

Setting up SOAR for FortiGate Firewall

<https://campus.barracuda.com/doc/104367469/>

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

Prerequisites

To configure SOAR for FortiGate Firewall, you will need to know the following:

- Ensure the FortiGate is on a version that supports API v2 (FortiOS 5.6.3 or later).
- Provide the External IP Address of the FortiGate Firewall

To set up SOAR for FortiGate Firewall, you must do the following:

- [To create an Administrator profile](#)
- [To create a REST API Admin and generate an API token](#)
- [To obtain the HTTPS port number for API calls](#)
- [To create an Address Group](#)
- [To configure XDR Dashboard](#)

To create an Administrator profile

1. In FortiGate Firewall, click **System > Admin Profiles > Create New**.
2. Create a new profile called Barracuda XDR API Admin.
3. In the **Access Permissions** table, under **Access Control**, click the **Custom** icon next to **Firewall**, then do the following:
 - Next to **Policy**, select **Read/Write**.
 - Next to **Address**, select **Read/Write**.

Name:

Comments:

Access Permissions

Access Control	Permissions
Security Fabric	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
FortiView	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
User & Device	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
Firewall	<input type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input checked="" type="radio"/> Custom
Policy	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
Address	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write
Service	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
Schedule	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
Others	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
Log & Report	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
Network	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
System	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
Security Profile	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write <input type="radio"/> Custom
VPN	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
WAN Opt & Cache	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write
WiFi & Switch	<input checked="" type="radio"/> None <input type="radio"/> Read <input type="radio"/> Read/Write

4. Slide **Override Idle Timeout** to **On**. Then slide **Never Timeout** to **On**.

☒ **Override Idle Timeout**

Never Timeout ☒

5. Make a note of the profile name, to use when you create the REST API Admin.
6. Click **OK**.

To create a REST API Admin and generate an API token

1. In FortiGate Firewall, navigate to **System > Administrators > Create New > REST API Admin**.
2. In **Username**, type the username **Barracuda XDR API Admin** and select the **Administrator Profile** you created in **Create an Administrator Profile**, **Barracuda XDR API Admin**.

New REST API Admin

Username:

Comments: 0/255

Administrator profile:

PKI Group: ☐

CORS Allow Origin: ☐

Restrict login to trusted hosts

Trusted Hosts: ☒

3. In the **Restrict logins to Trusted Hosts** section, **do the following**:
 - Slide the **Trusted Hosts** slider to on.
 - Type the IP address 44.209.49.222 as a trusted host so the authentication is successful from the Barracuda side to be able to implement the IP Blocking.

Adding 44.209.49.222 as a trusted host is necessary so the authentication is successful from the Barracuda side to be able to implement the IP Blocking
4. Click **OK**.

An API token is generated.

5. Make a note of the API token.

New API key

New API key for Barracuda XDR API Admin:

ⓘ This is the only place this key will be provided. Keep this information secure. The bearer of this API key will be granted all access privileges assigned to this account.

The token is only shown once and cannot be retrieved.

6. Click **Close**.
7. Send the API Token to the Barracuda XDR team.

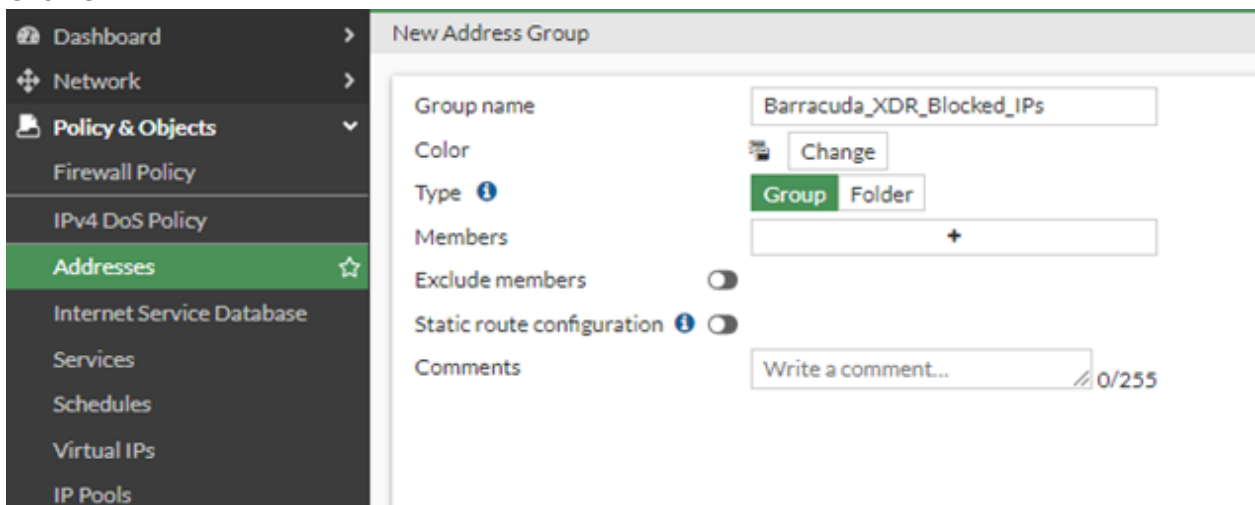
To obtain the HTTPS port number for API calls

1. If you are not using the default port (Port 443), for administrative access, please copy the correct port and the external IP address from the URL. For example, https://<IP Address>:<port> ,
2. The port can be found in the URL along with the external IP address. For example, https://<IP Address>:<port>, where <IP Address> is the external IP address and <port> is the port to use for administrative access.
3. Provide the port number to the Barracuda XDR team.

