How to Enable HTTP/2

https://campus.barracuda.com/doc/48660876/

Hypertext Transfer Protocol Version 2 (HTTP/2.0) is an upgraded version of protocol HTTP/1.1. HTTP/2 enables a more efficient use of network resources and reduced latency by introducing header field compression and allowing multiple concurrent exchanges on the same connection. It also introduces unsolicited push of representations from servers to clients. Overall, the goal for designing HTTP/2 was to improve the page load time and user experience. For more information on HTTP/2.0, refer to RFC 7540.

The Barracuda Web Application Firewall supports protocol HTTP/2.0 for front-end as well as back-end connections. When HTTP/2 is enabled for a service, the Barracuda Web Application Firewall and the client use HTTP/2 to communicate with each other. For v11.0 or higher, back-end support for HTTP/2 is also provided. With this support, the server and Barracuda Web Application Firewall can use HTTP/2 to communicate with each other.

Front-End HTTP/2

How the Barracuda Web Application Works when Front-end HTTP/2 Is Enabled for a Service

1. The client sends an HTTP/2 request.
2. The Barracuda Web Application Firewall understands the HTTP/2 protocol and parses HTTP/2 frames as they arrive.
3. The Barracuda Web Application Firewall coverts the HTTP/2 request to a HTTP/1.1 request.
4. The HTTP/1.1 request is passed through the Barracuda Web Application Firewall security modules for inspection and sanitization.
5. After performing security validations, the HTTP/1.1 request is sent to the back-end server. The server responds to the response.
6. The Barracuda Web Application Firewall converts the response to the HTTP/2 format frames and forwards it to the client.

Head-of-Line Blocking

Multiple HTTP/2 streams can be active at any point of time and the Barracuda Web Application Firewall allows clients to establish multiple HTTP/2 streams. When these streams are received, they are separated out into individual HTTP/1 requests and sent to the back-end server using connection pooling. Since the Barracuda Web Application Firewall recognizes that the client is HTTP/2 capable, it does not block if any of the back-end HTTP/1 requests is not complete. Rather, it gathers the responses from the completed HTTP/1 requests and streams them out to the client after converting

them to HTTP/2 streams.

Each of the HTTP/2 stream corresponding to a HTTP request can also be load balanced by the Barracuda Web Application Firewall, and sent to the back-end servers in parallel, assuming persistence settings allow such distribution.

Enabling Front-End HTTP/2 for a Service

It is recommended that you enable HTTP/2 for a service if there are clients that are ready to communicate via HTTP/2 protocol, and need improved user experience and page load performance.

Perform the following steps to enable HTTP/2 for a service:

1. Go to the **ADVANCED > System Configuration** page.
2. In the **Advanced Settings** section, set **Show Advanced Settings** to *Yes*.
3. Go to the **BASIC > Services** page.
4. In the **Services** section, identify the service to which you want to enable HTTP/2.
5. Click **Edit** next to it. The **Service** window appears.
6. In the **Service** window:
    1. Scroll down to the **Advanced Configuration** section.
    2. Set **Enable HTTP2** to *Yes*.
    3. Specify values for other parameters (if required).
    4. Click **Save**.

Back-End HTTP/2

How the Barracuda Web Application Firewall Works when Back-End HTTP/2 Is Enabled

1. If the server supports HTTP/2, then the Barracuda WAF and server negotiate using the HTTP/2 protocol.
2. The Barracuda WAF converts the HTTP 1.1 request to HTTP/2 before sending it to the back-end server.
3. After the request is converted, the HTTP/2 request is passed to the server.
4. The server responds to the request.
5. The Barracuda WAF converts the response from HTTP/2 to HTTP 1.1, and then the response is passed through security modules for inspection and sanitization.

Back-end HTTP/2 is enabled at two levels:

1. Service
2. Server

Enabling Back-End HTTP/2 at the Service Level

Back-end HTTP/2 can be enabled only for SSL services. To enable back-end HTTP/2, the front-end HTTP/2 must be enabled.

1. Go to the **BASIC > Services** page.
2. Identify the service to which you want to enable back-end HTTP/2 and click **Edit** next to it.
3. On the **Service** window, do the following in the **Advanced Configuration** section:
    1. Set **Enable HTTP2** to **Yes**.
    2. Set **Enable Backend HTTP2** to **Yes**.
4. Click **Save**.

Enabling Back-End HTTP/2 at the Server Level

You can enable HTTP/2 for the server(s) that support HTTP/2 protocol.

1. Go to the **BASIC > Services** page.
2. Identify the server to which you want to enable back-end HTTP/2 and click **Edit** next to it.
3. On the **Server Configuration** window, do the following:
    1. In the **SSL** section, set **Enable HTTP2** to **Yes**.
    2. In the **Connection Pooling** section, set **Enable Connection Pooling** to **No**.
4. Click **Save**.

- Before enabling HTTP/2 for the server, make sure you disable the **Connection Pooling** option.
- Make sure you always select the server as SSL for HTTP/2 back-end connections to work.
- Make sure that all the servers have HTTP/2 enabled for back-end connections to work.
- When the server is added to HTTP/2 enabled service, make sure it supports HTTP/2 protocol.

The initial request is upgraded to HTTP/2 by the Barracuda WAF using the TLS extension Application-Layer Protocol Negotiation (ALPN). Therefore, it is required to disable the other upgrade mechanism, which is HTTP response header-based. This can be achieved by creating a web translation rule on the Barracuda WAF.

Add a **HTTP Response Rewrite** rule on the **WEBSITES > Website Translations** page to remove the **Upgrade** header for **h2,h2c** for the service that has the back-end HTTP/2 enabled. Configure the following values in the HTTP Response Rewrite rule:

- **ACTION** - Remove header
- **HEADER NAME** - upgrade
- **OLD VALUE** - h2,h2c
- **REWRITE VALUE** - *