ASA 8. x Anyconnect Аутентификация с бельгийской Картой EID

Содержание

Введение

Этот документ описывает, как установить ASA 8.x аутентификация Anyconnect для использования бельгийской карты EID.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- ASA 5505 с соответствующим программным обеспечением ASA 8.0
- AnyConnect Client
- ASDM 6.0

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

EID является PKI (Инфраструктура открытых ключей) карта, выполненная бельгийским правительством, которое пользователи должны использовать для аутентификации на удаленном Компьютере с операционной системой Windows. Клиентское программное обеспечение AnyConnect установлено на локальном компьютере и берет учетные данные для аутентификации от удаленного ПК. Как только аутентификация завершена, удаленный пользователь получает доступ к центральным ресурсам через полный туннель SSL. Удаленный пользователь настроен с IP-адресом, полученным из пула, которым управляет ASA.

Настройка локального компьютера

ОПЕРАЦИОННАЯ СИСТЕМА

Операционная система (Windows, MacOS, Unix или Linux) на вашем локальном компьютере должна быть текущей со всеми установленными необходимыми исправлениями.

Картридер

Электронный картридер должен быть установлен на вашем локальном компьютере для использования карты EID. Электронный картридер является аппаратным устройством что establishs канал связи между программами на компьютере и микросхемой на удостоверении личности.

Для списка утвержденных картридеров обратитесь к этому URL:

http://www.cardreaders.be/en/default.htm

Примечание: Для использования картридера необходимо установить драйверы, рекомендуемые поставщиком аппаратного обеспечения.

программное обеспечение Времени выполнения EID

Необходимо установить программное обеспечение времени выполнения EID, предоставленное бельгийским правительством. Это программное обеспечение позволяет удаленному пользователю читать, проверять, и распечатывать содержание карты EID. Программное обеспечение доступно на французском и нидерландском языке для Windows, MAC OS X и Linux.

Для получения дополнительной информации обратитесь к этому URL:

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

Опознавательный сертификат

Необходимо импортировать опознавательный сертификат в хранилище Microsoft Windows на локальном компьютере. Если вы будете не в состоянии импортировать сертификат в хранилище, то Клиент AnyConnect будет неспособен установить подключение SSL к ASA.

Процедура

Для импорта опознавательного сертификата в хранилище Windows выполните эти шаги:

1. Вставьте свой EID в картридер и запустите промежуточное программное обеспечение для доступа к содержанию карты EID.Содержание карты EID появляется.
2. Нажмите вкладку **Certificats (FR)**.Иерархия сертификатов отображена.
3. Разверните **Узел CA Бельгии**, и затем разверните **CA. Гражданина**
4. Выберите **Опознавательную** версию своего именованного сертификата.
5. Нажмите кнопку **Enregistrer (FR)**.Сертификат скопирован в хранилище Windows.

Примечание: При нажатии кнопки **Details** окно появляется, который отображает подробные данные о сертификате. Во вкладке Details выберите **Поле Тема** для просмотра поля Serial Number. Поле Serial Number содержит уникальное значение, которое используется для авторизации пользователя. Например, серийный номер “56100307215” представляет пользователя, дата рождения которого 3-го октября 1956 с порядковым номером 072 и контрольным разрядом 15. *Необходимо отправить запрос для утверждения федеральных властей для хранения этих номеров. Это - ваша обязанность сделать соответствующие официальные объявления отнесенными к обслуживанию базы данных бельгийских граждан в вашей стране*.

Проверка

Чтобы проверить, что сертификат, импортированный успешно, выполните эти шаги:

1. На машине Windows XP откройте Окно DOS и введите **mmc** команду.Консольное приложение появляется.
2. Выберите **File> Add/Remove Snap - в** (или нажмите Ctrl+M).Добавить/Удалить Моментальный снимок - в диалоговом окне появляется.

