# Cómo permitir campañas simuladas de plataforma de suplantación de identidad a través de Cisco Email Security Appliance

## Contenido



## Introducción

Este documento describe los pasos de configuración en Cisco Email Security Appliance (ESA) para permitir campañas simuladas de plataformas de suplantación de identidad correctamente.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Creación de filtros de mensajes y contenido en el ESA.
- Configuración de la tabla de acceso de host (HAT).
- Información sobre el flujo de correo electrónico entrante de Cisco ESA.

### Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

Las plataformas simuladas de suplantación de identidad permiten a los administradores ejecutar campañas de suplantación de identidad como parte de un ciclo para gestionar una de las amenazas más importantes que utiliza los sistemas de correo electrónico como vector de ataques de ingeniería social.

# Problema

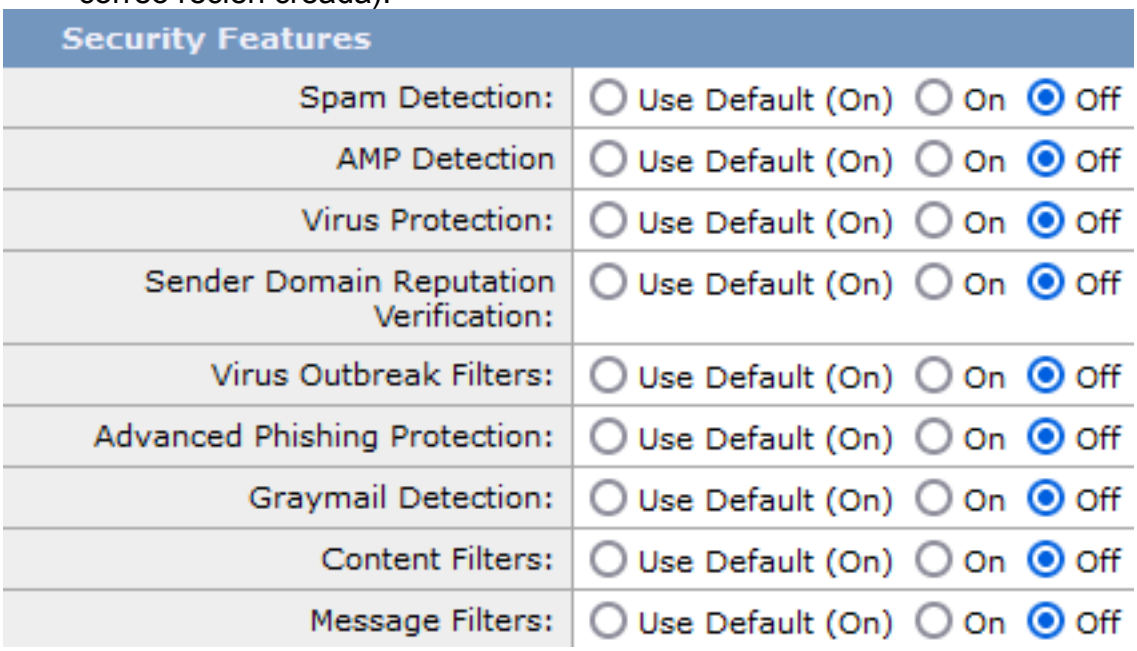
Cuando el ESA no está preparado para tales simulaciones, no es raro que sus motores de escaneo detengan los mensajes de campaña de suplantación de identidad, lo que da lugar a fallos o a una disminución de la eficacia de las simulaciones.

# Solución

> **Precaución:** En este ejemplo de configuración, se selecciona *TRUSTED* mail flow policy para permitir que el ESA pase por campañas simuladas de phishing más grandes sin ninguna limitación. La ejecución continua de campañas de suplantación de identidad de gran volumen puede afectar al rendimiento del procesamiento del correo electrónico.

Para asegurarse de que ningún componente de seguridad de la configuración ESA debe poner en marcha los mensajes de campaña de suplantación de identidad.

