配置ASA AnyConnect安全移动客户端身份验证

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

配置

- AnyConnect证书
- ASA上的证书安装
- 用于单一身份验证和证书验证的ASA配置
  - 测试
  - 调试
- 用于双重身份验证和证书验证的ASA配置
  - 测试
  - 调试
- 用于双重身份验证和预填充的ASA配置
  - 测试
  - 调试
- 用于双重身份验证和证书映射的ASA配置
  - 测试
  - 调试

故障排除

- 有效证书不存在

相关信息

简介

本文档介绍ASA AnyConnect安全移动客户端访问的配置，该配置使用双重身份验证和证书验证。

先决条件

要求

Cisco 建议您了解以下主题：

- 基本了解ASA命令行界面(CLI)配置和安全套接字层(SSL)VPN配置
- X509证书的基本知识

使用的组件

本文档中的信息基于以下软件版本：

- 思科自适应安全设备(ASA)软件8.4版及更高版本
- Windows 7与Cisco AnyConnect安全移动客户端3.1

假设您使用外部证书颁发机构(CA)生成：

- 用于ASA的公钥#12密标准#12证(PKCS)base64编码证书(AnyConnect.pfx)
- 用于AnyConnect#12PKCS安全证书

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍自适应安全设备(ASA)Cisco AnyConnect安全移动客户端访问的配置示例，该访问使用双重身份验证和证书验证。作为AnyConnect用户，您必须提供主身份验证和辅助身份验证的正确证书和凭证才能获得VPN访问。本文档还提供了使用预填充功能的证书映射示例。

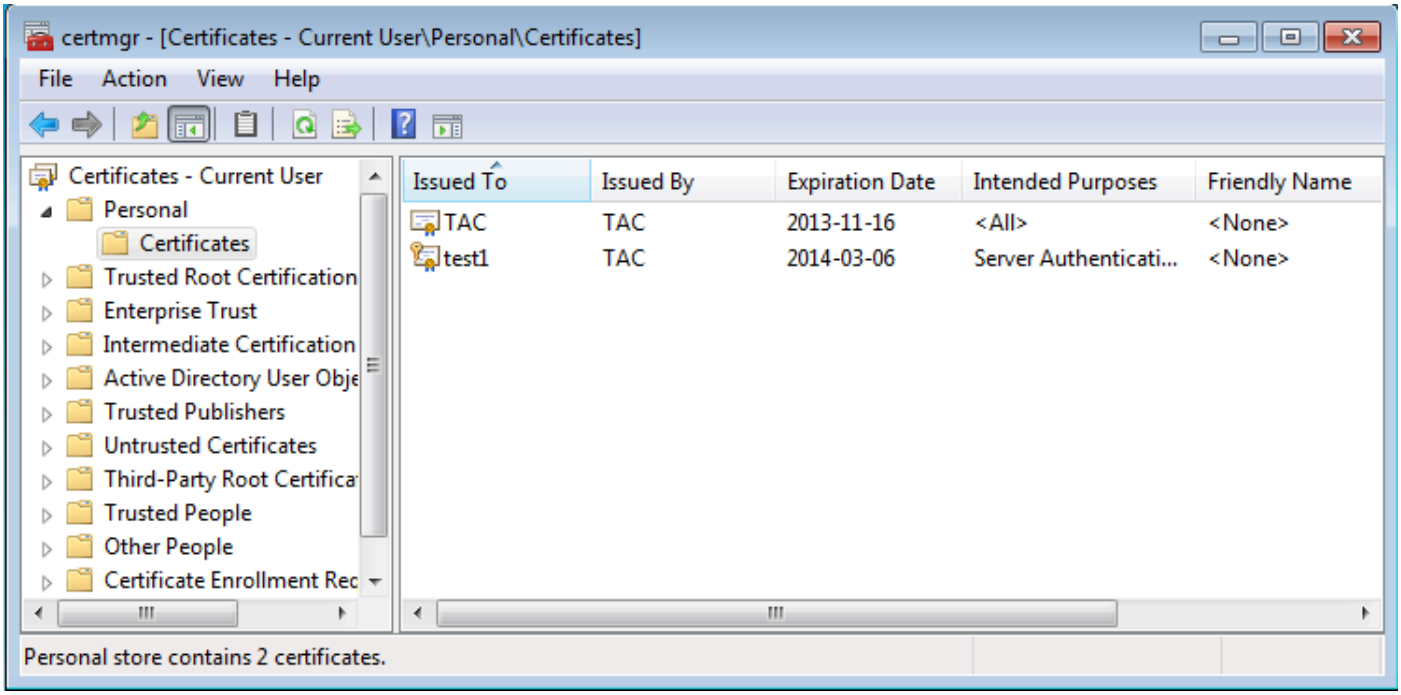
配置

注意：使用命令查找工具可获取本节所用命令的详细信息。只有注册的思科用户才能访问内部思科工具和信息。

AnyConnect证书

要安装示例证书，请双击AnyConnect.pfx文件，然后将该证书安装为个人证书。

使用证书管理器(certmgr.msc)验证安装：



默认情况下，AnyConnect尝试在Microsoft用户存储区查找证书。无需对AnyConnect配置文件进行

任何更改。

ASA上的证书安装

此示例显示ASA如何导入base64 PKCS #12证书：

<#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
```

使用show crypto ca certificates命令验证导入：

```
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
```



注意：命令输出解释程序工具支持某些 show 命令。使用Output Interpreter工具查看show命令输出的分析。只有注册的Cisco用户才能访问内部Cisco工具和信息。

用于单一身份验证和证书验证的ASA配置

ASA同时使用身份验证、授权和记帐(AAA)身份验证和证书身份验证。必须验证证书。AAA身份验证使用本地数据库。

此示例显示具有证书验证的单一身份验证。

<#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
```

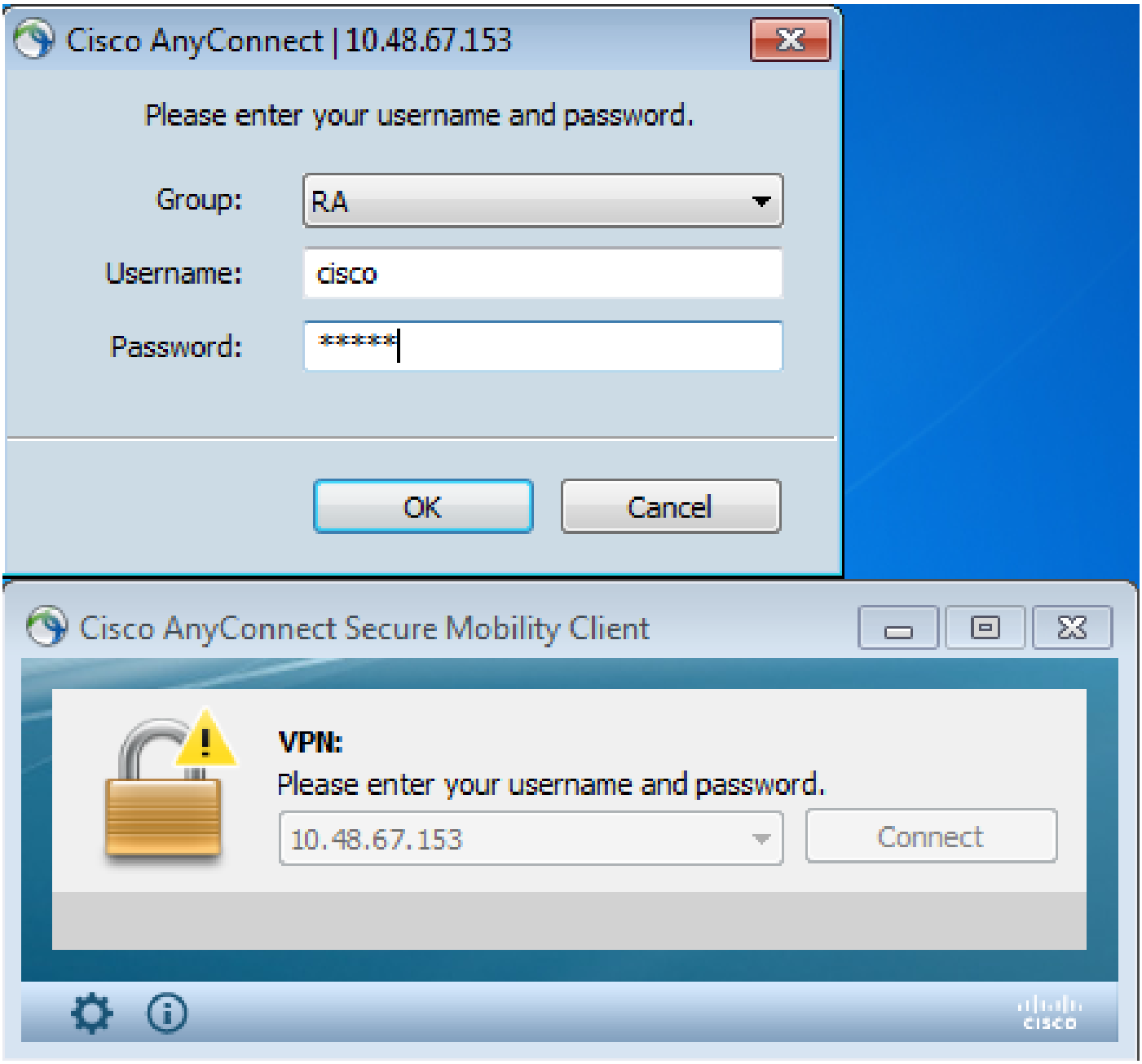
除了此配置之外，还可以使用来自特定证书字段(例如证书名称(CN))的用户名执行轻量级目录访问协议(LDAP)授权。 然后可以检索其他属性并将其应用于VPN会话。有关身份验证和证书授权的详细信息，请参阅使用自定义方案和证书的ASA AnyConnect VPN和OpenLDAP授权配置示例。

测试



注意：命令输出解释程序工具支持某些 show 命令。使用Output Interpreter工具查看show命令输出的分析。只有注册的Cisco用户才能访问内部Cisco工具和信息。

要测试此配置，请提供本地凭证（用户名cisco和密码cisco）。 证书必须存在：



在ASA上输入show vpn-sessiondb detail AnyConnect命令：

<#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 :
```

调试

注意：使用 debug 命令之前，请参阅有关 Debug 命令的重要信息。

在本示例中，证书未缓存在数据库中。已找到对应的CA，使用了正确的密钥用法(ClientAuthentication)，并且证书已成功验证：

<#root>

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

debug webvpn AnyConnect 255

```
debug crypto ca 255
```

详细的调试命令(如debug webvpn 255命令)可以在生产环境中生成许多日志，并给ASA带来沉重的负载。为清楚起见，删除了某些WebVPN调试：

<#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
```

这是查找匹配隧道组的尝试。没有特定证书映射规则，并且使用您提供的隧道组：

<#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)
```

以下是SSL和常规会话调试：

<#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.

用于双重身份验证和证书验证的ASA配置

这是双重身份验证的示例，其中主身份验证服务器是LOCAL，辅助身份验证服务器是LDAP。证书验证仍处于启用状态。

此示例显示LDAP配置：

```
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
```

下面是添加辅助身份验证服务器：

```
<#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
```

您在配置中看不到authentication-server-group LOCAL，因为这是默认设置。

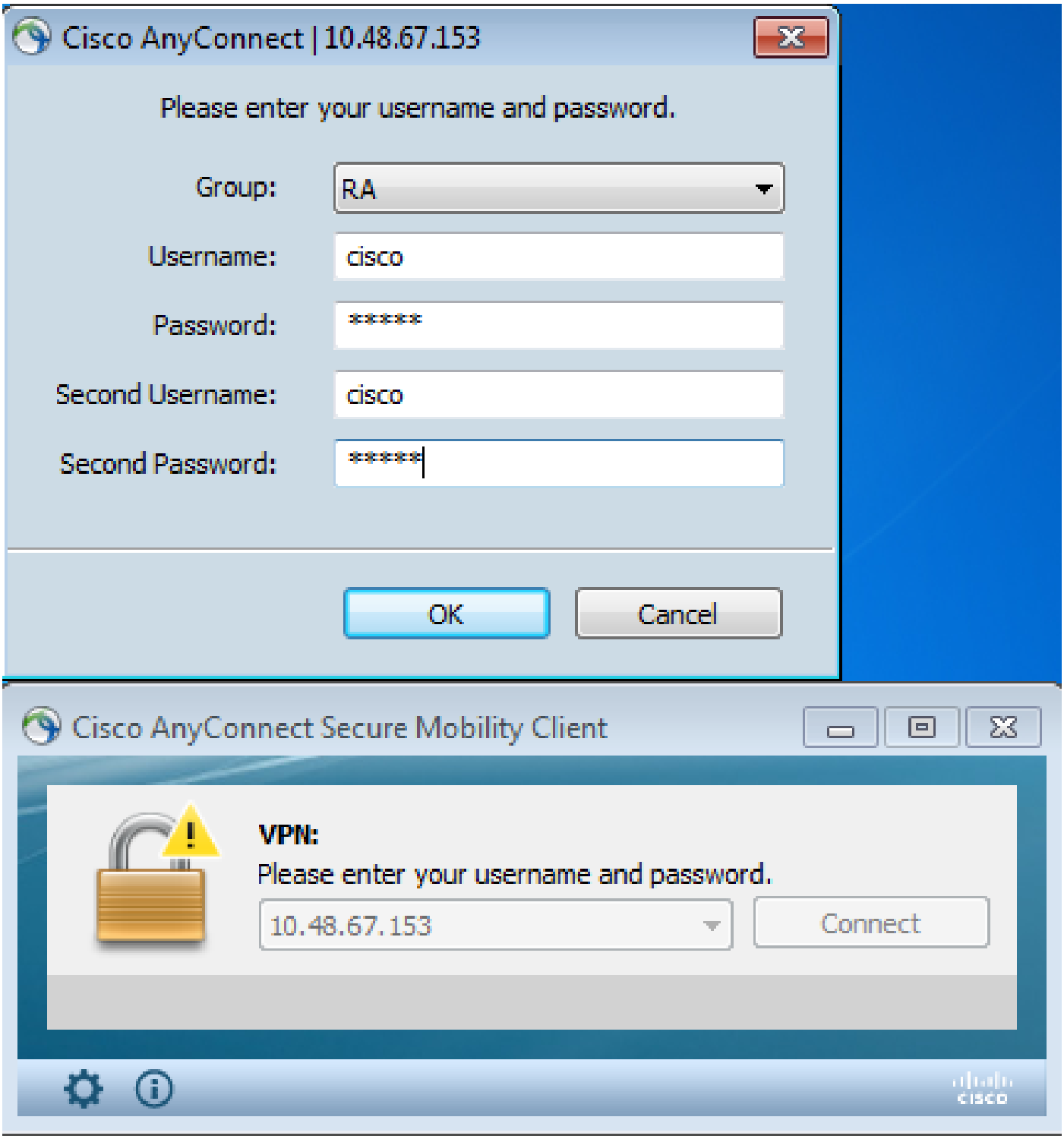
任何其他AAA服务器都可用于authentication-server-group。对于secondary-authentication-server-group，可以使用除安全动态国际(SDI)服务器之外的所有AAA服务器。在这种情况下，SDI仍可能是主身份验证服务器。

测试

注意：命令输出解释程序工具支持某些 show 命令。使用Output Interpreter工具查看show命令输出的分析。只有注册的Cisco用户才能访问内部Cisco工具和信息。

要测试此配置，请提供本地凭证（用户名cisco和密码cisco）和LDAP凭证（用户名cisco和密码

LDAP的密码）。 证书必须存在：



在ASA上输入show vpn-sessiondb detail AnyConnect命令。

结果与单一身份验证的结果相似。有关单一身份验证和证书验证的ASA配置，请参阅“测试”。

调试

WebVPN会话的调试和身份验证类似。有关单一身份验证和证书验证的ASA配置，请参阅Debug。系统将显示另一个身份验证过程：

<#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

LDAP的调试显示可能因LDAP配置而变化的详细信息：

```
[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
```

用于双重身份验证和预填充的ASA配置

可以将某些证书字段映射到用于主要身份验证和辅助身份验证的用户名：

```
<#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
```

在本示例中，客户端使用证书：cn=test1,ou=Security，o=Cisco，l=Krakow，st=PL，c=PL。

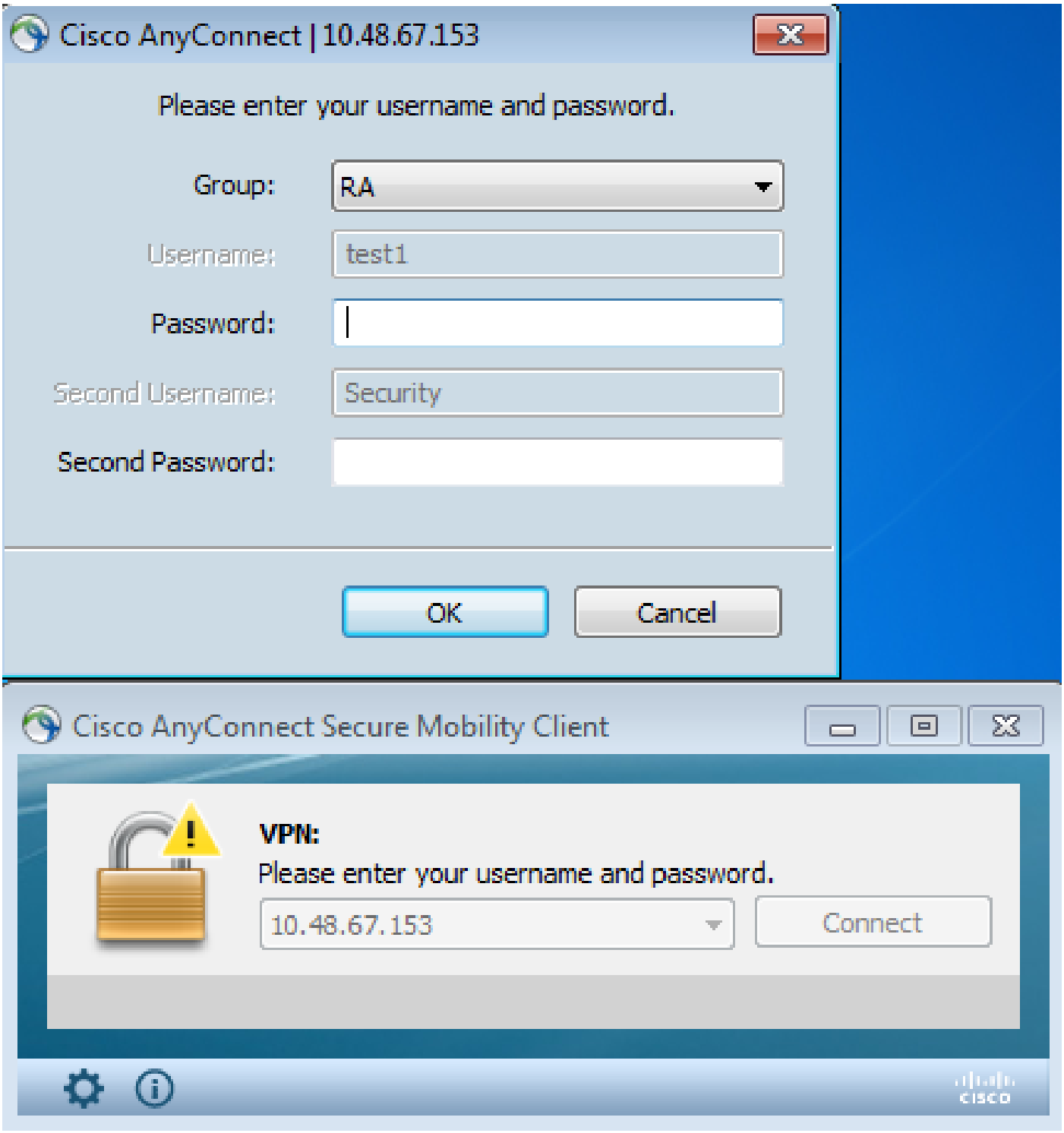
对于主要身份验证，用户名取自CN，因此创建了本地用户test1。

对于辅助身份验证，用户名取自组织单位(OU)，这就是在LDAP服务器上创建用户安全的原因。

也可以强制AnyConnect使用预填充命令以预填充主要和辅助用户名。在真实情况下，主要身份验证服务器通常是AD或LDAP服务器，而辅助身份验证服务器是使用令牌密码的Rivest、Shamir和Adelman(RSA)服务器。在此方案中，用户必须提供AD/LDAP凭证（用户知道）、RSA令牌密码（用户拥有）和证书（在使用的计算机上）。

测试

请注意，无法更改主要或辅助用户名，因为它是从证书CN和OU字段预填充的：



调试

此示例显示发送到AnyConnect的预填充请求：

```
%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]
```

在这里，您可以看到身份验证使用正确的用户名：

<#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**

用于双重身份验证和证书映射的ASA配置

也可以将特定客户端证书映射到特定隧道组，如下例所示：

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

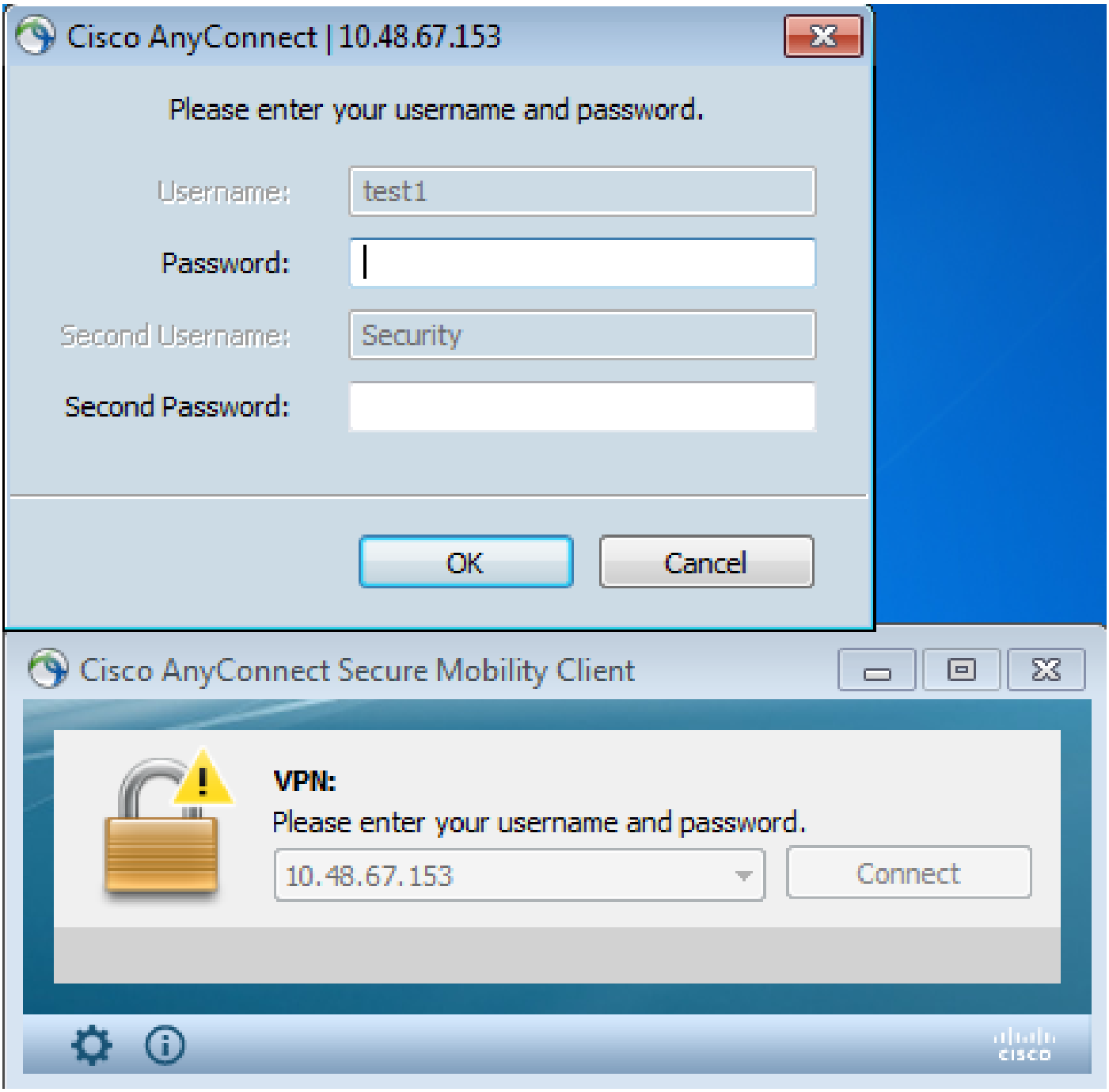
webvpn
 certificate-group-map CERT-MAP 10 RA
```

这样，思科技术支持中心(TAC)CA签署的所有用户证书都将映射到名为“RA”的隧道组。

注意：SSL的证书映射配置与IPsec的证书映射不同。对于IPsec，在全局配置模式下使用“tunnel-group-map”规则进行配置。对于SSL，在webvpn配置模式下使用“certificate-group-map”进行配置。

测试

请注意，启用证书映射后，您无需再选择隧道组：



调试

在本示例中，证书映射规则允许找到隧道组：

<#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

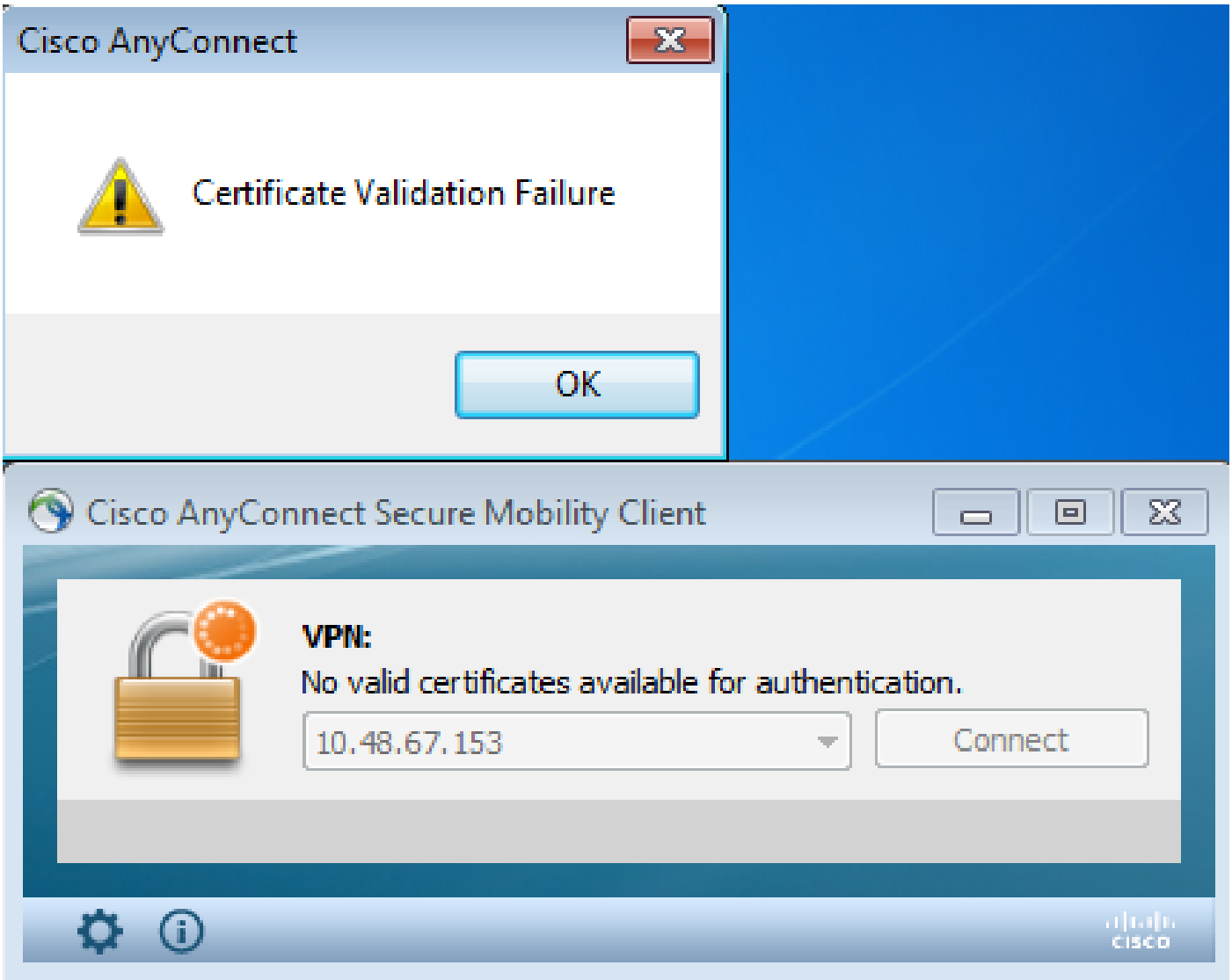
, Peer certificate:
serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,
l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

有效证书不存在

从Windows7中删除有效证书后，AnyConnect找不到任何有效证书：



在ASA上，会话似乎由客户端终止(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

相关信息

- 配置隧道组、组策略和用户：配置双重身份验证
- 为安全设备用户授权配置外部服务器
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。