Setting up ATR 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 **ATR Settings** > **Firewalls** section. Please note that these instructions are only for customers using a Cisco Meraki Firewall.

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

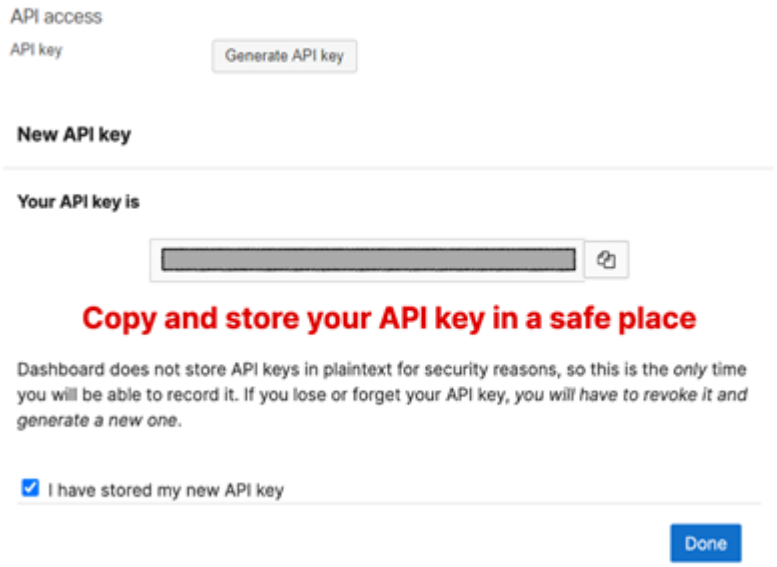
- **To enable API Access and generate an API Key from the Meraki Dashboard**
- **To collect the Organization ID and the Network ID**
- **To create a Network Group Policy Name**
- **To ensure the IP address can make inbound connections to the firewall**
- **To configure the Barracuda XDR Dashboard**

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**.

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**.



To collect the Organization ID and the Network ID

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

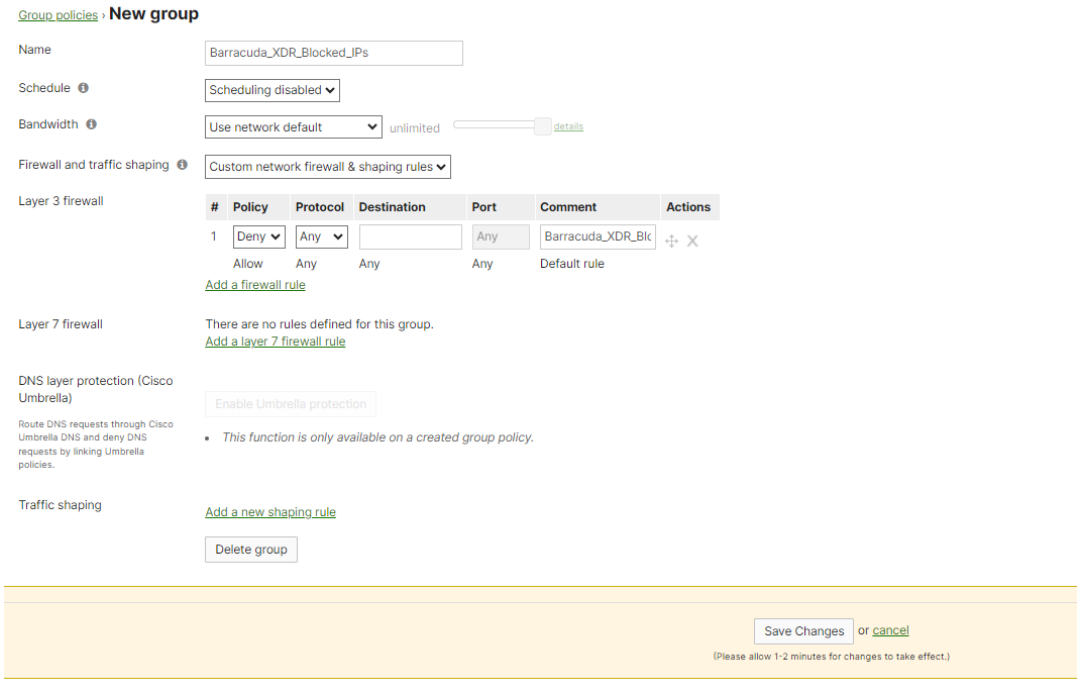
2. From the Meraki dashboard, copy the ID of the network.
   For more information on finding the network ID, see the Meraki documentation.
3. Save these ids for use in the *To configure the Barracuda XDR Dashboard* procedure.

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 ATR 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**.



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.

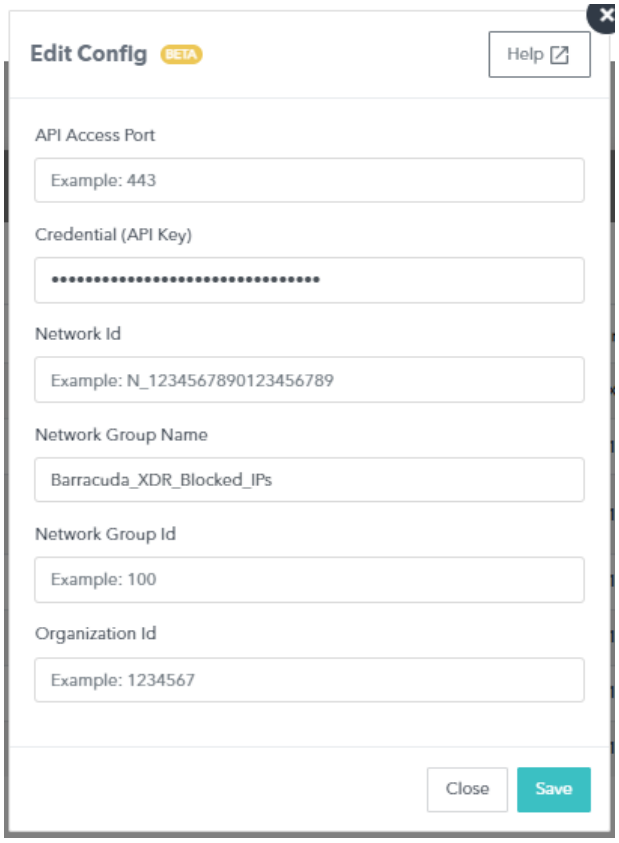
   'manage/configure/group_policies#/groups/100/edit

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 ATR 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 **ATR Settings** > **Firewalls.**
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 - Type** `Barracuda_XDR_Blocked_IPS`.
   - **Organization ID**



5. Click **Save**.

If you need to edit the configuration at any time, follow the Editing XDR ATR Settings for a Firewall procedure.

Figures