1. Crear un nuevo grupo de remitentes: **GUI > Políticas de correo > Descripción general de HAT** y enlazarla a la política de flujo de correo *TRUSTED* (alternativamente, se puede crear una nueva política con opciones similares bajo **GUI > Políticas de correo > Políticas de flujo de correo**).
2. Agregue los hosts de envío o las IP de la plataforma de suplantación de identidad simulada a este grupo de remitentes. Si la plataforma de suplantación de identidad simulada tiene un amplio rango de IP, puede agregar nombres de host parciales en su lugar o rangos de IP si corresponde.
3. Ordene el Grupo de Enviadores sobre su Grupo de Enviadores *BLOCKLIST* para asegurarse de que se hace una correspondencia estática en lugar de SBRS.
4. Inhabilite toda la función de seguridad para la política de flujo de correo *TRUSTED* bajo **GUI > Políticas de correo > Políticas de flujo de correo > CONFIABLE** (o su política de flujo de correo recién creada):




5. **Envíe estos cambios y confirme.**

**Precaución:** En este ejemplo de configuración, se selecciona *TRUSTED* mail flow policy para permitir que el ESA pase por campañas simuladas de phishing más grandes sin ninguna limitación. La ejecución continua de campañas de suplantación de identidad de gran volumen puede afectar al rendimiento del procesamiento del correo electrónico.

Para asegurarse de que ningún componente de seguridad de la configuración ESA debe poner en marcha los mensajes de campaña de suplantación de identidad.

1. Crear un nuevo grupo de remitentes: **GUI > Políticas de correo > Descripción general de HAT** y enlazarla a la política de flujo de correo *TRUSTED*.
2. Agregue los hosts de envío o las IP de la plataforma de suplantación de identidad simulada a este grupo de remitentes. Si la plataforma de suplantación de identidad simulada tiene un amplio rango de IP, puede agregar nombres de host parciales en su lugar o rangos de IP si corresponde.
3. Ordene el Grupo de Enviadores sobre su Grupo de Enviadores *BLOCKLIST* para asegurarse de que se hace una correspondencia estática en lugar de SBRS.
4. **Envíe estos cambios y confirme.**
5. Navegue hasta la CLI y agregue un nuevo filtro de mensajes, **CLI > Filtros,** copie y modifique la sintaxis y agregue el filtro.
6. 
```
skip_engines_for_simulated_phishing:
if (sendergroup == "name_of_the_newly_created_sender_group")
{
insert-header("x-sp", "uniquevalue");
log-entry("Skipped scanning engines for simulated phishing");
skip-spamcheck();
skip-viruscheck();
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
skip-filters();
}
.
```
7. Pida el filtro de mensajes en la lista para asegurarse de que no se salte con otro filtro de mensaje encima del mismo, que incluye la acción de omisión de filtros.
8. Pulse la tecla Intro para volver al símbolo del sistema principal de AsyncOS y ejecute el comando "**commit**" para registrar los cambios. (no haga clic en CTRL+C: borrará todos los cambios).
9. Vaya a la **GUI> Políticas de correo > Filtros de contenido entrante**
10. Cree un nuevo filtro de contenido entrante con la condición ***"Otro encabezado"*** establecida para buscar el encabezado personalizado **"x-sp"** y su valor **único** configurado en el filtro de mensaje y configure la acción Omitir filtros de contenido restante (Acción final).
11. Pida el filtro de contenido a "1" para asegurarse de que otros filtros no actuarán contra el mensaje de suplantación de identidad simulado.
12. Navegue hasta **GUI > Políticas de correo > Políticas de correo entrante** y asigne el filtro de contenido a la política requerida.
13. **Enviar y registrar cambios.**

14. Ejecute la campaña de la plataforma de suplantación de identidad simulada y supervise los registros_de_correo/Rastreo de mensajes para verificar la coincidencia de reglas de flujo y políticas.