VPN de acceso remoto ASA con verificación OCSP en Microsoft Windows 2012 y OpenSSL

Contenido

Introducción **Prerequisites** Requirements Componentes Utilizados Configurar Diagrama de la red Acceso remoto a ASA con OCSP CA de Microsoft Windows 2012 Instalación de servicios Configuración de CA para la plantilla OCSP Certificado de servicio OCSP Nonces del servicio OCSP Configuración de CA para extensiones de OCSP **OpenSSL** ASA con varias fuentes de OCSP ASA con OCSP firmado por una CA diferente Verificación ASA - Obtener certificado a través de SCEP AnyConnect - Obtener certificado a través de la página web Acceso remoto VPN ASA con validación OCSP Acceso remoto VPN ASA con varias fuentes OCSP Acceso remoto a VPN ASA con OCSP y certificado revocado Troubleshoot Servidor OCSP inactivo Hora no sincronizada Nonces Firmados No Soportados Autenticación del servidor IIS7 Información Relacionada

Introducción

Este documento describe cómo utilizar la validación del Protocolo de estado de certificados en línea (OCSP) en un Cisco Adaptive Security Appliance (ASA) para los certificados presentados por usuarios de VPN. Se presentan ejemplos de configuraciones para dos servidores OCSP (Microsoft Windows Certificate Authority [CA] y OpenSSL). La sección Verificación describe los

flujos detallados en el nivel de paquete, y la sección Resolución de problemas se centra en los errores y problemas típicos.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de la interfaz de línea de comandos (CLI) del dispositivo de seguridad adaptable de Cisco y configuración de VPN de capa de socket seguro (SSL)
- Certificados X.509
- Servidor de Microsoft Windows
- Linux/OpenSSL

Componentes Utilizados

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

- Software Adaptive Security Appliance de Cisco, versión 8.4 y posteriores
- Microsoft Windows 7 con Cisco AnyConnect Secure Mobility Client, versión 3.1
- Microsoft Server 2012 R2
- Linux con OpenSSL 1.0.0j o posterior

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). If your network is live, make sure that you understand the potential impact of any command.

Configurar

Nota: Use el Command Lookup Tool (únicamente clientes registrados) para obtener más información sobre los comandos que se utilizan en esta sección.

Diagrama de la red

El cliente utiliza VPN de acceso remoto. Este acceso puede ser Cisco VPN Client (IPSec), Cisco AnyConnect Secure Mobility (SSL/Intercambio de claves de Internet versión 2 [IKEv2]) o WebVPN (portal). Para iniciar sesión, el cliente proporciona el certificado correcto, así como el nombre de usuario/contraseña que se configuraron localmente en el ASA. El certificado de cliente se valida a través del servidor OCSP.



Acceso remoto a ASA con OCSP

ASA está configurado para el acceso SSL. El cliente está usando AnyConnect para iniciar sesión. El ASA utiliza el Protocolo de inscripción de certificado simple (SCEP) para solicitar 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

Se crea un mapa de certificado para identificar a todos los usuarios cuyo nombre de sujeto contiene la palabra administrador (no distingue entre mayúsculas y minúsculas). Estos usuarios están vinculados a un grupo de túnel denominado 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 una autorización correcta (es decir, un certificado validado). También requiere las credenciales correctas para el nombre de usuario definido localmente (authentication aaa):

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

```
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
```

CA de Microsoft Windows 2012

Nota: Consulte la <u>Guía de configuración de Cisco ASA serie 5500 con CLI, 8.4 y 8.6:</u> <u>Configuración de un servidor externo para la autorización de usuario de dispositivos de</u> <u>seguridad</u> para obtener detalles sobre la configuración de ASA a través de CLI.

Instalación de servicios

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

1. Vaya a Administrador del servidor > Administrar > Agregar roles y características. El servidor de Microsoft necesita estos servicios de rol:

Entidad emisora de certificadosCertification Authority Web Enrollment, que utiliza el clienteRespondedor en línea, necesario para OCSPNetwork Device Enrollment Service, que contiene la aplicación SCEP utilizada por ASA Si es necesario, se puede agregar un servicio Web con directivas.

Role Services		DESTINATION SEF WIN-35QVH03PQE3.lab.
Credentials	Select Role Services to configure	
Role Services		
Setup Type	Certification Authority	
CA Type	Certification Authority Web Enrollment	
Private Key	Network Device Enrollment Service	
Cryptography	Certificate Enrollment Web Service	
CA Name	 Certificate Enrollment Policy Web Service 	
Validity Period		
Certificate Database		
Authentication Type for C		
Confirmation		
Progress		
	More about AD CS Server Roles	
1		

- 3.
- 4. Cuando agregue características, asegúrese de incluir las Herramientas del Respondedor en línea, ya que incluye un complemento de OCSP que se utilizará más adelante:

elect features		DESTINATION SERVER WIN-35QVH03PQE3.Jab.com
Before You Begin	Select one or more features to install on the selected server.	
Installation Type	Features	Description
Server Selection		Online Responder Tools includes th
Server Roles	Role Administration Tools (12 of 28 installed)	Online Responder Management
Features	AD DS and AD LDS Tools (4 of 5 installed)	snap-in.
AD CS	Hyper-V Management Tools Bemote Desites Sensies Tools (1 of 2 insti-	
Role Services	Windows Server Update Services Tools	
Confirmation	▲ ✓ Active Directory Certificate Services Tools	
	Certification Authority Management Toc Continue Responder Tools	
	Active Directory Rights Management Servic DHCP Server Tools (Installed)	
	DNS Server Tools (Installed)	
	Fax Server Tools	
	File Services Tools	
	✓ Network Policy and Access Services Tools (
	 III III 	

Configuración de CA para la plantilla OCSP

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

- Uso de clave extendido = firma OCSP
- Verificación de no revocación de OCSP

Este certificado es necesario para evitar bucles de validación de OCSP. ASA no utiliza el servicio OCSP para intentar comprobar el certificado presentado por el servicio OCSP.

 Agregue una plantilla para el certificado en la CA. Navegue hasta CA > Certificate Template > Manage, seleccione OCSP Response Signing y duplique la plantilla. Vea las propiedades de la plantilla recién creada y haga clic en la pestaña Seguridad. Los permisos describen a qué entidad se le permite solicitar un certificado que utiliza esa plantilla, por lo que se requieren los permisos correctos. En este ejemplo, la entidad es el servicio OCSP que se ejecuta en el mismo host (TEST-CISCO\DC) y el servicio OCSP necesita privilegios de inscripción automática:

	Certific	ate Templates Console	_ 🗆 X
File Action View Help			
🔶 🔿 📷 🖾 🗟 📷			
Certificate Templates (DC.test-c	Template Display Name	Schema Verrion Verri Intended I	Actions
	Administrator	× p Templates	
	Authenticated Session	Cubicut Name Country Income	Provinces and sticks
	Basic EFS	Compatibility General Request Handling Cryptograph	v Key Attestation
	CA Exchange	Superseded Templates Extensions	Securty ponse Signi A
	Code Signing	Group or user names:	ctions 🕨
	Computer	& Authenticated Users	
	Copy of OCSP Response Signing	Administrator	
	Cross Certification Authority	Domain Admins (TEST-CISCO\Domain Admins)	
	Directory Email Replication	Enterprise Admins (TEST-CISCO\Enterprise Admins)	
	Domain Controller Authentication		
	EFS Recovery Agent		
	Enrollment Agent	Add	Remove
	Enrollment Agent (Computer)	Demission for DC	
	Exchange Signature Only	Femissions for DC Allow	
	R Exchange User	Read	
	IPSec	Write	
	IPSec (Offline request)	Enrol	
	Key Recovery Agent	Autoenrol	
	OCSP Response Signing		
	RAS and IAS Server	For special permissions or advanced settings, click	Adversed
	Root Certification Authority	Advanced.	Advanced
	Router (Offline request)		
	Smartcard Logon		
	Subordinate Certification Authority	OK Cancel Apply	Help
	Trust List Signing	1 3.1	×
< III >	< III		>

El resto de la configuración de la plantilla se puede establecer en el valor predeterminado.

2. Active la plantilla. Navegue hasta CA > Plantilla de certificado > Nuevo > Plantilla de certificado para emitir, y seleccione la plantilla duplicada:



Certificado de servicio OCSP

Este procedimiento describe cómo utilizar Online Configuration Management para configurar OCSP:

- 1. Vaya a Administrador del servidor > Herramientas.
- 2. Navegue hasta **Revocation Configuration > Add Revocation Configuration** para agregar una nueva configuración:

9	ocsp - [Online Responder: DC.test-cisco.com\Re	vocation Configuration]
File Action View Help		
🗢 🔿 🙍 🕞		
P Online Responder: DC.test-cisco.cc	Name Signing Certi	ficate Selec Enrollment Ter
 	There are no items to show in thi	is view.
	Add Revocation Configuration	? X
Choose CA C	ertificate	
Getting started with addi Name the Revocation Co Select CA Certificate Loca	In order to check the status of a certificate, a revocation configuration Responder must identify the CA that issued the certificate. You can identify this CA by selecting a CA certificate published in Act by locating a CA computer.	i for the Online ive Directory or
Choose CA Certificate Select Signing Certificate	Browse CA certificates published in Active Directory	Browse
Revocation Provider	Select Certification Authority ?	
	Select a certification authority (CA) you want to use.	rowse
	CA Computer	
	test-cisco-DC-CA DC.test-cisco.com	
	< III > Cancel	Cancel

OCSP puede utilizar la misma CA empresarial. Se genera el certificado para el servicio OCSP.

3. Utilice la entidad emisora de certificados de empresa seleccionada y elija la plantilla creada anteriormente. El certificado se inscribe automáticamente:



4. Confirme que el certificado está inscrito y que su estado es Working/OK:



Revocation Configuration Status	
Signing Certificate: Ok	
<u>View Signing Certificate</u> Revocation Provider Status	
Type: Microsoft CRL-based revocation status provider	^
The revocation provider is successfully using the current configuration	
I	
	\sim

5. Navegue hasta CA > Certificados emitidos para verificar los detalles del certificado:

i	certsrv - [Certification Authority (Local)\test-cisco-[C-CA	ssued Certificate	es]
File Action View Help				
* 🔿 🙎 🖻 📓	Certificate X			
Certification Authority (Local) test-cisco-DC-CA Revoked Certificates Pending Requests Failed Requests Certificate Templates	General Details Certification Path Show: <all> Field Value ^ Wald to Thursday, October 24, 2013 6 Subject DC.test-cisco.com Public key RSA (2048 Bits) Certificate Template Inform Template=1.3.6.1.4.1.311.21 Enhanced Key Usage OCSP Signing (1.3.6.1.5.5.7.3 Application/Policies [1]Application Certificate Polic OCSP No Revocation Checking 05 00 Authority Key Identifier KeyID=9f 99 7f b2 3b 61 90 0 OCSP Signing (1.3.6.1.5.5.7.3.9)</all>	late ler (nent (CEP ques ques ques 8.16	Serial Number 24000000206c 240000003d86 2400000057d8 2400000057d8 24000000639b 2400000082d2 24000000082d2 24000000084 240000000648 240000000648 240000000647c 240000000680d 24000000021221c	Certificate Effective Date 10/10/2013 7:25 AM 10/10/2013 7:33 AM 10/10/2013 7:33 AM 10/10/2013 11:54 AM 10/10/2013 11:54 AM 10/11/2013 12:05 AM 10/11/2013 12:05 AM 10/10/2013 12:27 PM 10/10/2013 1:27 PM 10/10/2013 1:27 PM 10/10/2013 1:28 PM 10/10/2013 1:30 PM 10/10/2013 2:06 PM 10/10/2013 6:51 PM

Nonces del servicio OCSP

La implementación de Microsoft de OCSP cumple con <u>RFC 5019 El perfil del protocolo ligero de</u> <u>estado de certificados en línea (OCSP) para entornos de gran volumen</u>, que es una versión simplificada del <u>protocolo de estado de certificados en línea de la infraestructura de clave pública</u> <u>de Internet RFC 2560 X.509 - OCSP</u>.

ASA utiliza RFC 2560 para OCSP. Una de las diferencias entre los dos RFC es que RFC 5019 no acepta solicitudes firmadas enviadas por ASA.

Es posible forzar al servicio OCSP de Microsoft a aceptar esas solicitudes firmadas y responder

con la respuesta firmada correcta. Navegue hasta **Revocation Configuration** > **RevocationConfiguration1 > Edit Properties**, y seleccione la opción para **Habilitar el soporte de extensión NONCE**.



El servicio OCSP ya está listo para utilizarse.

Aunque Cisco no recomienda esto, los nonces se pueden inhabilitar en el ASA:

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

Configuración de CA para extensiones de OCSP

Ahora debe volver a configurar la CA para incluir la extensión de servidor OCSP en todos los certificados emitidos. ASA utiliza la URL de esa extensión para conectarse al servidor OCSP cuando se valida un certificado.

- 1. Abra el cuadro de diálogo Propiedades del servidor de la CA.
- Haga clic en la pestaña Extensions. Se necesita la extensión Authority Information Access (AIA) que apunta al servicio OCSP; en este ejemplo, es http://10.61.208.243/ocsp. Habilite estas dos opciones para la extensión AIA:

Incluir en el AIA la extensión de los certificados expedidosIncluir en la extensión del protocolo de estado de certificados en línea (OCSP)

ته c	test-cisco-DC-CA Properties ?					
File Action View Help	Enrollment Agents	Auditing	Recover	y Agents	Security	
🔄 🛸 🔟 📋 🖄 🛸 🚺	General	Policy Mo	dule	Exit	Module	
Certification Authority (Local)	Extensions	lanagers				
⊿ 👼 test-cisco-DC-CA	Select extension:					
Revoked Certificates	Authority Information	Access (AIA)			~	
Pending Requests	Specify locations from	which users car	n obtain the o	certificate for	r this CA.	
Failed Requests						
Certificate Templates	C:\Windows\system32\CertSrv\CertEnroll\ <serverdnsname>_<caname: Idap:///CN=<catruncatedname>,CN=AIA,CN=Public Key Services,CN=S http://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><ce file://<serverdnsname>/CertEnroll/<serverdnsname>_<caname><cert http://10.61.208.243/ocsp</cert </caname></serverdnsname></serverdnsname></ce </caname></serverdnsname></serverdnsname></catruncatedname></caname: </serverdnsname>					
	< III >					
			Add	d	Remove	
	✓ Include in the AIA	extension of issu	ed certificate	es		
	Include in the onlin	e certificate stat	us protocol (OCSP) exter	nsion	

Esto garantiza que todos los certificados emitidos tengan una extensión correcta que apunte al servicio OCSP.

OpenSSL

Nota: Consulte la <u>Guía de configuración de Cisco ASA serie 5500 con CLI, 8.4 y 8.6</u>: <u>Configuración de un servidor externo para la autorización de usuario de dispositivos de</u> <u>seguridad</u> para obtener detalles sobre la configuración de ASA a través de CLI.

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

Este procedimiento describe cómo generar el certificado OCSP:

1. Estos parámetros son necesarios para el respondedor de OCSP:

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

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

authorityInfoAccess = OCSP;URI:http://10.61.208.243

- 3. Los certificados deben ser generados y firmados por la CA.
- 4. Inicie 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 de ejemplo:

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

Hay más ejemplos disponibles en el sitio web de OpenSSL .

OpenSSL, como ASA, soporta nonces de OCSP; los nonces se pueden controlar con el uso de los switches -nonce y -no_nonce.

ASA con varias fuentes de OCSP

ASA puede anular la URL de OCSP. Incluso si el certificado de cliente contiene una URL de OCSP, la configuración del ASA lo sobrescribe:

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/ocsp

La dirección del servidor OCSP se puede definir explícitamente. Este ejemplo de comando hace coincidir todos los certificados con administrator en subject name, utiliza un punto de confianza OPENSSL para validar la firma OCSP y utiliza la dirección URL de http://11.11.11.11/ocsp para enviar la solicitud:

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

El orden utilizado para encontrar la URL de OCSP es:

- 1. Un servidor OCSP configurado con el comando match certificate
- 2. Un servidor OCSP configurado con el comando ocsp url
- 3. El servidor OCSP en el campo AIA del certificado de cliente

ASA con OCSP firmado por una CA diferente

Una respuesta de OCSP puede estar firmada por una CA diferente. En tal caso, es necesario utilizar el comando **match certificate** para utilizar un punto de confianza diferente en el ASA para

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, ASA utiliza la reescritura de URL de OCSP para todos los certificados con un nombre de sujeto que contiene administrador. ASA se ve obligado a validar el certificado de respondedor OCSP frente a otro punto de confianza, OPENSSL. Los certificados de usuario se siguen validando en el punto de confianza WIN2012.

Dado que el certificado del respondedor de OCSP tiene la extensión 'OCSP sin comprobación de revocación', el certificado no se verifica, incluso cuando OCSP se ve obligado a realizar la validación con el punto de confianza de OPENSSL.

De forma predeterminada, se buscan todos los puntos de confianza cuando el ASA intenta verificar el certificado de usuario. La validación del certificado del respondedor de OCSP es diferente. ASA busca el certificado de usuario sólo en el punto de confianza que ya se ha encontrado (WIN2012 en este ejemplo).

Por lo tanto, es necesario utilizar el comando **match certificate** para forzar al ASA a utilizar un punto de confianza diferente para la validación de certificados OCSP (OPENSSL en este ejemplo).

Los certificados de usuario se validan con respecto al primer punto de confianza coincidente (WIN2012 en este ejemplo), que luego determina el punto de confianza predeterminado para la validación del respondedor de OCSP.

Si no se proporciona ningún punto de confianza específico en el comando **match certificate**, el certificado OCSP se valida con el mismo punto de confianza 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 <u>herramienta Output Interpreter Tool</u> (<u>sólo</u> clientes <u>registrados</u>) admite ciertos comandos **show**. Utilice la herramienta para ver una análisis de información de salida del comando show.

ASA - Obtener certificado a través de SCEP

Este procedimiento describe cómo obtener el certificado mediante el uso de SCEP:

 Este es el proceso de autenticación de punto de confianza para obtener el certificado de la 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:
               27dda0e5 eled3f4c e3a2c3da 6d1689c2
Fingerprint:
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 solicitar el certificado, el ASA necesita tener una contraseña SCEP de un solo uso que se puede obtener de la consola de administración en http://IP/certsrv/mscep_admin:



3. Utilice esa contraseña para solicitar 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.
```

```
% 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

Algunos resultados se han omitido para mayor claridad.

4. Verifique los certificados de CA y ASA:

```
BSNS-ASA5510-3(config) # show crypto ca certificates
Certificate
Status: Available
Certificate Serial Number: 240000001cbf2fc89f44fe81970000000001c
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 no muestra la mayoría de las extensiones de certificado. Aunque el certificado de ASA contiene la extensión 'OCSP URL in AIA', la CLI de ASA no la presenta. La identificación de error de Cisco <u>CSCui44335</u>, "ASA ENH Certificate x509 extensions played," solicita esta mejora.

AnyConnect - Obtener certificado a través de la página web

Este procedimiento describe cómo obtener el certificado mediante el uso del explorador web en el cliente:

1. Se puede solicitar un certificado de usuario de AnyConnect a través de la página web. En el equipo cliente, utilice un navegador web para ir a la CA en http://*IP*/certsrv:

← → C □ 192.168.10.100/certsrv/
Microsoft Active Directory Certificate Services test-cisco-DC-CA
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you ca depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation li
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.
Select a task: Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

2. El certificado de usuario se puede guardar en el almacén del explorador web y, a continuación, exportarse al almacén de Microsoft, en el que AnyConnect realiza la búsqueda. Utilice certmgr.msc para verificar el certificado recibido:



AnyConnect también puede solicitar el certificado siempre que haya un perfil de AnyConnect correcto.

Acceso remoto VPN ASA con validación OCSP

Este procedimiento describe cómo comprobar la validación de OCSP:

 A medida que intenta conectarse, ASA informa que se está comprobando si el certificado tiene OCSP. Aquí, el certificado de firma de OCSP tiene una extensión sin verificación y no se ha verificado a través de 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: 240000001B2AD208B1281168740000000001B, 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.
```

Algunos resultados se han omitido para mayor claridad.

2. El usuario final proporciona las credenciales de usuario:

🕙 Cisco AnyConn				
Username:	cisco			
Password:				
	OK Cancel			
🕥 Cisco AnyCon	nect Secure Mobility Client			8
	VPN: Contacting 10.48.67.229. 10.48.67.229	-	Connect	
Q ()				ahah cisco

3. La sesión VPN ha finalizado correctamente:

%ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with serial number: 24000001B2AD208B128116874000000001B, 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: 24000001B2AD208B12811687400000000001B, 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

 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 Pkts Tx : 8 Bytes Rx : 32236 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 : none VLAN Mapping : N/A 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 Hashing : SHA1 TCP Src Port : 51406 Auth Mode : Certificate and Encryption : RC4 Encapsulation: TLSv1.0 TCP Dst Port : 443 userPassword Idle TO Left : 29 Minutes Idle Time Out: 30 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 Hashing : SHA1 UDP Src Port : 58053 Auth Mode : Certificate and Encryption : AES128 Encapsulation: DTLSv1.0 UDP Dst Port : 443 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 Pkts Tx : 0 Bytes Rx : 29664 : 201 Pkts Rx

