

How to Pass Client Certificate Details to a Backend Server

<https://campus.barracuda.com/doc/4259847/>

This article applies to the Barracuda Web Application Firewall 460 or higher.

You can configure the Barracuda Web Application Firewall to pass information from a client to the backend server through the Barracuda Web Application Firewall. Using this feature, web servers can access client authentication information like client certificate parameters or authenticated username and password.

On the Barracuda Web Application Firewall, you can add client information to a request by configuring a request rewrite. Headers can be inserted into the request, or existing headers can be rewritten or deleted before passing the request to the web server, which can then extract the added information. The Barracuda Web Application Firewall provides macros you can use to communicate request parameters like client certificate details or authenticated user information through headers.

Configure Request Rewrite to Pass Client Information to a Web Application

To configure a request rewrite rule, perform the following steps:

1. Go to the **WEBSITES > Web Site Translations** page, and in the **HTTP Request Rewrite** section specify values for the following fields:
 - **Rule Name** - Enter a name for the request rewrite rule.
 - **Sequence Number** - Set the sequence number for the request rewrite policy. The sequence number determines the order of execution for multiple configured policies from highest (1) to lowest (1500).
 - **Action** - Select the action. To modify client information sent to the web application, the request rewrite action should be set to **Insert Header** or **Rewrite Header**.
 - **Header Name** - Enter the relevant header name, for example, X-Forwarded-For.
 - **Old Value** - Enter the initial request header to be rewritten if the Action is **Rewrite Header**. An asterisk (*) rewrites all named headers, or specify the value or expression to be rewritten.
 - **Rewrite Value** - Enter the new value of the header to be rewritten when the **Action** is set to **Insert Header** or **Rewrite Header**. Use the macros listed below to specify parameters from the client. When rewriting a header, you can specify one or more fields using the separators such as colon (:), semicolon (;), space () and comma (,). In Rewrite Value, the fields can be defined for example: "Name=abc_cookie; Domain=example.com:Path=/". The rewrite-value supports substring addressing of matches, i.e., the matching substrings can be referenced using \$1,\$2,...\$n. The following macros are supported for rewrite values:
 - **\$X509_ORGANIZATION, \$X509_LOCALITY, \$X509_CN, \$X509_COUNTRY,**

\$X509_OU, \$X509_STATE, \$X509_EMAIL, \$X509_SUBJECT, \$X509_WHOLE, \$X509_ISSUER: Fields in the X.509 client certificate when client authentication is **On**.

- **\$SRC_ADDR:** The client IP from which the request originated.
- **\$DST_ADDR:** The destination address.
- **\$URI:** URI.
- **\$AUTH_USER:** Username of the authenticating user.
- **\$AUTH_PASSWD:** Password of the authenticating user.
- **\$AUTH_GROUPS:** Group associated to the authenticating user.
- **Rewrite Condition** – Set the condition under which a rewrite should occur. An asterisk (*) indicates there are no conditions (applies to all). Details on the format of the Rewrite Condition are explained below in [Rewrite Condition Format](#).

2. Click **Add** to add the above settings.

Note: When multiple policies are configured, the request continues to be processed by other (higher sequence number) policies. To stop processing after a particular rule is matched, click **Edit** next to the rule and set **Continue Processing** to **No**.

Rewrite Condition Format

The request **Rewrite Condition** specifies when a rewrite should occur. The **Rewrite Condition** is made up of expressions combining [Request Rewrite Tokens](#) and [Operations](#) on those tokens. These expressions can then be joined with each other using logical or (or, OR, ||) or logical and (and, AND, &&). Examples of **Rewrite Conditions**: (Header User-Agent co mozilla) , (URI rco /abc*html), (Client-IP eq 10.0.0.1)&&(Method eq POST). An asterisk indicates there are no conditions for rewrite, so the rewrite is done in every case.

© Barracuda Networks Inc., 2020 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.