How to Configure a DHCP Relay over a VPN Tunnel

https://campus.barracuda.com/doc/96026057/

To use the same DHCP server in two different networks that are connected by a VPN tunnel, configure DHCP relays on both the local and remote Barracuda CloudGen Firewalls. The DHCP server is located on the local site; the DHCP clients reside on the remote site.
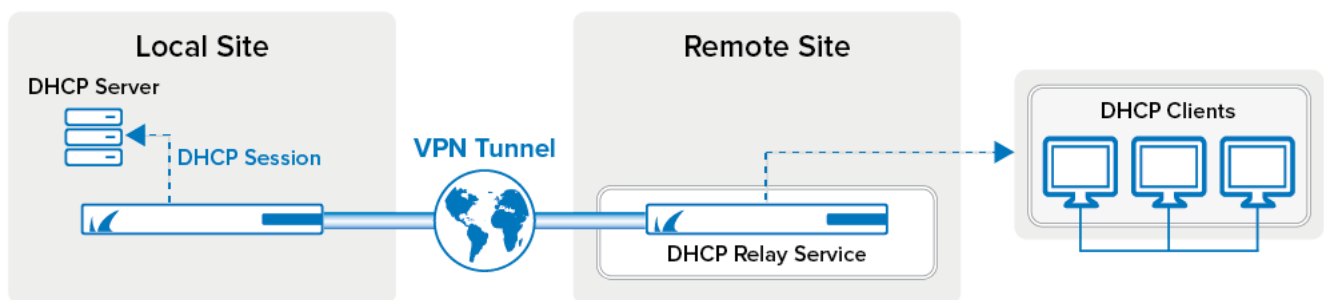
Before You Begin

- Create a Site-to-Site VPN tunnel between both locations.
- Use a separate DHCP server, such as the DHCP server on Windows Servers in your network. It is not possible to use the DHCP service on the CloudGen Firewall in this scenario.

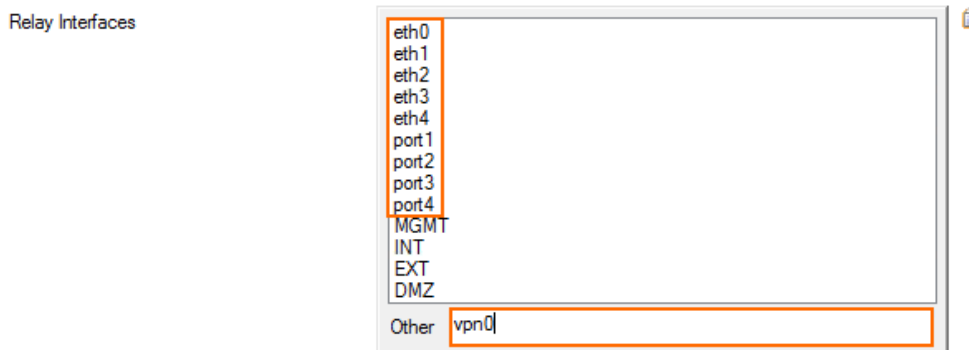## Step 1. Create an Access Rule on the Local Firewall

Create a PASS access rule allowing the management IP address of the remote CloudGen Firewall access to the DHCP server.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Right-click in the main are and select **New** and **Rule**. The **Edit Rule** window opens.
4. Create the following access rule:
   - **Action** – Select **PASS**.
   - **Source** – Enter the management IP address of the remote CloudGen Firewall.
   - **Service** – Create and select a Service object for UDP Port 67.
   - **Destination** – Enter the IP address of the DHCP server.
   - **Connection** – Select **Original Source IP**.
5. Click **OK**.
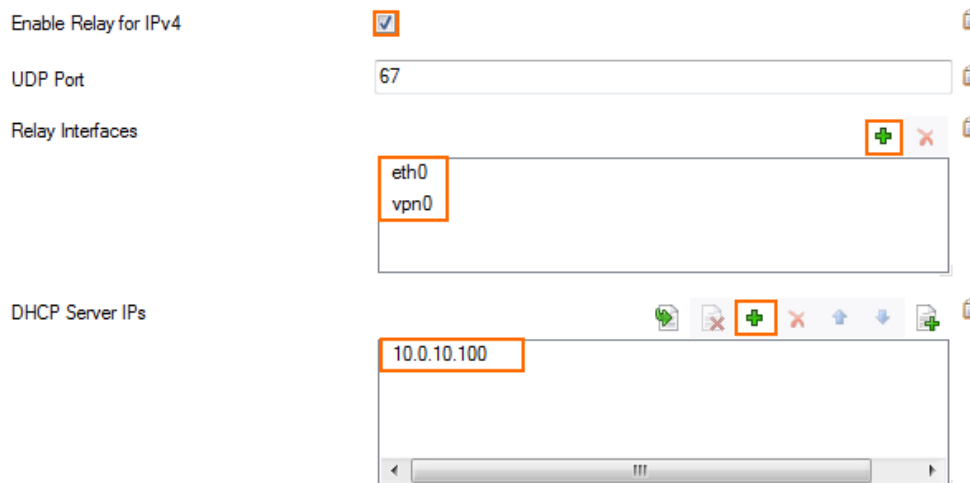6. Click **Send Changes** and **Activate**.

Step 2. Create a DHCP Relay on the Remote Firewall

Configure DHCP Relay on the remote CloudGen Firewall to pass along

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > DHCP Relay > DHCP Relay Settings**.
2. Click **Lock**.
3. Select the **Enable Relay for IPv4** check box.
4. Click **+** for each **Relay Interface** the DHCP Relay listens on:
    1. Select the internal interface used to connect to the DHCP server from the list. E.g., **eth0**
    2. Enter the VPN interface used for the Site-to-Site tunnel in the **Other** textbox. E.g., vpn0

5. Click **+** and add the **DHCP Server IPs**. E.g., 10.0.10.100

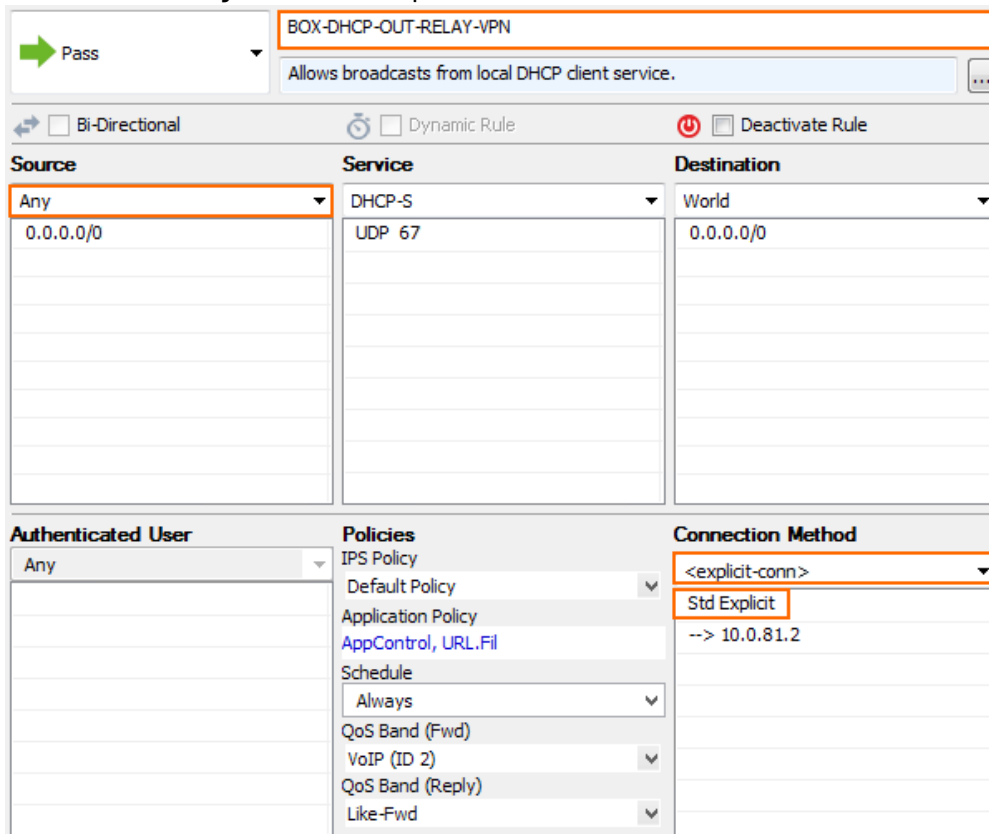6. Click **Send Changes** and **Activate**.

Step 3. Create a Host Firewall Rule on the Remote Firewall

Create an access rule to allow the traffic of the DHCP Relay service into the VPN tunnel.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Host**

Firewall Rules.
2. Click **Lock**.
3. Click on the **Outbound** rule set.
4. Create a new PASS access rule. The **Edit Rule** window opens.
5. Enter the **Name** of the rule. E.g., `BOX-DHCP-OUT-RELAY-VPN`
6. Use the following settings for the access rule:
    ○ **Action** – Select **PASS**.
    ○ **Source** – Select **Any**.
    ○ **Service** – Select **DHCP-S**.
    ○ **Destination** – Select **World**.
7. Select **<explicit-conn>** from the **Connection Method** list.
8. Double-click **Std Explicit** in the **Connection Method** section. The **Edit / Create a Connection Object** window opens.

9. From the **Translated Source IP** list, select **Explicit IP**.
10. Enter the management IP address of the CloudGen Firewall as the **Explicit IP**.

> In case the management IP/network is not inside the VPN Site-to-Site tunnel, you must enter an available server IP that is also part of the tunnel configuration (local network), to reach the DHCP server.

11. Click **OK**.
12. Click **OK**.
13. Place the access rule above the **BOX-DHCP-OUT** rule.
14. Click **Send Changes** and **Activate**.

Clients in the remote network can now receive DHCP leases from the DHCP server in the local network.

Figures

1. dhcp_rel_vpn01.png
2. relay01.png
3. relay02.png
4. relay05.png
5. relay06.png