How to Create an AutoVPN Tunnel via the Command Line Interface on CloudGen Firewall Devices 8.0

https://campus.barracuda.com/doc/79463507/

This article describes the AutoVPN function of CloudGen Firewall firmware version 8.0. only. For the documentation of AutoVPN in 8.0.1 or higher, see AutoVPN for CloudGen Firewall Devices 8.0.1 or Higher.

AutoVPN is a feature that is available only for CloudGen Firewalls in the cloud. The feature creates a session that automatically configures a TINA VPN tunnel between two CloudGen Firewalls and handles the traffic through it. Configuration must be initiated in two steps by an administrator on the command line. The first step is to initiate a server session on the first firewall that listens to incoming VPN connection requests from the second firewall. The second step is to connect from the second firewall to the first one by authenticating with a password that was previously generated on the first firewall.

	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

- You must have root level access on the command line to both CloudGen Firewalls to initiate the configuration of an AutoVPN TINA tunnel.
- AutoVPN uses port 694. Ensure that this port is not used for any other purpose. For more information, see Best Practice - Core System Configuration Files and Ports Overview.
- You must preserve a 2-bit network (e.g., 192.168.255.252/30) within a private network common for both firewalls, e.g., 192.168.224.0/19.

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. Log into the first firewall (e.g., 34.241.43.25) as user root.
2. On the command line, enter the following command to create a listener: `autovpn -l 52.213.101.0/24`.
3. AutoVPN will display an output to inform you that the listener is up and running: `Created new server session <sessionID>: peer(s) 52.213.101.0/24, valid for 24 hours`.
4. AutoVPN will also display a password generated for authentication of the second firewall: `Please use this password on the other side of AutoVPN connection: <password>`.
5. Double-click the password to copy the password to the clipboard.

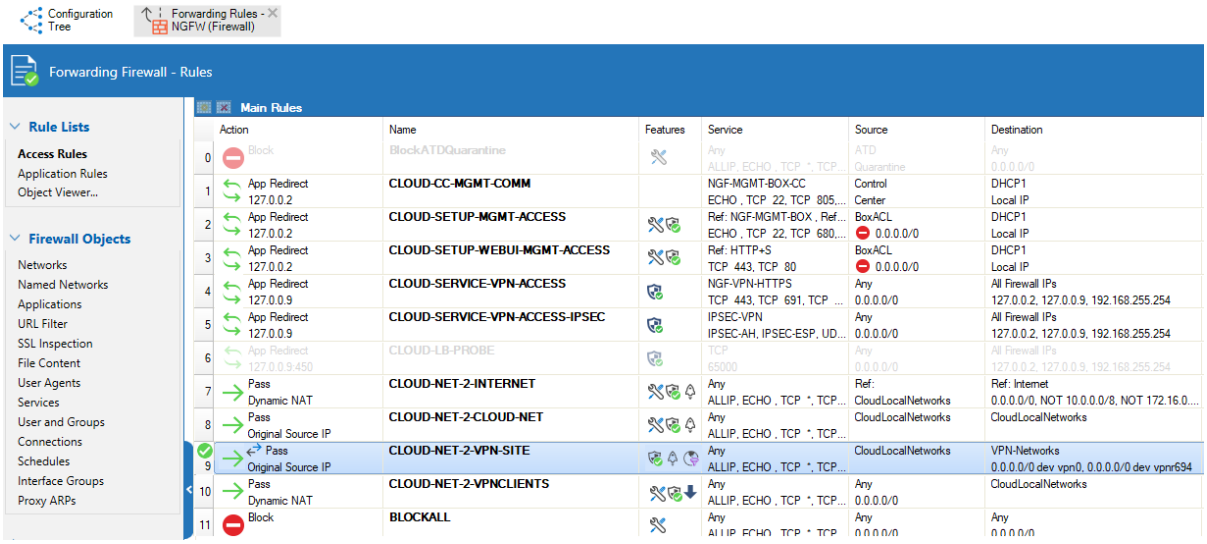
Step 2. Create a Session on the Second Firewall to Connect to the First Firewall Waiting for Connection Requests

1. Log into the second firewall (e.g., 52.213.101.46) as user root.
2. On the command line, enter the following command to connect to the listener on the first firewall:
   `autovpn -c 34.241.43.25 -p <password>`.
   To enter the password, right-click with your mouse at the cursor position.
3. AutoVPN will display an output to inform you that the connection has been established successfully:
   `Created new client session <sessionID>: peer(s) 34.241.43.25, valid for 24 hours`.

