

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](#).

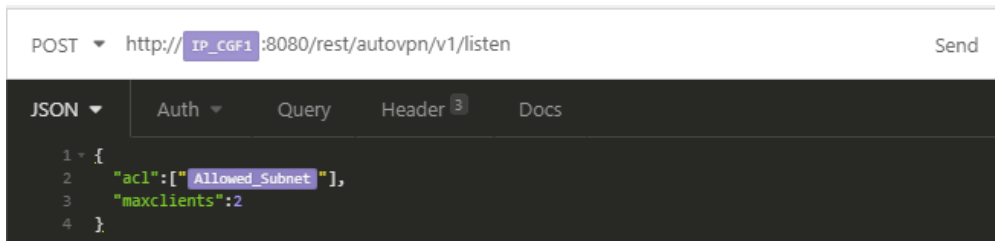
Step 1. Create a Session on the First Firewall Initiating a Listener

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:

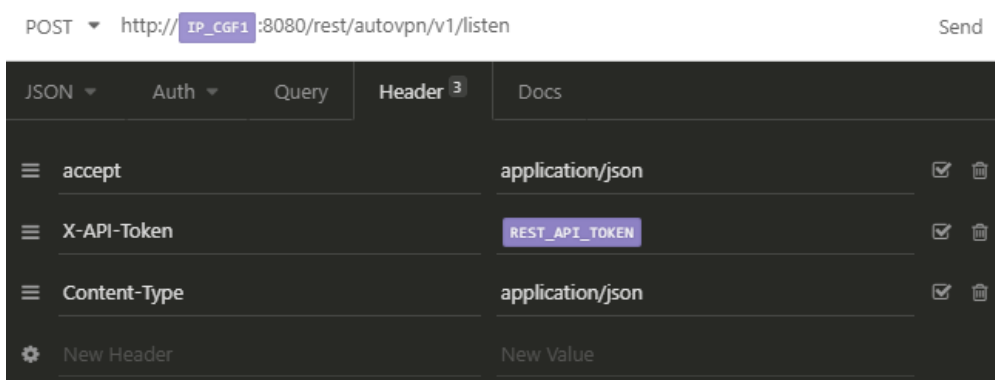
```
{"acl":["52.213.101.0/24"],"maxclients":2}
```

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.



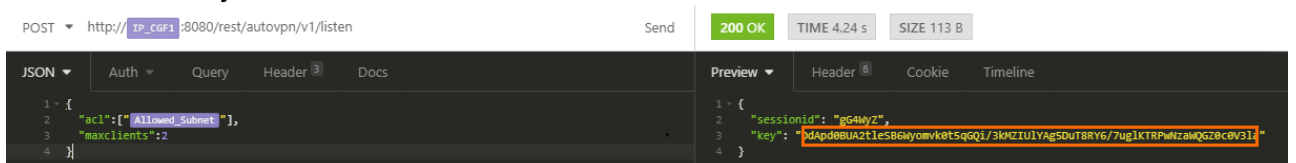
5. In the header section, enter the following header names and the following values:

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**.

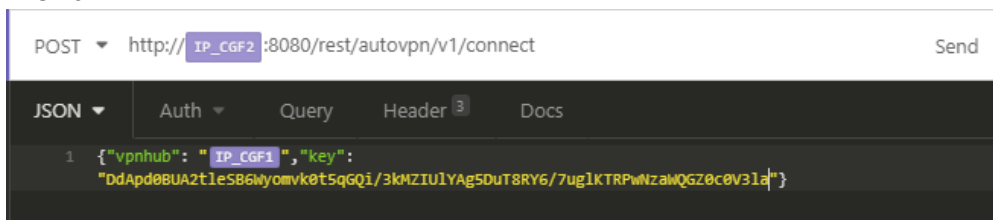
Step 2. Create a Session on the Second Firewall to Connect to the First Firewall Waiting for Connection Requests

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>"}
```

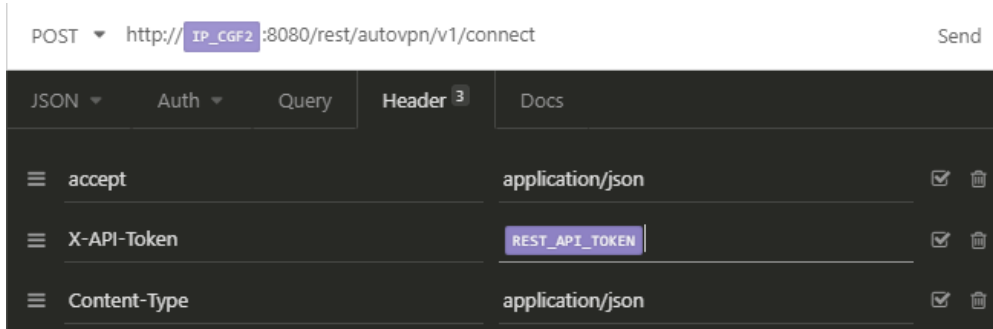
4. **VPNHUB** is the IP address of the first firewall, and the token is the token created by the first firewall.



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.

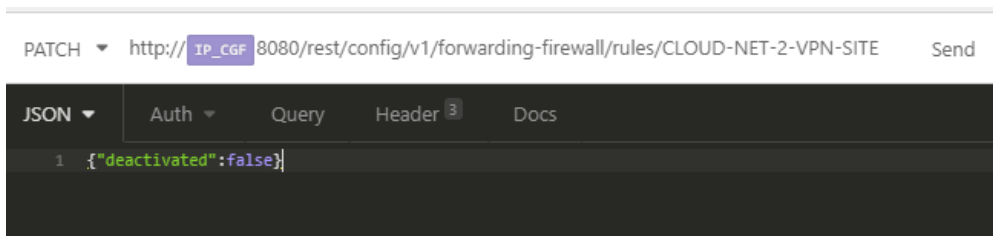
Activate the access rule **CLOUD-NET-2-VPN-SITE**. Repeat the following steps for both firewalls.

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:

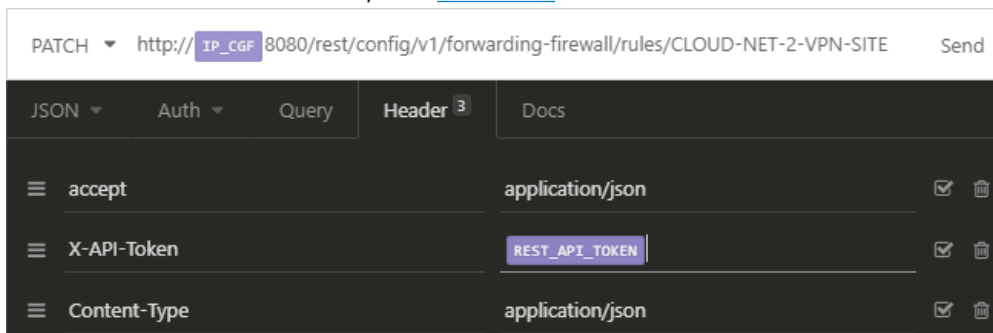
```
{"deactivated":false}
```



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

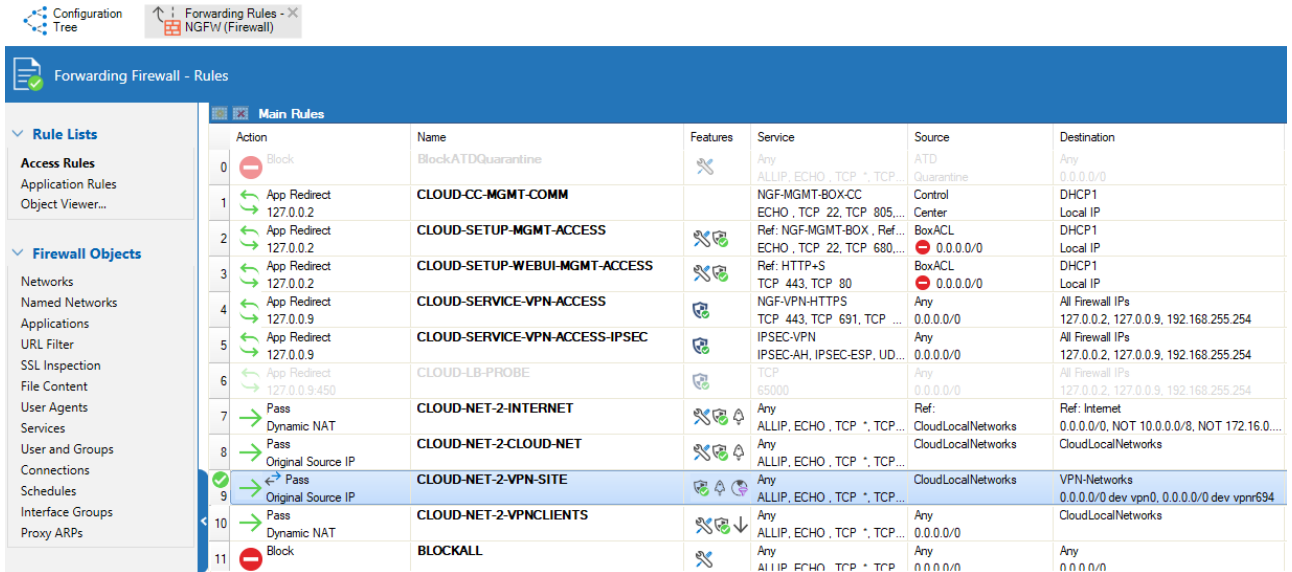
To create a REST API token, see [REST API](#) .



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.



Action	Name	Features	Service	Source	Destination
0 Block	BlockATDQuarantine		Any	ATD Quarantine	Any
1 App Redirect 127.0.0.2	CLOUD-CC-MGMT-COMM		NGF-MGMT-BOX-CC ECHO , TCP 22, TCP 805...	Control Center	DHCP1 Local IP
2 App Redirect 127.0.0.2	CLOUD-SETUP-MGMT-ACCESS		Ref: NGF-MGMT-BOX , Ref... ECHO , TCP 22, TCP 680...	BoxACL 0.0.0.0/0	DHCP1 Local IP
3 App Redirect 127.0.0.2	CLOUD-SETUP-WEBUI-MGMT-ACCESS		Ref: HTTP+S TCP 443, TCP 80	BoxACL 0.0.0.0/0	DHCP1 Local IP
4 App Redirect 127.0.0.9	CLOUD-SERVICE-VPN-ACCESS		NGF-VPN-HTTPS TCP 443, TCP 691, TCP ...	Any	All Firewall IPs 127.0.0.2, 127.0.0.9, 192.168.255.254
5 App Redirect 127.0.0.9	CLOUD-SERVICE-VPN-ACCESS-IPSEC		IPSEC-VPN IPSEC-AH, IPSEC-ESP, UD...	Any	All Firewall IPs 127.0.0.2, 127.0.0.9, 192.168.255.254
6 App Redirect 127.0.0.9:450	CLOUD-LB-PROBE		TCP 65000	Any	All Firewall IPs 127.0.0.2, 127.0.0.9, 192.168.255.254
7 Pass Dynamic NAT	CLOUD-NET-2-INTERNET		Any	Ref: CloudLocalNetworks	Ref: Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172.16.0...
8 Pass Original Source IP	CLOUD-NET-2-CLOUD-NET		Any	CloudLocalNetworks	CloudLocalNetworks
9 Pass Original Source IP	CLOUD-NET-2-VPN-SITE		Any	CloudLocalNetworks	VPN-Networks 0.0.0.0/0 dev vpn0, 0.0.0.0/0 dev vpn694
10 Pass Dynamic NAT	CLOUD-NET-2-VPNCLIENTS		Any	0.0.0.0/0	CloudLocalNetworks
11 Block	BLOCKALL		Any	0.0.0.0/0	Any 0.0.0.0/0

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}
```

```
PATCH http://IP_CGF 8080/rest/config/v1/forwarding-firewall/rules/BOX-LAN-2-VPN-SITE Send
JSON Auth Query Header 3 Docs
1 {"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

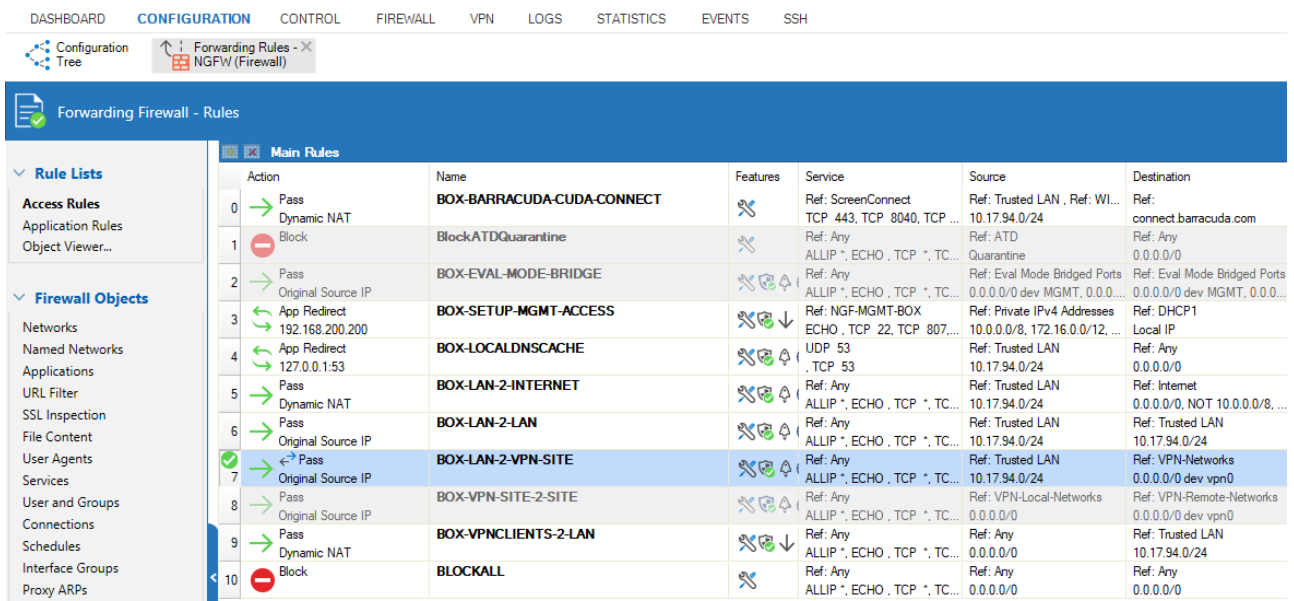
To create a REST API token, see [REST API](#).

```
PATCH http://IP_CGF 8080/rest/config/v1/forwarding-firewall/rules/BOX-LAN-2-VPN-SITE Send
JSON Auth Query Header 3 Docs
accept application/json
X-API-Token REST_API_TOKEN
Content-Type application/json
```

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.



The screenshot shows the Firewall Admin interface with the 'Forwarding Firewall - Rules' page open. The 'Main Rules' table is visible, listing various rules. The rule 'BOX-LAN-2-VPN-SITE' is highlighted in blue, indicating it is selected. The table columns include Action, Name, Features, Service, Source, and Destination.

Action	Name	Features	Service	Source	Destination
0 → Pass	BOX-BARRACUDA-CUDA-CONNECT		Ref: ScreenConnect TCP 443, TCP 8040, TCP ...	Ref: Trusted LAN , Ref: WI... 10.17.94.0/24	Ref: connect.barracuda.com
1 - Block	Block.ATDQuarantine		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: ATD Quarantine	Ref: Any 0.0.0.0/0
2 → Pass	BOX-EVAL-MODE-BRIDGE		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: Eval Mode Bridged Ports 0.0.0.0/0 dev MGMT, 0.0.0...	Ref: Eval Mode Bridged Ports 0.0.0.0/0 dev MGMT, 0.0.0...
3 → App Redirect	BOX-SETUP-MGMT-ACCESS		Ref: NGF-MGMT-BOX ECHO , TCP 22, TCP 807...	Ref: Private IPv4 Addresses 10.0.0.0/8, 172.16.0.0/12, ...	Ref: DHCP1 Local IP
4 → App Redirect	BOX-LOCALDNSCACHE		UDP 53 , TCP 53	Ref: Trusted LAN 10.17.94.0/24	Ref: Any 0.0.0.0/0
5 → Pass	BOX-LAN-2-INTERNET		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: Trusted LAN	Ref: Internet 0.0.0.0/0, NOT 10.0.0.0/8, ...
6 → Pass	BOX-LAN-2-LAN		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: Trusted LAN	Ref: Trusted LAN 10.17.94.0/24
7 → Pass	BOX-LAN-2-VPN-SITE		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: Trusted LAN 10.17.94.0/24	Ref: VPN-Networks 0.0.0.0/0 dev vpn0
8 → Pass	BOX-VPN-SITE-2-SITE		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: VPN-Local-Networks 0.0.0.0/0	Ref: VPN-Remote-Networks 0.0.0.0/0 dev vpn0
9 → Pass	BOX-VPNCLIENTS-2-LAN		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: Any 0.0.0.0/0	Ref: Trusted LAN 10.17.94.0/24
10 - Block	BLOCKALL		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: Any 0.0.0.0/0	Ref: Any 0.0.0.0/0

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

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

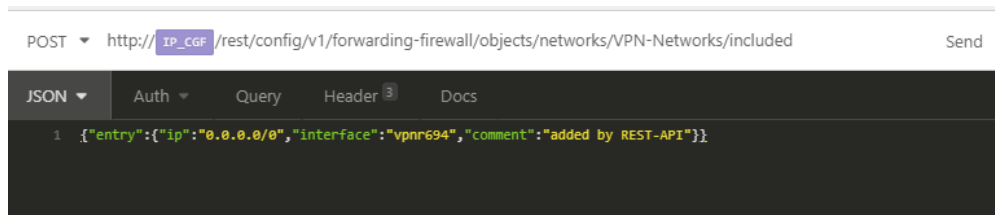
This can be done using either Firewall Admin or REST API.

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:

```

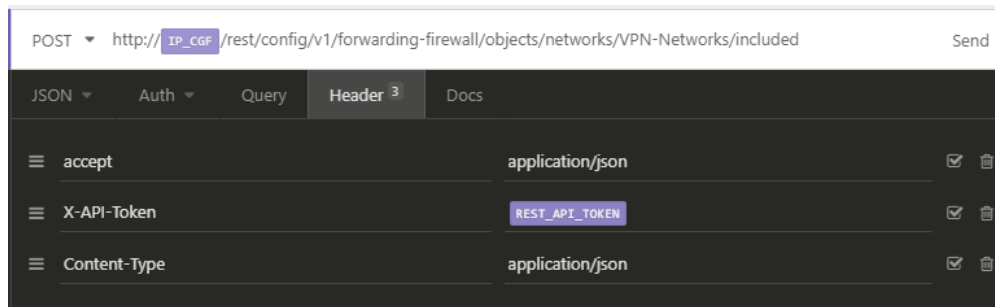
{"entry":{"ip":"0.0.0.0/0","interface":"vpn694","comment":"added by REST-API"}}
    
```



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](#).

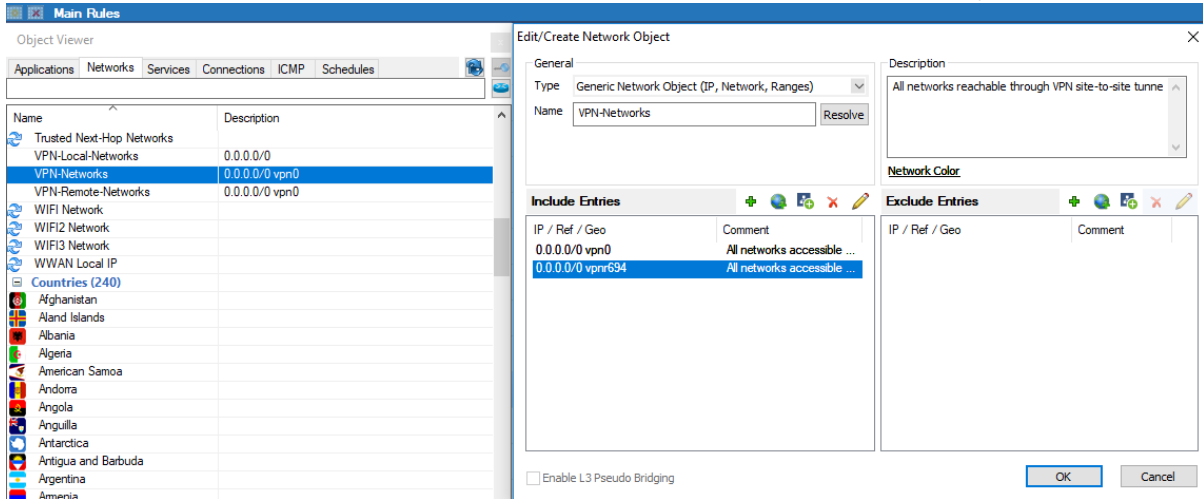


5. Click **Send**.

Configuration in Firewall Admin

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

- In the list, double-click the network object **VPN-Networks** for modifying.
- Click **+** to add IP `0.0.0.0/0` with interface `vpn694` to the network object **VPN-Networks**.

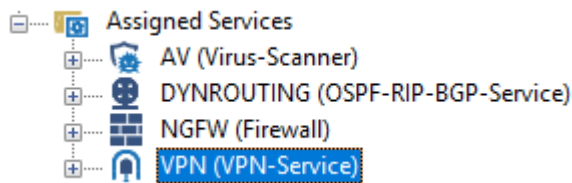


- Click **OK**.
- Click **Send Changes** and **Activate**.

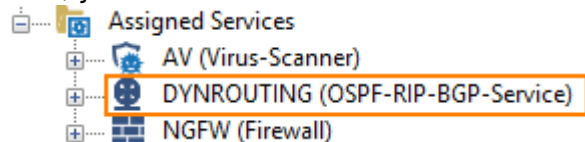
Step 6. (optional) Verify that the AutoVPN TINA Tunnel is Set Up Correctly on the First Firewall

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.

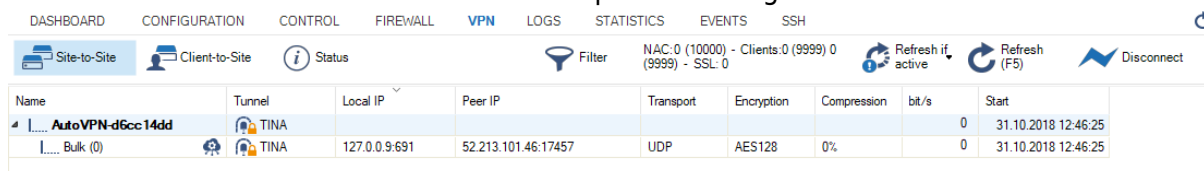
- On your first firewall, go to **CONFIGURATION > Configuration Tree > Box > Assigned Services**. Because no VPN service has been set up prior to this configuration, you will now see the new, automatically configured VPN service:



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



- 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:

Network	Next Hop	Metric	From/Via	Tag	Valid Time
10.0.0.0/24	192.168.255.253	2	192.168.255.253	0	< 02:38
10.0.1.0/24	192.168.255.253	2	192.168.255.253	0	< 02:38
10.0.2.0/24	192.168.255.253	2	192.168.255.253	0	< 02:38
10.0.3.0/24	192.168.255.253	2	192.168.255.253	0	< 02:38
10.0.4.0/24	192.168.255.253	2	192.168.255.253	0	< 02:38
172.31.0.0/20	0.0.0.0	1	self	0	
172.31.16.0/20	0.0.0.0	1	self	0	
172.31.32.0/20	0.0.0.0	1	self	0	
172.31.64.0/20	0.0.0.0	1	self	0	
172.31.128.0/20	0.0.0.0	1	self	0	
172.31.192.0/20	0.0.0.0	1	self	0	
192.168.255.252/30	0.0.0.0	1	self	0	

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table vprnlocal, From all							
Table dhcp1, From 0.0.0.0							
Table main, From all							
0.0.0.0/0	up	gateway...	dhcp	-	0	172.31.16.1	
127.0.0.0/24	up	direct-b...	lo	127.0.0.2	0	-	boxnet
172.31.16.0/20	up	direct-k...	dhcp	172.31.21.6	0	-	
10.0.0.0/24	up	gateway...	vpn694	-	2	192.168.255.253	
10.0.1.0/24	up	gateway...	vpn694	-	2	192.168.255.253	
10.0.2.0/24	up	gateway...	vpn694	-	2	192.168.255.253	
10.0.3.0/24	up	gateway...	vpn694	-	2	192.168.255.253	
10.0.4.0/24	up	gateway...	vpn694	-	2	192.168.255.253	
127.0.3.0/24	up	direct-k...	vpn694	127.0.3.1	0	-	
192.168.255.252/30	up	direct-k...	vpn694	192.168.255.254	0	-	
224.0.0.9/32	up	multicas...	vpn694	-	0	-	
Table default, From all							

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.

DASHBOARD CONFIGURATION **CONTROL** FIREWALL VPN LOGS STATISTICS EVENTS SSH

Server Network Resources Licenses Box Sessions Refresh if active Refresh (F5) Disconnect

Interfaces/IPs IPs Interfaces Proxy ARPs ARPs Statistics OSPF RIP **BGP** Switch Info IPv6 ND Cache

Network	Status	Next Hop	Metric	From/Via	Tag	Valid Time
10.0.0.0/24	✓	0.0.0.0	1	self	0	
10.0.1.0/24	✓	0.0.0.0	1	self	0	
10.0.2.0/24	✓	0.0.0.0	1	self	0	
10.0.3.0/24	✓	0.0.0.0	1	self	0	
10.0.4.0/24	✓	0.0.0.0	1	self	0	
172.31.0.0/20	✓	192.168.255.254	2	192.168.255.254	0	< 02:54
172.31.16.0/20	✓	192.168.255.254	2	192.168.255.254	0	< 02:54
172.31.32.0/20	✓	192.168.255.254	2	192.168.255.254	0	< 02:54
172.31.64.0/20	✓	192.168.255.254	2	192.168.255.254	0	< 02:54
172.31.128.0/20	✓	192.168.255.254	2	192.168.255.254	0	< 02:54
172.31.192.0/20	✓	192.168.255.254	2	192.168.255.254	0	< 02:54
192.168.255.252/30	✓	0.0.0.0	1	self	0	

TABLES ALL

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table vpnlocal, From all							
Table dhcp 1, From 0.0.0.0							
Table main, From all							
0.0.0.0/0	✓	up	gateway...	dhcp	-	0	10.0.3.1
10.0.3.0/24	✓	up	direct-k...	dhcp	10.0.3.42	0	-
127.0.0.0/24	✓	up	direct-b...	lo	127.0.0.2	0	-
127.0.3.0/24	✓	up	direct-k...	vpn694	127.0.3.1	0	-
192.168.255.252/30	✓	up	direct-k...	vpn694	192.168.255.253	0	-
224.0.0.9/32	✓	up	multicas...	vpn694	-	0	-
172.31.0.0/20	✓	up	gateway...	vpn694	-	2	192.168.255.254
172.31.128.0/20	✓	up	gateway...	vpn694	-	2	192.168.255.254
172.31.16.0/20	✓	up	gateway...	vpn694	-	2	192.168.255.254
172.31.192.0/20	✓	up	gateway...	vpn694	-	2	192.168.255.254
172.31.32.0/20	✓	up	gateway...	vpn694	-	2	192.168.255.254
172.31.64.0/20	✓	up	gateway...	vpn694	-	2	192.168.255.254
Table default, From all							

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

1. autovpn_tina_tunnel.png
2. rest_listen_body.png
3. rest_listen_header.png
4. rest_listen_result.png
5. rest_connect.png
6. rest_connect_header.png
7. rest_connect_result.png
8. rest_activate_rule_cloud.png
9. rest_header_activate_rule_cloud.png
10. autovpn_activate_access_rule_fwfw.png
11. rest_activate_rule_box.png
12. rest_header_activate_rule_box.png
13. rule_box2vpn.png
14. post_network_vpnr.png
15. vpnr_header.png
16. autovpn_add_vpnr694.png
17. autovpn_vpn_configured_automatically_vpn_service.png
18. autovpn_routing_configured_automatically.png
19. autovpn_vpn_tunnel_up.png
20. autovpn_rip_on_first_firewall.png
21. autovpn_rip_on_second_firewall.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.