Autenticación Anyconnect ASA 8.x con la tarjeta eID belga

Contenido

Introducción

Este documento describe cómo configurar la autenticación Anyconnect ASA 8.x para utilizar la tarjeta eID belga.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA 5505 con el software ASA 8.0 apropiado
- 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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

El eID es una tarjeta PKI (Infraestructura de Clave Pública) emitida por el gobierno belga que los usuarios deben utilizar para autenticarse en un equipo Windows remoto. El cliente de software AnyConnect está instalado en el equipo local y toma las credenciales de autenticación del equipo remoto. Una vez finalizada la autenticación, el usuario remoto obtiene acceso a los recursos centrales a través de un túnel SSL completo. El usuario remoto recibe una dirección IP obtenida de un conjunto administrado por el ASA.

Configuración de PC local

Sistema operativo

El sistema operativo (Windows, MacOS, Unix o Linux) del PC local debe estar al día con todos los parches necesarios instalados.

Lector de tarjetas

Para utilizar la tarjeta eID, debe instalar un lector de tarjetas electrónicas en su equipo local. El lector de tarjetas electrónicas es un dispositivo de hardware que establece un canal de comunicación entre los programas en el equipo y el chip en la tarjeta de identificación.

Para obtener una lista de lectores de tarjetas aprobados, consulte esta URL: http://www.cardreaders.be/en/default.htm

Nota: Para utilizar el lector de tarjetas, debe instalar los controladores recomendados por el proveedor de hardware.

Software de tiempo de ejecución eID

Debe instalar el software eID Runtime proporcionado por el gobierno belga. Este software permite al usuario remoto leer, validar e imprimir el contenido de la tarjeta eID. El software está disponible en francés y holandés para Windows, MAC OS X y Linux.

Para obtener más información, consulte esta URL:

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

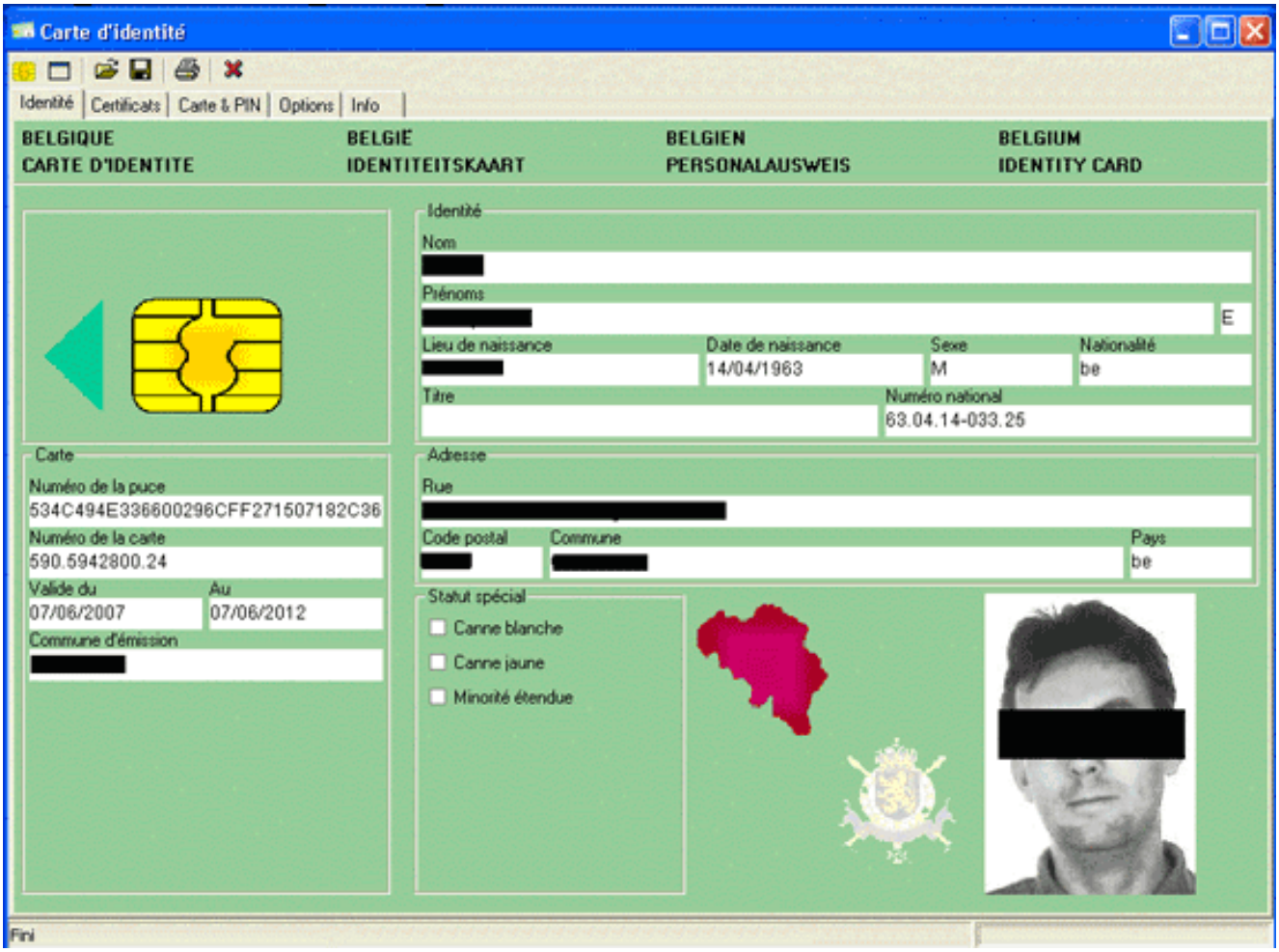
Certificado de autenticación

Debe importar el certificado de autenticación en el almacén de Microsoft Windows del equipo local. Si no puede importar el certificado en el almacén, AnyConnect Client no podrá establecer una conexión SSL con el ASA.

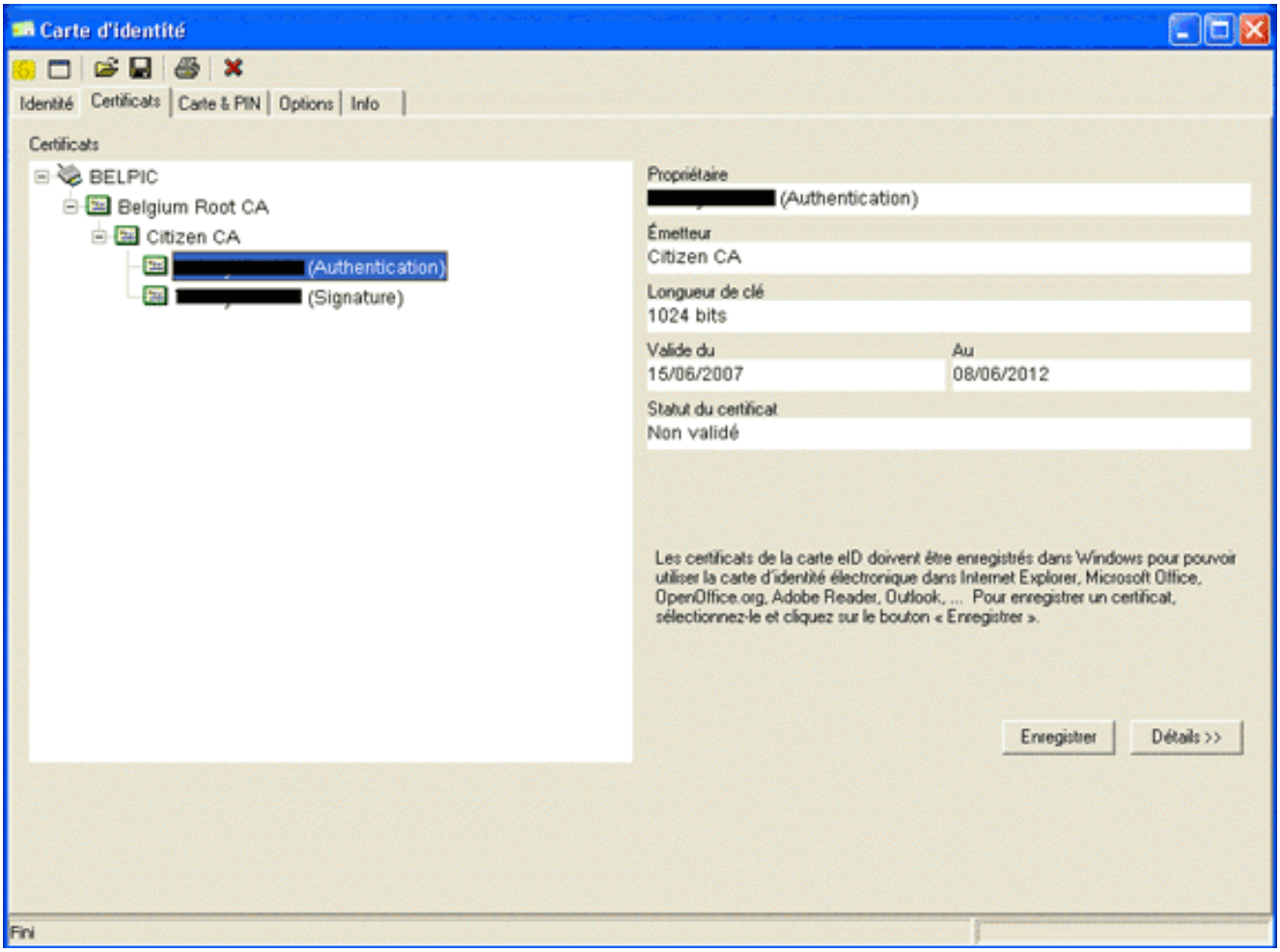
Procedimiento

Para importar el certificado de autenticación al almacén de Windows, complete estos pasos:

1. Inserte su eID en el lector de tarjetas e inicie el middleware para acceder al contenido de la tarjeta eID.Aparece el contenido de la tarjeta eID.



2. Haga clic en la pestaña **Certificados** (FR).Se muestra la jerarquía de certificados.



3. Expanda **Bélgica Root CA** y luego expanda **Citizen CA**.
4. Elija la versión **de autenticación** de su certificado con nombre.
5. Haga clic en el botón **Enregistration** (FR).El certificado se copia en el almacén de Windows.

Nota: Al hacer clic en el botón **Detalles**, aparece una ventana que muestra los detalles del certificado. En la ficha Detalles, seleccione el campo **Asunto** para ver el campo Número de serie. El campo Número de serie contiene un valor único que se utiliza para la autorización del usuario. Por ejemplo, el número de serie "56100307215" representa un usuario cuya fecha de nacimiento es el 3 de octubre de 1956 con un número de secuencia de 072 y un dígito de verificación de 15. *Debe enviar una solicitud de aprobación de las autoridades federales para almacenar estos números. Es su responsabilidad hacer las declaraciones oficiales pertinentes relacionadas con el mantenimiento de una base de datos de ciudadanos belgas en su país*.

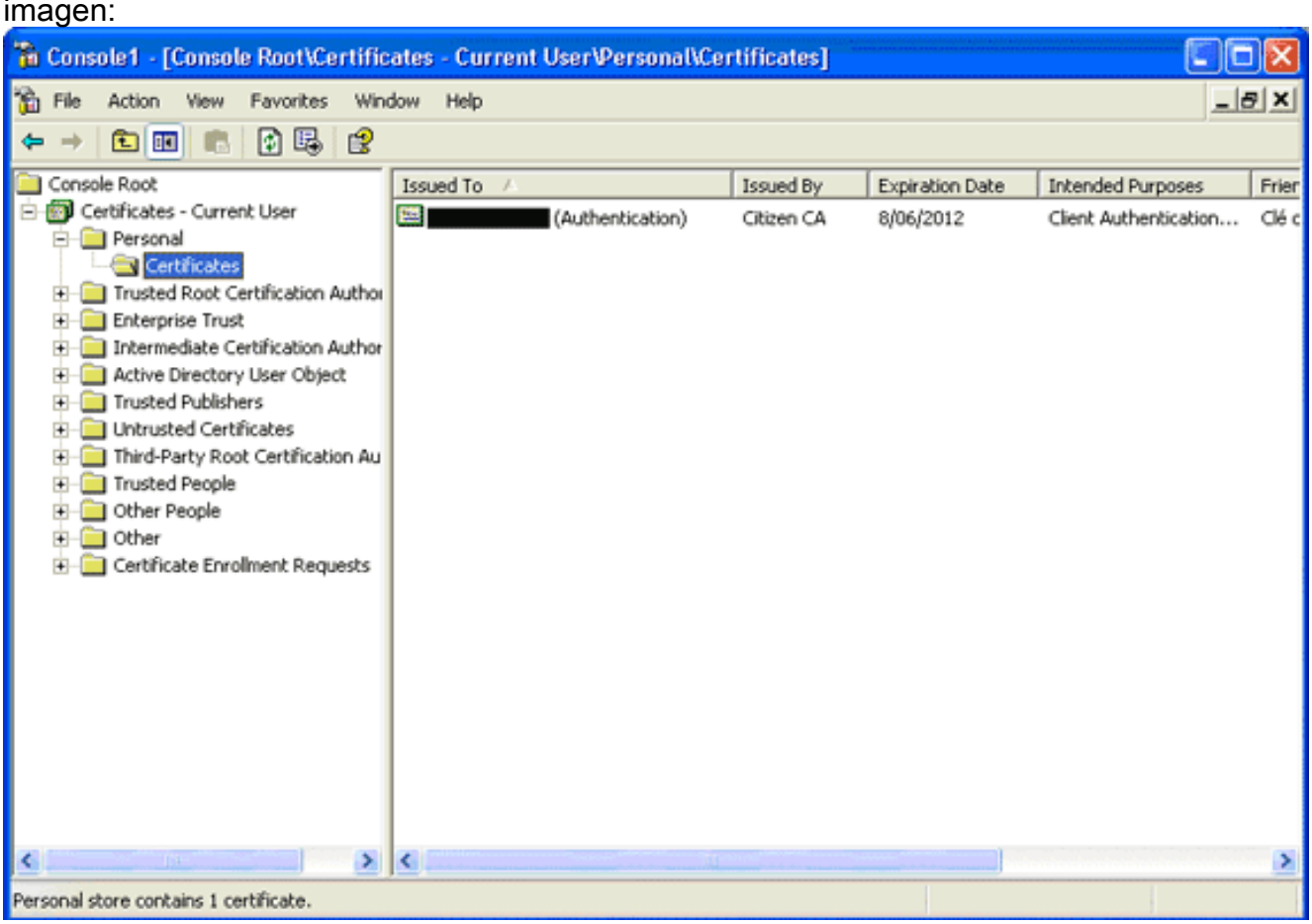
Verificación

Para verificar que el certificado se importó correctamente, complete estos pasos:

1. En una máquina con Windows XP, abra una ventana DOS y escriba el comando **mmc**.Aparece la aplicación Console.
2. Elija **File > Add/Remove Snap-in** (o presione Ctrl+M).Aparecerá el cuadro de diálogo Agregar o quitar complemento.
3. 'Haga clic en el botón Add (Agregar).'Aparece el cuadro de diálogo Agregar complemento independiente.
4. En la lista Complementos autónomos disponibles, elija **Certificados** y haga clic en **Agregar**.
5. Haga clic en el botón de opción **Mi cuenta de usuario** y haga clic en **Finalizar**.El complemento Certificado aparece en el cuadro de diálogo Agregar o quitar complemento.
6. Haga clic en **Cerrar** para cerrar el cuadro de diálogo Agregar complemento independiente y

luego haga clic en **Aceptar** en el cuadro de diálogo Agregar/quitar complemento para guardar los cambios y volver a la aplicación Consola.

7. En la carpeta Raíz de la consola, expanda **Certificados - Usuario actual**.
8. Expanda **Personal** y, a continuación, expanda **Certificados**.El certificado importado debe aparecer en el almacén de Windows como se muestra en esta imagen:



Instalación de AnyConnect

Debe instalar AnyConnect Client en el equipo remoto. El software AnyConnect utiliza un archivo de configuración XML que se puede editar para establecer previamente una lista de gateways disponibles. El archivo XML se almacena en esta ruta en el equipo remoto:

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

donde *%USERNAME%* es el nombre del usuario en el equipo remoto.

El nombre del archivo XML es *Preferences.xml*. A continuación se muestra un ejemplo del contenido del archivo:

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

donde *192.168.0.1* es la dirección IP del gateway ASA.

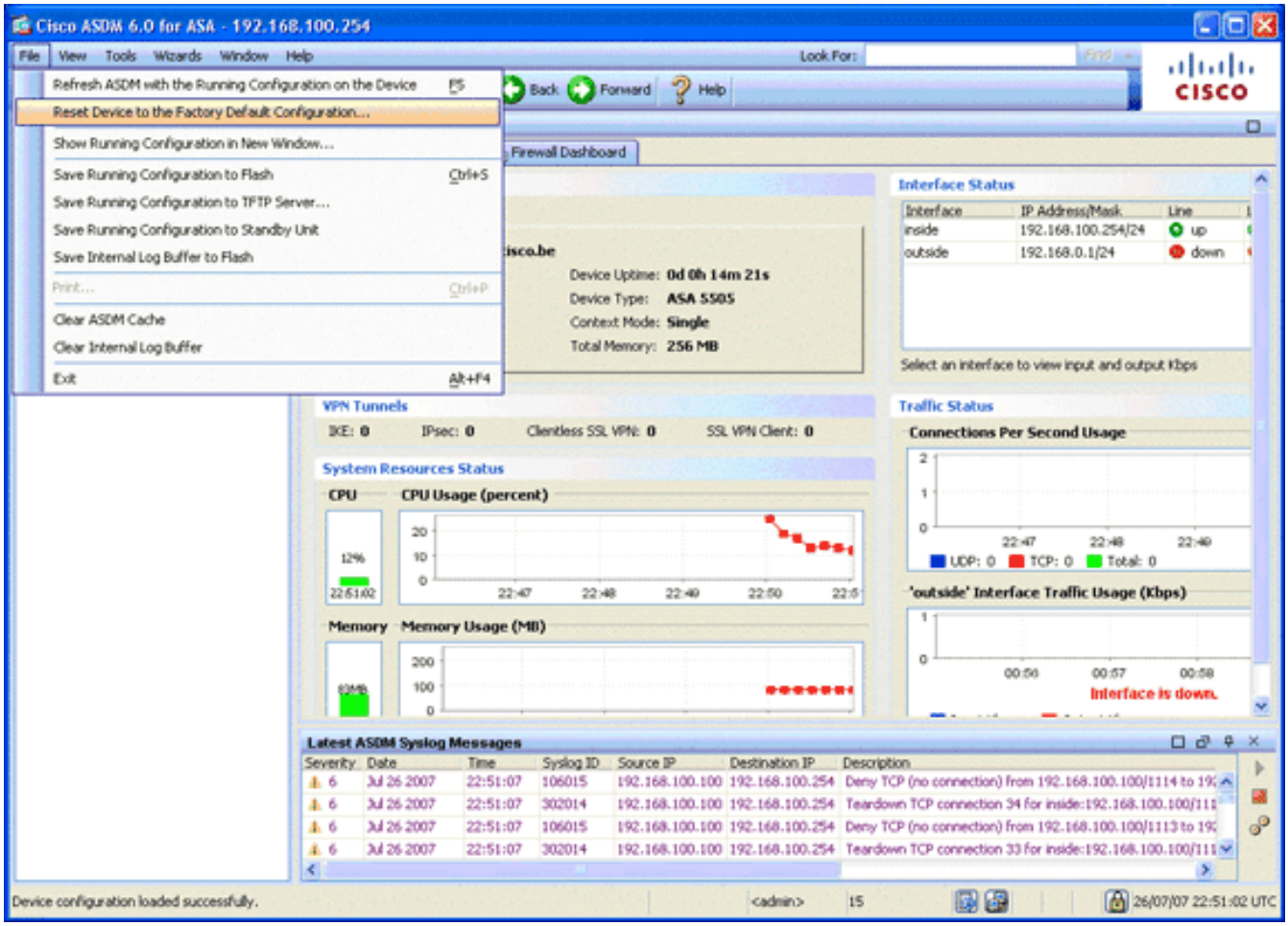
Requisitos de ASA

Asegúrese de que ASA cumple estos requisitos:

- AnyConnect y ASDM deben ejecutarse en la memoria flash.Para completar los procedimientos en este documento, utilice un ASA 5505 con el software ASA 8.0 apropiado instalado. Las aplicaciones AnyConnect y ASDM deben precargarse en la memoria flash. Utilice el comando **show flash** para ver el contenido de la memoria 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
```

- ASA debe ejecutarse con los valores predeterminados de fábrica.Puede omitir este requisito si utiliza un nuevo chasis ASA para completar los procedimientos en este documento. De lo contrario, complete estos pasos para restablecer el ASA a los valores predeterminados de fábrica:En la aplicación ASDM, conéctese al chasis ASA y elija **Archivo > Restablecer dispositivo a la configuración predeterminada de fábrica**.



Deje los valores predeterminados en la plantilla.Conecte el PC en la interfaz interna Ethernet 0/1 y renueve la dirección IP que proporcionará el servidor DHCP del ASA.**Nota:** Para restablecer el ASA a los valores predeterminados de fábrica desde la línea de comandos, utilice estos comandos :

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

Configuración ASA

Una vez restablecidos los valores predeterminados de fábrica de ASA, puede iniciar ASDM a 192.168.0.1 para conectarse al ASA en la interfaz interna Ethernet 0/1.

Nota: La contraseña anterior se conserva (o puede quedar en blanco de forma predeterminada).

De forma predeterminada, el ASA acepta una sesión de administración entrante con una dirección IP de origen en la subred 192.168.0.0/24. El servidor DHCP predeterminado habilitado en la interfaz interna del ASA proporciona direcciones IP en el rango 192.168.0.2-129/24, válidas para conectarse a la interfaz interna con ASDM.

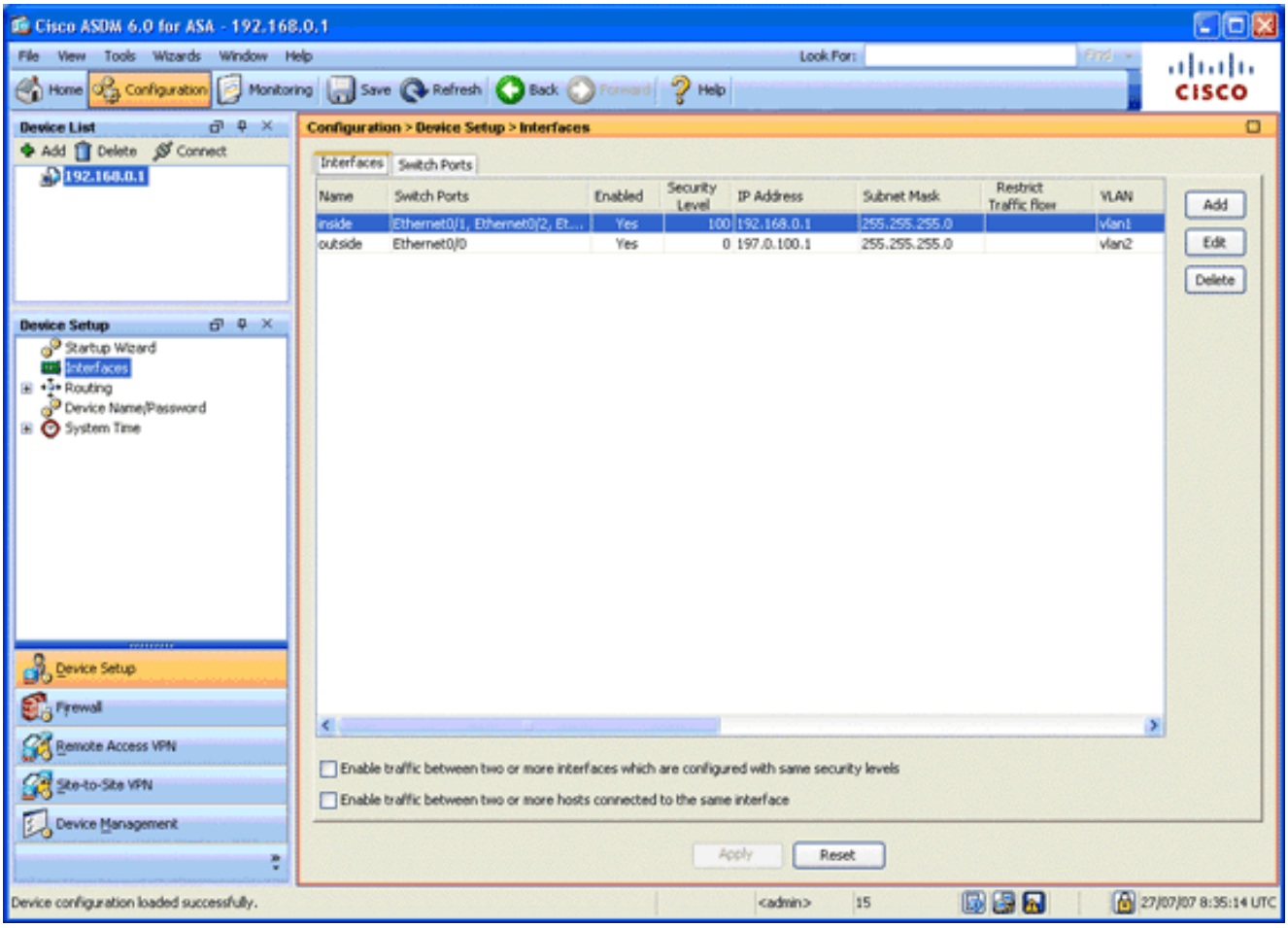
Complete estos pasos para configurar el ASA:

1. Habilitar la interfaz externa
2. Configure el nombre de dominio, la contraseña y la hora del sistema
3. Habilitar un servidor DHCP en la interfaz externa
4. Configure el eID VPN Address Pool
5. Importar el certificado de CA raíz de Bélgica
6. Configuración de la capa de sockets seguros
7. Definir la política de grupo predeterminada
8. Definir la asignación de certificados
9. Agregar un usuario local
10. Reinicie ASA

Paso 1. Habilitar la interfaz externa

Este paso describe cómo habilitar la interfaz externa.

1. En la aplicación ASDM, haga clic en **Configuration** y, a continuación, haga clic en **Device Setup**.
2. En el área Device Setup , elija **Interfaces** y luego haga clic en la pestaña **Interfaces**.

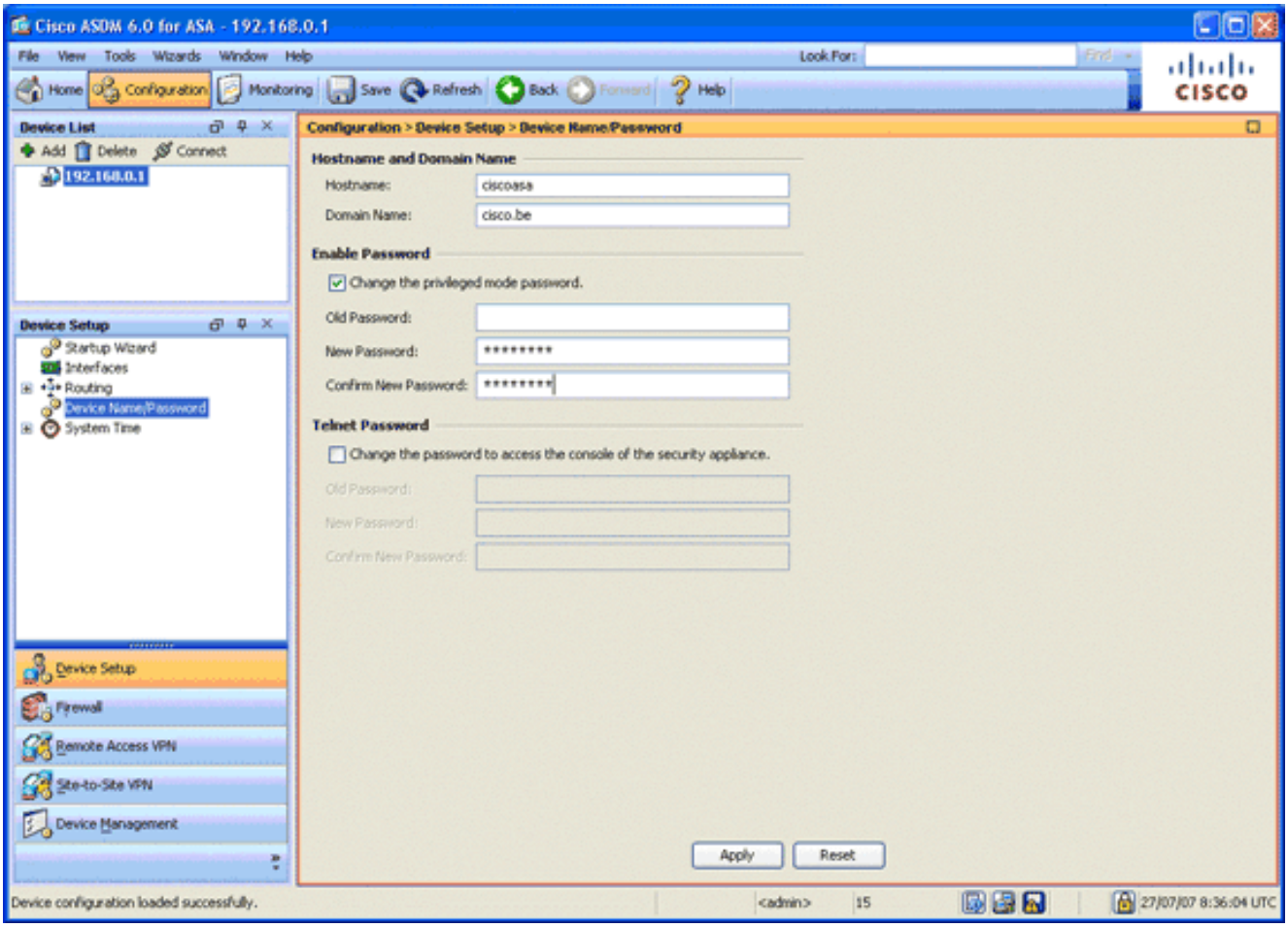


3. Seleccione la interfaz exterior y haga clic en **Editar**.
4. En la sección Dirección IP de la ficha General, elija la opción **Usar IP estática**.
5. Ingrese **197.0.100.1** para la dirección IP y **255.255.255.0** para la máscara de subred.
6. Haga clic en Apply (Aplicar).

Paso 2. Configure el nombre de dominio, la contraseña y la hora del sistema

Este paso describe cómo configurar el nombre de dominio, la contraseña y la hora del sistema.

1. En el área Device Setup , elija **Device Name/Password**
   .

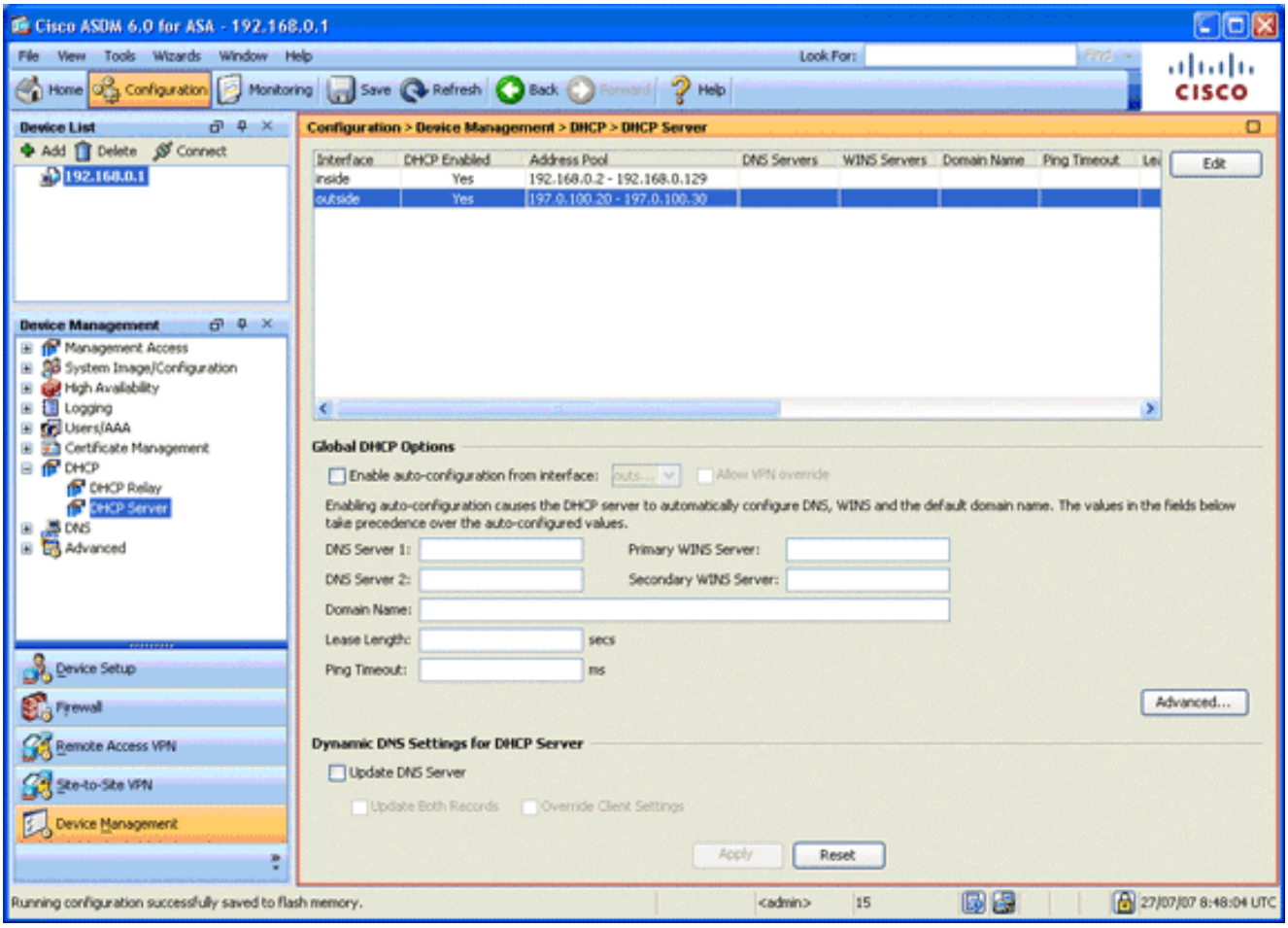


2. Ingrese **cisco.be** para el nombre de dominio e ingrese **cisco123** para el valor Enable Password.**Nota:** De forma predeterminada, la contraseña está en blanco.
3. Haga clic en Apply (Aplicar).
4. En el área Device Setup , elija **System Time** y cambie el valor del reloj (si es necesario).
5. Haga clic en Apply (Aplicar).

Paso 3. Habilite un servidor DHCP en la interfaz externa.

Este paso describe cómo habilitar un servidor DHCP en la interfaz exterior para facilitar las pruebas.

1. Haga clic en **Configuration** y luego en **Device Management**.
2. En el área Administración de dispositivos, expanda **DHCP** y elija **servidor DHCP**.

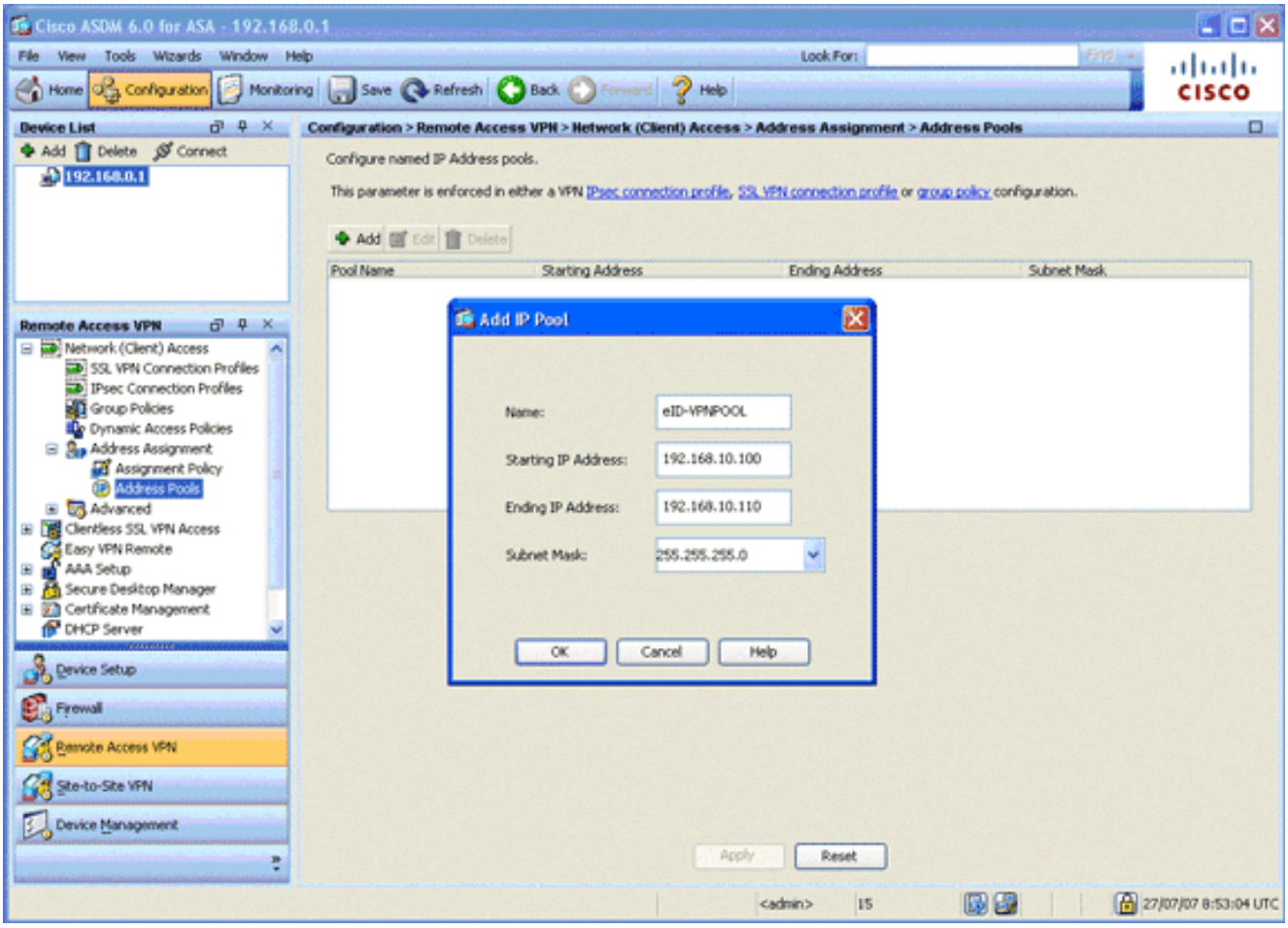


3. Seleccione la interfaz externa de la lista Interfaz y haga clic en **Editar**.Aparecerá el cuadro de diálogo Editar servidor DHCP.
4. Marque la casilla de verificación **Enable DHCP Server** .
5. En DHCP Address Pool, ingrese una dirección IP de 197.0.100.20 a 197.0.100.30.
6. En el área Opciones DHCP globales, desmarque la casilla de verificación **Habilitar configuración automática desde la interfaz**.
7. Haga clic en Apply (Aplicar).

Paso 4. Configure el eID VPN Address Pool

Este paso describe cómo definir un conjunto de direcciones IP que se utilizan para aprovisionar los clientes AnyConnect remotos.

1. Haga clic en **Configuration** y luego en **Remote Access VPN**.
2. En el área Remove Access VPN, expanda **Network (Client) Access** y luego expanda **Address Assignment**.
3. Elija **Conjuntos de Direcciones** y luego haga clic en el **botón Agregar** ubicado en el área Configurar agrupaciones de Direcciones IP con Nombre.Aparece el cuadro de diálogo Agregar Pool
   IP.



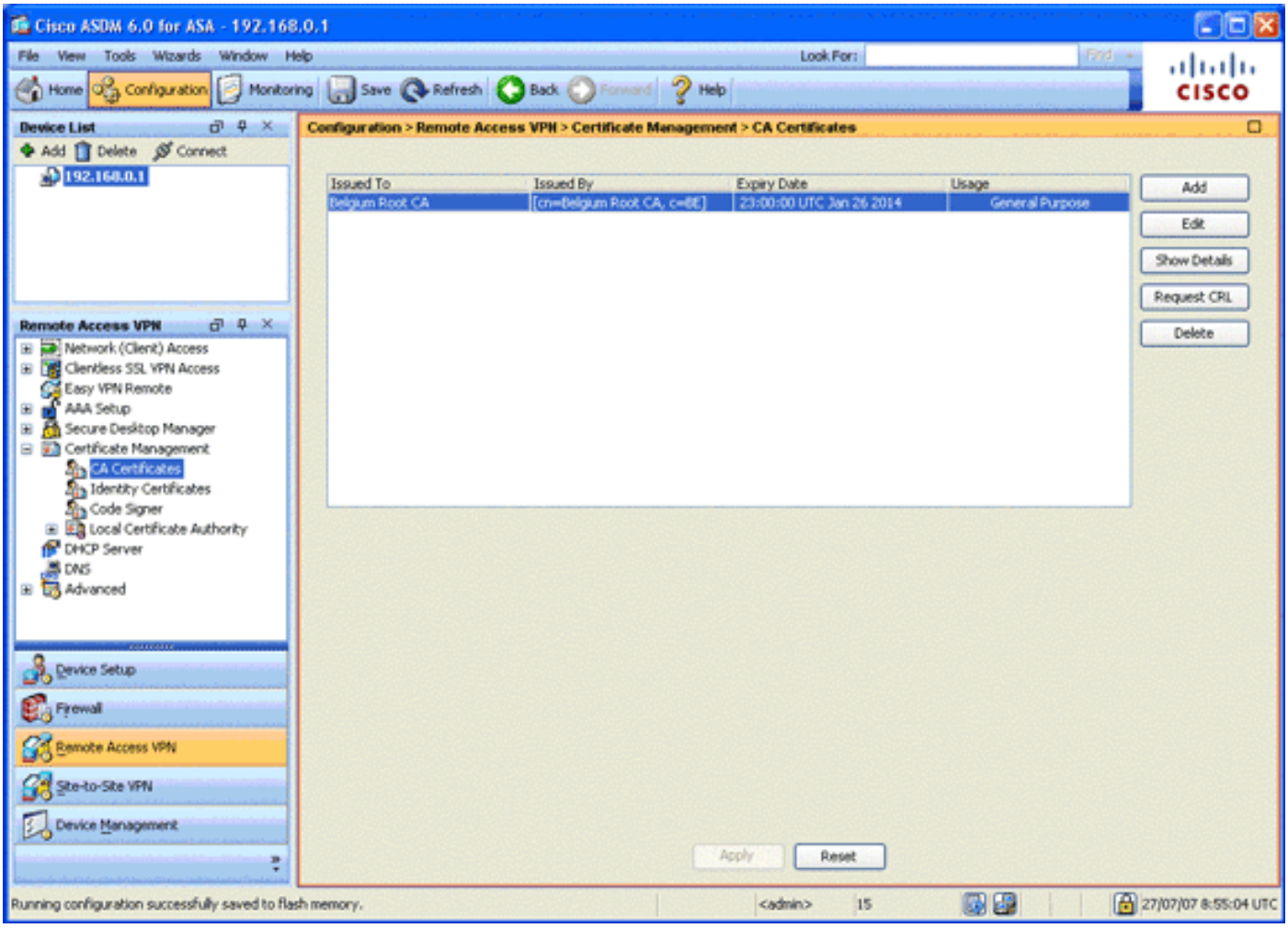
4. En el campo Nombre, ingrese **eID-VPNPOOL**.
5. En los campos Starting IP Address (Dirección IP inicial) y Ending IP Address (Dirección IP final), introduzca un intervalo de direcciones IP entre 192.168.10.100 y 192.168.10.110.
6. Elija **255.255.255.0** en la lista desplegable Máscara de subred, haga clic en **Aceptar** y, a continuación, haga clic en **Aplicar**.

Paso 5. Importar el certificado de CA raíz de Bélgica

Este paso describe cómo importar al ASA el certificado de CA raíz de Bélgica.

1. Descargue e instale los certificados de CA raíz de Bélgica (belgiumrca.crt y belgiumrca2.crt) del sitio web del gobierno y guárdelos en su equipo local.El sitio web del gobierno belga se encuentra en esta URL: http://certs.eid.belgium.be/
2. En el área Remote Access VPN, expanda **Certificate Management** y elija **CA Certificates**.
3. Haga clic en **Agregar** y, a continuación, haga clic en **Instalar desde el archivo**.
4. Busque la ubicación en la que guardó el archivo de certificado de CA raíz de Bélgica (belgiumrca.crt) y haga clic en **Instalar certificado**.
5. Haga clic en **Aplicar para guardar los cambios.**

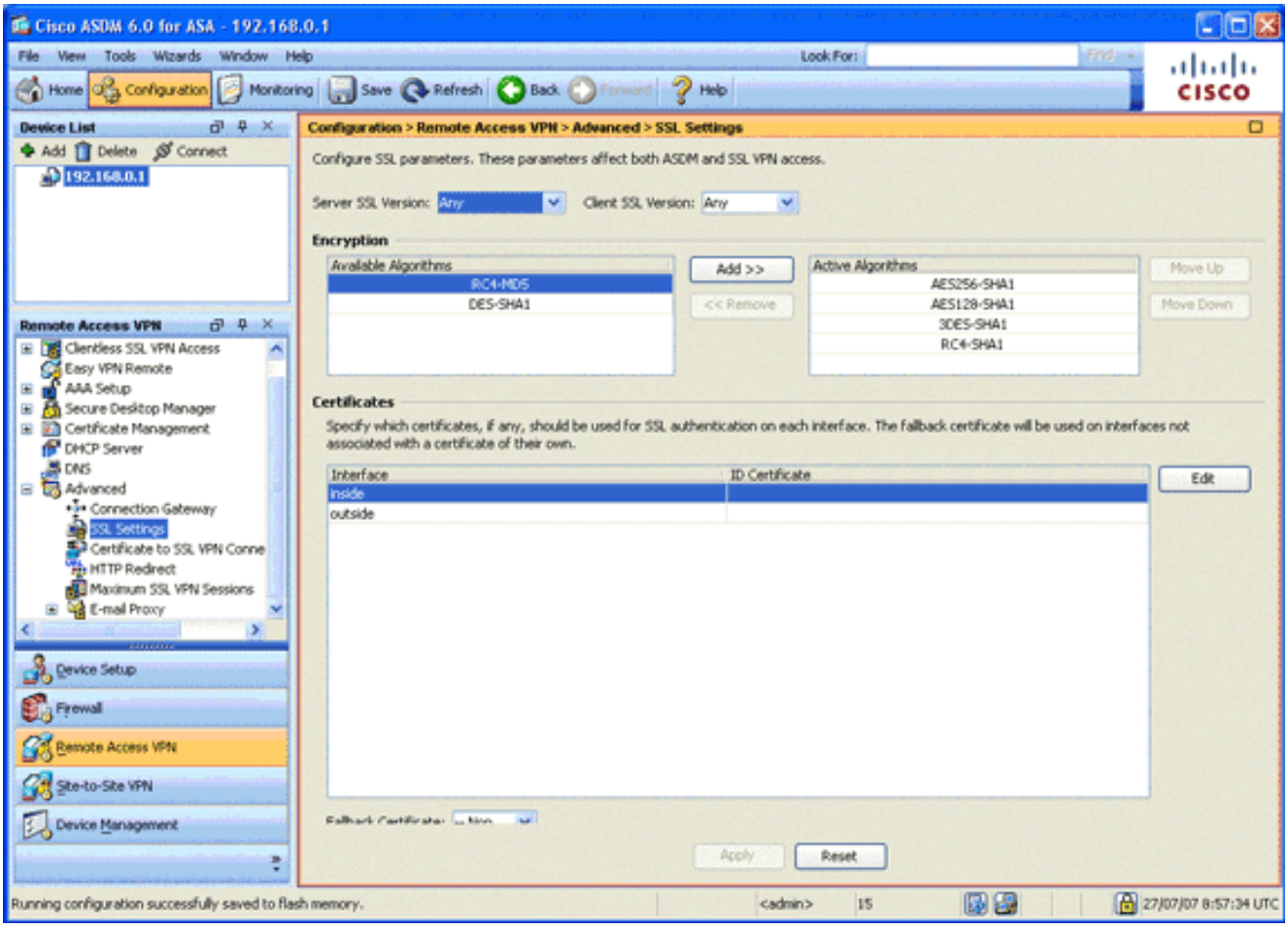
Esta imagen muestra el certificado instalado en el ASA:



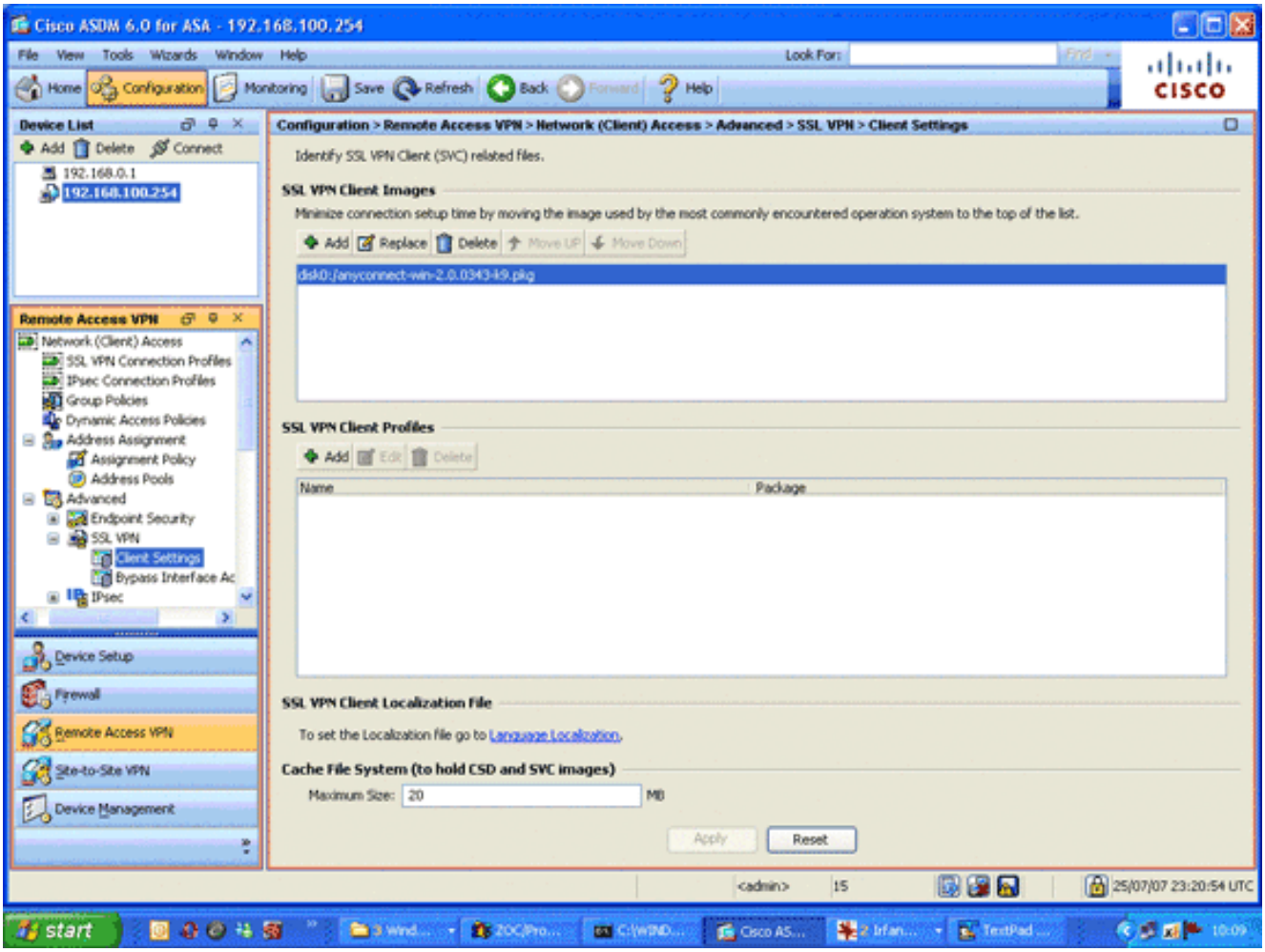
Paso 6. Configuración de la capa de sockets seguros

Este paso describe cómo dar prioridad a las opciones de cifrado seguro, definir la imagen del cliente SSL VPN y definir el perfil de conexión.

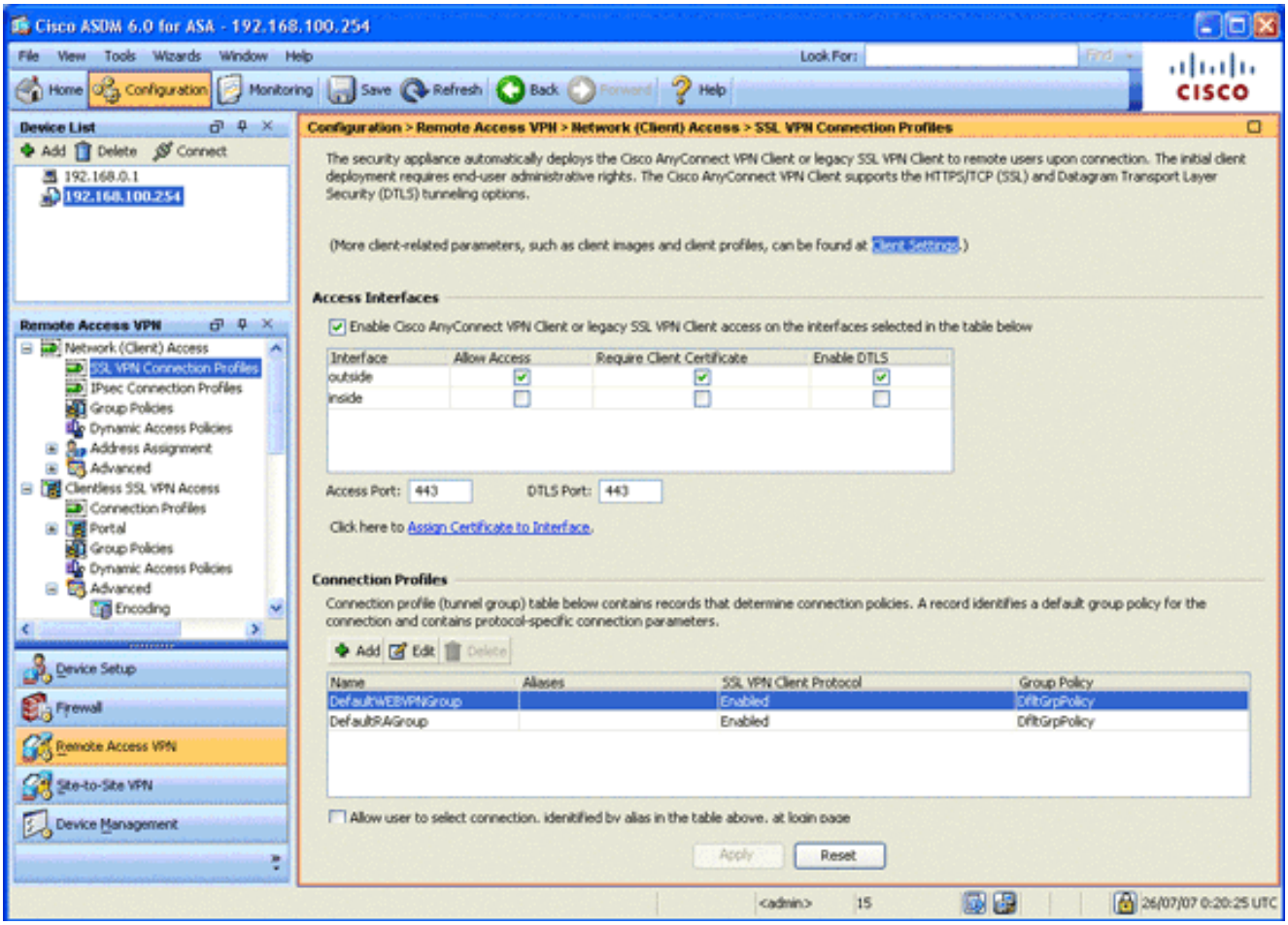
1. Dé prioridad a las opciones de cifrado más seguras.En el área Remote Access VPN, expanda **Advanced** y elija **SSL Settings**. En la sección Cifrado, los algoritmos activos se apilan, de arriba hacia abajo, de la siguiente manera:AES256-SHA1AES128-SHA13DES-SHA1RC4-
   SHA1



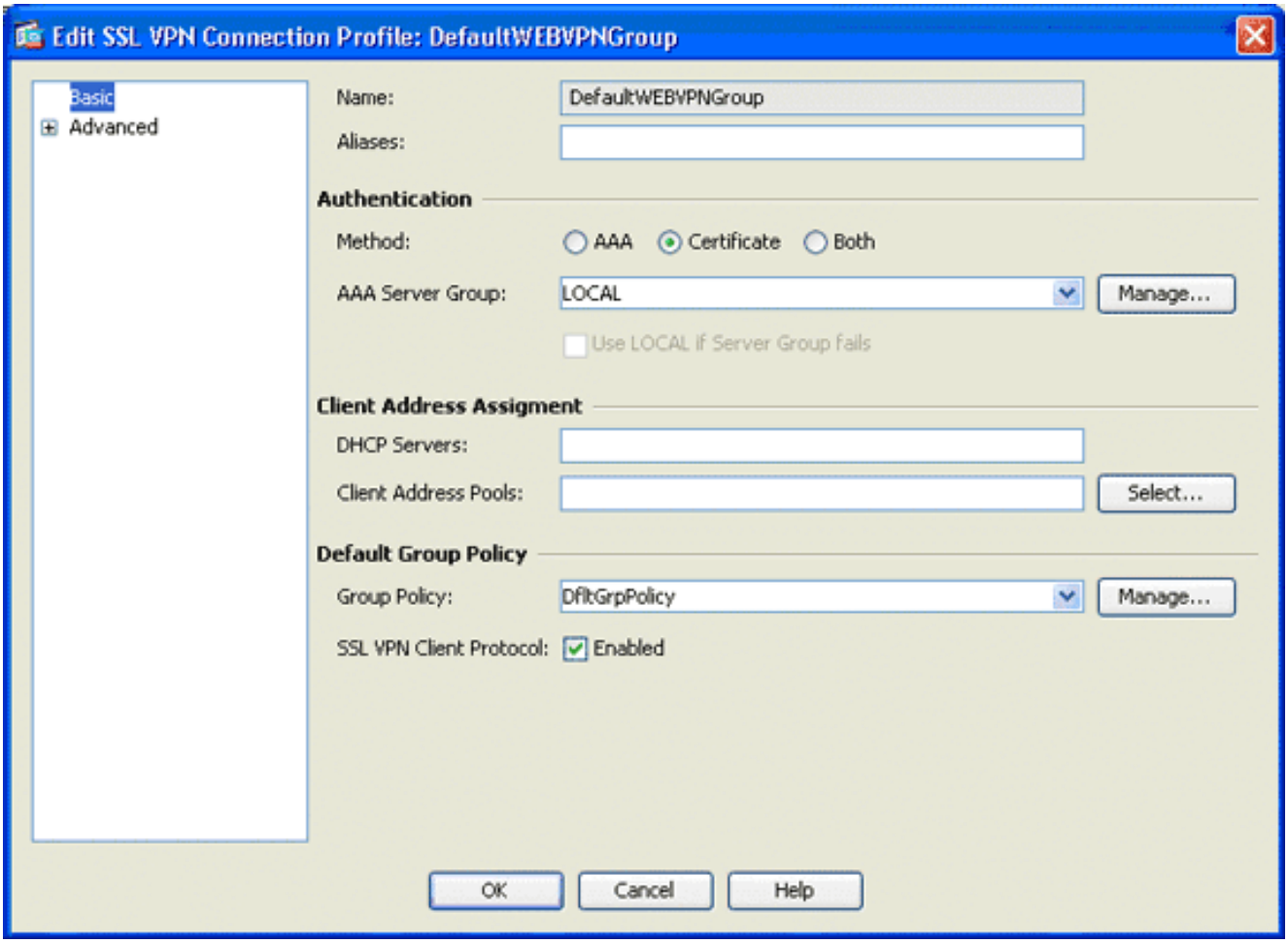
2. Defina la imagen de cliente VPN SSL para AnyConnect Client.En el área Remote Access VPN, expanda **Advanced**, expanda **SSL VPN** y elija **Client Settings**.En el área SSL VPN Client Images, haga clic en **Add**.Elija el paquete AnyConnect que se almacena en la memoria flash.El paquete AnyConnect aparece en la lista de imágenes de SSL VPN Client, como se muestra en esta
imagen:



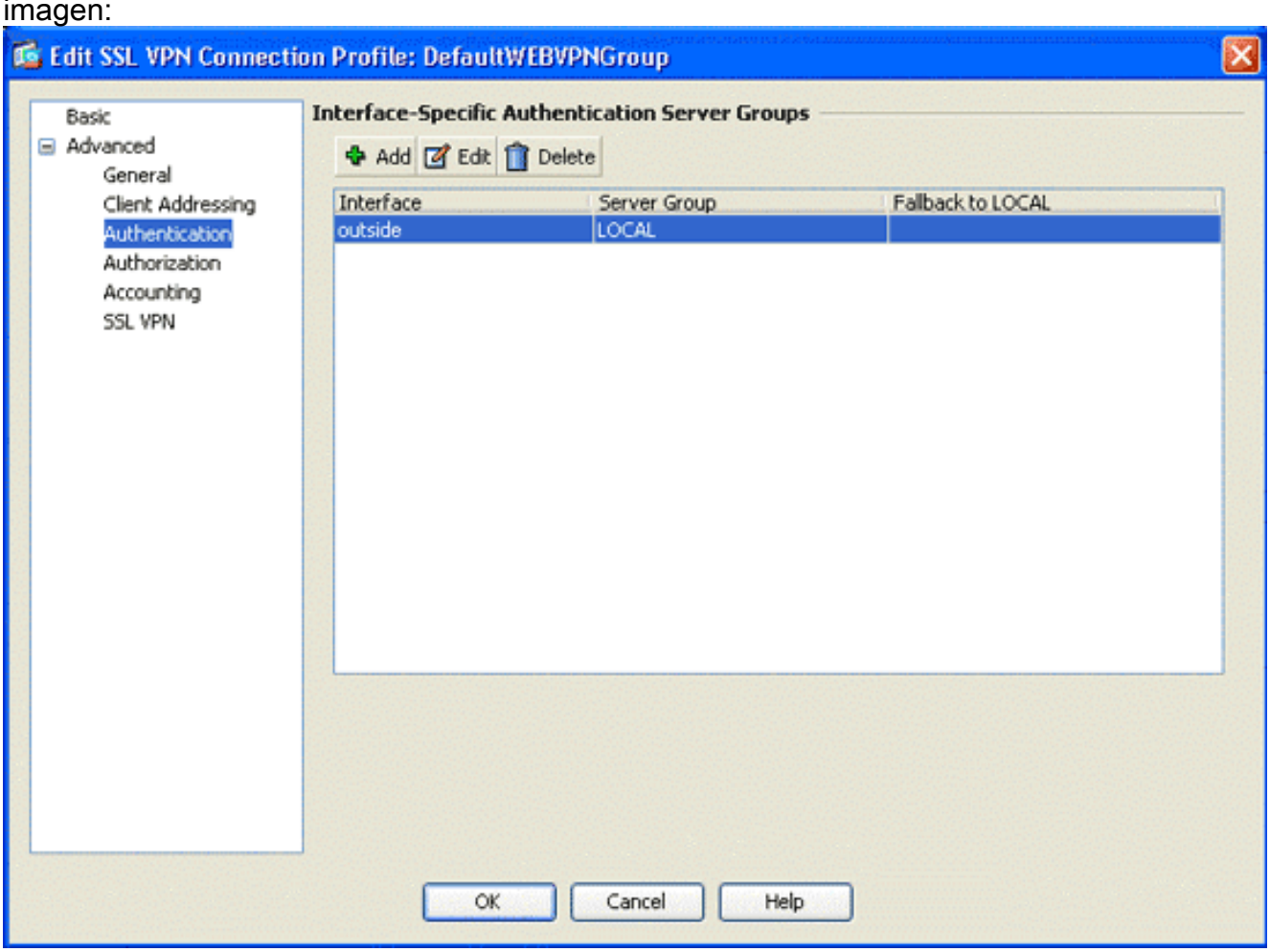
3. Defina el perfil de conexión DefaultWEBVPNGroup.En el área Remote Access VPN, expanda **Network (Client) Access** y elija **SSL VPN Connection Profiles**.En el área Interfaces de acceso, marque la **casilla de verificación Enable Cisco AnyConnect VPN Client**.Para la interfaz exterior, marque las casillas de verificación **Allow Access**, **Require Client Certificate** y **Enable DTLS**, como se muestra en esta imagen:



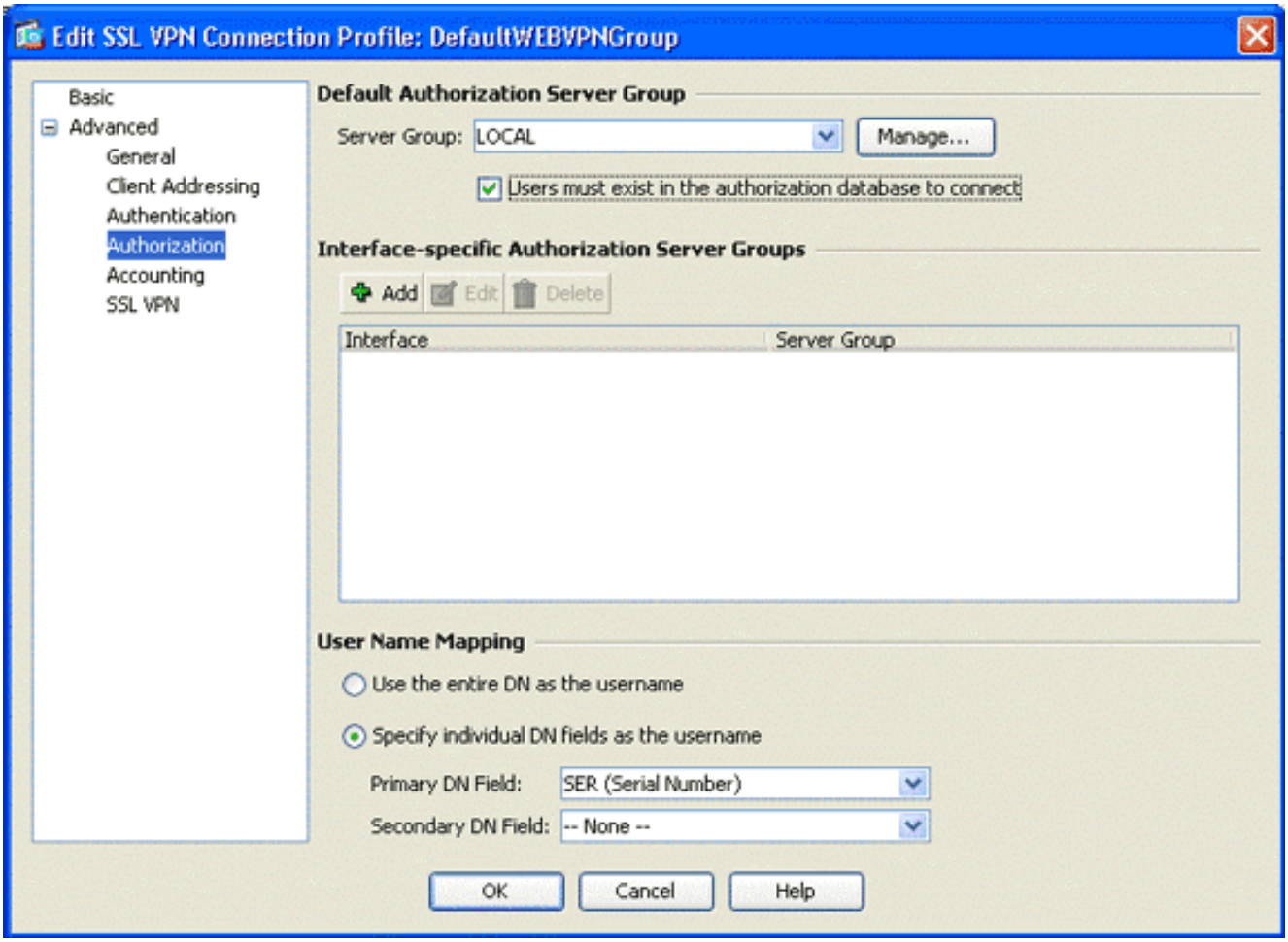
En el área Perfiles de Conexión, elija **DefaultWEBVPNGroup** y haga clic en **Editar**.Aparecerá el cuadro de diálogo Editar perfil de conexión VPN
SSL.



En el área de navegación, elija **Basic**.En el área Authentication (Autenticación), haga clic en el botón de opción **Certificate (Certificado)**.En el área Política de Grupo Predeterminada, marque la casilla de verificación **SSL VPN Client Protocol** .Expanda **Avanzado** y elija **Autenticación**.Haga clic en **Agregar** y agregue la interfaz exterior con un grupo de servidores local como se muestra en esta
imagen:



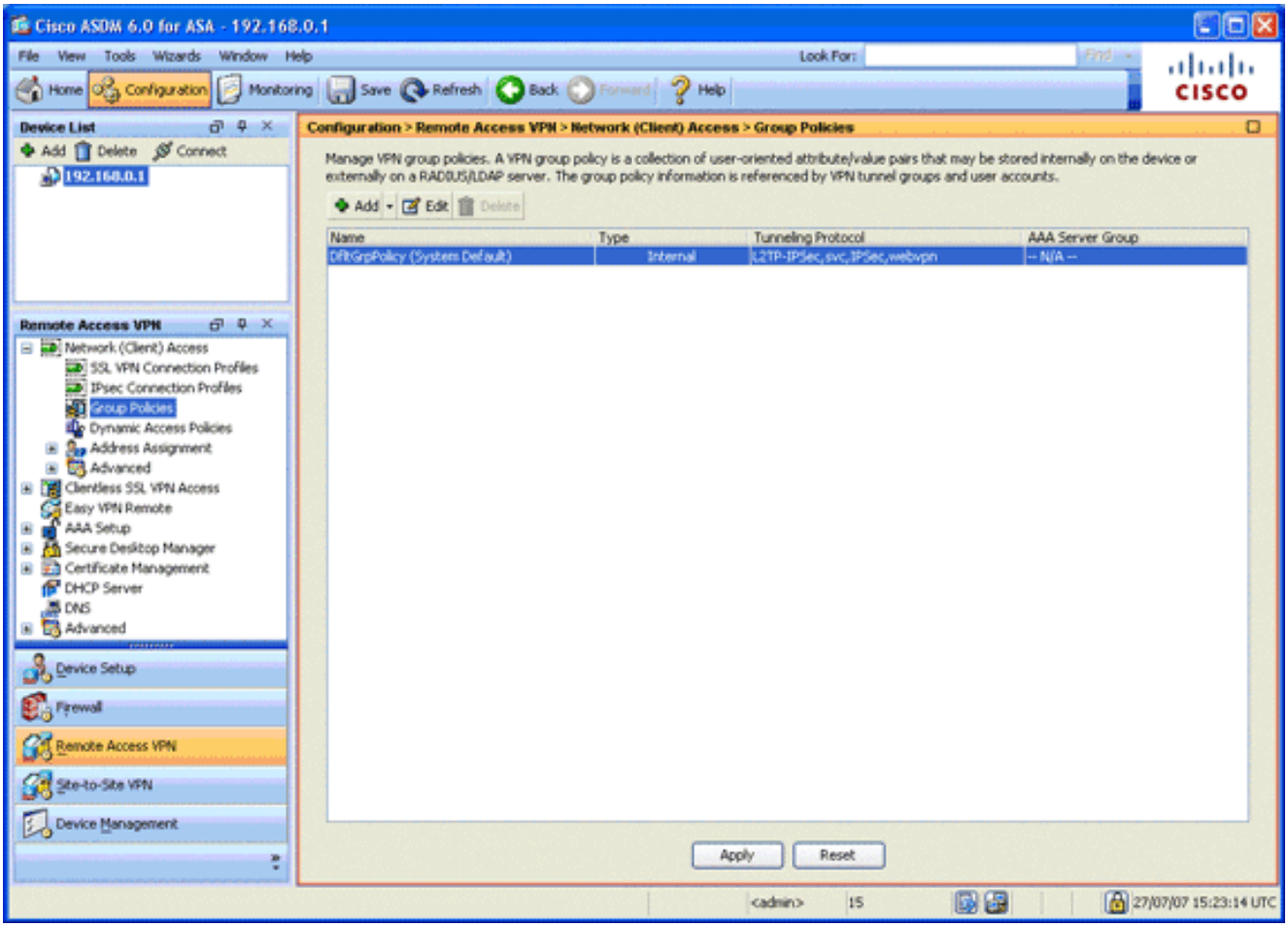
En el área de navegación, elija **Autorización**.En el área Default Authorization Server Group , elija **LOCAL** de la lista desplegable Server Group y marque la **casilla de verificación Users debe existir en la base de datos de autorización para conectarse**.En el área Asignación de nombre de usuario, elija **SER (Número de serie)** en la lista desplegable Campo DN principal, elija **Ninguno** en el Campo DN secundario y haga clic en
Aceptar.



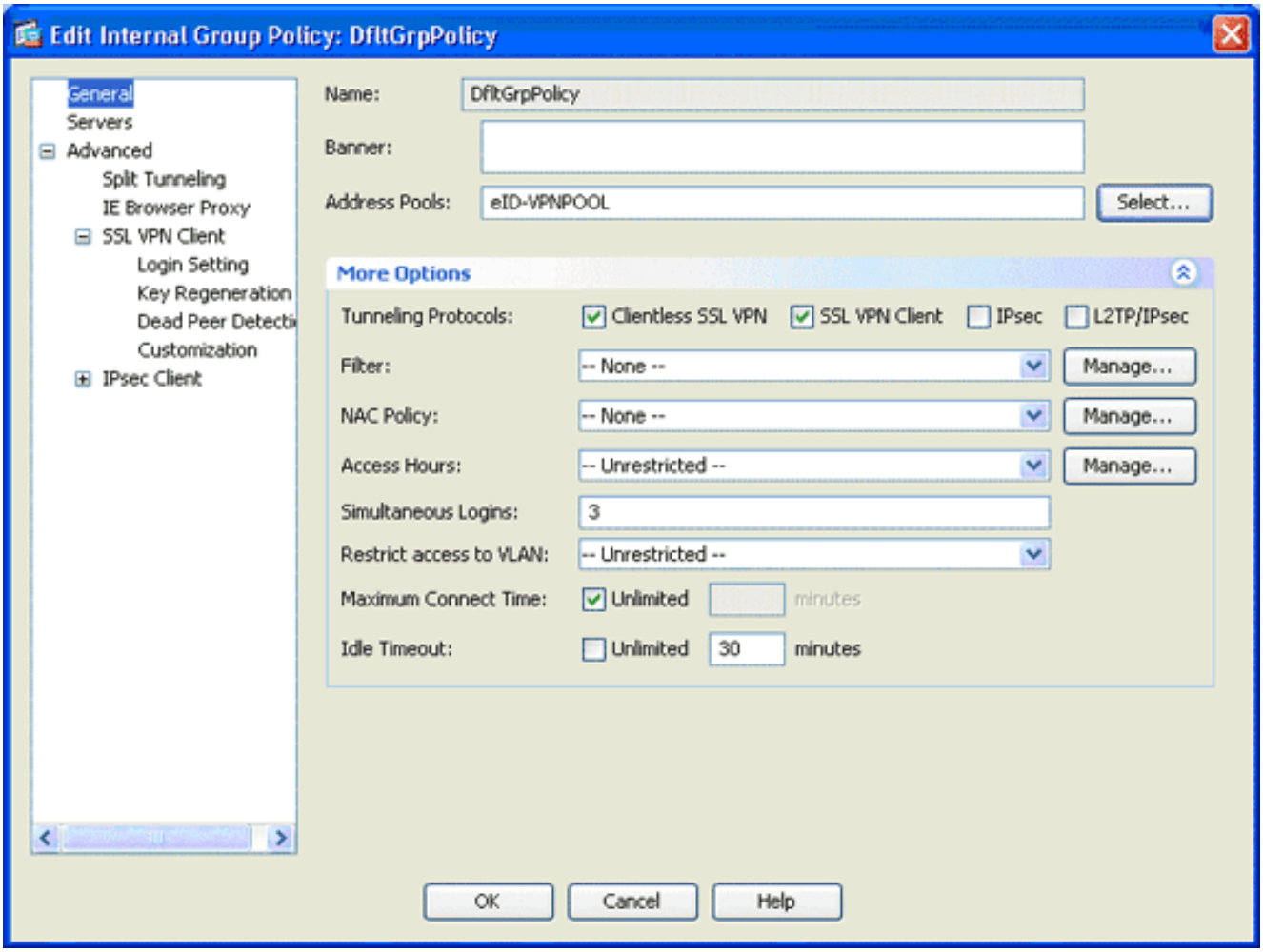
Paso 7. Definir la política de grupo predeterminada

Este paso describe cómo definir la política de grupo predeterminada.

1. En el área Remote Access VPN, expanda **Network (Client) Access** y elija **Group Policies**.



2. Elija **DfltGrpPolicy** de la lista de políticas de grupo y haga clic en **Editar**.
3. Aparecerá el cuadro de diálogo Editar política de grupo interna.

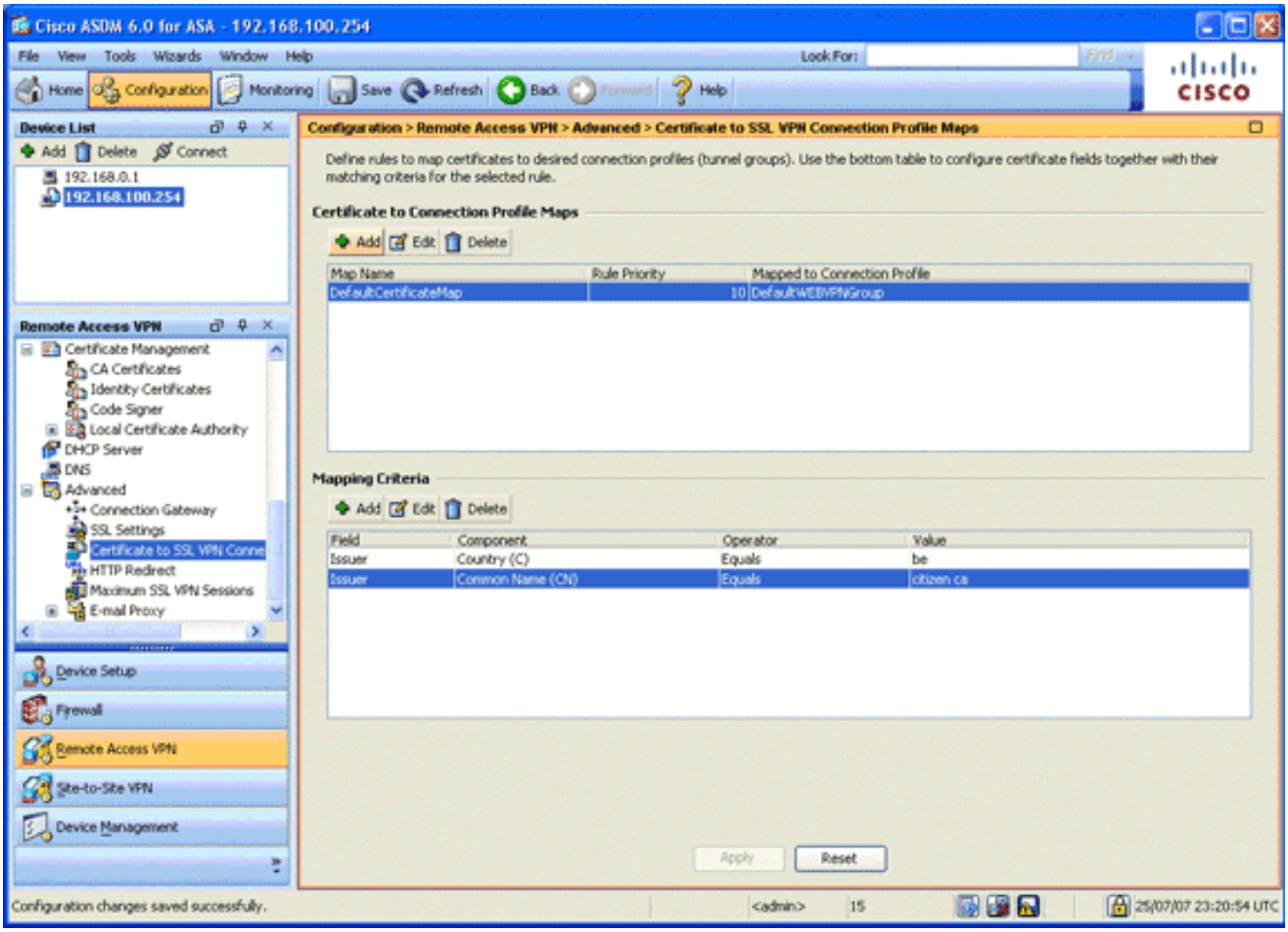


4. En el área de navegación, elija **General**.
5. Para los Conjuntos de Direcciones, haga clic en **Seleccionar** para elegir un conjunto de direcciones, y elija **eID-VPNPOOL**.
6. En el área More Options, desmarque las casillas de verificación **IPsec** y **L2TP/IPsec**, y haga clic en **OK**.

Paso 8. Definir la asignación de certificados

Este paso describe cómo definir los criterios de asignación de certificados.

1. En el área Remote Access VPN, haga clic en **Advanced** y elija **Certificate to SSL VPN Connection Profile Maps**.
2. En el área Certificate to Connection Profile Maps, haga clic en **Add** y elija **DefaultCertificateMap** en la lista de mapa.Este mapa debe coincidir con *DefaultWEBVPNProfile* en el campo Mapped to Connection Profile .
3. En el área Criterios de asignación, haga clic en **Agregar** y agregue estos valores:Campo: Emisor, País (C), Igual, "be"Campo: Emisor, nombre común (CN), igual a "ciudadano ca"Los criterios de asignación deben aparecer como se muestra en esta imagen:

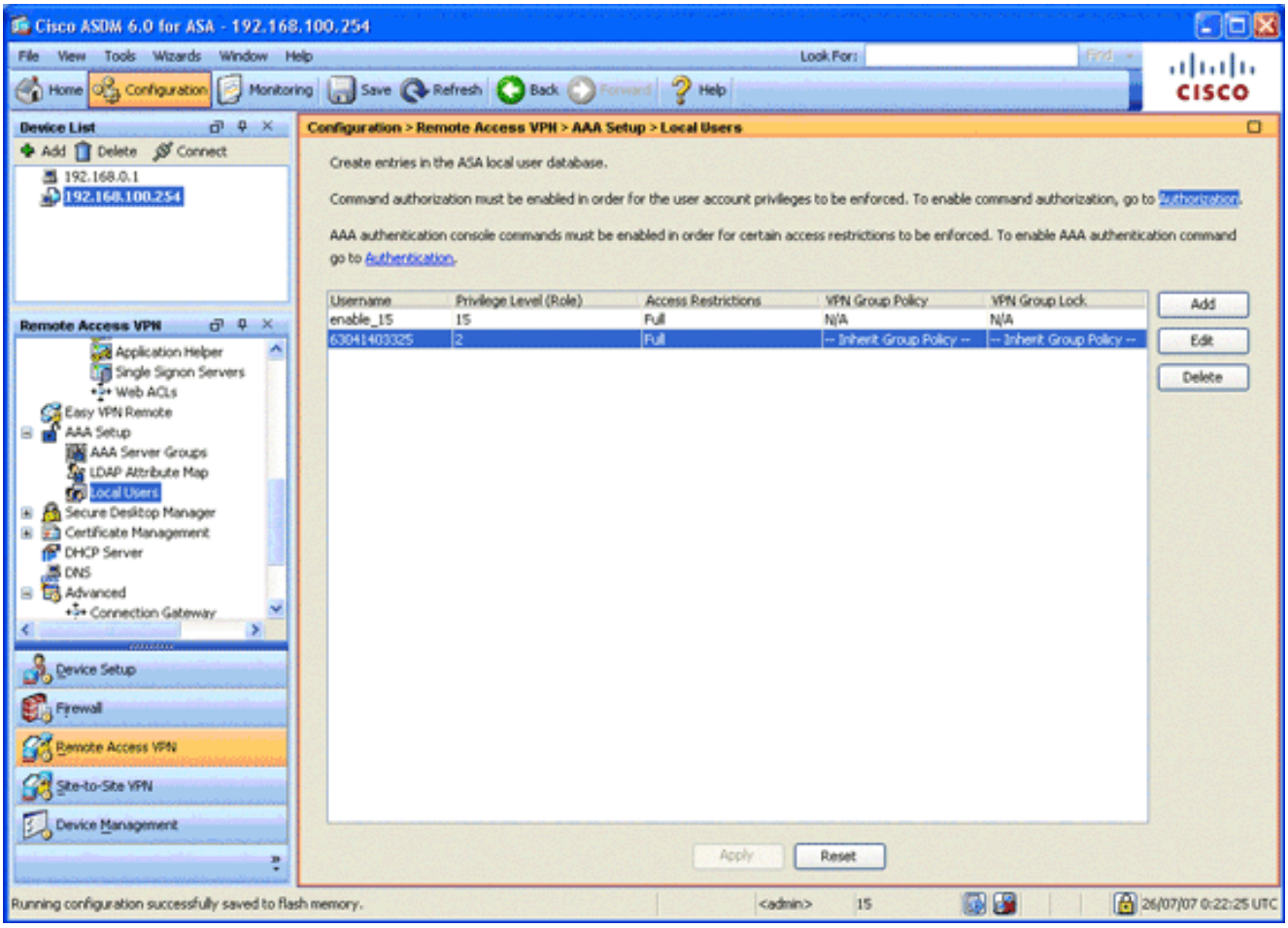


4. Haga clic en Apply (Aplicar).

Paso 9. Agregar un usuario local

Este paso describe cómo agregar un usuario local.

1. En el área Remote Access VPN, expanda **AAA Setup** y elija **Local Users**.
2. En el área Usuarios locales, haga clic en **Agregar**.
3. En el campo Nombre de usuario, introduzca el número de serie del certificado de usuario. Por ejemplo, 56100307215 (como se describe en la sección Certificado de Autenticación de este
documento).



4. Haga clic en Apply (Aplicar).

Paso 10. Reinicie ASA

Reinicie el ASA para asegurarse de que todos los cambios se apliquen a los servicios del sistema.

Ajuste

Durante la prueba, es posible que algunos túneles SSL no se cierren correctamente. Dado que el ASA asume que el cliente AnyConnect puede desconectarse y reconectarse, el túnel no se descarta, lo que le da la oportunidad de volver. Sin embargo, durante las pruebas de laboratorio con una licencia base (2 túneles SSL de forma predeterminada), puede agotar la licencia cuando los túneles SSL no se cierren correctamente. Si ocurre este problema, utilice el comando **vpn-sessiondb logoff <*option*>** para cerrar todas las sesiones SSL activas.

Configuración de un minuto

Para crear rápidamente una configuración en funcionamiento, restablezca su ASA al valor predeterminado de fábrica y pegue esta configuración en el modo de configuración:

ciscoasa
ciscoasa#**conf t** ciscoasa#**clear configure all** ciscoasa#**domain-name cisco.be**

```
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
```

Información Relacionada

- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems