How to Configure VPN Access via a Dynamic WAN IP Address

https://campus.barracuda.com/doc/73719162/

Services running on a virtual server can not 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 VPN service to listen on a localhost IP address (127.0.0.X) and then create an app redirect access rule to redirect all incoming VPN traffic to the local VPN service. For IPsec you can alternatively, configure the VPN service to create a listener on every available IP address, making the app redirect access rule unnecessary.

Configure VPN Service Listener on 127.0.0.9

Configure the virtual server and the VPN service to listen on 127.0.0.9 and then use an app redirect access rule to redirect VPN traffic to the VPN service on the localhost.

Step 1. Add the Virtual Server IP Address

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Server Properties**.
2. Click **Lock**.
3. In the **Additional IP** table, click **+**. The **Additional IP** window opens:
   - **Additional IP** – Enter `127.0.0.9`
   - **Reply to Ping** – Select **Yes**.
4. Click **OK**.
5. Click **Send Changes** and **Activate**.

Services running on the virtual server can now use 127.0.0.9 as a listening IP address.

Step 2. Configure the VPN Service IP

Configure the VPN service to use the 127.0.0.9 listening IP address configured in step 1 as a Service IP address.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > 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

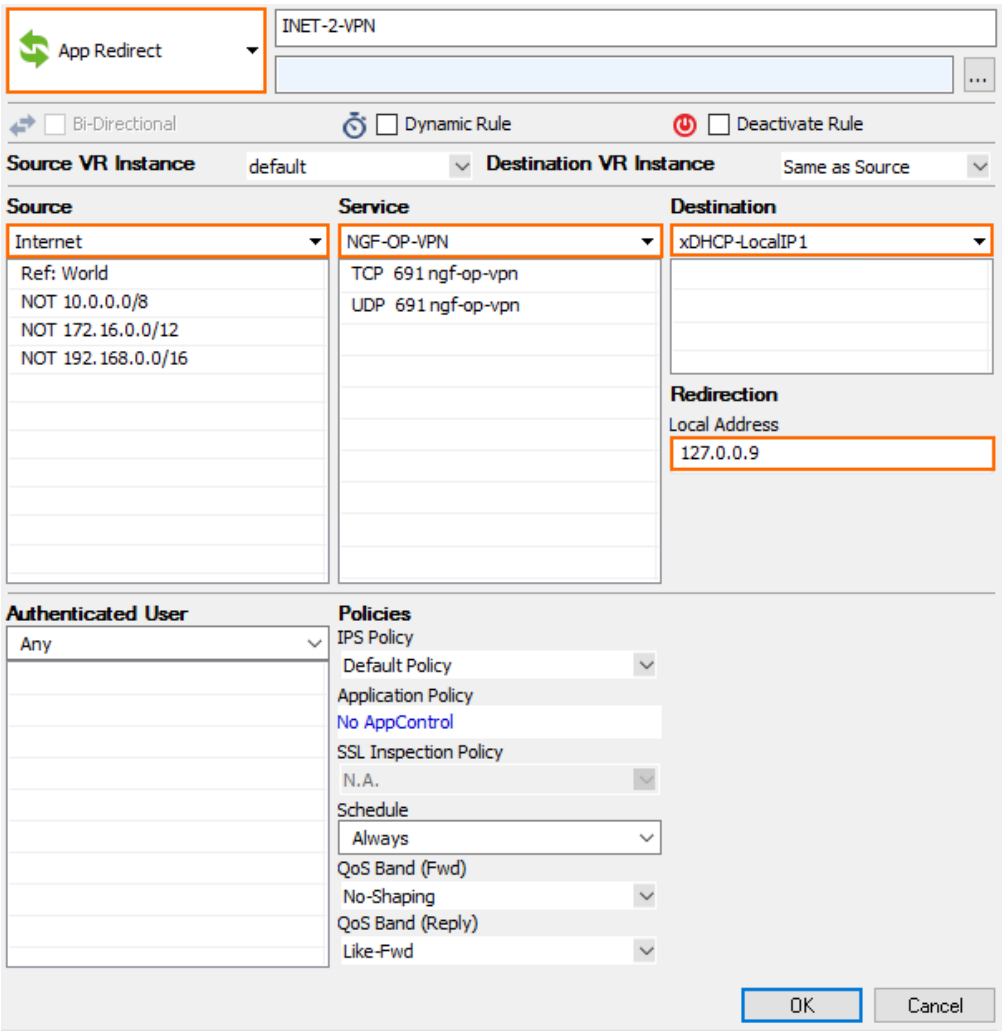
Create a VPN TINA tunnel. On the local firewall, under the **Local** tab, select **Explicit List (ordered)** as the **IP Address used for Tunnel Address**. Select **Explicit List (ordered)** and enter `0.0.0.0` as the listening IP address.

