¿Cómo configuro el ESA para omitir el análisis de antivirus o antispam para mis remitentes de confianza?

Contenido

Pregunta

¿Cómo configuro el ESA para omitir el análisis de antivirus o antispam para mis remitentes de confianza?

Respuesta

AsyncOS ofrece tres herramientas principales que puede utilizar para omitir la comprobación de anti-spam o antivirus de sus remitentes de mayor confianza. Tenga en cuenta que el ESA no aconseja saltarse la comprobación de antivirus en ningún momento, ni siquiera para los remitentes de mayor confianza, debido a la posibilidad de infección involuntaria con virus. A continuación se describe una explicación de las tres formas en que puede omitir la comprobación antispam de algún subconjunto del flujo de mensajes.

La primera herramienta disponible son las políticas de flujo de correo de la tabla de acceso de host (HAT). Mediante Políticas de flujo de correo, puede identificar remitentes por dirección IP (mediante direcciones IP numéricas o nombres DNS PTR), por puntuación SenderBase o por una lista de permitidos o lista de bloqueo de DNS local. Una vez que haya identificado a los remitentes como de confianza dentro de un grupo de remitentes en la HAT, puede marcar ese grupo de remitentes para omitir el análisis antispam.

Por ejemplo, supongamos que deseaba identificar a un partner empresarial específico, EXAMPLE.COM, que no debería tener una comprobación antispam en su correo. Tendría que averiguar las direcciones IP del servidor de correo de SCU.COM (o registros de puntero DNS). En este caso, supongamos que EXAMPLE.COM tiene servidores de correo que tendrán direcciones IP con registros DNS PTR de "smtp1.mail.escu.com" a través de "smtp4.mail.escu.com". Recuerde en este caso que estamos buscando el registro PTR (a veces llamado DNS inverso) para los servidores de correo; esto no tiene nada que ver con el nombre de dominio que los usuarios de SCU.COM usarán para el correo saliente.

Puede crear un nuevo grupo de remitentes (o utilizar un grupo de remitentes existente, como ALLOWLIST) con Políticas de correo>Descripción>Agregar grupo de remitentes. Creemos uno llamado "NotSpammers". Después de enviar esta página, volverá a la pantalla Políticas de correo>Descripción general, donde tendrá la oportunidad de agregar una nueva política para este grupo de remitentes. Si hace clic en "Agregar política", se le dará la oportunidad de crear una nueva política. En este caso, sólo queremos invalidar la política predeterminada en un área: Detección de spam. Asigne un nombre a la política y establezca el comportamiento de la

conexión en "Aceptar". A continuación, desplácese hasta la sección Detección de spam y establezca esta política para omitir la comprobación de spam. Envíe esa nueva política y no olvide "Registrar cambios".

Un enfoque alternativo es utilizar las políticas de correo entrante para omitir el análisis antispam. La diferencia entre las políticas de HAT y de correo entrante es que la HAT se basa completamente en la información de IP del remitente: la verdadera dirección IP, la dirección IP como se refleja en el DNS, la puntuación SenderBase (que se basa en la dirección IP) o una lista de permitidos DNS o entrada de lista de bloqueo basada en la dirección IP. Las políticas de correo entrante se basan en la información del sobre del mensaje: quién es el mensaje o de quién es. Esto significa que son susceptibles de ser engañados por alguien que se hace pasar por un remitente de mensaje. Sin embargo, si simplemente desea omitir toda la comprobación antispam de correo entrante procedente de personas que tienen direcciones de correo electrónico que terminan en "@example.com", también puede hacerlo.

Para crear tal política, vaya a **Políticas de correo > Políticas de correo entrante > Agregar política**. Esto le permitirá agregar una política que defina un conjunto de remitentes (o destinatarios). Cuando defina la política de correo entrante, aparecerá en la pantalla de información general (Políticas de correo>Políticas de correo entrante). A continuación, puede hacer clic en la columna "Anti-Spam" y editar los parámetros específicos para antispam para este usuario en particular.

La configuración Anti-Spam de una política en particular tiene muchas opciones, pero en este caso, simplemente queremos omitir la verificación anti-spam. Observe aquí otra diferencia entre la política basada en HAT y las políticas de correo entrante: la HAT sólo puede permitirle omitir o no el análisis antispam, mientras que las políticas de correo entrante tienen un control mucho mayor. Por ejemplo, podría optar por poner en cuarentena el spam de ciertos remitentes y eliminar el spam de otros remitentes.

La tercera opción para saltar el análisis antispam es mediante la configuración y el uso de un filtro de mensajes.

> **Nota:** Los filtros de contenido no se pueden utilizar para esto porque los filtros de contenido se producen después de que ya se haya realizado el análisis antispam

Una de las acciones de Filtros de mensajes es "saltar-enviar-spam". El siguiente filtro de mensaje omitirá la comprobación antispam de los remitentes que tienen una dirección IP determinada o que proceden de un nombre de dominio determinado:

```
SkipSpamcheckFilter:
   if ( (remote-ip == '192.168.195.101') or
        (mail-from == '@example\\.com$')      )
   {
       skip-spamcheck();
   }
```

Para obtener más información sobre cómo utilizar filtros de mensajes, revise la guía del usuario para su versión de AsyncOS implementada.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems