FortiMail Best Practices Antispam Tuning

Although your FortiMail unit will catch almost all threats that are sent to your network, there are some things you should be aware of if you want to maximize security.

The Best Practices recipes will cover specific tips to ensure the most secure and reliable operation of your FortiMail unit.

This recipe covers the best practices for Antispam tuning.

Antispam Tips

The following are some tips to limit the amount of spam you receive.

1. Black and white lists can sometimes cause false positives and false negatives if not properly configured. For example, a white list entry *.edu allows all mail from the .edu top level domain to bypass the FortiMail unit's antispam.
2. Do not whitelist protected domains. Whitelisted domains bypass antispam scans, so email with spoofed sender addresses in the protected domains will bypass antispam features.
3. Use a combination of recipient verification and sender reputation to prevent directory harvest attacks (DHA). DHA utilizes recipient verification in an attempt to determine an email server's valid email address. It is a common method of attack made by spammers.

   If *Recipient address Verification* is enabled, each recipient address is verified with the protected email server. For email destined for invalid recipient addresses, the FortiMail unit returns *User Unknown* messages to the SMTP client. Spammers utilize this response to guess and learn valid recipient address.

   You can prevent this from occurring if you enable *Enable sender reputation checking* in session profiles, located under **Profile > Session > Session.** Sender reputation weighs each SMTP client's IP address and assigns them a score. If the SMTP client sends several email messages to unknown recipients, the sender's reputation score increases significantly. If the sender's reputation score exceeds the threshold, the SMTP client's SMTP sessions are terminated at connection level.

4. Enable bounce verification to prevent delivery status notification (DSN) spam.

Spammers may use the DSN to bypass antispam measures. The spammer spoofs the email address of a legitimate sender and sends spam to an undeliverable recipient, expecting that the recipient's email server will send a DSN back to the sender to notify him/her of the delivery failure. Many antispam mechanisms may be unable to detect the difference between a legitimate and spoofed DSN.

You can prevent this from occurring by enabling bounce address tagging and verification, located in **AntiSpam > Bounce Verification > Settings**. Select *Use antispam profile settings* for the Bounce verification action option. Disable both the *Bypass bounce verification* option (**Mail Settings > Domains > Domains**) and the *Bypass bounce verification check option (***Profile > Session > Session**). Finally, verify both outgoing and incoming email is routed through the FortiMail unit. The FortiMail unit cannot tag email, or recognize legitimate DSN for previously sent email, if all email does not pass through the unit.