

Setting up SOAR for Barracuda CloudGen Standalone Firewall

https://campus.barracuda.com/doc/104367493/

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

To configure SOAR for Barracuda CloudGen Standalone Firewall, you must do the following:

- To send the External IP Address of the Standalone firewall to Barracuda XDR
- To enable the REST API for HTTPS
- To create an Admin Account for the REST API
- To generate an API Token for authentication
- To create a Firewall Network Object for the Barracuda XDR Automated Threat Response
- To add the IP address 44.209.49.222 to the Peer IP Restriction list for the REST API Admin
- To configure XDR Dashboard

To send the External IP Address of the Standalone firewall to Barracuda XDR

• Send the external IP address of the standalone firewall to the Barracuda XDR team.

To enable the REST API for HTTPS

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

- 1. In Barracuda CloudGen, navigate to CONFIGURATION > Configuration Tree > Box > Infrastructure Services > REST API Service.
- 2. Click Lock.
- 3. In the HTTP interface window, select Enable HTTPS
- 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 an Admin Account for the REST API

- 1. Go to **CONFIGURATION > Configuration Tree > Box > Administrators**.
- 2. Click Lock.
- 3. In the **Administrators** section, click + to add an administrator account.
- 4. Type the name **BarracudaXDRAdmin** for the account and click **OK**.



The Administrators window opens. This account name is used to log into the firewall.

- 5. Type the **Full Name** of the administrator or a description for the account (**BarracudaXDRAdmin**).
- 6. In the Assigned Roles table, add the Manager administrative role for the user. For authentication against the REST API, a user with the appropriate permissions must be present either on the Control Center for centrally managed firewalls or on the firewall itself for stand-alone firewalls. In both cases, the user must have the Manager role assigned.
- 7. From the **System Level Access** list, select **No OS Login**.
- 8. For the Authentication Level, choose Password.
- 9. When using a password, select the corresponding scheme from the **Password Validation** list.
- 10. Enter the password for the Barracuda Firewall Admin login. When creating an account, the new password must be entered in both the Current and New fields, even though the password has not yet been created. The password must be confirmed by re-entering it in the Confirm field.
- Use the Peer IP Restriction table to set an access restriction on IP address and/or subnet level on which Barracuda Firewall Admin runs.
 Add the IP address 44.209.49.222 to the Peer IP Restriction list. This specifies the IP

address the admin can use to access the Barracuda CloudGen Firewall.

- 12. From the Login Event list, select Service Default (default).
- 13. Click Send Changes and Activate.

To generate an API Token for authentication

- 1. Navigate to CONFIGURATION > Configuration Tree > Box > Infrastructure Services > REST API Service.
- 2. Click Lock.
- 3. In the left menu, click **Access Tokens**.
- 4. In the Access Tokens section, click +.
- 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 will be the name of the admin account created in *To create an Admin Account for the REST API* above (**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. Send the API Token to the Barracuda XDR team.

To create a Firewall Network Object for the Barracuda XDR Automated Threat Response

Create a Firewall **Network Object** for Barracuda XDR Automated Threat Response, called **Barracuda_XDR_Blocked_IPs**. This **Network Group** is used by XDR for automatically blocking IPs on the firewall.



- 1. Navigate to CONFIGURATION > Configuration Tree > Box > Assigned Services > NGFW (Firewall) > Forwarding Rules.
- 2. Click **Lock**.
- 3. In the left menu, scroll down to **Firewall Objects** and click **Networks**.
- 4. In the Networks section, click + to create a network object.
- 5. For the Type, select Generic Network Object.
- 6. Type the name *Barracuda_XDR_Blocked_IPs* for the network object.
- 7. (Optional) Enter a description for the Network.
- 8. Click **OK**.
- 9. Click Send Changes and Activate.
- 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 44.209.49.222 to the Peer IP Restriction list for the REST API Admin

• 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.

Marracuda.	Seath Q		Account: Across Inc. Two
n Home	Linited Assistsing 🖸		
⊕ intelligence →	Filmer: (normal) Add (Block 🖗 Creat All 🗣		
M Reports	Freeds		
B) Infrastructure 2			
🖌 İstansaraya 👘 👻	View Audd Pattory		
Li revente e	Freed.	Instance	Status
Downloads	Cisco Maraki	192.0.100.0	Configured
	Terroule CoulGet	112.0.600.0	Configured
Administration	Fortinet FortiGate Freewalt	192.0.200.0	Configured
	Sonic/WALL Firmual	792.0.300.0	Configured
	Sephes NG	192.0.500.0	Configured
	x x 1 x 21 v Remarka		

- 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

Barracuda XDR



Edit Config	Help 🛛
External IP	
Example: 12.34.567.890	
API Access Port	
Example: 443	
Credential (API Key)	
•••••	
Group Name	
Barracuda_XDR_Blocked_IPs	
Туре	
Standalone Control Center	

4. Click Save.

Barracuda XDR



Figures

- 1. Firewallsscreen.png
- 2. EditConfigDashboard.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.