Двойная аутентификация AnyConnect ASA с проверкой достоверности сертификата, сопоставлением и руководством по конфигурации перед заливкой

Содержание

Введение

Этот документ описывает пример конфигурации для доступа защищенного мобильного клиента Cisco AnyConnect Secure Mobility Устройства адаптивной защиты (ASA), который использует двойную аутентификацию с проверкой достоверности сертификата. Как пользователь AnyConnect, необходимо предоставить корректный сертификат и учетные данные для основного и вспомогательной проверки подлинности для получения доступа VPN. Этот документ также предоставляет примеру сопоставления сертификата с функцией перед заливкой.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о конфигурации интерфейса командной строки (CLI) ASA и конфигурации VPN Протокола SSL
- Базовые знания о сертификатах X509

Используемые компоненты

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

- Программное обеспечение Cisco Adaptive Security Appliance (ASA), версия 8.4 и позже
- Windows 7 с защищенным мобильным клиентом Cisco AnyConnect Secure Mobility 3.1

Предполагается, что вы использовали внешний Центр сертификации (CA) для генерации:

- Стандарт криптографии общего ключа #12 (PKCS #12) закодированный base64 сертификат для ASA (anyconnect.pfx)
- PKCS #12 сертификат для AnyConnect

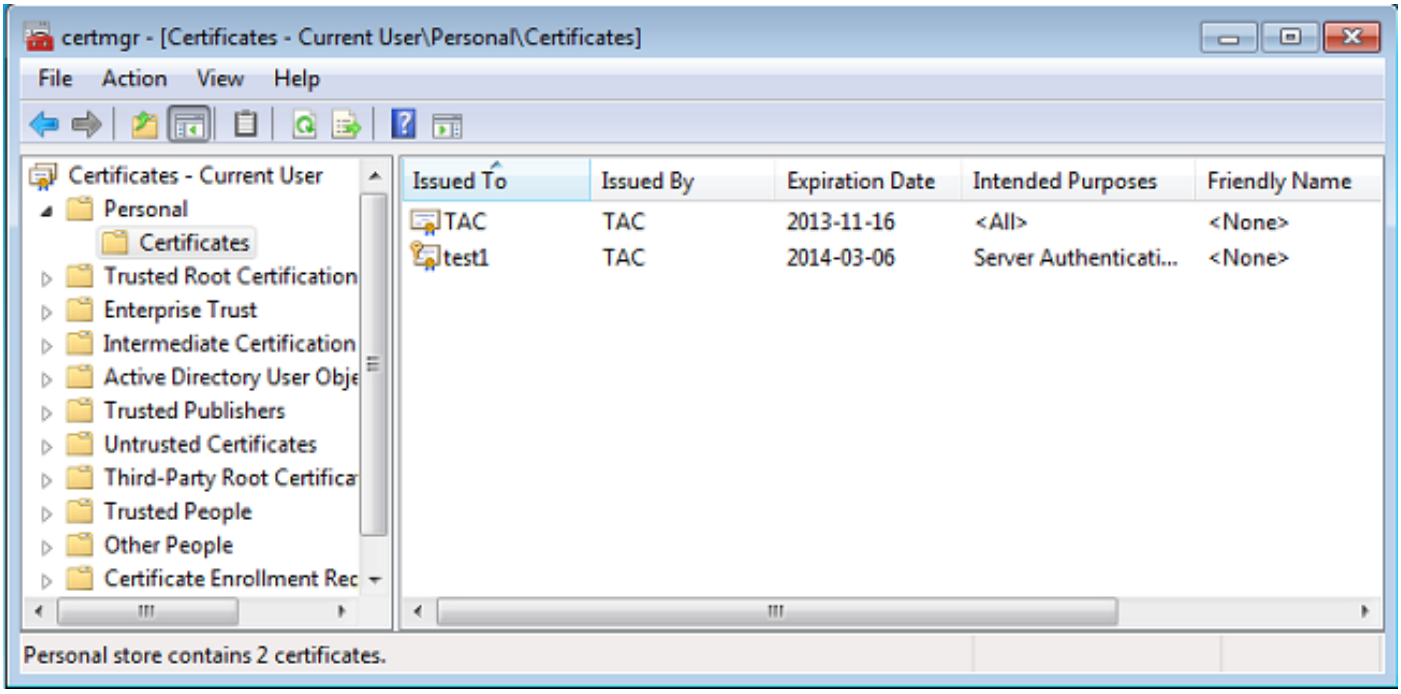
Настройка

> **Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Сертификат для AnyConnect

Для установки сертификата в качестве примера дважды нажмите anyconnect.pfx файл и установите тот сертификат как персональный сертификат.

Используйте Менеджера сертификатов (certmgr.msc) для проверки установки:



По умолчанию AnyConnect пытается найти сертификат в пользовательском хранилище Microsoft; нет никакой потребности внести любые изменения в профиле AnyConnect.

Установка сертификатов на ASA

Данный пример показывает, как ASA может импортировать PKCS base64 #12 сертификат:

```
BSNS-ASA5580-40-1(config)# crypto ca import CA pkcs12 123456

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJAQIBAzCCCMcGCSqGSIb3DQEHAaCCCLgEggi0MIIIsDCCBa8GCSqGSIb3DQEH
...
<output ommitted>
...
83EwMTAhMAkGBSsOAwIaBQAEFCS/WBSkrOIeT1HARHbLF1FFQvSvBAhu0j9bTtZo
3AICCAA=
quit

INFO: Import PKCS12 operation completed successfully
```

Используйте **команду show crypto ca certificates** для проверки импорта:

```
BSNS-ASA5580-40-1(config)# crypto ca import CA pkcs12 123456

Enter the base 64 encoded pkcs12.
End with the word "quit" on a line by itself:
MIIJAQIBAzCCCMcGCSqGSIb3DQEHAaCCCLgEggi0MIIIsDCCBa8GCSqGSIb3DQEH
...
<output ommitted>
...
83EwMTAhMAkGBSsOAwIaBQAEFCS/WBSkrOIeT1HARHbLF1FFQvSvBAhu0j9bTtZo
3AICCAA=
quit

INFO: Import PKCS12 operation completed successfully
```

Примечание: [Средство интерпретации выходных данных (только зарегистрированные клиенты)] поддерживает **некоторые команды show. Используйте Средство**

интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.

Конфигурация ASA для одиночной аутентификации и проверки достоверности сертификата

ASA использует и аутентификацию аутентификации, авторизации и учета (AAA) и проверку подлинности сертификата. Проверка достоверности сертификата является обязательной. Аутентификация AAA (проверка подлинности, авторизация и учет) использует локальную базу данных.

Данный пример показывает одиночную аутентификацию с проверкой достоверности сертификата.

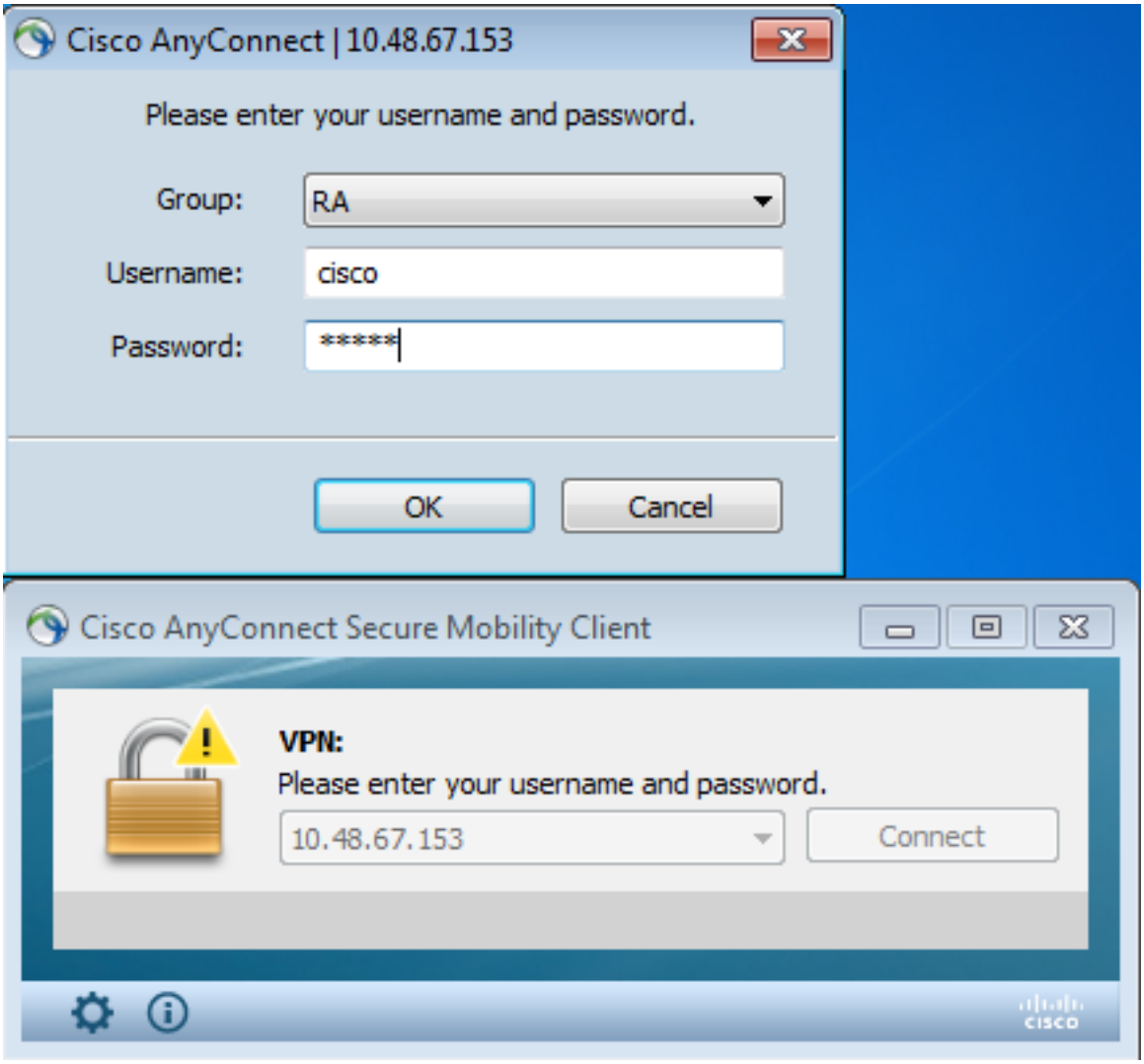
```
ip local pool POOL 10.1.1.10-10.1.1.20
username cisco password cisco

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.01065-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

group-policy Group1 internal
group-policy Group1 attributes
 vpn-tunnel-protocol ssl-client ssl-clientless
 address-pools value POOL

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 authentication-server-group LOCAL
 default-group-policy Group1
 authorization-required
tunnel-group RA webvpn-attributes
 authentication aaa certificate
 group-alias RA enable
```

В дополнение к этой конфигурации возможно выполнить авторизацию Протокола LDAP с именем пользователя от определенного поля сертификата, такого как название сертификата (CN). Дополнительные атрибуты могут тогда быть получены и применены к сеанс VPN. Для получения дополнительной информации об аутентификации и авторизации сертификата, обратитесь к "ASA VPN Anyconnect и Авторизацию OpenLDAP с Пользовательской Схемой и Примером конфигурации Сертификатов".

Тест

Примечание: Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Для тестирования этой конфигурации предоставьте локальные учетные данные (имя пользователя cisco с паролем cisco). Сертификат должен присутствовать:



Введите **подробность покажите vpn-sessiondb anyconnect** команда на ASA:

```
BSNS-ASA5580-40-1(config-tunnel-general)# show vpn-sessiondb detail anyconnect
Session Type: AnyConnect Detailed

Username     : cisco                  Index       : 10
Assigned IP : 10.1.1.10               Public IP   : 10.147.24.60
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing     : none SHA1
Bytes Tx     : 20150                  Bytes Rx    : 25199
Pkts Tx      : 16                     Pkts Rx     : 192
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : Group1                 Tunnel Group : RA
Login Time   : 10:16:35 UTC Sat Apr 13 2013
Duration     : 0h:01m:30s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN        : none

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

AnyConnect-Parent:
 Tunnel ID    : 10.1
 Public IP    : 10.147.24.60
 Encryption   : none                   TCP Src Port : 62531
 TCP Dst Port : 443                    Auth Mode    : Certificate
```

```
and userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 28 Minutes
 Client Type : AnyConnect
 Client Ver  : 3.1.01065
 Bytes Tx    : 10075                 Bytes Rx    : 1696
 Pkts Tx     : 8                     Pkts Rx     : 4
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID   : 10.2
 Assigned IP : 10.1.1.10              Public IP   : 10.147.24.60
 Encryption  : RC4                   Hashing     : SHA1
 Encapsulation: TLSv1.0               TCP Src Port : 62535
 TCP Dst Port : 443                   Auth Mode   : Certificate
and userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 28 Minutes
 Client Type : SSL VPN Client
 Client Ver  : Cisco AnyConnect VPN Agent for Windows 3.1.01065
 Bytes Tx    : 5037                  Bytes Rx    : 2235
 Pkts Tx     : 4                     Pkts Rx     : 11
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

DTLS-Tunnel:
 Tunnel ID   : 10.3
 Assigned IP : 10.1.1.10              Public IP   : 10.147.24.60
 Encryption  : AES128                Hashing     : SHA1
 Encapsulation: DTLSv1.0              UDP Src Port : 52818
 UDP Dst Port : 443                   Auth Mode   : Certificate
and userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client Type : DTLS VPN Client
 Client Ver  : 3.1.01065
 Bytes Tx    : 0                     Bytes Rx    : 21268
 Pkts Tx     : 0                     Pkts Rx     : 177
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

NAC:
 Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
 SQ Int (T)  : 0 Seconds             EoU Age(T)  : 92 Seconds
 Hold Left (T): 0 Seconds             Posture Token:
 Redirect URL :
```

.debug

> **Примечание:** Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

В данном примере сертификат не кэшировался в базе данных, соответствующий CA был найден, корректное Ключевое использование использовалось (ClientAuthentication), и сертификат был проверен успешно:

```
debug aaa authentication
debug aaa authorization
debug webvpn 255
debug webvpn anyconnect 255
debug crypto ca 255
```

Подробные команды отладки, такие как **debug webvpn 255** команд, могут генерировать, многие входят в производственную среду, и разместите нагрузку большая в ASA. Некоторые отладки WebVPN были удалены для ясности:

```
CERT_API: Authenticate session 0x0934d687, non-blocking cb=0x00000000012cfc50
CERT API thread wakes up!
CERT_API: process msg cmd=0, session=0x0934d687
CERT_API: Async locked for session 0x0934d687
CRYPTO_PKI: Checking to see if an identical cert is
 already in the database...
CRYPTO_PKI: looking for cert in handle=0x00007ffd8b80ee90, digest=
ad 3d a2 da 83 19 e0 ee d9 b5 2a 83 5c dd e0 70   | .=........*.\..p
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI: Cert not found in database.
CRYPTO_PKI: Looking for suitable trustpoints...
CRYPTO_PKI: Storage context locked by thread CERT API
CRYPTO_PKI: Found a suitable authenticated trustpoint CA.
CRYPTO_PKI(make trustedCerts list)CRYPTO_PKI:check_key_usage: ExtendedKeyUsage
OID = 1.3.6.1.5.5.7.3.1
CRYPTO_PKI:check_key_usage:Key Usage check OK

CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting to
retrieve revocation status if necessary
CRYPTO_PKI:Certificate validated. serial number: 00FE9C3D61E131CDB1, subject name:
cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL.
CRYPTO_PKI: Storage context released by thread CERT API
CRYPTO_PKI: Certificate validated without revocation check
```

