Fortigate SMTP “splice” behavior and ‘Replacement Messages’

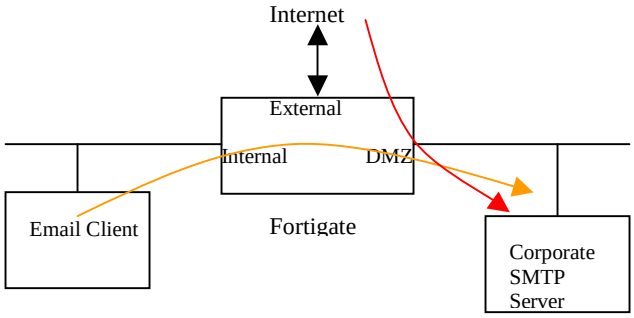
The way the SMTP mail Replacement Messages are added by the Fortigate, and viewed by the email client software, depends on the following factors:

- SMTP “splice” feature (enabled or disabled)*****
- Whether the email is being sent or received by an email client.
- The type of email client software used.

***Note: As of v2.80MR7 (B318), SMTP splice is automatically enabled (and can’t be disabled) when Anti-Virus scanning is enable.**

Example Network Diagram:
In the diagram shown below, the internal email client sends his outgoing email to his corporate SMTP server on the DMZ, which then transfers it to the destination SMTP server on the Internet. Incoming email is delivered to the corporate SMTP server on the DMZ, and the email client retrieves this email via POP3, IMAP or MAPI protocol. Fortigate Firewall Policies are applied on SMTP from Internal ->DMZ and from External->DMZ, with an anti-virus and file blocking Protection Profile.

Additional Firewall Policies will be required to allow the internal clients to retrieve their incoming email, and to allow the corporate SMTP server to transmit the email to the external SMTP servers. The explanations provided below only concern the traffic flow as initiated by the colored lines in the diagram, and not any additional FW Protection policies.



With SMTP “splice” enabled:

- When the internal email client sends a blocked/virus infected email, the FGT aborts the SMTP communication and returns a 554 SMTP error message to the client and includes the Replacement Message with the 554 code. This is viewed by the client as a communication error, and the Replacement Message may only be viewable in the client email software’s error log/window. The destined email client never receives the email nor any notification.
- When an external SMTP server is sending a blocked/virus infected email to the DMZ corporate SMTP server, the FGT will abort the SMTP communication and return a 554 SMTP error message to the sending server. The 554 SMTP error message will include the Replacement Message as additional information. The sending SMTP server will then send a NDR (non delivery report) email back to the original sender, stating that the email could not be delivered due to the following reason(s). The reason should include the 554 error code and its associated message (the Fortigate’s Replacement Message). The way this NDR email is formatted depends on the remote SMTP server’s configuration. The Replacement Message may be included as an attachment instead of within the body of the email. The original email attachment(s) may also be ‘bounced’ back to the sender in this NDR email.

With SMTP “splice” disabled:

- When the internal email client sends a blocked/virus infected email, the FGT delivers the email to the corporate DMZ SMTP server, but removes the blocked/infected attachment. It then includes the Replacement Message within the body of the email, and then transmits this ‘modified’ email to the remote external SMTP server. The email client on the receiving side, will receive an email without the infected/blocked attachment, and with a Replacement Message included inline within the body of the email. The internal sender is not aware that this modification has occurred to his original email, and only the external receiver sees the modification.

- When an external SMTP server is sending a blocked/virus infected email to the DMZ corporate SMTP server, the FGT will deliver this email to the DMZ server, but will remove the blocked/infected attachments and will include the Replacement Message within the body of the email. The external sender is not aware that this modification has occurred to his original email, and only the internal receiver sees the modification. The internal receiver will then retrieve this 'modified' email via POP, IMAP or MAPI.

Attachments and email client software:

Different email clients will display attachments in different manners:
- some indicate it only as an attachment (ex. Outlook).
- some as an attachment and display it inline with the email body as well (ex. PocoMail)
- some display it inline with the body but not as an attachment (ex. Outlook Express).