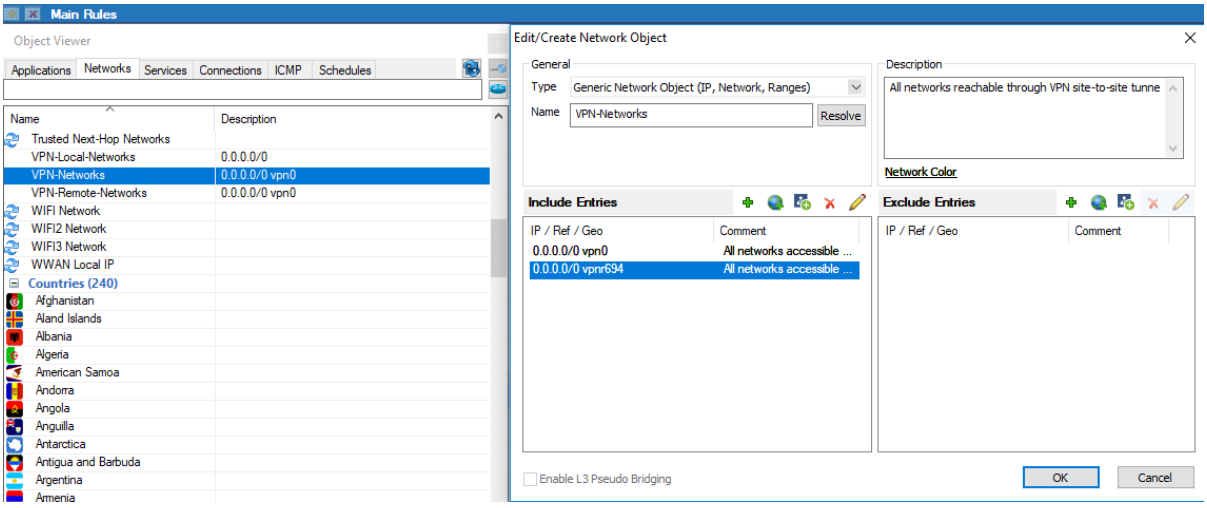
Step 3. Activate Routing Between Local Cloud Networks

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

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** in the list.



5. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
6. In the left menu, click **Networks**.
7. In the list, double-click the network object **VPN-Networks** for modifying.
8. Click **+** to add `IP 0.0.0.0/0` with interface `vpnr694` to the network object **VPN-Networks**.
9. Click **OK**.
10. Click **Send Changes.**
11. **Click Activate**.

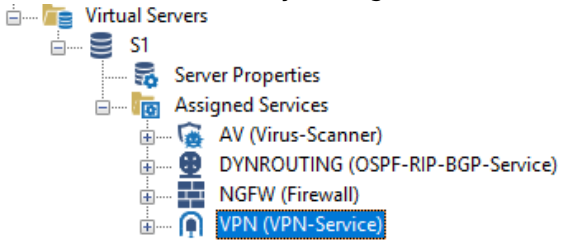


Step 4. Verify that the AutoVPN TINA Tunnel is Set Up Correctly on the First Firewall

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.

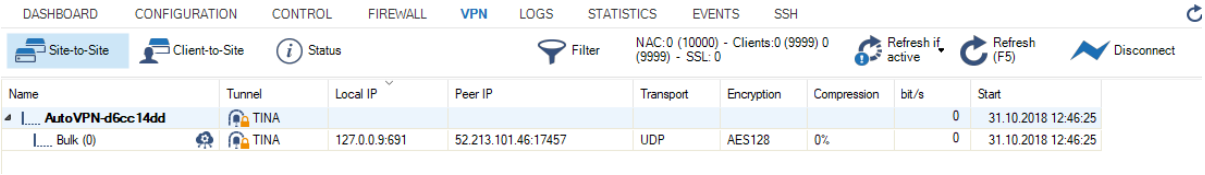
1. On your first firewall, go to **CONFIGURATION > Configuration Tree > Box > Assigned Services**. Because no VPN service has been set up prior to this configuration, you will now see

the new, automatically configured VPN service:

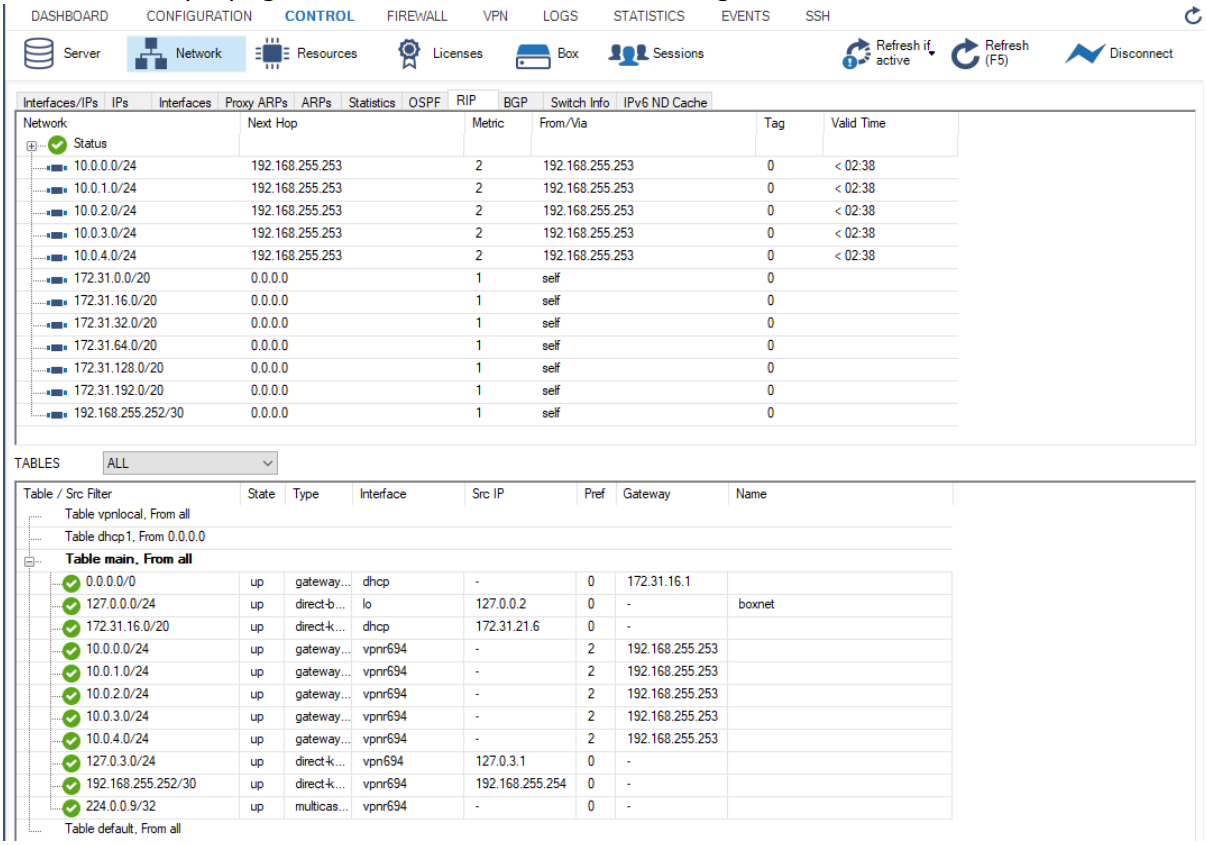


2. Also, you can see the service node created for dynamic routing (RIP):

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

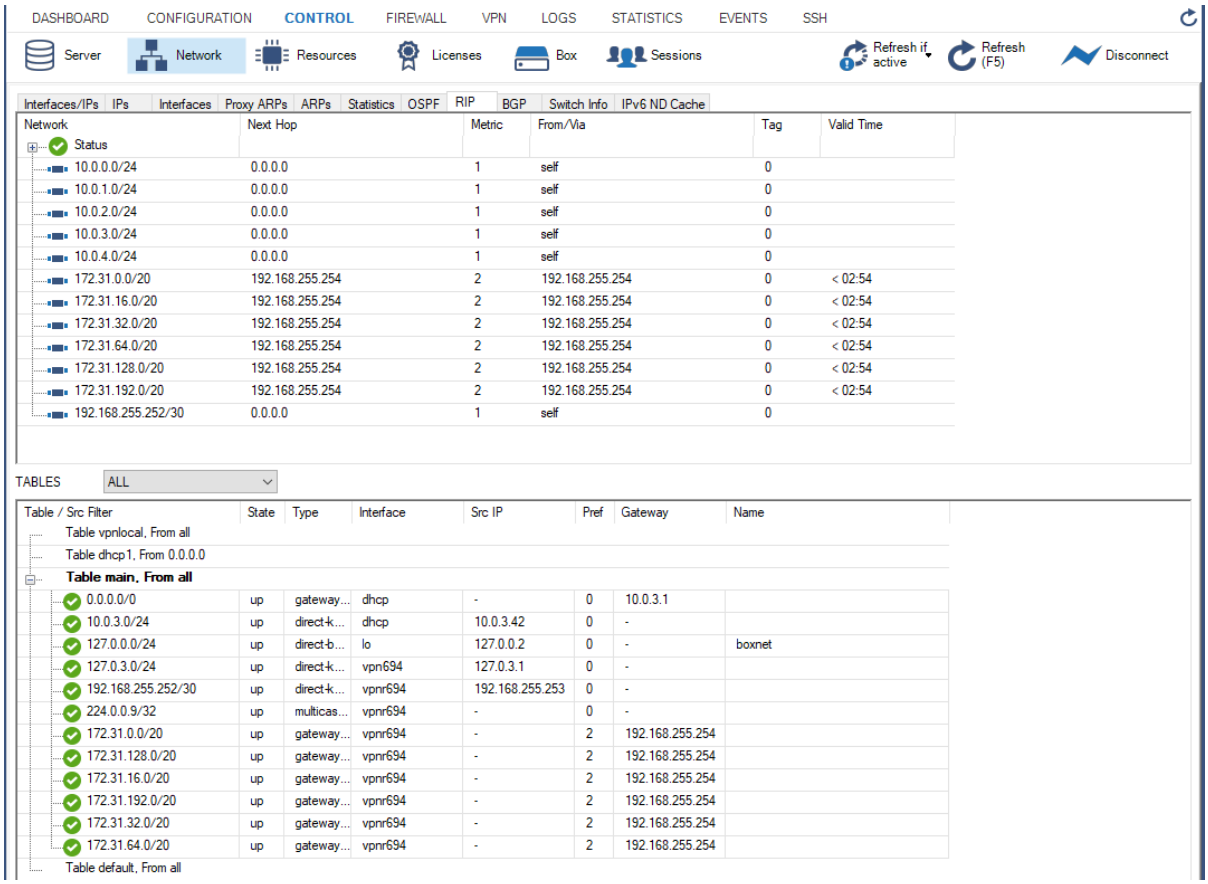


4. Go to **CONFIGURATION > Configuration Tree > Box > Network** to verify that local cloud networks are propagated via the AutoVPN tunnel using RIP:



Step 5. (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 3 above. For the services, the output will be the same. However, the entries for the network will be different on the second firewall:



Figures

1. autovpn_tina_tunnel.png
2. autovpn_acticate_access_rule_fwfw.png
3. autovpn_add_vpnr694.png
4. autovpn_vpn_configured_automatically.png
5. autovpn_rip_configured_automatically.png
6. autovpn_vpn_tunnel_up.png
7. autovpn_rip_on_first_firewall.png
8. autovpn_rip_on_second_firewall.png