FortiMail Best Practices High Availability

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 high availability.

High Availability Tips

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

1. Isolate HA interface connections from your overall network. Heartbeat and synchronization packets contain sensitive configuration information and can consume considerable network bandwidth.

   For an active-passive or a config-only HA group consisting of only two FortiMail units, directly connect the HA interfaces using a crossover cable. For a config-only HA group consisting of more than two FortiMail units, connect the HA interfaces to a switch and do not connect this switch to your overall network.

2. Use FortiMail active-passive HA to provide failover protection so that if your primary FortiMail unit fails, the backup FortiMail unit can continue processing email with only a minor interruption to your email traffic.

3. Use config-only HA if you want to create a mail server farm for a large organization. You can also install a FortiMail config-only HA group behind a load balancer. The load balancer can balance the mail processing load to all FortiMail units in the config-only HA group, improving mail processing capacity.

4. Maintain the HA heartbeat connection between HA members. If HA heartbeat communication is interrupted and no remote services are detected, HA synchronization is disrupted and, for active-passive HA groups, the backup unit will assume that the primary unit has failed and become the new primary unit.

5. License all FortiMail units in the HA group for the FortiGuard Antispam and FortiGuard Antivirus services. If you only license the primary unit in an active-

passive HA group, after a failover the backup unit cannot connect to the FortiGuard Antispam service. Also, antivirus engine and antivirus definition versions are not synchronized between the primary and backup units.

6. Configure HA to synchronize the system mail directory and the user home directory to prevent email loss during a failover.

7. Do not synchronize or back up the MTA spool directories. The content of the MTA spool directories is very dynamic, so synchronizing MTA spool directories between FortiMail units may use a lot of bandwidth.

8. Store mail data on a NAS server while operating an HA group. Backing up your NAS server regularly helps prevent loss of FortiMail mail data. Additionally, if your FortiMail unit experiences a temporary failure, you can still access the mail data on the NAS server.

9. If you are using a NAS server, disable mail data synchronization. If mail data synchronization is enabled both the primary and backup units store the mail data to the NAS server, resulting in duplicate traffic.

   Disable mail data synchronization to conserve system resources and network bandwidth.

10. Use SNMP, syslog, or email alerts to monitor a cluster for failover messages. These alert messages may aid in quick discovery and diagnosis of network problems.

    Configure SNMP in **System** > **Configuration** > **SNMP.**