FortiMail Best Practices Performance 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 performance tuning.

Performance Tuning Tips

1. To avoid performance problems and prevent FortiMail from refusing SMTP connections that are heavy mail traffic, configure the recipient address verification, located in **Mail Settings > Domains > Domains** with an SMTP or LDAP server. This is especially important when quarantining is enabled because of the potentially large amount of quarantined mail for invalid recipients.

2. A great way to limit the amount of resources required to identify spam is to enable greylisting. You can enable greylisting by going to **Profile > AntiSpam > AntiSpam.**

3. Apply spam throttling features by creating an IP-based policy in **Policy > Policies > Policies,** with a session profile in **Profile > Session > Session**. Sender reputation, session limiting, and error handling are particularly useful.

4. If you have FortiGuard enabled in an antispam profile, you'll also need to enable caching and *Enable Black IP* to query for the blacklist status of the IP addresses of all SMTP servers appearing in the Received: lines of header lines. You can enable caching in **Maintenance > FortiGuard > AntiSpam**.

5. To reduce latency associated with DNS queries, use a DNS server on your local network.

6. If logs are stored on the FortiMail unit, set logging rotation size (located in **Log and Report > Log Settings > Local Log Settings**) to between 10 MB and 20 MB, and set the event logging level to warning or greater. Delete or back up old logs regularly to free storage space.

7. Make sure to regularly delete or backup old reports, quarantined mail, and mail queue entries to reduce the number of reports on the local disk.

8. Be sure to schedule resource intensive and tasks that are not time critical, such as report generation to low-traffic periods.

9. Disable resource intensive scans, such as the heuristic scan (located in **Profile > AntiSpam > AntiSpam)**, when spam capture rate is satisfactory.

10. Enable the *Max message size to scan and Bypass scan on SMTP authentication* in the *Scan Conditions* section of the antispam profile, located in **Profile > AntiSpam > AntiSpam.**

11. Regularly format the mail and log disks to improve disk performance.

    Important: Make sure to back up logs and mail before formatting the hard disk. Formatting log disks deletes all log entries.