Back-end SSL Server Configuration

https://campus.barracuda.com/doc/4259900/

To use SSL encryption between the Barracuda Web Application Firewall and a server, **Edit** the server from the list of servers in the **BASIC > Services** list and set **Server uses SSL** to *Yes* in the SSL (Server) section. The Barracuda Web Application Firewall can validate the server certificate using trusted certificates. If the server provides a self-signed certificate, **Validate Server Certificate** should be *No*. You can also configure a client certificate for the service to present to the server. This certificate configuration is needed if the server requires client authentication, because the service acts as a client to the back-end server when it forwards requests. Online help provides more detailed instructions for configuring these settings.

SSL for Barracuda Web Application Firewall to Server Transmissions

The Barracuda Web Application Firewall also provides server-side encryption, and can provide a certificate to the servers for client authentication (the Barracuda Web Application Firewall acting as the client to the back-end servers). This protects services configured on the Barracuda Web Application Firewall. The client-server negotiations include the following:

- The Barracuda Web Application Firewall receives and verifies the real server's certificate.
- The Barracuda Web Application Firewall may provide a certificate in return if client authentication is required by the back-end server.

The SSL handshake allows the server and the Barracuda Web Application Firewall to authenticate each other. Once mutually authenticated, both use keys for encryption, decryption, and tamper detection during the SSL sessions.

To configure the Barracuda Web Application Firewall to use SSL in Server communications, add a **Server** for the respective service on the **BASIC > Services** page using the **Add** column, and configure the Barracuda Web Application Firewall to validate the server certificate. For more information on client certificates, refer to How to Use Client Certificates.

© Barracuda Networks Inc., 2024 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.