ESA - Sostituzione della chiave DKIM esistente senza tempi di inattività

Sommario

Introduzione

In questo documento viene descritto come sostituire la chiave di firma DKIM esistente in una chiave pubblica ESA e DKIM nel DNS senza tempi di inattività.

Requisiti

1. Accesso a Email Security Appliance (ESA).
2. Accesso a DNS per aggiungere/rimuovere record TXT.
3. L'ESA deve già firmare i messaggi con un profilo DKIM.

Crea una nuova chiave di firma DKIM

Ènecessario creare una nuova chiave di firma DKIM sull'ESA:

1. Andare a Criteri di posta > Chiavi di firma e selezionare "Aggiungi chiave..."
2. Assegnare un nome alla chiave DKIM e generare una nuova chiave privata oppure incollare una chiave esistente. **Nota:** *Nella maggior parte dei casi è consigliabile scegliere una dimensione della chiave privata di 2048 bit*.
3. Eseguire il commit delle modifiche.
   Nota: Questa modifica non influirà sulla firma DKIM o sul flusso di posta. È in corso l'aggiunta di una chiave di firma DKIM e non l'applicazione di tale chiave a nessun profilo di firma DKIM.

Genera un nuovo profilo di firma DKIM e pubblica il record DNS in DNS

Sarà quindi necessario creare un nuovo profilo di firma DKIM, generare un record DNS DKIM dal profilo di firma DKIM e pubblicare il record in DNS:

1. Andare a Criteri di posta > Profili di firma e fare clic su "Aggiungi profilo..." Assegnare al

profilo un nome descrittivo nel campo "Nome profilo".Immettere il dominio nel campo "Nome dominio".Immettere una nuova stringa nel campo "Selettore".
Nota: *Il selettore è una stringa arbitraria utilizzata per consentire più record DNS DKIM per un determinato dominio. Verrà utilizzato il selettore per consentire più di un record DNS DKIM nel DNS per il dominio. È importante utilizzare un nuovo selettore diverso dal profilo di firma DKIM esistente.*
Selezionare la chiave di firma DKIM creata nella sezione precedente nel campo "Chiave di firma".Nella parte inferiore del profilo di firma aggiungere un nuovo "Utente". Questo utente deve essere un indirizzo di posta elettronica segnaposto inutilizzato. **Attenzione:** *È importante aggiungere un indirizzo di posta elettronica inutilizzato come utente per questo profilo di firma. In caso contrario, il profilo potrebbe firmare i messaggi in uscita prima della pubblicazione del record DKIM TXT, causando l'esito negativo della verifica DKIM. L'aggiunta di un indirizzo di posta elettronica inutilizzato come utente garantisce che questo profilo di firma non firmi alcun messaggio in uscita.*Fare clic su Invia.
2. Fare clic su "Genera" nella colonna "Record di testo DNS" per il profilo di firma appena creato e copiare il record DNS generato. Dovrebbe essere simile alla seguente:

```
selector2._domainkey.example.com. IN TXT "v=DKIM1;
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMaX6wMAk4iQoLNWiEkj0BrIRMDHXQ7743OQUOYZQqEXS
s+jMGomOknAZJpjR8TwmYHVPbD+30QRw0qEiRY3hYcmKOCWZ/hTo+NQ8qj1CSc1LTMdV0HWAi2AGsVOT8BdFHkyxg40
oyGWgktzc1q7zIgWM8usHfKVWFzYgnattNzyEqHsfI7lGilz5gdHBOvmF8LrDSfN"
"KtGrTtvIxJM8pWeJm6pg6TM/cy0FypS2azkrl9riJcWWDvu38JXFL/eeYjGnB1zQeR5Pnbc3sVJd3cGaWx1bWjepyN
QZ1PrS6Zwr7ZxSRa316Oxc36uCid5JAq0z+IcH4KkHqUueSGuGhwIDAQAB;"
```

3. Eseguire il commit delle modifiche.
4. Inviare il record DKIM DNS TXT al passaggio 2 a DNS.
5. Attendere che il record DKIM DNS TXT sia stato completamente propagato.

Elimina il profilo di firma precedente e rimuove l'utente segnaposto dal nuovo profilo di firma

Dopo aver inviato il record DKIM TXT a DNS e aver verificato che sia stato propagato, il passaggio successivo consiste nell'eliminare il vecchio profilo di firma e rimuovere l'utente segnaposto dal nuovo profilo di firma:

> **Nota:** *Si consiglia di eseguire il backup del file di configurazione ESA prima di procedere con i seguenti passaggi. Infatti, se si elimina il vecchio profilo di firma DKIM e occorre ripristinare la configurazione precedente, sarà possibile caricare facilmente il file di configurazione di cui è stato eseguito il backup.*

1. Andare a Mail Policies > Signing Profiles (Policy di posta > Profili di firma), selezionare il vecchio profilo di firma DKIM e fare clic su "Delete" (Elimina).
2. Accedere al nuovo profilo di firma DKIM, selezionare l'utente segnaposto corrente e fare clic su Rimuovi.
3. Fare clic su Invia.
4. Nella colonna "Profilo di prova" fare clic su "Prova" per il nuovo profilo di firma DKIM. Se il test ha esito positivo, passare al passaggio successivo. In caso contrario, verificare che il record DKIM DNS TXT sia stato propagato completamente.
5. Eseguire il commit delle modifiche apportate.

Verifica del flusso di posta per confermare i passaggi DKIM

A questo punto non è più necessario configurare DKIM. È tuttavia consigliabile verificare la firma DKIM per assicurarsi che stia firmando i messaggi in uscita come previsto e superando la verifica DKIM:

1. Inviare un messaggio tramite l'ESA assicurandosi che quest'ultima firmi DKIM e che DKIM sia verificata da un altro host.
2. Dopo aver ricevuto il messaggio dall'altra parte, controllare le intestazioni del messaggio per l'intestazione "Authentication-Results" (Risultati autenticazione). Cercare la sezione DKIM dell'intestazione per verificare se ha superato o meno la verifica DKIM. L'intestazione dovrebbe essere simile alla seguente:
   ```
   Authentication-Results: mx1.example.net; spf=SoftFail smtp.mailfrom=user1@example.net;
   dkim=pass header.i=none; dmarc=fail (p=none dis=none) d=example.net
   ```
3. Cercare l'intestazione "DKIM-Signature" e verificare che siano stati utilizzati il selettore e il dominio corretti:

   ```
   DKIM-Signature: a=rsa-sha256; d=example.net; s=selector2;
     c=simple; q=dns/txt; i=@example.net;
     t=1117574938; x=1118006938;
     h=from:to:subject:date;
     bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
     b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
              VoG4ZHRNiYzR
   ```
4. Dopo aver verificato che il DKIM funziona come previsto, attendere almeno una settimana prima di rimuovere il record DKIM TXT precedente. In questo modo, tutti i messaggi firmati dalla vecchia chiave DKIM vengono elaborati.