Configuración de la lista de excepciones de dominio de remitente para gateway de correo electrónico seguro

Contenido

Introducción

En este documento se describen los "Nuevos cambios" de la opción de configuración de Reputación de dominio del remitente (SDR) Lista de excepciones de dominio para Cisco Secure Email Gateway (SEG).

Colaboración de Chris Arellano, ingeniero del TAC de Cisco.

Prerequisites

Se requiere un conocimiento general de los parámetros y la configuración de SEG.

AsyncOS 15.0 y posterior para Cisco Secure Email Gateway (SEG).

Comprensión general de la función SDR.

Requirements

Habilite el servicio de reputación de dominio del remitente y cree una lista de direcciones con la opción Domain Only.

Componentes Utilizados

- La información que contiene este documento se basa en las siguientes versiones de software y hardware.
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 y versiones posteriores.

- Reputación de dominio de remitente SEG.
- Lista de direcciones.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Sender Domain Reputation es un servicio en la nube que recopila varios valores de remitentes, deriva veredictos y proporciona opciones para tomar medidas en función de dichos veredictos. SDR permite a la configuración omitir los dominios de confianza mediante el uso de una lista de direcciones aplicada a la lista de excepciones de dominio.

La Lista de excepciones de dominio SDR en las versiones de AsynOS anteriores a SEG 15.0 tenía 2 opciones:

- Habilitado = Coincide con el dominio de origen del sobre para omitir la acción de SDR.
- Desactivado = Coincidir sólo si todos están presentes: Desde sobre + De descriptivo + Responder a + SPF + DKIM + DMARC .

La Lista de excepciones de dominio para SEG 15.0 y las opciones más recientes:

- Habilitado = Coincide con el dominio de origen del sobre para omitir la acción de SDR.
- Deshabilitado = Coincidir si el dominio está presente en cualquiera de los valores:
    - HELO
    - RDNS
    - De sobre
    - Desde
    - Responder a

Configurar

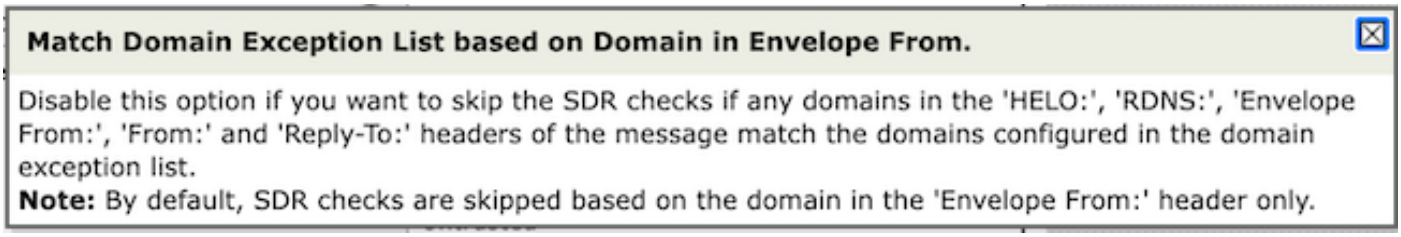
El enfoque de este artículo es solo la nueva configuración de la Lista de excepciones de dominio. La guía del usuario incluye la configuración y la instalación completa de SDR.

Navegue dentro de la interfaz de usuario web hasta Servicios de seguridad > Reputación de dominio.

- La opción Coincidir con la lista de excepciones de dominio basada en la parte del nombre de dominio del remitente del sobre está activada de forma predeterminada.
    - Si la casilla de verificación está activada, sólo el valor "De sobre, encabezado" coincidirá con el mensaje y lo omitirá en caso de condena.
    - Si la casilla de verificación está en blanco, la lista de excepciones de dominio de SDR coincidirá con cualquiera de estos campos de encabezado: 'HELO:', 'RDNS:', 'Envelope From:', 'From:' y 'Reply-To:', coincidirá con el mensaje y lo omitirá si se le