3. **Нажмите кнопку Add.**Добавление Автономного Моментального снимка - в диалоговом окне появляется.
4. В Доступном Автономном Поспешном-ins списке выберите **Certificates** и **нажмите Add**.
5. Нажмите **Мою** кнопку с зависимой фиксацией **учетной записи пользователя** и нажмите **Finish**.Моментальный снимок Сертификата - в появляется в Добавить/Удалить Моментальном снимке - в диалоговом окне.
6. Нажмите **Close**, чтобы закрыть Добавление Автономного Моментального снимка - в диалоговом окне, и затем нажать **OK** в Добавить/Удалить Моментальном снимке - в диалоговом окне, чтобы сохранить ваши изменения и возвратиться к Консольному приложению.
7. Под Корневой папкой консоли разверните **Сертификаты - Текущий пользователь**.
8. Расширьтесь **Персональный**, и затем разверните **Сертификаты**.Импортированный сертификат должен появиться в хранилище Windows как показано в этом образе:

Установка AnyConnect

Необходимо установить Клиента AnyConnect на удаленном ПК. Программное обеспечение AnyConnect использует конфигурационный XML-файл, который может быть отредактирован для предварительной установки списка доступных шлюзов. XML-файл сохранен в этом пути на удаленном ПК:

C : \Documents и параметры настройки *ИМЯ ПОЛЬЗОВАТЕЛЯ % %\Application* Data\Cisco\Cisco клиент AnyConnect VPN Client

где *%USERNAME %* является именем пользователя на удаленном ПК.

Название XML-файла является *preferences.xml*. Вот пример содержания файла:

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

где *192.168.0.1* IP-адрес шлюза ASA.

Требования ASA

Гарантируйте, что ASA удовлетворяет эти требования:

- AnyConnect и ASDM должны работать во флэш-памяти.Для завершения процедур в этом документе используйте ASA 5505 с соответствующим установленным программным обеспечением ASA 8.0. AnyConnect и приложения ASDM должны быть предварительно загружены во флэш-памяти. Используйте **команду show flash** для просмотра содержания флэш-памяти:`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 должен работать с заводскими настройками.Можно пропустить это требование при использовании нового шасси ASA для завершения процедур в этом документе. В противном случае выполните эти шаги для сброса ASA к заводским настройкам:В приложении ASDM соединитесь с шасси ASA и выберите **File> Reset Device к Заводской конфигурации по умолчанию**.Оставьте значения по умолчанию в шаблоне.Подключите

свой ПК на Ethernet 0/1 внутренний интерфейс и возобновите ваш IP-адрес, который будет настроен сервером DHCP ASA.**Примечание:** Для сброса ASA к заводским настройкам из командной строки используйте эти команды:`ciscoasa#`**`conf t`**
`ciscoasa#`**`config factory-default 192.168.0.1 255.255.255.0`**

Конфигурация ASA

Как только вы перезагружаете заводские настройки ASA, можно запустить ASDM к 192.168.0.1 для соединения с ASA на Ethernet 0/1 внутреннего интерфейса.

Примечание: Ваш предыдущий пароль сохранен (или это может быть пробел по умолчанию).

По умолчанию ASA принимает входящий сеанс управления с IP - адресом источника в подсети 192.168.0.0/24. Сервер DHCP по умолчанию, который включен на внутреннем интерфейсе ASA, предоставляет IP-адреса в диапазоне 192.168.0.2-129/24, допустимый для соединения с внутренним интерфейсом с ASDM.

Выполните эти шаги для настройки ASA:

1. Включите внешний интерфейс
2. Настройте доменное имя, пароль и системное время
3. Включите сервер DHCP на внешнем интерфейсе
4. Настройте Пул адресов VPN EID
5. Импортируйте корневой сертификат CA Бельгии
6. Настройте уровень защищенных сокетов
7. Определите политику группы по умолчанию
8. Определите сопоставление сертификата
9. Добавьте локального пользователя
10. Перезагрузите ASA

Шаг 1. Включите внешний интерфейс

Этот шаг описывает, как включить внешний интерфейс.

1. В приложении ASDM нажмите **Configuration**, и затем нажмите **Device Setup**.
2. В области Device Setup выберите **Interfaces**, и затем нажмите вкладку **Interfaces**.
3. Выберите внешний интерфейс и нажмите **Edit**.
4. В разделе IP-адреса Вкладки Общие выберите опцию **Use Static IP**.
5. Войдите **197.0.100.1** для IP-адреса и **255.255.255.0** для маски подсети.
6. **Щелкните "Применить".**

Шаг 2. Настройте доменное имя, пароль и системное время

Этот шаг описывает, как настроить доменное имя, пароль и системное время.

1. В области Device Setup выберите **Device Name / Пароль**.
2. Введите **cisco.be** для доменного имени и введите **cisco123** для значения Enable Password.**Примечание:** По умолчанию пароль является пробелом.

3. **Щелкните "Применить".**
4. В области Device Setup выберите **System Time** и измените значение часов (если необходимый).
5. **Щелкните "Применить".**

Шаг 3. Включите сервер DHCP на внешнем интерфейсе.

Этот шаг описывает, как включить сервер DHCP на внешнем интерфейсе для упрощения тестирования.

1. **Нажмите кнопку Configuration, после чего нажмите Device Management.**
2. В области Device Management разверните **DHCP** и выберите **DHCP Server**.
3. Выберите внешний интерфейс от Списка интерфейсов и нажмите **Edit**.Диалоговое окно Edit DHCP Server появляется.
4. Проверьте флажок **Enable DHCP Server**.
5. В пуле адресов DHCP введите IP-адрес от 197.0.100.20 до 197.0.100.30.
6. В области Global DHCP Options снимите флажок **с Разрешать автоматической конфигурацией от** коробки **проверки интерфейса**.
7. **Щелкните "Применить".**

Шаг 4. . Настройте Пул адресов VPN EID

Этот шаг описывает, как определить пул IP-адресов, которые используются для инициализации удаленных Клиентов AnyConnect.

1. **Щелкните Configuration, а затем выберите Remote Access VPN.**
2. В области Remove Access VPN разверните **сетевой доступ (клиент)**, и затем разверните **Назначение адреса**.
3. Выберите **Address Pools**, и затем нажмите**, кнопка Add**, расположенная в Настраивании именованного IP-адреса, объединяет область.Появится окно Add IP Pool.
4. В Поле имени введите **eID-VPNPOOL**.
5. В Стартовом IP-адресе и Конечных полях IP Address, введите диапазон IP-адреса от 192.168.10.100 до 192.168.10.110.
6. Выберите **255.255.255.0** из выпадающего списка Маски подсети, **нажмите OK**, и затем нажмите **Apply**.

Шаг 5. . Импортируйте корневой сертификат CA Бельгии

Этот шаг описывает, как импортировать в ASA Корневой сертификат CA Бельгии.

1. Загрузите и установите Корневые сертификаты CA Бельгии (belgiumrca.crt и belgiumrca2.crt) от правительственного веб-сайта и сохраните его на своем локальном компьютере.Правительственный веб-сайт Бельгии расположен в этом URL: http://certs.eid. бельгия. будьте /
2. В области Remote Access VPN разверните **Управление сертификатами** и выберите **CA Certificates**.
3. **Нажмите Add**, и затем нажмите **Install от файла**.
4. Перейдите к местоположению, в котором вы сохранили Корневой сертификат CA

Бельгии (belgiumrca.crt) файл, и нажмите **Install Certificate**.
5. Нажмите **Apply** для сохранения изменений.

Этот образ показывает сертификат, установленный на ASA:

Шаг 6. Настройте уровень защищенных сокетов

Этот шаг описывает, как расположить по приоритетам опции надежного шифрования, определить образ VPN-клиента SSL (SVC) и определить профиль подключения.

1. Расположите по приоритетам большинство опций надежного шифрования.В области Remote Access VPN расширьтесь **Усовершенствованный**, и выберите **SSL Settings**. В разделе Шифрования Активные Алгоритмы сложены, вершина вниз, следующим образом:AES256-SHA1AES128-SHA1SHA1 3DESSHA1 RC4
2. Определите образ VPN-клиента SSL (SVC) для Клиента AnyConnect.В области Remote Access VPN разверните **Усовершенствованный**, разверните **VPN SSL** и выберите **Client Settings**.В области SSL VPN Client Images **нажмите Add**.Выберите пакет AnyConnect, который сохранен во флэш-памяти.Пакет AnyConnect появляется в списке Образов VPN-клиента SSL (SVC) как показано в этом образе:
3. Определите профиль подключения DefaultWEBVPNGroup.В области Remote Access VPN разверните **сетевой доступ (клиент)** и выберите **SSL VPN Connection Profiles**.В области Access Interfaces проверьте **флажок Enable Cisco AnyConnect VPN Client**.Для внешнего интерфейса проверьте **Предоставить Доступ**, **Потребуйте Сертификата клиента** и флажков **Enable DTLS** как показано в этом образе:В области Connection Profiles выберите **DefaultWEBVPNGroup** и нажмите **Edit**.Диалоговое окно Edit SSL VPN Connection Profile появляется.В области навигации выберите **Basic**.В области Authentication нажмите кнопку с зависимой фиксацией **Certificate**.В области политики Группы по умолчанию проверьте флажок **SSL VPN Client Protocol**.Расширьтесь **Усовершенствованный**, и выберите **Authentication**.**Нажмите Add** и добавьте внешний интерфейс с группой локального сервера как показано в этом образе:В области навигации выберите **Authorization**.В области Default Authorization Server Group выберите **LOCAL** из выпадающего списка Группы серверов и проверьте**, что Пользователи должны существовать в базе данных авторизации к флажку connect**.В области User Name Mapping выберите **SER (Serial Number)** из Первичного DN Полевого выпадающего списка, выберите **None** из Дополнительного DN Поля и нажмите **OK**.

Шаг 7. Определите политику группы по умолчанию

Этот шаг описывает, как определить политику группы по умолчанию.

1. В области Remote Access VPN разверните **сетевой доступ (клиент)** и выберите **Group Policies**.
2. Выберите **DfltGrpPolicy** из списка групповых политик и нажмите **Edit**.
3. Диалоговое окно Edit Internal Group Policy появляется.
4. От области навигации выберите **General**.
5. Для Пулов адресов нажмите **Select**, чтобы выбрать пул адресов и выбрать **eID-VPNPOOL**.
6. В области More Options снимите флажок с флажками **IPsec и L2TP/IPsec** и нажмите **OK**.

Шаг 8. Определите сопоставление сертификата

Этот шаг описывает, как определить критерии сопоставления сертификата.

1. В области Remote Access VPN нажмите **Advanced** и выберите **Certificate to SSL VPN Connection Profile Maps**.
2. В области Certificate to Connection Profile Maps **нажмите Add** и выберите **DefaultCertificateMap** из списка карты.Эта карта должна совпасть *с DefaultWEBVPNProfile* в поле Mapped to Connection Profile.
3. В Области критериев Сопоставления **нажмите Add** и добавьте эти значения:Поле: отправитель, страна (C), равняется, “быть”Поле: Отправитель, Общее имя (CN), Равняется, “гражданин приблизительно”Критерии Сопоставления должны появиться как показано в этом образе:
4. **Щелкните "Применить".**

Шаг 9. Добавьте локального пользователя

Этот шаг описывает, как добавить локального пользователя.

1. В области Remote Access VPN разверните **Настройку AAA** и выберите **Local Users**.
2. В области Local Users **нажмите Add**.
3. В Поле имени пользователя введите серийный номер сертификата пользователя. Например, 56100307215 (как описано в Опознавательном разделе Сертификата этого документа).
4. **Щелкните "Применить".**

Шаг 10. Перезагрузите ASA

Перезагрузите ASA, чтобы гарантировать, что все изменения применены к работам системы.

Точная настройка

При тестировании некоторые туннели SSL не могли бы закрыть должным образом. Так как ASA предполагает, что Клиент AnyConnect может разъединить и воссоединиться, туннель не отброшен, который дает ему шанс возвратиться. Когда туннели SSL не закрыты должным образом, Однако во время лабораторных испытаний с базовой лицензией (2 туннеля SSL по умолчанию), вы могли бы исчерпать свою лицензию. Если эта проблема происходит, используйте команду *<option>* **выхода из системы vpn-sessiondb**, чтобы выйти из системы все активные сеансы SSL.

Одноминутная конфигурация

Для быстрого создания действующей конфигурации перезагрузите ASA к заводской настройке и вставьте эту конфигурацию в режиме конфигурации:

cisco ASA
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
```

Дополнительные сведения

- Cisco PIX Firewall Software
- Справочники по командам для межсетевого экрана PIX Cisco Secure
- Уведомления о дефектах продуктов по безопасности (включая PIX)
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация