Criptografar e Descriptografar IM&Chave de Criptografia de Conformidade IP

Contents

Introdução

Este documento descreve como criptografar e descriptografar a chave de criptografia gerada pelo IM&P para a configuração criptografada de conformidade.

Pré-requisitos

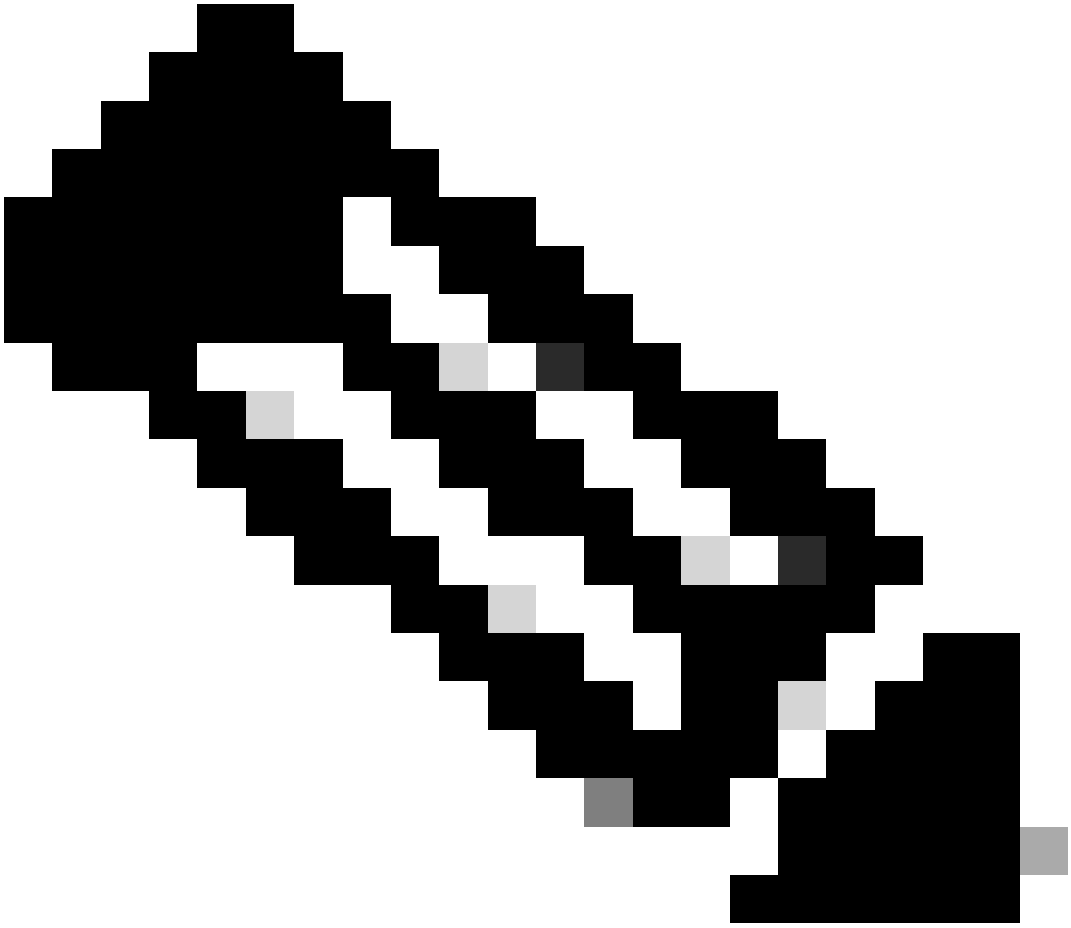
A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Message Archiver
- OpenSSL

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- MacOS 15.5
- IM e Presence(IM&P) versão 15su2
- OpenSSL 3.3.6



Note: Os comandos mostrados neste documento podem variar com base na sua versão ou plataforma OpenSSL. A Internet é uma boa fonte para encontrar aqueles que se adaptam ao seu ambiente.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O recurso Arquivador de Mensagens fornece uma solução básica de conformidade de IM. Esse recurso permite que seu sistema esteja em conformidade com as regulamentações que exigem o registro de todo o tráfego de mensagens instantâneas em sua empresa. Muitos setores exigem que as mensagens instantâneas obedeçam às mesmas diretrizes de conformidade normativa de todos os outros registros de negócios. Para estar em conformidade com essas normas, o sistema

deve registrar e arquivar todos os registros de negócios, e os registros arquivados devem ser recuperáveis.

Para maior segurança, você pode ativar um banco de dados criptografado para o Arquivador de Mensagens. Quando esta opção está habilitada, o Serviço de IM e Presença criptografa os IMs antes de arquivá-los no banco de dados externo. Com essa opção, todos os dados no banco de dados são criptografados e você não pode ler mensagens instantâneas arquivadas, a menos que possua a chave de criptografia.

A chave de criptografia pode ser baixada do Serviço de IM e Presença e usada em conjunto com qualquer ferramenta que você usar para exibir dados a fim de descriptografar dados arquivados.

Criptografar/descriptografar

1. Abra seu terminal OpenSSL.
2. Gerar chave privada.

```
openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:2048
```

3. Extraia a chave pública da chave privada.

```
openssl rsa -pubout -in private_key.pem -out public_key.pem
```

4. Neste ponto, temos 2 arquivos private_key.pem e public_key.pem.

- chave_privada.pem: Usado para descriptografar a chave criptografada do IM&P.
- public_key.pem: Esta é a chave que você compartilha com o servidor IM&P para permitir que eles criptografem a chave AES e IV.

Além disso, o servidor IM&P adiciona a codificação Base64 à chave de criptografia criptografada.

5. Baixe a chave de criptografia do servidor IM&P. Consulte a seção Download Encryption Key no guia Instant Messaging Compliance Guide for the IM and Presence Service.
6. Neste ponto, você tem 3 arquivos private_key.pem, public_key.pem e encrypted_key.pem.
7. Nesse caso encrypted_key.pem é codificado com base64 para transmissão segura.
8. Decodificar a chave criptografada codificada na Base64.

```
base64 -D -i encrypted_key.pem -o encrypted_key.bin
```

Isso remove a codificação Base64 e produz um arquivo de 256 bytes que foi originalmente

criptografado com sua chave RSA pública.

9. Descriptografe a chave criptografada com sua chave privada RSA.

```
openssl pkeyutl -decrypt -inkey private_key.pem -in encrypted_key.bin -out decryptedkey.bin
```

Isso descriptografa a chave AES (K) e o IV usados para a criptografia de mensagens IM&P.

Exemplo de arquivo descriptografado:

chave = 0ec39f2a22abf63d4452b932f12de

iv = 6683bb3d7e59e82e3fa9f42

10. Descriptografe as mensagens criptografadas AES.

```
openssl enc -aes-256-cbc -d -in encrypted.bin -out decrypted.txt -K <hex_key> -iv <hex_iv>
```

Troubleshooting

Um erro comum ao tentar descriptografar o arquivo criptografado é:

```
Public Key operation error 60630000:error:0200006C:rsa routines:rsa_ossl_private_decrypt:data greater t
```

Este erro ocorre quando você tenta RSA-descriptografar dados que são muito grandes para o tamanho de sua chave privada RSA. RSA só pode descriptografar dados até o tamanho de seu módulo. Em nosso caso, uma chave RSA de 2048 bits só pode descriptografar 256 bytes.

Se você verificar o arquivo de chave criptografada gerado por IM&P, itis 344 bytes. Você pode apenas descriptografar 256 bytes com nossa chave privada.

```
-rw-rw-rw-@ 1 testuser staff 344 Jun 5 13:10 encrypted_key.pem
```

Conforme mencionado anteriormente neste documento, a chave criptografada é codificada na Base64 para transmissão segura, o que adiciona bytes ao tamanho do arquivo.

Depois de remover a codificação Base64, você tem um arquivo de 256 bytes, facilmente descriptografável com nossa chave privada.

```
-rw-r--r-- 1 testuser staff 256 Jun 12 09:16 encrypted_key.bin
```

Práticas recomendadas de segurança

- Armazene sua chave privada (private_key.pem) com segurança.
- Não compartilhe sua chave privada com outras pessoas nem carregue-a em sistemas não confiáveis.
- Limpe arquivos temporários como decryptedkey.bin após a descriptografia.

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.