

# **Server Connectivity Test**

https://campus.barracuda.com/doc/99616182/

You can use the **Test Connectivity** option on the **Servers** page to check if the server(s) associated with the application is accessible from the Application Security Enforcer (Traffic inspection module). The Barracuda WAF-as-a-Service uses the configured server settings to connect to the backend server.

To run the test separately on each server, click the three dots under **MORE** next to the server and select **Test Connectivity**.

After the completion of the test, the results are displayed under each server (in case of multiple servers). The Barracuda WAF-as-a-Service performs network layer and application layer tests:

- Network connectivity tests are performed using the **SSL** parameters configured in the Server configuration.
- Application connectivity tests are performed using the Health Check parameters configured in the Server configuration.

The server connectivity test is enforced on the server(s) even when **Health Check** is disabled.

The server connectivity test can be used to validate:

- Network connectivity between the Application Security Enforcer and Application Server.
- Application connectivity to check if the connection is established with the configured server.
- SSL parameters such as TLS version, SNI, certificates, etc.
- Health check parameters (Application layer health check).

### **Response Errors and Solutions**

Following are some of the errors and solutions.

### **Error 1: Test Parameters are not Configured**

The following message is displayed when the application layer test is not configured.

Server Connectivity Test 1/5

### Barracuda WAF-as-a-Service





Device Id

Successfully connected to the server 72fbec12-02fe-488c-97fd-18d36bc35a02

Test parameters are not configured



#### Solution

1. Click the **Configure** option and provide the required values.

#### OR

- 2. Click the three dots under **MORE** next to the server and select **Edit Server**.
- 3. On the **Edit Server** window:
  - 1. Select the **HEALTH CHECKS** tab.
  - 2. Specify the URL in the **Request URL** field.
  - 3. Configure other parameters as required and click **Save**.
- 4. Rerun the test.

### Error 2: SSL\_NO\_PROTOCOLS\_AVAILABLE

The error is displayed if the server uses HTTPS protocol and TLS versions are not enabled.



### **Solution:**

- Click the three dots under MORE next to the server and select Edit Server.
- 2. On the Edit Server window:
  - 1. Select the **SSL** tab.
  - 2. Select the TLS versions that are supported by the server.
  - 3. Click Save.
- 3. Rerun the test.

### Error 3: SSLV3\_ALERT\_HANDSHAKE\_FAILURE

The error is displayed when an unsupported TLS version is selected for the server.

Path 2: Failed		Path 2: Failed	
Details	HTTPSConnectionPool(host='52.237.137.230', port=443): Max retries exceeded with url: / (Caused by SSLError(SSLError(1, '[SSL: SSLV3_ALERT_HANDSHAKE_FAILURE] sslv3 alert handshake failure (_ssl.c:1131)')))	Details	HTTPSConnectionPool(host='52.237.137.230', port=443): Max retries exceeded with url: / (Caused by SSLError(SSLError(1, '[SSL: SSLV3_ALERT_HANDSHAKE_FAILURE] sslv3 alert handshal failure (_ssl.c:1131)')))
Device Id	72fbec12-02fe-488c-97fd-18d36bc35a02	Device Id	72fbec12-02fe-488c-97fd-18d36bc35a02

Server Connectivity Test 2 / 5



#### **Solution:**

- 1. Click the three dots under **MORE** next to the server and select **Edit Server**.
- 2. On the **Edit Server** window:
  - 1. Select the **SSL** tab.
  - 2. Select the TLS versions that are supported by the server.
  - 3. Click **Save**.
- Rerun the test.

### Error 4: SSL\_CERTIFICATE\_VERIFY\_FAILED

The error is displayed when certificate validation and SNI is enabled but a wrong SNI domain name is configured or there is a domain mismatch.



### **Solution:**

- 1. Click the three dots under **MORE** next to the server and select **Edit Server**.
- 2. On the **Edit Server** window:
  - 1. Select the **HEALTH CHECKS** tab.
  - 2. Specify the correct domain name in the **SNI Domain** field.
  - 3. Click Save.
- 3. Rerun the test.

### Error 5: Expected status code is 301 and response status code is 200

The error is displayed when the expected status code does not match with the response code.



### **Solution:**

- 1. Click the three dots under **MORE** next to the server and select **Edit Server**.
- 2. On the **Edit Server** window:
  - 1. Select the **HEALTH CHECKS** tab.

Server Connectivity Test 3 / 5



- 2. Specify the correct code in the **Expected Status Code** field.
- 3. Click Save.
- 3. Rerun the test.

### Error 6: Expected string not found in response

The error is displayed when the expected string is not found in the response HTML content.



#### Solution:

- 1. Click the three dots under **MORE** next to the server and select **Edit Server**.
- 2. On the **Edit Server** window:
  - 1. Select the **HEALTH CHECKS** tab.
  - 2. Specify the correct string in the **Expected String in Response** field.
  - 3. Click **Save**.
- 3. Rerun the test.

Server Connectivity Test 4 / 5

## Barracuda WAF-as-a-Service



# **Figures**

- 1. Test Parameters.png
- 2. SSL\_No\_Protocols\_Available.png
- 3. SSLV3\_Alert\_Handshake\_Failure.png
- 4. SSL Certificate Verify Failed.png
- 5. Response Status Code.png
- 6. String Not Found.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.

Server Connectivity Test 5 / 5