与比利时eID卡的ASA 8.x Anyconnect认证

目录

简介

本文描述如何设置ASA 8.x Anyconnect验证使用比利时eID卡。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 与适当的ASA 8.0软件的ASA 5505
- AnyConnect Client
- ASDM 6.0

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

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

eID是用户在一个远程Windows PC必须使用为了验证的比利时政府发出的PKI (公共钥匙结构)卡。AnyConnect软件客户端在本地PC安装并且采取从远程PC的认证证书。一旦验证完成，远程用户获得访问到中央资源通过一个全双工SSL通道。远程用户配置有从池获取的IP地址管理由ASA。

本地PC设置

操作系统

操作系统(Windows、MacOS、Unix或者Linux)在您的本地PC一定是当前与安装的所有所需的补丁。

读卡器

一个电子卡读者在您的本地计算机必须安装为了使用eID卡。电子卡读者是establishs通信信道程序在计算机和芯片之间的在ID卡的硬件设备。

对于已批准卡片阅读机列表，参考此URL ：http://www.cardreaders.be/en/default.htm

注意： 为了使用卡片阅读机，您必须安装硬件厂商推荐的驱动程序。

eID运行时间软件

您必须安装比利时政府提供的eID运行时软件。此软件允许远程用户读，验证和打印eID卡的内容。软件是可用的用法语和荷兰语为Windows、MAC OS X和Linux。

欲知更多信息，参考此URL ：

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

验证证书

您必须导入验证证书到本地PC的Microsoft Windows存储。如果不能导入证书到存储，

AnyConnect客户端无法建立对ASA的SSL连接。

步骤

为了导入验证证书到Windows存储，请完成这些步骤：

1. 插入您的eID到卡片阅读机，并且启动中间件为了访问eID卡的内容。eID卡的内容出现。
2. 点击**Certificats** (FR)选项卡。证书层级显示。
3. 展开**比利时根CA**，然后展开**公民CA。**
4. 选择您的已命名证书**验证**版本。
5. 点击**Enregistrer** (FR)按钮。证书复制到Windows存储。

注意： 当您点击**详细信息按钮时**，窗口看来关于证书的显示详细信息。在详细信息选项卡，请选择**主题字段**为了查看Serial Number字段。Serial Number字段包含使用用户授权的一个唯一值。例如，序列号“56100307215"代表出生日期是十月第3的用户， 1956年与序号072和校验数字15。*您必须提交一个要求从联邦权限的批准为了存储这些编号。是您的责任做与比利时公民数据库的维护涉及的适当的正式说明您的国家的。*

验证

为了验证顺利地导入的证书，完成这些步骤：

1. 在Windows XP计算机，请打开DOS窗口，并且键入**mmc**命令。控制台应用程序出现。
2. 选择**File>添加/删除管理单元**(或请按Ctrl+M)。添加/删除卡扣式对话框出现。
3. 单击 **Add** 按钮。添加独立卡扣式对话框出现。
4. 在独立Snap-ins列出的联机，选择**证书**，并且单击**添加**。
5. 点击**我的用户帐户**单选按钮，并且点击**芬通社**。证书管理单元在添加/删除管理单元对话框出现。
6. 点击**Close**为了关闭添加独立卡扣式对话框，然后点击OK键在添加/删除卡扣式对话框内为了保存您的更改和返回对控制台应用程序。
7. 在控制台根文件夹下，请展开**证书-当前用户**。
8. 展开**个人**，然后展开**证书**。如此镜像所显示，已导入证书必须在Windows存储出现：

AnyConnect安装

您必须安装远程PC的AnyConnect客户端。AnyConnect软件使用可以编辑为了预先设定可用的网关列表的一个XML配置文件。XML文件在远程PC的此路径存储：

C:\Documents and Settings\ *%USERNAME%* \应用程序数据\思科\ Cisco AnyConnect VPN客户

那里*%USERNAME%*是用户的名称远程PC的。

XML文件的名称是*preferences.xml。这*是文件的内容的示例：

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

那里*192.168.0.1*是ASA网关的IP地址。

ASA需求

保证ASA符合这些要求：

- AnyConnect和ASDM在闪存必须运行。为了完成在本文的步骤，请以安装的适当的ASA 8.0软件使用ASA 5505。在闪存必须预先输入AnyConnect和ASDM应用程序。请使用**show flash命令**为了查看flash:内容`ciscoasa#show flash: --#-- --length-- -----date/time------ path 66 14524416 Jun 26 2007 10:24:02 asa802-k8.bin 67 6889764 Jun 26 2007 10:25:28 asdm-602.bin 68 2635734 Jul 09 2007 07:37:06 anyconnect-win-2.0.0343-k9.pkg`
- ASA必须以出厂默认设置运行。如果使用一个新的ASA机箱为了完成在本文的步骤您能跳过此需求。否则，请完成这些步骤为了重置ASA到出厂默认设置：在ASDM应用程序，请连接对ASA机箱，并且选择**File>重置设备对工厂默认配置**。留下在模板的默认值。连接您的在Ethernet0/1内部接口的PC，并且更新将由ASA的DHCP服务器设置的您的IP地址。**注意：** 为了重置ASA到从line命令的出厂默认设置，请使用这些命令：`ciscoasa#conf t ciscoasa#config factory-default 192.168.0.1 255.255.255.0`

ASA 配置

一旦重置ASA出厂默认设置，您能开始ASDM到192.168.0.1为了连接到在Ethernet0/1内部接口的ASA。

注意： 您的上一个密码保留默认情况下(或可以是空白的)。

默认情况下，ASA接受有一源IP地址的一流入管理会话在子网192.168.0.0/24。默认DHCP服务器在ASA的内部接口启用提供在范围192.168.0.2-129/24的IP地址，有效连接到与ASDM的内部接口。

完成这些步骤为了配置ASA ：

1. 启用外部接口
2. 配置域名、密码和系统时间
3. 启用在外部接口的一个DHCP服务器
4. 配置eID VPN地址池
5. 导入比利时根CA证书
6. 配置安全套接字协议层
7. 定义默认组策略
8. 定义证书映射
9. 添加一个本地用户
10. 重新启动ASA

步骤1.启用外部接口

此步骤描述如何启用外部接口。

1. 在ASDM应用程序，请点击**配置**，然后单击**设备设置**。
2. 在设备设置地区中，请选择**接口**，然后单击**接口**选项卡。
3. 选择外部接口，并且单击**编辑**。
4. 在常规选项卡的IP地址部分，请选择**使用静态IP**选项。
5. 进入IP地址的子网掩码的**197.0.100.1**和**255.255.255.0**。
6. 单击 **Apply**。

步骤2.配置域名、密码和系统时间

此步骤描述如何配置域名、密码和系统时间。

1. 在设备设置地区中，请选择**设备名/密码**。
2. 输入域名的**cisco.be**和回车cisco123for特权密码值。**注意：** 默认情况下，密码是空白的。
3. 单击 **Apply**。
4. 在设备设置地区中，请选择**系统时间**，并且更改时钟值(如果需要)。
5. 单击 **Apply**。

步骤3.启用在外部接口的DHCP服务器。

此步骤描述如何使在外部接口的一个DHCP服务器为了实现测试。

1. 单击 **Configuration**，然后单击 Device Management。
2. 在设备管理地区中，请展开**DHCP**，并且选择**DHCP服务器**。
3. 选择从接口列表的外部接口，并且单击**编辑**。编辑DHCP服务器对话框出现。
4. 检查**Enable (event) DHCP服务器**复选框。
5. 在DHCP地址池，请输入从197.0.100.20的一个IP地址到197.0.100.30。
6. 在全局DHCP选项地区中，请不选定**从接口检查**复选框的**Enable (event)自动配置**。
7. 单击 **Apply**。

步骤4.配置eID VPN地址池

此步骤描述如何定义使用设置远程AnyConnect客户端IP地址的池。

1. 单击 **Configuration**，然后单击 Remote Access VPN。
2. 在删除接入VPN地区中，请展开**网络(客户端)访问**，然后展开**地址分配**。
3. 选择**地址池**，然后单击**Add按钮**位于在名为的Configure IP地址游泳池周围。此时将出现 Add IP Pool 对话框。
4. 在Name字段，回车EID **VPNPOOL**。
5. 在开始的IP地址和结束IP地址字段，请输入范围从192.168.10.100的IP地址到192.168.10.110。
6. 从子网掩码下拉列表选择**255.255.255.0**，点击OK键和然后单击**应用**。

步骤5.导入比利时根CA证书

此步骤描述如何导入到ASA比利时根CA证书。

1. 下载并且安装比利时根CA证书(belgiumrca.crt和belgiumrca2.crt)从政府网站并且存储它在您的本地PC。比利时政府网站查找在此URL ：http://certs.eid.belgium.be/
2. 在远程访问VPN地区中，请展开**证书管理**，并且选择**CA证书**。
3. 单击**添加**，然后单击**安装从文件**。
4. 浏览到您保存比利时根CA证书的位置(belgiumrca.crt)文件，并且点击InstallCertificate。
5. 单击**应用**为了保存您的更改。

