# 与比利时eID卡的ASA 8.x Anyconnect认证

## 目录


简介
先决条件
要求
使用的组件
规则
背景信息
本地PC设置
操作系统
读卡器
eID运行时软件
身份验证证书
AnyConnect安装
ASA要求
ASA 配置
步骤1.启用外部接口
步骤2.配置域名、口令和系统时间
步骤3.在外部接口上启用DHCP服务器。
步骤4.配置eID VPN地址池
步骤5.导入比利时根CA证书
步骤6.配置安全套接字层
步骤7.定义默认组策略
步骤8.定义证书映射
步骤9.添加本地用户
步骤10.重新启动ASA
微调
一分钟配置
相关信息


## 简介

本文档介绍如何设置ASA 8.x Anyconnect身份验证以使用比利时eID卡。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA 5505，带适当的ASA 8.0软件
- AnyConnect Client
- ASDM 6.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

## 背景信息

eID是比利时政府颁发的PKI（公钥基础设施）卡，用户必须使用该卡才能在远程Windows PC上进行身份验证。AnyConnect软件客户端安装在本地PC上，并从远程PC获取身份验证凭证。身份验证完成后，远程用户通过完整SSL隧道获得对中央资源的访问权。为远程用户调配从ASA管理的池获取的IP地址。

## 本地PC设置

### 操作系统

本地PC上的操作系统（Windows、MacOS、Unix或Linux）必须是最新的，且必须安装所有必需的修补程序。

### 读卡器

必须在本地计算机上安装电子读卡器才能使用eID卡。电子读卡器是一种硬件设备，它在计算机上的程序和ID卡上的芯片之间建立通信通道。

有关已批准读卡器的列表，请参阅以下URL:http://www.cardreaders.be/en/default.htm

**注意：**要使用读卡器，必须安装硬件供应商推荐的驱动程序。

### eID运行时软件

必须安装比利时政府提供的eID运行时软件。此软件允许远程用户读取、验证和打印eID卡的内容。该软件以法语和荷兰语提供，适用于Windows、MAC OS X和Linux。

有关详细信息，请参阅此URL:

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

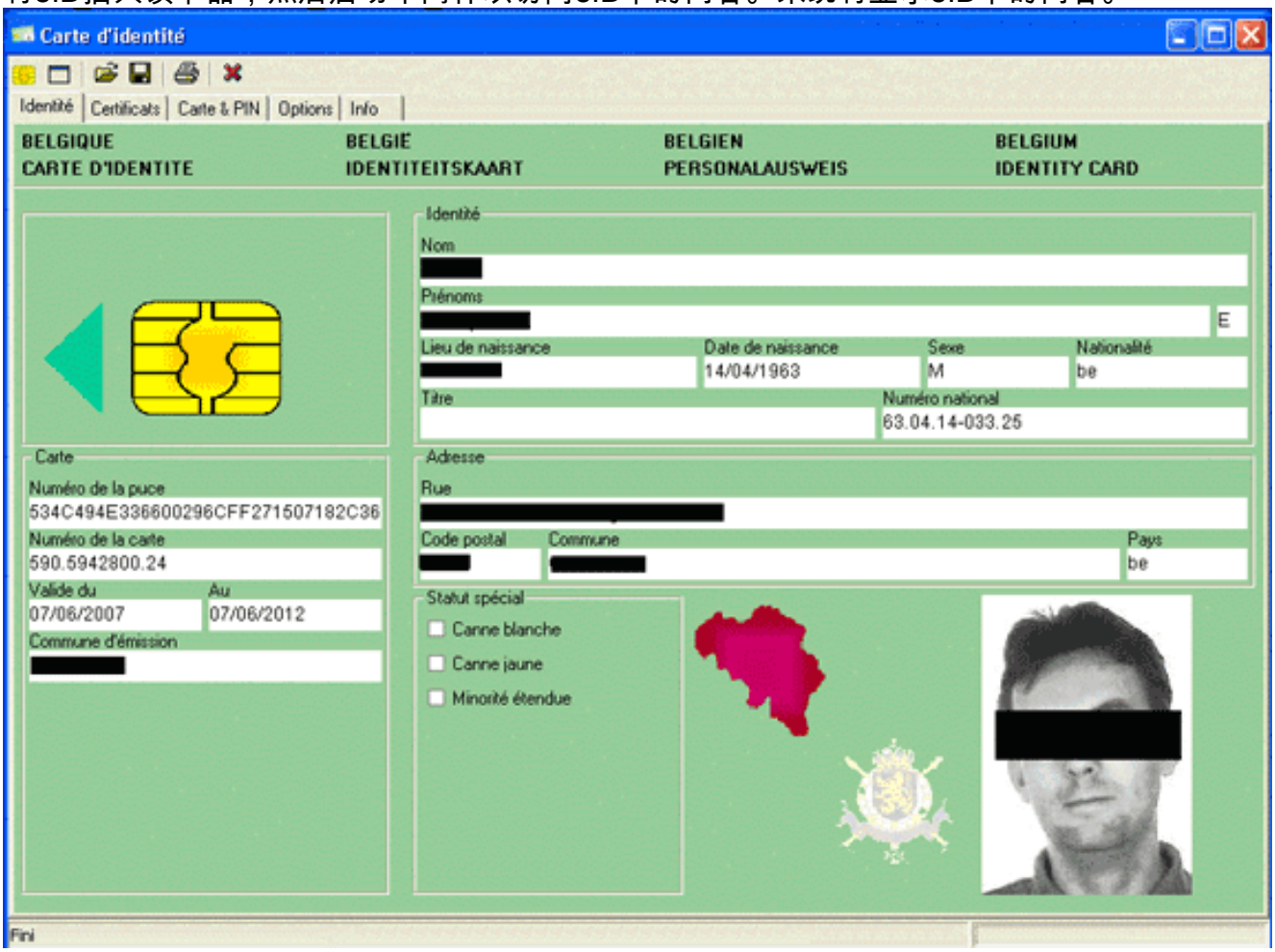
### 身份验证证书

您必须将身份验证证书导入本地PC上的Microsoft Windows存储区。如果无法将证书导入存储，AnyConnect客户端将无法建立到ASA的SSL连接。

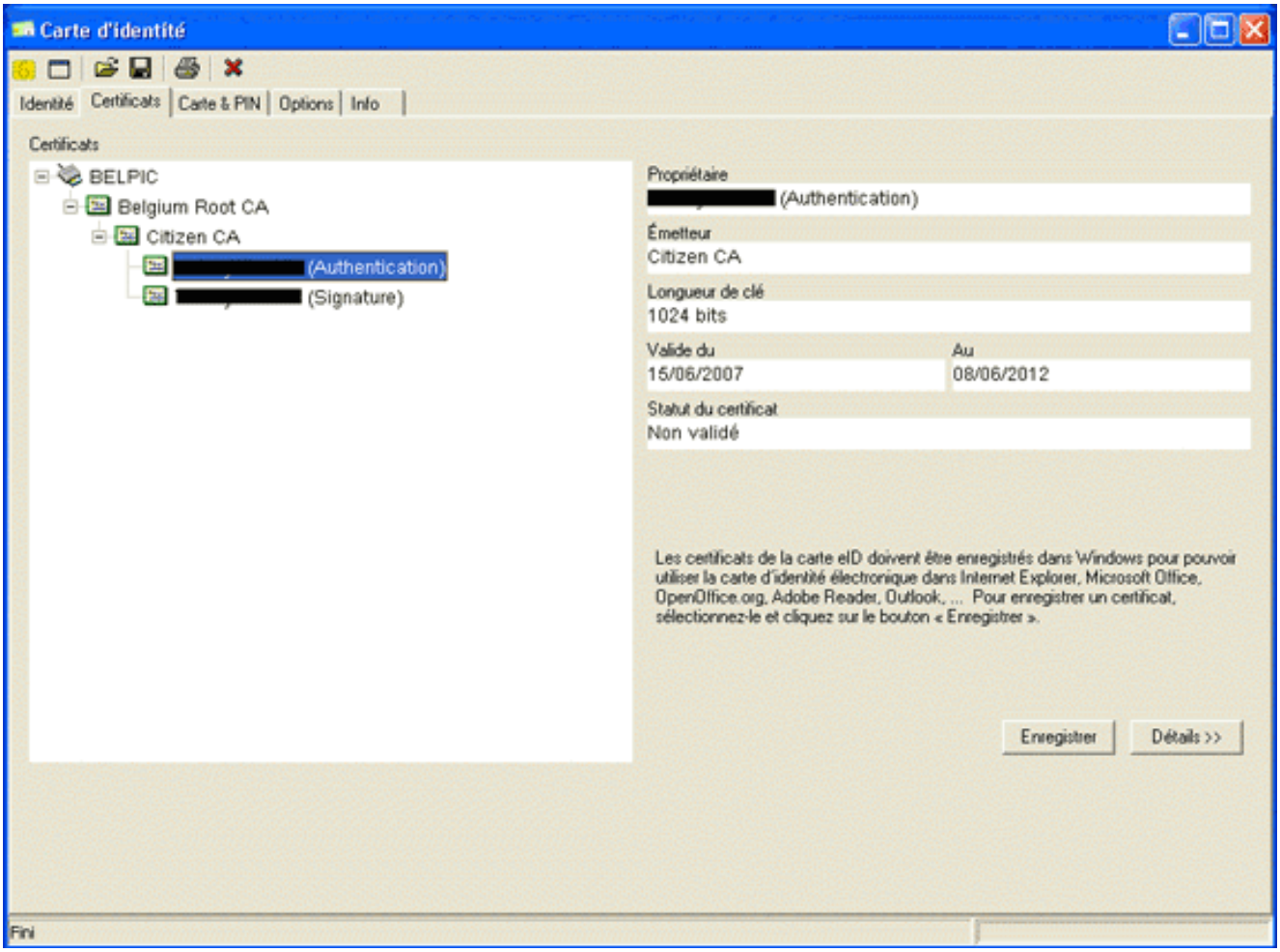
**步骤**

要将身份验证证书导入Windows存储，请完成以下步骤：

1. 将eID插入读卡器，然后启动中间件以访问eID卡的内容。系统将显示eID卡的内容。




2. 单击**Certificates**(FR)选项卡。系统将显示证书层次结构。



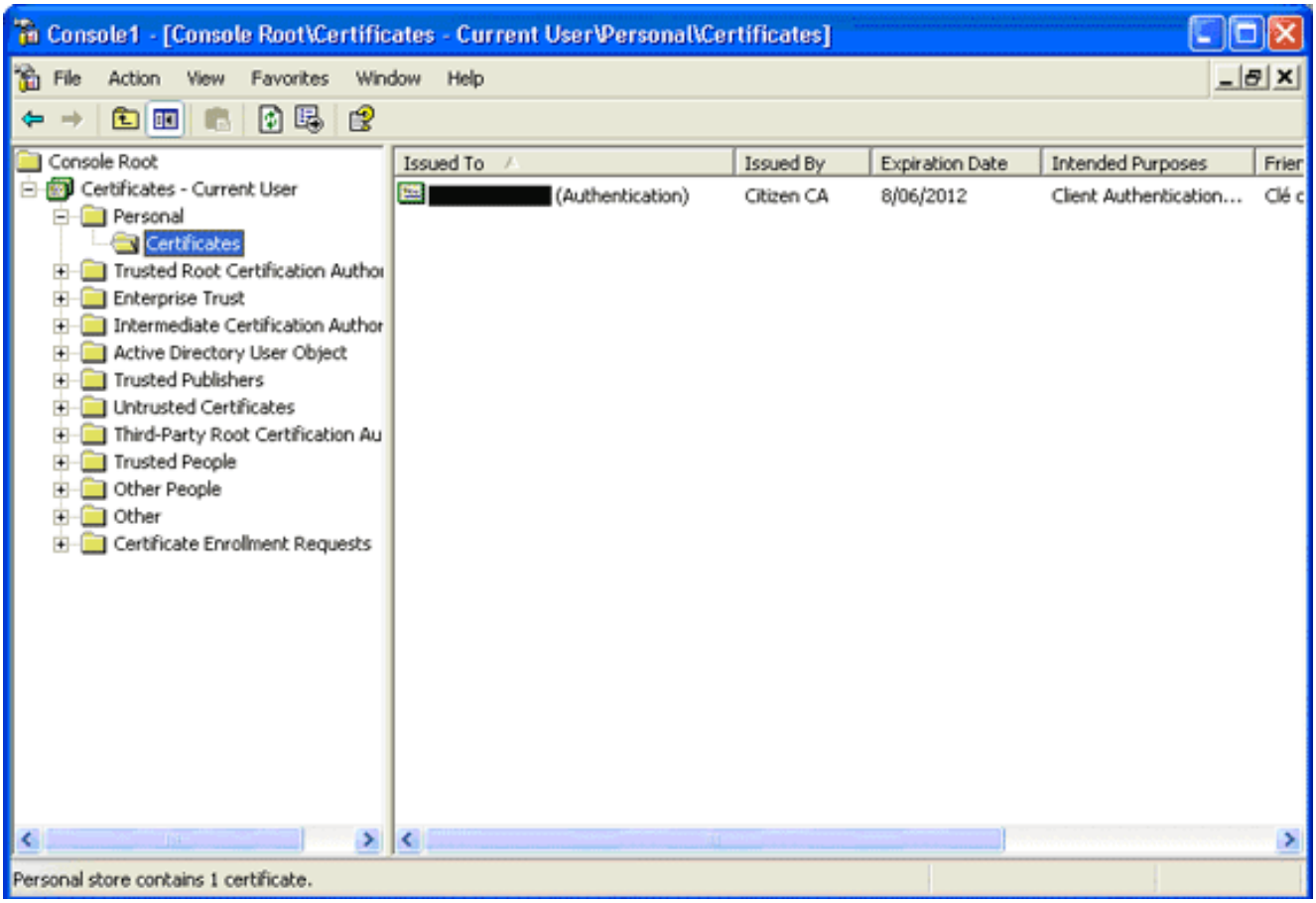

3. 展开**比利时根CA**，然后展开**公民CA**。
4. 选择**Authentication** 版本的**指定证**书。
5. 单击**Enregistrer**(FR)按钮。证书将复制到Windows存储中。

**注：单**击“详细信**息”**按钮时，将出现一个窗口，显示有关证书的详细信息。在“详细信息”选项卡中，选择**主题**字段以查看“序列号”字段。“序列号”字段包含用于用户授权的唯一值。例如，序列号“56100307215”表示出生日期为1956年10月3日、序列号为072且支票数字为15的*用户。您必须提交联邦当局的批准请求以存储这些号码。您有责任作出与在贵国维护比利时公民数据库相关的适当官方声明。*

## 验证

要验证证书是否已成功导入，请完成以下步骤：

1. 在Windows XP计算机上，打开DOS窗口，然后键入**mmc**命令。系统将显示控制台应用。
2. 选择**文件>添加/删除管理单**元（或按Ctrl+M）。系统将显示“添加/删除管理单元”对话框。
3. 单击 **Add 按钮。**系统将显示“添加独立管理单元”对话框。
4. 在“可用的独立管理单元”列表中，选择“证**书”**，然后单击“**添加”**。
5. 单击“My user account(**我的用户帐户**)”单选按钮，然后单**击“Finish(完成**)”。“证书”管理单元显示在“添加/删除管理单元”对话框中。
6. 单击**关闭**以关闭“添加独立管理单元”对话框，然后单击“添加/删除管理单元”对话框中的**确定**，以保存更改并返回到控制台应用程序。
7. 在Console Root文件夹下，展开Certificates **- Current User**。
8. 展开**个人**，然后展开**证书**。导入的证书必须显示在Windows存储中，如下图所示：




## AnyConnect安装

您必须在远程PC上安装AnyConnect客户端。AnyConnect软件使用可编辑的XML配置文件来预设可用网关列表。XML文件存储在远程PC的此路径中：

C:\Documents and Settings*%USERNAME%*\应用程序Data\Cisco\Cisco AnyConnect VPN Client

其中*%USERNAME%*是远程PC上用户的名称。

XML文件的名称是preferences.*xml*。以下是文件内容的示例：

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

其中*192.168.0.1*是ASA网关的IP地址。

## ASA要求

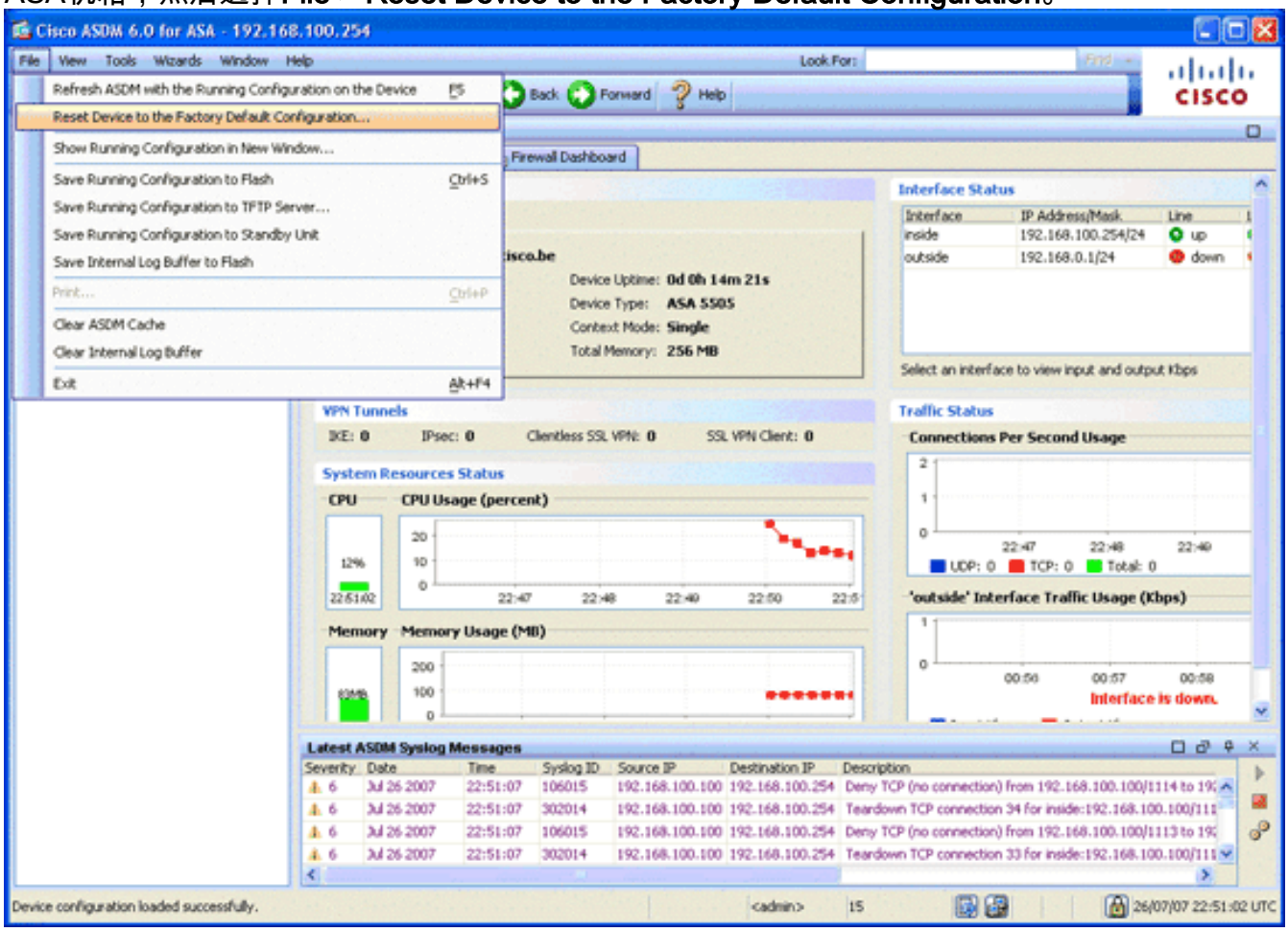
确保ASA满足以下要求：

- AnyConnect和ASDM必须在闪存中运行。要完成本文档中的步骤，请使用安装了相应ASA 8.0软件的ASA 5505。AnyConnect和ASDM应用必须预装在闪存中。使用**show flash**命令查看闪存的内容：

```
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
```

- ASA必须使用出厂默认设置运行。如果您使用新的ASA机箱来完成本文档中的步骤，则可以跳过此要求。否则，请完成以下步骤以将ASA重置为出厂默认设置：在ASDM应用中，连接到ASA机箱，然后选择**File > Reset Device to the Factory Default Configuration**。




保留模板中的默认值。在Ethernet 0/1内部接口上连接PC，并更新将由ASA的DHCP服务器调配的IP地址。**注意**：要将ASA重置为命令行的出厂默认值，请使用以下命令：

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

# ASA 配置

重置ASA出厂默认设置后，可以启动ASDM到192.168.0.1，以便在Ethernet 0/1内部接口上连接到ASA。

**注意**：您以前的密码将保留（或者默认为空）。

默认情况下，ASA接受源IP地址为192.168.0.0/24的传入管理会话。在ASA的内部接口上启用的默认DHCP服务器提供范围为192.168.0.2-129/24的IP地址，该IP地址有效地连接到ASDM的内部接口。

要配置ASA，请完成以下步骤：

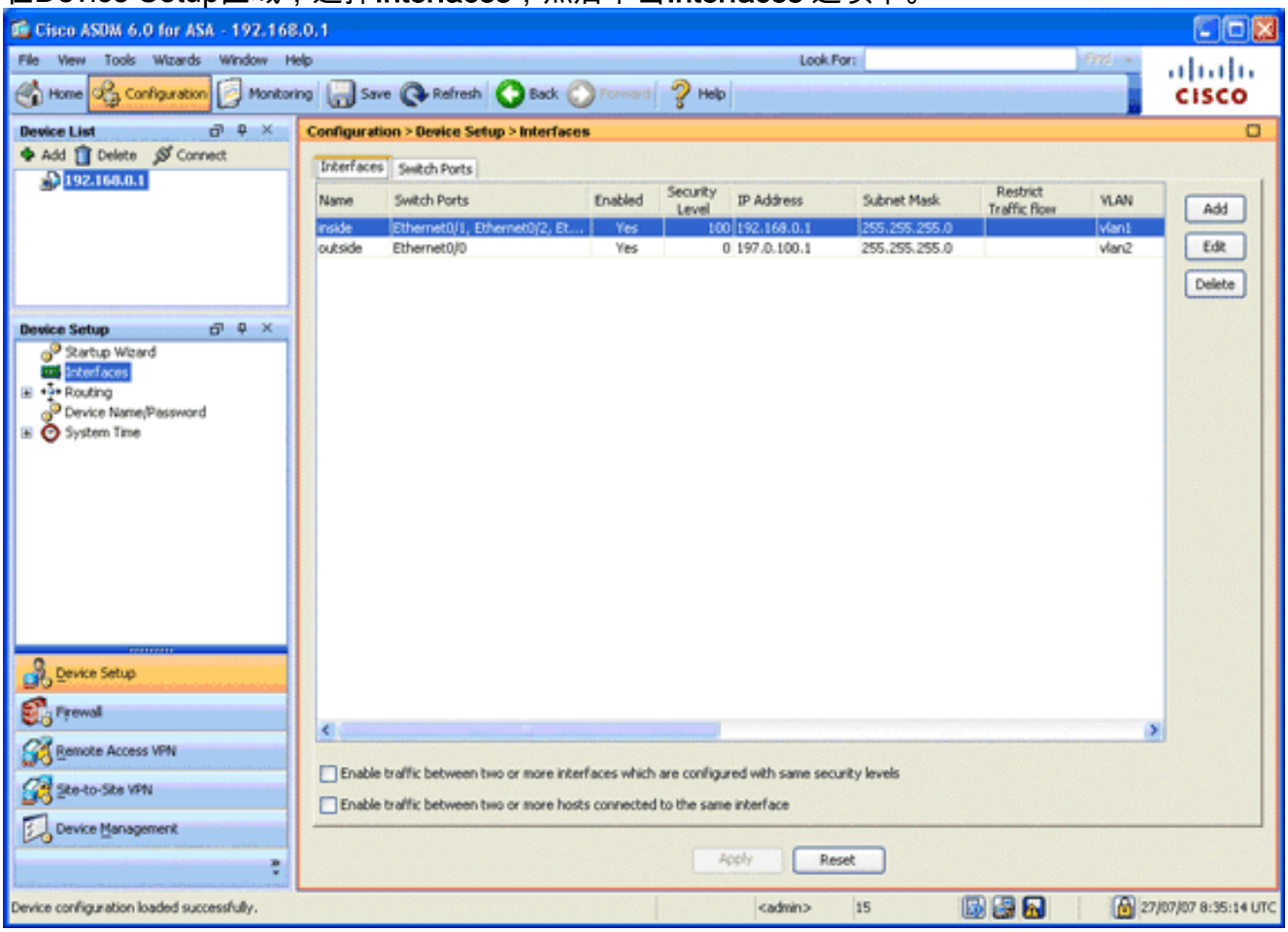
1. 启用外部接口
2. 配置域名、密码和系统时间
3. 在外部接口上启用DHCP服务器
4. 配置eID VPN地址池

5. 导入比利时根CA证书
6. 配置安全套接字层
7. 定义默认组策略
8. 定义证书映射
9. 添加本地用户
10. 重新启动ASA

## 步骤1.启用外部接口

此步骤介绍如何启用外部接口。

1. 在ASDM应用中，单击**Configuration**，然后单击**Device Setup**。
2. 在Device Setup区域，选择**Interfaces**，然后单击**Interfaces** 选项卡。

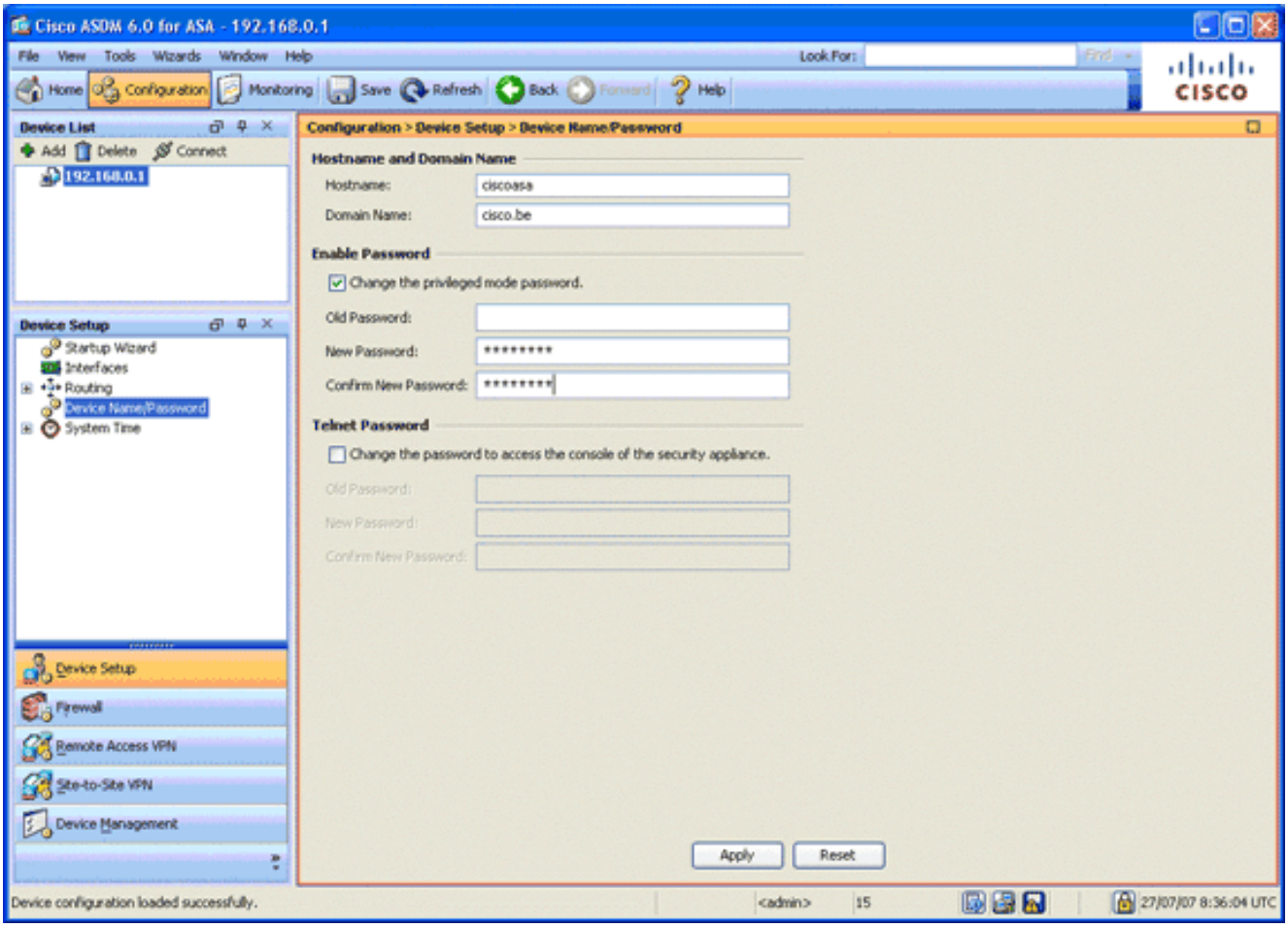



3. 选择外部接口，然后单击“**编辑**”。
4. 在“常规”选项卡的“IP地址”部分，选择“**使用静态IP**”选项。
5. 输入197.0.100.1作为IP地址，**输入**255.255.255.0作为子网掩码。
6. 单击 **Apply**。

## 步骤2.配置域名、口令和系统时间

此步骤介绍如何配置域名、口令和系统时间。

1. 在Device Setup区域，选择**Device Name/Password**。

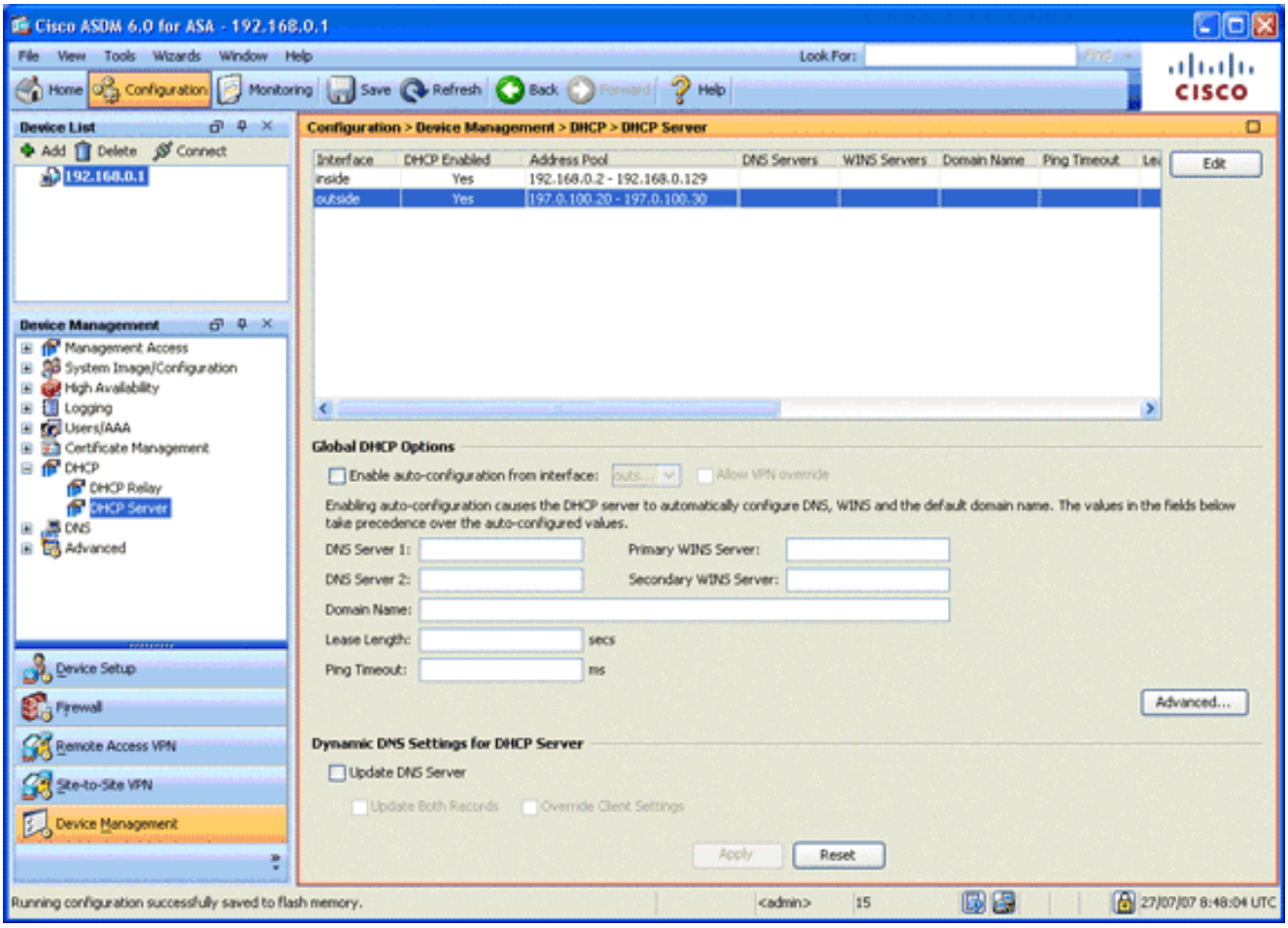



2. 输入**cisco.be**作为域名，并输入**cisco123**作为Enable Password（启用密码）值。**注意：**默认情况下，密码为空。
3. 单击 **Apply**。
4. 在Device Setup区域中，选择**System Time**，然后更改时钟值（如果需要）。
5. 单击 **Apply**。

## 步骤3.在外部接口上启用DHCP服务器。

此步骤介绍如何在外部接口上启用DHCP服务器以便于测试。

1. 单击 **Configuration**，然后单击 Device Management。
2. 在Device Management区域，展开**DHCP**，然后选择**DHCP Server**。

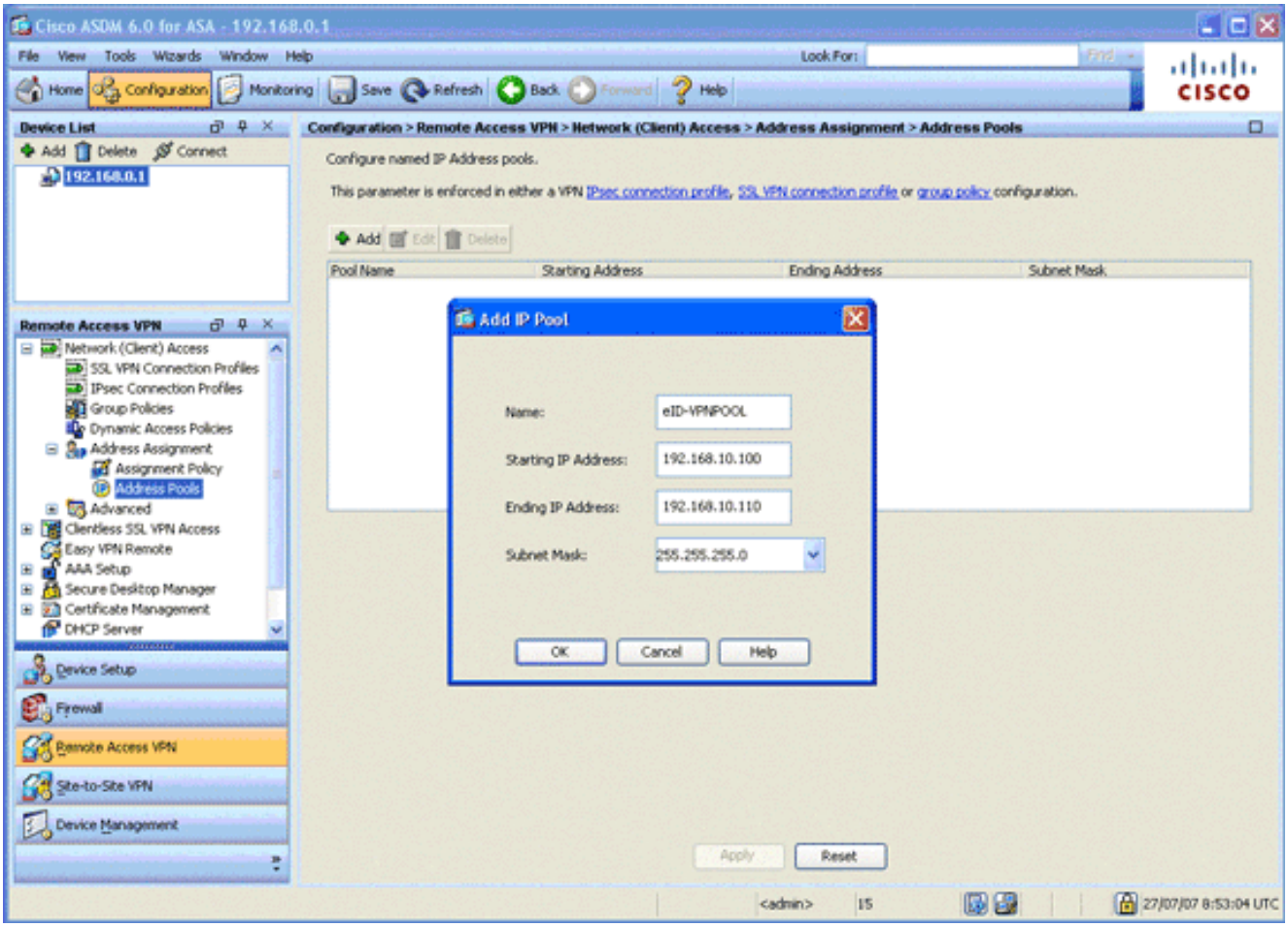



3. 从接口列表中选择外部接口，然后单击**编辑**。系统将显示Edit DHCP Server对话框。
4. 选中启**用DHCP服务器**复选框。
5. 在DHCP地址池中，输入从197.0.100.20到197.0.100.30的IP地址。
6. 在Global DHCP Options（全局DHCP选项）区域，取消选中**Enable auto-configuration from interface(从接口启用自动配**置)复选框。
7. 单击 **Apply**。

## 步骤4.配置eID VPN地址池

此步骤介绍如何定义用于调配远程AnyConnect客户端的IP地址池。

1. 单击 **Configuration**，然后单击 Remote Access VPN。
2. 在Remove Access VPN区域中，展开Network**(Client)Access，然**后展开Address Assignment**。**
3. 选择**Address Pools**，然后单击Configure named IP Address pools区域中的**Add按**钮。此时将出现 Add IP Pool 对话框。



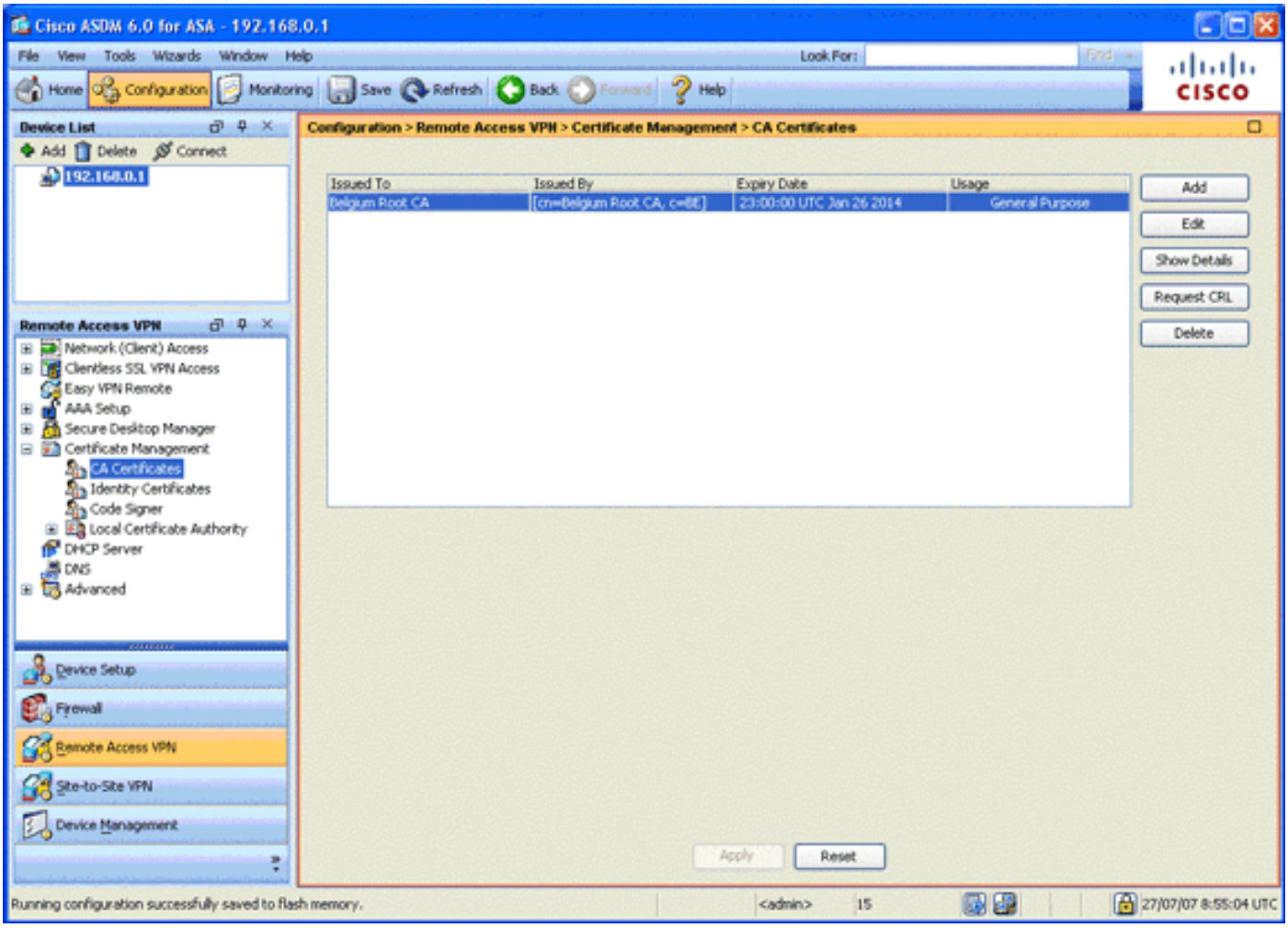

4. 在Name字段中，输入**eID-VPNPOOL**。
5. 在“起始IP地址”和“结束IP地址”字段中，输入IP地址范围（从192.168.10.100到192.168.10.110）。
6. 从“子**网掩码”下拉列**表中选择255.255.255.0，单击**确定**，然后单击**应用**。

## 步骤5.导入比利时根CA证书

此步骤介绍如何导入比利时根CA证书到ASA。

1. 从政府网站下载并安装比利时根CA证书（belgiumrca.crt和belgiumrca2.crt），并将其存储在您当地的PC上。比利时政府网站位于以下URL:http://certs.eid.belgium.be/
2. 在Remote Access VPN区域中，展开Certificate Management，**然**后选择**CA Certificates**。
3. 单击**Add**，然**后单击Install from file**。
4. 浏览到保存比利时根CA证书(belgiumrca.crt)文件的位置，然后单击“安装证**书”**。
5. 点击**应用以保存更改。**

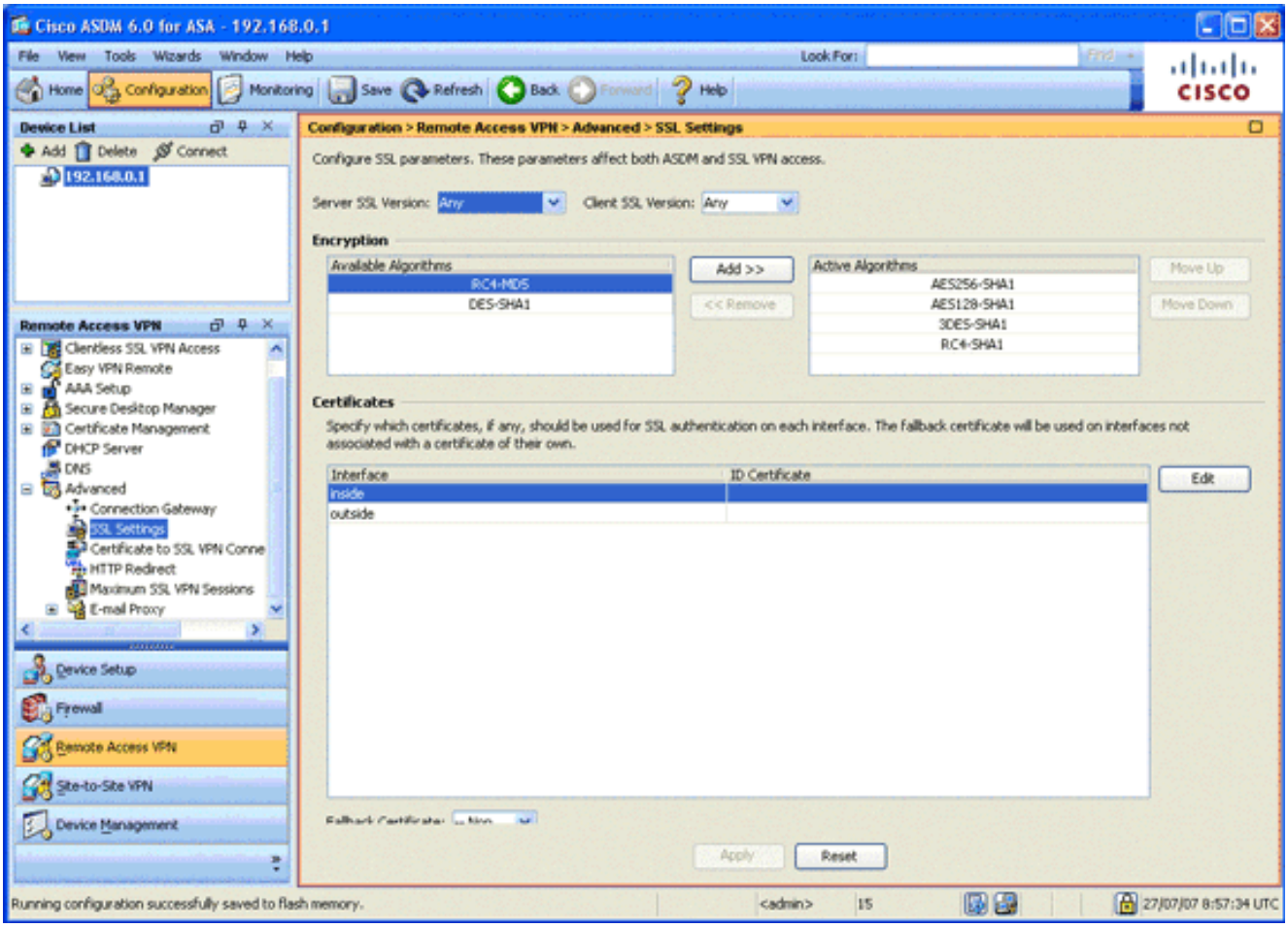
下图显示ASA上安装的证书：



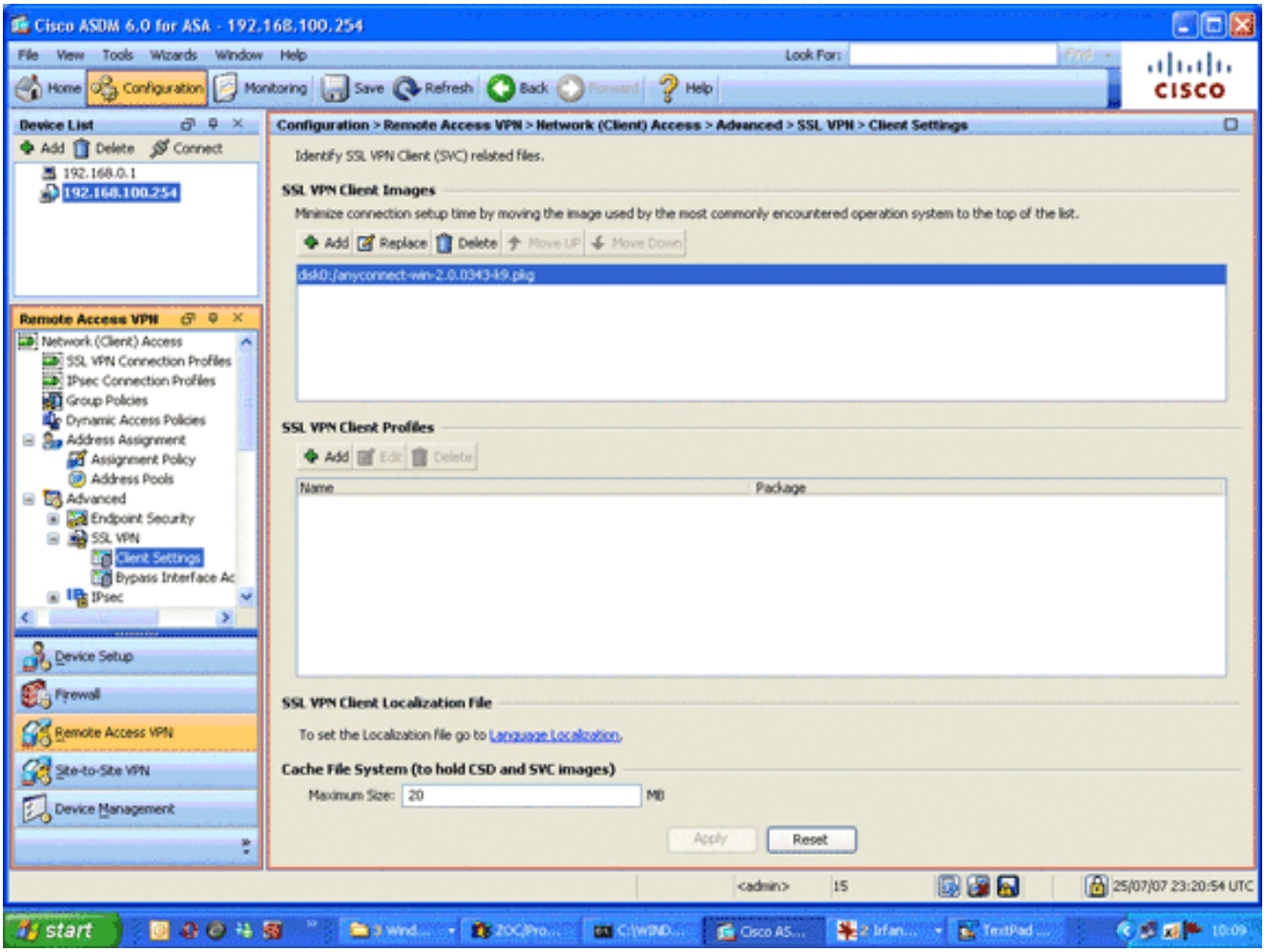

## 步骤6.配置安全套接字层

此步骤介绍如何确定安全加密选项的优先级、定义SSL VPN客户端映像和定义连接配置文件。

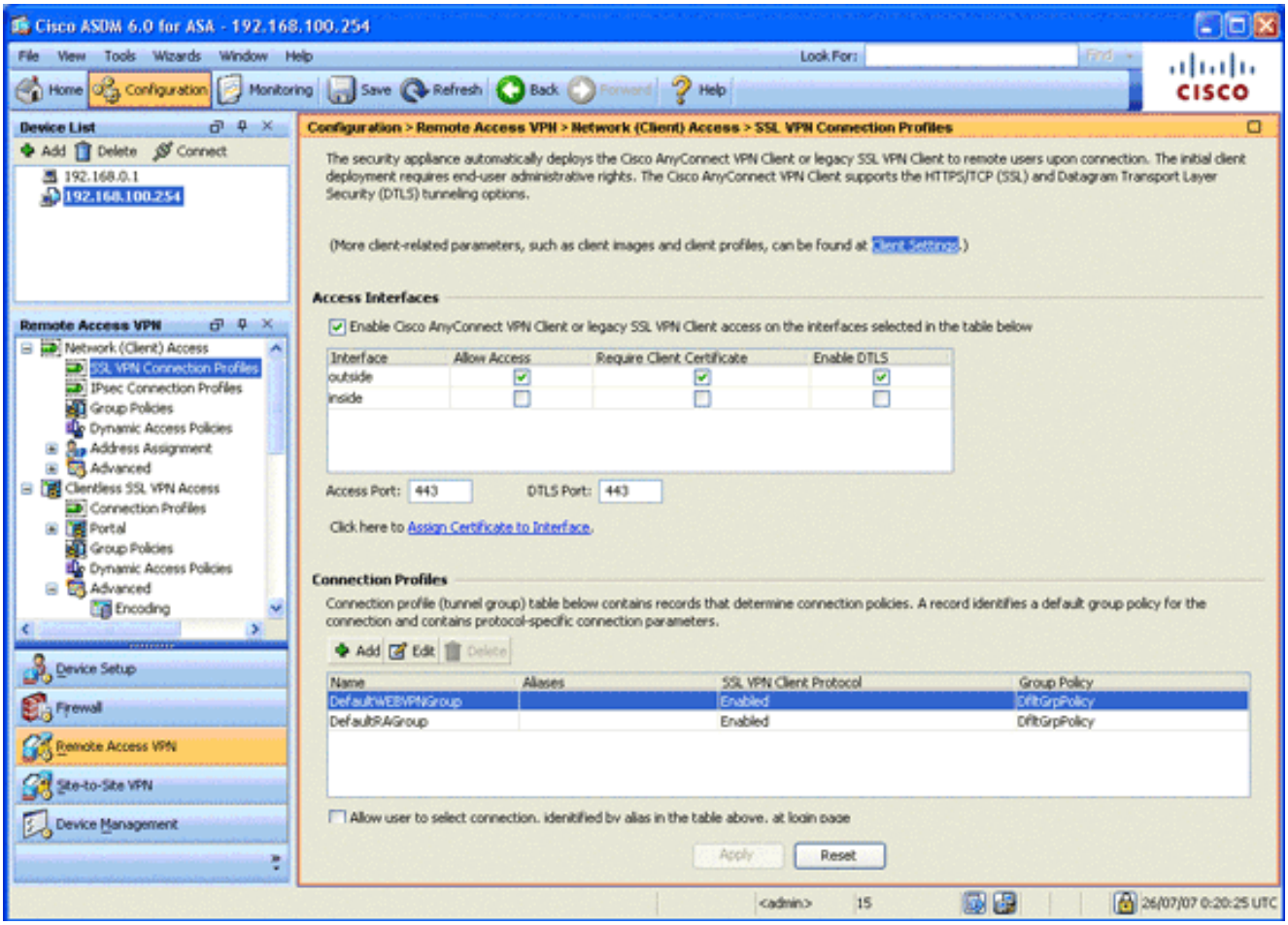
1. 确定最安全加密选项的优先级。在Remote Access VPN区域中，展开**Advanced**，然后选择**SSL Settings**。在“加密”(Encryption)部分，活动算法(Active Algorithms)按如下方式自上而下堆叠：AES256-SHA1AES128-SHA13DES-SHA1RC4-
SHA1



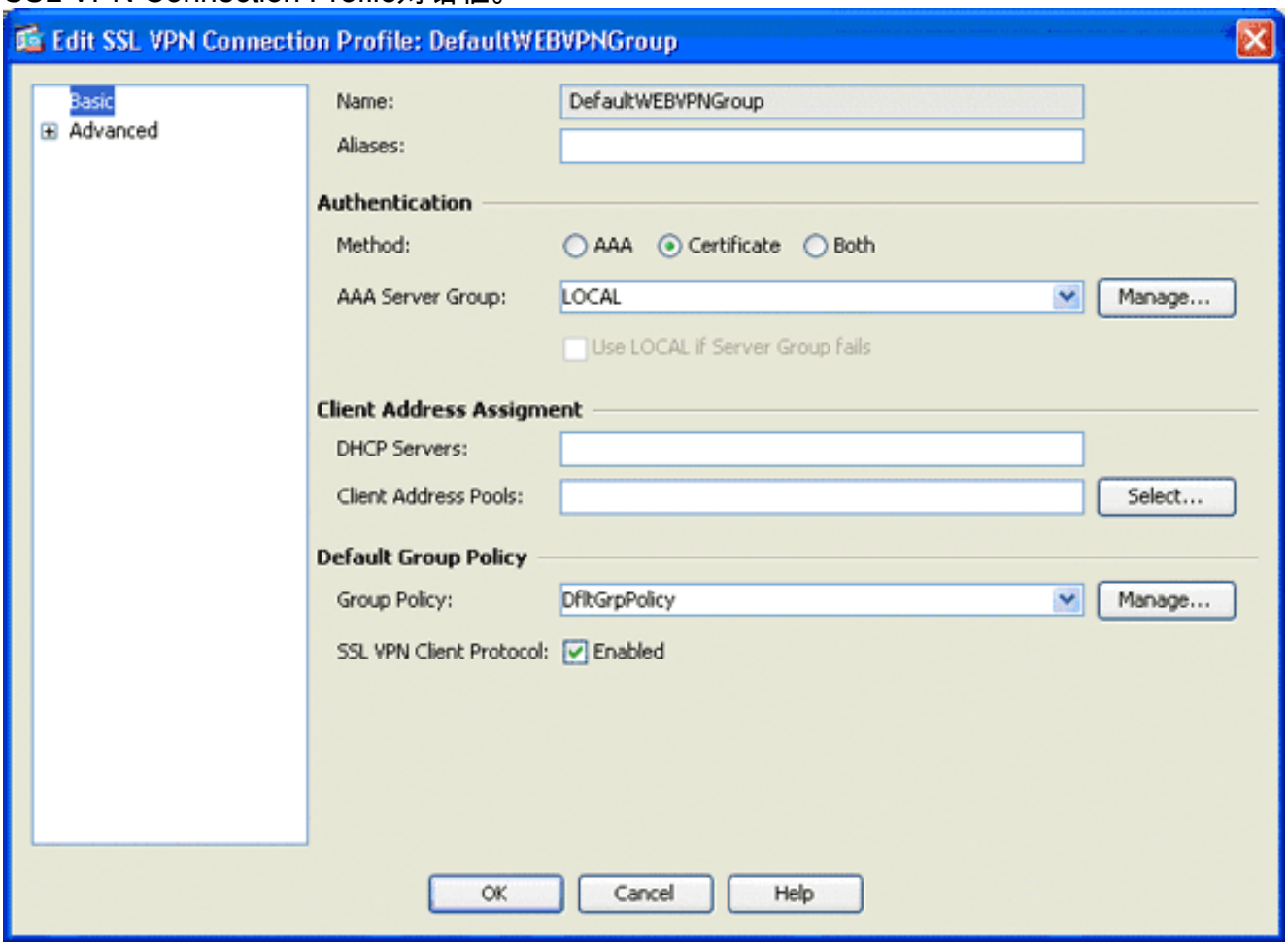

2. 定义AnyConnect客户端的SSL VPN客户端映像。在Remote Access VPN区域中，展开Advanced，**展开SSL VPN，然后选择Client Settings**。在SSL VPN Client Images区域中，单击**Add**。选择存储在闪存中的AnyConnect软件包。AnyConnect软件包显示在SSL VPN客户端映像列表中，如下图所示
：




3. 定义DefaultWEBVPNGroup连接配置文件。在Remote Access VPN区域中，展开Network**(Client)Access，然**后选择**SSL VPN Connection Profiles**。在Access Interfaces区域中，选中**Enable Cisco AnyConnect VPN Client复选框**。对于外部接口，选中**允许访问、要求客户端证书**和**启用DTLS**复选框，如下图所示：

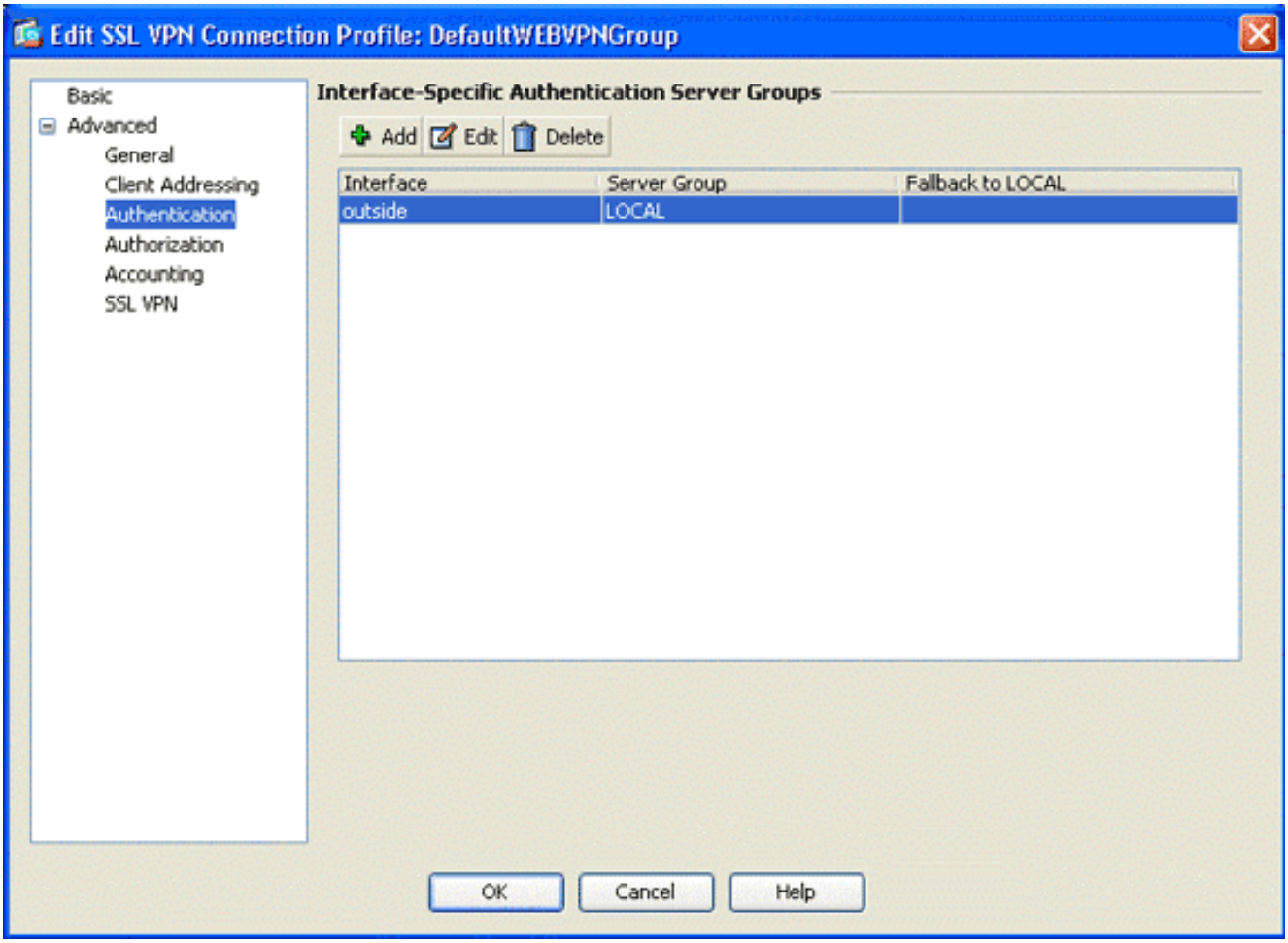



在“连接配置文件”区域中，选择**DefaultWEBVPNGroup**，然后单击“**编辑**”。系统将显示Edit SSL VPN Connection Profile对话框。

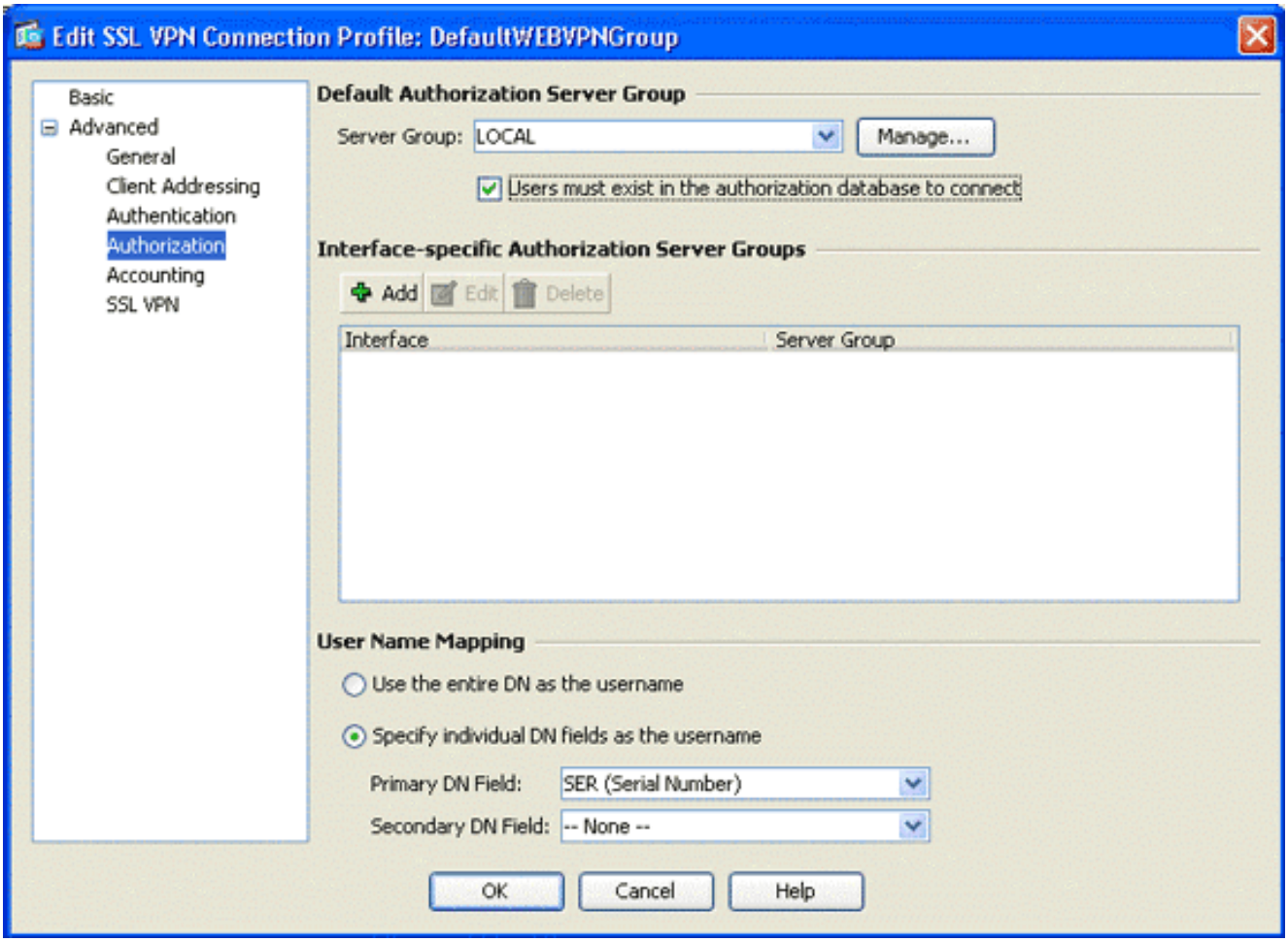



在导航区域中，选择**Basic**。在Authentication区域中，单击**Certificate**单选按钮。在Default

Group Policy（默认组策略）区域，选中**SSL VPN Client Protocol(SSL VPN Client协**议)复选框。展开**Advanced**，然后选**择Authentication(身份验证)**。单击**Add**，然后添加外部接口和本地服务器组，如下图所示
：



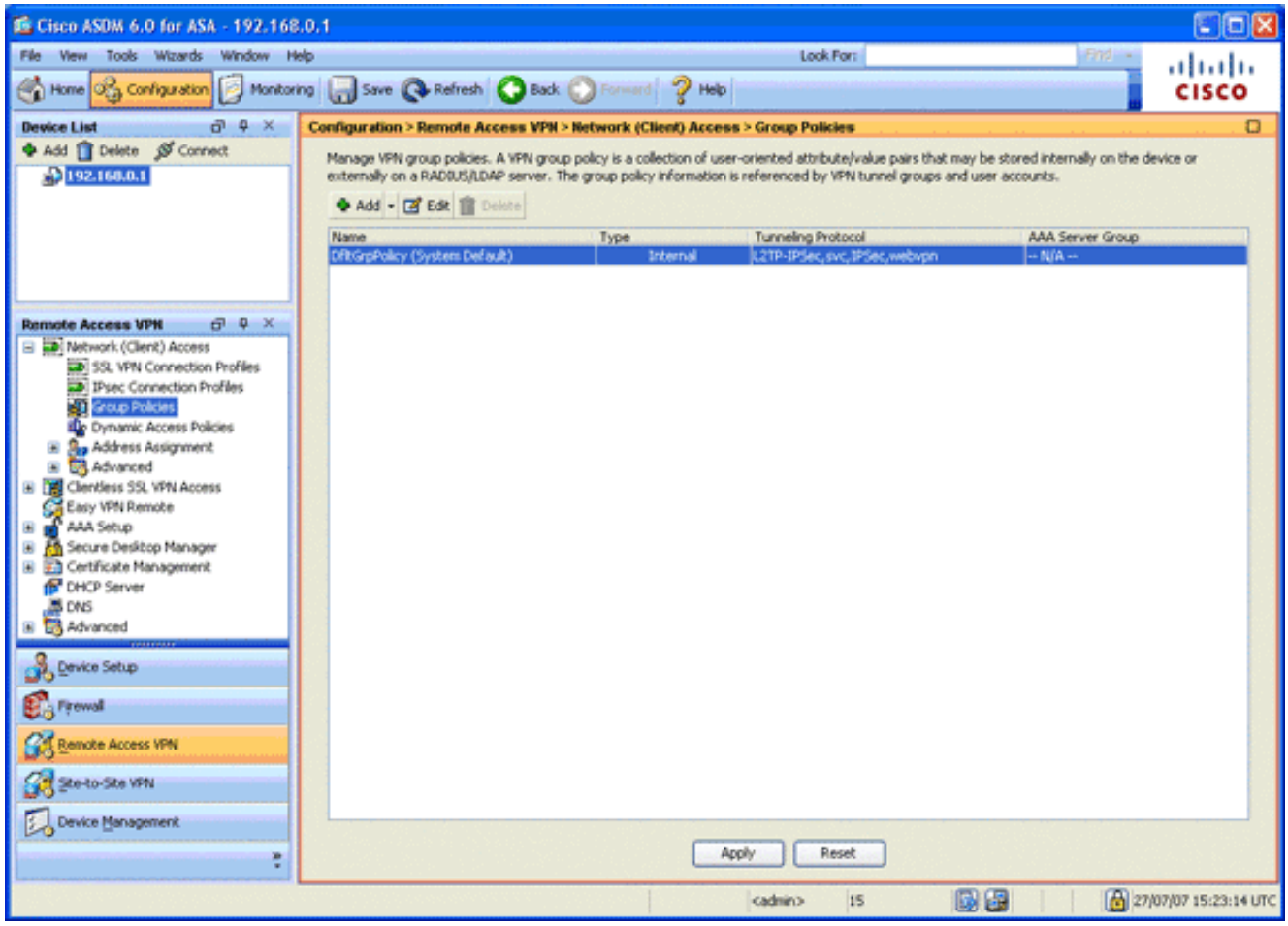

在导航区域中，选择**授权**。在Default Authorization Server Group区域，从Server Group下拉列表中选择**LOCAL**，并选中**Users must exist in the authorization database to connect复选**框。在User Name Mapping区域，从Primary DN Field下拉列表中**选择SER(Serial Number)**，从Secondary DN Field中选择**None**，然后单击**OK**。



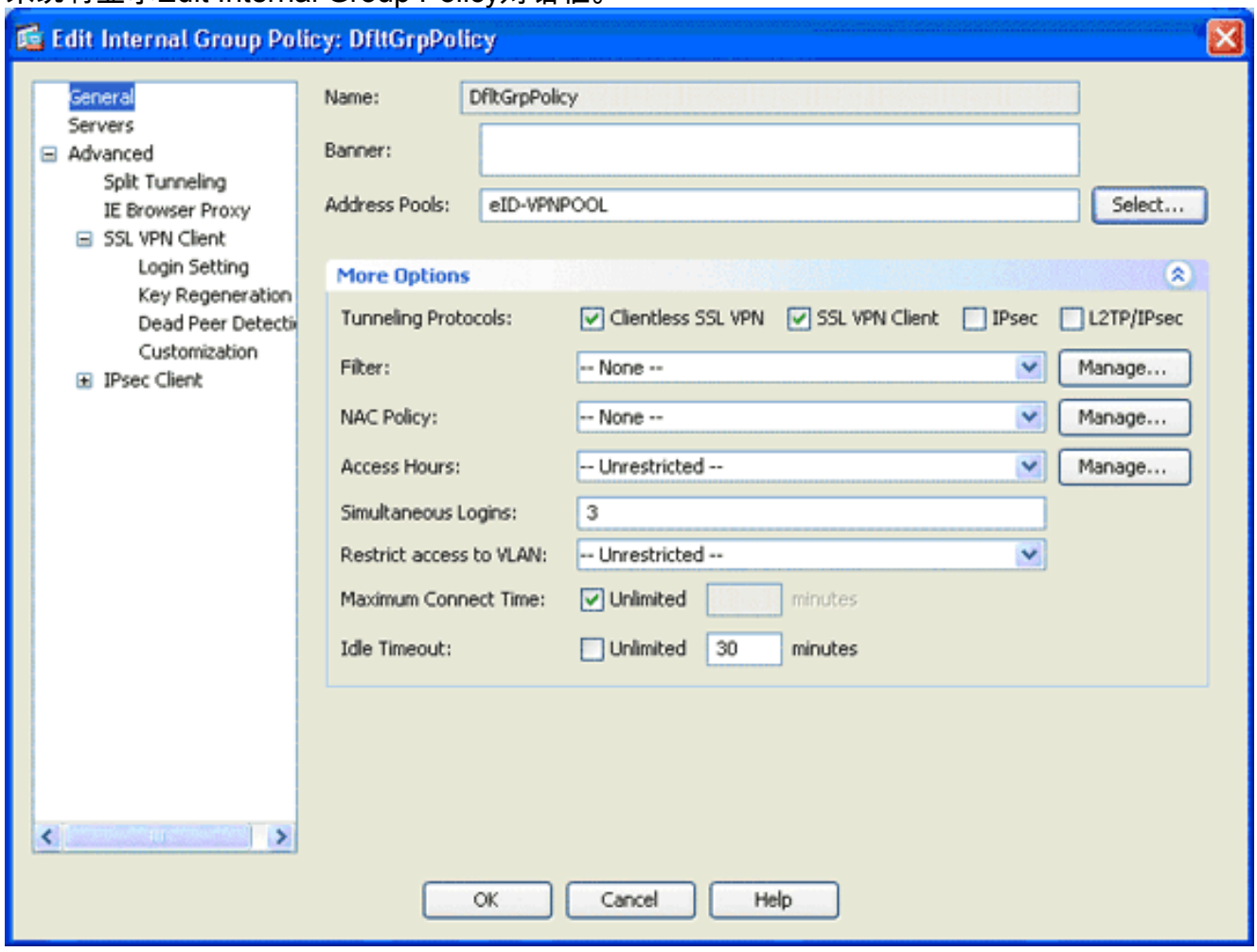

## 步骤7.定义默认组策略

此步骤介绍如何定义默认组策略。

1. 在Remote Access VPN区域中，展开Network(Client)Access，然后选择Group Policies。




2. 从组策**略列**表中选择DfltGrpPolicy，然后单击**Edit**。
3. 系统将显示Edit Internal Group Policy对话框。

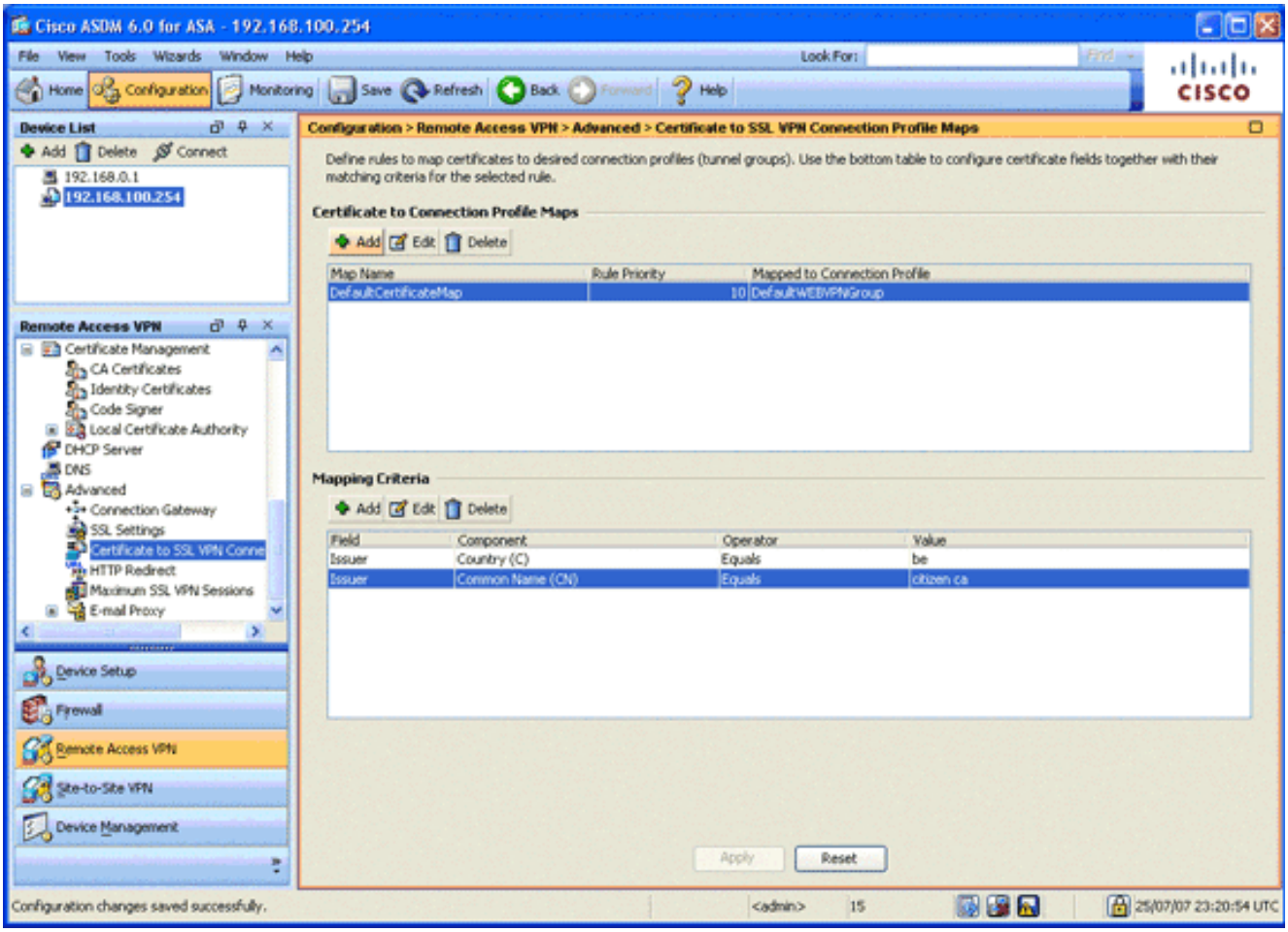


4. 从导航区域中，选择**General**。
5. 对于地址池，单击**选择**以选择地址池，然后选择**eID-VPNPOOL**。
6. 在“更多选项”区域，取消选中**IPsec**和**L2TP/IPsec**复选框，然后单击**确定**。

## 步骤8.定义证书映射

此步骤介绍如何定义证书映射条件。

1. 在Remote Access VPN区域中，单击**Advanced**，然后选择**Certificate to SSL VPN Connection Profile Maps**。
2. 在Certificate to Connection Profile Maps区域中，单击**Add**，然后从映射列表中选择**DefaultCertificateMap**。此映射必须与“映射到连接配置文件”(Mapped to Connection Profile)字段中的*DefaultWEBVPNProfile*匹配。
3. 在“映射条件”(Mapping Criteria)区域中，单击**添加**，然后添加以下值：字段:颁发者，国家(C)，等于，"be"字段:颁发者、公用名(CN)、等号、“公民ca”映射条件应显示如下图所示：



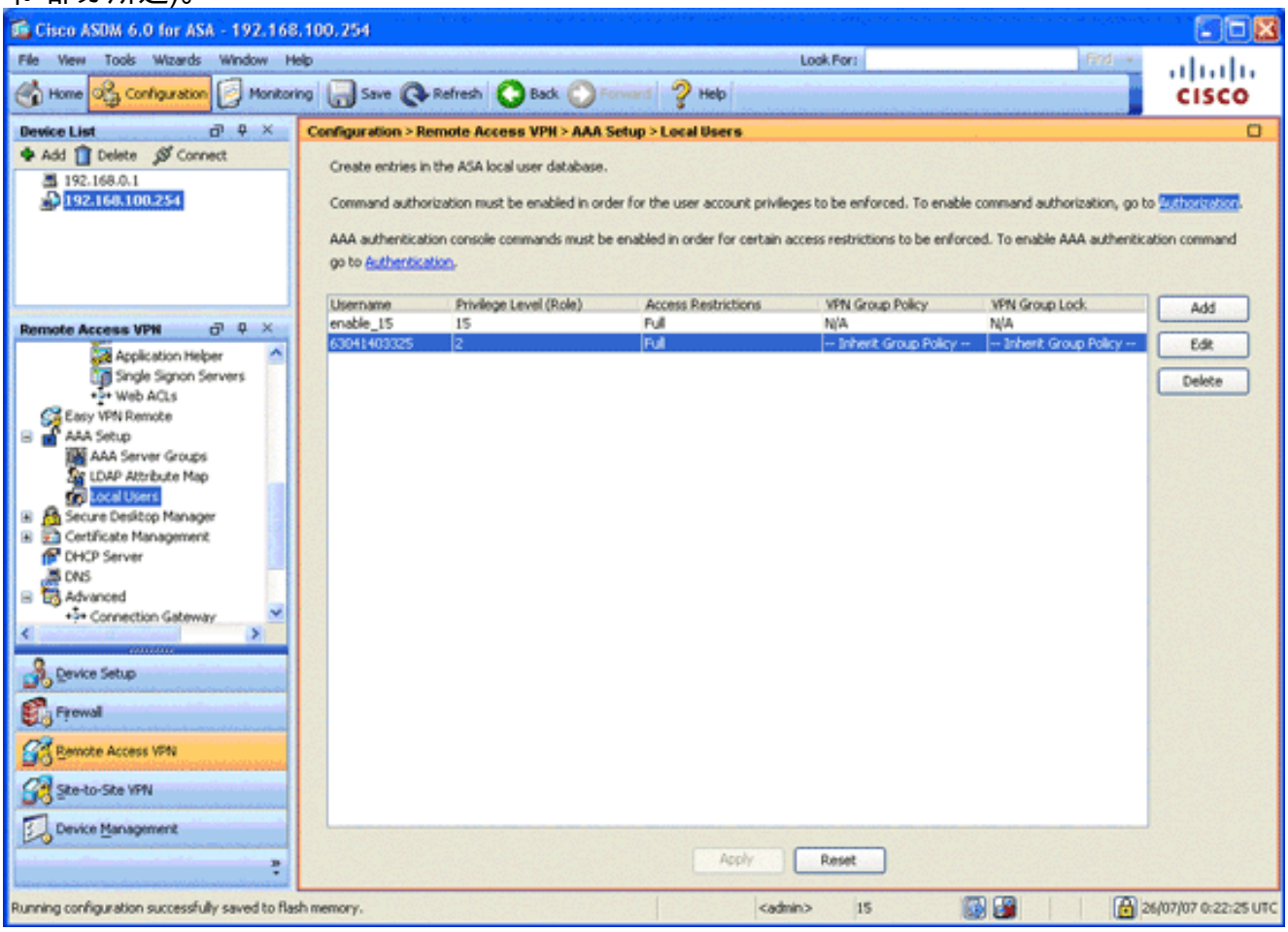

4. 单击 **Apply**。

## 步骤9.添加本地用户

此步骤介绍如何添加本地用户。

1. 在Remote Access VPN区域中，展开**AAA Setup**，然后选择**Local Users**。
2. 在“本地用户”区域中，单击**添加**。
3. 在Username字段中，输入用户证书的序列号。例如，56100307215(如本文档的“身份验证证

书”部分所述)。




4. 单击 Apply。

## 步骤10.重新启动ASA

重新启动ASA，以确保所有更改都应用于系统服务。

# 微调

测试时，某些SSL隧道可能无法正确关闭。由于ASA假设AnyConnect客户端可能断开连接并重新连接，因此隧道不会丢弃，这为它提供了返回的机会。但是，在使用基本许可证（默认为2个SSL隧道）进行实验测试期间，当SSL隧道未正确关闭时，可能会耗尽许可证。如果出现此问题，请使用 **vpn-sessiondb logoff < *option* >** 命令注销所有活动的SSL会话。

# 一分钟配置

要快速创建工作配置，请将ASA重置为出厂默认设置，并将此配置粘贴到配置模式：

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

## 相关信息

- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems