Encryption of Outbound Mail

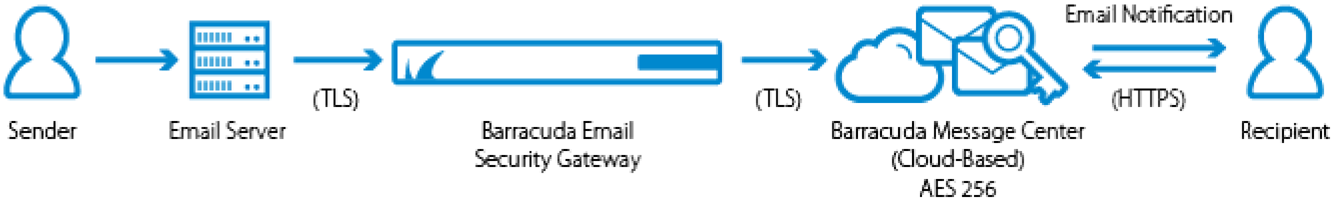
https://campus.barracuda.com/doc/11141444/

Overview

For health care providers, governmental agencies and other entities who need to protect private, sensitive and valuable information communicated via email, the Barracuda Email Security Gateway allows creating multiple policies to specify exactly which outbound emails to encrypt. Emails that match policy are securely (via TLS) sent to the Barracuda Message Center.

Encryption is configured at the per-domain level, but actual encryption policy (by sender domain, email address, recipient, etc.) is only configurable at the global level using the **BLOCK/ACCEPT** pages. These global encryption policies will apply to all domains from which encrypted email messages are sent.

Figure 1: The sender's email is encrypted by the Barracuda Email Encryption Service, then stored at the Barracuda Message Center for retrieval.


Sender
Email Server
(TLS)
Barracuda Email Security Gateway
(TLS)
Barracuda Message Center (Cloud-Based) AES 256
Email Notification
(HTTPS)
Recipient

Encrypting Messages From the MS Outlook Client

You can download the **Barracuda Outlook Add-In** for your Microsoft Exchange Server to enable users to choose encryption from the **New Message** window in their MS Outlook client. See the Barracuda Email Security Gateway Outlook Add-In Deployment Guide or the **USERS > User Features** page in the Barracuda Email Security Gateway web interface for information on deploying the Outlook Add-In. For details about sending and retrieving encrypted messages as applies to this add-in, see steps 4-6 of **Sending and Receiving Encrypted Messages** below.

Secured Message Contents

When the Barracuda Email Security Gateway encrypts the contents of a message, the *message body will not be displayed* on the **BASIC > Message Log**, **BASIC > Outbound Quarantine**, or the **ADVANCED > Queue Management** pages.

Encryption Privacy

Only the sender of the encrypted message(s) and the recipient can view the body of a message encrypted by the Barracuda Email Encryption Service. For Mail Journaling and the download features in the Message Viewer, the message body will not be sent to the Mail Journaling account and cannot be downloaded to the Desktop.

If you already have an email encryption server or service, you can specify a hostname (FQDN) or IP address and port in the **Redirection Mail Server TCP/IP Configuration** section of the **BASIC > IP Configuration** page to which the Barracuda Email Security Gateway should redirect outbound mail for encryption. You can then select the *Redirect* action for outbound filtering policies in the **BLOCK/ACCEPT** pages. Redirection of outbound mail per policy is only available at the global (not per-domain) level.

Configuring and Using Encryption

To get started enabling and configuring encryption and encryption policies, please see How to Use DLP and Encryption of Outbound Mail.

Archiving Encrypted Emails

If you have a Barracuda Message Archiver, you can choose to archive encrypted emails and replies to those emails. From the **BASIC > Administration** page, enter the IP address of the Barracuda Message Archiver in the **Email Encryption Service** section. Note that encrypted messages are *not* sent in encrypted format to the Barracuda Message Archiver. It is recommended that this email traffic from the Barracuda Email Security Gateway to the Barracuda Message Archiver be sent over internal networks.

Requirements for Using Encryption

Before applying encryption policy, make sure of the following:

- Your Energize Updates subscription is current. See the Subscription Status section on the **BASIC > Dashboard** page of the Barracuda Email Security Gateway.
- You validate all sending domains that are allowed to send encrypted messages, using the **DOMAINS > Manage Domain > ADVANCED > Encryption** page. Several validation methods are available from this page.

Setting Encryption Policy for Outbound Mail

From the **BLOCK/ACCEPT** pages you can create global custom encryption policy for secure transmission of outbound mail based on:

- Sender email address and/or domain
- Recipient email address and/or domain
- Attachment Filename pattern and/or type as well as attachment content
- Content and content type (such as, for example, secured credit card info.)

These policies will apply for ALL domains from which you send encrypted email.

Branding

You can brand encryption notification emails (see **Sending and Receiving Encrypted Messages** below) as well as encrypted messages with an image and a domain name to be displayed with the image. Once you have validated a domain through the Barracuda Email Security Gateway, branding is configured at the per-domain level on the **ADVANCED > Encryption** page where you can upload an image from your local drive or network. You can optionally create custom text or html notification message content and subject from the same page.

Encryption and Quarantine, Blocking and Queuing

If an encrypted message is quarantined, the administrator will not see the message contents, but can view the message header information and the reason the message was encrypted as well as the reason it was quarantined on the **BASIC > Message Log** page. From either the **BASIC > Message Log** page or the **BASIC > Outbound Quarantine** page, the message can be delivered, rejected, deleted or forwarded.

If an encrypted message is blocked due to policy, the administrator will not see the message contents, but can view the message header information and the reason the message was encrypted as well as the reason it was blocked on the **BASIC > Message Log** page. The administrator can then deliver the message if desired.

For encrypted messages in the queue, the administrator will not see the message contents but can view the message header information and why the message was encrypted. From the **ADVANCED > Queue Management** page, the administrator can deliver, re-queue or delete the message.

Sending and Receiving Encrypted Messages

The Barracuda Message Center provides a web-based email client for recipients to manage email messages encrypted and sent via the Barracuda Email Security Gateway. The email client looks and behaves much like any web-based email program. See Barracuda Message Center User's Guide for details on the user experience.

For organizations such as credit card companies, for example, that do not wish recipients to reply to encrypted messages, the **Allow Replies** option can be set to *No* on the **ADVANCED > Encryption** page.

The workflow for email encryption is as follows:

1. The administrator creates a filter from one or more of the **BLOCK/ACCEPT** pages to encrypt certain types of outbound messages.
2. Outbound messages that meet this filtering criteria are sent over a secure TLS channel to the Barracuda Message Center for encryption.
3. The outbound message information appears in the Barracuda Email Security Gateway Message Log, but the message body does not, as it is encrypted for security purposes.
4. The Barracuda Message Center sends a notification to the recipient of the email message that includes a link the recipient can click to view and retrieve the message from the Barracuda Message Center. Notifications can be branded as described above.
5. The first time the recipient clicks this link, the Barracuda Message Center will prompt for creation of a password. Thereafter the recipient can re-use that password to pick up subsequent encrypted messages.
6. The recipient logs into the Barracuda Message Center and is presented with a list of email messages, much like any web-based email program. All encrypted messages received will appear in this list for a finite retention period or until deleted by the recipient.

When the recipient replies to the encrypted email message, the response will also be encrypted and the sender will receive a notification that includes a link to view and retrieve the message from the Barracuda Message Center.

Recalling Encrypted Messages

The **Admin** or **Domain Admin** roles can choose to recall an encrypted message before it is read by the recipient. From the **BASIC > Message Log** page, clicking on the message brings up the **Message Viewer**, which includes a **Recall** button if the message has been encrypted. Clicking this button recalls the message from the Barracuda Message Center under the following conditions:

- The recipient has not yet read the message.
- The Remove Barracuda Headers feature is set to *No* on the **ADVANCED > Email Protocol** page.

If the message is recalled, the **Delivery Status** for the message in the log will change to **Recalled**.

Figures