¿Cuál es la diferencia entre las cuarentenas del brote y del virus?

Contenido

Pregunta:

¿Cuál es la diferencia entre las cuarentenas del brote y del virus?

Respuesta:

Las cuarentenas de AsyncOS incluyen dos cuarentenas incorporadas que no puedan ser borradas: Brote y virus.

La cuarentena del brote es utilizada solamente por el brote de virus filtra (si está habilitada.)

Los mensajes que resuelven o exceden el umbral configurado del nivel de la amenaza del virus en el dispositivo de seguridad del correo electrónico de Cisco (ESA) se llevan a cabo en la cuarentena del brote en vez de la entrega. Los mensajes se pueden liberar o borrar de la cuarentena del brote a discreción del administrador de la cuarentena. Los mensajes también saldrán de la cuarentena si se excede el tiempo o los límites de tamaño configurados, y serán manejados con la configuración de la política predeterminada de la cuarentena a la cancelación o a la versión si se alcanzan estos límites.

La versión de siguiente de la cuarentena del brote, los mensajes es pre-explorada por el módulo del contra virus, y medidas se toman según la directiva antivirus. Dependiendo de esta directiva, un mensaje se puede entregar, borrar, o entregar con las conexiones virales eliminadas. Se espera que los virus sean encontrados a menudo durante la pre-exploración después de la versión de la cuarentena del brote. Los archivos de los mail_logs ESA o Seguimiento de mensajes se pueden consultar para determinar si un mensaje individual que fue observado en la cuarentena fueron encontrados para ser viral, y si y cómo él fue entregado.

La cuarentena del virus está disponible recibir los mensajes que Sophos clasifica según lo virus-infectado, cifrado u O.N.U-scannable. En cada uno de estos casos el mensaje es viral o potencialmente viral. Seguirá habiendo los mensajes enviados a la cuarentena del virus allí hasta que el administrador de la cuarentena elija liberarlos o borrar, o se alcanza el tamaño configurado o los límites de tiempo de la cuarentena. La acción predeterminada cuando se alcanzan los límites de la cuarentena es configurable.

Los mensajes liberados de la cuarentena no son pre-explorados por el módulo del contra virus; sin embargo, mientras que en la cuarentena el administrador de la cuarentena puede explorar un

mensaje individual para determinar si es viral según el conjunto actual del virus IDE cargado en el ESA.

Nota: Los nuevos virus quarantined, pero los más viejos mensajes de la cuarentena se vacian para hacer el sitio para los nuevos. Éste es “primero adentro, primero hacia fuera” directiva. Sin embargo, la disposición de los más viejos mensajes se basa en cómo la cuarentena se configura, significando que los mensajes están borrados prematuramente o que liberados prematuramente.

Aunque las cuarentenas incorporadas no puedan ser borradas, la cantidad de espacio afectada un aparato a ellas puede ser configurada de nuevo. La cantidad de espacio disponible para las cuarentenas varía por el modelo ESA, y se visualiza en la página de las cuarentenas de Monitor->Quarantines->Manage en el GUI. El tamaño mínimo para una cuarentena es 250MB. Teniendo un límite superior fijo a las cuarentenas asegura que un aumento súbito en la actividad de la cuarentena no puede afectar las colas de administración del tráfico del correo ESA y afectar a la salida del mensaje normal.