

Configurar verificação de chave grande DKIM para gateway de email seguro

Contents

[Introdução](#)

[Pré-requisitos](#)

[Componentes Utilizados](#)

[Overview](#)

[Configurar](#)

[Verificar](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve o recurso expandido de verificação de tamanho de chave maior do DKIM para e-mails assinados.

Pré-requisitos

É desejável ter conhecimento geral das definições e da configuração do SEG.

Componentes Utilizados

- Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 e mais recente
- Perfis de verificação DKIM
- Políticas de fluxo de e-mail

"As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que você compreende o impacto potencial de qualquer comando."

Overview

O SEG pode executar a verificação de entrada de e-mails assinados por DKIM.

Historicamente, o intervalo de chaves de verificação do SEG era de 512 a 2048 antes do AsyncOS 15.5.

O AsyncOS 15.5 suporta o intervalo de chaves de 1024-4096 bits

As chaves com tamanho de 512 e 768 bits^{15.5} estão agora obsoletas, embora os perfis contendo

512-768 antes da atualização permaneçam em serviço.

Configurar

A configuração do SEG é muito mínima para acomodar os novos tamanhos de chave.

Navegue na WebUI para:

- Políticas de e-mail
 - Chaves de domínio
 - Perfis de verificação DKIM

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:

Perfil de verificação DKIM

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"/>

Página Resumo de Perfis de Verificação DKIM

Aplique os novos perfis de verificação DKIM às políticas de fluxo de e-mail de entrada desejadas:

- Políticas de e-mail
 - Políticas de fluxo de e-mail

- Escolha a Política de fluxo de e-mail desejada para aplicar o novo Perfil de verificação DKIM com base em suas preferências organizacionais.
 - Role para baixo até a seção Recursos de segurança e localize "Verificação DKIM:"
 - Selecione o perfil apropriado de sua escolha.



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

Use DKIM Verification Profile: DEFAULT
✓ DKIM_Large

 Observação: antes do AsyncOS 15.5, a verificação DKIM era limitada a 2048 bits e passaria um tamanho de chave maior como não assinado.

Verificar

O SEG não registra detalhes sobre o tamanho da chave nos logs de e-mail ou no rastreamento de mensagem.

Antes do AsyncOS 15.5, uma grande assinatura DKIM 1024-4096 passaria como não assinada.

Alguns indicadores pequenos do tamanho de chave grande DKIM exigem verificações pós-processamento.

- Recuperação do cabeçalho e revisão do valor $b=$. Esse valor é maior com o tamanho de chave maior, embora não seja um valor direto a ser computado.
- O registro DNS DKIM exibe a chave pública do par que aumenta em tamanho de (estimado) 180 bytes para 512 bits para 800 bytes para 4096 bits.
- Uma pesquisa pública para "DKIM key size check" (verificação do tamanho da chave DKIM) poderia produzir vários sites contendo ferramentas de pesquisa para recuperar registros DKIM. Usando o Seletor e o domínio, esses sites consultam o registro DNS e geram o tamanho do bit da chave, e os resultados da consulta DNS na saída.

Informações Relacionadas

- [Cisco Secure Email Gateway - Guia de configuração](#)
- [Página inicial do Cisco Secure Email Gateway para guias de suporte](#)
- [Cisco Secure Email Gateway - Notas de versão](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.