ASA AnyConnect Secure Mobility Client 인증 구성

목차

소개

이 문서에서는 인증서 검증과 함께 이중 인증을 사용하는 ASA AnyConnect Secure Mobility Client 액세스를 위한 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA CLI(Command Line Interface) 컨피그레이션 및 SSL(Secure Socket Layer) VPN 컨피그레이션에 대한 기본 지식
- X509 인증서에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco ASA(Adaptive Security Appliance) 소프트웨어 버전 8.4 이상
- Cisco AnyConnect Secure Mobility Client 3.1이 설치된 Windows 7

다음을 생성하기 위해 외부 CA(Certificate Authority)를 사용했다고 가정합니다.

- ASA용 PKCS #12(public-key cryptography standard #12) base64 인코딩 인증서 (AnyConnect.pfx)
- AnyConnect용 PKCS #12 인증서

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 인증서 검증과 함께 이중 인증을 사용하는 ASA(Adaptive Security Appliance) Cisco AnyConnect Secure Mobility Client 액세스의 컨피그레이션 예를 설명합니다. AnyConnect 사용자는 VPN 액세스를 얻기 위해 기본 및 보조 인증에 대한 올바른 인증서 및 자격 증명을 제공해야 합니다. 또한 이 문서에서는 미리 채우기 기능이 있는 인증서 매핑의 예도 제공합니다.

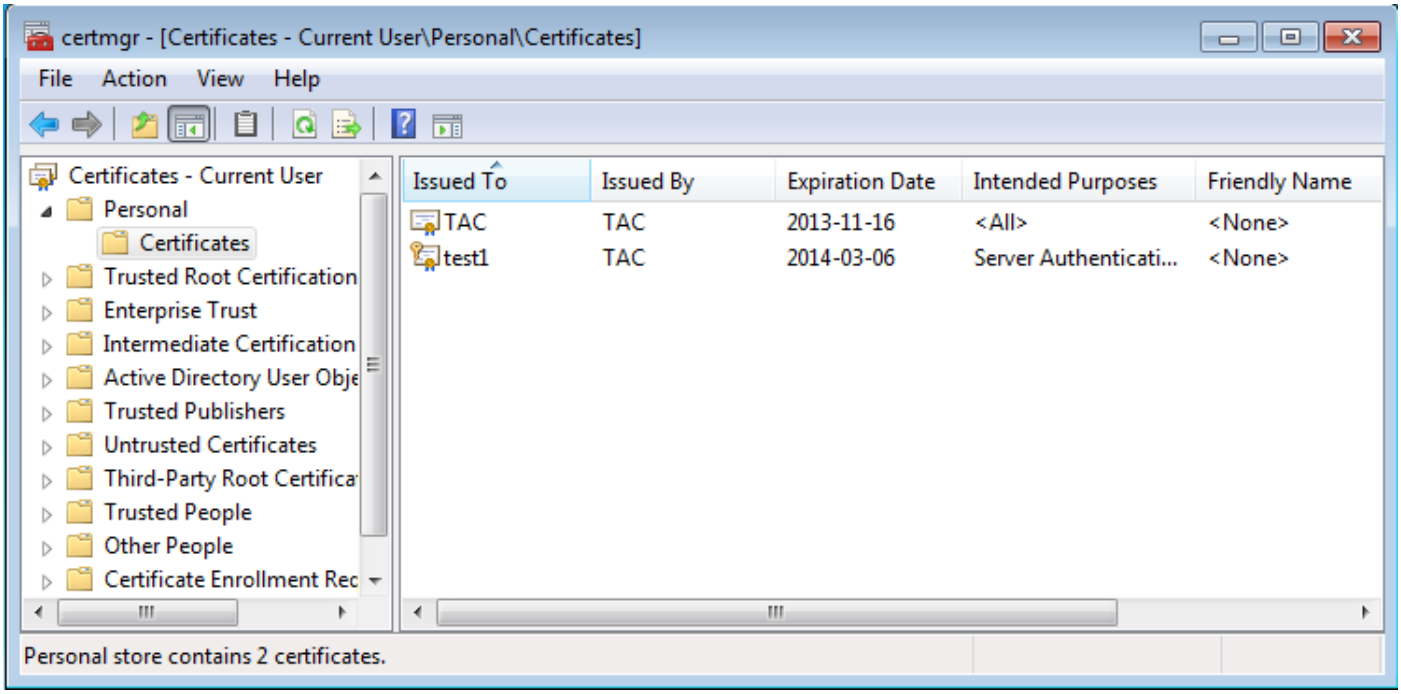
구성

참고: 이 섹션에서 사용되는 명령에 대한 자세한 내용을 보려면 명령 조회 도구를 사용하십시오. 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

AnyConnect용 인증서

예제 인증서를 설치하려면 AnyConnect.pfx 파일을 두 번 클릭하고 해당 인증서를 개인 인증서로 설치합니다.

인증서 관리자(certmgr.msc)를 사용하여 설치를 확인합니다.



기본적으로 AnyConnect는 Microsoft 사용자 저장소에서 인증서를 찾으려고 하므로 AnyConnect 프로파일을 변경할 필요가 없습니다.

ASA에 인증서 설치

다음 예에서는 ASA가 base64 PKCS #12 인증서를 가져오는 방법을 보여 줍니다.

<#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
```

가져오기를 확인하려면 show crypto ca certificates 명령을 사용합니다.

```
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
```

참고: 출력 인터프리터 도구는 특정 show 명령을 지원합니다. show 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다. 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

단일 인증 및 인증서 검증을 위한 ASA 컨피그레이션

ASA는 AAA(authentication, authorization, and accounting) 인증과 인증서 인증을 모두 사용합니다. 인증서 검증은 필수입니다. AAA 인증은 로컬 데이터베이스를 사용합니다.

이 예에서는 인증서 검증을 사용하는 단일 인증을 보여 줍니다.

<#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

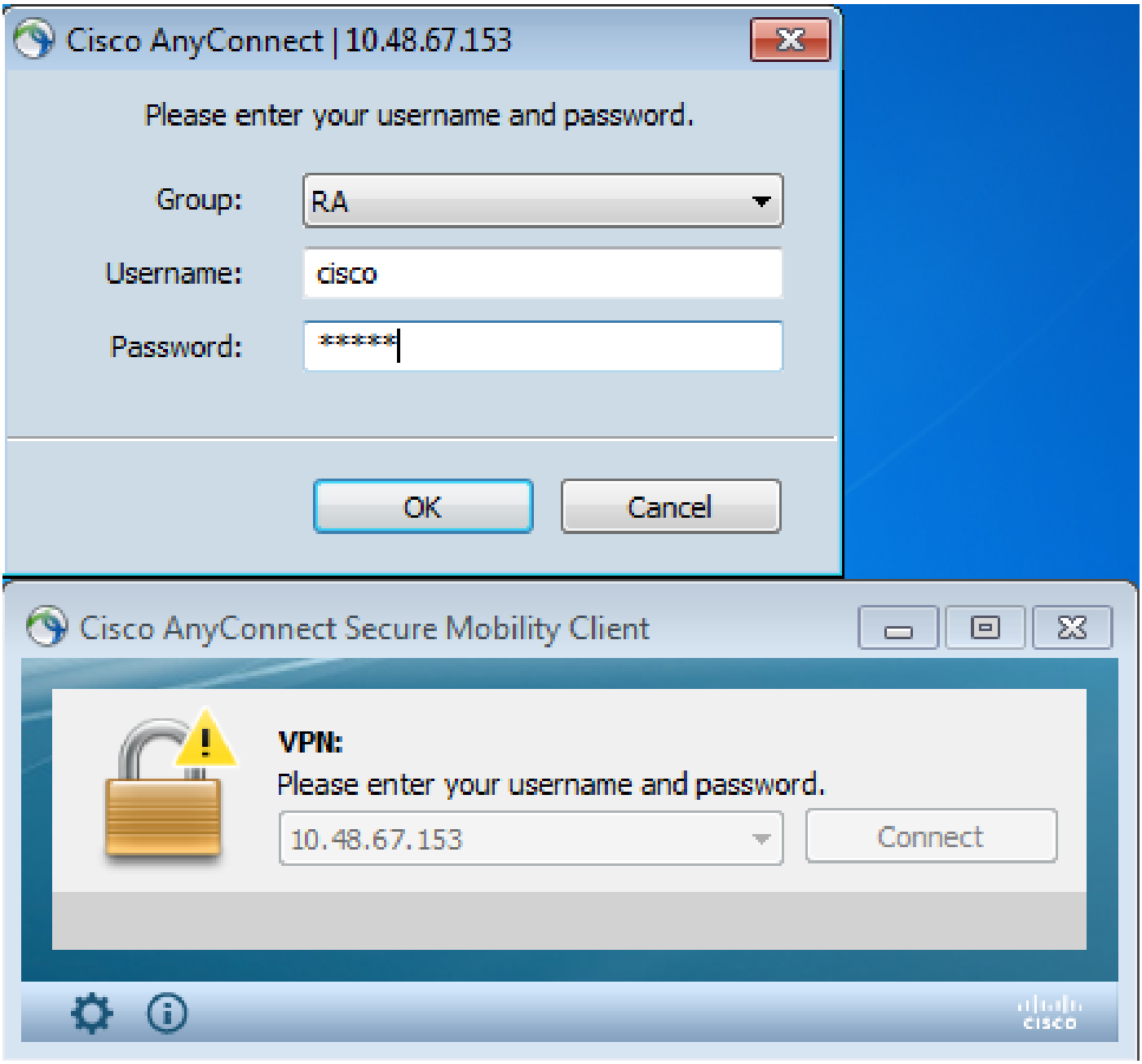
```
 group-alias RA enable
```

이 컨피그레이션 외에도 인증서 이름(CN)과 같은 특정 인증서 필드의 사용자 이름으로 LDAP(Lightweight Directory Access Protocol) 권한 부여를 수행할 수 있습니다. 그런 다음 추가 특성을 검색하여 VPN 세션에 적용할 수 있습니다. 인증 및 인증서 권한 부여에 대한 자세한 내용은 "ASA AnyConnect VPN 및 OpenLDAP Authorization with Custom Schema and Certificates Configuration Example"을 참조하십시오.

테스트

참고: 출력 인터프리터 도구는 특정 show 명령을 지원합니다. show 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다. 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

이 컨피그레이션을 테스트하려면 로컬 자격 증명(사용자 이름 cisco 및 비밀번호 cisco)을 제공합니다. 인증서가 있어야 합니다.



ASA에서 show vpn-sessiondb detail AnyConnect 명령을 입력합니다.

<#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 :
```

디버그

참고: debug 명령을 사용하기 전에 Debug 명령에 대한 중요 정보를 참조하십시오.

이 예에서는 인증서가 데이터베이스에 캐시되지 않았고, 해당 CA가 발견되었으며, 올바른 키 사용이 사용되었으며(ClientAuthentication), 인증서의 유효성 검사가 성공적으로 완료되었습니다.

<#root>

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

debug webvpn AnyConnect 255

```
debug crypto ca 255
```

debug webvpn 255 명령 같은 자세한 debug 명령은 프로덕션 환경에서 많은 로그를 생성하고 ASA에 과중한 부하를 가져올 수 있습니다. 명확성을 위해 일부 WebVPN 디버그가 제거되었습니다 .

<#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
```

일치하는 터널 그룹을 찾으려는 시도입니다. 특정 인증서 매핑 규칙이 없으며 사용자가 제공하는 터널 그룹이 사용됩니다.

<#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)
```

다음은 SSL 및 일반 세션 디버깅입니다.

<#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.
```

이중 인증 및 인증서 검증을 위한 ASA 컨피그레이션

이중 인증의 예로, 기본 인증 서버는 LOCAL이고 보조 인증 서버는 LDAP입니다. 인증서 유효성 검사가 아직 활성화되어 있습니다.

다음 예에서는 LDAP 컨피그레이션을 보여줍니다.

```
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
```

다음은 보조 인증 서버 추가입니다.

```
<#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
```

'authentication-server-group LOCAL'은 기본 설정이므로 컨피그레이션에 표시되지 않습니다.

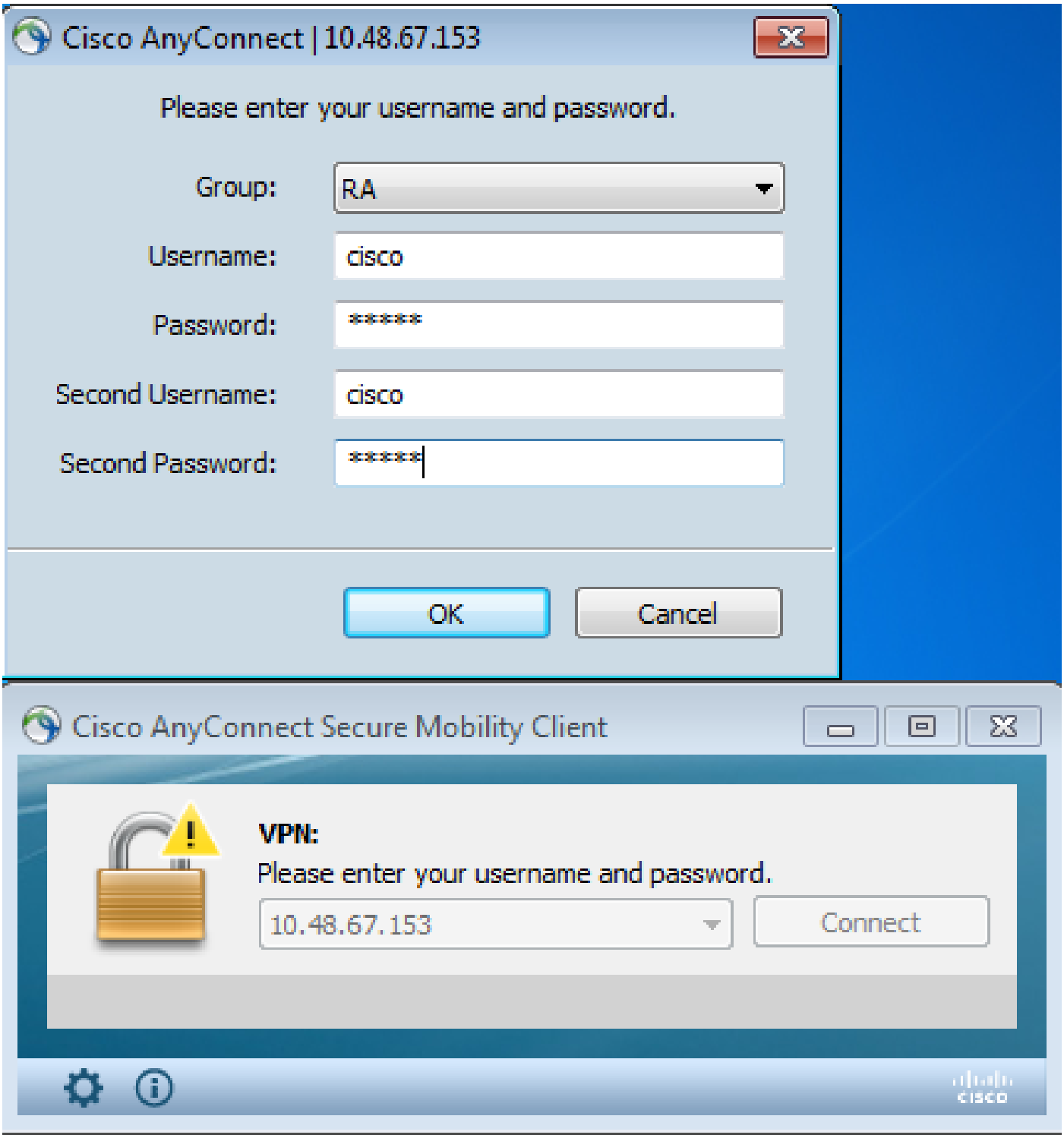
다른 AAA 서버는 'authentication-server-group'에 사용할 수 있습니다. 'secondary-authentication-server-group'의 경우 SDI(Security Dynamics International) 서버를 제외한 모든 AAA 서버를 사용할 수 있습니다. 이 경우 SDI가 여전히 기본 인증 서버일 수 있습니다.

테스트

참고: 출력 인터프리터 도구는 특정 show 명령을 지원합니다. show 명령 출력의 분석을 보려

면 아웃풋 인터프리터 툴을 사용합니다. 등록된 Cisco 사용자만 내부 Cisco 툴 및 정보에 액세스할 수 있습니다.

이 컨피그레이션을 테스트하려면 로컬 자격 증명(사용자 이름 cisco with password cisco) 및 LDAP 자격 증명(사용자 이름 cisco with password from LDAP)을 제공합니다. 인증서가 있어야 합니다.



ASA에서 show vpn-sessiondb detail AnyConnect 명령을 입력합니다.

결과는 단일 인증의 결과와 유사합니다. "단일 인증 및 인증서 검증, 테스트를 위한 ASA 구성"을 참조하십시오.

디버그

WebVPN 세션 및 인증에 대한 디버깅은 유사합니다. "단일 인증 및 인증서 검증을 위한 ASA 컨피그레이션, 디버그"를 참조하십시오. 한 가지 추가 인증 프로세스가 나타납니다.

<#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
```

LDAP에 대한 디버깅은 LDAP 컨피그레이션에 따라 달라질 수 있는 세부사항을 표시합니다.

```
[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
```

이중 인증 및 사전 채우기를 위한 ASA 컨피그레이션

기본 및 보조 인증에 사용되는 사용자 이름에 특정 인증서 필드를 매핑할 수 있습니다.

```
<#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
```

이 예에서 클라이언트는 cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL 인증서를 사용합니다
.

기본 인증의 경우 사용자 이름은 CN에서 가져온 것이므로 로컬 사용자 'test1'이 생성되었습니다.

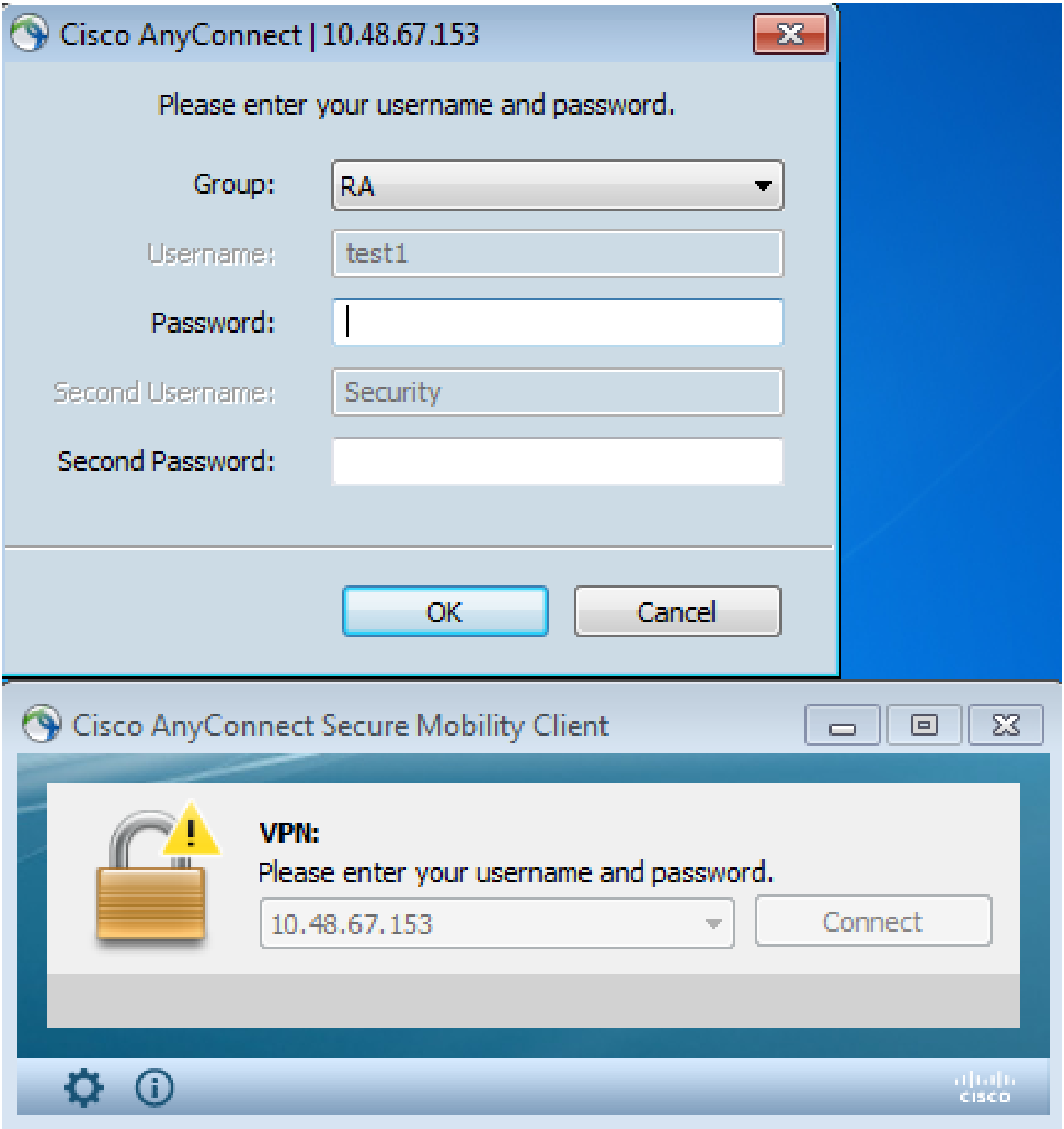
보조 인증의 경우 사용자 이름은 OU(Organizational Unit)에서 가져오므로 LDAP 서버에 'Security' 사용자가 생성되었습니다.

또한 AnyConnect가 기본 및 보조 사용자 이름을 미리 채우기 위해 pre-fill 명령을 사용하도록 강제할 수도 있습니다.

실제 시나리오에서 기본 인증 서버는 일반적으로 AD 또는 LDAP 서버인 반면, 보조 인증 서버는 토큰 비밀번호를 사용하는 RSA(Rivest, Shamir, and Adelman) 서버입니다. 이 시나리오에서 사용자는 AD/LDAP 자격 증명(사용자가 알고 있음), RSA 토큰 비밀번호(사용자가 가지고 있음) 및 인증서(사용되는 컴퓨터에서)를 제공해야 합니다.

테스트

기본 또는 보조 사용자 이름은 인증서 CN 및 OU 필드에서 미리 입력되므로 변경할 수 없습니다.



디버그

다음 예에서는 AnyConnect로 전송된 미리 채우기 요청을 보여줍니다.

```
%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]
```

여기서 인증이 올바른 사용자 이름을 사용함을 알 수 있습니다.

```
<#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
```

이중 인증 및 인증서 매핑을 위한 ASA 컨피그레이션

다음 예에 표시된 것처럼 특정 클라이언트 인증서를 특정 터널 그룹에 매핑할 수도 있습니다.

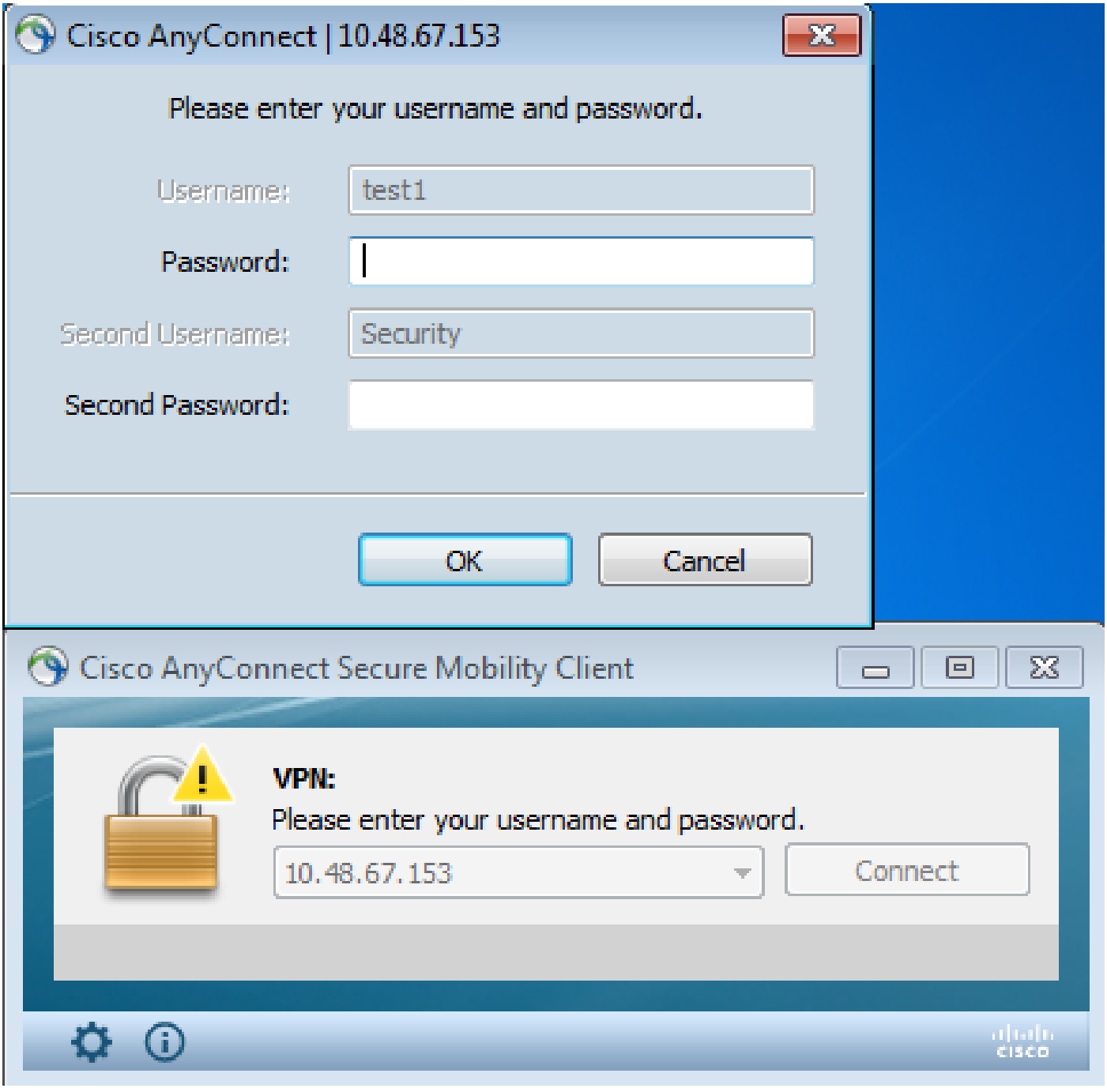
```
crypto ca certificate map CERT-MAP 10
 issuer-name co tac

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

이렇게 하면 Cisco TAC(Technical Assistance Center) CA가 서명한 모든 사용자 인증서가 'RA'라는 터널 그룹에 매핑됩니다.

참고: SSL에 대한 인증서 매핑은 IPsec에 대한 인증서 매핑과 다르게 구성됩니다. IPsec의 경우 전역 컨피그레이션 모드에서 'tunnel-group-map' 규칙으로 구성됩니다. SSL의 경우 webvpn 컨피그레이션 모드에서 'certificate-group-map'으로 구성됩니다.

테스트

인증서 매핑이 활성화되면 터널 그룹을 더 이상 선택할 필요가 없음을 확인합니다.



디버그

이 예에서는 인증서 매핑 규칙을 사용하여 터널 그룹을 찾을 수 있습니다.

<#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

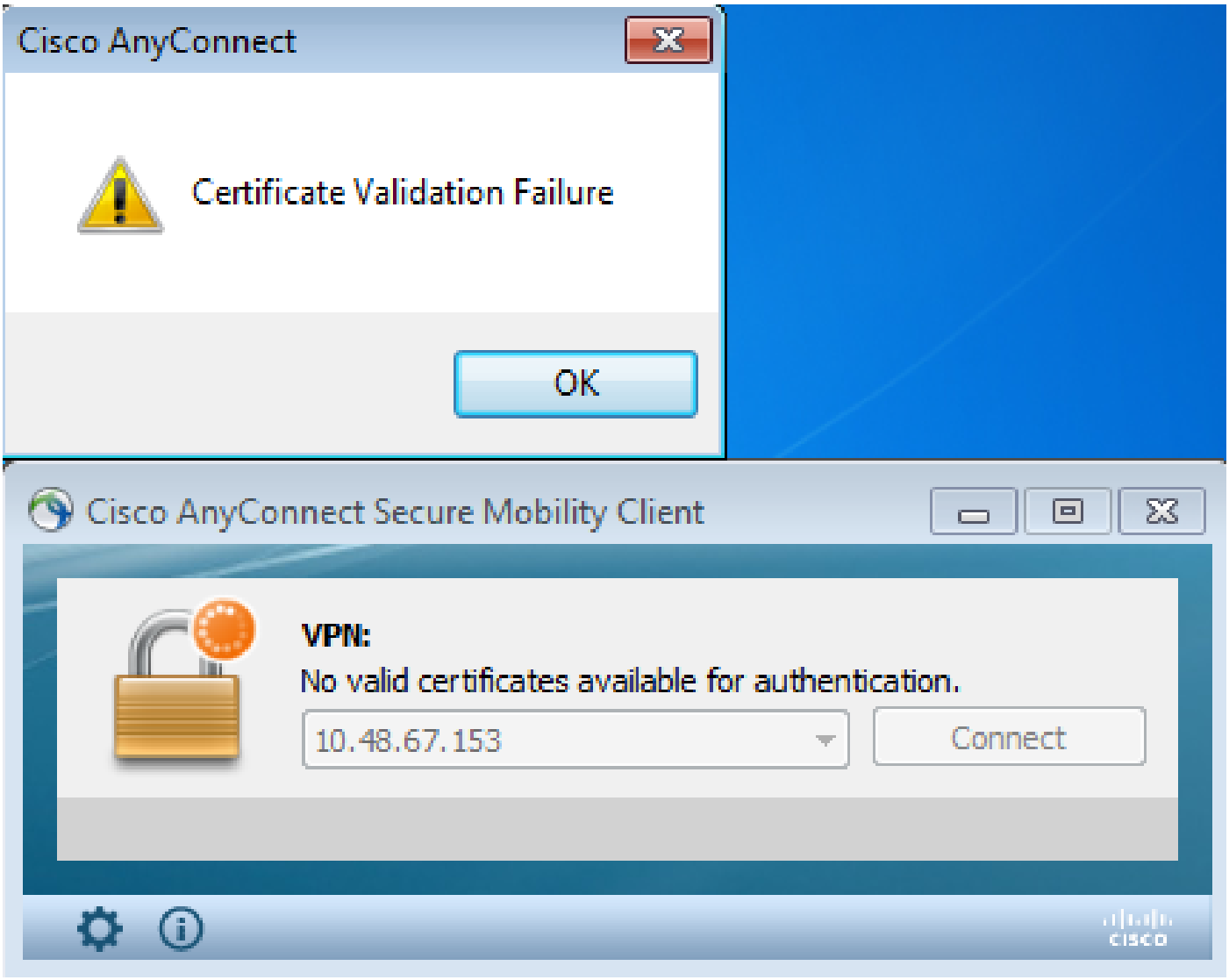
, Peer certificate:
serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,
l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

유효한 인증서가 없습니다.

Windows7에서 유효한 인증서를 제거한 후 AnyConnect에서 유효한 인증서를 찾을 수 없습니다.



ASA에서는 세션이 클라이언트에 의해 종료된 것 같습니다(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

관련 정보

- 터널 그룹, 그룹 정책 및 사용자 구성: 이중 인증 구성
- 보안 어플라이언스 사용자 권한 부여를 위한 외부 서버 구성
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.