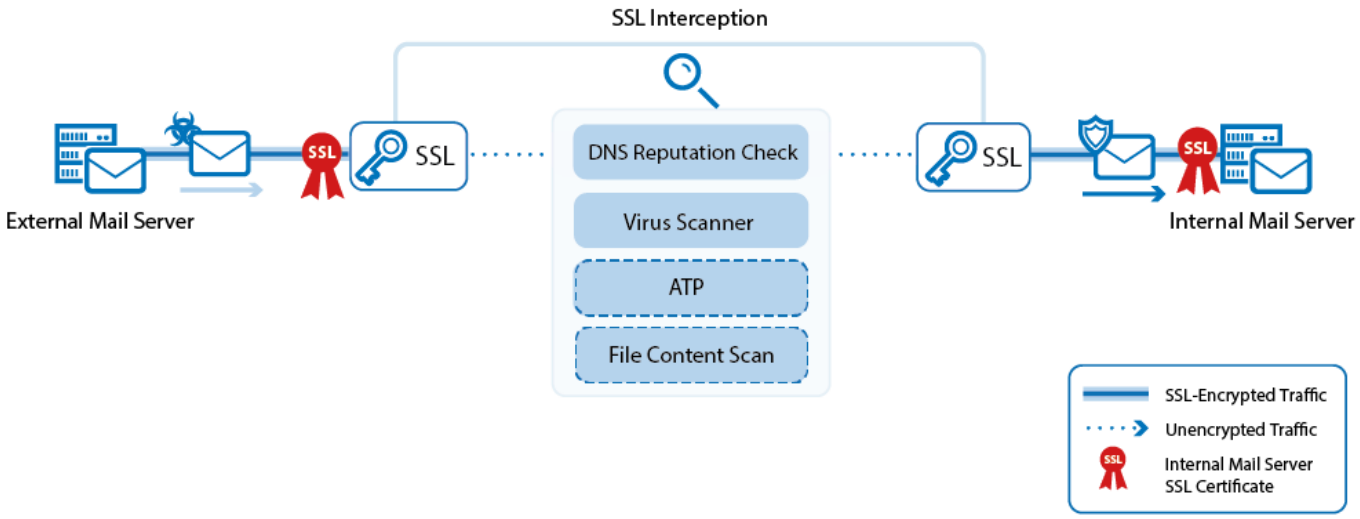
Mail Security in the Firewall

https://campus.barracuda.com/doc/73697817/

The 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 inbound and outbound connections. Outbound SSL-encrypted SMTP connections are SSL-intercepted by using a dynamically generated SSL certificate derived from the root certificate uploaded in the SSL Interception configuration. Inbound SSL-encrypted connections are inspected by using the same SSL certificate chain as is installed on the internal mail server. The SSL certificates are bound to the IP address on 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 identify of the server it is connecting to. To avoid certificate errors, you must install the SSL Interception root certificate on all mail clients connecting to a mail server via an SSL-intercepted SMTP connection.

Virus Scanning for Mail

Both inbound and outbound email attachments are scanned by the Virus Scanner. If malware is

detected in an email attachment, the infected file is removed and replaced by an attachment containing a customizable text. The Virus Scanner Block All / Allow All policy does not apply to SMTP and SMTPS connections. If Application Control and Virus Scanner are not enabled, emails with attachments are not scanned. Instead, they are delivered as-is to the internal mail server.

Advanced Threat Protection (ATP)

ATP scans SMTP and SMTPS traffic against advanced malware that is not detected by the Virus Scanner or Intrusion Prevention System. ATP analyzes files in the Barracuda ATP cloud and assigns a risk score. Local ATP policies determine how files with a high, medium, or low risk score are treated. To use ATP, you must have an Energize Updates and an Advanced Threat Protection subscription.

DNS Blacklisting

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 Virus Scanning for Mail Traffic.

Figures

1. virus_scanning_mail_traffic_atp-01.png