

¿Cómo configuro el ESA para saltar la exploración del anti-Spam y/o del contra virus para mis remitentes de confianza?

Contenido

Pregunta:

¿Cómo configuro el ESA para saltar la exploración del anti-Spam y/o del contra virus para mis remitentes de confianza?

AsyncOS ofrece tres herramientas principales que usted pueda utilizar para saltar el anti-Spam o el contra virus que marca para saber si hay sus remitentes más de confianza. Observe por favor que el ESA no aconseja el contra virus que salta que marca en cualquier momento, incluso para saber si hay sus remitentes más de confianza, debido al potencial para la infección inadvertida con los virus. Lo que sigue es una discusión de las tres maneras que usted puede saltar el anti-Spam que marca para saber si hay cierto subconjunto de su flujo de mensajes.

La primera herramienta disponible para usted es las directivas del flujo de correo de la tabla del acceso del host (SOMBRERO). Usando las directivas del flujo de correo, usted puede identificar los remitentes por la dirección IP (usando los IP Addresses numéricos o los nombres DNS PTR), por la calificación de SenderBase, o por una lista blanca del DNS local o la lista negra. Una vez que usted ha identificado los remitentes según lo confiado en dentro de un grupo del remitente en el SOMBRERO, usted puede entonces marcar ese grupo del remitente para saltar la exploración del anti-Spam.

Por ejemplo, déjenos suponen que usted quiso identificar a un partner comercial específico, EXAMPLE.COM, que no debe tener anti-Spam que marca en su correo. Usted tendría que descubrir los expedientes de los IP Addresses (o del DNS Pointer) del mail server SCU.COM. En este caso, déjenos asumen que EXAMPLE.COM tiene servidores del correo que tengan IP Addresses con los expedientes PTR DNS de "smtp1.mail.scu.com" al "smtp4.mail.scu.com." recordar en este caso que estamos mirando el expediente PTR (a veces llamado el revés DNS) para los servidores del correo; esto no tiene nada hacer con el Domain Name que la gente en SCU.COM utilizará para el correo saliente.

Usted podría crear un nuevo grupo del remitente (o utilizar un grupo existente del remitente, tal como WHITELIST) con el grupo del remitente de Políticas>Overview>Add del correo. Creemos uno llamado "NotSpammers". Después de que usted haya presentado esta página, le volverán a la pantalla de Políticas>Overview del correo, donde usted tendrá la oportunidad de agregar una nueva directiva para este grupo del remitente. Si usted hace clic en "agregue la directiva," usted será dado la oportunidad de crear una nueva directiva. En este caso, queremos reemplazar solamente la política predeterminada en una área: Detección del Spam. Dé a directiva un nombre y fije el comportamiento de la conexión para ser "validan," entonces navegue hacia abajo a la sección de la detección del Spam y fijado esta directiva para saltar marcar del Spam. Someta esa nueva directiva, y no olvide "confiar los cambios."

Un enfoque alternativo es utilizar las directivas del correo entrante para saltar la exploración del anti-Spam. La diferencia entre el SOMBRERO y las directivas del correo entrante es que el SOMBRERO está basado totalmente en la información IP en el remitente: la dirección IP verdadera, la dirección IP como se refleja en el DNS, la calificación de SenderBase (que se basa en la dirección IP) o una entrada de la lista blanca o de la lista negra DNS basada en la dirección IP. Las directivas del correo entrante se basan en la información del sobre del mensaje: quién el mensaje es o quién es el mensaje. Esto significa que son susceptibles a ser engañado por alguien que personifica un emisor del mensaje. Sin embargo, si usted quiere saltar simplemente todo el anti-Spam que marca para saber si hay el correo entrante que viene de la gente que tiene direcciones de correo electrónico que terminen en “@example.com,” usted podría hacer eso también.

Para crear tal directiva, vaya a enviar la directiva de Políticas>Add del correo de Políticas>Incoming. Esto le dejará agregar una directiva que defina un conjunto de los remitentes (o de los beneficiarios). Una vez que usted define la directiva del correo entrante, aparecerá en la pantalla de la descripción (directivas del correo de Políticas>Incoming del correo). Usted puede después hacer clic en la columna del “Anti-Spam” y editar las configuraciones específicas para el anti-Spam para este usuario determinado.

Las configuraciones del Anti-Spam para una directiva determinada tienen porciones de opciones, pero en este caso, queremos simplemente saltar marcar del anti-Spam. Observe aquí otra diferencia entre la directiva y las directivas Sombrero-basadas del correo entrante: el SOMBRERO puede le dejó solamente saltar o no saltar la exploración del anti-Spam, mientras que las directivas del correo entrante tienen control mucho mayor. Por ejemplo, usted podría elegir quarantine el Spam de ciertos remitentes, y el Spam de la cancelación de otros remitentes.

La tercera opción para la exploración del anti-Spam que salta está en los filtros del mensaje. (Nota que los filtros contenidos no se pueden utilizar para esto porque ocurren los filtros contenidos después de que haya ocurrido la exploración del anti-Spam ya). Una de las acciones en los filtros del mensaje es “salto-spamcheck.” El filtro del mensaje abajo saltará el anti-Spam que marca para saber si hay remitentes que tengan un IP Address particular o que vengan de un Domain Name determinado:

```
SkipSpamcheckFilter:
  si ((== '192.168.195.101' del IP remoto) o
      (\ del @example de correo-de == "\ .com$"))
  {
    salto-spamcheck();
  }
```