How to Create an AutoVPN Tunnel via REST API

https://campus.barracuda.com/doc/87785550/

AutoVPN allows you to establish a VPN connection between two or more CloudGen Firewalls using the command line interface or the REST API. To use AutoVPN on the CLI, see How to Create an AutoVPN Tunnel via the Command Line Interface.

First, initiate a server session on the first firewall that listens to incoming VPN connection requests from the second firewall. Next, connect the second firewall to the first one by authenticating with a token that was previously generated on the first firewall. To connect more than one firewall to the listener, repeat the second step on each firewall you want to connect to the first one.

	First Firewall	Second Firewall
Public IP	34.241.43.25	52.213.101.46
Private Network	172.31.0.0/20	10.0.0.0/24

Before You Begin

- Enable REST API on your CloudGen Firewall. See REST API.
- Download and install a REST API client on your client. For example, you can use Insomnia: https://insomnia.rest/.
- AutoVPN uses TCP port 694 for configuration and UDP port 691 for the TINA tunnel. Ensure that these ports are not used for any other purpose and are both reachable. For more information, see Best Practice - Core System Configuration Files and Ports Overview.
- AutoVPN listens on the IP address of the VPN service. If there is no VPN service, AutoVPN creates it and uses the default settings for the listening IP. Verify that the ports 691 and 694 are linked to the VPN service.
- On CloudGen Firewall deployments in the public cloud, Cloud Integration must be configured. For more information, see Cloud Integration.

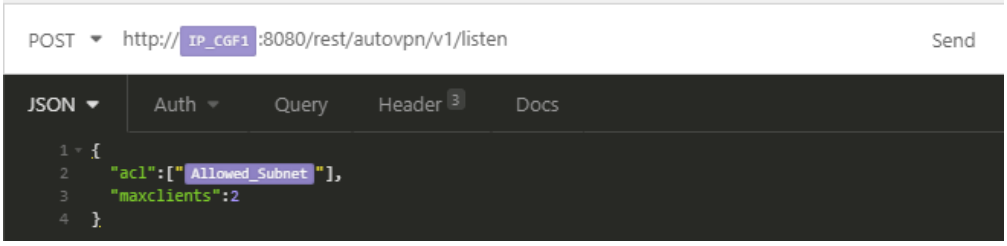
Step 1. Create a Session on the First Firewall Initiating a Listener

The listener will wait for connection requests from a firewall in the network 52.213.101.0/24.

1. Open your REST API client.
2. Select **POST** as **method** and enter `http://34.241.43.25:8080/rest/autovpn/v1/listen` in the URL field.
3. Select **JSON** as body type and enter the following value for the body:

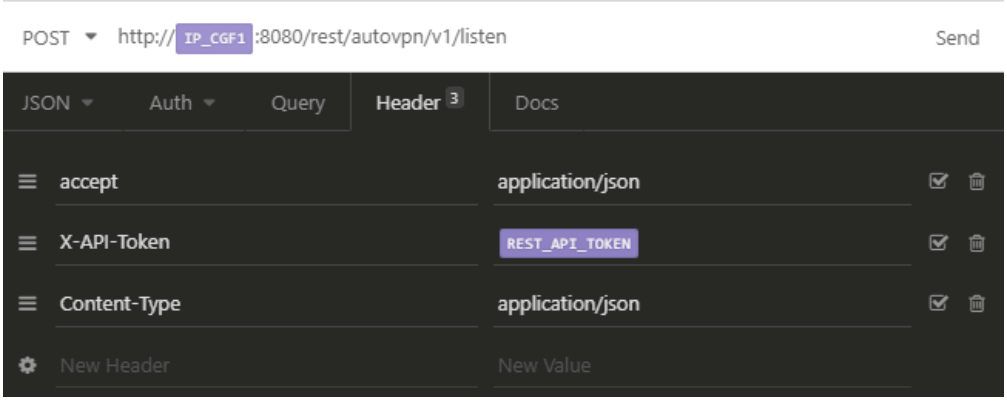
```
{"acl":["52.213.101.0/24"],"maxclients":2}
```

4. **ACL** is the subnet of the client connecting to the first firewall, and **maxclients** is the number of maximum allowed clients that can connect to the first firewall.



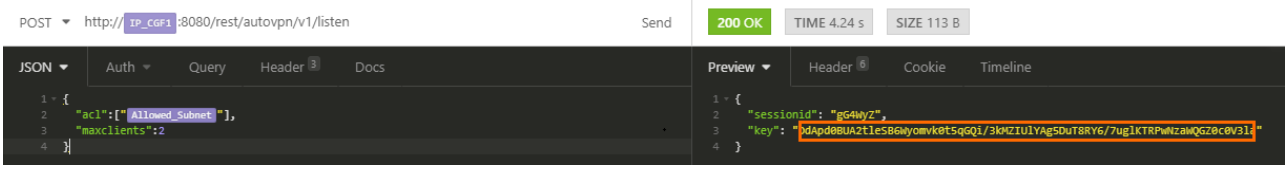
5. In the header section, enter the following header names and the following values:

Header Name	Header Value
accept	application/json
X-API-Token	<your_REST_API_token_1st_firewall>
Content-Type	application/json



To create a REST API token, see REST API.

6. Click **Send** and you will receive the session ID and the token from the first firewall.



7. Copy the token. You can find it in the line **key**.

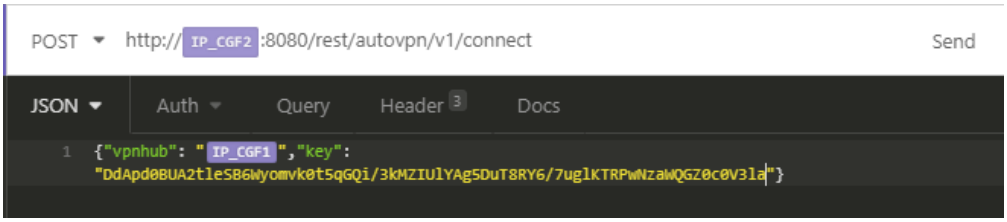
Step 2. Create a Session on the Second Firewall to Connect to the First Firewall Waiting for Connection Requests

Repeat this step on each CloudGen Firewall you want to connect to the first firewall.

1. Open your REST API client.
2. Select **POST** as **method** and enter `http://52.213.101.46:8080/rest/autovpn/v1/connect` in the URL field.
3. Select **JSON** as body type and enter the following value for the body:

   ```
   {"vpnhub": "34.241.43.25","key": "<token_created_by_first_firewall>"}
   ```

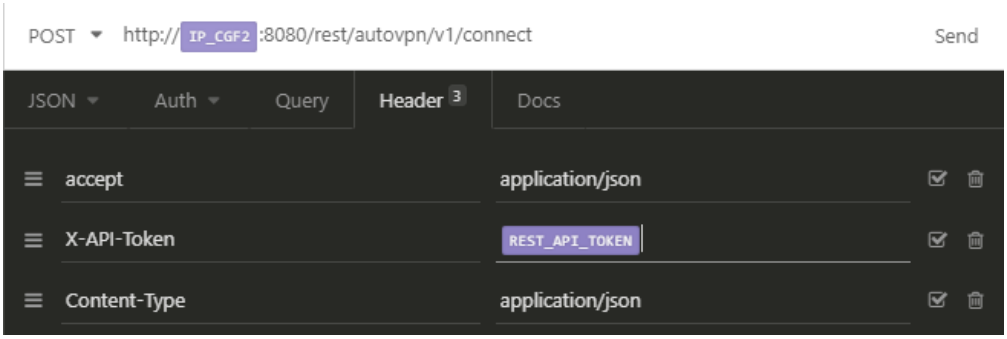
4. **VPNHUB** is the IP address of the first firewall, and the token is the token created by the first firewall.

5. In the header section, enter the following header names and the following values:

Header Name	Header Value
accept	application/json
X-API-Token	<your_REST_API_token_2nd_firewall>
Content-Type	application/json

   To create a REST API token, see REST API.

6. Click **Send** and you will receive the session ID.

7. The VPN tunnel is now established.

Step 3. (for public cloud deployments only) Activate Routing Between Local Cloud Networks and the VPN-Site on Both Firewalls

This step is necessary only on CloudGen Firewall deployments in the public cloud. For all other deployments, continue with Step 4.

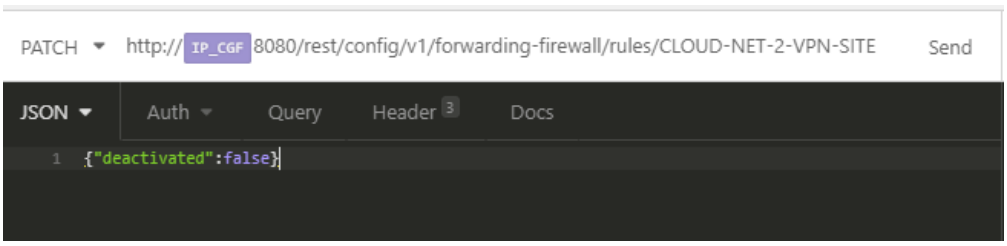
Activate the access rule **CLOUD-NET-2-VPN-SITE**. Repeat the following steps for both firewalls.

This can be done using either Firewall Admin or REST API.

Configuration via REST API

1. Open your REST API client.
2. Select **PATCH** as **method** and enter `http://<CGF_IP>:8080/rest/config/v1/forwarding-firewall/rules/CLOUD-NET-2-VPN-SITE` in the URL field.
3. Select **JSON** as body type and enter the following value for the body:

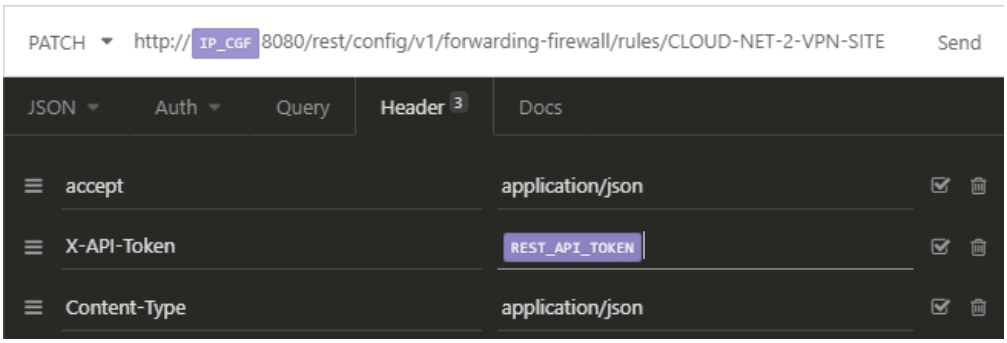
   ```
   {"deactivated":false}
   ```

4. In the header section, enter the following header names and the following values:

Header Name	Header Value
accept	application/json
X-API-Token	<your_REST_API_token>
Content-Type	application/json

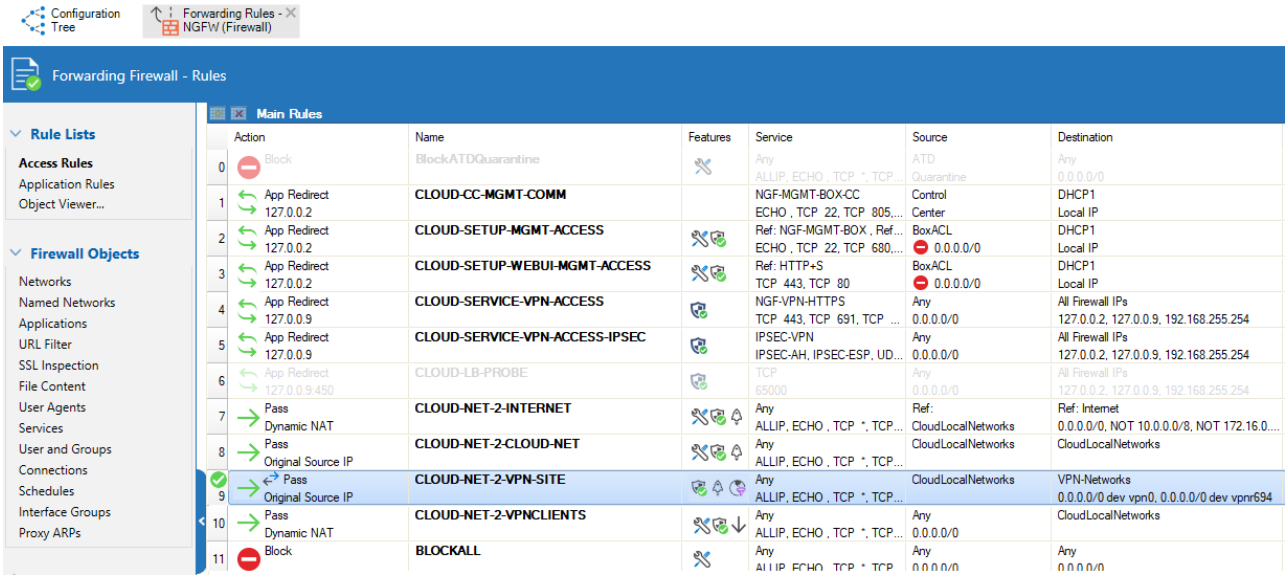
   To create a REST API token, see REST API .

5. Click **Send.**

Configuration in Firewall Admin

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules.**
2. Click **Lock**.
3. Right-click the access rule **CLOUD-NET-2-VPN-SITE**.
4. Click **Activate Rule** in the list.



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

Step 4. (for all deployments except public cloud) Activate Routing Between Local Networks and the VPN-Site on Both Firewalls

This step is necessary on all deployments except public cloud deployments.

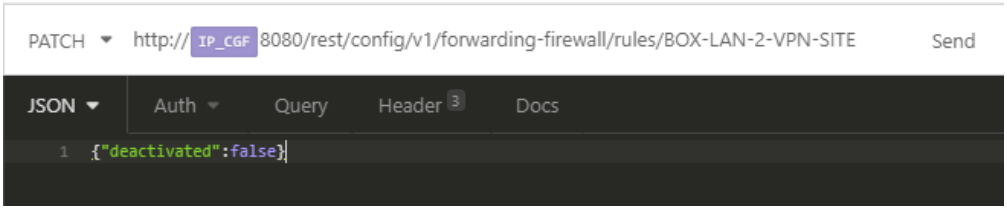
Activate the access rule **BOX-LAN-2-VPN-SITE**. Repeat the following steps for both firewalls.

This can be done using either Firewall Admin or REST API.

Configuration via REST API

1. Open your REST API client.
2. Select **PATCH** as **method** and enter `http://<CGF_IP>:8080/rest/config/v1/forwarding-firewall/rules/BOX-LAN-2-VPN-SITE` in the URL field.
3. Select **JSON** as body type and enter the following value for the body:

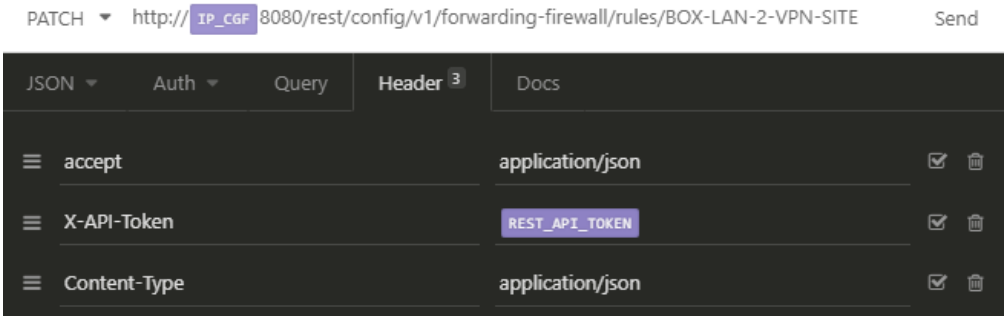
```
{"deactivated":false}
```



4. In the header section, enter the following header names and the following values:

Header Name	Header Value
accept	application/json
X-API-Token	<your_REST_API_token>
Content-Type	application/json

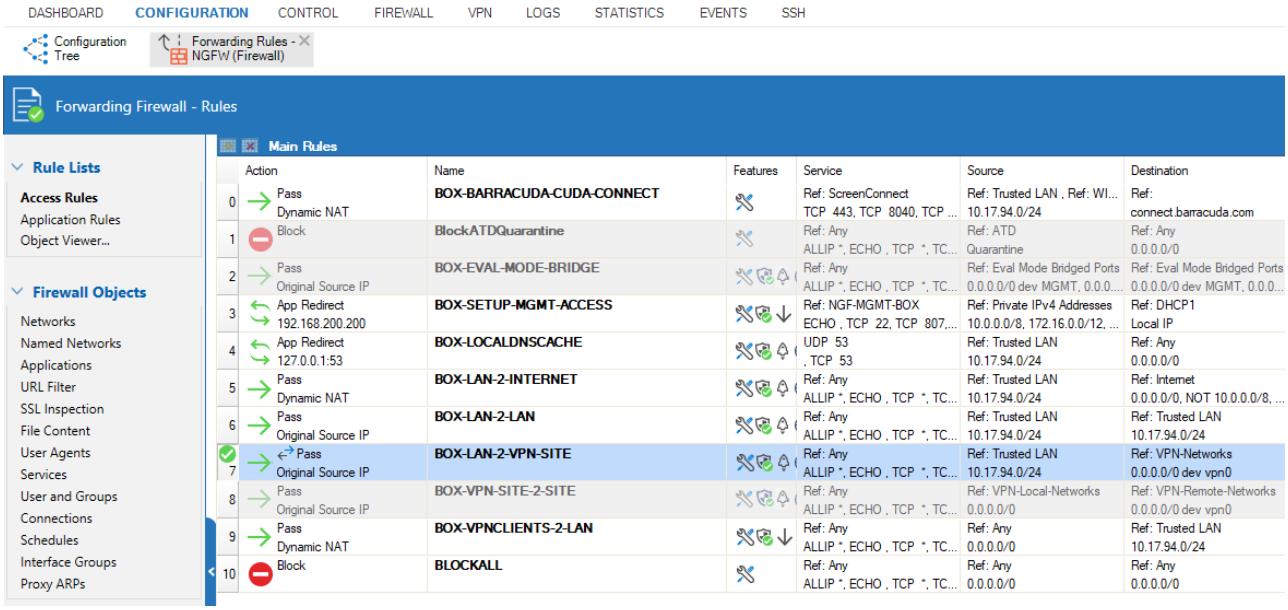
To create a REST API token, see REST API.



5. Click **Send**.

Configuration in Firewall Admin

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Right-click the access rule **BOX-LAN-2-VPN-SITE**.
4. Click **Activate Rule** in the list.



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

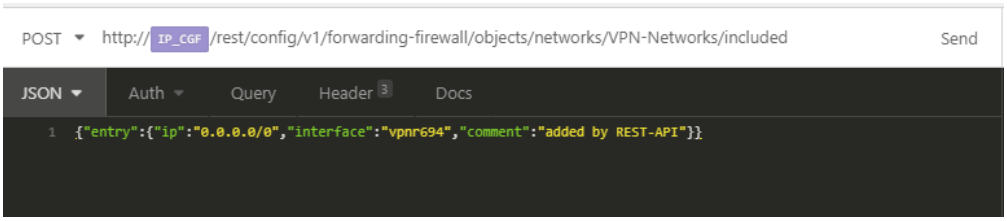
Step 5. Add AutoVPN to the Network Object VPN-Networks on Both Firewalls

This can be done using either Firewall Admin or REST API.

Configuration via REST API

1. Open your REST API client.
2. Select **POST** as **method** and enter `http://<CGF_IP>:8080/rest/config/v1/forwarding-firewall/objects/networks/VPN-Networks/included` in the URL field.
3. Select **JSON** as body type and enter the following value for the body:

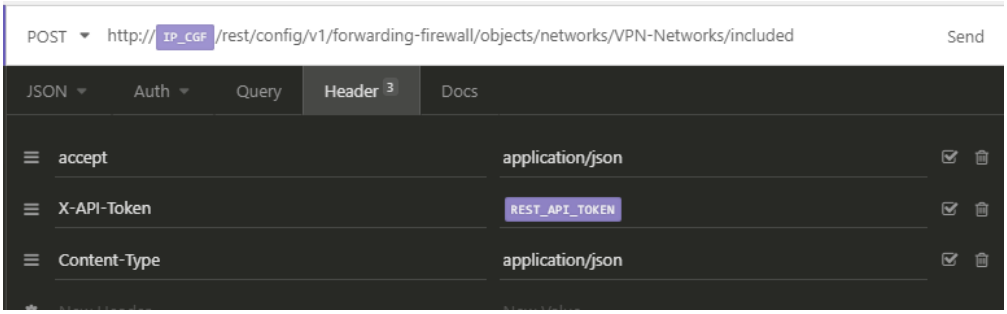
```
{"entry":{"ip":"0.0.0.0/0","interface":"vpnr694","comment":"added by REST-API"}}
```



4. In the header section, enter the following header names and the following values:

Header Name	Header Value
accept	application/json
X-API-Token	<your_REST_API_token>
Content-Type	application/json

To create a REST API token, see REST API.

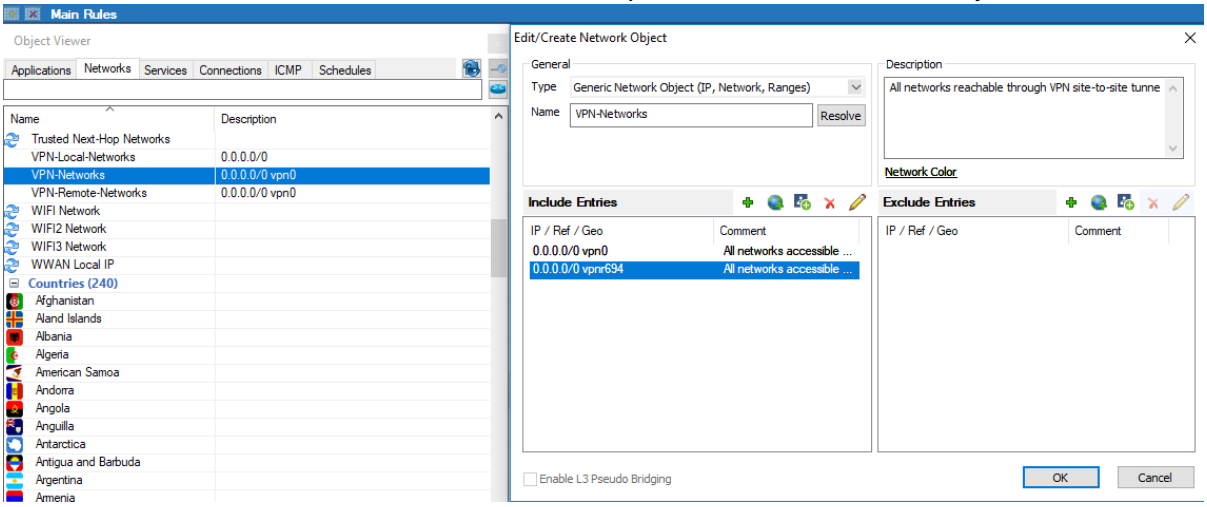


5. Click **Send**.

Configuration in Firewall Admin

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, cli ck **Networks**.

3. In the list, double-click the network object **VPN-Networks** for modifying.
4. Click **+** to add `IP 0.0.0.0/0` with interface `vpnr694` to the network object **VPN-Networks**.

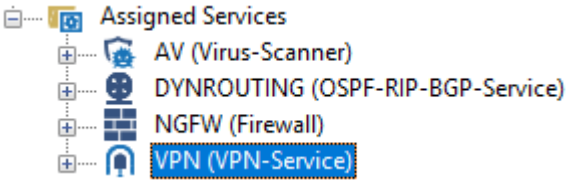


5. Click **OK**.
6. Click **Send Changes** and **Activate**.

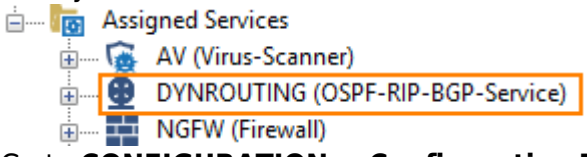
Step 6. (optional) Verify that the AutoVPN TINA Tunnel is Set Up Correctly on the First Firewall

Log into the first firewall. Verify that the VPN and dynamic routing services have been set up correctly and that the AutoVPN TINA tunnel is up.

