Crear una directiva de la lista blanca en Cisco ESA para las pruebas de la educación del phishing

Contenido

Introducción

Este documento describe cómo crear una directiva de la lista blanca en el caso de la Seguridad del correo electrónico del dispositivo de seguridad (ESA) o de la nube del correo electrónico de Cisco (CES) para permitir las pruebas/las campañas de la educación del phishing.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Navegando y configurando las reglas en Cisco ESA/CES en el WebUI.
- Crear los filtros del mensaje en Cisco ESA/CES en el comando line interface(cli).
- Conocimiento del recurso usado para la campaña/la prueba del phishing.

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.

Antecedentes

Los administradores que ejecutan las pruebas o las campañas de la educación del phishing tendrán correos electrónicos generados con la información que será correspondida con contra las reglas actuales de Talos en los conjuntos de la regla para filtros del Anti-Spam y/o del brote. En tal evento, los correos electrónicos de la campaña del phishing no alcanzarán a los usuarios finales y actioned por Cisco ESA/CES sí mismo que causa así la prueba a un alto. Los administradores necesitarían asegurarse que el ESA/CES permita a través de estos correos electrónicos realizar su campaña/prueba.

Configurar

> **Advertencia:** La postura de Cisco en los vendedores whitelisting de la simulación y de la educación del phishing global no se permite. Aconsejamos a los administradores trabajar con el servicio del simulador del phishing *(por ejemplo: PhishMe)* para obtener sus IP entonces los agrega localmente a la lista blanca. Cisco debe proteger a nuestros clientes ESA/CES contra esos IP si cambian nunca las manos o hacen realmente una amenaza.

> Precaución: Los administradores deben mantener solamente estos IP una lista blanca mientras que prueban, dejar el externo IP en una prueba del poste de la lista blanca durante un largo período de tiempo puede traer no solicitado o los correos electrónicos malévolos a los usuarios finales estos IP se comprometen.

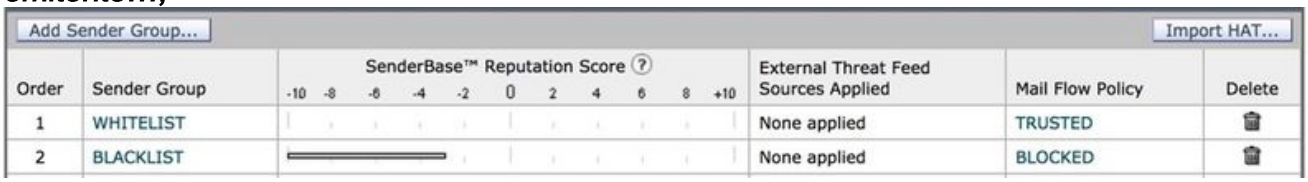
En el dispositivo de seguridad del correo electrónico de Cisco (ESA), cree un nuevo grupo del remitente para su simulación del phishing y asígnelo a la directiva del flujo de correo $TRUSTED. Esto permitirá que todos los correos electrónicos de la simulación del phishing sean entregados a los usuarios finales. Los miembros de este nuevo grupo del remitente no están conforme a la tarifa que limita, y el contenido de esos remitentes no es analizado por el motor antispam de Cisco IronPort, sino todavía es analizado por el software del contra virus.

> Nota: Por abandono, la directiva del flujo de correo $TRUSTED tiene el contra virus habilitado pero Anti-Spam apagado.

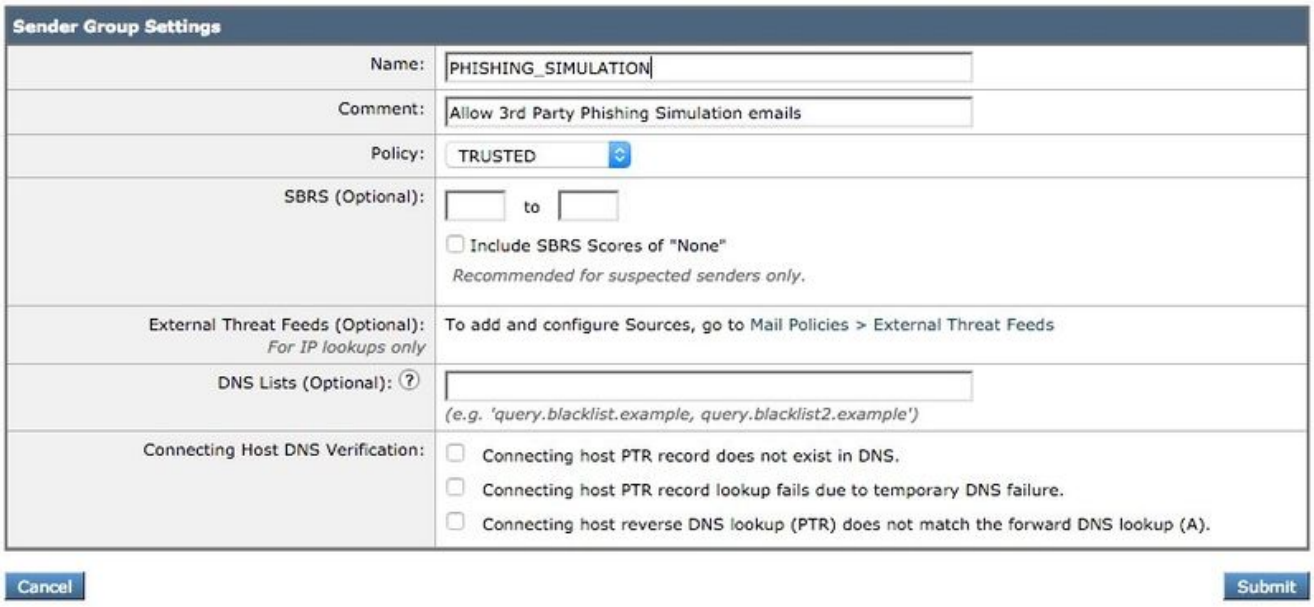
Crear el grupo del remitente

1. Haga clic la lengueta de las ***directivas del correo***.
2. Bajo sección de la ***tabla del acceso del host***, seleccione la ***descripción del SOMBRERO***

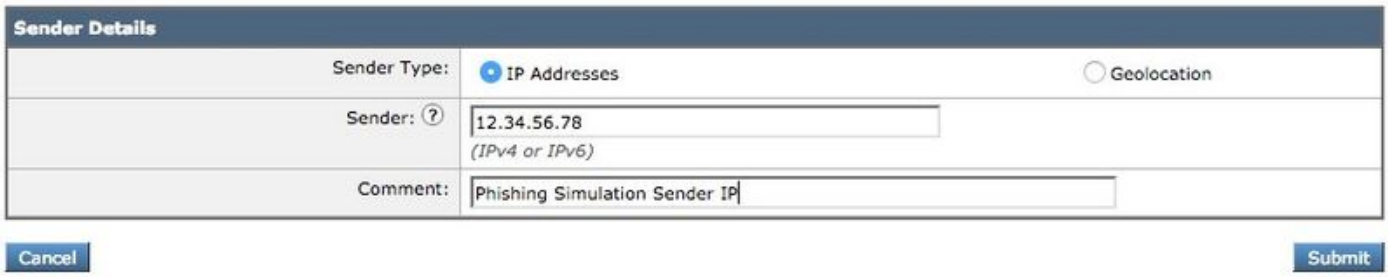
3. A la derecha, aseegurese a su módulo de escucha de ***InboundMail*** se selecciona actualmente,
4. De la columna del ***grupo del remitente*** abajo, el tecleo ***agrega el grupo del remitente…,***



5. Complete el ***nombre*** y los ***campos de comentario***. Bajo ***directiva*** dropdown, "**$TRUSTED** selectos" y entonces hacen clic ***someten y agregan los remitentes >>.***



6. Ingrese el IP o el nombre de host que usted quiere a Whitelist en el primer campo. Su partner de la simulación del phishing proveerá de usted la información IP del remitente.



Cuando usted acaba de agregar las entradas, haga clic el ***botón Submit Button***. Recuerde hacer clic los ***cambios del cometer*** abotonan para salvar sus cambios.

Crear el filtro del mensaje

Después de crear el grupo del remitente para permitir puente del Anti-Spam y del contra virus, un filtro del mensaje se requiere para saltar los otros motores de la Seguridad que pueden hacer juego la campaña/la prueba del phishing.

1. Conecte con el CLI del ESA.
2. Funcione con los ***filtros del*** comando.
3. Funcione con el comando new de crear un nuevo filtro del mensaje.
4. La copia y pega el ejemplo siguiente del filtro, haciendo edita para sus nombres del grupo reales del remitente si es necesario:

```
skip_amp_graymail_vof_for_phishing_campaigns:
if(sendergroup == "PHISHING_SIMULATION")
{
skip-ampcheck();
skip-marketingcheck();
skip-socialcheck();
skip-bulkcheck();
skip-vofcheck();
}
```

5. Vuelva al prompt principal y al Presione ENTER CLI.
6. Ejecute el ***cometer*** para salvar la configuración.

Verificación

Utilice el recurso de tercera persona para enviar una campaña/una prueba del phishing y verificar los resultados en Seguimiento de mensajes los registros para asegurar todos los motores fueron saltados y el correo electrónico fue entregado.