Navegar no cliente EKU Sunset com Expressway x15.5

Introdução

Este documento descreve a navegação no cliente EKU sunset com o Cisco Expressway x15.5.

Informações de Apoio

Os certificados digitais são credenciais eletrônicas emitidas por Autoridades de Certificação (CAs) confiáveis que protegem a comunicação entre servidores e clientes, garantindo a autenticação, a integridade dos dados e a confidencialidade. Estes certificados contêm campos de Uso Estendido de Chave (EKU) que definem sua finalidade:

- EKU de Autenticação do Servidor (id-kp-serverAuth é usado quando um servidor apresenta seu certificado para comprovar a identidade.
- O EKU de autenticação do cliente (id-kp-clientAuth) é usado em conexões TLS mútuas (mTLS) onde ambas as partes se autenticam.

Tradicionalmente, um único certificado pode conter EKUs de Autenticação de Servidor e de Cliente, permitindo que ele sirva a duas finalidades. Isso é particularmente importante para produtos como o Cisco Expressway que atuam como servidor e cliente em diferentes cenários de conexão.

Definição do problema

Mudança de política do programa Chrome Root

A partir de junho de 2026, a Política do programa raiz do Chrome restringe os certificados de Autoridade de certificação raiz (CA) incluídos no Chrome Root Store, eliminando gradualmente as raízes multiuso para alinhar todas as hierarquias de infraestrutura de chave pública (PKI) para servir apenas casos de uso de autenticação de servidor TLS.

Principais requisitos da política

- As CAs de raiz públicas devem declarar Uso Estendido de Chave (EKU) SOMENTE para Autenticação de Servidor (id-kp-serverAuth).
- É proibido incluir EKU de Autenticação de Cliente nesses certificados.
- Não há mais CAs raiz de uso misto para certificados TLS de servidor público.
- Cronograma de aplicação: Junho de 2026

Cronograma de Resposta de CA Pública

- outubro de 2025: Muitas CAs públicas (DigiCert, Sectigo, SSL) começaram a emitir certificados somente de servidor por padrão.
- Maio de 2026: Os servidores públicos de CA param de emitir certificações EKU de Autenticação de Cliente
- Junho de 2026: A política do programa Chrome Root torna-se totalmente eficaz

---

Note: Esta política se aplica somente a certificados emitidos por autoridades de certificação públicas. PKI particular e certificados autoassinados não são afetados por esta política.

Se você estiver interessado em ler sobre o impacto do desligamento do EKU do cliente no Expressways, consulte Preparar o Expressway para o Desligamento do EKU de Autenticação do Cliente em Certificados CA Públicos.

Expressway versão x15.5 com solução

Expressway x15.5

O Expressway x15.5 vem com uma correção proposta para um problema que surge devido ao desligamento do EKU do cliente por todas as autoridades de certificação públicas. Esse é um problema global e afeta todos os fornecedores/implantações que optam por usar certificados PKI públicos.

x15.4, uma versão anterior, tinha um switch de comando CLI que permitia que o administrador carregasse o certificado somente EKU de servidor (nenhum EKU de cliente presente) no Expressway E.

EnableServerEkuUpload de CVS de certificado TLS XCP xConfiguration: Ligado

---

Note: Este comando foi preterido em x15.5.

Adição de Repositório de Certificados X15.5

O x15.5 tem dois armazenamentos de certificados:

1. Repositório de certificados do servidor

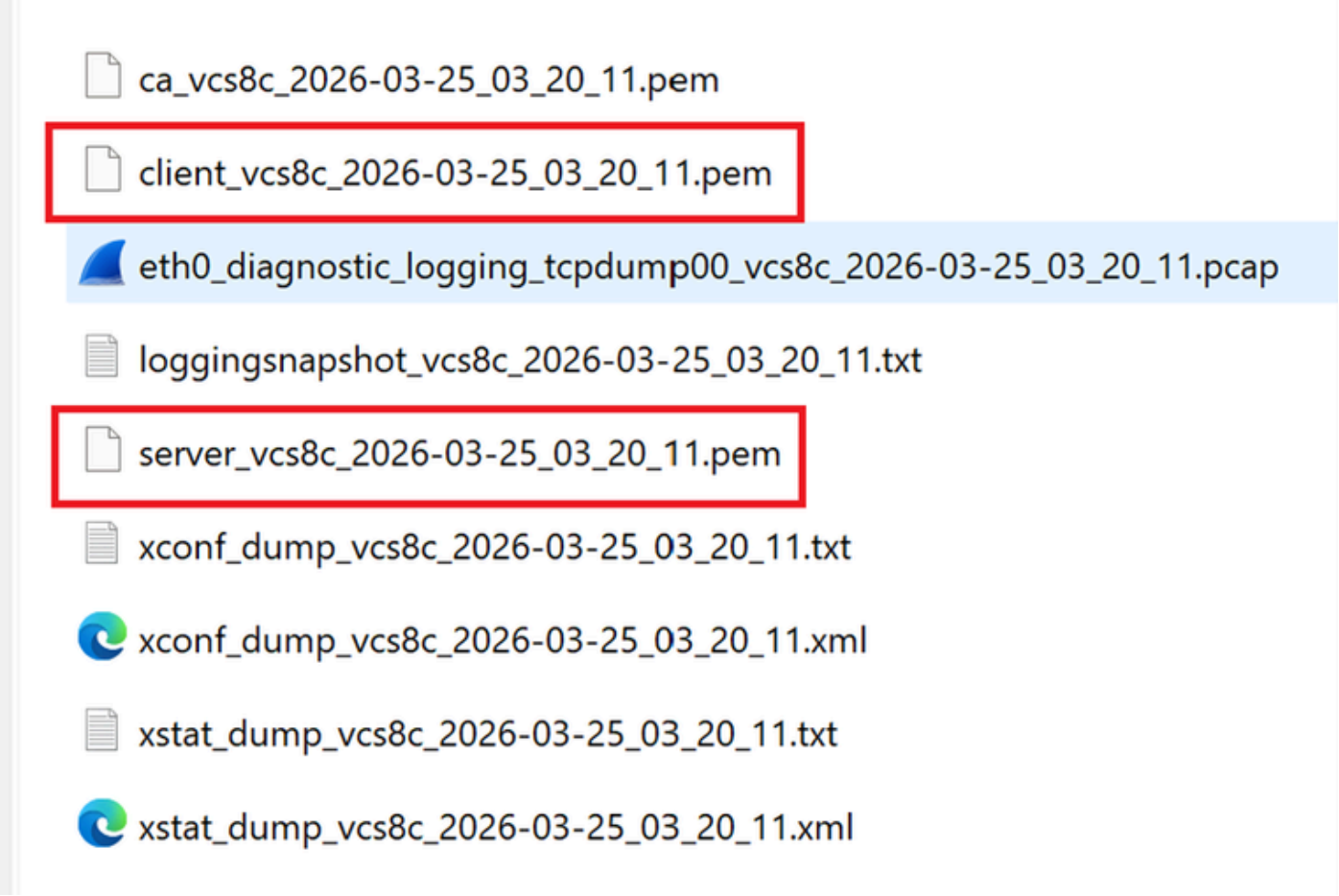
2. Repositório de certificados do cliente

Expressways (Nic única ou Nic dupla): Ambas as interfaces Expressway podem usar 2 armazenamentos de certificados conforme necessário.

Exemplo:

- Quando o expressway atua como um cliente durante o handshake TLS, o certificado do cliente é apresentado.
- Quando o expressway atua como servidor durante o handshake TLS, o certificado do servidor é apresentado.

Note: Ambos os armazenamentos de certificados (Cliente e Servidor) usam a mesma biblioteca de CAs confiáveis. Verifique se a autoridade de certificação que assinou os certificados de servidor e cliente está carregada corretamente no repositório Confiável. Os logs de diagnóstico agora incluem o certificado do servidor e o certificado do cliente no formato de arquivo PEM.



Atualização de X15.4 ou versão anterior para X15.5

Quando uma atualização é executada, o certificado do servidor de x15.4 ou versão anterior, o armazenamento de certificados do servidor Expressway é copiado para o armazenamento de certificados do cliente em x15.5. Os armazenamentos de certificados do cliente e do servidor em x15.5 têm o mesmo certificado.

Exemplo com capturas de tela

Servidor Expressway na versão 15.4, Número de Série do certificado do servidor atual 46:df:76:aa:00:00:00:00:00:29

Certificado:

Versão: 3 (0x2)

Número de série:

46:df:76:aa:00:00:00:00:00:29

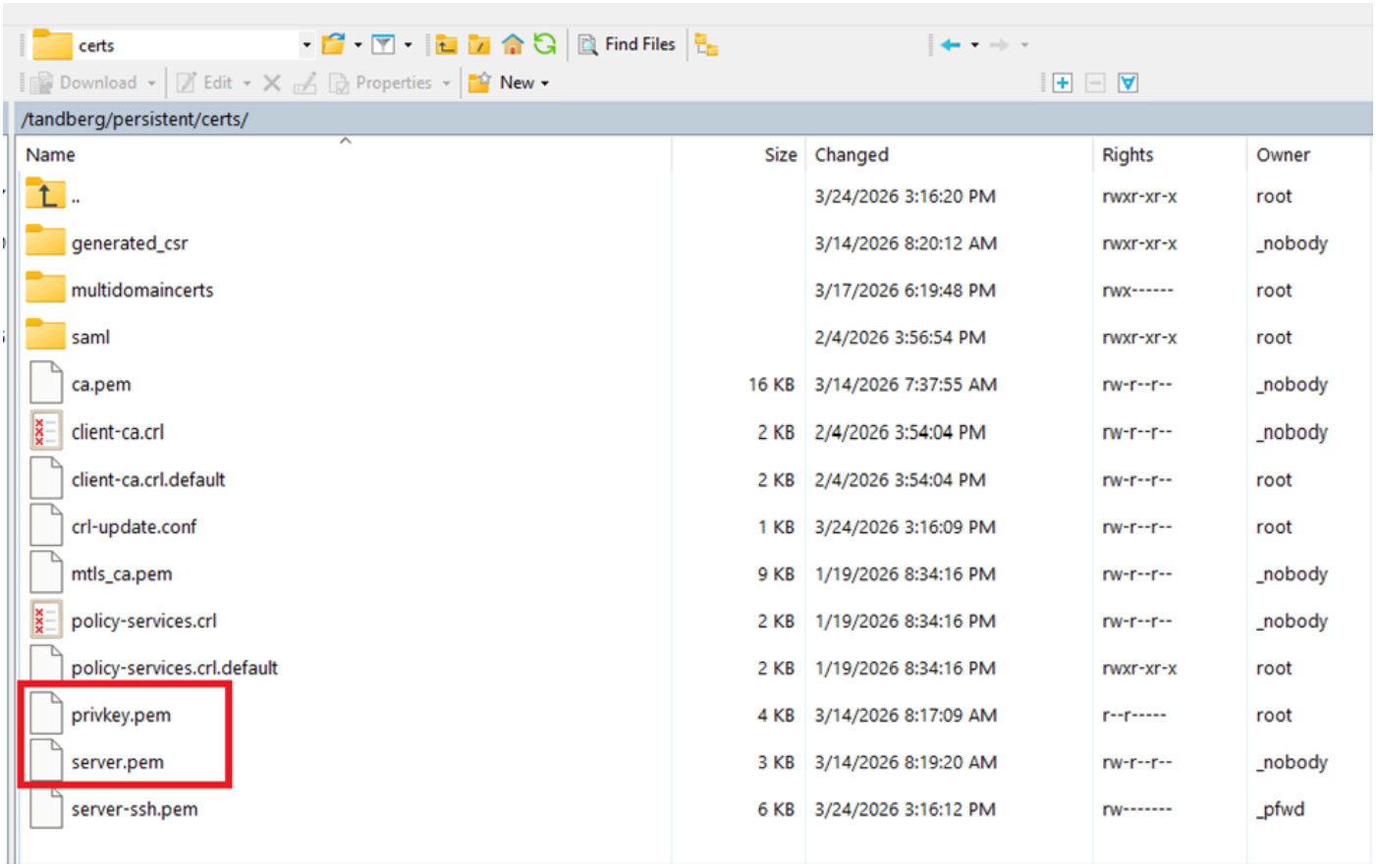
Validade

Não Antes: Mar 14 02:37:40 2026 GMT

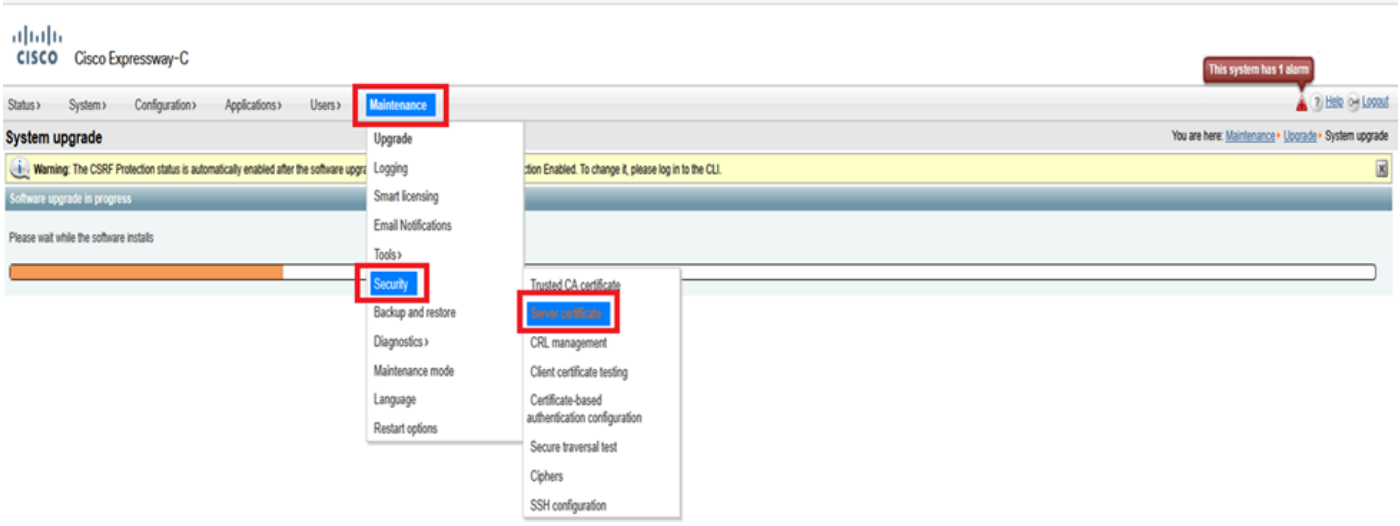
Não depois de: Mar 14 02:47:40 2028 GMT

Assunto: C = IN, ST = KA, L = KA, O = Cisco, OU = TAc, CN = cluster.s.com

Diretório persistente/certificado do sistema de arquivos Expressway em x15.4:

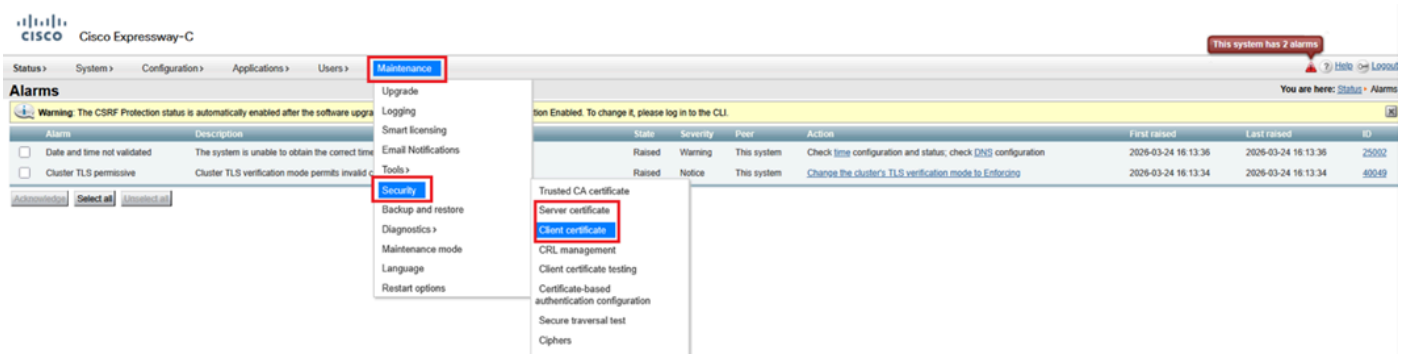


Menu Expressway (Manutenção > Segurança > Certificado do servidor) em x15.4 (apenas campo de certificado do servidor presente):



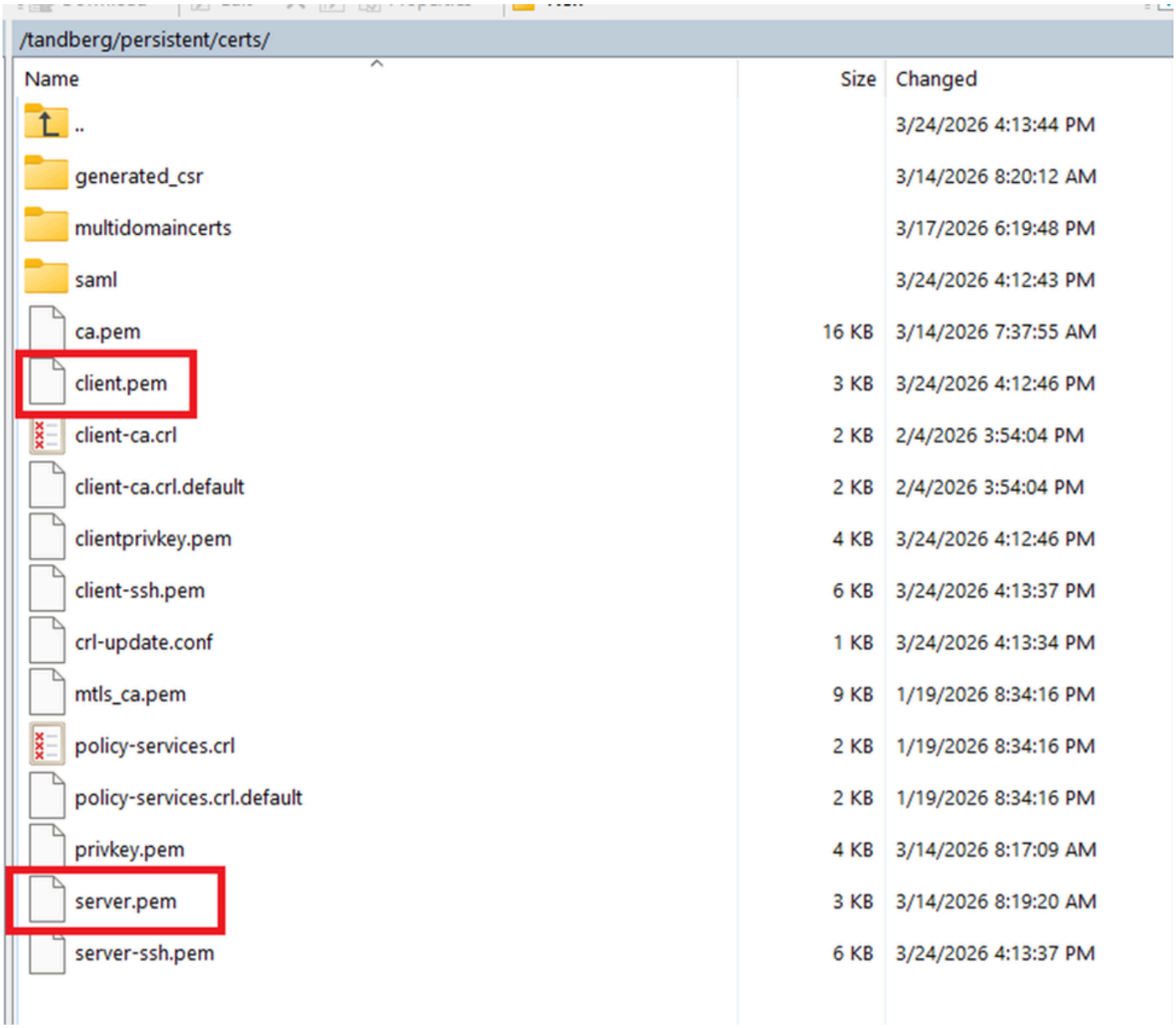
Após a atualização bem-sucedida para x15.5

Aqui, você vê 2 opções de certificado em Manutenção > Segurança > certificado do cliente e certificados do servidor. Após a atualização para x15.5, os portais de certificado do servidor e do cliente na administração da Web mostram o mesmo certificado porque o certificado do servidor de x15.4 foi copiado para o armazenamento de certificados do cliente em x15.5.



O certificado e a chave privada existentes após a atualização para x15.5 foram copiados para o armazenamento de certificados do cliente.

Diretório persistente/certificado do sistema de arquivos Expressway em x15.5:



Verificação de EKU X15.5 durante handshake TLS

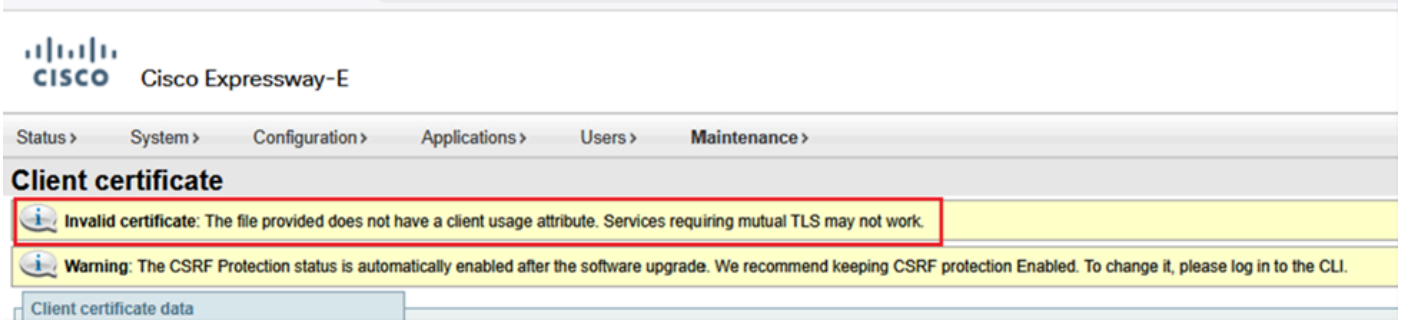
Em x15.5, um novo comando CLI foi introduzido para verificar o uso estendido de chave (EKU - Extended Key Usage) durante o handshake TLS. O valor padrão é "LIGADO". O conjunto de comandos é válido em Expressway Core e Edge.

O conjunto de comandos aciona uma verificação de todas as conexões SIP TLS de ENTRADA no Expressway. (saudações/certificado de cliente de entrada apresentado). Quando ativada, esta opção verifica se o certificado apresentado pelo iniciador TLS contém ou não EKU de cliente no certificado. SE DESLIGADO, a verificação é ignorada; no entanto, o EKU do servidor é verificado se ele está presente no certificado.

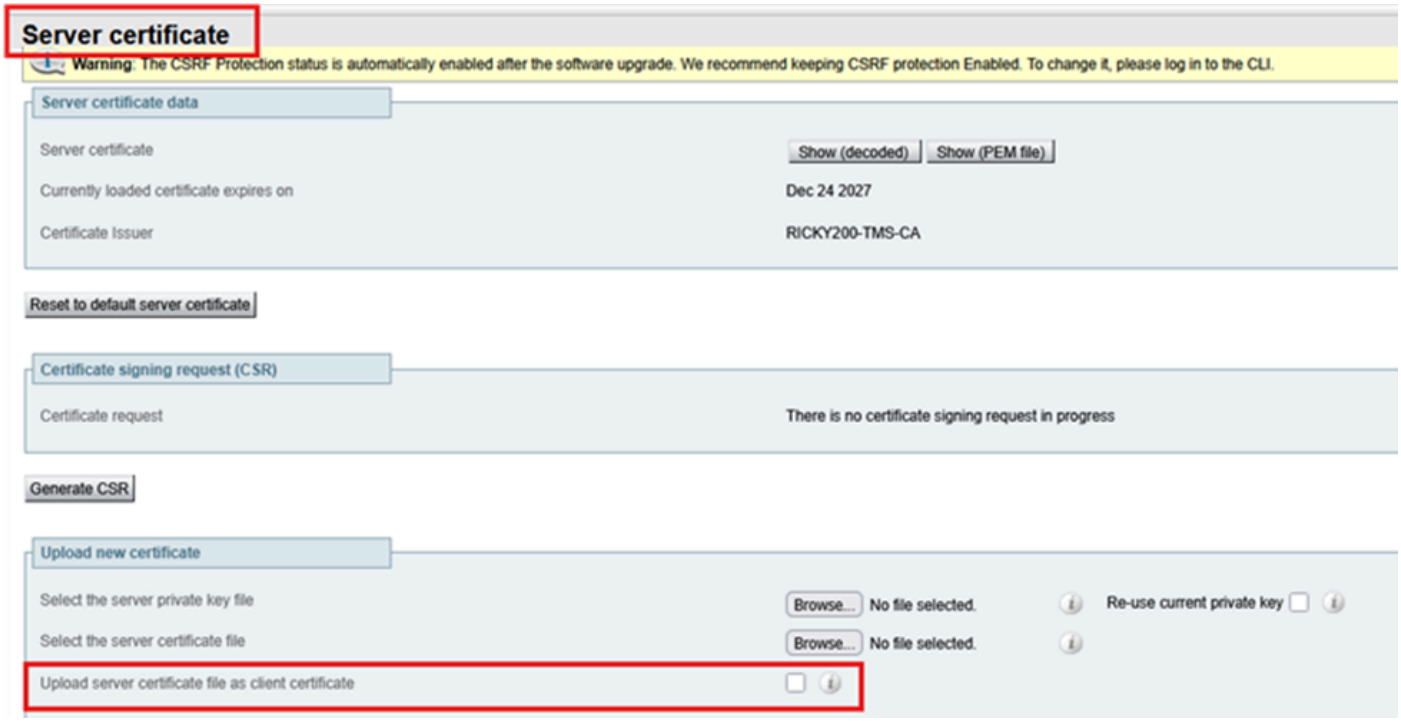
Modo de Verificação ExtendedKeyUsage do Certificado TLS SIP do xconfiguration: LIGAR/DESLIGAR:

Note: Se você gerar um certificado de cliente, assinando um CSR que não contenha EKU de cliente (um exemplo de certificado assinado por uma CA pública), não será possível carregar esse certificado manualmente no armazenamento de certificados de cliente. Portanto, você precisa garantir que os certificados gerados pela assinatura de um CSR sempre contenham o EKU do cliente (uma CA privada pode ser usada para inserir o EKU do cliente).

Tip: Esse erro fica evidente quando você tenta carregar um certificado assinado CSR, que não tem o EKU do cliente, no repositório de certificados do cliente.



No entanto, se você optar por carregar um certificado que tenha apenas um EKU de servidor (sem EKU de cliente) através do armazenamento de certificados do servidor e selecionar Carregar arquivo de certificado do servidor como certificado de cliente, o certificado será copiado para o armazenamento de certificados do cliente. Os administradores que não desejam usar um certificado assinado por uma CA privada no Expressway-Edge podem optar por copiar a EKU do servidor somente do armazenamento de certificados do servidor para o armazenamento de certificados do cliente.

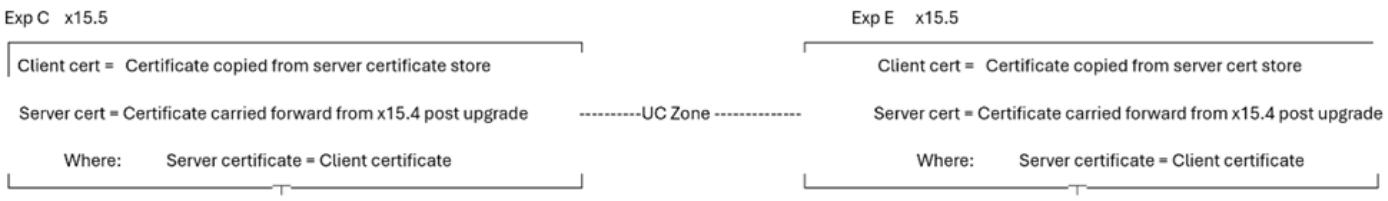


Vários armazenamentos de certificados, vários cenários de implantação

Como agora há dois armazenamentos de certificados no Expressway, há vários cenários de armazenamentos de certificados.

Condição 1: Atualização

Quando o Expressway é atualizado de x15.4 ou anterior a x15.5, essa condição é verdadeira. Os certificados existentes da versão x15.4 são copiados em dois (2) armazenamentos de certificados. No cliente e no servidor x15.5, os certificados são os mesmos.

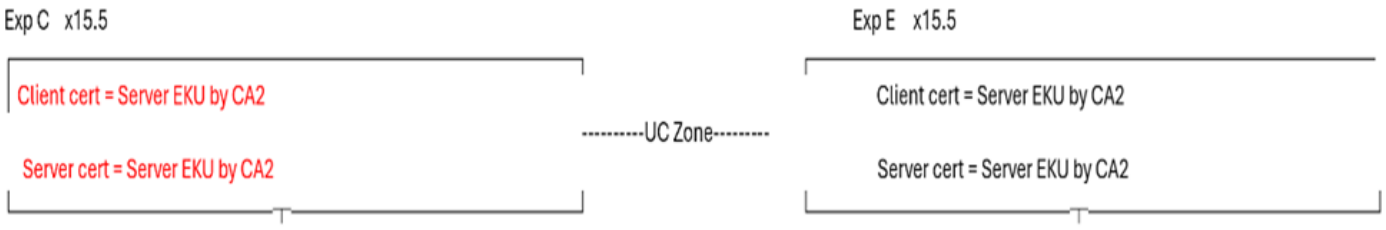


Condição 2: Quando o administrador instala um novo certificado em x15.5 (certificados existentes expirados)

CA 1 = CA interna

CA 2 = CA pública

Na figura a seguir, o Expressway Core tem um certificado de cliente com EKU de servidor assinado somente por CA 2 (CA pública) e um certificado de servidor com EKU de servidor assinado somente por CA 2 (CA pública). Da mesma forma, o Expressway E tem um certificado de cliente com o servidor EKU assinado por CA2 (CA pública) e um certificado de servidor com o servidor EKU assinado somente por CA 2 (CA pública).



Se o certificado do servidor núcleo Expressway não tiver um EKU de cliente, zona de passagem de comunicações unificadas, MRA, o proxy WebRTC não funcionará. Certifique-se de que o certificado do servidor núcleo Expressway tenha um EKU cliente. Este é um caso de uso comum em que os usuários optam por assinar todos os certificados de uma CA pública. Como a CA pública não inclui o EKU do cliente em certificados, a zona de passagem de comunicações unificadas se torna ativa.

Para tornar a zona UC ativa, uma correção rápida é desativar a verificação de EKU no Expressway E. Isso ativa a zona de UC. No entanto, os túneis SSH permanecem inativos. A partir de hoje, a comunicação do túnel SSH no 2222 requer a validação do EKU cliente.

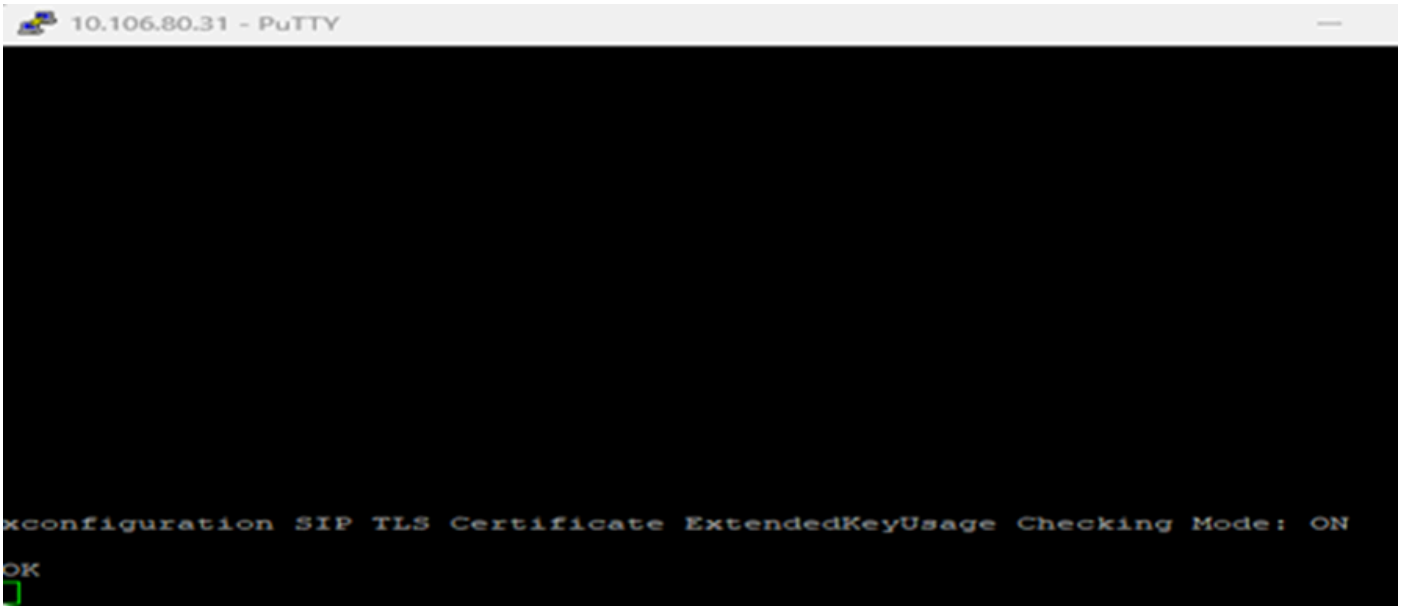
O logon do cliente MRA e as funções proxy WebRTC não funcionam. Você poderia ter que recorrer a CA privada.

Caso de teste 1

- Quando a verificação EKU está "ON" no Expressway E
- Quando o certificado de Cliente e Servidor no núcleo do Expressway tem somente EKU de Servidor
- O status da zona UC é FALHA

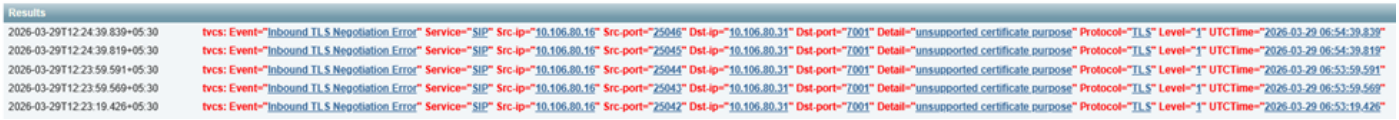
Em Expressway-Edge ExtendedKeyUsage, verifique ON.

Modo de Verificação ExtendedKeyUsage do Certificado TLS SIP do xconfiguration: Ligado:



Falha na zona de comunicação unificada:

Os logs do Expressway E mostram onde 10.106.80.16 = Expressway Core, 10.106.80.31 = Expressway Edge:

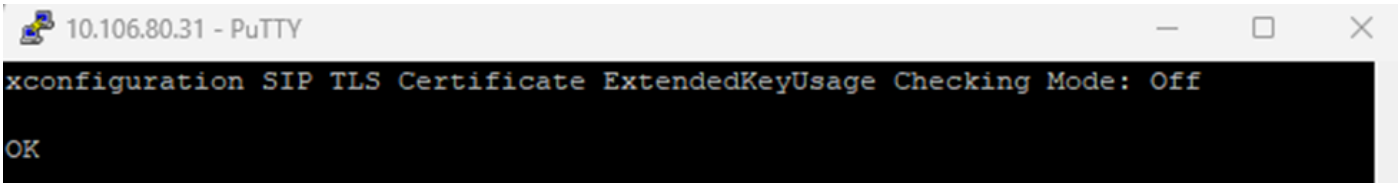


Caso de teste 2

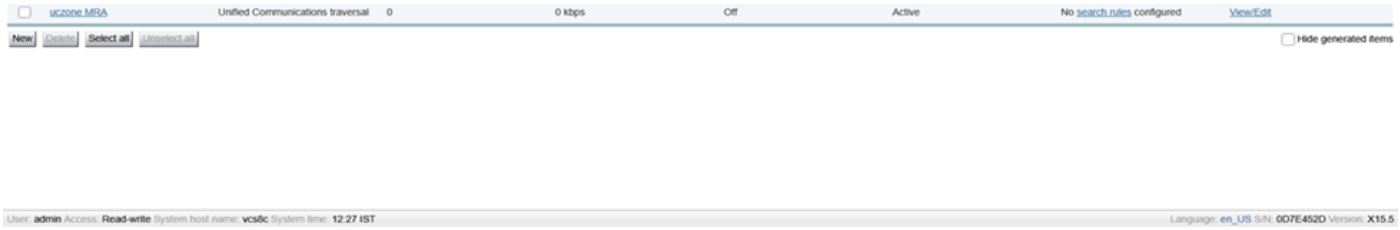
- Quando a verificação EKU está DESATIVADA no Expressway E
- Quando o certificado de Cliente e Servidor no Expressway Core tiver somente EKU de servidor
- O status da zona UC é ATIVO

Desative a verificação de EKU no Expressway E.

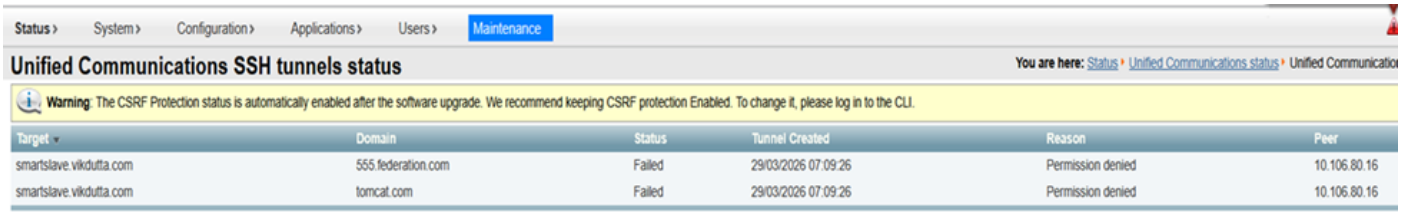
Modo de Verificação ExtendedKeyUsage do Certificado TLS SIP do xconfiguration: Off



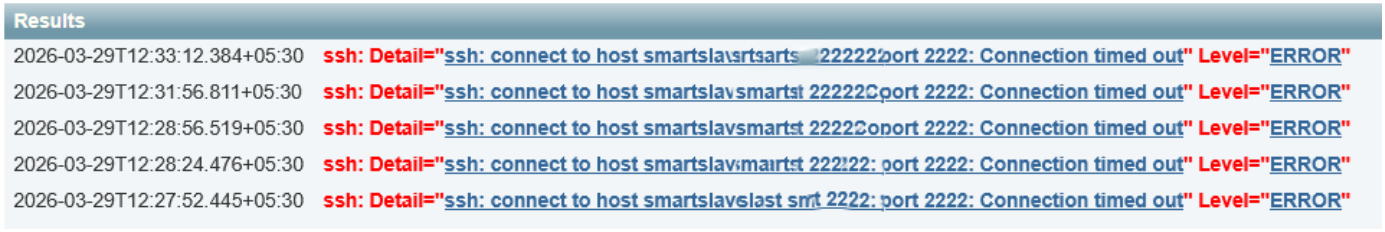
Zona de comunicação unificada ativa:



No entanto, os túneis ssh ainda falharam:



Logs de eventos do Expressway:



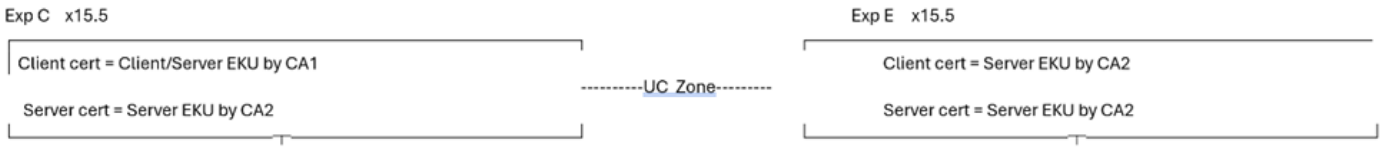
Condição 2.1: Caso de sucesso

CA 1 = CA interna

CA 2 = CA pública

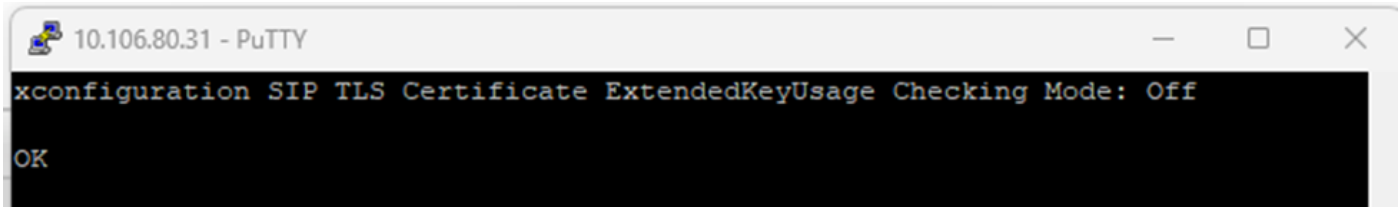
- Onde o certificado de cliente principal do Expressway é assinado pela CA 1 (CA interna) e inclui, EKU cliente/servidor ambos.
- O certificado do servidor núcleo Expressway é assinado por CA 2 pública e inclui somente EKU de servidor.

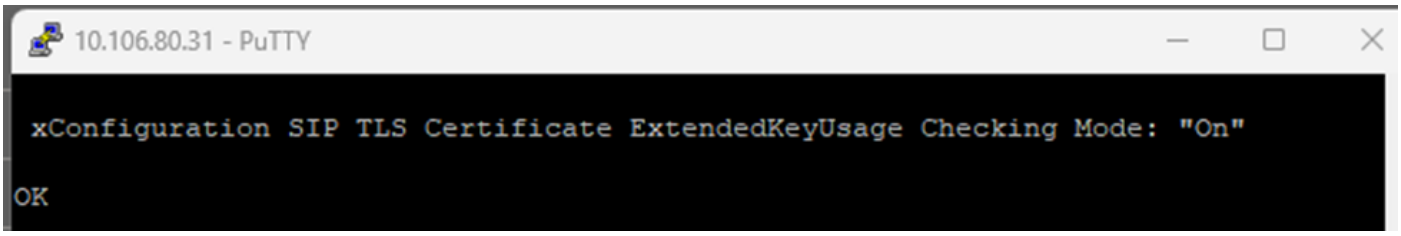
- O certificado do Servidor de Borda do Expressway é assinado pela CA 2 pública e inclui somente a EKU do Servidor.
- O certificado do cliente de Borda do Expressway é assinado pela CA 2 pública e inclui somente EKU do Servidor.



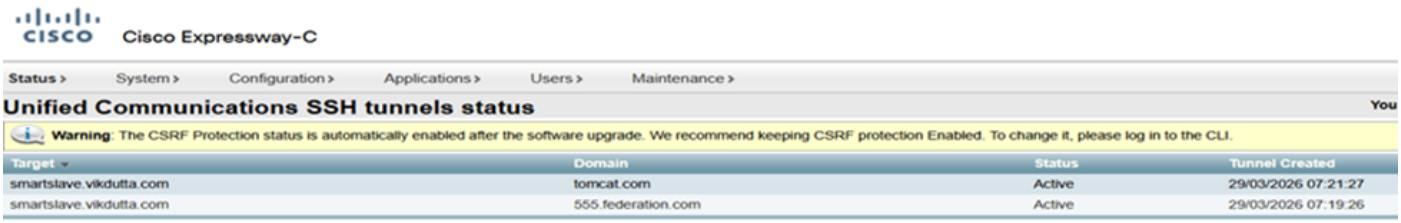
Essa condição é um caso de sucesso. Independentemente de o modo de verificação EKU ser ON/OFF, a zona de Comunicação Unificada e o túnel SSH se tornam ativos. Os clientes MRA funcionam.

Não importa se a verificação de EKU de borda do Expressway está DESATIVADA ou ATIVADA. O certificado de cliente principal do Expressway contém EKU de cliente:

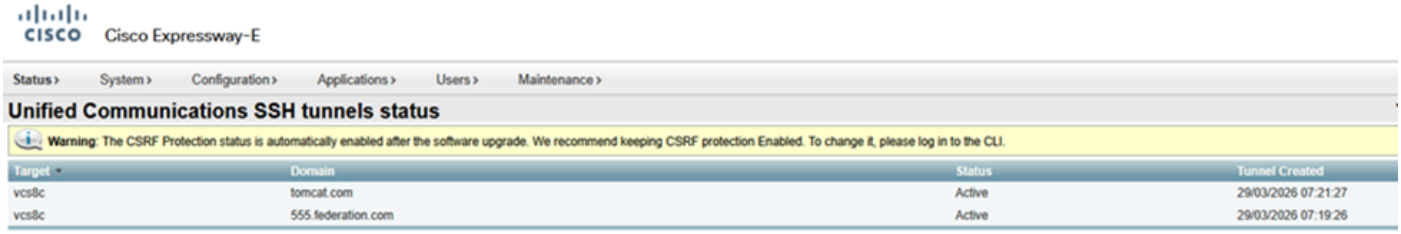




Túneis SSH no núcleo do Expressway Ativos:

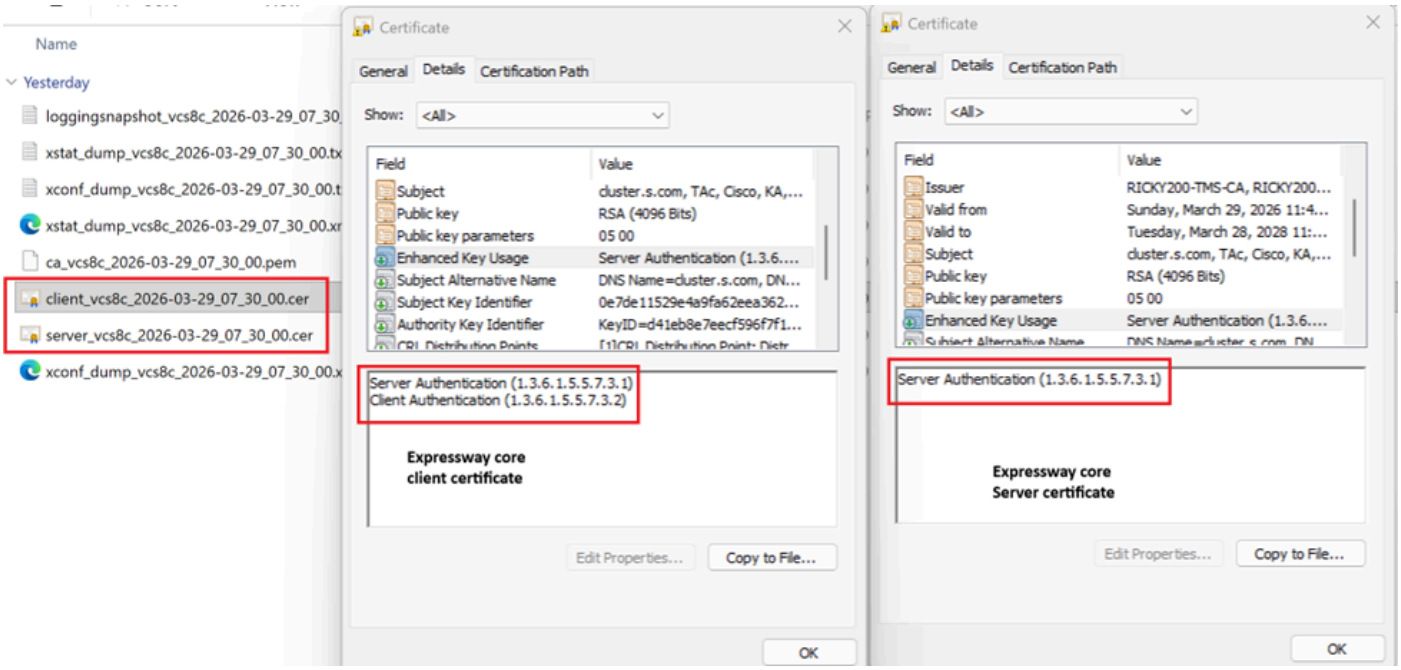


Túneis SSH na Borda do Expressway Ativos:

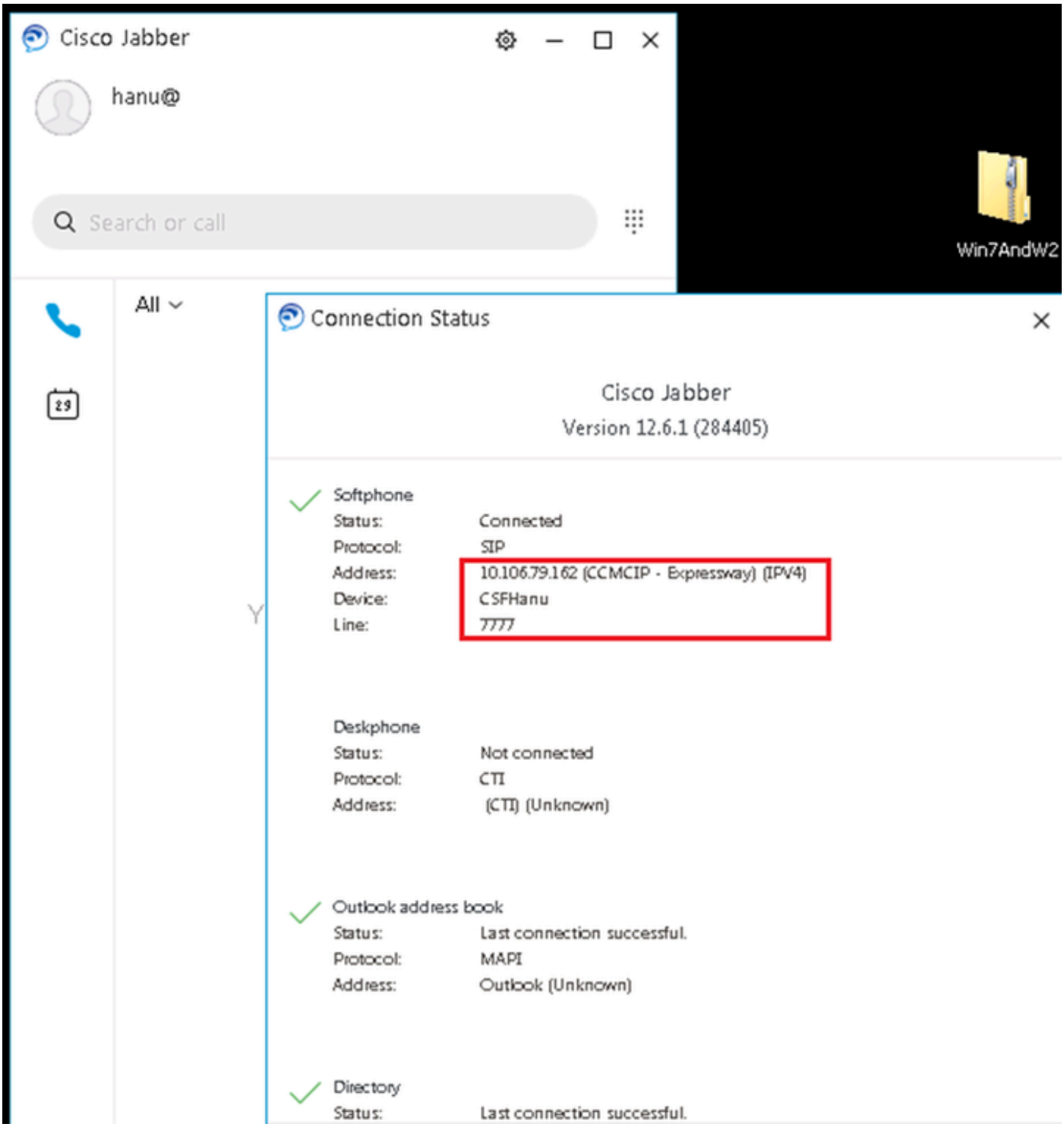


Status Ativo da Zona MRA de Comunicação Unificada:

- O certificado do cliente Expressway-Core tem EKU de servidor e EKU de cliente.
- O certificado do servidor central do Expressway tem somente EKU de servidor.



O cliente MRA faz logon e está registrado:

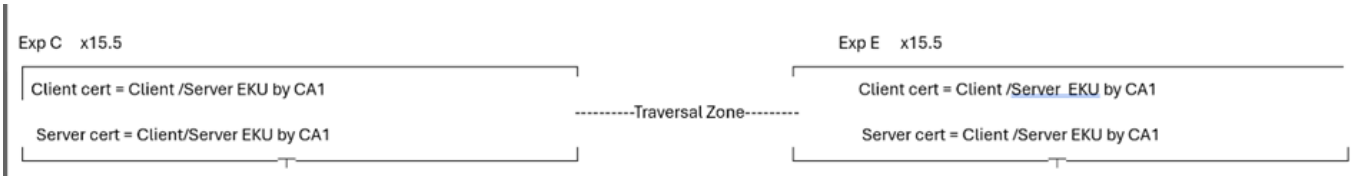


Note: Compare e anote as EKUs presentes nos certificados para que o proxy MRA e WebRTC funcionem. É uma comparação entre uma implantação funcional e uma não funcional.

Condição 3: Assina todos os certificados com uma AC privada

CA 1 = CA interna

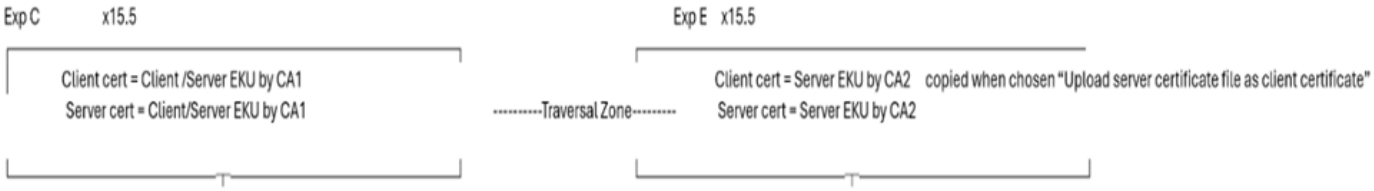
CA 2 = CA pública



Na condição 3, todos os certificados são assinados pela CA interna (CA1) .

- Quando o Expressway-E envia uma conexão TLS, a raiz/intermediário CA 1 precisa ser trocada com a entidade da extremidade oposta. Se a extremidade oposta não tiver capacidade ou não permitir que um certificado de CA privado seja carregado, a conexão TLS não será bem-sucedida.
- Os clientes MRA obtêm certificados para aceitar pop-ups se o certificado privado não estiver no armazenamento confiável do SO.

Condição 4: A Borda do Expressway tem Certificados Públicos com EKU de Servidor Somente



Na condição 4, os certificados de cliente e servidor núcleo do Expressway são (CA1) CA interna assinada e têm EKU de cliente e servidor presentes. O certificado do servidor Expressway E é uma CA pública assinada e tem somente EKU de servidor. O certificado do servidor é copiado para o repositório de certificados do cliente, escolhendo Carregar arquivo de certificado do servidor como certificado do cliente.

Na condição 4, quando a conexão TLS é feita à extremidade oposta, se o Expressway -E envia uma saudação de cliente TLS, a extremidade oposta precisa desabilitar a verificação de EKU do cliente (pois o certificado do cliente não tem EKU de autenticação do cliente) ou a conexão TLS não é bem-sucedida.

Pode haver muito mais condições ou cenários no campo com base na implantação de usuários e casos de uso, e todos não podem ser cobertos devido ao meu fluxo limitado de ideias. No entanto, os pontos a serem lembrados são:

- # SE o Expressway se tornar um cliente durante o handshake TLS, o certificado do cliente

será apresentado aos pares.
- #IF Expressway torna-se servidor durante o handshake TLS; o certificado do servidor é apresentado ao par.

Este raciocínio foi estabelecido com estes casos de testes.

Cenário 1

Para esse cenário, o Expressway apresenta o certificado do cliente durante o handshake MTLS com o Webex.

Uma chamada de vídeo para a reunião do Webex:

Exemplo de fluxo de chamada Jabber -à CUCM -à Exp Core —à Exp Edge —à Webex

10.106.80.31= Expressway Edge

163.129.37.33 = Webex

2026-03-24T11:54:26.106+00:00 tvcs smartslave: UTCTime="2026-03-24 11:54:26,106" Module="network.sip" Level="DEBUG": Action="Enviado" Local-ip="10.106.80.31" Local-port="25002" Dst-ip="163.129.37.33" Dst-port="5061"

Expressway Edge tem certificado de cliente com esse número de série (2f0000004c869c77c8981becde00000000004c).

O Expressway Edge envia hello do cliente para o "Webex durante a negociação TLS e, em seguida, envia o certificado do cliente.

Número de série 2f0000004c869c77c8981becde00000000004c:

1. Expressway Edge envia hello do cliente (pkt= 13699) para ‘Webex durante a negociação mTLS.

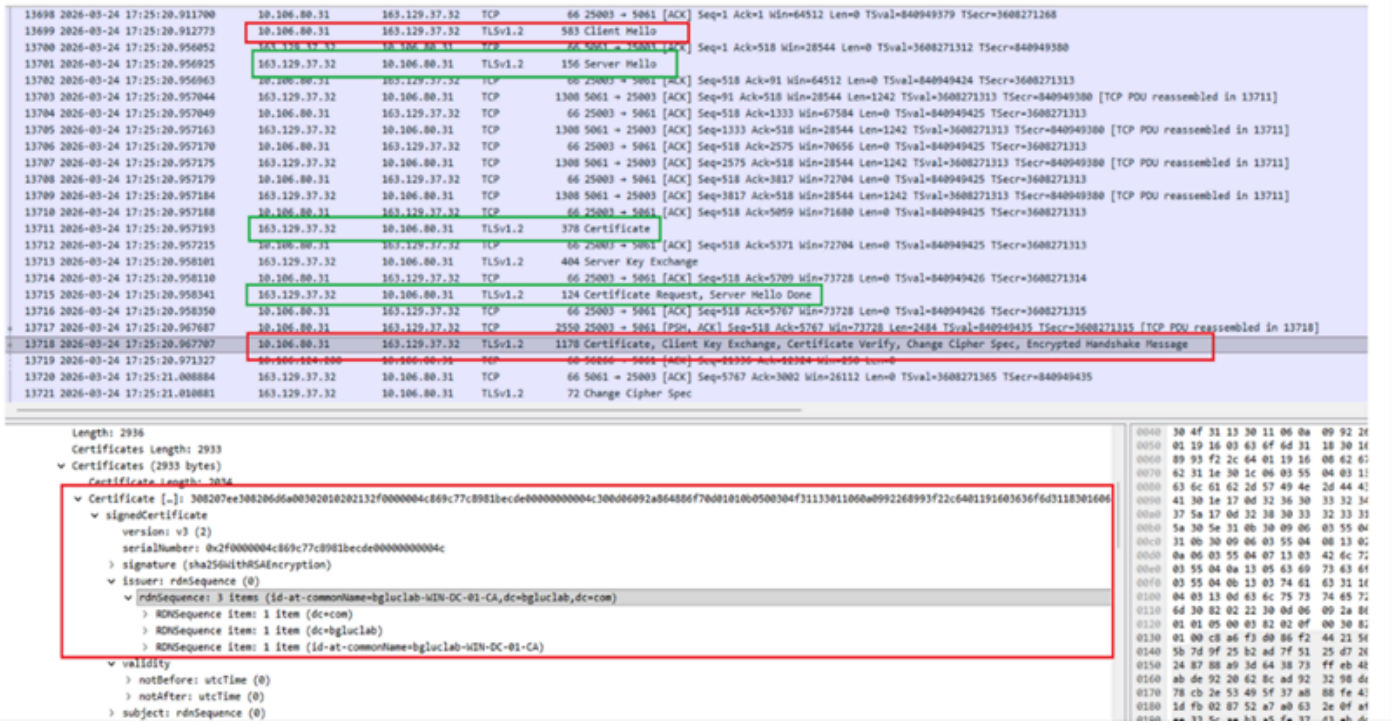
2. O Webex envia um hello de servidor para Expressway Edge (pkt=13701).

3. Webex envia seu certificado para Expressway Edge (pkt=13711).

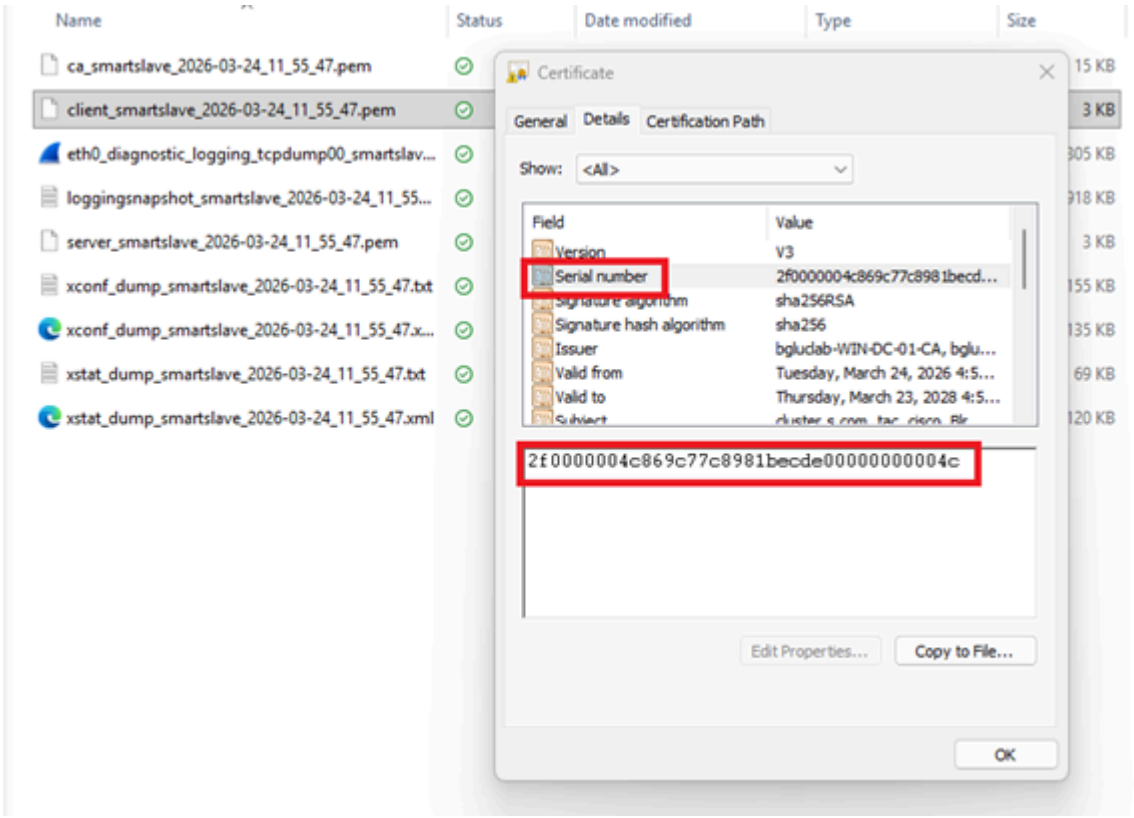
4. Webex solicita "CertificateRequest" de certificado de borda Expressway (pkt=13715).

5. Expressway Edge envia seu certificado para o Webex (pkt=13718).

(captura de tela)



Certificado de cliente da Borda do Expressway:



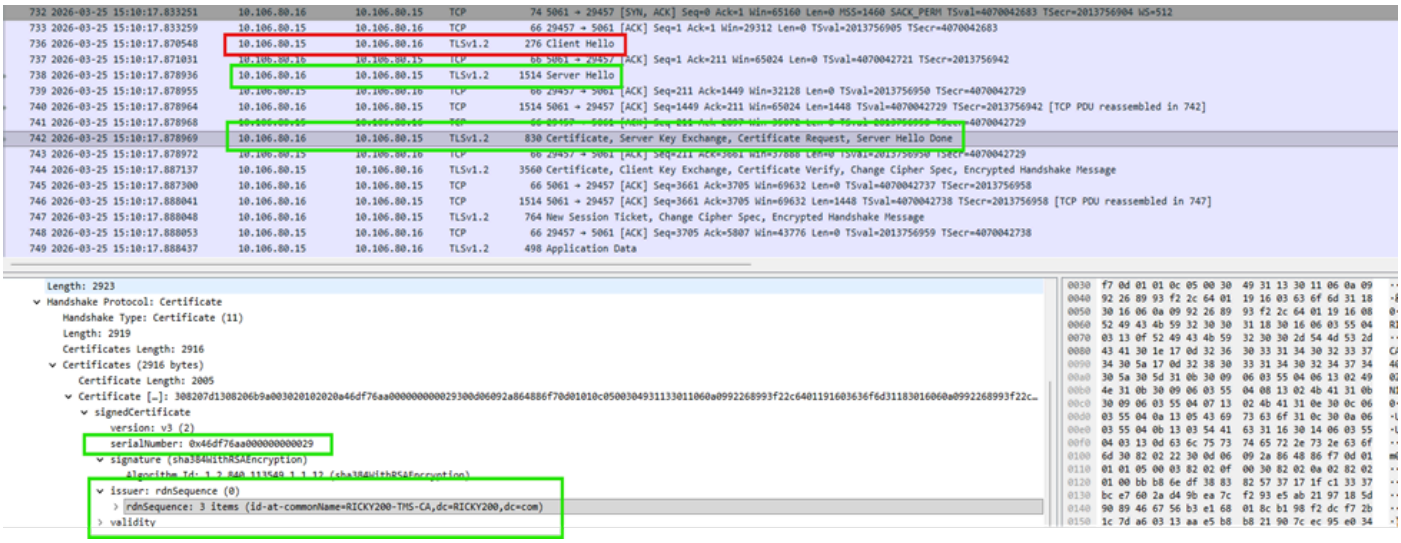
Cenário 2

O Expressway torna-se uma entidade de servidor durante o handshake mTLS e apresenta seu certificado de servidor:

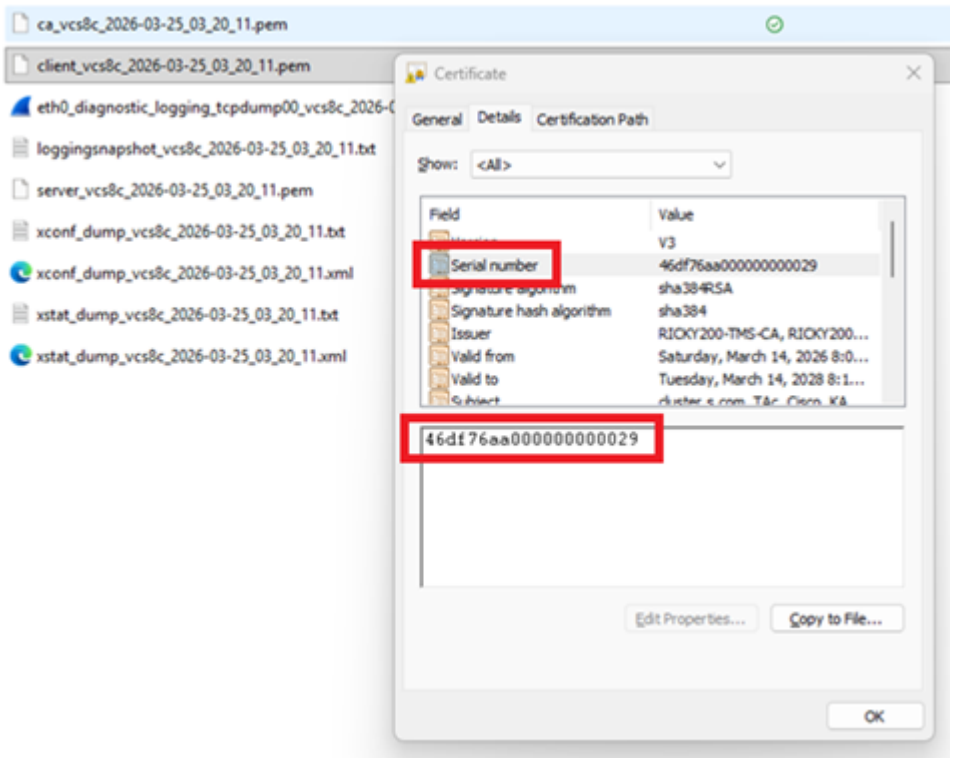
Onde o Expressway apresenta o certificado do servidor, o Expressway tem uma zona de vizinho segura sobre 5061 com o nome de verificação LIGADO.

Zona vizinha segura entre o nó Expressway x15.5 e o nó Expressway x8.11.4:

```
10.106.80.15 (x8.11.4) sends a client hello to 10.106.80.16 (x15.5) (pkt=736)

10.106.80.16 sends a server hello to 10.106.80.15 (pkt=738)

10.106.80.16 (x15.5) presents its server cert during TLS handshake (pkt=742) and requests client's cert

10.106.80.15 (x8.11.4) sends client certificate (pkt=744)
```



Esta captura de tela mostra o certificado do servidor quando o número de série corresponde a:



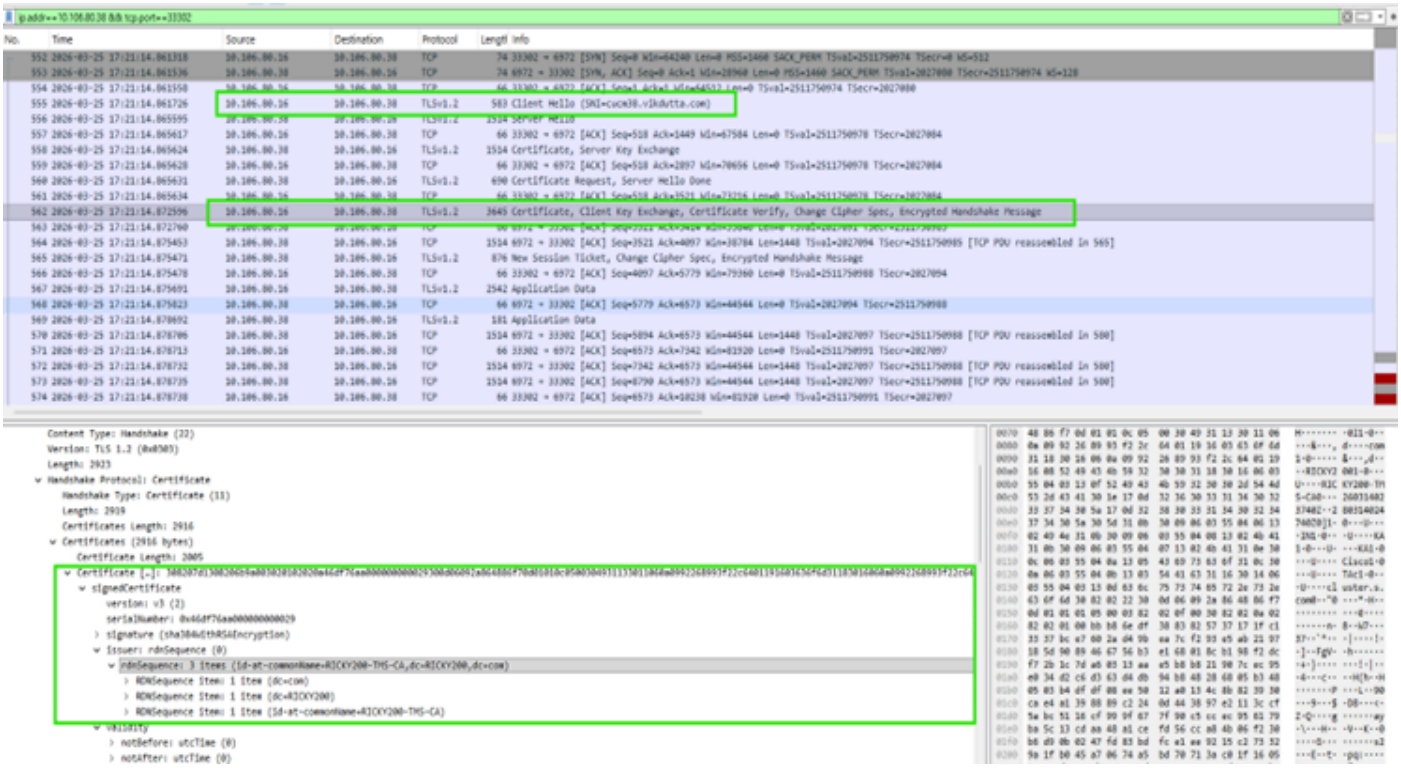
Caso de teste 3: o cliente MRA é provisionado para login e o fluxo de trabalho inclui verificação de certificado do servidor de tráfego entre o Expressway Core e o CUCM.

10.106.80.16 = Expressway Core x15.5

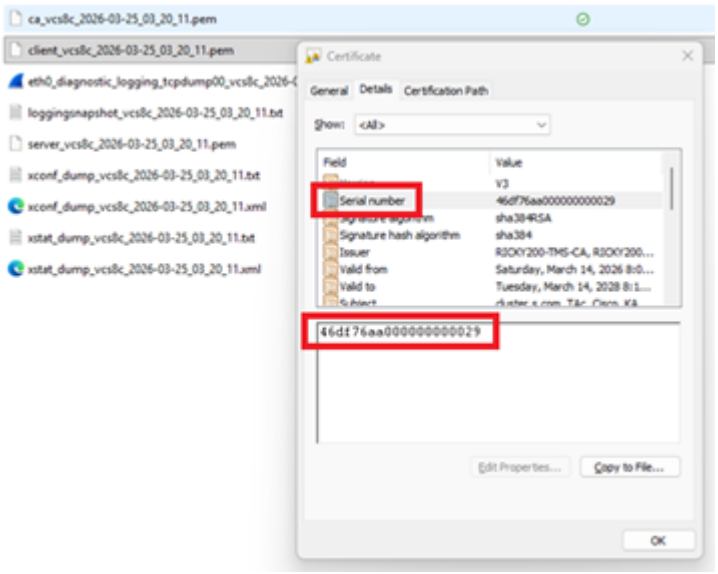
10.106.80.38 = CUCM

- O Exp C 16 envia uma saudação de cliente em 6972 TFTP.

- O Exp C 16 envia um certificado de cliente durante o handshake TLS.



Certificado de cliente principal do Expressway:



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.