How to Integrate the Barracuda CloudGen Firewall with Nozomi Networks

https://campus.barracuda.com/doc/98219000/

Nozomi Networks is a non-intrusive continuous network monitoring solution that was purposely built to provide the required visibility and security for organizations adopting advanced Industrial IoT and OT technologies. Integrating the Barracuda CloudGen Firewall with Nozomi Networks allows the CloudGen Firewall API to create appropriate rules to block malicious hosts or connections. For this process to work, you must configure a distributed firewall rule set to apply the appropriate action.

Before You Begin

- Configure REST API access to your Barracuda CloudGen Firewall or Firewall Control Center. For more information, see REST API.
- Configure the distributed firewall service. For more information, see Distributed Firewall.

Step 1. Create an API Key

Create an API key for the CloudGen Firewall or Firewall Control Center.

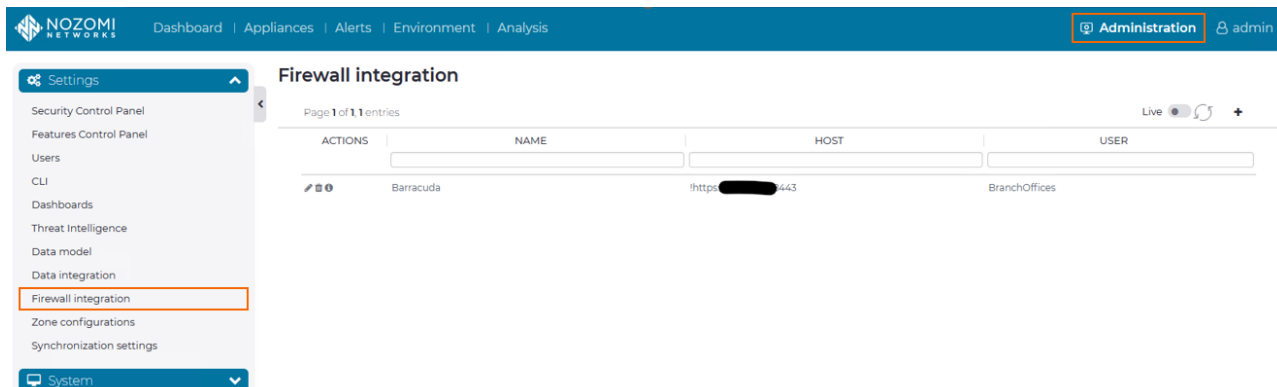- For information on how to configure administrative accounts on a Control Center, see: How to Create a CC Admin to Access the REST API.
- For information on how to configure administrative accounts on a stand-alone firewall, see How to Create a New Administrator Account.

Make a note of the created API token.

Step 2. Configure Firewall Integration on Nozomi Guardian

1. Log into your Nozomi instance.
2. Go to **Administration > Settings > Firewall integration**. The **Firewall integration** window opens.
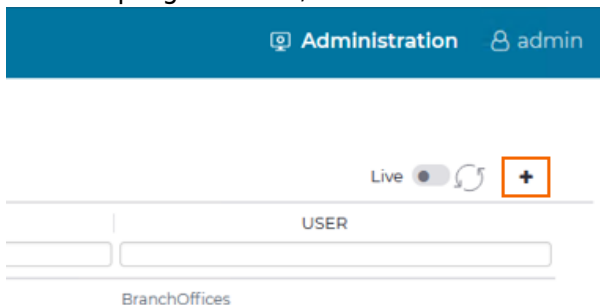
3. In the top-right corner, click **+** to add a new integration.
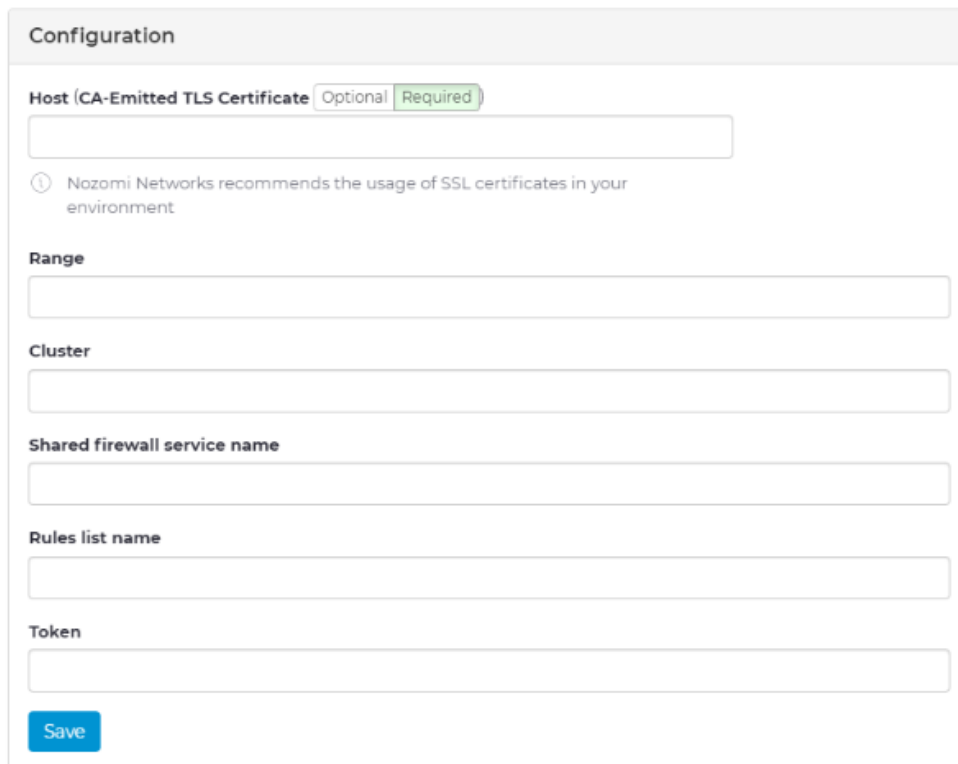
The **Choose Firewall** window opens.

4. Configure the settings according to your requirements:
    - **Host** – Enter the management IP address of the CloudGen Firewall you wish to integrate with Nozomi Networks.

- ○ **Range** – Enter the range the CloudGen Firewall resides in.
- ○ **Cluster** – Enter the cluster the CloudGen Firewall resides in.
- ○ **Shared firewall service name** – Enter the name of your CloudGen Firewall.
- ○ **Rule list name** – Enter the name of your configured distributed firewall rule set.
- ○ **Token** – Enter the API token created in the previous step.

A rule list will be added to the (distributed) firewall service within the configured Range and Cluster. In this rule list, rules to block suspicious traffic and detected anomalies will be introduced.

> You must add a *Cascade* rule to the main rule list in order to control the priority of automated actions.

5. In the **Options** section:
   1. Select **Enable nodes blocking** to quarantine specific IP addresses.
   2. Select **Enable link blocking** to block connections between source and destination IP address.
6. Click **Save**.

Figures

1. nozomi_conf_01.png
2. nozomi_conf_02.png
3. nozomi_conf_03.png