Configuring Server Settings

https://campus.barracuda.com/doc/4259867/

A server hosts the actual content for a service. You can configure one or more servers to load balance the incoming web traffic. For information on how to add a server, see How to Add a Real Server. The added server is displayed next to the service or rule group with the default security settings in the **Services** section on the **BASIC > Services** page. To modify the server security settings, click **Edit** next to the server. The **Server Configuration** window appears with the following sections:

- Server (Basic Configuration)
- SSL (Server)
- In Band Health Checks
- Out of Band Health Checks
- Application Layer Health Checks
- Connection Pooling

Server (Basic Configuration)

Edit the basic configuration settings of a server using the Server (Basic Configuration) section.

- **Server Name** – Enter a name to identify the server.
- **IP Address** – Enter the IP address of the server hosting the service.
- **Port** – Enter the port on which the service resides.
- **Status** – Select the status for the server from the drop-down list to handle the requests.
  - *In Service* – Denotes that the requests can be forwarded to the server.
  - *Out of Service All* – Denotes that requests should not be forwarded to the server. Select this if you wish to terminate all connections to the server immediately.
  - *Out of Service Maintenance* – Denotes that requests should not be forwarded to the server. Select this if you wish to take a server out of service for maintenance or software upgrade, etc. In this case, existing connections are terminated only after the requests in progress are completed.
  - *Out of Service Sticky* – This applies only when a **Persistence Method** is selected using **Load Balance** on the **Edit Service** page. If selected, persistent client(s) requests are forwarded to the server.
- **Backup Server** – Set to *Yes* to designate this server as a last resort server to be used when all other servers configured under the service fail.
- **Weight** – Assign a weight for the server. The value indicates the capacity of the server, and is applicable only when the load balancing algorithm is set to weighted round robin (WRR). Requests are passed to servers in the proportion indicated by weight, so the server with the highest weighted round robin (WRR) weight will get the most requests. For example, consider two servers (server1 with weight 50 and server2 with weight 100) for a service. Server1 will get half the number of requests that server2 gets.

SSL for Servers

To configure SSL for communication between the Barracuda Web Application Firewall and the backend servers, see Configuring SSL for Services and Servers.

In-Band Health Checks

Set the threshold to monitor the health of the server. In In-Band health monitoring, the Barracuda Web Application Firewall checks the server connections and responses for any network issue/error that is preventing a client from reaching the intended server. If the server error responses exceed the specified number, the server is marked as out-of-service. Servers in the out-of-service state are disregarded as potential servers for serving content. If other servers are defined to load balance requests, traffic will be routed to the other servers. If only one server is defined, and it is in the out-of-service state, it will result in an error response to the browser.

By default, the counter is reset every 1024 requests. If the number of errors exceeds the respective setting (Max HTTP Errors, Max Refused, Max Timeout Failures, or Max Other Failures) within the 1024 requests, probing stops and the server is marked as out-of-service.

If **Enable OOB Health Checks** is set to *No* in the **Out-of-Band Health Checks** section, the server remains in the out-of-service state and no requests are sent to that server. If set to *Yes*, the server remains in out-of-service state until the next probe is sent after the specified time interval, and a valid response is received from the server.

- **Max HTTP Errors** – Set the maximum number of HTTP error responses to be allowed per 1024 requests before marking the server as out-of-service
- **Max Refused** – Set the maximum number of connection-refused errors to be allowed per 1024 connections before marking the server as out-of-service.
- **Max Timeout Failures** – Set the maximum number of connection time-out errors to be allowed per 1024 connections before marking the server as out-of-service.
- **Max Other Failures** – Set the maximum number of other errors to be allowed per 1024 connections before marking the server as out-of-service.

Out-of-Band Health Checks

Out-of-Band health check is performed at Layer 4 and Layer 7. A periodic probe is sent to check the health of the server. If the server health check fails, the server is marked as out-of-service. The server

continues to be monitored, so if the server health check succeeds, the server's status reverts to in-service. This is unlike In-Band health checks, where the server can only be placed in the out-of-service status, but can never revert because no further user traffic is directed towards an out-of-service server. To send periodic probes to check the health of the server, configure the following:

- **Enable OOB Health Checks** – Set to *Yes* to enable Out-of-Band monitoring. Note that disabling Out-of-Band Monitoring means that if a server is marked as out-of-service by In-Band monitoring, it cannot be put back into service without manual intervention. For this reason, In-Band monitoring is disabled when you disable Out-of-Band monitoring.
- **Interval** – Set the interval (time in seconds) between the probes sent by the Barracuda Web Application Firewall to the server to determine the health status.

- Network Layer probes involve a series of 3 connection attempts within the interval. Application Layer probes involve one HTTP request during the specified interval. This affects how quickly a 'server down' condition will be detected, and also how quickly it will be marked as healthy again.
- HTTP/1.1 for application health check (OOB) is supported.

Application Layer Health Checks

Application Layer health checks involve making an HTTP request to see if the server is responding correctly. If the server responds correctly, the server is said to be healthy. Otherwise, the server is marked as out-of-service. The settings for Application Layer determine what kind of HTTP request is made (URL, method, headers), and how to determine if the response was a good response (status code and match content string).

Application Layer health checks are governed by the Out-of-Band (OOB) module. To enforce the Application Layer health check policy, set **Enable OOB Health Checks** to *Yes*.

To enable Application Layer health check, configure the following fields:

- **URL** – Enter the URL to be used in the HTTP request to determine the server health. A URL such as /index.html is recommended that is always expected to be available, and the unavailability of which can only mean that the server is down.
- **Method** – Select the HTTP method to be used for the request from the drop-down list.
- **Additional Headers** – Enter any additional headers you want to send with the OOB HTTP request. The headers should be specified with the following format: *<header name>: <header value>*. The Barracuda Web Application Firewall inserts the specified headers in the request while sending OOB HTTP requests to the server. Each header should be added on a separate line. For example:

<header1>: <value1>
<header2>: <value2>

- **Status Code** – Specify the expected HTTP response status code when accessing the URL. Any other status code is considered to be unsuccessful, and will result in setting the server as 'out-of-service'. Typically, a status code of 200 is used to indicate a successful response, but in some cases, 300, 301, and 302 may also be considered successful (these status codes indicate redirect responses).
- **Match Content String** – Enter the string that needs to be matched in the response. If specified, the response must contain the string. If the response does not contain the string, the probe is deemed unsuccessful, and the server will be marked out-of-service. This helps detect encode errors in the response page. Note: The strings are case sensitive.
- **Domain** - Enter the SNI domain to be used to access the backend server for Application Level health check. This connection is established only when the field **Enable SNI** is set to “Yes”.

Connection Pooling

For information on connection pooling, see Using Connection Pooling: How and Why.