How does PoliteMail work with security appliances like Mimecast or Proofpoint?

Last Modified on 06/03/2024 11:40 am EDT

Email Security Appliances

In some cases, organizations will employ a Mail Security Appliance, such as Proofpoint or Mimecast Barracuda, to filter spam emails and block others. This is usually a security requirement and sometimes creating a receive connector that routes around the Mail Application is not possible.

In this case, PoliteMail will need to be properly whitelisted within this environment so that messages are not marked as external, and are not blocked as phishing. However, this creates a problem with the Treat as Internal requirement as a mail route cannot easily be dedicated for PoliteMail to mark messages as internal. Instead, a Group Policy Object (GPO) push is required to allow images to download automatically in Outlook on Windows Machines. In addition, PoliteMail will need to be configured as a safe sender in Outlook, as described in this Microsoft help article.

If utilizing SPAM firewalls such as ProofPoint or Barracuda in addition to Exchange Online Protection (EOP), an exception must be added to prevent unintentional filtering of internal email being routed through the PoliteMail Server IP.2.

Note that when you decide to route PoliteMail messages externally via SMTP (which means it will enter through your email firewall), you will also be responsible for the following steps in order for it to properly function:

1. Set up SPF/DMARC of the PoliteMail dedicated, static SMTP IP address.
2. Trust the static IP with your Mail Security Appliance to prevent blocking.
3. Disable the flagging of the message as "External".
4. Preform any other whitelisting/exemption to allow messages to flow at volume without disturbance.

PoliteMail can also be configured to ignore Proofpoint security proxy hits by using either IP or User Agents IIS Filtering.