El ESA experimenta una tormenta de la despedida (NDR)

Contenido

Introducción

Este documento describe un problema encontrado donde su dispositivo de seguridad del correo electrónico (ESA) experimenta una tormenta de la despedida y ofrece una solución al problema.

Antecedentes

Una tormenta de la despedida es un efecto secundario de un trabajo de Joe o de un retrodifusor del Spam del correo electrónico.

Trabajo de Joe

Un trabajo de Joe es un ataque del Spam que utiliza los datos y los objetivos del remitente del spoofed para deslustrar la reputación del remitente evidente y/o para inducir a los beneficiarios que tomen medidas contra el remitente evidente.

Retrodifusor

Un retrodifusor es un efecto secundario del Spam del correo electrónico, virus, y los gusanos donde los servidores de correo electrónico que reciben el Spam y el otro correo envían los mensajes de despedida a una parte inocente. Esto ocurre porque el remitente del sobre del mensaje original se forja para contener la dirección de correo electrónico de la víctima. Puesto que estos mensajes no fueron solicitados por los beneficiarios, son substancialmente similares el uno al otro, y se entregan en las cantidades a granel, califican como el correo electrónico o Spam

a granel no solicitado. Como tal, los sistemas que generan el retrodifusor del correo electrónico pueden llegar a ser mencionados en las diversas listas negras del Sistema de nombres de dominio (DNS) (DNSBLs) y estar con violación de los términos de los Proveedores de servicios de Internet del servicio.

Problema

Su ESA experimenta una tormenta de la despedida donde hay un diluvio de los mensajes inyectados en el ESA. Los puntos de la cuenta de la conexión entrante durante tal ataque. La aplicación pudo desarrollar un respaldo del workqueue. Para verificar si el dispositivo está conforme a tal ataque, grep que el correo registra para el correo del direccionamiento. Despide (informes de la falta de entrega - Los NDR) tienen un correo vacío del sobre del direccionamiento.

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

Un dispositivo que está conforme a una tormenta de la despedida tendrá la mayoría de los mensajes con el correo del sobre del direccionamiento del “**<>**”.

Solución

Hay varias opciones para manejar una tormenta de la despedida.

Verificación de la despedida

Para combatir estos ataques dirigidos mal de la despedida, AsyncOS incluye la verificación de la despedida de Cisco. Cuando está habilitada, esta característica marca el direccionamiento del remitente con etiqueta del sobre para los mensajes enviados vía el ESA. Entonces marcan al beneficiario del sobre para cualquier mensaje de despedida recibido por el ESA para saber si hay la presencia de esta etiqueta. Cuando se reciben los mensajes de despedida legítimos, la etiqueta que fue agregada al remitente del sobre que se quita el direccionamiento y la despedida se entrega al beneficiario. Los mensajes de despedida que no contienen la etiqueta se pueden manejar por separado.

AsyncOS considera las despedidas como correo con un correo nulo del direccionamiento (**<>**). Los mensajes que son de los direccionamientos tales como mailer-daemon@example.com o postmaster@example.com no son considerados las despedidas por el sistema y no están conforme a la verificación de la despedida.

Direccionamiento de la verificación de la despedida de la configuración que marca las claves con etiqueta

El direccionamiento de la verificación de la despedida que marca el anuncio de claves con etiqueta muestra que su clave y cualquier actuales unpurged le cierra utilizó en el pasado. Para agregar una nueva clave, complete estos pasos:

1. En las **directivas del correo >** la página de la **verificación de la despedida**, haga clic la **nueva clave**.

2. Ingrese una cadena de texto y el tecleo **somete**.

3. Confíe sus cambios.

Purga de las claves

Usted puede purgar su viejo direccionamiento que marca las claves con etiqueta si usted selecciona una regla para purgar del menú desplegable y hace clic la **purgación.**

Configuraciones de la verificación de la despedida de Cisco de la configuración

Las configuraciones de la verificación de la despedida determinan que acción a tomar cuando se recibe una despedida inválida.

- Elija las **directivas del correo** > la **verificación de la despedida**.
- El tecleo **edita las configuraciones**.
- Seleccione si rechazar las despedidas inválidas o agregar una encabezado de encargo al mensaje. Si usted quiere agregar una encabezado, ingrese el nombre y el valor de la encabezado.
- Opcionalmente, habilite las excepciones elegantes. Esta configuración permite los mensajes del correo entrante y los mensajes de despedida generados por los servidores de correo interno que se eximirán automáticamente del proceso de la verificación de la despedida (incluso cuando utilizan a un solo módulo de escucha para el correo entrante y saliente).
- Someta y confíe sus cambios.

Configure la verificación de la despedida de Cisco con el CLI

Usted puede utilizar los comandos del **bvconfig** y del **destconfig** en el CLI para configurar la verificación de la despedida. Estos comandos se discuten en el guía de referencia de Cisco AsyncOS CLI.

Verificación y configuración de clúster de la despedida de Cisco

La verificación de la despedida trabaja en una configuración de clúster mientras ambos dispositivos de Cisco utilicen la misma “clave de la despedida.” Cuando usted utiliza la misma clave, cualquier sistema debe poder validar un bounceback legítimo. La etiqueta/la clave modificadas de la encabezado no es específicas a cada dispositivo de Cisco.

Filtro de correo

Si usted no puede utilizar la verificación de la despedida porque usted utiliza los dispositivos separados para el recibo y la salida, usted puede configurar un filtro del mensaje para bloquear los mensajes que tienen un correo vacío del direccionamiento.

Bloque del correo

Puesto que estos mensajes de despedida tendrán muy probablemente un direccionamiento receptor del sobre inexistente, usted puede las direcciones no válidas de bloque vía la validación receptora del Lightweight Directory Access Protocol (LDAP) de la conversación para ayudar más bajo al impacto de tales mensajes.