此镜像显示在ASA安装的证书：

步骤6.配置安全套接字协议层

此步骤描述如何优先安排安全加密选项，定义SSL VPN客户端镜像和定义连接配置文件。

1. 确定优先级多数安全加密选项。在远程访问VPN地区中，请展开**先进**，并且选择**SSL设置**。在加密部分，激活算法被堆积，顶部下来，如下：AES256-SHA1AES128-SHA13DES-SHA1RC4-SHA1
2. 定义AnyConnect客户端的SSL VPN客户端镜像。在远程访问VPN地区中，请展开**先进**，展开**SSL VPN**，并且选择**客户端设置**。在SSL VPN客户端镜像地区中，请单击**添加**。选择在闪存存储的AnyConnect包。如此镜像所显示， AnyConnect包在SSL VPN客户端镜像列表出现：
3. 定义DefaultWebVPNGroup连接配置文件。在远程访问VPN地区中，请展开**网络(客户端)访问**，并且选择**SSL VPN连接配置文件**。在访问接口地区中，请检查**Enable (event) Cisco AnyConnect VPN客户复选框**。如此镜像所显示，对于外部接口，请检查**允许**，**要求客户端证书**，并且**启用DTL**复选框：在连接配置文件地区中，请选择**DefaultWebVPNGroup**，并且单击**编辑**。编辑SSL VPN连接配置文件对话框出现。在定位区域中，请选择**基本**。在验证地区中，请点击**证书**单选按钮。在默认组政策方面中，请检查**SSL VPN客户端协议**复选框。展开**先进**，并且选择**验证**。如此镜像所显示，单击**添加**，并且添加与当地服务器组的外部接口：在定位区域中，请选择**授权**。在默认授权服务器组地区中，请从服务器组下拉列表选择**本地**，并且检查**用户必须存在授权数据库到Connect复选框**。在映射区域的用户名，请勿从主要的DN字段下拉列表选择**SER (序列号)**，从第二DN字段选择，并且点击OK键。

步骤7.定义默认组策略

此步骤描述如何定义默认组策略。

1. 在远程访问VPN地区中，请展开**网络(客户端)访问**，并且选择**组策略**。
2. 从组策略列表选择**DfltGrpPolicy**，并且单击**编辑**。
3. 编辑内部组策略对话框出现。
4. 从定位区域，请选择**常规**。
5. 对于地址池，请单击**精选**为了选择地址池，并且选择EID **VPNPOOL**。
6. 在更多选项地区中，请非选定**IPsec**和**L2TP/IPsec**复选框，并且点击OK键。

步骤8.定义证书映射

此步骤描述如何定义证书映射标准。

1. 在远程访问VPN地区中，请点击**先进**，并且选择**证书到SSL VPN连接配置文件地图**。
2. 在对连接配置文件地图地区的证书，请单击从地图列表**添加**，并且选择**DefaultCertificateMap**。此地图必须匹配在的*DefaultWEBVPNProfile*被映射对连接配置文件字段。
3. 在映射标准地区，请单击**添加**，并且添加这些值：字段：发布者，国家(c)，等于，“是”字段：发布者，共同名称(CN)，等于，“公民加州”如此镜像所显示，映射标准应该出现：
4. 单击 **Apply**。

步骤9.添加本地用户

此步骤如何描述添加本地用户。

1. 在远程访问VPN地区中，请展开**AAA设置**，并且选择**本地用户**。
2. 在本地用户用户区域中，请单击**添加**。
3. 在用户名字段，请输入用户证书的序列号。例如， 56100307215 (正如本文的验证证书部分所描述)。

4. 单击 Apply。

步骤10.重新启动ASA

重新启动ASA为了保证所有更改应用对系统服务。

优化

当测试时，一些SSL通道也许不适当地关闭。因为ASA假设， AnyConnect客户端可能断开和重新连接，通道没有丢弃，提供它机会回来。然而，在与基础许可证(2个SSL通道的实验室测试期间默认情况下)，您也许用尽您的许可证，当SSL通道没有适当地时关闭。如果此问题出现，请使用**vpn-sessiondb注销<option>**命令为了注销所有激活SSL会话。

一分钟配置

为了迅速创建工作配置，请重置您的ASA对出厂默认设置，并且粘贴在配置模式的此配置：

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
```

相关信息

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