Verifique que el DKIM trabaje

Contenido

Introducción

Este documento describe cómo verificar que el DKIM trabaja.

Verificación

En el dispositivo de seguridad del correo electrónico de Cisco (ESA), la manera más fácil de verificar que el DKIM esté trabajando es enviar un correo electrónico a una cuenta del exterior y marcar las encabezados. En el ejemplo abajo, un mensaje fue enviado a una cuenta @gmail.com:

```
Delivered-To: user@gmail.com
Return-Path: <bob@example.com>
Received-SPF: pass (google.com: domain of bob@example.com
designates <IP Address> as permitted sender)
client-ip=<IP Address>;
Authentication-Results: mx.google.com; spf=pass
(google.com: domain of bob@example.com designates
<IP Address> as permitted sender) smtp.mail=bob@example.com;
dkim=pass (test mode) header.i=bob@example.com
```

Usted debe ver los dkim=pass en la línea de los Autenticación-resultados.

> **Note**: Sea por favor consciente que algunos clientes tales como Yahoo tienden a eliminar muchas encabezados. Compruebe por favor esto los clientes múltiples para estar seguro que está trabajando.

Usted puede también referir a algunas de estas fuentes externas para verificar su configuración:

http://www.kitterman.com/spf/validate.html

dkim-test@testing.dkim.org

Hay otros reflectores disponibles también:

Actualmente verificando con el RFC4871:
Puerto 25: check-auth@verifier.port25.com

Actualmente verificar ambo RFC4871 (y el RFC4870):
Alternativo: dkim-test@altn.com

Actualmente verificar ambo RFC4871 (y el RFC4870):
Sendmail: sa-test@sendmail.net

Actualmente verificar el proyecto allman-00 y allman-01:
Elandsys: autorespond+dkim@dk.elandsys.com

Actualmente verificar ambo RFC4871 (y el RFC4870):
Blackops: dktest@blackops.org

Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final
- Soporte Técnico y Documentación - Cisco Systems