

## Setting up SOAR for Cisco Meraki Firewall

<https://campus.barracuda.com/doc/30183/>

The documentation below outlines the requirements for the Barracuda XDR Automated Threat Response. All action items listed under the Customer Requirements must be completed. All required data will need to be uploaded to the Customer Security Dashboard in the **SOAR Settings > Firewalls** section. Please note that these instructions are only for customers using a Cisco Meraki Firewall.

To set up SOAR for Cisco Meraki Firewall, do the following:

- **To enable API Access and generate an API Key from the Meraki Dashboard**
- **To collect the Organization ID and the Network ID**
- **To create a Network Group Policy Name**
- **To ensure the IP address can make inbound connections to the firewall**
- **To configure the Barracuda XDR Dashboard**

**To enable API Access and generate an API Key from the Meraki Dashboard**

For access to the API, you must first enable the API for your organization.

1. Log in to the Meraki dashboard: <https://dashboard.meraki.com>.
2. Navigate to **Organization > Settings**.
3. Ensure the API Access is set to **Enable access to the Cisco Meraki Dashboard API**.

### Dashboard API access

API Access ⓘ

☒ Enable access to the Cisco Meraki Dashboard API

4. After enabling the API, navigate to the profile page by clicking on your account email address in the upper right. Then click **My profile**.
5. Scroll down to **API Access** to generate the API key.
6. Copy, then store the API key in a safe place. Click **Done**.

API access

API key

---

**New API key**

---

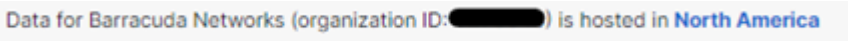
Your API key is

**Copy and store your API key in a safe place**

Dashboard does not store API keys in plaintext for security reasons, so this is the only time you will be able to record it. If you lose or forget your API key, you will have to revoke it and generate a new one.

☒ I have stored my new API key

### To collect the Organization ID and the Network ID

1. From the Meraki dashboard, from the bottom of the page, copy the **Organization ID**.  

2. From the Meraki dashboard, copy the ID of the network.  
For more information on finding the network ID, see the [Meraki documentation](#).
3. Save these ids for use in the *To configure the Barracuda XDR Dashboard* procedure.

### To create a Network Group Policy Name

Name the **Network Group Policy** "Barracuda\_XDR\_Blocked\_IPs". Barracuda XDR uses the Group Policy to automatically block IPs on the firewall.

**NOTE** Don't include a space in the **Network Group Policy** name or SOAR won't function properly. We highly recommend using *Barracuda\_XDR\_Blocked\_IPs*.

1. In the Meraki dashboard, navigate to **Network-wide > Configure > Group policies**.
2. Click **Add a group** to create a new policy.
3. Do the following:
  1. In **Name**, type Barracuda\_XDR\_Blocked\_IPs.
  2. In **Schedule**, select **Scheduling disabled**.
  3. In **Bandwidth**, select **Use network default**.
  4. In **Firewall and traffic shaping**, select **Custom network & shaping rules**.

[Group policies](#) > **New group**

Name

Schedule ⓘ

Bandwidth ⓘ  unlimited [details](#)

Firewall and traffic shaping ⓘ

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	Any		Any	Barracuda_XDR_Blk	⚙️ ✕
	Allow	Any	Any	Any	Default rule	

[Add a firewall rule](#)

Layer 7 firewall

There are no rules defined for this group.  
[Add a layer 7 firewall rule](#)

DNS layer protection (Cisco Umbrella)

Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.

- This function is only available on a created group policy.

Traffic shaping

[Add a new shaping rule](#)

or [cancel](#)

(Please allow 1-2 minutes for changes to take effect.)

4. Click **Save Changes**.

5. Copy the **Group Policy ID** from the URL at the top of the **Group Policies** page to use in the *To configure the Barracuda XDR Dashboard* procedure.

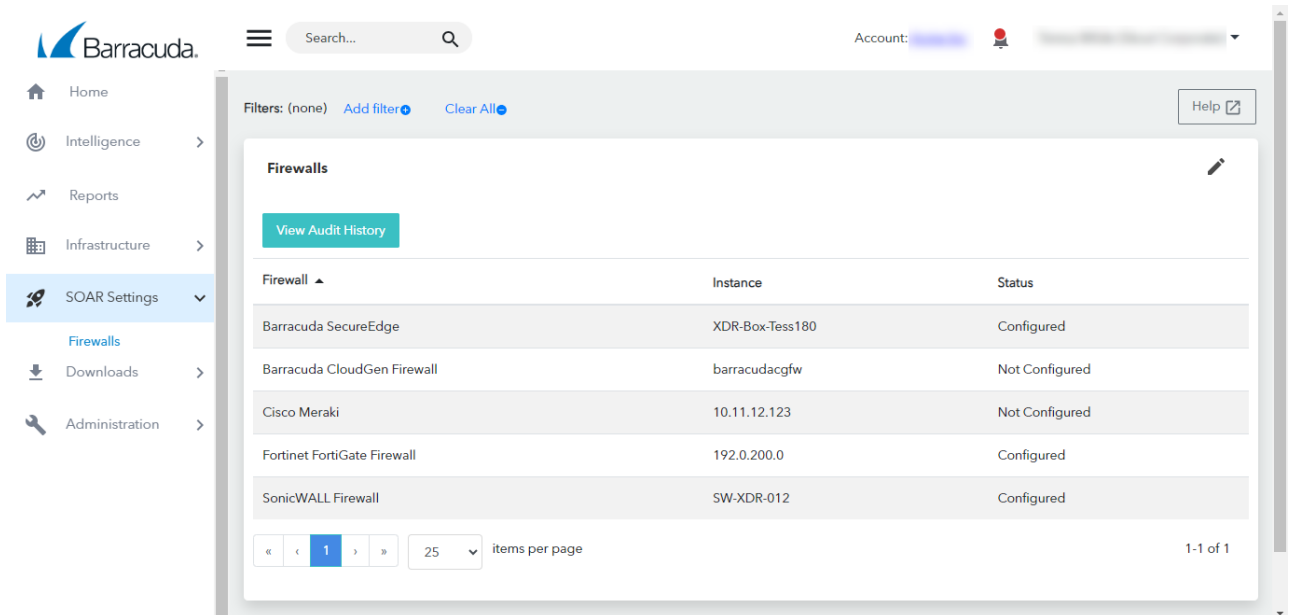
`/manage/configure/group_policies#/groups/100/edit`

