Configure DKIM Large Key Verification for Secure Email Gateway

Contents

Introduction

Prerequisites

Components Used

Overview

Configure

Verify

Related Information

Introduction

This document describes the expanded DKIM larger key size verification capability for signed emails.

Prerequisites

General knowledge of the SEG settings and configuration is desired.

Components Used

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 and newer
- DKIM Verification Profiles
- Mail Flow Policies

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

The SEG can perform inbound verification of DKIM signed email.

Historically the SEG verification key range was 512-2048 before 15.5 AsyncOS.

AsyncOS 15.5 supports the key range of 1024-4096 bits

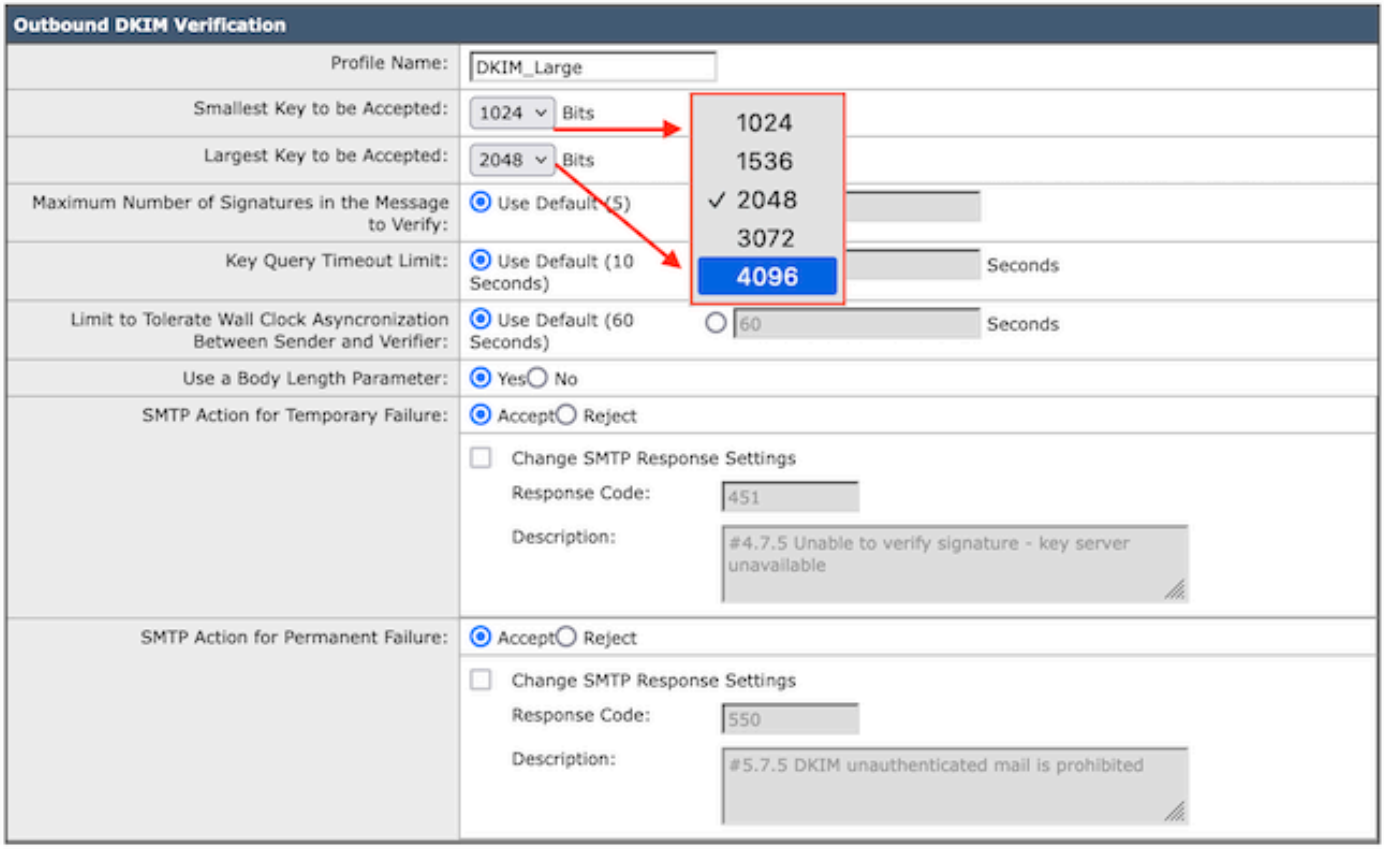
512 and 768-bit sized keys15.5 are now deprecated, although profiles containing 512-768 before the upgrade remain in service.

Configure

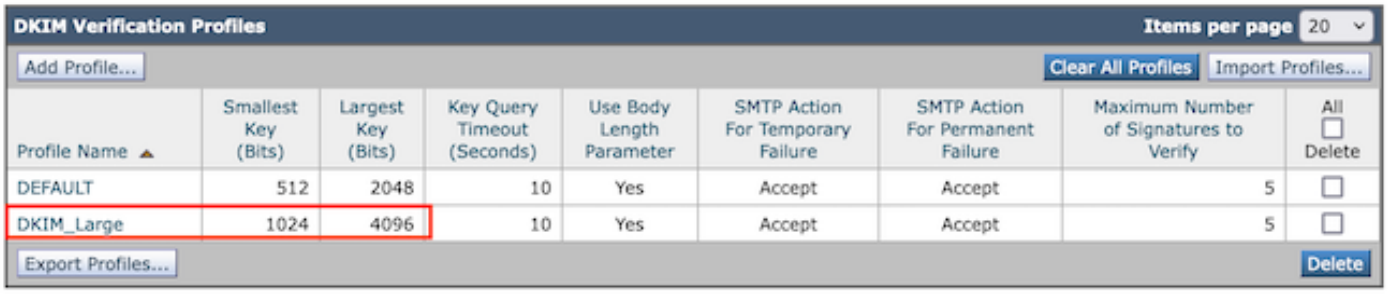
The SEG setup is very minimal to accommodate the new key sizes.

Navigate within the WebUI to:

- Mail Policies
  - Domain Keys
    - DKIM Verification Profiles



DKIM Verification Profile



DKIM Verification Profiles Summary Page

Apply the new DKIM Verification Profiles to the desired Incoming Mail Flow Policies:

- Mail Policies
  - Mail Flow Policies
    - Choose the desired Mail Flow Policy to apply the new DKIM Verification Profile based on your organizational preferences.
      - Scroll down to the Security Features section and locate "DKIM Verification:"
        - Select the appropriate profile of your choosing.



Note: Prior to AsyncOS 15.5, DKIM Verification was limited to 2048 bit and would pass a larger key size as unsigned.

Verify

The SEG does not log details regarding the key size within the Mail Logs or Message Tracking.

Before AsyncOS 15.5 a large 1024-4096 DKIM signing would pass as unsigned.

Some small indicators of the DKIM large key size require post-processing checks.

- Header retrieval and review of the b= value. This value is larger with the larger key size although it is not a direct value to compute.
- DKIM DNS record displays the public key of the pair which increases in size from (estimated) 180 bytes for 512-bit to 800 bytes for 4096-bit.
- A public search for "DKIM key size check," could produce multiple websites containing search tools to retrieve DKIM records. Using the Selector and domain, these sites query the DNS record and generate the key bit size, and DNS query results in the output.

Related Information

- Cisco Secure Email Gateway Launch Page to Support Guides
- Cisco Secure Email Gateway - Release Notes