ESA - Configure la firma DKIM

Contenido

[Introducción](#)
[Requisitos](#)
[Asegúrese de que la firma DKIM esté apagada](#)
[Cree una clave de firma DKIM](#)
[Genere un nuevo perfil de firma DKIM y publique el expediente DNS al DNS](#)
[Dé vuelta al DKIM que firma encendido](#)
[Pruebe el flujo de correo para confirmar los pasos DKIM](#)

Introducción

Este documento describe cómo configurar el DKIM que firma en un ESA.

Requisitos

1. Acceso al dispositivo de seguridad del correo electrónico (ESA).
2. El acceso al DNS a agregar/quita los expedientes de TXT.

Asegúrese de que la firma DKIM esté apagada

Antes de que realicemos cualquier cambio, queremos asegurarnos de que la firma DKIM está apagado en todas las directivas del flujo de correo. Esto permitirá que configuremos el DKIM que firma sin ningún impacto al flujo de correo:

1. Vaya a las directivas del correo > a las directivas del flujo de correo.
2. Vaya a cada directiva del flujo de correo y asegúrese de que el “dominio Key/DKIM que firma” está fijado a “apagado.”

Cree una clave de firma DKIM

Usted primero necesitará crear una nueva clave de firma DKIM en el ESA:

1. Van a las directivas del correo > las claves de firma y seleccionan el “agregar clave…”
2. Nombre la clave DKIM y genere una nueva clave privada o goma en existente. **Note**: *En la mayoría de los casos, ha recomendado que usted elige un tamaño de la clave privada de 2048 bits*.
3. Confíe los cambios.

Genere un nuevo perfil de firma DKIM y publique el expediente DNS al DNS

Después, usted necesitará crear un nuevo perfil de firma DKIM, genera un expediente DKIM DNS de ese perfil de firma DKIM y publica ese expediente al DNS:

1. Van a las directivas del correo > los perfiles de firma y el tecleo “agrega el perfil…” Dé a perfil un nombre descriptivo en el campo “nombre del perfil.”Ingrese su dominio en el campo “Domain Name.”Ingrese una nueva cadena del selector en el campo “selector.”
   Note: *El selector es una cadena arbitraria que se utiliza para permitir los expedientes múltiples DKIM DNS para un dominio dado.*
   Seleccione la clave de firma DKIM creada en la sección anterior en el campo de “clave firma.”Haga clic en Submit (Enviar).
2. De aquí, el tecleo “genera” en la columna “expediente del texto DNS” para el perfil de firma que usted acaba de crear y copia el expediente DNS se genera que. Debe parecer similar al siguiente:

   ```
   selector2._domainkey.example.com. IN TXT "v=DKIM1;
   p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwMaX6wMAk4iQoLNWiEkj0BrIRMDHXQ7743OQUOYZQqEXS
   s+jMGomOknAZJpjR8TwmYHVPbD+30QRw0qEiRY3hYcmKOCWZ/hTo+NQ8qj1CSc1LTMdV0HWAi2AGsVOT8BdFHkyxg40
   oyGWgktzc1q7zIgWM8usHfKVWFzYgnattNzyEqHsfI7lGilz5gdHBOvmF8LrDSfN"
   "KtGrTtvIxJM8pWeJm6pg6TM/cy0FypS2azkrl9riJcWWDvu38JXFL/eeYjGnB1zQeR5Pnbc3sVJd3cGaWx1bWjepyN
   QZ1PrS6Zwr7ZxSRa316Oxc36uCid5JAq0z+IcH4KkHqUueSGuGhwIDAQAB;"
   ```
3. Confíe los cambios.
4. Someta el expediente DKIM DNS TXT en el paso 2 al DNS.
5. Espere hasta que el expediente DKIM DNS TXT se haya propagado completamente.
6. Van a las directivas del correo > los perfiles de firma.
7. Bajo la columna “pruebe el perfil”, tecleo “prueba” para el nuevo perfil de firma DKIM. Si la prueba es acertada, continúe con esta guía. Si no, confirme que el expediente DKIM DNS TXT se ha propagado completamente.

Dé vuelta al DKIM que firma encendido

Ahora que el ESA se configura a los mensajes de la muestra DKIM, podemos dar vuelta al DKIM que firman encendido:

1. Vaya a las directivas del correo > a las directivas del flujo de correo.
2. Vaya a cada directiva del flujo de correo que tenga el “comportamiento de la conexión” de la “retransmisión” y dé vuelta al “dominio Key/DKIM que firma” a “encendido.”
   Note: *Por abandono, la única directiva del flujo de correo con un “comportamiento de la conexión” de la “retransmisión” es la directiva del flujo de correo llamada “retransmitida.” El asunto importante a recordar aquí es que queremos solamente a los mensajes de la muestra DKIM que son salientes.*
3. Confíe los cambios.

Pruebe el flujo de correo para confirmar los pasos DKIM

A este punto, le hacen con configurar el DKIM más lejos. Sin embargo, usted debe probar el DKIM que firma para asegurarse de que está firmando sus mensajes de salida como se esperaba y está pasando la verificación DKIM:

1. Envíe un mensaje con el ESA asegurándose de que consigue el DKIM firmado por el ESA y

el DKIM verificado por otro host.

2. Una vez que el mensaje se recibe en el otro extremo, controle las encabezados del mensaje para saber si hay la encabezado “Autenticación-resultados.” Busque la sección DKIM de la encabezado para confirmar si pasó la verificación DKIM o no. La encabezado debe parecer similar al siguiente:

```
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. Busque la encabezado “DKIM-firma” y confirme que se están utilizando el selector y el dominio correctos:

```
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
```