What's the difference between the Outbreak and Virus quarantines?

Document ID: 118114

Contributed by Jackie Fleming and Stephan Bayer, Cisco TAC Engineers.

Jul 31, 2014

Contents

Question:

What's the difference between the Outbreak and Virus quarantines?

Answer:

AsyncOS quarantines include two built−in quarantines that cannot be deleted: Outbreak and Virus.

The Outbreak quarantine is used only by Virus Outbreak Filters (if enabled.)

Messages that meet or exceed the configured Virus Threat Level threshold on the Cisco Email Security Appliance (ESA) are held in the Outbreak quarantine instead of being delivered. Messages can be released or deleted from the Outbreak quarantine at the discretion of the quarantine manager. Messages will also leave the quarantine if the configured time or size limits are exceeded, and they will be handled with the Default policy setting of the quarantine to either delete or release if these limits are reached.

Following release from the Outbreak quarantine, messages are re−scanned by the anti−virus module, and action is taken according to anti−virus policy. Depending on this policy, a message may be delivered, deleted, or delivered with viral attachments stripped. It is expected that viruses will often be found during re−scan after release from the Outbreak quarantine. The ESA mail_logs files or Message Tracking can be consulted to determine if an individual message that was noted in the quarantine was found to be viral, and if and how it was delivered.

The Virus quarantine is available to receive messages that Sophos classifies as virus−infected, encrypted or un−scannable. In each of these cases the message is viral or potentially viral. Messages sent to the virus quarantine will remain there until either the quarantine manager chooses to release or delete them, or the configured size or time limits of the quarantine are reached. The default action when the quarantine limits are reached is configurable.

Messages released from the quarantine are not re−scanned by the anti−virus module; however, while in the quarantine the quarantine manager can scan an individual message to determine if it is viral according to the current set of virus IDEs loaded on the ESA.

Note: New viruses will be quarantined, but the oldest messages in the quarantine are flushed to make room for the new ones. This is a "first in, first out" policy. However, the disposition of the oldest messages is based on

how the quarantine is configured, meaning the messages are either deleted prematurely or are released prematurely.

Although the built−in quarantines cannot be deleted, the amount of space allocated to them can be reconfigured. The amount of space available for quarantines varies by ESA model, and is displayed on the Monitor−>Quarantines−>Manage Quarantines page in the GUI. The minimum size for a quarantine is 250MB. Having a fixed upper limit to quarantines assures that a sudden increase in quarantine activity cannot impact the ESA's mail queues and affect normal message delivery.

Updated: Jul 31, 2014 Document ID: 118114