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

Step 4. Create an App Redirect Access Rule

Create an access 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

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 > Virtual Servers > your virtual server > Assigned Services > VPN-Service > VPN Settings**.
2. Click **Lock**.
3. Click the **Click here for Server Settings** link. The **Server Settings** window opens.
4. Click on the **Advanced** tab.
5. In the **IKE Parameter** section, set **Use IPSec dynamic IPs** to **Yes**.
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Create a VPN Tunnel

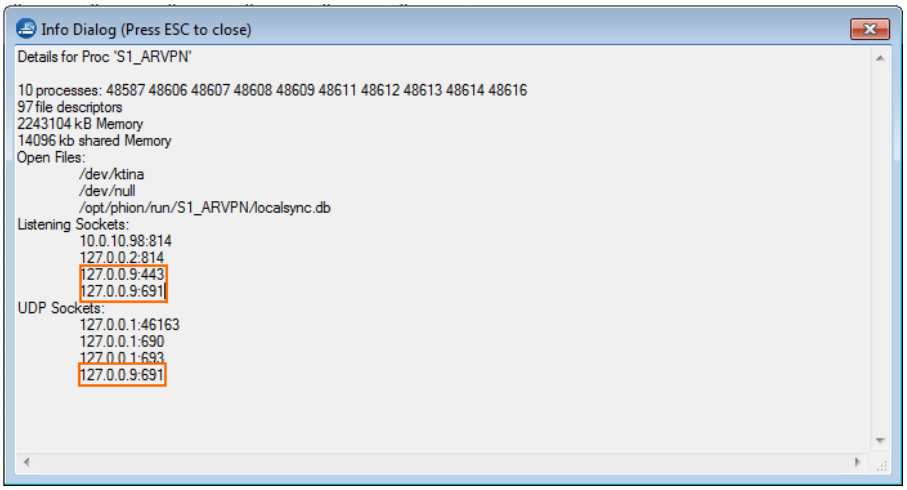
Create a VPN IPsec tunnel. For IKEv1: On the local firewall, in the **Local Networks** settings, enter `0.0.0.0` or `::0` as the **Local IKE Gateway**. For IKEv2: On the local firewall, under the **Network Local** tab, enter `0.0.0.0` as the **Local Gateway**.

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.

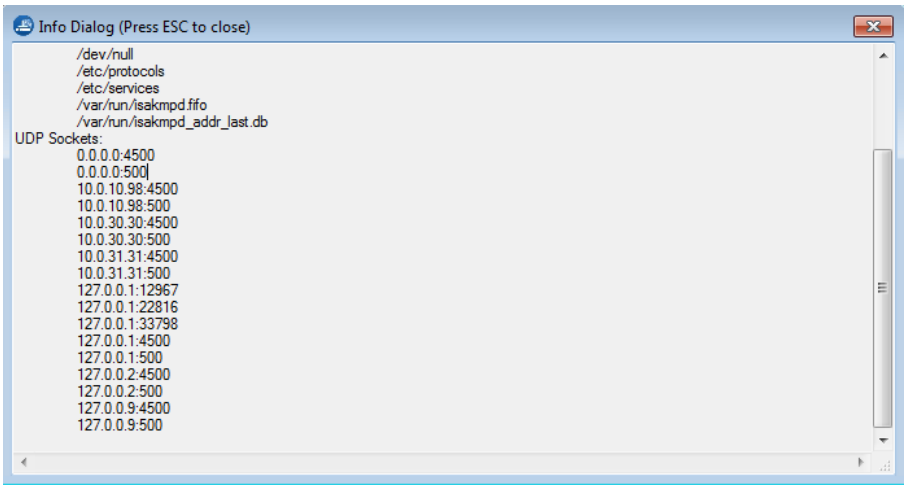
Verify the Listening IP Addresses for the VPN Service

Open the **CONTROL > Resources** page and double click on the VPN service process (e.g., S1_ARVPN) for TINA tunnels, or 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 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. VPN_dynWAN01.png
2. VPN_dynWAN03.png
3. VPN_dynWAN02.png