to use a localhost IP address (127.0.0.X) and configure the VPN service to listen on the DCHP device. Alternatively, you can configure the VPN service to use the localhost IP address as a listening IP and create an app redirect access rule to redirect all incoming VPN traffic to the local VPN service. For IPsec, you can configure the VPN service to create a listener on every available IP address, making the app redirect access rule unnecessary.

Step 1. Configure VPN Service Listening IP on the Firewall

Verify that services running on the box can use 127.0.0.9 as a listening IP address.

- Go to **CONFIGURATION > Configuration Tree > Box > Network**.
- Scroll down to the **Shared Networks and IPs** section and make sure that the IP address is listed under **Shared Networks and IPs**.
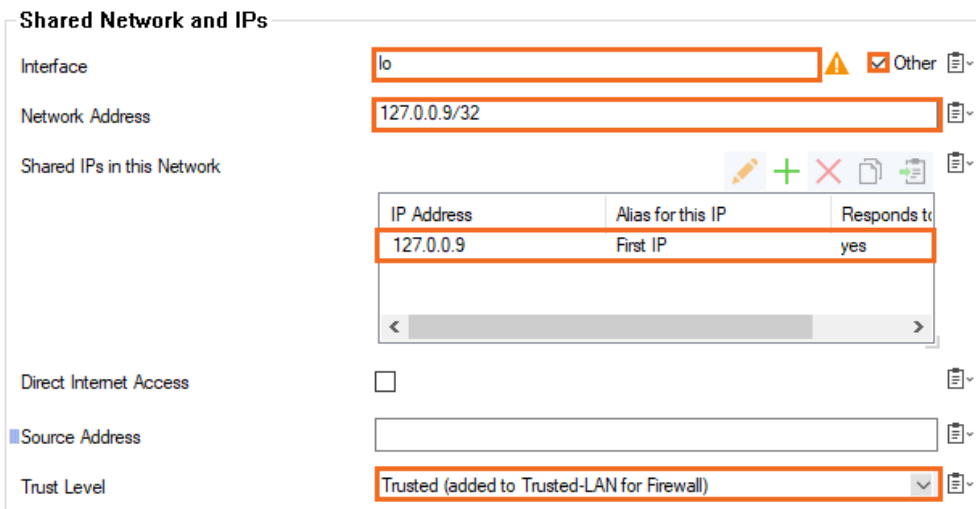

If there is no local address configured, add the shared network.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. In the **Shared Networks and IPs** section, click **+**. The **Shared Networks and IPs** window opens.
3. Enter a name for the new shared network.
4. Click **OK**. The **Shared Networks and IPs <your shared network name>** window opens.
5. For **Interface**, select **Other** and enter `lo` for the local interface on which the shared network must be reachable.
6. Enter the **Network Address** `127.0.0.9/32` for the network on the selected interface.
7. Next to **Shared IPs in this Network**, click **+**. The **Shared IP Address Configuration** window opens.
8. In the **IP Address** field, enter `127.0.0.9`
9. For **Alias for this IP**, select **First IP**.
10. Set **Responds to Ping** to **yes**.
11. Click **OK**.

12. For **Trust Level**, select **Trusted**.

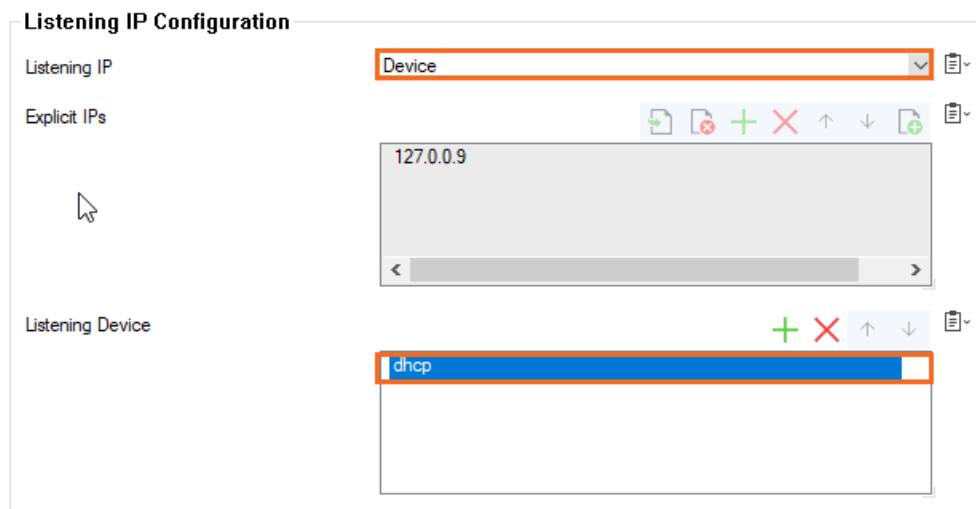13. Click **OK**. The shared IP address is added to the list of **Shared IPs in this Network**.
14. Click **OK**.
15. Click **Send Changes** and **Activate**.

