# Autenticação do ASA 8.x Anyconnect com o cartão eID belga

## Contents


Introduction
Prerequisites
Requirements
Componentes Utilizados
Conventions
Informações de Apoio
Configuração local do PC
Sistema operacional
Leitor de cartão
Software de tempo de execução eID
Certificado de autenticação
Instalação do AnyConnect
Requisitos do ASA
Configuração do ASA
Etapa 1. Ative a interface externa
Etapa 2. Configure o nome do domínio, a senha e a hora do sistema
Etapa 3. Ative um servidor DHCP na interface externa.
Etapa 4. Configurar o pool de endereços VPN eID
Etapa 5. Importar o certificado CA raiz belga
Etapa 6. Configurar camada de soquetes segura
Passo 7. Definir a política de grupo padrão
Etapa 8. Definir o mapeamento de certificados
Etapa 9. Adicionar um usuário local
Etapa 10. Reinicie o ASA
Ajuste fino
Configuração de um minuto
Informações Relacionadas


## Introduction

Este documento descreve como configurar a autenticação do ASA 8.x Anyconnect para usar a placa eID belga.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ASA 5505 com o software ASA 8.0 apropriado
- Cliente AnyConnect
- ASDM 6.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

### Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

## Informações de Apoio

O eID é um cartão PKI (Public Key Infrastructure, Infraestrutura de Chave Pública) emitido pelo governo belga que os usuários devem usar para se autenticar em um PC Windows remoto. O cliente de software do AnyConnect está instalado no PC local e recebe credenciais de autenticação do PC remoto. Quando a autenticação é concluída, o usuário remoto obtém acesso aos recursos centrais por meio de um túnel SSL completo. O usuário remoto é provisionado com um endereço IP obtido de um pool gerenciado pelo ASA.

## Configuração local do PC

### Sistema operacional

O sistema operacional (Windows, MacOS, Unix ou Linux) no PC local deve estar atualizado com todos os patches necessários instalados.

### Leitor de cartão

Um leitor de cartão eletrônico deve ser instalado no computador local para que você use a placa eID. O leitor de cartão eletrônico é um dispositivo de hardware que estabelece um canal de comunicação entre os programas no computador e o chip na placa de identificação.

Para obter uma lista de leitores de cartão aprovados, consulte este URL: http://www.cardreaders.be/en/default.htm

**Nota:** Para usar o leitor de cartão, você deve instalar os drivers recomendados pelo fornecedor do hardware.

## Software de tempo de execução eID

Você deve instalar o software de tempo de execução eID fornecido pelo governo belga. Este software permite que o usuário remoto leia, valide e imprima o conteúdo do cartão eID. O software está disponível em francês e holandês para Windows, MAC OS X e Linux.

Para obter mais informações, consulte este URL:

- http://www.belgium.be/zip/eid_datacapture_nl.html

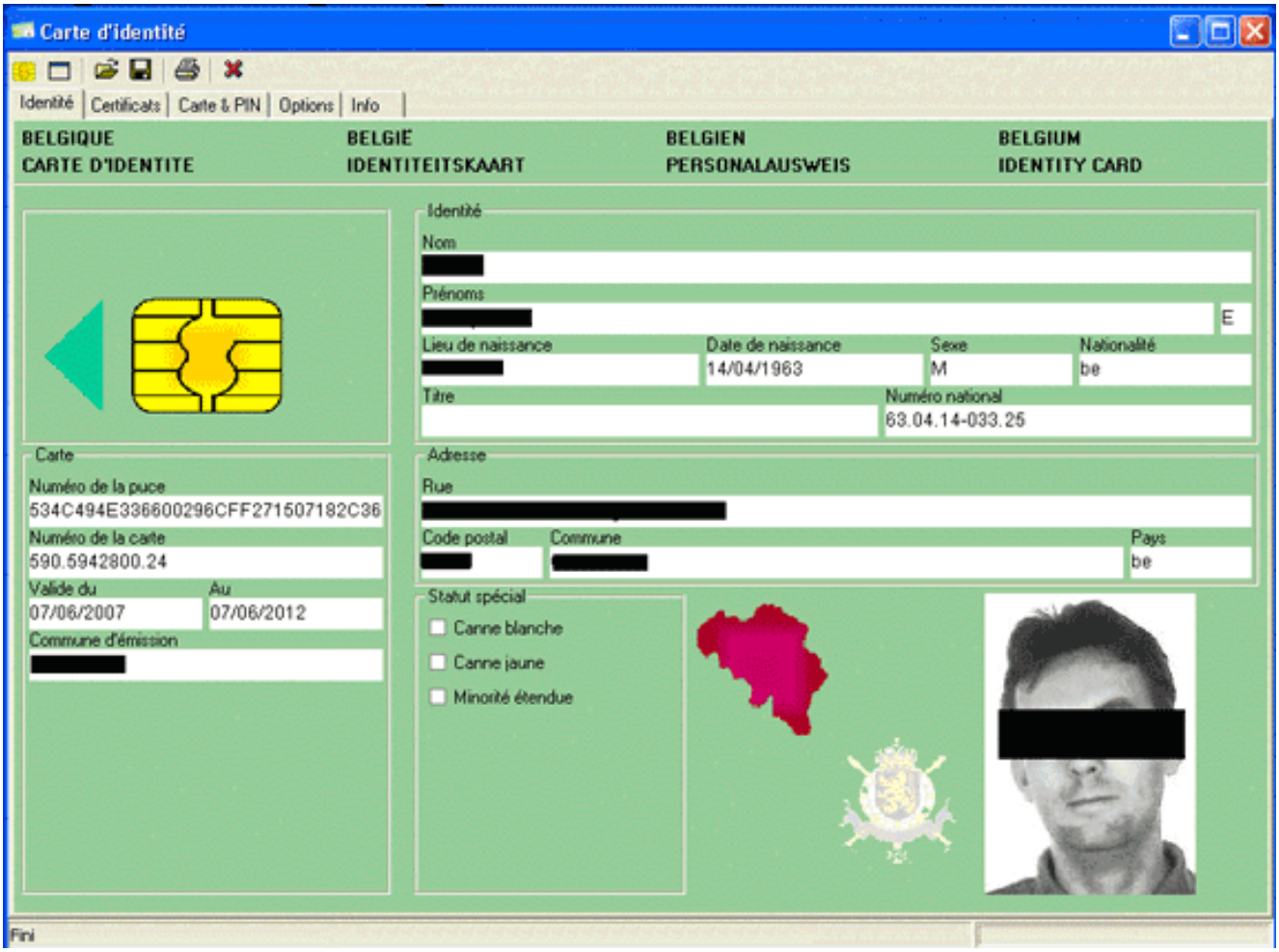
## Certificado de autenticação

Você deve importar o certificado de autenticação para o repositório do Microsoft Windows no PC local. Se você não importar o certificado para o armazenamento, o AnyConnect Client não poderá estabelecer uma conexão SSL com o ASA.

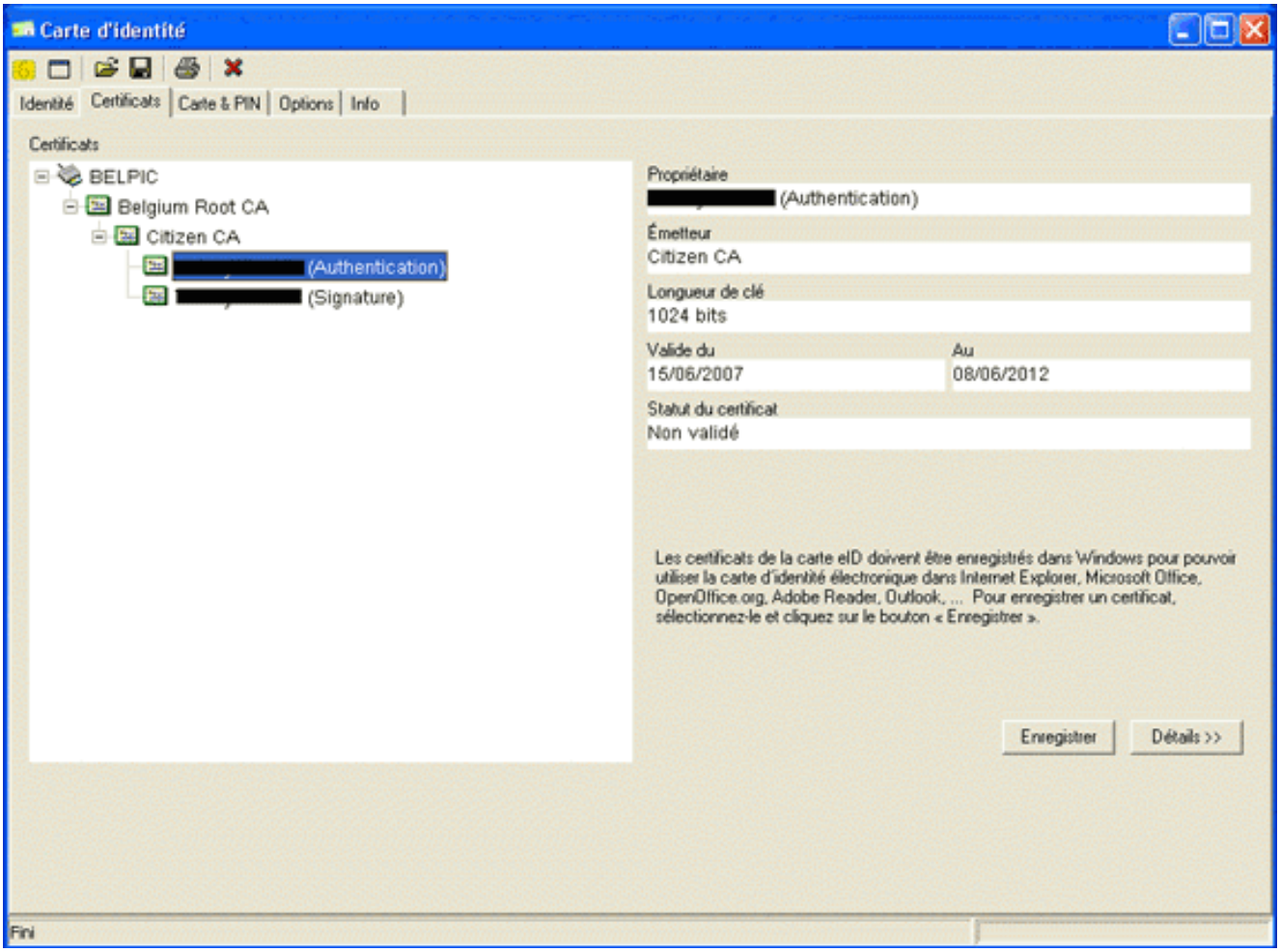
### Procedimento

Para importar o certificado de autenticação para o repositório do Windows, faça o seguinte:

1. Insira seu eID no leitor de cartão e inicie o middleware para acessar o conteúdo da placa eID.O conteúdo do cartão eID é exibido.




2. Clique na guia **Certificats** (FR).A hierarquia de certificados é exibida.




3. Expanda **Bélgica Root CA** e expanda **Citizen CA**.
4. Escolha a versão de **autenticação** do certificado nomeado.
5. Clique no botão **Registrando** (FR).O certificado é copiado no arquivo do Windows.

**Observação:** quando você clica no botão **Detalhes**, uma janela é exibida mostrando detalhes sobre o certificado. Na guia Detalhes, selecione o campo **Assunto** para exibir o campo Número de série. O campo Número de série contém um valor exclusivo que é usado para autorização do usuário. Por exemplo, o número de série "56100307215" representa um usuário cuja data de nascimento é 3 de outubro de 1956 com um número de sequência 072 e um dígito de verificação 15. *Você deve enviar uma solicitação de aprovação das autoridades federais para armazenar esses números. É da vossa responsabilidade fazer as declarações oficiais adequadas relacionadas com a manutenção de uma base de dados de cidadãos belgas no vosso país*.

