ThreatQuotient

Citrix (Netscaler) WAF Connector Guide

Version 1.0.1

March 10, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Contents

Versioning **4**
Introduction **5**
Installation **6**
Configuration **9**
ThreatQ UI 9
Citrix VPX 10
Usage **11**
Basic Usage 11
Command Line Arguments 11
CRON **12**
Change Log **13**

Versioning

- Current integration version: 1.0.1
- Supported on ThreatQ versions >= 4.30.0

OPERATING SYSTEM	OS VERSION	PYTHON VERSION	NOTES
RedHat/CentOs	7	2.7.12	
Ubuntu	16.04	2.7.12	This has not been tested
Windows	2012R2/10	2.7.12	This has not been tested

Introduction

The Citrix Netscaler WAF is a custom connector that sends IP Addresses from ThreatQ to a block list in Citrix VPX. This uses Citrix's IP reputation functionality built into the platform.

Installation

The connector can be installed from the ThreatQuotient repository with YUM credentials or offline via a .whl file.

> **Upgrading Users** - Review the Change Log for updates to configuration parameters before updating. If there are changes to the configuration file (new/removed parameters), you must first delete the previous version's configuration file before proceeding with the install steps listed below. Failure to delete the previous configuration file will result in the connector failing.

1. Install the connector using one of the following methods:

   ThreatQ Repository

   a. Run the following command:

   ```
   pip install tq_conn_citrix_waf
   ```

   Offline via .whl file

   To install this connector from a wheel file, the wheel file (.whl) will need to be copied via SCP into your ThreatQ instance.

   a. Download the connector whl file with its dependencies:

   ```
   mkdir /tmp/tq_conn_citrix_waf
   pip download tq_conn_citrix_waf -d
   /tmp/tq_conn_citrix_waf/
   ```

   b. Archive the folder with the .whl files:

   ```
   tar -czvf tq_conn_tenable_sc.tgz /tmp/tq-conn-citrix-waf/
   ```

   c. Transfer all the whl files, the connector and all the dependencies, to the ThreatQ instance.

   d. Open the archive on ThreatQ:

   ```
   tar -xvf tq_conn_citrix_waf.tgz
   ```

   e. Install the connector on the ThreatQ instance.

> The example assumes that all the whl files are copied to /tmp/conn on the ThreatQ instance.

```
pip install /tmp/conn/tq-conn-citrix-waf.whl --no-index --find-links /tmp/conn/
```

> A driver called tq-conn-tenable-sc is installed. After installing with pip or setup.py, a script stub will appear in /usr/bin/tq-conn-citrix-waf.

2. Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the mkdir -p command. See example below:

   Creating Integration Directories Example

   ```
   mkdir -p /etc/tq_labs/
   mkdir -p /var/log/tq_labs/
   ```

3. Perform an initial run using the following command:

   ```
   tq-conn-citrix-waf -c /path/to/config/directory/ -ll /path/to/log/directory/ -v VERBOSITY_LEVEL
   ```

   Enter the following parameters when prompted:

PARAMETER	DESCRIPTION
ThreatQ Host	This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.
Client ID	This is the OAuth id that can be found at Settings Gear → User Management → API details within the user's details.
Email Address	This is the User in the ThreatQ System for integrations.
Password	The password for the above ThreatQ account.
Status	This is the default status for objects that are created by this Integration. It is common to set this to "Review", but Organization SOPs should be respected when setting this.

Example Output

```
tq-conn-citrix-waf -c /path/to/config/directory/ -ll /path/to/log/directory/ -v VERBOSITY_LEVEL
ThreatQ Host: <ThreatQ Host IP or Hostname>
Client ID: <ClientID>
E-Mail Address: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Review
Connector configured. Set information in UI
```

You will still need to configure and then enable the connector.

Configuration

Use the steps provided below to configure the integration in ThreatQ and in Citrix VPX.

ThreatQ UI

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Labs** option from the *Category* dropdown (optional).

   > If you are installing the connector for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
API IP/ Hostname	The Hostname or IP address of the Citrix WAF API.
Username	The username for the Citrix WAF API.
Password	The password for the Citrix WAF API.
Data Collection	The name of the data collection in the ThreatQ instance and can also be a comma-separated list of data collections.
IP Block List	The name of a block list created on the Citrix VPX appliance.
Use HTTPS	Check this box if the connection to the Citrix VPX appliance is secure.

5. Review the **Settings** configuration, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Citrix VPX

Follow these steps below to configure Citrix to accept the IP addresses sent via the connector, and add them to a block list on the device.

1. Login to Citrix VPX via the UI
2. Click on the **Configuration** tab
3. Confirm that **IP Reputation** is enabled by clicking on **Security** in the left pane menu. If there is an exclamation mark next to **Reputation**, you will need to enable it. Right click on the **Reputation** menu, and then click on **Enable Feature** in the pop up.

   The next step is to configure a block list, if there are none.
4. Click on the **Configuration** tab and then on **AppExpert** in the menu on the left pane menu, and then on **Data Sets.**
5. If there are no block lists under **Data Sets**, create a new one by clicking on the **Add** button. Enter a name for the new block list, and make sure that the type is **ipv4**. Once this is done, click on the **Create** button
6. Go to your ThreatQ instance and create a data collection from within the Threat Library.

   > ⚠ Confirm that the data collection is only for IPs as this is the only indicator type Citrix will accept. When the integration is executed, it will skip over all the indicators that are not an IP Address.

Usage

This connector is used just like any other custom connector.

Basic Usage

```
tq-conn-citrix-waf -c /path/to/config/directory/ -ll /path/to/log/directory/ -v VERBOSITY_LEVEL
```

Command Line Arguments

This connector supports the following custom command line arguments:

ARGUMENT	DESCRIPTION
-h, --help	Shows this help message and exits.
-ll LOGLOCATION, --loglocation LOGLOCATION	Sets the logging location for the connector. The location should exist and be writable by the current. A special value of 'stdout' means to log to the console (this happens by default).
-c CONFIG, --config CONFIG	This is the location of the configuration file for the connector. This location must be readable and writable by the current user. If no config file path is given, the current directory will be used. This file is also where some information from each run of the connector may be put (last run time, private oauth, etc.)
-v {1,2,3}, --verbosity {1,2,3}	This is the logging verbosity level where **3** means everything. The default is **1** (Warning).

CRON

Automatic CRON configuration has been removed from this script. To run this script on a recurring basis, use CRON or some other jobs scheduler. The argument in the CRON script must specify the config and log locations.

Add an entry to your Linux crontab to execute the connector at a recurring interval. Depending on how quickly you need updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

In the example below, the command will execute the connector every two hours.

1. Log into your ThreatQ host via a CLI terminal session.
2. Enter the following command:

   ```
   < > crontab -e
   ```

   This will enable the editing of the crontab, using vi. Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.

3. Enter the commands below:

   Every 2 Hours Example

   ```
   < > 0 */2 * * * tq-conn-citrix-waf -c /path/to/config/directory/ -ll /path/to/log/
   directory/ -ll /path/to/config/directory/ -v3
   ```

4. Save and exit CRON.

Change Log

- **Version 1.0.1**
  - Naming update - Saved Search is now Data Collection
  - Updated Threat Library class to reflect updated ThreatQ SDK documentation.
- **Version 1.0.0**
  - Initial Release