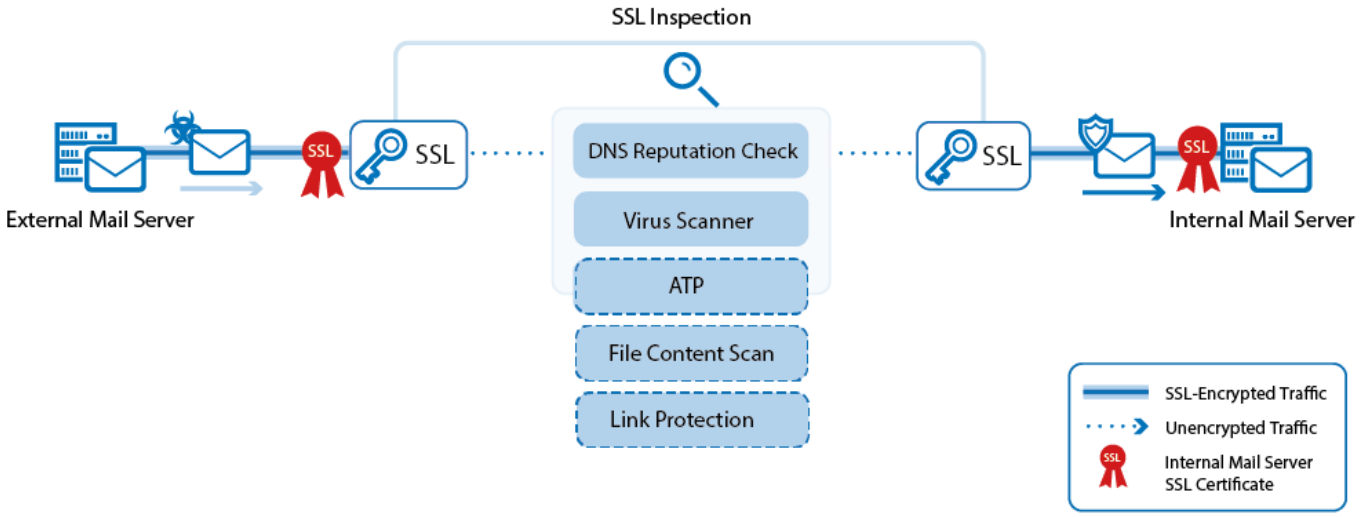
Mail Security in the Firewall

https://campus.barracuda.com/doc/73719337/

The CloudGen Firewall enforces mail security in the firewall by transparently scanning SMTP(s) and POP3(s) connections to the internal mail server for malware and checking the reputation of the sender's IP address via a DNS blacklist (DNSBL). Connections are supported on the following ports:

- **SMTP** and **SMTP with StartTLS** – TCP 25
- **SMTPS** – TCP 465
- **POP3** – TCP 110
- **POP3S** – TCP 995



SSL Inspection for Mail

SSL-encrypted SMTP and POP3 connections are decrypted differently for inbound and outbound connections. Outbound SSL-encrypted connections are SSL-intercepted using a dynamically generated SSL certificate derived from the root certificate uploaded in the SSL Inspection 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 CloudGen 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. You must install the SSL Inspection root certificate on all mail clients connecting to a mail server via an SSL-intercepted SMTP connection to avoid certificate errors.

For more Information see SSL Inspection in the Firewall.

Virus Scanning and Advanced Threat Protection 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, and the **5005 Virus Scan file blocked** event is triggered. If Advanced Threat Protection (ATP) is enabled on the system, attachments that have passed the Virus Scanner are uploaded and analyzed in the Barracuda ATP cloud. Mail attachments are scanned either in **Deliver first, then scan** or in **Scan first, then deliver** mode.

In **Deliver first, then scan** mode, if malware is found by ATP, the result is only reported and the email recipient is not placed in quarantine. In **Scan first, then deliver** mode, mail attachments are ATP-scanned before final delivery. The original message is forwarded to the final receiving server, with the potentially malicious attachments replaced by a message indicating the pending scan. If the result of the scan is not malicious, the attachment is delivered. Otherwise, the receiver is informed and the file is discarded.

The Virus Scanner's fail-close policy does not apply to SMTP and SMTPS connections. If the virus scanning service is unavailable, emails with attachments are not scanned by either the Virus Scanner or ATP. Instead, they are delivered as-is to the internal mail server. To enable a dedicated virus-scan log file, go to **Firewall > Security Policy > Virus Scanner Configuration > Advanced** and select the **Enable SMTP Virus Scan Log** check box.

DNS Blacklist

Inbound emails can also be classified according to DNS blacklists (DNSBL), such as the Barracuda Reputation Block List. When an external mail server transmits emails, the IP address of its sending message transfer agent (MTA) is sent to the Barracuda Reputation Block List as a DNS request. If the IP address of the MTA is found in the blacklist, '<SPAM>' is prepended to the text in the subject line, e.g., '<SPAM> This is subject XY'. The header of the email is rewritten so that it contains information like 'X-Spam-Prev-Subject:This is subject XY', 'X-Spam-Flag: YES', 'X-Spam-Status: Yes' and 'X-Spam-Level: ***'.

DNSRBL is only supported for SMTP (TCP25) and SMTP+STARTLS (TCP465). For details about the mail classification, log into your firewall and go to **LOGS**. From **Select Log File**, select ***Your virtual server* > NGFW > SSL** to view the contents of the log file.

Link Protection

Link Protection protects users from fraudulent links inside of plain-text and HTML emails. Such links are the result either of mistyping a URL or of domains not known to users as being fraudulent. Link Protection requires an active ATP subscription.

Link Categorization

When an email contains an embedded URL that starts with HTTP(S)/FTP, the URL will be rewritten. The firewall replaces the original URL with **https://linkprotect.cudasvc.com**. The user then receives the email with the rewritten link.

When the user clicks the URL, a web page opens in the browser. Depending on the detected risk, there are now two options:

- The embedded URL is considered fraudulent: The user is presented a web page with a block message and a description why the original URL is considered fraudulent.
- There is no risk for the original URL: The user is redirected to the original URL.

The following URL categories are blocked by Link Protection: hacking, phishing fraud, spam, spyware, malicious sites, and typo-squatted URLs.

URL Rewrite

Rewriting of URLs is done only for HTTP, HTTPS, or FTP links. Links without protocols are rewritten to include the proper protocol. The following URLs are not rewritten:

- URLs using a different protocol, such as skype://, or torrent://
- The URL is exempt.
- The URL is contained in an encrypted or protected message.
- The URL is inside of an attachment.

For more Information see How to Configure Link Protection for Mail Security in the Firewall.

Figures

1. virus_scanning_mail_traffic_atp_link.png