Configuración de la firma DKIM en ESA

Contenido

Introducción

Este documento describe cómo configurar la firma de correo identificado por DomainKeys (DKIM) en un dispositivo de seguridad de correo electrónico (ESA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso al dispositivo de seguridad Email Security Appliance (ESA).
- Acceso de edición de DNS para agregar o quitar registros TXT.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Asegúrese de que la firma DKIM está desactivada

Debe asegurarse de que la firma DKIM está desactivada en todas las políticas de flujo de correo. Esto le permite configurar la firma DKIM sin ningún impacto en el flujo de correo:

1. Vaya a **Políticas de correo > Políticas de flujo de correo**.
2. Navegación a cada política de flujo de correo y asegúrese de que **Domain Key/DKIM Signing** esté configurado en **Off**.

Crear una clave de firma DKIM

Debe crear una nueva clave de firma DKIM en el ESA:

1. Navegue hasta **Políticas de correo > Llaves de firma** y seleccione **Agregar clave...**
2. Asigne un nombre a la **clave DKIM** y genere una nueva clave privada o péguela en una clave actual.

   Nota: en la mayoría de los casos, se recomienda que elija un tamaño de clave privada de 2048 bits.

   ---

3. Realice los cambios.

Generar un nuevo perfil de firma DKIM y publicar el registro DNS en DNS

A continuación, debe crear un nuevo perfil de firmas DKIM, generar un registro DNS DKIM a partir de ese perfil de firmas DKIM y publicar ese registro en DNS:

1. Vaya a **Políticas de correo > Perfiles de firma** y haga clic en **Agregar perfil**.
   1. Asigne un nombre descriptivo al perfil en el campo **Profile Name**.
   2. Introduzca su dominio en el campo **Domain Name**.
   3. Ingrese una nueva cadena de selector en el campo **Selector**.

      Nota: El selector es una cadena arbitraria que se utiliza para permitir varios registros DNS DKIM para un dominio determinado.

      ---

   4. Seleccione la clave de firma DKIM creada en la sección anterior en el campo **Signing Key**.
   5. Haga clic en Submit (Enviar).
2. Desde aquí, haga clic en **Generate** en la columna **DNS Text Record** para el perfil de firma que acaba de crear y copie el registro DNS que se genera. Debe tener un aspecto similar al siguiente:

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

3. Realice los cambios.
4. Envíe el registro DKIM DNS TXT del paso 2 a DNS.
5. Espere hasta que el registro DKIM DNS TXT se haya propagado completamente.
6. Vaya a **Políticas de correo > Perfiles de firma**.
7. En la columna **Test Profile**, haga clic en **Test** para el nuevo perfil de firmas DKIM. Si la prueba es correcta, continúe con esta guía. Si no es así, confirme que el registro DKIM DNS TXT se ha propagado completamente.

Activar inicio de sesión DKIM

Ahora que ESA está configurado para firmar mensajes DKIM, podemos activar la firma DKIM:

1. Vaya a **Políticas de correo > Políticas de flujo de correo**.
2. Vaya a cada política de flujo de correo que tenga el **Comportamiento de Conexión** de **Relay** y gire **Domain Key/DKIM Signing** a **On**.

> **Nota**: de forma predeterminada, la única política de flujo de correo con un **comportamiento de conexión** de **retransmisión es la política de flujo de correo denominada retransmitido.** Debe asegurarse de que sólo los mensajes de firma DKIM son salientes.

3. Realice los cambios.

Probar flujo de correo para confirmar pasadas de DKIM

En este punto, se configura el DKIM. Sin embargo, debe probar la firma DKIM para asegurarse de que firma los mensajes salientes como se espera y de que pasa la verificación DKIM:

1. Envíe un mensaje a través del ESA y asegúrese de que obtiene DKIM firmado por el ESA y DKIM verificado por otro host.
2. Una vez que el mensaje se recibe en el otro extremo, verifique los encabezados del mensaje para el encabezado **Authentication-Results**. Busque la sección DKIM del encabezado para confirmar si pasó o no la verificación DKIM. El encabezado debe ser similar a este ejemplo:
<#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. Busque el encabezado "DKIM-Signature" y confirme que se utilizan el selector y el dominio correctos:

<#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
```

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente no existe una forma específica de solucionar problemas de esta configuración.

Información Relacionada

- **Asistencia técnica y descargas de Cisco**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).