Access Control

Feature Availability

This article applies to the Barracuda Load Balancer ADC 540 and above, version 5.1 and above, and to all Barracuda Load Balancer ADC models in version 5.2 and above.

On the Barracuda Load Balancer ADC 340 and above, you can integrate external authentication servers and configure authorization policies to control the access of end users to your web applications. LDAP, RADIUS, and Kerberos authentication protocols are supported.

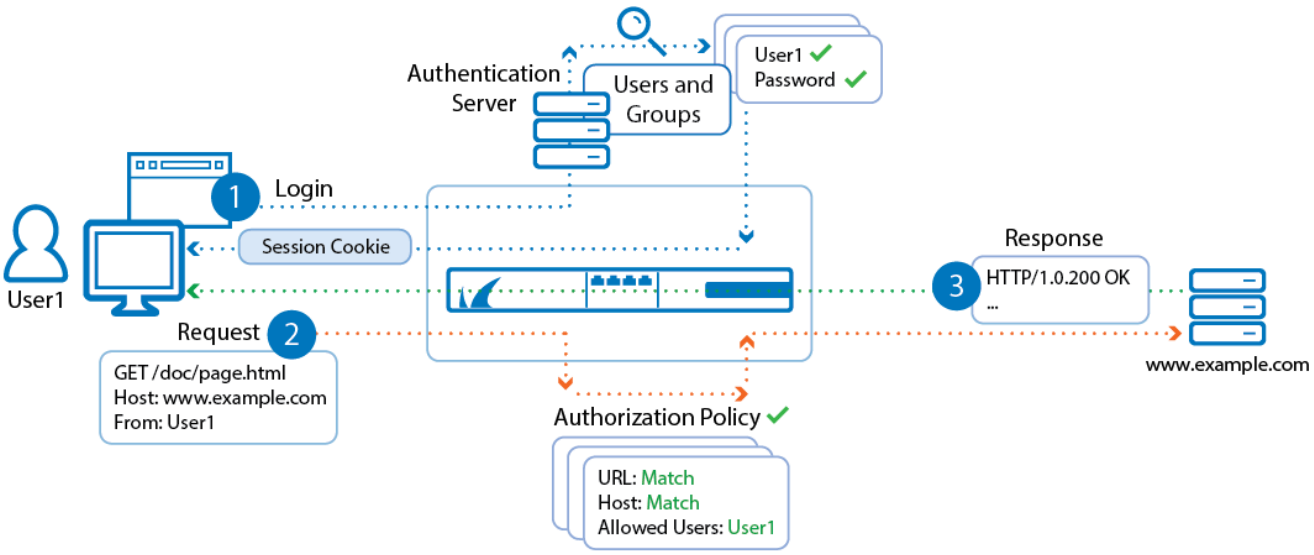
Overview of Access Control

To access resources from an application, end users must:

1. Provide a username and password for validation by an authentication server that has been integrated for the service of the application.
2. Have access privileges from an authorization policy that has been configured for the service of the application.

After users submit their initial request to the application, they must complete and submit a login form with a valid username and password. The Barracuda Load Balancer ADC compares the submitted information with information from the external authentication server. If two-factor authentication is configured, users are also redirected to a challenge page to enter the additional credentials (e.g., PIN or passcode). Users who fail authentication are redirected to a page that notifies them that they have failed authentication. Successfully authenticated users receive a cookie and are redirected to a page that notifies them that they have been authenticated.

Any requests from authenticated users must then be allowed by an authorization policy. When the Barracuda Load Balancer ADC receives a request, it compares the request to all authorization policies. Policies are matched to requests by URL, host, and other expressions. Policies also contain lists of allowed and restricted users and groups. If a matching policy lets the user access the requested resource, the Barracuda Load Balancer ADC forwards the request to the application server. If a matching policy does not allow the user to access the requested resource, the user is redirected to a denied authorization page.



Configuring Access Control

For instructions on configuring access control and options such as single sign-on, custom login pages, and two-factor client authentication with SMS PASSCODE®, see these articles:

Figures