

Outbound Mail Scanning

<https://campus.barracuda.com/doc/3211275/>

Important

Before using the Barracuda Email Security Service outbound filter, go to <http://barracudacentral.org/lookups> and verify that your outbound IP address is not on the Barracuda Reputation list. If present on the list, contact [Barracuda Networks Technical Support](#) and request removal before using the outbound service.

Table 1. Outbound Mail Settings.

Feature	Description
Outbound Mail Scanning	<p>All messages, inbound and outbound, routed through Email Gateway Defense are subject to a 300MB size limit. This includes all headers, body, and attached content. This size can be lowered on a per domain basis by contacting Barracuda Networks Technical Support.</p> <p>Outbound mail scanning includes:</p> <ul style="list-style-type: none"> • Spam Scanning with Block or Quarantine actions • Virus Scanning • IP Address Filtering • Sender Domain, Username or Email Address Filtering • Recipient Email Address Filtering • Content Filtering (Subject, Header and Body) with Block, Allow, Quarantine, Encrypt, or Do not encrypt actions • Attachment Filtering • Intent Analysis <p>The following tools <i>are not</i> applied to outbound mail:</p> <ul style="list-style-type: none"> • IP Reputation, a sender authentication mechanism • Sender Policy Framework (SPF), a sender authentication mechanism • DomainKeys (DKIM) inspection • Exempt/block list <p>See also:</p> <ul style="list-style-type: none"> • Outbound Quarantine
Outbound Mail Encryption	<p>To prevent data leakage and ensure compliance with financial, healthcare, and other federally regulated agency information policies, you can require all email sent from any or all configured domains to be encrypted by configuring outbound mail encryption policies on the Outbound Settings > Content Policies page at the domain level.</p> <p>Inbound and outbound email transmission can also be required over a TLS channel.</p> <p>See also:</p> <ul style="list-style-type: none"> • How to Use DLP and Outbound Mail Encryption • Secured Message Transmission

Outbound Message Footer	You can configure Barracuda Email Security Service to append a custom text and/or html footer to each outbound message at the global level on the Outbound Settings > Tagline/Footer page. Appending a footer to outbound messages will cause outbound messages to fail a DKIM check, affecting mail delivery for recipients who check for DKIM.
----------------------------	---

© Barracuda Networks Inc., 2022 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.