Perché l'ESA gestisce il risultato dell'autenticazione DKIM come "permfail"?

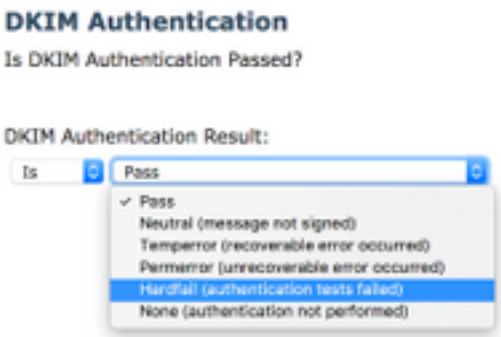
Sommario

Introduzione

In questo documento viene descritto come Email Security Appliance (ESA) gestisce i risultati dell'autenticazione DKIM (DomainKeys Identified Mail).

Perché l'ESA gestisce il risultato dell'autenticazione DKIM come "permfail"?

La condizione del filtro contenuti ESA Autenticazione DKIM dispone di diverse opzioni, come mostrato in questa immagine:



Quando la condizione DKIM Authentication Result è impostata su **Hardfail**, i messaggi consentfail vengono visualizzati nel file di log di posta e nei messaggi rilevati, come mostrato nell'esempio seguente:

Message 815204 DKIM: permfail body hash did not verify [final] (d=sub.example.com s=selector1-sub-com i=@sub.example.com)

L'ESA considera che permfail sia uguale all'hardfail e include il risultato nell'intestazione Authentication-Results come dkim=hardfail. I nomi ESA per gli eventi DKIM sono diversi dai nomi RFC6376. Nelle intestazioni dei risultati di autenticazione (e nei messaggi tracciati), ESA deve mostrare stringhe RFC6376 corrette, mentre il filtro dei contenuti usa nomi di eventi diversi.

Questi eventi sono mappati: RFC6376.PERMFAIL == Errore hardware filtro contenuto ESA

Gli errori di verifica dell'hash del corpo del messaggio e della firma costituiscono la maggior parte degli errori di verifica. Gli errori di verifica dell'hash del corpo indicano che il corpo del messaggio non corrisponde al valore hash (digest) nella firma. Gli errori di verifica della firma indicano che il valore della firma non verifica correttamente i campi dell'intestazione firmata (che includono la firma stessa) nel messaggio.

Le cause possibili di questi due errori sono diverse. Il messaggio potrebbe essere stato modificato durante la trasmissione (ad esempio da una lista di distribuzione o da un mittente); la firma o i valori hash potrebbero essere stati calcolati o applicati in modo non corretto dal firmatario; è possibile che nel DNS (Domain Name System) sia stato pubblicato un valore di chiave pubblica non corretto; oppure il messaggio potrebbe essere stato falsificato da un'entità che non possiede la chiave privata necessaria per calcolare una firma corretta.

Èmolto difficile distinguere queste cause analizzando il messaggio, anche se l'indirizzo IP di origine può fornire alcune utili analisi legali nel caso di un messaggio falsificato. Tuttavia, per motivi di privacy non abbiamo accesso ai messaggi stessi, quindi tale analisi non è possibile.

Sono presenti messaggi le cui firme non vengono verificate per altri motivi, spesso a causa di errori di configurazione facilmente evitabili nei record a chiave pubblica (selettori) pubblicati in DNS.

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).