Secured Message Transmission

https://campus.barracuda.com/doc/3211266/

If you make setting changes, allow a few minutes for the changes to take effect.

To prevent data leakage and ensure compliance with financial, health care and other federally-regulated agency information policies, the Barracuda Email Security Service provides several types of encryption for inbound and outbound message traffic.

Send Messages Over an Encrypted Channel

TLS provides secure transmission of email content, both inbound and outbound, over an encrypted channel using the Secure Sockets Layer (SSL).

To require mail to be sent *outbound* from the Barracuda Email Security Service over a TLS connection, you can enable **Force TLS** for each domain on the **Outbound Settings > DLP/Encryption** page. Mail sent to these domains must be transmitted across a TLS connection. If a TLS connection cannot be established, then the mail will not be delivered.

To require mail coming *inbound* to Email Gateway Defense to use a TLS connection, use the **SMTP Encryption** section on the **Domains > Edit Settings** page for each domain.

- Select **Required** for **Use TLS from Barracuda to your mail server(s)** to send inbound mail over a TLS connection if TLS is available on your organization's mail server. If TLS is not available, mail is sent in cleartext.
- Use the **Require TLS to Barracuda from these domains** list to require a TLS connection from certain domains to Barracuda. You can manually add specific domains one at a time or use the **Bulk Edit** button.

Outbound Mail Encryption

For guaranteed message encryption and ensured delivery of outbound messages, use the **Barracuda Message Center** to encrypt the contents of certain outbound messages. You can create policies for when to encrypt outbound messages on the **Outbound Settings > Content Policies** page for a domain. For details about using encryption with the Barracuda Message Center, see How to Use Encryption of Outbound Mail. For end-users, see the Barracuda Message Center User's Guide.

© 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.