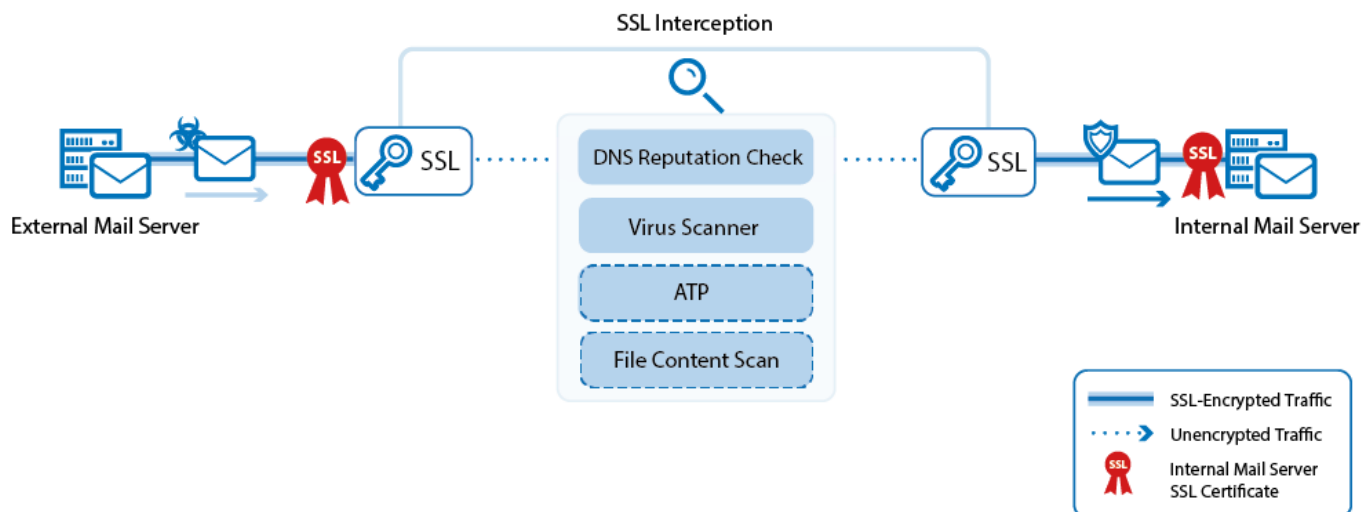


Mail Security in the Firewall

<https://campus.barracuda.com/doc/46208892/>

The Barracuda NextGen F-Series Firewall enforces mail security in the firewall by transparently scanning incoming and outgoing SMTP connections for malware and checking the reputation of the sender's IP address via a DNS blacklist (DNSBL). SMTP connections are supported on the following ports:

- **SMTP** and **SMTP with StartTLS** - TCP 25, TCP 587
- **SMTPS** - TCP 465



SSL Interception for Mail

SSL-encrypted SMTP connections are decrypted differently for in and outbound connections. Outbound SSL-encrypted SMTP connections are SSL-intercepted using a dynamically generated SSL certificate derived from the root certificate uploaded in the SSL Interception configuration. Inbound SSL-encrypted connections are intercepted using the same SSL certificate chain as is installed on the internal mail server. The SSL certificates are bound to the IP address on the F-Series Firewall that the mail server domain's MX record resolves to. This allows remote MTAs to use the information included in the SSL certificate to verify the identity of the server it is connecting to. You must install the SSL Interception root certificate on all mail clients connecting to a mail server via an SSL-intercepted SMTP connection to avoid certificate errors.

Virus Scanning for Mail

Both inbound and outbound email attachments are scanned by the virus scanner service. If malware is detected in an email attachment, the infected file is removed and replaced by an attachment containing a customizable text. If ATP is enabled on the system, attachments can also be scanned in the **Deliver first, then scan** mode. ATP scans are only reported; placing email recipients in

quarantine is not supported. The virus scanner fail-close policy does not apply to SMTP and SMTPS connections. If the virus scanning service is unavailable, emails with attachments are not scanned and delivered as-is to the internal mail server.

DNS Blacklist

Inbound email can also be classified according to DNS blacklists (DNSBL), such as the Barracuda Reputation Block List. For sender IP addresses blacklisted by the DNSBL, **[SPAM]** is prepended to the subject line of the email, and the MIME headers of the email are modified to allow the email to be immediately identified as spam by the mail server. If the DNSBL server is not available, the email is not modified. The email itself is delivered to the internal mail server.

For more information, see [How to Configure Mail Security in the Firewall](#).

Figures

1. virus_scanning_mail_traffic_atp-01.png

© Barracuda Networks Inc., 2021 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.