REST API

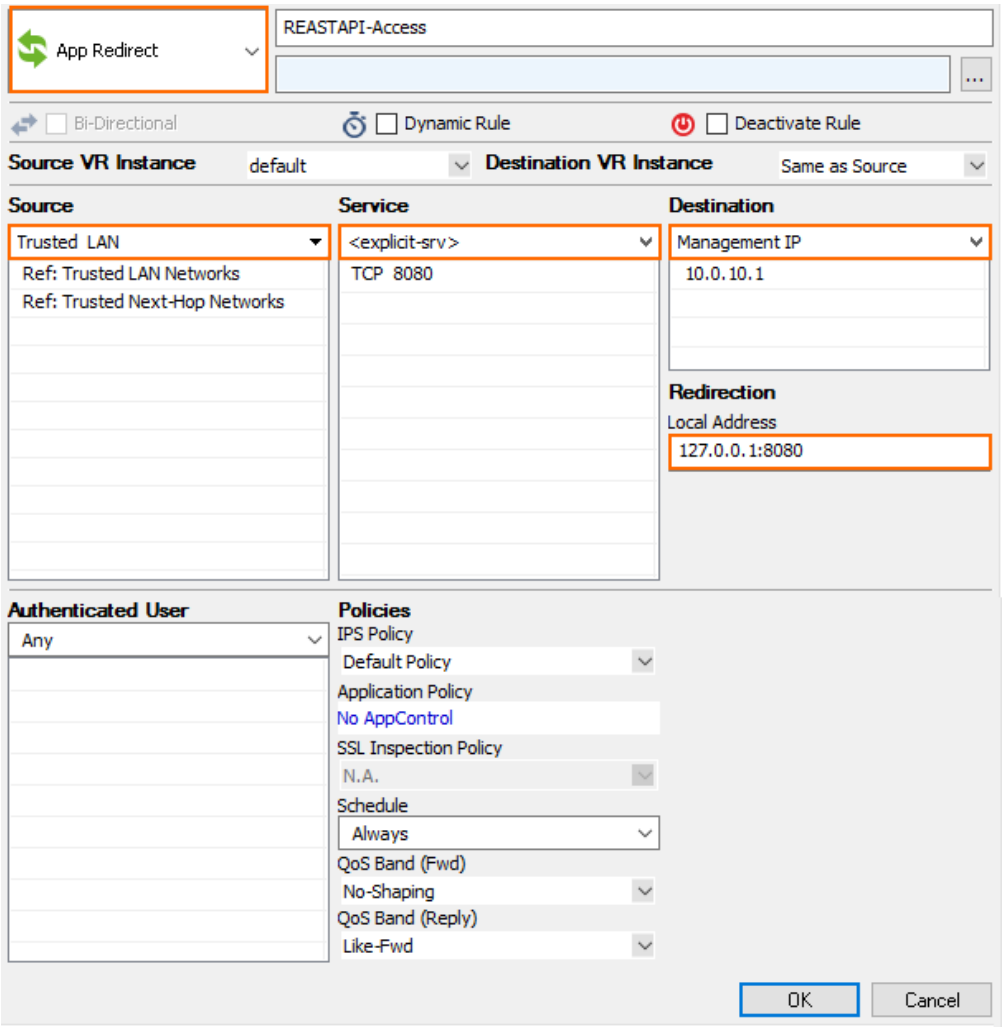
https://campus.barracuda.com/doc/73718915/

The Barracuda CloudGen Firewall REST API provides remote administration and configuration of the Barracuda CloudGen Firewall. This article gives a brief description of REST API and the API methods you can use to access your Barracuda CloudGen Firewall. The API framework provides get or set variables inside a JSON-RPC request corresponding to field values in the configuration database of the firewall .

Enable the REST API for HTTP

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > REST API Service**.
2. Click **Lock**.
3. In the **HTTP interface** window, select **Enable HTTP interface**.
4. In the **HTTP Port** field, enter the desired port for API calls.
5. Click **Send Changes** and **Activate**.
6. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.

Communication via HTTP is intended to be done from within the internal network and is thus only available on the loopback interface 127.0.0.1:<HTTP Port>. Thus, it is required to create an App Redirect access rule that redirects API calls to the loopback interface.



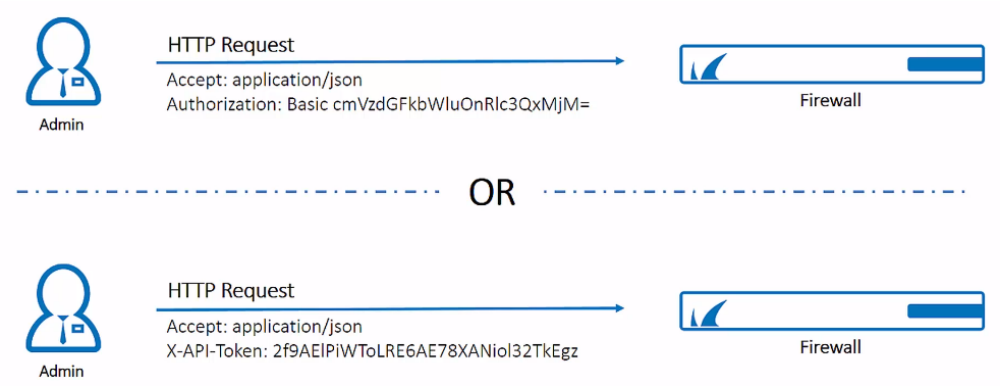
Enable the REST API for HTTPS

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > REST API Service**.
2. Click **Lock**.
3. In the **HTTP interface** window, select **Enable HTTPS interface**.
4. In the **HTTPS Port** field, enter the desired port for API calls.
5. (Optional) To enable API calls via management IP addresses instead of the loopback interface, select **Bind to Management IPs**.
6. Click **New Key** to create a private key of the desired length, or import your personal private key.
7. Click **Ex/import** to create a self-signed certificate, or import an existing one.

   The common name in the certificate must match the URI where you are sending the request. For example, if the URI is `https://CGF1.example:8443`, then the common name must be `CGF1.example`.

Authentication

The Barracuda CloudGen Firewall supports basic authentication by using either the basic authorization header or the X-API-Token header. Using the authorization header method corresponds to the traditional username:password authentication. The X-API-Token allows you to create a token to be used for all REST calls. Note that basic authentication uses base64-encoded credentials.



Create an Administrator Account for REST API Authentication

For authentication against the REST API, a user with the respective permissions must be present either on the Control Center for centrally managed firewalls or on the firewall itself for stand-alone firewalls. In both cases, the user must have the **Manager** role assigned.

- For more information on how to configure Administrators accounts on a Control Center, see How to Create a CC Admin to Access the REST API
- For more information on how to configure Administrators accounts on a stand-alone firewall, see How to Create a New Administrators Account

Create an X-API Token for Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > REST API Service**.
2. Click **Lock**.
3. In the left menu, click **Access Tokens**.
4. Click **+** in the **Access tokens** section.
5. Enter a **Name** for the token and click **OK**. The **Access tokens** window opens.
6. Click **Generate new token**.
7. Enter the **Admin name** for the user used for authentication.
8. In the **Time to live** field, enter the number of days the token should be valid for.
9. Click **OK**.

Rest API for the CloudGen Firewall

The following list shows the REST API for the CloudGen Firewall. Authentication is done using HTTP basic authentication with the username and password of the administrators with the appropriate permission set.

For more information, see Developer Documentation for the F-Series Firewall 7.2 REST API.

Figures

1. AppRedirecttoRESTAPI.png
2. REST-Auth-Methods.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.