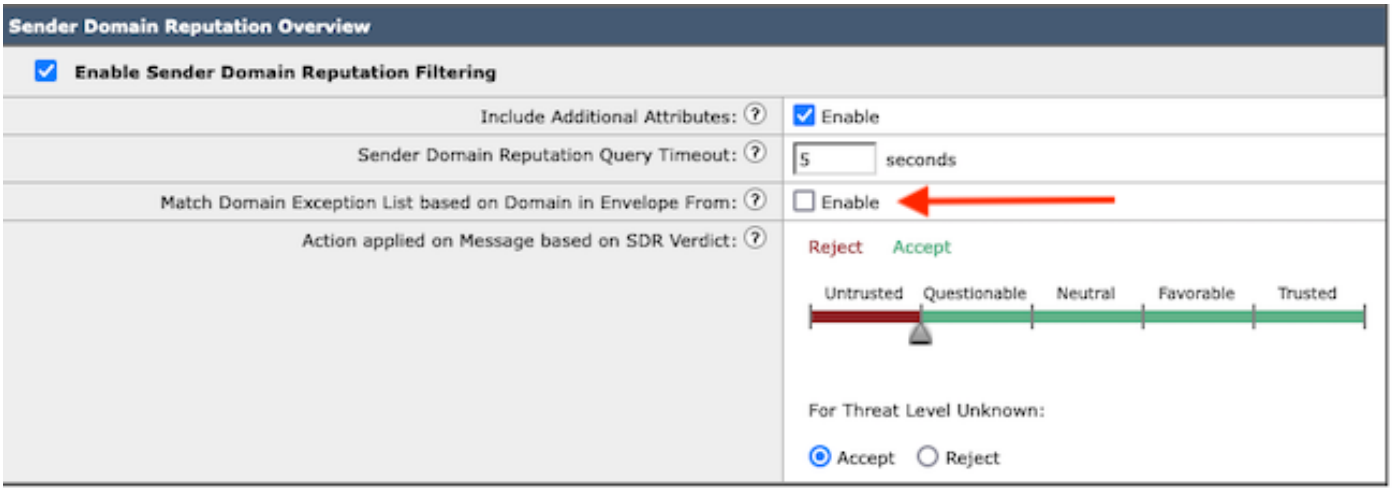
considera culpable.

Si el icono ? informativo asociado está seleccionado, se muestran los detalles de la configuración.



Nota: de forma predeterminada, las comprobaciones de SDR se omiten en función del dominio del encabezado 'De sobre:' solamente.

Seleccione Edit Global Settings para quitar la opción de casilla de verificación, como se muestra en la imagen:



La Lista de excepciones de dominio en sí es una Lista de direcciones que contiene nombres de dominio.

Verificación

Para verificar el funcionamiento correcto utilizando la nueva funcionalidad de Desactivar, se requiere un mensaje de prueba enviado al SEG con un valor de dominio coincidente en uno de los 5 valores de encabezado.

Un registro de ejemplo que indica una excepción dentro de la Lista global de excepciones y que coincide dentro de una política de flujo de correo presentaría en la etapa inicial a mail_logs:

```
Info: MID 14 SDR: MID 14 containing domain name'test1.example.com' matched the global domain exception
```

Un registro de ejemplo que indica una excepción contendría el dominio y el nombre de la lista de

excepciones.

```
Info: MID 16 containing domain name 'test3.example.com' matched the domain exception list 'SDR-TEST-3'
```

Troubleshoot

Si surgen preguntas sobre la precisión de un veredicto de mensaje seleccionado, los valores se documentan y se comparan con el seguimiento de mensajes.

- Documente la Configuración de Reputación de Dominio Global > Configuración de Seguridad > Reputación de Dominio.
- Verifique la lista de direcciones asociada configurada en la configuración de Reputación de dominio global.
- Verifique la política de flujo de correo coincidente basada en el rastreo de mensajes.
- Compruebe y anote los detalles de cualquier filtro de mensajes o filtro de contenido con listas de excepciones de dominio configuradas.

Recopile Rastreo de mensajes, registros de correo y los encabezados de correo electrónico originales.

- Si la excepción global coincide en un mensaje, no hay entradas de registro para Reputación de dominio, simplemente una línea que indica el dominio coincidente.
- Si la Lista global de excepciones no coincide en un mensaje, hay entradas de registro para Reputación de dominio desde las que comparar valores.
    - Información: MID 16 SDR: Dominios para los que se solicita SDR: host DNS inverso: No presente, helo: mail1.example.com, env-from: test2.example.com, header-from: te destination.example.com, responder a: test2.example.com
- Los encabezados de correo electrónico incluyen cualquiera de los 5 valores presentes en un correo electrónico individual para compararlos con la configuración.

Una vez recopilados todos los datos, compruebe si hay coincidencias o falta de coincidencias para determinar la funcionalidad adecuada.

Información Relacionada

- Guía de configuración de Email Security
- Página de inicio de Cisco Secure Email Gateway para las guías de asistencia

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).