How to Use DLP and Encryption of Outbound Mail

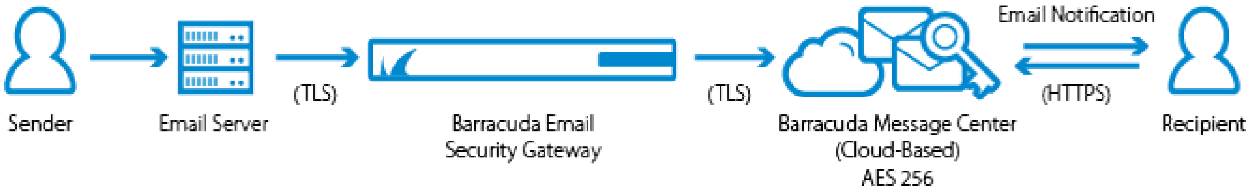
https://campus.barracuda.com/doc/24216158/

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 includes DLP (Data Loss Prevention) features. DLP enables your organization to satisfy email compliance filtering for corporate policies and government regulations such as HIPAA and Sarbanes-Oxley.

Advanced content scanning is applied for keywords inside commonly used text attachments, as well as email encryption. Configure email encryption per domain on the **DOMAINS > Manage Domain > ADVANCED > Encryption** page. DLP/Encryption is included with your Energize Updates subscription.

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.

Encryption is performed by the Barracuda Email Encryption Service, which also provides a web interface, the Barracuda Message Center, for recipients to retrieve encrypted messages.


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

When the Barracuda Email Encryption Service encrypts the contents of a message, the *message body will not be displayed* in the **Message Log**. Only the sender of the encrypted message(s) and the recipient can view the body of an encrypted message. For more information about privacy, please see the Barracuda Networks Privacy Policy.

Workflow for Creating, Sending and Receiving Encrypted Messages

Step 1: Configure Encryption for Selected Domains

1. Begin by confirming that you Barracuda Email Security Gateway can communicate with the Barracuda Email Encryption Service. If you are running version 6.0 or higher, from the **BASIC > Administration** page, enter a valid test email address in the **Email Encryption Service** section and use the **Test Encryption Connection** button. If you

are running 5.1.x, navigate to the **BASIC > IP Configuration** page and, in the **Encryption Service Test** section, enter a valid test email address and use the **Test Encryption Connection** button.
2. If you are running version 6.0 or higher, and 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.
3. Make sure that your **Energize Updates** subscription is current. See the **Subscription Status** section on the **BASIC > Dashboard** page of the Barracuda Email Security Gateway.
4. 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 and are detailed in the Help page.
5. Add the following to the SPF (Sender Policy Framework) record for domains protected by the Barracuda Email Security Gateway:
   ```
    include:spf.ess.barracudanetworks.com
   ```
   This ensures validation of the header FROM address by the recipient, avoiding failures with DMARC, a domain-based message authentication system.

Step 2: Create Policies for DLP/Encryption of Outbound Messages

The administrator creates one or more filters for *outbound* mail from the **BLOCK/ACCEPT** pages, selecting *Encrypt* as the **Action**. Note that, though encryption is configured at the per-domain level, actual encryption policy (by sender domain, email address, recipient address, attachment filename patterns, message content, etc.) is only configurable at the global level. These global encryption policies will apply to all domains from which encrypted email messages are sent. In addition to criteria mentioned above, you can select the *Encrypt* action for outbound email messages that contain matches to pre-made patterns in the subject line, message body or attachment. Use the **Predefined Filters** on the **BLOCK/ACCEPT > Content Filtering** page to configure the following pre-defined data loss patterns (specific to U.S. - see Note below) to meet HIPAA and other email security regulations:

- **Credit Cards** - Messages sent through the Barracuda Email Security Service containing recognizable Master Card, Visa, American Express, Diners Club or Discover card numbers will be subject to the action you choose.
- **Social Security** - Messages sent with valid social security numbers will be subject to the action you choose. U.S. Social Security Numbers (SSN) must be entered in the format nnn-nn-nnnn.
- **Privacy** - Messages will be subject to the action you choose if they contain two or more of the following data types, using common U.S. data patterns only: credit cards (including Japanese Credit Bureau), expiration date, date of birth, Social Security number, driver's license number, street address, or phone number. Phone numbers must be entered in the format `nnn-nnn-nnnn` or `(nnn)nnn-nnnn` or `nnn.nnn.nnnn` .
- **HIPAA** - Messages will be subject to the action you choose if they contain TWO of the types of items as described in Privacy above and ONE medical term, or ONE Privacy item, ONE Address and ONE medical term. A street address can take the place of Privacy patterns. So, for example, a U.S. Social Security Number (SSN), an address, and one medical term is enough to trigger the

HIPAA filter.

The format of this data varies depending on the country, and these filters are more commonly used in the U.S.; they do not apply to other locales. Because of the millions of ways that any of the above information can be formatted, a determined person will likely be able to find a way to defeat the patterns used. These filter options are no match for educating employees about what is and is not permissible to transmit via unencrypted email.

If you use the **Predefined Filters** on the **BLOCK/ACCEPT > Content Filtering** page of the Barracuda Email Security Gateway, and you have a problem with the credit card filter taking action with spreadsheet files that do NOT contain credit card numbers, please see How to Use DLP Filters With Spreadsheets.

Archiving Encrypted Messages

You can choose to archive all encrypted correspondence for your validated domains on the Barrracuda Email Security Gateway to your Barracuda Message Archiver. Enable this feature by entering the IP address of your Barracuda Message Archiver in the **Email Encryption Service** section of the **BASIC > Adminstration** page of the Barracuda Email Security Gateway. For more information, see Archiving Encrypted Email Messages.

Port 4234 should be open for transmission of encrypted mail to the Barracuda Message Archiver.

Step 3: Sending and Receiving Encrypted Messages

The **Barracuda Message Center** is a web-based email client for receiving and managing encrypted email sent by the Barracuda Email Security Service or the Barracuda Email Security Gateway. The email client looks and behaves much like any web-based email program. For a user's guide, please see Barracuda Message Center User's Guide. The workflow for sending and receiving encrypted messages is as follows:

1. Outbound messages that meet this filtering criteria and policies configured as described above are encrypted and appear in the **Message Log**, but the message body does not appear in the log for security purposes.
2. 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.
3. 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.

4. 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.

Figures