Barracuda Firewall Insights Integration

https://campus.barracuda.com/doc/79463296/

Barracuda Firewall Insights is a virtual appliance purpose-built for rapidly generating aggregated / dedicated reports for CloudGen Firewalls while maintaining or improving the accuracy of reporting data. Unlike a firewall that retains data for a maximum of 7 days, Firewall Insights caches data for up to 12 months. Creating reports is done using schedules. Since Firewall Insights enables CloudGen Firewalls to use less disk space on their internal SSDs, it contributes to longer SSD lifetimes. It also provides an aggregate view of data for customers with multiple connected devices.

Host names for stand-alone firewalls used on Firewall Insights must be unique. When using Firewall Insights in connection with more than one Control Center, the range IDs of the Control Centers must not overlap. This restriction does not apply to stand-alone firewalls. HA clusters are displayed as a single unit on Firewall Insights using the name of the primary firewall. The authentication data is transmitted through a TLS connection on TCP port 2400; the log stream is transmitted through a TLS connection on TCP port 8001.

The following data is sent to Firewall Insights:

- Firewall activity data
- SDWAN statistics
- Information about detected threats.

Before You Begin

- You must provide a shared secret that is configured beforehand on Firewall Insights. The shared secret will serve for authenticating the firewall to Firewall Insights, see Firewall Insights - Getting Started .

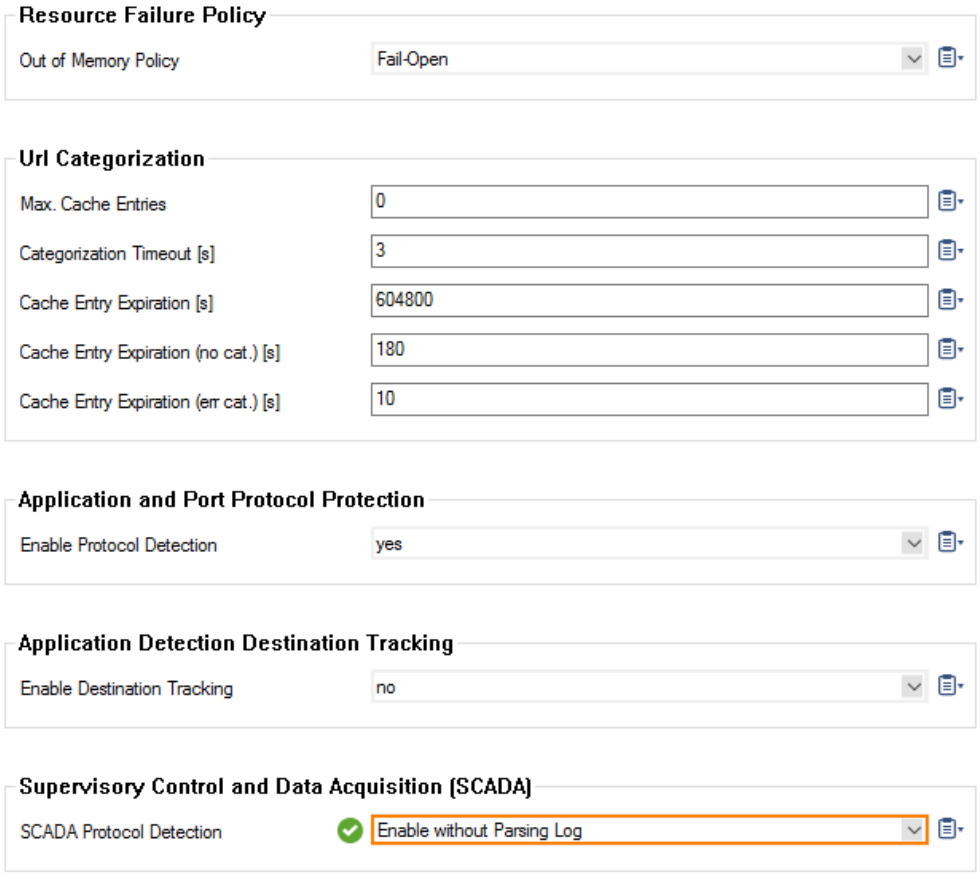
The shared secret can consist of small and capital characters, numbers, and non-alpha-numeric symbols, except the hash sign (#).

- Your Barracuda Firewall Insights must be running and reachable via the network for all local CloudGen Firewalls. For remote Firewalls, use a remote management tunnel to establish the connection to Firewall Insights. See How to Stream Data to Firewall Insights via a Remote Management Tunnel.
- Verify that your CloudGen Firewall is supported by Barracuda Firewall Insights. See Supported CloudGen Firewall Firmware.

Step 1. (optional) Enable SCADA Protocol Detection

If you are using SCADA, the corresponding protocol detection must be activated.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Service > General Firewall Configuration**.
2. Click **Lock**.
3. In the left navigation menu, click **Switch to Basic** mode.
4. In the left menu, click **Application Detection**.
5. In the **Supervisory Control and Data Acquisition (SCADA)** section, select **Enable without Parsing Log** for **SCADA Protocol Detection**.

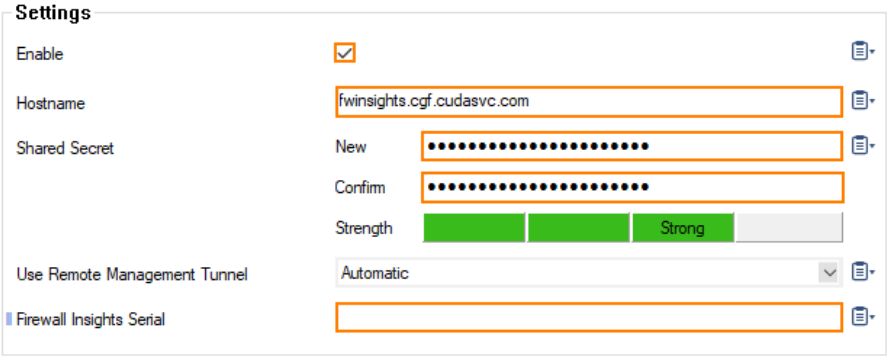


6. Click **Send Changes** and **Activate**.

Step 2. Enable Streaming to Barracuda Firewall Insights

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Syslog Streaming**.
2. In the left navigation bar, click **Barracuda Firewall Insights**.

3. Click **Lock**.
4. Select the **Enable** check box.
5. Enter the **Hostname** or the IP address of Firewall Insights.
6. Enter the **Shared Secret** from your Firewall Insights in the **New** edit field.
7. Re-enter the **Shared Secret** into the **Confirm** edit field.
8. (optional) Enter the Firewall Insights serial number you received together with the Barracuda Firewall Insights license.



9. Click **Send Changes** and **Activate**.

Your firewall will now send data to Barracuda Firewall Insights.

Step 3. (optional) Specify the location of the CloudGen Firewall

On CC-manged boxes, you can specify the location of your CloudGen Firewall. This will make the location information on Barracuda Firewall Insights more precise.

1. Go to **CONFIGURATION > Configuration Tree > Multi-Range > *your range* > *your cluster* > *your box* > Properties**.
2. In the left menu, select **Geo Location**.
3. Click **Lock**.
4. Specify the location of the system in the **Location Specific Settings** section.
    1. **Appliance Location** – Enter the name of the geolocation.
    2. **Located in Country** – Select the country your appliance is located in from the drop-down menu .
       Located in Timezone – Select the time zone your appliance is located in from the drop-down menu.
    3. Enter the **GPS Coordinates** of the location of the CloudGen Firewall.
5. In the **Barracuda Earth Integration** section, enable **Include in Barracuda Earth** by selecting **yes** from the drop-down menu.
6. Click **Send Changes** and **Activate.**

Further Information

If you have several devices to configure, save the configuration to Repository and link your devices to it. See Repositories for detailed information.

Before you link your **General Firewall Configuration** settings to a repository, ensure that you do not need different settings on the linked box or different settings for each box.

Figures

1. enable_SCADA_logs.png
2. fwinsights_enable.png