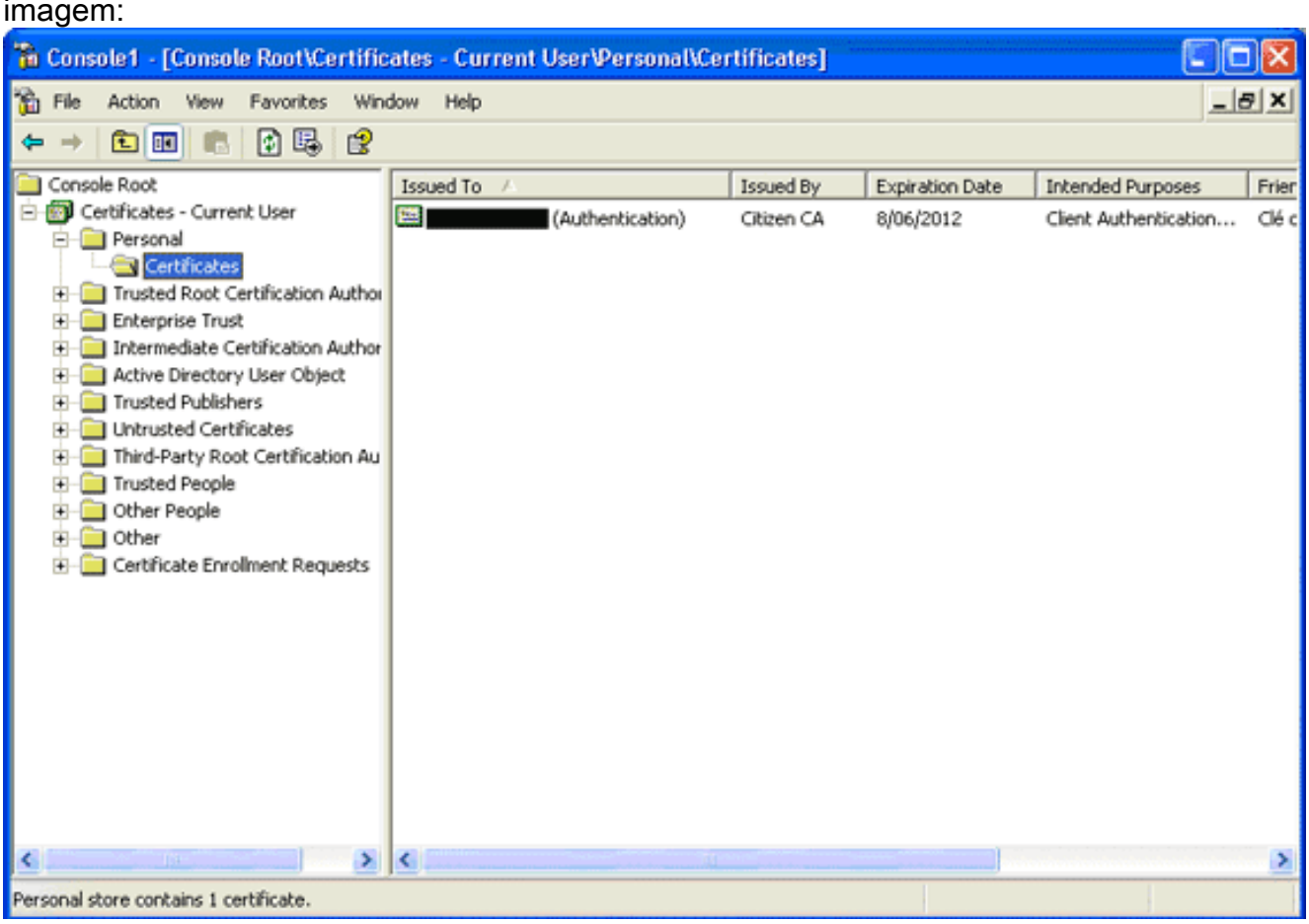
## Verificar

Para verificar se o certificado foi importado com êxito, faça o seguinte:

1. Em uma máquina Windows XP, abra uma janela do DOS e digite o comando **mmc**.O aplicativo Console é exibido.
2. Escolha **File > Add/Remove Snap-in** (ou pressione Ctrl+M).A caixa de diálogo Add/Remove Snap-in é exibida.
3. Clique no botão Adicionar.A caixa de diálogo Add Standalone Snap-in é exibida.
4. Na lista Snap-ins independentes disponíveis, escolha **Certificados** e clique em **Adicionar**.
5. Clique no botão de opção **Minha conta de usuário** e clique em **Concluir**.O snap-in Certificado é exibido na caixa de diálogo Adicionar/remover snap-in.
6. Clique em **Fechar** para fechar a caixa de diálogo Adicionar snap-in autônomo e, em seguida, clique em **OK** na caixa de diálogo Adicionar/remover snap-in para salvar suas alterações e

retornar ao aplicativo de console.

7. Na pasta Raiz do Console, expanda **Certificados - Usuário Atual**.
8. Expanda **Pessoal** e expanda **Certificados**.O certificado importado deve aparecer no repositório do Windows conforme mostrado nesta imagem:




# Instalação do AnyConnect

Você deve instalar o AnyConnect Client no PC remoto. O software AnyConnect usa um arquivo de configuração XML que pode ser editado para predefinir uma lista de gateways disponíveis. O arquivo XML é armazenado neste caminho no PC remoto:

C:\Documents and Settings*%USERNAME%*\Application Data\Cisco\Cisco AnyConnect VPN Client

onde *%USERNAME%* é o nome do usuário no PC remoto.

O nome do arquivo XML é *preference.xml*. Aqui está um exemplo do conteúdo do arquivo:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectPreferences>
<DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences>
```

onde *192.168.0.1* é o endereço IP do gateway ASA.

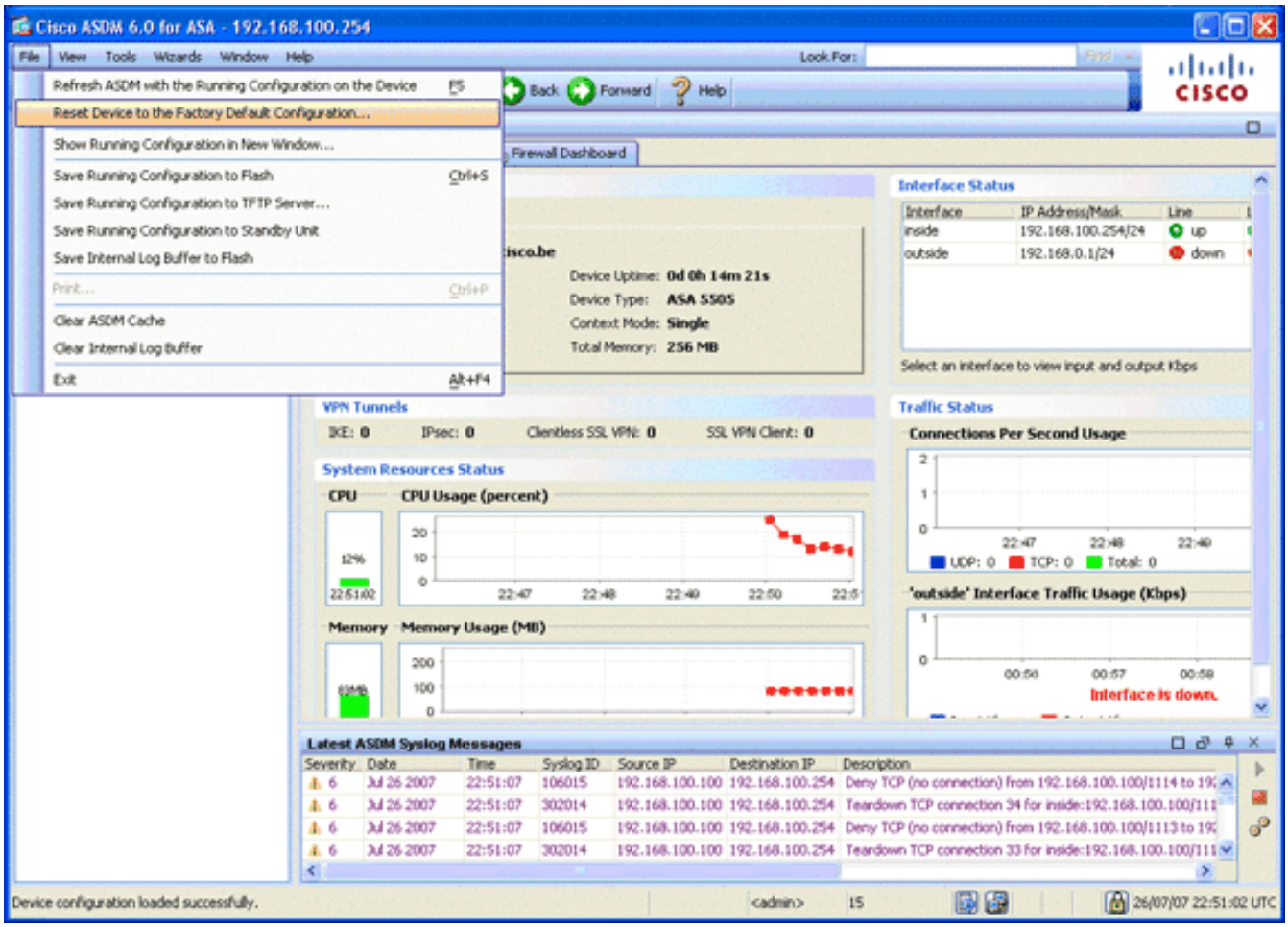
# Requisitos do ASA

Assegure-se de que o ASA atenda a estes requisitos:

- O AnyConnect e o ASDM devem ser executados na memória flash.Para concluir os procedimentos neste documento, use um ASA 5505 com o software ASA 8.0 apropriado instalado. Os aplicativos AnyConnect e ASDM devem ser pré-carregados na memória flash. Use o comando **show flash** para exibir o conteúdo da flash:

```
ciscoasa#show flash:
--#--  --length--  -----date/time------  path
   66  14524416    Jun 26 2007 10:24:02  asa802-k8.bin
   67  6889764     Jun 26 2007 10:25:28  asdm-602.bin
   68  2635734     Jul 09 2007 07:37:06  anyconnect-win-2.0.0343-k9.pkg
```

- O ASA deve ser executado com os padrões de fábrica.Você pode ignorar esse requisito se usar um novo chassi ASA para concluir os procedimentos neste documento. Caso contrário, faça o seguinte para redefinir o ASA para os padrões de fábrica:No aplicativo ASDM, conecte-se ao chassi do ASA e escolha **Arquivo > Redefinir dispositivo para a configuração padrão de fábrica**.




Deixe os valores padrão no modelo.Conecte seu PC à interface interna Ethernet 0/1 e renove seu endereço IP que será provisionado pelo servidor DHCP do ASA.**Observação:** para redefinir o ASA para os padrões de fábrica a partir da linha de comando, use estes comandos:

```
ciscoasa#conf t
ciscoasa#config factory-default 192.168.0.1 255.255.255.0
```

# Configuração do ASA

Depois de redefinir os padrões de fábrica do ASA, você pode iniciar o ASDM para 192.168.0.1

para se conectar ao ASA na interface interna Ethernet 0/1.

**Observação:** sua senha anterior é preservada (ou pode estar em branco por padrão).

Por padrão, o ASA aceita uma sessão de gerenciamento de entrada com um endereço IP de origem na sub-rede 192.168.0.0/24. O servidor DHCP padrão habilitado na interface interna do ASA fornece endereços IP no intervalo 192.168.0.2-129/24, válidos para conexão à interface interna com o ASDM.

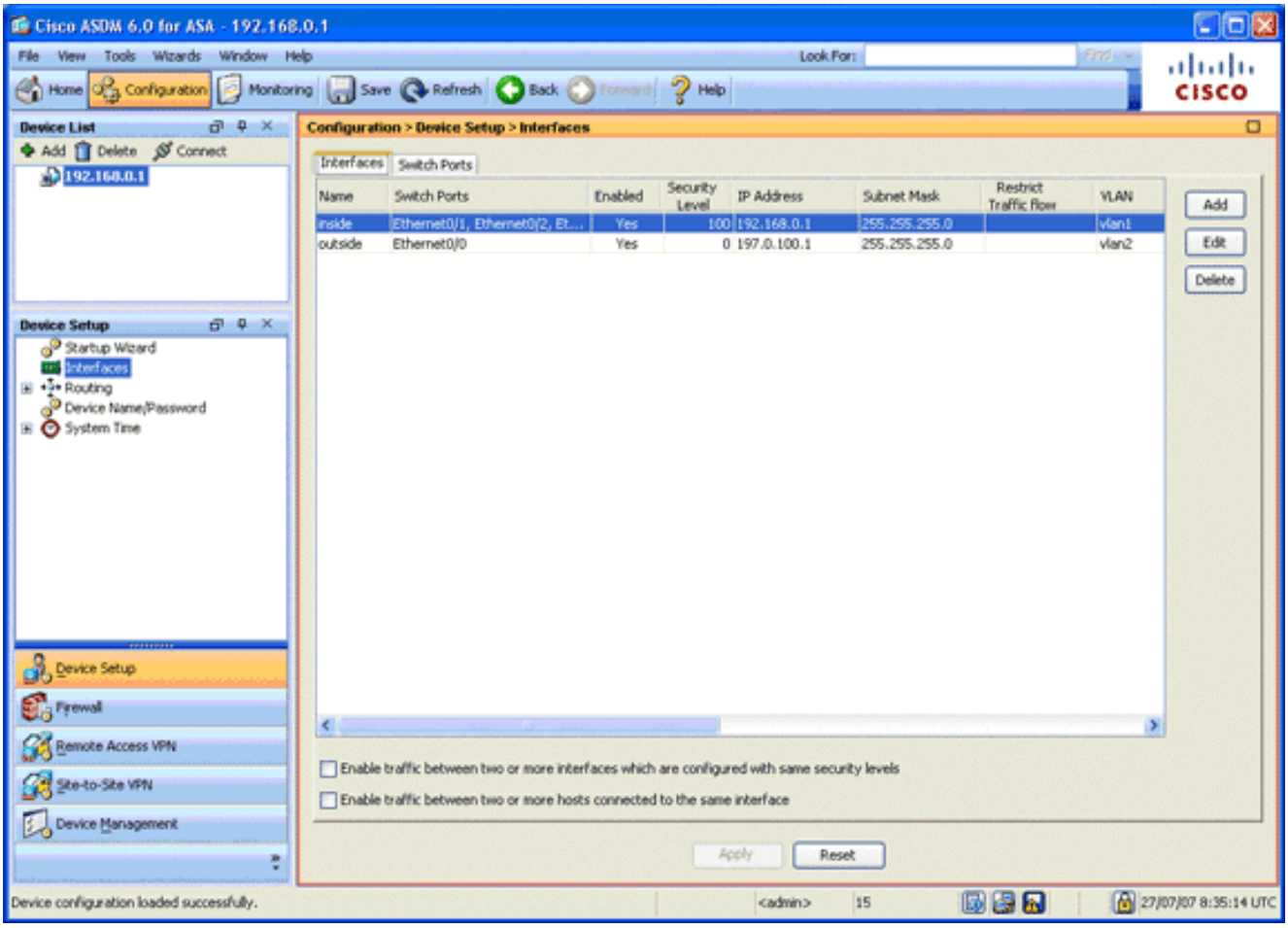
Conclua estes passos para configurar o ASA:

1. Ative a interface externa
2. Configure o nome do domínio, a senha e a hora do sistema
3. Ative um servidor DHCP na interface externa
4. Configurar o pool de endereços VPN eID
5. Importar o certificado CA raiz belga
6. Configurar camada de soquetes segura
7. Definir a política de grupo padrão
8. Definir o mapeamento de certificados
9. Adicionar um usuário local
10. Reinicie o ASA

## Etapa 1. Ative a interface externa

Esta etapa descreve como ativar a interface externa.

1. No aplicativo ASDM, clique em **Configuration** e em **Device Setup**.
2. Na área Device Setup (Configuração do dispositivo), escolha **Interfaces** e clique na guia **Interfaces**.

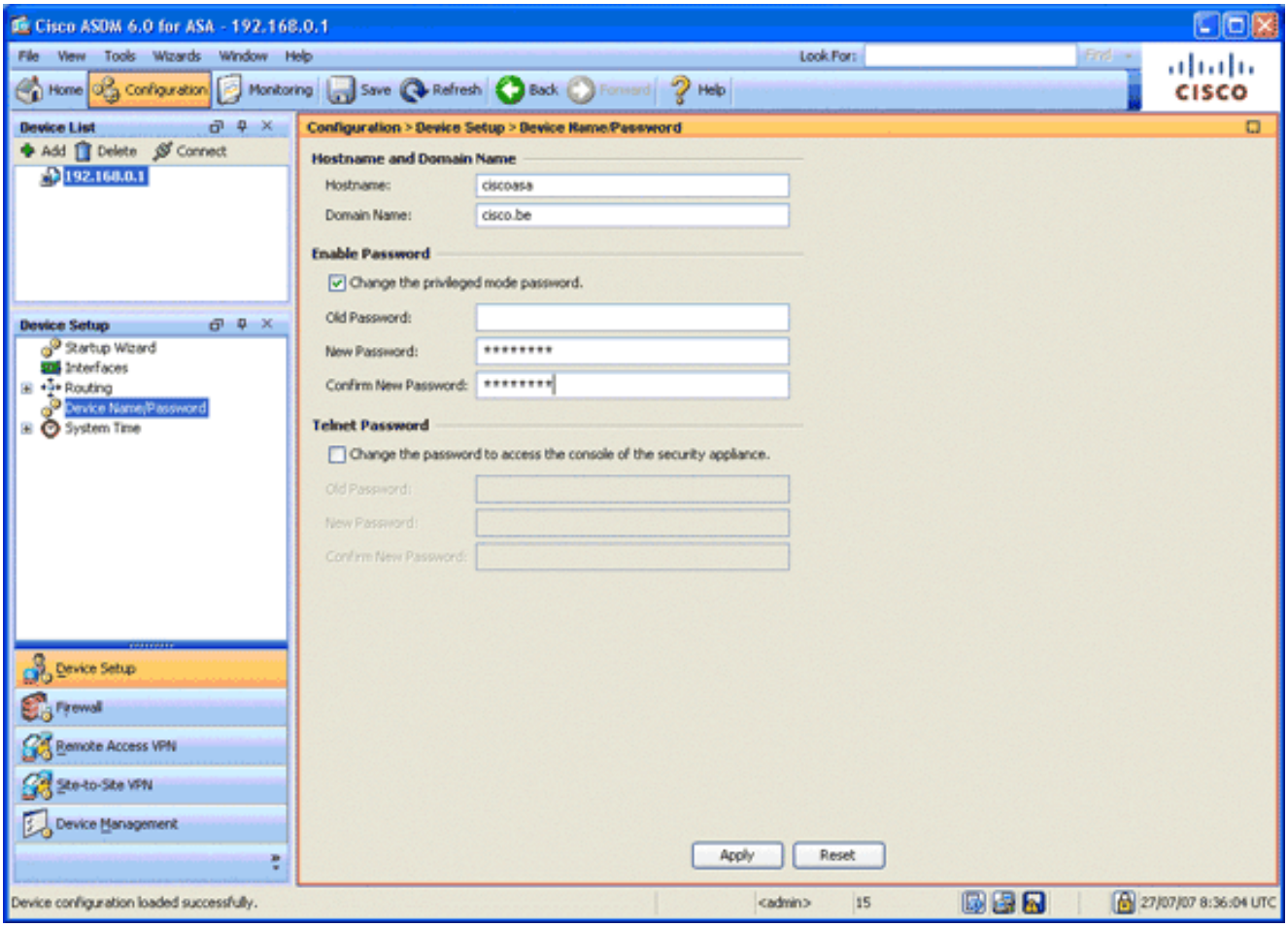



3. Selecione a interface externa e clique em **Editar**.
4. Na seção Endereço IP da guia Geral, escolha a opção **Usar IP estático**.
5. Digite **197.0.100.1** para o endereço IP e **255.255.255.0** para a máscara de sub-rede.
6. Clique em Apply.

## Etapa 2. Configure o nome do domínio, a senha e a hora do sistema

Esta etapa descreve como configurar o nome de domínio, a senha e a hora do sistema.

1. Na área Device Setup (Configuração do dispositivo), escolha **Device Name/Password (Nome do dispositivo/Senha)**.

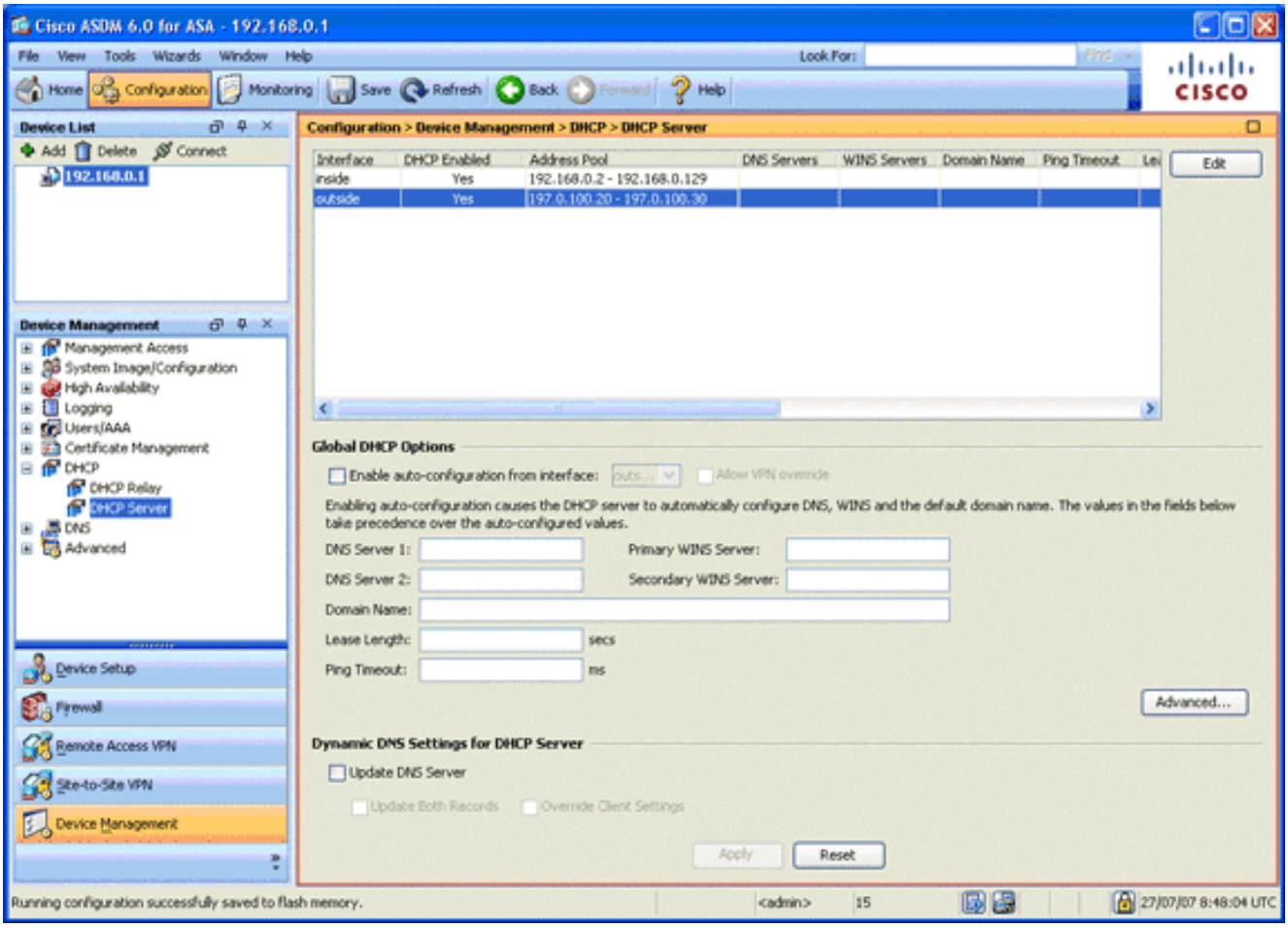



2. Insira **cisco.be** para o nome de domínio e **cisco123** para o valor Enable Password (Habilitar senha).**Observação:** por padrão, a senha está em branco.
3. Clique em Apply.
4. Na área Device Setup (Configuração do dispositivo), escolha **System Time (Hora do sistema**) e altere o valor do relógio (se necessário).
5. Clique em Apply.

## Etapa 3. Ative um servidor DHCP na interface externa.

Esta etapa descreve como ativar um servidor DHCP na interface externa para facilitar o teste.

1. Clique em **Configuração** e, em seguida, clique em **Gerenciamento de dispositivos**.
2. Na área Gerenciamento de dispositivos, expanda **DHCP** e escolha **Servidor DHCP**.

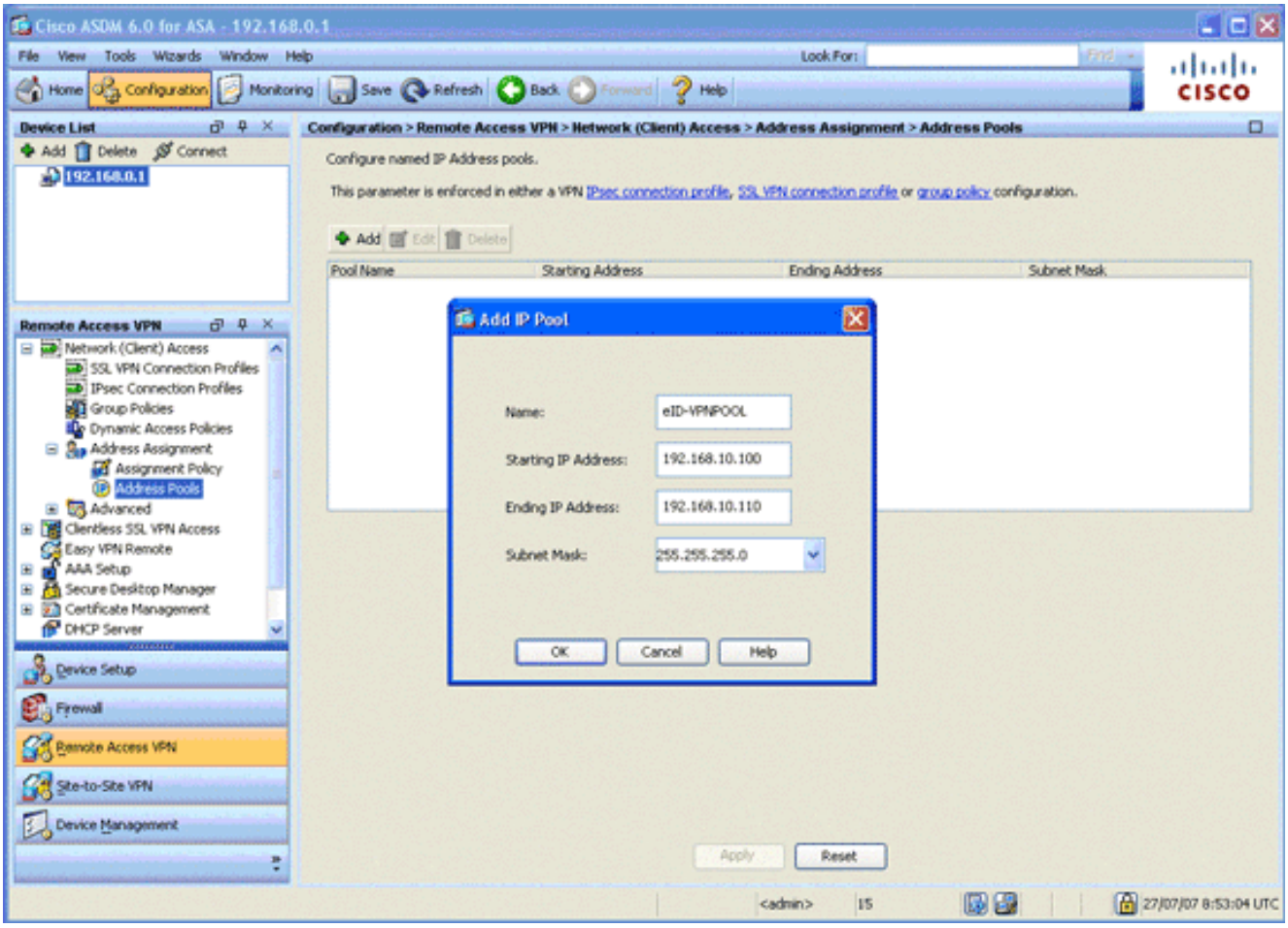



3. Selecione a interface externa na lista Interface e clique em **Editar**.A caixa de diálogo Editar servidor DHCP é exibida.
4. Marque a caixa de seleção **Habilitar servidor DHCP**.
5. No pool de endereços DHCP, insira um endereço IP de 197.0.100.20 a 197.0.100.30.
6. Na área Opções globais de DHCP, desmarque a caixa de seleção **Habilitar configuração automática da interface**.
7. Clique em Apply.

## Etapa 4. Configurar o pool de endereços VPN eID

Esta etapa descreve como definir um pool de endereços IP que são usados para provisionar os clientes AnyConnect remotos.

1. Clique em **Configuration** e, em seguida, clique em **Remote Access VPN**.
2. Na área Remove Access VPN, expanda **Network (Client) Access** e expanda **Address Assignment**.
3. Escolha **Pools de endereços** e clique no botão **Adicionar** localizado na área Configurar pools de endereços IP nomeados.A caixa de diálogo Add IP Pool é exibida.



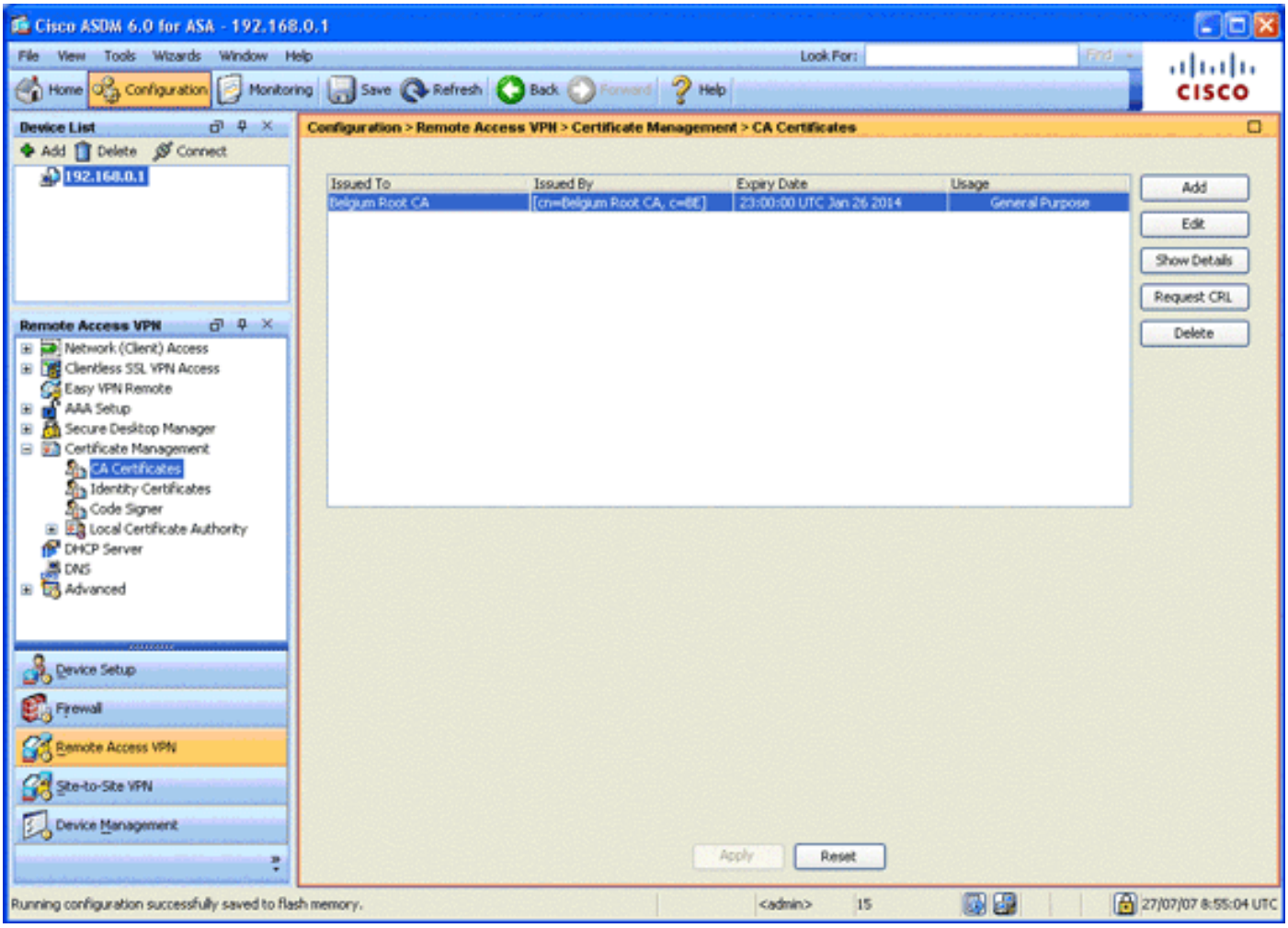

4. No campo Nome, insira **eID-VPNPOOL**.
5. Nos campos Endereço IP inicial e Endereço IP final, insira um intervalo de endereços IP de 192.168.10.100 a 192.168.10.110.
6. Escolha **255.255.255.0** na lista suspensa Máscara de sub-rede, clique em **OK** e clique em **Aplicar**.

## Etapa 5. Importar o certificado CA raiz belga

Esta etapa descreve como importar para o ASA o certificado de CA raiz da Bélgica.

1. Baixe e instale os certificados CA raiz da Bélgica (belgiumrca.crt e belgiumrca2.crt) no site do governo e armazene-os em seu PC local.O sítio Web do Governo belga está localizado no seguinte URL: http://certs.eid.belgium.be/
2. Na área VPN de acesso remoto, expanda **Gerenciamento de certificados** e escolha **Certificados de CA**.
3. Clique em **Adicionar** e, em seguida, clique em **Instalar do arquivo**.
4. Navegue até o local em que você salvou o arquivo do certificado CA raiz belga (belgiumrca.crt) e clique em **Instalar certificado**.
5. Clique em **Aplicar para salvar suas alterações.**

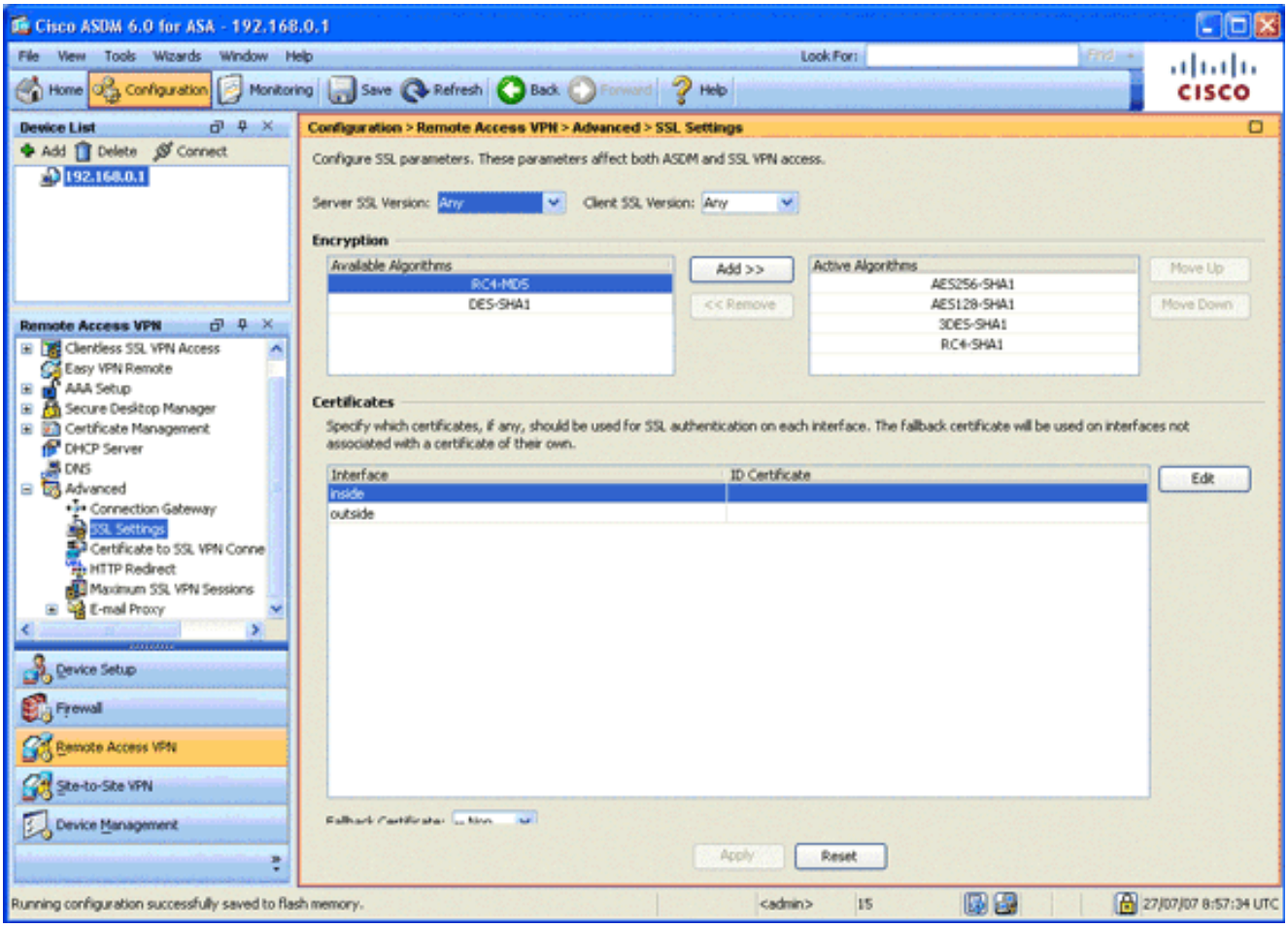
Esta imagem mostra o certificado instalado no ASA:



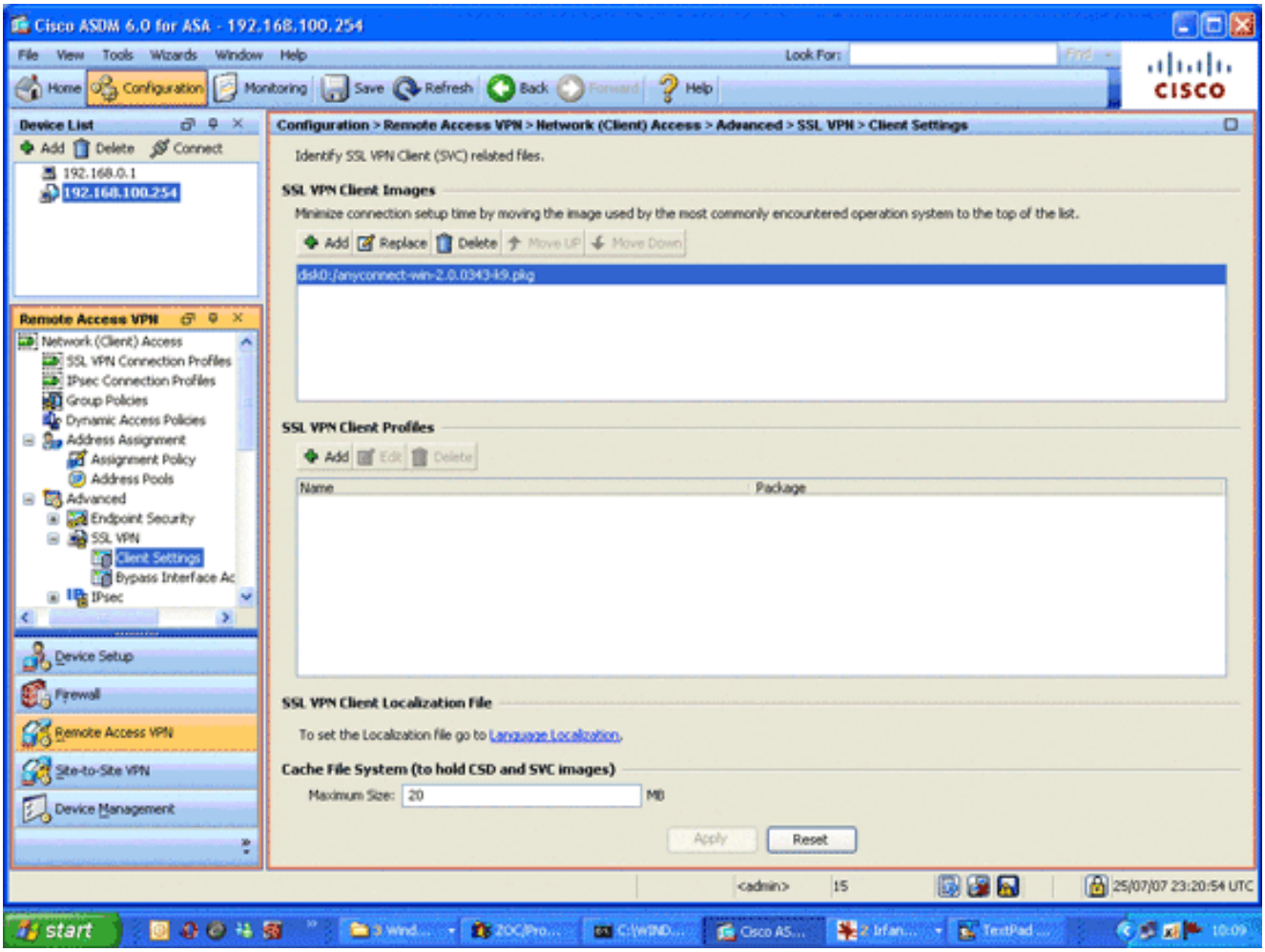

## Etapa 6. Configurar camada de soquetes segura

Esta etapa descreve como priorizar opções de criptografia segura, definir a imagem do cliente VPN SSL e definir o perfil de conexão.

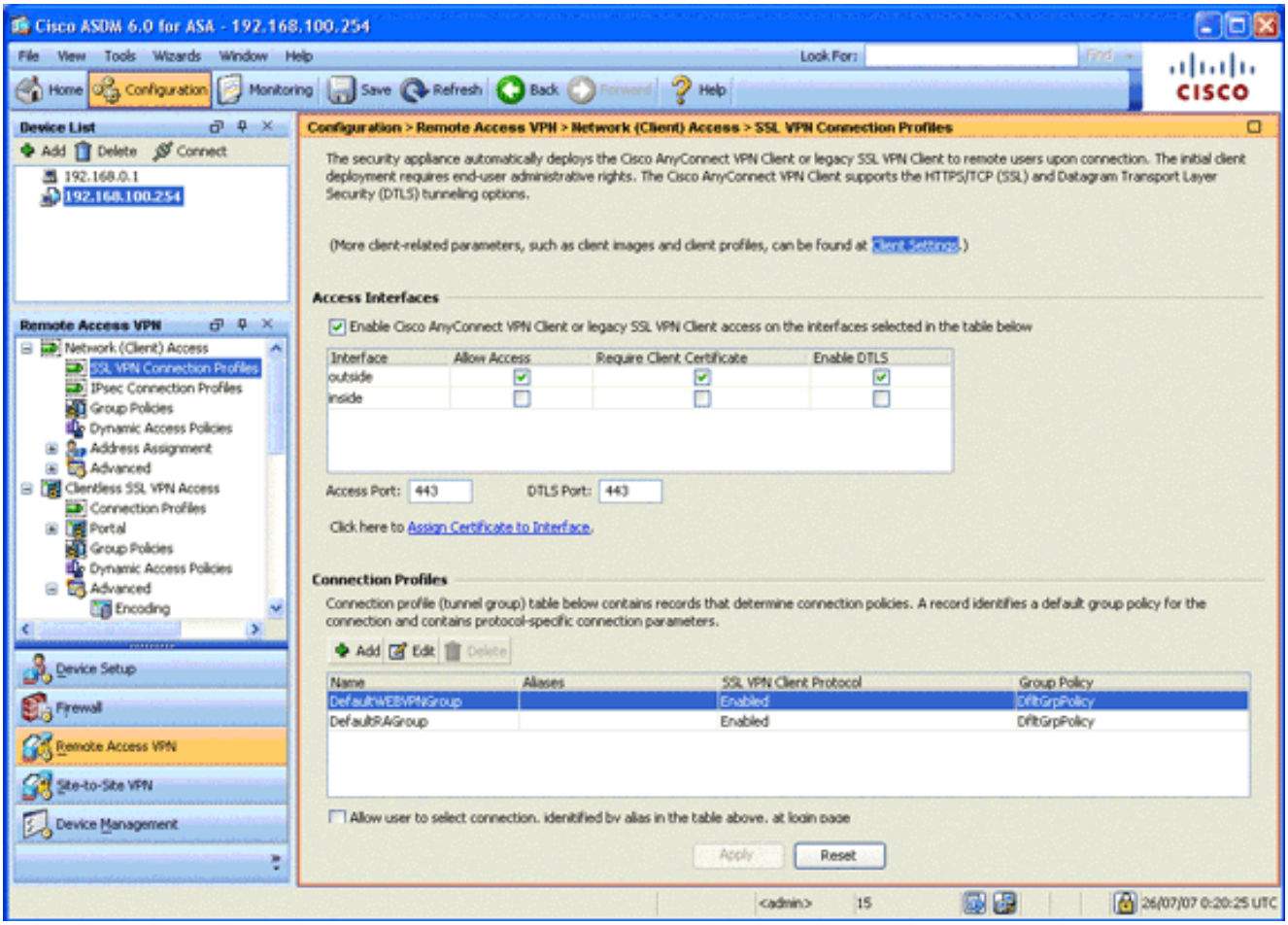
1. Priorize as opções de criptografia mais seguras.Na área VPN de acesso remoto, expanda **Avançado** e escolha **Configurações SSL**. Na seção Criptografia, os algoritmos ativos são empilhados, de cima para baixo, da seguinte forma:AES256-SHA1AES128-SHA13DES-SHA1RC4-
SHA1



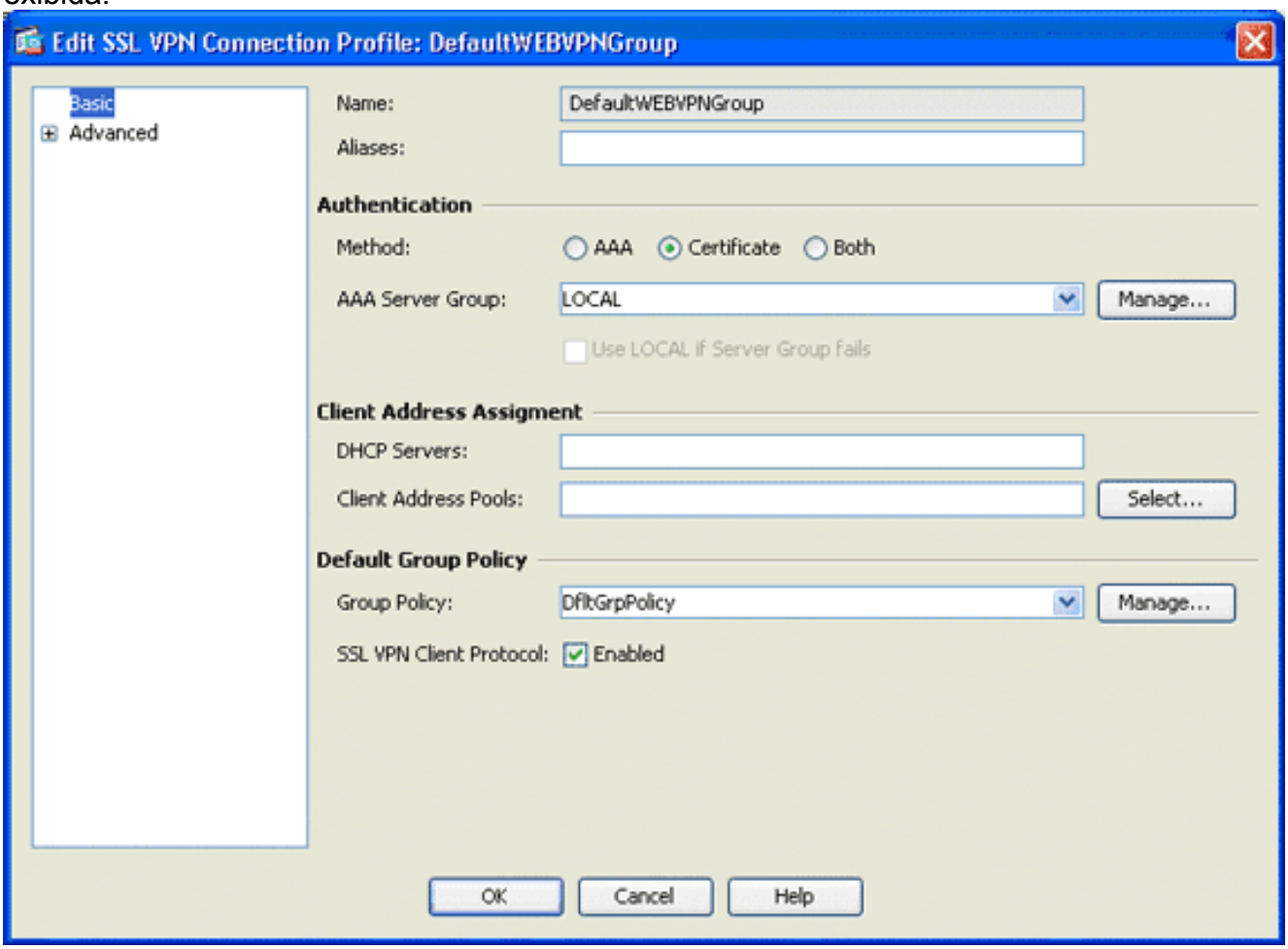

2. Defina a imagem do cliente VPN SSL para o AnyConnect Client.Na área VPN de acesso remoto, expanda **Avançado**, expanda **VPN SSL** e escolha **Configurações do cliente**.Na área SSL VPN Client Images, clique em **Add**.Escolha o pacote do AnyConnect armazenado na flash.O pacote do AnyConnect aparece na lista de Imagens do Cliente VPN SSL como mostrado nesta
imagem:



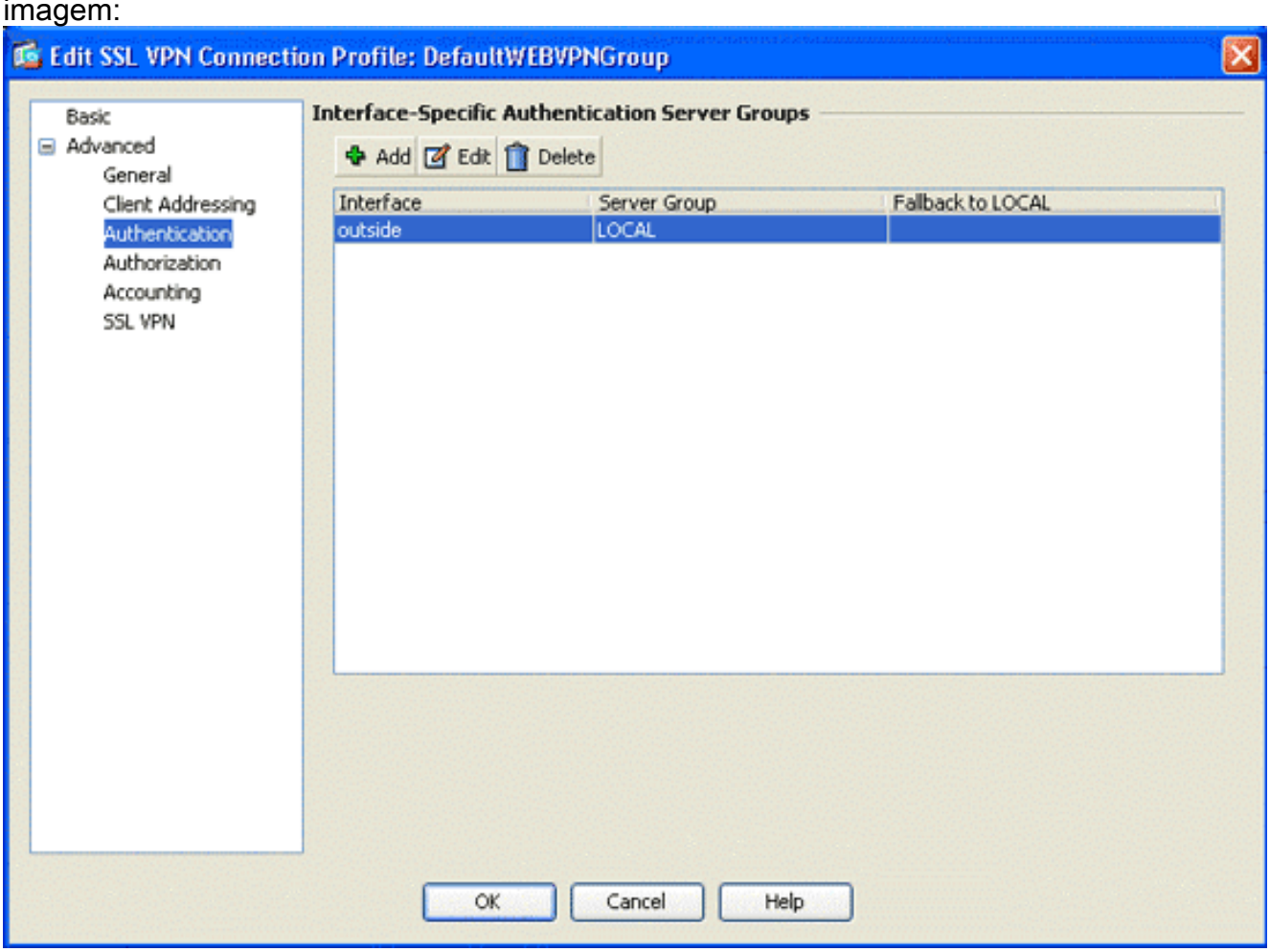

3. Defina o perfil de conexão DefaultWEBVPNGroup.Na área de VPN de acesso remoto, expanda **Acesso de Rede (Cliente)** e escolha **Perfis de Conexão VPN SSL**.Na área Access Interfaces (Interfaces de acesso), marque a **caixa de seleção Enable Cisco AnyConnect VPN Client (Ativar Cisco AnyConnect VPN Client)**.Para a interface externa, marque as caixas de seleção **Allow Access**, **Require Client Certificate** e **Enable DTLS** conforme mostrado nesta
imagem:



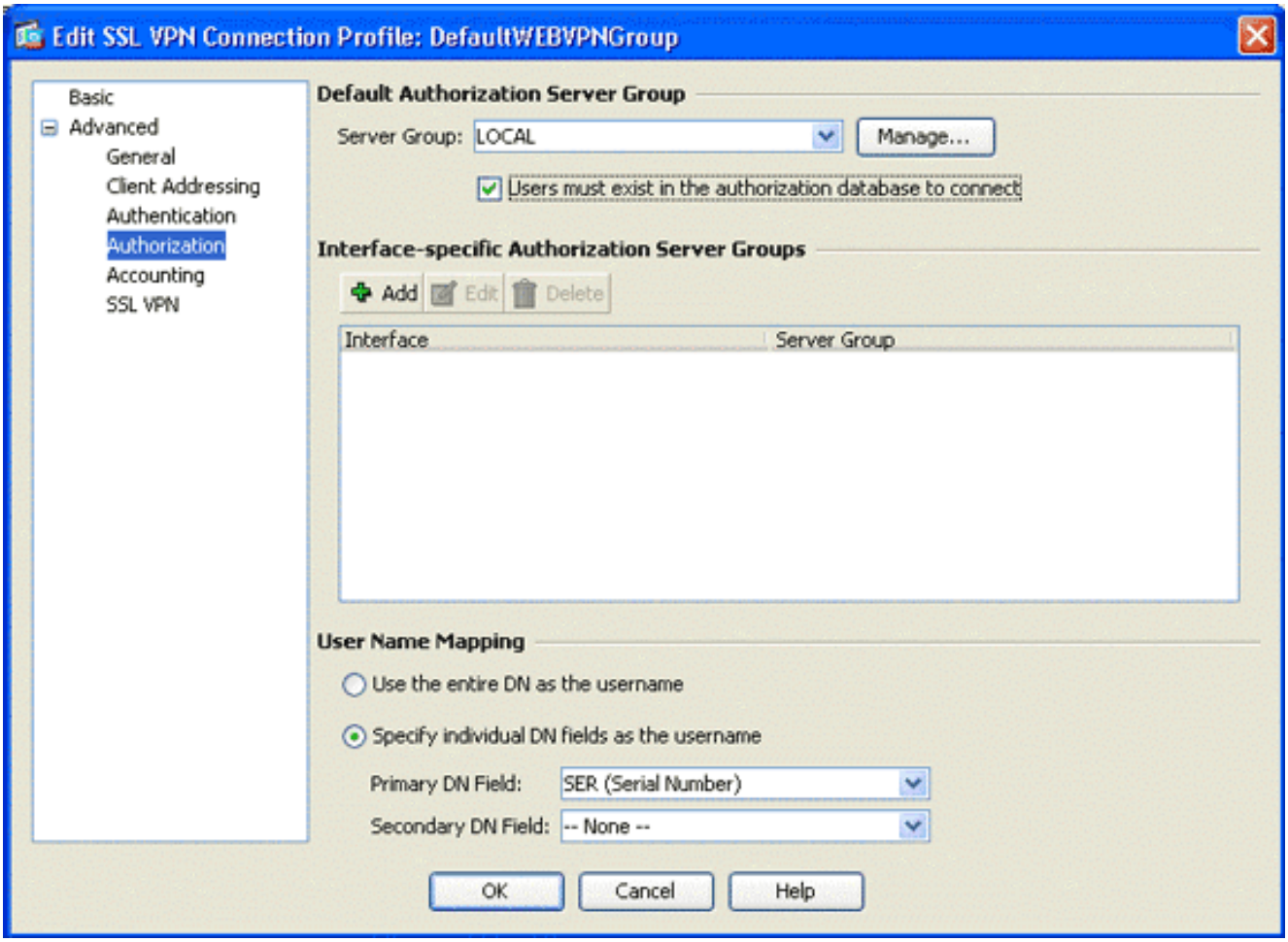

Na área de Perfis de conexão, escolha **DefaultWEBVPNGgroup** e clique em **Edit**.A caixa de diálogo Editar perfil de conexão VPN SSL é exibida.



Na área de navegação, escolha **Basic**.Na área Authentication (Autenticação), clique no botão de opção **Certificate (Certificado)**.Na área Default Group Policy, marque a caixa de seleção **SSL VPN Client Protocol**.Expanda **Avançado** e escolha **Autenticação**.Clique em **Adicionar** e adicione a interface externa a um grupo de servidores local como mostrado nesta
imagem:



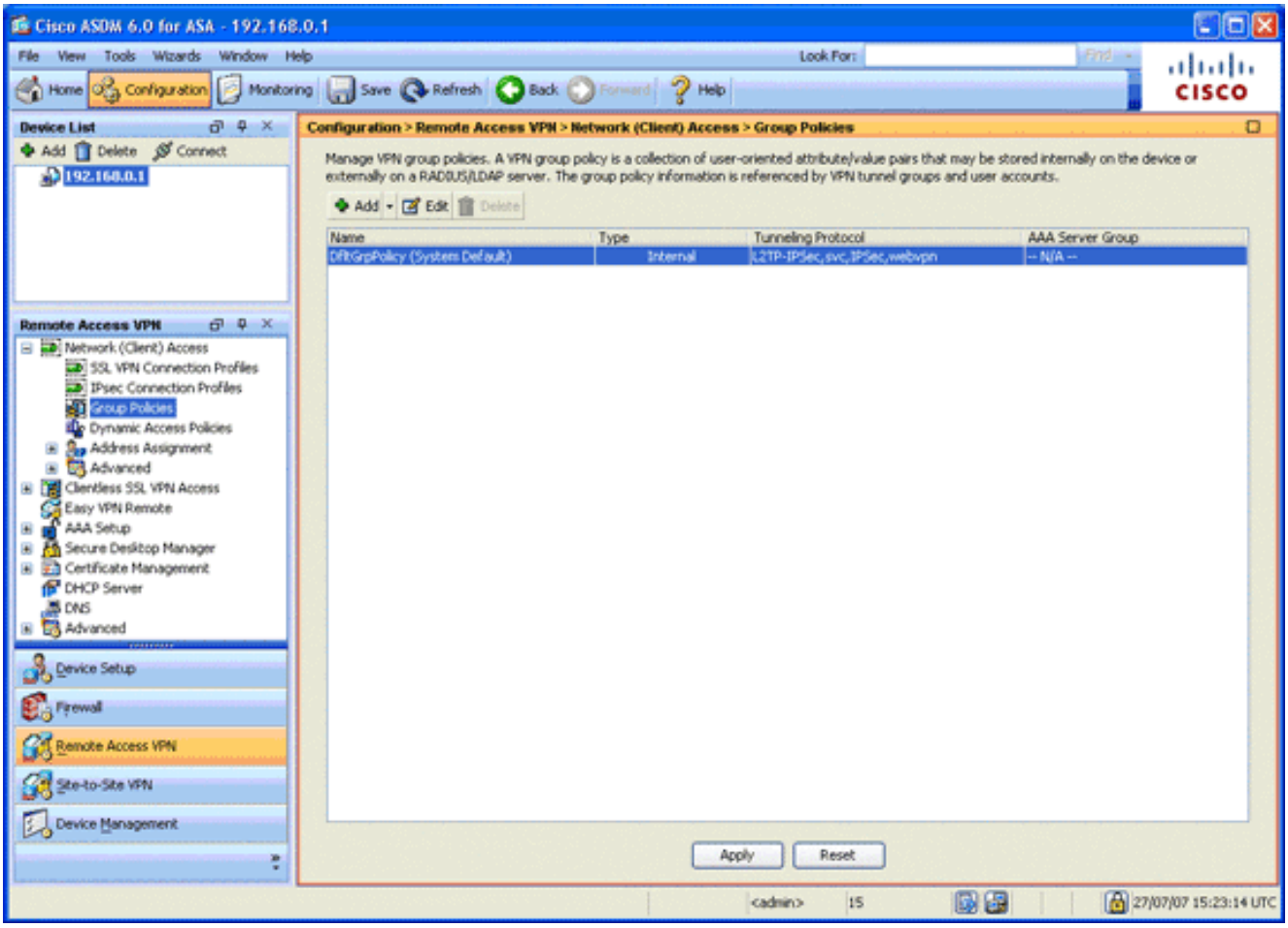

Na área de navegação, escolha **Autorização**.Na área Default Authorization Server Group (Grupo de servidores de autorização padrão), escolha **LOCAL** na lista suspensa Server Group (Grupo de servidores) e marque a caixa de seleção **Users must exist (Usuários devem existir) no banco de dados de autorização para se conectar**.Na área User Name Mapping, escolha **SER (Serial Number)** na lista suspensa Primary DN Field, escolha **None** no Secondary DN Field e clique em
**OK**.



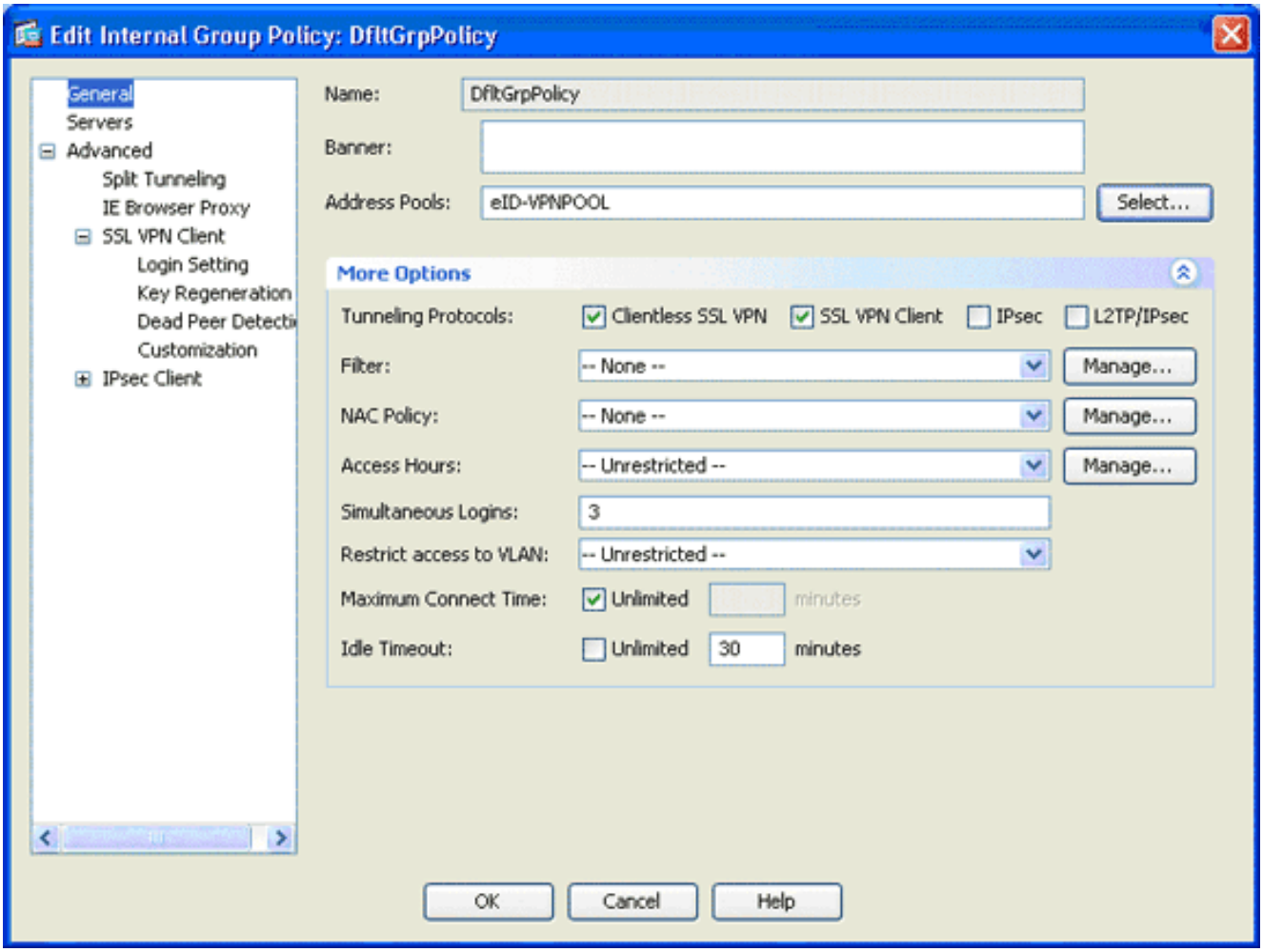

## Passo 7. Definir a política de grupo padrão

Esta etapa descreve como definir a política de grupo padrão.

1. Na área de VPN de acesso remoto, expanda **Acesso de Rede (Cliente)** e escolha **Políticas de Grupo**.




2. Escolha **DfltGrpPolicy** na lista de políticas de grupo e clique em **Edit**.
3. A caixa de diálogo Editar política de grupo interno é exibida.

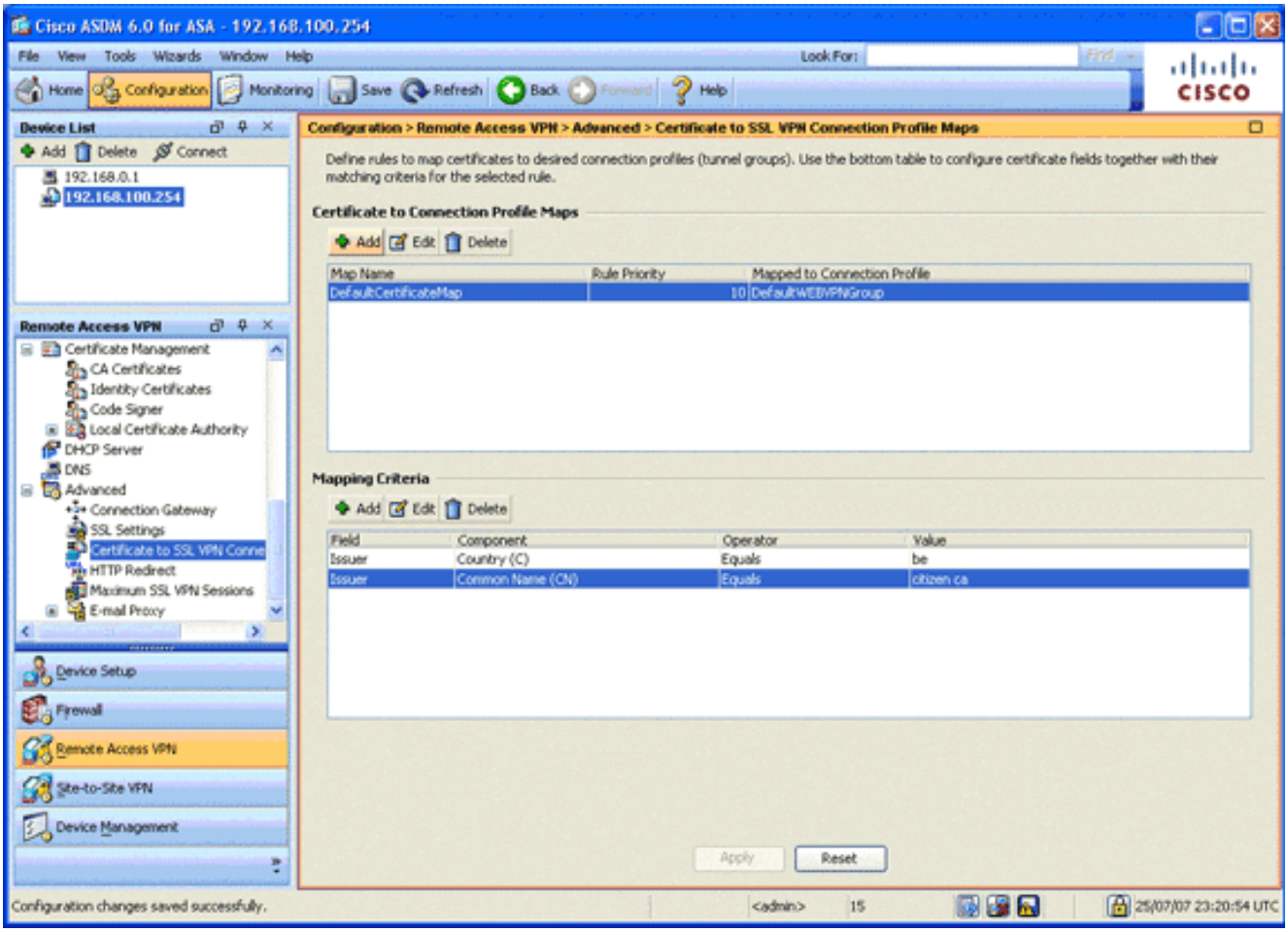



4. Na área de navegação, escolha **Geral**.
5. Para Pools de endereços, clique em **Select** para escolher um pool de endereços e escolha **eID-VPNPOOL**.
6. Na área More Options (Mais opções), desmarque as caixas de seleção **IPsec** e **L2TP/IPsec** e clique em **OK**.

## Etapa 8. Definir o mapeamento de certificados

Esta etapa descreve como definir os critérios de mapeamento de certificado.

1. Na área de VPN de acesso remoto, clique em **Avançado** e escolha **Mapas de perfil de conexão de VPN de certificado para SSL**.
2. Na área "Certificate to Connection Profile Maps", clique em **Add** e escolha **DefaultCertificateMap** na lista de mapas.Este mapa deve corresponder ao *perfil DefaultWEBVPNProfile* no campo Mapped to Connection Profile.
3. Na área Critérios de mapeamento, clique em **Adicionar** e adicione estes valores:Campo: Emitente, País (C), Igual a "be"Campo: Emitente, Nome Comum (CN), Iguais, "Cidadão"Os critérios de mapeamento devem aparecer como mostrado nesta imagem:

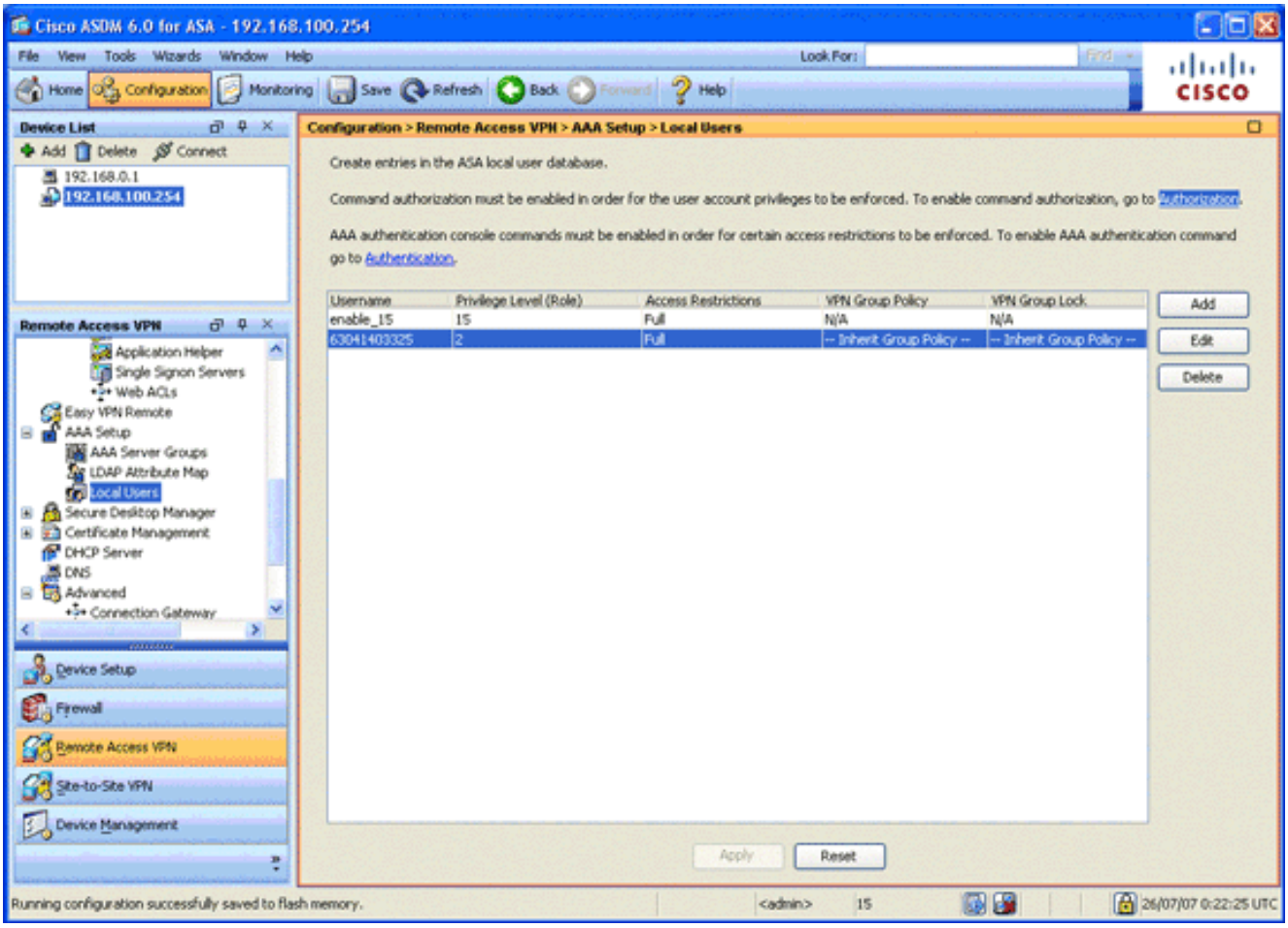



4. Clique em Apply.

## Etapa 9. Adicionar um usuário local

Esta etapa descreve como adicionar um usuário local.

1. Na área VPN de acesso remoto, expanda **Configuração de AAA** e escolha **Usuários locais**.
2. Na área Usuários locais, clique em **Adicionar**.
3. No campo Nome de usuário, insira o número de série do certificado de usuário. Por exemplo, 56100307215 (conforme descrito na seção Certificado de Autenticação deste documento).




4. Clique em Apply.

## Etapa 10. Reinicie o ASA

Reinicie o ASA para garantir que todas as alterações sejam aplicadas aos serviços do sistema.

# Ajuste fino

Durante o teste, alguns túneis SSL podem não ser fechados corretamente. Como o ASA assume que o AnyConnect Client pode se desconectar e reconectar, o túnel não é descartado, o que lhe dá a chance de voltar. Entretanto, durante os testes de laboratório com uma licença básica (2 túneis SSL por padrão), você pode esgotar sua licença quando os túneis SSL não forem fechados corretamente. Se esse problema ocorrer, use o comando **vpn-sessiondb logoff <*option*>** para fazer logoff de todas as sessões SSL ativas.

# Configuração de um minuto

Para criar rapidamente uma configuração funcional, redefina seu ASA para o padrão de fábrica e cole esta configuração no modo de configuração:

| ciscoasa |
| --- |
| `ciscoasa#conf t`<br>`ciscoasa#clear configure all`<br>`ciscoasa#domain-name cisco.be`<br>`ciscoasa#enable password 9jNfZuG3TC5tCVH0 encrypted` |

```
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
interface Vlan2
 nameif outside
 security-level 0
 ip address 197.0.100.1 255.255.255.0
interface Ethernet0/0
 switchport access vlan 2
 no shutdown
interface Ethernet0/1
 no shutdown
!
passwd 2KFQnbNIdI.2KYOU encrypted
dns server-group DefaultDNS
 domain-name cisco.be
ip local pool eID-VPNPOOL 192.168.10.100-192.168.10.110
mask 255.255.255.0
asdm image disk0:/asdm-602.bin
no asdm history enable
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.255.0 inside
crypto ca trustpoint ASDM_TrustPoint0
 enrollment terminal
 crl configure
crypto ca certificate map DefaultCertificateMap 10
 issuer-name attr c eq be
 issuer-name attr cn eq citizen ca
crypto ca certificate chain ASDM_TrustPoint0
 certificate ca 580b056c5324dbb25057185ff9e5a650
    30820394 3082027c a0030201 02021058 0b056c53
24dbb250 57185ff9 e5a65030
    0d06092a 864886f7 0d010105 05003027 310b3009
06035504 06130242 45311830
    16060355 0403130f 42656c67 69756d20 526f6f74
20434130 1e170d30 33303132
    36323330 3030305a 170d3134 30313236 32333030
30305a30 27310b30 09060355
    04061302 42453118 30160603 55040313 0f42656c
6769756d 20526f6f 74204341
    30820122 300d0609 2a864886 f70d0101 01050003
82010f00 3082010a 02820101
    00c8a171 e91c4642 7978716f 9daea9a8 ab28b74d
c720eb30 915a75f5 e2d2cfc8
    4c149842 58adc711 c540406a 5af97412 2787e99c
e5714e22 2cd11218 aa305ea2
    21b9d9bb fff674eb 3101e73b 7e580f91 164d7689
a8014fad 226670fa 4b1d95c1
    3058eabc d965d89a b488eb49 4652dfd2 531576cb
145d1949 b16f6ad3 d3fdbcc2
    2dec453f 093f58be fcd4ef00 8c813572 bff718ea
96627d2b 287f156c 63d2caca
    7d05acc8 6d076d32 be68b805 40ae5498 563e66f1
30e8efc4 ab935e07 de328f12
    74aa5b34 2354c0ea 6ccefe36 92a80917 eaa12dcf
6ce3841d de872e33 0b3c74e2
    21503895 2e5ce0e5 c631f9db 40fa6aa1 a48a939b
a7210687 1d27d3c4 a1c94cb0
    6f020301 0001a381 bb3081b8 300e0603 551d0f01
```

```
01ff0404 03020106 300f0603
    551d1301 01ff0405 30030101 ff304206 03551d20
043b3039 30370605 60380101
    01302e30 2c06082b 06010505 07020116 20687474
703a2f2f 7265706f 7369746f
    72792e65 69642e62 656c6769 756d2e62 65301d06
03551d0e 04160414 10f00c56
    9b61ea57 3ab63597 6d9fddb9 148edbe6 30110609
60864801 86f84201 01040403
    02000730 1f060355 1d230418 30168014 10f00c56
9b61ea57 3ab63597 6d9fddb9
    148edbe6 300d0609 2a864886 f70d0101 05050003
82010100 c86d2251 8a61f80f
    966ed520 b281f8c6 dca31600 dacd6ae7 6b2afa59
48a74c49 37d773a1 6a01655e
    32bde797 d3d02e3c 73d38c7b 83efd642 c13fa8a9
5d0f37ba 76d240bd cc2d3fd3
    4441499c fd5b29f4 0223225b 711bbf58 d9284e2d
45f4dae7 b5634544 110d2a7f
    337f3649 b4ce6ea9 0231ae5c fdc889bf 427bd7f1
60f2d787 f6572e7a 7e6a1380
    1ddce3d0 631e3d71 31b160d4 9e08caab f094c748
755481f3 1bad779c e8b28fdb
    83ac8f34 6be8bfc3 d9f543c3 6455eb1a bd368636
ba218c97 1a21d4ea 2d3bacba
    eca71dab beb94a9b 352f1c5c 1d51a71f 54ed1297
fff26e87 7d46c974 d6efeb3d
    7de6596e 069404e4 a2558738 286a225e e2be7412
b004432a
  quit
no crypto isakmp nat-traversal
!
dhcpd address 192.168.0.2-192.168.0.129 inside
dhcpd enable inside
dhcpd address 197.0.100.20-197.0.100.30 outside
dhcpd enable outside
!
service-policy global_policy global
ssl encryption aes256-sha1 aes128-sha1 3des-sha1 rc4-
sha1
ssl certificate-authentication interface outside port
443
webvpn
 enable outside
 svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
 svc enable
certificate-group-map DefaultCertificateMap 10
DefaultWEBVPNGroup
group-policy DfltGrpPolicy attributes
 vpn-tunnel-protocol svc webvpn
 address-pools value eID-VPNPOOL
username 63041403325 nopassword
tunnel-group DefaultWEBVPNGroup general-attributes
 authentication-server-group (outside) LOCAL
 authorization-server-group LOCAL
 authorization-required
 authorization-dn-attributes SER
tunnel-group DefaultWEBVPNGroup webvpn-attributes
 authentication certificate
exit
copy run start
```

# Informações Relacionadas

- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems