Configuración de la verificación de clave grande DKIM para gateway de correo electrónico seguro

Contenido

Introducción

Este documento describe la capacidad de verificación de tamaño de clave DKIM mayor expandida para correos electrónicos firmados.

Prerequisites

Se requiere un conocimiento general de los parámetros y la configuración de SEG.

Componentes Utilizados

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 y versiones posteriores
- Perfiles de verificación DKIM
- Políticas de flujo de correo

"La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si su red está activa, asegúrese de comprender el impacto potencial de cualquier comando".

Overview

El SEG puede realizar la verificación entrante del correo electrónico firmado DKIM.

Históricamente, el rango de la clave de verificación SEG era de 512-2048 antes de 15.5 AsyncOS.

AsyncOS 15.5 admite el rango de claves de 1024-4096 bits

Las claves de 512 y 768 bits15.5 ya no están aprobadas, aunque los perfiles que contenían 512-

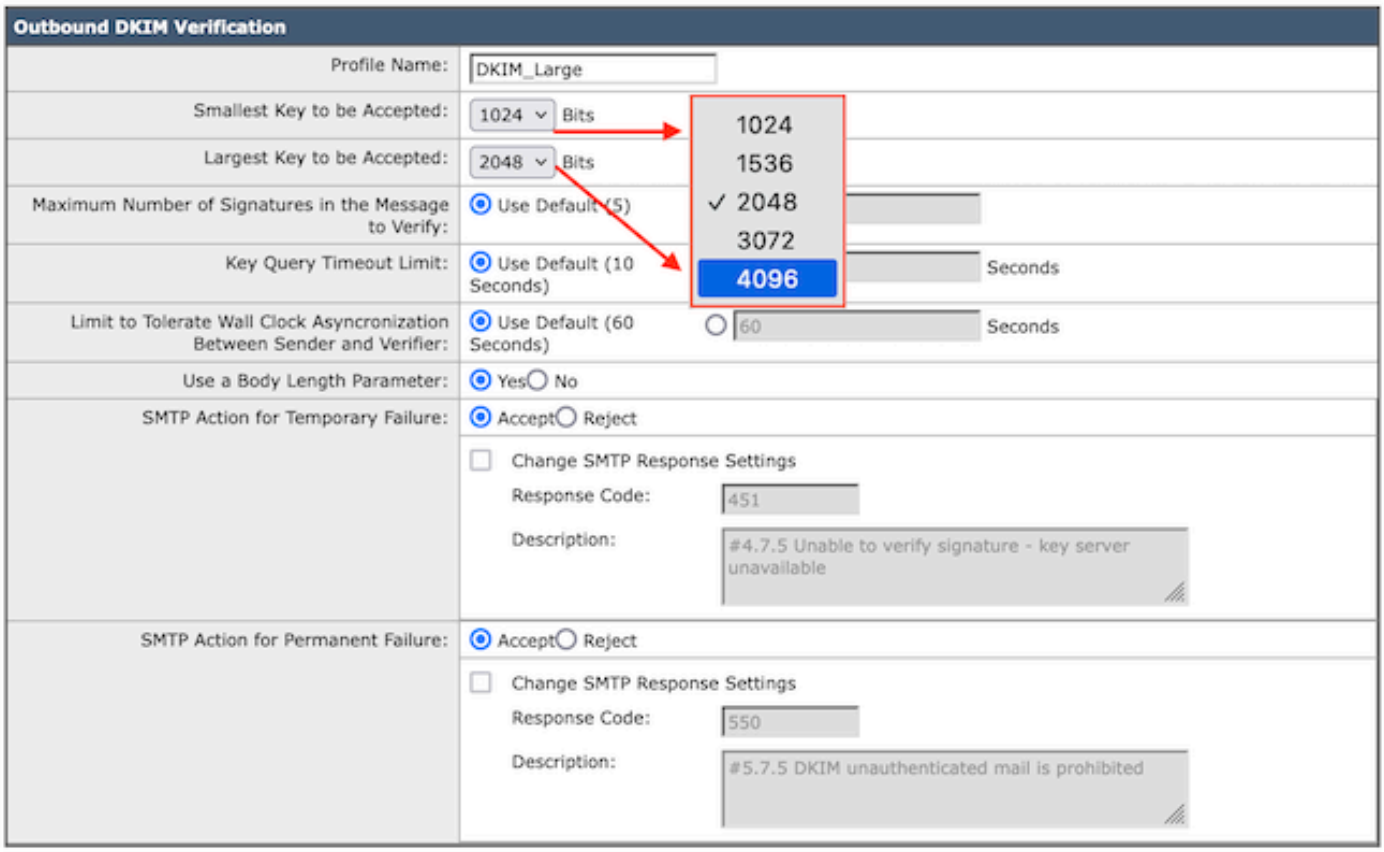
768 antes de la actualización siguen en servicio.

Configurar

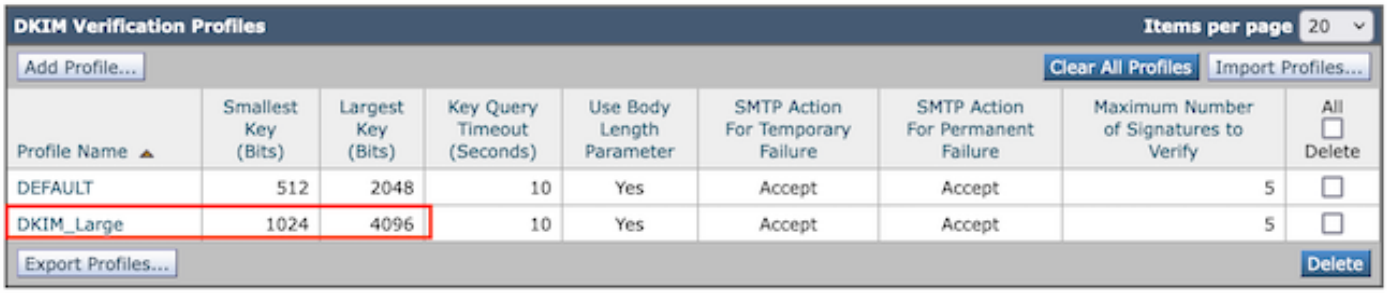
La configuración SEG es mínima para admitir los nuevos tamaños de clave.

Desplácese dentro de la interfaz de usuario Web para:

- Políticas de correo
  - Claves de dominio
    - Perfiles de verificación DKIM



Perfil de verificación DKIM



Página de resumen Perfiles de verificación DKIM

Aplique los nuevos perfiles de verificación DKIM a las políticas de flujo de correo entrante deseadas:

- Políticas de correo

- Políticas de flujo de correo
  - Elija la política de flujo de correo que desee para aplicar el nuevo perfil de verificación DKIM en función de las preferencias de su organización.
    - Desplácese hasta la sección Security Features (Funciones de seguridad) y localice "DKIM Verification:".
      - Seleccione el perfil que desee.

Nota: antes de AsyncOS 15.5, la verificación DKIM estaba limitada a 2048 bits y pasaba un tamaño de clave mayor como sin firmar.

Verificación

El SEG no registra detalles con respecto al tamaño de clave en los registros de correo o el rastreo de mensajes.

Antes de AsyncOS 15.5, una firma DKIM grande 1024-4096 pasaba como sin firmar.

Algunos indicadores pequeños del tamaño de clave grande DKIM requieren comprobaciones posteriores al procesamiento.

- Recuperación y revisión del encabezado del valor b=. Este valor es mayor con el tamaño de clave mayor, aunque no es un valor directo que calcular.
- El registro DNS DKIM muestra la clave pública del par, cuyo tamaño aumenta de (estimado) 180 bytes para 512 bits a 800 bytes para 4096 bits.
- Una búsqueda pública de "comprobación del tamaño de clave DKIM" podría generar varios sitios web que contengan herramientas de búsqueda para recuperar registros DKIM. Mediante el selector y el dominio, estos sitios consultan el registro DNS y generan el tamaño del bit de clave y los resultados de la consulta DNS en la salida.

Información Relacionada

- Cisco Secure Email Gateway - Guía de configuración
- Página de inicio de Cisco Secure Email Gateway para las guías de asistencia
- Cisco Secure Email Gateway - Notas de la versión

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).