Contenu

Introduction

Ce document décrit les conditions qui produisent certains résultats d'authentification pour DKIM.

Résultats

DomainKeys a identifié la messagerie (DKIM) est un système de validation d'email conçu pour détecter la mystification d'email en fournissant un mécanisme pour permettre recevoir des messagers pour vérifier que la messagerie entrante d'un domaine est autorisée par les administrateurs de ce domaine.

L'appliance de sécurité du courrier électronique de Cisco (ESA) peut produire le résultat suivant avec la signature DKIM et la vérification "MARCHE/ARRÊT" :

Signature DKIM (Envoyant l'extrémité)	Vérification DKIM (Extrémité réceptrice)	Résultat
SUR	SUR	Passage/Permerror/Temperror/Hardfail
SUR	OUTRE DE	Aucun
OUTRE DE	OUTRE DE	Aucun
OUTRE DE	SUR	Neutre

- Passez. Le message passé les tests d'authentification.
- Neutre. L'authentification n'a pas été exécutée.
- Temperror. Une erreur réparable s'est produite.
- Permerror. Une erreur irrémédiable s'est produite.
- Incident permanent. Les tests d'authentification ont manqué.
- Aucun. Le message n'a pas été signé.

Si la vérification de DKIM est HORS FONCTION dans des stratégies de flux de courrier à l'extrémité réceptrice, alors le résultat DKIM ne sera pas affiché dans des logs de messagerie. Cependant, un résultat de « aucun » peut être apparié dans les filtres satisfaits.

Informations connexes

- Guide utilisateur d'email d'AsyncOS
- L'information de contact de support GLO
- Support et documentation techniques - Cisco Systems