ベルギーの eID カードを使った ASA 8.x Anyconnect の認証

目次

概要

このドキュメントでは、ASA 8.x の Anyconnect 認証を設定して、ベルギーの eID のカードを使用する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- 適切な ASA 8.0 ソフトウェアを搭載する ASA 5505
- AnyConnect Client
- ASDM 6.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

eID は、ユーザがリモート Windows PC 上で認証するために使用する必要のあるベルギー政府発行の PKI（公開キー インフラストラクチャ）カードです。 AnyConnect ソフトウェア クライアントは、ローカル PC にインストールされ、リモート PC から認証クレデンシャルを取得します。 認証が完了すると、リモート ユーザは完全な SSL トンネルを経由して中央にあるリソースにアクセスできます。 リモート ユーザは ASA が管理するプールから取得される IP アドレスでプロビジョニングされます。

ローカル PC のセットアップ

オペレーティング システム

ローカル PC 上のオペレーティング システム（Windows、Mac OS、Unix、または Linux）は、必要なすべてのパッチがインストールされた最新の状態にしておく必要があります。

カード リーダー

eID カードを使用するためには、ローカル コンピュータに電子カード リーダーを設置する必要があります。 電子カード リーダーとは、コンピュータ上のプログラムと ID カード上のチップの間に通信チャネルを確立するハードウェア デバイスのことです。

承認済みカード リーダーのリストについては、次の URL を参照してください。
http://www.cardreaders.be/en/default.htm

注: カード リーダーを使用するには、ハードウェア ベンダーが推奨するドライバをインストールする必要があります。

eID ランタイム ソフトウェア

ベルギー政府が提供する eID ランタイム ソフトウェアをインストールする必要があります。 このソフトウェアを使用すると、リモート ユーザが eID カードのコンテンツを読み取り、検証し、印刷することができます。 このソフトウェアは、フランス語版とオランダ語版の Windows、Mac OS X、および Linux で使用できます。

詳細については、次の URL を参照してください。

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

認証証明書

ローカル PC で Microsoft Windows ストアに認証証明書をインポートする必要があります。 証明書をストアにインポートできない場合は、AnyConnect クライアントが ASA への SSL 接続を確立できません。

手順

認証証明書を Windows ストアにインポートするには、次の手順を実行します。

1. eID をカード リーダーに挿入し、ミドルウェアを起動して、eID カードの内容にアクセスします。eID カードの内容が表示されます。
2. [Certificats] (フランス語) タブをクリックします。証明書の階層が表示されます。
3. [Belgium Root CA] を展開し、[Citizen CA] を展開します。
4. 名前付き証明書の [Authentication] バージョンを選択します。
5. [Enregistrer] (フランス語) ボタンをクリックします。証明書が Windows ストアにコピーされます。

注: [Details] ボタンをクリックすると、ウィンドウが開き、証明書に関する詳細情報が表示されます。 [Details] タブで [Subject] フィールドを選択して、[Serial Number] フィールドを表示します。 [Serial Number] フィールドには、ユーザ認証に使用される固有の値が表示されます。 たとえば、シリアル番号「56100307215」は、誕生日が 1956 年 10 月 3 日、シーケンス番号が 072、検査数字が 15 であるユーザを表します。 *これらの番号を保存するには、連邦政府機関による承認を求める要求を送信する必要があります。 いずれかの国でベルギー市民のデータベースを維持する際は、所定の方法で公式に通知してください。*

検証

証明書が正常にインポートされたことを検証するには、次の手順を実行します。

1. Windows XP マシンで DOS ウィンドウを開き、**mmc** コマンドを入力します。Console アプリケーションが表示されます。
2. [File] > [Add/Remove Snap-in] を選択します (または Ctrl を押した状態で M を押します)。[Add/Remove Snap-in] ダイアログボックスが表示されます。
3. [Add] ボタンをクリックします。[Add Standalone Snap-in] ダイアログボックスが表示されます。
4. [Available Standalone Snap-ins] リストから [Certificates] を選択し、[Add] をクリックします。
5. [My user account] オプション ボタンをクリックし、[Finish] をクリックします。[Add/Remove Snap-in] ダイアログボックスに [Certificate snap-in] が表示されます。

6. [Close] をクリックして [Add Standalone Snap-in] ダイアログボックスを閉じたら、[Add/Remove Snap-in] ダイアログボックスで [OK] をクリックし、Console アプリケーションに戻ります。
7. [Console Root] フォルダ下の [Certificates - Current User] を展開します。
8. [Personal] を展開してから、[Certificates] を展開します。次の図のように、インポートされた証明書が Windows ストアに表示されます。

AnyConnect のインストール

リモート PC に AnyConnect クライアントをインストールする必要があります。 AnyConnect ソフトウェアは、編集可能な XML 設定ファイルを使用して、使用可能なゲートウェイのリストをプリセットします。 XML ファイルはリモート PC 上の次のパスに保存されます。

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

ここで *%USERNAME%* は、リモート PC 上のユーザ名です。

XML ファイルの名前は *preferences.xml* です。 *以下*はファイルの内容の例です。

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

ここで *192.168.0.1* は ASA ゲートウェイの IP アドレスです。

ASA の要件

ASA が次の要件を満たしていることを確認します。

- AnyConnect と ASDM はフラッシュで実行する必要があります。このドキュメントの手順を完了するには、適切な ASA 8.0 ソフトウェアがインストールされている ASA 5505 を使用してください。 AnyConnect および ASDM アプリケーションをフラッシュにプリロードする必要があります。 **show flash コマンド**を使用して、フラッシュの内容を確認します。
  ```
  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 は工場出荷時の初期状態で実行する必要があります。このドキュメントの手順を完了するために新しい ASA シャーシを使用する場合は、この要件を省略できます。 それ以外の場合は、次の手順に従って、ASA を工場出荷時の初期状態にリセットします。ASDM アプリケーションで ASA シャーシに接続し、[File] > [Reset Device to the Factory Default Configuration] を選択します。テンプレートのデフォルト値をそのまま使用します。イーサネット 0/1 内部インターフェイスで PC を接続し、ASA の DHCP サーバによってプロビジョニングされる IP アドレスを更新します。**注:** コマンド ラインで ASA を工場出荷時の初期状態にリセットするには、次のコマンドを使用します。`ciscoasa#conf t ciscoasa#config factory-default 192.168.0.1 255.255.255.0`

ASA の設定

ASA を工場出荷時の初期状態にリセットしたら、192.168.0.1 で ASDM を開始して、イーサネッ

ト 0/1 の内部インターフェイスで ASA に接続します。

注: 以前のパスワードが保持されます (またはデフォルトで空白になることもあります) 。

ASA はデフォルトで、サブネット 192.168.0.0/24 の送信元 IP アドレスとの着信管理セッションを受け入れます。 ASA の内部インターフェイスで有効化されたデフォルトの DHCP サーバは、192.168.0.2-129/24 の範囲の IP アドレスを提供します。これは、ADSM で内部インターフェイスへ接続するために有効な範囲です。

ASA を設定するには、次の手順を実行します。

1. 外部インターフェイスを有効にする
2. ドメイン名、パスワード、システム時刻を設定する
3. 外部インターフェイスで DHCP サーバを有効にする
4. eID VPN アドレス プールを設定する
5. ベルギーのルート CA 証明書をインポートする
6. セキュア ソケット レイヤを設定する
7. デフォルトのグループ ポリシーを定義する
8. 証明書マッピングを定義する
9. ローカル ユーザを追加する
10. ASA を再起動する

手順 1 : 外部インターフェイスを有効にする

この手順では、外部インターフェイスを有効にする方法について説明します。

1. ASDM アプリケーションで [Configuration] をクリックし、[Device Setup] をクリックします。
2. [Device Setup] 領域で [Interfaces] を選択し、[Interfaces] タブをクリックします。
3. 外部インターフェイスを選択し、[Edit] をクリックします。
4. [General] タブの [IP address] セクションで [Use Static IP] オプションを選択します。
5. IP アドレスとして **197.0.100.1** と入力し、サブネット マスクとして **255.255.255.0** と入力します。
6. [Apply] をクリックします。

手順 2 : ドメイン名、パスワード、システム時刻を設定する

この手順では、ドメイン名、パスワード、およびシステム時刻を設定する方法について説明します。

1. [Device Setup] 領域で [Device Name/Password] を選択します。
2. ドメイン名として **cisco.be** と入力し、[Enable Password] の値に cisco123 と入力します。
   注: デフォルトでは、パスワードは空白です。
3. [Apply] をクリックします。
4. [Device Setup] 領域で [System Time] を選択し、必要に応じてクロックの値を変更します。
5. [Apply] をクリックします。

手順 3 : 外部インターフェイスで DHCP サーバを有効にする

この手順では、外部インターフェイスで DHCP サーバを有効にして、テストを効率よく実行する方法について説明します。

1. **Configuration** をクリックし、次に **Device Management** をクリックします。
2. [Device Management] 領域で [DHCP] を展開し、[DHCP Server] を選択します。
3. インターフェイス リストから外部インターフェイスを選択し、[Edit] をクリックします。[Edit DHCP Server] ダイアログボックスが表示されます。
4. [Enable DHCP Server] チェックボックスをオンにします。
5. DHCP の [Address Pool] に IP アドレスとして 197.0.100.20 ~ 197.0.100.30 を入力します。
6. [Global DHCP Options] 領域の [Enable auto-configuration from interface] チェックボックスをオフにします。
7. [Apply] をクリックします。

手順 4：eID VPN アドレス プールを設定する

この手順では、リモート AnyConnect クライアントをプロビジョニングするために使用する IP アドレスのプールを定義する方法について説明します。

1. [Configuration] をクリックして、[Remote Access VPN] をクリックします。
2. [Remove Access VPN] 領域で [Network (Client) Access] を展開し、[Address Assignment] を展開します。
3. [Address Pools] を選択し、[Configure named IP Address pools] 領域にある [Add] ボタンをクリックします。[Add IP Pool] ダイアログボックスが表示されます。
4. [Name] フィールドに **eID-VPNPOOL** と入力します。
5. [Starting IP Address] フィールドと [Ending IP Address] フィールドに、IP アドレスの範囲 192.168.10.100 ~ 192.168.10.110 を入力します。
6. [Subnet Mask] ドロップダウン リストから [255.255.255.0] を選択し、[OK] をクリックして、[Apply] をクリックします。

手順 5：ベルギーのルート CA 証明書をインポートする

この手順では、ベルギーのルート CA 証明書を ASA にインポートする方法について説明します。

1. ベルギーのルート CA 証明書（belgiumrca.crt および belgiumrca2.crt）を政府の Web サイトからローカル PC にダウンロードし、保存してインストールします。ベルギー政府の Web サイトは次の URL にあります。 http://certs.eid.belgium.be/
2. [Remote Access VPN] 領域で [Certificate Management] を展開し、[CA Certificates] を選択します。
3. [Add] をクリックして、[Install from file] をクリックします。
4. ベルギーのルート CA 証明書（belgiumrca.crt）ファイルを保存した場所を参照し、[Install Certificate] をクリックします。
5. [Apply] をクリックして、変更を保存します。

次の図は、ASA にインストールされた証明書です。

手順 6：セキュア ソケット レイヤを設定する

この手順では、安全な暗号化オプションに優先順位を付け、SSL VPN クライアント イメージを

定義し、接続プロファイルを定義する方法について説明します。

1. 最も安全な暗号化オプションを優先順位付けします。[Remote Access VPN] 領域で [Advanced] を展開し、[SSL Settings] を選択します。 [Encryption] セクションで [Active Algorithms] が次のように上から順にスタックされます。AES256-SHA1AES128-SHA13DES-SHA1RC4-SHA1
2. AnyConnect クライアントの SSL VPN クライアント イメージを定義します。[Remote Access VPN] 領域で [Advanced] を展開し、[SSL VPN] を展開し、[Client Settings] を選択します。[SSL VPN Client Images] 領域で [Add] をクリックします。フラッシュに保存される AnyConnect パッケージを選択します。次の図のように AnyConnect パッケージが [SSL VPN Client Images] リストに表示されます。
3. DefaultWEBVPNGroup 接続プロファイルを定義します。[Remote Access VPN] 領域で [Network (Client) Access] を展開し、[SSL VPN Connection Profiles] を選択します。[Access Interfaces] 領域で [Enable Cisco AnyConnect VPN Client] チェックボックスをオンにします。次の図のように、外部インターフェイスの [Allow Access]、[Require Client Certificate]、および [Enable DTLS] チェックボックスをオンにします。[Connection Profiles] 領域で [DefaultWEBVPNGroup] を選択し、[Edit] をクリックします。[Edit SSL VPN Connection Profile] ダイアログボックスが表示されます。ナビゲーション領域で [Basic] を選択します。[Authentication] 領域で [Certificate] オプション ボタンをクリックします。[Default Group Policy] 領域で [SSL VPN Client Protocol] チェックボックスをオンにします。[Advanced] を展開し、[Authentication] を選択します。[Add] をクリックし、次の図のように外部インターフェイスをローカル サーバ グループとともに追加します。ナビゲーション領域で [Authorization] を選択します。[Default Authorization Server Group] 領域で [Server Group] ドロップダウン リストから [LOCAL] を選択し、[Users must exist in the authorization database to connect] チェックボックスをオンにします。[User Name Mapping] 領域で [Primary DN Field] ドロップダウン リストから [SER (Serial Number)] を選択し、[Secondary DN Field] で [None] を選択し、[OK] をクリックします。

手順 7：デフォルトのグループ ポリシーを定義する

この手順では、デフォルトのグループ ポリシーを定義する方法について説明します。

1. [Remote Access VPN] 領域で [Network (Client) Access] を選択し、[Group Policies] を選択します。
2. グループ ポリシーのリストから [DfltGrpPolicy] を選択し、[Edit] を選択します。
3. [Edit Internal Group Policy] ダイアログボックスが表示されます。
4. ナビゲーション領域で [General] を選択します。
5. [Address Pools] でアドレスのプールを選択するために [Select] をクリックして、[eID-VPNPOOL] を選択します。
6. [More Options] 領域で [IPsec] チェックボックスと [L2TP/IPsec] チェックボックスをオフにして、[OK] をクリックします。

手順 8：証明書マッピングを定義する

この手順では、証明書のマッピング基準を定義する方法について説明します。

1. [Remote Access VPN] 領域で [Advanced] をクリックし、[Certificate to SSL VPN Connection Profile Maps] を選択します。

2. [Certificate to Connection Profile Maps] 領域で [Add] をクリックし、マップ リストから [DefaultCertificateMap] を選択します。このマップは [Mapped to Connection Profile] フィールドの [DefaultWEBVPNProfile] と一致する必要があります。
3. [Mapping Criteria] 領域で [Add] をクリックし、以下の値を追加します。Field： Issuer、Country (C)、Equals、「be」Field： Issuer、Common Name (CN)、Equals、「citizen ca」[Mapping Criteria] が次の図のようになります。
4. [Apply] をクリックします。

手順 9：ローカル ユーザを追加する

この手順では、ローカル ユーザを追加する方法について説明します。

1. [Remote Access VPN] 領域で [AAA Setup] を展開し、[Local Users] を選択します。
2. [Local Users] 領域で [Add] をクリックします。
3. [Username] フィールドにユーザ証明書のシリアル番号を入力します。 たとえば、56100307215 と入力します（このドキュメントのセクション「認証証明書」を参照してください）。
4. [Apply] をクリックします。

手順 10：ASA を再起動する

ASA を再起動して、システム サービスにすべての変更が適用されていることを確認します。

微調整

テスト中に、一部の SSL トンネルが正しく閉じないことがあります。 ASA は AnyConnect クライアントが切断してから再接続する可能性があることを想定しているため、トンネルはドロップされません。そのため接続し直すことができます。 ただし基本ライセンス（デフォルトでは 2 つの SSL トンネル）を使用したラボのテスト中には、SSL トンネルが正しく閉じていないとライセンスを使い尽くしてしまう可能性があります。 この問題が発生したら、**vpn-sessiondb logoff <option>** コマンドを使用して、すべてのアクティブな SSL セッションからログオフします。

簡単設定

動作する設定を素早く作成するには、ASA を工場出荷時の設定にリセットし、設定モードでこの設定を貼り付けます。

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
```

関連情報

- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice（PIX を含む）
- Requests for Comments（RFC）
- テクニカルサポートとドキュメント - Cisco Systems