Errores comunes de configuración en el ESA

Contenido

Introducción

Este documento describe los errores de configuración comunes en el dispositivo de seguridad Email Security Appliance (ESA).

¿Cuáles son los errores de configuración comunes en el ESA?

Tanto si está configurando una nueva evaluación como si está examinando una configuración existente, puede consultar esta lista de comprobación de errores de configuración comunes.

HAT

- No coloque puntuaciones SBRS positivas como +5 o +7 en ALLOWLIST. Un rango de 9.0-10.0 estaría bien, pero incluir puntuaciones más bajas solo hará que sea más probable que el spam llegue.
- Desactive la verificación de DNS del remitente del sobre DESCONOCIDO y la verificación de DNS del host de conexión a menos que realmente las necesite y las entienda.
- En lugar de cambiar el tamaño del mensaje y otros ajustes de política en cada política de flujo de correo, vaya al menú Políticas de flujo de correo y elija la última opción, "Parámetros de política predeterminados".
- Limite el número máximo de conexiones a tres para la mayoría de remitentes, y haga que este sea el valor predeterminado para las nuevas políticas de flujo de correo.
- Verifique que las puntuaciones de SenderBase de -10.0 a -2.0 estén incluidas en la LISTA DE BLOQUEO. Los asistentes de documentación y configuración son demasiado conservadores; actualmente no tenemos falsos positivos en este rango.

Política

- Asigne a las políticas el nombre de quién las obtiene, no de qué hacen. Asigne un nombre a los filtros de contenido después de lo que hacen y utilice abreviaturas como

Q_basic_Attachments, D_spoofers, Strip_Multi-Media, donde Q significa cuarentena y D significa descartar.
- Las políticas no predeterminadas deben ser "Usar configuración predeterminada" para Anti-Spam, Anti-Virus, Filtros de contenido y Filtros de brote de virus, excepto cuando realmente necesite configuraciones especiales. No vuelva a crear esas configuraciones en cada directiva si no es necesario.
- Desmarque "Descartar archivos adjuntos infectados" o, de lo contrario, pasará muchos correos electrónicos en blanco en los que se haya eliminado el virus.
- La configuración antivirus para el correo saliente debe notificar al remitente, no al destinatario
- Los filtros de brote de virus y Anti-Spam deben desactivarse en el

Retransmisiones entrantes

Si "Monitor > Overview" muestra las conexiones de sus propios servidores y dominios, deberá agregarlas a la configuración de Retransmisiones entrantes. Un error muy común, al utilizar la GUI, es pensar que ha habilitado la función de retransmisión entrante cuando todo lo que ha hecho es agregar las entradas a la tabla. Además:

- Agregue un grupo de remitentes HAT especial para ellos, sobre ALLOWLIST, a efectos de generación de informes. Elija no rate limit ni DHAP, pero la detección de spam y virus está bien.
- Agregue un filtro de mensaje para que coincida con la acción de la política BLOCKLIST. Por ejemplo:

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop();}
```

En casos raros en los que se está reinyectando correo electrónico (por ejemplo, reprocesando el correo entre suscriptores a través de la política de correo entrante), el filtro también tendrá que eximir la interfaz de reinyección. Normalmente esto no es necesario.

DNS

Muchos clientes obligan al ESA a consultar sus servidores DNS internos por costumbre. En la mayoría de las instalaciones, el 100% de los registros DNS que necesitamos se encuentran en Internet, no en el DNS interno. Tiene más sentido consultar los servidores raíz de Internet, reduciendo la carga de reenvío en el DNS interno.

Filtros de contenido y mensajes

El error más común es colocar las condiciones coincidentes en los Filtros de contenido donde no se requieren. La mayoría de los filtros deben enumerar algunas acciones, pero la condición debe dejarse en blanco. El filtro será *verdadero* siempre y siempre se ejecutará. Para controlar qué usuarios/políticas reciben estas acciones, cree nuevas políticas de correo entrante o saliente según sea necesario y aplique este filtro a la política. Estos son ejemplos incorrectos y correctos:

- Es casi siempre un error utilizar la condición rcpt-to en un filtro de mensaje. El procedimiento

correcto es escribir un filtro de contenido entrante y hacerlo específico para un usuario concreto mediante la adición de una política de correo entrante basada en el destinatario.
- Es casi siempre un error tener una prueba de filtro de contenido para la presencia de un adjunto y luego descartar el adjunto. El método correcto es descartar siempre ese adjunto, sin probar su presencia.
- Es casi siempre un error utilizar deliver(). Entregar significa omitir los filtros restantes y, a continuación, entregar. Si sólo desea realizar la entrega sin saltar el resto de los filtros, no se requiere ninguna acción explícita (entrega implícita).

Prevención de retransmisión abierta

Algunos servicios comprobarán si el agente de transferencia de mensajes (MTA) acepta direcciones que podrían dar lugar a condiciones de retransmisión abierta. Puesto que dejar su MTA como relé abierto en funcionamiento es incorrecto, estos sitios pueden agregarle a una LISTA BLOQUEADA a menos que rechace estas direcciones peligrosas en la conversación SMTP.

Agregue un grupo de remitentes HAT especial para ellos, sobre ALLOWLIST, a efectos de generación de informes. Elija no rate limit ni DHAP, pero permita la detección de spam y virus.

- Cambiar a análisis de dirección estricta (Loose es el valor predeterminado). Esto es necesario para evitar los signos de @ dobles en las direcciones.
- Rechazar (no eliminar) caracteres no válidos. Esto también es necesario para evitar los signos de @ dobles en las direcciones.
- Rechazar (no aceptar) literales e introducir los siguientes caracteres: *%!\/?

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems