FortiMail Best Practices SMTP Connectivity

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 SMTP connectivity.

SMTP Connectivity Tips

The following are some tips to ensure maximum safety for your network.

1. **C**onfigure a fully qualified domain name (FQDN) that is different than that of your protected email server (gateway mode and transparent mode).

   Go to **Mail Settings** > **Settings** > **Mail Server Settings.**

2. Use a different host name for each FortiMail unit when managing multiple FortiMail units of the same model or when configuring an HA cluster.

   The host name is set in **Mail Setting**s > **Settings** > **Mail Server Settings.**

3. If the FortiMail unit is used as an outbound relay (gateway mode and server mode only) or if remote email users will view their per-recipient quarantines, the FortiMail unit's FQDN must be globally DNS-resolvable.

   External SMTP servers require that A records and reverse DNS records be configured on public DNS servers for both forward and reverse lookup of the FQDN and its IP address.

4. Configure the public DNS records for each of your protected domains with only one MX record that routes incoming email through the FortiMail unit (gateway mode). With only one MX record, spammers cannot bypass the FortiMail unit by using lower-priority mail gateways.

5. If the FortiMail unit is operating in transparent mode, SMTP clients are configured for authentication, and you have disabled the Use client-specified SMTP Server to send email option for SMTP proxies, you must configure and

apply an authentication profile.

To configure the authentication profile, go to **Profile** > **Authentication** > **Authentication**. Without the authentication profile, authentication with the FortiMail unit will fail.

Additionally, you must configure an access control rule to allow relay to external domains. To configure the access control rule, go to **Policy** > **Access Control** > **Receive.**