

Konfigurieren der Verifizierung für große DKIM-Schlüssel für ein sicheres E-Mail-Gateway

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Überblick](#)

[Konfigurieren](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird die erweiterte DKIM-Funktion zur Überprüfung der Schlüssellänge für signierte E-Mails beschrieben.

Voraussetzungen

Allgemeine Kenntnisse der SEG-Einstellungen und -Konfiguration sind erwünscht.

Verwendete Komponenten

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 und höher
- DKIM-Verifizierungsprofile
- Mail Flow-Richtlinien

"Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Befehle verstehen."

Überblick

Die SEG kann eingehende Überprüfungen von DKIM-signierten E-Mails durchführen.

Früher lag der SEG-Verifizierungsschlüsselbereich bei 512-2048 vor 15.5 AsyncOS.

AsyncOS 15.5 unterstützt den Schlüsselbereich von 1024-4096 Bit.

Die Schlüssel 15.5 mit 512 und 768 Bit sind jetzt veraltet, obwohl Profile mit 512-768 vor dem Upgrade im Einsatz bleiben.

Konfigurieren

Die SEG-Konfiguration ist sehr klein, um die neuen Schlüsselgrößen zu berücksichtigen.

Navigieren Sie in der WebUI zu:

- Mail-Policys
 - Domänenschlüssel
 - DKIM-Verifizierungsprofile

Outbound DKIM Verification

Profile Name:

Smallest Key to be Accepted: Bits

Largest Key to be Accepted: Bits

Maximum Number of Signatures in the Message to Verify: Use Default (5)

Key Query Timeout Limit: Use Default (10 Seconds)

Limit to Tolerate Wall Clock Asynchronization Between Sender and Verifier: Use Default (60 Seconds)

Use a Body Length Parameter: Yes No

SMTP Action for Temporary Failure: Accept Reject

Change SMTP Response Settings

Response Code:

Description:

SMTP Action for Permanent Failure: Accept Reject

Change SMTP Response Settings

Response Code:

Description:

DKIM-Verifizierungsprofil

DKIM Verification Profiles Items per page 20

Profile Name ▲	Smallest Key (Bits)	Largest Key (Bits)	Key Query Timeout (Seconds)	Use Body Length Parameter	SMTP Action For Temporary Failure	SMTP Action For Permanent Failure	Maximum Number of Signatures to Verify	All <input type="checkbox"/> Delete
DEFAULT	512	2048	10	Yes	Accept	Accept	5	<input type="checkbox"/>
DKIM_Large	1024	4096	10	Yes	Accept	Accept	5	<input type="checkbox"/>

DKIM-Verifizierungsprofile - Zusammenfassungsseite

Wenden Sie die neuen DKIM-Verifizierungsprofile auf die gewünschten Richtlinien für den eingehenden E-Mail-Fluss an:


- Mail-Policys
 - Mail Flow-Richtlinien

- Wählen Sie die gewünschte Mail Flow Policy (E-Mail-Fluss-Richtlinie) aus, um das neue DKIM-Verifizierungsprofil basierend auf Ihren organisatorischen Einstellungen anzuwenden.
 - Blättern Sie nach unten zum Abschnitt Sicherheitsfunktionen, und suchen Sie nach "DKIM Verification:".
 - Wählen Sie das gewünschte Profil aus.



DKIM Verification: Use Default (On: DEFAULT) On Off

Use DKIM Verification Profile: DEFAULT ✓ DKIM_Large

 Hinweis: Vor AsyncOS 15.5 war die DKIM-Verifizierung auf 2048 Bit beschränkt und würde eine größere Schlüssellänge als nicht signiert weitergeben.

Überprüfung

Die SEG protokolliert keine Details bezüglich der Schlüsselgröße in den Mail-Protokollen oder der Nachrichtenverfolgung.

Vor AsyncOS 15.5 wird eine große 1024-4096 DKIM-Signatur als unsigniert weitergeleitet.

Einige kleine Indikatoren für die große DKIM-Schlüsselgröße erfordern Prüfungen nach der Verarbeitung.

- Header-Abruf und Überprüfung des b=-Werts. Dieser Wert ist mit der größeren Schlüssellänge größer, obwohl es sich nicht direkt um einen zu berechnenden Wert handelt.
- Der DKIM-DNS-Eintrag zeigt den öffentlichen Schlüssel des Paares an, dessen Größe von (geschätzten) 180 Byte für 512 Bit auf 800 Byte für 4096 Bit zunimmt.
- Eine öffentliche Suche nach "DKIM key size check" könnte mehrere Websites mit Suchwerkzeugen zum Abrufen von DKIM-Datensätzen erstellen. Mithilfe der Auswahlfunktion und der Domäne fragen diese Sites den DNS-Eintrag ab und generieren die Schlüssel-Bitgröße sowie DNS-Abfrageergebnisse in der Ausgabe.

Zugehörige Informationen

- [Cisco Secure Email Gateway - Einrichtungsleitfaden](#)
- [Cisco Secure Email Gateway Launch-Website für Support-Leitfäden](#)
- [Cisco Secure Email Gateway - Versionshinweise](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.