تكوين مصادقة ASA AnyConnect Secure Mobility Client

المحتويات

المقدمة

يصف هذا المستند تكوين الوصول ASA AnyConnect Secure Mobility Client يستخدم مصادقة مزدوجة مع التحقق من صحة الشهادة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بتكوين واجهة سطر أوامر ASA (CLI) وتكوين طبقة مأخذ التوصيل الآمنة (SSL) VPN
- معرفة أساسية بشهادات X509

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج التالية:

- برنامج أجهزة الأمان المعدلة Cisco Adaptive Security Appliance (ASA)، الإصدار 8.4 والإصدارات الأحدث
- Windows 7 مع Cisco AnyConnect Secure Mobility Client، الإصدار 3.1

من المفترض أنك أستخدمت مرجع شهادات خارجي (CA) لإنشاء:

- تشفير قياسي بمفتاح عام رقم 12 (PKCS #12) شهادة مرمز بالأساس 64 ل ASA (AnyConnect.pfx)
- شهادة PKCS #12 ل AnyConnect

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يصف هذا المستند مثال لتكوين جهاز الأمان القابل للتكيف (ASA) Cisco AnyConnect Secure Mobility Client access الذي يستخدم المصادقة المزدوجة مع التحقق من صحة الشهادة. بصفتك مستخدم AnyConnect، يجب عليك توفير الشهادة وبيانات الاعتماد الصحيحة للمصادقة الأساسية والثانوية للحصول على وصول VPN. كما يقدم هذا المستند مثال لتعيين الشهادة باستخدام ميزة التعبئة المسبقة.

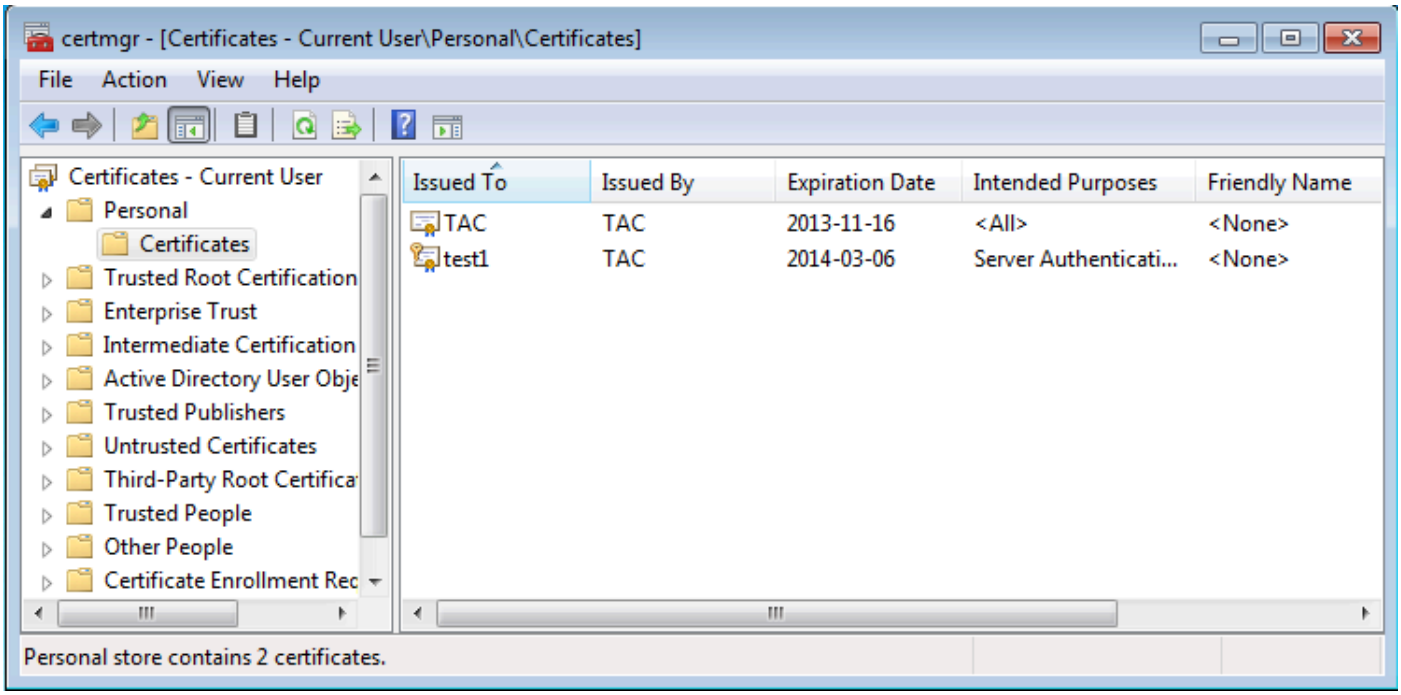
التكوين

ملاحظة: استعملت [أداة lookup الأمر](#) in order to نلت كثير معلومة على الأمر يستعمل في هذا قسم. يمكن فقط لمستخدمي Cisco المسجلين الوصول إلى أدوات Cisco ومعلومات داخلية.

شهادة AnyConnect

لتثبيت شهادة مثال، انقر نقرا مزدوجا على ملف AnyConnect.pfx، وقم بتثبيت الشهادة كشهادة شخصية.

أستخدم مدير الشهادات (certmgr.msc) للتحقق من التثبيت:



بشكل افتراضي، يحاول AnyConnect العثور على شهادة في مخزن مستخدمي Microsoft. لا حاجة إلى إجراء أي تغييرات في ملف تعريف AnyConnect.

تثبيت الشهادة على ASA

يوضح هذا المثال كيف يمكن لـ ASA إستيراد شهادة PKCS #12 base64:

<#root>

```
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/WBSkrOIeT1HARHbLF1FFQvSvBAhuOj9bTtZo
3AICCAA=
quit


INFO: Import PKCS12 operation completed successfully
```

أستخدم الأمر show crypto ca certificates للتحقق من الاستيراد:

```
BSNS-ASA5580-40-1(config)# show crypto ca certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 00cf946de20d0ce6d9
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
```

```
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=TAC
    ou=RAC
    o=TAC
    l=Warsaw
    st=Maz
    c=PL
  Subject Name:
    cn=TAC
    ou=RAC
    o=TAC
    l=Warsaw
    st=Maz
    c=PL
  Validity Date:
    start date: 08:11:26 UTC Nov 16 2012
    end   date: 08:11:26 UTC Nov 16 2013
  Associated Trustpoints: CA

Certificate
  Status: Available
  Certificate Serial Number: 00fe9c3d61e131cda9
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=TAC
    ou=RAC
    o=TAC
    l=Warsaw
    st=Maz
    c=PL
  Subject Name:
    cn=IOS
    ou=UNIT
    o=TAC
    l=Wa
    st=Maz
    c=PL
  Validity Date:
    start date: 12:48:31 UTC Nov 29 2012
    end   date: 12:48:31 UTC Nov 29 2013
  Associated Trustpoints: CA
```

ملاحظة: تدعم أداة مترجم الإخراج بعض أوامر show. أستخدم "أداة مترجم الإخراج" لعرض تحليل مخرج الأمر show. يمكن فقط لمستخدمي Cisco المسجلين الوصول إلى أدوات Cisco ومعلومات داخلية.

تكوين ASA للمصادقة الأحادية والتحقق من الشهادة

يستخدم ASA المصادقة والتفويض والمحاسبة (AAA) ومصادقة الشهادة. التحقق من صحة الشهادة إلزامي. تستخدم مصادقة AAA قاعدة بيانات محلية.

يوضح هذا المثال مصادقة واحدة مع التحقق من صحة الشهادة.

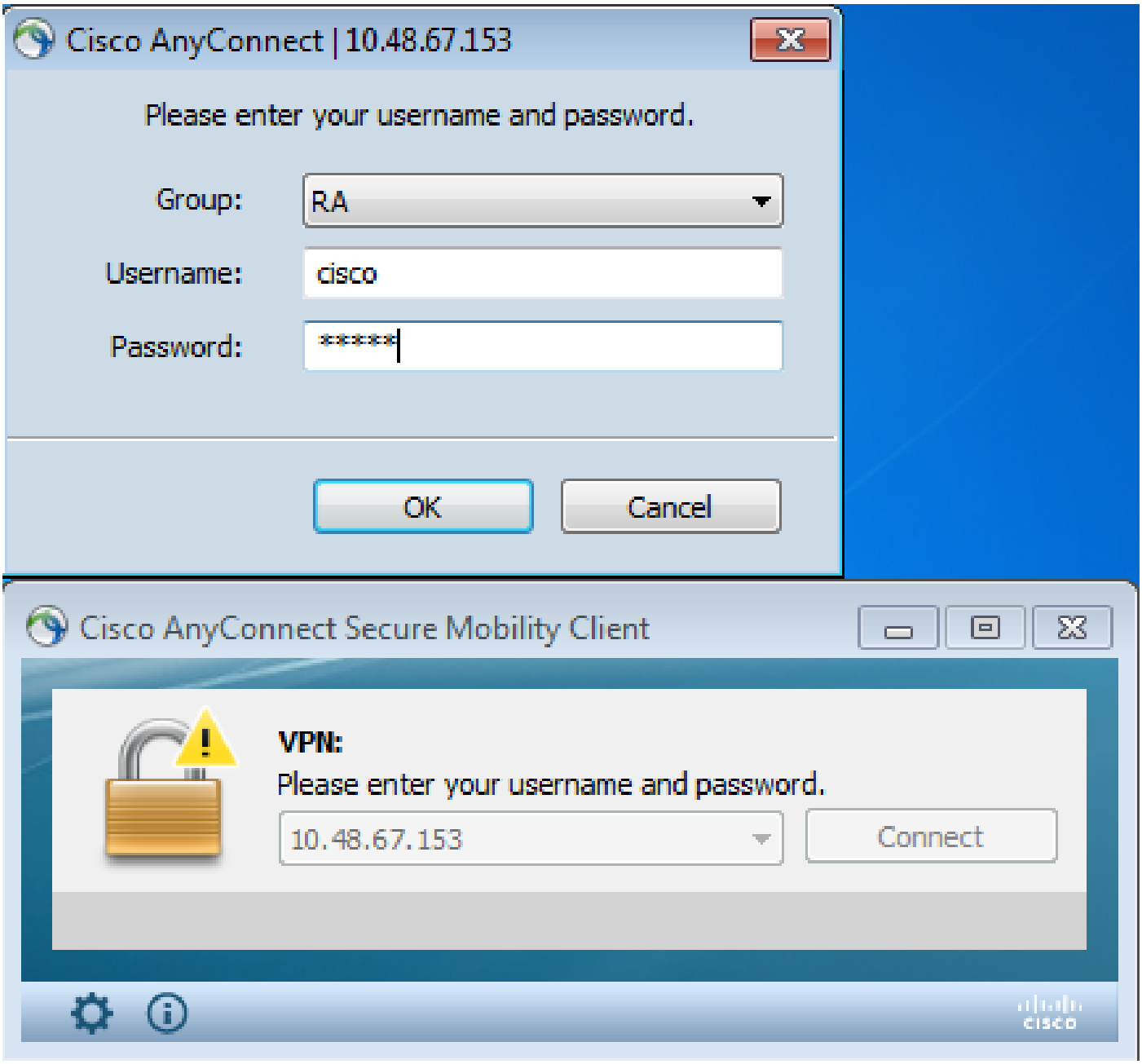
```
<#root>

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
```

بالإضافة إلى هذا التكوين، من الممكن تنفيذ تفويض بروتوكول الوصول إلى الدليل الخفيف (LDAP) باستخدام اسم المستخدم من حقل شهادة محدد، مثل اسم الشهادة (CN). بعد ذلك يمكن إستردادسمات إضافية وتطبيقها على جلسة عمل الشبكة الخاصة الظاهرية (VPN). لمزيد من المعلومات حول المصادقة وتفويض الشهادة، ارجع إلى ASA AnyConnect VPN وتخويل OpenLDAP مع مخطط مخصص ومثال تكوين الشهادات.

إختبار

ملاحظة: تدعم أداة مترجم الإخراج بعض أوامر show. أستخدم "أداة مترجم الإخراج" لعرض تحليل مخرج الأمر show. يمكن فقط للمستخدمي Cisco المسجلين الوصول إلى أدوات Cisco ومعلومات داخلية.

تأكد in order to اختبرت هذا تشكيل، ال مسوغات محلي (username cisco مع كلمة cisco). يجب أن تكون الشهادة موجودة:



دخلت العرض vpn-sessionDB تفصيل AnyConnect أمر على ال ASA:

<#root>

```
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 :
```

تصحيح الأخطاء

ملاحظة: ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر debug.

في هذا المثال، لم يتم تخزين الشهادة مؤقتا في قاعدة البيانات. تم العثور على مرجع مصدق مطابق، تم إستخدام إستخدام المفتاح الصحيح (ClientAuthentication)، وتم التحقق من صحة الشهادة بنجاح:

<#root>

```
debug aaa authentication
debug aaa authorization
debug webvpn  255
```

debug webvpn AnyConnect 255

```
debug crypto ca 255
```

يمكن أن تقوم أوامر تصحيح الأخطاء التفصيلية، مثل الأمر debug webVPN 255، بإنشاء العديد من السجلات في بيئة إنتاج ووضع حمل كبير على ASA. تمت إزالة بعض تصحيح أخطاء WebVPN للوضوح:

<#root>

```
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

هذه هي محاولة العثور على مجموعة نفق مطابقة. لا توجد قواعد تعيين شهادات محددة، ويتم إستخدام مجموعة النفق التي توفرها:

<#root>

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)

هذه هي SSL وتصحيح أخطاء الجلسة العامة:

<#root>

%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.
```

تكوين ASA لمصادقة مزدوجة والتحقق من الشهادة

هذا مثال على المصادقة المزدوجة، حيث يكون خادم المصادقة الأساسي محليا، وخادم المصادقة الثانوي هو LDAP. الغاز التحقق من صحة الشهادة ممكنا.

يوضح هذا المثال تكوين LDAP:

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host 10.147.24.60
 ldap-base-dn DC=test-cisco,DC=com
 ldap-scope subtree
 ldap-naming-attribute uid
 ldap-login-password *****
 ldap-login-dn CN=Manager,DC=test-cisco,DC=com
 server-type openldap
```

فيما يلي إضافة خادم مصادقة ثانوي:

```
<#root>

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
```

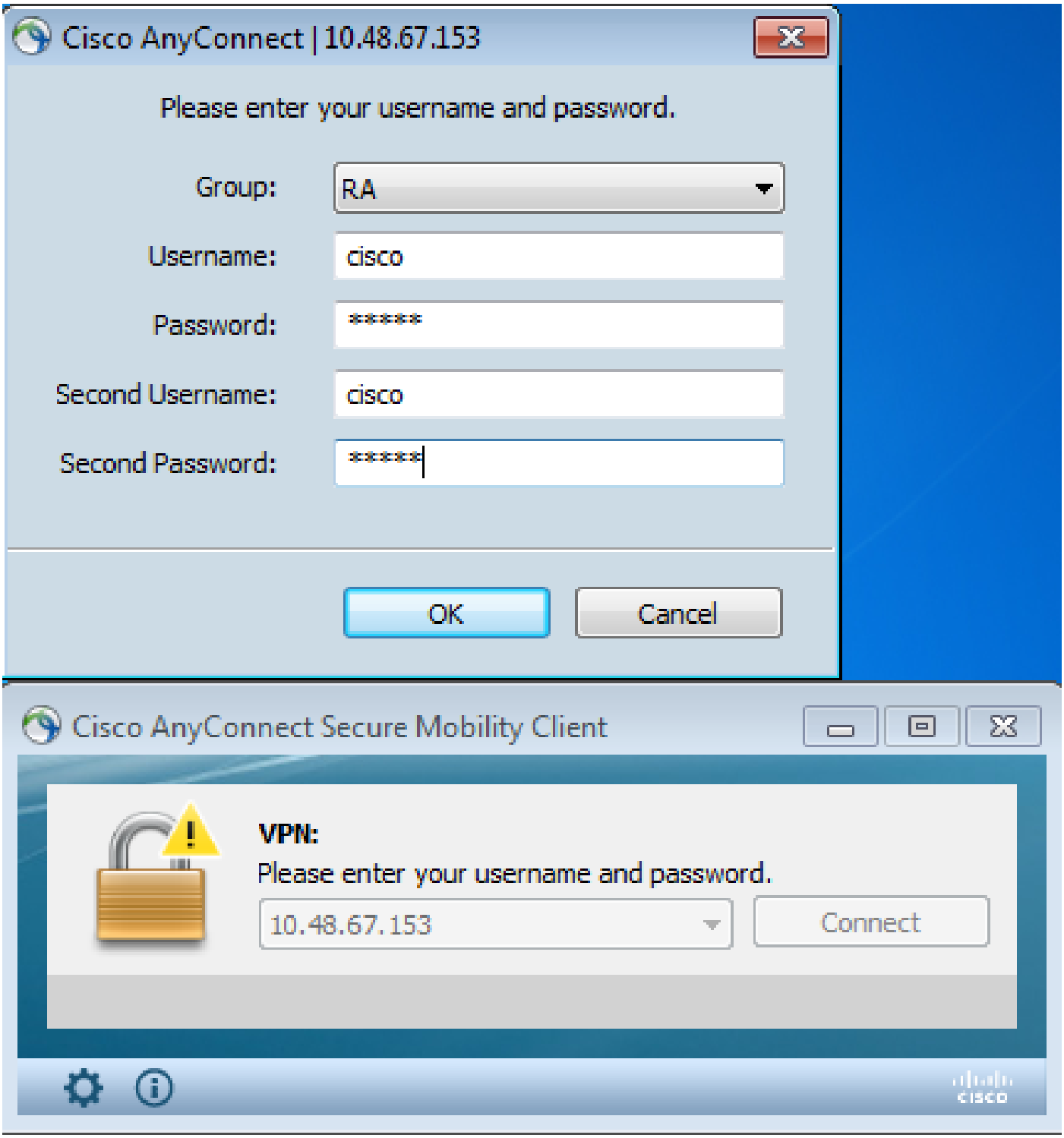
ترى AUTHENTICATION-server-group LOCAL في التكوين لأنه إعداد افتراضي.

يمكن إستخدام أي خادم AAA آخر لمصادقة server-group. بالنسبة لمجموعة خوادم المصادقة الثانوية، من الممكن إستخدام جميع خوادم AAA باستثناء خادم Security Dynamics International (SDI). في هذه الحالة، يمكن أن يظل SDI هو خادم المصادقة الرئيسي.

إختبار

ملاحظة: تدعم أداة مترجم الإخراج بعض أوامر show. أستخدم "أداة مترجم الإخراج" لعرض تحليل مخرج الأمر show. يمكن فقط لمستخدمي Cisco المسجلين الوصول إلى أدوات Cisco ومعلومات داخلية.

أصدرت in order to اختبرت هذا تشكيل، ال محلي وقرة اعتماد (username cisco مع كلمة cisco) و LDAP وقرة اعتماد (username cisco مع كلمة من LDAP). يجب أن تكون الشهادة موجودة:



دخلت العرض vpn-sessionDB تفصيل AnyConnect أمر على ال ASA.

النتائج مماثلة لتلك الخاصة بالمصادقة الأحادية. ارجع إلى تكوين ASA للمصادقة

الأحادية والتحقق من الشهادة والاختبار .

تصحيح الأخطاء

تتماثل عمليات تصحيح الأخطاء لجلسة WebVPN والمصادقة. ارجع إلى تكوين ASA للمصادقة الأحادية والتحقق من الشهادة وتصحيح الأخطاء. تظهر عملية مصادقة إضافية واحدة:

```
<#root>

%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
```

يبدي تصحيح أخطاء LDAP تفاصيل يمكن أن تختلف مع تكوين LDAP:

```
[34] Session Start
[34] New request Session, context 0x00007ffd8d7dd828, reqType = Authentication
[34] Fiber started
[34] Creating LDAP context with uri=ldap://10.147.24.60:389
[34] Connect to LDAP server: ldap://10.147.24.60:389, status = Successful
[34] supportedLDAPVersion: value = 3
[34] Binding as Manager
[34] Performing Simple authentication for Manager to 10.147.24.60
[34] LDAP Search:
        Base DN = [DC=test-cisco,DC=com]
        Filter  = [uid=cisco]
        Scope   = [SUBTREE]
[34] User DN = [uid=cisco,ou=People,dc=test-cisco,dc=com]
[34] Server type for 10.147.24.60 unknown - no password policy
[34] Binding as cisco
[34] Performing Simple authentication for cisco to 10.147.24.60
[34] Processing LDAP response for user cisco
[34] Authentication successful for cisco to 10.147.24.60
[34] Retrieved User Attributes:
[34]    cn: value = John Smith
[34]    givenName: value = John
[34]    sn: value = cisco
[34]    uid: value = cisco
[34]    uidNumber: value = 10000
[34]    gidNumber: value = 10000
[34]    homeDirectory: value = /home/cisco
[34]    mail: value = name@dev.local
```

```
[34]    objectClass: value = top
[34]    objectClass: value = posixAccount
[34]    objectClass: value = shadowAccount
[34]    objectClass: value = inetOrgPerson
[34]    objectClass: value = organizationalPerson
[34]    objectClass: value = person
[34]    objectClass: value = CiscoPerson
[34]    loginShell: value = /bin/bash
[34]    userPassword: value = {SSHA}pndf5sfjscTPuyrhL+/QUqhK+i1UCUTy
[34] Fiber exit Tx=315 bytes Rx=911 bytes, status=1
[34] Session End
```

تكوين ASA لمصادقة مزدوجة وتعبئة مسبقة

من الممكن تعيين حقول شهادة معينة لاسم المستخدم المستخدم المستخدم للمصادقة الأساسية والثانوية:

```
<#root>

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
```

في هذا المثال، يستخدم العميل الشهادة: cn=test1، ou=security، o=cisco، l=krakow، st=pl، c=pl.

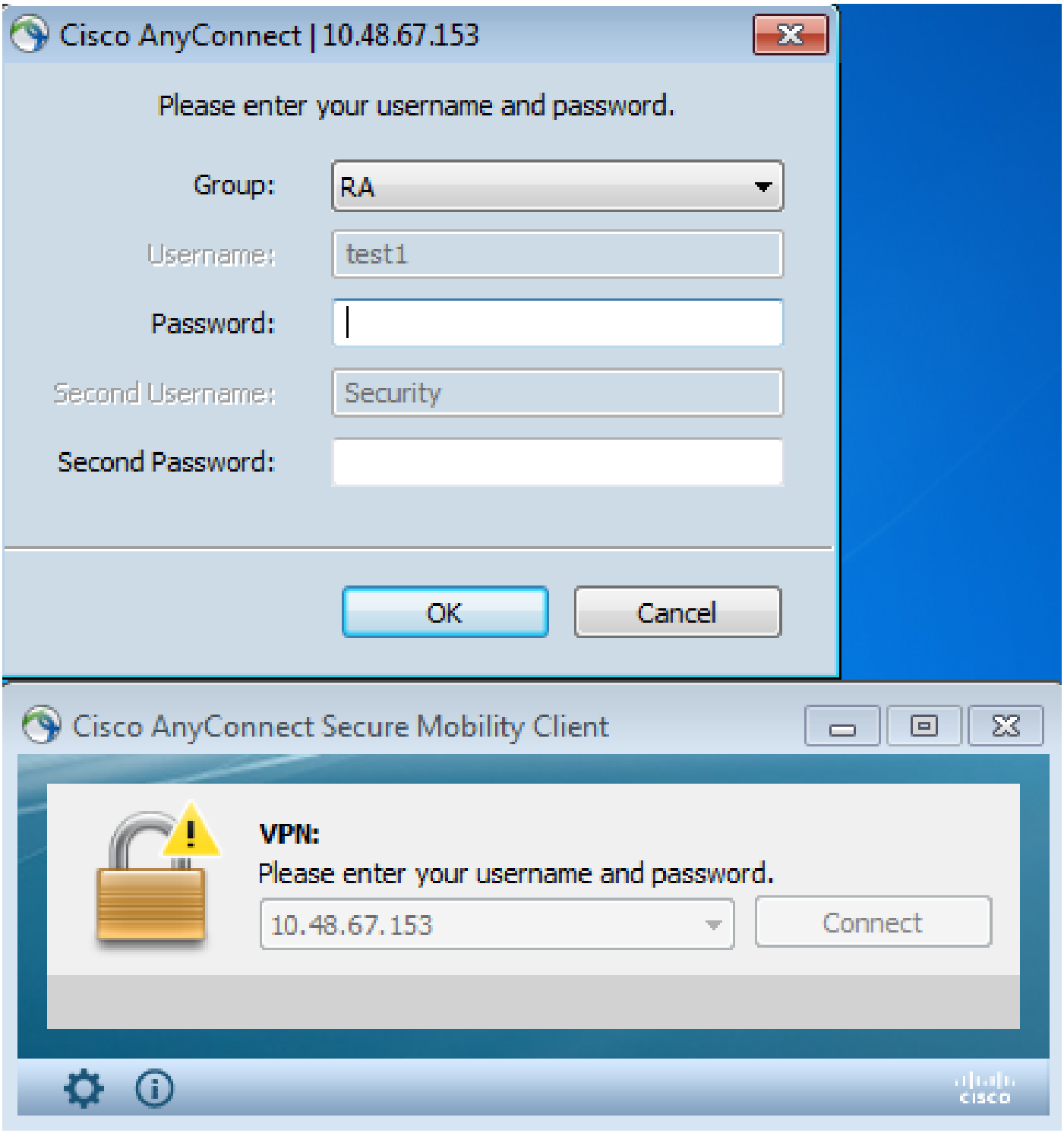
بالنسبة للمصادقة الأساسية، يتم أخذ اسم المستخدم من CN، ولهذا السبب تم إنشاء إختبار المستخدم المحلي 1.

بالنسبة للمصادقة الثانوية، يتم أخذ اسم المستخدم من الوحدة التنظيمية (OU، ولهذا السبب تم إنشاء أمان المستخدم على خادم LDAP.

من الممكن أيضا فرض إستخدام أسماء مستخدم مختلفة للمصادقة الأساسية والثانوية على AnyConnect مع التعبئة المسبقة لاسم المستخدم الأساسي والثانوي مسبقا. في سيناريو العالم الحقيقي، عادة ما يكون خادم المصادقة الأساسي خادم AD أو LDAP، بينما يكون خادم المصادقة الثانوي خادم Rivest و Shamir و Adadman (RSA) الذي يستخدم رموز الرمز المميز. في هذا السيناريو، يجب على المستخدم توفير بيانات اعتماد AD/LDAP (التي يعلمها المستخدم) ورمز مميز RSA (الذي يمتلكه المستخدم) وشهادة (على الجهاز الذي يتم إستخدامه).

إختبار

لاحظ أنه لا يمكنك تغيير اسم المستخدم الأساسي أو الثانوي لأنه معبأ مسبقا من حقلي CN و OU للشهادة:



تصحيح الأخطاء

يوضح هذا المثال طلب التعبئة المسبقة الذي تم إرساله إلى AnyConnect:

```
%ASA-7-113028: Extraction of username from VPN client certificate has been
requested.  [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has started.
[Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has finished
successfully.  [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has completed.
```

```
[Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has been
requested.  [Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has started.
[Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has finished
successfully.  [Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has completed.
[Request 6]
```

هنا ترى أن المصادقة تستخدم أسماء المستخدمين الصحيحة:

```
<#root>

%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
```

تكوين ASA لمصادقة مزدوجة وتخطيط شهادات

من الممكن أيضا تعيين شهادات عميل محددة إلى مجموعات أنفاق معينة، كما هو موضح في هذا المثال:

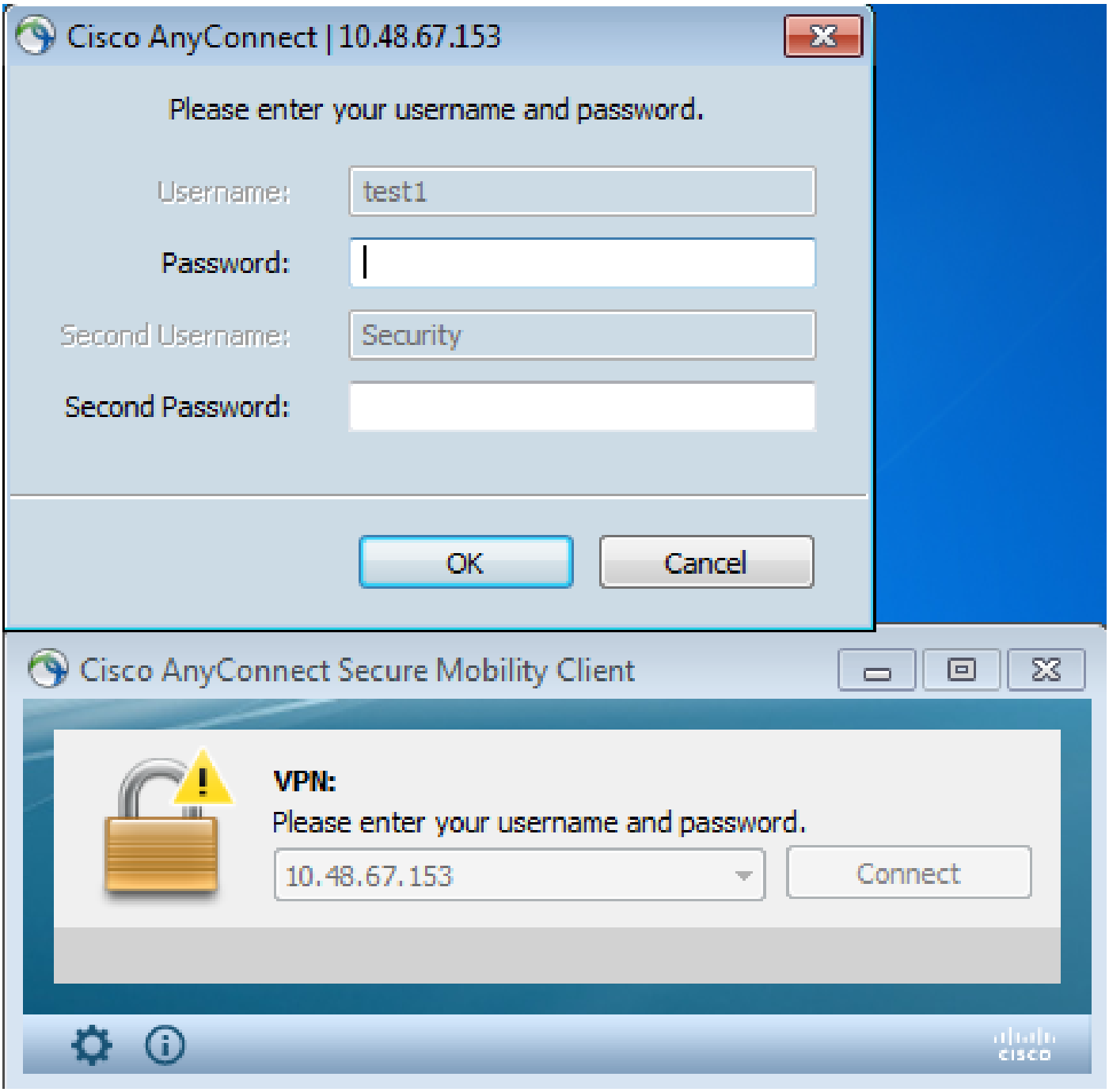
```
crypto ca certificate map CERT-MAP 10
 issuer-name co tac

webvpn
 certificate-group-map CERT-MAP 10 RA
```

بهذه الطريقة، يتم تعيين جميع شهادات المستخدم الموقعة من قبل TAC (مركز المساعدة التقنية (TAC) CA من Cisco إلى مجموعة نفق باسم 'RA.'

ملاحظة: تم تكوين تعيين الشهادة ل SSL بشكل مختلف عن تعيين الشهادة ل IPsec. بالنسبة ل IPsec، يتم تكوينه باستخدام قواعد 'tunnel-group-map' في وضع التكوين العام. بالنسبة ل SSL، يتم تكوينه باستخدام 'certificate-group-map' ضمن وضع تكوين WebVPN.

إختبار

لاحظ أنه بمجرد تمكين تعيين الشهادة، لن تحتاج لاختيار مجموعة النفق بعد الآن:



تصحيح الأخطاء

في هذا المثال، تسمح قاعدة تعيين الشهادة بالعثور على مجموعة النفق:

<#root>

%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,

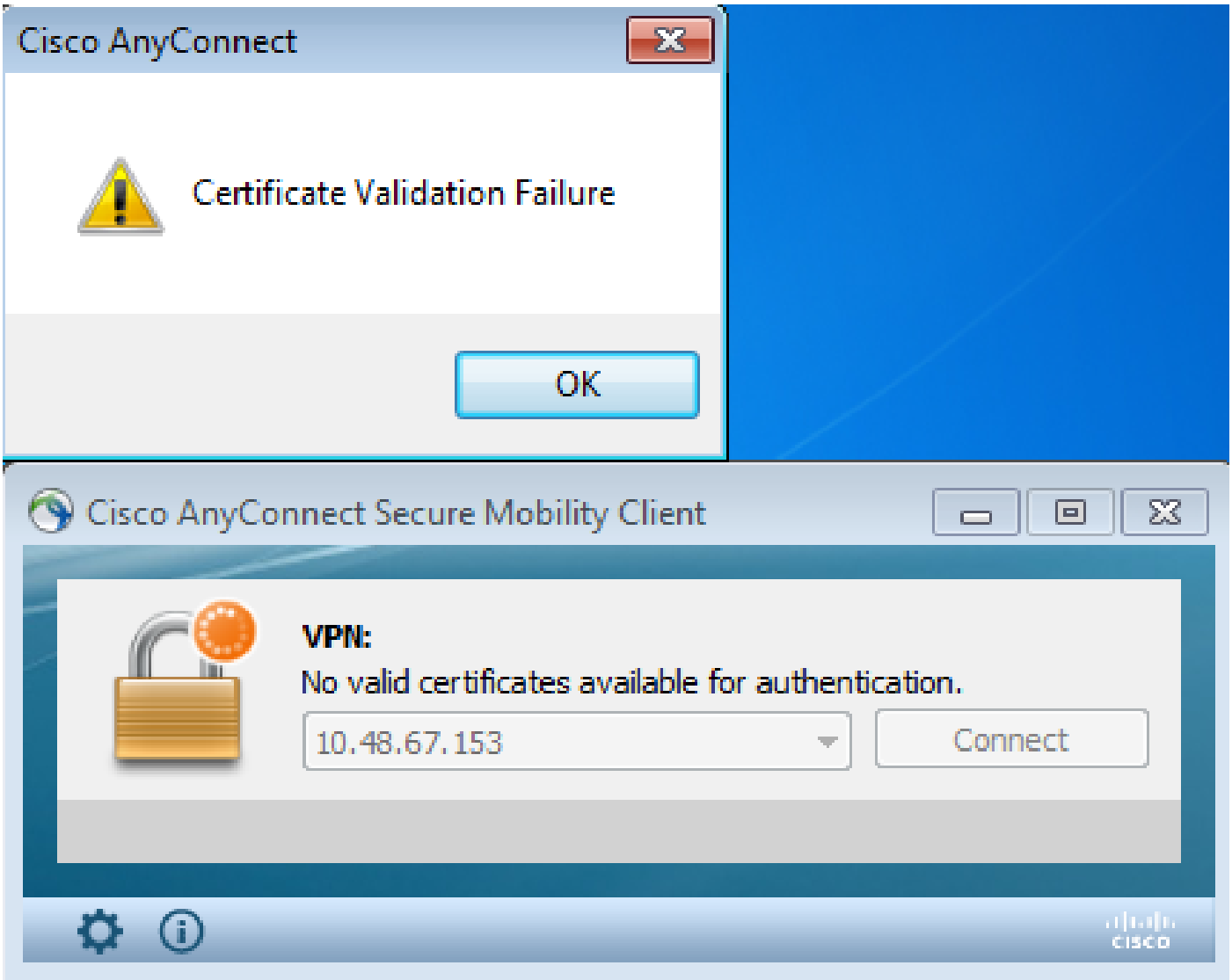
```
l=Warsaw,st=Maz,c=PL.
%ASA-7-717038:

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.
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

الشهادة الصالحة غير موجودة

بعد إزالة شهادة صالحة من Windows7، يتعذر على AnyConnect العثور على أي شهادات صالحة:



على الـ ASA، يبدو أن الجلسة أنهيت من قبل العميل (reset-i):

<#root>

```
%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

معلومات ذات صلة

- تكوين مجموعات النفق ونهج المجموعة والمستخدمين: تكوين المصادقة المضاعفة
- تكوين خادم خارجي لتفويض مستخدم جهاز الأمان
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).