Configuration de la vérification de clé importante DKIM pour la passerelle de messagerie sécurisée

Table des matières

Introduction

Ce document décrit la fonctionnalité étendue de vérification de taille de clé supérieure DKIM pour les e-mails signés.

Conditions préalables

Une connaissance générale des paramètres et de la configuration du SEG est souhaitée.

Composants utilisés

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 et versions ultérieures
- Profils de vérification DKIM
- Stratégies de flux de messagerie

"Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est actif, assurez-vous de comprendre l'impact potentiel de toute commande. »

Aperçu

Le SEG peut effectuer une vérification entrante des e-mails signés DKIM.

Historiquement, la plage de clés de vérification SEG était 512-2048 avant 15.5 AsyncOS.

AsyncOS 15.5 prend en charge la plage de clés de 1 024 à 4 096 bits

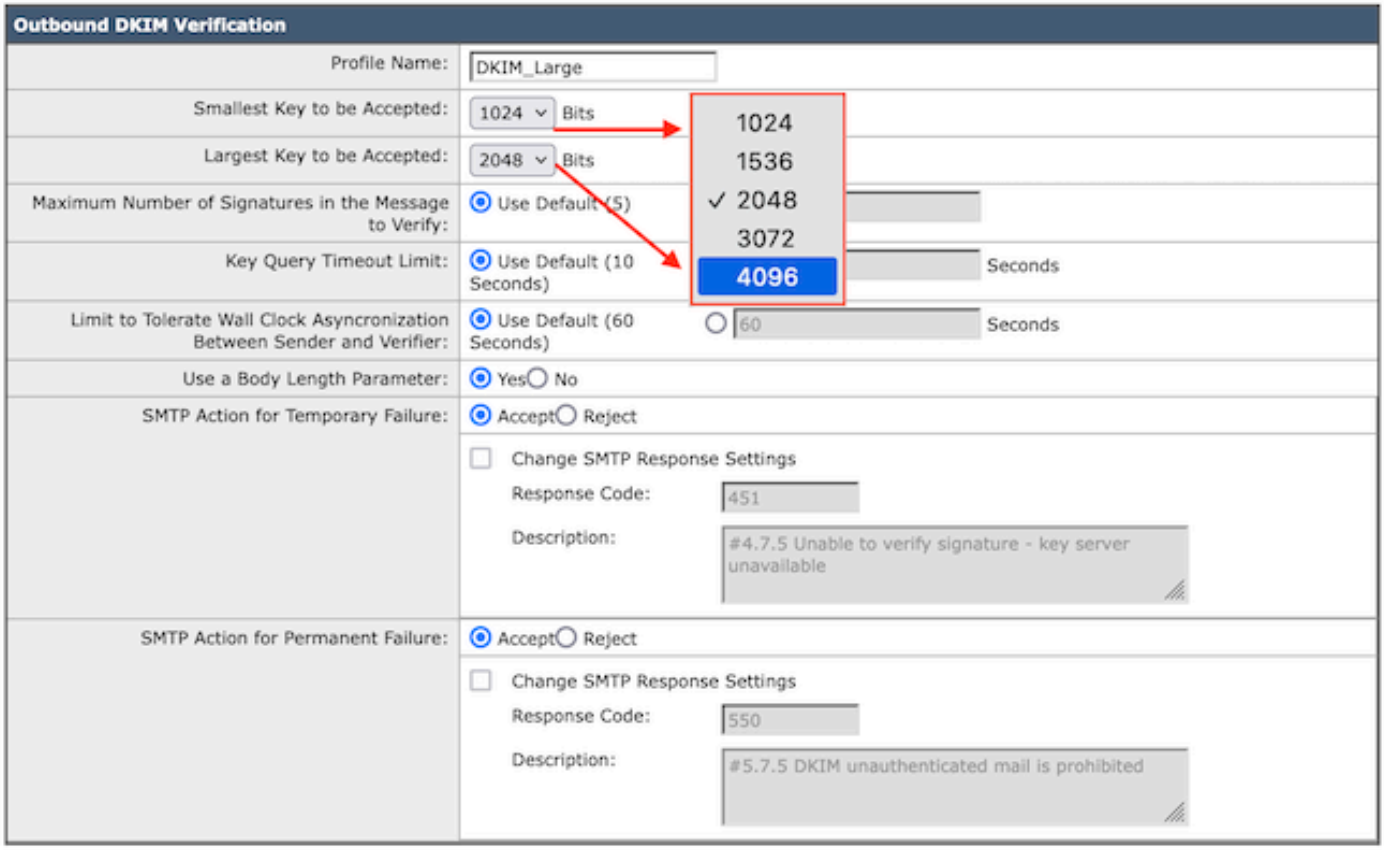
Les clés de taille 512 et 768 bits15.5 sont désormais déconseillées, bien que les profils contenant 512-768 avant la mise à niveau restent en service.

Configurer

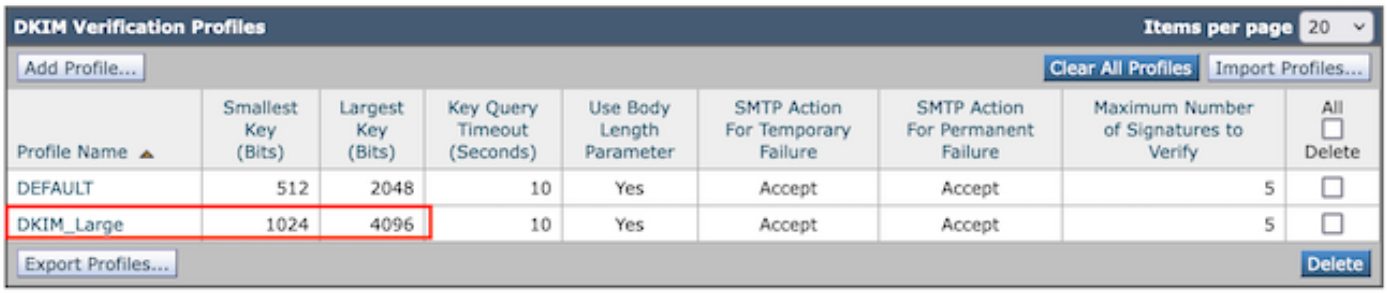
La configuration du SEG est très minimale pour s'adapter aux nouvelles tailles de clés.

Naviguez dans l'interface WebUI pour :

- Stratégies de messagerie
  - Clés de domaine
    - Profils de vérification DKIM



Profil de vérification DKIM



Page Récapitulatif des profils de vérification DKIM

Appliquez les nouveaux profils de vérification DKIM aux stratégies de flux de messages entrants souhaitées :

- Stratégies de messagerie
  - Stratégies de flux de messagerie
    - Sélectionnez la stratégie de flux de courrier souhaitée pour appliquer le nouveau profil de vérification DKIM en fonction de vos préférences organisationnelles.
      - Faites défiler jusqu'à la section Security Features (Fonctions de sécurité) et recherchez « DKIM Verification: » (Vérification DKIM :)
        - Sélectionnez le profil de votre choix.

Remarque : avant AsyncOS 15.5, la vérification DKIM était limitée à 2048 bits et passait une taille de clé plus importante comme non signée.

Vérifier

Le SEG ne consigne pas les détails concernant la taille de clé dans les journaux de messagerie ou le suivi des messages.

Avant AsyncOS 15.5, une signature DKIM 1024-4096 importante était considérée comme non signée.

Certains petits indicateurs de la taille de clé importante de DKIM nécessitent des contrôles post-traitement.

- Récupération de l'en-tête et révision de la valeur b=. Cette valeur est plus grande avec la taille de clé plus grande, bien qu'il ne s'agisse pas d'une valeur directe à calculer.
- L'enregistrement DNS DKIM affiche la clé publique de la paire, dont la taille passe de (estimée) 180 octets pour 512 bits à 800 octets pour 4 096 bits.
- Une recherche publique pour "vérification de la taille de clé DKIM" pourrait produire plusieurs sites Web contenant des outils de recherche pour récupérer des enregistrements DKIM. À l'aide du sélecteur et du domaine, ces sites interrogent l'enregistrement DNS et génèrent la taille de bit clé, et les résultats de la requête DNS sont affichés.

Informations connexes

- Cisco Secure Email Gateway - Guide de configuration
- Guides d'assistance de la page de lancement de Cisco Secure Email Gateway
- Cisco Secure Email Gateway - Notes de version

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.