# VPN de acceso remoto ASA con la verificación OCSP bajo Microsoft Windows 2012 y el OpenSSL

## Contenido



## Introducción

Este documento describe cómo utilizar la validación en línea del protocolo status del certificado (OCSP) en un dispositivo de seguridad adaptante de Cisco (ASA) para los Certificados

presentados por los usuarios de VPN. Los ejemplos de configuración para dos servidores OCSP (Certificate Authority de Microsoft Windows [CA] y OpenSSL) se presentan. La sección del verificar describe los flujos detallados en el nivel del paquete, y la sección del Troubleshooting se centra en los errores frecuentes y los problemas.

# Prerrequisitos

## Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración del comando line interface(cli) del dispositivo de seguridad de Cisco y configuración VPN adaptantes del Secure Socket Layer (SSL)
- Certificados X.509
- Microsoft Windows server
- Linux/OpenSSL

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Software adaptante del dispositivo de seguridad de Cisco, versión 8.4 y posterior
- Microsoft Windows 7 con el Cliente de movilidad Cisco AnyConnect Secure, versión 3.1
- R2 del servidor de Microsoft 2012
- Linux con OpenSSL 1.0.0j o más adelante

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

# Configurar

> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

## Diagrama de la red

El cliente utiliza el VPN de acceso remoto. Este acceso puede ser Cliente Cisco VPN (IPSec), movilidad segura de Cisco AnyConnect (versión 2 [IKEv2] del intercambio de claves SSL/Internet), o WebVPN (porta). Para iniciar sesión, el cliente proporciona el certificado correcto, así como el nombre de usuario/la contraseña que fue configurada localmente en el ASA. El certificado del cliente se valida vía el servidor OCSP.

## Acceso Remoto ASA con OCSP

El ASA se configura para el acceso SSL. El cliente está utilizando AnyConnect para iniciar sesión. El ASA utiliza el protocolo simple certificate enrollment (SCEP) para pedir el certificado:

```
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
```

Una correspondencia del certificado se crea para identificar a todos los usuarios cuyo tema-nombre contenga al administrador de la palabra (sin diferenciación entre mayúsculas y minúsculas). Esos usuarios están limitados a un grupo de túnel nombrado 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
```

La configuración VPN requiere la autorización exitosa (es decir, un certificado validado). También requiere las credenciales correctas para el nombre de usuario localmente definido (autenticación aaa):

```
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

> Nota: Vea la guía de configuración de las 5500 Series de Cisco ASA que usa el CLI, los 8.4 y los 8.6: Configurar a un servidor externo para la autorización de usuario del dispositivo de seguridad para los detalles en la configuración del ASA con el CLI.

### Instalación de los servicios

Este procedimiento describe cómo configurar los servicios de función para el servidor de Microsoft:

1. Navegue al **administrador de servidor > manejan >** Add los **papeles y las características**. El servidor de Microsoft necesita estos servicios de función:

   Autoridades de certificaciónInscripción de la red de las autoridades de certificación, que es utilizada por el clienteRespondedor en línea, que es necesario para OCSPEl servicio de la inscripción del dispositivo de red, que contiene la aplicación SCEP utilizó por el ASA El servicio web con las directivas puede ser agregado si es necesario.

2.
3.
4. Cuando usted agrega las características, esté seguro de incluir las herramientas en línea del respondedor porque incluye un OCSP broche-en eso se utiliza más adelante:

### Configuración de CA para la plantilla OCSP

El servicio OCSP utiliza un certificado para firmar la respuesta OCSP. Un certificado especial en el servidor de Microsoft se debe generar y debe incluir:

- Uso dominante extendido = firma OCSP
- OCSP el ningún marcar de la revocación

Este certificado es necesario para prevenir los loopes de la validación OCSP. El ASA no utiliza el servicio OCSP para intentar marcar el certificado presentado por el servicio OCSP.

1. Agregue una plantilla para el certificado en el CA navegan a **CA >** al **Certificate Template plantilla de certificado > manejan**, **respuesta** selecta **OCSP que firma**, y duplican la plantilla. Vea las propiedades para la plantilla creada recientemente, y haga clic la **ficha de seguridad**. Los permisos describen qué entidad se permite pedir un certificado que utilice esa plantilla, así que se requieren los permisos correctos. En este ejemplo, la entidad es el servicio OCSP que se está ejecutando en el mismo host (TEST-CISCO \ DC), y las necesidades del servicio OCSP Autoenroll los privilegios:

   El resto de las configuraciones para la plantilla se pueden fijar para omitir.

2. Active la plantilla. Navegue a **CA >** al **Certificate Template plantilla de certificado > nuevo > Certificate Template plantilla de certificado a publicar**, y para seleccionar la plantilla duplicado:

### Certificado del servicio OCSP

Este procedimiento describe cómo utilizar configuración en línea la Administración para configurar OCSP:

1. Navegue al **administrador de servidor >** a las **herramientas**.

2. Navegue a la **configuración de la revocación de la configuración de la revocación >** Add para agregar una nueva configuración:

   OCSP puede utilizar la misma empresa CA. El certificado para el servicio OCSP se genera.

3. Utilice la empresa seleccionada CA, y elija la plantilla creada anterior. El certificado se alista automáticamente:

4. Confirme que el certificado está alistado y su estatus es Working/OK:

5. Navegue a **CA >** los **Certificados publicados** para verificar a los detalles del certificado:

### Nonces del servicio OCSP

La implementación de Microsoft de OCSP es obediente con el RFC 5019 el perfil en línea ligero del protocolo status del certificado (OCSP) para los entornos en grandes cantidades, que es una versión simplificada del protocolo status en línea del certificado del Public Key Infrastructure de Internet del RFC 2560 X.509 - OCSP.

El ASA utiliza el RFC 2560 para OCSP. Una de las diferencias en los dos RFC es que el RFC 5019 no valida las peticiones firmadas enviadas por el ASA.

Es posible forzar el servicio de Microsoft OCSP para validar esas peticiones firmadas y para contestar con la respuesta firmada correcta. Navegue a la **configuración de la revocación >** a **RevocationConfiguration1 > Edit Properties**, y seleccione la opción **para habilitar el soporte de la extensión del NONCE**.

El servicio OCSP es listo para utilizar ahora.

Aunque Cisco no recomiende esto, el nonces se puede inhabilitar en el ASA:

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

### Configuración de CA para las Extensiones OCSP

Usted debe ahora configurar de nuevo CA para incluir la extensión de servidor OCSP en todos los Certificados publicados. El URL de esa extensión es utilizado por el ASA para conectar con el servidor OCSP cuando se valida un certificado.

1. Abra el cuadro de diálogo Propiedades para el servidor en CA.

2. Haga clic la lengueta de las **Extensiones**. La extensión del acceso a la información de la autoridad (AYA) que señala al servicio OCSP es necesaria; en este ejemplo, es http://10.61.208.243/ocsp. Habilite ambas opciones para la extensión de AYA:

   Incluya en la extensión de AYA de los Certificados publicadosIncluya en la extensión en línea del protocolo status del certificado (OCSP)

   Esto se asegura de que todos los Certificados publicados tengan una extensión correcta esas puntas al servicio OCSP.

## OpenSSL

> Nota: Vea la guía de configuración de las 5500 Series de Cisco ASA que usa el CLI, los 8.4 y los 8.6: Configurar a un servidor externo para la autorización de usuario del dispositivo de seguridad para los detalles en la configuración del ASA con el CLI.

Este ejemplo asume que el servidor del OpenSSL está configurado ya. Esta sección describe solamente la configuración y los cambios OCSP que son necesarios para la configuración de CA.

Este procedimiento describe cómo generar el certificado OCSP:

1. Estos parámetros son necesarios para el respondedor OCSP:

```
[ OCSPresponder ]
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = OCSPSigning
```

2. Estos parámetros son necesarios para los Certificados de usuario:

```
[ UserCerts ]
authorityInfoAccess = OCSP;URI:http://10.61.208.243
```

3. Los Certificados necesitan ser generados y ser firmados por CA.

4. Encienda el servidor OCSP:

```
openssl ocsp -index ourCAwebPage/index.txt -port 80 -rsigner
ocspresponder.crt -rkey ocspresponder.key -CA cacert.crt -text -out
log.txt
```

5. Pruebe el certificado del ejemplo:

```
openssl ocsp -CAfile cacert.crt -issuer cacert.crt -cert example-cert.crt
-url http://10.61.208.243 -resp_text
```

Más ejemplos están disponibles en el sitio web del OpenSSL.

El OpenSSL, como el ASA, soporta el nonces OCSP; el nonces se puede controlar con el uso -nonce y - del Switches del no_nonce.

## ASA con las fuentes múltiples OCSP

El ASA puede reemplazar el OCSP URL. Incluso si el certificado del cliente contiene un OCSP URL, es sobregrabado por la configuración en el ASA:

```
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
```

La dirección del servidor OCSP puede ser definida explícitamente. Este comando example hace juego todos los Certificados con el administrador en el asunto, utiliza un trustpoint del OPENSSL para validar la firma OCSP, y utiliza el URL de http://11.11.11.11/ocsp para enviar la petición:

```
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
```

La orden usada para encontrar OCSP URL es:

1. Un servidor OCSP que usted fijó con el **comando certificate de la coincidencia**
2. Un servidor OCSP que usted fijó con el **comando url del ocsp**
3. El servidor OCSP en el campo de AYA del certificado del cliente

## ASA con OCSP firmado por diverso CA

Una respuesta OCSP se puede firmar por un diverso CA en tal caso, él es necesaria utilizar el **comando certificate de la coincidencia** para utilizar un diverso trustpoint en el ASA para la validación de certificado OCSP.

```
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
```

En este ejemplo, el ASA utiliza la reescritura OCSP URL para todos los Certificados con un tema-nombre que contenga al administrador. El ASA se fuerza a validar el certificado del respondedor OCSP contra otro trustpoint, OPENSSL. Los Certificados de usuario todavía se validan en el trustpoint WIN2012.

Puesto que el certificado del respondedor OCSP tiene el “OCSP ninguna revocación que marca” la extensión, el certificado no se verifica, incluso cuando OCSP se fuerza a validar contra el trustpoint del OPENSSL.

Por abandono, se busca todo el trustpoints cuando el ASA está intentando verificar el Certificado de usuario. La validación para el certificado del respondedor OCSP es diferente. El ASA busca solamente el trustpoint que se ha encontrado ya para el Certificado de usuario (WIN2012 en este ejemplo).

Así, es necesario utilizar el **comando certificate de la coincidencia** para forzar el ASA para utilizar un diverso trustpoint para la validación de certificado OCSP (OPENSSL en este ejemplo).

Los Certificados de usuario se validan contra el primer trustpoint correspondido con (WIN2012 en este ejemplo), que entonces determina el trustpoint predeterminado para la validación del respondedor OCSP.

Si no se proporciona ningún trustpoint específico en el **comando certificate de la coincidencia**, el certificado OCSP se valida contra el mismo trustpoint que los Certificados de usuario (WIN2012 en este ejemplo).:

```
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
```

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

> Nota: La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

## ASA - Consiga el certificado vía el SCEP

Este procedimiento describe cómo obtener el certificado con el uso del SCEP:

1. Éste es el proceso de autenticación del trustpoint para conseguir el certificado de CA:

```
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. Para pedir el certificado, el ASA necesita tener una contraseña de una sola vez SCEP que

se pueda obtener de la consola admin en http://IP/certsrv/mscep_admin:

3. Utilice esa contraseña para pedir el certificado en el ASA:

```
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
```

Una cierta salida se ha omitido para mayor clareza.

4. Verifique los Certificados de CA y ASA:

```
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
```

El ASA no visualiza la mayor parte de las Extensiones del certificado. Aunque el certificado ASA contiene “OCSP URL en la extensión de AYA”, el ASA CLI no la presenta. Id. de bug Cisco CSCui44335, “Extensiones del certificado x509 ASA ENH visualizadas,” pide esta mejora.

## AnyConnect - Consiga el certificado vía la página web

Este procedimiento describe cómo obtener el certificado con el uso del buscador Web en el cliente:

1. Un Certificado de usuario de AnyConnect se puede pedir con la página web. En PC del cliente, utilice a un buscador Web para ir a CA en http:// *IP/certsrv*:

2. El Certificado de usuario se puede guardar en el almacén del buscador Web, después exportar a Microsoft el almacén, que es buscado por AnyConnect. Utilice certmgr.msc para verificar el certificado recibido:

   AnyConnect puede también pedir el certificado mientras haya un perfil correcto de AnyConnect.

## Acceso Remoto ASA VPN con la validación OCSP

Este procedimiento describe cómo marcar la validación OCSP:

1. Mientras que intenta conectar, el ASA señala que el certificado se está marcando para saber si hay OCSP. Aquí, el certificado de firma OCSP tiene una extensión del ninguno-control y no se ha marcado vía OCSP:

   ```
   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: 240000001B2AD208B128116874000000000001B, 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.
```

Una cierta salida se ha omitido para mayor clareza.

2. El usuario final proporciona los credenciales de usuario:

3. Acaban a la sesión de VPN correctamente:

```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps
for peer certificate with serial number:
240000001B2AD208B128116874000000000001B, 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: 240000001B2AD208B128116874000000000001B,
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. Se crea la sesión:

```
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. Usted puede utilizar los debugs detallados para la validación OCSP:

```
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. En el nivel de la captura de paquetes, ésta es la petición OCSP y la respuesta correcta OCSP. La respuesta incluye la firma correcta - extensión del nonce habilitada en Microsoft OCSP:

## Acceso Remoto ASA VPN con las fuentes múltiples OCSP

Si un certificado de la coincidencia se configura como se explica en el ASA con las fuentes múltiples OCSP, toma la precedencia:

```
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
```

Cuando se utiliza una invalidación OCSP URL, los debugs son:

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

## Acceso Remoto ASA VPN con OCSP y el certificado revocado

Este procedimiento describe cómo revocar el certificado y confirmar el estatus revocado:

1. Revoque el certificado del cliente:

2. Publique los resultados:

3. [Optional] los pasos 1 y 2 se pueden también hacer con la utilidad CLI del certutil en el shell del poder:

```
c:\certutil -crl
CertUtil: -CRL command completed succesfully.
```

4. Cuando el cliente intenta conectar, hay un error de la validación de certificado:

5. Los registros de AnyConnect también indican el error de la validación de certificado:

```
[2013-10-13 12:49:53] Contacting 10.48.67.229.
[2013-10-13 12:49:54] No valid certificates available for authentication.
[2013-10-13 12:49:55] Certificate Validation Failure
```

6. El ASA señala que el estatus del certificado está revocado:

```
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. Las capturas de paquetes muestran una respuesta acertada OCSP con el estatus del certificado de revocado:

# Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

## Servidor OCSP abajo

El ASA señala cuando el servidor OCSP está abajo:

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

Las capturas de paquetes pueden también ayudar con el troubleshooting.

## Tiempo no sincronizado

Si la hora actual en el servidor OCSP es más vieja que en el ASA (las pequeñas diferencias son aceptables), el servidor OCSP envía una respuesta desautorizada, y el ASA la señala:

```
CRYPTO_PKI: OCSP response status - unauthorized
```

Cuando el ASA recibe una respuesta OCSP a partir de las épocas futuras, también falla.

## Nonces firmado no soportado

Si el nonces en el servidor no se soporta (que es el valor por defecto en el r2 de Microsoft Windows 2012), se vuelve una respuesta desautorizada:

## Autenticación de servidor IIS7

Los problemas con una petición SCEP/OCSP son a menudo el resultado de la autenticación incorrecta en los Servicios de Internet Information Server 7 (IIS7). Asegúrese de que el acceso anónimo esté configurado:

# Información Relacionada

- TechNet de Microsoft: Instalación, configuración, y guía de Troubleshooting en línea del respondedor

- TechNet de Microsoft: Configure CA para soportar a los respondedores OCSP
- Referencia de comandos de la serie de Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems