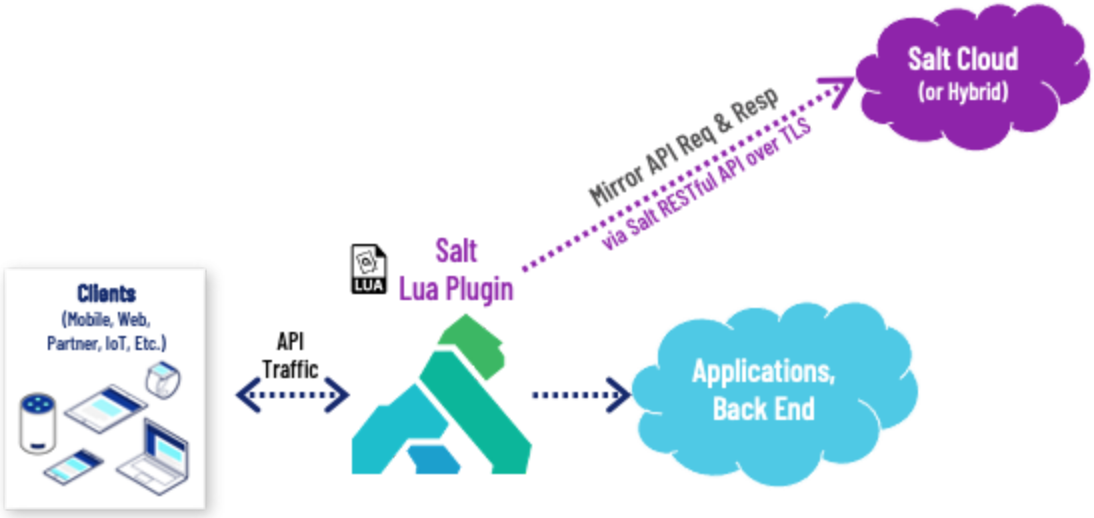
Traffic Mirroring Plugin for Kong Integration Guide

Table of Contents

Overview

The Salt Security Mirroring Plugin for Kong is used to capture a mirror of application traffic from the Kong API Gateway and send it to the Salt Security Service for analysis.

This solution uses an HTTP Connector to pass requests and responses over a secure SSL/TLS connection to the Salt Security HTTP mirroring API.



Authentication

Accessing the Salt Security HTTP mirroring API requires authentication to prevent unauthorized access. Authentication is done by a basic authentication scheme, which is sent via the request's authorization header:

- *Authorization: Basic {TOKEN}*

NOTE: The TOKEN value is unique per customer and shall be provided by the Salt Security team.

Firewall Considerations

Option 1: Mirroring from Kong server → Salt Security Hybrid Server

In your private network firewalls/security settings, make sure traffic is allowed to the Salt Security Hybrid Server. Below is the list of ports required for communication from your Kong server to the

Salt Security Hybrid Server (**NOTE**: this is only required if traffic is being sent to the Salt Security Hybrid Server):

URL	IP Address	Outbound Ports	Description
<hybrid url/ip>	<hybrid url/ip>	31443 (TCP/TLS)	Sensor Data path

Option 2: Mirroring from Kong server → Salt Cloud Service

URL	Static IP	Port	Description
traffic-receiver-http-a.dnssf.com	169.47.178.245	443 (TLS/TCP)	Sensor Data path

The Plugin

The Salt Security Mirroring Plugin for Kong consists of a LuaRocks package which results in a deployable *rock* file that contains the lua implementation.

Plugin Configuration

A Kong Lua Traffic Collector configuration is configured through the kong administrative API. Below is a list of parameters that you can pass when configuring:

Parameter	Type	Possible Values	Description
salt_domain	String	Salt Security FQDN or IP	***Required*** URL or IP used to mirror the transaction request data.
salt_backend_port	Number	Port for Salt Security Sensor traffic	***Required*** Port number used by the plugin to communicate with the Salt infrastructure
salt_token	String	Salt Security Authentication Token	***Required**** Authentication token provided by Salt to authenticate with Salt Security RESTful API.
salt_uuid	String	Universal unique identifier	A UUID used to identify the collector.[1]
salt_labels	String	comma-separated list of key=value Label pairs	A list of labels used to tag and manage the collector. For example: env=prod,region=us-east

Deploying the plugin

In the steps below, you will configure the salt-sensor plugin to enable mirroring HTTP traffic to the Salt Security Service.

Here's Kong official guide on how to enable and install a plugin on Kong API Gateway:
https://docs.konghq.com/2.0.x/getting-started/enabling-plugins/

[1] A UUID can be generated using Online UUID Generator.

Deploying directly on a system running Kong WITHOUT containers

1. **Deploying the package:**
   - Place the kong-plugin-salt-sensor-1.5.0-0.src.rock file in a folder of your choice
   - Switch to that folder before running the next steps

2. **Installing salt-sensor plugin:**
   Run the following command to install the salt-sensor plugin:

```
$ luarocks install kong-plugin-salt-sensor-1.5.0-0.src.rock
```

   Make sure you see this output:

```
kong-plugin-salt-sensor 1.5.0-0 is now installed in <path>
```

3. **Update the kong configuration file (kong.conf) with the following:**
   Add `*salt-sensor*` under the `*plugins*` property in your Kong configuration file. It should look like that:

```
...
plugins = <existing plugins>,salt-sensor
...
```

   Optional (in case you get a Lua related error), add the path to the Lua deployment location similar to this:

```
...
lua_package_path = <existing lua paths>;/usr/local/?.lua;
...
```

   Then, restart kong with the latest configuration:

```
$ kong restart -c </path/to/kong.conf>
```

4. **Configuring salt-sensor plugin:**
   The configuration for the salt-sensor plugin consists of Salt Security integration settings:
   (1) The address of the HTTP mirroring API

(2) The private authentication token provided by Salt Security

Before configuring the salt-sensor plugin for the service you configured in Kong, make sure you are provided with the above information from the Salt Security representative.

Deploying when Kong is running in a Docker Container

1. Navigate to your salt-kong-sensor/Docker directory
2. Review both the Dockerfile and dockercompose.yaml files. If needed, adjust the files to suit your environment
3. Execute the following command to add the Salt-Sensor plugin to Docker

```
$  docker-compose up -d
```

Deploying when Kong is running in Hybrid Mode

If Kong is deployed in hybrid mode, meaning the control-plane and data-planes are separated, the Salt plugin must be installed or part of the image on both the data-planes and control-plane. If using Kong Konnect SaaS, Kong's hosted Control Plane offering, please contact Kong Support to assist with the installation of the Salt Plugin on the Kong managed control-plane.

Configuring the Salt Plugin for Kong

The minimal configuration for the salt-sensor plugin requires the following information:

- SALT_MIRRORING_API_DOMAIN - The address of the HTTP mirroring API
- TOKEN - The private authentication token provided by Salt Security
- SALT_MIRRORING_API_PORT - The port used for communicating with Salt

Before configuring the salt-sensor plugin, make sure you are provided with the above information from the Salt Security representative.

Deploy the Salt plugin for a specific service

```
$ curl -i -X POST \
    --url http://<KONG_DOMAIN>:<KONG_PORT>/services/<MONITORED_SERVICE>/plugins/ \
    --data-urlencode 'name=salt-sensor' \
```

```
    --data-urlencode 'config.salt_domain=<SALT_MIRRORING_API_DOMAIN>' \
    --data-urlencode 'config.salt_backend_port=<SALT_MIRRORING_API_PORT>' \
    --data-urlencode 'config.salt_token=<TOKEN>'
```

Deploy the Salt plugin globally

```
$ curl -i -X POST \
    --url http://<KONG_DOMAIN>:<KONG_PORT>/plugins/ \
    --data-urlencode 'name=salt-sensor' \
    --data-urlencode 'config.salt_domain=<SALT_MIRRORING_API_DOMAIN>' \
    --data-urlencode 'config.salt_backend_port=<SALT_MIRRORING_API_PORT>' \
    --data-urlencode 'config.salt_token=<TOKEN>'
```

Restart kong after configuring the plugin

```
$ kong restart -c </path/to/kong.conf>
```

Removing the plugin

To remove the salt plugin, you first need to get the plugin ID:

```
$ curl -s localhost:8001/plugins | grep salt-sensor | cut -d',' -f3
"id":"b0343874-677a-4ab5-9c4b-8fa1a2fde214"
```

In this case, the ID is **b0343874-677a-4ab5-9c4b-8fa1a2fde214**

Next, run this command to remove the plugin, using the ID that we identified above:

```
$ curl -X DELETE localhost:8001/plugins/b0343874-677a-4ab5-9c4b-8fa1a2fde214
```

Restart kong after removing the plugin

```
$ kong restart -c </path/to/kong.conf>
```

Optional: remove the Salt Plugin Lua package

```
$ luarocks remove kong-plugin-salt-sensor-1.5.0-0.src.rock
```

Upgrading the plugin

A plugin upgrade is done by performing an uninstallation followed by installing the new version using the instructions provided above.

Troubleshooting

Salt Security Mirroring Plugin is writing its logs to the Kong log files.

Follow the instruction here to ensure traffic is successfully mirrored to Salt Security Service by enriching logs with debug logs.

This can be done in 2 ways:

I. **Using kong.conf:**
Add this line to kong.conf file:

```
log_level = debug
```

Then, restart kong with the latest configuration:

```
$ kong restart -c </path/to/kong.conf>
```

II. **Using environment variable:**
Add an environment variable to override default configuration:

```
$ export KONG_LOG_LEVEL=debug
```

Advanced Debugging mode. When Kong is in debug log level mode, the Salt plugin can be configured to provide transaction based advanced logging to the Kong logs for troubleshooting purposes. Below is an example of CURL command showing advanced debugging enabled with the Salt plugin configuration.

```
$ curl -i -X POST \
    --url http://<KONG_DOMAIN>:<KONG_PORT>/services/<MONITORED_SERVICE>/plugins/ \
    --data-urlencode 'name=salt-sensor' \
    --data-urlencode 'config.salt_domain=<SALT_MIRRORING_API_DOMAIN>' \
    --data-urlencode 'config.salt_backend_port=<SALT_MIRRORING_API_PORT>' \
    --data-urlencode 'config.salt_token=<TOKEN>' \
    --data-urlencode 'config.salt_debug=true'
```

Connectivity Check

To verify connectivity between the Kong Node and the Salt Mirroring APIs, use *hello RESTful API*. To simplify the connectivity check on the hybrid environment, the Hello RESTful API will not force authentication; nevertheless, if authentication credentials are provided, the Hello RESTFul API will respond with an indication of whether authentication succeeded or failed.

GET /api/v1/http/hello

Headers

Field	Type	Description
`Authorization`	String	Basic Authorization token. Optional on Hybrid environments

CURL Example

```
curl -k -X GET \
  'https://{SALT_MIRRORING_API_DOMAIN}:{SALT_MIRRORING_API_PORT}/api/v1/http/hello' \
  -H 'Authorization: Basic QWxhZGRpbjpPcGVuU2VzYW1l'
```

Success-Response Example:

```
HTTP/1.1 200 OK
It Works! Welcome To Salt Security Hybrid
Authentication Succeeded
```