Step 2. Configure the Listener on the VPN Service

Configure the VPN service to listen on the DHCP device.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Service Properties**.
2. Click **Lock**.
3. From the **Listening IP** drop-down menu, select **Device**.
4. Next to **Listening Device**, click **+** and enter dhcp.

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

Alternatively, you can configure the VPN service to use the 127.0.0.9 listening IP address configured in Step 1 as a service IP address. In this case, you must also create an app redirect rule.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Service Properties**.
2. Click **Lock**.
3. From the **Service Availability** drop down, select **Explicit**.
4. Click **+** and add the IP address `127.0.0.9` to the **Explicit Service IPs** table.
5. Click **Send Changes** and **Activate**.
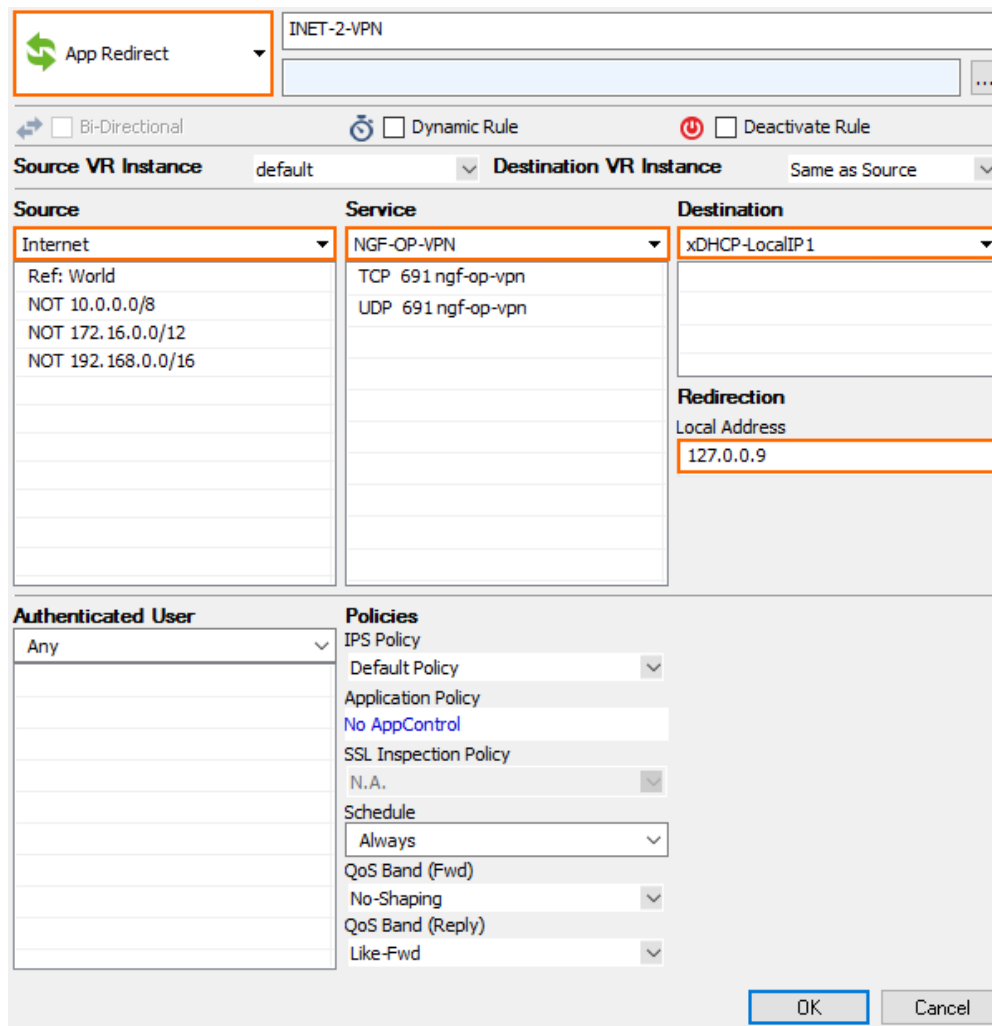
Step 3. Create a VPN Tunnel