Это - попытка найти соответствующую туннельную группу. Нет никаких определенных правил сопоставления сертификата, и туннельная группа, которую вы предоставляете, используется:

```
CRYPTO_PKI: Attempting to find tunnel group for cert 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.
CRYPTO_PKI: No Tunnel Group Match for peer certificate.
CERT_API: Unable to find tunnel group for cert using rules (SSL)
```

Это отладки сеанса SSL и генеральной сессии:

```
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client
outside:10.147.24.60/64435
%ASA-7-717025: Validating certificate chain containing 1 certificate(s).
%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.
%ASA-7-717030: Found a suitable trustpoint CA to validate certificate.
%ASA-6-717022: Certificate was successfully validated. serial number:
00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,
c=PL.
%ASA-6-717028: Certificate chain was successfully validated with warning,
revocation status was not checked.
%ASA-6-725002: Device completed SSL handshake with client outside:
10.147.24.60/64435
%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.
%ASA-4-717037: Tunnel group search using certificate maps failed for 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.
%ASA-6-113012: AAA user authentication Successful : local database : user = cisco
%ASA-6-113009: AAA retrieved default group policy (Group1) for user = cisco
%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.grouppolicy = Group1
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
```

```
Session Attribute aaa.cisco.username = cisco
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.username1 = cisco
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.username2 =
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.tunnelgroup = RA
%ASA-6-734001: DAP: User cisco, Addr 10.147.24.60, Connection AnyConnect: The
following DAP records were selected for this connection: DfltAccessPolicy
 %ASA-6-113039: Group <Group1> User <cisco> IP <10.147.24.60> AnyConnect parent
session started.
```

Конфигурация ASA для двойной аутентификации и проверки достоверности сертификата

Это - пример двойной аутентификации, где первичный сервер аутентификации ЛОКАЛЕН, и сервер вспомогательной проверки подлинности является LDAP. Проверка достоверности сертификата все еще включена.

Данный пример показывает Конфигурацию LDAP:

```
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client
outside:10.147.24.60/64435
%ASA-7-717025: Validating certificate chain containing 1 certificate(s).
%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.
%ASA-7-717030: Found a suitable trustpoint CA to validate certificate.
%ASA-6-717022: Certificate was successfully validated. serial number:
00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,
c=PL.
%ASA-6-717028: Certificate chain was successfully validated with warning,
revocation status was not checked.
%ASA-6-725002: Device completed SSL handshake with client outside:
10.147.24.60/64435
%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.
%ASA-4-717037: Tunnel group search using certificate maps failed for 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.
%ASA-6-113012: AAA user authentication Successful : local database : user = cisco
%ASA-6-113009: AAA retrieved default group policy (Group1) for user = cisco
%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.grouppolicy = Group1
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.username = cisco
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.username1 = cisco
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.username2 =
%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:
Session Attribute aaa.cisco.tunnelgroup = RA
%ASA-6-734001: DAP: User cisco, Addr 10.147.24.60, Connection AnyConnect: The
following DAP records were selected for this connection: DfltAccessPolicy
 %ASA-6-113039: Group <Group1> User <cisco> IP <10.147.24.60> AnyConnect parent
session started.
```

Вот добавление сервера вспомогательной проверки подлинности:

```
tunnel-group RA general-attributes
 authentication-server-group LOCAL
secondary-authentication-server-group LDAP
 default-group-policy Group1
 authorization-required
tunnel-group RA webvpn-attributes
 authentication aaa certificate
```

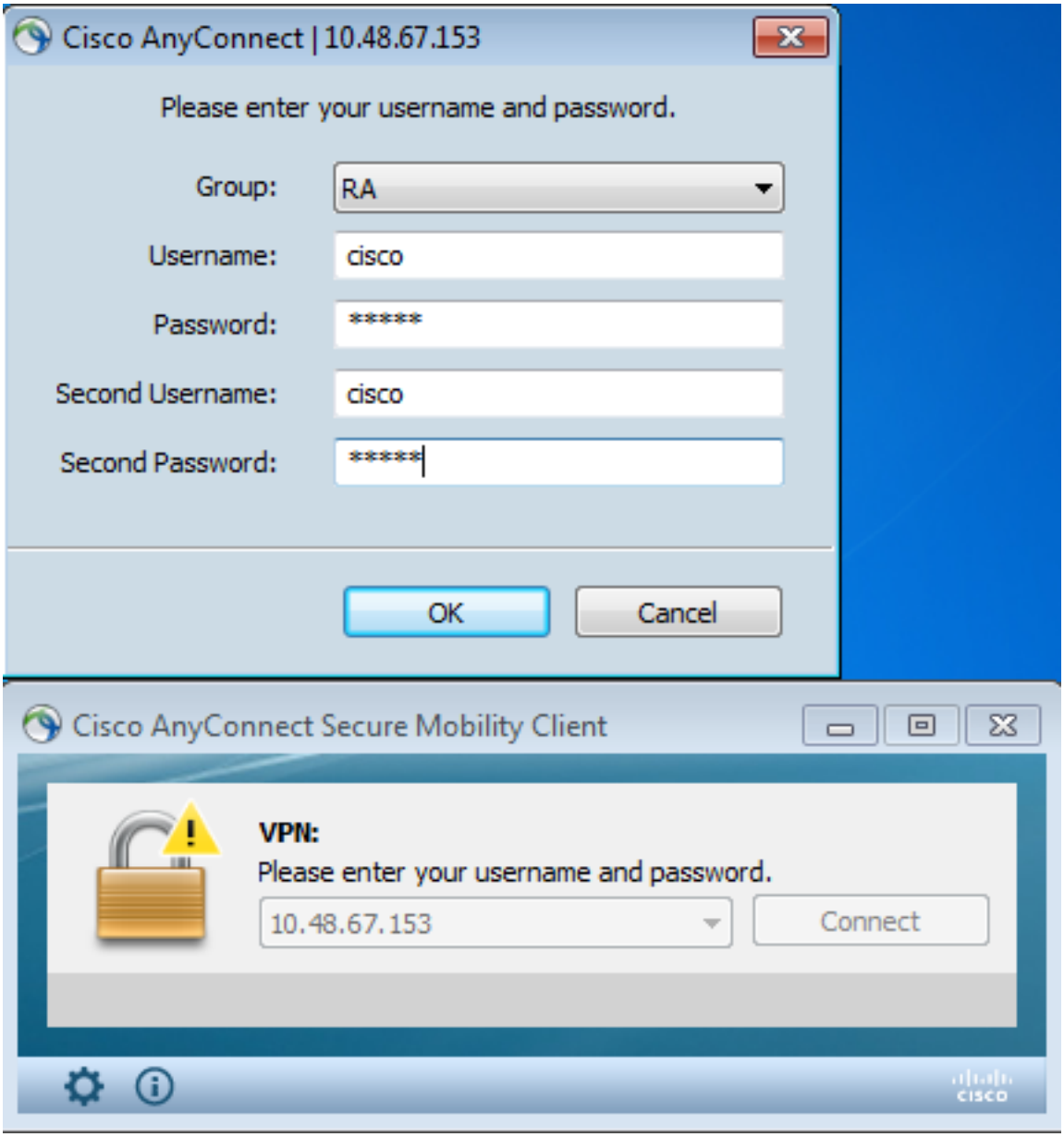
Вы не видите 'группу сервера аутентификации, ЛОКАЛЬНУЮ' в конфигурации, потому что это - настройка по умолчанию.

Любой другой AAA-сервер может использоваться для 'группы сервера аутентификации'. Для 'secondary-authentication-server-group' возможно использовать все AAA-серверы за исключением сервера Security Dynamics International (SDI); в этом случае SDI мог все еще быть первичным сервером аутентификации.

Тест

> **Примечание:** Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

Для тестирования этой конфигурации предоставьте локальные учетные данные (имя пользователя cisco с паролем cisco) и учетные данные LDAP (имя пользователя cisco с паролем от LDAP). Сертификат должен присутствовать:



Введите **подробность покажите vpn-sessiondb anyconnect** команда на ASA.

Результаты подобны тем для одиночной аутентификации. См. "Конфигурацию ASA для Одиночной Аутентификации и Проверки достоверности сертификата, Теста".

.debug

Отладки для сеанса WebVPN и аутентификации подобны. См. "Конфигурацию ASA для Одиночной Аутентификации и Проверки достоверности сертификата, Отладки". Один дополнительный процесс проверки подлинности появляется:

```
%ASA-6-113012: AAA user authentication Successful : local database : user = cisco
%ASA-6-302013: Built outbound TCP connection 1936 for outside:10.147.24.60/389
(10.147.24.60/389) to identity:10.48.67.153/54437 (10.48.67.153/54437)
%ASA-6-113004: AAA user authentication Successful : server = 10.147.24.60 :
user = cisco
%ASA-6-113009: AAA retrieved default group policy (Group1) for user = cisco
%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
```

Отладки для LDAP показывают подробные данные, которые могли бы меняться в зависимости от Конфигурации LDAP:

```
%ASA-6-113012: AAA user authentication Successful : local database : user = cisco
%ASA-6-302013: Built outbound TCP connection 1936 for outside:10.147.24.60/389
(10.147.24.60/389) to identity:10.48.67.153/54437 (10.48.67.153/54437)
%ASA-6-113004: AAA user authentication Successful : server = 10.147.24.60 :
user = cisco
%ASA-6-113009: AAA retrieved default group policy (Group1) for user = cisco
%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
```

Конфигурация ASA для двойной аутентификации и предварительной заливки

Возможно сопоставить определенные поля сертификата с именем пользователя, которое используется для основного и вспомогательной проверки подлинности:

```
username test1 password cisco
tunnel-group RA general-attributes
 authentication-server-group LOCAL
 secondary-authentication-server-group LDAP
 default-group-policy Group1
 authorization-required
 username-from-certificate CN
 secondary-username-from-certificate OU
tunnel-group RA webvpn-attributes
 authentication aaa certificate
 pre-fill-username ssl-client
 secondary-pre-fill-username ssl-client
 group-alias RA enable
```

В данном примере клиент использует сертификат: **cn=test1**, **ou=Security**, o=Cisco, l=Krakow, st=PL, c=PL.

Для основной аутентификации имя пользователя взято от CN, который является, почему был создан локальный пользователь 'test1'.

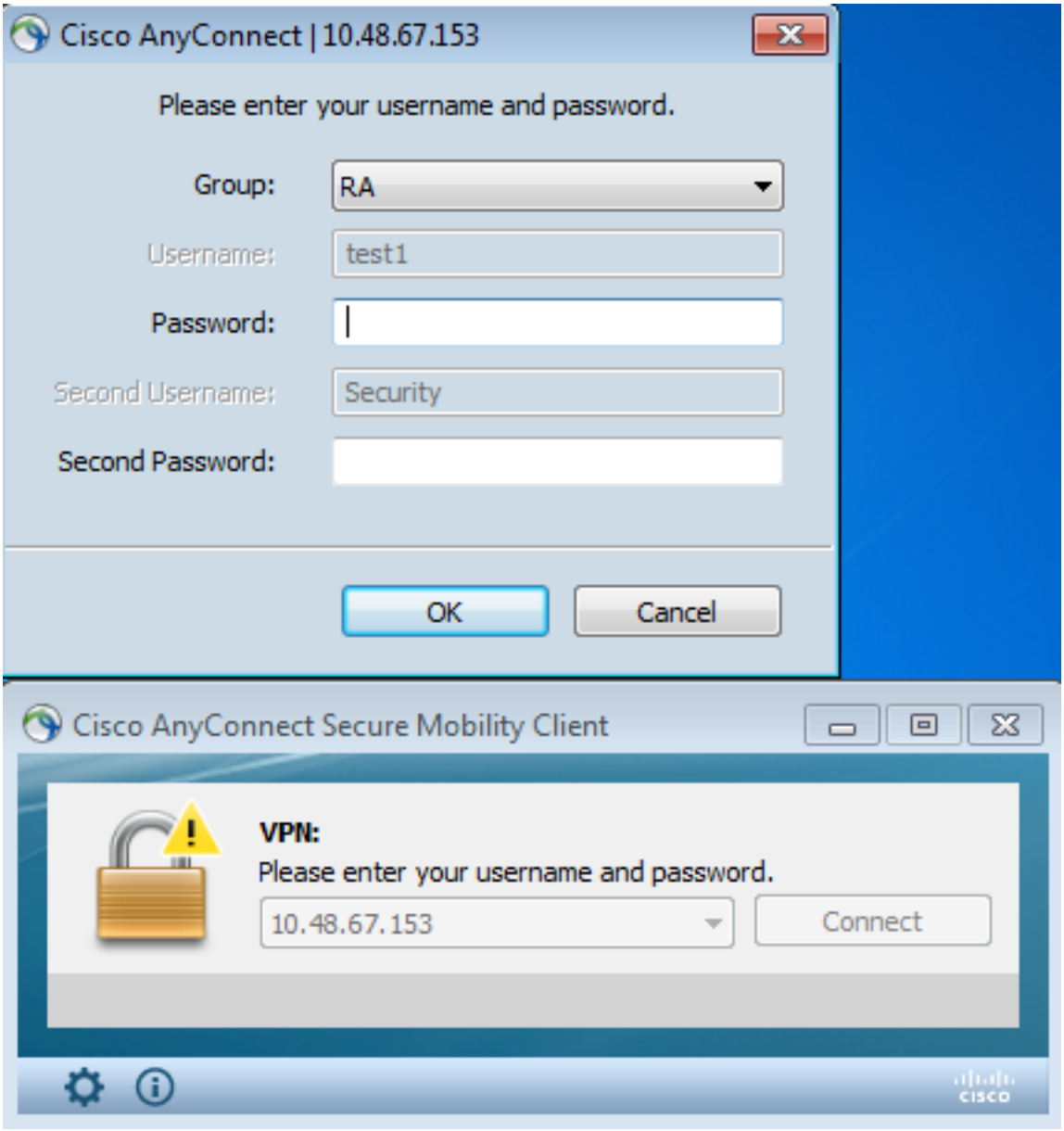
Для вспомогательной проверки подлинности имя пользователя взято от подразделения (OU, который является, почему пользователь 'Безопасность' был создан на Сервере LDAP.

Также возможно вынудить AnyConnect использовать команды перед заливкой, чтобы предварительно заполнить основное и вторичное имя пользователя.

В сценарии реальных условий первичный сервер аутентификации является обычно AD или Сервером LDAP, в то время как сервер вспомогательной проверки подлинности является Rivest, Shamir и Adelman (RSA) сервер, который использует пароли токена. В этом сценарии пользователь должен предоставить учетные данные AD/LDAP (который пользователь знает), пароль токена RSA (который пользователь имеет), и сертификат (на машине, которая используется).

Тест

Заметьте, что вы не можете изменить основное или вторичное имя пользователя, потому что оно предварительно заполнено от полей CN и OU сертификата:



.debug

Данный пример показывает запрос перед заливкой, отправленный AnyConnect:

```
username test1 password cisco
tunnel-group RA general-attributes
 authentication-server-group LOCAL
 secondary-authentication-server-group LDAP
 default-group-policy Group1
 authorization-required
 username-from-certificate CN
 secondary-username-from-certificate OU
tunnel-group RA webvpn-attributes
 authentication aaa certificate
 pre-fill-username ssl-client
 secondary-pre-fill-username ssl-client
 group-alias RA enable
```

Здесь вы видите, что аутентификация использует корректные имена пользователей:

```
%ASA-6-113012: AAA user authentication Successful : local database : user = test1
%ASA-6-302013: Built outbound TCP connection 2137 for outside:10.147.24.60/389
(10.147.24.60/389) to identity:10.48.67.153/46606 (10.48.67.153/46606)
```

```
%ASA-6-113004: AAA user authentication Successful : server = 10.147.24.60 :
user = Security
```

Конфигурация ASA для сопоставления двойной аутентификации и сертификата

Также возможно сопоставить определенные сертификаты клиента с определенными туннельными группами, как показано в данном примере:

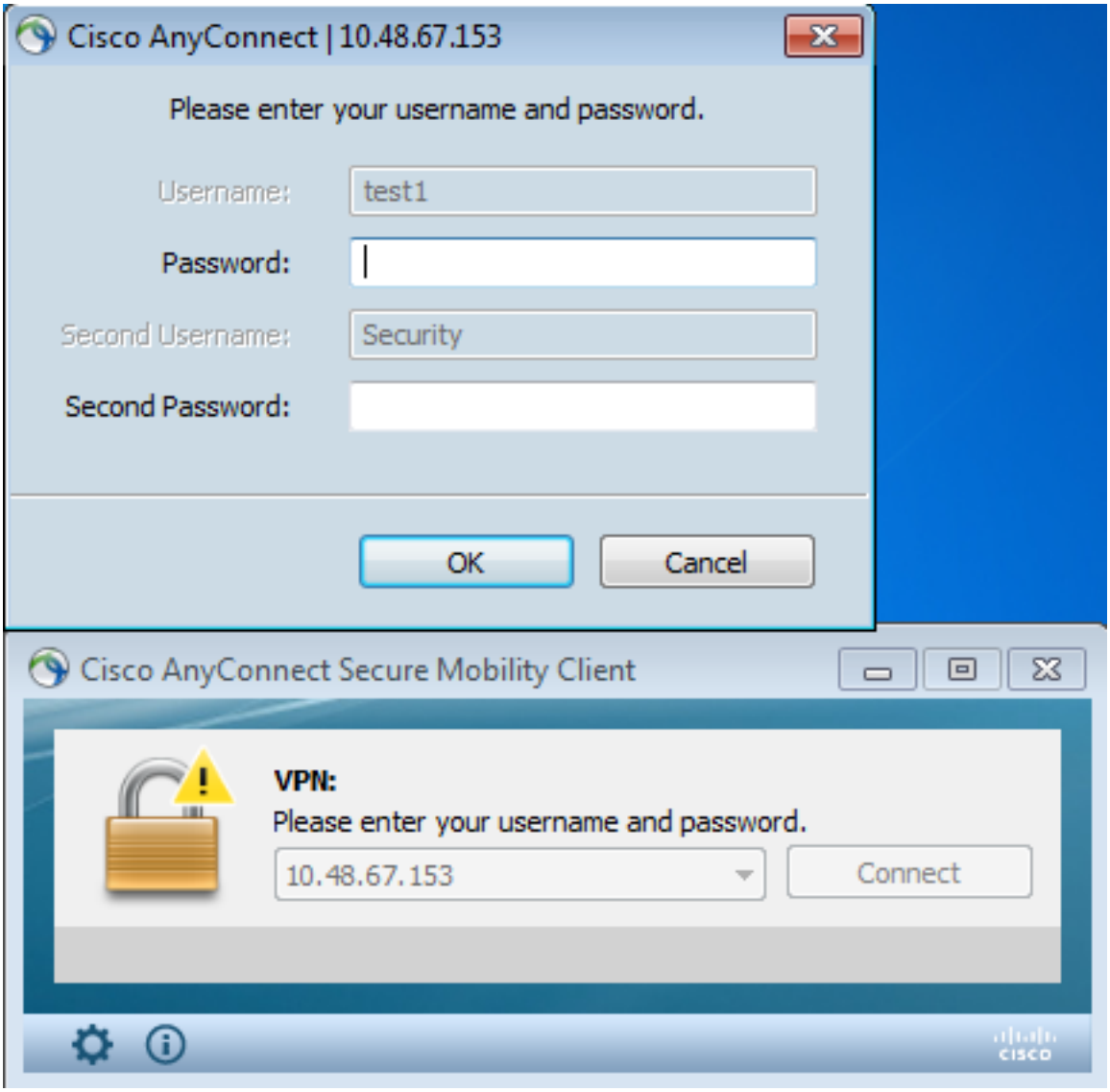
```
%ASA-6-113012: AAA user authentication Successful : local database : user = test1
%ASA-6-302013: Built outbound TCP connection 2137 for outside:10.147.24.60/389
(10.147.24.60/389) to identity:10.48.67.153/46606 (10.48.67.153/46606)
%ASA-6-113004: AAA user authentication Successful : server = 10.147.24.60 :
user = Security
```

Таким образом, все сертификаты пользователя, подписанные Центром технической поддержки Cisco (TAC) CA, сопоставлены с туннельной группой под названием 'RA'.

> **Примечание:** Сопоставление сертификата для SSL настроено по-другому, чем сопоставление сертификата для IPsec. Для IPsec это настроено с помощью правил 'карты туннельной группы' в режиме глобальной конфигурации. Для SSL это настроено с помощью 'карты группы сертификата' под режимом конфигурации webvpn.

Тест

Заметьте, что, как только сопоставление сертификата включено, вы не должны больше выбирать туннельную группу:



.debug

В данном примере правило сопоставления сертификата позволяет туннельной группе быть найденной:

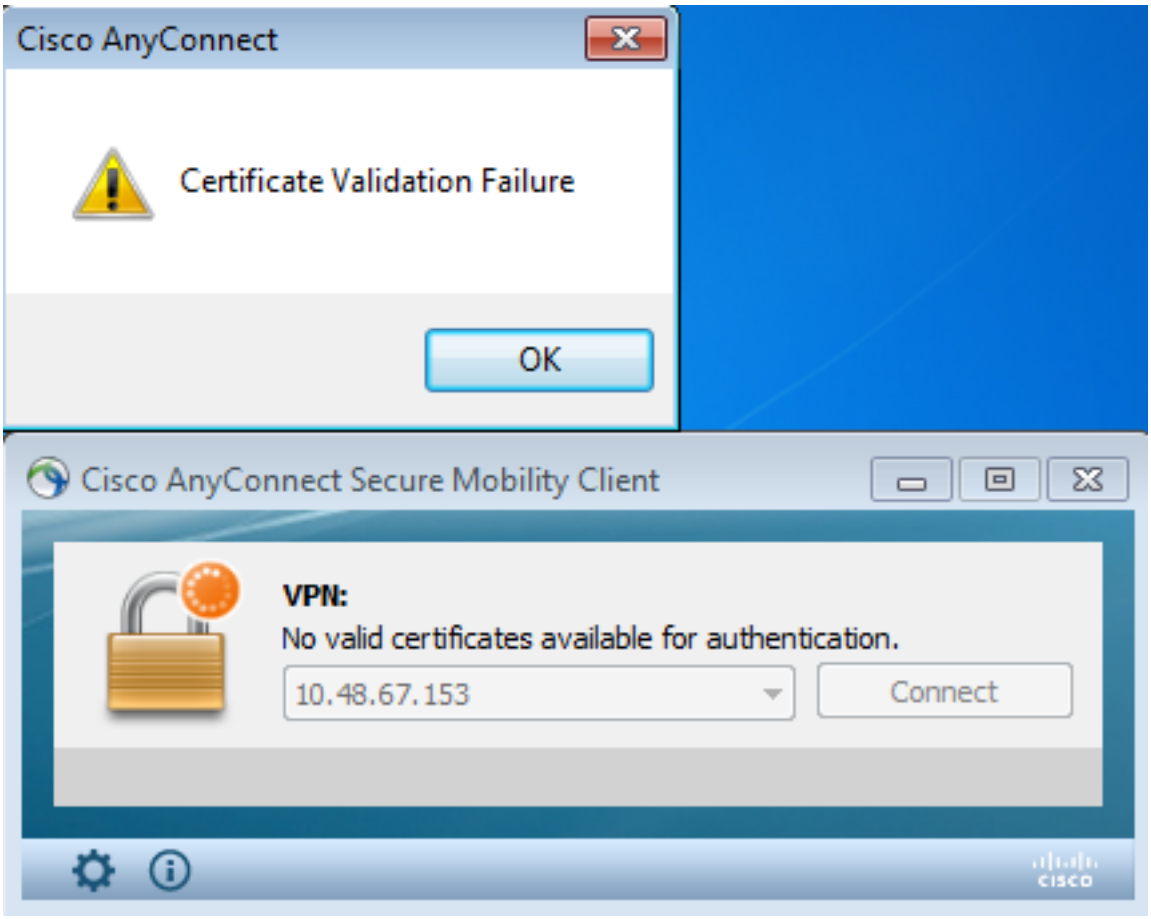
```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps for
peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,
l=Warsaw,st=Maz,c=PL.
%ASA-7-717038: Tunnel group match found. 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.
```

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Подтвержденный сертификат, не существующий

После удаления подтвержденного сертификата из Windows7 AnyConnect не может найти подтвержденные сертификаты:



На ASA похоже, что сеанс завершен клиентом (Сброс-I):

```
%ASA-6-302013: Built inbound TCP connection 2489 for outside:10.147.24.60/52838
(10.147.24.60/52838) to identity:10.48.67.153/443 (10.48.67.153/443)
%ASA-6-725001: Starting SSL handshake with client outside:10.147.24.60/52838 for
TLSv1 session.
%ASA-7-725010: Device supports the following 4 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725011: Cipher[3] : AES256-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725008: SSL client outside:10.147.24.60/52838 proposes the following 8
cipher(s).
%ASA-7-725011: Cipher[1] : AES128-SHA
%ASA-7-725011: Cipher[2] : AES256-SHA
%ASA-7-725011: Cipher[3] : RC4-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725011: Cipher[5] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[6] : DHE-DSS-AES256-SHA
%ASA-7-725011: Cipher[7] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[8] : RC4-MD5
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client
outside:10.147.24.60/52838
%ASA-6-302014: Teardown TCP connection 2489 for outside:10.147.24.60/52838 to
identity:10.48.67.153/443 duration 0:00:00 bytes 1448 TCP Reset-I
```

Дополнительные сведения

- Туннель Настройки Grouips, групповые политики и пользователи: двойная аутентификация Настройки
- Настройка внешний сервер для авторизации пользователя на устройстве безопасности
- Cisco Systems – техническая поддержка и документация