DKIM-signalering op ESA configureren

Inhoud

Inleiding

Dit document beschrijft hoe u DomainKeys Identified Mail (DKIM) kunt configureren door te ondertekenen met een e-mail security applicatie (ESA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot e-mail security applicatie (ESA).
- DNS bewerkt toegang om TXT-records toe te voegen/te verwijderen.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Controleer of de DKIM-signalering uit is

U moet ervoor zorgen dat DKIM-ondertekening is uitgeschakeld in alle mailflow-beleid. Zo kunt u DKIM-signalering configureren zonder dat dit gevolgen heeft voor de e-mailstroom:

1. Navigatie naar **Mail Policies > Mail Flow Policies**.
2. Navigatie naar elk poststroombeleid en zorg ervoor dat de **Domain Key/DKIM Signing** is ingesteld op **Off**.

Een DKIM-ondertekeningstoets maken

U moet een nieuwe DKIM-ondertekeningssleutel maken op de ESA:

1. Navigeer naar **Mail Policies > Ondertekeningstoetsen** en selecteer **Toevoegen Sleutel...**
2. Geef de **DKIM-toets een naam** en genereer een nieuwe private-toets of plak deze in een huidige toets.

   Opmerking: in de meeste gevallen is het aan te raden om een 2048-bits privé-sleutelgrootte te kiezen.

   ---

3. Breng de veranderingen aan.

Een nieuw DKIM-ondertekeningsprofiel genereren en de DNS-record naar DNS publiceren

Vervolgens moet u een nieuw DKIM-ondertekeningprofiel maken, een DKIM DNS-record genereren van dat DKIM-ondertekeningprofiel en dat record publiceren naar DNS:

1. Navigation to **Mail Policies > Profielen ondertekenen** en klik op **Add Profile**.
   1. Geef het profiel een beschrijvende naam in het veld **Profielnaam**.
   2. Voer uw domein in het veld **Domeinnaam in**.
   3. Voer een nieuwe selectortekenreeks in het veld **Selector in**.

      Opmerking: de selector is een willekeurige string die wordt gebruikt om meerdere DKIM DNS-records voor een bepaald domein toe te staan.

      ---

   4. Selecteer de DKIM-ondertekensleutel die in de vorige sectie in het veld **Ondertekensleutel is** gemaakt.
   5. Klik op **Verzenden**.
2. Klik hier op **Generate** in de kolom **DNS Text Record** voor het ondertekeningsprofiel dat u zojuist hebt gemaakt en kopieer het DNS-record dat is gegenereerd. Deze moet er als volgt uitzien:

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

3. Breng de wijzigingen aan.
4. Verzend de DKIM DNS TXT-record in stap 2 naar DNS.
5. Wacht totdat de DKIM DNS TXT-record volledig is gepropageerd.
6. Ga naar **Mail Beleid > Ondertekeningsprofielen**.
7. Klik onder de kolom **Test Profile** op **Test** voor het nieuwe DKIM-ondertekenprofiel. Als de test succesvol is, gaat u verder met deze handleiding. Zo niet, bevestig dat de DKIM DNS TXT-record volledig is gepropageerd.

DKIM-signalering inschakelen

Nu de ESA is ingesteld op DKIM gebarenberichten, kunnen we de DKIM-ondertekening inschakelen:

1. Ga naar **Mail Policies > Mail Flow Policies**.
2. Ga naar elk beleid voor e-mailstromen dat het **Verbindingsgedrag** van **Relay** heeft en schakel **Domain Key/DKIM-signalering in** op **On**.

   Opmerking: standaard is het enige e-mailstroombeleid met een **Connection Behavior** of **Relay**

   ---

het e-mailstroombeleid dat **Relayed** wordt genoemd. U moet ervoor zorgen dat alleen DKIM-gebarentekenberichten uitgaand zijn.

3. Breng de veranderingen aan.

Test Mail Flow om DKIM-passen te bevestigen

Op dit punt is de DKIM ingesteld. U moet echter DKIM-signalering testen om er zeker van te zijn dat het uitgaande berichten ondertekent zoals verwacht en dat het de DKIM-verificatie doorgeeft:

1. Verzend een bericht via de ESA en zorg ervoor dat de DKIM wordt ondertekend door de ESA en de DKIM wordt geverifieerd door een andere gastheer.
2. Zodra het bericht op het andere eind wordt ontvangen, controleer de kopballen van het bericht voor de kopbal **verificatie-Resultaten**. Zoek naar het DKIM gedeelte van de header om te bevestigen of het is geslaagd voor DKIM verificatie of niet. De header moet er hetzelfde uitzien als dit voorbeeld:
<#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. Zoek naar de kop "DKIM-Signature" en bevestig dat de juiste selector en het domein worden gebruikt:

<#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
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke manier om problemen op te lossen voor deze configuratie.

Gerelateerde informatie

- **Cisco technische ondersteuning en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.