Setting up SOAR for Barracuda CloudGen Control Center Firewall

https://campus.barracuda.com/doc/101713745/

The documentation below outlines the requirements for the Barracuda XDR Security Orchestration, Automation, and Response (SOAR) for Barracuda CloudGen Control Center Firewall. When you've set this up, all required data is uploaded to the Customer Security Dashboard in the **SOAR Settings** > **Firewalls** section.

You'll have to do the following things to prepare your CloudGen Firewall for Barracuda XDR's Automated Threat Response:

You will need to provide the Barracuda XDR team with the following so they can enable Automated Threat Response for Barracuda CloudGen Firewall

- The external IP address of the Control Center firewall
- The API token
- The **Generic Network Object Group** name — If you follow the procedure below, the group is named *Barracuda_XDR_Blocked_IPs*

To enable the REST API for HTTPS

Reference: https://campus.barracuda.com/product/cloudgenfirewall/doc/96025925/rest-api/

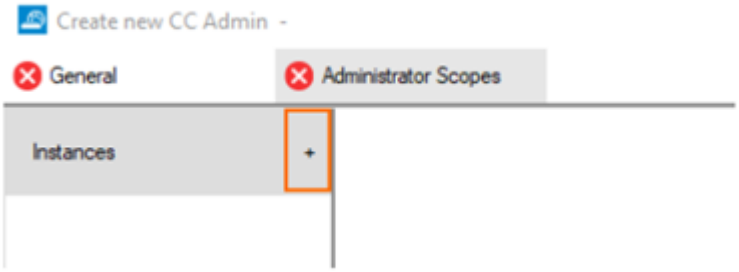
1. In **Barracuda Firewall Control Center**, navigate to **CONFIGURATION** > **Configuration Tree** > **Box** > **Infrastructure Services** > **REST API Service**.
2. Click **Lock**.
3. In the **HTTP interface** window, select **Enable HTTPS** interface.
4. In the **HTTPS Port** field, enter the desired port for API calls.
5. (Optional) To enable API calls via management IP addresses instead of 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.
8. Click **Send Changes and Activate**.
9. Provide the port number to the Barracuda XDR team.

To create a custom administrative role to access the REST API

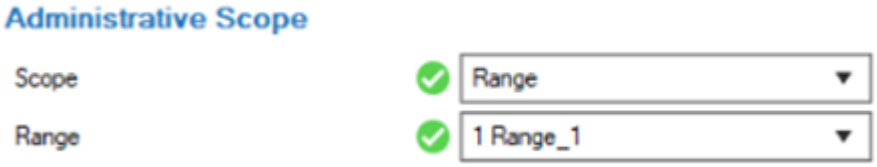
1. In **Barracuda Firewall Control Center**, go to **CONFIGURATION** > **Configuration Tree** > **Multi-Range** > **Global Settings** > **Administrative Roles**.
2. Click **Lock**.
3. In the **Roles** section, click **+** to create a new role.
4. Enter a number for the role in the **Name** field and click **OK**.
   The **Roles configuration** window opens.
5. Enter the **Role Name**: **BarracudaXDRAdmin**.
6. (Optional) Enter a **Description**. Ex: Barracuda XDR Automated Threat Response.
7. Scroll down to add the REST API access rights to the administrative role:
   - In the **REST API** section, select the **Access to REST API** check box.
   - Click **Set/Edit** to configure detailed permissions.
   - Configure the **Write Access** – Provides write access on the selected interface.
8. Click **OK**.
9. Click **OK**.
10. Click **Send Changes and Activate**.

To create an admin account to access the REST API

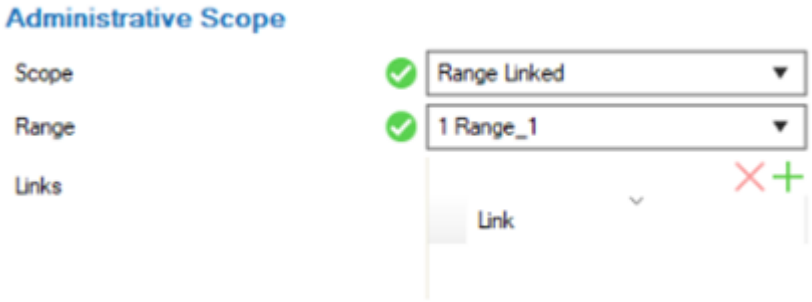
1. In **Barracuda Firewall Control Center**, click the **ADMINS** tab.
2. Do one of the following:
   1. Click **+ New Admin** on the top right of the window.
   2. Right-click the list, and select **Create New Admin**.
      The **Create New CC Admin** window opens.
3. For local authentication, configure the username and password:
   1. **Login** - *BarracudaXDRAdmin*
   2. **Full Name** - *BarracudaXDRAdmin*
   3. **Authentication Level** - select **Password**. Click the cogwheel icon next to the **Password** field, define a password for the administrative user, and click **OK**.
4. Configure the following additional settings:
   1. **Assigned Range** - This option, in combination with linked ranges, controls which entries an administrator can see in **CONFIGURATION** > **State Info** > **Sessions**, in the **Configuration Sessions** window.
   2. **Login Event** – Select **Service Default**.
   3. **ACL** - Add the IP address **44.209.49.222** to the **Peer IP Restriction** list.
      This specify the IP address the admin can use to access the Barracuda CloudGen Firewall.
5. After creating the **Admin** account, one or more specific scope(s) must be defined to be associated with the administrator.
6. In the window, click the **Administrator Scopes** tab.
7. Click **+** next to **Instances**.
   A new instance of the category **Global** is displayed.



8. Configure the **Administrative Scope**.
9. Set the scope to **Global**, a specific **Range**, or **Cluster**. Alternatively, select **Ranges** and/or **Clusters** with the **Global/Range Link** option for the administrative scope.



10. Click **+** to add selected nodes to the **Links** list.
    The options **Global Linked** and **Range Linked** associate the configured administrative rights with any individually selected node (in the **Links** list) at or below a configured **Global Linked** or **Range Linked** node (in the **Range** list).



11. Configure **Administrative Rights**.
    - **Configuration Level**: A configuration level of 2 or lower means write access, 99 or lower means read access. Usually, the write level is lower than the read level. For more information on the configuration level: https://campus.barracuda.com/product/cloudgenfirewall/doc/96026459/control-center-admins.
    - **Assign Roles**: Click **+** and add the role created in **To Create a Custom Administrative Role to Access the REST API**: *BarracudaXDRAdmin*.
    - **Shell Level**: Select **No**.
12. Click **OK**.
    The CC admin user you just created can now access the REST API interface for the ranges and clusters assigned to the user.

To generate an API token for authentication

1. In **Barracuda Firewall Control Center**, navigate to **Configuration** > **Configuration Tree** > **Box** > **Infrastructure Services** > **REST API Service**.
2. Click **Lock**.
3. In the left menu, click **Access Tokens**.
4. Click **+** in the **Access tokens** section.
5. Type the name *BarracudaXDRAPI* for the token and click **OK**.
   The **Access tokens** window opens.
6. Click **Generate** new token.
7. Enter the **Admin name** for the user used for authentication.
   This is the name of the Admin Account previously created (**BarracudaXDRAdmin**)
8. In the **Time to live** field, enter the number of days the token should be valid for.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.
11. Make a note of the name of the **API Token** to give to the Barracuda XDR team.

To create a firewall network object for the Barracuda XDR Automated Threat Response

Barracuda XDR uses the **Network Group** to block IPs on the firewall. You must create a **Firewall Network Object** called **Barracuda_XDR_Blocked_IPs**.

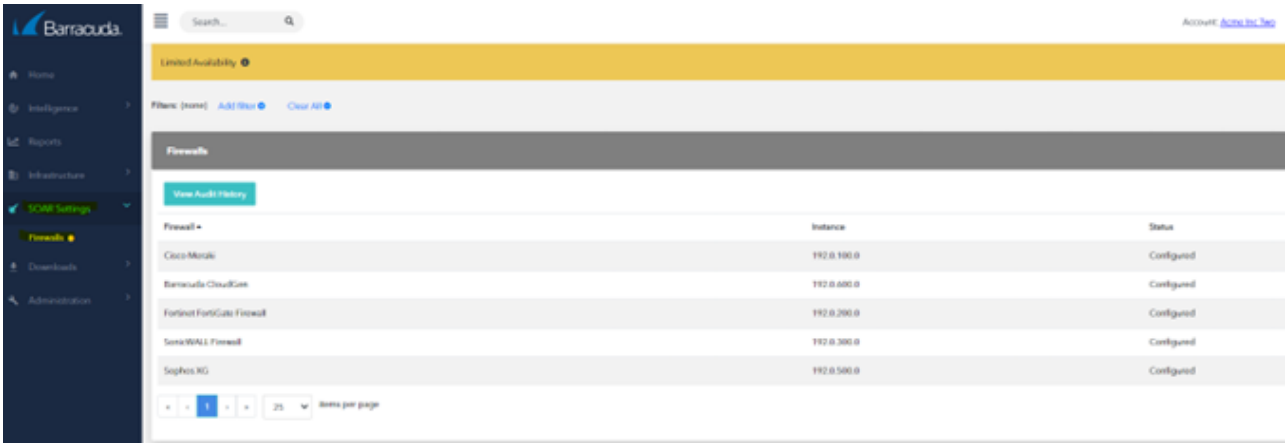
1. In **Barracuda Firewall Control Center**, go to **Configuration** > **Configuration Tree** > **Multi-Range** > (**Global**, **Range**, or **Cluster Level**) > **Firewall Objects/Policies**.
   Based on the customer firewall set up, create a **Firewall Network Object** within the administrative scope that was chosen for the configuration.
2. Click **Lock**.
3. In the left menu, scroll to **Firewall Objects** and click **Networks**.
4. Click **+** in the **Networks** section to create a network object.
5. For the **Type**, select **Generic Network Object**.
6. Enter the name **Barracuda_XDR_Blocked_IPs** for the network object.
7. (Optional) Enter a description for the **Network**, for example, *Barracuda XDR Automated Threat Response*.
8. Click **OK**.
9. Click **Send Changes and Activate**.
10. Add the **Network Object** to any preexisting firewall policies created to block traffic to/from anomalous IP addresses.
11. Send the **Network Object Name** to the Barracuda XDR team.

To add the IP address to the Peer IP restriction list

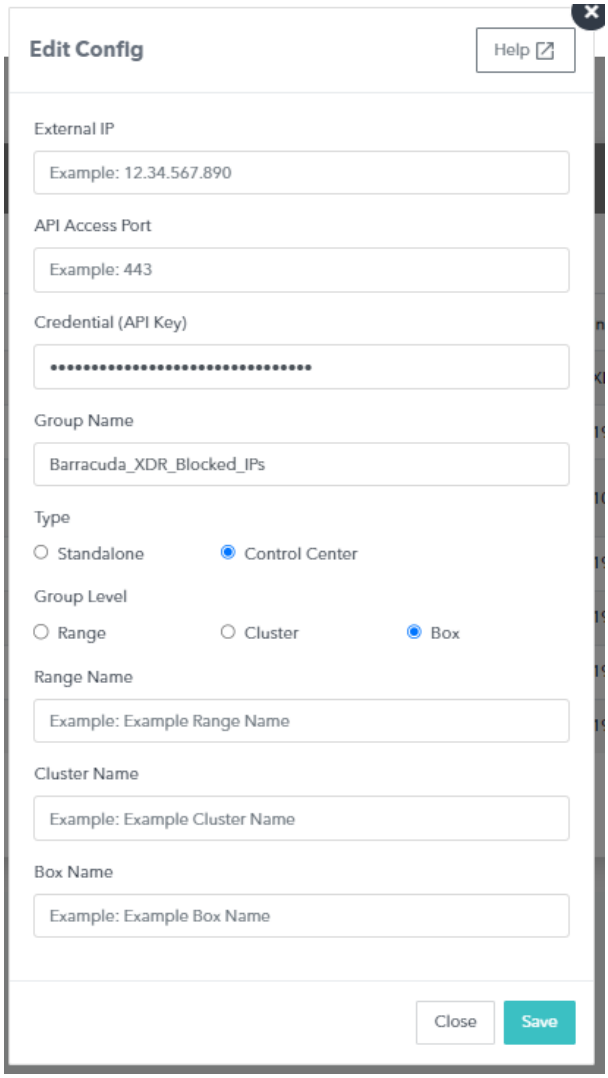
- For the **Admin Account**, add the IP address *44.209.49.222* to the **Peer IP Restriction** list.

To configure XDR dashboard

1. In **Barracuda XDR Dashboard**, click **SOAR Settings** > **Firewalls.**



2. Click **Config**.
3. In the **Edit Config** dialog box, enter the following:
    - **External IP**
    - **API Access Port**
    - **Credential (API Key)**
    - **Group Name**
    - **Firewall Type**
    - **Group Level**
    - **Range Name**
    - **Cluster Name**
    - **Box Name**


Edit Config
Help
External IP
Example: 12.34.567.890
API Access Port
Example: 443
Credential (API Key)
Group Name
Barracuda_XDR_Blocked_IPs
Type
Standalone
Control Center
Group Level
Range
Cluster
Box
Range Name
Example: Example Range Name
Cluster Name
Example: Example Cluster Name
Box Name
Example: Example Box Name
Close
Save

4. Click **Save**.

Figures

1. Picture3.png
2. Picture1.png
3. Picture2.png
4. Firewallsscreen.png
5. EditConfigDashboard.png