# 配置ASA AnyConnect安全移動客戶端身份驗證

目錄 簡介 必要條件 <u>需求</u> <u>採用元件</u> <u>背景資訊</u> 設定 <u>AnyConnect證書</u> ASA上的證書安裝 <u>用於單一身份驗證和證書驗證的ASA配置</u> 測試 偵錯 <u>用於雙重身份驗證和證書驗證的ASA配置</u> <u>測試</u> <u> 偵錯</u> <u>用於雙重身份驗證和預填充的ASA配置</u> <u>測試</u> <u> 偵錯</u> <u>用於雙重身份驗證和證書對映的ASA配置</u> 測試 偵錯 <u>疑難排解</u> 有效證書不存在 相關資訊

## 簡介

本文檔介紹使用證書驗證的雙身份驗證的ASA AnyConnect安全移動客戶端訪問的配置。

## 必要條件

## 需求

思科建議您瞭解以下主題:

- ASA命令列介面(CLI)配置和安全套接字層(SSL)VPN配置的基本知識
- X509證書的基本知識

## 採用元件

本檔案中的資訊是根據以下軟體版本:

- Cisco Adaptive Security Appliance(ASA)軟體8.4版及更高版本
- Windows 7和Cisco AnyConnect安全移動客戶端3.1

假設您使用外部憑證授權單位(CA)來產生:

- 用於ASA的公鑰加密#12準證書(PKCS #12)base64編碼證書(AnyConnect.pfx)
- 用於AnyConnect#12PKCS證書

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

## 背景資訊

本文檔介紹自適應安全裝置(ASA)Cisco AnyConnect安全移動客戶端訪問的配置示例,該配置使用 帶證書驗證的雙重身份驗證。作為AnyConnect使用者,您必須提供主身份驗證和輔助身份驗證的正 確證書和憑據才能獲得VPN訪問許可權。本文還提供使用預填充功能的證書對映示例。

## 設定

N註:使用命令查詢工具可獲取本節所用命令的詳細資訊。只有註冊的思科使用者才能訪問內 部思科工具和資訊。

## AnyConnect證書

若要安裝示例證書,請按兩下AnyConnect.pfx檔案,並將該證書安裝為個人證書。

使用證書管理器(certmgr.msc)驗證安裝:

🚡 certmgr - [Certificates - Current User\Personal\Certificates]					
File Action View Help					
🙀 Certificates - Current User	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
A Personal	TAC	TAC	2013-11-16	<all></all>	<none></none>
Certificates	🛱 test1	TAC	2014-03-06	Server Authenticati	<none></none>
Enterprise Trust					
Intermediate Certification					
Active Directory User Obje					
Trusted Publishers					
Untrusted Certificates					
Third-Party Root Certifica					
Trusted People					
Other People					
👂 🚞 Certificate Enrollment Rec 👻					
	•				F.
Personal store contains 2 certificates.					

預設情況下,AnyConnect嘗試在Microsoft使用者儲存區中找到證書。無需對AnyConnect配置檔案

進行任何更改。

ASA上的證書安裝

此示例顯示ASA如何匯入base64 PKCS #12證書:

<#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: MIIJAQIBAzCCCMcGCSqGSIb3DQEHAaCCCLgEggiOMIIIsDCCBa8GCSqGSIb3DQEH ... <output ommitted> ... 83EwMTAhMAkGBSsOAwIaBQAEFCS/WBSkrOIeT1HARHbLF1FFQvSvBAhu0j9bTtZo 3AICCAA= quit

INFO: Import PKCS12 operation completed successfully

使用show crypto ca certificates命令以驗證匯入:

```
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
    1=Warsaw
    st=Maz
    c=PL
 Subject Name:
    cn=TAC
    ou=RAC
    o=TAC
   1=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=I0S ou=UNIT o=TAC ]=₩a 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

◇ 附註:<u>輸出直譯器工具</u>支援某些show命令。使用「輸出直譯器」工具可檢視show命令輸出的 分析。只有已註冊的思科使用者才能訪問內部思科工具和資訊。

## 用於單一身份驗證和證書驗證的ASA配置

ASA同時使用身份驗證、授權和記帳(AAA)身份驗證和證書身份驗證。證書驗證是必需的。AAA身 份驗證使用本地資料庫。

此範例顯示具有憑證驗證的單一驗證。

```
<#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,還可以使用來自特定證書欄位(例如證書名稱(CN))的使用者名稱執行輕量級目錄 訪問協定(LDAP)授權。 然後可以檢索其他屬性並將其應用於VPN會話。有關身份驗證和證書授權 的詳細資訊,請參閱<u>使用自定義架構和證書的ASA AnyConnect VPN和OpenLDAP授權配置示例</u>。

### 測試

✤ 附註:<u>輸出直譯器工具</u>支援某些show命令。使用「輸出直譯器」工具可檢視show命令輸出的 分析。只有已註冊的思科使用者才能訪問內部思科工具和資訊。

為了測試此組態,請提供本機憑證(使用者名稱cisco和密碼cisco)。 證書必須存在:

S Cisco AnyConnect   10.48.67.153			
Please enter your username and password.			
Group:	RA		
Username:	cisco		
Password:	****		
	OK Cancel		
Sisco AnyConi	nect Secure Mobility Client 🔲 🖾		
VPN:         Please enter your username and password.         10.48.67.153         Connect			
<b>Ö</b> ()	alialia cisco		

在ASA上輸入show vpn-sessiondb detail AnyConnect命令:

## <#root>

License

Encryption

: RC4 AES128

```
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
           : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
Protocol
           : AnyConnect Premium
```

Hashing

: none SHA1

Bytes Tx : 20150 Bytes Rx : 25199 : 192 Pkts Tx : 16 Pkts Rx Pkts Tx Drop : 0 Pkts Rx Drop : 0 Group Policy : Group1 Tunnel Group : RA Login Time : 10:16:35 UTC Sat Apr 13 2013 : 0h:01m:30s Duration Inactivity : 0h:00m:00s : Unknown NAC Result VLAN VLAN Mapping : N/A : 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 Pkts Rx : 8 : 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 - 1 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 Rx : 11 Pkts Tx : 4 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 Hashing Encryption : AES128 : SHA1 UDP Src Port : 52818 Encapsulation: DTLSv1.0 UDP Dst Port : 443 Auth Mode - 1 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: 0Pkts Rx: 177Pkts Tx Drop : 0Pkts Rx Drop : 0NAC:Reval Int (T): 0 SecondsSQ Int (T): 0 SecondsHold Left (T): 0 SecondsRedirect URL :

### 偵錯

💊 附註:使用 debug 指令之前,請先參閱<u>有關 Debug 指令的重要資訊。</u>

在本例中,未在資料庫中快取證書。已找到對應的CA,已使用正確的金鑰用法 (ClientAuthentication),且已成功驗證憑證:

<#root>

debug aaa authentication debug aaa authorization debug webvpn 255

debug webvpn AnyConnect 255

debug crypto ca 255

詳細的debug命令(如debug webvpn 255命令)可以在生產環境中生成許多日誌,並給ASA帶來沈重 負擔。為清楚起見,某些WebVPN調試已刪除:

#### <#root>

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

#### 這是查詢匹配隧道組的嘗試。沒有特定憑證對映規則,且使用您提供的通道組:

#### <#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和常規會話調試:

#### <#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,1=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,
1=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,1=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,
1=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.
```

## 用於雙重身份驗證和證書驗證的ASA配置

以下是雙重身份驗證的示例,其中主身份驗證伺服器是LOCAL,輔助身份驗證伺服器是LDAP。證 書驗證仍然啟用。

此示例顯示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
```

#### 以下是新增的輔助驗證伺服器:

#### <#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

您在配置中未看到authentication-server-group LOCAL,因為它是預設設定。

任何其他AAA伺服器都可以用於authentication-server-group。對於secondary-authenticationserver-group,可以使用Security Dynamics International(SDI)伺服器以外的所有AAA伺服器。在這 種情況下,SDI仍可能是主身份驗證伺服器。

### 測試

N註:<u>輸出直譯器工具</u>支援某些show命令。使用「輸出直譯器」工具可檢視show命令輸出的 分析。只有已註冊的思科使用者才能訪問內部思科工具和資訊。

為了測試此配置,請提供本地憑據(使用者名稱cisco和密碼cisco)和LDAP憑據(使用者名稱

S Cisco AnyConnect   10.48.67.153				
Please enter your username and password.				
Group:	RA			
Username:	cisco			
Password:	****			
Second Username:	cisco			
Second Password:	*****			
	OK Cancel			
Scisco AnyConnect S	Secure Mobility Client			
VPN:         Please enter your username and password.         10.48.67.153				
<b>\$</b> (i)	al tal ta cisco			

在ASA上輸入show vpn-sessiondb detail AnyConnect命令。

結果與單一身份驗證的結果相似。請參閱ASA配置以瞭解單一身份驗證和證書驗證,測試。

偵錯

WebVPN會話的調試和身份驗證類似。請參閱ASA配置以瞭解單一身份驗證和證書驗證,調試。出 現一個額外的身份驗證過程:

#### <#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調試顯示因LDAP配置而異的詳細資訊:

```
[34] Session Start
[34] New request Session, context 0 \times 00007 \text{ff} d8 d7 dd828, 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:
       cn: value = John Smith
[34]
        givenName: value = John
[34]
       sn: value = cisco
[34]
[34]
       uid: value = cisco
       uidNumber: value = 10000
[34]
       gidNumber: value = 10000
[34]
[34]
       homeDirectory: value = /home/cisco
       mail: value = name@dev.local
[34]
[34]
       objectClass: value = top
        objectClass: value = posixAccount
[34]
[34]
        objectClass: value = shadowAccount
        objectClass: value = inetOrgPerson
[34]
[34]
        objectClass: value = organizationalPerson
        objectClass: value = person
[34]
        objectClass: value = CiscoPerson
[34]
        loginShell: value = /bin/bash
[34]
        userPassword: value = {SSHA}pndf5sfjscTPuyrhL+/QUqhK+i1UCUTy
[34]
[34] Fiber exit Tx=315 bytes Rx=911 bytes, status=1
[34] Session End
```

## 用於雙重身份驗證和預填充的ASA配置

可以將某些證書欄位對映到用於主身份驗證和輔助身份驗證的使用者名稱:

```
<#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
```

在本範例中,使用者端使用憑證:cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL。

對於主要身份驗證,使用者名稱取自CN,這就是建立本地使用者test1的原因。

對於輔助身份驗證,使用者名稱從組織單位(OU)獲取,這就是在LDAP伺服器上建立使用者安全的 原因。

也可以強制AnyConnect使用預填充命令來預填充主要和輔助使用者名稱。在真實情況下,主要身份 驗證伺服器通常是AD或LDAP伺服器,而輔助身份驗證伺服器是使用令牌密碼的Rivest、Shamir和 Adelman(RSA)伺服器。在此方案中,使用者必須提供AD/LDAP憑證(使用者知道)、RSA令牌密 碼(使用者擁有)和證書(在使用機器上)。

#### 測試

請注意,您無法更改主要或次要使用者名稱,因為它是從證書CN和OU欄位預填充的:

N Cisco AnyConnect   10.48.67.153				
Please enter your username and password.				
Group:	RA			
Username:	test1			
Password:	1			
Second Username:	Security			
Second Password:				
-	OK Cancel			
Sisco AnyConnect	Secure Mobility Client			
VPN:         Please enter your username and password.         10.48.67.153				
<b>\$</b> (i)		altalta cisco		

## 偵錯

此示例顯示傳送到AnyConnect的預填充請求:

%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]

#### 此處您看到身份驗證使用正確的使用者名稱:

<#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

## 用於雙重身份驗證和證書對映的ASA配置

也可以將特定客戶端證書對映到特定隧道組,如以下示例所示:

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

webvpn

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

如此一來,所有由思科技術協助中心(TAC)CA簽署的使用者憑證都會對應到名為「RA」的通道群組 。

◇ 附註:SSL的證書對映的配置與IPsec的證書對映的配置不同。對於IPsec,它在全域性配置模 式下配置了「tunnel-group-map」規則。對於SSL,在webvpn配置模式下配置為「certificategroup-map」。

測試

請注意,一旦啟用憑證對應,就不再需要選擇通道群組:

S Cisco AnyConnect   10.48.67.153				
Please enter y	our username and password.			
Username:	test1			
Password:				
Second Username:	Security			
Second Password:				
	OK Cancel			
Sisco AnyConnect	Secure Mobility Client			
VPN:         Please enter your username and password.         10.48.67.153				
<b>‡</b> ()		alialia cisco		

## 偵錯

在本例中,證書對映規則允許找到隧道組:

#### <#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.
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

有效證書不存在

從Windows7中刪除有效證書後,AnyConnect找不到任何有效證書:

Cisco AnyConnec	t 💌	
🔔 Certifi	cate Validation Failure	
	ОК	
Sisco AnyCor	nnect Secure Mobility Client	
	VPN: No valid certificates available fo 10.48.67.153	or authentication.
<b>\$</b> (i)		cisco

在ASA上,會話似乎由客戶端終止(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

## 相關資訊

- <u>配置隧道組、組策略和使用者: 配置雙重身份驗證</u>
- 為安全裝置使用者授權配置外部伺服器
- <u>思科技術支援與下載</u>

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。