Create a VPN TINA tunnel. On the local firewall, under the **Local** tab, select **Explicit List (ordered)** as the **IP Address used for Tunnel Address**. Select **Explicit List (ordered)** and enter `0.0.0.0` as the listening IP address.

For more information, see How to Create a TINA VPN Tunnel between CloudGen Firewalls.

Step 4. (optional) Create an App Redirect Access Rule

If the VPN service is configured to use the 127.0.0.9 listening IP address as service IP address, create an app redirect rule to redirect all incoming VPN traffic on the dynamic WAN interface to the VPN service:

- **Action** – Select **App Redirect**.
- **Source** – Select **Internet**.
- **Service** – Select **NGF-OP-VPN**.
- **Destination** – Select the network object for your dynamic WAN connection. E.g., **xDHCP-LocalIP1** or **xDSL-LocalIP1**.
- **Redirection** – Enter `127.0.0.9`.

For more information, see How to Create an App Redirect Access Rule.

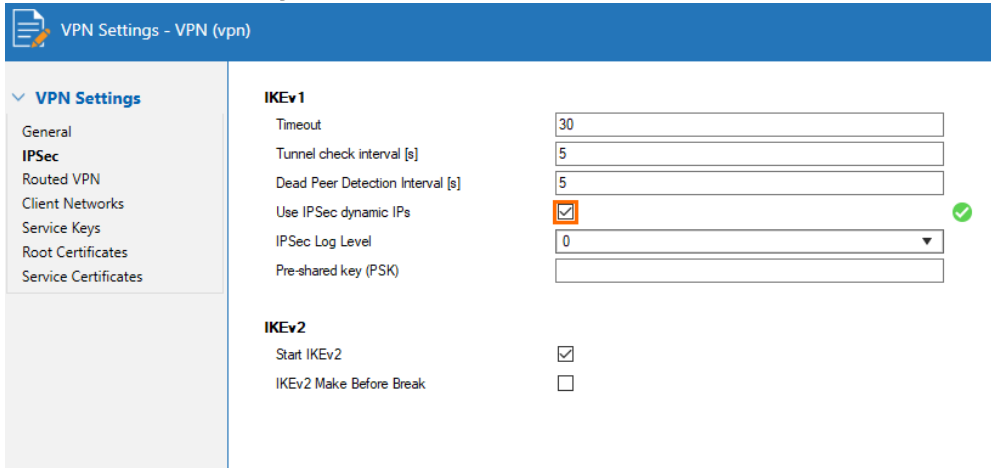All incoming VPN traffic is now redirected to the VPN service listening on 127.0.0.9.

IPsec VPN Service Listener on All IP Addresses

When using IPsec, configure the VPN service to listen on all available IP addresses including all dynamic IP addresses. No additional access rules are required.

This parameter is limited to IPsec VPN configurations.

Configure the VPN Service IP

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. In the left navigation bar, click **IPSec**.
4. Enable **Use IPSec dynamic IPs**.

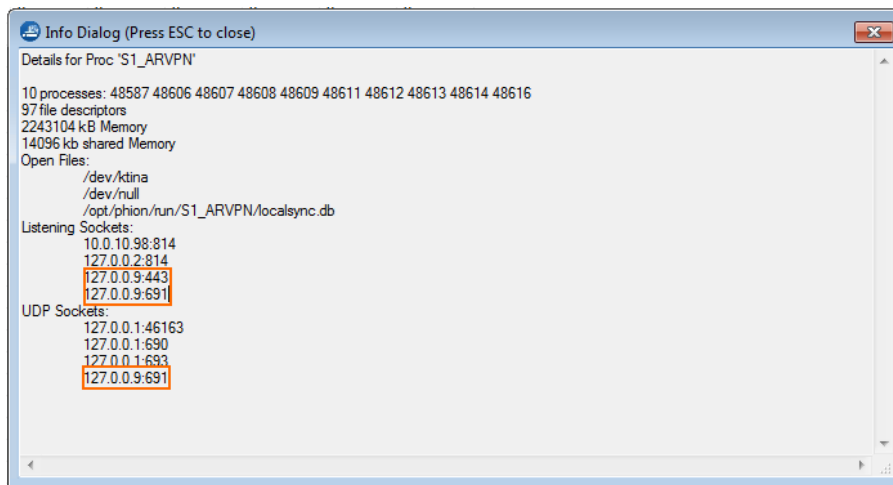5. Click **Send Changes** and **Activate**.

Create a VPN Tunnel

Create a VPN IPsec tunnel. For IKEv1: On the local firewall, in the **Local Networks** settings, enter `0.0.0.0` or `::0` as the **Local IKE Gateway**. For IKEv2: On the local firewall, under the **Network Local** tab, enter `0.0.0.0` as the **Local Gateway**.

For more information, see How to Configure a Site-to-Site IPsec IKEv1 VPN Tunnel and How to Configure a Site-to-Site IPsec IKEv2 VPN Tunnel.
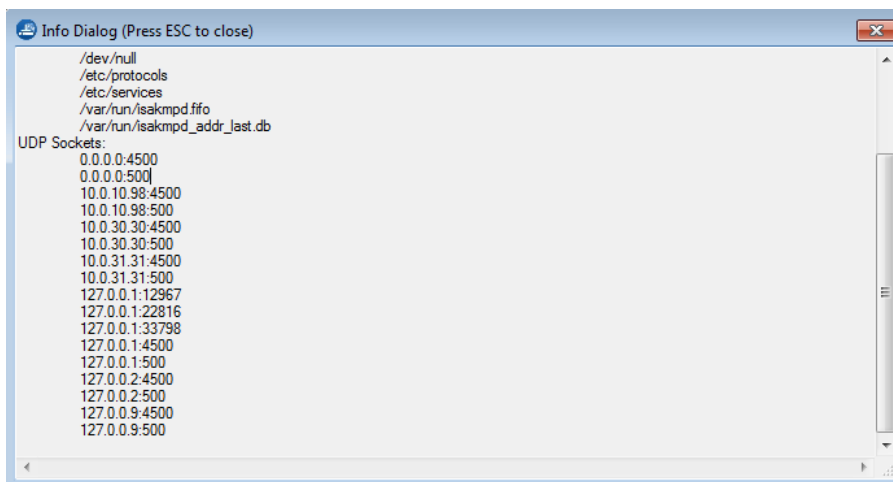
Verify the Listening IP Addresses for the VPN Service

Open the **CONTROL > Resources** page and double-click either on the VPN service process (e.g., S1_ARVPN) for TINA tunnels, or on the **ike3** process for IPsec tunnels. In the **Info Dialog** window, check to see if the VPN service is listening on the IP addresses you configured above (e.g., 127.0.0.1 or 0.0.0.0/0).

VPN service

ike3 process with Use dynamic IPs enabled

DynDNS

Dynamic WAN connections may change the public IP address regularly. Configure DynDNS to continuously update a DynDNS hostname to always resolve to the current public IP address used by the CloudGen Firewall. VPN clients then use the DynDNS hostname to connect to the CloudGen Firewall VPN service.

Figures

1. local_vpn.png
2. local_vpn_conf.png
3. device_conf.png
4. VPN_dynWAN01.png
5. enable_UseIPSecdynamicIPs.png
6. VPN_dynWAN03.png
7. VPN_dynWAN02.png