Überprüfen Sie, ob DKIM funktioniert.

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie überprüfen können, ob DKIM funktioniert.

Überprüfung

Auf der Cisco E-Mail Security Appliance (ESA) können Sie am einfachsten überprüfen, ob DKIM funktioniert, indem Sie eine E-Mail an ein externes Konto senden und die Kopfzeilen überprüfen. Im folgenden Beispiel wurde eine Nachricht an ein @gmail.com-Konto gesendet:

```
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
```

In der Zeile Authentifizierungsergebnisse sollte dkim=pass angezeigt werden.

> **Hinweis**: Bitte beachten Sie, dass einige Clients wie Yahoo dazu neigen, viele Header zu entfernen. Bitte überprüfen Sie dies auf mehreren Clients, um sicherzustellen, dass es funktioniert.

Sie können auch auf einige der folgenden externen Quellen zurückgreifen, um Ihre Konfiguration zu überprüfen:

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

dkim-test@testing.dkim.org

Es stehen auch verschiedene andere Reflektoren zur Verfügung:

Aktuell mit RFC4871 verifiziert:
Port 25: check-auth@verifier.port25.com

Derzeit werden sowohl RFC4871 (als auch RFC4870) überprüft:
Alt-N: dkim-test@altn.com

Derzeit werden sowohl RFC4871 (als auch RFC4870) überprüft:
Sendmail: sa-test@sendmail.net

Aktuell sowohl Draft allman-00 als auch allman-01 überprüfen:
Landschaften: autorespond+dkim@dk.elandsys.com

Aktuell sowohl RFC4871 (als auch RFC4870) überprüfen:
Blackops: dktest@blackops.org

Zugehörige Informationen

- Cisco Email Security Appliance - Benutzerhandbücher
- Technischer Support und Dokumentation - Cisco Systems