

# 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.

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**.

## Barracuda XDR



API key	Generate API key
	Control and An I hay
New API key	
Your API key is	
	2
Сору	and store your API key in a safe place
Copy Dashboard does you will be able to generate a new o	and store your API key in a safe place not store API keys in plaintext for security reasons, so this is the only to o record it. If you lose or forget your API key, you will have to revoke it one.
Copy Dashboard does you will be able to generate a new of	P and store your API key in a safe place not store API keys in plaintext for security reasons, so this is the only to o record it. If you lose or forget your API key, you will have to revoke it one.

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

- 1. From the Meraki dashboard, from the bottom of the page, copy the **Organization ID**. Data for Barracuda Networks (organization ID:
- 2. From the Meraki dashboard, copy the ID of the network. For more information on finding the network ID, see the <u>Meraki documentation</u>.
- 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.



Group policies > New group								
Name	Bar	rracuda_XD	R_Blocked_	IPs				
Schedule ()	Sch	neduling dis	abled 🗸					
Bandwidth 🚯	Use	e network d	lefault	✓ unlimited ⊂		details		
Firewall and traffic shaping 0	Cu	stom netwo	ork firewall &	shaping rules 🗸				
Layer 3 firewall	#	Policy	Protocol	Destination	Port	Comment	Actions	
	1	Deny 🗸	Any 🗸		Any	Barracuda_XDR_Bk	ΦX	
		Allow	Any	Any	Any	Default rule		
	Add	a firewall r	ule					
Layer 7 firewall	The <u>Add</u>	re are no ru I a layer 7 fi	iles defined rewall rule	for this group.				
DNS layer protection (Cisco Umbrella)								
Route DNS requests through Cisco Umbrella DNS and deny DNS requests by linking Umbrella policies.	• 7	This functio	n is only av	ailable on a created	group polic;	<i>.</i>		
Traffic shaping	Add	a new sha	ping rule					
	De	elete group						
								Save Changes or cancel
							(Ple	ease 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 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

# Barracuda XDR



	help E
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

### 5. Click Save.

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



### Figures

- 1. Cisco Meraki.png
- 2. Cisco Meraki1.png
- 3. OrgID.png
- 4. networkgrouppolicyname.png
- 5. Cisco Meraki3.png
- 6. 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.