ASA VPN Anyconnect и авторизация OpenLDAP с пользовательской схемой и примером конфигурации сертификатов

Содержание

Введение

Этот документ описывает, как настроить OpenLDAP с пользовательской схемой для поддержки атрибутов по каждому пользователю для защищенного мобильного клиента Cisco AnyConnect Secure Mobility, который соединяется с устройством адаптивной защиты Cisco (ASA). Конфигурация ASA является довольно основной, поскольку все атрибуты пользователя получены из сервера OpenLDAP. Также описанный в этом документе различия в проверке подлинности LDAP и авторизации, когда используется наряду с сертификатами.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о конфигурации Linux
- Базовые знания о Настройке интерфейса командной строки ASA

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Версия 8.4 Cisco ASA и позже
- Версия 2.4.30 OpenLDAP

Настройка

Основная конфигурация OpenLDAP

Шаг 1. Настройте сервер.

Данный пример использует дерево ldap тестового cisco.com.

файл ldap.conf используется для установки настроек по умолчанию уровня системы, которые могут использоваться локальным клиентом ldap.

Примечание: Несмотря на то, что вы не обязаны устанавливать настройки по умолчанию уровня системы, они могут помочь тестировать и устранять неполадки servier, когда вы выполняете локального клиента ldap.

/etc/openldap/ldap.conf:

```
BASE   dc=test-cisco,dc=com
```

файл slapd.conf используется для конфигурации сервера OpenLDAP. Файлы схемы по умолчанию включают широко используемые определения LDAP. Например, *человек* названия класса объекта определен в core.schema файле. Это использование конфигурации, что общая схема и определяет свою собственную схему для определяемых Cisco атрибутов.

/etc/openldap/slapd.conf:

```
include         /etc/openldap/schema/core.schema



include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/openldap.schema
include /etc/openldap/schema/nis.schema

# Defines backend database type and redirects all # queries with specified suffix to that
database
database hdb
suffix "dc=test-cisco,dc=com"
checkpoint 32 30

# Rootdn will be used to perform all administrative tasks.
rootdn          "cn=Manager,dc=test-cisco,dc=com"

# Cleartext passwords, especially for the rootdn, should be avoid.
rootpw          secret
```

```
directory /var/lib/openldap-data
index objectClass eq
```

Шаг 2. Проверьте Конфигурацию LDAP.

Чтобы проверить, что основной OpenLDAP работает, выполните эту конфигурацию:

```
include         /etc/openldap/schema/core.schema



include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/openldap.schema
include /etc/openldap/schema/nis.schema

# Defines backend database type and redirects all # queries with specified suffix to that
database
database hdb
suffix "dc=test-cisco,dc=com"
checkpoint 32 30

# Rootdn will be used to perform all administrative tasks.
rootdn          "cn=Manager,dc=test-cisco,dc=com"

# Cleartext passwords, especially for the rootdn, should be avoid.
rootpw          secret

directory /var/lib/openldap-data
index objectClass eq
```

Шаг 3. Добавьте записи на базу данных.

Однажды вы hve протестированный и настроенный everthing должным образом, добавьте записи на базу данных. Для добавления основных контейнеров для пользователей и групп, выполните эту конфигурацию:

```
include         /etc/openldap/schema/core.schema



include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/openldap.schema
include /etc/openldap/schema/nis.schema

# Defines backend database type and redirects all # queries with specified suffix to that
database
database hdb
suffix "dc=test-cisco,dc=com"
checkpoint 32 30

# Rootdn will be used to perform all administrative tasks.
rootdn          "cn=Manager,dc=test-cisco,dc=com"

# Cleartext passwords, especially for the rootdn, should be avoid.
rootpw          secret

directory /var/lib/openldap-data
index objectClass eq
```

Пользовательская схема Openldap

Теперь, когда базовая конфигурация работает, можно добавить пользовательскую схему. В этом примере конфигурации создан новый тип класса объекта по имени *Сископерсон*, и эти атрибуты создаются и используются в этом классе объекта:

- CiscoBanner
- CiscoACLin
- CiscoDomain
- CiscoDNS
- CiscoIPAddress
- CiscoIPNetmask
- CiscoSplitACL
- CiscoSplitTunnelPolicy
- CiscoGroupPolicy

Шаг 1. Создайте новую схему в cisco.schema.

```
include         /etc/openldap/schema/core.schema



include /etc/openldap/schema/cosine.schema
include /etc/openldap/schema/inetorgperson.schema
include /etc/openldap/schema/openldap.schema
include /etc/openldap/schema/nis.schema

# Defines backend database type and redirects all # queries with specified suffix to that
database
database hdb
suffix "dc=test-cisco,dc=com"
checkpoint 32 30

# Rootdn will be used to perform all administrative tasks.
rootdn          "cn=Manager,dc=test-cisco,dc=com"

# Cleartext passwords, especially for the rootdn, should be avoid.
rootpw          secret

directory /var/lib/openldap-data
index objectClass eq
```

Важные примечания

- Используйте OID частного предприятия для своей компании. Любые OID будут wor, но оптимальный метод должен использовать OID, назначенные IANA. Тот, настроенный в данных примерах, начинается от 1.3.6.1.4.1.9 (который зарезервирован Cisco: http://www.iana.org/assignments/enterprise-numbers).
- Следующая часть OID (500.1.1-500.1.9) использовалась для не вмешательства непосредственно в основное дерево OID Cisco ("1.3.6.1.4.1.9").
- Эта база данных использует класс объекта *Человека*, определенный в schema/core.ldif. Тот объект имеет тип TOP, и записи могут включать только один такой атрибут (который является, почему класс объекта *Сископерсона* имеет Вспомогательный тип).
- Класс объекта по имени *Сископерсон* должен включать SN или CN и может включать любой из пользовательских атрибутов Cisco, определенных ранее. Обратите внимание на то, что это может также включать любые другие атрибуты, определенные в другие схемы (такие как *userPassword* или *telephoneNumber*).
- Помните, что каждый объект должен иметь другой номер OID.

- Настраиваемые атрибуты нечувствительны к регистру и *строкового типа* с кодированием UTF 8 и максимальные 128 символов (определенный SYNTAX).

Шаг 2. Включайте схему в sldap.conf.

```
pluton openldap # cat slapd.conf | grep include
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/cisco.schema
```

Шаг 3. Перезапустите службы.

```
pluton openldap # cat slapd.conf | grep include
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/cisco.schema
```

Шаг 4. . Add a New User со всеми настраиваемыми атрибутами.

В данном примере пользователь принадлежит множественным объектам objectClass, и он наследовал атрибуты от всех них. С этим процессом легко добавить дополнительную схему или атрибуты без изменений к записям существующей базы данных.

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

Шаг 5. . Установите пароль для пользователя.

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

Шаг 6. Проверка конфигурации.

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
```

```
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

Конфигурация ASA

Шаг 1. Настройте интерфейс и сертификат.

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

Шаг 2. Генерируйте подписанный сертификат.

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
```

```
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

Шаг 3. Включение WebVPN на внешнем интерфейсе.

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

Шаг 4. . Разделите конфигурацию списков управления доступом (ACL).

Название ACL возвращено OpenLDAP:

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
```

```
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

Шаг 5. . Создайте имя группы туннелей, которое использует групповую политику по умолчанию (DfltAccessPolicy).

Пользователи с определенным атрибутом LDAP *(CiscoGroupPolicy)* сопоставлены с другой политикой: POLICY1

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
```

```
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

Конфигурация aaa-server ASA использует карту атрибутов LDAP для сопоставления от атрибутов, возвращенных OpenLDAP к атрибутам, которые могут быть интерпретированы ASA для пользователей Anyconnect.

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

Шаг 6. Включите Сервер LDAP для аутентификации для указанной туннельной группы.

```
pluton # cat users.ldiff
# User account
dn: uid=cisco,ou=people,dc=test-cisco,dc=com
cn: John Smith
givenName: John
sn: cisco
uid: cisco
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cisco
mail: jsmith@dev.local
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: CiscoPerson
loginShell: /bin/bash
userPassword: {CRYPT}*
CiscoBanner: This is banner 1
```

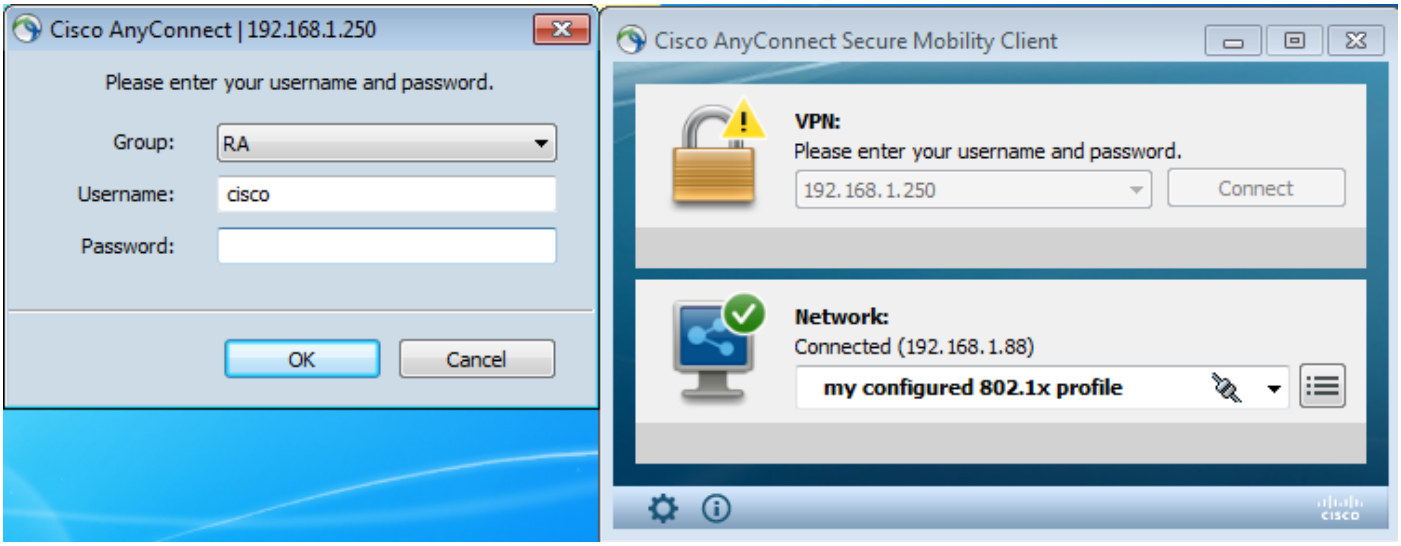
```
CiscoIPAddress: 10.1.1.1
CiscoIPNetmask: 255.255.255.128
CiscoDomain: domain1.com
CiscoDNS: 10.6.6.6
CiscoACLin: ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
CiscoSplitACL: ACL1
CiscoSplitTunnelPolicy: 1
CiscoGroupPolicy: POLICY1

pluton # ldapadd -h 192.168.10.1 -D "CN=Manager,DC=test-cisco,DC=com"
-w secret -x -f users.ldiff
adding new entry "uid=cisco,ou=people,dc=test-cisco,dc=com"
```

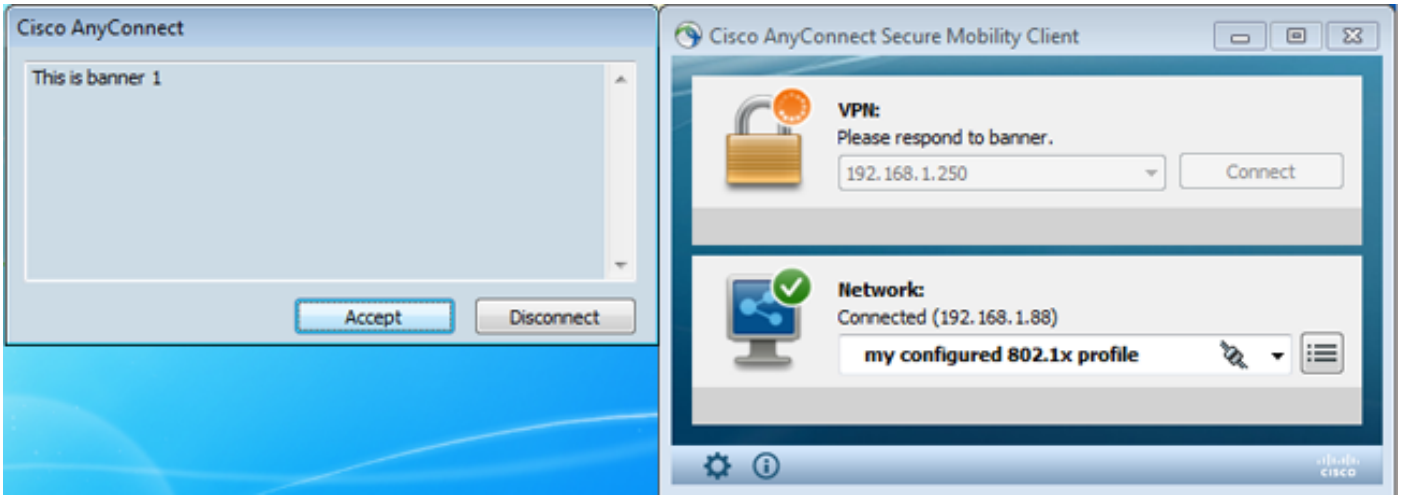
Проверка

Тестовый доступ VPN

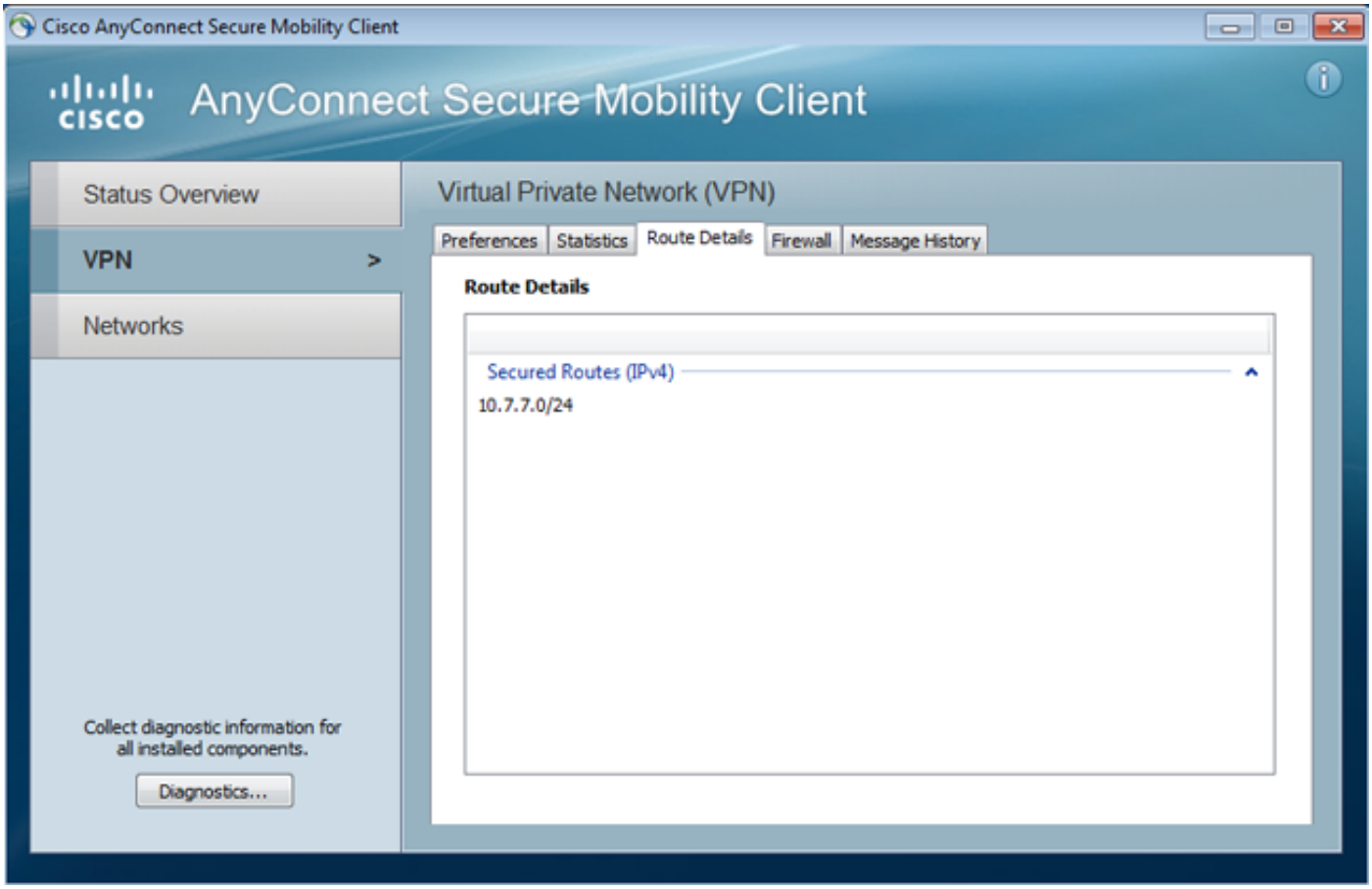
Anyconnect настроен для соединения с 192.168.1.250. Войдите *имя пользователя cisco* и *пароль pass1*.



После аутентификации используется корректный баннер.



Корректный раздельный ACL передается (ACL1, определенный на ASA).



Интерфейс Anyconnect настроен с IP: 10.1.1.1 и маска подсети 255.255.255.128. Домен является domain1.com, и сервер DNS 10.6.6.6.

```
Ethernet adapter Połączenie lokalne 2:

   Connection-specific DNS Suffix  . : domain1.com
   Description . . . . . . . . . . . : Cisco AnyConnect Secure Mobility Client V
irtual Miniport Adapter for Windows x64
   Physical Address. . . . . . . . . : 00-05-9A-3C-7A-00
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2015:d34b:e3a8:1787%14(Preferred)
   Link-local IPv6 Address . . . . . : fe80::3a02:5a4a:4b9b:ddf2%14(Preferred)
   Link-local IPv6 Address . . . . . : fe80::4fd8:3523:c111:ad1d%14(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.1.1.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.128
   Default Gateway . . . . . . . . . : ::
   DNS Servers . . . . . . . . . . . : 10.6.6.6
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

На ASA пользовательский *Cisco* получил IP: 10.1.1.1 и назначен на групповую политику *POLICY1*.

```
ASA# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 29
Assigned IP  : 10.1.1.1               Public IP    : 192.168.1.88
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : RC4                    Hashing      : none SHA1
Bytes Tx     : 10212                  Bytes Rx     : 856
Pkts Tx      : 8                      Pkts Rx      : 2
Pkts Tx Drop : 0                       Pkts Rx Drop : 0
Group Policy : POLICY1                 Tunnel Group : RA
Login Time   : 10:18:25 UTC Thu Apr 4 2013
Duration     : 0h:00m:17s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
```

```
VLAN Mapping : N/A                    VLAN        : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1

AnyConnect-Parent:
 Tunnel ID   : 29.1
 Public IP   : 192.168.1.88
 Encryption  : none                   TCP Src Port : 49262
 TCP Dst Port : 443                    Auth Mode   : userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Client Type : AnyConnect
 Client Ver  : 3.1.01065
 Bytes Tx    : 5106                   Bytes Rx    : 788
 Pkts Tx     : 4                      Pkts Rx     : 1
 Pkts Tx Drop : 0                      Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID   : 29.2
 Assigned IP : 10.1.1.1               Public IP   : 192.168.1.88
 Encryption  : RC4                    Hashing     : SHA1
 Encapsulation: TLSv1.0                TCP Src Port : 49265
 TCP Dst Port : 443                    Auth Mode   : userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
 Client Type : SSL VPN Client
 Client Ver  : Cisco AnyConnect VPN Agent for Windows 3.1.01065
 Bytes Tx    : 5106                   Bytes Rx    : 68
 Pkts Tx     : 4                      Pkts Rx     : 1
 Pkts Tx Drop : 0                      Pkts Rx Drop : 0
 Filter Name : AAA-user-cisco-E0CF3C05

NAC:
 Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
 SQ Int (T)  : 0 Seconds              EoU Age(T)  : 17 Seconds
 Hold Left (T): 0 Seconds              Posture Token:
```

Кроме того, динамический список доступа установлен для того пользователя:

```
ASA# show access-list AAA-user-cisco-E0CF3C05
access-list AAA-user-cisco-E0CF3C05; 1 elements; name hash: 0xf9b6b75c (dynamic)
access-list AAA-user-cisco-E0CF3C05 line 1 extended permit
ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
(hitcnt=0) 0xf8010475
```

Отладка

После включения отладок можно отследить каждый шаг сеанса WebVPN.

Данный пример показывает проверку подлинности LDAP наряду с извлечением атрибута:

```
ASA# show debug
debug ldap enabled at level 255
debug webvpn anyconnect enabled at level 254
ASA#
[63] Session Start
[63] New request Session, context 0xbbe10120, reqType = Authentication
[63] Fiber started
[63] Creating LDAP context with uri=ldap://192.168.11.10:389
[63] Connect to LDAP server: ldap://192.168.11.10:389, status = Successful
[63] supportedLDAPVersion: value = 3
[63] Binding as Manager
[63] Performing Simple authentication for Manager to 192.168.11.10
[63] LDAP Search:
```

```
       Base DN = [DC=test-cisco,DC=com]
       Filter = [uid=cisco]
       Scope  = [SUBTREE]
[63] User DN = [uid=cisco,ou=People,dc=test-cisco,dc=com]
[63] Server type for 192.168.11.10 unknown - no password policy
[63] Binding as cisco
[63] Performing Simple authentication for cisco to 192.168.11.10
[63] Processing LDAP response for user cisco
[63] Authentication successful for cisco to 192.168.11.10
[63] Retrieved User Attributes:
[63]   cn: value = John Smith
[63]   givenName: value = John
[63]   sn: value = cisco
[63]   uid: value = cisco
[63]   uidNumber: value = 10000
[63]   gidNumber: value = 10000
[63]   homeDirectory: value = /home/cisco
[63]   mail: value = jsmith@dev.local
[63]   objectClass: value = top
[63]   objectClass: value = posixAccount
[63]   objectClass: value = shadowAccount
[63]   objectClass: value = inetOrgPerson
[63]   objectClass: value = organizationalPerson
[63]   objectClass: value = person
[63]   objectClass: value = CiscoPerson
[63]   loginShell: value = /bin/bash
```

Важно! Пользовательские атрибуты LDAP сопоставлены с атрибутами ASA, как определено в карте атрибутов LDAP:

```
[63]   CiscoBanner: value = This is banner 1
[63]           mapped to Banner1: value = This is banner 1
[63]   CiscoIPAddress: value = 10.1.1.1
[63]           mapped to IETF-Radius-Framed-IP-Address: value = 10.1.1.1
[63]   CiscoIPNetmask: value = 255.255.255.128
[63]           mapped to IETF-Radius-Framed-IP-Netmask: value = 255.255.255.128
[63]   CiscoDomain: value = domain1.com
[63]           mapped to IPSec-Default-Domain: value = domain1.com
[63]   CiscoDNS: value = 10.6.6.6
[63]           mapped to Primary-DNS: value = 10.6.6.6
[63]   CiscoACLin: value = ip:inacl#1=permit
ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
[63]           mapped to Cisco-AV-Pair: value = ip:inacl#1=permit
ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0
[63]   CiscoSplitACL: value = ACL1
[63]           mapped to IPSec-Split-Tunnel-List: value = ACL1
[63]   CiscoSplitTunnelPolicy: value = 1
[63]           mapped to IPSec-Split-Tunneling-Policy: value = 1
[63]   CiscoGroupPolicy: value = POLICY1
[63]           mapped to IETF-Radius-Class: value = POLICY1
[63]           mapped to LDAP-Class: value = POLICY1
[63]   userPassword: value = {SSHA}5s81Fmi/9aG/WfPSy3lGmw1ORI4lywWC
[63] ATTR_CISCO_AV_PAIR attribute contains 68 bytes
[63] Fiber exit Tx=315 bytes Rx=907 bytes, status=1
[63] Session End
```

Сеанс LDAP закончен. Теперь, ASA обрабатывает и применяет те атрибуты.

Динамический ACL создан (на основе ACE запись в Cisco-av-pair):

```
webvpn_svc_parse_acl: processing ACL: name: 'AAA-user-cisco-E0CF3C05',
list: YES, id -1
webvpn_svc_parse_acl: before add: acl_id: -1, acl_name: AAA-user-cisco-E0CF3C05
webvpn_svc_parse_acl: after add: acl_id: 5, acl_name: AAA-user-cisco-E0CF3C05,
```

```
refcnt: 1
```

Доходы сеанса WebVPN:

```
webvpn_rx_data_tunnel_connect
CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 192.168.1.250'
Processing CSTP header line: 'Host: 192.168.1.250'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.01065'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent
for Windows 3.1.01065'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.01065'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=1476503744@122880@
1365070898@908F356D1C1F4CDF1138088854AF0E480FDCB1BD'
Processing CSTP header line: 'Cookie: webvpn=1476503744@122880@
1365070898@908F356D1C1F4CDF1138088854AF0E480FDCB1BD'
Found WebVPN cookie: 'webvpn=1476503744@122880@
1365070898@908F356D1C1F4CDF1138088854AF0E480FDCB1BD'
WebVPN Cookie: 'webvpn=1476503744@122880@1365070898@
908F356D1C1F4CDF1138088854AF0E480FDCB1BD'
IPADDR: '1476503744', INDEX: '122880', LOGIN: '1365070898'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
Setting version to '1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: admin-Komputer'
Processing CSTP header line: 'X-CSTP-Hostname: admin-Komputer'
Setting hostname to: 'admin-Komputer'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1367'
Processing CSTP header line: 'X-CSTP-MTU: 1367'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Local-Address-IP4: 192.168.1.88'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1468'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Remote-Address-IP4: 192.168.1.250'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: F5ADDD0151261404504FC3B165C3B68A90E51
A1C8EB7EA9B2FE70F1EB8E10929FFD79650B07E218EC8774678CDE1FB5E'
Processing CSTP header line: 'X-DTLS-Master-Secret: F5ADDD015126140450
4FC3B165C3B68A90E51A1C8EB7EA9B2FE70F1EB8E10929FFD79650B07E2
18EC8774678CDE1FB5E'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:
DES-CBC3-SHA:DES-CBC-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol:
Copyright (c) 2004 Cisco Systems, Inc.'
```

Затем, назначение адреса происходит. Предупреждение там не является никаким пулом IP, определенным на ASA. Если LDAP не возвращает атрибут *CiscoIPAddress* (который сопоставляется с *IETF-Radius-Framed-IP-Address* и используется для присвоения IP-адреса), конфигурация отказала бы на данном этапе.

```
Validating address: 10.1.1.1
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 10.1.1.1/255.255.255.128
webvpn_cstp_accept_ipv6_address: No IPv6 Address
CSTP state = HAVE_ADDRESS
```

Сеанс WebVPN завершает:

```
SVC: NP setup
np_svc_create_session(0x1E000, 0xb5eafa80, TRUE)
webvpn_svc_np_setup
SVC ACL Name: AAA-user-cisco-E0CF3C05
SVC ACL ID: 5
SVC ACL ID: 5
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
```

ASA отдельная проверка подлинности и авторизация

Иногда лучше разделить процесс проверки подлинности и авторизация. Например, используйте проверку подлинности с помощью пароля для локально определенных пользователей; тогда, после успешной локальной проверки подлинности, получите все атрибуты пользователя из Сервера LDAP:

```
SVC: NP setup
np_svc_create_session(0x1E000, 0xb5eafa80, TRUE)
webvpn_svc_np_setup
SVC ACL Name: AAA-user-cisco-E0CF3C05
SVC ACL ID: 5
SVC ACL ID: 5
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
```

Различие находится на сеансе LDAP. В предыдущем примере, ASA:

- связанный к OpenLDAP с учетными данными Менеджера,
- выполненный поиск пользовательского *Cisco*, и
- связанный (простая проверка подлинности) к OpenLDAP с учетными данными Cisco.

В настоящее время, с авторизацией LDAP, шаг третий больше не необходим, так как пользователь уже аутентифицировался через локальную базу данных.

Больше общих сценариев включает использование маркеров RSA для процесса проверки подлинности и атрибутов LDAP/AD для авторизации.

Атрибуты ASA от LDAP и локальной группы

Важно понять различие между атрибутами LDAP и атрибутами RADIUS.

При использовании LDAP ASA не позволяет сопоставлять с любым *атрибутом RADIUS*. Например, при использовании RADIUS возможно возвратиться*, Cisco-av-pair* приписывают 217 (Пулы адресов). Тот атрибут определяет локально настроенный пул IP-адресов, которые используются для присвоения IP-адресов.

С сопоставлением LDAP невозможно использовать тот определенный атрибут *Cisco-av-pair*. Атрибут *Cisco-av-pair* с сопоставлением LDAP может использоваться только для определения различных типов ACL.

Эти ограничения в LDAP препятствуют тому, чтобы он был так же гибок как Радиус. К workaroud эта локально определенная групповая политика может быть создана на ASA с атрибутами, которые не могут быть сопоставлены от ldap (как Пулы адресов). Как только пользователь LDAP аутентифицируется, они назначены на ту групповую политику (в нашем примере POLICY1) и non определяемые пользователем атрибуты повторно полученный из групповой политики.

Полный список атрибутов, поддерживаемый сопоставлением LDAP, может быть найден в этом документе: руководство по настройке Cisco ASA 5500 с помощью CLI, 8.4 и 8.6

Можно выдержать сравнение с полным списком атрибутов VPN3000 RADIUS, поддерживаемых ASA; обратитесь к этому документу: руководство по настройке Cisco ASA 5500 с помощью CLI, 8.4 и 8.6

См. этот документ для полного списка атрибутов IETF RADIUS, поддерживаемых ASA: руководство по настройке Cisco ASA 5500 с помощью CLI, 8.4 и 8.6

ASA и LDAP с проверкой подлинности сертификата

ASA не поддерживает извлечение атрибута сертификата LDAP и двоичное сравнение с сертификатом, предоставленным Anyconnect. Та функциональность зарезервирована для ACS Cisco или ISE (и только для соискателей 802.1x), потому что аутентификация VPN завершена на устройстве доступа к сети (NAD).

Существует другой soluction. Когда проверка подлинности пользователя использует сертификаты, ASA выполняет проверку достоверности сертификата и может получить

атрибуты LDAP на основе определенных полей от сертификата (например, CN):

```
SVC: NP setup
np_svc_create_session(0x1E000, 0xb5eafa80, TRUE)
webvpn_svc_np_setup
SVC ACL Name: AAA-user-cisco-E0CF3C05
SVC ACL ID: 5
SVC ACL ID: 5
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
```

После того, как сертификат пользователя проверен ASA, авторизация LDAP выполнена, и атрибуты пользователя (от поля CN) получены и применены.

Отладка

Сертификат пользователя использовался: cn=test1, ou=Security, o=Cisco, l=Krakow, st=PL, c=PL

Сопоставление сертификата настроено для сопоставления того сертификата с туннельной группой RA:

```
SVC: NP setup
np_svc_create_session(0x1E000, 0xb5eafa80, TRUE)
webvpn_svc_np_setup
SVC ACL Name: AAA-user-cisco-E0CF3C05
SVC ACL ID: 5
SVC ACL ID: 5
vpn_put_uauth success!
SVC IPv6 ACL Name: NULL
SVC IPv6 ACL ID: -1
SVC: adding to sessmgmt
SVC: Sending response
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP state = CONNECTED
```

Проверка достоверности сертификата и сопоставление:

```
ASA# show debug
debug ldap enabled at level 255
debug webvpn anyconnect enabled at level 254
debug crypto ca enabled at level 3
debug crypto ca messages enabled at level 3
debug crypto ca transactions enabled at level 3Apr 09 2013 17:31:32: %ASA-7-717025: Validating
certificate chain containing 1 certificate(s).Apr 09 2013 17:31:32: %ASA-7-717029: Identified
client certificate within certificate chain. serial number: 00FE9C3D61E131CDB1, subject name:
cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL.Apr 09 2013 17:31:32: %ASA-6-717022:
Certificate was successfully validated. Certificate is resident and trusted, serial number:
00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL.Apr 09 2013
```

17:31:32: %ASA-6-717028: **Certificate chain was successfully validated** with revocation status check.Apr 09 2013 17:31:32: %ASA-6-717028: **Certificate chain was successfully validated** with revocation status check.Apr 09 2013 17:31:32: %ASA-7-717036: **Looking for a tunnel group match based on certificate maps** for peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.Apr 09 2013 17:31:32: %ASA-7-717038: **Tunnel group match found. Tunnel Group: RA**, Peer certificate: serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.

Экстракция имени пользователя от сертификата и авторизации с помощью LDAP:

Apr 09 2013 17:31:32: %ASA-7-113028: **Extraction of username from VPN client certificate has been requested**. [Request 53]Apr 09 2013 17:31:32: %ASA-7-113028: **Extraction of username from VPN client certificate has been requested**. [Request 53]Apr 09 2013 17:31:32: %ASA-7-113028: **Extraction of username from VPN client certificate has been requested**. [Request 53]Apr 09 2013 17:31:32: %ASA-7-113028: **Extraction of username from VPN client certificate has been requested**. [Request 53]Apr 09 2013 17:31:32: %ASA-7-113028: **Extraction of username from VPN client certificate has been requested**. [Request 53]Apr 09 2013 17:31:32: %ASA-6-113004: **AAA user authorization Successful : server = 192.168.11.10 : user = test1**Apr 09 2013 17:31:32: %ASA-6-113004: **AAA user authorization Successful : server = 192.168.11.10 : user = test1**Apr 09 2013 17:31:32: %ASA-6-113004: **AAA user authorization Successful : server = 192.168.11.10 : user = test1**Apr 09 2013 17:31:32: %ASA-6-113004: **AAA user authorization Successful : server = 192.168.11.10 : user = test1**Apr 09 2013 17:31:32: %ASA-6-113004: **AAA user authorization Successful : server = 192.168.11.10 : user = test1**

Извлечение атрибутов от LDAP:

Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**cn = John Smith**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**givenName = John**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**sn = test1**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**uid = test1**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**uidNumber = 10000**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**gidNumber = 10000**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**homeDirectory = /home/cisco**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**mail = jsmith@dev.local**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**objectClass.1 = top**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**objectClass.2 = posixAccount**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**objectClass.3 = shadowAccount**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**objectClass.4 = inetOrgPerson**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**objectClass.5 = organizationalPerson**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**objectClass.6 = person**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**objectClass.7 = CiscoPerson**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**loginShell = /bin/bash**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**userPassword = {CRYPT}***Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**CiscoBanner = This is banner 1**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**CiscoIPAddress = 10.1.1.1**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**CiscoIPNetmask = 255.255.255.128**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**CiscoDomain = domain1.com**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**CiscoDNS = 10.6.6.6**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**CiscoACLin = ip:inacl#1=permit ip 10.1.1.0 255.255.255.128 10.11.11.0 255.255.255.0**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**CiscoSplitACL = ACL1**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**CiscoSplitTunnelPolicy = 1**Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.ldap.**CiscoGroupPolicy = POLICY1**

Cisco сопоставила attibutes:

```
Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.cisco.grouppolicy = POLICY1Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr
192.168.1.88: Session Attribute aaa.cisco.ipaddress = 10.1.1.1Apr 09 2013 17:31:32: %ASA-7-
734003: DAP: User test1, Addr 192.168.1.88: Session Attribute aaa.cisco.username = test1Apr 09
2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr 192.168.1.88: Session Attribute
aaa.cisco.username1 = test1Apr 09 2013 17:31:32: %ASA-7-734003: DAP: User test1, Addr
192.168.1.88: Session Attribute aaa.cisco.username2 = Apr 09 2013 17:31:32: %ASA-7-734003: DAP:
User test1, Addr 192.168.1.88: Session Attribute aaa.cisco.tunnelgroup = RAApr 09 2013 17:31:32:
%ASA-6-734001: DAP: User test1, Addr 192.168.1.88, Connection AnyConnect: The following DAP
records were selected for this connection: DfltAccessPolicyApr 09 2013 17:31:32: %ASA-6-113039:
Group <POLICY1> User <test1> IP <192.168.1.88> AnyConnect parent session started.Apr 09 2013
17:31:32: %ASA-6-113039: Group <POLICY1> User <test1> IP <192.168.1.88> AnyConnect parent
session started.
```

Вспомогательная проверка подлинности

Если двухфакторная аутентификация требуется, возможно использовать пароль токена наряду с проверкой подлинности LDAP и авторизацией:

```
Apr 09 2013 17:31:32: %ASA-6-113039: Group <POLICY1> User <test1> IP <192.168.1.88> AnyConnect
parent session started.
```

Затем пользователь должен предоставить имя пользователя и пароль от RSA (что-то, что пользователь имеет — маркер), наряду с именем пользователя/паролем LDAP (что-то, что пользователь знает). Также возможно использовать имя пользователя от сертификата для вспомогательной проверки подлинности. Для получения дополнительной информации о двойной аутентификации, обратитесь к руководству по настройке Cisco ASA 5500 с помощью CLI, 8.4 и 8.6.

Дополнительные сведения

- Руководство по настройке Cisco ASA 5500 с помощью CLI, 8.4 и 8.6
- Программное обеспечение OpenLDAP руководство 2.4 администраторов
- Номера частного предприятия
- Cisco Systems – техническая поддержка и документация