

Setting up SonicWALL Firewall Collector

<https://campus.barracuda.com/doc/99621490/>

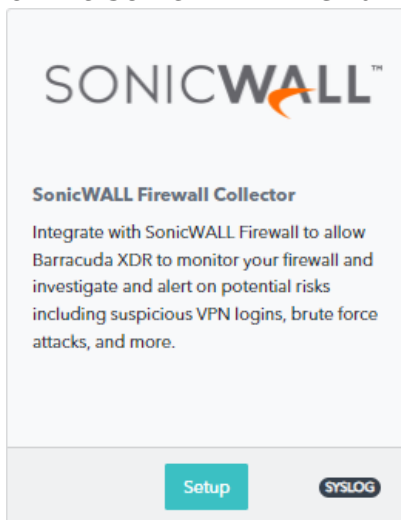
This setup is for the XDR Collector only. If you are using a physical or virtual sensor, refer to [Integrating SonicWALL Firewall](#).

To set up the SonicWALL Firewall Collector, follow the procedures below:

- **Enable the SonicWALL Firewall Collector integration**
- **Install the XDR Collector**
- **Configure the Firewall**
- **Open the port on the XDR Collector Host**

Enable SonicWALL Firewall

1. In **Barracuda XDR Dashboard**, navigate to **Administration > Integrations**.
2. On the **SonicWALL Firewall Collector** card, click **Setup**.



3. Select the **Enable** check box.



4. Click **Save**.

Install the XDR Collector

When collecting logs from one or more integrated data sources, always set up the XDR Collector on a dedicated host server. Don't use an existing server because the amount of data produced by logs can impact critical infrastructure.

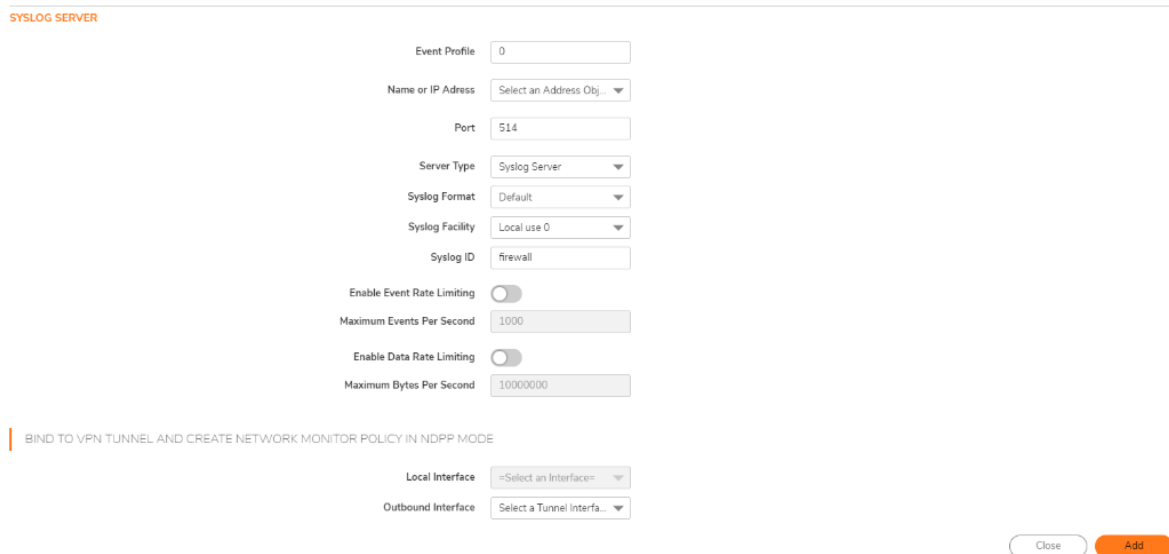
- If you haven't already set up the XDR Collector, do one of the following:
 - [Setting up the XDR Collector for Windows](#)
 - [Setting up the XDR Collector for Linux](#)

Configure the Firewall

1. In SonicWALL Firewall, go to **Device > Log > Syslog**.
2. Click **Syslog Servers** tab.
3. Click **Add**.

The **Add Syslog Server** dialog appears.

Add Syslog Server



4. Specify the **Event Profile** for this server.
The minimum value is 0 (1 group), the maximum is 23 (24 groups), and the default is 0. Each group can have a maximum of 7 Syslog servers. For GMS, the **Event Profile** must be 0.
5. Select the Syslog server **Name** or **IP address**.
Messages from the firewall are then sent to the servers.
6. In the **Port Number** field, type 9204.
7. Select the **Syslog Format**.
The default is **Default**. For **GMS**, the Syslog format must be **Default**.
8. Select the **Syslog Facility**.
The default is **Local Use 0**. For **GMS**, the Syslog format must be **Local Use 0**.
9. Type the **Syslog ID**.

The default ID is firewall.

10. Optionally, to limit events logged and therefore, prevent the internal or external logging mechanism from being overwhelmed by log events, select **Enable Event Rate Limiting**. Event rate limiting is applied regardless of Log Priority of individual events. Specify the maximum number of events in the Maximum Events Per Second field; the minimum number is 0, the maximum is 1000, and the default is 1000 per second.
11. Optionally, to limit events logged and therefore, prevent the internal or external logging mechanism from being overwhelmed by log events, select **Enable Data Rate Limiting**. Data rate limiting is applied regardless of Log Priority of individual events. Specify the maximum number of bytes in the Maximum Bytes Per Second field; the minimum is number is 0, the maximum is 1000000000, and the default is 10000000 bytes per second. This control limits data logged to prevent the internal or external logging mechanism from being overwhelmed by log events.
12. To bind to a VPN tunnel and create a network monitor policy in NDPP mode:
 1. Optionally, choose a **Local Interface**.
 2. Optionally, choose an **Outbound Interface**.
13. Click **Add**.

For more information, see the [SonicWALL Firewall Documentation](#).

Open port on the XDR Collector Host

Ensure incoming traffic is allowed on UDP port 9204.

Linux

```
sudo ufw allow 9204/udp
```

Windows

```
netsh advfirewall firewall add rule name="SonicWALL Firewall Events" dir=in  
action=allow protocol=UDP localport=9204
```

Figures

1. 2024-02-29_13-17-49.png
2. 2024-02-29_13-18-30.png
3. sonicwall-syslog-server-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.