Risolvere gli errori DMARC correggendo l'allineamento di SPF e DKIM

Sommario

Problema

Le e-mail da domini specifici vengono bloccate da Cisco Secure Email Gateway (CES/ESA) a causa di errori di verifica DMARC. L'analisi della verifica dei messaggi indica che questi messaggi di posta elettronica vengono conservati nella coda di lavoro e messi in quarantena o rifiutati, impedendo loro di raggiungere i destinatari previsti.

Ambiente

- Appliance Cisco Secure Email Gateway (CES/ESA)
- I criteri SPF, DKIM e DMARC sono configurati e applicati

Risoluzione

Tabella di riepilogo dell'allineamento SPF/DKIM (esempi)

Meccanismo	Stato allineamento	Envelope/Signature Domain	Da dominio intestazione	Logica
SPF	In allineamento	sender@example.com	sender@example.com	Corrispondenza diretta

SPF	In allineamento	sender@child.example.com	sender@example.com	Corrispondenza dominio padre
SPF	Non in allineamento	sender@test.com	sender@example.com	Dominio non corrispondente
DKIM	In allineamento	example.com	sender@example.com	Corrispondenza diretta
DKIM	In allineamento	example.com	sender@child.example.com	Corrispondenza modalità rilassata
DKIM	Non in allineamento	example.com	sender@test.com	Dominio non corrispondente

Coordina con il mittente (scelta consigliata)

- Collaborare con gli amministratori del dominio mittente per correggere gli errori DMARC garantendo un corretto allineamento SPF e DKIM a livello di intestazione.
- Il mittente deve:
    - Verificare che il dominio utilizzato nell'identità MAIL FROM o HELO/EHLO convalidata da SPF sia allineato al dominio nell'intestazione From del messaggio di posta elettronica.
    - Implementare la firma DKIM quando il dominio specificato nel tag d= della firma DKIM è allineato al dominio dell'intestazione From.
    - Verificare che i criteri DMARC siano configurati correttamente per applicare la modalità di allineamento (rigorosa o rilassata) e le opzioni di report desiderate.
- Questo approccio affronta la root cause dei guasti DMARC concentrandosi sull'allineamento dei domini autenticati con il dominio dell'intestazione From visibile, che è fondamentale per il recapito della posta elettronica a lungo termine.

Crea eccezione DMARC (alternativa)

- Se non è possibile ovviare al problema da parte del mittente, creare un'eccezione sul dispositivo ESA affinché l'indirizzo specifico del mittente ignori i controlli DMARC.
- Si tratta di una soluzione temporanea che deve essere accompagnata da un monitoraggio.

Monitoraggio e convalida

- Dopo aver implementato le modifiche, monitorare il recapito dei messaggi di posta elettronica di avviso ai destinatari previsti.
- Esaminare i log di verifica dei messaggi per verificare che gli errori DMARC siano stati risolti.
- Continua ad analizzare i dati di verifica dei messaggi aggiornati se persistono problemi di recapito.

Causa

La causa principale della quarantena o del rifiuto della posta elettronica è un errore di verifica DMARC causato da problemi di allineamento SPF e DKIM. Questi errori indicano che, sebbene i record SPF e DKIM possano essere pubblicati correttamente, i domini autenticati durante lo scambio di e-mail non sono allineati con il dominio dell'intestazione From, con conseguente quarantena dei messaggi di posta elettronica.

Informazioni sull'allineamento DMARC, SPF e DKIM:

- SPF autentica il dominio nei comandi SMTP MAIL FROM o HELO/EHLO e richiede che questo dominio sia allineato al dominio nell'intestazione From per la conformità DMARC.
- DKIM utilizza firme crittografiche con un dominio di firma specificato nel tag d=, che deve essere allineato con il dominio dell'intestazione From.
- DMARC si basa su SPF e DKIM richiedendo che almeno uno di questi domini autenticati sia allineato al dominio dell'intestazione From, esattamente (modalità strict) o come sottodominio (modalità rilassata).

Il mancato allineamento di questo dominio porta a errori DMARC e al successivo rifiuto o quarantena dell'e-mail, anche se i record SPF e DKIM stessi sono correttamente pubblicati e validi.

Questo elemento di allineamento garantisce che l'identità autenticata corrisponda all'identità visibile del mittente, impedendo lo spoofing e migliorando l'affidabilità della posta elettronica.

Contenuto correlato

- Informazioni sull'allineamento SPF
- Informazioni sull'allineamento DKIM
- Best practice per l'autenticazione e-mail - Metodi ottimali per installare SPF, DKIM e DMARC - Cisco
- Configurazione del filtro in entrata in base alla verifica DKIM in ESA - Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).