Quelle est la différence entre les quarantaines d'épidémie et de virus ?

Contenu

Question :

Quelle est la différence entre les quarantaines d'épidémie et de virus ?

Réponse :

Les quarantaines d'AsyncOS incluent deux quarantaines intégrées qui ne peuvent pas être supprimées : Épidémie et virus.

La quarantaine d'épidémie est utilisée seulement par attaque de virus filtre (si activée.)

Des messages qui rencontrent ou dépassent le seuil configuré de niveau de menace de virus sur l'appliance de sécurité du courrier électronique de Cisco (ESA) sont tenus dans la quarantaine d'épidémie au lieu de l'livraison. Des messages peuvent être libérés ou supprimés de la quarantaine d'épidémie à la discrétion du gestionnaire de quarantaine. Les messages partiront également de la quarantaine si le temps ou les limites de taille configuré sont dépassés, et ils seront manipulés avec la configuration de stratégie par défaut de la quarantaine à l'effacement ou à la release si ces limites sont atteintes.

La release suivante de la quarantaine d'épidémie, des messages sont rebalayées par le module d'antivirus, et une mesure est prise selon la stratégie d'antivirus. Selon cette stratégie, un message peut être fourni, supprimé, ou fourni avec les connexions virales éliminées. On s'attend à ce que des virus souvent soient trouvés pendant le retour après que release de la quarantaine d'épidémie. Les fichiers de mail_logs ESA ou le cheminement de message peuvent être consultés pour déterminer si un message individuel qui a été noté dans la quarantaine s'avéraient viral, et si et comment il a été livré.

La quarantaine de virus est disponible pour recevoir les messages que Sophos classifie comme infecté par le virus, chiffré ou ONU-analysable. Dans chacun de ces cas le message est viral ou potentiellement viral. Les messages envoyés à la quarantaine de virus demeureront là jusqu'à ce que le gestionnaire de quarantaine choisisse de les libérer ou supprimer, ou la taille configurée ou des délais de la quarantaine sont atteintes. L'action par défaut quand les limites de quarantaine sont atteintes est configurable.

Des messages libérés de la quarantaine ne sont pas rebalayés par le module d'antivirus ; cependant, alors que dans la quarantaine le gestionnaire de quarantaine peut balayer un

message individuel pour déterminer s'il est viral selon l'ensemble en cours d'ides de virus chargées sur l'ESA.

Remarque: De nouveaux virus seront mis en quarantaine, mais les messages les plus anciens dans la quarantaine sont vidés pour faire de la place pour les neufs. C'est « d'abord dedans, d'abord » stratégie. Cependant, la disposition des messages les plus anciens est basée sur la façon dont la quarantaine est configurée, signifiant que les messages sont supprimés pr3maturément ou sont libérés pr3maturément.

Bien que les quarantaines intégrées ne puissent pas être supprimées, l'espace alloué à elles peut être modifié. L'espace disponible pour des quarantaines varie par le modèle ESA, et est affiché à la page de quarantaines de Monitor->Quarantines->Manage dans le GUI. La taille minimum pour une quarantaine est 250MB. Ayant une limite supérieure fixe aux quarantaines s'assure qu'une augmentation soudaine d'activité de quarantaine ne peut pas affecter les files d'attente de la messagerie de l'ESA et affecter la livraison normale de message.