Welche Bedingungen erzeugen welche Authentifizierungsergebnisse für DKIM?

Inhalt

Einführung

Dieses Dokument beschreibt die Bedingungen, die bestimmte Authentifizierungsergebnisse für DKIM ergeben.

Ergebnisse

DomainKeys Identified Mail (DKIM) ist ein E-Mail-Validierungssystem, das E-Mail-Spoofing erkennt, indem es einen Mechanismus bereitstellt, mit dem Empfänger-Mail-Empfänger überprüfen können, ob eingehende E-Mails aus einer Domäne von den Administratoren dieser Domäne autorisiert werden.

Die Cisco E-Mail Security Appliance (ESA) kann mit DKIM-Signierung und -Verifizierung EIN/AUS folgende Ergebnisse liefern:

DKIM-Signatur (Sending End)	DKIM-Verifizierung (Empfangsende)	Ergebnis
EIN	EIN	Pass/Permerror/Temperror/Hardfail
EIN	AUS	Keine
AUS	AUS	Keine
AUS	EIN	Neutral

- Bestehen. Die Nachricht hat die Authentifizierungstests bestanden.
- Neutral. Die Authentifizierung wurde nicht durchgeführt.
- Temperament. Ein behebbarer Fehler ist aufgetreten.
- Permerror. Ein nicht behebbarer Fehler ist aufgetreten.
- Hardfail. Die Authentifizierungstests sind fehlgeschlagen.
- Keine. Die Nachricht wurde nicht signiert.

Wenn die Überprüfung von DKIM in Mail Flow Policies (Mail-Fluss-Richtlinien) am empfangenden Ende deaktiviert ist, wird das DKIM-Ergebnis nicht in Mail-Protokollen angezeigt. Das Ergebnis "none" kann jedoch in den Content-Filtern abgeglichen werden.

Zugehörige Informationen

- AsyncOS E-Mail-Benutzerhandbuch
- Kontaktdaten des GLO-Supports
- Technischer Support und Dokumentation - Cisco Systems