

Configurazione della verifica della chiave grande DKIM per Secure Email Gateway

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Panoramica](#)

[Configurazione](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la funzionalità estesa di verifica delle dimensioni della chiave DKIM maggiori per i messaggi di posta elettronica firmati.

Prerequisiti

Si desidera una conoscenza generale delle impostazioni e della configurazione di SEG.

Componenti usati

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 e versioni successive
- Profili di verifica DKIM
- Criteri flusso di posta

"Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi".

Panoramica

Il SEG può eseguire la verifica in entrata dei messaggi e-mail con firma DKIM.

Storicamente, l'intervallo di chiavi per la verifica SEG era 512-2048 prima delle 15.5 di AsyncOS.

AsyncOS 15.5 supporta l'intervallo di chiavi di 1024-4096 bit

Le chiavi da 512 e 768 bit15.5 sono obsolete, anche se i profili contenenti 512-768 prima dell'aggiornamento rimangono in servizio.

Configurazione

L'impostazione SEG è molto minima per adattarsi alle nuove dimensioni della chiave.

Spostarsi all'interno di WebUI per:

- Criteri di posta
 - Chiavi di dominio
 - Profili di verifica DKIM

Outbound DKIM Verification

Profile Name:

Smallest Key to be Accepted: Bits

Largest Key to be Accepted: Bits

Maximum Number of Signatures in the Message to Verify: Use Default (5)

Key Query Timeout Limit: Use Default (10 Seconds)

Limit to Tolerate Wall Clock Asynchronization Between Sender and Verifier: Use Default (60 Seconds)

Use a Body Length Parameter: Yes No

SMTP Action for Temporary Failure: Accept Reject

Change SMTP Response Settings

Response Code:

Description:

SMTP Action for Permanent Failure: Accept Reject

Change SMTP Response Settings

Response Code:

Description:

Profilo di verifica DKIM

DKIM Verification Profiles Items per page 20

Profile Name ▲	Smallest Key (Bits)	Largest Key (Bits)	Key Query Timeout (Seconds)	Use Body Length Parameter	SMTP Action For Temporary Failure	SMTP Action For Permanent Failure	Maximum Number of Signatures to Verify	All <input type="checkbox"/> Delete
DEFAULT	512	2048	10	Yes	Accept	Accept	5	<input type="checkbox"/>
DKIM_Large	1024	4096	10	Yes	Accept	Accept	5	<input type="checkbox"/>

Pagina di riepilogo dei profili di verifica DKIM

Applica i nuovi profili di verifica DKIM ai criteri di flusso della posta in arrivo desiderati:

- Criteri di posta
 - Criteri flusso di posta
 - Scegli la politica del flusso di posta desiderata per applicare il nuovo profilo di


verifica DKIM in base alle tue preferenze organizzative.

- Scorrere fino alla sezione Funzioni di sicurezza e individuare "Verifica DKIM:"
 - Selezionare il profilo desiderato.



DKIM Verification: Use Default (On: DEFAULT) On Off

Use DKIM Verification Profile: DEFAULT ✓ DKIM_Large

 Nota: prima della versione AsyncOS 15.5, la verifica DKIM era limitata a 2048 bit e superava una dimensione della chiave maggiore come unsigned.

Verifica

Il SEG non registra i dettagli relativi alle dimensioni della chiave all'interno dei log di posta o di verifica messaggi.

Prima della versione AsyncOS 15.5, una firma DKIM 1024-4096 di grandi dimensioni passava come senza segno.

Alcuni piccoli indicatori della dimensione grande della chiave DKIM richiedono controlli post-elaborazione.

- Recupero dell'intestazione e revisione del valore $b=$. Questo valore è maggiore con le dimensioni maggiori della chiave, anche se non è un valore diretto da calcolare.
- Il record DNS DKIM visualizza la chiave pubblica della coppia che aumenta le dimensioni da (stimate) 180 byte per 512 bit a 800 byte per 4096 bit.
- Una ricerca pubblica per "controllo dimensioni chiave DKIM", potrebbe produrre più siti web contenenti strumenti di ricerca per recuperare i record DKIM. Utilizzando il selettore e il dominio, questi siti eseguono una query sul record DNS e generano le dimensioni in bit della chiave, mentre i risultati della query DNS vengono restituiti nell'output.

Informazioni correlate

- [Cisco Secure Email Gateway - Guida alla configurazione](#)
- [Pagina di avvio di Cisco Secure Email Gateway per il supporto delle guide](#)
- [Cisco Secure Email Gateway - Note sulla release](#)

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).