Configuration de l'authentification client ASA AnyConnect Secure Mobility

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Configurer
  - Certificat pour AnyConnect
  - Installation du certificat sur ASA
  - Configuration ASA pour authentification unique et validation de certificat
    - Essai
    - Déboguer
  - Configuration ASA pour la double authentification et la validation des certificats
    - Essai
    - Déboguer
  - Configuration ASA pour double authentification et pré-remplissage
    - Essai
    - Déboguer
  - Configuration ASA pour double authentification et mappage de certificat
    - Essai
    - Déboguer
- Dépannage
  - Certificat valide non présent
- Informations connexes

Introduction

Ce document décrit une configuration pour l'accès au client ASA AnyConnect Secure Mobility qui utilise une double authentification avec validation de certificat.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de la configuration de l'interface de ligne de commande (CLI) ASA et de la configuration VPN SSL (Secure Socket Layer)
- Connaissances de base des certificats X509

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel Cisco Adaptive Security Appliance (ASA), versions 8.4 et ultérieures
- Windows 7 avec Cisco AnyConnect Secure Mobility Client 3.1

Nous supposons que vous avez utilisé une autorité de certification (CA) externe afin de générer :

- Certificat codé en base64 #12 (PKCS #12) standard de cryptographie à clé publique pour ASA (AnyConnect.pfx)
- Un certificat PKCS #12 pour AnyConnect

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit un exemple de configuration pour l'accès au client Cisco AnyConnect Secure Mobility de l'appliance de sécurité adaptatif (ASA) qui utilise une double authentification avec validation de certificat. En tant qu'utilisateur AnyConnect, vous devez fournir le certificat et les informations d'identification corrects pour l'authentification principale et secondaire afin d'obtenir un accès VPN. Ce document fournit également un exemple de mappage de certificat avec la fonctionnalité de pré-remplissage.

Configurer

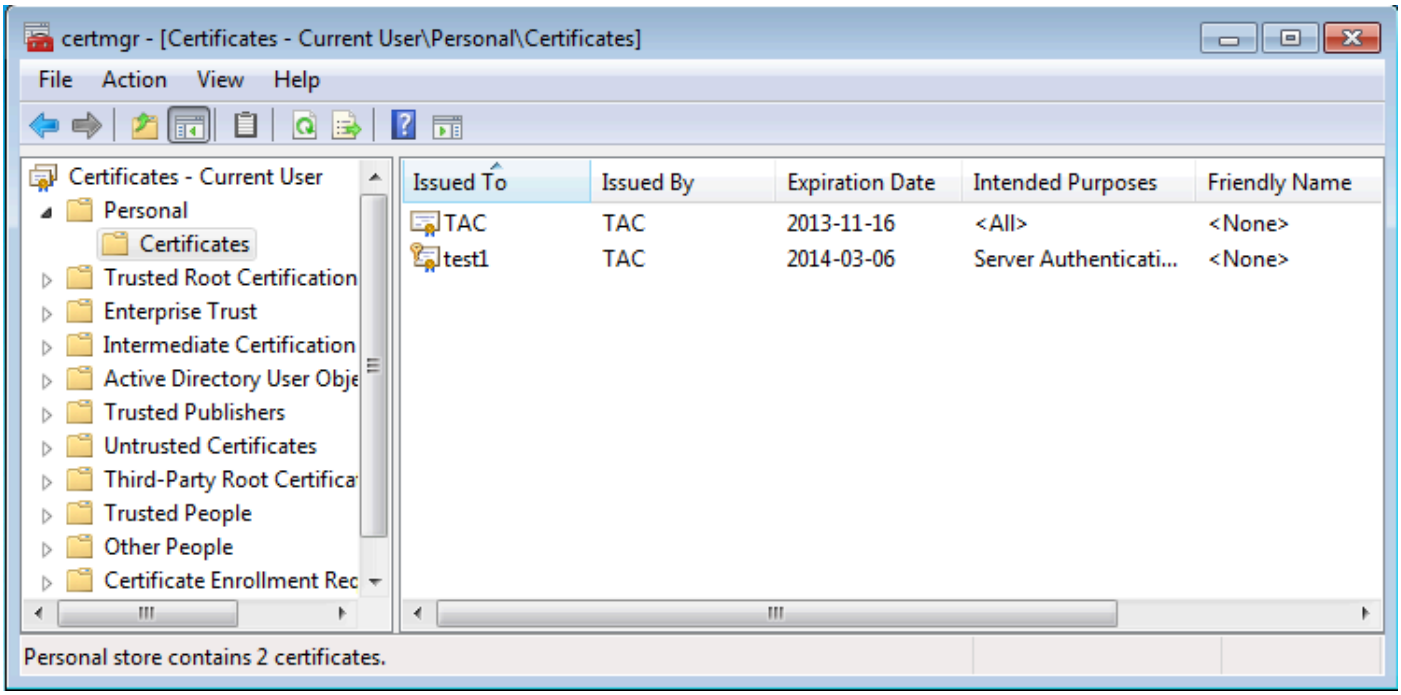


Remarque : Utilisez l'outil Command Lookup Tool afin d'obtenir plus d'informations sur les commandes utilisées dans cette section. Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils Cisco internes.

Certificat pour AnyConnect

Afin d'installer un exemple de certificat, double-cliquez sur le fichier AnyConnect.pfx, et installez ce certificat en tant que certificat personnel.

Utilisez le Gestionnaire de certificats (certmgr.msc) afin de vérifier l'installation :



Par défaut, AnyConnect tente de trouver un certificat dans le magasin d'utilisateurs Microsoft. Il n'est pas nécessaire de modifier le profil AnyConnect.

Installation du certificat sur ASA

Cet exemple montre comment ASA peut importer un certificat 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
```

Utilisez la commande show crypto ca certificates afin de vérifier l'importation :

```
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
```



Remarque : L'outil Interpréteur de sortie peut traiter certaines commandes show. Utilisez l'outil Output Interpreter Tool afin d'afficher une analyse de la sortie de la commande show. Seuls les utilisateurs inscrits de Cisco peuvent accéder aux outils et informations internes de Cisco.

Configuration ASA pour authentification unique et validation de certificat

ASA utilise à la fois l'authentification, l'autorisation et la comptabilité (AAA) et l'authentification de certificat. La validation du certificat est obligatoire. L'authentification AAA utilise une base de données locale.

Cet exemple montre une authentification unique avec validation de certificat.

<#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

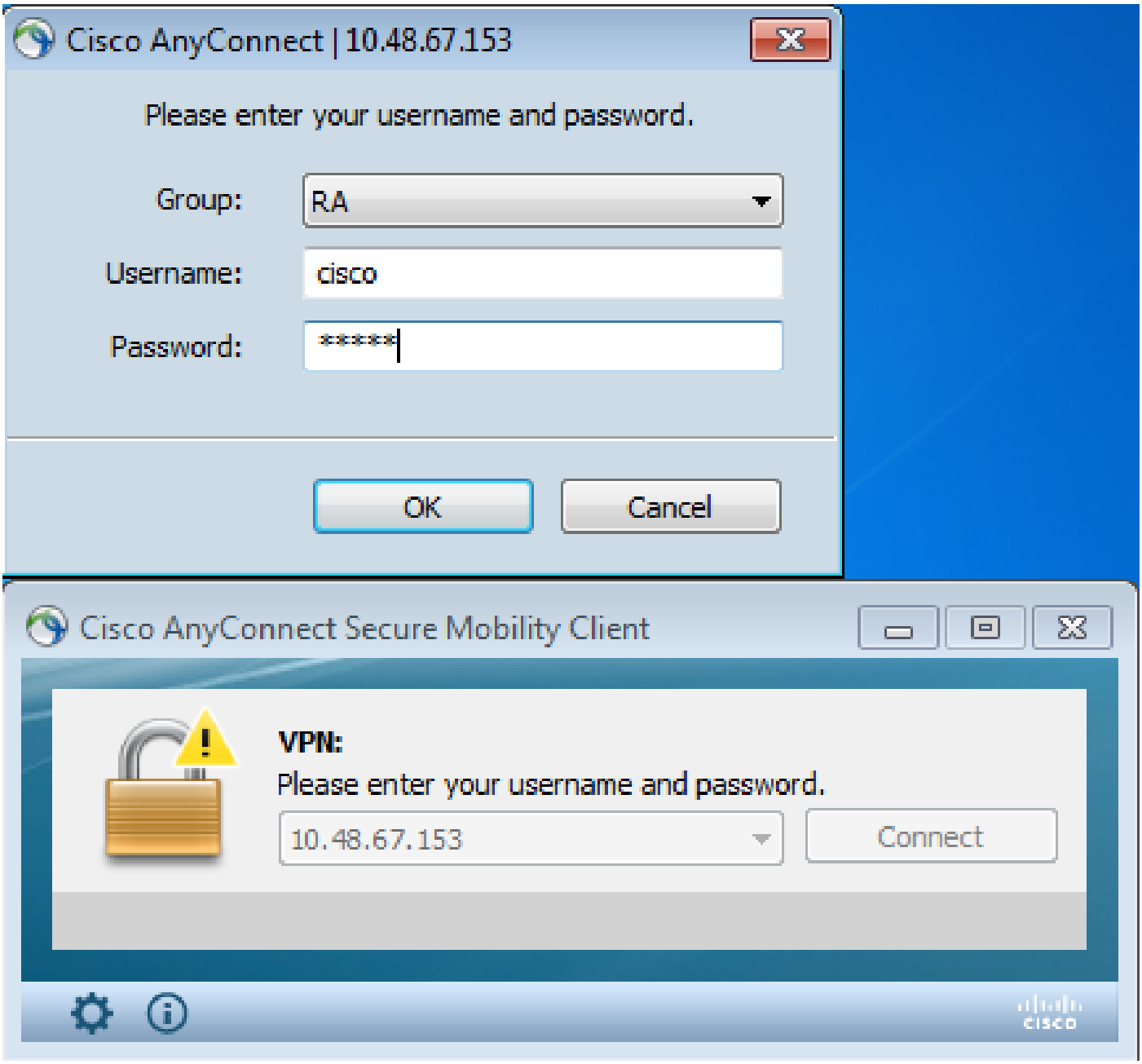
 group-alias RA enable
```

En plus de cette configuration, il est possible d'effectuer une autorisation LDAP (Lightweight Directory Access Protocol) avec le nom d'utilisateur à partir d'un champ de certificat spécifique, tel que le nom de certificat (CN). Des attributs supplémentaires peuvent ensuite être récupérés et appliqués à la session VPN. Pour plus d'informations sur l'authentification et l'autorisation de certificat, référez-vous à Exemple de configuration d'ASA AnyConnect VPN et d'autorisation OpenLDAP avec un schéma et des certificats personnalisés.

Essai

Remarque : L'outil Interpréteur de sortie peut traiter certaines commandes show. Utilisez l'outil Output Interpreter Tool afin d'afficher une analyse de la sortie de la commande show. Seuls les utilisateurs inscrits de Cisco peuvent accéder aux outils et informations internes de Cisco.

Afin de tester cette configuration, fournissez les informations d'identification locales (nom d'utilisateur cisco avec mot de passe cisco). Le certificat doit être présent :



Entrez la commande show vpn-sessiondb detail AnyConnect sur l'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 :
```

Déboguer



Remarque : Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Dans cet exemple, le certificat n'a pas été mis en cache dans la base de données. Une autorité de certification correspondante a été trouvée, l'utilisation de clé correcte a été utilisée (ClientAuthentication) et le certificat a été validé avec succès :

<#root>

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

debug webvpn AnyConnect 255

```
debug crypto ca 255
```

Les commandes de débogage détaillées, telles que la commande debug webvpn 255, peuvent générer de nombreux journaux dans un environnement de production et placer une charge lourde sur un ASA. Certains débogages WebVPN ont été supprimés pour plus de clarté :

<#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
```

Il s'agit de la tentative de trouver un groupe de tunnels correspondant. Il n'existe aucune règle de mappage de certificat spécifique et le groupe de tunnels que vous fournissez est utilisé :

<#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)
```

Voici les débogages SSL et de session générale :

<#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.
```

Configuration ASA pour la double authentification et la validation des certificats

Voici un exemple de double authentification, où le serveur d'authentification principal est LOCAL et le serveur d'authentification secondaire est LDAP. La validation du certificat est toujours activée.

Cet exemple montre la configuration 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
```

Voici l'ajout d'un serveur d'authentification secondaire :

```
<#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
```

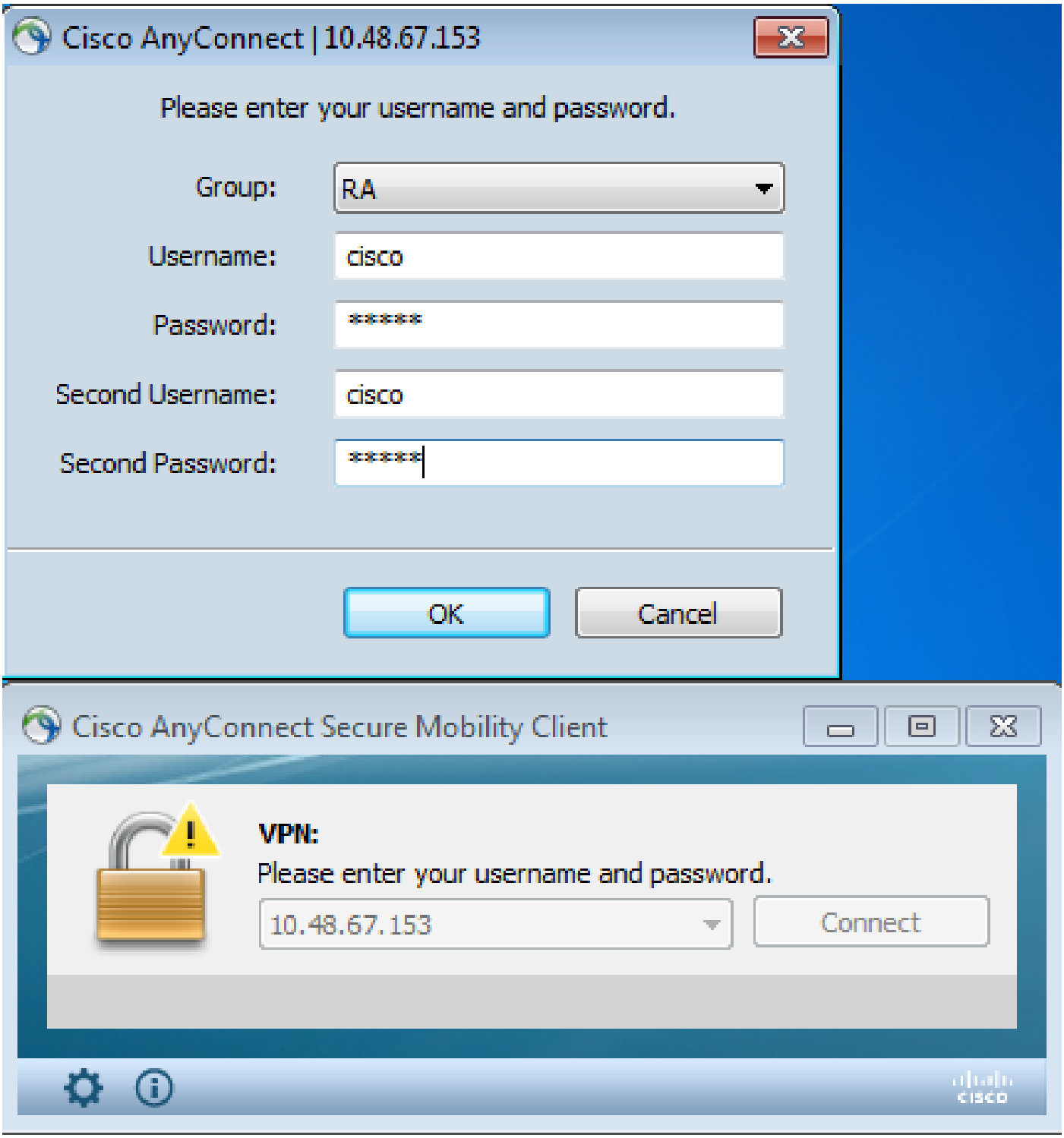
Vous ne voyez pas authentication-server-group LOCAL dans la configuration, car il s'agit d'un paramètre par défaut.

Tout autre serveur AAA peut être utilisé pour authentication-server-group. Pour le groupe de serveurs d'authentification secondaire, il est possible d'utiliser tous les serveurs AAA à l'exception d'un serveur Security Dynamics International (SDI). Dans ce cas, le SDI peut toujours être le serveur d'authentification principal.

Essai

Remarque : L'outil Interpréteur de sortie peut traiter certaines commandes show. Utilisez l'outil Output Interpreter Tool afin d'afficher une analyse de la sortie de la commande show. Seuls les utilisateurs inscrits de Cisco peuvent accéder aux outils et informations internes de Cisco.

Afin de tester cette configuration, fournissez les identifiants locaux (nom d'utilisateur cisco avec mot de passe cisco) et les identifiants LDAP (nom d'utilisateur cisco avec mot de passe LDAP). Le certificat doit être présent :



Entrez la commande show vpn-sessiondb detail AnyConnect sur l'ASA.

Les résultats sont similaires à ceux de l'authentification unique. Référez-vous à Configuration ASA pour l'authentification unique et la validation de certificat, Test .

Déboguer

Les débogages pour la session WebVPN et l'authentification sont similaires. Référez-vous à Configuration ASA pour authentification unique et validation de certificat, débogage. Un processus d'authentification supplémentaire apparaît :

<#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

Les débogages pour LDAP affichent des détails qui peuvent varier en fonction de la configuration 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
```

Configuration ASA pour double authentification et pré-remplissage

Il est possible de mapper certains champs de certificat au nom d'utilisateur utilisé pour l'authentification principale et secondaire :

<#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
```

Dans cet exemple, le client utilise le certificat : cn=test1, ou=Security, o=Cisco, l=Cracovie, st=PL, c=PL.

Pour l'authentification principale, le nom d'utilisateur provient du CN, c'est pourquoi l'utilisateur local test1 a été créé.

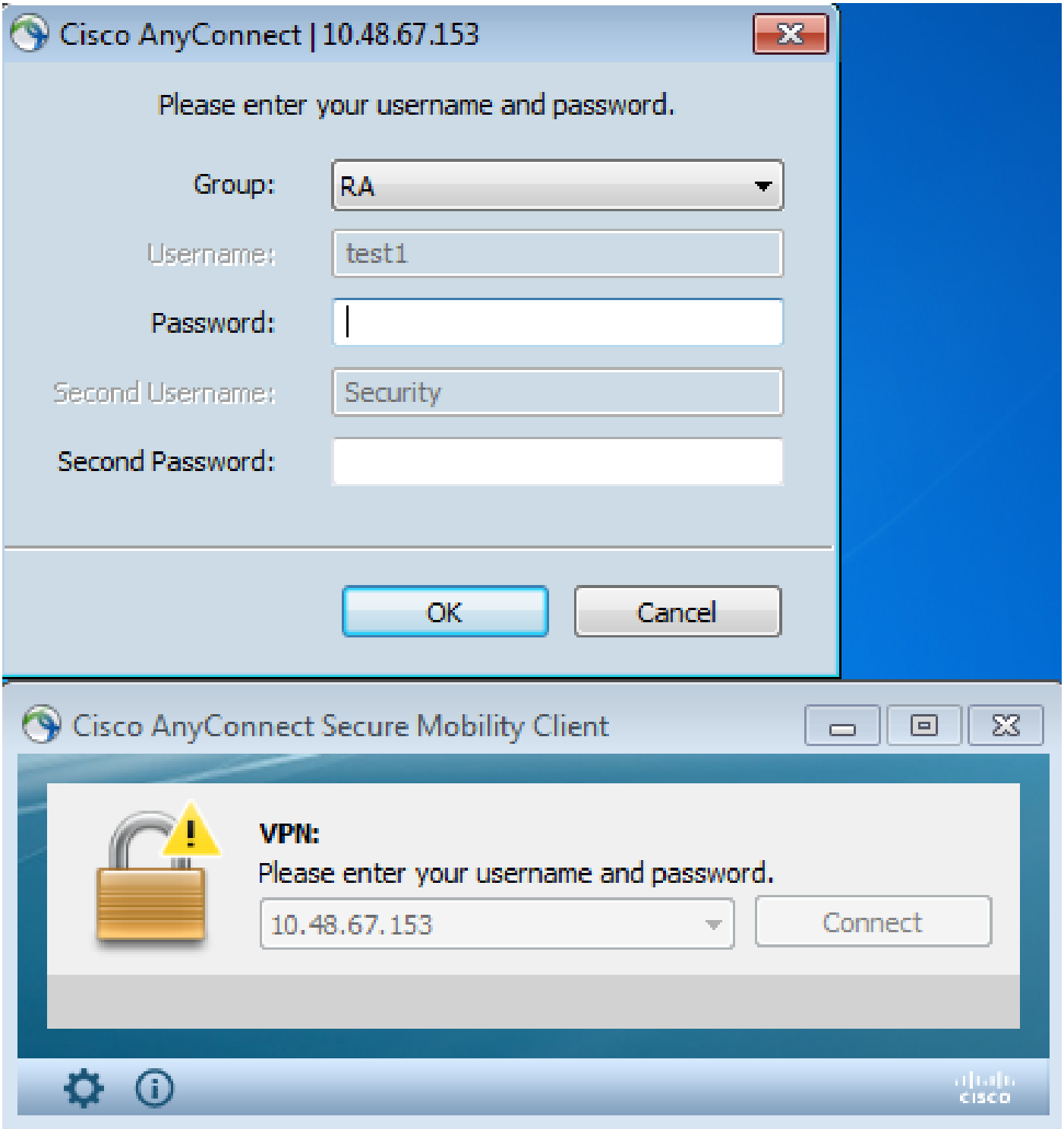
Pour l'authentification secondaire, le nom d'utilisateur provient de l'unité d'organisation (OU), raison pour laquelle la sécurité de l'utilisateur a été créée sur le serveur LDAP.

Il est également possible de forcer AnyConnect à utiliser des commandes de pré-remplissage afin de pré-remplir les noms d'utilisateur principal et secondaire. Dans un scénario réel, le serveur d'authentification principal est généralement un serveur AD ou LDAP, tandis que le serveur d'authentification secondaire est le serveur Rivest, Shamir et Adelman (RSA) qui utilise des mots de passe de jeton. Dans ce scénario, l'utilisateur doit fournir des informations d'identification

AD/LDAP (qu'il connaît), un mot de passe de jeton RSA (qu'il possède) et un certificat (sur l'ordinateur utilisé).

Essai

Notez que vous ne pouvez pas modifier le nom d'utilisateur principal ou secondaire, car il est pré-rempli à partir des champs CN et OU du certificat :



Déboguer

Cet exemple montre la demande de pré-remplissage envoyée à 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]
```

Ici, vous voyez que l'authentification utilise les noms d'utilisateur corrects :

<#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**

Configuration ASA pour double authentification et mappage de certificat

Il est également possible de mapper des certificats clients spécifiques à des groupes de tunnels spécifiques, comme illustré dans cet exemple :

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

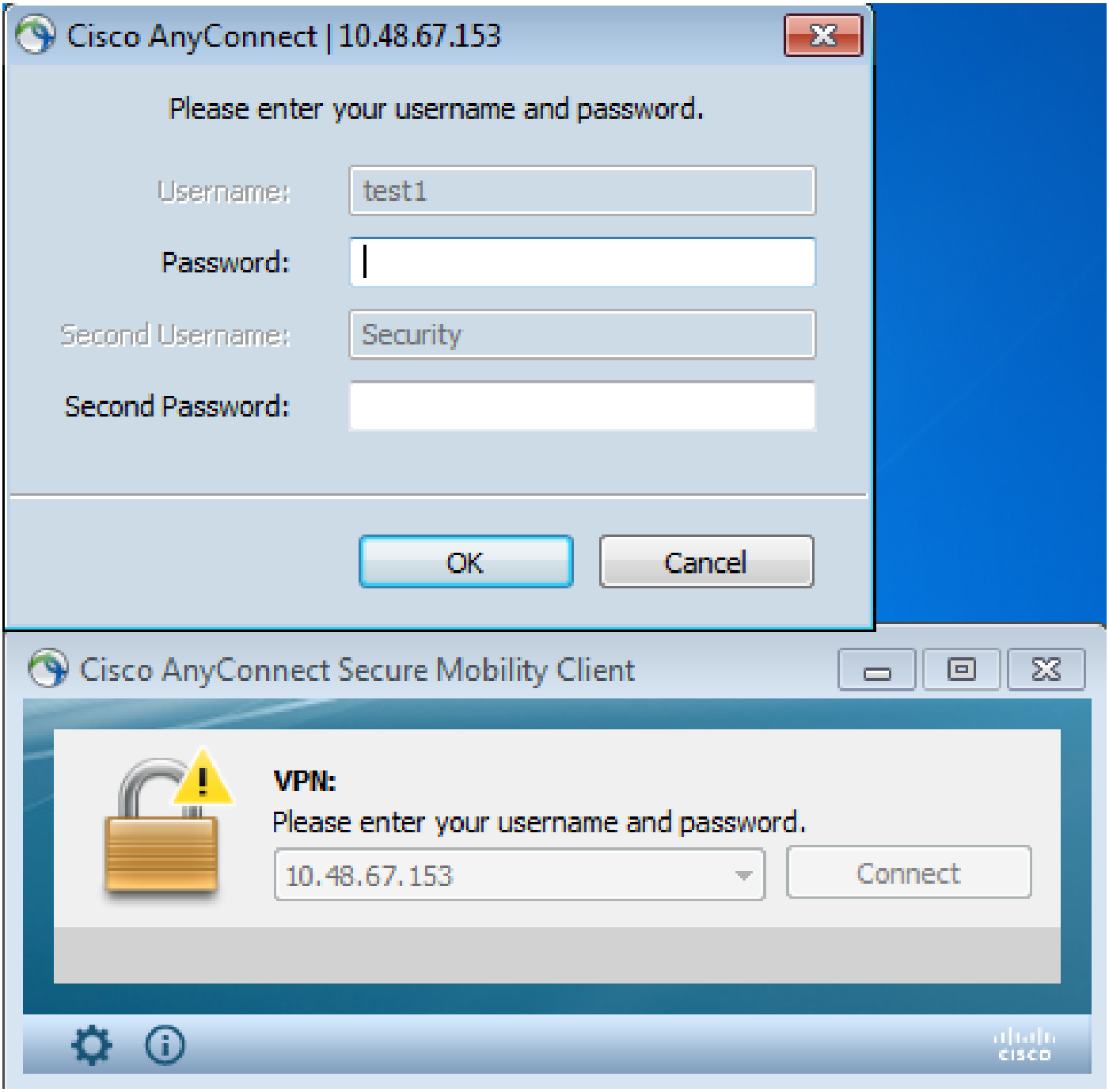
webvpn
 certificate-group-map CERT-MAP 10 RA
```

De cette façon, tous les certificats utilisateur signés par l'autorité de certification du centre d'assistance technique Cisco (TAC) sont mappés à un groupe de tunnels nommé « RA ».

Remarque : Le mappage de certificat pour SSL est configuré différemment du mappage de certificat pour IPsec. Pour IPsec, il est configuré avec les règles « tunnel-group-map » en mode de configuration globale. Pour SSL, il est configuré avec « certificate-group-map » en mode de configuration webvpn.

Essai

Notez qu'une fois le mappage de certificat activé, vous n'avez plus besoin de choisir tunnel-group :



Déboguer

Dans cet exemple, la règle de mappage de certificat permet de trouver le groupe de tunnels :

<#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

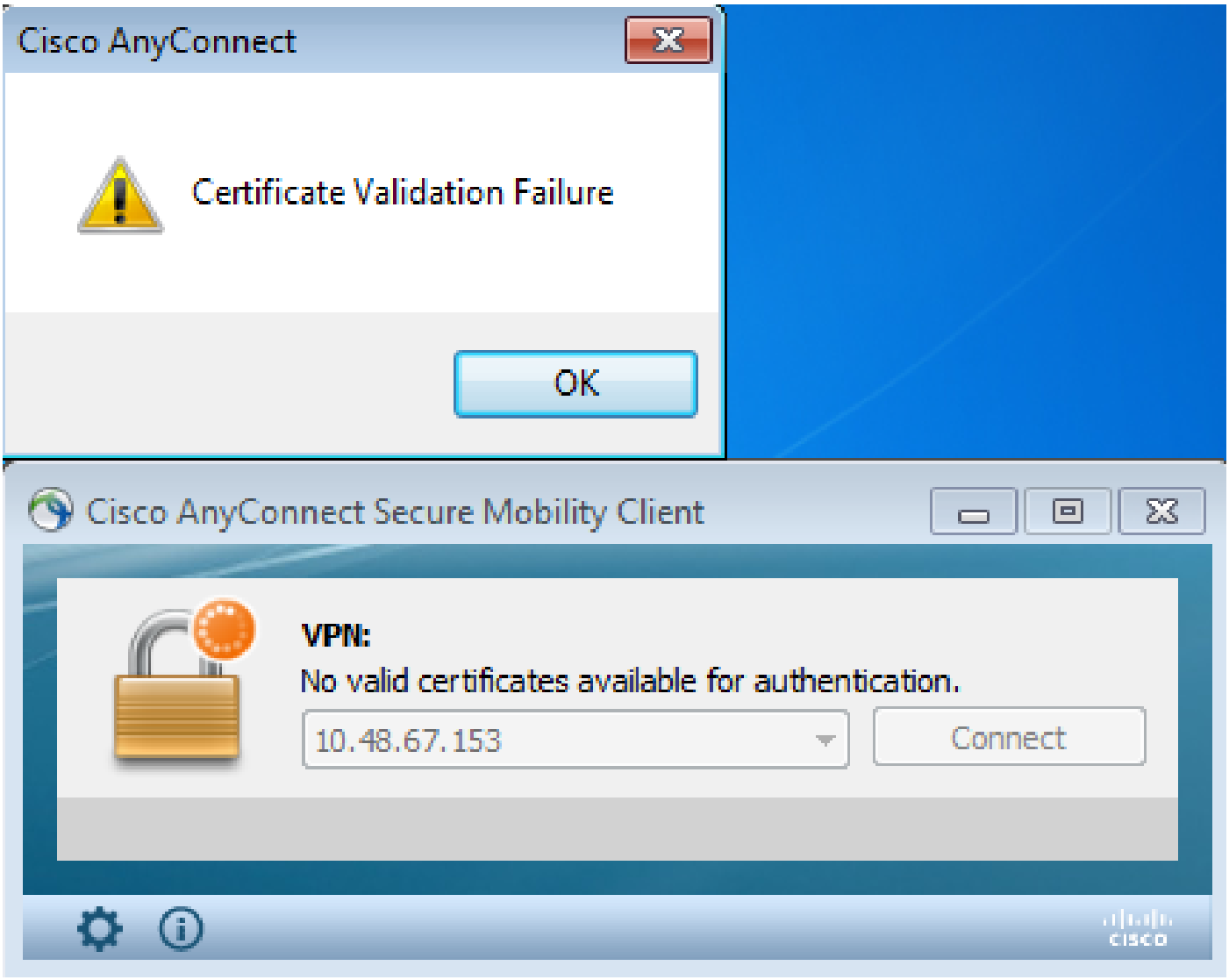
, Peer certificate:
serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,
l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Certificat valide non présent

Une fois que vous avez supprimé un certificat valide de Windows 7, AnyConnect ne trouve aucun certificat valide :



Sur l'ASA, il semble que la session soit terminée par le client (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

Informations connexes

- Configurer les groupes de tunnels, les stratégies de groupe et les utilisateurs : Configurer la double authentification
- Configurer un serveur externe pour l'autorisation utilisateur du dispositif de sécurité
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.