Resolución de fallos de DMARC mediante la corrección de la alineación SPF y DKIM

Contenido

Problema

Cisco Secure Email Gateway (CES/ESA) bloquea los correos electrónicos de dominios específicos debido a fallos de verificación de DMARC. El análisis del seguimiento de mensajes indica que estos correos electrónicos se mantienen en la cola de trabajo y se ponen en cuarentena o se rechazan, lo que impide que lleguen a los destinatarios deseados.

Entorno

- Dispositivos Cisco Secure Email Gateway (CES/ESA)
- Se configuran y aplican las políticas SPF, DKIM y DMARC

Resolución

Tabla de resumen de alineación de SPF/DKIM (ejemplos)

Mecanismo	Estado de alineación	Dominio de sobre/firma	Desde dominio de encabezado	Lógica
SPF	En alineación	sender@example.com	sender@example.com	Coincidencia directa

SPF	En alineación	sender@child.example.com	sender@example.com	Coincidencia de dominio principal
SPF	No en alineación	sender@test.com	sender@example.com	Discordancia de dominio
DKIM	En alineación	example.com	sender@example.com	Coincidencia directa
DKIM	En alineación	example.com	sender@child.example.com	Coincidencia de modo relajado
DKIM	No en alineación	example.com	sender@test.com	Discordancia de dominio

Coordinar con remitente (recomendado)

- Colabore con los administradores del dominio del remitente para remediar los fallos de DMARC garantizando una alineación SPF y DKIM adecuada en el nivel del encabezado.
- El remitente debe:
    - Asegúrese de que el dominio utilizado en la identidad MAIL FROM o HELO/EHLO validada por SPF esté alineado con el dominio en el encabezado From del correo electrónico.
    - Implemente la firma DKIM donde el dominio especificado en la etiqueta d= de la firma DKIM esté alineado con el dominio del encabezado From.
    - Compruebe que la política de DMARC está correctamente configurada para aplicar el modo de alineación deseado (estricto o relajado) y las opciones de informes.
- Este enfoque aborda la causa raíz de los fallos de DMARC centrándose en la alineación de los dominios autenticados con el dominio de encabezado De visible, que es fundamental para la entrega de correo electrónico a largo plazo.

Crear excepción de DMARC (alternativa)

- Si la remediación por parte del remitente no es factible, cree una excepción en el dispositivo ESA para que la dirección del remitente específico omita las comprobaciones de DMARC.
- Se trata de una solución temporal y debe ir acompañada de supervisión.

Supervisión y validación

- Después de implementar los cambios, supervise la entrega de correos electrónicos de alerta a los destinatarios deseados.
- Revise los registros de seguimiento de mensajes para confirmar que se han resuelto los fallos de DMARC.
- Continúe analizando los datos de seguimiento de mensajes actualizados si persisten los problemas de entrega.

Causa

La causa principal de cuarentena o rechazo de correo electrónico es un error de verificación de DMARC debido a problemas de alineación de SPF y DKIM. Estos errores indican que, aunque los registros SPF y DKIM se pueden publicar correctamente, los dominios autenticados durante el intercambio de correo electrónico no se alinean con el dominio de encabezado De, lo que da lugar a la cuarentena de correos electrónicos.

Descripción de la alineación de DMARC, SPF y DKIM:

- SPF autentica el dominio en los comandos MAIL FROM o HELO/EHLO SMTP y requiere que este dominio se alinee con el dominio en el encabezado From para cumplir con DMARC.
- DKIM utiliza firmas criptográficas con un dominio de firma especificado en la etiqueta d=, que debe alinearse con el dominio de encabezado From.
- DMARC se basa en SPF y DKIM al exigir que al menos uno de estos dominios autenticados se alinee con el dominio de encabezado From, ya sea exactamente (modo estricto) o como subdominio (modo relajado).

El fallo de esta alineación de dominios provoca fallos en DMARC y el consiguiente rechazo o cuarentena de correos electrónicos, incluso si los registros SPF y DKIM se publican

correctamente y son válidos.

Este enfoque de alineación garantiza que la identidad autenticada coincida con la identidad visible del remitente, lo que evita la suplantación y mejora la fiabilidad del correo electrónico.

Contenido relacionado

- Información de alineación SPF
- Información de alineación DKIM
- Prácticas recomendadas para la autenticación de correo electrónico: formas óptimas de implementar SPF, DKIM y DMARC (Cisco)
- Configuración del filtro de entrada basado en la verificación DKIM en ESA - Cisco

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).