Whitelist Requirements for SMTP Services

Category: How-To

Description:

This document describes what to whitelist for successful E-Mail service delivery.

Purpose:

The purpose of this document is to describe the whitelisting requirements for SMTP E-Mail services.

DNS Domain Modification:

When an E-mail message is sent by a domain where the sender is different than the SMTP server's domain, it will report out as a softfail through MIME headers. Some clients prevent E-mails which report a softfail from coming through their SMTP server. To validate the client's domain as a valid sender for our SMTP servers, thus preventing a softfail, the following DNS modifications are needed:

1. Update domain's root TXT SPF record by adding:
   include:_spf.mitracloud.com

Firewall Filter Rule:

Some clients restrict incoming traffic with respect to incoming E-mail. These clients require the IP address of our SMTP servers in order to allow access. A new tcp protocol rule for the following addresses may be required:

mailod.mitracloud.com	**166.78.81.73**	**US-Only**	**Prod**
maildw.mitracloud.com	**98.129.166.181**	**US-Only**	**Non-prod**
maill3.mitracloud.com	**94.236.35.193**	**UK-Only**	**Prod**
maill5.mitracloud.com	**162.13.228.166**	**UK-Only**	**Non-prod**