5. Puede utilizar depuraciones detalladas para la validación de OCSP:

 $\texttt{CRYPTO_PKI: Starting OCSP revocation}$ CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial number: 2400000019F341BA75BD25E91A00000000019, 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: 240000001221CFA239477CE1C000000000012, 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: 240000001221CFA239477CE1C000000000012, 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 captura de paquetes, esta es la solicitud OCSP y la respuesta OCSP correcta. La respuesta incluye la firma correcta - extensión nonce habilitada en Microsoft OCSP:

No.	Source	Destination	Protocol	Length	Info		
24	10.48.67.229	10.61.208.243	0CSP	545	Request		
31	10.61.208.243	10.48.67.229	0CSP	700	Response		
4							
▶ Hy	pertext Transfer Prot	tocol					
<mark>∽ 0n</mark>	line Certificate Stat	tus Protocol					
	responseStatus: succe	ssful (0)					
⊽	responseBytes						
	ResponseType Id: 1.3	3.6.1.5.5.7.48.1.1 (id-pkix-	ocsp-ba	sic)		
-	Basic0CSPResponse						
	🔻 tbsResponseData						
	▷ responderID: byK	ey (2)					
	producedAt: 2013	-10-12 14:48:27 (UTC	.)				
	▹ responses: 1 ite	m					
	responseExtensio	ns: 1 item					
	<pre>▼ Extension</pre>						
	Id: 1.3.6.1.5	.5.7.48.1.2 (id-pkix	.48.1.2)			
	BER: Dissector for OID:1.3.6.1.5.5.7.48.1.2 not implemented.						
	signatureAlgorithm (shaWithRSAEncryption)						
	Padding: 0						
	signature: 353fc46	01732dc47b1d167ebace6	677a0877	65b48ed	b3b284c		
	⊳ certs: 1 item						

Acceso remoto VPN ASA con varias fuentes OCSP

Si se configura un certificado de coincidencia como se explica en <u>ASA con varias fuentes de</u> <u>OCSP</u>, tiene prioridad:

```
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 de URL de OCSP, 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 a VPN ASA con OCSP y certificado revocado

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

1. Revocar el certificado de cliente:

certsrv - [Certification Authority (Local)\test-cisco-DC-CA\Issued							
File Action View Help							
🗢 🔿 🙎 🗟 🗟							
🙀 Certification Authority (Local)	Request	ID	Requester	Na	ame	Binary Certificate	Certif
⊿ 🚽 test-cisco-DC-CA	-		TEST-CISC	0	\Ad	BEGIN CERTI	IPSec
Revoked Certificates	5 7		TEST-CISC	0	\Ad	BEGIN CERTI	IPSec
Issued Certificates	58 💭		TEST-CISC	0	\Ad	BEGIN CERTI	IPSec
Pending Requests	5 9		TEST-CISC	0	\Ad	BEGIN CERTI	User
Failed Requests	🔄 10		TEST-CISC	0	\Ad	BEGIN CERTI	User
Certificate Templates	🔄 11		TEST-CISC	0	\Ad	BEGIN CERTI	User
	🔄 12		TEST-CISC	0	∖Ad	BEGIN CERTI	User
	🔄 13		TEST-CISC	0	∖Ad	BEGIN CERTI	User
	🔄 14		TEST-CISC	0	\Ad	BEGIN CERTI	IPSec
	🔄 18		TEST-CISC	0	\DC\$	BEGIN CERTI	Сору
	🔄 19		TEST-CISC	0	∖Ad	BEGIN CERTI	IPSec
	l 🔄 20		TEST-CISC	0	∖Ad	BEGIN CERTI	IPSec
	l 🔄 21		TEST-CISC	0	∖Ad	BEGIN CERTI	User
	-	0			Ad	BEGIN CERTI	User
		Open		_	Ad	BEGIN CERTI	User
		All Ta	sks	۲		View Attributes/Extensi	ons
R		Refresh			Export Binary Data		
		Help	lp			Revoke Certificate	
	28		TEST-CISC	0	∖Ad	BEGIN CERTI	IPSec
	<						
Contains actions that can be performed on the item.							

2. Publicar los resultados:



3. [Opcional] Los pasos 1 y 2 también se pueden realizar con la utilidad CLI certutil en Power Shell:

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

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

Cisco AnyConnect	
Certificate Validation Failure	
ОК	
Scisco AnyConnect Secure Mobility Client	
VPN: No valid certificates available f 10.48.67.229	For authentication.
Ö (i)	alada
₩ 0	CISCO

5. Los registros de AnyConnect también indican el error de validación del 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 informa que el estado del certificado es revocado:

```
CRYPTO_PKI: Starting OCSP revocation
CRYPTO_PKI: OCSP response received successfully.
CRYPTO_PKI: OCSP found in-band certificate: serial number:
240000001221CFA239477CE1C00000000012, 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: 240000001B2AD208B1281168740000000001B, 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 de OCSP exitosa con el estado de certificado de revocado:

No.	Source	Destination	Protocol	Length	Info			
24	1 10.48.67.229	10.61.209.83	0CSP	544	Request			
33	L 10.61.209.83	10.48.67.229	0CSP	721	Response			
4								
⊳ Hy	pertext Transfer Pro	tocol						
⊽ Or	🗢 Online Certificate Status Protocol							
responseStatus: successful (0)								
~	✓ responseBytes							
	ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)							
· ·	▼ Basic0CSPResponse							
	▼ tbsResponseData							
	▷ responderID: byKey (2)							
	producedAt: 2013-10-13 10:47:02 (UTC)							
	▼ responses: 1 item							
	▼ SingleResponse							
▷ certID								
certStatus: revoked (1)								
thisUpdate: 2013-10-13 10:17:51 (UTC)								
nextUpdate: 2013-10-14 22:37:51 (UTC)								
singleExtensions: 1 item								
responseExtensions: 1 item								
	signatureAlgorithm (shaWithRSAEncryption)							

Troubleshoot

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

configuración.

Servidor OCSP inactivo

ASA informa cuando el servidor OCSP está inactivo:

CRYPTO_PKI: unable to find a valid OCSP server. CRYPTO PKI: OCSP revocation check has failed. Status: 1800. Las capturas de paquetes también pueden ayudar con la resolución de problemas.

Hora no sincronizada

Si la hora actual en el servidor OCSP es anterior a la de ASA (se aceptan pequeñas diferencias), el servidor OCSP envía una respuesta no autorizada y ASA informa de ello:

CRYPTO_PKI: OCSP response status - unauthorized Cuando ASA recibe una respuesta de OCSP de tiempos futuros, también falla.

Nonces Firmados No Soportados

Si no se admiten nonces en el servidor (que es el valor predeterminado en Microsoft Windows 2012 R2), se devuelve una respuesta no autorizada:

No.	Source	Destination	Protocol	Length	Info			
56	10.48.67.229	10.61.208.243	0CSP	545	Request			
59	10.61.208.243	10.48.67.229	0CSP	337	Response			
4								
▶ Frame 59: 337 bytes on wire (2696 bits), 337 bytes captured (2696 bits)								
Ethernet II, Src: Cisco_2a:c4:a3 (00:06:f6:2a:c4:a3), Dst: Cisco b8:6b:25 (00:17:5								
▶ In	Internet Protocol Version 4, Src: 10.61.208.243 (10.61.208.243), Dst: 10.48.67.229							
▶ Tr	ansmission Control P	rotocol, Src Port: h	ttp (80)	, Dst P	ort: 14489 (1	.4489), Seq		
▶ Hy	pertext Transfer Pro	tocol						
▼ 0n	Online Certificate Status Protocol							
responseStatus: unauthorized (6)								

Autenticación del servidor IIS7

Los problemas con una solicitud SCEP/OCSP suelen ser el resultado de una autenticación incorrecta en Internet Information Services 7 (IIS7). Asegúrese de que el acceso anónimo esté configurado:

File View Help									
Connections	Authentication								
 DC (TEST-CISCO\Administrat Application Pools Sites Opfault Web Site Opfault Web Site	Name Anonymous Authentication ASP.NET Impersonation Basic Authentication Digest Authentication Forms Authentication Windows Authentication	Status Enabled Disabled Disabled Disabled Disabled	Response Type HTTP 401 Challenge HTTP 401 Challenge HTTP 302 Login/Redirect HTTP 401 Challenge						

Información Relacionada

- Microsoft TechNet: Guía de instalación, configuración y solución de problemas de Online <u>Responder</u>
- Microsoft TechNet: configuración de una CA para admitir responsables de OCSP
- <u>Referencia de Comandos de la Serie ASA de Cisco</u>
- Soporte Técnico y Documentación Cisco Systems

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).