#### To ensure the IP address can make inbound connections to the firewall

- **35.155.74.247** and **44.239.173.232** are the static addresses of Barracuda XDR's SOAR platform. Barracuda XDR authenticates from these IPs to remediate threats. Ensure that **35.155.74.247** and **44.239.173.232** can make inbound connections to the firewall.

#### To configure the Barracuda XDR Dashboard

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

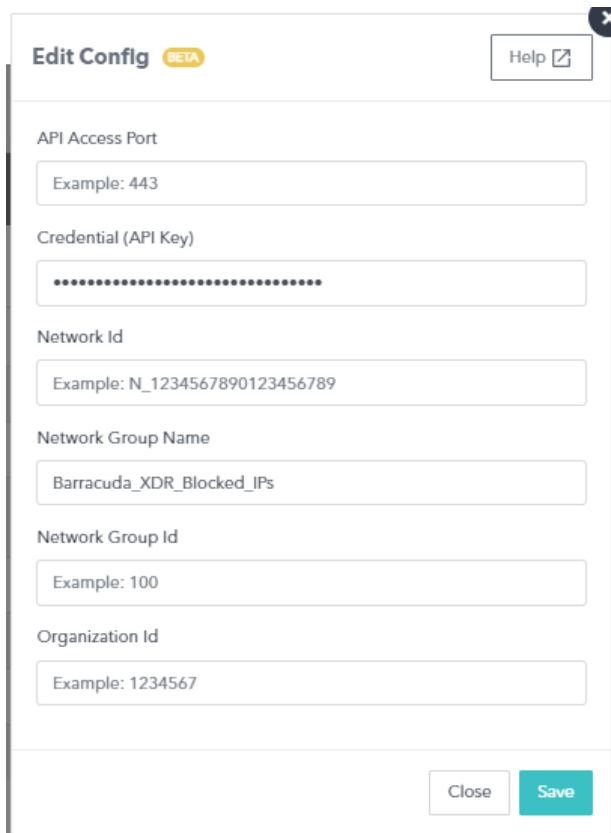


The screenshot shows the Barracuda XDR web interface. On the left is a navigation menu with options: Home, Intelligence, Reports, Infrastructure, SOAR Settings (selected), Downloads, and Administration. The main content area is titled 'Firewalls' and contains a table with the following data:

Firewall	Instance	Status
Barracuda SecureEdge	XDR-Box-Tess180	Configured
Barracuda CloudGen Firewall	barracadacgfw	Not Configured
Cisco Meraki	10.11.12.123	Not Configured
Fortinet FortiGate Firewall	192.0.200.0	Configured
SonicWALL Firewall	SW-XDR-012	Configured

Below the table is a pagination control showing '1' of 1 items per page. A 'View Audit History' button is located above the table.

2. In the **Firewalls** table, click the **Palo Alto Firewall** row.
3. Click **Edit Config**.
4. In the **Edit Config** dialog box, enter the following:
  - **API Access Port**  
**NOTE** Unless you have set a custom port for REST API calls, the port is 443.
  - **External IP**
  - **Network ID**
  - **Network Group Name**
  - **Network Group ID**
  - **Organization ID**



**Edit Config** BETA Help

API Access Port  
Example: 443

Credential (API Key)  
.....

Network Id  
Example: N\_1234567890123456789

Network Group Name  
Barracuda\_XDR\_Blocked\_IPs

Network Group Id  
Example: 100

Organization Id  
Example: 1234567

Close Save

5. Click **Save**.

If you need to edit the configuration at any time, follow the [Editing XDR SOAR Settings for a Firewall](#) procedure.

## Figures

1. Cisco Meraki.png
2. Cisco Meraki1.png
3. OrgID.png
4. networkgrouppolicyname.png
5. Cisco Meraki3.png
6. SOARFirewalls.png
7. ConfigDashboard.png

© Barracuda Networks Inc., 2025 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.