How to Route Outbound Mail from the Barracuda Email Security Gateway

https://campus.barracuda.com/doc/3866676/

Barracuda Networks recommends reading About Scanning of Outbound Mail before proceeding.

- If you are using Google Workspace Business and Education editions with the Barracuda Email Security Gateway as your outbound mail gateway, see How to Configure Google Workspace for Inbound and Outbound Mail in addition to reading this article.
- If you are deploying the Barracuda Email Security Gateway on Amazon Web Services, see Routing Mail Through AWS in addition to this article.

You can relay outbound mail through the Barracuda Email Security Gateway simultaneously with scanning inbound mail, where outbound mail will be subject to the same spam and virus scanning and, for the most part, the same custom policy as inbound mail with some exceptions.

The following scanning tools are not applied to outbound mail:

- IP Reputation, a sender authentication mechanism
- SPF (Sender Policy Framework), a sender authentication mechanism
- DKIM (DomainKeys), an email authentication system designed to verify the DNS domain of an email sender
- Per-user Allow List/Block List
- Per-domain Allow List/Block List

To relay outbound mail to the Barracuda Email Security Gateway:

In most cases, the only thing that needs to be done is to enter the IP address of the outgoing mail server or other trusted relay server in the **Relay Using Trusted IP/Range** field on the **BASIC > Outbound** page, as described in **Simple configuration of outbound relay of mail** below. Outbound mail is scanned for spam, as is inbound mail, as well as filtered for policies you create from the **BLOCK/ACCEPT** filtering pages.

If you need to configure additional options for outbound relay, click the **Help** button on the **BASIC > Outbound** page.

Simple configuration of outbound relay of mail

1. Configure your mail server to relay outbound mail to the Barracuda Email Security Gateway. If

you have a Microsoft Exchange Server, enter your Smart host IP address in the next step and configure the Smart host on your mail server to relay outgoing mail to the Barracuda Email Security Gateway.

2. Enter the IP address or host/domain name of your default mail server or another trusted relay server that can relay outbound mail through the Barracuda Email Security Gateway to the Internet. Use the **Relay Using Trusted IP/Range** and/or the **Relay Using Trusted Host/Domain** fields.

   To protect your system against domain spoofing, it is strongly recommended to use IP addresses and NOT domain names for specifying Trusted Relays. As such, it is recommended to specify your mail server and/or trusted outbound relay servers in the **Relay Using Trusted IP/Range** field as opposed to specifying a host/domain name

   However, if you are using the **Relay Using Trusted Host/Domain** field, it is recommended to configure either SMTP AUTH or LDAP authentication on this page as well.
   Note that LDAP Routing is available on the Barracuda Email Security Gateway 600 and higher, configurable on the **ADVANCED > LDAP Routing** page.
   If using your default mail server to relay outbound mail through the Barracuda Email Security Gateway, enter the IP address of your **Destination Mail Server** as specified on the **BASIC > IP Configuration** page or in the **DOMAINS > Manage Domain > BASIC > IP Configuration** page per-domain setting.
   The following steps cover additional options for outbound relay:
3. To configure the Barracuda Email Security Gateway to relay outgoing mail through your normal outbound SMTP host or Smart host to the Internet, enter the IP address or hostname and TCP port in the **Outbound SMTP Host/Smart Host** fields. This is the destination server through which outbound email will be sent from the Barracuda Email Security Gateway for routing to the Internet, and whose IP address will appear in the outgoing mail headers.
4. Barracuda Networks recommends enforcing use of a secure TLS connection to send mail through the Barracuda Email Security Gateway (inbound and outbound) for all domains. To do so, set **Force TLS** to *Yes.* SMTP over TLS/SSL defines the SMTP command STARTTLS. This command advertises and negotiates an encrypted channel with the peer for this SMTP connection. This encrypted channel is only used when the peer also supports it.
5. To authenticate senders of outbound email, specify the authentication type in the **Enable SASL/SMTP Authentication** field. (SASL is the Simple Authentication and Security Layer, a method for adding authentication support to connection-based protocols. To use SASL, a protocol includes a command for identifying and authenticating a user to a server and for optionally negotiating protection of subsequent protocol interactions.)
   - **SMTP AUTH Proxy** - SMTP AUTH/SASL authentication enables the SMTP *AUTH* command to authenticate users before allowing them to relay outgoing mail through this Barracuda Email Security Gateway. Either set **Use Destination Mail Server as SMTP AUTH Proxy** to *Yes,* or fill in the IP address of another proxy server that is set up to support the SMTP *AUTH* authentication command (e.g. MS-Exchange or Sendmail) to authenticate senders of outbound mail. To use this authentication method, you must also enable *Use name and password* or a similar option in your email client. Also, since the password transmits in cleartext, Barracuda Networks strongly recommends secure transmission by enabling **SMTP over TLS** on the **ADVANCED > Email Protocol** page on the Barracuda Email Security Gateway. **NOTE**: If you enable SSLv3, you must also set TLSv1.0 to *Yes* if you want the Barracuda Email Security Gateway to talk over TLSv1.0, TLSv1.1, or

TLSv1.2.

- **LDAP** - Use your LDAP directory to authenticate senders. Fill in the LDAP settings as described in the **Relay Using Authentication** on the **LDAP** tab. See also LDAP Error Codes.

  IMPORTANT: The Barracuda Email Security Gateway integrates with other systems and services in your environment, like your LDAP server and mail servers. Barracuda Networks recommends creating separate service accounts for these integration points, rather than personal accounts, and then using the principle of least privilege. This integration strategy is part of an overall security policy. For more information, see Security for Integrating with Other Systems - Best Practices.

6. To limit outbound relay capability to certain users or domain names, enter them in the **Senders With Relay Permission** field. To prevent against domain spoofing, *Barracuda Networks strongly recommends not specifying sender email address or domain names* that can relay outbound mail through the Barracuda Email Security Gateway. Use this setting *only* for trusted senders, and note Barracuda Networks recommends using one of the sender authentication methods described above as well for added security.

Basic Outbound/Relay Settings

- **Outbound SMTP Host** (Smart host) - The IP address or host name of the destination server through which outbound email will be sent from the Barracuda Email Security Gateway for routing to the Internet, and whose IP address will appear in the outgoing mail headers.
- **Port** - The TCP port of your SMTP host or Smart host through which you want to relay outbound mail.
- **Username** - Only necessary if required for authentication with the SMTP host or Smart host.
- **Password** - Only necessary if required for authentication with the SMTP host or Smart host. IMPORTANT: As noted above, Barracuda Networks recommends creating separate service accounts for integration points, rather than personal accounts, and then using the principle of least privilege. For more information, see Security for Integrating with Other Systems - Best Practices.
- **Force TLS** - (Barracuda Networks recommends): Set to *Yes* if you want to enforce using a secure TLS connection for all mail leaving the Barracuda Email Security Gateway (inbound and outbound). SMTP over TLS/SSL defines the SMTP command STARTTLS. This command advertises and negotiates an encrypted channel with the peer for this SMTP connection. This encrypted channel is *only* used when the peer also supports it. To select which TLS versions the Barracuda Email Security Gateway supports, configure the **Supported SSL Protocols** setting on the **ADVANCED > Secure Administration** page.

To configure relay using authentication and other relay options, click the **Help** button on the **BASIC > Outbound** page.

Advanced Routing of Outbound Mail

If you want outbound email go to through a specific host before final routing to the Internet and/or default MX records, you can specify that SMTP server on the **DOMAINS > Smart Hosts** page.

Example: You might want all emails to **gmail.com** to go through an additional virus scanning service or cloud-hosted relay service.