Troubleshooting

https://campus.barracuda.com/doc/12194096/

The following diagnostic tools should help you troubleshoot most problems. Please read this article before contacting Barracuda Networks Technical Support.

Basic Troubleshooting Tools

The **ADVANCED > Troubleshooting** page provides a suite of tools to help you troubleshoot network connectivity issues that might be impacting the performance of your Barracuda NextGen X-Series Firewall.

For example, you can test your X-Series Firewall's connection to the Barracuda Networks update servers to verify that it can successfully download the latest Energize Update definitions. You can also ping or telnet to other devices from the X-Series Firewall, perform dig/NS-lookup, TCP dump, and perform a trace route from the X-Series Firewall to any another system.

Connect to Barracuda Networks Support Servers

To let technical support engineers troubleshoot your system, you can initiate a connection between your X-Series Firewall and the Barracuda Networks Technical Support Center. On the **ADVANCED > Troubleshooting** page, in the **Support Connection** section, click **Establish Connection to Barracuda Networks Support Center**. The connection to Barracuda Networks' Support Center is established via a VPN over SSH 2.0 tunnel with RSA 2048bit key length using AES128-cbc hmac-md5 hash functions.

Rebooting the System in Recovery Mode

If your X-Series Firewall experiences a serious issue that impacts its core functionality, you can use diagnostic and recovery tools that are available from the reboot menu to return your system to an operational state. Before you use the diagnostic and recovery tools:

- Use the built-in troubleshooting tools on the **ADVANCED > Troubleshooting** page to help diagnose the problem.
- Perform a system restore from the last known good backup file.
- Contact Barracuda Networks Technical Support for additional troubleshooting tips.

As a last resort, you can reboot your X-Series Firewall and run a memory test or perform a complete system recovery, as described below.

To perform a system recovery or hardware test:

1. Connect a monitor and keyboard directly to your X-Series Firewall.
2. Reboot the system by doing one of the following:
   - In the web interface: Go to the **BASIC > Administration** page, navigate to the **System Reload/Shutdown** section, and click **Restart**.
   - At the front panel of the X-Series Firewall: Press the **Power** button on the front panel to turn off the system, and then press the **Power** button again to turn the system on.

   The splash screen displays with the following three boot options:
   - Barracuda
   - Recovery
   - Hardware_Test
3. Use your keyboard to select a boot option, and then press the **Enter** key. You must select the boot option within three seconds after the splash screen appears. If you do not select an option within three seconds, the X-Series Firewall starts up in **Normal** mode (first option). For a description of each boot option, refer to the **Reboot Options** below.

To stop a hardware test, reboot your X-Series Firewall by pressing **Ctrl**+**Alt**+**Del**.

Reboot Options

The table below describes the options available at the reboot menu.

Reboot Options	Description
Barracuda	Starts the X-Series Firewall in the normal (default) mode. This option is automatically selected if no other option is specified within the first three seconds of the splash screen appearing.

Recovery	Displays the Recovery Console, where you can select the following options: • **Barracuda Repair (no data loss**) – Repairs the file system on the X-Series Firewall. • **Full Barracuda Recovery (all data lost**) – Restores the factory settings on your X-Series Firewall and clears out the configuration information. • **Enable remote administration (reverse runnel)** – Turns on the reverse tunnel that lets Barracuda Networks Technical Support access the system. You can also enable remote administration by going to the **ADVANCED >Troubleshooting** page and clicking **Establish Connection to Barracuda Networks Support Center**. • **Diagnostic memory test** – Runs a diagnostic memory test from the operating system. If problems are reported when running this option, we recommend running the Hardware_Test option next.
Hardware_Test	Performs a thorough memory test that shows most memory-related errors within a two-hour time period. The memory test is performed outside of the operating system and can take a long time to complete. To stop the hardware test, reboot your X-Series Firewall.

Replacing a Failed System

Before you replace your X-Series Firewall, use the tools provided on the **ADVANCED > Troubleshooting** page to try to resolve the problem, or call Barracuda Networks Technical Support.

Barracuda Instant Replacement Service

If you purchased the Instant Replacement service and the X-Series Firewall fails, you can call Barracuda Networks Technical Support and arrange for a new unit to be shipped out within 24 hours.

After receiving the new system, ship the old X-Series Firewall back to Barracuda Networks at the address below, with an RMA number marked clearly on the package. Barracuda Networks Technical Support can provide details on the best way to return the unit.

Barracuda Networks

3175 S. Winchester Blvd

Campbell, CA   95008

attn: RMA # <your RMA number>

To set up the new X-Series Firewall so that it has the same configuration as your old failed system, first manually configure the new system's IP information on the **BASIC > IP Configuration** page, and then restore the backup file from the old system onto the new system. For information on restoring data, see How to Backup and Restore the Barracuda NextGen Firewall X.