CloudGen Access Proxy

https://campus.barracuda.com/doc/93883031/

The CloudGen Access Proxy is a service that brings secure access to your network resources. Unlike VPN, CloudGen Access provides secure access to enterprise resources on a per-user / per-device basis without the drawback of giving a user total access to a complete private network. As part of three main components, the CloudGen Access Proxy is the instance that effectively grants or denies access to the flow of packets between an access app and a special network resource.

Before You Begin

- IMPORTANT: Ensure that the timebase of your firewall is configured correctly!
  For more information, see How to Configure Time Server (NTP) Settings.
- Ensure that you are familiar with the architecture of the CloudGen Access suite of apps and services.
  For more information, see Overview.
- Ensure that CloudGen Access Enterprise Console is up and running and all necessary users and devices are registered.
  For more information, see CloudGen Access Console.
- Ensure that you have already installed the CloudGen Access App on your client device.
- Ensure that you have licensed Energize Updates.
  For more information, see How to License a CloudGen Firewall.
- Ensure that you have a valid Access Key. This key is a URL that is necessary for the CloudGen Access Proxy service to connect to the CloudGen Access Enterprise Console.
  For more information, see Add Proxy.
- You must be familiar with creating an assigned service. For more information, see How to Assign Services.

Ensure that the service IP for the CloudGen Access Proxy is configured as follows:

- **Explicit** for a single Shared IP.
- **First-IP** if you have configured multiple **Shared IPs** in the list of **Shared Networks and IPs**.

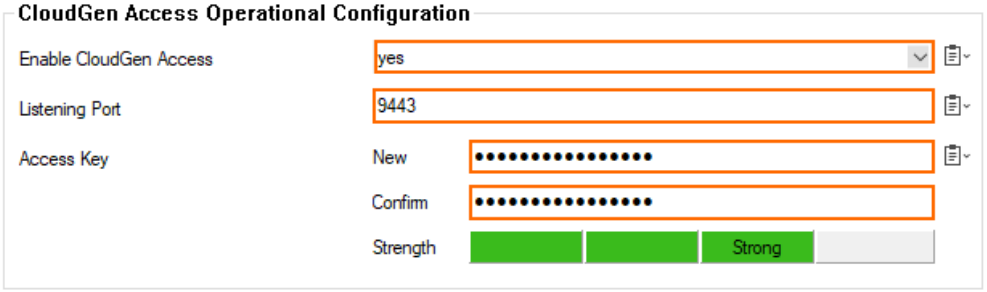
For more information on how to configure Shared Network and IPs, see Understanding the Usage of Operational-Relevant IP Addresses on the CloudGen Firewall, and How to Configure Shared Networks and IPs, and Assigned Services.

Step 1. Configure the CloudGen Access Proxy Service

1. On a stand-alone firewall: Go to **CONFIGURATION > Configuration Tree > Box > Assigned**

Services > CloudGen Access Proxy > CloudGen Access Proxy Configuration.
On a Control Center for a managed firewall: Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > Boxes > *your box* > Assigned Services > CloudGen Access Proxy > CloudGen Access Proxy Configuration**.

2. Click **Lock**.
3. For **Enable CloudGen Access**, select **yes**.
4. For **Listening Port**, enter 9443.
5. For **Access Key**:
   1. For **New**, copy the URL from the CloudGen Enterprise Console in the corresponding edit field.
   2. For **Confirm**, re-enter the access key in the corresponding edit field.



Step 2. Enable an Access Rule to Allow Global Access to the CloudGen Access Proxy Service

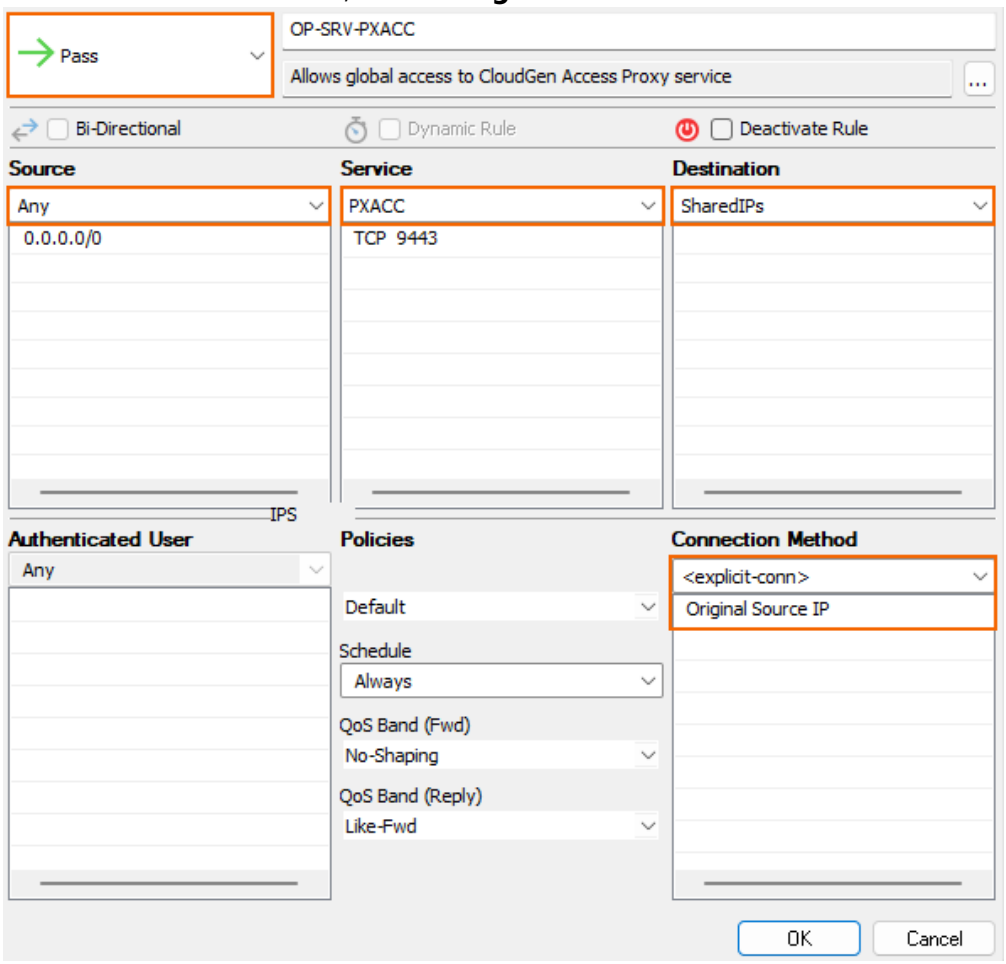
If you have upgraded your firewall to support the CloudGen Access service via a hotfix, you must add an access rule to the host firewall to allow global access to the CloudGen Access Proxy service. This is referred to as Option #1 below.

In case you have not already modified the ruleset on the host firewall, you can also rebuild it with the new access rule included by copying it from the default. This is referred to as Option #2 below.

Option 1: Add an Access Rule to the Host Firewall Ruleset

1. On a stand-alone firewall: Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Host Firewall Rules**.
   On a Control Center: Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > Boxes > *your box* > Infrastructure Services > Host Firewall Rules**.
2. Click **Lock**.
3. Click the green **+** in the upper-right corner at the top of the list.
4. The **Edit Rule:New Rule** window is displayed.
5. For the rule type, select **Pass**.
6. For the name of the rule, enter `OP-SRV-PXACC`.
7. Enter a description, e.g.: `Allows global access to CloudGen Access Proxy service`.

8. For **Source**, select **Any**.
9. For **Service**, select **PXACC** from the list.
10. For Destination, select **SharedIPs**.
11. For **Connection Method**, select **Original Source IP**.



12. Click **OK**.
13. Click **Send Changes** and **Activate**.

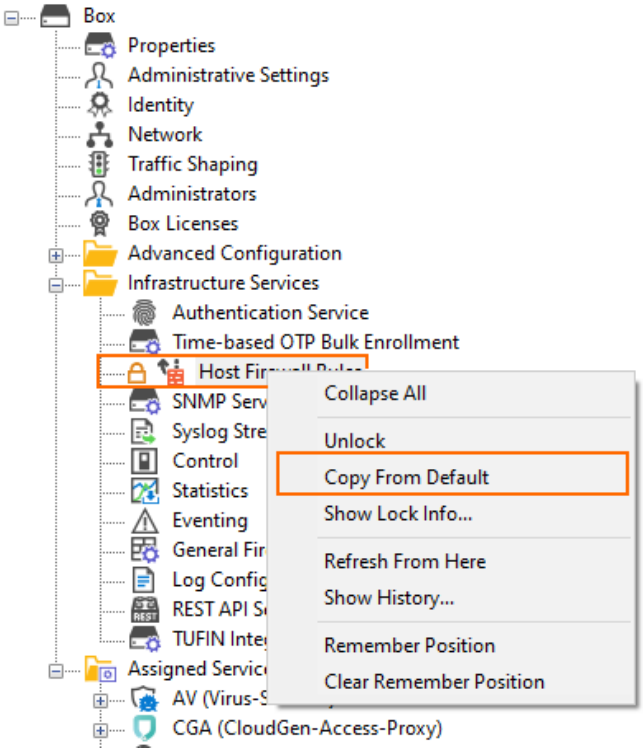
Option 2: Rebuild the Host Firewall Ruleset

Rebuilding the host firewall ruleset will replace the current one by a new set of default access rules.

Do not rebuild the host firewall ruleset if you have already added an entry manually!

1. On a stand-alone firewall: Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services**.
   On a Control Center: Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > Boxes > *your box* > Infrastructure Services**.
2. Right-click **Host Firewall Rules**.

3. From the list, select **Lock**.
4. Right-click **Host Firewall Rules**.
5. From the list, select **Copy From Default**.



Step 3. Verify the Access Rule

On a stand-alone firewall: Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Host Firewall Rules**. On a Control Center: Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > Boxes > *your box* > Infrastructure Services > Host Firewall Rules** .

The access rule is located in the section for operative services and can be identified by its name OP-SRV-PXACC.

23	Pass Original Source IP (same p...	**OP-SRV-SIP**		UDP 5060 , TCP 5060 , TCP 5061	Any 0.0.0.0/0	All-LocalIPs 10.17.94.84
24	Pass Original Source IP (same p...	**OP-SRV-SNMP**		UDP 161	Any 0.0.0.0/0	SharedIPs
25	Pass Original Source IP (same p...	**OP-SRV-PX**		PROXY TCP 3128	Any 0.0.0.0/0	SharedIPs
26	Pass Original Source IP (same p...	**OP-SRV-PXACC**		PXACC TCP 9443	Any 0.0.0.0/0	SharedIPs
27	Pass Original Source IP (same p...	**OP-SRV-NTP**		NTP UDP 123	LocalBoxNetworks 10.17.94.0/24, 127.0.0.9	NTPListenIPs 10.17.94.84
28	Pass Original Source IP (same p...	**OP-SRV-ICMP**		ICMP ECHO	Any 0.0.0.0/0	Ref: SharedIPs , Ref: VPN Next Hop IPs
29	Pass Original Source IP (same p...	**BOX-ICMP-PING**		ICMP ECHO	Any 0.0.0.0/0	All-LocalIPs 10.17.94.84

Figures

1. xfw_password_cloudgen_access_proxy.png
2. rule_op_srv_pxacc.png
3. cga_host_firewall_copy_from_default.png
4. rule_in_host_firewall.png

© Barracuda Networks Inc., 2024 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.