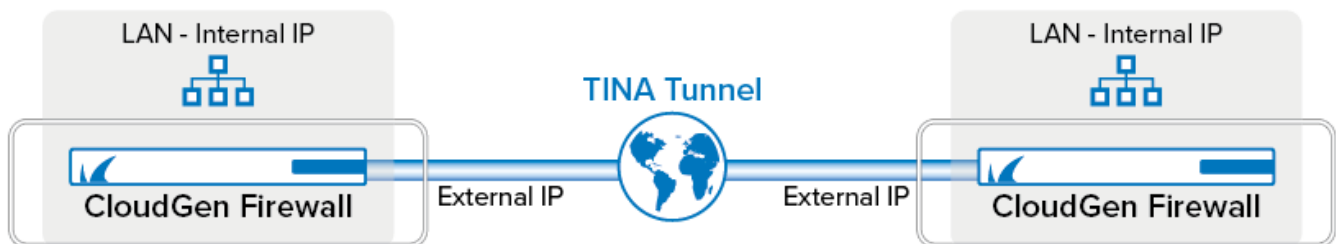


How to Create an AutoVPN Tunnel via the Command Line Interface

<https://campus.barracuda.com/doc/87785508/>

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 via REST API, see [How to Create an AutoVPN Tunnel via REST API](#).



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

- You must have root level access on the command line to both CloudGen Firewalls in order to initiate the configuration of an AutoVPN TINA tunnel.
- 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. 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 listen <allowed_subnet>` e.g. `autovpn listen 52.213.101.0/24`.
3. AutoVPN will display an output to inform you that the listener is up and running. It also displays a token generated for authentication of the second firewall and the session ID:

```
[2019-07-22 14:08 UTC] [-root shell-] [-Barracuda Networks-]
[root@CA-801-284-autovpn1:~]# autovpn listen 52.213.101.0/24
Successfully initiated a new listener session KiYTy6
Please use the following token for AutoVPN connections to this firewall:
C20jDhLgA2tleSC0hoHsmtf9jERiu48rRmR/P5bLHDDgNsrrA5n+QsbEiwNzaWQGS2lZVHk2
[2019-07-22 14:08 UTC] [-root shell-] [-Barracuda Networks-]
[root@CA-801-284-autovpn1:~]#
```

4. 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

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

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 connect 34.241.43.25 <token>`.
To enter the token, 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:

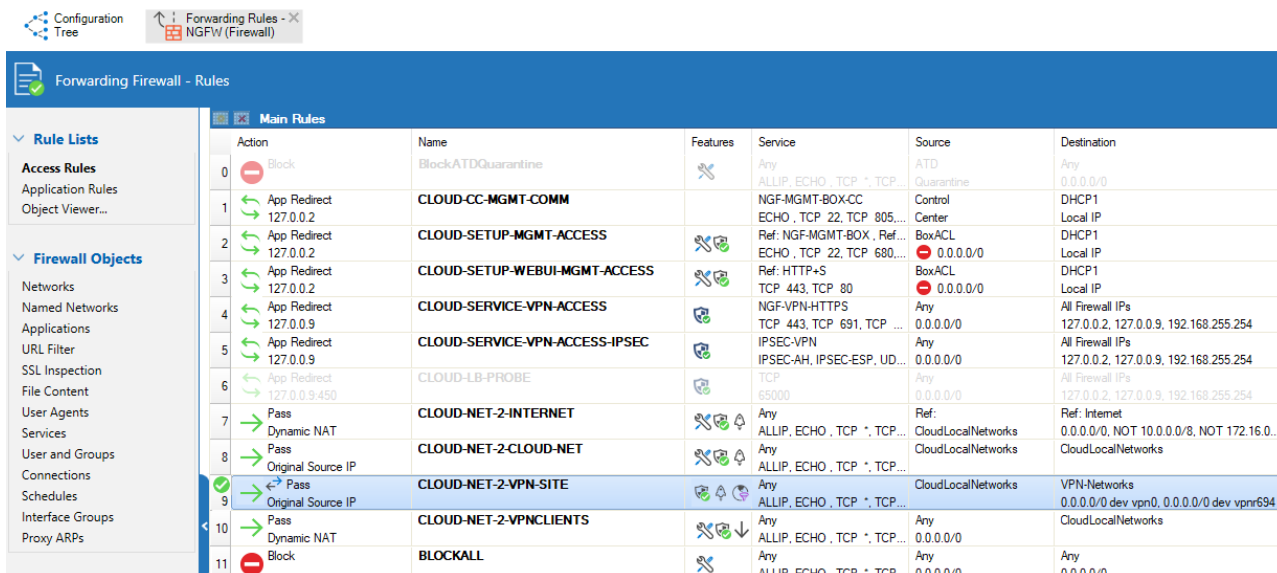
```
[root@Clemens-autovpn2:~]# autovpn connect 34.241.43.25 C20jDhLgA2tleSC0hoHsmtf9jERiu48rRmR/P5bLHDDgNsrrA5n+QsbEiwNzaWQGS2lZVHk2
connecting to 34.241.43.25
preparing configuration update for session keqq2N
negotiating tunnel parameters
creating VPN tunnel AutoVPN-keqq2N-1
configuring VPN next hop interface; routing IP is 192.168.255.2
setting up dynamic routing with BGP; ASN is 65530
applying configuration changes
successfully finished configuration update for session keqq2N
```

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:

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
Block	BlockATDQuarantine		Any	ATD Quarantine	Any 0.0.0.0/0
App Redirect 127.0.0.2	CLOUD-CC-MGMT-COMM		NGF-MGMT-BOX-CC ECHO , TCP 22, TCP 805...	Control Center	DHCP1 Local IP
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
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
App Redirect 127.0.0.9	CLOUD-SERVICE-VPN-ACCESS		NGF-VPN-HTTPS TCP 443, TCP 691, TCP ...	Any 0.0.0.0/0	All Firewall IPs 127.0.0.2, 127.0.0.9, 192.168.255.254
App Redirect 127.0.0.9	CLOUD-SERVICE-VPN-ACCESS-IPSEC		IPSEC-VPN IPSEC-AH, IPSEC-ESP, UD...	Any 0.0.0.0/0	All Firewall IPs 127.0.0.2, 127.0.0.9, 192.168.255.254
App Redirect 127.0.0.9:450	CLOUD-LB-PROBE		TCP 65000	Any 0.0.0.0/0	All Firewall IPs 127.0.0.2, 127.0.0.9, 192.168.255.254
Pass Dynamic NAT	CLOUD-NET-2-INTERNET		Any ALLIP, ECHO , TCP * , TCP...	Ref: CloudLocalNetworks	Ref: Internet 0.0.0.0/0, NOT 10.0.0.0/8, NOT 172.16.0...
Pass Original Source IP	CLOUD-NET-2-CLOUD-NET		Any ALLIP, ECHO , TCP * , TCP...	CloudLocalNetworks	CloudLocalNetworks
Pass Original Source IP	CLOUD-NET-2-VPN-SITE		Any ALLIP, ECHO , TCP * , TCP...	CloudLocalNetworks	VPN-Networks 0.0.0.0/0 dev vpn0, 0.0.0.0/0 dev vpn694
Pass Dynamic NAT	CLOUD-NET-2-VPNCLIENTS		Any ALLIP, ECHO , TCP * , TCP...	Any 0.0.0.0/0	CloudLocalNetworks
Block	BLOCKALL		Any ALLIP, ECHO , TCP * , TCP...	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:

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.

DASHBOARD CONFIGURATION CONTROL FIREWALL VPN LOGS STATISTICS EVENTS SSH

Configuration Tree ↑ Forwarding Rules - X NGFW (Firewall)

Forwarding Firewall - Rules

Action	Name	Features	Service	Source	Destination
0 → Pass Dynamic NAT	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	BlockATDQuarantine		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: ATD Quarantine	Ref: Any 0.0.0.0/0
2 → Pass Original Source IP	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 192.168.200.200	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 127.0.0.1:53	BOX-LOCALDNSCACHE		UDP 53 TCP 53	Ref: Trusted LAN 10.17.94.0/24	Ref: Any 0.0.0.0/0
5 → Pass Dynamic NAT	BOX-LAN-2-INTERNET		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: Trusted LAN 10.17.94.0/24	Ref: Internet 0.0.0.0/0, NOT 10.0.0.0/8, ...
6 → Pass Original Source IP	BOX-LAN-2-LAN		Ref: Any ALLIP *, ECHO , TCP *, TC...	Ref: Trusted LAN 10.17.94.0/24	Ref: Trusted LAN 10.17.94.0/24
7 → Pass Original Source IP	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 Original Source IP	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 Dynamic NAT	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

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **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 **vpn694** to the network object **VPN-Networks**.

Object Viewer

Applications Networks Services Connections ICMP Schedules

Name	Description
Trusted Next-Hop Networks	
VPN-Local-Networks	0.0.0.0/0
VPN-Networks	0.0.0.0/0 vpn0
VPN-Remote-Networks	0.0.0.0/0 vpn0
WiFi Network	
WiFi2 Network	
WiFi3 Network	
WWAN Local IP	
Countries (240)	
Afghanistan	
Aland Islands	
Albania	
Algeria	
American Samoa	
Andorra	
Angola	
Anguilla	
Antarctica	
Antigua and Barbuda	
Argentina	
Armenia	

Edit/Create Network Object

General

Type: Generic Network Object (IP, Network, Ranges)

Name: VPN-Networks

Description: All networks reachable through VPN site-to-site tunne

Network Color

Include Entries

IP / Ref / Geo	Comment
0.0.0.0/0 vpn0	All networks accessible ...
0.0.0.0/0 vpn694	All networks accessible ...

Exclude Entries

IP / Ref / Geo	Comment
----------------	---------

Enable L3 Pseudo Bridging

OK Cancel

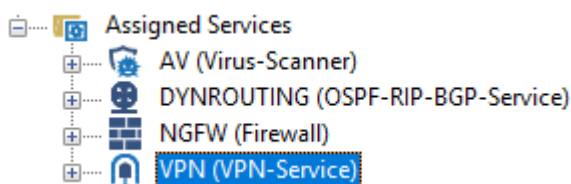
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

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

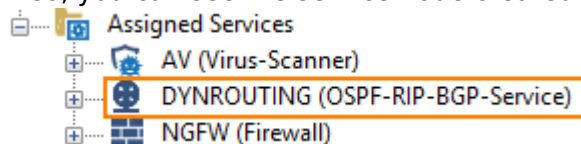
Firewall

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.

Name	Tunnel	Local IP	Peer IP	Transport	Encryption	Compression	bit/s	Start
AutoVPN-d6cc14dd	TINA	127.0.0.9:691	52.213.101.46:17457	UDP	AES128	0%	0	31.10.2018 12:46:25
Bulk (0)	TINA						0	31.10.2018 12:46:25

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

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	✓	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	

TABLES ALL

Table / Src Filter	State	Type	Interface	Src IP	Pref	Gateway	Name
Table vpnlocal, 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	boxnet
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 via REST API see, [How to Create an AutoVPN Tunnel via REST API](#).
- For information about BGP and routing, see [Dynamic Routing Protocols \(OSPF/RIP/BGP\)](#).

Figures

1. autovpn_tina.png
2. listen.png
3. connect.png
4. autovpn_activate_access_rule_fwfw.png
5. rule_box2vpn.png
6. autovpn_add_vpnr694.png
7. autovpn_vpn_configured_automatically_vpn_service.png
8. autovpn_routing_configured_automatically.png
9. autovpn_vpn_tunnel_up.png
10. autovpn_rip_on_first_firewall.png
11. 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.