

Troubleshooting

<https://campus.barracuda.com/doc/6160413/>

The Barracuda Networks backup process does NOT back up your SSL certificates, therefore, if you do not manually back up SSL certificates, you must redeploy using a new certificate.

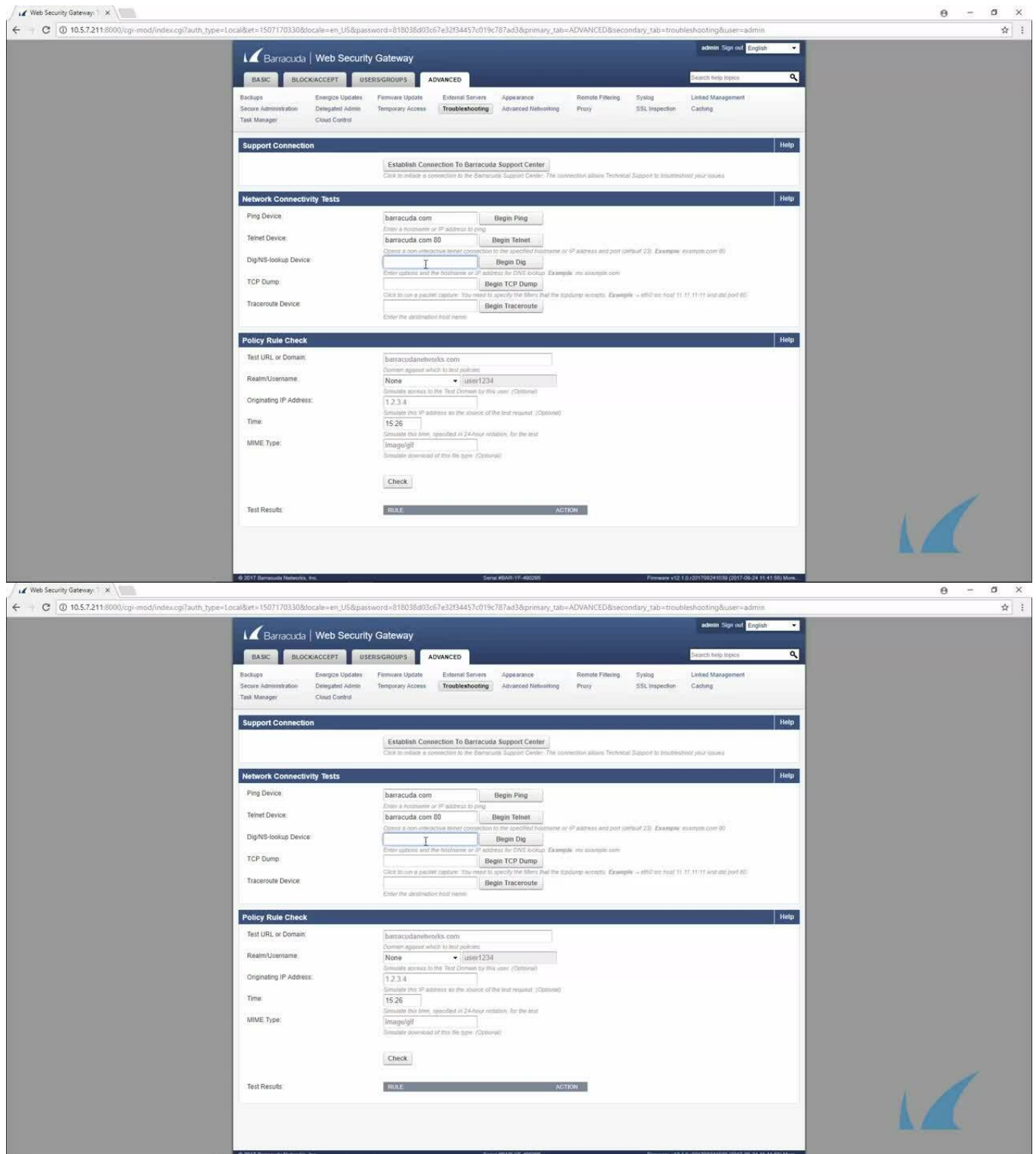
Basic Troubleshooting Tools

The **ADVANCED > Troubleshooting** page provides various tools that help troubleshoot network connectivity issues that may be impacting the performance of your Barracuda Web Security Gateway.

Examples include:

- Test the connection between the Barracuda Web Security Gateway to Barracuda Central to make sure it can successfully download the latest virus and spyware definitions.
- Open a support tunnel to allow Barracuda Networks Support to connect with your appliance and troubleshoot any issues.
- Ping or telnet to devices from the Barracuda Networks appliance.
- Perform a traceroute from the Barracuda Networks system to a destination server
- Run a packet capture
- Test what action the Barracuda Web Security Gateway would take with particular URLs, domains, MIME types, etc. based on block/accept policies and exceptions you create. See [Policy Rule Checking](#).
- Barracuda Networks recommends using the AUX port for management of the Barracuda Web Security Gateway, while the LAN/WAN ports are used for user data and web traffic. The Auxiliary (AUX) port for management of the Barracuda Web Security Gateway is available in all deployment modes.

This video describes how to use the troubleshooting tools available in the Barracuda Web Security Gateway.



The image displays two screenshots of the Barracuda Web Security Gateway interface, specifically the Troubleshooting section. The top screenshot shows the 'Network Connectivity Tests' section, which includes fields for Ping Device, Telnet Device, Dig/NS-lookup Device, TCP Dump, and Traceroute Device. The bottom screenshot shows the 'Policy Rule Check' section, which includes fields for Test URL or Domain, Realm/Username, Originating IP Address, Time, and MIME Type. Both screenshots show the 'Begin' buttons for each test and the 'Check' button for the Policy Rule Check.

Videolink:

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

LDAP Issues

If your LDAP server is slow in responding to search requests, increase the **LDAP Server Timeout** timeout value on the **USERS/GROUPS > Configuration** page. Default is 30 seconds.

Connect to Barracuda Networks Support Servers

In the **Support Diagnostics** section of the **ADVANCED > Troubleshooting** page, you can initiate a connection between your Barracuda Web Security Gateway and the [Barracuda Networks Support](#), which allows technical support engineers to troubleshoot any issues you may be experiencing. See [How to Open a Support Tunnel](#) for details.

Rebooting the System in Recovery Mode

If your Barracuda Web Security Gateway experiences a serious issue that impacts its core functionality, you can use diagnostic and recovery tools that are available at the reboot menu to return your system to an operational state.

Before you use the diagnostic and recovery tools, do the following:

- 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 Barracuda Web Security Gateway and run a memory test or perform a complete system recovery, as described in this section.

To perform a system recovery or hardware (memory) test:

1. Connect a monitor and keyboard directly to your Barracuda Web Security Gateway.
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 Barracuda Web Security Gateway: 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

- Use your keyboard to select the desired boot option, and 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 Barracuda Web Security Gateway starts up in *Normal* mode (first option).
 For a description of each boot option, refer to **Reboot Options** below.

IMPORTANT!

After you start a hardware test, *the test will continue to run until you stop it manually*. To stop a hardware test, reboot your Barracuda Web Security Gateway by pressing the Ctrl-Alt-Del keys.

Reboot options

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

Reboot Options	Description
Barracuda	Starts the Barracuda Web Security Gateway 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: <ul style="list-style-type: none"> • Perform File System Repair — Repairs the file system on XFS, EXT3 and EXT4 based filesystems. Full System re-image should only be done if problems persist after performing a file system repair. Select this option only if the serial number on your Barracuda Web Security Gateway is below 24364; otherwise select the Perform Full System Re-image option. • Perform Full System Re-image — Restores the factory settings on your Barracuda Web Security Gateway and clears out the configuration information. Select this option if the serial number on your Barracuda Web Security Gateway is 24364 or above. • Enable Remote Administration — Turns on reverse tunnel that allows Barracuda Networks Technical Support to access the system. Another method for enabling remote administration is to click Establish Connection to Barracuda Networks Support Center on the ADVANCED > Troubleshooting page. • Run 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. Reboot your Barracuda Web Security Gateway to stop the hardware test.

Replacing a failed system

Before you replace your Barracuda Web Security Gateway, use the tools provided on the **ADVANCED > Troubleshooting** page to try to resolve the problem. In the event that a Barracuda Web Security Gateway system fails and you cannot resolve the issue, see [Replacing a Failed System](#).

Using the AUX Port

The AUX port on the Barracuda Web Security Gateway can be used:

- For management of the device while the LAN/WAN ports are used for user data and web traffic.
- If there is a problem with LAN or WAN port connectivity – that is, if the AUX port is the only port functional on the Barracuda Web Security Gateway, it can be used for Support access to investigate various issues. By default, access via the AUX port is disabled. If you enable AUX port access and enable the Support Tunnel, Barracuda Networks Support can try to connect using the AUX port. To enable AUX port access, see [How to Enable Auxiliary Port Access](#).

Figures

© 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.