REST API

https://campus.barracuda.com/doc/53248236/

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

The API provides an easier way to perform frequent tasks that may be time consuming to do one-by-one using Barracuda NextGen Admin. For example, using the API, you can retrieve virtual server and service states, and you can block or restart virtual servers.

REST API

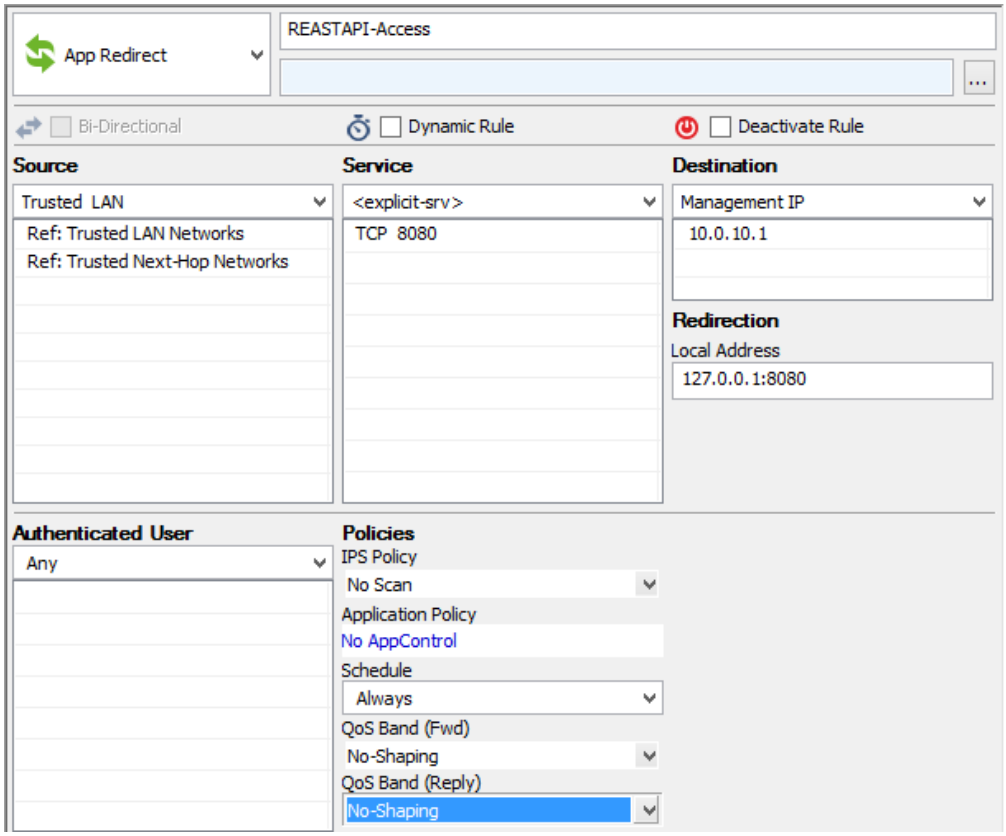
Representational State Transfer (REST) is a stateless architecture that runs over HTTP. REST API is a simple web service API you can use to interact with the Barracuda NextGen Firewall F.

For more information on REST API, please visit http://en.wikipedia.org/wiki/Representational_state_transfer.

Enabling 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 > Infrastructure Services > REST API Service**.
7. 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.



Enabling 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. To enable API calls via all management IP addresses in addition to 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://NGF1.example:8443`, then the common name must be NGF1.example.

Create CC Admin for REST API access

Admin users can access the REST API interface through a configured profile with the appropriate

administrative role. Authentication must be done using HTTP basic authentication with the username and password of one of the administrators with the REST API access rights.

For information, see How to Create a CC Admin to Access the REST API.

Rest API for the F-Series Firewall

The following list shows the REST API for the NextGen Firewall F-Series. 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 REST API.

Figures

1. AppRedirecttoRESTAPI.png