

Setting up SOAR for SonicWall Firewall

<https://campus.barracuda.com/doc/104367544/>

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

Prerequisites

- Before proceeding, ensure SonicWall firewall is version 7.0 or higher.
- Send the external IP address of the SonicWall firewall to the Barracuda XDR team.

To set up SOAR for SonicWall Firewall, do the following

- To select an authentication method for SonicOS API
- To create an Admin user for the API
- To obtain the HTTPS port number for API calls
- To ensure the HTTPS User Login option is enabled
- To create an address group
- To add the IP address to the Trusted Users group
- To configure the Barracuda XDR Dashboard

To select an authentication method for SonicOS API

The SonicOS API is enabled by default in SonicOS 7.0 and SonicOSX.

1. Navigate to **Device > Settings > Administration > Audit/SonicOS API**.
2. Toggle the switch to **RFC-2617 HTTP Basic Access authentication**.
3. Click **Accept**.

To create an Admin user for the API

1. Log in to SonicWall Firewall.
2. Click **Device**.
3. Navigate to **Users > Local Users & Groups**.
4. Click **Local Users**
5. Click **Add User**.
6. In **Name**, type the username BarracudaXDRAAdmin.
7. In **Password**, type a password for the user.
8. Click on **Groups**.
9. Click the group you want to give the user **Administrator**.
10. Select the **SonicWall Administrators** group to allow the user to make configuration changes.

The XDR admin must be able to make configuration changes to block IP addresses on the firewall. For more details on admin rights for Local Users, please see

<https://www.sonicwall.com/support/knowledge-base/access-rights-for-administrators/1705>

03478923672/.

11. Click **Save**.
12. Send the **Username** and **Password** to the Barracuda XDR team.

To obtain the HTTPS port number for API calls

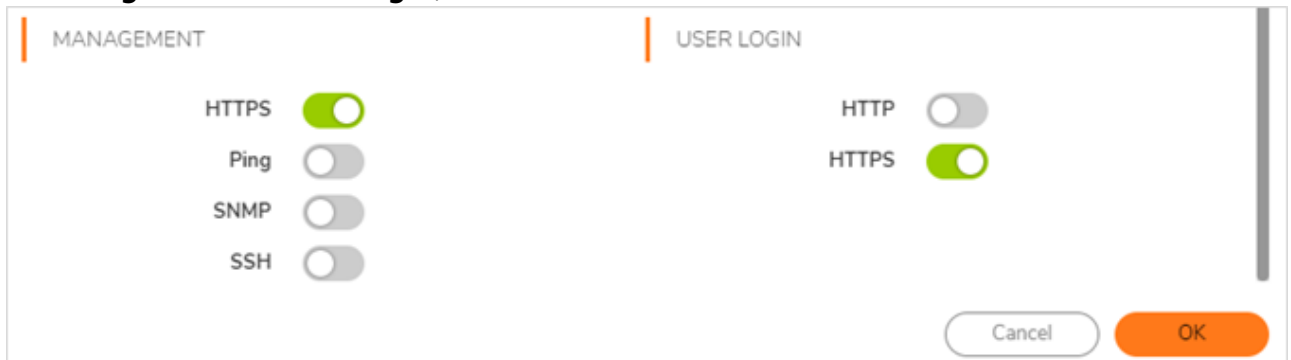
You can find the the port can be found in the URL along with the external IP address. For example, in `https://<IP Address>:<port>`, where <IP Address> is the external IP address and <port> is the port number.

Another way to verify the port number would be to do the following:

1. Navigate to **Home > API**.
2. Click on the link <https://sonicos-api.sonicwall.com>. Swagger will prepopulate your SonicWalls's IP, MGMT Port, Firmware. The port number should be visible in the URL when you navigate to the website.
3. Provide the port number to the Barracuda XDR team.

To ensure the HTTPS User Login option is enabled

1. Log in to **SonicWall Firewall**.
2. Navigate to **Network > System > Interfaces**.
3. Click the **Edit** button of the interface.
4. In **Management & User Login**, select **HTTPS**.



5. Click **Save**.

Admin access from the WAN interface is needed for XDR to have remote access to the firewall device. Please make sure to restrict the https management access so that the device responds only to the XDR SOAR IP: **44.209.49.222**. Additional reference:

<https://www.sonicwall.com/support/knowledge-base/how-can-i-restrict-admin-access-to-the-device/170503259079248/>

6. Navigate to **Policy > Access Rules**.
7. Modify the **WAN -> WAN** default rule to lock down the **Source Address** to 44.209.49.222.

	GENERAL		ZONE		ADDRESS		SERVICE	USER	SCHEDULE	PROFILES
	PRIORITY	NAME	SOURCE	DESTINATION	SOURCE	DESTINATION	DESTINATION PORT	USERS	SCHEDULE	ACTION
<input type="checkbox"/>	5	Default Access Rule_200_10	WAN	WAN	Barracuda XDR SOAR IP	All X2 Management IP	HTTPS Management	All	Always	

To create an address group

1. In **SonicWall Firewall**, navigate to **Object > Match Objects > Addresses > Address Groups**.
2. Click **Add** to add the new address group called **Barracuda_XDR_Blocked_IPs**.
Barracuda XDR uses the **Address Group** when automatically blocking IPs on the firewall. If you do not have a preexisting policy in place, create one and add the address group. For more information, see <https://www.sonicwall.com/support/knowledge-base/using-firewall-access-rules-to-block-incoming-and-outgoing-traffic/170503532387172/#Resolution1>.
3. Add the **Barracuda_XDR_Blocked_IPs** group to any preexisting firewall policies that were created to block traffic to/from anomalous IP addresses.
4. Send the **Address Group Name** to the Barracuda XDR team.

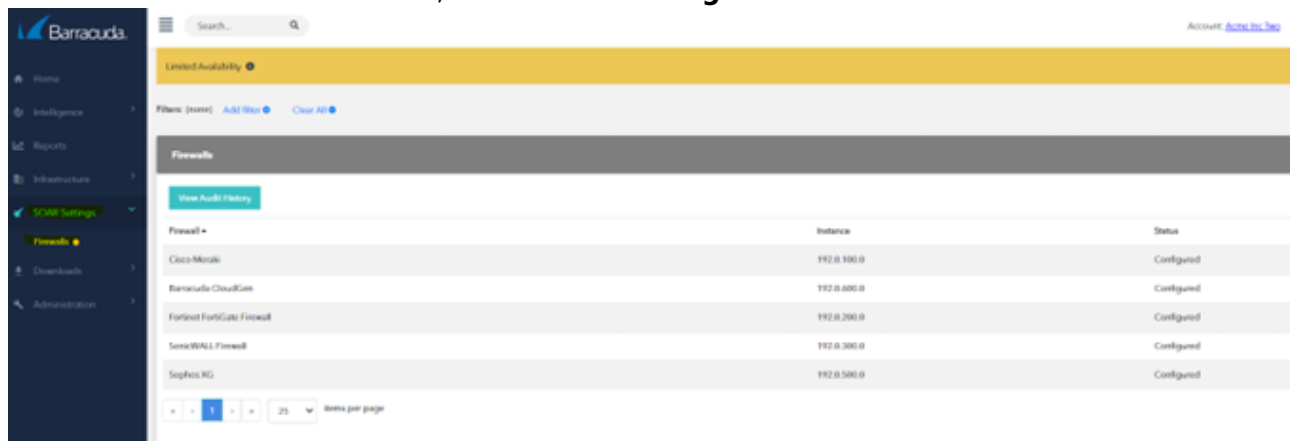
To add the IP address to the Trusted Users group

44.209.49.222 is the static address of Barracuda XDR's SOAR platform. Barracuda XDR authenticates from this IP to remediate threats.

- Follow this procedure to add the IP address 44.209.49.222 to the Trusted Users Group: [How to add IPs to Connection Management and Trusted Networks](#).

To configure the Barracuda XDR Dashboard

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



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

Edit Config BETA Help

External IP

Example: 12.34.567.890

API Access Port

Example: 443

Username

Example: Example Username

Credential

.....

Group Name

Barracuda_XDR_Blocked_IPs

Close

Save

4. Click **Save**.

Figures

1. WAN interface.png
2. Picture2.png
3. Firewallsscreen.png
4. SonicWALL config.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.