与OCSP验证的ASA远程访问VPN在Microsoft Windows 2012和Openssl下

目录

简介

本文描述如何使用在思科可适应安全工具(ASA)的联机证书状态协议(OCSP)验证VPN用户提交的证书。(Microsoft Windows认证机关[CA]和Openssl)提交两个OCSP服务器的配置示例。Verify部分描述在数据包级别上的详细的流，并且Troubleshoot部分着重典型的错误和问题。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco可适应安全工具命令行界面(CLI)配置和安全套接字层SSL VPN配置
- X.509证书
- MS Windows服务器
- Linux/Openssl

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco可适应安全工具软件，版本8.4和以上
- 有Cisco AnyConnect安全移动客户端的Microsoft Windows 7，版本3.1
- Microsoft服务器2012 R2
- 与Openssl 1.0.0j或以上的Linux

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

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。

网络图

客户端使用远程访问VPN。此访问可以是Cisco VPN Client (IPSec)， Cisco AnyConnect安全移动性(SSL/Internet密钥交换版本2 [IKEv2])，或者WebVPN (门户)。为了登陆，客户端提供在ASA配置本地的正确证书，以及用户名/密码。客户端证书通过OCSP服务器验证。

与OCSP的ASA远程访问

ASA为SSL访问配置。客户端使用AnyConnect为了登陆。ASA使用简单认证登记协议(SCEP)为了请求证书：

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.147.25.80:80/certsrv/mscep/mscep.dll

crypto ca certificate map MAP 10
 subject-name co administrator
```

subject-name包含词管理员的证书地图创建为了识别所有用户(不区分的案件)。那些用户一定给隧道群名为RA ：

```
webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.1.02040-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
 certificate-group-map MAP 10 RA
```

VPN配置要求成功的授权(即一验证的证书)。它也要求本地定义的用户名的(验证aaa)正确凭证：

```
username cisco password xxxxxxx
ip local pool POOL 192.168.11.100-192.168.11.105 mask 255.255.255.0

aaa authentication LOCAL
aaa authorization LOCAL

group-policy MY internal
group-policy MY attributes
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client ssl-clientless

tunnel-group RA type remote-access
tunnel-group RA general-attributes
 address-pool POOL
 default-group-policy MY
 authorization-required
tunnel-group RA webvpn-attributes
 authentication aaa certificate
 group-alias RA enable
```

Microsoft Windows 2012 CA

> **注意**：使用CLI， 8.4和8.6，请参阅Cisco ASA 5500系列配置指南：配置安全工具用户授权的一个外部服务器关于在ASA的配置的详细信息通过CLI。

服务安装

此步骤描述如何配置角色Microsoft服务器的服务：

1. 导航给**服务器管理器>管理>**Add**角色和功能**。Microsoft服务器需要这些角色服务：

   证书颁发机构证书颁发机构Web登记，客户端使用联机响应方，为OCSP是需要的网络设备登记服务，包含SCEP应用程序由ASA使用了 与策略的若需要网站服务可以被添加。

2.
3.
4. 当您添加功能时，请务必包括联机响应方工具，因为使用的以后的它包括OCSP管理单元：

OCSP模板的CA配置

OCSP服务使用一证书签署OCSP答复。必须生成在Microsoft服务器的一特殊证书并且必须包括：

- 延长密钥用法= OCSP签字

- OCSP没有撤销检查

此证书是需要的为了防止OCSP验证环路。ASA不使用OCSP服务设法检查OCSP服务提交的证书。

1. 添加证书的一个模板在CA.导航对**CA >认证模板>管理**，**签字**挑选**OCSP的答复**，并且复制模板。查看新建立的模板的属性，并且点击**安全选项卡**。权限描述哪个实体允许请求使用该模板的证书，因此正确权限要求。在本例中，实体是在同一台主机的OCSP服务(TEST-CISCO \ DC)运作，并且OCSP服务需要自动登记权限：

   模板的其他设置可以设默认。

2. 激活模板。导航对**CA >认证模板发出**和选择重复的模板的>New **>认证模板**：

OCSP服务证书

此步骤描述如何使用联机配置管理为了配置OCSP ：

1. 导航到**服务器管理器>工具**。
2. 导航对**撤销Configuration>添加撤销配置**为了添加一新的配置：

   OCSP能使用同样企业CA。OCSP服务的证书生成。

3. 请使用选定企业CA，并且选择创建的模板前。证书自动地被登记：

4. 确认证书被登记，并且其状态是Working/OK ：

5. 导航对**CA >已签发证书**为了验证证书详细信息：

OCSP服务目前

OCSP的Microsoft实施与RFC 5019是兼容的大容积环境的轻量级联机证书状态协议(OCSP)配置文件，是RFC 2560 X.509互联网公共钥匙结构联机证书状态协议简化版本- OCSP。

OCSP的ASA用途RFC 2560。其中一在两个RFC的差异是RFC 5019不接受ASA发送的签字的请求。

迫使Microsoft OCSP服务接受那些签字的请求和回复与正确签字的答复是可能的。导航对**撤销Configuration> RevocationConfiguration1** > Edit Properties，并且选择选项**启用NONCE分机支持**。

OCSP服务当前是立即可用的。

虽然思科不推荐此，目前在ASA可以禁用：

```
BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce
```

OCSP扩展的CA配置

您在所有已签发证书必须当前重新配置CA包括OCSP服务器分机。当证书验证时， ASA用于从该分机的URL为了连接到OCSP服务器。

1. 打开服务器的Properties对话框在CA。
2. 点击**扩展**选项卡。指向OCSP服务的权限信息存取(AIA)分机是需要的;在本例中，它是http://10.61.208.243/ocsp。启用AIA分机的这两个选项：

   包括在已签发证书AIA分机包括在联机证书状态协议(OCSP)分机

   这保证所有已签发证书有指向OCSP服务的一正确分机。

Openssl

> **注意**：使用CLI， 8.4和8.6，请参阅Cisco ASA 5500系列配置指南：配置安全工具用户授权的一个外部服务器关于在ASA的配置的详细信息通过CLI。

此示例假设， Openssl服务器已经配置。此部分描述为CA配置是需要的仅的OCSP配置和更改。

此步骤描述如何生成OCSP证书：

1. 这些参数为OCSP响应方是需要的：

   ```
   BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce
   ```
2. 这些参数为用户证书是需要的：

   ```
   BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce
   ```
3. 证书需要由CA生成和签字。
4. 启动OCSP服务器：

   ```
   BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce
   ```
5. 测试示例证书：

   ```
   BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce
   ```

更多示例在Openssl网站可以找到。

Openssl，类似ASA，支持OCSP目前;目前可以控制与使用-目前和- no_nonce交换机。

与多OCSP来源的ASA

ASA能改写OCSP URL。即使客户端证书包含OCSP URL，由在ASA的配置覆盖：

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 ocsp url http://10.10.10.10/ocsp
```

OCSP服务器地址可以明确地定义。此example命令匹配与管理员的所有证书主题名称的，使用OPENSSL信任点为了验证OCSP签名，并且使用http://11.11.11.11/ocsp URL为了发送请求：

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 match certificate MAP override ocsp trustpoint OPENSSL 10 url
http://11.11.11.11/ocsp

crypto ca certificate map MAP 10
 subject-name co administrator
```

用于的命令查找OCSP URL是：

1. OCSP服务器您与**certificate命令的匹配的**集
2. OCSP服务器您集用**ocsp url**命令
3. OCSP服务器在客户端证书的AIA字段

与不同的CA签字的OCSP的ASA

OCSP答复可以由不同的CA.在这种情况下签字，它是必要使用**certificate命令的匹配**为了使用在ASA的一不同的信任点OCSP证书确认。

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 match certificate MAP override ocsp trustpoint OPENSSL 10 url
http://11.11.11.11/ocsp

crypto ca certificate map MAP 10
 subject-name co administrator

crypto ca trustpoint OPENSSL
enrollment terminal
revocation-check none
```

在本例中， ASA使用OCSP URL重写所有证书与包含管理员的subject-name。ASA被迫验证OCSP响应方证书另一信任点， OPENSSL。用户证书在WIN2012信任点仍然验证。

因为OCSP响应方证书有'OCSP没有检查'分机的撤销，证书没有验证，既使当OCSP被迫验证OPENSSL信任点。

默认情况下，当ASA尝试验证用户证书时，所有信任点被搜索。OCSP响应方证书的验证不同的。ASA搜索为用户证书仅的信任点(在本例中的WIN2012已经被找到)。

因此，是必要的使用**certificate命令的匹配**为了强制ASA使用一不同的信任点OCSP证书确认(在本例

中的OPENSSL)。

用户证书验证第一匹配的信任点(在本例中的WIN2012)，然后确定OCSP响应方验证的默认信任点。

如果特定信任点在**certificate命令的匹配没有**提供， OCSP证书验证信任点和用户证书(在本例中的WIN2012一样)。：

```
crypto ca trustpoint WIN2012
 revocation-check ocsp
 enrollment url http://10.61.209.83:80/certsrv/mscep/mscep.dll
 match certificate MAP override ocsp 10 url http://11.11.11.11/ocsp
```

验证

使用本部分可确认配置能否正常运行。

> **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。

ASA -通过SCEP获得证书

此步骤描述如何通过使用SCEP获取证书：

1. 这是获得CA证书的信任点认证过程：

```
debug crypto ca
debug crypto ca messages
debug crypto ca transaction

BSNS-ASA5510-3(config-ca-crl)# crypto ca authenticate WIN2012
Crypto CA thread wakes up!

CRYPTO_PKI: Sending CA Certificate Request:
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=
WIN2012 HTTP/1.0
Host: 10.61.209.83

CRYPTO_PKI: http connection opened

INFO: Certificate has the following attributes:
Fingerprint:     27dda0e5 e1ed3f4c e3a2c3da 6d1689c2
Do you accept this certificate? [yes/no]:

% Please answer 'yes' or 'no'.
Do you accept this certificate? [yes/no]:
yes

Trustpoint CA certificate accepted.
```

2. 为了请求证书， ASA需要有可以从http://IP/certsrv/mscep_admin的admin控制台得到的一个一次性SCEP密码：

3. 请使用该密码请求在ASA的证书：

```
BSNS-ASA5510-3(config)# crypto ca enroll WIN2012
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the
configuration.
  Please make a note of it.
Password: ****************
Re-enter password: ****************


% The fully-qualified domain name in the certificate will be:
BSNS-ASA5510-3.test-cisco.com
% Include the device serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: JMX1014K16Y

Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
BSNS-ASA5510-3(config)#

CRYPTO_PKI: Sending CA Certificate Request:
GET /certsrv/mscep/mscep.dll/pkiclient.exe?operation=GetCACert&message=
WIN2012 HTTP/1.0
Host: 10.61.209.83

CRYPTO_PKI: http connection opened

CRYPTO_PKI: Found a subject match - inserting the following cert record
into certList若干输出为了清晰省略。
```

4. 验证CA和ASA证书：

```
BSNS-ASA5510-3(config)# show crypto ca certificates
Certificate
 Status: Available
 Certificate Serial Number: 240000001cbf2fc89f44fe819700000000001c
 Certificate Usage: General Purpose
 Public Key Type: RSA (1024 bits)
 Signature Algorithm: SHA1 with RSA Encryption
 Issuer Name:
   cn=test-cisco-DC-CA
   dc=test-cisco
   dc=com
 Subject Name:
    hostname=BSNS-ASA5510-3.test-cisco.com
   serialNumber=JMX1014K16Y
 CRL Distribution Points:
   [1]  ldap:///CN=test-cisco-DC-CA,CN=DC,CN=CDP,
CN=Public%20Key%20Services,CN=Services,CN=Configuration,
DC=test-cisco,DC=com?certificateRevocationList?base?objectClass=
cRLDistributionPoint
 Validity Date:
   start date: 11:02:36 CEST Oct 13 2013
   end   date: 11:02:36 CEST Oct 13 2015
 Associated Trustpoints: WIN2012

CA Certificate
```

```
Status: Available
Certificate Serial Number: 3d4c0881b04c799f483f4bbe91dc98ae
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
   cn=test-cisco-DC-CA
  dc=test-cisco
  dc=com
Subject Name:
  cn=test-cisco-DC-CA
  dc=test-cisco
  dc=com
Validity Date:
  start date: 07:23:03 CEST Oct 10 2013
  end   date: 07:33:03 CEST Oct 10 2018
Associated Trustpoints: WIN2012
```

ASA不显示大多证书扩展。即使ASA证书在AIA包含'OCSP URL'分机， ASA CLI不提交它。Cisco Bug ID CSCui44335 ， "ASA ENH显示的证书x509扩展"，请求此增强。

AnyConnect -通过网页获得证书

此步骤描述如何通过使用在客户端的Web浏览器获取证书：

1. AnyConnect用户证书可以通过网页请求。在客户端PC，请使用一Web浏览器努力去做CA在http:// *IP/certsrv* ：

2. 用户证书可以在Web浏览器存储保存，然后导出到Microsoft存储，由AnyConnect搜索。请使用certmgr.msc为了验证已接收证书：

   只要有一正确AnyConnect配置文件， AnyConnect能也请求证书。

与OCSP验证的ASA VPN远程访问

此步骤描述如何检查OCSP验证：

1. 当它尝试连接， ASA报道证书被检查OCSP。这里，签署证书的OCSP有一NO-检查分机和未通过OCSP被检查：

```
debug crypto ca
debug crypto ca messages
debug crypto ca transaction

%ASA-6-725001: Starting SSL handshake with client outside:
10.61.209.83/51262 for TLSv1 session.
%ASA-7-717025: Validating certificate chain containing 1 certificate(s).
%ASA-7-717029: Identified client certificate within certificate chain.
serial number: 240000001B2AD208B128116874000000000001B, subject name:
cn=Administrator,cn=Users,dc=test-cisco,dc=com.
Found a suitable trustpoint WIN2012 to validate certificate.
%ASA-7-717035: OCSP status is being checked for certificate. serial
```

```
number: 240000001B2AD208B1281168740000000001B, subject name:
cn=Administrator,cn=Users,dc=test-cisco,dc=com.
%ASA-6-302013: Built outbound TCP connection 1283 for outside:
10.61.209.83/80 (10.61.209.83/80) to identity:10.48.67.229/35751
(10.48.67.229/35751)
%ASA-6-717033: CSP response received.
%ASA-7-717034: No-check extension found in certificate. OCSP check
bypassed.
%ASA-6-717028: Certificate chain was successfully validated with
revocation status check.若干输出为了清晰省略。
```

2. 最终用户提供用户凭证：

3. VPN会话正确地完成：

```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps
for peer certificate with serial number:
240000001B2AD208B1281168740000000001B, subject name: cn=Administrator,
cn=Users,dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com.
%ASA-7-717038: Tunnel group match found. Tunnel Group: RA, Peer
certificate: serial number: 240000001B2AD208B1281168740000000001B,
subject name: cn=Administrator,cn=Users,dc=test-cisco,dc=com,
issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,dc=com.

%ASA-6-113012: AAA user authentication Successful : local database :
user = cisco
%ASA-6-113009: AAA retrieved default group policy (MY) for user = cisco
%ASA-6-113039: Group <MY> User <cisco> IP <10.61.209.83> AnyConnect parent
session started.
```

4. 会话创建：

```
BSNS-ASA5510-3(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username     : cisco                  Index        : 4
Assigned IP  : 192.168.11.100         Public IP    : 10.61.209.83
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
DTLS-Tunnel: (1)AES128
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10540                  Bytes Rx     : 32236
Pkts Tx      : 8                      Pkts Rx      : 209
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : MY                     Tunnel Group : RA
Login Time   : 11:30:31 CEST Sun Oct 13 2013
Duration     : 0h:01m:05s
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    : 4.1
 Public IP    : 10.61.209.83
 Encryption   : none                  Hashing      : none
 TCP Src Port : 51401                 TCP Dst Port : 443
 Auth Mode    : Certificate and userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : AnyConnect
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5270                  Bytes Rx     : 788
 Pkts Tx      : 4                     Pkts Rx      : 1
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

SSL-Tunnel:
 Tunnel ID    : 4.2
 Assigned IP  : 192.168.11.100        Public IP    : 10.61.209.83
 Encryption   : RC4                   Hashing      : SHA1
 Encapsulation: TLSv1.0               TCP Src Port : 51406
 TCP Dst Port : 443                   Auth Mode    : Certificate and
userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : SSL VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 5270                  Bytes Rx     : 1995
 Pkts Tx      : 4                     Pkts Rx      : 10
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0

DTLS-Tunnel:
 Tunnel ID    : 4.3
 Assigned IP  : 192.168.11.100        Public IP    : 10.61.209.83
 Encryption   : AES128                Hashing      : SHA1
 Encapsulation: DTLSv1.0              UDP Src Port : 58053
 UDP Dst Port : 443                   Auth Mode    : Certificate and
userPassword
 Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Client OS    : Windows
 Client Type  : DTLS VPN Client
 Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.02040
 Bytes Tx     : 0                     Bytes Rx     : 29664
 Pkts Tx      : 0                     Pkts Rx      : 201
 Pkts Tx Drop : 0                     Pkts Rx Drop : 0
```

5. 您能使用详细的调试OCSP验证：

```
CRYPTO_PKI: Starting OCSP revocation
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial number:
2400000019F341BA75BD25E91A000000000019, subject name: cn=Administrator,
cn=Users,dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com.
CRYPTO_PKI: No OCSP overrides found. <-- no OCSP url in the ASA config

CRYPTO_PKI: http connection opened
CRYPTO_PKI: OCSP response received successfully.
CRYPTO_PKI: OCSP found in-band certificate: serial number:
240000001221CFA239477CE1C0000000000012, subject name:
cn=DC.test-cisco.com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com
CRYPTO_PKI: OCSP responderID byKeyHash
CRYPTO_PKI: OCSP response contains 1 cert singleResponses responseData
sequence.

Found response for request certificate!
```

```
CRYPTO_PKI: Verifying OCSP response with 1 certs in the responder chain
CRYPTO_PKI: Validating OCSP response using trusted CA cert: serial number:
3D4C0881B04C799F483F4BBE91DC98AE, subject name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com

CERT-C: W ocsputil.c(538) : Error #708h
CERT-C: W ocsputil.c(538) : Error #708h

CRYPTO_PKI: Validating OCSP responder certificate: serial number:
240000001221CFA239477CE1C0000000000012, subject name:
cn=DC.test-cisco.com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com, signature alg: SHA1/RSA

CRYPTO_PKI: verifyResponseSig:3191
CRYPTO_PKI: OCSP responder cert has a NoCheck extension
CRYPTO_PKI: Responder cert status is not revoked <-- do not verify
responder cert
CRYPTO_PKI: response signed by the CA
CRYPTO_PKI: Storage context released by thread Crypto CA

CRYPTO_PKI: transaction GetOCSP completed
CRYPTO_PKI: Process next cert, valid cert. <-- client certificate
validated correctly
```

6. 在数据包捕获级别，这是OCSP请求和正确OCSP答复。答复包括正确签名-在Microsoft OCSP启用的目前分机：

与多个OCSP的ASA VPN远程访问来源

如果匹配证书配置按照与多OCSP来源的ASA说明，获得优先权：

```
CRYPTO_PKI: Processing map MAP sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:  =
cn=Administrator,cn=Users,dc=test-cisco,dc=com, map rule: subject-name
  co administrator.
CRYPTO_PKI: Peer cert has been authorized by map: MAP sequence: 10.
CRYPTO_PKI: Found OCSP override match. Override URL: http://11.11.11.11/ocsp,
Override trustpoint: OPENSSL
```

当使用时OCSP URL覆盖，调试是：

```
CRYPTO_PKI: No OCSP override via cert maps found. Override was found in
trustpoint: WIN2012, URL found: http://10.10.10.10/ocsp.
```

与OCSP和取消的证书的ASA VPN远程访问

此步骤描述如何废除证书和证实取消的状态：

1. 废除客户端证书：

2. 发布结果：

3. [Optional]步骤1和2可能用在电源Shell的certutil CLI工具也实行：

```
CRYPTO_PKI: No OCSP override via cert maps found. Override was found in
trustpoint: WIN2012, URL found: http://10.10.10.10/ocsp.
```

4. 当客户端设法连接时，有证书确认错误：

5. AnyConnect日志也指示证书确认错误：

```
CRYPTO_PKI: No OCSP override via cert maps found. Override was found in
trustpoint: WIN2012, URL found: http://10.10.10.10/ocsp.
```

6. ASA报告证书状态取消：

```
CRYPTO_PKI: Starting OCSP revocation
CRYPTO_PKI: OCSP response received successfully.
CRYPTO_PKI: OCSP found in-band certificate: serial number:
240000001221CFA239477CE1C0000000000012, subject name:
cn=DC.test-cisco.com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com
CRYPTO_PKI: OCSP responderID byKeyHash
CRYPTO_PKI: OCSP response contains 1 cert singleResponses responseData
sequence.

Found response for request certificate!
CRYPTO_PKI: Verifying OCSP response with 1 certs in the responder chain
CRYPTO_PKI: Validating OCSP response using trusted CA cert: serial number:
3D4C0881B04C799F483F4BBE91DC98AE, subject name: cn=test-cisco-DC-CA,
dc=test-cisco,dc=com, issuer_name: cn=test-cisco-DC-CA,dc=test-cisco,
dc=com

CRYPTO_PKI: verifyResponseSig:3191
CRYPTO_PKI: OCSP responder cert has a NoCheck extension
CRYPTO_PKI: Responder cert status is not revoked
CRYPTO_PKI: response signed by the CA
CRYPTO_PKI: Storage context released by thread Crypto CA

CRYPTO_PKI: transaction GetOCSP completed

CRYPTO_PKI: Received OCSP response:Oct 13 2013 12:48:03: %ASA-3-717027:
Certificate chain failed validation. Generic error occurred, serial
number: 240000001B2AD208B12811687400000000001B, subject name:
cn=Administrator,cn=Users,dc=test-cisco,dc=com.

CRYPTO_PKI: Blocking chain callback called for OCSP response (trustpoint:
WIN2012, status: 1)
CRYPTO_PKI: Destroying OCSP data handle 0xae255ac0
CRYPTO_PKI: OCSP polling for trustpoint WIN2012 succeeded. Certificate
status is REVOKED.
CRYPTO_PKI: Process next cert in chain entered with status: 13.
CRYPTO_PKI: Process next cert, Cert revoked: 13
```

7. 数据包捕获显示一成功的OCSP答复以证书状态取消：

故障排除

本部分提供的信息可用于对配置进行故障排除。

下来OCSP服务器

当OCSP服务器发生故障， ASA报道：

```
CRYPTO_PKI: unable to find a valid OCSP server.
CRYPTO PKI: OCSP revocation check has failed.  Status: 1800.
```

数据包捕获可也帮助与故障排除。

没同步的时间

如果在OCSP服务器的当前时间旧比在ASA (小差异是可接受)， OCSP服务器发送一未授权的答复，并且ASA报告它：

```
CRYPTO_PKI: unable to find a valid OCSP server.
CRYPTO PKI: OCSP revocation check has failed.  Status: 1800.
```

当ASA收到从将来时期时的OCSP答复，也发生故障。

不支持的签字的目前

如果不支持在服务器的目前(是在Microsoft Windows的默认2012个R2)，一未授权的答复返回：

IIS7服务器验证

与SCEP/OCSP请求的问题经常是不正确验证结果在互联网信息服务7 (IIS7)的。保证匿名访问配置：

相关信息

- Microsoft TechNet ：联机响应方安装、配置和故障排除指南
- Microsoft TechNet ：配置CA支持OCSP响应方
- 思科ASA系列命令参考
- 技术支持和文档 - Cisco Systems