About Scanning of Outbound Mail

https://campus.barracuda.com/doc/3866688/

The Barracuda Email Security Gateway may be configured to scan outgoing mail simultaneously with scanning inbound mail. Virus Scanning and Rate Control are applied to outbound mail as well as the following filters, if specifically enabled, which are configurable from the **BASIC > Spam Checking** and **BLOCK/ACCEPT** pages:

- Spam Scoring, with Block or Quarantine actions
- IP Address Filtering
- Sender Domain Filtering
- Sender Email Address Filtering
- Recipient Filtering
- Content Filtering (Subject, Header and Body)
- Attachment Filtering
- Fingerprint Analysis
- Image Analysis
- Intent Analysis

The following scanning tools are not applied to outbound mail:

- SPF (Sender Policy Framework), a sender authentication mechanism
- DKIM (DomainKeys), an email authentication system designed to verify the DNS domain of an email sender
- Regional Settings, the application of special spam analysis rules for particular languages
- Per-user Allow List/Block List
- Per-domain Allow List/Block List
- IP Reputation checks

These are the policies that can be applied to outbound mail using the **BLOCK/ACCEPT** pages:

- Encryption (see Encryption of Outbound Mail)
- Quarantine (see Managing Outbound Quarantine)
- Block
- Redirection

To scan outgoing mail with the Barracuda Email Security Gateway, you must configure outbound operation on the **BASIC > Outbound** page (see How to Route Outbound Mail from the Barracuda Email Security Gateway). There you'll specify your trusted outbound mail server IP address or domain name (either your mail server or another trusted relay), identify a Smart host if you have one, and, optionally, an authentication type. The Barracuda Email Security Gateway supports SMTP/SASL authentication and LDAP. If you are relaying though a Smart host, you must also configure the Smart host to send to the Internet.

Be aware that configuring the Barracuda Email Security Gateway to scan outbound as well as inbound mail will increase the load on the system. You may find that you need to upgrade your Barracuda Email Security Gateway to another model.

Note:

When configuring outbound mail, ensure that your network firewall blocks all port 25 traffic that doesn't originate from your Barracuda Email Security Gateway.

© 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.