# ASA 8.x AnyConnect-Authentifizierung mit der belgischen eID-Karte

# Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Lokale PC-Einrichtung Betriebssystem Kartenleser eID Laufzeitsoftware Authentifizierungszertifikat Installation von AnyConnect ASA-Anforderungen **ASA-Konfiguration** Schritt 1: Aktivieren der externen Schnittstelle Schritt 2: Konfigurieren von Domänenname, Kennwort und Systemzeit Schritt 3: Aktivieren Sie einen DHCP-Server auf der externen Schnittstelle. Schritt 4: Konfigurieren des elD-VPN-Adresspools Schritt 5: Importieren des Zertifikats der belgischen Stammzertifizierungsstelle Schritt 6: Konfigurieren der Secure Sockets Layer Schritt 7: Definieren der Standardgruppenrichtlinie Schritt 8: Definieren der Zertifikatszuordnung Schritt 9: Hinzufügen eines lokalen Benutzers Schritt 10: Neustarten der ASA Feineinstellung Einminütige Konfiguration Zugehörige Informationen

# **Einführung**

Dieses Dokument beschreibt, wie Sie die ASA 8.x AnyConnect-Authentifizierung für die Verwendung der belgischen eID-Karte einrichten.

# Voraussetzungen

### **Anforderungen**

Für dieses Dokument bestehen keine speziellen Anforderungen.

#### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA 5505 mit der entsprechenden ASA 8.0-Software
- AnyConnect-Client
- ASDM 6.0

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

## **Hintergrundinformationen**

Die elD ist eine PKI-Karte (Public Key Infrastructure), die von der belgischen Regierung ausgestellt wurde und von den Benutzern zur Authentifizierung auf einem Remote-Windows-PC verwendet werden muss. Der AnyConnect-Software-Client wird auf dem lokalen PC installiert und erhält Authentifizierungsinformationen vom Remote-PC. Sobald die Authentifizierung abgeschlossen ist, erhält der Remote-Benutzer über einen vollständigen SSL-Tunnel Zugriff auf die zentralen Ressourcen. Der Remote-Benutzer erhält eine IP-Adresse, die aus einem von der ASA verwalteten Pool stammt.

# Lokale PC-Einrichtung

#### **Betriebssystem**

Das Betriebssystem (Windows, MacOS, Unix oder Linux) auf Ihrem lokalen PC muss mit allen erforderlichen Patches auf dem neuesten Stand sein.

#### **Kartenleser**

Um die eID-Karte verwenden zu können, muss ein elektronisches Kartenlesegerät auf Ihrem lokalen Computer installiert sein. Der elektronische Kartenleser ist ein Hardwaregerät, das einen Kommunikationskanal zwischen den Programmen auf dem Computer und dem Chip auf der ID-Karte herstellt.

Eine Liste der zugelassenen Kartenleser finden Sie unter: <u>http://www.cardreaders.be/en/default.htm</u>

Hinweis: Um das Kartenlesegerät verwenden zu können, müssen Sie die vom Hardwareanbieter empfohlenen Treiber installieren.

#### elD Laufzeitsoftware

Sie müssen die von der belgischen Regierung bereitgestellte elD-Laufzeitsoftware installieren. Mit dieser Software kann der Remote-Benutzer den Inhalt der elD-Karte lesen, validieren und drucken. Die Software ist für Windows, MAC OS X und Linux auf Französisch und Niederländisch verfügbar.

Weitere Informationen finden Sie unter:

<u>http://www.belgium.be/zip/eid\_datacapture\_nl.html</u>

#### Authentifizierungszertifikat

Sie müssen das Authentifizierungszertifikat in den Microsoft Windows-Speicher auf dem lokalen PC importieren. Wenn Sie das Zertifikat nicht in den Speicher importieren, kann der AnyConnect Client keine SSL-Verbindung zur ASA herstellen.

#### Vorgehensweise

Gehen Sie wie folgt vor, um das Authentifizierungszertifikat in den Windows-Speicher zu importieren:

 Legen Sie Ihre eID in den Kartenleser ein, und starten Sie die Middleware, um auf den Inhalt der eID-Karte zuzugreifen.Der Inhalt der eID-Karte wird angezeigt.

| 🚥 Carte d'identité                               |   |                                     |                 | <b>E</b>   |   |
|--|---|-------------------------------------|-----------------|--|---|
| 😑 🗆 🖨 🗶  | San   | SC SHEEP CONTRACTOR SHE             | Sec. Sec.       | alan dan dan dan dari bertekan dari bertekan dari bertekan dari bertekan dari bertekan dari bertekan dari berte<br>Bertekan dari bertekan dari b |   |
| Identité Certificats Carte & PIN Option          | s Info  |                                     |                 |  |   |
| BELGIQUE   | BELGIË  | BELGIEN                             | BE              | LGIUM  |   |
| CARTE D'IDENTITE                                 | IDENTITEITSKAART  | PERSONALAUSWEIS                     | ID              | ENTITY CARD  |   |
|  | Identité  |                                     |                 |  |   |
|  | Nom   |                                     |                 |  |   |
|  |   |                                     |                 |  |   |
|  | Piénoms   |                                     |                 |  | E |
|  | Lieu de naissance   | Date de naissance                   | Sexe            | Nationalté   | - |
|  |   | 14/04/1963                          | M               | be   |   |
|  | Titre   |                                     | Numéro national |  |   |
|  |   |                                     | 63.04.14-033.28 | i  |   |
| Carte  | Adresse   |                                     |                 |  |   |
| Numero de la puce<br>534C494E336600296CEE2715071 | 82C36   |                                     |                 |  |   |
| Numéro de la carte                               | Code postal Comm  | une                                 |                 | Pays   | - |
| 590.5942800.24                                   |   |                                     |                 | be   |   |
| Valide du Au<br>07/06/2007 07/06/2012            | Statut spécial  |                                     |                 |  |   |
| Commune d'émission                               | Canne blanche   |                                     |                 |  |   |
|  | Canne jaune   |                                     | 1               |  |   |
|  | Minorité étendue  |                                     | 1               |  |   |
|  |   |                                     |                 |  |   |
|  |   |                                     | × -             |  |   |
|  |   |                                     |                 | i dan ing  |   |
|  |   |                                     |                 | 10 M   |   |
|  |   |                                     | 221.            | A State of the   |   |
|  |   |                                     |                 | ALL & F ALL  |   |
| Fini   | Street de la de | and a second a second second second |                 |  |   |

2. Klicken Sie auf die Registerkarte **Certificats** (FR).Die Zertifikathierarchie wird angezeigt.

| 🖛 Carte d'identité   |   | 300  |
|--|---|--|
| 1 🔁 🖬 🎒 🛪<br>Identité Certificats Carte & PIN Options Info   |   |  |
| Certificats    BELPIC  Citizen CA  Citizen | Propriétaire<br>(Authern<br>Émetteur<br>Citizen CA<br>Longueur de clé<br>1024 bits<br>Valide du<br>15/06/2007<br>Statut du certificat<br>Non validé<br>Les certificats de la carte e<br>utiliser la carte d'identité él<br>OpenOffice.org. Adobe Re<br>sélectionnez-le et cliquez s | Au<br>08/06/2012<br>ND doivent être enregistrés dans Windows pour pouvoir<br>ectronique dans Internet Explorer, Microsoft Office,<br>ader, Outlook, Pour enregistrer un certificat,<br>ur le bouton « Enregistrer ». |
|  |   |  |
| Eni  |   |  |

- 3. Erweitern Sie Belgium Root CA, und erweitern Sie dann Citizen CA.
- 4. Wählen Sie die Authentifizierungsversion Ihres benannten Zertifikats aus.
- 5. Klicken Sie auf die Schaltfläche **Anmelder** (FR).Das Zertifikat wird in den Windows-Speicher kopiert.

**Hinweis:** Wenn Sie auf die Schaltfläche **Details** klicken, wird ein Fenster mit Details zum Zertifikat angezeigt. Wählen Sie auf der Registerkarte Details das Feld **Betreff** aus, um das Feld Seriennummer anzuzeigen. Das Feld Seriennummer enthält einen eindeutigen Wert, der für die Benutzerautorisierung verwendet wird. Beispielsweise stellt die Seriennummer "56100307215" einen Benutzer dar, dessen Geburtsdatum der 3. Oktober 1956 ist, dessen Seriennummer 072 und die Prüfziffer 15 lautet. *Um diese Nummern zu speichern, müssen Sie bei den Bundesbehörden eine Genehmigung einreichen. Es liegt in Ihrer Verantwortung, die entsprechenden offiziellen Erklärungen zur Pflege einer Datenbank belgischer Bürger in Ihrem Land abzugeben.* 

#### Überprüfen

Gehen Sie wie folgt vor, um zu überprüfen, ob das Zertifikat erfolgreich importiert wurde:

- 1. Öffnen Sie auf einem Windows XP-Computer ein DOS-Fenster, und geben Sie den **mmc-**Befehl ein.Die Konsolenanwendung wird angezeigt.
- 2. Wählen Sie **Datei > Snap-In hinzufügen/entfernen aus** (oder drücken Sie Strg+M).Das Dialogfeld zum Hinzufügen/Entfernen von Snap-Ins wird angezeigt.
- 3. Klicken Sie auf die Schaltfläche **Hinzufügen**.Das Dialogfeld Standalone Snap-In hinzufügen wird angezeigt.
- 4. Wählen Sie in der Liste Verfügbare eigenständige Snap-Ins die Option **Zertifikate aus**, und klicken Sie auf **Hinzufügen**.
- 5. Klicken Sie auf das Optionsfeld **Mein Benutzerkonto** und anschließend auf **Fertig stellen**.Das Snap-In Zertifikat wird im Dialogfeld Snap-In hinzufügen/entfernen angezeigt.
- 6. Klicken Sie auf **Schließen**, um das Dialogfeld Standalone Snap-In hinzufügen zu schließen, und klicken Sie dann im Dialogfeld Add/Remove Snap-In auf **OK**, um die Änderungen zu speichern und zur Konsolenanwendung zurückzukehren.
- 7. Erweitern Sie unter dem Ordner Konsolenstamm die Option Zertifikate Aktueller Benutzer.
- 8. Erweitern Sie **Personal**, und erweitern Sie dann **Zertifikate**.Das importierte Zertifikat muss wie in diesem Bild gezeigt im Windows-Speicher angezeigt werden:

| 🚡 Console1 - [Console Root/Certificates - Current User/Personal/Certificates]   |  |            |                 |                       |       |  |  |  |
|---|--|------------|-----------------|-----------------------|-------|--|--|--|
| 📸 File Action View Favorites Wine   | File Action View Favorites Window Help |            |                 |                       |       |  |  |  |
|   |  |            |                 |                       |       |  |  |  |
| Console Root  | Issued To 🕖                            | Issued By  | Expiration Date | Intended Purposes     | Frier |  |  |  |
| Certificates - Current User     Personal     Certificates     Trusted Root Certification Author     Determediate Certification Author     Active Directory User Object     Trusted Publishers     Untrusted Certificates     Third-Party Root Certification Au     Trusted People     Other     Other     Certificate Enrollment Requests | (Authentication)                       | Citizen CA | 8/06/2012       | Client Authentication | Clé c |  |  |  |
|   | <                                      |            |                 |                       | >     |  |  |  |
| Personal store contains 1 certificate.  |  |            |                 |                       |       |  |  |  |

# Installation von AnyConnect

Sie müssen den AnyConnect Client auf dem Remote-PC installieren. Die AnyConnect-Software verwendet eine XML-Konfigurationsdatei, die bearbeitet werden kann, um eine Liste der verfügbaren Gateways vorzusehen. Die XML-Datei wird in diesem Pfad auf dem Remote-PC gespeichert:

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

wobei %USERNAME% der Name des Benutzers auf dem Remote-PC ist.

Der Name der XML-Datei lautet preferences.xml. Hier ein Beispiel für den Inhalt der Datei:

<?xml version="1.0" encoding="UTF-8"?> <AnyConnectPreferences> <DefaultHost>192.168.0.1</DefaultHost> </AnyConnectPreferences> wobei 192.168.0.1 die IP-Adresse des ASA-Gateways ist.

# ASA-Anforderungen

Stellen Sie sicher, dass die ASA diese Anforderungen erfüllt:

 AnyConnect und ASDM müssen im Flash-Speicher ausgeführt werden.Um die in diesem Dokument beschriebenen Verfahren abzuschließen, verwenden Sie eine ASA 5505-Appliance, auf der die entsprechende ASA 8.0-Software installiert ist. Die AnyConnect- und ASDM-Anwendungen müssen im Flash-Speicher vorgeladen werden. Verwenden Sie den Befehl **show flash**, um den Inhalt des Flash anzuzeigen:

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 muss mit den Werkseinstellungen ausgeführt werden. Sie können diese Anforderung überspringen, wenn Sie ein neues ASA-Chassis verwenden, um die in diesem Dokument beschriebenen Verfahren abzuschließen. Gehen Sie andernfalls wie folgt vor, um die ASA auf die Werkseinstellungen zurückzusetzen:Stellen Sie in der ASDM-Anwendung eine Verbindung zum ASA-Chassis her, und wählen Sie Datei > Gerät auf die werkseitige Standardkonfiguration zurücksetzen

| Cisco ASDM 6.0 for ASA        | 192.168.100.254                 |              |                     |                              |                                   |                                       |  |                |
|-------------------------------|---------------------------------|--------------|---------------------|------------------------------|-----------------------------------|---------------------------------------|--|----------------|
| Wew Tools Wizards V           | Andow Help                      |              |                     |                              | Look P                            | lors -                                | Find +                                 | l l.           |
| Refresh ASDM with the Runn    | ing Configuration on the Device | 15 🗅         | Back CD F           | werd 🤊 Help                  |                                   |                                       |  | cisco          |
| Reset Device to the Factory   | Default Configuration           |              |                     | 3                            |                                   |                                       |  |                |
| Show Running Configuration    | in New Window                   |              | and Death to a      |                              |                                   |                                       |  |                |
| Save Running Configuration    | o Flash                         | Ctrl+S       | ewai Lasribuc       | ru                           |                                   |                                       |  |                |
| Save Running Configuration    | to TFTP Server                  | -            |                     |                              |                                   | Interface Sta                         | itus                                   |                |
| Save Running Configuration    | n Standby Link                  |              |                     |                              |                                   | Interface                             | IP Address/Mask.<br>192.168.100.254/24 | Q up           |
| Save Internal Los Buffer to J | lach                            | isc          | o.be                |                              |                                   | outside                               | 192.168.0.1/24                         | o down         |
| Date alterna boy barrer to r  |                                 | -            | Device              | Uptime: Od Oh 14             | m 21s                             |                                       |  |                |
| PTICK                         |                                 | <u>C</u> M+P | Device              | Type: ASA 550                | 5                                 |                                       |  |                |
| Clear ASDM Cache              |                                 |              | Conte:              | t Mode: Single               |                                   |                                       |  |                |
| Clear Internal Log Buffer     |                                 |              | Total M             | lemory: 256 MB               |                                   | Salut as inter                        | face to view incut and outer           | ***            |
| Exit                          |                                 | At+F4        |                     |                              |                                   | Select an incen                       | race to view input and outp            | UK NDES        |
|                               | VPN Tunnels                     |              |                     |                              |                                   | Traffic Statu                         |  |                |
|                               | IKE: 0 IPse                     | x: 0 (       | Clientless 55L      | VPN: 0 SSL                   | VPN Client: 0                     | Connection                            | s Per Second Usage                     |                |
|                               | System Resource                 | e Statue     |                     |                              |                                   | 21                                    |  |                |
|                               | CRU CRUIA                       | ann (nerrer  | (to                 |                              |                                   | 1                                     |  |                |
|                               |                                 | sage (perces | in, /               |                              |                                   |                                       |  |                |
|                               | 20                              |              |                     |                              | -                                 | 0                                     | 22:47 22:48                            | 22:49          |
|                               | 12% 10                          |              |                     |                              |                                   | UDP;                                  | 0 📕 TCP: 0 📕 Total: (                  | )              |
|                               | 22.51.02                        | 22:40        | 7 22:4              | 22:40                        | 22:50 2                           | 2.5 'outside' In                      | terface Traffic Usage (K               | bps)           |
|                               | Memory Memo                     | ry lisage (M | (11)                |                              |                                   | 1                                     |  |                |
|                               | Cleanory Cleano                 | ry usage (-  | ,                   |                              |                                   |                                       |  |                |
|                               | 200 -                           |              |                     |                              |                                   | 0                                     | 00:56 00:57                            | 00:58          |
|                               | 834% 100                        |              |                     |                              |                                   |                                       | Interface                              | is down.       |
|                               | 0.4                             |              |                     | and the states               |                                   | -                                     |  |                |
|                               | Latest ASDM Syslog              | Messages     |                     |                              |                                   |                                       |  | 000            |
|                               | Severity Date                   | 22:51:07     | Syslog ID<br>106015 | Source IP<br>192,168,100,100 | Destination IP<br>192,168,100,254 | Description<br>Deny TCP (no connectio | n) from 192,168,100,100/1              | 114 to 19: A   |
|                               | A 6 3.4 26 2007                 | 22:51:07     | 302014              | 192.168.100.100              | 192.168.100.254                   | Teardown TCP connects                 | on 34 for inside:192.168.10            | 0.100/111      |
|                               | 4 6 Ad 26 2007                  | 22:51:07     | 106015              | 192.168.100.100              | 192-168-100-254                   | Deny TCP (no connectio                | n) from 192.168.100.100/1              | 113 to 19;     |
|                               | A 6 3.4 26 2007                 | 22:51:07     | 302014              | 192.168.100.100              | 192.168.100.254                   | Teardown TCP connecti                 | on 33 for inside:192.168.10            | 0.100/111      |
|                               |                                 | an and       |                     |                              |                                   |                                       |  | 2              |
| e configuration loaded surces | fully.                          |              |                     |                              | cadmin>                           | 15                                    | - A 26/                                | 07/07 22:51:00 |

Lassen Sie die Standardwerte in der Vorlage unverändert.Schließen Sie Ihren PC an die Ethernet 0/1-interne Schnittstelle an, und erneuern Sie Ihre IP-Adresse, die vom DHCP-Server der ASA bereitgestellt wird.**Hinweis:** Verwenden Sie die folgenden Befehle, um die ASA über die Befehlszeile auf die Werkseinstellungen zurückzusetzen: ciscoasa#conf t ciscoasa#config factory-default 192.168.0.1 255.255.255.0

# **ASA-Konfiguration**

Wenn Sie die ASA-Werkseinstellungen zurückgesetzt haben, können Sie ASDM auf 192.168.0.1 starten, um eine Verbindung zur ASA an der Ethernet 0/1-internen Schnittstelle herzustellen.

Hinweis: Ihr vorheriges Kennwort wird beibehalten (oder es kann sich um eine leere Zeichenfolge

handeln).

Standardmäßig akzeptiert die ASA eine eingehende Management-Sitzung mit einer Quell-IP-Adresse im Subnetz 192.168.0.0/24. Der standardmäßige DHCP-Server, der auf der internen Schnittstelle der ASA aktiviert ist, stellt IP-Adressen im Bereich 192.168.0.2-129/24 bereit, die für die Verbindung mit der internen Schnittstelle mit ASDM gültig sind.

Gehen Sie wie folgt vor, um die ASA zu konfigurieren:

- 1. Aktivieren der externen Schnittstelle
- 2. Konfigurieren von Domänenname, Kennwort und Systemzeit
- 3. Aktivieren eines DHCP-Servers auf der externen Schnittstelle
- 4. Konfigurieren des elD-VPN-Adresspools
- 5. Importieren des Zertifikats der belgischen Stammzertifizierungsstelle
- 6. Konfigurieren der Secure Sockets Layer
- 7. Definieren der Standardgruppenrichtlinie
- 8. Definieren der Zertifikatszuordnung
- 9. Hinzufügen eines lokalen Benutzers
- 10. Neustarten der ASA

### Schritt 1: Aktivieren der externen Schnittstelle

In diesem Schritt wird beschrieben, wie die externe Schnittstelle aktiviert wird.

- 1. Klicken Sie in der ASDM-Anwendung auf Konfiguration und dann auf Geräte-Setup.
- 2. Wählen Sie im Bereich Device Setup (Geräte-Setup) die Option Interfaces (Schnittstellen) aus, und klicken Sie dann auf die Registerkarte Interfaces (Schnittstellen).

| 🔂 Cisco ASDM 6.0 for ASA - 192.168   | .0.1        |  |  |                                      |                                    |               |                          |       |                    |
|--|-------------|--|--|--------------------------------------|------------------------------------|---------------|--------------------------|-------|--------------------|
| File View Tools Wizards Window He  | dp          |  |  |                                      | Look                               | For:          |                          | Find  | ahaha              |
| Home Configuration 🕑 Monitori  | ng 🔚 Sav    | e 📿 Refresh                              | G Back 🔘 Por                                     | өөд 🕉 нө                             | P                                  |               |                          |       | CISCO              |
| Device List ਰਾ 우 ×   | Configurati | on > Device Sets                         | up > Interfaces                                  |                                      |                                    |               |                          |       | 0                  |
| Add Toelete Scannect   | Interfaces  | Switch Ports                             |  |                                      |                                    |               |                          |       |                    |
| 192160.01  | Name        | Switch Ports                             | Ena  | ked Security                         | IP Address                         | Subnet Mask   | Restrict<br>Traffic flow | VLAN  | Add                |
|  | inside      | Ethernet0/1, Eth                         | hernet0/2, Et                                    | les 1                                | 0 192.168.0.1                      | 255.255.255.0 |                          | viant |                    |
| Device Setup<br>Startup Witard<br>Stateforce<br>* *2- Routing<br>Device Name,Password<br>* © System Time |             | <u>Currenteropu</u>                      |  |                                      | 0 199 10 100.1                     | 2012012000    |                          | Vid L | Delete             |
| Device Setup   |             |  |  |                                      |                                    |               |                          |       |                    |
| Remote Access VPN  | <           |  |  |                                      |                                    |               |                          |       |                    |
| Ste-to-Ske VPN   | Enable      | traffic between to<br>traffic between to | iio or more interfaces<br>iio or more hosts conr | which are config<br>ected to the sar | ured with same set<br>te interface | curity levels |                          |       |                    |
| Device Management  |             |  |  |                                      | Apply R                            | eset          |                          |       |                    |
| Device configuration loaded successfully.  |             |  |  |                                      | <admin></admin>                    | 15            | 🗊 🛃 🔂                    | 20    | /07/07 8:35:14 UTC |

- 3. Wählen Sie die externe Schnittstelle aus, und klicken Sie auf Bearbeiten.
- 4. Wählen Sie im Abschnitt IP-Adresse der Registerkarte Allgemein die Option Statische IP verwenden.
- 5. Geben Sie für die IP-Adresse 197.0.100.1 und für die Subnetzmaske 255.255.0 ein.
- 6. Klicken Sie auf Übernehmen.

## Schritt 2: Konfigurieren von Domänenname, Kennwort und Systemzeit

In diesem Schritt wird beschrieben, wie der Domänenname, das Kennwort und die Systemzeit konfiguriert werden.

1. Wählen Sie im Bereich Geräte-Setup die Option Gerätename/Kennwort aus.

| 🖆 Cisco ASDM 6.0 for ASA - 192.168            | 8.0.1                    |                                 |                     |             |                     |
|---|--------------------------|---------------------------------|---------------------|-------------|---------------------|
| File View Tools Wizards Window H              | telp                     |                                 | Look For:           | End +       | ahaha               |
| Home Configuration 🕞 Monitor                  | ring 🔚 Save 🔇 Refre      | sh 🔇 Back 🚫 Forward             | 2 Help              |             | CISCO               |
| Device List on P ×                            | Configuration > Device 5 | ietup > Device Kame/Passw       | ord                 |             | 0                   |
| Add 📋 Delete 🖉 Connect                        | Hostname and Domain      | Name                            |                     |             |                     |
| 192.160.0.1                                   | Hostname:                | ciscoasa                        |                     |             |                     |
|   | Domain Name:             | cisco.be                        |                     |             |                     |
|   | Enable Password          |                                 |                     |             |                     |
|   | Change the privilege     | nd mode password.               |                     |             |                     |
| Device Setup di D X                           | Old Password:            |                                 |                     |             |                     |
| g <sup>9</sup> Sartup Wizard                  | New Password:            | *******                         |                     |             |                     |
| Interfaces     H     * <sup>5</sup> * Routing | Confirm New Password:    | ******                          |                     |             |                     |
| Device Name/Password                          | Tabat Bacanad            |                                 |                     |             |                     |
| a 🕑 system i me                               | Change the passwo        | rd to access the console of the | security appliance. |             |                     |
|   |                          |                                 |                     |             |                     |
|   | Uto Password             |                                 |                     |             |                     |
|   | New Password:            |                                 |                     |             |                     |
|   | Confirm New Password:    |                                 |                     |             |                     |
|   |                          |                                 |                     |             |                     |
|   |                          |                                 |                     |             |                     |
| 3 Device Setup                                |                          |                                 |                     |             |                     |
| S. David                                      |                          |                                 |                     |             |                     |
| C.S.  |                          |                                 |                     |             |                     |
| Remote Access VPN                             |                          |                                 |                     |             |                     |
| Ste-to-Site VPN                               |                          |                                 |                     |             |                     |
| Device Management                             |                          |                                 |                     |             |                     |
|   |                          |                                 | Apply Reset         |             |                     |
| Device configuration loaded successfully.     |                          |                                 | <admin> 15</admin>  | 😡 🔐 🔂 🛛 🙆 z | //07/07 8:36:04 UTC |

- 2. Geben Sie **cisco.be** als Domänennamen ein, und geben Sie **cisco123** als Wert für das Enable Password (Kennwort aktivieren) ein.**Hinweis:** Das Kennwort ist standardmäßig leer.
- 3. Klicken Sie auf Übernehmen.
- 4. Wählen Sie im Bereich Device Setup (Geräte-Setup) die Option **System Time (Systemzeit**) aus, und ändern Sie ggf. den Wert für die Uhr.
- 5. Klicken Sie auf Übernehmen.

### Schritt 3: Aktivieren Sie einen DHCP-Server auf der externen Schnittstelle.

In diesem Schritt wird beschrieben, wie ein DHCP-Server auf der externen Schnittstelle aktiviert wird, um Tests zu vereinfachen.

- 1. Klicken Sie auf Konfiguration und dann auf Geräteverwaltung.
- 2. Erweitern Sie im Bereich Gerätemanagement die Option DHCP, und wählen Sie DHCP Server

aus.

| Pile       View       Tools       Witzerds       Window       Help       Look For:         Image: Home       Image: Configuration       Image: Management > DHCP > DHCP Server       Image: Management > DHCP > DHCP Server         Image: Management > DHCP = DHCP Server       Image: Management > DHCP > DHCP Server       Image: Management > DHCP Server   | ulu<br>sco |
|---|------------|
| Image: Configuration       Image: Monitoring       Image: Save (Configuration & Device Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Add Image: Device Management > DHCP = DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List       Image: Provide Management > DHCP > DHCP Server         Image: Device List  | sco        |
| Device List         O         P         Configuration > Device Management > DHCP > DHCP Server  |            |
| Add Delete S Connect Deterface DHCP Enabled Address Pool DNS Servers WINS Servers Domain Name Ping Teneout Lei  | 0          |
| Dissues as  | Edit       |
| riside Yes 192.168.0.2 - 192.168.0.129<br>outside Yes 197.0.100.20 - 197.0.100.30   |            |
|   |            |
|   |            |
|   |            |
| Device Management D Q ×   |            |
| B      B     System Image/Configuration   |            |
| B @ High Availability   |            |
| a go Users (AAA   |            |
| Certificate Management     Global DHCP Options  |            |
| CHCP Relay     Finables auto-computation ratios the FMTP server to automaticable configure DMS with shard the default domain name. The values in the fields I   | -          |
| And a strength of the str |            |
| K Server I: Primary WINS Server:  |            |
| DNS Server 2: Secondary WDXS Server:  |            |
| Domain Name:  |            |
| R Deside Salar  |            |
| Prig Inteouc:   |            |
| Sig Frend   | IG         |
| Remote Access VPN Dynamic DNS Settings for DHCP Server  |            |
| GR Ste-to-Ste VIN   |            |
| Update Both Records Override Clent Settings   |            |
| Apply Reset   |            |
|   | 40-041070  |

- 3. Wählen Sie die externe Schnittstelle aus der Liste Schnittstelle aus, und klicken Sie auf **Bearbeiten**.Das Dialogfeld DHCP-Server bearbeiten wird angezeigt.
- 4. Aktivieren Sie das Kontrollkästchen DHCP-Server aktivieren.
- 5. Geben Sie im DHCP-Adresspool eine IP-Adresse zwischen 197.0.100.20 und 197.0.100.30 ein.
- 6. Deaktivieren Sie im Bereich Globale DHCP-Optionen das Kontrollkästchen Automatische Konfiguration von Schnittstelle aktivieren.
- 7. Klicken Sie auf Übernehmen.

## Schritt 4: Konfigurieren des eID-VPN-Adresspools

In diesem Schritt wird beschrieben, wie Sie einen Pool von IP-Adressen definieren, die zur Bereitstellung der Remote-AnyConnect-Clients verwendet werden.

- 1. Klicken Sie auf Konfiguration und dann auf Remotezugriffs-VPN.
- 2. Erweitern Sie im Bereich Remove Access VPN (Access-VPN entfernen) die Option **Network** (Client) Access (Netzwerkzugriff), und erweitern Sie dann die Adressenzuweisung.
- 3. Wählen Sie Adresspools aus, und klicken Sie dann auf die Schaltfläche Hinzufügen im Bereich Namensnennte IP-Adresspools konfigurieren. Das Dialogfeld "IP-Pool hinzufügen" wird

angezeigt.

| Gisco ASDM 6.0 for ASA - 192.168   | .0.1   |   |   |                         |                        |                     |
|--|--|---|---|-------------------------|------------------------|---------------------|
| File View Tools Wizards Window He  | de de la companya de | an da anna an tao bar gan bhailtean an an | Alex Constant of the second of the                | Look For:               | Find +                 | ala da              |
| Home 🔏 Configuration 📴 Monitori  | ng 🔚 Seve 🔇 Refre  | sh 🔇 Back 🚫 Forwa                         | a 🦿 Help  |                         |                        | cisco               |
| Device List d P ×  | Configuration > Remote   | Access VPN > Hetwork (                    | Client) Access > Add                              | tress Assignment >      | Address Pools          |                     |
| Add 👔 Delete 🔊 Connect   | Configure named IP Add   | dress pools.                              |   |                         |                        |                     |
| 192.160.0.1  | This assumption is apple   | and in other a title many one             |   |                         | and a section and in a |                     |
|  | mo parameter o entre   | Counterrainer a tres process              | CELEBRATE AND | a contraction proved of | COLUMN CONSUMEROUS     |                     |
|  | Add 📑 Edt 📋  | Delete                                    |   |                         |                        |                     |
|  | Pool Name  | Starting Address                          |   | Ending Address          | Subnet Mask            |                     |
|  | _  |   |   |                         |                        |                     |
| Remote Access VPN 2 P ×  |  | Add IP Pool                               |   | ×                       |                        |                     |
| 😑 🗃 Network (Client) Access  🔺   |  |   |   |                         |                        |                     |
| SSL VPN Connection Profiles  |  |   |   |                         |                        |                     |
| IPsec Connection Profiles  |  |   |   | -                       |                        |                     |
| Group Policies   |  | Namec                                     | eID-VPNPOOL                                       |                         |                        |                     |
| Oynamic Access Policies  |  |   |   |                         |                        |                     |
| Assignment Policy  |  | Starting IP Address:                      | 192.168.10.100                                    |                         |                        |                     |
| Address Pools  |  |   |   |                         |                        |                     |
| 🗉 🐯 Advanced   | 1  | Ending IP Address:                        | 192.168.10.110                                    | 1000000                 |                        |                     |
| Clentless SSL VPN Access   |  |   |   |                         |                        |                     |
| Easy VPN Remote  |  | Subnet Mask:                              | 255.255.255.0                                     | ~                       |                        |                     |
| E AAA Setup  |  |   |   | 100 C                   |                        |                     |
| Certificate Management   |  |   |   |                         |                        |                     |
| P DHCP Server  |  |   |   |                         |                        |                     |
| Contraction of the Owner of the |  | OK  | Cancel Help                                       |                         |                        |                     |
| Bevice Setup   |  |   |   | _                       |                        |                     |
| Frewal   |  |   |   |                         |                        |                     |
| Bamote Access VPN  |  |   |   |                         |                        |                     |
| Ste-to-Site VPN  |  |   |   |                         |                        |                     |
| Device Management  |  |   |   |                         |                        |                     |
|  |  |   | Annh  | ( Beert                 |                        |                     |
| \$   |  |   | etba.   | Keset                   |                        |                     |
|  |  |   | <   | imin> 15                | 🔯 🚰 🔰 🙆 2              | 7/07/07 8:53:04 UTC |

- 4. Geben Sie im Feld Name den Namen elD-VPNPOOL ein.
- 5. Geben Sie in die Felder "Start IP Address" (Start-IP-Adresse) und "End IP Address" (Ende der IP-Adresse) einen Bereich von 192.168.10.100 bis 192.168.10.110 ein.
- 6. Wählen Sie **255.255.255.0** aus der Dropdown-Liste Subnetzmaske aus, klicken Sie auf **OK**, und klicken Sie dann auf **Übernehmen**.

## Schritt 5: Importieren des Zertifikats der belgischen Stammzertifizierungsstelle

In diesem Schritt wird beschrieben, wie das Zertifikat der belgischen Root-Zertifizierungsstelle in die ASA importiert wird.

- 1. Laden Sie die belgischen Root CA-Zertifikate (belgiumrca.crt und belgiumrca2.crt) von der Website der Regierung herunter und installieren Sie sie auf Ihrem lokalen PC.Die Website der belgischen Regierung finden Sie unter: <u>http://certs.eid.belgium.be/</u>
- 2. Erweitern Sie im Bereich Remote Access VPN die Option Certificate Management, und wählen Sie CA Certificates (Zertifizierungsstellen-Zertifikate) aus.
- 3. Klicken Sie auf Hinzufügen und dann auf Aus Datei installieren.
- 4. Navigieren Sie zu dem Speicherort, an dem Sie die Datei Belgiumrca.crt (Belgien Root CA-Zertifikat) gespeichert haben, und klicken Sie auf **Zertifikat installieren**.
- 5. Klicken Sie auf **Apply**, um die Änderungen zu speichern.

Dieses Bild zeigt das auf der ASA installierte Zertifikat:



## Schritt 6: Konfigurieren der Secure Sockets Layer

In diesem Schritt wird beschrieben, wie Sie sichere Verschlüsselungsoptionen priorisieren, das SSL VPN-Client-Image definieren und das Verbindungsprofil definieren.

 Priorisieren Sie die sichersten Verschlüsselungsoptionen.Erweitern Sie im Bereich Remote Access VPN (Remote-Access-VPN) die Option Advanced (Erweitert), und wählen Sie SSL Settings (SSL-Einstellungen) aus. Im Abschnitt Verschlüsselung werden die aktiven Algorithmen wie folgt oben nach unten gruppiert:AES256-SHA1AES128-SHA13DES-SHA1RC4-SHA1

| Cisco ASDM 6.0 for ASA - 192.168   | 8.0.1   | n al Contra De Maña en ante Contra dagende esterio.                        | an konserva v konserva minimiziana minimiziana a minimiziana politika da serva.<br>T |                      |
|--|---|--|--|----------------------|
| File View Tools Wizards Window H   | telp  |  | Look For: 91d -  | ahaha                |
| Home 🖧 Configuration 📴 Monitor   | ring 🔚 Save 🔇 Refresh 🔇 Back 🔘 Fo   | ward 🧳 Help  | restore onto the data and the second second second                                   | CISCO                |
| Device List ਰੋ 후 ×   | Configuration > Remote Access VPH > Advan   | ced > SSL Settings   |  | 0                    |
| Add Delete Ø Connect 192.166.0.1   | Configure SSL parameters. These parameters affe<br>Server SSL Version: Any Client | ct both ASDM and SSL VPN acco  | 55.  |                      |
|  | Encryption  |  |  |                      |
|  | Avaiable Alcorithms   |  | Artisa Algorithms  | Manalla              |
|  | RC1-MD5   | Add>>>   | AES256-SHA1  | Prove Up             |
|  | DES-SHA1  | << Remove  | AE5128-5HA1  | Move Down            |
| Remote Access VPN 🗗 🕈 🛪  |   |  | 30E5-SHA1  |                      |
| E Clentless SSL VPN Access   |   |  | RC4-SHA1   |                      |
| Easy VPN Remote  |   |  |  |                      |
| 🗄 💣 AAA Setup  |   |  |  |                      |
| 🗉 👸 Secure Desktop Manager   | Certificates  |  |  | 1                    |
| Certificate Management   | Specify which certificates, if any, should be used                                | for SSL authentication on each   | h interface. The fallback certificate will be used on interface.                     | aces not             |
| DHCP Server  | associated with a certificate or their own.                                       |  |  |                      |
| E DNS  | Interface   | ID Certificat  | e  | Edk                  |
| E to Advanced  | inside  |  |  |                      |
| Cornection sateway Confiction Stateway Certificate to SSL VPN Conne HITP Redrect Maximum SSL VPN Sessions E-mail Proxy C | outside   |  |  |                      |
| Revice Setup   |   |  |  |                      |
| 🕄 Frewal   |   |  |  |                      |
| Remote Access VPN  |   |  |  |                      |
| Ste-to-Site VPN  |   |  |  |                      |
| Device Management  | Balhark Cartificator (L. Krys 👘   | Apply [  | Reset  |                      |
| Running configuration successfully saved to fla  | sh memory.  | <admin< td=""><td>&gt; 15 😡 🛃 🔒</td><td>27/07/07 8:57:34 UTC</td></admin<> | > 15 😡 🛃 🔒   | 27/07/07 8:57:34 UTC |

2. Definieren Sie das SSL VPN-Client-Image für den AnyConnect-Client.Erweitern Sie im Bereich Remote Access VPN (Remote Access VPN) die Option Advanced (Erweitert), erweitern Sie SSL VPN, und wählen Sie Client Settings (Client-Einstellungen) aus.Klicken Sie im Bereich SSL VPN Client Images auf Add.Wählen Sie das im Flash-Speicher gespeicherte AnyConnect-Paket aus.Das AnyConnect-Paket wird in der Liste der SSL VPN Client-Images angezeigt, wie in diesem Bild gezeigt:

| 📫 Cisco ASDM 6.0 for ASA - 192.  | 168/100/254   |                    |
|--|---|--------------------|
| File View Tools Wizards Window   | Help Look For: Find +   | ahaha              |
| Home 🖧 Configuration 📴 Mo  | ntoring 🔚 Save 🔃 Refresh 🕓 Back 🚫 Forward 🧳 Help  | CISCO              |
| Device List 🗗 🔍  | Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings                                | 0                  |
| 🗣 Add 📋 Delete 🖋 Connect   | Identify SSL VPN Client (SVC) related files.  |                    |
| S 192.168.0.1  | SSL VPN Client Images   |                    |
| S. Contractioner   | Mininize connection setup time by moving the image used by the most commonly encountered operation system to the top of the list. |                    |
|  | Add C Replace Delete + Move UP & Move Down  |                    |
|  | dd/b Jawrenaet wei 2.0 0343-10 nin  |                    |
|  |   |                    |
| Remote Access VPH 🗇 🔍  |   |                    |
| Network (Client) Access  |   |                    |
| <ul> <li>SSC VPN Connection Profiles</li> <li>IPsec Connection Profiles</li> </ul>   |   |                    |
| Group Policies   |   |                    |
| Dynamic Access Policies  | SSL VPN Client Profiles   |                    |
| Assignment Policy  | 🗢 Add 🦉 Edt 🏢 Delete  |                    |
| Address Pools  | Name Package  |                    |
| Kovanced     Kovanced     Kovanced     Kovanced     Kovanced   |   |                    |
| 🗃 🙀 SSL VPN  |   |                    |
| Provide Action A |   |                    |
| 🔳 🎼 IPsec 🗹 🗹  |   |                    |
| < >  |   |                    |
| A Device Setup   |   |                    |
| 🐔 Firewal  | SSL VPN Client Localization File  |                    |
| Remote Access VPN  | To set the Localization file go to Language Localization,   |                    |
| Ste-to-Site VPN  | Cache File System (to hold CSD and SVC images)  |                    |
| Device Management  | Maximum Size: 20 MB   |                    |
| :  | Acoly Reset   |                    |
|  | (admin) 15 🔯 🔂 🙆 25/  | 07/07 23:20:54 UTC |
| 🏄 start 🔰 📴 🕹 🐵 😣  | 🛐 🦈 🔁 a Wind 👔 2003Ho 👔 01/W380 😭 Caso A5 🌺 2 Infan 🔂 TextBad 🤞   | S # 10.09          |

3. Definieren Sie das DefaultWEBVPNGroup-Verbindungsprofil.Erweitern Sie im Bereich Remote Access VPN (Remote-Access-VPN) die Option Network (Client) Access (Netzwerkzugriff), und wählen Sie SSL VPN Connection Profiles (SSL VPN-Verbindungsprofile).Aktivieren Sie im Bereich Access Interfaces (Zugriffsschnittstellen) das Kontrollkästchen Enable Cisco AnyConnect VPN Client (Cisco AnyConnect VPN-Client aktivieren).Aktivieren Sie für die externe Schnittstelle die Kontrollkästchen Zugriff zulassen, Client-Zertifikat anfordern und DTLS aktivieren, wie in diesem Bild gezeigt:

| Cisco ASDM 6.0 for ASA - 192.168   | 8,100,254  | a Brychia am Chaile an an State                     |  |   | an ang taona ang taopatén kanana pananakan<br>Panganakan              |                                   |  |  |  |  |
|--|--|---|--|---|---|-----------------------------------|--|--|--|--|
| File View Tools Wizards Window H   | elp  |   | A CARLES AND A COMPANY   | Look For:   | Find +  | alate                             |  |  |  |  |
| 😘 Home 🥰 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Porword 🦻 Help |  |   |  |   |   |                                   |  |  |  |  |
| Device List a P ×  | Configuration > Re   | mote Access VPH > 1                                 | letwork (Client) Access > SS   | L VPN Connection Profile                                    | 5   | 0                                 |  |  |  |  |
| Add      Delete      Connect     192.168.0.1                                 | The security appli<br>deployment require   | ance automatically depk<br>res end-user administrat | ays the Cisco AnyConnect VPN Cli<br>ave rights. The Cisco AnyConnect | ent or legacy SSL VPN Clien<br>t VPN Client supports the HT | t to remote users upon connection.<br>TPS/TCP (SSL) and Datagram Tran | The initial client<br>sport Layer |  |  |  |  |
| 192.160.100.254  | Security (DTLS) to   | Security (DTLS) tunneling options.                  |  |   |   |                                   |  |  |  |  |
|  | (More client-related parameters, such as client images and client profiles, can be found at and locations).) |   |  |   |   |                                   |  |  |  |  |
| Remote Access VPN d Q ×  | Enable Cisco /   | *<br>AnyConnect VPN Client of                       | or legacy SSL VPN Client access or                                   | n the interfaces selected in                                | the table below   |                                   |  |  |  |  |
| 🖃 🙀 Network (Client) Access 🔨  | Interface  | Allow Access  | Require Clerk Certificate  | Frable DTLS   | 7   |                                   |  |  |  |  |
| SS, VPN Connection Profiles  | outside  |   |  |   |   |                                   |  |  |  |  |
| Group Policies   | inside   |   |  |   |   |                                   |  |  |  |  |
| Dynamic Access Policies  | 100  |   |  |   |   |                                   |  |  |  |  |
| 🖻 🎭 Address Assignment   | 1.1  |   |  |   |   |                                   |  |  |  |  |
| 🖹 🔄 Advanced   |  |   |  |   |   |                                   |  |  |  |  |
| Chendless SS, VPN Access   | Access Port: 44  | 3 DTLS Po   | rt: 443  |   |   |                                   |  |  |  |  |
| Portal   | Click here to Assi   | on Certificate to Interfa                           | œ,   |   |   |                                   |  |  |  |  |
| Group Policies   |  |   |  |   |   |                                   |  |  |  |  |
| Dynamic Access Policies  | Connection Profil  |   |  |   |   |                                   |  |  |  |  |
| B B Advanced   | Connection profile   | (hunnel group) table he                             | how contains records that determ                                     | ine connection policies. A re                               | word identifies a default record only                                 | v for the                         |  |  |  |  |
| Eg theoding  | connection and co  | ontains protocol-specific                           | connection parameters.   | The contraction posters. A fi                               | con a rate his to a dei ant. A colo hos                               |                                   |  |  |  |  |
|  | Add T Edit   | TT Delete   |  |   |   |                                   |  |  |  |  |
| B Device Setup   |  |   |  |   | 4   |                                   |  |  |  |  |
| a  | Defaultiversizes   | Allases   | SOL VPN<br>Eoshied   | Client Protocol   | Group Policy  |                                   |  |  |  |  |
| Stop Firewall  | DefaultRAGroup   |   | Enabled  |   | DfltGrpPolicy   |                                   |  |  |  |  |
| Remote Access VPN  |  |   |  |   |   |                                   |  |  |  |  |
| Ste-to-Ste VPN   |  |   |  |   |   |                                   |  |  |  |  |
| Device Management  | Allow user to  | select connection. idenit                           | ified by alias in the table above.                                   | at login page   |   |                                   |  |  |  |  |
| :  |  |   | Apply  | Reset   |   |                                   |  |  |  |  |
|  |  |   | <  | dmin> 15  | 😡 🕼 🔰 🙆 2   | 6/07/07 0:20:25 UTC               |  |  |  |  |

Wählen Sie im Bereich Verbindungsprofile die Option **DefaultWEBVPNGroup aus**, und klicken Sie auf **Edit**.Das Dialogfeld "SSL VPN-Verbindungsprofil bearbeiten" wird angezeigt.

| 🖆 Edit SSL VPN Connecti | on Profile: DefaultWEE  | 3VPNGroup                       | 8      |  |  |  |
|-------------------------|---|---------------------------------|--------|--|--|--|
| Basic                   | Name:<br>Aliases:   | DefaultWEBVPNGroup              | ]      |  |  |  |
|                         | Authentication  | O AAA O Contribute O Buth       |        |  |  |  |
|                         | AAA Server Group:   |                                 | Manage |  |  |  |
|                         |   | Use LOCAL If Server Group fails |        |  |  |  |
|                         | Client Address Assigne  | ent                             |        |  |  |  |
|                         | DHCP Servers:   |                                 | ]      |  |  |  |
|                         | Client Address Pools:   |                                 | Select |  |  |  |
|                         | Default Group Policy  |                                 |        |  |  |  |
|                         | Group Policy:   | DfltGrpPolicy                   | Manage |  |  |  |
|                         | SSL VPN Client Protocol:  | C Enabled                       |        |  |  |  |
|                         | ОК  | Cancel Help                     |        |  |  |  |
|                         | Default Group Policy<br>Group Policy:<br>SSL VPN Client Protocol:<br>OK | DfltGrpPolicy  Cancel Help      | Manage |  |  |  |

Wählen Sie im Navigationsbereich die Option **Basic (Grundlegend)** aus.Klicken Sie im Bereich Authentifizierung auf das Optionsfeld **Zertifikat**.Aktivieren Sie im Bereich Default Group Policy (Standardgruppenrichtlinie) das Kontrollkästchen **SSL VPN Client Protocol**.Erweitert **Erweitert**, und wählen Sie **Authentifizierung aus**.Klicken Sie auf **Hinzufügen**, und fügen Sie die externe Schnittstelle mit einer lokalen Servergruppe hinzu, wie in diesem Bild

| gezeigt:  |  |                             |                                  |   |  |
|---|--|-----------------------------|----------------------------------|---|--|
| 🕵 Edit SSL VPN Connecti   | on Profile: Default1   | WEBVPNGroup                 |                                  | × |  |
| Basic<br>Advanced<br>General<br>Client Addressing<br>Authentication | Interface-Specific #<br>Add 2 Edit 1<br>Interface<br>outside | Authentication Server Group | er Groups<br>P Fallback to LOCAL |   |  |
| Authorization<br>Accounting<br>SSL VPN                              |  |                             |                                  |   |  |
|   | OK   | Cancel Hel                  | P                                |   |  |

Wählen Sie im Navigationsbereich **Authorization (Autorisierung)** aus.Wählen Sie im Bereich Default Authorization Server Group (Standardautorisierungsserver-Gruppe) **LOCAL** aus der Dropdown-Liste Server Group (Servergruppe) aus, und aktivieren Sie das Kontrollkästchen **Users must (Benutzer muss in der Autorisierungsdatenbank vorhanden sein, um eine Verbindung herzustellen**.Wählen Sie im Bereich "Benutzernamenzuordnung" in der Dropdown-Liste Primärer DN-Feld die Option **SER (Seriennummer)** aus, wählen Sie **None** aus dem Feld Sekundäre DN, und klicken Sie auf **OK**.

|   | Edit SSL VPN Connecti | on Profile: DefaultWEBVPNGroup  | $\mathbf{X}$ |  |  |  |
|---|-----------------------|---|--------------|--|--|--|
| Basic<br>Advanced<br>General<br>Client Addressing<br>Authentication<br>Authorization<br>Accounting<br>SSL VPN |                       | Default Authorization Server Group Server Group: LOCAL  |              |  |  |  |
|   |                       | Interface Server Group  |              |  |  |  |
|   |                       | User Name Mapping Use the entire DN as the username Specify individual DN fields as the username Primary DN Field: SER (Serial Number) Secondary DN Field: None |              |  |  |  |
|   |                       | OK Cancel Help  |              |  |  |  |

## Schritt 7: Definieren der Standardgruppenrichtlinie

In diesem Schritt wird beschrieben, wie die Standardgruppenrichtlinie definiert wird.

1. Erweitern Sie im Bereich Remote Access VPN (Remote-Access-VPN) den Network (Client) Access (Netzwerkzugriff), und wählen Sie Group Policies (Gruppenrichtlinien) aus.

| 🖀 Cisco ASDM 6.0 for ASA - 192.168      | 8.0.1                            |                                   |                                       |                                      |                     |
|---|----------------------------------|-----------------------------------|---------------------------------------|--------------------------------------|---------------------|
| File View Tools Wizards Window H        | юþ                               |                                   | Look For:                             | Find -                               | ahaha               |
| Home 🔏 Configuration 📴 Monitor          | ring 🔚 Save 🔇 Refresh 🔇          | Back 🔘 Forward 🧳 🖓 He             | P                                     |                                      | CISCO               |
| Device List of 9 ×                      | Configuration > Remote Access    | VPH > Network (Client) Acco       | ss > Group Policies                   |                                      |                     |
| Add Delete S Connect                    | Manage VPN group policies. A VPP | group policy is a collection of u | ser-oriented attribute/value pairs th | at may be stored internally on the d | evice or            |
| a contraction                           | Add - R Edt I Turben             | ver. me group poicy in ormade     | is referenced by time dates group     | s and user accounts.                 |                     |
|   | Name                             | Type                              | Turneling Protocol                    | AAA Server Group                     |                     |
|   | OfRGrpPolicy (System Default)    | Internal                          | L2TP-IPSec, svc, IPSec, webvpr        | N/A                                  |                     |
|   |                                  |                                   |                                       |                                      |                     |
| Remote Access VPN 🗗 🔍 🗙                 |                                  |                                   |                                       |                                      |                     |
| Network (Client) Access                 |                                  |                                   |                                       |                                      |                     |
| IPsec Connection Profiles               |                                  |                                   |                                       |                                      |                     |
| Group Policies                          |                                  |                                   |                                       |                                      |                     |
| 🗉 💁 Address Assignment                  |                                  |                                   |                                       |                                      |                     |
| Clentless SSL VPN Access                |                                  |                                   |                                       |                                      |                     |
| Easy VPN Remote                         |                                  |                                   |                                       |                                      |                     |
| AAA Setup     Secure Desktop Manager    |                                  |                                   |                                       |                                      |                     |
| Certificate Management     Child Secure |                                  |                                   |                                       |                                      |                     |
| A DNS                                   |                                  |                                   |                                       |                                      |                     |
| Advanced                                |                                  |                                   |                                       |                                      |                     |
| Burvice Setup                           |                                  |                                   |                                       |                                      |                     |
| 🕄 Firewal                               |                                  |                                   |                                       |                                      |                     |
| Remote Access VPN                       |                                  |                                   |                                       |                                      |                     |
| Ste-to-Ste VPN                          |                                  |                                   |                                       |                                      |                     |
| Device Management                       |                                  |                                   |                                       |                                      |                     |
| :                                       |                                  |                                   | Apply Reset                           |                                      |                     |
|   |                                  |                                   | cadnin> 15                            | 27                                   | /07/07 15:23:14 UTC |

- 2. Wählen Sie die **DfltGrpPolicy** aus der Liste der Gruppenrichtlinien aus, und klicken Sie auf **Bearbeiten**.
- 3. Das Dialogfeld "Richtlinie für interne Gruppen bearbeiten" wird angezeigt.

| 🖆 Edit Internal Group Po  | licy: DfltGrpPolicy    |                                     | ×                |
|---|------------------------|-------------------------------------|------------------|
| General   | Name: DfitGr           | Policy                              |                  |
| Servers  Advanced Split Tunneling IE Browser Proxy SSL VPN Client Login Setting | Banner:                | VPNPOOL                             | Select           |
|   | More Options           |                                     |                  |
| Dead Peer Detecti<br>Customization  | Tunneling Protocols:   | Clientless SSL VPN V SSL VPN Client | IPsec L2TP/IPsec |
| <ul> <li>IPsec Client</li> </ul>  | Filter:<br>NAC Policy: | None                                | Manage           |
|   | Access Hours:          | Unrestricted                        | Manage           |
|   | Simultaneous Logins:   | 3                                   |                  |
|   | Maximum Connect Tin    | ne: Unlimited minutes               |                  |
|   | Idle Timeout:          | Unlimited 30 minutes                |                  |
|   |                        |                                     |                  |
|   |                        |                                     |                  |
| < >   |                        |                                     |                  |
|   | OK                     | Cancel Help                         |                  |

- 4. Wählen Sie im Navigationsbereich die Option Allgemein aus.
- 5. Klicken Sie für Adresspools auf **Auswählen**, um einen Adresspool auszuwählen, und wählen Sie **eID-VPNPOOL aus**.
- 6. Deaktivieren Sie im Bereich More Options (Mehr Optionen) die Kontrollkästchen IPsec und L2TP/IPsec, und klicken Sie auf OK.

## Schritt 8: Definieren der Zertifikatszuordnung

In diesem Schritt wird beschrieben, wie die Kriterien für die Zertifikatszuordnung definiert werden.

- 1. Klicken Sie im Bereich Remote Access VPN (Remote-Access-VPN) auf Advanced (Erweitert), und wählen Sie Certificate to SSL VPN Connection Profile Maps (Zertifikate an SSL VPN-Verbindungsprofilzuordnungen) aus.
- 2. Klicken Sie im Bereich Certificate to Connection Profile Maps (Zertifikat zu Verbindungsprofilzuordnungen) auf Add (Hinzufügen), und wählen Sie DefaultCertificateMap aus der Zuordnungsliste aus.Diese Zuordnung muss mit der DefaultWEBVPNProfile im Feld "Dem Verbindungsprofil zugeordnet" übereinstimmen.
- Klicken Sie im Bereich Zuordnungskriterien auf Hinzufügen, und fügen Sie folgende Werte hinzu:Feld: Emittent, Land (C), Equals, "BE"Feld: Emittent, Common Name (CN), Equals, "Citizen CA"Die Zuordnungskriterien sollten wie in diesem Bild gezeigt angezeigt werden:

| 📽 Cisco ASDM 6.0 for ASA - 192.168                             | .100.254  | anna - phong e ann faoint Anna Anna Anna A               | la marte este e tudo des formanies | Alimeter and Long Coloris South |                           | una esta de latina da consta da latinean conste da s | , en |                    |
|--|---|--|------------------------------------|---------------------------------|---------------------------|--|--|--------------------|
| File View Tools Wizards Window H                               | elp   |  |                                    | Loo                             | k For:                    | 用  | nd +                                     | . dealer           |
| Home 🔓 Configuration 🗾 Monitor                                 | ng 🔒 Save Q   | Refresh 🔇 Back 🤇   | Forward 🤗 H                        | de                              | an an tha an tha an air t |  |  | cisco              |
| Device List d <sup>a</sup> 4 ×                                 | Configuration > R   | emote Access VPH > A                                     | dvanced > Certifica                | te to SSL VPN Co                | mnection Profile I        | Aapo   |  | 0                  |
| ◆ Add ① Delete Ø Connect<br>■ 192.168.0.1<br>№ 192.168.100.251 | Define rules to map certificates to desired connection profiles (tunnel groups). Use the bottom table to configure certificate fields together<br>matching criteria for the selected rule.<br>Certificate to Connection Profile Maps<br>Add C Edit Delete |  |                                    |                                 |                           |  |  |                    |
|  | Plap Name<br>DefaultCertifical  | tellan   | Rule Priority                      | Mapped to C                     | Johnection Profile        |  |  |                    |
| Remote Access VPN • ×  | Mapping Criteria<br>Add C to<br>Field<br>Issuer<br>Issuer   | t Delete<br>Component<br>Country (C)<br>Common Name (CN) |                                    | Operator<br>Equals<br>Equals    | Value<br>be<br>citizer    | 1/cå   |  |                    |
| Configuration changes saved successfully.                      |   |  | 1                                  | <admin></admin>                 | 15                        | 🕼 🕃 🔂  | 25/0                                     | 17/07 23:20:54 UTC |

4. Klicken Sie auf Übernehmen.

## Schritt 9: Hinzufügen eines lokalen Benutzers

In diesem Schritt wird beschrieben, wie Sie einen lokalen Benutzer hinzufügen.

- 1. Erweitern Sie im Bereich Remote Access VPN die Option AAA Setup, und wählen Sie Local Users (Lokale Benutzer).
- 2. Klicken Sie im Bereich Lokale Benutzer auf Hinzufügen.
- Geben Sie im Feld Benutzername die Seriennummer des Benutzerzertifikats ein. Beispiel: 56100307215 (wie im Abschnitt <u>Authentifizierungszertifikat</u> dieses Dokuments beschrieben).

| Gisco ASOM 6.0 for ASA - 192.168.                 | 100.254           | c rebene i anto anto representa no co   | 0.9 (CCC) (C | and the second | and a set of the state of the set |                     |
|---|-------------------|---|--|---|--|---------------------|
| File View Tools Wizards Window He                 | þ                 |   |  | Look For:   | Find +   | ahaha               |
| Home 🖧 Configuration 📴 Monitorin                  | ig 🔚 Save 🔇       | 🖓 Refresh 🔇 Back 🔘 Fi                   | rward 🦿 Help   |   |  | CISCO               |
| Device List 라우×                                   | Configuration > R | emote Access VPH > AAA S                | etup > Local Users   |   |  | 0                   |
| Add Delete S Connect                              | Create entries in | the ASA local user database.            |  |   |  |                     |
| A 192.168.0.1<br>192.168.100.254                  | Command autho     | vization must be enabled in ord         | er for the user account privile  | oes to be enforced. To enabl  | e command authorization, go to   | Contraction.        |
| -   |                   |   |  |   |  |                     |
|   | go to Authentica  | tion console commands must be<br>ation. | enabled in order for certain a   | access restrictions to be enror   | ced. To enable AAA authentica  | oon command         |
|   |                   |   |  |   |  |                     |
| Demote Arrease VDM 20 0 X                         | enable_15         | Privilege Level (Role)<br>15            | Access Restrictions<br>Full  | VPN Group Policy<br>N/A   | VPN Group Lock   | Add                 |
| Androite Helter                                   | 63041403325       | 2                                       | Ful  | - Inherit Group Policy -  | <ul> <li>Inherit Group Policy</li> </ul>   | Edit                |
| Single Signon Servers                             |                   |   |  |   |  | Delete              |
| +>+ Web ACLs                                      |                   |   |  |   |  |                     |
| R AAA Setup                                       |                   |   |  |   |  | 10-11-24-19-19-1    |
| AAA Server Groups                                 |                   |   |  |   |  |                     |
| Se LDAP Attribute Map                             |                   |   |  |   |  |                     |
| Secure Desitop Manager                            |                   |   |  |   |  |                     |
| 🗉 🔁 Certificate Management                        |                   |   |  |   |  |                     |
| M DHCP Server                                     |                   |   |  |   |  |                     |
| B B Advanced                                      |                   |   |  |   |  |                     |
| +5+ Connection Gateway                            |                   |   |  |   |  |                     |
| -   |                   |   |  |   |  |                     |
| Device Setup                                      |                   |   |  |   |  |                     |
| 🕄 Firewall  |                   |   |  |   |  |                     |
| Remote Access VPN                                 |                   |   |  |   |  |                     |
| Ste-to-Site VPN                                   |                   |   |  |   |  |                     |
| Device Management                                 |                   |   |  |   |  |                     |
| :   |                   |   | Apply  | Reset   |  |                     |
| Running configuration successfully saved to flash | h memory.         |   | <adm< td=""><td>in&gt;  15  </td><td>🗟 📓 🔰 🙆 2</td><td>(/07/07 0:22:25 UTC</td></adm<>   | in>  15   | 🗟 📓 🔰 🙆 2  | (/07/07 0:22:25 UTC |

4. Klicken Sie auf Übernehmen.

## Schritt 10: Neustarten der ASA

Starten Sie die ASA neu, um sicherzustellen, dass alle Änderungen auf die Systemdienste angewendet werden.

## **Feineinstellung**

Beim Testen schließen einige SSL-Tunnel möglicherweise nicht ordnungsgemäß. Da die ASA davon ausgeht, dass der AnyConnect-Client die Verbindung trennen und wieder herstellen kann, wird der Tunnel nicht verworfen, wodurch er die Möglichkeit erhält, zurückzukehren. Bei Labortests mit einer Basislizenz (standardmäßig 2 SSL-Tunnel) können Sie Ihre Lizenz jedoch erschöpfen, wenn SSL-Tunnel nicht ordnungsgemäß geschlossen sind. Wenn dieses Problem auftritt, können Sie mit dem **Befehl vpn-sessiondb logoff** *option>* alle aktiven SSL-Sitzungen abmelden.

# Einminütige Konfiguration

Um schnell eine funktionierende Konfiguration zu erstellen, setzen Sie die ASA auf die Werkseinstellungen zurück, und fügen Sie diese Konfiguration in den Konfigurationsmodus ein:

#### 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 1 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 rc4sha1 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

# Zugehörige Informationen

- <u>Cisco PIX Firewall-Software</u>
- <u>Cisco Secure PIX Firewall Befehlsreferenzen</u>
- Problemhinweise zu Sicherheitsprodukten (einschließlich PIX)
- Anforderungen für Kommentare (RFCs)
- <u>Technischer Support und Dokumentation Cisco Systems</u>