To create an Address Group

Next, create an **Address Group** called `Barracuda_XDR_Blocked_IPs`. Barracuda XDR uses this group to automatically block IPs on the firewall. Add this group to any preexisting firewall policies that block traffic to/from anomalous IP addresses.

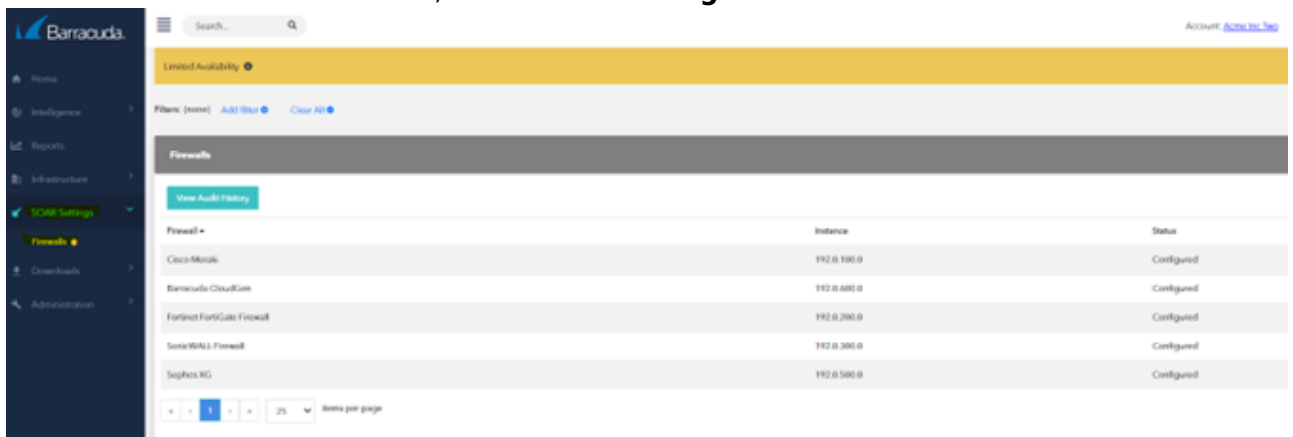
1. In the left navigation menu, click **Policy & Objects > Addresses**.
2. Click **Create New > Address Group**.
3. In **Group Name**, type `Barracuda_XDR_Blocked_IPs`.
4. In **Type**, select **Group**.
5. Click **OK**.



6. Send the **Address Group** name to the Barracuda XDR team.

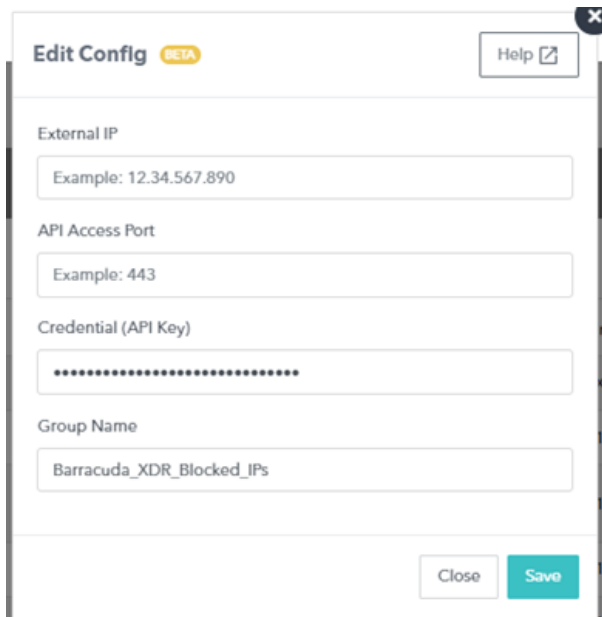
To configure XDR Dashboard

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



Firewall	Instance	Status
Cisco Meraki	192.0.100.0	Configured
Barracuda CloudGen	192.0.100.0	Configured
Fortinet FortiGate Firewall	192.0.200.0	Configured
SenseWALL Firewall	192.0.300.0	Configured
Sophos NG	192.0.500.0	Configured

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



Edit Config BETA [Help](#)

External IP
Example: 12.34.567.890

API Access Port
Example: 443

Credential (API Key)
.....

Group Name
Barracuda_XDR_Blocked_IPs

Close Save

4. Click **Save**.

Figures

1. Fortigate1.png
2. sliders.png
3. Fortigate2.png
4. Fortigate3.png
5. Fortigate4.png
6. Fortigate5.png
7. FirewallEditConfigDashboard.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.