SAML Authentication

https://campus.barracuda.com/doc/42047827/

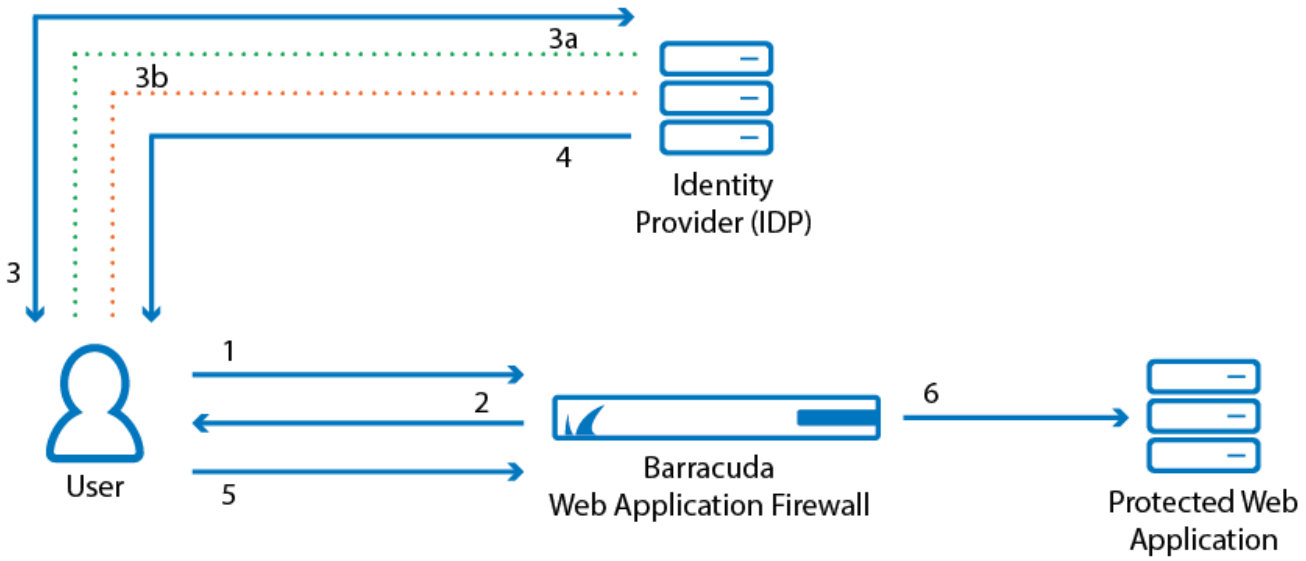
The Barracuda Web Application Firewall supports Security Assertion Markup Language (SAML) 2.0, which provides federated authentication and authorization across different domains. The data is exchanged between three main entities called User/Principal, Service Provider (SP), and Identity Provider (IDP).

- **User** – A user who attempts to access a secure domain.
- **Service Provider (SP)** – A service provider is an entity that hosts web applications, and relies on trusted Identity Providers (IDPs) to authenticate users. The SP authorizes users accessing the web applications based on the configured access rules.
- **Identity Provider (IDP)** – An IDP is a service/website that certifies the identities of users by means of security tokens.

In the SAML environment, the Barracuda Web Application Firewall can act as the SAML Service Provider (SP) that relies on the configured Identity Providers (IDPs) to authenticate users. The Identity Provider (IDP) authenticates the user and issues security tokens (XML assertions with attributes) to the Barracuda Web Application Firewall. The Barracuda Web Application Firewall authorizes users accessing the secure web application based on the attributes configured in the access rules. The user is granted access to the secure web application *only* if the attribute(s) and their values are matched successfully.

Single sign-on (SSO) is a mechanism where a single set of user credentials is used for authentication and authorization to access multiple applications across different web servers and platforms, without having to re-authenticate.

How SAML SSO Works



1. User sends a request to a web application.
2. The Barracuda Web Application Firewall identifies that the web application is protected by SAML authentication service, and redirects the request to the user.
3. The user's browser redirects the user to the IDP server for authentication.
    1. The IDP server challenges the user to provide the login credentials.
    2. The user enters the credentials.
4. If the user is authenticated, the IDP sends the SAML assertions to the user.
5. The user forwards the assertions to the Barracuda Web Application Firewall using the POST method. The Barracuda Web Application Firewall validates the assertions.
6. If successful, the user is granted access to the requested web application. If any access rule is configured, the Barracuda Web Application Firewall authorizes the user by matching the request with specified attributes in the access rule. If successful, the user is granted access to the requested web application. If not, the Barracuda Web Application Firewall redirects the user to the Access Denied page.

To enable SAML authentication for a service on the Barracuda Web Application Firewall, perform the following steps:

1. Configure SAML on the Barracuda Web Application Firewall
2. Configure Identity Provider (IdP)

Figures

© 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.