Utilizar o EEM para automatizar e-mails seguros para o usuário

Contents

Introdução

Este documento descreve o processo necessário para utilizar a ação "servidor de e-mail" no Embedded Event Manager (EEM) no Cisco IOS® XE para enviar e-mails seguros para um servidor SMTP usando o Transport Layer Security (TLS) na porta 587.

Há muitas advertências que você pode encontrar durante este processo, e é por isso que este artigo foi escrito para documentar as etapas necessárias para realizar isso.

Caso de uso

Muitos clientes consideram importante receber uma notificação por e-mail automaticamente após a ocorrência de um determinado evento. O subsistema EEM é uma ferramenta poderosa para detecção de eventos de rede e automação integrada, e pode fornecer uma maneira eficiente de automatizar notificações por e-mail em um dispositivo Cisco IOS XE. Por exemplo, talvez você queira monitorar um controle IPSLA e, em resposta a um syslog indicando uma alteração de estado, tomar algum tipo de ação e alertar os administradores de rede sobre o evento por e-mail. Essa ideia de "notificação por e-mail" pode ser aplicada a muitos outros cenários como um meio de chamar a atenção para qualquer evento específico que você deseja destacar.

Background

PEM significa "Privacy Enhanced Mail" e é um formato frequentemente usado para representar certificados e chaves. Este é o formato de certificado que os dispositivos Cisco IOS XE utilizam.

Os aplicativos seguros (como HTTPS ou SMTP seguro) frequentemente têm um "PEM empilhado", em que há vários certificados envolvidos, incluindo:

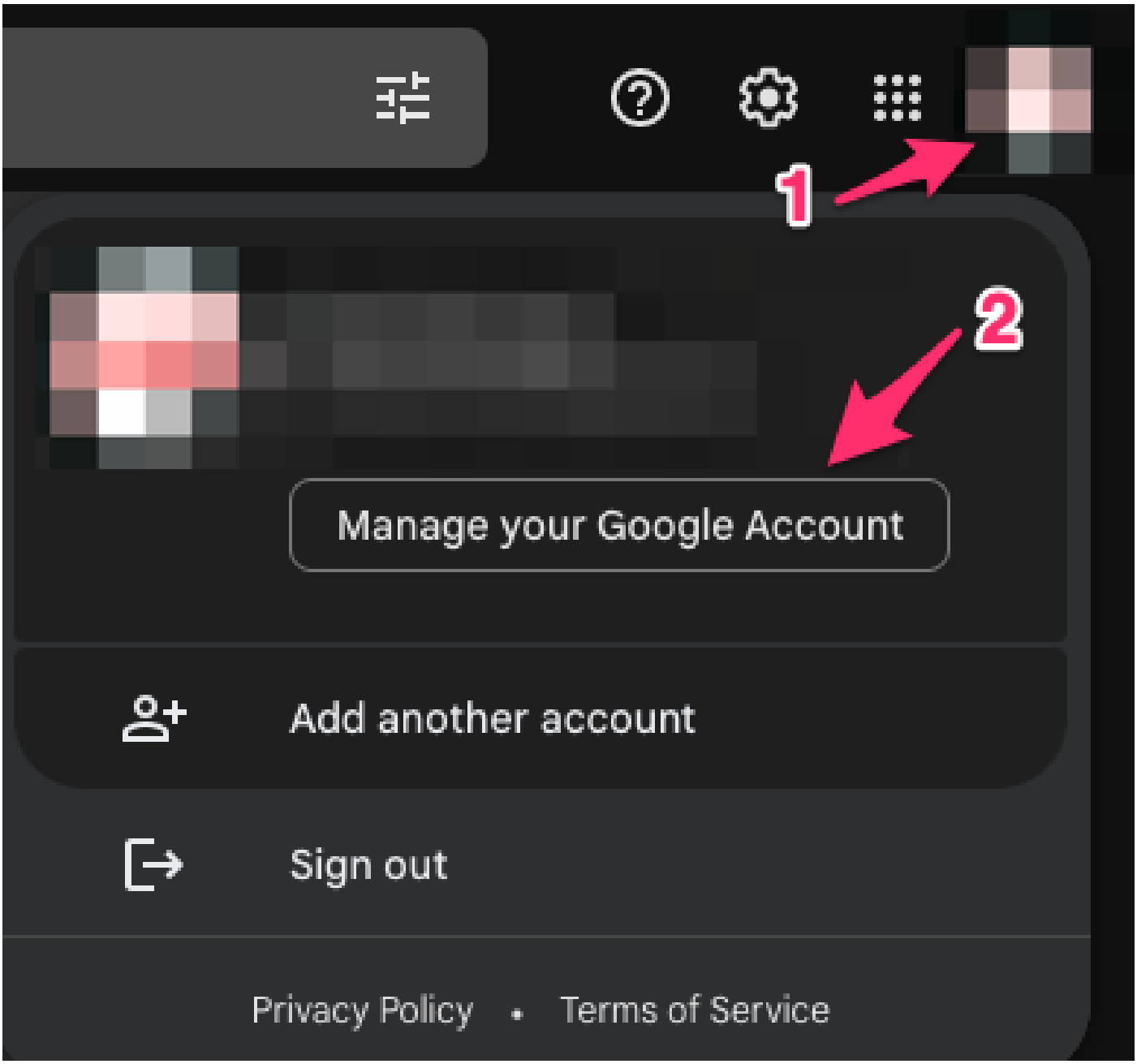
- Certificado raiz
- Certificado de assinatura (intermediário)
- Certificado de usuário final (ou servidor)

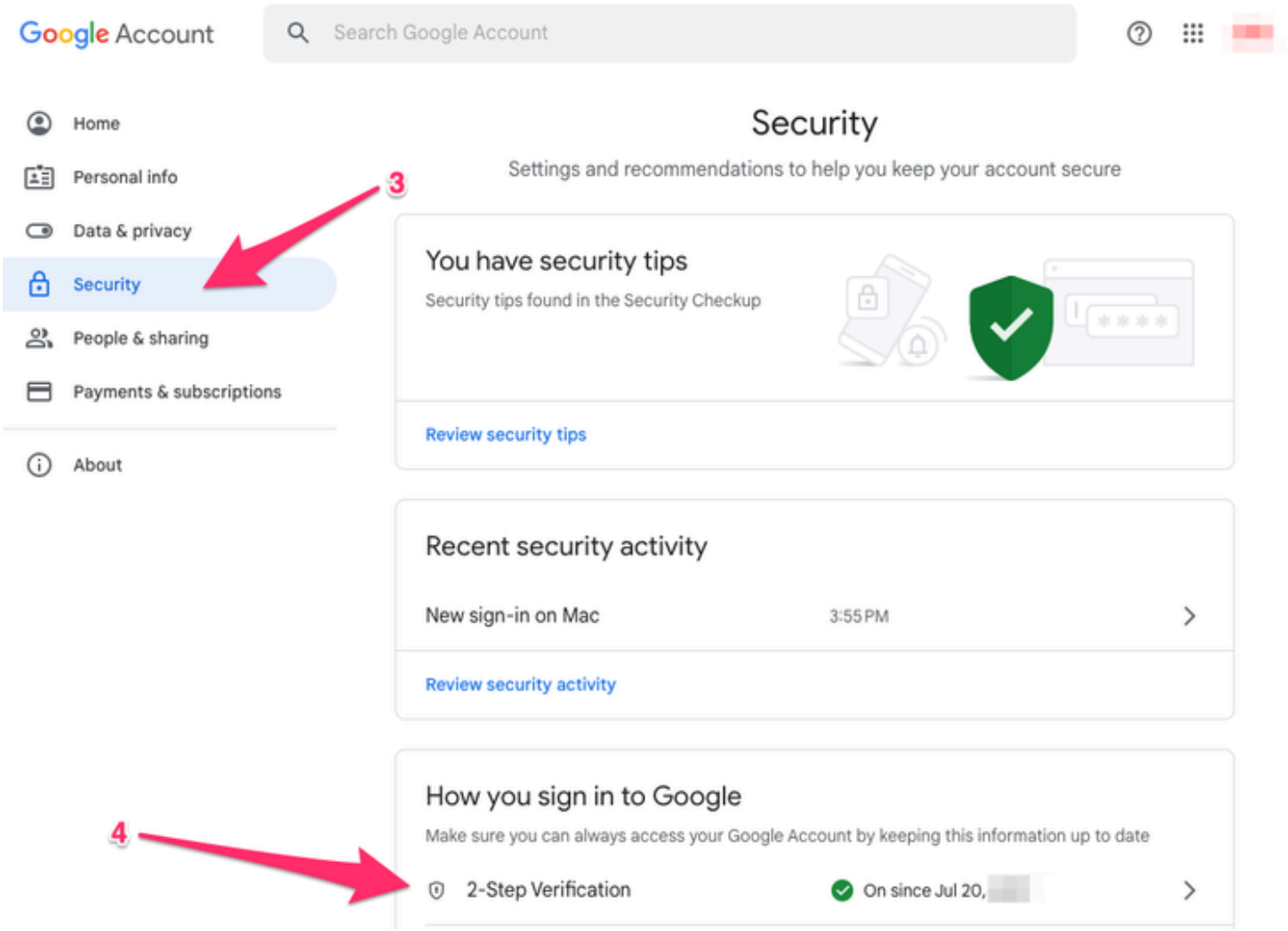
Configuração da conta do Gmail

Os serviços SMTP do Google serão usados como exemplo neste artigo. Os pré-requisitos são que você tenha uma conta do Gmail previamente configurada.

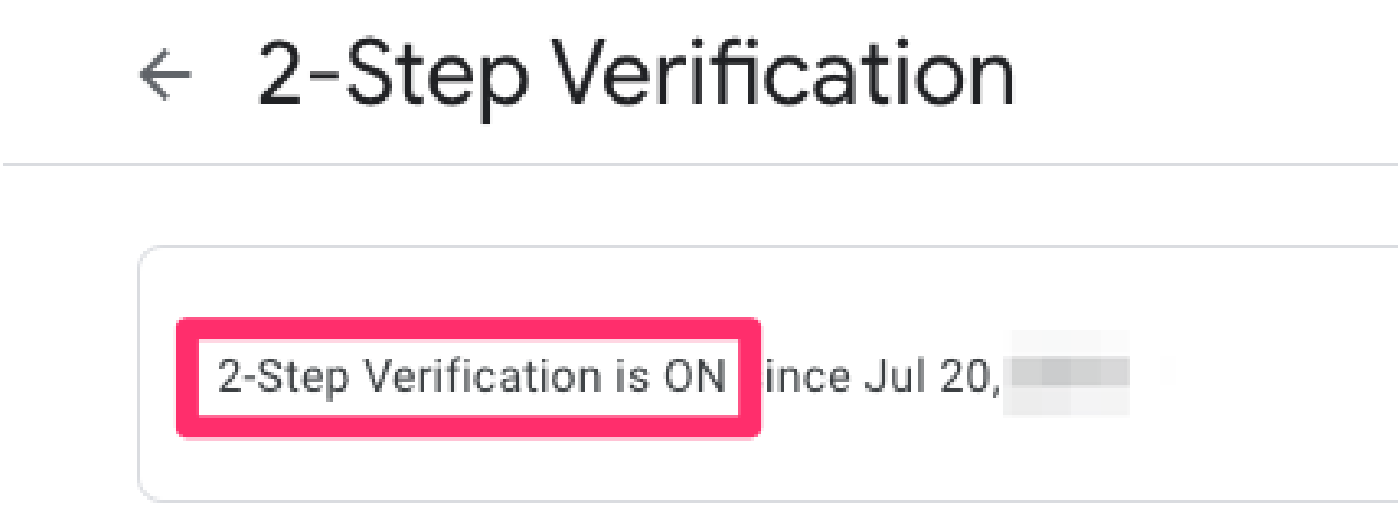
O Google permite enviar e-mails de clientes remotos para o Gmail. Havia uma configuração no Gmail para "aplicativos não seguros", e o aplicativo enfrentaria um erro se essa configuração não fosse permitida no final do Google. Essa configuração foi removida e, em seu lugar, é uma opção "Aplicativos Seguros", que pode ser acessada por meio de:

mail.google.com > Clique no seu Perfil (#1) > Gerencie a sua Conta do Google (#2) > Segurança (#3) > Como iniciar sessão no Google > Verificação em 2 Etapas (#4)


1
2
Manage your Google Account
Add another account
Sign out
Privacy Policy • Terms of Service



Nesta página, certifique-se de que a verificação em 2 etapas esteja ATIVADA.



Você pode rolar para baixo até "Senhas do aplicativo" para que o Gmail gere uma senha que possa ser usada para entrar em sua conta do Google a partir de um aplicativo que não suporta verificação em 2 etapas.

App passwords

App Passwords aren't recommended and are unnecessary in most cases. To help keep your account secure, use "Sign in with Google" to connect apps to your Google Account.

App passwords

None

← App passwords

App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

You don't have any app passwords.

Select the app and device you want to generate the app password for.

Mail | Select device

- **iPhone**
- **iPad**
- **BlackBerry**
- **Mac**
- **Windows Phone**
- **Windows Computer**
- **Other *(Custom name)***

GENERATE

App passwords

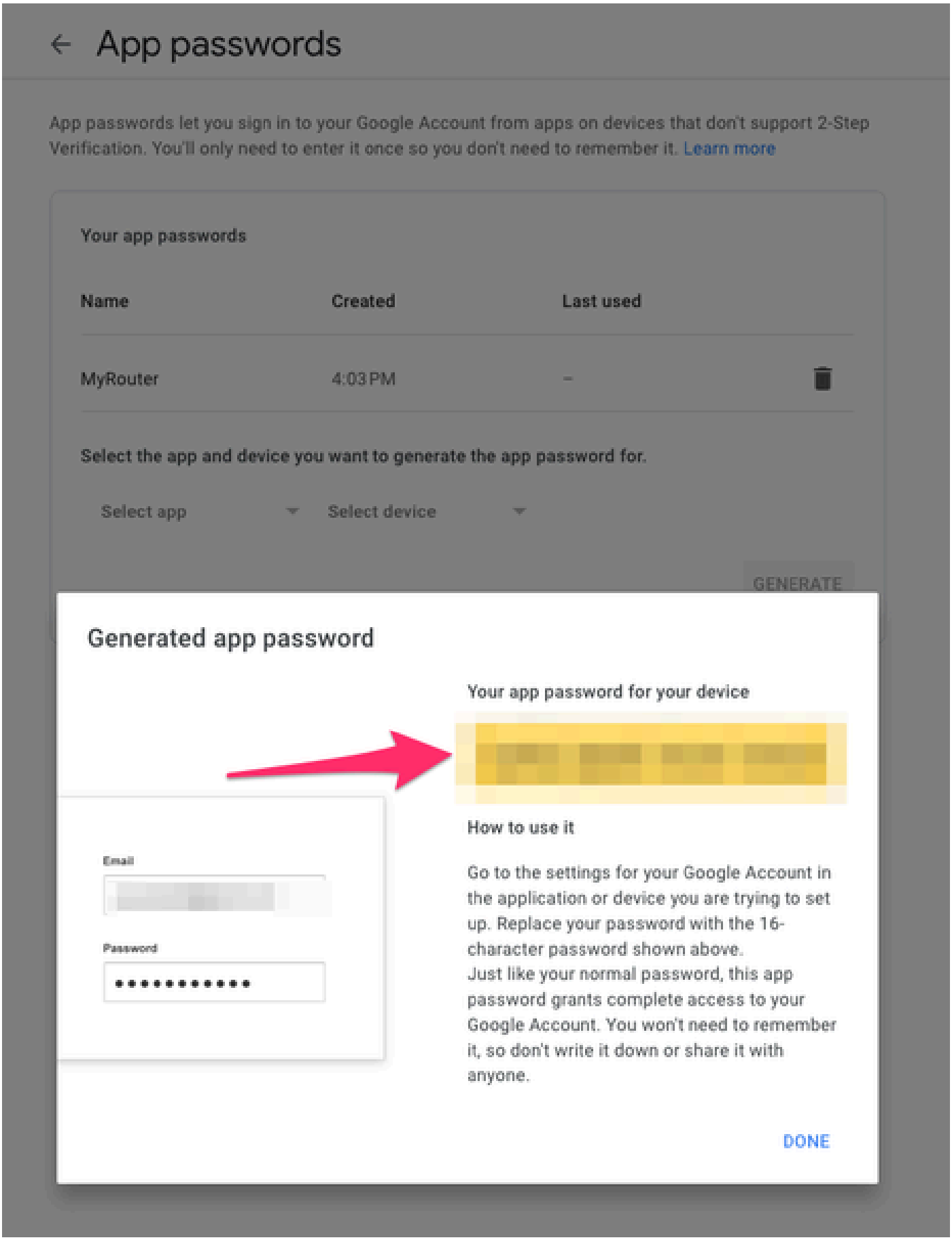
App passwords let you sign in to your Google Account from apps on devices that don't support 2-Step Verification. You'll only need to enter it once so you don't need to remember it. Learn more

You don't have any app passwords.

Select the app and device you want to generate the app password for.

MyRouter

GENERATE



A senha do aplicativo de 16 caracteres nesta captura de tela ficou indefinida, pois está vinculada a uma conta pessoal do Gmail.

Agora que você tem uma senha de aplicativo para o Gmail, você pode usá-la, juntamente com o nome da sua conta do Gmail, como o servidor de e-mail a ser usado para encaminhar o e-mail. O formato para especificar o servidor é "username:password@host".

Configuração EEM básica

Há muitas maneiras de personalizar um script de EEM para atender às suas necessidades exatas, mas este exemplo é um script de EEM básico para executar a funcionalidade de e-mail seguro:

```
(config)# event manager environment _email_from <username@gmail.com>
(config)# event manager environment _email_to <EMAIL@domain.com>
(config)# event manager environment _email_server <username>:<password>@smtp.gmail.com

(config)# event manager applet SendSecureEmailEEM
(config-applet)#  event none
(config-applet)#    action 0010 mail server "$_email_server" to "$_email_to" from "$_email_from" cc "$_
```

As configurações primeiro criam três variáveis de ambiente do EEM: _email_from, _email_to e _email_server. Cada uma delas é definida em uma variável para facilitar as alterações de configuração. Em seguida, crie o script SendSecureEmailEEM. O evento de disparo aqui é "none", de modo que você pode executar manualmente o script EEM à vontade usando "# event manager run SendSecureEmailEEM" (em vez de esperar um evento específico ser disparado). Em seguida, você tem apenas uma única ação de "servidor de e-mail" que cuida da geração de e-mail. As opções "secure tls" e "port 587" instruem o dispositivo a negociar o TLS na porta 587, que os servidores Gmail ouvirão.

Você também precisa garantir que seu campo "De" seja válido. Se você estiver autenticando como "Alice", mas estiver tentando enviar um email de "Bob", ocorrerá um erro porque Alice está falsificando o endereço de email de outra pessoa. O campo "De" precisa estar alinhado com a conta que está sendo usada para enviar o e-mail no servidor.

Problema visto com apenas certificados padrão instalados

O EEM utiliza o openssl para fazer uma conexão com o servidor SMTP. Para comunicação segura, o servidor envia de volta um certificado para o openssl em execução no Cisco IOSd. O IOSd procurará um ponto confiável associado a esse certificado.

Em um dispositivo Cisco IOS XE, os certificados para os servidores SMTP Gmail não são instalados por padrão. Eles devem ser importados manualmente para que a confiança seja estabelecida. Sem os certificados instalados, o handshake TLS falhará devido a um "certificado inválido".

Essas depurações são extremamente úteis para depurar qualquer problema de certificado:

```
debug event manager action mail
debug crypto pki API
debug crypto pki callbacks
debug crypto pki messages
debug crypto pki scep
debug crypto pki server
debug crypto pki transactions
debug crypto pki validation
debug ssl openssl errors
debug ssl openssl ext
debug ssl openssl msg
debug ssl openssl states
```

Você pode iniciar um Embedded Packet Capture (EPC) no roteador para capturar qualquer tráfego de ou para o servidor de e-mail quando o EEM for disparado:

```
! Trigger the EEM:
# event manager run SendSecureEmailEEM

<SNIP>

*Mar 15 21:51:32.798: CRYPTO_PKI: (A0693) Check for identical certs
*Mar 15 21:51:32.798: CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-

*Mar 15 21:51:32.798: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A

*Mar 15 21:51:32.799: CRYPTO_PKI: Cert record not found for issuer serial.
*Mar 15 21:51:32.799: CRYPTO_PKI : (A0693) Validating non-trusted cert
*Mar 15 21:51:32.799: CRYPTO_PKI: (A0693) Create a list of suitable trustpoints
*Mar 15 21:51:32.799: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer()
*Mar 15 21:51:32.799: CRYPTO_PKI: Unable to locate cert record by issuername
*Mar 15 21:51:32.799: CRYPTO_PKI: No trust point for cert issuer, looking up cert chain

*Mar 15 21:51:32.799: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
*Mar 15 21:51:32.799: CRYPTO_PKI: (A0693) No suitable trustpoints found
*Mar 15 21:51:32.799: CRYPTO_PKI: (A0693) Removing verify context

*Mar 15 21:51:32.799: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 32, ref
*Mar 15 21:51:32.799: CRYPTO_PKI: ca_req_context released
*Mar 15 21:51:32.799: CRYPTO_OPSSL: Certificate verification has failed
*Mar 15 21:51:32.799: CRYPTO_PKI: Rcvd request to end PKI session A0693.
*Mar 15 21:51:32.799: CRYPTO_PKI: PKI session A0693 has ended. Freeing all resources.
*Mar 15 21:51:32.800: >>> ??? [length 0005]
*Mar 15 21:51:32.800: 15 03 03 00 02
*Mar 15 21:51:32.800:
*Mar 15 21:51:32.800: >>> TLS 1.2 Alert [length 0002], fatal bad_certificate
*Mar 15 21:51:32.800: 02 2A
*Mar 15 21:51:32.800:
*Mar 15 21:51:32.800: SSL3 alert write:fatal:bad certificate
*Mar 15 21:51:32.801: P11:C_OpenSession slot 1 flags 6
*Mar 15 21:51:32.801: SSL_connect:error in error
*Mar 15 21:51:32.801: 0:error:1416F086:SSL routines:tls_process_server_certificate:certificate verify f
```

Por fim, o openssl não pode estabelecer a sessão TLS segura com o servidor SMTP, por isso ele

lança um erro de "certificado inválido", que faz com que o EEM pare de ser executado:

```
*Mar 15 21:51:32.801: %HA_EM-3-FMPD_SMTP: Error occurred when sending mail to SMTP server: username:pas
*Mar 15 21:51:32.802: %HA_EM-3-FMPD_ERROR: Error executing applet SendSecureEmailEEM statement 0010
```

A captura de pacote documentada a partir dessa troca está anexada como "NoCertificateInstalled.pcap". O pacote TLS final do roteador (10.122.x.x) para o servidor SMTP do Gmail (142.251.163.xx) mostra que a negociação TLS foi encerrada devido à mesma mensagem "Bad Certificate" vista anteriormente nas depurações.

```
Frame 33: 61 bytes on wire (488 bits), 61 bytes captured (488 bits)
Ethernet II, Src: Cisco_a3:c5:f0 (74:86:0b:a3:c5:f0), Dst: Cisco_f0:44:45 (00:08:30:f0:44:45)
Internet Protocol Version 4, Src: 10.122.xx.xx, Dst: 142.251.163.xx
Transmission Control Protocol, Src Port: 13306, Dst Port: 587, Seq: 189, Ack: 4516, Len: 7
Transport Layer Security
TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Bad Certificate)
Content Type: Alert (21)
Version: TLS 1.2 (0x0303)
Length: 2
Alert Message
Level: Fatal (2)
Description: Bad Certificate (42)
```

Certificados para Proteção de SMTP

Como os certificados que permitem que o dispositivo Cisco IOS XE confie nos servidores do Gmail estão ausentes, a correção é instalar um/todos esses certificados em um ponto confiável no dispositivo.

Por exemplo, as depurações completas do teste anterior mostram essas pesquisas de certificado que ocorreram:

```
CRYPTO_PKI(Cert Lookup) issuer="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US" serial number= 52 87 E0
CRYPTO_PKI(Cert Lookup) issuer="cn=GTS Root R1,o=Google Trust Services LLC,c=US" serial number= 02 03 B
CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-sa,c=BE" serial number
```

Um certificado para cada um desses emissores precisa ser instalado em um ponto confiável para que o dispositivo possa estabelecer uma sessão segura com os servidores SMTP do Gmail. Você pode criar um ponto confiável para cada emissor usando estas configurações:

```
crypto pki trustpoint CA-GTS-1C3
  enrollment terminal
```

```
  revocation-check none
  chain-validation stop

crypto pki trustpoint CA-GTS-Root-R1
  enrollment terminal
  revocation-check none
  chain-validation stop

crypto pki trustpoint CA-GlobalSign-Root
  enrollment terminal
  revocation-check none
  chain-validation stop

crypto pki trustpoint CA-gmail-SMTP
  enrollment terminal
  revocation-check none
  chain-validation stop
```

Agora você tem um ponto de confiança para cada emissor configurado; no entanto, ainda não há certificados reais associados a eles. Eles são essencialmente pontos de confiança em branco:

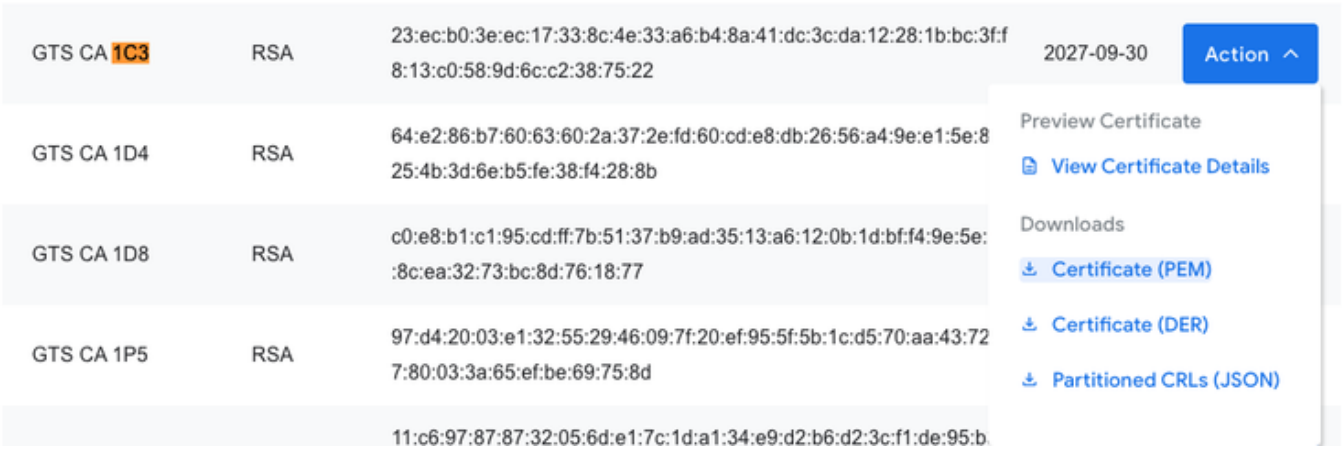
```
# show run | sec crypto pki certificate chain CA-
crypto pki certificate chain CA-GTS-1C3
crypto pki certificate chain CA-GTS-Root-R1
crypto pki certificate chain CA-GlobalSign-Root
crypto pki certificate chain CA-gmail-SMTP
```

Você deve rastrear onde esses certificados estão e instalá-los no dispositivo.

Procurando on-line por "Google Trust Services 1C3", encontramos rapidamente o repositório de certificados do Google Trust Services:

https://pki.goog/repository/

Depois de expandir todos os certificados nessa página, você pode procurar "1C3", clicar no menu suspenso "Ação" e fazer o download do certificado PEM:



Abrir o arquivo PEM baixado com um editor de texto mostra que este é apenas um certificado que pode ser importado para o dispositivo Cisco IOS XE sob o ponto de confiança que você criou anteriormente:

```
-----BEGIN CERTIFICATE-----
MIIFljCCA36gAwIBAgINAgO8U1lrNMcY9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU
<snip>
AJ2xDx8hcFH1mt0G/FX0Kw4zd8NLQsLxdxP8c4CU6x+7Nz/OAipmsHMdMqUybDKw
juDEI/9bfU1lcKwrmz3O2+BtjjKAvpafkmO8l7tdufThcV4q5O8DIrGKZTqPwJNl
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDBlHz4n/FsRC6UfTd
-----END CERTIFICATE-----
```

Você pode importá-lo no ponto de confiança "CA-GTS-1C3" usando os comandos de configuração:

```
(config)# crypto pki authenticate CA-GTS-1C3

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIFljCCA36gAwIBAgINAgO8U1lrNMcY9QFQZjANBgkqhkiG9w0BAQsFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU
<snip>
juDEI/9bfU1lcKwrmz3O2+BtjjKAvpafkmO8l7tdufThcV4q5O8DIrGKZTqPwJNl
1IXNDw9bg1kWRxYtnCQ6yICmJhSFm/Y3m6xv+cXDBlHz4n/FsRC6UfTd

Certificate has the following attributes:
Fingerprint MD5: 178EF183 43CCC9E0 ECB0E38D 9DEA03D8
Fingerprint SHA1: 1E7EF647 CBA15028 1C608972 57102878 C4BD8CDC
Certificate validated - Signed by existing trustpoint CA certificate.

Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)#
```

E então você pode confirmar se o certificado foi instalado:

```
# show run | sec crypto pki certificate chain CA-GTS-1C3
crypto pki certificate chain CA-GTS-1C3
 certificate ca 0203BC53596B34C718F5015066
  30820596 3082037E A0030201 02020D02 03BC5359 6B34C718 F5015066 300D0609
  2A864886 F70D0101 0B050030 47310B30 09060355 04061302 55533122 30200603
  55040A13 19476F6F 676C6520 54727573 74205365 72766963 6573204C 4C433114
  <snip>
  E1715E2A E4EF0322 B18A653A 8FC09365 D485CD0F 0F5B8359 1647162D 9C243AC8
  80A62614 859BF637 9BAC6FF9 C5C30651 F3E27FC5 B1100BA51 F4DD
    quit
```

```
#show crypto pki certificates verbose CA-GTS-1C3
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 0203BC53596B34C718F5015066
  Certificate Usage: Signature
  Issuer:
    cn=GTS Root R1
    o=Google Trust Services LLC
    c=US
  Subject:
    cn=GTS CA 1C3
    o=Google Trust Services LLC
    c=US
  CRL Distribution Points:
    http://crl.pki.goog/gtsr1/gtsr1.crl
  Validity Date:
    start date: 00:00:42 UTC Aug 13 2020
    end date: 00:00:42 UTC Sep 30 2027
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: 178EF183 43CCC9E0 ECB0E38D 9DEA03D8
  Fingerprint SHA1: 1E7EF647 CBA15028 1C608972 57102878 C4BD8CDC
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 71351D27
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: E4AF2B26 711A2B48 27852F52 662CEFF0 8913713E
    Authority Info Access:
        OCSP URL: http://ocsp.pki.goog/gtsr1
        CA ISSUERS: http://pki.goog/repo/certs/gtsr1.der
    X509v3 CertificatePolicies:
        Policy: 2.23.140.1.2.2
        Policy: 2.23.140.1.2.1
        Policy: 1.3.6.1.4.1.11129.2.5.3
            Qualifier ID: 1.3.6.1.5.5.7.2.1
            Qualifier Info: https://pki.goog/repository/
    Extended Key Usage:
        Client Auth
        Server Auth
  Cert install time: 02:31:20 UTC Mar 16 2023
Cert install time in nsec: 1678933880873946880
  Associated Trustpoints: CA-GTS-1C3
```

Em seguida, você pode instalar os certificados para os outros dois emissores.

CA-GTS-Root-R1:

Configuração:

Spoiler (Realce para ler)

```
(config)# crypto pki authenticate CA-GTS-Root-R1

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIFVzCCAz+gAwIBAgINAgPlk28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQsw
CQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU
<snip>
2tIMPNuzjsmhDYAPexZ3FL//2wmUspO8IFgV6dtxQ/PeEMMA3KgqlbbC1j+Qa3bb
bP6MvPJwNQzcmRk13NfIRmPVNnGuV/u3gm3c

Certificate has the following attributes:
Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40
Fingerprint SHA1: E58C1CC4 913B3863 4BE9106E E3AD8E6B 9DD9814A

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)# end
```

(config)# crypto pki authenticate CA-GTS-Root-R1Insira o certificado CA codificado na base 64.Termine com uma linha em branco ou a palavra "quit" sozinha em uma linhaMIIFVzCCAz+AwIBAgINAgPlk28xsBNJiGuiFzANBgkqhkiG9w0BAQwFADBHMQswCQYDVQQGEwJVzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExMQzEU<snip>2tIMPNuzjsmhDYAPexZ3FL//2wNQzcmRk13NfIRmPVNnGuV/u3gm3cCertificate tem os seguintes atributos:Impressão digital MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40 Impressão digital SHA1: E58C1CC4 913B3863 4BE9106E E3AD8E 9DD9814A% Você aceita este certificado? [sim/não]: simCertificado CA Trustpoint aceito.% Certificado importado com êxito (config)# end

Verificação de configuração atual:

Spoiler (Realce para ler)

```
# show run | sec crypto pki certificate chain CA-GTS-Root-R1
crypto pki certificate chain CA-GTS-Root-R1
 certificate ca 0203E5936F31B01349886BA217
  30820557 3082033F A0030201 02020D02 03E5936F 31B01349 886BA217 300D0609
  2A864886 F70D0101 0C050030 47310B30 09060355 04061302 55533122 30200603
  <snip>
  6775C119 3A2B474E D3428EFD 31C81666 DAD20C3C DBB38EC9 A10D800F 7B167714
  BFFFDB09 94B293BC 205815E9 DB7143F3 DE10C300 DCA82A95 B6C2D63F 906B76DB
  6CFE8CBC F270350C DC991935 DCD7C846 63D53671 AE57FBB7 826DDC
    quit
```

show run | sec crypto pki certificate chain CA-GTS-Root-R1crypto pki certificate chain CA-GTS-Root-R1 certificate ca 0203E5936F31B01349886BA217 30820557 3082033F A0030201 02020D02 03E5936F 31B01349 886BA217 300D0609 2A864886 F70D0 101 0C050030 47310B30 09060355 04061302 55533122 30200603 <snip> 6775C119 3A2B474E D3428EFD 31C81666 DAD20C3C DBB38EC9 A10D800F 7B167714 BFFFDB09 94B293BC 205815E9 DB7143F3 DE110 C300 DCA82A95 B6C2D63F 906B76DB 6CFE8CBC F270350C DC991935 DCD7C846 63D53671 AE57FBB7 826DDC quit

Mostrar verificação de criptografia:

Spoiler (Realce para ler)

```
# show crypto pki certificates verbose CA-GTS-Root-R1
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 0203E5936F31B01349886BA217
  Certificate Usage: Signature
  Issuer:
    cn=GTS Root R1
    o=Google Trust Services LLC
    c=US
  Subject:
    cn=GTS Root R1
    o=Google Trust Services LLC
    c=US
  Validity Date:
    start date: 00:00:00 UTC Jun 22 2016
    end date: 00:00:00 UTC Jun 22 2036
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (4096 bit)
  Signature Algorithm: SHA384 with RSA Encryption
  Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40
  Fingerprint SHA1: E58C1CC4 913B3863 4BE9106E E3AD8E6B 9DD9814A
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: E4AF2B26 711A2B48 27852F52 662CEFF0 8913713E
    X509v3 Basic Constraints:
        CA: TRUE
    Authority Info Access:
  Cert install time: 14:39:38 UTC Mar 13 2023
Cert install time in nsec: 1678718378546968064
  Associated Trustpoints: CA-GTS-Root-R1 Trustpool
```

show crypto pki certificates verbose CA-GTS-Root-R1CA Certificate Status: Available Version: 3 Certificate Serial Number (hex): 0203E5936F31B01349886BA217 Certificate Usage: Signature Issuer: cn=GTS Root R1 o=Google Trust Services LLC c=US Subject: cn=GTS Root R1 o=Google Trust Services LLC c=US Data de validade: data de início: 00:00:00 UTC Jun 2 2 Data final de 2016: 00:00:00 UTC 22 de junho de 2036 Informações da chave do assunto: Public Key Algorithm: rsaEncryption RSA Chave pública: (4096 bit) Algoritmo de assinatura: SHA384 com RSA Encryption Fingerprint MD5: 05FED0BF 71A8A376 63DA01E0 D852DC40 Impressão digital SHA1: E 58C1CC4 913B3863 4BE9106E E3AD8E6B 9DD9814A X509v3 extensões: X509v3 Uso da chave: 86000000 Assinatura digital Sinal de cert. assinatura CRL X509v3 ID da chave do assunto: E4AF2B26 711A2B48 27852F52 662CEFF0 8913713E X 509v3 Restrições Básicas: CA: TRUE Authority Info Acesso: Hora de instalação do certificado: 14:39:38 UTC 13 de março de 2023 Hora de instalação do certificado em nsec: 1678718378546968064 Pontos de Confiança Associados: CA-GTS-Root-R1 Trustpool

CA-GlobalSign-Root:

Este certificado foi encontrado neste local:

https://support.globalsign.com/ca-certificates/root-certificates/globalsign-root-certificates

Configuração:

Spoiler (Realce para ler)

```
(config)# crypto pki authenticate CA-GlobalSign-Root

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
A1UEBhMCQkUxGTAXBgNVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv
<snip>
DKqC5JlR3XC321Y9YeRq4VzW9v493kHMB65jUr9TU/Qr6cf9tveCX4XSQRjbgbME
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==

Certificate has the following attributes:
Fingerprint MD5: 3E455215 095192E1 B75D379F B187298A
Fingerprint SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)# end
```

(config)# crypto pki authenticate CA-GlobalSign-RootInsira o certificado CA codificado na base 64.Termine com uma linha em branco ou a palavra "quit" sozinha em uma linhaMIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkGA1UEBhM NVBAoTEEdsb2JhbFNpZ24gbnYtc2ExEDAOBgNVBAsTB1Jv<snip>DKqC5JlR3XC321Y9YeRq4VzW9v4 IBvFSDJ3gyICh3WZlXi/EjJKSZp4A==O certificado tem os seguintes atributos:Impressão digital MD5: 3E455215 095192E1 B75D379F B187298A Impressão digital SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C% Aceita este certificado? [sim/não]: simCertificado CA Trustpoint aceito.% Certificado importado com êxito (config)# end

Verificação de configuração atual:

Spoiler (Realce para ler)

```
# show run | sec crypto pki certificate chain CA-GlobalSign-Root
crypto pki certificate chain CA-GlobalSign-Root
 certificate ca 040000000001154B5AC394
  30820375 3082025D A0030201 02020B04 00000000 01154B5A C394300D 06092A86
  <snip>
  2AC45631 95D06789 852BF96C A65D469D 0CAA82E4 9951DD70 B7DB563D 61E46AE1
  5CD6F6FE 3DDE41CC 07AE6352 BF5353F4 2BE9C7FD B6F7825F 85D24118 DB81B304
  1CC51FA4 806F1520 C9DE0C88 0A1DD666 55E2FC48 C9292669 E0
    quit
```

show run | sec crypto pki certificate chain CA-GlobalSign-Rootcrypto pki certificate chain CA-GlobalSign-Root certificate ca 040000000001154B5AC394 30820375 3082025D A0030201 02020B04 00000000 01154B5A C394300D 06092A86 <snip> 2AC45631 95D06789 852BF96C A65D469D 0CAA82E4 9951DD70 B7DB 563D 61E46AE1 5CD6F6FE 3DDE41CC 07AE6352 BF5353F4 2BE9C7FD B6F7825F 85D24118 DB81B304 1CC51FA4 806F1520 C DE0C88 0A1DD66 55E2FC888 C9292669 E0 quit

Mostrar verificação de criptografia:

Spoiler (Realce para ler)

```
#show crypto pki certificates verbose CA-GlobalSign-Root
CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 040000000001154B5AC394
Certificate Usage: Signature
Issuer:
cn=GlobalSign Root CA
ou=Root CA
o=GlobalSign nv-sa
c=BE
Subject:
cn=GlobalSign Root CA
ou=Root CA
o=GlobalSign nv-sa
c=BE
Validity Date:
start date: 12:00:00 UTC Sep 1 1998
end date: 12:00:00 UTC Jan 28 2028
Subject Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (2048 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: 3E455215 095192E1 B75D379F B187298A
Fingerprint SHA1: B1BC968B D4F49D62 2AA89A81 F2150152 A41D829C
X509v3 extensions:
X509v3 Key Usage: 6000000
Key Cert Sign
CRL Signature
X509v3 Subject Key ID: 607B661A 450D97CA 89502F7D 04CD34A8 FFFCFD4B
X509v3 Basic Constraints:
CA: TRUE
Authority Info Access:
Cert install time: 03:03:01 UTC Mar 16 2023
Cert install time in nsec: 1678935781942944000
Associated Trustpoints: CA-GlobalSign-Root
```

#show Certificados crypto pki verbose CA-GlobalSign-RootCA CertificateStatus: AvailableVersion: 3Certificate Serial Number (hex): 040000000001154B5AC394Certificate Usage: SignatureIssuer: cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BESubject: cn=GlobalSign Root CAou=Root CAo=GlobalSign nv-sac=BEValidity Data: 12:00:00 UTC p 1 1998data final: 12:00:00 UTC 28 Jan 2028Informações da chave do assunto:Algoritmo de chave pública: rsaEncryptionChave pública RSA: (2048 bit)Algoritmo de assinatura: SHA1 com criptografia

RSAImpressão digital MD5: 3E455215 095192E1 B75D379F B187298A Impressão digital SHA1: B1BC968B D4F49D 62 2Extensões 2A89A81 F2150152 A41D829C X509v3:X509v3 Uso da chave: 6000000Sinal de cert. de chaveAssinatura CRLX509v3 ID da chave do assunto: 607B661A 450D97CA 89502F7D 04CD34A8 FFFCFD4B X509v3 Restrições básicas:CA TRUEAuthority Info Acesso:Hora de instalação do certificado: 03:03:01 UTC 16 de março de 2023 Hora de instalação do certificado em nsec: 1678935781942944000Pontos de Confiança Associados: CA-GlobalSign-Root

CA-gmail-SMTP:

O certificado TLS para os servidores do Gmail (CA-gmail-SMTP) foi encontrado usando as etapas documentadas aqui: Use certificados TLS para transporte seguro

Configuração:

Spoiler (Realce para ler)

```
(ca-trustpoint)# crypto pki authenticate CA-gmail-SMTP

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIEhjCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d3w9DANBgkqhkiG9w0BAQsFADBG
MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
<snip>
b1J2gZAyjyd4nfFRG1jeL5KrsfUR9hIXufqySvlPUoPuKSi3fvsIS21BYEXEe8uZ
gBxJaeTUjncvow==

Trustpoint 'CA-gmail-SMTP' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
Fingerprint MD5: 19651FBE 906A414D 6D57B783 946F30A2
Fingerprint SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

(config)#
```

(ca-trustpoint)# crypto pki authenticate CA-gmail-SMTPEnsira o certificado CA codificado de base 64.Termine com uma linha em branco ou a palavra "quit" sozinha em uma linhaMIIEhjCCA26gAwIBAgIQUofgQKT+9wcSaLBP3d9w9DANBgkqhkiG9w0BAQsFADBGMQswCQYDV
JVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM<snip>b1J2gZAyjyd4nfFRG1jeL5KrsfUR
JaeTUjncvow==Trustpoint 'CA-gmail-SMTP' é uma CA subordinada.mas o certificado não é uma CA.É necessária verificação manualO certificado tem os seguintes atributos:Impressão digital MD5: 19651FBE 906A414D 6D57B783 946F30A2 Impressão digital SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2 825% Você aceita este certificado? [sim/não]: simCertificado CA Trustpoint aceito.% Certificado importado com êxito(config)#

Verificação de configuração atual:

Spoiler (Realce para ler)

```
# show run | sec crypto pki certificate chain CA-gmail-SMTP
 crypto pki certificate chain CA-gmail-SMTP
  certificate ca 5287E040A4FEF7071268B04FDDDDF0F4
  30820486 3082036E A0030201 02021052 87E040A4 FEF70712 68B04FDD DDF0F430
  0D06092A 864886F7 0D01010B 05003046 310B3009 06035504 06130255 53312230
  <snip>
  92ABB1F5 11F61217 B9FAB24A F94F5283 EE2928B7 7EFB084B 6D416045 C47BCB99
  801C4969 E4D48E77 2FA3
    quit
```

show run | sec crypto pki certificate chain CA-gmail-SMTP crypto pki certificate chain CA-gmail-SMTP certificate ca 5287E040A4FEF7071268B04FDDDF0F4 30820486 3082036E A0030201 02021052 87E040A4 FEF70712 68B04FDD DDF0F430 0D06092A 864886F7 0D01010B 05003046 310B300906035504 06130255 53312230 <snip> 92ABB1F5 11F61217 B9FAB24A F94F5283 E2928B7 7EFB084B 6D416045 C47BCB9 801C4969 E4D48E77 2FA3 quit

Mostrar verificação de criptografia:

Spoiler (Realce para ler)

```
# show crypto pki certificates verbose CA-gmail-SMTP
CA Certificate
Status: Available
Version: 3
Certificate Serial Number (hex): 5287E040A4FEF7071268B04FDDDDF0F4
Certificate Usage: Signature
Issuer:
cn=GTS CA 1C3
o=Google Trust Services LLC
c=US
Subject:
cn=smtp.gmail.com
CRL Distribution Points:
http://crls.pki.goog/gts1c3/moVDfISia2k.crl
Validity Date:
start date: 09:15:03 UTC Feb 20 2023
end date: 09:15:02 UTC May 15 2023
Subject Key Info:
Public Key Algorithm: ecEncryption
EC Public Key: (256 bit)
Signature Algorithm: SHA256 with RSA Encryption
Fingerprint MD5: 19651FBE 906A414D 6D57B783 946F30A2
Fingerprint SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825
X509v3 extensions:
X509v3 Key Usage: 80000000
Digital Signature
X509v3 Subject Key ID: 5CC36972 D07FE997 510E1A67 8A8ECC23 E40CFB68
X509v3 Basic Constraints:
CA: FALSE
X509v3 Subject Alternative Name:
smtp.gmail.com
IP Address :
OtherNames :
X509v3 Authority Key ID: 8A747FAF 85CDEE95 CD3D9CD0 E24614F3 71351D27
Authority Info Access:
OCSP URL: http://ocsp.pki.goog/gts1c3
```

```
CA ISSUERS: http://pki.goog/repo/certs/gts1c3.der
X509v3 CertificatePolicies:
Policy: 2.23.140.1.2.1
Extended Key Usage:
Server Auth
Cert install time: 03:10:41 UTC Mar 16 2023
Cert install time in nsec: 1678936241822955008
Associated Trustpoints: CA-gmail-SMTP
```

show crypto pki certificates verbose CA-gmail-SMTPCA CertificateStatus: AvailableVersion: 3Certificate Serial Number (hex): 5287E040A4FEF7071268B04FDDDF0F4Certificate Usage: SignatureIssuer: cn=GTS CA 1C3o=Google Trust Services LLCc=USSubject: cn=smtp.gmail.comCRL Distribution Points: http://crls.pki.goog/gts1c3/moVDfISia2k.crlValidity Data: data de início: 09:15:03 UTC Fev 20 2023data final: 09:15:02 UTC 15 de maio de 2023Informações da chave do assunto:Algoritmo de chave pública: ecEncryptionEC Chave pública: (256 bits)Algoritmo de assinatura: SHA256 com criptografia RSAImpressão digital MD5: 19651FBE 906A414D 6D57B783 946F30A2 Impressão digital SHA1: 4EF392CB EEB46D5E 47433953 AAEF313F 4C6D2825 X509v3 extensões:X509v3 Uso da chave: 80000000Assinatura digitalX509v3 ID da chave do assunto: 5CC36972 D07FE97 510E1A67 8A8ECC23 E40CFB68 X509v3 Restrições Básicas:CA: FALSEX509v3 Nome Alternativo do Assunto:smtp.gmail.com Endereço IP: OutrosNomes: X509v3 ID da Chave de Autoridade: 8A747FAF 85CDE95 CD3D9CD0 E24614F3 71351D27 Acesso a Informações de Autoridade:URL do OCSP: http://ocsp.pki.goog/gts1c3CA EMISSORES: http://pki.goog/repo/certs/gts1c3.derX509v3 CertificatePolicies:Política: 2.23.140.1.2.1Uso Estendido de Chave:Hora de instalação do AuthCert do Servidor: 03 10:41 UTC 16 de março de 2023 Tempo de instalação do certificado em nsec: 1678936241822955008Pontos de Confiança Associados: CA-gmail-SMTP

Uma maneira mais fácil de encontrar os certificados

Como alternativa, você pode tentar usar uma chamada openssl de um servidor/laptop como uma maneira mais fácil de obter os certificados de um servidor SMTP sem ter que usar depurações e procurar no Google para rastreá-los:

```
openssl s_client -showcerts -verify 5 -connect gmail-smtp-in.l.google.com:25 -starttls smtp
```

Você também pode use smtp.gmail.com:

```
openssl s_client -showcerts -verify 5 -connect smtp.gmail.com:25 -starttls smtp
```

As saídas dessa chamada incluirão os próprios certificados reais que podem ser usados para as configurações de "crypto pki authenticate <trustpoint>".

Testando novamente o EEM com SMTP seguro

Agora que os certificados são aplicados ao dispositivo Cisco IOS XE, o script EEM enviará as mensagens SMTP seguras como esperado.

```
# event manager run SendSecureEmailEEM
```

Verifique o Spoiler para obter todas as saídas de depuração de criptografia e ssl:

Spoiler (Realce para ler)

```
# event manager run SendSecureEmailEEM

*Mar 16 03:28:50.673: CRYPTO_OPSSL: Allocated the memory for OPSSLContext
*Mar 16 03:28:50.673: CRYPTO_OPSSL: Set cipher specs to mask 0x02FC0000 for version 128
*Mar 16 03:28:50.674: Set the Default EC Curve list: 0x70Set the EC curve list: secp521r1:secp384r1:prin
*Mar 16 03:28:50.674: opssl_SetPKIInfo entry
*Mar 16 03:28:50.674: CRYPTO_PKI: (A069B) Session started - identity selected (TP-self-signed-486541296)
*Mar 16 03:28:50.674: CRYPTO_PKI: Begin local cert chain retrieval.
*Mar 16 03:28:50.674: CRYPTO_PKI(Cert Lookup) issuer="cn=IOS-Self-Signed-Certificate-486541296" serial n

*Mar 16 03:28:50.674: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
1C 7F 3D 52 67 66 D5 59 E2 66 58 E7 8B E7 9B 8E

*Mar 16 03:28:50.675: CRYPTO_PKI: Done with local cert chain fetch 0.
*Mar 16 03:28:50.675: CRYPTO_PKI: Rcvd request to end PKI session A069B.
*Mar 16 03:28:50.675: CRYPTO_PKI: PKI session A069B has ended. Freeing all resources.TP-self-signed-486
*Mar 16 03:28:50.675: opssl_SetPKIInfo done.
*Mar 16 03:28:50.675: CRYPTO_OPSSL: Common Criteria is disabled on this session.Disabling Common Criter

*Mar 16 03:28:50.675: CRYPTO_OPSSL: ciphersuites ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA
*Mar 16 03:28:50.676: Handshake start: before SSL initialization
*Mar 16 03:28:50.676: SSL_connect:before SSL initialization
*Mar 16 03:28:50.676: >>> ??? [length 0005]
*Mar 16 03:28:50.676: 16 03 01 00 95
*Mar 16 03:28:50.676:
*Mar 16 03:28:50.676: >>> TLS 1.2 Handshake [length 0095], ClientHello
*Mar 16 03:28:50.676: 01 00 00 91 03 03 26 4B 9F B3 44 94 FD 5F FD A1
<snip>
*Mar 16 03:28:50.679: 03 03 01 02 01
*Mar 16 03:28:50.679:
*Mar 16 03:28:50.679: SSL_connect:SSLv3/TLS write client hello
*Mar 16 03:28:50.692: <<< ??? [length 0005]
*Mar 16 03:28:50.692: 16 03 03 00 3F
*Mar 16 03:28:50.692:
*Mar 16 03:28:50.692: SSL_connect:SSLv3/TLS write client hello
*Mar 16 03:28:50.692: <<< TLS 1.2 Handshake [length 003F], ServerHello
*Mar 16 03:28:50.692: 02 00 00 3B 03 03 64 12 7E 05 25 F6 7A BD A0 2E
*Mar 16 03:28:50.692: 58 83 12 7F 90 CD F4 AB E2 69 53 A8 C7 FC 44 4F
*Mar 16 03:28:50.692: 57 4E 47 52 44 01 00 C0 2B 00 00 13 00 17 00 00
*Mar 16 03:28:50.693: FF 01 00 01 00 00 0B 00 02 01 00 00 23 00 00
*Mar 16 03:28:50.693: TLS server extension "unknown" (id=23), len=0
TLS server extension "renegotiate" (id=65281), len=1
```

```
*Mar 16 03:28:50.693: 00
*Mar 16 03:28:50.693: TLS server extension "EC point formats" (id=11), len=2

*Mar 16 03:28:50.693: 01 00
*Mar 16 03:28:50.693: TLS server extension "session ticket" (id=35), len=0

*Mar 16 03:28:50.693: <<< ??? [length 0005]
*Mar 16 03:28:50.693: 16 03 03 0F 9A
*Mar 16 03:28:50.694:
*Mar 16 03:28:50.702: SSL_connect:SSLv3/TLS read server hello
*Mar 16 03:28:50.702: <<< TLS 1.2 Handshake [length 0F9A], Certificate
*Mar 16 03:28:50.702: 0B 00 0F 96 00 0F 93 00 04 8A 30 82 04 86 30 82
*Mar 16 03:28:50.702: 03 6E A0 03 02 01 02 02 10 52 87 E0 40 A4 FE F7
<snip>
*Mar 16 03:28:50.763: 82 35 CF 62 8B C9 24 8B A5 B7 39 0C BB 7E 2A 41
*Mar 16 03:28:50.763: BF 52 CF FC A2 96 B6 C2 82 3F
*Mar 16 03:28:50.763:
*Mar 16 03:28:50.765: CC_DEBUG: Entering shim layer app callback function
*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Session started - identity not specified
*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Adding peer certificate
*Mar 16 03:28:50.767: CRYPTO_PKI: Added x509 peer certificate - (1162) bytes
*Mar 16 03:28:50.767: CRYPTO_PKI: (A069C) Adding peer certificate
*Mar 16 03:28:50.768: CRYPTO_PKI: Added x509 peer certificate - (1434) bytes
*Mar 16 03:28:50.768: CRYPTO_PKI: (A069C) Adding peer certificate
*Mar 16 03:28:50.770: CRYPTO_PKI: Added x509 peer certificate - (1382) bytes
*Mar 16 03:28:50.770: CRYPTO_OPSSL: Validate Certificate Chain Callback
*Mar 16 03:28:50.770: CRYPTO_PKI(Cert Lookup) issuer="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US" s

*Mar 16 03:28:50.770: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
A7 CC 4B 0F 36 C3 AC D1 2F 77 DD 1D 9A 37 DC FC

*Mar 16 03:28:50.770: CRYPTO_PKI(Cert Lookup) issuer="cn=GTS Root R1,o=Google Trust Services LLC,c=US"

*Mar 16 03:28:50.771: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
03 9F CF 59 82 EE 09 CC 4F 53 AE D8 02 7E 4B AF

*Mar 16 03:28:50.771: CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-

*Mar 16 03:28:50.771: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A

*Mar 16 03:28:50.771: CRYPTO_PKI: Cert record not found for issuer serial.
*Mar 16 03:28:50.772: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
*Mar 16 03:28:50.772: CRYPTO_PKI: Found a subject match
*Mar 16 03:
#28:50.772: CRYPTO_PKI: ip-ext-val: IP extension validation not required:Incrementing refcount for cont
*Mar 16 03:28:50.773: CRYPTO_PKI: create new ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 35
*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C)validation path has 1 certs

*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C) Check for identical certs
*Mar 16 03:28:50.773: CRYPTO_PKI(Cert Lookup) issuer="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-

*Mar 16 03:28:50.774: CRYPTO_PKI: looking for cert in handle=7F41EE523CE0, digest=
94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A

*Mar 16 03:28:50.774: CRYPTO_PKI: Cert record not found for issuer serial.
*Mar 16 03:28:50.774: CRYPTO_PKI : (A069C) Validating non-trusted cert
*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Create a list of suitable trustpoints
*Mar 16 03:28:50.774: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer()
*Mar 16 03:28:50.774: CRYPTO_PKI: Found a issuer match
*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Suitable trustpoints are: CA-GlobalSign-Root,
*Mar 16 03:28:50.775: CRYPTO_PKI: (A069C) Attempting to validate certificate using CA-GlobalSign-Root p
```

```
*Mar 16 03:28:50.775: CRYPTO_PKI: (A069C) Using CA-GlobalSign-Root to validate certificate
*Mar 16 03:28:50.775: CRYPTO_PKI(make trusted certs chain)
*Mar 16 03:28:50.775: CRYPTO_PKI: Added 1 certs to trusted chain.
*Mar 16 03:28:50.775: CRYPTO_PKI: Prepare session revocation service providers
*Mar 16 03:28:50.776: P11:C_CreateObject:
*Mar 16 03:28:50.776: CKA_CLASS: PUBLIC KEY
*Mar 16 03:28:50.776: CKA_KEY_TYPE: RSA
*Mar 16 03:28:50.776: CKA_MODULUS:
DA 0E E6 99 8D CE A3 E3 4F 8A 7E FB F1 8B 83 25
6B EA 48 1F F1 2A B0 B9 95 11 04 BD F0 63 D1 E2
<snip>

*Mar 16 03:28:50.780: CKA_PUBLIC_EXPONENT: 01 00 01
*Mar 16 03:28:50.780: CKA_VERIFY_RECOVER: 01
*Mar 16 03:28:50.780: CRYPTO_PKI: Deleting cached key having key id 45
*Mar 16 03:28:50.781: CRYPTO_PKI: Attempting to insert the peer's public key into cache
*Mar 16 03:28:50.781: CRYPTO_PKI:Peer's public inserted successfully with key id 46
*Mar 16 03:28:50.781: P11:C_CreateObject: 131118
*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 type 3 (invalid mechanism)
*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 type 1
*Mar 16 03:28:50.781: P11:C_VerifyRecoverInit - 131118
*Mar 16 03:28:50.781: P11:C_VerifyRecover - 131118
*Mar 16 03:28:50.781: P11:found pubkey in cache using index = 46
*Mar 16 03:28:50.781: P11:public key found is :
30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01
01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01
<snip>
CF 02 03 01 00 01

*Mar 16 03:28:50.788: P11:CEAL:CRYPTO_NO_ERR
*Mar 16 03:28:50.788: P11:C_DestroyObject 2:2002E
*Mar 16 03:28:50.788: CRYPTO_PKI: Expiring peer's cached key with key id 46
*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificate is verified
*Mar 16 03:28:50.788: CRYPTO_PKI: Remove session revocation service providers
*Mar 16 03:28:50.788: CRYPTO_PKI: Remove session revocation service providersCA-GlobalSign-Root:validat
*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificate validated without revocation check:cert refcount
*Mar 16 03:28:50.790: CRYPTO_PKI: Populate AAA auth data
*Mar 16 03:28:50.790: CRYPTO_PKI: Unable to get configured attribute for primary AAA list authorization
*Mar 16 03:28:50.790: PKI: Cert key-usage: Digital-Signature , Certificate-Signing , CRL-Signing
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C)chain cert was anchored to trustpoint CA-GlobalSign-Root, and
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Removing verify context

*Mar 16 03:28:50.790: CRYPTO_PKI: destroying ca_req_context type PKI_VERIFY_CHAIN_CONTEXT,ident 35, ref
*Mar 16 03:28:50.790: CRYPTO_PKI: ca_req_context released
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Validation TP is CA-GlobalSign-Root
*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Certificate validation succeeded
*Mar 16 03:28:50.790: CRYPTO_OPSSL: Certificate verification is successful
*Mar 16 03:28:50.790: CRYPTO_PKI: Rcvd request to end PKI session A069C.
*Mar 16 03:28:50.790: CRYPTO_PKI: PKI session A069C has ended. Freeing all resources.:cert refcount aft
*Mar 16 03:28:50.791: <<< ??? [length 0005]
*Mar 16 03:28:50.791: 16 03 03 00 93
*Mar 16 03:28:50.791:
*Mar 16 03:28:50.791: SSL_connect:SSLv3/TLS read server certificate
*Mar 16 03:28:50.791: <<< TLS 1.2 Handshake [length 0093], ServerKeyExchange
*Mar 16 03:28:50.791: 0C 00 00 8F 03 00 17 41 04 3D 49 34 A3 52 D4 EB
*Mar 16 03:28:50.791: DE A2 9E CC B0 91 AA CB 1B 39 D0 26 1B 7D FF 31
*Mar 16 03:28:50.792: E0 D7 D5 9C 75 C0 7D 5B D6 B2 0A B5 CC EA E1 4B
*Mar 16 03:28:50.792: 4E E5 72 7B 54 5D 9B B2 95 91 E0 CC D6 A5 8E CE
*Mar 16 03:28:50.792: 8D 36 C9 83 42 B0 4D AC 0C 04 03 00 46 30 44 02
*Mar 16 03:28:50.792: 20 67 B3 F1 DA D1 BF 13 72 DD B6 B2 11 3B 6E 6F
*Mar 16 03:28:50.793: 87 52 D9 00 F7 44 31 C3 C2 5E BE 2D FF 93 4E F0
*Mar 16 03:28:50.793: A8 02 20 24 42 91 BE B7 10 1C D1 C0 12 28 FB 1F
```

```
*Mar 16 03:28:50.793: E4 DE 81 0B AA 66 19 CD 28 5A A0 30 7D 3C 4A 56
*Mar 16 03:28:50.793: 0D 94 E2
*Mar 16 03:28:50.793:
*Mar 16 03:28:50.794: P11:C_FindObjectsInit:
*Mar 16 03:28:50.794: CKA_CLASS: PUBLIC KEY
*Mar 16 03:28:50.794: CKA_KEY_TYPE: : 00 00 00 03

*Mar 16 03:28:50.794: CKA_ECDSA_PARAMS:
30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A
86 48 CE 3D 03 01 07 03 42 00 04 63 B6 D3 1A 28
<snip>

*Mar 16 03:28:50.796: P11:C_FindObjectsFinal
*Mar 16 03:28:50.796: P11:C_VerifyInit - Session found
*Mar 16 03:28:50.796: P11:C_VerifyInit - key id = 131073
*Mar 16 03:28:50.796: P11:C_Verify
*Mar 16 03:28:50.800: P11:CEAL:CRYPTO_NO_ERR
*Mar 16 03:28:50.800: <<< ??? [length 0005]
*Mar 16 03:28:50.800: 16 03 03 00 04
*Mar 16 03:28:50.800:
*Mar 16 03:28:50.800: SSL_connect:SSLv3/TLS read server key exchange
*Mar 16 03:28:50.800: <<< TLS 1.2 Handshake [length 0004], ServerHelloDone
*Mar 16 03:28:50.801: 0E 00 00 00
*Mar 16 03:28:50.801:
*Mar 16 03:28:50.801: SSL_connect:SSLv3/TLS read server done
*Mar 16 03:28:50.810: >>> ??? [length 0005]
*Mar 16 03:28:50.810: 16 03 03 00 46
*Mar 16 03:28:50.811:
*Mar 16 03:28:50.811: >>> TLS 1.2 Handshake [length 0046], ClientKeyExchange
*Mar 16 03:28:50.811: 10 00 00 42 41 04 26 C3 EF 02 05 6C 82 D1 90 B3
*Mar 16 03:28:50.811: 17 31 9A CD DD 8C 81 91 BA E8 C0 86 40 7B 2C E4
*Mar 16 03:28:50.811: 9A 2C 18 9D D1 6A C0 56 A0 98 2E B7 3B AB B3 EB
*Mar 16 03:28:50.811: BB CD 5E 42 C5 76 C0 C4 BF 15 F4 87 F2 7C AD 74
*Mar 16 03:28:50.812: 97 0A 97 2B 06 B5
*Mar 16 03:28:50.812:
*Mar 16 03:28:50.812: SSL_connect:SSLv3/TLS write client key exchange
*Mar 16 03:28:50.812: >>> ??? [length 0005]
*Mar 16 03:28:50.812: 14 03 03 00 01
*Mar 16 03:28:50.812:
*Mar 16 03:28:50.812: >>> TLS 1.2 ChangeCipherSpec [length 0001]
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 35
*Mar 16 03:28:51.116:
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 1A
*Mar 16 03:28:51.116:
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 30
*Mar 16 03:28:51.116:
*Mar 16 03:28:51.116: >>> ??? [length 0005]
*Mar 16 03:28:51.116: 17 03 03 00 1B
*Mar 16 03:28:51.117:
*Mar 16 03:28:51.713: <<< ??? [length 0005]
*Mar 16 03:28:51.713: 17 03 03 00 6D
*Mar 16 03:28:51.713:
*Mar 16 03:28:51.714: >>> ??? [length 0005]
*Mar 16 03:28:51.714: 17 03 03 00 1E
*Mar 16 03:28:51.714:
*Mar 16 03:28:51.732: <<< ??? [length 0005]
*Mar 16 03:28:51.732: 17 03 03 00 71
*Mar 16 03:28:51.732:
```

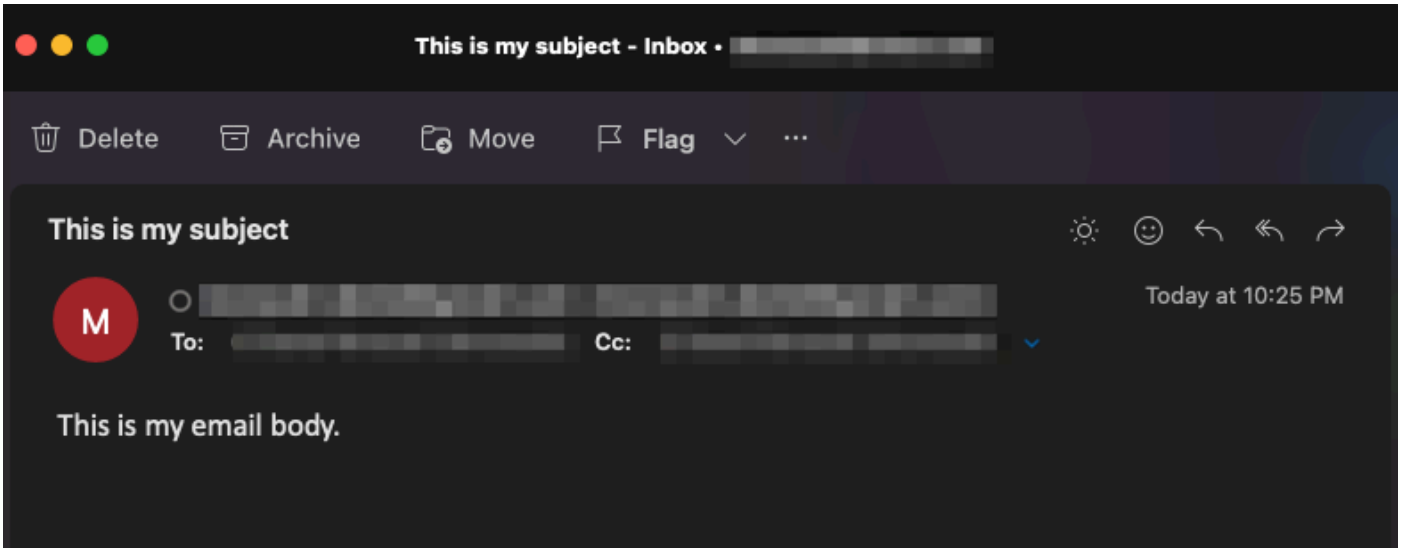
execução do gerenciador de eventos SendSecureEmailEEM*Mar 16 03:28:50.673: CRYPTO_OPSSL: Alocou a memória para OPSSLContext*Mar 16 03:28:50.673: CRYPTO_OPSSL: Defina as especificações de cifra para a máscara 0x02FC0000 para a versão 128*Mar 16 03:28:50.674: Defina Lista de curvas EC: 0x70Defina a lista de curvas EC: secp521r1:secp384r1:prime256v1*Mar 16 03:28:50.674: opssl_SetPKIInfo entry*Mar 16 03:28:50.674: CRYPTO_PKI: (A069B) Sessão iniciada - identidade selecionada (TP-self-signed-486541296)xTP-self-signed-486541296:refcount após o incremento = 1*Mar 16 03:28:50.674: CRYPTO_PKI: Iniciar recuperação da cadeia de certificados local.*Mar 16 03:28:50.674: CRYPTO_PKI(Pesquisa de Certificados) issuers="cn=IOS-Self-Signed-Certificate-486541296" número de série= 01*Mar 16 03:28:50.674: CRYPTO_PKI: procurando certificado no identificador=7F41EE523CE0, digest=1C 7F 3D 52 67 66 D5 59 E2 66 58 E7 8B E7 9B 8E*Mar 16 03:28:50.675: CRYPTO_PKI: Concluído com busca de cadeia de certificado local 0.*Mar 16 03:28:50.675: CRYPTO_PKI YPTO_PKI: Solicitação de recebimento para encerrar a sessão PKI A069B.*Mar 16 03:28:50.675: CRYPTO_PKI: A sessão PKI A069B foi encerrada. Liberando todos os recursos.TP-self-signed-486541296:trustpoint desbloqueado TP-self-signed-486541296, refcount is 0*Mar 16 03:28:50.675: opssl_SetPKIInfo done.*Mar 16 03:28:50.675: CRYPTO_OPSSL: Critérios comuns desabilitados nesta sessão.Desabilitando a funcionalidade do modo Critérios comuns no CiscoSSL em SSL CTX 0x7F41F28EAFF8 Mar 16 03:28:50.675: CRYPTO_OPSSL: conjuntos de cifras ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-DHGCM-SHA384:256E-RSA-AES256-SHA256:AES256-GCM-SHA384:AES256-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:AES128-GCM-SHA256:AES128-SHA256*Mar 16 03:28:50.676: Início do handshake: antes da inicialização SSL*Mar 16 03:28:50.67 6: SSL_connect:antes da inicialização de SSL*16 de março 03:28:50.676: >>> ??? [comprimento 0005]*Mar 16 03:28:50.676: 16 03 01 00 95*Mar 16 03:28:50.676: *Mar 16 03:28:50.676: >>> Handshake TLS 1.2 [comprimento 0095], ClienteHello*Mar 16 03:28:50.676: 01 00 00 91 03 03 26 4B 9F B3 44 94 FD 5F FD A1<snip>*Mar 16 03:28:50.679: 03 03 01 02 01*Mar 16 03:28:50.679: *Mar 16 03:28:50.679: SSL_connect:SSLv3/SSL LS write client hello*Mar 16 03:28:50.692: <<< ??? [length 0005]*Mar 16 03:28:50.692: 16 03 03 00 3F*Mar 16 03:28:50.692: *Mar 16 03:28:50.692: SSL_connect:SSLv3/TLS write client hello*Mar 16 03:28:50.692: <<< TLS 1.2 Handshake [comprimento 003F], ServidorHello*Mar 16 03:28:50.692: 02 00 00 3B 03 03 64 12 7E 05 25 F6 7A BD A0 2E*Mar 16 03:28:50.692: 58 83 12 7F 90 CD F4 AB E2 69 53 A8 C7 FC 44 4F*16 03:28:50.692: 57 4E 47 52 44 01 00 C0 2B 00 00 13 00 17 00 00*Mar 16 03:28:50.693: FF 01 00 01 00 00 0B 00 02 01 00 00 23 00 00*Mar 16 03:28:50.693: Extensão de servidor TLS "desconhecida" (id=23), len=0Extensão de servidor TLS "renegociar" (id=65281), len=1*Mar 16 03:28:50.693: 00*Mar 16 03:28:50.693: Extensão de servidor TLS "formatos de ponto EC" (id=11), len=2*Mar 16 03:28:50.693: 01 00*Mar 16 03:28:50.693: "tíquete de sessão" da extensão do servidor TLS (id=35), len=0*Mar 16 03:28:50.693: <<< ??? [length 0005]*Mar 16 03:28:50.693: 16 03 03 0F 9A*Mar 16 03:28:50.694: *Mar 16 03:28:50.702: SSL_connect:SSLv3/TLS read server hello*Mar 16 03:28:50.702: <<< TLS 1.2 Handshake comprimento 0F9A], Certificado*Mar 16 03:28:50.702: 0B 00 0F 96 00 0F 93 00 04 8A 30 82 04 86 30 82*Mar 16 03:28:50.702: 03 6E A0 03 02 01 02 02 10 52 87 E0 40 A4 FE7 F snip>*Mar 16 03:28:50.763: 82 35 CF 62 8B C9 24 8B A5 B7 39 0C BB 7E 2A 41*Mar 16 03:28:50.763: BF 52 CF A2 96 B6 C2 82 3F*Mar 16 03:28:50.763: *Mar 16 03:2 8:50.765: CC_DEBUG: Inserindo função de retorno de chamada do aplicativo da camada de shim*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Sessão iniciada - identidade não especificada*Mar 16 03:28:50.765: CRYPTO_PKI: (A069C) Adicionando

certificado de peer*Mar 16 03:28:50.7 67: CRYPTO_PKI: Certificado par x509 adicionado - (1162) bytes*Mar 16 03:28:50.767: CRYPTO_PKI: (A069C) Adicionando certificado par*Mar 16 03:28:50.768: CRYPTO_PKI: Certificado par x509 adicionado - (1434) bytes*Mar 16 0 3:28:50.768: CRYPTO_PKI: (A069C) Adicionando certificado de mesmo nível*Mar 16 03:28:50.770: CRYPTO_PKI: Certificado de mesmo nível x509 adicionado - (1382) bytes*Mar 16 03:28:50.770: CRYPTO_OPSSL: Validar Retorno de Chamada da Cadeia de Certificados*Mar 16 03:2 8:50.770: CRYPTO_PKI(Cert Lookup) issuer="cn=GTS CA 1C3,o=Google Trust Services LLC,c=US" número de série= 52 87 E0 40 A4 FE F7 07 12 68 B0 4F DD F0 F4*Mar 16 03:28:50.770: CRYPTO_PKI: procurando certificado no identificador=7F41EE52 3CE0, digest=A7 CC 4B 0F 36 C3 AC D1 2F 77 DD 1D 9A 37 DC FC*Mar 16 03:28:50.770: CRYPTO_PKI(Cert Lookup) issuiser="cn=GTS Root R1,o=Google Trust Services LLC,c=US" número de série= 02 03 BC 53 59 6B 34 C7 18 F5 01 50 66*1 6 03:28:50.771: CRYPTO_PKI: procurando cert no identificador=7F41EE523CE0, digest=03 9F CF 59 82 EE 09 CC 4F 53 AE D8 02 7E 4B AF*Mar 16 03:28:50.771: CRYPTO_PKI(Pesquisa de Cert) issuer="cn=GlobalSign Root CA,ou=ot CA,o=GlobalSign nv-sa,c=BE" número de série= 77 BD 0D 6C DB 36 F9 1A EA 21 0F C4 F0 58 D3 0D*Mar 16 03:28:50.771: CRYPTO_PKI: procurando certificado no identificador=7F41EE523CE0, digest=94 40 D1 90 A0 A3 5D 47 E5 B5 31 F 63 AD 1B 0A*Mar 16 03:28:50.771: CRYPTO_PKI: Registro de certificado não encontrado para série de emissor.*Mar 16 03:28:50.772: CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()*Mar 16 03:28:50.772: CRYPTO_PKI: Correspondência de assunto encontrada*1 6 03:#28:50.772: CRYPTO_PKI: ip-ext-val: validação de extensão IP não necessária:Incrementando refcount para id-35 de contexto para 1*Mar 16 03:28:50.773: CRYPTO_PKI: criar novo ca_req_context tipo PKI_VERIFY_CHAIN_CONTEXT,ident 35*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C)o caminho de validação tem 1 certs*Mar 16 03:28:50.773: CRYPTO_PKI: (A069C) Verificar certs idênticos*Mar 16 03:28:50.773: CRYPTO_PKI(Pesquisa de Cert) issuler="cn=GlobalSign Root CA,ou=Root CA,o=GlobalSign nv-sa,c=BE" número serial= 77 BD 0D 6C DB 36 F9 1A EA 21 0F C4 F0 58 D3 0D*Mar 16 03:28:50.774: CRYPTO_PKI: procurando certificado no identificador=7F41EE523CE0, digest=94 40 D1 90 A0 A3 5D 47 E5 B5 31 F6 63 AD 1B 0A*16 Mar 03:2 8:50.774: CRYPTO_PKI: Registro de certificado não encontrado para série do emissor.*Mar 16 03:28:50.774: CRYPTO_PKI : (A069C) Validando certificado não confiável*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Criar uma lista de pontos de confiança adequados*Mar 16 03:2 8:50.774: CRYPTO_PKI: crypto_pki_get_cert_record_by_issuer()*Mar 16 03:28:50.774: CRYPTO_PKI: Correspondência de emissor encontrada*Mar 16 03:28:50.774: CRYPTO_PKI: (A069C) Os pontos de confiança adequados são: CA-GlobalSign-Root, Mar*16 3:28:50.775: CRYPTO_PKI: (A069C) Tentando validar o certificado usando CA-GlobalSign-Root policy*Mar 16 03:28:50.775: CRYPTO_PKI: (A069C) Usando CA-GlobalSign-Root para validar o certificado*Mar 16 03:28:50.775: CRYPTO_PKI(A069C) criar cadeia de certificados confiáveis)*Mar 16 03:28:50.775: CRYPTO_PKI: Adicionado 1 certificado à cadeia confiável.*Mar 16 03:28:50.775: CRYPTO_PKI: Preparar provedores de serviços de revogação de sessão*Mar 16 03:28:50.776: P11:C_CreateObject:*Mar 16 03:28:50.77 6: CKA_CLASS: PUBLIC KEY*Mar 16 03:28:50.776: CKA_KEY_TYPE: RSA*Mar 16 03:28:50.776: CKA_MODULUS: DA 0E6 99 8D CE A3 E3 4F 8A 7E FB F1 8B 83 25 6B EA 48 1F1 2A B0 B9 95 11 04 BD F0 3 D1 E2 <snip>*Mar 16 03:28:50.780: CKA_PUBLIC_EXPONENT: 01 00 01*Mar 16 03:28:50.780: CKA_VERIFY_RECOVER: 01*Mar 16 03:28:50.780: CRYPTO_PKI: Excluindo chave em cache com id de chave 45*Mar 16 3:28:50.781: CRYPTO_PKI: Tentando inserir a chave pública do par no cache*Mar 16 03:28:50.781: CRYPTO_PKI:Público do par inserido com êxito com a ID da chave 46*Mar 16 03:28:50.781: P11:C_CreateObject: 131118*Mar 16 03:28:50.78 1:

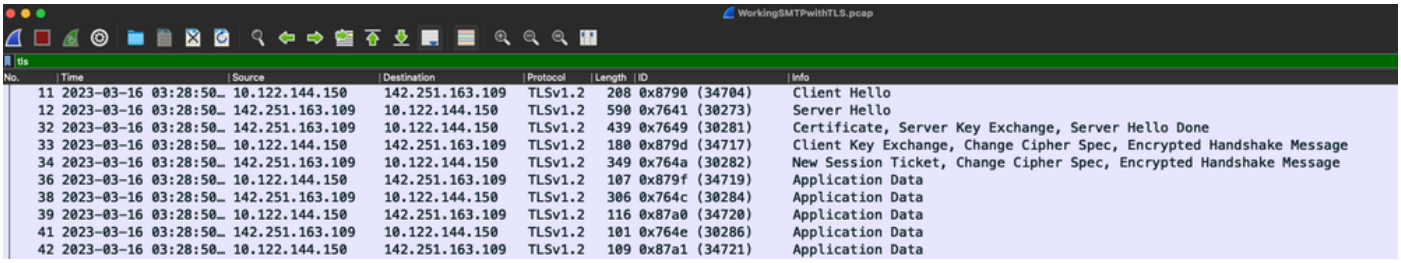
P11:C_GetMechanismInfo slot 1 tipo 3 (mecanismo inválido)*Mar 16 03:28:50.781: P11:C_GetMechanismInfo slot 1 tipo 1*Mar 16 03:28:50.781: P11:C_VerifyRecoverInit - 131118*Mar 16 03:28:50.781: P11:C_VerifyInit - 131118*Mar 16 03:28:50.781: P11:pubkey encontrado em cache usando índice = 46*Mar 16 03:28:50.781: P11:public key encontrado é : 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 <snip>CF 02 03 01 00 01*Mar 16 03:28:50.788: P11:CEAL:CRYPTO_NO_ERR*Mar 16 03:28:50.788: P11:C_DestroyObject 2:2002E*Mar 16 03:28:50.788: CRYPTO_PKI: Chave armazenada em cache de peer expirando com id de chave 46*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificado verificado*Mar 16 03:28:50.788: CRYPTO_PKI: Remover provedores de serviços de revogação de sessão*Mar 16 03:28:50.7 88: CRYPTO_PKI: Remover provedores de serviços de revogação de sessãoCA-GlobalSign-Root:status de validação - CRYPTO_VALID_CERT_WITH_WARNING*Mar 16 03:28:50.788: CRYPTO_PKI: (A069C) Certificado validado sem verificação de revogação:certificado refcount após incremento = 1*Mar 16 03:28:50.790: CRYPTO_PKI: Preencher dados de autenticação AAA*Mar 16 03:28:50.790: CRYPTO_PKI: Não é possível obter atributo configurado para autorização de lista AAA primária.*Mar 16 03:28:50.790: PKI: Uso da chave de certificado: Assinatura Digital, Assinatura de Certificado, Assinatura de CRL*Mar 16 03:28:50.790: CRYPTO_PKI: (A060 C) o certificado da cadeia foi ancorado no ponto confiável CA-GlobalSign-Root, e o resultado da validação da cadeia foi: CRYPTO_VALID_CERT_WITH_WARNING*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Removendo contexto de verificação*Mar 16 03:28:50.790: CRYPTO_PKI: destruindo ca_req_context type PKI_VERIFY CHAIN_CONTEXT,ident 35, ref count 1:Decrementing refcount para context id-35 para 0*Mar 16 03:28:50.790: CRYPTO_PKI: ca_req_context release*Mar 16 03:28:50.790: CRYPTO_PKI: (A069C) Validation TP is CA-GlobalSign-Root*Mar 16 03:28:5 0,790: CRYPTO_PKI: (A069C) Validação de certificado bem-sucedida*Mar 16 03:28:50.790: CRYPTO_OPSSL: Verificação de certificado bem-sucedida*Mar 16 03:28:50.790: CRYPTO_PKI: Solicitação de recebimento para encerrar a sessão PKI A069C.*Mar 16 03:28:50.790: CRYPTO_PKI: A sessão PKI A069C terminou. Liberação de todos os recursos.:refcount de certificado após decremento = 0*Mar 16 03:28:50.791: <<< ??? [length 0005]*Mar 16 03:28:50.791: 16 03 03 00 93*Mar 16 03:28:50.791: *Mar 16 03:28:50.791: SSL_connect:SSLv3/TLS read server certificate*Mar 16 03:28:50.791: << TLS 1.2 shake [length 0093], ServerKeyExchange*Mar 16 03:28:50.791: 0C 00 00 8F 03 00 17 41 04 3D 49 34 A3 52 D4 EB*Mar 16 03:28:50.791: DE A2 9E CC B0 91 AA CB 1B 39 D0 26 1B 7D FF 31 Mar*1 03:28:50.792: E0 D7 D5 9C 75 C0 7D 5B D6 B2 0A B5 CC EA E1 4B*Mar 16 03:28:50.792: 4E E5 72 7B 54 5D 9B2 95 91 E0 CC D6 A5 8E CE*Mar 16 03:28:50.792: 8D 36 C9 83 2 B0 4D AC 0C 04 03 00 46 30 44 02*Mar 16 03:28:50.792: 20 67 B3 F1 DA D1 BF 13 72 DD B6 B2 11 3B 6E 6F*Mar 16 03:28:50.793: 87 52 D9 00 F7 44 31 C3 FF2 5E BE 2D 93 4E F0*Mar 16 03:28:50.793: A8 02 20 24 42 91 BE B7 10 1C D1 C0 12 28 FB 1F*Mar 16 03:28:50.793: E4 DE 81 0B AA 66 19 CD 28 5A0 30 7D 3C 4A 56*Mar 03:28 50.793: 0D 94 E2*Mar 16 03:28:50.793: *Mar 16 03:28:50.794: P11:C_FindObjectsInit:*Mar 16 03:28:50.794: CKA_CLASS: CHAVE PÚBLICA*Mar 16 03:28:50.794: CKA_CLASS EY_TYPE: : 00 00 00 03*Mar 16 03:28:50.794: CKA_ECDSA_PARAMS: 30 59 30 13 06 07 2A 86 48 CE 3D 02 01 06 08 2A 86 48 CE 3D 03 01 07 03 42 00 04 63 B6 D3 1A 28 p>*Mar 16 03:28:50.796: P11:C_FindObjectsFinal*Mar 16 03:28:50.796: P11:C_VerifyInit - Sessão encontrada*Mar 16 03:28:50.796: P11:C_VerifyInit - id da chave = 131073*Mar 16 03:28:50.79 6: P11:C_Verify*Mar 16 03:28:50.800: P11:CEAL:CRYPTO_NO_ERR*Mar 16 03:28:50.800: <<< ??? [comprimento 0005]*Mar 16 03:28:50.800: 16 03 03 00 04*Mar 16 03:28:50.800: *Mar 16 03:28:50.800: SSL_connect:SSLv3/TLS read server key exchange*Mar 16 03:28:50.800: <<< TLS 1.2

Handshake [length 0004], ServerHelloDone*Mar 16 03:28:50.801: 0E 00 00 00*Mar 16 03:28:50.801: *Mar 16 03:28:50.801: SSL_connect:SSLv3/TLS read server done*Mar 16 03:28:50.810: >>> ??? [comprimento 0005]*Mar 16 03:28:50.810: 16 03 03 00 46*Mar 16 03:28:50.811: *Mar 16 03:28:50.811: >>> Handshake TLS 1.2 [comprimento 0046], ClientKeyExchange*Mar 16 03:28:50.81 1: 10 00 00 42 41 04 26 C3 EF 02 05 6C 82 D1 90 B3*Mar 16 03:28:50.811: 17 31 9A CD DD 8C 81 91 BA E8 C0 86 40 7B 2C E4*Mar 16 03:28:50.811: 9A 2C 18 9D1 6A 56 A0 98 2E B7 3B AB B3 EB*Mar 16 03:28:50.811: BB CD 5E 42 C5 76 C0 C4 BF 15 F4 87 F2 7C AD 74*Mar 16 03:28:50.812: 97 0A 97 2B 06 B5*Mar 16 03:28:50.812: *1 6 03:28:50.812: SSL_connect:SSLv3/TLS write client key exchange*Mar 16 03:28:50.812: >>> ??? [comprimento 0005]*Mar 16 03:28:50.812: 14 03 03 00 01*Mar 16 03:28:50.812: *Mar 16 03:28:50.812: >>> TLS 1.2 ChangeCipherSpec [comprimento 0001]*Mar 16 03:28:51.11 6: >>> ??? [comprimento 0005]*Mar 16 03:28:51.116: 17 03 03 00 35*Mar 16 03:28:51.116: *Mar 16 03:28:51.116: >>> ??? [comprimento 0005]*Mar 16 03:28:51.116: 17 03 03 00 1A*Mar 16 03:28:51.116: *Mar 16 03:28:51.116: >>> ??? [comprimento 0005]*Mar 16 03:28:51.116: 17 03 03 00 30*Mar 16 03:28:51.116: *Mar 16 03:28:51.116: >>> ??? [comprimento 0005]*Mar 16 03:28:51.116: 17 03 03 00 1B*Mar 16 03:28:51.117: *Mar 16 03:28:51.713: <<< ??? [comprimento 0005]*Mar 16 03:28:51.713: 17 03 03 00 6D*Mar 16 03:28:51.713: *Mar 16 03:28:51.714: >>> ??? [comprimento 0005]*Mar 16 03:28:51.714: 17 03 03 00 1E*Mar 16 03:28:51.714: *Mar 16 03:28:51.732: <<< ??? [comprimento 0005]*Mar 16 03:28:51.732: 17 03 03 00 71*Mar 16 03:28:51.732:

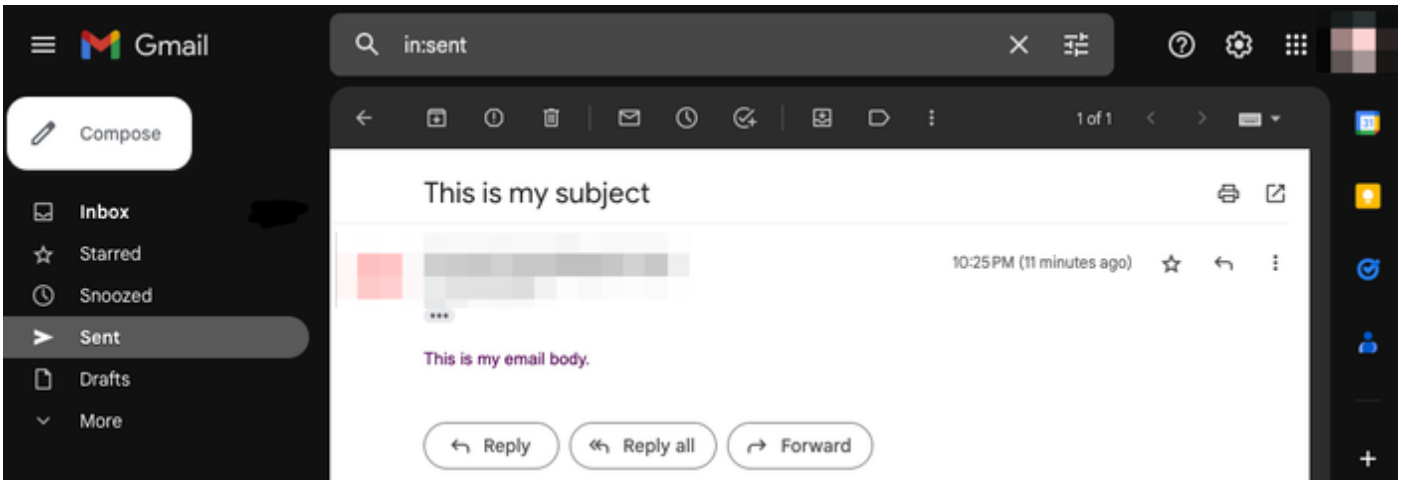
Você pode verificar se o e-mail foi recebido e se todos os campos (para, de, cc, assunto, corpo) estão preenchidos corretamente:



Você também pode verificar se o handshake TLS e a sessão ocorreram a partir da captura de pacotes no dispositivo Cisco IOS XE (anexado como "WorkingSMTPwithTLS.pcap"):



Você pode até mesmo verificar se os e-mails estão refletidos na pasta "Enviados" da conta de e-mail usada:



Outras advertências e considerações

Nomes de usuário com símbolos @

Podem ser observados problemas ao tentar utilizar um relé SMTP. Devido à retransmissão SMTP, a string do servidor tem este formato (um "@" no nome de usuário):

```
event manager environment _email_server email.relay@My.Domain.Name:MyPasswordString@smtp-relay.gmail.co
```

O código para analisar o nome de usuário e a senha divide a sequência de caracteres na primeira ocorrência do símbolo "@". Como resultado, o sistema pensa que o nome de host do servidor começa imediatamente após o primeiro símbolo "@" pelo resto da sequência de caracteres e interpreta tudo o que antes disso como o "nome de usuário:senha".

A implementação TCL do SMTP usa uma expressão regular (regex) que manipula essas informações de nome de usuário/senha/servidor de forma diferente. Devido a essa diferença, o TCL permite nomes de usuário com um símbolo "@"; no entanto, o TCL do Cisco IOS XE não suporta criptografia, portanto, não há opção para enviar e-mails seguros por TLS.

Para resumir:

- Se o e-mail precisar ser seguro, você não poderá enviá-lo com TCL.
- Se houver um "@" em seu nome de usuário, você não poderá enviá-lo com um EEM.

O bug da Cisco ID CSCwe75439 foi preenchido para tratar dessa oportunidade de melhorar o recurso de e-mail do EEM; no entanto, não há um roteiro para essa solicitação de aprimoramento atualmente.

Conclusão

Como mostrado aqui, é possível enviar e-mails seguros via SMTP com TLS usando o miniaplicativo Embedded Event Manager (EEM). Ele requer alguma configuração no lado do servidor, bem como a configuração dos certificados necessários para permitir a confiança, mas é viável se você quiser gerar notificações de e-mail automatizadas e seguras.

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.