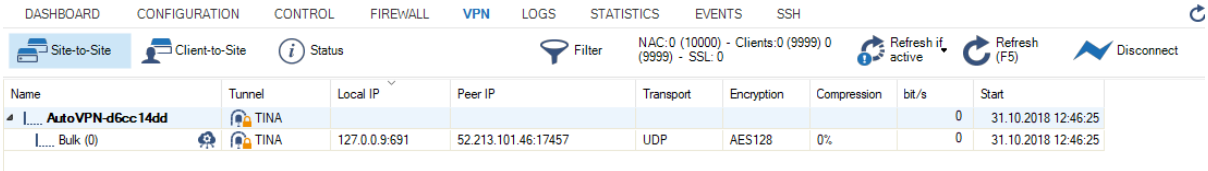
1. On your first firewall, go to **CONFIGURATION > Configuration Tree > Box > Assigned Services**. Because no VPN service has been set up prior to this configuration, you will now see the new, automatically configured VPN service:



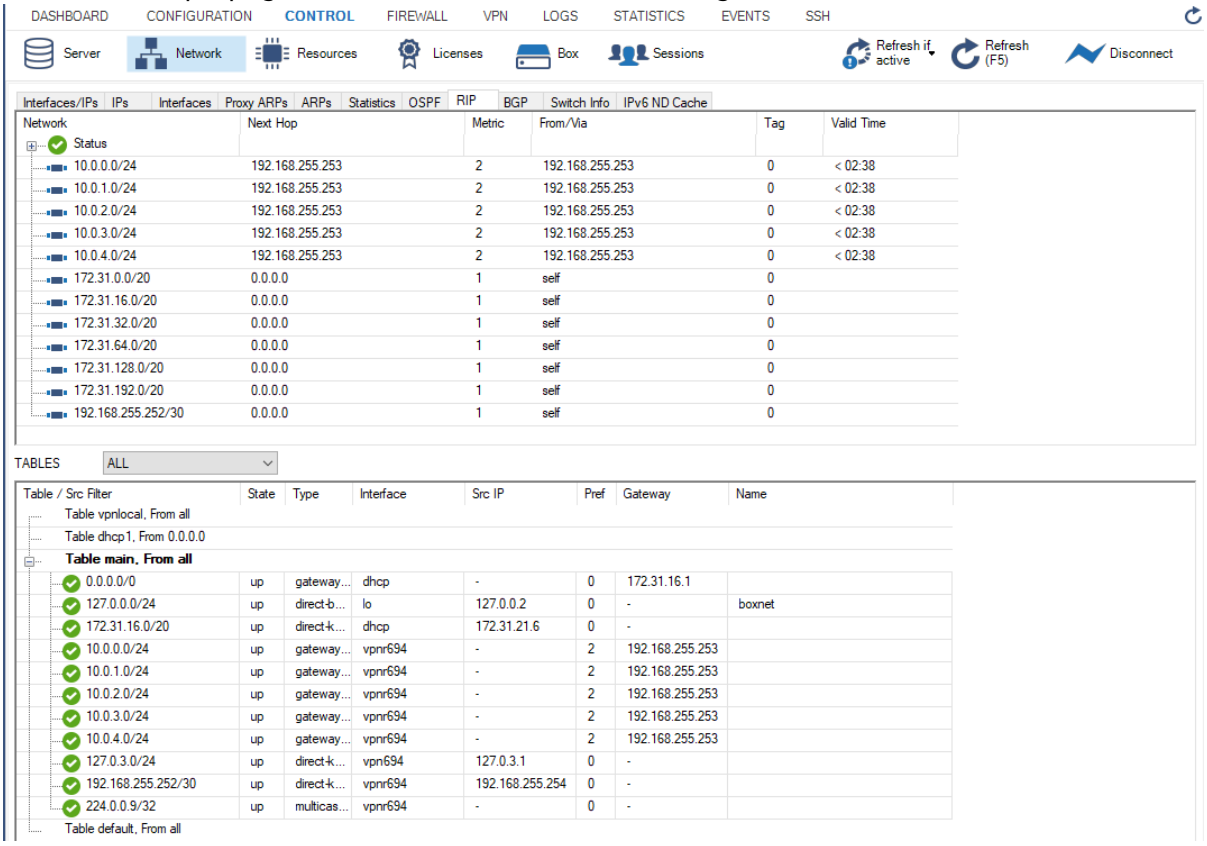
2. Also, you can see the service node created for dynamic routing:



3. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN > Site to Site**. You will see that the VPN tunnel is up and running:

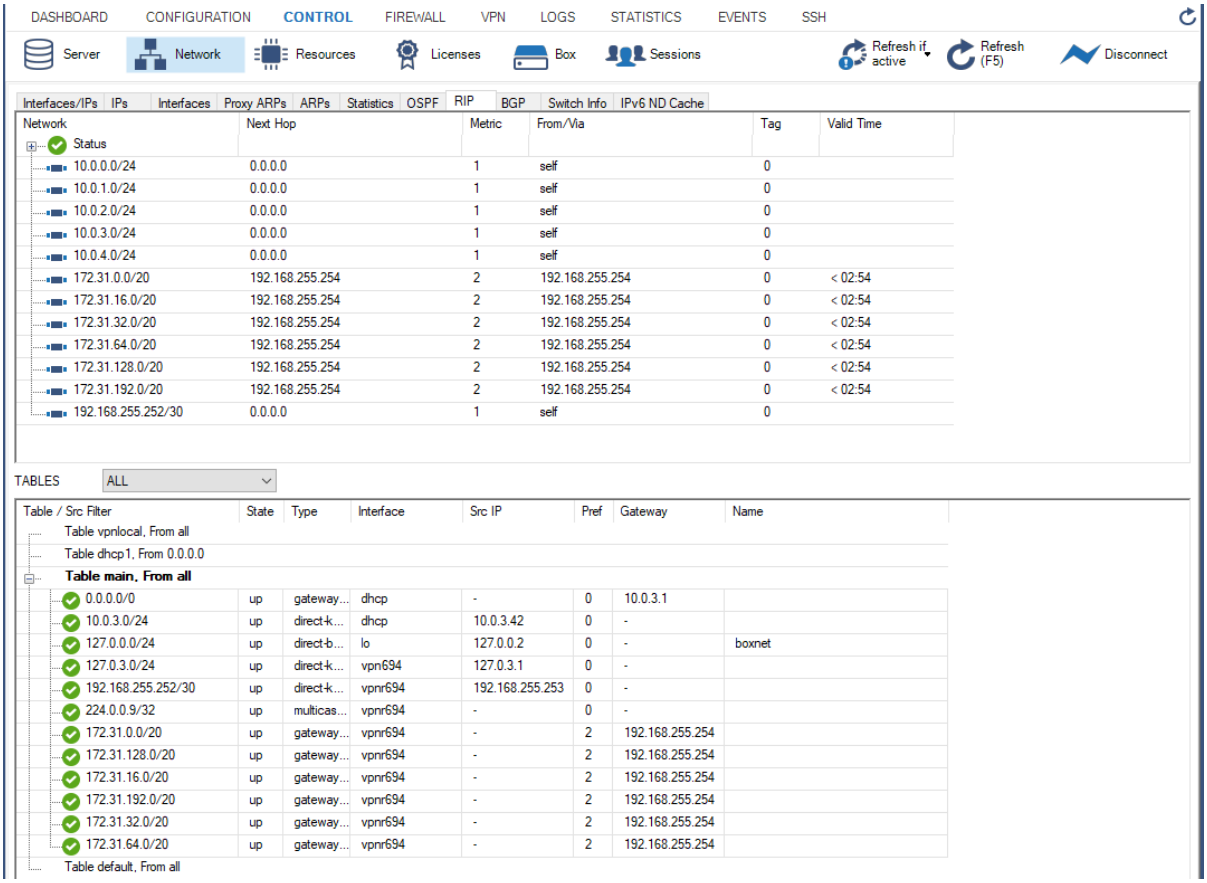


4. Go to **CONFIGURATION > Configuration Tree > Box > Network** to verify that local cloud networks are propagated via the AutoVPN tunnel using RIP:



Step 7. (optional) Verify that the AutoVPN TINA Tunnel is Set Up Correctly on the Second Firewall

To verify the state of the AutoVPN TINA tunnel, log into the second firewall and repeat the steps from Step 6 above. For the services, the output will be the same. However, the entries for the network will be different on the second firewall.



To route traffic through the AutoVPN tunnel, make sure that you enable the **Advertise Route** setting for the network routes that should be propagated by the BGP router. See How to Configure Direct Attached Routes, How to Configure Gateway Routes and How to Configure an ISP with Dynamic IP Addresses (DHCP).

Further Information

- For information about the AutoVPN feature, see AutoVPN.
- To use AutoVPN on CLI see, How to Create an AutoVPN Tunnel via the Command Line Interface.
- For a list of all available REST API functions, see Developer Documentation for the CloudGen Firewall REST API.
- For information about BGP and routing, see Dynamic Routing Protocols (OSPF/RIP/BGP).

Figures