Errores de la configuración común en el ESA

Contenido

Introducción

Este documento describe los errores de la configuración común en el dispositivo de seguridad del correo electrónico (ESA).

¿Cuáles son los errores de la configuración común en el ESA?

Si usted está configurando una nueva evaluación o está mirando sobre una configuración existente, usted puede referir a esta lista de verificación de errores de la configuración común.

1. SOMBRERO

- No ponga las calificaciones positivas SBR como +5 o +7 en el WHITELIST. Un rango de 9.0-10.0 sería ACEPTABLE, pero incluir calificaciones más bajas lo hará solamente más probablemente que el Spam conseguirá a través.
- Inhabilite el UNKNOWNLIST, la verificación del remitente DNS del sobre y la conexión de la verificación del host DNS a menos que usted necesite y entienda realmente éstos.
- En vez del tamaño del mensaje cambiante y de otras configuraciones de la directiva en cada directiva del flujo de correo, van al flujo de correo menú Policies (Políticas) y eligen la última opción, los “parámetros de la política predeterminada”.
- Limite las cantidades máximas de conexiones a tres para la mayoría de los remitentes, y haga esto el valor por defecto para las nuevas directivas del flujo de correo.

- Marque que las calificaciones de SenderBase a partir del -10.0 a -2.0 están incluidas en la LISTA NEGRA. La documentación y los asistentes para la configuración han terminado conservadores; no tenemos actualmente ningún falso positivo en este rango.

2. Política

- Nombre las directivas después de quién lo consigue, no qué él lo hace. Nombre cualquier filtro contento después de lo que él hace, y utilice las abreviaturas como Q_basic_attachments, D_spoofers, Strip_Multi-Media, en donde Q significa que la cuarentena y D significa el descenso.

- Directivas no valor por defecto si “utilice las configuraciones predeterminadas” para el Anti-Spam, el Anit-virus, los filtros contentos y los filtros del brote a menos que donde usted necesita realmente las configuraciones especiales. No reconstruya esas configuraciones en cada directiva si no es necesario.

- Untick “descenso infectó las conexiones” o bien usted pasará encendido muchos correos electrónicos en blanco donde se ha eliminado el virus.

- Las configuraciones del contra virus para saliente deben notificar el remitente, no el beneficiario

- Los filtros y el Anti-Spam del brote se deben inhabilitar en saliente

3. Retransmisiones entrantes

Si el “monitor > la descripción” muestra las conexiones de sus propios servidores y dominios, usted necesita agregarlos a la configuración entrante de las retransmisiones. Mismo un error común, al usar el GUI, es pensar que usted ha habilitado la función de relay entrante cuando es todo lo que usted ha hecho agrega las entradas a la tabla. Además:

- Agregue un grupo especial del remitente del SOMBRERO para ellas, sobre el WHITELIST, para señalar los propósitos. No elija ninguna limitación de la tarifa o DHAP, sino mande spam y la detección del virus es ACEPTABLE.

- Agregue un filtro del mensaje para hacer juego su acción de política de la LISTA NEGRA. Por ejemplo:

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

En los casos pocos probables donde usted está reinyectando el email (por ejemplo, tratando de nuevo el correo del inter-suscriptor con la directiva entrante del correo), su filtro también necesitará eximir la interfaz del reinjection. Esto no es normalmente necesario.

4. DNS

Muchos clientes fuerzan el ESA para preguntar a sus servidores DNS internos fuera del hábito. En la mayoría de las instalaciones, el 100% de los expedientes DNS que necesitamos está en Internet, no en los DN internos. Tiene más sentido de preguntar a los servidores de raíz de Internet, reduciendo la carga de la expedición en los DN internos.

5. Filtros del mensaje y del contenido

La mayoría del error común es poner las condiciones que corresponden con en los filtros contentos donde no se requieren. La mayoría de los filtros deben enumerar algunas acciones, pero la condición se debe dejar en blanco. El filtro será *verdad* siempre, y se ejecutará siempre. Usted controla que los usuarios/las directivas reciben estas acciones creando las nuevas directivas entrantes o salientes del correo según las necesidades, y aplicando este filtro a la directiva. Aquí están los ejemplos incorrectos y correctos:

- Es casi siempre un error para utilizar RCPT-a la condición en un filtro del mensaje. El procedimiento correcto es escribir un filtro contento entrante, y hace específico para un usuario determinado agregando una directiva beneficiario-basada del correo entrante.

- Es casi siempre un error para tener una prueba contenta del filtro para la presencia de una conexión, después cae la conexión. El método correcto es caer siempre esa conexión, sin la prueba para su presencia.

- Es casi siempre un error para utilizar el deliver(). Entregue significa el salto cualquier filtro restante, después lo entrega. Si usted apenas quiere entregar sin saltar el resto de los filtros, no se requiere ninguna acción explícita (implicado entregue).

7. Abra la prevención de la retransmisión

Algunos servicios marcarán para considerar si su agente de transferencia de mensajes (MTA) valida los direccionamientos que potencialmente podrían dar lugar a las condiciones abiertas de la retransmisión. Puesto que dejar su MTA como retransmisión abierta de funcionamiento es malo, estos sitios pueden agregarle a las listas negras a menos que usted rechace estos direccionamientos peligrosos en la conversación SMTP.

Agregue un grupo especial del remitente del SOMBRERO para ellos, sobre el WHITELIST, para señalar los propósitos. No elija ninguna limitación de la tarifa o DHAP, sino permita la detección del Spam y del virus.

- Cambie al direccionamiento estricto que analiza (Loose es el valor por defecto). Esto es necesario prevenir el doble @ ingresa los direccionamientos.

- Caracteres no válidos del rechazo (no tira). Esto es también necesario prevenir el doble @ ingresa los direccionamientos.

- Rechace (no validar) los literales, y ingrese los caracteres siguientes: ¡el *%! ¿\ \/?

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems