Configurar a inscrição de certificado com o protocolo ACME no firewall seguro

Contents

Introdução

Este documento descreve o processo para registrar um certificado TLS (Transport Layer Security) usando o protocolo ACME (Automated Certificate Management Environment) no Secure Firewall ASA.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Firewall Adaptative Security Appliance (ASA)
- Public Key Infrastructure (PKI)

Componentes Utilizados

- Cisco ASAv versão 9.23.1.
- Cisco ASDM versão 7.23(1).
- Servidor de Autoridade de Certificação (CA) que suporta o protocolo ACME.

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.

Requisitos e limitações

Os requisitos e limitações atuais para a inscrição da ACME no Secure Firewall ASA são:

- Suportado no ASA versão 9.23.1 e ASDM 7.23.1 em diante
- Não suportado em contexto múltiplo
- O ACME não suporta a criação de certificados curinga. Cada solicitação de certificado deve especificar um nome de domínio exato.
- Cada ponto confiável registrado por meio do ACME é limitado a uma única interface, o que significa que os certificados registrados com o ACME não podem ser compartilhados em várias interfaces.
- Os pares de chaves são gerados automaticamente e não podem ser compartilhados para certificados registrados através do ACME. Cada certificado usa um par de chaves exclusivo, aumentando a segurança, mas limitando a reutilização de chaves.

Considerações sobre downgrade

Após o downgrade para uma versão que não ofereça suporte à inscrição de ACME no Secure Firewall ASA (9.22 e anterior):

- Todas as configurações de ponto confiável relacionadas à ACME novas para 9.23.x ou mais recentes são perdidas
- Todos os certificados registrados via ACME permanecem acessíveis, mas a chave privada é desassociada após a primeira gravação e reinicialização pós-downgrade

Se for necessário fazer um downgrade, execute o próximo procedimento alternativo recomendado:

1. Antes do downgrade, certifique-se de exportar os certificados ACME no formato PKCS12.
2. Antes do downgrade, certifique-se de remover a configuração do ponto de confiança do ACME.
3. Após o downgrade, importe o certificado PKCS12. O ponto confiável resultante ainda é

válido até que o certificado emitido via ACME expire.

Informações de Apoio

O protocolo ACME foi projetado para simplificar o gerenciamento de certificados TLS para administradores de rede. Ao usar o ACME, os administradores podem automatizar os processos envolvidos na obtenção e renovação de certificados TLS. Essa automação é particularmente benéfica ao utilizar autoridades de certificação (CAs) como Let's Encrypt, que oferecem certificados gratuitos, automatizados e abertos usando o protocolo ACME.

O ACME suporta a emissão de certificados de validação de domínio (DV). Esses certificados são um tipo de certificado digital que confirma o controle do detentor do certificado sobre domínios especificados. O processo de validação para certificados DV é normalmente conduzido através de um mecanismo de desafio baseado em HTTP. Neste mecanismo, o requerente coloca um ficheiro específico no seu servidor Web, que a Autoridade de Certificação (AC) verifica acessando o ficheiro através do servidor HTTP do domínio. A conclusão com êxito deste desafio demonstra à autoridade de certificação que o requerente tem o controlo sobre o domínio, permitindo a emissão do certificado de VD.

O processo para concluir a inscrição é o seguinte:

1. Iniciar solicitação de certificado: O cliente solicita um certificado do servidor ACME e especifica o(s) domínio(s) para o(s) qual(is) o certificado é necessário.
2. Receber desafio HTTP-01: O servidor ACME fornece um desafio HTTP-01 com um token exclusivo para o cliente usar para provar o controle do domínio.
3. Preparar resposta de desafio:
    - O cliente cria uma autorização de chave combinando o token do servidor ACME com sua chave de conta.
    - O cliente configura seu servidor Web para servir esta autorização de chave em um caminho de URL específico.
4. O servidor ACME recupera o desafio: O servidor ACME faz uma solicitação HTTP GET ao URL especificado para recuperar a autorização da chave.
5. O servidor ACME verifica a propriedade: O servidor verifica se a autorização da chave recuperada corresponde ao valor esperado para confirmar o controle do cliente sobre o domínio.
6. Emitir certificado: Após a validação bem-sucedida, o servidor ACME emite o certificado SSL/TLS para o cliente.

Fluxo de Autenticação HTTP-01 da Inscrição ACME.

Os benefícios mais relevantes do uso do protocolo ACME para registrar certificados TLS são:

- O ACME facilita a aquisição e a manutenção de certificados de domínio TLS para as interfaces TLS do Secure Firewall ASA. Essa automação reduz significativamente as tarefas manuais e ajuda a manter os certificados atualizados sem supervisão constante.
- Com os pontos de confiança habilitados para ACME, os certificados são renovados automaticamente quando estão prestes a expirar. Esse recurso reduz a necessidade de envolvimento administrativo, garantindo segurança ininterrupta e evitando a expiração inesperada do certificado.

Configurar

Configuração de pré-requisitos

Antes de iniciar o processo de inscrição no ACME, certifique-se de que as próximas condições sejam atendidas:

1. Nome de Domínio Resolvível: O nome de domínio para o qual você solicita um certificado deve poder ser resolvido pelo servidor ACME. Isso garante que o servidor possa verificar a propriedade do domínio.
2. Acesso seguro de firewall ao servidor ACME: O firewall seguro deve ter a capacidade de acessar o servidor ACME por meio de uma de suas interfaces. Esse acesso não precisa ser feito através da interface para a qual o certificado é solicitado.
3. Disponibilidade da porta TCP 80: Permita a porta TCP 80 do servidor ACME CA para a

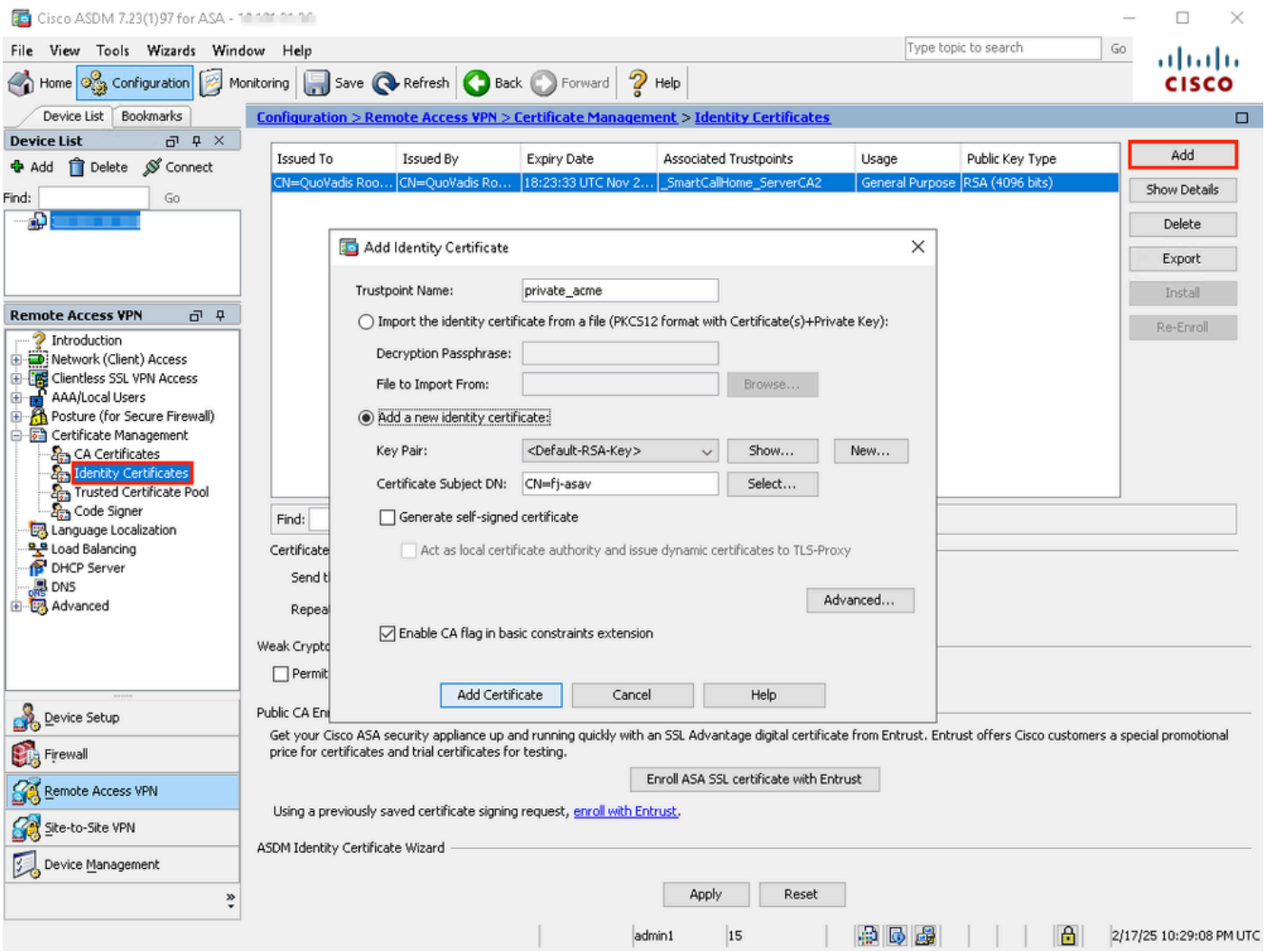
interface que corresponde ao nome de domínio. Isso é necessário durante o processo de troca do ACME para concluir o desafio HTTP-01.

Note: Durante o período em que a porta 80 está aberta, somente os dados de desafio do ACME estão acessíveis.

Inscrição ACME com ASDM

1. Adicione um novo Certificado de Identidade.

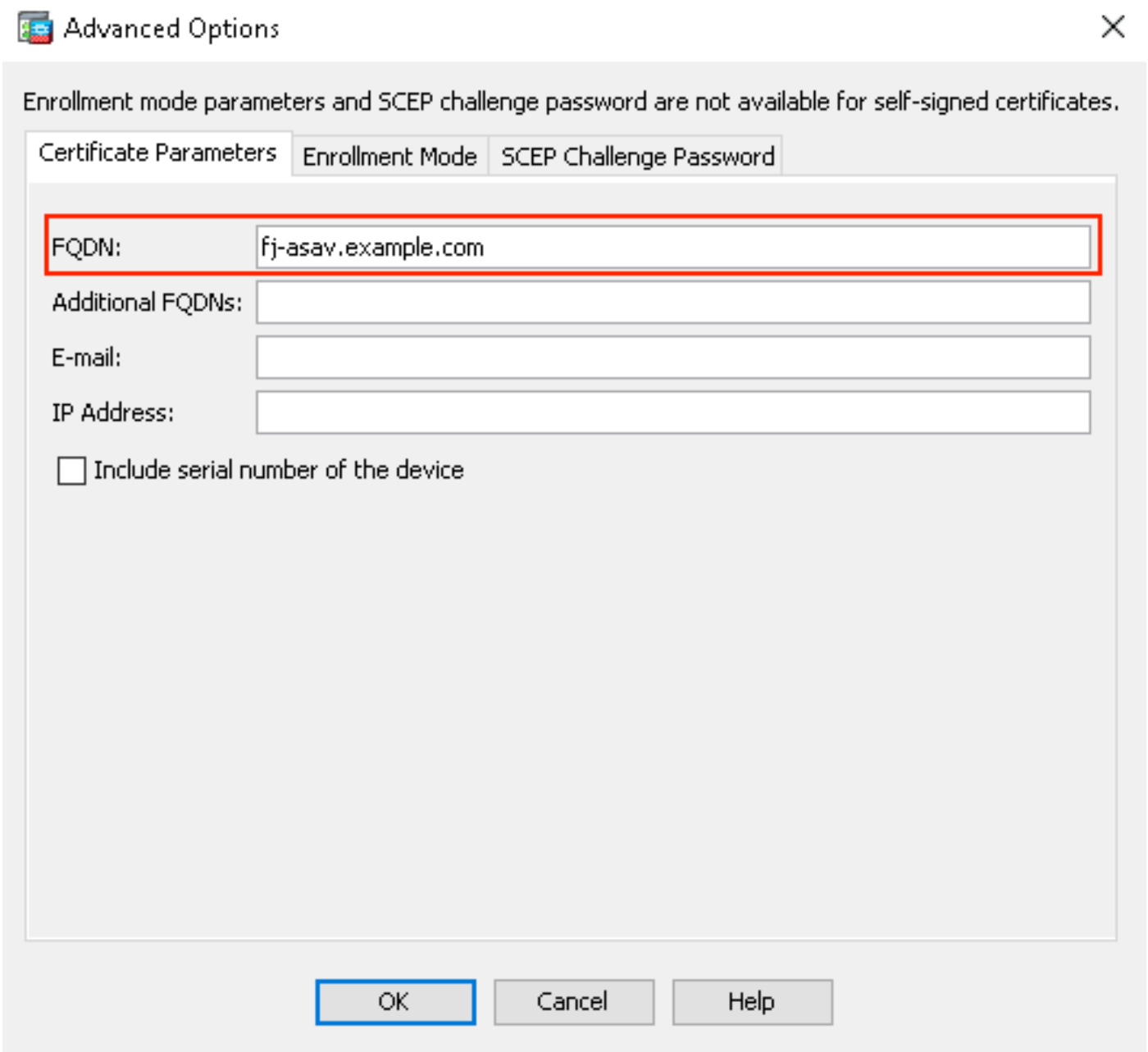
- Navegue até Configuration > Remote Access VPN > Certificate Management > Identity Certificates.
- Clique no botão Add e selecione Add a new identity certificate.



Inscrição ACME Certificado de Identidade ASDM.

2. Especifique o FQDN para o Certificado de Identidade.

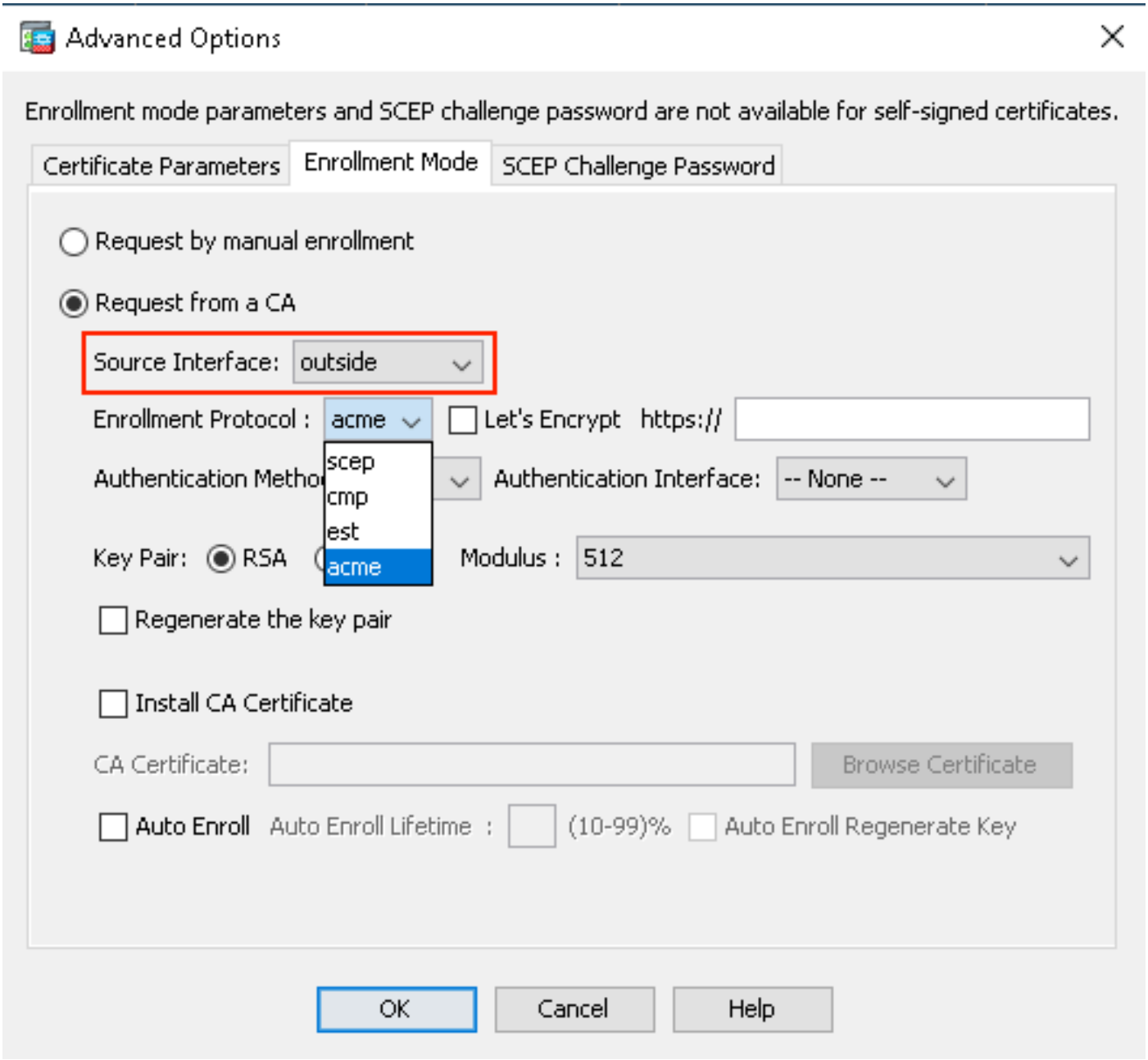
- Clique no botão Avançado.
- Na guia Certificate Parameters, especifique o FQDN que o certificado deve ter.



FQDN do ASDM de inscrição no ACME.

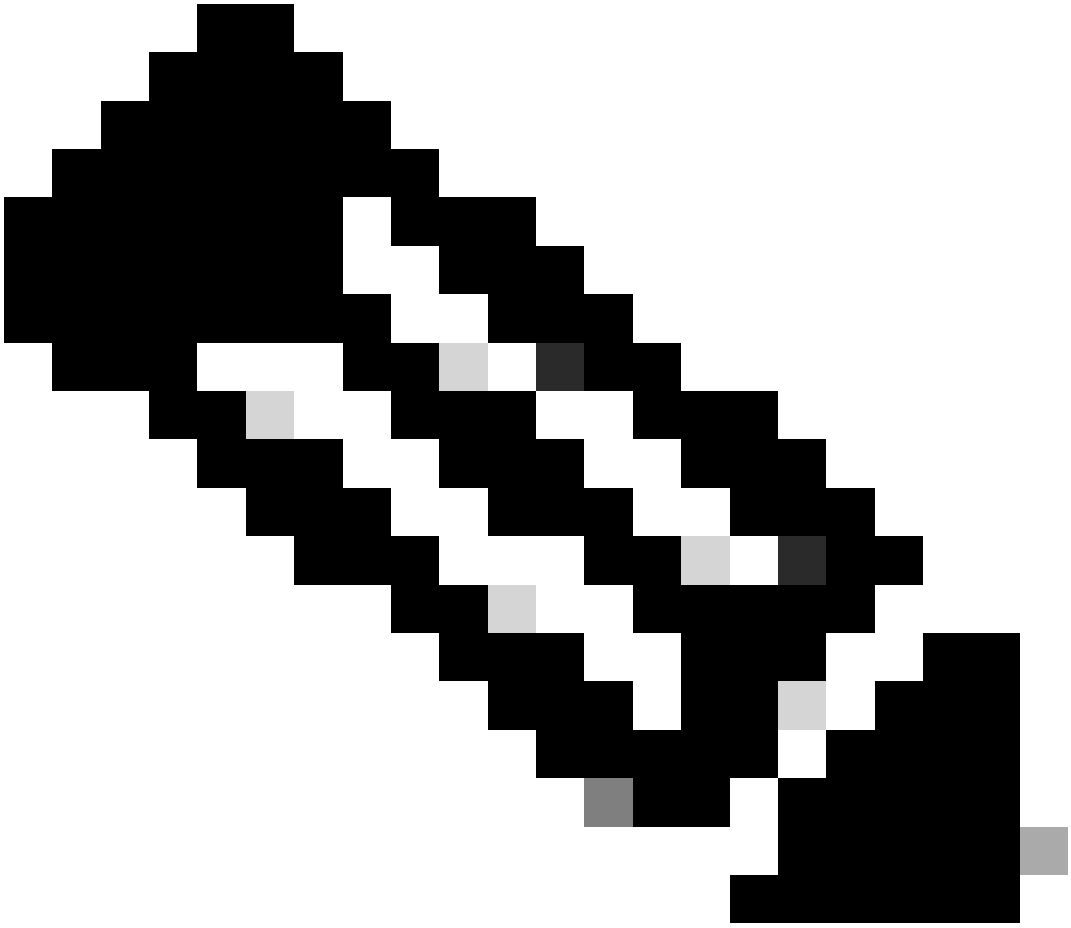
3. Selecione ACME como o protocolo de inscrição.

- Na guia Enrollment Mode, selecione a opção Request from CA.
- Especifique a interface de origem e selecione acme como o protocolo de registro.

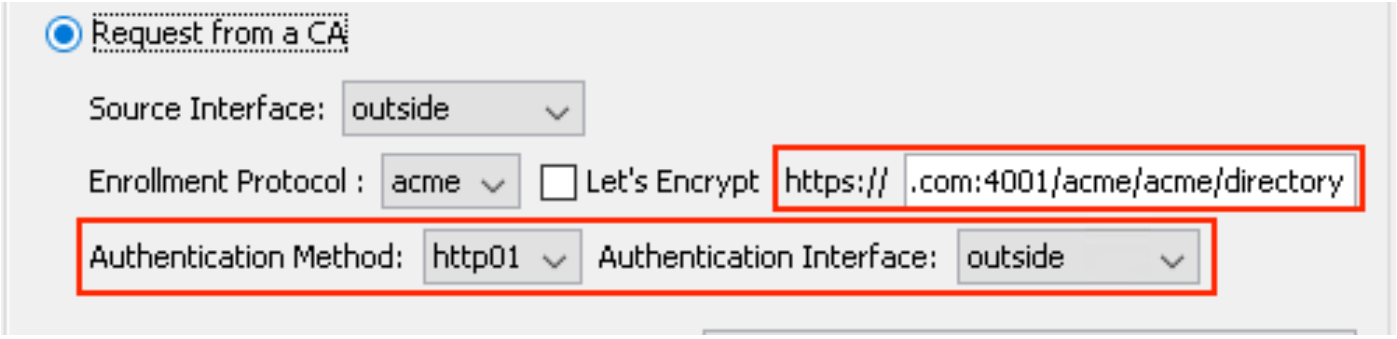


Inscrição ACME Protocolo ASDM acme. seleção

4. Selecione Vamos Criptografar para que o certificado seja assinado por Vamos Criptografar a CA pública. Caso contrário, especifique o URL da sua CA interna que suporta o protocolo de registro ACME. Além disso, especifique a interface de autenticação.



Note: Quando a caixa de seleção Let's Encrypt é marcada, a URL do servidor é preenchida automaticamente.



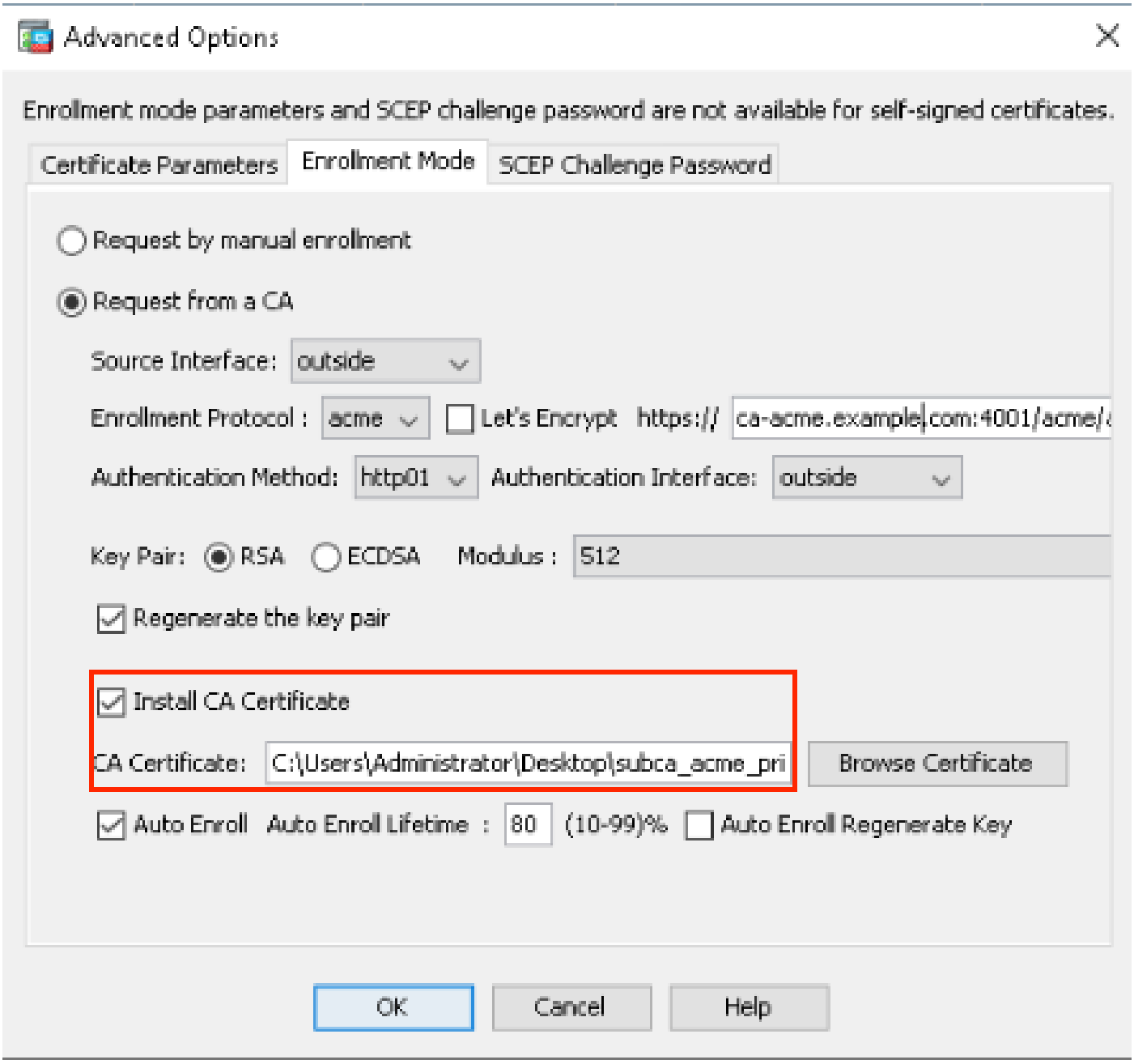
Método de Autenticação ASDM de Inscrição ACME.

5. Instale o Certificado CA.

Se a opção Install CA Certificate estiver marcada, você deverá carregar o certificado da CA imediata que emite seu certificado.

Note: Se o certificado CA já existir no Firewall Seguro, seja de uma instalação anterior ou dentro do pool confiável, não será necessário marcar essa opção. Deixe a caixa de seleção Install CA Certificate desmarcada.

Note: Quando você selecionar a opção Let's Encrypt, deixe a caixa de seleção Install CA Certificate desmarcada, pois os certificados raiz de CA para Let's Encrypt já estão incluídos no pool de confiança do Secure Firewall.

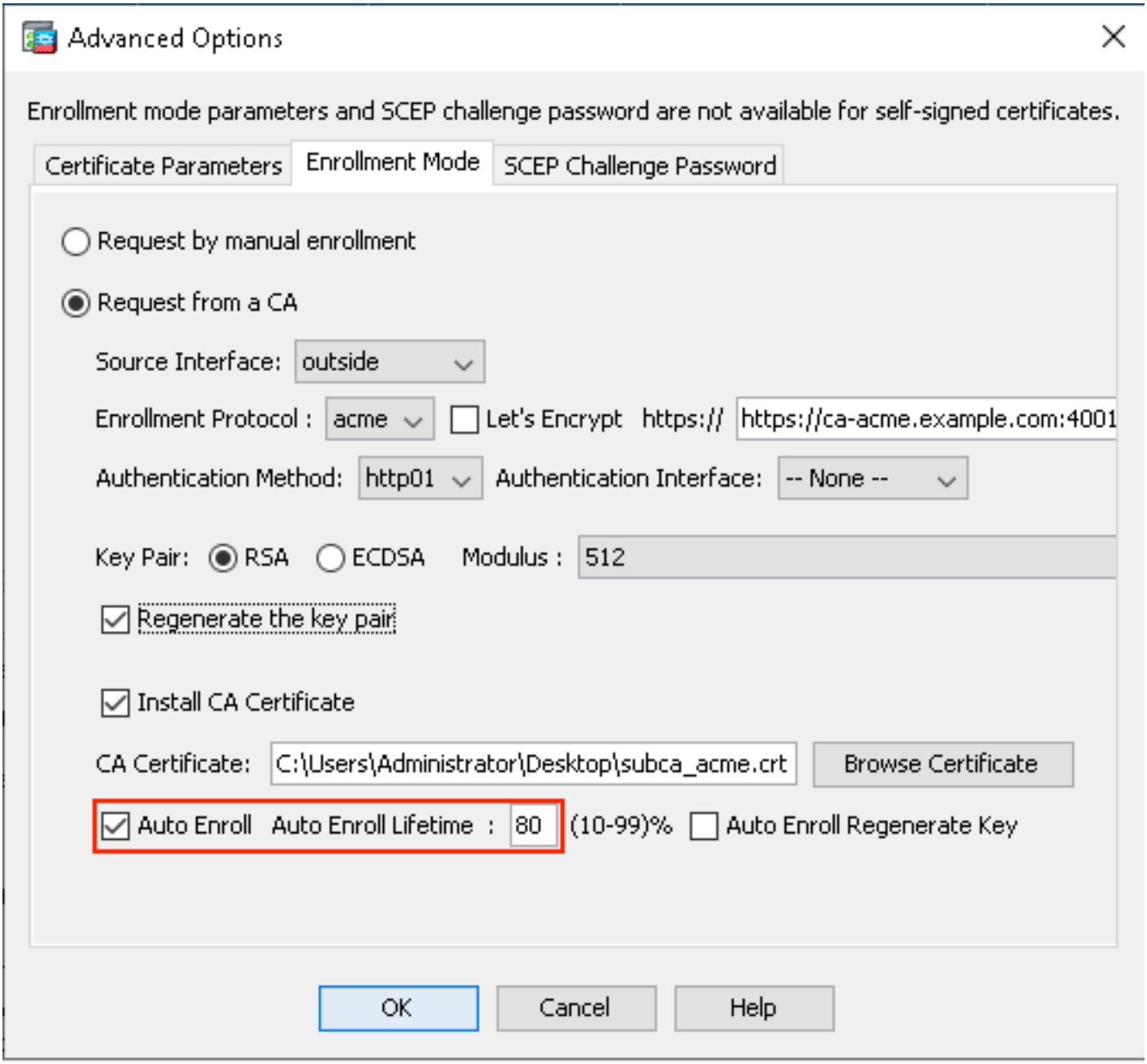


Inscrição ACME Instalação de CA ASDM.

6. (Opcional) Ative a Inscrição Automática para o Certificado de Identidade.

Marque a caixa de seleção Inscrição automática e especifique a porcentagem para o Tempo de vida da inscrição automática.

Este recurso garante que o certificado seja renovado automaticamente antes de expirar. A porcentagem determina com que antecedência da expiração do certificado o processo de renovação começa. Por exemplo, se definido como 80%, o processo de renovação começa quando o certificado atinge 80% de seu período de validade.



Inscrição ACME Inscrição automática ASDM.

7. Clique em OK e Salvar a configuração.

Inscrição na ACME com o Secure Firewall ASA CLI

1. Crie um novo Ponto Confiável.

Crie um ponto confiável e especifique acme como o protocolo de registro.

<#root>

```
asav(config)# crypto ca trustpoint private_acme
asav(config-ca-trustpoint)# enrollment protocol ?

crypto-ca-trustpoint mode commands/options:

acme Automatic Certificate Management Environment

  cmp Certificate Management Protocol Version 2
  est Enrollment over Secure Transport
  scep Simple Certificate Enrollment Protocol
```

2. Selecione o método HTTP-01 para autenticação a fim de verificar o controle do domínio.

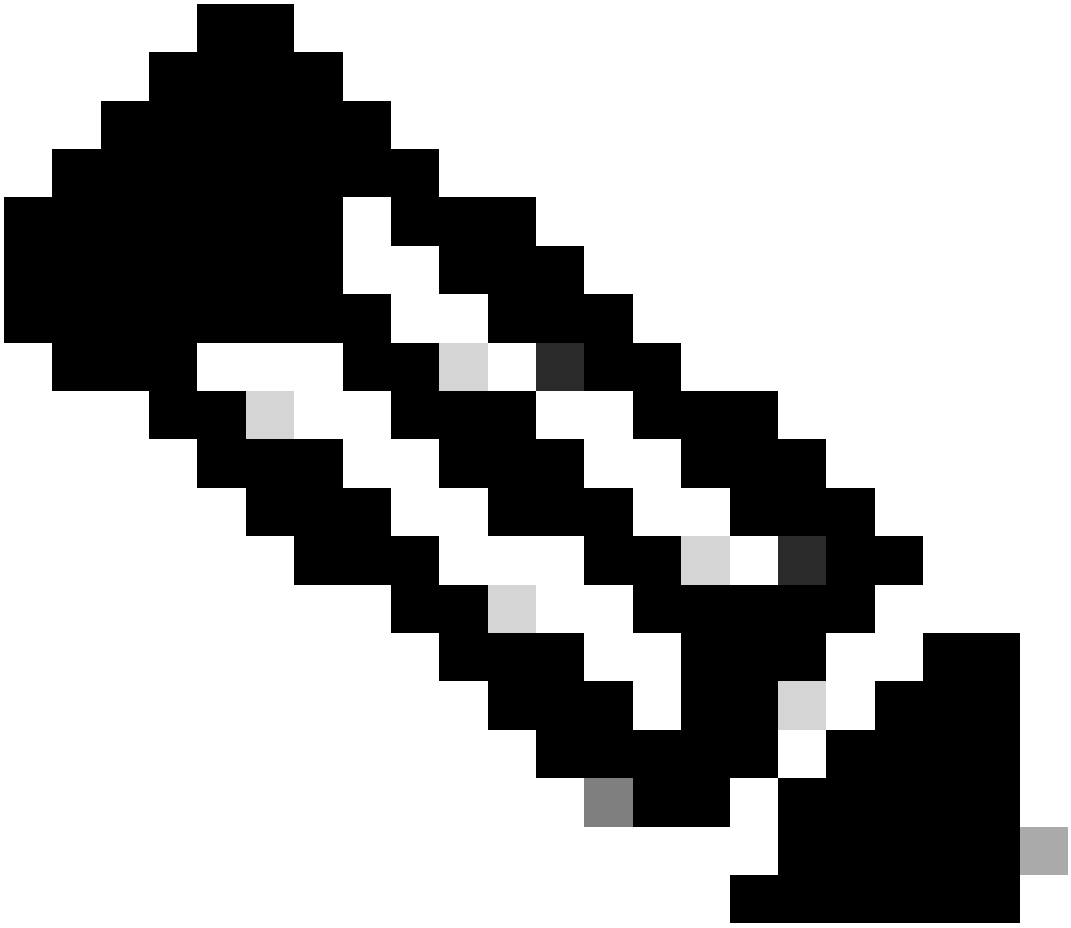
```
asav(config-ca-trustpoint)# enrollment protocol acme authentication ?

crypto-ca-trustpoint mode commands/options:
http01 Use the HTTP-01 method, which opens port 80 on the specified
interface
```

3. Selecione Let's Encrypt as the ACME CA (Vamos criptografar como ACME CA). Se estiver usando outra CA que suporte o protocolo ACME, forneça o URL apropriado.

```
asav(config-ca-trustpoint)# enrollment protocol acme url ?

crypto-ca-trustpoint mode commands/options:
LINE < 477 char URL
LetsEncrypt Use the Let's Encrypt CA
```



Note: Quando a palavra-chave LetEncrypt é configurada, a URL do servidor Let's Encrypt é preenchida automaticamente.

4. Defina o par de chaves RSA, o FQDN (Fully Qualified Domain Name, Nome de domínio totalmente qualificado) e o Nome do assunto do certificado.

```
crypto ca trustpoint private_acme
 enrollment interface outside
 enrollment protocol acme authentication http01 outside
 enrollment protocol acme url https://ca-acme.example.com:4001/acme/acme/directory
 fqdn fj-asav.cisco.com
 subject-name CN=fj-asav.example.com
 keypair rsa modulus 4096
 auto-enroll 80 regenerate
 crl configure
```

5. Autentique o ponto de confiança.

Note: Se a CA já existir no firewall seguro ou ao usar Let's Encrypt, esta etapa poderá ser ignorada.

```
asav(config)# crypto ca authenticate private_acme
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
-----BEGIN CERTIFICATE-----
MIIBwzCCAWqgAwIBAgIQedxaTDOJ1G6tLgAGti6tizAKBggqhkjOPQQDAjAsMRAw
DgYDVQQKEwdjYS1hY21lMRgwFgYDVQQDEw9jYS1hY21lIFJvb3QgQOEwHhcNMjQx
[truncated]
ADBEAiB7S4YZfnOK82K2yz5F5CzMe2t98LCpLRzoPJXMo7um1AIgH+K8EZMLstLN
AJQoplycJENo5D7kUmVrwUBBjREqv9I=
-----END CERTIFICATE-----
quit

INFO: Certificate has the following attributes:
Fingerprint: 40000000 40000000 40000000 40000000
Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.
```

6. Registre o certificado.

```
asav(config)# crypto ca enroll private_acme
% Start certificate enrollment ..
% The subject name in the certificate will be: CN=fj-asav.cisco.com

% The fully-qualified domain name in the certificate will be: fj-asav.example.com

% Include the device serial number in the subject name? [yes/no]: no

Request certificate from CA? [yes/no]: yes
```

Verificar

Exibir certificado instalado no ASA

Confirme se o certificado está registrado e verifique a data de renovação.

```
asav# show crypto ca certificates private_acme
```

```
CA Certificate
Status: Available
Certificate Serial Number: 79d000000000000000000008b
Certificate Usage: General Purpose
Public Key Type: ECDSA (256 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=ca-acme Root CA
O=ca-acme
Subject Name:
CN=ca-acme Intermediate CA
O=ca-acme
Validity Date:
start date: 23:20:19 UTC Nov 26 2024
end date: 23:20:19 UTC Nov 24 2034
Storage: config
Associated Trustpoints: private_acme
Public Key Hashes:
SHA1 PublicKey hash: 8c8200000000000000000000000000000000000077
SHA1 PublicKeyInfo hash: 974c0000000000000000000000000000000009e1

Certificate
Status: Available
Certificate Serial Number: 666000000000000000000000000000be
Certificate Usage: General Purpose
Public Key Type: RSA (4096 bits)
Signature Algorithm: ecdsa-with-SHA256
Issuer Name:
CN=ca-acme Intermediate CA
O=ca-acme
Subject Name:
CN=fj-asav.example.com
Validity Date:
start date: 20:51:00 UTC Feb 14 2025
end date: 20:52:00 UTC Feb 15 2025
renew date: 16:03:48 UTC Feb 15 2025
Storage: immediate
Associated Trustpoints: private_acme
Public Key Hashes:
SHA1 PublicKey hash: e6e000000000000000000000000000000000089a
SHA1 PublicKeyInfo hash: 5e300000000000000000000000000000000009f
```

Eventos de Syslog

Há novos syslogs no Firewall Seguro para capturar eventos relacionados ao registro de certificado usando o protocolo ACME:

- 717067 : Fornece informações sobre quando começa a inscrição do certificado ACME

```
%ASA-5-717067: Starting ACME certificate enrollment for the trustpoint <private_acme> with CA <ca-acme.
```

- 717068 : Fornece informações sobre quando o registro do certificado ACME é bem-sucedido

```
%ASA-5-717068: ACME Certificate enrollment succeeded for trustpoint <private_acme> with CA <ca-acme.exa
```

- 717069 : Fornece informações sobre quando a inscrição no ACME falha

```
%ASA-3-717069: ACME Certificate enrollment failed for trustpoint <private_acme>
```

- 717070 : Fornece Informações relacionadas ao par de chaves para registro ou renovação de certificado

```
%ASA-5-717070: Keypair <Auto.private_acme> in the trustpoint <private_acme> is regenerated for <manual>
```

Troubleshooting

Se uma inscrição de certificado ACME falhar, considere as próximas etapas para identificar e resolver o problema:

- Verifique a conectividade com o servidor: Confirme se o Secure Firewall tem conectividade de rede com o servidor ACME. Verifique se não há problemas de rede ou regras de firewall bloqueando a comunicação.
- Verifique se o Nome de domínio do firewall seguro pode ser resolvido: Verifique se o nome de domínio configurado no Firewall Seguro pode ser resolvido pelo servidor ACME. Essa verificação é crucial para que o servidor valide a solicitação.
- Confirmar propriedade de domínio: Verifique se todos os nomes de domínio especificados no ponto de confiança pertencem ao Firewall Seguro. Isso garante que o servidor ACME possa validar a propriedade do domínio.

Comandos de solução de problemas

Para obter informações adicionais, colete a saída dos próximos comandos de depuração:

- debug crypto ca acme <1-255>
- debug crypto ca <1-14>

Erros comuns de inscrição no ACME:

Código de erro	Razão	Possível causa ou correção
7	Não é possível conectar ao servidor	O servidor está acessível, mas o serviço ACME não está em execução.
28	Não é possível conectar ao servidor	O servidor não está acessível. Verifique o acesso básico à rede para o servidor ACME.
60	Não é possível validar o certificado do servidor	Certifique-se de que a CA raiz ou do emissor esteja presente em um ponto confiável ou no pool confiável.
124	timeout de processamento ACME	Certifique-se de que todos os FQDNs solicitados resolvam para a interface configurada para autenticação HTTP-01. Verifique se o URL do ACME configurado está correto.

Informações Relacionadas

Para obter assistência adicional, entre em contato com o TAC. É necessário um contrato de suporte válido: Contatos de suporte da Cisco no mundo inteiro.
Você também pode visitar a Cisco VPN Community aqui.

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.