

# ASA AnyConnect双重身份验证用证书确认、映射和预先充满配置指南

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[AnyConnect的证书](#)

[ASA的认证安装](#)

[单个验证和证书确认的ASA配置](#)

[测验](#)

[调试](#)

[双重身份验证和证书确认的ASA配置](#)

[测验](#)

[调试](#)

[双重身份验证和预先充满的ASA配置](#)

[测验](#)

[调试](#)

[双重身份验证和证书映射的ASA配置](#)

[测验](#)

[调试](#)

[故障排除](#)

[不现在的有效证书](#)

[相关信息](#)

## 简介

本文描述以证书确认使用双重身份验证的可适应安全工具(ASA) Cisco AnyConnect安全移动客户端访问的配置示例。作为AnyConnect用户，您必须为主要的和附属验证提供正确证书和凭证为了获得VPN访问。本文也提供证书映射示例预先充满功能。

## [先决条件](#)

## [要求](#)

Cisco 建议您了解以下主题：

- ASA命令行界面(CLI)配置和安全套接字层SSL VPN配置基础知识
- X509证书基础知识

## 使用的组件

本文档中的信息基于以下软件版本：

- Cisco可适应安全工具(ASA)软件，版本8.4和以上
- 与Cisco AnyConnect安全移动客户端3.1的Windows 7

假设，您使用一外部Certificate Authority (CA)为了生成：

- ASA的(anyconnect.pfx)一公钥加密标准#12 (PKCS-12) base64-encoded证书
- AnyConnect的一PKCS-12证书

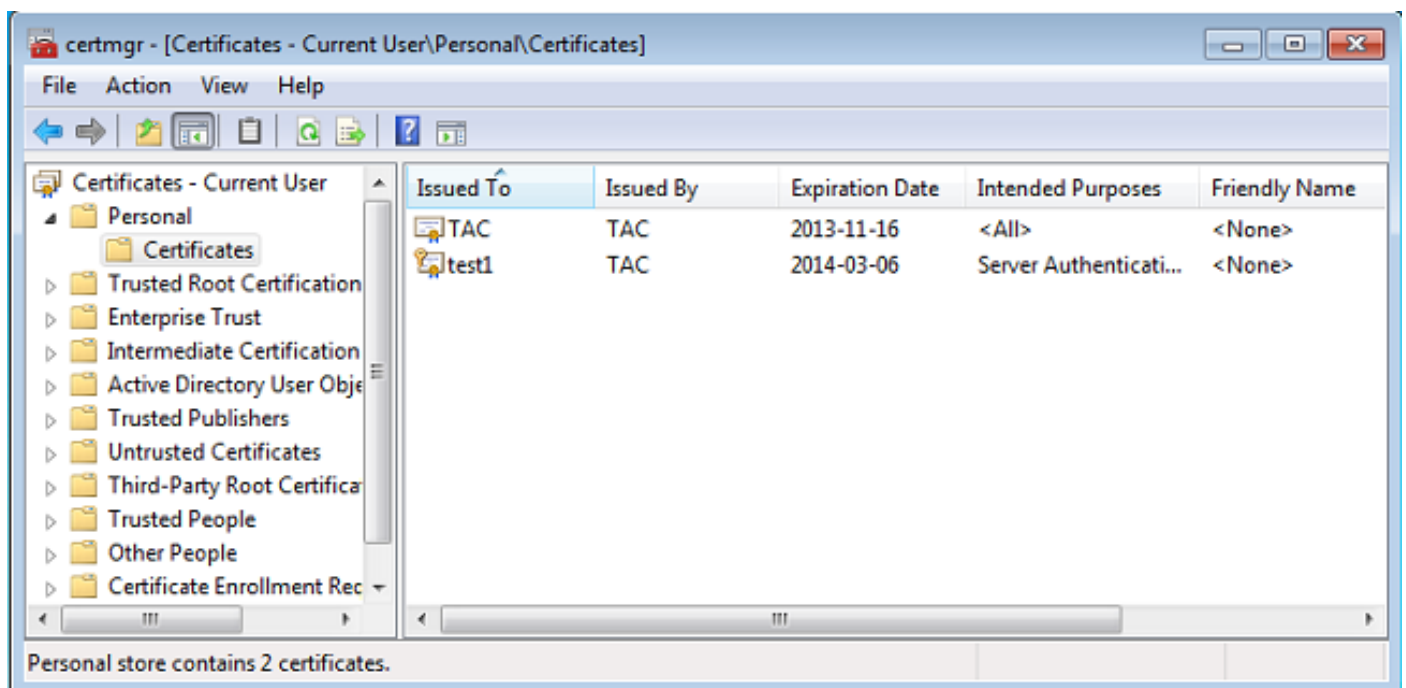
## 配置

**注意：**使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

## AnyConnect的证书

为了安装示例证书，请双击anyconnect.pfx文件，并且安装该证书作为个人证书。

请使用认证管理器(certmgr.msc)为了验证安装：



默认情况下，AnyConnect在Microsoft用户存储设法查找一证书;没有需要做AnyConnect配置文件的所有变动。

## ASA的认证安装

此示例显示ASA如何能导入base64 PKCS-12证书：

```
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:
MIIJAQIBAzCCCMcGCSqGSIb3DQEHAaCCCLgEggi0MIIIIsDCCBa8GCSqGSIb3DQEH
...
<output ommitted>
...
83EwMTAhMAKGBSsOAwIaBQAEFCS/WBSkrOIeTlHARHbLF1FFQvSvBAhu0j9bTtZo
3AICCAA=
quit
```

**INFO: Import PKCS12 operation completed successfully**

请使用**show crypto ca certificates**命令为了验证导入：

```
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](#) ( [仅限注册用户](#) ) 支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

## 单个验证和证书确认的ASA配置

ASA使用验证、授权和统计(AAA)验证和证书验证。证书确认是必须。AAA认证使用一个本地数据库。

此示例显示与证书确认的单个验证。

```
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

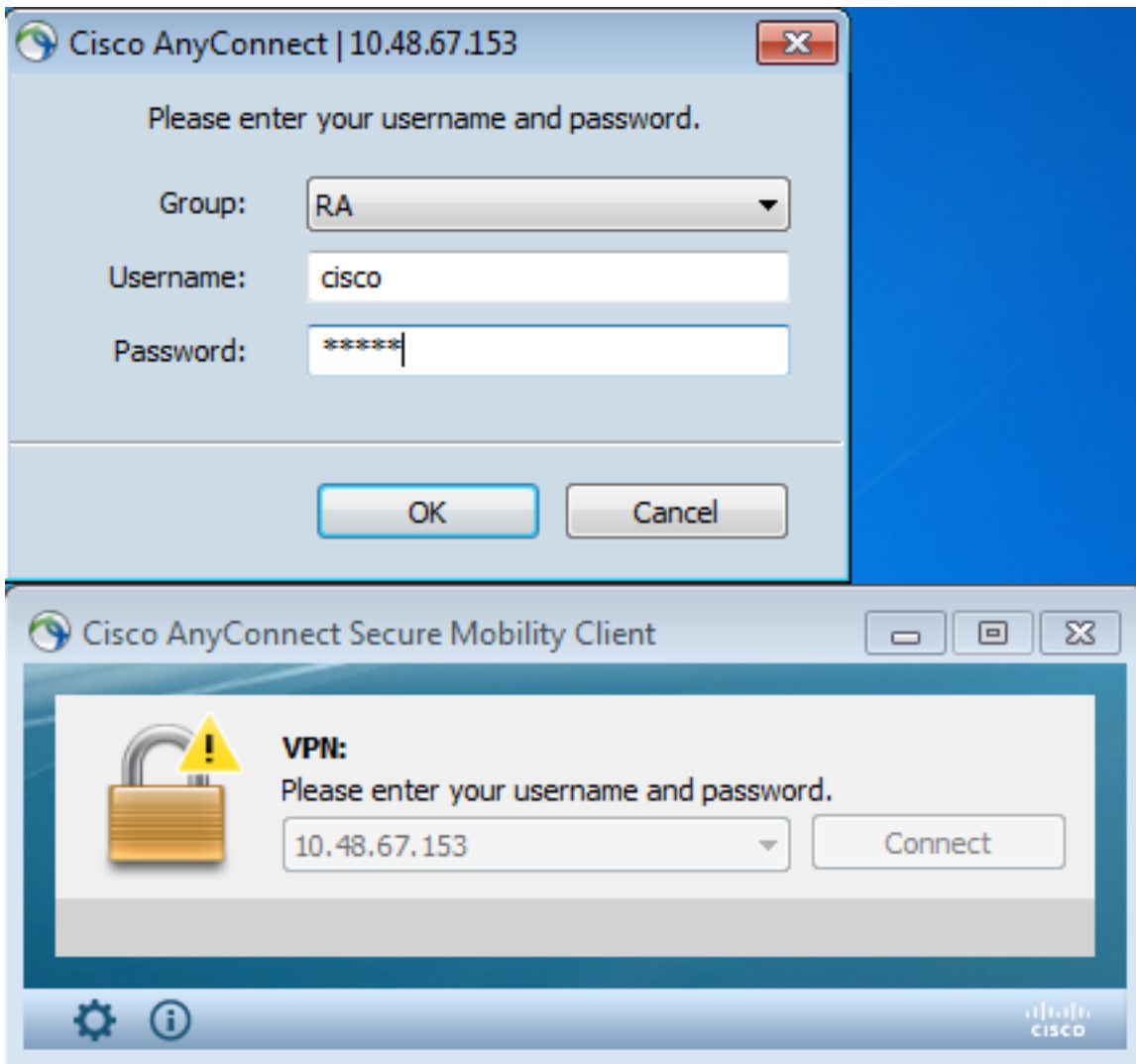
tunnel-group RA type remote-access
tunnel-group RA general-attributes
  authentication-server-group LOCAL
  default-group-policy Group1
  authorization-required
tunnel-group RA webvpn-attributes
  authentication aaa certificate
  group-alias RA enable
```

除此配置之外，是可能的执行轻量级目录访问协议(LDAP)授权与从一个特定证书字段的用户名，例如验证名称(CN)。另外的属性可能然后获取和应用到VPN会话。关于验证和证书授权的更多信息，参考“[ASA Anyconnect VPN和与自定义模式和证书配置示例的OpenLDAP授权](#)”。

## 测验

**注意：** [命令输出解释程序工具](#) ( [仅限注册用户](#) ) 支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

为了测试此配置，请提供本地凭证(用户名cisco用密码cisco)。证书一定存在：



输入显示vpn-sessiondb详细信息anyconnect on命令ASA :

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

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

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

```
AnyConnect-Parent:
Tunnel ID      : 10.1
Public IP      : 10.147.24.60
Encryption     : none
TCP Dst Port   : 443
TCP Src Port   : 62531
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](#)。

在本例中，证书在数据库未被缓存，找到了对应的CA，使用了正确密钥用法 (ClientAuthentication)，并且证书顺利地验证：

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

详细的调试指令，例如**debug webvpn 255**命令，在ASA能生成许多登录生产环境和放置重载。一些WebVPN调试为了清晰删除：

```
CERT_API: Authenticate session 0x0934d687, non-blocking cb=0x0000000012cfc50
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
这是尝试找到一匹配的隧道群。没有特定证书映射规则，并且您提供使用的隧道群：
```

```
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)
这些是SSL和全体会议调试：
```

```
%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.
```

## 双重身份验证和证书确认的ASA配置

这是双重身份验证示例，主要的认证服务器是本地，并且附属认证服务器是LDAP。证书确认仍然启用。

此示例显示IDAP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
```

这是一个附属认证服务器的新增内容：

```
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
```

因为它是默认设置，您看不到‘验证服务器组本地’在配置里。

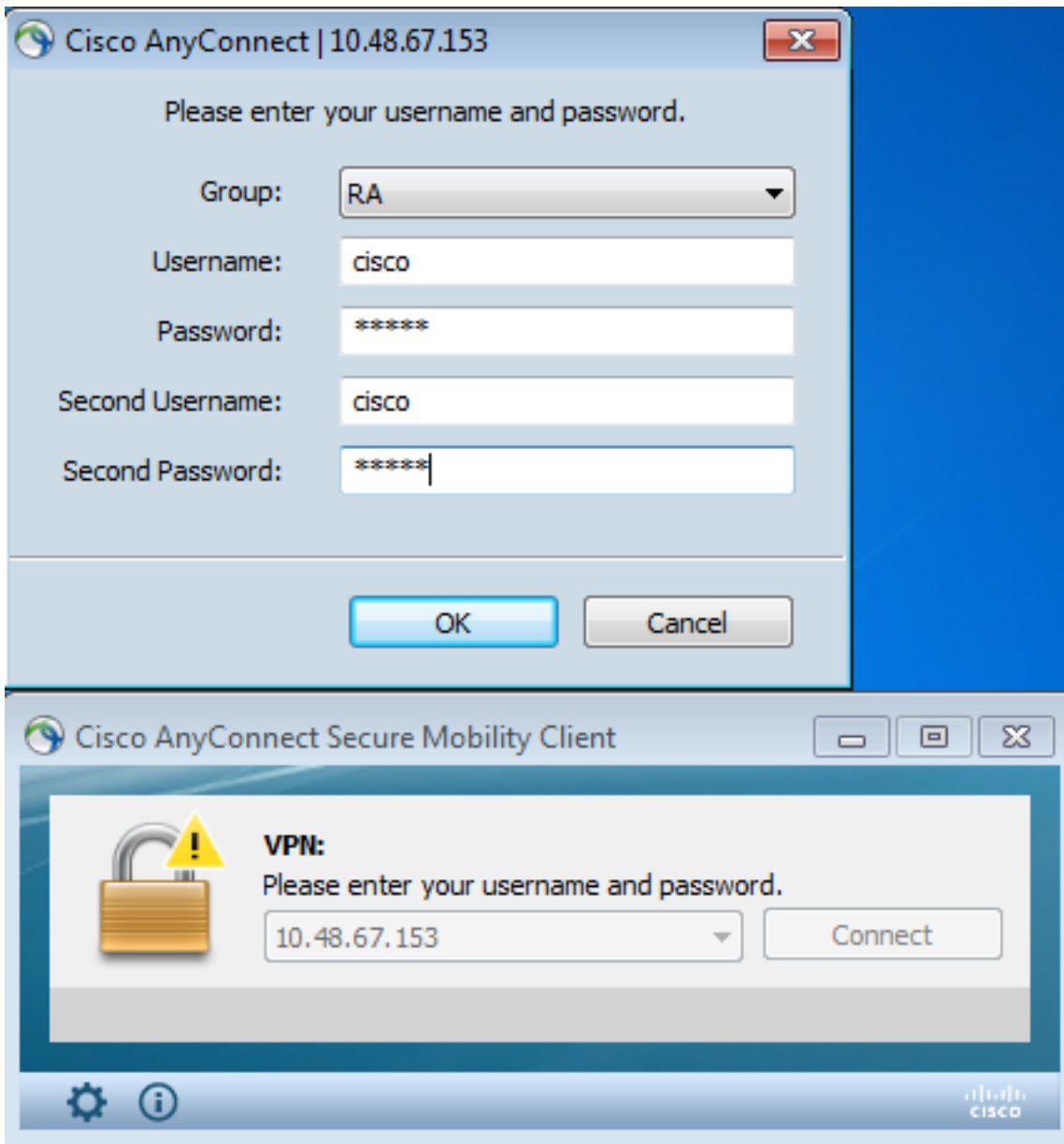
所有其他AAA服务器可以用于‘验证服务器组’。对于‘第二验证服务器组’，使用所有AAA服务器除了Security Dynamics International (SDI)是可能的服务器;在那种情况下，SDI能仍然是主要的认证服务器。

## 测验

**注意：** [命令输出解释程序工具](#) ( [仅限注册用户](#) ) 支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

为了测试此配置，请提供本地凭证(用户名cisco用密码cisco)和LDAP凭证(用户名cisco用从LDAP的密码)。证书一定存在：





输入显示vpn-sessiondb详细信息anyconnect on命令ASA。

结果类似于那些为单个验证。[单个验证和证书确认](#) 参考的“[ASA配置，测验](#)”。

## 调试

WebVPN会话的调试和验证是类似的。[单个验证和证书确认](#) 参考的“[ASA配置，调试](#)”。一另外的认证过程出现：

```
%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的调试显示也许随LDAP配置变化的详细信息：

```
[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 = jsmith@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

```

## 双重身份验证和预先充满的ASA配置

映射某些证书字段到使用主要的和附属验证的用户名是可能的：

```

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。

对于主要的验证，用户名从CN被采取，是本地用户'test1'为什么创建。

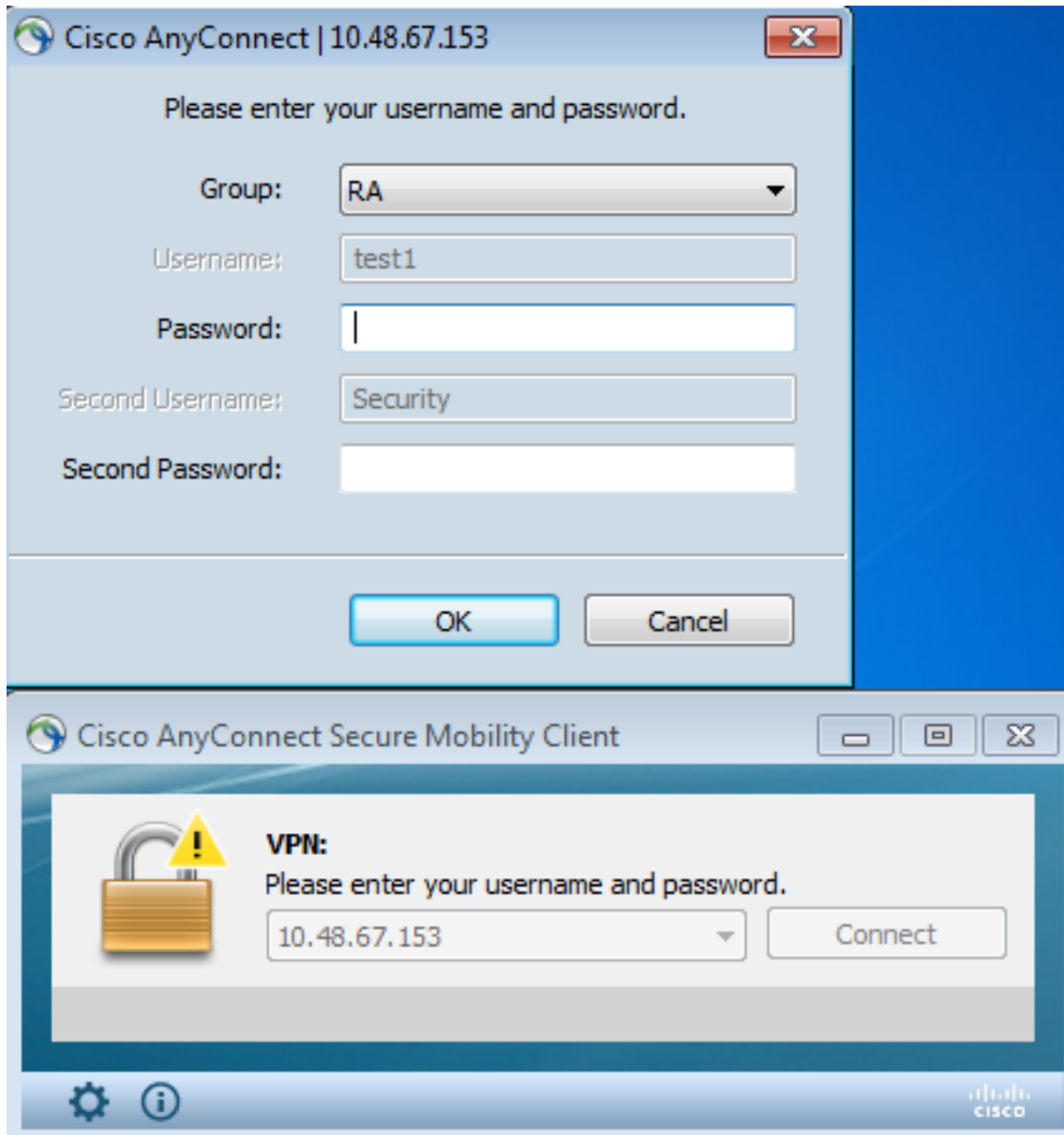
对于附属验证，用户名从组织单位(OU被采取，是用户'安全'为什么在LDAP服务器创建。

强制AnyConnect使用预先充满命令为了预先填入主要的和附属用户名也是可能的。

在真实世界方案中，主要的认证服务器通常是AD或LDAP服务器，而附属认证服务器是使用令牌的密码的Rivest、沙米尔和Adelman (RSA)服务器。在此方案中，用户必须提供用户认识的AD/LDAP凭证(用户有)的RSA令牌的密码(和使用)的证书(在计算机)。

## 测验

注意到您不能更改主要的或附属用户名，因为从证书CN和OU字段被预先填入：



## 调试

此示例显示预先充满请求发送对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]
```

您看到验证使用正确用户名：

```
%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
```

## 双重身份验证和证书映射的ASA配置

映射特定客户端证书对特定隧道群，如此示例所显示，也是可能的：

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

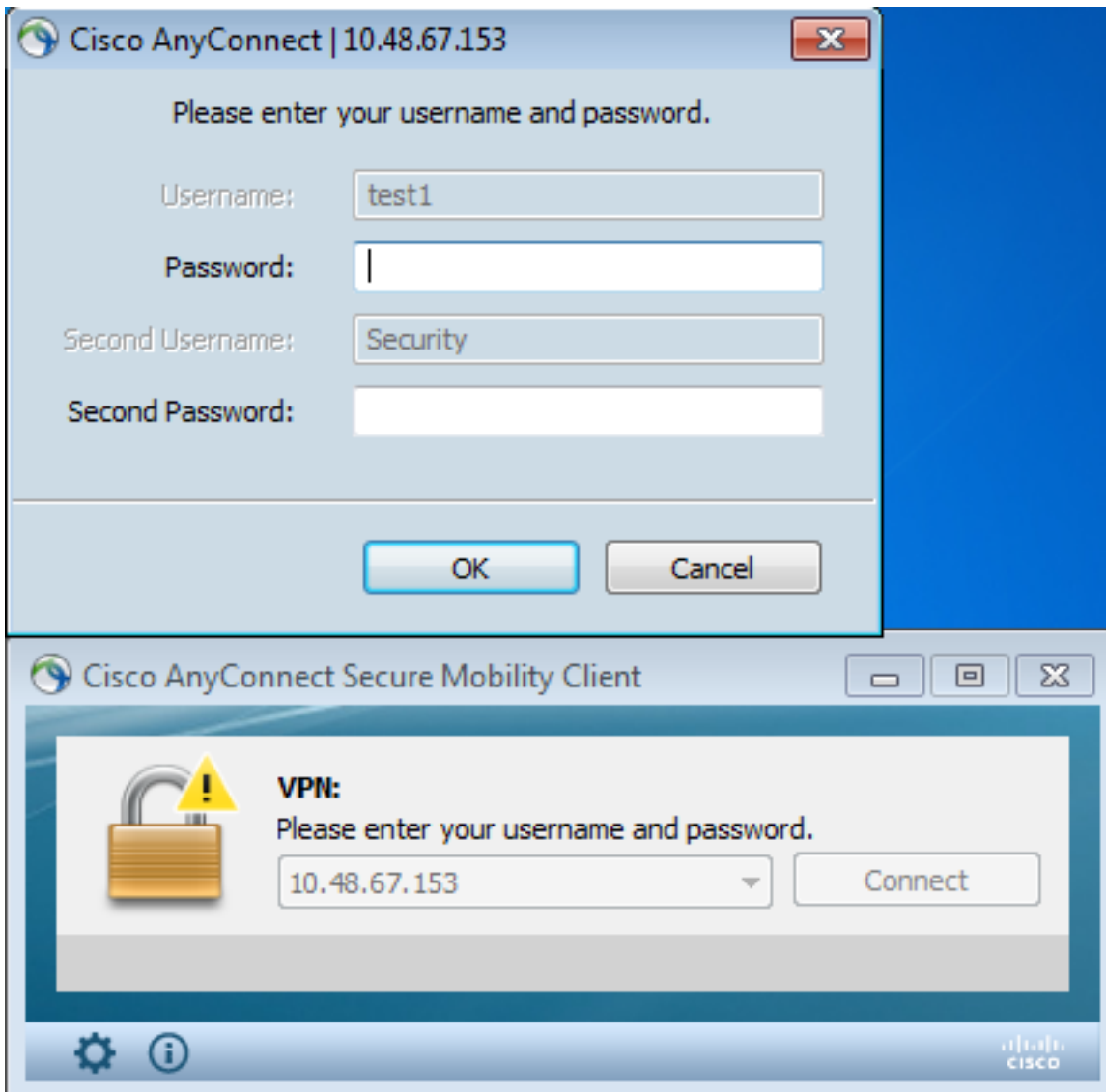
```
webvpn
  certificate-group-map CERT-MAP 10 RA
```

这样，Cisco技术支持中心(TAC) CA签字的所有用户证书被映射给隧道群名为'RA'。

**注意：**SSL的证书映射跟IPsec的证书映射不同地配置。使用'在全局配置模式的通道组MAP'规则对于IPsec，它配置。使用'证书组MAP'在WebVPN配置模式下，对于SSL，它配置。

## 测验

注意到，一旦证书映射启用，您不需要再选择隧道群：



## 调试

在本例中，证书映射规则准许隧道群将找到：

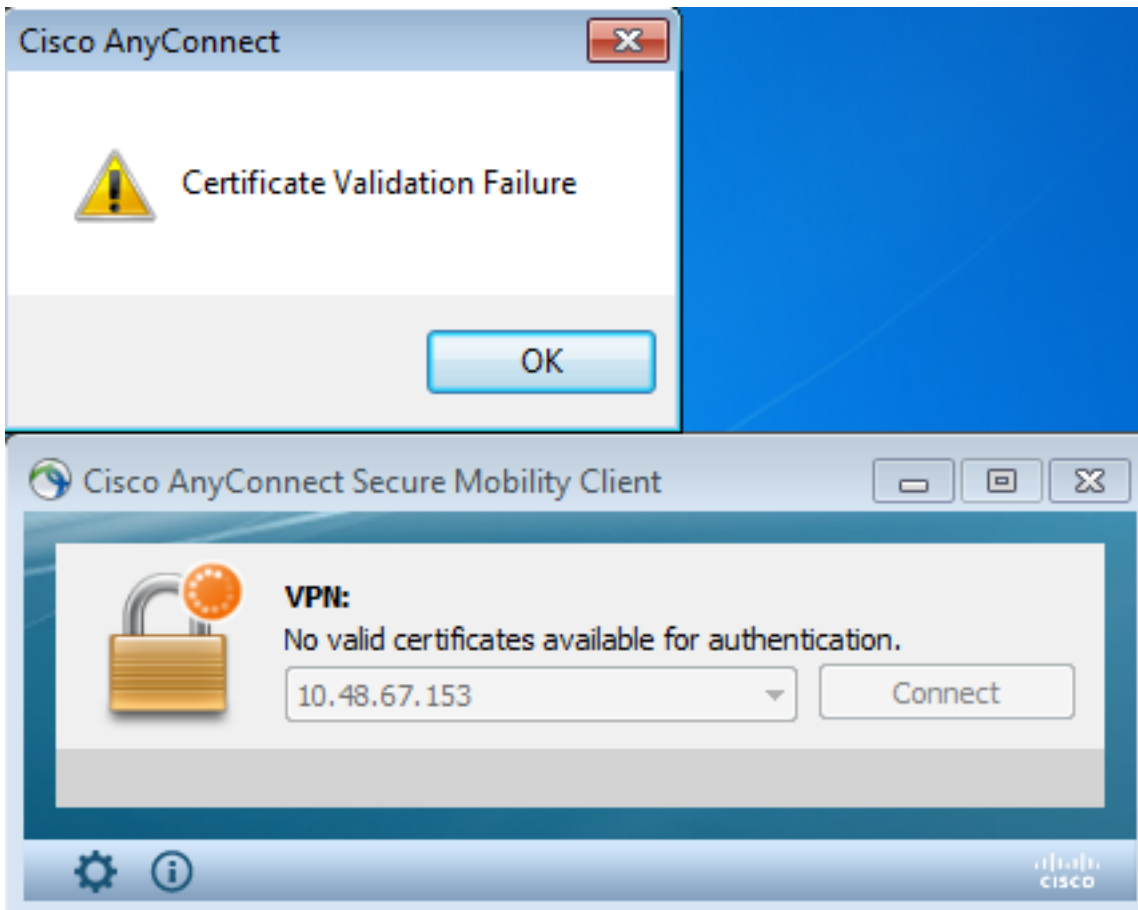
```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1, ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.  
%ASA-7-717038: Tunnel group match found.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

### 不现在的有效证书

在您从Windows7后删除有效证书，AnyConnect找不到所有有效证书：



在ASA，它看起来象会话由客户端(重置我)终止：

```
%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

- [配置通道Groups，组策略和用户：配置双重身份验证](#)
- [配置安全工具用户授权的一个外部服务器](#)
- [技术支持和文档 - Cisco Systems](#)