

AutoVPN

<https://campus.barracuda.com/doc/87197072/>

AutoVPN creates a session that automatically configures a UDP TINA VPN tunnel between two CloudGen Firewalls and handles the traffic through it. In addition, all necessary services are created if they do not already exist. 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 AutoVPN connection requests from the second firewall. The second step is to connect the second firewall to the first one by authentication with a token that was previously generated on the first firewall. AutoVPN uses BGP for routing and TLS for securing the connection during parameter negotiation. You can define how many CloudGen Firewall devices can connect to the listener. Per default, 250 connections are allowed. AutoVPN can also be configured using REST API.

- This feature is available only for stand-alone Cloud Gen Firewalls. For CC-managed firewall devices, please use the [GTI Editor](#) .
- This feature is available only on the command line or via REST API if you are using Firewall Admin. For CloudGen Firewall devices managed by the web UI, AutoVPN is not available.

Commands

This section lists all CLI commands. For detailed information on the REST API commands, please see the [Developer Documentation for the CloudGen Firewall REST API](#).

AutoVPN provides four commands, which are described in the table below. Each command has various options. To show all available options, enter the command you are interested in and type `--help` after the command and press Enter. All commands must be entered in the CLI of the desired firewall.

| Command | Syntax | Function |
|-----------------------|---|---|
| autovpn listen | <code>autovpn listen <access_control_list></code> | Starts an AutoVPN hub. Listens to connections from the allowed subnet or subnets if more than one subnet is declared. An access control list is either a single subnet in CIDR format or a comma-separated list of subnets in CIDR format. |

| | | |
|------------------------|--|---|
| autovpn connect | autovpn connect <IP_address_listener> <token> | Connects to a listener. The token is displayed on the AutoVPN hub. Note that IP_address_listener and token are two parameters separated by a blank. |
| autovpn status | autovpn status | Shows the status of established connections or sessions. |
| autovpn remove | autovpn remove --session <session_ID> | Removes all tunnels belonging to the specified session and the listener session itself on the listening device. |
| | autovpn remove --tunnel <tunnel_name> | Removes the specified AutoVPN tunnel on the connecting device. |
| autovpn --help | autovpn --help | Shows the help for the AutoVPN. |

Options are entered in the format: autovpn command --option

For example, type autovpn listen --help to show the help for the listen command.

AutoVPN Hub

- Per default, 250 connections are allowed on the AutoVPN Hub. To limit the number of connections, you must use the **maxclients** option:

```
autovpn listen <allowed_subnet_in_CIDR_format> --maxclients <number_maximum_allowed_clients>
```
- The timeout for the listener session is set to 60 minutes per default. If you want to specify another timeout, use the following command specifying the timeout in minutes. Use 0 to create an unlimited listener session:

```
autovpn listen <allowed_subnet_in_CIDR_format> --timeout <minutes>
```

Further Information

- [How to Create an AutoVPN Tunnel via the Command Line Interface](#)
- [How to Create an AutoVPN Tunnel via REST API](#)
- [REST API](#)
- [Developer Documentation for the CloudGen Firewall REST API](#)

© 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.