Configurazione della firma DKIM su ESA

Sommario

Introduzione

In questo documento viene descritto come configurare la firma DKIM (DomainKeys Identified Mail) su un'appliance ESA (Email Security Appliance).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso a Email Security Appliance (ESA).
- Accesso di modifica DNS per aggiungere/rimuovere record TXT.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Verificare che la firma DKIM sia disattivata

È necessario verificare che la firma DKIM sia disattivata in tutti i criteri del flusso di posta. In questo modo è possibile configurare la firma DKIM senza alcun impatto sul flusso di posta:

1. Passare a **Mail Policies > Mail Flow Policies**.
2. Spostamento ai criteri del flusso di posta e verifica che la **chiave di dominio/firma DKIM** sia impostata su **Disattivato**.

Crea una chiave di firma DKIM

È necessario creare una nuova chiave di firma DKIM sull'ESA:

1. Passare a **Mail Policies > Signing Keys** (Policy di posta > Chiavi di firma), quindi selezionare **Add Key...**
2. Assegnare un nome alla **chiave DKIM** e generare una nuova chiave privata o incollarla in una chiave corrente.

   Nota: nella maggior parte dei casi è consigliabile scegliere una dimensione della chiave privata pari a 2048 bit.

   ---

3. Eseguire il commit delle modifiche.

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

È 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. Passare a **Mail Policies > Signing Profiles (Policy di posta > Profili di firma)** e fare clic su **Add Profile (Aggiungi profilo)**.
   1. Assegnare al profilo un nome descrittivo nel campo **Nome profilo**.
   2. Immettere il dominio nel campo **Nome dominio**.
   3. 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.

      ---

   4. Selezionare la chiave di firma DKIM creata nella sezione precedente nel campo **Chiave di firma**.
   5. Fare clic su **Invia**.
2. Da qui, fare clic su **Genera** nella colonna **Record di testo DNS** per il profilo di firma appena creato e copiare il record DNS generato. Deve essere simile alla seguente:

   ```
   selector2._domainkey.domainsite IN TXT "v=DKIM1; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMa
   ```

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.
6. Fare clic su **Mail Policies > Signing Profiles** (Policy di posta > Profili di firma).
7. Nella colonna **Profilo di prova** fare clic su **Prova** per il nuovo profilo di firma DKIM. Se il test ha esito positivo, continuare con questa guida. In caso contrario, verificare che il record DKIM DNS TXT sia stato propagato completamente.

Attiva firma DKIM

Ora che l'ESA è configurata per i messaggi di firma DKIM, possiamo attivare la firma DKIM:

1. Selezionare **Mail Policies > Mail Flow Policies**.

2. Passare a ogni criterio del flusso di posta con il **comportamento** di **connessione** di **Relay** e impostare **Domain Key/DKIM Signing** su **On**.

> **Nota**: per impostazione predefinita, l'unico criterio del flusso di posta con un **comportamento** di **connessione** di **Relay** è il criterio del flusso di posta denominato **Relayed**. È necessario verificare che solo i messaggi con firma DKIM siano in uscita.

---

3. Eseguire il commit delle modifiche.

Test del flusso di posta per la conferma dei passaggi DKIM

A questo punto, il DKIM è configurato. È tuttavia necessario verificare la firma DKIM per assicurarsi che stia firmando i messaggi in uscita come previsto e che abbia superato la verifica DKIM:

1. Inviare un messaggio tramite lâ€™ESA e assicurarsi che questâ€™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 la verifica DKIM. L'intestazione deve essere simile all'esempio seguente:
<#root>

```
Authentication-Results: mx1.domainsite; spf=SoftFail smtp.mailfrom=user1@domainsite;
dkim=pass
 header.i=none; dmarc=fail (p=none dis=none) d=domainsite
```

3. Cercare l'intestazione "DKIM-Signature" e verificare che siano stati utilizzati il selettore e il dominio corretti:

<#root>

```
DKIM-Signature: a=rsa-sha256;
d=domainsite
;
s=selector2
;
   c=simple; q=dns/txt; i=@domainsite;
   t=1117574938; x=1118006938;
   h=from:to:subject:date;
   bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
   b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
            VoG4ZHRNiYzR
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Attualmente non esiste un modo specifico per risolvere i problemi relativi a questa configurazione.

Informazioni correlate

- **Supporto tecnico e download 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).